Recall

$E/k$ an e.c.

$f(x,y) \in k[E]$

$$f(x,y) = v(x) + y\,w(x)$$

in canonical form

Def $\deg(f) = \max\{2 \cdot \deg_x(v),\ 3 + 2 \cdot \deg_x(w)\}$

$$\begin{pmatrix} \deg y = 3 \\ \deg x = 2 \end{pmatrix}$$

Def: $N_f = f \cdot \bar{f} \in k[x]$

$$\bar{f}(x,y) = v(x) - y\,w(x)$$

Lemma: Let $E/k = E_{A,B}$ an e.c.

and $s_E(x) = x^3 + Ax + B$.

For $f, g \in k[E]$:

(1) $\deg(f) = \deg_x(N_f)$

(2) $\deg(f \cdot g) = \deg f + \deg g$.

Proof: (1) Write $f$ in canonical

form: $f(x,y) = v(x) + y\,w(x)$.

Then $N_f(x) = v(x)^2 - s_E(x)\,w(x)^2$.

Since $\deg_x(v^2)$ and $\deg_x(w^2)$

are even and $\deg_x(s_E)$

is odd,

$$\deg_x(N_f) = \max\{\deg(v^2), \deg(s)+\deg w^2\}$$

$$= \max\{2\cdot\deg v, 3+2\cdot\deg w\}$$

$$= \deg(f). \quad \text{exercise}$$

(2) $\deg(f\cdot g) = \deg_x(N_{fg}) \overset{\checkmark}{=} \deg_x(N_f\cdot N_g)$

$$= \deg(N_f) + \deg(N_g)$$

$$\overset{(1)}{=} \deg(f) + \deg(g). \quad //$$

Recall: $r \in \overline{k}(E)$

$\longleftrightarrow$ $r : E(\overline{k}) \longrightarrow \mathbb{P}^1$

$P \in E(\overline{k})$ is called

zero of $r$ if $r(P) = 0$

and a pole of $r$ if

$r(P) = \infty$.

Want: define & study multiplicity of zeros and poles.

Goal:

To sketch (Abel-Jacobi):

→ Theorem

With the appropriate notion of multiplicity, two rational functions $r, s \in \mathbb{k}(E)$ that the same set of zeros and of pole, with the same multiplicity, differ by a constant, ie

$\exists\, \lambda \in \mathbb{k}$ s.th

$$r = \lambda \cdot s.$$

---

$$\mathbb{k}(E) := \left\{ r(x,y) = \frac{f(x,y)}{g(x,y)} \right|$$

$y^2 = x^3 + Ax + B$

$\varphi = y^2 - x^3 - Ax - B$

$f, g \in k[E], g \neq 0 \}$

$\frac{f}{g} = \frac{f'}{g'}$ $(=)$ $k[x,y]/(\varphi)$

$f \cdot g' = f' \cdot g$ in $k[E]$

$r \in k(E) \rightsquigarrow r : E(k) \to \mathbb{P}^1$

---

To define multiplicity of zero/pole $P$ of $r \in k(E)$

Consider first the one variable case.

$k(x) = \left\{ r(x) = \frac{f(x)}{g(x)} \;\middle|\; \begin{matrix} f, g \\ \in k[x] \\ g \neq 0 \end{matrix} \right.$

Say $r = \frac{f}{g}$ and $\gcd(f,g) = 1$,

if $x_0$ is a zero of $r$

then $f(x_0) = 0 \wedge g(x_0) \neq 0$

so $\exists\, n$ s.th

$$(x - x_0)^n \mid f(x)$$

and $$(x - x_0)^{n+1} \nmid f(x).$$

We set $mult_r(x_0) = n$.

