23.02.

1 Algebraic function fields

1.1. Consider extensions $\mathbb{R} \subseteq \mathbb{R}(x) \subseteq \mathbb{C}(x)$

(a) Prove that $\mathbb{R}(x)$ and $\mathbb{C}(x)$ are AFFs over $\mathbb{R}$,

(b) compute the field of constants $\tilde{\mathbb{R}}$ of the AFF $\mathbb{R}(x)$,

(c) compute the field of constants $\tilde{\mathbb{R}}$ of the AFF $\mathbb{C}(x)$,

(d) find a transcendental element $\alpha \in \mathbb{C}(x)$ such that $[\mathbb{C}(x) : \mathbb{R}(\alpha)]$ is minimal.

(a) It is enough to take the transcendental element x and compute using Proposition 2.3

$$[\mathbb{C}(x) : \mathbb{R}(x)] = [\mathbb{C} : \mathbb{R}] = 2 \quad \text{and} \quad [\mathbb{R}(x) : \mathbb{R}(x)] = 1.$$

(b) By the proof of Lemma 2.6 we know that $[\tilde{\mathbb{R}} : \mathbb{R}] \leq [\mathbb{R}(x) : \mathbb{R}(x)] = 1$, so $\tilde{\mathbb{R}} = \mathbb{R}$.

(c) Using (a) and the argument from (b) we can see that $[\tilde{\mathbb{R}} : \mathbb{R}] \leq [\mathbb{C}(x) : \mathbb{R}(x)] = 2$. As $\mathbb{C} \subseteq \tilde{\mathbb{R}}$ and $[\mathbb{C} : \mathbb{R}] = 2$ we obtain that $\tilde{\mathbb{R}} = \mathbb{C}$.

(d) We know that $[\mathbb{C}(x) : \mathbb{R}(x)] = 2$. Since

$$[\mathbb{C}(x) : \mathbb{R}(\alpha)] \geq [\tilde{\mathbb{R}}(\alpha)) : \mathbb{R}(\alpha)] = [\tilde{\mathbb{R}} : \mathbb{R}] = 2$$

by Proposition 2.3, and $[\mathbb{C}(x) : \mathbb{R}(x)] = 2$, the element $\alpha = x$ is a transcendental element with a minimal value of $[\mathbb{C}(x) : \mathbb{R}(\alpha)]$. $\square$

1.2. Let $K \subseteq U$ be a finite degree extension. Prove that $U(x)$ is an AFF over K with the field of constants $\tilde{K} = U$.

Applying Proposition 2.3 we can compute $[U(x) : K(x)] = [U : K] < \infty$ again, where x is transcendental and $U \subseteq \tilde{K}$. As

$$[U : K] \leq [\tilde{K} : K] = [\tilde{K}(x) : K(x)] \leq [U(x) : K(x)] = [U : K],$$

it holds $\tilde{K} = U$. $\square$

1.3. Prove that $\mathbb{Q}(\sqrt[3]{5}, \pi)$ is an AFF over $\mathbb{Q}$ and determine the field of constants $\tilde{\mathbb{Q}}$.

Observe that $\mathbb{Q}(\sqrt[3]{5}, x)\mathbb{Q}(\sqrt[3]{5})(x) \cong \mathbb{Q}(\sqrt[3]{5}, \pi)$. Now it remains to apply 1.2, which implies that $\tilde{\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{5})$. $\square$

1.4. Let $g \in K[x, y]$ be an irreducible polynomial, $R := K[x, y]/(g)$, L be a fraction field of R. Prove that L is an AFF over K.

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 $R = K[\xi, \upsilon] = K(\xi, \upsilon) = L$. Note that K-algebras $K[x]$ and $K[y]$ are infinitely dimensional as K-spaces, which implies $(g) \cap K[x] \neq 0$ and $(g) \cap K[y] \neq 0$. Then $g \in K^*$, a contradiction.

Since either 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. $\square$

02.03.

