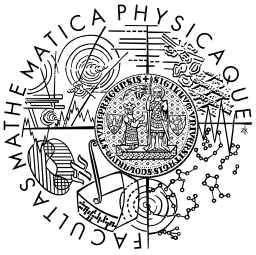

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

František Čech

Rozhodnutelnost teorie komutativních grup

Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Šaroch, Ph.D

Studijní program: Matematika

Studijní obor: obecná matematika

Praha 2016

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Rozhodnutelnost teorie komutativních grup

Autor: František Čech

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Šaroch, Ph.D , katedra

Abstrakt: V práci bude proveden důkaz rozhodnutelnosti teorie abelovských grup. Tento výsledek už byl dokázán v roce 1955 autorkou W. Szmielew. Důkaz zde předvedený se však ubírá jinou cestou. Výsledek bude dokázán za pomoci výsledků z teorie modulů a teorie modelů uvedených v článku M. Zieglera Model theory of modules. Závěrečná část důkazu sleduje závěr důkazu uvedený v článku The elementary theory of Abelian groups P. C. Eklofa a E. R. Fishera.

Klíčová slova: rozhodnutelnost matematická logika

Title: Decidability of theory of commutative groups

Author: František Čech

Department: Department of algebra

Supervisor: Mgr. Jan Šaroch, Ph.D , department

Abstract: In this thesis will be demonstrated proof of decidability of theory of commutative groups. This result was already shown in year 1955 by author W.Szmielew. However proof shown here takes different path. Result will by shown with use of results from theory of modules and theory of modeles prooved in article by M. Ziegler Model theory of modules. Final part of proof follows proof shown in article The elementary theory of Abelian groups by P. C. Eklofa and E. R. Fishera.

Keywords: decidability mathematical logic

Děkuji vedoucímu Janu Šarochovi za vedení práce, nejužší rodině za podporu a Janu Grebíkovi za všechno.

Obsah

Úvod

Téma této práce je na pomezí matematické logiky a algebry. K pochopení hlavního výsledku stačí pouze intuitivní představa o obou oborech. Jak je vidět z původního článku W. Szmielew dokonce ani k jeho důkazu není třeba znalostí jak z logiky tak algebry. Tento přístup, kdy jsou veškeré nástroje zavedeny a posány na začátku článku s sebou ovšem nese dlouhé pasáže technických lemmat. V této práci bude využito postupů z teorie modulů, díky nimž bude závěr obecnější a teorie modelů, díky nimž bude cesta k cíly rychlejší a elegantnější. Všechny potřebné definice a věty budou uvedeny v první kapitole, ale pouze v rozsahu potřebném pro hlavní výsledek. K jejich detailnějšímu pochopení bych odkázal na jiné práce.

1. Průběh důkazu rozhodnutelnosti teorie abelovských grup

Tato kapitola slouží pouze jako nastínění, kudy se bude důkaz ubírat. Měla by pomoci k snadnější orientaci v práci a k pochopení důvodů k zavedení pojmů ještě před jejich zavedením. Všechny konstrukce zde zmíněné budou později důkladně probrány.

Z podkapitoly 2.2 bude zřejmé, že pro nalezení rozhodovacího postupu pro teorii abelovských grup $T_{(AG)}$ stačí najít efektivní postup jak určit, je-li daná formule φ konzistentní s teorií $T_{(AG)}$. Tedy náš problém: "Je φ platná v každém modelu teorie $T_{(AG)}$?"se redukuje na problém: "Existuje model teorie $T_{(AG)}$ takový, že v něm platí φ?"V kapitole 5 ukážeme, že existuje množina $\mathbb{S}$ abelovských grup taková, že každá $T_{(AG)}$-konzistentní formule platí v nějaké grupě z $\mathbb{S}$ a že množina $\mathbb{S}$ je algoritmicky očíslovatelná přirozenými čísly (rekurzivně spočetná). Z existence této množiny už relativně snadno vyvodíme rozhodnutelnost $T_{(AG)}$.

K nalezení množiny S z předchozího odstavce se přesuneme do obecnější teorie modulů, kde dokážeme, že každý modul je elementárně ekvivalentní diretktní sumě $\bigoplus M_i$ nerozložitelných čistě injektivních modulů, kde se kopie každého sčítance vyskytuje nejvýše spočetněkrát. A dále, že nad Dedekindovským okruhem R (tedy i nad $\mathbb{Z}$, jinými slovy v abelovských grupách) jsou nerozložitelné čistě injektivní (až na isomorfismus) jen moduly R/P^n, Q, $Q/R_{(P)}$ a $\overline{R_{(P)}}$, kde P je maximální ideál R, $R_{(P)}$ je lokalizace okruhu v P, Q je podílové těleso R, $\overline{R}$ je uzávěr vzhledem k určité topologii. Tyto výsledky jsou nejnáročnější z celé práce. Abychom se k nim dostali, ukážeme, že každá formule je v teorii modulů elementárně ekvivalentní booleovské kombinaci formulí určitého poměrně jednoduchého tvaru tzv. pp-formulí a důsledků tohoto. Odkud budeme pokračovat zkoumáním čistě injektivních modulů.

S těmito výsledky přejdeme do teorie abelovských grup, kde ukážeme, že výše popsané direktní sumy $\bigoplus M_i$ jsou v teorii abelovských grup axiomatizovatelné pomocí sentencí ze spočetné množiny Szmielew invariantních sentencí, které představíme později. Odsud pomocí (z logiky známé) Compactness theorem vyvodíme, že se dále můžeme omezit pouze na ty direktní sumy $\bigoplus M`_i$, kde se vyskytuje pouze konečně mnoho různých grup a každá z nich pouze v konečně mnoha kopiích. Poté si pomocí jednoduchých pozorování uvědomíme, že množina direktních sum $\bigoplus M`_i$ už je rekurzivně spočetná a budeme moci dokázat rozhodnutelnost $T_{(AG)}$.

2. Logika prvního řádu a teorie modelů

Tato kapitola je spíše přehledová. Bude zde uvedena pouze minimální sada nástrojů potřebných k dosažení našeho cíle (vyjma těch základních). Budeme se spíše snažit o pochopení uvedených pojmů, než o jejich rigorózní výklad, pro ten budou uvedeny odkazy do literatury.

Od čtenáře se očekává znalost základů práce s moduly, grupami, modely a základy logiky prvního řádu. Pro případné doplnění znalostí zde neuvedených bych odkázal na literaturu. Pro matematickou logiku na knihu Základy matematické logiky A. (2001), pro teorii modelů na D. (2002), pro teorii modulů na W. (1992), pro teorii grup na D. (10)

Definice 1. *Teorie T je bezesporná množina sentencí. Množinu všech sentencí dokazatelných z teorie T budeme značit $Thm(T)$, množinu všech sentencí sporných s teorií T budeme značit $Cont(T)$ a množinu všech sentencí konzistentních s teorií T budeme značit $Cons(T)$.*

Nás bude zajímat teorie abelovských grup

$$T_{(AG)} = \{identita, invers, asociativita, komutativita\}$$

kde

$$identita = \forall x \quad 0 + x = x + 0$$

$$invers = \forall x \quad x + (-x) = 0 \wedge (-x) + x = 0$$

$$asociativita = \forall x \forall y \forall z \quad (x + y) + z = x + (y + z)$$

$$komutativita = \forall x \forall y \quad x + y = y + x$$

2.1 Algoritmus a Turingův stroj

Abychom mohli začít mluvit o rozhodnetulnosti budeme chvíli mluvit o algoritmech a turingových strojích. Začneme s intuitivním vymezením algoritmu.

