Def: Let E/k and $P \in E(k)$.

A uniformizer at P is a rational function $u \in k(E)$ w/ $u(P) = 0$

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

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

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

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

---

3 cases

(i) For $P = (a, b)$ $P \in E(k) \setminus \{O\}$ w/

$2P \neq O$

$u(x, y) = x - a$

(ii) For $P = (a, 0) \in E(\mathbb{k})$

(w/ $2P = 0$)

$$u(x,y) = y.$$

(iii) For $0 \in E(\mathbb{k})$

$$u(x,y) = \frac{x}{y}.$$

Rem: uniformizer are not unique!

Proposition: Let $E/\mathbb{k}$ be an e.c. and $P \in E(\mathbb{k})$. Then

for any uniformizer $u_P = u$ at P, and $r \in \mathbb{k}(E)$,

the int $d \in \mathbb{Z}$ s.th

d

$r = u^{\cdot} \cdot s$

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

is unique.

Proof: Let $u, u' \in k(E)$ be uniformizers at P.

Then $\exists\ a, b \in \mathbb{Z}$ and $P, Q \in k(E)$ s.t.h

$$\begin{cases} u = (u')^{a} \cdot P \\ u' = u^{b} \cdot Q \end{cases}$$

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

$\Rightarrow$

$$u = (u')^{a} P = u^{ab} \cdot Q^{a} \cdot P$$

($\Rightarrow$)

$$u^{ab-1} \cdot q^a \cdot p = 1$$

If $ab \neq 1$, then evaluating at p gives $0 = 1$ ↯.

So $ab = 1 \iff a = b = -1$

$\vee$ $a = b = 1$.

If $a = b = -1$, we get

$$u = (u')^{-1} \cdot p \iff uu' = p$$

and evaluating at $p \Rightarrow 1$.

Thus $a = b = 1$.

$$(*) \begin{cases} u = u' \cdot p \\ u' = u \cdot q \end{cases}$$

Let $r \in \mathrm{Ik}(E) \setminus \{0\}$. Then $\exists d, d' \in \mathbb{Z}$

and $s, s' \in k(F)$ w/ $s(P), s'(P) \neq 0, \infty$

s.th

$$\begin{cases} r = u^d \cdot s \\ r = (u')^{d'} \cdot s' \end{cases}$$

$$\Rightarrow u^d \cdot s = (u')^{d'} \cdot s' = (uq)^{d'} \cdot s'$$

$$= u^{d'} \cdot q^{d'} \cdot s'$$

$$\Leftrightarrow \boxed{u^{d-d'} = \frac{q^{d'} \cdot s'}{s}}$$

If $d \neq d'$ we get a contradiction: evaluating at P give $LSH = 0$

$$RSS \neq 0.$$

So $d = d'$. //

Rem: (*) shows that a uniformizer is unique up to mult. by a rational function f that has no zero or pole at P.

Def: Let E/k be an e.c. and $P \in E(k)$, $r \in k(E) - \{0\}$. The multiplicity / order of r at P is

$$\mathrm{ord}_P(r) = d \in \mathbb{Z}$$

where d is the unique d in the previous proposition.

Inf

Obs: For $r \in k(E)$, a point $P \in E(k)$ satisfies $\operatorname{ord}_P(r) = 0$ iff P is neither a zero nor a pole of r.

Proof: If $\operatorname{ord}_P(r) = 0$ then for a uniformizer u we can write

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

$$\Rightarrow \quad r(P) \neq 0, \infty.$$

Conversely: If $r(P) \neq 0, \infty$ we can write ($\forall u$)

$$r = u^0 \cdot r$$

So $\operatorname{ord}_P(r) = 0$.

Example: $E/k = E_{A,B}$ and $P = (a, b) \in E(k)$ is finite and not of order 2.

Want: calculate multiplicities of zeros & poles of

$$\rightarrow \boxed{r(x,y) = x - a} = \frac{x-a}{1}$$

$\deg = 2$

Zeros: P, $-P = (a, -b)$ deg 0.

in this case $\boxed{u(x,y) = x - a = r}$ is a uniformizer.

$$r = r^1 \cdot 1$$

$$\Rightarrow \operatorname{ord}_P(r) = 1$$

$$\operatorname{ord}_{-P}(r) = 1.$$

Poles: $r(0) = \infty \quad (0 = (\infty^2, \infty^3))$

$u(x,y) = \frac{x}{y}$ is a uniformizer at 0.

