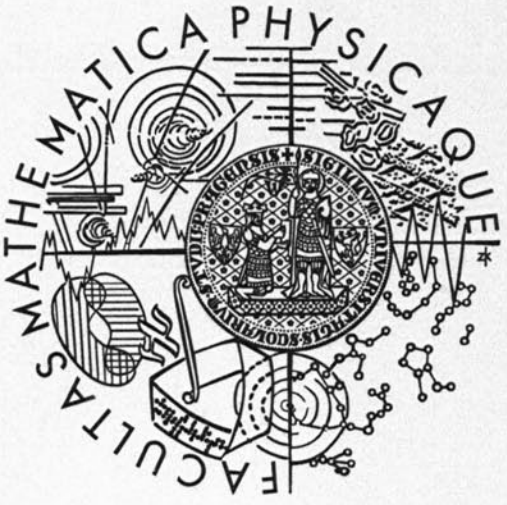
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Matěj Görner

Rozhodnutelnost abelovských grup

Katedra algebry

Vedoucí bakalářské práce: Mgr. Libor Barto Ph.D.
Studijní program: Obecná matematika (MOM)

2007

V první řadě bych zde moc rád poděkoval Liborovi, za dobré nápady a trpělivost, dále panu Hybnerovi a celé knihařské dílně na VŠUP.

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

V Praze dne 1.5.2007

Matěj Görner

Matěj Görner

Obsah

Název práce: Rozhodnutelnost abelovských grup
Autor: Matěj Görner
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Libor Barto Ph.D.
e-mail vedoucího: jetel@matfyz.cz

Abstrakt: V této práci reprodukuji jeden z klasických výsledků matematické logiky, totiž rozhodnutelnost kategorie abelovských grup, který publikovala Wanda Szmielew v roce 1949 [3]. Mým úkolem bylo důkaz pochopit a současnou a srozumitelnou formou ho prezentovat. Mé zásahy do důkazu jsou více méně omezeny na koncepční a terminologickou rovinu. Také jsem důkaz opatřil několika komentáři.
Klíčová slova: rozhodnutelnost, abelovská grupa, aritmetická třída.

Title: Decidability of Abelian groups
Author: Matěj Görner
Department: Department of Algebra
Supervisor: Mgr. Libor Barto Ph.D.
Supervisor's e-mail address: jetel@matfyz.cz

Abstract: A classical result of mathematical logic is reproduced in this work — namely decidability of Abelian Groups — publicated in 1955 by W. Szmielew [3]. The aim of this work is to present the proof in a contemporary and straightaway form. Changes in the original proof are limited in a structural and terminology side of the problem and some commentaries were added.

Keywords: decidability, Abelian group, arithmetic class.

Ustanovení základních pojmů

Předpokládám, že obsah níže uváděných pojmů je každému důvěrně znám, proto vše proberu v rychlosti, především, aby se předešlo terminologickým nedorozuměním.

1. Definice

- Algebraické proměnné (tedy proměnné, za které se dosazují prvky konkrétních algeber), budu v celé své práci důsledně značit v_i, $i \in \omega$.

- Term jayzka $\{+\}$ definujme induktivně:

  1. v_i, $i \in \omega$ je term,
  2. Jsou-li t_1 a t_2 termy jazyka $\{+\}$, pak je i $t_1 + t_2$ term jazyka $\{+\}$.
  - ◇ Term jazyka $\{+\}$ je neprázdná posloupnost znaků vzniklá konečným použitím pravidel 1. a 2.

- Formuli (jazyka $\{+\}$) definujeme opět induktivně:

  1. Jsou-li t_1 a t_2 termy jazyka $\{+\}$, potom $(t_1 = t_2)$ je formule ,
  2. jsou-li φ, ψ formule potom také $(\neg\psi)$; $(\psi \to \varphi)$, $(\forall v_i)(\psi)$ pro $i \in \omega$ jsou formule.
  - ◇ Všechny formule jazyka $\{+\}$ vzniknou konečným užitím pravidel 1. a 2.
  - ◇ Množinu všech formulí jazyka $\{+\}$ označme Fm_{+}.

- Formule je otevřená, pokud se v ní nevyskytuje žádný ze symbolů $\forall$. Formule je uzavřená, neboli se jedná o sentenci, pokud se v ní vyskytuje s každým výskytem v_i i výraz $(\forall v_i)$, který tento výskyt proměnné v_i kvantifikuje.

- Nechť $v_{i_1}, \ldots, v_{i_k}$ jsou právě všechny proměnné vyskytující se ve φ. Potom generálním uzávěrem φ, značíme $\mathrm{Gen}(\varphi)$, nazveme sentenci $(\forall v_{i_1}) \cdots (\forall v_{i_k})\, \varphi$.

Přijmeme běžnou konvencí o zjednodušeném zápise formulí, jako je vypouštění okrajových závorek, slučování stejných kvantifikátorů atp. Také známým způsobem obohatíme jazyk logiky o symboly $\vee$, $\wedge$, $\exists$ a budeme

používat speciální symbol $\equiv$, kterým budeme vyjadřovat skutečnost, že výraz na jeho levé straně je definován výrazem vpravo. Občas například budeme místo φ psát φ^1 a místo $\neg\varphi$ budeme psát φ^0. Tuto skutečnost můžeme tedy vyjádřit $\varphi^1 \equiv \varphi$ a $\varphi^0 \equiv \neg\varphi$.

Rovněž bez bližšího upozornění budeme používat fakt, že každá formule φ lze upravit na logicky ekvivalentní formuli (tj. formuli odvozenou z φ jen pomocí axiomů logiky a axiomů pro $\forall$), jenž má tvar:

$$(Q_0 v_o)\cdots(Q_n v_n)\Big(\bigvee_{i<m}\bigwedge_{j<n}(*)\varphi_{ij}\Big), \tag{1}$$

kde Q_k zastupuje $\exists$ nebo $\forall$, $(*)$ zastupuje buď $\neg$ nebo $\neg(\neg)$ a φ_{ij} jsou otevřená formule.

2. Definice

- $\mathcal{A} = \langle A, + \rangle$ nechť nadále označuje třídu všech algeber s jednou binární operací, $\mathcal{G} \subseteq \mathcal{A}$ nechť značí třídu všech grup a konečně $\mathcal{AG} \subseteq \mathcal{G}$ nechť označuje všechny abelovské grupy.

- Za teorii T jazyka $\{+\}$ budeme považovat jakoukoli množinu sentencí z $\frac{\mathsf{Fm}}{+}$. Specálně jako teorii grup je

$$T_G = \{(\forall v_1, \ldots, v_7)(\exists v_8, v_9) \quad ((v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)) \\ \wedge (v_4 + v_8 = v_5) \wedge (v_9 + v_6 = v_7)\}$$

  a teorie abelovských grup $T_{AG} = T_G \cup \{(\forall v_1, v_2)(v_1 + v_2 = v_2 + v_1)\}$.

- Model teorie T (jazyka $\{+\}$) bude jakákoli $A \in \mathcal{A}$, taková, že pro každou sentenci $\varphi \in T$, bude v A platná sentence φ^A, která vznikne z φ tak, že každý výraz $(\forall v_i)$ vyskytující se ve φ zaměníme za $(\forall a_i \in A)$ a každý jiný výskyt „v_j“ ve φ zaměníme za „a_j“. Skutečnost, že A je modelem T značíme $T \models A$.

- Třídu všech modelů teorie T označujeme $\mathfrak{M}_T$. Model abelovských grup označujme prostě $\mathfrak{M}^+_{AG}$. V kapitole II. ukážeme, že platí $\mathcal{AG} = \mathfrak{M}_{AG}$. Třídu modelů teorie $H = T \cup \{\varphi\}$ označujeme také $\mathfrak{M}_T(\varphi)$ a každou takovou třídu nazveme aritmetickou třídou teorie T. Množinu všech aritmetických tříd teorie T_{AG} označíme ArC. Tedy ArC$= \{\mathfrak{M}_T(\varphi);\ \varphi \in \frac{\mathsf{Fm}}{+}\}$.

- Pro teorii T zavedeme T-ekvivalenci na sentencích $\varphi, \psi \in \frac{\mathsf{Fm}}{+}$ tak, aby $\varphi \sim_T \psi$ právě tehdy když $\mathfrak{M}_T(\varphi) = \mathfrak{M}_T(\psi)$. Místo $\sim_\emptyset$ píšeme běžně pouze $\sim$ a díky větě o úplnosti logiky prvního řádu je tato relace identická s „logickou ekvivalencí", vzniklou aplikací logických axiomů. Dvě teorie H, H' jsou T-ekvivalentní, $H \sim_T H'$, pokud pro všechny sentence $\varphi \in H$ existuje $\varphi' \in H'$ tak, že $\varphi \sim_T \varphi'$, a pro všechny $\psi \in H'$ existuje $\psi' \in H$, že $\psi \sim_T \psi'$.

Rozhodnutelnost

3. Definice Teorie T jazyka $\{+\}$ je rozhodnutelná, pokud množina všech sentencí pravdivých v T je rekurzivní.

Poznámka V našem důkaze si vystačíme s naivní teorií rekurzivity. Za algoritmus budeme považovat takový ustálený výpočetní postup, ve kterém se používá sčítání, násobení, faktorizování, vybírají se z konečné množiny prvky dobře[1] definovaných vlastností a při kterém si smíme pamatovat mezivýsledky. Intuitivní definice rozhodnutelnosti má potom podobu:

Teorie je rozhodnutelná, pokud existuje algoritmus, který o každé sentenci $\varphi \in (\frac{\mathsf{Fm}}{+})$ teorie T rozhodne, zda platí:

$$T \vdash \varphi.$$

Což je přirozeně ekvivalentní s existencí algoritmu, který rozhodne, zda pro každou sentenci $\varphi \in (\frac{\mathsf{Fm}}{+})$ platí: $T \cup \{\varphi\} \vdash \bot$, kde $\bot$ je zápis pro spor (tedy $\bot \equiv \psi \wedge (\neg\psi)$).

Předmětem práce je dokázat, že $\mathcal{AG}$ je rozhodnutelná. Použijeme následující strategii. Nejprve si zvolíme jistou množinu formulí, kterou budeme označovat jako základní množinu formulí, $\mathbf{B}$, tak, aby nejmenší Booleova algebra obsahující $\mathbf{B}$ byla ekvivalentní s $\frac{\mathsf{Fm}}{+}$. Na druhou stranu požadujeme, aby $\mathbf{B}$ měla dostatečně "čitelnou" strukturu. Výběr množiny $\mathbf{B}$ je nejchoulostivějším bodem tohoto důkazu a bude realizován v kapitole II.

Rozhodovací algoritmus bude sestávat za dvou kroků: Nejprve ke každé formuli φ z $\frac{\mathsf{Fm}}{+}$, najdeme formuli β skládající se z konečných disjunkcí konečných konjunkcí formulí z $\mathbf{B}$ a jejich doplňků (tedy z Booleovy algebry generované $\mathbf{B}$). Této části se říká *eliminace kvantifikátorů* a provedeme ji ve kapitole III.

Druhým krokem bude samotný rozhodovací akt. Problém jsme převedli na otázku, kdy je β sporná. Přitom nám postačuje vyšetřit všechny klauzule

[1] tedy definovaná pomocí efektivních aritmetických operací

tvaru $\bigwedge \beta_i$, $\beta_i \in \mathbf{B}$. V tomto smyslu jsem myslil „čitelnost“ **B** a tato diskuse bude náplní kapitoly IV.

4. Definice

a. Pro $K \subseteq \frac{\mathsf{Fm}}{+}$ definujeme generála K jako $K^\bullet = \{\mathrm{Gen}(\varphi), \varphi \in K\}$

b. Booleovský obal množiny formulí K, značení $\mathrm{bool}(K)$, je nejmenší nadmnožina K uzavřená na konjunkce, disjunkce a negace,

$$\mathrm{bool}(K) = \Big\{ \bigvee_{k<m} \bigwedge_{l<n} \varphi_{kl}^{(r(k,l))};\ r \underset{\sim}{\in} {}^{m\times n}2, \varphi \in K \Big\}.$$

c. Řekneme, že množina $B \subseteq \frac{\mathsf{Fm}}{+}$ je *základní množina formulí teorie* T, pokud $(\mathrm{bool}(B))^\bullet \sim_T (\frac{\mathsf{Fm}}{+})^\bullet$. Dále S nazvěme *základní množina sentencí* T, pokud splňuje $\mathrm{bool}(S^\bullet) \sim_T (\frac{\mathsf{Fm}}{+})^\bullet$.

5. Lemma Množina $B \subseteq \frac{\mathsf{Fm}}{+}$ je základní množina formulí T, pokud jsou splněny následující podmínky:

i. Je-li $\varphi(v_i, v_j) \in B$ a v_j je volná proměnná, tak i $\varphi'(v_j, v_i)$ náleží do B, kde φ' vzniklo prohozením proměnných v_j a v_i ve φ ,

ii. $\forall i, j, k \in \omega$: $(v_i + v_j = v_k) \in \mathrm{bool}(B)$ a $(v_i = v_k) \in \mathrm{bool}(B)$,

iii. $\varphi_1, \ldots, \varphi_n \in B$, $r \underset{\sim}{\in} {}^n2$, potom $(\exists v_o)(\bigwedge_{i<n} \varphi_i^{(r(i))}) \sim_T \varphi$; $\varphi \in \mathrm{bool}(B)$.

Důkaz: Množina K obsahující všechny formule $v_i + v_j = v_k$ a $v_i = v_k$, která je uzavřená na operace $\exists$, $\bigvee$ a $\neg$ již splňuje $K \sim \frac{\mathsf{Fm}}{+}$. Ukažme nyní, že $K \sim_T B$. Mějme tedy $\varphi \in K$ a sestrojme k ní ekvivalentní formuli $\psi \in B$. Převeďme φ do tvaru (1) a postupujme indukcí podle počtu kvantifikátorů. Je-li na pozici $(Q_k v_s)$ existenční kvantifikátor můžeme zaměnit podle i. v_o za v_s a na základě iii. zaměnit $(Q_k v_s)\varphi$ za $\psi \in \mathrm{bool}(B)$, která již kvantifikátor neobsahuje a potom nazpátek provést záměnu v_o za v_s. Pokud Q_k reprezentuje generální kvantifikátor použijeme $\forall v_o\, \varphi \sim \neg(\exists v_0\, \neg\varphi)$ a uzavřenosti $\mathrm{bool}(B)$ na negaci. □

II. Elementární vlastnosti abelovských grup.

Definice grupy

V I.2 jsme zavedli pojem *teorie grup* T_G jako jedinou sentenci jazyka $\{+\}$, která je ekvivalentní podmínkám G1), G2), G3).

