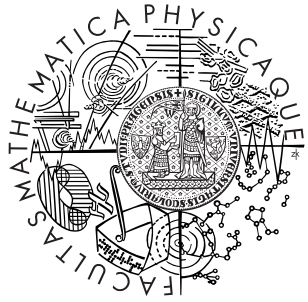
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Miroslav Korbelář

Komutativní nilpotentní okruhy

Katedra algebry
Vedoucí diplomové práce: Prof. RNDr. Tomáš Kepka, DrSc.
Studijní program: Matematika
Studijní obor: Matematické struktury

Chtěl bych poděkovat Mgr. Robertu El Bashirovi, Dr. za podnětné připomínky a trpělivost, s jakou mě pokaždé vyslechl, svému školiteli Prof. RNDr. Tomáši Kepkovi, DrSc. a svým blízkým, bez jejichž podpory by tento dokument nevznikl.

Prohlašuji, že jsem svou diplomovou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce.

V Praze dne 5. července 2006 Miroslav Korbelář

Obsah

Název práce: Komutativní nilpotentní okruhy
Autor: Miroslav Korbelář
Katedra (ústav): Katedra algebry
Vedoucí diplomové práce: Prof. RNDr. Tomáš Kepka, DrSc.
e-mail vedoucího: Tomas.Kepka@mff.cuni.cz
Abstrakt: Nechť A je komutativní nilpotentní algebra konečné dimenze nad tělesem F. Eggertova hypotéza z roku 1971 říká, že pokud $charF = p > 0$, pak je $p \cdot dimA^{(p)} \leq dimA$, kde $A^{(p)}$ je podalgebra generovaná prvky a^p, kde $a \in A$. Ukážeme, že toto je pravda, pokud $A^{(p)}$ je jako algebra nejvýše 2-generovaná. Hypotézu zobecníme pro tzv. dobrý pár (A, p) a dokážeme, že odhad $p \cdot dimA^{(p)} \leq dimA$ platí, pokud je dobrý pár 2-generovaný. Ukážeme dále, že pro každou A generovanou prvky $a_1, \ldots, a_n$ lze najít určitou kanonickou bázi $\mathcal{B}_A$, která umožňuje lepší pohled do struktury algebry A. Nakonec dokážeme odhad $(1 + dimA) \leq p^n(1 + dimA^{(p)})$, kde n je počet generátorů algebry A, $p = charF > 0$ a uvedeme protipříklad k postupu v článku L. Hammoudiho, který tvrdí, že E. hypotézu dokázal.
Klíčová slova: komutativní nilpotentní okruhy, nilpotentní p-algebry, Eggertova hypotéza

Title: Commutative nilpotent rings
Author: Miroslav Korbelář
Department: Department of Algebra
Supervisor: Prof. RNDr. Tomáš Kepka, DrSc.
Supervisor's e-mail address: Tomas.Kepka@mff.cuni.cz
Abstract: Let A be a finite dimensional commutative nilpotent algebra over a field F. Eggert's conjecture from 1971 says, that if $charF = p > 0$, then holds $p \cdot dimA^{(p)} \leq dimA$, where $A^{(p)}$ is the subalgebra generated by a^p, $a \in A$. We will show that this is true, if $A^{(p)}$ has at most 2 generators as an algebra. We generalize the conjecture for so called good pair (A, p) and proof, that the inequality $p \cdot dimA^{(p)} \leq dimA$ holds for a 2-generated good pair (A, p). We show next that for every A generated by $a_1, \ldots, a_n$ we can find a sort of canonical base $\mathcal{B}_A$, which makes the structure of A a little bit clearer. At the end we proof that $(1 + dimA) \leq p^n(1 + dimA^{(p)})$ holds, where n is the number of generators of the algebra A, $p = charF > 0$ and will show a counterexample to the paper of L. Hammoudi, who claims he already proved the E. conjecture.
Keywords: commutative nilpotent rings, nilpotent p-algebras, Eggert's conjecture

Kapitola 1

Úvod

V této práci se budeme zabývat okruhy, které jsou současně vektorovými prostory (tato struktura se obvykle nazývá algebra) a které jsou navíc komutativní a nilpotentní.

Definice 1 *Nechť A je asociativní, komutativní okruh v širším smyslu (tj. nemusí obsahovat jednotku), F komutativní těleso. Řekneme, že A je F-algebra právě když A je vektorovým prostorem nad F a pro každé $\lambda \in F$ a každé $a, b \in A$ platí $\lambda(ab) = (\lambda a)b = a(\lambda b)$.*

Definice algebry bývá obvykle obecnější (zejména se vynechává požadavek komutativnosti), ale pro naše účely bude vhodnější výše uvedené znění. Místo A je F-algebra budeme také říkat algebra nad tělesem F, případne jen algebra, pokud nebude potřeba zdůrazňovat těleso.

Dále budeme používat toto značení: $\mathbb{N}$ bude označovat množinu přirozených čísel $\{1, 2, \ldots\}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. $F[x_1, \ldots, x_n]$ bude okruh polynomů nad množinou proměnných $\{x_1, \ldots, x_n\}$ a tělesem F. Pro prvek $f \in R = F[x_1, \ldots, x_n]$ budeme ideál v R generovaný f značit standardně jako Rf. Kongruenci podle ideálu I v R označme $\equiv_I$, případně jen $\equiv$, pokud bude zřejmé, o jaký ideál se jedná. Dále pro reálné číslo r buď $\lfloor r \rfloor$ (dolní) celá část (tj. $n \in \mathbb{Z}$ takové, že $n \leq r < n + 1$) a $\lceil r \rceil$ horní celá část (tj. $n \in \mathbb{Z}$ takové, že $n - 1 < r \leq n$). $|X|$ bude označovat velikost množiny X. Algebra generovaná množinou $X \subseteq A$ bude označena $\langle X \rangle$ a vektorový prostor nad F generovaný množinou X pak $[X]$.

Homomorfismem F-algeber budeme rozumět homomorfismus okruhů (ne nutně s jednotkou), který je současně F-lineární zobrazení.

Definice 2 *Nechť A je algebra. $X, Y \subseteq A$. Položme $X.Y = [\{xy|\ x \in X, y \in Y\}]$ (pro $X = \{a\}$ pišme pouze $a.Y$).*
Dále označme $A^k = [\{a_1 \dots a_k|\ a_i \in A\}]$, $A^{(k)} = [\{a^k|\ a \in A\}]$ a
$A_k = [\{a \in A|\ a^k = 0\}]$.

Algebra A se nazývá nilpotentní $\Leftrightarrow$ ex. $k \geq 1$ takové, že $A^k = 0$.

Protože A je asociativní okruh, platí $A^k = \underbrace{A \dots A}_{k}$ a A je tak nilpotentní právě když je to nilpotentní prvek v pologrupě všech podmnožin A s operací násobení množin z předchozí definice. Zřejmě jsou dále A^k, $A^{(k)}$ a A_k algebry a A^k, A_k jsou navíc ideály v A (podalgebra $I \subseteq A$ je ideál v $A \Leftrightarrow (\forall a \in A)(\forall b \in I)(ab \in I)$).

Nilpotentní F-algebra A nemůže být okruhem s jednotkou (protože pak by $0 \neq 1 \in A^n$ pro každé n). Lze ji však vnořit do vhodné F-algebry, která už jednotku obsahovat bude. To ukazuje následující věta.

Věta 3 *Nechť A je nilpotentní F-algebra. Na vektorovém prostoru $F \oplus A$ definujme násobení předpisem $(\lambda + a).(\mu + b) = \lambda\mu + (\lambda b + \mu a + ab)$, kde $\lambda, \mu \in F$ a $a, b \in A$. Pak platí:*

1) $F \oplus A$ je F-algebra s jednotkou,

2) A a F jsou F-podalgebry $F \oplus A$,

3) A je jediný maximální ideál okruhu $F \oplus A$.

Důkaz: Body 1), 2) a to, že A je ideál v $F \oplus A$ se snadno ověří. A bude jediný max. ideál v $F \oplus A$ právě když $(F \oplus A) \setminus A$ bude množinou všech invertibilních prvků okruhu $F \oplus A$. Protože $A^n = 0$ pro vhodné n, je $a^n = 0$ pro všechna $a \in A$. Prvky A jsou tedy nilpotentní a tedy nejsou invertibilní. Nechť naopak $\lambda + a \in (F \oplus A) \setminus A$. Pak je $\lambda \neq 0$ a tudíž $\lambda + a = \lambda(1 + \lambda^{-1}a)$. λ je zřejmě invertibilní a prvek $1 + b$, kde $b \in A$, také, neboť jeho inverze je $\sum_{k=0}^{\infty}(-b)^k$. $\square$

Tato věta nám umožňuje používat zápisy jako $a(1 + b)$, případně $a.b^0$ pro $a, b \in A$.

Připomeňme ještě známý fakt, že pokud $charF = p > 0$ pak pro každé $a, b \in A$ platí $(a + b)^p = a^p + b^p$.

Protože dále budeme pracovat už téměř pouze s nilpotentními algebrami, *budeme pro jednoduchost slovem* `algebra` *myslet vždy* `nilpotentní algebru`, nebude-li řečeno jinak. Slovo "nilpotentní" pak použijeme, když budeme chtít tuto vlastnost zdůraznit.

Kapitola 2

Historie Eggertovy hypotézy a související problémy

Ke každé nilpotentní F-algebře A můžeme zkonstruovat (viz článek [1]) tzv. quasiregulární grupu $Q_A = (A, \circ)$ s operací $a \circ b = a + b + ab$ pro všechna $a, b \in A$. Že se jedná o ábelovskou grupu je ihned zřejmé z monomorfismu grupoidů $\phi : (A, \circ) \to (F \oplus A, \cdot)$, $\phi(a) = 1 + a$ a toho, že $Im\phi = \{1 + a |\ a \in A\}$ je multiplikativní grupa (neboť $(1 + a)^{-1} = 1 + \sum_{k=1}^{\infty} (-a)^k$). Nadále budeme grupy Q_A a $\{1 + a |\ a \in A\}$ ztotožnovat.

Pokud navíc je $charF = p > 0$, pak Q_A je p-grupa.

Důkaz: Z nilpotence A plyne, že existuje k takové, že $a^{p^k} = 0$ pro všechna $a \in A$. Je tedy $(1 + a)^{p^k} = 1 + a^{p^k} = 1$, takže Q_A je p-grupa. □

V dalším textu se bude zabývat následujícím výrokem.

$(*)$ **Eggertova hypotéza:** Nechť A je nilpotetní F-algebra konečné dimenze, $charF = p > 0$. Pak platí $p \cdot dimA^{(p)} \leq dimA$.

Tato hypotéza neměla od začátku výše uvedený tvar, ale postupně se zobecňovala spolu s uveřejňovanými výsledky. Vyslovil ji v roce 1971 K. H. Eggert ve svém článku [1]. Týkala se však jen konečných algeber. Ukázal zde, že pokud $(*)$ platí, dají se popsat všechny grupy, které jsou izomorfní nějaké Q_A, kde A je konečná. Současně dokázal, že $(*)$ platí, pokud A je konečná a $dimA^{(p)} \leq 2$.

Další výsledek se objevil až v roce 1996 v článku C. Stack [2] a sice, že $(*)$

platí, pokud F je perfektní těleso a $dim A^{(p)} \leq 2$ (algebra A dokonce nemusela být komutativní). O 2 roky později [3] pak autorka předpoklady zeslabila na $dim A^{(p)} \leq 3$ pro (nyni už komutativní) algebru A nad perfektním tělesem.

V roce 2001 B. Amberg a L. Kazarin [4] ukázali, že pro algebru A nad (libovolným) tělesem F charakteristiky $p > 0$ platí $p^n \cdot dim A^{(p^n)} \leq dim A$ pro $n \geq 1$, pokud $dim A^{(p)} = 3$. Současně našli protipříklad, který vyvrací analogii Eggertovy hypotézy pro nekomutativní algebry.

Ze stejného roku je pak článek [5], kde tíž autoři dokázali platnost $(*)$ pro případ, kdy $dim A^{(p)} \leq 4$.

Poslední publikovaný výsledek vyšel v roce 2004 a K. R. McLean [6] zde ukázal, že $(*)$ platí v těchto případech:

- když A je graduovaná (viz následující definice) a je splněna alespoň jedna z následujících podmínek i)-iv):

i) $(A^{(p)})^2 = 0$,

ii) $p = 2$ a $(A^{(p)})^4 = 0$,

iii) $p = 3$ a $(A^{(p)})^3 = 0$,

iv) $A^{(p)}$ je generována 2 prvky,

- nebo když $A \cong Rad(F[G])$, kde $F[G]$ je grupová algebra (zde tedy ne nutně nilpotentní) pro nějakou konečnou grupu G.

Definice 4 *Algebra A se nazývá graduovaná $\Leftrightarrow$ A je direktním součtem vektorových podprostorů $N_i \subseteq A$, $i \geq 1$ takových, že $N_i.N_j \subseteq N_{i+j}$ pro všechna $i, j \geq 1$ a $A = \langle N_1 \rangle$.*

Je třeba ještě poznamenat, že existuje článek [7] z roku 2002, v němž L. Hammoudi tvrdí, že Eggertovu hypotézu dokázal. Celkem snadno se však dají najít příklady, pro které postupy (příp. lemmata) zde uvedené neplatí (více viz Dodatek, Příklad D). Platnost $(*)$ tak zůstává stále otevřeným problémem.

Důkazy používané v uvedených článcích jsou (s vyjímkou [1] a [7]) standardně "algebraického" charakteru a, jak je vidět z výsledků, jde většinou o snahu postupovat nějak podle dimenze $A^{(p)}$. Není ale vůbec zřejmé, jak tyto myšlenky zobecnit pro vyšší hodnoty $dim A^{(p)}$.

Přístup, který použijeme v další kapitole, bude spíše "kombinatorický" a bude záviset na počtu generátorů algebry $A^{(p)}$ a nikoliv na její dimenzi.

Přejdeme nyní k otázkám, které s Eggertovou hypotézou souvisí.

Nechť A je F-algebra konečné dimenze, F perfektní těleso, $charF = p > 0$. Uvažme zobrazení $f : A \to A^{(p)}$, $f(a) = a^p$. Je zřejmé, že f je okruhový epimorfismus a jako zobrazení mezi vektorovými prostory je semilineární (neboť $f(\lambda a) = \alpha(\lambda)f(a)$, kde α je Frobeniův automorfismus tělesa F). Protože $kerf = A^{(p)}$, tak máme, že $dim(A/A_p) = dimA^{(p)}$ a dostáváme tak následující ekvivalence:

$$p \cdot dimA^{(p)} \leq dimA \;\Leftrightarrow\; p \cdot dim(A/A_p) \leq dimA \;\Leftrightarrow\; \tfrac{p-1}{p} \cdot dimA \leq dimA_p$$

Vidíme tedy, že v případě perfektních těles je hypotéza $(*)$ ekvivalentní s právě uvedeným odhadem dimenze algebry A_p .

Dále ukážeme, že $(*)$ souvisí také s odhadem Prüferova ranku grup (prevzato z [8]).

Definice 5 *Nechť G je grupa, $r \in \mathbb{N}_0$. Řekneme, že G má konečný Prüferův rank $r \Leftrightarrow r$ je nejmenší takové, ze každá konečně generovaná podgrupa grupy G má r generátorů. (rank se pak označuje jako $r(G)$)*

Lemma 6 *Nechť G je konečná ábel. p-grupa. Pak $r(G) = dim_{\mathbb{Z}_p}(Soc(G))$.*

Důkaz: Zřejmě $r((\mathbb{Z}_p)^n) = n$, neboť $(\mathbb{Z}_p)^n$ můžeme chápat jako vektorový prostor nad $\mathbb{Z}_p$. Dále $\mathbb{Z}^n$ je volný $\mathbb{Z}$-modul, $\mathbb{Z}$ je obor hlavních ideálu, a proto každý $\mathbb{Z}$-podmodul $\mathbb{Z}^n$ je volný s hodností $\leq n$. Tedy je $n \geq r(\mathbb{Z}^n)$. Z teorie grup víme, že $G \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p^{k_i}}$ pro nějaké $n \geq 0$ a $k_i \geq 1$. Zřejmě je $G \geq Soc(G) = \{a \in G |\ p \times a = 0\} \cong (\mathbb{Z}_p)^n$ a tedy $r(G) \geq r(Soc(G)) = n$. Současně je G homomorfním obrazem $\mathbb{Z}^n$ a tedy $n \geq r(\mathbb{Z}^n) \geq r(G)$, čímž je důkaz u konce. □

Důsledek 7 *Nechť A je konečná F-algebra, $charF = p$, $|F| = p^n$. Pak $r(Q_A) = n \cdot dim_F(A_p)$.*

Důkaz: $Q_A = \{1 + a |\ a \in A\}$ je multiplikativní p-grupa. Podle předchozího lemmatu máme $r(Q_A) = dim_{\mathbb{Z}_p}(Soc(Q_A))$. Přitom je $Soc(Q_A) = \{1 + a |\ a \in A \;\&\; (1+a)^p = 1\} = \{1 + a |\ a \in A \;\&\; a^p = 0\}$. Je tedy $|Soc(Q_A)| = |A_p|$, takže dostáváme $dim_{\mathbb{Z}_p}(Soc(Q_A)) = ln_p|Soc(Q_A)| = ln_p|A_p| = n.dim_F(A_p)$, kde ln_p je logaritmus se základem p. □

Z předchozích úvah vidíme, že v případě konečných F-algeber je hypotéza $(*)$ ekvivalentní s odhadem Prüferova ranku grupy Q_A, který má tvar $n.\frac{p-1}{p}dimA \leq r(Q_A)$, kde $|F| = p^n$, $charF = p$.

