Algebraic Number Theory (Math 223b)

0. Overview

0.1. Geometry and arithmetic of curves

Let $C \subset \mathbb{P}^m$ be an irreducible smooth projective curve defined ~~over~~ $\mathbb{Q}$.

What can we say about $C(\mathbb{Q})$?

Question: Is $C(\mathbb{Q})$ infinite?

Def: The height of a point $p = [x_0 : \dots : x_m] \in \mathbb{P}^m(\mathbb{Q})$ with $x_0, \dots, x_m \in \mathbb{Z}$, $\gcd(x_0, \dots, x_m) = 1$ is $H(p) = \max(|x_0|, \dots, |x_m|) \geq 1$.

Question: If $C(\mathbb{Q})$ is infinite, how quickly does $\#\{p \in C(\mathbb{Q}) \mid H(p) \leq T\}$ grow as $T \to \infty$?

Example: $C = \mathbb{P}^1$ $\quad \boxed{g=0}$

$\# C(\mathbb{Q}) = \infty$

$$\#\{p \in C(\mathbb{Q}) \mid H(p) \leq T\} = \underbrace{\#\{(x,y) \in \mathbb{Z}^2 \mid |x|,|y| \leq T, \gcd(x,y)=1\}}_{2}$$

$$\asymp T^2 \quad \text{as } T \to \infty \qquad (I)$$

$A \asymp B$ means that $\exists\, C, D > 0$: $|A| \geq C \cdot |B|$, $|B| \geq D \cdot |A|$ for sufficiently large T

__Example__ Circle $C=\{[x:y:z] \mid x^2+y^2=z^2\}\subseteq \mathbb{P}^2$

There are ∞ many Pythagorean triples (x,y,z) with $\gcd(x,y,z)=1$.

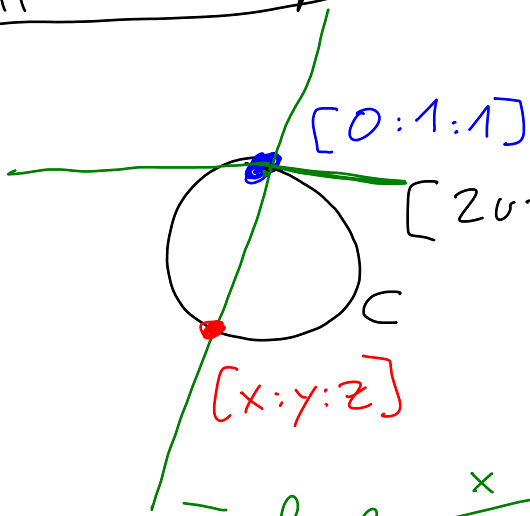
$\boxed{g=0}$

$\Rightarrow \#C(\mathbb{Q})=\infty$.

Geometric explanation: $C \cong \mathbb{P}^1$ over $\mathbb{Q}$

$\Rightarrow C(\mathbb{Q}) \longleftrightarrow \mathbb{P}^1(\mathbb{Q})$

__Affine ($z=1$) picture__



$[x:y:z] \longmapsto [x:y-z]$ (unless $x=y-z=0$)

$=[y+z:-x]$ (unless $y+z=-x=0$)

$[2ut:u^2-t^2:-u^2-t^2] \longleftarrow [t:u]$

$-$ slope $\dfrac{x}{y-z} = \dfrac{y+z}{-x}$

$\gcd(2ut,\ u^2-t^2,\ -u^2-t^2)$

$\mid \gcd(2u^2, 2t^2)=2$ if $\gcd(t,u)=1$.

$\max(|2ut|, |u^2-t^2|, |-u^2-t^2|) \asymp \max(|t|,|u|)^2$

$\Rightarrow H([2ut:\dots]) \asymp H([t:u])^2$

$\overset{(I)}{\Rightarrow} \#\{p\in C(\mathbb{Q}) \mid H(p)\leq T\} \asymp T$

Example $C = \{x^2 + y^2 = -z^2\} \subseteq \mathbb{P}^2$

$C(\mathbb{Q}) = \emptyset$

$\boxed{g = 0}$

Here, $C \cong \mathbb{P}^1$ over $\mathbb{C}$, but $C \not\cong \mathbb{P}^1$ over $\mathbb{Q}$.
(same argument as before)

"Geometry over $\mathbb{C}$" $\neq$ "Geometry over $\mathbb{Q}$".

Example Fermat curve $C = \{X^3 + Y^3 = Z^3\} \subseteq \mathbb{P}^2$

$C(\mathbb{Q}) = \{[0:1:1], [1:0:1], [1:-1:0]\}$. $\boxed{g=1}$

This was proved using <u>infinite descent</u>:

Consider any other point $p \in C(\mathbb{Q})$ with minimal height $H(p)$. You can use it to construct a point $q \in C(\mathbb{Q})$ with $H(q) < H(p)$. $\lightning$

Example Fermat curve $C = \{X^n + Y^n = Z^n\} \subseteq \mathbb{P}^2$

$C(\mathbb{Q}) = \{[0:1:1], [1:0:1], [1:-1:0]\}$ for $n \geq 4$

This is Fermat's Last Theorem (Wiles 1995).

$$\boxed{g = \frac{(n-1)(n-2)}{2} \geq 3}$$

<u>Example</u> $C = \{3X^3 + 4Y^3 + 5Z^3 = 0\}$

$C(\mathbb{Q}) = \emptyset$ although $C(\mathbb{Q}_p) \neq \emptyset$ $\forall p$ and $C(\mathbb{R}) \neq \emptyset$

(Selmer, 1951) $\boxed{g=1}$

<u>Example</u> Elliptic curve $C = \{X^3 - 5XZ^2 = Y^2 Z\} \subseteq \mathbb{P}^2$

$\# C(\mathbb{Q}) = \infty$

$\# \{P \in C(\mathbb{Q}) \mid H(P) \leq T\} \asymp (\log T)^{1/2}$ $\boxed{g=1}$

<u>Example</u> (Elkies, Klagsbrun) $C = \ldots$ ell. curve

$\# C(\mathbb{Q}) = \infty$

$\# \{ \ldots \} \asymp (\log T)^{20/2}$. $\boxed{g=1}$

What does this have to do with algebraic geometry? A geometric invariant of C is its <u>genus</u> $g \geq 0$.

Thm If $g=0$, then either

a) $C(\mathbb{Q})=\emptyset$ or

b) $C \cong \mathbb{P}^1$ over $\mathbb{Q}$

$\#C(\mathbb{Q})=\infty$

$\#\{p\in C(\mathbb{Q}) \mid H(p)\le T\} \asymp T^{\alpha}$ for some $\alpha>0$.

Idea of pf as for the circle curve. $\square$

Thm If $g=1$, then either

a) $C(\mathbb{Q})=\emptyset$ or

b) $\#\{p\in C(\mathbb{Q}) \mid H(p)\le T\} \asymp (\log T)^{r/2}$

for some $r\in \mathbb{Z}_{\ge 0}$.

(Note: $\#C(\mathbb{Q})<\infty \iff r=0$.)

Idea of pf

- Pick a point $O\in C(\mathbb{Q})$.
- Geometrically construct a abelian group operation + on $C(\mathbb{Q})$ with identity O. ("Elliptic curve").
- Show that the group $C(\mathbb{Q})$ is finitely generated (Mordell-Weil Theorem).
- $r := \mathrm{rk}(C(\mathbb{Q})) \rightsquigarrow C(\mathbb{Q}) \cong \mathbb{Z}^r \times (\text{fin. grp.})$
- Show that $\log H \approx$ quadratic form on $C(\mathbb{Q}) \approx \mathbb{Z}^r \times (\text{fin. grp})$ $\square$

Thm (Faltings, 1983) Vojta, Bombieri
If $g \geq 2$, then $\# C(\mathbb{Q}) < \infty$.

Idea of pf. Assume $C(\mathbb{Q}) \neq \emptyset$. There is no good "geometric" group operation on $C(\mathbb{Q})$.

But we can embed C into a smooth projective g-dimensional variety $J \subseteq \mathbb{P}^s$ (the Jacobian variety of C) with a geometrically defined group operation $+$ on $J(\mathbb{Q})$.

$$C(\mathbb{Q}) \subseteq \underbrace{J(\mathbb{Q})}_{\substack{\text{finitely generated abelian group} \\ \text{(Mordell-Weil Theorem)}}}$$

If $J(\mathbb{Q})$ is finite, we're done!

$J(\mathbb{Q})$ has "few" points:
$$\#\{D \in J(\mathbb{Q}) \mid H(D) \leq T\} \approx (\log T)^{r/2}$$
for some $r \geq 0$.

You wouldn't expect many to satisfy the equations defining the 1-dimensional subvariety C of J. Use heavy machinery/ diophantine approximation to prove there are only finitely many such points. $\square$

0.2 Diophantine Approximation

"How well can you approximate a given real number α by rational numbers?"

<u>Thm</u> A rational number $\frac{p}{q}$ (with $\gcd(p,q)=1$) satisfies $|p - q\alpha| < |p' - q'\alpha|$ for all $\frac{p'}{q'} \neq \frac{p}{q}$ with $|q'| \leq |q|$ if and only if $\frac{p}{q}$ is the result of a truncation of the continued fraction expansion of α. (A <u>convergent</u>.)

<u>Rmk</u> Replacing the inequality $|p - q\alpha| < |p' - q'\alpha|$ by $\left|\frac{p}{q} - \alpha\right| < \left|\frac{p'}{q'} - \alpha\right|$, you get slightly more such numbers $\frac{p}{q}$ (still arise from the continued fraction expansion of α).

<u>Question</u> How quickly do the "best" approximations $\frac{p}{q}$ with $|q| \leq N$ converge to α as $N \to \infty$?

Dirichlet's Approximation Theorem

For any $\alpha \in \mathbb{R}$ and $N \geq 1$, there is some $\frac{p}{q} \in \mathbb{Q}$ with $|q| \leq N$ and $|p - q\alpha| < \frac{1}{N}$.

Pf HW. $\square$

Roth's Theorem

For any algebraic number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and any $\varepsilon > 0$, there is a constant $C > 0$ such that

$$|p - q\alpha| > \frac{C}{|q|^{1+\varepsilon}} \text{ for any } \frac{p}{q} \in \mathbb{Q}.$$

Rmk False for $\alpha \in \mathbb{Q}$.

Rmk False for $\varepsilon = 0$ by Dirichlet's Approx Thm.

Rmk False for some transcendental numbers $\alpha \in \mathbb{R}$.

Take $\alpha = \sum_{i=1}^{\infty} 2^{-a_i}$ with $a_1 < a_2 < \dots \longrightarrow \infty$ very quickly.

Thue's Theorem

Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a squarefree homogeneous degree n polynomial.
Consider its n roots in $\mathbb{P}^1(\mathbb{C})$.
Assume one of the following:
a) f has root in $\mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$.
b) $n \geq 3$.

Then, for any $r \in \mathbb{Q}^\times$, there are only finitely many solutions $(x,y) \in \mathbb{Z}^2$ to the Thue equation
$$f(x,y) = r.$$

Ex $f(X,Y) = X^2 + Y^2$ satisfies a)
$x^2 + y^2 = r$ has only fin. many sol. $(x,y) \in \mathbb{Z}^2$.
($\exists$ fin. many $z = x + iy \in \mathbb{Z}[i]$ with $N(z) = r$)

Ex $f(X,Y) = X^2 - 3Y^2$ doesn't satisfy a) or b)
$x^2 - 3y^2 = 1$ has ∞ many sol. $(x,y) \in \mathbb{Z}^2$
(corr. to $z \in x + \sqrt{3}y \in \mathbb{Z}[\sqrt{3}]$ with $N(z) = 1$, so at least any $z \in \mathbb{Z}[\sqrt{3}]^{\times 2}$).

Pf using Roth's Theorem assuming f has $n \geq 3$ roots in $\mathbb{P}^1(\mathbb{R}) \setminus \mathbb{P}^1(\mathbb{Q})$

W.l.o.g. the X^n-coeff. in $f(X,Y)$ is 1.

Write $f(X,Y) = (X - \alpha_1 Y) \cdots (X - \alpha_n Y)$ with distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{R} \setminus \mathbb{Q}$.

$$|X - \alpha_i Y| + |X - \alpha_j Y| \geq |\alpha_i - \alpha_j| \cdot |Y| \quad \forall i,j$$

$$\Rightarrow |X - \alpha_i Y| \text{ or } |X - \alpha_j Y| \geq \frac{|\alpha_i - \alpha_j|}{2} \cdot |Y| \quad \forall i,j$$

$$\Rightarrow |X - \alpha_k Y| \geq D \cdot |Y| \text{ with } D = \frac{1}{2} \min_{i \neq j} |\alpha_i - \alpha_j|$$

for all but at most one index k.

But $\prod_{i=1}^{n} (X - \alpha_i Y) = f(X,Y) = r$, so

$$\frac{C}{|Y|^{1.5}} \leq |X - \alpha_l Y| \leq \frac{|r|}{(D \cdot |Y|)^{n-1}}$$

for the remaining index l.

$$\Rightarrow |Y|^{n-2.5} < \frac{|r|}{C \cdot D^{n-1}} \Rightarrow |Y| \text{ is bounded}$$

$\Rightarrow |X|$ is bounded. $\square$

1. Varieties (Review of Algebraic Geometry)

1.1. Affine varieties

Let k be a field.

Def To an ideal $I \subseteq k[x_1, \dots, x_n]$, we associate the set of zeros

$$V(I) = \{(x_1, \dots, x_n) \in \overline{k}^n \mid f(x_1, \dots, x_n) = 0 \ \forall f \in I\}.$$

Def An affine variety defined over k is a set $X \subseteq \overline{k}^n$ of the form $X = V(I)$ with $I \subseteq k[x_1, \dots, x_n]$.

We write $X \subseteq \mathbb{A}^n_k$.

Def For $X \subseteq \mathbb{A}^n_k$, we write

$$X(k) = X \cap k^n.$$

$$X(\overline{k}) = X$$

Ex $k = \mathbb{R}$, $n = 1$, $I = (x^2+1)$

$\Rightarrow V(I) = \{\pm i\} \subseteq \mathbb{A}^1_{\mathbb{R}}$ is an affine variety over $\mathbb{R}$

$I' = (1) \Rightarrow V(I') = \emptyset$

$V(I) \neq V(I')$, but $\underbrace{V(I)(\mathbb{R})}_{=\emptyset} = \underbrace{V(I')(\mathbb{R})}_{=\emptyset}$

But $\{i\}$ isn't an affine variety over $\mathbb{R}$, but is an affine variety over $\mathbb{C}$.

<u>Def</u> An affine variety $X \neq \emptyset$ over K is <u>irreducible</u> if we can't write $X = X_1 \cup X_2$ with affine varieties $X_1, X_2 \subsetneq X$ over K.

<u>Rmk</u> "irreducible over K" $\overset{\Leftarrow}{\not\Rightarrow}$ "irreducible over $\overline{K}$"

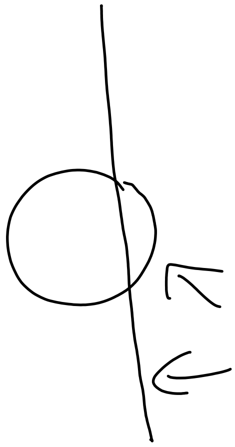
E.g. $V(x^2+1) = \{\pm i\}$ is irreducible ~~over~~ $\mathbb{R}$ (because x^2+1 is)

but not irreducible over $\mathbb{C}$

<u>Def</u> ~~Ir~~reducible over $\overline{K}$ is called <u>geometrically irreducible</u>.

<u>Lemma/Def</u> Any affine variety X over K can be written uniquely as $X = X_1 \cup \dots \cup X_r$ with $X_1, \dots, X_r$ irreducible and $X_i \not\subseteq X_j$ $\forall i,j$.
The $X_1, \dots, X_r$ are called the <u>irreducible components</u> of X.

Exe $I\big((x^2+y^2-1)(x-\tfrac{1}{2})\big)$



Def The closed subsets of $\overline{K}^n$ w.r.t. the Zariski topology over K are the affine varieties $X \subseteq \overline{K}^n$ over K.
We equip any affine variety $X \subseteq \overline{K}^n$ with the subspace topology.

Def To an affine variety $X \subseteq \mathbb{A}^n_K$, we associate the vanishing ideal

$$I(X)=\{f\in K[x_1,\dots,x_n] \mid f(P)=0 \ \forall P\in X(\overline{K})\}.$$

Rmk (Hilbert's Nullstellensatz)

$$I(V(J))=\sqrt{J},$$ the radical of J:

$$\sqrt{J}=\{f\in K[x_1,\dots,x_n] \mid f^n\in J \text{ for some } n\geq 1\}.$$

Rmk $I(X)$ is a radical ideal:

if $f^n\in I(X)$, then $f\in I(X)$.

1.2. Rings of functions

Def The *coordinate ring* of an affine variety X over K is

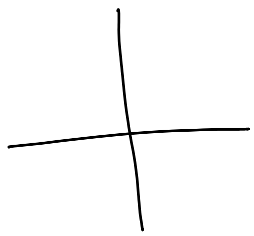
$$\Gamma(X) = \Gamma(X, \mathcal{O}_X) = \mathcal{O}_X(X) := K[x_1, \dots, x_n]/I(X).$$

Its elements are the *(regular) functions* on X.

Rmk $\mathcal{O}_X(X)$ is *reduced*: has no nilpotent elements $f \neq 0$.

Rmk $\mathcal{O}_X(X)$ is an integral domain if and only if X is irreducible.

Ex $X = V(x_1 x_2) \subseteq \mathbb{A}^2$ is not irreducible



$\mathcal{O}_X(X) = K[x_1, x_2]/(x_1 \cdot x_2)$ is not an integral domain

Def If X is irreducible, its *field of rational functions* $K(X)$ is the field of fractions of $\mathcal{O}_X(X)$.

Def An element $t \in K(X)$ is <u>defined at</u> $P \in X(\overline{K})$ if we can write $t = \frac{f}{g}$ with $f, g \in \mathcal{O}_X(X)$ and $g(P) \neq 0$.

Ex $X = V(xy - z^2) \subseteq \mathbb{A}^3_K$

$$\mathcal{O}_X(X) = K[x, y, z]/(xy - z^2)$$

The rational functions $\frac{x}{z}$ and $\frac{z}{y}$ on X are the same! $\left(xy = z^2 \Rightarrow \frac{x}{z} = \frac{z}{y} \right)$.

$t = \frac{x}{z} = \frac{z}{y}$ is defined everywhere on X except at the points with $y = z = 0$.

Def Let $X \subseteq \mathbb{A}^n_K$ be irreducible.

For an open subset $\emptyset \neq U \subseteq X$, the ring of rationals functions on X defined on U is

$$\Gamma(U, \mathcal{O}_X) = \mathcal{O}_X(U) := \{ t \in K(X) \mid t \text{ defined at } P \ \forall P \in U(\overline{K}) \}$$

$$\Gamma(\emptyset, \mathcal{O}_X) = \mathcal{O}_X(\emptyset) = 0$$

Rmk $\emptyset \neq U \subseteq U' \subseteq X \Rightarrow \mathcal{O}_X(U) \supseteq \mathcal{O}_X(U')$.

Rmk $$K(X) = \bigcup_{\substack{\emptyset \neq U \subseteq X \\ \text{open}}} \mathcal{O}_X(U)$$

Rmk $\mathcal{O}_X$ is called the sheaf of functions on X.

Rmk For $U = X$, this agrees with the previous definition $\Gamma(X) = \mathcal{O}_X(X) = k[x_1, \dots, x_n]/I(X)$.

Def For an irreducible closed $Y \subseteq X$ (e.g. a point in $X(k)$), the ring of rational functions on X defined around Y is
$$\mathcal{O}_{X,Y} := \{ t \in K(X) \mid t \text{ defined at } P \ \forall P \in Y(\bar{k}) \}.$$

Rmk $Y \subseteq Y' \subseteq X \Rightarrow \mathcal{O}_{X,Y} \supseteq \mathcal{O}_{X,Y'}$

Rmk $$\mathcal{O}_{X,Y} = \bigcup_{\substack{Y \subseteq U \subseteq X \\ \text{open}}} \mathcal{O}_X(U)$$

1.3. Dimension

Def The <u>dimension</u> of an irreducible affine variety V is the transcendence degree of the field $K(V)$.

Rmk $V(\overline{K})$ is a finite set if and only if $\dim(V)=0$.

Def
- V is a <u>curve</u> if $\dim(V)=1$.
- <u>surface</u> if $\dim(V)=2$.

Ex $V=V(x^2+1)\subset \mathbb{A}^1_{\mathbb{R}}$ irred.

$V(\mathbb{R})=\emptyset$, $V(\mathbb{C})=\{\pm i\}$.

$\Gamma(V)=\mathcal{O}_V(V)=\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$

$K(V)=\mathbb{C}$ alg. extension of $\mathbb{R}$

$\Rightarrow \dim(V)=$ transcendence degree $=0$.

Ex $V = V(0) \subset \mathbb{A}^1_k$ irred.

$\Gamma(V) = \mathcal{O}_V(V) = k[X]$

$k(V) = k(X)$

$\Rightarrow \dim(V) =$ transcendence degree $= 1$.

$U = V \setminus \{a_1, \dots, a_r\}$ $(a_1, \dots, a_r \in k)$

$$\Rightarrow \mathcal{O}_V(U) = \left\{ \frac{f}{(X-a_1)^{e_1} \cdots (X-a_r)^{e_r}} \;\middle|\; f \in k[X],\ e_1, \dots, e_r \geq 0 \right\}.$$

$Z = \{a\}$ $(a \in k)$

$$\Rightarrow \mathcal{O}_{V,Z} = \left\{ \frac{f}{g} \;\middle|\; f, g \in k[X],\ g(a) \neq 0 \right\}.$$

Ex $V = V(X^2 + Y^2 - 1) \subset \mathbb{A}^2_k$ irred.

$\mathcal{O}_V(V) = k[X,Y]/(X^2+Y^2-1)$

$k(V) =$ quotient field of $\mathcal{O}_V(V)$

$= k(X)[Y]/(X^2+Y^2-1)$

$\Rightarrow \dim(V) =$ tr. deg $= 1$.

1.4. Morphisms

From now on, assume that the field K is perfect (every alg. ext. of K is separable), e.g. $\mathrm{char}(K) = 0$.

Def Let $V \subseteq \mathbb{A}^n_K$ and $W \subseteq \mathbb{A}^m_K$.

A *morphism* $f : V \to W$ is a map

$$f : V(\overline{K}) \longrightarrow W(\overline{K})$$

which is given by regular functions: There exist $f_1, \dots, f_m \in \Gamma(V)$ such that

$$f(x) = (f_1(x), \dots, f_m(x)) \in \mathbb{A}^m_K \quad \forall x \in V(\overline{K}).$$

Rmk We obtain a K-algebra hom.

$$\begin{array}{cccc} f^* : & \Gamma(W) & \longrightarrow & \Gamma(V) \\ & \| & & \| \\ & K[Y_1, \dots, Y_m]/I(W) & & K[X_1, \dots, X_n]/I(V) \\ & Y_i & \longmapsto & f_i \end{array}$$

sending $a \in \Gamma(W)$ to $a \circ f \in \Gamma(V)$.

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[dr, "a \circ f = f^*(a)"'] & W \arrow[d, "a"] \\ & \mathbb{A}^1_K \end{tikzcd}$$

Rmk We get a bijection

$$\{\text{morphism } f: V \to W\} \longleftrightarrow \{K\text{-alg. hom. } \Gamma(W) \to \Gamma(V)\}.$$

Ex If $W(\overline{K})$ consists of just one point, then $W(K) = W(\overline{K})$.

There is exactly one morphism $V \to W$ for any V.

$$\Gamma(W) = K[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n) = K.$$

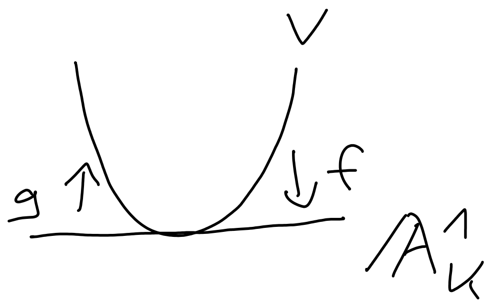
if $W(K) = \{a_1, \dots, a_n\}$.

Ex We have a bij.

$$\{\text{morphism } f: V \to \mathbb{A}^n_K\} \longleftrightarrow \{(f_1, \dots, f_m) \mid f_i \in \Gamma(V)\}.$$

Ese $f: \mathbb{A}^n_k \longrightarrow \mathbb{A}^m_k$ any linear map.

Ese Let $V = V(Y_2 - Y_1^2) \subset \mathbb{A}^2_K$

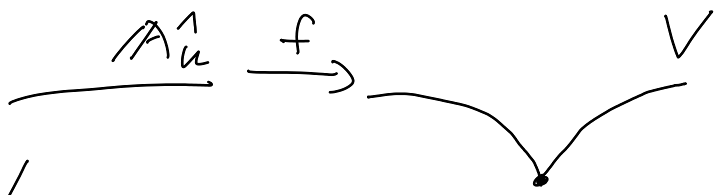


$$f: V \longrightarrow \mathbb{A}^1_K$$
$$(y_1, y_2) \longmapsto y_1$$

is an isomophism with inverse

$$g: \mathbb{A}^1_k \longrightarrow V$$
$$x \longmapsto (x, x^2)$$

Ese Let $V = V(Y_1^2 - Y_3^3) \subset \mathbb{A}^2_k$



$$f: \mathbb{A}^1_k \longrightarrow V$$
$$x \longmapsto (x^3, x^2)$$

is a morphism.

The map $f: \mathbb{A}^1_k(L) \longrightarrow V(L)$, where $\mathbb{A}^1_k(L) = L$ and $V(L) = \{(y_1, y_2) \in L^2 \mid y_1^2 = y_2^3\}$,

is a bijection for any field $K \subseteq L \subseteq \overline{K}$.

But f is not an isomorphism: The k-alg. hom.

$$f^*: k[Y_1, Y_2]/(Y_1^2 - Y_2^3) \longrightarrow k[X]$$
$$Y_1 \longmapsto X^3$$
$$Y_2 \longmapsto X^2$$

isn't surjective! (The image doesn't contain X.)

This has to do with the tangent space of V at $(0,0)$.

1.5. Tangent spaces

Def The tangent space to $V = V(I) \subset \mathbb{A}^n_K$ at a point $P \in V(K)$ is the K-vector space

$$T_{V,P} := \bigcap_{f \in I} \ker(Df(P)) \subseteq K^n$$

where $Df(P) : K^n \longrightarrow K$ is the Jacobian map of f at P. ("derivative")

Rmk It suffices to consider generators $f_1, \dots, f_r$ of the ideal I.

Pf (sketch)

Product rule: $Dfg(P) = \underbrace{f(P)}_{0} \cdot Dg(P) + g(P) \cdot Df(P)$

for $f \in I$, $g \in K[x_1, \dots, x_n]$

$\Rightarrow$ If $Df(P)(a) = 0 \Rightarrow Dfg(P)(a) = 0$. $\square$

Def Its dual $T^*_{V,P}$ is the cotangent space.

Rmk[A] $T^*_{V,P} = (K^n)^* / \{Df(P) \mid f \in I\}$

(as a K-vector space).

Pf Every lin. fct. $T_{V,P} \to K$ is the restriction of a lin. fct. $t : K^n \to K$.
The restriction of t to $T_{V,P}$ is zero if and only if for all $a \in K^n$:

If $Df(P)(a) = 0 \ \forall f \in I$, then $t(a) = 0$.

This is equivalent to

$t \in$ span of $\{Df(P) \mid f \in I\}$

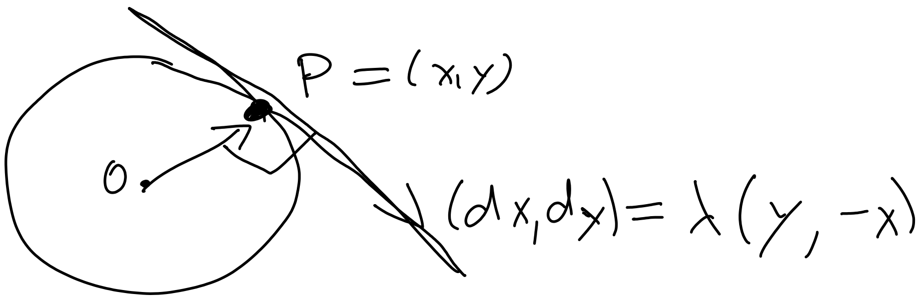
$= \{Df(P) \mid f \in I\}$. $\square$

Ex $V = V(0) = \mathbb{A}^n_K$

$\Rightarrow T_{V,P} = K^n$.

Ex $V = V(\underbrace{x^2+y^2-1}_{f}) \subset \mathbb{A}^2_k$

$P=(x,y) \in V(k)$ $\qquad (x^2+y^2=1)$



$Df(P): k^2 \longrightarrow k$

$(dx,dy) \longmapsto 2x\,dx + 2y\,dy$

$\Rightarrow T_{V,P} = \ker(Df(P))$

$= \{(dx,dy) \in k^2 \mid x\,dx + y\,dy = 0\}$

$= \{(a,b) \in k^2 \mid xa + yb = 0\}$

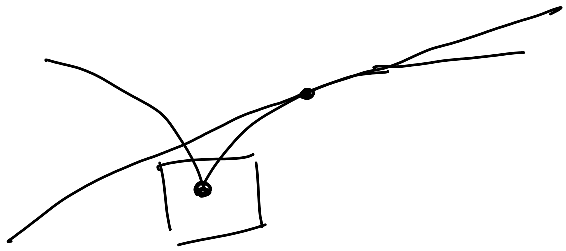
$= \langle (y,-x) \rangle_k$

x or y ≠ 0

$T^*_{V,P} = \langle \underbrace{dx, dy}_{\text{standard basis of } (k^2)^*} \rangle \Big/ \langle x\,dx + y\,dy \rangle$

Ex $V = V(x^2 - y^3) \subset \mathbb{A}^2_K$

$P = (x,y) \in V(K) \qquad (x^2 = y^3)$



$Df(P) : K^2 \longrightarrow K$

$(dx, dy) \longmapsto 2x\,dx - 3y^2\,dy$

$$\Rightarrow T_{V,P} = \begin{cases} \langle (3y^2, 2x) \rangle, & x, \cancel{y} \neq 0 \\ K^2, & x = y = 0 \end{cases}$$

Rmk If $V \subseteq \mathbb{A}^n_K$ is irreducible, then $\dim(T_{V,P}) \geq \dim(V)$ $\forall P \in V(\overline{K})$.

Def An irreducible variety $V \subseteq \mathbb{A}^n_K$ is smooth if $\dim(T_{V,P}) = \dim(V)$ $\forall P \in V(\overline{K})$.

Otherwise, V is singular. The points P with $\dim(T_{V,P}) > \dim(V)$ are the singular points of V.

Ex $V(X^2+Y-1)\subset \mathbb{A}^2_K$ is smooth

Ex $(0,0)$ is the singular point of

$$V(X^2-Y^3)\subset \mathbb{A}^2_K.$$

Def We denote the vanishing ideal of a point $P=(a_1,\dots,a_n)\in K^n$ by

$$m_P=(X_1-a_1,\dots,X_n-a_n).$$

If $V\subseteq \mathbb{A}^n_K$ and $P\in V(K)$, so $m_P\supseteq I(V)$, we let $m_{V,P}\subseteq \Gamma(V)$ be the image of m_P in $\Gamma(V)=K(X_1,\dots,X_n)/I(V)$.
(It's an ideal of $\Gamma(V)$.)

Thm There's a natural isomorphism

$$m_{V,P}/m^2_{V,P}\cong T^*_{V,P}$$

of K-vector spaces.

<u>Pf</u> W.l.o.g. $P=(0,\ldots,0)$.

$m_P=(x_1,\ldots,x_n)$.

$$m_{V,P}/m_{V,P}^2 \cong m_P/(I(V)+m_P^2)$$

$$=(x_1,\ldots,x_n)/(I(V)+(x_1^2,x_1x_2,\ldots,x_n^2))$$

We have $f(P)=0\ \forall f\in I(V)$.

Consider

$$J=\left\{\sum_i \frac{\partial f}{\partial x_i}(P)\cdot x_i \;\middle|\; f\in I(V)\right\}$$

the set of linearizations of elements of $I(V)$.
(k-vector space)

$$\Rightarrow m_{V,P}/m_{V,P}^2 \cong (x_1,\ldots,x_n)/((J)+(x_1^2,x_1x_2,\ldots))$$

$$=\langle x_1,\ldots,x_n\rangle/J$$

$$=T_{V,P}^*.$$

Remk A

Cor For any morphism $f: \underset{\mathbb{A}^n_k}{\overset{\cap}{V}} \longrightarrow \underset{\mathbb{A}^m_k}{\overset{\cap}{W}}$ and

any point $P \in V(k)$, the map

$$f^* : \Gamma(W) \longrightarrow \Gamma(V)$$

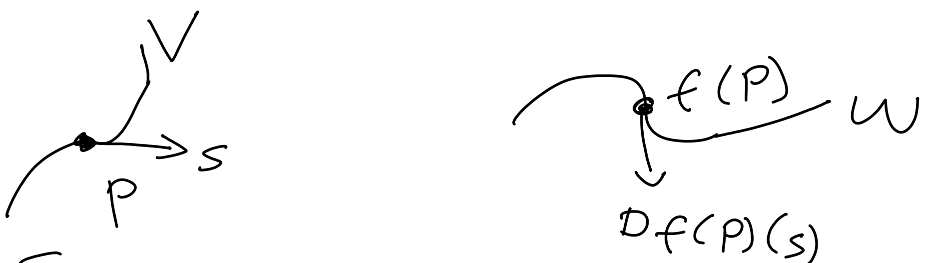
induces a (well-defined!) linear map

$$Df^*(P) : \underset{\displaystyle m_{W,f(P)}/m_{W,f(P)}^2}{\overset{\|}{T^*_{W,f(P)}}} \longrightarrow \underset{\displaystyle m_{V,P}/m_{V,P}^2}{\overset{\|}{T^*_{V,P}}}$$

and therefore a dual map

$$Df(P) : T_{V,P} \longrightarrow T_{W,f(P)}$$

(the derivative of f at P).



Rmk For any (Zariski) open neighborhood U of P, if you let $n = m_{V,P}\,\mathcal{O}_V(U)$ be the ideal of $\mathcal{O}_V(U)$ generated by $m_{V,P}$, then $n/n^2 \cong T^*_{V,P}$.

Same with $\mathcal{O}_{V,P}$ instead of $\mathcal{O}_V(U)$!

("Tangent spaces only depend on points close to U").

Rmk This explains why $f: \mathbb{A}^1_k \to V = V(y_1^2 - y_2^3) \subseteq \mathbb{A}^2_k$
$x \mapsto (x^3, x^2)$

isn't an isomorphism:

The derivative $Df(0): \underset{\overset{\parallel}{k}}{T_{\mathbb{A}^1,0}} \longrightarrow \underset{\overset{\parallel}{k^2}}{T_{V,(0,0)}}$

isn't an isomorphism.

Thm Let $V \subseteq \mathbb{A}^n_k$ be a smooth curve and let $P \in V(k)$. Then, the ring $\mathcal{O}_{V,P}$ is a discrete valuation ring with maximal ideal $m_{V,P}\,\mathcal{O}_{V,P}$ of functions vanishing at P. We denote the valuation by v_P.

Intuitively, $v_P(f)$ is the multiplicity of the root of f at P.

An element f of $\mathcal{O}_{V,P}$ with $v_P(f) = 1$, is called a uniformiser at P.

