دانشگاه تبریز

دانشکده‌ی علوم ریاضی

گروه ریاضی محض

رساله

برای دریافت درجه‌ی دکتری در رشته‌ی

ریاضی محض، گرایش منطق

عنوان

تصمیم‌پذیری نظریه‌های ضربی و ترتیبی اعداد

استاد راهنما

دکتر سعید صالحی پورمهر

استاد مشاور

دکتر جعفر صادق عیوضلو

پژوهشگر

زیبا اسعدی گلزار

۱۳۹۷

بسم الله الرحمن الرحیم

تقدیم به:

استاد گرانقدر و پرمایه ام

که لحظات ناب آموختن،

لذت و غرور دانستن،

جسارت خواستن و عظمت رسیدن را

مدیون حضور سبز ایشانم.

به شکر ایزد و استاد در مقام سجود　　نهاده سر به زمین همچو کلک و پرگارم
ز کس به دهر خجل نیستم بحمد الله　　مگر ز ایزد و استاد صدر احرارم

:::::::::::::::::
:::::::::::::::::

از آن قبل که سر عالم بقا دارم　　بدین سرای فنا سر فرو نمی‌آرم
هزار شکر کنم فیض و فضل یزدان را　　که داد دانش و دین گر نداد دینارم
ز خلق گوشه گرفتم که تا همی ساید　　کلاه گوشه همت به چرخ دوارم
به شکر صدر زمان هر زمان به بحر سخن　　صدف مثال دهان را به در بینبارم
ملک صفاتی کاندر ممالک شرفش　　سپهر گفت که من کمترین عمل دارم
ایا غیاث ضعیفان و غیث درویشان　　به باغ مدح تو بر شاخ معرفت بارم
به پیش فیض تو ز آن آمدم به استقا　　که وارهانی ازین خشکسال تیمارم

— خاقانی

به نام خداوندگار دانش و پژوهش و آفریدگار ریاضی و منطق

درود و سپاسی بیکران بر استاد راهنمای فرزانه‌ام جناب آقای دکتر **سعید صالحی‌پورمهر** که فراوان از او آموختم و اگر نبود دستگیری دلسوزانه‌ی ایشان در وادی پر پیچ و خم دانش، اکنون این نوشته راه به جایی نمی‌برد.
همچنین از جناب آقای دکتر **جعفرصادق عیوضلو** که زحمت مطالعه و مشاوره‌ی این رساله را تقبل فرمودند کمال امتنان و تشکر را دارم.
از اساتید محترم جناب آقای دکتر **سید محمد باقری** (دانشگاه تربیت مدرس — تهران) و جناب آقایان دکتر **محمد شهریاری** و **جابر کریم‌پور** (دانشگاه تبریز) که زحمت داوری پایان‌نامه اینجانب را متقبل شده‌اند، تقدیر و تشکر می‌نمایم.
محبت‌های بی‌دریغ پدر و مادرم را خاضعانه ارج می‌نهم و مهر آسمانی‌اشان را پاس می‌دارم.
از خواهر و برادر عزیزم صمیمانه سپاسگزارم که وجودشان شادی بخش و صفایشان مایه‌ی آرامش است.

زیبا اسعدی گلزار
۱۳۹۷

نام خانوادگی دانشجو: اسعدی گلزار نام: زیبا

عنوان: تصمیم‌پذیری نظریه‌های ضربی و ترتیبی اعداد

استاد راهنما : دکتر سعید صالحی پورمهر

استاد مشاور : دکتر جعفر صادق عیوضلو

مقطع تحصیلی: دکتری رشته: ریاضی محض گرایش: منطق دانشگاه تبریز

دانشکده علوم ریاضی تاریخ فارغ التحصیلی: ۱۳۹۷ تعداد صفحات: ۷۴

کلید واژه‌ها: تصمیم‌پذیری، تصمیم‌ناپذیری، تمامیت، ناتمامیت، نظریه‌ی مرتبه‌ی اول، حذف سور، ساختارهای مرتب.

چکیده

در این رساله ساختارهای ترتیبی اعداد طبیعی، صحیح، گویا و حقیقی مورد مطالعه قرار گرفته‌اند. نظریه‌های این اعداد در زبان ترتیب تصمیم‌پذیر و به طور متناهی اصل‌پذیر می‌باشند. همچنین نظریه‌های آنها در زبان ترتیب و جمع تصمیم‌پذیر بوده و به طور نامتناهی اصل‌پذیر هستند. برای زبان ترتیب و ضرب، اعداد طبیعی و صحیح تصمیم‌ناپذیر (و بنابراین اصل‌ناپذیر) می‌باشند. از قضیه‌ی تارسکی نتیجه می‌شود که ساختار ضربی و ترتیبی اعداد حقیقی نیز تصمیم‌پذیر است. در این رساله این نتیجه مستقیماً (با حذف سور) اثبات شده و یک اصل‌بندی (به طور نامتناهی) برای آن ارایه می‌شود. همچنین تصمیم‌پذیری نظریه‌ی ضربی و ترتیبی اعداد گویا با حذف سور نشان داده شده و اثبات می‌شود که این نظریه اصل‌پذیر نامتناهی است. نتایج حاصل از این رساله، در مقاله‌ی زیر ارایه شده‌اند:

Z. Assadi & S. Salehi; `On Decidability and Axiomatizability of Some Ordered Structures`, *Soft Computing* 23:11 (2019) 3615–3626. DOI: 10.1007/s00500-018-3247-1.

فهرست مطالب

مقدمه

مساله‌ی تصمیم،[1] یکی از مسایل اساسی منطق (ریاضی)، یافتن الگوریتمی تک ورودی و با خروجی بولی می‌باشد که با گرفتن فرمول φ به عنوان ورودی در صورت معتبر منطقی بودن φ خروجی «بله» و در غیر این صورت خروجی «خیر» را چاپ می‌کند. اکنون می‌دانیم که این مساله حل شدنی (به طور محاسبه پذیر) نیست. وجود یک نظریه‌ی اساساً تصمیم‌ناپذیر و متناهیاً اصل‌پذیر دلیلی بر این ادعا است [۲۰]؛ اثباتی دیگر در قضیه‌ی 11.2 از [۳] موجود است. با این حال، با توجه به قضیه‌ی تمامیت گودل[2] مجموعه‌ی فرمول‌های معتبر منطقی به طور محاسبه‌پذیر قابل شمارش است، یعنی یک الگوریتم بدون ورودی وجود دارد که (بعد از اجرا) همه‌ی فرمول‌های معتبر منطقی (و فقط این فرمول‌ها) را لیست می‌کند. برای ساختارها، از آنجایی که نظریه‌ی آنها کامل است، داستان متفاوت است: نظریه‌ی یک ساختار یا تصمیم‌پذیر است یا آن ساختار اصل‌پذیر نیست (یعنی توسط هیچ مجموعه‌ی به طور الگوریتمی شمارش‌پذیری از جملات اصل‌بندی نمی‌شود؛ برای مثال گزاره‌های 25G و 26I از [۷] یا قضیه‌ی 15.2 از [۱۲] را مشاهده نمایید). اصل‌پذیری یا تصمیم‌پذیری نظریه‌های اعداد طبیعی، صحیح، گویا، حقیقی و مختلط در زبان‌های مختلف (که ممکن است شامل رابطه‌ی ترتیب یا عمل جمع یا ضرب باشند) از دیرباز مورد توجه منطق‌دانان و

[1] *Entscheidungsproblem*

[2] Gödel's Completeness Theorem

ریاضی‌دانان قرار گرفته‌اند. برای مثال، تصمیم‌پذیری نظریه‌ی جمعی اعداد طبیعی $\langle \mathbb{N}; + \rangle$ توسط پرسبورگر[3] در سال ۱۹۲۹ نشان داده شد (و نیز توسط اسکولم[4] در سال ۱۹۳۰ ثابت گردید [۱۹]). تصمیم‌پذیری نظریه‌ی ضربی اعداد طبیعی $\langle \mathbb{N}; \times \rangle$ توسط اسکولم در سال ۱۹۳۰ اعلام شد. سپس انتظار می‌رفت که نظریه‌ی جمعی و ضربی اعداد طبیعی نیز در تأیید برنامه‌ی هیلبرت[5] تصمیم‌پذیر باشد. اما قضیه‌ی ناتمامیت گودل[6] در سال ۱۹۳۱ دنیا را شگفت زده کرد؛ این قضیه دلالت بر تصمیم‌ناپذیری نظریه‌ی $\langle \mathbb{N}; +, \times \rangle$ دارد (مراجعه کنید به بخش ۱.۴). در این رساله نظریه‌های مجموعه‌های $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ در زبان‌های $\{<\}$، $\{<, +\}$ و $\{<, \times\}$ مورد مطالعه قرار می‌گیرند؛ جدول زیر نمای کلی را به تصویر می‌کشد:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$
$\{<\}$	قضیه ۲۲.۱.۲	قضیه ۱۶.۱.۲	قضیه ۱۱.۱.۲	قضیه ۱۱.۱.۲
$\{<, +\}$	قضیه ۳.۵.۳	قضیه ۳.۴.۳	قضیه ۱.۲.۳	قضیه ۱.۲.۳
$\{<, \times\}$	گزاره ۱.۱.۴	گزاره ۲.۲.۴	نتیجه ۱۱.۴.۴	قضیه ۳.۳.۴
$\{+, \times\}$	ناتمامیت [۷]	گزاره ۱.۲.۴	گزاره ۱۲.۴.۴	بخش ۳.۴

توجه می‌کنیم که رابطه‌ی ترتیب در زبان $\{+, \times\}$ در این مجموعه‌ها تعریف‌پذیر است: در $\mathbb{N}$ توسط فرمول $x < y \iff \exists z (z + z \neq z \wedge x + z = y)$ و در $\mathbb{Z}$ توسط قضیه‌ی چهار مربع

[3] Presburger

[4] Skolem

[5] Hilbert's Program

[6] Gödel's Incompleteness Theorem

لاگرانژ[۷] رابطه‌ی $x < y$ معادل است با $\exists t, u, v, w\, (x \neq y \wedge x+t\cdot t+u\cdot u+v\cdot v+w\cdot w=y)$.
قضیه‌ی چهار مربع لاگرانژ در $\mathbb{Q}$ نیز برقرار است: برای هر $p/q \in \mathbb{Q}^+$ چون $pq > 0$، اعداد صحیح a، b، c و d وجود دارند به طوری که رابطه‌ی $pq = a^2+b^2+c^2+d^2$ برقرار است. پس داریم: $p/q = pq/q^2 = (a/q)^2+(b/q)^2+(c/q)^2+(d/q)^2$. بنابراین فرمول مشابهی رابطه‌ی ($x < y$) را در $\mathbb{Q}$ تعریف می‌کند. سرانجام در $\mathbb{R}$ رابطه‌ی $x < y$ با فرمول $\exists z(z+z \neq z \wedge x + z\cdot z = y)$ معادل است.

تصمیم‌پذیری $\mathbb{N}$ ، $\mathbb{Z}$ ، $\mathbb{Q}$ و $\mathbb{R}$ در زبان‌های $\{<\}$ و $\{<,+\}$ قبلاً شناخته شده‌اند. همچنین ثابت شده است که نظریه‌های $\mathbb{N}$ و $\mathbb{Z}$ در زبان $\{<,\times\}$ تصمیم‌ناپذیر می‌باشند؛ زیرا با توجه به اتحاد تارسکی_رابینسون[۸] جمع توسط ضرب و ترتیب در دامنه‌ی اعداد طبیعی تعریف‌پذیر است؛ بنابراین نظریه‌ی $\langle \mathbb{N}; \times, \leqslant \rangle$ تصمیم‌ناپذیر است. این مطلب با نشان دادن تعریف‌پذیری جمع در $\langle \mathbb{Z}; \times, \leqslant \rangle$ به دامنه‌ی اعداد صحیح $\mathbb{Z}$ گسترش می‌یابد که تصمیم‌ناپذیری ساختار $\langle \mathbb{Z}; \times, \leqslant \rangle$ را نتیجه می‌دهد. نظریه‌ی $\mathbb{R}$ نیز در زبان $\{<,\times\}$ بنا بر قضیه‌ی تارسکی_سیدنبرگ[۹] تصمیم‌پذیر است. این قضیه بیان می‌دارد که نظریه‌ی ساختار $\langle \mathbb{R}; <, +, \times \rangle$ توسط نظریه‌ی میدان‌های مرتب بسته‌ی حقیقی اصل‌پذیر می‌باشد. در حقیقت، برای اصل‌بندی نظریه‌ی ضربی و ترتیبی اعداد حقیقی نیازی به ابزارهای سنگین نیست. اثبات قضیه‌ی تارسکی در کتاب‌های اندک منطق (مانند [۱] و [۱۰]) موجود است. جالب است که در حقیقت، برهان هندسه‌ی جبری (مانند [۵] و [۴]) این قضیه بسیار زیباتر و گویاتر می‌باشد. با اینکه این قضیه تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{R}; \times, < \rangle$ را فوراً نتیجه می‌دهد، یک اصل‌بندی برای این نظریه از این قضیه به دست نمی‌آید. اینجا ما این مطلب

[7] Lagrange's Four Square Theorem

[8] Tarski-Robinson Identity

[9] Tarski-Seidenberg

را مستقیماً با ارایه کردن یک اصل‌بندی صریح اثبات می‌کنیم. سرانجام ساختار $\langle \mathbb{Q}; <, \times \rangle$ برای اولین بار در این رساله مورد مطالعه قرار می‌گیرد. ما با روش حذف سور نشان می‌دهیم که این نظریه تصمیم‌پذیر بوده و به طور نامتناهی اصل‌پذیر است. اینجا (ابر-)ساختار $\langle \mathbb{Q}; +, \times \rangle$ قابل استفاده نیست زیرا نظریه‌ی $\langle \mathbb{Q}; +, \times \rangle$ تصمیم‌ناپذیر است (این مطلب توسط رابینسون [۱۶] اثبات شده است؛ همچنین مراجعه کنید به قضیه‌ی 8.30 از [۱۹]). از طرف دیگر (زیر-)ساختار $\langle \mathbb{Q}; \times \rangle$ تصمیم‌پذیر است (اثبات شده توسط موستوفسکی[10] [۱۳]؛ همچنین رجوع شود به [۱۷]). بنابراین سه ساختار $\langle \mathbb{Q}; +, \times \rangle$ و $\langle \mathbb{Q}; <, \times \rangle$ و $\langle \mathbb{Q}; \times \rangle$ متفاوت از یکدیگرند، زیرا که رابطه‌ی ترتیب $<$ در ساختار $\langle \mathbb{Q}; \times \rangle$ تعریف‌پذیر نمی‌باشد و همچنین عمل جمع $+$ (همچنان که خواهیم دید) در ساختار $\langle \mathbb{Q}; <, \times \rangle$ تعریف‌پذیر نیست.

[10] Mostowski

فصل ۱

تعاریف و پیش‌نیازها

۱.۱ ساختارهای مرتب

تعریف ۱.۱.۱ (ساختار مرتب خطی). یک ساختار مرتب، سه‌تایی به صورت $\langle A; <, \mathcal{L}\rangle$ است به طوری که A یک مجموعه‌ی ناتهی و $<$ یک رابطه‌ی دوتایی روی A است که در اصول زیر صدق می‌کند:

$$(O_1) \quad \forall x, y (x < y \rightarrow y \not< x)$$

$$(O_2) \quad \forall x, y, z (x < y < z \rightarrow x < z)$$

$$(O_3) \quad \forall x, y (x < y \vee x = y \vee y < x)$$

و $\mathcal{L}$ یک زبان است. ⊛

اینجا $\mathcal{L}$ می‌تواند تهی یا هر زبان دیگری باشد، برای مثال $\{+\}$ یا $\{\times\}$ یا $\{+, \times\}$.