Než ukážeme další důsledek $(*)$ je potřeba něco vědět o struktuře jednogenerovaných algeber.

Věta 8 *Nechť A je F-algebra, $R = F[x]$, $a \in A$ takové, že $A = \langle a \rangle$. Pak ex. $n \geq 0$ takové, že A je izomorfní F-algebře Rx/Rx^{n+1}.*

Důkaz: Uvažme zobrazení $\phi : Rx \to A$, $\phi(f) = f(a)$. ϕ je epimorfismus F-algeber a proto platí $A \cong (Rx/ker\phi)$. R je obor hlavních ideálů a tedy $ker\phi = Rg(x)$ pro nějaké $g(x) \in Rx$. Dále zřejmě existuje $n \geq 0$ takové, že $g(x) = x^{n+1}(\lambda + f(x))$ pro nějaké $0 \neq \lambda \in F$ a $f(x) \in Rx$. Je tedy $0 = g(a) = a^{n+1}(\lambda + f(a))$ a protože $\lambda + f(a)$ je invertibilní v $F \oplus A$ (viz Věta 3), tak $a^{n+1} = 0$ a tedy $ker\phi = R.x^{n+1}$. □

Lemma 9 *Nechť $n \geq 0$, $R = F[x]$, $I = R.x^{n+1}$. Označme $A = Rx/I$. Pak platí:*

1) A je nilpotentní F-algebra s bází $\{x + I, \ldots, x^n + I\}$ a $A = \langle x + I \rangle$,

2) je-li navíc $charF = p > 0$, pak $dimA^{(p)} = \left\lfloor \frac{n}{p} \right\rfloor$, $dimA_p = n - \left\lfloor \frac{n}{p} \right\rfloor$.

Tedy platí $p \cdot dimA^{(p)} \leq dimA$.

Důkaz: Bod 1) se snadno ověří. Nechť je tedy $charF = p > 0$. Pak je (díky tomu, že umocňování na p je aditivní) zřejmě $A^{(p)} = [\{x^{pi} |\ pi \leq n \ \&\ i \geq 1\}]$ a tedy $dimA^{(p)} = |\{i |\ 1 \leq i \leq \frac{n}{p}\}| = \left\lfloor \frac{n}{p} \right\rfloor$. Podobně máme $A_p = [\{\sum_i \lambda_i x_i |\ (\sum_i \lambda_i x_i)^p \equiv 0\}] = [\{x^i |\ n < pi \ \&\ i \geq n\}]$ a tedy $dimA^{(p)} = |\{i |\ \frac{n}{p} < i \leq n\}| = n - dimA^{(p)}$. □

Nyní už můžeme ukázat další důsledek hypotézy $(*)$ (převzato z [5]).

Věta 10 *Nechť F je konečné těleso charakteristiky p, $\mathcal{S} = \{A |\ A$ je konečná F-algebra$\}$. Pak následující je ekvivalentní:*

1) $(\forall A \in \mathcal{S})(p \cdot dimA^{(p)} \leq dimA)$,

2) $(\forall A \in \mathcal{S})(\exists n \in \mathbb{N})(\exists L_1, \ldots, L_n \in \mathcal{S})$ takové, že L_i jsou jednogenerované a $Q_A \cong \bigoplus_{i=1}^{n} Q_{L_i}$.

Důkaz: Nejdříve si uvědomíme, že pro $A \in \mathcal{S}$ platí $|A| = |Q_A|$, $|A| = |F|^{dimA}$, $|A_p| = |Soc(Q_A)|$ a tedy, že

$$p \cdot dimA^{(p)} \leq dimA \ \Leftrightarrow\ \tfrac{p-1}{p} \cdot dimA \leq dimA_p \ \Leftrightarrow\ |Q_A|^{\frac{p-1}{p}} \leq |Soc(Q_A)|.$$

2) $\Rightarrow$ 1): Nechť $Q_A \cong \bigoplus_{i=1}^{n} Q_{L_i}$, kde $L_i \in \mathcal{S}$ a L_i je jednogenerovaná. Pak $|Q_A| = \prod_{i=1}^{n} |Q_{L_i}|$, $|Soc(Q_A)| = \prod_{i=1}^{n} |Soc(Q_{L_i})|$. Protože L_i splňují Eggertovu hypotézu (viz předchozí lemma), je $|Q_{L_i}|^{\frac{p-1}{p}} \leq |Soc(Q_{L_i})|$. Vynásobením těchto nerovností dostáváme platnost 1).

1) $\Rightarrow$ 2): Nejdříve si uvědomme, že platí následující:

a) Nechť $A \in \mathcal{S}$, pak $Q_A/Soc(Q_A) \cong Q_{A/A_p}$. (K důkazu stačí uvážit přirozený homomofrismus $\pi : A \to A/A_p$. Ten indukuje přidružený homomorfismus grup $\pi_* : Q_A \to Q_{A/A_p}$, $\pi_*(1+a) = 1+\pi(a)$, který je zřejmě na a platí, že $ker\pi_* = \{1+a|\ a^p = 0\} = \{1+a|\ (1+a)^p = 1\} = Soc(Q_A)$.)

b) Nechť G, H jsou konečné p-grupy, $|G| = |H|$ a $G/Soc(G) \cong H/Soc(H)$. Pak $G \cong H$. (To je známý fakt z teorie grup, který plyne ihned z toho, že konečné p-grupy jsou direktními součty cyklických grup.)

Implikaci 1) $\Rightarrow$ 2) nyní dokážeme indukcí podle $dimA$:

- případ $dimA = 0$ je zřejmý,

- indukční krok: Mějme $A \in \mathcal{S}$. Zřejmě $dim(A/A_p) < dimA$ (jinak by bylo $A = A_p$ a tedy $A_p = (A_p)_p = A_{p^2}$ atd., což by byl spor s nilpotentností A). Proto podle ind. předpokladu ex. jednogenerované $S_1, \ldots, S_n \in \mathcal{S}$ takové, že $Q_{A/A_p} \cong \bigoplus_{i=1}^{n} Q_{S_i}$. Odsud vyplývá, že $dim(A/A_p) = \sum_{i=1}^{n} dimS_i$. Z platnosti 1) máme, že $m = dimA - p.dimA^p \geq 0$. Definujme nyní L_i takto: pro $1 \leq i \leq n$ bud L_i jednogenerovaná a taková, že $dimL_i = p.dimS_i$, a pro $n < i \leq n+m$ nechť L_i je taková, že $dimL_i = 1$ (existence L_i plynou z předchozího lemmatu). Definujme ještě $S_i = 0$ pro $n < i \leq n+m$.

Podle Lemmatu 9 je $dim(L_i/(L_i)_p) = \left\lfloor \frac{dimL_i}{p} \right\rfloor = dimS_i$ a tedy podle Věty 8 a Lemmatu 9 je $L_i/(L_i)_p \cong S_i$ pro všechna $1 \leq i \leq n+m$. Označme $G = \bigoplus_{i=1}^{n+m} Q_{L_i}$. Dostáváme tak

$G/Soc(G) \cong \bigoplus_{i=1}^{n+m} (Q_{L_i}/Soc(Q_{L_i})) \cong \bigoplus_{i=1}^{n+m} Q_{L_i/(L_i)_p} \cong \bigoplus_{i=1}^{n+m} Q_{S_i} \cong Q_{A/A_p} \cong$

$\cong Q_A/Soc(Q_A)$. A protože je $ln_{|F|}|G| = ln_{|F|} \prod_{i=1}^{n+m} |L_i| = \sum_{i=1}^{n+m} dimL_i = m + p.\sum_{i=1}^{n} dimS_i = dimA = ln_{|F|}|Q_A|$ (zde $ln_{|F|}$ je opět logaritmus se základem $|F|$), tak podle b) platí $Q_A \cong G = \bigoplus_{i=1}^{n+m} Q_{L_i}$. Což jsme chtěli dokázat. $\square$

Vidíme tedy, že Eggertova hypotéza je pro konečné algebry ekvivalentní s popisem struktury quasiregularních grup pomocí jednogenerovaných algeber.

Podle článku [1] pro $A \in \mathcal{S}$, $charF = p$ a $|F| = p^n$ platí, že $Q_A \cong \bigoplus_{i=1}^{k} (\mathbb{Z}_{p^i})^{nt_i}$, kde k je nejmenší takové, že $a^{p^k} = 0$ pro všechna $a \in A$, $t_i = r_{i-1} + r_{i+1} - 2r_i$ pro $1 \leq i \leq k$, $r_i = dimA^{(p^i)}$ pro $i \geq 0$.

Pokud by tedy ke každé grupě $(\mathbb{Z}_{p^j})^n$ existovala jednogenerovaná F-algebra L taková, že $Q_L \cong (\mathbb{Z}_{p^j})^n$, pak by byla Eggertova hypotéza (alespoň v rámci konečných algeber) vyřešena. Pro algebru L by pak tudíž muselo platit, že $|L| = |Q_L| = p^{nj} = |F|^j$ a tedy $dimL = j$. Podle Lemmatu 9 by pak posloupnost čísel r_i pro L byla následující: $r_0 = j$, $r_{i+1} = \left\lfloor \frac{r_i}{p} \right\rfloor$ pro $i \geq 0$. Pokud na základě této posloupnosti spočítáme čísla t_i, které určují tvar Q_L, tak obecně nedostaneme $(\mathbb{Z}_{p^j})^n$, což se dá snadno na mnoha příkladech ověřit.

Na závěr ještě poznamenejme, že platnost Eggertovy hypotézy by přispěla také k lepšimu poznání konečných lup. Způsob, jakým se zde hypotéza $(*)$ uplatňuje, spočívá v tom, že se jisté struktury týkající se lup přeloží do řeči p-grup a odtud pak do nilpotentních p-okruhů, neboli nilpotentních algeber nad tělesem $\mathbb{Z}_p$. Tento postup je však dost složitý a zdlouhavý a navíc je tento problém zatím stále ještě rozpracován. Proto ho zde nebudeme podrobněji rozvádět.

(Zde by bylo vhodné zmínit se, že problém $(*)$ mi byl zadán právě v souvislosti s lupami. Tehdy ovšem nebyl v uvedeném tvaru, nýbrž zněl: Nechť R je konečný okruh takový, že platí $p \times a = 0$ pro každé $a \in R$ a p je prvočíslo. Platí pak, že $dimR_p \geq \frac{1}{2}.dimR$, kde $R_p = \{a \in R | a^p = 0\}$?.

Po té, co se mi podařilo uvedenou nerovnost dokázat pro $p = 2$ a R dvougenerovaný, jsem na internetu zjistil, že problém se nazývá Eggertova hypotéza, a našel několik výše uvedených článků.

Proto, ač se to může zdát nepravděpodobné, nebyl postup, který bude uveden v další kapitole, inspirován ani Eggertovým článkem [1] a ani článkem L. Hammoudiho [7]. Odsud jsem pouze převzal značení, protože se mi zdálo vhodné.)

Kapitola 3

Zobecnění Eggertovy hypotézy a nový výsledek

Z publikovaných výsledků (viz výše) je vidět, jak se Eggertova hypotéza postupně vyvíjela od konečných těles, přes perfektní až k libovolným tělesům charakteristiky $p > 0$.

Víme už, že pro perfektní tělesa je $dim(A/A_p) = dimA^{(p)}$. Pro tělesa charakteristiky $p > 0$ to už obecně není pravda (viz Dodatek Příklad B). Platí ale, že $dim(A/A_p) \geq dimA^{(p)}$.

Důkaz: Zvolme bázi $e_1, \ldots, e_k$ vekt. prostoru A_p a doplňme ji o vektory $e_{k+1}, \ldots, e_n$ tak, aby celek tvořil bázi A. Zřejmě je $(e_i)^p = 0$ pro $1 \leq i \leq k$ a tedy $A^{(p)} = [\{a^p |\ a \in A\}] = [(e_1)^p, \ldots, (e_n)^p] = [(e_{k+1})^p, \ldots, (e_n)^p]$. Takže $dimA^{(p)} \leq dimA - dimA_p$. □

Můžeme se tudíž přirozeně ptát, zda neplatí silnější nerovnost $p \cdot dim(A/A_p) \leq dimA$ nebo ekvivalentní $\frac{p-1}{p} \cdot dimA \leq dimA_p$.

Při zobecňování lze jít i jiným směrem a zkoumat např. pro jaká $k \in \mathbb{N}$ bude platit, že $k \cdot dimA^{(k)} \leq dimA$. Přitom nemusíme nutně trvat na tom, aby pro pevně zvolené k byl odhad splněn pro všechny algebry A, ale můžeme se pokusit najít nějaký vztah mezi číslem k a algebrou A tak, aby uvedená nerovnost platila. V tomto případě můžeme do úvahy zahrnout i tělesa, co mají charakteristiku 0. Takovéto zobecnění bude výsledkem v této práci.

Nejdříve je potřeba uvést několik definic.

Definice 11 *(1) Na množině* $(\mathbb{N}_0)^n \cup \{\infty\}$ *zaveďme lexikografické uspořádání* " $\leq$ ":

$(\alpha_1, \ldots, \alpha_n) < (\beta_1, \ldots, \beta_n) \Leftrightarrow$ *ex. i, že* $1 \leq i \leq n$ *a* $\alpha_j = \beta_j$ *pro* $1 \leq j < i$ *a* $\alpha_i < \beta_i$.

$(\alpha_1, \ldots, \alpha_n) < \infty$ *pro všechna* $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}_0)^n$.

a uspořádání " $\leq_\Pi$ " *(produktové):*

$(\alpha_1, \ldots, \alpha_n) \leq_\Pi (\beta_1, \ldots, \beta_n) \Leftrightarrow \alpha_i \leq \beta_i$ *pro všechna* $1 \leq i \leq n$.

$(\alpha_1, \ldots, \alpha_n) \leq_\Pi \infty$ *pro všechna* $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}_0)^n$.

Nechť $p \in \mathbb{N}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}_0)^n$. *Definujme* $p \cdot \infty = \infty$ *a* $p \cdot \alpha = (p\alpha_1, \ldots, p\alpha_n)$. *Dále položme* $\alpha + \infty = \infty + \alpha = \infty$ *a* $\alpha \cdot \infty = \infty \cdot \alpha = \infty$ *pro všechna* $\alpha \in (\mathbb{N}_0)^n \cup \{\infty\}$. *Na množině* $(\mathbb{N}_0)^n$ *budeme uvažovat přirozené sčítání a násobení prvků po složkách.*

(2) Pro $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}_0)^n$ *definujme* $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in F[x_1, \ldots, x_n]$.

Pro $f = f(x_1, \ldots, x_n) = \sum_\alpha \lambda_\alpha x^\alpha \in F[x_1, \ldots, x_n]$, $(\lambda_\alpha \in F)$ *definujme* $f_\alpha = \lambda_\alpha$ *a* $f(x^\alpha) = f(x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}) = \sum_\beta \lambda_\beta x^{\alpha\beta}$ *a* $f(x^p) = f(x_1^p, \ldots, x_n^p)$ *pro* $p \in \mathbb{N}$.

(3) Pro $f \in F[x_1, \ldots, x_n]$ *definujme* $M(f) = min_\leq\{\alpha \in (\mathbb{N}_0)^n |\ f_\alpha \neq 0\}$, *pokud* $f \neq 0$ *a* $M(f) = \infty$ *pokud* $f = 0$.

Poznámka:

1) Definice x^α a $f(x^\alpha)$ nejsou v rozporu.

2) Pokud je $n \geq 2$, pak symbol f_α pro $\alpha \in (\mathbb{N}_0)^n$ nelze zaměnit s případnou indexací polynomů f_i, $i \in \mathbb{N}$. V dalším textu tomu tak vždy bude.

Lemma 12 *Nechť* $\alpha, \beta, \gamma \in (\mathbb{N}_0)^n \cup \{\infty\}$ *a* $f, g \in F[x_1, \ldots, x_n]$. *Pak platí:*

1) $\alpha \leq_\Pi \beta \Rightarrow \alpha \leq \beta$,

2) $\alpha \leq_\Pi \beta \Rightarrow \alpha + \gamma \leq_\Pi \beta + \gamma$, $\alpha \leq_\Pi \beta \Rightarrow \alpha \cdot \gamma \leq_\Pi \beta \cdot \gamma$,

3) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$, $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$,

4) $M(fg) = M(f) + M(g)$, $M(f(x^\alpha)) = \alpha M(f)$ *pro* $\alpha \neq \infty$,

5) $min_\leq\{M(f), M(g)\} \leq M(f + g)$, *pokud navíc je* $M(f) < M(g)$, *pak* $M(f + g) = M(f)$.

Důkaz: Snadný. □

Definice 13 *Nechť* A *je nilpotentní* F*-algebra,* $2 \leq p \in \mathbb{N}$, $a_1, \ldots, a_n \in A$, $R = F[x_1, \ldots, x_n]$. *Řekneme, že dvojice* (A, p) *je dobrý pár generovaný uspořádanou n-ticí* $(a_1, \ldots, a_n) \Leftrightarrow$

1) $A = \langle a_1, \ldots, a_n \rangle$,

2) $(\forall f \in Rx_1 + \cdots + Rx_n)(\exists g \in Rx_1 + \cdots + Rx_n)(f^p(a_1, \ldots, a_n) = g(a_1^p, \ldots, a_n^p)$ & $M(g) \leq_\Pi M(f))$.