Kvazidefinice 1. *Algoritmus je konečná posloupnost jednoduchých instrukcí, která vede k řešení zadané úlohy.*

Formálně se algoritmus většinou definuje pomocí Turingových strojů (budeme zkracovat na TS). Jde o abstraktní velice jednoduché výpočetní stroje schopné provést libovolný algoritmus (podle Church-Turing teze).

Teze 1 (Church-Turing)**.** *Ke každému algoritmu v intuitivním smyslu existuje Turingův stroj, který jej implementuje.*

Výpočet TS probíhá v krocích. TS se skládá z potenciálně nekonečné pásky (na kterou se zapisují symboly kódující mezivýsledky), sloužící jako operační paměť, hlavy, která se umí po pásce pohybovat, číst a přepisovat symboly z pásky a konečné množiny stavů.

Potenciálně nekonečnou páskou myslíme, že je páska dost velká pro jeho výpočet, ale vždy je na ní zapsáno jen konečně symbolů. Stav je instrukce, říkající co má v daném kroku výpočtu TS uděat (jestli a kam má posunout hlavu po pásce, jestli a jak má přepsat políčko pásky, nad kterým je zrovna hlava a na který stav se má posunout).

Stavy TS jsou napevno definovány před začátkem výpočtu. Před začátkem výpočtu je na pásce zapsán konečný počet symbolů, to je vstup výpočtu. Výpočet TS začíná na začátečním políčku pásky, dále probíhá v krocích a buď skončí nebo také skončit nemusí. Pokud skončí, TS se zastaví na terminálním políčku pásky, kam zapíše výsledek výpočtu, kterému budeme říkat výstup.

Zevrubnější a více matematický popis Turingových strojů lze nalézt

Je-li TS sestrojený k provedení algoritmu musí se jeho výpočet pro každý vstup po nejvíce konečně krocích zastavit.

Definice 2. *Výpočtu TS, který se zastavit nemusí zde budeme říkat pseudoalgoritmus.*

2.2 Rozhodnutelnost

Definice 3. *Teorie T v jazyce L je rekurzivně zadaná, pokud existuje algoritmus který určí, jestli je libovolná sentence v jazyce L v dané teorii, či nikoliv.*

V našem případě teorie abelovských grup je tento algoritmus velice prostý, pouze si pamatuje čtyři sentence na které řekne ano a ostatní odmítne.

Definice 4. *Řekneme, že množina formulí S v jazyce J je rozpoznatelná pokud existuje turingův stroj TS, jehož výpočet se vstupem $f \in S$ se zastaví po konečném počtu kroků s výstupem 1 a jehož výpčet se vstupem $f \notin S$ se buď nezastaví po konečném množství kroků, nebo se zastaví s výstupem 0.*

Poznámka. Známým výsledkem z matematické logiky je, že pro rekurzivně zadanou teorii T je $Thm(T)$ rozpoznatelná množina. To je proto, že rekurzivně zadaná teorie je spočetná a tedy i množina důkazů z ní zkonstruovatelných je spočetná. Máme-li tedy určit je-li formule $f \in Thm(T)$, budeme postupně procházet všechny důkazy a sledovat jestli nedokazují f. Podobně bychom mohli hledat důkaz formule f a ukázat, že množina $Cont(T)$ je také rozpoznatelná. Pokud je T navíc úplná, tento postup nám dá rozhodovací algoritmus.

Definice 5. *Teorie T v jazyce L je rozhodnutelná, pokud existuje turingův stroj TS jehož výpočet se vstupem formule f v jazyce L se vždy zastaví a jeho výstup bude 1 pokud f je dokazatelná z T a 0 pokud f není dokazatelná T.*

Poznámka. Opět uvažujme rekurzivně zadanou teorii T. Jelikož $Thm(T)$ i $Cont(T)$ jsou rozpoznatelné, pro dokázání rozhodnutelnosti T stačí ukázat, že i $Cons(T)$ je rozpoznatelná. Pokud je totiž $Cons(T)$ rozpoznatelná můžeme sestrojit TS který dostane-li sentenci f na vstupu, bude provádět střídavě po jednom kroku z výpočtu turinguvých strojů počítajících zda-li je $f \in Thm(T)$, $f \in Cons(T)$, $f \in Cont(T)$ a $\neg f \in Cons(T)$. Z těchto čtyr výpočtů se vždy aspoň dva zastaví a z jejich výstupu budu zřejmé do jaké z množin $Thm(T)$, $Cont(T)$, $Cons(T)$ f náleží. Rozmyslet si jaké možnosti mohou nastat a jaký výsledek z toho vyplyne už ponechám čtenáři.

2.3 Teorie modelů

Zde pouze uvedeme definice a věty potřebné v práci bez důkazů, podle knihy Model Theory: An Introduction D. (2002)

Po celou tuto sekci buď T úplná teorie ve spočetném jazyce, taková že má nekonečný model.

Definice 6 (Typy)**.** *Buď L jazyk, M L-struktura a $A \subseteq M$. Buď L_A jazyk získaný přidáním symbolu pro konstantu do L pro každé $a \in A$. Buď p množina L_A-formulí se všemi volnými proměnnými z $v_1, \ldots, v_n$. Množinu p nazveme n-typem pokud je $p \cup Th_A(M)$ splnitelná, kde $Th_A(M)$ je množina všech L_A-sentencí pravdivých v M. Řekneme, že p je úplný n-typ pokud $\varphi \in p$ nebo $\varphi \notin p$, pro každou L_A-formuli φ s se všemi volnými proměnnými z $v_1, \ldots, v_n$. Množinu všech úplných n-typů budeme značit $S_n^M(A)$.*

Řekneme, že $\bar{a} \in M^n$ realizuje typ p pokud $M \models \varphi(\bar{a})$ pro každé $\varphi \in p$. V opačném případě řekneme, že M vynechává p.

Definice 7 (Saturovaný model)**.** *Buď κ nekonečný kardinál. Řekneme, že model $M \models T$ je κ-saturovaný, pokud pro každou množinu $A \subseteq M$ takovou, že $|(|\, A) < \kappa$ a $p \in S_n^M(A)$, je p realizovaný v M.*

Definice 8 (Slabě saturovaná sktruktura)**.** *Zachovejme značení z předchozí definice. Řekneme, že M je slabě saturovaný, pokud realizuje každý 1-typ p.*

Pozorovani 2. *Zachovejme značení posledních dvou definic. Potom pokud je M κ-saturovaný je i slabě saturovaný.*

Věta 3 (Existence saturovaných struktur)**.** *Buď κ kardinál $\kappa > \aleph_0$, potom pro každý model M existuje κ^+-saturované elementární rozšíření N takové, že $|(|\, N) \leq |(|\, M)^\kappa$.*

3. pp-formule v modulech

Hlavním výsledkem této kapitoly je tvrzení 9 a jeho důsledky, díky kterým budeme moci v příští kapitole popsat strukturu algebraicky kompaktních modulů. Materiál této kapitoly je čerpán (až na pár prostých důkazů z teorie grup) z knihy Model Theory and Modules M. (1988)

V této kapitole budeme pracovat s otevřenými formulemi a množinami které definují. Abychom se vyhnuli neustálému komentování počtu volných proměnných ve formulích, zavedeme následující značení, které bude jejich počet ignorovat. Můžeme si to dovolit, protože nás ve většině případů nebude zajímat. V ojedinělých případech, kdy tomu tak nebude, délku vektorů proměnných samozřejmě ignorovat nebudeme.

