Úvod do komutativní algebry: cvičení 6

21. prosince 2023

1. Rozhodni, které z následujících množin jsou algebraické:

a) $\{(t, t^2, t^3) \in K^3 \mid t \in K\}$,
b) $\{(\cos t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$,
c) $\mathbb{Z}$ jako podmnožina $\mathbb{R}$,
d) * $\mathbb{Z}^2$ jako podmnožina $\mathbb{R}^2$,
e) * $\{(t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$.

Řešení. Všude nechť X značí zadanou množinu.

a) Tvrdím $X = V(x^2 - y, x^3 - z)$, což dosvědčí, že X je algebraická. Dokažme dvě inkluze. Každý bod tvaru (t, t^2, t^3) bude nulou obou dvou polynomů, protože

$$(t)^2 - (t^2) = 0, \qquad (t)^3 - (t^3) = 0,$$

tedy $X \subset (x^2-y, x^3-z)$. Pro opačnou inkluzi, ať v $(a, b, c) \in K^3$ nabývají nuly oba polynomy $x^2 - y$, $x^3 - z$. To značí, že

$$b = a^2, \qquad c = a^3,$$

označíme-li tedy $t := a$, pak už bude $(a, b, c) = (t, t^2, t^3) \in X$, čímž je dokázáno $X = V(x^2 - y, x^3 - z)$.

b) $X = V(x^2 + y^2 - 1)$, tedy je to algebraická množina. Inkluze $\subset$ je jasná z Pythagorejské rovnosti $(\cos t)^2 + (\sin t)^2 = 1$. Pro opačnou inkluzi, ať $(a, b) \in \mathbb{R}^2$ splňuje $a^2 + b^2 - 1 = 0$, potom

$$1 = a^2 + b^2 \geq a^2,$$

tedy $|a| \leq 1$. Tedy a leží v obrazu funkce $\cos : \mathbb{R} \to [-1, 1]$, existuje proto $t \in \mathbb{R}$ takové, že $a = \cos t$. Pak platí

$$a^2 + (\sin t)^2 = (\cos t)^2 + (\sin t)^2 = 1,$$

porovnáním rovností tak $b^2 = (\sin t)^2$. Nyní pokud $b = \sin t$, pak $(a, b) = (\cos t, \sin t) \in X$, naopak když $b = -\sin t$, potom $(a, b) = (\cos(-t), \sin(-t)) \in X$. Tím je dohromady dokázáno i $V(x^2 + y^2 - 1) \subset X$.

c) Není algebraická. Pro spor ať $X = \mathbb{Z} = V(I)$ pro nějaký ideál $I \leq \mathbb{R}[x]$. Kdyby $I = (0)$, pak $V(I) = \mathbb{R} \neq \mathbb{Z}$. Tedy I obsahuje nějaký nenulový polynom f. Prvky $V(I)$ pak musí být jeho kořeny (ne nutně všechny kořeny, máme jen inkluzi), ale nenulový polynom má jen konečně mnoho kořenů, tedy $V(I) \subset V(f)$ je konečná, což ale $\mathbb{Z}$ není, tedy spor.

d) X není algebraická. Pokud by byla, muselo by $V(I(X)) = X$, stačí tedy ukázat $V(I(X)) \supsetneq X$. Ať je $f(x, y) \in I(X)$. Uvažme polynom $f(x, 0) \in \mathbb{R}[x]$ vzniklý dosazením nuly za y a ponecháním x jako neznámé. Tento polynom má míti nulovou hodnotu v každém celém čísle, tedy má mít nekonečně mnoho kořenů. Ale jediným polynomem jedné proměnné s nekonečně mnoha kořeny je nulový polynom, tedy $f(x, 0) = 0 \in \mathbb{R}[x]$. To už ale značí, že f se nuluje na celé přímce $\mathbb{R} \times \{0\}$. Toto jsme provedli pro libovolné $f \in I(X)$, tedy $\mathbb{R} \times \{0\} \subset V(I(X))$, což už implikuje $V(I(X)) \supsetneq X$, jak jsme chtěli. (Opakovaným použitím téže myšlenky bychom dokonce mohli dokázat $I(X) = (0)$.)

e) X není algebraická, lze dokázat podobně jako d). Ve zkratce, uvážením $f(x, b)$ pro konstanty $b \in [-1, 1]$ zjistíme, že cokoliv z $I(X)$ už by se nulovalo na celém $\mathbb{R} \times [-1, 1]$, což dá spor s algebraičností. (Podobné úvahy lze vést dále a ukázat, že ve skutečnosti $I(X) = (0)$.)

