

1 Rational Functions on Hyperelliptics

The goal of this chapter is to look at rational functions on the curve $y^2 = C(x)$ and to develop a reasonable notion of the order of a function in a point on the curve. We then give some basic properties for this order function before we introduce divisors and proceed to look at functions with a specified number of poles at infinity as a final preparation for the proof of associativity on **J**. xxx

1.1 Function Field and Order of Rational Functions

Definition 1: Define the ring of rational functions on the curve as

$$\mathcal{F} = K(x)[y] / (y^2 - C(x)).$$

As $y^2 - C(x)$ is irreducible in $K(x)[y]$, this is a field and $\mathcal{F} = K(x) + K(x)y$, so write elements $f \in \mathcal{F}$ as $f = g + hy$ where $g, h \in K(x)$. Define $\bar{f} = g - hy$.

We will occasionally write things like $K[x, y] \subset \mathcal{F}$ but xxx we always implicitly mean this in conjunction with $y^2 = C(x)$.

~

We now wish to define the order of a function f in a point \mathcal{Q} , $\text{ord}_{\mathcal{Q}}(f) \in \mathbb{Z}$ for $f \in \mathcal{F}^*$ and $\mathcal{Q} \in H(\bar{K})$. To this end we first construct a K -homomorphism

$$\lambda_{\mathcal{Q}} : \mathcal{F} \rightarrow \bar{K}((t))$$

with the intent of defining $\text{ord}_{\mathcal{Q}}(f) = \text{ord } \lambda_{\mathcal{Q}}(f)$.

Reminder: If τ is a formal Laurent series of the form $\tau = 1 + \sum_{i=1}^{\infty} a_i t^i$ then it has a unique squareroot of the form $\sigma = 1 + \sum_{i=1}^{\infty} b_i t^i$ meaning $\sigma^2 = \tau$. Write $\sigma = \sqrt{\tau} = 1 + \dots$

From now on we will use an ellipsis to denote terms of ascending order everywhere where we are not interested in the specifics.

Definition 2: Because $C(\lambda_{\mathcal{Q}}(x)) = (\lambda_{\mathcal{Q}}(y))^2$ has to be fulfilled, we first decide on $\lambda_{\mathcal{Q}}(x)$ and deduce $\lambda_{\mathcal{Q}}(y)$. For this, we distinguish between three cases for $\mathcal{Q} \in H(\bar{K})$:

1. Let $\mathcal{Q} = (x_0, y_0) \in H_0(\bar{K})$ with $y_0 \neq 0$ and consequently $C(x_0) \neq 0$.

Define $\lambda_Q(x) = x_0 + t$. Now

$$\begin{aligned} C(\lambda_Q(x)) &= C(x_0 + t) \\ &= C(x_0) + \dots + t^5 \\ &= C(x_0)(1 + \dots) \\ &= y_0^2 \tau_1 \quad \text{with } \tau_1 \in K((t)). \end{aligned}$$

Define $\lambda_Q(y) = y_0 \sigma_1$ where $\sigma_1 = \sqrt{\tau_1}$.

2. Let $Q = (x_0, y_0) \in H_0(\overline{K})$ with $y_0 = 0$. Note that $C(x_0) = 0$ and write $C(x) = \prod_{i=1}^5 (x - \alpha_i)$ for $\alpha_i \in \overline{K}$ and for instance $\alpha_1 = x_0$.

Define $\lambda_Q(x) = x_0 + t^2$. Now

$$\begin{aligned} C(\lambda_Q(x)) &= t^2 \prod_{i=2}^5 (x_0 - \alpha_i + t^2) \\ &= \mu t^2 (1 + \dots) \end{aligned}$$

with $\mu \in \overline{K}$ being $\prod_{i=2}^5 (x_0 - \alpha_i) = C'(x_0)$ which is non-zero because our curve is non-singular. Write therefore $C(\lambda_Q(x)) = \mu t^2 \tau_2$ with $\tau_2 = 1 + \dots$ and define $\lambda_Q(y) = \nu t \sigma_2$ with $\sigma_2 = \sqrt{\tau_2}$ and $\nu^2 = \mu$.

3. Let $Q = \infty$. Define $\lambda_Q(x) = \frac{1}{t^2}$. It follows that

$$\begin{aligned} C\left(\frac{1}{t^2}\right) &= \frac{1}{t^{10}} + \frac{a}{t^8} + \frac{b}{t^6} + \frac{c}{t^4} + \frac{d}{t^2} + e \\ &= \frac{1}{t^{10}} (1 + \dots) \end{aligned}$$

So define $\lambda_Q(y) = \frac{1}{t^5} \sigma_3$ with the notation $\sigma_3 = \sqrt{\tau_3}$ as before.

