Function fields

$\mathbb{k}$ field

Recall that $\mathbb{k}[x]$ is analogous to $\mathbb{Z}$.

to push the analogy, we can imitate the construction of $\mathbb{Q}$ from $\mathbb{Z}$:

Define $\sim$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$

$$(a,b) \sim (c,d) \iff ad = cb.$$

" $\frac{a}{b}$ " " $\frac{c}{d}$ "

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$$

$$\frac{a}{b} := [(a,b)]$$

Thus the function field in one variable is

$$\mathbb{k}(x) = \mathbb{k}[x] \times (\mathbb{k}[x] \setminus \{0\}) / \sim$$

where

$$(f, g) \sim (h, i)$$

$$(=) \quad f \cdot i = h \cdot g.$$

so

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

is a field

$$\left(\frac{f}{g}\right)^{-1} = \frac{g}{f}.$$

Rem: We saw that $\mathbb{k}(x)$

Rem: ... is the minimal field containing $\mathbb{k}$ and x

When we talk about elliptic curves we wont the 2 variable version

Def:

$$\mathbb{k}(x,y) = \left\{ \frac{f(x,y)}{g(x,y)} \;\middle|\; f,g \in \mathbb{k}[x,y] \text{ and } g \neq 0 \right\}$$

is called the function field / field of rational functions.

Example: $E/\mathbb{k}$ and

$\ldots E(\mathbb{k})$ then

$p \in C(x,y)$

$$\underline{\underline{2p}} = \left(r(x,y), r'(x,y) \right)$$

where $r, r' \in \mathbb{k}(x,y)$

- Every $\underline{\underline{\frac{f}{g}}} \in \mathbb{k}(x,y)$

defines a partial function

$$\mathbb{A}^2 \longrightarrow \mathbb{k}$$

$$(x_0, y_0) \longmapsto \underline{\frac{f(x_0,y_0)}{g(x_0,y_0)}}$$

(not defined on

$$C_g : g(x,y) = 0 \ )$$

Note: if $\underline{f} \sim \underline{f'}$

$g \qquad g'$

$$(\Rightarrow \quad f \cdot g' - f' g = 0$$

E.g. Consider

$$\frac{x^2}{xy} = \frac{xy}{y^2} \in k(x,y)$$

Def: We say that

$r(x,y) \in k(x,y)$ is regular

at $\underline{p} = (x,y) \in \mathbb{A}^2$ if

there is a representation

$$r(x,y) = \frac{f(x,y)}{g(x,y)} \quad \text{s.t. } h$$

$g(P) \neq 0$.

In this case we define

$$r(P) = \frac{f(P)}{g(P)}$$ for

the appropriate rep'n.

Now let $E/\mathbb{k}$ be an e.c

w/ $E: \varphi(x,y) = y^2 - x^3 - Ax - B = 0$.

For any <u>finite</u> point

$P \in E(\mathbb{k})$ (ie $P \neq O$)

$\in \mathbb{A}^2$.

So we can consider any

rational function

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

as restricted to

$$E(k) \setminus \{O\} \subseteq \mathbb{A}^2.$$

Note that if

$\varphi(x,y) \mid g(x,y)$ then

$r(x,y)$ is not defined

on any $E(k) \setminus \{O\}$

O/w, if $\varphi \nmid g$, then

$f(x,y)$ is defined or
$g(x,y)$

all points (x_0, y_0)

s.th $g(x_0, y_0) \neq 0$.

Rem: By Bezout's thm,

$$E \cap C_g \leq \deg \varphi \cdot \deg g.$$

We will call $\frac{f(x,y)}{g(x,y)} \in \mathbb{k}(x,y)$

s.th $\varphi \nmid g$,

a rational function on E.

We define an equivalence rel'n on such functions by

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

$$\iff \varphi \mid (f \cdot g' - f' g)$$

$$\left(\mathbb{k}[x]/\varphi \hookrightarrow \text{mod } \varphi \text{ arithmetic} \right.$$

$$f \sim g \hookrightarrow f - g = 0 \bmod \varphi$$

$$\iff \varphi \mid f - g. \Big)$$

In other words

$$\mathbb{k}[x,y]/(\varphi)$$

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

the polynomials on E is

$$\mathbb{K}[E] = \mathbb{K}[x,y] / \varphi$$

$$= \mathbb{K}[x,y] / (y^2 - x^3 - Ax - B = 0)$$

By def'n, if $f \in \mathbb{K}[E]$

we can replace any term y^2 w/ $x^3 + Ax + B$.

Thus, $f(x,y)$ can be written <u>canonical form</u>

$$f(x,y) \overset{\mathbb{K}[E]}{=} v(x) + y\,w(x)$$

for $v, w \in \mathbb{k}(x)$.

Proposition: The canonical form is unique.

Proof: Say $f(x,y) = v(x) + y w(x)$

$= v'(x) + y w'(x)$.

