$\boxed{w = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) \text{ is a smooth WEP, } E(K) = V_w(K) \cup \{\infty\} \text{ is equiped by the operations } \oplus, \ominus}$

Theorem 8.8 Let w be smooth at $V_w(K)$. Then $(E(K), \oplus, \ominus, \infty)$ is a commutative group. If $\gamma = (\gamma_1, \gamma_2)$, $\delta = (\delta_1, \delta_2)$, $\eta = (\eta_1, \eta_2) \in V_w(K)$, then

(1) $\ominus\gamma = (\gamma_1, -\gamma_2 - a_1\gamma_1 - a_3)$

Comment: We describe the structure of $\mathrm{Pic}^0(L(K))$ on the curve using computational Lemma 8.7

(2) if $\gamma \neq \ominus\delta$ and $\eta = \gamma \oplus \delta \Rightarrow (\eta_1, \eta_2) = (-\gamma_1 - \delta_1 + \lambda^2 + a_1\lambda - a_2, \lambda(\gamma_1 - \eta_1) - \gamma_2 - a_1\eta_1 - a_3)$

where $\lambda = \frac{\delta_2 - \gamma_2}{\delta_1 - \gamma_1}$ if $\gamma_1 \neq \delta_1$ or $\lambda = \frac{3\gamma_1^2 + 2a_2\gamma_1 - a_1\gamma_2 + a_4}{2\gamma_2 + a_1\gamma_1 + a_3}$ if $\gamma_1 = \delta_1$

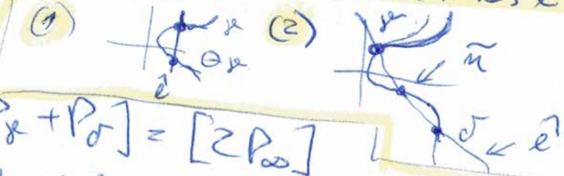
Comment: λ is a direction of line crossing γ & δ

Proof: By the definition $E(K) \to \mathbb{P}^{(1)}_{L(K)}$, $\gamma \to P_\gamma$ is a bijection compatible with $\oplus$ & $\ominus$

$\overset{8.6(3)}{\Rightarrow} E(K) \cong \mathrm{Pic}^0(L(K))$ is a commutative group.

Note: (*) $\gamma \oplus \delta = \eta \overset{8.6(4)}{\iff} [P_\gamma + P_\delta] = [P_\eta + P_\infty]$

Comment: We derive lines $\hat{l}$



(1) Let $\hat{l} := x - \gamma_1 \in K[x, y] \overset{8.7(1)}{\Rightarrow} \exists!\, \delta = (\gamma_1, \delta_2) : [P_\gamma + P_\delta] = [2P_\infty]$

$\overset{(*)}{\Rightarrow} \gamma \oplus \delta = \infty$, i.e. $\delta = \ominus\gamma$ where $\delta = (\gamma_1, -\gamma_2 - a_1\gamma_1 - a_3)$ again by 8.7(1)

(2) Let $\gamma, \delta \in V_w(K)$, $\gamma \neq \ominus\delta$, then (a) $\hat{l} := A_\gamma(w)$ if $\gamma = \delta$

(b) $\hat{l} = y - \frac{\gamma_2 - \delta_2}{\gamma_1 - \delta_1}x + \frac{\gamma_1\delta_2 - \delta_1\gamma_2}{\gamma_1 - \delta_1}$ if $\gamma \neq \delta$ $\overset{8.7(2)}{\Rightarrow} \exists\, \tilde{\eta} \in V_w(K) : [P_\gamma + P_\delta + P_{\tilde{\eta}}] = [3P_\infty]$

Note that $\frac{\partial w}{\partial y}(\gamma) = 2\gamma_2 + a_1\gamma_1 + a_3 = 0 \overset{8.7(1)}{\iff} \delta = \ominus\gamma$ $\Rightarrow \gamma \oplus \delta \oplus \tilde{\eta} = \infty$

$\Rightarrow \gamma_1 = \delta_1$ iff $\delta \in \{\gamma, \ominus\gamma\}$

Then we put $\hat{l} : y - \lambda x - \mu$ where (a) $\lambda = \frac{\partial w}{\partial x}(\gamma) \Big/ \frac{\partial w}{\partial y}(\gamma)$ for $\gamma = \delta$

