Algebraic Geometric Codes

Recitation 10

Shir Peleg

Tel Aviv University

May 11, 2022

Elliptic Curves

Let F/K be a function field with genus 1, with a prime divisor q of $deg(q) = 1$.
Last week we saw:

Elliptic Curves

Let F/K be a function field with genus 1, with a prime divisor q of $deg(q) = 1$.
Last week we saw:

1. There $x, y \in F \setminus K$ s.t $F = K(x, y)$, and $y^2 = d(x)$ where $d \in K[x]$.

Elliptic Curves

Let F/K be a function field with genus 1, with a prime divisor q of $deg(q) = 1$.
Last week we saw:

1. There $x, y \in F \setminus K$ s.t $F = K(x, y)$, and $y^2 = d(x)$ where $d \in K[x]$.
2. $\deg(d) = 3$, and d has no multiple factors.

Elliptic Curves

Let F/K be a function field with genus 1, with a prime divisor q of $deg(q) = 1$.
Last week we saw:

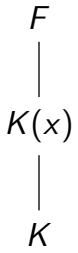
1. There $x, y \in F \setminus K$ s.t $F = K(x, y)$, and $y^2 = d(x)$ where $d \in K[x]$.
2. $\deg(d) = 3$, and d has no multiple factors.
3. $(x)_\infty = 2q$, $(y)_\infty = 3q$.

$F = K(x, y),\ y^2 = d(x).$

We want to categorize all the rational (degree 1) places of F.

$F = K(x, y),\ y^2 = d(x).$

We want to categorize all the rational (degree 1) places of F.
We have the following diagram



Where the first extension has $tr - deg$ of 1, and the second extension is algebraic.

Degree one palaces

Note that p has degree one only if it sits over a place p' of $K(x)$, where p' has degree one (this is necessary but not sufficient). Recall that the degree one places in $k(x)$ are the places

$$\{p_\infty\} \cup \{p_\alpha \mid \alpha \in K\}.$$

We need to consider extensions of these valuations.

Degree 1 places.

We already saw that there is only one place q that satisfies $q|_{K(x)} = p_\infty$.

Degree 1 places.

We already saw that there is only one place q that satisfies $q|_{K(x)} = p_\infty$.
We want to find $\varphi : F \to K$, with $\varphi' = \varphi\ |_{K(x)} = \varphi_\alpha$. It follows that

$$\varphi(y)^2 = \varphi(y^2) = \varphi(d(x)) = d(\varphi(x)).$$

Thus, it must be that $\varphi(y)^2 = d(\varphi(x))$.

Degree 1 places.

We already saw that there is only one place q that satisfies $q|_{K(x)} = p_\infty$.
We want to find $\varphi : F \to K$, with $\varphi' = \varphi\ |_{K(x)} = \varphi_\alpha$. It follows that

$$\varphi(y)^2 = \varphi(y^2) = \varphi(d(x)) = d(\varphi(x)).$$

Thus, it must be that $\varphi(y)^2 = d(\varphi(x))$.

Degree 1 places.

We already saw that there is only one place q that satisfies $q|_{K(x)} = p_\infty$.
We want to find $\varphi : F \to K$, with $\varphi' = \varphi\ |_{K(x)} = \varphi_\alpha$. It follows that

$$\varphi(y)^2 = \varphi(y^2) = \varphi(d(x)) = d(\varphi(x)).$$

Thus, it must be that $\varphi(y)^2 = d(\varphi(x))$. If $Y^2 - d(\varphi(x))$ does not have a root in K, then $Im(\varphi)$ is in a degree 2 extension of K, and the corresponding place has degree 2.
Note that indeed this is the only extension of the place φ'. From the fundamental equality.

Degree 1 places.

If $Y^2 - d(\varphi(x))$ does have a root in K, then $Im(\varphi) = K$, and the corresponding place has degree 1. There are two such places $\varphi(y) = \pm\sqrt{d(\varphi(x))}$.

Degree 1 places.

