1. Hilbertova věta o nulách

5.cvičení (16.3.)

1.1. Spočítejte $V(I)$, $I(V(I))$ nad tělesem komplexních čísel a $\dim_{\mathbb{C}}(R/I)$, jestliže
(1) $I = (x^2 + y^2, x^2 - y^2)$ je ideál oboru $R = \mathbb{C}[x, y]$
(2) $I = (x_1, x_2^2, \dots, x_n^n)$ je ideál oboru $R = \mathbb{C}[x_1, \dots, x_n]$,
(3) $I = ((x-2)^6, (x+y)^5, (z^2+1)^3)$ je ideál oboru $R = \mathbb{C}[x, y, z]$.

(1) Nejprve najdeme hezčí množinu generátorů ideálu I, tedy ukážeme že $I = (x^2, y^2)$. Zřejmě $I \subseteq (x^2, y^2)$ a naopak

$$x^2 = \frac{1}{2}(x^2 + y^2 + x^2 - y^2), y^2 = x^2 + y^2 - x^2 \in I,$$

proto $(x^2, y^2) = I$. Nyní snadno dokážeme, že $1 + I, x + I, y + I, xy + I$ tvoří bázi $\mathbb{C}[x, y]/I$ jako vektorového prostoru nad tělesem $\mathbb{C}$. Nejprve si všimneme, že máme-li lineární kombinaci

$$a + bx + cy + dxy + I = a(1 + I) + b(x + I) + c(y + I) + d(xy + I) = 0 + I$$

pro $a, b, c, d \in \mathbb{C}$, pak $a + bx + cy + dxy \in I$ Proto $a = b = c = d = 0$, tedy posloupnost $1 + I, x + I, y + I, xy + I$ je lineárně nezávislá. Uvážíme-li libovolný polynom $p \in \mathbb{C}[x, y]$, pak například pomocí dělení se zbytkem, vyjádříme p nejprve jako $p = qx^2 + \alpha x + \beta$, kde $q \in \mathbb{C}[x, y]$ a $\alpha, \beta \in \mathbb{C}[y]$ a poté koeficienty $\alpha = sy^2 + dy + b$ a $\beta = ty^2 + cy + a$, kde $s, t \in \mathbb{C}[y]$ a $a, b, c, d \in \mathbb{C}$, což znamená, že

$$p + I = a + bx + cy + dxy + qx^2 + (sx + t)y^2 = a + bx + cy + dxy + I.$$

To znamená, že $1 + I, x + I, y + I, xy + I$ je báze $\mathbb{C}[x, y]/I$ nad tělesem $\mathbb{C}$, a proto $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I) = 4$.

Dále máme $x, y \in \sqrt{I}$, neboť $x^2, y^2 \in I$ a podle Hilbertovy věty o nulách platí, že $\sqrt{I} = I(V(I))$. Tudíž $I \subseteq (x, y) \subseteq \sqrt{I}$, kde (x, y) je maximální ideál. Protože je každý maximální ideál prvoideálem, $I \subseteq (x, y)$ a platí, že

$$\sqrt{I} = \bigcap \{P \subseteq \mathbb{C}[x, y] |\ I \subseteq P, P \text{ je prvoideál}\},$$

dostáváme rovnost $I(V(I)) = \sqrt{I} = (x, y)$. Konečně, nyní víme, že $V(I) = V(I(V(I))) = V(x, y)$, odkud okamžitě plyne, že $V(I) = \{(0, 0)\}$.

(2) Podobně jako v (1) vidíme, že $I \subseteq (x_1, x_2, \dots, x_n) \subseteq \sqrt{I}$, kde $(x_1, x_2, \dots, x_n)$ je maximální ideál, proto

$$I(V(I)) = \sqrt{I} = (x_1, x_2, \dots, x_n) \quad \text{a} \quad V(I) = V(x_1, x_2, \dots, x_n) = \{(0, \dots, 0)\}.$$

Indukční variantou úvahy z (1) zjistíme, že bázi $\mathbb{C}[x_1, \dots, x_n]/I$ tentokrát tvoří množina $B = \{\prod_{i \le n} x_i^{j_i} + I |\ j_i < i\}$, proto $\dim_{\mathbb{C}}(\mathbb{C}[x_1, \dots, x_n]/I) = |B| = (n-1)!$.

