

Recall that  $\deg: \text{Div}(L/k) \rightarrow \mathbb{Z}$  is a group homomorphism and that  $\text{Princ}(L/k) \stackrel{(2.5)}{\subseteq} \ker(\deg) \subseteq \text{Div}(L/k)$ .

**T&N**  $\text{Pic}^0(L/k) := \ker(\deg) / \text{Princ}(L/k)$  is called the Picard group. Denote  $[A] := A + \text{Princ}(L/k) \in \text{Pic}^0(L/k)$   
(the coset given by  $A$ )

Lemma 8.6 Let  $L$  be an EFF over  $k$ ,  $P_1, P_2, Q \in \mathbb{P}_{L/k}^{(1)}$   
and  $A \in \text{Div}(L/k)$ . Then

- (1) if  $P_1 - P_2 \in \text{Princ}(L/k) \Rightarrow P_1 = P_2$ ,
- (2) if  $\deg A = 1 \Rightarrow \exists! P \in \mathbb{P}_{L/k}^{(1)} : P - A \in \text{Princ}(L/k)$ ,
- (3) The mapping  $\psi_Q: \mathbb{P}_{L/k}^{(1)} \rightarrow \text{Pic}^0(L/k)$  defined by the rule  $\psi_Q(P) := [P - Q]$  is a bijection.

proof: Note that  $\deg A \geq 1 \stackrel{2.6(a)}{\Rightarrow} \ell(A) = \deg(A)$

(1) ??  $\lambda \in L \cdot K : P_1 = P_2 + (\lambda) \stackrel{\text{definition}}{\Rightarrow} \lambda, 1 \in \mathcal{L}(1P_2)$  are LI  $\Rightarrow$

$\Rightarrow \ell(1P_2) = \dim_K(\mathcal{L}(1P_2)) \geq 2 > \dim_K(1P_2) = 1 \Rightarrow$  a contradiction

$\Rightarrow P_1 = P_2$

(2) existence: (a) if  $A \geq 0, \deg A = 1 \Rightarrow \exists P \in \mathbb{P}_{L/K}^{(1)} : A = 1P \checkmark$

(b) Let  $A$  is general such that  $\deg A = 1 \stackrel{\text{def.}}{\Rightarrow} \exists \lambda \in L^* : \lambda \in \mathcal{L}(A)$

$\stackrel{\text{def.}}{\Rightarrow} A + (\lambda) \geq 0 \stackrel{(a)}{\Rightarrow} \exists P \in \mathbb{P}_{L/K}^{(1)} : A + (\lambda) = P \Rightarrow$

uniquely if  $A - P_1, A - P_2 \in \text{Prime}(L/K) \quad P - A = (0) \in \text{Prime}(L/K)$

$\Rightarrow P_1 - P_2 \in \text{Prime}(L/K) \stackrel{(1)}{\Rightarrow} P_1 = P_2$

(3) injectivity if  $\psi_Q(P_1) = \psi_Q(P_2) \stackrel{(a)}{\Rightarrow} [P_1 - P_2] = [0]$   
 $\stackrel{(a)}{\Rightarrow} P_1 = P_2$

Surjectivity if  $B \in \text{Der}(L/k)$  such that  $\deg B = 0 \Rightarrow$   
 $\deg(Q+B) = 1 \stackrel{(2)}{\Rightarrow} \exists ! P \in \mathbb{P}_{L/k}^{(1)} : P - (B+Q) \in \text{Princ}(L/k)$

T&W Let  $L$  be an EFF,  $Q \in \mathbb{P}_{L/k}^{(1)}$ , we define an operation  
 $\oplus$  on  $\mathbb{P}_{L/k}^{(1)} : P_1 \oplus P_2 := \gamma_Q^{-1}(\gamma_Q(P_1) + \gamma_Q(P_2))$  for  $P_1, P_2 \in \mathbb{P}_{L/k}^{(1)}$   
 $\Rightarrow \gamma_Q(P) = [P-Q] = [B]$

Observation Let  $L$  be an EFF over  $k$ ,  $Q, P_0, P_1, \dots, P_n \in \mathbb{P}_{L/k}^{(1)}$   
 and  $\gamma_Q$  as in 8.6(3). Then:

- (1)  $\mathbb{P}_{L/k}^{(1)}$  forms an abelian group with  $\oplus$  a neutral element  $Q$ ,
- (2)  $\gamma_Q$  is a group isomorphism,
- (3)  $P_1 \oplus P_2 = P_3 \Leftrightarrow [P_1 + P_2] = [P_3 + Q]$ ,
- (4)  $P_1 \oplus \dots \oplus P_n = P_0 \Leftrightarrow -P_0 + (1-n)Q + \sum_{i=1}^n P_i \in \text{Princ}(L/k)$

**TXN** | Let  $\hat{l} = cx + dy + e \in K[x, y]$  for  $c, d, e \in K$  4  
 $(c, d) \neq (0, 0)$

Then  $l = \hat{l} + (w) = \hat{l}(\alpha, \beta) \in K[V_w] = K[\alpha, \beta]$  for  $\alpha = x + (w)$ ,  
 $\beta = y + (w)$

is called a line on  $V_w$  represented by  $\hat{l}$ , we say  
 that l passes through  $\mathcal{P} \in V_w$  if  $\mathcal{P} \in V_{\hat{l}}$ .

Lemma 8.7 Let  $w = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$   $= f(x)$   
 a smooth WEP of  $V_w(k)$ ,  $\mathcal{P} = (P_1, P_2) \in V_w(k)$  and  $\hat{l} \in K[x, y]$   
 represents a line  $l = \hat{l} + (w) \in K[V_w]$ .

(1) if  $\hat{l} = x - P_1 \Rightarrow \exists! \mathcal{D} = (D_1, D_2) \in V_w(k)$  such that  $(l) = P_{\mathcal{P}} + P_{\mathcal{D}} - 2P_{\infty}$   
 and  $\boxed{D_2 = -a_1P_1 - a_3 - P_2}$

(2) if  $\hat{l} = y - \lambda x - \mu$  for  $\lambda, \mu \in K$  and  $l$  passes through  $\mathcal{P}$  then  
 $(l) = 3P_{\infty}$  and either:

(a)  $\exists P \in P_{w,k} : \deg_0 P = 2$  and  $(l)_+ = P_{\mathcal{P}} + P$ ,  $\hat{l} \notin (d_{\mathcal{P}}(w))$ , and  $\leftarrow$  (tangent at  $\mathcal{P}$ )  
 $V_w(k) \cap V_{\hat{l}} = \{\mathcal{P}\}$

$\sigma_2(k) \exists \sigma = (\sigma_1, \sigma_2), \eta = (\eta_1, \eta_2) \in V_w(k) : (L)_+ = P_\eta + P_\sigma + P_\gamma$

$V_w \cap V_{\hat{L}} = \{\gamma, \sigma, \eta\}, \eta_1 = \gamma_1 - \sigma_1 - a_2 + 1^2 + a_1 \cdot 1$ , and

$\hat{L} \in (L_x(w)) \Leftrightarrow \gamma \in \{\sigma, \eta\}$

Proof: Recall:  $\alpha = x + (w), \beta = y + (w), L = \hat{L}(\alpha, \beta) \in K[V_w] = K[x, y]$   
and  $K(\alpha, \beta) = L$ .

(1) By 8.3:  $(L)_- = (\alpha - \gamma_1)_- \stackrel{(v_p(\gamma_1)=0 \vee p)}{=} (\alpha)_- \stackrel{8.3(5)}{=} 2P_\infty$

by 8.8  $P_\gamma \leq (L)_+$  as  $\hat{L}(\gamma) = 0$ , by 8.3(4):  $\deg P_\gamma = 1$

$\stackrel{6.5}{\Rightarrow} \exists! P \in \mathbb{P}_{L/K}^{(1)} : (L)_+ = P_\gamma + P \stackrel{8.3(4)}{\Rightarrow} \exists! \sigma = (\sigma_1, \sigma_2) \in V_w(k) :$

$P = P_\sigma \Rightarrow (L)_+ = P_\gamma + P_\sigma \Rightarrow$

$\Rightarrow P_\sigma \leq (L)_+ \stackrel{8.8}{\Rightarrow} \sigma \in V_{\hat{L}} \Rightarrow \boxed{\sigma_1 = \gamma_1}$

