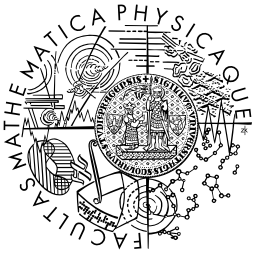

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

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. 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 popsány na začátku článku s sebou ovšem nese dlouhé pasáže technických lemmat. V této práci bude využito postupů z teorie modulů, díky nimž bude cesta k cíly rychlejší a elegantnější.

Dále nastíním průběh důkazu.

Z podkapitoly 1.2 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 4 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 $\mathbb{S}$ z předchozího odstavce se přesuneme do 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) Věty o kompaktnosti 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 $T_{(AG)}$.

1. 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 Sochor (2001), pro teorii modelů na Marker (2002), pro teorii modulů na Anderson (1992), pro teorii grup na Stanovský (2010)

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

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

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

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

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

1.1 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 z předem zvolené konečné množiny, tzv. abecedy, 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 výpočet TS, 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 v terminálním stavu, symboly zapsané na pásce, když je TS v terminálním stavu jsou výstup.

Zevrubnější a více matematický popis Turingových strojů lze nalézt v dodatku ke čtvrté kapitole v knize Sochor (2001)

Pozorování 2. *Výpočet každého Turingova stroje T_1 pracujícího nad abecedou menší než 2^k, kde k je přirozené číslo, se dá provést na nějakém Turingově stroji T_2 pracujícím nad abecedou* 0,1.

To je proto, že každý symbol z abecedy stroje T_1 se dá zapsat v maximálně k-dlouhém binomickém zápisu. Aby stroj T_2 přečetl z pásky stejnou informaci jako stroj T_1 přečte místo jednoho 2^k symbolů a to jakému symbolu z abecedy stroje T_1 je právě čtená 2^k-tice symbolů ekvivalentní si bude ukládat ve stavech.

1.1.1 Kódování formulí nad konečným jazykem do přirozených čísel

Abychom mohli uvažovat stroj pracující s formulemi nad jazykem teorie komutativních grup, musíme umět dát stroji takovou formuli na vstup. Jelikož počet proměnných v takové formuli není shora omezen, konečná abeceda TS by nám pro prostý zápis nestačila. Dále tedy ukážeme, že se formule nad zvoleným konečným jazykem dají kódovat do přirozených čísel. Tedy, že se každé formuli f v daném konečném jazyce L dá algoritmicky přiřadit přirozené číslo n a zpětně dostaneme-li přirozené číslo m, kódující nějakou formuli g v jazyce L, jde algoritmicky zjistit její tvar.

Abychom toto ukázali, bude se nám hodit následující pozorování

Pozorování 3. *Funkce* $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *definovaná*

$$g(m,n) := \begin{cases} 0 & \text{pokud } m = n = 0 \\ 2^{m-1}(2n-1) & \text{jinak.} \end{cases}$$

je bijekce. To je proto, že každé kladné přirozené číslo se dá jednoznačně zapsat jako součin mocniny dvojky a lichého čísla.

Nyní popíšeme kódování:

Mějme konečný jazyk L a formuli f v zápisu $:= s_1 \dots s_l$ kde $s_i \in L$ $i \in \{1, \dots, l\}$.

Očíslujme všechny symboly až na proměnné jazyka L čísly $1, \dots, k$, kde $k \in \mathbb{N}$ a všechny proměnné vyskytující se ve formuli f $k+1, \dots, k+m$ Definujeme funkci $L\colon L \to \mathbb{N}$

$$h(s) := \begin{cases} k & \text{pokud s je k-tý symbol, který není proměnná} \\ 2i & \text{pokud s je i-tá proměnná.} \end{cases}$$

Přiřadíme formuli f číslo n pomocí funkce g definované v předchozím pozorování 3. Definujeme $n_1 \coloneqq g(h(s_1),h(s_2))$ a $n_i \coloneqq g(n_{i-1},h(s_i))$ a $n \coloneqq n_l$.

Přirozené číslo $K \coloneqq g(n,l)$ je výsledný kód formule f.

Máme-li naopak číslo $K \in \mathbb{N}$ kódující nějakou formuli f v jazyce L, pomocí k g inverzní funkce g^{-1} zjistíme délku l zakódované formule: $g^{-1}(K) = (n,l)$. A dále použitím g^{-1} l-krát nejspíš již zřejmým způsobem postupně všechny symboly formule f.

