CURVES AND FUNCTION FIELDS

1. Algebras over a field

T&N. K-algebra

2. Valuation rings

K is a field. $R \leq K$ means that R is a subring of K.

T&N. The notation (R, M) will mean that R is a *l*ocal ring, i.e. there exists a unique maximal ideal M.

Lemma 2.1. Let (R, M) be a local ring and A a fintely generated ideal such that $AM = A$. Then $A = 0$.

Proposition 2.2. Let (R, M) be a local domain with $M = (t)$ for $t \neq 0$ and put $A := \bigcap_i M^i = \bigcap_i (t^i)$. Then

(1) for each $s \in R \setminus A$ there exist unique $i \geq 0$ and $u \in R^*$ such that $s = t^i u$,
(2) if A is finitelly generated, then $A = 0$.

Corollary 2.3. If (R, M) is a noetherian local domain with the fraction field K and $M = (t)$ for some $t \in M$, then

(1) for each $s \in R \setminus \{0\}$ there exist unique $i \geq 0$ and $u \in R^*$ such that $s = t^i u$,
(2) for each $s \in K \setminus \{0\}$ there exist unique $i \in \mathbb{Z}$ and $u \in R^*$ such that $s = t^i u$,

Lemma 2.4. Let $R \leq K$, $\alpha \in K \setminus R$ such that $\alpha^{-1} \notin R$. If J is a proper ideal of R, then either $J[\alpha] \subsetneq R[\alpha]$ or $J[\alpha^{-1}] \subsetneq R[\alpha^{-1}]$.

T&N. If $R \leq K$, R is called a valuation ring (VR) of K if for every $\alpha \in K \setminus \{0\}$ either $\alpha \in R$ or $\alpha^{-1} \in R$. R is a VR if it is VR in its fraction field. R is uniserial, if for every pair of ideals I, J either $I \subseteq J$ or $J \subseteq I$.

Proposition 2.5. If $R \leq K$ and I is an ideal such that $0 \neq I \neq R$, then there exists a valuation ring S of the field K with the maximal ideal M for which $R \subseteq S \subsetneq K$ and $I \subseteq M$.

Lemma 2.6. Let R and S be noetherian VR's of K with maximal ideals $M = R \setminus R^*$, $N = S \setminus S^*$, then

(1) M and N are principal,
(2) R and S are maximal proper subrings of K,
(3) $M \subseteq N$ iff $M = N$ iff $R = S$ iff $R \subseteq S$.

Date: June 13, 2020.

Lemma 2.7. Let $a, b \in K[x, y]$ be coprime, then

(1) $(a, b) \cap K[x] \neq 0$,
(2) if P is a prime ifdeal containing (a, b), then P is a maximal ideal of $K[x, y]$.

Corollary 2.8. Prime ideals of $K[x, y]$ are exactly:
(a) $\{0\}$, (b) (p) for $p \in K[x, y]$ irreducible, (c) maximal ideals.

T&N. A map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ is a *d*iscrete valuation of K if for each $a, b \in K$:

(D1) $\nu(ab) = \nu(a) + \nu(b)$,
(D2) $\nu(a + b) \geq \min(\nu(a), \nu(b))$,
(D3) $\nu(a) = \infty$ iff $a = 0$.

ν is the trivial discrete valuation if $\nu(K^*) = 0$. We will suppose that all discrete valuations are nontrivial.

Let R be a noetherian domain and $p \in R$ a prime element. For each $a, b \in R \setminus \{0\}$ define $\nu_p(a) = \max i \mid p^i/a$ and $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.

Example 2.9. Let $R \leq K$, R be noetherian, K the fraction field of R and p a prime. Then ν_p is a correctly defined discrete valuation of K.

Definition. Let $R \leq K$. R is said to be a *d*iscrete valuation ring (DVR), if there is a discrete valuation ν such that $R = \{a \in K \mid \nu(a) \geq 0\}$.

Proposition 2.10. Let R be a domain. with $M = (t)$ for $t \neq 0$ and put $A := \bigcap_i M^i = \bigcap_i (t^i)$. Then the following is equivalent:

(1) R is a discrete valuation ring,
(2) R is a noetherian valuation ring,
(3) R is a local principal ideal domain,
(4) R is a a noetherian local ring with a principal maximal ideal.

T&N. If R is a DVR with the maximal ideal (t) then t is called a *u*niformizing element and ν_t is called a normalized discrete valuation.

Example 2.11. For R noetherian and p a prime element, the localiyation $R_{(p)}$ is a DVR.

Lemma 2.12. Let $R \leq K$ and R be a DVR with a uniformizing element t, then for each discrete valuation μ with $R = \{a \in K \mid \mu(a) \geq 0\}$ there exists unique $k \in \mathbb{N}$ for which $\mu = k\nu_t$.

Lemma 2.13. If ν is a discrete valuation and $\nu(a) \neq \nu(b)$, then $\nu(a+b) = \min(\nu(a), \nu(b))$.

T&N. Let L be an AFF over K. We say that R is a valuation ring of the AFF L over K, if R is a valuation ring and $K \subseteq R$. ν is a (normalized) discrete valuation of the AFF L over K, if ν is a (normalized) discrete valuation and $\nu(K^*) = 0$.

Define $\nu_\infty(\frac{a}{b}) = \deg(a) - \deg(b)$ for $a, b \in K[x]$ on the AFF $K(x)$.

Proposition 2.14. Normalized discrete valuation (NDV) of the AFF $K(x)$ over K is either ν_∞ or ν_p for prime $p \in K[x]$.

Theorem 2.15. Let L be an AFF over K, $P \in \mathbb{P}_{L/K}$ and $\tilde{K}$ the field of constants of L. Then

(1) $\tilde{K} \subseteq \mathcal{O}_P$,
(2) $\mathcal{O}_P$ is a uniquely defined discrete valuation ring,
(3) $\deg P$ is finite.

Let L be an AFF over K and $\tilde{K}$ be its field of constants.

T&N. For $P \in \mathbb{P}_{L/K}$ denote by $\nu_P = \nu_t$ the NDV determined by $\mathcal{O}_P$ where $P = (t)$.
Let $a = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in K[x?1, \dots, x_n]$. Then mult$a = \min(\sum_{j=1}^{n} i_j \mid a_{i_1 \dots i_n} \neq 0)$.

Lemma 2.16. If $z \in L \setminus \tilde{K}$, then there exist $P, Q \in \mathbb{P}_{L/K}$ for which $\nu_P(z) > 0$ and $\nu_Q(z) < 0$.