Definition 3: For $Q \in H(\overline{K})$ and $f \in \mathcal{F}^*$ define $\text{ord}_Q(f) = \text{ord } \lambda_Q(f)$.

Lemma 1: Let $f \in K[x, y] \subset \mathcal{F}$, $f \neq 0$ and $Q \in H_0(\overline{K})$, $Q = (x_0, y_0)$. Then

- (a) $\text{ord}_Q f \geq 0$ and
- (b) if $f(Q) = 0$ then $\text{ord}_Q f \geq 1$.

Proof.

- (a) Because $Q \in H_0(\overline{K})$ we have $\lambda_Q(x), \lambda_Q(y) \in \overline{K}[[t]]$ and with $f \in K[x, y]$ we have $\text{ord}_Q(f) \geq 0$.
- (b) Write $f = A(x, y)$, $A(X, Y) \in K[X, Y]$. First, let $y_0 \neq 0$.

$$\begin{aligned} \text{ord}_Q f &= \text{ord } A(\lambda_Q(x), \lambda_Q(y)) \\ &= \text{ord } A(x_0 + t, y_0 \sigma_1). \end{aligned}$$

But $A(x_0 + t, y_0\sigma_1) = \sum_{i=0}^{\infty} a_i t^i$ so with $t = 0$ we get $A(x_0, y_0) = a_0$ but the former is $f(\mathcal{Q})$ which is 0, so $a_0 = 0$ and the claim follows.

If $y_0 = 0$ we would have $\text{ord}_{\mathcal{Q}} f = \text{ord} A(x_0 + t^2, \sqrt{\mu}t\sigma_2)$ instead. But like before, this means $0 = f(\mathcal{Q}) = A(x_0, 0) = a_0$ so again $\text{ord}_{\mathcal{Q}}(f) \geq 1$.

□

Lemma 2: Let $f \in K(x)$, $f \neq 0$, $\mathcal{Q} \in H(\overline{K})$. Then

- (a) $\text{ord}_{\mathcal{Q}}(f) = \text{ord}_{x_0} f(x)$ if $\mathcal{Q} = (x_0, y_0) \in H_0(\overline{K})$ with $y_0 \neq 0$.
- (b) $\text{ord}_{\mathcal{Q}}(f) = 2\text{ord}_{x_0} f(x)$ if $\mathcal{Q} = (x_0, 0) \in H_0(\overline{K})$.
- (c) $\text{ord}_{\infty}(f) = 2\text{ord}_0 f(\frac{1}{x}) = 2\text{ord}_{\infty} f(x)$.

Note that the righthand sides of the equalities refer to the usual definition of the order of a rational function in a point $x_0 \in \overline{K} \cup \{\infty\}$. We renamed the infinity in order to avoid a clash of notations.

Proof. First take $f \in K[x]$ and define $e = \text{ord}_{x_0} f \in \mathbb{N}$ so $f = (x - x_0)^e g(x)$ with $g \in \overline{K}[x]$ and $g(x_0) \neq 0$.

- (a) If $\mathcal{Q} = (x_0, y_0)$, $y_0 \neq 0$ then $\lambda_{\mathcal{Q}}(f) = f(x_0 + t) = t^e g(x_0 + t)$ and so $\text{ord} \lambda_{\mathcal{Q}}(f) = e$ because $g(x_0 + t) = g(x_0) + \dots$ with $g(x_0) \neq 0$.
- (b) Here $\lambda_{\mathcal{Q}}(f) = f(x_0 + t^2) = t^{2e} g(x_0 + t^2)$ and again $g(x_0 + t^2) = g(x_0) + \dots$ so $\text{ord} \lambda_{\mathcal{Q}}(f) = 2e$.
- (c) For $\mathcal{Q} = \infty$ we have $\lambda_{\mathcal{Q}}(f) = f(\frac{1}{t^2}) = \frac{\alpha}{t^{2d}} + \dots$ with $\alpha \neq 0$ if $d = \deg f$. Obviously, $\text{ord}_0 f(\frac{1}{x}) = \text{ord}_0 \frac{\alpha + \dots}{x^d} = -d$ so $\text{ord} \lambda_{\mathcal{Q}}(f) = 2\text{ord}_0 f(\frac{1}{x})$.