1.2 Rozhodnutelnost

Definice 2. *Teorie T v jazyce L je rozhodnutelná, pokud existuje algoritmus který určí, jestli je libovolná sentence v jazyce L v dané teorii, či nikoliv. Jinými slovy, 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.*

Definice 3. *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 výpočet se vstupem $f \notin S$ se buď nezastaví po konečném množství kroků, nebo se zastaví s výstupem* 0.

Pozorování 4. *Pro rozhodnutelnou teorii T je $Thm(T)$ rozpoznatelná množina.*

Důkaz. Rozhodnutelná 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 $\neg f$ a ukázat, že množina $Cont(T)$ je také rozpoznatelná. Pokud je T navíc úplná, tento postup nám dá rozhodovací algoritmus. □

Pozorování 5. *Rozpoznatelná teorie je rozhodnutelná pokud T je $Cons(T)$ je rozpoznatelná množina.*

Důkaz. Pokud je $Cons(T)$ 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 je jednoduché. □

1.3 Teorie modelů

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

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

Definice 4 (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 $Th_A(M)$ množina všech L_A-sentencí pravdivých v M. 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. Řekneme, že p je úplný n-typ pokud $\varphi \in p$ nebo $\neg\varphi \in p$, 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 n-typ p pokud $M \models \varphi(\bar{a})$ pro každé $\varphi \in p$. Pokud neexistuje $\bar{a} \in M^n$ realizující p, řekneme, že M vynechává p.

Definice 5 (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 6 (Slabě saturovaná sktruktura)**.** *Řekneme, že M je slabě saturovaný, pokud realizuje každý 1-typ p.*

Pozorování 6. *Pokud je M κ-saturovaný je i slabě saturovaný.*

Věta 7 (Existence saturovaných struktur)**.** *Buď κ kardinál $\kappa > \aleph_0$, potom pro každý model M existuje κ^+-saturované elementární rozšíření N takové, že $|N| \leq |M|^\kappa$.*

2. pp-formule v modulech

Hlavním výsledkem této kapitoly je tvrzení 13 a jeho důsledky, díky kterým budeme moci v příští kapitole popsat strukturu algebraicky kompaktních modulů. Materiál této kapitoly je čerpán z knihy Model Theory and Modules Prest (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. Zápis budeme používat pouze v místech, kde bude správná délka zřejmá.*
Je-li M modul, zápisem $\bar{b} \in M$ budeme myslet $\bar{b} \in M^l$, kde l je délka vektoru $\bar{b}$.

Definice 7.

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

Definice 8. *Bud M modul. Řekneme, že podgrupa $A \subseteq M^n$ je pp-definovatelná, pokud existují pp-formule $\varphi(\bar{x},\bar{y})$ v jazyce modulů a $\bar{a} \in M^{l(\bar{y})}$ takové, že $A = \varphi(M,\bar{a}) = \{\bar{b} : M \models \varphi(\bar{b},\bar{a})\}$.*

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

Lemma 8. *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) $M \models \varphi(\bar{0})$,

(4) pp-definovatelná množina je, spolu se sčítáním definovaným po složkách podle M, abelovská grupa,

(5) $\varphi(M,\bar{a})$ je prázdná nebo coset grupy $\varphi(M,\bar{0})$ pro každé vhodné $\bar{a} \in M$,

(6) částečně uspořádaná množina v M pp-definovatelných podrgup M^l tvoří podsvaz svazu všech podgrup M^l.
S průnikem a součtem definovanými následovně:

$$\varphi(M) \cap \psi(M) = (\varphi \wedge \psi)(M)$$

$$\varphi(M) + \psi(M) = (\varphi + \psi)(M),$$

kde $(\varphi + \psi)(\bar{x}) := \exists \bar{z} \exists \bar{w} (\bar{z} + \bar{w} = \bar{x}) \wedge \varphi(\bar{w}) \wedge \psi(\bar{z})$.

