

1 Basic notions

1.1. Describe sets V_f and $V_f(\mathbb{R})$ if

- (a) $f = x^2 - y^2 \in \mathbb{R}[x, y]$,
- (b) $f = (x^2 - y^2)(x + y) \in \mathbb{R}[x, y]$,
- (c) $f = x^3 - y^3 \in \mathbb{R}[x, y]$

(a) Since linear polynomials $x + y$ and $x - y$ are irreducible and $x^2 - y^2 = (x + y)(x - y)$, we have irreducible decomposition of the curve:

$$V_{x^2-y^2} = V_{x+y} \cup V_{x-y}, \quad V_{x^2-y^2}(\mathbb{R}) = V_{x+y}(\mathbb{R}) \cup V_{x-y}(\mathbb{R}),$$

where $V_{x+y} = \text{Span}_{\mathbb{C}}((1, -1))$ and $V_{x-y} = \text{Span}_{\mathbb{C}}((1, 1))$ are complex lines and $V_{x+y}(\mathbb{R}) = \text{Span}_{\mathbb{R}}((1, -1))$ and $V_{x-y}(\mathbb{R}) = \text{Span}_{\mathbb{R}}((1, 1))$ are real lines.

(b) Since

$$\sqrt{((x^2 - y^2)(x + y))} = \sqrt{((x - y)(x + y)^2)} = ((x - y)(x + y)) = (x^2 - y^2),$$

we have the same irreducible decomposition of V_f and $V_f(\mathbb{R})$ into two lines as in (a)

$$V_{(x^2-y^2)(x+y)} = V_{x+y} \cup V_{x-y}, \quad V_{(x^2-y^2)(x+y)}(\mathbb{R}) = V_{x+y}(\mathbb{R}) \cup V_{x-y}(\mathbb{R}),$$

(c) We can easily calculate the decomposition of $x^3 - y^3$ into linear factors in $\mathbb{C}[x, y]$:

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2) = (x - y)\left(x + \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)y\right)\left(x + \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)y\right),$$

hence $V_{x^3-y^3} = V_{x-y} \cup V_{x+(\frac{1}{2}+\frac{\sqrt{3}}{2}i)y} \cup V_{x+(\frac{1}{2}-\frac{\sqrt{3}}{2}i)y}$ is an irreducible decomposition into three complex lines.

Now, we consider the decomposition $V_{x^3-y^3}(\mathbb{R}) = V_{x-y}(\mathbb{R}) \cup V_{x^2+xy+y^2}(\mathbb{R})$. Revoking linear algebra we can show that the real quadratic form $g_2 = x^2 + xy + y^2$ is positively definite, since its matrix

$$\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \sim_s \begin{pmatrix} 1 & 0 \\ 0 & \frac{3}{4} \end{pmatrix}$$

is positively definite, hence $\{(x, y) \in \mathbb{R}^2 \mid g_2(x, y) = 0\} = \{(0, 0)\}$. It means that $V_{x^3-y^3}(\mathbb{R}) = V_{x-y}(\mathbb{R}) = \text{Span}_{\mathbb{R}}((1, 1))$ is a real line. \square

1.2. Describe the function field $K(V_f)$ for a general field K and

- (a) $f = x + y$,
- (b) $f = ax + by + c$ where $(a, b) \neq (0, 0)$.

First note that any non-constant linear polynomial is irreducible and that the function field $K(V_f)$ is a field of fractions of the coordinate ring $K[V_f]$. So it is enough to describe coordinate rings.