Rmk $f \in \mathcal{O}_{V,P}$ is a uniformiser at P if and only if $f(P) = 0$ and $\underbrace{Df(P)}_{\text{map } T_{V,P} \longrightarrow T_{\mathbb{A}^1,0}} \neq 0$.

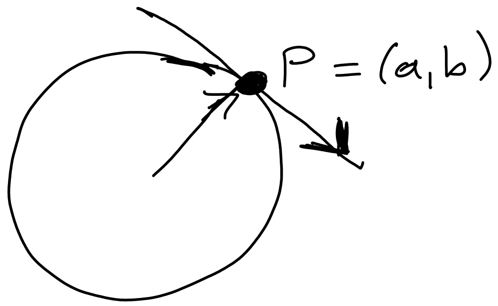
$T_{V,P} \cong k$, $T_{\mathbb{A}^1,0} \cong k$

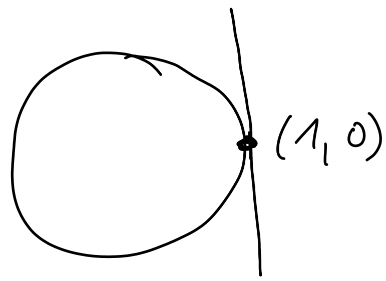
Ese $V = V(X^2+Y^2-1) \subseteq \mathbb{A}^1_k$

$P = (a, b) \in V \qquad a^2+b^2 = 1$

$f = X - a$ is a uniformizer at P

if and only if $b \neq 0$.





$T_{V,P} = \langle (b, -a) \rangle$

If $P = (1,0)$, then $V_P(X-1) = 2$:

$Y - 0$ is a uniformizer at P (same reason as before) and

$$\frac{X-1}{Y^2} \underset{\boxed{X^2+Y^2-1=0}}{=} \frac{X-1}{1-X^2} = -\frac{1}{X+1},$$

which has value $-\frac{1}{2} \neq 0$ at $P = (1,0)$.

$$\Rightarrow V_P\left(\frac{X-1}{Y^2}\right) = 0$$

$$\| $$

$$V_P(X-1) - 2V_P(Y) = V_P(X-1) - 2.$$

$xb - ya$ is always a uniformiser at any point $P = (a, b)$.

1.6. Differentials

Def Let A be a k-algebra. Its module of differentials is the quotient

$\Omega_k(A) = F/Q$, where F is the free A-module with basis $([x])_{x \in A}$ and $Q \subseteq F$ is the submodule generated by elements of the following forms:

a) $[x+y] - [x] - [y]$ with $x, y \in A$

b) $[\lambda x] - \lambda [x]$ with $\lambda \in k$, $x \in A$

c) $[xy] - x[y] - y[x]$ with $x, y \in A$.

The image of $[x]$ in $\Omega_k(A)$ is called dx.

Rmk
$$\left.\begin{array}{l} a)\ d(x+y) = dx + dy \\ b)\ d(\lambda x) = \lambda dx \\ c)\ d(xy) = x dy + y dx \end{array}\right\}$$
(Define differentiation for polynomials)

Thm $\Omega_k(k[x_1,\dots,x_n])$ is the free $k[x_1,\dots,x_n]$-module with basis $dx_1,\dots,dx_n$.

We have $df = \frac{\partial f}{\partial x_1}\cdot dx_1 + \dots + \frac{\partial f}{\partial x_n}\cdot dx_n$.

Thm Let $A = k[x_1,\dots,x_n]/I$ for any ideal I of $k[x_1,\dots,x_n]$. Then, $\Omega_k(A) = F'/Q'$, where F' is the free A-module with basis $dx_1,\dots,dx_n$ and Q' is the A-module

$$Q' = \{ df \quad | f\in I\}$$

Pf HW $\square$

Rmk If $I = (f_1,\dots,f_m)$, then Q' is generated by $df_1,\dots,df_m$.

Ex $\Omega_k(k[x,y]/(x^2+y^2-1))$

$=$ (free mod. with basis (dx, dy)) / (module gen. by $2x\,dx+2y\,dy$).

Def Let $V \subseteq \mathbb{A}^n_K$, $I = I(V)$

and $r \in \Omega_K(\underbrace{\Gamma(V)}_{K[X_1,\dots,X_n]/I})$

$$\| \qquad g_1(X)\,dX_1 + \dots + g_n(X)\,dX_n$$

$(g_i \in K[X_1,\dots,X_n]/I)$.

To any point $P \in V(K)$, we can then associate the element

$$\underbrace{g_1(P)}_{\in K}\,dX_1 + \dots + \underbrace{g_n(P)}_{\in K}\,dX_n$$

of the cotangent space $T^*_{V,P}$

(where we identify dX_i with the map $K^n \longrightarrow K$ as before).

$(y_1,\dots,y_n) \longmapsto y_i$

Def Let $V \subseteq \mathbb{A}^n_K$ be irreducible. For any open $U \subseteq V$, let $\Gamma(U, \Omega_V) = \Omega_V(U)$

$$:= \Omega_K(\mathcal{O}_V(U))$$

("set of rational differentials defined at every point in U") (Ω_K = "cotangent bundle")

Rmk $\Omega_V(U) = \Omega_V(V) \otimes_{\mathcal{O}_V(V)} \mathcal{O}_V(U)$.

Rmk For any morphism $f: V \to W$
$$\begin{array}{ccc} V & \longrightarrow & W \\ \cap & & \cap \\ \mathbb{A}^n_K & & \mathbb{A}^m_K \end{array}$$

and any open $U \subseteq W$, we obtain a map $Df^*: \Omega_W(U) \to \Omega_V(\underbrace{f^{-1}(U)}_{\subseteq V \text{ open}})$.

1.7. Projective varieties

<u>Def</u> The n-dimensional <u>projective space</u> $\mathbb{P}^n_K$ over K is the set of lines through the origin in $(n+1)$-dimensional affine space $\overline{K}^{n+1}$. The line through $(x_0, \dots, x_n) \neq 0$ by $[x_0 : \dots : x_n] \in \mathbb{P}^n_K$.

<u>Rmk</u> $\mathbb{P}^n_K$ is covered by $n+1$ subsets $H_0, \dots, H_n$, where

$$H_i = \{ [x_0 : \dots : x_n] \in \mathbb{P}^n_K \mid x_i \neq 0 \}.$$

For any i, we get a bijection

$$\begin{aligned} \varphi_i : \quad H_i &\longrightarrow \mathbb{A}^n_K \\ [x_0 : \dots : x_n] &\longmapsto \left(\frac{x_0}{x_i}, \dots, \widehat{\frac{x_i}{x_i}}, \dots, \frac{x_n}{x_i} \right) \end{aligned}$$

$\boxed{\text{omit!}}$

$$\Big[x_0^{(i)} : \dots : x_{i-1}^{(i)} : \underset{\substack{\| \\ x_i^{(i)}}}{1} : x_{i+1}^{(i)} : \dots : x_n^{(i)} \Big] \longleftarrow \left(x_0^{(i)}, \dots, \widehat{x_i^{(i)}}, \dots, x_n^{(i)} \right)$$

<u>Def</u> A <u>projective variety</u> defined over K is a subset $V \subseteq \mathbb{P}^n_K = \{[x_0 : \cdots : x_n] \mid x_0, \ldots, x_n \in \bar{K}\}$ such that $\varphi_i(V \cap H_i)$ is a subvariety of $\mathbb{A}^n_K$ defined over K for all i.

We then write $V \subseteq \mathbb{P}^n_K$.

For $V \subseteq \mathbb{P}^n_K$, we write $V(K) = V \cap \mathbb{P}^n_K(K)$ where $\mathbb{P}^n_K(K) = \{[x_0 : \cdots : x_n] \mid x_0, \ldots, x_n \in K\}$.

(So $V(\bar{K}) = V$.)

The closed subsets of $\mathbb{P}^n_K$ w.r.t. the Zariski topology (over K) are the proj. varieties $V \subseteq \mathbb{P}^n_K$.

<u>Rmk</u> The topology on $\mathbb{A}^n_K \overset{\varphi_i}{\cong} H_i \subseteq \mathbb{P}^n_K$ is the subspace top.

<u>Rmk</u> The topology on $\mathbb{P}^n_K$ is obtained by "glueing" the topologies on $H_0, \ldots, H_n$.

Def To a homogeneous polynomial $f \in K[X_0, \dots, X_n]$, we associate the set $V(f) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n_K(\overline{K}) \mid f(x_0, \dots, x_n) = 0\}$ $\subseteq \mathbb{P}^n_K$

independent of the choice of representative $(x_0, \dots, x_n)$ of $[x_0 : \dots : x_n]$ because f is homogeneous

Rmk $V(f)$ is a projective variety with $\varphi_i(V(f) \cap H_i) = V(f_i) \subseteq \mathbb{A}^n_K$, where

$$f_i = f(x_0^{(i)}, \dots, x_{i-1}^{(i)}, 1, x_{i+1}^{(i)}, \dots, x_n^{(i)}) \in K[\underbrace{x_0^{(i)}, \dots, x_{i-1}^{(i)}, x_{i+1}^{(i)}, \dots, x_n^{(i)}}_{n \text{ variables}}]$$

Ese The hyperplane $\overline{H_i} := V(X_i = 0) \subseteq \mathbb{P}^n_K$ is a proj. var. $\Rightarrow H_i = \mathbb{P}^n_K \setminus \overline{H_i}$ is an open subset of $\mathbb{P}^n_K$.

Def If $I \subseteq k[X_0, \dots, X_n]$ is an ideal generated by homogeneous polynomials, we write

$$V(I) = \bigcap_{\substack{f \in I \\ \text{homogeneous}}} V(f) \subseteq \mathbb{P}^n_k.$$

Thm Every $V \subseteq \mathbb{P}^n_k$ is of the form $V = V(I)$ for I as above.

Def $\emptyset \neq V \subseteq \mathbb{P}^n_k$ is irreducible if we can't write $V = V_1 \cup V_2$ with projective varieties $V_1, V_2 \subsetneq V$ defined over k.

Rmk If $\emptyset \neq V \subseteq \mathbb{P}^n_k$ is irreducible, then for all i, $V \cap H_i = \emptyset$ or $\varphi_i(V \cap H_i) \subseteq \mathbb{A}^n_k$ is irreducible (as a variety in $\mathbb{A}^n_k$).

Warning The converse doesn't hold!

E.g. $V = \{[1:0], [0:1]\} \subset \mathbb{P}^1_k$ isn't irreducible, but $V \cap H_0 = \{[1:0]\}$, $V \cap H_1 = \{[0:1]\}$ are!

Reminder We've covered $\mathbb{P}^n_k$ by open subsets $H_0, \dots, H_n$ and defined isomorphisms $\varphi_i : H_i \to \mathbb{A}^n_k$.
(bijections, homeomorphisms)

$$\mathbb{P}^n_k \supseteq H_i \xrightarrow[\varphi_i]{\sim} \mathbb{A}^n_k$$

$$[x_0 : \dots : x_n] \longmapsto \left(x_j^{(i)}\right)_{j \neq i},$$

(with $x_i \neq 0$)

where $x_j^{(i)} = \dfrac{x_j}{x_i}$

$$\left(x_i^{(i)} = \frac{x_i}{x_i} = 1 \right)$$

Change of coordinates:

$$[x_0 : \cdots : x_n] \in H_i \cap H_j$$

$$\begin{tikzcd}
 & {[x_0:\cdots:x_n]} \arrow[dl, mapsto, "\varphi_i"'] \arrow[dr, mapsto, "\varphi_j"] & \\
\mathbb{A}^n_k \ni (x^{(i)}_k)_{k\neq i} \arrow[rr, "\psi_{ij}"] & & (x^{(j)}_k)_{k\neq j} \in \mathbb{A}^n_k,
\end{tikzcd}$$

where $\boxed{x^{(j)}_k = \dfrac{x_k}{x_j} = \dfrac{\frac{x_k}{x_i}}{\frac{x_j}{x_i}} = \dfrac{x^{(i)}_k}{x^{(i)}_j}}$

This defines an isomorphism (bij, homeon.) between the open subset
$\varphi_i(H_i \cap H_j) = \{(x^{(i)}_k)_{k\neq i} \mid x^{(i)}_j \neq 0\}$ of $\mathbb{A}^n_k$
and the open subset
$\varphi_j(H_i \cap H_j) = \{(x^{(j)}_k)_{k\neq j} \mid x^{(j)}_i \neq 0\}$ of $\mathbb{A}^n_k$

We can then define a function on $V \subseteq \mathbb{P}^n_k$ (or on an open subset U of V) to be a collection of functions $f_0, \ldots, f_n$ on $\underset{\cap \mathbb{A}^n_k}{\varphi_0(V \cap H_0)}, \ldots, \underset{\cap \mathbb{A}^n_k}{\varphi_n(V \cap H_n)}$ (def. on $\varphi_0(U \cap H_0), \ldots$) so that f_i and f_j agree on $V \cap H_i \cap H_j$ (on $U \cap H_i \cap H_j$).

$\rightsquigarrow \mathcal{O}_V(U) = \{(f_0, \dots, f_n) \in \prod_i \mathcal{O}_{\varphi_i(V \cap H_i)}(\varphi_i(U \cap H_i)) \mid$

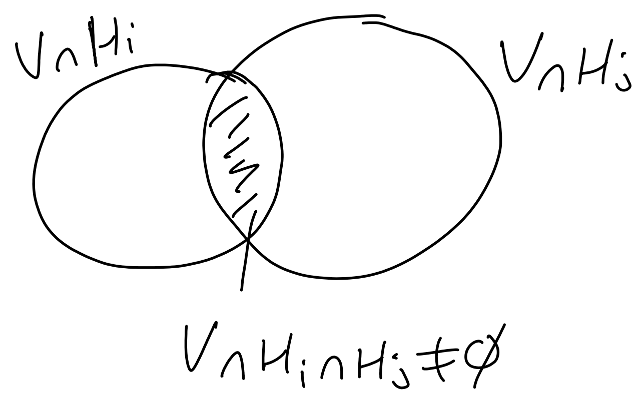
$$f_i|_{U \cap H_i \cap H_j} = f_j|_{U \cap H_i \cap H_j} \ \forall i,j\}.$$

<u>Def</u> For any irreducible $V \subseteq \mathbb{P}^n_k$, its <u>field of rational functions</u> is

$$K(V) = K(\underbrace{\varphi_i(V \cap H_i)}_{\subseteq \mathbb{A}^n_k}) \quad \text{for any } i \text{ such that } V \cap H_i \neq \emptyset.$$

<u>Rmk</u> This is independent of i: since V is irreducible, we have

$V \cap H_i \cap H_j \neq \emptyset$ whenever $V \cap H_i \neq \emptyset$ and $V \cap H_j \neq \emptyset$



<u>Rmk</u> $K(V) = \bigcup_{\emptyset \neq U \subseteq V \text{ open}} \mathcal{O}_V(U)$

Prob $\mathcal{O}_{\mathbb{P}^n_k}(\mathbb{P}^n_k) = k$, the ring of constant functions.

Pf Elements of $\mathcal{O}_{\mathbb{P}^n_k}(\mathbb{P}^n_k)$ correspond to tuples $(f_0, \dots, f_n)$, where $f_i \in \mathcal{O}_{\mathbb{A}^n_k}(\mathbb{A}^n_k)$

and $f_j = f_i \circ \varphi_{ij}$.

f_j is a polynomial in the variables

$$x^{(j)}_k = \frac{x^{(i)}_k}{x^{(i)}_j}.$$

But if f_j is a nonconstant polynomial in these variables, then f_i cannot be a polynomial in the variables $x^{(i)}_k$ (for any $i \neq j$).

$\Rightarrow f_i \notin \mathcal{O}_{\mathbb{A}^n_k}(\mathbb{A}^n_k)$. ↯ $\square$

Ex The "function" $\mathbb{P}^1_k \longrightarrow k$ has a

$$[x:y] \longmapsto \frac{x}{y}$$

pole at $[0:1]$.

Summary

$K(V)$ = field of rat. fcts

$\mathcal{O}_V(V)$ = ring of fcts. on V defined everywhere on V

$\mathcal{O}_V(U)$ = ring of fcts. on V defined everywhere on U

$\mathcal{O}_{V,p}$ = ring of fcts. on V defined at p

Rmk $K(\mathbb{P}^n_k) = \left\{ \frac{f}{g} \;\middle|\; \begin{array}{l} f, g \in k[x_0, \dots, x_n] \text{ homogenous} \\ \text{of the same degree}, \\ g \neq 0 \end{array} \right\}$

Note: $$\frac{f(\lambda x_0, \dots, \lambda x_n)}{g(\lambda x_0, \dots, \lambda x_n)} = \frac{\cancel{\lambda^d} f(x_0, \dots, x_n)}{\cancel{\lambda^d} g(x_0, \dots, x_n)},$$

so $\frac{f}{g}(x)$ is independent of the choice of representative $(x_0, \dots, x_n)$ of $[x_0 : \dots : x_n] \in \mathbb{P}^n_k$.

Def For a k-vector space $L \subseteq k[x_0, \dots, x_n]$ and $d \geq 0$, let $L_d \subseteq L$ be the subspace of homogeneous degree d polynomials.

Rmk Let $V \subseteq \mathbb{P}^n_K$ be irreducible.

Then, $K(V) = \left\{ \frac{f}{g} \mid f, g \in K[x_0, \dots, x_n]_d / I(V)_d \right.$
for some $d \geq 0$
$\left. g \neq 0 \right\}$

Def If $V \subseteq \mathbb{P}^n_K$ is irreducible,

$\dim(V) :=$ transcendence degree of $K(V)$

$= \dim(\varphi_i(V \cap H_i))$ if $V \cap H_i \neq \emptyset$.

Ex $\dim(\mathbb{P}^n_K) = n$.

Def An irred. variety $V \subseteq \mathbb{P}^n_K$ is smooth if

$\varphi_i(V \cap H_i) \subseteq \mathbb{A}^n_K$ is smooth for all i such that $V \cap H_i$.

The tangent space at $P \in V(K)$ is

$T_{V,P} := T_{\underbrace{\varphi_i(V \cap H_i)}_{\subseteq \mathbb{A}^n_K}, \varphi_i(P)}$ for any i such that $P \in H_i(K)$.

$\mathcal{O}_{V,P} := \mathcal{O}_{\varphi_i(V \cap H_i), \varphi_i(P)}$ for any i such that $P \in H_i(K)$.

Def Let $V \subseteq \mathbb{P}^n_K$ and $W \subseteq \mathbb{P}^m_K$.

A *morphism* $f: V \longrightarrow W$ is a map

$$f: V(\overline{K}) \longrightarrow W(\overline{K}) \text{ which satisfies}$$

one of the following equivalent conditions:

a) There is a covering of V by (finitely many) open sets U_s ($s \in S$) such that for each s, there are functions

$$f_0, \dots, f_m \in \mathcal{O}_V(U_s) \text{ such that}$$

$$f(P) = [f_0(P) : \dots : f_m(P)] \quad \forall P \in U_s(\overline{K}).$$

b) $f: V(\overline{K}) \to W(\overline{K})$ is continuous w.r.t. the Zariski topologies over K and for $i = 0, \dots, m$, there are functions $f_j^{(i)} \in \mathcal{O}_V(f^{-1}(H_i))$ $(f_i^{(i)} = 1)$ such that

$$\underbrace{\varphi_i(\underbrace{f(P)}_{\in H_i})}_{\in \mathbb{A}^n_K} = \underbrace{\left(f_0^{(i)}, \dots, \widehat{f_i^{(i)}}, \dots, f_n^{(i)}\right)}_{\in \mathbb{A}^n_K} \quad \forall P \in f^{-1}(H_i).$$

$\underline{\text{Exe}}$ $\mathbb{P}^1_k \longrightarrow \mathbb{P}^{d+1}_k$ (Veronese embedding of degree d)

$$[x:y] \longmapsto [x^d : x^{d-1}y : \dots : xy^{d-1} : y^d]$$

$\underline{\text{not}}$ rational functions on $\mathbb{P}^1_k$.

$$= \left[\left(\frac{x}{y}\right)^d : \left(\frac{x}{y}\right)^{d-1} : \dots : 1\right]$$

fct. on $\mathbb{P}^1_k$ defined on $\{[x:y] \mid y \neq 0\}$

$$= \left[1 : \dots : \left(\frac{y}{x}\right)^{d-1} : \left(\frac{y}{x}\right)^d\right]$$

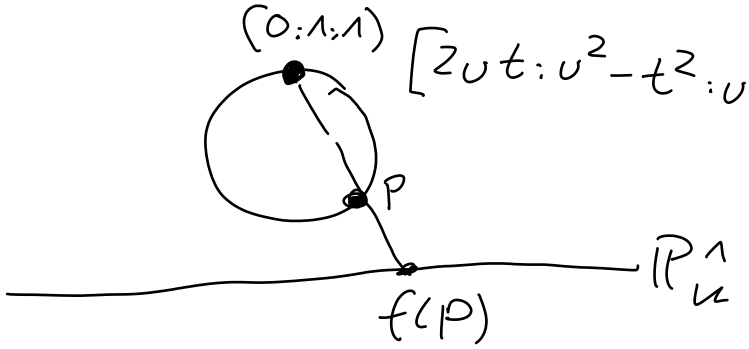
fcts on $\mathbb{P}^1_k$ defined on $\{[x:y] \mid x \neq 0\}$

$\{y \neq 0\}$ and $\{x \neq 0\}$ form an open cover of $\mathbb{P}^1_k$.

$\underline{\text{Exe}}$ $\mathbb{P}^2_k \supseteq \{[x:y:z] \mid x^2+y^2=z^2\} =: C \longrightarrow \mathbb{P}^1_k$ (see first lecture)

$[x:y:z] \longmapsto [x : y-z]$ if $x \neq 0$ or $y-z \neq 0$

$= [y+z : -x]$ if $y+z \neq 0$ or $-x \neq 0$



$[2ut : u^2-t^2 : u^2+t^2] \longleftarrow [t:u]$

Ese Embedding $\mathbb{P}^n_k \longrightarrow \mathbb{P}^m_k$ $(n \leq m)$

$$[x_0 : \cdots : x_n] \mapsto [x_0 : \cdots : x_n : 0 : \cdots : 0]$$

Warning There is no "projection" morphism

$$f : \mathbb{P}^2_k \longrightarrow \mathbb{P}^1_k$$
$$[x : y : z] \longmapsto [x : y] \text{ for } (x, y) \neq (0, 0)$$

Pf $f([0 : y : 1]) = [0 : y] = [0 : 1] \quad \forall y \neq 0$

$f([x : 0 : 1]) = [x : 0] = [1 : 0] \quad \forall x \neq 0$

$\Rightarrow$ By continuity, $f([0 : 0 : 1]) = [0 : 1]$

and $f([0 : 0 : 1]) = [1 : 0]$. $\lightning$ $\square$

Lemma Let C be a smooth projective curve and let $t \in k(C)$. Then, there is a morphism $C \longrightarrow \mathbb{P}^1_k$

$$P \longmapsto \begin{cases} \underbrace{[t(P) : 1]}_{\cong\, t(P)} & \text{if } t \text{ is defined at } P, \\ \underbrace{[0 : 1]}_{\cong\, \infty} & \text{if } t \text{ isn't defined at } P \\ & (= \text{"pole at } P\text{"}) \end{cases}$$

Pf $K(C)$ is the field of fractions of $\mathcal{O}_{V,P}$.

$$\left.\begin{array}{l} t \text{ defined at } P \Leftrightarrow v_{V,P}(t) \geq 0 \\ \frac{1}{t} \text{ defined at } P \Leftrightarrow v_{V,P}(t) \leq 0 \end{array}\right\}$$ Here, we use smoothness!

We can define

$$C \longrightarrow \mathbb{P}^1_k$$

$$P \longmapsto \begin{cases} [t(P):1] & \text{if } t \text{ is def. at } P, \\ [1:\frac{1}{t}(P)] & \text{if } \frac{1}{t} \text{ is def. at } P. \end{cases}$$

$\square$

Rmk The lemma fails for singular curves! (It's possible that P looks like a zero when approaching in one direction and like a pole in a different direction).

Reference

Hartshorne, Algebraic Geometry, Chapter I.

1.8. Divisors

<u>Reference</u> • Fulton, Algebraic Curves, Chapter 8

• Hartshorne, Algebraic Geometry, Chapter IV

Assume char$(K) = 0$.

Let be a smooth projective curve over K.

<u>Def</u> A <u>(Weil) divisor</u> on C (defined over K) is a

formal sum $\sum_{P \in C(\bar{K})} n_P P = \sum_{P \in C(\bar{K})} n_P [P]$

with $n_P \in \mathbb{Z}$ $\forall P$ and $n_P = 0$ for all but finitely many P, which is invariant under the action of $Gal(\bar{K}|K)$: $n_{\sigma(P)} = n_P$ $\forall \sigma \in Gal(\bar{K}|K)$, $P \in C(\bar{K})$.

The (additive) group of divisors is denoted by $Div(C)$.

<u>Equivalent def</u> A Weil divisor is a finite formal sum

$$\sum_{S \subseteq C} n_S S$$

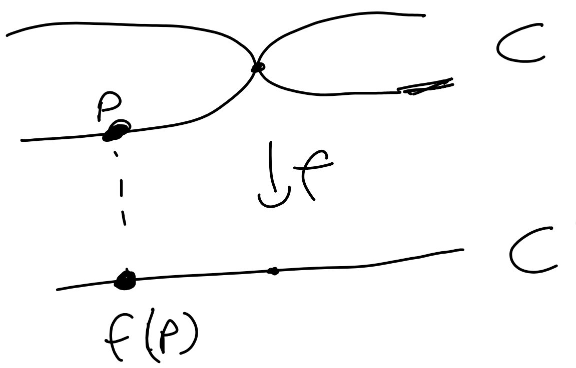
$$\left.\begin{array}{l} S \subseteq C \\ \text{0-dimensional} \\ \text{irreducible} \\ \text{subvarieties} \\ \text{defined over } K \end{array}\right\} = Gal(\bar{K}|K)\text{-orbit of points in } C(\bar{K}).$$

Def The <u>degree</u> of $D = \sum n_P P$ is $\deg(D) = \sum n_P$.

The subgroup of divisors of degree 0 is $\mathrm{Div}^0(C)$.

Def Let $f : C \to C'$ be a morphism between smooth proj. curves over K. The <u>image</u> of $D = \sum n_P P \in \mathrm{Div}(C)$ is

$$f(D) = \sum n_P f(P) \in \mathrm{Div}(C').$$



Rmk $\deg(f(D)) = \deg(D)$.

Def Consider a nonconstant morphism $f : C \to C'$ as above.

It induces a field homomorphism

$$\begin{aligned} K(C') &\hookrightarrow K(C) \\ t &\longmapsto t \circ f \end{aligned}$$

$\Rightarrow$ We can interpret $K(C)$ as a field ext. of $K(C')$. The <u>degree</u> of f is

$$\deg(f) := [K(C) : K(C')].$$

For $Q \in C'(\bar{K})$, denote a uniformiser at Q by $t_{C',Q}$. (It's a rational function on C' with coefficients in $\bar{K}$.)

For $P \in C(\bar{K})$, $Q = f(P)$, let

$$e_{P|Q} = v_{C,P}(t_{C',Q} \circ f) \quad (\geq 1),$$

the <u>ramification index</u> of f at P.

<u>Thm</u> For any $Q \in C'(\bar{K})$,

$$\sum_{\substack{P \in C(\bar{K}): \\ f(P) = Q}} e_{P|Q} = \deg(f).$$

Analogy with extensions of number fields

$$\begin{array}{c|c} K(C) & L \\ | & | \\ K(C') & K \end{array}$$

$$\begin{array}{c|c} \mathcal{O}_C(f^{-1}(C' \cap H_i)) & \mathcal{O}_L \\ | & | \\ \mathcal{O}_{C'}(\underbrace{C' \cap H_i}_{\subseteq \mathbb{A}^n}) & \mathcal{O}_K \end{array}$$

$$\begin{array}{c|c} \mathrm{Gal}(\overline{K}|K)\text{-orbits of } P \in f^{-1}(C' \cap H_i)(\overline{K}) & \mathfrak{P} \subseteq \mathcal{O}_L \\ \downarrow f & | \\ \mathrm{Gal}(\overline{K}|K)\text{-orbits of } Q \in (C' \cap H_i)(K') & \mathfrak{q} \subseteq \mathcal{O}_K \end{array}$$

$e_{P|Q}$ | $e_{\mathfrak{P}|\mathfrak{q}}$

$$f_{P|Q} = [\underbrace{\mathcal{O}_C(\dots)/m_P}_{K_P}\, : \,\underbrace{\mathcal{O}_{C'}(\dots)/m_Q}_{K_Q}] \qquad \Bigg| \qquad f_{\mathfrak{P}|\mathfrak{q}} = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{q}]$$

K_P, the smallest field ext. of K s.t. $P \in C(K_P)$

K_Q, the smallest field ext. of K s.t. $Q \in C'(K_Q)$

$$f_{P|Q} = \frac{\text{size of } \mathrm{Gal}(\overline{K}|K)\text{-orbit of } P}{\text{size of } \mathrm{Gal}(\overline{K}|K)\text{-orbit of } Q}$$

$$\sum_{\substack{P \in C(\overline{K}): \\ f(P) = Q}} e_{P|Q} = [K(C) : K(C')] = \deg(f) \qquad \Bigg| \qquad \sum_{\mathfrak{P}|\mathfrak{q}} e_{\mathfrak{P}|\mathfrak{q}} f_{\mathfrak{P}|\mathfrak{q}} = [L : K]$$

$\mathrm{Div}(C)$ | group of fractional ideals of $\mathcal{O}_L$

<u>Thm</u> $e_{P|Q} = 1$ for all but finitely many points $P \in C(\bar{K})$ $\quad (Q = f(C))$

($\hat{=}$ $\mathcal{O}_L | \mathcal{O}_K$ only ramified at finitely many primes)

<u>Def</u> The <u>ramification divisor</u> of f is

$$R_f := \sum_{\substack{P \in C(\bar{K}) \\ Q = f(C)}} (e_{P|Q} - 1) P.$$

($R_f \hat{=}$ different of $\mathcal{O}_L | \mathcal{O}_K$)

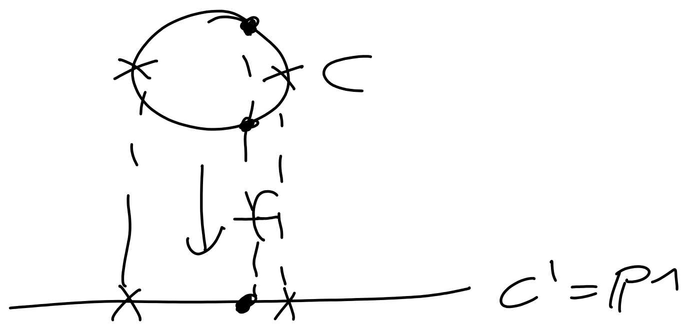
($f(R_f) \hat{=}$ discriminant of $\mathcal{O}_L | \mathcal{O}_K$).

Ese $C = \{[x:y:z] \mid x^2+y^2=z^2\} \subset \mathbb{P}^2$

$$\begin{array}{c} C \\ \downarrow f \\ C' = \mathbb{P}^1 \end{array}$$

$$C \xrightarrow{\ f\ } C'$$

$$[x:y:z] \longmapsto [x:z]$$



Look at the restriction

$$\begin{array}{ccc} C\cap H_2 & \xrightarrow{\ f\ } & C'\cap H_1 \\ \shortparallel & & \shortparallel \\ \{(x,y)\in\mathbb{A}^2 \mid x^2+y^2=1\} & & \mathbb{A}^1 = \{s\in\mathbb{A}^1\} \end{array}$$

$$K(C') = K(C'\cap H_1) = K(s)$$

$$\downarrow$$

$$K(C) = K(C\cap H_2) = K(x)[y]/(x^2+y^2-1)$$

$$K(C') \longrightarrow K(C)$$

$$s \longmapsto x$$

$$\deg(f) = [K(x)[y]/(x^2+y^2-1) : K(x)] = 2$$

The preimages of $s\in\mathbb{A}^1$ are $(s, \pm\sqrt{1-s^2}) \in C(\bar{K})$.

If $s \neq \pm 1$, there are two preimages, each with multiplicity 1.

If $s = \pm 1$, there is one preimage, with multiplicity 2.

Also check the point $\infty = [1:0] \in \mathbb{P}^1$: There are two preimages $[1 : \pm\sqrt{-1} : 0]$, each with multiplicity 1.

$$\Rightarrow R_f = (1,0) + (-1,0) = [1:0:1] + [-1:0:1].$$

$$\mathbb{A}^2 \subset \mathbb{P}^2$$

Def The <u>preimage</u> of $D' = \sum n_Q Q \in \mathrm{Div}(C')$ is
$$f^*(D') = \sum_{\substack{P \in C(\bar{K}) \\ f(P) = Q}} n_Q \, e_{P|Q} \, P.$$

<u>Cor</u> a) $f_*(f^*(D')) = \deg(f) \cdot D'$

b) $\deg(f^*(D')) = \deg(f) \cdot \deg(D')$

Def To a rational function $f \in K(C)^\times$, we associate the divisor

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} \underbrace{v_{C,P}(f)}_{\substack{>0 \text{ iff } f \text{ has a zero at } P \\ <0 \text{ iff } f \text{ has a pole at } P}} P$$

Rmk $\mathrm{div} : K(C)^\times \longrightarrow \mathrm{Div}(C)$ is group hom.

Def The divisor class group of C is

$$\mathrm{Cl}(C) := \mathrm{Div}(C) / K(C)^\times$$ (the cokernel of the map $\mathrm{div} : K(C)^\times \to \mathrm{Div}(C)$).

($\hat{=}$ ideal class group)

Thm $\deg(\mathrm{div}(f)) = 0 \quad \forall f \in K(C)^\times$

(Number of zeros with mult. = number of poles with mult.)

Pf If $f \neq 0$ is constant, $\mathrm{div}(f) = 0$.

If f is nonconstant, interpret it as $f : C \to \mathbb{P}^1$.

$$\Rightarrow \mathrm{div}(f) = f^*([0] - [\infty])$$

with $[0], [\infty] \in \mathbb{P}^1$

$$\Rightarrow \deg(\mathrm{div}(f)) = \deg(f) \cdot \underbrace{\deg([0] - [\infty])}_{0} = 0$$

$\square$

Thm $\mathrm{div}(f) = 0 \Leftrightarrow f = $ constant

Pf If $f \neq$ const, then $f : C(\overline{K}) \to \mathbb{P}^1(\overline{K})$ is surjective. $\Rightarrow f$ has a zero. $\Rightarrow \mathrm{div}(f) \neq 0$ $\square$

Cor $\mathcal{O}_C(C) = K$.

Pf $f : C(\overline{K}) \to \mathbb{P}^1(\overline{K})$ surjective

$\Rightarrow f$ has a pole ($=$ preimage of ∞) $\square$

Def $\mathcal{Cl}^0(C) := \mathrm{Div}^0(C) / K(C)^\times$.

Rmk The image of $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ is nonzero (take $D = \mathrm{Gal}(\overline{K}|K)$-orbit of any point $P \in C(\overline{K})$).

$\Rightarrow \deg(\mathrm{Div}(C)) \cong \mathbb{Z}$

$\Rightarrow \mathrm{Div}(C) \cong \mathrm{Div}^0(C) \times \mathbb{Z}$

$\mathcal{Cl}(C) \cong \mathcal{Cl}^0(C) \times \mathbb{Z}$

Warning The map $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ might not be surjective.

Ese $\deg : Cl(\mathbb{P}1) \longrightarrow \mathbb{Z}$ is an isomorphism.

Pf surjective: $\deg([O]) = 1$.

injective: Let $D = \sum_P n_P P \in Div^0(C)$.