2.1 Několik předběžností z teorie grup

V důkazu, že teorie modulů má pp-eliminaci kvantifikátorů nám později poslouží lemmata 9, 11 a 12. 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 vlastnosti. Dále budeme-li mluvit o pokrytí grupy, budeme myslet pokrytí nosné množiny dané grupy. Dále zavedeme speciální definici indexu cosetu, podobnou klasické definici indexu podgrupy s několika zřejmými vlastnostmi.

Definice 9 (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 9. *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 $[G\colon K] = [G\colon H] \cdot [H\colon K]$.

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

Definice 10 (Index cosetu). *Buďte $X^0 \subseteq Y_i^0 \subseteq G$, komutativní grupy pro $i \in I$ kde I je nějaká množina indexů. Dále buď $Y = \bigcup_{i\in I} Y_i$, kde $Y_i = a_i + Y_i^0$ pro nějaké $a_i \in G$ a X nějaký coset X^0. Potom definujeme $[Y : X]$ jako nejmenší počet cosetů X potřebný k pokrytí Y.*

Pozorování 10 (Vlastnosti indexu cosetu). *Zachovejme značení z předchozí definice a předpokládejme, že $[Y : X]$ 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.

Lemma 11 (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 $H = \bigcup_{i=0}^{n} a_i + H_i$ a tedy $H_k = H \cap H_K$. (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).

Dále z předpokladu, že pokrytí podgrupy H cosety $a_i + H_i$ je minimální, vyvodíme, že $[H\colon H_i]$ 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 $0 \leq j < n$. Z minimality pokrytí víme, že

$$\exists g \in H \setminus \bigcup \{a_i + H_i\colon H_i = H_j\}$$

. Potom

$$g + H_j \subseteq \bigcup \{a_i + H_i\colon H_i \neq H_j\}$$

a tedy platí

$$H_j \subseteq \bigcup \{a_i - g + H_i\colon H_i \neq H_j\}$$

. Potom i

$$a_k + H_k \subseteq \bigcup \{a_k - g + a_i + H_i\colon H_i \neq H_j\}$$

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. □

Důkaz následujícího lemmatu je k nalezení v Prest (1988, Lemma 2.14)

Lemma 12. *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 podmnožinu $I \subseteq \{1, \ldots, n\}$ platí

$$\bigcap_{i \in I} C_i = \emptyset$$

pravě 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 $H = \bigcup_1^n D_i$

2.2 pp-eliminace kvantifikátorů v modulech

Nyní zavedeme invarianty a invariantní tvrzení a dokážeme hlavní tvrzení kapitoly, 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 13 (pp-eliminace kvantifikátorů)**.** *Každá formule v jazyce modulů je ekvivalentní nějaké booleovské kombinaci pp-formulí a invariantních tvrzení v teorii modulů.*

Důkaz. Formule budeme eliminovat indukcí podle složitosti. Atomické formule jsou ekvivalentní formulím tvaru $\sum r_i x_i = 0$ a tedy zřejmě pp-formule. Dále z indukce stačí eliminovat formule tvaru $\exists y\varphi(y,\bar{x})$, kde $\varphi(y,\bar{x})$ je booleovská kombinace pp-formulí a invariantních tvrzení. Protože jsou invariantní tvrzení uzavřené formule, kvantifikátor $\exists y$ se nevztahuje k proměnným v nich a můžeme tedy uvažovat, ze $\varphi(y,\bar{x})$ je booleovská kombinace pp-formuli. Tedy po převedení do normálního tvaru můžeme předpokládat, že

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

, kde φ_j a ψ_{ij} jsou pp-formule. Dále z matematické logiky víme, že je možné prohodit $\exists$ a $\vee$ a dostáváme, že pro důkaz lemmatu stačí eliminovat formule tvaru

$$\exists y(\varphi(y,\bar{x}) \wedge \bigwedge_i \neg\psi_i(y,\bar{x})),$$

kde φ,ψ_i jsou pp-formule.

Dále můžeme předpokládat, že $\psi_i(y,\bar{x}) = \varphi(y,\bar{x}) \wedge \psi_i'(y,\bar{x})$, kde $\psi_i'(y,\bar{x})$ je pp-formule.

Dále buď M modul, H grupa taková, že

$$H \coloneqq \{a \in M : \exists \bar{c} \in M^{l(\bar{x})}, M \models \varphi(a,\bar{c})\}$$

, $G_i \coloneqq \psi_i(M,\bar{0})$, $G \coloneqq \varphi(M,\bar{0})$ její podgrupy a $\bar{b} \in M^{l(\bar{x})}$.