Značení 1. *Zápisem $\bar{x}$ budeme myslet vektor proměnných nebo prvků modulu správné délky, obě tyto informace budou zřejmé z kontextu.*
Je-li M modul, zápisem $\bar{b} \in M$ budeme myslet $\bar{b} \in M^l$, kde l je délka vektoru $\bar{b}$.

Definice 9.

Formule v jazyce modulů $\varphi(\bar{x})$ je pp-formule (primitivně pozitivní) pokud je ekvivalentní formuli tvaru $\exists y_1, \ldots, y_n \bigwedge_{j=1}^{m} (\sum_{i=1}^{n} r_{ij} x_i + \sum_{k=1}^{l} s_{kj} y_k)$.

Poznámka.

Důkaz následujícího lemmatu lze nalézt v M. (1988, Corollary 2.2)

Lemma 4. *Buďte $\varphi(\bar{x})$ a $\psi(\bar{y})$ dvě pp-formule, M modul, potom*

(1) můžeme BÚNO předpokládat, že $l(\bar{x}) = l(\bar{y})$.

(2) $\varphi(\bar{x}) \wedge \psi(\bar{y})$ je pp-formule.

(3) $\varphi(\bar{0})$ je logicky platné tvrzení.

(4) je-li navíc $\bar{a} \in M^{l(\bar{x})}, \bar{b} \in M^{l(\bar{y})}$, potom $M \models (\varphi(\bar{a}) \wedge \psi(\bar{b})) \to \varphi(\bar{a} - \bar{b})$

(5) Pp-definovatelná množina je, spolu se sčítáním definovaným po složkách podle M, abelovská grupa.

(6) dosadíme-li $l(\bar{a}) \in M^{l(\bar{x})-k=m}$ kde $k < l(\bar{x})$ za posledních m proměnných v $(\bar{x})$ potom množina $\varphi(M,\bar{a}) \coloneqq \{\bar{c} \in M^k \colon M \models \varphi(\bar{c},\bar{a})\}$ je prázdná nebo rozkladová třída grupy $\varphi(M,\bar{0})$

(7) částečně uspořádaná množina v M pp-definovatelných podrgup M^l tvoří podsvaz svazu všech podgrup M^l.
S průnikem a součtem definovanými následovně:
$\varphi(M) \cap \psi(M) = \varphi \wedge \psi(M)$
$\varphi(M) + \psi(M) = \varphi + \psi(M)$

3.1 Několik předběžností z teorie grup

V důkazu, že teorie modulů má pp-eliminaci kvantifikátorů nám později poslouží lemmata 5, 7 a 8. Napřed budeme muset zavést několik pojmů. Množinám, kterým se v české literatuře o teorii grup říká rozkladové třídy budeme říkat anglickým názvem coset. Ve zkratce připomeneme jejich základní vlastosti. Dále budeme-li mluvit o pokrytí, budeme myslet pokrytí příslušných množin. Dále zavedeme speciální definici indexu cosetu, podobnou klasické definici indexu podgrupy s několika zřejmými vlastnostmi.

Definice 10 (coset)**.** *Buď G grupa $a \in G$ a H podgrupa G, množinu $a + H = \{a+h\colon h \in H\}$ nazveme cosetem grupy H v grupě G. Kardinalitě množiny cosetů H v G budeme říkat index H v G a budeme ho značit $[G\colon H]$.*

Lemma 5. *Buď G grupa a H podgrupa G. Potom*

(1) $|G| = |H| \cdot [G : H]$

(2) Coset H v G má stejnou mohutnost jako H.

(3) Cosety H v G pokrývají G.

(4) Každé dva cosety H v G jsou buď disjunktní nebo sobě rovny.

(5) Pokud je navíc K podgrupa H platí $[G\colon K] = [G\colon H] \cdot [G\colon K]$.

(6) Pokud je navíc K podgrupa G platí $[G\colon H \cap K] \leq [G\colon H] \cdot [G\colon K]$.

Důkaz. Důkaz provedeme pouze zběžně.

(1) Důkaz k nalezení v D. (10, Věta 7.15)

(2) Zřejmé.

(3) Zřejmé.

(4) Pokud $a_i + (b_j + K)$ jsou po dvou různé je důkaz hotov, předpokládkejme tedy, že $a_p + (b_q + K) = a_r + (b_s + K)$ pro nějaké $p,r \in I$ a $q,s \in J$. Potom $a_p + H \supseteq a_p + (b_q + K)$ a $a_r + H \supseteq a_r + (b_s + K)$ a tedy podle tvrzení (4) $a_p + H = a_r + H$ a protože jsou tyto cosety z minimálního pokrytí, $a_p = a_r$. Obdobně se ukáže, že $b_q = b_s$.

(5) Buďte $C_{H\cap K} \coloneqq \{g_i + (H \cap K)\colon i \in I\}$ množina všech cosetů podgrupy $H \cap K$, C_H množina všech cosetů podgrupy H, C_K množina všech cosetů podgrupy K, $f\colon C_{H\cap K} \to C_H \times C_K$ zobrazení definované $f(g_i + (H \cap K)) \coloneqq (g_i + H, g_i + K)$ pro všechny $i \in I$.
Je třeba ukázat, že f je správně definované a prosté. Obojí plyne ze známé ekvivalence $r_1 + S = r_2 + S \Leftrightarrow r_1 - r_2 \in S$ platící pro libovolné grupy $S \subseteq R$, $r_1,r_2 \in R$. Pro první je třeba ukázat, že z $g_l + (H \cap K) = g_k + (H \cap K)$ plyne $g_l + H = g_k + H$ a $g_l + K = g_k + K$. Předpokládejme tedy, že $g_l + H \neq g_k + H$ potom $g_l - g_k \notin H$ a proto $g_l - g_k \notin H \cap K$, tedy $g_l + (H \cap K) \neq g_k + (H \cap K)$. Obdobně bychom ukázali totéž pro podgupu K.
Prostost f by se ukázala podobně.

□

Pozorovani 6 (Vlastnosti indexu cosetu)**.** *Zachovejme značení z předchozí definice a předpokládejme, že* $[Y\colon X]$ *je správně definováno, potom*

(1) pokud je navíc Y *coset nějaké podgrupy* $Y^0 \subseteq G$*, platí* $[Y\colon X] = [Y^0\colon X^0]$*.*

(2) pokud je navíc Z *coset nějaké podgrupy* $Z^0 \subseteq X^0$*, platí* $[Y\colon Z] = [Y\colon X] \cdot [X\colon Z]$*.*

(3) pokud je navíc W *coset nějaké podgrupy* $W^0 \subseteq G$ *a* $[W\colon X]$ *je správně definováno, potom* $[W \cup Y\colon X] = [W\colon X] + [Y\colon X] - [W \cap Y\colon X]$*, jsou-li obě strany rovnosti konečné.*

Důkaz. Tvrzení

(1) Je-li $Y = a + Y^0$ a $\{a_i + X^0\}$ nějaké pokrytí Y^0, $\{a + a_i + X^0\}$ je pokrytí Y. Druhá nerovnost se dokáže analogicky.

(2) Buď $C = \{a_i + X^0\}$ nějaké minimální pokrytí Y. Na pokrytí každého cosetu z C je třeba $[X\colon Z]$ cosetů Z a odsud podobně jako v CosetLemma04 v lemmatu 5 plyne požadované.

(3) Plyne snadno z lemmatu 5.