Take $f(X, Y) = \prod_{a \in \overline{K} \subset \mathbb{P}1} (X - aY)^{n_{[a]}} \cdot X^{n_{[\infty]}}$.

Since $\sum n_P = 0$, the numerator and denominator of f are homogeneous of the same degree, so $f(X, Y) \in K(\mathbb{P}1)$.

Furthermore,

$$div(f) = \sum_{a \in \overline{K}} n_{[a]}[a] + n_{[\infty]}[\infty]$$

$$= \sum n_P P = D. \qquad \square$$

Def We write $D \leq D'$ if $n_P \leq n_P'$ $\forall P$.
$$\underset{\sum n_P P}{\overset{\shortparallel}{D}} \leq \underset{\sum n_P' P}{\overset{\shortparallel}{D'}}$$

D is <u>effective</u> if $D \geq 0$.

Def For any $D \in \mathrm{Div}(C)$, we let

$$L(D) = \{ f \in K(C)^\times \mid \mathrm{div}(f) + D \geq 0 \} \cup \{0\}.$$

Lemma $L(D)$ is a K-vector space.

Pf
- $\mathrm{div}(\lambda f) = \mathrm{div}(f)$ $\forall \lambda \in K^\times$
- $v_P(f+g) \geq \min(v_P(f), v_P(g))$

nonarch.
triangle inequality

"if f has a root of order a at P,
and g — " — b at P,
then $f+g$ — " — $\geq \min(a,b)$ at P"

$\square$

Def $\ell(D) := \dim(L(D))$ as a K-vector space.

Rmk $L(D + \mathrm{div}(g)) \cong L(D)$ for any $g \in K(C)^\times$,
$$f \mapsto fg$$

so $\ell(D)$ only depends on the divisor class of D in $\mathrm{Cl}(C)$.

Ex Let $C = \mathbb{P}^1_K$ and let $D \in \mathrm{Div}(C)$ of degree d.
Then,
$$\ell(D) = \begin{cases} 0, & d < 0, \\ d+1, & d \geq 0. \end{cases}$$

Pf Let $d \geq 0$. w.l.o.g. $D = d \cdot \underbrace{[1:0]}_{\infty}$.

$\Rightarrow L(D) = \{ f \in K(C) \mid f$ has at most a pole of order d at $[1:0]$ and no other poles $\}$

$$= \left\{ \frac{f(X,Y)}{Y^d} \;\middle|\; f(X,Y) \text{ homogeneous of degree } d \right\}.$$

$\square$

Remark $L(0) = \mathcal{O}_C(C) = K$

Remark $L(D)=0$ if $\deg(D)<0$

Pf $\deg(\operatorname{div}(f)+D) = \deg(D)<0$.

$\Rightarrow \operatorname{div}(f)+D \not\geq 0$. $\square$

Remark $L(D)=0$ if $\deg(D)=0$ but $[D]\neq 0$ in $Cl(C)$.

Pf let $f\neq 0$. $\deg(\operatorname{div}(f)+D) = \deg(D)=0$

$\Rightarrow$ If $\operatorname{div}(f)+D \geq 0$, then $\operatorname{div}(f)+D=0$. $\square$

Remark $L(D)\subseteq L(D')$ if $D\leq D'$.

(Important) Remark $l(D)$ doesn't depend on the base field K: If we denote the corresponding $\overline{K}$-vector space of rational functions defined over $\overline{K}$ by $\overline{L}(D)\subseteq K(C)\otimes_K \overline{K}$, then $\overline{L}(D) = L(D)\otimes_K \overline{K}$.

Lemma $l(D)-1\leq l(D-P)\leq l(D)$ $\forall D\in Div(C), P\in C(\overline{K})$

Cor $l(D)<\infty$.

Pf of Lemma Let $D=\sum_Q n_Q Q$. The the linear map $L(D)\longrightarrow K$, $f\longmapsto (f t_P^{n_P})(P)$ has kernel $L(D-P)$. $\square$

Rmk For any $f \in K(C)^\times$ and any divisor $D' \in \mathrm{Div}(C)$, there are only finitely many $D \leq D'$ such that $f \in L(D)$.

Pf $f \in L(D) \Leftrightarrow -\mathrm{div}(f) \leq D \leq D'$
and $D \leq D'$

$\square$

Cor 1.10 For any $D \in \mathrm{Div}(C)$ with $L(D) \neq 0$,

$\ell(D-P) = \ell(D)$ for finitely many $P \in C(\bar{K})$,
and $\ell(D-P) = \ell(D) - 1$ for all other $P \in C(\bar{K})$.

Pf Pick any $0 \neq f \in L(D)$. According to the remark, there are only finitely many P s.t. $f \in L(D-P)$.

$\square$

Lemma 1.11 $\ell(D) + \ell(E) \leq \ell(D+E) + 1 \quad \forall D, E$

Pf Consider the bilinear map

$$L(D) \times L(E) \longrightarrow L(D+E)$$
$$(f, g) \longmapsto fg$$

$$\underbrace{(\mathrm{div}(f) + D)}_{\geq 0} + \underbrace{(\mathrm{div}(g) + E)}_{\geq 0} = \underbrace{\mathrm{div}(fg) + D + E}_{\geq 0}.$$

Let $0 \neq h \in L(D+E)$. There are only fin. many ways of writing $\mathrm{div}(h) + D + E = D' + E'$ with $D', E' \geq 0$. We have $\mathrm{div}(f) + D =$ $\mathrm{div}(f') + D$ if and only if $f' = \lambda f$ for some $\lambda \in K^\times$.

$\Rightarrow$ Any nonempty preimage of any $0 \neq h \in L(D+E)$ has dimension 1.

$\Rightarrow \dim(L(D)) + \dim(L(E)) \leq \dim(L(D+E)) + 1.$

$\square$

1.9. Maps to projective space

Let C be a smooth projective curve.

Def Let $F \subset K(C)$ be an $(n+1)$-dimensional with basis $f_0, \dots, f_n$. Consider the minimal divisors $D = \sum n_P P$ such that $F \subseteq L(D)$.

$$(-n_P = \min_{f \in F} v_P(f) = \min(v_P(f_0), \dots, v_P(f_n)).$$

The morphism $\varphi: C \to \mathbb{P}^n_K$ associated to $f_0, \dots, f_n$ (or to F) is in a neighborhood U of $P \in C(\bar{K})$ given by

$$\varphi(Q) = \left[(f_0 \cdot t_P^{n_P})(Q) : \quad \dots \quad : (f_n \cdot t_P^{n_P})(Q) \right] \text{ for } Q \in U.$$

all well-def. at P,
not all 0 at P
(and therefore in a small nbhd. of P)

Rmk Multiplying $f_0, \dots, f_n$ by $g \in K(C)^\times$ doesn't change φ.

Rmk This generalizes the earlier construction of the morphism $\varphi: C \to \mathbb{P}^1$ associated to $f \in \mathbb{P}^1_K$ (take $f_0 = f$, $f_1 = 1$).

Thm Every morphism $\varphi: C \to \mathbb{P}^n_K$ whose image isn't contained in a hyperplane in $\mathbb{P}^n_K$ is of this form.

Thm φ is a closed embedding (= isomorphism onto its image) if and only if

$$L(D-P-Q) \subsetneq L(D-P) \text{ for all } P, Q \in C(\overline{K}).$$

Pf of "$\Rightarrow$" w.l.o.g. $L(D-P) \cap F$ is spanned by $f_1, \dots, f_n$.

$$\Rightarrow \varphi(P) = [(f_0 t_P^{n_P})(P) : 0 : \dots : 0] = (1 : 0 : \dots : 0]$$

If $L(D-Q) \subseteq L(D-P-Q) = L(D-P)$ for some $Q \neq P$, then $\varphi(Q) = [1:0:\dots:0]$ for the same reason.

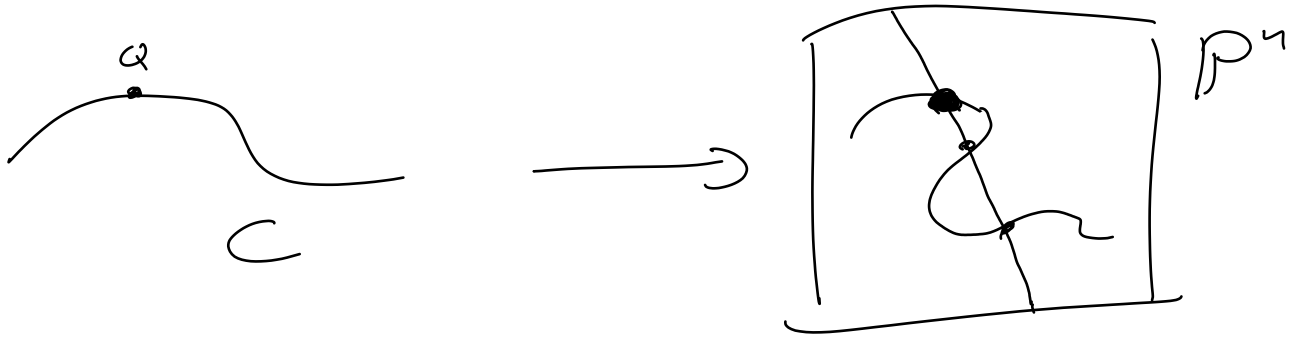
$\Rightarrow \varphi$ isn't injective. $\Rightarrow \varphi$ not an isom. onto its image.

If $L(D-2P) = L(D-P)$, then

$f_1 t_P^{n_P}, \dots, f_n t_P^{n_P}$ have a root of multiplicity at least 2 at P. Hence, the derivative of φ at P is zero. $\Rightarrow \varphi$ not an isom. onto $\varphi(C)$. $\square$

Thm. Let $H \subset \mathbb{P}^n_k$ be a hyperplane which intersects $\varphi(C) \subset \mathbb{P}^n_k$ in the points $P_1, \dots, P_r$ which multiplicities $m_1, \dots, m_r$. Let $D' = m_1 P_1 + \dots + m_r P_r \in \mathrm{Div}(\varphi(C))$.

Assume φ is a closed embedding.



Then, $[\varphi^*(D')] = [D]$ in $\mathcal{Cl}(C)$.

Sketch of proof W.l.o.g. $H = \{[x_0 : \dots : x_n] \mid x_0 = 0\}$.

Then, $\overset{\sum n''_Q Q}{D''} := \varphi^*(D') = \mathrm{div}(f_0) + D$:

Let $Q \in C(\overline{k})$ with $\varphi(Q) = P_i$. Then,

$$n''_Q = v_Q(f_0 t_Q^{n_Q}) = v_Q(f_0) + n_Q. \qquad \square$$

1.10. Canonical divisor class

Let C be a sm. proj. curve.

Thm 1.12

a) The module of differentials $\Omega_K(K(C))$ is a one-dimensional $K(C)$-vector space.

b) Let $f \in K(C)$. Then, $df = 0$ if and only if $f \in K$.

Pf b) "$\Leftarrow$" clear

"$\Rightarrow$" Pick $a \in K$ such that $f-a$ has a root $P \in C(\bar{K})$ of mult. 1 (possible since $f: C \to \mathbb{P}^1$ is only ramified at finitely many points).

$\Rightarrow$ f has nonzero derivative at P.

$\Rightarrow df \neq 0$.

a) Let $f, g \in K(C)$. Since $K(C)$ has transcendence degree 1, the elements f, g are algebraically dependent over K.

Let $0 \neq \varphi \in K[S,T]$ be of minimal degree such that $\varphi(f,g) = 0$.

$$\Rightarrow 0 = d\varphi(f,g) = \underbrace{\frac{\partial \varphi}{\partial S}(f,g)}_{\in K(C)} df + \underbrace{\frac{\partial \varphi}{\partial T}(f,g)}_{\in K(C)} dg$$

We can't have $\frac{\partial\varphi}{\partial S}(f,g) = \frac{\partial\varphi}{\partial T}(f,g) = 0$ since $\frac{\partial\varphi}{\partial S} \neq 0$ or $\frac{\partial\varphi}{\partial T} \neq 0$, and both have smaller degree than φ.
$\Rightarrow$ df and dg aren't linearly independent over $K(C)$.

$\square$

Def To a nonzero differential $\omega \in \Omega_K(K(C))$, we associate the divisor $\operatorname{div}(\omega) = \sum_{P \in C(\bar{K})} v_P\Big(\underbrace{\frac{\omega}{dt_P}}_{\in K(C)}\Big) P$

$\in K(C)$ by Thm 1.12

independent of the choice of uniformizer t_P!

Def The divisors of the form $\operatorname{div}(\omega)$ are called the canonical divisors of C.

Rmk By Thm 1.12, they form a divisor class, denoted by $W = W_C$ (or K_C).

Def The genus of C is $g = g_C = \ell(W) \geq 0$.

Eg $C = \mathbb{P}^1_k$, $\mathcal{O}_{\mathbb{P}^1}(H_0) = K[X_1^{(0)}]$

$$\mathcal{O}_{\mathbb{P}^1}(H_1) = K[X_0^{(1)}]$$

$$X_0^{(1)} = (X_1^{(0)})^{-1}$$

$$\omega = dX_1^{(0)} = -\frac{dX_0^{(1)}}{(X_0^{(1)})^2}.$$

$X_1^{(0)} - a$ is a uniformizer at $a \in \mathbb{A}^1 \cong H_0$.
$X_0^{(1)} - a$ — " — $a \in \mathbb{A}^1 \cong H_1$.

$$\Rightarrow v_P\left(\frac{\omega}{dt_P}\right) = \begin{cases} 0, & P \neq [0:1], \\ -2, & P = [0:1]. \end{cases}$$

$\Rightarrow \operatorname{div}(\omega) = -2 \cdot [0:1]$

$\Rightarrow W_{\mathbb{P}^1} \in \mathcal{Cl}(\mathbb{P}^1) = \mathbb{Z}$ is the divisor class of degree -2.

$\Rightarrow g_{\mathbb{P}^1} = \ell(-2 \cdot [0:1]) = 0.$

1.11. Riemann-Roch and Hurwitz formulas

Thm (Riemann-Roch)

For any divisor $D \in \mathrm{Div}(C)$:

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

Pf See for example Fulton. $\square$

Cor
a) $\deg(W) = 2g-2$
b) $\ell(D) \geq \deg(D) + 1 - g$
c) $\ell(D) = \deg(D) + 1 - g$ if $\deg(D) > \deg(W) = 2g-2$
d) $\ell(D) \leq \frac{1}{2}\deg(D) + 1$ if $0 \leq \deg(D) \leq 2g$

Pf
a) $D = W$
b) $\ell(W-D) \geq 0$
c) $\ell(W-D) = 0$ if $\deg(W-D) < 0$.
d) By Lemma 2.11,

$$\ell(D) + \ell(W-D) \leq \ell(W) + 1 = g+1$$

or $\ell(D) = 0$ or $\ell(W-D) = 0$

$$\Downarrow$$

$$\ell(D) = \deg(D) + 1 - g$$
$$\leq \frac{1}{2}\deg(D) + 1. \quad \square$$

Thm Let $f: C \to C'$ be a nonconstant morphism between smooth projective curves. Then,

$$W_C = f^*(W_{C'}) + R_f. \qquad (I)$$

Pf Let $0 \neq \omega'$ be a differential on C'.

$\Rightarrow 0 \neq \omega := f^*(\omega')$ is a differential on C.

$$\operatorname{div}(\omega) = f^*(\operatorname{div}(\omega')) + R_f$$

$$\uparrow$$

$$\underbrace{v_{C,P}\left(\frac{\omega}{dt_P}\right)}_{\text{mult. of } P \text{ in } \operatorname{div}(\omega)} = \underbrace{v_{C,P}\left(\frac{f^*(\omega')}{f^*(dt_{f(P)})}\right)}_{\underbrace{e_{P|f(P)} \cdot \underbrace{v_{C',f(P)}\left(\frac{\omega'}{dt_{f(P)}}\right)}_{\text{mult. of } P \text{ in } \operatorname{div}(\omega')}}_{\text{mult. of } P \text{ in } f^*(\operatorname{div}(\omega'))}} + \underbrace{v_{C,P}\left(\frac{f^*(dt_{f(P)})}{dt_P}\right)}_{\text{mult. of } P \text{ in } R_f}$$

$\square$

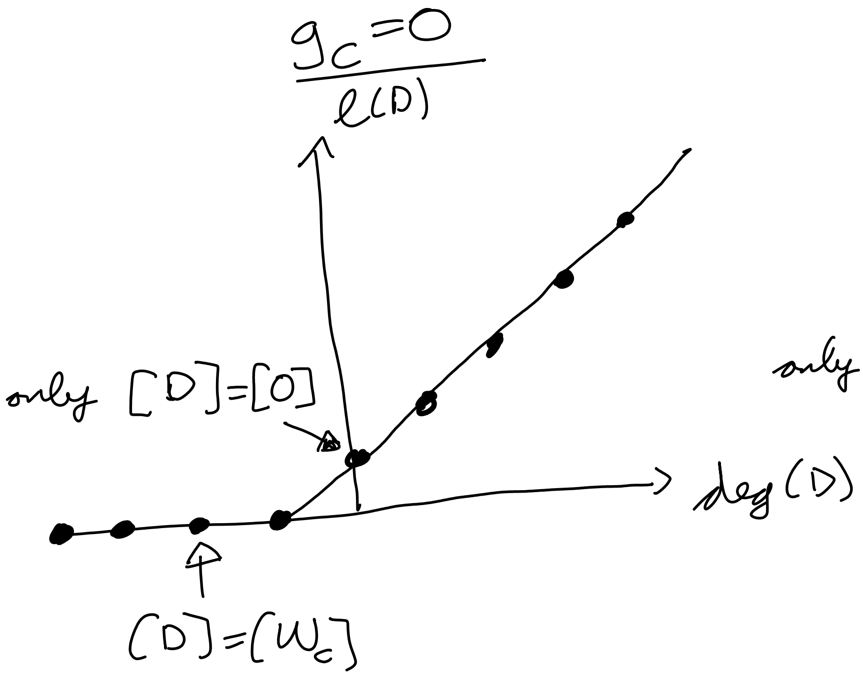
Cor (Riemann-Hurwitz)

$$2g_C - 2 = \deg(f)\cdot(2g_{C'} - 2) + \deg(R_f).$$

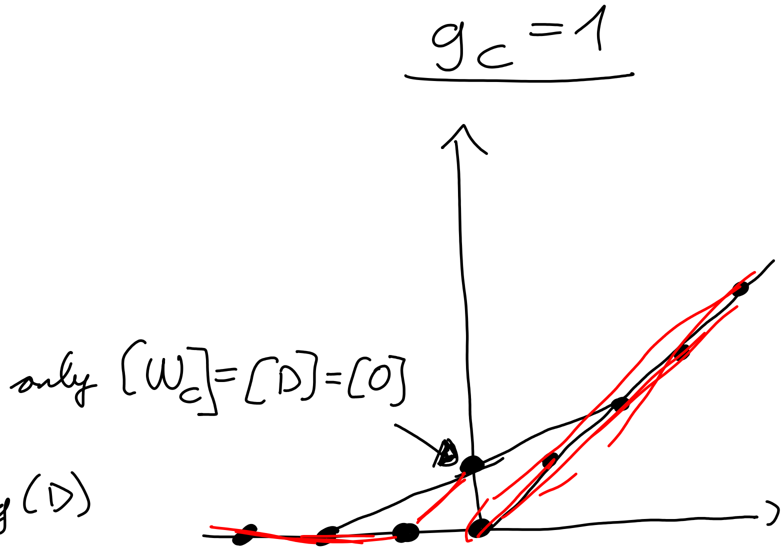
Pf Take degrees of both sides of (I). $\square$

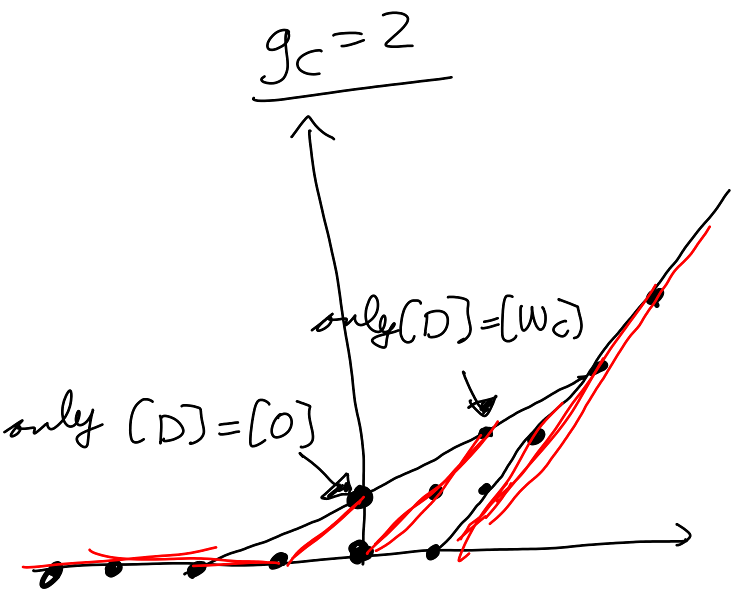
Summary

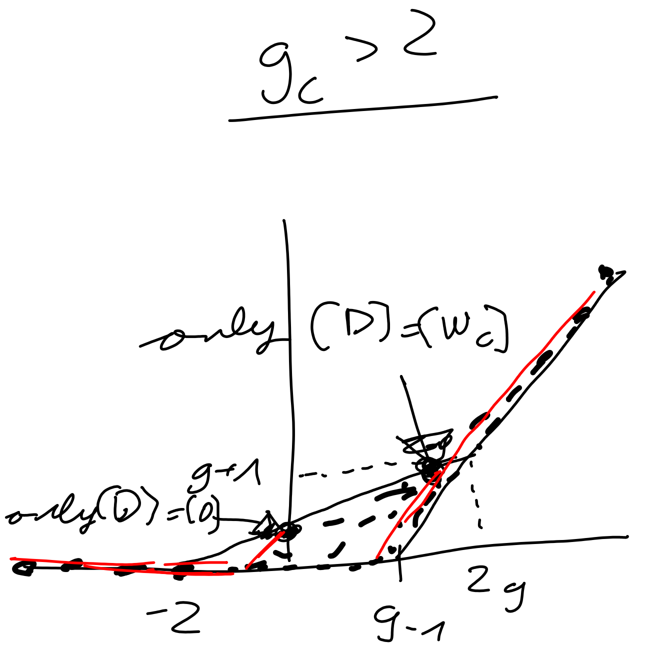
$S = \{(\deg(D), \ell(D)) \mid D \in \mathrm{Div}(C)\}$ is a subset of the set of dots in the following pictures:



$\Rightarrow \ell\ell^0(C) = 0$







If $k=\bar{k}$, then all points on red lines lie in S according to Cor 1.10.

Genus 0

Thm If $g_C = 0$ and $C(K) \neq \emptyset$, then $C \cong \mathbb{P}^1_K$ (over K).

Pf Let $P_0 \in C(K)$.

$$\ell(P_0) = 2, \quad \ell(P_0 - P) = 1, \quad \ell(P_0 - P - Q) = 0 \quad \forall P, Q \in C(\bar{K}).$$

$\Rightarrow$ The morphism $\varphi: C \to \mathbb{P}^1_K$ arising from a basis (f_0, f_1) of $L(P_0)$ and the divisor $D = P_0$ is a closed embedding.

$\Rightarrow$ It's an isomorphism. $\square$

Thm If $g_C = 0$, then C is isomorphic to a (smooth) conic in $\mathbb{P}^2_K$.

Pf $\ell(-W_C) = 3$, $\ell(-W_C - P) = 2$, $\ell(-W_C - P - Q) = 1$.

$\Rightarrow$ The morphism $\varphi: C \to \mathbb{P}^2_K$ arising from a basis of $L(-W_C)$ is a closed embedding.

Since $\deg(-W_C) = 2$ and $-W_C = \varphi^*(D')$, where $D' \in \mathrm{Div}(\varphi(C))$ is the intersection divisor with a hyperplane H, we have

$$2 = \deg(-W_C) = \underbrace{\deg(\varphi: C \to \varphi(C))}_{1} \cdot \deg(D') = \deg(D')$$

$\Rightarrow$ By Bézout's theorem, $\varphi(C) \subset \mathbb{P}^2_K$ is a conic. $\square$

Rmk
Conversely, every smooth conic $C \subset \mathbb{P}^2_K$ has genus 0.

2. Elliptic curves

2.1. Introduction

Genus 1

References: • Silverman, Tate: Rational points on elliptic curves
• Silverman: The Arithmetic of elliptic curves

Def An elliptic curve is a pair (E, O), where E is a smooth projective curve of genus 1, and $O \in E(K)$.

Thm We have a bijection

$$\begin{aligned} E(K) &\longleftrightarrow Cl^0(E) \\ P &\longmapsto [P]-[O] \end{aligned}$$

Pf injective: Assume $[P]-[O] = [Q]-[O]$ in $Cl(E)$.

$\Rightarrow [P]-[Q] = \operatorname{div}(f)$ for some $f \in K(E)^\times$.

$$\left.\begin{array}{l} \Rightarrow f \in L(Q) \\ \left.\begin{array}{l} \ell(Q)=1 \\ L(Q) \supseteq K \end{array}\right\} \Rightarrow L(Q) = K \end{array}\right\} f = \text{const.}$$

$\Rightarrow \operatorname{div}(f) = 0$

$\Rightarrow P = Q$

surjective: Let $D \in \mathrm{Div}^0(E)$.

$\ell(D + [O]) = 1$

Let $0 \neq f \in L(D + [O])$.

$\Rightarrow \underbrace{D + [O] + \mathrm{div}(f)}_{\deg(\cdot)=1} \geq 0$

$\Rightarrow D + [O] + \mathrm{div}(f) = [P]$ for some $P \in E(K)$.

$\Rightarrow D = [P] - [O]$ in $\mathrm{Cl}(E)$. $\square$

$\leadsto$ The group law on $\mathrm{Cl}^0(E)$ gives rise to a group law on $E(K)$ with identity $O \in E(K)$.

Thm There is a closed embedding $\varphi: E \to \mathbb{P}^2_K$ whose image is of the form

$$\{[x:y:z] \mid Y^2Z + a_1XYZ + a_3YZ^2$$
$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

and $\varphi(O) = [0:1:0]$.

We also get a degree 2 morphism $\psi: E \to \mathbb{P}^1_K$ with $\psi(P) = [x:z]$ if $\varphi(P) = [x:y:z]$.

Pf $\quad L([O]) \subseteq L(2[O]) \subseteq L(3[O])$

$$\begin{array}{ccc} \| & \| & \| \\ \langle 1 \rangle & \langle 1, f \rangle & \langle 1, f, g \rangle \\ \dim = 1 & \dim = 2 & \dim = 3 \end{array}$$

Since $\ell(3[O]-[P]) = 2$, $\ell(3[O]-[P]-[Q]) = 1$ $\forall P, Q \in E(\bar{k})$,

we obtain a closed embedding $\varphi : E \to \mathbb{P}^2_k$ associated to $(f, g, 1)$ and the divisor $D = 3[O]$ and similarly a degree 2 morphism $\psi : E \to \mathbb{P}^1_k$ associated to $(f, 1)$ and the divisor $D' = 2[O]$.

$$v_0(f) = -2, \quad v_0(g) = -3, \quad v_0(1) = 0$$

$\uparrow$

$f \in L(2[O]) \setminus L([O])$

$\Rightarrow \varphi(O) = [0 : 1 : 0]$.

Now $g^2 \cdot 1$, $fg \cdot 1$, $g \cdot 1^2$, f^3, $f^2 \cdot 1$, $f \cdot 1^2$, $1^3 \in L(6[O])$ must be linearly dependent because $\ell(6[O]) = 6$. Since $1, f, f^2, g, fg$ have pairwise different valuations $v_0(\cdot)$, they are linearly independent. Also, g^2, f^3 have different $v_0(\cdot)$ than $1, f, f^2, g, fg$. $\Rightarrow$ Both g^2, f^3 occur in the linear dependency.

Rescaling f and g, we can make both coefficients $=1$.

$\Rightarrow \varphi(E) \subseteq \{[X:Y:Z] \mid Y^2Z + \dots = \dots\}$

as in the statement of the theorem.

By Bézout's Theorem, the image $\varphi(E)$ is a degree 3 curve in $\mathbb{P}^2_k$.

$\Rightarrow \varphi(E) = \dots$ $\square$

<u>Rmk</u> If $\mathrm{char}(k) \neq 2, 3$, we can make $a_1 = a_2 = a_3 = 0$ using a linear transformation, so

$$\varphi(E) = \{[X:Y:Z] \mid Y^2Z = X^3 + a_4XZ^2 + a_6Z^3\}.$$

Then, we get the affine chart

$$\varphi(E) \cap \{Z \neq 0\} \cong \{(x,y) \in \mathbb{A}^2_k \mid y^2 = x^3 + a_4x + a_6\}$$

and the point at infinity:

$$\varphi(E) \cap \{Z = 0\} = \{[0:1:0]\} = \{\varphi(O)\}.$$

Assume now that $\varphi(E)$ is of this form (<u>Weierstraß form</u>).

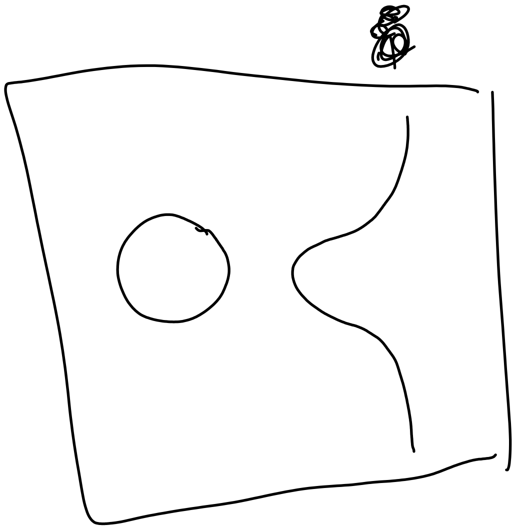
Rmk $E := \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}$ is an elliptic curve if and only if

$f(X,Z) := X^3 + a_4 X Z^2 + a_6 Z^3$ has no double root in $\mathbb{P}^1(\overline{K})$. ($\Leftrightarrow$ f is squarefree)

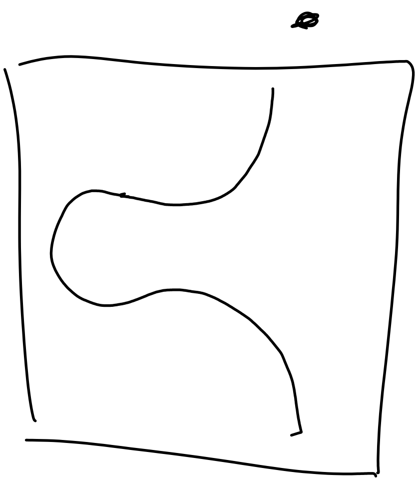
Pf Problem 1b on problem set 2 shows that $E \cap \{[x:y:z] \mid z \neq 0\}$ is smooth if and only if $f(x,z)$ has no double root. E is automatically smooth at $[0:1:0] \in E$.

By problem 1c on problem set 4, the genus is then $g_E = \frac{1}{2}(3-1)(3-2) = 1$. $\square$

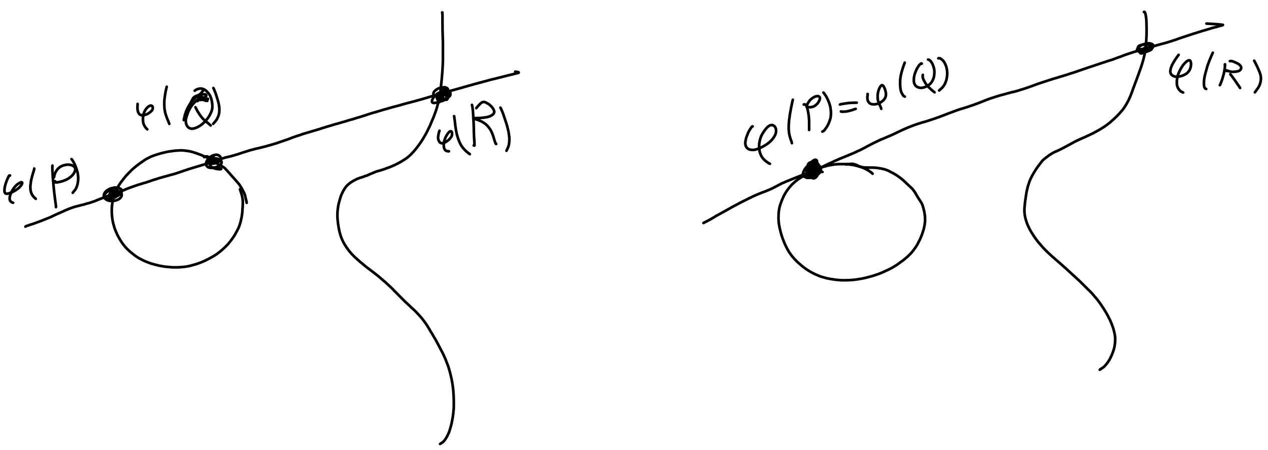
Rmk Let E be an elliptic curve over $\mathbb{R}$. Then, $\{[x:y:1] \in \varphi(E(\mathbb{R}))\} \subset \mathbb{R}^2$ "looks like this":



or



<u>Thm</u> Let $P, Q, R \in E(K)$. Then, $P+Q+R=\mathcal{O}$ if and only if $\varphi(P), \varphi(Q), \varphi(R) \in \mathbb{P}^2_{\bar{K}}$ are the three points of intersection of $\varphi(E)$ with a line $l \subset \mathbb{P}^2_K$ with multiplicities.



<u>Pf</u> $P+Q+R=O$

$\iff [P]-[O]+[Q]-[O]+[R]-[O]=0$ in $Cl(E)$

$\iff \exists f \in K(E)^\times : \operatorname{div}(f)=[P]+[Q]+[R]-3[O]$.

"$\Leftarrow$" Say $\varphi(P), \varphi(Q), \varphi(R)$ are the intersections of E with l. Let $a(X,Y,Z)$ be the linear polynomial defining l.

Let $f=\varphi^*\left(\dfrac{a(X,Y,Z)}{Z}\right)$. Then,

$\operatorname{div}(f)=[P]+[Q]+[R]-3[O]$

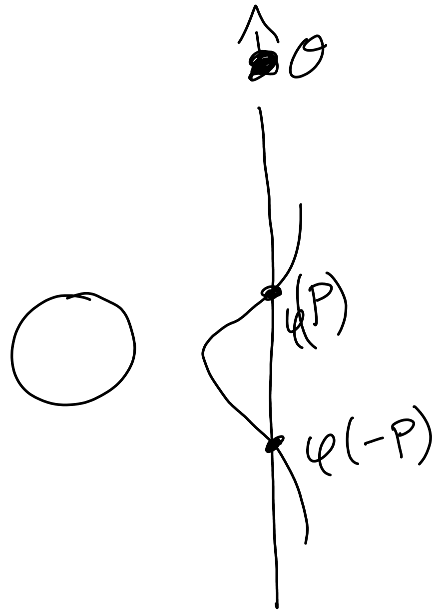
because $\varphi(O)$ is the only point of intersection of $\varphi(E)$ with $\{Z=0\}$ (with multiplicity 3).

"$\Rightarrow$" For any $P, Q \in E(K)$, there is exactly one line intersecting $\varphi(E)$ in $\varphi(P)$ and $\varphi(Q)$ with multiplicity. By Bézout, it intersects $\varphi(E)$ in exactly one more point $\varphi(R')$, which by "$\Leftarrow$" is the point satisfying $P+Q+R'=O$.

$\square$

Cor If $\varphi(P)=[x:y:z]$, then $\varphi(-P)=[x:-y:z]$.