Potom máme, že

$$M \models \neg(\exists y(\varphi(y,\bar{b}) \wedge \bigwedge_{i<n} \neg\psi_i(y,\bar{b})))$$

, právě když $\varphi(M,\bar{b}) = \bigcup_{i<n} \psi_i(M,\bar{b})$.

Předpokládejme, že $\varphi(M,\bar{b}) = \bigcup_{i<n} \psi_i(M,\bar{b})$. Podle Neumannova lemmatu, můžeme z daného pokrytí vynechat takové cosety, že $[G : G_i] > n!$.

Budeme chtít použít lemma 12 a k tomu použijeme formule $\alpha_{M,\bar{b}}(\bar{x})$, která je booleovská kombinace pp-formulí a invariantních tvrzení a v které je

(1) pro která $j < n$ je $[G : G_j] \leq n!$ (to umíme vyjádřit pomocí invariantních tvrzení).. Dále uvažujme J množinu těchto indexů j a máme konečný horní odhad na $[\bigcap_{j\in J} G_j : \bigcap_{i\in I} G_i])$ pro $I \subseteq J \subseteq \{0,...,n-1\}$.

(2) pro $M,\bar{b}$ "správná"(splněná $\bar{b}$ v M) booleovská kombinace pp-formulí, která říká je-li průnik všech možných kombinací uvažovaných G_i "posunutých do b"(hned upřesníme formulí) prázdný nebo neprázdný. Myslíme tím všechny "správné" $\pm\exists y \bigwedge_{k\in K} \psi_k(y,\bar{b})$ případně i konjukce s $\varphi(y,\bar{b})$), kde $K \subseteq \{0,...,n-1\}$.

Podle lemmatu 12 máme pro jiné M', $\bar{b}'$

$$M' \models \alpha_{M,\bar{b}}(\bar{b}') \Rightarrow M' \models \neg(\exists y(\varphi(y,\bar{b}) \wedge \bigwedge_{i<n} \neg\psi_i(y,\bar{b})))$$

Díky Neumannovu lemmatu máme

$$|\{\alpha_{M,\bar{b}}(\bar{x}) : M \models \neg(\exists y(\varphi(y,\bar{b}) \wedge \bigwedge_{i<n} \neg\psi_i(y,\bar{b})))\}| = m, m \in \mathbb{N}$$

a vidíme, že negace formule, z které jsme chtěli eliminovat kvantifikátor, je konjukcí konečně mnoha výše popsaných formulí. □

2.3 Důsledky pp-eliminace kvantifikátorů

Důkazy lze nalézt v kapitole 2.5 knihy Prest (1988)

Důsledek 14. *Každá sentence v jazyce R-modulů je modulo teorie R-modulů ekvivalentní invariantnímu tvrzení.*

Důsledek 15. *Každá formule v jazyce R-modulů je v nějaké úplné teorii R-modulů ekvivalentní nějaké booleovské kombinaci pp-formulí.*

Důsledek 16. *Dva modely M_1,M_2 teorie R-modulů jsou elementárně ekvivalentní, pravě když pro každé dvě pp-formule ψ,ρ takové, že $\psi \to \rho$ platí $Inv(M_1,\rho,\psi) = Inv(M_2,\rho,\psi)$*

Důsledek 17. *Pro M_i, $i \in I$ moduly, ψ,ρ pp-formule*

$$Inv(\bigoplus_{i\in I} M_i,\rho,\psi) = \prod_{i\in I} Inv(M_i,\rho,\psi)$$

Důsledek 18. *Pro M modul, κ nekonečný kardinál*

$$M^\kappa \equiv M^{\aleph_0}$$

Pozorování 19. *Buďte M, N, S moduly, ze $M \equiv N$, pak $M \oplus S \equiv N \oplus S$.*

Důkaz. Díky větě o eliminaci kvantifikátorů víme, že každá sentence teorie abelovských grup je ekvivalentní invariantním tvrzením. Dále pro libovolné moduly K, L platí $Inv(K \oplus L,\varphi,\psi) = Inv(K,\varphi,\psi)Inv(L,\varphi,\psi)$ *mod* ∞ z a odsud plyne tvrzení. □

3. 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.

