CURVES AND FUNCTION FIELDS

Motivation

Objective: to build an (algebraic) apparatus for describing curves over finite fields.
Idea: generalization of geometric theory (with geometrically descriptive analogies)
Key tool: description of the structure of function fields (places $\leftrightarrow$ points at a curve)
Key problem: situation $\mathbb{R} \subseteq \mathbb{C}$ easier than $\mathbb{F}_q \subseteq \overline{\mathbb{F}_q}$ ($[\mathbb{C} : \mathbb{R}] = 2$ vs. $[\overline{\mathbb{F}_q} : \mathbb{F}_q] = \infty$)

Lecture structure:

(1) *Rings* - algebras over a field, valuation rings,
(2) *Polynomials* - WEP, coordinate rings,
(3) *Ideals* - places in function fields,
(4) *Spaces* - divisors, Weil differentials,
(5) *Groups* - function fields of elliptic curves.

1. Algebras over a field

A *ring* always means commutative ring with operations $+$, $-$, $\cdot$, 0 and 1 and we will usually write R instead $(R, +, -, \cdot, 0, 1)$.

T&N. Let K be a field and A a ring containing K as a subring. Then A is called *K-algebra* (or algebra over K). If A and B are two K-algebras, then $f : A \to B$ is a *homomorphism of K-algebras*, if it is a ring homomorphism and $f(k) = k$ for every $k \in K$.

K always denotes a field and $R \leq K$ means that R a subring of K.

Observation. If A and B are K-algebras and I is a proper ideal of A, then

(1) A/I is a K-algebra,
(2) A is a vector space over K and I is its subspace,
(3) if $f : A \to B$ is a homomorphism of K-algebras, then f is K-linear.

T&N. Let R be a ring, $M \subset R$ a $a \in R$. Then (M) denotes the ideal of R generated by the set M and $(a) := (\{a\})$. $R[x_1, \dots, x_n]$ denotes a polynomial ring over R and $K(x_1, \dots, x_n)$ is a field of fractions of $K[x_1, \dots, x_n]$.

Example 1.1. (1) $K[x]$, $K[x, y]$, $K(x)[y]$ and $K(x, y)$ are K-algebras.
(2) $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{2}]$ are $\mathbb{Q}$-algebras.
(3) $\mathbb{Q}[x] \cong \mathbb{Q}[\pi] \not\cong \mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ are $\mathbb{Q}$-algebras.

T&N. If A and B are two vector spaces over K (for short K-spaces), then $\mathrm{Hom}_K(A, B)$ is an abelian group of all linear maps $A \to B$ and $C \leq A$ means that C is a subspace of A.

Lemma 1.2. If A a B are two vector spaces over K, $I \leq A$, $J \leq B$ such that $\varphi \in \mathrm{Hom}_K(A, B)$ satisfies $\varphi(I) \subseteq J$, then $\tilde{\varphi}(a+I) = \varphi(a) + J$ is a well-defined linear map $\tilde{\varphi} \in \mathrm{Hom}(A/I, B/J)$ and

(1) $\tilde{\varphi}$ is injective iff $\varphi^{-1}(J) = I$,
(2) $\tilde{\varphi}$ is surjective and $J \subseteq \varphi(A)$ iff φ is surjective.

Lemma 1.3. Let V be a vector space over K such that $A, B, C \leq V$, and $A \leq C$.

(1) $A + (B \cap C) = (A + B) \cap C$,
(2) if $\dim(C/A) < \infty$, then $\dim((C+B)/(A+B)) = \dim(C/A) - \dim((C\cap B)/(A\cap B))$.

T&N. If V is a vector space over K $A \leq V$, then we denote

$$V^* = \mathrm{Hom}_K(V, K) \text{ and } A^o = \{f \in V^* \mid f(A) = 0\}.$$

Lemma 1.4. Let V be a vector space over K and $A, B \leq V$, then

(1) V^* is a vector space over K and $A^o, B^o \leq V^*$,
(2) $A^o \cong (V/A)^*$,
(3) if $\dim(V/A) < \infty$, then $A^o \cong V/A$,
(4) if $A \leq B$, then $B^o \leq A^o$,
(5) $(A \cap B)^o = A^o + B^o$, $(A + B)^o = A^o \cap B^o$,

Proposition 1.5. Let $K \subseteq L$ be an extension of the fields, V an L-space. Then V is a K-space and we can define multiplication by each $l \in L$ on V^* by the rule $l\varphi(v) = \varphi(lv)$ for all $\varphi \in V^* = \mathrm{Hom}_K(V, K)$ and $v \in V$. Then

(1) $l\varphi \in V^*$ $\forall l \in L, \varphi \in V^*$,
(2) V^* is an L-space,
(3) if $A_K \leq V_K$ and $\alpha \in L \setminus \{0\}$, then $\alpha^{-1}A^o = (\alpha A)^o$.

2. Algebraic function fields

T&N. Let R be a subring of a field K, and V a K-space. We say that $A \subset V$ is *linearly dependent* (LD) over R, if $\exists\{a_1 \dots, a_k\} \subseteq A$ a $\exists r_1, \dots, r_k \in R \setminus \{0\}$ such that $\sum_i r_i a_i = 0$, otherwise A is *linearly independent* (LI) over R.

Lemma 2.1. Let R be a domain, K its fraction field, V a vector space over K and $M \subset V$. Then M is LI over $R \Leftrightarrow M$is LI over K.

Lemma 2.2. Let V be a vector space over $K(x)$ and $v_1, \dots, v_n \in V$. Then $v_1, \dots, v_n$ is LD over $K(x) \Leftrightarrow \exists a_1, \dots a_n \in K[x]$ such that $\sum_i a_i v_i = 0$ and $a_j(0) \neq 0$ for at least one j.

T&N. Let R be a ring and $A, B \subset R$, then we denote

$AB := \langle ab \mid a \in A, b \in B\rangle$ a subgroup of the additive group $(R, +, -, 0)$ generated by the set $\{ab \mid a \in A, b \in B\}$,
$A[B] := \{f(b_1, \dots, b_k) \mid k \in \mathbb{N}, f \in A[x_1 \dots, x_k], b_1, \dots, b_k \in B\}$,
$A[b_1, \dots, b_k] := A[\{b_1, \dots, b_k\}]$ pro $b_1, \dots, b_k \in R$.

Observation. Let R be a ring and $A, B, C \subset R$, then

(1) $AB = BA$ and $A(BC) = (AB)C$,

(2) if A, B are subrings (ideals) of R, then $AB = A[B]$ is a subring (AB is an ideal) of R,
(3) $A[b_1, \ldots, b_k] = \{f(b_1, \ldots, b_k) \mid f \in A[x_1 \ldots, x_k]\}\ \forall b_1, \ldots, b_k \in R$.

In the sequel $K \subseteq L$ means a field extension of K by L and recall that $[L : K] = \dim_K L$ and $[U : K] = [U : L][L : K]$ for extensions $K \subseteq L \subseteq U$.

Proposition 2.3. Let $K \subseteq L$ be an algebraic extension.
(1) If B is a basis of L as a K-space, then B is a basis of $L(x)$ as a $K(x)$-space,
(2) $[L(x) : K(x)] = [L : K]$.

Lemma 2.4. Let V be a $K(x)$-space and $M \subset V$. Then

$$M \text{ is LD over} K(x) \quad \Leftrightarrow \quad \{vx^j \mid v \in M, j \geq 0\} \text{ is LD over } K.$$

Definition. Let $K \subseteq L$. L is called an *algebraic function field* (AFF) over K , if $\exists \alpha \in L$ transcendental over K for which $[L : K(\alpha)] < \infty$.

Example 2.5. (1) $\mathbb{R}(x)$ and $\mathbb{C}(x)$ are an AFF over $\mathbb{R}$.
(2) $\mathbb{Q}(\sqrt[3]{5})(x) = \mathbb{Q}(\sqrt[3]{5}, x) \cong \mathbb{Q}(\sqrt[3]{5}, \pi) \subseteq \mathbb{R}$, then $\mathbb{Q}(\sqrt[3]{5}, x)$ is an AFF over $\mathbb{Q}$.
(3) Let $g \in K[x, y]$ be an irreducible polynomial, $R := K[x, y]/(g)$, L be a fraction field of R. Put $\xi := x + (g)$ and $\upsilon := y + (g)$. Then $R = K[\xi, \upsilon]$ and $L = K(\xi, \upsilon)$. Assume to contrary that ξ, υ are both algebraic over K, then $[K(\xi, \upsilon) : K] < \infty$, hence $R = K[\xi, \upsilon] = K(\xi, \upsilon) = L$, which implies $(g) \cap K[x] \neq 0$ and $(g) \cap K[y] \neq 0$. Then $g \in K^*$, a contradiction. Thus ξ or υ is transcendental over K. Let w.l.o.g. $\alpha := \xi$ transcendental, then $g(\alpha, \upsilon) = 0$, and so $[L : K(\alpha)] < \infty$. We have proved that L is an AFF over K.

Lemma 2.6. If $K \subseteq U \subseteq L$ are field extensions, L is an AFF over K and U is algebraic over K, then $[U : K] < \infty$.

T&N. Let $K \subseteq L$ and L be an AFF over K, then

$$\tilde{K} := \{\alpha \in L \mid [K(\alpha) : K] < \infty\}$$

is said to be the *field of constants* (of the AFF).

Corollary 2.7. $\tilde{K}$ is a subfield of L and $[\tilde{K} : K] < \infty$ for any AFF L over K.

Theorem 2.8. Let $K \subseteq L$, α be transcendental over K and $[L : K(\alpha)] < \infty$. Then the following conditions are equivalent for each $u \in L$:
(1) $[L : K(u)] < \infty$,
(2) $\exists g \in K[x, y]$ for which $g(x, u) \neq 0$ and $g(\alpha, u) = 0$,
(3) u is transcendental over K.

3. Valuation rings

K is a field. $R \leq K$ means that R is a subring of K and R^* is the group of invertible elements of R.

T&N. The notation (R, M) means that R is a *l*ocal ring with the unique maximal ideal M.

Observation. The following conditions are equivalent for an ideal M of a ring R:

(1) (R, M) is a local ring,
(2) each proper ideal of R is contained in M,
(3) $M = R \setminus R^*$,
(4) $R^* = R \setminus M$.

Lemma 3.1. Let (R, M) be a local ring and A a finitely generated ideal such that $AM = A$. Then $A = 0$.

Proposition 3.2. 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 unique $u \in R^*$ such that $s = t^i u$,
(2) if A is finitely generated, then $A = 0$.

T&N. Recall that a ring R is *noetherian* if all its ideals are finitely generated, and R is *uniserial* if for every pair of ideals I, J either $I \subseteq J$ or $J \subseteq I$.

Corollary 3.3. If (R, M) is a noetherian local domain with the field of fractions 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 unique $u \in R^*$ such that $s = t^i u$,
(2) for each $s \in K \setminus \{0\}$ there exist unique $i \in \mathbb{Z}$ and unique $u \in R^*$ such that $s = t^i u$,
(3) R is a uniserial principal ideal domain.

T&N. If $R \leq K$, R is called a *valuation ring* (VR) of K if for every $\alpha \in K^*$ either $\alpha \in R$ or $\alpha^{-1} \in R$.

Observation. Let K be the fraction field of a domain R and let $i : K^* \to K^*$ is defined $i(\alpha) = \alpha^{-1}$.

(1) R is a VR $\Rightarrow$ R is uniserial $\Rightarrow$ R is local,
(2) $i(R^*) = R^*$
(3) if R is a VR, then $i(M \setminus \{0\}) = i(R \setminus (R^* \cup \{0\}) = K^* \setminus R$.

Example 3.4. (1) $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}, p \text{ does not divide } b\}$ is a VR for each prime p (of the field of fractions $\mathbb{Q}$).