If $Y^2 - d(\varphi(x))$ does have a root in K, then $Im(\varphi) = K$, and the corresponding place has degree 1. There are two such places $\varphi(y) = \pm\sqrt{d(\varphi(x))}$.
To conclude we have that:

$$\{\varphi_{\alpha,\beta} = F[x,y] \to K, x \to \alpha, y \to \beta \mid b^2 = d(\alpha)\}.$$

We need to show that no two of these places are equivalent. This follows from the fact that for every $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$ either $\varphi_{\alpha_1,\beta_1}|_{K(x)}$ is not equivalent to $\varphi_{\alpha_2,\beta_2}|_{K(x)}$ or $\varphi_{\alpha_1,\beta_1}|_{K(y)}$ is not equivalent to $\varphi_{\alpha_2,\beta_2}|_{K(y)}$.

Degree 1 places.

If $Y^2 - d(\varphi(x))$ does have a root in K, then $Im(\varphi) = K$, and the corresponding place has degree 1. There are two such places $\varphi(y) = \pm\sqrt{d(\varphi(x))}$.
To conclude we have that:

$$\{\varphi_{\alpha,\beta} = F[x,y] \to K, x \to \alpha, y \to \beta \mid b^2 = d(\alpha)\}.$$

We need to show that no two of these places are equivalent. This follows from the fact that for every $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$ either $\varphi_{\alpha_1,\beta_1}|_{K(x)}$ is not equivalent to $\varphi_{\alpha_2,\beta_2}|_{K(x)}$ or $\varphi_{\alpha_1,\beta_1}|_{K(y)}$ is not equivalent to $\varphi_{\alpha_2,\beta_2}|_{K(y)}$.
Again, from the fundamental inequality we know we found all the relevant places.

Elliptic curves

Let us denote:

- $\mathbb{P}_1(K) = \{p \in \mathbb{P} \mid \deg(p) = 1\}$.
- $\mathbb{P}_1'(K) = \mathbb{P}_1(K) \setminus \{q\}$.
- $\mathcal{E}'(K) = \{(a, b) \mid b^2 = d(a)\}$.

We proved that there is a one to one and onto correspondence, $\mathbb{P}_1'(K) \to \mathcal{E}'(K)$.

Elliptic curves

Let us denote:

- $\mathbb{P}_1(K) = \{p \in \mathbb{P} \mid \deg(p) = 1\}$.
- $\mathbb{P}'_1(K) = \mathbb{P}_1(K) \setminus \{q\}$.
- $\mathcal{E}'(K) = \{(a, b) \mid b^2 = d(a)\}$.

We proved that there is a one to one and onto correspondence, $\mathbb{P}'_1(K) \to \mathcal{E}'(K)$.
Let extend the correspondence $\mathbb{P}_1(K) \to \mathcal{E}(K) := \mathcal{E}'(K) \cup \{0\}$.

Elliptic curves

Let us denote:

- $\mathbb{P}_1(K) = \{p \in \mathbb{P} \mid \deg(p) = 1\}$.
- $\mathbb{P}'_1(K) = \mathbb{P}_1(K) \setminus \{q\}$.
- $\mathcal{E}'(K) = \{(a, b) \mid b^2 = d(a)\}$.

We proved that there is a one to one and onto correspondence, $\mathbb{P}'_1(K) \to \mathcal{E}'(K)$.
Let extend the correspondence $\mathbb{P}_1(K) \to \mathcal{E}(K) := \mathcal{E}'(K) \cup \{0\}$.

Claim 0.1

Let $p_1, p_2 \in \mathbb{P}_1(K)$. $[p_1] = [p_2] \iff p_1 = p_2$.

Elliptic curves

Let us denote:

- $\mathbb{P}_1(K) = \{p \in \mathbb{P} \mid \deg(p) = 1\}$.
- $\mathbb{P}'_1(K) = \mathbb{P}_1(K) \setminus \{q\}$.
- $\mathcal{E}'(K) = \{(a, b) \mid b^2 = d(a)\}$.

We proved that there is a one to one and onto correspondence, $\mathbb{P}'_1(K) \to \mathcal{E}'(K)$.
Let extend the correspondence $\mathbb{P}_1(K) \to \mathcal{E}(K) := \mathcal{E}'(K) \cup \{0\}$.

Claim 0.1

Let $p_1, p_2 \in \mathbb{P}_1(K)$. $[p_1] = [p_2] \iff p_1 = p_2$.

Proof.