(3) Díky afinní transformaci existuje okruhový $\mathbb{C}$-automorfismus φ, pro který $\widehat{I} = \varphi(I) = (x^6, y^5, (z^2+1)^3)$. Budeme pracovat s ideálem $\widehat{I}$. I tentokrát dostáváme inkluzi $(x, y, (z^2+1)) \subseteq \sqrt{\widehat{I}}$ navíc nám aplikace Hilbertovy věty o nulách dává $I(V(\widehat{I})) = \sqrt{\widehat{I}} =$

$$= \sqrt{(x^6, y^5, (z^2+1)^3)} \subseteq (x, y, (z - i)) \cap (x, y, (z + i)) = I(\{(0, 0, i)\}) \cap I(\{(0, 0, -i)\}).$$

Protože oba ideály $(x, y, (z - i))$ $(x, y, (z + i))$ jsou maximální a například pomocí dělení se zbytkem monomy x a y není těžké nahlédnout, že

$$(x, y, (z - i)) \cap (x, y, (z + i)) = (x, y, (z^2 + 1)) \subseteq \sqrt{(x^6, y^5, (z^2 + 1)^3)},$$

dostáváme rovnosti

$$V(\widehat{I}) = \{(0,0,i),(0,0,-i)\} \quad \text{a} \quad I(V(\widehat{I})) = (x, y, z^2+1).$$

Nyní inverzní afinní transformací zjistíme, že

$$V(I) = \{(2,-2,i),(2,-2,-i)\},\ I(V(I)) = (x-2, x+y, z^2+1) = (x-2, y+2, z^2+1).$$

Konečně obdobnou úvahou jako v (1) a (2) spočítáme, že množina

$$C = \{x^i y^j z^k \mid i < 6, j < 5, k < 6\}$$

tvoří reprezentanty báze vektorového prostoru $\mathbb{C}[x,y,z]/\widehat{I} \cong \mathbb{C}[x,y,z]/I$ nad tělesem $\mathbb{C}$, a tudíž $\dim_{\mathbb{C}}(\mathbb{C}[x,y,z]/I) = |C| = 180$. □

6.cvičení (23.3.)

1.2. Nechť $p, q \in T[x,y]$ jsou dva nesoudělné polynomy. Dokažte, že $V(p,q)$ je konečná množina.

Na polynomy p, q můžeme nahlížet jako na prvky oboru $T(x)[y]$, kde $T(x)$ značí podílové těleso oboru $T[x]$, tedy obor racionálních lomených funkcí v jedné neurčité x. Tento obor je Eukleidův, proto musí existovat $u, v \in T(x)[y]$, pro něž $up + vq = 1$. Vezmeme-li nějakého společného jmenovatele $h \in T[x]$ všech koeficientů polynomů u, v, pak $hup + hvq = h$, kde už $hu, hv \in T[x,y]$. Protože je h nenulový, existuje jen konečně mnoho kořenů K_x polynomu h. Nyní stejnou úvahou pro obor $T(y)[x]$ najdeme polynomy $g \in T[y]$ a $r, s \in T[x,y]$, pro něž $rp + sq = g$. Označíme-li K_y všechny kořeny polynomu g, pak vidíme, že

$$V(p,q) \subseteq V(g,h) = K_x \times K_y.$$

Tedy $V(p,q)$ je konečná množina. □

1.3. Je-li $g \in T[x,y]$ ireducibilní polynom a $V(g)$ nekonečné, dokažte, že $IV(g) = (g)$, a že je $V(g)$ varieta.

Víme, že $(g) \subseteq IV(g)$. Předpokládejme $f \in IV(g) \setminus (g)$. Protože je g ireducibilní a g nedělí f, jsou polynomy f a g v $T[x,y]$ nesoudělné. Dále $V(g) = VIV(g) \subseteq V(f,g)$, neboť $(f,g) \subseteq IV(g)$. Ovšem $V(f,g)$ je podle 1.2 je konečné, což je ve sporu s předpokladem, že $V(g)$ je nekonečná množina. Závěr, že je $V(g)$ varieta okamžitě plyne z faktu, že $IV(g) = (g)$ je prvoideál. □

1.4. Dokažte, že je $V(x^2 + xy + y) \subseteq A^2(\mathbb{C})$ varieta.

Využijeme 1.3, a proto stačí, abychom nahlédli, že je polynom $x^2 + xy + y$ ireducibilní a $V(x^2 + xy + y)$ nekonečné. Přímým výpočtem dostaneme

$$\{(t, -\frac{t^2}{t+1} \mid t \in \mathbb{C} \setminus \{-1\})\} \subseteq V(x^2 + xy + y),$$

tudíž druhá podmínka zřejmě platí. Protože je v proměnné y polynom $x^2 + xy + y$ stupně 1 a v proměnné x stupně 2 a navíc tento polynom zjevně není součinem polynomu stupně 0 nad x a polynomu stupně 0 nad y (tj. jednoho prvku oboru $\mathbb{C}[x]$ a jednoho prvku oboru $\mathbb{C}[y]$), znamenala by jeho reducibilita, že by byl tvaru $(x-\alpha)(x-\beta)$ pro $\alpha, \beta \in \mathbb{C}[y]$, což nenastává. □