(2) $R_{x,y} = \{\frac{r}{s} \in \mathbb{R}(x, y) \mid r, s \in \mathbb{R}[x, y], s(0, 0) \neq 0\} \subseteq \mathbb{R}(x, y)$ is noetherian local domain with the maximal ideal (x, y), which is not a VR: for instance neither $\frac{x+y}{xy}$ nor $\frac{xy}{x+y}$ belongs to $R_{x,y}$.

Lemma 3.5. 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 $J[\alpha^{-1}] \subsetneq R[\alpha^{-1}]$.

Theorem 3.6. Let $R \leq K$ and I be an ideal satisfying $0 \neq I \neq R$.

(1) There exists a VR S of K with the maximal ideal M, for which $R \subseteq S \subsetneq K$ and $I \subseteq M$.
(2) If R is maximal subring of K, then it is a VR.

Observation. Let R_j, $j = 1, 2$, be valuation rings of K, $0 \neq M_j = R_j \setminus R_j^*$ and define $i(a) = a^{-1}$ $\forall a \in K^*$. Then

(1) $M_1 \subseteq M_2 \Leftrightarrow K \setminus R_1 = i(M_1 \setminus \{0\}) \subseteq i(M_2 \setminus \{0\}) = K \setminus R_2 \Leftrightarrow R_2 \subseteq R_1$,

(2) $M_1 = M_2 \Leftrightarrow R_1 = R_2$.

Observation. If R is a subring of a ring S and P is a prime ideal of S, then $P \cap R$ is a prime ideal of R.

Lemma 3.7. Let R_i be a noetherian VR of K with the maximal ideal $0 \neq M_i = R_i \setminus R_i^*$ for $= 1, 2$. Then for $i = 1, 2$

(1) R_i is a principal ideal domain, in particular M_i is principal,
(2) R_i is a maximal subring of K,
(3) $M_1 \subseteq M_2 \Leftrightarrow M_1 = M_2 \Leftrightarrow R_1 = R_2 \Leftrightarrow R_1 \subseteq R_2$.

4. Discrete valuation rings

In this section, R is a domain and $R \leq K$ means that K is the field of fractions of R.

Definition. A map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ is a *discrete valuation* (DV) 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 said to be the trivial discrete valuation if $\nu(K^*) = 0$.

We will suppose that all discrete valuations are nontrivial.

T&N. Let $R \leq K$, where R is noetherian and $p \in R$ a prime element. For each $a, b \in R \setminus \{0\}$ let us define

$$\nu_p(a) = \max\{i \mid p^i/a\}, \quad \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b), \quad \nu_p(0) = \infty.$$

Example 4.1. Let $R \leq K$, R be noetherian, and p a prime element. Then ν_p is a correctly defined discrete valuation of K.

Note that if $(R, (p))$ is a local ring, then p is prime.

Observation. Let ν be a discrete valuation of K and let us define

$$S = \{x \in K \mid \nu(x) \geq 0\}, \quad M = \{x \in K \mid \nu(x) > 0\}.$$

Then for each $x \in K^*$

(1) $\nu|_{K^*}$ is a group homomorphism of $(K^*, \cdot, ^{-1}, 1)$ into $(\mathbb{Z}, +, -, 0)$ by (D1), hence $\nu(1) = \nu(-1) = 0$ a $\nu(x^{-1}) = -\nu(x)$,
(2) S is a subring of K, M its ideal and S is a VR of K,
(3) $\nu(x) = 0 \Leftrightarrow \nu(x^{-1}) = -\nu(x) = 0 \Leftrightarrow x \in S^*$, $M = S \setminus S^*$ is the maximal ideal of S,
(4) if $I \neq 0$ is an ideal of S and $a \in I \setminus \{0\}$ is of minimal value $\nu(a)$, then $(a) = I$, since for $b \in I$ satisfying $\nu(b) \geq \nu(a)$ we get $\nu(ba^{-1}) \geq 0$, hence $ba^{-1} \in S$ a $b = aba^{-1} \in (a)$,
(5) S is a principal ideal domain.

Definition. Let $R \leq K$. R is said to be a *discrete valuation* ring (DVR), if there is a discrete valuation ν such that $R = \nu^{-1}(\langle 0, \infty\rangle) = \{a \in K \mid \nu(a) \geq 0\}$.

Proposition 4.2. The following is equivalent for a domain R which is not a field:

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 noetherian local ring such that its maximal ideal is principal.

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

Example 4.3. For a noetherian domain R and a prime element p, the localization $R_{(p)}$ is a DVR with the discrete valuation ν_p from 4.1.

In particular, $\mathbb{Z}_{(p)} \leq \mathbb{Q}$ from 3.4(1) is a DVR for each prime p.

Lemma 4.4. Let $R \leq K$ and R be a DVR with a uniformizing element t. Then for each DV μ with $R = \mu^{-1}(\langle 0, \infty\rangle)$ there exists unique $k \in \mathbb{N}$ for which $\mu = k\nu_t$.

Corollary 4.5. Let ν be a DV of K. Then ν is a NDV $\Leftrightarrow \exists t \in K : \nu(t) = 1$.

Lemma 4.6. If ν is a DV of K and $a, b \in K$ satisfies $\nu(a) \neq \nu(b)$, 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 of L and $K \subseteq R$. ν is a (normalized) discrete valuation of the AFF L over K, if ν is a (normalized) discrete valuation of L and $\nu(K^*) = 0$.

We define $\nu_\infty(\frac{a}{b}) = \deg(b) - \deg(a)$ for $a, b \in K[x] \setminus \{0\}$ on the AFF $K(x)$ and $\nu_\infty(0) = \infty$.

Observation. x^{-1} is a prime element of $K[x^{-1}]$ ($\cong K[x]$), $K(x) = K(x^{-1})$ and $\nu_\infty = \nu_{x^{-1}}$ is a NDV of the AFF $K(x)$ over K.

Proposition 4.7. A normalized discrete valuation of the AFF $K(x)$ over K is either ν_∞ or ν_p for an irreducible polynomial $p \in K[x]$.

In the sequel, L is an AFF over K and $\tilde{K}$ its field of constants.

Definition. Let us define

$\mathbb{P}_{L/K} = \{M \subset L \mid \exists$ a valuation ring of the AFF L over K $R : K \subseteq R \subsetneq L, M = R \setminus R^*\}$.

Every element $P \in \mathbb{P}_{L/K}$ is said to be a *place* of the AFF L over K, $\mathcal{O}_P$ denotes a VR of the AFF determined by P and the number

$$\deg P = \dim_K(\mathcal{O}_P/P) = [\mathcal{O}_P/P : \ (K+P)/P]$$

is called *degree* of P.

Theorem 4.8. If $P \in \mathbb{P}_{L/K}$, then

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

T&N. For any $P \in \mathbb{P}_{L/K}$ 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 $\mathrm{mult}(a) = \min(\sum_{j=1}^n i_j \mid a_{i_1 \dots i_n} \neq 0)$ is called *multiplicity* of the polynomial a.

Observation. If $a \in K[x]$, then $\mathrm{mult}(a) = \max\{i \geq 0 \mid x^i \text{ divides } a\}$, hence it is the multiplicity of the root 0.

Lemma 4.9. Let $z \in L \setminus \tilde{K}$, $a \in K[x]$, $P \in \mathbb{P}_{L/K}$. Then
(1) $\exists\, Q_1, Q_2 \in \mathbb{P}_{L/K}$ for which $\nu_{Q_1}(z) > 0 > \nu_{Q_1}(z)$,
(2) $\nu_P(z) \geq 0 \Rightarrow \nu_P(a(z)) \geq 0$,
(3) $\nu_P(z) > 0 \Rightarrow \nu_P(a(z)) = \mathrm{mult}(a) \cdot \nu_P(z)$,
(4) $\nu_P(z) < 0 \Rightarrow \nu_P(a(z)) = \deg(a) \cdot \nu_P(z)$.

5. Weierstrass equations

Recall that K is a field. $K \leq L$ denotes a field extension and $n \in \mathbb{N}$.

T&N. Let $K \leq L$ and A be a K-algebra. Denote
$\mathrm{End}_K(A) = \{\varphi : A \to A \mid \varphi \text{ is a } K\text{-homomorphism}\}$
$\mathrm{Aut}_K(A) = \{\varphi \in \mathrm{End}_K(A) \mid \varphi \text{ is a bijection}\}$
Let $A \in K^{n\times n}$, $b \in K^n$, define a map $\vartheta_A, \tau_b : K^n \to K^n$ by rules $\vartheta_A(v) = Av$, $\tau_b(v) = v + b$. Denote $\mathrm{Aff_n(K)} = \{\tau_b\vartheta_A \mid \mathrm{A \in GL_n(K), b \in K^n}\}$, elements of $\mathrm{Aff_n(K)}$ are called *affine maps.*

Observation. Let $K \leq L$, $A, B \in K^{n\times n}$, $b, c \in K^n$. Then
(1) $\tau_b\tau_c = \tau_{b+c}$, $\vartheta_A\vartheta_B = \vartheta_{AB}$, $\vartheta_A\tau_b = \tau_{\vartheta_A(b)}\vartheta_A$,
(2) $\tau_b\vartheta_A$ is a bijection $\Leftrightarrow A \in GL_n(K)$,
(3) $\mathrm{Aff_n(K)}$ is a subgroup of the permutation group $S(K^n)$,
(4) $\mathrm{Aff_n(K)}$ is a subgroup of $\mathrm{Aff}_n(L)$, where we identify $\tau_b\vartheta_A$ on K^n and L^n.

T&N. Let $\sigma \in \mathrm{Aff_n(K)}$ and $\mathbf{x} = (x_1, \ldots, x_n)$. Define $\sigma^* \in \mathrm{End}_K(K[\mathbf{x}])$ by

$$\sigma^*(f(x_1, \ldots, x_n)) = f(\sigma((x_1, \ldots, x_n))),$$

where σ is viewed as an element of $\mathrm{Aff}_n(K(\mathbf{x}))$. Elements of $\mathrm{Aff}_n^*(K) = \{\sigma^* \mid \sigma \in \mathrm{Aff_n(K)}\}$ are said to be *affine automorphisms.*

Observation. Let $\sigma, \rho \in \mathrm{Aff_n(K)}$, $\mathbf{x} = (x_1, \ldots, x_n)$ and $f \in K[\mathbf{x}]$
(1) $\rho^*\sigma^*(f(\mathbf{x})) = \rho^*(f(\sigma(\mathbf{x}))) = f(\sigma\rho(\mathbf{x})) = (\sigma\rho)^*(f(\mathbf{x}))$,
(2) $\mathrm{id}^*_{K^n} = \mathrm{id}_{K[\mathbf{x}]}$, $(\sigma^{-1})^* = (\sigma^*)^{-1}$,
(3) $\mathrm{Aff}_n^*(K)$ is a subgroup of $\mathrm{Aut}(K[\mathbf{x}])$.

T&N. Denote
- $T_n(K) = \{(d_{ij}) \in K^{n\times n} \mid d_{ii} \neq 0 \forall i,\ d_{ij} = 0 \forall i < j\}$,
- $U_n(K) = \{(d_{ij}) \in T_n(K) \mid d_{ii} = 1 \forall i\}$,
- $D_n(K) = \{(d_{ij}) \in T_n(K) \mid d_{ij} = 0 \forall i \neq j\}$.

Observation. $T_n(K)$, $U_n(K)$ a $D_n(K)$ are subgroups of $GL_n(K)$ and it holds that $T_n(K) = U_n(K)D_n(K) = D_n(K)U_n(K)$.

Definition. Let $f, g \in K[x]$ such that $\deg g \leq 1$, $\deg f = 3$, $lc(f) = 1$. Then the equation of the form $y^2 + yg(x) = f(x)$ is called a *Weierstrass equation* (WE), any polynomial $y^2 + yg(x) - f(x) \in K[x, y]$ is said to be a *Weierstrass (equation) polynomial* (WEP).

Observation. Let $w = y^2 + yg(x) - f(x)) \in K[x, y]$ be a WEP, $A = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \in U_2(K)$, $b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in K^2$.

