ZARISKÉHO LEMMA POMOCÍ ARTIN-TATEOVA LEMMATU

JAN ŠŤOVÍČEK

1. Zariského lemma

Cílem tohoto textu je dokázat klíčové algebraické tvrzení, které stojí za Hilbertovou větou o nulách, a sice tzv. Zariského lemma (ve skriptech jako [1, tvrzení 3.13]:

Tvrzení 1.1 (Zariského lemma)**.** *Buď $K \subset L$ okruhově konečné rozšíření těles. Pak je $K \subset L$ dokonce modulově konečné rozšíření, jinými slovy $[L : K] < \infty$.*

Zde prezentovaný důkaz je jiný než ve skriptech [1], využívá tzv. Artinovo-Tateovo lemma. Terminologie je také trochu jiná než ve skriptech, proto ji vysvětlíme.

Definice 1.2. Buď $R \subset S$ rozšíření okruhů (v tomto textu vždy komutativních s jednotkou). Řekneme, že rozšíření je

(1) *okruhově konečné*, pokud existuje $n \geq 1$ a prvky $a_1, \ldots, a_n \in S$ takové, že $S = R[a_1, \ldots, a_n]$;
(2) *modulově konečné*, pokud S je konečně generované jako R-modul, tj. existuje $n \geq 1$ a prvky $a_1, \ldots, a_n \in S$ takové, že $S = Ra_1 + \cdots + Ra_n$.

Poznámka 1.3.

(1) Z definice je vidět, že každé modulově konečné rozšíření je nutně okruhově konečné.
(2) Naopak to obecně neplatí. Je-li K těleso a $n \geq 1$, pak $K \subset K[x_1, \ldots, x_n]$ je okruhově konečné rozšíření, ale není modulově konečné.
(3) Z [1, tvrzení 2.1] plyne, že okruhově konečné rozšíření oborů je celistvé rozšíření.

2. Noetherovské okruhy a moduly

Než se pustíme do důkazu, rozebereme si některé základní vlastnosti noetherovských okruhů a modulů, které ve skriptech [1] výslovně uvedeny nejsou.

Lemma 2.1. *Buď $R \subset S$ okruhově konečné rozšíření okruhů takové, že R je noetherovský. Pak je S také noetherovský.*

Důkaz. Zvolme $a_1, \ldots, a_n \in S$ tak, aby $S = R[a_1, \ldots, a_n]$, a uvažujme dosazovací homomorfismus

$$\begin{aligned} \varphi\colon R[x_1, \ldots, x_n] &\longrightarrow S, \\ f &\longmapsto f(a_1, \ldots, a_n). \end{aligned}$$

Obraz φ je rovný $R[a_1, \ldots, a_n]$, tedy φ je na. Podle první věty o isomorfismu máme $R[x_1, \ldots, x_n]/\operatorname{Ker}\varphi \simeq S$. Jelikož $R[x_1, \ldots, x_n]$ je noetherovský podle Hilbertovy věty o bázi (konkrétně [1, důsledku 1.12]) a S je isomorfní faktorokruhu $R[x_1, \ldots, x_n]$, je i S noetherovský. □

Dále potřebujeme dvě fakta o noetherovských modulech. První je ze cvičení:

Date: 9. prosince 2021.

Tvrzení 2.2. *Buď R okruh a uvažujme R-modul M a jeho podmodul $N \subset M$. Pak M je noetherovský R-modul, právě když jsou N i M/N zároveň noetherovské.*

Důkaz. Je-li M noetherovský, noetherovskost N a M/N se nahlédne snadno přímo z definice nebo z [1, tvrzení 1.10]. Detaily přenecháváme jako cvičení.

Zaměříme se na opačnou implikaci a budeme předpokládat, že N i M/N jsou noetherovské. Podle [1, tvrzení 1.10] máme ukázat, že každý R-podmodul $L \subset M$ je konečně generovaný. Z předpokladu jsou ale podmoduly

$$L \cap N \subset N \qquad \text{a} \qquad (L+N)/N \subset M/N$$

konečně generované. Navíc podle třetí věty o isomorfismu pro moduly (která se dokáže tak, že se použije první věta o isomorfismu na $\pi|_L \colon L \to M/N$, kde $\pi \colon M \to M/N$ je kanonická projekce) máme isomorfismus R-modulů daný předpisem

$$\begin{aligned} L/(L\cap N) &\xrightarrow{\sim} (L+N)/N, \\ \ell + (L\cap N) &\longmapsto \ell + N. \end{aligned}$$

Speciálně i $L/(L \cap N)$ je konečně generovaný R-modul.