Since  $w(\gamma) = 0 = w(\sigma) \exists \lambda \in K$  such that  $\sigma_2, \gamma_2$  are roots of  $\lambda^2 + a_1 \gamma_1 \lambda + a_3 \lambda + 1 \in K[\lambda] \Rightarrow \boxed{\sigma_2 + \gamma_2 = -a_1 \gamma_1 - a_3}$

(2) Again by 8.3(4) & 5.8:  $(\mathcal{L})_- = 3P_\infty$  and  $P_x \leq (\mathcal{L})_+$

Then by 6.5

- either (a):  $(\mathcal{L})_+ = P_x + P$  for  $P \in \mathcal{P}_{\mathcal{L}(k)}$  of degree  $\geq 2 \Rightarrow$   
 $\Rightarrow P_\sigma \not\leq (\mathcal{L})_+ \forall \sigma \in V_m(k) - \{P\} \Rightarrow V_m(k) \cap V_2 = \{P\}$

- or (b)  $(\mathcal{L})_+ = P_x + P_\sigma + P_\eta$  for some  $\sigma = (\sigma_1, \sigma_2), \eta = (\eta_1, \eta_2) \in V_m(k)$

Note:

~~if~~  $\mathcal{L} \in (\mathcal{L}_x(m)) \xleftrightarrow{5.8} 2P_x \leq (\mathcal{L})_+ \Leftrightarrow \mathcal{L} \in \{\sigma, \eta\}$   
(which is impossible in the case (a))

Let  $w = \eta_1^2 + a_1 \eta_1 + a_2 \eta_2 = f(x)$  with  $f(x) = x^2 + a_2 x^2 + a_1 x + a_0$

Suppose (b):  $(\mathcal{L})_+ = P_x + P_\sigma + P_\eta$  and  $\mu \in K[\mathcal{L}]$

$$g(\mathcal{L}) = -w(\mathcal{L}, \mathcal{L} + \mu) = f(\mathcal{L}) - (\mathcal{L} + \mu)^2 - a_1(\mathcal{L} + \mu) - a_2(\mathcal{L} + \mu)$$

cf  $P \in \{\sigma_1, \sigma_2, \eta_1\}$  or  $(P, \mathcal{L}) \in V_m \cap V_2 \Rightarrow g(P) = 0$  deg g = 3

if  $|R| = 3$  or (if  $|R| < 3 \Rightarrow \hat{z} \in (\Delta, \mathbb{R})$  for some  $\xi \in R \Rightarrow \frac{\partial \sqrt{\xi}}{\partial \xi}(\hat{z}) \neq 0$ )  
 by 8.9  $\Rightarrow$  The multiplicity of the root  $\rho \in \{\gamma_1, \delta_1, \eta_1\}$  is

equal  $\nu_{\rho}^{\text{hor}}$  for the corresponding  $\rho \in \{P_{\gamma_1}, P_{\delta_1}, P_{\eta_1}\}$

$\Rightarrow \{\gamma_1, \delta_1, \eta_1\}$  are exactly all roots of the monic polynomial  $g(x)$

$\Rightarrow$  the coefficient of  $x^2$  of  $g$  is  $\boxed{-(\alpha_1 + \beta_1 + \gamma_1) = a_2 - x^2 - a_1 x}$

Definition: Let  $w$  be a smooth WEP and  $L$  be an EFF (given by  $w(\alpha, \beta) = 0$ ). Consider the group structure on

$\mathbb{P}_{L|K}^{(1)}$  determined by  $\Psi_{P_{\infty}}$  from 8.6(3). Put  $E(K) := V_w(K) \cup \{\infty\}$

and define operations  $\oplus$  and  $\ominus$  on  $E(K)$ ;  $\gamma, \delta, \eta \in E(K)$ :

$$\boxed{\gamma \oplus \delta = \eta} \stackrel{\text{def}}{=} P_{\gamma} \oplus P_{\delta} = P_{\eta} \stackrel{\text{obs. (5)}}{\Leftrightarrow} [P_{\gamma} + P_{\delta}] = [P_{\eta} + P_{\infty}]$$

$$\boxed{\ominus \gamma = \delta} \stackrel{\text{def}}{=} P_{\gamma} \oplus P_{\delta} = P_{\infty}$$