1.5. Dokažte, že je $V(I)$ varieta a popište její souřadnicový okruh, jestliže

(1) $I = (x^2 + xy + y)^{666}$ v $\mathbb{C}[x,y]$,

(2) $I = ((xz - y^2)^3, (z^3 - x^5)^7, y^3 + x^4)$ v $\mathbb{C}[x, y, z]$.

(1) Připomeňme, že jsme v 1.4 dokázali, že $V(x^2+xy+y)$ je varietou, protože x^2+xy+y je ireducibilní polynom. Nyní můžeme přímo využít tohoto faktu nebo znovu zužitkovat Hilbertovu větu o nulách.

Protože je těleso $\mathbb{C}$ algebraicky uzavřené, víme díky přímému odmocnění polynomu $(x^2 + xy + y)^{666}$ a Hilbertově větě o nulách, že $(x^2 + xy + y) \subseteq \sqrt{I} = I(V(I))$. Zřejmě $I = (x^2 + xy + y)^{666} \subseteq (x^2 + xy + y)$, kde $(x^2 + xy + y)$ je prvoideál, a proto $I(V(I)) = (x^2 + xy + y)$ a a tudíž souřadnicový okruh této variety je tvaru $\mathbb{C}[x, y]/(x^2 + xy + y)$.

(2) Nejprve si všimněme, že $I \subseteq (xz - y^2, z^3 - x^5, y^3 + x^4)$, proto

$$\sqrt{I} \subseteq \sqrt{(xz - y^2, z^3 - x^5, y^3 + x^4)},$$

a naopak, protože $(xz - y^2, z^3 - x^5, y^3 + x^4) \subseteq \sqrt{I}$, dostáváme obrácenou inkluzi

$$\sqrt{(xz - y^2, z^3 - x^5, y^3 + x^4)} \subseteq \sqrt{\sqrt{I}} = \sqrt{I}.$$

I tentokrát použijeme Hilbertovy věty o nulách a dostaneme

$$I(V(I)) = \sqrt{I} = \sqrt{(xz - y^2, z^3 - x^5, y^3 + x^4)} = I(V((xz - y^2, z^3 - x^5, y^3 + x^4))).$$

Zjistili jsme, že $V((xz - y^2, z^3 - x^5, y^3 + x^4)) = \{(t^3, -t^4, t^5)|\ t \in \mathbb{C}\}$ je varieta, proto je $V(I) = \{(t^3, -t^4, t^5)|\ t \in \mathbb{C}\}$ tatáž varieta s týmž souřadnicovým okruhem

$$\mathbb{C}[x, y, z]/I(\{(t^3, -t^4, t^5)|\ t \in \mathbb{C}\}) \cong \{\sum_i h_i t^i \in \mathbb{C}[t]|\ h_1 = h_2 = 0\} \subseteq \mathbb{C}[t].$$

□

7.cvičení (30.3.)

1.6. Spočítejte $V(I)$ a rozhodněte, zda se jedná o varietu určenou nad tělesem reálných čísel pro ideály

(1) $I = (x^2 + xy + y) \subseteq \mathbb{R}[x, y]$,
(2) $I = (xz - y^2, z^3 - x^5, y^3 + x^4)$ v $\mathbb{R}[x, y, z]$.

V obou případech nás zajímají nuly daných ideálů nad v komplexních afinních prostorech. Protože stačí uvažovat generátory, úlohu už jsme už vyřešili, tedy

$$V(x^2 + xy + y) = \{(t, -\frac{t^2}{1+t})|\ t \in \mathbb{C} \setminus \{-1\}\}$$
$$V(xz - y^2, z^3 - x^5, y^3 + x^4) = \{(t^3, -t^4, t^5)|\ t \in \mathbb{C}\}$$

Protože $I(V(I)) = \sqrt{I}$ jsou prvoideály okruhů polynomů s komplexními koeficienty a průnik $P \cap \mathbb{R}[x_1, \ldots, x_n]$ je prvoideálem pro každý prvoideál oboru $\mathbb{C}[x_1, \ldots, x_n]$, dostáváme i tentokrát prvoideály. To znamená, že obě algebraické množiny $V(I)$ jsou i nad $\mathbb{R}$ variety. □

1.7. Pro množinu X určete $I(X)$ $V(I(X))$ nad tělesem reálných čísel a rozhodněte, zda je X a $V(I(X))$ varieta, jestliže

(1) $X = \{(1, 2)\}$,
(2) $X = \{(1 - i, 2 + i)\}$

(1) Okamžitě vidíme, že $I((1, 2)) = (x-1, y-2)$ je maximální ideál, tedy $V(I(X)) = X$ je varieta, neboť $I(V(I(X))) = I(X)$.