Materiál této kapitoly je čerpán z Zieglerova článku Ziegler (1984). Důkazy, které zde nebudou uvedeny nebo budou nekompletní jsou k nalezení v témže článku.

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

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 $a \in M$.

Lemma 20. *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*

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* 21 *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* 21, *která je podobná jedné z možných definic injektivních modulů ("Modul je injektivní, pokud je direktním sčítancem v každém nadmodulu").*

Věta 21. *Pro každý modul jsou následující podmínky ekvivalentní:*

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

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

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

(4) M je kompakt.

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

Lemma 22. *Direktní sčítance kompakního modulu jsou kompaktní.*

Důkaz. Důkaz analogický důkazu implikace (1) $\Longrightarrow$ (3) věty 21. □

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

Definice 15. *Buď M modul, $a \in M$. Řekneme, že typ p tvaru $\{\varphi(x) : \varphi\ pp-formule,\ M \models \varphi(a)\} \cup \{\varphi(x) : \neg\varphi\ pp-formule,\ M \models \varphi(a)\}$ je pp-úplný typ.*

Pozorování 23. *Každý pp-úplný typ daný prvkem $a \in M$ určuje celý typ prvku a nad M. Díky eleminaci kvantifikátorů a z vlastnosti obalu plyne, že $H(a)$ je až na isomorfismus jednoznačně zadán pp-úplným typem p, tedy můžeme psát $H(p)$.*

Definice 16. *Řekneme, že pp-úplný typ p je nerozložitelný, pokud $H(p)$ je nerozložitelný.*

Pozorování 24. *Každý nerozložitelný modul U je izomorfní $H(p)$ pro vhodný nerozložitelný typ p.*

Věta 25. *Obal $H(A)$ existuje a je určen jednoznačně.*

Důkaz k nalezení v Ziegler (1984, Theorem 3.6.)

Pozorování 26. *Předpokládejme, že $\varphi/\psi(M) > 1$, kde φ, ψ jsou pp-formule takové, že $\psi(M) \subseteq \varphi(M)$. Potom existuje nerozložitelný pp-úplný typ p, který obsahuje φ,$\neg\psi$.*

Definice 17. *Buď M modul, řekneme, že $\widehat{M}$ je čistý obal M pokud*

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

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

Věta 27. *Ke každému modulu M existuje až na isomorfismus jedinečný čistý obal.*

Věta 28. *Buď M modul, potom $\widehat{M}$ je elementární rozšíření M.*

3.1 Nerozložitelné kompakty

Definice 18. *Neprázdný kompaktní modul M, nazveme nerozložitelným kompaktem, pokud není direktní sumou dvou neprázdných modulů.*

Lemma 29. *Nechť je U neprázdný kompakt, potom je U nerozložitelný kompakt, 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 20 je M čistý podmodul U a z lemmatu 22 je M kompaktní a přitom $M \subsetneq U$.

Pokud $a \in U \setminus 0$, $H(a)$ je podle (1) z věty 21 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 Ziegler (1984, Corollary 4.2.)

Lemma 30.

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

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

Poznámka. Díky lemmatu 30 můžeme z každé třídy ekvivalence isomorfismu nerozložitelných kompakt vybrat jednoho zástupce U a uvažovat množinu všech U. Kdybychom neměli horní dohad (1), museli bychom uvažovat jestli vůbec mohou tvořit množinu.

3.2 Krull-Remak-Schmidt theorem

Věta 31 (Krull-Remak-Schmidt)**.** *Buď M kompaktní modul, potom existuje rozklad $M = \widehat{\bigoplus_{i\in I} U_i} \oplus E$, kde I je nějaká indexová množina, U_i jsou nerozložitelné kompakty a E je modul, který nemá žádný nerozložitelný kompakt jako direktní sčítanec.*

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

Definice 19. *Buď U nerozložitelný kompakt a M kompaktní modul. Potom definujme $U-dim(M) := |\{i \in I : U \simeq U_i\}|$, kde U_i jsou z rozkladu $M = \widehat{\bigoplus_{i\in I} U_i} \oplus E$*

Pozorování 32. *Buď M, N kompakty, kde M je slabě saturovaný. Pokud $M \equiv N$, pak*

$$U - dim(N) \leq U - dim(M) \ mod \ \infty$$

pro každý nerozložitelný modul U.