Můžeme tedy zvolit konečnou posloupnost $a_1, \dots, a_n$ generátorů $L \cap N$ a konečnou posloupnost $b_1 + (L \cap N), \dots, b_m + (L \cap N)$ generátorů $L/(L \cap N)$. Teď už stačí ověřit, že $a_1, \dots, a_n, b_1, \dots, b_m$ generuje L (pak bude L konečně generovaný, jak jsme chtěli). Zvolíme-li $\ell \in L$ libovolné, pak existují $r_1, \dots r_m \in R$ takové, že

$$\ell + (L \cap N) = (r_1 b_1 + \dots + r_m b_m) + (L \cap N),$$

aneb $\ell - (r_1 b_1 + \dots + r_m b_m) \in L \cap N$. Dále víme, že existují $\tilde{r}_1, \dots \tilde{r}_n \in R$ takové, že

$$\ell - (r_1 b_1 + \dots + r_m b_m) = \tilde{r}_1 a_1 + \dots + \tilde{r}_n a_n.$$

Jinými slovy, $\ell = \tilde{r}_1 a_1 + \dots + \tilde{r}_n a_n + r_1 b_1 + \dots + r_m b_m$. □

Druhým faktem je klasickým důsledkem předchozího.

Důsledek 2.3. *Konečně generovaný R-modul nad noetherovským okruhem R je noetherovský modul.*

Důkaz. Buď R noetherovský okruh a $M = Rm_1 + \dots + Rm_{n-1} + Rm_n$ konečně generovaný R-modul. Ukážeme, že M je noetherovský, indukcí podle počtu generátorů n.

Případ $n = 1$. Máme $M = Rm_1$ a snadno ověříme, že zobrazení

$$\begin{aligned} \pi \colon R &\longrightarrow M, \\ r &\longmapsto r m_1 \end{aligned}$$

je surjektivní homomorfismus R-modulů. Podle první věty o isomorfismu máme isomorfismus R-modulů $M \simeq R/\operatorname{Ker}\pi$. Jelikož R je noetherovský jakožto modul sám nad sebou, je noetherovský i M.

Buď nyní $n > 1$. Z indukčního předpokladu je $N = Rm_1 + \dots + Rm_{n-1}$ noetherovský a jednoduše M/N je generovaný jediným prvkem $m_n + N$. Tedy M/N je také noetherovský podle předchozího odstavce a použijeme tvrzení 2.2. □

3. Artinovo-Tateovo lemma

Artinovo-Tateovo lemma je technické tvrzení, pomocí kterého už půjde důkaz tvrzení 1.1 jednoduše provést. Říká následující:

Tvrzení 3.1 (Artinovo-Tateovo lemma)**.** *Buď R noetherovský okruh a uvažujme jeho rozšíření $R \subset S \subset T$. Pokud je*

(1) *rozšíření $R \subset T$ okruhově konečné a*
(2) *rozšíření $S \subset T$ modulově konečné,*

pak je rozšíření $R \subset S$ okruhově konečné.

Důkaz. Nejprve najdeme *noetherovský* okruh S_0 takový, že $R \subset S_0 \subset S$ a rozšíření $S_0 \subset T$ je stále modulově konečné. K tomu zvolíme

(1) prvky $a_1, \dots, a_n \in T$ takové, že $T = R[a_1, \dots, a_n]$ (to můžeme, protože T je okruhově konečné rozšíření R) a
(2) prvky $t_1, \dots, t_m \in T$ takové, že $T = St_1 + \cdots + St_m$ (to můžeme, protože T je modulově konečné rozšíření S).