Lemma 2.17. Let $z \in L \setminus \tilde{K}$, $a \in K[x]$, $P \in \mathbb{P}_{L/K}$. Then
(1) $\nu_P(z) \geq 0$ implies $\nu_P(a(z)) \geq 0$,
(2) $\nu_P(z) > 0$ implies $\nu_P(a(z)) = \mathrm{mult}(a) \cdot \nu_P(z)$,
(3) $\nu_P(z) < 0$ implies $\nu_P(a(z)) = \deg(a) \cdot \nu_P(z)$

3. Weierstrass equation polynomials

K is a field.

T&N.

Lemma 3.1.

Lemma 3.2.

Proposition 3.3. Let $w \in K[x, y]$ be a WEP and $\sigma \in$ Aff2(K). Then the following is equivalent:
(1) there exists $\lambda \in K^*$ such that $\lambda \sigma^*(w)$ is a WEP,
(2) there exists a WEP $\tilde{w}$ such that $(\sigma^*(w)) = (\tilde{w})$,
(3) there exists $c \in K^*$, $d \in K$ and $\mathbf{b} \in \mathbb{A}^2(K)$ such that $A = \begin{pmatrix} c^2 & 0 \\ d & c^3 \end{pmatrix}$ and $\sigma = \tau_{\mathbf{b}} \theta_A$.

Corollary 3.4.

Corollary 3.5.

Example 3.6.

Example 3.7.

T&N.

Lemma 3.8.

Lemma 3.9.

Lemma 3.10.

Corollary 3.11.

Proposition 3.12. Let $charK \neq 2$ and $w = y^2 - f(x)$ be a short WEP.

(1) w has at most 1 singularity,
(2) if K is perfect, then a singularity is K-rational,
(3) w is smooth if and only if f is separable.

Example 3.13.

4. Coordinate rings

K is a field and $\overline{K}$ its algebraic closure. $\mathbb{X} := \{x_1, \ldots, x_n\}$.

T&N. Let $U \subseteq \mathbb{A}^n$. Then

$$I_U = \{a \in K[\mathbb{X}] \mid a(\alpha) = 0 \forall \alpha \in U\}, \overline{I}_U = \{a \in \overline{K}[\mathbb{X}] \mid a(\alpha) = 0 \forall \alpha \in U\}$$

and $I_\alpha = I_{\{\alpha\}}$, $\overline{I}_\alpha = \overline{I}_{\{\alpha\}}$.

Lemma 4.1.

Proposition 4.2. If P is a prime ideal of $K[\mathbb{X}]$ such that $P \cap K[x_i] \neq 0$ for all $i = 1, \ldots n$, then there exists $\alpha \in \mathbb{A}^n$ for which $P = I_\alpha$

Proposition 4.3. If P is a prime ideal of $K[x, y]$, then either (a) $P = \{0\}$, or (b) $P = (p)$ for $p \in K[x, y]$ irreducible, or (c) P is maximal and there exists $\alpha \in \mathbb{A}^n$ for which $P = I_\alpha$.

Corollary 4.4. Let P be a nonzero prime ideal of $K[x, y]$.

(1) P is maximal iff there exists $\alpha \in \mathbb{A}^n$ for which $P = I_\alpha$ iff V_P is finite.
(2) there exists $p \in K[x, y]$ irreducible such that $P = (p)$ iff $V_a \subsetneq \mathbb{A}^2$ is infinite.
(3) If $p, q \in K[x, y]$ are irreducible such that $q \notin (p)$, then $V_{\{p,q\}} = V_p \cap V_q$ is finite.

Example 4.5.

Lemma 4.6.

Proposition 4.7. Let $w \in K[x, y]$ be irreducible, $C = V_w$, $\alpha = x + (w)$, $\beta = y + (w) \in K[C] \subset K(C) = K(\alpha, \beta)$. Then

(1) α is transcendental iff $\deg_y w > 0$,
(2) if α is transcendental, then $[K(C) : K] = \deg_y w$,
(3) $K(C)$ is an AFF over K.

Corollary 4.8. Let $L = K(\alpha, \beta)$. Then L is an AFF if and only if there exists an irreducible affine curve $C \subset \mathbb{A}^2$ such that $L \cong_K K(C)$.

Lemma 4.9.

Lemma 4.10.

Corollary 4.11.

Example 4.12.

T&N.

K is a field and $w = yg(x,y) + h(x) + y \in K[x,y]$ where $h \in K[x]$, $g \in K[x,y]$, $m := \text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$.

T&N. Let $a = \sum_{i,j \geq 0} a_{ij} x^i y^j$, then define:
$\mu(a) := \text{mult}(a(x, y^m))$,
$s(a) := \{(i,j) | \; i,j \geq 0, i + jm = \mu(a)\}$,
$S(a) := \sum_{(i,j) \in s(a)} a_{ij} x^i y^j$.

T&N. Denote by Λ the K-endomorphims of $K[x,y]$ defined by the rule

$$\Lambda(u(x,y)) := u(x, -h(x) - yg(x,y))$$

for every $u \in K[x,y]$.

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

Example 5.2.

Lemma 5.3. There exists $P \in \mathbb{P}_{L/K}$ such that $\nu_P(\alpha) > 0$ $\nu_P(\beta) > 0$. Moreover, then $\nu_P(\beta) = m\nu_P(\alpha)$.

Lemma 5.4. Let $u \in K[\alpha, \beta] \setminus \{0\}$ and $k := \mu(u)$. Then there exist $\lambda \in K^*$ and $b \in K[x,y]$ such that $\mu(b) > k$ and $u = \lambda x^k + b(\alpha, \beta)$.

Proposition 5.5. There exists a unique $P \in \mathbb{P}_{L/K}$ such that $\nu_P(\alpha) > 0$ $\nu_P(\beta) > 0$. For such $\nu_P(\alpha) = 1$ and $\nu_P(\beta) = m$ and $\nu_P(u \cdot v^{-1}) = \mu(u) - \mu(v)$ for each $u, v \in K[\alpha, \beta] \setminus \{0\}$.

L is an algebraic function field over K given by the equality $w(\alpha, \beta) = 0$ for $w = yg(x,y) + h(x) + y$ where $h \in K[x]$, $g \in K[x,y]$, $\text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$.

Example 5.6.

Observation. For each $\sigma \in Aff_2(K)$ there exists a unique $\overline{\sigma} \in Aff_2(L)$ such that $\sigma(\gamma) = \overline{\sigma}(\gamma)$ for each $\gamma \in \mathbb{A}^2(K)$

T&N. $\overline{\sigma}$ denotes the extension of σ from the last observation.

L is an algebraic function field over K given by the (general) equality $f(\alpha, \beta) = 0$.

