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.

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

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

□

Cor (Riemann-Hurwitz)

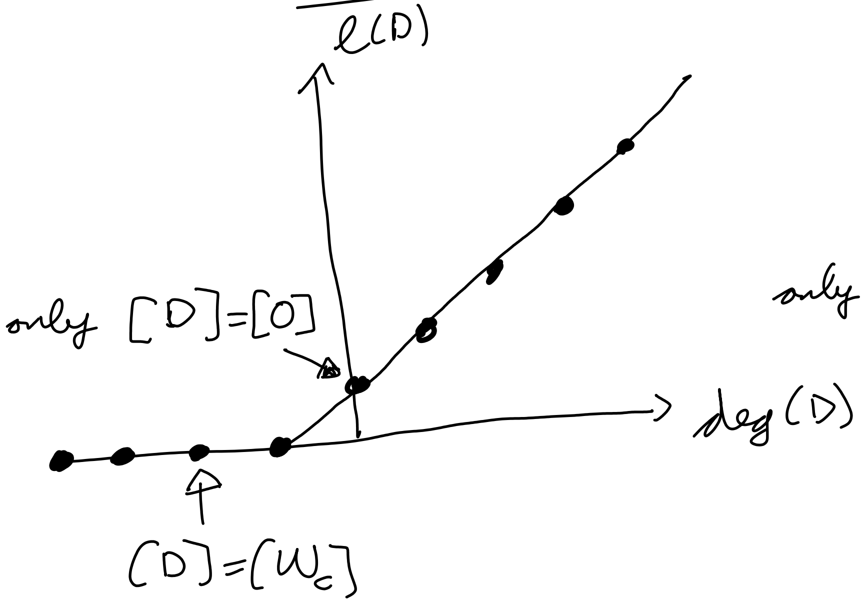
$$2g_C - 2 = \deg(f)\cdot(2g_{C'} - 2) + \deg(R_f).$$

Pf Take degrees of both sides of (I). □

Summary

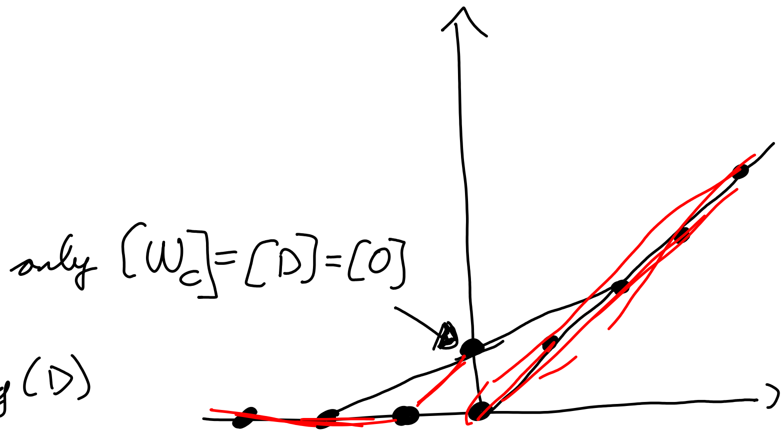
$S = \{(\deg(D), \ell(D)) \mid D \in \mathrm{Div}(C)\}$ is a subset of the set of dots in the following pictures:

$g_C = 0$

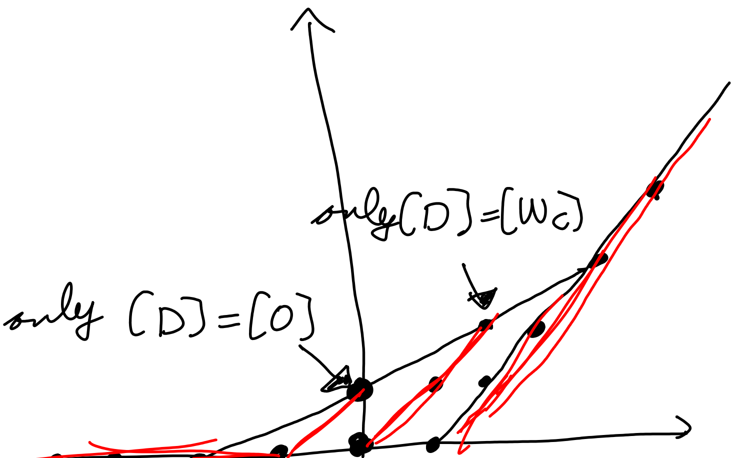


$\Rightarrow \ell\ell^0(C) = 0$

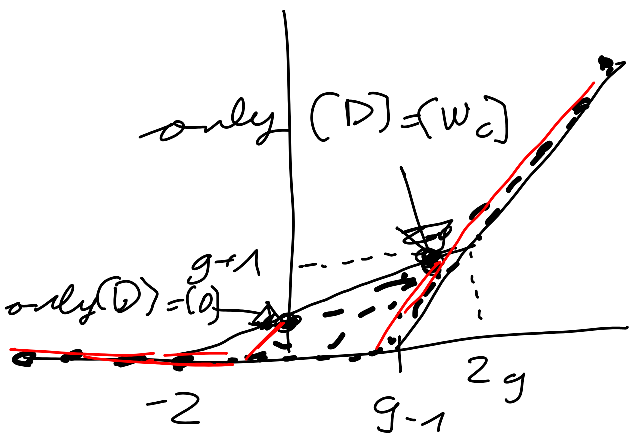
$g_C = 1$



$g_C = 2$



$g_C > 2$



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

$$E(K) \longleftrightarrow \mathrm{Cl}^0(E)$$
$$P \longmapsto [P] - [O]$$

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

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

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

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

$\Rightarrow P = Q$

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 $\mathrm{Cl}(E)$. $\square$

$\rightsquigarrow$ 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

$$\{[X:Y:Z] \mid Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 X Z^2 + a_6 Z^3\}$$

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

$$\begin{array}{ccc} L([O]) & L(2[O]) & L(3[O]) \\ \| & \| & \| \\ \langle 1 \rangle & \langle 1, f \rangle & \langle 1, f, g \rangle \\ \dim = 1 & \dim = 2 & \dim = 3 \end{array}$$

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 $=1$.

$\Rightarrow \varphi(E) \subseteq \{[x:y:z] \mid y^2 z + \ldots = \ldots\}$

as in the statement of the theorem.

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

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

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

$$\varphi(E) = \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}.$$

Then, we get the affine chart

$$\varphi(E) \cap \{z \neq 0\} \mathrel{\hat{=}} \{(x,y) \in \mathbb{A}^2_k \mid y^2 = x^3 + a_4 x + a_6\}$$

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>).