Into the weeds of EC pairings

Ariel Gabizon
Aztec)

Divisors on $\mathbf{k}(\mathbf{X})$

$$\mathbf{P} := \mathbf{k} \cup \infty.$$

Divisors on $k(X)$

$P := k \cup \infty$.

A divisor is a formal sum

$$D = \sum_{a \in P} d_a \cdot [a]$$

where $d_a \in \mathbb{Z}$ is non-zero except for finitely many a.

Evaluating at ∞ via projective space

Evaluating $f(x) = \frac{x^2+x+1}{3x^2+1}$ at ∞:

Evaluating at ∞ via projective space

Evaluating $f(x) = \frac{x^2+x+1}{3x^2+1}$ at ∞:

Homogenize: $--> \frac{x^2+xz+z^2}{3x^2+z^2}$

Evaluating at ∞ via projective space

Evaluating $f(x) = \frac{x^2+x+1}{3x^2+1}$ at ∞:

Homogenize: $-- > \frac{x^2+xz+z^2}{3x^2+z^2}$

Evaluate at $(x, z) = (1, 0)$**:**$\frac{1}{3}$

Divisors of functions

$f \in k(X)$

$$\operatorname{div}(f) = \sum o_\alpha(f) \cdot [\alpha]$$

where $o_\alpha(f)$ is the order of f at α:

Divisors of functions

$f \in k(X)$

$$\mathrm{div}(f) = \sum o_a(f) \cdot [a]$$

where $o_a(f)$ is the order of f at a:

$$f = (x - a)^{o_a(f)}(g(x))$$

where $g(a) \neq 0, \infty$

Divisors of functions

$f \in k(X)$

$$\operatorname{div}(f) = \sum o_a(f) \cdot [a]$$

where $o_a(f)$ is the order of f at a:

$$f = (x - a)^{o_a(f)}(g(x))$$

where $g(a) \neq 0, \infty$

How to compute $o_\infty(f)$? If $f = g/h$ for polys g, h,
$o_\infty(f) = \deg(h) - \deg(g)$

example:

$$f = \frac{(X-1)^2(X-2)}{X-3}$$

$$\operatorname{div}(f) = 2\cdot[1] + [2] - [3] - 2[\infty].$$

example:

$$f = \frac{(X-1)^2(X-2)}{X-3}$$

$div(f) = 2 \cdot [1] + [2] - [3] - 2[\infty]$.
Define $deg(D) := \sum_{a \in P} d_a$.
For $f \in k(X)$ we always have $deg(div(f)) = 0$.

The divisor class group

- The set of divisors is a group under coordinate wise addition

The divisor class group

- The set of divisors is a group under coordinate wise addition
- The set of divisors of degree zero is a subgroup $\mathbf{Div^0}$ under this rule.

The divisor class group

- The set of divisors is a group under coordinate wise addition
- The set of divisors of degree zero is a subgroup $\mathbf{Div^0}$ under this rule.
- If $\mathbf{D} = \mathbf{div}(\mathbf{f})$ for $\mathbf{f} \in \mathbf{k}(\boldsymbol{x})$ we call $\mathbf{D}$ a principal divisor.

The divisor class group

- The set of divisors is a group under coordinate wise addition
- The set of divisors of degree zero is a subgroup $\mathbf{Div^0}$ under this rule.
- If $\mathbf{D} = \mathbf{div}(\mathbf{f})$ for $\mathbf{f} \in \mathbf{k}(\mathbf{x})$ we call $\mathbf{D}$ a principal divisor.
- The *divisor class group of degree 0* is: $\mathbf{Div^0}$/(principal divisors).

Is this an interesting group?

The divisor class group

- The set of divisors is a group under coordinate wise addition
- The set of divisors of degree zero is a subgroup $\mathbf{Div^0}$ under this rule.
- If $\mathbf{D} = \mathbf{div}(\mathbf{f})$ for $\mathbf{f} \in \mathbf{k}(\mathbf{x})$ we call $\mathbf{D}$ a principal divisor.
- The *divisor class group of degree 0* is: $\mathbf{Div^0}$/(principal divisors).