Budeme také říkat stručněji, že (A, k) *je n-generovaný dobrý pár, případně jen, že* (A, k) *je dobrý pár.*

V této kapitole dokážeme následující tvrzení:

(T1): Nechť (A, p) je 2-generovaný dobrý pár. Pak $p \cdot dimA^{(p)} \leq dimA$.

(T2): Nechť A je F-algebra konečné dimenze, $charF = p > 0$. Nechť $A^{(p)}$ je jako algebra 2-generovaná, pak $p \cdot dimA^{(p)} \leq dimA$.

Tvrzení **(T1)** nás vede přirozeně k vyslovení následujícího:

Zobecněná Eggertova hypotéza: Nechť (A, p) je dobrý pár. Pak $p \cdot dimA^{(p)} \leq dimA$.

Z definice dobrého páru (A, p) generovaného $a_1, \ldots, a_n$ snadno vyplývá, že $A^{(p)} = \langle a_1^p, \ldots, a_n^p \rangle$. Nabízí se tedy otázka, zda by se definice nedala zeslabit a požadavek 2) nahradit podmínkou

2') $A^{(p)} = \langle a_1^p, \ldots, a_n^p \rangle$

nebo ekvivalentním

2") $(\forall f \in Rx_1 + \cdots + Rx_n)(\exists g \in Rx_1 + \cdots + Rx_n)(f^p(a_1, \ldots, a_n) = g(a_1^p, \ldots, a_n^p))$

Ukazuje se však, že za těchto podmínek by zobecněná Eggertova hypotéza už neplatila (viz Dodatek Příklad C).

Dále - aby mělo smysl mluvit o nějakém zobecnění $(*)$ měli bychom ukázat, že existují i jiné než "triviální" dobré páry (viz Dodatek Příklad D).

A nakonec - v článku [6] byl jeden z výsledků tento: Eggertova hypotéza platí, pokud A je graduovaná algebra a $A^{(p)}$ je generovaná 2 prvky (jako algebra). Pokud by tedy každá algebra A taková, že $A^{(p)}$ je generovaná 2 prvky, byla graduovaná, tak bychom pro původní Eggertovu hypotézu žádný nový výsledek nedostali. Bylo by tudíž vhodné ukázat, že např. existují i jiné 2-generované algebry než jen ty graduované (proč to stačí ukázat: zřejmě když $charF = p > 0$ a A je n-generovaná, pak i $A^{(p)}$ je n-generovaná). Vhodné příklady budou v Dodatku v části E.

Nyní tedy přikročme k důkazu výše uvedených tvrzení. Nejdříve ukážeme, že **(T2)** plyne z **(T1)** a ve zbytku kapitoly dokážeme **(T1)**.

Na začátku si uvědomme následující snadná fakta:

1) Nilpotentní F-algebra je konečně generovaná (jako algebra) právě když má konečnou dimenzi (nad F).

2) Nechť A je F-algebra, $charF = p > 0$. Pak (A, p) je dobrý pár pro libovolnou n-tici, která generuje A.

Lemma 14 *Nechť A je F-algebra, $a_1, \ldots, a_n \in A$, $\pi : A \to A/A^2$ přirozená projekce.*

Pak $A = \langle a_1, \ldots, a_n \rangle \Leftrightarrow A/A^2 = [\pi(a_1), \ldots, \pi(a_n)]$.

Důkaz: A/A^2 je F-algebra s triviálním násobením, takže ji stačí chápat jako vekt. prostor.
$\Rightarrow$: plyne z toho, že π je epimorfismus algeber.
$\Leftarrow$: indukcí podle k ukážeme, že platí: $(\forall a \in A)(\exists b \in \langle a_1, \ldots, a_n \rangle)(a - b \in A^k)$. Odsud už pak díky nilpotenci A budeme mít snadno $A = \langle a_1, \ldots, a_n \rangle$.

$k = 1$: zřejmé

indukční krok: mějme $a - b = \sum_i a_{i,1}, \ldots, a_{i,k} \in A^k$, kde $a_{i,j} \in A$. Protože $\pi(a_1), \ldots, \pi(a_n)$ generuje A/A^2, $\pi(a_{i,j}) \in A/A^2$, tak máme $a_{i,j} = c_{i,j} + r_{i,j}$, kde $c_{i,j} \in [a_1, \ldots, a_n]$, $r_{i,j} \in A^2$. Po dosazení tak obdržíme $a - (b + \sum_i c_{i,1}, \ldots, c_{i,k}) \in A^{k+1}$. □

Důsledek 15 *Nechť $A = \langle a_1, \ldots, a_n \rangle$ a $A = \langle b_1, \ldots, b_m \rangle$, $m \leq n$. Pak ex. $i_1, \ldots, i_m$ taková, že $A = \langle a_{i_1}, \ldots, a_{i_m} \rangle$.*

Důkaz: Plyne snadno z předchozího lemmatu a ze známých faktů o vektorových prostorech. □

Poznámka: Nejmenší počet generátorů A bychom tedy mohli celkem oprávněně nazvat např. algebraickou dimenzí A.

Věta 16 *Nechť platí tvrzení **(T1)**. Pak platí i tvrzení **(T2)**.*

Důkaz: Nechť A je F-algebra konečné dimenze, $charF = p > 0$ a nechť $A^{(p)}$ je jako algebra 2-generovaná. Je tedy $A = \langle a_1, \ldots, a_n \rangle$ pro nějaké $a_i \in A$ a nějaké $n \geq 1$. Zřejmě je pak $A^{(p)} = \langle a_1^p, \ldots, a_n^p \rangle$ a podle předchozího důsledku máme bez újmy na obecnosti, že $A^{(p)} = \langle a_1^p, a_2^p \rangle$. Uvažme nyní algebru $B = \langle a_1, a_2 \rangle$.

(B,p) je 2-generovaný dobrý pár a platí, že $A^{(p)} = B^{(p)}$. Podle předpokladu tedy dostáváme $p \cdot dimA^{(p)} = p \cdot dimB^{(p)} \leq dimB \leq dimA$. □

Ve zbytku dokážeme tvrzení **(T1)**.

Věta 17 *1) Nechť A je F-algebra, $A = \langle a_1, \ldots, a_n \rangle$, $R = F[x_1, \ldots, x_n]$. Označme $I = \{f \in Rx_1 + \cdots + Rx_n |\ f(a_1, \ldots, a_n) = 0\}$. Pak I je ideál v R a ex. $k \geq 1$, že $x_1^k, \ldots, x_n^k \in I$. Zobrazení $\phi : Rx_1 + \cdots + Rx_n/I \to A$, $\phi(f + I) = f(a_1, \ldots, a_n)$ je pak izomorfismus F-algeber.*

Pokud navíc je (A,p) dobrý pár generovaný n-ticí $(a_1, \ldots, a_n)$, pak $(Rx_1 + \cdots + Rx_n/I, p)$ je dobrý pár generovaný n-tici $(x_1 + I, \ldots, x_n + I)$.

2) Nechť I je ideál v $R = F[x_1, \ldots, x_n]$, $I \subseteq Rx_1 + \cdots + Rx_n$. Pak $A = Rx_1 + \cdots + Rx_n/I$ je nilpotentní F-algebra právě když ex. $k \geq 1$, že $x_1^k, \ldots, x_n^k \in I$. A je pak generovaná prvky $x_1 + I, \ldots, x_n + I$ a tedy je konečné dimenze (nad F).

Důkaz: Snadný. □

Tato věta nám tedy říká, že při studiu F-algeber se stačí omezit na algebry tvaru $Rx_1 + \cdots + Rx_n/I$, kde ideál I má vhodné vlastnosti.

Všechny další úvahy a důkazy vycházejí z následující názorné představy, jak pracovat s polynomy v nilpotentní algebře $Rx_1 + \cdots + Rx_n/I$. Pro jednoduchost ji uvedeme jen pro $n = 2$. Mějme čtvercovou síť, kde jednotlivá políčka představují prvky $(i,j) \in (\mathbb{N}_0)^2$ (případně polynomy $x^i y^j$ nebo prvky $x^i y^j + I$). Polynom $f \in Rx + Ry$ si můžeme představovat jako (např. černě) vyznačená políčka v místech, kde má f nenulové koeficienty. Násobení prvkem x pak odpovídá posunutí takto označené oblasti (vodorovně) doprava (podobně dělení x - pokud je to samozřejmě vůbec možné). Je dobré si uvědomit, jaký tvar má při této představě polynom z následující definice.

Definice 18 *Nechť $f \in F[x_1, \ldots, x_n]$. Řekneme, že polynom f je v normálním tvaru $\Leftrightarrow (\forall \alpha \in (\mathbb{N}_0)^n)(M(f) <_\Pi \alpha \ \Rightarrow f_\alpha = 0)$.*

Připomeňme, že (podle dohody z úvodu) výrok "$Rx_1 + \cdots + Rx_n/I$ je algebra " znamená, že se jedná o nilpotetní komutativní asociativní algebru konečné dimenze (neboť je zřejmě konečně generovaná).

(V následujícím lemmatu se mi nepodařilo najít vhodnější důkaz, který by se vyhnul množství indexů, než ten, který je tu uvedený.)

Lemma 19 *Nechť $R = F[x_1, \dots, x_n]$, $A = Rx_1 + \cdots + Rx_n/I$ je algebra, $f \in Rx_1 + \cdots + Rx_n$. Pokud $f \equiv 0$, pak ex. $g \in Rx_1 + \cdots + Rx_n$ takový, že $M(g) = M(f)$, $g \equiv 0$ a g je v normálním tvaru.*

Důkaz: Pro $f = 0$ je tvrzení zřejmé, nechť je tedy $f \neq 0$. Položme $\alpha_0 = M(f)$. A je nilpotentní a tedy ex. $k \geq 1$, že $x_i^k \equiv 0$ pro $1 \leq i \leq n$ a $\alpha_0 + (1, \dots, , 1) \leq_\Pi (k, \dots, , k)$. Označme $\mathcal{I} = \{\alpha \in (\mathbb{N}_0)^n |\ \alpha_0 \leq_\Pi \alpha \leq_\Pi (k, \dots, k)\}$ a
$\mathcal{M} = \{\alpha \in \mathcal{I} |\ (\exists h \in I)(M(h) = \alpha_0\ \&\ (\forall \beta \in \mathcal{I})(\alpha_0 \neq \beta \leq \alpha \Rightarrow h_\beta = 0))\}$. Pak je $\alpha_0 \in \mathcal{M}$ (stačí vzít polynom f) a tedy $\mathcal{M}$ je konečná neprázdná množina. Ukážeme, že $(k, \dots, k) \in \mathcal{M}$:

sporem: Nechť tomu tak není a nechť α je největší prvek $\mathcal{M}$ vzhledem k $\leq$ ($\leq$ je dobré uspořádání) a nechť h je příslušný polynom k α. Pak $\alpha < (k, \dots, k)$ a existuje tedy $\tilde{\alpha}$ následník α v intervalu $\mathcal{I}$ vzhledem k $\leq$. Ukážeme, že $\tilde{\alpha} \in \mathcal{M}$ (což bude požadovaný spor).

Označme $\tilde{h} = h - \frac{h_{\tilde{\alpha}}}{f_{\alpha_0}} f.x^{\tilde{\alpha}-\alpha_0}$. Pak je $\tilde{h} \equiv 0$ a protože $M(f.x^{\tilde{\alpha}-\alpha_0}) = M(f) + M(x^{\tilde{\alpha}-\alpha_0}) = \tilde{\alpha} > \alpha_0$ tak máme (podle lemmatu 12) $M(\tilde{h}) = M(h - \frac{h_{\tilde{\alpha}}}{f_{\alpha_0}} f.x^{\tilde{\alpha}-\alpha_0}) = M(h) = \alpha_0$. Nechť je nyní $\beta \in \mathcal{I}$ takové, že $\alpha_0 \neq \beta \leq \tilde{\alpha}$. Pak je buď $\beta = \tilde{\alpha}$ a tedy $\tilde{h}_{\tilde{\alpha}} = h_{\tilde{\alpha}} - \frac{h_{\tilde{\alpha}}}{f_{\alpha_0}} (f.x^{\tilde{\alpha}-\alpha_0})_{\tilde{\alpha}} = 0$ nebo je $\alpha_0 \neq \beta < \tilde{\alpha}$ a (vzhledem k volbě $\tilde{\alpha}$) je tedy $\alpha_0 \neq \beta \leq \alpha$ a tudíž máme $\tilde{h}_\beta = h_\beta - \frac{h_{\tilde{\alpha}}}{f_{\alpha_0}} (f.x^{\tilde{\alpha}-\alpha_0})_\beta = h_\beta = 0$. Zjistili jsme tedy, že $\alpha < \tilde{\alpha} \in \mathcal{M}$, což je (jak už bylo řečeno) spor s volbou α.

Nyní víme, že $(k, \dots, k) \in \mathcal{M}$ a tedy ex. h takový, že platí $h \equiv 0$, $M(h) = M(f)$ a $(\forall \beta \in (\mathbb{N}_0)^n)(\alpha_0 <_\Pi \beta \leq_\Pi (k, \dots, k) \ \Rightarrow h_\beta = 0)$. Z volby k plyne, že $x^\beta \equiv 0$ pro všechna $\beta \not\leq_\Pi (k, \dots, k)$. Polynom g nyní dostaneme tak, že z polynomu h odstraníme členy $h_\beta x^\beta$ pro $\beta \not\leq_\Pi (k, \dots, k)$. □

Toto lemma nám umožňuje vyslovit následující definici.

Definice 20 *Nechť $R = F[x_1, \dots, x_n]$, $A = Rx_1 + \cdots + Rx_n/I$ je algebra. Položme $\mathcal{C}_A = \{\alpha \in (\mathbb{N}_0)^n |$ ex. $f \in I$ takové, že $M(f) = \alpha\} =$*
$= \{\alpha \in (\mathbb{N}_0)^n |$ ex. $f \in I$ takové, že $M(f) = \alpha$ a f je v normálním tvaru$\}$ a $\mathcal{B}_A = (\mathbb{N}_0)^n \setminus \mathcal{C}_\mathcal{A}$.

Věta 21 *Nechť $R = F[x_1, \dots, x_n]$, $A = Rx_1 + \cdots + Rx_n/I$ je algebra. Pak*

1) $\mathcal{C}_A$ je horní množina vzhledem k $\leq_\Pi$ v $(\mathbb{N}_0)^n$
(tj. $(\mathcal{C}_A \ni \alpha \leq_\Pi \beta \in (\mathbb{N}_0)^n) \ \Rightarrow \beta \in \mathcal{C}_A$),
2) $(0, \dots, 0) \in \mathcal{B}_A$ a $\mathcal{B}_A$ je dolní množina vzhledem k $\leq_\Pi$ v $(\mathbb{N}_0)^n$
(tj. $(\alpha \leq_\Pi \beta \in \mathcal{B}_A) \ \Rightarrow \alpha \in \mathcal{B}_A$),
3) Množina $M = \{x^\alpha + I |\ \alpha \in \mathcal{B}_A \setminus \{0, \dots, 0)\}\}$ je báze algebry A.

Důkaz: 1) Polynom pro α stačí přenásobit polynomem $x^{\alpha-\beta}$.

2) Z definice $\mathcal{C}_A$ máme snadno, že $\mathcal{C}_A \subseteq (\mathbb{N}_0)^n \setminus \{(0,\dots,0)\}$ (neboť polynomy definující $\mathcal{C}_A$ jsou z $Rx_1 + \cdots + Rx_n$). Zbytek plyne ihned z 1).

3) M generuje A jako vektorový prostor: A je nilpotentní a tedy ex. $k \geq 1$, že $x_i^k \equiv 0$ pro všechna $1 \leq i \leq n$. Označme $\mathcal{I} = \{\alpha |\ (0,\dots,0) <_\Pi \alpha \leq_\Pi (k,\dots,k)\}$. Protože zřejmě $A = [\{x^\alpha + I |\ \alpha \in \mathcal{I}\}]$ (neboť ostatní $x^\alpha + I$ pro $\alpha \not\leq_\Pi (k,\dots,k)$ jsou nulové), tak stačí ukázat, že pro každé $\alpha \in \mathcal{I}$ je $x^\alpha + I \in [M]$:

sporem: Nechť α je největší prvek $\mathcal{I}$ vzhledem k $\leq$ takový, že $x^\alpha + I \notin [M]$. Pak musí být $\alpha \in \mathcal{C}_A$ a tedy (z definice $\mathcal{C}_A$) je $x^\alpha \equiv \sum\limits_{\alpha<\beta} \lambda_\beta x^\beta$ pro vhodné $\lambda_\beta \in F$. Protože pro $\beta > \alpha$ je buď $\beta \notin \mathcal{I}$ a pak musí být $x^\beta + I = 0 + I \in [M]$ nebo je $\beta \in \mathcal{I}$ a pak z volby α je opět $x^\beta + I \in [M]$. Dostáváme tak, že $x^\alpha \in [M]$, což je spor.

M je lineárně nezávislá: sporem: Nechť ex. netriviální kombinace $f = \sum\limits_{\alpha\in\mathcal{B}_A} \lambda_\alpha x^\alpha \equiv 0$. Pak ovšem máme, že $M(f) \in \mathcal{B}_A$, což je spor s definicí množiny $\mathcal{B}_A$. □

Právě uvedená věta vystihuje základní (a vlastně také jediné) vlastnosti množin $\mathcal{B}_A$ a $\mathcal{C}_A$. V dalším textu je budeme velmi často používat (aniž bychom se přitom na uvedenou větu nějak zvlášť odvolávali).