1. $\tau_b^*(w) = (y+b_2)^2 + (y+b_2)g(x+b_1) - f(x+b_1) = y^2 + y(2b_2 + g(x+b_1)) - (f(x+b_1) - b_2^2 - b_2 g(x+b_1))$ is a WEP,
2. $\vartheta_A^*(w) = (y+ux)^2 + (y+ux)g(x) - f(x) = y^2 + y(2ux + g(x)) - (f(x) - u^2x^2 - uxg(x))$ is a WEP,
3. $U^* = \{(\tau_c\vartheta_B)^* \mid c \in K^2, B \in U_2(K)\}$ is a subgroup of $\mathrm{Aff}_2(\mathrm{K})$ and $\sigma^*(w)$ is a WEP for each $\sigma^* \in U^*$.

Lemma 5.1. If $\operatorname{char} K \neq 2$ and $\in K[x, y]$ is a WEP, then $\exists A \in U_2(K)$ and $\exists b \in K^2$ such that $(\tau_b\vartheta_A)^*(w) = y^2 - h(x)$ for some $h \in K[x]$, $\deg h = 3$ and $lc(h) = 1$, hence $y^2 - h(x)$ is a WEP as well.

T&N. A WEP is said to be *short*, if $\exists a_2, a_4, a_6 \in K$ such that it is of the form

(SH1) $y^2 - (x^3 + a_4x + a_6)$ if $\operatorname{char} K \neq 2, 3$,
(SH2) $y^2 - (x^3 + a_4x + a_6)$ or $y^2 + xy - (x^3 + a_4x + a_6)$ if $\operatorname{char} K = 2$,
(SH3) $y^2 - (x^3 + a_4x + a_6)$ or $y^2 - (x^3 + a_2x^2 + a_6)$ if $\operatorname{char} K = 3$.

By a better choice of b in 5.1 it could be shown the next observation.

Observation. If $\operatorname{char} K \neq 2, 3$ and $\in K[x, y]$ is a WEP, then there exists $\sigma \in \mathrm{Aff}_\mathrm{n}(\mathrm{K})$ such that $\sigma^*(w)$ is a short WEP.

Lemma 5.2. Let $\lambda \in K^*$, w be a WEP and $\sigma \in \mathrm{Aff}_2(\mathrm{K})$. Then $\exists$ WEP $\tilde{w}$ for which $\sigma^*(w) = \lambda\tilde{w} \Leftrightarrow w\exists\alpha, \delta, \gamma \in K$ a $\exists b \in K^2$such that $\alpha^3 = \delta^2 = \lambda$, $A = \begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix}$ and $\sigma = \tau_b\vartheta_A$.

If we consider $c = \delta\alpha^{-1}$, we get the following easy result:

Observation. Let $\alpha, \delta \in K^*$. Then $\alpha^3 = \delta^2 \Leftrightarrow \exists c \in K^*$ satisfying $\delta = c^3$ a $\alpha = c^2$.

Proposition 5.3. Let $w \in K[x, y]$ be a WEP and $\sigma \in \mathrm{Aff}_2(\mathrm{K})$. Then the following conditions are 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 $b \in \mathbb{A}^2(K)$ such that $A = \begin{pmatrix} c^2 & 0 \\ d & c^3 \end{pmatrix}$ and $\sigma = \tau_b\vartheta_A$.

T&N. We say that two WEPs $w, \tilde{w} \in K[x, y]$ are *K-equivalent* provided $\exists\sigma \in \mathrm{Aff}_2(\mathrm{K})$ satisfying $(\sigma^*(w)) = (\tilde{w})$ as ideals of $K[x, y]$.

Corollary 5.4. The following conditions are equivalent for two WEPs $w, \tilde{w} \in K[x, y]$:

1. w and $\tilde{w}$ are K-equivalent,
2. $\exists\ c \in K^*$, $d \in K$ and $b \in K^2$ such that $(\tau_b^*\vartheta_A^*(w)) = (\tilde{w})$ for $A = \begin{pmatrix} c^2 & 0 \\ d & c^3 \end{pmatrix}$,
3. $\exists\ c \in K^*$ and $d, b_1, b_2 \in K$ such that $\tilde{w} = c^{-6}w(c^2x + b_1, c^3y + dx + b_2)$.

Example 5.5. (1) Let $w = y^2 + y(2x+2) - (x^3 - 4x^2 + 1) \in \mathbb{R}[x, y]$. Then w is a WEP. We find a short WEP which is $\mathbb{R}$-equivalent to w. Applying linear algebra machinery we remove the term $2xy$: $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in U_2(\mathbb{R})$:

$$\vartheta_A^*(w) = (y-x)^2 + (y-x)(2x+2) - (x^3 - 4x^2 + 1) = y^2 + 2y - (x^3 - 3x^2 + 2x + 1)$$

then we use $b = (1, -1)$ to exclude monomials y and x^2:

$\tau_b^* \vartheta_A^*(w) = (y-1)^2 + 2(y-1) - ((x+1)^3 - 3(x+1)^2 + 2(x+1) + 1) = y^2 - (x^3 - x + 2)$.

(2) The polynomial $\tilde{w} = y^2 - (x^3 - x + 2)$ is

(a) $\mathbb{R}$-equivalent for example to the polynomial $y^2 - (x^3 - \frac{1}{16}x + \frac{1}{32})$ since $\vartheta_{A_1}^*(\tilde{w}) = 64y^2 - 64(x^3 - \frac{1}{16}x + \frac{1}{32})$ for $A_1 = \begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$,

(b) $\mathbb{C}$-equivalent to $y^2 - (x^3 - x - 2)$, because $\vartheta_{A_2}^*(\tilde{w}) = -y^2 - (-x^3 + x + 2)$ for $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$.

6. Singularities

$\overline{K}$ denotes the algebraic closure of a field K and $\mathbf{x} := (x_1, \dots, x_n)$ in this section.

T&N. Let $K \leq L \leq \overline{K}$. Let us denote the affine spaces

- $\mathbb{A}^n := \overline{K}^n$ over a field $\overline{K}$ and
- $\mathbb{A}^n(L) := L^n$ over a field L (L-rational points of $\mathbb{A}^n$).

For $a \in K[\mathbf{x}]$, $M \subset K[\mathbf{x}]$ we will denote:

- $V_M = \{\alpha \in \mathbb{A}^n \mid a(\alpha) = 0 \forall a \in M\}$ (*variety*),
- $V_M(L) = V_M \cap \mathbb{A}^n(L)$, $V_a = V_{\{a\}}$, $V_a(L) = V_{\{a\}}(L)$.

If $a \in K[x, y]$ and $\deg a \geq 1$, then V_a is said to be an *affine (planar) curve.*

Recall that it is well known that $V_M = V_{(M)}$ for each $M \subset K[\mathbf{x}]$.

Observation. Let $a \in K[\mathbf{x}]$ and $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{A}^n$. Then $\operatorname{mult} \tau_\beta^*(a) \geq 1 \Leftrightarrow \operatorname{mult} a(x_1 + \beta_1, \dots, x_n + \beta_n) \geq 1 \Leftrightarrow a(\beta_1, \dots, \beta_n) = 0 \Leftrightarrow \beta \in V_a$.

T&N. Let $a = \sum_{i_1 \dots i_n} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} = \sum_j b_j x_i^j \in K[\mathbf{x}]$, where $b_j \in K[\mathbf{x} \setminus \{x_i\}]$. Then

$$L(a) = \sum_{i_1 \dots i_n : \sum_j i_j = 1} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} = \sum_{j=1}^{n} a_{\delta_{1j} \dots \delta_{nj}} x_j$$

is called the *linear part* of a polynomial a and

$\frac{\partial a}{\partial x_i} = \sum_j (j+1) b_{j+1} x_i^j$ is a (partial) *derivative* of a polynomial a in a variable x_i.

If $\alpha = (\alpha_1, \dots, \alpha_n) \in V_a$ and $c_i := \frac{\partial a}{\partial x_i}(\alpha)$. Then $t_\alpha(a) := \sum_i c_i x_i - \sum_i c_i \alpha_i = \sum_i c_i(x_i - \alpha_i)$ is called a *tangent* of a (or V_a) at the point α, and we say that a (or V_a) is *smooth* at α if $t_\alpha(a) \neq 0$, and *singular* at α if $t_\alpha(a) = 0$.

Definition. Polynomial a (or variety V_a) is

- *smooth* if it is smooth at all points $\alpha \in V_a$ and
- *singular* if $\exists$ a singular point $\alpha \in V_a$ (such an α is called a *singularity* of V_a).

Observation. If $a \in K[\mathbf{x}]$ and $\alpha \in V_a$, then

(1) a is smooth at $\alpha \Leftrightarrow \exists i \frac{\partial a}{\partial x_i}(\alpha) \neq 0$,

(2) $\alpha \in V_{t_\alpha(a)}$.

Example 6.1. Let $w = y^2 - (x^3 + x - 2) \in \mathbb{R}[x, y]$ be a short WEP. Then $L(w) = -x$, $\frac{\partial w}{\partial x} = -3x^2 - 1$, $\frac{\partial w}{\partial y} = 2y$.

For $\alpha = (1, 0) \in V_w$ we get $t_\alpha(w) = -4(x - 1)$.

Lemma 6.2. Let $a \in \overline{K}[\mathbf{x}]$, $\alpha \in \mathbb{A}^n$, and $\sigma \in \mathrm{Aff_n}(\overline{\mathrm{K}})$. Then

(1) $t_\alpha(a) = \tau^*_{-\alpha}(L(\tau^*_\alpha(a)))$, whenever $\alpha \in V_a$,

(2) $\alpha \in V_{\sigma*(a)} \Leftrightarrow \sigma(\alpha) \in V_a$; in such a case $t_\alpha(\sigma^*(a)) = \sigma^*(t_{\sigma(\alpha)}(a))$,

(3) $\sigma(V_{\sigma*(a)}) = V_a$,

(4) $\sigma^*(a)$ is singular at $\alpha \in V_{\sigma*(a)} \Leftrightarrow a$ is singular at $\sigma(\alpha) \in V_a$.

Corollary 6.3. Let $w, \tilde{w} \in K[x, y]$ be K-equivalent WEPs. Then w is smooth $\Leftrightarrow \tilde{w}$ is smooth.

Recall that a polynomial is *separable* if all its rots in its splitting field are simple and the field is *perfect*, provided all its irreducible polynomials separable.

Proposition 6.4. If $w = y^2 - f(x)$ is a WEP for $f(x) \in K[x]$, then w has at most 1 singularity. If, furthermore, $char K \neq 2$, then

(1) w is smooth $\Leftrightarrow f$ is separable,

(2) a singularity is K-rational whenever K is perfect.

Example 6.5. (1) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ is a smooth short WEP,

(2) $(y + 1)^2 - (x^3 + 1) \in \mathbb{F}_3[x, y]$ is a singular WEP with the singularity $(2, 2)$,

(3) $y^2 - (x^3 - x^2 - x + 1) \in \mathbb{R}[x, y]$ is a singular WEP with the singularity $(1, 0)$.

7. Coordinate rings

Let us denote $\mathbf{x} := (x_1, \dots, x_n)$ and $\mathbb{A}^n$ is an affine space over $\overline{K}$.

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

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

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

Observation. (1) If I is an ideal of $K[\mathbf{x}]$ such that $I \cap K[x_i] = (a_i) \neq 0 \ \forall i$, then $K[\mathbf{x}]/I$ is generated as a K-space by the set $\{\prod_i x_i^{j_i} \mid j_i < \deg(a_i)\}$, hence $\dim_K K[\mathbf{x}]/I \leq \prod_i \deg(a_i) < \infty$.

(2) If R is a domain and a K-algebra satisfying $\dim_K R < \infty$, then $K[\alpha]$ is a field for every $\alpha \in R$, thus R is a field as well.

Lemma 7.1. Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{A}^n$

(1) I_α is a maximal ideal,

(2) $\alpha \in \mathbb{A}^n(K) \Leftrightarrow K + I_\alpha = K[\mathbf{x}] \Leftrightarrow I_\alpha = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$.