Generally, if $f \in K(x)$ we can write $f = \frac{p}{q}$ for $p, q \in K[x]$ and we apply the above to p and q , subtracting $\text{ord}_{\mathcal{Q}} q$ from $\text{ord}_{\mathcal{Q}} p$. □

Lemma 3: For $f \in \mathcal{F}^*$ and $\mathcal{Q} \in H(\overline{K})$ the order satisfies $\text{ord}_{\mathcal{Q}}(\overline{f}) = \text{ord}_{\overline{\mathcal{Q}}}(\overline{f})$

Proof.

1. For $\mathcal{Q} \in H_0(\overline{K})$ with $y_0 \neq 0$ we've got $\lambda_{\mathcal{Q}}(x) = x_0 + t$ and $\lambda_{\mathcal{Q}}(y) = y_0 \sqrt{\tau}$. Therefore $\lambda_{\overline{\mathcal{Q}}}(x) = x_0 + t = \lambda_{\mathcal{Q}}(\overline{x})$ and $\lambda_{\overline{\mathcal{Q}}}(y) = -y_0 \sqrt{\tau} = \lambda_{\mathcal{Q}}(\overline{y})$ so

$$\begin{aligned} \lambda_{\overline{\mathcal{Q}}}(f(x, y)) &= f(\lambda_{\overline{\mathcal{Q}}}(x), \lambda_{\overline{\mathcal{Q}}}(y)) \\ &= \lambda_{\mathcal{Q}}(f(\overline{x}, \overline{y})) \\ &= \lambda_{\mathcal{Q}}(\overline{f}(x, y)). \end{aligned}$$

2. If $\mathcal{Q} \in H_0(\overline{K})$ with $y_0 = 0$ then $\overline{\mathcal{Q}} = \mathcal{Q}$. Write $f = g(x) + h(x)y$ so

$$\lambda_{\mathcal{Q}}(\overline{f}) = g(x_0 + t^2) - h(x_0 + t^2)\nu t \sqrt{\tau}.$$

Calling this $l(t) = \lambda_Q(\bar{f})$ and looking at the construction of λ_Q we see that τ sports only even powers of t so we see above that $l(-t) = \lambda_Q(f)$. As interchanging t with $-t$ doesn't change the order, we're done.

3. For $Q = \infty$, $\tau = 1 + at^2 + bt^4 + ct^6 + dt^8 + et^{10}$ features only even powers as well, so again $l(-t) = \lambda_Q(f)$ for $l(t) = \lambda_Q(\bar{f}) = g(\frac{1}{t^2}) - h(\frac{1}{t^2})\frac{1}{t^5}\sqrt{\tau}$. Finally, $\lambda_Q(f)$ is equal to $\lambda_{\bar{Q}}(f)$ since $\infty = \overline{\infty}$. Again $\text{ord} l(t) = \text{ord} l(-t)$.

□

Lemma 4: If $f \in \mathcal{F}^*$ then the set $\{Q \in H(\bar{K}) \mid \text{ord}_Q f \neq 0\}$ is finite and

$$\sum_{Q \in H(\bar{K})} \text{ord}_Q f = 0.$$

Proof. First take $f \in K[x, y]$, $f \neq 0$ and let $Q = (x_0, y_0) \in H_0(\bar{K})$ with $\text{ord}_Q f \neq 0$. By Lemma 1 (a) we know that $\text{ord}_Q f \geq 1$. It follows that $\text{ord}_Q(f\bar{f}) = \text{ord}_Q f + \text{ord}_Q \bar{f} \geq 1$. Now since $f = g + hy$, $f\bar{f} = g^2 - h^2 C(x)$ which lies in $K[x]$, so by Lemma 2 we have $\text{ord}_{x_0}(f\bar{f}) > 0$. But there are only finitely many such x_0 and so only finitely many $y_0 = \pm\sqrt{C(x_0)}$.

For $f \in K(x, y)$, $f = \frac{f_1}{f_2}$, $f_1, f_2 \in K[x, y]$ we have $\text{ord}_{x_0} f = \text{ord}_{x_0} f_1 - \text{ord}_{x_0} f_2$ so there are also only finitely many x_0 for which this differs from zero.

For the second claim, give a name to our sum

$$s(f) = \sum_{Q \in H(\bar{K})} \text{ord}_Q f$$

and note that $s(f) = s(\bar{f})$ due to Lemma 3 and the fact that we take the sum over all Q . Because $\text{ord}_Q(f\bar{f}) = \text{ord}_Q(f) + \text{ord}_Q(\bar{f})$ we can see that

$$s(f\bar{f}) = s(f) + s(\bar{f}) = 2s(f).$$

But because $f\bar{f} \in K(x)$ we can use Lemma 2 to write this out as

$$\begin{aligned} 2s(f) &= \sum_{Q \in H(\bar{K})} \text{ord}_Q f\bar{f} \\ &= 2 \sum_{\substack{x_0 \neq \infty \\ x_0 \neq \alpha_i}} \text{ord}_{x_0} f\bar{f} + 2 \sum_{x_0 = \alpha_i} \text{ord}_{x_0} f\bar{f} + 2 \sum_{x_0 = \infty} \text{ord}_{x_0} f\bar{f} \\ &= 2 \sum_{x_0 \in \bar{K} \cup \{\infty\}} \text{ord}_{x_0} f\bar{f}. \end{aligned}$$

