Elliptic Function Fields

Recitation 12

Tomer Manket

Tel Aviv University

Function fields of genus 1

Lemma 1

Let F/K be a function field of genus $g = 1$. Suppose $F = K(x, y)$ where $y^2 = d(x)$ for $d \in K[X]$ of degree 3. Then there exists a prime divisor $\mathfrak{p}$ of degree 1 such that $(x)_\infty = 2\mathfrak{p}$.

Proof.

First,

$$\deg(x)_\infty = [F : K(x)] = [K(x)(y) : K(x)] \leq 2.$$

If $[F : K(x)] = 1$ then $F = K(x)$ is a rational function field and so $g = 0$, a contradiction. Hence $\deg(x)_\infty = 2$.

Proof cont.

As $\deg(x)_\infty = 2$ and $(x)_\infty \geq 0$, there are 3 possibilities:

- $(x)_\infty = \mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}$ of $\deg \mathfrak{p} = 2$.
- $(x)_\infty = 2\mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}$ of $\deg \mathfrak{p} = 1$.
- $(x)_\infty = \mathfrak{p} + \mathfrak{q}$ for some $\mathfrak{p}, \mathfrak{q} \in \mathbb{P}$ with $\deg \mathfrak{p} = \deg \mathfrak{q} = 1$.

However, note that

$$2(y)_\infty = (y^2)_\infty = (d(x))_\infty = \deg(d) \cdot (x)_\infty = 3(x)_\infty.$$

That implies that all the coefficients in $(x)_\infty$ are even. Thus, it must be that $(x)_\infty = 2\mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}$ of degree 1. □

Conversely, we have

Theorem 2

Let K be a field with $\mathrm{char}(K) \neq 2$, and let F/K be a function field of genus $g = 1$ that has a prime divisor $\mathfrak{p}$ of degree 1. Then $F = K(x, y)$ where $y^2 = d(x)$ for a square-free $d \in K[X]$ of degree 3, and $(x)_\infty = 2\mathfrak{p}$.

Proof.

For each $n \in \mathbb{N}$, $\deg(n\mathfrak{p}) = n \deg \mathfrak{p} = n$. Therefore, if $n > 2g - 2 = 0$ then by Riemann-Roch,

$$\dim \mathcal{L}(n\mathfrak{p}) = \dim n\mathfrak{p} = n + 1 - g = n.$$

Furthermore,

$$K = \mathcal{L}(\mathfrak{p}) \subset \mathcal{L}(2\mathfrak{p}) \subset \cdots \subset \mathcal{L}(n\mathfrak{p}).$$

Proof cont.

In particular, there exist $x, y \in F$ such that

$$\mathcal{L}(2\mathfrak{p}) = \mathrm{Span}_K\{1, x\} \quad \text{and} \quad \mathcal{L}(3\mathfrak{p}) = \mathrm{Span}_K\{1, x, y\}.$$

Since $x \in \mathcal{L}(2\mathfrak{p}) \setminus \mathcal{L}(\mathfrak{p})$ we must have $(x)_\infty = 2\mathfrak{p}$. Similarly, $y \in \mathcal{L}(3\mathfrak{p}) \setminus \mathcal{L}(2\mathfrak{p})$ implies that $(y)_\infty = 3\mathfrak{p}$. Then for $i, j \in \mathbb{N}$ we have

$$(x^i y^j)_\infty = (2i + 3j)\mathfrak{p}.$$

It is easy to verify that

$$\begin{aligned} \mathcal{L}(\mathfrak{p}) &= \mathrm{Span}_K\{1\} & \mathcal{L}(2\mathfrak{p}) &= \mathrm{Span}_K\{1, x\} \\ \mathcal{L}(3\mathfrak{p}) &= \mathrm{Span}_K\{1, x, y\} & \mathcal{L}(4\mathfrak{p}) &= \mathrm{Span}_K\{1, x, y, x^2\} \\ \mathcal{L}(5\mathfrak{p}) &= \mathrm{Span}_K\{1, x, y, x^2, xy\} & \mathcal{L}(6\mathfrak{p}) &= \mathrm{Span}_K\{1, x, y, x^2, xy, x^3, y^2\} \end{aligned}$$

Proof cont.