(a) To find the coordinate ring $K[V_{x+y}] \cong K[x, y]/(x + y)$, we intend to use the First Isomorphism Theorem. Consider evaluating homomorphism $\varphi : K[x, y] \rightarrow K[x]$ given by $\varphi(p) = p(x, -x)$, then, obviously $x + y \in \ker(\varphi)$, hence $(x + y) \subseteq \ker(\varphi)$. If $q(y) \in \ker(\varphi)$, where we consider q as a polynomial in variable y with coefficients in the domain $K[x]$, we can observe that $-x$ is a root of q , thus $(y + x) \mid q$ and so $q \in (x + y)$. Since $\varphi(p)$ is surjective and we have shown that $\ker(\varphi) = (x + y)$, then the First Isomorphism Theorem gives us

$$K[V_{x+y}] \cong K[x, y]/(x + y) = K[x, y]/\ker(\varphi) \cong K[x].$$

It means that the function field $K(V_{x+y})$ is isomorphic to the field of rational functions in one variable $K(x)$.

(b) W.l.o.g we may suppose that $b \neq 0$, otherwise we switch the variables x and y . We repeat the arguments of (a) for the evaluating homomorphism $\psi : K[x, y] \rightarrow K[x]$ given by the rule $\psi(p) = p(x, -\frac{a}{b}x - \frac{c}{b})$, which is onto $K[x]$. Then $\ker(\psi) = (ax + by + c)$ and by the First Isomorphism Theorem we get the isomorphism.

$$K[V_{ax+by+c}] \cong K[x, y]/(ax + by + c) = K[x, y]/\ker(\psi) \cong K[x].$$

Thus $K(V_{ax+by+c}) \cong K(x)$ again. □

1.3. Let p be a prime number, $q = p^n$ for $n \in \mathbb{N}$ and $f \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$.

- (a) If f is irreducible, describe a rupture field of f .
- (b) If f is irreducible, describe a splitting field of f .
- (c) For which k does the field \mathbb{F}_{q^k} contain a root of f ?
- (d) Construct an algebraic closure of the field \mathbb{F}_p .

(a), (b) We know that the factor ring $\mathbb{F}_q[x]/(f)$ is a field containing a root of f , i.e. a rupture field of f . Note that $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^{\deg f}}$ is even a splitting field of polynomials f and $x^{q^{\deg f}} - x$ and that $f \mid x^{q^{\deg f}} - x$ in $\mathbb{F}_q[x]$.

(c) Since \mathbb{F}_{q^k} is a splitting field of a polynomial $x^{q^k} - x = \prod_{a \in \mathbb{F}_{q^k}} x - a$ and it contains all roots of irreducible polynomials of degree dividing k , \mathbb{F}_{q^k} contain a root of f if and only if $\deg \gcd(f, x^{q^k} - x) > 0$, which is true if and only if there exists an irreducible factor of f of degree dividing k .

(d) Recall that $\mathbb{F}_{p^{k!}}$ is a subfield of $\mathbb{F}_{p^{(k+1)!}}$ since $\mathbb{F}_{p^a} \leq \mathbb{F}_{p^b}$ iff $a \mid b$. Put $K = \bigcup_{k \in \mathbb{N}} \mathbb{F}_{p^{k!}}$.

Observer that for each $\alpha \in K$ there exists m for which α is a root of the polynomial $x^{p^m} - x$, hence $K \subseteq \overline{\mathbb{F}_p}$. On the other hand let $f \in K[x]$. Then there exist k such that $f \in \mathbb{F}_{p^{k!}}[x]$ and by (c) there is $l \leq \deg f$ such that $\mathbb{F}_{p^{k!l}} \leq \mathbb{F}_{p^{(k!l)!}} \leq K$ contains a root of f . This proves that K is an algebraic closure of the field \mathbb{F}_p . □

1.4. Let K be a field and $F \in K[X, Y, Z]$ be irreducible of positive degree. Prove that

$$K(V_F) = \left\{ \frac{A + (F)}{B + (F)} \mid A, B \in K[X, Y, Z], B \notin (F), \deg A = \deg B \right\}$$

be a subfield of a field of fractions of the domain $\in K[X, Y, Z]/(F)$.

