Vybrané kapitoly z algebry[1]

Jaroslav Guričan

[1]Moja vďaka patrí Tiborovi Katriňákovi a Antonovi Legéňovi

Obsah

Kapitola 1

Moduly a kanonické tvary matíc

1.1 Smithov kanonický tvar

Budeme sa zaoberať maticami $A = ||a_{ij}||_{m\times n}$ nad euklidovským okruhom R. (R môže byť pole F alebo okruh polynómov $F[x]$ nad poľom, alebo okruh Z celých čísel, a podobne) Ako zaujímavý príklad takejto matice je matica $xI - A$ nad okruhom polynómov $F[x]$ (A je matica nad poľom F, I je identická matica nad poľom F.) Ohodnotenie v euklidovskom okruhu budeme označovať znakom g.

Na maticiach budeme robiť *elementárne úpravy*. Dovolené sú nasledujúce tri typy úprav:

1. Výmena i-teho riadku (stĺpca) s j-tym riadkom (stĺpcom)
2. Vynásobenie i-teho riadku (stĺpca) matice A deliteľom jednotky $c \in R$
3. Pripočítanie c násobku i-teho riadku (stĺpca) ku j-temu riadku (stĺpcu) ($i \neq j$ a c je ľubovoľný prvok z R).

Uvedené úpravy budeme zrejmým spôsobom rozdeľovať na *riadkové* a *stĺpcové*. Ak nezáleží na tom, či je úprava riadková alebo stĺpcová, budeme jednoducho hovoriť o elementárnej úprave.

Poznámka. Všimnime si, že uvedené úpravy pre prípad, že R je pole dávajú naše známe elementárne úpravy.

Definícia 1.1.1 *1. Štvorcovú maticu B nad R nazývame* elementárnou *(typu 1 – 3), ak vznikne z identickej matice I jednou elementárnou úpravou (1 – 3)*

2. Matice A a B rovnakého typu nad okruhom R nazývame riadkovo ekvivalentné (stĺpcovo ekvivalentné, ekvivalentné), ak existuje konečná postupnosť riadkových elementárnych úprav (stĺpcových elementárnych úprav, (miešaných) elementárnych úprav), pomocou ktorých sa dostaneme od matice A ku matici B. Budeme používať označenia $A \doteq_r B$, $A \doteq_s B$, $A \doteq B$.

Cvičenie 1 *Dokážte, že každá elementárna úprava je reverzibilná, t.j. ak vieme od matice A prejsť ku matici B pomocou jednej elementárnej úpravy ku matici B, tak existuje elementárna úprava taká, ktorou prejdeme od matice B ku matici A.*

Cvičenie 2 *Dokážte, že relácie $\doteq_r$, $\doteq_s$ a $\doteq$ sú relácie ekvivalencie na množine matíc rovnakého typu nad euklidovským okruhom R.*

Cvičenie 3 *Nech matica B vznikla z matice A pomocou jednej riadkovej (stĺpcovej) elementárnej úpravy. Potom $B = I_rA$ ($B = AI_s$), kde I_r (I_s) je elementárna matica, ktorá vznikne z I rovnakou riadkovou (stĺpcovou) úpravou ako bola tá, ktorou z A vznikla B.*

Cvičenie 4 *$A \doteq_r B$ ($A \doteq_s B$, $A \doteq B$) práve vtedy, keď existujú elementárne matice $E_1, \ldots, E_r$ ($E'_1, \ldots, E'_s$) také, že $B = E_1 \ldots E_rA$ ($B = AE'_1 \ldots E'_s$, $B = E_1 \ldots E_rAE'_1 \ldots E'_s$).*

Cvičenie 5 *Ukážte, že elementárne matice sú delitele jednotky v okruhu štvorcových matíc nad okruhom R (t.j. ku každej elementárnej matici A existuje štvorcová matica B toho istého typu (bude tiež elementárna) taká, že $AB = BA = I$).*

Cvičenie 6 *Nech R je komutatívny okruh s jednotkou. Sformulujte definíciu determinantu štvorcovej matice nad R. Overte, že pre tieto determinanty platia všetky tvrdenia známe z prvého ročníka (pozor na matice nad okruhmi s charakteristikou 2 — resp. v ktorých existujú prvky rádu 2 vzhľadom na sčítanie)*

Definícia 1.1.2 *Maticu $D = ||d_{ij}||_{m\times n}$ nazývame diagonálnou, ak $d_{ij} = 0$ vždy, keď $i \neq j$.*
Diagonálnu maticu zvykneme zapisovať ako $D = \mathrm{diag}(d_1, d_2, \ldots)$, kde $d_i = d_{ii}$.

Veta 1.1.3 (Smithov kanonický tvar matice) *Majme maticu A typu $m \times n$ nad euklidovským okruhom R. Potom existuje diagonálna matica $D = \mathrm{diag}(d_1, d_2, \ldots)$ ekvivalentná s A a taká, že platí:*

1. *$d_i \mid d_j$ pre prípustné i, j také, že $i \leq j$*

Matica D je jednoznačne určená až na asociovanosť, t.j. ak $C = \mathrm{diag}(c_1, c_2, \ldots)$ je iná matica ekvivalentná s A pre ktorú tiež platí $c_i \mid c_j$ pre prípustné $i \leq j$, potom pre všetky možné i je $c_i \doteq d_i$.

Poznámka. Diagonálnu maticu D zo znenia vety nazývame Smithov kanonický tvar matice.

Dôkaz. Najprv existencia. Urobíme konštruktívny dôkaz (algoritmus), ktorý budeme nazývať proces diagonalizácie. Ak $A = ||\,0\,||_{m\times n}$ tak A je v diagonálnom tvare. Nech teda $A \neq ||\,0\,||_{m\times n}$. Našim prvým cieľom je vynulovať všetky prvky v prvom riadku a prvom stĺpci okrem ľavého horného prvku.

Krok 1a: (**Vstup:** Matica A.
Výstup: Matica A', v ktorej má ľavý horný prvok minimálne euklidovské ohodnotenie spomedzi všetkých prvkov matice A'.)

Vyberme spomedzi nenulových prvkov prvkv matice A (t.j. spomedzi $a_{ij} \neq 0$) taký, pre ktorý nadobúda jeho ohodnotenie $g(a_{ij})$ minimálnu hodnotu spomedzi všetkých prvkov matice A. Ak a_{11} je prvok s minimálnym ohodnotením, tak ho necháme na mieste. Ak nie je, pomocou elementárnych operácií výmeny riadkov a stĺpcov dopravíme prvok a_{ij} s minimálnym ohodnotením do ľavého horného rohu. Maticu, ktorá vznikne označíme A' a bude obsahovať prvky $A = ||a'_{ij}||_{m\times n}$ (ktoré sú len poprehadzovaním prvkov matice A).

Krok 1b: (**Vstup:** Matica A, v ktorej má ľavý horný prvok minimálne euklidovské ohodnotenie spomedzi všetkých prvkov matice A.
Výstup: Matica $A^- = ||a^-_{ij}||_{m\times n}$, v ktorej všetky prvky v prvom riadku a prvom stĺpci okrem ľavého horného sú buď nuly, alebo majú menšie ohodnotenie ako ľavý horný prvok a^-_{11}.)

Predpokladáme teda, že a_{11} má minimálne ohodnotenie. Vydeľme teraz so zvyškom všetky ostatné prvky v prvom riadku a v prvom stĺpci prvkom a_{11}. Dostaneme postupne

$$a_{1j} = a_{11}q_{1j} + r_{1j}, \quad \text{kde} \quad r_{1j} = 0 \quad \text{alebo} \quad g(r_{1j}) < g(a_{11})$$

a podobne

$$a_{i1} = a_{11}q_{i1} + r_{i1}, \quad \text{kde} \quad r_{i1} = 0 \quad \text{alebo} \quad g(r_{i1}) < g(a_{11}).$$

Pre každé $j = 2, \ldots, n$ teraz pripočítame $-q_{1j}$ násobok prvého stĺpca ku j-temu stĺpcu a pre každé $i = 2, \ldots, m$ pripočítame $-q_{i1}$ násobok prvého riadku k i-temu riadku. Tým dostaneme v prvom riadku postupne prvky a_{11}, $r_{12}, \ldots r_{1n}$ a v prvom stĺpci a_{11}, $r_{21}, \ldots, r_{m1}$.

Označme túto maticu ako $A^- = ||a^-_{ij}||_{m\times n}$.

Pôvodnú maticu označme aj ako $A^{(1)}$. Položme $A^{(2)} = ((A^{(1)})')^-$, t.j. $A^{(2)} = ||a^{(2)}_{ij}||_{m\times n}$ vznikne z $A^{(1)}$ tak, že na ňu najprv aplikujeme krok 1a a na výsledok $(A^{(1)})'$ aplikujem krok 1b. Buď sú už všetky prvky $a^{(2)}_{12}, \ldots, a^{(2)}_{1n}$ a $a^{(2)}_{21}, \ldots, a^{(2)}_{m1}$ nulové, alebo nie. Ak áno, pokračujeme krokom 2. Ak nie, aplikujeme postupne kroky 1a a 1b. Dostaneme maticu $A^{(3)} = ((A^{(2)})')^- = ||a^{(3)}_{ij}||_{m\times n}$. Platí, že $g(a^{(1)}_{11}) \geq g(a^{(2)}_{11}) > g(a^{(3)}_{11})$ a všetky prvky $a^{(3)}_{12}, \ldots, a^{(3)}_{1n}$ a $a^{(3)}_{21}, \ldots, a^{(3)}_{m1}$ sú nulové alebo majú menšie ohodnotenie ako $a^{(3)}_{11}$ (druhá, ostrá nerovnosť platí preto, lebo ľubovoľný nenulový prvok z prvého riadku či stĺpca matice $A^{(2)}$ má menšie ohodnotenie ako $a^{(2)}_{11}$ a teda pri kroku 1a sa do ľavého horného rohu presunie prvok s (ostro) menším ohodnotením. Krok 1b tento prvok nezmení).

Ak sú v matici $A^{(3)}$ v prvom riadku a prvom stĺpci už len nulové prvky (samozrejme, okrem prvku $a^{(3)}_{11}$), pokračujeme krokom 2. Ak nie, opakujeme kroky 1a a 1b. Vytvárame tak postupne matice $A^{(4)}$, ... Platí, že $g(a^{(3)}_{11}) > g(a^{(4)}_{11}) > \ldots$. Tento proces sa musí zastaviť, lebo inak by sme dostali nekonečnú klesajúcu postupnosť. To, že "sa musí zastaviť" znamená, že v istom kroku už nemusíme pokračovať krokmi 1a a 1b, ale že pokračujeme krokom 2. Krokom 2 ale pokračujeme práve vtedy, keď sme "vynulovali" všetky prvky prvého riadku a prvého stĺpca (okrem ľavého horného).

Výsledok predošlého postupu je matica $A^{(i)}$, ktorá má v prvom riadku a prvom stĺpci okrem $a^{(i)}_{11}$ nulové prvky.

Krok 2: (**Vstup:** Matica $A = ||a_{ij}||_{m\times n}$, ktorá má v prvom riadku a prvom stĺpci nulové prvky okrem a_{11}.
Výstup: Diagonálna matica A'.) Predošlú procedúru (potrebný počet opakovaní krokov 1a a 1b) vykonáme na podmatici $(m-1) \times (n-1)$, ktorú dostaneme vynechaním prvého riadku a prvého stĺpca z matice A). Tak dostaneme maticu s nulovými prvým a druhým riadkom a prvým a druhým stĺpcom okrem prvkov na diagonále. (Rozmyslite si, ako sa prenášajú elementárne operácie z matice $(m-1)\times(n-1)$ do pôvodnej matice.) Pokračujeme na podmatici $(m-2) \times (n-2)$,... (Ináč povedané: konštrukciu robíme induktívne, t.j. predpokladáme, že vieme

urobiť diagonálnu maticu pre matice typu $1 \times k$ a $l \times 1$ — štart indukcie, toto sa urobí pomocou potrebného počtu krokov $1a$ a $1b$ a ďalej predpokladáme, že to vieme urobiť pre všetky matice typu $(m-1) \times (n-1)$ — tento predpoklad vlastne "simulujeme" krokom 2. Pripomenieme, že krokom 2 sa nesnažíme zabezpečiť deliteľnosti požadované v znení vety, ale len "vyrobiť" diagonálnu maticu pomocou elementárnych úprav — t.j., pri indukčnom predpoklade teraz požadujeme len to, že daná matica $(m-1) \times (n-1)$ sa dá upraviť na diagonálnu).

Po vykonaní predošlých dvoch krokov dostaneme diagonálnu maticu $B = \mathrm{diag}(b_1, b_2, \ldots)$ ekvivalentnú s pôvodnou maticou. Ak už platí 1 zo znenia vety, skončili sme. Nech táto podmienka nie je splnená. Pokračujeme krokom 3. Bez ujmy na všeobecnosti môžeme predpokladať, že diagonálne prvky sú zoradené podľa veľkosti ich ohodnotení, t.j. pre všetky prípustné i platí, že $g(b_i) \geq g(b_{i+1})$ (toto vieme zabezpečiť výmenou riadkov).

Krok 3: (**Vstup:** Diagonálna matica B, v ktorej neplatí podmienka 1 zo znenia vety, t.j. existujú indexy $k < j$ také, že $b_k \not| b_j$, ale pre všetky prípustné i platí, že $g(b_i) \geq g(b_{i+1})$.

Výstup: Diagonálna matica B', jej vlastnosti popíšeme neskôr.)

Nech k je najmenší index taký, že existuje $j > k$, pre ktorý platí b_k nedelí b_j. Teda pre $i < k$ a ľubovoľný prípustný index už platí $i \leq l$ $b_i \,|\, b_l$. Nech j je najmenší taký index, že b_k nedelí b_j.

V matici B pripočítajme j-ty riadok ku k-temu a vzniknutú maticu diagonalizujme (ako to bolo popísané vyššie). (Koniec kroku 3.)

Vlastnosti výslednej matice: dostaneme maticu $B' = \mathrm{diag}(b_1, \ldots, b_{k-1}, b'_k, \ldots)$. Označme pre jednoduchosť aj $b'_1 = b_1$, $\ldots$, $b'_{k-1} = b_{k-1}$. Naďalej platí, že pre $i < k$ a $l > i$ $b'_i \,|\, b'_l$, lebo prvky b'_k, $\ldots$, b'_l,$\ldots$ sú lineárnymi kombináciami prvkov b_k, $\ldots$, b_l,$\ldots$ (kroky $1a$ a $1b$ zaručujú, že prvky matíc, ktoré pri nich vznikajú sú lineárnymi kombináciami prvkov pôvodných matíc). Naviac $g(b_k) > g(b'_k)$ — "práca" pri diagonalizácii začne na prvku b_k a v skutočnosti sa realizuje sa na podmatici

$$\begin{pmatrix} b_k & 0 & \ldots & 0 & b_j \\ 0 & b_{k+1} & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & b_{j-1} & 0 \\ 0 & 0 & \ldots & 0 & b_j \end{pmatrix}$$

Pre všetky prípustné indexy platí $g(b_i) \geq g(b'_i)$ a pre (aspoň) jeden index platí ostrá nerovnosť, a to $g(b_k) > g(b'_k)$.

Sú dve možnosti: buď už $b'_i \,|\, b'_j$ pre všetky prípustné $j > i$ alebo nie. Ak áno, máme splnenú podmienku 1 zo znenia vety a teda sme skončili. Ak ešte nespĺňa, krok 3 zopakujeme toľkokrát, koľko to bude potrebné. Tento proces skončí po konečnom počte krokov, pretože v matici B je na diagonále konečný počet prvkov a preto ich všetky hodnoty $g(b_i)$ môžu ostro klesnúť iba konečný počet krát. Krok 3 neopakujeme práve vtedy, keď už platí podmienka 1. Ako sme práve ukázali, po konečnom počte krokov ho už urobiť netreba, a teda v momente, keď skončíme, máme skonštruovanú diagonálnu maticu D ekvivalentnú s A spĺňajúcu podmienku 1.

Týmto sme ukončili dôkaz existencie. Jednoznačnosť. Urobíme pomocou tzv. *determinantových deliteľov* η_1, $\ldots$, η_r, $\ldots$ Nech A je matica $m \times n$ nad našim euklidovským okruhom R (ako sa presvedčíte v cvičeniach, dokonca stačí, aby bol R okruh hlavných ideálov). Nech $1 \leq i_1 < \cdots < i_r \leq m$ a $1 \leq j_1 < \cdots < j_r \leq n$. Potom zápisom $A \begin{pmatrix} i_1 & \ldots & i_r \\ j_1 & \ldots & j_r \end{pmatrix}$ označíme podmaticu matice A, ktorá vznikne tým že zoberieme len prvky nachádzajúce sa v riadkoch i_1, $\ldots$, i_r a stĺpcoch j_1, $\ldots$, j_r, t.j. maticu $|| a_{i_k j_l} ||_{r \times r}$. Uvažujme o všetkých štvorcových podmaticiach matice A typu $r \times r$ a ich determinantoch, ktoré nazývame subdeterminanty matice A (alebo minory A) rádu r. Najväčší spoločný deliteľ všetkých minorov matice A rádu i označíme znakom $\eta_i(A)$. Teda napr. $\eta_1(A)$ je najv. spol. deliteľ všetkých prvkov matice a ak je matica A štvorcová typu $n \times n$, tak $\eta_n(A)$ je determinant matice A.

Dokážeme si jedno pomocné tvrdenie:

Lema 1.1.4 *Nech matica B vznikne z matice A jednou elementárnou úpravou (uvedené matice sú typu $m \times n$). Potom*

1. *Každý minor matice B rádu r je lineárnou kombináciou (najviac dvoch) minorov matice A rádu r. (Pre všetky prípustné r.)*

2. *Pre všetky prípustné r platí $\eta_i(A) \doteq \eta_i(B)$*

Dôkaz. Z časti 1 priamo vyplýva, že $\eta_r(A) \,|\, \eta_r(B)$ a teda aj časť 2 ak si uvedomíme, že elementárne operácie sú reverzibilné.

Dokážeme teda časť 1 a urobíme ju len pre riadky, pre stĺpce sa to dostane transponovaním predošlého výsledku.

Jediný zaujímavý prípad je tretia elementárna operácia kedy maticu B dostaneme pripočítaním c násobku i-teho riadku ku j-temu riadku. matice A. Máme viacero možností:

1. ani jeden z indexov i, j sa nenachádza medzi $i_1, \ldots, i_r$, alebo i sa nachádza a j sa nenachádza medzi $i_1, \ldots, i_r$, alebo sa oba indexy i, j sa nachádzajú medzi $i_1, \ldots, i_r$. V týchto prípadoch bude platiť rovnosť

$$\left|B\begin{pmatrix} i_1 & \ldots & i_r \\ j_1 & \ldots & j_r \end{pmatrix}\right| = \left|A\begin{pmatrix} i_1 & \ldots & i_r \\ j_1 & \ldots & j_r \end{pmatrix}\right| .$$

   (Pre prvé dva prípady platí rovnosť aj pre matice, len pre tretí prípad potrebujeme použiť determinanty.)

2. index j sa nachádza a index i sa nenachádza medzi $i_1, \ldots, i_r$. Nech $j = i_l$. Potom pre príslušné poddeterminanty platí:

$$\left|B\begin{pmatrix} i_1 & \ldots & i_r \\ j_1 & \ldots & j_r \end{pmatrix}\right| = \left|\begin{pmatrix} a_{i_1 j_1} & \ldots & a_{i_1 j_r} \\ \vdots & & \vdots \\ c\cdot a_{ij_1} + a_{i_l j_1} & \ldots & c\cdot a_{ij_r} + a_{i_l j_r} \\ \vdots & & \vdots \\ a_{i_r j_1} & \ldots & a_{i_r j_r} \end{pmatrix}\right| =$$

$$\left|\begin{pmatrix} a_{i_1 j_1} & \ldots & a_{i_1 j_r} \\ \vdots & & \vdots \\ c\cdot a_{ij_1} & \ldots & c\cdot a_{ij_r} \\ \vdots & & \vdots \\ a_{i_r j_1} & \ldots & a_{i_r j_r} \end{pmatrix}\right| + \left|A\begin{pmatrix} i_1 & \ldots & j & \ldots & i_r \\ j_1 & & \ldots & & j_r \end{pmatrix}\right|$$

   Teraz si stačí uvedomiť, že riadky $i_1, \ldots, i_{l-1}, i, i_{l+1}, \ldots, i_r$ vieme poprehadzovať tak, aby boli v rastúcom poradí a z toho vidíme, že prvý poddeterminant na pravej strane tejto rovnice je $\pm c$ násobok nejakého minoru matice A rádu r.

   (**Poznámka.** V skutočnosti by sme mohli aj označenie zaviesť a aj lemu formulovať pre ľubovoľné postupnosti indexov, dokonca ani opakované prvky by nevadili. Nemuseli by sme potom dávať pozor na znamienka. Rozmyslite si to!)

□

Vráťme sa k dôkazu jednoznačnosti našej diagonálnej matice. Nech $D = \mathrm{diag}(d_1, d_2, \ldots)$ a $E = \mathrm{diag}(e_1, e_2, \ldots)$ sú dve matice ekvivalentné s pôvodnou maticou A a spĺňajúce podmienku 1 zo znenia vety. Podľa práve dokázanej lemy pre všetky prípustné indexy r platí $\eta_r(D) \doteq \eta_r(E)$. Ako sa ale dá ľahko vidieť, $d_1 \doteq \eta_1(D)$, $d_1 d_2 \doteq \eta_2(D)$, ... Rovnaké vzťahy platia pre maticu E, t.j. $e_1 \cdot \ldots \cdot e_r \doteq \eta_r(E)$. (Urobte podrobne!) Preto nakoniec (položme ešte pre ľubovoľnú maticu X $\eta_0(X) = 1$) pre ľubovoľný prípustný index r platí $d_r \doteq \eta_r(D)/\eta_{r-1}(D) \doteq \eta_r(E)/\eta_{r-1}(E) \doteq e_r$.
□

Poznámka. V dôkaze vety sú vlastne uvedené dve metódy na výpočet Smithovho kanonického tvaru matice (konštruktívna diagonalizácia a pomocou minorov $\eta_i(A)$). Prvky na diagonále Smithovho kan. tvaru matice A nazývame *invariantnými faktormi matice A*.

Pre zaujímavosť uvedieme, že veta o Smithovom kanonickom tvare platí aj v prípade, že okruh R je okruh hlavných ideálov, t.j. komutatívny obor integrity s jednotkou, v ktorom je každý ideál hlavný (uvidíme aj dôvod, prečo existencia nemusí platiť nad všeobecným gaussovským okruhom).

Potrebujeme všeobecnejšiu definíciu ekvivalencie matíc: Matice A, B typu $m \times n$ nazveme ekvivalentnými (zápis $A \doteq B$), ak existujú štvorcové matice P a Q, ktoré sú delitele jednotky v príslušných okruhoch matíc a platí $A = PBQ$. Podľa cvičení vieme, že ak sú matice ekvivalentné nad euklidovským okruhom, tak sú ekvivalentné aj v duchu tejto novej definície, na konci tejto časti dokážeme, že tieto dve definície sú pre prípad matíc nad euklidovskými okruhmi ekvivalentné, takže tým získavame zovšeobecnenie predošlej definície (z euklidovských okruhov na ľubovoľné okruhy).

Aby sme dokázali príslušnú vetu pre okruhy hlavných ideálov, potrebujeme urobiť hlavné kroky z dôkazu vety 1.1.3. Ako je vidieť, stačí preformulovať krok 1*b* a nájsť hodnotu, ktorá sa pre prvok v ľavom hornom rohu bude zmenšovať (ale stále to bude prirodzené číslo). V okruhu hlavných ideálov sa každý prvok rôzny od nuly dá jednoznačne (až na poradie a asociovanosť) zapísať ako súčin deliteľa jednotky a ireducibilných prvkov. Danému prvku $a \neq 0$ priradíme počet ireducibilných prvkov v (každom) takomto rozklade. Toto číslo označíme ako $g(a)$.

Predpokladajme teda, že máme nenulovú maticu A s nenulovým prvkom v ľavom hornom rohu a že $g(a_{11})$ nadobúda spomedzi všetkých $g(a_{ij})$ minimálnu hodnotu. Úlohou kroku $1b$ je získať v prvom riadku a stĺpci prvky s hodnotami $g(a_{1j}^-)$, $g(a_{k1}^-)$ nižšími ako bola hodnota $g(a_{11})$. Máme dve možnosti: $a_{11} \mid a_{1j}$, alebo nie. Ak áno, tento prvok sa vynuluje pomocou elementárnej operácie tretieho typu. Nech to neplatí. Potom určite $a_{1j} \not| a_{11}$ (bol by to spor s minimalitou hodnoty $g(a_{11})$). Položme $a = a_{11}$, $b = a_{1j}$. Najväčší spoločný deliteľ (a, b) označíme g. Potom existujú prvky c, d také, že $g = ac + bd$ (práve toto tvrdenie — platné v OHI, ale nie vo všeobecných gaussovských okruhoch — umožňuje pokračovať v dôkaze). Nech $a = g\bar{a}$, $b = g\bar{b}$. Potom máme $1 = \bar{a}c + \bar{b}d$. Uvažujeme teraz o maticiach U a U' definovaných nasledovne:

$$U = \begin{pmatrix} c & \dots & \bar{b} & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ d & \dots & -\bar{a} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & & \dots & & 1 \end{pmatrix} \qquad U' = \begin{pmatrix} \bar{a} & \dots & \bar{b} & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ d & \dots & -c & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & & \dots & & 1 \end{pmatrix},$$

kde sa vyznačené prvky nachádzajú v prvom a j-tom riadku a stĺpci. Na diagonálach v oboch maticiach sa mimo vyznačených prvkov nachádzajú len 1 a všetky ostatné prvky sú nuly. Ľahko sa presvedčíme, že $UU' = U'U = I$. Všimnime si ako vyzerá $B = AU$. Platí, že $b_{11} = g$ a $b_{1j} = 0$. Toto urobíme pre všetky prvky v prvom riadku (okrem ľavého horného, samozrejme). V tomto prípade sa mení prvok v ľavom hornom rohu už počas práce s jedným riadkom, ale stále platí pôvodná vlastnosť, že dĺžka rozkladu prvku v ľavom hornom rohu je v ľubovoľnom kroku úpravy prvého riadku menšia ako dĺžka rozkladu ľubovoľného iného nenulového prvku v prvom riadku. Urobíme krok $1a$ a potom robíme analogické operácie pre prvý stĺpec (dostaneme napr. transponovaním, rozmyslite si to!) Pozor, keď sme už vynulovali prvý riadok a nulujeme prvý stĺpec, môže sa pokaziť už urobený prvý riadok. Nevadí. Pri týchto operáciách sa stále skracuje dĺžka rozkladu prvku nachádzajúceho sa v ľavom hornom rohu — dĺžka tohoto rozkladu však nesmie klesnúť pod nulu a preto v konečnom počte krokov musíme prísť k matici, ktorá už v prvom riadku a stĺpci obsahuje len nuly (okrem ľavého horného rohu). Ďalej už pokračujeme presne podľa dôkazu vety 1.1.3. Tým dokážeme existenciu hľadanej matice. Jednoznačnosť sa opäť dokáže pomocou minorov a hodnôt $\eta_i(A)$, musíme však sformulovať a dokázať príslušnú lemu pre všeobecnejší prípad okruhu hlavných ideálov (zmenili sme totiž definíciu ekvivalencie matíc!). Toto bude predmetom cvičení.

Ešte si uveďme sľúbený dôkaz ekvivalentnosti definícií "ekvivalencie" matíc pomocou riadkových/stĺpcových operácií a pomocou násobenia zľava a sprava maticami, ktoré sú deliteľmi jednotky v príslušných okruhoch matíc pre matice nad euklidovskými okruhmi. Vzhľadom na cvičenia z úvodu stačí dokázať nasledujúcu vetu:

Veta 1.1.5 *Nech A je taká matica nad euklidovským okruhom, že existuje A' taká, že $AA' = I$, potom A je súčin elementárnych matíc (t.j. A sa dá z matice I "vyrobiť" pomocou elementárnych riadkových operácií).*

Dôkaz. Ak $AA' = I$ tak $\det(A).\det(A') = 1$ a teda $\det(A) \sim 1$. Vďaka vete o SKT pre maticu A existujú matice P a Q, ktoré sú súčinmi elementárnych matíc (P riadkových a Q stĺpcových, ale riadkové a stĺpcové sú to isté) také, že $PAQ = \mathrm{diag}(d_1, d_2, \dots)$.

Podľa dôkazu jednoznačnosti pre SKT vieme, že $1 \sim \det(A) = \eta_n(A) \sim \eta_n(\mathrm{diag}(d_1, d_2, \dots)) = d_1 \cdot d_2 \cdot \dots \cdot d_n$, t.j. všetky prvky $d_1, \dots, d_n$ sú delitele 1 a teda matica $\mathrm{diag}(d_1, d_2, \dots)$ môže byť priamo I.

Takže existujú matice P a Q, ktoré sú súčinmi elementárnych matíc také, že $PAQ = I$. Potom $A = P'Q'$, kde P' je súčin inverzných elementárnych matíc definujúcich P v opačnom poradí (t.j. ak $P = E_n E_{n-1} \dots E_1$ tak $P' = E_1^{-1} \dots E_{n-1}^{-1} E_n^{-1}$ a podľa jedného z cvičení vieme, že každá elementárna riadková operácia je invertibilná pomocou (dokonca práve jednej) riadkovej operácie, t.j. E_i^{-1} je tiež "riadková" elementárna matica) a podobne Q' zodpovedá príslušným inverzným stĺpcovým operáciám v opačnom poradí ako to bolo pri Q. Ale inverzná operácia ku stĺpcovej operácii je stĺpcová operácia a každá stĺpcová operácia je vlastne riadková operácia (výmena i-tého a j-tého stĺpca je to isté ako výmena i-tého a j-tého riadku, podobne s operáciou typu 2 a pre stĺpcovú operáciu 3-ieho typu, t.j. pripočítanie c násobku i-tého stĺpca ku j-tému stĺpcu je to isté ako pripočítanie c násobku j-tého riadku ku i-tému riadku). Teda aj P' aj Q' je súčin "riadkových" elementárnych matíc, t.j. aj A je súčin "riadkových" elementárnych matíc. □

Cvičenie 7 *Nech A a B sú matice ekvivalentné nad gaussovským okruhom R (použijeme rovnakú definíciu ako pre okruhy hlavných ideálov). Potom každý minor rádu r matice B (A) je lineárnou kombináciou minorov rádu r matice A (B).*

Cvičenie 8 *Nech A a B sú matice ekvivalentné nad gaussovským okruhom R Potom pre všetky prípustné indexy i platí $\eta_i(A) \doteq \eta_i(B)$. Ak matica A má Smithov kanonický tvar, tak je tento určený až na asociovanosť*

jednoznačne. Invariantné faktory matice A sa v tomto prípade dajú vypočítať pomocou hodnôt $\eta_i(A)$, rovnako, ako je to uvedené v poznámke za vetou 1.1.3.

Cvičenie 9 *Nech R je gaussovský okruh a nech $a, b \in R$ sú také, že $1 = (a, b)$, ale neexistujú také $u, v \in R$, že $1 = au + bv$. Potom diagonálna štvorcová matica 2×2 s diagonálnymi prvkami a, b nemá Smithov kanonický tvar. Dokážte!*

Cvičenie 10 *Dokážte, že štvorcová diagonálna matica $D = \mathrm{diag}(d_1, d_2, \ldots)$ nad Gaussovským okruhom je deliteľom jednotky práve vtedy, keď pre každé prípustné i platí $d_i \mid 1$ (v danom okruhu).*

Cvičenie 11 *Nech $d = (a_1, \ldots, a_n)$ (najv.spol.del.) v okruhu R hlavných ideálov. Dokážte, že existuje štvorcová matica A $n \times n$ taká, že $(a_1, \ldots, a_n) \cdot A = (d, 0, \ldots, 0)$.*

Cvičenie 12 *Nech prvky $a_{11}, a_{12}, \ldots, a_{1n}$ sú nesúdeliteľné prvky okruhu hlavných ideálov R. Dokážte, že existuje matica $A = ||a_{ij}||_{m \times n}$, ktorá je deliteľom jednotky v okruhu štvorcových matíc typu $n \times n$ nad R.*

Cvičenie 13 *Nájdite Smithov kanonický tvar matice A nad $Q[x]$. Určte aj matice P, Q s vlastnosťou $PAQ = D$ (= kanonický tvar matice A).*

$$A = \begin{pmatrix} x-17 & 8 & 12 & -14 \\ -46 & x+22 & 35 & -41 \\ 2 & -1 & x-4 & 4 \\ -4 & 2 & 2 & x-3 \end{pmatrix}$$

1.2 Úvod do teórie modulov

Definícia 1.2.1 *Nech R je okruh a nech $(M,+)$ je komutatívna grupa. Potom dvojicu (R,M) spolu s "binárnym párovaním" $\odot : R \times M \to M$ nazývame* ľavostranným modulom nad okruhom R *ak:*

1. *pre $a \in R$ a $x,y \in M$ platí $a \odot (x+y) = (a \odot x) + (a \odot y)$*
2. *pre $a,b \in R$ a $x \in M$ platí $(a+b) \odot x = (a \odot x) + (b \odot x)$*
3. *pre $a,b \in R$ a $x \in M$ platí $a \odot (b \odot x) = (ab) \odot x$*

Podobne sa definuje pravostranný modul nad R. Binárne párovanie z uvedenej definície sa zvyčajne nazýva *skalárny súčin*. My sa budeme zaoberať výlučne ľavostrannými modulmi. Naviac nás budú zaujímať len moduly nad komutatívnymi okruhmi s jednotkou spĺňajúce ešte podmienku

4. pre $x \in M$ platí $1 \odot x = x$.

Moduly nad komutatívnymi okruhmi s jednotkou spĺňajúce túto podmienku nazývame *unitárne* moduly.

Príklady

1. Každý vektorový priestor $V(F)$ nad poľom F je ľavostranný modul nad poľom F.
2. Nech $(M,+)$ je kom. grupa. Ukážeme, že (Z,M) je unitárny modul nad okruhom celých čísel Z: nech $n \in Z$, $x \in M$. Položme $n \odot x = x + x + \cdots + x$ (n-krát, dá sa to definovať aj induktívnou definíciou). Ďalej položme $0 \odot x = 0$ a nakoniec $(-n) \odot x = -(n \odot x)$ pre záporné čísla. Presvedčte sa, že (Z,M) spĺňa podmienky 1 až 4 z definície modulov.
3. Nech I je ideál okruhu R. Potom (R,I) je modul nad R, ak skalárny súčin definujeme ako násobenie v okruhu R. Zrejme $ax \in I$, lebo I je ideál. Podmienky 1 až 4 vyplývajú priamo z definície okruhu.
4. Pre nás bude najdôležitejsí nasledujúci príklad: Nech $V(F)$ je konečnorozmerný vektorový priestor nad poľom F. Nech A je lineárna transformácia na tomto priestore. S touto transformáciou máme hneď aj transformácie $A^2, A^3, \ldots$ Ďalej pre $a \in F, k \in N$ máme transformáciu označovanú ako aA^k a definovanú vzťahom $x(aA^k) = (ax)A^k$ $(= a(xA^k))$. Nakoniec, pre ľubovoľný "polynóm $f \in F[\gamma]$ v bode A" $(f(A))$ môžeme vytvoriť transformáciu $f(A) = a_0I + a_1A + \cdots + a_kA^k$ položiac $x(a_0I + a_1A + \cdots + a_kA^k) = a_0x + x(a_1A) + \cdots + x(a_kA^k)$. Je to transformácia na $V(F)$. Ak v okruhu polynómov $F[\gamma]$ platí $h(\gamma) = f(\gamma)g(\gamma)$, tak $h(A) = f(A) \circ g(A)$, kde $\circ$ znamená skladanie zobrazení (v prípade, že transformáciu A reprezentujeme maticou, môžeme aj $f(A)$, $g(A)$, $h(A)$ reprezentovať maticami a potom je $\circ$ násobenie matíc. (Overte!)

   Teraz definujeme (ľavostranný) unitárny modul $(F[\gamma], V(F), A)$ určený lineárnou transformáciou A na $V(F)$. Pre $f(\gamma) \in F[\gamma]$ a $x \in V(F)$ položíme $f(\gamma) \odot x = xf(A)$. Overte platnosť podmienok 1 až 4 z definície (ľavostranného) unitárneho modulu.

Namiesto $a \odot x$ budeme (ak nebude hroziť nedorozumenie) písať len ax. Podobne, ak bude jasná transformácia A, budeme vyššie uvedený modul písať len ako $(F[\gamma], V)$.

Definícia 1.2.2 *Nech (R,M) je modul. Nech K je podgrupa grupy $(M,+)$. Potom (R,K) nazývame podmodulom modulu (R,M), ak pre $a \in R$ a $x \in K$ je vždy $ax \in K$.*

Nech (R,M), (R,K) sú dva moduly nad R. Nech $\varphi : M \to K$ je grupový homomorfizmus. Potom hovoríme, že φ je modulový homomorfizmus, ak naviac pre každé $a \in R$ a $x \in M$ platí $(ax)\varphi = a(x\varphi)$.

Lema 1.2.3 *Majme modul (R,M). Majme neprázdny systém podmodulov $\{K_\alpha;\ \alpha \in I\}$ modulu (R,M). Potom $\bigcap\{K_\alpha;\ \alpha \in I\}$ je podmodul modulu (R,M).*

Dôkaz. D.Ú. □

Definícia 1.2.4 *Majme $\emptyset \neq X \subseteq M$, kde (R,M) je modul. Nech $[X]$ značí množinový prienik všetkých podmodulov modulu (R,M) obsahujúcich množinu X. Predošlá lema zabezpečuje skutočnosť, že $[X]$ je tiež podmodul modulu (R,M). Nazývame ho podmodul generovaný množinou X. Prvky z množiny X sa nazývajú generátormi (pod)modulu $[X]$. Ak pre nejakú konečnú množinu $X \subseteq M$ je $[X] = M$, hovoríme, že (R,M) je* konečne generovaný *modul.*

Cvičenie 14 *Nech (R, M) je modul, R je komutatívny okruh. Pre $a \in R$ a $x \in M$ definujme $x \odot a = ax$ (pomocou ľavostranného skalárneho súčinu sme definovali pravostranný). Dokážte, že týmto dostaneme pravostranný modul nad R.*

Odteraz sa už budeme zaoberať len ľavostrannými modulmi.

Cvičenie 15 *Nech (R, M) je modul. Dokážte nasledujúce rovnice:*

$$a0 = 0, \quad a(-x) = -(ax), \quad 0x = 0, \quad (-a)x = -(ax).$$

Cvičenie 16 *Nech (R, M) je unitárny modul. Potom (R, K) je podmodul modulu (R, M) práve vtedy, keď $a, b \in R$ a $x, y \in K$ implikuje $ax + by \in K$.*

Cvičenie 17 *Nech (R, K) je modul nad komutatívnym okruhom R, nech $X \subseteq M$. Dokážte, že*

$$\begin{aligned}[X] = \{z \in K;\ z &= n_1 \times x_1 + \cdots + n_r \times x_r + a_1 y_1 + \cdots + a_s y_s \ \& \\ &\& \quad r, s \in N \ \&\ n_1, \ldots, n_r \in Z \ \&\ a_1, \ldots, a_s \in R \ \& \\ &\& \quad x_1, \ldots, x_r, y_1, \ldots, y_s \in X\}.\end{aligned}$$

Ak (R, K) je unitárny modul, potom vieme predošlú formulu "zjednodušiť":

$$[X] = \{z \in K;\ z = a_1 y_1 + \cdots + a_s y_s \ \&\ s \in N \ \&\ a_1, \ldots, a_s \in R \ \&\ y_1, \ldots, y_s \in X\}.$$

Cvičenie 18 *Relácia ekvivalencie Θ na M sa nazýva kongrueniou modulu (R, M), ak Θ je kongrueniou na grupe M a $x \cong y\,(\Theta)$ implikuje $ax \cong ay\,(\Theta)$ pre všetky $a \in R$.*
Dokážte:

(i) Ak Θ je kongruencia na (R, M), tak jadro tejto kongruencie $\{z \in M;\ z \cong 0\,(\Theta)\}$ je podmodul modulu (R, M)

(ii) Nech K je podmodul modulu (R, M). Definujme $\Theta[K]$ nasledovne: $x \cong y\,(\Theta)$ práve vtedy, keď $x - y \in K$. Potom $\Theta[K]$ je kongruencia na (R, M) a jadro tejto kongruencie $\operatorname{Ker}\Theta[K] = K$. Dokážte!

(iii) Dokážte, že dve kongruencie na module (R, M) sa rovnajú práve vtedy, keď majú rovnaké jadrá.

Cvičenie 19 *Nech Θ je kongruencia na module (R, M). Nech $K = \operatorname{Ker}\Theta$. Označme faktorovú množinu $M/\Theta = M/K = \{x + K;\ x \in M.\}$ Dokážte, že $(R, M/\Theta)$ (t.j. $(R, M/K)$) je modul, ak položíme $a(x + K) = ax + K$ pre $a \in R$. Nazývame ho faktorovým modulom, alebo aj diferenčným modulom a označujeme ho $M - K$.*

Cvičenie 20 *Nech $\varphi : M \to K$ je homomorfizmus modulov. Dokážte:*

1. *ak L je podmodul modulu M, tak $\varphi(L) = \{z \in K;\ (\exists x \in L)\, z = \varphi(x)\}$ je podmodul modulu K*
2. *ak L je podmodul modulu K, tak $\varphi^{-1}(L) = \{z \in M;\ \varphi(z) \in L\}$ je podmodul modulu M*
3. *relácia Θ_φ definovaná vzťahom $x \cong y\,(\Theta_\varphi)$ práve vtedy, keď $\varphi(x) = \varphi(y)$ je kongruencia na module M*
4. *nech je homomorfizmus φ surjekciou. Potom je diferenčný modul M/Θ_φ izomorfný s modulom K. (Označenie: $M/\Theta_\varphi \cong K$)*
5. *nech Θ je kongruencia na module M. Utvorme faktorový modul M/Θ. Dokážte, že existuje epimorfizmus (tzv. kanonický) $\tau : M \to M/\Theta$, jadrom ktorého je práve jadro kongruencie Θ, t.j., že platí*

$$\operatorname{Ker}\tau = \{z \in M;\ \tau(z) = 0\} = \operatorname{Ker}\Theta$$

Cvičenie 21 *Nech $\varphi : M \mapsto K$ je homomorfimus modulov (nad rovnakým okruhom), nech $L \subseteq M$ je podmodul M. Potom $L\varphi$ je podmodul modulu K.*

Dokážte nasledovné tvrdenia: zobrazenie $\overline{\varphi} : M/L \mapsto K/L\varphi$ definované vzťahom $\overline{\varphi}(m + L) = \varphi(m) + L\varphi$ je naozaj zobrazením — t.j. nezávisí od výberu m v definícii — a je to homomorfizmus. Ak je φ izomorfizmus, aj $\overline{\varphi}$ je izomorfizmus.

1.2.1 Voľné moduly

Definícia 1.2.5 *Unitárny modul (R, M) nazývame* voľným modulom nad množinou voľných generátorov S, *ak*

1. $[S] = (R, M)$ *a*
2. *ak* $a_1x_1 + \cdots + a_nx_n = 0$ *pre* $a_i \in R$ *a po dvoch rôzne* $x_1, \ldots, x_n \in S$, *tak* $a_1 = a_2 = \cdots = a_n = 0$.

V takomto prípade budeme pre (R, M) používať tiež označenie $F_R(S)$. Množinu voľných generátorov S tiež nazývame bázou voľného modulu $F_R(S)$. $F_R(n)$ znamená voľný modul s n prvkovou bázou. $F_R(0)$ je jednoprvkový (triviálny) modul, obsahuje len nulový vektor.

Je hneď vidieť, že vo voľnom module sa dá každý nenulový prvok a napísať ako lineárna kombinácia konečne veľa po dvoch rôznych prvkov bázy *jednoznačným spôsobom* (bez nulových koeficientov, nulové koeficitenty môžu „nejednoznačnosť“), lebo rozdiel dvoch spôsobov zápisu toho istého prvku musí byť nula, t.j. takýto rozdiel musí mať rovnaké koeficienty s opačným znamienkom pri rovnakých prvkoch z S.

Nasledujúca veta sa často používa ako alternatívna definícia pojmu voľný modul.

Veta 1.2.6 *Nech (R, M) je unitárny modul. Potom (R, M) je voľný modul práve vtedy, ak*

1. $[S] = (R, M)$,
2. *každé zobrazenie $f : S \to K$ do (ľubovoľného) unitárneho modulu (R, K) sa dá jediným spôsobom rozšíriť na homomorfizmus $\varphi : M \to K$, t.j. $\varphi \restriction S = f$ (t.j. $(\forall x \in S)(\varphi(x) = f(x))$).*

Dôkaz. Nech je teda (R, M) voľný modul. Dokážeme len druhú podmienku uvedenú v tejto vete. Nech $f : S \to K$. Nech $a \in (R, M) = [S]$, t.j. $a = a_1x_1 + \cdots + a_nx_n$ pre vhodné (a jednoznačne určené) $a_i \in R$ a po dvoch rôzne $x_i \in S$. Položme

$$\varphi(a) = a_1f(x_1) + \cdots + a_nf(x_n).$$

Z jednoznačnosti zápisu prvku a plynie to, že φ je *zobrazenie* $M \to K$.

Z definície je tiež hneď vidieť, že $\varphi \restriction S = f$.

Ešte overíme, že φ je homomorfizmus. Nech $a = a_1x_1 + \cdots + a_nx_n$ a $b = b_1x_1 + \cdots + b_nx_n$ (bez újmy na všeobecnosti môžeme predpokladať takýto tvar prvkov a a b, lebo v prípade potreby môžeme dať ako niektoré z koeficientov nuly). Potom

$$\begin{aligned}
\varphi(a + b) &= \varphi((a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n) \\
&= (a_1 + b_1)f(x_1) + \cdots + (a_n + b_n)f(x_n) \\
&= a_1f(x_1) + \cdots + a_nf(x_n) + b_1f(x_1) + \cdots + b_nf(x_n) \\
&= \varphi(a) + \varphi(b)
\end{aligned}$$

Nech je $c \in R$. Potom

$$\begin{aligned}
\varphi(c \odot a) &= \varphi(ca_1x_1 + \cdots + ca_nx_n) = ca_1f(x_1) + \cdots + ca_nf(x_n) = \\
&= c \odot (a_1f(x_1) + \cdots + a_nf(x_n)) = c \odot \varphi(a)
\end{aligned}$$

Je tiež vidieť, že ak má byť φ homomorfizmus, tak sme ho nemohli definovať inak, než ako sme to urobili.

Teraz dokážeme druhú implikáciu, opäť sa sústredíme len na dôkaz druhej vlastnosti z definície voľného modulu. Nech teda $a_1x_1 + \cdots + a_nx_n = 0$, x_i sú po dvoch rôzne. Uvažujme teraz o zobrazení $f_i : S \to R$ definovanom predpisom

$f_i(x_i) = 1$ a $f_i(x) = 0$ pre $x \in S - \{x_i\}$

(tu pokladáme R za unitárny modul (R, R), R je okruh s 1). Podľa predpokladu existuje rozšírenie f_i na homomorfizmus $\varphi_i : M \to R$ a pre tento platí

$$0 = \varphi_i(0) = \varphi_i(a_1x_1 + \cdots + a_nx_n) = a_1f_i(x_1) + \cdots + a_nf_i(x_n) = a_i \odot 1 = a_i.$$

□

Naznačíme spôsob, akým sa konštruujú tzv. priame súčiny modulov (konečného) počtu modulov nad R. Nech $(R, M_1), (R, M_2), \ldots, (R, M_n)$ sú moduly nad R. Nech $M = M_1 \times M_2 \times \ldots \times M_n$ je priamy súčin grúp (t.j. kartézsky súčin s operáciou definovanou po zložkách). Binárne párovanie z $R \times M$ do M definujeme tiež po zložkách, t.j. pre $a \in R$ a $(x_1, \ldots, x_n) \in M$ položíme $a \odot (x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$. Ľahko sa dá overiť, že týmto je definovaný modul (R, M).

Lema 1.2.7 *Nech je modul (R, M) (izomorfný s) priamym súčinom modulov (R, M_1), (R, M_2), ..., (R, M_n). Potom pre $i = 1, \ldots, n$ existujú podmoduly P_i modulu (R, M) tak, že platí:*

1. *$M_i \cong P_i$ pre všetky $i = 1, \ldots, n$*
2. *$M = [P_1 \cup \cdots \cup P_n]$ a*
3. *$\{0\} = P_i \cap [P_1 \cup \cdots \cup P_{i-1}]$ pre všetky $i = 2, \ldots, n$.*

Dôkaz. Dôkaz urobíme len pre prípad, keď je modul (R, M) priamym súčinom (R, M_1), (R, M_2), ..., (R, M_n). (Prípad s izomorfizmom si rozmyslite ako D.Ú.) Položme

$$P_i = \{(0, \ldots, 0, x_i, 0, \ldots, 0);\ x_i \in M_i\}$$

(x_i sa v n-tici uvedenej v definícii množiny P_i nachádza na i-tom mieste, všetky ostatné miesta sú zaplnené nulami.) Zrejme takto definované podmoduly modulu (R, M) spĺňajú všetky potrebné podmienky. □

Veta 1.2.8 *Modul (R, M) je izomorfný s priamym súčinom konečného počtu modulov práve vtedy, ak existuje $n \in N$ a existujú podmoduly P_i modulu (R, M) tak, že platí:*

1. *$M = [P_1 \cup \cdots \cup P_n]$ a*
2. *$\{0\} = P_i \cap [P_1 \cup \cdots \cup P_{i-1}]$ pre všetky $i = 2, \ldots, n$.*

Ak sú splnené uvedené dve podmienky, tak $(R, M) \cong (R, P_1 \times P_2 \times \ldots \times P_n)$.

Dôkaz. Vďaka predošlej leme stačí už dokázať postačujúcosť uvedených podmienok. Na to, aby sme dokázali, že $(R, P_1 \times P_2 \times \ldots \times P_n) \cong (R, M))$, potrebujeme nájsť izomorfizmus. Nech $(x_1, \ldots, x_n) \in P_1 \times P_2 \times \ldots \times P_n$. Položme

$$\varphi((x_1, \ldots, x_n)) = x_1 + \cdots + x_n.$$

Z prvej podmienky vo vete vidíme, že toto zobrazenie je surjektívne.

Dokážeme injektivitu φ: Nech $x_1 + \cdots + x_n = y_1 + \cdots + y_n$. Nech i je posledný index pre ktorý platí $x_i \neq y_i$. Nech je $i > 1$. Potom

$$x_i - y_i = y_1 - x_1 + \cdots + y_{i-1} - x_{i-1}.$$

Prvok na ľavej strane tejto rovnosti patrí do P_i a prvok na pravej strane patrí do $[P_1 \cup \cdots \cup P_{i-1}]$, z druhej vlastnosti požadovanej v tejto vete preto vyplýva, že $x_i - y_i = 0$ — spor.

Prípad $i = 1$ je tiež veľmi jednoduchý (D.Ú.). Teda pre žiadny index neplatí $x_i \neq y_i$ a zobrazenie φ je injektívne. Na overenie homomorfnosti φ slúžia nasledujúce jednoduché výpočty:

$$\begin{aligned}
\varphi((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) &= \varphi((x_1 + y_1, \ldots, x_n + y_n)) = \\
&= (x_1 + y_1) + \cdots + (x_n + y_n) = \\
&= (x_1 + \cdots + x_n) + (y_1 + \cdots + y_n) = \\
&= \varphi((x_1, \ldots, x_n)) + \varphi((y_1, \ldots, y_n))
\end{aligned}$$

$$\begin{aligned}
\varphi(c \odot (x_1, \ldots, x_n)) &= \varphi((cx_1, \ldots, cx_n)) = cx_1 + \cdots + cx_n = \\
&= c \odot (x_1 + \cdots + x_n) = c \odot \varphi((x_1, \ldots, x_n))
\end{aligned}$$

□

Priamy súčin modulov $(R, M_1 \times M_2 \times \ldots \times M_n)$ budeme tiež zapisovať ako $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

Veta 1.2.9 *Nech R je okruh, nech $M = [e_1, \ldots, e_n]$. Potom $M = [e_1] \oplus \cdots \oplus [e_n]$ práve vtedy, keď z rovnice $a_1e_1 + \cdots + a_ne_n = 0$ vyplýva, že $a_1e_1 = \cdots = a_ne_n = 0$.*

Dôkaz. Nech $a_1e_1 + \cdots + a_ne_n = 0$, nech i je najväčšie také, že $a_ie_i \neq 0$. Potom

$$\overbrace{a_1e_1 + \cdots + a_{i-1}e_{i-1}}^{\in [e_1 \cup \cdots \cup e_{i-1}]} = \overbrace{-a_ie_i}^{\in [e_i]} \qquad (\neq 0),$$

čo je ale spor s predošlou vetou.

Nech naopak pre niektoré i je $[e_1, \ldots, e_{i-1}] \cap [e_i] \neq \{0\}$. Potom existujú $a_1, \ldots, a_i$ tak, že $a_ie_i \neq 0$ a

$$a_1e_1 + \cdots + a_{i-1}e_{i-1} = -a_ie_i,$$

t.j. $a_1e_1 + \cdots + a_ie_i = 0$ a $a_ie_i \neq 0$. □

Veta 1.2.10 *Nech R je okruh s 1. Potom modul $(R, R_1 \times \ldots \times R_n)$, $n \geq 1$, kde $R_1 = \cdots R_n = R$ (ktorý je zrejme unitárny) je voľný modul nad n prvkovou množinou voľných generátorov $S = \{e_1, \ldots, e_n\}$, kde $e_1 = (1, 0, \ldots, 0)$,...,$e_n = (0, \ldots, 0, 1)$.*

Dôkaz. Zrejme $(x_1, \ldots, x_n) = x_1e_1 + \cdots + x_ne_n$, t.j. $[S] = R_1 \times \ldots \times R_n$. Druhá vlastnosť požadovaná definíciou voľného modulu vyplýva zo základných vlastností usporiadaných n-tíc (dve n-tice sa rovnajú práve vtedy, keď ...) □

Veta 1.2.11 *Nech R je OHI. Potom každý podmodul voľného modulu $F_R(n)$ je voľný modul s konečnou bázou o $m \leq n$ prvkoch (t.j. existuje báza, ktorá má najviac n prvkov).*

Dôkaz. Dôkaz urobíme indukciou. Pre $n = 0$ je $F_R(n)$ totožný s jediným svojím podmodulom, tvrdenie teda platí.

Majme dané $n \geq 1$. Nech tvrdenie platí pre každé $m < n$, dokážeme, že platí pre n. Nech $L \neq \{0\}$ je podmodul modulu $F_R(n)$. Nech $u_1, \ldots, u_n$ je báza $F_R(n)$. Položme

$$R_L = \{a_1 \in R;\, (\exists a_2, \ldots, a_n \in R)\, a_1u_1 + \cdots + a_nu_n \in L\}.$$

Overíme, že R_L je ideál okruhu R. Nech $a_1, b_1 \in R_L$. Potom existujú $a_2, \ldots, a_n \in R$ a $b_2, \ldots, b_n \in R$ také, že $a_1u_1 + \cdots + a_nu_n \in L$ a tiež $b_1u_1 + \cdots + b_nu_n \in L$. Potom ale

$$a_1u_1 + \cdots + a_nu_n + b_1u_1 + \cdots + b_nu_n = (a_1 + b_1)u_1 + \cdots + (a_n + b_n)u_n \in L$$

a

$$r \odot (a_1u_1 + \cdots + a_nu_n) = (ra_1)u_1 + \cdots + (ra_n)u_n \in L,$$

(r je ľubovoľný prvok z R) pretože L je podmodul. Preto $a_1 + b_1$, $ra_1 \in R_L$ a R_L je skutočne ideál.