Here α_i are the points on which $C(x)$ vanishes and since

$$\sum_{x_0 \in \overline{K} \cup \{\infty\}} \text{ord}_{x_0} g = 0$$

for any $g \in K(x)$ we have $2s(f) = 0$ meaning $s(f) = 0$ in \mathbb{Z} . \square

1.2 Divisors and Lemmas

Definition 4: The divisor of a function $f \in \mathcal{F}$ is the formal sum

$$(f) = \sum_{\mathcal{Q} \in H(\overline{K})} \text{ord}_{\mathcal{Q}} f \cdot \mathcal{Q}$$

where the empty sum is written $(f) = 0$ in case $f = 0$. Thanks to Lemma 4 the sum is finite and the sum of coefficients is 0.

Points $\mathcal{Q} \in H(\overline{K})$ with a positive coefficient in (f) are called zeroes of f while those with a negative coefficient are called poles.

Lemma 5: If $f \in \mathcal{F}^*$ has no poles then f is constant.

Proof. With $f = g + hy$, $\text{ord}_{\mathcal{Q}} f \geq 0$ for every $\mathcal{Q} \in H(\overline{K})$ we take a look at $f + \bar{f} = 2g \in K(x)$ and $f\bar{f} = g^2 - h^2C \in K(x)$ and observe that

$$\begin{aligned} \text{ord}_{\mathcal{Q}}(f + \bar{f}) &\geq \min\{\text{ord}_{\mathcal{Q}} f, \text{ord}_{\mathcal{Q}} \bar{f}\} \\ &= \min\{\text{ord}_{\mathcal{Q}} f, \text{ord}_{\overline{\mathcal{Q}}} f\} \geq 0. \end{aligned}$$

with Lemma 3 and similarly

$$\text{ord}_{\mathcal{Q}}(f\bar{f}) = \text{ord}_{\mathcal{Q}} f + \text{ord}_{\overline{\mathcal{Q}}} f \geq 0.$$

Both are greater than zero because f has no poles and with the help of Lemma 2 we conclude that $\text{ord}_{x_0}(f + \bar{f}) \geq 0$ and $\text{ord}_{x_0}(f\bar{f}) \geq 0$ respectively.

But in $\overline{K}(x)$, a function q with $\text{ord}_{x_0} q \geq 0$ for every $x_0 \in \overline{K} \cup \{\infty\}$ must be constant, so both $f + \bar{f}$ and $f\bar{f}$ are constant functions. Since f is a root of $(T - f)(T - \bar{f}) = T^2 - (f + \bar{f})T + f\bar{f}$ which lies in $\overline{K}[T]$, f lies in \overline{K} . \square

Lemma 6: Suppose $f \in \mathcal{F}^*$ has at most one pole at ∞ i.e. $\text{ord}_{\infty} f \geq -1$ and none for any other $\mathcal{Q} \in H_0(\overline{K})$ so $\text{ord}_{\mathcal{Q}} f \geq 0$. Then f is a constant.

Proof. With $f = g + hy$ such that $\text{ord}_{\mathcal{Q}} f \geq 0$ for every $\mathcal{Q} \in H_0(\overline{K})$ and $\text{ord}_{\infty} f = -1$ we can write $\lambda_{\infty}(f) = \frac{\alpha}{t} + \dots$ with $\alpha \in \overline{K}$. Since we are only

Now remember that $\lambda_\infty(x) = \frac{1}{t^2}$ so $\lambda_\infty(x - f^2) = \frac{\beta}{t} + \dots$, $\beta \in \overline{K}$ and finally we have a regular power series $\lambda_\infty(x - f^2 - \beta f)$ so

$$\text{ord}_\infty(x - f^2 - \beta f) \geq 0$$

and for any other $\mathcal{Q} \in H_0(\overline{K})$ we have

$$\text{ord}_\mathcal{Q}(x - f^2 - \beta f) \geq \min\{\text{ord}_\mathcal{Q}(x), \text{ord}_\mathcal{Q}(f^2), \text{ord}_\mathcal{Q}f\}$$

which is positive by virtue of the prerequisite on f and $\lambda_\mathcal{Q}(x) = x_0 + \dots$. The previous Lemma now implies $x - f^2 - \beta f \in \overline{K}$ so we see $x = f^2 + \beta f$ as a polynomial $x = X(f)$ with $X(T) \in \overline{K}[T]$.