Zde ukončíme tvrzení, která se vlastně týkala n-generovaných algeber a dále budeme pokračovat jen pro $n = 2$. Zatím totiž není jasné, jak a zda by šla zobecnit tak, abychom dostali požadovaný odhad dimenze pro $A^{(p)}$. Naznačili jsme alespoň, kterým směrem by se mohly ubírat další úvahy.

Nechť nadále (až do konce kapitoly) R značí vždy okruh $F[x,y]$. V dalším textu budeme definovat určitá čísla a polynomy, které se týkají algebry $A = Rx + Ry/I$. Kvůli tomu, že s jinou algebrou než s A pracovat nebudeme (a také pro větší přehlednost), nebudeme u daných objektů uvádět indexaci naznačující, že se vztahují k A. Aby nedošlo k nedorozumění, tak symboly pro tyto objekty nepoužijeme v jiném smyslu. Konkrétně jde o: $s_i, \bar{s}_i, S_i$ (čísla) a p_i (polynomy).

Nechť $A = Rx + Ry/I$ je algebra. Protože je konečně generovaná, a tedy konečné dimenze, je podle předchozí věty množina $\mathcal{B}_A$ konečná. Můžeme proto vyslovit následující definici.

Definice 22 *Nechť $A = Rx + Ry/I$ je algebra, $i \geq 0$.*

Označme $s_i = |\mathcal{B}_A \cap (\{i\} \times \mathbb{N}_0)| \in \mathbb{N}_0$.

Nechť A je algebra, $a \in A$ a $n \geq 1$ nejmenší takové, že $a^n = 0$. Číslo n se nazývá stupeň nilpotence prvku a a budeme jej značit $\|a\|$.

Uvědomme si ještě, jak vypadají polynomy $f \in Rx + Rx$, které jsou v normálním tvaru. Pro $M(f) = (i, j)$ je můžeme psát jako $f = \lambda.x^i(y^j - x.g)$, kde $0 \neq \lambda \in F$ a $g \in R$ je vhodný polynom. Speciálně pro $M(f) = (i, 0)$ je pak $f = \lambda.x^i$, pro nějaké $0 \neq \lambda \in F$.

Lemma 23 *Nechť $A = Rx + Ry/I$ je algebra, $\|x + I\| = n + 1$, $n \geq 0$. Pak platí:*

1) $s_0 \geq s_1 \geq \ldots \geq s_n > 0 = s_{n+1} = s_{n+2} = \cdots$,
2) $\sum_{i=0}^{\infty} s_i = \sum_{i=0}^{n} s_i = |\mathcal{B}_A| = 1 + dim A$,
3) $\mathcal{B}_A = \{\alpha|$ *ex. i takové, že* $0 \leq i \leq n,\ \alpha <_\Pi (i, s_i)\}$,
4) $\mathcal{C}_A = \{\alpha|\ $ *ex. i takové, že* $0 \leq i \leq n + 1,\ (i, s_i) \leq_\Pi \alpha\}$.

Důkaz: Označme $\mathcal{I}_i = \{\alpha|\ (i, 0) \leq_\Pi \alpha <_\Pi (i, s_i)\}$. Pak je $|\mathcal{I}_i| = s_i$. Z definice s_i a z bodu 1) a 2) předchozí věty máme snadno, že $\mathcal{I}_i = \mathcal{B}_A \cap (\{i\} \times \mathbb{N}_0))$. Je tedy $(i, s_i) \in \mathcal{C}_A$ (jinak by muselo být $(i, s_i) \in \mathcal{B}_A$ a tedy $(i, s_i) \in \mathcal{I}_i$, což by byl spor) a tudíž je $(i + 1, s_i) \in \mathcal{C}_A$. Musí tedy platit, že $s_{i+1} \leq s_i$ (kdyby ne pak by bylo $(i + 1, s_i) \in \mathcal{I}_{i+1} \subseteq \mathcal{B}_A$, což by byl spor).

Dále protože $x^{n+1} \equiv 0$, tak je $(n + 1, 0) \in \mathcal{C}_A$. $\mathcal{C}_A$ je horní množina a tedy $s_{n+1} = |\mathcal{B}_A \cap (\{n + 1\} \times \mathbb{N}_0)| = 0$. K tomu, že je $s_n > 0$, stačí ukázat, že $(n, 0) \in \mathcal{B}_A$. Pro $n = 0$ to plyne z předchozí věty (bod 2)). Nechť je tedy $n \geq 1$. Předpokládejme, že $(n, 0) \in \mathcal{C}_A$. Z definice $\mathcal{C}_A$ ex. polynom f v normálním tvaru takový, že $M(f) = (n, 0)$ a $f \equiv 0$. Normální tvar implikuje, že musí být $0 \equiv f = \lambda x^{(n,0)}$, $0 \neq \lambda \in F$, což je ale spor s definicí $\|x\|$. Je tedy skutečně $s_n > 0$.

Body 1) a 2) jsou nyní už zřejmé. Je také zřejmě $\mathcal{I}_i = \emptyset$ pro $i \geq n + 1$ (neboť $|\mathcal{I}_i| = s_i$). Tudíž máme $\mathcal{B}_A = \bigcup_{i=0}^{\infty}(\mathcal{B}_A \cap (\{i\} \times \mathbb{N}_0)) = \bigcup_{i=0}^{n} \mathcal{I}_i = \{\alpha|$ ex. i takové, že $0 \leq i \leq n,\ \alpha <_\Pi (i, s_i)\}$.

Nyní dokážeme poslední - bod 4): Protože $\mathcal{C}_A$ je horní množina a platí, že $(i, s_i) \in \mathcal{C}_A$ pro všechna i, je zřejmě $\{\alpha|$ ex. i takové, že $0 \leq i \leq n + 1$, $(i, s_i) \leq_\Pi \alpha\} \subseteq \mathcal{C}_A$.

Pro opačnou inkluzi předpokládejme $(i, j) \in \mathcal{C}_A$. Pokud je $n + 1 \leq i$, pak $(n + 1, s_{n+1}) = (n + 1, 0) \leq_\Pi (i, j)$. A pokud je $i \leq n$, pak musí být $(i, s_i) \leq_\Pi (i, j)$ (jinak by $(i, j) \in \mathcal{I}_i \subseteq \mathcal{B}_A$, což by byl spor). □

Vidíme tedy, že množina $\mathcal{B}_A$ má tvar jakýchsi "schodů".

Věta 24 *Nechť $A = Rx + Ry/I$ je algebra. Nechť $W \subseteq I$, všechny polynomy $q \in W$ jsou v normálním tvaru a $\mathcal{C}_A = \{\alpha |$ ex. $q \in W$ takové, že $M(q) \leq_\Pi \alpha\}$. Pak $I = \sum_{q \in W} Rq$.*

Důkaz: Označme $\tilde{I} = \sum_{q \in W} Rq$ a $\equiv_{\tilde{I}}$ kongruenci podle ideálu $\tilde{I}$. A je nilpotentní a tedy ex. $k \geq 1$, ze $x^k \equiv 0 \equiv y^k$. Tedy platí, že $(k,0),(0,k) \in \mathcal{C}_A$ a tudíž ex. $q_1, q_2 \in W$, že $(i_1, j_1) = M(q_1) \leq_\Pi (k,0)$ a $(i_2, j_2) = M(q_2) \leq_\Pi (0,k)$. Protože q_1, q_2 jsou v normálním tvaru můžeme bez újmy na obecnosti psát $x^{i_1} \equiv_{\tilde{I}} 0$ a $y^{j_2} - x.g \equiv_{\tilde{I}} 0$, kde g je vhodný polynom. Je tedy $y^{i_1 j_2} \equiv_{\tilde{I}} x^{i_1}.g^{i_1} \equiv_{\tilde{I}} 0$, takže $\tilde{A} = Rx + Ry/\tilde{I}$ je nilpotentní algebra (podle věty 17).

Zřejmě je $\tilde{I} \subseteq I$ a máme tedy přirozenou projekci $\pi : \tilde{A} \to A$, $\pi(f + \tilde{I}) = f + I$. Díky polynomům $q \in W$ je $M(q) \in \mathcal{C}_{\tilde{A}}$ a z předpokladu tudíž dostáváme, že $\mathcal{C}_A \subseteq \mathcal{C}_{\tilde{A}}$ a tedy $\mathcal{B}_{\tilde{A}} \subseteq \mathcal{B}_A$ neboli $dim\tilde{A} \leq dimA$. Odsud a z toho, že π je epimorfismus máme, že je to také izomorfismus. Je tedy $0 = ker\pi = I/\tilde{I}$ a tudíž je $I = \tilde{I}$, což jsme chtěli dokázat. □

Nechť $A = Rx + Ry/I$ je algebra. Z lemmatu 23 máme, že $(i, s_i) \in \mathcal{C}_A$ a díky definici $\mathcal{C}_A$ pomocí polynomů v normálním tvaru můžeme vyslovit následující "definici".

Definice 25 *Nechť $A = Rx + Ry/I$ je algebra, $\|x + I\| = n + 1$, $n \geq 0$. Pro $0 \leq i \leq n$ označme p_i takové polynomy, které jsou tvaru $p_i = x^i(y^{s_i} - x.f_i) \in I$, pro vhodné $f_i \in R$ a dále položme $p_{n+1} = x^{n+1} \in I$.*

Slovo definice bylo použito v uvozovkách oprávněně. Polynomy p_i totiž obecně nejsou jednoznačně určeny. To však pro naše účely není ani potřeba. My budeme prostě jen uvažovat jednu takovou volbu.

Věta 26 *Nechť $A = Rx + Ry/I$ je algebra, $\|x + I\| = n + 1$, $n \geq 0$. Nechť $f \equiv 0$ a $M(f) \geq (i,0)$.*

Pak $f \in Rp_i + \cdots + Rp_{n+1}$ pro $0 \leq i \leq n+1$ a $f \in Rx^{i-(n+1)}p_{n+1}$ pro $n + 1 \leq i$.

Důkaz: Pokud je $n + 1 \leq i$, pak je zřejmě $f = x^i.g$ pro nějaké $g \in R$, takže $f = g.x^{i-(n+1)}p_{n+1}$.

Nechť je tedy $0 \leq i < n+1$ pevně zvolené. Označme $q = f/x^i$ a $q_j = p_j/x^i$ pro j takové, že $i \leq j \leq n+1$. Definujme $\tilde{I} = Rq + Rq_i + \cdots + Rq_{n+1}$. Protože

$q_i = y^{s_i} - xf_i$ pro vhodné $f_i \in R$ a $q_{n+1} = x^{n+1-i}$, tak stejně jako v důkazu předchozí věty se dá snadno ukázat, že $\tilde{A} = Rx + Ry/\tilde{I}$ je nilpotentní algebra.

Označme nyní $\mathcal{C} = \{\alpha |$ ex. j takové, že $i \leq j \leq n+1,\ M(q_j) \leq_\Pi \alpha\}$. Ukážeme, že $\mathcal{C} = \mathcal{C}_{\tilde{A}}$.

$\subseteq$: Z definice $\mathcal{C}_{\tilde{A}}$ je zřejmě $M(q_j) \in \mathcal{C}_{\tilde{A}}$ a tedy $\mathcal{C} \subseteq \mathcal{C}_{\tilde{A}}$.

$\supseteq$: Protože platí $M(q_j) = (j, s_j) - (i, 0)$, tak máme, že $\mathcal{C} = \{\alpha |$ ex. j takové, že $i \leq j \leq n+1,\ (j, s_j) \leq_\Pi \alpha + (i, 0)\}$. Nechť je nyní $\alpha = (i', j') \in \mathcal{C}_{\tilde{A}}$. Existuje tedy polynom h takový, že $M(h) = \alpha$ a $h \in \tilde{I}$. Tudíž je $x^i h \in x^i \tilde{I} \subseteq I$ a $M(x^i h) = \alpha + (i, 0)$. Tedy $\alpha + (i, 0) \in \mathcal{C}_A$ a podle lemmatu 23 4) máme, že existuje j_0 takové, že $0 \leq j_0 \leq n+1$ a $(j_0, s_{j_0}) \leq_\Pi \alpha + (i, 0)$. Nyní tedy (vzhledem k uvedenému tvaru $\mathcal{C}$) stačí ukázat, že j_0 lze volit tak, aby $i \leq j_0 \leq n+1$. Předpokládejme, že $j_0 < i$. Pak je $s_i \leq s_{j_0}$ a protože současně máme $(j_0, s_{j_0}) \leq_\Pi \alpha + (i, 0) = (i' + i, j')$, tak zřejmě platí také, že $(i, s_i) \leq_\Pi (i' + i, j') = \alpha + (i, 0)$ (neboť je $i \leq i' + i$ a $s_i \leq s_{j_0} \leq j'$). Místo j_0 tedy můžeme použít i.

Ukázali jsme tak, že $\mathcal{C} = \mathcal{C}_A$ a podle předchozí věty (pro množinu $W = \{q_i, \ldots, q_{n+1}\} \subseteq \tilde{I}$) dostáváme, že $Rq_i + \cdots + Rq_{n+1} = \tilde{I} \ni q$. Tento vztah nyní stačí už jen přenásobit x^i. □

Důsledek 27 *Nechť $A = Rx + Ry/I$ je algebra, $\|x + I\| = n+1$, $n \geq 0$. Pak platí:*

1) $I = Rp_1 + \cdots + Rp_{n+1}$,

2) $xp_i \in Rp_{i+1} + \cdots + Rp_{n+1}$ pro $0 \leq i \leq n$,

3) $y^{s_{i-1}-s_i} p_i - xp_{i-1} \in Rp_{i+1} + \cdots + Rp_{n+1}$ pro $1 \leq i \leq n$, a
$y^{s_n - s_{n+1}} p_{n+1} - xp_n \in Rxp_{n+1}$.

Důkaz: Plyne snadno z lemmatu 23 4) a předchozí věty 26, pokud uvážíme, že

1) $M(f) \geq (0, 0)$ pro všechny $f \in I$,

2) $M(xp_i) = (i+1, s_i) \geq (i+1, 0)$,

3) $y^{s_{i-1}-s_i} p_i - xp_{i-1} = x^i(y^{s_{i-1}} - x.y^{s_{i-1}-s_i} f_i) - x^i(y^{s_{i-1}} - x.f_{i-1}) = x^{i+1}(f_{i-1} - y^{s_{i-1}-s_i} f_i)$ pro vhodné $f_i \in R$ (a $f_{n+1} = 0$).

A tedy $M(y^{s_{i-1}-s_i} p_i - xp_{i-1}) \geq (i+1, 0)$. □

Nyní se podíváme, jak se dosud zjištěná fakta dají použít pro popis vztahu algeber A a $A^{(p)}$.

Věta 28 *Nechť $A = Rx + Ry/I$ a (A, p) je dobrý pár generovaný dvojicí $(x+I, y+I)$. Označme $J = \{f \in R |\ f(x^p, y^p) \in I\}$. Pak $A^{(p)} = \langle x^p + I, y^p + I\rangle$ a $\phi : Rx + Ry/J \to A^{(p)}$, $\phi(f + J) = f + I$ je izomorfismus F-algeber.*

Důkaz: J je zřejmě ideál v R. Zbytek plyne snadno z definice dobrého páru a z věty 17, pokud uvážíme, že $f(x^p + I, y^p + I) = 0 + I \Leftrightarrow f(x^p, y^p) \in I$. □

Tato věta nám tedy říká, že pro $A^{(p)}$ smíme použít předchozí výsledky. Můžeme tedy vyslovit následující definici.

Definice 29 *Nechť $A = Rx + Ry/I$ a (A, p) je dobrý pár generovaný dvojicí $(x + I, y + I)$, $J = \{f \in R |\ f(x^p, y^p) \in I\}$. Definujme $\mathcal{C}_{A^{(p)}} = \mathcal{C}_{Rx+Ry/J}$ a $\mathcal{B}_{A^{(p)}} = \mathcal{B}_{Rx+Ry/J}$.*

Dále položme $\bar{s}_i = |\mathcal{B}_{A^{(p)}} \cap (\{i\} \times \mathbb{N}_0)|$ a $S_i = \sum_{k=pi}^{pi+p-1} s_k$, pro $i \geq 0$.

Nechť je navíc $dimA > 0$ a nechť α_0 je maximální prvek $\mathcal{B}_A$ vzhledem k $\leq$. Označme $w_A = x^{\alpha_0} \in Rx + Ry$.

Lemma 30 *Nechť A je nilpotentní algebra, $a \in A$. Nechť $\|a\| = n+1$, $n \geq 0$. Pak $\|a^p\| = \left\lfloor \frac{n}{p} \right\rfloor + 1$.*

Důkaz: Plyne z definice stupně nilpotence prvku a nerovnosti $p \left\lfloor \frac{n}{p} \right\rfloor \leq n < p(\left\lfloor \frac{n}{p} \right\rfloor + 1)$. □

Důsledek 31 *Nechť $A = Rx + Ry/I$ je algebra, $\|x + I\| = n + 1$, $n \geq 0$. Nechť (A, p) je dobrý pár generovaný dvojicí $(x + I, y + I)$. Pak platí:*

1) $\bar{s}_0 \geq \bar{s}_1 \geq \ldots \geq \bar{s}_{\lfloor \frac{n}{p} \rfloor} > 0 = \bar{s}_{\lfloor \frac{n}{p} \rfloor + 1} = \bar{s}_{\lfloor \frac{n}{p} \rfloor + 2} = \cdots$,

2) $\sum_{i=0}^{\infty} \bar{s}_i = \sum_{i=0}^{\lfloor \frac{n}{p} \rfloor} \bar{s}_i = |\mathcal{B}_{A^{(p)}}| = 1 + dimA^{(p)}$,

3) $\mathcal{B}_{A^{(p)}} = \{\alpha |$ *ex. i takové, že* $0 \leq i \leq \left\lfloor \frac{n}{p} \right\rfloor,\ \alpha <_\Pi (i, \bar{s}_i)\}$,

4) $\mathcal{C}_{A^{(p)}} = \{\alpha |$ *ex. i takové, že* $0 \leq i \leq \left\lfloor \frac{n}{p} \right\rfloor + 1,\ (i, \bar{s}_i) \leq_\Pi \alpha\}$.