$T_G: \mathbf{G} = \langle \mathbf{G}, + \rangle$	$T'_G: \mathbf{G}' = \langle \mathbf{G}, +, -, \mathbf{0} \rangle$
G1) $\forall x, y, z: x + y + z = x + (y + z)$	G1) $\forall x, y, z: x + y + z = x + (y + z)$
G2) $\forall x, y \exists z: x + z = y$	G2') $\forall x: x + 0 = x = 0 + x$
G3) $\forall x, y \exists z: z + x = y$	G3') $x + (-x) = 0$
GK) $\forall x, y: x + y = y + x$	GK) $\forall x, y: x + y = y + x$

"Standardní" definice grupy, podle které byl tento pojem zaveden v úvodním kurzu na naší fakultě, pohlíží na grupy jako na algebraickou strukturu s jednou binární operací $(+)$, jednou unární operací $(-)$ a jednou konstantou (0), splňující podmínky (G1), (G2') a (G3'), které označme T'_G. Pokusme se na úvod této kapitoly prokázat ekvivalenci obou přístupů. Mějme tedy algebru $G \in \mathcal{A}$ v níž platí T_G. Pro nějaký prvek $a \in G$ nejdeme podle (G2) prvek e tak, aby $a + e = a$. Nyní pro jakýkoli prvek $b \in G$ najdeme podle (G3) prvek c tak, aby $c + a = b$. Tedy s využitím (G1) máme $b + e = c + a + e = c + a = b$, čili e má vlastnost (G2') a dále (G3') plyne opětovnou aplikací (G2).

Mějme nyní algebru $G' = \langle G, +, -, 0 \rangle$, splňující T'_G. Nejprve ukažme, že $-(-x) = x$ tedy $x = x + (-x + (-(-x))) = x + (-x) + (-(-x)) = (-(-x))$. Dále pro každé x, y volme $z = -x + y$, $z' = y - x$, takže dostáváme $x + z = y$, $z' + x = y$ a platí (G2) a (G3).

Definice grupy pomocí T_G, je pro naši snahu o eliminaci kvantifikátorů užitečnější, než definice pomocí T'_G. Indukční struktura formulí nad jazykem $\{+\}$ tak, jak byla zavedena v I.1 by *měla být formálně jednodušší*, než struktura formulí nad jazykem $\{+, -, 0\}$, ačkoli jsou samozřejmě obě množiny formulí identické ve smyslu definice III.13 (tzn. pro každou formuli z jedné množiny existuje identická formule z druhé množiny ve smyslu odkazované definice).

Nyní je nejvhodnější čas zmínit se, že dnes se k dokazování rozhodnutelnosti různých algeber používají elegantnější nástroje vycházející z univerzální algebry. Jako přirozený přístup ke zkoumání rozhodnutelnosti se ukázal přístup přes algebraické variety. Pro zajímavost alespoň nastiňme, co to variety jsou. Třídu algeber nad daným jazykem nazveme varieta, pokud je uzavřená na podstruktury, homomorfní obrazy a direktní součiny.

Ekvivalentně můžeme varietu definovat, jako množinu všech algeber, ve kterých je univerzálně platná nějaká soustava identit (generálních uzávěrů otevřených formulí). Vše bude jasné, až napíšeme rovnice, které určují varitu abelovských grup:

$$\begin{aligned} T''_G: &\quad \mathbf{G} = \langle \mathbf{G}, +, - \rangle \\ \text{G1"}) \ \forall x,y,z: &\quad x+y+z = x+(y+z) \\ \text{G2"}) \ \forall x,y: &\quad x+(-x) = y+(-y) \\ \text{G3"}) \ \forall x,y: &\quad x+(y+(-y)) = x \\ \text{GK}) \ \forall x,y: &\quad x+y = y+x \end{aligned}$$

Varieta je lokálně konečná, pokud každá její konečně generovaná algebra je konečná. Ralph McKanzie a Mathew Valeriote například v [1] charakterizovali rozhodnutelné lokálně konečné variety a to dokonce i nad nekonečnými jazyky (zde je ovšem potřeba poopravit definici rozhodnutelnosti). Ačkoli se přístup, kterým jsem se vydal já zde, může někomu zdát zastaralý, má dodnes svoji aktuálnost. Eliminace kvantifikátorů nám dává o struktuře aritmetických tříd T_{AG} i další informace, než jen pouhou rozhodnutelnost, těmto důsledkům se zde však nebudeme věnovat.

Lineární nezávislost modulo $[p;k]$

Následující tvrzení jsem převzal z [2], kde může zájemce vyhledat i patřičné důkazy.

6. Tvrzení Pro každou konečnou abelovskou grupu G platí $G \cong Z_0 \oplus \cdots \oplus Z_{m-1}$, kde $|Z_i| = p_i^{k_i}$; $i \leq m$ jsou cyklické grupy řádu mocnin prvočísel, které navíc splňují následující podmínku jednoznačnosti: Pokud existují $W_0, \ldots, W_{n-1}$ takové, že $|W_i| = q_i^{l_i}$; $i \leq n$ jsou cyklické řádu mocnin prvočísel a $G \cong W_0 \oplus \ldots \oplus W_{n-1}$, pak existuje taková bijekce $\pi : m \to n$, že $p_{\pi(i)} = q_j$ a $k_{\pi(i)} = l_j$ pro všechna $i < m$.

Každá torzní (tj. každý prvek je konečného řádu) konečně generovaná grupa $G \in \mathcal{AG}$ je konečná.

Pro každou konečně generovanou abelovskou grupu platí, že $G = G_T \oplus F$, kde G_T je maximální torzní část G a F je volná abelovská grupa. Jelikož G_T tvoří podgrupu G a každá podgrupa konečně generované je konečně generovaná, můžeme G_T zapsat jako direktní součet cyklických grup. Dále pak každá konečně generovaná volná grupa F je konečným direktním součtem grup $Z \cong \mathbb{Z}$.

Z výše uvedeného již plyne, že můžeme každou konečně generovanou $G \in \mathcal{AG}$ vyjádřit jako direktní součet cyklických grup.

Pro $a, b \in \mathbb{Z}$ a prvky g, h grupy G chápejme:

$$ag = \begin{cases} g + \cdots + g & \text{pro } a > 0 \\ 0 & \text{pro } a = 0 \\ (-g) + \cdots + (-g) & \text{pro } a < 0 \end{cases}$$

Dále říkáme, že a dělí g (neboli g je a-divizibilní, g kongruentní s 0 modulo a), pokud exisuje $h \in G$ tak že $ah = g$. Prvky $g, g' \in G$ jsou kongruentní modulo a, značíme $g \equiv g' \pmod{a}$, pokud a dělí $g - g'$. Pokud g, g' nejsou kongruentní modulo a, potom jsou inkongruentní modulo a, tedy $g \not\equiv g' \pmod{a}$.

7. Definice Buď G abelovská grupa, p prvočíslo a $k, a_0, \ldots, a_{m-1}$ celá čísla. Řekneme, že prvky $x_0, \ldots, x_{m-1}$ *jsou lineárně nezávislé modulo* p^k, neboli symbolicky mají vlastnost $ln[p; k]$ pokud platí:

$$a_0x_0 + \cdots + a_{m-1}x_{m-1} = 0 \quad \textbf{implikuje} \quad a_0 \equiv 0, \cdots, a_{m-1} \equiv 0 \pmod{p^k}.$$

Dále řekneme, že prvky $x_0, \ldots, x_{m-1}$ jsou *silně lineárně nezávislé modulo* p^k, neboli symbolicky mají vlastnost $ln_S[p; k]$ pokud platí:

$$a_0x_0 + \cdots + a_mx_m \text{ je dělitelné } p^k \quad \textbf{implikuje} \quad a_0 \equiv 0, \cdots, a_m \equiv 0 \pmod{p^k}.$$

Řekneme, že prvky $x_0, \ldots, x_{m-1}$ mají vlastnost $ln^O[p; k]$, pokud jsou lineárně nezávislé modulo p^k a každý z nich je řádu p^k. A nakonec řekneme, že prvky mají vlastnost ln_S^O, pokud mají vlastnost $ln_S[p; k]$ a zároveň vlastnost $ln^O[p; k]$.

Symbol $ln^*[p; k]$ bude zastupovat buď vlastnost $ln^O[p; k]$ nebo $ln[p; k]$, zjednodušíme si tím vyjadřování. Ve stejném kontextu vždy stejně uložená hvězdička bude znamenat stejný znak. Podobnou konvenci zaveďme i o $ln_*[p; k]$ a $ln_*^*[p; k]$. Pro konkrétní upřesnění, jakou z 10 smysluplných kombinací symbolu mám na mysli, budu používat výrazy $\binom{O}{*}$, $\binom{-}{S}$, ...(přitom pomlka zastupuje prázdný znak).

Následuje několik pozorování ohledně vlastností $ln_*^*[p; k]$. G značí vždy abelovskou grupu a x_i, y_i její prvky, dále ať a_i, $i \in \omega$ značí celá čísla, ať k, n, n_1, n_2 značí čísla nezáporná a p prvočíslo.

Pokud $X \subseteq G$ má vlastnost $ln_*^*[p; k]$, potom i každá $X' \subset X$ má vlastnost $ln_*^*[p; k]$. Pokud má x_0 vlastnost $ln_*^*[p; k]$, potom řád prvku x_0 je buďto nekonečný, nebo je dělitelný p^k.

$x_1, \ldots, x_m$ jsou $ln^*_*[p;k]$	potom	$x_1, \ldots, x_m$ jsou $ln[p;k]$,
$x_1, \ldots, x_m$ jsou $ln^O_S[p;k]$	potom	$x_1, \ldots, x_m$ jsou $ln^*_*[p;k]$
$x_1, \ldots, x_m$ jsou $ln_*[p;k]$	implikuje	$x_1, \ldots, x_m$ jsou $ln_*[p, k-1]$
$x_1, \ldots, x_m$ jsou $ln^O[p;k]$	implikuje	$px_1, \ldots, px_m$ jsou $ln^O[p, k-1]$,

Následuje praktické kritérium (silné) lineární nezávislosti modulo p^k. Prvky $x_0, \ldots, x_{m-1}$ mají vlastnost $ln_*[p;k]$ právě tehdy když platí:

$$\left.\begin{array}{ll} p^{k-1}\sum_{i<m} a_i x_i = 0 & \text{pro } \binom{-}{*} = \binom{-}{-} \\ p^{k-1}\sum_{i<m} a_i x_i \text{ je dělitelné } p^k & \text{pro } \binom{-}{*} = \binom{-}{S} \end{array}\right\} \textbf{implikuje } p \text{ dělí všechna } a_i$$

8. Definice Pro p prvočíslo, k nezáporné a abelovskou grupu G označme $\dim^*_*[p;k](G)$ maximální počet pvků z G majících vlastnost $ln^*_*[p;k]$. Dále ať pro celé číslo s značí $sG = \{sg;\ g \in G\}$ všechny s-divizibilní prvky G, $\mathrm{ord}[p^k](G) = \{g \in G;\ p^k g = 0\}$ všechny prvky řádu p^k a konečně $\mathrm{sub}[p^k](G) = \{g \in G/p^k G\}$ všechny prvky G, které nejsou dělitelné p^k.

Pro každé $s \in \mathbb{Z}$ je sG podgrupa v G a $\dim^*_*[p,k](G)$ nabývá hodnot $[0; \infty,]$.

Navíc platí, že $\dim^*_*[p;k](G) = n$ $(n \in \omega \cup \{\infty\})$, právě tehdy když:

- množina $\mathrm{ord}[p^k](p^{k-1}G)$ má právě p^n prvků pro volbu $\binom{*}{*} = \binom{O}{-}$,
- v množině $(p^{k-1}G)$ je právě p^n prvků, jsou po dvou nekongruentí modulo p^k pro volbu $\binom{*}{*} = \binom{-}{S}$,
- v množině $\mathrm{ord}[p^k](p^{k-1}G)$ je právě p^n prvků, které jsou po dvou nekongruentní modulo p^k pro $\binom{*}{*} = \binom{O}{S}$.

Neexistuje žádná podobná charakterizace pro $\dim[p;k]$, ale můžeme obdobné ideje použít k charakterizaci $\dim^O$ a $\dim_S$:

- $\dim^O[p;k](G) = \dim[p;k](\mathrm{ord}(G))$ a $\dim_S[p;k](G) = \dim[p;k](\mathrm{sub}(G))$, kde výraz $\dim[p;k]$ uvažujeme ve zobecněném smyslu oproti definici, jelikož připouštíme jako jeho argument i pologrupu.

Platí: Nechť prvky $x_0, \ldots, x_{m-1}$ mají vlastnost $ln^O_S[p;k]$ a prvky $y_0, \ldots, y_{n-1}$ mají vlastnost $ln^O[p, k+1]$. Potom prvky $x_0, \ldots, x_{m-1}, py_0, \ldots, py_{n-1}$ mají vlastnost $ln^O[p,k]$.

Nechť prvky $x_0, \ldots, x_{m-1}$ mají vlastnost $ln_S^O[p;k]$ a prvky $y_0, \ldots, y_{n-1}$ mají vlastnost $ln_S[p,k+1]$. Potom prvky $x_0, \ldots, x_{m-1}, py_0, \ldots, py_{n-1}$ mají vlastnost $ln_S[p,k]$.

Pro každé G, prvočíslo p a celé číslo k platí:

$$\begin{aligned} \dim^O[p;k](G) &= \dim^O[p;k+1] + \dim_S^O[p;k] \\ \dim_S[p;k](G) &= \dim_S[p;k+1] + \dim_S^O[p;k] \end{aligned}$$

9. Definice Pro všechna prvočísla p a celá čísla n, k uvažujme následující logické funkce, jejichž definčním oborem je $\mathcal{AG}$:

- $\mathsf{N}[d;n](G)$ je pravdivá pravdivá, právě tehdy když je v dG alespoň n různých prvků.
- $\mathsf{N}^{\mathsf{O}}[p,k;n](G)$ je pravdivá, právě tehdy když je v $\mathrm{ord}[p^k](p^{k-1}G)$ alespoň n rozdílných prvků.
- $\mathsf{N}_{\mathsf{S}}[p,k;n](G)$ je pravdivá, právě tehdy když je v $(p^{k-1}G)$ alespoň n prvků po dvou inkongruentních modulo p^k.
- $\mathsf{N}_{\mathsf{S}}^{\mathsf{O}}[p,k;n](G)$ je pravdivá, právě tehdy když je v $\mathrm{ord}[p^k](p^{k-1}G)$ alespoň n prvků po dvou inkongruentních modulo p^k.

◇ Množinu všech těchto funkcí označme **S'** a říkejme jí množina prvotních sentencí.

Pojem *logické funkce* jsem převzal od A. Tarského, záhy si ukážeme, jak tyto *logické funkce* vyjádřit pomocí korektně definovaných formulí, a tak tento pojem ponechávám v intuitivní rovině. Koho by to jakkoli znepokojovalo, ať, prosím, považuje následující lemma za korektní matematickou definici.