Lemma 5.7. Let $\gamma = (\gamma_1, \gamma_2) \in \mathbb{A}^2(K)$, $A \in \text{GL}_2(K)$, $\sigma := \theta_A \tau_{-\gamma}$, $(u,t) := \overline{\sigma}(\alpha, \beta)$, $w_\sigma := (\sigma^{-1})^*(f)$. Then

(1) L is an algebraic function field over K given by $w_\sigma(u,t) = 0$.
(2) If f is smooth at $\gamma \in V_f(K)$, then there exists A such that either $w_\sigma = y$ or $w_\sigma = yg(x,y) + h(x) + y$ where $h \in K[x] \setminus \{0\}$, $g \in K[x,y]$, $\text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$.

(3) Let $t_\gamma(f) = a_1(x-\gamma_1)+a_2(y-\gamma_2)$ for $\gamma \in V_f(K)$, then A is a matrix form (2) (i.e. $\sigma := \theta_A\tau_{-\gamma}$ satisfies that $w_\sigma = yg(x,y)+h(x)+y$ for $h \in K[x]\setminus\{0\}$, $g \in K[x,y]$, $\operatorname{mult}(h) \geq 2$, $\operatorname{mult}(g) \geq 1$) if and only if there is $(b_1,b_2) \in K^2 \setminus \operatorname{Span}((a_1,a_2))$ such that $A = \begin{pmatrix} b_1, b_2 \\ a_1, a_2 \end{pmatrix}$.

Theorem 5.8. Let f be smooth at $\gamma = (\gamma_1,\gamma_2) \in V_f(K)$.

(1) There exists a unique $P \in \mathbb{P}_{L/K}$ such that $\nu_P(\alpha-\gamma_1) > 0$ $\nu_P(\beta-\gamma_2) > 0$.

(2) If $l = l_0 + l_1x + l_2y \in K[x,y]$ where $l_0, l_1, l_2 \in K$ then it holds for P from (1):

$$\nu_P(l(\alpha,\beta)) \begin{cases} = 0 & \text{if } l(\gamma) \neq 0 \\ = 1 & \text{if } l(\gamma) = 0 \text{ and } l \notin (t_\gamma(f)) \\ \geq 2 & \text{if } l(\gamma) = 0 \text{ and } l \in (t_\gamma(f)) \end{cases}$$

L is an algebraic function field over K given by the (general) equality $f(\alpha,\beta) = 0$ with $\deg f \geq 2$, which is simultaniously given by the equality $w_\sigma(u,v) = 0$ where $w_\sigma = yg(x,y)+h(x)+y$ for $h \in K[x] \setminus 0$, $g \in K[x,y]$, $\operatorname{mult}(h) \geq 2$, $\operatorname{mult}(g) \geq 1$.

T&N. Let $p \in K[x]$ and $\gamma \in K$. The multiplicity of (the root) γ of (the polynomial) p is a non-negative integer k satisfying $(x-\gamma)^k | p$ and $(x-\gamma)^{k+1} \not| p$.

Proposition 5.9. Let $\gamma = (\gamma_1,\gamma_2) \in V_f(K)$, $\frac{\partial f}{\partial y}(\gamma) \neq 0$, $\lambda, \mu \in K$ such that $\gamma_2 = \lambda\gamma_1 + \mu$. Then there exists a unique $P \in \mathbb{P}_{L/K}$ for which $\{\alpha-\gamma_1, \beta-\gamma_2\} \subset P$, and $\nu_P(\beta - \lambda\alpha + \mu)$ is equal to the multiplicity of the root γ of the polynomial $\hat{f}(x) = f(x, \lambda x + \mu)$.

Example 5.10.

T&N. Let $\gamma = (\gamma_1,\gamma_2) \in V_f(K) \subset \mathbb{A}^2(K)$. Then $(f) \subseteq I_\gamma = (x-\gamma_1, y-\gamma_2)$. Denote by

$$R_\gamma := K[x,y]_{(I_\gamma)} = \{\frac{a}{b} \mid a, b \in K[x,y] : b(\gamma) \neq 0\}$$

the localization of $K[x,y]$ in the maximal ideal I_γ, $(I_\gamma) = \{\frac{a}{b} \in R_\gamma \mid a \in I_\gamma\}$ denotes the (unique) maximal ideal of R_γ and $\omega_\gamma : R_\gamma \to L$ is defined by the rule $\omega_\gamma(\frac{a}{b}) = \frac{a(\alpha,\beta)}{b(\alpha,\beta)}$.

Denote

$${}_f\mathcal{O}_\gamma := \{\rho \in L \mid \exists r \in R_\gamma : \omega_\gamma(r) = \rho\}, \quad {}_f\mathcal{P}_\gamma := \{\rho \in L \mid \exists r \in (I_\gamma) : \omega_\gamma(r) = \rho\}.$$

If f is fixed we will write $\mathcal{O}_\gamma$ instead ${}_f\mathcal{O}_\gamma$ and $\mathcal{P}_\gamma$ instead ${}_f\mathcal{P}_\gamma$.

Lemma 5.11. If f is singuar at $\gamma \in V_f(K)$, then $\mathcal{O}_\gamma$ is not a valuation ring.

Lemma 5.12. Let L be an algebraic function field over K given by the equality $w_\sigma(u,v) = 0$ where $w_\sigma = yg(x,y)+h(x)+y$ for $h \in K[x]$, $g \in K[x,y]$, $\operatorname{mult}(h) \geq 2$, $\operatorname{mult}(g) \geq 1$. Suppose that $P \in \mathbb{P}_{L/K}$ such that $u, v \in P$, $\nu_P(u) = 1$. If $z \in K[u,v] \setminus \{0\}$, then there exists $a, b \in K[x,y]$ with $a(0) \neq 0$, $b(0) \neq 0$ (i.e. $\operatorname{mult}(a) = \operatorname{mult}(b) = 0$) and $\frac{z}{u^{\nu_P(z)}} = \frac{a(u,v)}{b(u,v)} \in_w \mathcal{O}^*_{(0,0)} = {}_w\mathcal{O}_{(0,0)} \setminus {}_w\mathcal{P}_{(0,0)}$

Proposition 5.13. Let f be smooth at $\gamma = (\gamma_1,\gamma_2) \in V_f(K)$ and $P \in \mathbb{P}_{L/K}$, $\frac{\partial f}{\partial y}(\gamma) \neq 0$ such that $\nu_P(\alpha-\gamma_1) > 0$, $\nu_P(\beta-\gamma_2) > 0$. Then

(1) there exists $u \in P_\gamma$ such that $\nu_P(u) = 1$ and $\frac{z}{u^{\nu_P(z)}} \in \mathcal{O}_\gamma^*$ for each $r \in K[\alpha, \beta]$.
(2) $P = P_\gamma$.

Example 5.14.

L is an AFF over K given by the equality $f(\alpha, \beta) = 0$ for transcendental α, β.

Lemma 5.15. Let $P \in \mathbb{P}_{L/K}$ and $\tilde{P} = P \cap K[\alpha, \beta]$.

