Last time, we constructed rational maps

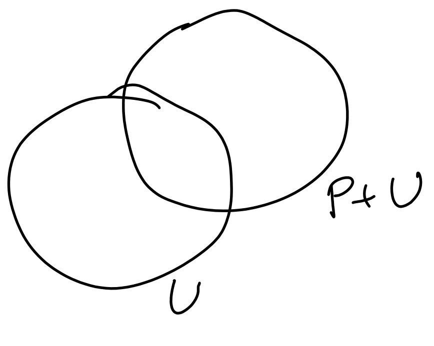
$$C^{(g)} \times C^{(g)} \dashrightarrow C^{(g)} \text{ and } C^{(g)} \dashrightarrow C^{(g)}$$

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 $\tilde{\varphi}_1, \dots, \tilde{\varphi}_g : C \to J$ 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~~ an injective morphism $\iota : C \longrightarrow J$ 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

$$\mathcal{Cl}^\circ(C_L) \xrightarrow{\sim} J(L) \text{ of groups.}$$

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.")

Eg 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.

$$U_1 = \{(x,y) \in \mathbb{A}^2_k \mid y^2 = f(x,1)\} \text{ and}$$

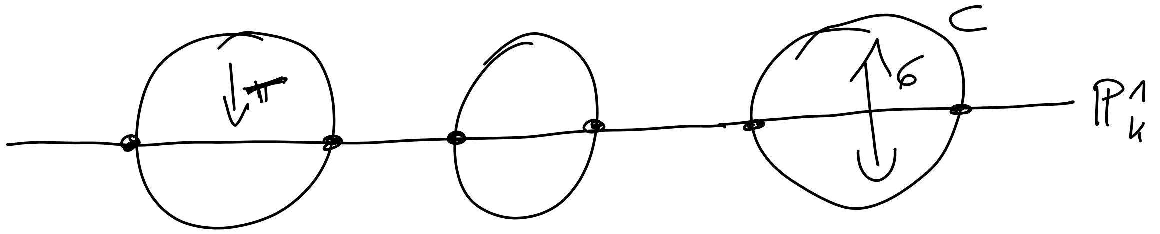
$$U_2 = \{(z,y) \in \mathbb{A}^2_k \mid y^2 = f(1,z)\}$$

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>Rmk</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 projective space</u>.

$$\mathbb{P}_k^{1,g+1,1} = k^3 / \{(\lambda^1, \lambda^{g+1}, \lambda^1) \mid \lambda \in k^\times\}$$

$$\cong \qquad [a : b^{g+1} : c]$$

$$\mathbb{P}^2_k / G, \qquad [a:b:c] \mapsto [a : b^{g+1} : c]$$

where $G = \mu_{g+1} \subset k^\times$ (group of $(g+1)$-th roots of unity)

acts on $\mathbb{P}^2_k$ by $v \cdot [a:b:c] = [a : vb : c]$

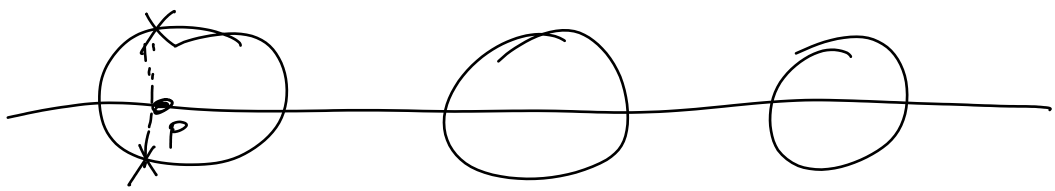
<u>Ex</u> Some examples of principal divisors:

1) Let h be a rat. fct. on $\mathbb{P}^1_k$,

$$\operatorname{div}(h) = \sum_{P \in \mathbb{P}^1_k} n_P P.$$

Then, $\operatorname{div}(h \circ \pi) = \pi^*(\operatorname{div}(h))$

$$= \sum_{P = [x:z] \in \mathbb{P}^1_k} n_P \left([x : \sqrt{f(x,z)} : z] + [x : -\sqrt{f(x,z)} : z] \right)$$



2) $$\operatorname{div}\Big(\underbrace{\frac{y}{z^{g+1}}}\Big) = \sum_{\substack{[x:z]\in\mathbb{P}^1 \\ f(x,z)=0}} [x:0:z] - (g+1)\Big([1:\sqrt{f(1,0)}:0] + [1:-\sqrt{f(1,0)}:0]\Big)$$

well-def.
rat. map
on $\mathbb{P}^{1,g+1,1}$
$\curvearrowright$
and therefore on C

Remark 3.6.1 Let $P \in C(K)$ and let $D \in \mathrm{Div}^0(C)$.
Then, $\ell(D+nP) = 1$ for some $0 \le n \le g$ by R–R. $\Rightarrow$ We obtain a divisor $D' \ge 0$ 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 $P = [1:0:0]$.
(so $f(x,z)$ is divisible by z)
This point is denoted by $\infty = [1:0:0]$.