# 8. The associative law

$\boxed{\text{Let } L \text{ be an AFF over } K \text{ of genus } g}$

**Proposition 8.1** Let $\mathbb{P}^{(1)}_{L|K} \neq \emptyset$. Then

$$g = 0 \iff \exists\, s \in L \text{ such that } L = K(s).$$

**Proof:** ($\Rightarrow$) Let $P \in \mathbb{P}^{(1)}_{L|K} \overset{2.6(2)}{\Longrightarrow} \ell(1 \cdot P) = \overbrace{\deg P}^{=1} + 1 - \overset{0}{g} = 2$

$7.9(1) \Rightarrow \ell(0) = 1 \Rightarrow \exists\, s \in \mathcal{L}(1P) \setminus \mathcal{L}(0 \cdot P) \overset{7.9(2)}{\Longrightarrow} (s)_- = 1P$

$\overset{6.5}{\Longrightarrow} [L : K(s)] = \deg((s)_-) = 1 \Rightarrow L = K(s)$.

($\Leftarrow$) follows from Example 7.10

**Definition** An AFF $L$ is called an *elliptic function field* (EFF) if it is of genus 1 and $\mathbb{P}^{(1)}_{L|K} \neq \emptyset$.

**Lemma 8.2** Let $L$ be an EFF and $P \in \mathbb{P}^{(1)}_{L|K}$. Then

(1) $L$ is full constant and $\mathcal{L}(1P) = K$,

(2) $\mathcal{L}(2P) \setminus \mathcal{L}(1P) \neq \emptyset \neq \mathcal{L}(3P) \setminus \mathcal{L}(2P)$,

(3) $\forall u \in \mathcal{L}(2P) \setminus \mathcal{L}(1P)$, $\forall v \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$ $\exists$ WEP $w \in K[x,y]$ and $\exists \lambda \in K^*$ such that $L$ is given by $w(\lambda u, \lambda v) = 0$.

proof: (1) follows from 7.9(1).

(2) by (1) & 7.6(2) $\ell(iP) = \deg(iP) = i \;\; \forall i \geq 1$

$\Rightarrow \ell(1P) < \ell(2P) < \ell(3P) < \dots \Rightarrow \mathcal{L}(1P) \subsetneqq \mathcal{L}(2P) \subsetneqq \mathcal{L}(3P) \subsetneqq \dots$

(3) by 7.9(3) $(u)_- = 2P$ & $(v)_- = 3P \overset{6.5}{\Longrightarrow} \begin{cases} [L : K(u)] = 2 \\ [L : K(v)] = 3 \end{cases}$

Since $(u^2)_- = 2(u)_- = 4P$, $(uv)_- = (u)_- + (v)_- = 5P \Rightarrow$
$B = \{1, u, v, u^2, uv\}$ is a basis of $\mathcal{L}(5P)$ (of dimension 5)

$(u^3)_- = 3(u)_- = 6P = (v^2)_- \overset{\text{Rg}(8)}{\Longrightarrow}$ $\left.\begin{array}{l} B \cup \{u^3\} \\ B \cup \{v^2\} \end{array}\right\}$ are bases of $\mathcal{L}(6P)$

$\overset{\text{linear}}{\underset{\text{algebra}}{\Longrightarrow}}$ $\exists c, d \in K^* \ \exists b_1, b_2, b_3, b_4, b_6 \in K$ such that

$$c v^2 + b_1 u v + b_3 v = d u^3 + b_2 u^2 + b_4 u + b_6 \qquad (+)$$

Let $\boxed{\lambda := \frac{d}{c}}$ and multiply $(+)$ by $\frac{d^2}{c^3}$, then

for $w := y^2 + \frac{b_1}{c} xy + \frac{d b_3}{c^2} y - \left(x^3 + \frac{b_2}{c} \cdot x^2 + \frac{b_4 d}{c^2} \cdot x + \frac{b_6 d^2}{c^3}\right)$ $\in K[x,y]$

an WEP it holds $w(\lambda u, \lambda v) = 0$

$4.9 \Rightarrow w$ is irreducible $\Rightarrow [K(\lambda u, \lambda v) : K(\lambda u)] = \deg_y w = 2$