2. (protipříklad Hilbertovy věty bez algebraické uzavřenosti) Najdi v $\mathbb{R}[x]$ maximální ideál, který neobsahuje žádný lineární polynom.

Řešení. Funguje třeba $(x^2 + 1)$: faktorokruh je $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$, což je těleso, takže je to maximální ideál. Lineární polynom však neobsahuje, protože (nenulový) násobek kvadratického polynomu bude mít stupeň ≥ 2.

3. *Jacobsonův radikál* okruhu R definujeme jako $\mathcal{J}(R) := \bigcap_{M<R \text{ maximální}} M$. Nahlédni, že $a \in \mathcal{J}(R)$, právě když je $1 - ar$ jednotka pro každé $r \in R$.

Řešení. Zaprvé buď $a \in \mathcal{J}(R)$ a $r \in R$ libovolné a dokažme, že $1 - ar$ je jednotka. Pro spor ať $1 - ar$ není jednotka, to znamená, že $(1 - ar)$ je vlastní ideál v R. Každý vlastní ideál je obsažen v nějakém maximálním, mějme tedy $(1 - ar) \subseteq M < R$ pro M maximální ideál. Pak ale $1 - ar \in M$ a zároveň $a \in \mathcal{J}(R) \subset M$, v důsledku tedy i $1 = (1 - ar) + r \cdot a \in M$, což je spor. Tudíž $1 - ar$ musela být jednotka.

Za druhé buď $1 - ar$ jednotkou pro všechna r a dokažme, že $a \in \mathcal{J}(R) = \bigcap_{M \text{ maximální}} M$. Pro spor ať tomu tak není, tedy existuje maximální ideál M takový, že $a \notin M$. To znamená $a + M \neq 0 + M$ ve faktorokruhu R/M, což je maximalitou M těleso. Pak existuje $b + M \in R/M$ splňující $(a + M)(b + M) = 1 + M$, neboli pro kterýkoliv reprezentant $b \in R$ je $1 - ab \in M$. To už ale značí, že při volbě $r := b$ nebude $1 - ab$ jednotkou, protože $(1 - ab) \subsetneq R$.

4. Urči v oboru celých čísel $\mathbb{Z}$

a) $\sqrt{(0)}$, $\mathcal{J}(\mathbb{Z})$,
b) $\sqrt{(25)}$, $\sqrt{(125)}$, $\sqrt{(50)}$, $\sqrt{(100)}$, $\sqrt{(\prod_i p_i^{r_i})}$ pro po dvou různá prvočísla p_i.

Dále urči

c) $\mathcal{J}(\mathbb{Z}/(100))$,
d) * kdy je $(\mathbb{Z}/(n))/\mathcal{J}(\mathbb{Z}/(n)$ těleso.

Řešení.

a) (0) (protože $\mathbb{Z}$ je obor, určitě tedy nemá jiné nilpotentní prvky než 0 samotnou), (0) (nenulové číslo nemůže být dělitelné všemi prvočísly),
b) (5), (5), (10), (10), $(\prod_i p_i)$. Stačí dokázat poslední, obecný tvar: pokud $r := \max r_i$, pak $(\prod_i p_i)^r \in (\prod_i p_i^{r_i})$, tedy $(\prod_i p_i) \subset \sqrt{(\prod_i p_i^{r_i})}$ naopak ale pro $a^n \in \sqrt{(\prod_i p_i^{r_i})}$ nutně musí být $p_i \mid a^n$, tedy $p_i \mid a$ pro všechna i, tedy už $a \in (\prod_i p_i)$.
c) (10)/(100), protože $\mathbb{Z}/(100)$ má jako jediné maximální ideály (2)/(100) a (5)/(100).
d) Je to přesně pro $n = p^k$, p prvočíslo, $k \geq 1$. Aby se jednalo o těleso, má $\mathcal{J}(\mathbb{Z}/(n))$ být maximální ideál v $\mathbb{Z}/(n)$, tedy zde musí existovat právě jeden maximální ideál (protože průnik dvou či více maximálních ideálů už nemůže být maximální). Maximální ideály v $\mathbb{Z}/(n)$ odpovídají maximálním ideálům v $\mathbb{Z}$ obsahujícím (n), tedy prvočíslům dělícím n, takže přesně potřebujeme, aby bylo n násobkem pouze jednoho prvočísla.

5. V oboru $\mathbb{C}[x]$ polynomů nad komplexními čísly

a) spočítej $\sqrt{(0)}$, $\mathcal{J}(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6 - x^4 - x^2 + 1)}$,
b) dokaž, že $\sqrt{(p)} = (\frac{p}{\text{NSD}(p,p')})$, kde $p \in \mathbb{C}[x]$.

