Elliptic Function Fields

Abraham Rojas

ICMC - USP

abraham.rojas@usp.br

Introduction

Let K be a perfect field. An elliptic function field (E.F.F.) is an algebraic function field F/K, with field of constant K, such that

1. the genus of F/K is 1
2. there exists a divisor $D \in \mathrm{Div}(F)$ with $\deg A = 1$.

We assume some facts from the theory of algebraic function fields, whose importance goes beyond the present topic:

- **The Riemann-Roch Theorem** is an essential equation that relates divisors and the genus.
- Most of the theorems that appears in this poster are consequence of the **Hurwitz genus formula**.
- **Ramification of places** is used in calculations, existence proofs and in other situations.

E.F.F when $\mathrm{char}\, K \neq 2$

There exist $x, y \in F$ such that

$$F = K(x, y) \quad \text{and} \quad y^2 = f(x) \qquad \text{(i)}$$

where $f \in K[x]$ is square-free and has degree 3.

Proof. It's easy to show the existence of a place P of degree 1. By Riemann-Roch Theorem $\ell(iP) = i$ for $i > 0$, hence $\mathscr{L}(P) = K$ and $\mathscr{L}((i+1)P) \supsetneq \mathscr{L}(iP)$.
Choose $x_1 \in \mathscr{L}(2P) \setminus K$ and $y_1 \in \mathscr{L}(3P) \setminus \mathscr{L}(2P)$. Then $(x_1)_\infty = 2P$ and $(y_1) = 3P$, so $[F : K(x_j)] = j$, hence $F = K(x_1, y_1)$. Since $\ell(6P) = 6$: $1, x_1, y_1, x_1^2, x_1y_1, x_1^3, y_1^2 \in \mathscr{L}(6P)$ are L.D. over K. Replacing x_1 and y_1 by appropiate multiples, say x_2 and y_2 then $F = K(x_2, y_2)$ and

$$y_2^2 + (\beta x_2 + \gamma)y_2 = x_2^3 + \epsilon x_2^2 + \lambda x_2 + \mu \qquad \text{(ii)}$$

When $\mathrm{char}\, K \neq 2$, we set $y = y_2 + (\beta_2 x_2 + \gamma_2)/2$ and $x = x_2$. Then $F = K(x, y)$ and $y^2 = f(x)$ has degree 3. If f had a zero of multiplicity 2, we can show that F/K is rational, which is impossible.

Conversely, if (i) holds then $F/K(x)$ is a Kummer extension of degree 3. So we can use the following

Theorem 1. *Let F'/F be a Kummer extension of degree n, set $r_p = \gcd(n, v_p(y^n)) > 0$ for $P \in \mathbb{P}_F$. If there exists $Q \in \mathbb{P}_F$ with $r_Q = 1$ then K is alg. closed in F' and*

$$g' = 1 + n(g-1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) \deg P$$

In our case, F is a Kummer extension of $K(x)$. Let $P_i \in \mathbb{P}_F$ be the place of $p_i(x)$, then $v_{P_i}(f(x)) = 1$, also $v_{P_\infty}(f(x)) = -3$, so $r_P = 1$ for all $P \in \mathbb{P}_F$. Therefore the genus of F/K is 1.
Ramification of places can be used to prove the existence of a divisor of degree 1.

Example. Let $\mathcal{M}(\Gamma)$ be set of elliptic functions with respect to the lattice $\Gamma = \mathbb{Z}\gamma_1 \bigoplus \mathbb{Z}\gamma_2$, i.e., meromorphic functions f s.t. $f(z + \gamma) = f(z)$, $\forall \gamma \in \Gamma$. The **Weierstrass $\mathfrak{p}$- function** is

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{0 \neq \gamma \in \Gamma} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right)$$

We have that $\mathcal{M}(\Gamma) = \mathbb{C}(\mathfrak{p}, \mathfrak{p}')$ and $\mathfrak{p}' = 4\mathfrak{p}^3 - a\mathfrak{p} - b \in \mathbb{C}[\mathfrak{p}]$ is square-free. Hence $\mathcal{M}(\Gamma)/\mathbb{C}$ is an E.F.F.

E.F.F when $\mathrm{char}\, K = 2$

There exist $x, y \in F$ such that $F = K(x, y)$ and one the following equations holds

$$y^2 + y = f(x) \in K[x] \quad \text{with } \deg f = 3 \qquad \text{(iii)}$$

$$y^2 + y = x + \frac{1}{ax + b} \quad \text{with } a, b \in K \text{ and } a \neq 0 \qquad \text{(iv)}$$

Proof. (ii) holds. To show $\beta_2 x_2 + \gamma_2 \neq 0$ we use

Proposition 1. *Let F/K be a function field. Then $F^{p^n} := \{z^{p^n} \mid z \in F\}$ is the unique $K \subset L \subset F$ s.t. F/L is purely inseparable of degree p^n. Also $F^{p^n} \simeq F$ (Frobenius map).*

Now, set $y_3 = y_2(\beta_2 x_2 + \gamma_2)^{-1}$, then $F = K(x_2, y_3)$. If $\beta = 0$, equation (ii) has the form (iii). If $\beta \neq 0$, equation (ii) has the form

$$y_3^3 + y_3 = \nu x_2 x_2 + \rho + \frac{\sigma}{(\beta_2 x_2 + \gamma_2)^2} + \frac{\tau}{\beta_2 x_2 + \gamma_2} \qquad \text{(v)}$$

with $\nu \neq 0$. As K is perfect, $\sigma = \sigma_1^2$ for some σ_1^2. Set $y = y_3 + \sigma_1(\beta_2 x_2 + \gamma_2)^{-1}$. This makes equation (v) to have the form (iv) (as before, one uses that F/K is not rational).