Do the same thing with $\lambda_\mathcal{Q}(y) = \frac{1}{t^5}\sqrt{\tau} = \frac{1}{t^5} + \dots$ so

$$\begin{aligned}\lambda_\mathcal{Q}(y - f^5) &= \frac{\gamma}{t^4} + \dots, \\ \lambda_\mathcal{Q}(y - f^5 - \gamma f^4) &= \frac{\delta}{t^3} + \dots\end{aligned}$$

so finally $\lambda_\mathcal{Q}(y - f^3 - \gamma f^2 - \delta f)$ is a power series again and must actually be in \overline{K} . Like before, $y = f^3 + \gamma f^2 + \delta f = Y(f)$ with $Y(T) \in \overline{K}[T]$.

Combined we have $Y(f)^2 = C(X(f))$ but K is algebraically closed, so either $f \in \overline{K}$ or $Y(T)^2 = C(X(T))$. The latter can't be true since xxx proves/says $X, Y \in \overline{K}$ but both are of degree strictly higher than one. \square

Lemma 7: If $f \in \mathcal{F}^*$ has at most two poles at ∞ then f is of the form $f = \alpha + \beta x$ with $\alpha, \beta \in K$.

Proof. \square

Lemma 8: If $f \in \mathcal{F}^*$ has at most three poles at ∞ then f is of the form $f = \alpha + \beta x$ with $\alpha, \beta \in K$.

Proof. \square

Lemma 9: If $f \in \mathcal{F}^*$ has at most four poles at ∞ then f is of the form $f = \alpha + \beta x + \gamma x^2$ with $\alpha, \beta, \gamma \in K$.

Proof. \square

Minilemma 1: If f is such that $\lambda_\infty(f) = \gamma t^e + \dots$ then $\lambda_\infty(\overline{f}) = -\gamma t^e + \dots$

Proof. Let $\lambda_\infty(\bar{f}) = \tilde{\gamma}t^e + \dots$. Since $f + \bar{f} = 2p$ and $\text{ord}_\infty(p)$ is always even for $p \in K(x)$, we must have $(\gamma + \tilde{\gamma})t^{-3} + \dots = \sigma t^{-2} + \dots$ so $\gamma = -\tilde{\gamma}$. \square

Lemma 2: Let $f \in \mathcal{F}^*$ with $(f) = \frac{***}{3_\infty}$. Then $f = \alpha + \beta x$.

Proof. Let $f = p + qy$ with $p, q \in K(t)$. We have $\lambda_\infty(f + \bar{f}) = \sigma t^{-2} + \dots$ so $p = \frac{1}{2}(f + \bar{f}) = \alpha + \beta x$.

Now, consider $f - \bar{f} = 2qy$. We get $\lambda_\infty(f - \bar{f}) = 2\lambda_\infty(q)t^{-5}\sqrt{\tau} = 2\gamma t^{-3} + \dots$ and since $\sqrt{\tau}$ is a series of the form $1 + \dots$ we must have $\lambda_\infty(q) = \gamma t^2 + \dots$

Suppose $q \neq 0$, this implies $\frac{1}{q} = \tilde{\delta} + \tilde{\epsilon}x$. Rewriting to accomodate for $q = 0$ gives $q = \frac{\epsilon}{x - \delta}$ with $\delta, \epsilon \in K$ as well so

$$f = \alpha + \beta x + \frac{\epsilon}{x - \delta}y$$

However, now $\lambda_\mathcal{Q}(f) = \alpha + \beta(t^2 + \delta) + \epsilon\sqrt{\mu}\frac{t\sqrt{\tau}}{t^2}$ for $\mathcal{Q} = (\delta, 0)$ which is equal to $\epsilon\sqrt{\mu}t^{-1} + \dots$. If $\epsilon \neq 0$ (μ is non zero anyway) this means that \mathcal{Q} is a new (true) pole for f which contradicts $(f) = \frac{***}{3_\infty}$, so q must be 0. \square

Lemma 3: Let $f \in \mathcal{F}^*$ with $(f) = \frac{****}{4_\infty}$. Then $f = \alpha + \beta x + \gamma x^2$.

Proof. (different function f): With $\lambda_\infty(f) = \gamma t^{-4} + \dots$ so $\lambda_\infty(f - \gamma x^2)$ being of the form $\sigma t^{-3} + \dots$ we fall into the case above and the claim follows. \square