10. Lemma Ke každé logické funkci f z $\mathbf{S}'$ můžeme najít sentenci $\varphi \in (\frac{\mathsf{Fm}}{+})^\bullet$, tak, že $\mathfrak{M}^+_{AG}(\varphi) = \{G \in \mathcal{AG}; f(G) \text{ je pravdivá}\}$ (tedy sentence φ platí právě v těch grupách, pro které je f pravdivá). Dále již nebudeme rozlišovat, zda je φ logická funkce nebo formule.

Důkaz:

$$\mathsf{N}[d;n] \equiv \exists v_0,\ldots,v_{n-1}: \quad \begin{array}{llll} (dv_0 \neq dv_1) \wedge & \cdots & \wedge (dv_0 \neq dv_{n-1}) \\ & \ddots & \vdots \\ & & \wedge (dv_{n-1} \neq dv_{n-1}) \end{array}$$

$$\mathsf{N}_\mathsf{S}[p,k;n] \equiv \exists v_0,\ldots,v_{n-1}: \quad \begin{array}{llll} (p^k v_0 = 0) \wedge & \cdots & \wedge (p^k v_{n-1} = 0) \\ (p^{k-1}v_0 \neq p^{k-1}v_1) \wedge & \cdots & \wedge (p^{k-1}v_0) \neq (p^{k-1}v_{n-1}) \\ & \ddots & \vdots \\ & & \wedge (p^{k-1}v_{n-1} \neq p^{k-1}v_{n-1}) \end{array}$$

Podobně se postupuje v konstrukci N_S a $\mathsf{N}^\mathsf{O}_\mathsf{S}$, akorát se místo testování nerovnosti prvků musí provést testování na nekongruenci modulo d:

$$\forall v_n,\ldots,v_{n(n+1)/2}: \quad \begin{array}{llll} (v_o - v_1 \neq dv_n) \wedge & \cdots & \wedge (v_o - v_{n-1} \neq dv_{2n-1}) \\ & \ddots & \vdots \\ & & \wedge (v_{n-2} - v_{n-1} \neq dv_{n(n+1)/2}) \end{array}$$

□

Ukážeme, že každou sentenci o abelovských grupách lze ekvivalentně zapsat jako booleovskou kombinaci formulí z $\mathbf{S}'$. Ovšem tato množina není pro naše účely ještě dostatečně čitelná — zlobí formule typu $\mathsf{N}[d;n]$ — a tak si s ní v kapitole IV. budeme ještě chvíli hrát.

11. Definice Pro p prvočíslo, l,k nezáporná, a celá čísla $a_0,\ldots,a_{m-1}$ zaveďme formule:

- *Rovnostní formule*

$$\mathsf{E}[a_0,\ldots,a_{m-1}] \equiv (a_0v_o + \cdots + a_{m-1}v_{m-1} = 0)$$

- *Divizibilní formule (modulo p^l)*

$$\mathsf{C}[p^l;a_0,\ldots,a_{m-1}] \equiv (\exists v_m)(p^l v_m = a_0v_o + \cdots + a_{m-1}v_{m-1})$$

- Jako *základní množina formulí* pojmenujme množinu:

$\mathbf{B} = \mathbf{S}' \cup \{\varphi;\ \varphi$ je rovnostní f. nebo φ je divizibilní f. a a_0 je mocnina prvočísla$\}$

Dále, pro lepší optickou přehlednost dlouhých formulí, si označíme:

- *Nerovnostní formule*

$$\star\mathsf{E}[a_0,\ldots,a_{m-1}] \equiv \neg\mathsf{E}[a_0,\ldots,a_{m-1}]$$

- *Nedivizibilní formule*

$$\star \mathsf{C}[n; a_0, \ldots, a_{m-1}] \equiv \neg \mathsf{C}[n; a_0, \ldots, a_{m-1}]$$

12. Věta Množina formulí **B** splňuje podmínky lemmatu 5 a tudíž se jedná o základní množinu formulí $\mathcal{AG}$. Navíc množina S' je množina základních sentencí $\mathcal{AG}$.

Důkaz: Ověříme jednotlivé předpoklady lemmatu 5. i. Platí triviálně, ii. stačí vzít rovnostní formuli a vektor, který má na i-té pozici jedničku a na k-té pozici minus jedničku nebo ještě navíc na j-té pozici jedničku, iii. důkaz bude obsahem následující kapitoly. Jako bonus dostaneme i dodatek o prvotní množině sentencí. □

III. Ubití malého kvantifikátoru.

Nejprve začněme u značení. Písmenka a, a_i, a_{ij}, b, b_i, b_{ij} budou v celé kapitole zastupovat celá čísla a automaticky budeme předpokládat, že $\bar{\boldsymbol{a}} = (a_0, \ldots, a_{k-1})$, $\bar{\boldsymbol{a}}_i = (a_{i1}, \ldots, a_{i,k-1})$, obdobně pro $\bar{\boldsymbol{b}}$ nebo $\bar{\boldsymbol{b}}_i$. Analogicky bude $\bar{\boldsymbol{v}} = (v_o, \ldots)$ bude značit nekonečný (či raději libovolně dlouhý) vektor algebraických proměnných. Ve speciálních případech (viz. definice níže) bude $\bar{\boldsymbol{x}} = (x_0, \ldots, x_k)$, $\bar{\boldsymbol{y}} = (y_0, \ldots, y_k)$, $x_i, y_i \in G \in \mathcal{AG}$ atp. označovat výběr konkrétních prvků z předem zvolené grupy, vše by mělo býti jasné z kontextu. $\ell\bar{\boldsymbol{a}}$ nechť značí počet prvků vektoru $\bar{\boldsymbol{a}}$. S vektory budeme provádět běžné početní operace, jako sčítání nebo odčítání $\bar{\boldsymbol{a}} \pm \bar{\boldsymbol{b}} = (a_0 \pm b_0, \ldots, a_{k-1} \pm b_{k-1})$, kde $k = \max(\ell\bar{\boldsymbol{a}}, \ell\bar{\boldsymbol{b}})$ s tím, že zbylé pozice kratšího vektoru nastavíme nulami. Násobení skalárem $n \in \mathbb{Z}$, je rovněž dobře známé — pro $n \in \mathbb{Z}$ ho definujeme jako $n\bar{\boldsymbol{a}} = (na_0, \ldots, na_{\ell\bar{\boldsymbol{a}}-1})$.

Jako formální skalární součin označíme $\bar{\boldsymbol{a}}\bar{\boldsymbol{v}} = \sum_{i<\ell\bar{\boldsymbol{a}}} a_i v_i$, tedy term jazyka $\frac{\mathsf{Fm}}{+}$. Pro $\bar{\boldsymbol{a}}$ budeme $\bar{\boldsymbol{a}}'$ značit $(a_1, \ldots, a_k)$, jedná se tedy o původní vektor ochuzený o první člen, důležité přitom je, že indexování prvků v $\bar{\boldsymbol{a}}'$ začíná od jedničky. Původní vektor $\bar{\boldsymbol{a}}$ potom budeme občas zapisovat jako $\bar{\boldsymbol{a}} = a_0|\bar{\boldsymbol{a}}'$.

Relaci $\equiv$ jsme zatím používali výhradně, pokuď jsme chtěli přiřadit nějaké formuli její název. Z matematického hlediska je to znak pro dosazení formule do formulové proměnné. Jelikož jsme ale žádné formulové proměnné nezaváděli, interpretovali jsme doposud $\equiv$ jako výraz matematického metajazyka. Dále ovšem budeme potřebovat nástroj na jemnější porovnávání formulí v rámci $\frac{\mathsf{Fm}}{+}$, než byla doposud užívaná $\sim$, jejíž význam je zejména porovnávání uzavřených formulí. K tomuto účelu naložíme $\equiv$ korektní matematický význam, který nebude v rozporu s jejím dřívějším používáním.

13. Definice Pokud maximální index volné proměnné v otevřené formuli $\varphi \in \frac{\mathsf{Fm}}{+}$ je k (tedy pro všechna $i > k$ je v_i buď vázaná proměnná a nebo se ve formuli φ vůbec nevyskytuje), pak tuto formuli můžeme proměnit v sentenci tak, že si zvolíme nějakou algebru $A \in \mathcal{A}$ a nějaký $\bar{\boldsymbol{x}} \in {}^kA$ a do formule φ dosadíme x_i za v_i pro každou v_i volnou proměnnou ve φ. Pokud jsou splněny všechny výše psané podmínky, stručně říkáme, že vektor $\bar{\boldsymbol{x}}$ můžeme dosadit do φ a tuto okolnost vyznačujeme $\varphi(\bar{\boldsymbol{x}}/\bar{\boldsymbol{v}})$.

Řekneme, že formule φ je $\mathcal{AG}$-podřízená formuli ψ, značíme $\varphi \ll_{\mathcal{AG}} \psi$ pokud pro každou $G \in \mathcal{AG}$ platí: Můžeme-li vektor $\bar{\boldsymbol{x}} \in {}^kG$ dosadit do φ a vznikne-li nám takto pravdivá sentence, potom můžeme rovněž $\bar{\boldsymbol{x}}$ dosadit do ψ a vzniklá formule bude rovněž pravdivá.

Konečně řekneme, že formule φ, $\psi \in \frac{\mathsf{Fm}}{+}$ jsou $\mathcal{AG}$-identické, nebo prostě

jen identické, což značíme $\varphi \equiv \psi$, pokud $\varphi \ll_{\mathcal{AG}} \psi$ a $\psi \ll_{\mathcal{AG}} \varphi$.

Pokoud v definicích výše zaměníme "pro každou abelovskou grupu $G \in \mathcal{AG}$" za "pro každou algebru $A \in \mathcal{A}$", dostaneme definici (univerzální) podřízenosti a univerzální identity.

Často budeme používat rozbor formule φ podle možností $\gamma \in \frac{\mathsf{Fm}}{+}$, a to následujícím způsobem:

$$\text{Pro } \varphi \in \mathbf{B} \text{ budeme chtít ukázat, že } \exists v_0\, \varphi \in \mathbf{B}$$

k čemuž nám stačí, že:

$$\exists v_0\, \varphi \wedge \gamma \ \in \mathrm{bool}(\mathbf{B}) \text{ a zároveň } \exists v_0\, \varphi \wedge (\neg\gamma) \in \mathrm{bool}(\mathbf{B}).$$

Rozbor podle možností $\gamma_0, \ldots, \gamma_{n-1}$ potom bude znamenat, že:

$$\exists v_0\, \varphi \wedge \bigwedge_{i<n} \gamma^{r(i)} \in \mathrm{bool}(\mathbf{B}) \quad \text{pro každé} \quad r \in {}^2n, \text{ kde } \begin{matrix} \gamma^0 \equiv \neg\gamma \\ \gamma^1 \equiv \gamma \end{matrix}$$

14. Definice Ještě nadefinujme dva typy formulí. Zavádíme pro ně speciální označení, protože rozbor možností budeme provádět především podle nich a už v této větě bych ocenil, kdybych je mohl pojmenovat určitěji než jen „nich". Podmínka *dělitelnosti* $\mathrm{div}[a_0|\bar{\boldsymbol{a}}] \equiv (\exists v_0)(a_0 v_0 = \bar{\boldsymbol{a}}'\bar{\boldsymbol{v}}')$, pro $a_0 \neq 0$. $\mathrm{div}[\bar{\boldsymbol{a}}] \in \mathrm{bool}(\mathbf{B})$ — máme-li $0 \neq a_0 = \prod_{i<m} p_i^{k_i}$ prvočíselný rozklad a_0, tak

$$\mathrm{div}[\bar{\boldsymbol{a}}] \equiv \exists v_0\, \mathsf{E}[a_0|\bar{\boldsymbol{a}}'] \equiv \bigwedge_{i<m} \mathsf{C}[p_i^{k_i}; 0|\bar{\boldsymbol{a}}],$$

přičemž při $a_0 = 1$ považujeme prázdnou konjunkci za tautologii teorie grup. Užitečnost podmínky div tkví v tom, že její první proměnná je vázaná a tudíž ji lze při eliminaci vytknout před kvantifikátor.

Dále uvažujme funkci *vektorové nezávislosti* $\mathrm{nez}[\bar{\boldsymbol{a}}_0, \ldots, \bar{\boldsymbol{a}}_{m-1}]$, které klademe jako parametr libovolné konečné množství vektorů. Dosazením $\mathrm{nez}(\bar{\boldsymbol{x}}/\bar{\boldsymbol{v}})$ dostaneme pravdivou sentenci právě když $\bar{\boldsymbol{a}}_i\bar{\boldsymbol{x}} \neq \bar{\boldsymbol{a}}_j\bar{\boldsymbol{x}}$ pro $i < j < m$. Snadno nahlédneme, že:

$$\mathrm{nez}[\bar{\boldsymbol{a}}_1, \ldots, \bar{\boldsymbol{a}}_k] \equiv \bigwedge_{i<j\leq k} \star\mathsf{E}(\bar{\boldsymbol{a}}_i - \bar{\boldsymbol{a}}_j)$$

Podmínka existence soustavy nerovnic

15. Lemma Mějme vektory $\bar{a}_0, \bar{a}_1$ a $d = \mathrm{NsD}(a_{00}, a_{10})$. Potom umíme najít posloupnosti $\bar{b}', \bar{b}'_0, \bar{b}'_1$, že:

$$\mathsf{E}[\,\bar{a}_0\,] \wedge \mathsf{E}[\,\bar{a}_1\,] \equiv \mathsf{E}[\,d|\bar{b}'\,] \wedge \mathsf{E}[\,0|\bar{b}'_0\,] \wedge \mathsf{E}[\,0|\bar{b}'_1\,]$$

$$\mathsf{E}[\,\bar{a}_0\,] \wedge \star\mathsf{E}[\,\bar{a}_1\,] \equiv \big(\mathsf{E}[\,d|\bar{b}'\,] \wedge \star\mathsf{E}[\,0|\bar{b}'_0\,] \wedge \mathsf{E}[\,0|\bar{b}'_1\,]\big) \vee \big(\mathsf{E}[\,\bar{a}_0\,] \wedge \star\mathsf{E}[\,d|\bar{b}'\,]$$

Důkaz: Pro nějaká celá čísla s, s' platí $sa_{00} + s'a_{10} = d$. Dosadíme-li

$$\bar{b}' = s\bar{a}'_0 + s'\bar{a}'_1,\ \bar{b}'_0 = s\bar{b}'_3,\ \bar{b}'_1 = s'\bar{b}'_3,$$

kde $\bar{b}'_3$ zastupuje výraz $\left(\frac{a_{00}}{d}\bar{a}'_0 - \frac{a_{10}}{d}\bar{a}'_1\right)$. □