Důkaz. Buď U nerozložitelný modul a p nerozložitelný typ takový, že $U = H(p)$. Definujme typ

$$p_n(x_0,...,x_{n-1}) := \bigcup_{i<n} p(x_i) \cup \{\varphi(x_0,...,x_i,...,x_{n-1}) \to \varphi(x_0,...,0,...,x_{n-1}) :$$

$$\varphi(\bar{x}) \ pp - formula, \ i < n\}.$$

Pokud je $U - dim(N) \geq n$ pak je p_n realizován v N a tedy je $M-$konzistentní, protože $M \equiv N$. Protože M je slabě saturovaný je p_n realizován i v M. Dále platí, že

$$\sum_{i<n} H(b_i) = \bigoplus_{i<n} H(b_i) \simeq \bigoplus_{i<n} U,$$

tedy $U - dim(M) \geq n$ a tedy $U - dim(N) \leq U - dim(M)$. □

Věta 33. *Buď M slabě saturovaný a kompaktní modul. Dále buď*

$$M = \widehat{\bigoplus_{i\in I} U_i} \oplus E$$

rozklad jako v předchozí větě. Potom $M \equiv \widehat{\bigoplus_{i\in I} U_i}$.

V tomto důkazu budeme používat narozdíl od předchozí kapitoly Zieglerova úspornějšího značení pro invarianty. Místo $Inv(M,\varphi,\psi$ budeme psát $\varphi/\psi(M)$, pro modul M

Důkaz. Díky eliminaci kvantifikátorů a obdobné úvaze jako v pozorování 19 stačí dokázat, že

$$\varphi/\psi(E) > 1 \implies \varphi/\psi(\widehat{\bigoplus_{i\in I} U_i}) = \infty.$$

Předpokládejme, že $\varphi/\psi(E) > 1$. Z pozorovaní 26 víme, že existuje $E-$konzistentní nerozložitelný typ p obsahující $\varphi,\neg\psi$. Mějme kompakt N, který realizuje p a $N \equiv E$ a definujeme $U \coloneqq H(p)$. Potom $U - dim(N) > 0$ a $\varphi/\psi(N) > 1$. Z pozorovaní 19 a pozorování 32 potom vyplyne

$$U - dim(\widehat{\bigoplus_{i\in I} U_i}) + U - dim(N) \leq U - dim(M) = U - dim(\widehat{\bigoplus_{i\in I} U_i}) \ mod \ \infty.$$

Tedy $\{i \in I : U \simeq U_i\}$ je nekonečná a podobně jako v pozorování 19 by se dalo ukázat, že

$$\varphi/\psi(\bigoplus_{i\in I} U_i) = \prod_{i\in I} \varphi/\psi(U_i)$$

a tedy $\varphi/\psi(\widehat{\bigoplus_{i\in I} U_i}) = \infty$. □

Důsledek 34. *Každý modul je elementárně ekvivalentní nějaké direktní sumě nerozložitelných kompaktů*

Důkaz. Plyne z vět 33 a 28 □

4. Rozhodnutelnost teorie komutativních grup

V této kapitole 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 Fisher (1972)

Budeme chtít použít větu 33 a podle věty 39 nerozložitelné moduly nad $\mathbb{Z}$ jsou právě grupy uvedené v následující definici.

Definice 20. *Buď p prvočíslo, $n \in N$, G abelovská grupa*

(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) $\mathbb{Z}_{p^n}$ *cyklickou grupu řádu* p^n

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

Definice 21. *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 konečného ranku pokud jen konečně exponentů $\alpha_{p,n}$, β_p a γ_p je nenulových a všechny jsou konečné.

Definice 22. *Buď p prvočíslo, $n \in N$, G abelovská grupa*

(1) $p^nG \coloneqq \{g \in G \colon p^n \mid g\}$

(2) $p^nG[p] \coloneqq \{g \in G \colon pg = 0 \wedge p^n \mid g\}$

Definice 23. *Buď p prvočíslo, $n \in N$, G abelovská grupa,*
Szmielew invarianty budeme zvát invarianty