Conversely, if (iii) or (iv) holds then $F/K(x)$ is an Artin-Schreier extension of degree 2. So we can use the following

Theorem 2. *Let F'/F be an Artin-Schreier extension with $\mathrm{char}\, K = p > 0$. For $P \in \mathbb{P}_F$ define*

$$m_P := \begin{cases} m & \text{if } \exists z \in F \text{ s.t. } p \nmid v_P(u - (z^p - z)) = -m < 0 \\ -1 & \text{if } \exists z \in F \text{ s.t. } v_P(u - (z^p - z)) \geq 0 \end{cases}$$

If there is $Q \in \mathbb{P}_F$ with $m_Q > 0$ then K is alg.closed in F' and

$$g' = p \cdot g + \frac{p-1}{2} \left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P \right)$$

We proceed as in the previous case to finish the proof.

The group law

Proposition 2. *Let $F = K(x, y)$ be an elliptic function field and let $\mathbb{P}_F^{(1)}$ be the set of places of degree 1, then:*

- *For each $A \in Div(F)$ s.t. $\deg A = 1$ there exists a unique place with $A \sim P$. In particular $\mathbb{P}_F^{(1)} \neq \emptyset$.*
- *If we fix $P_0 \in \mathbb{P}_F^{(1)}$ then we have a bijection*

$$\Phi : \begin{cases} \mathbb{P}_F^{(1)} \longrightarrow \mathrm{Cl}^0(F) \\ P \longmapsto [P - P_0] \end{cases}$$

where $Cl^0(F) = \{[A] \in Cl(F) \mid \deg A = 0\}$ ($Cl(F)$ is the divisor class group of F/K).

Now, for $P, Q \in \mathbb{P}_F^{(1)}$, we can define

$$P \oplus Q = \Phi^{-1}(\Phi(P) + \Phi(Q))$$

This operation turns $\mathbb{P}_F^{(1)}$ into an abelian group, isomorphic to $Cl^0(F)$, with zero element P_0.

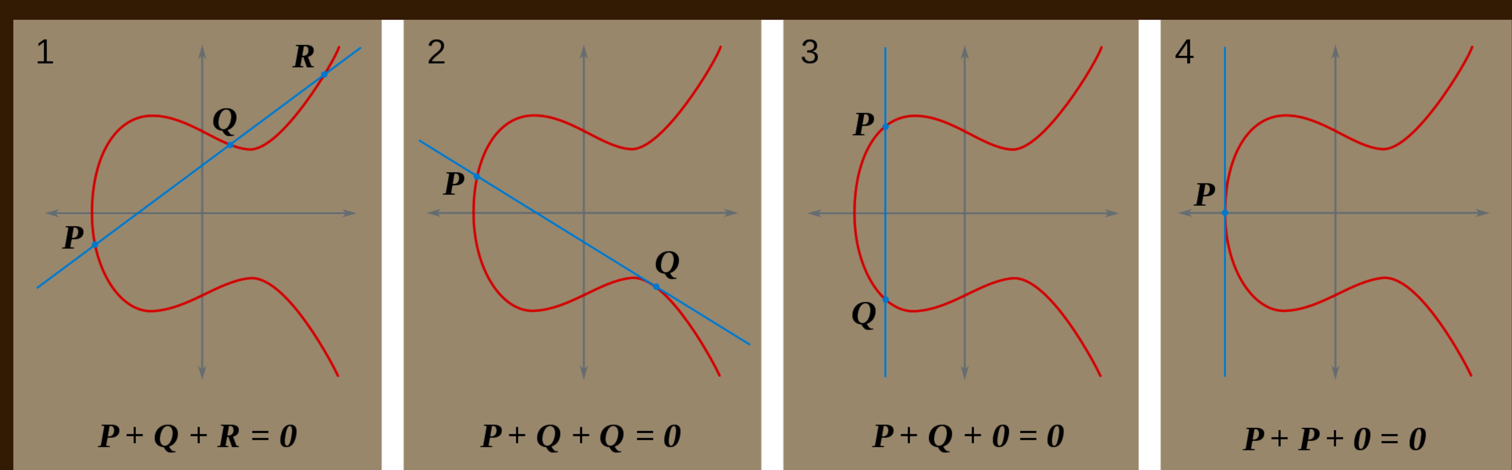

Figure 1: The group law as in [1].

References

[1] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2nd edition, 2009.

[2] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, 1st edition, 2010.