۲.۱ انواع مختلف ترتیب

تعریف ۱.۲.۱ (ترتیب خطی چگال)**.** یک رابطه‌ی ترتیب خطی $<$، چگال نامیده می‌شود هرگاه فرمول زیر برقرار باشد:

$$(\mathrm{O}_۴)\quad \forall x,y(x<y\to\exists z[x<z<y])$$

⊛

تعریف ۲.۲.۱ (ترتیب بی‌ابتدا و بی‌انتها)**.** یک رابطه‌ی ترتیب $<$، بی‌ابتدا و بی‌انتها نامیده می‌شود هرگاه داشته باشیم:

$$(\mathrm{O}_۵)\quad \forall x\exists y(x<y)$$

$$(\mathrm{O}_۶)\quad \forall x\exists y(y<x)$$

⊛

تعریف ۳.۲.۱ (ترتیب گسسته)**.** در یک ترتیب گسسته، برای هر عضو یک عضو بزرگ‌تر موجود است به طوری که هیچ عضو دیگری مابین آن دو وجود ندارد. اگر تالی x با $\mathfrak{s}(x)$ نشان داده شود، در این صورت هر ترتیب گسسته اصل زیر را ارضاء می‌کند:

$$(\mathrm{O}_۷)\quad \forall x,y(x<y\ \leftrightarrow\ \mathfrak{s}(x)<y\vee\mathfrak{s}(x)=y)$$

⊛

یادکرد ۴.۲.۱. تالی هر عدد صحیح x، برابر است با $\mathfrak{s}(x)=x+۱$. ⌖

۳.۱ لم اصلی حذف سور

تعریف ۱.۳.۱ (صورت نرمال فصلی)**.** صورت نرمال فصلی یک فرمول منطقی، فرمولی است معادل با آن که برابر است با ترکیب فصلی چند زیرفرمول که هر کدام از آن‌ها برابر ترکیب عطفی چند اتم یا نقیض اتم می‌باشند. ⊛

یادکرد ۲.۳.۱. با حذف ادات ترکیب «$\rightarrow$» و «$\leftrightarrow$» و با استفاده از قوانین دمورگان و نفی مضاعف، هر فرمول بدون سور را می‌توان معادلاً به صورت نرمال فصلی نوشت. ⌖

اثبات لم زیر که به لم «حذف سور» معروف است، در مراجع زیر موجود است: قضیه‌ی 31F از مرجع [۷]، لم 2.4.30 از مرجع [۹]، قضیه‌ی 1 (فصل 4) از مرجع [۱۰]، لم 3.1.5 از مرجع [۱۱] و لم 4.1 از مرجع [۱۹].

لم ۳.۳.۱ (لم اصلی حذف سور)**.** یک نظریه (یا یک ساختار) حذف سور می‌پذیرد اگر و تنها اگر هر فرمول به صورت $\exists x(\bigwedge_i \alpha_i)$ با یک فرمول بدون سور معادل باشد، که در آن هر α_i یک فرمول اتمی یا نقیض یک فرمول اتمی می‌باشد.

برهان. قسمت «تنها اگر» روشن است. قسمت «اگر» را به استقرا روی پیچیدگی فرمول دلخواه φ اثبات می‌کنیم. برای فرمول‌های بدون سور، حکم برقرار است. بنابراین کافی است سورهای $\forall$ و $\exists$ بررسی شوند. از طرفی سور عمومی نیز با عبارت $\forall x\varphi \equiv \neg\exists x\neg\varphi$ به سور وجودی تبدیل می‌شود.

پس کافی است فرمول $\exists x\varphi$ حذف سور شود که در آن φ خالی از سور است. حال بنا به یادکرد ۲.۳.۱ هر فرمول بدون سور را می‌توان به صورت نرمال فصلی نوشت، بنابراین داریم:

$$\exists x\varphi \equiv \exists x \bigvee_j (\bigwedge_i \alpha_i) \equiv \bigvee_j (\exists x(\bigwedge_i \alpha_i))$$

طبق فرض، فرمول $\exists x(\bigwedge_i \alpha_i)$ معادل با یک فرمول بدون سور است. پس فرمول $\exists x\varphi$ نیز با یک فرمول بدون سور معادل است. ⊠

نکته ۴.۳.۱. با توجه به اصول $\{O_1, O_2, O_3\}$، رابطه‌های $(s \neq t) \leftrightarrow (s < t \vee t < s)$ و $(s \nless t) \leftrightarrow (t \leqslant s)$ برقرار می‌باشند. بنابراین هرگاه زبان فقط شامل روابط «$<$» و «$=$» باشد، نیازی به در نظر گرفتن فرمول‌های نقیض اتمی نداریم. ⌖

فصل ۲

ساختارهای مرتب اعداد

۱.۲ اصل‌پذیری و حذف سور ساختارهای مرتب

تعریف ۱.۱.۲ (نظریه). یک نظریه، مجموعه‌ای از جمله‌ها است که تحت استلزام منطقی بسته باشد. ⊛

تعریف ۲.۱.۲ (نظریه‌ی تمام). نظریه‌ی T تمام است هرگاه به ازای هر جمله‌ی σ، یا $\sigma \in T$ یا $(\neg\sigma) \in T$. ⊛

نکته ۳.۱.۲. از آنجایی که نظریه‌ی یک ساختار، مجموعه‌ی جملاتی است که در آن ساختار ارضاء می‌شوند، این نظریه تمام است. ⌖

تعریف ۴.۱.۲ (مجموعه‌ی تصمیم‌پذیر). مجموعه‌ی A تصمیم‌پذیر است هرگاه یک روش کارآمد وجود داشته باشد که به ازای هر αی داده شده تصمیم بگیرد که $\alpha \in A$ یا $\alpha \notin A$.

تعریف ۵.۱.۲ (مجموعه‌ی شمارای کارآمد). مجموعه‌ی A شمارای کارآمد است هرگاه روشی کارآمد وجود داشته باشد که عضوهای A را به ترتیبی فهرست کند.

تعریف ۶.۱.۲ (اصل‌پذیری)**.** نظریه‌ی ساختار $\mathcal{A} = \langle A; \mathcal{L} \rangle$ اصل‌پذیر است هرگاه یک مجموعه‌ی تصمیم‌پذیر از $\mathcal{L}$–جملات یافت شود به طوری که نتایج منطقی این مجموعه از جملات با نظریه‌ی ساختار $\mathcal{A}$ برابر باشد. ⊛

• هرگاه مجموعه‌ی جملات فوق متناهی باشد، ساختار $\mathcal{A}$ را به طور متناهی اصل‌پذیر نامند.

گزاره ۷.۱.۲. برای یک زبان متناهی یا شمارا،

(۱) یک نظریه‌ی اصل‌پذیر، به طور کارآمد شمارش‌پذیر است.

(۲) یک نظریه‌ی اصل‌پذیر تمام، تصمیم‌پذیر است.

برهان. در نتایج 25F و 25G و 26I از مرجع [۷] ثابت شده‌اند. ⊠

نتیجه ۸.۱.۲. با توجه به نکته‌ی ۳.۱.۲ و گزاره‌ی ۷.۱.۲، نظریه‌ی یک ساختار در صورت اصل‌پذیری، تصمیم‌پذیر است. ⊠

تعریف ۹.۱.۲. گوییم (نظریه) ساختار $\mathcal{A} = \langle A; \mathcal{L} \rangle$ حذف سور می‌پذیرد هرگاه الگوریتمی وجود داشته باشد که هر فرمول در زبان $\mathcal{L}$ را به یک فرمول بدون سور دیگر زبان $\mathcal{L}$ با همان متغییرهای آزاد طوری تبدیل نماید که دو فرمول در (نظریه) ساختار $\mathcal{A}$ باهم معادل باشند.

• از آنجایی که هر اتم را می‌توان استنتاج یا ابطال کرد، جمله‌های بی‌سور را نیز می‌توان استنتاج یا ابطال کرد. بنابراین الگوریتمی که برای حذف سور به کار می‌بریم، در واقع الگوریتم تصمیم می‌باشد.

• ما در اینجا اصولی برای ساختارها ارایه کرده و به کمک این اصول ساختارها را حذف سور می‌کنیم. به این ترتیب اصل‌پذیری و تصمیم‌پذیری ساختارها اثبات می‌شوند.

۱.۱.۲ اصل‌پذیری متناهی ساختارهای $\langle \mathbb{R}; < \rangle$ و $\langle \mathbb{Q}; < \rangle$

یادکرد ۱۰.۱.۲ . اصول نظریه‌ی ترتیب‌های خطی چگال بی‌ابتدا و بی‌انتها عبارتند از:

$$(O_1) \quad \forall x, y(x < y \to y \nless x)$$

$$(O_2) \quad \forall x, y, z(x < y < z \to x < z)$$

$$(O_3) \quad \forall x, y(x < y \vee x = y \vee y < x)$$

$$(O_4) \quad \forall x, y(x < y \to \exists z[x < z < y])$$

$$(O_5) \quad \forall x \exists y(x < y)$$

$$(O_6) \quad \forall x \exists y(y < x)$$

⌖

قضیه‌ی زیر در مراجع [۱۱] (قضایای 2.4.1 و 3.1.3) و [۱۵] (قضیه‌ی 2.3) اثبات شده است.

- ما در اینجا یک برهان نحوی[1] ارایه می‌کنیم.

قضیه ۱۱.۱.۲ . نظریه‌ی متناهی ترتیب‌های خطی چگال بی‌ابتدا و بی‌انتها (که شامل اصول $\{O_1, O_2, O_3, O_4, O_5, O_6\}$ می‌باشد)، به طور کامل نظریه‌ی ترتیبی اعداد حقیقی و گویا را اصل‌بندی کرده و تحت آن ساختارهای $\langle \mathbb{R}; < \rangle$ و $\langle \mathbb{Q}; < \rangle$ حذف سور می‌پذیرند و بنابراین نظریه‌های آن‌ها تصمیم‌پذیر می‌باشند.

برهان. با توجه به نکته‌ی **۴.۳.۱**، همه‌ی فرمول‌های اتمی برای متغیرهای u و v به دو صورت $u < v$ یا $u = v$ می‌باشند. اگر هر دو متغیر برابر باشند، آنگاه $u < u$ بنا بر O_1 معادل با $\perp$ و $u = u$ معادل با $\top$ خواهند بود. بنابراین با توجه به لم **۳.۳.۱**، کافی است

[1] proof-theoretic (syntactic)

فرمول زیر حذف سور شود:

$$\exists x(\bigwedge_{i<\ell} y_i < x \wedge \bigwedge_{j<m} x < z_j \wedge \bigwedge_{k<n} x = u_k) \qquad (۱.۲)$$

که در آن y_iها، z_jها و u_kها متغیر هستند.

حال اگر $n \neq 0$، آنگاه فرمول (۱.۲) معادل با فرمول بدون سور زیر است:

$$\bigwedge_{i<\ell} y_i < u_0 \wedge \bigwedge_{j<m} u_0 < z_j \wedge \bigwedge_{k<n} u_0 = u_k.$$

بنابراین فرض می‌کنیم $n = 0$. در این صورت اگر $m = 0$ یا $\ell = 0$ آنگاه طبق اصول (به ترتیب) O_5 و O_6 (همراه O_2, O_3) فرمول (۱.۲) معادل با جمله $\top$ می‌باشد و اگر $\ell, m \neq 0$، آنگاه طبق O_4 (همراه O_2, O_3) معادل با فرمول بدون سور $\bigwedge_{i<\ell, j<m} y_i < z_j$ است. ⊠

نتیجه ۱۲.۱.۲ . برای هر مجموعه‌ی A به طوری که $\mathbb{Q} \subseteq A \subseteq \mathbb{R}$، ساختار $\langle A; < \rangle$ به طور کامل توسط مجموعه‌ی متناهی اصول $\{O_1, O_2, O_3, O_4, O_5, O_6\}$ اصل‌بندی می‌شود. ⊠

۲.۱.۲ اصل‌پذیری متناهی ساختار $\langle \mathbb{Z}; < \rangle$

گزاره ۱۳.۱.۲ . نظریه‌ی ساختار $\langle \mathbb{Z}; < \rangle$ حذف سور نمی‌پذیرد.

برهان. نشان می‌دهیم فرمول $\exists x(y < x < z)$ با هیچ فرمول بدون سوری در زبان $\{<\}$ معادل نمی‌باشد (توجه می‌کنیم که فرمول فوق با فرمول $y < z$ معادل نیست): همه‌ی فرمول‌های اتمی برای متغیرهای آزاد y و z عبارتند از $y < z$، $z < y$، $y = y(\equiv \top)$، $z = z(\equiv \top)$، $y < y(\equiv \bot)$ و $z < z(\equiv \bot)$ که هیچ ترکیب گزاره‌ای از آن‌ها در $\mathbb{Z}$ با فرمول $\exists x(y < x < z)$ معادل نمی‌شود. ⊠

تبصره ۱۴.۱.۲ . با افزودن عملگر تالی $\mathfrak{s}$ به زبان خواهیم داشت:

$$\exists x(y < x < z) \iff \mathfrak{s}(y) < z$$

و نشان خواهیم داد که حذف سور در این زبان انجام می‌پذیرد [قضیه‌ی ۱۶.۱.۲]. ⟐

یادکرد ۱۵.۱.۲ . نظریه‌ی متناهی ترتیب‌های خطی گسسته‌ی بی‌ابتدا و بی‌انتها توسط اصول

$$(\mathfrak{O}_1) \quad \forall x, y(x < y \to y \not< x)$$

$$(\mathfrak{O}_2) \quad \forall x, y, z(x < y < z \to x < z)$$

$$(\mathfrak{O}_3) \quad \forall x, y(x < y \vee x = y \vee y < x)$$

$$(\mathfrak{O}_7) \quad \forall x, y(x<y \leftrightarrow \mathfrak{s}(x)<y \vee \mathfrak{s}(x)=y)$$

$$(\mathfrak{O}_8) \quad \forall x\exists y(\mathfrak{s}(y) = x)$$

اصل‌بندی می‌شود. ⟐

مطلب زیر در قضیه‌ی 2.12 از مرجع [۱۵] به نحوی دیگر ثابت شده است:

قضیه ۱۶.۱.۲ . نظریه‌ی متناهی ترتیب‌های خطی گسسته‌ی بی‌ابتدا و بی‌انتها (که شامل اصول $\{\mathfrak{O}_1, \mathfrak{O}_2, \mathfrak{O}_3, \mathfrak{O}_7, \mathfrak{O}_8\}$ می‌باشد)، به طور کامل نظریه‌ی ترتیبی اعداد صحیح را اصل‌بندی می‌کند و نیز ساختار $\langle \mathbb{Z}; <, \mathfrak{s}\rangle$ حذف سور می‌پذیرد و بنابراین دارای نظریه‌ی تصمیم‌پذیر می‌باشد.