(2) Tentokrát víme, že $V(I(X))$ je uzavřené na akci Galoisovou grupou, proto s každým prvkem obsahuje hodnotu komplexně sdruženou. Tudíž $\{(1 - i, 2 + i), (1 + i, 2 - i)\} \subseteq$

$V(I(X))$. Dále vezměme minimální polynom $x^2 - 2x + 2$ prvku $1 - i$ nad tělesem reálných čísel a všimněme si, že dvojice $(1-i, 2+i)$ je řešením lineární rovnice s reálnými koeficienty $x + y = 3$. To znamená, že

$$J = (x^2 - 2x + 2, x + y - 3) \subseteq I(X).$$

Nyní ověříme, že je J maximální ideál oboru $\mathbb{R}[x, y]$. Uvažme dosazovací homomorfismus $\Omega : \mathbb{R}[x, y] \to \mathbb{R}[x]$ daný vztahem $\Omega(f(x, y)) = f(x, 3 - x)$ a dále mějme přirozenou projekci $\pi : \mathbb{R}[x] \to \mathbb{R}[x]/(x^2 - 2x + 2)$. Snadno zjistíme, že složení $\pi\Omega$ je homomorfismus na těleso $\mathbb{R}[x]/(x^2 - 2x + 2)$ (protože polynom $x^2 - 2x + 2$ je ireducibilní nad $\mathbb{R}$). Navíc ukážeme, že

$$\ker \pi\Omega = \Omega^{-1}(x^2 - 2x + 2) = J.$$

Inkluze $J \subseteq \ker \pi\Omega$ je triviální a vezmeme-li polynom $f \in \ker \pi\Omega$, můžeme ho vydělit se zbytkem v proměnné y (monickým) polynomem $y + (x - 3)$, tedy $f = q(x + y - 3) + r$ pro vhodné $q \in \mathbb{R}[x, y]$ a $r \in \mathbb{R}[x]$. To znamená, že

$$\pi(r) = \pi\Omega(r) = \pi\Omega(f - q(x + y - 3)) = \pi\Omega(f) = 0,$$

proto $r \in \mathrm{Ker}\pi = (x^2 - 2x + 2)$, proto $r \in J$ a tudíž $f \in J$, čímž jsme ověřili platnost inkluze $\ker \pi\Omega \subseteq J$.

Podle první věty o izomorfismu pro okruhu dostáváme, že $\mathbb{R}[x, y]/J \cong \mathbb{R}[x]/(x^2 - 2x + 2)$, tedy J je maximální ideál. Protože $I(X) \neq \mathbb{R}[x, y]$ a $J \subseteq I(X)$, dostáváme z maximality J, že $J = I(X)$.

Odtud už se přímočaře dopočítá, že $VI(X) = \{(1 - i, 2 + i), (1 + i, 2 - i)\}$ a protože $IVI(X) = I(X) = J$ je prvoideál, je množina $VI(X)$ varietou. Závěrem poznamenejme, že množina $X = \{(1 - i, 2 + i)\}$ není algebraická, tedy se nejedná o varietu. $\square$

8.cvičení (13.4.)

1.8. Pro množinu X určete $I(X)$ $V(I(X))$ nad tělesem reálných čísel a spočítejte ireducibilní rozklad algebraické množiny $V(I(X))$, jestliže

(1) $X = \{(1 - i, 2 + i), (1 + 2i, i)\} \subset A^2(\mathbb{C})$
(2) $X = \{(\alpha_j, \beta_j) |\ j \leq k\} \subset A^2(\mathbb{C})$,
(3) $X = \{(1 - i, 2 + i, 1), (1, 2 - i, 3 + 2i)\} \subset A^3(\mathbb{C})$.