Lemma 7.2. Let $K \leq L$ be an extension such that $[L : K] < \infty$ and I an ideal of $K[\mathbf{x}]$.

(1) $(IL[\mathbf{x}]) \cap K[\mathbf{x}] = I$,

(2) if I is prime with $I \cap K[x_i] \neq 0$ for all $i = 1, \dots n$, then there exists $\alpha \in \mathbb{A}^n$ for which $I = I_\alpha$.

Lemma 7.3. If $a, b \in K[x, y] \setminus K$ are coprime, then $(a, b) \cap K[x] \neq 0 \neq (a, b) \cap K[y]$.

Theorem 7.4. Let P be a nonzero prime ideal of $K[x, y]$. Then

(1) either P is maximal, then it is not principal and there exists $\gamma \in \mathbb{A}^2$ for which $P = I_\gamma$,

(2) or $P = (p)$ for some irreducible $p \in K[x, y]$.

Note that V_P is finite for P maximal, and if $p, q \in K[x, y]$ are non-associated irreducible, $V_{(p)}$ is infinite and $V_{\{p,q\}} = V_p \cap V_q$ finite.

Example 7.5. For a WEP $w = y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ for example ideals

$$(w) \subseteq (y, x+1) = I_{(-1,0)}, \quad (y, x^2 - x + 1) = I_u, \quad (y^2 + 1, x + \sqrt[3]{2}) = I_{(-\sqrt[3]{2}, i)},$$

$u = (e^{\frac{\pi}{3} i}, 0)$, are prime.

T&N. Let $C = V_a$ be an affine planar curve for $a \in K[x, y]$ such that $I_C = (a)$. Then $K[C] = K[x, y]/I_C = K[x, y]/(a)$ is a *coordinate ring* of the curve C. The curve C is said to be *irreducible* if $K[C]$ is a domain and an element $p(x, y) + I_C$ is called a *polynomial at* C for any $p \in K[x, y]$.

If w is a WEP, then V_w is called a *Weierstrass curve.*

Observation. Let $a \in K[x, y]$ be irreducible, $C = V_a$ and $I_C = (a)$.

(1) C is irreducible $\Leftrightarrow$ $I_C = (a)$ is prime $\Leftrightarrow$ a is irreducible,

(2) the map $\iota : K[C] \to \overline{K}^C$ given by the rule $\iota(p + (a))(\alpha) = p(\alpha)$ for each $\alpha \in C$ is a well-defined injective map.

T&N. If $a \in K[x, y]$ is irreducible and $C = V_a$, then the field of fractions

$$K(C) = \{\frac{n + (a)}{d + (a)} \mid n \in K[x, y], d \in K[x, y] \setminus (a)\}$$

of $K[C]$ is said to be a *function field* of the irreducible curve C.

Proposition 7.6. Let $a \in K[x, y]$ be irreducible, $C = V_a$, $\alpha = x + (a)$, $\beta = y + (a) \in K[C]$. Then $K(C) = K(\alpha, \beta)$ is an AFF over K and α is transcendental over K $\Leftrightarrow$ $[K(C) : K(\alpha)] = \deg_y a > 0$.

Corollary 7.7. Let $K \leq L$. Then $\exists \alpha, \beta \in L$ such that $L = K(\alpha, \beta)$ is an AFF over K $\Leftrightarrow$ $\exists$ an irreducible affine curve $C \subset \mathbb{A}^2$ satisfying $L \cong_K K(C)$.

T&N. Let $w \in K[x, y]$, L is an AFF over K and $\alpha, \beta \in L$. We say that an *AFF L is given by* (the equation) $w(\alpha, \beta) = 0$ (over K) , if

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

(2) w is irreducible,

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

Example 7.8. If $w \in K[x, y]$ is irreducible and $\alpha = x + (w)$, $\beta = y + (w)$, then $K(V_w)$ is given by $w(\alpha, \beta) = 0$ over K.

8. Absolutely irreducible polynomials

T&N. $f \in K[x,y]$ is called *absolutely irreducible*, if f is irreducible in the domain $\overline{K}[x,y]$.

Example 8.1. The polynomial x^2+y^2 is irreducible but not absolutely irreducible in $\mathbb{R}[x,y]$ ($\mathbb{F}_3[x,y]$), since $x^2+y^2=(x+iy)(x-iy)$ in $\mathbb{C}[x,y]$ (i stands for an element of the order 4 in $\mathbb{F}_9^* \subset \overline{\mathbb{F}}_3$).

Polynomial x^2+y is absolutely irreducible in $\mathbb{R}[x,y]$ ($\mathbb{F}_3[x,y]$).

Lemma 8.2. If for $f,g \in K[x]$ holds true that $\deg g \leq 1$ and $\deg f \geq 3$ is odd, then $w = y^2 + yg(x) - f(x)$ is absolutely irreducible in $K[x,y]$.

Proposition 8.3. Let $w \in K[x,y]$ be irreducible and $\tilde{K}$ be the field of constants of the AFF $K(V_w)$ over K. Then $K=\tilde{K} \Leftrightarrow w$ is irreducible in $\tilde{K}[x,y]$.

Corollary 8.4. If $w \in K[x,y]$ is a WEP and $C=V_w$ is a Weierstrass curve, then w is absolutely irreducible and all elements $K(C)\setminus K$ are transcendental over K.

Example 8.5. Let $w=y^2+yx+x^3+1 \in \mathbb{F}_2[x,y]$ be a WEP and denote L the fraction field of $\mathbb{F}_2[x,y]/(w)$, hence L is the function field of the curve V_w, which is an AFF over $\mathbb{F}_2$ by 7.6. Since w is absolutely irreducible by 8.2, we can compute the field of constants $\tilde{\mathbb{F}_2}=\mathbb{F}_2$ using 8.3. Since for example polynomials x^2+x+1 and x^3+x+1 has no root in $\mathbb{F}_2$ they have no root in L, so both are irreducible over L.

9. Places determined by a pair

In this section, L denotes an AFF over K given by $w(\alpha,\beta)=0$ with $\deg(w)\geq 2$.

Observation. Let $a \in K[x,y] \subseteq L[x,y]$, $\sigma \in \mathrm{Aff}_2(\mathrm{K})$, and $\tilde{\alpha}$, $\tilde{\beta} \in L$. Denote by $\overline{\sigma} \in \mathrm{Aff}_2(\mathrm{L})$ the unique extension of σ and put $u=\sigma^*(x)(\tilde{\alpha},\tilde{\beta})$, $v=\sigma^*(y)(\tilde{\alpha},\tilde{\beta})$. Then

(1) $(\sigma^{-1})^*(a(\sigma^*(x),\sigma^*(y)))=a(x,y)$,
(2) $w(x,y)=a(\sigma^*(x),\sigma^*(y)) \Leftrightarrow a=(\sigma^{-1})^*(w)$,
(3) $\overline{\sigma}^*(a)=\sigma^*(a)\in K[x,y]$.
(4) $(u,v)=(\sigma^*(x)(\tilde{\alpha},\tilde{\beta}),\sigma^*(y)(\tilde{\alpha},\tilde{\beta}))=\overline{\sigma}(\tilde{\alpha},\tilde{\beta})$,
(5) $(\tilde{\alpha},\tilde{\beta})=\overline{\sigma}^{-1}(u,v)$, hence $K(\tilde{\alpha},\tilde{\beta})=K(u,v)$
(6) $(\sigma^{-1})^*(w)(u,v)=w(\overline{\sigma}^{-1}(u,v))=w(\tilde{\alpha},\tilde{\beta})$.

We will use notation $\overline{\sigma}$ from the last observation in the sequel. Put $\mathrm{mult}(0)=\infty$.

Lemma 9.1. Let w be smooth at $\gamma=(\gamma_1,\gamma_2)\in V_w(K)$, $A\in \mathrm{GL}_2(K)$, $\sigma := \vartheta_A\tau_{-\gamma}$ and put $(u,v)=\overline{\sigma}(\alpha,\beta)$ and $f_\sigma=(\sigma^{-1})^*(w)$. Then

(1) L is an AFF over K given by $f_\sigma(u,v)=0$,
(2) $\exists$ a matrix A such that $f_\sigma = yg(x,y)+h(x)+y$ where $h\in K[x]\setminus\{0\}$, $g\in K[x,y]$, $\mathrm{mult}(h)\geq 2$, $\mathrm{mult}(g)\geq 1$,
(3) if $t_\gamma(f)=a_1(x-\gamma_1)+a_2(y-\gamma_2)$, then A is a matrix from (2) $\Leftrightarrow A=\begin{pmatrix} b_1,b_2\\ a_1,a_2\end{pmatrix}$ for $(b_1,b_2)\in K^2\setminus \mathrm{Span}_{\mathrm{K}}((a_1,a_2))$.

Let us suppose that L is an AFF over K given by $w(\alpha,\beta)=0$ with $\deg(w)\geq 2$ and simultaneously by $f(u,v)=0$, where $f=yg(x,y)+h(x)+y\in K[x,y]$, $h\in K[x]\setminus\{0\}$, $g\in K[x,y]$, $\mathrm{mult}(h)\geq 2$, $\mathrm{mult}(g)\geq 1$.

Put $m:=\mathrm{mult}(h)$ (which is finite by 9.1).

T&N. Let $a=\sum_{i,j\geq 0}a_{ij}x^iy^j\in K[x,y]\setminus\{0\}$, then define:
$\mu(a):=\mathrm{mult}(a(x,y^m))$,
$s(a):=\{(i,j)\in\mathbb{Z}^2|\ i,j\geq 0, i+jm=\mu(a)\}$,
$S(a):=\sum_{(i,j)\in s(a)}a_{ij}x^iy^j$.

Observation. Let $a,b=\sum_{i,j}b_{ij}x^iy^j\in K[x,y]\setminus\{0\}$ and $i,j,k,l\geq 0$. Then

(1) $\mathrm{mult}(a\cdot b)=\mathrm{mult}(a)+\mathrm{mult}(b)$,
and if $\mathrm{mult}(a)<\mathrm{mult}(b)$, then $\mathrm{mult}(a+b)=\mathrm{mult}(a)$,

(2) $\mu(a\cdot b)=\mathrm{mult}(a(x,y^m)\cdot b(x,y^m))=\mathrm{mult}(a(x,y^m))+\mathrm{mult}(b(x,y^m))=\mu(a)+\mu(b)$, and if $\mu(a)<\mu(b)$, then $\mu(a+b)=\mu(a)\geq\mathrm{mult}(a)$,

(3) If $(i+jm)+(k+lm)=\mu(a)+\mu(b)=\mu(ab)$ and $(i+jm)>\mu(a)\Rightarrow(k+lm)<\mu(b)$ $\Rightarrow b_{kl}=0$, hence

$$S(a)S(b)=\sum_{(i,j)\in s(a)}\sum_{(k,l)\in s(b)}a_{ij}b_{kl}x^{i+k}y^{j+l}=\sum_{(q,r)\in s(ab)}x^qy^r\sum_{(i,j)+(k,l)=(q,r)}a_{ij}b_{kl}=S(ab),$$

(4) $\mu(a)=\mu(S(a))$, and if $\mu(a)<\mu(b)$, then $S(a+b)=S(a)$.

T&N. Denote by Λ the K-endomorphism of $K[x,y]$ defined for each $a\in K[x,y]$ by the rule

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

Lemma 9.2. $\mu(\Lambda(x^iy^j))=i+jm$ and there exists $\lambda\in K\setminus\{0\}$ such that $S(\Lambda(x^iy^j))=\lambda x^{i+jm}$ for each $i,j\geq 0$.

Example 9.3. Let $w=(y+x+1)^2-(x^3+2x+1)\in\mathbb{R}[x,y]$.

