

Recall that every WEP is absolutely irreducible (4.9) and if  $w \in k[x, y]$  is absolutely irreducible, then (4.10)  $k = \tilde{k} \cap k(V_w)$ . Thus:

Corollary 4.11 If  $C$  is a Weierstrass curve, then each  $\gamma \in k(C) \setminus k$  is transcendental over  $k$ .

Example 4.12:  $w = y^2 + yx + x^3 + 1 \in \mathbb{F}_2[x, y]$  is WEP

$L :=$  the fraction field of  $\mathbb{F}_2[x, y]/(w) \cong \mathbb{F}_2[x, y]_{(w)}/(w)$   
 $(\mathbb{F}_2(V_w))$

$\uparrow$   
 the localization of  $\mathbb{F}_2[x, y]$  at  $(w)$

Then  $\tilde{\mathbb{F}}_2 = \mathbb{F}_2$  are all (only 2!) algebraic elements of  $L$  over  $\mathbb{F}_2$

Then e.g.  $X^2 + X + 1$  or  $X^3 + X + 1$  are irreducible polynomials over  $L$ .

Similarly:  $w \in \mathbb{F}_{2^m}[x, y]$  (the same polynomial)

gives  $\tilde{\mathbb{F}}_{2^m} = \mathbb{F}_{2^m} \cap \mathbb{F}_{2^m}(V_w)$ .

2

T&N Let  $w \in K[x, y]$ ,  $L$  be an AFF over  $K$ ,  $\alpha, \beta \in L$ .

We say that an AFF  $L$  is given by (the equation)  $w(\alpha, \beta) = 0$

if (1)  $L = K(\alpha, \beta)$

(2)  $w$  is irreducible

(3)  $w(\alpha, \beta) = 0$  on  $L$ .

Observation Let  $L := K(V_w)$  for irreducible  $w \in K[x, y]$  and  $\alpha := x + (w)$ ,  $\beta := y + (w)$ . Then  $L$  is an AFF given by  $w(\alpha, \beta) = 0$ .

## S. Places

In this section  $K$  is a field and

$w = y g(x, y) + h(x) + y \in K[x, y]$  where  $h \in K[x]$ ,  $y \in K[x, y]$

$\underline{m} := \text{mult}_x(h) \geq 2$  and  $\text{mult}_y(g) \geq 1$

**T&N** Let  $a = \sum_{\substack{i \geq 0 \\ j \geq 0}} a_{ij} x^i y^j \in K[x, y] - \{0\}$

$\mu(a) := \text{mult}(a(x, y^m)) = \min \{i + jm \mid a_{ij} \neq 0\}$  *"m-weighted multiplicity"*

$\Lambda(a) := \{(i, j) \mid i + jm = \mu(a), i \geq 0, j \geq 0\}$

$S(a) := \sum_{(i, j) \in \Lambda(a)} a_{ij} x^i y^j \in K[x, y] - \{0\}$  *"m-socket"*

Observation Let  $a, b \in K[x, y] - \{0\}$

- (1)  $\text{mult}(a \cdot b) = \text{mult}(a) + \text{mult}(b)$ ,  
 if  $\text{mult}(a) < \text{mult}(b) \Rightarrow \text{mult}(a+b) = \text{mult}(a)$   
 (a ~~technical~~ technical exercise, hint: use the lexicographic order on indices  $(i, j)$  of  $a_{ij}$ ; it's an analogy of properties of  $\text{deg}$ )
- (2)  $\mu(a \cdot b) = \text{mult}(a(x, y^m) \cdot b(x, y^m)) \stackrel{(1)}{=} \text{mult}(a(x, y^m)) + \text{mult}(b(x, y^m))$   
 $= \mu(a) + \mu(b)$   
 if  $\mu(a) < \mu(b)$  or  $\text{mult}(a(x, y^m)) < \text{mult}(b(x, y^m)) \Rightarrow$   
 $\Rightarrow \mu(a+b) = \mu(a)$

(3) If  $(i+jm) + (r+lm) = \mu(a) + \mu(h) \stackrel{(a)}{=} \mu(a \cdot h)$  &  $(i+jm) > \mu(a)$  <sup>4</sup>