برهان. توجه می‌کنیم که همه‌ی ترم‌های زبان $\{<, \mathfrak{s}\}$ به شکل $\mathfrak{s}^n(y)$ برای یک متغیر y و یک عدد $n \in \mathbb{N}$ می‌باشند. بنابراین با توجه به نکته‌ی ۴.۳.۱، همه‌ی فرمول‌های اتمی برای متغیرهای u و v به دو صورت $\mathfrak{s}^n(u) = \mathfrak{s}^m(v)$ یا $\mathfrak{s}^n(u) < \mathfrak{s}^m(v)$ می‌باشند. هرگاه متغیر x در هر دو طرف فرمول اتمی ظاهر شود، در این صورت فرمول‌های اتمی به صورت

$\mathfrak{s}^n(x) = \mathfrak{s}^m(x)$ یا $\mathfrak{s}^n(x) < \mathfrak{s}^m(x)$ خواهند بود. فرمول $\mathfrak{s}^n(x) = \mathfrak{s}^m(x)$ برای $n = m$ معادل با $\top$ و در غیر این صورت معادل با $\perp$ می‌باشد. همچنین فرمول $\mathfrak{s}^n(x) < \mathfrak{s}^m(x)$ برای $n < m$ معادل با $\top$ و در غیر این صورت معادل با $\perp$ می‌باشد. بنابراین کافی است فرمول‌های اتمی به فرم $t < \mathfrak{s}^n(x)$ یا $\mathfrak{s}^n(x) < t$ یا $\mathfrak{s}^n(x) = t$ را برای هر ترم t آزاد از x و $n \in \mathbb{N}^+$ در نظر بگیریم. حال با توجه به لم ۳.۳.۱، فرمول زیر را حذف سور می‌کنیم:

$$\exists x(\bigwedge_{i<\ell} t_i < \mathfrak{s}^{p_i}(x) \wedge \bigwedge_{j<m} \mathfrak{s}^{q_j}(x) < s_j \wedge \bigwedge_{k<n} \mathfrak{s}^{r_k}(x) = u_k). \qquad (۲.۲)$$

با استفاده از اصل $\mathrm{O}_۷$ روابط $[a < b] \leftrightarrow [\mathfrak{s}(a) < \mathfrak{s}(b)]$ و $[a = b] \leftrightarrow [\mathfrak{s}(a) = \mathfrak{s}(b)]$ اثبات می‌شوند؛ بنابراین می‌توان همه‌ی p_iها، q_jها و r_kها در فرمول (۲.۲) را یکسان گرفته و برابر α فرض کرد. در این صورت با فرض $y = \mathfrak{s}^\alpha(x)$ برای ترم‌های جدید t'_i, s'_j, u'_k، با استفاده از اصل $\mathrm{O}_۸$ فرمول (۲.۲) با فرمول زیر معادل می‌شود:

$$\exists y(\bigwedge_{i<\ell} t'_i < y \wedge \bigwedge_{j<m} y < s'_j \wedge \bigwedge_{k<n} y = u'_k). \qquad (۳.۲)$$

حال اگر $n \neq ۰$، آنگاه فرمول (۳.۲) معادل با فرمول بدون سور زیر است:

$$\bigwedge_{i<\ell} t'_i < u'_۰ \wedge \bigwedge_{j<m} u'_۰ < s'_j \wedge \bigwedge_{k<n} u'_۰ = u'_k.$$

و اگر فرض کنیم $n = ۰$، آنگاه فرمول

$$\exists y(\bigwedge_{i<\ell} t'_i < y \wedge \bigwedge_{j<m} y < s'_j) \qquad (۴.۲)$$

با استفاده از اصل ۵۷ با فرمول بدون سور

$$\bigwedge_{i,j} \mathfrak{s}(t'_i) < s'_j$$

معادل می‌شود. ⊠

۳.۱.۲ اصل‌پذیری متناهی ساختار $\langle \mathbb{N}; < \rangle$

گزاره ۱۷.۱.۲ . نظریه‌ی ساختار $\langle \mathbb{N}; < \rangle$ حذف سور نمی‌پذیرد.

برهان. نشان می‌دهیم فرمول $\exists x(x < y)$ با هیچ فرمول بدون سوری معادل نمی‌باشد. همه‌ی فرمول‌های اتمی برای متغیر آزاد y به دو صورت $y < y$ یا $y = y$ می‌باشند که روابط $\bot \equiv (y < y)$ و $\top \equiv (y = y)$ نشان می‌دهند فرمول $\exists x(x < y)$ با هیچ کدام از ترکیبات گزاره‌ای آن‌ها معادل نیست، زیرا فرمول فوق بستگی به مقدار y دارد: برای $y = 0$ معادل $\bot$ و برای $y \neq 0$ معادل $\top$ است. ⊠

تبصره ۱۸.۱.۲ . با افزودن ثابت $\mathbf{0}$ به زبان $\{<\}$ خواهیم داشت:

$$\exists x(x < y) \iff \mathbf{0} < y.$$

ولی باز هم حذف سور ممکن نمی‌باشد [گزاره‌ی ۱۹.۱.۲ زیر]. ⌖

گزاره ۱۹.۱.۲ . نظریه‌ی ساختار $\langle \mathbb{N}; <, \mathbf{0} \rangle$ حذف سور نمی‌پذیرد.

برهان. برای اثبات کافی است نشان دهیم که فرمول $\exists x(y < x < z)$ با هیچ فرمول بدون سوری معادل نیست. همه‌ی فرمول‌های اتمی برای متغیرهای آزاد y و z به شکل‌های

$y=\mathbf{0}$، $z=\mathbf{0}$، $\mathbf{0}<y$، $\mathbf{0}<z$، $y=y(\equiv\top)$، $z=z(\equiv\top)$، $y<y(\equiv\bot)$، $z<z(\equiv\bot)$، $y=z$، $z=y$، $y<z$ و $z<y$ هستند که هیچ کدام از ترکیبات گزاره‌ای آن‌ها با فرمول $\exists x(y<x<z)$ معادل نیست. ⊠

تبصره ۲.۱.۲۰. با افزودن عملگر تالی $\mathfrak{s}$ به زبان $\{<\}$ خواهیم داشت:

$$\exists x(y<x<z) \iff \mathfrak{s}(y)<z.$$

حال نشان می‌دهیم که $\langle\mathbb{N};<,\mathfrak{s}\rangle$ حذف سور ندارد. [گزاره‌ی ۲.۱.۲۱ زیر] ⌖

گزاره ۲.۱.۲۱. نظریه‌ی ساختار $\langle\mathbb{N};<,\mathfrak{s}\rangle$ حذف سور نمی‌پذیرد.

برهان. نشان می‌دهیم که فرمول $\exists x(\mathfrak{s}(x)=y)$ با هیچ فرمول بدون سوری معادل نیست. همه‌ی فرمول‌های اتمی برای متغیر آزاد y به شکل‌های $\mathfrak{s}^n(y)<\mathfrak{s}^m(y)$ و $\mathfrak{s}^n(y)=\mathfrak{s}^m(y)$ می‌باشند که وابسته به مقدار y نیستند و معادل یکی از حالت‌های $\top$ یا $\bot$ می‌باشند. بنابراین فرمول $\exists x(\mathfrak{s}(x)=y)$ (که برای $y=0$ معادل $\bot$ و برای $y\neq 0$ معادل $\top$ است) معادل هیچ کدام از ترکیبات گزاره‌ای آن‌ها نمی‌باشد. ⊠

در ادامه حذف سور نظریه‌ی ساختار $\langle\mathbb{N};<,\mathfrak{s},\mathbf{0}\rangle$ را نشان خواهیم داد. این قضیه در مرجع [۷] اثبات شده است (قضیه‌ی 32A).

قضیه ۲۲.۱.۲ . اصول زیر به طور کامل نظریه‌ی ترتیبی اعداد طبیعی را اصل‌بندی می‌کند:

(O۱) $\forall x,y(x<y\to y\not< x)$

(O۲) $\forall x,y,z(x<y<z\to x<z)$

(O۳) $\forall x,y(x<y\vee x=y\vee y<x)$

(O۷) $\forall x,y(x<y\ \leftrightarrow\ \mathfrak{s}(x)<y\vee\mathfrak{s}(x)=y)$

(O۸) $\forall x\exists y(x\neq\mathbf{0}\to\mathfrak{s}(y)=x)$

(O۹) $\forall x(x\not<\mathbf{0})$,

همچنین ساختار $\langle\mathbb{N};<,\mathfrak{s},\mathbf{0}\rangle$ حذف سور می‌پذیرد و بنابراین تصمیم‌پذیر است.

برهان. همه‌ی فرمول‌های اتمی با متغیر آزاد u در زبان $\{<,\mathfrak{s},\mathbf{0}\}$ به یکی از صورت‌های $\mathfrak{s}^n(u)=\mathfrak{s}^m(u)$ یا $\mathfrak{s}^n(u)<\mathfrak{s}^m(u)$ یا $\mathfrak{s}^n(\mathbf{0})=\mathfrak{s}^m(u)$ یا $\mathfrak{s}^n(\mathbf{0})<\mathfrak{s}^m(u)$ یا $\mathfrak{s}^n(u)<\mathfrak{s}^m(\mathbf{0})$ می‌باشند. فرمول $\mathfrak{s}^n(u)=\mathfrak{s}^m(u)$ برای $n=m$ معادل با $\top$ و در غیر این صورت معادل با $\perp$ می‌باشد. همچنین فرمول $\mathfrak{s}^n(u)<\mathfrak{s}^m(u)$ برای $n<m$ معادل با $\top$ و در غیر این صورت معادل با $\perp$ می‌باشد. بنابراین کافی است فرمول‌های اتمی به فرم $t<\mathfrak{s}^n(x)$ یا $\mathfrak{s}^n(x)<t$ یا $\mathfrak{s}^n(x)=t$ را برای هر ترم t آزاد از x و $n\in\mathbb{N}^+$ در نظر بگیریم. حال با توجه به لم **۳.۳.۱** و این نکته که در حضور $<$ نیازی به در نظر گرفتن $\neg$ نیست، فرمول زیر را حذف سور می‌کنیم:

$$\exists x(\bigwedge_{i<\ell}t_i<\mathfrak{s}^{p_i}(x)\wedge\bigwedge_{j<m}\mathfrak{s}^{q_j}(x)<s_j\wedge\bigwedge_{k<n}\mathfrak{s}^{r_k}(x)=u_k).\qquad(۵.۲)$$

قرار می‌دهیم: $N=\max\{p_i,q_j,r_k\}$. با توجه به فرمول‌های اثبات‌پذیر زیر

$$\mathfrak{s}(x)<\mathfrak{s}(y)\Leftrightarrow x<y\quad \text{و}\quad \mathfrak{s}(x)=\mathfrak{s}(y)\Leftrightarrow x=y,$$

فرمول (۵.۲) با فرمول زیر معادل است:

$$\exists x\Big(\bigwedge_{i<\ell}\mathfrak{s}^{N-p_i}(t_i)<\mathfrak{s}^N(x)\wedge\bigwedge_{j<m}\mathfrak{s}^N(x)<\mathfrak{s}^{N-q_j}(s_j)\wedge\bigwedge_{k<n}\mathfrak{s}^N(x)=\mathfrak{s}^{N-r_k}(u_k)\Big).$$

حال برای $y=\mathfrak{s}^N(x)$، $t'_i=\mathfrak{s}^{N-p_i}(t_i)$، $s'_j=\mathfrak{s}^{N-q_j}(s_j)$ و $u'_k=\mathfrak{s}^{N-r_k}(u_k)$ فرمول بالا معادل فرمول زیر است:

$$\exists y(\bigwedge_{i<\ell}t'_i<y\wedge\bigwedge_{j<m}y<s'_j\wedge\bigwedge_{k<n}y=u'_k\quad\wedge\quad\mathfrak{s}^N(\mathbf{0})\leqslant y).$$

پس کافی است فرمول‌های به صورت زیر حذف سور شوند:

$$\exists y(\bigwedge_{i<\ell}t_i<y\wedge\bigwedge_{j<m}y<s_j\wedge\bigwedge_{k<n}y=u_k).\tag{۶.۲}$$

اگر $n\neq ۰$، آنگاه فرمول (۶.۲) معادل با فرمول بدون سور زیر است:

$$\bigwedge_{i<\ell}t_i<u_۰\wedge\bigwedge_{j<m}u_۰<s_j\wedge\bigwedge_{k<n}u_۰=u_k.$$

و اگر فرض کنیم $n=۰$، آنگاه فرمول زیر باید حذف سور شود:

$$\exists y(\bigwedge_{i<\ell}t_i<y\wedge\bigwedge_{j<m}y<s_j).\tag{۷.۲}$$

حال اگر $\ell=۰$، آنگاه فرمول (۷.۲) معادل فرمول بدون سور روبرو است: $\bigwedge_{j<m}\mathbf{0}<s_j$. اگر $m=۰$، آنگاه فرمول (۷.۲) معادل $\top$ است. و اگر $\ell\neq ۰\neq m$، آنگاه فرمول (۷.۲) معادل فرمول بدون سور روبرو است: $\bigwedge_{i,j}\mathfrak{s}(t_i)<s_j$. ⊠

فصل ۳

ساختارهای مرتب جمعی اعداد

در این فصل ساختارهای مجموعه‌های $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ در زبان $\{+,<\}$ را مطالعه می‌کنیم.

۱.۳ مفاهیمی از گروه‌های مرتب

تعریف ۱.۱.۳ (گروه)**.** یک گروه، ساختاری مانند $\langle G;*,\mathsf{e},\iota\rangle$ می‌باشد که $*$ یک عملگر دوتایی روی G بوده و e یک ثابت (یک عضو خاص G) و ι یک عملگر یک‌تایی روی G است که در اصول زیر صدق می‌کنند:

$$\forall x,y,z\,[x*(y*z)=(x*y)*z];$$
$$\forall x(x*\mathsf{e}=x);$$
$$\forall x(x*\iota(x)=\mathsf{e}).$$

$\circledast$

• یک گروه نابدیهی است هرگاه

$$\exists x(x \neq \mathsf{e}).$$

تعریف ۲.۱.۳ (گروه آبلی). گروه آبلی گروهی است که اصل زیر در آن صدق کند:

$$\forall x, y(x * y = y * x).$$

⊛

تعریف ۳.۱.۳ (گروه بخش‌پذیر). گروه بخش‌پذیر گروهی است که برای $n \in \mathbb{N}$ اصل زیر در آن صدق کند:

$$\forall x \exists y[x = \underbrace{y * \cdots * y}_{n\text{–بار}}].$$

⊛

تعریف ۴.۱.۳ (گروه مرتب). گروه مرتب گروهی است با یک رابطه‌ی ترتیب $<$ (که اصول $\mathsf{O}_۱, \mathsf{O}_۲, \mathsf{O}_۳$ را ارضاء می‌کند) به طوری که اصل زیر در آن صادق است:

$$\forall x, y, z(x < y \ \rightarrow \ x * z < y * z \ \wedge \ z * x < z * y).$$

⊛

یادکرد ۵.۱.۳. اصول نظریه‌ی گروه‌های مرتب آبلی بخش‌پذیر نابدیهی در زبان $\mathcal{L} = \{<, +, -, \mathbf{0}\}$

عبارتند از:

$$(\mathtt{O}_1)\quad \forall x,y(x<y\to y\not< x)$$

$$(\mathtt{O}_2)\quad \forall x,y,z(x<y<z\to x<z)$$

$$(\mathtt{O}_3)\quad \forall x,y(x<y\vee x=y\vee y<x)$$

$$(\mathtt{A}_1)\quad \forall x,y,z\,(x+(y+z)=(x+y)+z)$$

$$(\mathtt{A}_2)\quad \forall x(x+\mathbf{0}=x)$$

$$(\mathtt{A}_3)\quad \forall x(x+(-x)=\mathbf{0})$$

$$(\mathtt{A}_4)\quad \forall x,y(x+y=y+x)$$

$$(\mathtt{A}_5)\quad \forall x,y,z(x<y\to x+z<y+z)$$

$$(\mathtt{A}_6)\quad \exists y(y\neq\mathbf{0})$$

$$(\mathtt{A}_7)\quad \forall x\exists y(x=n\centerdot y)\qquad n\in\mathbb{N}^+$$

⌖

۲.۳ اعداد گویا و حقیقی با ترتیب و جمع

۱.۲.۳ حذف سور گستره‌های $\langle\mathbb{R};<,+\rangle$ و $\langle\mathbb{Q};<,+\rangle$

قضیه ۱.۲.۳ (نتیجه‌ی 3.1.17 از مرجع [۱۱]). نظریه‌ی نامتناهی گروه‌های آبلی بخش‌پذیر مرتب نابدیهی (که شامل اصول $\{\mathtt{O}_1,\mathtt{O}_2,\mathtt{O}_3,\mathtt{A}_1,\mathtt{A}_2,\mathtt{A}_3,\mathtt{A}_4,\mathtt{A}_5,\mathtt{A}_6,\mathtt{A}_7\}$ می‌باشد)، به طور کامل نظریه‌ی ترتیبی و جمعی اعداد حقیقی و اعداد گویا را اصل‌بندی می‌کند. همچنین نظریه ساختارهای $\langle\mathbb{R};<,+,-,\mathbf{0}\rangle$ و $\langle\mathbb{Q};<,+,-,\mathbf{0}\rangle$ حذف سور می‌پذیرند و بنابراین دارای نظریه‌هایی تصمیم‌پذیر هستند.