Take $s(x,y) = \frac{x^3 - ax^2}{y^2}$

and get

$$u(x,y)^{-2} \cdot s(x,y) = \frac{y^2}{x^2} \cdot \frac{x^3 - ax^2}{y^2}$$

$$= x - a = r(x,y)$$

$$\Rightarrow \boxed{d = -2.}$$

Observe:

$$\sum_{P \in E(k)} \mathrm{ord}_P(r) = \mathrm{ord}_0(r) + \mathrm{ord}_{-0}(r)$$

$+ \operatorname{ord}_Q(f)$

$= 1 + 1 + -2 = 0.$

Example: Let $E/\mathbb{k} : y^2 = x^3 + Ax + B$ be an e.c. and $\mathbb{k} = \overline{\mathbb{k}}$ and

$\rightarrow$ $\boxed{f(x,y) = y \in \mathbb{k}(E).}$ $\uparrow$

Want: $\sum_{P \in E(\mathbb{k})} \operatorname{ord}_P(f)$:

Zeros: points $P \in E(\mathbb{k})$ $\nearrow$ s.t $P = (a, 0)$

$(\Leftarrow)$ $2P = \mathcal{O}$.

Write $x^3 + Ax + B = (x-a)(x-b)(x-c)$

non-zero $\{(a,0), (b,0), (c,0)\}$

pts of order 2. $= \{(a,0), (b,0), (c,0)\}$

$P_a \quad P_b \quad P_c$

$=$ $=$

What is $\operatorname{ord}_{P_a}(r)$?

$r(x,y) = u(x,y) = y$ is a uniformizer for P_a

$\Rightarrow \quad r(x,y) = u(x,y)^1 \cdot 1$

$\Rightarrow \operatorname{ord}_{P_a}(r) = 1$.

Poles: $O \in E(k)$ is a pole of $r(x,y) = y$.

To calculate $\operatorname{ord}_O(r)$

take the uniformizer

$\frac{x}{y}$

$u(x,y) = u_3(x,y) = \boxed{\frac{y}{x}}$ $\quad \frac{0}{x} = 3_0$

Take $\quad s(x,y) = \dfrac{x^3 y}{y^3}$

and get

$$u(x,y)^{-3} \cdot s(x,y) = \frac{y^3}{x^3} \cdot \frac{x^3 y}{y^3}$$

$$= y = r(x,y)$$

$$\Rightarrow \quad d = -3. \quad \operatorname{ord}_0(r) = -3$$

$$r = u^d \cdot s \qquad s(0) \neq 0, \infty$$

$$\Rightarrow \sum_{P \in E(\mathbb{k})} \operatorname{ord}_P(r) = 1+1+1 - 3 = 0.$$

Obs: In the last example,

if k is not alg. closed

and $x^3 + Ax + B$ does

not factor linearly over

k ($\Leftrightarrow$ it does not have

3 distinct roots in k)

$$\sum_{P \in E(k)} \operatorname{ord}_P(r) = -3 + 1 \neq 0$$

or $= -3 \neq 0$

Obs: In the last example

$r(x,y) = y$

Zeros

$P_a = (a,0)$, $P_b = (b,0)$

$P_c = (c,0)$

Pole

$$0 \in \Sigma(k)$$

$$\downarrow \qquad \downarrow$$

$$\mathrm{ord}_{p_a}(r) \cdot P_a +$$

$$\mathrm{ord}_{p_b}(r) \cdot P_b +$$

$$\mathrm{ord}_{p_c}(r) \cdot P_c +$$

$$\mathrm{ord}_{0}(r) \cdot O =$$

$$P_a + P_b + P_c + (-3) \cdot O$$

$$= P_a + P_b + P_c = O$$

$$\text{Claim: } P_a + P_b + P_c = O$$

Claim: $P_a + P_b + P_c = 0$

Proof: Let $E[2] = \{P_a, P_b, P_c, 0\}$

Then $E[2] \leq E(k)$

a subgp:

if $P, Q \in E[2]$

then $2(P+Q) = 2P + 2Q = 0$

$\Rightarrow P+Q \in E[2]$

and $2 \cdot (-P) = -2P = 0$

$\Rightarrow -P \in E[2]$

$E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$P_a \quad P_b \quad P_c$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{ (0,0), (1,0), (0,1), (1,1) \}$$

$$(1,0) + (0,1) + (1,1) =$$

$$(1,1) + (1,1) = (2,2)$$

$$= (0,0).$$

- In the other example

$$1 \cdot P + 1 \cdot (-P) - 2 \cdot O$$

$$= O.$$

Proposition: Let E/k be a e.c., $P \in E(k)$ and $r, r' \in k(E) \setminus \{0\}$. Then