R je podľa predpokladu OHI a preto existuje $d \in R$ také, že $R_L = (d)$. Ak $d = 0$, znamená, že $L \subseteq [u_2, \ldots, u_n]$, kde $[u_2, \ldots, u_n]$ je zrejme $F_R(n-1)$ a teda podľa indukčného predpokladu tvrdenie platí. Nech teda $d \neq 0$ a nech $L' = L \cap [u_2, \ldots, u_n]$. L' je podmodul modulu $F_R(n-1)$, je to teda (ind. predpoklad) voľný modul o nanajvýš $n-1$ generátoroch. Nech teda $v_2, \ldots, v_k$, $k \leq n$ tvoria bázu L'. Nech v_1 je ľubovoľný prvok z L taký, že $v_1 = du_1 + a_2u_2 + \cdots a_nu_n$ pre nejaké $a_2, \ldots, a_n \in R$. (dôležité, je, že prvá "súradnica" vektora v_1 je d)

Dokážeme, že $v_1, \ldots, v_k$ je báza L.

Najprv dokážeme, že $v_1, \ldots, v_k$ generuje L. Nech teda $v \in L$, nech $v \notin L'$. Potom $v = a_1u_1 + \cdots + a_nu_n$, kde $d|a_1$, lebo $a_1 \in R_L$ t.j. $a_1 = ad$. Potom $v - av_1 \in L'$ a preto $v - av_1 = b_2v_2 + \cdots + b_kv_k$. Nakoniec dostávame, že $v = av_1 + b_2v_2 + \cdots + b_kv_k$, t.j. $L = [v_1, \ldots, v_k]$.

Nakoniec nám ešte ostalo dokázať nezávislosť vektorov $v_1, \ldots, v_k$. Nech teda $a_1v_1 + \cdots + a_kv_k = 0$. Potom $a_1v_1 + \cdots + a_kv_k = a_1du_1 + b_2u_2 + \cdots + b_nu_n$ pre vhodné $b_2, \ldots, b_n \in R$, pretože $v_2, \ldots, v_k \in L' \subseteq [u_2, \ldots, u_n]$. Keďže $u_1, \ldots, u_n$ je báza $F_R(n)$, musí byť $a_1d = 0$ a pretože sme v obore integrity, je $a_1 = 0$. To znamená, že $a_2v_2 + \cdots + a_kv_k = 0$. Pretože $v_2, \ldots, v_k$ tvoria bázu L', platí, že $a_2 = \cdots = a_k = 0$. Tým je lineárna nezávislosť vektorov $v_1, \ldots, v_k$ dokázaná. □

Veta 1.2.12 *Nech R je obor integrity s 1, nech (R, M) je konečnogenerovaný voľný modul, nech $\alpha_1, \ldots, \alpha_n$ a $\beta_1, \ldots, \beta_m$ sú dve bázy tohoto modulu. Potom $m = n$.*

Dôkaz. Vnorením nášho modulu do vektorového priestoru $M(Q(R))$, kde $Q(R)$ je podielové pole oboru integrity R zistíme, že $\alpha_1, \ldots, \alpha_n$ sú (v tomto vektorovom priestore) vektory, ktoré generujú celý priestor. Ak by potom $n < m$, tak vektory $\beta_1, \ldots, \beta_m$ musia byť lineárne závislé nad poľom $Q(R)$, t.j. niektorý z nich je lineárnou kombináciou predošlých. Nech teda napr.

$$\beta_k = a_1\beta_1 + \cdots + a_{k-1}\beta_{k-1},$$

kde $a_i \in Q(R)$. Potom vynásobením vhodným prvkom $a \in R$ (najmenší spoločný násobok menovateľov prvkov $a_1, \ldots, a_{k-1}$) dostaneme nad okruhom R rovnicu

$$a\beta_k = b_1\beta_1 + \cdots + b_{k-1}\beta_{k-1},$$

kde $a, b_i \in R$, čo znamená, že $\beta_1, \ldots, \beta_n$ boli už závislé nad okruhom R — spor. □

Až táto veta nám umožňuje dívať sa na bázu voľného modulu (nad oborom integrity) ako na bázu vektorového priestoru.

Pripomeňme si definíciu priameho súčinu modulov:

Definícia 1.2.13 *Nech* $\{(R, M_i)\,;\, i \in I\}$ *je množina modulov. Potom*

$$\Pi(M_i \,:\, i \in I) = \{f\colon I \to \bigcup(M_i \,:\, i \in I)\,;\, f(i) \in M_i, i \in I\}$$

je tzv. kartézsky súčin množín M_i, $i \in I$. *Na tejto množine definujme operácie* $\oplus$ *a* $\odot$ *po zložkách, t.j. pre* $f, g \in \Pi(M_i \,:\, i \in I)$ *kladieme* $(f \oplus g)(i) = f(i) + g(i)$ *a* $(f \odot g)(i) = f(i) \cdot g(i)$ *pre* $i \in I$. *Operácie* $+$ *a* $\cdot$ *v predošlých rovniciach sú vždy príslušné operácie v moduloch* M_i.

Cvičenie 22 *Nech* (R, M_i), $i \in I$ *sú unitárne moduly. Potom priamy súčin týchto modulov* $K = \Pi(M_i\,;\, i \in I)$ *je tiež unitárny modul. Uvažujme o podmnožine* $L = \{f \in K;\, f(i) = 0$ *pre skoro všetky (t.j. všetky až na konečný počet)* $i \in I\}$. *Dokážte, že* L *je podmodul modulu* (R, K) *- toto tvrdenie platí aj bez predpokladu na unitárnosť modulov* M_i. *Modul* L *nazývame priamy súčet modulov* (R, M_i), $i \in I$ *a značíme ho* $\Sigma(M_i\,;\, i \in I)$.

Cvičenie 23 *Nech* K *je priamy súčet modulov* (R, M_i), $i \in I$. *Dokážte:* K *obsahuje podmoduly* P_i, $i \in I$ *také, že*

1. $P_i \cong M_i$
2. $K = [\bigcup(P_i;\, i \in I)]$
3. *pre všetky* $i \in I$ *platí* $\{0\} = P_i \cap [\bigcup(P_j;\, j \in I - \{i\})]$

Cvičenie 24 *Dokážte aj nasledujúce zovšeobecnenie príslušnej vety dokázanej pre konečne mnoho modulov:*
Modul (R, M) *je (izomorfný s) priamym súčtom modulov nad* R *indexovaných množinou* I *práve vtedy, keď existujú podmoduly* P_i, $i \in I$ *modulu* (R, M) *také, že*

1. $M = [\bigcup(P_i;\, i \in I)]$
2. *pre všetky* $i \in I$ *platí* $\{0\} = P_i \cap [\bigcup(P_j;\, j \in I - \{i\})]$

Ak sú splnené tieto dve podmienky, tak $(R, M) \cong \Sigma(P_i\,;\, i \in I)$.

Cvičenie 25 *Dokážte aj nasledujúce zovšeobecnenie príslušnej vety dokázanej pre konečne mnoho modulov:*
Nech R *je okruh s* 1. *Potom priamy súčet modulov* $\Sigma(R_i\,;\, i \in I)$, *kde pre všetky* $i \in I$ *je* $R_i \cong R$ *je voľný modul nad* R *s množinou voľných generátorov* $S = \{e_i;\, i \in I\}$, *kde* $e_i(j) = 1$ *ak* $i = j$ *a* $e_i(j) =$ *ak* $j \in I - \{i\}$.

Cvičenie 26 *Nech* R *je komutatívny obor integrity s* 1, *nech nie je OHI (napr.* $R = Z[x]$*). Dokážte, že* (R, R) *je voľný modul s jednoprvkovou bázou, ale obsahuje podmodul, pre ktorý neplatí veta 1.2.11.*

Cvičenie 27 *Nech* (R, M) *je voľný modul s jednou konečnou bázou (žiadny špeciálny predpoklad na* R *nerobíme, môže to byť ľubovoľný komutatívny okruh s* 1*). Potom všetky bázy tohoto modulu sú konečné a všetky majú rovnaký počet prvkov.*

Toto cvičenie je asi dosť náročné, pri jeho dôkaze je dobre využiť pojem determinantu ako alternujúcej multilineárnej funkcie z daného konečne generovaného (voľného) modulu do okruhu R (viď napr. príslušné časti v kapitole IX, tvrdenie nášho cvičenia je vlastne veta 7 v IX.4 v [**?**]).

Lema 1.2.14 *Nech* $t_1, \ldots, t_n$ *a* $p_1, \ldots, p_n$ *sú dve bázy voľného modulu* (R, M). *Potom matica prechodu od bázy* $p_1, \ldots, p_n$ *ku báze* $t_1, \ldots, t_n$, *t.j. matica* $A = ||a_{ij}||_{n\times n}$ *nad okruhom* R *určená vzťahmi* $t_i = \Sigma_{j=1}^n a_{ij} p_j$ *pre každé* $i = 1, \ldots, n$ *je deliteľom jednotky v príslušnom okruhu matíc, t.j. má inverznú maticu.*

Dôkaz. Keďže aj $t_1, \ldots, t_n$ je báza, existuje $B = ||b_{ij}||_{n\times n}$ matica prechodu od bázy $t_1, \ldots, t_n$ ku báze $p_1, \ldots, p_n$, t.j. b_{ij} sú také, že $p_i = \Sigma_{j=1}^n b_{ij} t_j$. Počítajme teraz napr.

$$p_i = \Sigma_{j=1}^n b_{ij} t_j = \Sigma_{j=1}^n b_{ij}(\Sigma_{k=1}^n a_{jk} p_k) = \Sigma_{k=1}^n (\Sigma_{j=1}^n b_{ij} a_{jk}) p_k$$

Keďže p_i má v báze $p_1, \ldots, p_n$ jednoznačný zápis, a to $p_i = 0 \cdot p_1 + \cdots + 0 \cdot p_{i-1} + 1 \cdot p_i + 0 \cdot p_{i+1} + \cdots + 0 \cdot p_n$, dostávame odtiaľ, že $\Sigma_{j=1}^n b_{ij} a_{jk} = \delta_{ij}$, v maticovom zápise $BA = E$. Podobne sa dá dokázať, že $AB = E$, t.j. A má inverznú maticu. □

Lema 1.2.15 *Nech* $A = ||a_{ij}||_{n\times n}$ *je štvorcová matica nad komutatívnym okruhom* R *s* 1. *Nech ku* A *existuje inverzná matica* $B = ||b_{ij}||_{n\times n}$. *Nech* (R, M) *je voľný modul s bázou* $t_1, \ldots, t_n$, *nech sú vektory* $p_1, \ldots, p_n$ *definované vzťahmi* $p_i = \Sigma_{j=1}^n a_{ij} t_j$ *pre* $i = 1, \ldots n$. *Potom* $p_1, \ldots, p_n$ *tiež tvoria bázu modulu* (R, M).

Dôkaz. Rovnosť $[p_1, \ldots, p_n] = M$ dokážeme tým, že dokážeme, že pre všetky $i = 1, \ldots n$ platí, že $t_i \in [p_1, \ldots, p_n]$. Z faktu, že $BA = E$ vyplýva, že pre každé prípustné i platí: $\Sigma_j b_{ij} p_j = \Sigma_j b_{ij} (\Sigma_{k=1}^n a_{jk} t_k) = \Sigma_k (\Sigma_j b_{ij} a_{jk}) t_k = t_i$.

Ešte potrebujeme dokázať, že vektory $p_1, \ldots, p_n$ sú "nezávislé": nech teda $c_1 p_1 + \cdots + c_n p_n = 0$. Platí

$$c_1 p_1 + \cdots + c_n p_n = (\Sigma c_i a_{i1}) t_1 + \cdots + (\Sigma c_i a_{in}) t_n = 0$$

Keďže $t_1, \ldots, t_n$ je báza, je každý súčet tvaru $\Sigma c_i a_{i1}$ rovný nule, čo môžeme zapísať v maticovom tvare ako $(c_1, \ldots, c_n)A = (0, \ldots, 0)$, ale potom $(c_1, \ldots, c_n) = (c_1, \ldots, c_n)E = (c_1, \ldots, c_n)AB = (0, \ldots, 0)B = (0, \ldots, 0)$. Teda skutočne sú všetky koeficienty $c_1, \ldots, c_n$ nulové. Lema je tým dokázaná. □

Uveďme si jednu zaujímavú aplikáciu vety o SKT (a tým aj využitie príslušného algoritmu, v tomto prípade pre euklidovský okruh celých čísiel).

Chceme riešiť nasledovnú úlohu: Nech $H = [(2,4,1), (3,2,7), (1,2,4)] \subseteq Z^3$ — t.j. H je podgrupa grupy Z^3. Zistite, či napr. $(1,1,1) \in H$ (tzv. problém "náležania", membership-u).

Nech $A = \begin{pmatrix} 2 & 4 & 1 \\ 3 & 2 & 7 \\ 1 & 2 & 4 \end{pmatrix}$. Podľa vety o SKT existujú matice P a Q také, že

$$\begin{array}{ccccccc} & & P & \cdot & A & \cdot & Q & \\ v' & & & v & & t & & t' \end{array} = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$$

s vlastnosťou deliteľnosti $d_1 \mid d_2 \mid d_3$ pre výslednú maticu $\mathrm{diag}(d_1, d_2, \ldots)$.

"Indexy" v', v, t, t' predstavujú "bázy" s príslušnými "maticami" prechodu, pričom v zodpovedá "báze" (určite je presnejšie, keď povieme, že sa má jednať o množinu, generujúcu podgrupu H — ako podgrupu a nie ako vektorový priestor) $v_1 = (2,4,1)$, $v_2 = (3,2,7)$ a $v_3 = (1,2,4)$ a t zodpovedá "štandardnej" báze $(1,0,0), (0,1,0), (0,0,1)$ grupy Z^3.

Skúsme si teda predstaviť, že existuje lineárna kombinácia (s celočíselnými koeficientami c_1, c_2, c_3) $c_1 v_1 + c_2 v_2 + c_3 v_3 = (1,1,1)$ (t.j. $(1,1,1) \in H$, maticovo to znamená, že $(c_1, c_2, c_3)A = (1,1,1)$). Potom podľa lemy 1.2.15 existujú celočíselné a_1, a_2, a_3 také, že $(a_1, a_2, a_3)P = (c_1, c_2, c_3)$ a preto

$$(a_1, a_2, a_3)PAQ = (a_1, a_2, a_3) \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix} = (a_1 d_1, a_2 d_2, a_3 d_3)$$

Ale

$$(a_1, a_2, a_3)PAQ = (c_1, c_2, c_3)AQ = (1,1,1)Q = (a_1 d_1, a_2 d_2, a_3 d_3)$$

Z tohoto vyplýva, že $(1,1,1) \in H$ práve vtedy, keď $(1,1,1)Q$ je vektor, ktorý je na prvej súradnici násobok d_1, na druhej súradnici násobok d_2 a na tretej súradnici násobok d_3.

Konkrétne (Maple):

```
[> with(linalg);
...
[> A:=matrix([[2,4,1],[3,2,7],[1,2,4]]);
```

$$A := \begin{bmatrix} 2 & 4 & 1 \\ 3 & 2 & 7 \\ 1 & 2 & 4 \end{bmatrix}$$

```
[> ismith(A,P,Q);
```

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 28 \end{bmatrix}$$

```
[> eval(P);
```

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & -3 \\ 1 & -7 & 19 \end{bmatrix}$$

```
[> eval(Q);
```

$$\begin{bmatrix} 1 & 2 & 6 \\ 0 & 1 & 5 \\ 0 & -1 & -4 \end{bmatrix}$$

Teraz spočítajme $(1,1,1)Q$:

```
[> my_vector:=vector([1,1,1]);
[> multiply(my_vector,Q);
```

$$[1,2,7]$$

Keďže posledná súradnica výsledného vektora nie je násobkom čísla 28, znamená to, že $(1,1,1) \notin H$.

Môžeme ešte vyskúšať, či generujúce vektory $v_1 = (2,4,1)$, $v_2 = (3,2,7)$ a $v_3 = (1,2,4)$ patria (v zmysle uvedeného algoritmu) do H — to by malo fungovať:

```
[> v1:=vector([2,4,1]);
[> multiply(v1,Q);
```

$$[2,7,28]$$

```
[> v2:=vector([3,2,7]);
[> multiply(v2,Q);
```

$$[3,1,0]$$

a nakoniec

```
[> v3:=vector([1,2,4]);
[> multiply(v3,Q);
```

$$[1,0,0]$$

t.j. v zmysle vyjadrenia v bázach t a t' (t' sme vlastne ani nemuseli počítať) platí:

$$\begin{aligned} (2,4,1)_t &= (2,7,28)_{t'} \\ (3,2,7)_t &= (3,1,0)_{t'} \\ (2,4,1)_t &= (1,0,0)_{t'} \end{aligned}$$

Všetky súradnice v báze t' sú teda násobkami správnych čísiel a teda všetko je v poriadku.

1.2.2 Veta o rozklade modulov

Majme vektorový priestor (F, V) s nejakou bázou $e_1, \ldots, e_n$. Ďalej nech A je lineárne zobrazenie A: $V \to V$ s maticou $A = ||a_{ij}||_{n\times n}$. Uvažujme o voľnom module $F_{F[\gamma]}(t_1, \ldots, t_n)$ a o homomorfizme φ: $F_{F[\gamma]}(t_1, \ldots, t_n) \to (F[\gamma], V, A)$, ktorý definujeme ako (jednoznačné) rozšírenie zobrazenia f, ktoré zobrazuje: $t_i \to e_i$, t.j.

$$\varphi(f_1(\gamma)t_1 + \cdots + f_n(\gamma)t_n) = e_1 f_1(A) + \cdots + e_n f_n(A)$$

Toto zobrazenie je zrejme epimorfizmus a nás zaujíma podmodul $\mathrm{Ker}\,\varphi$, platí tvrdenie:

Lema 1.2.16 *Bázu voľného podmodulu* $\mathrm{Ker}\,\varphi$ *tvoria prvky* $v_1, \ldots, v_n$ *také, že*

$$\begin{aligned} v_1 &= (\gamma - a_{11})t_1 + (-a_{12})t_2 + \cdots + (-a_{1n})t_n \\ v_2 &= (-a_{21})t_1 + (\gamma - a_{22})t_2 + \cdots + (-a_{1n})t_n \\ &\vdots \qquad\quad \vdots \\ v_n &= (-a_{n1})t_1 + (a_{n2})t_2 + \cdots + (\gamma - a_{nn})t_n \end{aligned}$$

Dôkaz. Najprv si uvedomme, že $\varphi(v_i) = e_i A - (\sum_j a_{ij}e_j) = 0$ a teda skutočne $v_i \in \mathrm{Ker}\,\varphi$. Teraz si ukážme, že vektory $v_1, \ldots, v_n$ skutočne generujú $\mathrm{Ker}\,\varphi$. Začnime s jedným špeciálnym poznatkom:

$$\gamma t_i = v_i + \sum_j a_{ij}t_j$$

Potom existujú $f_1, \ldots, f_n \in F[x]$ a $b_1, \ldots, b_n \in F$ také, že

$$\gamma^2 t_i = \gamma(v_i + \sum_j a_{ij}t_j) = f_1(\gamma)v_1 + \cdots + f_n(\gamma)v_n + b_1t_1 + \cdots + b_nt_n$$

Teraz síce vieme napr. vyčísliť, že pre $k \neq i$ platí $f_k(\gamma) = a_{ik}$ a $f_i(\gamma) = \gamma + a_{ii}$, prípadne vieme napísať podobné explicitné vzorce aj pre $b_1, \ldots, b_n$. To však nie je podstatné. Dôležité je, že vieme (indukciou) tento výsledok zovšeobecniť na tvrdenie: Pre $j \geq 1$ existujú $f_1, \ldots, f_n \in F[x]$ a $b_1, \ldots, b_n \in F$ také, že

$$\gamma^j t_i = f_1(\gamma)v_1 + \cdots + f_n(\gamma)v_n + b_1t_1 + \cdots + b_nt_n$$

a dokonca že pre $g \in F[x]$ a každé prípustné i existujú $f_1, \ldots, f_n \in F[x]$ a $b_1, \ldots, b_n \in F$ také, že

$$g(\gamma)t_i = f_1(\gamma)v_1 + \cdots + f_n(\gamma)v_n + b_1t_1 + \cdots + b_nt_n.$$

Nech teraz $g_1(\gamma)t_1 + \cdots + g_n(\gamma)t_n \in \mathrm{Ker}\,\varphi$. Potom existujú $f_1, \ldots, f_n \in F[x]$ a $b_1, \ldots, b_n \in F$ také, že

$$g_1(\gamma)t_1 + \cdots + g_n(\gamma)t_n = f_1(\gamma)v_1 + \cdots + f_n(\gamma)v_n + b_1t_1 + \cdots + b_nt_n$$

a preto

$$\varphi(g_1(\gamma)t_1 + \cdots + g_n(\gamma)t_n) = \varphi(f_1(\gamma)v_1 + \cdots + f_n(\gamma)v_n + b_1t_1 + \cdots + b_nt_n) = b_1e_1 + \cdots + b_ne_n = 0$$

a teda (vďaka tomu, že $e_1, \ldots, e_n$ je báza vektorového priestoru), musí byť $b_1 = b_2 = \cdots = b_n = 0$. To ale znamená, že

$$g_1(\gamma)t_1 + \cdots + g_n(\gamma)t_n = f_1(\gamma)v_1 + \cdots + f_n(\gamma)v_n,$$

čiže skutočne $g_1(\gamma)t_1 + \cdots + g_n(\gamma)t_n \in [v_1, \ldots, v_n]$.

Posledná časť dôkazu sa bude zaoberať dôkazom nezávislosti vektorov $v_1, \ldots, v_n$. Podľa definície $v_1, \ldots, v_n$ vidíme, že pre $g_1, \ldots, g_n \in F[x]$ platí

$$g_1(\gamma)v_1 + \cdots + g_n(\gamma)v_n = (\gamma g_1(\gamma) - \sum_j a_{j1}g_j(\gamma))t_1 + \cdots + (\gamma g_n(\gamma) - \sum_j a_{jn}g_j(\gamma))t_n.$$

Nech teraz $g_1(\gamma)v_1 + \cdots + g_n(\gamma)v_n = 0$ a nech g_i je polynóm maximálneho stupňa spomedzi $g_1, \ldots, g_n$. Potom keďže $t_1, \ldots, t_n$ je báza modulu $F_{F[x]}(t_1, \ldots, t_n)$, musí byť špeciálne i-ty koeficient v predošlej rovnosti rovný nule a teda

$$\gamma g_i(\gamma) = \sum_j a_{ji}g_j(\gamma)$$

Keďže ale formálne má polynóm na ľavej strane tejto rovnosti stupeň o 1 väčší ako polynóm na pravej strane, je táto rovnosť splnená len vtedy, keď má polynóm g_i a teda aj všetky ostatné stupeň $-\infty$, t.j. všetky polynómy $g_1, \ldots, g_n$ sú nulové. Preto sú vektory $v_1, \ldots, v_n$ lineárne nezávislé. □

Definícia 1.2.17 *Nech (R, M) je modul, R je okruh hlavných ideálov. Ak $a \in M$, tak generátor (hlavného) ideálu $\{r \in R;\, ra = 0\}$ sa nazýva rád prvku a.*

Rád prvku a označujeme $\mathrm{rad}(a)$*, je určený jednoznačne až na asociovanosť. Ak je (R, M) unitárny, je* $\mathrm{rad}(a) \doteq 1 \Leftrightarrow a = 0$.

Lema 1.2.18 *Nech (R, M) je modul, nech R je OHI. Potom $M_1 = \{x \in M;\, \mathrm{rad}(x) \neq 0\}$ je podmodul modulu M.*

Poznámka: Modul M_1 nazývame podmodul prvkov konečného rádu modulu M.

Dôkaz. Zrejme 0 je prvok konečného rádu, takže $M_1 \neq \emptyset$.

Nech $a, b \in M_1$. Potom $\mathrm{rad}(a)\mathrm{rad}(b)(a+b) = \mathrm{rad}(b)\mathrm{rad}(a)a + \mathrm{rad}(a)\mathrm{rad}(b)b = 0 + 0 = 0$, a, samozrejme, $\mathrm{rad}(a)\mathrm{rad}(b) \neq 0$, lebo R je obor integrity.

Podobne, ak $v \in R$, $a \in M_1$, potom $\mathrm{rad}(a)(va) = v \cdot \mathrm{rad}(a)a = v \cdot 0 = 0$.

Teda M_1 je podmodul M. □

Lema 1.2.19 *Nech (R, M) je unitárny modul, R je OHI. Nech*

$$M = [e_1] \oplus \cdots \oplus [e_k] \oplus \cdots \oplus [e_n],$$

pričom $e_1, \ldots, e_k$ sú konečného rádu a $e_{k+1}, \ldots, e_n$ majú rád 0. Potom

$$M_1 = [e_1] \oplus \cdots \oplus [e_k]$$

(tu držíme označenie z predošlej lemy, t.j. M_1 je podmodul prvkov konečného rádu)

Dôkaz. Nech $y = a_1e_1 + \cdots + a_ne_n \in M$ je prvok konečného rádu. Potom

$$\mathrm{rad}(y)y = \mathrm{rad}(y)a_1e_1 + \cdots + \mathrm{rad}(y)a_ke_k + \cdots + \mathrm{rad}(y)a_ne_n = 0$$

a vzhľadom na to, že M je priamy súčet, dostávame vďaka príslušnej leme a vďaka tomu, že $\mathrm{rad}(e_{k+1}) = \cdots = \mathrm{rad}(e_n) = 0$, že $\mathrm{rad}(y)a_{k+1} = \cdots = \mathrm{rad}(y)a_n = 0$. Ale keďže $\mathrm{rad}(y) \neq 0$ a R je obor integrity, musí byť $a_{k+1} = \cdots = a_n = 0$, t.j.

$$y = a_1e_1 + \cdots + a_ke_k \in [e_1] \oplus \cdots \oplus [e_k]$$

Teda $M_1 \subseteq [e_1] \oplus \cdots \oplus [e_k]$. Opačná inklúzia je zrejmá. □

Nakoniec ešte uveďme jedno tvrdenie, ktoré bude užitočné pri dôkaze nasledujúcej vety.

Lema 1.2.20 *Nech $(R, [e])$ a $(R, [f])$ sú dva unitárne moduly, R je OHI. Potom $[e] \cong [f]$ práve vtedy keď* $\mathrm{rad}(e) \doteq \mathrm{rad}(f)$.

Dôkaz. Nech φ: $R \to [e]$ je homomorfizmus, ktorý je (jednoznačným) rozšírením zobrazenia, ktoré zobrazí $1 \in R$ na e, t.j. $\varphi(1) = e$. Potom

$$\mathrm{Ker}\,\varphi = \{r \in R;\, \varphi(r \cdot 1) = re = 0\} = (\mathrm{rad}(e)).$$

Zobrazenie φ je vďaka unitárnosti surjektívne a preto

$$R/(\mathrm{rad}(e)) \cong [e]$$

Teraz je už zrejmé, že izomorfizmus medzi modulmi $[e]$ a $[f]$ súvisí s asociovanosťou prvkov $\mathrm{rad}(e)$ a $\mathrm{rad}(f)$, ako je to uvedené v tvrdení vety.

Ešte iný argument: nech $\varphi : [e] \to [f]$ je izomorfizmus. Potom vďaka surjektívnosti φ a cykličnosti modulu $[e]$ existuje $a \in R$ také, že $\varphi(ae) = f$. Potom ale

$$\mathrm{rad}(e)f = \mathrm{rad}(e)\varphi(ae) = \varphi(\mathrm{rad}(e)ae) = \varphi(0) = 0.$$

Preto $\mathrm{rad}(f) | \mathrm{rad}(e)$. Podobne vieme dokázať, že $\mathrm{rad}(f) | \mathrm{rad}(e)$, t.j. $\mathrm{rad}(e) \doteq \mathrm{rad}(f)$. □

Veta 1.2.21 *Nech (R, M) je konečne generovaný unitárny modul nad okruhom hlavných ideálov R. Potom existuje rozklad na cyklické podmoduly*

$$M = [f_1] \oplus [f_2] \oplus \cdots \oplus [f_k]\,,$$

kde $\mathrm{rad}(f_i) \,|\, \mathrm{rad}(f_j)$ pre $1 \leq i \leq j \leq k$. Ďalej, ak $\mathrm{rad}(f_1) \not\doteq 1$, tak tento rozklad je jednoznačný, presnejšie povedané, ak $M = [f_1'] \oplus [f_2'] \oplus \cdots \oplus [f_s']$ a je splnené, že $\mathrm{rad}(f_1') \not\doteq 1$ a tiež $\mathrm{rad}(f_i') \,|\, \mathrm{rad}(f_j')$ pre $1 \leq i \leq j \leq s$, tak $k = s$ a $\mathrm{rad}(f_i) \doteq \mathrm{rad}(f_i')$.

Dôkaz. Existencia. Nech $e_1,\dots,e_n$ sú generátory modulu M. Uvažujme o voľnom module $F_R(t_1,\dots,t_n)$. Majme epimorfizmus $\varphi: F_R(t_1,\dots,t_n)\to M$ s vlastnosťou $\varphi(t_i)=e_i$ pre všetky $i=1,\dots,n$. Všimnime si bližšie $\operatorname{Ker}\varphi$. Ak $\operatorname{Ker}\varphi=\{0\}$, tak φ je bijekcia a teda M je tiež voľný modul a preto $M=[e_1]\oplus\cdots\oplus[e_n]$ je hľadaný rozklad.

Nech je $\operatorname{Ker}\varphi\neq\{0\}$. $\operatorname{Ker}\varphi$ je tiež voľný podmodul a má bázu $v_1,\dots,v_m$, $m\le n$. Potom pre $i=1,\dots,m$ existujú koeficienty a_{ij} také, že $v_i=a_{i1}t_1+\cdots+a_{in}t_n$. Týmto je určená matica $A=||a_{ij}||_{m\times n}$. Podľa Smithovej vety existujú matice P a Q ktoré sú deliteľmi jednotky v príslušnom okruhu matíc nad R (P typu $m\times m$ a Q typu $n\times n$) tak, že $D=PAQ$, kde D je diagonálna matica $D=\operatorname{diag}(d_1,d_2,\dots)$ s vlastnosťou $d_i\mid d_j$ pre $1\le i\le j\le m$. Matica P je maticou prechodu ku novej báze $v'_1,\dots,v'_m$ a matica Q^{-1} je maticou prechodu ku novej báze $t'_1,\dots,t'_n$ — v prvom prípade v podmodule $\operatorname{Ker}\varphi$, v druhom v module $F_R(t_1,\dots,t_n)$.

Nový bázový vektor v'_i má v báze $v'_1,\dots,v'_m$ súradnice ϵ_i, v starej báze $v_1,\dots,v_m$ má súradnice ϵ_iP, potom v báze $t_1,\dots,t_n$ má súradnice ϵ_iPA a nakoniec v báze $t'_1,\dots,t'_n$ má súradnice $\epsilon_iPAQ=\epsilon_iD$. Preto

$$v'_1=d_1t'_1,\ v'_2=d_2t'_2,\ \dots,v'_m=d_mt'_m\quad\text{pre } d_i\neq0.$$

Označme $B=||b_{ij}||=Q^{-1}$. Pre $i=1,\dots,n$ položme $e'_i=\varphi(t'_i)=b_{i1}e_1+\cdots+b_{in}e_n$. Dokážeme, že toto sú hľadané prvky, t.j. že $M=[e'_1]\oplus\cdots\oplus[e'_n]$ s potrebnými vlastnosťami o rádoch. Vďaka definícii matice B pre každé $i=1,\dots,n$ platí $e_i=q_{i1}e'_1+\cdots+q_{in}e'_n$. Odtiaľto vyplýva, že $[[e'_1]\cup\ldots\cup[e'_n]]=M$. Ešte potrebujeme dokázať "nezávislosť", t.j., že

$$[[e'_1]\cup\ldots\cup[e'_{j-1}]]\cap[e'_j]=\{0\}.$$

Na to ale stačí dokázť, že ak $c_1e'_1+\cdots+c_ne'_n=0$, tak $c_ie'_i=0$ pre všetky $i=1,\dots n$. Ale $F_R(t_1,\dots,t_n)=F_R(t'_1,\dots,t'_n)$ a už vieme, že $\varphi(t'_i)=e'_i$. Preto ak $c_1e'_1+\cdots+c_ne'_n=0$, tak $c_1t'_1+\cdots+c_nt'_n\in\operatorname{Ker}\varphi$. Čiže

$$c_1t'_1+\cdots+c_nt'_n=s_1v'_1+\cdots+s_mv'_m=s_1d_1t'_1+\cdots+s_md_mt'_m.$$

Pretože $t'_1,\dots,t'_n$ je bázou voľného modulu, dostávame

$$c_1=s_1d_1,\ \dots,c_m=s_md_m,\ c_{m+1}=\cdots=c_n=0.$$

Pretože $v'_i=d_it'_i$, tak $\varphi(v'_i)=0=d_ie'_i$ pre $i=1,\dots,m$. Odtiaľ vidíme, že pre každé $i=1,\dots,n$ platí $c_ie'_i=0$, čo sme chceli dosiahnuť.

Teda M sa dá rozložiť, ešte skontrolujme časť o rádoch. Ako sme práve videli, je $d_ie'_i=0$ a teda $\operatorname{rad}(e'_i)\mid d_i$. Na druhej strane $c_ie'_i=0$ znamená, že $c_it'_i\in\operatorname{Ker}\varphi$ a preto — ako je vidieť z predošlého postupu — je $c_it'_i=s_id_it'_i$, čiže $d_i\mid c_i$. Preto $\operatorname{rad}(e'_i)=d_i$ a prvky $d_1,\dots,d_m$ majú požadovanú vlastnosť vďaka tvrdeniu Smithovej vety.

Jednoznačnosť. Ak (R,M) je voľný modul, tak vieme, že jednoznačnosť platí (1.2.12). Nech teda M obsahuje aspoň jeden prvok konečného rádu. Nech M_1 je podmodul modulu M prvkov konečného rádu. Majme teda dva rozklady $M=[e_1]\oplus\cdots\oplus[e_k]=[e'_1]\oplus\cdots\oplus[e'_{k'}]$, pričom $\operatorname{rad}(e_i)\not|1$, $\operatorname{rad}(e'_i)\not|1$, $\operatorname{rad}(e_i)\mid\operatorname{rad}(e_j)$ a $\operatorname{rad}(e'_i)\mid\operatorname{rad}(e'_j)$ pre všetky prípustné indexy $i\le j$. Podľa lemy 1.2.19 existujú r, r' také, že $M_1=[e_1]\oplus\cdots\oplus[e_r]=[e'_1]\oplus\cdots\oplus[e'_{r'}]$. Faktormodul M/M_1 je voľný a platí

$$M/M_1=[e_{r+1}]\oplus\cdots\oplus[e_k]=[e'_{r'+1}]\oplus\cdots\oplus[e'_{k'}].$$

Podľa vety 1.2.12 je $k-r=k'-r'$. Ešte dokážeme jednoznačnosť pre M_1. Celý dôkaz je urobený indukciou podľa počtu ireducibilných prvkov v rozklade najmenšieho možného súčinu $d_1d_2\dots d_k$, pričom existuje rozklad $M_1=[e_1]\oplus\cdots\oplus[e_k]$, $d_i=\operatorname{rad}(e_i)$, $d_i\not|1$ a pre $i\le j$ je $d_i\mid d_j$. (Samozrejme, predpokladáme, že M_1 obsahuje len prvky konečného rádu.) Najprv si urobíme analýzu problému, z ktorej bude jasné, ako urobiť indukciu.

Nech $p\in R$ je ireducibilný prvok a nech $py=0$ pre nejaké $y\in M_1$. Položme $M_2=\{y\in M_1;\,py=0\}$. M_2 je podmodul M_1 (preverte!). Nech $y\in M_2$. Potom $y=c_1e_1+\cdots+c_re_r$. Ďalej $py=c_1pe_1+\cdots+c_rpe_r=0$. Preto $c_ipe_i=0$, z čoho $d_i\mid c_ip$, kde $d_i=\operatorname{rad}(e_i)$. Máme dve možnosti: buď $(d_i,p)\doteq p$, alebo $(d_i,p)\doteq1$. Inak povedané, $p\mid d_i$, alebo $d_i\mid c_i$. Ale ak $p\mid d_i$, potom $p\mid d_j$ pre všetky $j\ge i$. Nech teda $m-1$ je najväčší index taký, že $p\not|\,d_{m-1}$. Pre $i=1,\dots,m-1$ teda $d_i\mid c_i$ a preto zo zápisu prvku y môžeme vynechať prvých $m-1$ členov, t.j. $y=c_me_m+\cdots+c_re_r$ (a toto tvrdenie nezávisí od prvku $y\in M_2$, ale len od toho, kedy už "p začne deliť prvky d_i"). Pre $i=m,\dots,r$ je $p\mid d_i$ a $d_ip^{-1}\mid c_i$ (d_ip^{-1} je formálny zápis toho, že v rozklade d_i na ireducibilné prvky vynecháme jedno p — tiež budeme písať d_i/p (ak je $d_i=p$, tak kladieme $d_i/p=1$)).

Vidíme teda, že $M_2=[(d_m/p)e_m]\oplus\cdots\oplus[(d_r/p)e_r]$. Rovnakou úvahou pre druhý rozklad dostaneme, že $M_2=[(d'_{m'}/p)e'_{m'}]\oplus\cdots\oplus[(d'_{r'}/p)e'_{r'}]$ pre vhodné m'.

Teraz trochu odbočíme. $R/(p)$ je pole, lebo (p) je maximálny ideál (v OHI sú netriviálne prvoideály a max. ideály to isté!). Na modul (R,M_2) sa dá pozerať ako na modul nad $R/(p)$: nech $\overline{a}=a+(p)$ je prvok $R/(p)$. Pre $x\in M_2$ položme $\overline{a}x=ax$ — vďaka tomu, že $px=0$ je toto skalárne násobenie dobre definované. Keďže $R/(p)$ je pole, je $(R/(p),M_2)$ vektorový priestor. Rozklady $M_2=[(d_m/p)e_m]\oplus\cdots\oplus[(d_r/p)e_r]$ a $M_2=[(d'_{m'}/p)e'_{m'}]\oplus\cdots\oplus[(d'_{r'}/p)e'_{r'}]$ sú teda rozkladmi $(R/(p),M_2)$ na direktný súčet jednorozmerných vektorových priestorov, inými slovami čísla $r-m$

a $r' - m'$ sú obe dimenziou vektorového priestoru $(R/(p), M_2)$. Preto $r - m = r' - m'$. Zvoľme teraz ireducibilný prvok p tak, aby $p \mid d_1$. Potom $m = 1$. Keďže je $m' \geq 1$, dostávame, že $r' \geq r$. Ak zvolíme ireducibilný p tak, aby $p \mid d'_1$, dostaneme, že $m' = 1$ a keďže v tomto prípade je $m \geq 1$, je $r \geq r'$. Nakoniec teda $r = r'$ a naviac $p \mid d_1$ práve vtedy, keď $p \mid d'_1$. Teda počet priamych sčítancov v rozklade M_1 a teda aj M je rovnaký a získali sme ešte jednu užitočnú informáciu naviac.

Ešte ostáva ukázať, že $d_i \doteq d'_i$ pre $i = 1, \ldots, r$. Nech $pM_1 = \{y;\ (\exists x \in M_1)\, y = px\}$. pM_1 je podmodul modulu M_1. Ak $p \mid d_1$ je ireducibilný, tak

$$pM_1 = [pe_1] \oplus \cdots \oplus [pe_r] = [pe'_1] \oplus \cdots \oplus [pe'_r]$$

(urobte podrobnejšie). Na tomto mieste môžeme použiť indukčný predpoklad, totiž počet ireducibilných prvkov v rozklade prvku $(d_1/p)(d_2/p)\ldots(d_r/p)$ o r menší ako v rozklade prvku $d_1 d_2 \ldots d_r$. Podľa indukčného predpokladu teda $\operatorname{rad}(pe_i) \doteq \operatorname{rad}(pe'_i)$, odkiaľ už $\operatorname{rad}(e_i) \doteq \operatorname{rad}(e'_i)$. □

Poznámka. Čísla $d_1, \ldots, d_r$ sa nazývajú *torzné koeficienty* modulu (R, M).

Dôsledok 1.2.22 *Nech (R, M) je konečne generovaný unitárny modul nad okruhom hlavných ideálov. Potom $M = M_1 \oplus F$, kde M_1 je podmodul prvkov konečného rádu a F je voľný modul nad R.*

Poznámka. Dimenzia podmodulu (voľného sčítanca) F je určená jednoznačne (podmodul F nie je určený jednoznačne!) a nazýva sa *Bettiho číslom* modulu (R, M).

Dôsledok 1.2.23 *Konečne generovaná komutatívna grupa je priamym súčinom komutatívnej periodickej grupy a voľnej komutatívnej grupy.*

Dôsledok 1.2.24 *Konečne generovaná komutatívna grupa je priamym súčinom cyklických grúp.*

Cvičenie 28 *Dokážte všetky tvrdenia uvedené bez dôkazu v dôkaze vety 1.2.21 a všetky dôsledky.*

Cvičenie 29 *V nasledujúcich cvičeniach tohoto článku predpokladáme, že (R, M) je unitárny modul nad OHI. Bez použitia vety 1.2.21 dokážte: $[e] \cong [f]$ práve vtedy, keď $\operatorname{rad}(e) \doteq \operatorname{rad}(f)$.*

Cvičenie 30 *Majme $e_1, \ldots, e_k \in M$. Nech $\operatorname{rad}(e_1), \ldots, \operatorname{rad}(e_k)$ sú po dvoch nesúdeliteľné. Potom $[e_1] \oplus \cdots \oplus [e_k] = [f]$ pre vhodné $f \in M$.*

Cvičenie 31 *Predošlé cvičenie nemusí platiť bez predpokladu na nesúdeliteľnosť. Nájdite protipríklad.*

Cvičenie 32 *Homomorfný obraz cyklického modulu je cyklický modul.*

Cvičenie 33 *Nech $R = F[\gamma]$ alebo $R = Z$. Potom podmodul cyklického modulu je cyklický modul.*

Cvičenie 34 *Sformulujte vetu 1.2.21 pre komutatívne grupy. Sú cyklické grupy z rozkladu v tejto vete už nerozložiteľné?*

1.3 Podobnosť matíc, Jordanov kanonický tvar

Podľa definície sú dve štvorcové matice A, B typu $n \times n$ s prvkami z poľa F podobné, ak existuje regulárna matica P taká, že $B = PAP^{-1}$, alebo ekvivalentne, ak sú matice A, B maticami toho istého lineárneho zobrazenia daného vektorového priestoru pri (možno) rôznych bázach.

Potrebujeme dať odpoveď na dve otázky:

1. Kedy sú matice A, B podobné
2. Ako vyzerá "najjednoduchšia" matica podobná danej matici A

Samozrejme, za "najjednoduchšiu" maticu považujeme maticu blízku k diagonálnej, ktorá by mala pekné vlastnosti vzhľadom na nejaké ďalšie operácie.

Nech $A = ||a_{ij}||_{n\times n}$ je matica nad F. Táto matica je maticou lineárneho zobrazenia (budeme ho tiež označovať A) A: $V_n(F) \to V_n(F)$ — zobrazenie uvažujeme pri štandardnej ϵ-ovej báze. Uvažujme teraz o unitárnom module $M = (F[\gamma], V_n(F), A)$. Keďže prvky $\epsilon_1, \ldots, \epsilon_n$ generujú tento modul, je M konečne generovaný modul nad OHI $F[\gamma]$. Podľa vety o rozklade teda existujú prvky $g_1, \ldots, g_k$ také, že

$$M = [g_1] \oplus \cdots \oplus [g_k],$$

pričom $\mathrm{rad}(g_i)|\mathrm{rad}(g_{i+1})$

Uvažujeme teraz o $M_i = [g_i]$. Platí nasledujúce jednoduché tvrdenie:

Lema 1.3.1 *Každý cyklický podmodul M_i je podpriestor vektorového priestoru $V_n(F)$. Naviac tento podpriestor je invariantný vzhľadom na lin. zobrazenie A, t.j.*

$$(\forall \alpha \in M_i)\, \alpha A \in M_i$$

Dôkaz. Ukážeme len invariantnosť: nech $\alpha \in M_i$, teda existuje $f(\gamma) \in F[g]$ také, že $\alpha = f(\gamma)g_i$. Potom

$$\alpha A = (f(\gamma)g_i)A = (g_i f(A))A = g_i(f(A)A) = \gamma f(\gamma)g_i \in M_i.$$

□

Podľa tejto vety je teda vyššie uvedený rozklad modulu M na cyklické podmoduly zároveň direktným rozkladom vektorového priestoru $V_n(F)(= M)$. Ak teraz vyberieme bázu $V_n(F)$ pozostávajúcu z báz podpriestorov M_i, matica lin. zobrazenia A pri takejto báze bude blokovo diagonálna, rozmer každého bloku bude zodpovedať dimenzii príslušného podpriestoru M_i.

Pripomeňme si, ako nájdeme vektory g_i a ich rády, s ktorými ešte budeme pracovať. Postupujeme podľa vety o rozklade modulov. Vo $V_n(F)$ budeme pracovať s bázou $\epsilon_1, \ldots, \epsilon_n$, kde $\epsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, pričom 1 sa nachádza na i-tom mieste. Začneme pracovať s homomorfizmom

$$\varphi : F_{F[\gamma]}(t_1, \ldots, t_n) \to V_n(F),$$

ktorý je rozšírením zobrazenia f: $\{t_1, \ldots, t_n\} \to V_n(F)$ fungujúceho tak, že $f(t_i) = \epsilon_i$ pre všetky prípustné i. Báza jadra tohoto zobrazenia je podľa príslušnej vety množina vektorov

$$\begin{aligned} v_1 &= (\gamma - a_{11})t_1 - a_{12}t_2 - \ldots - a_{1n}t_n \\ &\vdots \\ v_n &= -a_{n1}t_1 - \ldots - a_{nn-1}t_{n-1} + (\gamma - a_{n1})t_n \end{aligned}$$

a matica vektorov tejto bázy vyjadrených v báze $t_1, \ldots, t_n$ teda je $\gamma I - A$. Nájdeme Smithov kanonický tvar tejto matice, t.j. diagonálnu maticu $D = \mathrm{diag}(d_1, d_2, \ldots)$ takú, že $D = P(\gamma I - A)Q$ pre vhodné delitele jednotiek P, Q v príslušných okruhoch matíc s vlastnosťou deliteľnosti $d_1 \,|\, d_2 \,|\, \cdots$. Pripomeňme si, že prvky d_i sú polynómy.

Položíme $B = Q^{-1} = ||b_{ij}||$. Aj tu sú prvky b_{ij} polynómy. Potom

$$g_i' = b_{i1}\epsilon_1 + \ldots + b_{in}\epsilon_n = \epsilon_1 b_{i1}(A) + \ldots + \epsilon_n b_{in}(A)$$

Vzhľadom na to, že niekoľko prvých vektorov, ktoré takto získame sú nulové vektory, tieto jednoducho vynecháme a začneme počítať až od prvého nenulového - tak získame $g_1, \ldots, g_k$. Rády týchto prvkov budú príslušné (po „posunutí" indexov) $d_i = d_i(\gamma)$.

Definícia 1.3.2 *1. Minimálny polynóm $m_{A,\alpha}(\gamma)$ transformácie (matice) A v bode α je normovaný polynóm, ktorý generuje ideál*

$$M_{A,\alpha} = \{f \in F[\gamma];\ \alpha f(A) = \mathbf{0}\}$$

2. Minimálny polynóm $m_{A,S}(\gamma)$ transformácie (matice) A na podpriestore $S \subseteq V_n(F)$ je normovaný polynóm, ktorý generuje ideál

$$M_{A,S} = \{f \in F[\gamma];\ (\forall \alpha \in S)\ \alpha f(A) = \mathbf{0}\} = \bigcap_{\alpha \in S} M_{A,\alpha}$$

3. Minimálny polynóm $m_A(\gamma)$ transformácie (matice) A (na priestore $V_n(F)$) je normovaný polynóm, ktorý generuje ideál

$$M_{A,V_n} = \{f \in F[\gamma];\ (\forall \alpha \in V_n)\ \alpha f(A) = \mathbf{0}\} = \bigcap_{\alpha \in V_n} M_{A,\alpha}$$

Z tejto definície hneď vyplýva, že ak $\alpha \in S \subseteq V_n$, tak

$$m_{A,\alpha}(\gamma) \,|\, m_{A,S}(\gamma) \,|\, m_{A,V_n}(\gamma)$$

Keď porovnáme túto definíciu minimálneho polynómu transformácie A v bode α s definíciou rádu prvku α v module $(F[\gamma], V_n, A)$, vidíme, že sa jedná (až na požiadavku normovanosti) o tú istú definíciu.

Teda $m_{A,\alpha}(\gamma) \doteq \mathrm{rad}(\alpha)$. Potom ak $\alpha \neq \mathbf{0}$, je $1 \cdot \alpha \neq \mathbf{0}$ a teda $m_{A,\alpha}(\gamma) \neq 1$.

Keďže sú vektory $\alpha, \alpha A, \alpha A^2, \ldots, \alpha A^n$ lineárne závislé vektory vektorového priestoru V_n, príslušné koeficienty nám umožnia získať netriviálny (t.j. nenulový) polynóm, ktorým keď vynásobíme vektor α (ako v module $(F[\gamma], V_n, A)$) dostaneme nulu a teda $m_{A,\alpha}(\gamma) \neq 0$.

T.j. rád každého nenulového prvku v module $(F[\gamma], V_n, A)$ je rôzny od nuly a nie je asociovaný s jednotkou.

Popíšme si "rozumnú" bázu priestoru $M_i = [g_i]$. Uvažujme o množine vektorov

$$g_i, g_i A, g_i A^2, \ldots, g_i^{st(d_i)-1}$$

Ľahko sa dá presvedčiť, že je to naozaj báza a je vidieť, že transformácia A zúžená na podpriestor M_i má pri tejto báze maticu ($d_i = \mathrm{rad}(g_i) \doteq m_{A,g_i}(x) = x^m + a_{m-1} + \cdots + a_1 x + a_0$)

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & & \cdots & -a_{m-1} \end{pmatrix}$$

Túto maticu nazveme pridruženou maticou k polynómu $x^m + a_{m-1} + \cdots + a_1 x + a_0$. Toto znamená, že matica A je podobná blokovo diagonálnej matici $C = \mathrm{diag}(C_1, \ldots, C_k)$, kde C_i sú matice pridružené ku polynómom $d_i(\gamma)$. Maticu C nazývame *Jordanovým kanonickým tvarom matice A prvého druhu*. Vieme ju nájsť vždy a nad každým poľom, máme na to algoritmus.

Avšak pridružené matice ku polynómu nie sú diagonálne, skúsme preto pokračovať. Nasledujúci postup už nemusí vždy ísť (algoritmicky). Uvažujme o ďalšom rozklade matice C_i.

Nech teraz (bez újmy na všeobecnosti) $M = (F[\gamma], V(F), A) = [g]$ a nech $\mathrm{rad}(g) = m_1(\gamma) m_2(\gamma) \ldots m_l(\gamma)$, pričom m_i, m_j sú nesúdeliteľné polynómy (pre prípustné $i \neq j$). Položme $\hat{m}_i(\gamma) = \frac{\mathrm{rad}(g)}{m_i(\gamma)}$. Platí

Veta 1.3.3 *Existujú $e_1, \ldots, e_l$ také, že*

$$M = [g] = [e_1] \oplus [e_2] \oplus \cdots \oplus [e_l]$$

a $\mathrm{rad}(e_i) = m_i(\gamma)$.

Dôkaz. Položme $e_i = \hat{m}_i(\gamma) g = g \hat{m}_i(A)$.

1. Najprv dokážeme, že $M = [e_1, \ldots, e_l]$: Polynómy $\hat{m}_1(\gamma), \hat{m}_2(\gamma), \ldots, \hat{m}_l(\gamma)$ sú ako systém polynómov nesúdeliteľné (preverte!) a preto existujú polynómy $u_1, \ldots, u_l$ také, že $1 = u_1 \hat{m}_{11} + \cdots + u_l \hat{m}_{1l}$. Platí

$$\begin{aligned} g &= 1\dot{g} = (u_1 \hat{m}_1 + \cdots + u_l \hat{m}_l) g = g(u_1 \hat{m}_1(A) + \cdots + u_l \hat{m}_l(A)) \\ &= u_1 g \hat{m}_1(A) + \cdots + u_l g \hat{m}_l(A) = u_1 e_1 + \cdots + u_l e_l \end{aligned}$$

Samozrejme, keď vieme pomocou $e_1, \dots, e_l$ vygenerovať generátor g modulu M, vieme vygenerovať celý modul M.

Teraz overíme, že uvedený súčet modulov je direktný. Nech $u_1e_1 + \cdots + u_le_l = 0$. Dokážeme, že pre všetky prípustné i je $u_ie_i = 0$.

Pôvodnú podmienku prepíšme do tvaru

$$0 = u_1e_1 + \cdots + u_le_l = u_1g\hat{m}_1(A) + \cdots + u_lg\hat{m}_l(A) = (u_1\hat{m}_1 + \cdots + u_l\hat{m}_l)g$$

Toto znamená, že $\mathrm{rad}(g)|u_1\hat{m}_1 + \cdots + u_l\hat{m}_l$. Zoberme si polynóm $m_i(\gamma)$. Tento polynóm delí aj $\mathrm{rad}(g)$ aj všetky polynómy $\hat{m_j}$ pre $j \neq i$. Z predošlej deliteľnosti teda vyplýva, že $m_i|u_i\hat{m}_i$, ale keďže m_i a $\hat{m}_i$ sú nesúdeliteľné, musí m_i deliť u_i. Zvoľme teraz i, nech $u_i = m_iq$. Potom $u_ie_i = m_iq\hat{m}_ig = q\mathrm{rad}(g)g = q0 = 0$.

Nakoniec potrebujeme dokázať, že $\mathrm{rad}(e_i) = m_i$. Keďže $0e_1 + \cdots + 0e_{i-1} + \mathrm{rad}(e_i)e_i + 0e_{I+1} + \cdots + 0e_l = \mathrm{rad}(e_i)e_i = 0$, z predošlej úvahy plynie, že $m_i|\mathrm{rad}(e_i)$. Naopak, $\mathrm{rad}(e_i)$ delí každý polynóm $g(\gamma)$, ktorý má vlastnosť $g(\gamma)e_i = 0$. Ale $m_ie_i = m_i\hat{m}_ig = \mathrm{rad}(g)g = 0$. Čiže $\mathrm{rad}(e_i) = m_i$. Veta je dokázaná. □

Táto veta umožňuje rozložiť jednotlivé bloky Jordanovej kanonickej matice prvého druhu nasledovným spôsobom: Blok C_i je pridružený ku polynómu (invariantnému faktoru matice A), ktorý napíšeme v tvare

$$d_i(\gamma) = p_{i1}^{k_{i1}}(\gamma) \cdots p_{is_i}^{k_{is_i}}(\gamma)$$

kde $p_{i1}, p_{i2}, \dots, p_{is_i}$ sú po dvoch nesúdeliteľné ireducibilné normované polynómy. Potom na základe predošlej vety (a tiež predchádzajúcich úvah) vieme ešte blok C_i rozložiť na blokovo diagonálnu maticu $\mathrm{diag}(B_{i1}, \dots, B_{is_i})$, kde každé B_{ij} je matica pridružená ku polynómu $p_{ij}^{k_{ij}}(\gamma)$.

Polynómy $p_{ij}^{k_{ij}}(\gamma)$, $i = 1, \dots, l; j = 1, \dots, s_i$ sa nazývajú *elementárne delitele matice* A. Na nájdenie elementárnych deliteľov už vo všeobecnosti nemáme algoritmus (záleží to od poľa, nad ktorým pracujeme).

Teda matica A je pri vhodnej báze podobná s blokovo diagonálnou maticou pozostávajúcou z blokov pridružených ku jednotlivým elementárnym deliteľom.

