Recall

Def: Let $E/\mathbb{k}$ be an e.c.

and fix $P \in E(\mathbb{k})$.

A uniformizer for P is

a rational function $u_P = u$

s.th $\forall\ r \in \mathbb{k}(E) \setminus \{0\}$,

$\exists\ s \in \mathbb{k}(E)$ and $d \in \mathbb{Z}$

s.th $r = u^d \cdot s \in \mathbb{k}(E)$

and 1) $u(P) = 0$

2) $s(P) \neq 0, \infty$.

Note: If $r(P) \neq 0, \infty$ then

$r = u^0 \cdot r$

$\forall u$, $f = u^{\cdots}$

We prove existence of uniformizers for 3 classes of points in $E(\mathbb{k})$

1) finite pts that are not of order 2.

2) finite pts that are of order 2.

3) pt at ∞. (O)

Proposition: Let $E/\mathbb{k}$ be an e.c. and $P = (a,b) \in E(\mathbb{k}) \setminus \{O\}$ s.th $2P \neq O$. Then the rational function $u_P = u(x,y) = x - a$ is a uniformizer at P.

Proof: Note: $u(P) = 0$.

Now let $r \in \Bbbk(E) \setminus \{0\}$

If $r(P) \neq 0, \infty$, then take

$s = r$ and $r = u^0 \cdot s$.

Next, it is enough to show that

u is a uniformizer in case

$r(P) = 0$: if now $r(P) = \infty$

then $\frac{1}{r}(P) = 0$ and we

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

for some $d \in \mathbb{Z}$ and $s \in \Bbbk(E)$

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

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

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

Suppose $\underline{\underline{r(P) = 0}}$. We can write

$r = \frac{f}{g}$ w/ $\boxed{f(P) = 0}$, $g(P) \neq 0$

If can present f as

$$\boxed{f = u^d \cdot s}$$

w/ $s(P) \neq 0, \infty$

then we are done, since

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

and $\frac{s}{g}(P) \neq 0, \infty$.

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

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

and distinguish two cases:

1) $\underline{\bar{s}_i(P) = 0}$:

Since $2P \neq 0$, $y(P) = b \neq 0$

Thus the system

$$\begin{cases} v_i(a) + b w_i(a) = 0 & s_i(P) = 0 \\ v_i(a) - b w_i(a) = 0 & \bar{s}_i(P) = 0 \end{cases}$$

has a solution

$$\Longrightarrow \underline{\underline{v_i(a) = w_i(a) = 0.}}$$

Thus

$$s_i(x,y) = v_i(x) + y w_i(x)$$

$$= (x-a)\, v_{i+1}(x) + y\,(x-a)\, w_{i+1}(x)$$

$$= \underbrace{(x-a)}_{u} \cdot \underbrace{\left(v_{i+1}(x) + y\, w_{i+1}(x) \right)}_{\substack{!! \\ s_{i+1}}}$$

$$\Rightarrow \quad \boxed{s_i = u \cdot s_{i+1}}$$

2) $\underline{\bar{s}_i(P) \neq 0}$:

$$* \quad s_i\Big|_P = \frac{s_i \bar{s}_i}{\bar{s}_i}\Big|_P = \frac{N_{s_i}}{\bar{s}_i}\Big|_P$$

Now $s_i(P) = 0$ and $\bar{s}_i(P) \neq 0$

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

Thus

$$N_{s_i}(x) = (x - a) \cdot h(x)$$

for some $h(x) \in \mathbb{k}[x]$

Then set

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

and again

$$s_i = u \cdot s_{i+1}$$

If the process terminates at iteration i, ie $s_i(P) \neq 0$

then $\underline{\underline{f}} = s_0 = u \cdot s_1 =$

$$= \ldots = \underline{\underline{u^i s_i}}$$

$$\underline{\underline{s_i}}(P) \neq \underline{\underline{0}}, \underline{\underline{\infty}}$$

Finally to see why the process terminates:

$\forall i \quad f = u^i \cdot s_i$

$u^i s_i = \underline{\underline{u^i \left(v_i(x) + y\, w_i(x) \right)}}$

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

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

$$= (x-a)^{2i} \left(V_i(x)^2 - y^2 W_i(x)^2 \right)$$

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

We see that i is bounded since

$$\deg f = 2i + \deg N_{s_i}$$

$$\Rightarrow \quad i < \deg f - \deg N_{s_i}$$

This completes the proof. //

<u>Proposition</u>: Let $E/\mathbb{k}$ an e.c

w/ $\quad E: y^2 = \underbrace{x^3 + Ax + B}_{S_E(x)}$.

Let $P \in \underline{\underline{E(\mathbb{k})}} \setminus \{O\}$ be s.th

$2P = O$. Then

$$u_P = u(x,y) = y \in \mathbb{k}(E)$$

is a uniformizer at P.

<u>Proof</u>: First over $\overline{\mathbb{k}}$,

$$s_E(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

w/ $\alpha_1, \alpha_2, \alpha_3$ distinct.