برهان. ابتدا توجه می‌کنیم که $\mathtt{O}_4$، $\mathtt{O}_5$ و $\mathtt{O}_6$ از اصول فوق نتیجه می‌شوند: اگر $a<b$، در این صورت بنا بر اصل $\mathtt{A}_7$ عددی مانند c وجود دارد که $c+c=a+b$. می‌توان نشان داد

که $a < c < b$؛ پس اصل $\mathtt{O}_۴$ اثبات می‌شود. برای اثبات $\mathtt{O}_۵$، با توجه به اصل $\mathtt{A}_۵$، برای هر $a > 0$ داریم: $a < a + a$. دوگان بحث فوق اصل $\mathtt{O}_۶$ را اثبات می‌کند. همچنین رابطه‌های

$$(i) \quad [a < b] \leftrightarrow [n \centerdot a < n \centerdot b]$$
$$(ii) \quad [a = b] \leftrightarrow [n \centerdot a = n \centerdot b]$$

توسط اصول اثبات می‌شوند: (i) با توجه به اصل $\mathtt{A}_۵$ (همراه با اصول $\mathtt{O}_۱$، $\mathtt{O}_۲$ و $\mathtt{O}_۳$) اثبات می‌شود. با توجه به رابطه‌ی $\forall x(n \centerdot x = \mathbf{0} \to x = \mathbf{0})$ که از اصول فوق نتیجه می‌شود، (ii) نیز اثبات می‌شود.

اکنون هر ترم شامل x را می‌توان به صورت $n \centerdot x + t$ برای هر ترم t آزاد از x و $n \in \mathbb{Z} - \{0\}$ نوشت. بنابراین هر فرمول اتمی شامل x معادل با $n \centerdot x \square t$ می‌باشد که $\square \in \{=, <, >\}$. که از آنجا با توجه به لم ۳.۳.۱ کافی است ثابت شود که فرمول

$$\exists x(\bigwedge_{i<\ell} t_i < p_i \centerdot x \wedge \bigwedge_{j<m} q_j \centerdot x < s_j \wedge \bigwedge_{k<n} r_k \centerdot x = u_k) \qquad (۱.۳)$$

با یک فرمول بدون سور معادل است. توسط رابطه‌های (i) و (ii) می‌توانیم همه‌ی p_iها، q_jها و r_kها را در فرمول (۱.۳) برابر α فرض کنیم. در این صورت با توجه به اصل $\mathtt{A}_۷$ فرمول (۱.۳) با فرمول

$$\exists y(\bigwedge_{i<\ell} t'_i < y \wedge \bigwedge_{j<m} y < s'_j \wedge \bigwedge_{k<n} y = u'_k) \qquad (۲.۳)$$

برای ترم‌های جدید t'_i, s'_j, u'_k و $y = \alpha \centerdot x$ معادل است.

حال اگر $n \neq 0$، آنگاه فرمول (۲.۳) معادل با فرمول بدون سور زیر است:

$$\bigwedge_{i<\ell} t'_i < u_\circ \wedge \bigwedge_{j<m} u_\circ < s'_j \wedge \bigwedge_{k<n} u_\circ = u'_k.$$

بنابراین فرض می‌کنیم $n = 0$. در این صورت اگر $m = 0$ یا $\ell = 0$ آنگاه به ترتیب با توجه به اصول O_5 و O_6 (و نیز O_2 و O_3) فرمول (۲.۳) معادل با فرمول بدون سور $\top$ می‌باشد و اگر $\ell, m \neq 0$، آنگاه با توجه به O_4 (و نیز O_2 و O_3) با فرمول بدون سور $\bigwedge_{i<\ell,j<m} t'_i < s'_j$ معادل است (با اثبات قضیه‌ی ۱۱.۱.۲ مقایسه شود). ⊠

۲.۲.۳ اصل‌ناپذیری متناهی ساختارهای $\langle \mathbb{R}; <, + \rangle$ و $\langle \mathbb{Q}; <, + \rangle$

گزاره ۲.۲.۳. ساختارهای $\langle \mathbb{R}; <, + \rangle$ و $\langle \mathbb{Q}; <, + \rangle$ به طور متناهی اصل‌پذیر نمی‌باشند.

برهان. برای عدد طبیعی به اندازه‌ی کافی بزرگ N زیرمجموعه‌ی زیر از اعداد گویا

$$\mathbb{Q}/N! = \{m/(N!)^k \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$$

را در نظر می‌گیریم که در آن $N! = 2 \times 3 \times \cdots \times N$. این مجموعه تحت عمل جمع بسته می‌باشد و اصول O_1، O_2، O_3، A_1، A_2، A_3، A_4، A_5، A_6 و تعدادی متناهی مورد از اصل A_7 (برای $n = 1, \cdots, N$) را ارضاء می‌کند. اما برای $n = p$ که p عدد اولی بزرگ‌تر از $N!$ است، این مجموعه اصل A_7 را ارضاء نمی‌کند. ⊠

۳.۳ باقی‌مانده‌های چینی

برای حذف سور ساختار $\langle \mathbb{Z}; <, + \rangle$ روابط (دوتایی) هم‌نهشتی $\{\equiv_n\}_{n\geqslant ۲}$ (به پیمانه‌ی اعداد طبیعی استاندارد) را به زبان اضافه می‌کنیم؛ توجه می‌کنیم که فرمول $a \equiv_n b$ معادل با $\exists x(a+n\centerdot x=b)$ می‌باشد. درباره‌ی این روابط هم‌نهشتی، قضایای باقی‌مانده‌ی چینی مفید خواهند بود.

قضیه‌ی باقی‌مانده‌ی چینی برای اولین بار در چین باستان در اولین قرن بعد از میلاد ظاهر شد. این قضیه ابزار مهمی در محاسبات نجومی و تعیین مناسبات مذهبی (محاسبات تقویمی) بوده است. همچنین از آن به عنوان منبعی برای طرح معماهای ریاضی استفاده شده است. در جبر قضیه‌ی باقی‌مانده‌ی چینی به صورت یکریختی یک تصویر همیومورفیک حلقه‌ای از یک نوع با حاصل ضرب دو تصویر همیومورفیک همان حلقه بیان می‌شود. دانشمندان علوم کامپیوتر از این قضیه برای حصول دقت چند برابر استفاده کرده‌اند. این قضیه همچنین در منطق برای کد گذاری دنباله‌های متناهی و رمز نگاری به کار می‌رود. برای بیان قضیه‌ی باقی‌مانده‌ی چینی دانستن اندکی نظریه‌ی مقدماتی اعداد یا مقدماتی از جبر مجرد مانند «هم‌نهشتی» و مفاهیمی مربوط به «اول بودن نسبی اعداد» لازم است.

۱.۳.۳ قضیه‌ی بزو

لم ۱.۳.۳ (قضیه بزو[1]). برای دو عدد صحیح a و b که حداقل یکی از آنها مخالف صفر است، اگر d بزرگ‌ترین مقسوم‌علیه مشترک آن‌ها باشد، آن‌گاه دو عدد صحیح m و n چنان وجود دارند که

$$d = ma + nb.$$

[1] Bézout's Identity

برهان. مجموعه‌ی همه‌ی ترکیب‌های خطی مثبت a و b را به صورت زیر در نظر می‌گیریم:

$$A = \{sa + tb \mid s, t \in \mathbb{Z}, \quad sa + tb > 0\}.$$

مجموعه‌ی A ناتهی است و چون همه‌ی اعضای آن مثبت می‌باشند، دارای کوچک‌ترین عضو می‌باشد. این عضو را d می‌نامیم. بنابراین اعداد صحیحی مانند s' و t' وجود دارند به طوری که $d = s'a + t'b$. عدد d مقسوم علیه مشترک a و b می‌باشد زیرا در غیر این صورت بنا به الگوریتم تقسیم با تقسیم a بر d اعداد صحیح q و r $(0 \leq r < d)$ وجود دارند به طوری که $a = dq + r$. از طرفی داریم:

$$r = a - dq = a - (s'a + t'b)q = a - as'q - bt'q = a(1 - s'q) + b(-t'q).$$

بنابراین r در صورت مثبت بودن عضوی از مجموعه‌ی A خواهد بود که کمتر از d می‌باشد که این تناقض است. بنابراین $r = 0$ و این یعنی d مقسوم علیه a می‌باشد. به همین ترتیب d مقسوم علیه b نیز می‌باشد.

حال کافی است نشان دهیم d بزرگ‌ترین مقسوم علیه مشترک a و b است. برای این منظور فرض کنید d' بزرگ‌ترین مقسوم علیه مشترک a و b باشد، در این صورت چون a و b بر d' بخش‌پذیر هستند پس هر ترکیب خطی آن‌ها نیز به ویژه $d = s'a + t'b$ بر d' بخش‌پذیر است. یعنی d از d' کوچک‌تر نیست پس برابر خود d' است. ⊠

۲.۳.۳ قضیه‌ی باقی‌مانده‌ی چینی

گزاره ۲.۳.۳ (قضیه‌ی باقی‌مانده‌ی چینی). برای اعداد صحیح $n_0, n_1, \cdots, n_k \geqslant 2$ که دو به دو نسبت به هم اولند و اعداد صحیح $t_0, t_1, \cdots, t_k$، عدد صحیح xای وجود دارد به طوری که برای $i = 0, 1, \cdots, k$ داریم: $x \equiv_{n_i} t_i$.

برهان. قرار می‌دهیم $m = n_0 n_1 \cdots n_k$. چون اعداد صحیح $n_0, n_1, \cdots, n_k$ دو به دو نسبت به هم اولند، داریم:

$$\begin{cases} (n_0, \frac{m}{n_0}) = 1 \\ (n_1, \frac{m}{n_1}) = 1 \\ \quad \vdots \\ (n_k, \frac{m}{n_k}) = 1 \end{cases} \tag{۳.۳}$$

با توجه به لم ۱.۳.۳ و رابطه‌ی (۳.۳) اعداد صحیح $c_0, c_1, \cdots, c_k$ و $d_0, d_1, \cdots, d_k$ وجود دارند به طوری که

$$\begin{cases} c_0 n_0 + d_0 \frac{m}{n_0} = 1 \\ c_1 n_1 + d_1 \frac{m}{n_1} = 1 \\ \quad \vdots \\ c_k n_k + d_k \frac{m}{n_k} = 1 \end{cases} \tag{۴.۳}$$

نشان می‌دهیم که

$$x = \sum_{i=0}^{k} d_i t_i \frac{m}{n_i}$$

جواب مطلوب است.

برای $j = ۰, ۱, \cdots, k$ داریم:

$$x = d_j t_j \frac{m}{n_j} + \sum_{i \neq j} d_i t_i \frac{m}{n_i}$$

با توجه به (۴.۳)

$$= t_j(۱ - c_j n_j) + \sum_{i \neq j} d_i t_i \frac{m}{n_i}$$

$$= t_j + n_j(-t_j c_j + \sum_{i \neq j} d_i t_i \frac{m}{n_j n_i})$$

و این یعنی $x \equiv_{n_j} t_j$ برای $j = ۰, ۱, \cdots, k$ برقرار است. ⊠

۳.۳.۳ قضیه‌ی باقی‌مانده‌ی چینی تعمیم‌یافته

لم ۳.۳.۳. برای اعداد صحیح $n_۰, n_۱, \cdots, n_{k+۱}$ داریم:

$$n_{k+۱} \wedge (n_۰ \vee n_۱ \vee \cdots \vee n_k) = (n_{k+۱} \wedge n_۰) \vee (n_{k+۱} \wedge n_۱) \vee \cdots \vee (n_{k+۱} \wedge n_k)$$

که در آن $n_i \vee n_j = \max\{n_i, n_j\}$ و $n_i \wedge n_j = \min\{n_i, n_j\}$ می‌باشند.

برهان. ابتدا قرار می‌دهیم:

$\alpha = n_{k+۱} \wedge (n_۰ \vee n_۱ \vee \cdots \vee n_k)$ و $\beta = (n_{k+۱} \wedge n_۰) \vee (n_{k+۱} \wedge n_۱) \vee \cdots \vee (n_{k+۱} \wedge n_k)$.

بدون از دست دادن کلیت فرض می‌کنیم $n_۰ \geqslant n_۱ \geqslant \cdots \geqslant n_k$. سه حالت زیر را تشخیص می‌دهیم:

(الف) $n_{k+1} \geqslant n_{0}$، که در این صورت

$$\alpha = n_{0} = \beta.$$

(ب) $n_j \geqslant n_{k+1} \geqslant n_{j+1}$ برای یک $0 \leqslant j < k$، که در این صورت

$$\alpha = n_{k+1} = \beta.$$

(ج) $n_k \geqslant n_{k+1}$، که در این صورت

$$\alpha = n_{k+1} = \beta.$$

⊠

لم ۴.۳.۳. برای اعداد صحیح $n_{0}, n_{1}, \cdots, n_{k+1}$، اگر n را کوچک‌ترین مضرب مشترک $n_{0}, n_{1}, \cdots, n_k$ و $d_{i,j}$ را بزرگ‌ترین مقسوم علیه مشترک n_i و n_j برای $i \neq j$ قرار دهیم، آنگاه بزرگ‌ترین مقسوم علیه مشترک n و n_{k+1} با کوچک‌ترین مضرب مشترک $d_{0,k+1}, \cdots, d_{k,k+1}$ برابر خواهد بود.