□

Lemma 7 (Neumannovo lemma)**.** *Buď* G *grupa* $H, H_i \subseteq G$ *podgrupy,* $a, a_i \in G$ *pro* $i = 1, \ldots, n$*, takové, že* $a + H \subseteq \bigcup_{i=0}^{n} a_i + H_i$*. Potom můžeme z tohoto pokrytí vynechat všechny cosety* $a_k + H_k$ *takové, že* $[H\colon H \cap H_k] > n!$*, aby zůstalo pokrytím.*

Důkaz. Předpokládejme BÚNO, že $H = \bigcup_{i=0}^{n} a_i + H_i$. (K tomuto předpokladu lze od původního přejít přechodem od H_i k podgrupám $H \cap H_i$, odečtením od obou stran vzniklé rovnosti a a změnou značení. Nyní je $H_i \subseteq H$ a tedy pokud pro $h \in H_i$ máme $a_i + h \notin H$, platí $a_i + H_i \cap H = \emptyset$ a $a_i + H_i$ můžeme z pokrytí vynechat).

Napřed dokážeme slabší tvrzení, že můžeme z daného pokrytí vynechat takové H_k, že $[H\colon H \cap H_k]$, je konečné, aby zůstalo pokrytím.

Dále z předpokladu, že pokrytí podgrupy H cosety $a_i + H_i$ je minimální, vyvodíme, že $[H\colon H \cap H_i]$ je konečné pro všechna i. Tedy, že podgrupy $a_i + H_i$, které tuto podmínku nesplňují jsou v pokrytí navíc.

Předpokládejme tedy, že pokrytí grupy H je minimální a mezi grupami H_i je l různých grup. Dále budeme pokračovat indukcí podle l.

Pro $l = 1$ je tvrzení zřejmé z definice indexu a předpokladů.

Buď $l > 1$. Vyberme nějaký index $0 < j < n$. Z minimality pokrytí víme, že $\exists g \in H \setminus \bigcup\{a_i + H_i\colon H_i = H_j\}$. Potom $g + H_j \subseteq H \setminus \bigcup\{a_i + H_i\colon H_i \neq H_j\}$ ** a tedy platí $H_j \subseteq \bigcup\{a_k - g + a_i + H_i\colon H_i \neq H_j\}$. Potom i $a_k + H_k \subseteq \bigcup\{(-g) + a_i + H_i\colon H_i \neq H_j\}$ pro každé k takové, že $H_k = H_j$. Máme tedy, že část grupy H pokrytá množinami $a_k + H_k$, kde $H_k = H_j$ se dá pokrýt množinami $a_i + H_i$ kde $H_i \neq H_j$ a tedy totéž platí pro celou grupu H. Grup H_i že $H_i \neq H_j$ je $l - 1$, můžeme tedy použít indukční předpoklad a dostáváme tvrzení pro všechny

podgrupy $H_i \neq H_j$. Index j jsme ale vybrali náhodně, tedy je první slabší tvrzení dokázané.

Dále ukážeme, že pro nějaké $i \in \{1, \ldots, n\}$ platí $[H\colon H \cap H_i] \leq n$

Buď $K \coloneqq \bigcap_1^n H_i$ a $m \coloneqq [H\colon K]$. Podle předchozího je m konečné. Pro spor předpokládejme, že

$$[H\colon H_i] = [H\colon K]/[H_i\colon K] > n$$

pro každé $i \in \{1, \ldots, n\}$. Potom $[H_i\colon K] < m/n$ a $[a_i + H_i\colon K] < m/n$.

Potom $[\bigcup_1^n a_i + H_i\colon K] \leq \sum_1^n [H_i\colon K] < n(m/n) = [H\colon K]$ a to je ve sporu s $H = \bigcup_1^n a_1 + H_1$ a tvrzení je dokázáno.

Nakonec ukážeme, že $[H : H_i] \leq n!$

Důkaz provedeme indukcí podle l, počtu různých grup mezi grupami H_i, jejichž cosety pokrýváme H v námi uvažovaném pokrytí. Případ $l = 1$ je dokázaný z předchozího. Proveďme tedy indukční krok a předpokládejme, že $l \geq 2$ a že $[H : H_i] \leq n$. Dále si zafixujme nějaké $i \geq 2$ a ukažme, že $[H : H_i] \leq n!$. Pokud $H_i = H_1$ je tvrzení dokázané, předpokládejme tedy opak.

Buď $g \in H \setminus \bigcup\{a_j + H_j\colon j \neq i\}$. Podobně jako na začátku důkazu vyvodíme $g + H_1 \subseteq \bigcup\{a_k + H_k\colon H_k \neq H_1\}$. Z tohoto pokrytí vybereme nějaké minimální pokrytí $C = \{a_k + H_k\colon k \in X, X \subseteq \{1, \ldots, n\}\}$. Máme $a_i + H_i \in C$ protože g je pouze v tomto cosetu a navíc víme, že v C figuruje maximálně $l - 1$ různých podgrup. Odečtením g dostaneme pokrytí $H_1 \subseteq \bigcup\{a_k - g + H_k : k \in X\}$ a protnutím s H_1 dostaneme minimální pokrytí. V tomto pokrytí je maximálně $n-1$ cosetů. Použitím indukčního předpokladu dostáváme, $[H_1\colon H_1 \cap H_k] \leq n!$ pro $k \in X$. Protože $i \in X$ máme $[H\colon H_i] \leq [H\colon H_1 \cap H_i] = [H\colon H_1] \cdot [H_1\colon H_1 \cap H_i] \leq n \cdot (n-1)! = n!$ a tvrzení je dokázané. □

Lemma 8. *Buď G grupa a $G_1, \ldots, G_n$ její podgrupy, H grupa a $H_1, \ldots, H_n$ její podgrupy. Pro $i = 1, \ldots, n$ buďte C_i coset grupy G_i a D_i coset grupy H_i, pokud je G_i, respektive H_i neprázdná. Dále předpokládejme, že*

(1) pro každé dvě podmnožiny $I \subseteq J \subseteq \{1, \ldots, n\}$ jsou si indexy $[\bigcap_{i\in I} G_i\colon \bigcap_{j\in J} G_j]$ a $[\bigcap_{i\in I} H_i\colon \bigcap_{j\in J} H_j]$ rovné, pokud jsou konečné.

(2) pro každou pdomnožinu $I \subseteq \{1, \ldots, n\}$ platí $\bigcap_{i\in I} C_i = \emptyset$ právě tehdy když $\bigcap_{i\in I} D_i = \emptyset$

Potom $[\bigcup_1^n C_i\colon \bigcap_1^n G_i] = [\bigcup_1^n D_i\colon \bigcap_1^n H_i]$ a speciálně $G = \bigcup_1^n C_i$ právě když $H = \bigcup_1^n D_i$

Důkaz. Důkaz provedeme indukcí podle n. Pro $n = 1$ je tvrzení zřejmé z předpokladů.
Pro indukční krok předpokládejme, že tvrzení platí pro každé $n \leq k$ potom

$$[\bigcup_1^{k+1} C_i\colon \bigcap_1^{k+1} G_i] = [\bigcup_1^{k} C_i\colon \bigcap_1^{k+1} G_i] + [C_{k+1}\colon \bigcap_1^{k+1} G_i] - [(\bigcup_1^{k} C_i) \cap C_{k+1}\colon \bigcap_1^{k+1} G_i]$$

podle (3) z pozorování 6

$$= [\bigcup_1^{k+1} C_i\colon \bigcap_1^{k} G_i] \cdot [\bigcap_1^{k} G_i\colon \bigcap_1^{k+1} G_i] + [C_{k+1}\colon \bigcap_1^{k+1} G_i] - [\bigcup_1^{k} (C_i \cap C_{k+1})\colon \bigcap_1^{k} (G_i \cap H_{k+1})]$$

podle (2) z pozorování 6

$$= [\bigcup_1^k D_i \colon \bigcap_1^k H_i] \cdot [\bigcap_1^k H_i \colon \bigcap_1^{k+1} H_i] + [D_{k+1} \colon \bigcap_1^{k+1} H_i] - [\bigcup_1^k (D_i \cap D_{k+1}) \colon \bigcap_1^k (G_i \cap H_{k+1})]$$

podle indukčního předpokladu s použitím předpokladů (1) a (2)
$= \ldots$ obrácením kroků z dosavadního postupu podle potřeby

$$= [\bigcup_1^{k+1} D_i \colon \bigcap_1^{k+1} H_i]$$

□

3.2 pp-eliminace kvantifikátorů v modulech

První poznámka podrobněji popisuje vztah lemmatu 8 k důkazu věty, že teorie modulů má pp-eliminaci kvantifikátorů. Čtenář se k této poznámce může vrátit až během zmíněného důkazu.