(b) $\lambda = \frac{\delta_2 - \gamma_2}{\delta_1 - \gamma_1}$ for $\gamma \neq \delta$

$\overset{8.7(2)}{\Rightarrow} \tilde{\eta} = (-\gamma_1 - \delta_1 + \lambda^2 + a_1\lambda - a_2, \lambda\tilde{\eta}_1 + \mu)$ and put $\eta := \ominus\tilde{\eta} \Rightarrow$

$\lambda\eta_1 + \mu = -(\lambda\eta_1 + \mu) + a_1\eta_1 - a_3$ as $\hat{l}(\gamma_1, \gamma_2) = 0 \overset{by\,(1)}{\Rightarrow} \eta = (\tilde{\eta}_1, \lambda(\gamma_1 - \eta_1) - \gamma_2 + a_1\eta_1 - a_3)$

Corollary 8.9 If $K \subseteq F \subseteq \bar{K}$ is a field extension $\Rightarrow E(K) \leq E(F)$

Comment: The structure of $E(F)$ is "the same" as $E(K)$, i.e. the operations coincides

Example 8.10 Let $y^2 = x^3 + 1 \in \mathbb{F}_5[x, y]$ be Weierstrass equation, with the smooth curve (by 3.12): $E(\mathbb{F}_5) = \{(0,1), (0,4), (4,0), (2,2), (2,3), \infty\}$ ($\cong \mathbb{Z}_6$)

$(0,1) \oplus (0,4) = (4,0) \oplus (4,0) = (2,2) \oplus (2,3) = \infty$, $\underline{(0,4) \oplus (4,0)} = (0 - 4 + 1, 4(0 - 2) - 4) = (2,3)$

$a_1 = a_3 = a_2 = a_4 = 0$, $\lambda = -1$

9. Projective curves

Comment: We briefly translate the concept of curves, places & etc to projective spaces, as usual the picture will be wider and more symmetric

$\boxed{\text{TBN}}$ $\boxed{n \geq 1, K \text{ is a field, } \bar{K} \text{ is algebraic closure of } K}$

Denote $a = (a_0 : a_1 : \dots : a_n) = \mathrm{Span}_K((a_0, \dots, a_n)) \subseteq K^{n+1}$ a projective point with a-homogeneous coordinates

$\mathbb{P}^n(K) := \{(a_0 : a_1 : \ldots : a_n) \mid (a_0 \ldots a_n) \in K^{n+1} \setminus \{0\}\}$, $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$ – a projective space of dimension n (with K-rational points $\mathbb{P}^n(K)$)

Comment: Reminder of classical terminology

$F \in K[X_0, \ldots, X_n]$ is a homogeneous polynomial of degree $d \geq 0$ if $F \in H_d$:

$F \in H_d := \mathrm{Span}(\{X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n} \mid \sum_{j=0}^{n} i_j = d\})$ (i.e. $\deg F = $ mult $F = d$ or $F = 0$)

$K[X_0, X_1, \ldots, X_n] = \bigcup_{d \geq 0} H_d \ (\subseteq K[X_0 \ldots X_n])$ denotes the set of all homogeneous polynomials

$K(\mathbb{P}^n) := \{0\} \cup \{\frac{F}{G} \mid \exists d \geq 0 : F, G \in H_d \subseteq K[X_0 \ldots X_n]\} \subseteq K(x_0, \ldots, x_n)$

Let $F \in K[X_0, \ldots, X_n]$: $F((a_0 : a_1 : \ldots : a_n)) := F(a_0, \ldots, a_n)$ where $(a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n$

F is smooth at $a \in \mathbb{P}^n$ if $\exists j : \frac{\partial F}{\partial X_j}(a) \neq 0$ and F is singular otherwise

$a \in \mathbb{P}^n$ is a homogeneous zero of F if $F(a) = 0$; Let $M \subseteq K[X_0, \ldots, X_n]$

$V_M := \{a \in \mathbb{P}^n \mid F(a) = 0 \ \forall F \in M\}$, $V_F := V_{\{F\}}$, $V_M(K) := V_M \cap \mathbb{P}_n(K)$