برهان. فرض می‌کنیم $\rho_{0}, \rho_{1}, \rho_{2}, \cdots$ دنباله‌ی همه‌ی اعداد اول $(2, 3, 5, \cdots)$ را نشان دهد. اگر $n_j = \prod_i \rho_i^{m_i(j)}$ برای $j = 0, 1, \cdots, k+1$، آنگاه

$$[n_{0}, n_{1}, n_{2}, \cdots, n_k] = \prod_i \rho_i^{m_i(0) \vee m_i(1) \vee \cdots \vee m_i(k)}$$

و

$$d_{j,k+1} = (n_j, n_{k+1}) = \prod_i \rho_i^{m_i(j)\wedge m_i(k+1)}.$$

پس طبق لم **۳.۳.۳** داریم:

$$\begin{aligned}
(n_{k+1}, [n_0, n_1, n_2, \cdots, n_k]) &= \prod_i \rho_i^{m_i(k+1)\wedge(m_i(0)\vee m_i(1)\vee\cdots\vee m_i(k))} \\
&= \prod_i \rho_i^{(m_i(k+1)\wedge m_i(0))\vee(m_i(k+1)\wedge m_i(1))\vee\cdots\vee(m_i(k+1)\wedge m_i(k))} \\
&= [(n_0, n_{k+1}), (n_1, n_{k+1}), \cdots, (n_k, n_{k+1})] \\
&= [d_{0,k+1}, d_{1,k+1}, \cdots, d_{k,k+1}]
\end{aligned}$$

⊠

گزاره ۵.۳.۳ **(قضیه‌ی باقی‌مانده‌ی چینی تعمیم‌یافته [۸]).** برای اعداد صحیح $t_0, t_1, \cdots, t_k$ و $2 \leqslant n_0, n_1, \cdots, n_k$ داریم:

$$\exists x(\bigwedge_{i=0}^{k} x \equiv_{n_i} t_i) \iff \bigwedge_{0\leqslant i<j\leqslant k} t_i \equiv_{d_{i,j}} t_j$$

که در آن $d_{i,j}$ بزرگ‌ترین مقسوم‌علیه مشترک n_i و n_j برای $i \neq j$ می‌باشد.

برهان. برای اثبات قسمت «تنها اگر» فرض کنیم برای اعداد صحیح $2 \leqslant n_0, n_1, \cdots, n_k$ و $t_0, t_1, \cdots, t_k$، عدد صحیح xای وجود دارد به طوری که برای $i = 0, 1, \cdots, k$ رابطه‌ی $x \equiv_{n_i} t_i$ برقرار می‌باشد. با توجه به روابط $d_{i,j} \mid n_i$ و $d_{i,j} \mid n_j$ برای $i \neq j$، خواهیم داشت:

$$x \equiv_{d_{i,j}} t_j \quad \text{و} \quad x \equiv_{d_{i,j}} t_i.$$

و بنابراین $t_i \equiv_{d_{i,j}} t_j$.

حال قسمت «اگر» را با استقرا بر روی k ثابت می‌کنیم. برای $k = 0$ حکم بدیهی است. برای $k = 1$ با توجه به لم **۱.۳.۳** اعداد صحیح a_0 و a_1 وجود دارند به طوری که

$$a_0 n_0 + a_1 n_1 = d_{0,1}. \tag{۵.۳}$$

همچنین با توجه به فرض مساله عدد صحیحی مانند c وجود دارد که

$$t_0 - t_1 = c d_{0,1}. \tag{۶.۳}$$

حال اگر x را برابر $a_0(n_0/d_{0,1})t_1 + a_1(n_1/d_{0,1})t_0$ قرار دهیم، با توجه به **(۵.۳)** و **(۶.۳)** خواهیم داشت:

$$x = t_0 - a_0 n_0 c \quad \text{و} \quad x = t_1 + a_1 n_1 c.$$

و بنابراین روابط زیر برقرارند:

$$x \equiv_{n_0} t_0 \quad \text{و} \quad x \equiv_{n_1} t_1.$$

برای مرحله‌ی $(k+1)$–ام استقرا توجه می‌کنیم که طبق فرض، رابطه‌ی $t_i \equiv_{d_{i,j}} t_j$ برای $0 \leqslant i < j \leqslant k+1$ درست است و فرض می‌کنیم برای یک عدد صحیح x روابط زیر برقرار باشند (فرض استقرا):

$$\begin{cases} x \equiv_{n_0} t_0 \\ x \equiv_{n_1} t_1 \\ \quad \vdots \\ x \equiv_{n_k} t_k \end{cases} \tag{۷.۳}$$

فرض کنیم n کوچک‌ترین مضرب مشترک اعداد صحیح $n_0, n_1, \cdots, n_k$ باشد. اگر m را بزرگ‌ترین مقسوم علیه مشترک n و n_{k+1} بگیریم، بنا به لم **۴.۳.۳**، m با کوچک‌ترین مضرب مشترک $d_{0,k+1}, \cdots, d_{k,k+1}$ برابر خواهد بود.
حال با توجه به رابطه‌ی (۷.۳) داریم:

$$\begin{cases} x \equiv_{d_{0,k+1}} t_0 \\ x \equiv_{d_{1,k+1}} t_1 \\ \quad \vdots \\ x \equiv_{d_{k,k+1}} t_k \end{cases} \tag{۸.۳}$$

با توجه به فرض داریم:

$$\begin{cases} t_0 \equiv_{d_{0,k+1}} t_{k+1} \\ t_1 \equiv_{d_{1,k+1}} t_{k+1} \\ \quad \vdots \\ t_k \equiv_{d_{k,k+1}} t_{k+1} \end{cases} \tag{۹.۳}$$

با توجه به روابط (۸.۳) و (۹.۳) داریم:

$$\begin{cases} x \equiv_{d_{0,k+1}} t_{k+1} \\ x \equiv_{d_{1,k+1}} t_{k+1} \\ \quad\vdots \\ x \equiv_{d_{k,k+1}} t_{k+1} \end{cases} \tag{۱۰.۳}$$

از رابطه‌ی (۱۰.۳) رابطه‌ی $x \equiv_m t_{k+1}$ نتیجه می‌شود و بنابراین برای یک عدد صحیح c داریم:

$$x - t_{k+1} = mc. \tag{۱۱.۳}$$

با توجه به لم (۱.۳.۳) اعداد صحیحی مانند a و b وجود دارند به طوری که

$$an + bn_{k+1} = m. \tag{۱۲.۳}$$

حال با توجه به روابط (۱۱.۳) و (۱۲.۳) برای $y = x - anc$ داریم:

$$y = t_{k+1} + bn_{k+1}c \equiv_{n_{k+1}} t_{k+1}.$$

همچنین رابطه‌ی $y \equiv_{n_i} x \equiv_{n_i} t_i$ برای $0 \leqslant i \leqslant k$ برقرار است. این همان نتیجه‌ی مطلوب است. ⊠

۴.۳ اعداد صحیح با ترتیب و جمع

۱.۴.۳ حذف سور گستره‌ی $\langle \mathbb{Z}; <, + \rangle$

قضیه‌ی **۳.۴.۳** در مراجع زیر به شکل‌های گوناگون اثبات شده است:

بخش 4 (فصل III) از مرجع [۱۹]، قضیه‌ی 13.10 از مرجع [۱۲]، نتیجه‌ی 3.1.21 از مرجع [۱۱]، بخش III (فصل 4) از مرجع [۱۰]، نتیجه‌ی 2.5.18 از مرجع [۹]، قضیه‌ی 32E از مرجع [۷] و فصل 24 از مرجع [۳].

• ما در اینجا اثباتی خواهیم آورد که اندکی متفاوت است.

یادکرد ۱.۴.۳ . اصول نظریه‌ی گروه‌های آبلی مرتب باقی‌مانده‌دار گسسته‌ی نابدیهی عبارتند از:

$$(\mathtt{O}_1) \quad \forall x, y(x < y \to y \not< x)$$

$$(\mathtt{O}_2) \quad \forall x, y, z(x < y < z \to x < z)$$

$$(\mathtt{O}_3) \quad \forall x, y(x < y \vee x = y \vee y < x)$$

$$(\mathtt{A}_1) \quad \forall x, y, z\,(x + (y + z) = (x + y) + z)$$

$$(\mathtt{A}_2) \quad \forall x(x + \mathbf{0} = x)$$

$$(\mathtt{A}_3) \quad \forall x(x + (-x) = \mathbf{0})$$

$$(\mathtt{A}_4) \quad \forall x, y(x + y = y + x)$$

$$(\mathtt{A}_5) \quad \forall x, y, z(x < y \to x + z < y + z)$$

$$(\mathtt{O}^{\circ}_{\vee}) \quad \forall x, y\big(x < y \leftrightarrow x + \mathbf{1} \leqslant y\big)$$

$$(\mathtt{A}^{\circ}_{\vee}) \quad \forall x \exists y\,\big(\mathbb{W}_{i<n}\, x = n \centerdot y + \bar{i}\,\big) \qquad n \in \mathbb{N}^{+}, \quad \bar{i} = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{i\text{–بار}}$$

⟡

گزاره ۲.۴.۳ . نظریه‌ی ساختار $\langle \mathbb{Z}; <, +, -, \mathbf{0}, \mathbf{1} \rangle$ حذف سور نمی‌پذیرد.

برهان. برای اثبات کافی است نشان دهیم که $\exists x(x+x=y)$ با هیچ فرمول بدون سوری معادل نیست. همه‌ی ترم‌های شامل متغیر y در زبان $\langle +,-,\mathbf{0},\mathbf{1}\rangle$ برابر $m.y$ برای یک $m\in\mathbb{Z}$ هستند، پس همه‌ی فرمول‌های اتمی $\langle \mathbb{Z};<,+,-,\mathbf{0},\mathbf{1}\rangle$ به صورت $m.y=k$ یا $m.y>k$ یا $m.y<k$ برای $m,k\in\mathbb{Z}$ می‌باشند. پس به راحتی می‌توان دید که مجموعه‌های تعریف‌پذیر ساختار فوق همگی متناهی یا مکمل‌ـ متناهی هستند، در حالی‌که مجموعه‌ی $\{y\in\mathbb{Z}|\exists x(x+x=y)\}$ نه متناهی است نه مکمل‌ـ متناهی. ⊠

قضیه ۳.۴.۳. نظریه‌ی نامتناهی گروه‌های آبلی مرتب باقی‌مانده‌دار گسسته‌ی نابدیهی (که شامل اصول $\{\mathsf{O}_۱,\mathsf{O}_۲,\mathsf{O}_۳,\mathsf{A}_۱,\mathsf{A}_۲,\mathsf{A}_۳,\mathsf{A}_۴,\mathsf{A}_۵,\mathsf{O}_۷^\circ,\mathsf{A}_۷^\circ\}$ می‌باشد)، به طور کامل نظریه‌ی ترتیبی و جمعی اعداد صحیح را اصل‌بندی می‌کند. همچنین ساختار $\langle \mathbb{Z};<,+,-,\mathbf{0},\mathbf{1},\{\equiv_n\}_{n\geqslant ۲}\rangle$ حذف سور می‌پذیرد و بنابراین دارای نظریه‌ی تصمیم‌پذیر است.

برهان. اصل $\mathsf{A}_۷^\circ$ فرمول زیر را نتیجه می‌دهد:

$$\forall x \bigvee_{i<n}\big(x\equiv_n \bar{i}\wedge \bigwedge_{i\neq j<n} x\not\equiv_n \bar{j}\big),$$

و بنابراین علامت‌های نقیض پشت هم‌نهشتی‌ها توسط رابطه‌ی زیر حذف می‌شوند:

$$(a\not\equiv_n b)\leftrightarrow \bigvee_{\circ<i<n}(a\equiv_n b+\bar{i}\,).$$

از آنجایی که هر ترم شامل x را می‌توان به صورت $n\,.\,x+t$ برای هر ترم t آزاد از x و $n\in\mathbb{Z}-\{\circ\}$ نوشت، بنابراین هر فرمول اتمی شامل x معادل با $n\,.\,x\Box t$ می‌باشد که

$\square\in\{=,<,>,\{\equiv_n\}_{n\geqslant ۲}\}$. بنابراین با توجه به لم ۳.۳.۱ کافی است ثابت شود که فرمول

$$\exists x(\bigwedge_{i<m} a_i \cdot x \equiv_{n_i} t_i \ \wedge \ \bigwedge_{j<p} u_j < b_j \cdot x \ \wedge \ \bigwedge_{k<q} c_k \cdot x < v_k \ \wedge \ \bigwedge_{\ell<r} d_\ell \cdot x = w_\ell) \quad (۱۳.۳)$$

با یک فرمول بدون سور معادل است، که در آن a_iها، b_jها، c_kها و d_ℓها اعداد طبیعی و t_iها، u_jها، v_kها و w_ℓ ها ترم‌های آزاد از x هستند.

با توجه به روابط

$$(i) \quad [a<b] \leftrightarrow [n \cdot a < n \cdot b]$$
$$(ii) \quad [a=b] \leftrightarrow [n \cdot a = n \cdot b]$$
$$(iii) \quad [a \equiv_m b] \leftrightarrow [n \cdot a \equiv_{nm} n \cdot b]$$

که از اصول نتیجه می‌شوند، می‌توانیم همه‌ی a_iها، b_jها، c_kها و d_ℓها را در فرمول (۱۳.۳) برابر α فرض کنیم. در این صورت فرمول (۱۳.۳) با فرمول

$$\exists y(y \equiv_\alpha \mathbf{0} \ \wedge \ \bigwedge_{i<m} y \equiv_{n_i} t'_i \ \wedge \ \bigwedge_{j<p} u'_j < y \ \wedge \ \bigwedge_{k<q} y < v'_k \ \wedge \ \bigwedge_{\ell<r} y = w'_\ell) \quad (۱۴.۳)$$

برای ترم‌های جدید $t'_i, u'_j, v'_k, w'_\ell$ و $y=\alpha \cdot x$ معادل است.

حال اگر $r \neq ۰$، آنگاه فرمول (۱۴.۳) با جانشینی $w'_۰$ به جای y، معادل با یک فرمول بدون سور است. بنابراین کافی است فرمول زیر حذف سور شود:

$$\exists x(\bigwedge_{i<m} x \equiv_{n_i} t_i \ \wedge \ \bigwedge_{j<p} u_j < x \ \wedge \ \bigwedge_{k<q} x < v_k). \quad (۱۵.۳)$$

اکنون توجه می‌کنیم که فرمول $\exists x(\theta(x) \wedge u_0 < x \wedge u_1 < x)$ با فرمول زیر معادل است:

$$\left[\exists x(\theta(x)\wedge u_0 < x)\wedge u_1 \leqslant u_0\right]\vee\left[\exists x(\theta(x)\wedge u_1 < x)\wedge u_0 \leqslant u_1\right].$$

پس می‌توانیم فرض کنیم $p \leqslant 1$ (و بنابراین با توجه به بحث دوگان، $q \leqslant 1$). همچنین با توجه به گزاره‌ی **۵.۳.۳**، فرمول زیر

$$\exists x(\theta(x) \wedge x \equiv_{n_0} t_0 \wedge x \equiv_{n_1} t_1)$$

با دو x–هم‌نهشتی، معادل فرمول زیر

$$\exists x(\theta(x) \wedge x \equiv_n t) \wedge t_0 \equiv_d t_1$$

با یک x–هم‌نهشتی می‌باشد، که در آن d بزرگ‌ترین مقسوم‌علیه مشترک n_0 و n_1، عدد n کوچک‌ترین مضرب مشترک آن‌ها و $t = a_0(n_0/d)t_1 + a_1(n_1/d)t_0$ می‌باشند (با توجه به اثبات گزاره‌ی **۵.۳.۳**، a_0 و a_1 اعداد در اتحاد بزو $a_0 n_0 + a_1 n_1 = d$ صدق می‌کنند). بنابراین به همین ترتیب می‌توانیم فرض کنیم $m \leqslant 1$.
حال اگر $m = 0$، فرمول (**۱۵.۳**) با توجه به قضیه‌ی **۱۶.۱.۲** معادل با یک فرمول بدون سور خواهد بود (با در نظر گرفتن $\mathfrak{s}(x) = x + \mathbf{1}$ به همان شکلی که فرمول (**۴.۲**) معادل با یک فرمول بدون سور شد).
بنابراین فرض کنیم $m = 1$. در این حالت، اگر p یا q برابر ۰ باشند، آنگاه فرمول (**۱۵.۳**) معادل با $\top$ می‌باشد (زیرا هر هم‌نهشتی می‌تواند جواب‌های بی‌نهایت بزرگ یا بی‌نهایت کوچک داشته باشد).

