8. The associative law

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

Comment: Using Ex. 7.10 we show that of genus 0 are exactly fields $\cong K(x) \ncong K(\text{lines})$

Proposition 8.1: Let $\mathbb{P}^{(1)}_{L|K} \neq \emptyset$. Then $g = 0 \iff \exists \alpha \in L$ such that $L = K(\alpha)$.

Proof ($\Rightarrow$) Let $P \in \mathbb{P}^{(1)}_{L|K} \overset{7.6(2)}{\Longrightarrow} \ell(1P) = \overbrace{\deg_K P}^{=1} + 1 - \overbrace{g}^{=0} = 2$ & $\ell(0) = 1$ by 7.9(1)

$\Rightarrow \exists \alpha \in \mathcal{L}(1P) - \mathcal{L}(0P) \overset{7.9(2)}{\Longrightarrow} (\alpha)_- = 1P \overset{6.5}{\Longrightarrow} [L:K(\alpha)] = \deg_K((\alpha)_-) = 1$

($\Leftarrow$) follows from Example 7.10. $\qquad \Rightarrow L = K(\alpha)$

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

Comment: We will work on the proof that EFFs are exactly AFFs given by non-singular WEP.

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

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

Comment: To construct "generators" α, β of AFF/EFF it is enough to choose arbitrary $\alpha \in \mathcal{L}(2P) - \mathcal{L}(1P)$ & $\beta \in \mathcal{L}(3P) - \mathcal{L}(2P)$

Proof: (1) follows from 7.9(1)

(2) by (1) & 7.6(2) $\ell(iP) = \deg_K(iP) = i \ \forall i \geq 1 \Rightarrow \ell(1P) < \ell(2P) < \ell(3P) < \dots \Rightarrow \mathcal{L}(1P) \subsetneq \mathcal{L}(2P) \subsetneq \mathcal{L}(3P)$.

(3) by 7.9(3): $(\mu)_- = 2P$, $(\nu)_- = 3P \overset{6.5}{\Longrightarrow} [L:K(\mu)] = 2$, $[L:K(\nu)] = 3$

$(\mu^2)_- = 2(\mu)_- = 4P$, $(\mu\nu)_- = (\mu)_- + (\nu)_- = 5P \Rightarrow B = \{1, \mu, \nu, \mu^2, \mu\nu\}$ is LI in $\mathcal{L}(5P)$

As $\dim_K \mathcal{L}(5P) = \ell(5P) = 5$, B is a basis of $\mathcal{L}(5P)$

Comment: The proof is only "linear algebra upon Riemann-Roch spaces"

$(\mu^3)_- = 3(\mu)_- = 6P = 2(\nu)_- = (\nu^2)_- \overset{7.9(2)}{\Longrightarrow} B \cup \{\mu^3\}$ and $B \cup \{\nu^2\}$ are bases of $\mathcal{L}(6P)$

$\overset{\text{linear algebra}}{\Longrightarrow} \exists c, d \in K^*, \exists b_1, b_2, b_3, b_4, b_6 \in K$: $c\nu^2 + b_1\mu\nu + b_3\nu = d\mu^3 + b_2\mu^2 + b_4\mu + b_6$ (*)

Let $\boxed{\lambda = \frac{d}{c}}$ and let multiply the equation (*) by $\frac{d^2}{c^3} \Rightarrow w(\lambda\mu, \lambda\nu) = 0$ for the WEP $w := y^2 + \frac{b_1}{c}xy + \frac{d b_3}{c^2} y - \left(x^3 + \frac{b_2}{c}x^2 + \frac{b_4 d}{c^2}x + \frac{b_6 d^2}{c^3}\right) \in K[x,y]$

4.9 $\Rightarrow$ w is (absolutely) irreducible $\Rightarrow [K(\lambda\mu, \lambda\nu) : K(\lambda\mu)] = \deg_y w = 2$

Since $[L : K(\lambda\mu)] = [L : K(\mu)] \Rightarrow L = K(\lambda\mu, \lambda\nu)$

Proposition 8.3 Let $w \in K[x,y]$ be a WEP and L be given by $w(\alpha, \beta) = 0$

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

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

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

Comment: (1)-(3) recapitulate main results of the chapter 5

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

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

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

Proof : (1)-(3) follows from 5.15 & 5.23

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

Let $x \in V_w(K)$, then 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 $\frac{a}{b} \in \mathcal{O}^*_{P_x} = \mathcal{O}_{P_x} \setminus P_x$ $\Rightarrow$ $k := v_{P_x}(a) = v_{P_x}(b)$

$\overset{5.13(1)}{\Longrightarrow}$ $\exists\, u \in P_x$: $\frac{a}{u^k}, \frac{b}{u^k} \in \mathcal{O}^*_x$ $\Rightarrow$ $\frac{a}{b} = \left(\frac{a}{u^k}\right)\cdot\left(\frac{b}{u^k}\right)^{-1} \in \mathcal{O}^*_x$ $\Rightarrow$ $\mathcal{O}_x = \mathcal{O}_{P_x}$