Pokúsme sa ešte vylepšiť posledný tvar. Uvažujme teraz o module $M = (F[\gamma], [g], A)$, pričom $\mathrm{rad}(g) = p^k(\gamma)$, $p(\gamma)$ je ireducibilný polynóm (t.j. pokúsime sa "vylepšiť" blok typu B_{ij} z predošlého rozkladu). Nech

$$p(\gamma) = \gamma^q + c_{q-1}\gamma^{q-1} + c_{q-2}\gamma^{q-2} + \cdots + c_2\gamma^2 + c_1\gamma + c_0$$

Vo vektorovom priestore $[g](F)$ (t.j. modul $[g]$ berieme ako vektorový priestor nad poľom F) vyrobme nasledovné vektory:

$$\begin{array}{llll}
g_1 = g & g_2 = gA & \dots & g_q = gA^{q-1} \\
g_{q+1} = gp(A) & g_{q+2} = gp(A)A & \dots & g_{q+q} = gp(A)A^{q-1} \\
g_{2q+1} = gp^2(A) & g_{2q+2} = gp^2(A)A & \dots & g_{2q+q} = gp^2(A)A^{q-1} \\
\vdots & \vdots & & \vdots \\
g_{(k-1)q+1} = gp^{k-1}(A) & g_{(k-1)q+2} = gp^{k-1}(A)A & \dots & g_{(k-1)q+q} = gp^{k-1}(A)A^{q-1}
\end{array}$$

Keďže $p^k(\gamma) = m_{[g],A}$ je minimálny polynóm, je $\dim([g](F)) = st(p^k(\gamma)) = kq$. Uvedených vektorov je tiež kq a teda na to, aby sme dokázali, že tvoria bázu stačí dokázať, že sú lineárne nezávislé.

Nech teda $d_1g_1 + \cdots + d_{kq}g_{kq} = 0$, $d_i \in F$. Túto rovnosť môžeme napísať v tvare $(d_1m_1(\gamma) + \cdots + d_{kq}m_{kq}(\gamma))g = 0$, kde m_i sú polynómy tvaru $p^s(\gamma)\gamma^r$ stupňa menšieho ako kq. Zrejme je $st(m_i) = i - 1$. To znamená, že $d = st(d_1m_1(\gamma) + \cdots + d_{kq}m_{kq}(\gamma)) < kq$ a preto, keďže $d < st(\mathrm{rad}(g))$, musí byť polynóm $d_1m_1(\gamma) + \cdots + d_{kq}m_{kq}(\gamma)$ rovný nule. Ak je teraz i posledný (najvačší) index taký, že $d_i \neq 0$, polynóm $d_1m_1(\gamma) + \cdots + d_{kq}m_{kq}(\gamma)$ bude zrejme mať pri γ^i koeficient d_i, lebo tento sa nemá čím "vyrušiť". Teda ak existuje $d_i \neq 0$, polynóm nebude nulový - spor.

Ako vyzerá matica B transformácie A pri báze $g_1, \dots, g_{kq}$? Platí

$$g_1A = g_2, g_2A = g_3, \dots, g_{q-1}A = g_q$$

Ďalej,

$$g_qA = g_1A^q = g_1p(A) - c_{q-1}gA^{q-1} - \cdots - c_1gA - c_0g = -c_0g_1 - \cdots - c_{q-1}g_q + g_{q+1}$$

Prvých q riadkov matice B bude:

$$\left(\begin{array}{cccccc|cccc}
0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\
 & & & & & & & & & \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\
-c_0 & -c_1 & -c_2 & \cdots & -c_{q-2} & -c_{q-1} & 1 & 0 & \cdots & 0
\end{array}\right)$$

Skúsme urobiť "indukčný" krok: Ak $i < k - 1$ platí

$$g_{iq+1}A = g_{iq+2}, g_{iq+2}A = g_{iq+3}, \ldots, g_{iq+q-1}A = g_{(i+1)q}$$

a

$$\begin{aligned} g_{(i+1)q}A &= g_{iq}A^q = g_{iq}p(A) - c_{q-1}g_{iq}A^{q-1} - \cdots - c_1 g_{iq}A - c_0 g_{iq} \\ &= -c_0 g_{iq+1} - \cdots - c_{q-1}g_{iq+q} + g_{(i+1)q+1} \end{aligned}$$

Tieto výpočty určujú riadky $iq+1, \ldots, (i+1)q$ matice B a zasiahnu jej stĺpce $iq+1, \ldots, (i+1)q+q$. Uvedený blok matice B bude vyzerať rovnako ako sme uviedli pri prvých q riadkoch.

Pre $i = k-1$

$$g_{(k-1)q+1}A = g_{(k-1)q+2}, g_{(k-1)q+2}A = g_{(k-1)q+3}, \ldots, g_{(k-1)q+q-1}A = g_{kq}$$

a

$$\begin{aligned} g_{kq}A &= g_{(k-1)q}A^q = g_{(k-1)q}p(A) - c_{q-1}g_{(k-1)q}A^{q-1} - \cdots - c_1 g_{(k-1)q}A - c_0 g_{(k-1)q} \\ &= -c_0 g_{(k-1)q+1} - \cdots - c_{q-1}g_{(k-1)q+q} \end{aligned}$$

lebo $g_{(k-1)q}p(A) = g_1 p^k(A) = 0$ ($p^k(\gamma)$ je minimálny polynóm).

Tu sa už teda neuplatní podmatica uvedená pri prvých q riadkoch za čiarou. Ak označíme

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & & & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{q-2} & -c_{q-1} \end{pmatrix}$$

a

$$N = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ & & & \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

bude B bloková matica tvaru

$$B = \begin{pmatrix} P & N & 0 & \cdots & 0 & 0 \\ 0 & P & N & \cdots & 0 & 0 \\ & & & & & \\ 0 & 0 & 0 & \cdots & P & N \\ 0 & 0 & 0 & \cdots & 0 & P \end{pmatrix}$$

Takúto maticu budeme nazývať *Jordanovou maticou polynómu* $p^k(\gamma)$ (čítaj Žordan), označíme ju J_{p^k}. Blokovo diagonálnu maticu B, ktorá vznikne tak, že pre každý elementárny deliteľ $p_{ij}^{k_{ij}}(\gamma)$ matice A dáme na diagonálu blok $J_{p_{ij}^{k_{ij}}}$ (ak sa rovnaký polynóm v systéme elementárnych deliteľov opakuje , dáme ho tam toľko krát, koľko krát sa opakuje. Vzhľadom na to, že na poradí týchto blokov nezáleží, môžeme ich dať všetky rovnaké "za sebou") nazveme *Jordanov kanonický tvar matice A druhého druhu.*

Nad algebraicky uzavretým poľom F sú ireducibilné normované polynómy v tvare $x-a$, $a \in F$. Matica P je v tomto prípade 1×1 a obsahuje prvok a, matica N je tiež 1×1 a obsahuje prvok 1. V tomto prípade Jordanova matica $J_{(x-a)^k}$ je matica $k \times k$ tvaru

$$J_{(x-a)^k} = \begin{pmatrix} a & 1 & 0 & \cdots & 0 & 0 \\ 0 & a & 1 & \cdots & 0 & 0 \\ & & & & & \\ 0 & 0 & 0 & \cdots & a & 1 \\ 0 & 0 & 0 & \cdots & 0 & a \end{pmatrix}$$

Uveďme si základné vlastnosti menovaných kanonických tvarov matíc.

Veta 1.3.4 *Nech A, B sú matice $n \times n$ nad poľom F. Nasledujúce podmienky sú ekvivalentné:*

i) A a B sú podobné

ii) $\gamma I - A$ a $\gamma I - B$ sú ekvivalentné nad $F[\gamma]$ (t.j. majú "rovnaký" Smithov kanonický tvar)

iii) A a B majú rovnaké invariantné faktory

iv) A a B majú rovnaké systémy elementárnych deliteľov

Dôkaz. *i)* $\Rightarrow$ *ii)*: Nech $B = PAP^{-1}$. Odtiaľ dostaneme $\gamma I - B = \gamma I - PAP^{-1} = P(\gamma I - A)P^{-1}$, t.j. $\gamma I - A$ a $\gamma I - B$ sú ekvivalentné nad $F[\gamma]$, lebo každá regulárna matica je súčin elementárnych matíc nad F a teda aj nad $F[\gamma]$.

ii) $\Rightarrow$ *iii)*, *iii)* $\Rightarrow$ *iv)*: Keď sú $\gamma I - A$ a $\gamma I - B$ sú ekvivalentné nad $F[\gamma]$, majú rovnaké Smithove kanonické tvary. Preto majú rovnaké invariantné delitele. Invariantné delitele úplne určujú systémy elementárnych deliteľov a tieto preto musia byť rovnaké.

iv) $\Rightarrow$ *i)*: Ak majú A a B rovnaké systémy elementárnych deliteľov, majú rovnaké Jordanove kanonické tvary. Keďže matica je podobná svojmu Jordanovmu kanonickému tvaru a podobnosť je ekvivalencia na maticiach rovnakého typu nad rovnakým poľom, musia byť A a B podobné. □

Veta 1.3.5 *Nech A je matica nad poľom F. Nasledujúce podmienky sú ekvivalentné:*

i) A je podobná diagonálnej matici

ii) elementárne delitele matice A sú polynómy prvého stupňa

iii) posledný invariantný faktor má samé jednoduché korene a tie ležia všetky v poli F

Dôkaz. *i)* $\Rightarrow$ *ii)*: Nech diagonálna matica $D = \mathrm{diag}(d_1, d_2, \ldots)$ je podobná matici A. Matice A a D majú rovnaké Jordanove kanonické tvary. Jordanov kanonický tvar diagonálnej matice je však táto matica sama (overte!) Jednotlivé Jordanove bloky matice D a teda aj A sú bloky 1×1, ktoré preto prináležia elementárnym deliteľom prvého stupňa typu $\gamma - d_i$.
ii) $\Rightarrow$ *iii)*: Posledný invariantný faktor je súčin niekoľkých navzájom nesúdeliteľných elementárnych deliteľov, t.j. súčin niekoľkých nesúdeliteľných polynómov tvaru $\gamma - d_i$. T.j. posledný invariantný deliteľ má len jednoduché korene, ktoré všetky ležia v poli F.
iii) $\Rightarrow$ *i)*: Každý elementárny deliteľ matice A je deliteľom niektorého elementárneho deliteľa nachádzajúceho sa v poslednom invariantnom faktore (plynie zo vzájomnej deliteľnosti po sebe nasledujúcich invariantných faktorov). Posledne menované sú však prvého stupňa (lebo máme len jednoduché korene a všetky sú z F). Preto je Jordanov kanonický tvar prislúchajúci ku takejto matici diagonálna matica. □

Pripomeňme si, že podobné matice majú rovnaké charakteristické a minimálne polynómy. Vieme tiež, že tieto dve rovnosti nezabezpečia podobnosť matíc.

Veta 1.3.6 *Charakteristický polynóm matice A je súčin jej invariantných deliteľov (a teda aj všetkých elementárnych deliteľov).*

Dôkaz. Nech matica A je nad poľom F. Nech B je kanonický tvar 1. druhu matice A. Nech B_i je jeden z blokov v matici B, t.j. B_i je matica pridružená invariantnému faktoru $d_i(\gamma)$. Jednoduchou indukciou (rozpis determinantu podľa prvého stĺpca) zistíme, že charakteristický polynóm matice B_i pridruženej ku normovanému polynómu d_i je práve polynóm d_i, t.j. $ch_{B_i}(\gamma) = d_i(\gamma)$.

Samozrejme,

$$ch_A(\gamma) = ch_{B_1}(\gamma) \cdot \ldots \cdot ch_{B_k}(\gamma) = d_1(\gamma) \cdot \ldots \cdot d_k(\gamma)$$

□

Veta 1.3.7 *Minimálny polynóm matice A je jej posledný invariantný faktor.*

Dôkaz. Majme modul $(F[\gamma], V_n(F), A)$ napísaný v tvare

$$(F[\gamma], V_n(F), A) = [g_1] \oplus \cdots \oplus [g_k],$$

kde uvedený zápis vyhovuje zneniu vety o rozklade konečne generovaných modulov, t.j. pre každé prípustné i je $\mathrm{rad}(g_i) = d_i(\gamma)$, t.j. jeden z invariantných faktorov A. Vieme, že $d_i | d_{i+1}$. Preto pre posledný invariantný faktor d_k platí, že pre všetky i je $d_k g_i = 0$, t.j. $m_{A,V_n}(\gamma) \,|\, d_k$. Ale $d_k = m_{A,g_k}(\gamma) \,|\, m_{A,V_n}(\gamma)$, t.j. $d_k = m_{A,V_n}(\gamma)$. □

Dôsledok 1.3.8 *Matica A je podobná diagonálnej práve vtedy, keď jej minimálny polynóm má len jednoduché korene a tie všetky patria do poľa F.*

Dôkaz. □

Veta 1.3.9 (Cayley-Hamilton) *Nech $ch_A(\gamma) \in F[\gamma]$ je charakteristický polynóm matice A. Potom $ch_A(A) = 0$.*

Dôkaz. Z predošlých dvoch viet vieme, že pre minimálny a charakteristický polynóm matice A platí deliteľnosť $m_{A,V_n}(\gamma) \mid ch_A(\gamma)$. Keďže $m_{A,V_n}(A) = 0$, bude aj $ch_A(A) = 0$. □

1.4 Skalárny súčin a unitárna/ortogonálna podobnosť

1.4.1 Bilineárne formy, skalárny súčin

Štandardný skalárny súčin vo vektorovom priestore $V_n(R)$ je zobrazenie $g : V_n(R) \times V_n(R) \to R$ dané predpisom

$$g(x, y) = x_1y_1 + \cdots + x_ny_n, \text{ kde } x = (x_1, \ldots, x_n) \in V_n(R),\ y = (y_1, \ldots, y_n) \in V_n(R)$$

Vektorový priestor $\in V_n(R)$ spolu s uvedeným skalárnym súčinom nazývame $n-$rozmerným reálnym euklidovským priestorom. Vyššie uvedná funkcia $g(-,-)$ má nasledujúce vlastnosti (pre všetky $x, y, z) \in V_n(R)$, všetky $c \in R$):

1. $g(x, y) = g(y, x)$
2. $g(x + y, z) = g(x, z) + g(y, z)$
3. $g(x, y + z) = g(x, y) + g(x, z)$
4. $g(cx, y) = cg(x, y)$
5. $g(x, cy) = cg(x, y)$
6. $g(x, x) \geq 0$, $g(x, x) = 0$ práve vtedy, keď $x = \mathbf{0}$

Podobne vieme zadefinovať skalárny súčin na vektorovom priestore nad poľom komplexných čísiel C, keď použijeme zobrazenie $g : V_n(C) \times V_n(C) \to C$ dané predpisom

$$g(x, y) = x_1\overline{y}_1 + \cdots + x_n\overline{y}_n, \text{ kde } x = (x_1, \ldots, x_n) \in V_n(C),\ y = (y_1, \ldots, y_n) \in V_n(C)$$

Vektorový priestor $\in V_n(C)$ spolu s uvedeným skalárnym súčinom nazývame $n-$rozmerným komplexným euklidovským priestorom, alebo tiež unitárnym priestorom. Vyššie uvedná funkcia $g(-,-)$ má nasledujúce vlastnosti (pre všetky $x, y, z) \in V_n(C)$, všetky $c \in C$):

1. $g(x, y) = \overline{g(y, x)}$
2. $g(x + y, z) = g(x, z) + g(y, z)$
3. $g(x, y + z) = g(x, y) + g(x, z)$
4. $g(cx, y) = cg(x, y)$
5. $g(x, cy) = \overline{c}g(x, y)$
6. $g(x, x) \geq 0$, $g(x, x) = 0$ práve vtedy, keď $x = \mathbf{0}$

Zaujímavý je rozdiel vlastností 1 a 5, kde je v prípade komplexných čísiel potrebné použiť komplexné združenie.

V ďalšom budeme pracovať s poľom F s involúciou, t.j. automorfizmom poľa F $c \to \overline{c}$ s vlastnosťou $\overline{(\overline{c})} = c$. Komplexné združenie (t.j. priradenie komplexne združeného čísla danému komplexnému číslu) je involúciou poľa C. Každé pole pole má aspoň jeden automorfizmus, a to identické zobrazenie, takže toto nepredstavuje obmedzenie.

Definícia 1.4.1 *Nech F je pole s involúciou $c \to \overline{c}$, $V(F)$ je vektorový priestor (nie nutne konečnorozmený). Zobrazenie $g : V(F) \times V(F) \to F$ s vlastnosťami (pre všetky $x, y, z \in V(F)$, $c \in F$)*

1. $g(x + y, z) = g(x, z) + g(y, z)$
2. $g(x, y + z) = g(x, y) + g(x, z)$
3. $g(cx, y) = cg(x, y)$
4. $g(x, cy) = \overline{c}g(x, y)$

sa nazýva bilineárna forma na $V(F)$.

Ak naviac pre všetky $x, y \in V(F)$ platí

5 $g(x, y) = \overline{g(y, x)}$

nazývame g skalárnym súčinom.

Ak je g skalárny súčin, zobrazenie dané predpisom $x \to g(x, x)$ nazývame kvadratickou formou na $V(F)$.

Ak je F podpole poľa C, bilineárnu formu g nazývame pozitívne semidefinitnou (definitinou) ak je pre všetky $x \in F$

6 $g(x,x) \in R$, *dokonca* $g(x,x) \geq 0$ *(a pre definitnosť ešte požadujeme, aby* $g(x,x) = 0$ *práve vtedy, keď* $x = \mathbf{0}$*)*

Keďže najdôležitejší prípad pre nás stále ostane prípad $F = R$ s identickou involúciou alebo $F = C$ s komplexným združením, budeme používať nasledujúcu dohodu:

Definícia 1.4.2 *Skalárny súčin* g *na* $V(F)$ *voláme symetrickým, ak je zvolená involúcia identita. Ak je naviac* $F = R$*, budeme hovoriť o reálnom symetrickom skalárnom súčine.*

Skalárny súčin g *na* $V(F)$ *pre* $F = C$ *a voláme hermitovským, ak je zvolená involúcia komplexné združenie.*

Nech g je bilineárna forma na $n-$rozmernom vektorovom priestore $V(F)$, nech $e_1, \ldots, e_n$ je jeho báza. Potom môžeme definovať maticu (priradiť ju ku danej bil. forme g)

$$G = \begin{pmatrix} g(e_1,e_1) & \ldots & g(e_1,e_n) \\ \ldots & \ldots & \ldots \\ g(e_n,e_1) & \ldots & g(e_n,e_n) \end{pmatrix} = ||g(e_i,e_j||_{n\times n}$$

Ak použijeme zápis vektorov z priestoru $V(F)$ v súradniciach v báze $e_1, \ldots, e_n$, t.j. $x = x_1e_1 + \cdots + x_ne_n$ a $y = y_1e_1 + \cdots + y_ne_n$, tak

$$\begin{aligned} g(x,y) &= g(x_1e_1 + \cdots + x_ne_n, y_1e_1 + \cdots + y_ne_n) = x_1g(e_1, y_1e_1 + \cdots + y_ne_n) + \cdots + x_ng(e_n, y_1e_1 + \cdots + y_ne_n) = \\ &= \sum_{i=1}^{n} x_i(\sum_{j=1}^{n} g(e_i, e_j\overline{y}_j) = \sum_{i=1}^{n}(\sum_{j=1}^{n} x_ig(e_i,e_j)\overline{y}_j) \end{aligned}$$

čo očividne zodpovedá súčinu matíc

$$(x_1, \ldots, x_n) \begin{pmatrix} g(e_1,e_1) & \ldots & g(e_1,e_n) \\ \ldots & \ldots & \ldots \\ g(e_n,e_1) & \ldots & g(e_n,e_n) \end{pmatrix} \begin{pmatrix} \overline{y}_1 \\ \vdots \\ \overline{y}_n \end{pmatrix}$$

t.j. ak položíme $X = (x_1, \ldots, x_n)$ a $Y = (y_1, \ldots, y_n)$, $\overline{Y} = (\overline{y}_1, \ldots, \overline{y}_n)$ a X^T je transponovanie matíc, tak

$$g(x,y) = X G \overline{Y}^T$$

Naopak, matica G, ktorá je $n \times n$ pri danej báze $e_1, \ldots, e_n$ $n-$rozmerného vektorového priestoru $V(F)$ jednoznačne definuje bilineárnu formu, vlastnosti 1 a 2 z definície bilineárnej formy vyplývajú z distributívnosti násobenia (alebo ich vidieť aj z toho, že matica zodpovedá lineárnemu zobrazeniu).

Matica G nemusí mať nijakú špeciálnu vlastnosť. Aby však mohla byť pre g splnená vlastnosť 5, je nutné, aby pre prvky matice $G = ||g_{ij}||_{n\times n}$ platilo $g_{ij} = \overline{g}_{ji}$.

Pozrime sa čo sa stane, ak namiesto bázy $e_1, \ldots, e_n$ použijem inú bázu, $e'_1, \ldots, e'_n$. Nech $G' = ||g(e'_i, e'_j||_{n\times n}$ a nech $P = ||p_{ij}||_{n\times n}$ je taká matica, že $e'_i = \sum_{j=1}^{n} p_{ij}e_j$ (t.j. matica prechodu od bázy $e_1, \ldots, e_n$ ku báze $e'_1, \ldots, e'_n$, je to regulárna matica).

Potom podľa nášho vzorca na výpočet g pomocou matice G samozrejme

$$g(e'_i, e'_j) = (p_{i1}, \ldots, p_{in})G(\overline{p}_{j1}, \ldots, \overline{p}_{jn})^T$$

a teda

$$G' = PG\overline{P}^T$$

kde $\overline{P} = ||\overline{p}_{ij}||_{n\times n}$. Toto pozorovanie vedie k definícii

Definícia 1.4.3 *Nech* F *je pole s involúciou. Štvorcová matica* B *sa nazýva kogradientnou so štvorcovou maticou* A*, ak existuje regulárna (štvorcová) matica* P *taká, že* $B = PA\overline{P}^T$*.*

Cvičenie 35 *Dokážte, že ak je* A *matica nejakej bilineárnej formy* g *pri nejakej báze* $e_1, \ldots, e_n$*, a* B *je kogradientná s* A*, tak* B *je tiež matica formy* g *pri nejakej (možno inej) báze.*

Cvičenie 36 *Dokážte, že relácie kogradiencie je na maticiach* $n \times n$ *nad poľom* F *s involúciou relácia ekvivalencie.*

V ďalšej časti by sme sa chceli venovať hľadaniu jednoduchých matíc v triedach ekvivalencie vzhľadom na kogradienciu, t.j. úlohe nájsť čo "najjednoduchšiu" maticu (blízku k diagonálnej), ktorá je kogradientná s danou maticou A.

Pre jednoduchšiu formuláciu algoritmu a výsledkov pripomeňme nasledujúce označenia:

- $E_{i,j}$ je matica, ktorá vznikne z matice I výmenou $i-$tého a j-tého riadku
- $E_{c,i}$ je matica, ktorá vznikne z matice I vynásobením $i-$tého prvkom $c \in F$ $(c \neq 0)$
- $E_{c,i,j}$ je matica, ktorá vznikne z matice I pripočítaním c násobku $i-$tého riadku ku j-tému riadku $(i \neq j)$

Tieto matice nazývame elemantárne matice a umožňujú simulovať elementárne riadkové operácie pomocoou násobenia a vzhľadom na to, že každá regulárna matica sa dá napísať ako súčin elementárnych matíc (ktoré zodpo,vedajú úprave danej matice na trojuholníkový redukovaný tvar, ktorý je v prípade regulárnej matice samozrejme matica I).

Presnejšie pre regulárnu maticu P existujú také elementárne matice $E'_n, E'_{n-1}, \ldots, E'_1$, že $E'_n E'_{n-1} \ldots E'_1 P = I$ a vzhľadom na to, že inverzná matica ku elementárnej matici je opäť elementárna matica (ku E_{ij} je to samo E_{ij}, ku $E_{c,j}$ je to $E_{c^{-1},j}$, ku $E_{c,i,j}$ je to $E_{-c,i,j}$), tak $P = E_n E_{n-1} \ldots E_1$, t.j.

$$PA\overline{P}^T = E_n E_{n-1} \ldots E_1 \; A \; \overline{E}_1^T \overline{E}_2^T \ldots \overline{E}_n^T$$

Tieto úvahy nám umožnia jednoducho sformulovať dôkaz nasledujúcej vety:

Veta 1.4.4 *Nech F je pole s involúciou $c \to \bar{c}$, $char(F) \neq 2$ a A je obecná hermitovská matica nad F. Potom A je kogradientná s diagonálnou maticou D, v ktorej počet nenulových diagonálnych prvkov je hodnosť matice A.*

Dôkaz. Budeme postupovať indukciou. Ak je matica A typu 1×1, je to diagonálna matica a nemáme čo dokazovať.

Nech je matica A nenulová (ak je nulová, je diagonálna a opäť nie je čo robiť) a nech je teda typ matice A $n \times n$, $n > 1$ a nech tvrdenie platí pre všetky čísla menšie ako n.

Maticu A prevedieme pomocou kogradientnych úprav na tvar

$$B = \begin{pmatrix} b_{11} & 0 & \ldots & 0 \\ 0 & b_{22} & \ldots & b_{2n} \\ & & \ldots & \\ 0 & b_{n2} & \ldots & b_{nn} \end{pmatrix}$$

a využijeme indukčný predpoklad pre podmaticu $(n-1) \times (n-1)$ v pravom dolnom rohu.

Pri matici A máme tri základné možnosti:

1. prvok a_{11} je nenulový
2. prvok a_{11} je nulový, ale niektorý diagonálny prvok (napr. a_{ii}) je nenulový
3. všetky diagonálne prvky sú nulové, ale niektorý nediagonálny prvok (napr. a_{ij}, $i \neq j$) je nenulový

Základná varianta algoritmu pracuje s prípadom 1. Pre prípady 2 a 3 ukážeme, ako sa dajú previesť na prípad 1.

Prípad 2: ak je teda $a_{11} = 0$ a $a_{ii} \neq 0$, stačí vymeniť riadky 1 a i a následne stĺpce 1 a i. Táto symetrická úprava okrem iného navzájom vymení diagonálne prvky a_{11} a a_{ii} a teda v novej matici bude na pozícii a_{11} nenulový prvok.

Prípad 3: Nech sú všetky diagonálne prvky $a_{ii} = 0$ a nech $a_{ij} \neq 0$ $(i \neq j)$. Pripočítajme $1/a_{ij}$ násobok i-teho riadku ku prvému riadku a následne $1/\overline{a_{ij}}$ násobok i-teho stĺpca ku prvému stĺpcu. Touto úpravou získame na mieste a_{11} prvok 2, ktorý je podľa predpokladu nenulový.

Základný algoritmus, prípad 1: Keďže je $a_{11} \neq 0$, môžeme urobiť štadarntú elimináciu, len treba dať pozor na to, že všetky úpravy musíme robiť symetricky. T.j. pripočítajme $-a_{21}/a_{11}$ násobok 1-teho riadku ku druhéme riadku a následne $-\overline{a_{21}}/\overline{a_{11}}$ násobok 1-teho stĺpca ku druhému stĺpcu. Tým dostaneme na pozíciách a_{21} a a_{12} nuly.

Potom pripočítajme $-a_{31}/a_{11}$ násobok 1-teho riadku ku tretiemu riadku a následne $-\overline{a_{31}}/\overline{a_{11}}$ násobok 1-teho stĺpca ku tretiemu stĺpcu. Tým dostaneme na pozíciách a_{31} a a_{13} nuly.

Takto pokračujeme až k poslednému riadku, kedy pripočítaním $-a_{n1}/a_{11}$ násobku 1-teho riadku ku n-tému riadku a následne $-\overline{a_{n1}}/\overline{a_{11}}$ násobku 1-teho stĺpca ku n-tému stĺpcu dostaneme na pozíciách a_{n1} a a_{1n} nuly.

□

Jednoduchým dôsledkom uvedenej vety je

Veta 1.4.5 *Nech $g(x,y)$ je skalárny súčin na konečnorozmernom vektorovom priestore nad poľom F s involúciou a $char(F) \neq 2$. Potom existuje taká báza $e_1, \ldots, e_n$ tohoto vektorového priestoru, že $g(e_i, e_j) = 0$.*

Podobne ako v prípade reálneho vektorového priestoru so skalárným súčinom (euklidovského priestoru), bude užitočný pojem ortogonálnej a ortonormálnej bázy:

Definícia 1.4.6 *Majme vektový priestor V so skalárnym súčinom g. Vektory $x, y \in V$ nazývame ortogonálne (v skal. súčine g, vzhľadom na sk. súčin g), ak $g(x,y) = 0$ (píšeme $x \perp y$).*

Báza $\alpha_1, \ldots, \alpha_n$ sa nazýva ortonormálna ak $g(\alpha_i, \alpha_j) = \delta_{ij}$, t.j. 0 (ak $i \neq j$) alebo 1 (ak $i = j$).

Systém vektorov (bázu) $\alpha_1, \ldots, \alpha_n$ nazveme ortogonálnou, ak $g(\alpha_i, \alpha_i) \neq 0$ pre všetky $i = 1, .., n$ a $g(\alpha_i, \alpha_j) = 0$ pre všetky $i \neq j$.

1.4.2 Adjungované operátory

Definícia 1.4.7 *Nech (V, F) je vektorový priestor. Potom každé lineárne zobrazenie $\varphi : V \to F$ nazývame* (lineárnym) funkcionálom. *(F považujeme za jednorozmerný vektorový priestor nad samým sebou.)*

Najprv si uvedieme dôležitú vetu, ktorej vo všeobecnej funkcionálnej analýze zodpovedá Rieszova veta.

Veta 1.4.8 *Nech (V, F, g) je konečnorozmerný euklidovský priestor. Nech φ je funkcionál na (V, F). Potom existuje práve jeden vektor $y \in V$ taký, že $\varphi = g(-, y)$, t.j. pre všetky $x \in V$ platí $\varphi(x) = g(x, y)$.*

Dôkaz. Nech $\epsilon_1, \ldots, \epsilon_n$ je ortonormálna báza (V, F, g). Nech $x = a_1\epsilon_1 + \cdots + a_n\epsilon_n$. Potom vďaka linearite je $\varphi(x) = a_1\varphi(\epsilon_1) + \cdots + a_n\varphi(\epsilon_n)$ a teda ak položíme $y = \overline{\varphi(\epsilon_1)}\epsilon_1 + \cdots + \overline{\varphi(\epsilon_n)}\epsilon_n$, tak je vidieť, že $\varphi(x) = g(x, y)$. Nech teraz ešte y' je taký vektor, že tiež pre všetky $x \in V$ platí $\varphi(x) = g(x, y')$. Potom

$$0 = \varphi(x) - \varphi(x) = g(x, y) - g(x, y') = g(x, y - y').$$

Špeciálne teda $g(y - y', y - y') = 0$ a z pozitívnej definitnosti g vyplýva, že $y - y' = 0$, teda uvedené y je jediné. □

Zoberme lineárnu transformáciu (operátor) $A : V \to V$ n-rozmerného euklidovského priestoru. Namiesto $g(x, y)$ budeme odteraz písať len (x, y). Ak zvolíme pevné $y \in V$, tak $f(x) = (xA, y)$ je funkcionál na V a preto podľa predošlej lemy existuje jediné y' také, že $(xA, y) = (x, y')$. Označme zobrazenie $y \to y'$ ako A^*. Presvedčme sa, že $A^* : V \to V$ je tiež lineárne zobrazenie. Majme ešte $zA^* = z'$. Potom podľa definície platí, že $(xA, y + z) = (x, (y + z)A^*)$. Na druhej strane však z linearity skalárneho súčinu plynie $(xA, y + z) = (xA, y) + (xA, z) = (x, yA^*) + (x, zA^*)$. Teda (pre všetky $x \in V$) platí $(x, (y + z)A^*) = (x, yA^*) + (x, zA^*) = (x, yA^* + zA^*)$. Teda pre všetky $x \in V$ je $(x, (y + z)A^* - yA^* - zA^*) = 0$. Ak však zoberieme $x = (y + z)A^* - yA^* - zA^*$, máme $(x, x) = 0$ a teda vďaka pozitívnej definitnosti dostaneme, že $x = (y + z)A^* - yA^* - zA^* = 0$. Teda pre všetky $x, y \in V$ je $(y+z)A^* = yA^* + zA^*$. Ďalej nech $c \in F$. Potom $(xA, cy) = (x, (cy)A^*)$ podľa definície A^*. Z vlastností skalárneho súčinu vyplýva, že $(xA, cy) = \overline{c}(xA, y) = \overline{c}(x, yA^*) = (x, c(yA^*))$. Z týchto dvoch vzťahov dostaneme, že pre všetky $x \in V$ platí, že $(x, (cy)A^* - c(yA^*)) = 0$ a položením $x = (cy)A^* - c(yA^*)$ opäť zistíme, že $x = (cy)A^* - c(yA^*) = 0$ a teda pre všetky $y \in V$ platí $(cy)A^* = c(yA^*)$. Toto uzatvára dôkaz lineárnosti zobrazenia A^*. (Rozmyslite si, kde sme použili linearitu zobrazenia A!)

Veta 1.4.9 *Nech (V, F) je euklidovský vektorový priestor (reálny alebo komplexný). Potom ku každej lineárnej transformácii $A : V \to V$ existuje jediná lineárna transformácia $A^* : V \to V$ taká, že pre každé $x, y \in V$ platí*

$$(xA, y) = (x, yA^*).$$

Pre zobrazenie * z vekt. priestoru všetkých lineárnych zobrazení V do V do vekt. priestoru všetkých lineárnych zobrazení V do V platia nasledujúce vzťahy:

1. $I^* = I$
2. $(A + B)^* = A^* + B^*$
3. $(cA)^* = \overline{c}A^*$
4. $(A^*)^* = A$
5. $(AB)^* = B^*A^*$

Definícia 1.4.10 *Lineárnu transformáciu $A^* : V \to V$ nazývame adjungovanou (združenou, pridruženou) ku lin transformácii $A : V \to V$.*

Dôkaz. Existenciu a jednoznačnosť adjungovanej transformácie A^* sme už dokázali.
1: $(x, y) = (xI, y) = (x, yI^*)$. Teda pre všetky $x, y \in V$ je $(x, y - yI^*) = 0$ a odtiaľ pomocou argumentu podobnému tomu, ktorý sme už dvakrát použili dostávame $I^* = I$.
2: $(x, y(A+B)^*) = (x(A+B), y) = (xA, y)+(xB, y) = (x, yA^*)+(x, yB^*) = (x, yA^* + yB^*)$. Odtiaľ dostaneme $(A + B)^* = A^* + B^*$.
3: $(x, y(cA)^*) = (x(cA), y) = c(xA, y) = c(x, yA^*) = (x, y(\overline{c}A^*)$.
4: $(xA^*, y) = (x, y(A^*)^*) = \overline{(y, xA^*)} = \overline{(yA, x)} = (x, yA)$.
5: $(x, y(AB)^*) = (x(AB), y) = ((xA)B, y) = (xA, yB^*) = (x, (yB^*)A^*) = (x, y(B^*A^*))$. □

Ešte určime maticu adjungovanej transformácie pri karteziánskej báze $\epsilon_1, \ldots, \epsilon_n$ (t.j. $(\epsilon_i, \epsilon_j) = \delta_{ij}$). Nech matica transformácie A je $||a_{ij}||$. Nech je $\epsilon_i A^* = \sum_{j=1}^n b_{ij}\epsilon_j$. Teda $||b_{ij}||$ je matica zobrazenia A^* pri báze $\epsilon_1, \ldots, \epsilon_n$. Zoberme $b_{ij} = (\epsilon_i A^*, \epsilon_j) = (\epsilon_i, \epsilon_j A) = \overline{(\epsilon_j A, \epsilon_i)} = \overline{a_{ji}}$. Teda $||b_{ij}|| = \overline{||a_{ij}||}'$.

Definícia 1.4.11 *Lineárna transformácia (operátor) A na n-rozmernom euklidovskom priestore (V,F) sa nazýva* samoadjungovaná, *ak $A^* = A$ (pre $F = R$ hovoríme o* symetrickej *transformácii). A sa nazýva* kosohermitovská *(pre $F = R$* kososymetrická*) ak $A^* = -A$. A sa nazýva unitárna (pre $F = R$* ortogonálna*), ak $A^* = A^{-1}$.*

Cvičenie 37 *Nech (V,F) je n-rozmerný vektorový priestor s bázou $\epsilon_1, \ldots, \epsilon_n$. Nech V^* označuje množinu všetkých funkcionálov na (V,F). Ak definujeme cf pre $c \in F$ a $f \in V^*$ ako $cf(x) = f(cx)$ a $f+g$ pre $f, g \in V^*$ ako $(f+g)(x) = f(x) + g(x)$, tak (V^*, F) je vektorový priestor. Dokážte! Tento priestor nazývame duálnym vekt. priestorom ku (V,F). Nech $\epsilon_i^*(\epsilon_j) = \delta_{ij}$. Potom $\epsilon_1^*, \ldots, \epsilon_n^*$ je báza (V^*, F) a teda (V^*, F) je n-rozmerný vektorový priestor.*

Cvičenie 38 *Nech (V^{**}, F) je duálny priestor ku (V^*, F). Zoberme $x \in V$. Ukážte, že $f \to x(f) = f(x)$ je prvok V^{**}. Dokážte, že $x \to x(f)$ je izomorfizmus medzi (V^{**}, F) a (V^*, F).*

Cvičenie 39 *Na základe cvičenia 37 sú (V^*, F) a (V,F) izomorfné. Potom zobrazenie $(x,f) : V \times V^* \to F$ je bilineárne zobrazenie.*

Cvičenie 40 *Nech (V,F) je n-rozmerný euklidovský priestor. Majme lineárnu transformáciu $A : V \to V$. Ukážte, že (i) $(xA^*, y) = (x, yA)$; (ii) $f(x,y) = (xA, y)$ je bilineárna forma na (V,F); (iii) ku každej bilineárnej forme g na (V,F) existuje transformácia A tak, že $g(x,y) = (xA, y)$; (iv) zobrazenie $g \to A$ je bijekcia.*

Cvičenie 41 *Ukážte, že samoadjungovanej transformácii A zodpovedá hermitovská matica, symetrickej (kosohermitovskej, kososymetrickej) transformácii zodpovedá symetrická (kosohermitovská, kososymetrická) matica, unitárnej (ortogonálnej) transformácii zodpovedá unitárna (ortogonálna) matica a obrátene.*

Cvičenie 42 *Nech A je lineárna transformácia na n-rozmernom euklidovskom priestore. Nasledujúce tvrdenia sú ekvivalentné: (i) A je unitárna; (ii) A zachováva skalárny súčin (t.j. $(xA, yA) = (x,y)$; ak $F = R$, tak ešte aj s (iii) $(xA, xA) = (x,x)$, t.j. A zachováva dĺžky.*

Cvičenie 43 *Majme samoadjungované operátory A, B. Ukážte: AB je samoadjungovaný práve vtedy, keď $AB = BA$.*

Cvičenie 44 *Dokážte, že A je kosohermitovský operátor práve vtedy, keď $\imath A$ je samoadjungovaný.*

Cvičenie 45 *Ukážte, že každá linárna transformácia A na n-rozmernom euklidovskom priestore sa dá napísať ako $A = B + C$, kde B je samoadjungovaný operátor a C je kosohermitovský operátor. Naviac, tento rozklad je jednoznačný, a teda $B = (A + A^*)/2$, $B = (A - A^*)/2$.*

1.4.3 Samoadjungované, kosohermitovské a unitárne operátory

V tejto časti sa budeme zaoberať unitárnou a ortogonálnou kogradienciou — podobnosťou matíc. Začneme všeobecným tvrdením

Veta 1.4.12 *Nech $A = ||a_{ij}||$ je štvorcová matica typu $n \times n$ nad poľom F, (V,F) je euklidovský vektorový priestor (t.j. $F = R$ alebo $F = C$). Nech všetky vlastné čísla matice A sú z poľa F. Potom existuje horná trojuholníková matica T, ktorá je unitárne (ortogonálne ak $F = R$) podobná s maticou A.*

Dôkaz. Nech $a_n \in F$ je vlastné číslo matice A, nech $\alpha_n \in F^n$ je vlastný vektor matice A prislúchajúci ku a_n a ktorý má dĺžku 1. Nech $\alpha_1, \ldots, \alpha_{n-1}$ sú vektory v F^n, ktoré dopĺňajú α_n do ortonormálnej bázy priestoru (V,F). Transformácia s maticou A (t.j. A je matica tejto transformácie pri štandartnej báze) má v báze $\alpha_1, \ldots, \alpha_n$ maticu A', ktorej posledný riadok obsahuje len jeden zaujímavý prvok — posledný prvok je a_n a ostatné prvky v poslednom riadku sú nuly, t.j. ak sú riadky matice P po rade vektory $\alpha_1, \ldots, \alpha_n$, tak

$$\left(\begin{array}{c|c} & c_1 \\ \mathrm{B} & \vdots \\ & c_{n-1} \\ \hline 0 \ldots 0 & a_n \end{array}\right) = A' = PAP^*$$

Celý dôkaz teraz urobíme indukciou. Štart indukcie — matica A je 1×1, teda A je horná trojuholníková a nemáme čo dokazovať. Nech to teraz platí pre všetky matice B typu $(n-1) \times (n-1)$. Urobme vyššie uvedenú úvahu. Keďže pre charakteristické polynómy matíc A a B platí vzťah $ch_A(x) = (x - a_n) ch_B(x)$, každá vlastná hodnota matice B je vlastná hodnota matice A a preto všetky vlastné hodnoty matice B ležia v poli F. Matica B je podľa

indukčného predpokladu unitárne podobná hornej trojuholníkovej matici, označme ju T'. Teda existuje unitárna matica Q typu $(n-1)\times(n-1)$ taká, že $QBQ^* = T'$. Potom

$$\left(\begin{array}{c|c} Q & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \hline 0\ \dots\ 0 & 1 \end{array}\right) . \left(\begin{array}{c|c} B & \begin{matrix}c_1\\ \vdots\\ c_{n-1}\end{matrix} \\ \hline 0\ \dots\ 0 & a_n \end{array}\right) . \left(\begin{array}{c|c} Q^* & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \hline 0\ \dots\ 0 & 1 \end{array}\right) =$$

$$= \left(\begin{array}{c|c} QBQ^* & Q\gamma^T \\ \hline 0\ \dots\ 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} T' & Q\gamma^T \\ \hline 0\ \dots\ 0 & 1 \end{array}\right),$$

kde $\gamma = (c_1, \dots, c_{n-1})$. Posledná matica je ale horná trojuholníková matica. Keďže je matica

$$Q' = \left(\begin{array}{c|c} Q & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \hline 0\ \dots\ 0 & 1 \end{array}\right)$$

unitárna, je tým je ukončený dôkaz indukčného kroku. □

Unitárna podobnosť zachováva pojmy ako hermitovskosť, kosohermitovskosť a unitárnosť, t.j. ak je A hermitovská (kosohermitovská, unitárna) a P je unitárna matica, potom PAP^* je tiež hermitovská (kosohermitovská, unitárna). Ak je A (koso)hermitovská, a T je horná trojuholníková unitárne podobná s A, tak T je tiež (koso)hermitovská. To ale znamená, že T je diagonálna a pre prvok a z diagonály T platí $a = \overline{a}$ pre hermitovskú maticu a $a = -\overline{a}$ pre kosohermitovskú. Čiže ak je A hermitovská, je unitárne podobná s *reálnou* diagonálnou maticou a ak je A kosohermitovská, je unitárne podobná s *rýdzo imaginárnou* diagonálnou maticou. Platí teda

Dôsledok 1.4.13 *Nech A je komplexná matica. Ak je A hermitovská, tak vlastné čísla A sú reálne čísla, ak je A kosohermitovská, tak vlastné čísla A sú rýdzo imaginárne čísla a ak je A unitárna, tak vlastné čísla A sú komplexné čísla s dĺžkou* 1.

Dôkaz. Prvé dve tvrdenia vyplývajú z uvedených úvah a faktu, že podobné matice majú rovnaké vlastné čísla a vlastné čísla diagonálnej matice sú prvky z diagonály tejto matice.

Nech je A unitárna matica, nech a je vlastné číslo A, α nech je vlastný vektor dĺžky 1 prislúchajúci ku a. Potom $1 = (\alpha, \alpha) = (\alpha AA^*, \alpha) = (\alpha A, \alpha A) = (a\alpha, a\alpha) = a\overline{a}(\alpha, \alpha) = a\overline{a}$. To znamená, že a má dĺžku 1. □

Dôsledok 1.4.14 *Nech A je reálna symetrická matica. Potom je A ortogonálne podobná s diagonálnou maticou.*

Dôkaz. Matica A je podľa predpokladu hermitovská a teda má len reálne vlastné hodnoty. Podľa predošlej vety je teda ortogonálne podobná reálnej hornej trojuholníkovej matici a táto už nutne musí byť diagonálna. □

Všetky uvedené typy matíc sú teda unitárne podobné diagonálnej matici. Teraz sformulujeme podmienku, ktorá je ekvivalentná s unitárnou podobnoťou diagonálnej matici.

Definícia 1.4.15 *Štvorcovú maticu A nazveme normálnou, ak $AA^* = A^*A$.*

Uvedomme si, že pojem normálnosti sa tiež unitárnou podobnosťou zachováva.

Veta 1.4.16 *Matica A je unitárne podobná diagonálnej matici práve vtedy, keď je normálna.*

Dôkaz. Nech je najprv matica A unitárne podobná diagonálnej, t.j. $D = PAP^*$ pre vhodnú diagonálnu maticu D a unitárnu maticu P. Potom

$$\begin{aligned} AA^* &= P^*DP(P^*DP)^* = P^*DPP^*D^*P = P^*DD^*P = \\ &= P^*D^*DP = P^*D^*PP^*DP = A^*A \end{aligned}$$

a teda A je normálna matica.

Nech je A normálna matica. Vieme, že existuje horná trojuholníková matica T, ktorá je unitárne podobná matici A, t.j. $T = PAP^*$ pre vhodnú unitárnu maticu P. Potom T je tiež normálna matica. Indukciou dokážeme, že horná trojuholníková komplexná matica, ktorá je normálna je diagonálna. Pre matice 1×1 tvrdenie zrejme platí.

Nech $n \geq 2$ a nech

$$T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n-1} & t_{1n} \\ 0 & t_{22} & \dots & t_{2n-1} & t_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & t_{nn} \end{pmatrix}$$

Potom keďže $TT^* = T^*T$, rozpísaním ľavých horných prvkov v oboch týchto maticiach dostávame rovnicu

$$t_{11}\bar{t}_{11} + t_{12}\bar{t}_{12} + \dots + t_{1n}\bar{t}_{1n} = \bar{t}_{11}t_{11}$$

Odtiaľto je okamžite vidieť, že $t_{12} = \dots = t_{1n} = 0$ a teda

$$T = \left(\begin{array}{c|ccc} t_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & T' & \\ 0 & & & \end{array}\right),$$

kde T' je normálna horná trojuholníková matica. Podľa indukčného predpokladu je to diagonálna matica a teda celá matica T je diagonálna. □

Pre reálny prípad kosohermitovskej matice máme nasledovné tvrdenie:

Veta 1.4.17 *Nech A je (reálna) kososymetrická matica. Potom existuje blokovo diagonálna matica D s blokmi 1×1 obsahujúcimi 0 alebo blokmi 2×2 tvaru*

$$\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$$

a ortogonálna matica P tak, že platí $D = PAP^*$ (t.j. $D = PAP^{-1}$).

Dôkaz. Dôkaz urobíme indukciou. Pre maticu 1×1 tvrdenie platí. Nech $n \geq 2$ a nech tvrdenie platí pre všetky kososymetrické matice typu $m \times m$ také, že $m < n$.

Už vieme, že kosohermitovská a teda aj kososymetrická matica má rýdzoimaginárne vlastné hodnoty, t.j. 0 alebo ib, $b \in R$. Minimálny polynóm matice A má teda tvar $m_A(x) = x^k(x^2 + a_1)^{k_1} \dots (x^2 + a_l)^{k_l}$, kde a_i je kladné reálne číslo. Členy tvaru $x^2 + a_i$ tu zodpovedajú príslušným rýdzoimaginárnym nenulovým vlastným hodnotám. (Uvedomte si, že minimálny polynóm reálnej matice je reálny polynóm.)

Nech je $k > 0$, t.j. 0 je vlastná hodnota matice A. Nech α je reálny vlastný vektor taký, že $\alpha A = \mathbf{0}$. Nech $\|\alpha\| = 1$. Položme $V = [\alpha]$ (generovaný ako reálny priestor). Podpriestor V je zrejme invariantný vzhľadom na transformáciu určenú maticou A. Dokážeme, že aj ortogonálny doplnok $V^\perp$ je A-invariantný. Nech $\beta \in V^\perp$. Potom $(\beta, \alpha) = 0$. Ale vďaka kososymetričnosti matice A platí $(\beta A, \alpha) = (\beta, \alpha A^T) = (\beta, -\alpha A) = (\beta, \mathbf{0}) = 0$. Teda $\beta A \in V^\perp$. Ďalej uvažujeme o transformácii A zúženej na podpriestor $V^\perp$, označme ju ako A'. Táto transformácia je kososymetrická a teda matica, ktorá jej prislúcha v ľubovoľnej ortonormálnej báze je kososymetrická. Ak je teda $\alpha_2, \dots, \alpha_n$ je ortonormálna báza $V^\perp$, tak $\alpha, \alpha_2, \dots, \alpha_n$ je ortonormálna báza celého priestoru a teda matica A je ortonormálne podobná s blokovo-diagonálnou maticou pozostávajúcou z dvoch blokov: prvý blok (ľavý horný blok) je matica 1×1 obsahujúci prvok 0 a druhý (pravý dolný) je matica B zodpovedajúca transformácii A' pri báze $\alpha_2, \dots, \alpha_n$ (a teda B je kososymetrická typu $(n-1) \times (n-1)$). To znamená, že matica B sa dá podľa indukčného predpokladu previesť ortogonálnou podobnosťou do požadovaného tvaru. Odtiaľ vyplýva, že aj matica A sa dá previesť do požadovaného tvaru. (Príslušnú maticu prechodu nájdeme podobne ako vo vete 1.4.12.)

Ešte musíme dokázať, čo sa stane, ak uvažujeme o nenulových vlastných číslach. Označme teraz $a = a_1$. Nech α je taký (reálny) vektor, že $\alpha(A^2 + aI) = \mathbf{0}$ (taký vektor existuje, lebo podľa vety o rozklade modulov vieme celý náš priestor rozložiť na priamy súčet cyklických podpriestorov $V^\perp = [e_0] \oplus [e_1] \oplus \dots \oplus [e_l]$ tak, že rád$(e_i) = (x^2 + a_i)^{k_i}$ pre $i = 1, \dots, l$. Potom môžeme položiť $\alpha = e_1(A^2 + aI)^{k_1 - 1}$.) Nech naviac $\|\alpha\| = 1$. Potom $W = [\alpha, \alpha A]$ je dvojrozmerný podpriestor. Skutočne, keby bol vektor αA násobkom vektora α, koeficient by bolo vlastné číslo. Keďže je to reálne číslo, musela by to byť 0. Potom ale nemôže byť $\alpha(A^2 + aI) = \mathbf{0}$, lebo $a \neq 0$. Inak tiež $(\alpha, \alpha A) = (\alpha A, \alpha) = (\alpha, -\alpha A) = -(\alpha, \alpha A)$. (druhá rovnosť plynie z kososymetričnosti A) Preto $\alpha \perp \alpha A$ a teda vektory α a $\beta = \frac{\alpha A}{\|\alpha A\|}$ tvoria ortonormálu bázu priestoru W. Podpriestor W je invariantný vzhľadom na A, lebo $(\alpha A)A = -a\alpha$. Matica transformácie A zúženej na podpriestor W má v báze $\alpha,\ \beta$ tvar

$$\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix},$$

kde $b = \|\alpha A\|$. Minimálny a charakteristický polynóm tejto matice je $x^2 + b^2$ a je samozrejme totožný s polynómom $x^2 + a$. Odtiaľ dostaneme, že $b = \sqrt{a}$. Dokážeme, že $W^\perp$ je invariantný podpriestor. Nech $\gamma \in W^\perp$, t.j. $(\gamma, \alpha) =$

$0 = (\gamma, \alpha A)$. Potom $(\gamma A, \alpha) = (\gamma, -\alpha A) = -(\gamma, \alpha A) = 0$ a tiež $(\gamma A, \alpha A) = (\gamma, -\alpha A^2) = (\gamma, a\alpha) = a(\gamma, \alpha) = 0$. Teda $W^\perp$ je skutočne A-invariantný.

Teraz môžeme použiť indukčný predpoklad, že matica transformácie A zúženej na podpriestor $W^\perp$ má pri vhodnej ortogonálnej báze $\alpha_3, \ldots, \alpha_n$ blokovo diagonálny tvar s blokmi v požadovanom tvare. Potom na priestore $W \oplus W^\perp$ má pri (ortonormálnej!) báze $\alpha, \beta, \alpha_3, \ldots, \alpha_n$ blokovo diagonálny tvar ako je požadované. □

Nasledujúca veta o ortogonálnych transformáciách (maticiach) sa okrem iného dá použiť na klasifikáciu zhodných zobrazení v euklidovských priestoroch.

Veta 1.4.18 *Nech A je (reálna) ortogonálna matica. Potom existuje reálna blokovo diagonálna matica B s blokmi buď typu 1×1 obsahujúcimi ± 1, alebo typu 2×2 tvaru*

$$\begin{pmatrix} \cos(\alpha_k) & \sin(\alpha_k) \\ -\sin(\alpha_k) & \cos(\alpha_k) \end{pmatrix},$$

ktorá je s ňou ortogonálne podobná.

Dôkaz. Dôkaz urobíme podobne ako v predchádzajúcich prípadoch indukciou. Prvý krok indukcie je zahrnutý v indukčnom kroku.

Vieme, že vlastné čísla (nad poľom C) matice A sú komplexné čísla s absolútnou hodnotou 1. Teda reálne vlastné čísla ortogonálnej matice sú len ± 1. Ak je $a \in C$ komplexné vlastné číslo A, tak $a\overline{a} = 1$, teda $a = \cos(\alpha) + i\sin(\alpha)$ pre vhodné α a $(x-a)(x-\overline{a}) = x^2 - 2\cos(\alpha)x + 1$. Preto má charakteristický polynóm tvar $ch_A(x) = (x-1)^{k_1}(x+1)^{k_2}(x^2 - 2\cos(\alpha_3)x + 1)^{k_3} \ldots (x^2 - 2\cos(\alpha_l)x + 1)^{k_l}$ pre vhodné l. Pri dôkaze indukčného kroku musíme zvlášť rozobrať dva prípady: reálne vlastné číslo a komplexné (nie reálne) vlastné číslo.

Nech $a = \pm 1$. Nech y je reálny vlastný vektor A, ktorý má dĺžku 1 a $yA = \pm y$. Potom zrejme $V = [y]$ je A-invariantný podpriestor, matica transformácie určenej maticou A zúženej na V má tvar (a). Podpriestor $V^\perp$ je tiež A invariantný. Skutočne, nech $a \in V^\perp$, t.j. $(a, y) = 0$. Potom $(aA, y) = (aA, \frac{yA}{a}) = \pm(aA, yA) = \pm(aAA^T, y) = \pm(a, y) = 0$. Transformácia A zúžená na podpriestor $V^\perp$ je ortogonálna a preto matica tejto transformácie pri ľubovoľnej ortonormálnej báze je ortogonálna typu $(n-1)\times(n-1)$. Môžeme použiť indukčný predpoklad. Dokončite dôkaz.