سرانجام اگر $p = q = 1 = m$، آنگاه فرمول $\exists x(x \equiv_n t \wedge u<x \wedge x<v)$ معادل با فرمول $\exists y(r < n \cdot y \leqslant s)$ برای $x = t + n \cdot y$، $r = u - t$ و $s = v - t - 1$ می‌باشد. حال فرمول $\exists y(r < n \cdot y \leqslant s)$ معادل با فرمول بدون سور $\mathbb{W}_{i<n}(s \equiv_n \bar{i} \wedge r + \bar{i} < s)$ است. زیرا برای اعداد صحیح q و $i < n$ که $s = qn + i$، وجود yای که در رابطه‌ی $r < n \cdot y \leqslant s$ صدق کند، معادل با $r < nq \,(= s - i)$ می‌باشد. ⊠

۲.۴.۳ اصل‌ناپذیری متناهی ساختار $\langle \mathbb{Z}; <, + \rangle$

گزاره ۴.۴.۳. نظریه‌ی ساختار $\langle \mathbb{Z}; <, + \rangle$ به طور متناهی اصل‌پذیر نیست.

برهان. نشان می‌دهیم اصول $\mathtt{O}_1$، $\mathtt{O}_2$، $\mathtt{O}_3$، $\mathtt{A}_1$، $\mathtt{A}_2$، $\mathtt{A}_3$، $\mathtt{A}_4$، $\mathtt{A}_5$، $\mathtt{O}^\circ_7$ و تعداد متناهی مورد از اصل $\mathtt{A}^\circ_7$ نمی‌توانند همه‌ی موارد اصل $\mathtt{A}^\circ_7$ را اثبات کنند. برای این منظور عدد اول $\mathfrak{p}$ را به اندازه‌ی کافی بزرگ فرض می‌کنیم و قرار می‌دهیم $N = (\mathfrak{p} - 1)!$. مجموعه‌ی (ذکر شده در گزاره‌ی **۲.۲.۳**) $\mathbb{Q}/N = \{m/N^k \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$ تحت اعمال جمع و $x \mapsto x/n$ برای هر $1 < n < \mathfrak{p}$ بسته می‌باشد. مجموعه‌ی $\mathcal{A} = (\mathbb{Q}/N) \times \mathbb{Z}$ را در نظر می‌گیریم و روی آن ساختار $\mathfrak{A} = \langle \mathcal{A}; <_{\mathfrak{A}}, +_{\mathfrak{A}}, -_{\mathfrak{A}}, 0_{\mathfrak{A}}, 1_{\mathfrak{A}} \rangle$ را به صورت زیر تعریف می‌کنیم:

$$
\begin{aligned}
&(<_{\mathfrak{A}}): \quad (a, \ell) <_{\mathfrak{A}} (b, m) \iff (a < b) \vee (a = b \wedge \ell < m);\\
&(+_{\mathfrak{A}}): \quad (a, \ell) +_{\mathfrak{A}} (b, m) = (a + b, \ell + m);\\
&(-_{\mathfrak{A}}): \quad -_{\mathfrak{A}}(a, \ell) = (-a, -\ell);\\
&(\,\mathbf{0}_{\mathfrak{A}}\,): \quad \mathbf{0}_{\mathfrak{A}} = (\mathbf{0}, \mathbf{0});\\
&(\,\mathbf{1}_{\mathfrak{A}}\,): \quad \mathbf{1}_{\mathfrak{A}} = (\mathbf{0}, \mathbf{1}).
\end{aligned}
$$

مشاهده می‌کنیم که $\mathfrak{A}$ اصول $\mathtt{O}_1$، $\mathtt{O}_2$، $\mathtt{O}_3$، $\mathtt{A}_1$، $\mathtt{A}_2$، $\mathtt{A}_3$، $\mathtt{A}_4$، $\mathtt{A}_5$ و $\mathtt{O}^\circ_7$ را ارضاء می‌کند؛ اما اصل $\mathtt{A}^\circ_7$ را برای $n = \mathfrak{p}$ ارضاء نمی‌کند زیرا تساوی $\mathfrak{p} \cdot (a, \ell) + \bar{i} = (\mathbf{1}, \mathbf{0})$ برای یک

$a \in \mathbb{Q}/N$، $\ell \in \mathbb{Z}$ و $i \in \mathbb{N}$ $(i < \mathfrak{p})$ ایجاب می‌کند که $a = ۱/\mathfrak{p}$ در حالی که $۱/\mathfrak{p} \notin \mathbb{Q}/N$.
با این حال، $\mathfrak{A}$ تعداد متناهی از موارد اصل $\mathtt{A}^{\circ}_{۷}$ را ارضاء می‌کند (برای $۱ < n < \mathfrak{p}$): برای هر عضو دلخواه $(a,\ell) \in \mathcal{A}$ داریم: $a = m/N^k$ که $m \in \mathbb{Z}$، $k \in \mathbb{N}$ و طبق الگوریتم تقسیم رابطه‌ی $\ell = nq + r$ برای اعداد صحیح q و r که $۰ \leqslant r < n$، برقرار است. حال رابطه‌ی $(a,\ell) = n \centerdot (m'/N^{k+۱}, q) +_{\mathfrak{A}} (۰, r)$ برقرار است جایی که $m' = m \cdot (N/n) \in \mathbb{Z}$. بنابراین $(a,\ell) = n \centerdot (m'/N^{k+۱}, q) +_{\mathfrak{A}} \bar{r}$ که در آن داریم: $\bar{r} = \underbrace{\mathbf{1}_{\mathfrak{A}} +_{\mathfrak{A}} \cdots +_{\mathfrak{A}} \mathbf{1}_{\mathfrak{A}}}_{r\text{–بار}}$. ⊠

۵.۳ اعداد طبیعی با ترتیب و جمع

اصول زیر را در نظر بگیرید:

$(\mathtt{O}_۱)$ $\forall x, y(x < y \to y \not< x)$

$(\mathtt{O}_۲)$ $\forall x, y, z(x < y < z \to x < z)$

$(\mathtt{O}_۳)$ $\forall x, y(x < y \vee x = y \vee y < x)$

$(\mathtt{O}_۷)$ $\forall x, y(x<y \ \leftrightarrow\ x + \mathbf{1}<y \vee x + \mathbf{1}=y)$

$(\mathtt{O}^{\circ}_۸)$ $\forall x \exists y(x \neq \mathbf{0} \to y + \mathbf{1} = x)$

$(\mathtt{O}_۹)$ $\forall x(x \not< \mathbf{0})$

$(\mathtt{O}_{۱۰})$ $\forall x, y(x \leq y \leftrightarrow \exists z[z + y = y])$

$(\mathtt{A}_۱)$ $\forall x, y, z\,(x + (y + z) = (x + y) + z)$

$(\mathtt{A}_۲)$ $\forall x(x + \mathbf{0} = x)$

$(\mathtt{A}_۴)$ $\forall x, y(x + y = y + x)$

$(\mathtt{A}_۵)$ $\forall x, y, z(x < y \to x + z < y + z)$

$(\mathtt{A}^{\circ}_۷)$ $\forall x \exists y \left(\bigvee_{i<n} x = n \centerdot y + \bar{i} \right) \qquad n \in \mathbb{N}^+, \quad \bar{i} = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{i\text{–بار}}$

۱.۵.۳ اصل‌بندی ساختار $\langle \mathbb{N}; <, + \rangle$

قضیه ۱.۵.۳. اصول بالا نظریه‌ی $\langle \mathbb{N}; <, +, \mathbf{0}, \mathbf{1} \rangle$ را به طور کامل اصل‌بندی می‌کند؛ همچنین ساختار $\langle \mathbb{N}; <, +, \mathbf{0}, \mathbf{1}, \{\equiv_n\}_{n \geqslant ۲} \rangle$ حذف سور می‌پذیرد و بنابراین دارای نظریه‌ی تصمیم‌پذیر می‌باشد.

برهان. حذف سور ساختار فوق در قضیه‌ی 32E از مرجع [۷] آمده است. ⊠

۲.۵.۳ تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{N}; <, + \rangle$

در این بخش برای اثبات تصمیم‌پذیری نظریه‌ی ترتیبی و جمعی اعداد طبیعی از ابرـ ساختار آن ($\langle \mathbb{Z}; <, + \rangle$) استفاده می‌کنیم.

نکته ۲.۵.۳. مجموعه‌ی اعداد طبیعی در ساختار $\langle \mathbb{Z}; <, + \rangle$ توسط فرمول

$$\text{“}x \in \mathbb{N}\text{”} \iff \exists y (y + y = y \wedge y \leqslant x)$$

تعریف‌پذیر است. ⊠

قضیه ۳.۵.۳. نظریه‌ی ساختار $\langle \mathbb{N}; <, + \rangle$ تصمیم‌پذیر است.

برهان. نشان می‌دهیم که تصمیم‌پذیری ساختار $\langle \mathbb{Z}; <, + \rangle$، تصمیم‌پذیری ساختار $\langle \mathbb{N}; <, + \rangle$ را نتیجه می‌دهد. فرض کنیم فرمول $\psi^{\mathbb{N}}$ در زبان $\{<, +\}$ از فرمول ψ توسط جانشین کردن هر زیرفرمول $\forall x \theta(x)$ با $\forall x[\text{“}x \in \mathbb{N}\text{”} \to \theta(x)]$ و $\exists x \theta(x)$ با $\exists x[\text{“}x \in \mathbb{N}\text{”} \wedge \theta(x)]$ به دست آید. در این صورت با توجه به نکته‌ی **۲.۵.۳** داریم:

$$\langle \mathbb{N}; <, + \rangle \models \psi \iff \langle \mathbb{Z}; <, + \rangle \models \psi^{\mathbb{N}}.$$

بنابراین نظریه‌ی ساختار $\langle \mathbb{N}; <, + \rangle$ تصمیم‌پذیر است. ⊠

فصل ۴

ساختارهای مرتب ضربی اعداد

در این فصل نظریه‌های مجموعه‌ی اعداد $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ را در زبان $\{<,\times\}$ بررسی می‌کنیم.

۱.۴ اعداد طبیعی با ترتیب و ضرب

۱.۱.۴ اصل‌ناپذیری ساختار $\langle\mathbb{N};<,\times\rangle$

گزاره ۱.۱.۴. نظریه‌ی ساختار $\langle\mathbb{N};<,\times\rangle$ تصمیم‌ناپذیر است.

برهان. ابتدا توجه می‌کنیم که عمل جمع در ساختار $\langle\mathbb{N};<,\times\rangle$ تعریف‌پذیر است، زیرا

(۱) عملگر تالی $\mathfrak{s}$ توسط رابطه‌ی $<$ تعریف‌پذیر است:

$$y=\mathfrak{s}(x) \iff x<y \wedge \neg\exists z(x<z<y)$$

(۲) و جمع توسط عملگر تالی و عمل ضرب تعریف‌پذیر است:

$$z=x+y \iff$$
$$\big[\neg\exists u(\mathfrak{s}(u)=z)\wedge x=y=z\big]\vee\big[\exists u(\mathfrak{s}(u)=z)\wedge \mathfrak{s}(z\cdot x)\cdot\mathfrak{s}(z\cdot y)=\mathfrak{s}(z\cdot z\cdot\mathfrak{s}(x\cdot y))\big].$$

(اتحاد فوق نخستین بار توسط رابینسون [۱۶] معرفی شد. همچنین برای توضیحات بیشتر می‌توانید به فصل 24 از مرجع [۳] یا تمرین 2 در صفحه‌ی 281 از مرجع [۷] مراجعه کنید). با توجه به (۱) و (۲) ساختار $\langle\mathbb{N};<,\times\rangle$ می‌تواند ساختار $\langle\mathbb{N};+,\times\rangle$ را تعبیر کند که نظریه‌ی این ساختار با توجه به قضیه‌ی ناتمامیت گودل تصمیم‌ناپذیر است. بنابراین نظریه‌ی ساختار $\langle\mathbb{N};<,\times\rangle$ نیز تصمیم‌ناپذیر است.

(برای اثبات تصمیم‌ناپذیری نظریه‌ی ساختار $\langle\mathbb{N};+,\times\rangle$ و توضیحات بیشتر می‌توانید به قضیه‌ی 17.4 از مرجع [۳]، نتیجه‌ی 35A از مرجع [۷]، قضیه‌ی 4.1.7 از مرجع [۹]، یا نتیجه‌ی 6.4 در فصل III از مرجع [۱۹] مراجعه کنید.) ⊠

نتیجه ۲.۱.۴ . ساختار $\langle\mathbb{N};<,\times\rangle$ توسط هیچ مجموعه‌ی به طور محاسبه‌پذیر قابل شمارشی نمی‌تواند اصل‌بندی شود. ⊠

۲.۴ اعداد صحیح با ترتیب و ضرب

۱.۲.۴ اصل‌ناپذیری ساختار $\langle\mathbb{Z};<,\times\rangle$

تصمیم‌ناپذیری نظریه‌ی ساختار $\langle\mathbb{N};+,\times\rangle$، تصمیم‌ناپذیری نظریه‌های ساختارهای $\langle\mathbb{Z};+,\times\rangle$ و $\langle\mathbb{Z};<,\times\rangle$ را نیز ایجاب می‌کند.

گزاره ۱.۲.۴ . نظریه‌ی ساختار $\langle\mathbb{Z};+,\times\rangle$ تصمیم‌ناپذیر است.

برهان. مجموعه‌ی اعداد طبیعی $\mathbb{N}$ توسط قضیه‌ی چهار مربع لاگرانژ در ساختار $\langle\mathbb{Z};+,\times\rangle$

تعریف‌پذیر است (قضیه‌ی 16.6 از مرجع [۱۲]):

$$u \in \mathbb{N} \iff \exists x, y, z, t\ (u = x \cdot x + y \cdot y + z \cdot z + t \cdot t)$$

بنابراین $\langle \mathbb{N}; +, \times \rangle$ در $\langle \mathbb{Z}; +, \times \rangle$ تعریف‌پذیر است، که این رابطه بنا بر قضیه‌ی ناتمامیت، تصمیم‌ناپذیری ساختار $\langle \mathbb{Z}; +, \times \rangle$ را نشان می‌دهد (قضیه‌ی 16.7 از مرجع [۱۲] یا نتیجه‌ی 8.29 در فصل III از مرجع [۱۹] را ببینید). ⊠

گزاره ۲.۲.۴. نظریه‌ی ساختار $\langle \mathbb{Z}; <, \times \rangle$ تصمیم‌ناپذیر است.