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

Comment: Places of degree one 1-1 corresponds to rational points of the curve + ∞

(5) $\forall k \geq 2$ $\exists\, i, j \geq 0$: $2i + 3j = k$ $\Rightarrow$ $(\alpha^i \beta^j)_- = (2i+3j) P_\infty = k P_\infty$ by (3)

$\overset{2.9(4)}{\Longrightarrow}$ $g \leq 1$, by 8.1 [& (3)]. $g = 0 \Leftrightarrow \exists\, s : L = K(s)$ $\Rightarrow$ L is EFF otherwise

(6) 8.1 $\Rightarrow$ $g = 0$ $\Rightarrow$ $\{1, s\}$ is a basis of $\mathcal{L}(1P_\infty)$, $\{1, s, s^2\}$ of $\mathcal{L}(2P_\infty)$, $\{1, s, s^2, s^3\}$ of $\mathcal{L}(3P_\infty)$

Since $\alpha \in \mathcal{L}(2P_\infty) - \mathcal{L}(1P_\infty)$, $\beta \in \mathcal{L}(3P_\infty) - \mathcal{L}(2P_\infty)$ (cf. the proof of 8.2)

$\exists\, a_0, a_1, \overset{\neq 0}{a_2} \in K$, $b_0, b_1, b_2, \overset{\neq 0}{b_3} \in K$: $\alpha = \sum_{i=0}^{2} a_i s^i$, $\beta = \sum_{i=0}^{3} b_i s^i$

In the sequel $w = y^2 + a_1 xy + a_3 y - (x^3 + a_2 x^2 + a_4 x + a_6) \in K[x,y]$ is a WEP

Theorem 8.4 Let L be given by $w(\alpha,\beta) = 0$. L is an EFF $\Leftrightarrow$ w is smooth at $V_w(K)$

Proof: ($\Rightarrow$) $\mathbb{P}^{(1)}_{L|K} \neq \emptyset$ by 8.3. Suppose w is singular, w.l.o.g. by 3.10 we may assume that w is singular at $(0,0) \in V_w$

Comment: We can shift singularity by 3.10

$\Rightarrow$ $A_{(0,0)} \overset{3.8}{=} L(w) = 0$ $\Rightarrow$ $w = y^2 + a_1 xy - x^3 - a_2 x^2$ (i.e. mult $w = 2$)

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

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

Comments: For the reverse implication we will reverse the idea of ($\Rightarrow$) by choosing equivalent WEP describing singularity in clear way

($\Leftarrow$) Let w is not elliptic (we prove again indirectly)

8.3(5),(6) $\Rightarrow$ $\exists\, s \in L$: $L = K(s)$ & $\exists\, u(x), v(x)$ $K[x]$ $\alpha = u(s)$, $\beta = v(s)$, $\deg u = 2$, $\deg v = 3$; $u = \sum u_i x^i$, $v = \sum v_i x^i$

By 3.4 (& 3.10) we may assume w.l.o.g. that $u_2 = v_3 = 1$ (for $c := \frac{u_2}{v_3}$ from 3.4),

$u_1 = v_2$ (for suitable d in 3.4) and $v_1 = u_0$, $v_0 = 0$ (for suitable b in 3.4)

$\Rightarrow$ $v = xu$ $\Rightarrow$ $\beta = \alpha s$ $\Rightarrow$ $w(\alpha,\beta) = w(\alpha, \alpha s) = \alpha^2 s^2 + a_1 \alpha^2 s + a_3 \alpha s - (\alpha^3 + a_2 \alpha^2 + a_4 \alpha + a_6)$

$\Rightarrow$ $L(s) := \alpha^2 (s^2 + a_1 s - \alpha - a_2) = -a_3 \alpha s + a_4 \alpha + a_6 =: R(s) \in K[s] \cong K[x]$ as s is transcendental

?? $L(s) \neq 0$ $\Rightarrow$ $\deg_s L(s) \geq 4$ & $\deg_s(R) \leq 3$ $\Rightarrow$ a contradiction $\Rightarrow$ $R(s) = 0$ $\Rightarrow$ $a_3 = a_4 = a_6 = 0$ $\Rightarrow$ w singular at $(0,0)$

Example 8.5 (1) $f = y^2 + y + (x^3 + 1) \in \mathbb{F}_2[x]$ (5.24) $\overset{8.4}{\Longrightarrow}$ $\mathbb{F}_2(V_f)$ is genus 1

(2) $f = y^2 - (x^3 + x + 1) \in \mathbb{F}_2[x]$ is singular at $(1,1)$ $\Rightarrow$ — " — $0 = F(s)$ for some s