Since $\gcd(x^3+2x+1,3x^2+2)=1$, the polynomial w is a smooth WEP and it holds that $f=\frac{1}{2}w=\frac{1}{2}(y^2+x^2+2yx+2y-x^3)=y(x+\frac{1}{2}y)+\frac{1}{2}(x^2-x^3)+y$. so $f=yg(x,y)+h(x)+y$ for $g=x+\frac{1}{2}y$ and $h=\frac{1}{2}(x^2-x^3)$. Note that $\mathrm{mult}(g)=1$ and $m=\mathrm{mult}(h)=2$. Then compute
$\mu(g)=\mathrm{mult}(x+\frac{1}{2}y^2)=1$, $S(g)=x$,
$\mu(h)=\mathrm{mult}(h)=2$, $S(h)=\frac{1}{2}x^2$,
$\mu(x^3y^2)=3+2\cdot 2=7$, $\mu(x^2y^3)=2+3\cdot 2=8\Rightarrow\mu(x^3y^2+x^2y^3)=7$,
$S(\Lambda(x^3y^2+x^2y^3))=S(\Lambda(x^3y^2))=\frac{1}{4}x^7$ by 9.2.

Observation. Let $a=\sum_{ij}a_{ij}x^iy^j\in K[x,y]\setminus\{0\}$, $u,v\in P\in\mathbb{P}_{L/K}$ and $t=a(u,v)$.

(1) $\Lambda(a)(u,v)=a(u,-h(u)-vg(u,v))=a(u,v)$,

(2) $m\nu_P(u)=\nu_P(h(u))=\nu_P(v(-g(u,v)-1))=\nu_P(v)+\nu_P(-g(u,v)-1)=\nu_P(v)$ by 4.9,

(3) $\nu_P(t)\geq\min\{\nu_P(u^iv^j)\mid a_{ij}\neq 0\}=\min\{(i+mj)\nu_P(u)\mid a_{ij}\neq 0\}=\mu(a)\nu_P(u)$, hence $\mu(a)\leq\frac{\nu_P(t)}{\nu_P(u)}$.

T&N. Put $\mu(t)=\max\{\mu(a)\mid a\in K[x,y]:a(u,v)=t\}$ for each $t\in K[u,v]$.

Lemma 9.4. Let $t \in K[u,v]\setminus\{0\}$ and $k := \mu(t)$. Then there exist $\lambda \in K^*$ and $b \in K[x,y]$ satisfying $\mu(b) > k$ and $t = \lambda u^k + b(u,v)$.

Theorem 9.5. There exists a unique $P \in \mathbb{P}_{L/K}$ such that $u, v \in P$. Furthermore, it holds true that $\nu_P(u) = 1$, $\nu_P(v) = m$ and $\nu_P(r \cdot s^{-1}) = \mu(r) - \mu(s)$ for each $r, s \in K[u,v] \setminus \{0\}$.

Example 9.6. Consider a polynomial $f = y(x + \frac{1}{2}y) + \frac{1}{2}(x^2 - x^3) + y$ from 9.3. Then $L = \mathbb{R}(u,v)$ for $u = x + (f)$, $v = y + (f)$ and let P be the uniquely determined place from 9.5 Then $\nu_P(u) = 1$ and $\nu_P(v) = \mathrm{mult}(h) = 2$. Let us compute $\nu_P(u^2 + v)$ and $\nu_P(u^2 + 2v)$:

$f(u,v) = 0 \Rightarrow v = -v(u + \frac{1}{2}v) + \frac{1}{2}(u^3 - u^2)$, hence
$\nu_P(u^2 + v) = \nu_P(\frac{1}{2}u^2 - vu - \frac{1}{2}v^2 + \frac{1}{2}u^3) = \min(2,3,4,3) = 2$ and
$\nu_P(u^2{+}2v) = \nu_P(u^3{-}2vu{-}v^2) = \nu_P(u(u^3{-}2v){-}v^2) = \min(3,4) = 3$ since $\nu_P(u^2{-}2v) = \nu_P(-u^3 + 2vu + v^2 + 2u^2) = \min(2,3,4,3) = 2$ and so $\nu_P(u(u^3 - 2v)) = 3$.

Theorem 9.7. Let w be smooth at $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$.

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

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

T&N. If $p \in K[x]$ and $\gamma \in K$, denote by $\mathrm{mult}_\gamma(p) = \mathrm{mult}(\tau^*_{-\gamma}(p))$ the multiplicity of a root γ of p, i.e the non-negative integer k satisfying $(x-\gamma)^k | p$ and $(x-\gamma)^{k+1} \not| p$..

Observation. If $p, s \in K[x]$, $g \in K[x,y]$, $\gamma \in K$ is a root of s, $\mathrm{mult}_\gamma(g(x - \gamma, s(x))) \geq \mathrm{mult}(g)$.

This year we omit the proof of the following fact:

Proposition 9.8. Let $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$, $\frac{\partial w}{\partial y}(\gamma) \neq 0$, $\lambda, \mu \in K$ satisfy $l = y - \lambda x - \mu$ and $l(\gamma) = 0$, and $(\alpha - \gamma_1, \beta - \gamma_2) \subset P \in \mathbb{P}_{L/K}$. Then $\nu_P(l(\alpha,\beta)) = \mathrm{mult}_{\gamma_1}(w(x, \lambda x + \mu))$.

Example 9.9. Let $f = y^2 + xy + x^5 + 32 \in \mathbb{R}[x,y]$, then f is an absolutely irreducible by 8.2. Denote by L the AFF over $\mathbb{R}$ given by $f(\alpha,\beta) = 0$ for $\alpha = x + (f)$ and $\beta = y + (f) \in \mathbb{R}[x,y]/(f)$. Since $(-2,2) \in V_f$ and $\frac{\partial f}{\partial x} = y + 5x^4$, $\frac{\partial f}{\partial y} = 2y + x$, we get $\frac{\partial f}{\partial x}(-2,2) = 82$, $\frac{\partial f}{\partial y}(-2,2) = 2$ and $t = t_{(-2,2)}(f) = 82x + 2y + 160$.

By 9.7 there exists the unique $P \in \mathbb{P}_{L/K}$ containing $\alpha + 2, \beta - 2$.
For $u = \beta + 41\alpha + 80 = \frac{1}{2}t(\alpha,\beta)$ we determine the value $\nu_P(u)$ by applying 9.8:
$\hat{f} = f(x, -41x - 80) = x^5 + 40 \cdot 41x^2 - 80 \cdot 81 + 80^2 + 32$.
Since $0 = \hat{f}(-2) = \hat{f}'(-2) \neq \hat{f}''(-2)$ we get $\nu_P(u) = 2$.

10. Localization in a coordinate ring

Let us suppose again that L is an AFF over K given by $w(\alpha,\beta) = 0$ with $\deg(w) \geq 2$ and by $f(u,v) = 0$, where $f = yg(x,y) + h(x) + y \in K[x,y]$, $h \in K[x] \setminus \{0\}$, $g \in K[x,y]$, $m = \mathrm{mult}(h) \geq 2$, $\mathrm{mult}(g) \geq 1$.

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

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

the localization of $K[x,y]$ in the maximal ideal I_γ, $(I_\gamma) = \{\frac{a}{b} \in R_\gamma \mid a \in I_\gamma, b(\gamma) \neq 0\}$ denotes the (unique) maximal ideal of R_γ and $\omega_\gamma : R_\gamma \to L$ is a ring homomorphism defined by the rule $\omega_\gamma(\frac{a}{b}) = \frac{a(\alpha,\beta)}{b(\alpha,\beta)}$. Then let us denote

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

If w is fixed we will write $\mathcal{O}_\gamma$ instead $_w\mathcal{O}_\gamma$ and P_γ instead $_wP_\gamma$.

Observation. If $\gamma \in V_w(K)$, $\sigma \in \mathrm{Aff}_2(\mathrm{K})$ such that $f = (\sigma^{-1})^*(w)$ and $\sigma(\gamma) = (0,0)$ and denote $\mathcal{O}_\gamma =_w \mathcal{O}_\gamma$, $P_\gamma =_w P_\gamma$, then

(1) $\mathcal{O}_\gamma$ is a local ring with the maximal ideal P_γ,
(2) $\mathcal{O}_\gamma = K + P_\gamma$, hence $\dim_K(\mathcal{O}_\gamma / P_\gamma) = 1$,
(3) $\mathcal{O}_\gamma = {}_f\mathcal{O}_{(0,0)}$ a $P_\gamma = {}_fP_{(0,0)}$.

Lemma 10.1. If w is singular at $\gamma \in V_w(K)$, then $\mathcal{O}_\gamma$ is not a valuation ring.

Example 10.2. Let $w = (y+1)^2 - (x+2)^3$ and L be an AFF over $\mathbb{F}_5$ given by $w(\alpha, \beta) = 0$ for $\alpha = x + (w)$ and $\beta = y + (w) \in K[x,y]/(w)$ (cf. 7.8). Then $(3,4) \in V_w(\mathbb{F}_5)$ is a singularity of w and by the proof of 10.1 $\frac{\alpha+2}{\beta+1} \notin {}_wO_{(3,4)}$ and $\frac{\beta+1}{\alpha+2} \notin {}_wO_{(3,4)}$.

Lemma 10.3. Let $u, v \in P \in \mathbb{P}_{L/K}$ and $z \in K[u,v] \setminus \{0\}$. Then $\exists a, b \in K[x,y] \setminus I_{(0,0)}$ (i.e. $\mathrm{mult}(a) = \mathrm{mult}(b) = 0$) such that $\frac{z}{u^{\nu_P(z)}} = \frac{a(u,v)}{b(u,v)} \in {}_f\mathcal{O}^*_{(0,0)} = {}_f\mathcal{O}_{(0,0)} \setminus {}_fP_{(0,0)}$.

Proposition 10.4. Let w be smooth at $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$, and $(\alpha - \gamma_1, \beta - \gamma_2) \subseteq P \in \mathbb{P}_{L/K}$. Then

(1) $\exists\ \tilde{u} \in P_\gamma$ such that $\nu_P(\tilde{u}) = 1$ and $z\tilde{u}^{-\nu_P(z)} \in \mathcal{O}^*_\gamma$ for each $z \in K[\alpha, \beta] \setminus \{0\}$,
(2) $P = P_\gamma$,
(3) $\mathcal{O}_P = \mathcal{O}_\gamma$.

Example 10.5. Consider $f = y^2 + xy + x^5 + 32 \in \mathbb{R}[x,y]$ from 9.9, where L is an AFF over $\mathbb{R}$ given by $f(\alpha, \beta) = 0$. Put $t = t_{(-2,2)}(f) = 82x + 2y + 160$ and compute $P = P_{(-2,2)} \in \mathbb{P}_{L/\mathbb{R}}$. Since $(-2,2)$ is a zero of both lines $x+2$, $x+y$, and $x+2, x+y \notin (t)$, 9.7 implies that $\nu_P(\alpha+2) = \nu_P(\alpha+\beta) = 1$.

Hence $P_{(-2,2)} = (\alpha+2) = \{(\alpha+2)\frac{p(\alpha,\beta)}{q(\alpha,\beta)} \mid q(-2,2) \neq 0\}$.

Observation. Let $0 \neq M \subsetneq K[\alpha, \beta]$ be a prime ideal and $\hat{K} = K[\alpha,\beta]/M$. Then

(1) M a maximal ideal of $K[\alpha,\beta]$ and $\hat{K} = K[x,y]/I_\gamma$ for some $\exists \gamma \in V_w$ by 7.4,
(2) $\hat{K} = K[\alpha + M, \beta + M]$ is a field and $[\hat{K} : K] < \infty$,
(3) $\alpha + M, \beta + M$ are algebraic over K,
(4) $[\hat{K} : K] = 1 \Leftrightarrow \exists(\gamma_1, \gamma_2) \in V_w(K)$ such that $M = (\alpha - \gamma_1, \beta - \gamma_2)$ by 7.1(2) and (1).