(1) If $K[\alpha, \beta] \subseteq \mathcal{O}_P$, then $\tilde{P}$ is a maximal ideal of $K[\alpha, \beta]$, $\dim_K(K[\alpha, \beta]/\tilde{P}) < \infty$, $\nu_P(\alpha) \geq 0$, and $\nu_P(\beta) \geq 0$.
(2) If $K[\alpha, \beta] \nsubseteq \mathcal{O}_P$, then $\tilde{P} = 0$ and either $\nu_P(\alpha) < 0$ or $\nu_P(\beta) < 0$.
(3) If $K[\alpha, \beta] \nsubseteq \mathcal{O}_P$ and f is WEP, then $\nu_P(\alpha) < 0$, $\nu_P(\beta) < 0$ and $3\nu_P(\alpha) = 2\nu_P(\beta)$.

Proposition 5.16. Let $P \in \mathbb{P}_{L/K}$, $\deg P = 1$, f be smooth at all points $\gamma \in V_f(K)$. Then the following conditions are equivalent:

(1) $K[\alpha, \beta] \subseteq \mathcal{O}_P$,
(2) there exists unique $(\gamma_1, \gamma_2) \in V_f(K)$ for which $\nu_P(\alpha - \gamma_1) > 0$ and $\nu_P(\beta - \gamma_2) > 0$,
(3) there exists unique $\gamma \in V_f(K)$ for which $P = P_\gamma$.

Corollary 5.17. If f is a WEP smooth at all points $\gamma \in V_f(K)$ and $P \in \mathbb{P}_{L/K}$ is a place of degree 1, then either there exists $\gamma \in V_f(K)$ for which $P = P_\gamma$ or $\alpha^{-1}, \beta^{-1} \in P$.

Lemma 5.18. Let $n \geq 1$ and $P_1, \ldots, P_n$ be pairwise distinct places. If $\nu_i := \nu_{P_i}$ for all i, $a_1, \ldots a_n \in L$ and $z \in \mathbb{Z}$, then

(1) there exists $s \in L^*$ such that $\nu_1(s) > 0$ and $\nu_i(s) < 0$ for all $i = 2, \ldots, n$,
(2) there exists $t \in L$ such that $\nu_i(t - a_i) > z$ for all $i = 1, \ldots, n$.

Theorem 5.19 (Weak Approximation Theorem)**.** Let $n \geq 1$ and $P_1, \ldots, P_n$ be pairwise distinct places. If $a_1, \ldots a_n \in L$ and $z_1, \ldots, z_n \in \mathbb{Z}$, then there exists $s \in L$ such that $\nu_{P_i}(s - a_i) = z_i$ for all $i = 1, \ldots, n$.

T&N. If W is a subspace of a K-space V, we say that B is a *l*inearly independent set (a *b*asis) of V *m*odulo W if $\{b + w \mid b \in B\}$ forms a linearly independent set (a basis) of the factor V/W.

Corollary 5.20. (1) $\mathbb{P}_{L/K}$ is infinite,

(2)If $n \geq 1$, $e \geq 0$ and $P, P_1, \ldots, P_n$ are pairwise distinct places, then there exists a basis B of the K-algebra $\mathcal{O}_P$ modulo P such that $B \subset \bigcap_{j \geq 1} P_j$ (i.e. $\nu_{P_j}(b) > 0$ for each j and $b \in B$).

Proposition 5.21. Let $n \geq 1$ and $P_1, \ldots, P_n$ be pairwise distinct places and $\nu_i := \nu_{P_i}$ for all i. If $s \in \bigcap_{i=1}^n P_i$ (i.e. $\nu_P(s) \geq 1$ for every i), then $[L : K(s)] \geq \sum_{i=1}^n \nu_i(s) \deg P_i$

Corollary 5.22. If $s \in L^*$, then the set $\{P \in \mathbb{P}_{L/K} \mid \nu_P(s) \neq 0\}$ is finite.

Corollary 5.23. If f is a Weierstrass equaition polynomial and L is given by $f(\alpha, \beta) = 0$, then there exists unique $P_\infty \in \mathbb{P}_{L/K}$ such that $\nu_{P_\infty}(\alpha) < 0$. Furthermore, $\deg P_\infty = 1$, $\nu_{P_\infty}(\alpha) = -2$ and $\nu_{P_\infty}(\beta) = -3$.

Example 5.24. Let $f = y^2 + y - (x^3 + 1) = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ and $\alpha := x + (f)$, $\beta := y + (f) \in K[x, y]/(f)$. Then f is a Weierstrass equaition polynomial and $L := F_2(\alpha, \beta)$ is an AFF over $\mathbb{F}_2$ given by $f(\alpha, \beta) = 0$.

Let $P \in \mathbb{P}_{L/K}$ of degree 1. Then $P \in \{P_{(1,0)}, P_{(1,1)}, P_\infty\}$, since $V_f(\mathbb{F}_2) = \{(1, 0), (1, 1)\}$. By 5.20(1) $\mathbb{P}_{L/K}$ is infinite. hence other places are of degree greater than 1, for example for each ireducible $m \in \mathbb{F}_2[x]$ of degree greater than 1, there exists $P_m \in \mathbb{P}_{L/K}$ sch that $m(\alpha) \in P_m$, thus $\deg P_m \geq \deg(m) > 1$.

6. Divisors

Let L be an AFF over K and $\tilde{K}$ be its field of constants.

Definition. Let Div(L/K) $= \{\sum_{P\in\mathbb{P}_{L/K}} a_p P \mid a_p \in \mathbb{Z}\}$ denote the free abelian group with the free basis $\mathbb{P}_{L/K}$ (hence only finitely many a_p's are non-zero) and operations

$$\sum_{P\in\mathbb{P}_{L/K}} a_p P \pm \sum_{P\in\mathbb{P}_{L/K}} b_p P = \sum_{P\in\mathbb{P}_{L/K}} (a_p \pm b_p)P, \quad \underline{0} = \sum_{P\in\mathbb{P}_{L/K}} 0P.$$

A formal sum $\sum_{P\in\mathbb{P}_{L/K}} a_p P$ is called a *d*ivisor (of the AFF). Degree of a divisor is defined by $\deg_K(\sum_{P\in\mathbb{P}_{L/K}} a_p P) := \sum_{P\in\mathbb{P}_{L/K}} a_p \deg_K(P)$.

Example 6.1. $\sum_{P\in\mathbb{P}_{L/K}} \nu_p(r)P$ is a divisor by 5.22 for each $r \in L^*$.

T&N. A divisor $\sum_{P\in\mathbb{P}_{L/K}} \nu_p(r)P$ for each $r \in L^*$ is called principal divisor and it is denored by (r), Princ(L/K) $:= \{(r) \mid r \in L^*\}$.