1) $\operatorname{ord}_{\overline{P}}(\quad) = \operatorname{ord}_{\overline{P}}(\quad) - \operatorname{ord}_{\overline{P}}(\quad)$

2) $\operatorname{ord}_{\overline{P}}(r'/r) = \operatorname{ord}_{\overline{P}}(r) - \operatorname{ord}_{\overline{P}}(r')$

Proof: Let $u = u_P$ be a uniformizer at P. Then

$\exists\, d, d' \in \mathbb{Z}$ and $s, s' \in k(E)$ s.th $s(\overline{P}), s'(\overline{P}) \neq 0, \infty$

$r = u^d s \Rightarrow \operatorname{ord}_{\overline{P}}(r) = d$

$r' = (u')^{d'} \cdot s' \quad \operatorname{ord}_{\overline{P}}(r') = d'$.

1) Write

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

where $(s \cdot s')(P) = s(\overline{P}) \cdot s'(\overline{P}) \neq 0, \infty$.

$\Rightarrow \quad \text{ord}_P(r \cdot r') = d + d'$.

2) write

$$r/r' = \frac{u^d}{u^{d'}} \cdot \frac{s}{s'}$$

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

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

so $\text{ord}_P(r/r') = d - d'$ //

Def: Let E/k be an e.c.

A divisor (over E) is

a formal expression

$$D = \sum n_P [P]$$

$P \in E(\mathbb{K})$

where

1) $n_P \in \mathbb{Z}$

2) only finitely many n_P's are non-zero.

We denote by

$\mathrm{Div}_{\mathbb{K}} E$

the set of all divisors of E.

Obs: $\mathrm{Div}\, E$ has a canonical gp structure:

If $D, D' \in \mathrm{Div}\, E$

say

$$D = \sum_{P \in E} n_P \cdot [P]$$

$$D' = \sum_{P \in E} n'_P \cdot [P]$$

$$D + D' := \sum_{P \in E(\bar{k})} (n_P + n_{P'}) \cdot [P].$$

$$-D := \sum_{P \in E(\bar{k})} -n_P \cdot [P].$$

$$0 := \sum_{P \in E(\bar{k})} 0 \cdot [P]$$

We can define 2 gp homomorphisms (exercise)

1) $\deg : \mathrm{Div}_{\Bbbk} E \longrightarrow \mathbb{Z}$

$$D = \sum n_P \cdot [P] \longmapsto \deg(D) = \sum_{P \in E} n_P$$

2) $\boxed{\mathrm{sum} : \mathrm{Div}_{\Bbbk} E \to E(\Bbbk)}$ ←

$$D = \sum n_P \cdot [P] \longmapsto \mathrm{sum}(D) = \sum_{P \in E} n_P \cdot P \in E(\Bbbk)$$

In the examples:

$$r \rightsquigarrow \mathrm{Div}(r)$$

$$\deg(\mathrm{Div}(r)) = 0$$

$$\mathrm{sum}(\mathrm{Div}(r)) = O \in E(k).$$

Def: Let S be a set.

The free abelian gp on S is the set of all formal expressions:

$$\sum_{s \in S} n_s \cdot [s] \quad \text{with } n_s \in \mathbb{Z}$$

and only finitely many $\neq 0$.

with the obvious abelian gp structure.

Denoted $\mathbb{Z}\langle S \rangle$

eg $\mathrm{Div}\, E = \mathbb{Z}\langle E(\bar{k}) \rangle$.

$\deg : \mathbb{Z}\langle S \rangle \longrightarrow \mathbb{Z}$

$\sum_{s \in S} n_s \cdot [s] \longmapsto \sum_{s \in S} n_s$

$r \in \bar{k}(E)$

$\rightsquigarrow \underline{\mathrm{Div}(r)}$

$= \sum_{P \in E} \mathrm{ord}_P(r) \cdot [P]$