(1) Označme $J_1 = I((1 - i, 2 + i))$ a $J_2 = I((1 + 2i, i))$. V úloze 1.7(2) jsme spočítali

$$J_1 = (x^2 - 2x + 2, x + y - 3) \ \text{ a } \ IV(J_1) = \{(1 - i, 2 + i), (1 + i, 2 - i)\}.$$

Obdobnou úvahou pro minimální polynom prvku $1+2i$ a netriviální reálné řešení soustavy lineárních rovnic $a(1 + 2i) + bi + c = 0$ dostaneme

$$J_2 = (x^2 - 2x + 5, x - 2y - 1) \ \text{ a } \ IV(J_1) = \{(1 + 2i, i), (1 - 2i, -i)\}.$$

Navíc přímo z definice vidíme, že

$$I((1 - i, 2 + i), (1 + 2i, i)) = I((1 - i, 2 + i)) \cap I((1 + 2i, i)) = J_1 \cap J_2.$$

Zbývá spočítat $VI(X) = V(J_1 \cap J_2)$. Označme $Y_i = V(J_i)$ a $Y = Y_1 \cup Y_2$. Potom

$$Y_1 = \{(1 - i, 2 + i), (1 + i, 2 - i)\} \ \text{ a } \ Y_2 = \{(1 + 2i, i), (1 - 2i, -i)\}.$$

Protože $J_1 \cap J_2 \subseteq J_i$, máme

$$Y = V(J_1) \cup V(J_2) \subseteq V(J_1 \cap J_2) = VI(X).$$

Naopak, protože $J_1J_2 \subseteq J_1 \cap J_2$, dostáváme, že

$$VI(X) = V(J_1 \cap J_2) \subseteq V(J_1J_2) = V(J_1) \cup V(J_2) = Y.$$

Zjistili jsme, že $I(X) = J_1 \cap J_2$, dále $VI(X) = Y$ a $VI(X) = Y_1 \cup Y_2$ je rozklad algebraické množiny $VI(X)$ na variety.

(2) Tentokrát pouze indukčně zobecníme předchozí úvahy. Nejprve definujeme ideály J_j a Y_j následujícím způsobem:

(a) Jestliže $(\alpha_j, \beta_j) \in \mathbb{R}^2$, pak $J_j = (x - \alpha_j, y - \beta_j)$ a $Y_j = \{(\alpha_j, \beta_j)\}$.
(b) Jestliže $\alpha_j, \notin \mathbb{R}$, vezmeme $m_j \in \mathbb{R}[x]$ minimální polynom prvku α_j nad $\mathbb{R}$ a $(a_j, b_j, c_j) \in \mathbb{R}^3 \setminus \{(0,0,0)\}$ řešení rovnice $a_j\alpha_j + b_j\beta_j + c_j = 0$, pak $J_j = (m_j, ax + by + c)$ a $Y_j = \{(\alpha_j, \beta_j), (\overline{\alpha_j}, \overline{\beta_j})\}$.
(c) Jestliže $\alpha_j, \in \mathbb{R}$ a $\beta_j, \notin \mathbb{R}$, vezmeme $m_j \in \mathbb{R}[x]$ minimální polynom prvku β_j nad $\mathbb{R}$ a $(a_j, b_j, c_j) \in \mathbb{R}^3 \setminus \{(0,0,0)\}$ řešení rovnice $a_j\alpha_j + b_j\beta_j + c_j = 0$, pak opět $J_j = (m_j, ax + by + c)$ a $Y_j = \{(\alpha_j, \beta_j), (\overline{\alpha_j}, \overline{\beta_j})\}$.

Nyní stejnou úvahou jako v předchozím bodě zjistíme, že že $I(X) = \bigcap_j J_j$, $VI(X) = \bigcup_j Y_j$, kde Y_j jsou variety.

(3) Postupujeme analogicky předchozím úlohám. Nejprve označme

$$Y_1 = \{(1-i, 2+i, 1), (1+i, 2-i, 1)\} \quad \text{a} \quad Y_2 = \{(1, 2-i, 3+2i), (1, 2+i, 3-2i), \}.$$

Vezměme nejprve minimální polynomy $x^2 - 2x + 2$ prvku $1 - i$ a $y^2 - 4y + 5$ prvku $2 - i$ nad tělesem reálných čísel. Poté pro každou z nul najdeme dvě (netriviální) reálná lineárně nezávislá řešení rovnic

$$a(1-i) + b(2+i) + c(1) + d,$$

$$a(1) + b(2-i) + c(3+2i) + d.$$

Nyní vezmeme jim příslušné lineární polynomy a dostaneme tak generátory ideálů:

$$J_1 = (x^2 - 2x + 2, x + y - 3, z - 1), \quad J_2 = (y^2 - 4y + 5, x - 1, 2y + z - 7),$$