برهان. ابتدا توجه می‌کنیم که اعداد و اعمال زیر در ساختار $\langle \mathbb{Z}; <, \times \rangle$ تعریف‌پذیر هستند:

- عدد صفر:

$$u = \mathbf{0} \iff \forall x (x \cdot u = u).$$

- عدد یک:

$$u = \mathbf{1} \iff \forall x (x \cdot u = x).$$

- عدد $-\mathbf{1}$:

$$u = -\mathbf{1} \iff u \cdot u = \mathbf{1} \wedge u \neq \mathbf{1}.$$

- قرینه‌ی جمع:

$$y = -x \iff y = (-\mathbf{1}) \cdot x.$$

- تالی:

$$y = \mathfrak{s}(x) \iff x < y \wedge \neg \exists z (x < z < y).$$

- جمع:

$$z = x + y \iff [z = \mathbf{0} \wedge y = -x] \vee [z \neq \mathbf{0} \wedge \mathfrak{s}(z \cdot x) \cdot \mathfrak{s}(z \cdot y) = \mathfrak{s}(z \cdot z \cdot \mathfrak{s}(x \cdot y))].$$

تعریف زیبای دیگری برای $+$ در زبان $\{\mathfrak{s}, \times\}$ در $\mathbb{Z}$ وجود دارد (صفحه‌ی 187 از مرجع [۹]):

$$z = x + y \iff$$
$$[z \cdot \mathfrak{s}(z) = z \wedge \mathfrak{s}(x \cdot y) = \mathfrak{s}(x) \cdot \mathfrak{s}(y)] \vee [z \cdot \mathfrak{s}(z) \neq z \wedge \mathfrak{s}(z \cdot x) \cdot \mathfrak{s}(z \cdot y) = \mathfrak{s}(z \cdot z \cdot \mathfrak{s}(x \cdot y))].$$

بنابراین ساختار $\langle \mathbb{Z}; <, \times \rangle$ ساختار $\langle \mathbb{Z}; +, \times \rangle$ را نیز به نوعی شامل می‌شود، و با توجه به گزاره‌ی ۱.۲.۴ ، نظریه‌ی ساختار $\langle \mathbb{Z}; +, \times \rangle$ تصمیم‌ناپذیر است؛ پس نظریه‌ی ساختار $\langle \mathbb{Z}; <, \times \rangle$ نیز تصمیم‌ناپذیر است. ⊠

نتیجه ۳.۲.۴ . ساختار $\langle \mathbb{Z}; <, \times \rangle$ توسط هیچ مجموعه‌ی به طور محاسبه‌پذیر قابل شمارشی نمی‌تواند اصل‌بندی شود. ⊠

۳.۴ اعداد حقیقی با ترتیب و ضرب

تارسکی نشان داد که ساختار $\langle \mathbb{R}; <, +, \times \rangle$ می‌تواند به طور کامل توسط نظریه‌ی میدان‌های مرتب بسته‌ی حقیقی اصل‌بندی شود و بنابراین نظریه‌ی تصمیم‌پذیر دارد. اثبات تصمیم‌پذیری نظریه‌ی این ساختار در قضیه‌ی 7 در فصل 4 از مرجع [۱۰]، قضیه‌ی 3.3.15 از مرجع [۱۱] و قضیه‌ی 21.36 از مرجع [۱۲] موجود است.

نتیجه ۱.۳.۴ . از آنجایی که ساختار $\langle \mathbb{R}; <, \times \rangle$ مشمول در ساختار $\langle \mathbb{R}; <, +, \times \rangle$ نیز هست، نظریه‌ی ساختار $\langle \mathbb{R}; <, \times \rangle$ نیز تصمیم‌پذیر است. ⊠

• اینجا ما تصمیم‌پذیری این نظریه را مستقیماً (بدون استفاده از قضیه‌ی تارسکی) اثبات می‌کنیم و یک اصل‌بندی صریح برای آن ارایه می‌دهیم.

۱.۳.۴ اصل‌بندی و حذف سور گستره‌ی $\langle \mathbb{R}; <, \times \rangle$

ابتدا به ساختار $\langle \mathbb{R}^+; <, \times \rangle$ توجه می‌کنیم.

گزاره ۲.۳.۴. نظریه‌ی نامتناهی زیر (مربوط به گروه‌های آبلی مرتب بخش‌پذیر نابدیهی) به طور کامل نظریه‌ی ترتیبی و ضربی اعداد حقیقی مثبت را اصل‌بندی می‌کند:

$$(\mathtt{O}_۱) \quad \forall x, y(x < y \to y \not< x)$$

$$(\mathtt{O}_۲) \quad \forall x, y, z(x < y < z \to x < z)$$

$$(\mathtt{O}_۳) \quad \forall x, y(x < y \vee x = y \vee y < x)$$

$$(\mathtt{M}_۱) \quad \forall x, y, z\,(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$$

$$(\mathtt{M}_۲) \quad \forall x(x \cdot \mathbf{1} = x)$$

$$(\mathtt{M}_۳) \quad \forall x(x \cdot x^{-۱} = \mathbf{1})$$

$$(\mathtt{M}_۴) \quad \forall x, y(x \cdot y = y \cdot x)$$

$$(\mathtt{M}_۵) \quad \forall x, y, z(x < y \to x \cdot z < y \cdot z)$$

$$(\mathtt{M}_۶) \quad \exists y(y \neq \mathbf{1})$$

$$(\mathtt{M}_۷) \quad \forall x \exists y(x = y^n) \qquad n \geqslant ۲$$

ساختار $\langle \mathbb{R}^+; <, \times, \square^{-۱}, \mathbf{1} \rangle$ حذف سور می‌پذیرد، و بنابراین نظریه‌ی آن تصمیم‌پذیر است.

برهان. ساختار $\langle \mathbb{R}^+; <, \times \rangle$ (برای اعداد حقیقی مثبت) توسط نگاشت $x \mapsto \log(x)$ یکریخت (جبری) با ساختار $\langle \mathbb{R}; <, + \rangle$ می‌باشد. بنابراین قضیه‌ی **۱.۲.۳** تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{R}^+; <, \times \rangle$ را نتیجه می‌دهد. ⊠

قضیه ۳.۳.۴. نظریه‌ی نامتناهی زیر به طور کامل نظریه‌ی ترتیبی و ضربی اعداد حقیقی را اصل‌بندی می‌کند:

$$(\mathtt{O}_۱)\quad \forall x,y(x<y\to y\not< x)$$
$$(\mathtt{O}_۲)\quad \forall x,y,z(x<y<z\to x<z)$$
$$(\mathtt{O}_۳)\quad \forall x,y(x<y\vee x=y\vee y<x)$$
$$(\mathtt{M}_۱)\quad \forall x,y,z\,(x\cdot(y\cdot z)=(x\cdot y)\cdot z)$$
$$(\mathtt{M}^\circ_۲)\quad \forall x(x\cdot\mathbf{1}=x\ \wedge\ x\cdot\mathbf{0}=\mathbf{0}=-\mathbf{0})$$
$$(\mathtt{M}^\circ_۳)\quad \forall x(x\neq\mathbf{0}\to x\cdot x^{-۱}=\mathbf{1})$$
$$(\mathtt{M}_۴)\quad \forall x,y(x\cdot y=y\cdot x)$$
$$(\mathtt{M}^\circ_۵)\quad \forall x,y,z(x<y\wedge\mathbf{0}<z\to x\cdot z<y\cdot z)$$
$$(\mathtt{M}^\bullet_۵)\quad \forall x,y,z(x<y\wedge z<\mathbf{0}\to y\cdot z<x\cdot z)$$
$$(\mathtt{M}^\circ_۶)\quad \exists y(-\mathbf{1}<\mathbf{0}<\mathbf{1}<y)$$
$$(\mathtt{M}^\circ_۷)\quad \forall x\exists y(x=y^{۲n+۱})\qquad n\in\mathbb{N}$$
$$(\mathtt{M}_۸)\quad \forall x(x^{۲n}=\mathbf{1}\longleftrightarrow x=\mathbf{1}\vee x=-\mathbf{1})$$
$$(\mathtt{M}_۹)\quad \forall x\,(\mathbf{0}<x\longleftrightarrow\exists y[y\neq\mathbf{0}\wedge x=y^{۲}])$$

ساختار $\langle\mathbb{R};<,\times,\square^{-۱},-\mathbf{1},\mathbf{0},\mathbf{1}\rangle$ حذف سور می‌پذیرد، و بنابراین نظریه‌ی آن تصمیم‌پذیر است.

برهان. رابطه‌ی $(x<\mathbf{0})\leftrightarrow(\mathbf{0}<-x)$ از اصول $\mathtt{M}^\bullet_۵$، $\mathtt{M}^\circ_۲$، $\mathtt{M}^\circ_۶$، $\mathtt{M}_۴$ و $\mathtt{M}_۸$ نتیجه می‌شود که در آن $-x=(-\mathbf{1})\cdot x$. بنابراین برای هر فرمول η داریم:

$$\exists x\eta(x)\equiv\exists x>\mathbf{0}\eta(x)\vee\eta(\mathbf{0})\vee\exists y>\mathbf{0}\eta(-y).$$

همچنین اگر z متغیر دیگری در η باشد، در این صورت $\eta(x,z)$ با فرمول زیر معادل است:

$$[\mathbf{0} < z \wedge \eta(x,z)] \vee \eta(x,\mathbf{0}) \vee [\mathbf{0} < -z \wedge \eta(x,z)].$$

و سرانجام اگر فرض کنیم $z' = -z$، در این صورت $\mathbf{0} < -z \wedge \eta(x,z)$ با $\mathbf{0} < z' \wedge \eta(x,-z')$ معادل خواهد بود. بنابراین با معرفی ثابت‌های $\mathbf{0}$ و $-\mathbf{1}$ (و تغییر متغیر در صورت لزوم)، می‌توانیم فرض کنیم که همه‌ی متغیرهای یک فرمول بدون سور، مثبت هستند. حال با توجه به لم **۳.۳.۱** روند حذف سور به صورت زیر انجام می‌گیرد:
ما ابتدا ثابت‌های $\mathbf{0}$ و $-\mathbf{1}$ را حذف می‌کنیم و سپس قضیه را به گزاره‌ی **۲.۳.۴** تقلیل می‌دهیم. در مرحله‌ی نخست ترم‌ها را ساده‌تر می‌کنیم. به این ترتیب که هر ترم یا مثبت هست (همه‌ی متغیرها مثبت می‌باشند) یا برابر $\mathbf{0}$ هست یا نقیض ترم مثبت هست ($-t$ برای ترم مثبت t). سپس با تعویض $\mathbf{0} = \mathbf{0}$ با $\top$ و $\mathbf{0} < \mathbf{0}$ با $\perp$، می‌توانیم فرض کنیم که $\mathbf{0}$ حداکثر یک بار در هر فرمول اتمی ظاهر می‌شود. $-\mathbf{1}$ نیز حداکثر یک بار در هر فرمول اتمی ظاهر می‌شود زیرا $-t = -s$ با $t = s$ و $-t < -s$ با $s < t$ معادل می‌باشند. حال می‌توانیم ثابت $-\mathbf{1}$ را با تعویض فرمول‌های اتمی $-t = s$، $t = -s$ و $t < -s$ با $\perp$ و فرمول اتمی $-t < s$ با $\top$، برای ترم‌های مثبت یا صفر (با توجه به $\mathtt{M}_2^\circ$، $\mathbf{0} = -\mathbf{0}$) حذف کنیم. همچنین ثابت $\mathbf{0}$ با تعویض $\mathbf{0} < t$ با $\top$ و $t < \mathbf{0}$ و $t = \mathbf{0}$ (همچنین $\mathbf{0} = t$) با $\perp$ برای هر ترم مثبت t، می‌تواند حذف شود. بنابراین به فرمولی می‌رسیم که تمام متغیرهایش مثبت می‌باشند و به این ترتیب در قلمروی $\mathbb{R}^+$ هستیم. سرانجام برای مرحله‌ی دوم، فرمول به دست آمده با فرمول بدون سور حاصل از گزاره‌ی **۲.۳.۴** معادل است به شرطی که شکل نسبی اصول $\mathtt{O}_1$، $\mathtt{O}_2$، $\mathtt{O}_3$، $\mathtt{M}_1$، $\mathtt{M}_2$، $\mathtt{M}_3$، $\mathtt{M}_4$، $\mathtt{M}_5$، $\mathtt{M}_6$ و $\mathtt{M}_7$ در $\mathbb{R}^+$ را بتوان با استفاده از اصول $\mathtt{O}_1$، $\mathtt{O}_2$، $\mathtt{O}_3$، $\mathtt{M}_1$، $\mathtt{M}_2^\circ$، $\mathtt{M}_3^\circ$، $\mathtt{M}_4$، $\mathtt{M}_5^\circ$، $\mathtt{M}_5^\bullet$، $\mathtt{M}_6^\circ$، $\mathtt{M}_7^\circ$، $\mathtt{M}_8$ و $\mathtt{M}_9$ ثابت کرد. کافی است تنها اصول

M_6 و M_7 اثبات شوند که شکل نسبی آن‌ها در $\mathbb{R}^+$ به ترتیب به صورت

$$\exists y(\mathbf{0} < y \wedge y \neq \mathbf{1}) \quad \text{و} \quad \forall x \exists y[\mathbf{0} < x \rightarrow \mathbf{0} < y \wedge x = y^n]$$

می‌باشند. شکل نسبی اصل M_6 فوراً از اصل M_6° نتیجه می‌شود. برای نسبی کردن M_7، $a > 0$ و $n \in \mathbb{N}$ را در نظر بگیرید. قرار دهید $n = 2^k(2m + 1)$. با استفاده از اصل M_7° عدد حقیقی c وجود دارد به طوری که $a = c^{2m+1}$. و از اصول M_5° و $M_5^\bullet$ نتیجه می‌شود که $c > 0$. حال با استفاده از اصل M_9 و تکرار آن برای k بار، عدد حقیقی b باید وجود داشته باشد به طوری که $b^{2^k} = c$ و $b > 0$ (زیرا در غیر این صورت می‌توان از $-b$ به جای b استفاده کرد). بنابراین داریم: $a = c^{2m+1} = b^{2^k(2m+1)}$ و در نتیجه $a = b^n$. ⊠

۴.۳.۲ اصل‌ناپذیری متناهی ساختار $\langle \mathbb{R}; <, \times \rangle$

گزاره ۴.۳.۴. ساختار $\langle \mathbb{R}^+; <, \times \rangle$ به طور متناهی اصل‌پذیر نیست.

برهان. مجموعه‌ی زیر

$$\{ 2^{m \cdot (N!)^{-k}} \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$$

از اعداد حقیقی مثبت را برای N به اندازه‌ی کافی بزرگ، در نظر می‌گیریم. این مجموعه زیرگروه ضربی است و بنابراین همه‌ی اصول

$$(O_1, O_2, O_3, M_1, M_2, M_3, M_4, M_5, M_6)$$

و تعداد متناهی مورد از اصل M_7 (برای $n \leqslant N$) را ارضاء می‌کند ولی همه‌ی موارد این اصل را ارضاء نمی‌کند. برای مثال در مورد $n = p$ که p عدد اول بزرگ‌تر از $N!$ می‌باشد، اصل M_7 ارضاء نمی‌شود. ⊠

قضیه ۵.۳.۴. ساختار $\langle\mathbb{R};<,\times\rangle$ به طور متناهی اصل‌پذیر نیست.

