<u>Def</u> Assume ~~∞~~ $\infty \in C(K)$. A divisor $D \geq 0$ on C is <u>in general position</u> if

we don't have $D \geq [\infty]$ and

we don't have $D \geq [P] + [\bar{P}]$ for any $P \in C(\bar{K})$.

<u>Thm 3.6.2</u> We have a bijection

$$\{D \geq 0 \text{ in general pos.} \mid \deg(D) \leq g\} \xrightarrow{\sim} \mathcal{U}^0(C)$$
$$D \longmapsto D - \deg(D) \cdot [\infty].$$

<u>Pf</u> <u>existence</u>: 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 $(n_1+n_2)\cdot[\infty]$.

$$\Rightarrow \quad D_2 + \overline{D_1} - (n_1+n_2)\cdot[\infty] = \mathrm{div}(h)$$

with $h \in L((n_1+n_2)\cdot[\infty])$.

$$L((n_1+n_2)\cdot[\infty]) \underset{\substack{\uparrow \\ n_1, n_2 \leq g}}{\subseteq} L(2g\cdot[\infty])$$

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, $\underset{\substack{\parallel \\ D_2 + \overline{D}_1 - (n_1+n_2)[\infty]}}{\mathrm{div}(h)} = E + \overline{E}$ for some divisor E on C.

Since D_2, $\overline{D}_1$ are in general pos., this can only happen if $D_1 = D_2$.

$\square$

<u>Thm 3.6.3</u> (Mumford representation)

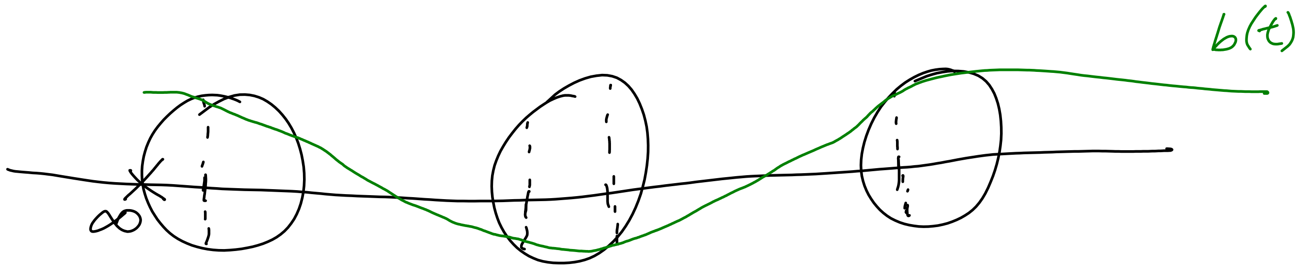
For any $n \geq 0$, we have a bijection

$$\{D \geq 0 \text{ in gen. pos.} \mid \deg(D) = n\}$$

$$\longleftrightarrow \{(a,b) \mid a, b \in K[X],$$
$$a \text{ monic of degree } n,$$
$$b \text{ has degree } < n,$$
$$\underbrace{f(X,1)}_{\text{pol. of deg } 2g+1} \equiv b(X)^2 \bmod a(X)\}$$

mult. of $(x-t)$ in a

$$\sum_{\substack{t \in \overline{K} \\ \text{root of } a}} v_t(a) \cdot [t : b(t) : 1] \longleftarrow\!\shortmid (a,b)$$



<u>Rmks</u> • 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.

<u>Pf</u> 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 $y_i = 0$.) $\square$

<u>Remark A</u> 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.)

<u>Remark B</u> 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 Remk A and repeatedly Remk B produces a "formula" for adding divisor classes in the Mumford representation.

3.7. Outlook

Remk 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 $P_1, \dots, P_m \in A$.

$\rightsquigarrow$ 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 $\hat{\phi}: E_2 \cong Cl^0(E_2) \longrightarrow Cl^0(E_1) \cong E_1$.

But for general ab. var., there is no natural bij. $A \cong Cl^0(A)$.

To fix this, we need to look at a subgroup $Pic(A)$ of $Cl^0(A)$.

We then obtain a <u>dual ab. variety</u>

$\hat{A} \cong Pic(A)$.

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 $\varphi : A \hookrightarrow \mathbb{P}^n$,

$$\#\{P \in A(\mathbb{Q}) \mid h(\varphi(P)) \leq T\} \sim T^{r/2} \quad \text{for } T \to \infty \qquad (\mathrm{I})$$

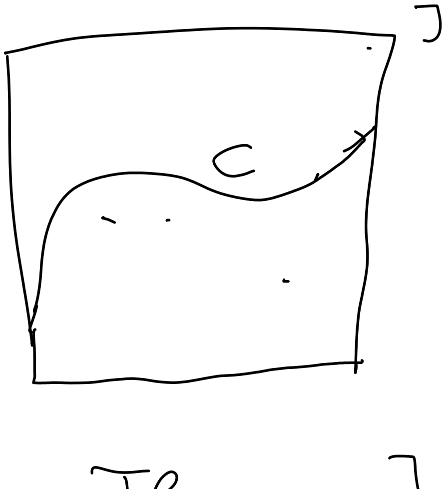
logarithmic height

<u>Cor</u> For any sm. proj. curve $C \subseteq \mathbb{P}^m_{\mathbb{Q}}$ of genus $g \geq 1$,

$$\#\{P \in C(\mathbb{Q}) \mid h(P) \leq T\} \ll T^{r/2} \quad \text{for } T \to \infty,$$

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 $\underset{\text{1-dim.}}{C} \hookrightarrow \underset{\text{g-dim.}}{J} \hookrightarrow \mathbb{P}^n$.

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 $\log|x_0|, \dots, \log|x_n| \leq T$ 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.)