If $x_0$ is a pole of $r$

then $g(x_0) = 0$

so $\exists\, n$ s.th

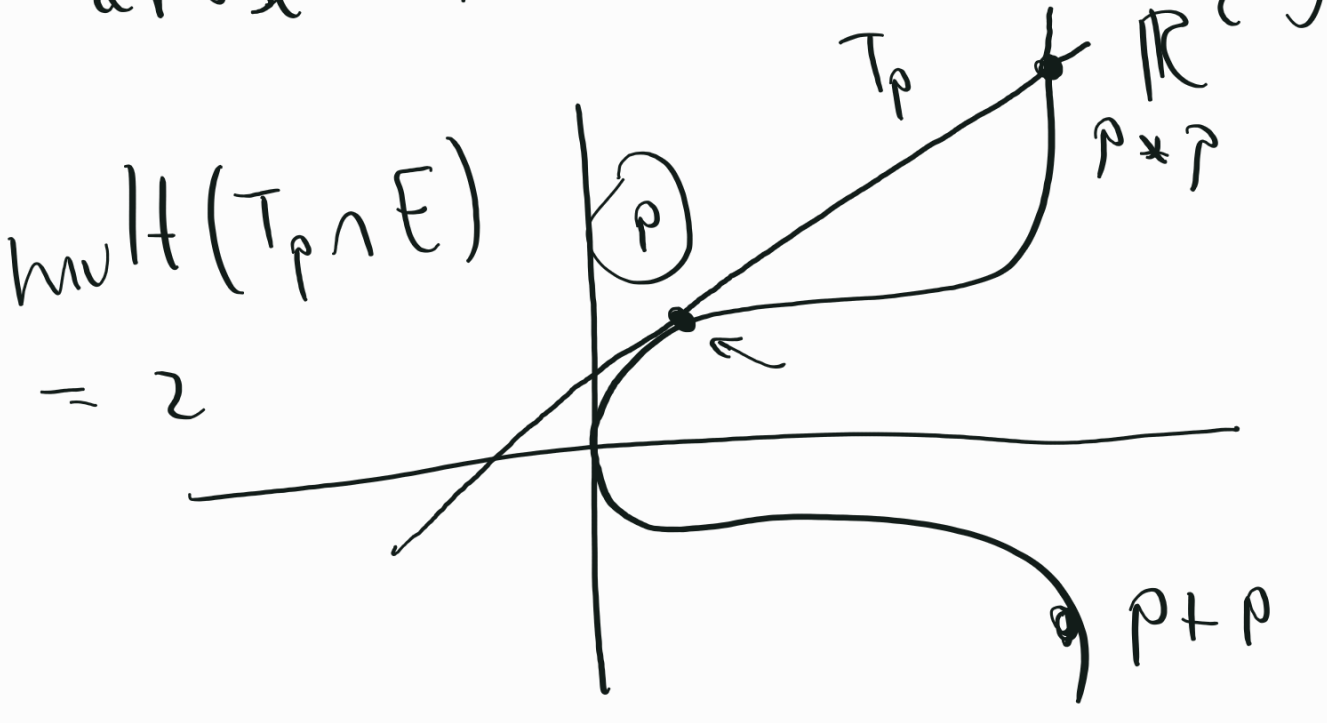
$$(x - x_0)^n \mid g(x)$$

but $(x - x_0)^{n+1} \nmid g(x)$

$\Rightarrow \quad mult_r(x_0) = -n.$

---

For $Ik(E)$ a hint for a notion of multiplicity, arose in the following




$$r(x,y) = \frac{f(x,y)}{g(x,y)}$$

$P \in E(\mathbb{k})$ is a zero

and $g(P) \neq 0$

ie $f(P) = 0$

$C_f : f(x,y) = 0$

$mult_P(r) = mult(E \cap C_f)$

---

If $(x_0, y_0)$ is a root

of $f(x,y)$ $\not\Rightarrow$

$f = g \cdot h$ for

some $g, h \in \mathbb{k}[x,y]$

**Def**: Let $E/\Bbbk = E_{A,B}$ be an e.c., and $P \in E(\Bbbk)$.
A rational function $u_P = u \in \Bbbk(E)$ is called **a uniformizer at $P$** if:

→ (1) $u(P) = 0$

(2) $\forall\, r \in \Bbbk(E)\setminus\{0\}$, $\exists\, d \in \mathbb{Z}$ and $\exists\, s \in \Bbbk(E)$ w/ $s(P) \neq 0, \infty$ s.th

$$r = u^{(d)} \cdot s.$$

**Remark**: if $r(P) \neq 0, \infty$ take $d = 0$ $\forall\, u \neq 0 \in \Bbbk(E)$

$$r = u^d \cdot s$$

$$s = r$$

---

If uniformizers exist for all $P \in E(k)$ then given $r \in k(E)$ and zero/pole $P$ of $r$, write $r = u_P^d \cdot s$ where $u_P \in k(E)$ and $s \in k(E)$ w/ $s(P) \neq 0, \infty$

---

Proposition: Let $E/k = E_{A,B}$ be an e.c., and

$P = (a,b) \in E(\bar{k})$ a finite point w $2P \neq O$.