(1) $U(p,n)(G) \coloneqq |p^nG[p]/p^{n+1}G[p]|$

(2) $Tf(p,n)(G) \coloneqq |p^nG/p^{n+1}G|$

(3) $D(p,n)(G) \coloneqq |p^nG[p]|$

(4) $Exp(p,n)(G) \coloneqq |p^nG|$

Pozorování 35. *Zápis $p^n \mid g$ je syntaktická zkratka pro $\exists w(p^n w - x = 0)$ a $(pg = 0)$ i $\exists w(p^n w - x = 0)$ jsou pp-formule. Szmielew invarianty tedy jsou invarianty ve smyslu definice 11.*

Definice 24 (Szmielew invariantní tvrzení)**.** *Buďte $n, k \in \mathbb{N}$, p prvočíslo, G abelovská grupa.*

Szmielew kladná invariantní tvrzení budeme zvát následující tvrzení

(1) $U(p,n)(G) > k$

(2) $Tf(p,n)(G) > k$

(3) $D(p,n)(G) > k$

(4) $Exp(p,n)(G) > k$

Jejich negacím budeme říkat Szmielew záporná invariantní tvrzení.
Dohromady jim budeme Szmielew invariantní tvrzení.

K důkazu následující věty si je pouze třeba uvědomit definice zmíněných grup a Szmielew invariantů.

Lemma 36. *Buďte p, q prvočísla $m, n \in \mathbb{N}$ potom*

1. (a) $U(p,n)(\mathbb{Z}_{q^m}) = \begin{cases} p & pokud\ p = q \wedge n = m - 1 \\ 1 & jinak. \end{cases}$

   (b) $U(p,n)(G) = 1$, *pro* $G \in \{\mathbb{Z}_{(q)}, \mathbb{Z}(q^\infty), \mathbb{Q}\}$

2. (a) $Tf(p,n)(\mathbb{Z}_{(q)}) = \begin{cases} p & pokud\ p = q \\ 1 & jinak. \end{cases}$

   (b) $Tf(p,n)(\mathbb{Z}_{q^m}) = \begin{cases} p & pokud\ p = q \wedge n < m \\ 1 & jinak. \end{cases}$

   (c) $Tf(p,n)(G) = 1$, *pro* $G \in \{\mathbb{Z}(q^\infty), \mathbb{Q}\}$

3. (a) $D(p,n)(\mathbb{Z}(q^\infty)) = \begin{cases} p & pokud\ p = q \\ 1 & jinak. \end{cases}$

   (b) $D(p,n)(\mathbb{Z}_{q^m}) = \begin{cases} p & pokud\ p = q \wedge n < m \\ 1 & jinak. \end{cases}$

   (c) $D(p,n)(G) = 1$, *pro* $G \in \{\mathbb{Z}_{(q)}, \mathbb{Z}(q^\infty), \mathbb{Q}\}$

4. (a) $Exp(p,n)(G)(\mathbb{Z}_{q^m}) = \begin{cases} p & pokud\ p = q \wedge m \leq n \\ q^m & jinak. \end{cases}$

   (b) $Exp(p,n)(G) = \infty$, *pro* $G \in \{\mathbb{Z}_{(q)}, \mathbb{Z}(q^\infty), \mathbb{Q}\}$

Pozorování 37. *Buď p prvočíslo, $n \in N$, S Szmielew grupa*

(1) Pro Szmielew invarianty platí věta 17

(2) Pro vyjádření toho, že se nějaká z grup $\mathbb{Z}_{(p^n)}$, $\mathbb{Z}_{(p)}$, $\mathbb{Z}(p^\infty)$, v S vyskytuje nekonečněkrát pomocí Szmielew invariantních tvrzení jich potřebujeme nekonečně mnoho.

(3)

(4)

Lemma 38. *Szmielew grupa konečného ranku je určena Szmielew invarianty.*

Důkaz následující věty lze nalézt z větší části v knize Model Theory and Modules Prest (1988, Corrollary 2Z.11)

Věta 39. *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 $n \in \mathbb{N}$.*

Důkaz následujícího lemmatu je k nalezení v Hodges (2008, Lemma A.2.4)

Lemma 40. *Pro abelovskou grup G jsou následující podmínky ekvivalentní*

1. *Existuje přirozené číslo n, že $nG = 0$*
2. *$G \equiv G \oplus \mathbb{Q}$*
3. *$G \equiv G \oplus \mathbb{Q}^{\aleph_0}$*