Konečně uvážíme dosazovací homomorfismy

$$\Omega_1 : \mathbb{R}[x, y, z] \to \mathbb{R}[x], \quad \Omega_2 : \mathbb{R}[x, y, z] \to \mathbb{R}[y]$$

dané vztahy

$$\Omega_1(f(x, y, z)) = f(x, 3 - x, 1), \quad \Omega_2(f(x, y, z)) = f(1, y, 7 - 2y)$$

a dvojici přirozených projekcí

$$\pi_1 : \mathbb{R}[x] \to \mathbb{R}[x]/(x^2 - 2x + 2), \quad \pi_2 : \mathbb{R}[y] \to \mathbb{R}[y]/(y^2 - 4y + 5)$$

na tělesa. Pak stejně jako v úloze 1.7 platí, že $J_j = \mathrm{Ker}\pi\Omega$ jsou maximální ideály a tedy stejně jako v předchozích dvou bodech $I(X) = J_1 \cap J_2$ $VI(X) = Y$ a $VI(X) = Y_1 \cup Y_2$ je rozklad algebraické množiny $VI(X)$ na variety. $\square$

9.cvičení (20.4.)

2. Algebraické množiny určené nad konečnými tělesy

2.1. Nechť T je komutativní těleso a n, d přirozená čísla a p prvočíslo. Dokažte, že jsou ekvivalentní následující tvrzení:

(a) d/n v $\mathbf{Z}$,
(b) $(q^d - 1)/(q^n - 1)$ v $\mathbf{Z}$.
(c) $(x^d - 1)/(x^n - 1)$ v $\mathbf{T}[x]$,

(a)$\to$(b) Jestliže $n = kd$, snadno spočítáme, že $p^n - 1 = (p^k - 1)\sum_{i=0}^{d-1} p^{ik}$.

(b)$\to$(a) Nechť $(p^k - 1)/(p^n - 1)$ a $n = kd + r$, kde $0 \leq r < k$. Víme, že

$$p^{kd} - 1 = (p^k - 1)\sum_{i=0}^{d-1} p^{ik} \quad \text{tedy} \quad (p^k - 1)/((p^n - 1) - (p^{kd} - 1)).$$

Protože $(p^n - 1) - (p^{kd} - 1) = p^{kd}(p^r - 1)$ a čísla $p^k - 1$ a p^{kd} jsou nesoudělná, máme $(p^k - 1)/(p^r - 1)$. Ovšem $r < k$, tudíž $r = 0$.

(a)$\leftrightarrow$(c) Použijeme obdobný argument jako v důkazu (a)$\leftrightarrow$(b). Uvážíme-li $n = kd + r$, kde $0 \leq r < k$, pak

$$x^n - 1 = x^r(x^{kd} - 1) + x^r - 1,$$

což znamená, že $d/n \quad \leftrightarrow \quad r = 0 \quad \leftrightarrow \quad (x^d - 1)/(x^r - 1) \quad \leftrightarrow \quad (x^d - 1)/(x^n - 1)$. $\square$

Uvážíme-li, že je konečné těleso $\mathbb{F}_{p^n}$ právě rozkladové nadtěleso polynomu $x^{p^n} - x$, je v tělese $\mathbb{F}_{p^n}$ podle předchozí úlohy (díky jednoznačnosti podgrup cyklické podgrupy jednoznačným způsobem) těleso $\mathbb{F}_{p^d}$ právě tehdy, když d/n. To vede k sérii následujícímu pozorování:

2.2. Nechť p je prvočíslo a $\mathbb{T} = \overline{\mathbb{F}_p}$ je algebraický uzávěr tělesa $\mathbb{F}_p$. Dokažte, že

(1) $\mathbb{T}$ obsahuje pro každé přirozené n právě jedno podtěleso izomorfní $\mathbb{F}_{p^n}$ (budeme ho značit rovněž $\mathbb{F}_{p^n}$),
(2) zobrazení, které $n \in \mathbb{N}$ přiřadí podtěleso $\mathbb{F}_{p^n}$ tělesa $\mathbb{T}$ je prostý homomorfismus svazů $(\mathbb{N}, /)$ a $(\{\mathbb{F}_{p^n} \subset \mathbb{T}\}, \subseteq)$,
(3) $\mathbb{T} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$,
(4) V $\mathbb{T}$ existuje systém nekonečných podtěles $(\mathbb{T}_j, j \in \mathbf{N})$ pro který platí $\mathbb{T}_i \cap \mathbb{T}_j = \mathbb{F}_p$, jestliže $i \neq j$.

(1) Existence i jednoznačnost plynou z toho, že všechny kořeny polynomu $x^{p^n} - x$, kterých je p^n určují právě těleso $\mathbb{F}_{p^n}$.