Thus, there is a linear combination (with $f \neq 0$)

$$y^2 = a + bx + cy + dx^2 + exy + fx^3, \tag{1}$$

i.e.

$$y^2 - (ex + c)y = a + bx + dx^2 + fx^3. \tag{2}$$

Now, as $\mathrm{char}(K) \neq 2$ we can complete the square to get

$$\left(y - \frac{1}{2}(ex + c)\right)^2 = a + bx + dx^2 + fx^3 + \frac{1}{4}(ex + c)^2. \tag{3}$$

Now letting $y' = y - \frac{1}{2}(ex + c)$ gives $y'^2 = d(x)$ for $d \in K[X]$ of degree 3.

Clearly, $K(x, y) = K(x, y')$. Thus it remains to show that $F = K(x, y)$ and that d is square-free.

Proof cont.

Indeed, we saw that $\deg(x)_\infty = 2$ and $\deg(y)_\infty = 3$ are coprime, so by Question 2 in PS 3 we obtain $F = K(x,y)$.

Finally, assume to the contrary that d is not square-free. By (3), it has degree 3 and leading coefficient f, so it must be of the form

$$d(X) = f \cdot (X-\alpha)^2(X-\beta).$$

But then for $z := \frac{y'}{x-\alpha} \in F$ we get $z^2 = \frac{y'^2}{(x-\alpha)^2} = f \cdot (x-\beta)$. But then

$$F = K(x,y') = K(x,z) = K(z)$$

so F is a rational function field, contradicting $g = 1$.

□

Elliptic Function Fields

Definition 3 (Elliptic function field)

A function field F/K is an *elliptic function field* if

1. the genus of F/K is $g = 1$, and
2. there exists a divisor $\mathfrak{a}$ with $\deg \mathfrak{a} = 1$.

Remark 1

If $\deg \mathfrak{a} = 1$ *then* $\deg \mathfrak{a} > 2g - 2 = 0$, *so by Riemann-Roch*

$$\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g = 1.$$

Taking $0 \neq x \in \mathcal{L}(\mathfrak{a})$ *we obtain* $\mathfrak{q} := \mathfrak{a} + (x) \geq 0$. *As* $\mathfrak{q} \geq 0$ *and* $\deg \mathfrak{q} = 1$, *we get that* $\mathfrak{q}$ *must be a prime divisor.*

Elliptic Function Fields

Corollary 4

Let F/K be an elliptic function field with $\operatorname{char}(K) \neq 2$. Then there exist

1. *a prime divisor $\mathfrak{q}$ with $\deg \mathfrak{q} = 1$,*
2. *a square-free polynomial $d \in K[X]$ with $\deg d = 3$, and*
3. *elements $x, y \in F/K$*

such that

1. *$F = K(x, y)$ and $y^2 = d(x)$,*
2. *$(x)_\infty = 2\mathfrak{q}$ and $(y)_\infty = 3\mathfrak{q}$.*

What are the rational (i.e. degree one) prime divisors of F/K?

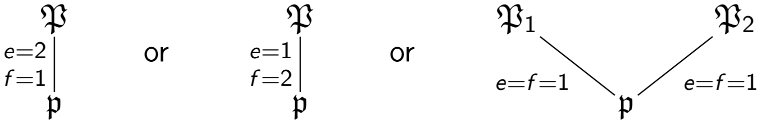
Degree one prime divisors of $F = K(x,y)$

Recall that a degree one prime divisor of F/K must lie above a degree one prime divisor of $K(x)/K$, i.e. above $\mathfrak{p}_\infty$ or $\mathfrak{p}_{x-a}$ for some $a \in K$.

By the fundamental equality, we know that for every $\mathfrak{p} \in \mathbb{P}^1_{K(x)}$,

$$\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) = [F : K(x)] = 2$$

So there are 3 possible cases:



Degree one prime divisors of $F = K(x, y)$

- For $\mathfrak{p} = \mathfrak{p}_\infty$: if $\mathfrak{P}$ lies above $\mathfrak{p}$ then $\nu_{\mathfrak{P}}(x) < 0$. Recall that $(x)_{F,\infty} = 2\mathfrak{q}$ (and $\mathfrak{q}$ has degree one) so we have

$$\begin{array}{c} \mathfrak{q} \\ {\scriptstyle e=2}\Big|{\scriptstyle f=1} \\ \mathfrak{p}_\infty \end{array}$$

  i.e. there is a unique prime divisor in F above $\mathfrak{p}_\infty$, and it has degree one.

- For $\mathfrak{p} = \mathfrak{p}_{x-a}$ (where $a \in K$):

  Case 1. $d(a) = b^2$ for some $b \in K^\times$.