Pf



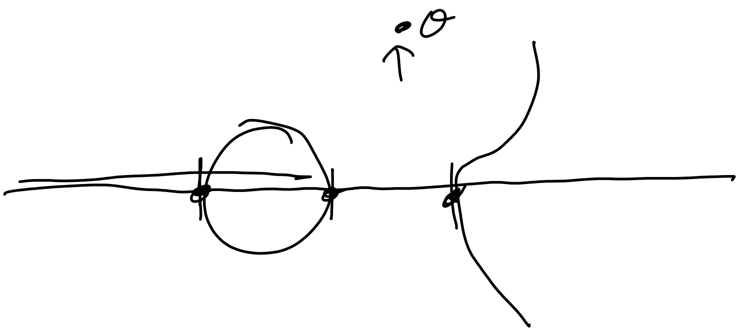
The "vertical" line through $\varphi(P)$ intersects $\varphi(E)$ in $[x:y:z], [x:-y:z], \underbrace{[0:1:0]}_{=\varphi(O)}$.

$\square$

Cor $2P=O$

$\Leftrightarrow y=0$ or $P=O$

$\Leftrightarrow$ The morphism $\psi: E \to \mathbb{P}^1$ is ramified at P.

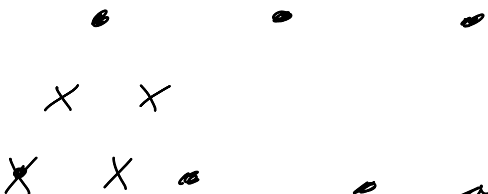


Rmk There are exactly four (distinct) points $P \in E(\overline{K})$ with $2P = O$.

Pf 1 They are $P = O$ and $P = [x : 0 : z]$, where $[x : z]$ is one of the roots of

$$f(x, z) = X^3 + a_4 X Z^2 + a_6 Z^3. \qquad \square$$

Pf 2 Use that $E(\mathbb{C}) = \mathbb{C}/\Lambda$ if $K \subseteq \mathbb{C}$. Even if $K \not\subseteq \mathbb{C}$, we can assume that $K \subseteq \mathbb{C}$ by the Lefschetz principle: Basically, show that we can assume that the field ext. $K|\mathbb{Q}$ is generated by finitely many elements. Then there is an embedding $K \hookrightarrow \mathbb{C}$ because $\mathbb{C}$ has infinite transcendence degree over $\mathbb{Q}$!



Pf 3 Riemann - Hurwitz for $\psi : E \longrightarrow \mathbb{P}^1$

$$\Rightarrow \underbrace{2g_E - 2}_{0} = \underbrace{\deg(\psi)}_{2} \cdot \underbrace{(2g_{\mathbb{P}^1} - 2)}_{-2} + \deg(R_E)$$

$$\Rightarrow \deg(R_E) = 4$$

Since $\deg(\psi) = 2$, every point has ramification index 1 or 2, so there are exactly 4 points of ramification. $\square$

Thm The maps $+ : E \times E \longrightarrow E$
$(P, Q) \longmapsto P+Q$

and $- : E \longrightarrow E$ are morphisms (defined over k).
$P \longmapsto -P$

(Cover $E \times E$ by open affine varieties U_i. Then, the restrictions $+ : U_i \longrightarrow E$ are morphisms.)

Ese Let $E = \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}$,
$P_1 = [x_1 : y_1 : 1]$, $P_2 = [x_2 : y_2 : 1]$.
If $P_1 \neq \pm P_2$, then $P_1 + P_2 = [x_3 : y_3 : 1]$,
where
$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \dots$$

If $P = [x : y : 1]$, $y \neq 0$, then
$2P = [x' : y' : 1]$, where
$$x_3 = \frac{x^4 - 2a_4 x^2 - 8a_6 x + a_4^2}{4x^3 + 4a_4 x + 4a_6}$$

$$y_3 = \dots$$

2.2. Isogenies

<u>Def</u> An <u>isogeny</u> between elliptic curves E_1, E_2 is a morphism $\phi : E_1 \longrightarrow E_2$ sending $O \in E_1$ to $O \in E_2$.

We denote the group of isogenies $\phi : E_1 \to E_2$ by $\mathrm{Hom}(E_1, E_2)$ (where $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$).

<u>Ex</u> The trivial ($=$ constant) isogeny $\phi = 0$:

$$\phi(P) = O \quad \forall P \in E_1(\bar{K})$$

<u>Ex</u> The multiplication by $m \in \mathbb{Z}$ isogeny

$$[m] : E \longrightarrow E$$
$$P \longmapsto mP$$

(It's a morphism because $+ : E \times E \to E$ and $- : E \to E$ are.)

<u>Rmk</u> We get a commutative diagram

$$\begin{tikzcd}
P \in E_1 \arrow[r, "\phi"] \arrow[d, leftrightarrow] & E_2 \ni \phi(P) \arrow[d, leftrightarrow] \\
{[P]-[O]} \in \mathrm{Cl}^0(E_1) \arrow[r, "\phi"'] & \mathrm{Cl}^0(E_2) \ni [\phi(P)] - [O]
\end{tikzcd}$$

<u>Cor</u> Any isogeny is a group homomorphism.

<u>Rmk</u> Any isogeny $\phi \neq 0$ is unramified.

In other words: Any $Q \in E_2(\overline{K})$ has exactly $\deg(\phi)$ preimages in $E_1(\overline{K})$.

In particular: $|\ker(\phi)(\overline{K})| = \deg(\phi)$.

<u>Pf 1</u> Riemann-Hurwitz:

$$\underbrace{2g_{E_1}-2}_{0} = \deg(\phi)\cdot(\underbrace{2g_{E_2}-2}_{0}) + \deg(R_f)$$

$$\Rightarrow \deg(R_f) = 0$$

□

<u>Pf 2</u> The preimage of $Q \in E_2(\overline{K})$ under the surjective group hom. $\phi: E_1(\overline{K}) \to E_2(\overline{K})$ is a coset of $\ker(\phi)(\overline{K})$.

$\Rightarrow$ All preimages have the same size.

$\Rightarrow$ Since ϕ can only be ramified at finitely many points, it's unramified everywhere.

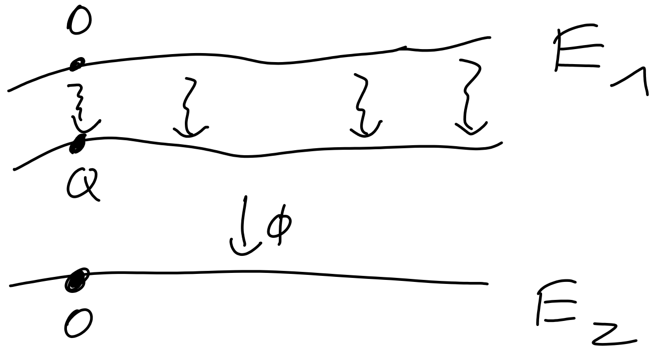
□

Lemma If $\phi : E_1 \to E_2$ is a nontrivial isogeny, then the map $\phi^* : K(E_2) \hookrightarrow K(E_1)$ makes $K(E_1)$ a Galois extension of $\phi^*(K(E_2))$.

We have a group isomorphism

$$\ker(\phi)(\bar{K}) \xrightarrow{\sim} \mathrm{Gal}(K(E_1) \mid \phi^*(K(E_2)))$$
$$Q \longmapsto \tau_Q^*$$

where $\tau_Q : E_1 \to E_1$ and $\tau_Q^* : K(E_1) \to K(E_1)$.
$P \mapsto P + Q$



Pf well-defined: We have

$$\phi(\tau_Q(P)) = \phi(P+Q) = \phi(P) \quad \forall P \in E_1(\bar{K}), \text{ so } \phi \circ \tau_Q = \phi.$$

$$\Rightarrow \tau_Q^* \circ \phi^* = \phi^*.$$

Hence, $\tau_Q^*(x) = x \quad \forall x \in \phi^*(K(E_1))$.

$\Rightarrow \tau_Q^* \in \mathrm{Gal}(K(E_1) \mid \phi^*(K(E_2)))$.

group hom: clear

injective: τ_Q^* determines τ_Q and therefore

$$Q = \tau_Q(O)$$

Gal. ext.
+ surjective: $[K(E_1) : \phi^*(K(E_2))] = \deg(\phi) = |\ker(\phi)(\overline{K})|$.

$\square$

Lemma If $\alpha : E_1 \longrightarrow E_3$, $\beta : E_1 \longrightarrow E_2$ are isogenies, there is an isogeny $\gamma : E_2 \to E_3$ with $\alpha = \gamma \circ \beta$ if and only if

$$\ker(\alpha)(\overline{K}) \supseteq \ker(\beta)(\overline{K})$$

$$\begin{tikzcd} E_1 \arrow[rr, "\alpha"] \arrow[dr, "\beta"'] & & E_3 \\ & E_2 \arrow[ur, dashed, "\gamma"'] & \end{tikzcd}$$

Rmk If $\beta \neq 0$, then $\beta : E_1(\overline{K}) \to E_2(\overline{K})$ is surjective, so γ is unique.

Pf of Lemma

Assume $\alpha, \beta \neq 0$. There is a (unique) group homomorphism $\gamma : E_2(\overline{K}) \to E_3(\overline{K})$ satisfying $\alpha = \gamma \circ \beta$. We need to show that it is a morphism.

$$\begin{tikzcd}
K(E_1) & & K(E_3) \arrow[ll, "\alpha^*"'] \arrow[dl, dashed, "\gamma^*"] \\
& K(E_2) \arrow[ul, bend left, "\beta^*"] &
\end{tikzcd}$$

$\ker(\alpha) \supseteq \ker(\beta)$ implies that

$Gal(K(E_1)/\alpha^*(K(E_3))) \supseteq Gal(K(E_1)/\beta^*(K(E_2)))$

$\Rightarrow \alpha^*(K(E_3)) \subseteq \beta^*(K(E_2))$

$\Rightarrow$ There is a field homomorphism $\overline{\gamma}^* : K(E_3) \hookrightarrow K(E_2)$ with $\alpha^* = \beta^* \circ \overline{\gamma}^*$.

Let $\overline{\gamma} : E_2 \dashrightarrow E_3$ be the corresponding rational map. Since $\alpha^* = \beta^* \circ \overline{\gamma}^*$, we have $\alpha = \overline{\gamma} \circ \beta$ on some nonempty open subset of $E_1(\overline{K})$. Then, $\overline{\gamma} = \gamma$ on some nonempty open subset U of $E_2(\overline{K})$ where $\overline{\gamma}$ is defined. Let $P \in U$ and consider any $Q \in E_2(\overline{K})$. Then,

$$\gamma(R) = \gamma(R - Q + P) + \gamma(Q - P)$$
$$= \overline{\gamma}(R - Q + P) + \gamma(Q - P)$$

for any $R \in U + Q - P$.

But then

$$\bar{\bar{\gamma}} : E_2 \dashrightarrow E_3$$
$$R \longmapsto \bar{\gamma}(R-Q+P) + \gamma(Q-P)$$

is a rational function which

a) is defined at every point in the open neighborhood $U+Q-P$ of Q, and

b) agrees with γ, and therefore with $\bar{\gamma}$, wherever both $\bar{\gamma}$ and $\bar{\bar{\gamma}}$ are defined, so in fact $\bar{\gamma} = \bar{\bar{\gamma}}$.

(some nonempty open subset of E_2)

$\Rightarrow \bar{\gamma}$ is defined everywhere. $\square$

<u>Note</u> Any rational map $C \dashrightarrow \mathbb{P}^n$ for a <u>smooth</u> curve C is a morphism!

(so the last part of the proof is unnecessary in this case. But it generalises nicely to higher-dimensional abelian varieties.)

Thm The group hom. $\mathbb{Z} \longrightarrow \mathrm{End}(E)$ is
$m \longmapsto [m]$

injective.

Pf Assume $[m] = 0$, $m \neq 0$.

$m \mid 2^k(2^l - 1)$ for some $k \geq 0$, $l \geq 1$.

We've shown that $\deg([2]) = 4$.

$\Rightarrow \deg([2^l]) = 4^l \neq 1$

$\Rightarrow [2^l] \neq [1] \Rightarrow [2^l - 1] \neq 0$

The morphisms $[2]$ and $[2^l - 1]$ are nonconstant (= dominant = surjective).

$\Rightarrow [2^k(2^l - 1)] \neq 0 \Rightarrow [m] \neq 0$.

$\square$

Def The *dual isogeny* $\hat{\phi}$ of $\phi \neq 0$ is the map given by the following commutative diagram:

$$\begin{tikzcd}
E_2 \arrow[d, leftrightarrow] & E_1 \arrow[l, "\hat{\phi}"'] \arrow[d, leftrightarrow] \\
Cl^0(E_2) & Cl^0(E_1) \arrow[l, "\phi^*"]
\end{tikzcd}$$

The dual of $\phi = 0$ is $\hat{\phi} = 0$.

Ex $\widehat{id} = id$

Rmk $\hat{\phi}$ is a group hom. because ϕ^* is.
But we need to prove it's a morphism!

Rmk $\widehat{\phi_1 \circ \phi_2} = \hat{\phi}_2 \circ \hat{\phi}_1$

Rmk $\phi \circ \hat{\phi} = [\deg(\phi)]$, where we let $\deg(\phi) = 0$ if $\phi = 0$.

Pf $\phi(\phi^*(D)) = \deg(\phi) \cdot D$ $\square$

Rmk $\hat{\phi} \circ \phi = [\deg(\phi)]$

Pf Let $P \in E_1$.

$$\begin{tikzcd}
\hat{\phi}(\phi(P)) \arrow[d, mapsto] & \phi(P) \arrow[l, mapsto] \arrow[d, mapsto] \\
\displaystyle\sum_{P' \in \phi^{-1}(\phi(P))} ([P'] - [O]) - \sum_{T \in \phi^{-1}(O)} ([T] - [O]) & {[\phi(P)] - [O]} \arrow[l, mapsto]
\end{tikzcd}$$

ϕ is unramified, so all multiplicities are 1

$$\Rightarrow \hat{\phi}(\phi(P)) = \sum_{P' \in \phi^{-1}(\phi(P))} P' - \sum_{T \in \phi^{-1}(O)} T$$

$$= \sum_{T \in \ker(\phi)} ((P+T) - T)$$

$$= \deg(\phi) \cdot P. \qquad \square$$

Thm $\hat{\phi}$ is a morphism (and therefore an isogeny).

Pf Assume $\phi \neq 0$.

$$\begin{tikzcd} E_1 \arrow[rr, "{[\deg(\phi)]}"] \arrow[dr, "\phi"'] & & E_1 \\ & E_2 \arrow[ur, dashed, "\hat{\phi}"'] & \end{tikzcd}$$

Since $|\ker(\phi)| = \deg(\phi)$, every element of $\ker(\phi)$ is $\deg(\phi)$-torsion.

$\Rightarrow \ker(\phi) \subseteq \ker([\deg(\phi)])$

$\Rightarrow$ There is a morphism $\tilde{\phi} : E_2 \to E_1$ such that $\tilde{\phi} \circ \phi = [\deg(\phi)]$.

Since $\hat{\phi} \circ \phi = [\deg(\phi)]$ and ϕ is surjective, we have $\tilde{\phi} = \hat{\phi}$. $\square$

Def Elliptic curves E_1, E_2 are isomorphic if there is an isogeny $\phi : E_1 \to E_2$ which is an isomorphism (i.e. has degree 1).

They are isogenous if there is a nonconstant isogeny $\phi : E_1 \to E_2$. (Symmetry follows from existence of $\hat{\phi}$.)

Thm $\widehat{\phi_1+\phi_2} = \hat{\phi}_1 + \hat{\phi}_2$ for any isogenies $\phi_1, \phi_2 : E_1 \longrightarrow E_2$.

Pf (For more details, see Thm III. 6.2 in Silverman, or Exercise 3.31 in Silverman).

For any $P \in E_1$,

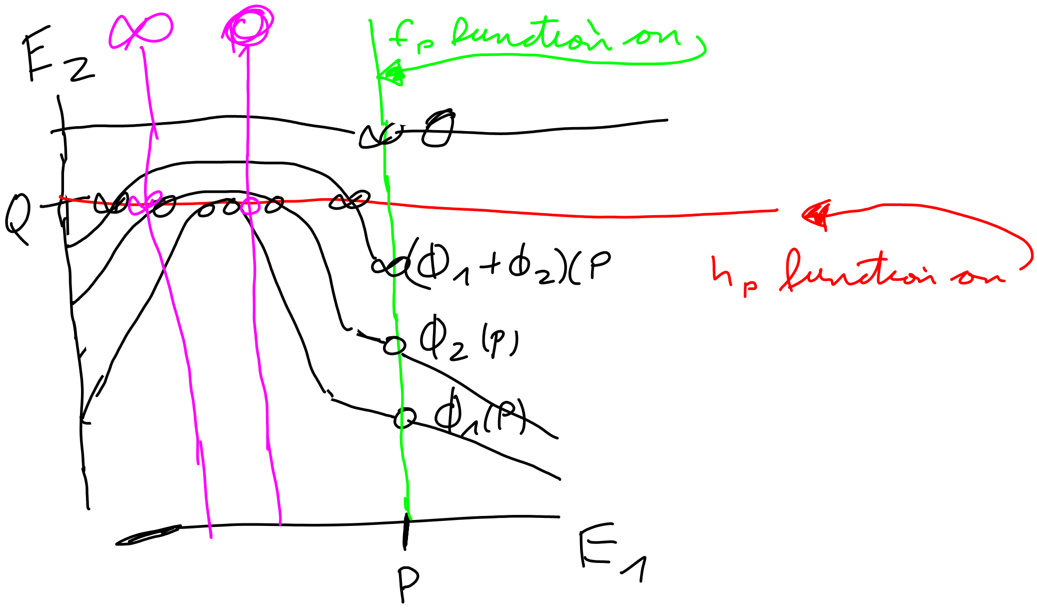
$(\phi_1+\phi_2)(P) = \phi_1(P) + \phi_2(P)$ in E_2 means that there is a rational function $f_P \in K(E_2)^\times$ such that

$$\big([\phi_1(P)]-[O]\big)+\big([\phi_2(P)]-[O]\big)-\big([(\phi_1+\phi_2)(P)]-[O]\big) = \operatorname{div}(f_P).$$

We take $f_P =$ quotient of two homogeneous degree 1 pol. with roots at

$\phi_1(P), \phi_2(P), -(\phi_1(P)+\phi_2(P))$
and at
$\phi_1(P)+\phi_2(P), -(\phi_1(P)+\phi_2(P)), O$.
respectively

The coefficients of the rational function f_P are rational functions in the coordinates of P (at all points P where they are defined).



$\leadsto$ We get a rational function g on $E_1 \times E_2$ with $g(P, Q) = f_P(Q)$ whenever both sides are defined.

For almost all $Q \in E_2$ (those not on a "horizontal" zero or pole of g), we get a rational function $h_Q \in K(E_1)^\times$, with $g(P, Q) = h_Q(P)$ whenever both sides are defined.

$$\operatorname{div}(h_Q) = \phi_1^*(Q) + \phi_2^*(Q) - (\phi_1+\phi_2)^*(Q) + D$$

for some fixed divisor $D \in \operatorname{Div}(E_1)$ independent of Q (corresponding to "vertical" zeros and poles of g).

$\Rightarrow \phi_1^*(Q) + \phi_2^*(Q) - (\phi_1+\phi_2)^*(Q) = -D$ in $\mathcal{Cl}(E_1)$
for almost all $Q \in E_2$

$\Rightarrow \underbrace{\hat{\phi}_1(Q) + \hat{\phi}_2(Q) - \widehat{\phi_1+\phi_2}(Q)}_{\text{morphism in } Q} = R$ for almost all $Q \in E_2$
and some <u>fixed</u> $R \in E_1$

$\underset{\substack{\uparrow \\ \text{continuity}}}{\Rightarrow} \hat{\phi}_1(Q) + \hat{\phi}_2(Q) - \widehat{\phi_1+\phi_2}(Q) = R$ for <u>all</u> $Q \in E_2$.

For $Q = 0$, $LHS = 0$. $\Rightarrow R = 0$

$\Rightarrow \hat{\phi}_1(Q) + \hat{\phi}_2(Q) = \widehat{\phi_1+\phi_2}(Q)$ for all $Q \in E_2$.

$\square$

<u>Cor</u> $\widehat{[m]} = [m]$

<u>Pf</u> Induction over $|m|$. $\square$

<u>Cor</u> $\deg([m]) = m^2$.

In other words, $\# E[m] = m^2$.

including all points with coordinates in $\overline{K}$

<u>Pf</u> $\widehat{[m]} \circ [m] = [\deg([m])]$.

$\widehat{[m]} \circ [m] = [m^2]$

Use that $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ is injective. $\square$

Cor $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.

Pf HW.

Thm $\deg(\hat{\phi}) = \deg(\phi)$

Pf assume $\phi \neq 0$.

$$\hat{\phi} \circ \phi = [\deg(\phi)]$$

$$\Rightarrow \deg(\hat{\phi}) \deg(\phi) = \deg(\phi)^2$$

$$\Rightarrow \deg(\hat{\phi}) = \deg(\phi).$$

□

Thm $\hat{\hat{\phi}} = \phi$

Pf $\hat{\hat{\phi}} \circ \hat{\phi} = [\deg(\hat{\phi})] = [\deg(\phi)] = \phi \circ \hat{\phi}$.

If $\phi \neq 0$, then $\hat{\phi} \neq 0$, so $\hat{\phi}$ is surjective.

$\Rightarrow \hat{\hat{\phi}} = \phi$.

□

Thm $\deg : \operatorname{End}(E) \longrightarrow \mathbb{Z}$ is a positive definite quadratic form.

In other words, the following is bilinear:

$$\langle \cdot , \cdot \rangle : \operatorname{End}(E) \times \operatorname{End}(E) \longrightarrow \tfrac{1}{2}\mathbb{Z}$$

$$(\phi_1, \phi_2) \longmapsto \tfrac{1}{2}(\deg(\phi_1 + \phi_2) - \deg(\phi_1) - \deg(\phi_2))$$

Pf $[\deg(\phi_1 + \phi_2) - \deg(\phi_1) - \deg(\phi_2)] = \widehat{\phi_1 + \phi_2} \circ (\phi_1 + \phi_2) - \hat{\phi}_1 \circ \phi_1 - \hat{\phi}_2 \circ \phi_2$

$= \hat{\phi}_1 \circ \phi_2 + \hat{\phi}_2 \circ \phi_1$, which is linear in ϕ_1, ϕ_2.

□

2.3. Aside: The Hasse-Weil bound

<u>Thm</u> Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then,

$$\left| \# E(\mathbb{F}_q) - (q+1) \right| \leq 2\sqrt{q}.$$

<u>Intuition</u> $E \cap \{z \neq 0\} = \{ y^2 = x^3 + a_4 x + a_6 \}$

The probability that a random number $t \in \mathbb{F}_q^\times$ is a square is $\frac{1}{2}$ if q is odd.

$\rightsquigarrow$ The expected number of $y \in \mathbb{F}_q$ such that $y^2 = t$ is 1.

$\rightsquigarrow$ Expect one point $(x, y) \in (E \cap \{z \neq 0\})(\mathbb{F}_q)$ on average for a given value $x \in \mathbb{F}_q$.

$\rightsquigarrow$ Expect $\#(E \cap \{z \neq 0\})(\mathbb{F}_q) \approx q$,

so $\# E(\mathbb{F}_q) \approx q + 1$.

<u>"Pf"</u> Consider the <u>Frobenius morphism</u>

$$\begin{aligned} \varphi : E &\longrightarrow E \\ [x:y:z] &\longmapsto [x^q : y^q : z^q] \end{aligned}.$$

For any $P \in E(\overline{\mathbb{F}}_q)$, we have $\varphi(P) = P$ if and only if $P \in E(\mathbb{F}_q)$.

Then, $E(\mathbb{F}_q) = \{ P \in E(\overline{\mathbb{F}_q}) \mid \varphi(P) = P \}$

$$= \{ P \in E(\overline{\mathbb{F}_q}) \mid (\varphi - id)P = 0 \}$$

$$= \ker(\varphi - id).$$

$$\Rightarrow \# E(\mathbb{F}_q) = \# \ker(\varphi - id) \underset{\varphi - id \text{ is separable}}{=} \deg(\varphi - id).$$

Since $\deg : End(E) \longrightarrow \mathbb{Z}$ is a positive definite quadratic form, we get the Cauchy-Schwarz inequality

$$|\langle \varphi, id \rangle| \leq \sqrt{\underbrace{\deg(\varphi)}_{q} \cdot \underbrace{\deg(id)}_{1}}$$

$$\|$$

$$\frac{1}{2} \left| \underbrace{\deg(\varphi - id)}_{\# E(\mathbb{F}_q)} - \underbrace{\deg(\varphi)}_{q} - \underbrace{\deg(id)}_{1} \right|$$

$$\Rightarrow \left| \# E(\mathbb{F}_q) - (q+1) \right| \leq 2\sqrt{q}.$$

$\square$

$$\boxed{\begin{array}{c} \mathbb{F}_p(T^{1/p}) \\ | \\ \mathbb{F}_p(T) \end{array}}$$

A. Heights

<u>Reference</u> Chapter 2 of Lectures on the Mordell-Weil Theorem by J-P Serre.

A.1. Definition

<u>Def</u> The <u>height</u> of $P = [x_0 : \dots : x_n] \in \mathbb{P}^n(\mathbb{Q})$ with $x_0, \dots, x_n \in \mathbb{Z}$ relatively prime is

$$H(P) := \max(|x_0|, \dots, |x_n|).$$

<u>Def</u> More generally, if K is a global field, the <u>height</u> of $P = [x_0 : \dots : x_n] \in \mathbb{P}^n(K)$ with $x_0, \dots, x_n \in K$ is

$$H_K(P) := \prod_{v \text{ place of } K} \max_i |x_i|_v .$$

(Here, $|x|_{\mathfrak{q}} = q^{-v_{\mathfrak{q}}(x)}$ if $v = v_{\mathfrak{q}}$ is nonarch. with residue field $\mathbb{F}_q$

$|x|_v = |i(x)|$ if v corresponds to the real embedding $i : K \hookrightarrow \mathbb{R}$

$|x|_v = |i(x)|^2$ if v corresponds to (nonreal) complex embedding $i : K \hookrightarrow \mathbb{C}$)

Rmk $\prod_v \max_i |\lambda x_i|_v = \underbrace{\prod_v |\lambda|_v}_{1} \cdot \prod_v \max_i |x_i|_v$

(product formula)

for any $\lambda \in K^\times$.

$\Rightarrow H_K(P)$ is well-defined (indep. of the choice of projective coordinates $x_0, \dots, x_n$ of P).

Rmk For $K = \mathbb{Q}$, the two definitions agree.

Pf If $x_0, \dots, x_n \in \mathbb{Z}$ are relatively prime, then $\max(|x_0|_p, \dots, |x_n|_p) = p^{-\min(v_p(x_0), \dots, v_p(x_n))}$

$= p^{-0} = 1$.

$\square$

Rmk $H_L(P) = H_K(P)^{[L:K]}$ for a separable field ext. $L|K$ and a point $P \in \mathbb{P}^n(K)$.

Pf If w is a place of L above a place v of K and $x \in K$, then $|x|_w = |x|_v^{e(w|v) f(w|v)}$.

$\sum_{w|v} e(w|v) f(w|v) = [L:K]$.

$\square$

Hence, the following makes sense:

Def $H_K(P) := H_L(P)^{\frac{1}{[L:K]}}$ for any $P \in \mathbb{P}^n(L)$ defined over a separable field ext. $L|K$.

Def The logarithmic height of P is

$$h_K(P) := \log H_K(P).$$

A.2. Properties

Rmk $H(P) \geq 1$, $h(P) \geq 0$ $\forall P \in \mathbb{P}^n(K)$.

Pf If $x_i \in K^\times$, then $\prod_v |x_i|_v = 1$.

$$\Rightarrow \prod_v \max_j |x_j|_v \geq 1.$$ $\square$

Thm A.2.1 For any K and any $t \geq 0$, there are only finitely many points $P \in \mathbb{P}^n(K)$ with $h(P) \leq t$.

(This is clear for $K = \mathbb{Q}$.)

Thm A.2.2 Let $M \in GL_{n+1}(K)$ and let $\alpha_M : \mathbb{P}^n_K \longrightarrow \mathbb{P}^n_K$ be the corresponding morphism. Then, $h_K(\alpha_M(P)) \underset{M}{\approx} h_K(P)$ for any $P \in \mathbb{P}^n(\bar{K})$.

(meaning: $|h(\alpha(P)) - h(P)| \leq C_M$ for some constant C_M depending on M, but not on P,
$h_K(\alpha_M(P)) = h_K(P) + O_M(1)$)

Pf HW. $\square$

Thm Consider the Segre embedding

$$\mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^{(n+1)(m+1)-1}$$

$$(P,Q) = ([x_0:\dots:x_n],[y_0:\dots:y_m]) \mapsto [x_0y_0 : x_0y_1 : \dots : x_ny_m] =: P \otimes Q$$

We have $h(P \otimes Q) = h(P) + h(Q)$.

Pf $H(P \otimes Q) = \prod_v \max_{i,j} |x_i y_j|_v = \prod_v \max_i |x_i|_v \cdot \max_j |y_j|_v$
$= H(P) \cdot H(Q)$. $\square$

Thm A.2.4 Consider the Veronese embedding of degree $d \geq 1$

$$\mathbb{P}^n \longrightarrow \mathbb{P}^{\binom{n+d}{d}-1}$$

$$P=[x_0:\cdots:x_n] \longmapsto [x_0^d : x_0^{d-1}x_1 : \cdots : x_n^d] =: P^{(d)}$$

all degree d monomials in $x_0, \ldots, x_n$

and the morphism

$$\mathbb{P}^n \longrightarrow \mathbb{P}^n$$

$$P=[x_0:\cdots:x_n] \longmapsto [x_0^d : \cdots : x_n^d] =: P^d.$$

We have $h(P^{(d)}) = h(P^d) = d \cdot h(P)$.

Pf $$H(P^{(d)}) = \prod_v \max_{\substack{e_0,\ldots,e_n \geq 0 \\ e_0+\cdots+e_n=d}} |x_0^{e_0}\cdots x_n^{e_n}|_v$$

$$= \prod_v \max_i \underbrace{|x_i^d|_v}_{|x_i|_v^d} = H(P^d) = H(P)^d.$$

$\square$

Thm A.2.5 Consider the projection

$$\pi : \mathbb{P}^n \setminus \{[0:\dots:0:1]\} \longrightarrow \mathbb{P}^{n-1}$$

$$[x_0 : \dots : x_n] \longmapsto [x_0 : \dots : x_{n-1}]$$

We have $h(\pi(P)) \leq h(P)$ for all

$[0:\dots:0:1] \neq P \in \mathbb{P}^n(\overline{K})$.

Pf $H(\pi(P)) = \prod_v \max_{i \leq n-1} |x_i|_v \leq \prod_v \max_{i \leq n} |x_i|_v = H(P)$.

$\square$

Rmk $h(\pi(P))$ can be arbitrarily much smaller than $h(P)$.

For example, take $P = [r : \dots : r : 1] \in \mathbb{P}^n(\mathbb{Q})$ with $0 \neq r \in \mathbb{Z}$.

$\Rightarrow \pi(P) = [r : \dots : r] = [1 : \dots : 1]$.

$\Rightarrow h(\pi(P)) = 0$, $h(P) = \log |r|$.

"For $q | r$, P is q-adically close to the point $[0 : \dots : 0 : 1]$ where π is not defined."

Lemma Let $V \subseteq \mathbb{P}^n_K$ be a hyperplane not containing $[0:\dots:0:1]$ and consider the projection $\pi: V \to \mathbb{P}^{n-1}$ as above. Then, $h(\pi(P)) \underset{V}{\approx} h(P)$ for all $P \in V(\overline{K})$.

Pf π is a linear isomorphism.
There is a linear transformation
$M: K^n \longrightarrow K^{n+1}$ with $\alpha_M(\pi(P)) = P$ for all $P \in V$.
Apply Thm A.2.2.: $\square$

More generally:

Thm A.2.6. Let $V \subseteq \mathbb{P}^n_K$ be a projective variety not containing $[0:\dots:0:1]$ and consider the projection

$$\pi : V \longrightarrow \mathbb{P}^{n-1}$$
$$[x_0:\dots:x_n] \mapsto [x_0:\dots:x_{n-1}]$$

Then, $h(\pi(P)) \underset{V}{\approx} h(P)$ for all $P \in V(\overline{K})$.

Pf Let $f \in K[X_0,\dots,X_n]$ be any homogeneous degree d polynomial which vanishes on V but not at $[0:\dots:0:1]$.

$\Rightarrow$ The monomial x_n^d occurs in f, so x_n^d is a fixed linear combination of the other degree d monomials in $x_0, \dots, x_n$ for any point $P \in V(\overline{K})$.

$\Rightarrow P^{(d)}$ lies in a fixed hyperplane $W \subseteq \mathbb{P}^{\binom{n+d}{d}-1}$ not containing $[0 : \dots : 0 : 1]$

coord. corr. to x_n^d.

$$\Rightarrow \quad d \cdot h(P)$$

$$= h(P^{(d)})$$

$$\underset{W}{\approx} h(\pi'(P^{(d)}))$$

Lemma

$\mathbb{P}^{\binom{n+d}{d}-1} \to \mathbb{P}^{\binom{n+d}{d}-2}$ omitting the coord. corr. to x_n^d

$$= h(P^{(d-1)} \otimes \pi(P))$$

coord. are the degree d mon. divisible by some x_i with $i \neq n$, so all the monomials except x_n^d

$$= h(P^{(d-1)}) + h(\pi(P))$$

$$= (d-1)\, h(P) + h(\pi(P)).$$

$$\Rightarrow h(\pi(P)) \underset{W}{\approx} h(P). \qquad \square$$

More generally:

Thm A.2.7 Let M be a linear map $K^{n+1} \to K^{m+1}$

and let $\alpha_M : \mathbb{P}^n \setminus \{[x_0 : \cdots : x_n] \mid M(x_0, \ldots, x_n) \neq 0\} \longrightarrow \mathbb{P}^m$

be the corr. morphism.

Then, $h(\alpha_M(P)) \underset{M}{\lesssim} h(P)$ for all $P \in \mathbb{P}^n(\bar{K})$ $\overset{\shortparallel}{[x_0 : \cdots : x_n]}$

with $M(x_0, \cdots, x_n) \neq 0$

(meaning $h(P) - h(\alpha_M(P)) \geq C_M$ for some constant C_M depending only on M,

$$h(\alpha(P)) \leq h(P) + O_M(1) \quad)$$

Pf After linear transformation on $\mathbb{P}^n$ and $\mathbb{P}^m$, we can assume (using Thm A.2.2) that M sends
$(x_0, \ldots, x_n)$ to $(x_0, \ldots, x_s, 0, \ldots, 0)$,
where $s = \text{rank}(M)$.

W.l.o.g. $s = m$, so M is the proj. onto the first $m+1$ coordinates, i.e.

the composition of $n-m$ projections as in Thm A.2.5. $\square$

<u>Thm A.2.8</u> Let M as above and let $V \subseteq \mathbb{P}^n_K$ be a proj. var. not containing any $P = [x_0 : \cdots : x_n] \in V(\bar{K})$ with $M(x_0, \dots, x_n) = 0$, so that $\alpha_M : V \longrightarrow \mathbb{P}^m$ is well-defined.

Then, $h(\alpha_M(P)) \underset{M,V}{\approx} h(P)$ for all $P \in V(\bar{K})$.