T&N. Let $A = \sum_{P\in\mathbb{P}_{L/K}} a_p P$, $B = \sum_{P\in\mathbb{P}_{L/K}} b_p P \in$ Div(L/K). Then let us denote:

$$\max(A, B) := \sum_{P\in\mathbb{P}_{L/K}} \max(a_p, b_p)P, \quad \min(A, B) := \sum_{P\in\mathbb{P}_{L/K}} \min(a_p, b_p)P,$$

$A_+ := \max(A, \underline{0})$, $A_- := -\min(A, \underline{0}) = (-A)_+$, and A is positive if $A = A_+$.

Define relations $\leq$ ($\geq$ is the oposite relation) and $\sim$ on Div(L/K):

$A \leq B$ ($B \geq A$) if $a_p \leq b_p$ for every $P \in \mathbb{P}_{L/K}$,

$A \sim B$ if $A - B \in$ Princ(L/K).

$\mathcal{L}(A) := \{r \in L^* \mid (r) + A \geq \underline{0}\} \cup \{0\}$.

T&N. Cl(L/K) := Div(L/K)/Princ(L/K) is the class group of the AFF.

If $A \in$ Div(L/K), then $\mathcal{L}(A)$ is said to be the Riemann-Roch space of the divisor A and $l(A) = \dim_{L/K} A = \dim_K \mathcal{L}(A)$.

If $K = \tilde{K}$, then L is a full constant AFF.

Lemma 6.2. If $A, B \in$ Div(L/K) such that $A \leq B$, then $\mathcal{L}(A)$ is a subspace of $\mathcal{L}(B)$ and $\dim_K(\mathcal{L}(B)/\mathcal{L}()) \leq \deg_K(B - A)$.

Proposition 6.3. For $K = \tilde{K}$ (i.e. L is a full constant AFF), and $A, B \in$ Div(L/K):

(D1) if $A \geq \underline{0}$, then $1 \leq l(A) \leq \deg A + 1$,

(D2) if $A < \underline{0}$, then $l(A) = 0$,

(D3) $l(A) < l(A_+) < \infty$,
(D4) if $A \le B$, then $\deg A - l(A) \le \deg B - l(B)$.

Lemma 6.4. If $s \in L \setminus \tilde{K}$ (i.e. s is transcendental over K), then there exists $B \in$ Div(L/K) such that $B \ge \underline{0}$ and for each $k \ge 0$:

(1) $(k+1)[L : K(s)] \le l(k \cdot (s)_- + B)$,
(2) $(k+1)[L : K(s)] \le k \cdot \deg((s)_)-+\deg B + 1$,
(3) $k[L : K(s)] - l(k \cdot (s)_-) \le \deg B - [L : K(s)]$.

Theorem 6.5. If $K = \tilde{K}$ and $s \in L \setminus \tilde{K}$ (i.e. L is a full constant AFF and s is transcendental over K), then $\deg((s)_-) = \deg((s)_+) = [L : K(s)]$ and $\deg((s)) = 0$.

Corollary 6.6. If $A \sim B$, then (1) $\deg A = \deg B$ and (2) $\dim_{L/K} A = \dim_{L/K} B$.

Example 6.7. Let L be an AFF over $\mathbb{F}_2$ given by $f(\alpha, \beta) = 0$ for $f = y^2 + y - (x^3 + 1) \in \mathbb{F}_2[x, y]$ as in 5.24. We will compute principal divisors $(\alpha + 1)$ adn $(\alpha + 1)$.

(a) By 6.5 $\deg((\alpha+1)_+) = \sum_{P:\alpha+1\in P} \nu_P(\alpha+1) \deg P = [K : \mathbb{F}_2(\alpha+1)] = [K : \mathbb{F}_2(\alpha)] = 2$. Since $\alpha + 1 \in P_{(1,0)} \cap P_{(1,1)}$ we can see that $\deg P_{(1,0)} = \deg P_{(1,1)} = 1$. Furthermore $\nu_{P_\infty}(\alpha + 1) = \nu_{P_\infty}(\alpha) = -2$, hence ${\mathbb{P}_{L/K}}^{(1)} = \{P_{(1,0)}, P_{(1,1)}, P_\infty\}$ is the set of all places of degree 1 and

$$(\alpha + 1) = 1 \cdot P_{(1,0)} + 1 \cdot P_{(1,1)} - 2 \cdot P_\infty$$

(b) Again by 6.5 $\deg((\alpha)_+) = \sum_{P:\alpha\in P} \nu_P(\alpha) \deg P = [K : \mathbb{F}_2(\alpha)] = 2$ and α is not an element of $P \in {\mathbb{P}_{L/K}}^{(1)}$, thus there exists a unique P_α such that $\alpha \in P_\alpha$ and $\deg P_\alpha = 2$ which means that

$$(\alpha) = 1 \cdot P_\alpha - 2 \cdot P_\infty$$

Proposition 6.8. For $K = \tilde{K}$ and $A, B \in$ Div(L/K):

(D5) $l(B - A) \ge 1$ if and only if there exists $A' \in$ Div(L/K) such that $A \sim A' \le B$,
(D6) if $l(B - A) \ge 1$, then $\deg A - l(A) \le \deg B - l(B)$,
(D7) $l(A) \ge 1$ if and only if there exists $s \in L^8$ such that $A + (s) \ge \underline{0}$,
(D8) if $\deg A < 0$, then $l(A) = 0$,
(D9) $\mathcal{L}((s)) = Ks^{-1} = \{ks^{-1|k\in K}\}$.

Lemma 6.9. Let $K = \tilde{K}$ and $A \in$ Div(L/K) such that $\deg A = 0$. Then

(1) $l(A) \in \{0, 1\}$,
(2) $l(A) = 1$ if and only if $A \in$ Princ(L/K).

Theorem 6.10 (Riemann)**.** If $K = \tilde{K}$, then there exists nonnegative integer γ such that $\deg(A) - l(A) < \gamma$ for each $A \in$ Div(L/K).

Definition. The minimal possible γ from the Riemann theorem for L over $\tilde{K}$ (i.e. minimal γ for which $\deg(A) - l(A) < \gamma$ for each $A \in$ Div(L/K)) is called the *genus* of the AFF L over K.

The genus of the AFF will be denoted by g in the sequel.

Lemma 6.11. There exists an integer γ such that for each $A \in \mathrm{Div(L/K)}$ with $\deg(A) \geq \gamma$ it holds that $\deg(A) = l(A) + g - 1$.

T&N. Let $\mathbb{P} := \mathbb{P}_{L/K}$ and consider the Cartesion power $L^{\mathbb{P}}$ as a L-algebtra with operations defined in coordinates where $l \to l * 1 \in L^{\mathbb{P}}$ identifies elements of L with constants of $L^{\mathbb{P}}$. $f \in L^{\mathbb{P}}$ is called adèle if the set $\{P \in \mathbb{P} \mid f(P) \neq 0\}$ is finite and $\mathcal{A}_{L/K}$ denotes the set of all adèles.