2 Local rings

2.1. Prove that each valuation ring is uniserial.

Assume to contrary that R is a non-uniserial VR, so there exists a pair of ideals I, J such that $I \not\subseteq J$ and $J \not\subseteq I$, Hence $\exists a \in I \setminus J$ and $\exists b \in J \setminus I$. Since R is a VR, either $\frac{a}{b} \in R$, which implies $a = b \cdot \frac{a}{b} \in J$ or $\frac{b}{a} \in R$, which implies $b = a \cdot \frac{b}{a} \in I$, a contardiction. $\square$

2.2. Let p be a prime number and define $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}, p \text{ does not divide } b\}$ is a VR.

It satisfies to observe that arbitrary non-zero element of $\mathbb{Q}$ (which is the field od fractions of $\mathbb{Z}$ and so of every subring of $\mathbb{Q}$) is of the form $\alpha = \frac{a}{b} \cdot p^i$ for $a, b, i \in \mathbb{Z}$ with a, b non-divisible by p. It imples that $\alpha \in \mathbb{Z}_{(p)}$ whenever $i \geq 0$, and $\alpha^{-1} \in \mathbb{Z}_{(p)}$ if $i \leq 0$. $\square$

2.3. Let $R_{x,y} = \{\frac{r}{s} \in \mathbb{R}(x, y) \mid r, s \in \mathbb{R}[x, y], s(0, 0) \neq 0\} \subseteq \mathbb{R}(x, y)$. Prove that

(a) $R_{x,y}$ is local,

(b) $R_{x,y}$ is not uniserial,

(c) $R_{x,y}$ is not valuation.

(a) It is enough to note that (x, y) is a maximal ideal of $R_{x,y}$ and that

$$R_{x,y} \setminus (x, y) = \{\frac{c + ax + by}{s} \in \mathbb{R}(x, y) \mid c \in \mathbb{R}^*, a, b, s \in \mathbb{R}[x, y] : s(0, 0) \neq 0\} = R^*_{x,y}$$

since $[c + ax + by](0, 0) = c \neq 0$.

(b) As $(x) \not\subseteq (y)$ and $(y) \not\subseteq (x)$, $R_{x,y}$ is not uniserial.

(c) It follows from (b) because every valuation ring is uniserial by 2.1, nevertheless, it is clear that both $\frac{xy}{x+y}, \frac{x+y}{xy} \notin R_{x,y}$. $\square$

2.4. Let (R, M) be a local ring (not necessary a domain) with $M = (t)$ for $t \neq 0$ and $A = \bigcap_i M^i = \bigcap_i (t^i)$. Prove that for each $s \in R \setminus A$ there exist unique $i \geq 0$ and some (not neceessary unique) $u \in R^*$ such that $s = t^i u$,

The proof of existence is the same as in Proposition 3.2 and we slightly modify the original proof of uniqueness:

Let $t^i u = t^j v$ for $i \geq j$ and $u, v \in R^*$, then $t^j(t^{i-j} - u^{-1}v) = 0$. If $i > j$ then $t^{i-j} - u^{-1}v \notin M$, hence $t^{i-j} - u^{-1}v \in R^*$, which implies $t^j = 0$, a contradiction. Thus $i = j$ and we are done. $\square$

08.03.

2.5. Let (R, M) be a local domain with $M = (t)$ for $t \neq 0$ and $A = \bigcap_i M^i = \bigcap_i (t^i)$. Prove that $AM = A$.

If there exists i for which $M^i = M^{i+1}$ then $A = M^i$, hence $AM = M^{i+1} = A$.

Let $a \in A = \bigcap_i M^i$ then for each $i > 0$ there exists $a_i \in M^i$ such that $a = a_i t$, since $R \setminus M = R^*$. As $a_i t = a = a_j t$, we get $(a_i - a_j)t = 0$, which implies $a_0 := a_i = a_j$ for each $i, j > 0$. Hence $a = a_0 t$ for $a_0 \in \bigcap_i M^i = A$. $\square$

09./11.03.

3 Discrete valuation rings

3.1. Let R be a noetherian ring and $p \in R$ a prime element. Prove that the localization $R_{(p)}$ is a DVR with the NDV ν_p.