Poznámka. Pokud jsou M,N dva moduly, $\bar{b} \in M, \bar{c} in N$, $\varphi(y,\bar{x}), \psi_i(y,\bar{x})$ pp-formule a $\varphi(y,\bar{x})\psi_i(y,\bar{x})$ pro $i = 1,..,n$, G, H grupy definované formulí $\varphi(x)$ v M respektive N a G_i, H_i grupy definované formulí $\psi_i(y,\bar{b})$ v M respektive $\psi_i(y,\bar{c})$ v N pro $i = 1,..,n$. Potom předcházející lemma říká, že jsou-li splněny předpoklady lemmatu, podmnožina v M definovaná $\varphi(y,\bar{b}) \setminus \bigcup_i \psi_i(y,\bar{b})$ je prázdná v M, právě když podmnožina v N definovaná $\varphi(y,\bar{c}) \setminus \bigcup_i \psi_i(y,\bar{c})$ prázdná v N.

Jelikož formule $\exists y \bigwedge_{i\in I} \neg\psi_i(y,\bar{x})$, kde $I \subseteq \{1,\ldots,n\}$ jsou pp-formule, prázdnost množiny $\varphi(y,\bar{b}) \setminus \bigcup_i \psi_i(y,\bar{b})$ v modulu splňujícím určité invariantní tvrzení, závisí pouze na pravdivosti určitých pp-formulí. Určitými invarianty myslím invarianty z (1) v lemmatu 8 s dosazením podle této poznámky a určitými pp-formulemi myslím formule $\exists y \bigwedge_{i\in I} \neg\psi_i(y,\bar{x})$, kde $I \subseteq \{1,\ldots,n\}$.

Nyní zavedeme invarianty a invariantní tvrzení a dokážeme hlavní tvrzení podkapitoly, v kterém ukážeme, že je-li formule $\varphi(y,\bar{x})$ ekvivalentní nějaké booleovské kombinaci pp-formulí, má tuto vlastnost i formule $\exists x\varphi(x,\bar{y})$. Odsud indukcí plyne, že každá formule je ekvivalentní nějaké booleovské kombinaci pp-formulí.

Definice 11 (invarianty a invariantní tvrzení)**.** *Buď M modul a ψ, φ pp-formule*

(1) definujejeme $Inv(M,\varphi,\psi) := |\varphi(M))/(\varphi(M) \cap \psi(M))|$. Těmto kardinálům budeme říkat invarianty (modulu M, formule φ vzhledem k formuli ψ).

(2) Buď α tvrzení následujícího tvaru

$$\alpha = \forall \bar{x_1},..,\bar{x_n} \exists \bar{x} (\varphi(\bar{x}) \wedge \bigwedge_1^n \neg\psi(\bar{x} - \bar{x_i}))$$

Formule α říká, že invariant je větší nebo roven n. Booleovské kombinaci tvrzení tvaru α budeme říkat invariantní tvrzení.

(3) Řekneme-li moduly specifikované invariantním tvrzením ρ, budeme myslet třídu všech modulů v kterých platí invariantní tvrzení ρ.

Poznámka. (1) Protože $\varphi(M)$ i $(\varphi(M) \cap \psi(M))$ jsou komutativní grupy,

$$Inv(M,\varphi,\psi) = [\varphi(M) \colon (\varphi(M) \cap \psi(M))]$$

.

Věta 9 (pp-eliminace kvantifikátorů)**.** *Každá formule v jazyce modulů je ekvivalentní nějaké booleovské kombinaci pp-formulí a invariantních tvrzení modulo teorie modulů.*

Důkaz. Důkaz provedeme indukcí podle složitosti formule. Atomické formule jsou ekvivalentní formulím tvaru $\sum r_i x_i$ a tedy zřejmě pp-formule.

Buď tedy $\varphi(y,\bar{x})$ libovolná booleovská kombinace pp-formulí a invariantních tvrzení. Z platnosti známé ekvivalence z výrokového kalkulu

$$\forall y \varphi(y,\bar{x}) = \neg \exists y \neg \varphi(y,\bar{x})$$

plyne, že pro indukční krok stačí ověřit, že $\exists y \varphi(y,\bar{x})$ splňuje podmínku z tvrzení. Tomuto budeme dále říkat, že se z $\varphi(y,\bar{x})$ dá elimonovat existenční kvantifikátor.

Pro zjednodušení zápisu si označíme existenční kvantifikátor, který se budeme snažit eliminovat $\exists^{el} y$. Značení nemá jiný sepciální význam.

Dále jelikož jsou invariantní tvrzení uzavřené formule, kvantifikátor $\exists^{el} y$ se nevztahuje k proměnným v nich a stačí tedy ukázat, že se dá z formule $\exists^{el} y \varphi(y,\bar{x})$ eliminovat existenční kvantifikátor, pokud neobsahuje žádné invariantní tvrzení.

Dále buď tedy $\varphi(y,\bar{x})$ libovolná formule ekvivalentní booleovské kombinaci pp-formulí. Množina definovaná formulí $\varphi(y,\bar{x})$ se dá vyjádřit jako $\bigcup_j (\varphi_j(y,\bar{x}) \cap \bigcap_i \neg \psi_{ij}(y,\bar{x}))$. Tedy $\exists^{el} y \varphi(y,\bar{x})$ je ekvivalentní formuli

$$\exists^{el} y \bigvee_j (\varphi_j(y,\bar{x}) \wedge \bigwedge_i \neg \psi_{ij}(y,\bar{x}))$$

. Protože prvek náleží do sjednocení množin právě když náleží do nějaké ze sjednocovaných množin, formule $\exists^{el} y \varphi(y,\bar{x})$ je ekvivalentní formuli

$$\bigvee_j \exists (\varphi_j(y,\bar{x}) \wedge \bigwedge_i \psi_{ij}(y,\bar{x}))$$

. Pro indukční krok důkazu tedy stačí ukázat, že se dá eliminovat existenční kvantifikátor z formulí tvaru $\exists y(\varphi(y,\bar{x}) \wedge \bigwedge_i \neg \psi_i(y,\bar{x}))$. Buď $\rho(\bar{x})$ nějaká formule tohoto tvaru.

Abychom mohli pracovat s formulemi pomocí množin, které definují, a použít Neumannova lemma, musíme pracovat v nějakých konkrétních modulech. Když si zafixujeme nějaký modul M a v něm nějaký vektor prvků $\bar{b}$ správné délky, sentence $\neg \rho(\bar{b})$ říká, že množina $\varphi(y,\bar{b}) \setminus \bigcup_i \psi_i(y,\bar{b})$ je prázdná. Vyřešení problému eliminace kvantifikátoru pro $\rho(\bar{x})$ je zřejmě ekvivalentní vyřešení problému pro $\neg \rho(\bar{x})$ a o to se budeme dále snažit.