Nech $x^2 - 2\cos(\alpha)x + 1$ je irebucibilný člen v charakteristickom polynóme $ch_A(x)$ (t.j. $ch_A(x) = (x^2 - 2\cos(\alpha)x + 1)^k g(x)$ pre vhodné číslo $k > 0$ a polynóm $g(x)$). Potom na základe rovnakých argumentov ako v predchádzajúcej vete existuje reálny vektor y taký, že

$$y(A^2 - 2\cos(\alpha)A + I) = \mathbf{0}.$$

Predpokladajme naviac, že y má dĺžku 1. Uvažujme o podpriestore $V = [y, yA]$. Priestor V je A-invariantný, lebo $(yA)A = 2\cos(\alpha)yA - y \in V$. Tento priestor je dvojrozmerný. Totiž ak $yA = by$ (ak je priestor jednorozmerný, je nutne yA násobkom y), potom nemôže byť splnená rovnosť $y(A^2 - 2\cos(\alpha)A + I) = \mathbf{0}$, lebo (podľa vety o jednoznačnom rozklade) žiadny reálny polynóm prvého stupňa (a teda ani $x - b$) nedelí polynóm $x^2 - 2\cos(\alpha)x - 1$. Uvažujme o transformácii A zúženej na podpriestor V — označme ju A'. Transformácia A' je ortogonálna a jej matica je pri ľubovoľnej ortonormálnej báze (podpriestoru V) ortogonálna. Takúto maticu budeme tiež označovať ako A'. Môžeme napísať, že $A' = B + C$, kde B je symetrická a C je kososymetrická (obidve sú samozrejme 2×2). Potom v podpriestore V existuje ortonormálna báza y_1, y_2 taká, pri ktorej má transformácia určená symetrickou maticou B maticu tvaru $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Kosometrická matica C má pri báze y_1, y_2 tvar $\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}$ (kososymetrická transformácia na 2-rozmernom priestore má pri každej ortormálnej báze maticu takéhoto tvaru!). Teda matica A' je ortogonálne podobná s maticou $A'' = \begin{pmatrix} a & c \\ -c & b \end{pmatrix}$. Charakteristický polynóm tejto matice je $(x-a)(x-b) + c^2$, ale zároveň je rovný polynómu $x^2 - 2\cos(\alpha)x + 1$. Z ortogonality matice A'' dostaneme, že $a(-c) + bc = 0$, odkiaľ je $a = b$ ($c = 0$ by totiž dalo, že $(x-a)(x-b)$ je charakteristický polynóm A'' — teda A'' má reálne vlastné čísla, čo nie je pravda). Z rovnice $x^2 - 2\cos(\alpha)x + 1 = x^2 - 2ax + (a^2 + c^2)$ dostaneme, že $a = \cos(\alpha)$ a $a^2 + c^2 = 1$, teda $c = \sin(\alpha)$. To znamená, že matica A'' má tvar požadovaný znením vety.

Ešte dokážeme, že $V^\perp$ je A-invariantný. Najprv si uvedomme, že $V = [y_1, y_2] = [y_1A, y_2A]$. Nech teraz $y \in V^\perp$, t.j. $(y, y_1) = (y, y_2) = 0$. Potom $(yA, y_1A) = (yAA^T, y_1) = (y, y_1) = 0$. Podobne aj $(yA, y_2A) = 0$ a teda vektor yA je kolmý na obidva bázové vektory podpriestoru V a preto $yA \in V^\perp$. Teda $V^\perp$ je naozaj A-invariantný. Zvyšok plynie z indukčného predpokladu. □

Kapitola 2

Sylowove vety, nilpotentné a riešiteľné grupy

2.1 Úvodné vety

Veta 2.1.1 *Pre konečné komutatívne grupy platí obrátenie Lagrangeovej vety, t.j. ak $n = |G|$ a $d|n$, potom existuje podgrupa H grupy G, ktorá má d prvkov.*

Dôkaz. Tvrdenie triviálne platí pre konečné cyklické grupy. Ak grupa G nie je cyklická, podľa vety o rozklade modulov aplikovanej na konečné komutatívne grupy vieme, že $G = Z_{n_1} \times \ldots \times Z_{n_k}$ a keď $d|n = n_1 \ldots n_k$, vieme napísať $d = a_1 \ldots a_k$ tak, že $a_i|n_i$ pre $i = 1, \ldots, k$. Potom v cyklickej grupe Z_{n_i} vyberieme podgrupu H_i, ktorá má a_i prvkov. Podgrupa $H = H_1 \times \cdots \times H_k$ má potom d prvkov, ako požaduje veta. □

Ako ukazuje nasledovný príklad, uvedené tvrdenie pre nekomutatívne grupy neplatí (neskôr uvidíme, že toto je najmenší možný príklad, t.j. predošlá veta platí pre všetky grupy - aj nekomutatívne - ktoré majú menej ako 12 prvkov) **Príklad.** Nájdime všetky podgrupy grupy A_4 (je to grupa všetkých párnych permutácií na štvorprvkovej množine).

Najprv si napíšme

$$\begin{aligned} A_4 \quad = \quad & \{(), \sigma_1 = (12)(34), \sigma_2 = (13)(24), \sigma_3 = (14)(23), \tau_1 = (123), \\ & \tau_2 = (124), \tau_3 = (134), \tau_4 = (132), \tau_5 = (142), \tau_6 = (143), \\ & \tau_7 = (213), \tau_8 = (231)\} \end{aligned}$$

Nebudeme sa zaoberať triviálnymi podgrupami. Dvojprvkové podgrupy sú generované prvkami $\sigma_1, \sigma_2, \sigma_3$, t.j. $[\sigma_1]$, $[\sigma_2]$, $[\sigma_3]$.

Trojprvkové podgrupy sú generované prvkami typu τ_i a sú štyri. (Sú totiž cyklické a teda musia byť generované prvkami rádu 3).

Štvorprvková grupa je jedna: $\{(), \sigma_1, \sigma_2, \sigma_3\}$. (Môžu do nej totiž patriť len prvky rádu 1 a 2 a tieto sú práve štyri a tvoria podgrupu.)

A_4 nemá šesťprvkovú podgrupu. Ak by mala a táto by sa volala H, tak H ako podgrupa indexu 2 v A_4 je normálna podgrupa. Teda existuje homomorfizmus φ: $A_4 \to Z_2$ taký, že $\mathrm{Ker}\,\varphi = H$.

Ďalej, ak g je ľubovoľný prvok z grupy G a φ: $G \to G_1$ ľubovoľný homomorfizmus, potom $\mathrm{rad}(\varphi(g))$ (ako prvok v G_1) delí $\mathrm{rad}(g)$ (ako prvok v G). Preto $\mathrm{rad}(\varphi(\tau_i))$ delí 3, ale keďže je to rád prvku v Z_2, musí to byť buď 1 alebo 2. Čiže $\mathrm{rad}(\varphi(\tau_i)) = 1$ a teda $\tau_i \in \mathrm{Ker}\,\varphi$. T.j. $\mathrm{Ker}\,\varphi$ má aspoň 8 prvkov, čo je spor.

Teda šesťprvková podgrupa skutočne neexistuje.

Definícia 2.1.2 *Nech M je neprázdna množina, $(G, \circ)$ je grupa. Akciou grupy G na M nazveme ľubovoľné "párovanie" α: $M \times G \to M$ také, že*

pre všetky $m \in M$ je $\alpha(m, e) = m$ (e je neutrálny prvok G)

pre všetky $m \in M$, $g_1, g_2 \in G$ je $\alpha(\alpha(m, g_1), g_2) = \alpha(m, g_1 \circ g_2)$ (prvý typ)

alebo

pre všetky $m \in M$ je $\alpha(m, e) = e$ (e je neutrálny prvok G)

pre všetky $m \in M$, $g_1, g_2 \in G$ je $\alpha(\alpha(m, g_1), g_2) = \alpha(m, g_2 \circ g_1)$ (druhý typ)

Ak bude jasné, o akú akciu (a grupu) sa jedná, uvedené vzťahy písať aj ako $me = m$ a $(mg_1)g_2 = m(g_1g_2)$.

Príklad. Nech G je grupa. Nech $M = G$, nech $\alpha_1(a, g) = gag^{-1}$ (v tomto prípade tiež budeme písať a^g, t.j. $a^g = gag^{-1}$).

Nech M je množina všetkých (neprázdnych) podmnožín množiny G, nech $X \subseteq G$, nech H je podgrupa grupy G. Položme $\alpha_H(X, h) = \{x^h;\ x \in X\}$ (aj tu budeme písať X^h).

Ľahko sa dá overiť, že obe uvedené párovania sú akcie (druhého typu) G na príslušnej množine.

Definícia 2.1.3 *Hovoríme, že $S_\alpha(m) = \{g \in G;\ \alpha(m, g) = m\}$ je stabilizátor prvku m v akcii α: $M \times G \to M$.*

Lema 2.1.4 *Stabilizátor ľubovoľného prvku $m \in M$ v akcii α je podgrupa grupy G.*

Dôkaz. Keďže $me = m$, je $e \in S_\alpha(m)$. Nech $g, h \in S_\alpha(m)$. Potom $m(gh) = (mg)h = mh = m$ a teda $gh \in S_\alpha(m)$.

(pre druhý typ: $m(gh) = (mh)g = mg = m$ a teda $gh \in S_\alpha(m)$) Nech $g \in S_\alpha(m)$. Potom $mg^{-1} = (mg)g^{-1} = m(gg^{-1}) = me = m$, t.j. $g^{-1} \in S_\alpha(m)$. Preto $S_\alpha(m)$ je podgrupa.

(pre druhý typ: $mg^{-1} = (mg)g^{-1} = m(g^{-1}g) = me = m$) □

Definícia 2.1.5 *Nech α: $M \times G \to M$ je akcia. Nech $m \in M$. Orbitou bodu m v akcii α nazveme množinu $O_\alpha(m) = \{n \in M;\ (\exists g \in G)\, mg = n\}$*

Lema 2.1.6 *Nech α: $M \times G \to M$ je akcia. Potom $|O_\alpha(m)| = [G : S_\alpha(m)]$, špeciálne $|O_\alpha(m)|$ delí $|G|$.*

Dôkaz. Nech $y_1, y_2 \in O_\alpha(m)$. T.j. existujú $g_1, g_2 \in G$ také, že $mg_1 = y_1$ a $mg_2 = y_2$. Čo nám zaručí vlastnosť $y_1 = y_2$?

$$\begin{aligned} mg_1 = mg_2 &\Leftrightarrow mg_1g_1^{-1} = mg_2g_1^{-1} \\ &\Leftrightarrow m = me = mg_2g_1^{-1} \\ &\Leftrightarrow g_2g_1^{-1} \in S_\alpha(m) \end{aligned}$$

t.j. g_1, g_2 patria do jednej triedy rozkladu podľa podgrupy $S_\alpha(m)$. Preto je prvkov množiny $O_\alpha(m)$ rovnako veľa ako je týchto tried, t.j. $|O_\alpha(m)| = [G : S_\alpha(m)]$. Dôkaz pre druhý typ akcie je v podstate rovnaký, spravte ako cvičenie. □

Lema 2.1.7 *Nech α: $M \times G \to M$ je akcia. Systém $\{O_\alpha(m);\ m \in M\}$ je rozklad M.*

Dôkaz. cvičenie □

Definícia 2.1.8 *Nech G je grupa. Nech $a, b \in G$. Hovoríme, že a, b sú konjugované prvky, ak $a \in O_{\alpha_G}(b)$, t.j. ak existuje $g \in G$ také, že $a = b^g$. Relácia „byť konjugované“ je zrejme ekvivalencia.*

Nech $g \in G$. Zobrazenie φ_g: $G \to G$ definované vzorcom $a\varphi_g = a^g$ sa nazýva konjugácia alebo vnútorný automorfizmus.

Lema 2.1.9 *Nech G je grupa, potom každá konjugácia je automorfizmus grupy G, t.j. bijektívny izomorfizmus. Množina $Inn(G) = \{\varphi_g;\ g \in G\}$ s operáciou skladania zobrazení je grupa.*
Zobrazenie ψ: $G \to Inn(G)$ definované vzťahom $g\psi = \varphi_g$ je (anti)homomorfizmus.

Dôkaz. Bijektívnosť konjugácie φ_g plynie z toho, že $\varphi_{g^{-1}}$ je jej obojstranný inverzný prvok. Ostatné je ľahké. □

Definícia 2.1.10 *Nech K, H sú podgrupy grupy G, $g \in G$. Hovoríme, že množina*

$$KgH = \{kgh;\ k \in K \quad \& \quad h \in H\}$$

je trieda rozkladu grupy G podľa dvojného modulu K, H.

Lema 2.1.11 *Nech K, H sú podgrupy grupy G. Množina $\{KgH;\ g \in G\}$ je rozklad grupy G.*

Dôkaz. Keďže pre neutrálny prvok e grupy G platí, že $e \in K, H$, je $\bigcup_{g\in G} KgH = G$.
Nech $a \in Kg_1H \cap Kg_2H$. Potom existujú k_1, h_1, k_2, h_2 v K a H také, že

$$a = k_1g_1h_1 = k_2g_2h_2.$$

Potom ale

$$g_2 = k_2^{-1}k_1g_1h_1h_2^{-1} \in Kg_1H$$

a preto $Kg_2H \subseteq Kg_1H$. Zo symetrie úlohy už plynie, že $Kg_1H = Kg_2H$. □

Trieda KgH rozkladu podľa dvojného modulu K, H obsahuje sama istý počet (ľavých) tried rozkladu podľa podgrupy H a istý počet (pravých) tried rozkladu podľa podgrupy K. Tieto počty sú zaujímavé, zistime si ich. Začneme s ľavými triedami podľa H.
Zvoľme $M = \{kgH;\, k \in K\}$ - triedu ľavých tried rozkladu podľa H v množine KgH. Zvoľme α: $M \times K \to M$,

$$\alpha(kgH, k_1) = k_1(kgH) = (k_1k)gH$$

Zrejme α je akcia grupy K na množine M. Potom ale počet hľadaných ľavých tried bude

$$|O_\alpha(gH)| = [K : S_\alpha(gH)]$$

Takže treba zistiť, čo bude $S_\alpha(gH)$.
Predovšetkým, $S_\alpha(gH) \subseteq K$. Nech teda $k \in K$. $k \in S_\alpha(gH)$ je práve vtedy, keď $kgH = gH$, čo je práve vtedy, keď $g^{-1}kg \in H$ alebo tiež $k \in gHg^{-1}$. Dostávame teda, že $S_\alpha(gH) = K \cap gHg^{-1}$. Teda hľadaný počet ľavých tried je $[K : K \cap gHg^{-1}]$ tiež (vďaka vete 2.1.9) $[g^{-1}Kg : g^{-1}Kg \cap H]$.
Pre pravé triedy odvodíme vzorce podobným spôsobom. Dostávame vetu:

Veta 2.1.12 *Nech K, H sú podgrupy grupy G, $g \in G$. Potom počet ľavých tried rozkladu podľa podgrupy H v množine KgH je $[K : K \cap gHg^{-1}]$ alebo tiež $[g^{-1}Kg : g^{-1}Kg \cap H]$.*
Počet pravých tried rozkladu podľa podgrupy K v množine KgH je $[g^{-1}Hg : K \cap gHg^{-1}]$ alebo tiež $[H : g^{-1}Kg \cap H]$.

Definícia 2.1.13 *Nech G je grupa, $X \subseteq G$. Množina $C_G(X) = \{z \in G;\, (\forall x \in X)\, zx = xz\}$ sa nazýva centralizátor množiny X v grupe G. Špeciálne sa používa ešte $Z(G) = C_G(G)$ a nazýva sa centrum grupy.*
Nech naviac H je podgprupa G. Množina $N_{G,H}(X) = \{h \in H;\, X^h = X\}$ sa nazýva normalizátor množiny X v grupe H. Špeciálne kladieme $N_G(X) = N_{G,G}(X)$ (Pre $X \subseteq G$, samozrejme.)

Ak $X = \{x\}$ je jednoprvková množina, potom $C_G(X) = \{z \in G;\, x^z = x\}$, t.j. $C_G(X)$ je stabilizátor prvku x v akcii α_1 a preto je to podgrupa. Platí tiež, že $C_G(\{x\}) = N_G(\{x\})$. (Pre jednoprvkové množiny budeme používať aj skrátený zápis $C_G(x), N_{G,H}(x), N_G(x)$).
Podobne je vidieť, že $N_{G,H}(X)$ je stabilizátor množiny X v akcii α_H a teda aj toto je podgrupa G (teraz už X je ľubovoľná podmnožina, samozrejme).
Keďže $C_G(X) = \bigcap\{C_G(\{x\});\, x \in X\}$ je prienik podgrúp, je to tiež podgrupa. Je hneď vidieť, že centrum grupy je dokonca invariantná podgrupa.
Dokázali sme tvrdenie

Lema 2.1.14 *Centralizátor a normalizátor ľubovoľnej podmnožiny je podgrupa danej grupy. Centrum grupy je normálna podgrupa danej grupy.*

Nech H je podgrupa G, $g \in G$. Koľko prvkov má množina $O_{\alpha_H}(g)$? V tomto prípade je $S_{\alpha_H}(g) = N_{G,H}(g)$ a preto vieme, že je to

$$|O_{\alpha_H}(g)| = [H : N_{G,H}(g)].$$

Špeciálne pre $H = G$ je $|O_{\alpha_G}(g)| = [H : N_G(g)]$ a keďže je $N_G(g) = C_G(g)$ dostávame nasledovné tvrdenie:

Lema 2.1.15 *Nech $g \in G$. Potom $|O_{\alpha_G}(g)| = 1$ práve vtedy, keď $g \in Z(G)$.*

Dôkaz. Totiž $|O_{\alpha_G}(g)| = 1$ práve vtedy, keď $[G : N_G(g)] = 1$, čo je práve vtedy, keď $N_G(g) = C_G(g) = G$ a to je práve vtedy, keď $g \in Z(G)$. □

2.2 Sylowove vety

Veta 2.2.1 *[Cauchy] Nech G je grupa, p nech je prvočíslo. Nech $p/|G|$. Potom existuje podgrupa H grupy G, ktorá má práve p prvkov.*

Dôkaz. Nech $|G| = pm$. Dôkaz urobíme indukciou podľa m. Pre $m = 1$ zrejme stačí položiť $H = G$.
Nech $m > 1$. Nech α_1 je akcia z príkladu, namiesto $O_{\alpha_1}(x)$ budeme písať len $O(x)$. Potom vieme, že

$$G = \underbrace{O(e) + O(g_1) + \cdots + O(g_k)}_{\text{majú po 1 prvku}} + \underbrace{O(g_{k+1}) + \cdots + O(g_l)}_{\text{majú po viac ako 1 prvku}}$$

(Znamienko + použité v predošlom zápise znamená disjunktné množinové zjednotenie, vieme, že uvedené množiny tvoria rozklad a z každej triedy sme vybrali jedného reprezentanta: e,$g_1, \ldots, g_l$. Je to zaužívaná konvencia, ktorú budeme aj naďalej používať.) Prvky e $(= g_0)$,$g_1, \ldots, g_l$ sú jednoducho tak zvolené, aby platilo, to čo je o nich pod svorkami napísané. Skupina $O(g_{k+1}) + \cdots + O(g_l)$ môže byť prázdna.

Nech je teraz $i > 0$ a g_{k+i} nech je také, že p nedelí $|O(g_{k+1})|$. Kedže $|O(g_{k+1})| = [G : N_G(g_{k+1})]$, znamená to, že p delí $|N_G(g_{k+1})|$, ale pretože $|O(g_{k+1})| \geq 2$, je $N_G(g_{k+1})$ vlastná podgrupa grupy G. Podľa indukčného predpokladu teda $N_G(g_{k+1})$ obsahuje podgrupu H s p prvkami. H je samozrejme podgrupa G, takže v tomto prípade tvrdenie platí.

Nech teda buď je druhá časť prázdna, alebo pre každé $i > 0$ platí, že p delí $|O(g_{k+1})|$. Pretože p delí počet prvkov ľavej strany (číslo $|G|$) a delí počet prvkov v každej množine druhej skupiny, musí deliť aj súčet prvkov v množinách prvej skupiny. Tieto sčítance sú len jednotky, t.j. p delí počet množín patriacich do prvej skupiny.

Ovšem $|O(g_i)| = 1$ práve vtedy, keď $g_i \in Z(G)$ a preto $Z(G) = \{g_0, g_1, \ldots, g_k\}$. Teda p delí $|Z(G)|$. Naviac $Z(G)$ je komutatívna grupa. Podľa vety 2.1.1 $Z(G)$ obsahuje podgrupu H s p prvkami. Táto podgrupa je samozrejme aj podgrupou grupy G. □

Analýzou druhej časti dôkazu dostaneme aj nasledujúce tvrdenie

Dôsledok 2.2.2 *Nech G je taká grupa, že existuje prvočíslo p s vlastnosťami:*
a) $p/|G|$, b) pre každú vlastnú podgrupu H p delí číslo $[G : H]$.
Potom $Z(G)$ je netriviálna podgrupa grupy G.

Dôkaz. Stačí si uvedomiť, že za uvedených predpokladov pre takto určené prvočíslo p platí, že počet prvkov v druhej skupine množín v predošlom dôkaze je deliteľný p... □

Poznámka. Vďaka Lagrangeovej vete vieme, že predpoklady predošlého dôsledku spĺňa napríklad každá grupa s p^k prvkami, p prvočíslo.

Veta 2.2.3 *[Prvá Sylowova veta] Nech $(G, \circ)$ je grupa, $|G| = p^k \cdot m$, p je prvočíslo, p, m sú nesúdeliteľné. Potom*

(a) pre každé $1 \leq l \leq k$ existuje podgrupa H grupy G taká, že $|H| = p^l$ a

(b) ak $1 \leq l < k$, potom každá podgrupa H grupy G s počtom prvkov p^l je normálna podgrupa nejakej podgrupy H' s počtom prvkov p^{l+1}.

Dôkaz. Vďaka Cauchyho vete vidíme, že stačí dokázať trvdenie (b). Tento dôkaz urobíme indukciou. Dôkaz indukcie pre $l = 1$ je zahrnutý v dôkaze indukčného kroku, takže sa sústredíme na dôkaz indukčného kroku.

Nech je H podgrupa grupy G, $|H| = p^l$, $l < k$. Urobme rozklad G podľa dvojného modulu (H, H), t.j.

$$G = HeH + Ha_1H + \cdots + Ha_iH + Ha_{i+1}H + \cdots + Ha_mH$$

Položme $a_0 = e$. Počet ľavých tried rozkladu G podľa H označme b (t.j. $b = [G : H]$), počet ľavých tried rozkladu dvojnej triedy Ha_jH podľa H označme $b_j = [H : H \cap a_jHa_j^{-1}]$, teda každé b_j je mocninou p. Keďže $l < k$, tak $p|b$. Bez újmy na všeobecnosti môžeme predpokladať, že prvky b_0,$b_1, \ldots, b_k$ sú také, že $p \nmid b_0, \ldots, p \nmid b_i$ (t.j. $b_0 = b_1 = \cdots = b_i = 1$) a $p|b_{i+1}, \ldots, p|b_m$ - určite $b_0 = 1$, a keďže $p|b$, je $i \geq 1$. Tiež vidíme, že $p|b_0 + b_1 + \cdots + b_i$.

Teraz ukážeme, že $N_G(H) = HeH + Ha_1H + \cdots + Ha_iH$. Ak $x \in Ha_jH$, tak $b_j = [H : H \cap a_jHa_j^{-1}] = [H : H \cap xHx^{-1}]$, lebo $\{HyH,\ y \in G\}$ je rozklad, preto $Ha_jH = HxH$ a b_j je počet tried rozkladu v Ha_jH (a teda aj HxH) podľa H. Keďže je tu $b_j = [H : H \cap xHx^{-1}] = 1$ a $H \cap xHx^{-1} \subseteq H$, musí byť $xHx^{-1} = H$ a teda prvok $x \in N_G(H)$. Podobne, ak $x \in N_G(H)$, tak $xHx^{-1} = H$, preto $[H : H \cap xHx^{-1}] = 1$ a teda $x \in Ha_uH$ pre vhodné $u \leq i$ (opäť vďaka tomu, že $HeH + Ha_1H + \cdots + Ha_iH + Ha_{i+1}H + \cdots + Ha_mH$ je rozklad). Preto $x \in HeH + Ha_1H + \cdots + Ha_iH$.

Pretože $i \geq 1$, je H vlastnou podgrupou $N_G(H)$, a samozrejme je to normálna podgrupa $N_G(H)$. Označme $J = N_G(H)$. Keďže $p|b_0 + b_1 + \cdots + b_i$ a $N_G(H) = HeH + Ha_1H + \cdots + Ha_iH$, platí $p^{l+1}| \, |J|$.

Preto faktorová grupa J/H má počet prvkov deliteľný číslom p a podľa Cauchyho vety má p prvkovú podgrupu, nech je to J'. Potom ak $\psi : J \to J/H$ je kanonický faktorový homomorfizmus, potom $H' = \psi^{-1}(J')$ je podgrupa $J = N_G(H)$ - preto je H normálna v H' a počet prvkov H' je p^{l+1}. Teda H' je grupa požadovaná časťou (b) tvrdenia vety. □

Definícia 2.2.4 *Nech p je prvočíslo. Grupa G sa nazýva $p-$grupa, ak rád každého prvku v grupe G je mocnina čísla p.*

Z Cauchyho vety je hneď vidieť, že konečná grupa G je $p-$grupa práve vtedy, keď počet prvkov G je mocnina p.

Definícia 2.2.5 *Nech p je prvočíslo, grupa G je taká, že $|G| = p^n \cdot m$, $(p, m) = 1$. Podgrupa H grupy G sa nazýva Sylowova $p-$podgrupa grupy G, ak $|H| = p^n$.*

Podgrupa H grupy G sa nazýva Sylowova podgrupa grupy G, ak existuje prvočíslo p také, že $p| \, |G|$ a H je Sylowova $p-$podgrupa grupy G.

Vďaka prvej Sylowovej vete vieme, že pre konečnú grupu G a každé prvočíslo p, ktoré delí počet prvkov grupy G existuje Sylowova $p-$podgrupa grupy G.

Veta 2.2.6 *[Druhá Sylowova veta] Nech S_1 a S_2 sú dve Sylowove $p-$podgrupy grupy G. Potom existuje $g \in G$ také, že $S_1 = gS_2g^{-1}$.*

Dôkaz. Urobme rozklad

$$G = S_1eS_2 + S_1a_1S_2 + \cdots + S_1a_nS_2$$

podľa dvojného modulu S_1, S_2, nech $a_0 = e$, b je počet tried rozkladu G podľa S_2, b_i je počet tried rozkladu $S_1a_iS_2$ podľa S_2. Keďže počet prvkov S_1 aj S_2 je mocnina prvočísla p, podľa vzorca pre počet tried rozkladu vieme, že každé b_i je mocnina p.

Tiež vieme, že p nedelí číslo b. Preto musí existovať j také, že p nedelí b_j a to znamená, že $b_j = 1$. Teda $1 = [S_1 : S_1 \cap a_jS_2a_j^{-1}]$, čo znamená, že $S_1 \cap a_jS_2a_j^{-1} = S_1$ a teda $S_1 = a_jS_2a_j^{-1}$, lebo počet prvkov S_2 a $a_jS_2a_j^{-1}$ je rovnaký ($\varphi : G \to G$, $x\varphi = a_jxa_j^{-1}$ je izomorfizmus). □

Nasledujúce tvrdenie nám poslúži v dôkaze ďalšej vety.

Lema 2.2.7 *Nech G je grupa, p je prvočíslo také, že $p| \, |G|$, H je Sylowova $p-$podgrupa. Potom H je jediná Sylowova $p-$podgrupa grupy G, ktorá je (celá) obsiahnutá v $N_G(H)$.*

Dôkaz. Predovšetkým, $H \subseteq N_G(H)$. Nech P je tiež Sylowova $p-$podgrupa grupy G. Ak je $P \subseteq N_G(H)$, tak P je tiež Sylowova podgrupa grupy $N_G(H)$, t.j. H aj P sú Sylowove $p-$podgrupy grupy $N_G(H)$ a preto sú podľa druhej sylowovej vety konjugované v $N_G(H)$, t.j. existuje $g \in N_G(H)$ také, že $P = gHg^{-1}$. Samozrejme, význam grupy $N_G(H)$ je taký, že ak $g \in N_G(H)$, tak, že $gHg^{-1} = H$. Teda ak $P \subseteq N_G(H)$, tak $P = H$. □

Veta 2.2.8 *[Tretia Sylowova veta] Nech G je grupa a p je také prvočíslo, že $p| \, |G|$. Ak označíme t počet Sylowových $p-$podgrúp grupy G, tak platí*

a) $t| \, |G|$

b) $t = 1 + k \cdot p$ pre vhodné k (t.j. $t \equiv 1 \mod p$)

Dôkaz. Ak zvolíme jednu Sylowovu $p-$podgrupu, napr. P, tak podľa druhej Sylowovej vety všetky Sylowove $p-$podgrupy tvoria orbitu $O_{\alpha_G}(P)$, kde α_G je akcia z druhej časti príkladu uvedeného za definíciou 2.1.2. Teda $t = |O_{\alpha_G}(P)|$. Pre počet prvkov orbity platí vzorec

$$|O_{\alpha_G}(P)| = [G : S_{\alpha_G}(P)]$$

Vďaka tomu platí časť a) našej vety.

Vyberme teraz jednu Sylowovu $p-$podgrupu, označme ju T.
Nech $M = \{H; H \text{ je Sylowova } p-\text{podgrupa grupy } G\} \setminus \{T\}$.

Na množine M zadefinujme akciu grupy T, $\alpha_T : M \times T \to M$ nasledovne:

$$\alpha_T(S, g) = gSg^{-1}.$$

Zrejme je to akcia. Rozdeľme M na orbity podľa tejto akcie,

$$M = O_{\alpha_T}(S_1) + \cdots + O_{\alpha_T}(S_n).$$

O počte prvkov jednotlivých orbít vieme: $|O_{\alpha_T}(S_i)| = [T : S_{\alpha_T}(S_i)]$. Preto každé z týchto čísel je mocnina p. Dôležité je, že žiadne z nich nie je 1. Fakt, že $|O_{\alpha_T}(S_i)| = 1$ totiž znamená, že pre každé $g \in T$ platí, že $S_i = gS_ig^{-1}$. Toto znamená, že $T \subseteq N_G(S_i)$ a teda T aj S_i sú Sylowove $p-$podgroupy grupy $N_G(S_i)$, čo podľa poslednej lemy znamená, že $T = S_i$. To ale nie je možné, lebo $T \notin M$.

To znamená, že

$$|M| = p^{a_1} + \cdots + p^{a_n}$$

a $a_1 > 0, \ldots a_n > 0$. Preto $p \,|\, |M|$. Počet všetkých Sylowových $p-$podgrúp je $|M| + 1$ a teda platí časť b) vety. □

Nasledujúce tvrdenie hovorí o istom dôležitom vzťahu medzi podgrupou a jej normalizátorovi. Tento vzťah použijeme v dôkaze nasledujúcej vety.

Veta 2.2.9 *Nech G je grupa, P jej Sylowova podgrupa a H je taká podgrupa, že $N_G(P) \subseteq H \subseteq G$. Potom $N_G(H) = H$.*

Dôkaz. Nech $a \in G$, $aHa^{-1} = H$. Keďže $P \subseteq N_G(P) \subseteq H$, je $aPa^{-1} \subseteq H$ a samozrejme, aj P aj $P_1 = aPa^{-1}$ sú Sylowove podgrupy grupy H (pre to isté prvočíslo p). Podľa druhej sylowovej vety existuje v H prvok h taký, že $hP_1h^{-1} = P$ a teda $haPa^{-1}h^{-1} = P$. Preto $ha \in N_G(P)$ a pretože $N_G(P) \subseteq H$, je $ha \in H$. Keďže $h \in H$, je aj $a \in H$. Preto $N_G(H) \subseteq H$. □

Ešte uvedieme dve pomocné tvrdenia

Lema 2.2.10 *Grupa G sa dá zapísať ako priamy súčin dvoch grúp práve vtedy, ak existujú podgrupy A, B také, že*

(a) A, B sú normálne v G

(b) $[A \cup B] = G$

(c) $A \cap B = \{e\}$, kde e je neutrálny prvok v G

Dôkaz. Zrejme ak $G = S \times T$, e_1 je neutrálny prvok S a e_2 je neutrálny prvok T tak ak položíme $A = S \times \{e_2\}$ a $B = \{e_1\} \times T$, podgrupy A a B budú vyhovovať podmienkam lemy.

Nech A a B vyhovujú podmienkam (a)-(c). Nech $a \in A$, $b \in B$. Dokážeme, že $ab = ba$. Pozrime sa na výraz $aba^{-1}b^{-1}$. aba^{-1} je konjugát prvku z B a keďže B je normálna, je $aba^{-1} \in B$ a preto $(aba^{-1})b^{-1} \in B$. Podobne $ba^{-1}b^{-1}$ ako konjugát prvku z A je prvok A a preto $a(ba^{-1}b^{-1}) \in A$. Podľa podmienky (c) teda $aba^{-1}b^{-1} = e$ a preto $ab = ba$. Pozor, toto neznamená, že podgrupy A, B sú komutatívne. Čo vieme je len to, že ak zoberieme prvky z rôznych podgrúp, tak tie komutujú.

Vo všeobecnosti je prvok x z generovanej podgrupy $[A \cup B]$ v tvare

$$x = a_1b_1a_2b_2 \cdots a_nb_n$$

kde $a_i \in A$, $b_j \in B$. (a_1 alebo b_n môžu byť e). Vďaka práve dokázanej komutativite teda $x = a_1 \cdots a_nb_1 \cdots b_n = ab$, kde $a = a_1 \cdots a_n \in A$, $b = b_1 \cdots b_n \in B$. Podľa podmienky (b) každý prvok $x \in G$ vieme napísať ako $x = ab$, $a \in A$, $b \in B$.

Definujme teraz zobrazenie $\varphi : A \times B \to G$ predpisom $(a, b)\varphi = ab$. Toto zobrazenie je teda surjektívne.

Dokážeme jeho injektivitu: Nech $(a, b)\varphi = (a', b')\varphi$, t.j. $ab = a'b'$. Potom $a'^{-1}a = b'b^{-1}$. Samozrejme, $a'^{-1}a \in A$, $b'b^{-1} \in B$ a preto vďaka (c) $a'^{-1}a = e = b'b^{-1}$, t.j. $a = a'$, $b = b'$. Takže φ je bijekcia.

Dokážeme, že je to aj homomorfizmus:

$$((a, b)(a', b'))\varphi = (aa', bb')\varphi = aa'bb' = aba'b' = (a, b)\varphi(a', b')\varphi$$

Pri výpočte sme tiež použili komutativitu medzi prvkami z podgrúp A, B. Takže φ je homomorfizmus a preto je to izomorfizmus. □

Predošlé tvrdenie je možné ľahko rozšíriť na rozklad na konečne veľa činiteľov.

Lema 2.2.11 *Nech G je grupa, $a \in G$, $\mathrm{rad}(a) = mn$, kde $(m,n) = 1$. Potom existujú $x, y \in G$ také, že $a = xy$, $\mathrm{rad}(x) = m$, $\mathrm{rad}(y) = n$, $xy = yx$. Dvojica x, y je naviac týmito vlastnosťami určená jednoznačne a x, y sú mocninami prvku a. (T.j. pre každú podgrupu H platí: $a \in H \implies x, y \in H$.)*

Dôkaz. Keďže $(m,n) = 1$, existujú $s, t \in Z$ také, že $sm + nt = 1$, položme $x = a^{nt}$, $y = a^{sm}$. Potom $a = a^1 = a^{nt}a^{sm} = xy = a^{sm}a^{nt} = yx$.

Tiež $x^m = (a^{nt})^m = a^{ntm} = (a^{mn})^t = e^t = e$, t.j. $\mathrm{rad}(x) \mid m$. Ďalej $e = x^{\mathrm{rad}(x)} = (a^{nt})^{\mathrm{rad}(x)} = a^{nt \cdot \mathrm{rad}(x)}$. Preto $mn \mid nt \cdot \mathrm{rad}(x)$, čiže $m \mid t \cdot \mathrm{rad}(x)$. Rovnica $sm + nt = 1$ hovorí, že $(m,t) = 1$ a preto $m \mid \mathrm{rad}(x)$. Čiže $\mathrm{rad}(x) = m$.

Nech ešte u, v majú uvedené vlastnosti, t.j. $a = uv = vu$ a $\mathrm{rad}(u) = m$, $\mathrm{rad}(v) = n$. Potom $au = (uv)u = u(vu) = ua$, podobne $av = (vu)v = v(uv) = va$. Keďže x, y sú mocniny a, znamená to, že aj $xu = ux$, $xv = vx$, $yu = uy$, $yv = vy$ a tiež $xu^{-1} = u^{-1}x$,...

Teda ak $xy = uv$, tak $u^{-1}x = vy^{-1}$. Keďže x, u^{-1} komutujú a ich rád je m, vieme, že $(u^{-1}x)^m = e$ a preto $\mathrm{rad}(u^{-1}x) \mid m$. Podobne $\mathrm{rad}(vy^{-1}) \mid n$. Takže ten istý prvok má na jednej strane rád, ktorý delí číslo m a na druhej strane rád, ktorý delí číslo n. Keďže $(m,n) = 1$, musí byť tento rád číslo 1, ale jediný prvok rádu 1 je e. Teda $xu^{-1} = e = u^{-1}x$. Čiže $x = u$, $v = y$, čo dokazuje jednoznačnosť uvedených prvkov x a y. □

Táto lema sa dá ľahko indukciou rozšíriť na nasledujúcu lemu.

Dôsledok 2.2.12 *Nech G je grupa, $a \in G$, $\mathrm{rad}(a) = m_1 m_2 \dots m_n$, kde m_i, m_j sú po dvoch nesúdeliteľné. Potom existujú $x_1, x_2, \dots, x_n \in G$ také, že $a = x_1 x_2 \cdots x_n$, $\mathrm{rad}(x_i) = m_i$, $x_i x_j = x_j x_i$. N-tica $x_1, \dots, x_n$ je naviac týmito vlastnosťami určená jednoznačne a $x_1, x_2, \dots, x_n$ sú mocninami prvku a. (T.j. pre každú podgrupu H platí: $a \in H \implies x_1, x_2, \dots, x_n \in H$.)*

Dôkaz. □

Veta 2.2.13 *Nech G je konečná grupa. Nasledujúce podmienky sú ekvivalentné:*

(a) Ak $H \subsetneq G$ je podgrupa, tak $H \neq N_G(H)$

(b) Pre každé prvočíslo p také, že $p \mid |G|$ existuje práve jedna Sylowova $p-$podgrupa

(c) G je priamy súčin svojich Sylowových podgrúp

Dôkaz. (a) $\implies$ (b): je dôsledok vety 2.2.9 a druhej sylowovej vety. Ak by totiž existovali dve Sylowove $p-$podgrupy - S, T, tieto sú konjugované v G a preto $N_G(S) \neq G$ a podľa vety 2.2.9 platí $N_G(N_G(S)) = N_G(S)$, čo je spor s (a).

(b) $\implies$ (c): Nech $|G| = p_1^{n_1} \cdots p_l^{n_l}$, kde p_i sú navzájom rôzne prvočísla, $P_1, \dots, P_l$ sú Sylowove podgrupy (podľa predpokladu jediné) prislúchajúce po rade prvočíslam $p_1, \dots, p_l$. Overíme predpoklady zovšeobecnia lemy o rozklade grupy na priamy súčin, čím dokážeme, že $G = P_1 \times \cdots \times P_l$. Keďže P_i je jediná Sylowova p_i-podgrupa, podľa druhej sylowovej vety musí byť normálna v G (v skutočnosti na to netreba druhú sylowovu vetu: ak H je jediná podgrupa grupy G s m prvkami, tak ju každý automorfizmus G musí (bijektívne, nie nutne identicky) zobraziť na podgrupu s m prvkami a teda na H. To znamená, že taká H je dokonca charakteristická podgrupa G).

Nech $x \in G$, potom $\mathrm{rad}(x) \mid |G|$, t.j. $\mathrm{rad}(x) = p_1^{a_1} \cdots p_l^{a_l}$, kde $a_1 \leq n_1, \dots, a_l \leq n_l$. Podľa dôsledku 2.2.12 existujú prvky $x_1, \dots, x_l$ také, že $x = x_1 \cdots x_l$, $\mathrm{rad}(x_i) = p^{a_i}$. Každý prvok rádu tvaru p^{a_i} musí byť prvok niektorej Sylowovej $p-$ podgrupy, t.j. $x_i \in P_i$, lebo P_i je jediná Sylowova $p-$ podgrupa. Preto $[P_1 \cup \cdots \cup P_l] = G$.

Nakoniec, ak $x \in P_i \cap P_j$ $(i \neq j)$, tak $\mathrm{rad}(x) \mid |P_i|$, $\mathrm{rad}(x) \mid |P_j|$. Keďže $p_i \neq p_j$, je $\mathrm{rad}(x) = 1$ a teda $x = e$. Preto $P_i \cap P_j = \{e\}$ (pre $i \neq j$).

(c) $\implies$ (a): Nech je teda

$$G = P_1' \times \cdots \times P_l',$$

kde $P_1', \dots, P_l'$ sú p_i-grupy. To znamená, že $|G| = p_1^{n_1} \cdots p_l^{n_l}$ pre vhodné exponenty $n_1, \dots, n_l$. Podľa zovšeobecnenia lemy 2.2.10 budeme pracovať s grupami P_i, ktoré sú izomorfné s P_i', sú invariantné v G, generujú G a $[P_1 \cup \cdots \cup P_i] \cap P_{i+1} = \{e\}$, teda $G = P_1 \cdots P_l$ a

$$\varphi : P_1' \times \cdots \times P_l' \to P_1 \times \cdots \times P_l$$

dané predpisom $\varphi(g_1, \dots, g_l) = g_1 \cdots g_l$ je izomorfizmus.

V prvom rade si treba uvedomiť, že p_i sú po dvoch rôzne, lebo inak $P_i' \times P_j'$ (t.j. $P_i \cdot P_j$) by bola p_i $(= p_j)$ podgrupa G, ktorá by bola väčšia ako ktorákoľvek z P_i, P_j a teda žiadna z P_i, P_j nie je Sylowova podgrupa.

Nech H je vlastná podgrupa grupy G, $x \in H$. Potom $\mathrm{rad}(x) = p_1^{a_1} \cdots p_l^{a_l}$ a podľa tvrdenia 2.2.12 je $x = g_1 \cdots g_l$, kde $g_1 \in P_1, \dots, g_l \in P_l$ (lebo každý prvok rádu p^a je prvok nejakej - a v našom prípade teda jedinej Sylowovej $p-$podgrupy) a naviac tieto prvky komutujú a sú mocniny x. Teda špeciálne, $(\forall i)\, g_i \in H$ a nakoniec $(\forall i)\, g_i \in P_i \cap H$.

To znamená, že $x \in (P_1 \cap H)\cdots(P_l \cap H)$, teda $H \subseteq (P_1 \cap H)\cdots(P_l \cap H)$. Inklúzia $(P_1 \cap H)\cdots(P_l \cap H) \subseteq H$ je splnená triválne a preto $H = (P_1 \cap H)\cdots(P_l \cap H)$.

Označme $H_i = P_i \cap H$. Keďže je $H \neq G$, existuje $H_i \neq P_i$. Podľa prvej Sylowovej vety existuje $H_i \subsetneq P \subset P_i$, v ktorej je H_i invariantná. Potom H je invariantná podgrupa v $H_1 \cdots H_{i-1}PH_{i+1}\ldots H_l$ a $H \subsetneq H_1 \cdots H_{i-1}PH_{i+1}\ldots H_l$. Tým sme dokázali podmienku z (a). □
Ešte dokážeme jednu zaujímavé tvrdenie týkajúce sa centra $p-$grupy.

Veta 2.2.14 *Nech G je konečná $p-$grupa (p je prvočíslo), H je invariantná podgrupa grupy G, $|H| = p$. Potom $H \subseteq Z(G)$.*

Dôkaz. Nech $e \neq a \in H$. Budeme pracovať s akciou konjugáciou na množine G, t.j. $\alpha : G \times G \to G$, $\alpha(g, x) = gxg^{-1}$. Vďaka tomu, že H je invariantná v G, je $O_\alpha(a) \subseteq H$. Keďže neneutrálny prvok nie je konjugovaný s neutrálnym, je $O_\alpha(a) \subsetneq H$, teda $|O_\alpha(a)| < p$.

Ale vieme, že $|O_\alpha(a)| = [G : S_\alpha(a)] = p^i$, lebo G je $p-$grupa. Jediná mocnina prvočísla p, ktorá je menšia ako p je $p^0 = 1$. Teda $|O_\alpha(a)| = 1$, respektíve $|S_\alpha(a)| = G$ a preto prvok a komutuje so všetkými prvkami v grupe G, t.j. je prvkom centra $Z(G)$. □

Dôsledok 2.2.15 *Grupa G, ktorá má p^2 prvkov (p prvočíslo) je komutatívna.*

Dôkaz. Nech G je grupa s p^2 prvkami. Nech $e \neq a \in G$. Potom buď $[a] = G$, t.j. G je cyklická a preto komutatívna, alebo $|[a]| = p$ a podľa prvej Sylowovej vety existuje podgrupa H grupy G, ktorá má p^{1+1} prvkov, v ktorej je $[a]$ invariantná. Samozrejme, v tomto prípade je $H = G$ a podľa poslednej vety je $[a] \subseteq Z(G)$, t.j. $a \in Z(G)$. Dokázali sme, že každý prvok $a \in G$ patrí do centra $Z(G)$ a preto je G komutatívna. □

2.3 Faktorizácia, charakteristické podgrupy

V tejto časti si ukážeme niekoľko vlastností faktorizácie grúp, zavedieme pojem zaujímavej triedy podgrúp a dokážeme dôležité tvrdenie o tejto triede.

Fakt, že H je normálna podgrupa grupy G sa zvyčajne zapisuje ako $H \triangleleft G$. Najprv jedno tvrdenie, ktoré hovorí o "modularite" medzi podgrupami:

Veta 2.3.1 *Ak A, B, H sú podgrupy grupy G, A je podgrupa B, H je normálna podgrupa G. Potom*

$$B \cap AH = A(B \cap H).$$

Dôkaz. Keďže je $H \triangleleft G$, je $AH = [A \cup H]$, takže dokazujeme vlastne rovnosť $B \cap [A \cup H] = A(B \cap H)$.
Očividne $A(B \cap H) \subseteq B \cap AH$, lebo $A \subseteq B$, $A \subseteq AH$, $B \cap H \subseteq B$, $B \cap H \subseteq AH$.
Naopak, nech $b = ah \in B \cap AH$ s tým, že $b \in B$, $a \in A$, $h \in H$. Potom $h = a^{-1}b \in B$, lebo $a \in A \subseteq B$, $b \in B$. Keďže aj $h \in H$, je $h \in B \cap H$ a teda $ah \in A(B \cap H)$. □

Veta 2.3.2 *Ak A, B sú podgrupy grupy G, A je normálna podgrupa B, H je normálna podgrupa G. Potom $AH \triangleleft BH$ a*

$$BH/AH \cong B/A(B \cap H).$$

Špeciálne, pre $A = \{e\}$ dostávame tzv. kosoštvorcovú vetu: H je normálna podgrupa BH a

$$BH/H \cong B/B \cap H.$$

Dôkaz. Nech $bh \in BH$, pričom $b \in B$, $h \in H$. Podgrupa H je normálna v G a preto $BH = HB$ a tiež platí, že, $AH = HA$ a $bA = Ab$, lebo A je normálna podgrupa B. Potom

$$(bh)AH = bhHA = bHA = HbA = HAb = AHb = AbH = AbHh = AH(bh)$$

a teda AH je normálna v BH. Pozrime sa na kompozíciu homomorfizmov

$$B \xrightarrow{i} BH \xrightarrow{\psi} BH/AH,$$

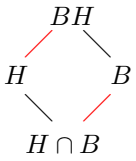
kde i je "inklúzia", ψ je kanonický faktorizačný homomorfizmus. Zrejme je $\mathrm{Ker}\,\psi \circ i = B \cap \mathrm{Ker}\,\psi = B \cap AH$. Podľa predošlej vety je $B \cap AH = A(B \cap H)$.

Homomorfizmus $\psi \circ i$ je surjektívny, lebo pre $b \in B$, $h \in H$ platí $bhAH = bhHA = bHA = bAH$ a preto podľa základnej vety o homomorfizme dostávame

$$B/\mathrm{Ker}\,\psi \circ i = B/A(B \cap H) \cong BH/AH$$

□

Druhá časť (kosoštvorcová veta) tvrdenia sa dá znázorniť pomocou diagramu (odtiaľ názov "kosoštvorcová"):



Pomocou tejto lemy dokážeme dôležitú vetu, tzv. Schreierovu vetu o zjemnení

Veta 2.3.3 *Nech $1 = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m = G$, $1 = A_0 \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n = G$ sú dva subnormálne rady (to znamená, že pre všetky prípustné indexy platí $A_i \triangleleft A_{i+1}$, podobne pre $B-$čka, ale nemusia to byť normálne podgrupy grupy G). Potom existujú ich zjemnenia, ktoré sú rovnakej dĺžky a sú faktorovo izomorfné.*

Dôkaz. Medzi každé dve grupy v rade "A-čok", t.j. medzi A_i a A_{i+1} vložíme podgrupy $A_{i,j} = A_i(A_{i+1} \cap B_j)$ pre $j = 0, \ldots, n$, t.j. $A_i = A_{i,0}$ a $A_{i+1} = A_{i,n}$.

Podobne, medzi každé dve grupy v rade "B-čok", t.j. medzi B_k a B_{k+1} vložíme podgrupy $B_{k,l} = B_k(B_{k+1} \cap A_l)$ pre $l = 0, \ldots, m$, t.j. $B_k = B_{k,0}$ a $B_{k+1} = B_{k,m}$.

Takto dostaneme zjemnenia pôvodných radov. Spočítaním $A_{i,j+1}/A_{i,j}$ pomocou lemy dostaneme

$$A_{i,j+1}/A_{i,j} = \frac{A_i(A_{i+1} \cap B_{j+1})}{A_i(A_{i+1} \cap B_j)} = \frac{\overbrace{(A_{i+1} \cap B_{j+1})}^{B}\overset{H}{A_i}}{(A_{i+1} \cap B_j)A_i} \cong \frac{A_{i+1} \cap B_{j+1}}{(A_{i+1} \cap B_j)(A_i \cap A_{i+1} \cap B_{j+1})} = \frac{A_{i+1} \cap B_{j+1}}{(A_{i+1} \cap B_j)(A_i \cap B_{j+1})}$$

a podobne

$$B_{k,l+1}/B_{k,l} = \frac{B_k(B_{k+1} \cap A_{l+1})}{B_k(B_{k+1} \cap A_l)} = \frac{\overbrace{(B_{k+1} \cap A_{l+1})}^{B}\overset{H}{B_k}}{(B_{k+1} \cap A_l)B_k} \cong \frac{B_{k+1} \cap A_{l+1}}{(B_{k+1} \cap A_l)(B_k \cap B_{k+1} \cap A_{l+1})} = \frac{B_{k+1} \cap A_{l+1}}{(B_{k+1} \cap A_l)(B_k \cap A_{l+1})}$$

Porovnaním posledných členov v týchto výpočtoch vidieť, že vždy platí $A_{i,j+1}/A_{i,j} \cong B_{j,i+1}/B_{j,i}$, pričom $i = 0, \ldots, m-1$, $i = 0, \ldots, n-1$.

Tieto zjemnenia sú teda faktorovo izomorfné. □

Dôsledkom tohoto tvrdenia je tiež veľmi dôležitá Jordan-Hölderova veta, ktorú uvedieme neskôr.

Pojem charakteristickej grupy je istým spôsobom podobný na pojem invariantnej podgrupy. Jeho definícia je

Definícia 2.3.4 *Pogrupa H grupy G sa nazýva charakteristická podgrupa G, ak pre každý automorfizmus $\varphi : G \to G$ platí $\varphi(H) = H$.*

Invariantnosť podgrupy H znamená, že ju "nehýbu" špeciálne automorfizmy (konjugácie). Pri charakteristickej požadujeme, aby ňou "nehýbali" všetky automorfizmy. Preto je každá charakteristická podgrupa automaticky invariantná.

Centrum ľubovoľnej grupy je jej charakteristická podgrupa. Ak je totiž $\varphi : G \to G$ automorfizmus, je to špeciálne surjektívny homomorfizmus. Nech je teda $a \in Z_G$, $g \in G$. Potom existuje $g' \in G$ také, že $\varphi(g') = g$ a teda $\varphi(a)g = \varphi(a)\varphi(g') = \varphi(ag') = \varphi(g'a) = \varphi(g')\varphi(a) = g\varphi(a)$ a preto $\varphi(a) \in Z_G$. Čiže $\varphi(Z_G) \subseteq Z_G$. Ale aj $\varphi^{-1} : G \to G$ je automorfizmus, takže aj $\varphi^{-1}(Z_G) \subseteq Z_G$. Odtiaľto ale vyplýva, že $\varphi(\varphi^{-1}(Z_G)) \subseteq \varphi(Z_G)$, t.j. $Z_G \subseteq \varphi(Z_G)$. Spolu dostávame, že $\varphi(Z_G) = Z_G$.

Toto tvrdenie sa dá zovšeobecniť na istý druh iterácií pojmu centra grupy pomocou lemy

Lema 2.3.5 *Nech G je grupa, H jej charakteristická podgrupa. Nech K je charakteristická podgrupa grupy G/H a $\psi : G \mapsto G/H$ je kanonický homomorfizmus, t.j. $\psi(g) = g \circ H$. Potom $J = \psi^{-1}(K)$ je charakteristická podgrupa grupy G.*

Dôkaz. Nech $\alpha : G \mapsto G$ je automorfizmus. Vieme, že $\alpha(H) = H$. Definujme $\overline{\alpha} : G/H \mapsto G/H$ nasledovne: $\overline{\alpha}(g \circ H) = \alpha(g) \circ H$.

Týmto je definované zobrazenie, ktoré je automorfizmom. Najprv, že je to zobrazenie. Nech $aH = bH$, t.j. $b^{-1}a \in H$. Potom $\alpha(b^{-1}a) \in H$, t.j. $\alpha(b)^{-1}\alpha(a) \in H$, t.j. $\alpha(a)H = \alpha(b)H$ a teda definícia $\overline{\alpha}$ nezávisí od výberu reprezentanta, ktorým definujeme triedu gH.

Homomorfnosť $\overline{\alpha}$ vyplýva z definície operácie vo faktorovej grupe a z faktu, že α je homomorfizmus:

$$\overline{\alpha}((aH)(bH)) = (\overline{\alpha}((ab)H) = \alpha(ab)H = \alpha(a)\alpha(b)H = (\alpha(a)H)(\alpha(b)H) = \overline{\alpha}(aH)\overline{\alpha}(bH)$$

Injektívnosť: Nech $gH \in \mathrm{Ker}\overline{\alpha}$, t.j. $\overline{\alpha}(gH) = H$. Preto $\alpha(g)H = H$, čo platí práve vtedy, keď $\alpha(g) \in H$. Ale z rovnosti $\alpha(H) = H$ a injektívnosti α vidíme, že toto nastáva práve vtedy, keď je $g \in H$. T.j. $\mathrm{Ker}\overline{\alpha} = H$, teda $\overline{\alpha}$ je injektívne zobrazenie.

Keďže α je surjektívne zobrazenie, je podľa definície aj $\overline{\alpha}$ surjektívne zobrazenie.

Nech je teraz K charakteristická podgrupa faktorovej grupy G/H, $J = \psi^{-1}(K)$, $\alpha : G \mapsto G$ automorfizmus grupy G. Vieme teda, že pre automorfizmus $\overline{\alpha} : G/H \mapsto G/H$ platí, že $\overline{\alpha}(K) = K$. Nech $a \in J$, čo je ekvivalentné s tým, že $aH \in K$. Potom $\overline{\alpha}(aH) \in K$, ale $\overline{\alpha}(aH) = \alpha(a)H$ a preto $\alpha(a) \in J$. Takže pre každý automorfizmus α vieme, že $\alpha(J) \subseteq J$. Keďže aj α^{-1} je automorfizmus a preto odtiaľ dostávame, že aj $\alpha^{-1}(J) \subseteq J$ a potom aj $\alpha(\alpha^{-1}(J)) \subseteq \alpha(J) \subseteq J$ a preto pre každý automorfizmus α platí, že $\alpha(J) = J$, t.j. J je charakteristická podgrupa grupy G. □

Z tejto lemy vyplýva, že všetky iterované centrá $Z_n(G)$ sú charakteristické podgrupy grupy G (a že tie iterované centrá vlastne vieme definovať).