By Example 4.1 ν_p is a NDV of the field od fractions K of R and it remains to observe that

$$R_{(p)} = \{\frac{a}{b} \in K \mid a \in R, b \in R \setminus (p)\} = \{\frac{a}{b} \in K \mid \nu(a) \geq 0, \nu(b) = 0\} = \nu_p^{-1}(\langle 0, \infty\rangle).$$

□

3.2. Let $S = \mathbb{F}_2[X]_{(x^2+x+1)}$ be a localization of $\mathbb{F}_2[X]$ in (x^2+x+1).

(a) Show that S is DVR and find all DV ν such that $S = \nu^{-1}(\langle 0, \infty\rangle)$,

(b) if ν is NDV determining S, compute $\nu(x^5)$, and $\nu(\frac{x^4+x^2+x}{(x+1)^5(x^2+x+1)^3})$,

(c) if ν is NDV determining S, M is the maximal ideal of S, $a \in M^2 \setminus M^3$ and $b \in M^3 \setminus M^4$, compute $\nu(ab)$ and $\nu(a+b)$.

(a) S is DVR by 3.1 and all DV determining S are of the form $k\nu_{x^2+x+1}$ for an arbitrary natural k by Lemma 4.4.

(b) As $\nu = \nu_{x^2+x+1}$ by Lemma 4.4 and x^2+x+1 does not divide x, we obtain that $\nu(x^5) = 5\nu(x) = 0$. Similarly, $\nu(\frac{x^4+x^2+x}{(x+1)^5(x^2+x+1)^3}) =$

$$= \nu(x) + \nu(x^3+x+1) - 5\nu(x+1) - 3\nu(x^2+x+1) = 0 + 0 - 0 - 3 = -3.$$

(c) Since $M = (t)$ for a uniformizing element t, the condition $a \in M^2 \setminus M^3 = (t^2) \setminus (t^3)$ mens that $\nu(a) = \nu(t^2) = 2$ and $b \in M^3 \setminus M^4$ implies that $\nu(b) = \nu(t^3) = 3$. Thus

$$\nu(ab) = \nu(a) + \nu(b) = 5 \quad \text{and} \quad \nu(a+b) = \min(2,3) = 2$$

by (D1) and Lemma 4.6. □

3.3. Let $R = \mathbb{Z}_{(5)} \leq \mathbb{Q}$ be a localization of $\mathbb{Z}$ in the prime ideal (5). Find for every $k \geq 2$ elements $a, b \in \mathbb{Z}_{(5)}$ such that $\nu_5(a) = \nu_5(b) = 2$ and $\nu_5(a+b) = k$.

Note that $\nu_5(25s) = 2$ for an arbitrary element $s \in R^*$ and $\nu_5(5^k) = k$, in particular $\nu_5(50) = \nu_5(-50) = 2$. Put $a = 5^k + 50$ and $b = 5^k - 50$, then

$$\nu_5(5^k \pm 50) = \nu(50) = 2 \ \ \forall k > 2 \ \text{ by Lemma 4.6. and}$$

$$\nu_5(5^2 + 50) = \nu(3 \cdot 25) = 2 = \nu_5(5^2 - 50) = \nu(-1 \cdot 25)$$

Now, clearly $\nu_5(a+b) = \nu_5(5^k) = k$. □

3.4. Let P be a place of an AFF L over K and $\nu_P(a) = 3$ for $a \in L$. Compute $\nu_P(a^2 - a)$ and $\nu_P(a^{-2} - a^{-1})$.

We can apply Lemma 4.9(3),(4): Since $p = x^2 + x$ is a polynomial of the degree 2 and the multiplicity 1, $\nu_P(a) = 3$ and so $\nu_P(a^{1-}) = -3$ we get that

$$\nu_P(a^2 - a) = \nu_P(a) \cdot \mathrm{mult}(x^2 + x) = 3 \cdot 1 = 3 \ \text{ by 4.9(3) and}$$

$$\nu_P(a^{-2} - a^{-1}) = \nu_P(a^{-1}) \cdot \deg(x^2 + x) = -3 \cdot 2 = -6 \ \text{ by 4.9(4).}$$

□

22.03.

4 Weierstrass equations

4.1. 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 linear algebra machinery used in the proofs of Section 5. 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 use $b = (1, -1)$ to exclude monomials y and x^2:

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

$\square$

4.2. 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 Corollary 5.4 for $c = 2$.