Podle Neumannova lemmatu 7 můžeme ze sjednocení $\bigcup_i \psi_i(y,\bar{b})$ vynechat grupy $\psi_i(y,\bar{b})$, takové, že $Inv(M,\varphi(y,\bar{0}),\psi_i(y,\bar{0})) > n!$, bez změny pravdivosti tvrzení "$\varphi(y,\bar{b}) \setminus \bigcup_i \psi_i(y,\bar{b})$ je prázdná".

Nyní už můžeme s pomocí Neumannova lemmatu 7 a poznámky 3.2 říct, jak bude vypadat námi hledaná formule $\alpha(\bar{x})$ ekvivalentní formuli $\neg\rho(\bar{x})$. Formule $\alpha(\bar{x})$ bude tvaru $\bigvee_{i\in I}\alpha_i(\bar{x})$, kde $\alpha_i(\bar{x})$ je tvaru $\bigvee_{i\in I}(\beta_i \wedge \bigvee_{j\in J_i}\gamma_{ij}(\bar{x}))$, kde β_i invariantní tvrzení a γ_{ij} je konjunkce pp-formulí.

Napřed popíšeme invariantní tvrzení v $\{\beta_i\colon i \in I\}$. Každé z těchto tvrzení specifikuje třídu modulů, v kterých lze o splňování $\neg\rho(\bar{x})$ vůbec uvažovat, přesněji podle Neumannova lemmatu 7 ty moduly, kde pro aspoň jedno $j \in \{1,\dots,n\}$ máme $Inv(-,\varphi(y,\bar{0}),\psi_j(y,\bar{0})) \leq n!$. Přesněji každá β_i bude konjunkce dvou invariantních tvrzení β_i^1 a β_i^2, kde β_i^1 bude konjunkce n invariantních tvrzení, kde j-té tvrzení bude buď $Inv(-,\varphi(y,\bar{0}),\psi_j(y,\bar{0})) = k$, kde $k \leq n!$, nebo $Inv(-,\varphi(y,\bar{0}),\psi_j(y,\bar{0})) \geq n!$ a β_i^2 bude konjunkce invariantních tvrzení $Inv(-,\theta(y,\bar{0}),\chi(y,\bar{0})) = l$, kde θ je buď φ nebo konjunkce nějakých ψ_j, takových, že v β_i^1 je $Inv(-,\varphi(y,\bar{0}),\psi_j(y,\bar{0})) = k_1$, kde $k_1 \leq n!$ a χ bude konjunkce nějakých ψ_j, takových, že v β_i^1 je $Inv(-,\varphi(y,\bar{0}),\psi_j(y,\bar{0})) = k_2$, kde $k_2 \leq n!$. Nyní protože v β_i^2 se vyskytují pouze ψ_j taková, že $Inv(-,\varphi(y,\bar{0}),\psi_j(y,\bar{0})) \leq n!$, existuje podle lemmatu 5 a poznamky 3.2) horní závoru i pro l aby β_i^1 nebyla ve sporu s β_i^2.

Invariantní tvrzení β tvaru popsaného v předchozím odstavci bude v $\{\beta_i\colon i \in I\}$, právě když v třídě modulů specifikovanou invariantním tvrzením β, existuje nějaký modul M, v němž platí $\neg\rho(\bar{b})$, kde $\bar{b} \in M$. Jiná tvrzení v $\{\beta_i\colon i \in I\}$ nejsou.

Shrneme-li tedy konstrukci množiny $\{\beta_i\colon i \in I\}$, zjistíme že každé tvrzení v ní je konjunkce invariantních tvrzení tvaru $Inv(-,\mu,\nu) = r$ kde μ i ν jsou z nějaké konečné množiny pp-formulí a pro s je kladné číslo, takové, že $r \leq s$ pro nějaké kladné r. Tedy víme, že $\{\beta_i\colon i \in I\}$ má konečně prvků.

Nyní popíšeme formule γ_{ij}. Buď $\beta_i \in \{\beta_m\colon m \in I\}$, $\mathbb{M}$ třída modulů specifikovaná invariantním tvrzením β_i a buď $K \subseteq \{1,\dots,n\}$ taková, že

$$Inv(M,\varphi(y,\bar{0}),\psi_k(y,\bar{0})) \leq n!$$

pro každý $M \in \mathbb{M}$. Dále buď $\Gamma \coloneqq \{\bigwedge(\pm\exists y \bigwedge_{l\in L}\psi_l(y,\bar{0}))\colon L \subseteq K\}$ (zde $\pm$ znamená, že je daná formule buď negovaná (pro minus), nebo není (pro plus)). Γ má zřejě konečně prvků. Nyní formule $\gamma_{ij}(\bar{x})$ jsou ty formule $\gamma(\bar{x}) \in \Gamma$ takové, že existuje modul $M \in \mathbb{M}$, že existuje $\bar{b} \in M$, že $\gamma_{ij}(\bar{x})$ platí.

Tím je popis formule $\alpha(\bar{x})$ u konce.Z Neumannova lemmatu 7 a poznámky 3.2 máme, že v každém modulu M platí $\forall\bar{x}(\exists y(\varphi(y,\bar{x}) \wedge \bigwedge_i \neg\psi_i(y,\bar{x})) \leftrightarrow \alpha(\bar{x}))$, čímž jsou indukční krok a tedy i celé tvrzení dokázány.

□

3.3 Přímé důsledky pp-eliminace kvantifikátorů

Dusledek 10. *Každá sentence v jazyce R-modulů je modulo teorie R-modulů ekvivalentní invariantnímu tvrzení.*

Dusledek 11. *Každá formule v jazyce R-modulů je modulo nějaké úplné teorie R-modulů ekvivalentní nějaké booleovské kombinaci pp-formulí.*

4. Moduly

V této kapitole budeme zkoumat strukturu algebraicky kompaktních modulů. Hlavní výsledek bude, že každý modul je elementárně ekvivalentní direktní sumě nerozložitelných algebraicky kompaktních modulů. Potom ukážeme jak vypadá každý algebraicky kompaktní modul nad Dedekindovým oborem a speciálně každá algebraicky kompaktní abelovská grupa. A odsud dostaneme s použitím předchozí kapitoly strukturu každé abelovské grupy až na elementární ekvivalenci.

většina materiálu této kapitoly je čerpána z Zieglerova článku

Značení 2. *V celé kapitole budeme předpokládat, že R je okruh a M je levý $R-Modul$.*

4.1 Hull

Definice 12. *Buďte M,N moduly, řekneme, že M je čistý podmodul N a že N je čistý nadmodul M, (budeme značit $M \subseteq_p N$) pokud $M \subseteq N$ a pokud*

$$N \models \varphi(a) \Leftrightarrow M \models \varphi(a)$$

pro φ pp-formuli a $a \in M$.

Pozorovani 12. *Implikace z leva do prava v předchozí definici platí pro každý (ne nutně čistý) podmodul $N \subseteq M$.*

Lemma 13. *Buď M modul, potom*

1. *diretní sčítanec N modulu je jeho čistý podmodul.*
2. *jsou-li B,C čisté podmoduly M, potom je i $B \oplus C$ čistý podmodul M*

Důkaz. 1. Pp-formule $\varphi(\bar{x})$ s dosazením $\bar{a}$ říká, že v modulu existuje řešení $\bar{b}$ rovnic daných formulí $\varphi(\bar{a})$. Obraz při přirozené projekci do direktního sčítance $\pi(\bar{b})$ je rovněž řešením těchto rovnic.