Konkrétnejšie, položme $Z_0(G) = \{e\}$ (e je neutrálny prvok grupy G). Predpokladajme, že $Z_i(G)$ je charakteristická a teda aj normálna podgrupa grupy G. Nech $\psi : G \mapsto G/Z_i(G)$ je kanonický homomorfizmus. Zoberme centrum grupy $G/Z_i(G)$, t.j. $H = Z(G/Z_i(G))$ a položme $Z_{i+1}(G) = \psi^{-1}(H)$. Keďže H je centrum a preto charakteristická podgrupa $G/Z_i(G)$, je podľa lemy $\psi^{-1}(H)$ charakteristická podgrupa G.

Takto dostávame postupnosť (nie nutne rôznych) podgrúp grupy G s vlastnosťou

$$Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_n(G) \subseteq \cdots \subseteq G$$

Definícia 2.3.6 *Ak existuje také n, že $Z_n(G) = G$, hovoríme, že G je nilpotentná grupa. Ak je G nilpotentná grupa, najmenšie n, pre ktoré platí, že $Z_n(G) = G$ nazývame stupeň nilpotentnosti.*

Podľa definície je každá komutatívna grupa nilpotentná a stupňa nilpotentnosti 1. Grupa G je komutatívna práve vtedy, keď je nilpotentná stupňa nilpotentnosti 1.

Dobrým príkladom nilpotentných grúp sú konečné p-grupy (p prvočíslo). Nech je G konečná p-grupa. Podľa dôsledku 2.2.2 má každá p-grupa netriviálne centrum. Každá faktorizácia p-grupy je podľa Lagrangeovej vety p-grupa a preto je $Z(G/Z_i(G)$ netriviálna (v tom zmysle, že obsahuje niečo viac ako neutrálny prvok) a preto ak $Z_i(G) \neq G$ je $Z_i(G) \subsetneq Z_{i+1}(G)$. Z konečnosti G potom dostávame, že G je nilpotentná grupa.

Cvičenie 46 *Súčin konečne veľa nilpotentných grúp je nilpotentná grupa. (dôkaz stačí pre 2, zvyšok je jednoduchá indukcia).*

2.4 Kompozičné rady

Kapitola 3

Voľné grupy a voľné súčiny

3.1 Definícia voľnej grupy

Prvky generujúcej množiny S grupy G môžu spĺňať nejaké vzťahy, alebo, inak povedané, nejaké súčiny prvkov z S a k nim inverzných sa môžu rovnať neutrálnemu prvku grupy G. Napríklad, pre ľubovoľný prvok $x \in S$ platí $xx^{-1} = e, \quad x^{-1}x = e$. Tieto dve rovnice (identity) sú dôsledkom axióm grúp (t.j. platia v každej grupe a platia pre ľubovoľné prvky, nielen pre prvky generujúcej množiny) a preto sa nazývajú *triviálne*.

Je vidieť, že existujú grupy s takými generujúcimi množinami, ktorých prvky nie sú "podriadené" žiadnym netriviálnym vzťahom. Cieľom tejto časti je dať všeobecný popis takýchto grúp a ukázať ich existenciu pre ľubovoľnú množinu generátorov.

Keď máme grupu G a v nej množinu S prvkov, ktoré nie sú zviazané žiadnymy vzťahmi, môžeme sa pozrieť na podgrupu $[S]$ grupy G generovanú prvkami množiny S. Toto štúdium nám poskytne informáciu ako "skonštruovať" abstraktnú grupu bez zbytočných vzťahov z ľubovoľnej množiny generátorov (t.j. bez predpokladu, že S je časťou nejakej grupy). Nech I je množina. Ak je G akákoľvek grupa generovaná prvkami $x_i, \quad i \in I$, jej prvky sa dajú napísať ako slová v tvare $x_1^{\epsilon_1} \dots x_m^{\epsilon_m}$, $\epsilon_j \in \{+1, -1\}$ a súčin je jednoducho pripísanie slova za slovo. Konštrukciu začne upresnením tohoto pozorovania.

Zoberme množinu X a označme $X^{-1} = \{x^{-1}; x \in X\}$ a $S = X \cup X^{-1}$.

Slovo v abecede X (presnejšie v abecede S) je buď prázdna (označuje sa ako 1) alebo konečná postupnosť prvkov z množiny S. Množinu všetkých slov v abecede X označujeme X^*. Počet prvkov postupnosti slova $a \in X^*$ nazývame *dĺžkou* tohoto slova. Označenie: $l(a)$. Slovo $a \in X^*$ nazývame *(ne)skrátiteľné*, ak (ne)obsahuje podslovo tvaru xx^{-1} alebo tvaru $x^{-1}x$, $x \in X$. Neskrátiteľné slovo nazývame tiež redukované. Rovnosť slov $a, b \in X^*$ označujeme znakom $\equiv$, t.j. $a \equiv b$.

Dve slová z X^* nazveme *susedné*, ak má jedno z nich tvar $ux^\epsilon x^{-\epsilon} v$ a druhé tvar uv, u, v sú slová z X^*, $\epsilon \in \{+1, -1\}$, $x \in X$. Slová $a, b \in X^*$ nazývame *ekvivalentné*, píšeme $a \sim b$, ak existuje postupnosť slov z X^* $a_0, a_1, \dots, a_k$ takých, že $a = a_0$, $b = a_k$ a slová a_i, a_{i+1} sú susedné pre všetky prípustné indexy. Relácia ekvivalencie medzi slovami je zrejme reláciou ekvivalencie na množine X^*. Všetky slová z množiny X^* ekvivalentné s daným slovom a tvoria triedu ekvivalencie, ktorú budeme označovať $[a]$.

Na slove $a \in X^*$ budeme definovať procedúru *redukcie sprava* nasledovne: Začneme z a a postupne budeme vyčiarkavať najviac vpravo sa nachádzajúce výskyty podslov tvaru $x^\epsilon x^{-\epsilon}$. Týmto spôsobom sa raz dostaneme k neskrátiteľnému slovu, ktoré označíme $r(a)$. (Formálnejšie: nech $a \in X^*$ je slovo také, že $a = ux^\epsilon x^{-\epsilon} v$, kde $x^\epsilon x^{-\epsilon}$ je najpravší výskyt podslova tohoto tvaru v slove a, t.j. v je neskrátiteľné slovo a nezačína sa znakom x^ϵ. Položíme $r'(a) = uv$. Ak je a redukované slovo, kladieme $r'(a) = a$. Nech teraz $a_0 = a$, $a_1 = r'(a)$, $a_2 = r'(a_1)$, ... a nech $k \in N$ je najmenší taký index, že $a_k = a_{k+1}$ (ak $a_i \neq a_{i+1}$, tak $l(a_i) > l(a_{i+1})$ a preto taký index existuje, inak by sme totiž dostali nekonečnú klesajúcu postupnosť prirodzených čísel). Položíme $r(a) = a_k$. Pre ľubovoľné slovo a je slovo $r(a)$ neskrátiteľné a je určené jednoznačne. Hovoríme, že slovo $r(a)$ vzniklo zo slova a *redukciou sprava*.)

Veta 3.1.1 *Funkcia $r : X^* \to X^*$ má nasledujúce vlastnosti:*
Pre $a, b \in X^*$, $x \in X$, $\epsilon = \pm 1$

1. $r(a) \sim a$
2. $r(a) \equiv a \iff$ *a je neskrátiteľné slovo*
3. $r(ab) \equiv r(ar(b))$
4. $r(x^\epsilon x^{-\epsilon} a) \equiv r(a)$

5. $r(ax^\epsilon x^{-\epsilon}b) \equiv r(ab)$ *(ktorékoľvek zo slov a, b môže byť prázdne)*

6. $r(ab) \equiv r(r(a)r(b))$

7. *Trieda $[a]$ obsahuje jediné neskrátiteľné slovo a to $r(a)$*

Dôkaz. Vlastnosti 1.–3. vyplývajú priamo z definície, 4. plynie z 3., 5. plynie z 3. a 4.

Trochu sa zastavme pri 6. Táto plynie z 5. indukciou podľa dĺžky slova ab, urobíme len indukčný krok: ak sú obe slová a a b neskrátiteľné, potom $r(a) = a$ a $r(b) = b$ a teda triviálne $r(ab) = r(r(a)r(b)$. Nech je niektoré zo slov a, b skrátiteľné, nech je to napr. a. Potom $a = ux^\epsilon x^{-\epsilon}v$ pre vhodné $u, v \in X^*$, $x \in X$ a $\epsilon = \pm 1$. Podľa 5. a indukčného predpokladu je postupne $r(ab) = r(uvb) = r((uv)b) = r(r(uv)r(b))$. Podľa 5. je aj $r(a) = r(uv)$, čiže $r(ab) = r(r(a)r(b))$.

Nakoniec 7. plynie z 5. a definície ekvivalencie (treba dokázať, že $a \sim b \Rightarrow r(a) \equiv r(b)$ - pre susedné slová to vyplýva z 5.). □

Veta 3.1.2 *Nech X je ľubovoľná množina. Na množine $X^*/\sim$, t.j. množine všetkých tried ekvivalencie $\sim$ definujme operáciu $*$ vzťahom $[a] * [b] = [ab]$. Táto operácia nezávisí od výberu reprezentantov a $(X^*/\sim, *)$ je grupa. Túto grupu sa nazývame voľnou grupou s voľnými generátormi X, označujeme $F(X)$. Znak operácie $*$ budeme zvyčajne vynechávať.*

Dôkaz. Overíme, že operácia $*$ nezávisí od výberu reprezentantov: podľa 1. a 6. v predchádzajúcej vete platí $ab \sim r(ab) = r(r(a)r(b))$. Vďaka 7. je $r(a)$ ($r(b)$, resp. $r(ab)$) jednoznačne určený prvok triedy $[a]$ (triedy $[b]$, resp. $[ab]$) a preto tieto rovnosti dokazujú potrebnú nezávislosť.

Asociativita operácie $*$ je triviálna. Neutrálnym prvkom je $[1]$. Ak $a = [a_1^\epsilon \dots a_k^\epsilon]$ ($a_i \in X$, $\epsilon = \pm 1$), potom $a^{-1} = [a_k^{-\epsilon} \dots a_1^{-\epsilon}]$. □

Poznámka. Predošlá definícia okrem iného hovorí, že ľubovoľná trieda $[a]$, ktorej redukované slovo $r(a)$ je neprázdne slovo je rôzna od neutrálneho prvku grupy $F(X)$, t.j. od triedy $[1]$. Táto skutočnosť hovorí, že sme presne dosiahli vytýčený cieľ — zadefinovali (skonštruovali) sme grupu v ktorej neplatia žiadne netriviálne vzťahy. Naviac je vidieť, že grupa $F(X)$ je generovaná svojou podmnožinou X. (Pri tomto stotožňujeme jednoprvkové postupnosti s prvkami, z ktorých tieto postupnosti pozostávajú.)

Mohutnosť množiny X voľných generátorov grupy $F(X)$ nazývame stupňom voľnosti. Ak je táto mohutnosť prirodzené číslo n (resp. ∞ - spočítateľné nekonečno) a generátory nie sú podstatné, budeme písať jednoducho F_n (resp. F_∞). Zvyčajne budeme písať len prvky namiesto tried, t.j. u, v, uv namiesto $[u]$, $[v]$, $[uv]$ a tiež budeme používať znamienko $=$ namiesto znamienka $\equiv$, t.j. $u = v$, $uv = w$ namiesto $[u] = [v]$ či $[uv] = [w]$. Vďaka vete 3.1.1 môžeme hovoriť aj o redukovanom zápise triedy, čím rozumieme (redukované) slovo $r(a)$ ľubovoľného reprezentanta a tejto triedy.

Cvičenie 47 *Voľné grupy stupňa voľnosti ≥ 2 sú nekomutatívne.*

Cvičenie 48 *Ak $a \neq 1$ je slovo, potom pre $n \geq 2$ platí nerovnosť $l(r(a^n)) > \max\{l(r(a)), l(r(a^{-1}))\}$. Špeciálne: každá voľná grupa je grupa bez torzie.*

Teraz dokážeme základnú vetu charakterizujúcu voľné grupy. Táto veta popisuje voľné grupy z hľadiska vzťahu ku všetkým ostatným grupám, čo je prístup charakteristický pre univerzálne algebry.

Veta 3.1.3 *Nech $(G, \circ)$ je grupa, nech $F(X)$ je voľná grupa s voľnými generátormi X. Nech $f : X \to G$ je ľubovoľné zobrazenie. Potom existuje jediný homomorfizmus $\varphi : F(X) \to G$, ktorý je rozšírením zobrazenia f, t.j. taký, že $\varphi|X = f$.*

Dôkaz. Označme $(x_1)f = g_1, \dots, (x_k)f = g_k$. Aby sme zabezpečili splnenie vlastnosti $\varphi|X = f$ a to, že φ má byť homomorfizmus, musíme definovať (týmto teda získavame jednoznačnosť):

$$[x_1^{\epsilon_1} \dots x_k^{\epsilon_k}]\varphi = g_1^{\epsilon_1} \circ \dots g_k^{\epsilon_k}.$$

Je ľahko vidieť, že takto máme definované zobrazenie (t.j. korektnosť), ktoré je skutočne homomorfizmus. □

Ak je homomorfizmus $\varphi : F(X) \to G$ z predchádzajúcej vety surjektívny, potom prvky normálnej podgrupy $H = Ker\,\varphi$ grupy $F(X)$ nazývame *reláciami* grupy $(G, \circ)$ v abecede X. Ak R je taká množina relácií, že najmenšia normálna podgrupa obsahujúca R je rovná podgrupe H (t.j. $N_{F(X)}(R) = H$), potom R nazývame *definujúcou množinou relácií* grupy $(G, \circ)$ v abecede X.

V tomto prípade platí $G \cong F(X)/H$, a preto je vidieť, že grupa $(G, \circ)$ je zadaním abecedy X a množiny R (t.j. podgrupy H) jednoznačne (až na izomorfizmus) určená. Dvojicu (X, R) nazývame *prezentácia* grupy $(G, \circ)$. Prezentácia grupy nie je jednoznačná, každá grupa môže mať viacero prezentácií. Ak (X, R) je prezentácia grupy $(G, \circ)$, píšeme $G = gr(X; R)$, pričom v prípade konečných množín X a R zvyčajne vynechávame množinové zátvorky; t.j. napr. $(Z, +) = gr(x;) = gr(x; \emptyset)$ alebo $(Z_n, +) = gr(x; x^n)$. V prezentácii grúp niekedy namiesto definujúcich relácií — teda prvkov z R — píšeme rovnosti, t.j. namiesto prvku x^n v poslednej prezentácii by sme napísali $x^n = 1$, alebo namiesto prvku z R tvaru $u_1 u_2^{-1}$ rovnicu $u_1 = u_2$. Ak existuje prezentácia grupy $(G, \circ)$ aká, že X a R sú konečné množiny, hovoríme, že grupa $(G, \circ)$ je *konečne prezentovateľná* (alebo konečne *definovateľná*).

Cvičenie 49 *Voľná komutatívna grupa s n generátormi má prezentáciu $gr(x_1, \ldots, x_n; x_i^{-1} x_j^{-1} x_i x_j,\ 1 \leq i < j \leq n)$.*

Cvičenie 50 $Z_2 \times Z_2 = gr(x, y; x^2 = 1, y^2 = 1, xy = yx)$.

Nasledujúca veta objasní vzťah medzi mohutnosťami množín voľných generátorov a typom izomorfizmu grúp:

Veta 3.1.4 *1. Nech $|X| = |Y|$. Potom $F(X) \cong F(Y)$.*

2. Nech $F(X) \cong F(Y)$. Potom $|X| = |Y|$.

Dôkaz.

1. Nech $f : X \to Y$ je bijekcia. Nech $\varphi : F(X) \to F(Y)$ je homomorfizmus, ktorý je rozšírením f. $Ker\,\varphi = \{1\}$, lebo vo voľnej grupe $F(Y)$ neplatia žiadne netriviálne vzťahy a $Im\,\varphi = F(Y)$, lebo Y generuje grupu $F(Y)$. Teda φ je izomorfizmus.

2. Keďže sú grupy $F(X)$ a $F(Y)$ izomorfné, majú rovnaký počet (v zmysle kardinality) normálnych podgrúp indexu 2. Každá normálna podgrupa H v grupe $F(X)$ indexu 2 je určená (a jednoznačne určuje) netriviálny homomorfizmus $\varphi_H : F(X) \to Z_2$ a tento jednoznačne určuje (a je jednoznačne určený) netriviálne zobrazenie $f_H : X \to Z_2$. (Netriviálnosť znamená, že sa aspoň jeden prvok zobrazí na 1 — to je nutné, aby H bola podgrupa indexu 2.) To znamená, že podgrupa $F(X)$ má $|2^X| - 1$ normálnych podgrúp indexu 2. Rovnakú úvahu môžeme samozrejme aplikovať aj na grupu $F(Y)$, táto má teda $|2^Y| - 1$ normálnych podgrúp indexu 2. Preto $|2^X| - 1 = |2^Y| - 1$ a teda tiež $|2^X| = |2^Y|$. Ak je jedna z množín X, Y konečná, vyplýva z tohoto, že X a Y majú rovnako veľa prvkov.

   Ak je niektorá nekonečná, vidíme, že sú obe nekonečné. Z axiómy výberu plynie, že pre ľubovoľnú nekonečnú množinu platí $|Z| = F(Z)$. V našom prípade teda $|X| = F(X)$ a $|Y| = F(Y)$ a keďže $F(X) \cong F(Y)$, platí že $|F(X)| = |F(Y)|$ a teda nakoniec $|X| = |Y|$.

□

3.2 Todd-Coxeterov algoritmus

Na získanie informácií o grupách zadaných (konečnou) prezentáciou je užitočný *Todd-Coxeterov* algoritmus — metóda "prečíslenia" vedľajších tried podľa nejakej podgrupy. Tento algoritmus sa podľa známej vety (Novikov) nemusí zastaviť, resp. vo všeobecnosti nevieme, či sa zastaví. Ak je H podgrupa grupy G a Todd-Coxeterov algoritmus sa zastaví, dostaneme informáciu o indexe $[G : H]$, špeciálne, pre $H = \{1\}$ získame informáciu o počte prvkov grupy G. (Výstup algoritmu je okrem iného číslo k také, že $[G : H]$ je deliteľom k.)

Tento algoritmus si ukážeme na grupe S_4, nájdeme jej konečnú prezentáciu. Ľahko sa dá overiť, že permutácie $a = (1234)$ a $b = (12)$ generujú S_4. Platí

$$a^4 = 1, \quad b^2 = 1 \quad \text{a} \quad (ab)^3 = 1.$$

Predpokladajme, že tieto vzťahy stačia na popis grupy S_4, t.j., pokúsime sa dokázať, že

$$S_4 = gr(a, b; a^4 = 1, b^2 = 1, (ab)^3 = 1).$$

Skúmajme teda grupu

$$G = gr(a, b; a^4 = 1, b^2 = 1, (ab)^3 = 1)$$

a nejakú jej podgrupu, napr. $H = [a]$. Podgrupa H má 4 prvky. Ak sa nám podarí dokázať, že $[G : H] \leq 6$ budeme hotoví. To totiž znamená, že G má najviac 24 prvkov. Ovšem už vieme (plynie to z úvah, ktorými sme dospeli

ku vzťahom medzi prvkami a a b v S_4), že 24 prvková grupy S_4 je homomorfný obraz grupy G, z čoho už plynie požadovaný záver, že totiž $S_4 \cong G$.

V súvislosti s definujúcimi reláciami v grupe G si načrtnime tri tabuľky, každú pre jednu reláciu. V záhlaví každej tabuľky bude slovo $u_1u_2\dots u_n$ z definujúcej relácie v tvare $u_1u_2\dots u_n = 1$ a v jednotlivých riadkoch budeme po stĺpcoch písať ako sa jednotlivé triedy správajú pri postupnom prenásobovaní prvkami zo slova napísaného v záhlaví tabuľky. Preto prvý a posledný prvok v každom riadku je rovnaký, lebo posledný prvok v riadku reprezentuje výsledok prvého prvku po prenásobení slovom zo záhlavia a teda jednotkou

a	a	a	a		b	b		a	b	a	b	a	b
1	1	1	1	1	1		1	1	1				1

a začneme číslovať vedľajšie triedy podľa H, pričom samotnú podgrupu H označíme cifrou 1. Zrejmú rovnosť $1a = 1$ ($a \in H$) sme už v tabuľkách vyznačili. Čo napíšeme na prázdne miesto v druhej tabuľke? Aby sme do našich vzťahov nevniesli niečo, čo nevyplýva z definujúcich vzťahov, položíme $1b = 2$, z čoho podľa druhej tabuľky hneď vyplýva $2b = 1$. Tento fakt "zanesieme" do všetkých tabuliek, pričom v každej tabuľke pridáme nový riadok, do ktorého budeme písať ako sa bude správať prvok (vedľajšia trieda označená ako) 2 pri násobení jednotlivými slovami z definujúcich vzťahov. Dostaneme

a	a	a	a		b	b		a	b	a	b	a	b
1	1	1	1	1	1	2	1	1	1	2			2	1
2				2	2	1	2	2			2	1	1	2

Ďalej položíme $2a = 3$ a $3a = 4$. Po tomto dostanú tabuľky tvar

a	a	a	a		b	b		a	b	a	b	a	b
1	1	1	1	1	1	2	1	1	1	2	3		2	1
2	3	4		2	2	1	2	2	3		2	1	1	2
3	4		2	3	3		3	3	4					3
4		2	3	4	4		4	4						4

Ak teraz položíme $4a = 5$, z druhého (alebo tretieho či štvrtého) riadku prvej tabuľky dostávame $5a = 2$, po dosadení 5 na tretie miesto do druhého riadku tretej tabuľky dostaneme $3b = 5$, odkiaľ znovu po vpísaní do tretieho riadku druhej tabuľky vidíme, že $5b = 3$. Teda sme dostali

a	a	a	a		b	b		a	b	a	b	a	b	
1	1	1	1	1	1	2	1	1	1	2	3	5	2	1
2	3	4	5	2	2	1	2	2	3	5	2	1	1	2
3	4	5	2	3	3	5	3	3	4			4	5	3
4	5	2	3	4	4		4	4	5	3	4			4
5	2	3	4	5	5	3	5	5	2	1	1	2	3	5

Ako vidíme, tabuľky sa zapĺňajú, čo je znak toho, že proces číslovania sa asi chýli ku koncu (inak by tabuľky s rastúcim počtom riadkov mali tendenciu rednúť). Chýba nám hodnota $4b$, položme preto $4b = 6$. Hodnotu 6 vpíšme do potrebných miest (štvrtý riadok v druhej tabuľke, druhý a tretí riadok v tretej tabuľke). Zo štvrtého riadku druhej tabuľky vidíme, že $6b = 4$, teda 6 môžeme vpísať do (posledných) prázdnych miest v druhom a treťom riadku v tretej tabuľke. Týmto tiež dostaneme $6a = 6$ a po doplnení šiesteho riadku teda dostaneme

a	a	a	a		b	b		a	b	a	b	a	b	
1	1	1	1	1	1	2	1	1	1	2	3	5	2	1
2	3	4	5	2	2	1	2	2	3	5	2	1	1	2
3	4	5	2	3	3	5	3	3	4	6	6	4	5	3
4	5	2	3	4	4	6	4	4	5	3	4	6	6	4
5	2	3	4	5	5	3	5	5	2	1	1	2	3	5
6	6	6	6	6	6	4	6	6	6	4	5	3	4	6

Keďže sa tabuľky uzavreli, je očíslovanie vedľajších tried skončené. Jeho výsledok je, že G/H má 6 prvkov. Samozrejme, mohlo sa stať, že sme si na niektorom mieste mohli nevšimnúť nejaký vzťah, t.j. nevyužili sme možnosť zaplnenia niektorých miest v danom kroku. To znamená, že niektoré vedľajšie triedy majú viac čísiel. Uzavretie tabuliek teda presne povedané znamená len, že $[G : H] \leq 6$, alebo presnejšie, že $[G : H]$ delí číslo 6. Ale v našom príklade už vieme, že $|G| \geq 24$ a teda musí byť $[G : H] = 6$. Tento proces sa dá veľmi pekne naprogramovať, viď napr. GAP.

Ešte si uveďme vetu charakterizujúcu homomorfizmy pre grupy zadané svojimi prezentáciami.

Veta 3.2.1 *Nech $G = gr(X; R)$ je prezentácia grupy G, H je grupa, $f : X \mapsto H$. Rozšírme f na $S = X \cup X^{-1}$ tak, že položíme $f(x^{-1}) = (f(x))^{-1}$. Zobrazenie f sa dá rozšíriť na homomorfizmus $\varphi : G \mapsto H$ práve vtedy, keď pre každý prvok $a \in R$, zapísaný v tvare $a = x_1^{\epsilon_1} \dots x_k^{\epsilon_k}$ platí $f(x_1)^{\epsilon_1} \dots f(x_k)^{\epsilon_k} = 1$ v grupe H ($x_i \in X$, $\epsilon_i \in \{\pm 1\}$)*

Dôkaz.
□

Cvičenie 51 *$S_3 = gr(x, y;\ x^2 = y^3 = (xy)^2 = 1)$. Dokážte!*

Cvičenie 52 *Očíslujte 5 vedľajších tried grupy*

$$G = gr(x, y, z;\ x^3 = y^3 = z^3 = (yz)^2 = (zx)^2 = (xy)^2 = 1)$$

podľa podgrupy $H = gr(x, y)$.

Cvičenie 53 *Nech H je podgrupa grupy $F(x, y)$ generovaná prvkami $x^n y x^n$, $n = 0, 1, \dots$ Dokážte, že H je voľná grupa (t.j. uvedené prvky nie sú v G "zviazané" žiadnymi reláciami).*
(Teda F_∞ je podgrupou grupy F_2 — resp. dá sa vnoriť.)

3.3 Podgrupy voľných grúp

Pri štúdiu grúp vždy hrá dôležitú úlohu štruktúra podgrúp tejto grupy. Napríklad veta 3.1.3 ukazuje dôležitosť invariantných podgrúp vo voľných grupách.

Nielsen a Schreier dokázali, že podgrupa voľnej grupy je voľná (pre komutatívne grupy podobný výsledok poznáme, dokonca vieme, že podgrupa má najviac toľko generátorov ako grupa — túto vlastnosť sa nám pre nekomutatívny prípad nepodarí dokázať). My si ukážeme (trochu zjednodušený) Schreierov dôkaz tohoto tvrdenia.

Začneme definíciou

Definícia 3.3.1 *Podmnožinu G voľnej grupy $F(X)$ (X je množina voľných generátorov) nazveme* schreierovským systémom*, ak pre každý prvok $g \in G$ platí*

1. *$g = x_1 \dots x_t$ je redukované slovo ($x_i \in X \cup X^{-1}$)*
2. *každé podslovo $x_1 \dots x_l$, $l \le t$ patrí do G (a tiež $1 \in G$)*

Ak G spĺňa naviac ešte vlastnosť

3. *každé podslovo $x_i \dots x_t$, $1 \le i$ patrí do G*

tak G nazývame obojstranným schreierovským systémom*.*

Nech je F voľná grupa generovaná množinou voľných generátorov S a U nech je jej podgrupa. Pri skúmaní pravého rozkladu podľa podgrupy H, t.j.

$$F = U \cdot 1 + U \cdot g_2 + \dots + U \cdot g_i + \dots$$

budeme ako reprezentanta vedľajšej triedy U vždy vyberať prvok 1 (i keď sa z vyššie uvedeného zápisu tak môže zdať, nepredpokladáme nič o mohutnosti množiny vedľajších tried F/U). Ako sa ukazuje, je výhodné vhodne vybrať reprezentantov jednotlivých (pravých) vedľajších tried.

Lema 3.3.2 (Zovšeobecnená Schreierova lema) *Nech U je podgrupa voľnej grupy F. Potom existuje systém G reprezentantov vedľajších tried grupy F podľa podgrupy U taký, že G je schreierovský systém. Ak je naviac U invariantná podgrupa, možno G vybrať tak, aby to bol obojstranný schreierov systém.*

Dôkaz. Nech je množina $S \cup S^{-1}$ generátorov a k nim inverzných prvkov nejakým spôsobom dobre usporiadaná (ak je S konečná, môžeme to urobiť napr. nasledovne: $s_1 < s_1^{-1} < s_2 < \dots < s_n < s_n^{-1}$, inak existencia takého usporiadania vyplýva napr. z axiómy výberu).

Toto dobré usporiadanie, ktoré budeme označovať znakom $<$ je možné predĺžiť do nasledujúceho lexikografického usporiadania redukovaných slov v abecede $S \cup S^{-1}$, t.j. prvkov grupy F (tiež budeme používať označenie $<$): ak máme redukované slová

$$\begin{aligned} f &= a_1 \dots a_t \\ g &= b_1 \dots b_u \end{aligned}$$

potom položíme $f < g$ ak je splnená jedna z nasledujúcich podmienok

1. $t < u$
2. $t = u$ a $a_1 < b_1$
3. $t = u$, pre vhodné $i < t$ je $a_1 = b_1, \ldots a_i = b_i$ a $a_{i+1} < b_{i+1}$

Takto definované lexikografické usporiadanie je dobrým usporiadaním a ľahko sa dá presvedčiť podľa definície, že má nasledujúce dve vlastnosti: ak $f < g$ sú dve redukované slová a ak je slovo gh redukované, tak $fh < gh$. Ak je $f < g$ a slovo hg je redukované, tak $hf < hg$. Tiež je vidieť, že 1 je prvý prvok množiny F pri tomto usporiadaní.

Nech teraz $U \cdot a$ je vedľajšia trieda rozkladu. Ako reprezentanta tejto triedy vyberme najmenší prvok tejto triedy, t.j. množiny $U \cdot a$ v našom dobrom usporiadaní $<$. Ukážeme, že takto vybratý systém reprezentantov G je schreierovský systém.

Predovšetkým každý prvok F a teda aj množiny $U \cdot a$ je redukované slovo. Zrejme sme pre triedu U vybrali prvok 1. Nech teraz redukované slovo $g = a_1 a_2 \ldots a_t \in G$, t.j. g je prvý prvok množiny $U \cdot g$. Tvrdíme, že potom je $g' = a_1 a_2 \ldots a_{t-1} \in G$, t.j. slovo $a_1 a_2 \ldots a_{t-1}$ je prvý prvok triedy $U \cdot a_1 a_2 \ldots a_{t-1}$. Sporom, nech $h = b_1 \ldots b_l$ je najmenší prvok v triede $U \cdot a_1 a_2 \ldots a_{t-1}$ a nech je rôzny od g'. Potom je $ha_t \in U \cdot g$ a teda podľa predpokladu je $g < ha_t$ (g je najmenší). Ale z faktu, že $h < g'$ plynie, že $ha_t < g'a_t = g$, lebo $g'a_t = g$ je redukované slovo. To je však spor. Teda $g' \in G$. Podobne sa dokáže druhá vlastnosť obojstranného schreierovského systému pre prípad invariantnej podgrupy. □

Uvedomme si, že práve dokázaná lema zabezpečuje existenciu schreierovského systému reprezenatantov vedľajších tried voľnej grupy F podľa jej podgrupy U, ale pre danú podgrupu môže takýchto schreierovských systémov existovať viacero.

Teraz vyslovíme základnú vetu tejto časti

Veta 3.3.3 *Ľubovoľná podgrupa voľnej grupy je voľná.*

Nech F je voľná grupa generovaná množinou S, nech U je jej podgrupa. Nech G je nejaký schreierovský systém reprezentantov pravých vedľajších tried grupy F podľa podgrupy U, t.j.

$$F = U \cdot 1 + U \cdot g_2 + \cdots + U \cdot g_i + \cdots \tag{3.1}$$

Začneme s dôkazom lemy, ktorá platí pre ľubovoľnú, nie nutne voľnú grupu F. Nech F je grupa generovaná množinou S, U nech je podgrupa grupy F.

Zadefinujeme zobrazenie $\Phi : F \to G$ nasledovne: ak $f \in U \cdot g$, $g \in G$, tak položíme $\Phi(f) = g$. Teda Φ je konštantná na každej vedľajšej triede a nadobúda na nej ako hodnotu príslušný reprezentant tejto triedy. Zrejme pre $u \in U$ je $\Phi(uf) = \Phi(f)$ a $\Phi(f) = 1$ práve vtedy, keď $f \in U$. Ďalej, keďže $\Phi(f)$ a f ($\Phi(g)$ a g) ležia v jednej vedľajšej triede rozkladu, pre ľubovoľné $f, g \in F$ platí $\Phi(\Phi(f)g) = \Phi(fg) = \Phi(f\Phi(g))$ a pre $g \in G$ je $\Phi(g) = g$.

Lema 3.3.4 *Nech F je ľubovoľná grupa (nie nutne voľná) s množinou generátorov S. Nech U je podgrupa F a nech G je množina reprezentantov pravých tried rozkladu grupy F podľa podgrupy U. Potom prvky tvaru $gs\Phi(gs)^{-1}$ $g \in G$, $s \in S$ generujú grupu U.*

Dôkaz. Najprv si uvedomme, že $gs\Phi(gs)^{-1} \in U$, lebo gs a $\Phi(gs)$ patria do tej istej triedy rozkladu podľa U.

Nech $f \in F$, $f = a_1 \ldots a_k$, $a_i \in S \cup S^{-1}$. Zadefinujme nasledovnú postupnosť:

$$h_0^f = \Phi(1) = 1,\ h_1^f = \Phi(a_1),\ \ldots,\ h_k^f = \Phi(f) = \Phi(a_1 \ldots a_k)$$

Ak je teraz $f \in U$, podľa vyššie uvedených vlastností funkcie Φ je $h_k^f = 1$ a preto platí (namiesto h_i^f budeme písať len h_i)

$$f = h_0 a_1 h_1^{-1} h_1 a_2 h_2^{-1} \ldots h_{k-1} a_k h_k^{-1}$$

(využili sme aj fakt, že $h_0 = 1$). Všimnime si teraz prvky tvaru $h_{i-1} a_i h_i^{-1}$, $i \leq k$.

Máme

$$\begin{aligned} h_{i-1} a_i h_i^{-1} &= \Phi(a_1 \ldots a_{i-1}) a_i \Phi(a_1 \ldots a_{i-1} a_i)^{-1} = \\ &= \Phi(a_1 \ldots a_{i-1}) a_i \Phi(\Phi(a_1 \ldots a_{i-1}) a_i)^{-1} = h_{i-1} a_i \Phi(h_{i-1} a_i)^{-1} \end{aligned}$$

pričom $\Phi(a_1 \ldots a_{i-1}) \in G$ a $a_i \in S \cup S^{-1}$. Ešte dokážeme, že $gs^{-1}\Phi(gs^{-1})^{-1}$ je $(hs'\Phi(hs')^{-1})^{-1}$ pre vhodné $h \in G$ a $s' \in S$ a teda uvedené prvky skutočne generujú množinu U. Počítajme teda

$$(gs^{-1}\Phi(gs^{-1})^{-1})^{-1} = \Phi(gs^{-1}) s g^{-1} = *$$

a ak položíme $h = \Phi(gs^{-1})$ tak $h \in G$ a

$$\Phi(hs) = \Phi(\Phi(gs^{-1})s) = \Phi(gs^{-1}s) = \Phi(g) = g$$

na základe vlastností funkcie Φ a teda

$$* = hsg^{-1} = hs\Phi(hs)^{-1}$$

□

Dôsledok 3.3.5 *Ak $g \in G$, $s \in S$ a $\Phi(gs^\epsilon) = h$, tak $\Phi(hs^{-\epsilon}) = g$. (tzv. "prehadzovačka")*

Dôsledok 3.3.6 *Ak F je konečne generovaná grupa a U je jej podgrupa konečného indexu, tak U je tiež konečne generovaná.*

Dôkaz. Vo výraze $gs\Phi(gs)^{-1}$ máme pre g aj s konečne veľa možností. Neskôr si dokážeme konkrétny počet generátorov. □

Všimnime si, že pri dôkaze tejto lemy sme potrebovali len fakt, že Φ je definovaná na prvkoch tvaru gs^ϵ pre $g \in G$ a $s \in S$ a že má nasledujúce vlastnosti (sú to už uvedené vlastnosti Φ, ale len pre uvedený definičný obor) (na odlíšenie definičných oborov budeme písať φ namiesto Φ):

1. $\varphi(gs^\epsilon) \in G$
2. ak $gs^\epsilon \in G$, tak $\varphi(gs^\epsilon) = gs^\epsilon$
3. $\varphi(\varphi(gs^\epsilon)s^{-\epsilon}) = g$

Odteraz už budeme pracovať v pôvodnom prostredí, t.j. predpokladáme, že F je voľná grupa generovaná množinou S, U je podgrupa F a G je schreierovský systém reprezentantov vedľajších tried grupy F podľa podgrupy U. Tiež budeme používať funkciu φ namiesto funkcie Φ, pričom budeme používať len vlastnosti vyplývajúce z práve uvedených vlastností (napr. vlastnosť "prehadzovačka" uvedená v prvom dôsledku za lemou z nich vyplýva).

Lema 3.3.7 *Nech $g \in G$, $s \in S$. Ak $u = gs^\epsilon\varphi(gs^\epsilon)^{-1} \neq 1$, potom u je redukované slovo.*

Dôkaz. Keďže g a $\varphi(gs^\epsilon)$ sú redukované slová, k redukcii môže dôjsť len na styku slov g a s^ϵ alebo na styku slov s^ϵ a $\varphi(gs^\epsilon)^{-1}$.

Najprv uvažujme prvú možnosť: v tomto prípade je $g = hs^{-\epsilon}$, pričom $h \in G$, lebo G je schreierovský systém. Po dosadení je $u = h\varphi(h)^{-1} = hh^{-1} = 1$ ($\varphi(h) = h$) — spor.

Druhý prípad: $\varphi(gs^\epsilon) = hs^\epsilon = h'$, opäť je $h, h' \in G$. Vypočítajme teraz

$$u^{-1} = hs^\epsilon s^{-\epsilon}g^{-1} = h's^{-\epsilon}g^{-1} = gg^{-1} = 1$$

lebo podľa našej prehadzovačky ak $\varphi(gs^\epsilon) = h'$, tak $\varphi(h's^{-\epsilon}) = g$ a tiež $\varphi(h's^{-\epsilon}) = \varphi(h) = h = h's^{-\epsilon}$. □

Definícia 3.3.8 *Nech $g \in G$, $s \in S$. Ak $u = gs^\epsilon\varphi(gs^\epsilon)^{-1} \neq 1$, potom s^ϵ nazveme význačným prvkom slova u.*

Nech teraz $u = gs^\epsilon\varphi(gs^\epsilon)^{-1} = g's'^{\epsilon'}\varphi(g's'^{\epsilon'})^{-1} \neq 1$. Ukážeme si, že tento zápis je jednoznačný, t.j. $g = g'$ a $s = s'$. Ak majú slová g a g' rovnakú dĺžku, tak $g = g'$, lebo u je redukované slovo aj pri zápise $u = gs^\epsilon\varphi(gs^\epsilon)^{-1}$ aj pri zápise $u = g's'^{\epsilon'}\varphi(g's'^{\epsilon'})^{-1}$ a teda tieto zápisy sa po prvkoch (generátoroch a k nim inverzných) musia rovnať, teda $g = g'$ a $s = s'$.

Ak by nemali rovnakú dĺžku, a napr. g by bolo kratšie ako g', tak $g' = gs^\epsilon a$ pre vhodné (redukované, možno prázdne) a. To ale znamená, že gs^ϵ je prvok G a teda $\varphi(gs^\epsilon) = gs^\epsilon$. Preto

$$u = gs^\epsilon\varphi(gs^\epsilon)^{-1} = gs^\epsilon(gs^\epsilon)^{-1} = 1$$

— spor.

Lema 3.3.9 *Nech $u = gs^\epsilon\varphi(gs^\epsilon)^{-1} \neq 1$, $v = g's'^{\epsilon'}\varphi(g's'^{\epsilon'})^{-1} \neq 1$ sú také slová, že $uv \neq 1$. Potom po redukcii týchto slov bude výsledné slovo uv obsahovať oba význačné prvky s^ϵ a $s'^{\epsilon'}$. (Voľne povedané, význačné prvky v súčine nezmiznú.)*

Dôkaz. Sporom: nech ako prvý "zmizne" význačný prvok $s'^{\epsilon'}$, t.j. slovo $g's'^{\epsilon'}$ je začiatočné podslovo slova $\varphi(gs^{\epsilon}) \in G$ a teda $g's'^{\epsilon'}$ je prvok z G. Preto $u = g's'^{\epsilon'}\varphi(g's'^{\epsilon'})^{-1} = g's'^{\epsilon'}(g's'^{\epsilon'})^{-1} = 1$ — spor.

Nech ako prvý zmizne význačný prvok s^{ϵ}. Uvažujme o súčine $(uv)^{-1} = v^{-1}u^{-1}$. Vieme, že $v^{-1} = h's'^{-\epsilon'}\varphi(h's'^{-\epsilon'})^{-1}$ pre vhodné $h' \in G$ ($h' = \varphi(g's'^{-\epsilon'})$) a podobne $u^{-1} = hs^{-\epsilon}\varphi(hs^{-\epsilon})^{-1}$ pre vhodné $h \in G$. Teraz v uvažovanom slove $v^{-1}u^{-1}$ pri redukcii musí zmiznúť ako prvý zmiznúť význačný prvok s^{ϵ} nachádzajúci sa v druhom slove tohoto súčinu, čím sme sa dostali do situácie predošlého prípadu.

Nakoniec, nech zmiznú oba význačné prvky súčastne, t.j. $\varphi(gs^{\epsilon})^{-1}g' = 1$ a $s^{\epsilon}\varphi(gs^{\epsilon})^{-1}g's'^{\epsilon'} = 1$. Odtiaľto a z prehadzovačky plynie $uv = g\varphi(g's^{-\epsilon})^{-1} = gg^{-1} = 1$ — spor. □

Lema 3.3.10 *Nech $u_i = g_i s_i^{\epsilon_i}\varphi(g_i s_i^{\epsilon_i})^{-1}$ pre $i = 1, \ldots, k$, pričom $u_i \neq 1$ a $u_i u_{i+1} \neq 1$ pre prípustné indexy. Potom slovo $u_1 u_2 \ldots u_k$ po redukcii bude obsahovať všetky význačné prvky vsetkých svojich súčiniteľov.*

Dôkaz. Indukcia pomocou predchádzajúcej lemy. □

Teraz dokončíme dôkaz Schreierovej vety.

Veta 3.3.11 *Nech $X = \{gs\varphi(gs)^{-1};\ gs\varphi(gs)^{-1} \neq 1\ \&\ g \in G\ \&\ s \in S\}$. Potom $U = F(X)$, t.j. množina X je množina voľných generátorov podgrupy U.*

Dôkaz. Podľa našich výsledkov viem, že X generuje U. Predošlá veta hovorí, že ak zoberieme slovo $u_1 \ldots u_k$ také, že $u_i \in X \cup X^{-1}$ a také, že slovo $u_1 \ldots u_k$ nie je 1 vo voľnej grupe generovanej písmenami u_1, u_2,..., u_k, tak $u_1 \ldots u_k$ obsahuje po redukcii v $F(S)$ všetky význačné prvky všetkých svojich činiteľov. Preto je $u_1 \ldots u_k \neq 1$ a teda v množine X neplatia žiadne netriviálne vzťahy. Preto je X množina *voľných* generátorov grupy U. □

Pre počet prvkov množiny X platí nasledovné tvrdenie:

Veta 3.3.12 *Ak U je podgrupa grupy F_r indexu n, tak X má $n(r-1)+1$ prvkov, t.j. $U \cong F_{n(r-1)+1}$.*

Dôkaz. Zápisov tvaru $gs\varphi(gs)^{-1}$ je nr, potrebujeme zistiť, ktoré z nich sú rovné 1. To je práve vtedy, keď $gs = \varphi(gs)$, čo je práve vtedy, keď $gs \in G$.

To znamená, že sa nám problém zmenil na problém nájdenia počtu prvkov v G, ktoré sú tvaru gs pre $g \in G$ a $s \in S$. Nech $1 \neq h \in G$, nech $h = h's^{-1}$ pre vhodné $h' \in G$ a $s \in S$. Potom zrejme $hs = h' \in G$. Inak je $h = h's$ pre vhodné $h' \in G$ a $s \in S$. Teda každému nejednotkovému prvku $h \in G$ vieme priradiť výraz tvaru $gs\varphi(gs)^{-1}$, ktorý sa rovná 1: ak $h = h's^{-1}$ ($h' \in G$, $s \in S$), tak to bude $hs\varphi(hs)^{-1}$, ak $h = h's$ ($h' \in G$ a $s \in S$), tak to bude $h's\varphi(h's)$.

Ešte ukážeme, že ak $gs\varphi(gs)^{-1} = 1$, tak sme ho dostali z jednoznačne určeného $1 \neq h \in G$: $gs = \varphi(gs) \in G$, máme dve možnosti: (a) g a s sa krátia, (b) g a s sa nekrátia.

Prípad (a): tu je $g = hs^{-1}$ a teda $gs\varphi(gs)^{-1}$ vznikol podľa vyššie uvedenej procedúry z prvku g.

Prípad (b): v tomto prípade zápis $gs\varphi(gs)^{-1}$ vznikol z prvku $gs \in G$.

Z uvedeného vyplýva, že nejednotkových prvkov v G je práve toľko, koľko je zápisov tvaru $gs\varphi(gs)^{-1}$, ktoré sa rovnajú 1. Preto má množina X $nr - (n-1) = n(r-1)+1$ prvkov. □

Teraz načrtneme dôkaz vety obrátenej k vete 3.3.11 a k vete 3.3.3

Veta 3.3.13 *Nech F je voľná grupa generovaná množinou voľných generátorov S, G nech je schreierovský systém. Nech φ je funkcia definovaná na množine argumentov typu $h = gs^{\epsilon}$, $g \in G$, $s \in S$, $\epsilon = \pm 1$ a spĺňajúca tri vlastnosti, ktoré sme požadovali od funkcie φ za dôsledkom 3.3.6.*

Potom množina $M = \{u = gs\varphi(gs)^{-1};\ u \neq 1,\ g \in G,\ s \in S\}$ je množina voľných generátorov voľnej grupy $U = [M]$, podgrupy grupy F a G je množina reprezentantov pravých tried rozkladu podľa podgrupy U.

Dôkaz. Už uvedené tvrdenia dokazujú prvú časť tvrdenia, t.j. že M je množina voľných generátorov grupy $U = [M]$.

Na dôkaz druhej časti tvrdenia použijeme procedúru podobnú procedúre z dôkazu lemy 3.3.4. Nech $f = a_1 \ldots a_k$, $a_i \in S \cup S^{-1}$. Zadefinujeme funkciu $\phi : (S \cup S^{-1})^* \to S \cup S^{-1}$. Položíme

$$\begin{aligned} h_0 &= 1 \\ h_i &= \varphi(h_{i-1}a_i) \\ \phi(f) &= h_k \end{aligned}$$

Funkcia ϕ má nasledujúce vlastnosti: (ϵ bude vždy niektoré z ± 1, $g, g_i \in G$, $s \in S$, $a_i \in S \cup S^{-1}$ a $f, f_i \in (S \cup S^{-1})^*$)

1. $\phi(a_1 \dots a_i a_{i+1} \dots a_k) = \phi(a_1 \dots a_i s^\epsilon s^{-\epsilon} a_{i+1} \dots a_k)$
2. $\phi(g) = g$
3. $\phi(f_1 f_2) = \phi(\phi(f_1) f_2)$
4. $\phi(gs^\epsilon) = \varphi(gs^\epsilon)$
5. $\phi(gs^\epsilon \varphi(gs^\epsilon)^{-1}) = 1$
6. $f \in U$ práve vtedy, keď $\phi(f) = 1$
7. $\phi(f) = g$ práve vtedy, keď $f \in Ug$
8. ak $g_i \neq g_j$, tak $Ug_i \neq Ug_j$ (t.j. prvky g_i a g_j ležia v rôznych triedach rozkladu podľa podgrupy U)

Z posledných dvoch uvedených vlastností vyplýva, že vedľajšie triedy tvaru Ug, $g \in G$ obsahujú všetky prvky z F a že takéto triedy sú pre rôzne g_i, g_j rôzne, čo je presne záver našej vety.
Vlastnosti 1-4 sú viacmenej zrejmé, stačí si rozmyslieť definíciu ϕ. 5 vyplýva hlavne z 3 a 4.
Vlastnosť 6, implikácia $\Rightarrow$: treba si uvedomiť, že $f \in U$ znamená, že pre vhodné $g_1, \dots, g_n, s_1, \dots, s_n, \epsilon_1, \dots, \epsilon_n$ je

$$f = g_1 s_1^{\epsilon_1} \varphi(g_1 s_1^{\epsilon_1})^{-1} \dots g_1 s_n^{\epsilon_n} \varphi(g_n s_n^{\epsilon_n})^{-1}$$

a potom viacnásobným použitím 3 a 5 vždy na "oddelenie" časti $g_i s_i^{\epsilon_i} \varphi(g_i s_i^{\epsilon_i})^{-1}$ postupne od $i = 1$ až po $i = n$ dostaneme, že $\phi(f) = 1$.
Opačná implikácia: Nech $f = a_1 \dots a_k$. Keďže $\phi(f) = 1 = h_k$ a $h_0 = 1$, je

$$f = f(\phi(f))^{-1} = h_0 a_1 h_1^{-1} h_2 a_3 h_3^{-1} \cdots h_{k-1}^{-1} h_{k-1} a_k h_k^{-1}$$

pričom vieme, že každý výraz tvaru $h_i a_{i+1} h_{i+1}^{-1}$ buď 1, alebo je to priamo jeden z generátorov $gs\varphi(gs)^{-1} \in M$ (ak $a_{i+1} = s \in X$), alebo je to inverzný prvok ku takémuto generátoru (ak $a_{i+1} = s^{-1} \in X^{-1}$) a teda vidíme, že $f \in [M]$.
Vlastnosť 7, implikácia $\Rightarrow$: Nech $f = a_1 \dots a_k$. Keďže $\phi(f) = g = h_k$ a $h_0 = 1$, je

$$fg = h_0 a_1 h_1^{-1} h_2 a_3 h_3^{-1} \cdots h_{k-1}^{-1} h_{k-1} a_k h_k^{-1} g$$

takže z rovnakého dôvodu ako pri 6 vidíme, že tento zápis znamená, že $f \in [M]g$.
Opačná implikácia sa dá vyargumentovať podobne ako v 6.
Pozrime sa ešte na poslednú vlastnosť: nech $Ug_i = Ug_j$, bez újmy na všeobecnosti budeme predpokladať, že $l(g_i) \geq l(g_j)$, t.j. g_j je kratšie alebo rovnako dlhé slovo ako g_i. Vlastnosť $Ug_i = Ug_j$ je ekvivalentná s tým, že $g_i \in Ug_j$, t.j. existujú $h_1, \dots, h_n \in G$ a $s_1, \dots, s_n \in X$ s vlastnosťou

$$g_i = h_1 s_1^{\epsilon_1} \varphi(h_1 s_1^{\epsilon_1})^{-1} \dots . h_n s_1^{\epsilon_n} \varphi(h_n s_n^{\epsilon_n})^{-1} g_j$$

Slovo g_i je podľa definície redukované. Pri redukcii slova na pravej strane tejto rovnosti môžu nastať dve možnosti: význačné písmeno prvého použitého generátora, t.j. $s_1^{\epsilon_1}$ nezmizne alebo zmizne. Ak nezmizne, tak to znamená, že slovo $h_1 s_1^{\epsilon_1}$ je podslovo slova g_i a preto je to prvok G a preto $\varphi(h_1 s_1^{\epsilon_1}) = h_1 s_1^{\epsilon_1}$, čiže $h_1 s_1^{\epsilon_1} \varphi(h_1 s_1^{\epsilon_1})^{-1} = 1$, ale toto je spor, pretože podľa definície množiny M takéto prvky ako generátory nepripúšťame.

Nech význačné písmeno t.j. $s_1^{\epsilon_1}$ zmizne. Potom určite zmizne význačné písmeno posledného použitého generátora, t.j. $s_n^{\epsilon_n}$. Potom slovo $\varphi(h_n s_n^{\epsilon_n}) s_n^{-\epsilon_n}$ je podslovo slova g_j a po označení $\varphi(h_n s_n^{\epsilon_n}) = g$ ($\in G$) pomocou "prehadzovačky" dostaneme $\varphi(g s_n^{-\epsilon_n}) = h$, t.j.

$$\varphi(h_n s_n^{\epsilon_n}) s_n^{-\epsilon_n} h_n^{-1} = g s_n^{-\epsilon_n} h_n^{-1} = g s_n^{-\epsilon_n} \varphi(g s_n^{-\epsilon_n})^{-1} = 1$$

lebo $g s_n^{-\epsilon_n} \in G$. Teda aj generátor $h_n s_1^{\epsilon_n} \varphi(h_n s_n^{\epsilon_n})^{-1}$ musí byť 1, čo je opäť spor. □

Dôkaz predošlej vety v skutočnosti obsahuje podstatne viac, a to procedúru na testovanie "prináležania" prvku do podgrupy:

Veta 3.3.14 *Nech je daný schreierovský systém G a funkcia $\varphi(gs^\epsilon)$ spĺňajúca požadované tri vlastnosti. Tieto dva údaje stačia na testovanie toho, či daný prvok $f \in F$ patrí do podgrupy U určenej systémom G a funkciou φ.*

Dôkaz. Stačí použiť v predošlom dôkaze definovanú funkciu ϕ a ako test použiť vlastnosť 6 (vo forme ekvivalencie) predošlej vety. □

Ešte je zaujímavé sa zaoberať otázkou pre ktoré schreierovské systémy G vo voľnej grupe F existuje funkcia φ potrebná v predošlých dvoch vetách (keď máme danú podgrupu U a schreierovský systém G reprezentantov (ľavých) tried rozkladu F podľa U, máme tým jednoznačne určenú funkciu φ, ale keď nemáme danú podgrupu, situácia nie je vôbec jasná).

Urobme najprv niekoľko pozorovaní. Predpokladajme, že funkcia φ existuje. Pre každé $s \in S$ definujme dve funkcie ($\epsilon = \pm 1$) nasledovne: $\pi(s^\epsilon) : G \to G$, $\pi(s^\epsilon)(g) = \varphi(gs^\epsilon)$. Z vlastnosti 3 funkcie φ vyplýva, že $\pi(s^\epsilon)\pi(s^{-\epsilon})$ je identita na G. Preto sú obe zobrazenia $\pi(s)$ aj $\pi(s^{-1})$ permutácie (bijekcie) množiny G a sú si navzájom inverzné. Podľa vlastnosti 2 funkcie φ niektoré z hodnôt tejto funkcie sú určené množinou G, ale žiadna z týchto hodnôt (priamo) nezávisí od podgrupy U.

Nech $s \in S$ je pevne daný prvok, g nech prebieha množinu G. Množinu G môžeme rozložiť na dve podmnožiny $C(s^\epsilon)$ a $C^*(s^\epsilon)$

$$\begin{aligned} g \in C(s^\epsilon) \quad &\iff \quad gs^\epsilon \in G \\ g \in C^*(s^\epsilon) \quad &\iff \quad gs^\epsilon \notin G \end{aligned}$$

Ak označíme mohutnosť množiny $C(s^\epsilon)$ ako $N(s^\epsilon)$ a mohutnosť množiny $C^*(s^\epsilon)$ ako $M(s^\epsilon)$, tak

$$N(s^\epsilon) + M(s^\epsilon) = N,$$

kde N je mohutnosť množiny G.