<u>Pf</u> as above, using Thm A.2.6. $\square$

Cor A.2.9 Let $f_0, \dots, f_m \in K(X_0, \dots, X_n)$ be homogeneous of degree d and consider the map

$$\varphi : \mathbb{P}^n \setminus V(f_0, \dots, f_m) \longrightarrow \mathbb{P}^m$$
$$[x_0 : \dots : x_n] \longmapsto [f_0(x_0, \dots, x_n) : \dots : f_m(x_0, \dots, x_n)]$$

Then, $h(\varphi(P)) \underset{\varphi}{\lesssim} d \cdot h(P) \; \forall P \in \mathbb{P}^n(\bar{K}) \setminus V(f_0, \dots, f_m)$

Cor A.2.10 Let $V \subseteq \mathbb{P}^n_K$ be a projective variety and let $f_0, \dots, f_m \in K[X_0, \dots, X_n]$ be homogeneous of degree d and assume that $f_0, \dots, f_m$ have no common zeroes in $V(\bar{K})$, so that

$$\varphi : V \longrightarrow \mathbb{P}^m$$
$$[x_0 : \dots : x_n] \longmapsto [f_0(x_0, \dots, x_n) : \dots]$$

is well-defined.

Then, $h(\varphi(P)) \underset{\varphi}{\approx} d \cdot h(P)$ for all $P \in V(\bar{K})$.

A.3. Height and divisor classes

Thm A.3.1 Let C be a smooth projective curve. We can associate to every $D \in \mathrm{Div}(C)$ a function $h_D : C(\overline{K}) \to \mathbb{R}$ such that

i) $h_D(P) \underset{\varphi}{\approx} h(\varphi(P))$ for any morphism $\varphi : C \to \mathbb{P}^n$ defined by functions $f_0, \dots, f_n \in K(C)$ with associated divisor $D = \sum_Q n_Q Q$ and any $P \in C(\overline{K})$.

(D minimal s.t. $f_0, \dots, f_n \in L(D)$.

or: $n_Q = - \min_i v_Q(f_i)$)

ii) $h_{D+D'}(P) \underset{D,D'}{\approx} h_D(P) + h_{D'}(P) \quad \forall P \in C(\overline{K})$.

Rmk: If D, D' lie in the same divisor class, then $h_D(P) \underset{D,D'}{\approx} h_{D'}(P)$ for any $P \in C(\overline{K})$.

Pf: If $\varphi : C \to \mathbb{P}^n$ is def. by $f_0, \dots, f_n$ with divisor D, then φ is also def. by $f_0 g, \dots, f_n g$ with divisor $D + \mathrm{div}(g)$ for any $g \in K(C)^\times$. $\square$

Remark h_D is unique up to bounded functions: If h'_D denotes other fcts as above, then

$$h_D(P) \underset{h_D,\, h'_D,\, D}{\approx} h'_D(P) \quad \forall D \in \mathrm{Div}(C),\ P \in C(\bar{K}).$$

Pf By Riemann-Roch, there is a morphism associated to any divisor of degree $\geq 2g_C$ (then, $\ell(D-P) = \ell(D) - 1\ \forall P$).
Any divisor D, can be written as $D = D_1 - D_2$ with $\deg(D_1), \deg(D_2) \geq 2g_C$.

$$\Rightarrow h_D(P) \underset{ii}{\approx} h_{D_1}(P) - h_{D_2}(P) \underset{i}{\approx} h(\varphi_1(P)) - h(\varphi_2(P))$$

$$\underset{i}{\approx} h'_{D_1}(P) - h'_{D_2}(P) \underset{ii}{\approx} h'_D(P),$$

where φ_i is any morphism associated to D_i.

$\square$

Rmk If $\deg(D)>0$, then

a) $h_D(P) \underset{D}{\gtrsim} 0 \quad \forall P \in C(\bar{K})$

b) For any finite field ext. $L|K$ and any $t \in \mathbb{R}$, there are only finitely many $P \in E(L)$ s.t. $h_D(P) \leq t$.

Pf For $n \geq 2g+1$, there is a closed embedding φ associated to nD, so

a) $n \cdot h_D(P) \underset{ii}{\approx} h_{nD}(P) \underset{i}{\approx} h(\underbrace{\varphi(P)}_{\in \mathbb{P}^m_K(\bar{K})}) \geq 0$

b) $h_D(P) \leq t \Rightarrow h_{nD}(P) \lesssim nt$

$$h_{nD}(P) \approx h(\underbrace{\varphi(P)}_{\in \mathbb{P}^m_K(L)})$$

By Thm A.2.1, there are only finitely many such $\varphi(P) \in \mathbb{P}^m_K(L)$ and hence finitely many such P (since φ is injective).

$\square$

Lemma A.3.2 If φ, φ' are defined by functions $f_0, \dots, f_n$ and $f_0', \dots, f_m'$ with the same divisor $D = \sum c_P P$, then

$$h(\varphi(P)) \underset{\varphi,\varphi'}{\approx} h(\varphi'(P)) \quad \forall P \in C(\bar{K}).$$

Pf W.l.o.g. (by transitivity), $f_0, \dots, f_n$ form a basis of $L(D)$.

$\Rightarrow f_0', \dots, f_m' \in L(D)$ are linear combinations of $f_0, \dots, f_n$.

W.l.o.g. (after invertible linear transformations on $\mathbb{P}^n, \mathbb{P}^m$ and omitting zeroes), we can assume that $m \leq n$, $f_0' = f_0, \dots, f_m' = f_m$.

If there were a point $P \in C(\bar{K})$ such $\varphi(P) = (x_0 : \dots : x_n) = \left[\frac{f_0}{t_P^{c_P}}(P) : \dots : \frac{f_n}{t_P^{c_P}}(P)\right]$ satisfies $x_0 = \dots = x_m = 0$, then

$v_P(f_0), \dots, v_P(f_m) > -c_P$.

$\Rightarrow f_0, \dots, f_m \in L(D-P)$, so $f_0, \dots, f_m$ don't actually have associated divisor D! ↯

$\Rightarrow$ We can apply Thm A.2.8. $\square$

Remark A.3.3 If φ, ψ are defined by functions $f_0, \dots, f_n$ and $g_0, \dots, g_m$ with divisors D, E, then we obtain a morphism η defined by functions $f_0 g_0, f_0 g_1, \dots, f_n g_m$ with associated divisor $D+E$ (since $\min_{i,j} v_p(f_i g_j) = \min_i v_p(f_i) + \min_j v_p(g_j)$)

where $\eta(P) = \underset{\substack{\uparrow \\ \text{Segre embedding}}}{\varphi(P) \otimes \psi(P)}$

and that $h(\eta(P)) \underset{\substack{\uparrow \\ \text{Thm A.2.3}}}{\approx} h(\varphi(P)) + h(\psi(P)) \ \forall P$.

Pf of Thm A.3.1

For any D, choose D_1, D_2 s.t. there $D = D_1 - D_2$ and there are morphisms φ_1, φ_2 corresponding to D_1, D_2. Let $h_D(P) := h(\varphi_1(P)) - h(\varphi_2(P))$.

i) If φ is a morphism assoc. to D, then

$h(\varphi(P)) \underset{\varphi}{\approx} h_D(P)$ because

$h(\underset{\substack{\wr \\ D = D_1 - D_2}}{\varphi(P)}) + h(\underset{\substack{\wr \\ D_2}}{\varphi_2(P)}) \approx h(\underset{\substack{\wr \\ D_1}}{\varphi_1(P)})$ by

Lemma A.3.2 and Remark A.3.3.

ii) Let $D = \underset{\varphi_1}{\underset{\geq}{D_1}} - \underset{\varphi_2}{\underset{\geq}{D_2}}$, $D' = \underset{\varphi_1'}{\underset{\geq}{D_1'}} - \underset{\varphi_2'}{\underset{\geq}{D_2'}}$,

$D + D' = \underset{\psi_1}{\underset{\geq}{E_1}} - \underset{\psi_2}{\underset{\geq}{E_2}}$ as above.

$$h_{D+D'}(P) = h(\psi_1(P)) - h(\psi_2(P))$$
$$h_D(P) = h(\varphi_1(P)) - h(\varphi_2(P))$$
$$h_{D'}(P) = h(\varphi_1'(P)) - h(\varphi_2'(P))$$

$\Rightarrow h_{D+D'}(P) \approx h_D(P) + h_{D'}(P)$ because

$$\underset{E_1}{\underset{\geq}{h(\psi_1(P))}} + \underset{D_2}{\underset{\geq}{h(\varphi_2(P))}} + \underset{D_2'}{\underset{\geq}{h(\varphi_2'(P))}} \approx \underset{E_2}{\underset{\geq}{h(\psi_2(P))}} + \underset{D_1}{\underset{\geq}{h(\varphi_1(P))}} + \underset{D_1'}{\underset{\geq}{h(\varphi_1'(P))}}$$

by Lemma A.3.2 and Remark A.3.3 (applied 4 times) because $E_1 + D_2 + D_2' = E_2 + D_1 + D_1'$.

$\square$

<u>Thm A.3.4</u> If $\psi : C \to C'$ is a nonconstant morphism between smooth proj. curves over K and $h_D : C(\overline{K}) \to \mathbb{R}$ for $D \in \mathrm{Div}(C)$ and $h'_{D'} : C(\overline{K}) \to \mathbb{R}$ for $D' \in \mathrm{Div}(C')$ are the corresponding height functions, then

$$h_{\psi^*(D')}(P) \underset{D',\psi}{\approx} h'_{D'}(\psi(P)) \qquad \forall P \in C(\overline{K}).$$

<u>Pf</u> We can assume (by ii) that there is a morphism $\varphi : C' \to \mathbb{P}^n$ defined by $f_0, \dots, f_n$ with divisor D'.

$\Rightarrow$ The morphism $\varphi \circ \psi : C \to \mathbb{P}^n$ is defined by $f_0 \circ \psi, \dots, f_n \circ \psi$ with divisor $D = \psi^*(D')$ (because $\mathrm{div}(f_i \circ \psi) = \psi^*(\mathrm{div}(f_i))$.)

$$\Rightarrow h_{\psi^*(D')}(P) \approx h(\varphi(\psi(P))) \approx h'_{D'}(\psi(P)).$$

$\square$

2.4. Heights of points on elliptic curves

Let E be an elliptic curve over K and let

$$\varphi : E \longrightarrow \mathbb{P}^2_K \quad , \quad \psi : E \longrightarrow \mathbb{P}^1_K$$

be the morphisms defined in section 2.1 (corr. to divisor $3[O]$, $2[O]$).

⇝ We get height function

$$h(\varphi(P)) \approx h_{3[O]}(P) \approx 3\, h_{[O]}(P)$$

$$h(\psi(P)) \approx h_{2[O]}(P) \approx 2\, h_{[O]}(P).$$

<u>Rmk</u> $\varphi(O) = [0:1:0]$

So the projection $[x:y:z] \longmapsto [x:z]$
$\varphi(P) \longmapsto \psi(P)$

is not well-def. at $\varphi(O) = [0:1:0]$ (the polynomials x, z have a common zero on the image $\varphi(E)$) although it <u>can</u> be extended to all of E! ($\psi(O) = [1:0]$)

And the height changes under this projection!

Thm 2.4.1 $\quad h_{[O]}(nP) \underset{\substack{n \\ (\text{and } E)}}{\approx} n^2 h_{[O]}(P) \quad \forall P \in E(\bar{k})$

Pf By Thm A.3.4 applied to $[n] : E \to E$,

$$h_{[n]^*([O])}(P) \approx h_{[O]}([n](P)) \quad \forall P \in E(\bar{k}).$$

But $[n]^*([O]) = \sum_{P \in E[n]} [P] = n^2[O] + \sum_{P \in E[n]} ([P]-[O])$

[n] unram.

lies in the same ~~divisor~~ class as $n^2[O]$

because $\sum_{P \in E[n]} P = O$ as $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

and $\sum_{v \in (\mathbb{Z}/n\mathbb{Z})^2} v = \sum_{x,y \in \mathbb{Z}/n\mathbb{Z}} \binom{x}{y} = 0.$

$$\Rightarrow h_{[n]^*([O])}(P) \approx h_{n^2[O]}(P) \approx n^2 h_{[O]}(P).$$

$\square$

<u>Cor 2.4.2</u> For every $P \in E(\overline{K})$, the limit

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{n^2} h_{[O]}(nP)$$ exists and it

satisfies

a) $\hat{h}(P) \approx h_{[O]}(P)$

b) $\hat{h}(mP) = m^2 \hat{h}(P)$.

<u>Def</u> $\hat{h}(P)$ is called <u>canonical</u> / <u>Neron–Tate</u> height of P. (Some authors use $2\hat{h}$ instead!)

<u>Pf</u> Let C_n be the error bound from Thm 2.4.1:

$$|h(nP) - n^2 h(P)| \leq C_n \quad \forall P \in E(\overline{K}). \quad (I)$$

First prove the claim when only considering powers of two: $n = 2^e$.

$$(I) \Rightarrow \left| \frac{1}{4^e} h(2^e P) - \frac{1}{4^{e-1}} h(2^{e-1} P) \right| \leq \frac{C_2}{4^e}$$

$$\Rightarrow \left| \frac{1}{4^e} h(2^e P) - h(P) \right| \leq \underbrace{\frac{C_2}{4^e} + \frac{C_2}{4^{e-1}} + \dots + \frac{C_2}{4}}_{\xrightarrow[e \to \infty]{} \frac{C_2}{3} < \infty}$$

$\Rightarrow$ The limit $\lim_{e \to \infty} \frac{1}{4^e} h(2^e P)$ exists and claim a) holds.

For b), note that

$$(I) \Rightarrow \left| \frac{1}{4^e} h(2^e m P) - \frac{m^2}{4^e} h(2^e P) \right| \le \frac{C_m}{4^e}$$

$$\begin{array}{ccc} \downarrow & \downarrow & \downarrow{\scriptstyle e \to \infty} \\ \hat{h}(mP) & m^2 \hat{h}(P) & 0 \end{array}.$$

For the limit's existence when considering all natural numbers n (not just powers of two): let D be the ~~error~~ bound from a).

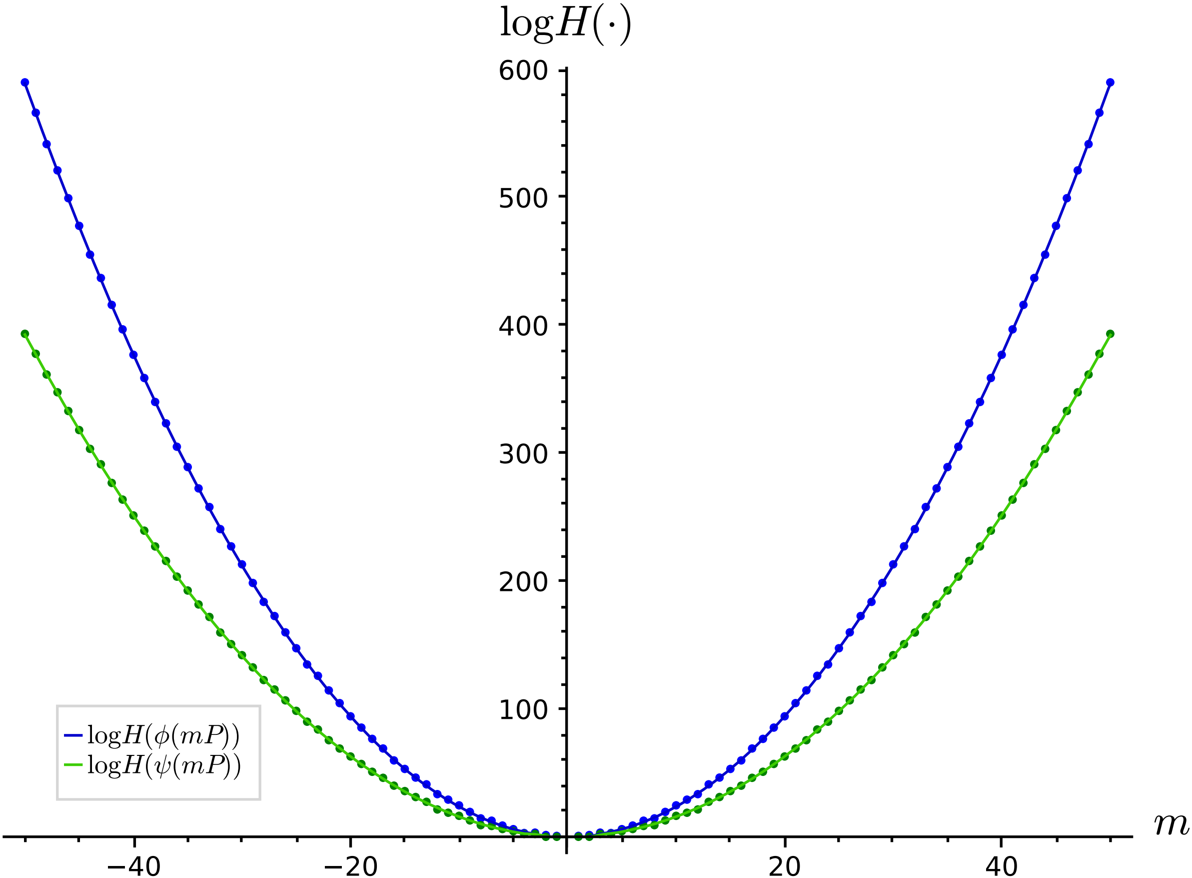
$$|\hat{h}(P) - h(P)| \le D \quad \forall P \in E(\bar{K}). \qquad (\#)$$

$\Rightarrow$ For any n, we get

$$|\underbrace{\hat{h}(nP)}_{n^2 \hat{h}(P)} - h(nP)| \le D$$

$$\Rightarrow \left| \hat{h}(P) - \frac{1}{n^2} h(nP) \right| \le \frac{D}{n^2} \xrightarrow{n \to \infty} 0.$$

$\square$



$\log H(\cdot)$
600
500
400
300
200
100
m
−40
−20
20
40
$\log H(\phi(mP))$
$\log H(\psi(mP))$

Thm 2.4.3 Let $P \in E(\overline{K})$, TFAE:

a) P is a torsion-point ($nP = O$ for some $n \geq 1$)

b) $h_{(0)}(nP)$ is bounded for $n \in \mathbb{N}$.

c) $\hat{h}(P) = 0$.

Pf a) $\Rightarrow$ b) clear

b) $\Rightarrow$ c) clear

b) $\Rightarrow$ a) Let $P \in E(L)$ for a fin. ext. $L|K$.

$\Rightarrow nP \in E(L) \; \forall n \geq 1$

But for any $T \geq 0$, there are only finitely many $Q \in E(L)$ with $h_{(0)}(Q) \leq T$.

$\Rightarrow nP = mP$ for some $n \neq m$.

c) $\Rightarrow$ b)

$$\begin{array}{c}\hat{h}(nP) = n^2 \hat{h}(P) = 0 \\ \wr\wr \\ h_{(0)}(nP)\end{array}$$

$\square$

B. Divisors on higher-dimensional varieties

Let V be an n-dimensional smooth variety defined ~~over~~ K.

<u>Def</u> A <u>(Weil) divisor</u> on V (def. over K) is a finite formal sum

$$\sum_{\substack{W \subseteq V \\ (n-1)\text{-dimensional} \\ \text{irred. subvar.} \\ \text{def. over } K}} n_W W \qquad \text{with } n_W \in \mathbb{Z}.$$

<u>Rmk</u> $\mathcal{O}_{V,W} := \left\{ \frac{a}{b} \in K(V) \,\middle|\, b|_W \neq 0 \right\}$ is a discrete valuation ring. Denote the normalized valuation $v_{V,W}$ and a uniformizer by $t_{V,W}$.

("$v_{V,W}(f)$ is the mult. of a zero of f along W, negative if there's a pole along f")

<u>Def</u> The divisor associated to $f \in K(V)^\times$ is

$$\operatorname{div}(f) = \sum_W v_{V,W}(f)\, W.$$

<u>Ex</u> $V = \mathbb{A}^2_k$, $f = \dfrac{x^2 - y}{y^3}$

$\rightsquigarrow \operatorname{div}(f) = \{(x,y) : x^2 - y = 0\} - 3 \cdot \{(x,y) : y = 0\}$.

<u>Def</u> For a morphism $\varphi : V \to V'$ between n-dimensional smooth varieties, the <u>image</u> of $D = \sum n_W W \in \operatorname{Div}(V)$ is

$$\varphi(D) = \sum_{\substack{W \subseteq V \\ \text{s.t.} \\ \overline{\varphi(W)} \subseteq V' \text{ is} \\ (n-1)\text{-dimensional}}} n_W \overline{\varphi(W)}$$

(It's always irreducible!)

If φ is dominant, the <u>pullback</u> of $D' = \sum n_{W'} W' \in \operatorname{Div}(V')$ is

$$\varphi^*(D') = \sum_{\substack{W \subseteq V \\ \dots \\ \text{s.t. } \overline{\varphi(W)} = W'}} n_{W'} e_{W|W'} W$$

with the <u>ramification index</u> $e_{W|W'} = v_{V,W}(t_{V',W'} \circ \varphi)$.

Def To a morphism $\varphi : V \longrightarrow \mathbb{P}^n_K$ whose image is not contained in any hyperplane $S \subseteq \mathbb{P}^n_K$, we associate the divisor class

$$D = \sum_{W \subseteq V} v_{V,W}\left(t_{\mathbb{P}^n_K, S} \circ \varphi\right) W \in \mathrm{Div}(V)$$

e.g. $\frac{a}{b}$ for lin. pol. $a, b \in K[x_0, \dots, x_n]$ where a vanishes on S and b vanishes on $S' \neq S$.

(Note that $\varphi(V) \subseteq S$ implies that $t_{\mathbb{P}^n_K, S} \circ \varphi$ is for any S a well-defined nonzero element of $K(V)$.)

Def A divisor $D \in \mathrm{Div}(V)$ is very ample if it is associated to some closed embedding $\varphi : V \longrightarrow \mathbb{P}^n_K$.

The question of very-ample-ness is more difficult than for curves, but at least:

Thm If V is a smooth proj. var., then any $D \in \mathrm{Div}(V)$ is the difference of two very ample divisors.

$\rightsquigarrow$ The definition of heights $h_D : V(\overline{K}) \to \mathbb{R}$ works "like for curves" (and satisfies the same properties).

2.4. Heights of points on elliptic curves (cont.)

Generalization of Thm 2.4.1:

Thm 2.4.4

$$h_{(O)}(P+Q) + h_{(O)}(P-Q) \approx 2\left(h_{(O)}(P) + h_{(O)}(Q)\right)$$
$$\forall P, Q \in E(\overline{K}).$$

Sketch of pf (cf. Silverman, Thm VIII.6.2)

Consider $V = E \times E$ and the morphism

$$\begin{aligned} S : E \times E &\longrightarrow \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8 \\ (P, Q) &\longmapsto (\phi(P), \phi(Q)) \\ &\qquad (R, S) \longmapsto R \otimes S \\ &\qquad ([x:y:z], [x':y':z']) \mapsto [xx' : xy' : \dots : zz'] \end{aligned}$$

Consider the hyperplane $H := \{[v_0 : \dots : v_8] \mid v_8 = 0\}$. Its preimage for $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$ is

$$\left(\{[x:y:z] \mid z=0\} \times \mathbb{P}^2\right) \cup \left(\mathbb{P}^2 \times \{[x':y':z'] \mid z'=0\}\right).$$

$\Rightarrow$ Its preimage for ζ is

$$(\{O\} \times E) \cup (E \times \{O\}).$$

$\Rightarrow$ The divisor associated to $\zeta : E \times E \to \mathbb{P}^8$ is

$$a\underbrace{\big((\{O\} \times E) + (E \times \{O\})\big)}_{=:D} \text{ for some } a \geq 1$$

(actually $a = 3$).

$$h_{aD}(P,Q) \approx h(\zeta(P,Q)) \approx h(\phi(P)) + h(\phi(Q))$$

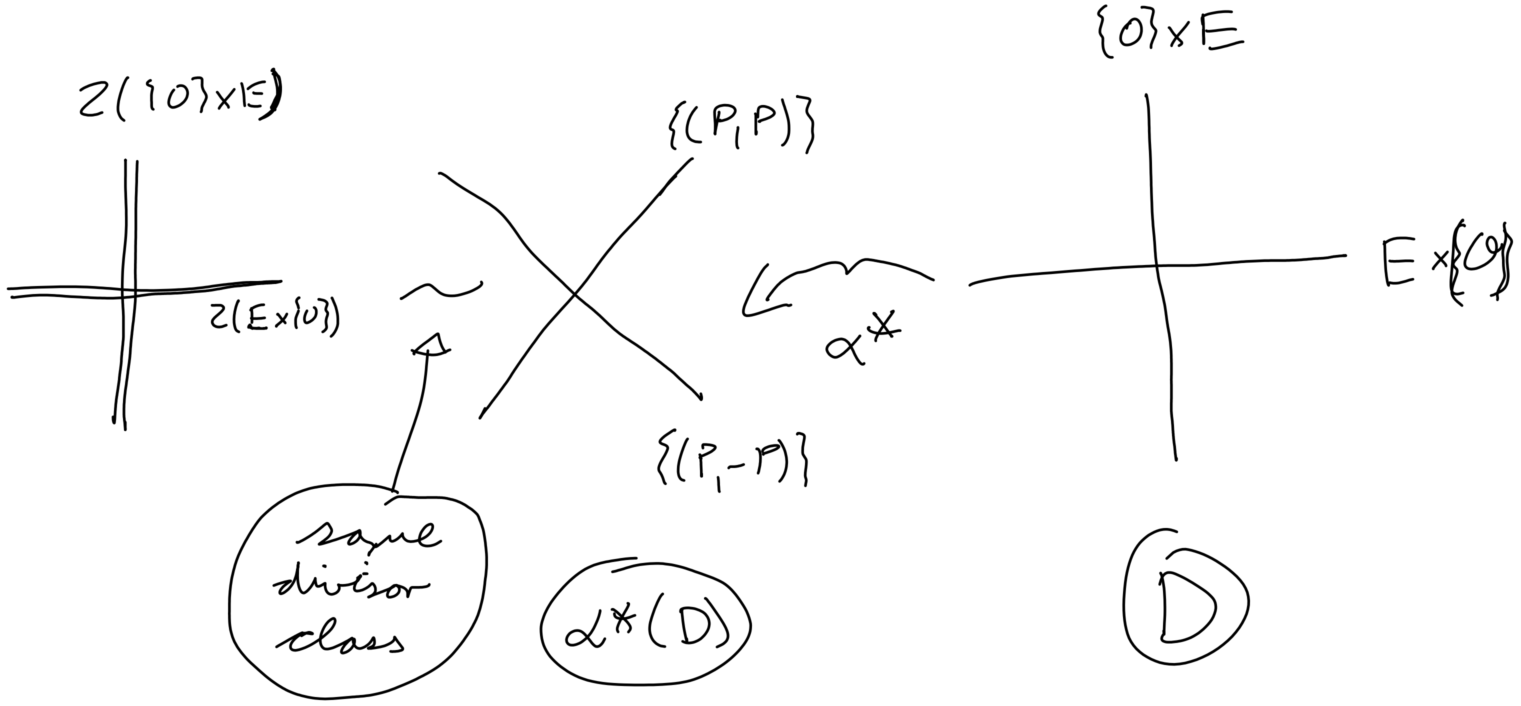
$$\approx 3h_{(O)}(P) + 3h_{(O)}(Q)$$

$$h_{aD}(P,Q) \approx a h_D(P,Q)$$

$$\Rightarrow h_D(P,Q) \approx \frac{3}{a}\left(h_{(O)}(P) + h_{(O)}(Q)\right).$$

Consider the morphism

$$\begin{aligned} \alpha : E \times E &\longrightarrow E \times E \\ (P,Q) &\longmapsto (P+Q, P-Q). \end{aligned}$$



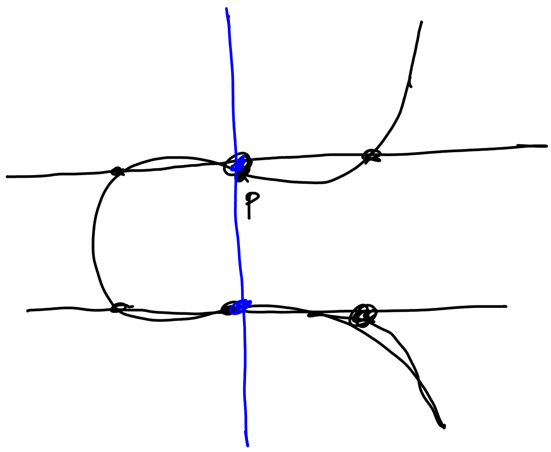
$$\alpha^*(D) = b\big(\{(P,P) \mid P\in E\} + \{(P,-P) \mid P\in E\}\big)$$

for some $b \geq 1$
(actually $b=1$).

The rational function f on $E\times E$ given by

$$f(P,Q) = \cancel{y_P^2 - y_Q^2} \quad x_P - x_Q$$

for $\phi(P) = [x_P : y_P : 1]$, $\phi(Q) = [x_Q : y_Q : 1]$



has divisor

$$c\left(\{(P,P) \mid P \in E\} + \{(P,-P) \mid P \in E\}\right)$$

$$- d\left(\underset{\substack{\uparrow \\ \text{poles of } x_P}}{\{O\} \times E} + \underset{\substack{\uparrow \\ \text{poles of } x_Q}}{E \times \{O\}}\right)$$

for some $c, d \geq 1$

(actually, $c = 1$, $d = 2$.)

$\Longrightarrow c \cdot \alpha^*(D)$ lies in the same divisor class as $bd(\{O\} \times E + E \times \{O\}) = bd\,D$.

$$\Longrightarrow \underset{\substack{\shortparallel \\ c \cdot h_D(P+Q,\, P-Q) \\ \approx \\ \frac{3c}{a}\left(h(P+Q) + h(P-Q)\right)}}{h_{cD}(\alpha(P,Q))} \approx h_{c\alpha^*(D)}(P,Q) \approx \underset{\substack{\approx \\ \frac{3}{a} bd\left(h(P) + h(Q)\right).}}{bd\,h_D(P,Q)}$$

$\forall P, Q \in E(\overline{K})$

$$\Longrightarrow h(P+Q) + h(P-Q) \approx \frac{bd}{c}\left(h(P) + h(Q)\right).$$

For $P = Q$, we get

$$\underset{\substack{\approx \\ 4h(P)}}{h(2P)} + \underset{\substack{\approx \\ 0}}{h(O)} \approx 2\frac{bd}{c}\, h(P) \quad \forall P \in E(\overline{K}).$$

If $h(P)$ is unbounded (for $P \in E(\overline{K})$) (it is!), this implies $\frac{bd}{c} = 2$,

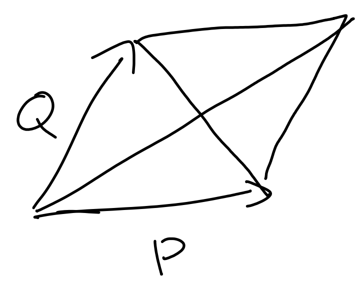
so $h(P+Q) + h(P-Q) \approx 2(h(P)+h(Q))$.

If $h(P)$ were bounded, then trivially
$$h(P+Q)+h(P-Q) \approx 0 \approx 2(h(P)+h(Q)).$$ $\square$

Cor 2.4.5 (Parallelogram law)

$$\hat{h}(P+Q)+\hat{h}(P-Q)=2(\hat{h}(P)+\hat{h}(Q))$$

Pf Apply the Thm to nP, nQ. Divide by n^2. Take $n \to \infty$. $\square$



Cor 2.4.6 $\hat{h}: E(\overline{K}) \to \mathbb{R}$ is a quadratic form:

$$\langle \cdot , \cdot \rangle : E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}$$
$$(P, Q) \mapsto \tfrac{1}{2}(\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q))$$

is bilinear.

Pf HW. "$\square$"

Final paper

7 - 10 pages

Due May 7 at 1:59pm (ET)

Draft: ~ May 2 (optional, but highly recommended!)

Some ideas for topics:

- Elliptic curves over $\mathbb{C}$

  $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for a rank 2 lattice Λ in $\mathbb{C}$

  (cf. Silverman-Tate, II.2 or Silverman, V)

- Complex multiplication:

  Class field theory over imaginary quadratic number fields has to do with elliptic curves over $\mathbb{C}$.

- Abelian varieties over $\mathbb{C}$

  $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ for a rank $2g$ lattice Λ in $\mathbb{C}^g$

  such that is a positive definite hermitian form $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^g$ with $\langle a, b \rangle \in \mathbb{Z}$ $\forall a, b \in \Lambda$.

- Nagell-Lutz theorem:

  "Torsion points have integral x and y-coordinates in the affine chart with $z = 1$."

- Bombieri-Lang Conjecture (higher-dimensional generalisation of Faltings's theorem),

  Erdős-Ulam problem

  (Is there a dense subset S of $\mathbb{R}^2$ for the Euclidean topology s.t. $d(x,y) \in \mathbb{Q}$ $\forall x, y \in S$?)

- Algorithms on ell. curves (Chapter II in Cremona, Algorithms for ell. curves)
- Elliptic curve factorization algorithm

2.5. The Mordell-Weil Theorem

M-W Thm Let E be an ell. curve over a number field K. Then, the group $E(K)$ is finitely generated.

Cor $E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$ for some $r \geq 0$

called the *rank* of E over K.

$E(K)_{tors}$ is finite!

Rmk Isogenous ell. curves have the same rank.

Pf Let $\phi: E_1 \to E_2$ be a nonzero isogeny (def. over K).

$$\begin{array}{ccc} \phi: E_1(K) & \longrightarrow & E_2(K) \\ \cong & & \cong \\ E_1(K)_{tors} \times \mathbb{Z}^{r_1} & & E_2(K)_{tors} \times \mathbb{Z}^{r_2} \end{array}$$

has finite kernel (of size $\leq \deg(\phi)$).

$\Rightarrow r_1 \leq r_2$

The dual isogeny $\hat{\phi}: E_2 \to E_1$ shows that $r_2 \leq r_1$. $\square$

Weak M-W Thm

Let K be a number field and $\phi : E_1 \to E_2$ be a nonzero isogeny between ell. curves over K with $\ker(\phi) \subseteq E_1(K)$. Then, the group $E_2(K) / \phi(E_1(K))$ is finite.

Pf that weak M-W implies M-W (Descent argument)

Pick $m \geq 2$ and consider the mult. by m isogeny $[m] : E \to E$. ($\rightsquigarrow$ m-descent)

We have $\ker([m]) = E[m] \subseteq E(L)$ for some finite field ext. $L|K$. Since any subgroup ($E(K)$) of any fin. gen. grp. ($E(L)$), we can assume that $E[m] \subseteq E(K)$.

By weak M-W, the group

$$E(K) / mE(K) \text{ is finite.}$$

Let $Q_1, \dots, Q_a \in E(K)$ be coset representatives. Recall that for any $T \in \mathbb{R}$, the set

$$S_T := \{ P \in E(K) \mid \underset{\approx h(P)}{\hat{h}(P)} \leq T \} \text{ is finite.}$$

Let G_T be the subgroup of $E(K)$ generated by $Q_1, \dots, Q_a$ and the elements of S_T.

We want to show that $G_T = E(K)$ for sufficiently large T.

Assume $P \in E(K) \setminus G_T$ with minimal $\hat{h}(P)$.