Then the rational function

$\rightarrow \boxed{u_P(x,y) = x - a} \in \bar{k}(E)$

is a uniformizer at $P$.

Proof: First note that $u_P(P) = 0$.

Now let $r \in \bar{k}(E) \setminus \{0\}$ be arbitrary. If $r(P) \neq 0, \infty$ we are done: $r = u^0 \cdot r$

w/ $s = r$ $(\Rightarrow s(P) \neq 0, \infty)$.

Suppose $\rightarrow \boxed{r(P) = 0}$. Note that if we proved that $u_P$

is a uniformizer in this case, we are done:

If $r(\mathfrak{P}) = \infty$ then

$$\frac{1}{r}(\mathfrak{P}) = 0 \quad \text{and}$$

then $\frac{1}{r} = u^d \cdot s$

w/ $s(\mathfrak{P}) \neq 0, \infty$.

and then

$$r = u^{-d} \cdot \frac{1}{s}$$

and $\frac{1}{s}(\mathfrak{P}) \neq 0, \infty$

---

So assume $r(\mathfrak{P}) = 0$.

and write $r = \frac{f}{g}$ w/

$f(\underline{P}) = 0 \quad \forall\, g(\underline{P}) \neq 0.$

Set $s_0(x,y) = f(x,y)$ and inductively repeat the following process while $s_i(P) = 0$:

Write $s_i(x,y) = v_i(x) + y\, w_i(x)$.

and distinguish 2 cases:

(1) $\underline{\overline{s_i}(\underline{P}) = 0}$ : because $2\underline{P} \neq 0$

$(P = (a,b)) \Rightarrow b \neq 0$

hence the system

$$\begin{cases} s_i(P) = 0 \\ \overline{s_i}(P) = 0 \end{cases} \begin{cases} v_i(a) + b\, w_i(a) = 0 \\ v_i(a) - b\, w_i(a) = 0 \end{cases}$$

has a solution when

$$\boxed{V_i(a) = W_i(a) = 0.}$$

Thus

$$S_i(x,y) = V_i(x) + y\,W_i(x)$$

$$= (x-a)\,V_{i+1}(x) + y\,(x-a)\,W_{i+1}(x)$$

for some $V_{i+1}, W_{i+1} \in k[x]$.

Refine

$$S_{i+1}(x) = V_{i+1}(x) + y\,W_{i+1}(x).$$

(2) $\overline{S_i}(P) \neq 0$ : multiply $S_i$ by $1 = \dfrac{\overline{S_i}}{\overline{S_i}}$

$$S_i(x,y) = \frac{N_{S_i}(x)}{\overline{S_i}(x,y)}$$

how $s_i(P) = 0$ and $\overline{s}_i(P) \neq 0$

$\Rightarrow N_{s_i}(a) = 0.$

So write

$$N_{s_i}(x) = \boxed{(x-a)}\, n(x)$$

for some $n(x) \in k[x]$.

Now set

$$s_{i+1}(x,y) = \frac{n(x)}{\overline{s}_i(x,y)}$$

Then $s_{i+1}(P) \neq \infty$

and

$$S_i(x,y) = (x-a) \cdot S_{i+1}(x)$$

---

$$S_0 \quad S_1 \quad S_2 \quad - - -$$

If the process terminates

say at $S_{i-1}$ ( $S_i(p) \neq 0$ )

set $d = i$

$$f(x,y) = (x-a)^i \cdot S_i(p)$$

and $S_i(p) \neq 0, \infty$

and we will be done:

$$r = \frac{f}{g} \qquad (d = i)$$

$$r(x,y) = (x-a)^i \cdot s(x,y)$$

$$\frac{f(x,y)}{g(x,y)}$$

$$r = u^i \cdot \frac{s}{g}$$

where $\frac{s}{g}(\underline{r}) \neq 0, \infty$

Finally, lets show that the process terminates:

$$N_f(x) = N_{u^i \cdot s_i}(x)$$

$$= \left( (x-a)^i \cdot v_i(x) \right)^2 -$$

$$y^2 \left( (x-a)^i w_i(x) \right)^2$$

$$= (x-a)^{2i} \cdot \left( v_i(x)^2 - y^2 w_i(x)^2 \right)$$

$$= (x-a)^{2i} \cdot N_{s_i}(x).$$

so

$$\deg(N_f) = 2i + \deg(s_i) \geq 2i$$

so $2i$ cannot exceed $\deg(N_f)$

$\Rightarrow$ process terminates. //