(2) Stačí připomenout, že $\mathbb{F}_{p^d}\mathbb{F}_{p^n}$, právě když d/n, tudíž pro všechna $n, m \in \mathbb{N}$

$$\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{\mathrm{NSD}(n,m)}}, \quad \langle \mathbb{F}_{p^n} \cup \mathbb{F}_{p^m} \rangle = \mathbb{F}_{p^{\mathrm{nsn}(n,m)}}.$$

(3) Inkluze $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n} \subseteq \mathbb{T}$ plyne z faktu, že v $\mathbb{T}$ musí ležet všechny kořeny polynomů $x^{p^n} - x$, naopak každý prvek $\mathbb{T}$ je algebraický nad $\mathbb{F}_p$, tudíž musí ležet v nějakém rozšíření konečného stupně $\mathbb{F}_{p^n}$.

(4) Stačí vzít $q_1 < q_2 < \dots$ libovolnou posloupnost prvočísel a pro každé i a n položit $t_{i,n} = p^{q_i^n}$ a položit $T_i = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{t_{i,n}}$. $\square$

2.3. Pro množinu X určete $I(X)$ $V(I(X))$ nad tělesem $\mathbb{F}_2$ a rozhodněte, zda je X a $V(I(X))$ varieta, jestliže $\alpha \in \overline{\mathbb{F}_2}$ je kořen polynomu $x^3 + x + 1$ a

(1) $X = V(x^3 + x + 1) \subseteq A^1(\overline{\mathbb{F}_2})$,
(2) $X = \{\alpha\} \subseteq A^1(\overline{\mathbb{F}_2})$,
(3) $X = \{(\alpha, \alpha^2 + 1)\} \subseteq A^2(\overline{\mathbb{F}_2})$

(1) Nejprve využijeme Frobeniova endomorfismu f_2, který permutuje kořeny polynomu s koeficienty v $\mathbb{F}_2$, proto

$$X = V(x^3 + x + 1) = \{\alpha, \alpha^2, \alpha^4\} = \{\alpha, \alpha^2, \alpha^2 + \alpha\},$$

neboť $0 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha$. Protože je polynom $x^3 + x + 1$ minimálním polynomem všech prvků z X nad tělesem $\mathbb{F}_2$, dostáváme $I(X) = (x^3 + x + 1)$ a $VI(X) =$

$(x^3+x+1) = \{\alpha, \alpha^2, \alpha^2+\alpha\}$. Protože je ideál $I(X) = (x^3+x+1)$ maximální v oboru $\mathbb{F}_2[x]$, je $X = VI(X)$ varieta.

(2) Protože $I(X) = (x^3+x+1)$, máme z předchozí úlohy $VI(X) = (x^3+x+1) = \{\alpha, \alpha^2, \alpha^2+\alpha\}$, tedy $VI(X)$ je varieta, zatímco X není algebraická množina.

10.cvičení (27.4.)

(3) Nyní postupujeme zcela analogicky úloze 1.7. Nejprve opět vezmeme minimální polynom x^3+x+1 prvku α nad tělesem $\mathbb{F}_2$ a dále uvážíme, že prvek α^2+1 je nad tělesem $\mathbb{F}_2$ lineárně závislý na bázi $B = \{1, \alpha, \alpha^2\}$ vektorového prostoru $F_{2^3} = \langle X \rangle$. Konkrétně snadno spočítáme, že

$$y(\alpha^2+1) = \alpha^2+1 = x^2+1(\alpha),$$

tedy prvek (α, α^2+1) je nulou polynomu $y+x^2+1$. Nyní vidíme, že To znamená, že

$$J = (x^3+x+1, y+x^2+1) \subseteq I(X).$$

Nyní potřebujeme opět dokázat, že je J maximální, k čemuž opět použijeme dosazovací homomorfismus $\Omega : \mathbb{R}[x,y] \to \mathbb{R}[x]$ daný vztahem $\Omega(f(x,y)) = f(x, x^2+1)$ a přirozenou projekci $\pi : \mathbb{R}[x] \to \mathbb{R}[x]/(x^3+x+1)$. I tentokrát se ukáže, že složení $\pi\Omega$ je homomorfismus na těleso $\mathbb{R}[x]/(x^3+x+1) \cong \mathbb{F}_8$ a $\ker \pi\Omega = J$ jeho jádro, tudíž maximální ideál. To znamená, že $I(X) = J$ a snadno dopočítáme, že

$$VI(X) = V(J) = \{(\alpha, \alpha^2+1), (\alpha^2, \alpha^4+1), (\alpha^2+\alpha, (\alpha^2+\alpha)^2+1)\} =$$
$$= \{(\alpha, \alpha^2+1), (\alpha^2, \alpha^2+\alpha+1), (\alpha^2+\alpha, \alpha+1)\}.$$