Then

$$\underbrace{(v(x) - v'(x))}_{v(x)} + y \underbrace{(w(x) - w'(x))}_{w(x)} = 0$$

It is enough to show that

$$v(x) + y w(x) = 0 \Rightarrow$$

$$v(x) = 0 \wedge w(x) = 0 .$$

Now

$$0 = \underset{\uparrow}{Q} \cdot \left(v(x) - y\,w(x) \right)$$

$$= \left(v(x) + y\,w(x) \right)\left(v(x) - y\,w(x) \right)$$

$$= v^2(x) - y^2\, w^2(x)$$

(even, odd + even)

$$= v^2(x) + \left(-s(x) \right) w^2(x)$$

(where $s(x) = x^3 + Ax + B$)

But $\deg_x(s)$ is odd

and $\deg(v^2)$ and $\deg(w^2)$

are even

so $w(x) = 0$

hence also $v(x) = 0$ //

Def: Let $f \in k[E]$ be

Def: Let $f \in k(E)$ be given in canonical form as $f(x,y) = v(x) + y\,w(x)$

The conjugate is

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

The norm of f is

$$N_f = f \cdot \bar{f} = v^2(x) - y^2 w^2(x)$$
$$= v^2(x) - (x^3 + Ax + B)\,w^2(x).$$
$$\in k[E].$$

(in $\mathbb{C}$: $z \cdot \bar{z} = \|z\|$)

Rem: $k[E] = k[x,y]/\varphi$

and d can be shown that

φ is irreducible

ie cannot be written

as $\varphi = a \cdot b$ for

non-constant

$a, b \in \mathbb{k}[x,y]$

and $\mathbb{k}[E]$ is not

a field. (eg x has

no mult. inverse)

Def: For $E/\mathbb{k}$ an e.c, the

set of rational functions

on E is

$$\underline{\underline{\Bbbk(E)}} := \Bbbk[E] \times \left(\Bbbk[E] \setminus \{0\}\right)/\sim$$

$\uparrow$ "$\frac{f}{g}$" "$\frac{f'}{g'}$"

$$(f,g) \underline{\underline{\sim}} (f',g') \iff$$

$$fg' - f'g \overset{\Bbbk[E]}{=} 0$$

($fg' - f'g = t \cdot \psi$ for some t)

to check if $\frac{f}{g} = \frac{f'}{g'}$

we can put $f \cdot g'$ and $f' \cdot g$ in canonical forms and compare coefficients

$$\Bbbk(E) = \left\{ f \mid f, g \in \Bbbk[E] \right\}$$

$$\mathbb{k}(E) = \left\{ \frac{f}{g} \;\middle|\; g \neq 0 \right\}$$

$$= \left\{ \frac{f}{g} \;\middle|\; \begin{array}{l} f, g \in \mathbb{k}[E] \\ \wedge\ g \neq 0 \end{array} \right\}$$

Rem: $\mathbb{k}(E)$ is a field

e.g. $\frac{f}{g} \cdot \frac{f'}{g'} := \frac{f \cdot f'}{g \cdot g'}$

$g \neq 0$
$f \neq 0$ $\left(\frac{f}{g}\right)^{-1} = \frac{g}{f}$

Rem: For $r = \frac{f}{g} \in \mathbb{k}(E)$

Write

$$\frac{f}{g} = \frac{f\bar{g}}{g\bar{g}} = \frac{f\bar{g}}{N_g}$$

we write $f\bar{g}$ in canonical form

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

and $N_g(x) = v^2(x) - s(x)\,w^2(x)$

So

$$\frac{f(x,y)}{g(x,y)} = \frac{v(x) + y\,w(x)}{v^2(x) - s(x)\,w^2(x)}$$

$$= r(x) + y \cdot r'(x)$$

this is the

and thus is [illegible]

canonical form of r.

Exercise the canonical form of $r \in k(E)$ is unique.

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

$f(x,y) \in k[x,y]$ $\quad y^2 = x^3 + Ax + B$

$k[x,y] \longrightarrow k[E] = k[x,y]/\varphi$

$f(x,y) \longmapsto f \pmod{\varphi}$

$V(x) + y\,W(x)$

Want: for $r \in k(E)$

what is $r(O)$?

"$O = (\infty, \infty)$"

In calculus, in one variable,

$$r(x) = \frac{x}{x^2+1}$$

to see what is

$$r(\infty) = \lim_{x \to \infty} \frac{x}{x^2+1}$$

$$\lim_{x \to \infty} \frac{\frac{x}{x^2}}{\frac{x^2}{x^2} + \frac{1}{x^2}} = \lim_{x \to \infty} \frac{\frac{1}{x}}{1 + \frac{1}{x^2}}$$

$$= \frac{0}{1+0} = 0$$

however

if

$$r'(x) = \frac{x^2}{x^2+1}$$

$$r'(\infty) = \lim_{x \to \infty} \frac{x^2}{x^2+1}$$

$$= \lim_{x \to \infty} \frac{\frac{x^2}{x^2}}{\frac{x^2}{x^2} + \frac{1}{x^2}} =$$

$$= \frac{1}{1+0} = 1$$

In $\mathbb{K}[E]$ the notion of $\deg(f)$ for $f \in \mathbb{K}[E]$

needs adjustment since

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

We set $f(x,y) = V(x) + yW(x)$

in canonical form

The rel'n between

$\deg(x)$ and $\deg(y)$

should be $\frac{2}{3}$

so we define

$$\deg(y) = 3$$

$$\deg(x) = 2$$

and hence

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