Řešení. $\mathbb{C}[x]$ je obor hlavních ideálů stejně jako $\mathbb{Z}$, úplně stejně tedy platí $\sqrt{(\prod_i g_i^{e_i})} = (\prod_i g_i)$ pro g_i navzájem neasociované ireducibilní polynomy.

a) Jsme v oboru ideálů, takže $\sqrt{(0)} = (0)$. Polynomy tvaru $x - c$ jsou určitě ireducibilní, takže $(x-c)$ je maximální ideál, takže každý prvek $\mathcal{J}(\mathbb{C}[x])$ musí mít za kořeny všechna komplexní čísla – může to tedy být jen nulový polynom, protože nenulový polynom jedné proměnné má jen konečně mnoho kořenů. Tedy $\mathcal{J}(\mathbb{C}[x]) = (0)$. Konečně skrze ireducibilní rozklad určíme

$$\begin{aligned}
\sqrt{(x-3)^5(x-1)^4(x^3+2)} &= \sqrt{(x-3)^5(x-1)^4(x+\sqrt[3]{2})(x+e^{2\pi i/3}\sqrt[3]{2})(x+e^{4\pi i/3}\sqrt[3]{2})} = \\
&= \left((x-3)(x-1)(x+\sqrt[3]{2})(x+e^{2\pi i/3}\sqrt[3]{2})(x+e^{4\pi i/3}\sqrt[3]{2})\right) = \\
&= \left((x-3)(x-1)(x^3+2)\right), \\
\sqrt{(x^6 - x^4 - x^2 + 1)} &= \sqrt{(x^2-1)(x^4-1)} = \sqrt{(x-1)^2(x+1)^2(x-i)(x+i)} = \\
&= ((x-1)(x+1)(x-i)(x+i)) = (x^4-1).
\end{aligned}$$

b) Ať je $p = \prod_i g_i^{e_i}$ rozklad na ireducibilní polynomy pro $p \neq 0$ (pro nulový polynom se tvrzení přímočaře ověří), pak víme $\sqrt{(p)} = (\prod_i g_i)$. Stačí tedy dokázat

$$\mathrm{NSD}(p, p') = \prod_i g_i^{e_i - 1}.$$

Zjevně musí $\mathrm{NSD}(p, p')$ dělit p, proto víme, že v rozkladu stačí uvažovat ireducibilní polynomy g_i, ne žádné další; zbývá tedy ukázat, že každý se vyskytne s exponentem $e_i - 1$. Zvolme pevně jedno i a označme $h := \frac{p}{g_i^{e_i}}$. Potom Leibnizovým pravidlem

$$p' = (g_i^{e_i} h) = (g_i^{e_i})' h + g_i^{e_i} h' = e_i g_i^{e_i - 1} h + g_i^{e_i} h' = g_i^{e_i - 1} \left(e_i h + g_i h'\right).$$

Derivace je tedy dělitelná g_i v $(e_i - 1)$-té mocnině, ale nikoliv v e_i-té, protože to by znamenalo $g_i \mid e_i h + g_i h'$, tudíž $g_i \mid e_i h$, což neplatí, protože e_i je konstanta a h je součinem samých ireducibilních polynomů neasociovaných s g_i. Tímto je důkaz hotov.

6. Pracujme nad $K = \mathbb{C}$:

a) Dokaž, že $I(V(x^2 - y)) = (x^2 - y)$ a že algebraická množina $V(x^2 - y) \subset \mathbb{C}^2$ je ireducibilní.
b) Urči množinu $V(y^4 - x^2, y^4 - x^2 y^2 + x y^2 - x^3) \subset \mathbb{C}^2$ a rozlož ji na ireducibilní komponenty.
c) * Rozlož $V(x^2 + y^2 - 1, x^2 - z^2 - 1) \subset \mathbb{C}^3$ na ireducibilní komponenty.