16. Lemma Pro každé $\bar{a}$ platí:

$$(\,\exists v_o\,\mathsf{E}[\,a_0|\bar{a}'\,]\,) \in \mathrm{bool}(\mathbf{B}) \tag{2}$$

Důkaz: Pro $a_0 = 0$ snadno sestrojíme ekvivalentní formuli, ve které v_o není volná, pokud $a_0 \neq 0$ tak jde o funkci $\mathrm{div}[\,\bar{a}\,]$. □

17. Lemma Pro $m \in \omega$ a libovolné vektory $\bar{a}'_i$, $i < m$ platí:

$$\left(\exists v_o \bigwedge_{i<m} \mathsf{E}[\,a_0|\bar{a}'_i\,]\right) \in \mathrm{bool}(\mathbf{B}) \tag{3}$$

Důkaz: Pro $a_0 = 0$ stejné jako výše, pro $a_0 \neq 0$ máme

$$\exists v_o \bigwedge_{i<m} \mathsf{E}[\,a_0|\bar{a}'_i\,] \equiv (\mathrm{div}[\,\bar{a}_0\,]) \wedge \Big(\bigwedge_{0<i<m} \mathsf{E}[\,0|(\bar{a}'_i - \bar{a}'_0)]\Big)$$

□

18. Lemma Pro jakékoli $m \in \omega$ a vektory $\bar{a}', \bar{a}_1, \ldots, \bar{a}_{m-1}$ platí:

$$\left(\exists v_o\,\mathsf{E}[\,1|\bar{a}'\,] \wedge \bigwedge_{i<m} \star\mathsf{E}[\,\bar{a}_i\,]\right) \in \mathrm{bool}(\mathbf{B}) \tag{4}$$

Důkaz: Odečteme výraz $a_{i0}\bar{a}'\bar{v}'$ od každé z nerovnic $\star\mathsf{E}[\,\bar{a}_i\,]$, čímž dostaneme:

$$\left(\exists v_0\,\mathsf{E}[\,1|\bar{a}'\,] \wedge \bigwedge_{i<m} \star\mathsf{E}[\,\bar{a}_i\,]\right) \equiv (\,\mathrm{nez}[\,0|(\bar{a}'_i - a_{i0}\bar{a}');\ i < m\,] \wedge (\mathrm{div}[\,1|\bar{a}'\,])\,), \tag{5}$$

a tento případ řeší (2). □

19. Lemma Pro $m, a_0 \in \omega$ a vektory $\bar{\boldsymbol{a}}'$, $\bar{\boldsymbol{a}}'_1, \ldots, \bar{\boldsymbol{a}}'_{m-1}$ platí:

$$\exists v_o \left(\mathsf{E}[\, a_0 | \bar{\boldsymbol{a}}' \,] \wedge \bigwedge_{i<m} [a_0 | \bar{\boldsymbol{a}}'_i \,] \right) \in \mathrm{bool}(\mathbf{B}). \tag{6}$$

Důkaz: Podobnou úpravou jako v minulém lemmatu dostaneme:

$$\exists v_o \left(\mathsf{E}[\, a_0 | \bar{\boldsymbol{a}}' \,] \wedge \bigwedge_{i<m} [a_0 | \bar{\boldsymbol{a}}'_i \,] \right) \equiv \left(\mathrm{nez}[\, (\bar{\boldsymbol{a}}'_i - \bar{\boldsymbol{a}}');\ i < m \,] \wedge \mathrm{div}[\, \bar{\boldsymbol{a}} \,] \right),$$

□

20. Věta Pro $m \in \omega$ a vektory $\bar{\boldsymbol{a}}'_i$, $i < m$ platí:

$$\text{Je-li} \quad \varphi \equiv \bigwedge_{i<m} (\neg \mathsf{E}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]), \qquad \text{tak potom} \qquad \exists v_0\, \varphi \in \mathrm{bool}(\mathbf{B}).$$

Důkaz: Pro $a_0 = 0$ zřejmé, předpokládejme tedy $a_0 \neq 0$. Nyní rozebereme jednotlivé případy podle formulí $\mathrm{div}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]$, $i < m$ a využijeme toho, že:

$$(\neg \mathrm{div}[\, \bar{\boldsymbol{a}}_i \,]) \text{ implikuje } (\exists v_0)(\star \mathsf{E}[\, \bar{\boldsymbol{a}}_i \,]) \tag{7}$$

Pro všechny $K \subseteq m$ dostáváme:

$$\xi_K \equiv \bigwedge_{i \in K} \left((\star \mathsf{E}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]) \wedge (\mathrm{div}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]) \right) \wedge \bigwedge_{i \in m-K} \left((\star \mathsf{E}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]) \wedge (\neg \mathrm{div}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]) \right)$$

Podle (7) máme:

$$(\exists v_0\, \xi_K) \equiv \left(\bigwedge_{i \in m-K} \neg \mathrm{div}[\bar{\boldsymbol{a}}_i] \right) \wedge \left(\exists v_0 \bigwedge_{i \in K} (\star \mathsf{E}[\, a_0 | \bar{\boldsymbol{a}}'_i \,] \wedge \mathrm{div}[\, a_0 | \bar{\boldsymbol{a}}'_i \,]) \right).$$

Čili pro $\xi_\emptyset$ jsme již kvantfikátor eliminovali. Dále rozeberme pro neprázdné K každé ξ_K na jednotlivé případy podle formulí $\mathsf{E}[0 | (\bar{\boldsymbol{a}}'_i - \bar{\boldsymbol{a}}'_j)]$ $j, i \in K$, $j < i$. Ovšem $\mathsf{E}[\, 0 | (\bar{\boldsymbol{a}}'_i - \bar{\boldsymbol{a}}'_j) \,] \equiv (\bar{\boldsymbol{a}}'_i = \bar{\boldsymbol{a}}'_j)$ což znamená, že $\xi_K \wedge \mathsf{E}[0 | (\bar{\boldsymbol{a}}'_i - \bar{\boldsymbol{a}}'_j)] \equiv \xi_{K-i}$ a tudíž nám stačí uvažovat formule

$$\xi_K \wedge \mathrm{nez}[\, \bar{\boldsymbol{a}}'_i;\ i \in K \,] \quad \text{pro } K \neq \emptyset.$$

Ukážeme, že v takovémto případě

$$\exists v_0\, \xi_K \equiv \mathsf{N}[\, a_0; |K| + 1 \,] \wedge \mathrm{nez}[\, \bar{\boldsymbol{a}}'_i;\ i \in K \,] \wedge \bigwedge_{i \in K} \mathrm{div}[\, a_0 | \bar{\boldsymbol{a}}_i \,] \tag{8}$$

Označme si pravou stranu v (8) jako ζ_K.

Zvolme si vektor $\bar{x}'$ z jisté, vlastně libovolné grupy $G \in \mathcal{AG}$, který můžeme dosadit do ζ_K tak, aby vznikla pravdivá sentence. Z toho ovšem plyne, že $\mathsf{N}[a_0; |K|+1]$ je pravdivá sentence o grupě G, čili se v této grupě nalézá alespoň $|K|+1$ prvků, které jsou dělitelné a_0, čili z Dirchletova principu holubníku vždy alespoň jeden prvek bude splňovat každou z $|K|$ nerovností určených ve ξ_K, neboli platí $\exists v_0\, \xi_K$. Čili máme $\zeta_K \ll_{\mathcal{AG}} \xi_K$.

Naopak v grupě G zvolme vektor $\bar{x}$, který lze dosadit do $\exists v_0\, \xi_K$ tak, aby vzniklá sentence byla pravdivá. Potom ovšem existuje v grupě G prvek, který je dělitelný a_0 (podle podmínky *div*) a přitom nesplňuje každou z $|K|$ nerovnic v ξ_K. Označíme-li $y_i = \bar{a}_i\bar{x}$ bude každý z těchto bodů dělitelný a_0 a přitom podle podmínky *nez* budou navzájem různé. Tedy grupa a_0G má alespoň $|K|+1$ navzájem různých prvků a tedy v G platí $\mathsf{N}[a_0; |K|+1]$, čili $\xi_K \ll_{\mathcal{AG}} \zeta_K$.

Máme tedy $\xi_K \equiv \zeta_K$ pro $\emptyset \neq K \subseteq m$, a tedy i $\xi_K \in \mathrm{bool}(\mathbf{B})$. Důkaz jsme provedli důkladně, dále budeme postupovat rychleji. □

21. Věta Pro $m \in \omega$, prvočíslo p a vektory $\bar{a}'_i$, $i < m$ platí:

$$\text{Je-li} \quad \varphi \equiv \bigwedge_{i<m} \big(\star\mathsf{E}[\,a|\bar{a}'_i\,] \wedge \mathsf{E}[\,pa|p\bar{a}'_i\,]\big), \quad \text{potom} \quad \exists v_0\, \varphi \in \mathrm{bool}(\mathbf{B}).$$

Důkaz: Pro $a = 0$ zřejmé, nechť $a \neq 0$. Rozebereme jednotlivé případy podle podmínek $\mathrm{div}[\,a_0|\bar{a}'_i\,]$, $i < m$ a zároveň podle podmínek $\star\mathsf{E}[\,0|(\bar{a}'_i - \bar{a}'_j)\,]$, $i < j \leq m$, přitom v případě, kdy nastane $(\neg\mathrm{div}[\,a|\bar{a}'_i\,])$ tak se nám podle (7) převede případ pro dané i na případ (3). Zbývá nám tedy vyšetřit formule:

$$\xi_K \equiv \mathrm{nez}[\,\bar{a}'_i;\, i \in K\,] \wedge \Big(\bigwedge_{i\in K} \mathrm{div}[a|\bar{a}'_i\,]\Big) \wedge \Big(\bigwedge_{i\in K} (\star\mathsf{E}[\,a|\bar{a}'_i\,] \wedge \mathsf{E}[\,pa|p\bar{a}'_i\,])\Big),$$

pro $\emptyset \neq K \in m$. Ať $a = p^l r$ a $\mathrm{nsn}(p, r) = 1$. $\mathrm{div}[\,a_0|\bar{a}'_i\,] \equiv \mathrm{div}[\,p^l|\bar{a}'_i\,] \wedge \mathrm{div}[\,r|\bar{a}'_i\,]$

Dále $\mathrm{div}[\,r|pa\,] \wedge \mathsf{E}[\,pa|p\bar{a}'_i\,] \ll_{\mathcal{AG}} \mathrm{div}[\,r|\bar{a}'_i\,]$. Jelikož $\mathrm{div}[\,r|pa\,]$ je $T_{\mathcal{AG}}$-tautologie můžeme psát:

$$\xi_K \equiv \mathrm{nez}[\,\bar{a}'_i;\, i \in K\,] \wedge \Big(\bigwedge_{i\in K} \mathrm{div}[\,p^l|\bar{a}'_i\,]\Big) \wedge \Big(\bigwedge_{i\in K} (\star\mathsf{E}[\,a|\bar{a}'_i\,] \wedge \mathsf{E}[\,pa|p\bar{a}'_i\,])\Big).$$

k dokončení důkazu zbývá nahlédnout, že:

$$\exists v_0\, \xi_K \equiv \mathsf{N}^{\mathsf{O}}[\,p, l+1; |K|+1\,] \wedge \Big(\textstyle\bigwedge_{i\in K} \mathrm{div}[\,p^l|\bar{a}'_i\,]\Big) \wedge$$
$$\wedge \Big(\textstyle\bigwedge_{i\in K} \mathsf{E}[\,pa|p\bar{a}'_i\,]\Big) \wedge \mathrm{nez}[\,\bar{a}'_i;\, i \in K\,], \qquad (9)$$

kde pravá strana je již booleovskou kombinací základních funkcí.

Najdeme $\bar{x}$, který lze dosadit do LS na pravdivou sentenci. A tedy existují v G prvky $w_0, \ldots, w_{|K|}$ mající vlastnost $\widetilde{\mathsf{ln}[\mathsf{p};\mathsf{l}+1]}$. Tudíž alespoň jeden z prvků $x_0 + p^l w_i$ vyhovuje každé z nerovnic. Tedy LS $\ll_{\mathcal{AG}} \exists v_o \xi_K$.

Naopak předpokládejme, že pro pevně zvolenou grupu G a pevně zvolený vektor $\bar{x}'$ platí LS v (9), tedy existuje x_0, že $\varphi((x_0|\bar{x})/\bar{v})$ je pravdivá. Zvolme si prvky g_i tak, aby $p^l g_i = \bar{a}_i' \bar{x}' - a x_0$, (existenci zaručuje podmínka div_i), tak z podmínky $\star\mathsf{E}_i$ plyne $p^l g \neq 0$ a z podmínky E_i plyne $p^{l+1} = 0$, což zajišťuje existenci $|K|+1$ různých (podmínka *nez*) prvků a splnění podmínky $\mathsf{N}^{\mathsf{O}}[p, l+1; |K|+1]$. Tedy ξ_K je podřízená pravé straně (9).

□

22. Lemma Nechť $m \in \omega$, a $\bar{a}_i, i < m$ vektory takové, že $0 \neq a_{00} = \cdots = a_{m-1,0} = a$ a $p_1, \ldots, p_{m-1}$ nechť jsou prvočíselní dělitelé čísla a, které nemusí být různé. Potom pokud

$$\varphi \equiv \bigwedge_{i<m} \left(\star\mathsf{E}\left[\frac{a}{p_i} \,\middle|\, \bar{a}_i' \right] \wedge \mathsf{E}[\, a | p_i \bar{a}_i'] \right), \qquad \text{tak platí } \exists v_0\, \varphi \in \mathrm{bool}(\mathbf{B}). \tag{10}$$

Důkaz: Označme s počet různých prvočísel mezi $p_0, \ldots, p_{m-1}$. Důkaz povedeme indukcí podle s. Případ $s = 1$ jsme probírali v minulém lemmatu, tvrzení teda platí. Předpokládejme dále, že tvrzení už je dokázané pro $s-1$. Pro přehlednost si přeoznačme prvočísla tak, aby $p_0 = \ldots = p_{t-1} \neq p_i$ pro $t \leq \imath < m$. Dále si najdeme algebraickou proměnnou v_k, která nemá výskyt v φ a vektory $\bar{a}_0, \ldots \bar{a}_{t-1}$ upravíme na vektory $\bar{b}_0', \bar{b}_0, \ldots, \bar{b}_{t-1}$ tak, že $b_{i0} = 0$ a $b_{ik} = \frac{a}{p_0}$, zkrátka jsme zaměnili proměnnou v_0 za v_k. Potom platí:

$$\begin{aligned} \exists v_o\, \varphi &\equiv (\exists v_o, v_k) \textstyle\bigwedge_{i<t} (\star\mathsf{E}[\, \bar{b}_i \,] \wedge \mathsf{E}[\, p_0 \bar{b} \,]) \\ &\wedge \textstyle\bigwedge_{t \leq i < m} (\star\mathsf{E}[a/p_i | p_i \bar{a}_i' \,] \wedge \mathsf{E}[\, a | \bar{a}_i' \,] \wedge (v_0 = v_k) \\ &\overset{*}{\equiv} \left(\exists v_k \textstyle\bigwedge_{i<t} (\star\mathsf{E}[\, \bar{b}_i \,] \wedge \mathsf{E}[\, p_0 \bar{b} \,]) \right) \wedge (\mathsf{E}[\, 0 | (p_t \bar{a}_t' - p_0 \bar{b}_0') \,] \\ &\wedge \left(\exists v_o \textstyle\bigwedge_{t \leq i < m} (\star\mathsf{E}[a/p_i | \bar{a}_i' \,] \wedge \mathsf{E}[\, a | p_i \bar{a}_i' \,]) \right) \end{aligned} \tag{11}$$

Přičemž u obou členů (11) již umíme kvantifikátor odstranit podle indukčního předpokladu. Zbývá tedy řádně zdůvodnit $(*)$. Nahradili jsme zde totiž podmínkou $v_o = v_k$ slabší podmínkou $a v_o = a v_k$, takže pro prvek x_0, který dosadíme za v_o do (11) by některá z podmínek $\star\mathsf{E}_i$ nemusila platit, což by přímo ohrožovalo předpokládanou existenci v_o ve φ. Použijeme ovšem tento záchranný trik: Ať $a = p_0^k r$, kde jsou p_0, r nesoudělná. Můžeme najít celá čísla s, s' tak, že $s p_0^k + s' r = 1$.