5) množina $\{(x^\alpha)^p + I |\ (0, 0) \neq \alpha \in \mathcal{B}_{A^{(p)}}\}$ *je bází* $A^{(p)}$,

6) $\sum_{i=0}^{\infty} S_i = \sum_{i=0}^{\left\lfloor \frac{n}{p} \right\rfloor} S_i = 1 + dimA.$

7) Nechť navíc je $f \in Rx + Ry$ *takové, že* $M(f) = (i, j)$, $y^m f(x^p, y^p) \equiv 0$. *Pak* $M(y^m f(x^p, y^p)) = (pi, pj + m)$ *a* $\bar{s}_i \leq \left\lceil \frac{pj+m}{p} \right\rceil$.

Důkaz: 1) - 5) plyne z věty 28, lemmatu 30 a lemmatu 23 2).

6) z nerovnosti $n + 1 \leq p(\left\lfloor \frac{n}{p} \right\rfloor + 1)$ a lemmatu 23 1) máme, že $s_i = 0$ pro $p(\left\lfloor \frac{n}{p} \right\rfloor + 1) \leq i$. Zbytek plyne z definice S_i a lemmatu 23 2).

7) Pokud je $\left\lfloor \frac{n}{p} \right\rfloor < i$ je $\bar{s}_i = 0$ podle 1) a tvrzení je tedy zřejmé. Nechť je tedy $i \leq \left\lfloor \frac{n}{p} \right\rfloor$. Zřejmě je $M(y^m f(x^p, y^p)) = M(y^m) + M(f(x^p, y^p)) = (0, m) + p \cdot M(f)$. Ať J je ideál z definice 29. Uvažujme $m = pk + r$, pro $k \geq 0$, $0 \leq r < p$.

Pokud je $r = 0$, pak platí $M(y^k f) = (i, j + k)$ a $y^k f \in J$ (neboť $(y^k f)(x^p, y^p) = y^m f(x^p, y^p) \in I$). Je tedy $(i, j + k) \in \mathcal{C}_{A^{(p)}}$. Z popisu $\mathcal{C}_{A^{(p)}}$ pomocí lemmatu 23 3) a 4) tak dostáváme, že musí platit $\bar{s}_i \leq j + k = \left\lceil \frac{pj+m}{p} \right\rceil$ (v opačném případě by totiž bylo $(i, j + k) <_{\Pi} (i, \bar{s}_i)$ a tedy podle lemmatu 23 3) by $(i, j + k) \in \mathcal{B}_{A^{(p)}}$, což by byl spor).

Pokud je nyní $r > 0$, pak podobně máme $M(y^{k+1} f) = (i, j + k + 1)$ a $y^{k+1} f \in J$ (neboť je $(y^{k+1} f)(x^p, y^p) = y^{m+p-r} f(x^p, y^p) \in I$). A tedy podobně dostáváme $\bar{s}_i \leq j + k + 1 = \left\lceil \frac{pj+m}{p} \right\rceil$. □

Uvedený důsledek už naznačuje, kterým směrem povedeme naše další úvahy. Budeme se snažit získat odhad zhruba ve tvaru "$p.\bar{s}_i \leq S_i$" a to tak, že se pokusíme najít vhodné polynomy takové, že $y^m f(x^p, y^p) \equiv 0$ a $M(f) = (i, j)$. (A kde je vzít? Zhruba řečeno to uděláme tak, že vezmeme ty, co už máme (tj. p_i) a budeme je posouvat "zpět" a "nahoru" (tj. dělit x a násobit y). Tím se nám také v exponentu y objeví součet s_j.)

Protože v odhadování hraje roli "horní celá část" (jak bylo vidět z právě provedeného důkazu), je potřeba si u polynomů, které budeme používat, vytvořit určitou rezervu vzhledem k násobení prvkem y (tj. vzhledem k posunování polynomu směrem vzhůru). To byl také důvod, proč jsme zavedli prvek w_A (viz definice 29).

Lemma 32 *Nechť* $A = Rx + Ry/I$ *je algebra,* $dimA > 0$, $\|x + I\| = n + 1$, $n \geq 0$. *Pak platí:*

1) $xw_A \equiv yw_A \equiv 0$ *a tedy* $[w_A + I]$ *je ideál v* A *(tj.* $\forall h \in R, hw_A + I \in [w_A + I]$*).*

2) Nechť $1 \leq i \leq n+1$, $f \equiv 0$, $M(f) \geq (i,0)$. *Pak* $y^{s_{i-1}-1}(f/x) + I \in [w_A + I]$.

3) Nechť $0 \leq j < i \leq n+1$, $f \equiv 0$, $M(f) \geq (i,0)$.

a) Položme $l = (\sum_{k=j}^{i-1} s_k) - 1$, *pak* $y^l(f/x^{i-j}) + I \in [w_A + I]$.

b) Nechť navíc je $s_{i-1} \geq s_{n-1} + 1$. *Položme* $l' = \sum_{k=j}^{i-1}(s_k - 1)$, *pak* $y^{l'}(f/x^{i-j}) + I \in [w_A + I]$.

Důkaz: 1) Nechť α_0 je maximální prvek v $\mathcal{B}_A$. Z lemmatu 23 3) vyplývá, že $\alpha_0 = (n, s_n - 1)$. Protože máme $0 \equiv p_n = x^n(y^{s_n} - x.f_n)$ a $0 \equiv p_{n+1} \equiv x^{n+1}$, tak platí, že $yw_A = y^{s_n}x^n \equiv x^{n+1}f_n \equiv 0$ a $xw_A = x^{n+1}y^{s_n-1} \equiv 0$.

Pro další úvahy si uvědomme, že díky $dimA > 0$ platí následující: Nechť $1 \leq i \leq n+1$, $f \equiv 0$, $M(f) \geq (i,0)$. Pak $y^{s_{i-1}-1}(f/x) \in Rx + Ry$. (Přepokládejme, že tomu tak není - pak by muselo být $M(y^{s_{i-1}-1}(f/x)) = (0,0)$ a tedy $s_{i-1} = 1$ a $M(f) = (1,0)$. Protože $f \equiv 0$, bylo by $(1,0) \in \mathcal{C}_A$ a tedy $\|x + I\| = 1$, tj. $n = 0$. Měli bychom tudíž $i = 1$ a tedy podle lemmatu 23 by muselo být $\mathcal{B}_A = \{(0,0)\}$ neboli $dimA = 0$, což by byl spor.) Toto pozorování nám tedy říká, že po výše uvedené transformaci polynomu f nemůžeme vypadnout z algebry $Rx + Ry/I$.

Pro důkaz bodu 2) a 3) nyní podle 1) stačí ukázat, že dané polynomy umíme napsat (až na kongruenci) ve tvaru hw_A pro nějaké $h \in R$.

2) Nechť $i = n+1$. Pak $f = x^{n+1}g$ pro $g \in R$, a tedy $y^{s_n-1}(f/x) = y^{s_n-1}x^n f = fw_A$.

Dále budeme postupovat následující indukcí. Nechť $1 \leq i < n+1$ a předpokládejme, že pro všechna k taková, že $i < k \leq n+1$ tvrzení 2) platí. Mějme tedy f takové, že $f \equiv 0$ a $M(f) \geq (i,0)$. Podle věty 26 máme $f = \sum_{k=i}^{n+1} g_k p_k$, kde $g_k \in R$, a podle důsledku 27 3) je $y^{s_{i-1}-s_i}(p_i/x) \equiv \sum_{k=i+1}^{n+1} h_k(p_k/x)$, pro $h_k \in R$. Můžeme tedy psát

$$y^{s_{i-1}-1}(f/x) = y^{s_{i-1}-1}\sum_{k=i}^{n+1} g_k(p_k/x) = g_i y^{s_i-1}\, y^{s_{i-1}-s_i}\,(p_i/x) +$$

$$+\; y^{s_{i-1}-1}\sum_{k=i+1}^{n+1} g_k(p_k/x) \equiv g_i y^{s_i-1}\sum_{k=i+1}^{n+1} h_k(p_k/x) +\; y^{s_{i-1}-1}\sum_{k=i+1}^{n+1} g_k(p_k/x) =$$

$$= \sum_{k=i+1}^{n+1}(g_i h_k + y^{s_{i-1}-s_i}g_k)y^{s_i-1}(p_k/x).$$

Protože $s_i \geq s_k$ pro $i < k \leq n+1$, tak z indukčního předpokladu (a díky bodu 1)) je $y^{s_i-1}(p_k/x) + I \in [w_A + I]$ a podle výše uvedého výpočtu je tedy $y^{s_i-1}(p_i/x) + I \in [w_A + I]$, což jsme chtěli dokázat.

3) a): Budeme postupovat indukcí podle $k = i - j$. Pro $k = 1$ to máme už dokázané z bodu 2). Mějme tedy $0 < j < i \leq n+1$ a f takové, že $f \equiv 0$ a $M(f) \geq (i, 0)$ a předpokládejme, že platí $y^l(f/x^{i-j}) + I \in [w_A + I]$, kde $l = (\sum_{k=j}^{i-1} s_k) - 1$. Položme $q = y^l(f/x^{i-j})$. Díky bodu 1) máme, že $yq \equiv 0$ a dále je $M(yq) = M(y^{l+1}(f/x^{i-j})) \geq (j, 0)$ (neboť $M(f) \geq (i, 0)$). Podle už dokázaného bodu 2) tedy máme $y^{s_{j-1}-1}(yq/x) + I \in [w_A + I]$, což je zřejmě to, co jsme chtěli ukázat.

b): Nejdříve si uvědomíme, že pro $s \geq s_{n-1}$ a $n \geq 1$ platí $y^s(w_A/x) + I \in [w_A + I]$: Vzhledem k 1) to zřejmě stačí ukaáat jen pro $s = s_{n-1}$. Protože $0 \equiv p_{n-1} = x^{n-1}(y^{s_{n-1}} - xf_{n-1})$ a $w_A = x^n y^{s_n-1}$ tak můžeme psát $y^{s_{n-1}}(w_A/x) = y^{s_n-1}(x^{n-1}y^{s_{n-1}}) \equiv y^{s_n-1}(x^n f_{n-1}) = w_A f_{n-1}$, což jsme chtěli ukázat.

Postupujme dále opět indukcí podle $k = i - j$. Pro $k = 1$ to máme opět už dokázáno v bodu 2). Mějme tedy $0 < j < i \leq n+1$ a f takové, že $f \equiv 0$ a $M(f) \geq (i, 0)$ a předpokládejme, že platí $y^{l'}(f/x^{i-j}) + I \in [w_A + I]$, kde $l' = \sum_{k=j}^{i-1}(s_k - 1)$. Položme $q = y^{l'}(f/x^{i-j})$. Je tedy $q - \lambda w_A \equiv 0$, pro vhodné $\lambda \in F$. Podle lemmatu 12 5) je $M(q - \lambda w_A) \geq min_{\leq}\{M(q), M(-\lambda w_A)\} \geq min_{\leq}\{(j, 0), (n, s_n - 1)\} = (j, 0)$. Můžeme tedy pro $q - \lambda w_A$ použít už dokázaný bod 2) a dostáváme tak $y^{s_{j-1}-1}(q - \lambda w_A)/x \equiv \mu w_A$ pro nějaké $\mu \in F$. Protože $s_{j-1} - 1 \geq s_{i-1} - 1 \geq s_{n-1}$, tak podle pozorování pro polynom w_A (ze začátku důkazu části 3)b)) máme $y^{s_{j-1}-1}(q/x) \equiv \lambda y^{s_{j-1}-1}(w_A/x) + \mu w_A \equiv \lambda h w_A + \mu w_A = (\lambda h + \mu) w_A$, pro nějaké $h \in R$. Což jsme chtěli ukázat. □

Věta 33 *Nechť $A = Rx + Ry/I$ je algebra, $dim A > 0$, $\|x + I\| = n+1$, $n \geq 0$, $p \geq 2$. Nechť $0 \leq i \leq \left\lfloor \frac{n}{p} \right\rfloor$ a nechť m_i je nejmenší takové, že $pi \leq m_i \leq pi+p-1$ a $s_{pi} \geq \ldots \geq s_{m_i} = s_{m_i+1} = \cdots s_{pi+p-1}$. Označme $l_i = [\sum_{k=pi}^{m_i-1}(s_k - 1)] - (p-1)s_{m_i}$. Pak platí:*

1) $(i < \left\lfloor \frac{n}{p} \right\rfloor \ \& \ l_i \geq 0) \ \Rightarrow \ y^{l_i} x^{pi}(p_{m_i}/x^{m_i})^p + I \in [w_A + I]$,

2) $(i < \left\lfloor \frac{n}{p} \right\rfloor \ \& \ l_i < 0) \ \Rightarrow \ x^{pi}(p_{m_i}/x^{m_i})^p \equiv 0$,

3) $i = \left\lfloor \frac{n}{p} \right\rfloor \ \Rightarrow \ y^{S_i - 1} x^{pi} + I \in [w_A + I]$.

Důkaz: Nechť $i < \left\lfloor \frac{n}{p} \right\rfloor$. Vezměme $l \geq 0$. Protože $0 \equiv p_{m_i} = x^{m_i}(y^{s_{m_i}} - xf_{m_i})$ tak použitím binomické věty (a pak jen změnou indexace $j' = pi + j$) dostáváme:

$$y^l x^{pi}(p_{m_i}/x^{m_i})^p = y^l x^{pi}(p_{m_i}/x^{m_i}) \cdot (p_{m_i}/x^{m_i})^{p-1} = y^l(p_{m_i}/x^{m_i - pi}) \cdot$$

$$\cdot (y^{s_{m_i}} - xf_{m_i})^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j}(-f_{m_i})^j \; y^{l+s_{m_i}(p-1-j)}(p_{m_i}/x^{m_i-(pi+j)}) =$$

$$= \sum_{j'=pi}^{pi+p-1} \binom{p-1}{j'-pi}(-f_{m_i})^{j'-pi} \; y^{l+s_{m_i}(pi+p-1-j')}(p_{m_i}/x^{m_i-j'}) \equiv$$

$$\equiv \sum_{j=pi}^{m_i-1} \binom{p-1}{j-pi}(-f_{m_i})^{j-pi} \; y^{l+s_{m_i}(pi+p-1-j)}(p_{m_i}/x^{m_i-j})$$

(při poslední úpravě jsme vynechali členy, pro které je $m_i - j' \leq 0$, neboť ty jsou díky $p_{m_i} \equiv 0$ kongruentní s 0). Odvození zřejmě platí i pro $m_i = pi$. Pokud je tedy nyní $m_i = pi$, pak je $l_i < 0$ a podle uvedeného výpočtu dostáváme příslušné tvrzení (tj. kongruenci s nulou).

Nechť je teď $m_i > pi$. Podle výpočtu (a podle lemmatu 32 1)) zřejmě stačí ukázat, že $y^{l+s_{m_i}(pi+p-1-j)}(p_{m_i}/x^{m_i-j}) + I$ leží buď v $[w_A + I]$ pro $l_i \geq 0$ a $l = l_i$ nebo je rovno $0 + I$ pro $l_i < 0$ a $l = 0$. Využijeme předchozí větu 32 3b).

Uvažme tedy nerovnost $l + s_{m_i}(pi + p - 1 - j) \geq \sum_{k=j}^{m_i-1}(s_k - 1)$, pro $pi \leq j < m_i$. Po snadné úpravě zjistíme, že je ekvivalentní s nerovností
$l \geq [\sum_{k=j}^{m_i-1}(s_k - (s_{m_i} + 1))] - (pi + p - 1 - m_i)s_{m_i}$, pro $pi \leq j < m_i$.

Platí $l_i = [\sum_{k=pi}^{m_i-1}(s_k - 1)] - (p-1)s_{m_i} = [\sum_{k=pi}^{m_i-1}(s_k - (s_{m_i}+1))] - (pi+p-1-m_i)s_{m_i}$ a protože v předchozí nerovnosti je pravá strana rostoucí funkcí v proměnné j (neboť $s_k \geq s_{m_i} + 1$ pro $pi \leq k < m_i$), je tato nerovnost splněna pro všechna j, $pi \leq j < m_i$, právě když $l \geq l_i$. Podobně když v těchto nerovnostech nahradíme nerovnost $\geq$ ostrou nerovností $>$, tak máme, že jsou splněny pro všechna j taková, že $pi \leq j < m_i$, právě když $l > l_i$.

Pro použití lemmatu 32 3a) ještě potřebujeme vědět následující: protože $i < \left\lfloor \frac{n}{p} \right\rfloor$, je $m_i \leq pi < p\left\lfloor \frac{n}{p} \right\rfloor \leq n$ a tedy máme (z definice m_i), že $s_{m_i-1} \geq s_{m_i} + 1 \geq s_{n-1} + 1$.