Let Q_i lie in the same coset as P, so we can write

$$P = Q_i + mP' \text{ for some } P' \in E(K).$$

Note that $P' \in E(K) \setminus G_T$, $P \pm Q_i \in E(K) \setminus G_T$

$$\hat{h}(P-Q_i) + \underbrace{\hat{h}(P+Q_i)}_{\substack{\geq \hat{h}(P) \\ \text{by assumption}}} = 2(\hat{h}(P) + \hat{h}(Q_i))$$

$$\Rightarrow \hat{h}(P-Q_i) \leq \hat{h}(P) + 2\hat{h}(Q_i)$$

$$\begin{array}{c} \| \\ \hat{h}(mP') = m^2 \hat{h}(P') \underset{\text{by assumption}}{\geq} m^2 \hat{h}(P) \end{array}$$

$$\Rightarrow \hat{h}(P) \leq \frac{2}{m^2-1} \cdot \hat{h}(Q_i).$$

$\Rightarrow$ If we choose

$$T \geq \underbrace{\frac{2}{m^2-1} \cdot \max(\hat{h}(Q_1), \dots, \hat{h}(Q_a))}_{\text{indep. of } P!},$$

then $P \in S_T \subseteq G_T$. $\lightning$

$\square$

Rmk $E(K) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$

because $P \otimes 1 = \underbrace{nP}_{0} \otimes \frac{1}{n} = 0$ if $nP = 0$.

Thm 2.5.1 The quadratic form $\hat{h}$ on $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ defined by $\hat{h}(\sum P_i \otimes a_i) = \sum_{i,j} \langle P_i, P_j \rangle a_i a_j$

(so $\langle \sum P_i \otimes a_i, \sum Q_j \otimes b_j \rangle = \sum_{i,j} \langle P_i, Q_j \rangle a_i b_j$)

is positive definite.

Pf of Thm

Assume $\hat{h}(x) \le 0$ for some

$$0 \neq x = \sum_{i=1}^{m} P_i \otimes a_i \in E(K) \otimes \mathbb{R}.$$

Let $\Lambda \subseteq E(K) \otimes \mathbb{R} \cong \mathbb{R}^r$ be the $\mathbb{Z}$-lattice spanned by the elements $Q \otimes 1$ with $Q \in E(K)$.

Choose a basis $e_1, \dots, e_r$ of $\mathbb{R}^r$ s.t.

$$\hat{h}(\Sigma c_i e_i) = \sum_{i=1}^{a} c_i^2 - \sum_{i=a+1}^{a+b} c_i^2$$

for all $c_1, \dots, c_r \in \mathbb{R}$.

By assumption, $a < r$.

The convex centrally symmetric set

$$S_\varepsilon := \left\{ \sum c_i e_i \;\middle|\; \sum_{i=1}^{a} c_i^2 < \varepsilon \right\}$$

has volume ∞ for all $\varepsilon > 0$.

By Minkowski's theorem, $\Lambda \cap S_\varepsilon$ contains a nonzero element

$$x = Q \otimes 1 \quad \text{with } Q \in E(K).$$

$$\Rightarrow \hat{h}(Q) < \varepsilon.$$

$$x \neq 0 \Rightarrow Q \notin E(K)_{\mathrm{tors}}$$

$\Rightarrow E(K)$ contains nontorsion points Q with arbitrarily small $\hat{h}(Q) > 0$.

But there are only fin. many $Q \in E(K)$ of bounded $\hat{h}(Q)$! $\lightning$ $\square$

2.6. Some algorithms

Let E be an ell. curve over a number field K.

Rmk The error bounds for approx. eq ($\approx$) in section 2.4 can be made explicit (using the coefficients of the elliptic curve).

Therefore, we can approximate

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}$$ to any given precision.

Thm 2.6.1 It's decidable whether a given point $P(K)$ is torsion.

Pf In parallel:

Compute $P, 2P, 3P, \ldots$

If P is torsion, you eventually find $nP = O$.

Compute more and more digits of $\hat{h}(P)$.

If P is non-torsion, then $\hat{h}(P) \neq 0$.

$\square$

More generally:

Thm 2.6.2 It's decidable whether $P_1, \ldots, P_n \in E(K)$ are linearly independent in $E(K) \otimes \mathbb{R} \cong \mathbb{R}^r$.

Pf If they are linearly dependent, there are $0 \neq (a_1, \ldots, a_n) \in \mathbb{Z}^n$ s.t. $a_1 P_1 + \cdots + a_n P_n = O$.

If they are lin. independent, then $(\langle P_i, P_j \rangle)_{i,j}$ has nonzero determinant because $\langle \cdot, \cdot \rangle$ is positive definite.

Compute more and more digits of the determinant until finding a nonzero digit. $\square$

Thm 2.6.3 Given points $Q_1, \dots, Q_d$ representing the cosets in $E(K)/mE(K)$, there's an algorithm to determine $E(K)_{tors}$ and the rank r of E, and points $P_1, \dots, P_r$ representing a $\mathbb{Z}$-basis of $E(K)/E(K)_{tors} \cong \mathbb{Z}^r$.

Pf By pf of "weak M-W $\Rightarrow$ M-W", you can find generators $R_1, \dots, R_b$ of $E(K)$.

The rank r of E over K is the size of a max. lin. indep. subset of $R_1 \otimes 1, \dots, R_b \otimes 1$ in $E(K) \otimes \mathbb{R}$.

Consider the map

$$f : \mathbb{Z}^b \twoheadrightarrow E(K) \otimes \mathbb{R} \cong \mathbb{R}^r$$
$$(a_1, \dots, a_b) \mapsto (a_1 R_1 + \dots + a_b R_b) \otimes 1.$$

We can find a matrix representing this map. $\Rightarrow$ We can find elements $v_1, \dots, v_c \in \ker(f)$ spanning $\ker(f) \otimes_{\mathbb{Z}} \mathbb{R}$.

Then, find elements $w_1, \dots, w_c$ spanning the free $\mathbb{Z}$-module $\ker(f)$.

We obtain points $P_1, \dots, P_c \in E(K)$ (P_i = the lin. comb. of $R_1, \dots, R_b$ corr. to $w_i \in \mathbb{Z}^b$) generating $E(K)_{tors}$. $\square$

Rmk We only have an algorithm that conjecturally determines $Q_1, \dots, Q_d$.
(It never produces wrong results, but we don't know if it always terminates!)

Rmk The above algorithms are far from optimal!

2.7. Hermite's finiteness theorem

Thm 2.7.1 For any $n \geq 1$, $T \geq 1$, there are only finitely many number fields K of degree n and discriminant satisfying
$|D_K| \leq T$.

Pf Let L be the Galois closure of $K|\mathbb{Q}$.
The embeddings $K \hookrightarrow \mathbb{C}$ correspond to elements of $Gal(L|\mathbb{Q})/Gal(L|K)$
(compose with a fixed embedding $L \hookrightarrow \mathbb{C}$).

For any $\mathbb{Q} \subseteq K' \subseteq K$

$$\begin{array}{c} L \\ | \\ K \\ | \\ K' \\ | \\ \mathbb{Q} \end{array}
\qquad
\begin{tikzcd}
\{\text{emb. } K \hookrightarrow \mathbb{C}\} \arrow[r, leftrightarrow] \arrow[d, "\text{restriction}"] & \mathrm{Gal}(L|\mathbb{Q})/\mathrm{Gal}(L|K) \arrow[d, "\text{quotient}", "{[K:K']\text{-to-1 map}}"'] \\
\{\text{emb. } K' \hookrightarrow \mathbb{C}\} \arrow[r, leftrightarrow] & \mathrm{Gal}(L|\mathbb{Q})/\mathrm{Gal}(L|K')
\end{tikzcd}$$

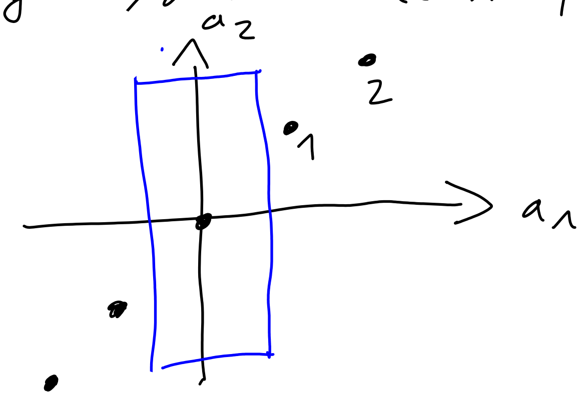
$\Rightarrow$ If $K' \subsetneq K$, then every embedding $K' \hookrightarrow \mathbb{C}$ has multiple extensions to K. (I)

For simplicity, consider only totally real number fields K, with n real embeddings $\sigma_1, \dots, \sigma_n$.

By Minkowski's theorem, there is a number $C>0$ depending on n and T, but not on K such that the convex centrally symmetric set

$$\{(a_1, \dots, a_n) \in \mathbb{R}^n \mid |a_1|, \dots, |a_{n-1}| < 1, \ |a_n| < C\}$$

contain a nonzero element of the integer lattice $\{(\sigma_1(a), \dots, \sigma_n(a)) \mid a \in \mathcal{O}_K\}$.



Since $1 \leq |\mathrm{Nm}(a)| = \underbrace{|\sigma_1(a)|}_{<1} \cdots \underbrace{|\sigma_{n-1}(a)|}_{<1} \cdot |\sigma_n(a)|$,

we have $|\sigma_n(a)| > 1$.

Hence, $\sigma_n(a) \neq \sigma_i(a)$ for $i = 1, \dots, n-1$, so the restriction of σ_n to $\mathbb{Q}(a)$ is different from the restrictions of $\sigma_1, \dots, \sigma_{n-1}$ to $\mathbb{Q}(a)$.

$\underset{(I)}{\Longrightarrow}$ $K = \mathbb{Q}(a)$.

The coeff. of the min. pol.

$$f(X) = (X - \underbrace{\sigma_1(a)}_{|\cdot|<1}) \cdots (X - \underbrace{\sigma_{n-1}(a)}_{|\cdot|<1})(X - \underbrace{\sigma_n(a)}_{|\cdot|<C}) \in \mathbb{Z}[X]$$

are bounded.

$\Rightarrow$ There are only fin. many possible minimal pol. $f(X)$.

$\Rightarrow$ Only fin. many possible $a \in \overline{\mathbb{Q}}$.

$\Rightarrow$ Only fin. many possible K. $\square$

Lemma 2.7.2 Let k be a nonarchimedean local field of characteristic 0, and $n \geq 1$. Then, there are only finitely many extensions $L|k$ of degree n.

Pf Since the Galois closure of $L|k$ has degree $\leq n!$, it suffices to consider only Galois extensions.

Since the Galois group of a Gal. ext. of local fields is solvable (follows from the theory of higher ramification groups), by induction, it suffices to consider only cyclic extensions.

By class field theory, they correspond to open subgroups U of $k^\times$ with $k^\times/U \cong \mathbb{Z}/n\mathbb{Z}$.

Note that ~~then~~ $U \supseteq k^{\times n}$. But $k^\times \cong \mathcal{O}_k^\times \times \mathbb{Z}$,

$$u \cdot \pi_k^t \leftarrow\!\shortmid (u, t)$$

so $k^{\times n} = \mathcal{O}_k^{\times n} \times n\mathbb{Z}$.

By Hensel's lemma, every $a \in \mathcal{O}_k^\times$ with $a \equiv 1 \mod \mathfrak{P}_k^{2v_{\mathfrak{P}}(n)+1}$ has an

n-th root in $\mathcal{O}_K^\times$. (Lift the root 1 of $X^n - a$ modulo $\mathfrak{q}_K^{2v_{\mathfrak{q}}(n)+1}$.)

$\Rightarrow \mathcal{O}_K^\times / \mathcal{O}_K^{\times n} \hookrightarrow \left(\mathcal{O}_K / \mathfrak{q}_K^{2v_{\mathfrak{q}}(n)+1}\right)^\times$ is finite.

$\Rightarrow K^\times / K^{\times n} = \mathcal{O}_K^\times / \mathcal{O}_K^{\times n} \times \mathbb{Z}/n\mathbb{Z}$ is finite

$\Rightarrow$ There are only finitely many U.

$\square$

Serre: Formules de masse ...

Thm 2.7.3 Let K be a number field, let S be a finite set of primes of K, and let $n \geq 1$. Then, there are only finitely many extensions $L|K$ of degree n which are unramified at every prime $\mathfrak{q} \notin S$.

Ex $\mathbb{Q}$ has no unramified extensions (other than $\mathbb{Q}$).

Pf To apply Thm 2.7.1, we need an upper bound on $|D_L|$. By the relative discriminant formula,

$$|D_L| = \underbrace{|Nm_{K|\mathbb{Q}}(disc(L|K))|}_{= \prod_{\mathfrak{q} \in S} Nm(\mathfrak{q})^{v_{\mathfrak{q}}(disc(L|K))}} \cdot |D_K|^{[L:K]}$$

If $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the primes of L above $\mathfrak{q}$, then

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathfrak{q}} \cong \mathcal{O}_{\mathfrak{P}_1} \times \cdots \times \mathcal{O}_{\mathfrak{P}_r}.$$

$$\begin{array}{cccc}
L & \mathfrak{P}_1 \ldots \mathfrak{P}_r & L_{\mathfrak{P}_1} \cdots L_{\mathfrak{P}_r} & \mathcal{O}_{\mathfrak{P}_1} \cdots \mathcal{O}_{\mathfrak{P}_r} \\
| & \backslash \; / & \backslash \; / & \backslash \; / \\
K & \mathfrak{q} & K_{\mathfrak{q}} & \mathcal{O}_{\mathfrak{q}}
\end{array}$$

$$\Rightarrow v_{\mathfrak{q}}(\mathrm{disc}(L|K)) = \underbrace{v_{\mathfrak{q}}(\mathrm{disc}(L_{\mathfrak{P}_1}|K_{\mathfrak{q}}))}_{\text{bounded}} + \ldots + \underbrace{v_{\mathfrak{q}}(\mathrm{disc}(L_{\mathfrak{P}_r}|K_{\mathfrak{q}}))}_{\text{bounded}}$$

(only finitely many possible $L_{\mathfrak{P}_i}$)

$\square$

2.8. The Chevalley-Weil theorem

Thm 2.8.1 Let $V \subseteq \mathbb{A}^a_K$, $W \subseteq \mathbb{A}^b_K$ be smooth varieties over a number field K and let $\varphi: V \longrightarrow W$ be a dominant finite unramified morphism.

Then, there is a finite set S of primes of K such that any $P \in V(\overline{K})$ with $Q := \varphi(P) \in W(\mathcal{O}_K)$ lies in $V(K')$ for a (finite) field ext. K' of K which is unramified at all primes $\mathfrak{q} \notin S$.

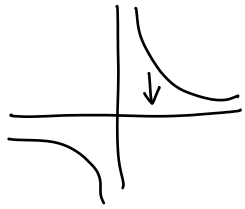
<u>Non-Ex</u> The morphism

$$\varphi : \mathbb{A}^1_{\mathbb{Q}} \longrightarrow \mathbb{A}^1_{\mathbb{Q}} \quad \text{is dominant and}$$
$$x \longmapsto x^2$$

finite, but ramified at 0.

The field ext. $\mathbb{Q}(\sqrt{y})|\mathbb{Q}$ for $y \in \mathbb{Z}$ can be ramified anywhere.

<u>Ex</u> The morphism



$$\varphi : \{(x,x') \in \mathbb{A}^2_K \mid xx' = 1\} \longrightarrow \{(y,y') \in \mathbb{A}^2_K \mid yy' = 1\}$$
$$(x,x') \longmapsto (x^2, x'^2)$$

is unramified.

The field ext. $K(\sqrt{y})|K$ for $(y,y') \in \mathcal{O}_K^2$ with $yy' = 1$ (so $y \in \mathcal{O}_K^\times$)

is unramified at all primes not dividing 2.

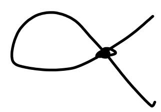
Some AG

Def An affine variety $V \subseteq \mathbb{A}^n_k$ is <u>normal</u> if it is irreducible and $\Gamma(V)$ is integrally closed in its field of fractions $k(V)$.

A projective variety $V \subseteq \mathbb{P}^n_k$ is <u>normal</u> if it is irreducible and its nonempty affine charts $V \cap H_i$ are normal.

Ex $\mathbb{A}^n$, $\mathbb{P}^n$, any smooth variety

Non-ex $V = \{(x,y) \mid x^2 = y^2(y+1)\} \subseteq \mathbb{A}^2_k$



$\frac{x}{y} \in k(V)$ is integral over $\Gamma(V)$, but not contained in $\Gamma(V)$.

$$\left(\frac{x}{y}\right)^2 = y+1$$

Def A morphism $\varphi : V \to W$ between affine varieties V, W is <u>finite</u> if $\Gamma(V)$ is an integral ring ext. of $\varphi^*(\Gamma(W))$.

A morphism $\varphi : V \to W$ between projective varieties V, W is <u>finite</u> if its restrictions to affine charts are finite.

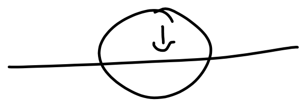
$$(\varphi^{-1}(W \cap H_j) \cap H_i \longrightarrow W \cap H_j).$$

Ex - Any inclusion

- $\varphi : \{(x,y) \in \mathbb{A}^2_K \mid x^2+y^2=1\} \longrightarrow \mathbb{A}^1_K$

$$(x,y) \longmapsto x$$

because $\Gamma(V) = K[X][Y]/(Y^2+(X^2-1))$ is an integral ring ext of $\Gamma(W) = K[X]$.



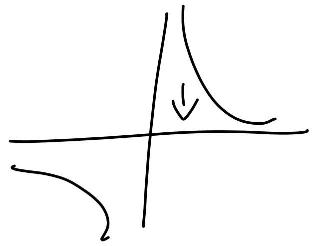
Non-ex - $\mathbb{A}^2_K \longrightarrow \mathbb{A}^1_K$

$$(x,y) \longmapsto x$$

- $\varphi : \{(x,y) \in \mathbb{A}^2_K \mid xy=1\} \longrightarrow \mathbb{A}^1_K$

$$(x,y) \longmapsto x$$

because $\Gamma(V) = K[X][Y]/(XY-1)$ is not an integral ring ext of $\Gamma(W) = K[X]$.



Rmk All fibers $\varphi^{-1}(P)$ $(P \in W(\overline{K}))$ of finite morphisms are finite.

Rmk Any dominant finite morphism is surjective (over $\overline{K}$).

Prop Compositions of finite morphisms are finite.

Cor Restrictions of finite morphisms are finite.

Prop If $\varphi: V \to W$ and $W \subseteq W'$, then $\varphi: V \to W$ is finite if and only if $\varphi: V \to W'$.

Cor Any finite morphism is closed: the image of any (Zariski) closed set is closed.

Prop Finite morphisms preserve dimension: $\dim(\varphi(X)) = \dim(X)$.

Prop Let $\varphi: V \to W$ be a morphism between smooth projective varieties. Then, φ is finite if and only if $\varphi^{-1}(P) \subseteq V(\overline{K})$ is finite for all $P \in W(\overline{K})$.

Ex Any nonconstant morphism between smooth projective curves is finite.

Def Let $\varphi : V \to W$ be dominant finite morphism between affine normal varieties, its *degree* $n = \deg(\varphi) = [K(V) : K(W)]$.

Rmk $\Gamma(V)$ is the integral closure of $\varphi^*(\Gamma(W))$ in $K(V)$.

We consider $\Gamma(W)$ a subring of $\Gamma(V)$ with the inclusion map $\varphi^* : \Gamma(W) \to \Gamma(V)$.

Def The *discriminant* $\operatorname{disc}(\Gamma(V) | \Gamma(W))$ is the ideal of $\Gamma(W)$ generated by the determinants $\det((\operatorname{Tr}_{K(V)|K(W)}(f_i f_j))_{i,j}) \in \Gamma(W)$ with $f_1, \dots, f_n \in \Gamma(V)$.

Rmk Like in number theory, the discriminant determines ramification:
For $S \subseteq V$, $T \subseteq W$ irred. of codim. 1, consider the ram. index

$$e_{S|T} = v_{V,S}(t_{W,T} \circ \varphi).$$

φ is unramified at T (meaning $e_{S|T} = 1 \ \forall S$) if and only if $\operatorname{disc}(\Gamma(V) | \Gamma(W)) \in \Gamma(W)$ doesn't vanish on T (meaning $v_{W,T}(\operatorname{disc}) = 0$).

Rmk φ is unramified if and only if every $Q \in W(\bar{k})$ has exactly n preimages $P \in V(\bar{k})$.

Rmk Assume φ is unramified.

Let $Q \in W(k)$ and let $m_Q \subset \Gamma(W)$ be the corr. maximal ideal.

Note that $P \in V(\bar{k})$ lies in $\varphi^{-1}(Q)$ if and only if

$$\underbrace{f(\varphi(P))}_{\varphi^*(f)(P)} = 0 \quad \forall f \in m_Q.$$

$\Rightarrow$ $\varphi^{-1}(Q) \subseteq V(\bar{k})$ is the vanishing locus of the ideal $(\varphi^*(m_Q))$ of $\Gamma(V)$.

Then,

$$\Gamma(V)/(\varphi^*(m_Q)) = \Gamma(\varphi^{-1}(Q)) = \prod_{\substack{R \subseteq \varphi^{-1}(Q) \\ \text{0-dim. subvar.}}} \Gamma(R)$$

$$\Gamma(\{(\pm i, 1)\}) = \Gamma(\{\pm i\}) = \mathbb{Q}[x]/(x^2+1) = \mathbb{Q}(i)$$

$$= \prod_{\substack{\text{Gal}(\bar{k}|k)\text{-orbit} \\ \text{of points } P \in \varphi^{-1}(Q)}} (\text{field of def. } \overset{\leftarrow}{k'} \text{ of } P)$$

We will prove a slightly stronger version of Thm 2.8.1.:

Thm 2.8.2 Let V, W be affine normal varieties over a number field K and let $\varphi : V^{\subseteq \mathbb{A}^n} \to W^{\subseteq \mathbb{A}^m}$ be a dominant finite unramified morphism. Then, there is a finite set S of primes of K such that the field of definition K' of any point $P \in V(\overline{K})$ with $Q := \varphi(P) \in W(K)$ is unramified at all primes $\mathfrak{p} \notin S$ for which $v_{\mathfrak{p}}(y_i) \geq 0$ for all coordinates y_i of Q.

Pf (see Lang, Fundamentals of Diophantine Geometry, Chapter 2.8)

$$\begin{array}{ccccc} K(V) & \supset & \Gamma(V) & \supset & B \\ {\scriptstyle \varphi^*}\uparrow & & \uparrow & & \uparrow \\ K(W) & \supset & \Gamma(W) & \supset & A \end{array}$$

Consider the discriminant ideal

$$\mathrm{disc}(\Gamma(V) \mid \Gamma(W)) \subseteq \Gamma(W).$$

Since φ is unramified, its vanishing locus is $\emptyset$.

By Hilbert's Nullstellensatz, this means that disc$(\Gamma(V)|\Gamma(W)) = \Gamma(W)$.

Consider polynomials $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ defining the morphism φ. Let S_1 be the set of primes of K such that some coeff. of some f_i has negative $\mathfrak{p}$-adic valuation.

Let $\mathcal{O}_K \subseteq \mathcal{O}_{S_1} < K$ be the ring of S_1-integers (the ring of $g \in K$ with $v_{\mathfrak{p}}(g) \geq 0 \; \forall \mathfrak{p} \notin S_1$).

$\Rightarrow f_1, \dots, f_m \in \mathcal{O}_{S_1}[X_1, \dots, X_n]$.

We obtain rings

$$A = \mathcal{O}_{S_1}[Y_1, \dots, Y_m] / (I(W) \cap \mathcal{O}_{S_1}[Y_1, \dots, Y_m])$$

$$B = \mathcal{O}_{S_1}[X_1, \dots, X_n] / (I(V) \cap \mathcal{O}_{S_1}[X_1, \dots, X_n]).$$

$$A \otimes_{\mathcal{O}_{S_1}} K = \Gamma(W) \quad , \quad B \otimes K = \Gamma(V)$$

A is integrally closed in $\Gamma(W)$

B is " — $\Gamma(V)$.

We have $\left(\mathrm{disc}(B|A)\right)_{\Gamma(W)} = \mathrm{disc}(\Gamma(V)|\Gamma(W)) = \Gamma(W)$.

$\Rightarrow$ $\mathrm{disc}(B|A) \subseteq A$ contains a nonzero constant $0 \neq c \in \mathcal{O}_{S_1}$.

Let $S := S_1 \cup \{ \mathfrak{q} \mid v_{\mathfrak{q}}(c) > 0 \}$.

Now, take $Q \in W(K)$ and $m_Q \subset \Gamma(W)$ the corr. max. ideal and $m_Q' = m_Q \cap A$.

$$A_Q := A/m_Q' \cong \mathcal{O}_{S_1}(Y_1, \dots, Y_m)/(I(W), Y_1 - q_1, \dots, Y_m - q_m)$$
$$\cong \mathcal{O}_{S_1} \text{ if } q_1, \dots, q_m \in \mathcal{O}_{S_1}.$$

$\Gamma(W)/m_Q \cong K$

$$\Gamma(V)/(\varphi^*(m_Q)) = \prod_{\substack{\text{Gal-orbit} \\ \text{of } P \in \varphi^{-1}(Q)}} (\text{field of def. } K' \text{ of } P)$$

$$B_Q := B/(\varphi^*(m_Q')) = \prod_{\dots} (\text{ring of } S_1\text{-integers}$$

of field of def. K' of P)
$\quad\quad ||$
int. cl. of $\mathcal{O}_{S_1}$ in K'

The discriminant ideal $\mathrm{disc}(B_{\mathfrak{q}}|A_{\mathfrak{q}})$ is the image of $\mathrm{disc}(B|A)$ under the map

$$A \longrightarrow A/\mathfrak{m}_{\mathfrak{q}}^{e}$$
$$x \longmapsto x \bmod \mathfrak{m}_{\mathfrak{q}}^{e}$$

$\Rightarrow$ $0 \neq c \in \mathcal{O}_{S_1}$ lies in $\mathrm{disc}(B_{\mathfrak{q}}|A_{\mathfrak{q}})$

$$\mathrm{disc}(B_{\mathfrak{q}}|A_{\mathfrak{q}}) = \prod \mathrm{disc}(\text{int. cl. of } \mathcal{O}_{S_1} \text{ in } K' \mid \mathcal{O}_{S_1})$$

$\Rightarrow$ None of the discr. on the RHS are divisible by any $\mathfrak{q} \notin S$.

$\mathrm{disc}(\mathcal{O}_{K'}|\mathcal{O}_K)$ $\quad$ $\mathrm{disc}(\ \cdots\ |\mathcal{O}_{S_1})$

$\Rightarrow$ $\mathcal{O}_{K'}|\mathcal{O}_K$ is unram. at all primes $\mathfrak{q} \notin S$.

"$\square$"

Cor 2.8.3 Let V, W be normal projective varieties over a number field K and let $\varphi: V \to W$ be a dom. finite unram. morphism. Then, there is a finite set S of primes of K such that the field of def. K' of any $P \in V(\bar{K})$ with $Q := \varphi(P) \in W(K)$ is unramified at all primes $\mathfrak{q} \notin S$.

Pf Let S_{ij} be the set from Thm 2.8.2 for the restriction $\varphi: \varphi^{-1}(W \cap H_i) \cap H_j \to W \cap H_i$.

Let $S = \bigcup_{i,j} S_{i,j}$.

Write $Q = [y_0 : \dots : y_m]$ and $\mathfrak{q} \notin S$.

W.l.o.g. $v_{\mathfrak{q}}(y_0) \le v_{\mathfrak{q}}(y_1) \le \dots$

Dividing by y_0, we can arrange that $v_{\mathfrak{q}}(y_i) \ge 0 \; \forall i$ and $y_0 = 1$.

$\Rightarrow$ By Thm 2.8.2, K' is unram. at $\mathfrak{q}$. $\square$

$y_1, \dots, y_m$ are the coord. of Q in the affine chart $W \cap H_0 \cong \mathbb{A}^n$

2.9. Proof of weak Mordell-Weil

<u>Weak M-W</u> Let K be a number field, $\phi : E_1 \to E_2$ a nonzero isogeny between ell. curves over K with $\ker(\phi) \subseteq E_1(K)$. Then, the group $E_2(K)/\phi(E_1(K))$ is finite.

<u>Pf</u> Apply Cor 2.8.3 to ϕ. Let S be the resulting set of primes.
By Hermite's thm., there are only fin. many field ext. $K'|K$ of degree $\leq \deg(\phi)$ unramified at all primes $\mathfrak{q} \notin S$.
Let L be the Galois closure of their compositum.
The field of def. of any $P \in E_1(\bar{K})$ with $Q := \phi(P) \in E_2(K)$ is unram. at all primes $\mathfrak{q} \notin S$ and has degree $\leq \deg(\phi)$.
$\Rightarrow \phi^{-1}(E_2(K)) \subseteq E_1(L)$.
Let $G := \mathrm{Gal}(L|K)$.

Claim: We obtain an injective group homomorphism

$$E_2(K)/\phi(E_1(K)) \hookrightarrow \mathrm{Hom}(G, \ker(\phi))$$
$$Q \longmapsto (\sigma \longmapsto \sigma(P) - P)$$

for any $P \in \phi^{-1}(Q) \subset E_1(L)$

Pf $\sigma(P) - P \in \ker(\phi)$:

$$\phi(\sigma(P)-P) = \phi(\sigma(P)) - \phi(P)$$
$$= \sigma(\underbrace{\phi(P)}_{Q}) - \underbrace{\phi(P)}_{Q}$$
$$= Q - Q = O$$

$\sigma(P) - P$ is indep. of the choice of P

$R \in \ker(\phi) \subseteq E_1(K)$

$\Rightarrow \sigma(R) - R = R - R = O$

$\Rightarrow$ If $P, P' \in \phi^{-1}(Q)$, then $P - P' \in \ker(\phi)$,

so $(\sigma(P) - P) - (\sigma(P') - P')$

$= \sigma(P - P') - (P - P') = O$.

hom. in σ

$$\sigma_1\sigma_2(P) - P = \sigma_1(\underbrace{\sigma_2(P) - P}_{\in \ker(\phi) \subseteq E_1(K)}) + (\sigma_1(P) - P)$$

$-: E \times E \to E$ is def. over K

$$= (\sigma_2(P) - P) + (\sigma_1(P) - P)$$

hom. in P

$\phi(P_1) = Q_1, \ \phi(P_2) = Q_2$

$\Rightarrow \phi_1(P_1 + P_2) = Q_1 + Q_2$

$\sigma(P_1+P_2) - (P_1+P_2) = (\sigma(P_1) - P_1) + (\sigma(P_2) - P_2)$

$\phi(E_1(K)) \mapsto O$

$Q \in \phi(E_1(K))$

$\Rightarrow$ can take $P \in E_1(K)$.

$\Rightarrow \sigma(P) - P = O$.

injective.

If $\sigma(P) - P = O \ \forall \sigma \in G = Gal(L|K)$,

then $\sigma(P) = P \ \forall \sigma$, so $P \in E_1(K)$.

$\Rightarrow Q = \phi(P) \in \phi(E_1(K))$. $\square$

G and $ker(\phi)$ are finite.

$\Rightarrow$ ~~Hom~~ $Hom(G, ker(\phi))$ is finite

$\Rightarrow E_2(K)/\phi(E_1(K))$ is finite. $\square$

Rmk If $\phi = [m]$, one can in fact take $S = \{\wp \mid E$ has bad reduction at $\wp$ or $\wp \mid m\}$.
(See Silverman.)

One can use this to obtain an explicit upper bound on the size of $E(K)/mE(K)$ and (using descent) on the rank of E over K.

Rmk Even if $\ker(\phi) \not\subseteq E_1(K)$, we still get an injective homomorphism

$$E_2(K)/\phi(E_1(K)) \hookrightarrow H^1(G, \ker(\phi))$$
$$Q \longmapsto (\sigma \mapsto \sigma(P) - P) \quad \text{for } P \in \phi^{-1}(Q)$$

to the (finite) cohomology group $H^1(G, \ker(\phi))$.

(Look at the exact sequence

$$0 \to \ker(\phi) \to E_1(\bar{K}) \xrightarrow{\phi} E_2(\bar{K}) \to 0$$

and the resulting long exact sequence in G-module cohomology:

$$\dots \to E_1(K) \xrightarrow{\phi} E_2(K) \xrightarrow{\delta} H^1(G, \ker(\phi)) \to H^1(G, E_1(\bar{K})).)$$

Conjecture (Lang) weak variant:

Let $E = \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}$ be an elliptic curve over $\mathbb{Q}$ with $a_4, a_6 \in \mathbb{Z}$ of rank r. For every $\varepsilon > 0$, there is a basis $P_1, \dots, P_r \in E(\mathbb{Q})$ of $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ with

$$\hat{h}(P_1), \dots, \hat{h}(P_r) \ll_{\varepsilon, r} \max(|a_4|^{\frac{1}{4}+\varepsilon}, |a_6|^{\frac{1}{6}+\varepsilon}).$$

Question Are there elliptic curves E over $\mathbb{Q}$ of arbitrarily large rank?

Conjecture (Néron, Honda, "folklore") No.

Conjecture (Cassels, Tate, "folklore") Yes.

Conjecture (Park-Poonen-Voight-Wood) No.

In fact, there are only fin. many ell. curves E over $\mathbb{Q}$ of rank > 21.

Record (Elkies) There is an (explicit) ell. curve E over $\mathbb{Q}$ of rank ≥ 28.

Conjecture (Elkies) (?) No. Any ell. curve E over $\mathbb{Q}$ has rank ≤ 28.

3. Abelian varieties

References:

- Milne's notes on Abelian Varieties
- Lang, Abelian Varieties

3.1. Overview

Def A group variety G over K is a variety over K and a group such that the maps $G \times G \to G$, $(g,h) \mapsto gh$ and $G \to G$, $g \mapsto g^{-1}$ are morphisms defined ~~over~~ K and with identity $e \in G(K)$.

Ex
- Ell. curve E over K
- The additive group $\mathbb{G}_a = \mathbb{A}^1_K$ (with addition)
- The multiplicative group
$$\mathbb{G}_m = \{(x,y) \in \mathbb{A}^2_K \mid xy = 1\} \cong \overline{K}^\times, \quad (x,y) \mapsto x$$
with mult.

- $GL_n = \{(M, N) \text{ pair of } n\times n\text{-matrices} \mid MN = I_n\}$ with mult.
- $SL_n = \{M \ n\times n\text{-matrice} \mid \det(M) = 1\}$.
- Any product of group varieties.

<u>Def</u> A variety V over K is <u>complete</u> if for every affine variety W over K, the projection $V \times W \longrightarrow W$ is a closed map (so the image of any closed set is closed).

<u>Ex</u> $\mathbb{A}^1_K$ is not complete: look at $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$, $(x, y) \mapsto y$

The image of $\{(x,y) \mid xy = 1\}$ is $\{y \mid y \neq 0\}$, which is not closed.

<u>Rmk</u> Complete var. behave like compact manifolds.

<u>Rmk</u> Any subvariety of a complete variety is complete.

Thm 3.1.1 $\mathbb{P}^n_k$ is complete.

Cor 3.1.2 Any $V \subseteq \mathbb{P}^n_k$ is complete.

(Rmk If $\varphi : V \to W$ is a morphism between varieties and V is complete, then φ is closed.)

<u>Remk</u> In the def. of complete varieties V, we could allow arbitrary (not just affine) varieties W.

<u>Pf</u> Let $W_1, \dots, W_n$ be the affine patches of W.

$$W = \bigcup_i W_i \quad , \quad W_i \subseteq W \text{ open.}$$

Consider a closed subset A of $V \times W$ and the proj. $\pi : V \times W \to W$.

$\pi(A \cap (V \times W_i))$ is closed in W_i.

$$\Rightarrow \pi(A) = \underbrace{\bigcap_i \left(\underbrace{\pi(A \cap (V \times W_i))}_{cl. \subseteq W_i} \cup \underbrace{(W \setminus W_i)}_{cl. \subseteq W} \right)}_{cl. \subseteq W}$$

is closed in W. $\square$

<u>Lemma 3.1.3</u> If $\varphi : V \to W$ is a morphism and V is complete, then $\varphi(V)$ is closed in W and complete.