$\Rightarrow r+lm < \mu(h) \Rightarrow b_{re} = 0$ , hence:

$$S(a) \cdot S(h) = \sum_{\substack{(i,j) \in \mathcal{D}(a) \\ (r,l) \in \mathcal{D}(h)}}} a_{ij} \cdot b_{rl} x^{i+r} y^{j+l} =$$

$$= \sum_{\substack{i,j,r,l: \\ i+jm+r+lm = \mu(a \cdot h)}} a_{ij} \cdot b_{rl} x^{i+r} y^{j+l} = S(a \cdot h)$$

(4)  $\mu(a) = \mu(S(a)) \geq \text{mult}(a)$ ,

if  $\mu(a) < \mu(h) \stackrel{(a)}{\Rightarrow} S(a \cdot h) = S(a)$

IRN Define a  $k$ -homomorphism

$\Lambda: k[x, y] \rightarrow k[x, y]$  & kernel

$\Lambda(x, y) := \mu(x, -d(x) - y g(x, y))$  (as substitution)

5

Lemma 5.1. For every  $i, j \geq 0$   $\mu(\Lambda(x^i y^j)) = i + j'm$   
 and  $\exists \lambda \in K^*$  such that  $S(\Lambda(x^i y^j)) = \lambda \cdot x^{i+j'm}$

Proof: Note that:  $\mu(-\mathcal{Q}) = \mu(\mathcal{Q}) = \text{mult}(\mathcal{Q}) = m$

$$\mu(-y^m) = \mu(y^m) \stackrel{\text{Ob. (2)}}{=} \mu(y) + \mu(y) \stackrel{\text{Ob. (2)}}{=} \mu(y) = \text{mult}(y^m) = m$$

$$\Rightarrow \mu(-\mathcal{Q} - y^m) \stackrel{\text{Ob. (2)}}{=} \mu(-\mathcal{Q}) = m$$

and  $S(-\mathcal{Q} - y^m) \stackrel{\text{Ob. (4)}}{=} S(-\mathcal{Q}) = -1 \cdot \mathcal{Q}_m \cdot x^m$  (where  $\mathcal{Q} = \sum \mathcal{Q}_i \cdot x^i$ )

$$\Rightarrow S(\Lambda(x^i y^j)) = S(x^i (-\mathcal{Q} - y^m)^j) \stackrel{\text{Ob. (3)}}{=} \underbrace{S(x)^i}_{x^i} \cdot \underbrace{S(-\mathcal{Q} - y^m)^j}_{(-\mathcal{Q}_m \cdot x^m)^j}$$

$$= \boxed{(-\mathcal{Q}_m)^j} x^{i+j'm} \Rightarrow \mu(\Lambda(x^i y^j)) = i + j'm$$

$\in K^*$

(As the assertions are rather technical, illustrate them on an example:

Example 5.12 Let  $\tilde{w} = (y+x+1)^2 - (x^3+2x+1) \in \mathbb{K}[x,y]$

Since  $\text{GCD}(x^3+2x+1, \underbrace{(x^3+2x+1)'}_{3x^2+2}) = 1$ ,  $\tilde{w}$  is a smooth RFP

$$\begin{aligned} \text{Put } w &:= \frac{1}{2}\tilde{w} = \frac{1}{2}(y^2 + x^2 + 2yx + 2y - x^3) = \\ &= y \underbrace{\left(x + \frac{y}{2}\right)}_{g(x,y)} + \underbrace{\frac{1}{2}(x^2 - x^3)}_{q(x)} + y \end{aligned}$$

$\text{mult}(g) = 1$ ,  $m := \text{mult}(q) = 2 \Rightarrow w$  is of a required type

$$\mu(g) = \text{mult}\left(\frac{y}{2} + x\right) = 1, \quad S(g) = x$$

$$\mu(q) = \text{mult}(q) = 2, \quad S(q) = \frac{1}{2}x^2$$

$$\mu(x^3y^2) = 3 + 2 \cdot 2 = 7, \quad \mu(x^2y^3) = 2 + 3 \cdot 2 = 8$$

$$\Rightarrow \mu(x^3y^2 + x^2y^3) = \mu(x^3y^2) = 7$$

$$S(\wedge(x^3y^2 + x^2y^3)) = S(\wedge(x^3y^2)) = \frac{1}{4}x^7 \quad (\text{by the proof of 5.1})$$