Clearly, $1 = \frac{1+(F)}{1+(F)} \in K(V_F)$. Since there exists a homogeneous polynomial $G \notin (F)$ of degree $d = \deg F$ (e.g. $G = X^d$ if $d > 1$ and $G = X$ or $G = Y$ if $d = 1$), we have $0 = \frac{F+(F)}{G+(F)} \in K(V_F)$. Let $\deg A = \deg B$ and $\deg C = \deg D$. Then it is easy to see that

$$\deg(AC) = \deg A + \deg C = \deg B + \deg D = \deg(BD),$$

hence $\frac{A+(F)}{B+(F)} \cdot \frac{C+(F)}{D+(F)} = \frac{AC+(F)}{BD+(F)} \in K(V_F)$. Similarly

$$\deg(AD) = \deg(BD) = \deg(BC),$$

which implies that $AD + BC = 0$ or $\deg(AD + BC) = \deg(BD)$, in both cases it means that

$$\frac{A+(F)}{B+(F)} + \frac{C+(F)}{D+(F)} = \frac{AD+BC+(F)}{BD+(F)} \in K(V_F).$$

□

1.5. Let $f \in \mathbb{R}[x, y]$ and $F \in \mathbb{R}[X, Y, Z]$ be its homogenization. Describe sets V_Z , $V_f(\mathbb{R})$, points in infinity of V_F and $V_F(\mathbb{R})$, and decide whether f and F are smooth if

(a) $f = x^2 + y^2 - 1$,

(b) $f = x^2 + y$.

Observe that $V_Z = \{(a : b : c) \in \mathbb{P}^2 \mid c = 0\} =$

$$= \{(a : b : 0) \in \mathbb{P}^2 \mid (a, b) \in \mathbb{C}^2 \setminus (0, 0)\} = \{(1 : 0 : 0)\} \cup \{(a : 1 : 0) \mid a \in \mathbb{C}\} = \mathbb{P}^2 \setminus \mathbb{A}^2.$$

05.03.

(a) Clearly, $V_f(\mathbb{R})$ is a unit circle. Now, we can easily determine the homogenization $F = X^2 + Y^2 - Z^2$ of f . The points in infinity $V_F \cap V_Z$ of V_F are those satisfying $X^2 + Y^2 = Z^2 = 0$. Since $X^2 + Y^2 = (X + iY)(X - iY)$, we get that $V_F \cap V_Z = \{(1 : \pm i : 0)\}$ and $V_F(\mathbb{R}) \cap V_Z = \emptyset$.

Now, let us compute partial derivatives

$$\frac{\partial f}{\partial x} = \frac{\partial x^2 + y^2 - 1}{\partial x} = 2x, \quad \frac{\partial f}{\partial y} = \frac{\partial x^2 + y^2 - 1}{\partial y} = 2y.$$

Observe that the condition $2x = 2y = 0$ implies that $f(x, y) = 1 \neq 0$, hence V_f has no singular points. It remains to check points $V_F \cap V_Z$, for which we can easily see that $\frac{\partial F}{\partial X}(1, \pm i, 0) = 2 \neq 0$, hence both F and f are smooth.

(b) This time $V_f(\mathbb{R})$ forms a parabola satisfying the equation $y = -x^2$. Since the homogenization of f is the polynomial $F = X^2 + YZ$ and the points in infinity $V_F \cap V_Z$ of V_F satisfy the equality $X^2 + YZ = X^2 = 0$, we can easily compute that $V_F \cap V_Z = V_F(\mathbb{R}) \cap V_Z = \{(0 : 1 : 0)\}$.

This time $\frac{\partial f}{\partial y} = \frac{\partial x^2 + y}{\partial y} = 1$, which shows that f is smooth. Finally, $\frac{\partial F}{\partial Z}(0, 1, 0) = 1 \neq 0$, hence F is smooth as well. □

1.6. Let $\beta = \frac{x^3+1}{(x^2-1)^2} \in \mathbb{R}(x)$. Calculate in the function field $\mathbb{R}(x)$ over \mathbb{R} the values of valuations:

(a) $v_{x+1}(\beta)$,

(b) $v_{x-1}(\beta)$,

(c) $v_x(\beta)$,

(d) $v_{x^2-x+1}(\beta)$.