Is this an interesting group?No, its trivial! But this gets more interesting when we do it over an elliptic curve instead of a field.

Suppose our curve E is $y^2 = x^3 - x$. Instead of $k(X)$ we'll work now over $H := k(x, y)/(y^2 - x^3 - x)$.

Suppose our curve E is $y^2 = x^3 - x$. Instead of $k(X)$ we'll work now over $H := k(x, y)/(y^2 - x^3 - x)$.

For example in H, $x = y^2 \cdot \frac{1}{x^2 - 1}$.

Suppose our curve E is $y^2 = x^3 - x$. Instead of $k(X)$ we'll work now over $H := k(x, y)/(y^2 - x^3 - x)$.

For example in H, $x = y^2 \cdot \frac{1}{x^2-1}$.

Now, a divisor is $D = \sum_{P \in E} d_j[P]$, and for $f \in H$ $div(f) = \sum_{P \in E} o_P(f)[P]$

Suppose our curve E is $y^2 = x^3 - x$. Instead of $k(X)$ we'll work now over $H := k(x, y)/(y^2 - x^3 - x)$.

For example in H, $x = y^2 \cdot \frac{1}{x^2-1}$.

Now, a divisor is $D = \sum_{P \in E} d_j[P]$, and for $f \in H$ $div(f) = \sum_{P \in E} o_P(f)[P]$
How to compute $o_P(f)$?

$$f = u^{o_P(f)} \cdot g$$

for g with $g(P) \neq 0, \infty$ and u with $o_P(u) = 1$.

It can be shown, like in $k(X)$ we always have $deg(div(f)) = 0$.

It can be shown, like in $k(X)$ we always have $deg(div(f)) = 0$.

Example: $f = x$ Compute $div(x)$. Can be shown $o_{\infty}(x) = -2, o_{(0,0)}(y) = 1$.

It can be shown, like in $k(X)$ we always have $deg(div(f)) = 0$.

Example: $f = x$ Compute $div(x)$. Can be shown $o_\infty(x) = -2, o_{(0,0)}(y) = 1$.

Since $x = y^2 \cdot \frac{1}{x^2-1}$, we have $o_{(0,0)}(x) = 2$.

So $div(x) = 2([0,0]) - 2[\infty]$.

The cool theorem

As before, we can define
$\mathbf{C} := \boldsymbol{Div}^{\mathbf{0}}/(\text{principal divisors})$.

The cool theorem

As before, we can define
$\mathbf{C} := \boldsymbol{Div}^{\mathbf{0}}/(\text{principal divisors})$.

It turns out $\mathbf{C}$ is isomorphic to $\mathbf{E}$ as a group!

The cool theorem

As before, we can define
$\mathbf{C} := \boldsymbol{Div^0}/(\text{principal divisors})$.

It turns out $\mathbf{C}$ is isomorphic to $\mathbf{E}$ as a group!

Proof sketch: We will show that every divisor $\mathbf{D}$ of degree zero can be written as
$\mathbf{D} = \mathbf{div}(\mathbf{g}) + [\mathbf{P}] - [\infty]$.

Proof sketch: We will show that every divisor D of degree zero can be written as
$D = div(g) + [P] - [\infty]$.

The idea is that divisors of line functions allow us to compress two points into one: If we have $[P_1] + [P_2]$ as part of divisor and $l(x, y)$ is the line passing through P_1, P_2 then

$$div(l) = [P_1] + [P_2] + [P_3] - 3[\infty]$$

Proof sketch: We will show that every divisor D of degree zero can be written as
$D = div(g) + [P] - [\infty]$.

The idea is that divisors of line functions allow us to compress two points into one: If we have $[P_1] + [P_2]$ as part of divisor and $l(x, y)$ is the line passing through P_1, P_2 then

$$div(l) = [P_1] + [P_2] + [P_3] - 3[\infty]$$

So can switch:
$[P_1] + [P_2] - -> div(l) - [P_3] - 3 \cdot [\infty]$