Vezmeme-li prvek $x = s'x_0 + sx_k$, (kde x_0 a x_k jsou prvky, které existují, pokud je pravdivá (11) po dosazení $\bar{x}$ za $\bar{v_0}$) tak, x je prvek, splňující každou z podmínek $\mathsf{E}_{i,i}$. Tedy $\exists v_0\, \varphi \ll_{\mathcal{AG}} (11)$. Opačná podřízenost je obecná zákonitost predikátové logiky. □

23. Lemma Ponechme značení u $m, a, p_i, \bar{\boldsymbol{a}}_i$, a φ z předešlého lemmatu. Nechť navíc $n \in \omega$ a $\bar{\boldsymbol{b}}, \bar{\boldsymbol{b}}_0, \ldots, \bar{\boldsymbol{b}}_{n-1}$ jsou vektory, pro které platí $b_0 = b_{00} = \cdots = b_{n-1,0} = a\,(= a_{i0})$. Pokud

$$\varphi_1 \equiv \mathsf{E}[\bar{\boldsymbol{b}}] \wedge \varphi, \tag{12}$$

$$\varphi_2 \equiv \mathsf{E}[\bar{\boldsymbol{b}}] \wedge \varphi \wedge \bigwedge_{i<n} \star\mathsf{E}[\bar{\boldsymbol{b}}_i], \tag{13}$$

$$\varphi_3 \equiv \mathsf{E}[\bar{\boldsymbol{b}}] \wedge \bigwedge_{i<m} \star\mathsf{E}[a/p_i|\bar{\boldsymbol{a}}'_i], \tag{14}$$

$$\varphi_4 \equiv \mathsf{E}[\bar{\boldsymbol{b}}] \wedge \bigwedge_{i<m} \star\mathsf{E}[a/p_i|\bar{\boldsymbol{a}}'_i] \wedge \bigwedge_{i<n} \mathsf{E}[\bar{\boldsymbol{b}}'_i], \tag{15}$$

potom platí $\exists v_o\, \varphi_k \in \mathrm{bool}(\mathbf{B})$ pro $k = 1, 2, 3, 4$.

Důkaz: Pro φ_1, φ_2 stačí dosadit obdobně jako v (6). U φ_3, φ_4 použijeme rozbor podle možností $\mathsf{E}[a|p_i\bar{\boldsymbol{a}}]$. □

24. Lemma Pro $m \in \omega$ a vektory $\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}_0, \ldots, \bar{\boldsymbol{a}}_{m-1}$ kde $a_{i0}, a_0 > 0$ platí:

$$\varphi \equiv \mathsf{E}[\bar{\boldsymbol{a}}] \wedge \bigwedge_{i<m} \star\mathsf{E}[\bar{\boldsymbol{a}}_i] \qquad \exists v_o \varphi \in \mathrm{bool}(\mathbf{B}). \tag{16}$$

Důkaz: Toto lemma se liší od všech dřívějších lemmat především tím, že jsme se konečně osmělili a předpokládáme, že a_{i0} a a_0 jsou zcela libovolné. Důkaz však přece přese všechno provedeme diskusí *všech* možných případů vztahu a_0 vůči a_{i0}. Nejprve každé formuli, která má tvar jako (16) přiřadíme tyto parametry, podle kterých budeme postupně provádět vnořenou indukci:

- Jako α_φ označíme a_0,
- jako β_φ označíme $|D| = |\{i,\ i < m$ a a_{i0} nedělí $a_0\}|$,
- jako γ_φ označíme $\max_{i<m} c_i$, kde $c_i = 0$, pokud $i \in D$ a c_i nechť vyznačuje počet všech (ne nutně rozdílných) členů prvočíselného rozkladu $\frac{a_0}{a_{i0}}$ pokud $i \notin D$ (přitom 1 považujeme za součin *nula* prvočísel),

- jako δ_φ označíme počet takových c_i, že $c_i = \gamma_\varphi$, neboli počet kolikrát se maxima nabývá.

Pokuď $\alpha_\varphi = 1$, má formule tvar (5), ve kterém již umíme kvantifikátor eliminovat. Předpokládejme tedy, že $\alpha_\varphi > 1$ a pro všechny formule ξ tvaru (16), u kterých je $\alpha_\xi < \alpha_\varphi$ lemma platí.

Uvažme nejprve, že $\beta_\varphi = 0$. Potom každé a_{i0} je dělitelem a_0. Pokud $\gamma_\varphi = 0$ tak má formule tvar (6). Pokud $\gamma_\varphi = 1$ znamená to, že pro každé i je $a_{i0} = \frac{a_0}{p}$, kde p je buď prvočíslo nebo jednička a φ je tudíž tvaru, který jsme probírali v (14) nebo (15). Dále tedy předpokládejme, že $\gamma_\varphi > 1$ a pro jakoukoli formuli ξ, která má tvar (16) a splňuje $\alpha_\xi = \alpha_\varphi$, $\beta_\xi = 0$, $\gamma_\xi < \gamma_\varphi$ již máme tvrzení dokázáno. Ať j je index, že $c_j = \gamma_\varphi$ a $a_0 = pa_{j0}r$, kde p prvočíslo a r celé číslo různé od 1. Nyní formuli rozebereme podle případu $\mathsf{E}[p\bar{\boldsymbol{a}}_0]$ a dostaneme tyto možnosti:

$$\xi \equiv \mathsf{E}[\bar{\boldsymbol{a}}] \wedge \mathsf{E}[p\bar{\boldsymbol{a}}_j] \wedge \bigwedge_{i<m} \star\mathsf{E}[\bar{\boldsymbol{a}}_i]$$

$$\zeta \equiv \mathsf{E}[\bar{\boldsymbol{a}}] \wedge \star\mathsf{E}[p\bar{\boldsymbol{a}}_j] \wedge \bigwedge_{\substack{i<m \\ i\neq j}} \star\mathsf{E}[\bar{\boldsymbol{a}}_i]$$

Přitom

$$\xi = \underbrace{\mathsf{E}[0|(\bar{\boldsymbol{a}}' - p_j s\bar{\boldsymbol{a}}'_j)] \wedge \mathsf{E}[p\bar{\boldsymbol{a}}_j] \wedge \bigwedge_{i<m} \star\mathsf{E}[\bar{\boldsymbol{a}}_i]}_{\substack{\text{je tvaru (16)} \\ \text{a má menší } \alpha \text{ než } \varphi}}$$

Dále ζ je tvaru (16) a $\alpha_\zeta = \alpha_\varphi$, $\beta_\zeta = 0$. Pokud $\delta_\varphi = 1$ tak $\gamma_{\xi 2} < \gamma_\varphi$ v opačném případě $\delta_\zeta < \delta_\varphi$.

Dále uvažme, že $\beta_\varphi > 0$ a lemma platí pro všechny formule, pokud je buď jejich α nebo β při stejně veliké α menší než u φ. Najděme tedy takový index j, že a_{j0} nedělí a_0. V případě, že naopak a_0 dělí a_{j0} máme:

$$\xi_1 = \underbrace{\star\mathsf{E}\left[0\,\middle|\left(\bar{\boldsymbol{a}}'_j - \frac{a_{j0}}{a_0}\,\bar{\boldsymbol{a}}'\right)\right] \wedge \mathsf{E}[\bar{\boldsymbol{a}}] \wedge \bigwedge_{\substack{i<m \\ i\neq j}} \star\mathsf{E}[\bar{\boldsymbol{a}}_i]}_{\substack{\text{je tvaru (16)} \\ \text{a má menší } \beta \text{ než } \varphi}}$$

Tak nám zbývá zvážit, co se stane, pokud a_{j0} nedělí a_0. Ať $d = \mathrm{NsD}(a_0, a_{j0})$. Podle lemmatu 15 můžeme efektivně najít $\bar{\boldsymbol{a}}', \bar{\boldsymbol{a}}'_1, \bar{\boldsymbol{a}}'_2$ a použít vzorec:

$$\mathsf{E}[\bar{\boldsymbol{a}}] \wedge \star\mathsf{E}[\bar{\boldsymbol{a}}_j] \equiv \left(\mathsf{E}[d|\bar{\boldsymbol{b}}'] \wedge \star\mathsf{E}[0|\bar{\boldsymbol{b}}'_1] \wedge \mathsf{E}[0|\bar{\boldsymbol{b}}'_2]\right) \vee \left(\mathsf{E}[\bar{\boldsymbol{a}}] \wedge \star\mathsf{E}[d|\bar{\boldsymbol{b}}']\right)$$

Po dosazení do φ:

$$\varphi \equiv \left(\star\mathsf{E}[\,0|\bar{b}'_1\,] \wedge \mathsf{E}[\,0|\bar{b}'_2\,] \wedge \xi\right) \vee \zeta,$$

kde ξ, ζ zastupují:

$$\xi \equiv \mathsf{E}[\,d|\bar{b}'\,] \wedge \bigwedge_{\substack{i<m \\ i\neq j}} \star\mathsf{E}[\,\bar{a}_i\,]; \qquad \zeta \equiv \mathsf{E}[\,\bar{a}\,] \wedge \star\mathsf{E}[\,d|\bar{b}\,] \wedge \bigwedge_{\substack{i<m \\ i\neq j}} \star\mathsf{E}[\,\bar{a}_i\,]$$

Tedy je okamžitě vidět, že $\alpha_\xi < \alpha_\varphi$. Dále pak zjevně $\alpha_\zeta = \alpha_\varphi$ a $\beta_\zeta < \beta_\varphi$. □

25. Věta Pro $m \in \omega$ a $\bar{a}_0, \ldots, \bar{a}_{m-1}$ konečně dostáváme:

$$\exists v_o \bigwedge_{i<m} \star\mathsf{E}[\,\bar{a}_i\,] \in \mathrm{bool}(\mathbf{B}) \tag{17}$$

Důkaz: Nechť $\varphi \equiv \bigwedge_{i<m} \star\mathsf{E}[\,\bar{a}_i\,]$. Můžeme předpokládat, že $a_{i0} > 0$ pro $i < m$. Nejprve si označme $n = \mathrm{Nsn}(a_{00}, \ldots, a_{m-1,0})$ a podobně jako v důkazu předešlého lemmatu budeme postupovat indukcí podle parametrů:

- Označme $\gamma_\varphi := \max_{i<m} c_i$, kde c_i je přesný počet prvočísel tvořících součin $\frac{n}{a_{i0}}$,
- jako δ_φ označme počet, kolikrát se maxima γ nabývá.

Pokud $\gamma_\varphi = 0$ má formule tvar probíraný v (6). Předpokládejme dále, že lemma máme dokázané pro všechny formule ξ, pro které $\gamma_\xi < \gamma_\varphi$. Nechť pro index j platí, že $c_j = \gamma_\varphi$, $n = pa_{j0}r$ pro p prvočíslo a $r > 1$ a rozložme φ na případy podle $\mathsf{E}[\,p\bar{a}_j\,]$:

$$\xi \equiv \mathsf{E}[\,p\bar{a}_j\,] \wedge \bigwedge_{i<m} \mathsf{E}[\,\bar{a}_i\,] \qquad \zeta \equiv \star\mathsf{E}[\,p\bar{a}_j\,] \bigwedge_{\substack{i<m \\ i\neq j}} \star\mathsf{E}[\,\bar{a}_i\,]$$

Případ ξ je předmětem minulého lemmatu; v případě ζ se oproti φ sníží buď α nebo γ. Tím je důkaz hotov. □

Obecný případ

Nyní obrátíme svoji k divizibilním formulím. Písmenka p, $p_0, \ldots, p_m$ zde budou vždy označovat prvočísla a písmenka k, l, n nechť označují celá čísla. V této kapitole budeme používat *dlouhé* vektory $\bar{a}^* \in {}^{\ell\bar{a}+1}\mathbb{Z}$:

$$\bar{a}^*_i = (a_{i*}, a_{i0}, \ldots\, a_{i\ell\bar{a}_i}) = a_{i*}|\bar{a}_i = a_{i*}|a_{i0}|\bar{a}'_i.$$

Dlouhé vekotry jsou vektory prodloužené o jeden prvek a_*, který bude na indexové pozici -1 a budeme dále chápat $\mathsf{E}[\,\bar{a}^*\,] = \mathsf{E}[\,\bar{a}\,]$ a $\mathsf{C}[\,\bar{a}^*\,] = \mathsf{C}[\,a_*; \bar{a}\,]$.

Jediná povolená operace s dlouhým vektorem $\bar{a}^*$ bude násobení skalárem $\bar{a}^* = (na_*, na_0, \ldots, na_{\ell\bar{a}})$, všechny ostatní početní úkony se odehrávají na jeho střední části $\bar{a}$.