Ak sú teraz prvky $g_i, g_j \in G$ také, že $g_i s = g_j$ (s je naše pevne dané), tak je $g_i = g_j s^{-1}$ a $g_i \in C(s)$, $g_j \in C(s^{-1})$. Týmto máme definovanú bijekciu medzi $C(s)$ a $C(s^{-1})$ a preto

$$N(s) = N(s^{-1}).$$

Ak je G konečná množina, vyplýva odtiaľto, že aj

$$M(s) = M(s^{-1}).$$

Pre nekonečnú množinu G ale posledná rovnosť nemusí platiť pre ľubovoľný schreierovský systém. Ak totiž napr. $G = \{1, s, s^2, \dots\}$, tak zrejme $M(s) = 0$ a $M(s^{-1}) = 1$. Ale existencia funkcie φ tiež zabezpečí, že $M(s) = M(s^{-1})$. Skutočne, $\pi(s)$ je bijekcia medzi G a G, ktorá prevedie množinu $C(s)$ na množinu $C(s^{-1})$ a preto musí zobraziť $C^*(s)$ na množinu $C^*(s^{-1})$. Teda rovnosť $M(s) = M(s^{-1})$ v tomto prípade platí. Táto rovnosť je aj postačujúcou podmienkou na existenciu funkcie φ pre daný schreierovský systém, ako o tom hovorí nasledujúca veta:

Veta 3.3.15 *Nech G je taký schreierovský systém vo voľnej grupe F, že pre každé $s \in S$ platí rovnosť $M(s) = M(s^{-1})$. Potom existuje funkcia $\varphi(gs^\epsilon)$ majúca vlastnosti*

1. *$\varphi(gs^\epsilon) \in G$*
2. *ak $gs^\epsilon \in G$, tak $\varphi(gs^\epsilon) = gs^\epsilon$*
3. *$\varphi(\varphi(gs^\epsilon)s^{-\epsilon}) = g$*

Pre pevné $s \in S$ je možné funkciu φ definovať nasledovne:

a) ak $gs \in G$, tak položíme $\varphi(gs) = gs$

b) ak $gs \notin G$, tak za $\varphi(gs)$ vyberieme ľubovoľný prvok z G, ale tak, aby zobrazenie $\pi(s) : g \to \varphi(gs)$ (ktoré vzniká pri definícii φ) bola bijekcia.

c) po definícii hodnôt $\varphi(gs)$ pre všetky $g \in G$ zadefinujeme hodnoty $\varphi(gs^{-1})$ tak, aby funkcia $\pi(s^{-1}) : g \to \varphi(gs^{-1})$ bola inverzná k funkcii $\pi(s)$.

Dôkaz. Bez dôkazu. □

3.4 Definícia voľného súčinu grúp

Nech G_i je množina grúp, $i \in I$, I je indexová množina. Budeme definovať voľný súčin $\prod_{i\in I} G_i$ grúp G_i podobne ako sme definovali voľnú grupu nad danou množinou generátorov.

Budeme skúmať slová

$$a_1 a_2 \dots a_k, \tag{3.2}$$

ktoré sú buď prázdne (označujeme ako 1) alebo pozostávajú z prvkov a_i, ktoré patria podgrupám G_{j_i}.

Pre tieto slová zadefinujeme reláciu *elementárnej* ekvivalencie: slovo

$$a_1 a_2 \dots a_{i-1} a_i a_{i+1} \dots a_k$$

je elementárne ekvivalentné slovu

$$a_1 a_2 \dots a_{i-1} a_{i+1} \dots a_k$$

ak je a_i jednotka v grupe G_{j_i}. Slovo

$$a_1 a_2 \dots a_{i-1} a_i a_{i+1} a_{i+2} \dots a_k$$

je elementárne ekvivalentné slovu $a_1 a_2 \dots a_{i-1} a_i^* a_{i+2} \dots a_k$ ak prvky a_i a a_{i+1} patria do jednej z grúp G_j (t.j. $G_{j_i} = G_{j_{i+1}}$) a ak $a_i a_{i+1} = a_i^*$. Ďalej, každé slovo je elementárne ekvivalentné so sebou samým.

Podľa tejto definície je relácia elementárnej ekvivalencie symetrická relácia. Povieme, že dve slová x a y sú *ekvivalentné*, ak existuje konečná postupnosť slov $x = x_1, x_2, \dots, x_n = y$ v ktorej sú každé dve po sebe nasledujúce slová (t.j. x_i a x_{i+1} pre $i = 1, 2, \dots, n-1$) elementárne ekvivalentné. Posledne definovaná relácia ako tranzitívny uzáver reflexívnej a symetrickej relácie je relácia ekvivalencie na množine všetkých slov. Všetky slová ekvivalentné s daným slovom x tvoria triedu ekvivalencie $[x]$.

Slovo $a_1 a_2 \dots a_k$ nazývame *neskrátiteľné* (*redukované*), ak je prázdne, alebo ak (1) ani jeden prvok a_i nie je jednotkou v grupe G_{j_i} a (2) prvky a_i, a_{i+1} nepatria jednej grupe G_j, $i = 1, 2, \dots, k-1$.

Teraz môžeme podobne ako v odseku definovať proces redukcie sprava: Podslovo $a_i a_{i+1}$ nazveme *zlé*, ak je buď $a_{i+1} = 1$ (vo svojej grupe), alebo ak a_i, a_{i+1} patria do tej istej grupy G_j. Nech x je slovo také, že $x = u a_i a_{i+1} v$, kde $a_i a_{i+1}$ je najpravší výskyt zlého podslova v slove x, t.j. v je neskrátiteľné slovo a prvok a_{i+2} nie je z tej istej grupy ako a_{i+1}. Ak je $a_{i+1} = 1$, položíme $r'(x) = u a_i v$, ak a_i a a_{i+1} sú z jednej grupy, tak položíme $r'(x) = u a_i^* v$, ak $a_i^* = a_i a_{i+1} \neq 1$, alebo $r'(x) = uv$ ak $a_i a_{i+1} = 1$. Ak x je tvaru $x = 1v$, v je neskrátileľné a 1 je neutrálny prvok v jednej z grúp G_i, tak položíme $r'(x) = v$. Ak je x redukované slovo, kladieme $r'(x) = x$. Nech teraz $x_0 = x$, $x_1 = r'(x)$, $x_2 = r'(x_1)$, ... a nech $k \in N$ je najmenší taký index, že $x_k = x_{k+1}$ (ak $x_i \neq x_{i+1}$, tak $l(x_i) > l(x_{i+1})$ a preto taký index existuje, inak by sme totiž dostali nekonečnú klesajúcu postupnosť prirodzených čísel). Položíme $r(x) = x_k$. Pre ľubovoľné slovo x je slovo $r(x)$ neskrátiteľné a je určené jednoznačne.

Hovoríme, že slovo $r(x)$ vzniklo zo slova x *redukciou sprava*.

Pre takto definovanú redukciu je možné dokázať vetu analogickú vete 3.1.1. Dôležité je, že platí

$$[x] = [y] \qquad \Longleftrightarrow \qquad r(x) = r(y) \tag{3.3}$$

a

$$r(xy) = r(r(x)r(y)), \tag{3.4}$$

a teda operácia súčinu definovaná ako

$$[x][y] = [xy] \tag{3.5}$$

nezávisí na výbere reprezentantov.

Platí teda veta

Veta 3.4.1 *Nech $\prod_{i\in I} G_i = \{[x]; x \text{ je slovo tvaru (3.2)}\}$. Potom binárna operácia definovaná vzťahom (3.5) je grupová operácia, t.j. $\prod_{i\in I} G_i$ je grupa.*

Grupa, ktorú sme práve definovali je v istom zmysle najvšeobecnejšia grupa obsahujúca grupy G_i ako svoje podgrupy. Toto je presne tvrdenie nasledujúcej vety

Veta 3.4.2 *Nech G je grupa generovaná svojimi podgrupami H_i, $i \in I$, nech pre všetky $i \in I$ platí $G_i \cong H_i$ a tento izomorfizmus označíme znakom φ_i. Potom je G homomorfným obrazom grupy $Q = \prod_{i\in I} G_i$.*

Dôkaz. Nech $x = a_1 a_2 \dots a_k$ je (redukované) slovo reprezentujúce prvok z Q. Položíme $\varphi([x]) = b_1 b_2 \dots b_k$, kde $b_i = \varphi_{j_i}(a_i)$ a $a_i \in G_{j_i}$. Z definície (elementárnej) ekvivalencie vyplýva, že toto je naozaj zobrazenie (ak pracujeme s redukovaným slovom x, tak korektnosť nepotrebujeme overovať, priamo vyplýva z 3.3). Z definície súčinu v Q je vidieť, že je to homorfizmus. □

3.5 Voľný súčin s amalgamáciou

Podobne ako v predošlom odseku, budeme sa zaoberať hľadaním najvšeobecnej grupy pre istú situáciu. Nech G_i pre $i \in I$ sú grupy a U_i ich podgrupy také, že všetky U_i sú navzájom izomorfné (a teda s nejakou grupou U a pre každé $i \in I$ máme vybratý konkrétny izomorfizmus $\varphi_i : U \to U_i$). Otázka je, či existuje grupa G, ktorá "obsahuje" všetky G_i ako svoje podgrupy a to tak, že všetky grupy U_i sa stotožnia (presnejšie: existujú injekcie $\imath_i : G_i \to G$ také, že $\imath_i(U_i) = \imath_j(U_j)$ a dokonca $\imath_i \circ \varphi_i^{-1} = \imath_j \circ \varphi_j^{-1}$). Ak áno, ako vyzerá najvšeobecnejšia grupa s touto vlastnosťou. Podľa vety 3.4.2 to musí byť homomorfný obraz voľného súčinu, v ktorom sa navzájom stotožnia príslušné prvky z grúp U_i a teda takáto grupa existuje. Ale vôbec nie je jasné, ako dochádza ku "stotožňovaniu" vo voľnom súčine na základe týchto stotožnení "rovnakých" prvkov z U_i.

Urobíme priamu definíciu voľného súčinu s amalgamáciou. Nech G_i, U_i, U, φ_i pre $i \in I$ sú ako je popísané vyššie.

Zaoberajme sa slovami tvaru 3.2. Na týchto slovách zadefinujeme *elementárnu ekvivalenciu* a *ekvivalenciu* podobne ako pri definícii voľného súčinu, naviac budeme len požadovať nasledujúcu vlastnosť pre elementárnu ekvivalenciu: ak je v slove $x = a_1 a_2 \dots a_i \dots a_k$ prvok $a_i = u_i \in U_{j_i}$, tak slová x a $y = a_1 a_2 \dots b_i \dots a_k$, kde $b_i = \varphi_l^{-1}(\varphi_{j_i}(a_i)) \in U_l$ (inými slovami, existuje $u_i \in U$ také, že $\varphi_l(u_i) = b_i$ a $\varphi_{j_i}(u_i) = a_i$) sú elementárne ekvivalentné.

Podobne, ako v dvoch predchádzajúcich prípadoch sa dá ukázať, že triedy ekvivalencie takto definovanej relácie tvoria grupu vzhľadom na súčin tvaru 3.5

Procedúru redukcie sprava tu však nemožno dobre uplatniť a preto sa tu postupuje podľa nasledujúceho postupu.

Každú grupu G_i môžeme napísať v tvare rozkladu na (pravé) vedľajšie triedy podľa podgrupy U_i:

$$G_i = U_i + U_i x_{i1} + U_i x_{i2} + \dots,$$

(za reprezentanta U_i vždy vyberieme 1, inak ľubovoľne, nemusí to byť spočítateľné) čo vďaka izomorfizmom φ_i možno napísať ako

$$G_i = U + U x_{i1} + U x_{i2} + \dots.$$

Preto každý prvok $g_i \in G_i$ možno jednoznačne vyjadriť buď ako $g_i = u \in U$, alebo $g_i = uz$, $u \in U$, $z = x_{ik} \neq 1$. Dá sa dokázať, že zápisy tvaru

$$f = u z_1 z_2 \dots z_k$$

($u \in U$, $z_i = x_{j_i k_i} \neq 1$) tvoria kanonické zápisy prvkov vo voľnom súčine s amalgamáciou, t.j. každý prvok je ekvivalentný práve s jedným prvkom v takomto tvare.

3.6 Kurošova veta

Veta 3.6.1 (Kuroš) *Nech $G = \prod_{i \in I} G_i$ je voľný súčin grúp. Nech $H \neq 1$ je podgrupa grupy G. Potom H je tiež voľný súčin grúp v tvare*

$$H = F \prod \alpha_j^{-1} B_j \alpha_j,$$

kde F je voľná grupa a každá z podgrúp $\alpha_j^{-1} B_j \alpha_j$ je podgrupa konjugovaná s podgrupou U_j niektorej z grúp G_i, $i \in I$.

Predpokladáme, že grupy G_i sú (až na neutrálny prvok 1) po dvoch disjunktné. Na množine $\bigcup_{i \in I} G_i$ zadefinujeme dobré usporiadanie nasledovne: najprv nech $<_I$ je dobré usporiadanie množiny I. Pre každé $i \in I$ nech je $<_i$ nejaké dobré usporiadanie množiny $G_i - \{1\}$. Teraz zadefinujeme sľúbené dobré usporiadanie $\lhd$ množiny $\bigcup_{i \in I} G_i$: Prvý prvok bude 1. Ak sú $a, b \in \bigcup_{i \in I} G_i - \{1\}$ z tej istej grupy G_i, tak položíme $a \lhd b$ práve vtedy, keď $a <_i b$. Ak $a, b \in \bigcup_{i \in I} G_i - \{1\}$ nie sú z tej istej grupy, t.j. $a \in G_i$ a $b \in G_j$ potom položíme $a \lhd b$ práve vtedy, keď $i <_I j$.

Pomocou uporiadania $\lhd$ budeme definovať *lexikografické* usporiadanie $\prec$ množiny $G = \prod_{i \in I} G_i$, presnejšie povedané množiny redukovaných slov z G. Ak $a = a_1 \dots a_k \in G$ a $b = b_1 \dots b_l \in G$ sú dve redukované slová (v zmysle definície redukovaného slova pre voľný súčin) a $k < l$, kladieme $a \prec b$ (1 ako slovo nulovej dĺžky bude prvý prvok v našom usporiadaní). Ak $k = l$ a slová a a b nie sú rovnaké, nech $i \leq k$ je prvý index taký, že $a_i \neq b_i$ (t.j. $a_1 = b_1, \dots, a_{i-1} = b_{i-1}$). Potom kladieme $a \prec b$ práve vtedy, keď $a_i \lhd b_i$. Takto definované usporiadanie je dobré usporiadanie na množine G.

Nakoniec pomocou dobrého usporiadania $\prec$ zadefinujeme tzv. *pololexikografické* usporiadanie $<$ na množine G: slovo 1 opäť položíme na prvé miesto v usporiadaní $<$. Ostatné (neprázdne) redukované slová napíšeme v tvare $\alpha\beta^{-1}$ alebo $\alpha a \beta^{-1}$, pričom slová α a β majú rovnakú dĺžku a $a \in \bigcup_{i \in I} G_i - \{1\}$ (prvý tvar použijeme pre slová párnej dĺžky a druhý pre slová nepárnej dĺžky; vždy, keď slovo napíšeme v jednom z týchto dvoch tvarov, budeme

predpokladať, že slová α a β majú rovnakú dĺžku, a $a \in \bigcup_{i\in I} G_i - \{1\}$ pre druhý tvar). Keďže sa jedná o redukované slová, vieme, že pri prvom tvare posledné písmeno (prvok) slova α a prvé písmeno (prvok) slova β^{-1} nie sú z tej istej grupy G_i a podobne pri druhom tvare, t.j. prvok a nie je z tej istej grupy ani ako posledné písmeno slova α, ani ako prvé písmeno slova β^{-1}.

Kratšie slovo je menšie v usporiadaní $<$ ako dlhšie slovo.

Nech sú teraz $a = \alpha\beta^{-1}$ a $b = \gamma\delta^{-1}$ dve slová párnej dĺžky, položíme $a < b$ ak je buď $\alpha \prec \gamma$, alebo $\alpha = \gamma$ a $\beta \prec \delta$.

Nech sú teraz $a = \alpha a'\beta^{-1}$ a $b = \gamma b'\delta^{-1}$ dve slová nepárnej dĺžky, položíme $a < b$ ak je buď $\alpha \prec \gamma$, alebo $\alpha = \gamma$ a $\beta \prec \delta$ alebo $\alpha = \gamma$ a $\beta = \delta$ a $a' \prec b'$. (Samozrejme, tu $a' \prec b'$ je ekvivalentné s $a' \lhd b'$.)

Takto definované pololexikografické usporiadanie je tiež dobré usporiadanie množiny G.

Položme teraz

$$K = \{k \in H;\, k \notin [\langle 1, k) \cap H]\},$$

kde $\langle 1, k)$ je polouzavretý interval v pololexikografickom usporiadaní $<$. (Samozrejme, $\langle 1, 1) = \emptyset$.) Množina K generuje podgrupu H a keď ju obohatíme o vhodné prvky, získame potrebnú informáciu pre zápis podgrupy H v požadovanom tvare polopriameho súčinu.

Najprv overíme fakt, že K generuje H. Ak $1 \neq k \in H$, tak $k \in K$ a preto je K neprázdna množina. Nech $k \in H$ je prvý prvok v pololexikografickom uporiadaní $<$, ktorý nepatrí do $[K]$. Potom $k \neq 1$ a podľa definície K je $k \in [\langle 1, k) \cap H]\}$ (ak $k \notin [K]$, je tým skôr $k \notin K$), t.j. je generovaný niektorými prvkami $a_1, \ldots, a_k \in H$, ktoré ho predchádzajú v usporiadaní $<$. Ale keďže $a_1, \ldots, a_k \in [K]$ (lebo k je prvý, ktorý túto vlastnosť nemá), je aj $k \in K$. Poznamenajme, že $1 \notin K$.

Teraz obohaťme množinu K. Pomôže nám nasledujúca úvaha: nech $u \neq 1$. Potom u nie je v tvare $\alpha\alpha^{-1}$. Ale u môže byť v tvare $u = \alpha a\alpha^{-1}$. Takýto prvok nazývame *konjugát*. Všetky konjugáty $u = \alpha a\alpha^{-1}$, kde $a \in G_i$ pre vhodné $i \in I$ a dané α tvoria spolu s neutrálnym prvkom podgrupu $\alpha\overline{B}_{\alpha,i}\alpha^{-1}$ konjugovanú s nejakou podgrupou $\overline{B}_{\alpha,i} \subseteq G_i$. Významnú úlohu v ďalšej konštrukcii hrajú grupy tvaru $\alpha B_{\alpha,i}\alpha^{-1} = [K \cap \alpha\overline{B}_{\alpha,i}\alpha^{-1}]$, ktoré sú opäť konjugované s nejakými podgrupami $B_{\alpha,i} \subseteq G_i$, menovite $B_{\alpha,i} = [\{b \in G_i;\, \alpha b\alpha^{-1} \in K\}]$, čo znamená, že $B_{\alpha,i}$ obsahuje prvky z G_i generované strednými prvkami konjugátov z K tvaru $\alpha b\alpha^{-1}$.

Položme

$$T = \{t \in H;\, t \in K \text{ alebo } t = \alpha a\alpha^{-1}, a \in G_i - \{1\} \text{ a } t \in \alpha B_{\alpha,i}\alpha^{-1}\}.$$

Podmienka $t \in H$ nie je žiadne obmedzenie, lebo oba členy v dizjunkcii definujúcej T nám môžu poskytnúť len prvky z H vďaka spôsobu, akým sa tam vyskytuje množina K. Aj tu upozorňujeme, že $1 \notin T$.

Nech teraz w je prvok z H. Keďže K generuje H, dá sa napísať ako slovo z K. Potom sa ale dá napísať ako slovo $w = v_1 \ldots v_n$ z $T \cup T^{-1}$ (t.j. $v_i \in T \cup T^{-1}$) s nasledujúcimi vlastnosťami: 1) neobsahuje podslovo tvaru aa^{-1} ($a \in T \cup T^{-1}$) a 2) prvky v_i, v_{i+1} nepatria do tej istej podgrupy $\alpha B_{\alpha,i}\alpha^{-1}$. Prvá vlastnosť sa dá zabezpečiť jednoducho (podobne ako pri definíci voľnej grupy či voľného súčinu) a druhá je vlastne presne zabezpečená prvkami, ktoré sme pridali do T oproti K (pridali sme práve tie prvky, ktoré zabezpečia splnenie tejto druhej podmienky - ak je totiž $v_i = \alpha a\alpha^{-1}$ a $v_{i+1} = \alpha a^*\alpha^{-1}$, kde $a, a^* \in B_{\alpha,i}$, potom v_i, v_{i+1} sú generované prvkami z množiny $K \cap \alpha B_{\alpha,i}\alpha^{-1}$, teda aj ich súčin $v_iv_{i+1} = \alpha aa^*\alpha^{-1}$ je tiež generovaný prvkami z tejto množiny a teda patrí do T — túto procedúru už robíme len pre také prvky, že $v_iv_{i+1} \neq 1$). Slová z $T \cup T^{-1}$ spĺňajúce obe uvedené podmienky nazývame *poloredukované*. Keby sme teda poloredukovanými slovami definovali nejakú grupu abstraktne (externe), výsledok by bol voľný súčin grúp tvaru $\alpha B_{\alpha,i}\alpha^{-1}$ a voľnej grupy generovanej prvakmi z K, ktoré nie sú konjugáty. Keďže sa naša podgrupa H nachádza v grupe G a teda poloredukované slová sú slová v tejto grupe, musíme ešte dokázať, že každé dve "formálne rôzne" (t.j. rôzne ako slová z $T \cup T^{-1}$) poloredukované slová sú rôzne ako prvky grupy G. Ekvivalentne, potrebujeme dokázať, že neprázdne poloredukované slovo nie je neutrálny prvok grupy G. Tým bude dôkaz o tom, že H je voľný súčin grúp v danom tvare ukončený.

Na dosiahnutie tohoto cieľa budeme skúmať, čo sa bude s poloredukovanými slovami diať, keď sa na ne začneme dívať ako na slová v grupe G — do tohoto momemntu sme sa na ne totiž dívali len pohľadu $T \cup T^{-1}$. Teraz môžu vzniknúť nové redukcie, ktoré predtým neboli možné. Podstatné je dokázať, že sa žiadne poloredukované slovo nezredukuje úplne.

Lema 3.6.2 *1. Nech $u \neq u^{-1}$, $u \in K$. Potom $u < u^{-1}$.*

2. Nech $u \in H$, $v \in K$, $u < v$, nech $w = u^\epsilon v^\sigma$ alebo $w = v^\sigma u^\epsilon$, $\epsilon, \sigma = \pm 1$. Potom w nie je pred v.

3. Nech $\alpha\beta^{-1}$, $\alpha a\beta^{-1} \in T$, kde $\alpha \neq \beta$. Potom $\alpha \prec \beta$.

Dôkaz. Prvá časť: Je $u \neq u^{-1}$. Nech teda $u^{-1} < u$. Ale $(u^{-1})^{-1} = u$, t.j. u sa dá vygenerovať menším prvkom a teda nepatrí do K.

Druhá časť: Sporom. Nech $w < v$. Vieme, že v sa dá vygenerovať prvkami u a w, ktoré sú od neho oba menšie a patria do H a teda $v \notin K$ — spor.

Tretia časť: Z podmienok plynie, že prvok $\alpha a\beta^{-1}$ nie je konjugát a teda oba prvky $u = \alpha\beta^{-1}$ a $u = \alpha a\beta^{-1}$ patria do K. Ďalej pokračujeme sporom. Nech $\beta \prec \alpha$. Zrejme je v oboch prípadoch $u \neq u^{-1}$. Potom je podľa definície pololexikografického usporiadania $u^{-1} < u$ (pre oba tvary u), čo je spor s prvou časťou tejto lemy. □

Podľa tejto lemy dostávame možné tvary prvkov v množine T:

1. $l(u)$ párne, $u = \alpha\beta^{-1}$, $\alpha \prec \beta$. Tu je $u \in K$.
2. $l(u)$ nepárne, $u = \alpha a\beta^{-1}$, $\alpha \prec \beta$. Tu je $u \in K$.
3. $l(u)$ nepárne, $u = \alpha a\alpha^{-1}$, t.j. u je konjugát generovaný konjugátmi z K toho istého typu.

Teraz uvedieme jednu technickú lemu, ktorej význam sa ukáže v dôkaze nasledujúceho tvrdenia.

Lema 3.6.3 *Nech $u \in T$, $v = \alpha a\alpha^{-1} \in T$ je konjugát, $a \in B_{\alpha,i}$. Nech $a^* \in B_{\alpha,i}$ nie je jednotka a $v^* = \alpha a^*\alpha^{-1}$. Nech $u < v$ a u, v nepatria do tej istej grupy $\alpha B_{\alpha,i}\alpha^{-1}$. Potom*

1. *ak $u < v$, potom $u < v^*$.*
2. *Nech $u < v$ a v slove w tvaru $w = u^\epsilon v^\sigma$ alebo $w = v^\sigma u^\epsilon$, $\epsilon, \sigma = \pm 1$ sa po vykrátení a vynásobení príslušných prvkov (redukcia slova w ako slova vo voľnom súčine) prvok a z výrazu $\alpha a\alpha^{-1}$ nevynásobí so svojim susedom (t.j. slovo w* bude *po redukcii vo voľnom súčine obsahovať podslovo tvaru $a\alpha^{-1}$ (alebo $a^{-1}\alpha^{-1}$, alebo αa alebo αa^{-1})). Potom ak $w < v$, tak $w^* < v^*$, kde w^* vznikne ako w, len namiesto v napíšeme v^*. (t.j. napr. ak $w = uv^{-1}$, tak $w^* = uv^{*-1}$.*

Dôkaz. (1) Ak $l(u) < l(v)$, potom aj $l(u) < l(v^*)$, t.j. $u < v^*$. Nech teda $l(u) < l(v)$, t.j. $u = \gamma b\delta^{-1}$. Pre $\gamma \neq \delta$ je $\gamma \prec \delta$, a preto buď $\gamma \prec \alpha$ alebo $\gamma = \alpha = \delta$. V prvom prípade však hneď vidieť, že $u = \gamma b\delta^{-1} < \alpha a^*\alpha = v^*$ (lebo stále je $\gamma \prec \alpha$). V druhom prípade teda $u = \alpha b\alpha^{-1}$ a keďže prvky u, v nepatria do tej istej podgrupy $\alpha B_{\alpha,i}\alpha^{-1}$, tak prvky a a b nepatria do tej istej grupy G_i. Ale keďže je $b \lhd a$, ak $b \in G_i$, $a \in G_j$, tak $i <_I j$. Potom ale $b \lhd a^*$ pre všetky nejednotkové prvky $a^* \in G_j$, t.j. $u < v^*$.

(2) Keďže sú prvky a a a^* z tej istej grupy, tak podmienka na redukciu v slove w hovorí, že $l(w) = l(w^*)$. Tiež máme $l(v) = l(v^*)$. Ak teda $l(w) < l(v)$, tak aj $l(w^*) < l(v^*)$, t.j. $w^* < v^*$.

Nech sa teda $l(w) = l(v)$. Rozoberme dva prípady: (A) $w = u^\epsilon v$ a (B) $w = u^\epsilon v^{-1}$ ($\epsilon = \pm 1$).

(A) $w = u^\epsilon v = u\alpha a\alpha^{-1} = \gamma a\alpha^{-1}$ (využívame predpoklad, že vo w musí po redukcii ostať podslovo $a\alpha^{-1}$). Preto $w < v$ a $l(w) = l(v)$ znamená, že $l(\gamma) = l(\alpha)$ a $\gamma \prec \alpha$. Potom ale $w^* = \gamma a^*\alpha^{-1} < \alpha a^*\alpha^{-1} = v^*$ pre ľubovoľné nejednotkové $a^* \in B_{\alpha,i}$

(B) $w = u^\epsilon v^{-1} = u^\epsilon \alpha a^{-1}\alpha^{-1} = \gamma a^{-1}\alpha^{-1}$ (opäť sme využili predpoklad na redukciu). Znovu vieme, že $l(\gamma) = l(\alpha)$ a teda $w < u$ keď buď (a) $\gamma \prec \alpha$ alebo (b) $\gamma = \alpha$ a $a^{-1} \lhd a$.

Rozoberme najprv (a). Tu, podobne ako v (A) hneď dostaneme $w^* = \gamma a^{*-1}\alpha^{-1} < \alpha a^*\alpha^{-1} = v^*$. Pozrime sa ešte na (b). Teraz $w = \alpha a^{-1}\alpha^{-1}$. Čiže $w = v^{-1}$. Toto ale znamená, že $u^\epsilon = 1$, čo je spor.

Podobne sa dajú dokázať prípady, keď je vo w u^ϵ na konci. □

Teraz už máme všetko pripravené na to, aby sme vyslovili a dokázali základnú vetu o tom ako sa správajú súčiny dvoch prvkov z T pri redukcii.

Veta 3.6.4 *Nech $u \neq v$, $u, v \in T$ sú prvky, ktoré neležia v jednej grupe typu $\alpha B_{\alpha,i}\alpha^{-1}$. Nech $w = u^\epsilon v^\sigma$ alebo $w = v^\sigma u^\epsilon$, $\epsilon, \sigma = \pm 1$. Potom $u < w$ a $v < w$ (v pololexikografickom usporiadaní).*

Dôkaz. Nech $u < v$. Najprv dokážeme, že $w \neq v$. Rovnosť $w = v$ totiž môže nastať len vtedy, ak (1) u=1, čo nie je možné, lebo $1 \notin T$, alebo (2) $u = v^{\pm 2}$.

Ak je v konjugát $v = \alpha a\alpha^{-1}$, tak $u = v^{\pm 2} = \alpha a^{\pm 2}\alpha^{-1}$, t.j u a v sú z jednej grupy $\alpha B_{\alpha,i}\alpha^{-1}$ — spor.

Ak v nie je konjugát, tak $l(v^{\pm 2}) > l(v)$ a teda $u > v$ — opäť spor.

Dokážeme ešte, že nie je možné, aby $w < v$. Najprv si uvedomme, že $w < v$ nemôže platiť, ak $v \in K$ — tento fakt priamo vyplýva z 2 lemy 3.6.2.

Teda v je konjugát, $v = \alpha a\alpha^{-1}$. Nech sú splnené predpoklady 2 v 3.6.3, t.j. pri redukcii v slove w nech redukcia zasiahne len $\alpha^{\pm 1}$. Nech $v^* = \alpha a^*\alpha^{-1}$ je prvok z K, ktorý je z grupy $\alpha B_{\alpha,i}\alpha^{-1}$. Podľa 1 v 3.6.3 je $u < v^*$ a $w^* < v^*$, čo podľa predošlej úvahy nemôže platiť, keďže $v^* \in K$.

Takže redukcia v slove w musí zasiahnuť prvok a v slove $v = \alpha a\alpha^{-1}$. Tento prvok sa buď vykráti, alebo vynásobí so svojim susedom pri redukcii. Čiže $u^\epsilon = \sigma a''\alpha^{-1}$, a'', $a \in G_i$, kde index i je ten istý ako index pri $v \in \alpha B_{\alpha,i}\alpha^{-1}$. Aby bolo $u < v = \alpha a\alpha^{-1}$, je buď $l(\sigma) < l(\alpha)$, alebo $l(\sigma) = l(\alpha)$ a $u = \sigma a''\alpha^{-1}$, $\sigma \prec \alpha$ (keďže a'', $a \in G_i$, u nemôže byť konjugát, potom obe nerovnosti $\sigma a''\alpha^{-1} < v$ a $\alpha a''\sigma^{-1} < v$ vedú na nerovnosť $\sigma < \alpha$, ale v takom prípade prvok $\alpha a''\sigma$ nemôže byť z K). Nech opäť $v^* = \alpha a^*\alpha^{-1}$ je prvok z K, ktorý je z grupy $\alpha B_{\alpha,i}\alpha^{-1}$. Potom v oboch prípadoch je $u < v^*$ a tiež $x = \sigma a''a^*a''^{-1}\sigma^{-1} < v^* = \alpha a^*\alpha^{-1}$ (prvky a^*, $a \in G_i$ a teda $a''^{-1}a^*a''$ je jednoprvkové

slovo). Ale zrejme $u^{-1}xu = v^*$. To znamená jednak, že $x \in H$,ale tiež, že u, x generujú v^* a teda v^* nemôže byť v K — spor. □

Dôsledok 3.6.5 *Nech $u \neq v$, $u, v \in T$ sú prvky, ktoré neležia v jednej grupe typu $\alpha B_{\alpha,i}\alpha^{-1}$. Nech $w = u^{\epsilon}v^{\sigma}$ alebo $w = v^{\sigma}u^{\epsilon}$, $\epsilon, \sigma = \pm 1$. Potom*

(a) zo žiadneho zo slov u, v sa pri redukcii slova w nevykráti viac ako polovica

(b) ak u je tvaru $\alpha\beta^{-1}$ $(\alpha < \beta)$, tak $\beta^{\pm 1}$ sa nevykráti (pri redukcii slova w). Ak sa vykráti $\alpha^{\pm 1}$, tak sa prvý znak (prvok) z $\beta^{\mp 1}$ nevynásobí so susedným prvkom (t.j. s prvkom, ktorý sa po vykrátení podslova $\alpha^{\pm 1}$ dostane "vedľa" podslova $\beta^{\mp 1}$)

(c) ak u je tvaru $\alpha a\beta^{-1}$ $(\alpha < \beta)$, tak sa podslovo $(\alpha a)^{\pm 1}$ nevykráti (pri redukcii slova w). Ak sa vykráti $\beta^{\mp 1}$, tak prvok a sa ani nevyruší, ani nevynásobí so susedným prvkom

(d) ak je u je tvaru $\alpha a\alpha^{-1} \in \alpha B_{\alpha,i}\alpha^{-1}$, tak sa podslovo $(\alpha a)^{\pm 1}$ nevykráti (pri redukcii slova w). Ak je $v\epsilon = \alpha a_1\sigma^{-1}$ (t.j. $\alpha^{\pm 1}$ sa vykráti) a a, $a_1 \in G_i$, potom a_1 je prvý prvok vo vedľajšej triede $B_{\alpha,i}a_1$

Dôkaz. (a) Keby sa vykrátila viac ako polovica slova u (v), tak by slovo w bolo pred v (u), lebo by malo menšiu dĺžku.

(b) Najprv dokážeme druhú časť: ak sa slovo $\alpha^{\pm 1}$ zo slova u vykráti, znamená to, že sa v slove v "nahradí" podslovo dĺžky $l(\alpha)$ nahradí slovom β rovnakej dĺžky. Ak by sa ešte v tomto vzniknutom slove niektoré prvky buď vynásobili alebo vykrátili, dostali by sme touto redukciou slovo menšej dĺžky ako bolo slovo v.

Teraz sa pozrime na prvú časť tvrdenia. Potrebujeme preveriť viac prípadov, urobíme len niekoľko. Nech $w = uv$.

Nech $v = \gamma\delta^{-1}$, $\gamma \prec \delta$. Ak by sa β vykrátilo, znamenalo by to, že $\gamma = \beta\omega$ pre vhodné ω (podľa (a)) . Potom ale v súčine w dostaneme $w = \alpha\omega\delta^{-1}$ (podľa druhej časti (b), ktorú sme už dokázali) a $\alpha\omega \prec \beta\omega = \gamma$, t.j. $w < u$ — spor s predošlou vetou. Rovnako to dopadne pre $v = \gamma a\delta^{-1}$ a pre $v = \gamma a\gamma^{-1}$.

Nech $w = uv^{-1}$, nech $v = \gamma\delta^{-1}$, $\gamma \prec \delta$. Potom $\delta = \beta\omega$ pre vhodné ω a $w = \alpha\omega\gamma^{-1}$ a $w^{-1} = \gamma\omega^{-1}\alpha^{-1}$ je menšie ako v, lebo $\alpha\omega \prec \beta\omega = \delta$. Podobne sa preveria všetky ostatné prípady.

(c) Vykrátenie podslova $(\alpha a)^{\pm 1}$ je v spore s (a). Rovnako vykrátenie podslova $(\beta a)^{\pm 1}$ je v spore s (a). Ešte ostalo dokázať, že ak sa $\beta^{\pm 1}$ vykráti, tak a sa nevynásobí so svojim susedom (ktorého dostane týmto krátením). Opäť treba preveriť viac možností, urobíme jednu na ilustráciu.

Nech napr. $v = \gamma b\delta^{-1}$, $(\gamma \prec \delta)$ $w = vu^{-1}$ a nech sa β vykráti. Potom buď $\beta = \delta$, alebo $\delta = \beta\omega$ pre vhodné ω nenulovej dĺžky. V prvom prípade by teda a a b patrili do tej istej grupy G_i a teda $ab = a^*$ pre vhodný prvok $a^* \in G_i$. Teda nakoniec $w = \gamma a^*\alpha^{-1}$ (viac sa už totiž krátiť ani "vynásobovať" nemôže - slovo w by sa príliš skrátilo) a keďže podľa predpokladu je $\alpha \prec \beta$ dostávame $w < u$.

V druhom prípade je $\omega = c\omega'$, kde už ω' môže byť aj prázdne slovo. Ak sa má a vynásobiť so svojim susedom, znamená to, že a a c patria do jednej grupy G_i a $ac = a^*$. Potom samozrejme $w = \gamma a(\alpha a^*\omega')^{-1}$ (ani tu už nemôže nastať žiadna ďalšia redukcia) a opäť $w < u$ (slovo $\alpha a^*\omega'$ má rovnakú dĺžku ako slovo $\delta = \beta c\omega'$ a zrejme $\alpha a^*\omega' \prec \beta c\omega'$).

(d) Vykrátenie podslova $(\alpha a)^{\pm 1}$ je v spore s (a). Ak $v = \alpha a_1\beta^{-1} (\in K)$, $a, a_1 \in G_i$ tak pre $w = uv = \alpha a^*\beta^{-1}$ $(a^* = aa_1)$ platí, že $v < w$ a teda $a_1 \lhd a^* = aa_1$ a teda a_1 je prvý v triede $B_{\alpha,i}a_1$. □

Teraz sme pripravení vysloviť a dokázať tvrdenie, ktorým uzavrieme dôkaz Kurošovej vety:

Lema 3.6.6 *Súčin $w = u_1u_2\dots u_n$, kde $u_i \in T \cup T^{-1}$ (pre $i = 1, \dots, n$), ktorý je poloredukoným slovom (t.j. $u_iu_{i+1} \neq 1$ $(i = 1, \dots, n-1)$, a dva susedené prvky u_i, u_{i+1} nepatria do tej istej grupy $\alpha B_{\alpha,i}\alpha$) je po redukcii vo voľnom súčine $G = \prod_{i\in I} G_i$ ukončený jedným z nasledujúcich podslov:*

1. *β^{-1}, ak $u_n = \alpha\beta^{-1}$, $\alpha \prec \beta$*
2. *$b^*\alpha^{-1}$, ak $u_n = (\alpha\beta^{-1})^{-1}$, $\alpha \prec \beta$*
3. *a^*b^{-1}, ak $u_n = \alpha a\beta^{-1}$, $\alpha \prec \beta$*
4. *$a^{-1}\alpha^{-1}$, $u_n = (\alpha a\beta^{-1})^{-1}$, $\alpha \prec \beta$*
5. *$a^*\alpha^{-1}$, ak $u_n = \alpha a\alpha^{-1}$*

Pritom b^* v prípade 2) a a^* v prípade 5) sú prvky (písmená), ktoré v súčine w bezprostredne predchádzajú u_n, alebo prvky, ktoré vzniknú vynásobením s analogickými prvkami súčinu (podslova) u_{n-1}; prvok a^* v 3) je podobne ako vyššie, prípadne môže vzniknúť vynásobením podslov u_{n-2}, u_{n-1} a u_n.

Dôkaz. Indukciou cez n. Pre $n = 1$ to zrejme platí. Pre $n = 2$ to priamo vyplýva z predchádzajúceho dôsledku. Pri prechode od n ku $n + 1$ len na každý z piatich možných zakončení uvedených v znení lemy a každú z piatich

možností, ako môže vyzerať podslovo u_{n+1} aplikujeme predchádzajúci dôsledok. V jednom prípade budeme potrebovať ešte urobiť jedno nové pozorovanie: Môže sa stať, že pre $u_n = \alpha a \alpha^{-1}$ sa α vykráti a a sa vynásobí s prvkom a'^{-1} z podslova $u_{n-1} = \sigma a' \alpha^{-1}$ a podobne že to dopadne s $u_{n+1} = \alpha a'' \lambda^{-1}$. Potom podľa časti (d) predošlej lemy dostaneme, že a' a a'' sú prvými prvkami vo svojich triedach $B_{\alpha,i}a'$ a $B_{\alpha,i}a''$. Ak by teraz bolo $a'^{-1}aa'' = 1$ (to by totiž znamenalo, že u_n sa celkom "stratilo" a keďže o vzťahu medzi σ a λ nevieme vôbec nič, mohlo by to mať zlé následky — tieto dve slová by sa možno mohli (čiastočne) krátiť a teda by nám neplatilo tvrdenie bodu 3)), tak $aa'' = a'$ a teda je $a' \in B_{\alpha,i}a''$, t.j. $B_{\alpha,i}a' = B_{\alpha,i}a''$. Teda a' a a'' sú prvými prvkami v triede $B_{\alpha,i}a'$ a teda $a' = a''$. To ale znamená, že a je konjugovaný s 1 a teda je to 1, t.j. $u_n = 1$ — spor. Preto $a'^{-1}aa'' \neq 1$ a redukovaný zápis podslova $u_{n-1}u_nu_{n+1}$ má tvar $\sigma a'^{-1}aa''\lambda^{-1}$. Toto je jediný prípad, keď môže redukcia zasiahnuť tri po sebe idúce členy poloredukovaného súčinu $w = u_1u_2 \dots u_n$ a spája prípad 5) (ako možný výsledok indukčného predpokladu) s prípadom 3) ako možnou hodnotou pre u_{n+1}. (viď poznámku o možnom pôvode prvku a^* z prípadu 3)). □

Vďaka tomu, že poznáme možné zakončenia (a tie sú neprázdne) slov po redukcii vo voľnom súčine dostávame ako špeciálny prípad, že pre poloredukované slovo w platí $w \neq 1$. Teda H je voľný súčin (nekonečných cyklických grúp generovaných prvkami tvaru $\alpha\beta^{-1}$ a $\alpha a \beta^{-1}$ ($\alpha \prec \beta$) a podgrúp tvaru $\alpha B_{\alpha,i}\alpha^{-1}$, ktoré sú konjugované s podgrupami $B_{\alpha,i}$ grúp G_i).

Kapitola 4

Moduly a okruhy

4.1 Okruhy a moduly ako priame súčiny

V celej tejto kapitole budeme pracovať s okruhmi s jednotkou. Dôsledkom tejto dohody je fakt, že každý homomorfizmus musí prenášať jednotku na jednotku.

Najprv uvedieme tvrdenie, ktoré platí ako pre moduly, tak aj pre okruhy, formuláciu uvedieme pre moduly.

Veta 4.1.1 *Nech T je podmnožina modulu A. Potom ľubovoľný podmodul B modulu A taký, že $B \cap T \subseteq \{0\}$ je obsiahnutý v niektorom module M, ktorý je maximálny vzhľadom na túto vlastnosť (t.j. na vlastnosť $M \cap T \subseteq \{0\}$).*

Pre okruhy treba zameniť slovo "modul" na "okruh" a slovo "podmodul" na "ideál"

Dôkaz. Pozrime sa na množinu

$$X = \{P;\ (B \subseteq P)\ \&\ P \text{ je podmodul modulu } A\ \&\ (P \cap T \subseteq \{0\})\}$$

podmodulov P modulu A obsahujúcich B, ktorých prienik s T obsahuje nanajvýš prvok 0. Samozrejme, $B \in X$, t.j. X je neprázdna množina. Prvky množiny X sú usporiadané reláciou inklúzie, nech $\{B_i;\ i \in I\}$ je neprázdna podmnožina X, ktorá je lineárne usporiadaná reláciou inklúzie. Potom $\Cup\{B_i;\ i \in I\}$ je tiež prvkom množiny X a preto podľa Zornovej lemy má množina X maximálny prvok. □

Nech je okruh R súčin modulov $R_i, i \in I$. Prvky $e_i \in R$ definované vzťahmi $e_i(j) = 1$ pre $i = j$ a $e_i(j) = 0$ pre $i \neq j$ majú nasledujúce vlastnosti: sú to tzv. centrálne prvky okruhu R, t.j pre všetky $r \in R$ a každé $i \in I$ platí $e_i r = r e_i$; sú to tzv. idempotentné prvky, t.j. platí pre ne rovnica $x \cdot x = x$ (t.j. pre všetky $i \in I$ platí $e_i \cdot e_i = e_i$); tvoria ortogonálny systém, t.j. pre $i \neq j$ je $e_i \cdot e_j = 0$.

Ak je prvok e centrálny idempotentný prvok okruhu R, potom je $e, 1 - e$ ortogonálny systém centrálnych idempotenov. Totiž $(1-e)^2 = 1 - e - e + e^2 = 1 - e$ (idempotentnosť), pre $r \in R$ platí $(1-e)r = r - er = r - re = r(1-e)$ (centrálnosť), a tiež $e(1-e) = e - e^2 = e - e = 0$ (ortogonálnosť systému).

Zrejme každý prvok $r \in R$ vieme napísať v tvare

$$r = er + (1-e)r,$$

kde $er \in eR$ a $(1-e)r \in (1-e)R$. Tento zápis je jednoznačný (ako zápis $r = x + y, \quad x \in eR, y \in (1-e)R$). Je to preto, lebo ak $r = ex + (1-e)y$, tak $er = e(ex + (1-e)y) = e^2x + e(1-e)y = ex$ a podobne $(1-e)r = (1-e)(ex+(1-e)y) = (1-e)ex+(1-e)^2y = (1-e)y$. To znamená, že okruh R je priamym súčinom ideálov (overte, že sú naozaj ideály!) eR a $(1-e)R$ a teda R je izomorfný priamemu súčinu $eR \times (1-e)R$. Treba si uvedomiť, že ideály eR a $(1-e)R$ sú okruhy: jednotky v nich sú po rade e a $1-e$. Samozrejme, akonáhle $e \neq 1, e \neq 0$, tak to nie sú podokruhy okruhu R, lebo podokruh musí mať rovnakú jednotku ako okruh.

V skutočnosti, ideál I okruhu R je okruhom práve vtedy, keď je priamym sčítancom (činiteľom) v okruhu R - t.j. ak existuje iný okruh S taký, že $R \cong I \times S$. Skutočne, ak okruh I je ideál okruhu R a e je jednotka I (potrebujeme odlíšiť jednotku 1 okruhu R od jednotky okruhu (ideálu) I), potom $I = eR$, $e^2 = e$, t.j e je idempotentný prvok R, keďže I je ideál, pre každé $r \in R$ je $er, re \in I$ a preto $er = e(er) = (er)e = e(re) = re$, lebo e je jednotka v I. T.j. e je centrálny prvok okruhu R. To znamená, že $I = eR$ a $R \cong I \times (1-e)R$.

Poznámka. Keď potrebujeme pri okruhoch hovoriť o priamom súčte dvoch (pod)okruhov A, B okruhu R, t.j. chceme napísať $R = A \oplus B$, tak vyžadujeme jednak

1) aby sa každý prvok z R dal jednoznačne napísať v tvare $a + b$ pre nejaké $a \in A$, $b \in B$, ale tiež aby

2) pre $a \in A$, $b \in B$ platilo, že $ab = 0$.

Táto druhá podmienka je ekvivalentná s tým, že A, B sú ideály. Totiž ak napr. $a \in A$ a $r = c + d \in R$, pričom $c \in A$, $d \in B$, tak $a(c + d) = ac + ad = ac + 0 = ac \in A$, lebo $a, c \in A$ a A je okruh, podobne sa dá dokázať, že $(c + d)a \in A$, teda A je obojstranný ideál. Naopak, nech je A ideál, $a \in A$, $b \in B$. Potom $ab \in A$ (lebo $a \in A$) a tiež $ab \in B$ (lebo $b \in B$) ale v prieniku $A \cap B$ je len nulový prvok (inak by sme prvok c z prieniku vedeli napísať dvoma spôsobmi $c + 0 = 0 + c$).

Podmienky 1) a 2) vychádzajú z izomorfizmu okruhu R ako súčinu okruhov, t.j. $R \simeq A \times B$

Uvedené úvahy môžeme ľahko zovšeobecniť na konečné ortogonálne systémy centrálnych idempotentov, ako o tom hovorí nasledujúca veta.

Veta 4.1.2 *Nasledujúce tvrdenia sú ekvivalentné:*

a) Okruh R je priamy súčin okruhov R_i $(i = 1, \ldots, n)$.

b) Existuje ortogonálny systém centrálnych idempotentov $e_i \in R$ $(i = 1, \ldots, n)$ takých, že $1 = \sum_{i=1}^{n} e_i$ a $e_i R \cong R_i$.

c) Okruh R je priamy súčin ideálov K_i takých, že pre všetky vhodné i platí $K_i \cong R_i$.

Nech modul A je priamy súčin $R-$modulov $\{A_i; i \in I\}$, t.j. $A = \Pi_{i \in I} A_i$. Uvažujme o kanonických surjektívnych homomorfizmoch $\pi_i : A \to A_i$ a injektívnych homomorfizmoch $\kappa_i : A_i \to A$, pre ktoré platí $\pi_i(a) = a(i)$, $\kappa_i(a_i)(j) = a_i$ pre $i = j$ a $\kappa_i(a_i)(j) = 0$ pre $i \neq j$.

Potom pre kompozíciu platí:

$$\pi_i \circ \kappa_i = 1 \qquad (1 \text{ je identita na } A_i) \text{ a}$$

$$\pi_i \circ \kappa_j = 0 \qquad \text{ak } i \neq j \qquad (0 \text{ je triviálne zobrazenie})$$

Poznamenajme, že π_i existuje aj pre okruhy, ale pre okruhy κ_i nie sú homomorfizmy (homomorfizmus musí zobraziť jednotku na jednotku).

Definícia 4.1.3 *Množina $\{a \in A = \Pi_{i \in I} A_i; a(i)$ je nenulové pre konečne veľa $i \in I\}$ sa nazýva (vonkajší) priamy súčet modulov $\{A_i; i \in I\}$ a označujeme ho*

$$\sum_{i \in I}{}^{\oplus} A_i.$$

$\sum_{i \in I}{}^{\oplus} A_i$ je tiež $R-$modul, pre konečnú indexovú množinu je priamy súčin a priamy súčet to isté. Priamy súčet dvoch modulov budeme bežne písať ako $A \oplus B$. Pre kanonické homomorfizmy π_i a κ_i platia v prípade priamych súčtov všetky uvedené vzťahy, ale naviac ešte má pre všetky $a \in \sum_{i \in I}{}^{\oplus} A_i$ zmysel a platí

$$\sum_{i \in I} \kappa_i \circ \pi_i(a) = a.$$

Túto rovnosť môžeme zapísať ako

$$\sum_{i \in I} \kappa_i \circ \pi_i = 1$$

(opäť, 1 tu označuje identitu, teraz na množine $\sum_{i \in I}{}^{\oplus} A_i$).

Ak teda uvažujeme o homomorfizmoch $\varepsilon_i = \kappa_i \circ \pi_i$, predošlé rovnosti znamenajú, že $\varepsilon_i \circ \varepsilon_i = \varepsilon_i$, $\varepsilon_i \circ \varepsilon_j = 0$ ak $i \neq j$ a naviac pre všetky $a \in \sum_{i \in I}{}^{\oplus} A_i$ je $\sum_{i \in I} \varepsilon_i(a) = a$. Budeme hovoriť, že systém $\varepsilon_i; i \in I$ tvorí úplný systém ortogonálnych idempotentných endomorfizmov modulu $\sum_{i \in I}{}^{\oplus} A_i$.

Pre tento prípad platí nasledovná analógia predošlej vety.

Veta 4.1.4 *Nasledujúce tvrdenia sú ekvivalentné:*

a) $R-$modul A je izomorfný (vonkajšiemu) priamemu súčtu $\sum_{i \in I}{}^{\oplus} A_i$.

b) $R-$modul A má úplný systém ortogonálnych idempotentných endomorfizmov $\varepsilon_i; i \in I$ taký, že pre všetky $i \in I$ platí $\varepsilon_i A \cong A_i$.

c) $R-$modul A je izomorfný (vonkajšiemu) priamemu súčtu svojich podmodulov $\{B_i; i \in I\}$ (t.j. $A \cong \sum_{i \in I}{}^{\oplus} B_i$) takých, že pre všetky $i \in I$ platí $B_i \cong A_i$

4.2 Artinovské a noetherovské moduly

Definícia 4.2.1 *Modul A sa nazýva artinovský, ak každá neprázdna množina podmodulov modulu A má minimálny prvok.*

Modul A sa nazýva noetherovský, ak každá neprázdna množina podmodulov modulu A má maximálny prvok.

Podobne môžeme definovať artinovské (Emil Artin) a noetherovské (Emmy Noether) okruhy - v predošlej defnícii treba zameniť slovo modul slovom okruh a slovo podmodul slovom ideál.

Nasledujúce dve vety hovoria o ekvivalentnej definícii týchto pojmov pomocou tzv. podmienok na reťazce (chain conditions):

Veta 4.2.2 *Modul A je artinovský práve vtedy, keď pre každú postupnosť podmodulov*

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$$

existuje $n \in N$ také,že pre všetky $k \geq n$ platí, že $A_n = A_k$.

Modul A je noetherovský práve vtedy, keď pre každú postupnosť podmodulov

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$$

existuje $n \in N$ také,že pre všetky $k \geq n$ platí, že $A_n = A_k$.

Pre ilustráciu uveďme dôkaz pre artinovskosť.

Dôkaz. Nech je modul A je artinovský a zoberme postupnosť jeho podmodulov

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$$

Podľa predpokladu má množina $A_1, A_2, A_3, \ldots$ minimálny prvok, nech teda A_n je minimálny prvok. Minimalita znamená, že pre všetky m platí $A_m \supseteq A_n$. Potom vďaka na inklúziám $A_n \supseteq A_{n+k}$ platí $A_n = A_{n+1} = A_{n+3} = \cdots$.

Naopak, nech modul A nie je artinovský. Zoberme neprázdnu množinu M, ktorá nemá minimálny prvok. Zoberme $A_1 \in M$. A_1 nie je minimálny prvok M, t.j. v M existuje modul A_2, ktorý je menší ako A_1, t.j. $A_1 \supsetneq A_2$. Ďalej môžeme pokračovať indukciou: ak sme už našli $A_n \in M$ s tým, že $A_1 \supsetneq A_2 \supsetneq \cdots \supsetneq A_n$, vieme, že A_n nie je minimálny prvok v M a preto v M existuje od neho menší A_{n+1}, čiže postupnosť vieme vždy predĺžiť o jeden člen a takto vytvoriť nekonečnú postupnosť $A_1 \supsetneq A_2 \supsetneq \cdots \supsetneq A_n \supsetneq \cdots$, ktorá sa teda nikdy "nestabilizuje".

□

Veta 4.2.3 *Modul A je noetherovský práve vtedy, keď každý jeho podmodul je konečnegenerovaný.*

Dôkaz. Nech je A noetherovský, B jeho podmodul, položme

$$M = \{C \subseteq B; C \text{ je konečne generovaný podmodul modulu } B\}$$

Množina M je zrejme neprázdna množina podmodulov modulu A, lebo obsahuje napr. podmodul $\{\mathbf{0}\}$ a každý jej prvok ako podmodul podmodulu B je aj podmodul modulu A. Vďaka noetherovskosti má maximálny prvok, označme ho C. Dokážeme, že $B = C$. Zrejme $C \subseteq B$. Nech existuje $b_0 \in B \setminus C$, nech C je generovaný prvkami $b_1, \ldots, b_n$, t.j. $C = [b_1, \ldots, b_n]$. Potom $[b_0, b_1, \ldots, b_n]$ je konečne generovaný podmodul modulu B, ktorý je vlastnou nadmnožinou podmodulu C, čo je spor s jeho maximalitou.