Navíc můžeme bez újmy na obecnosti předpokládat, že $a_1 = 1$ (jinak si jednotku mezi prvky a_i prostě přidáme). Dále si pak můžeme zvolit prvky $s_{ij} \in S$ (kde $1 \le i \le n$ a $1 \le j \le m$) a $\tilde{s}_{ijk} \in S$ (kde $1 \le i, j, k \le m$) takové, že

$$a_i = s_{i1}t_1 + \cdots + s_{im}t_m,$$
$$t_i t_j = \tilde{s}_{ij1}t_1 + \cdots + \tilde{s}_{ijm}t_m.$$

Za S_0 zvolíme nejmenší podokruh S obsahující R a všechny prvky s_{ij} a $\tilde{s}_{ijk}$, tj. $S_0 = R[s_{ij}, \tilde{s}_{ijk}]$. Podle lemmatu 2.1 je S_0 noetherovský, a musíme tedy ještě ukázat, že T je modulově konečné rozšíření S_0. Nejprve si všimneme, že množina $S_0t_1 + \cdots + S_0t_m$ je vlastně podokruhem T. Tato množina totiž zcela jistě obsahuje 0 a je v T uzavřená na sčítání a odčítání, obsahuje i jednotku (zvolili jsme $a_1 = 1$) a je uzavřená na násobení, protože pro všechna $c_1, \dots, c_m, d_1, \dots, d_m \in S_0$ platí

$$\Big(\sum_{i=1}^{m} c_i t_i\Big) \cdot \Big(\sum_{j=1}^{n} d_j t_j\Big) = \sum_{i,j=1}^{m} (c_i d_i)(t_i t_j) = \sum_{i,j,k=1}^{m} (c_i d_i \tilde{s}_{ijk}) t_k \in S_0t_1 + \cdots + S_0t_m.$$

Jelikož ale $S_0t_1 + \cdots + S_0t_m$ obsahuje R i všechny prvky $a_1, \dots, a_n$, máme $T = R[a_1, \dots, a_n] \subset S_0t_1 + \cdots + S_0t_m$. Tedy $T = S_0t_1 + \cdots + S_0t_m$ je modulově konečné rozšíření S_0, což jsme chtěli ukázat.

Nakonec pak z toho, že S je S_0-podmodul konečně generovaného S_0-modulu T a že S_0 je noetherovský okruh, pomocí důsledku 2.3 dostaneme, že S je také konečně generovaný S_0-modul. Existuje proto $p \ge 0$ a prvky $v_1, \dots, v_p \in S$ takové, že

$$S = S_0v_1 + \cdots + S_0v_p.$$

Z toho, že S je sám o sobě podokruh T, dostaneme rovnosti

$$S = S_0[v_1, \dots, v_p] = R[s_{ij}, \tilde{s}_{ijk}, v_i].$$

Čili S je okruhově konečné rozšíření R, jak bylo dokázati. □

4. Důkaz Zariského lemmatu

Teď už máme vše připraveno k důkazu tvrzení 1.1. Pro úplnost ještě připomeneme jedno lemma ze skript (vlastně nám stačí jen jeho speciální případ):

Lemma 4.1 ([1, lemma 3.11])**.** *Je-li K těleso, pak $K \subset K(x)$ (kde $K(x)$ je podílové těleso okruhu polynomů $K[x]$)* není *okruhově konečné rozšíření.*

Důkaz tvrzení 1.1. Mějme okruhově konečné rozšíření těles $K \subset L$ a zvolme $n \ge 1$ a prvky $v_1, \dots, v_n \in L$ takové, že $L = K[v_1, \dots, v_n]$. Indukcí podle n ukážeme, že $[L : K] < \infty$.

Pokud $n = 1$, máme $L = K(v_1)$. Kdyby v_1 bylo transcendentní nad K, měli bychom K-isomorfismus $K(v_1) \simeq K(x)$, ale $K \subset K(x)$ není podle lemmatu 4.1 okruhově konečné rozšíření. Proto musí být v_1 algebraické nad K, a dostaneme tedy

$$[L : K] = \deg m_{v_1,K} < \infty.$$

Předpokládejme nyní, že $n > 1$, a položme $K_1 = K(v_1) \subset L$. Potom $L = K_1[v_2, \dots, v_n]$ a podle indukčního předpokladu $[L : K_1] < \infty$. Teď použijeme tvrzení 3.1 na rozšíření $K \subset K_1 \subset L$ a dostaneme, že $K \subset K_1 = K(v_1)$ je okruhově

konečné. Stejně jako v předchozím odstavci odvodíme, že v_1 je nutně algebraický nad K, a tedy $[K_1 : K] < \infty$. Dohromady dostaneme, že

$$[L : K] = [L : K_1] \cdot [K_1 : K] < \infty,$$

což jsme měli dokázat. □

Reference

[1] V. Kala, *Komutativní okruhy*, elektronická skripta, http://karlin.mff.cuni.cz/~kala/files/KO-2021.pdf.