26. Definice Pro $k < l$ definujeme komplexní formuli:

$$C'\star C[p^l; p^k|\bar{a}'] = C[p^{l-1}; p^k|\bar{a}'] \wedge \star C[p^l; p^k|\bar{a}']$$

Ve stejném duchu jako podmínku nezávislosti budeme využívat podmínku nesoudělnosti modulo p^k:

$$\mathrm{nes}[p^k; \bar{a}'_0, \ldots, \bar{a}'_{m-1}] \equiv \bigwedge_{i<j<m} \star C[p^k; 0; \bar{a}'_j - \bar{a}'_i]$$

27. Lemma Buďte $l_a \geq l_b > k_b \geq k_a \geq 0$ a $\bar{a}', \bar{b}'$ dva vektory. Potom:

$$C[p^{l_a}; p^{k_a}|\bar{a}'] \wedge C[p^{l_b}, p^{k_b}|\bar{b}'] \equiv C[p^{l_a}; p^{k_a}|\bar{a}'] \wedge C[p^{l_b}; 0|p^{k_b-k_a}(\bar{a}' - \bar{b}')]$$

$C[p^{l_a}; p^{k_a}|\bar{a}'] \wedge \star C[p^{l_b}, p^{k_b}|\bar{b}'] \equiv C[p^{l_a}; p^{k_a}|\bar{a}'] \wedge \star C[p^{l_b}; 0|p^{k_b-k_a}(\bar{a}' - \bar{b}')]$ *Důkaz:* Odečtme $p^{k_b} \equiv p^{k_b-k_a}\bar{a}\bar{v} \pmod{p^{l_b}}$ od vektoru $\bar{b}$. □

28. Lemma Pro vektory $\bar{a}', \bar{b}'$, $k \leq l$ a takové a_0 které není dělitelné p^{k+1}, (tedy uvažujme $a_0 = p^n r$, p a r nesoudělná a $n \leq k$) platí:

$$\begin{aligned} E[\bar{a}] \wedge C[p^l; p^k|\bar{b}'] &\equiv E[\bar{a}] \wedge C[p^l; 0|r\bar{b}' - p^{k-n}\bar{a}'] \\ E[\bar{a}] \wedge \star C[p^l; p^k|\bar{b}'] &\equiv E[\bar{a}] \wedge \star C[p^l; 0|r\bar{b}' - p^{k-n}\bar{a}'] \end{aligned} \tag{18}$$

Důkaz: Zřejmě stačí dosadit do každé formule $-\bar{a}\bar{v}$. □

29. Lemma Pokuď pro celá čísla r, s, k, n platí $kn + rs = 1$ tak pro každý vektor $\bar{a}$ platí:

$$C[n; ra_0|\bar{a}'] \equiv C[n; a_0|s\bar{a};] \tag{19}$$

Důkaz: Ukažme, že $C[n; ra_0|\bar{a}'] \ll_{\mathcal{AG}} C[n; a_0|s\bar{a};]$. Jelikož n a s jsou zjevně nesoudělná, tak $ra_0 \equiv b \pmod n$ implikuje $rsa_0 \equiv sb \pmod n$ implikuje $a_0 \equiv sb \pmod n$, kde za b dosazujeme $-\bar{a}'\bar{x}$. Opačná podmínka plyne ze symetrie. □

30. Lemma

$$\exists v_o\, C[p^l; n|\bar{a}'] \in \mathrm{bool}(\mathbf{B}) \qquad \text{a pro } n = 1 \text{ jde o } \mathcal{AG}\text{-tautologii.}$$

Důkaz: Nechť $n = p^k r$; r je nesoudělné s p, nechť dále $k = la + k'$, kde $k' < l$.

Potom:

$$\exists v_0\, \mathsf{C}[p^l; n|\bar{a}'] \equiv \exists v_o\, \mathsf{C}[p^l; p^{k'}|\bar{a}'] \equiv \mathsf{C}[p^{k'}; 0|\bar{a}']$$

□

31. Věta Nechť $m \in \omega$, vektory $\bar{a}'_0, \ldots, \bar{a}'_{m-1}$ a celá čísla $k > l \leq 0$.

$$\exists v_o \bigwedge_{i<m} (\mathsf{C}[p^{l-1}; p^k|\bar{a}'_i] \wedge \star\mathsf{C}[p^l; p^k|\bar{a}'_i]) \equiv \exists v_o \bigwedge_{i<m} \mathsf{C}'\star\mathsf{C}[p^l; p^k|\bar{a}'_i] \in \mathrm{bool}(\mathbf{B})$$

Důkaz: Označme si $\varphi \equiv \bigwedge_{i<m} \mathsf{C}'\star\mathsf{C}[p^l; p^k|\bar{a}'_i]$. Nejprve rozebereme formuli podle možností $\mathsf{C}[p^l; (\bar{a}_i - \bar{a}_j)]$ pro $i < j < m$. Obdobně jako ve větě 21 dostáváme:

$$\xi_K \equiv \bigwedge_{i\in K} \mathsf{C}'\star\mathsf{C}[p^l; p^k|\bar{a}'_i] \wedge \mathrm{nes}[p^l; \bar{a}'_j - \bar{a}'_i;\ i \in K]$$

Pro každou $K \subseteq m$. Zbývá ukázat, že:

$$(\exists v_o)\xi_K \equiv \mathsf{N_S}[p, l; |K|+1] \wedge \Big(\bigwedge_{i\in K} \mathsf{C}[p^{l-1}; p^k|\bar{a}'_i] \Big) \wedge \mathrm{nes}[p^l; veca'_j - \bar{a}'_i;\ i, j \in K, i < j],$$

argumenty jsou analogické jako v lemmatu 21. □

32. Věta Pro $m \in \omega$ mějme $\varphi_0, \ldots, \varphi_{m-1}$, kde pro každé i je φ_i buďto rovnostní formule $\mathsf{E}[\bar{a}_i,]$ nebo nerovnostní formule $\star\mathsf{E}[\bar{a}_i]$ nebo divisibilní $\mathsf{C}[p_i^{l_i}; p_i^{k_i}|\bar{a}'_i]$ a nebo komplexní formule $\mathsf{C}'\star\mathsf{C}[p_i^{l_i}; p_i^{k_i}|\bar{a}'_i]$,

$$\psi \equiv \bigwedge_{i<m} \varphi_i \qquad \text{implikuje} \qquad \exists v_o\, \psi \in \mathrm{bool}(\mathbf{B})(20)$$

Důkaz: Označme si $\Phi := \{\varphi_0, \ldots, \varphi_{m-1}\}$. Nejprve větu vyřešíme s tímto dodatečným předpokladem:

(§) Jeli φ_i rovna $\star\mathsf{E}[\bar{a}_j]$ a je-li φ_j rovna $\mathsf{C}[p_i^{l_i}; p_i^{k_i}|\bar{b}'_i]$ nebo $\mathsf{C}'\star\mathsf{C}[p_i^{l_i}; p_i^{k_i}|\bar{b}'_i]$, tak potom $p_i^{k_i}$ je dělitelem a_{j0}.

Následující důkaz bude opět složen především z rozboru možností. Budeme postupovat indukcí podle m, kterémužto budeme říkat délka klauzule ψ. Předně pro $m = 1$ je řešením jedna z vět nebo lemmat 16, 30 nebo věta 31 . Nechť $m > 1$ a předpokládejme, že pro klauzule kratší než m již tvrzení platí.

Pro některé volby Φ už umíme tvrzení dokázat přímo:

i. Ve Φ jsou dvě různé funkce rovnosti $\mathsf{E}_i, \mathsf{E}_j$. Potom podle lemmatu 15 platí, že můžeme nalézt $\bar{b}$, $\bar{b}'_0$, $\bar{b}'_1$ a dále $\mathsf{E}_i \wedge \mathsf{E}_j \equiv \mathsf{E}[\bar{b}] \wedge \mathsf{E}[0|\bar{b}'_0] \wedge \mathsf{E}[0|\bar{b}'_1]$ a tedy můžeme přirozeně můžeme zkrátit délku klauzule. ◇

ii. Do Φ náleží E_i a C_j, takové, že a_{i0} není dělitelné $p_j^{k_j+1}$. Potom využijeme lemma 28. $\diamond$

iii. Do Φ náleží E_i a $\mathsf{C}'\star\mathsf{C}_j$ taková, že a_{i0} není dělitelné $p_j^{k_j+1}$. Potom využijeme hned dvakrát lemma 27. $\diamond$

iv. Do Φ náleží C_i a φ_j, φ_j je buď C_j a nebo $\mathsf{C}'\star\mathsf{C}_j$ a platí $p_i = p_j$, a $l_i \geq l_j > k_j \geq k_i$. Potom aplikujeme lemma 27. $\diamond$

v. Do Φ náleží $\mathsf{C}'\star\mathsf{C}_i$, $\mathsf{C}'\star\mathsf{C}_j$ a $p_i = p_j$, $k_i = k_j$ a $l_i \neq l_j$. Použijeme lemmatu 27. $\diamond$

vi. Nechť Φ nemá ani jednu z vlastností i.-v. a existuje $\mathsf{C}_j \in \Phi$ s těmito vlastnostmi:

$$\begin{array}{rlll} \mathsf{C}_i \in \Phi & \text{a zároveň} & p_i = p_j & \text{potom} \quad k_i \geq k_j \\ \mathsf{C}'\star\mathsf{C}_j \in \Phi & \text{a zároveň} & p_i = p_j & \text{potom} \quad k_i \geq k_j \end{array}$$

Zvolme dlouhé vektory $\bar{b}_i^* = (p_i^{k_i} | p_j^{k_j} \bar{a}_i$, pokud φ_i je divisibilní nebo komplexní funkce taková, že $p_i \neq p_j$; ve všech zbylých případech položme $\bar{b}_i^* = \bar{a}_i^*$. Platí tedy vždy $\varphi[\bar{a}_i^*] \equiv \varphi[\bar{b}_i^*]$ a zároveň a_{j0} dělí b_{i0}; $i < m$. Pokud $a_{j0} = p_j^0 = 1$, máme:

$$\exists v_o\, \psi \equiv v_o \bigwedge_{\substack{i<m \\ i\neq j}} \varphi_i \Big[b_{i,*} \Big| p_j^{l_j} b_{i0} \Big| (\bar{b}_i' - b_{i0}\bar{b}_j') \Big]$$

a s využitím lemmatu 29 můžeme formuli převést na formuli, která sestává opět z divizibilních a komplexních formulí, které mají na pozici a_{i0} mocninu prvočísla a tedy je tvaru vi., formule se tedy převede na tvar (20) a splní indukční předpoklad.

Pokud $a_{j0} = p_j^{k_j} > 1$, potom můžeme podmínku $\exists v_o\, \mathsf{C}_j$ nahradit podmínkou $\exists v_o [p_j^{k_j} | (1)] \wedge \mathsf{C}[p^l; 1 | \bar{a}_j']$ viz. (2) a protože a_{j0} dělí $b_{i0}\, i < m$, můžeme tímto způsobem vytknout a_{j0} z každé φ_i; $i < m$:

$$\exists v_o \psi \equiv \exists v_o \left([p_j^{k_j} | (1)] \wedge \mathsf{C}[p^l; 1 | \bar{a}_j'] \wedge \bigwedge_{\substack{i<m \\ i}} \varphi_i \Big[a_{i*} \Big| \frac{b_{i0}}{a_{j0}} \Big| \bar{b}_i' \Big] \right).$$

Dosadíme-li $\mathsf{C}[p_j^{l_j}; 1 | 0, \ldots] \wedge \mathsf{C}[p_j^{k_j}; 1 | \bar{a}_j'] \equiv \mathsf{C}[p_j^{k_j}; 0 | \bar{a}_j'] \wedge \mathsf{C}[p_j{}^{l_j} | 1 | \bar{a}_j']$

dle lemma 27, dostaneme se na předchozí případ. $\diamond$

vii. Nechť $\mathsf{C}'\star\mathsf{C}_j \in \Phi$ má tyto vlastnosti:

$$\begin{array}{rlllll} \mathsf{C}_i & \in \Phi & \text{a zároveň} & p_i = p_j & \text{potom} & k_i > k_j \\ \mathsf{C}'\star\mathsf{C}_i & \in \Phi & \text{a zároveň} & p_i = p_j & \text{potom} & k_i \geq k_j \\ \star\mathsf{E}_i & \in \Phi & \text{tak potom vždy} & p_j^{k_j+1} & \text{dělí} & a_{i0} \end{array}$$

Pokud je $\mathsf{C}'\star\mathsf{C}_i \in \Phi$ taková, že $p_i = p_j$ a $k_i = k_j$, pak podle bodu iv. a v. máme již vyřešený případ $l_i \neq l_j$. Mějme tedy právě n komplexních fukcí $\mathsf{C}'\star\mathsf{C}_i$, takových, že $p_i = p_j, k_i = p_j, l_i = l_j$ a pro pohodlnost si je přečíslujme jako $\varphi_0, \ldots, \varphi_{n-1}$ a přeznačme si $p_0, k_0, l_0, \bar{\boldsymbol{a}}_0, \mathsf{C}'\star\mathsf{C}_0$ na $p, k, l, \bar{\boldsymbol{a}}, \mathsf{C}'\star\mathsf{C}$. Pokud $n = m$, dostali jsme případ diskutovaný v lemmatu **??** budeme tedy dále uvažovat $n < m$. $\mathrm{Nsn}(a_{i0};\, i < m) = p^s r$; $s \geq k$, $\mathrm{NsD}(p, r) = 1$. Pro každou ψ vyhovující podmínce vi. označme $\alpha_\psi = s - k$.

Ať $\alpha_\psi = 0$. Pak z předpokladu na výběr $\star\mathsf{C}$, z ii. a z toho, že $\alpha_\psi = 0$ plyne, že každá z formulí $\varphi_n, \ldots, \varphi_{n-1}$ je buď divizibilní nebo nedivizibilní formule a v obou případech platí $p_i \neq p_j$. Ukažme, že:

$$\exists v_o \bigwedge_{i<m} \varphi_i \equiv \left(\exists v_o \bigwedge_{i<n} \varphi_i\right) \wedge \left(\exists v_0 \bigwedge_{n\leq i<m} \varphi_i\right) \tag{21}$$

čímž se sníží délka klauzule ve ψ. Nechť pro grupu G vektor $\bar{\boldsymbol{x}}' \in {}^{\ell\bar{\boldsymbol{x}}'}G$ lze dosadit do PS v (21) tak, aby vzniklá sentence byla pravdivá. Lze tedy speciálně dosadit do $\exists v_o \bigwedge_{i<n} \varphi_i$ tak, aby vznikla pravdivá sentence a označme x_0 prvek, jehož existenci sentence zajišťuje a dále lze dosadit do $\exists v_o \bigwedge_{n<i<m} \varphi_i$ tak, že dostaneme pravdivou sentenci a označme y_0 prvek, který nutně existuje. Určíme si $q = \mathrm{Nsn}(a_{i*};\, n \leq i < m) = p^s r$ a najdeme celá čísla m', n' aby $m'p^l + n'q = 1$. Položme:

$$z = m'x_0 + n'y_0.$$

Zbývá ověřit, že $(z|\bar{\boldsymbol{x}}')$ lze dosadit do $\bigwedge_{i<m} \varphi_i$ na pravdivou sentenci:

$$p^k z = p^k m'p^l \cdot x_0 + p^k(1 - m'p^l) \cdot y_0 = p^k x_0 + p^l(m'p^k)(x_0 - y_0)$$

a tedy $z|\bar{\boldsymbol{x}}'$ lze dosadit do $\exists v_o \bigwedge_{i<n} \varphi_i$ na pravdivou sentenci (jelikož $p^k z \equiv p^k x_0 \pmod{p^l}$). Symetricky pro každé $n \leq i < m$:

$$p_i^{k_i} z = p_i^{k_i} z + q(1 - n'p_i^{k_i}) \quad \text{a platí} \quad p_i^{l_i} | q,$$

čili $(z|\bar{\boldsymbol{x}}')$ lze dosadit do φ_i na pravdivou sentenci a tedy LS (21)$\ll_{\mathcal{AG}}$ PS(21). Opačná podřízenost je zřejmá.