Naopak, nech A nie je noetherovský. Potom existuje nekonečná postupnosť jeho podmodulov

$$A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \cdots$$

Potom očividne, podmodul $B = \bigcup\{A_i; i = 1, 2, \ldots\}$ nie je konečne generovaný. Totiž, každá konečná množina prvkov $b_1, \ldots, b_n \in B$ musí byť obsiahnutá v niektorom A_i a teda $[b_1, \ldots, b_n] \subseteq A_i$ a kedže $A_i \subsetneq A_{i+1} \subseteq B$, tak určite prvky $b_1, \ldots, b_n$ negenerujú podmodul B. □

Predchádzajúce dve vety ukazujú, že konečnorozmerné vektorové priestory sú artinovské a noetherovské moduly zároveň.

Grupa $(Z, +)$ ako modul nad okruhom $(Z, +, \cdot)$ je noetherovský modul, ale nie je artinovský modul.

Príklad artinovského modulu, ktorý nie je noetherovský:

Uvažujme o nasledovnom podmodule modulu Q/Z nad Z (t.j. racionálne čísla z intervalu $\langle 0, 1)$ sčítavané "modulo 1"): Nech p je prvočíslo, pre $i = 1, \ldots$ položme $A_{p^i} = \{0, \frac{1}{p^i}, \frac{2}{p^i}, \cdots, \frac{p^i-1}{p^i}\}$, tiež definujme $A_1 = A_{p^0} = \{0\}$. Potom $A_1 \subsetneq A_p \subsetneq A_{p^2} \subsetneq \cdots \subsetneq A_{p^i} \subsetneq \cdots$ a položme $G = \bigcup_{i=0}^{\infty} A_{p^i}$

G je grupa ($Z-$modul), ktorá má zaujímavé vlastnosti, jedna z nich je, že každá jej vlastná podgrupa je cyklická (to hneď dokážeme), ale sama nie je cyklická. V literatúre sa (izomorfný variant) dá nájsť pod označením $Z(p^\infty)$.

Priamo z konštrukcie G je vidieť, že to nie je noetherovský modul. Dokážme, že každá vlastná podgrupa je cyklická. Nech $H \subseteq G$ je podgrupa. Máme dve možnosti - H je konečná alebo je nekonečná. Ak je konečná, je podmnožinou (podgrupou) niektorej z A_{p^i}, ktorá je cyklická a preto je aj H cyklická. Ak je nekonečná, dokážeme, že je totožná s G a teda nie je vlastná. Nech $i \in N$, keďže H je nekonečná a A_{p^i} konečná, existuje prvok $a \in H$, $a \notin A_{p_i}$. Potom $a = \frac{m}{p^k}$ pre $k > i$ a m nesúdeliteľné s p^k, t.j. nesúdeliteľné s p. Potom existujú $s, t \in Z$ také, že $m \cdot s + t \cdot p^k = 1$ a preto platí, že

$$\frac{1}{p^k} = \frac{s \cdot m + t \cdot p^k}{p^k} \equiv s \cdot \frac{m}{p^k} \mod 1$$

čiže $\frac{1}{p^k} \in [a]$ a teda $A_{p^k} \subseteq [a] \subseteq H$. Takže sme dokázali, že pre každé $i \in N$ je $A_{p^i} \subseteq H$ a preto $G = H$, teda naozaj každá vlastná podgrupa je cyklická, konečná a z uvedeného dôkazu je vidieť, že naviac každá vlastná podgrupa je jedna z A_{p^i}, žiadne iné vlastné podgrupy grupa G nemá.

Teraz dokážeme, že G je artinovský modul. Nech $B_1 \supseteq B_2 \supseteq \cdots \supseteq B_i \supseteq \cdots$ sú podmoduly, t.j. podgrupy. Potom existujú také čísla $i_1, i_2, \ldots$, že $B_1 = A_{p^{i_1}}$, $B_2 = A_{p^{i_2}}$, $B_3 = A_{p^{i_3}}$,... Podmienka $B_k \supseteq B_{k+1}$ znamená, že $A_{p^{i_k}} \supseteq A_{p^{i_{k+1}}}$, t.j. $i_k \geq i_{k+1}$, preto je $i_1 \geq i_2 \geq i_3 \ldots$ a je to postupnosť prirodzených čísiel, ktorá sa musí "zastaviť". Preto je G artinovský modul.

Platí Hopkinsova veta - artinovský modul nad artinovským okruhom je noetherovský, ktorá trochu naznačuje, prečo je tento príklad takýto zložitý.

Veta 4.2.4 *Zväz podmodulov modulu A je modulárny, t.j. pre podmoduly B, C, D modulu A, také, že $B \subseteq C$ platí*

$$C \cap (D + B) = (C \cap D) + B$$

Dôkaz. Inklúzia $\supseteq$ platí, lebo $(C \cap D) \subseteq C$ aj $B \subseteq C$ (a teda $(C \cap D) + B \subseteq C$) a podobne $(C \cap D) \subseteq D + B$ aj $B \subseteq D + B$ (a teda $(C \cap D) + B \subseteq D + B$), sumárne teda $C \cap (D + B) \supseteq (C \cap D) + B$.

Opačná inklúzia: Nech $c = d + b \in C \cap (D + B)$, t.j. $c \in C,\ d \in D,\ b \in B$. Potom $d = c - b$ a keďže $c \in C$, $b \in B \subseteq C$ tak $d = c - b \in C$. Preto $d \in C \cap D$ a teda zápis $b + d \in B + C \cap D$, t.j. $c = d + b = b + d \in B + C \cap D$. □

Veta 4.2.5 *Nech B je podmodul modulu A. Modul A je artinovský (noetherovský) práve vtedy, keď sú oba moduly B a A/B artinovské (noetherovské).*

T.j. ak je A artinovský (noetherovský), tak je aj (každý) podmodul B a aj faktorový modul A/B artinovský (noetherovský). A tiež naopak, ak pre čo len jediný podmodul B modulu A je aj B aj A/B artinovský (noetherovský), tak už je A artinovský (noetherovský).)

Dôkaz.
Urobíme dôkaz pre artinovskosť, druhý je analogický/duálny.
Implikácia $\Rightarrow$: Nech B je podmodul modulu A, nech $B_1 \supseteq B_2 \supseteq B_3 \supseteq \cdots$ sú podmoduly modulu B. Potom sú to aj podmoduly modulu A a keďže je A artinovský, táto postupnosť sa stabilizuje.

Nech $B_1 \supseteq B_2 \supseteq B_3 \supseteq \cdots$ sú podmoduly faktorového modulu A/B. Keď použijeme kanonický homomorfizmus $\psi : A \mapsto A/B$ ($\psi(a) = a + B$), vieme, že $\psi^{-1}(B_i)$ sú podmoduly modulu A a keďže zrejme platí

$$\psi^{-1}(B_1) \supseteq \psi^{-1}(B_2) \supseteq \psi^{-1}(B_3) \supseteq \cdots$$

táto postupnosť sa stabilizuje, ale to znamená, že aj postupnosť $B_1 \supseteq B_2 \supseteq B_3 \supseteq \cdots$ sa musí stabilizovať.

Implikácia $\Leftarrow$: Nech A je taký, že pre jeden (dokonca to stačí takto) podmodul B modulu A platí, že aj B aj A/B sú artinovské. Zoberme postupnosť $A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$ podmodulov modulu A. Potrebujeme dokázať, že táto postupnosť sa stabilizuje.

Postupnosť $B \cap A_1 \supseteq B \cap A_2 \supseteq B \cap A_3 \supseteq \cdots$ je postupnosť podmodulov modulu B a preto sa vďaka jeho artinovskosti stabilizuje, povedzme pre k platí $B \cap A_k = B \cap A_{k+1} = B \cap A_{k+2} = \cdots$.

Podobne postupnosť $(A_1 + B)/B \supseteq (A_2 + B)/B \supseteq (A_3 + B)/B \supseteq \cdots$ sú podmoduly modulu A/B a preto sa stabilizuje, povedzme pre l platí $(A_l + B)/B = (A_{l+1} + B)/B = (A_{l+2} + B)/B = \cdots$. To ale znamená, že aj postupnosť "čitateľov" sa stabilizuje, t.j. $A_l + B \supseteq A_{l+1} + B = A_{l+2} + B = \cdots$.

Zoberme teraz $n = \max\{k, l\}$, t.j. platí aj $B \cap A_n = B \cap A_{n+1} = B \cap A_{n+2} = \cdots$ aj $A_n + B = A_{n+1} + B = A_{n+2} + B = \cdots$.

Počítajme

$$A_n = A_n \cap (A_n + B) = A_n \cap (A_{n+1} + B) = A_n \cap (B + A_{n+1}) = (A_n \cap B) + A_{n+1} = (A_{n+1} \cap B) + A_{n+1} = A_{n+1}$$

Druhá a predposledná rovnosť platia vďaka stabilizácii príslušných postupností a štvrtá vďaka modularite. Prvá a posledná sú očividné. Aj postupnosť $A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$ sa teda stabilizuje. □

Dôsledok 4.2.6 *Konečný priamy súčin modulov je artinovský (noetherovský) práve vtedy, keď je každý z činiteľov artinovský (noetherovský).*

Definícia 4.2.7 *Kompozičným radom modulu A nazývame takú konečnú rastúcu postupnosť podmodulov*

$$\{\mathbf{0}\} = A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \cdots \subsetneq A_n = A$$

pre ktorú platí, že sa nedá "zjemniť", t.j. medzi žiadne dva moduly A_i, A_{i+1} už nemôžeme vložiť podmodul B taký, že $A_i \subsetneq B \subsetneq A_{i+1}$.

Tu by sme si mali pripomenúť niektoré vety, ktoré poznáme pre normálne podgrupy nejakej grupy, vďaka modularite (zväzu podmodulov) platia aj v prípade modulov a ich podmodulov.

Veta 4.2.8 *Nech A, B, H sú podmoduly modulu M, $A \subseteq B$. Potom $(B+H)/(A+H) \cong B/(A \cap (B+H))$.*

Dôkaz.
Pozrime sa na diagram

$$B \xrightarrow{i} (B+H) \xrightarrow{\psi} (B+H)/(A+H),$$

kde $i : B \to B+H$ je vnorenie ako podmnožina a $\psi : (B+H) \to (B+H)/(A+H)$ je kanonický homomorfizmus modulu na faktorový modul. Jadro kompozície $\operatorname{Ker}\psi \circ i$ je očividne $B \cap (A+H)$, čo je vďaka modularite $A \cap (B+H)$. Naviac, kompozícia $\psi \circ i$ je surjektívna a preto

$$B/\operatorname{Ker}\psi \circ i \cong (B+H)/(A+H)$$

čo vďaka predošlým úvahám je presne tvrdenie vety. □

Veta 4.2.9 *(Schreierova veta o zjemnení) Nech $\{0\} = A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots \subseteq A_n = M$, $\{0\} = B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots \subseteq B_m = M$ sú postupnosti podmodulov modulu M. Potom existujú zjemnenia $\{0\} = A'_1 \subseteq A'_2 \subseteq A'_3 \subseteq \cdots \subseteq A'_k = M$ a $\{0\} = B'_1 \subseteq B'_2 \subseteq B'_3 \subseteq \cdots \subseteq B'_k = M$ (A' pre A, B' pre B) týchto dvoch postupností, ktoré majú rovnakú dĺžku a sú faktorovo izomorfné.*

Dôkaz. Pre dôkaz sa tu odvoláme na dôkaz, ktorý sme robili pri grupách (veta 2.3.3). □

Veta 4.2.10 *Modul A má kompozičný rad práve vtedy, keď je artinovský a noetherovský.*

Dôkaz. $\Rightarrow$: Nech $A = A_1 \supsetneq A_2 \supsetneq A_3 \supsetneq \cdots \supsetneq A_n = \{0\}$ je kompozičný rad. Dokážme napr. artinovskosť: Nech $B_1 \supsetneq B_2 \supsetneq B_3 \supsetneq \cdots \supsetneq B_n \supsetneq \cdots$ je postupnosť podmodulov modulu A.

Keď zoberieme $n+1$ členov postupnosti B_i a pripojíme k nim $B_0 = A$ (robíme to len v prípade, že $A \neq B_1$) a položíme $B_{n+2} = \{0\}$ (toto treba urobiť, lebo podľa predpokladu je pôvodné $B_{n+2} \neq \{0\}$), t.j. budeme pracovať s radom, ktorý obsahuje aspoň $n+1$ "skokov" (relácia $\supsetneq$). Podľa vety o zjemnení existuje spoločné zjemnenie, ale toto spoločné zjemnenie teda na jednej strane musí mať aspoň $n+1$ skokov (vďaka $B-$čkam), ale tiež vďaka kompozičnosti $A-$čiek vieme, že toto zjemnenie nemôže mať viac ako n skokov — spor. □

Poznámka. Jordan-Hölderova veta hovorí, že ak má modul kompozičný rad, tak všetky kompozičné rady majú rovnakú dĺžku (rovnako veľa podmodulov) a všetky takéto kompozičné rady sú faktorovo izomorfné (t.j. množina faktorových modulov

$$\{A_n/A_{n-1}, A_{n-1}/A_{n-2}, \ldots, A_3/A_2, A_2/A_1\})$$

je určená až na izomorfizmus jednoznačne. Toto tvrdenie platí pre moduly rovnako ako pre grupy.

Jedna zo zaujímavých vlastností vyplývajúca z artinovskosti/noetherovskosti je uvedená v nasledujúcej vete (porovnajte s príslušnými tvrdeniami o konečnorozmerných vektorových priestoroch).

Veta 4.2.11 *Nech A je artinovský modul, $\varphi : A \mapsto A$ je homomorfizmus. Potom φ je bijekcia práve vtedy, keď φ je injekcia.*

Nech A je noetherovský modul, $\varphi : A \mapsto A$ je homomorfizmus. Potom φ je bijekcia práve vtedy, keď φ je surjekcia.

Dôkaz. Nech A je artinovský a φ injekcia. Vďaka vlastnosti $X \subseteq Y \subseteq A \Rightarrow \varphi(X) \subseteq \varphi(Y)$ vidíme, že platí

$$A \supseteq \varphi(A) \supseteq \varphi^2(A) \supseteq \varphi^3(A) \supseteq \cdots \supseteq \varphi^n(A) \supseteq \cdots$$

Z artinovskosti A vyplýva, že existuje $n \in N$ také, že $\varphi^n(A) = \varphi^{n+1}(A) = \varphi^{n+2}(A) = \cdots$.

Potrebujeme dokázať, že φ je surjekcia, zoberme teda $b \in A$ a skúsme nájsť $a \in A$ také, že $\varphi(a) = b$. Začnime tým, že $\varphi^n(b) \in \varphi^n(A) = \varphi^{n+1}(A)$, čiže $\varphi^n(b) \in \varphi^{n+1}(A)$ a preto existuje $a \in A$ také, že $\varphi^n(b) = \varphi^{n+1}(a) = \varphi^n(\varphi(a))$. Zobrazenie $\varphi^n : A \mapsto A$ je injektívne, lebo φ je injektívne a kompozícia injektívnych zobrazení je injektívne zobrazenie. Z rovnosti $\varphi^n(b) = \varphi^n(\varphi(a))$ vďaka injektívnosti φ^n dostávame $b = \varphi(a)$, zobrazenie φ teda je surjektívne.

Nech A je noetherovský a φ surjekcia. Vďaka vlastnosti $X \subseteq Y \subseteq A \Rightarrow \varphi^{-1}(X) \subseteq \varphi^{-1}(Y)$ vidíme, že platí

$$\{\mathbf{0}\} \subseteq \varphi^{-1}(\{\mathbf{0}\}) \subseteq \varphi^{-2}(\{\mathbf{0}\}) \subseteq \varphi^{-3}(\{\mathbf{0}\}) \subseteq \cdots \subseteq \varphi^{-n}(\{\mathbf{0}\}) \subseteq \cdots$$

Z noetherovskosti A vyplýva, že existuje $n \in N$ také, že $\varphi^{-n}(\{\mathbf{0}\}) = \varphi^{-(n+1)}(\{\mathbf{0}\}) = \varphi^{-(n+2)}(\{\mathbf{0}\}) = \cdots$.

Potrebujeme dokázať, že φ je injektívne, t.j. napríklad, že $\mathrm{Ker}\varphi = \{\mathbf{0}\}$. Zoberme $a \in \mathrm{Ker}\varphi$, t.j. $\varphi(a) = \mathbf{0}$. Zo surjektívnosti φ vyplýva, že aj φ^n je surjektívne zobrazenie a preto existuje $b \in A$ také, že $\varphi^n(b) = a$ a teda $\varphi^{n+1}(b) = \varphi(\varphi^n(b)) = \varphi(a) = \mathbf{0}$, t.j. $b \in \varphi^{-(n+1)}(\{\mathbf{0}\}) = \varphi^{-n}(\{\mathbf{0}\})$, preto $b \in \varphi^{-n}(\{\mathbf{0}\})$, čiže $a = \varphi^n(b) = \mathbf{0}$. Dokázali sme implikáciu $\varphi(a) = \mathbf{0} \Rightarrow a = \mathbf{0}$, t.j. $\mathrm{Ker}\varphi = \{\mathbf{0}\}$ a preto φ je injektívne zobrazenie. □

4.3 Rozložiteľnosť, Fittingova lema, veta Krulla-Schmidta-Remaka-Wedderburna

Ak máme modul A, $\varphi, \psi : A \mapsto A$ sú endomorfizmy modulu A (t.j. modulové homomorfizmy, ktoré majú aj definčný obor aj obor hodnôt modul A). Tieto dva endomorfizmy môžeme prirodzeným spôsobom sčítať, pričom súčet je opäť endomorfizmus ($\varphi + \psi : A \mapsto A$ je definované vzťahom $(\varphi + \psi)(\alpha) = \varphi(\alpha) + \psi(\alpha)$). Podobne zložením (kompozíciou) týchto dvoch endomorfizmov dostávame tiež endomorfizmus $\varphi \circ \psi : A \mapsto A$.

Množina všetkých endomorfizmov modulu A s takto defininovanými operáciami $+, \circ$ je okruh, ktorý označujeme ako $(Hom(A, A), +, \circ)$. Asi jediné, čo je vhodné overiť je distributivita - napr. pravá distributivita: Pre každé $\alpha \in A$ platí

$$((\varphi + \psi) \circ \omega)(\alpha) = (\varphi + \psi)(\omega(\alpha)) = \varphi(\omega(\alpha)) + \psi(\omega(\alpha)) = \varphi \circ \omega(\alpha) + \psi \circ \omega(\alpha) = (\varphi \circ \omega + \psi \circ \omega)(\alpha)$$

a preto $(\varphi + \psi) \circ \omega = \varphi \circ \omega + \psi \circ \omega$.

Jednotkou v tomto okruhu je identické zobrazenie (ktoré je samozrejme endomorfizmom), budeme ho označovať $\mathbf{1}$.

Definícia 4.3.1 *Prvok $a \in A$ v okruhu $(A, +, \cdot)$ nazývame nilpotentný, ak existuje prirodzené číslo n také, že $a^n = 0$.*

Nasledujúce tvrdenie sa nazýva Fittingova lema. Pripomeňme, že $\varphi^n = \varphi \circ \varphi \circ \cdots \circ \varphi$ (kompozícia v pravej časti je n krát).

Veta 4.3.2 *Nech A je artinovský a noetherovský modul, $\varphi : A \mapsto A$ je endorfizmus. Potom existuje n také, že $A = \varphi^n(A) \oplus \varphi^{-n}(\{\mathbf{0}\})$.*

Dôkaz. Zoberme postupnosť podmodulov $A \supseteq \varphi(A) \supseteq \varphi^2(A) \supseteq \cdots$. Táto postupnosť sa vďaka artinovskosti stabilizuje, nech $\varphi^n(A) = \varphi^{n+1}(A) = \cdots$, označme $A' = \varphi^n(A)$. Potom $\varphi^n(A') = A'$ a preto $\varphi^n : A' \mapsto A'$ je surjektívne zobrazenie, A' je noetherovský modul (lebo je podmodul noetherovského modulu A) a preto $\varphi^n : A' \mapsto A'$ je bijekcia (automorfizmus). To znamená, že $\mathrm{Ker}\varphi^n \cap A' = \{\mathbf{0}\}$ ($\varphi^n : A \mapsto A$ nemusí byť injektívne, ale keď ho zúžime na A' už je injektívne, preto ten prienik s A'). To znamená, že ak zoberieme podmodul $T = A' + \varphi^{-n}(\{\mathbf{0}\})$, tak tento súčet je priamy súčet. Ešte potrebujeme dokázať, že $T = A$.

Nech $a \in A$. Skúsme ho zapísať v tvare $a = \varphi^n(b) + (a - \varphi^n(b))$, nech b vyberieme akokoľvek, bude $\varphi^n(b) \in A'$. Potrebujeme vybrať b také, aby $a - \varphi^n(b) \in \varphi^{-n}(\{\mathbf{0}\})$, t.j. aby $\varphi^n(a - \varphi^n(b)) = \mathbf{0}$, t.j. $\varphi^n(a) - \varphi^{n+n}(b) = \mathbf{0}$, t.j. $\varphi^n(a) = \varphi^{n+n}(b)$.

Toto ale je "návod" ako to urobiť. Totiž vieme, že $c = \varphi^n(a) \in A'$ a pretože $\varphi^n : A' \mapsto A'$ je surjektívne, existuje $b' \in A'$ také, že $\varphi^n(b') = c$. Ale $b' \in A' = \varphi^n(A)$, t.j. existuje $b \in A$ také, že $\varphi^n(b) = b'$, čiže $\varphi^n(\varphi^n(b)) = \varphi^n(b') = c$, t.j. $\varphi^{n+n}(b) = c = \varphi^n(a)$.

□

Dôsledok 4.3.3 *Nech A je artinovský a noetherovský nerozložiteľný modul (t.j. A sa nedá netriviálnym spôsobom zapísať v tvare $A = B \oplus C$, porovnajte s vetou 1.2.8), $\varphi : A \mapsto A$ je endorfizmus. Potom φ je buď automorfizmus (t.j. bijekcia), alebo je nilpotentný (t.j. existuje n také, že $\varphi^n = \mathbf{0}$, t.j pre každé $\alpha \in A$ platí $\varphi^n(\alpha) = \mathbf{0}$, t.j. kompozícia φ^n je triviálny homomorfizmus).*

Dôkaz. Podľa Fittingovej lemy vieme modul A rozložiť na súčet $A = \varphi^n(A) \oplus \varphi^{-n}(\{\mathbf{0}\})$ a teda je $\varphi^n(A) = \{\mathbf{0}\}$ alebo $\varphi^{-n}(\{\mathbf{0}\}) = \{\mathbf{0}\}$, lebo A je nerozložiteľný.

V prvom prípade je φ nilpotentný prvok v okruhu $(Hom(A, A), +, \circ)$ a v druhom prípade je aj $\varphi^{-1}(\{\mathbf{0}\}) = \{\mathbf{0}\}$ a teda φ je injektívne a keďže A je artinovský modul, je φ bijekcia, t.j. automorfizmus. □

Veta 4.3.4 *Nech A je artinovský a noetherovský nerozložiteľný modul, $\varphi : A \mapsto A$ je automorfizmus modulu A a $\omega_1, \ldots, \omega_n : A \mapsto A$ sú endomorfizmy také, že*

$$\varphi = \omega_1 + \cdots + \omega_n$$

Potom existuje i také, že ω_i je automorfizmus modulu A.

Dôkaz. φ je automorfizmus, preto existuje φ^{-1}, ktoré je tiež automorfimus a preto rovnicu z predpokladov vieme prepísať do tvaru

$$\mathbf{1} = \varphi \circ \varphi^{-1} = \omega_1 \circ \varphi^{-1} + \cdots + \omega_n \circ \varphi^{-1}$$

Dôkaz teda urobme indukciou. Pre $n = 2$ teda máme $\mathbf{1} = \omega_1 \circ \varphi^{-1} + \omega_2 \circ \varphi^{-1}$ alebo $\mathbf{1} = \delta + \eta$, kde $\delta = \omega_1 \circ \varphi^{-1}$, $\eta = \omega_2 \circ \varphi^{-1} : A \mapsto A$ sú endomorfizmy.

Podľa dôsledku vieme, že δ je buď nilpotentý alebo je automorfizmus. Ak je automorfizmus, je to OK. Ak je nilpotentný, povedzme $\delta^n = \mathbf{0}$, stačí si všimnúť, že $(\mathbf{1} - \delta) \circ (\mathbf{1} + \delta + \delta^2 + \cdots + \delta^{n-1}) = \mathbf{1}$ a aj $(\mathbf{1} + \delta + \delta^2 + \cdots + \delta^{n-1}) \circ (\mathbf{1} - \delta) = \mathbf{1}$, t.j. $\mathbf{1} - \delta$ má inverzný prvok a preto je bijekcia. Čiže ak je δ nilpotentný, tak $\eta = \mathbf{1} - \delta$ je automorfizmus a preto $\omega_2 = \eta \circ \varphi$ ako zloženie dvoch automorfizmov je automorfizmus.

Pre dokončenie dôkazu indukciou treba využiť, že tvrdenie platí pre 2 a pre $n - 1$ asi tak, že napíšeme

$$\varphi = \omega_1 + (\omega_2 \cdots + \omega_n)$$

a buď je ω_1 automorfizmus alebo je $\omega_2 \cdots + \omega_n$ automorfizmus (v tomto prípade sa využije štandardný indukčný predpoklad.) □

V nasledujúcej časti dokážeme, že rozklad vhodného "typu" modulu na nerozložiteľné podmoduly je v podstate jednoznačný (neplatí to všeobecne).

Najprv dokážeme jeden špeciálny prípad takéhoto tvrdenia.

Veta 4.3.5 *Nech $A = A_1 \times A_2$ je artinovský modul, $\lambda : A = A_1 \times A_2 \mapsto B = B_1 \times B_2$ je izomorfizmus modulov taký, že $\lambda(a, \mathbf{0}) = (\alpha(a), \beta(a))$, kde $\alpha : A_1 \mapsto B_1$ je izomorfizmus. Potom $A_2 \cong B_2$, t.j. je moduly A_2, B_2 sú izomorfné.*

Dôkaz. Najprv si všimnime, že z predpokladov vyplýva, že $\beta : A_1 \mapsto B_2$ je homomorfizmus (overte si to!). Pre špeciálny prípad, že $\mathrm{Im}\beta = \{\mathbf{0}\}$ platí:

$$A_2 \simeq \frac{A_1 \times A_2}{A_1 \times \{\mathbf{0}\}} \simeq \overline{\lambda}\left(\frac{A_1 \times A_2}{A_1 \times \{\mathbf{0}\}}\right) = \frac{\lambda(A_1 \times A_2)}{\lambda(A_1 \times \{\mathbf{0}\})} = \frac{B_1 \times B_2}{\alpha(A_1) \times \{\mathbf{0}\}} = \frac{B_1 \times B_2}{B_1 \times \{\mathbf{0}\}} \simeq B_2$$

(pre definíciu $\overline{\lambda}$ pozrite cvičenie 21 v kapitole 1.2)

Vo všeobecnom prípade sa pokúsime "opraviť" izomorfizmus λ, vyrobiť pomocou neho nový izomorfizmus $\mu : A_1 \times A_2 \mapsto B = B_1 \times B_2$, ktorý bude mať vlastnosť "$\mathrm{Ker}\,\beta = \{\mathbf{0}\}$".

Nech $\lambda(a_1, a_2) = (b_1, b_2)$. Položme $\mu(a_1, a_2) = (b_1, b_2 - \beta\alpha^{-1}(b_1))$. Zobrazenie μ spĺňa požadovanú vlastnosť: Nech $\lambda(a, \mathbf{0}) = (b_1, b_2) = (\alpha(a), \beta(a))$

$$\mu(a, \mathbf{0}) = (b_1, b_2 - \beta\alpha^{-1}(b_1)) = (b_1, \beta(a) - \beta\alpha^{-1}(\alpha(a))) = (b_1, \beta(a) - \beta(a)) = (b_1, \mathbf{0})$$

To znamená, že $\mu(a, \mathbf{0}) = (\alpha(a), \mathbf{0})$.

Ak označíme $\alpha' = \pi_1 \circ \lambda$ a $\beta' = \pi_2 \circ \lambda$ (π_1, π_2 sú projekcie na prvú a druhú zložku, t.j. $\pi_i : B_1 \times B_2 \mapsto B_i$, $\pi_i(b_1, b_2) = b_i$, t.j. homomorfizmy), tak $\lambda(a_1, a_2) = (\alpha'(a_1, a_2), \beta'(a_1, a_2)) = (b_1, b_2)$ a preto

$$\mu(a_1, a_2) = (\alpha'(a_1, a_2), \beta'(a_1, a_2) - \beta\alpha^{-1}\alpha'(a_1, a_2))$$

odkiaľ vidieť, že μ je homomorfizmus, lebo sme ho získali skladaním a sčítaním/odčítaním homomorfizmov ($\alpha^{-1} : B_1 \mapsto A_1$ je izomorfizmus, lebo α je izomorfizmus).

Ešte potrebujeme dokázať, že μ je bijekcia. Pozrime sa na zobrazenie $\mu\lambda^{-1} : B_1 \times B_2 \mapsto B_1 \times B_2$. Modul $B_1 \times B_2$ ako izomorfný obraz artinovského modulu je artinovský modul. Ak teda overíme, že $\mu\lambda^{-1}$ je injektívne, budeme vedieť, že je to bijekcia. Ale keď je $\mu\lambda^{-1}$ bijekcia, tak aj kompozícia $\mu\lambda^{-1}\lambda = \mu$ je bijekcia.

K injektívnosti $\mu\lambda^{-1}$: nech teda $\lambda(a_1, a_2) = (b_1, b_2)$, t.j. (izomorfnosť) $\lambda^{-1}(b_1, b_2) = (a_1, a_2)$ a preto (skúmame, kedy $(b_1, b_2) \in \mathrm{Ker}\,\mu\lambda^{-1}$)

$$(0, 0) = \mu\lambda^{-1}(b_1, b_2) = \mu(a_1, a_2) = (b_1, b_2 - \beta\alpha^{-1}(b_1))$$

Teda $b_1 = \mathbf{0}$ a keďže je α izomorfizmus a β homomorfizmus, je aj $\beta\alpha^{-1}(b_1) = \beta\alpha^{-1}(\mathbf{0}) = \mathbf{0}$ a teda keďže $\mathbf{0} = b_2 - \beta\alpha^{-1}(b_1) = b_2 - \mathbf{0}$, tak $b_2 = \mathbf{0}$ a teda $(b_1, b_2) = (0, 0)$, t.j. $\mu\lambda^{-1}$ je naozaj injektívne zobrazenie, t.j. je to bijekcia a preto μ je izomorfizmus. □

Teraz uvedieme vetu, ktorá sa pripisuje Krullovi, Remakovi, Schmidtovi, Wedderburnovi

Veta 4.3.6 *Nech $A = A_1 \times A_2 \times \cdots \times A_n$ je artinovský a noetherovský modul, ktorý je izomorfný s modulom $A' = A'_1 \times A'_2 \times \cdots \times A'_m$, pričom všetky moduly $A_1, \ldots, A_n, A'_1, \ldots, A'_m$ sú nerozložiteľné. Potom $n = m$ a (až na poradie, t.j. možno po vhodnom prečíslovaní) pre všetky prípustné i platí $A_i \cong A'_i$.*

Dôkaz. Nech $\kappa_i : A_i \mapsto A$, $\pi_j : A \mapsto A_i$ a $\kappa'_i : A'_i \mapsto A'$, $\pi'_j : A' \mapsto A'_i$ sú príslušné injekcie a projekcie potrebné ku definícii A a A' ako priamych súčinov, nech $\lambda : A \mapsto A'$ je izomorfizmus.

Zoberme zobrazenia $\alpha_i : A_1 \mapsto A'_i$ dané vzorcom $\alpha_i = \pi'_i\lambda\kappa_1$ (pre $i = 1, \ldots, m$) a $\beta_j : A'_j \mapsto A_1$ dané vzorcom $\beta_j = \pi_1\lambda^{-1}\kappa'_j$ (tiež pre $j = 1, \ldots, m$)

Potom $\sum_{i=1}^m \beta_i\alpha_i = \sum_{i=1}^m \pi_1\lambda^{-1}\kappa'_i\pi'_i\lambda\kappa_1 = \pi_1\lambda^{-1}(\sum_{i=1}^m \kappa'_i\pi'_i)\lambda\kappa_1 = \pi_1\lambda^{-1}\mathbf{1}_{A'}\lambda\kappa_1 = \pi_1\mathbf{1}_A\kappa_1 = \pi_1\kappa_1$ je zobrazenie $\sum_{i=1}^m \beta_i\alpha_i = \pi_1\kappa_1 = \mathbf{1}_{A_1} : A_1 \mapsto A_1$.

Modul A_1 je izomorfný s podmodulom modulu A a preto je artinovský aj noetherovský. Je nerozložiteľný a preto podľa vety 4.3.4 je jeden z homomorfizmov $\beta_i \circ \alpha_i$ automorfizmus. Pre zobrazenie $\alpha_i \circ \beta_i : A'_i \mapsto A'_i$ (aj modul A'_i je artinovský aj noetherovský a nerozložiteľný) podľa dôsledku za Fittingovou lemou platí, že je to buď automorfizmus alebo nilpotentný prvok. Nilpotentný však nie je, totiž ak by existovalo n také, že $(\alpha_i \circ \beta_i)^n = \mathbf{0}$, tak $(\beta_i \circ \alpha_i)^{n+1} = \beta_i \circ (\alpha_i \circ \beta_i)^n \circ \alpha_i = \beta_i \circ \mathbf{0} \circ \alpha_i = \mathbf{0}$, ale kompozícia $n + 1$ automorfizmov $\beta_i\alpha_i$ nemôže "dať" neinjektívne zobrazenie. Teda $\beta_i \circ \alpha_i$ je automorfizmus a preto α_i je injektívne a aj $\alpha_i \circ \beta_i$ je automorfizmus a preto je α_i surjektívne, t.j. $\alpha_i : A_1 \mapsto A'_i$ je izomorfizmus. Bez újmy na všeobecnosti môžeme predpokladať, že $i = 1$, t.j. že $\alpha_1 : A_1 \mapsto A'_1$ je izomorfizmus.

Položme teraz $B = A_2 \times \cdots \times A_n$, $B' = A'_2 \times \cdots \times A'_m$, dostávame $A = A_1 \times B \simeq A' = A'_1 \times B'$, $\lambda : A_1 \times B \mapsto A'_1 \times B'$ a $\lambda(a, 0) = (\alpha_1(a), *)$ (presnejšie $a \mapsto \overbrace{\kappa_1(a)}^{\in A} \mapsto \overbrace{\lambda(\kappa_1(a))}^{\in A'} \mapsto \overbrace{\pi'_1(\lambda(\kappa_1(a)))}^{\in A'_1} = \alpha_1(a)$), môžeme teda využiť predošlú vetu, ktorá hovorí, že $B \simeq B'$.

Celý dôkaz teraz môžeme dokončiť indukciou. Ak $n = 1$, je modul $A = A_1$ nerozložiteľný a preto aj $m = 1$ a $A_1 \simeq A'_1$. Pre druhý krok indukcie, ak obe čísla n, m sú ≥ 2 dostaneme uvedeným spôsobom, že $B = A_2 \times \cdots \times A_n$ a $B' = A'_2 \times \cdots \times A'_m$ sú izomorfné, artinovsko noetherovské, pričom $A_2, \ldots, A_n$, $A'_2, \ldots, A'_m$ sú nerozložiteľné a podľa indukčného predpokladu teda $n-1 = m-1$ (čiže $n = m$) a po vhodnom prečíslovaní sú moduly A_i izomorfné s príslušnými modulmi A'_j (a už vieme, že aj $A_1 \simeq A'_1$). □

Poznámka. Je vhodné si uvedomiť, že na dôkaz uvedeného tvrdenia nie je možné použiť Jordan-Hölderovu vetu. Dôvod je ten, že existujú moduly (noetherovsko-artinovské), ktoré sú nerozložiteľné (na priamy súčin), ale nie sú "jednoduché", t.j. majú netriviálne podmoduly.

4.4 Rozložiteľnosť okruhov

Analóg posledne uvedeného tvrdenia pre okruhy má úplne inú podstatu, dá sa dokázať podstatne silnejšie tvrdenie.

Definícia 4.4.1 *Štruktúra $(S, \wedge, 0, ')$ sa nazýva boolovská algebra, ak $(S, \wedge)$ je polozväz, (t.j. $\wedge$ je binárna komutatívna a idempotentná (t.j. $a \wedge a = a$) operácia na S), $0 \in S$ a $'$ je unárna operácia na S taká, že*

$$a \wedge b' = 0 \Leftrightarrow a \wedge b = a (\Leftrightarrow a \leq b)$$

Táto definícia nie je štandartná ale pre ciele, ktoré chceme dosiahnuť je postačujúca.

(Polozväz vzniká z čiastočne usporiadanej množiny, v ktorej každé dva prvky majú najväčšie dolné ohraničenie - položíme $a \wedge b =$ najmenšie dolné ohraničenie prvkov a, b.

"Duálne", ak máme polozväz $(S, \wedge)$ v zmysle vyššie uvedenej definície - t.j. $\wedge$ je binárna komutatívna idempotentná operácia na S, tak relácia $\leq$ na S definovaná vzťahom $a \leq b \Leftrightarrow a \wedge b = a$ je čiastočné usporiadanie, v ktorom každé dva prvky majú najväčšie dolné ohraničenie, a to $a \wedge b$.

Prvok a' sa nazýva komplement prvku a. Štandardne sa pre polozväzy s najmenším prvkom (s nulou) definuje tzv. pseudokomplement nasledovne: prvok a' sa nazýva pseudokomplement ku a práve vtedy, keď $x \leq a' \Leftrightarrow a \wedge x = 0$. To znamená, že a' — ak existuje — je minimálny z prvkov $x \in S;\ x \wedge a = 0$. Vo všeobecnosti nie je určený jednoznačne.)

Asi je dobré si uvedomiť, že 0 je najmenší prvok z S. Ak je totiž $c \leq 0$, tak podľa definície je $c \wedge 0' = 0$, ale ak je $c < 0$ tak $c \wedge$čokoľvek $\leq c < 0$ a teda nemôže byť $c \wedge 0' = 0$. Prvok neporovnateľný s 0 nemôže existovať, lebo potom by musel existovať prvok ostro menší ako 0.

Len pre zaujímavosť uveďme nasledovnú lemu, ktorá naznačí, že táto definícia je "dosť" dobrá.

Lema 4.4.2 *Nech $(S, \wedge, 0, ')$ je boolovská algebra, $a \in S$. Potom $a = a''$.*

Dôkaz. Najprv si uvedomme, že $a \leq a$ a preto podľa definície $a \wedge a' = 0$, čiže aj $a' \wedge a'' = 0$, t.j. $a'' \wedge a' = 0$, preto $a'' \leq a$. Potom aj $a'''' \leq a'' \leq a$, ale napríklad aj $a''' \leq a'$.

Skúsme zistiť, či platí $a''' = a'$. Na to ešte potrebujeme dokázať nerovnosť $a' \leq a'''$. Toto platí práve vtedy, keď $a' \wedge a'''' = 0 = a'''' \wedge a'$ čo je ekvivalentné s $a'''' \leq a$, čo je pravda. Takže $a' = a'''$.

Skúsme sa teraz pozrieť, či vieme dokázať nerovnosť $a \leq a''$. Táto nerovnosť vyplýva z faktu, že $a \wedge a''' = 0$, ale $a' = a'''$ a vieme, že $a \wedge a' = 0$. Takže $a \wedge a''' = 0$ a teda platí nerovnosť $a \leq a''$. □

Keď teraz na množine S zadefinujeme novú operáciu $\vee$ vzorcom $a \vee b = (a' \wedge b')'$ a položíme $1 := 0'$, dostaneme $(S, \wedge, \vee, 0, 1, ')$. pričom $(S, \wedge, \vee)$ bude distributívny zväz, $0, 1$ budú jeho najmenší a najväčší prvok a operácia $'$ bude operáciou komplementu, čím sa dostaneme ku "štandardnej" boolovskej algebre.

Veta 4.4.3 *Množina všetkých centrálnych idempotentných prvkov okruhu $(R, +, \cdot)$ tvorí boolovskú algebru, ktorú označujeme $B(R)$.*

Dôkaz. Asi treba upresniť znenie vety, potrebujeme vedieť operácie, aby $(B(R), \wedge, 0, ')$ "mohla" byť boolovská algebra. Položme $a \wedge b = a \cdot b$ a $a' = 1 - a$ pre centrálne idempotentné prvky $a, b \in B(R)$. $\wedge$ je komutatívna (centrálnosť), asociatívna (násobenie v okruhu), idempotentná (berieme len idempotentné prvky).

$a \wedge b' = a \cdot (1 - b) = 0$ práve vtedy, keď $a - a \cdot b = 0$, t.j. $a = ab = a \wedge b$, čiže b' funguje "správne" a preto je $(B(R), \wedge, 0, ')$ boolovská algebra. □

Definícia 4.4.4 *Nech $(S, \wedge, 0, ')$ je boolovská algebra. Hovoríme, že $0 \neq a \in S$ je atóm tejto b.a., ak $x < a \Rightarrow x = 0$, čiže ak sa "medzi" 0 a a nenachádza žiadny prvok z S.*

Lema 4.4.5 *Ak je $e \in R$ centrálny idempotentný prvok v R, potom je ideál eR nerozložiteľný okruh práve vtedy, keď je to atóm boolovskej algebry $(B(R), \wedge, 0, ')$ popísanej vyššie.*

Nech I je ideál okruhu R. Potom I je nerozložiteľný okruh práve vtedy, keď existuje $e \in B(R)$ také, že $I = eR$ a e je atóm tejto boolovskej algebry.

Dôkaz. Fakt, že I je okruh vlastne znamená hlavne to, že I má jednotku e. O prvku e vieme, že $e \in B(R)$ a že $I = eR$ (pozri úvod v 4.1). Ak e nie je atóm, t.j. existuje $0 < f < e$, $f \in B(R)$, tak $I = fI \oplus (e - f)I$, t.j. I je rozložiteľný.

Naopak, ak je okruh I rozložiteľný, t.j. $I = A \oplus B$, tak A má svoju jednotku f. Potom f je centrálny idempotentný prvok v I. Teda f je idempotentný. Ešte potrebujeme dokázať, že je centrálny v R, potom budeme vedieť, že je to prvok b.a. $B(R)$.

Keď je ideál I okruh, existuje S také, že $R = I \oplus S = A \oplus B \oplus S$, t.j. A je priamy sčítanec v R (a aj ideál) a preto je jeho jednotka f centrálnym prvkom v R — to všetko sme dokázali v úvode časti 4.1.

Prvok f je teda centrálny idempotent v okruhu R a ak je rozklad $I \simeq A \oplus B$ netriviálny, tak $0 \neq f \neq e$ a keďže platí $f = ef$ (lebo e je neutrálny prvok v I) a teda $f \leq e$, čiže $f < e$ a preto e nie je atóm. □

Veta 4.4.6 *Ak je okruh $(R, +, \cdot)$ priamy súčet konečného počtu nerozložiteľných ideálov (nerozložiteľných ako okruhy), potom tieto ideály "vyčerpávajú" množinu všetkých nerozložiteľných priamych sčítancov okruhu R (t.j. všetkých nerozložiteľných ideálov okruhu R, ktoré sú zároveň okruhmi).*

Dôkaz. Nech je okruh R zapísaný pomocou ortogonálneho systému centrálnych idempotentných prvkov ako priama suma

$$R = e_1R + e_2R + \cdots + e_nR$$

Potom vieme, že $1 = e_1 + \cdots + e_n$. Keďže sú všetky e_iR nerozložiteľné, sú všetky e_i atómy v boolovskej algebre $B(R)$. Dokážeme, že tieto prvky $e_1, \ldots, e_n$ vyčerpávajú všetky atómy. Zoberme nejaký atóm e. Potom pre atóm

e_i platí, že $ee_i \leq e$ a teda buď $ee_i = 0$ alebo $e = e_i$. Keďže $e = e \cdot 1 = e(e_1 + \cdots + e_n) = ee_1 + ee_2 + \cdots + ee_n$, nemôžu byť všetky sčítance ee_i nuly, t.j. pre nejaké i musí platiť, že $e = e_i$ a teda e je jeden z uvedených $e_1, \ldots, e_n$. To znamená, že každý nerozložiteľný priamy sčítanec okruhu R sa vyskytuje v zozname $e_1R, e_2R, \ldots, e_nR$. □

Cvičenie 54 *Ak je modul $A_1 \times A_2 \cong B_1 \times B_2$ artinovský a noetherovský a $A_1 \cong B_1$, tak $A_2 \cong B_2$. Dokážte!*

Cvičenie 55 *Nech M je artinovský alebo noetherovský modul. Potom sa M dá rozložiť na konečný priamy súčet nerozložiteľných modulov.*

4.5 Hilbertova veta o báze

Veta, ktorú si dokážeme v tejto sekcii je v istom zmysle základ algoritmizácie práce s okruhmi polynómov o viacerých premenných, keby táto veta neplatila, väčšina bežne používaných algoritmov by vôbec nemala zmysel.

Veta 4.5.1 *Nech $(A, +, \cdot)$ je noetherovský komutatívny okruh s 1, x transcendentný prvok nad A. Potom $A[x]$ je noetherovský okruh. (Špeciálne to po "iterácii" znamená, že okruh polynómov viacerých premenných nad poľom k, t.j. $k[x_1, \ldots, x_n]$ je noetherovský, t.j. každý jeho ideál je konečnegenerovaný.)*

Dôkaz. Pri dôkaze použijeme fakt, že A je noetherovský okruh práve vtedy, keď je každý jeho ideál konečne generovaný (veta 4.2.3, treba ju použiť v okruhovej verzii).

Dôkaz urobíme v dvoch krokoch. Najprv dokážeme, že je zaujímavé vedieť vygenerovať polynómy z daného ideálu s "malými" stupňami a potom dokážeme, že aj tie s malými stupňami vieme vygenerovať pomocou konečne veľa generátorov. Oba tieto kroky sa navzájom podobajú, v podstate je v dôkaze využitá jediná myšlienka.

Pre zjednodušenie zápisu si zadefinujme tzv. "leading coeficient" (vedúci koeficient) polynómu $f \in A[x]$: Nech $f \neq 0$, $f(x) = a_n x^n + \cdots + a_1 x + a_0$ je taký zápis, že $a_n \neq 0$. Položíme $lc(f) = a_n$. Ak $f = 0$ kladieme $lc(f) = 0$.

Nech I je ideál v $A[x]$. Aby sme mohli využiť predpoklad, je vhodné pomocou neho vyrobiť nejaký ideál v A. Vhodným kandidátom je niečo súvisiace s koeficientami polynómov v I. Konkrétne, položme

$$Lc_I = \{a \in A;\ (\exists f \in I)\, a = lc(f)\}$$

Zrejme $f = 0 \in I$, preto $0 \in Lc_I$. Dokážeme, že Lc_I je ideál v A.

Nech $a, b \in Lc_I$, $f, g \in I$ sú také, že $a = lc(f)$, $b = lc(g)$. Ak je $a = 0$ alebo $b = 0$, tak aj $a \pm b \in Lc_I$. Nech teda $a \neq 0 \neq b$. Ak $\mathrm{st}(f) = \mathrm{st}(g)$, tak zrejme $lc(f \pm g) = a \pm b$ a keďže $f \pm g \in I$, je $a \pm b \in Lc_I$. Ak $\mathrm{st}(f) \neq \mathrm{st}(g)$, nech (bez újmy na všeobecnosti) je $\mathrm{st}(f) > \mathrm{st}(g)$. Položme $k = \mathrm{st}(f) - \mathrm{st}(g)$. Potom bude $x^k \cdot g(x) \in I$ a $lc(x^k \cdot g(x)) = b$ a preto aj $f \pm x^k \cdot g \in I$ a preto $a \pm b = lc(f \pm x^k \cdot g) \in Lc_I$.

Násobenie je jednoduchšie: nech $a \in Lc_I$, $f \in I$ je taký, že $a = lc(f)$, $b \in A$. Potom $b \cdot f \in I$, $lc(b \cdot f) = b \cdot a$ a preto $b \cdot a \in A$. Podľa predpokladu je A komutatívny okruh a preto už vieme, že Lc_I je ideál v A.

Každý ideál v A je konečnegenerovaný, nech teda $Lc_I = (a_1, \ldots, a_n)$. Pre každé a_i z tejto množiny generátorov vyberme jeden polynóm $f_i \in I$ taký, že $lc(f_i) = a_i$ (a povedzme najnižšieho možného stupňa s týmito dvoma vlastnosťami - nie je to dôležité, ale "zefektívni" to výslednú množinu potrebných generátorov). Položme $k = \max\{\mathrm{st}(f_1), \ldots, \mathrm{st}(f_n)\}$ a označme $k_i = \mathrm{st}(f_i)$.

Zoberme taký $f \in I$, že $m = \mathrm{st}(f) \geq k$, nech $a = lc(f)$. Podľa definície je $a \in Lc_I$ a preto existujú $b_1, \ldots, b_n \in A$ také, že $a = a_1 b_1 + \cdots + a_n b_n$.

Položme $g = b_1 x^{m-k_1} f_1 + b_2 x^{m-k_2} f_2 + b_n x^{m-k_n} f_n$. Každý člen tvaru $b_i x^{m-k_i} f_i$ je stupňa $m = \mathrm{st}(f)$ a zrejme je $lc(g) = a_1 b_1 + \cdots + a_n b_n = a$. Preto $\mathrm{st}(f - g) < m$. Konečným počtom zopakovaní tohoto postupu (potrebujeme znížiť stupeň pod k, kým je "nad" k, tak ho znížiť vieme) zistíme, že pre daný polynóm f stupňa $\mathrm{st}(f) \geq k$ vieme nájsť také polynómy $g_1, \ldots, g_n$, že polynóm $f - \sum_1^n g_i f_i$ má stupeň menší ako k.

Takže už vieme, že problém (ak by sa nejaký vyskytol) musí nastať pri "malých" stupňoch, prvý krok máme za sebou.

Druhý krok urobíme analogicky. Pre každé $l < k$ vyrobme množinu

$$Lc_{I,l} = \{a \in A;\ (\exists f \in I)\, \mathrm{st}(f) = l \ \&\ a = lc(f)\} \cup \{0\}$$

čiže množinu všetkých vedúcich koeficientov polynómov z I, ktorých stupeň je práve l (a pridaním "povinnej" 0). Každá z množín $Lc_{I,l}$ je ideál v A — dôkaz je vlastne ešte jednoduchší ako pre množinu Lc_I, lebo tu nemáme problém s polynómami rôznych stupňov, ktorý sme vtedy museli "ošetriť".

Ideály $Lc_{I,k-1}, Lc_{I,k-2}, \ldots, Lc_{I,1}, Lc_{I,0}$ sú konečnegenerované, nech

$$\begin{aligned} Lc_{I,k-1} &= (a_{1,k-1}, \ldots, a_{n_{k-1},k-1}) \\ Lc_{I,k-2} &= (a_{1,k-2}, \ldots, a_{n_{k-2},k-2}) \\ Lc_{I,1} &= (a_{1,1}, \ldots, a_{n_1,1}) \end{aligned}$$

a nakoniec pre konštanty patriace do I

$$Lc_{I,0} = (a_{1,0}, \ldots, a_{n_0,0})$$

a vyberme polynómy $f_{1,k-1}, \ldots, f_{n_{k-1},k-1} \in I$ stupňa $k-1$ také, že $lc(f_{1,k-1}) = a_{1,k-1}$, ..., $lc(f_{n_{k-1},k-1}) = a_{n_{k-1},k-1}$, polynómy $f_{1,k-2}, \ldots, f_{n_{k-2},k-2} \in I$ stupňa $k-2$ také, že $lc(f_{1,k-2}) = a_{1,k-2}$,...,$lc(f_{n_{k-2},k-2}) = a_{n_{k-2},k-2}$, ..., polynómy $f_{1,1}, \ldots, f_{n_1,1} \in I$ stupňa 1 také, že $lc(f_{1,1}) = a_{1,1}$, ..., $lc(f_{n_1,1}) = a_{n_1,1}$, a nakoniec konštanty $f_{1,0}, \ldots, f_{n_0,0} \in I$ (t.j. polynómy stupňa 0) také, že $lc(f_{1,0}) = a_{1,0}$, ..., $lc(f_{n_0,0}) = a_{n_0,0}$

Dokážeme, že polynómy

f_1	f_1	...	f_n	— "pokryjú" stupeň väčší alebo rovný k
$f_{1,k-1}$	$f_{1,k-1}$	...	$f_{n_{k-1},k-1}$	— pre stupeň $k-1$
$f_{1,k-2}$	$f_{1,k-2}$	...	$f_{n_{k-2},k-2}$	— pre stupeň $k-2$
$f_{1,1}$	$f_{1,1}$	...	$f_{n_1,1}$	— pre stupeň 1
$f_{1,0}$	$f_{1,0}$	...	$f_{n_0,0}$	— pre stupeň 0

generujú ideál I.

Sporom (v podstate je to vlastne dôkaz indukciou): nech $f \in I$ je najmenšieho možného stupňa s vlastnosťou, že sa nedá pomocou uvedených polynómov vygenerovať, t.j. nedá sa napísať ako ich kombinácia s koeficientami v $A[x]$. Vieme, že $\mathrm{st}(f) < k$, lebo inak vyššie uvedený polynóm $f - \sum_1^n g_i f_i$ má stupeň menší ako k, t.j. je nižšieho stupňa ako $\mathrm{st}(f)$ a ak sa nedá vygenerovať f, nedá sa vygenerovať ani $f - \sum_1^n g_i f_i$.

Nech teda $m = \mathrm{st}(f) < k$, $a = lc(f)$, t.j. $a \in Lc_{I,m} = (a_{1,m}, \ldots, a_{n_m,m})$, preto existujú $b_1, \ldots, b_{n_m}$ také, že $a = b_1 a_1 + \cdots + b_{n_m} a_{n_m}$ a preto

$$lc(f) = lc(b_1 f_1 + \cdots + b_{n_m} f_{n_m})$$

čiže $\mathrm{st}(f - (b_1 f_1 + \cdots + b_{n_m} f_{n_m})) < m$. Ak sa nedal vygenerovať f, nedá sa vygenerovať ani $f - (b_1 f_1 + \cdots + b_{n_m} f_{n_m})$, ktorý je ale nižšieho stupňa - spor (resp. na tomto mieste využijeme indukčný predpoklad). □

Postup naznačený v dôkaze tejto vety je v istom zmysle konštruktívny, t.j. za dobrých okolností sa pomocou neho (aspoň) teoreticky dá vyrobiť generujúca množina. Museli by sme ale vedieť "efektívne" nájsť množiny Lc_I a $Lc_{I,l}$ pre $l = 0, \ldots, k-1$, potom efektívne nájsť ich generujúce množiny, k prvkom z generujúcej množiny efektívne nájsť polynómy s príslušnými vedúcimi koeficientami. Určite by sa nám teda hodil aspoň "algoritmus" na nájdenie generujúcej množiny pre ideály v I, ale to samo o sebe ešte nestačí.

4.6 Radikály okruhov, Birkhoffova veta

Všetky okruhy v tejto časti budú komutatívne okruhy s jednotkou.