Lemma 10.6. 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 $K[\alpha,\beta] \not\subseteq \mathcal{O}_P$, then $\tilde{P} = 0$ and either $\nu_P(\alpha) < 0$ or $\nu_P(\beta) < 0$.
(3) If $K[\alpha,\beta] \not\subseteq \mathcal{O}_P$ and w is a WEP, then $3\nu_P(\alpha) = 2\nu_P(\beta) < 0$.

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

Theorem 10.7. Let $P \in \mathbb{P}^{(1)}_{L/K}$ and a polynomial w be smooth at all points of $\gamma \in V_w(K)$. Then the following conditions are equivalent:
(1) $K[\alpha,\beta] \subseteq \mathcal{O}_P$,
(2) $\exists$ a unique $(\gamma_1,\gamma_2) \in V_w(K)$ for which $\nu_P(\alpha-\gamma_1) > 0$ and $\nu_P(\beta-\gamma_2) > 0$,
(3) $\exists$ a unique $\gamma \in V_w(K)$ for which $P = P_\gamma$.

Corollary 10.8. If a WEP w is smooth at all points $\gamma \in V_w(K)$ and $P \in \mathbb{P}^{(1)}_{L/K}$ then either $\exists \gamma \in V_w(K)$ for which $P = P_\gamma$ or $\alpha^{-1}, \beta^{-1} \in P$.

11. Weak Approximation Theorem

L is an AFF over K with the field of constants $\tilde{K}$.

Observation. Let $a, b \in L$.
(1) If $a \notin \tilde{K}$, then $\exists P \in \mathbb{P}_{L/K}$ such that $\nu_P(a) > 0$ by 3.6,
(2) $\tilde{K}^* = \{s \in L \mid \nu_P(s) = 0 \ \forall P \in \mathbb{P}_{L/K}\}$ by (1) and 4.8,
(3) if $P \in \mathbb{P}_{L/K}$ satisfies $\nu_P(a) \neq 0 \neq \nu_P(b)$, then $\nu_P(a+b^k) = \min(\nu_P(a), k\nu_P(b))$ for all but one k by 4.6, hence $\exists k_0$ such that the equality holds $\forall k \geq k_0$.

Lemma 11.1. Let $n \geq 1$ and $P_1, \dots, P_n \in \mathbb{P}_{L/K}$ be pairwisely distinct places. If $\nu_i := \nu_{P_i}$ for all i, $a_1, \dots a_n \in L$ and $z \in \mathbb{Z}$, then
(1) $\exists\ s \in L^*$ such that $\nu_1(s) > 0$ and $\nu_i(s) < 0$ for each $i = 2, \dots, n$,
(2) $\exists\ t \in L$ such that $\nu_i(t - a_i) > z$ for each $i = 1, \dots, n$.

Theorem 11.2 (Weak Approximation Theorem)**.** Let $n \geq 1$ and $P_1, \dots, P_n \in \mathbb{P}_{L/K}$ be pairwise distinct places. If $a_1, \dots a_n \in L$ and $z_1, \dots, z_n \in \mathbb{Z}$, then there exists $s \in L$ such that $\nu_{P_i}(s - a_i) = z_i$ for all $i = 1, \dots, n$.

Corollary 11.3. $\mathbb{P}_{L/K}$ is infinite.

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

Corollary 11.4. If $n \geq 1$, $e \geq 0$ and $P, P_1, \dots, P_n$ are pairwise distinct, then $\exists$ a basis B of the K-algebra $\mathcal{O}_P$ modulo P such that $B \subset P_j^e \setminus P_j^{e+1}$ $\forall j = 1, \dots, n$.

Observation. Let $P \in \mathbb{P}_{L/K}$ and $b_1, \dots, b_n \in \mathcal{O}_P$ is linearly independent modulo P over K, $t \in P$, $\nu_P(t) = 1$, λ_i, $\lambda_{ij} \in K$ for $i = 1, \dots, n$, $j = 0, \dots, e-1$ and $\exists i : \lambda_i \neq 0$ and $\exists (i,j) : \lambda_{ij} \neq 0$. Then
(1) $\nu_P(\sum_i \lambda_i b_i) = 0$, since $\sum_i \lambda_i b_i \notin P$,
(2) $\nu_P(\sum_i \lambda_i b_i t^j) = \nu_P(\sum_i \lambda_i b_i) + \nu_P(t^j) = j$,

(3) $\nu_P(\sum_{ij} \lambda_{ij} b_i t^j) = \min\{j \mid \exists i : \lambda_{ij} \neq 0\}$ by 4.6,

(4) $\{b_i t^j \mid i = 1, \dots, n,\ j = 0, \dots, e-1\}$ is linearly independent modulo P^e.

Proposition 11.5. Let $P_1, \dots, P_n \in \mathbb{P}_{L/K}$ be pairwise distinct places for $n \geq 1$. If $s \in \bigcap_{i=1}^n P_i$, then $[L : K(s)] \geq \sum_{i=1}^n \nu_{P_i}(s) \deg P_i$.

Corollary 11.6. If $s \in L^*$, then the set $\{P \in \mathbb{P}_{L/K} \mid \nu_P(s) \neq 0\}$ is finite.

Corollary 11.7. If w is a WEP and L is given by $w(\alpha, \beta) = 0$, then there exists unique $P_\infty \in \mathbb{P}_{L/K}$ such that $\alpha^{-1} \in P_\infty$ or $\beta^{-1} \in P_\infty$. Furthermore, $P_\infty \in \mathbb{P}^{(1)}_{L/K}$, $\nu_{P_\infty}(\alpha) = -2$ and $\nu_{P_\infty}(\beta) = -3$.

T&N. The uniquely determined place from 11.7 is denoted by P_∞.

Proposition 11.8. If w is a smooth WEP at $V_w(K)$, then

$$\mathbb{P}^{(1)}_{L/K} = \{P_\infty\} \cup \{P_\gamma \mid \gamma \in V_w(K)\}.$$

Example 11.9. Let $f = y^2 + y - (x^3 + 1) = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ and $\alpha := x + (f)$, $\beta := y + (f) \in \mathbb{F}_2[x, y]/(f)$. Then f is a Weierstrass equation polynomial and $L = \mathbb{F}_2(\alpha, \beta)$ is an AFF over $\mathbb{F}_2$ given by $f(\alpha, \beta) = 0$.

Let $P \in \mathbb{P}_{L/K}$ of degree 1. Then $\mathbb{P}^{(1)}_{L/K} = \{P_{(1,0)}, P_{(1,1)}, P_\infty\}$ by 11.8, since $V_f(\mathbb{F}_2) = \{(1, 0), (1, 1)\}$.

By 11.3 $\mathbb{P}_{L/K}$ is infinite, hence other places are of degree greater than 1, for example for each irreducible $m \in \mathbb{F}_2[x]$ of degree greater than 1, there exists $P_m \in \mathbb{P}_{L/K}$ such that $m(\alpha) \in P_m$, thus $\deg P_m \geq \deg(m) > 1$.

12. Divisors

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

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 *divisor* (of the AFF L over K). *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 12.1. $\sum_{P \in \mathbb{P}_{L/K}} \nu_p(r) P$ is a divisor by 11.6 for each $r \in L^*$ and note that $\sum_{P \in \mathbb{P}_{L/K}} \nu_P(a) P = \underline{0} \Leftrightarrow \nu_P(a) = 0\ \forall P \in \mathbb{P}_{L/K} \Leftrightarrow a \in \tilde{K}$.

T&N. A divisor $\sum_{P \in \mathbb{P}_{L/K}} \nu_p(r) P$ for $r \in L^*$ is called *principal* divisor and it is denoted by (r) and let Princ(L/K) $:= \{(r) \mid r \in L^*\}$ be the set of all principal divisors of L over K.

Observation. Put $k = [\tilde{K} : K] < \infty$, $P \in \mathbb{P}_{L/K}$, $A \in$ Div(L/K).

(A1) $\mathbb{P}_{L/\tilde{K}} = \mathbb{P}_{L/K}$ and Div(L/$\tilde{\text{K}}$) = Div(L/K),

(A2) $\deg_K P = \dim_K \mathcal{O}_P/P = k \cdot \deg_{\tilde{K}} P$ and $\deg_K(A) = k \cdot \deg_{\tilde{K}}(A)$, (A3) $\deg_K : \mathrm{Div(L/K)} \to \mathbb{Z}$ is a group homomorphism,

(A4) the map $r \to (r)$ forms a homomorphism of $(L^*, \cdot, ^{-1}, 1)$ and $(\mathrm{Div(L/K)}, +, -, \underline{0})$ since $(rs) = \sum_{P\in\mathbb{P}_{L/K}} \nu_p(rs)P = \sum_{P\in\mathbb{P}_{L/K}} (\nu_p(r) + \nu_p(s))P = (r) + (s)$,

(A5) $\mathrm{Princ(L/K)}$ is a subgroup of $\mathrm{Div(L/K)}$ where $-(r) = (r^{-1})$ and $\underline{0} = (1)$, furthermore, $(r) = (s) \Leftrightarrow \exists\, \lambda \in \tilde{K}^*$ satisfying $r = \lambda s$.

T&N. Let $A = \sum_{P\in\mathbb{P}_{L/K}} a_pP$, $B = \sum_{P\in\mathbb{P}_{L/K}} b_pP \in \mathrm{Div(L/K)}$. 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 called *positive* if $A = A_+$.

Define relations $\le$ and $\sim$ on $\mathrm{Div(L/K)}$: $A \le B$ if $a_p \le b_p$ $\forall$ $P \in \mathbb{P}_{L/K}$, $A \sim B$ if $A - B \in \mathrm{Princ(L/K)}$. $\ge$ denotes the opposite relation.

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

Observation. Let $r \in L^*$ and $A \in \mathrm{Div(L/K)}$.

(B1) $\sim$ is a congruence on $\mathrm{Div(L/K)}$ and $\le$ is an ordering on $\mathrm{Div(L/K)}$ compatible with the operation $+$ (i.e. $A \le B$, $C \le D \Rightarrow A + C \le B + D$ for $A, B, C, D \in \mathbb{P}_{L/K}$),

(B2) if $r \in L \setminus \tilde{K}$, then $(r) \not\ge \underline{0}$ by Lemma 4.9(1),

(B3) $\mathcal{L}(A)$ is a $\tilde{K}$-space and so K-space and

$$\mathcal{L}(\underline{0}) := \{r \in L^* \mid (r) + (1) \ge \underline{0}\} \cup \{0\} = \tilde{K}.$$

T&N. $\mathrm{Cl(L/K)} := \mathrm{Div(L/K)}/\mathrm{Princ(L/K)}$ is called the *class group* of the AFF L over K.

If $A \in \mathrm{Div(L/K)}$, then $\mathcal{L}(A)$ is said to be *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.

Observation. Let $i \le j \in \mathbb{Z}$, $(p) = P \in \mathbb{P}_{L/K}$ and denote $P^i = p^i\mathcal{O}_P$.

(C1) The map $\psi_j : \mathcal{O}_P/P \to P^{j-1}/P^j$ determined by the rule $\psi_j(a + P) = ap^{j-1} + P^j$ is an isomorphism of K-spaces,

(C2) $\deg P = \dim_K \mathcal{O}_P/P = \dim_K P^{j-1}/P^j$,

(C3) $\dim_K(P^i/P^j) = \sum_{k=i+1}^{j} \dim(P^{k-1}/P^k) = (j - i)\deg P$.

Lemma 12.2. If $A, B \in \mathrm{Div(L/K)}$ such that $A \le B$, then $\mathcal{L}(A)$ is a subspace of $\mathcal{L}(B)$ and $\dim_K(\mathcal{L}(B)/\mathcal{L}(A)) \le \deg_K(B - A)$.

Lemma 12.3. If $\mathbb{P}^{(1)}_{L/K} \ne \emptyset$, then $K = \tilde{K}$

We will suppose in the rest of the lecture that $K = \tilde{K}$, i.e. L is a full constant AFF.

Proposition 12.4. If $A, B \in \mathrm{Div(L/K)}$, then

(D1) $1 \le l(A) \le \deg A + 1$ if $A \ge \underline{0}$,

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

(D3) $l(A) \le l(A_+) < \infty$,

(D4) $\deg A - l(A) \le \deg B - l(B)$, if $A \le B$.