Věta 41. *Každá abelovská grupa je elementárně ekvivalentní nějaké Szmielew grupě.*

Důkaz. Modul M je podle věty 34 elementárně ekvivalentní direktní sumě nerozložitelných kompaktů, kde se navíc podle vět 18 a 19 každý direktní sčítanec vyskytuje nejvýše spočetněkrát. Pro abelovské grupy máme s použitím věty 39 a lemmatu 40 požadované. □

Důkaz k následující větě je k nalezení v Hodges (2008, Lemma A.2.4 - A.2.6)

Důsledek 42. *Abelovské grupy G, H si jsou elementárně ekvivalentní, právě když mají stejné Szmielew invarianty.*

Důsledek 43. *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 41 elementárně ekvivalentní nějaké Szmielew grupě S. □

Důsledek 44. *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 důsledku 43 a věty o kompaktnosti z matematické logiky. □

Důkaz následující věty jen nastíníme

Důsledek 45. *Každá sentence $f \in Cons(T_{(AG)})$ platí v nějaké Szmielew grupě konečného ranku.*

Důkaz. Tvrzení je důsledkem důsledku 44, věty 43 a toho, že abychom řekli, že nějaký Szmielew invariant je v dané grupě nekonečný, potřebujeme nekonečně mnoho Szmielew invariantních tvrzení. Pro úplný důkaz by bylo třeba určit exponenty hledané Szmielew grupy, analogicky jako v Eklof a Fisher (1972, Theorem 2.10.) □

Důsledek 46. *Pro Szmielew grupu konečného ranku S umíme popsat konečnou množinu tvrzení axiomatizující S a množina S_{True} v S platných tvrzení je rozpoznatelná.*

Důkaz. Pro S máme konečný počet Szmielew kladných invariantních tvrzení S^+_{Inv}, které v S platí a konečný počet Szmielew záporných invariantních tvrzení S^-_{Inv}, z nichž vyplývají všechna Szmielew záporná invariantní tvrzení, která v S platí. Podle věty 44 je každé tvrzení platné v S důsledkem $T_{(AG)} \cup S^+_{Inv} \cup S^-_{Inv}$. □

Nyní závěrečné tvrzení práce

Věta 47. *$T_{(AG)}$ je rozhodnutelná teorie.*

Důkaz. Podle poznámky 5 stačí ukázat, že $Cons(T_{(AG)})$ je rozpoznatelná.

Je jednoduché si rozmyslet, že je rozpoznatelná množina konečných posloupností $S_{Ind} \coloneqq \{\langle \overline{\alpha_p}, \beta_p, \gamma_p, \delta\rangle : p \in F\}$, kde F je konečná podmnožina prvočísel, $\overline{\alpha_p}$ je konečná posloupnost $\langle \alpha_{p,1}, \dots \alpha_{p,n}\rangle$ přirozených čísel, β_p, γ_p jsou přirozená čísla a δ je buď 0 nebo 1. Proměnné jsou sugestivně pojmenovány stejně jako exponenty v definici 21, aby bylo zřejmé, že i množina $\mathbb{S}_{fin}$ Szmielew grup konečného ranku je rozpoznatelná.

Dále tedy předpokládejme, že máme prvky množiny $\mathbb{S}_{fin}$ nějak očíslované přirozenými čísly.

Podle věty 46 je pro $S_i \in \mathbb{S}_{fin}$ množina S_i^{Tvrz} tvrzení platných v S_i rozpoznatelná a můžeme ji tedy očíslovat přirozenými čísly. Buď tedy f_{ij} j-tý prvek S_i^{Tvrz}.

Nyní uvažujme bijekci $\pi\colon \mathbb{N} \to \mathbb{N}\times\mathbb{N}$, třeba funkci inverzní Cantorově párovací funkci a mějme $k,i,j \in \mathbb{N}$, že $\pi(k) = (i,j)$. A definujme $f_k \coloneqq f_{ij}$. Podle věty 45 se nám podařilo očíslovat všechny prvky $Cons(T_{(AG)})$ a práce je u konce. □

Seznam použité literatury

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

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

Hodges, W. (2008). *Model theory.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1 edition. ISBN 9780521066365,0521066360.

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

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

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

Stanovský, D. (2010). *Základy algebry.* Matfyzpress, Praha. ISBN 978-80-7378-105-7.

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