Budiž $\alpha_\psi > 0$ a předpokládejme, že tvrzení věty platí pro každé φ, $\alpha_\varphi < \alpha_\psi$. Rozebereme funkci podle možností $\mathsf{C}[p^{l+1}; p^{k+1} | p\bar{\boldsymbol{a}}'_i]$ a označme $\zeta = \bigwedge_{n \le i < m} \varphi_i$. Pro $K \subseteq n$ máme:

$$\xi_K \equiv \bigwedge_{i \in K} (\varphi_i \wedge \mathsf{C}[p\bar{\boldsymbol{a}}^*_i]) \wedge \bigwedge_{i \in n-K} (\varphi_i \wedge \star\mathsf{C}[p\bar{\boldsymbol{a}}^*_i]) \wedge \zeta$$

Pro $K = \emptyset$ provedeme:

$$\rho \equiv \bigwedge_{i<n} (\mathsf{C}[p^{l-1}; \bar{\boldsymbol{a}}_i] \wedge \mathsf{C}[p^l; p\bar{\boldsymbol{a}}_i] \wedge \star\mathsf{C}[p\bar{\boldsymbol{a}}^*_i]) \wedge \zeta \equiv nes[p^{l-1}; (\bar{\boldsymbol{a}}_i - \bar{\boldsymbol{a}}_0); 0 < i < n] \wedge \rho_2,$$

$$\rho_2 \equiv \mathsf{C}[p^{l-1}; p^k, \bar{\boldsymbol{a}}_0] \wedge \bigwedge_{i<n} (\mathsf{C}[p^l; p\bar{\boldsymbol{a}}_i] \wedge \star\mathsf{C}[p\bar{\boldsymbol{a}}^*_i]) \wedge \zeta,$$

ρ_2 má tvar, který jsme diskutovali v odstavci vi., proto použijeme stejné úpravy a dostaneme formuli, která bude mít délku klausule rovnou m (ρ_2 má délku $m+1$) a jež bude opět tvaru vii, ale její hodnota α bude menší než hodnota α_ψ. Uvažujme dále případ $K \neq \emptyset$ a bez újmy na obecnosti nechť $0 \in K$.

$$\xi_K \equiv \bigwedge_{i \in n-M} (\mathsf{C}[p^{l-1}; (\bar{\boldsymbol{a}}'_i - \bar{\boldsymbol{a}}'_0)] \wedge \star\mathsf{C}[p^{l+1}; p(\bar{\boldsymbol{a}}_i - \bar{\boldsymbol{a}}_0)]) \wedge \underbrace{\bigwedge_{i \in M} (\varphi_i \wedge \mathsf{C}[p\bar{\boldsymbol{a}}^*_i]) \wedge \zeta}_{\xi'_K}$$

Rozebereme ξ'_K na případy podle $\mathsf{C}[p^l; 0 | (\bar{\boldsymbol{a}}_i - \bar{\boldsymbol{a}}_j)]$ pro $i, j \in K, i < j$. Přitom případy, kdy platí $\mathsf{C}[p^l; 0 | (\bar{\boldsymbol{a}}_i - \bar{\boldsymbol{a}}_j)]$ budou zahrnuty v diskuzi ξ_{K-i}. Dostáváme tedy:

$$\xi'_K \equiv \zeta \wedge \bigwedge_{i \in K} (\varphi_i \wedge \mathsf{C}[p\bar{\boldsymbol{a}}^*_i]) \wedge \mathrm{nes}[\bar{\boldsymbol{a}}'_j - \bar{\boldsymbol{a}}'_i,\ i, j \in K,\ i < j] \qquad (22)$$

A stačí ukázat, že

$$\exists v_o\, \xi'_K \equiv \exists v_o\, \zeta \wedge \mathsf{N}^{\mathsf{O}}_{\mathsf{S}}[p, l; |K|+1] \wedge \bigwedge_{i \in K} \mathsf{C}[p\bar{\boldsymbol{a}}^*_i] \wedge \mathrm{nes}[p^{l-1}; \bar{\boldsymbol{a}}'_j - \bar{\boldsymbol{a}}'_i;\ j, i \in K,\ i < j].$$

◇

viii. Předpokládejme, že Φ nesplňuje žádnou z podmínek i.-vii. Vyberme si $\mathsf{C}'\star\mathsf{C}_j$, tak, aby platilo:

$$\begin{array}{rlllll} \mathsf{C}_i & \in \Phi & \text{a zároveň} & p_i = p_j & \text{potom} & k_i > k_j \\ \mathsf{C}'\star\mathsf{C}_i & \in \Phi & \text{a zároveň} & p_i = p_j & \text{potom} & k_i \geq k_j \end{array}$$

Prohoďme indexy u $\mathsf{C}'\star\mathsf{C}_j$ na $\mathsf{C}'\star\mathsf{C}_0$ a $p_j, k_j, l_j, \bar{\boldsymbol{a}}_j$ na $p, k, l, \bar{\boldsymbol{a}}$. Mějme tedy právě $n > 0$ formulí $\star\mathsf{E}_i$, takových, že p^{k+1}nedělí a_{i0}. Jednu z nich označme $\mathsf{E}_1[\,\bar{\boldsymbol{a}}_1\,]$. Provedeme indukci podle n.

Platí tedy podle (§), že $a_{10} = p^k r$ a $\mathrm{NsD}(p, r) = 1$.

$$\mathsf{C}'\star\mathsf{C}_0 \wedge \mathsf{E}_1 \equiv \underbrace{(\mathsf{C}'\star\mathsf{C}_0 \wedge \mathsf{E}_1 \wedge \mathsf{C}[p^{l-1}; \bar{\boldsymbol{a}}_1\,])}_{\zeta} \vee \underbrace{(\mathsf{C}'\star\mathsf{C}_0 \wedge \mathsf{C}_1 \wedge \star\mathsf{C}[p^{l-1}; \bar{\boldsymbol{a}}_1\,])}_{\xi},$$

a dosadíme:

$$\xi \equiv \mathsf{C}'\star\mathsf{C}_0 \wedge \star\mathsf{C}[p^{l-1}; \bar{\boldsymbol{a}}_1\,] \equiv \mathsf{C}[p^{l-1}; \bar{\boldsymbol{a}}_0\,] \wedge \star\mathsf{C}[p^l; \bar{\boldsymbol{a}}_0\,] \wedge \star\mathsf{C}[p^{l-1}; 0|(\bar{\boldsymbol{a}}'_1 - r\bar{\boldsymbol{a}}'_0)\,]$$

a tedy $\xi \wedge \bigwedge_{1<i<m} \varphi_i$ má délku klausule kratší než ψ.

Dále na ζ můžeme použít rozbor podle $\mathsf{C}[p^l; \bar{\boldsymbol{a}}_1\,]$:

$$\zeta \equiv \underbrace{(\mathsf{C}'\star\mathsf{C}_0 \wedge \mathsf{C}[p^{l-1}; \bar{\boldsymbol{a}}_1\,] \wedge \star\mathsf{C}[p^l; \bar{\boldsymbol{a}}_1\,])}_{\rho_1} \vee \underbrace{(\mathsf{C}'\star\mathsf{C}_0 \wedge \mathsf{E}_1 \wedge \mathsf{C}[p^l; \bar{\boldsymbol{a}}_1\,])}_{\rho_2}$$

a můžeme najít s, s' tak, aby $s'p^l + sr = 1$ a použít (19) na:

$$\begin{array}{ll} \mathsf{C}[p^{l-1}; p^k r|\bar{\boldsymbol{a}}'_1\,] \equiv \mathsf{C}[p^{l-1}; p^k|s\bar{\boldsymbol{a}}'_1\,] & \mathsf{C}[p^l; p^k r|\bar{\boldsymbol{a}}'_1\,] \equiv \mathsf{C}[p^l; p^k|s\bar{\boldsymbol{a}}'_1\,] \\ \rho_1 \equiv \mathsf{C}'\star\mathsf{C}[p^l; \bar{\boldsymbol{a}}_0\,] \wedge \mathsf{C}'\star\mathsf{C}[p^l; p^k|s\bar{\boldsymbol{a}}'_1\,] & \rho_2 \equiv \mathsf{C}'\star\mathsf{C}[p^l; 0|(\bar{\boldsymbol{a}}'_0 - s\bar{\boldsymbol{a}}'_1)\,] \end{array}$$

A stačí ověřit že $\rho_1 \wedge \bigwedge_{1<i<m} \varphi_i$ má délku klusule shodnou s ψ a splňuje indukční předpoklad; v případu $\rho_2 \wedge \bigwedge(\Phi - \mathsf{C}'\star\mathsf{C}_0)$ zopakujeme postup z bodu vi.

$\diamond$

(-§) Takto pokud jsme předpokládali (§). Nyní obecný případ. Označme si jako K množinu dvojic indexů $(i, j) \in m \times m$ takových, že φ_i je komplexni nebo divizibilní funkce, φ_j je nerovnostní funkce a a_{i0} nedělí a_{j0}. Provedeme indukci podle $|K|$. Samozřejmě $K = \emptyset$ je ekvivalentní s (§). Zvolme $(i, j) \in K$, tedy $a_{j0} = p_i^n r$; $n < k_i$, $\mathrm{NsD}(p, r) = 1$. Označme $p_i = p$, $k_i = k$.

$$\varphi_i \wedge \varphi_j \equiv \varphi_i \wedge \varphi_j \underbrace{\wedge(\mathsf{E}[p^k r|p^{k-n}\,\bar{\boldsymbol{a}}'_j]}_{\zeta} \vee \underbrace{\mathsf{E}[p^{k_i} r|p^{k_i-n}\bar{\boldsymbol{a}}'_j]\,)}_{\xi}$$

$$\varphi_i \wedge \varphi_j \wedge \xi \equiv \varphi_i \wedge \mathsf{E}[p^k | p^{k-n} \bar{a}'_j]$$

a podle lemma 27 rozložme:

$$\varphi_i \wedge \varphi_j \wedge \zeta \equiv \varphi_j \wedge \mathsf{C}[p^{l_i}; 0 | \bar{b}'] \wedge \mathsf{E}[p^k r | p^{k-d} \bar{b}],$$

podařilo se nám tedy přejít k ekvivalentní množině formulí, jež má menší $|K|$.

33. Věta Mějme $\Phi = \{\varphi_0 \ldots, \varphi_{m-1}\}$, kde buď $\varphi_i \in \mathbf{B}$ nebo $\neg\varphi \in \mathbf{B}$. Potom

$$\exists v_0 \bigwedge \Phi \in \mathrm{bool}(\mathbf{B}) \tag{23}$$

Důkaz: Označme Ψ množinu všech $\star\mathsf{C}_i[p_i^{k_i}; p_i^{k_i} | \bar{a}'_i] \in \Phi$, že $\mathsf{C}[p_i^{l_i-1}; p_i^{k_i} | \bar{a}'_i] \notin \Phi$. Pro každou množinu formulí $\Phi \subseteq \mathrm{bool}(\mathbf{B})$ splňující podmínky této věty proveďme:

- Jako α_Φ označme $|\Psi|$,
- jako β_Φ označme $\max\{l_i - k_i;\ \varphi_i \in \Psi\}$,
- jako γ_Φ označme počet, kolikrát se maxima β nabývá.

Budeme postupovat indukcí podle α_Φ a β_Φ. Pro $\alpha_\Phi = 0$ můžeme $\bigwedge \Phi$ přezávorkovat, aby se v ní vyskytovaly pouze komplexní funkce a žádná funkce $\star\mathsf{C}$, čili jde o případ minulého lemmatu. Nechť $\alpha_\Phi > 0$. Pro $\beta_\Phi = 0$ můžeme každou $\star\mathsf{C}_i$ vytknout před kvantifikátor. Nechť $\alpha_\Phi, \beta_\Phi > 0$ a pro jejich jakékoli menší hodnoty již máme tvrzení dokázáno. Zvolme si nějakou $\star\mathsf{C}[\bar{a}_i^*]$, na které nabývá β_Φ maxima a přeznačme $p_i, k_i, l_i, \bar{a}_i$ na $p, k, l, \bar{a}$.

$$\mathsf{C}[\bar{a}^*] \equiv \underbrace{(\mathsf{C}[p^{l-1}; \bar{a}] \wedge \star\mathsf{C}[\bar{a}^*])}_{\zeta} \vee \underbrace{\star\mathsf{C}[p^{l-1}, \bar{a}]}_{\xi}$$

Nyní pro $\Delta = \zeta \cup \Phi - \{\star\mathsf{C}_i\}$ je $\alpha_\Delta < \alpha_\Phi$ a pro $\Theta = \xi \cup \Phi - \{\star\mathsf{C}_i\}$ je buď $\beta_\Theta < \beta_\Phi$ čímž je důkaz hotov nebo $\gamma_\Theta < \gamma_\Phi$ a můžeme postup opakovat tak dlouho, až $\gamma_\Theta = 0$. □

Takto jsme se dopočítali ke kladné odpovědi na bod c. lemmatu I.5. K dokončení důkazu věty II.12 si zbývá rozmyslit, že množina $\mathbf{S}'$ opravdu tvoří základní množinu sentencí $\mathcal{AG}$. K tomu je zapotřebí znovu si bedlivě projít důkaz a uvažovat podobu všech formulí, na které byla převedena formule s kvantifikátorem. Jsou to jednak formule tvaru div, nez, nes, $\mathsf{C}[p^l; 0 | \bar{a}]$ atp., které jsou ovšem bez volných proměnných vždy sentencemi triviálními[2] a dále jsou to formule tvaru $\mathsf{N}, \mathsf{N}^{\mathsf{O}}, \mathsf{N}_{\mathsf{S}}$ a $\mathsf{N}^{\mathsf{O}}_{\mathsf{S}}$. Z tohoto se dá již vyvodit, že pokud budeme výše probíraný proces eliminace kvantifikátorů uplatňovat na nějakou sentenci, tak nám vždy vypadne booleovská kombinace sentencí $\mathsf{N}, \mathsf{N}^{\mathsf{O}}, \mathsf{N}_{\mathsf{S}}, \mathsf{N}^{\mathsf{O}}_{\mathsf{S}}$.