Řešení.

a) Analogicky s úlohou 1a) lze dokázat, že $V(x^2 - y) = \{(t, t^2) \mid t \in \mathbb{C}\}$. Dokažme, že pokud se nějaký polynom $f \in \mathbb{C}[x, y]$ nuluje na celé této množině, pak je to násobek $x^2 - y$. Uvažujme $\tilde{f} := f(x, x^2) \in \mathbb{C}[x]$. Potom platí $\tilde{f}(t) = f(t, t^2)$, takže pokud $f \in I(V(x^2 - y))$, pak $\tilde{f}(t) = 0$. To znamená, že $\tilde{f}$ je polynom jedné proměnné, který má nekonečně mnoho kořenů, takovým je ale jen $\tilde{f} = 0$. Tím tedy víme $f(x, x^2) = 0$, na což můžeme nahlížet tak, že x^2 je kořenem $f \in (\mathbb{C}[x])[y]$, takže můžeme vytknout kořenový dvojčlen $y - x^2$:

$$f = (y - x^2) \cdot f_0 \qquad \text{pro nějaké } f_0 \in (\mathbb{C}[x])[y] = \mathbb{C}[x, y].$$

To už přesně znamená, že $f \in (x^2 - y)$, tedy jsme dokázali inkluzi $I(V(x^2 - y)) \subseteq (x^2 - y)$. Opačná inkluze je triviální, takže máme dokázánu rovnost.
Nyní ukažme ireducibilitu $V(x^2 - y)$. K tomu nechť $V(x^2 - y) = A \cup B$ pro nějaké algebraické množiny A, B a dokažme, že nutně jedna z A, B je rovna $V(x^2 - y)$. Víme, že $V(x^2 - y) = \{(t, t^2) \mid t \in \mathbb{C}\}$ je nekonečná množina, takže alespoň jedna z A, B je nekonečná, BÚNO ať je to A. Potom ale nutně $I(A) \subseteq (x^2 - y)$ skrze analogický důkaz k předchozímu odstavci: tam jsme jako kořeny t polynomu $\tilde{f}$ mohli brát všechna komplexní čísla, ale bohatě nám stačilo, že *nějakých nekonečně mnoho* komplexních čísel jsou kořeny. Každý bod v A je tvaru (t, t^2) a takové t bude kořenem $\tilde{f}$ pro každé $f \in I(A)$, takže opět budeme mít $I(A) \subseteq (x^2 - y)$. Aplikováním V na inkluzi $I(A) \subseteq (x^2 - y)$ dostaneme

$$V(x^2 - y) \subseteq V(I(A)) = A$$

(využíváme toho, že V obrací inkluze a že $V(I(A)) = A$ pro algebraickou množinu A), takže už nutně $V(x^2 - y) = A$, jak jsme chtěli dokázat. Tedy $V(x^2 - y)$ je ireducibilní.

b) Zde prostě řešíme soustavu polynomálních rovnic

$$\begin{aligned} y^4 - x^2 &= 0, \\ y^4 - x^2 y^2 + x y^2 - x^3 &= 0 \end{aligned}$$

nad $\mathbb{C}$. První rovnice se faktorizuje na $(y^2 - x)(y^2 + x) = 0$, takže stačí zvlášť řešit případy $y^2 \mp x = 0$. V těch můžeme pomocí $y^2 = \pm x$ zjednodušovat druhou rovnici na

$$\begin{aligned} (\pm x)^2 - x^2(\pm x) + x(\pm x) - x^3 &= 0, \\ x^2(1 \mp x \pm 1 - x) &= 0, \\ x^2(1 - x)(1 \pm 1) &= 0. \end{aligned}$$

Zde už je vidět, že pro $\pm = +$ řešíme $2x^2(1-x) = 0$, což má (dvojnásobný) kořen 0 a dále kořen 1. Naproti tomu pro $\pm = -1$ se celá rovnice trivializuje, což znamená, že každá dvojice (x, y) splňující $y^2 = -x$ je řešením druhé rovnice. Z prvního případu tak máme konečně mnoho řešení, zatímco z druhého celou křivku nulových bodů. Dohromady:

$$V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) = \{(0,0), (1,1), (1,-1)\} \cup V(y^2 + x).$$

Jednobodové množiny jsou vždy algebraické a ireducibilní, zatímco $V(y^2+x) = \{(-t^2, t) \mid t \in \mathbb{C}\}$ je ireducibilní (lze dokázat podobně jako v podúloze a)), takže máme ireducibilní rozklad

$$V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) = \{(0,0)\} \cup \{(1,1)\} \cup \{(1,-1)\} \cup V(x^2 + y).$$

7. Je-li K konečné těleso, pak je každá podmnožina v K^n algebraická.

Řešení. Jednobodové množiny jsou algebraické, protože

$$\{(a_1, \ldots, a_n)\} = V(x_1 - a_1, \ldots, x_n - a_n).$$

Dále víme, že sjednocení dvou algebraických množin je algebraická množina, protože $V(IJ) = V(I) \cup V(J)$. Snadnou indukcí z toho plyne, že libovolné sjednocení konečně mnoha algebraických množin je opět algebraická množina. Pokud se tedy pohybujeme nad konečným tělesem K, pak pro libovolnou neprázdnou $A \subseteq K^n$ máme

$$A \;=\; \bigcup_{(a_1,\ldots,a_n)\in A} \{(a_1, \ldots, a_n)\},$$

což je konečné sjednocení algebraických množin, čili algebraická množina. (Prázdná množina je také algebraická skrze $\emptyset = V(1)$.)