2. Zřejmé z definice pp-formule.

□

Definice 13. *Buďte N, N' moduly , takové, že $N' \subseteq_p N$. Potom řekneme, že modul M je algebraicky kompaktní (dále budeme říkat jen kompaktní, nebo kompakt), pokud se každý homomorfismus z N' do M dá rozšířit na homomorfismus z N do M.*

Značení 3. *V této práci budeme používat pojmenování užité v Zieglerově článku. Termín "algebraicky kompaktní"(zkracovaný na "kompaktní") odkazuje na vlastnost* (3) *z věty* 14 *těchto modulů podobnou vlastnosti, která se obvykl uvádí jako definice algebraicky kompaktních modulů: "Každá konečně řešitelná soustava lineárních rovnic nad modulem je řešitelná". Konečně řešitelná znamená, že každá konečná podmnožina soustavy má řešení a řešitelná znamená, že má celá soustava řešení.*

Běžneji se v literatuře používá pojmenování "pure-injective", které odkazuje na vlastnost (1) *z věty* 14, *která je podobná jedné z možných definic injektivních modulů ("Modul je injektivní, pokud je direktním sčítancem v každém nadmodulu").*

Věta 14. *Pro každý modul jsou následující podmínky ekvivalentní:*

(1) M je direktní sčítanec v každém čistém nadmodulu.

(2) Každý bezesporný pp-typ $p(x)$ nad $A \subseteq M$, že $|A| \leq |R| + \aleph_0$ je realizovaný v M.

(3) Každý bezesporný pp-typ $p(x)$ nad M je realizovaný v M.

(4) M je kompakt.

Důkaz je k nalezení v M. (1984, Theorem 3.1.)

Dusledek 15. *(1) $(|R| + \aleph_0)^+$ saturované moduly jsou kompaktní*

(2) každý modul je elementárně ekvivalentní nějakému kompaktnímu modulu

Důkaz. (1) Podle (3) z věty 14.

(2) Přímý důsledek věty 3 a (1) z této věty.

□

Lemma 16. *Direktní sčítance kompakního modulu jsou kompaktní.*

Důkaz. Důkaz analogický důkazu implikace (1) $\implies$ (3) věty 14. □

Definice 14. *Buď A podmnožina kompaktu M. V inkluzi minimální čistý kompaktní podmodul $H_M(A)$ modulu M, který je nadmnožinou A, nazveme hullem množiny A v M. Pokud z kontextu bude jasné, v kterém kompaktním nadmodulu je hull obsažen budeme psát pouze $H(A)$.*

Věta 17. *Zachovejme značení z předchozí definice. Potom hull $H(A)$ existuje a je určen jednoznačně.*

M. (1984, Theorem 3.6.)

Definice 15. *Buď M modul, řekneme, že $\bar{M}$ je čistý hull M pokud*

(1) $\bar{M}$ je čistý kompaktní nadmodul modulu M.

(2) pokud je N čistý kompaktní nadmodul modulu M, $\bar{M}$ je nad M isomorfní čistému podmodulu N.

Věta 18. *Ke každému modulu M existuje až na isomorfismus jedinečný čistý hull.*

4.2 Nerozložitelné kompakty

V následující definici je netradičně navíc požadavek na algebraickou kompaknost modulu. Je to proto, že nás budou zajímat pouze rozklady na algebraicky kompaktní moduly.

Definice 16. *Neprázdný kompaktní modul M, nazveme nerozložitelným, pokud není direktní sumou dvou neprázdných modulů.*

Lemma 19. *Nechť je U neprázdný kompakt, potom je U nerozložitelný, právě tehdy když platí $U = H(a)$ pro všechny $a \in U \setminus 0$.*

Důkaz. Pokud je $U = M \oplus N$ nějaký netriviální rozklad U a $a \in M \setminus 0$, potom $U \neq H(a)$ jelikož z lemmatu 13 je M čistý podmodul U a z lemmatu 16 je M kompaktní a přitom $M \subsetneq U$.

Pokud $a \in U \setminus 0$, $H(a)$ je podle (1) z věty 14 netriviální direktní sčítanec v U, protože z definice je $H(a)$ kompaktní čistý podmodul U. □

Z tohoto lemmatu plyne následující lemma. Důkaz lze nalézt v M. (1984, Corollary 4.2.)

Lemma 20.

(1) Existuje nejvýše $2^{|R|+\aleph_0}$ neisomorfních nerozložielných R-modulů

(2) Nerozložitelný modul má mohutnost nejvýše $2^{|R|+\aleph_0}$.

Poznámka. Díky lemmatu 20 můžeme z každé třídy ekvivalence isomorfismu nerozložitelných modulů vybrat jednoho zástupce U a uvažovat množinu všech U. Kdybychom neměli horní dohad (1), museli bychom uvažovat jestli vůbec mohou tvořit množinu a zaobírat se teorií množin. Máme to dobrý.

Následující charakterizace nerozložitelných modulů bude později užitečná. Důkaz lze nalézt v M. (1984, Theorem 4.3.)

Věta 21. *Neprázdný kompaktní modul U je nerozložitelný, právě tehdy když je jeho okruh endomorfismů lokální, tedy pokud pro každý endomorfismus $f \in End(U)$ platí $id_U - f$ nebo f je automorfismus.*

4.3 Krull-Remak-Schmidt theorem

V této podkapitole nejsou uvedeny důkazy. Jsou náročné.

Věta 22 (Krull-Remak-Schmidt)**.** *Buď M kompaktní modul, potom existuje rozklad $M = \overline{\bigoplus_{i\in I} U_i} \oplus E$, kde I je nějaká indexová množina, U_i jsou nerozložitelné moduly a E je modul, který nemá žádný nerozložitelný direktní sčítanec.*

Důkaz je k nalezení v M. (1984, Theorem 6.1.)

Věta 23. *Buď M slabě saturovaný a kompaktní modul. Pokud $M = \bigoplus_i \bar{\in} IU_i \oplus E$ je rozklad jako ve větě 4.3 potom $M \equiv \bigoplus_i \bar{\in} IU_i$*

Důkaz je k nalezení v M. (1984, Theorem 6.8.)

5. Rozhodnutelnost teorie komutativních grup

V této kapitole dokážeme použijeme výsledky předchozích kapitol a ukážeme, že teorie komutativních grup je rozhodnutelná. Většina materiálu této kapitoly je čerpána z článku Eklofa a Fishera Eklof a R. (1972)

Budeme chtít použít větu 23 a jak se za chvíli ukáže, nerozložitelné moduly nad $\mathbb{Z}$ jsou právě grupy uvedené v následující definici.

Definice 17. *Buď p prvočíslo*

(1) $\mathbb{Z}(p^\infty)$ značí prüferovu grupu

(2) $\mathbb{Z}_{(p)}$ aditivní grupu všech racionálních čísel $\frac{m}{n}$ takových, že $NSD(p,n) = 1$

(3) $\mathbb{Z}(p^n)$ aditivní grupu všech racionálních čísel $\frac{m}{p^k}$ takových, že $0 \leq \frac{m}{p^k} \leq 1$, se sčítáním modulo 1.