<u>Cor 3.1.4</u> φ is closed

<u>Pf</u> If $A \subseteq V$ is closed, A is also complete. Apply the lemma to the restriction $\varphi : A \to W$.

$\square$

Pf of Lemma

$\varphi(V)$ closed: Consider the graph of φ:

$$\{(v,w)\in V\times W \mid w=\varphi(v)\}$$

It's a closed subset of $V\times W$.

Its image under the proj. $V\times W\to W$ is $\varphi(V)$.

$\varphi(V)$ complete

W.l.o.g. φ is dominant, and hence surjective (over $\overline{K}$). $W=\varphi(V)$

Let Z be an affine var. and $A\subseteq W\times Z$ closed

$$V\times Z \xrightarrow{\psi} W\times Z \xrightarrow{\pi} Z$$
$$(v,z)\mapsto(\varphi(v),z)$$

$$\pi(A)=\pi\circ\psi(\underbrace{\psi^{-1}(A)}_{\text{closed}})$$ is closed in Z because

V is complete. □

Lemma 3.1.5 An affine variety $V\subseteq \mathbb{A}^n_K$ is complete if and only if $\#V(\overline{K})<\infty$.

Pf "$\Leftarrow$" clear

"$\Rightarrow$" Consider the projection $\varphi_i : V\to \mathbb{A}^1_K$.
$(x_1,\dots,x_n)\mapsto x_i$

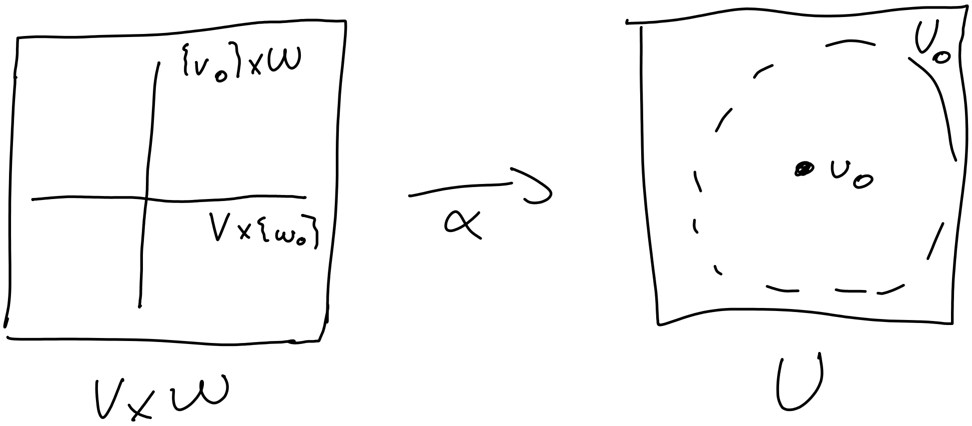
By the lemma, the image $\varphi_i(V)$ is closed, complete in $\mathbb{A}^1_K$.
$\Rightarrow \#\varphi_i(V)<\infty \ \forall i$ □

Thm 3.1.6 (Rigidity theorem)

Let V be complete and W, U be arbitrary var.

Assume that $V \times W$ is irred.

Let $\alpha : V \times W \to U$ be a morphism such that $\alpha(V \times \{w_0\}) = \alpha(\{v_0\} \times W) = \{u_0\}$ for some $v_0 \in V(k)$, $w_0 \in W(k)$, $u_0 \in U(k)$.



Then, $\alpha(V \times W) = \{u_0\}$.

Pf Let $u_0 \in U_0 \subseteq U$ be an affine patch.

Then, $Z := \{w \in W \mid \exists v \in V : \alpha(v,w) \notin U_0\}$

is the image of the closed set

$\alpha^{-1}(U \setminus U_0) \subseteq V \times W$ under the proj.

$V \times W \to W$.

$\Rightarrow Z \subseteq W$ is closed

V complete

$\Rightarrow w_0 \in W \setminus Z \subseteq W$ is open

For any $w \in W \setminus Z$, consider the morphism

$$\begin{aligned} V &\longrightarrow U_0 . \\ v &\longmapsto \alpha(v,w) \end{aligned}$$

Its image is complete and affine, hence finite. The image contains $\alpha(v_0, w) = v_0$. Since V is irred. (because $V \times W$ is), the image is also irred. Hence, the image is $\{v_0\}$.

$\Longrightarrow \alpha(v,w) = v_0 \quad \forall v \in V, \ w \in W \setminus Z$

But $V \times (W \setminus Z)$ is a nonempty open subset of the irred. var $V \times W$, hence dense.

$\Longrightarrow \alpha(v,w) = v_0 \quad \forall v \in V, w \in W.$ $\square$

3.2. Basic properties of algebraic groups

Lemma 3.2.1 Let G be an alg-group.

The connected component G_0 of G containing the identity $e \in G$ is a normal subgroup of G. The quotient G/G_0 is the (finite) group of connected components of G.

Pf Let A, B be conn. comp. of G.

$\Rightarrow$ $A \times B \subseteq G \times G$ is connected

$\Rightarrow$ Its image $A \cdot B$ under the morphism

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\longmapsto gh \end{aligned}$$

is connected.

$\Rightarrow$ $A \cdot B$ is contained in some conn. comp.

Similarly, A^{-1} is contained in some conn. comp.

$\Rightarrow$ We obtain a (well-def!) group law on $S := \{\text{conn. comp.}\}$ with a group hom. $f: G \twoheadrightarrow S$

$$\begin{aligned} g &\longmapsto \text{conn. comp. containing } g \\ e &\longmapsto G_0 \end{aligned}$$

Then, $G_0 = \ker(f)$. $\square$

Lemma 3.2.2 Any connected alg. group G is irreducible and in fact smooth.

Pf Say $G = V_1 \cup \ldots \cup V_r$ is the decomposition into irred. comp.

Rmk Any conn. (over K) alg. group G is geometrically (over $\overline{K}$) connected.

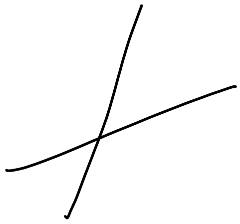
Pf $Gal(\overline{K}|K)$ acts transitively on the conn. comp. of $G(\overline{K})$ over $\overline{K}$. But $e \in G(K)$ is fixed by every el. of $Gal(\overline{K}|K)$ and lies in just one conn. comp. $\square$

$\leadsto$ w.l.o.g. $K = \overline{K}$.

For any $g \in G(\overline{K})$, the translation morphism
$$\tau_g : G \to G, \quad h \mapsto gh$$
is an isomorphism of varieties and hence permutes the irred. comp.

G irred: Consider the alg. set

$$S = \bigcup_{i \neq j} (V_i \cap V_j) \subseteq G(\overline{k}).$$



$$\Rightarrow \underset{\substack{\| \\ g\cdot S}}{\tau_g(S)} = S \quad \forall g \in G(\overline{k})$$

$$\Rightarrow S = \emptyset \quad \text{or} \quad S = G(\overline{k})$$

$S = \emptyset$ $\Downarrow$ $V_i \cap V_j = \emptyset \ \forall i,j$ $\Downarrow$ ⇐ G conn: just one irred. comp.

$S = G(\overline{k})$: impossible because

$$\dim(S) \leq \max_{i \neq j} \dim(V_i \cap V_j) < \max_i \dim(V_i) = \dim(G)$$

G smooth: Let $S' \subseteq G(\overline{k})$ be the set of singular points. $\Rightarrow \underbrace{gS' = \tau_g(S')}$ $= S'$

$$\Rightarrow S' = \emptyset \quad \text{or} \quad S' = G(\overline{k})$$

$S' = G(\overline{k})$: impossible by problem 2b from problem set 2.

$\square$

Def A homomorphism of alg. groups is a group hom. which is also a morphism.

Rmk The kernel of a hom. of alg. groups is an alg. group.

Lemma 3.2.3 The image of a hom. $\varphi: G \to H$ of alg. groups is a closed subgroup of H.

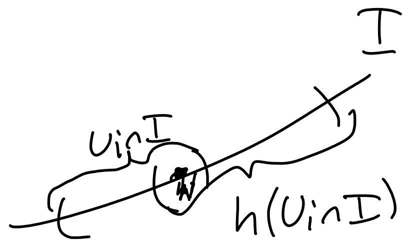
Pf Let $I = \overline{\varphi(G)}$.

W.l.o.g. G is connected (...), so G and I are irred. Of course $\varphi(G)$ is a subgr. of H. $\Rightarrow$ By continuity of mult., inverse, the closure I is also a subgroup of H.

By Chevalley's theorem, $\varphi(G) \subseteq H$ is locally closed, so $\varphi(G) = \bigcup_{i=1}^{n} (U_i \cap T_i)$ for open $U_i \subseteq G$ and closed $T_i \subseteq I$ with $U_i \cap T_i \neq \emptyset$. Since $I = \overline{\varphi(G)} \subseteq \bigcup_i T_i$ is irred., we have $T_i = I$ for some i.

$\Rightarrow \varphi(G) \supseteq U_i \cap I \neq \emptyset$

Take any $h \in I$. Then, both



$$U_i \cap I$$

and

$$h \cdot (U_i \cap I)$$

are nonempty open subsets of I.

Since I is irred., they intersect.

Take $h' \in (U_i \cap I) \cap (h \cdot (U_i \cap I))$.

$$\subseteq \varphi(G) \cap (h \cdot \varphi(G)).$$

$\Rightarrow \exists\, g, g' \in G : \varphi(g) = h' = h \cdot \varphi(g')$

$\Rightarrow h = \varphi(g)\varphi(g')^{-1} = \varphi(g g'^{-1}) \in \varphi(G)$.

$\Rightarrow \varphi(G) = I = \overline{\varphi(G)}$. $\square$

3.3. Basic properties of abelian varieties

Def An abelian variety is a complete irreducible group variety.

Ex Elliptic curves

Non-ex $\mathbb{G}_a, \mathbb{G}_m$ (!!!)
$\mathbb{G}_a = \mathbb{A}^1_K$

Thm 3.3.1 Any abelian variety A is commutative(!)

Pf $T = \{(x, yxy^{-1}) \mid x, y \in A\}$ is the image of
$$A \times A \longrightarrow A \times A \qquad (x,y) \longmapsto (x, yxy^{-1})$$
and hence closed (because A is complete) and irreducible (because A is (geom.) irreducible).

Also, T contains exactly one point of the form (e, a) with $a \in A$, namely (e,e).

$\Rightarrow$ The preimage of e under the proj. $T \to A$, $(s,t) \mapsto s$ is just the point (e,e).

$$\Rightarrow \quad \dim(T) \leq \dim(A).$$

$\dim(\pi^{-1}(y)) \geq \dim(X) - \dim(Y)$
for any $\pi : X \to Y$
and $y \in \pi(X)$

On the other hand, $\underbrace{\{(x,x) \mid x \in A\}}_{\dim(\cdot) = \dim(A)} \subseteq \underset{\text{irred.}}{T}$.

$$\Rightarrow \{(x,x) \mid x \in A\} = T.$$

$$\Rightarrow yxy^{-1} = x \quad \forall x, y \in A. \qquad \square$$

⇝ We write ab. var. additively.

<u>Thm 3.3.2</u> Let A, B be abelian varieties. Then, any morphism $\varphi : A \to B$ sending $0 \in A$ to $0 \in B$ is a group hom.

<u>Pf</u> Consider the morphism

$$\begin{aligned} \alpha : A \times A &\longrightarrow B \\ (a_1, a_2) &\longmapsto \varphi(a_1 + a_2) - \varphi(a_1) - \varphi(a_2) \end{aligned}$$

We have $\alpha(A \times \{0\}) = \{0\} = \alpha(\{0\} \times A)$. Since A is complete and (geometrically) irreducible, Thm 3.1.6 (Rigidity) shows $\alpha(A \times A) = \{0\}$. $\square$

Cor 3.3.3 The group operation on an abelian variety A is determined by the variety A and the identity element $0 \in A(k)$.

Pf The identity morphism $id : A \to A$ is a group hom. for any ab. var. structures on the LHS and RHS. $\square$

Rmk The Thm is wrong for general group var. A, B:

E.g. $\mathbb{G}_m \hookrightarrow \mathbb{G}_a$ is not a group hom.

$x = (x, x^{-1}) \longmapsto x$

Rmk The Thm is correct if A is ~~an~~ ab. var. and B is any group var.

(The image of A is an ab. var.)

Rmk The Thm is correct if B is an ab. var. and A is any group var. (need another version of the rigidity thm ...)

Lemma 3.3.4 Let V be a smooth (or just normal) variety, W be a complete variety. Then, any rational map $\varphi : V \dashrightarrow W$ is defined on (= can be extended to) an open subset $U \subseteq V$ with $\dim(V \setminus U) \leq \dim(V) - 2$.

Exe
$$\begin{aligned} \mathbb{A}^2_K &\dashrightarrow \mathbb{P}^1_K \\ (x,y) &\longmapsto [x:y] \end{aligned}$$
is def. everywhere except at O.

Rmk Completeness required:
$$\begin{aligned} \mathbb{A}^1_K &\dashrightarrow \mathbb{A}^1_K \\ x &\longmapsto \frac{1}{x} \end{aligned}$$
can't be extended to O

Rmk Smoothness (or normality) required
$$\begin{aligned} \{(x,y) \in \mathbb{A}^2_K \mid x^3 = y^2\} &\dashrightarrow \mathbb{P}^1_K \\ (x,y) &\longmapsto [x:y] \end{aligned}$$
can't be extended to O

(The composition
$$\begin{aligned} \mathbb{A}^1_K \to \{\ldots\} &\to \mathbb{P}^1_K \\ t \mapsto (t^2,t^3) &\underset{\substack{\uparrow \\ \text{for } t \neq 0}}{\longmapsto} [t^2:t^3] = [1:t] \end{aligned}$$
would by continuity send every t to $[1:t]$, so it's "the identity" $\mathbb{A}^1 \to \mathbb{A}^1$. But its derivative at $t=0$ is O.)

Cor 3.3.5 If V is a smooth curve and W is complete, then any rat. map $V \dashrightarrow W$ is (= can be extended to) a morphism $V \to W$.

Lemma 3.3.6 Let V be a smooth var, G be a group variety, and let $\varphi : V \dashrightarrow G$ be a rational map defined on an open set $U \subseteq V$ (which can't be extended to a larger open subset). Then, every irred. comp. of $V \setminus U$ has codimension 1 in V.

Pf Consider the rational map

$$\alpha : V \times V \dashrightarrow G$$
$$(x, y) \longmapsto \varphi(x)\varphi(y)^{-1}$$

Let α be defined on the open set $S \subseteq V \times V$ (and not extendable to any larger open set).

Claim: $x \in U \iff (x,x) \in S$

Pf: "$\Rightarrow$" Clear. In fact, $U \times U \subseteq S$.

"$\Leftarrow$" Since V is irred., the nonempty open subsets $U \subseteq V$ and $\{y \in V \mid (x,y) \in S\} \subseteq V$ intersect. Let $y \in U$ with $(x,y) \in S$.

Consider the open set

$U' = \{x' \in V \mid (x', y) \in S\}$ containing x

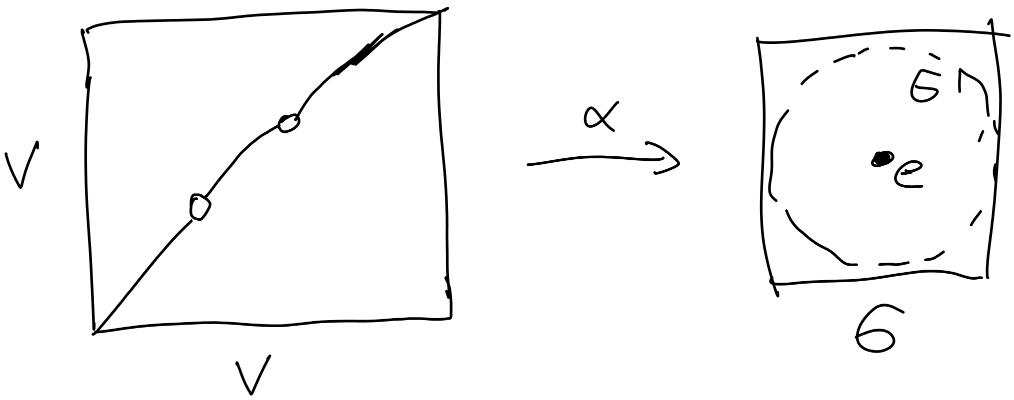
and the morphism

$$\varphi' : U' \longrightarrow G .$$
$$x' \longmapsto \alpha(x', y)\varphi(y)$$

Note that φ and φ' agree on $U \cap U' \subseteq V$.

$\Rightarrow$ φ can be extended to the open neighborhood $U \cup U'$ of x. $\Rightarrow x \in U$. $\square$

If α is def. at (x, x), then $\alpha(x,x) = \varphi(x)\varphi(x)^{-1} = e$.



Let $G' \subseteq G$ be an (open) affine patch containing e. Let $G' \subseteq \mathbb{A}^n_K$ be an embedding.

We obtain a rat. map $\alpha' : V \times V \dashrightarrow G' \subseteq \mathbb{A}^n_K$ given by rat. fcts. $\alpha'_1, \dots, \alpha'_n \in K(V \times V)$.

Consider the divisor $D_i = \operatorname{div}(\alpha'_i) \subseteq V \times V$.

Write $D_i = \sum\limits_{\substack{Z \subseteq V \\ \text{irred.} \\ \text{codim } 1}} c_{i,Z} Z$.

φ def. at x

$\Leftrightarrow \alpha$ def. at (x,x)

$\Leftrightarrow \alpha'$ def. at (x,x)

$\Leftrightarrow (x,x) \notin \bigcup_i \underbrace{\bigcup_{Z : c_{i,Z} < 0} Z}_{\text{pole divisor of } \alpha_i'}$

For any $Z \subseteq V \times V$ irred. of codimension 1 as above, each irred. comp. of

$$\{x \in V \mid (x,x) \in Z\} \subseteq V$$

has codimension ≤ 1 in V. $\square$

<u>Thm 3.3.7</u> Let V be a smooth variety and A an abelian variety. Then, any rat. map $V \dashrightarrow A$ is (= can be extended to) a morphism $V \longrightarrow A$.

<u>Pf</u> By Lemma 3.3.5, it is def. everywhere or undef. on a set of codim. 1.

By Lemma 3.3.4, it's undef. at most on a set of codim ≥ 2. $\square$

Lemma 3.3.8 Any smooth curve C is an open subset of a (unique) smooth projective curve C'.

Lemma 3.3.9 For any irred. curve C with smooth locus $U \subseteq C$, there is a smooth curve C' (the normalization of C) with a morphism $\pi : C' \to C$ which induces an isomorphism $U' \to U$ for $U' = \pi^{-1}(U)$.

Pf See Chapter I. 6 in Hartshorne. □

Exe
$$\mathbb{A}^1_K \longrightarrow \{(x,y) \mid x^3 = y^2\}$$
$$t \longmapsto (t^2, t^3)$$

Rmk If $C \subseteq \mathbb{A}^n_K$ is an affine curve, let R be the integral closure of $\Gamma(C)$ in $K(C)$. It's a fin.-gen.-ring ext. of K, say $R = K[f_1, \dots, f_m]$. Let I be the kernel of
$$K[X_1, \dots, X_m] \to R.$$
$$X_i \mapsto f_i$$

$\Gamma(C) \subseteq R = K[X_1, \dots, X_m]/I$. Take $C' = V(I) \subseteq \mathbb{A}^m_K$, $C' \to C$ corr. to the inclusion $\Gamma(C) \hookrightarrow R$.

Ex $C = \{(x,y) \mid y^2 = x^2(x+1)\}$

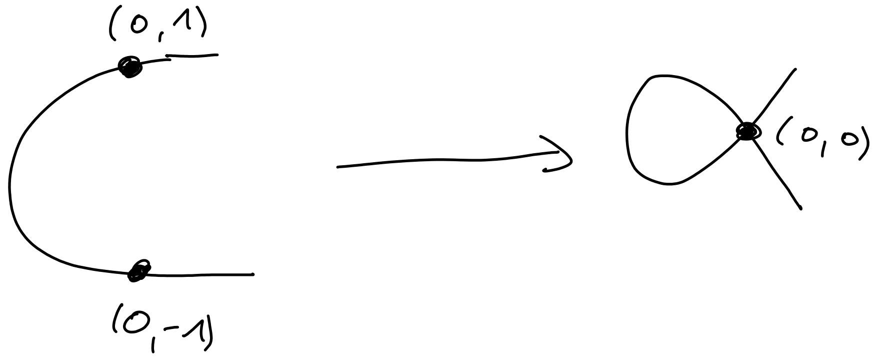
$$\Gamma(C) = K[X,Y]/(Y^2 - X^2(X+1))$$

$$R = \Gamma(C)[\underbrace{\tfrac{Y}{X}}_{Z}] = K[X,Z]/(Z^2-(X+1))$$

$$C' = \{(x,z) \mid z^2 = x+1\}$$

$$C' \longrightarrow C$$

$$(x,z) \longmapsto (x, xz)$$



Thm 3.3.10 (Rigidity theorem 2)

Let V, W be smooth varieties, A an abelian variety, $V \times W$ geom. irred.
Let $\alpha : V \times W \to A$ be a morphism such that

$$\alpha(V \times \{w_0\}) = \alpha(\{v_0\} \times W) = \{a_0\}$$

for some $v_0 \in V(K)$, $w_0 \in W(K)$, $a_0 \in A(K)$.

Then, $\alpha(V \times W) = \{a_0\}$.

Pf W.l.o.g. K is alg. closed and $V \subseteq \mathbb{A}^n_K$.

If $V = C$ is a curve:

Let $C' \supseteq C$ be a smooth proj. curve.
By Thm 3.3.7, $\alpha : C \times W \to A$ extends to $\alpha' : C' \times W \to A$
By continuity, we still have
$$\alpha'(C' \times \{w_0\}) = \alpha'(\{v_0\} \times W) = \{a_0\}.$$
Since C' is complete, we can then apply the original rigidity theorem.

For any V: Consider an irreducible curve $v_0 \in C \subseteq V$ which is smooth at v_0. Let $\pi : C' \to C$ be a normalisation. It induces a morphism

$\alpha' : C' \times W \to A$ with

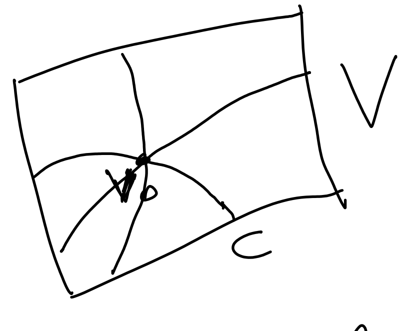
$$\alpha'(C' \times \{w_0\}) = \alpha'(\{\pi^{-1}(v_0)\} \times W) = \{a_0\}$$

a single point because C is nonsingular at v_0

We saw above that this implies

$$\alpha'(C' \times W) = \{a_0\}.$$

Then, the claim follows by continuity from the following Lemma. □



Lemma 3.3.11 Let k be alg. closed, $V \subseteq \mathbb{A}^n_k$ irred., $v_0 \in V(k)$ a nonsingular point. Then, the union of the irred. curves $v_0 \in C \subseteq V$ which are nonsingular at v_0 is (Zariski) dense in V.

Cor 3.3.12 Let V, W be smooth, $v_0 \in V(k)$, $w_0 \in W(k)$, $V \times W$ geom. irred., A an abelian variety, $\alpha : V \times W \to A$ a morphism with $\alpha(v_0, w_0) = 0$. Then, there are (unique) morphisms $\varphi : V \to A$, $\psi : W \to A$ such that $\alpha(v, w) = \varphi(v) + \psi(w)$ for all $v \in V(\bar{k})$, $w \in W(\bar{k})$ and $\varphi(v_0) = \psi(w_0) = 0$.

Pf We need to take

$$\varphi(v) = \alpha(v, w_0), \quad \psi(w) = \alpha(v_0, w).$$

Then, $\alpha'(v, w) := \alpha(v, w) - \varphi(v) - \psi(w)$ satisfies the assumptions of the rigidity theorem 2. $\Rightarrow \alpha'(V \times W) = \{0\}$. $\square$

Cor 3.3.13 Let $\varphi : G \to A$ be a morphism of varieties from a connected group var G to an abelian var. A sending the identity $e \in G$ to identity $0 \in A$. Then, φ is a group homomorphism.

Pf Same as Thm 3.3.2 but using rigidity theorem 2. $\square$

Cor 3.3.14 Any morphism $\varphi : \mathbb{A}^n_k \to A$ to an abelian variety is constant.

Pf $n=1$: The morphism

$$\mathbb{A}^1_k = \mathbb{G}_a \longrightarrow A$$
$$x \longmapsto \varphi(x) - \varphi(0)$$

is a group homomorphism.

The morphism

$$\mathbb{A}^1_k \supset \mathbb{G}_m \longrightarrow A$$
$$(x, x^{-1}) \longmapsto \varphi(x) - \varphi(1)$$

is a group homomorphism.

$$\Rightarrow \varphi(x+y) + \varphi(0) = \varphi(x) + \varphi(y) \quad \forall x,y \in \bar{k}$$
$$\varphi(xy) + \varphi(1) = \varphi(x) + \varphi(y) \quad \forall x,y \in \bar{k}^\times$$

$$\Rightarrow \varphi(x+y) + \varphi(0) = \varphi(xy) + \varphi(1) \quad \forall x,y \in \bar{k}^\times$$

Pick $y = -x$.

$$\Rightarrow 2\varphi(0) = \varphi(-x^2) + \varphi(1) \quad \forall x \in \bar{k}^\times$$

$$\Rightarrow 2\varphi(0) = \varphi(x) + \varphi(1) \quad \forall x \in \bar{k}^\times$$

$$\Rightarrow \varphi(x) = \text{const.}$$

$n > 1$: Use induction and Cor 3.3.12. $\square$

3.4. The Jacobian variety

Let C be a smooth proj. curve over K of genus g with $C(K) \neq \emptyset$.

__Goal__: Construct an abelian variety $J = J_C$ (the __Jacobian variety__ of C) such that we have a group isomorphism

$$J(K) = \mathcal{Cl}^0(C).$$

__Ex__ If C is an ell. curve, we have previously considered ~~the~~ the bijection

$$C(K) \xrightarrow{\sim} \mathcal{Cl}^0(C)$$
$$P \longmapsto [P]-[O]$$

$\rightsquigarrow$ The Jacobian variety of an ell. curve E is $J_E = E$.

__Ex__ If $C = \mathbb{P}^1_K$, we have shown
$\mathcal{Cl}^0(C) = 1$.

$\rightsquigarrow$ The Jacobian variety of $\mathbb{P}^1_K$ is the trivial abelian variety 1.

Rmk In fact, we want a group isom.

$$J(L) = \mathcal{Cl}^0(C_L) \text{ for every field}$$

ext. $L|K$, where C_L is the same curve C, but with base field L. The isom. should commute:

$$\begin{tikzcd} J(L) \arrow[r, phantom, "="] \arrow[d, hook] & \mathcal{Cl}^0(C_L) \arrow[d, hook] \\ J(L') \arrow[r, phantom, "="] & \mathcal{Cl}^0(C_{L'}) \end{tikzcd} \qquad \begin{matrix} L' \\ | \\ L \\ | \\ K \end{matrix}$$

Rmk If $C(K) \neq \emptyset$ and $L|K$ is a Gal. ext., we have

$$\mathcal{Cl}^0(C) = \mathcal{Cl}^0(C_L)^{\mathrm{Gal}(L|K)}.$$

Rmk We will obtain a map

$$\begin{aligned} C(K) &\longrightarrow \mathcal{Cl}^0(C) = J(K) \\ P &\longmapsto [P]-[Q] \end{aligned}$$

for any fixed $Q \in C(K)$.

$C \hookrightarrow J$ is injective if $g \geq 1$.

Idea of construction of J

Fix some point $P \in C(K)$. Then,

$$\underbrace{C(\bar{K}) \times \dots \times C(\bar{K})}_{g} / S_g \longrightarrow \mathcal{C}\ell^0(C_{\bar{K}})$$

$$(Q_1, \dots, Q_g) \longmapsto Q_1 + \dots + Q_g - gP$$

is "almost a bijection", where S_g denotes the symmetric group of order $g!$ (acting on $C \times \dots \times C$ by permutation).

Surjective: Let $D \in \mathcal{C}\ell^0(C_{\bar{K}})$.

$\Rightarrow \deg(D + gP) = g$

$\underset{R-R}{\Rightarrow} \ell(D + gP) \geq 1$

$\Rightarrow$ $D + gP$ lies in the same divisor class as some divisor $E \geq 0$ (of degree g). Write $E = Q_1 + \dots + Q_g$.

Almost injective:

For "generic" $D \in \mathrm{Div}^0(C_{\bar{u}})$, we have only one preimage $(Q_1, \dots, Q_g)$ because $\ell(D + gP) = 1$:

By R-R, $\ell(2gP) = g + 1$.

By Cor 1.10,

$$\ell(2gP - R_1) = g \text{ for a.a. } R_1 \in C(\bar{u}).$$

For any such R_1, by Cor 1.10,

$$\ell(2gP - R_1 - R_2) = g - 1 \text{ for a.a. } R_2 \in C(\bar{u}).$$

$$\vdots$$

$$\ell(\underbrace{2gP - R_1 - \dots - R_g}_{\text{div of deg } g}) = 1 \text{ for a.a. } R_g \in C(\bar{u})$$

$\Rightarrow \emptyset \neq \{(R_1, \dots, R_g) \mid P, R_1, \dots, R_g \text{ distinct}, \ \ell(2gP - R_1 - \dots - R_g) = 1\} =: T$

Claim: This set T is an open subset of $C \times \dots \times C$.

Pf Let $P, R_1, \dots, R_g$ be distinct. Then,

$2gP - R_1 - \dots - R_g + \mathrm{div}(h) \geq 0 \Leftrightarrow 2gP + \mathrm{div}(h) \geq 0$, $h(R_1) = \dots = h(R_g) = 0$.

Hence, if $f_1, \dots, f_{g+1}$ form a basis of $L(2gP)$, then $(R_1, \dots, R_g) \in T$ if and only if the matrix $(f_i(R_j))_{ij}$ has rank g. $\square$

<u>Steps</u>:

1) Pick $\emptyset \neq U \subseteq C$ open and affine s.t. $U \times \dots \times U / S_g \longrightarrow \mathcal{Cl}^0(C_{\bar{K}})$ is injective.

2) Construct an affine variety $U^{(g)}$ whose pts are in bijection with elements of $U \times \dots \times U / S_g$.

3) Show that the group op. $+$ on $\mathcal{Cl}^0(C_{\bar{K}})$ is described by a rational map $U^{(g)} \times U^{(g)} \dashrightarrow U^{(g)}$.

4) Cover $\mathcal{Cl}^0(C_{\bar{K}})$ by translates of the image of $U^{(g)}$. These translates will form affine charts of J_C.

5) Show that the variety J_C is <u>complete</u>.

C. Quotients of varieties by finite groups

Reference: Joe Harris, Alg. Geom. (A first course), lecture 10

Q Let G be a finite group acting on a variety V (def. over K) such that for any $g \in G$, the map $\tau_g : V \longrightarrow V$, $x \mapsto gx$ is a morphism (def. over K).

Assume $V \subseteq \mathbb{A}^n_K$.
The morphism $\tau_g : V \to V$ corr. to a K-alg. hom. $\tau_g^* : \Gamma(V) \to \Gamma(V)$, $f \mapsto f \circ \tau_g$, so we have a (right) action of G on $\Gamma(V)$.

Lemma C.1 The ring of invariants

$$\Gamma(V)^G = \{ f \in \Gamma(V) \mid \tau_g^*(f) = f \ \forall g \in G \}$$

is a finitely generated K-alg.

Def Let $\Gamma(V)^G \cong K[Y_1, \dots, Y_m]/I$. Then, we define the quotient variety
$V^G := V(I) \subseteq \mathbb{A}^m_K$ (with $\Gamma(V^G) = \Gamma(V)^G$)

and the <u>quotient morphism</u>

$\pi : V \to V^G$ is the morphism corr. to

the inclusion $\pi^* : \Gamma(V^G) = \Gamma(V)^G \hookrightarrow \Gamma(V)$.

<u>Note</u> By def., $\underset{\underset{\pi\circ\tau_g(x)}{\shortparallel}}{\pi(gx)} = \pi(x)$ $\forall g \in G, x \in V$.

(because $\tau_g^* \circ \pi^* = \pi^*$)

<u>Ex</u> Let the symm. gr. S_n act on $V = \mathbb{A}_k^n$
by permuting coordinates.
It acts on $\Gamma(V) = k[X_1, \ldots, X_n]$ by
permuting variables.

$$\Gamma(V)^{S_n} = k[X_1, \ldots, X_n]^{S_n} = \text{ring of symm. pol.}$$

$$k[X_1, \ldots, X_n]^{S_n} \cong k[Y_1, \ldots, Y_n]$$

i-th elem. symm. pol. $\leftarrow\!\shortmid$ Y_i

$X_1 + \ldots + X_n \leftarrow\!\shortmid Y_1$

$X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n \leftarrow\!\shortmid Y_2$

$X_1 \cdots X_n \leftarrow\!\shortmid Y_n$

$\rightsquigarrow (\mathbb{A}^n_k)^{S_n} = \mathbb{A}^n_K$

$\pi : \mathbb{A}^n_k \longrightarrow \mathbb{A}^n_K$

$(x_1, \dots, x_n) \longmapsto (y_1, \dots, y_n)$ where

y_i is the i-th elem. symm. pol. in $x_1, \dots, x_n$.

Pf of Lemma

Since $V \subseteq \mathbb{A}^n_k$, $\Gamma(V)$ is fin. gen.

W.l.o.g., the set of generators is closed under the action of G.

Say $\Gamma(V) = k[X_1, \dots, X_r]/I$ and G acts on $X_1, \dots, X_r$ by permutation.

(so we have an embedding $V \subseteq \mathbb{A}^r_k$ such that the action of G on V is the restriction of a permutation action on the coord. in $\mathbb{A}^r_k$.)

Consider the quotient hom.

$$k[X_1, \dots, X_r]^G \longrightarrow (k[X_1, \dots, X_r]/I)^G.$$

It is <u>surjective</u>:

Let $f \in K[X_1, \dots, X_r]$ such that $\tau_g^*(f) \equiv f \mod I \;\; \forall g \in G$.

Then, the "orbit average":

$$\frac{1}{|G|} \sum_{g \in G} \tau_g^*(f) \text{ lies in } K[X_1, \dots, X_r]^G$$

and is $\equiv f \mod I$.

But $K[X_1, \dots, X_r]^{S_r} \subseteq K[X_1, \dots, X_r]^G \subseteq K[X_1, \dots, X_r]$.

LHS is a fin. gen. K-alg. and RHS is a fin. gen. LHS-mod.

$\Rightarrow K[X_1, \dots, X_r]^G$ is a fin. gen. K-alg.

$\Rightarrow \Gamma(V)^G = (K[X_1, \dots, X_r]/I)^G$ is a fin. gen. K-alg.

$\square$

<u>Ex</u> $G = \{\pm 1\}$ act on $V = \mathbb{A}_K^2$ by $(-1) \cdot (x, y) = (-x, -y)$.

We have $K[X, Y]^G = K[X^2, XY, Y^2]$

$\cong K[A, B, C] / (AC - B^2)$ (Syzygy)

$\rightsquigarrow V^G = \{(a, b, c) \in K^3 \mid ac = b^2\}$

$\pi : V \to V^G$

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

Lemma C.2 The map $\pi : V(\overline{K}) \to V^G(\overline{K})$ is surj. and each fiber is a G-orbit in $V(\overline{K})$.