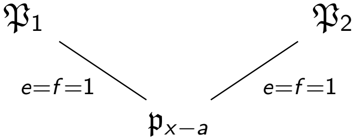
  The minimal polynomial of y over $K(x)$ is $\varphi(T) = T^2 - d(x) \in K(x)[T]$ and

$$\varphi_a(T) := T^2 - d(a) = T^2 - b^2 = (T + b)(T - b).$$

Degree one prime divisors of $F = K(x, y)$

$$\varphi_a(T) := T^2 - d(a) = T^2 - b^2 = (T + b)(T - b).$$

Thus by Kummer Theorem, in this case we have



i.e. there are two degree one prime divisors above $\mathfrak{p}$ in F, with corresponding places $\varphi_{\mathfrak{P}_1}, \varphi_{\mathfrak{P}_2}$ such that

$$\varphi_{\mathfrak{P}_1}(x) = \varphi_{\mathfrak{P}_2}(x) = a,$$

$$\varphi_{\mathfrak{P}_1}(y) = -b \quad \textit{and} \quad \varphi_{\mathfrak{P}_2}(y) = b.$$

Degree one prime divisors of $F = K(x, y)$

Case 2. $d(a) \neq b^2$ for all $b \in K$.

Then $\varphi_a(T) := T^2 - d(a)$ is irreducible over K, so by Kummer Theorem

$$\begin{array}{c} \mathfrak{P} \\ {\scriptstyle e=1 \atop f=2} \Big| \\ \mathfrak{p}_{x-a} \end{array}$$

i.e. there is a unique prime divisor in F lying above $\mathfrak{p}$, but it has degree 2.

Case 3. $d(a) = 0$.

In this case $\varphi_a(T) = T^2$ is not a product of distinct irreducible polynomials, so we cannot use Kummer's Theorem.

Degree one prime divisors of $F = K(x, y)$

Still, we can use the theorem about Kummer extensions (with $n = 2$) to get that if $\mathfrak{P}$ lies above $\mathfrak{p}$, then

$$e(\mathfrak{P}/\mathfrak{p}) = \frac{n}{r_p} \quad \text{where} \quad r_p = \gcd(n, \nu_{\mathfrak{p}}(d(x))).$$

Since $d(x)$ is square-free and $d(a) = 0$, we have $(x - a) \mid d(x)$ but $(x - a)^2 \nmid d(x)$, hence

$$\nu_{\mathfrak{p}}(d(x)) = \nu_{\mathfrak{p}_{x-a}}(d(x)) = 1 \implies r_{\mathfrak{p}} = \gcd(n, 1) = 1$$

and so $e(\mathfrak{P}/\mathfrak{p}) = \frac{2}{1} = 2$.

Degree one prime divisors of $F = K(x, y)$

It follows that there is a unique prime divisor $\mathfrak{P}$ in F lying above $\mathfrak{p}$, and it has degree one.

$$\begin{array}{c} \mathfrak{P} \\ {\scriptstyle e=2 \atop f=1}\Big| \\ \mathfrak{p}_{x-a} \end{array}$$

Moreover, $x - a \in \mathfrak{m}_{\mathfrak{p}}$ so $x - a \in \mathfrak{m}_{\mathfrak{P}}$, i.e. $\varphi_{\mathfrak{P}}(x) = a$.

In addition,

$$2\nu_{\mathfrak{P}}(y) = \nu_{\mathfrak{P}}(y^2) = \nu_{\mathfrak{P}}(d(x)) = e(\mathfrak{P}/\mathfrak{p}) \cdot \nu_{\mathfrak{p}}(d(x)) = 2 \cdot 1 = 2$$

so $\nu_{\mathfrak{P}}(y) = 1 > 0$ and therefore $\varphi_{\mathfrak{P}}(y) = 0$.

Degree one prime divisors of $F = K(x, y)$

Thus, if we denote

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

we get that there is a bijection

$$\mathbb{P}_1'(K) \cong \mathcal{E}'(K)$$

which is given by

$$\mathfrak{p} \mapsto (\varphi_{\mathfrak{p}}(x), \varphi_{\mathfrak{p}}(y))$$

Now, let $\mathcal{E}(K) := \mathcal{E}'(K) \cup \{O\}$.

Then we can extend the bijection to $\mathbb{P}_1(K) \to \mathcal{E}(K)$ by mapping $\mathfrak{q} \mapsto O$.