[2]sentence, která je buďto $\mathcal{AG}$-spor nebo $\mathcal{AG}$-tautologie

IV. Diskuze na závěr.

Pro každou sentenci $\varphi \in (\frac{\mathsf{Fm}}{+})^{\bullet}$ jsme schopní efktivně najít $k \in \omega$ a $(\psi_{ij})_{i,j=1}^{k}$, že buď $\psi_{ij} \in \mathbf{S}'$ nebo $\neg\psi_{ij} \in \mathbf{S}'$, tak, aby:

$$\varphi \sim \bigvee_{i<k} \bigwedge_{j<k} \psi_{ij},$$

a tento vztah se přirozeně přenáší i na struktu aritmetické třídy vymezené φ:

$$\mathfrak{M}^{+}_{AG}(\varphi) = \bigcup_{i<k} \bigcap_{j<k} \mathfrak{M}^{+}_{AG}(\psi_{ij})$$

A naší snahou je nyní najít způsob jak rozhodnout, kdy je daná aritmetická třída prázdná. Připomeňme si nyní vztah, který jsme uvedli v kapitole II, který platí pro jakoukoli volbu $G \in \mathcal{AG}$, p prvočíslo a k celé:

$$\left.\begin{array}{r}\dim^{O}_{S}[p;k](G) = a \\ \dim^{O}[p;k+1](G) = b\end{array}\right\} \quad \textbf{právě tehdy když } \dim^{O}[p;k](G) = a+b$$

$$\left.\begin{array}{r}\dim^{O}_{S}[p;k](G) = a \\ \dim_{S}[p;k+1](G) = b\end{array}\right\} \quad \textbf{právě tehdy když } \dim_{S}[p;k](G) = a+b$$

Odtud plynou pravidla platná pro každou grupu G a každé prvočíslo p:

i. Existuje-li index $j_p \in \omega$, tak, pro $j > j_p$ platí $\dim^{O}_{S}[p;j] = 0$, potom existují konstanty $a_p, b_p \in \omega$, tak, že:

$$\dim^{O}[p;k](G) = a_p + \sum_{k \le i \le j_p} \dim^{O}_{S}[p;i] \tag{24}$$

$$\dim_{S}[p;k](G) = b_p + \sum_{k \le i \le j_p} \dim^{O}_{S}[p;i], \tag{25}$$

ii. pokud takový index j_p neexistuje, potom pro všechna $k \in \omega$ je $\dim^{O}[p;k]G = \infty$ a $\dim_{S}[p;k](G) = \infty$

Nyní ukážeme, že pro každou volbu a_p, b_p a $\bar{c}_p$ již existuje grupa $G = G[a_p, b_p, \bar{c}']$, pro niž platí:

$$\dim^{O}_{S}[p;k](G) = c_k \text{ a zároveň (25) a (24)}$$

34. Definice Aditivní grupu racionálních čísel si značme $\mathbb{Q}^{+}$, q ať vyznačuje prvočíslo a l přirozené číslo.

- jako $C(q,l)$ uvažujme cyklickou grupu řádu q^l, pro potřeby definice níže si ji reprezentujme jako $\{\frac{m}{q^l}$; kde $m < q^l\}$ s obvyklým sčítáním modulo 1.

- jako $A(q)$ uvažujme Prüferovu grupu $\mathbb{Z}_{q^\infty}$; $A(q) = \bigcup_{k\in\omega} C(q,l)$
- Jako $B(q) \leq \mathbb{Q}^+$ uvažujme všechny zlomky typu $\frac{m}{n}$, které mají čitatel n nesoudělný s q.

35. Lemma Pro p, q prvočísla a k, l celá čísla mají výše definované grupy níže uvedené dim:

	$A(q)$	$B(q)$	$C(q,l)$
$\dim^O[p;k]$	1 pokud $p=q$ jinak 0	0	1 pokud $p=q \wedge k \leq l$ jinak 0
$\dim_S[p;k]$	0	1 pokud $p=q$ jinak 0	1 pokud $p=q \wedge k \leq l$ jinak 0
$\dim^O_S[p;k]$	0	0	1 pokud $p=q \wedge k=l$ jinak 0

36. Lemma Mějme abelovské grupy $G_1, G_2, \ldots$. Potom pokud za $(^*_*)$ volíme (^-_S) nebo $(^O_-)$ nebo (^O_S) tak platí:

$$\dim^*_*[p;k]\left(\prod_{i\in\omega} G_i\right) = \sum_{i\in\omega} \dim^*_*[p;k](G_i)$$

Důkaz: Předopkládejme, že $\dim^*_*(G_i) \neq 0$ jen pro konečně mnoho i, jinak je vše triviální. K dokončení důkazu můžeme použít například charakterizace konkrétní $\dim^*_*$ pomocí po dvou nekongruentních prvků (popř. prvků řádu p^k, popř. nekongruentních prvků řádu p^k) v grupě $p^{k-1}G_i$. Vzhledem k tomu, že $p^n p^m = p^{n+m}$, zbývá si uvědomit, že pro $g_1, h_1 \in G_1$ a pro $g_2, h_2 \in G_2$ platí:

1) Pokud $g_1 \in \mathrm{ord}[p;k](G_1)$ a $g_2 \in \mathrm{ord}[p;k](G_2)$ tak $(g_1, g_2) \in \mathrm{ord}[p;k](G_1 \times G_2)$

2) pokud $g_1 \not\equiv h_1, g_2 \not\equiv h_2 \pmod{p}$ tak $(g_1, g_2) \not\equiv (h_1, h_2) \pmod{p}$. □

Nyní je již očividné, že:

$$G[a_p, b_p, \bar{c}] = A(p)^{a_p} \times B(p)^{b_p} \times \prod_{i\leq \ell\bar{c}} C(p,k)^{c_k}.$$

37. Věta Uvažujme formuli $\psi \equiv \bigwedge_{i<m} \psi_i$, kde $\psi_i = \mathsf{N}^{\mathsf{O}*}_*[p_i, k_i; n_i]$ nebo $\neg\mathsf{N}^*_{\mathsf{S}*}[p_i, k_i, n_i]$ nebo $\mathsf{N}[d_i, n_i]$ nebo $\neg\mathsf{N}[d_i, n_i]$. Potom existuje algoritmus, který rozfhodne, zda je formule splnitelná v $\mathcal{AG}$, čili zda $\mathfrak{M}^+_{AG}(\psi)$ je neprázdná.

Důkaz: Nejprve vyřešme úlohu s tímto předpokladem:

(‡) Ani jedna sentence ψ_i není rovna $\mathsf{N}[d;n]$ nebo $\neg\mathsf{N}[d;n]$.

Označme si $\xi_p \equiv \bigwedge_{i\in J_p}\psi_i$, kde I_p je množina všech i, které mají $p_i = p$. ψ je splnitelá, pokud, je splnitelná každá ξ_p, p prvočíslo,

Víme, že pro $p^m \leq n < p^{m+1}$ a volbu $(\underset{-}{O})$,$(\overline{S})$ nebo $(\underset{S}{O})$ je výrok:

$\mathsf{N}^*_*[p,k;n](G)$ je logicky ekvivalentní s výrokem $\dim^*_*[p;k](G) \geq m$

$\neg\mathsf{N}^*_*[p,k;n](G)$ je logicky ekvivalentní s výrokem $\dim^*_*[p;k](G) < m$

Proveďme tedy odpovídající záměnu pro každé ψ_i, $i \in J_p$. Problém, zda je ξ_p splnitelná je tedy redukován na to, zda existují a_p, b_p a $\bar{c}$ ($d := \ell\bar{c}$), takové, že:

- pokud $\psi_i = \mathsf{N}^{\mathsf{O}}_{\mathsf{S}}[p_i,k_i;n_i]$, tak $c_{pk} \geq m_i$,
- pokud $\psi_i = \neg\mathsf{N}^{\mathsf{O}}_{\mathsf{S}}[p_i,k_i;n_i]$, tak $c_{pk} < m_i$,
- pokud $\psi_i = \mathsf{N}_{\mathsf{S}}[p_i,k_i;n_i]$, tak $b_p + \sum_{k_i\leq i<d} c_{pi} \geq m_i$,
- pokud $\psi_i = \neg\mathsf{N}_{\mathsf{S}}[p_i,k_i;n_i]$, tak $b_p + \sum_{k_i\leq i<d} c_{pi} < m_i$,
- pokud $\psi_i = \mathsf{N}^{\mathsf{O}}[p_i,k_i;n_i]$, tak $a_p + \sum_{k_i\leq i<d} c_{pi} \geq m_i$,
- pokud $\psi_i = \neg\mathsf{N}^{\mathsf{O}}[p_i,k_i;n_i]$, tak $a_p + \sum_{k_i\leq i<d} c_{pi} < m_i$,

Takto se dostaneme konečný systém nerovnic pro $a_p, b_p, \bar{c}_p$, který se převede na konečnou booleovu algebru výroků a konečně se vyřeší.

Uvažujme obecný případ bez podmínky (‡). Pro $t \in \omega$ si uveďme novou *nilpotentní* sentenci:

$$\mathsf{Q}[t] \equiv \forall v_o\, tv_o = 0$$

a určeme definitivní *množinu základních sentencí* $\mathbf{S}$:

$$\mathbf{S} = \{\mathsf{N}^{\mathsf{O}}[p,k,n], \mathsf{N}_{\mathsf{S}}[p,k,n], \mathsf{N}^{\mathsf{O}}_{\mathsf{S}}[p,k,n], \mathsf{Q}[n]; \text{pro prvočísla } p \text{ a } k,n \in \omega\}$$

Pro každou $\Psi \subseteq \mathrm{bool}(\mathbf{S})$ platí, že lze algoritmicky rozhodnout, zda $\bigwedge\Psi$ je splnitelná. K tomu stačí zvážit, že v každé grupě $G[a_p, b_p, \bar{c}_p]$, pro každé prvočíslo p a celé číslo k platí:

$\mathsf{Q}[n](G)$ **právě když** $a_p, b_p = 0$ a pokud p^k nedělí n, tak také $c_{pk} = 0$.

Uzavřme celý důkaz tvrzením: $\mathbf{S} \sim \mathbf{S}'$ ($\sim (\underset{+}{\mathsf{Fm}})^\bullet$). Zvolme se tedy $\mathsf{N}[d;n]$ a stačí ukázat, že jsme ji schopni ekvivalentně vyjádřit jako booleovskou kombinací formulí z $\mathbf{S}$.

Ať $P = (p_1, p_2, \ldots)$ značí posloupnost všech prvočísel uspořádanou podle velikosti.

Pro nějaké $r \in \omega$ platí $p_{r-1} < n \leq p_r$, a utvoříme posloupnost $k_1, \ldots, k_r$ tak, aby $d = \prod p_i^{k_i}$.

Pro každé $0 \leq i \leq r$ najděme takové l_i, aby $p_i^{l_i} < n < p_i^{l_i+1}$. Definujme konečně $s := \prod_{i<r} p_i^{l_i+k_i}$.

Rozložíme nyní formuli $\mathsf{N}[d;n]$ podle možností $\mathsf{Q}[s]$

$$\mathsf{N}[d;n] \equiv \underbrace{(\mathsf{N}[d;n] \wedge \mathsf{Q}[s])}_{\xi} \vee \underbrace{(\mathsf{N}[d;n] \wedge \neg\mathsf{Q}[s])}_{\zeta}$$

Ovšem platí $\zeta \equiv \neg\mathsf{Q}[s]$, jelikož v každé grupě G, ve které platí $\mathsf{Q}[s]$ existuje prvek $z \in G$ a $sz \neq 0$, a tedy i $mz \neq 0, 2mz \neq 0, \ldots, nmz \neq 0$, přičemž všechny tyto prvky jsou přirozeně různé, tedy platí $\mathsf{N}[d;n](G)$.

Na druhou stranu, každá grupa G, ve které platí ξ má přirozeně všechny prvky konečného řádu. Lze tedy dle tvrzení 6 najít vyjádření pomocí cyklických grup $C(q_j;t_j)$ řádů mocnin prvočísel $q_j^{t_j}$:

$$G \cong \prod_{j\in J} C(q_j;t_j), \text{ kde } q_j < p_s, t_j < k_j + l_j,\ j \in J \tag{26}$$

$$dG \cong \prod_{j\in J'} C(q_j;t_j - d), \text{ kde } j \in J' \subseteq J \text{ pokud } t_j - d \geq 0 \tag{27}$$

$$|dG| > n \quad \textbf{pokud a potud} \quad \prod_{j\in J'} q_j^{t_j} \geq n \tag{28}$$

Množin Q uspořádaných dvojic (q_j, t_j) splňujících (26, 27, 28) a tuto podmínku minimality:

je jistě jen konečně. Očíslujme si je tedy všechny čísly $1, \ldots, x$ a označme $\mathcal{Q} = \{Q_1, \ldots, Q_x\}$. Vytvořme množinu $\mathcal{I} = \{I_1, \ldots, I_x\}$, kde každé $I_j = \{(q_{j_1}, t_{j_1}, h_{j_1}), \ldots$ $\ldots, (q_{j_y}, t_{j_y}, h_{j_y})\}$, tak, že každé (q_{j_i}, t_{j_i}) se vyskytuje v Q_j právě g krát a $q_{j_i}^{h_{j_i}} \leq g < q_{j_i}^{h_{j_i}}$. Prvky I_j jsou tedy uspořádané trojice a budeme je značit $(q_{j_y}, t_{j_y}, h_{j_y}) = \iota_{ji}$. Nyní, pokud vše pečlivě uvážíme, dostaneme tuto identitu:

$$\xi \equiv \bigvee_{I_j \in \mathcal{I}} \bigwedge_{\iota_{j_i} \in I_j} \mathsf{N}^{\mathsf{O}}_{\mathsf{S}}[\iota_{j_i}].$$

Tedy $\mathsf{N}[d;n] \sim \neg\mathsf{Q}[s] \vee \bigvee\bigwedge \mathsf{N}^{\mathsf{O}}_{\mathsf{S}}[\iota_{i_j}]$ a tedy $\mathbf{S} \sim \mathbf{S}'$. Tím jsme ovšem přidali poslední dílek mozaiky, a můžeme nazřít celý důkaz v plné kráse $\square$

$\square\square\square$

Literatura

[1] McKenzie R., Valeriote M.: *The Structure of Decidable Locally Finite Varieties*, Birkhäuser, Boston, 1985.

[2] Procházka L. a kol.: *Algebra*, Academia, Praha, 1990.

[3] Szmielew W.: *Elementary properties of Abelian groups*, Fund. Math., **41**: 203-71, 1955