If F is irreducible, then $\boxed{K(V_F) := \{\frac{G + (F)}{H + (F)} \mid G, H \in K[X_0 \ldots X_n], \deg G = \deg H\}}$

V_M is called a projective affine set, if $F \in K[X_0, X_1, X_2]$ is irreducible then V_F is projective irreducible curve

Observation A Let $d \geq 0$, $i_0, \ldots, i_n \geq 0$, $F \in K[X_0, \ldots X_n]$ is of degree d

(1) If $\sum_{j=0}^{n} i_j = d \Rightarrow \sum_{k=0}^{n} \frac{\partial \prod_{j=0}^{n} X_j^{i_j}}{\partial X_k} = d \prod_{j=0}^{n} X_j^{i_j} \Rightarrow$ (2) $\sum_{k=0}^{n} \frac{\partial F}{\partial X_k} = dF$.

(3) $K(\mathbb{P}^n)$ is a subfield of $K(x_0, \ldots x_n)$

(4) $K(V_F)$ —— " —— the fraction field of $K[X_0, \ldots X_n]/(F)$

$\boxed{\text{T\&N}}$ Let $f \in K[X_1, \ldots, X_n] \setminus \{0\}$: $\hat{f} := X_0^{\deg f} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$, $\hat{0} = 0 \in K[X_0, \ldots X_n]$

$\forall j \geq 0$ define $\pi_j : K[X_0, \ldots, X_n] \to K[x_0, \ldots x_{j-1}, x_{j+1}, \ldots x_n]$

$\pi_j(F) = F(x_0, x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots x_n)$

$\forall a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ define $\hat{a} := (1 : a_1 : a_2 : \ldots : a_n) \in \mathbb{P}^n$

$\forall j \geq 0$ denote $\mu_j : \mathbb{P}^n \to \mathbb{A}^n$ a partial mapping $\mu_j((a_0 : a_1 : \ldots : a_n)) = (\frac{a_0}{a_j}, \ldots \frac{a_{j-1}}{a_j}, \frac{a_{j+1}}{a_j}, \ldots)$ if $a_j \neq 0$

Observation B Let $f, g \in K[x_1, \ldots x_n]$:

Comment: Beware! "$K[V_F]$" is not a subring while $K(V_F)$ is, it is even a field, cf (3), (4)

(1) $\hat{f} \in K[X_0, \ldots, X_n]$, $\widehat{fg} = \hat{f} \cdot \hat{g}$, $\pi_0(\hat{f}) = f$,

(2) if $0 \notin \{f, g, f+g\} \Rightarrow X_0^{\deg g} \hat{f} + X_0^{\deg f} \hat{g} = X_0^{s} \widehat{(f+g)}$ for $s = \deg f + \deg g - \deg(f+g)$

(3) f is irreducible $\Leftrightarrow$ $\hat{f}$ is irreducible

(4) $a \in V_f \Leftrightarrow \hat{a} \in V_{\hat{f}}$ for $a \in \mathbb{A}^n$,

(5) $\mu_0(V_{X_0^s \hat{f}}) = V_f \ \forall s \geq 0$

Comment: smooth elements are carried from V_f to $V_{\hat{f}}$.

Lemma 9.1 If $f \in K[x_1, \ldots x_n]$, $a \in V_f$. Then f is smooth at $a \Leftrightarrow \hat{f}$ is smooth at $\hat{a}$.

Proof By Obs. B(4): $\hat{a} \in V_{\hat{f}}$ & $\frac{\partial f}{\partial x_j}(a) = \frac{\partial \hat{f}}{\partial X_j}(\hat{a}) \ \forall j \geq 1$

($\Rightarrow$) $\exists j \geq 0 : \frac{\partial \hat{f}}{\partial X_j}(\hat{a}) = \frac{\partial f}{\partial x_j}(a) \Rightarrow \hat{f}$ is ~~smooth~~ smooth

($\Leftarrow$) if f is singular $\overset{\text{Obs A(2)}}{\Rightarrow} \frac{\partial \hat{f}}{\partial X_0}(\hat{a}) = d\hat{f}(\hat{a}) - \sum \frac{\partial f}{\partial x_j}(a) = 0 \Rightarrow \hat{f}$ is singular