Nechť je tedy nyní konečně $l_i \geq 0$. Pak, položíme-li $l = l_i$, dostáváme (jak už bylo řečeno) z lemmatu 32 1) a 3b) požadované tvrzení. Podobně pokud je $l_i < 0$ a položíme-li $l = 0$, pak platí, že $l > l_i$. Díky ostrým nerovnostem tak opět z lemmatu 32 1) a 3b) máme, že $y^{l+s_{m_i}(pi+p-1-j)}(p_{m_i}/x^{m_i-j}) + I = 0 + I$

a tedy opět dostáváme požadované tvrzení.

Nechť je nyní $i = \left\lfloor \frac{n}{p} \right\rfloor$. Pak je $0 \leq pi \leq n$ a z lemmatu 32 3a) (při volbě $f = p_{n+1} = x^{n+1} \equiv 0$) dostáváme, že $[w_A + I] \ni y^m x^{-(n+1-pi)} f + I = y^m x^{pi} + I$, kde $m = (\sum_{k=pi}^{n} s_k) - 1 = S_i - 1$ (poslední rovnost platí, protože $s_k = 0$ pro $n+1 \leq k \leq p \left\lfloor \frac{n}{p} \right\rfloor + p - 1$).

Tímto je důkaz ukončen. □

Věta 34 *Nechť $A = Rx + Ry/I$ je algebra, $dim A > 0$, $\|x + I\| = n+1$, $n \geq 0$. Nechť (A, p) je dobrý pár generovaný dvojící $(x + I, y + I)$. Pro $0 \leq i \leq \left\lfloor \frac{n}{p} \right\rfloor$ pak nastává alespoň jedna z následujících situací:*

1) $p\bar{s}_i \leq S_i$,

2) ex. $k \geq 0$, $f \in Rx + Ry$, $0 \neq \lambda \in F$ takové, že $f(x^p, y^p) \equiv \lambda w_A$, $M(f) = (i, k)$, $S_i = pk + p - 1$, $p\bar{s}_i \leq S_i + 1$,

3) $i = \left\lfloor \frac{n}{p} \right\rfloor$ a ex. $k \geq 0$, $0 \neq \lambda \in F$ takové, že $(i, k) \neq (0, 0)$, $x^{pi} y^{pk} \equiv \lambda w_A$, $S_i = pk + 1$, $p\bar{s}_i \leq S_i + p - 1$,

4) $i = \left\lfloor \frac{n}{p} \right\rfloor$ a $p\bar{s}_i \leq S_i + p - 2$.

Důkaz: Použijeme předchozí větu. Nechť l_i a m_i mají stejný význam jako v předchozí větě.

A) Nechť je $i < \left\lfloor \frac{n}{p} \right\rfloor$ a $l_i \geq 0$. Pak musí být zřejmě $m_i \geq pi + 1$ a $s_k \geq 1$ pro $pi \leq j \leq pi + p - 1$ (neboť je $pi + p - 1 \leq n$). Máme tedy $ps_{m_i} + l_i = ps_{m_i} + [\sum_{k=pi}^{m_i - 1} (s_k - 1)] - (p-1)s_{m_i} = s_{m_i} + \sum_{k=pi}^{m_i - 1} (s_k - 1) \leq s_{m_i} + \sum_{k=pi}^{m_i - 1} (s_k - 1) + \sum_{k=m_i+1}^{ip+p-1} (s_k - 1) = S_i - (p-1)$. Podle věty 33 1) ex. $\mu \in F$, že $y^{l_i} x^{pi} (p_{m_i}/x^{m_i})^p \equiv \mu w_A$. Protože je $m_i < n + 1$, tak platí, že $(i, s_{m_i}) \neq (0, 0)$. Můžeme tedy použít definici dobrého páru a máme tudíž, že ex. $g \in Rx + Ry$ takové, že $x^{pi}(p_{m_i}/x^{m_i})^p \equiv g(x^p, y^p)$ a $M(g) \leq_\Pi M(x^i(p_{m_i}/x^{m_i})) = (i, s_{m_i})$. Nechť je $M(g) = (i', s)$, pak celkem máme, že $y^{l_i} x^{p(i-i')} g(x^p, y^p) \equiv \nu w_A$ pro nějaké $\nu \in F$ (obecně různé od μ). Přitom je zřejmě $M(x^{i-i'} g) = (i, s)$ a $s \leq s_{m_i}$.

Nechť je nyní

i) $S_i = pk + r$, $k \geq 0$, $0 \leq r \leq p - 2$. Pak z lemmatu 32 1) je $y^{l_i+1} x^{p(i-i')} g(x^p, y^p) \equiv 0$ a podle důsledku 31 dostáváme $\bar{s}_i \leq \left\lceil \frac{ps + l_i + 1}{p} \right\rceil \leq$

$\left\lceil \frac{ps_{m_i}+l_i+1}{p} \right\rceil \leq \left\lceil \frac{S_i-(p-1)+1}{p} \right\rceil = \left\lceil \frac{pk+r+2-p}{p} \right\rceil = k + \left\lceil \frac{r+2-p}{p} \right\rceil \leq k + \frac{r}{p} = \frac{S_i}{p}$. (dostali jsme případ 1))

ii) $S_i = pk + p - 1$, $k \geq 0$. Položme $l = S_i - (p-1) - (ps + l_0) \geq 0$ (nezápornost l plyne z odhadu výše). Pak dostáváme $y^{l_i+l}x^{p(i-i')}g(x^p, y^p) \equiv \lambda w_A$ pro nějaké $\lambda \in F$. Pokud je $\lambda = 0$, pak podle důsledku 31 je $\bar{s}_i \leq \left\lceil \frac{ps+l_i+l}{p} \right\rceil = \left\lceil \frac{S_i-(p-1)}{p} \right\rceil = k \leq \frac{S_i}{p}$. (dostali jsme případ 1))

Nechť je $\lambda \neq 0$. Položme $f = y^{k-s}x^{i-i'}g$ (zřejmě z definice l je $k - s \geq 0$). Máme $M(y^{k-s}x^{i-i'}g) = (i - i', k - s) + (i, s) = (i, k)$. Podle lemmatu 32 1) je $y^{l_i+l+1}x^{p(i-i')}g(x^p, y^p) \equiv 0$ a tedy podle důsledku 31 máme $\bar{s}_i \leq \left\lceil \frac{ps+l_i+l+1}{p} \right\rceil = \left\lceil \frac{pk+1}{p} \right\rceil = k + 1 = \frac{S_i+1}{p}$. (dostali jsme případ 2))

B) Nechť je $i < \left\lfloor \frac{n}{p} \right\rfloor$ a $l_i < 0$. Podle věty 33 2) je $x^{pi}(p_{m_i}/x^{m_i})^p \equiv 0$. Ze stejných důvodů jako v části A) můžeme použít definici dobrého páru a dostáváme tak, že ex. $g \in Rx + Ry$ takový, že $x^{pi}(p_{m_i}/x^{m_i})^p \equiv g(x^p, y^p)$ a $M(g) \leq_\Pi M(x^i(p_{m_i}/x^{m_i})) = (i, s_{m_i})$. Necht je $M(g) = (i', s)$. Pak dostáváme, že $x^{p(i-i')}g(x^p, y^p) \equiv 0$, $M(x^{i-i'}g) = (i, s)$ a $s \leq s_{m_i}$. Z definice m_i máme snadno, že $s_{m_i} \leq s_k$ pro $pi \leq k \leq pi + p - 1$. Podle důsledku 31 tak platí, že $p\bar{s}_i \leq ps \leq ps_{m_i} \leq \sum_{k=pi}^{pi+p-1} s_k = S_i$. (dostali jsme případ 1))

C) Nechť je $i = \left\lfloor \frac{n}{p} \right\rfloor$. Podle věty 33 3) ex. $\lambda \in F$, že $y^{S_i-1}x^{pi} \equiv \lambda w_A$. Podle lemmatu 32 1) je pak $y^{S_i}x^{pi} \equiv 0$. Zřejmě platí $S_i \geq 1$ (viz definice S_i a lemma 23 1)). Musí také být $(i, S_i - 1) \neq (0, 0)$ (jinak by $0 = i = \left\lfloor \frac{n}{p} \right\rfloor$ a $S_0 = 1$, což by podle důsledku 31 6) znamenalo, že $dim A = 0$, což by byl spor s předpokladem).

i) Nechť je $S_i = pk$, $k \geq 1$. Podle důsledku 31 máme, že $\bar{s}_i \leq \left\lceil \frac{S_i}{p} \right\rceil = \frac{S_i}{p}$. (dostali jsme případ 1))

ii) Nechť je $S_i = pk + 1$, $k \geq 0$. Pokud $\lambda = 0$, pak z důsledku 31 je $\bar{s}_i \leq \left\lceil \frac{S_i-1}{p} \right\rceil = k = \frac{S_i}{p}$. (dostali jsme případ 1))

Nechť je $\lambda \neq 0$. Podle důsledku 31 máme, že $\bar{s}_i \leq \left\lceil \frac{S_i}{p} \right\rceil = \left\lceil \frac{pk+1}{p} \right\rceil = k+1 = \frac{S_i+p-1}{p}$. (dostali jsme případ 3)).

iii) Nechť je $S_i = pk + r$, $k \geq 0$, $2 \leq r < p$. Podle důsledku 31 je $\bar{s}_i \leq \left\lceil \frac{S_i}{p} \right\rceil = \left\lceil \frac{pk+r}{p} \right\rceil = k + 1 \leq \frac{S_i+p-2}{p}$. (dostali jsme případ 4)) □

Pozorování 35 *Mějme stejné předpoklady jako ve větě 34. Nechť* $f, g \in Rx +$

Ry jsou takové, že $M(f) < M(g)$ *a* $f(x^p, y^p) \equiv \lambda w_A$, $g(x^p, y^p) \equiv \mu w_A$, *kde* $\lambda, \mu \in F$, $\mu \neq 0$.

Pak pro $q = f - \frac{\lambda}{\mu} g$ *platí* $M(q) = M(f)$ *a* $q(x^p, y^p) \equiv 0$.

Pokud je navíc $M(f) = (i, k)$ *a* $S_i = pk + p - 1$, *pak z důsledku 31 dostáváme* $\bar{s}_i \leq \left\lceil \frac{pk}{p} \right\rceil = k = \frac{S_i - (p-1)}{p} \leq \frac{S_i}{p}$.

(tj. případ 1) z věty 34)

Důkaz: Zřejmý. □

Věta 36 *Nechť* $A = Rx + Ry/I$ *je algebra. Nechť* (A, p) *je dobrý pár generovaný dvojicí* $(x + I, y + I)$. *Pak* $p \cdot dim A^{(p)} \leq dim A$.

Důkaz: Pokud je $dim A = 0$, je to zřejmé. Nechť je tedy $dim A > 0$.

Nechť $\|x + I\| = n + 1$. Podle důsledku 31 je $\sum_{i=0}^{\lfloor \frac{n}{p} \rfloor} S_i = 1 + dim A$ a $\sum_{i=o}^{\lfloor \frac{n}{p} \rfloor} \bar{s}_i = 1 + dim A^{(p)}$.

Nechť je nejdříve $\left\lfloor \frac{n}{p} \right\rfloor = 0$. Podle předchozí věty 34 3) je tedy $p \cdot dim A^{(p)} = p\bar{s}_0 - p \leq (S_0 + p - 1) - p = dim A$.

Nechť je nyní $\left\lfloor \frac{n}{p} \right\rfloor \geq 1$. Označme $i_0 = \left\lfloor \frac{n}{p} \right\rfloor$. Důkaz rozdělíme na dva případy.

A) Nechť i_0 splňuje bod 1) nebo 4) z věty 34. Pak zřejmě $ps_{i_0} \leq S_{i_0} + p - 2$. Uvažme množinu $M = \{i |\ 0 \leq i < i_0,\ i$ splňuje bod 2) z věty 34) $\}$. Pokud je $M \neq \emptyset$ označme i_1 největší prvek M a pokud je $M = \emptyset$, pak položme $i_1 = 0$. Podle předchozího pozorování 35, pak vždy dostáváme $ps_{i_1} \leq S_{i_1} + 1$ a $ps_i \leq S_i$ pro $i \neq i_0, i_1$. Můžeme tedy psát $p \cdot dim A^{(p)} = p\bar{s}_{i_0} + p\bar{s}_{i_1} + (p. \sum_{i \neq i_0, i_1} \bar{s}_i) - p \leq (S_{i_0} + p - 2) + (S_{i_1} + 1) + (\sum_{i \neq i_0, i_1} S_i) - p = (\sum_i S_i) - 1 = dim A$.

B) Nechť i_0 splňuje bod 2) nebo 3) z věty 34. Pak zřejmě $ps_{i_0} \leq S_{i_0} + p - 1$. Pro i takové, že $0 \leq i < i_0$ pak podle předchozího pozorování 35 dostáváme, že $p\bar{s}_i \leq S_i$. Můžeme tedy psát $p \cdot dim A^{(p)} = p\bar{s}_{i_0} + (p. \sum_{i \neq i_0} \bar{s}_i) - p \leq (S_{i_0} + p - 1) + (\sum_{i \neq i_0} S_i) - p = (\sum_i S_i) - 1 = dim A$. □

Dokázali jsme tak konečně tvrzení **(T1)** ze začátku kapitoly. (Důkaz plyne z vět 17 1) a 36).) Připomínáme ještě, že tvrzení **(T2)** plyne z věty 16.

Kapitola 4

Dodatek

Zde si nejdříve dokážeme větu, která nám umožní konstruovat příklady nilpotentních 2-generovaných algeber, které budou mít vhodní vlastnosti.

I v této kapitole mějme vždy $R = F[x, y]$ (pokud nebude řečeno jinak). Označení "algebra" pak bude stále znamenat nilpotentní algebru.

Věta 37 *Nechť $n, s'_i \geq 0$. Nechť $p'_i \in R$ jsou polynomy pro $0 \leq i \leq n+1$ a nechť jsou splněny následující předpoklady:*

1) $s'_0 \geq \ldots \geq s'_n > 0 = s'_{n+1}$,

2) $p'_0 = y^{s'_0} - xf_0$ kde $f_0 \in R$, $M(p'_i) = (i, s'_i)$ pro $1 \leq i \leq n$ a $p'_{n+1} = x^{n+1}$,

3) $xp'_i \in Rp'_{i+1} + \cdots + Rp'_{n+1}$ pro $0 \leq i \leq n$.

Položme $I = Rp'_0 + \cdots + Rp'_{n+1}$. Pak $A = Rx + Ry/I$ je nilpotentní algebra, $\|x + I\| = n+1$, $s_i = s'_i$ pro $0 \leq i \leq n+1$ a $\mathcal{B}_A = \{\alpha |$ ex. i takové, že $0 \leq i \leq n,\ \alpha <_{\Pi} (i, s'_i)\}$.

Důkaz: Protože $x^{n+1} \equiv 0$ a $y^{s'_0} - xf_0 \equiv 0$, dostáváme $y^{s'_0(n+1)} \equiv x^{n+1} f_0^{n+1} \equiv 0$ a A je tak nilpotentní podle věty 17 b). Nejdříve ukážeme následující pozorování:

Nechť $f \in I$, $M(f) \geq (i, 0)$, $0 \leq i \leq n+1$. Pak musí být $f \in Rp'_i + \cdots + Rp'_{n+1}$.

Mějme tedy příslušné f. Nechť j je největší takové, že $0 \leq j \leq n+1$ a $f \in Rp'_j + \cdots + Rp'_{n+1}$. Pro spor předpokládejme, že $j < i$. Pak zřejmě můžeme psát $f = (g(y) + xh)p'_j + \sum_{k=j+1}^{n+1} h_k p'_k$, kde $h, h_k \in R = F[x, y]$, $g(y) \in F[y]$. Pokud by bylo $g(y) \neq 0$, měli bychom zřejmě $M(g(y)p'_j) < (j+1, 0)$ a protože je $M(xhp'_j + \sum_{k=j+1}^{n+1} h_k p'_k) \geq (j+1, 0)$, tak bychom podle lemmatu 12 5) měli, že $(i, 0) \leq M(f) = M(g(y)p'_j) < (j+1, 0) \leq (i, 0)$, což je spor. Je tedy $g(y) = 0$

a protože $xp'_j \in Rp'_{j+1} + \cdots + Rp'_{n+1}$, tak je také $f \in Rp'_{j+1} + \cdots + Rp'_{n+1}$, což je spor s volbou j. Musí proto být $i \leq j$.

Vzhledem k lemmatu 23 3) teď stačí ukázat jen, že $\|x + I\| = n + 1$ a $s_i = s'_i$ pro $0 \leq i \leq n + 1$.

$\|x + I\| = n + 1$: Máme $x^{n+1} = p_{n+1} \equiv 0$. Pokud je $n = 0$, je to zřejmé. Nechť je tedy $n \geq 1$. Kdyby bylo $x^n \equiv 0$, pak bychom z výše dokázaného pozorování měli $x^n = hp'_n + gp'_{n+1}$ kde $g, h \in R$. Podle lemmatu 12 5) by pak bylo $(n, 0) = M(x^n) = M(hp'_n + gp'_{n+1}) \geq min_{\leq}\{M(h) + M(p'_n), M(g) + M(p'_{n+1})\} \geq min_{\leq}\{(0, 0)+(n, s'_n), (0, 0)+(n+1, 0)\} = (n, s'_n)$. Dostali bychom tak $0 \geq s'_n$, což je spor.