Since $[L : K(\lambda u)] = [L : K(u)] = 2$ $\Rightarrow L = K(\lambda u, \lambda v)$

**Proposition 8.3** Let $w\in K[x,y]$ be $^{g}$WCP and $L$ be given by $w(\alpha,\beta)=0$. Then

(1) $\exists!\ P=P_\infty\in\mathbb{P}_{L|K}$ such that $v_P(\alpha)<0$ or $v_P(\beta)<0$,

(2) $K[\alpha,\beta]\subseteq\mathcal{O}_Q\quad\forall Q\in\mathbb{P}_{L|K}\setminus\{P_\infty\}$

(3) $P_\infty\in\mathbb{P}^{(1)}_{L|K}$, $(\alpha)_-=2P_\infty$, $(\beta)_-=3P_\infty$,
$P_\infty\cap K[V_w]=P_\infty\cap K[\alpha,\beta]=0$, $\mathcal{O}_{P_\infty}\cap K[\alpha,\beta]=K$,

(4) if $w$ is smooth at $V_w(K)$ $\Rightarrow$ $\mathbb{P}^{(1)}_{L|K}=\{P_\infty\}\cup\{P_\gamma\mid\gamma\in V_w(K)\}$

(5) $L$ is either an EFF (if $g=1$) or
$\exists\, s\in L$ such that $L=K(s)$ (if $g=0$)

(6) if $L=K(s)$ $\Rightarrow$ $\exists\, a,b\in K[x]$, $\deg a=2$, $\deg b=3$: $\alpha=a(s)$, $\beta=b(s)$.

<u>proof of 8.3</u>: (1)–(3) follows from 5.15 & 5.23

(4) $5.17 \Rightarrow \mathbb{P}^{(1)}_{L|k} \subseteq \{P_\infty\} \cup \{P_x \mid x \in V_w(k)\}$, $(3) \Rightarrow P_\infty \in \mathbb{P}^{(1)}_{L|k}$

Let $x \in V_w(k)$, $5.13(2) \Rightarrow P_x \in \mathbb{P}_{L|k}$, $\mathcal{O}_x \subseteq \mathcal{O}_{P_x}$, $\dim_k \mathcal{O}_x/P_x = 1$

Let $a, b \in k[\alpha,\beta] - \{0\}$ such that $\frac{a}{b} \in \mathcal{O}^*_{P_x} = \mathcal{O}_{P_x} \setminus P_x \Rightarrow$

$\Rightarrow r := v_{P_x}(a) = v_{P_x}(b) \overset{5.13(1)}{\Longrightarrow} \exists u \in P_x : \frac{a}{u^r}, \frac{b}{u^r} \in \mathcal{O}^*_x \Rightarrow \frac{a}{b} \in \mathcal{O}^*_x$

$\Rightarrow \mathcal{O}_x = \mathcal{O}_{P_x} \Rightarrow \deg P_x = \dim \mathcal{O}_x/P_x = 1 \Rightarrow P_x \in \mathbb{P}^{(1)}_{L|k}$

(5) Note that $\forall r \geq 2\ \exists i, j \geq 0 : 2i + 3j = r$ & $(\alpha^i\beta^j)_- = (2i+3j)P_\infty$

$\overset{7.9(4)}{\Longrightarrow} g \leq 1 \Rightarrow$ the rest follows from 8.1

(6) $8.1 \Rightarrow g = 0 \Rightarrow 1, \dots, s^i$ is a basis of $\mathcal{L}(iP_\infty)$ by the argument
$i \geq 1$ of the proof of 8.2

$\alpha \in \mathcal{L}(2P_\infty) - \mathcal{L}(1P_\infty)$, $\beta \in \mathcal{L}(3P_\infty) - \mathcal{L}(2P_\infty) \Rightarrow \exists a_i, b_i \in k : a_2 \neq 0, b_3 \neq 0$
such that $\alpha = \sum^2 a_i s^i$, $\beta = \sum^3 b_i s^i$

In the sequel $w = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$ is a WEP

Theorem 8.4: Let $L$ be given by $w(\alpha,\beta) = 0$. Then

$L$ is an EFF $\Leftrightarrow$ $w$ is smooth at $V_w(K)$.