8. Nahlédni, že pro ideál $I < R$ je $\sqrt{I}$ roven $\pi^{-1}(\sqrt{0/I})$, kde $\pi : R \twoheadrightarrow R/I$ je přirozená projekce.

Řešení. $a^n \in I \iff \pi(a)^n = 0$.

9. Buď K nekonečné těleso a $V = \{(t, t^2, t^3, \ldots, t^n) \mid t \in K\} \subset K^n$. Urči $I(V)$ (s důkazem!) a na základě úlohy z DÚ (V ireducibilní $\iff$ $I(V)$ prvoideál) vyvoď, že V je ireducibilní.

Řešení. (náznak) Platí $I(V) = (x_1^k - x_k \mid x = 2, \ldots, n) =: P$, což je prvoideál, protože $K[x_1, \ldots, x_n]/P \simeq K[x_1]$ je obor integrity (izomorfismus je $f \mapsto f(x_1, x_1^2, \ldots, x_1^n)$). Skrz ekvivalenci z domácího úkolu tedy vidíme, že V je ireducibilní množina.

10. Rozmysli si následující charakterizace ideálů pomocí faktorokruhů: $I < R$ je

- maximální, právě když jsou všechny nenulové prvky R/I invertibilní,
- prvoideál, právě když je součin nenulových prvků v R/I vždy nenulový,
- radikálový, právě když je mocnina nenulového prvku v R/I vždy nenulová.

Řešení. První dvě odrážky říkají jen věci, které už známe: I je maximální, právě když je R/I těleso, resp. I je prvoideál, právě když je R/I obor integrity.

I je radikálový, právě když $\sqrt{I} = I$, tedy když $(\exists n)(a^n \in I) \iff a \in I$. Když totéž přeformulujeme ve faktor okruhu, tak chceme, aby pro libovolné $a + I \in R/I$ platilo, že

$$(\exists n)((a+I)^n = 0 + I) \iff a + I = 0 + I.$$

To ale přesně říká, že mocnina může být nulová pouze tehdy, když už její základ byl nulový, tedy že mocnina nenulového prvku v R/I už je nenulová.

11. Dokaž, že $f(x, y) = y^2 + x^2(x-1)^2 \in \mathbb{R}[x, y]$ je ireducibilní polynom, ale množina $V(f) \subset \mathbb{R}^2$ je reducibilní.

Řešení. V $\mathbb{R}$ jsou druhé mocniny nezáporné, tudíž pro $(a,b) \in \mathbb{R}^2$ nastane $f(a,b) = 0$ právě tehdy, když $b = 0$ a zároveň $a(a-1) = 0$, tedy $V(f) = \{(0,0),(1,0)\}$, což je zjevně reducibilní množina.

Naproti tomu f je ireducibilní: pro spor at není, pak se rozkládá na $f = gh$, kde g i h jsou nekonstantní. Vzhledem k $\deg_y(f) = 2$ by pak BÚNO g mělo $\deg_y(g) \leq 1$. Díváme-li se na f jako na prvek $\mathbb{R}[x][y]$, pak má vedoucí koeficient jedna, tedy $\deg_y(g) = 0$ by znamenalo $g \mid 1$, tedy g je konstantní, což je spor.

Tedy musíme mít $\deg_y(g) = \deg_y(h) = 1$. Přitom f je ve smyslu $f \in \mathbb{R}[x][y]$ monický, tedy i g, h musí být monické, neboli

$$g = y + g_0, \qquad\qquad h = y + h_0$$

pro nějaká $g_0, h_0 \in \mathbb{R}[x]$. Pak už nám porovnání koeficientů v

$$y^2 + x^2(x-1)^2 = f = (y+g_0)(y+h_0) = y^2 + (g_0+h_0)y + g_0h_0$$

dá $h_0 = -g_0$ a následně $(x(x-1))^2 = g_0h_0 = -g_0^2$. Je-li nyní $a \in \mathbb{R}$ vedoucí koeficient g_0, pak máme vzetím vedoucích koeficientů na obou stranách $1 = -a^2$, což zjevně reálné číslo nemůže splnit.

Tedy dohromady je f ireducibilní, jak jsme chtěli.