$s_i \leq s'_i$: Protože $p_i \equiv 0$ je (z definice $\mathcal{C}_A$) $(i, s'_i) \in \mathcal{C}_A$. Kdyby bylo $s'_i < s_i$, tak by podle lemmatu 23 3) platilo, že $(i, s'_i) \in \mathcal{B}_A$, což by byl spor.

$s'_i \leq s_i$: sporem: nechť je $s_i \leq s'_i - 1$, pak podle lemmatu 23 4) je $(i, s'_i - 1) \in \mathcal{C}_A$ a tedy ex. $f \in I$, že $M(f) = (i, s'_i)$. Podle dokázaného pozorování je tudíž $f = \sum_{k=i}^{n+1} h_k p_k$. Takže podle lemmatu 12 5) můžeme psát $(i, s'_i - 1) = M(f) = M(\sum_{k=i}^{n+1} h_k p_k) \geq min_{\leq}\{M(h_k) + M(p_k) |\ i \leq k \leq n + 1\} \geq min_{\leq}\{(0, 0) + (k, s'_k) |\ i \leq k \leq n + 1\} = (i, s'_i)$ a tedy je $s'_i - 1 \geq s'_i$, což je spor. □

Důsledek 38 *Mějme polynomy $p'_0 = y^k - xf$, $p'_{n+1} = x^{n+1}$, kde $k \geq 1$, $n \geq 0$, $f \in R$. Položme $I = Rp'_0 + Rp'_{n+1}$. Pak $A = Rx + Ry/I$ je nilpotentní algebra, $\|x + I\| = n + 1$, $s_i = k$ pro $0 \leq i \leq n$, $s_i = 0$ pro $n + 1 \leq i$ a $\mathcal{B}_A = \{\alpha |\ \alpha \leq_{\Pi} (n, k - 1)\}$.*

Důkaz: Plyne ihned z předchozí věty, pokud položíme $p'_i = x^i.p'_0$ pro $1 \leq i \leq n$. □

Věta 37 tedy umožňuje konstruovat algebry s předem zadaným tvarem množiny $\mathcal{B}_A$. Stačí totiž položit např. $p'_i = x^i y^{s'_i}$. Při této volbě ale získáme jen velmi "jednoduchou" algebru, kde prvek $x^i y^j + I$ je buď v bázi nebo je nulový. Speciálně bude graduovaná (zřejmě stačí vzít $N_k = [\{x^i y^j + I |\ i + j = k\}]$).

Podmínka 3) ve větě 39 však říká, jak se dají pro pevně zvolenou množinu $\mathcal{B}_A$ všechny polynomy p'_i zkonstruovat:

Protože má být $M(p'_i) = (i, s'_i)$ a $xp'_i = h_{i,i+1}p'_{i+1} + \sum_{j=i+2}^{n+1} h_{i,j}p'_j$ pro nějaké $h_{i,j} \in R$, tak pomocí lemmatu 12 snadno spočítáme, že musí platit $M(h_{i,i+1}) = (0, s'_i - s'_{i+1})$ a dále vzhledem k tvaru polynomu p'_0 musí být $h_{0,1} = y^{s'_0 - s'_1} +$

xg pro nějaké $g \in R$. Naopak pokud takto rekurzivně (počínaje polynomem $p'_{n+1} = x^{n+1}$) definujeme p'_i, pak budou zřejmě splňovat předpoklady věty 37.

Ukázali jsme tak (díky lemmatu 23 a dusledku 27), jak se dají popsat a zkonstruovat všechny 2-generované nilpotentní algebry tvaru $A = Rx + Ry/I$.

4.1 Příklad A

L.Hammoudi v článku [7] tvrdí, že Eggertovu hypotézu dokázal. Ve svém "důkazu" však používá tvrzení, která buď neplatí nebo není nijak zřejmé, proč by platit měla. Snaží se přitom postupovat indukcí podle počtu generátorů algebry A. Pro nilpotentní algebry tvaru $A = Rx + Ry/I$ pak z tohoto článku (i přes někdy nejasné formulace) vyplývá toto: (značení je převzato)

Nechť $\mathcal{B} \subseteq \{(pi, pj) |\ (0,0) \neq (i,j) \in (\mathbb{N}_0)^2\}$ a $\bar{\mathcal{B}} \subseteq (\mathbb{N}_0)^2 \setminus \{(0,0)\}$ jsou takové, že $\mathcal{B} \subseteq \bar{\mathcal{B}}$ a množiny $\{x^\alpha + I |\ \alpha \in \mathcal{B}\}$ a $\{x^\alpha + I |\ \alpha \in \bar{\mathcal{B}}\}$ tvoří po řadě báze algeber $A^{(p)}$ a A (stručně budeme říkat, že $\bar{\mathcal{B}}$ je bází A a podobně pro $\mathcal{B}$).

Nechť $A' = \langle x + I \rangle$ (tj. A' je jednogenerovaná). Označme $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}}) = \{\alpha \neq (0,0) |\ (\exists \beta \in \bar{\mathcal{B}})(x^\alpha \equiv x^\beta)\}$ a podobně $\mathbb{Z}^2_{\geq 0}(\mathcal{B}) = \{\alpha \neq (0,0) |\ (\exists \beta \in \mathcal{B})(x^\alpha \equiv x^\beta)\}$. Pak se (mimo jiné) tvrdí, že má platit:

i) $dim A' = |\ \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}}) \cap (\mathbb{N}_0 \times \{0\})|$,

ii) $((i,j) \in \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})\ \&\ j \geq 2) \ \Rightarrow\ (i, j-1) \in \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$.

Všimněme si nejdříve, že $dim A = |\bar{\mathcal{B}}|$ a $\bar{\mathcal{B}} \subseteq \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ (a podobně to platí i pro $\bar{\mathcal{B}}$). Protože však $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ je obecně větší než $\bar{\mathcal{B}}$ (jak bude vidět z následujícího příkladu) a protože autor uvádí, že vztah $p \cdot dim A^{(p)} \leq dim A$ je ekvivalentní s $p \cdot |\mathbb{Z}^2_{\geq 0}(\mathcal{B})| \leq |\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})|$, tak je pravděpodobné, že se jedná o další z mnoha nepřesností v tomto článku a množinou $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ měl na mysli původní $\bar{\mathcal{B}}$ (a podobně i $\mathbb{Z}^2_{\geq 0}(\mathcal{B})$) a pouze věc špatně formuloval. My na příkladu ukážeme, že tvrzení ii) a níže uvedená tvrzení iii) a iv) neplatí ani v uvedeném tvaru ani pokud všechna $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ nahradíme $\bar{\mathcal{B}}$.

Předpokládejme nyní na chvíli, že množinou $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ měl autor opravdu na mysli $\bar{\mathcal{B}}$. Myšlenka článku [7] je pak asi následující: Bázi $\bar{\mathcal{B}}$ rozdělíme na $\bar{\mathcal{B}} \cap (\mathbb{N}_0 \times \{0\})$ a na zbytek. Podobně to uděláme i s $\mathcal{B}$. Pokud bude nyní platit, že $\bar{\mathcal{B}} \cap (\mathbb{N}_0 \times \{0\})$ je bází A' a $\mathcal{B} \cap (\mathbb{N}_0 \times \{0\})$ je bází $(A')^{(p)}$ a pokud bude

splněno ii), pak z indukčního předpokladu pro A' snadno dostaneme platnost Eggertovy hypotézy pro A. Jak však bude vidět z příkladu, tak jednoduchá situace zase není.

Uvědomme si nyní ještě, že pokud prohodíme značení proměnných (tj. místo x budeme psát y a naopak) a uvážíme "transponované" množiny $\bar{\mathcal{B}}^T$ a $\mathcal{B}^T$ (kde pro $X \subseteq (\mathbb{N}_0)^2$ značíme $X^T = \{(i,j)|\ (j,i) \in X\}$), pak musí uvedená tvrzení i) a ii) platit i pro tuto "novou" algebru. V původní algebře (tj. v původním značení) to tedy znamená, že položíme-li $A'' = \langle y + I \rangle$, pak by mělo platit:

iii) $dim A'' = |\ \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}}) \cap (\{0\} \times \mathbb{N}_0)|$,

iv) $((i,j) \in \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})\ \&\ i \geq 2) \ \Rightarrow\ (i-1,j) \in \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$.

Než ukážeme protipříklad pro tvrzení ii), iii) a iv), uvedeme nejdříve následující:

Pozorování 39 *Nechť $A = Rx + Ry/I$ je F-algebra, $charF = p > 0$. Pak $\bar{s}_i \leq s_{pi}$.*

Důkaz: Z lemmatu 23 1) a 4) máme, že $(pi, s_{pi}) \in \mathcal{C}_A$ a tedy (z definice $\mathcal{C}_A$) ex. $f \in Rx + Ry$ v normálním tvaru takový, že $M(f) = (pi, s_{pi})$ a $f \equiv 0$. Je tedy $f = x^{pi}(y^{s_{pi}} - xg)$ pro vhodné $g \in R$. Máme tudíž $0 \equiv x^{pi}(y^{s_{pi}} - xg)^p =: h(x^p, y^p)$ a zřejmě je $M(h(x^p, y^p)) = (pi, ps_{pi})$. Podle důsledku 31 je tedy $\bar{s}_i \leq \left\lceil \frac{ps_{pi}}{p} \right\rceil = s_{pi}$. □

Uvažme nyní následující:

`Příklad`
Nechť F je charakteristiky $p > 0$, I je ideál v R generovaný $y^2 - x(1+x)y$ a x^{2p}, $A = Rx + Ry/I$. Podle důsledku 38 je A nilpotetní a $\mathcal{B}_A = \{\alpha|\ \alpha \leq_\Pi (2p-1, 1)\}$.

Platí:

1) $y^p \equiv x^{p-1}y(1+x)^{p-1} = x^{p-1}y - x^p y + \sum_{i=2}^{p-1} \binom{p-1}{i} x^{i+p-1}y$.

Důkaz: Z $y^2 \equiv x(1+x)y$ indukcí snadno odvodíme, že $y^n \equiv x^{n-1}(1+x)^{n-1}y$ pro $n \geq 2$. Pak stačí položit $n = p$ a použít ještě, že $p - 1 = -1$ v F. □

2) $x^p y^p \equiv xy^{2p-1} \equiv x^{2p-1}y \not\equiv 0$.

Důkaz: Z 1) máme (po vynásobení x^p) že $x^p y^p \equiv x^{2p-1}y - x^{2p}y(1+\ldots) \equiv x^{2p-1}y$ (neboť $x^{2p} \equiv 0$). Opakovaným použitím 1) pak dále dostaneme $xy^{2p-1} \equiv x^p y^p (1+x)^{p-1} \equiv x^{2p-1}y(1+x)^{2(p-1)} = x^{2p-1}y + x^{2p}y(\ldots) \equiv x^{2p-1}y$ (opět protože $x^{2p} \equiv 0$). A konečně protože je $(2p-1,1) \in \mathcal{B}_A$ (tj. je to prvek báze) tak musí být $x^{2p-1}y \not\equiv 0$. □

3) $\mathcal{B}_{A^{(p)}} = \{\alpha |\ \alpha \leq_\Pi (1,1)\}$ a tedy $\mathcal{B} = \{(pi,pj) |\ (0,0) \neq (i,j) \in \mathcal{B}_{A^{(p)}}\} = \{(p,0),(p,p),(0,p)\}$ je báze $A^{(p)}$.

Důkaz: Podle důsledku 38 je $\|x+I\| = 2p$. Zřejmě platí $\left\lfloor \frac{2p-1}{p} \right\rfloor = 1$. Podle pozorování 39 , důsledku 38 a důsledku 31 1) je tedy $\bar{s}_1 \leq \bar{s}_0 \leq s_0 = 2$. Z důsledku 31 3) pak máme $\mathcal{B}_{A^{(p)}} = \{\alpha |\ \alpha <_\Pi (0,\bar{s}_0) \ \vee \ \alpha <_\Pi (1,\bar{s}_1)\} \subseteq \{\alpha |\ \alpha \leq_\Pi (1,1)\}$. Stačí tedy ukázat, že $(1,1) \in \mathcal{B}_{A^{(p)}}$ (neboť $\mathcal{B}_{A^{(p)}}$ je dolní množina - viz věta 21 2)).

Předpokládejme opak, tj. $(1,1) \in \mathcal{C}_{A^{(p)}}$. Podle definice 29 a 20 ex. polynom $f \in Rx + Ry$ v normálním tvaru takový, že $f = x(y - xg)$ pro vhodné $g \in R$ a $0 \equiv f(x^p, y^p) = x^p y^p - x^{2p} g(x^p, y^p)$. Tedy je $x^p y^p \equiv 0$ (neboť $x^{2p} \equiv 0$). To je ovšem spor s 2).

To, že $\mathcal{B}$ je báze $A^{(p)}$ pak plyne z důsledku 31. □

Doplňme $\mathcal{B}$ o prvky z $\mathcal{B}_A \setminus (0,0)$ tak, abychom dostali množinu $\bar{\mathcal{B}}$, která bude bází A (to lze vzhledem k větě 21 3)). Dále platí:

4) $(1,2p-1) \in \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}}) \setminus \bar{\mathcal{B}}$ (a tedy $\bar{\mathcal{B}} \subsetneq \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$).

Důkaz: Podle 2) platí $xy^{2p-1} \equiv x^{2p-1}y$. Víme, že $(2p-1,1) \in \bar{\mathcal{B}}$ a tudíž je $(1,2p-1) \in \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ (podle definice $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$). Zřejmě $(1,2p-1) \notin \bar{\mathcal{B}}$ (neboť $(1,2p-1) \notin \{(0,p),(p,p)\} \cup \mathcal{B}_A \setminus (0,0)$). □

5) $(p,p) \in \bar{\mathcal{B}} \subseteq \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$, ale $(1,p) \notin \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ (a tedy take $(1,p) \notin \bar{\mathcal{B}}$). Tedy neplatí iv).

Důkaz: Podle 1) je $xy^p \equiv x^p y - x^{p+1}y + \sum_{i=2}^{p-1} \binom{p-1}{i} x^{i+p}y$. Prvek xy^p tak máme vyjádřený pomocí báze $\mathcal{B}_A \setminus (0,0)$. Protože díky 2) známe i vyjádření ostatních prvků z $\bar{\mathcal{B}} \subseteq \{(0,p),(p,p)\} \cup \mathcal{B}_A \setminus (0,0)$ pomocí báze $\mathcal{B}_A \setminus (0,0)$ a toto vyjádření

je jednoznačné, tak je zřejmé, že neexistuje $\alpha \in \bar{\mathcal{B}}$, tak aby $xy^p \equiv x^\alpha$. □

Nechť je nyní navíc $p \geq 3$. Pak platí:

6) $(0,p) \in \bar{\mathcal{B}} \subseteq \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$, ale $(0,2) \notin \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ (a tedy také $(0,2) \notin \bar{\mathcal{B}}$). Tedy neplatí ii).

Důkaz: Máme $y^2 \equiv xy + x^2y \not\equiv 0$ (což je opět vyjádření prvku pomocí báze $\mathcal{B}_A \setminus (0,0)$). Analogicky jako v důkazu 5) ukážeme, že $(0,2) \notin \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$. □

7) $dimA'' > |\, \mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}}) \cap (\{0\} \times \mathbb{N}_0)| \geq |\, \bar{\mathcal{B}} \cap (\{0\} \times \mathbb{N}_0)|$. Tedy neplatí iii).

Důkaz: Položme $K = \{(0,i)|\ y^i \not\equiv 0 \ \&\ i \geq 1\}$. Zřejmě musí být $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}}) \cap (\{0\} \times \mathbb{N}_0) \subseteq K$ (neboť $\mathbb{Z}^2_{\geq 0}(\bar{\mathcal{B}})$ nemůže obsahovat prvky kongruentní s nulou). Z lemmatu 8 a 9 plyne, že $dimA'' = |K|$. Vzhledem k 6) nyní stačí ukázat, že $(0,2) \in K$. To je ovšem ihned zřejmé z toho, že $y^2 \equiv xy + x^2y \not\equiv 0$ (viz důkaz bodu 6)). □

4.2 Příklad B

Zde ukážeme, že pro algebry A nad tělesem F charakteristiky $p > 0$, které není perfektní, nemusí platit, že $dim(A/A_p) = dimA^{(p)}$. Konkrétně zkonstruujeme F-algebru A, pro kterou bude $dim(A/A_p) > dimA^{(p)}$.

`Příklad`
Nechť je tedy $charF = p > 0$, $\lambda \in F$ takové, že $(\forall \mu \in F)(\lambda \neq \mu^p)$. Nechť $k, n \geq 1$ jsou taková, že $p.k \leq n$. Uvažme ideál I v okruhu $R = F[x,y]$ generovaný polynomy $y^p - \lambda x^{pk}$ a x^{n+1} a položme $A = Rx + Ry/I$.

Podle důsledku 38 je A nilpotentní a $\mathcal{B}_A = \{\alpha|\ \alpha \leq_\Pi (n, p-1)\}$.

Platí:

1) $dim[x^k + I, y + I] = 2$.

Důkaz: $(0,1), (k,0) \in \mathcal{B}_A \setminus \{(0,0)\}$, což je báze A a tedy $x^k + I$ a $y + I$ musí být lineárně nezávislé. □

2) $[x^k + I, y + I] \cap A_p = 0$.