(b) Now, we chose the complex matrix $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$. Since $\vartheta_{A_2}^*(\tilde{w}) = -y^2 - (-x^3 + x + 2)$, the same argument as in (a) proves $\mathbb{C}$-equivalence of $\tilde{w}$ and $y^2 - (x^3 - x - 2)$. $\square$

4.3. 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 4.1).

(a) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ is a smooth short WEP by Proposition 6.4 since the polynomial $x^3 + 1$ is separable,

(b) $(y+1)^2 - (x^3+1) \in \mathbb{F}_3[x, y]$ is a singular WEP, since 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 4.1 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 6.4, so $y^2 + y(2x+2) - (x^3 - 4x^2 + 1)$ is smooth by Corollary 6.3. $\square$

29.03.

4.4. Find at least 3 maximal ideals in $\mathbb{R}[x,y]$ containing the WEP $w = y^2 - (x^3+1)$.

Since maximal ideal of $\mathbb{R}[x,y]$ are of the form $I_{(c_1,c_2)}$ for $c_1, c_2 \in \mathbb{C}$ by Theorem 7.4 and $w \in I_{(c_1,c_2)} \Leftrightarrow w(c_1,c_2) = 0$, it is enough to find 3 zeros of w. We get for example maximal ideals containing w:

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

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

06.04.

5 Computing discrete valuations

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

(a) Show that w is a WEP,

(b) compute $\mu(g), S(g)$ and $\mu(h), S(h)$,

(c) compute $\mu(x^3y^2)$, $\mu(x^2y^3)$ and $\mu(x^3y^2 + x^2y^3)$,

(d) find $S(\Lambda(x^3y^2))$ and $S(\Lambda(x^3y^2 + x^2y^3))$.

(a) It is easy to see by applying the substitution $\hat{y} \leftarrow y+x+1$ that $\hat{y} - (x^3+2x+1) \in \mathbb{R}[x,y]$ is a short WEP equivalent to w by. Since $\gcd(x^3+2x+1, 3x^2+2) = 1$, the polynomial w is a smooth WEP by Corollary 6.3 and Proposition 6.4.

(b) Note that $\mathrm{mult}(g) = 1$ and $m = \mathrm{mult}(h) = 2$. Then it is easy to compute

$$\mu(g) = \mathrm{mult}(x + \frac{1}{2}y^2) = 1, S(g) = x \;\text{ and }\; \mu(h) = \mathrm{mult}(h) = 2, S(h) = \frac{1}{2}x^2.$$

(c) By the definition we can see that $\mu(x^3y^2) = 3 + 2\cdot 2 = 7$, $\mu(x^2y^3) = 2 + 3\cdot 2 = 8$ hence $\mu(x^3y^2 + x^2y^3) = 7$ by Observation (2) on page 13.

(d) Using the proof of Lemma 9.2 we observe that

$$S(\Lambda(x^3y^2)) = (-\frac{1}{2})^2 x^{\mu(x^3y^2)} = \frac{1}{4}x^7.$$

Since Λ is K-endomorphisms of the K-algebra $K[x,y]$ we can compute

$$S(\Lambda(x^3y^2 + x^2y^3)) = S(\Lambda(x^3y^2) + \Lambda(x^2y^3)) = S(\Lambda(x^3y^2)) = \frac{1}{4}x^7.$$

by Observation (4) on page 13, because $\mu(\Lambda(x^3y^2)) = 8 > 7 = \mu(\Lambda(x^2y^3))$. □

12.04.

5.2. Let $f = yg(x,y) + h(x) + y = y(x + \frac{1}{2}y) + \frac{1}{2}(x^2 - x^3) + y \in \mathbb{R}[x,y]$ for $g = x + \frac{1}{2}y$ and $h = \frac{1}{2}(x^2 - x^3)$ from 5.1. Put $u = x + (f)$, $v = y + (f)$ and note that $L = \mathbb{R}(u,v)$ is an AFF over $\mathbb{R}$ given by $f(u,v) = 0$. Let P be the uniquely determined place from Theorem 9.5 containing u, v. Compute

(a) $\nu_P(u)$, $\nu_P(v)$,

(b) $\nu_P(u+v)$,

(c) $\nu_P(u^2+v)$, $\nu_P(u^2+2v)$.