4.6.1 Radikály okruhov, polopriama (ne-)rozložiteľnosť okruhov

Lema 4.6.1 *Nech I je ideál okruhu R, $r \in R$. Potom $I + rR = \{i + r.x;\ i \in I, x \in R\}$ je ideál (najmenší ideál obsahujúci $I \cup \{r\}$, t.j. $I + rR = (I \cup \{r\})$. Ak $r \notin I$, tak $I \subsetneq I + rR$.*

Dôkaz. Zrejme $0 = 0 + r.0 \in I + rR$. Nech $a = i_1 + r.x_1, b = i_2 + r.x_2 \in I + rR$. Potom $a - b = (i_1 - i_2) + r(x_1 - x_2) \in I + rR$, lebo $i_1 - i_2 \in I$ a $x_1 - x_2 \in R$.
Tiež $x(i_1 + rx_1) = xi_1 + xrx_1 \in I + rR$, lebo $xi_1 \in I$ a $xrx_1 = r(xx_1) \in rR$.
Keďže R je komutatívny okruh, je to ideál. Ostatné tvrdenia sú zrejmé. □

Lema 4.6.2 *Nech $0 \notin A \subseteq R$ a I je taký ideál okruhu R, že $I \cap A = \emptyset$. Potom existuje maximálny ideál $J \subsetneq R$ okruhu R taký, že $I \subseteq J$ a $J \cap A = \emptyset$. Maximalita je vyžadovaná vzhľadom na túto vlastnosť (t.j. J nemusí byť maximálny ideál okruhu R)*

Dôkaz. Dôkaz je jednoduchá aplikácia Zornovej lemy. Za M zoberme množinu všetkých vlastných ideálov obsahujúcich I, ktorých prienik s A je prázdny. Je ľahko vidieť, že $M \neq \emptyset$ a ak $N \subseteq M$ je taká podmnožina, že každé dva jej prvky sú porovnateľné (t.j. ak $X, Y \in N$ tak buď $X \subseteq Y$ alebo $Y \subseteq X$) tak $\bigcup N$ je ideál s vlastnosťou $(\bigcup N) \cap A$, ktorý je teda horným ohraničením N v M. Podľa Zornovej lemy (čo je tvrdenie ekvivalentné s axiómou výberu) množina M teda má maximálne prvky. □

Ak v predošlej leme použijeme $A = \{1\}$, dostaneme, že pre každý vlastný ideál I existuje maximálny (v "štandardnom" zmysle) ideál M obsahujúci I.

Lema 4.6.3 *Nech R je okruh. Prvok $a \in R$ je invertibilný práve vtedy, keď pre každý vlastný ideál I je $a \notin I$ (t.j. práve vtedy, keď pre každý maximálny ideál M platí, že $a \notin M$).*

Dôkaz. Prvok a je invertibilný práve vtedy, keď existuje b také, že $ab = 1$. Ak I je ideál taký, že $a \in I$, tak $ab \in I$, t.j. $1 \in I$, čiže I nie je vlastný ideál. Tvrdenie v zátvorke potom vyplýva z predošlej lemy. □

Táto lema nám umožní vysloviť charakterizáciu maximálnych ideálov pomocou prvkov:

Lema 4.6.4 *Nech R je okruh. Ideál $M \subsetneq R$ je maximálny práve vtedy, keď*

$$(\forall r \notin M)(\exists x \in R)\ 1 - rx \in M$$

Dôkaz. Podmienka vlastne hovorí, že pre každé $r \notin M$ ideál $M + rR$ obsahuje 1 a teda to nie je vlastný ideál (presnejšie, že $M + rR = R$) a preto je to ekvialentné s faktom, že M je maximálny ideál. □

Pripomeňme si definíciu prvoideálu:

Definícia 4.6.5 *ideál $I \subsetneq R$ sa nazýva prvoideál ak $ab \in I \Rightarrow (a \in I \vee b \in I)$ (ekvivalentne pre ideály A, B platí $AB \subseteq I \Rightarrow (A \subseteq I \vee B \subseteq I)$).*

Maximálne ideály sú (v komutatívnych okruhoch s jednotkou) prvoideály. Naopak to neplatí, napr. $\{0\}$ je prvoideál v $(Z, +, \cdot)$, ale nie je to maximálny ideál. Pri prvoideáloch má zmysel hovoriť o minimálnych ideáloch v zmysle nasledujúcej lemy:

Lema 4.6.6 *Nech ideál A je podmnožinou nejakého prvoideálu B, potom množina prvoideálov P takých, že $A \subseteq P \subseteq B$ má minimálne prvky.*

Dôkaz. Opäť použijeme Zornovu lemu. Zoberme množinu $M = \{P; P \text{ je prvoideál a } A \subseteq P \subseteq B\}$. M je neprázdna, nech $N \subseteq M$ je reťazec, t.j. každé dva prvky z N sú porovnateľné reláciou inklúzie ($\subseteq$). Potom $\bigcap N$ je prvoideál.

Určite vieme, že $\bigcap N$ je ideál (prienik ideálov je ideál). Nech $ab \in \bigcap N$, a $b \notin \bigcap N$, nech teda $P_0 \in N$ je taký, že $b \notin P_0$. Keďže $ab \in P_0$, musí byť $a \in P_0$. Nech $P \in N$ je taký, že $P \subseteq P_0$. Potom $b \notin P \subseteq P_0$ a preto $a \in P$.Nech $P \in N$ je taký, že $P_0 \subseteq P$. Potom keďže $a \in P_0$, je aj $a \in P$. Teda pre všetky $P \in N$ sme dostali, že $a \in P$ a preto $\bigcap N$ je prvoideál. Čiže každý reťazec v M má dolné ohraničenie a preto má minimálne prvky. □

Nasledujúce dva pojmy majú v teórii okruhov veľký význam:

Definícia 4.6.7 *Nech R je okruh. Ideál $Rad(R) = \bigcap\{M;\ M \text{ je maximálny ideál okruhu } R\}$ nazývame (Jacobsonov) radikál okruhu R.*
Ideál $rad(R) = \bigcap\{P;\ P \text{ je prvoideál okruhu } R\}$ nazývame nil-radikál okruhu R.

Zrejme pre každý (komutatívny, s 1) okruh platí, že $rad(R) \subseteq Rad(R)$ (každý maximálny ideál je prvoideál).

Nasledujúce dve vety popisujú $Rad(R)$ a $rad(R)$ v jazyku prvkov.

Veta 4.6.8 *Nech R je okruh, $r \in R$. Potom $r \in Rad(R) \Leftrightarrow (\forall x \in R)\ 1 - rx$ je invertibilný.*

Dôkaz. Konkrétny element tvaru $1 - rx$ je invertibilný práve vtedy, keď pre všetky maximálne ideály M, platí, že $1 - rx$ do nich nepatrí. To ale podľa lemy 4.6.4 znamená, že r je prvkom každého maximálneho ideálu M.

Inak: $A' \Leftrightarrow B'$: $(\exists x \in R)\ 1 - rx$ nie je invertibilný $\Leftrightarrow (\exists x \in R)(\exists M)\ M$ je maximálny ideál a $1 - rx \in M \Leftrightarrow (\exists M)\ M$ je maximálny ideál a $r \notin M \Leftrightarrow r \notin Rad(R)$. □

Veta 4.6.9 *Nech R je okruh, $r \in R$. Potom $r \in rad(R) \Leftrightarrow r$ je nilpotentný.*

Dôkaz. Nech $r \in R$ nie je nilpotentný, t.j. množina $T = \{1, r, r^2, \ldots, r^n, \ldots\}$ neobsahuje 0. Ideál $I = \{0\}$ má s množinou T prázdny prienik a preto existuje maximálny ideál P s vlastnosťou $P \cap T = \emptyset$.

Dokážeme, že P je prvoideál. Sporom. Nech $ab \in P$ sú také, že $a, b \notin P$. Potom vzhľadom na maximalitu P platí, že ideály $P + aR$ a $P + bR$ majú s T neprázdny prienik, nech povedzme $r^n \in P + aR$ a $r^m \in P + bR$.

Potom $r^{n+m} = r^n \cdot r^m \in (P + aR)(P + bR) \subseteq P + abR$. Podľa predpokladu ale $ab \in P$ a teda $P + abR = P$. Čiže $r^{n+m} \in P$, čo je spor s predpokladom.

Takže sme dokázali tvrdenie, že $r \in R$ nie je nilpotentný práve vtedy, keď existuje taký prvoideál P, že $r \notin P$, čo je ekvivalentné s tvrdením vety (ekvivalencia negácií). □

V dôkaze vety sme využili len isté vlastnosti množiny T, hlavne fakt, že ak $r^n, r^m \in T$, tak aj $r^n \cdot r^m \in T$, sformulujme si ich do bodov:

1. $a, b \in T$, tak aj $a \cdot b \in T$
2. $1 \in T$
3. $0 \notin T$

Jednotkový prvok 1 môžeme pokladať za súčin prvkov patriacich do prázdnej množiny $\emptyset$, namiesto bodov 1 a 2 môžeme hovoriť, že T je uzavretá na konečné súčiny. Dostaneme tak lemu

Lema 4.6.10 *Nech $T \subseteq R$ je množina uzavretá na konečné súčiny neobsahujúca 0. Potom maximálny ideál, ktorý má s T prázdny prienik je prvoideál.*

Keď zoberieme $T = \{1\}$, je to množina spĺňajúca predpoklady predošlej lemy a preto maximálny ideál, ktorý má prázdny prienik s T — čo je v tomto prípade "štandardný" maximálny ideál — je prvoideál. Toto je samozrejme známa skutočnosť, ale dôkaz teraz neprechádzal cez faktorizáciu.

Definícia 4.6.11 *Okruh R sa nazýva poloprimitívny (polojednoduchý) ak $Rad(R) = \{0\}$. Okruh R sa nazýva poloprvotný ak $rad(R) = \{0\}$.*

Vzhľadom na inklúziu $rad(R) \subseteq Rad(R)$ vidíme, že poloprimitívny okruh je poloprvotný. Nasledujúca veta ukazuje, ako sú tieto pojmy prepojené pomocou faktorizácie.

Veta 4.6.12 *Okruh $R/Rad(R)$ je poloprimitívny a okruh $R/rad(R)$ je poloprvotný.*

Dôkaz. Časť o $R/Rad(R)$: Potrebujeme dokázať, že $Rad(R/Rad(R)) = \{\mathbf{0}\}$, kde $\mathbf{0} = 0 + Rad(R) \in R/Rad(R)$. Použijeme charakterizáciu, ktorá hovorí, že $r \in Rad(R) \Leftrightarrow (\forall x \in R)\ 1 - rx$ je invertibilný. V našom prípade teda $r+Rad(R) \in Rad(R/Rad(R))$ práve vtedy, keď $(\forall x+Rad(R) \in R/Rad(R))\ (1+Rad(R))-(r+Rad(R))(x+Rad(R))$ je invertibilný v $R/Rad(R)$.

Prepíšme poslednú časť pomocou "kongruencie", dostaneme $(1-rx)$ je invertibilný $\mod Rad(R)$, t.j. existuje také $y \in R$, že $(1-rx)y = 1 \mod Rad(R)$. Preto $1 - y(1-rx) \in Rad(R)$, čo znamená, že pre každé $z \in R$ je $1 - z(1 - y(1-rx)))$ je invertibilný, špeciálne pre $z = 1$ dostaneme, že $y(1-rx)$ je invertibilný a teda existuje také $u \in R$, že $uy(1-rx) = 1$. Toto ale znamená, že $1 - rx$ je invertibilný (pre všetky $x \in R$), t.j. $r \in Rad(R)$.

Dokázali sme teda, že $r + Rad(R) \in Rad(R/Rad(R)) \Leftrightarrow r \in Rad(R)$.

Časť o $R/rad(R)$: Použijeme chrakterizáciu $rad(R)$ cez nilpotentnosť. $r + rad(R)rad(R/rad(R))$ práve vtedy, keď existuje také n, že $r^n + rad(R) = 0 + rad(R)$, t.j. $r^n \in rad(R)$. Ale prvky $rad(R)$ sú nilpotentné prvky, t.j. existuje m také, že $(r^n)^m = 0$, čiže $r^{nm} = 0$ a teda r je nilpotentný nad R a teda $r \in rad(R)$.

Dokázali sme teda, že $r + rad(R) \in rad(R/rad(R)) \Leftrightarrow r \in rad(R)$. □

Teraz sa pokúsime popísať poloprimitívne a poloprvotné okruhy pomocou špeciálneho typu súčinu "peknýchˮ okruhov. Najprv uvedieme definíciu tzv. polopriameho súčinu okruhov — tento typ súčinu sa veľmi intenzívne využíva a skúma v univerzálnej algebre, špeciálny prípad jednej z netriviálnych viet o tomto type súčinu si uvedieme v nasledujúcom odseku.

Treba dať pozor na to, že pre grupy má názov "polopriamy súčin" iný význam, nižšie uvedená definícia zodpovedá tzv. podpriamemu súčinu.

Definícia 4.6.13 *Hovoríme, že okruh R je polopriamy súčin systému okruhov $\{S_i;\ i \in I\}$ ak existuje monomorfizmus (injektívny homomorfizmus) $\kappa : R \mapsto \prod_{i\in I} S_i$ taký, že kompozície s projekciami $\pi_i \circ \kappa : R \mapsto S_i$ sú surjektívne.*

Voľne povedané, podokruh R priameho súčinu $\prod_{i\in I} S_i$ je polopriamy súčin, ak projekcia z R na každú zložku je surjektívna.

Najprv si uveďme charakterizáciu polopriamych súčinov.

Veta 4.6.14 *Okruh R je polopriamy súčin okruhov $S_i;\ i \in I$ práve vtedy, keď existujú také ideály $K_i;\ i \in I$ okruhu R, že pre všetky $i \in I$ je $R/K_i \cong S_i$ a $\bigcap_{i\in I} K_i = \{0\}$.*

Dôkaz. Nech teda R je polopriamy súčin $S_i;\ i \in I$ a $\kappa : R \mapsto \prod_{i\in I} S_i$ je taký monomorfizmus, že kompozície s projekciami $\pi_i \circ \kappa : R \mapsto S_i$ sú surjektívne.

Pre $i \in I$ položme $K_i = \mathrm{Ker}\,(\pi_i \circ \kappa)$. Vďaka surjektívnosti $\pi_i \circ \kappa$ a vete o homomorfizmoch vieme, že $R/K_i \cong S_i$.

Ak $a \in \bigcap_{i\in I} K_i$, tak pre všetky $i \in I$ je $(\pi_i \circ \kappa)(a) = 0$, t.j. $\kappa(a) = 0$ a teda $a = 0$, lebo κ je injektívny homomorfizmus. Takže $\bigcap_{i\in I} K_i = \{0\}$.

Naopak, nech existujú také ideály $K_i;\ i \in I$, že $\bigcap_{i\in I} K_i = \{0\}$. Položme $S_i = R/K_i$ pre $i \in I$ a $\kappa : R \mapsto \prod_{i\in I} S_i$ definujme vzťahmi $f = \kappa(a)$ ak $f(i) = a + K_i \in S_i$, čiže $\kappa(a)(i) = a + K_i$.

Takto definované κ je zrejme homomorfizmus. Ľahko overíme, že je injektívny: nech $a \in \mathrm{Ker}\,\kappa$, t.j. pre všetky $i \in I$ je $\kappa(a)(i) = 0 + K_i$, ale podľa našej definície to znamená, že $a \in K_i$ pre všetky $i \in I$ a teda $a \in \bigcap_{i\in I} K_i = \{0\}$, čiže $\mathrm{Ker}\,\kappa = \{0\}$, preto je κ monomorfizmus.

Ešte potrebujeme overiť surjektívnosť zobrazení $\pi_i \circ \kappa$: zoberme $a + K_i \in S_i$. Potom $(\pi_i \circ \kappa)(a) = \kappa(a)(i) = a + K_i$, čo je presne požadovaná surjektívnosť. □

Kombináciou tejto vety s tým, čo vieme o poloprimitívnych a poloprvotných okruhoch dostaneme

Dôsledok 4.6.15 *(Komutatívny, s jednotkou) okruh R je polopriamy súčin polí práve vtedy, keď je to poloprimitívny okruh. Je polopriamy súčin oborov integrity práve vtedy, keď je to poloprvotný okruh.*

Dôkaz. Okrem predošlej lemy asi treba len pripomenúť, že pre nejaký ideál I okruhu R je R/I pole práve vtedy, keď je I maximálny ideál (preto polia verzus Rad(R) a teda polia a poloprimitívnosť). R/I je obor integrity práve vtedy keď je I prvoideál a preto obory integrity a poloprvotnosť. □

Dôsledok 4.6.16 *(Komutatívny, s jednotkou) okruh R je poloprvotný práve vtedy, keď je izomorfný s podokruhom priameho súčinu oborov integrity.*

Dôkaz. Podľa predošlého dôsledku je priamy súčin oborov integrity poloprvotný okruh a podokruh poloprvotného okruhu je poloprvotný (lebo niltpotenosť prvku "nezávisí" od toho, či ju skúmame z hľadiska okruhu alebo podokruhu), a aj každý okruh izomorfný s poloprvotným okruhom je poloprvotný okruh.

Naopak, ak je okruh R poloprvotný, je to polopriamy súčin oborov integrity a preto je izomorfný s podokruhom priameho súčinu oborov integrity. □

Dôsledok 4.6.17 *(Komutatívny, s jednotkou) okruh R je poloprvotný práve vtedy, keď je izomorfný s podokruhom priameho súčinu polí.*

Dôkaz. Tento dôsledok vyplýva z predošlého dôsledku a faktu, že každý obor integrity sa dá vložiť do nejakého poľa (napr. do svojho "poľa zlomkov"). □

4.6.2 Birkhoffova veta

V súvisosti s polopriamymi súčinmi má zmysel hovoriť o polopriamo nerozložiteľných okruhoch (alebo všeobecnejšie polopriamo nerozložiteľných univerzálnych algebrách).

Definícia 4.6.18 *Okruh R sa nazýva polopriamo nerozložiteľný práve vtedy, keď je prienik všetkých nenulových ideálov nenulový ideál.*

Zmysel tejto definície je asi najlepšie vidieť z vety 4.6.14. Z tejto vety je tiež vidieť, že polopriama nerozložiteľnosť okruhu je ekvivalentná s tým, že ak R napíšeme ako polopriamy súčin (alebo aj ako priamy súčin) nejakého systému okruhov, tak jeden z tých okruhov je izomorfný s okruhom R, alebo tiež s tým, že existuje najmenší nenulový ideál okruhu R.

Nasledujúca veta je vlastne špeciálny prípad veľmi všeobecnej vety z univerzálnej algebry, tzv. Birkhoffovej vety.

Veta 4.6.19 *Každý okruh je polopriamy súčin polopriamo nerozložiteľných okruhov.*

Dôkaz. Pre každý prvok $0 \neq r \in R$ vyberme jeden ideál M_r, ktorý je maximálny spomedzi takých ideálov I, že $r \notin I$ (t.j. $I \subseteq R - \{r\}$). Existencia ideálov M_r vyplýva z lemy 4.6.2.

Očividne $\bigcap_{r\in R\setminus\{0\}} M_r = \{0\}$ a teda R je podľa lemy 4.6.14 polopriamym súčinom príslušných faktorových okruhov, t.j. s $\prod_{r\in R\setminus\{0\}} R/M_r$.

Ešte dokážeme, že každý z okruhov R/M_r je polopriamo nerozložiteľný. Keď zoberieme kanonický homomorfizmus $\psi : R \mapsto R/M_r$ a nejaký nenulový ideál J okruhu R/M_r, tak $\psi^{-1}(J)$ je ideál v R, a má vlastnosť, že $M_r \subsetneq \psi^{-1}(J)$, t.j. špeciálne $r \in \psi^{-1}(J)$. Ideál M_r je preto podmnožina prieniku ideálov v tvare $\psi^{-1}(J)$. Ale tento prienik nemôže byť priamo M_r, lebo r do toho prieniku patrí, ale nepatrí do M_r. □

Kapitola 5

Hilbertova veta o nulách

5.1 Celé rozšírenia okruhov

V celej tejto časti budeme pracovať s komutatívnymi okruhmi s jednotkou.

Definícia 5.1.1 *Ak je okruh A podokruhom okruhu $(R, +, \cdot)$, okruh R nazývame rozšírením A (pri tom musí byť jednotka okruhu A jednotkou okruhu R).*

Ak je R rozšírením okruhu A, tak prvok $\alpha \in R$ nazývame celým prvkom nad A, ak existuje normovaný polynóm $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$ taký, že $f(\alpha) = 0$.

Ak je každý prvok rozšírenia R okruhu A celý prvok nad A, hovoríme, že okruh R je celé rozšírenie A.

Definícia 5.1.2 *$A-$modul M sa nazýva A exaktný (alebo exaktný nad A), ak z rovnosti $a \cdot M = \{\mathbf{0}\}$ pre $a \in A$ vyplýva $a = 0$.*

Poznámka. Ako za chvíľu uvidíme, dôležitý je fakt, že normovaným polynómom môžeme so zvyškom deliť ľubovoľný polynóm.

Lema 5.1.3 *Nech R je rozšírenie okruhu A. Nasledujúce podmienky sú ekvivalentné: 1. $\alpha \in R$ je celý prvok nad A*

2. okruhové rozšírenie $A[\alpha]$ je konečne generovaný $A-$modul

3. Existuje $A-$modul M, ktorý je konečne generovaný (nad A), ktorý je zároveň $A[\alpha]-$modulom a je exaktný nad $A[\alpha]$

Dôkaz. 1$\Rightarrow$ 2: Nech $\beta \in A[\alpha]$, $\beta = b_m\alpha^m + \cdots + b_1\alpha + b_0$, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ je taký, že $f(\alpha) = 0$, $g(x) = b_mx^m + \cdots + b_1x + b_0$ a nakoniec nech $g(x) = p(x)f(x) + r(x)$ je delenie so zvyškom, t.j. $r(x) = 0$ alebo $\mathrm{st}(r) < \mathrm{st}(f) = n$. V prvom prípade je $\beta = 0$, v druhom prípade, ak $r(x) = r_kx^k + \cdots + r_1x + r_0$, t.j. $k < n$, tak $\beta = r_k\alpha^k + \cdots + r_1\alpha + r_0$. To znamená, že prvky $1, \alpha, \ldots, \alpha^{n-1}$ generujú $A[\alpha]$ ako A-modul.

2 $\Rightarrow$ 3: Stačí položiť $M = A[\alpha]$. Vďaka tomu, že $1 \in A[\alpha]$, je M exaktný nad $A[\alpha]$.

3 $\Rightarrow$ 1: Nech je M konečne generovaný A-modul, ako A-modul nech je generovaný prvkami $w_1, \ldots, w_n$. Keďže M je $A[\alpha]-$modul, platí, že $\alpha \cdot M \subseteq M$. Potom pre každé i je zrejme $\alpha w_i \in M$ a teda existujú prvky $a_{ij} \in A$ také, že

$$\alpha w_i = a_{i1}w_1 + \cdots + a_{in}w_n$$

pre $i = 1, \ldots, n$. Odtiaľ dostávame (po prehodení pravej časti na ľavú a nahradením ľavej časti nulami), že determinant $|\alpha I - A| \cdot M = \{\mathbf{0}\}$, kde $A = ||a_{ij}||$ a preto vďaka exaktnosti M nad $A[\alpha]$[1] je $|\alpha I - A| = 0$. Zmenou na $|xI - A|$ dostávame normovaný polynóm z $A[x]$ s koreňom α, teda α je celý prvok nad A. □

Dôsledok 5.1.4 *Nech B je celé rozšírenie okruhu A, B je konečne generované nad A (ako okruh, t.j. existuje konečne veľa prvkov $\alpha_1, \ldots, \alpha_n$ tak, že $B = A[\alpha_1, \ldots, \alpha_n]$). Potom B je konečne generovaný A-modul.*

Veta 5.1.5 *Nech $A \subseteq B \subseteq C$ je postupnosť rozšírení okruhov (t.j. C je rožšírenie B a B je rošírenie A). Potom C je celé rozšírenie A práve vtedy, keď C je celé rozšírenie B a B je celé rozšírenie A.*

[1] Tu je použité tvrdenie o determinantoch, hovoriace: Ak je M konečne generovaný $A-$modul, generovaný prvkami $w_1, \ldots, w_n$ a pre maticu N nad A platí $N(w_1, \ldots, w_n)^T = (0, \ldots, 0)^T$, tak pre všetky i platí $\det(N) \cdot w_i = 0$, t.j. aj $\det(N) \cdot M = \{\mathbf{0}\}$. Dôkaz je založený na fakte, že $adj(N) \cdot N = \det(N) \cdot I$, t.j. $\det(N) \cdot (w_1, \ldots, w_n)^T = \det(N) \cdot I \cdot (w_1, \ldots, w_n)^T = adj(N) \cdot N \cdot (w_1, \ldots, w_n)^T = adj(N) \cdot (0, \ldots, 0)^T = (0, \ldots, 0)^T$.

Dôkaz. Implikácia $\Rightarrow$ je zrejmá. Naopak, nech C je celé rozšírenie B a B je celé rozšírenie A. Dokážeme, že C je celé rozšírenie A.

Nech $\alpha \in C$. Keďže C je celé nad B, existuje polynóm $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in B[x]$ taký, že $f(\alpha) = 0$. Položme $B_0 = A[b_0, \ldots, b_{n-1}]$. B_0 je podľa predošlej vety konečne generovaný $A-$modul (lebo $B_0 \subseteq B$ a preto je to celé rozšírenie A). Ďalej položme $B_1 = B_0[\alpha]$. Keďže B_1 je modul nad B_0 a α je celý prvok nad B_0, je B_1 ako modul nad B_0 konečne generovaný. Z konečnej generovanosti $A-$modulu B_0 teraz vyplýva, že B_1 je tiež konečne generovaný nad A. Keďže $A[\alpha] \subseteq B_1$ a $1 \in B_1$, je B_1 exaktný nad $A[\alpha]$. Podľa podmienky 3 lemy je preto prvok α celý nad A a teda C je celé rozšírenie A. □

Veta 5.1.6 *Nech B je rozšírenie okruhu A, $\alpha \in B$. Ak α je celý prvok nad A, tak rošírenie $A[\alpha]$ je celé rozšírenie A.*

Dôkaz. Nech $\beta \in A[\alpha]$. $A[\alpha]$ je konečne generovaný $A-$modul a keďže $A[\beta] \subseteq A[\alpha]$ a $1 \in A[\alpha]$, je $A[\alpha]$ exaktný modul nad $A[\beta]$. Preto je β celý prvok nad A. Teda $A[\alpha]$ je celé rozšírenie A. □

Dôsledok 5.1.7 *Nech C je rozšírenie okruhu A, B je množina prvkov z C, ktoré sú celé nad A. Potom B je podokruh okruhu C.*

Dôkaz. Podľa predošlej vety, ak $\alpha, \beta \in C$ sú celé nad A, tak $A \subseteq A[\alpha] \subseteq A[\alpha, \beta]$ je postupnosť rozšírení okruhov, pričom $A[\alpha]$ je celý nad A a $A[\alpha, \beta]$ je celý nad $A[\alpha]$. Preto je $A[\alpha, \beta]$ celý nad A. Prvky $\alpha \pm \beta, \alpha\beta \in A[\alpha, \beta]$ sú preto celé prvky nad A a preto je B okruh. □

Veta 5.1.8 *Nech B je celé rozšírenie okruhu A, $\sigma\colon B \to R$ je homomorfizmus okruhov. Potom $\sigma(B)$ je celý nad $\sigma(A)$.*

Dôkaz. Ak $\alpha \in B$ a $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$ je taký, že $f(\alpha) = 0$. Potom aplikáciou σ dostaneme

$$\sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(a_0) = 0$$

a teda máme normovaný polynóm s koeficientami v $\sigma(A)$, ktorého koreňom je $\sigma(\alpha)$. □

Dôsledok 5.1.9 *Nech B je celé rozšírenie okruhu A, nech I je ideál B taký, že $I \subseteq A$. Potom B/I je celé rozšírenie A/I.*

Ak je I ideál okruhu B, potom $A/I = \{a+I; a \in A\}$ ako podokruh okruhu B/I je izomorfný s okruhom $A/(A \cap I)$ a vzhľadom na tento izomorfizmus je B/I celý nad okruhom $A/(A \cap I)$.

Dôkaz. Pri druhej časti je treba uvážiť zloženie homomorfizmov

$$A \to B \to B/I,$$

kde prvý homomorfizmus je vloženie a druhý je kanonická projekcia. Jadrom kompozície týchto dvoch homomorfizmov zrejme je $A \cap I$ a obrazom tejto kompozície je $A/I = \{a + I; a \in A\}$. Tvrdenie teda vyplýva z vety o homomorfizmoch a prvej časti dôsledku.

□

Lema 5.1.10 *(Nakayama) Nech A je okruh, $I \subseteq Rad(A)$ (t.j. I je ideál obsiahnutý v každom maximálnom ideále okruhu A), M je konečnegenerovaný A-modul. Potom ak $IM = M$, tak $M = \{0\}$.*

Dôkaz. Dôkaz urobíme indukciou vzhľadom na počet generátorov A-modulu M. Nech je M ako A-modul generovaný prvkami $w_1, \ldots, w_n$. Keďže $M = IM$, prvok w_1 sa dá napísať ako lineárna kombinácia

$$w_1 = a_1w_1 + \cdots + a_nw_n$$

kde $a_i \in I$ a teda

$$(1 - a_1)w_1 = a_2w_2 + \cdots + a_nw_n$$

Ak prvok $1 - a_1$ nie je deliteľ jednotky v A, existuje maximálny ideál I_M okruhu A, do ktorého patrí. Keďže $a_1 \in I \subseteq I_M$, dostávame, že $1 \in I_M$, čo nie je možné. Teda $1 - a_1$ je deliteľ jednotky v A. Ak $(1 - a_1)u = 1$, $u \in A$ potom

$$w_1 = (1 - a_1)uw_1 = a_2uw_2 + \cdots + a_nuw_n$$

a teda M je generovaný $n-1$ prvkami. Postupne dokážeme, že $M = \{0\}$. □

Ak $\mathfrak{p}$ je prvoideál okruhu A, $S = A \setminus \mathfrak{p}$ a B je rozšírenie A, budeme písať $B_\mathfrak{p}$ namiesto $S^{-1}B$ (okruh zlomkov s menovateľmi z S. Toto by možno bolo vhodné popísať podrobnejšie, ale konštrukcia je rovnaká ako pri konštrukcii podielového poľa pre obor integrity, dôležitý je fakt, že $\mathfrak{p}$ je prvoideál a teda aj pri sčítaní aj násobení "zlomkov", ktorých menovatele sú z S (nie sú z $\mathfrak{p}$), menovateľ výsledného zlomku je tiež prvok S (nie je z $\mathfrak{p}$) — overte si to). Na $B_\mathfrak{p}$ sa dá hľadieť ako na $A_\mathfrak{p} = S^{-1}A$-modul. Okruh $A_\mathfrak{p}$ má práve jeden maximálny ideál (t.j. je to tzv. lokálny okruh) a to množinu tých zlomkov x/y pre ktoré je čitateľ $x \in \mathfrak{p}$. Táto množina (označme ju $m_\mathfrak{p}$) je zrejme ideál. Ak $x \notin \mathfrak{p}$ tak y/x je inverzný ku x/y - faktorizácia $A_\mathfrak{p}/m_\mathfrak{p}$ je pole a preto $m_\mathfrak{p}$ je maximálny ideál $A_\mathfrak{p}$. Nech $x/y \in A_\mathfrak{p}$ nie je deliteľ jednotky v $A_\mathfrak{p}$. To znamená, že $y/x \notin A_\mathfrak{p}$. Teda $x \in \mathfrak{p}$ a preto $m_\mathfrak{p}$ je jediný maximálny ideál.

Ľahko sa dá overiť, že ak je B celým rozšírením A, tak $B_\mathfrak{p}$ ako okruh je celým rozšírením okruhu $A_\mathfrak{p}$ - priamo nájdeme príslušný normovaný polynóm.

Definícia 5.1.11 *Nech B je rozšírenie A, $\mathfrak{p}$ je prvoideál v A a $\mathfrak{P}$ je prvoideál v B. Hovoríme, že $\mathfrak{P}$ leží nad $\mathfrak{p}$, ak $\mathfrak{P} \cap A = \mathfrak{p}$.*

Veta 5.1.12 *Nech B je celé rozšírenie okruhu A, $\mathfrak{p}$ je prvoideál okruhu A. Potom $\mathfrak{p}B \neq B$ a existuje prvoideál $\mathfrak{P}$ okruhu B taký, že $\mathfrak{P} \cap A = \mathfrak{p}$ (t.j. $\mathfrak{P}$ leží nad $\mathfrak{p}$).*

Dôkaz. Podľa poznámky vyššie je okruh $B_\mathfrak{p}$ celý nad okruhom $A_\mathfrak{p}$ a vieme, že $A_\mathfrak{p}$ je lokálny okruh. Ak je $\mathfrak{p}$ prvoideál A a $m_\mathfrak{p}$ maximálny ideál okruhu $A_\mathfrak{p}$ a $\mathfrak{p}B = B$, potom plati

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}S^{-1}AB_\mathfrak{p} = S^{-1}\mathfrak{p}B_\mathfrak{p} = m_\mathfrak{p}B_\mathfrak{p}$$

a tiež $\mathfrak{p}B_\mathfrak{p} = B_\mathfrak{p}$. Teda aj $m_\mathfrak{p}B_\mathfrak{p} = B_\mathfrak{p}$. To znamená, že tvrdenie stačí dokázať pre prípad, keď je A lokálny okruh. Nech teda pre prvoideál $\mathfrak{p}$ lokálneho okruhu A platí: $\mathfrak{p}B = B$. Potom $1 \in \mathfrak{p}B$, t.j. existujú $a_1, \ldots, a_n \in \mathfrak{p}$, $b_1, \ldots, b_n \in B$ také, že

$$1 = a_1b_1 + \cdots + a_nb_n$$

Okruh $A[b_1, \ldots, b_n]$ je konečne generovaný A modul, označme ho B_0. Pre tento modul je splnená rovnosť $\mathfrak{p}B_0 = B_0$. Totiž $\mathfrak{p}B_0 \subseteq AB_0 = B_0$. Naopak, keďže $1 \in B_0$, je $B_0 = B_0B_0$ a keďže $1 \in \mathfrak{p}B_0$, tak $B_0 \subseteq \mathfrak{p}B_0B_0 = \mathfrak{p}B_0$. Tiež sú splnené aj ostatné predpoklady Nakayamovej lemy (nezabudnime, že pracujeme s lokálnym okruhom A a teda prvoideál $\mathfrak{p}$ je podmnožinou jediného - a teda všetkých maximálnych ideálov v okruhu A). Z Nakayamovej lemy plynie, že $B_0 = \{0\}$, čo nie je možné, lebo $A \subseteq B_0$. Preto $\mathfrak{p}B \neq B$.

To znamená, že pre špeciálny prípad prvoideálu $m_\mathfrak{p}$ okruhu $A_\mathfrak{p}$ a jeho celého rozšírenia $B_\mathfrak{p}$ platí, že $m_\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$ a preto existuje maximálny ideál $\mathfrak{M}_\mathfrak{p}$ okruhu $B_\mathfrak{p}$ taký, že

$$m_\mathfrak{p}B_\mathfrak{p} \subseteq \mathfrak{M}_\mathfrak{p}.$$

Pozrime sa na komutatívny diagram

$$\begin{array}{ccc} B & \to & B_\mathfrak{p} \\ \uparrow & & \uparrow \\ A & \to & A_\mathfrak{p} \end{array}$$

Vzor ideálu $\mathfrak{M}_\mathfrak{p}$ v $A_\mathfrak{p}$ je vlastný (lebo $1 \notin \mathfrak{M}_\mathfrak{p}$) ideál, ktorý je nad $m_\mathfrak{p}$ a keďže $m_\mathfrak{p}$ je maximálny v $A_\mathfrak{p}$, je tento vzor presne $m_\mathfrak{p}$. Ak zoberieme vzor $\mathfrak{M}_\mathfrak{p}$ v B (a označíme ho $\mathfrak{M}$), vieme, že $\mathfrak{M}$ je prvoideál (jadro netriviálneho homomorfizmu do poľa je prvoideál). Vzhľadom na to, že $\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p}$, je vzor $\mathfrak{m}_\mathfrak{p}$ v okruhu A rovný práve $\mathfrak{p}$ a z komutativity uvedého diagramu dostávame, že $A \cap \mathfrak{M} = \mathfrak{p}$, t.j. $\mathfrak{M}$ je prvoideál ležiaci nad $\mathfrak{p}$. □

Veta 5.1.13 *Nech B je celé rozšírenie okruhu A, $\mathfrak{p}$ je prvoideál okruhu A. Prvoideál $\mathfrak{P}$ okruhu B ležiaci nad prvoideálom $\mathfrak{p}$ okruhu A je maximálny (v B) práve vtedy, keď je $\mathfrak{p}$ maximálny (v A).*

Dôkaz. Nech $\mathfrak{p}$ je maximálny v A. Potom $A/\mathfrak{p}$ je pole a $B/\mathfrak{P}$ je podľa dosledku 5.1.9 celým rozšírením poľa $A/\mathfrak{p}$. Preto ľubovoľný prvok $0 \neq \alpha \in B/\mathfrak{P}$ je celý nad poľom $A/\mathfrak{p}$, ale to znamená, že je to algebraický prvok a preto $(A/\mathfrak{p})[\alpha]$ je algebraické rozšírenie poľa a preto je to pole. Ale pole $(A/\mathfrak{p})[\alpha]$ je podokruhom okruhu $B/\mathfrak{P}$. To znamená, že každý prvok $0 \neq \alpha \in B/\mathfrak{P}$ ako prvok poľa má inverzný prvok, t.j. $B/\mathfrak{P}$ je pole a preto je $\mathfrak{P}$ maximálny ideál.

Naopak, nech $\mathfrak{P}$ je maximálny v B. Teda $B/\mathfrak{P}$ je pole, ktoré je celým rozšírením okruhu $A/\mathfrak{p}$. Ak $A/\mathfrak{p}$ nie je pole, obsahuje netriviálny maximálny ideál, povedzme $\mathfrak{m}$. Podľa predošlej vety v $B/\mathfrak{P}$ existuje prvoideál $\mathfrak{M}$ ležiaci nad $\mathfrak{m}$ a samozrejme plati $\mathfrak{M} \neq \{0\}$ - spor (pole $B/\mathfrak{P}$ neobsahuje netriviálny ideál). □

5.2 Rozšírenia homomorfizmov

Veta 5.2.1 *Nech pole L je algebraické rozšírenie poľa F, K je algebraicky uzavreté pole, $\varphi\colon F \to K$ je homomorfizmus (polí). Potom existuje rozšírenie homomorfizmu φ na L.*

Dôkaz. Skúmajme systém dvojíc (E, ψ), E je nadpole F a podpole L a $\psi\colon E \to K$ je rozšírenie φ. Zaveďme na týchto dvojiciach reláciu (bude to usporiadanie) $\leq$ tak, že $(E, \psi) \leq (E', \psi')$ ak E je podpole E' a ψ' je rozšírenie ψ. Usporiadanie $\leq$ je induktívne a podľa Zornovej lemy má maximálny prvok. Tento maximálny prvok (E, ψ) musí mať prvú zložku $E = L$, inak totiž vieme urobiť rozšírenie ψ' homomorfizmu ψ na algebraickom rozšírení $E[\alpha]$ pre nejaké $\alpha \in L \setminus E$, α je algebraický prvok nad F - spor s maximalitou. □

Pozrime sa teraz na lokálny okruh. Nech A je okruh, $\mathfrak{p}$ je prvoideál v A. Množina (okruh) $A_\mathfrak{p}$ je okruh zlomkov x/y, kde $x, y \in A, y \notin \mathfrak{p}$. $A_\mathfrak{p}$ je lokálny okruh, jeho jediný maximálny ideál pozostáva zo zlomkov x/y, kde $x \in \mathfrak{p}$. Nech L je pole a $\varphi\colon A \to L$ je homomorfizmus, ktorého jadro je $\mathfrak{p}$ (pripomeňme, že jadro homomorfizmu do poľa je prvoideál). Potom φ môžeme rozšíriť na homomorfizmus $\varphi'\colon A_\mathfrak{p} \to L$ tak, že položíme

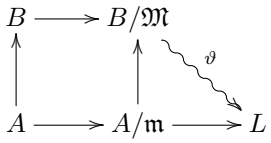
$$\varphi'(x/y) = \varphi(x)/\varphi(y)$$

Ďalej, nech A je lokálny okruh s maximálnym ideálom $\mathfrak{m}$, B je celé rozšírenie A, $\varphi\colon A \to L$ je homomorfizmus do nejakého algebraicky uzavretého poľa L, pričom $\mathfrak{m} = \operatorname{Ker}\varphi$. Existuje prvoideál $\mathfrak{M}$ v B ležiaci nad $\mathfrak{m}$ a tento je maximálny, lebo $\mathfrak{m}$ je maximálny, t.j. $\mathfrak{M} \cap A = \mathfrak{m}$ a $B/\mathfrak{M}$ je pole, ktoré je ako okruh celé nad $A/\mathfrak{m}$, čo je tiež pole a teda $B/\mathfrak{M}$ je algebraické rozšírenie poľa $A/\mathfrak{m}$. Samozrejme, pole $A/\mathfrak{m}$ je izomorfné podpoľu $\varphi(A)$ poľa L, lebo $\mathfrak{m} = \operatorname{Ker}\varphi$.

Môžeme vybrať taký izomorfizmus poľa $A/\mathfrak{m}$ na $\varphi(A)$, že kompozícia homomorfizmov

$$A \to A/\mathfrak{m} \to L$$

bude φ. Podľa vety o rozšírení homomorfizmu poľa na algebraické rozšírenie potom existuje také vloženie ϑ algebraického rozšírenia $B/\mathfrak{M}$ do L, že diagram



komutuje. Tým získame rozšírenie φ na B (do L).

Pomocou tohoto získame nasledujúcu vetu:

Veta 5.2.2 *Nech B je celé rozšírenie okruhu A, nech $\varphi\colon A \to L$ je homomorfizmus do algebraicky uzavretého poľa L. Potom φ má rozšírenie na $\varphi'\colon B \to L$.*

Dôkaz. Nech $\mathfrak{p}$ je jadro φ a $S = A \setminus \mathfrak{p}$ je príslušný doplnok. Máme komutatívny diagram

$$\begin{array}{ccccc} B & \to & S^{-1}B & & \\ \uparrow & & \uparrow & & \\ A & \to & S^{-1}A & = & A_\mathfrak{p} \end{array}$$

Homomorfizmus φ môžeme "prepustiť" cez kanonický homomorfizmus okruhu A do $A_\mathfrak{p} = S^{-1}A$. Okrem toho, okruh $S^{-1}B$ je celý nad $S^{-1}A$ a okruh $S^{-1}A = A_\mathfrak{p}$ je lokálny. Požadovaný výsledok teda dostaneme na základe predošlých úvah. □

5.3 Hilbertova veta o nulách

Aby sme mohli formulovať dôkaz nasledujúcej vety, potrebujeme pojem algebraickej nezávislosti množiny nad poľom a pojem bázy transcendentnosti.

Definícia 5.3.1 *Nech pole K je rozšírenie poľa k a $S \subseteq K$. Hovoríme, že S je algebraicky nezávislá nad k, ak z rovnosti*

$$0 = \sum a_{(\nu)} M_\nu(S) \quad (= \sum a_{(\nu)} \prod_{x \in S} x^{\nu(x)})$$

s koeficientami $a_{(\nu)} \in k$, ktoré sú (možno až na konečne mnoho nulové) vyplýva, že sú všetky nulové. V uvedenej rovnosti $M_\nu(S)$ je tzv. monomiál s prvkami z S, t.j. výraz tvaru $x_1^{k_1}x_2^{k_2}\dots x_l^{k_l}$ pre $x_1, \dots, x_l$ po dvoch rôzne prvky množiny S, samozrejme, predpokladáme, že ak $\nu \neq \mu$, tak $M_\nu(S) \neq M_\mu(S)$ - táto definícia $M_\nu(S)$ je naznačená rovnosťou uvedenou v zátvorke.

Zrejme množiny $S \subseteq K$ algebraicky nezávislé nad k tvoria vzhľadom na usporiadanie $\subseteq$ tvoria induktívnu množinu a preto na základe Zornovej lemy má maximálny prvok. Každý takýto maximálny prvok nazveme bázou transcendentnosti poľa K nad poľom k.

Poznámka: Ak $S = \{x\}$, t.j. S je jednoprvková, tak S je algebraicky nezávislá nad k práve vtedy, keď x je transcendentný prvok nad k.

Poznámka: zrejme pre bázu transcendentnosti S poľa K, rozšírenia poľa K nad k platí tvrdenie: K je algebraické rozšírenie $k(S)$. Pre zaujímavosť si uveďme jednu vetu, hovoriacu o základnej vlastnosti báz transcendentnosti. (Analógia Steinitzovej vety).

Veta 5.3.2 *Nech pole K je rozšírenie poľa k. Všetky bázy transcendentnosti poľa K nad poľom k majú rovnakú mohutnosť. Ak Γ je množina generátorov K nad k (t.j. $K = k(\Gamma)$) a $S \subseteq \Gamma$ je algebraicky nezávislá množina, potom existuje báza transcendentnosti $\mathcal{B}$ poľa K nad k taká, že*

$$S \subseteq \mathcal{B} \subseteq \Gamma.$$

Dôkaz. Dokážeme, že ak existuje jedna konečná báza transcendentnosti, povedzme $\{x_1, \dots, x_m\}, m \geq 1$, potom každá iná báza trancendentnosti tiež obsahuje m prvkov. Nech teda $w_1, \dots, w_n \in K$ sú algebraicky nezávislé prvky nad k. Dokážeme, že $n \leq m$ (rovnosť potom plynie zo symetrie tejto úlohy). Podľa predpokladu teda existuje nenulový polynóm f_1 v $m+1$ premenných s koeficientami v k taký, že

$$f_1(w_1, x_1, \dots, x_m) = 0.$$

V polynóme f_1 sa musí vyskytovať w_1 a aspoň jedno x_i, bez újmy na všeobecnosti nech je to x_1. Inak by nemohlo w_1 byť prvkom algebraicky nezávislej množiny. Preto je prvok x_1 algebraicky závislý nad $k(w_1, x_2, \dots, x_m)$. Predpokladajme ďalej, že po vhodnom prečíslovaní prvkov množiny $x_2, \dots, x_m$ nájdeme $w_1, \dots, w_r$ $(r < n)$ také, že K je algebraické nad

$$k(w_1, \dots, w_r, x_{r+1}, \dots, x_m).$$

Potom existuje nenulový polynóm f v $m+1$ premenných s koeficientami v k, pre ktorý

$$f(w_{r+1}, w_1, \dots, w_r, x_{r+1}, \dots, x_m) = 0,$$

pričom w_{r+1} sa skutočne v tomto polynóme vyskytuje. Znova, keďže sú $w_1, \dots, w_n$ nad k algebraicky nezávislé, musí sa v f vyskytovať aj niektorý z prvkov $x_{r+1}, \dots, x_m$ a po prečíslovaní môžeme predpokladať, že je to x_{r+1}. Potom je x_{r+1} algebraický nad

$$k(w_1, \dots, w_{r+1}, x_{r+2}, \dots, x_m).$$

Keďže algebraické rozšírenie algebraického rozšírenia je opäť algebraické rozšírenie, je K algebraické nad $k(w_1, \dots, w_{r+1}, x_{r+2}, \dots, x_m)$. Túto procedúru môžeme zopakovať niekoľkokrát a ak je $n \geq m$, zámenou všetkých prvkov "typu" x za prvky w vidíme, že K je algebraické nad $k(w_1, \dots, w_m)$. Tým je dokázané, že $n \geq m$ implikuje $n = m$. Týmto sme dokázali, že buď sú všetky bázy transcendentnosti K nad k konečné a majú rovnaký počet prvkov, alebo sú všetky nekonečné. Dôkaz rovnakej mohutnosti si urobte ako cvičenie. Rovnako ponecháme ako cvičenie tvrdenie o možnosti výberu bázy transcendentnosti z danej generujúcej množiny. □

Veta 5.3.3 *Nech k je pole, $k[x] = k[x_1, \dots, x_n]$ je konečne generovaný okruh nad k a $\varphi\colon k \to L$ je injektívny homomorfizmus do algebaricky uzavretého poľa L. Potom existuje rozšírenie φ na homomorfizmus z $k[x]$ do L.*

Dôkaz. Najprv ukážeme, že tvrdenie stačí dokázať v prípade, že $k[x]$ je pole. Nech je $\mathfrak{M}$ je maximálny ideál v $k[x]$ a nech $\sigma\colon k[x] \to k[x]/\mathfrak{M}$ je kanonická projekcia. Potom $\sigma k[\sigma x_1, \dots, \sigma x_n]$ je pole (lebo je to $k[x]/\mathfrak{M}$), ktoré je rozšírením poľa σk. Ak teda tvrdenie platí pre pole σk a jeho rozšírenie $\sigma k[\sigma x_1, \dots, \sigma x_n]$ s homomorfizmom $\varphi \circ \sigma^{-1}$ zúženým na σk, bude výsledné rozšírenie rozšírením na homomorfizmus z $k[x]$ do L. Ďalej, zrejme stačí uvažovať $L = \overline{k}$ a identické vnorenie.

Nech je teda $k[x]$ pole. Ak je algebraickým rozšírením k, výsledok sme dokázali vo vete 5.2.1. (Ako sa ukáže v dôsledku tejto vety, v skutočnosti nastáva práve tento prípad a žiadny iný, ale teraz to žiaľ nevieme.) Nech je $t_1, \dots, t_r$ báza transcendentnosti poľa $k[x]$ nad k, $r \geq 1$. Každý prvok $x_1, \dots, x_n$ je algrebraický nad $k(t_1, \dots, t_r)$. Keď vynásobíme polynóm $m_{x_i}(X)$ (minimálny polynóm prvku x_i nad poľom $k(t_1, \dots, t_r)$) vhodným nenulovým prvkom z $k[t_1, \dots, t_r]$ (napr. súčin menovateľov zlomkov jednotlivých koeficientov), dostaneme polynóm nulujúci

x_i s koeficientami z $k[t_1, \ldots, t_r]$. Nech vedúci koeficient takto získaného polynómu je $a_i(t_1, \ldots, t_r)$. Označme $t = t_1, \ldots, t_r$. Položme

$$a(t) = a_1(t) \ldots a_r(t)$$

Keďže je $a(t) \neq 0$, v poli $\overline{k}$ existujú prvky $t'_1, \ldots, t'_n$ také, že pre $t' = (t'_1, \ldots, t'_n)$ je $a(t') \neq 0$ a teda aj pre každé i je $a_i(t') \neq 0$. [2]

Zrejme každý prvok x_i je celý nad okruhom

$$k[t_1, \ldots, t_r, \frac{1}{a_1(t)}, \ldots, \frac{1}{a_r(t)}].$$

Uvažujme o homomorfizme

$$\varphi\colon k[t_1, \ldots, t_r] \to \overline{k},$$

ktorý je identita na k a pre ktorý je $\varphi(t_i) = t'_i$. Nech je prvoideál $\mathfrak{p}$ jeho jadro. Potom $a(t), a_i(t) \notin \mathfrak{p}$. Homomorfizmus φ má rozšírenie na $k[t]_{\mathfrak{p}}$ a podľa vety 5.2.2 aj na $k[t]_{\mathfrak{p}}[x_1, \ldots, x_n]$ (a obor hodnôt tohoto rozšírenia je $\overline{k}$). Ďalej vieme, že

$$k \subseteq k[t_1, \ldots, t_r] \subseteq k[t_1, \ldots, t_r]_{\mathfrak{p}},$$

a preto je aj

$$k[x_1, \ldots, x_n] \subseteq k[t_1, \ldots, t_r]_{\mathfrak{p}}[x_1, \ldots, x_n].$$

Teda uvedené rozšírenie je aj rozšírenie na $k[x_1, \ldots, x_n]$ a veta je dokázaná. □

Dôsledok 5.3.4 (Hilbertova veta o nulách, slabá forma) *Nech k je pole, $k[x] = k[x_1, \ldots, x_n]$ je konečne generovaný okruh nad k. Ak je $k[x]$ pole, potom je algebraické nad k.*

Dôkaz. Pomocou vloženia poľa k do svojho algebraického uzáveru $\overline{k}$ a predošlej vety dostaneme, že $k[x]$ má homomorfný obraz v $\overline{k}$. Posledne menovaný homomorfizmus, ako homomorfizmus poľa musí byť izomorfizmus (určite nie je triviálny). Ale všetky prvky v $\overline{k}$ sú algebraické nad k. Preto aj všetky prvky $k[x]$ sú algebraické nad k. □

Dôsledok 5.3.5 *Nech $k[x_1, \ldots, x_n]$ je konečne generovaný obor integrity nad poľom k a nech $y_1, \ldots, y_m$ sú nenulové prvky tohoto okruhu. Potom existuje taký homomorfizmus*

$$\varphi : k[x_1, \ldots, x_n] \to \overline{k},$$

že pre všetky $y_1, \ldots, y_m$ je $\varphi(y_i) \neq 0$.

Dôkaz. Stačí aplikovať predošlú vetu na okruh $k[x_1, \ldots, x_n, y_1^{-1}, \ldots, y_m^{-1}]$ a vnorenie k do $\overline{k}$ (ako podmnožina). Takže je definovaná hodnota $\varphi(y_i^{-1})$ a keďže $y_i \in k[x_1, \ldots, x_n] \subseteq k[x_1, \ldots, x_n, y_1^{-1}, \ldots, y_m^{-1}]$, je definovaná aj hodnota $\varphi(y_i)$ a pretože φ je homomorfizmus, platí, že $\varphi(y_i)\varphi(y_i^{-1}) = \varphi(y_i y_i^{-1}) = \varphi(1) = 1$ a preto $\varphi(y_i) \neq 0$ (a tiež $\varphi(y_i^{-1}) \neq 0$). □

Veta 5.3.6 *Nech k je algebraicky uzavreté pole. Maximálny ideál v okruhu polynómov viacerých premenných $k[X_1, \ldots, X_n]$ má tvar $(X_1 - a_1, \ldots, X_n - a_n)$ pre vhodné $a_1, \ldots, a_n \in k$.*

Dôkaz. D.Ú. □

Veta 5.3.7 (Hilbertova veta o nulách, originálna forma) *Nech I je ideál v $k[X] = k[X_1, \ldots, X_n]$ a každá nula $(c) = (c_1, \ldots, c_n)$ ideálu I (t.j. pre každý polynóm $f \in I$ je $f(c) = 0$) v $\overline{k}^n$ je nula polynomu viacerých premenných $f \in k[X]$, t.j. $f(c) = 0$. Potom existuje $m \geq 0$ také, že $f^m \in I$.*

Dôkaz. Sporom, nech pre každé $m \geq 0$ platí: $f^m \notin I$. Označme $S = \{f^m; m \in N\}$, S je uzavretá na konečné súčiny a preto maximálny ideál J taký, že $I \subseteq J$ a $J \cap S = \emptyset$ je prvoideál (dokazovali sme to v časti o radikáloch, lema 4.6.10). Uvažujme o

$$k[X_1, \ldots, X_n]/J = k[x_1, \ldots, x_n]$$

Okruh $k[x_1, \ldots, x_n]$ je konečnegenerovaný, je to obor integrity, lebo J je prvoideál a $f(x_1, \ldots, x_n) \neq 0$, lebo $f \notin J$. Podľa dôsledku existuje homomorfizmus

$$\varphi\colon k[x_1, \ldots, x_n] \to \overline{k}$$

[2] Urobte si to ako cvičenie. Návod: každé algebraicky uzavreté pole (teda aj $\overline{k}$) je nekonečné.

taký, že $\varphi(f(x_1, \ldots, x_n)) \neq 0$ (ktorý je rozšírením vnorenia $k \to \overline{k}$). Ale $\varphi(f(x_1, \ldots, x_n)) = f(\varphi(x_1), \ldots, \varphi(x_n))$. Dokážeme, že $c = (\varphi(x_1), \ldots, \varphi(x_n))$ je spoločná nula ideálu J a tým skôr spoločná nula ideálu I.

To je ale spor s tým, že $f(a) = 0$ pre každú spoločnú nulu a ideálu I.

Prečo je $c = (\varphi(x_1), \ldots, \varphi(x_n))$ spoločná nula ideálu J:

Nech $g(X_1, \ldots, X_n) \in J$, potom $g(x_1, \ldots, x_n) = g(X_1 + J, \ldots, X_n + J) = g(X_1, \ldots, X_n) + J = 0$ (0 sa myslí v $k[x_1, \ldots, x_n]$). Potom

$$0 = \varphi(0) = \varphi(g(x_1, \ldots, x_n)) = g(\varphi(x_1), \ldots, \varphi(x_n))$$

čiže $c = (\varphi(x_1), \ldots, \varphi(x_n))$ je koreň každého polynómu z ideálu J. $\square$