The set $\mathcal{E}(K)$ is called an elliptic curve, with O "the point at infinity".
Such curves have a special structure - their points form an abelian group with respect to a certain geometric action.

Our goal is to derive the group action from the corresponding elliptic function field.

Recall that the divisors group $\mathrm{Div}(F)$ has a subgroup

$$\mathrm{Prin}(F) := \{(x) \mid x \in F^\times\}.$$

The divisors class group is the quotient group

$$\mathcal{C}(F) := \mathrm{Div}(F)/\mathrm{Prin}(F).$$

We denote the class of $\mathfrak{a}$ by $[\mathfrak{a}]$, so $[\mathfrak{a}_1] = [\mathfrak{a}_2]$ iff

$$\mathfrak{a}_1 = \mathfrak{a}_2 + (z) \text{ for some } z \in F^\times.$$

Recall that in this case $\deg \mathfrak{a}_1 = \deg \mathfrak{a}_2$ and $\dim \mathfrak{a}_1 = \dim \mathfrak{a}_2$.

Claim 4.1

Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{P}_1(K)$. *Then* $[\mathfrak{p}_1] = [\mathfrak{p}_2] \iff \mathfrak{p}_1 = \mathfrak{p}_2$.

Proof.

The direction $(\Leftarrow)$ is trivial. Conversely, suppose $[\mathfrak{p}_1] = [\mathfrak{p}_2]$. Then $\mathfrak{p}_2 = \mathfrak{p}_1 + (z)$ for some $z \in F^\times$. In particular, $\mathfrak{p}_1 + (z) \geq 0$ and so $z \in \mathcal{L}(\mathfrak{p}_1)$. As $\mathfrak{p}_1 \geq 0$, we have $K = \mathcal{L}(0) \subseteq \mathcal{L}(\mathfrak{p}_1)$. In addition, by Riemann-Roch, $\dim \mathfrak{p}_1 = \deg \mathfrak{p}_1 + 1 - g = 1$. Thus $\mathcal{L}(\mathfrak{p}_1) = K$ and so $z \in K^\times$. It follows that $(z) = 0$ and $\mathfrak{p}_2 = \mathfrak{p}_1$. □

Finally, consider the following subgroup of $\mathcal{C}(F)$:

$$\mathcal{C}_0 := \{\mathfrak{a} \in \mathrm{Div}(F) \mid \deg \mathfrak{a} = 0\}/\mathrm{Prin}(F).$$

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

Claim 4.2

The mapping $\Phi \colon \mathbb{P}_1(K) \to \mathcal{C}_0$ *given by*

$$\mathfrak{p} \mapsto [\mathfrak{p} - \mathfrak{q}]$$

is a bijection.

Proof.

First, note that $\mathfrak{p} \in \mathbb{P}_1(K) \implies \deg(\mathfrak{p} - \mathfrak{q}) = \deg \mathfrak{p} - \deg \mathfrak{q} = 1 - 1 = 0$.
One to one: Suppose $[\mathfrak{p} - \mathfrak{q}] = [\mathfrak{p}' - \mathfrak{q}]$. Then there exists $z \in F^\times$ s.t. $\mathfrak{p} - \mathfrak{q} = \mathfrak{p}' - \mathfrak{q} + (z)$. Hence $\mathfrak{p} = \mathfrak{p}' + (z)$, so $[\mathfrak{p}] = [\mathfrak{p}']$ and by the previous claim $\mathfrak{p} = \mathfrak{p}'$.

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

Proof.

Onto: Let $[\mathfrak{a}] \in \mathcal{C}_0$. Then $\deg(\mathfrak{a} + \mathfrak{q}) = 1$, so again by Riemann-Roch, $\dim(\mathfrak{a} + \mathfrak{q}) = 1$. Hence there exists $0 \neq z \in \mathcal{L}(\mathfrak{a} + \mathfrak{q})$, i.e. $z \in F^\times$ s.t. $(z) + \mathfrak{a} + \mathfrak{q} \geq 0$. As $\deg((z) + \mathfrak{a} + \mathfrak{q}) = 1$, it must be that $(z) + \mathfrak{a} + \mathfrak{q} = \mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}_1(K)$. Therefore $\mathfrak{p} - \mathfrak{q} = \mathfrak{a} + (z)$, and $[\mathfrak{a}] = [\mathfrak{p} - \mathfrak{q}] = \Phi(\mathfrak{p})$.