(a) $\nu_P(u) = 1$ and $\nu_P(v) = \mathrm{mult}(h) = 2$ follows immediately form Theorem 9.5
(b) Using (a) and Lemma 4.6 we get $\nu_P(u+v) = \min(\nu_P(u), \nu_P(v)) = 1$.
(c) Since $f(u,v) = 0$, we get $v = -v(u + \frac{1}{2}v) + \frac{1}{2}(u^3 - u^2)$, hence

$$\nu_P(u^2+v) = \nu_P(\frac{1}{2}u^2 - vu - \frac{1}{2}v^2 + \frac{1}{2}u^3) = \min(2,3,4,3) = 2.$$

Note that $\nu_P(u^2 - 2v) = \nu_P(-u^3 + 2vu + v^2 + 2u^2) = \min(2,3,4,3) = 2$, which implies $\nu_P(u(u^3 - 2v)) = 3$. Thus

$$\nu_P(u^2+2v) = \nu_P(u(u^3 - 2v) - v^2) = \min(3,4) = 3.$$

again by Lemma 4.6 □

19.04.

5.3. Let $f = y^2 + xy + x^5 + 32 \in \mathbb{R}[x,y]$ and denote by L the AFF over $\mathbb{R}$ given by $f(\alpha,\beta) = 0$ for $\alpha = x + (f)$ and $\beta = y + (f) \in \mathbb{R}[x,y]/(f)$.

(a) Determine the field of constants of L the AFF over $\mathbb{R}$,

(b) show that $(-2,2) \in V_f$ and compute $t_{(-2,2)}(f)$,

(c) if $P \in \mathbb{P}_{L/K}$ contains $\alpha+2, \beta-2$, compute $\nu_P(\alpha+2)$ and $\nu_P(\alpha+\beta)$ and

(d) describe the structure of P.

(a) Since f is an absolutely irreducible by Lemma 8.2, the the field of constants $\tilde{\mathbb{R}} = \mathbb{R}$ by Proposition 8.3.

(b) It is easy to see that $f((-2,2)) = 0$, hence $(-2,2) \in V_f$. Since

$$\frac{\partial f}{\partial x} = y + 5x^4, \quad \frac{\partial f}{\partial y} = 2y + x,$$

we get

$$\frac{\partial f}{\partial x}(-2,2) = 82, \quad \frac{\partial f}{\partial y}(-2,2) = 2, \quad \text{hence} \quad t = t_{(-2,2)}(f) = 82x + 2y + 160.$$

(c) Note $(-2,2)$ is a zero of both lines $x+2$, $x+y$. As $x+2, x+y \notin (t)$ we get that $\nu_P(\alpha+2) = \nu_P(\alpha+\beta) = 1$ by Theorem 9.7.

(c) By (c) both elements $\alpha+2$ and $\alpha+\beta$ are uniformizing elements of the DVR $\mathcal{O}_P$, i.e. the generators of its maximal ideal P. Thus by Proposition 10.4 and Theorem 9.7 $P = P_{(-2,2)} = (\alpha+2) = \{(\alpha+2)\frac{p(\alpha,\beta)}{q(\alpha,\beta)} \mid q(-2,2) \neq 0\}$. □

26.04.

6 Places and divisors

6.1. Let $f = y^2 + y - (x^3 + 1) = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ and denote by L the AFF over $\mathbb{F}_2$ given by $f(\alpha, \beta) = 0$ for $\alpha = x + (f)$ and $\beta = y + (f) \in \mathbb{F}_2[x, y]/(f)$.

(a) Find all points of $V_f(\mathbb{F}_2)$, which of them are smooth?

(b) Determine $\mathbb{P}^{(1)}_{L/K}$.

(c) Find $P \in \mathbb{P}_{L/K} \setminus \mathbb{P}^{(1)}_{L/K}$.

(a) We can directly compute that $V_f(\mathbb{F}_2) = \{(1, 0), (1, 1)\}$. As

$$\frac{\partial f}{\partial x} = x, \quad \frac{\partial f}{\partial y} = 1,$$

we compute $t_{(1,0)}(f) = x + y + 1$ and $t_{(1,1)}(f) = x + y$, hence both points of $V_f(\mathbb{F}_2)$ are smooth.