Let $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P \in \mathrm{Div(L/K)}$. Then $\mathcal{A}_{L/K}(A) := \{f \in L^{\mathbb{P}} \mid \nu_P(f(P)) + a_P \geq 0 \forall P \in \mathbb{P}\}$ and $i(A) := g - 1 - \deg(A) - l(A) \geq 0$ is said to be the *i*ndex of speciality of A. A is called *s*pecial if $i(A) > 0$ and A is called /nonspecial if $i(A) = 0$.

Lemma 6.12. Let $K = \tilde{K}$, $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P$, $B = \sum_{P \in \mathbb{P}_{L/K}} b_p P \in \mathrm{Div(L/K)}$ and $s \in L^*$. Then

(1) if $A \leq B$, then $\mathcal{A}_{L/K}(A) \subseteq \mathcal{A}_{L/K}(B)$ and $\dim_K(\mathcal{A}_{L/K}(B)/\mathcal{A}_{L/K}(A)) = \deg(B - A)$,
(2) if $A \leq B$, then $\dim_K((\mathcal{A}_{L/K}(B) + L)/(\mathcal{A}_{L/K}(A) + L)) = i(A) - i(B)$,
(3) $\mathcal{A}_{L/K}(A) \cap \mathcal{A}_{L/K}(B) = \mathcal{A}_{L/K}(\min(A, B))$, $\mathcal{A}_{L/K}(A) + \mathcal{A}_{L/K}(B) = \mathcal{A}_{L/K}(\max(A, B))$,
(4) $\dim_K(\mathcal{A}_{L/K}/(\mathcal{A}_{L/K})/(\mathcal{A}_{L/K}(A) + L) = i(A)$,
(5) $\mathcal{A}_{L/K} = \mathcal{A}_{L/K}(A) + L$ if and only if $i(A) =$,
(6) $s\mathcal{A}_{L/K}(A) = \mathcal{A}_{L/K}(A - (s))$

Lemma 6.13. Let $\mathcal{S} \subsetneqq \mathbb{P}_{L/K}$, , $P_1, \ldots, P_n \in \mathcal{S}$ be pairwise distinct places, $a_1, \ldots a_n \in L$ and $z \in \mathbb{Z}$. Then there exists $t \in L$ such that $\nu_{P_i}(t - a_i) > z$ for all $i = 1, \ldots, n$ and $\nu_P(t) \geq 0$ for all $P \in \mathcal{S} \setminus \{P_1 \ldots, P_n\}$.

Theorem 6.14 (Strong Approximation Theorem)**.** Let $\mathcal{S} \subsetneqq \mathbb{P}_{L/K}$, , $P_1, \ldots, P_n \in \mathcal{S}$ be pairwise distinct places. If $a_1, \ldots a_n \in L$ and $z_1, \ldots, z_n \in \mathbb{Z}$, then there exists $s \in L$ such that $\nu_{P_i}(s - a_i) = z_i$ for all $i = 1, \ldots, n$ and $\nu_P(s) \geq 0$ for all $P \in \mathcal{S} \setminus \{P_1 \ldots, P_n\}$.

7. Weil differntials

Let L be an AFF over K of genus g and $\tilde{K}$ be its field of constants.

T&N. Let $A \in \mathrm{Div(L/K)}$. Then

$$\Omega_{L/K}(A) := (\mathcal{A}_{L/K}(A) + L)^{o}_{K} = \{\omega \in {\mathcal{A}_{L/K}}^* \mid \omega(\mathcal{A}_{L/K}(A) + L) = 0, \}$$

$$\Omega_{L/K} := \bigcup_{B \in \mathrm{Div(L/K)}} \Omega_{L/K}(B) = \{\omega \in {\mathcal{A}_{L/K}}^* \mid \omega(L) = 0, \exists B \in \mathrm{Div(L/K)} : \omega(\mathcal{A}_{L/K}(B)) = 0\}$$

Elements of $\Omega_{L/K}$ are called *Weil differntials* (of the AFF).

Lemma 7.1. Let $\omega \in \Omega_{L/K} \setminus \{0\}$ and $K = \tilde{K}$. Then there exists a unique $W \in \mathrm{Div(L/K)}$ such that $\omega(\mathcal{A}_{L/K}(W)) = 0$ and for each $A \in \mathrm{Div(L/K)}$ satisfies that $A \leq W$ whenever $\omega(\mathcal{A}_{L/K}(A))$.

T&N. The divisor W from 7.1 uniquely determained by a a Weil differntial ω is called the *canonical divisor* of ω and it is denoted (ω).

Lemma 7.2. Let $\omega, \tilde{\omega} \in \Omega_{L/K} \setminus \{0\}$, $A \in \mathrm{Div(L/K)}$, and $K = \tilde{K}$. Define $\Psi_\omega := s \cdot \omega l$ for every $s \in L$. Then

(1) if $s \in L^*$, then $(s\omega) = (s) + (\omega)$,
(2) Ψ_ω is an L- and so K-linear embedding, and $\Psi_\omega(\mathcal{L}((\omega) - A)) \subseteq \Omega_{L/K}(A)$
(3) there exists $B \in \mathrm{Div(L/K)}$ such that $\Psi_\omega(\mathcal{L}((\omega) - B)) \cap \Psi_\omega(\mathcal{L}((\omega) - B)) \neq 0$.

Theorem 7.3. Let $K = \tilde{K}$. Then

(1) $\dim_L(\Omega_{L/K}) = 1$,
(2) if $\omega \in \Omega_{L/K} \setminus \{0\}$ and $A \in \mathrm{Div(L/K)}$, then $\Psi_{\omega,A} : \mathcal{L}((\omega) - A) \to \Omega_{L/K}(A)$ given by $\Psi_{\omega,A}(s) = s\omega$ is a K-isomoprhism.

Corollary 7.4. Let $K = \tilde{K}$. The canonical divisors form exactly one coset modulo Princ(L/K) (i.e. for W, a canonical divisor, $A \sim W$ iff A is canonical).

Theorem 7.5 (Riemann-Roch)**.** If $K = \tilde{K}$ and W a canonical divisor, then

$$l(A) = \deg A + l(W - A) + 1 - g$$

for every $A \in \mathrm{Div(L/K)}$.

Corollary 7.6. Let $K = \tilde{K}$ and $A, W \in \mathrm{Div(L/K)}$, then:

(1) if W is canonical, then $l(W) = g$, $\deg W = 2g - 2$, $i(W) = 1$,
(2) (Main consequence of the Riemann-Roch Theorem) if $\deg A \geq 2g - 1$, then

$$l(A) = \deg A + 1 - g.$$

Lemma 7.7. Let $K = \tilde{K}$ and $A \in \mathrm{Div(L/K)}$, then:

(1) if $\deg A = 2g - 2$ and $l(A) \geq g$, then A is canonical,
(2) if $g = 1$, then A is canonical if and only if A is principal.