The bijection $\Phi \colon \mathbb{P}_1(K) \to \mathcal{C}_0$ can be used to carry over the group structure of $\mathcal{C}_0$ to the set $\mathbb{P}_1(K)$ as follows:

Definition 5

For $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{P}_1(K)$, define

$$\mathfrak{p}_1 \oplus \mathfrak{p}_2 := \Phi^{-1}(\Phi(\mathfrak{p}_1) + \Phi(\mathfrak{p}_2)).$$

Claim 5.1

$(\mathbb{P}_1(K), \oplus)$ is an abelian group with $\mathfrak{q}$ the zero element.
For $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \in \mathbb{P}_1(K)$,

$$\mathfrak{p}_1 \oplus \mathfrak{p}_2 = \mathfrak{p}_3 \iff [\mathfrak{p}_1 + \mathfrak{p}_2] = [\mathfrak{p}_3 + \mathfrak{q}]$$

Proof.

$$\begin{aligned} \mathfrak{p}_1 \oplus \mathfrak{p}_2 = \mathfrak{p}_3 &\iff \Phi^{-1}(\Phi(\mathfrak{p}_1) + \Phi(\mathfrak{p}_2)) = \mathfrak{p}_3 \iff \\ \Phi(\mathfrak{p}_1) + \Phi(\mathfrak{p}_2) = \Phi(\mathfrak{p}_3) &\iff [\mathfrak{p}_1 - \mathfrak{q}] + [\mathfrak{p}_2 - \mathfrak{q}] = [\mathfrak{p}_3 - q] \iff \\ [\mathfrak{p}_1 - \mathfrak{q} + \mathfrak{p}_2 - \mathfrak{q}] = [\mathfrak{p}_3 - \mathfrak{q}] &\iff [\mathfrak{p}_1 + \mathfrak{p}_2] = [\mathfrak{p}_3 + \mathfrak{q}] \end{aligned}$$

□

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

Recall that we also have a bijection $\mathbb{P}_1(K) \to \mathcal{E}(K)$ (with $\mathfrak{q} \mapsto O$), which can be used to get a group structure on $\mathcal{E}(K)$, with O the zero element.

We want to understand this action - what is $(a, b) \oplus (c, d)$?

Key observation: Let $(a, b) \in \mathcal{E}'(K)$ be a point with corresponding $\mathfrak{p} \in \mathbb{P}_1(K)$ (i.e. $\varphi_\mathfrak{p}(x) = a$, $\varphi_\mathfrak{p}(y) = b$). Let ℓ be the line $\alpha X + \beta Y + \gamma = 0$ (where $\alpha, \beta, \gamma \in K$, and $\alpha \neq 0$ or $\beta \neq 0$). Consider the function

$$z := \alpha x + \beta y + \gamma \in F.$$

Then $(a, b) \in \ell$ iff

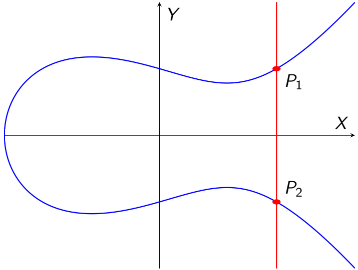
$$\alpha a + \beta b + \gamma = 0 \iff \alpha\varphi_\mathfrak{p}(x) + \beta\varphi_\mathfrak{p}(y) + \gamma = 0 \iff$$
$$\varphi_\mathfrak{p}(\alpha x + \beta y + \gamma) = 0 \iff \varphi_\mathfrak{p}(z) = 0 \iff \nu_\mathfrak{p}(z) > 0 \iff \mathfrak{p} \leq (z)_0.$$

Let us consider two particular cases.

Case 1: Suppose $(a, b) \in \mathcal{E}'(K)$ and $b \neq 0$. Clearly, $(a, -b) \in \mathcal{E}'(K)$ as well.

Claim 5.3

$(a, b) \oplus (a, -b) = O$, *i.e.* $(a, -b) = -(a, b)$.



Proof.

Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{P}'_1(K)$ be the prime divisors corresponding to (a, b) and $(a, -b)$, respectively. We need to show that $\mathfrak{p}_1 \oplus \mathfrak{p}_2 = \mathfrak{q}$, i.e. $[\mathfrak{p}_1 + \mathfrak{p}_2] = [\mathfrak{q} + \mathfrak{q}]$.