(b) $\mathbb{P}^{(1)}_{L/K} = \{P_{(1,0)}, P_{(1,1)}, P_\infty\}$, since $V_f(\mathbb{F}_2) = \{(1, 0), (1, 1)\}$ by Proposition 11.8.

(c) Note that by Corollary 11.3 $\mathbb{P}_{L/K}$ is infinite, hence $P \in \mathbb{P}_{L/K} \setminus \mathbb{P}^{(1)}_{L/K}$ is infinite. Fix for example an irreducible polynomial $m \in \mathbb{F}_2[x]$ of degree greater than 1. Then there exists $P_m \in \mathbb{P}_{L/K}$ such that $m(\alpha) \in P_m$ since $m(\alpha)$ is transcendental over $\mathbb{F}_2$. Note that $K[\alpha]/(m(\alpha))$ is a K-space of dimension $\deg(m)$ which is embeddable into the K-algebra $\mathcal{O}_P/P$ since $P \cap K[\alpha] = (m(\alpha)$. Thus

$$\deg P_m = \dim_K(\mathcal{O}_P/P) \geq \dim_K(K[\alpha]/(m(\alpha))) = \deg(m) > 1.$$

If we choose for example $m = x^2 + x + 1$, then $\deg P_m \geq 2$. $\square$

03.05.

6.2. Consider the AFF given by $f(\alpha, \beta) = 0$ for $f = y^2 + y - (x^3 + 1) = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ from 6.1.

(a) Compute degrees of positive and negative parts of principal divisors $(\alpha + 1)$ and (α)

(b) Determine divisors $(\alpha + 1)$ and (α) as elements of free group $Div(L/\mathbb{F}_2)$.

(a) By 12.6

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

and similarly $\deg((\alpha)_+) = \deg((\alpha)_+) = [L : \mathbb{F}_2(\alpha)] = 2$.

(b) Recall that $(\alpha+1)_+ = \sum_{P:\ \alpha+1 \in P} \nu_P(\alpha+1)P$. It is easy to compute that $\alpha + 1 \in P_{(1,0)} \cap P_{(1,1)}$ and we know that $\nu_{P_\infty}(\alpha + 1) = \nu_{P_\infty}(\alpha) = -2$ by 17.7, so we get

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

Since $\alpha \notin P$ 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

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

$\square$

17.05.

6.3. Compute the genus of an AFF $K(x)$ over o field K.

By 4.7 we know the structure of places $K(x)$:

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

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). $\square$

6.4. Describe ale principal divisors of $K(x)$ over o field K.

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. $\square$

18.05.

6.5. Decide whether $\mathbb{F}_2(V_w)$ is an EFF, if (a) $w = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x,y]$, (b) $w = y^2 + x^3 + x + 1 \in \mathbb{F}_2[x,y]$

(a) We have computed in 6.1 that w is smooth at rational points $V_w(\mathbb{F}_2) = \{(1,0),(1,1))\}$. Thus by 15.4 the genus of $\mathbb{F}_2(V_w)$ is 1, hence it is an EFF.

(b) Since there is a singularity at $(1,1) \in V_w(\mathbb{F}_2)$, $\mathbb{F}_2(V_w)$ is of genus 0 again by by 15.4. $\square$

6.6. If there exists, find s such that $\mathbb{F}_2(s) = \mathbb{F}_2(V_w)$ for w from ref6.5.

(a) Since $\mathbb{F}_2(V_w)$ is an EFF, $\mathbb{F}_2(s) \subsetneqq \mathbb{F}_2(V_w)$ for each $s \in \mathbb{F}_2(V_w)$ by Proposition 14.6.

(b) As $(1,1) \in V_w(\mathbb{F}_2)$ is a singularity, there exists $s \in \mathbb{F}_2(V_w)$ such that $\mathbb{F}_2(s) = \mathbb{F}_2(V_w)$ by 15.3. Using the proof of 15.3, 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 $w(\alpha, \beta) = 0$. $\square$