Důkaz: Mějme $\mu_1, \mu_2 \in F$ takové, že $(\mu_1 x^k + \mu_2 y) + I \in A_p$. Pak musí být $0 \equiv (\mu_1 x^k + \mu_2 y)^p = (\mu_1)^p x^{pk} + (\mu_2)^p y^p$. Současně platí $0 \equiv \lambda x^{pk} - y^p$ a máme tedy soustavu lineárních rovnic s netriviálním řešením (neboť $(pk, 0) \in \mathcal{B}_A$ a tedy je $x^{pk} \not\equiv 0$). Determinant takové soustavy musí být nulový a tedy $(\mu_1)^p + (\mu_2)^p \lambda = 0$. Vzhledem k volbě λ dostáváme $\mu_1 = \mu_2 = 0$. □

Díky bodům 1) a 2) nyní můžeme vytvořit bázi algebry A tvaru $e_1, \ldots, e_m$, $x^k + I, y + I, e'_1, \ldots, e'_l$, kde $e_1, \ldots, e_m$ je báze A_p. Dostáváme tak, že $A^{(p)} = [(e_1)^p, \ldots, (e_m)^p, x^{pk} + I, y^p + I, (e'_1)^p, \ldots, (e'_l)^p] = [x^{pk} + I, (e'_1)^p, \ldots, (e'_l)^p]$ (neboť $(e_i)^p = 0$ a $y^p \equiv \lambda x^{pk}$). Proto je $dim A^{(p)} < l + 2 = dim A - dim A_p = dim(A/A_p)$.

4.3 Příklad C

Pokud v definici dobrého páru (definice 13) nahradíme požadavek 2) slabší verzí 2") $(\forall f \in Rx_1 + \cdots + Rx_n)(\exists g \in Rx_1 + \cdots + Rx_n)(f^p(a_1, \ldots, a_n) = g(a_1^p, \ldots, a_n^p))$, pak zobecněná Eggertova hypotéza pro takovéto dobré páry už obecně neplatí.

Předpokládejme, že tomu tak není. Pak musí zobec. Egger. hypotéza platit pro každou konečnou algebru A a každé $p \geq 2$ (neboť pokud $A = \{a_1, \ldots, a_n\}$, pak jistě pro $f \in Rx_1 + \cdots + Rx_n$ ex. i takové, že $1 \leq i \leq n$ a $f(a_1, \ldots, a_n) = a_i$ a tedy stačí položit $g = x_i$).

Uvažme nyní následující:

`Příklad`
Nechť F je konečné těleso. Zvolme $p \geq 2$ tak, aby $p \times 1 \neq 0$ v F. Položme $R = F[x]$ a $A = Rx/Rx^{p+2}$. Pak A je nilpotentní konečná algebra (podle lemmatu 9) a platí $(x+x^2)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p+i} \equiv x^p + p.x^{p+1}$. Protože $x^p + I, (x+x^2)^p + I \in A^{(p)}$ dostáváme, že také $x^{p+1} + I \in A^{(p)}$. Z lemmatu 9 pak máme, že $x^p + I$ a $x^{p+1} + I$ jsou lineárně nezávislé a tedy je $p \cdot dim A^{(p)} \geq 2p > p + 1 = dim A$. Což jsme chtěli ukázat.

4.4 Příklad D

Ukážeme, že existují i jiné dobré páry (A, p) než jen případy, kdy buď

1) $charF = q > 0$ a $p = q^n$ pro nějaké $n \geq 1$ (že je to dobrý pár: $(a+b)^p = a^p + b^p$ pro každé $a, b \in A$, takže je to zřejmé)

nebo

2) $a^p = 0$ pro každé $a \in A$ (že je to dobrý pár: pro $f \in Rx_1 + \cdots + Rx_n$ a $\alpha = M(f)$ stačí vzít $g = x^\alpha$, pak totiž zřejmě máme $(f(a_1, \ldots, a_n))^p = 0 = g(a_1^p, \ldots, a_n^p)$).

`Příklad`
Nechť je nyní q prvočíslo, $F = \mathbb{Z}_q$, $R = F[x]$ a $k \geq 0$. Položme $p = q^k(1 + l(q-1))$, kde $l \geq 1$. Nechť dále n je takové, že $p + 1 \leq n + 1 \leq p + q^k$. Položme $A = Rx/Rx^{n+1}$. Pak je A nilpotentní podle lemmatu 9. Ukažeme, že platí $(a+b)^p = a^p + b^p$ pro každé $a, b \in A$ (pak už zřejmě (A, p) bude dobrý pár generovaný prvkem $x + I$).

Důkaz: Nejdříve dokážeme, že platí $\mu^p = \mu$ pro každé $\mu \in F$. Pro $\mu = 0$ je to zřejmé. Nechť je tedy $\mu \neq 0$. Pak z Langrangeovy věty je $\mu^{q-1} = 1$ a tedy $\mu^q = \mu$ takže dostáváme $\mu^p = (\mu^{q^k})^{l(q-1)+1} = \mu^{l(q-1)+1} = (\mu^{q-1})^l \mu = \mu$. Pro každé $\lambda, \mu \in A$ tedy máme $(\lambda + \mu)^p = \lambda + \mu = \lambda^p + \mu^p$. Pro $\lambda \in F$ a $g \in R$ dále platí $(\lambda x + x^2 g)^p = x^p(\lambda + xg)^p = x^p(\lambda^{q^k} + x^{q^k} g^{q^k})^{1+l(q+1)} = \lambda^p x^p + x^{p+q^k}(\ldots) \equiv \lambda^p x^p$ (neboť $x^{n+1} \equiv 0$ a $n+1 \leq p+q^k$). Protože každé dva prvky $a, b \in A$ lze psát ve tvaru $a = (\lambda_1 x + x^2 g_1) + I$ a $b = (\lambda_2 x + x^2 g_2) + I$ pro vhodné $\lambda_i \in F$ a $g_i \in R$, tak dostáváme $(a+b)^p = ((\lambda_1 + \lambda_2)x + x^2(g_1 + g_2))^p + I = (\lambda_1 + \lambda_2)^p x^p + I = (\lambda_1^p + \lambda_2^p)x^p + I = a^p + b^p$. Což jsme chtěli dokázat. □

Zřejmě lze nyní p volit tak, aby $p \neq q^m$ pro každé $m \geq 1$ (např. jako $p = q^k(1 + q(q-1)s)$ pro $s \geq 1$) a zřejmě je $x^p + I \neq 0 + I$ (viz lemma 9).

4.5 Příklad E

V článku [6] byl jeden z částečných výsledků tento: Eggertova hypotéza platí, pokud A je graduovaná algebra a $A^{(p)}$ je generovaná 2 prvky. (graduovanost - viz definice 4)

Zde najdeme dostatečný počet příkladů (viz lemma 41), kdy A je generovaná 2 prvky (a tedy $A^{(p)}$ je taktéž generovaná 2 prvky, neboť $p = charF$) a přitom A není graduovaná.

Lemma 40 *Nechť A je nilpotentní graduovaná algebra, $a, b \in A$, $A = \langle a, b \rangle$. Pak ex. $a', b' \in A$ a U vektorový podprostor A takový, že $a' - a, b' - b \in A^2$,*

$U = [a', b']$ *a* $A = \bigoplus_{i=1}^{\infty} U^i$ *(A je direktním součtem vektorových podprostorů* $U^i = [\{a_1 \dots a_i |\ a_j \in U\}]$*).*

Důkaz: A je graduovaná a tedy ex. vektorové prostory $N_i \leq A$ takové, že $A = \bigoplus_{i=1}^{\infty} N_i$, $N_i.N_j \subseteq N_{i+j}$ pro každé $i, j \geq 1$, $A = \langle N_1 \rangle$. Označme $U = N_1$. Pak je $U^i \subseteq N_i$ a tedy máme $A = \langle N_1 \rangle = \langle U \rangle = \bigoplus_{i=1}^{\infty} U^i$ $(\leq \bigoplus_{i=1}^{\infty} N_i)$. Prvky $a, b \in A$ tak můžeme psát ve tvaru $x = \sum_i x_i,\ y = \sum_i y_i$, kde $x_i, y_i \in U^i$. Platí tedy, že $xy = \sum_{i,j} x_i y_j \in \bigoplus_{i=2}^{\infty} U^i$ a tudíž $A^2 \subseteq \bigoplus_{i=2}^{\infty} U^i$. Opačná inkluze $\bigoplus_{i=2}^{\infty} U^i \subseteq A^2$ je zřejmá z definice U^i. Celkem jsme zjistili, že $A = U \oplus A^2$, což nám spolu s přirozenou projekcí $\pi : A \to A/A^2 = [\pi(a), \pi(b)]$ dává požadované tvrzení (neboť $\pi|U : U \to A/A^2 = [\pi(a), \pi(b)]$ je lineární izomorfismus). □

Lemma 41 *Nechť* $A = \langle a, b \rangle$ *je nilpotentní algebra. Nechť* $n, k \geq 1$ *jsou taková, že platí* $n < k$, $k + 1 \leq 2n$, $a.A^n = 0$, $b.A^k = 0$ *a* $0 \neq a^n = b^k$. *Pak A není graduovaná.*

Důkaz: Postupujme sporem: nechť A je graduovaná. Pak podle předchozího lemmatu ex. $a', b' \in A$ a vekt. podprostor $U \leq A$ takový, že $a' = a + u$, $b' = b + v$ (kde $u, v \in A^2$), $A = \bigoplus_{i=1}^{\infty} U^i$ a $U = [a', b']$. Z předpokladů $a.A^n = 0$, $b.A^k = 0$, $A = \langle a, b \rangle$ a $n < k$ snadno obdržíme, že $A^{k+1} = 0$.

Dále je $(a')^n = (a+u)^n = a^n + aw + u^n$, kde $w = \sum_{i=1}^{n-1} \binom{k}{i} a^{n-i-1} u^i$ a podobně $(b')^k = (b+v)^k = b^k + bt + v^k$, kde $t = \sum_{i=1}^{k-1} \binom{k}{i} b^{k-i-1} v^i$. Díky předpokladům a tomu, že je $u, v \in A^2$, dostáváme následující vztahy: $w \in \sum_{i=1}^{n-1} A^{n-i-1+2i} \subseteq A^n$, $u^n \in A^{2n} \subseteq A^{k+1} = 0$, $t \in \sum_{i=1}^{k-1} A^{k-i-1+2i} \subseteq A^k$, $v^k \in A^{2k} \subseteq A^{2n} \subseteq A^{k+1} = 0$. Dohromady tedy platí, že $a^n = (a')^n \in U^n$, $b^k = (b')^k \in U^k$ a $0 \neq a^n = b^k$, což je spor s direktností součtu prostorů U^n a U^k. □

Pozorování 42 *Nechť* $A = \langle a, b \rangle$ *je nilpotentní algebra.*
Pak $A^k = [\{a^i b^j |\ i, j \geq 0,\ i + j \geq k\}]$ *pro každé* $k \geq 1$.

Důkaz: Plyne snadno z definice A^k (viz definice 2). □

Nyní tedy konečně zkonstruujeme příklad algebry, která bude splňovat předpoklady předchozího lemmatu 41:

`Příklad`
Nechť $n, k \geq 1$ jsou taková, že platí $n < k$, $k+1 \leq 2n$. Položme $p'_0 = y^k - x^n$, $p'_i = x^i y^{n+1-i}$ pro $1 \leq i \leq n+1$. Nechť I je ideál v $R = F[x,y]$ generovaný těmito polynomy. Položme $A = Rx + Ry/I$, $a = x + I$ a $b = y + I$. Snadno se ověří, že uvedené polynomy splňují přepoklady věty 37. Z této věty a předpokladů pak také snadno máme, že A je nilpotentní algebra a $(n,0) \in \mathcal{B}_A$ (a tedy $0 \not\equiv x^n \equiv y^k$). Zbývá už jen ukázat, že $a.A^n = b.A^k = 0$. Podle předchozího pozorování 42 to znamená, že stačí overit, zda $x^{i+1}y^j \equiv 0$ pro $i + j = n$ (což evidentně platí) a dále, zda $x^i y^{j+1} \equiv 0$ pro $i + j = k$, $i \geq 0$ (což pro $i \geq 1$ plyne z právě uvedené předchozí "evidentní" kongruence, neboť je $n < k$. Pro $i = 0$ je pak $y^{k+1} \equiv x^n.y \equiv 0$, jak už víme).

4.6 Dolní odhad $dimA^{(p)}$

Většina dosud publikovaných výsledků týkajících se Eggertovy hypotézy vychází z předpokladu, že $dimA^{(p)}$ je malá, konkrétně ≤ 4. Následující věta ukazuje spodní odhad dimenze algebry $A^{(p)}$ pomocí dimenze A za předpokladu, že $charF = p > 0$ a že známe počet generátorů algebry A. Stačí tedy mít dostatečně "velkou" 2-generovanou algebru (tu získáme např. z důsledku 38), aby dimenze $A^{(p)}$ přesáhla libovolně zvolenou mez.

Definice 43 *Nechť $X \subseteq (\mathbb{N}_0)^n$, $p \geq 1$. Označme $pX = \{p.\alpha |\ \alpha \in X\}$.*

Položme $\epsilon = (1, \ldots, 1) \in (\mathbb{N}_0)^n$. Nechť $\alpha \in (\mathbb{N}_0)^n$. Označme $\mathcal{I}_\alpha = \{\beta |\ \alpha \leq_\Pi \beta \leq \alpha + (p-1)\epsilon\}$.

Zřejmě platí $|X| = |pX|$, $|\mathcal{I}_\alpha| = p^n$, $(\mathbb{N}_0)^n = \cup\{\mathcal{I}_{p\alpha} |\ \alpha \in (\mathbb{N}_0)^n\}$. (kde poslední sjednocení je dokonce disjunktní).

Věta 44 *Nechť A je nilpotentní F-algebra, $charF = p > 0$ a $a_1 \ldots, a_n \in A$ jsou takové, že $A = \langle a_1, \ldots, a_n \rangle$.*

Pak $1 + dimA \leq p^n(1 + dimA^{(p)})$.

Důkaz: Položme $R = F[x_1, \ldots, x_n]$. Vzhledem k větě 17 stačí uvažovat $A = Rx_1 + \cdots + Rx_n/I$, kde I je vhodný ideál v R a $a_i = x_i + I$. Zřejmě je

$A^{(p)} = \langle a_1^p, \ldots, a_n^p \rangle$. Položme $J = \{g \in R |\ g(x^p) \in I\}$ (J je ideál v R) a $C = Rx_1 + \cdots + Rx_n/J$. Zřejmě je C nilpotentní algebra (např. podle věty 17) a zobrazení $\phi : C \to A^{(p)}$, $\phi(f+J) = f(a_1^p, \ldots, a_n^p) = f(x^p) + I$ je izomorfismus F-algeber.

Položme nakonec $\mathcal{B} = (p\mathcal{B}_C) \cap \mathcal{B}_A$. Ukážeme, že platí $\mathcal{B}_A \subseteq \cup\{\mathcal{I}_\alpha |\ \alpha \in \mathcal{B}\}$. Nechť $\beta \in \mathcal{B}_A \subseteq (\mathbb{N}_0)^n = \cup\{\mathcal{I}_{p\alpha} |\ \alpha \in (\mathbb{N}_0)^n\}$. Pak ex. (právě jedno) α takové, že $\beta \in \mathcal{I}_{p\alpha}$. $\mathcal{B}_A$ je dolní množina a tedy $p\alpha \in \mathcal{B}_A$. Kdyby nyní bylo $\alpha \in \mathcal{C}_C$ tak ex. polynom $f \in J$ takový, že $M(f) = \alpha$. Tedy by platilo, že $f(x^p) \in I$ a $M(f(x^p)) = p\alpha$, tj. bylo by $p\alpha \in \mathcal{C}_A$, což je zřejmě spor. Dostali jsme tak, že $p\alpha \in \mathcal{B}$, což jsme chtěli.

Nyní tedy pomocí dokázaného můžeme psát $1 + dim A = |\mathcal{B}_A| \leq$
$\leq |\cup\{\mathcal{I}_\alpha | \alpha \in \mathcal{B}\}| \leq \sum_{\alpha \in \mathcal{B}} |\mathcal{I}_\alpha| = p^n |\mathcal{B}| \leq p^n |p\mathcal{B}_C| = p^n |\mathcal{B}_C| = p^n (1 + dim A^{(p)})$.

□

Literatura

[1] Eggert N.H. (1971): Quasi regular groups of finite commutative algebras. *Pacific Journal of Mathematics* **36(3)**, 631-634.

[2] Stack C. (1996): Dimension of nilpotent algebras over fields of prime characteristic. *Pacific Journal of Mathematics* **176(1)**, 631-634.

[3] Stack C. (1998): Some results on the structure of finite nilpotent algebras over fields of prime characteristic. *The Journal of Combinatorial Mathematics and Combinatorial Computing* **28**, 327-335.

[4] Amberg B., Kazarin L. S. (2001): On the dimension of nilpotent algebras. *Mathematical Notes* **70(4)**, 439-446

[5] Amberg B., Kazarin L. S. (2001): Commutative nilpotent p-algebras with small dimension. Topics in infinite groups (Curzio M.), Seconda Univerzita di Napoli, 3-19

[6] McLean K. R. (2004): Eggert's conjecture on nilpotent algebras. *Communication in Algebra* **32(3)**, 997-1006

[7] Hammoudi L. (2002): Eggert's conjecture on the dimensions of nilpotent algebras. *Pacific Journal of Mathematics* **202(1)**, 93-97

[8] Amberg B., Kazarin L. S. (1999): On the rank of a product of two finite p-groups and nilpotent p-algebras. *Communication in Algebra* **27(8)**, 3895-3907