Cor C.3 $\dim(V^G) = \dim(V)$.

Ese $S_n \curvearrowright \mathbb{A}^n_K$

$\rightsquigarrow$ The preimage of $(y_1, \dots, y_n) \in \overline{K}^n$ is the set of $(x_1, \dots, x_n) \in \overline{K}^n$ such that

$$(T - x_1) \cdots (T - x_n) = T^n - y_1 T^{n-1} + \dots + (-1)^n y_n$$

(the root-with-correct-multiplicity-tuples).

Rmk ~~Im~~part. $\pi : V(K) \to V^G(K)$ is in general **not** surjective.

Pf of Lemma W.l.o.g. $K = \overline{K}$.

surj Let $Q \in V^G(K)$ and let $m_Q \subseteq \Gamma(V^G)$ be the corr. max. ideal. We want to show that

$$\emptyset \neq \{P \in V(\overline{K}) \mid \pi(P) = Q\}$$
$$= \{P \in V(\overline{K}) \mid \underset{\pi^*(f)(P)}{\underset{\shortparallel}{f(\pi(P))}} = 0 \ \forall f \in m_Q\}.$$

(π^* is the inclusion map $\Gamma(V)^G \to \Gamma(V)$)

By Hilbert's Nsts, this is equivalent to

$1 \notin$ (id. of $\Gamma(V)$ gen. by $\cancel{\pi^*}(m_Q)$).

Say $1 = \sum_i h_i f_i$ with $h_i \in \Gamma(V)$,

$f_i \in m_Q \subseteq \Gamma(V)^G$.

$$\Rightarrow 1 = \frac{1}{|G|} \sum_{g \in G} \sum_i \underbrace{\tau_g^*(h_i f_i)}_{\tau_g^*(h_i) f_i}$$

$$= \frac{1}{|G|} \sum_i \underbrace{\left(\sum_g \tau_g^*(h_i)\right)}_{\in \Gamma(V)^G} \underbrace{f_i}_{\substack{\in m_Q \\ (\text{id. of } \Gamma(V)^G)}} \in m_Q$$

$\lightning$

<u>fibers are G-orbits</u> Let $P_1, P_2 \in V(\bar{k})$.

If $P_1 \notin \{g P_2 \mid g \in G\}$, by the chin. remainder theorem, there is a fct. $h \in \Gamma(V)$ with $h(P_1) = 0$, $h(gP_2) = 1 \; \forall g \in G$.

Consider $f := \prod_{g \in G} \tau_g^*(h) \in \Gamma(V)^G$.

We have $f(P_1) = 0$, $f(P_2) = 1 \neq 0$.

$\Rightarrow \pi(P_1) \neq \pi(P_2)$ because $f = \pi^*(f)$. $\square$

Def Let $V \subseteq \mathbb{A}^n_k$ and $r \geq 1$. The <u>r-th symmetric power</u> of V is

$$V^{(r)} := (\underbrace{V \times \dots \times V}_{r})^{S_r}.$$

Lemma C.3 Assume $C/\mathbb{A}^n_k$ is a smooth curve. Then, $C^{(r)}$ is smooth (of dim. r).

Rmk $((\mathbb{A}^n_k)^r)^{S_r}$ is singular for $n, r \geq 2$. (?)

(at the image of $(0, \dots, 0) \in (\mathbb{A}^n)^r$ in $((\mathbb{A}^n)^r)^{S_r}$)

Pf (sketch) w.l.o.g. $k = \overline{k}$.

Consider a point $(P, \dots, P) \in C \times \dots \times C$.
Let Q be its image in $C^{(r)}$.

The local ring $\mathcal{O}_{C,P}$ is a DVR with residue field $k = \overline{k}$ and uniformizer $t_{C,P}$.
Let $\widehat{\mathcal{O}}_{C,P}$ be its completion with max. ideal $\widehat{m}_{C,P} = m_{C,P} \widehat{\mathcal{O}}_{C,P}$.
We obtain an isomorphism $k[[T]] \to \widehat{\mathcal{O}}_{C,P}$.
$T \mapsto t_{C,P}$

("Analytically, any curve looks like $\mathbb{A}^1$ near a smooth point.")

The completion of $\mathcal{O}_{C^{(r)},Q}$ (at $m_{C^{(r)},Q}$)

is $\hat{\mathcal{O}}_{C^{(r)},Q} = \varprojlim_{n\to\infty} \mathcal{O}_{C^{(r)},Q} / m^n_{C^{(r)},Q}$

$$\cong k[[T_1, \ldots, T_r]]^{S_r}$$

$$\cong k[[\underbrace{U_1, \ldots, U_r}_{\substack{\text{elem. symm.} \\ \text{pol. in } T_1,\ldots,T_r}}]]$$

The max. ideal $\hat{m}_{C^{(r)},Q}$ of this ring is $(U_1, \ldots, U_r)$. It satisfies

$$\begin{array}{ccc} \hat{m}_{C^{(r)},Q} / \hat{m}^2_{C^{(r)},Q} & \cong & \hat{m}_{(\mathbb{A}^1)^{(r)},0} / \hat{m}^2_{(\mathbb{A}^1)^{(r)},0} \\ \| & & \| \\ m_{C^{(r)},Q} / m^2_{C^{(r)},Q} & & m_{(\mathbb{A}^1)^r,0} / m^2_{(\mathbb{A}^1)^r,0} \\ & & \cong \\ & & k^r \end{array}$$

$\Rightarrow$ dim (cotangent space at Q) $= r = \dim(C^{(r)})$.

("Same" for other tuples $(P_1, \ldots, P_r)$ ...) $\square$

Rmk You can perform a similar construction for $V \subseteq \mathbb{P}^n_k$.

Rmk If E is an ell. curve (def. over k) and $T \subseteq E(\bar{k})$ is a finite subgroup, this allows us to construct a quotient E/T, which is again an ell. curve with isogeny $E \to E/T$.

If $T \subseteq E$ is def. over K, then E/T is def. over K.

Rmk: The constructed bijection

$$V^G(\overline{K}) \longleftrightarrow (G\text{-orbit in } V(\overline{K}))$$

is $Gal(\overline{K}|K)$-equivariant.

In particular, it restricts to a bijection

$$V^G(K) \longleftrightarrow (G\text{-orbits } S \text{ in } V(\overline{K}) \text{ with } \sigma(S) = S \ \forall \sigma \in Gal(\overline{K}|K))$$

3.5. The Jacobian variety (cont.)

Reference: Lang, Abelian Varieties, II.2

Let C be a smooth projective curve over K of genus g and fix a point $P \in C(K)$.

Recall the surjective and "almost injective" map

$$d: C^{(g)}(\overline{K}) \longrightarrow \mathcal{Cl}^0(C_{\overline{K}})$$

$$[(Q_1, \dots, Q_g)] \longmapsto [Q_1] + \dots + [Q_g] - g[P]$$

(which is a bijection if C is an ell. curve)

and the corr. map

$$D: C^{(g)}(\overline{K}) \longrightarrow \mathrm{Div}^0(C_{\overline{K}})$$

$$[(Q_1, \dots, Q_g)] \longmapsto [Q_1] + \dots + [Q_g] - g[P],$$

Lemma 7.5.1 There are rational maps

$$\alpha : C^{(g)} \times C^{(g)} \dashrightarrow C^{(g)}$$

$$\beta : C^{(g)} \dashrightarrow C^{(g)}$$

such that $d(\alpha(x,y)) = d(x) + d(y)$ for (x,y) in a dense open subset of $C^{(g)} \times C^{(g)}$

and $d(\beta(x)) = -d(x)$ for x in a dense open subset of $C^{(g)}$.

Rmk This is not even obvious when d is a bijection. (For ell. curves C, we explicitly constructed the group op. α, β on C.)

Trick Let V be an irred. affine variety over K. Let $L = K(V)$ be its field of rational functions. Denote by V_L the variety V over the base field $L \supseteq K$. Then, $V_L(L)$ contains a "natural" point T called the generic point:

Consider an embedding $V \subseteq \mathbb{A}^n_K$, so

$V = \{Q \in \mathbb{A}^n_K \mid f(Q) = 0 \ \forall f \in I\}$ for some set $I \subseteq K[x_1, \ldots, x_n]$

$V_L = \{ Q \in \mathbb{A}^n_L \mid f(Q) = 0 \; \forall f \in I \}$.

Let a_i be the image of X_i in the field of fractions L of $K(X_1, \dots, X_n)/I$.

Let $T = (a_1, \dots, a_n) \in L^n$.

Note that $f(X_1, \dots, X_n) \equiv 0 \mod I$, so

$$f(a_1, \dots, a_n) = 0 \text{ in } L$$

for all $f \in I$.

$\Rightarrow T \in V_L(L)$.

This single point $T \in V_L(L)$ with coordinates in L encodes information about all points $Q \in V(K)$ with coord. in K because can "<u>specialize</u>" T to Q by plugging the coordinates of Q in for the variables that are the coordinates of T.

<u>Pf of Lemma</u> Let U be an affine patch of C.

$U \subseteq C$ dense open

$U^{(g)} \subseteq C^{(g)}$ dense open

Let $L = K(C^{(g)}) = K(U^{(g)})$

$= (K(\underbrace{U \times \cdots \times U}_{g}))^{S_g} = (K(\underbrace{C \times \cdots \times C}_{g}))^{S_g}$.

Let $T \in U_L^{(g)}(L)$ be the generic point.

We obtain a "generic divisor"

$$D(T) \in \mathrm{Div}^0(C_L).$$

Consider the divisor $E = -D(T) + g[P] \in \mathrm{Div}(C_L)$ of degree g.

Apply R-R to this divisor (over the base field L!).

$\Rightarrow \ell(E) \geq 1$.

the vector space, not the field L!

Let $f_1, \ldots, f_r \in K(C_L)$ be a basis of $\mathcal{L}(E)$.

There is a dense open subset $U' \subset U^{(g)}$ such that for all $S \in U'$, plugging the coordinates of S into the coeff. of $f_1, \ldots, f_r$ (which are elements of L and therefore rational functions on C) and into the coordinats of the points in the divisor E (which are also elements of L) produces well-defined elements $f_1, \dots, f_r \in K(C)$ and $E \in \mathrm{Div}(C)$ and $f_1^{(S)}, \dots, f_r^{(S)}$ are linearly independent (because linear dependence is a polynomial condition, which doesn't hold for all $S \in C^{(g)}$ because $f_1, \dots, f_r \in K(C_L)$ were linearly independent) and

$$f_1^{(S)}, \dots, f_r^{(S)} \in L(\underbrace{E^{(S)}}_{-D(S)+g[P]}).$$

<u>Claim</u> There is a dense open subset $U'' \subset U^{(g)}$ such that for all $S \in U''$, we have $\ell(\underbrace{-d(S) + g[P]}_{\deg = g}) = 1$.

<u>Pf</u> In the proof of "almost-injectivity" (in the first part of 3.4), we saw that there is a dense open subset $U''' \subset \underbrace{U \times \dots \times U}_{g}$ such that

$$\ell(2g[P] - Q_1 - \dots - Q_g) = 1 \text{ for all } (Q_1, \dots, Q_g) \in U'''.$$

Let U'' be the image of U''' in $U^{(g)}$. $\square$

Since $U', U'' \subset U^{(g)}$ are dense open subsets, $U' \cap U'' \neq \emptyset$.

On U', $\ell \geq r$. On U'', $\ell = 1$.

$\Rightarrow$ $r = 1$, so $\ell(E) = 1$.

Write $f = f_1$ for the generator of $L(E)$.

Then, $\underbrace{E + \mathrm{div}(f)}_{\text{div. of degree } g} \geq 0$.

$\rightsquigarrow$ Write $E + \mathrm{div}(f) = Q_1 + \dots + Q_g$

with $Q_1, \dots, Q_g \in C_L(\overline{L})$

!!!

Since $Q_1 + \dots + Q_g \in \mathrm{Div}(C_L)$ is $\mathrm{Gal}(\overline{L}|L)$-invariant, the multiset $\{Q_1, \dots, Q_g\}$ is $\mathrm{Gal}(\overline{L}|L)$-invariant, so the tuple $(Q_1, \dots, Q_g)$ corr. to a point $T' \in C_L^{(g)}(L)$. $\leftarrow$ (important!)

$$E + \mathrm{div}(f) = -D(T) + g[P] + \mathrm{div}(f).$$
$$\shortparallel$$
$$Q_1 + \dots + Q_g$$

$\Rightarrow \ -D(T) + \operatorname{div}(f) = D(T')$, so

$-D(T)$ and $D(T')$ lie in the same divisor class on C_L.

The coord. of $T' \in C_L(L)$ are elements of L and therefore rational functions on $C^{(g)}$. They define a rational map

$\beta : C^{(g)} \dashrightarrow C^{(g)}$.

There is a dense open subset $U''' \subset U^{(g)}$ such that for all $S \in U'''$, plugging the coord. of S into the coord. of T' and into the coeff. of f produces well-def. $\beta(S) = T'^S \in C^{(g)}$ and $f^{(S)} \in K(C)$ with

$$-D(S) + \operatorname{div}(f^{(S)}) = D(\underbrace{T'^S}_{\beta(S)}),$$

so $-D(S)$ lies in the same divisor class as $D(\beta(S))$.

$\rightsquigarrow \ d(\beta(S)) = -d(S)$ for $S \in U'''$.

For constructing α, use the same technique, over the field
$$L = K(C^{(g)} \times C^{(g)}).$$

Only difference:

Claim There is a dense open subset $U'' \subset U^{(g)} \times U^{(g)}$ such that for all $(S_1, S_2) \in U''$, we have
$$\ell(\underbrace{d(S_1) + d(S_2) + g[P]}_{\deg.\, g}) = 1.$$

Pf Let W be a canonical divisor.

R-R: $\ell(D) - \ell(W-D) = \deg(D) + 1 - g$ for all divisors $D \in \mathrm{Div}(C)$.

Also, $\ell(\underbrace{W + g[P]}_{\deg = 3g-2}) = 2g-1$.

As in the proof of "almost-injectivity", there is a dense open subset

$$U'' \subset \underbrace{U \times \dots \times U}_{g} \times \underbrace{U \times \dots \times U}_{g}$$ such that

$$\ell(W + g(P) - (Q_1) - \dots - (Q_{2g-1})) = 0$$

for all $(Q_1, \dots, Q_g) \in U''$

$$\|$$

$$\ell(W + g(P) - (Q_1) - \dots - (Q_{2g}))$$

$$\underset{R-R}{\Longrightarrow} \ell(((Q_1) + \dots + (Q_g) - g(P)) + ((Q_{g+1}) + \dots + (Q_{2g}) - g(P)) + g(P))$$

$$= \ell(Q_1 + \dots + Q_{2g} - g(P))$$

$$= g + 1 - g + 0 = 1$$

Let U' be the image of U'' in $U^{(g)} \times U^{(g)}$.

$\square$

" $\square$ "

Last time, we constructed rational maps

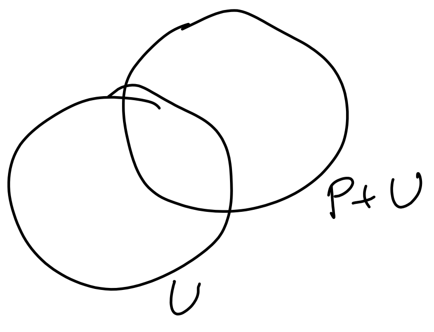
$$C^{(g)} \times C^{(g)} \dashrightarrow C^{(g)} \text{ and } C^{(g)} \dashrightarrow C^{(g)}$$

corr. to the group operations in $\mathcal{Cl}^0(C)$.

These rat. maps satisfy the group axioms.

It turns out that there is then an (actual) group variety J birational to $C^{(g)}$ such that the group op. on J agree with the group op. on $C^{(g)}$ (wherever defined).

(This is first constructed as an abstract variety by affine charts which are translates of suff. small dense open subsets of $C^{(g)}$.)



One can then show that J is a complete variety, and hence an abelian variety.

By Thm 3.3.7, the rat. map

$C^{(g)} \dashrightarrow J$ can be extended to a morphism $\varphi: C^{(g)} \longrightarrow J$.

By Cor 3.3.12, the composition

$$C \times \dots \times C \xrightarrow[\pi]{} C^{(g)} \xrightarrow[\varphi]{} J$$

is of the form

$$\varphi(\pi(Q_1, \dots, Q_g)) = \tilde{\varphi}_1(Q_1) + \dots + \tilde{\varphi}_g(Q_g) + R$$

for some morphisms $\tilde{\varphi}_1, \dots, \tilde{\varphi}_g : C \longrightarrow J$ and some point $R \in J(K)$.

Because it factors through $C^{(g)}$, we in fact have $\tilde{\varphi}_1 = \dots = \tilde{\varphi}_g =: \tilde{\varphi}$.

("$\tilde{\varphi}(Q) = Q - P$ in $Cl^0(C)$").

, - - -

<u>Thm 3.5.2</u> Let C be a sm. proj. curve over K (of genus $g \geq 1$), $P \in C(K)$. Then, there is a g-dimensional abelian variety J over K (called the <u>Jacobian</u> variety of C) and an injective morphism $\rho : C \longrightarrow J$ over K such that for all field ext. $L|K$, we obtain a map

$$\mathrm{Div}(C_L) \longrightarrow J(L),$$
$$\sum_P n_P[P] \longmapsto \sum_P n_P\, \rho(P)$$

which gives rise to an isomorphism

$$\mathcal{C}\ell^0(C_L) \xrightarrow{\sim} J(L) \text{ of groups.}$$

Furthermore, for any morphism $\alpha: C \to A$ into an abelian var., there is a unique hom. $\beta: J \to A$ of abelian var. and a unique point $R \in A(k)$ such that $\alpha(Q) = \beta(\rho(Q)) + R$ for all $Q \in \bar{k}$.

$$\begin{tikzcd} C \arrow[r, "\rho"] \arrow[dr, "\alpha"'] & J \arrow[d, dashed, "\beta"] \\ & A \end{tikzcd}$$

("The Jacobian var. J is the smallest abelian var. containing C.")

<u>Eg</u> If C is an ell. curve, $J = C$.

3.6. Hyperelliptic curves

Reference: Stoll, Arithmetic of Hyperelliptic Curves (Lecture notes from his webpage)

Def A hyperell. curve is a sm. proj. curve C such that there is a degree 2 map $\pi: C \to \mathbb{P}^1_K$.

Ex Ell. curves are hyperell.

Rmk By R-H, π is ramified at exactly $2g_C + 2$ points.

Rmk By R-R (as for ell. curves), there is a squarefree homogeneous degree $2g+2$ pol. $f(X, Z) \in K[X, Z]$ such that C is covered by the affine var.

$$U_1 = \{(x,y) \in \mathbb{A}^2_K \mid y^2 = f(x,1)\} \text{ and}$$

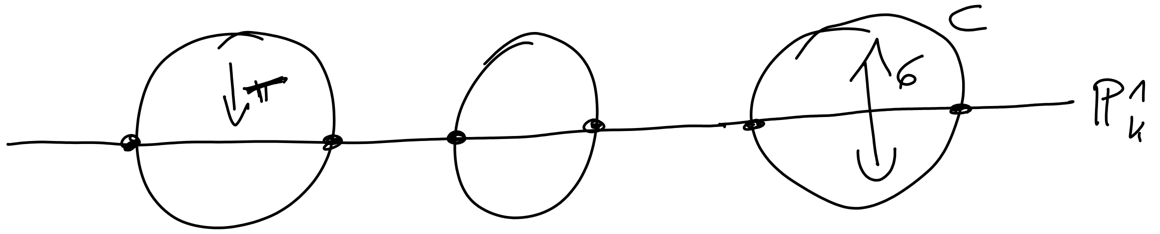
$$U_2 = \{(z,y) \in \mathbb{A}^2_K \mid y^2 = f(1,z)\}$$

with transition map

$$f(1, \tfrac{1}{x}) = \frac{1}{x^{2g+2}} f(x,1)$$

$$U_1 \cap \{x \neq 0\} \xrightarrow{\sim} U_2 \cap \{z \neq 0\}$$

$$(x,y) \longmapsto \left(\frac{1}{x}, \frac{1}{x^{g+1}} \cdot y\right)$$



and the morphism $\pi : C \to \mathbb{P}^1_k$ is given by $\pi : C \to \mathbb{P}^1_k$ is given by

$$U_1 \to \mathbb{P}^1 \qquad \text{and } U_2 \to \mathbb{P}^1 .$$
$$(x,y) \mapsto [x:1] \qquad (z,y) \mapsto [1:z]$$

The ramification points of π are the points with $y=0$. (corr. to the $2g+2$ roots of f in $\mathbb{P}^1$)

We have an automorphism $\sigma : C \to C$ sending $(x,y) \mapsto (x,-y)$ and $(z,y) \mapsto (z,-y)$ called the <u>hyperelliptic involution</u>.

We write $\sigma(P) = \overline{P}$.

<u>Remk</u> C can be described as the subvariety

$$\{[x:y:z] \in \mathbb{P}^{1,g+1,1}_k \mid y^2 = f(x,z)\}$$

of the <u>weighted</u> <u>projective space</u>

$$\mathbb{P}_k^{1,g+1,1} = k^3 \Big/ \{(\lambda^1, \lambda^{g+1}, \lambda^1) \mid \lambda \in k^\times\}$$

$$\begin{array}{ccc} & & [a : b^{g+1} : c] \\ \cong & & \uparrow \\ \mathbb{P}_k^2 / G, & & [a:b:c] \end{array}$$

where $G = \mu_{g+1} \subset k^\times$ (group of $(g+1)$-th roots of unity)

acts on $\mathbb{P}_k^2$ by $v \cdot [a:b:c] = [a:vb:c]$

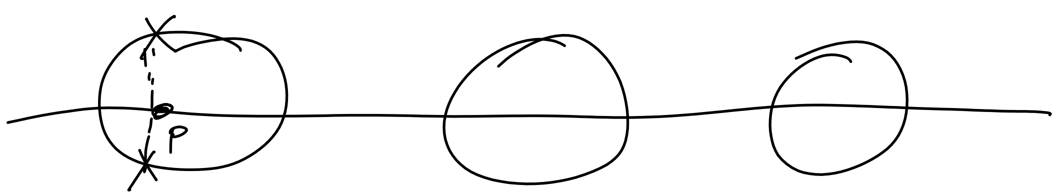
<u>Ex</u> Some examples of principal divisors:

1) Let h be a rat. fct. on $\mathbb{P}_k^1$,

$$\mathrm{div}(h) = \sum_{P \in \mathbb{P}_k^1} n_P P.$$

Then, $\mathrm{div}(h \circ \pi) = \pi^*(\mathrm{div}(h))$

$$= \sum_{P = [x:z] \in \mathbb{P}_k^1} n_P \Big([x : \sqrt{f(x,z)} : z] + [x : -\sqrt{f(x,z)} : z] \Big)$$



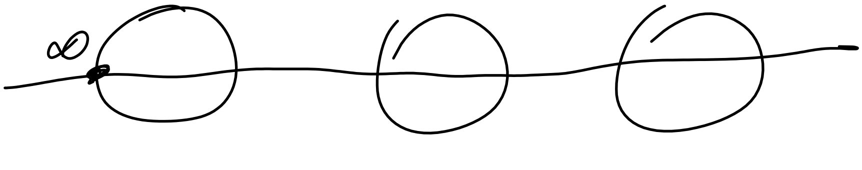
2) $\operatorname{div}\Bigg(\underbrace{\frac{y}{z^{g+1}}}_{\substack{\text{well-def.}\\ \text{rat. map}\\ \text{on } \mathbb{P}^{1,g+1,1}\\ \text{and therefore on } C}}\Bigg) = \sum_{\substack{[x:z]\in\mathbb{P}^1\\ f(x,z)=0}} [x:0:z] - (g+1)\Big([1:\sqrt{f(1,0)}:0] + [1:-\sqrt{f(1,0)}:0]\Big)$

Remark 3.6.1 Let $P \in C(K)$ and let $D \in \mathrm{Div}^0(C)$.

Then, $\ell(D+nP) = 1$ for some $0 \leq n \leq g$ by R–R. $\Rightarrow$ We obtain a divisor $D' \geq 0$ of degree n in the same divisor class as $D+nP$.

Now, assume $P \in C(K)$ is a ramification point. After a lin. transf. of $\mathbb{P}^1$, we can assume that $\pi(P) = [1:0]$, so $P = [1:0:0]$.
($\rightsquigarrow f(x,z)$ is divisible by z)

This point is denoted by $\infty = [1:0:0]$.



Def Assume $\infty \in C(K)$. A divisor $D \geq 0$ on C is in general position if

we don't have $D \geq [\infty]$ and

we don't have $D \geq [P] + [\bar{P}]$ for any $P \in C(\bar{K})$.

Thm 3.6.2 We have a bijection

$$\{D \geq 0 \text{ in general pos.} \mid \deg(D) \leq g\} \xrightarrow{\sim} \mathcal{U}^0(C)$$
$$D \longmapsto D - \deg(D) \cdot [\infty].$$

Pf existence: Using ~~Rmk~~ 3.5.1, for any divisor D' of degree 0, pick the smallest $0 \leq n \leq g$ s.t. the divisor class $D' + n \cdot [\infty]$ contains a divisor $D \geq 0$.

Then, D is in general position:

If $D \geq [\infty]$, then $D - [\infty] \geq 0$ which lies in the same div. cl. as $D' + (n-1) \cdot [\infty]$. $\mathcal{E}$

If $D \geq [P] + [\bar{P}]$, then $D - [P] - [\bar{P}] \geq 0$, which lies in the same div. cl. as $D - 2 \cdot [\infty]$ and therefore $D' + (n-2) \cdot [\infty]$. (see ex. 1)

$\Rightarrow$ D is in general position

<u>uniqueness</u>: Assume $D_1, D_2 \geq 0$ are in general position and $D_1 - n_1[\infty]$ lies in the same div. class as $D_2 - n_2[\infty]$, where $n_i = \deg(D_i)$.

By exe 1, $D_1 + \overline{D_1} - 2n_1[\infty]$ is a principal divisor.

$\Rightarrow 0 \leq D_2 + \overline{D_1}$ lies in the same div. cl. as $(n_1 + n_2)\cdot[\infty]$.

$$\Rightarrow \quad D_2 + \overline{D_1} - (n_1 + n_2)\cdot[\infty] = \operatorname{div}(h)$$

with $h \in L((n_1+n_2)\cdot[\infty])$.

$$L((n_1+n_2)\cdot[\infty]) \underset{n_1, n_2 \leq g}{\subseteq} L(2g\cdot[\infty])$$

By R-R, $\ell(2g\cdot[\infty]) = g+1$.
But $1, \frac{x}{z}, \ldots, \left(\frac{x}{z}\right)^g$ are lin. indep. el. of $L(2g\cdot[\infty])$, so in fact

$$L(2g\cdot[\infty]) = \langle 1, \tfrac{x}{z}, \ldots, \left(\tfrac{x}{z}\right)^{g+1} \rangle.$$

$\Rightarrow$ Any el. h of $L((n_1+n_2)\cdot[\infty])$ is of the form $h = \tilde{h} \circ \pi$ for some rat. ~~fct~~. $\tilde{h}$ on $\mathbb{P}^1_K$.

By ex. 1, $\underset{\substack{\| \\ D_2 + \overline{D}_1 - (n_1+n_2)[\infty]}}{\mathrm{div}(h)} = E + \overline{E}$ for some divisor E on C.

Since D_2, $\overline{D}_1$ are in general pos., this can only happen if $D_1 = D_2$.

$\square$

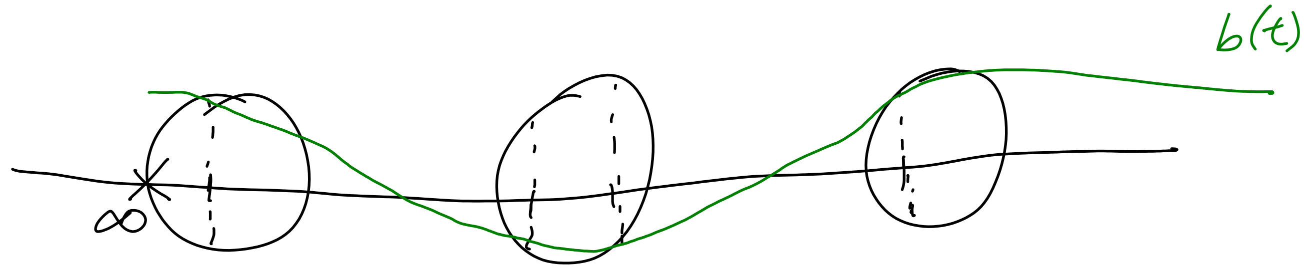
Thm 3.6.3 (Mumford representation)

For any $n \geq 0$, we have a bijection

$$\{D \geq 0 \text{ in gen. pos.} \mid \deg(D) = n\}$$

$$\longleftrightarrow \{(a,b) \mid a, b \in K[X],$$
$$a \text{ monic of degree } n,$$
$$b \text{ has degree} < n,$$
$$\underbrace{f(X,1)}_{\text{pol. of deg } 2g+1} \equiv b(X)^2 \bmod a(X)\}$$

$$\sum_{\substack{t \in \overline{K} \\ \text{root of } a}} \underbrace{v_t(a)}_{\text{mult. of } (x-t) \text{ in } a} \cdot [t : b(t) : 1] \longleftarrow\!\shortmid (a,b)$$



Rmks • The cond. $f(X,1) \equiv b(X)^2 \bmod a(X)$ ensures that $[t:b(t):1]$ lies on C for all roots t of a.

• The cond. $\deg(b)<n$ is there simply because reducing b mod a doesn't change the LHS.

Pf To construct the inverse map, consider $D = \sum_i m_i [P_i]$ where $m_i \geq 1$, $P_i = [x_i : y_i : 1] \in C$

Let $a(X) = \prod_i (X - x_i)^{m_i}$.

and $b(X)$ such that $b(x_i) = y_i$

$(\Leftrightarrow b(X) \equiv y_i \bmod X - x_i)$

and $b(X)^2 \equiv f(X,1) \bmod (X - x_i)^{m_i}$.

(We know that there is a pol. $b(X) \equiv y_i \bmod X - x_i$ such that $b(x)^2 \equiv f(x,1) \bmod X - x_i$, namely, $b(X) = y_i$.

Apply Hensel's Lemma, using that $m_i = 1$ if $y_i = 0$.) $\square$

Remark A If $D = D_1 + D_2$ is in gen. pos., D_1 corr. to (a_1, b_1), D_2 corr. to (a_2, b_2), $\gcd(a_1, a_2) = 1$, then D corr. to (a, b) with $a = a_1 a_2$, $b \equiv b_1 \bmod a_1$, $b \equiv b_2 \bmod a_2$.

(See Thm 4.18 in Stoll for a general formula.)

Remark B Let D be in gen. pos. corr. to (a,b), $\deg(D) > g$. Write $f(x,1) - b(x)^2 = \lambda\, a(x)\tilde{a}(x)$ with $\lambda \in K^\times$, $\tilde{a} \in K(x)$ monic (of degree $< \deg(a)$).

Let $\tilde{b} \equiv -b \bmod \tilde{a}$, $\deg(\tilde{b}) < \deg(\tilde{a})$.

$\Rightarrow (\tilde{a}, \tilde{b})$ corr. to a divisor $\tilde{D}$ in gen. pos. with $\deg(\tilde{D}) < \deg(D)$ such that $D - \deg(D)\cdot(\infty)$ lies in the same div. cl. as $\tilde{D} - \deg(\tilde{D})\cdot(\infty)$.

Applying Rmk A and repeatedly Rmk B produces a "formula" for adding divisor classes in the Mumford representation.

3.7. Outlook

Rmk Any abelian variety A can be embedded into some projective space. (see Milne)

Idea of pf Find a morphism $\varphi : A \longrightarrow \mathbb{P}^n$ which restricts to an embedding on some dense open subset U of A.

Let $A = \bigcup_{i=1}^{m} (P_i + U)$ with $P_1, \dots, P_m \in A$.

$\leadsto$ Embedding

$$A \hookrightarrow \underbrace{\mathbb{P}^n \times \dots \times \mathbb{P}^n}_{m} \xhookrightarrow{\text{Segre}} \mathbb{P}^{(n+1)m-1}$$

$$Q \longmapsto (\varphi(Q-P_1), \dots, \varphi(Q-P_m))$$

"$\square$"

We hence obtain a "nice" theory of heights on abelian varieties (as on elliptic curves).

We obtain a canonical height, which is again a nondegenerate quadratic form.

The Mordell–Weil Theorem holds:

$A(K)$ is finitely generated for any number field K.

<u>Warning</u> For ell. curves E_1, E_2 and an isogeny $\phi : E_1 \to E_2$, we defined its dual $\hat{\phi} : E_2 \cong \mathcal{C}\ell^0(E_2) \longrightarrow \mathcal{C}\ell^0(E_1) \cong E_1$.

But for general ab. var., there is no natural bij. $A \cong \mathcal{C}\ell^0(A)$.

To fix this, we need to look at a subgroup $\mathrm{Pic}(A)$ of $\mathcal{C}\ell^0(A)$.

We then obtain a <u>dual ab. variety</u>

$\hat{A} \cong \mathrm{Pic}(A)$.

For an isogeny $\phi : A_1 \to A_2$, we obtain a dual isogeny $\hat{\phi} : \hat{A}_2 \to \hat{A}_1$.

$\Rightarrow$ For any $\varphi : A \hookrightarrow \mathbb{P}^n$,

$$\#\{P \in A(\mathbb{Q}) \mid h(\varphi(P)) \le T\} \sim T^{r/2} \quad \text{(I)}$$

for $T \to \infty$

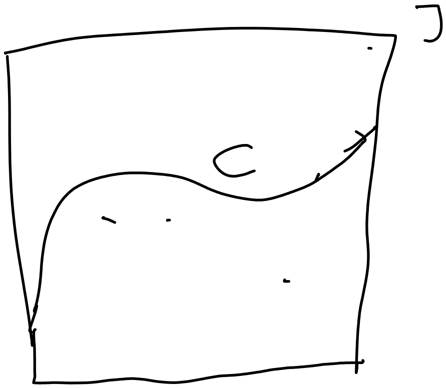
logarithmic height

<u>Cor</u> For any sm. proj. curve $C \subseteq \mathbb{P}^m_{\mathbb{Q}}$ of genus $g \geq 1$,

$$\#\{P \in C(\mathbb{Q}) \mid h(P) \le T\} \ll T^{r/2} \text{ for } T \to \infty,$$

where r is the rank of the Jacobian.

<u>Pf</u> Apply (I) to the images of pts under the embedding $C \hookrightarrow J$.



<u>Faltings's Thm</u> If $g \geq 2$, then $\#C(\mathbb{Q}) < \infty$.

Heuristic argument

Embed $C \hookrightarrow J \hookrightarrow \mathbb{P}^n$.

$$\underset{\text{1-dim.}}{C} \hookrightarrow \underset{\text{g-dim.}}{J} \hookrightarrow \mathbb{P}^n$$

Let $f \in \mathbb{Z}[X_0, \dots, X_n]$ be hom of deg d

with $f \in I_{\mathbb{P}^n}(C) \setminus I_{\mathbb{P}^n}(J)$.

A "random" point $(x_0, \dots, x_n) \in \mathbb{Z}^n$ with $\log|x_0|, \dots, \log|x_n| \le T$ perhaps satisfies $f(x_0, \dots, x_n) = 0$ with prob. $\sim e^{-dT}$.

$\rightsquigarrow$ expect about

$$< \sum_{T \geq 0} T^{r/2-1} \cdot e^{-dT} < \infty$$

points in $J(\mathbb{Q}) \cap C$. "$\square$"

(The actual proofs use Diophantine Approximation.)