Both (a, b) and $(a, -b)$ lie on the line $X - a = 0$, so by the observation the function $z = x - a \in F^\times$ satisfies $(z)_0 \geq \mathfrak{p}_1 + \mathfrak{p}_2$.

Since $(x)_\infty = 2\mathfrak{q}$ we have that $(z)_\infty = (x - a)_\infty = 2\mathfrak{q}$. Therefore $\deg(z)_0 = \deg(z)_\infty = 2$ and $(z)_0 = \mathfrak{p}_1 + \mathfrak{p}_2$. Overall,

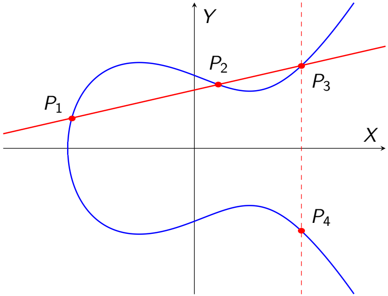
$$(z) = (z)_0 - (z)_\infty = \mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{q} \implies \mathfrak{p}_1 + \mathfrak{p}_2 = 2\mathfrak{q} + (z)$$

so $[\mathfrak{p}_1 + \mathfrak{p}_2] = [2\mathfrak{q}]$ as desired. $\square$

In fact, the claim holds also when $b = 0$. In this case, $\mathfrak{p}_1 = \mathfrak{p}_2$ lies above $\mathfrak{p}_{x-a}$ in $K(x)$, and $(z)_0 = 2\mathfrak{p}_1$. Indeed, as we saw,

$$\nu_{\mathfrak{P}}(x - a) = e(\mathfrak{p}_1/\mathfrak{p}_{x-a}) \cdot \nu_a(x - a) = 2 \cdot 1 = 2.$$

Case 2: Suppose $(a, b), (c, d) \in \mathcal{E}'(K)$ and that the line passing through them intersects $\mathcal{E}'(K)$ in a third (other) point (e, f) (in particular, $a \neq c$).

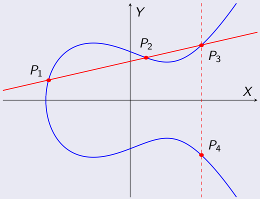


Claim 5.4

$$(a, b) \oplus (c, d) = -(e, f) = (e, -f)$$

Proof.

Let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \in \mathbb{P}'_1(K)$ be the (distinct) prime divisors corresponding to $(a, b), (c, d), (e, f)$ respectively. Since $a \neq c$, the line passing through (a, b) and (c, d) is of the form $\alpha X + \beta Y + \gamma = 0$ with $\beta \neq 0$.



Consider the function $z = \alpha x + \beta y + \gamma \in F^\times$. Note that by the observation, $(z)_0 \geq \mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3$. As for $(z)_\infty$, we have (by the strict triangle inequality) that $(z)_\infty = 3\mathfrak{q}$. Hence $\deg(z)_0 = \deg(z)_\infty = 3$ and $(z)_0 = \mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3$.

Proof.

Now, let $\mathfrak{p}_4 \in \mathbb{P}'_1(K)$ be the prime divisor corresponding to $-(e, f) = (e, -f)$. We saw that $(z) = (z)_0 - (z)_\infty = \mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 - 3\mathfrak{q}$. Adding $\mathfrak{p}_4$ to both sides, we get

$$(z) + \mathfrak{p}_4 = \mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 + \mathfrak{p}_4 - 3\mathfrak{q}. \tag{4}$$

By the proof of the previous claim, we know that $\mathfrak{p}_3 + \mathfrak{p}_4 = 2\mathfrak{q} + (w)$ where $w = x - e \in F^\times$. Substituting this in Equation (4), we obtain

$$(z) + \mathfrak{p}_4 = \mathfrak{p}_1 + \mathfrak{p}_2 + 2\mathfrak{q} + (w) - 3\mathfrak{q}.$$

Since $(z) - (w) = \left(\frac{z}{w}\right)$, this gives

$$\mathfrak{p}_1 + \mathfrak{p}_2 = \mathfrak{p}_4 + \mathfrak{q} + (z/w)\,,$$

i.e. $[\mathfrak{p}_1 + \mathfrak{p}_2] = [\mathfrak{p}_4 + \mathfrak{q}]$ which means $\mathfrak{p}_1 \oplus \mathfrak{p}_2 = \mathfrak{p}_4$, as desired. □