Protože $IVI(X) = I(X)$ je prvoideál, je $VI(X)$ varieta a X opět není algebraická množina. $\square$

3. Projektivní prostory

3.1. Pro afinní křivky $V = V_{afin}(f) \subseteq \mathbb{A}^2(\mathbb{C})$ určené nad $\mathbb{R}$ spočítejte jejich body v nekonečnu, tedy průniky $V^* \cap H_\infty$, jestliže:

(1) $f = y_1y_2 - 1$,
(2) $f = y_1^2 - y_2$,
(3) $f = y_2^2 - y_1(y_1^2 - 1)$,

(1) Víme, že platí $V^* = V_{proj}(f^*) = V_{proj}(X_1X_2 - X_0^2)$ a že $H_\infty = V_{proj}(X_0)$, proto

$$V^* \cap H_\infty = V_{proj}(X_1X_2 - X_0^2, X_0) = V_{proj}(X_1X_2, X_0) = \{(0:1:0), (0:0:1)\}$$

(2) Nyní $V^* = V_{proj}(f^*) = V_{proj}(X_1^2 - X_0X_1)$ tedy

$$V^* \cap H_\infty = V_{proj}(X_1^2 - X_0X_1, X_0) = V_{proj}(X_1^2, X_0) = \{(0:1:0)\}$$

(3) Konečně $V^* = V_{proj}(f^*) = V_{proj}(X_2^2X_0 - X_1(X_1^2 - X_0^2))$ tedy

$$V^* \cap H_\infty = V_{proj}(X_2^2X_0 - X_1(X_1^2 - X_0^2), X_0) = V_{proj}(X_1^3, X_0) = \{(0:1:0)\}$$

$\square$

3.2. Nechť $S = \{y_1y_2 - 1, y_2^2 - 1\} \subseteq \mathbb{R}[y_1, y_2]$, ukažte, že $(V_{afin})^* \neq V_{proj}(\{f^* | \ f \in S\})$.

Snadno spočteme $V_{afin} = \{(1,1), (-1,-1)\}$. A protože

$$\varphi_0(V_{afin}) = \{(1:1:1), (1:-1:-1)\} = V_{proj}(x_1 - x_0, x_2 - x_0) \cup V_{proj}(x_1 + x_0, x_2 + x_0)$$

je projektivní množina dostáváme $(V_{afin})^* = \{(1:1:1),(1:-1:-1)\}$. Zbývá si uvědomit, že $V_{proj}(\{(y_1y_2-1)^*,(y_2^2-1)^*\}) =$

$$= V_{proj}(\{X_1X_2 - X_0, X_2^2 - X_0\}) = \{(1:1:1),(1:-1:-1),(0:1:0)\}.$$

□

3.3. Uvažujme polynomy $f, g \in \mathbb{C}[y_1, y_2, y_3]$, $f = y_1^2 - y_2$, $g = y_1^3 - y_3$. Připomeňme, že jsme v domácím úkolu ukázali, že $I_{afin}V_{afin}(f,g) = (f,g)$. Jestliže $U = V_{afin}(f,g)$, ověřte, že

(1) $X_3X_0 - X_1X_2 \in I_{proj}(U^*) = (f,g)^* \subseteq \mathbb{C}[X_0, X_1, X_2, X_3]$,
(2) $X_3X_0 - X_1X_2 \notin (f^*, g^*) \subseteq \mathbb{C}[X_0, X_1, X_2, X_3]$.

(1) Zřejmě $(y_1f - g)^* = (y_3 - x_1x_2)^* = X_3X_0 - X_1X_2$.

(2) Stačí prozkoumat obraz ideálu $K = (f^*, g^*) = (X_1^2 - X_2X_0, X_1^3 - X_3X_0^2)$ ve faktorovém okruhu $\mathbb{C}[X_0, X_1, X_2, X_3]/L$, kde $\mathcal{L} = (X_0^iX_1^jX_2^kX_3^l \mid i+j+k+l = 3)$. Potom $\mathcal{K} + \mathcal{L}/\mathcal{L} = (X_1^2 - X_2X_0) + L/L$ má strukturu jednodimenzionálního vektorového prostoru nad tělesem $\mathbb{C}$ a zřejmě $(X_3X_0 - X_1X_2) + \mathcal{L} \notin (X_1^2 - X_2X_0) + \mathcal{L}/\mathcal{L}$, proto $X_3X_0 - X_1X_2 \notin \mathcal{K}$. □