Recall that $v_p(a) = \max(k \mid p^k \mid a)$ and $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$ for $a, b \in \mathbb{R}[x] \setminus \{(0)\}$.

(a) $v_{x+1}(\beta) = v_{x+1}(x^3+1) - v_{x+1}(x^2-1)^2 = 1 - 2 = -1$.

(b) $v_{x-1}(\beta) = v_{x-1}(x^3+1) - v_{x-1}(x^2-1)^2 = 0 - 2 = -2$.

(c) $v_x(\beta) = v_x(x^3+1) - v_x(x^2-1)^2 = 0 - 0 = 0$.

(d) $v_{x^2-x+1}(\beta) = v_{x^2-x+1}(x^3+1) - v_{x^2-x+1}(x^2-1)^2 = 1 - 0 = 1$. □

1.7. Let $v_\infty : K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ be defined by the rules

$$v_\infty(0) = \infty, \quad v_\infty\left(\frac{a}{b}\right) = \deg(b) - \deg(a)$$

for all $a, b \in K[x] \setminus \{(0)\}$. Prove that v_∞ is a normalized discrete valuation on the function field $K(x)$ over a field K .

First observe that the definition of v_∞ is correct. If $a, b, c, d \in K[x] \setminus \{(0)\}$ satisfies $\frac{a}{b} = \frac{c}{d}$ then

$$v_\infty\left(\frac{a}{b}\right) = \deg(b) - \deg(a) = \deg(d) - \deg(c) = v_\infty\left(\frac{c}{d}\right).$$

since $ad = bc$ and so $\deg(a) + \deg(d) = \deg(b) + \deg(c)$.

Let $a, b, c, d \in K[x] \setminus \{(0)\}$. Then $v_\infty\left(\frac{a}{b} \frac{c}{d}\right) = v_\infty\left(\frac{ac}{bd}\right) =$

$$= \deg(bd) - \deg(ac) = \deg(b) + \deg(d) - \deg(a) - \deg(c) = v_\infty\left(\frac{a}{b}\right) + v_\infty\left(\frac{c}{d}\right)$$

and

$$v_\infty\left(\frac{a}{b} + \frac{c}{d}\right) = v_\infty\left(\frac{ad + bc}{bd}\right) = \deg(bd) - \deg(ad + bc).$$

As $\deg(ad + bc) \leq \max(\deg(ad), \deg(bc)) = \max(\deg(a) + \deg(d), \deg(b) + \deg(c))$ we get that

$$\begin{aligned} v_\infty\left(\frac{a}{b} + \frac{c}{d}\right) &= \deg(bd) - \deg(ad + bc) \geq \\ &= \deg(bd) - \max(\deg(a) + \deg(d), \deg(b) + \deg(c)) = \\ &= \min(\deg(b) - \deg(a), \deg(d) - \deg(c)) = \min\left(v_\infty\left(\frac{a}{b}\right), v_\infty\left(\frac{c}{d}\right)\right). \end{aligned}$$

Finally note that $v_\infty\left(\frac{1}{x}\right) = 1$ and that $v_\infty(a) = \infty$ if and only if $a = 0$, which finishes the proof that all axioms (DV1)–(DV4) are satisfied. □

2 Weierstrass equations

2.1. Find a short WEP which is \mathbb{R} -equivalent to the WEP

$$w = y^2 + y(2x + 2) - (x^3 - 4x^2 + 1) \in \mathbb{R}[x, y].$$

We apply standard linear algebra machinery of Lemma 2.1. First, we remove the term $2xy$. Let $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in U_2(\mathbb{R})$, which represents replacement of y by $y - x$ and compute

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

Now we apply τ_b^* for $b = (1, -1)$ to exclude monomials y and x^2 :

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

□

2.2. Show that the real polynomial $\tilde{w} = y^2 - (x^3 - x + 2)$ is

(a) \mathbb{R} -equivalent to $y^2 - (x^3 - \frac{1}{16}x + \frac{1}{32})$,

(b) \mathbb{C} -equivalent to $y^2 - (x^3 - x - 2)$.