Proposition 7.8. Let $K = \tilde{K}$ and $A, B \in \mathrm{Div(L/K)}$ and $g = 0$. Then:

(1) A is principal if and only if $\deg A = 0$,
(2) $A \sim W$ if and only if $\deg A = \deg B$,
(3) A is canonical if and only if and only if $\deg A = -2$.

T&N. $\mathbb{P}^{(1)}_{L/K} := \{P \in \mathbb{P}_{L/K} \mid \deg P = 1\}$.

Lemma 7.9. Let $P \in \mathbb{P}^{(1)}_{L/K} \neq \emptyset$, $h \in \mathbb{Z}$, $h \geq 0$, $s \in L$. Then

(1) $K = \tilde{K}$,
(2) $s \in \mathcal{L}(iP) \setminus \mathcal{L}((i-1)P)$ if and only if $(s)_- = iP$, where $i \geq 1$,
(3) if there exists $k \geq 0$ such that $l(iP) \geq i - h + 1$ for each $i \geq k$, then $g \leq h$,
(4) if for each $i \geq h + 1$ there exists $s_i \in L$ such that $(s)_- = iP$, then $g \leq h$.

Example 7.10. x be a variable. Then $K(x)$ is an AFF over K. By 2.14

$$\mathbb{P}_{K(x)/K} = \{P_p \mid p \in K[x] \text{ is irreducible}\} \cup \{P_\infty\}$$

where P_p is the maximal ideal of the localization $K[x]_{((p))}$ with $\nu_{P_p} = \nu_p$ and P_∞ is given by the dicsrete valuation $\nu_\infty(\frac{a}{b}) = \deg(b) - \deg(a)$.

Then $\nu_p(x^i) \geq 0$ for every $i \geq 0$ and $nu_\infty(x^i) = -i$ for every $i \geq 0$, hence $(x^i)_- = iP_\infty$. Thus $K(x)$ is of genus 0 by 7.9(4).

Let L be an AFF over K of genus g.

Proposition 8.1. Let $\mathbb{P}^{(1)}_{L/K} \neq \emptyset$. Then $g = 0$ if and only if there exists $s \in L$ such that $L = K(s)$

Definition. An Aff L is called an *eliptic 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) $\mathcal{L}(1P) \subsetneqq \mathcal{L}(2P) \subsetneqq \mathcal{L}(3P)$,
(3) For every $u \in \mathcal{L}(2P) \setminus \mathcal{L}(1P)$ and every $v \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$ there exists a WEP $w \in K[x, y]$ and $\lambda \in K^*$ such that L is given by $w(\lambda u, \lambda v) = 0$.

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

(1) There exists unigue $P = P_\infty \in \mathbb{P}_{L/K}$ such that $\nu_P(\alpha) < 0$ or $\nu_P(\beta) < 0$,
(2) $K[\alpha, \beta] \subseteq \mathcal{O}_Q$ for all $Q \in \mathbb{P}_{L/K} \setminus \{P_\infty\}$,
(3) $P_\infty \in \mathbb{P}^{(1)}_{L/K}$, $(\alpha)_- = 2P_\infty$, $(\beta)_- = 3P_\infty$, $P_\infty \cap K[V_w] = P_\infty \cap K[\alpha, \beta] = 0$, and $\mathcal{O}_{P_\infty} \cap K[\alpha, \beta] = K$,
(4) if w is smooth at $V_w(K)$, then $\mathbb{P}^{(1)}_{L/K} = \{P_\infty\} \cup \{P_\gamma \mid \gamma \in V_w(K)\}$,
(5) L is either an EFF (and $g = 1$) or there is $s \in L$ such that $L = K(s)$ (and $g = 0$),
(6) if $L = K(s)$, then there exists polynomials $u, v \in K[x]$ for which $\alpha = u(s)$, $\beta = v(s)$, and $\deg u = 2$, $\deg v = 3$.

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

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

Example 8.5. (1) Let $f = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ be a WEP. Since it is smooth at $V_f(\mathbb{F}_2)$, it is of genus 1 by 8.4 and $\mathbb{F}_2(s) \subsetneqq \mathbb{F}_2(V_f)$ for each $s \in \mathbb{F}_2(V_f)$
(2) Let $f = y^2 + x^3 + x + 1 \in \mathbb{F}_2[x, y]$ be a WEP. Since it is singular $\mathbb{F}_2(V_w)$, it is of genus 1 by 8.4 and there exists $s \in \mathbb{F}_2(V_f)$ such that $\mathbb{F}_2(s) = \mathbb{F}_2(V_f)$.

T&N. $\mathrm{Pic}^0(L/K) := \mathrm{Ker(deg)/Princ(L/K)}$ is called the *P*icard group, $[A] := A + \mathrm{Princ(L/K)}$ denotes the cosets of $\mathrm{Pic}^0(L/K)$.

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

(1) if $P_1 - P_2 \in \mathrm{Princ(L/K)}$, then $P_1 = P_2$,
(2) if $\deg A = 1$, then there exist a unique place $Q \in \mathbb{P}^{(1)}_{L/K}$ such that $P - A \in \mathrm{Princ(L/K)}$,

(3) the mapping $\Psi_Q : \mathbb{P}^{(1)}_{L/K} \to \mathrm{Pic}^0(L/K)$ defined by $\Psi_Q(P) := [P - Q]$ is a bijection.

T&N. L be an EFF over K, then we can define for each $Q \in \mathbb{P}^{(1)}_{L/K}$ a binary operation $\oplus$ by the rule $P_1 \oplus P_2 := \Psi_Q^{-1}(\Psi_Q(P_1) + \Psi_Q(P_2))$ for the mapping Ψ_Q from the previous lemma.

T&N. L be an EFF over K, then we can define for each $Q \in \mathbb{P}^{(1)}_{L/K}$ a binary operation $\oplus$ by the rule $P_1 \oplus P_2 := \Psi_Q^{-1}(\Psi_Q(P_1) + \Psi_Q(P_2))$ for the mapping Ψ_Q from the previous lemma.

T&N. Let $\hat{l} = cx + dy + e \in K[x, y]$ for $c, d, e \in K$ where $(c, d) \neq (0, 0)$. Then $l = \hat{l} + (w) \in K[V_w] = K[\alpha, \beta]$ for $\alpha = x + (w), \beta = y + (w)$ is called a *line* represented by $\hat{l}$. We say that l passes through γ if $\gamma \in V_{\hat{l}}$.

Lemma 8.7. Let w be smooth at $V_w(K)$, $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$, $\hat{l} \in K[x, y]$ represents a line $l = \hat{l} + (w) \in K[V_w]$.