Proof: ($\Rightarrow$) Note that $\mathbb{P}^{(1)}_{L|K} \neq \emptyset$ by 8.3. Suppose $w$ is singular

W.l.o.g. by 3.10 we may suppose $w$ is singular at $(0,0) \in V_w$

$\Rightarrow \Delta_{(0,0)} \overset{3.8}{=} L(w) = 0 \Rightarrow w = y^2 + a_1xy - x^3 - a_2x^2$ (i.e. $\mathrm{mult}\, w = 2$)

Put $\boxed{s := \frac{\beta}{\alpha}} \Rightarrow 0 = \frac{w(\alpha,\beta)}{\alpha^2} = s^2 + a_1 s - \alpha - a_2 \Rightarrow$

$\Rightarrow \alpha = s^2 + a_1 s - a_2 \in K(s)$ & $\beta = \alpha s \in K(s) \Rightarrow$

$\Rightarrow L = K(s) \overset{8.3(5)}{\Longrightarrow}$ $L$ is not elliptic

($\Leftarrow$) Let $w$ is not elliptic $\overset{8.3(5),(6)}{\Longrightarrow} \exists s \in L : L = K(s)$

& $\exists\, u, v \in K[x]$ $\deg u = 2$, $\deg v = 3$ & $\alpha = u(s)$, $\beta = v(s)$

Let $u = \sum^{2} u_i x^i$, $v = \sum^{3} v_i x^i$. Then by 3.4 $\boxed{3.10}$ (when $c := \frac{u_2}{v_3}$) we may assume w.l.o.g $u_2 = v_3 = 1$, (for suitable $a$ in 3.4) $u_1 = v_2$, and (choosing suitable $b$ in 3.4) $v_1 = u_0$ & $v_0 = 0$

$\Rightarrow v = x u \Rightarrow \beta = \alpha \Delta \Rightarrow$

$$w(\alpha, \beta) = w(\alpha, \alpha\Delta) = \alpha^2\Delta^2 + a_1\alpha^2\Delta + a_3\alpha\Delta - (\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6)$$

$$\Rightarrow L(\Delta) = \alpha^2(\Delta^2 + a_1\Delta - \alpha - a_2) = \overbrace{-a_3\alpha\Delta + a_4\alpha + a_6}^{R(\Delta)} \in K[\Delta]$$

$\Delta$ is transcendental $\Rightarrow K[\Delta] \cong_K K[x]$

$$\left.\begin{array}{l} ??\ L(\Delta) \neq 0 \Rightarrow \deg_\Delta L(\Delta) \geq 4 \\ \deg_\Delta R(\Delta) \leq 3 \end{array}\right\} \Rightarrow \text{a contradiction}$$

$\Rightarrow L(\Delta) = R(\Delta) = 0 \Rightarrow a_3 = a_4 = a_6 = 0 \Rightarrow w$ is singular at $(0, 0)$.

Example 8.5 (1) Let $f = y^2 + y - (x^3+1) \in \mathbb{F}_2[x]$

$f$ is WEP smooth at $V_f(\mathbb{F}_2)$ by 8.24

$\xRightarrow{8.4}$ $\mathbb{F}_2(V_f)$ is of genus 1 $\xRightarrow{8.3}$ $\forall s \in \mathbb{F}_2(V_f): [\mathbb{F}_2(V_f):\mathbb{F}_2(s)] > 1$

(2) Let $f = y^2 - (x^3 + x + 1) \in \mathbb{F}_2[x]$ be a WEP

Since $f$ is singular at $(1,1)$ $\xRightarrow{8.4,\ 8.3(5)}$ $\mathbb{F}_2(V_f)$ is of genus 0

$\xRightarrow{8.2}$ $\exists s \in \mathbb{F}_2(V_f): \mathbb{F}_2(s) = \mathbb{F}_2(V_f)$