Assume $p_2 = p_1 + (z)$, then $p_1 + (z) \geq 0$, and thus $z \in \mathcal{L}(p_1)$. From RRT, $\dim \mathcal{L}(p_1) = 1$, as $p_1 > 0$, therefore $K = \mathcal{L}(0) \subseteq \mathcal{L}(p_1) = K$ and $(z) = 0$. □

Group action on $\mathbb{P}_1(K)$

Define $\mathcal{C}_0 = \{a \in \mathcal{D} \mid \deg(a) = 0\}/\{(z), \forall z \in F^\times\}$.
This is a group of cosets.

Group action on $\mathbb{P}_1(K)$

Define $\mathcal{C}_0 = \{a \in \mathcal{D} \mid \deg(a) = 0\}/\{(z), \forall z \in F^\times\}$.
This is a group of cosets.

Claim 0.2

The map $p \to [p - q]$ is a bijection from $\mathbb{P}_1(K)$ to $\mathcal{C}_0$.

Group action on $\mathbb{P}_1(K)$

Define $\mathcal{C}_0 = \{a \in \mathcal{D} \mid \deg(a) = 0\}/\{(z), \forall z \in F^\times\}$.
This is a group of cosets.

Claim 0.2

The map $p \to [p - q]$ is a bijection from $\mathbb{P}_1(K)$ to $\mathcal{C}_0$.

Proof.

First we note that $\deg(p - q) = 0$.

Group action on $\mathbb{P}_1(K)$

Define $\mathcal{C}_0 = \{a \in \mathcal{D} \mid \deg(a) = 0\}/\{(z), \forall z \in F^\times\}$.
This is a group of cosets.

Claim 0.2

The map $p \to [p - q]$ is a bijection from $\mathbb{P}_1(K)$ to $\mathcal{C}_0$.

Proof.

First we note that $\deg(p - q) = 0$.
One to one: assume $[p - q] = [p' - q]$, then there is $z \in F^\times$ s.t.
$p - q = p' - q + (z)$, that means that $p = p' + (x)$, thus $[p] = [p']$ and from the claim before $p = p'$.

Group action on $\mathcal{E}(K)$

Proof.

Onto: let $[a] \in \mathcal{C}_0$. $\deg(a+q) = 1$, From RRT, $\dim \mathcal{L}(a+q) = 1$. Thus there is $z \in F^\times$ s.t. $(z) + a + q \geq 0$. As $\deg((z) + a + q) = 1$, it must be that $(z) + a + q = p$ for some $p \in \mathbb{P}_1(K)$, therefore $p - q = a + (z)$, and $[a] = [p - q]$.

Group action on $\mathcal{E}(K)$

Proof.

Onto: let $[a] \in \mathcal{C}_0$. $\deg(a+q) = 1$, From RRT, $\dim \mathcal{L}(a+q) = 1$. Thus there is $z \in F^\times$ s.t. $(z) + a + q \geq 0$. As $\deg((z) + a + q) = 1$, it must be that $(z) + a + q = p$ for some $p \in \mathbb{P}_1(K)$, therefore $p - q = a + (z)$, and $[a] = [p - q]$.

Corollary 1

This bijection provides an abelic group action on $\mathcal{E}(K)$ (from the decomposition $(\mathcal{E}(K) \to \mathbb{P}_1(K) \to \mathcal{C}_0$ which is a group). The zero of the group is the added point 0.

Group action on $\mathcal{E}(K)$

Proof.

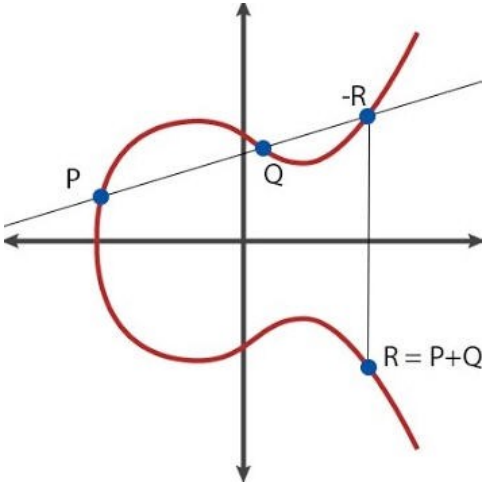
Onto: let $[a] \in \mathcal{C}_0$. $\deg(a+q) = 1$, From RRT, $\dim \mathcal{L}(a+q) = 1$. Thus there is $z \in F^\times$ s.t. $(z) + a + q \geq 0$. As $\deg((z) + a + q) = 1$, it must be that $(z) + a + q = p$ for some $p \in \mathbb{P}_1(K)$, therefore $p - q = a + (z)$, and $[a] = [p - q]$.