(a) It is enough to take the matrix $A_1 = \begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$ and compute $\vartheta_{A_1}^*(\tilde{w}) = 64y^2 - 64(x^3 - \frac{1}{16}x + \frac{1}{32})$, hence $y^2 - (x^3 - x + 2)$ and $y^2 - (x^3 - \frac{1}{16}x + \frac{1}{32})$ are \mathbb{R} -equivalent by the Fact from the lecture where we take $c = 2$ and $d = 0$.

(b) Now, we chose the complex matrix $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$ and calculate

$$\vartheta_{A_2}^*(\tilde{w}) = -y^2 - (-x^3 + x + 2).$$

Then the same argument as in (a) proves \mathbb{C} -equivalence of \tilde{w} and $y^2 - (x^3 - x - 2)$. □

2.3. Decide which of the following WEPs are smooth and find all singularities of singular ones:

(a) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$,

(b) $(y + 1)^2 - (x^3 + 1) \in \mathbb{F}_3[x, y]$,

(c) $y^2 - (x^3 - x^2 - x + 1) \in \mathbb{R}[x, y]$,

(d) $y^2 + y(2x + 2) - (x^3 - 4x^2 + 1) \in \mathbb{R}[x, y]$ (from 2.1).

(a) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ is a smooth short WEP by Proposition 2.2 since the polynomial $x^3 + 1$ is separable. The same result also follows from the Corollary 2.3 as

$$4 \cdot 0^3 + 27 \cdot 1^2 = 1 \neq 0.$$

(b) $w = (y + 1)^2 - (x^3 + 1) \in \mathbb{F}_3[x, y]$ is a singular WEP, since w is \mathbb{F}_3 -equivalent to $y^2 - (x^3 + 1)$ and the polynomial $x^3 + 1 = (x + 1)^3$ has the root 2 of multiplicity 3. It is easy to see that the only singularity is $(2, 2)$,

(c) $y^2 - (x^3 - x^2 - x + 1) \in \mathbb{R}[x, y]$ is also a singular WEP, since the root 1 of $x^3 - x^2 - x + 1$ has the multiplicity 2. Then the singularity is $(1, 0)$.

(d) Using the equivalent short form $y^2 - (x^3 - x + 2)$ computed in 2.1 we can easily see that the polynomial $f = x^3 - x + 2$ is separable. Indeed, the roots of $f' = 3x - 1$ are $\pm \frac{1}{\sqrt{3}}$ and $f(\pm \frac{1}{\sqrt{3}}) \neq 0$, so there is no multiple root of f . This means that $y^2 - (x^3 - x + 2)$ is smooth by Proposition 2.2, hence $y^2 + y(2x + 2) - (x^3 - 4x^2 + 1)$ is smooth by Fact from the lecture. \square

2.4. Let $f = y - x^3 \in \mathbb{C}[x, y]$. Find all singularities of V_f and of the projective extension V_F .

Since $\frac{\partial f}{\partial y} = 1$, the tangent $t_\alpha(f) \neq 0$ for each $\alpha \in V_f$, hence V_f is a smooth affine curve.

Clearly, $F = YZ^2 - X^3$. Then $V_F \cap V_Z = \{(0 : 1 : 0)\}$ since

$$F(\alpha : \beta : 0) = 0 \Leftrightarrow \alpha^3 = 0 \Leftrightarrow \alpha = 0 \Leftrightarrow (\alpha : \beta : 0) = (0 : 1 : 0).$$

We calculate

$$\frac{\partial F}{\partial X} = -3X^2, \quad \frac{\partial F}{\partial Y} = Z^2, \quad \frac{\partial F}{\partial Z} = 2YZ,$$

and so $t_{(0:1:0)}(F) = 0$. Thus F is singular at $(0 : 1 : 0)$ and V_F is a singular projective curve. \square