(1) if $\hat{l} = x - \gamma_1$, then there exists unique $\delta = (\gamma_1, \delta_2) \in V_w(K)$ such that $(l) = P_\gamma + P_\delta - 2P_\infty$ and $\delta_2 = -a_1\gamma_1 - a_3 - \gamma_2$,

(2) if $\hat{l} = y - \lambda x - \mu$ and l passes through γ, then $(l)_- = 3P_\infty$ and

(a) either there exists $P \in \mathbb{P}_{L/K}$ of degree 2 such that $(l)_+ = P_\gamma + P$ $\hat{l} \notin (t_\gamma(w))$ and $V_w(K) \cap V_{\hat{l}} = \{\gamma\}$,

(b) or there exist points $\delta = (\delta_1, \delta_2), \eta(\eta_1, \eta_2) \in V_w(K)$ such that $(l)_+ = P_\gamma + P_\delta + P_\eta$ $\hat{l} \notin (t_\gamma(w))$ and $V_w(K) \cap V_{\hat{l}} = \{\gamma\}$, $V_w \cap V_{\hat{l}} = \{\gamma, \delta, \eta\}$, $\eta_1 = \gamma_1 - \delta_1 - a_2 + \lambda^2 + a_1\lambda$ and $\hat{l} \in (t_\gamma(w))$ iff $\gamma \in \{\delta, \eta\}$.

Definition. Let w be smooth and L be an EFF given by w. Consider the group structure on $\mathbb{P}_{L/K}{}^{(1)}$ determined by Ψ_{P_∞}. Put $E(K) = V_w(K) \cup \{\infty\}$ and define the operations $\oplus$, *ominus* on $E(K)$:

$$\gamma \oplus \delta = \eta \Leftrightarrow P_\gamma \oplus P_\delta = P_\eta, \quad \ominus\gamma = \delta \Leftrightarrow P_\gamma \oplus P_\delta = P_\infty$$

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

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

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

(a) $\lambda = \frac{\delta_2 - \gamma_2}{\delta_1 - \gamma_1}$ if $\gamma_1 \neq \delta_1$.

(b) $\lambda = \frac{3\gamma_1^2 + 2a_2\gamma_1 - a_1\gamma_2 + a_4}{2\gamma_2 + a_1\gamma_1 + a_3}$ if $\gamma_1 = \delta_1$.

9. Projective curves

Let $n \geq 1$, K be a field and $\overline{K}$ the algebraic closure of K.

T&N. Denote $a = (a_0 : a_1 : \cdots : a_n) = \mathrm{Span}((\mathrm{a_0, a_1, \ldots, a_n})) \subset \mathrm{K^{n+1}}$ a projective point of the projective space

$$\mathbb{P}^n(K) = \{(a_0 : a_1 : \cdots : a_n) \mid (a_0, a_1, \ldots, a_n) \in K^{n+1} \setminus \{0\}\}$$

of the homogeneous coordinates $(a_0 : a_1 : \cdots : a_n)$ and put $\mathbb{P}^n := \mathbb{P}^n(\overline{K})$.

$K[X_0, X_1, \ldots, X_n]$ denotes the set of all homogeneous polynomials and put

$$K(X_0, X_1, \ldots, X_n) := \{\frac{H}{G} \mid H, G \in K[X_0, X_1, \ldots, X_n], \exists d \geq 0 : \deg H = \deg G\} \cup \{0\}$$

Let $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ and $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$. We define

$$\hat{f} := X_0^{\deg f} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}), \hat{0} := 0 \in K[X_0, X_1, \ldots, X_n], \quad \hat{a} := (1 : a_1 : \cdots : a_n) \in \mathbb{P}^n$$

Lemma 9.1. Let $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ and $a \in V_f$. Then f is smooth at a if and only if $\hat{f}$ is smooth at $\hat{a}$.

Proposition 9.2. Let $H, F \in K[X_0, X_1, X_2]$, F be irreducible and $j \in \{0, 1, 2\}$.

(1) Then either $H \in (F)$, hence $H(a) = 0$ for all $a \in V_F$, or $H \notin (F)$ and $V_F \cap V_H$ is finite.
(2) If $x_j \notin (F)$, then $|\{(a_0 : a_1 : \cdots : a_n) \in V_F \mid a_j = 0\}|$ is finite.

Corollary 9.3. Let $F, G \in K[X_0, X_1, X_2]$, $V_F = V_G$, $a \in V_F$. Then

(1) there exists $\lambda \in K^*$ such that ,
(2) F is smooth at a iff G is smooth at a.

Proposition 9.4. Let $f \in K[x_1, x_2]$ be irreducible and $F = \hat{f}$. Define the mappings $\epsilon_f : K(V_f) \to K(V_F)$ and $\epsilon : K(x) \to K(\mathbb{P}^1)$ by the rules

$$\epsilon_f \left(\frac{g + (f)}{h + (f)} \right) = \frac{X_0^{\deg(h)} \hat{g} + (F)}{X_0^{\deg(g)} \hat{h} + (F)} \quad \text{and} \quad \epsilon \left(\frac{g}{h} \right) = \frac{X_0^{\deg(h)} \hat{g}}{X_0^{\deg(g)} \hat{h}}.$$

Then ϵ_f and ϵ are K-isomorphisms of fields.

T&N. Let $A, B, G \in K[X_0, X_1]$, $B \neq 0$. Define

$$\nu_G(A) := \max\{e \geq 0 \mid G^e / A\}, \quad \nu_G \left(\frac{A}{B} \right) := \nu_G(A) - \nu_G(B), \quad \nu_G(0) = \infty.$$

Lemma 9.5. Let ν be a normalized discrete valuation of the AFF $K(\mathbb{P}^1)$ over K.

(1) There exists $G \in K[X_0, X_1]$ irreducible such that $\nu = \nu_G$,
(2) degree of the place $\{U \in K(\mathbb{P}^1) \mid \nu_G(U) > 0\}$ is equal to $\deg G$,
(3) the map $(a_0 : a_1) \to \{U \in K(\mathbb{P}^1) \mid \nu_{a_1 X_0 - a_0 X_1}(U) > 0\}$ is a bijection $\mathbb{P}^1 \to \mathbb{P}^{(1)}_{L/K}$.

Theorem 9.6. Let $F \in K[X_0, X_1, X_2]$, be irreducible and $P \in \mathbb{P}_{K(V_F)/K})$, $a \in V_F$. Then

(1) there exists $b \in V_F$ such that $P_b \subseteq P$,
(2) if $\deg P = 1$ and $P_a \subseteq P$, then $a \in V_F(K)$,
(3) if F is smooth at $a \in V_F(K)$, then $P_a = P$ and $\deg P_a = 1$.