Corollary 1

This bijection provides an abelic group action on $\mathcal{E}(K)$ (from the decomposition $(\mathcal{E}(K) \to \mathbb{P}_1(K) \to \mathcal{C}_0$ which is a group). The zero of the group is the added point 0.

We want to understand this action (i.e. what is $(a, b) + (c, d)$?).

Geometric structure



We consider 0 on a line ℓ
iff ℓ is parallel to the y axis.

Geometric structure

Theorem 2

Let A_1, A_2, A_3 be different in $\mathcal{E}(K)$. Then

$$A_1 + A_2 + A_3 = 0 \iff A_1, A_2, A_3 \text{ are on the same line}$$

Geometric structure

Theorem 2

Let A_1, A_2, A_3 be different in $\mathcal{E}(K)$. Then

$$A_1 + A_2 + A_3 = 0 \iff A_1, A_2, A_3 \text{ are on the same line}$$

Proof.

Assume w.l.o.g $A_1, A_2 \neq 0$, Let $\ell = \alpha X + \beta Y + \gamma = 0$ be the line that goes through A_1, A_2.

Geometric structure

Theorem 2

Let A_1, A_2, A_3 be different in $\mathcal{E}(K)$. Then

$$A_1 + A_2 + A_3 = 0 \iff A_1, A_2, A_3 \text{ are on the same line}$$

Proof.

Assume w.l.o.g $A_1, A_2 \neq 0$, Let $\ell = \alpha X + \beta Y + \gamma = 0$ be the line that goes through A_1, A_2. Set $z = \alpha x + \beta y + \gamma \in F$.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

□

Geometric structure

Claim 2.1

Let $p = (a, b) \in \mathcal{E}'(K)$ *then* $\varphi_p(z) = 0 \iff (a, b) \in \ell$.

Geometric structure

Claim 2.1

Let $p = (a, b) \in \mathcal{E}'(K)$ *then* $\varphi_p(z) = 0 \iff (a, b) \in \ell$.

Proof.

$$\varphi_p(z) = \varphi_p(\alpha x + \beta y + \gamma) = \alpha\varphi_p(x) + \beta\varphi_p(y) + \gamma = \alpha a + \beta b + \gamma.$$

□

Geometric structure

Claim 2.1

Let $p = (a, b) \in \mathcal{E}'(K)$ *then* $\varphi_p(z) = 0 \iff (a, b) \in \ell$.

Proof.

$$\varphi_p(z) = \varphi_p(\alpha x + \beta y + \gamma) = \alpha\varphi_p(x) + \beta\varphi_p(y) + \gamma = \alpha a + \beta b + \gamma.$$

□

Back to the proof of the theorem

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$.

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 2q$. Let $A_3 \in \ell$ then if $A_3 \in \mathcal{E}'(K)$ then $\varphi_{p_3}(z) = 0$, and thus $p_3 \leq (z)_0$ in contradiction to the fact that $\deg((z)_\infty) = 2$.

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 2q$. Let $A_3 \in \ell$ then if $A_3 \in \mathcal{E}'(K)$ then $\varphi_{p_3}(z) = 0$, and thus $p_3 \leq (z)_0$ in contradiction to the fact that $\deg((z)_\infty) = 2$. Thus $A_3 = 0$ and we need to prove that $A_1 + A_2 = 0$.

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 2q$. Let $A_3 \in \ell$ then if $A_3 \in \mathcal{E}'(K)$ then $\varphi_{p_3}(z) = 0$, and thus $p_3 \leq (z)_0$ in contradiction to the fact that $\deg((z)_\infty) = 2$. Thus $A_3 = 0$ and we need to prove that $A_1 + A_2 = 0$. Indeed, as $\deg((z)_\infty) = 2$ it follows that $(z) = p_1 + p_2 - 2q$ and thus $[p_1 - q] + [p_2 - q] = 0$.