(4) $\mathbb{Q}$ značí aditivní grupu racionálních čísel

Definice 18. *Buď M modul, Szmielew invarianty budeme zvát invarianty*

$$Inv_1[p,n](M) \coloneqq Inv(M, p^n|x \wedge p^{n+1}x = 0, x = 0)$$

$$Inv_2[p,n](M) \coloneqq Inv(M, p^n|x, p^{n+1}|x)$$

$$Inv_3[p,n](M) \coloneqq Inv(M, p^{n-1}|x \wedge p^n x = 0, p^n|x \cap p^{n+1}x = 0)$$

kde p je prvočíslo a $n \in \mathbb{N}$.

Invariantním tvrzením říkajícím jakou hodnotu mají Szmielew invarianty budeme říkat Szmielew invariantní tvrzení.

Důkaz následující věty je technický a proto ho vynecháme.

Věta 24. *Buďte p, q prvočísla $m, n \in \mathbb{N}$ potom*

1. $Inv_1[p,n](\mathbb{Z}(q^\infty)) = \begin{cases} 1 & \text{pokud } p = q \\ 0 & \text{jinak.} \end{cases}$

2. $Inv_2[p,n](\mathbb{Z}_{(q)}) = \begin{cases} 1 & \text{pokud } p = q \\ 0 & \text{jinak.} \end{cases}$

3. $Inv_3[p,n](\mathbb{Z}(q^m)) = \begin{cases} 1 & \text{pokud } p = q \wedge m = n \\ 0 & \text{jinak.} \end{cases}$

4. pro $i = 1,2$ $Inv_i[p,n](\mathbb{Z}(q^m)) = \begin{cases} 1 & \text{pokud } p = q \wedge m \leq n \\ 0 & \text{jinak.} \end{cases}$

5. pro $i = 2,3$ $Inv_i[p,n](\mathbb{Z}(q^\infty)) = 0$

6. pro $i = 1,3$ $Inv_i[p,n](\mathbb{Z}_{(q)}) = 0$

7. *pro* $i = 1,2,3$ $Inv_i[p,n](\mathbb{Q}) = 0$

Dusledek 25. *Szmielew grupy S, T mají stejné hodnoty všech Szmielew invariantů, právě když jsou isomorfní.*

Důkaz následující věty je pracný a lze ho nalézt z větší části v knize Model Theory and Modules M. (1988, Corrollary 2Z.11), kde začíná a s odkazy do Zieglerova článku) (1984)

Věta 26. *Nad $\mathbb{Z}$ jsou nerozložitelné pouze moduly $\mathbb{Z}(p^\infty)$, $\mathbb{Z}_{(p)}^-$, $\mathbb{Z}(p^n)$ a $\mathbb{Q}$, kde p je prvočíslo a $n \in \mathbb{N}$.*

Definice 19. *Szmielew grupou S budeme značit každou grupu tvaru*

$$S = \bigoplus_{p,n} \mathbb{Z}(p^n)^{(\alpha_{p,n})} \oplus \bigoplus_{p} \mathbb{Z}_{(p)}^{(\beta_p)} \oplus \bigoplus_{p} \mathbb{Z}(p^\infty)^{(\gamma_p)} \oplus \mathbb{Q}^{(\delta)}$$

kde exponenty $\alpha_{p,n}$, β_p a γ_p jsou nejvýše spočetné a δ je 0 nebo 1.

Řekneme, že Szmielew grupa je konečné hodnosti pokud jen konečně exponentů $\alpha_{p,n}$, β_p a γ_p je nenulových a všechny jsou konečné.

Věta 27. *Každá abelovská grupa G je elementárně ekvivalentní nějaké Szmielew grupě S.*

Důkaz. Podle důsledku 15 je každý modul elementárně ekvivalentní nějakému kompaktnímu modulu. Kompaktní modul M je podle 23 elementárně ekvivalentní direktní sumě nerozložitelných modulů, kde se navíc podle M. (1988, Corrollary 2.24) každý direktní sčítanec vyskytuje nejvýše spočetněkrát. Protože je navíc každý elementárně ekvivalentní svému čistému hullu máme pro abelovské grupy s použitím 26 požadované. □

Dusledek 28. *Abelovské grupy G, H si jsou elementárně ekvivalentní, právě když mají stejné Szmielew invarianty.*

Důkaz. Jedna implikace je zřejmá. Druhá implikace plyne z 25 a 27. □

Dusledek 29. *Každá sentence $f \in Cons(T_{(AG)})$ je splněna v nějaké Szmielew grupě.*

Důkaz. Známý výsledek z matematické logiky je, že každá konzistentní teorie má model. Buď tedy G model $T_{(AG)} \cup f$. Grupa G je podle věty 27 elementárně ekvivalentní nějaké Szmielew grupě S. □

Dusledek 30. *Každá sentence $f \in Cons(T_{(AG)})$ je důsledkem $T_{(AG)} \cup S$ kde S je konečná množina Szmielew invariantních tvrzení.*

Důkaz. Tvrzení je zřejmý důsledek 28 a známé věty o kompaktnosti z matematické logiky. □

Dusledek 31. *Každá sentence $f \in Cons(T_{(AG)})$ platí v nějaké Szmielew grupě konečného ranku.*

Důkaz. Tvrzení je důsledkem 30. □

Věta 32. *Množina* $\mathbb{S}$ *všech Szmielew grup konečného ranku je rekurzivně spočetná.*

Důkaz. Každá grupa v $\mathbb{S}$ je určena vektorem přirozených konečnou množinou přirozených čísel určujících hodnotu jejích Szmielew invariantů. Buďte pro $i \in \mathbb{N}$ všechny možné různé $S_i := \{\delta p, \bar{\alpha_p}, \beta_p, \gamma_p \colon p \in F\}$ kde δ je buď 0 nebo 1, F je konečná množina prvočísel a $\bar{\alpha_p}$ je k-tice čísel pro nějaké k. Množina všech prvočísel je rekurzivně spočetná, její konečné podmnožiny také, konečné podmnožiny přirozených čísel také a tedy množiny S_i také a $\mathbb{S}$ také. □

Nyní závěrečné tvrzení práce

Věta 33. $T_{(AG)}$ *je rozhodnutelná teorie.*

Důkaz. Podle podznámky 2.2 stačí ukázat, že $Cons(T_{(AG)})$ je rozpoznatelná. Buď tedy f sentence v jazyku abelovských grup a $\mathbb{S}$ množina $\mathbb{S}$ všech Szmielew grup konečného ranku. Budeme-li postupně procházet $\mathbb{S}$ podle nějakého očíslování přirozenými čísly (které existuje podle předchozí věty), můžeme v každé z nich v konečném počtu kroků (podle poznámky 2.2) zjistit jestli zde f je splněna. Pokud je $f \in Cons(T_{(AG)})$, podle 31 tímto posupem, dříve nebo později, najdeme grupu v níž je f splněna. Pokud $f \notin Cons(T_{(AG)})$ naše hledání nebude mít konce. □

Seznam použité literatury

A., S. (2001). *Klasická matematická logika*. Vydání první. Nakladatelství Karolinum, Praha. ISBN 80-246-0218-0.

D., M. (2002). *Model Theory : An Introduction*. Springer-Verlag, New York. ISBN 0387987606.

D., S. (10). Matfyzpress, Praha. ISBN 978-80-7378-105-7.

Eklof, P. C. a R., F. E. (1972). The elementary theory of abelian groups. **4** (2), 115–171.

M., P. (1988). *Model Theory and Modules*. II. Series. Cambridge University Press, Cambridge. ISBN 0-521-34833-1.

M., Z. (1984)). Model theory of modules. *Annals of Pure and Applied Logic*, **26**, 149–213.

W., A. F. (1992). *Rings and Categories of Modules*. Springer-VerlagM, New York. ISBN 978-0-387-97845-1.