Since $2P = O$, $P = (\alpha_1, 0)$ (wlog) ie $\alpha_1 \in \mathbb{k}$.

$$\boxed{\frac{s_E(x)}{x-\alpha_1} = \sigma(x) \in \mathbb{k}[x]}$$

(although α_2, α_3 might only be in $\overline{\mathbb{k}}$)

Let $r \in \mathbb{k}(E) \setminus \{0\}$ s.th

$r(P) = 0$. Then $\exists$ a

presentation $r = \frac{\,}{g}$ s.t.

$$f(P) = 0 \wedge g(P) \neq 0.$$

Focusing on f, write $\boxed{P = (\alpha_1, 0)}$

$$f(x,y)\big|_P = v(x) + y\,W(x)\big|_P$$

w/ $v(\alpha_1) = 0$

Thus, $v(x) = (x - \alpha_1)\, v_1(x)$

w/ $\deg v_1 < \deg v$.

Then

$$f(x,y) = \left[(x - \alpha_1)\, v_1(x) + y\,W(x)\right] \frac{\sigma(x)}{\sigma(x)}$$

$$= \frac{s_E(x)\, v_1(x) + y\,\sigma(x)\, W(x)}{\sigma(x)}$$

$W(x) \cdot \sigma(x)$

Set $\quad w_1(x) = \underline{\underline{w(x)\ \sigma(x)}}$

$$= \frac{y^2\, v_1(x) + y\, w_1(x)}{\sigma(x)}$$

$$u(x,y) \cdot \underbrace{\frac{y\, v_1(x) + w_1(x)}{\sigma(x)}}_{W(x,y).}$$

Note that $W(P) \neq \infty$

since $\sigma(\alpha_1) \neq 0$.

If $\underline{\underline{W(P) \neq 0}}$ we are done $\quad r = \frac{f}{g} = u \cdot \frac{W}{g}$

otherwise, $W(P)=0$, define $r' = W/g$

and repeat ie

$r'(P) = 0 \implies$

$$r'(x,y) = \underbrace{\frac{\left(y\,v_1(x) + w_1(x)\right)\Big|_{P=(\alpha_1,0)}}{g(x,y)\cdot \sigma(x)}}$$

$$\implies \quad w_1(\alpha_1) = 0$$

hence, $\quad w_1(x) = \underbrace{(x-\alpha_1)\,w_2(x)}$

Then

$$W(x,y) = \frac{y\,v_1(x) + w_1(x)}{\sigma(x)}$$

$$= \frac{y\,v_1(x) + (x-\alpha_1)\,\sigma(x)\cdot w_2(x)}{\sigma(x)}$$

$$= \frac{y\,v_1(x) + s_E(x)\;w_2(x)}{\sigma(x)}$$

2

$$= \frac{y\, v_1(x) + y^2\, w_2(x)}{\sigma(x)}$$

$$\Rightarrow \quad u(x,y) \underbrace{\frac{v_1(x) + y\, w_2(x)}{\sigma(x)}}_{W'}$$

As before $W'(P) \neq \infty$

and if $W'(P) \neq 0$

We are done since

$$s' = \frac{W'}{g}$$

$$\Rightarrow \quad \underline{\underline{r'}} = u \cdot s' \quad \text{w/ } s'(P) \neq 0, \infty$$

$$r = u^2 \cdot s'$$

The process terminates

since $\deg v_i < \deg v_{i-1}$

$\deg w_i < \deg w_{i-1}$

At termination, we get

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

w $s(P) \neq 0, \infty$

Finally, if P is a pole of r, then $\frac{1}{r}(P) = 0$

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

for s w/ $s(P) \neq 0, \infty$

and then

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

w/ $s^{-1}(P) \neq 0, \infty$

$w/ \quad s(1) \neq 0, \infty.$ //

<u>Proposition</u>: Let $E/\mathbb{k}$ be an e.c.

Then $u(x,y) = \frac{x}{y}$ is a uniformizer at O.

<u>Proof</u>: Since $3 = \deg y > \deg x = 2$,

$\underline{\underline{u}}(O) = \underline{\underline{0}}$.

Let $r = \frac{f}{\underline{\underline{g}}} \in \mathbb{k}(E) \setminus \{0\}$

be s.th $\underline{r(O) = 0}$ or

$\underline{r(O) = \infty}$. This means

that $\underline{\underline{d}} = \deg g - \deg f \neq 0$

We <u>would</u> like to take

$\underline{s(x,y)} = \left(\frac{y}{x}\right)^d \cdot r(x,y)$

since then

$$(*) \quad r(x,y) = \underbrace{\left(\frac{x}{y}\right)^d}_{u^d} \cdot \underbrace{\left(\frac{y}{x}\right)^d r(x,y)}_{s}$$

But we need to verify that $s(0) \neq 0, \infty$.

We have

$$s(x,y) = \frac{y^d f(x,y)}{x^d g(x,y)}.$$

$$\left(\deg(y^d \cdot f) - \deg(x^d \cdot g)\right)$$

$$= (3d + \deg f) - (2d + \deg g)$$

$$= d + (\deg f - \deg g)$$

$$= 0$$

and thus

$$s(0) \neq 0, \infty.$$

as desired. //

Next time: d is unique