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 2q$. Let $A_3 \in \ell$ then if $A_3 \in \mathcal{E}'(K)$ then $\varphi_{p_3}(z) = 0$, and thus $p_3 \leq (z)_0$ in contradiction to the fact that $\deg((z)_\infty) = 2$. Thus $A_3 = 0$ and we need to prove that $A_1 + A_2 = 0$. Indeed, as $\deg((z)_\infty) = 2$ it follows that $(z) = p_1 + p_2 - 2q$ and thus $[p_1 - q] + [p_2 - q] = 0$.
The other direction, let A_3 s.t. $A_1 + A_2 + A_3 = 0$. We saw that $A_1 + A_2 = 0$, and thus $A_3 = 0$, which is on the line. □

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$.

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$)

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q$

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$. $\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q \Rightarrow [p_1 - q] + [p_2 - q] + [p_3 - q] = 0$.

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q \Rightarrow [p_1 - q] + [p_2 - q] + [p_3 - q] = 0$.
$\Rightarrow$ let A_3 s.t. $A_1 + A_2 + A_3 = 0$. $A_3 \neq 0$ (from the prev case)

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q \Rightarrow [p_1 - q] + [p_2 - q] + [p_3 - q] = 0$.
$\Rightarrow$ let A_3 s.t. $A_1 + A_2 + A_3 = 0$. $A_3 \neq 0$ (from the prev case) thus $p_1 - q + p_2 - q + p_3 - q = (z')$, for some $z' \in F^\times$.

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q \Rightarrow [p_1 - q] + [p_2 - q] + [p_3 - q] = 0$.
$\Rightarrow$ let A_3 s.t. $A_1 + A_2 + A_3 = 0$. $A_3 \neq 0$ (from the prev case) thus $p_1 - q + p_2 - q + p_3 - q = (z')$, for some $z' \in F^\times$. We also have that $\deg((z)_0) = 3$, thus $(z) = p_1 + p_2 + p_3' - 3q$ for some place $p_3' \neq q$.

Geometric structure

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q \Rightarrow [p_1 - q] + [p_2 - q] + [p_3 - q] = 0$.
$\Rightarrow$ let A_3 s.t. $A_1 + A_2 + A_3 = 0$. $A_3 \neq 0$ (from the prev case) thus $p_1 - q + p_2 - q + p_3 - q = (z')$, for some $z' \in F^\times$. We also have that $\deg((z)_0) = 3$, thus $(z) = p_1 + p_2 + p_3' - 3q$ for some place $p_3' \neq q$.
$(z/z') = p_3' - p_3$, and so $[p_3'] = [p_3]$ and $p_3' = p_3$.

Proof.

$$(z)_\infty = (\alpha x + \beta y + \gamma)_\infty = \begin{cases} 2q & \beta = 0 \\ 3q & \beta \neq 0 \end{cases}$$

$A_1, A_2 \in \ell$ thus $\varphi_{p_1}(z) = \varphi_{p_2}(z) = 0$, thus $p_1, p_2 \leq (z)_0$. Assume $(z)_\infty = 3q$.
$\Leftarrow$ Let $A_3 \in \ell$ then we know that $A_3 \in \mathcal{E}'(K)$ (as $\beta \neq 0$) $\varphi_{p_3}(z) = 0$, thus $p_3 \leq (z)_0$ and $(z) = p_1 + p_2 + p_3 - 3q \Rightarrow [p_1 - q] + [p_2 - q] + [p_3 - q] = 0$.
$\Rightarrow$ let A_3 s.t. $A_1 + A_2 + A_3 = 0$. $A_3 \neq 0$ (from the prev case) thus $p_1 - q + p_2 - q + p_3 - q = (z')$, for some $z' \in F^\times$. We also have that $\deg((z)_0) = 3$, thus $(z) = p_1 + p_2 + p_3' - 3q$ for some place $p_3' \neq q$.
$(z/z') = p_3' - p_3$, and so $[p_3'] = [p_3]$ and $p_3' = p_3$. This implies that $\varphi_{p_3}(z) = 0$ and $A_3 \in \ell$. □