Lemma 12.5. If $s \in L \setminus K$, then $\exists B \in \mathrm{Div(L/K)}$ such that $B \ge \underline{0}$ and for each $k \ge 0$:

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

Theorem 12.6. If $s \in L \setminus K$ then $\deg((s)_-) = \deg((s)_+) = [L:K(s)]$ and $\deg((s)) = 0$.

Corollary 12.7. If $A \sim B$, then $\deg A = \deg B$ and $\dim_{L/K} A = \dim_{L/K} B$.

Example 12.8. Let L be an AFF over $\mathbb{F}_2$ given by $w(\alpha, \beta) = 0$ for $w = y^2 + y - (x^3+1) \in \mathbb{F}_2[x,y]$ as in 11.9. We will compute principal divisors $(\alpha+1)$ and (α).

(a) By 12.6

$$\deg((\alpha+1)_+) = \sum_{P:\ \alpha+1 \in P} \nu_P(\alpha+1) \deg P = [L:\mathbb{F}_2(\alpha+1)] = [L:\mathbb{F}_2(\alpha)] = 2.$$

Since $\alpha+1 \in P_{(1,0)} \cap P_{(1,1)}$ and $\nu_{P_\infty}(\alpha+1) = \nu_{P_\infty}(\alpha) = -2$ by 11.7, we get

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

(b) Again by 12.6 is $\deg((\alpha)_+) = \sum_{P:\ \alpha \in P} \nu_P(\alpha) \deg P = [L:\mathbb{F}_2(\alpha)] = 2$ and $\alpha \notin P$ for all $P \in {\mathbb{P}_{L/K}}^{(1)}$, hence there exists a unique P such that $\alpha \in P$ and $\deg P = 2$, which means that

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

Observation. For $A, B \in \mathrm{Div(L/K)}$ it holds:

(D5) $l(A) \geq 1 \Leftrightarrow \exists s \in L^*$ such that $s \in \mathcal{L}(A) \Leftrightarrow \exists s \in L^*$ such that $A + (s) \geq \underline{0}$,
(D6) $l(B-A) \geq 1 \Leftrightarrow \exists s \in L^*$ such that $A - (s) \leq B \Leftrightarrow \exists A' \in \mathrm{Div(L/K)}$ such that $A \sim A' \leq B$,
(D7) if $l(B-A) \geq 1$, then $\deg A - l(A) \leq \deg A' - l(A') \leq \deg B - l(B)$ for A' from (D6) by (D4),
(D8) if $\deg A < 0$, then $\deg(A + (s)) = \deg A < 0\ \forall s \in L^*$, hence $l(A) = 0$,
(D9) $\mathcal{L}((s)) = \{r \in L^* \mid (rs) \geq \underline{0}\} \cup \{0\} = Ks^{-1} (= \{ks^{-1} \mid k \in K\})\ \forall s \in L^*$.

Lemma 12.9. If $A \in \mathrm{Div(L/K)}$ such that $\deg A = 0$, then

(1) $l(A) \in \{0, 1\}$,
(2) $l(A) = 1 \Leftrightarrow A \in \mathrm{Princ(L/K)}$.

Theorem 12.10 (Riemann)**.** There exists an integer γ such that for each $A \in \mathrm{Div(L/K)}$

$$\deg(A) - l(A) < \gamma.$$

Definition. The minimal possible γ such that $\deg(A) - l(A) < \gamma$ for each $A \in \mathrm{Div(L/K)}$, which exists by Theorem 12.10, is called the *genus* of the AFF L over $\tilde{K}$. Furthermore, $i(A) := g - 1 - \deg(A) + l(A) \geq 0$ is said to be the *index of specialty* of A (A is called *special* if $i(A) > 0$ and A is called *nonspecial* if $i(A) = 0$).

Corollary 12.11. Let $A, D \in \mathrm{Div(L/K)})$ and suppose $\deg(D) - l(D) = g - 1$ for the genus g.

(E1) $g > \deg(\underline{0}) - l(\underline{0}) = -1$, hence $g \geq 0$,
(E2) $\deg(A - D) - l(A - D) \leq g - 1$, hence $l(A - D) \geq \deg(A) - \deg(D) - g + 1$,
(E3) if $\deg(A) \geq \deg(D) + g$, then $l(A - D) \geq 1$ by (E2),

(E4) if either $l(A-D) \geq 1$ or $D \leq A$ then by (D4) and (D6) $g-1 = \deg(D) - l(D) \leq \deg(A) - l(A) \leq g-1$, hence $\deg(A) - l(A) = g-1$ and $i(A) = 0$,
(E5) if $\deg(D) + g \leq \deg(A)$, then $l(A-D) \geq 1$ by (E3), thus $l(A) = \deg(A) - g + 1$ and $i(A) = 0$ by (E4).

13. Adèles and Weil differentials

We suppose that L is a full constant AFF over $K = \tilde{K}$ of genus g.

T&N. Let $\mathbb{P} := \mathbb{P}_{L/K}$ and consider the Cartesian power $L^{\mathbb{P}}$ as an L-algebra with component-wise defined operations where $l \to l \cdot 1 \in L^{\mathbb{P}}$ identifies elements of L with constants of $L^{\mathbb{P}}$. Let $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P \in \mathrm{Div(L/K)}$. Then

$$\mathcal{A}_{L/K}(A) := \{f \in L^{\mathbb{P}} \mid \nu_P(f(P)) + a_P \geq 0 \ \forall P \in \mathbb{P}\}.$$

An element of $\mathcal{A}_{L/K} = \bigcup_{B \in \mathrm{Div(L/K)}} \mathcal{A}_{L/K}(B)$ is called *adèle.*

If $P = (p) \in \mathbb{P}_{L/K}$, then $P^k = p^k \mathcal{O}_P = \{r \in L \mid \nu_P(r) \geq k\}$ for each $k \in \mathbb{Z}$.

Observation. Let $r \in L$, $f \in L^{\mathbb{P}_{L/K}}$, $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P \in \mathrm{Div(L/K)}$ and $s \in L^*$.

(1) $f \in \mathcal{A}_{L/K} \Leftrightarrow \{P \in \mathbb{P} \mid \nu_P(f(P)) < 0\}$ is finite, hence $r \in \mathcal{A}_{L/K}$ by 11.6,
(2) $\mathcal{A}_{L/K}$ is a subalgebra of the L-algebra $L^{\mathbb{P}_{L/K}}$,
(3) $\mathcal{A}_{L/K}(A) = \prod_{P \in \mathbb{P}_{L/K}} P^{-a_P}$ is a subspace of the K-space $\mathcal{A}_{L/K}$ and $\mathcal{A}_{L/K}(A) \cap L = \mathcal{L}(A)$.

Lemma 13.1. Let $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P$, $B = \sum_{P \in \mathbb{P}_{L/K}} b_p P \in \mathrm{Div(L/K)}$ and $s \in L^*$.

(1) $A \leq B \Rightarrow \mathcal{A}_{L/K}(A) \subseteq \mathcal{A}_{L/K}(B)$ and $\dim_K(\mathcal{A}_{L/K}(B)/\mathcal{A}_{L/K}(A)) = \deg(B-A)$,
(2) $A \leq B \Rightarrow \dim_K((\mathcal{A}_{L/K}(B) + L)/(\mathcal{A}_{L/K}(A) + L)) = i(A) - i(B)$,
(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) $\dim_K(\mathcal{A}_{L/K}/(\mathcal{A}_{L/K}(A) + L)) = i(A)$,
(5) $\mathcal{A}_{L/K} = \mathcal{A}_{L/K}(A) + L \Leftrightarrow i(A) = 0$,
(6) $s\mathcal{A}_{L/K}(A) = \mathcal{A}_{L/K}(A - (s))$.

T&N. Let $A \in \mathrm{Div(L/K)}$. Then
$\Omega_{L/K}(A) := (\mathcal{A}_{L/K}(A) + L)^o_K = \{\omega \in \mathcal{A}_{L/K}{}^* \mid \omega(\mathcal{A}_{L/K}(A) + L) = 0, \}$

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

We define $\forall \omega \in \Omega_{L/K}$ and $\forall s \in L^*$ multiplication on $\Omega_{L/K}$ by the rules $(s \cdot \omega)(t) = \omega(st)$ $\forall s \in L^*$ and $0 \cdot \omega = 0$. Elements of $\Omega_{L/K}$ are called *Weil differentials* (of the AFF).

Corollary 13.2. Let $A, B \in \mathrm{Div(L/K)}$ a $s \in L^*$.

(1) $\dim_K(\Omega(A)) = \dim(\mathcal{A}_{L/K}/(\mathcal{A}_{L/K}(A) + L) = i(A)$ by 1.4(2), 13.1(4),
(2) $A \leq B \Rightarrow \Omega_{L/K}(B) \subseteq \Omega_{L/K}(A)$ by 1.4(3, 13.1(1)),
(3) $\Omega_{L/K}(A) \cap \Omega_{L/K}(B) = (\mathcal{A}_{L/K}(A) + \mathcal{A}_{L/K}(B) + L)^o = \Omega_{L/K}(\max(A,B))$,
$\Omega_{L/K}(A) + \Omega_{L/K}(B) = ((\mathcal{A}_{L/K}(A) + L) \cap (\mathcal{A}_{L/K}(B) + L))^o \subseteq \Omega_{L/K}(\min(A,B))$ by 1.4(1),(4), 13.1(3),
(4) $s\Omega_{L/K}(A) = (s^{-1}(\mathcal{A}_{L/K}(A))^o = \Omega_{L/K}(A + (s)$ by 1.5(3), 13.1(6),

(5) $\Omega_{L/K}$ forms an L-space by 1.5, (3) a (4).

Lemma 13.3. If $\omega \in \Omega_{L/K} \setminus \{0\}$, then there exists a unique $W \in \mathrm{Div(L/K)}$ such that $\omega(\mathcal{A}_{L/K}(W)) = 0$ and each $A \in \mathrm{Div(L/K)}$ satisfies $A \leq W$ whenever $\omega(\mathcal{A}_{L/K}(A)) = 0$.

T&N. Let $\omega \in \Omega_{L/K} \setminus \{0\}$. The divisor W from 13.3 uniquely determined by ω is called the *canonical divisor* of ω and it is denoted by (ω).

Let us define a map $\Psi_\omega : L \to \Omega_{L/K}$ by $\Psi_\omega(s) = s \cdot \omega \ \forall s \in L$.

Lemma 13.4. Let $\omega, \tilde{\omega} \in \Omega_{L/K} \setminus \{0\}$ and $A \in \mathrm{Div(L/K)}$. Then

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

Theorem 13.5. Let $\omega \in \Omega_{L/K} \setminus \{0\}$ and $A \in \mathrm{Div(L/K)}$, then

(1) $\dim_L(\Omega_{L/K}) = 1$,
(2) Ψ_ω induces a K-isomorphism $\mathcal{L}((\omega) - A) \to \Omega_{L/K}(A)$.

As a consequence we can easily see that all the canonical divisors form exactly one coset modulo Princ(L/K).

The following two results will be skipped this year.

Lemma 13.6. Let $\mathcal{S} \subsetneq \mathbb{P}_{L/K}$, , $P_1, \dots, P_n \in \mathcal{S}$ be pairwise distinct places, $a_1, \dots a_n \in L$ and $z \in \mathbb{Z}$. Then there exists $t \in L$ such that $\nu_{P_i}(t - a_i) > z \ \forall i = 1, \dots, n$ and $\nu_P(t) \geq 0$ $\forall P \in \mathcal{S} \setminus \{P_1 \dots, P_n\}$.

Theorem 13.7 (Strong Approximation Theorem)**.** Let $\mathcal{S} \subsetneq \mathbb{P}_{L/K}$, , $P_1, \dots, P_n \in \mathcal{S}$ be pairwise distinct places. If $a_1, \dots a_n \in L$ and $z_1, \dots, z_n \in \mathbb{Z}$, then $\exists s \in L$ such that $\nu_{P_i}(s - a_i) = z_i$ for each $i = 1, \dots, n$ and $\nu_P(s) \geq 0$ for each $P \in \mathcal{S} \setminus \{P_1 \dots, P_n\}$.

14. Riemann-Roch Theorem

L is a full constant AFF over $K = \tilde{K}$ of genus g.

Theorem 14.1 (Riemann-Roch)**.** If W is a canonical divisor and $A \in \mathrm{Div(L/K)}$, then

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

If we put $W = \underline{0}$ and $W = A$, then we get the following consequence:

Corollary 14.2.] If $W \in \mathrm{Div(L/K)}$ is canonical, then $l(W) = g$, $\deg W = 2g - 2$, $i(W) = g - 1 - \deg W + l(W) = 1$.

Corollary 14.3 (Main consequence of the Riemann-Roch Theorem)**.** If $\deg A \geq 2g - 1$ for $A \in \mathrm{Div(L/K)}$, then $l(A) = \deg A + 1 - g$.

Lemma 14.4. Let $P \in \mathbb{P}^{(1)}_{L/K}$, $h \in \mathbb{Z}$, $h \geq 0$, $s \in L$. Then

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

Example 14.5. Recall that the field $K(x)$ is an AFF over K and by 4.7

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

where P_p is the maximal ideal of the localization with $\nu_{P_p} = \nu_p$ and P_∞ is given by the discrete valuation $\nu_\infty(\frac{a}{b}) = \deg(b) - \deg(a)$. Then $\nu_p(x^i) \geq 0$ for each $i \geq 0$ and p is irreducible monic. Furthermore $\nu_\infty(x^i) = -i$ for each $i \geq 0$, hence $(x^i)_- = iP_\infty$. Thus $K(x)$ is of genus 0 by 14.4(3).

For every $s \in K(x)^*$ there exist $k \in K^*$, irreducible, pairwisely non-associated polynomials $p_i \in K[x]$ and exponents $e_i \in \mathbb{Z}$, for which $s = k\prod_i p_i^{e_i}$. If we put $d = \sum_i e_i \deg p_i$, then $(s) = \sum_i e_i P_{p_i} - dP_\infty$ forms a principal divisor and it holds $e_i = \nu_{p_i}(s) = \nu_{P_{p_i}}(s)$. This presents a way of searching of an element of L determining a divisor of degree 0, which is in this case necessarily principal.

Proposition 14.6. Let $\mathbb{P}^{(1)}_{L/K} \neq \emptyset$. Then $g = 0 \Leftrightarrow$ there exists $s \in L$ such that $L = K(s)$.

15. Elliptic function fields

Let L be an AFF over K of genus g.

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

Observation. If L is an EFF over K and $P \in \mathbb{P}^{(1)}_{L/K}$, then is L full constant by 12.3, and $l(iP) = \deg(iP) = i$ for each $i \geq 1$ by 14.3, hence $K = \mathcal{L}(1P) \subsetneqq \mathcal{L}(2P) \subsetneqq \mathcal{L}(3P)$.

Proposition 15.1. If L is an EFF over K and $P \in \mathbb{P}^{(1)}_{L/K}$, then $\forall u \in \mathcal{L}(2P) \setminus \mathcal{L}(1P)$ and $v \in \forall \mathcal{L}(3P) \setminus \mathcal{L}(2P)$ there exists a WEP $w \in K[x, y]$ and $\lambda \in K^*$ such that L is given by $w(\lambda u, \lambda v) = 0$.

Corollary 15.2. Every EFF is given by a Weierstrass equation (i.e. there are a WEP w and elements α, β such that the EFF is given by $w(\lambda u, \lambda v) = 0$).

Recall that if w is smooth at $V_w(K)$, then $\mathbb{P}^{(1)}_{L/K} = \{P_\infty\} \cup \{P_\gamma \mid \gamma \in V_w(K)\}$ by 11.8.

Lemma 15.3. If $w \in K[x, y]$ is a WEP and L over K is given by $w(\alpha, \beta) = 0$ and it is not an EFF, then $g = 0$, and $\exists s \in L$ and $\exists a, b \in K[x]$, for which $L = K(s)$, $\alpha = a(s)$, $\beta = b(s)$ and $\deg a = 2$, $\deg b = 3$.

Theorem 15.4. Let L be given by $w(\alpha, \beta) = 0$ for a WEP $w \in K[x, y]$. Then L is an EFF $\Leftrightarrow$ w is smooth at $V_w(K)$.

Example 15.5. (1) Let $w = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ is a WEP from 11.9. Since it is smooth at rational points $V_w(\mathbb{F}_2) = \{(1, 0), (1, 1))\}$, then by 15.4 the genus of $\mathbb{F}_2(V_w)$ is 1, hence it is an EFF and $\mathbb{F}_2(s) \subsetneqq \mathbb{F}_2(V_w)$ for each $s \in \mathbb{F}_2(V_w)$.

(2) Let $w = y^2 + x^3 + x + 1 \in \mathbb{F}_2[x, y]$ be a WEP. Since it is singular at $(1, 1) \in V_w(\mathbb{F}_2)$. Hence by 15.4 it is of genus 0 and there exists $s \in \mathbb{F}_2(V_w)$ such that $\mathbb{F}_2(s) = \mathbb{F}_2(V_w)$. It is easy to compute that e.g. $s = \frac{\beta+1}{\alpha+1}$ for $\alpha = x + (w)$, $\beta = y + (w)$, hence $\mathbb{F}_2(V_w) = \mathbb{F}_2(\alpha, \beta)$ is given by $w(\alpha, \beta) = 0$.

In the rest of the section L is an EFF over K.

T&N. The factor group $\mathrm{Pic}^0(L/K) := \mathrm{Ker(deg)/Princ(L/K)}$ is called the *Picard group* and $[A] := A + \mathrm{Princ(L/K)}$ denotes the cosets of $\mathrm{Pic}^0(L/K)$ and a mapping $\Psi_Q : \mathbb{P}^{(1)}_{L/K} \to \mathrm{Pic}^0(L/K)$ is given by the rule

$$\Psi_Q(P) := [P - Q] \text{ for } Q \in \mathbb{P}^{(1)}_{L/K}.$$

Lemma 15.6. Let $P, Q \in \mathbb{P}^{(1)}_{L/K}$, and $A \in \mathrm{Div(L/K)}$.

(1) if $P - Q \in \mathrm{Princ(L/K)}$, then $P = Q$,
(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 $\Psi_Q : \mathbb{P}^{(1)}_{L/K} \to \mathrm{Pic}^0(L/K)$ is a bijection.

T&N. We define for a fixed $Q \in \mathbb{P}^{(1)}_{L/K}$ operations by the rule $P_1 \oplus P_2 = \Psi_Q^{-1}(\Psi_Q(P_1) + \Psi_Q(P_2))$ and $\ominus P = \Psi_Q^{-1}(-\Psi_Q(P))$.

Corollary 15.7. If $Q, P_0, P_1, \dots, P_n \in \mathbb{P}^{(1)}_{L/K}$, then

(1) $(\mathbb{P}^{(1)}_{L/K}, \oplus, \ominus, Q)$ forms an abelian group and Ψ_Q is a group isomorphism,
(2) $P_1 \oplus P_2 = P_0 \Leftrightarrow [P_1 + P_2] = [P_0 + Q]$,
(3) $P_1 \oplus \cdots \oplus P_n = P_0 \Leftrightarrow -P_0 + (1-n)Q + \sum_{i=1}^n P_i \in \mathrm{Princ(L/K)}$.

In the rest, L denotes an EFF over K given by $w(\alpha, \beta) = 0$ for a WEP w.

Definition. Let us consider on $\mathbb{P}^{(1)}_{L/K} = \{P_\infty\} \cup \{P_\gamma \mid \gamma \in V_w(K)\}$ (from 11.8) a group structure determined by Ψ_{P_∞}, put $E(K) = V_w(K) \cup \{\infty\}$ and define operations $\oplus$, $\ominus$ on $E(K)$:

$$\gamma \oplus \delta = \eta \Leftrightarrow P_\gamma \oplus P_\delta = P_\eta \Leftrightarrow [P_\gamma + P_\delta] = [P_\eta + P_\infty],$$
$$\ominus\gamma = \delta \Leftrightarrow \ominus P_\gamma = P_\delta \Leftrightarrow [P_\gamma + P_\delta] = [2P_\infty].$$

Now we formulate a consequence of main results of the course, including 9.7, 11.8 and 12.5:

Proposition 15.8. Let $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$, $l_0 + l_1 x + l_2 y \in K[x, y]$ such that $l_0, l_1, l_2 \in K$ and $(l_1, l_2) \neq (0, 0)$, and put $V = V_w(K) \cap V_l(K)$.

(1) $(E(K), \oplus, \ominus, \infty)$ is an abelian group isomorphic to $\mathrm{Ker(deg)/Princ(L/K)}$,
(2) $\gamma \in V_l(K) \Leftrightarrow \nu_{P_\gamma}(l(\alpha, \beta)) \geq 1 \Leftrightarrow 1P_\gamma \leq (l(\alpha, \beta))_+$,
(3) $\gamma \in V_l(K)$ and $l \in (t_\gamma(w)) \Leftrightarrow \nu_{P_\gamma}(l(\alpha, \beta)) \geq 2 \Leftrightarrow 2P_\gamma \leq (l(\alpha, \beta))_+$,
(4) $(l(\alpha, \beta))_- = 2P_\infty$ whenever $l_2 = 0$, and $(l(\alpha, \beta))_- = 3P_\infty$ otherwise,
(5) if $l_2 = 0$, then $l \in (x - \gamma_1)$ and $\exists! \delta \in V$ such that $(l(\alpha, \beta)) = P_\gamma + P_\delta - 2P_\infty$, i.e. $\ominus\gamma = \delta$ for $V = \{\gamma, \delta\}$,
(6) if $l_2 \neq 0$ and $\delta \in V$ such that $P_\gamma + P_\delta \leq (l(\alpha, \beta))_+$ then $\exists! \eta \in V$ such that $(l(\alpha, \beta)) = P_\gamma + P_\delta + P_\eta - 3P_\infty$, i.e. $\gamma \oplus \delta \oplus \eta = \infty$ for $V = \{\gamma, \delta, \eta\}$.

The rest was not presented at the lecture this year.

Corollary 15.9. If $K \subseteq F \subseteq \overline{K}$ is a field extension, then $E(K)$ is a subgroup of $E(F)$.

Denote by $w = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) \in K[x, y]$ for a WEP smooth at $V_w(K)$.

Theorem 15.10. $(E(K), \oplus, \ominus, \infty)$ is a commutative group and for $\gamma = (\gamma_1, \gamma_2)$, $\delta = (\delta_1, \delta_2)$, $\eta = (\eta_1, \eta_2) \in V_w(K)$ it holds:

(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
$\eta = (-\gamma_1 - \delta_1 + \lambda^2 + a_1\lambda - a_2, \lambda(\gamma_1 - \eta_1) - \gamma_2 - a_1\eta_1 - a_3)$, where
(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 $\gamma_1 = \delta_1$.

Example 15.11. Let $w = y^2 - x^3 - 1 \in \mathbb{F}_5[x]$ be a WEP. Since $(x^3 + 1)' = 3x^2$ and 0 is not a root of $x^3 + 1$, w is smooth.

Since $E(\mathbb{F}_5) = \{(0, 1), (0, 4), (4, 0), (2, 2), (2, 3), \infty\}$ is a commutative group of the order 6, we know that $E(\mathbb{F}_5) \cong \mathbb{Z}_6$. By applying 15.7 we compute:
$(0, 1) = \ominus(0, 4)$ $(4, 0) \oplus (4, 0) = (2, 2) \oplus (2, 3) = \infty$ and $(0, 4) \oplus (4, 0) = (2, 3)$.

Contents