برهان. مجموعه‌ی زیر

$$\{\text{۰}\}\cup\{-\text{۲}^{m\cdot(N!)^{-k}},\text{۲}^{m\cdot(N!)^{-k}}\mid m\in\mathbb{Z},k\in\mathbb{N}\}$$

از اعداد حقیقی برای $N>$ ۲ همه‌ی اصول قضیه‌ی ۳.۳.۴ را به جز اصل $\mathtt{M}^{\circ}_{\text{۷}}$ ارضاء می‌کند. اگرچه تعداد متناهی از موارد این اصل (برای $N\geqslant$ ۲$n+$۱) را ارضاء می‌کند ولی همه‌ی موارد ارضاء نمی‌شوند. برای مثال وقتی که ۲$n+$۱ عدد اول بزرگ‌تر از $N!$ می‌باشد، اصل $\mathtt{M}^{\circ}_{\text{۷}}$ ارضاء نمی‌شود. ⊠

۴.۴ اعداد گویا با ترتیب و ضرب

روش اثبات قضیه‌ی ۳.۳.۴ نظرمان را به ساختار ترتیبی و ضربی اعداد گویای مثبت یعنی $\langle\mathbb{Q}^{+};<,\times\rangle$ جلب می‌کند. در حقیقت در آن قضیه ما کل مجموعه $\mathbb{R}$ همراه با رابطه‌ی $<$ و عمل $\times$ را به کمک $\mathbb{R}^{+}$ اصل‌بندی نمودیم. روش اثبات نیز بدین ترتیب بود که با اضافه کردن ثوابت $\mathbf{0}$ و $-\mathbf{1}$ تمام متغیرها را بدین گونه تعیین علامت می‌کردیم: برای هر x در $\mathbb{R}$ داریم $\mathbf{0}<x$ یا $x=\mathbf{0}$ یا $-x>\mathbf{0}$. این در $\mathbb{Q}$ نیز برقرار است؛ پس با اضافه کردن ثوابت $\mathbf{0}$ و $-\mathbf{1}$ و با همان تکنیک برهان قضیه‌ی ۳.۳.۴ باید بتوان $\mathbb{Q}$ را به همراه $<$ و $\times$ توسط $\mathbb{Q}^{+}$ اصل‌بندی نمود. بنابراین نخست توجه خود را به نظریه‌ی اعداد گویای مثبت در زبان ضرب و ترتیب معطوف می‌داریم.

۱.۴.۴ حذف سور گستره‌ی $\langle \mathbb{Q}; <, \times \rangle$

گزاره ۱.۴.۴ . نظریه‌ی ساختار $\langle \mathbb{Q}^{+}; <, \times \rangle$ حذف سور نمی‌پذیرد.

برهان. نشان می‌دهیم فرمول $\exists x (y = x^n)$ برای $n > 1$ با هیچ فرمول بدون سوری معادل نمی‌باشد. همه‌ی فرمول‌های اتمی برای متغیر آزاد y به شکل‌های $y^n < y^m$ یا $y^n = y^m$ می‌باشند که وابسته به مقدار y نیستند و معادل یکی از حالت‌های $\top$ یا $\bot$ می‌باشند. بنابراین فرمول $\exists x (y = x^n)$ (که وابسته به مقدار y و n است و می‌تواند $\top$ یا $\bot$ باشد) معادل هیچ کدام از آن‌ها نمی‌باشد. ⊠

تعریف ۲.۴.۴ ($\Re$)**.** برای $n > 1$، $\Re_n(y)$ را فرمول $\exists x (y = x^n)$ تعریف می‌کنیم که بیان می‌کند: «y، $n-$امین توان یک عدد است». ⊛

نکته ۳.۴.۴ . برای عدد گویای داده شده‌ی $r \in \mathbb{Q}$ و عدد طبیعی $n \in \mathbb{N}$، می‌توان به طور الگوریتمی تصمیم گرفت که $\Re_n(r)$ برقرار هست یا نه: برای این منظور کافی است که $r \in \mathbb{Q}$ را به عوامل اول تجزیه کرده (مثلاً عدد $\frac{۴۰}{۴۵}$ پس از ساده کردن به صورت $\frac{۸}{۹}$ است که تجزیه‌ی آن به عوامل اول برابر است با $۲^{۳} \times ۳^{-۲}$) و بخش‌پذیری تمامی توان‌های ظاهر شده را به n بررسی نمود. ⌖

تعریف ۴.۴.۴ (TQ)**.** فرض کنید TQ نظریه‌ای باشد که توسط اصول

(O۱) $\forall x,y(x<y\to y\not< x)$

(O۲) $\forall x,y,z(x<y<z\to x<z)$

(O۳) $\forall x,y(x<y\vee x=y\vee y<x)$

(M۱) $\forall x,y,z\,(x\cdot(y\cdot z)=(x\cdot y)\cdot z)$

(M۲) $\forall x(x\cdot\mathbf{1}=x)$

(M۳) $\forall x(x\cdot x^{-1}=\mathbf{1})$

(M۴) $\forall x,y(x\cdot y=y\cdot x)$

(M۵) $\forall x,y,z(x<y\to x\cdot z<y\cdot z)$

(M۶) $\exists y(y\neq\mathbf{1})$

(M۱۰) $\forall x,z\exists y(x<z\to x<y^n<z)$ $\quad n\in\mathbb{N}$

(M۱۱) $\forall\{x_j\}_{j<q}\,\exists y\forall z\bigwedge_{m_j\nmid n\,(j<q)}(y^n\cdot x_j\neq z^{m_j})$ برای $n\geqslant 1$ و $(m_j>1)$

اصل‌بندی می‌شود. ⊛

در ادامه توضیحاتی به ترتیب درباره‌ی M۱۰ و M۱۱ ارایه می‌دهیم:

اصل M۱۰ در $\mathbb{Q}^+$ به این ترتیب تعبیر می‌شود که $\mathbb{Q}^+$ نه تنها در اعضای خودش بلکه در رادیکال‌های آن‌ها نیز چگال است (برای هر $x,z\in\mathbb{Q}^+$، $y\in\mathbb{Q}^+$ وجود دارد به طوری که $\sqrt[n]{x}<y<\sqrt[n]{z}$).

تعبیر اصل M۱۱ در $\mathbb{Q}^+$ در واقع معادل است با اینکه برای هر دنباله‌ی $x_0,\cdots,x_{q-1}\in\mathbb{Q}^+$ و $m_0,\cdots,m_{q-1}\in\mathbb{N}^+$ که هیچ کدام از آن‌ها n را عاد نمی‌کنند (به عبارتی $m_j\nmid n$)، $y\in\mathbb{Q}^+$ وجود دارد به طوری که $\bigwedge_{j<q}\neg\Re_{m_j}(y^n\cdot x_j)$. این اصل در $\mathbb{R}^+$ درست نمی‌باشد (در حالی که اصل M۱۰ در آن درست است) و برای مشاهده‌ی درستی اصل M۱۱ در $\mathbb{Q}^+$ کافی است توجه کنیم که برای دنباله‌ی داده شده‌ی $x_0,\cdots,x_{q-1}$ می‌توان y را عدد اولی

فرض کرد که در صورت و مخرج کسر ساده شده‌ی هیچ x_jای ظاهر نشود. در این حالت $y^n \cdot x_j$ فقط وقتی می‌تواند توان m_j–ام (عدد گویای مثبت) باشد که m_j، عدد n را عاد کند. شرط $m_j \nmid n$ لازم می‌باشد زیرا در غیر این صورت (اگر $m_j \mid n$ و) اگر برای x_jای رابطه‌ی $\Re_{m_j}(x_j)$ ارضاء شود، آنگاه برای هیچ yای رابطه‌ی $\neg\Re_{m_j}(y^n \cdot x_j)$ ارضاء نمی‌شود.

• اکنون نشان خواهیم داد که نظریه‌ی ساختار $\langle \mathbb{Q}^+; <, \times, \square^{-1}, \mathbf{1}, \{\Re_n\}_{n>1} \rangle$ به طور کامل توسط نظریه‌ی TQ اصل‌بندی می‌شود و این ساختار حذف سور می‌پذیرد، بنابراین نظریه‌ی ساختار $\langle \mathbb{Q}^+; <, \times \rangle$ تصمیم‌پذیر است. برای این منظور به لم‌های زیر نیاز خواهیم داشت.

لم ۵.۴.۴. برای هر $x \in \mathbb{Q}^+$ و $n_1, n_2 > 1$، داریم:

$$\Re_{n_1}(x) \wedge \Re_{n_2}(x) \iff \Re_n(x)$$

که در آن n کوچک‌ترین مضرب مشترک n_1 و n_2 می‌باشد.

برهان. با توجه به اینکه هر دوی n_1 و n_2، n را عاد می‌کنند، قسمت $\Leftarrow$ ثابت می‌شود. برای اثبات قسمت $\Rightarrow$، فرض کنیم $x = y^{n_1} = z^{n_2}$. با استفاده از اتحاد بزو $c_1, c_2 \in \mathbb{Z}$ وجود دارند به طوری که تساوی $c_1 n/n_1 + c_2 n/n_2 = 1$ برقرار است؛ بنابراین

$$x = x^{c_1 n/n_1} \cdot x^{c_2 n/n_2} = y^{c_1 n} \cdot z^{c_2 n} = (y^{c_1} z^{c_2})^n$$

که این اثبات را تمام می‌کند. ⊠

لم ۶.۴.۴. برای اعداد طبیعی $\{n_i\}_{i<p}$ که $n_i > ۱$ و اعداد گویای مثبت $\{t_i\}_{i<p}$ و x داریم:

$$\bigwedge_{i<p} \Re_{n_i}(x \cdot t_i) \iff \Re_n(x \cdot \beta) \wedge \bigwedge_{i \neq j} \Re_{d_{i,j}}(t_i \cdot t_j^{-۱})$$

که در آن n کوچک‌ترین مضرب مشترک n_iها، $d_{i,j}$ بزرگ‌ترین مقسوم علیه مشترک n_i و n_j (برای هر $i \neq j$) و $\beta = \prod_{i<p} t_i^{c_i(n/n_i)}$ که رابطه‌ی $\sum_{i<p} c_i(n/n_i) = ۱$ برای c_iها برقرار است.

برهان. برای t_iها، n_iها، c_iها، $d_{i,j}$ها و n مفروض، هرگاه رابطه‌ی $\bigwedge_{i \neq j} \Re_{d_{i,j}}(t_i \cdot t_j^{-۱})$ برقرار باشد، نشان می‌دهیم برای هر $k < p$، رابطه‌ی $\Re_{n_k}(t_k \cdot \beta^{-۱})$ نیز برقرار است: فرض کنیم $m_{k,i}$ کوچک‌ترین مضرب مشترک n_k و n_i باشد (که مقسوم علیه n هست). توجه می‌کنیم که $d_{k,i}/n_i = n_k/m_{k,i}$. از آنجایی که $\Re_{d_{k,i}}(t_k \cdot t_i^{-۱})$، باید $w_{k,i}$هایی (برای $k \neq i$) وجود داشته باشند به طوری که $t_k \cdot t_i^{-۱} = w_{k,i}^{d_{k,i}}$. حال رابطه‌ی $\Re_{n_k}(t_k \cdot \beta^{-۱})$ از تساوی‌های زیر به دست می‌آید:

$$\begin{aligned} t_k \cdot \beta^{-۱} &= t_k^{\sum_i c_i(n/n_i)} \cdot \prod_i t_i^{-c_i(n/n_i)} \\ &= \prod_{i \neq k} (t_k \cdot t_i^{-۱})^{c_i(n/n_i)} \\ &= \prod_{i \neq k} (w_{k,i}^{d_{k,i}})^{c_i(n/n_i)} \\ &= \prod_{i \neq k} w_{k,i}^{c_i \cdot n_k(n/m_{k,i})} \\ &= (\prod_{i \neq k} w_{k,i}^{c_i(n/m_{k,i})})^{n_k}. \end{aligned}$$

($\Rightarrow$): روابط $\Re_{n_i}(x \cdot t_i)$ و $\Re_{n_j}(x \cdot t_j)$ فوراً ایجاب می‌کنند که $\Re_{d_{i,j}}(x \cdot t_i)$ و $\Re_{d_{i,j}}(x \cdot t_j)$ و بنابراین $\Re_{d_{i,j}}(t_i \cdot t_j^{-۱})$. برای نشان دادن $\Re_n(x \cdot \beta)$، کافی است با استفاده از لم **۵.۴.۴** نشان دهیم که رابطه‌ی $\Re_{n_i}(x \cdot \beta)$ برای هر $i < p$ برقرار است. و این نیز فوراً از رابطه‌ی $\Re_{n_i}(t_i \cdot \beta^{-۱})$ که در ابتدا ثابت شد و فرض $\Re_{n_i}(x \cdot t_i)$ نتیجه می‌شود.

(⇐): از قسمت اول، رابطه‌ی $\Re_{n_k}(t_k \cdot \beta^{-1})$ را برای هر $k < p$ داریم. حال با توجه به لم ۵.۴.۴ از رابطه‌ی $\Re_n(x \cdot \beta)$، رابطه‌ی $\Re_{n_k}(x \cdot \beta)$ نتیجه می‌شود و بنابراین برای هر $k < p$ داریم: $\Re_{n_k}(x \cdot t_k)$. ⊠

• توجه می‌کنیم که لم‌های ۵.۴.۴ و ۶.۴.۴ در نظریه‌ی TQ قابل اثبات می‌باشند. ایده‌ی اثبات لم ۶.۴.۴ از مرجع [۱۴] گرفته شده است.

لم ۷.۴.۴. جملات زیر برای هر $n > ۱$ در نظریه‌ی TQ قابل اثبات می‌باشند:

$$\forall u \exists y [\Re_n(y \cdot u)],$$

$$\forall x, u \exists y [x < y \wedge \Re_n(y \cdot u)],$$

$$\forall z, u \exists y [y < z \wedge \Re_n(y \cdot u)],$$

$$\forall x, z, u \exists y [x < z \to x < y < z \wedge \Re_n(y \cdot u)].$$

برهان. کافی است فرمول آخر را اثبات کنیم. با استفاده از $\mathtt{M}_{۱۰}$ از تعریف ۴.۴.۴، vای وجود دارد که $x \cdot u < v^n < z \cdot u$. در این صورت برای $y = v^n \cdot u^{-۱}$ خواهیم داشت: $x < y < z$ و $\Re_n(y \cdot u)$. ⊠

لم ۸.۴.۴. جملات زیر برای هر $\{m_j > ۱\}_{j<q}$ در نظریه‌ی TQ قابل اثبات می‌باشند:

$$\forall \{x_j\}_{j<q} \exists y [\textstyle\bigwedge_j \neg \Re_{m_j}(y \cdot x_j)],$$

$$\forall \{x_j\}_{j<q}, u \exists y [u < y \wedge \textstyle\bigwedge_j \neg \Re_{m_j}(y \cdot x_j)],$$

$$\forall \{x_j\}_{j<q}, v \exists y [y < v \wedge \textstyle\bigwedge_j \neg \Re_{m_j}(y \cdot x_j)],$$

$$\forall \{x_j\}_{j<q}, u, v \exists y [u < v \to u < y < v \wedge \textstyle\bigwedge_j \neg \Re_{m_j}(y \cdot x_j)].$$

برهان. اولین جمله نتیجه‌ی فوری اصل $\mathtt{M}_{۱۱}$ از تعریف ۴.۴.۴ برای $n = ۱$ می‌باشد. حال کافی است جمله‌ی آخر را اثبات کنیم. با استفاده از اصل $\mathtt{M}_{۱۱}$، γای وجود دارد به

طوری که $\bigwedge\!\!\!\bigwedge_j \neg\Re_{m_j}(\gamma\cdot x_j)$. فرض کنیم $M=\prod_j m_j$؛ با استفاده از اصل $\mathtt{M}_{10}$، δای وجود دارد به طوری که $u\cdot\gamma^{-1}<\delta^M<v\cdot\gamma^{-1}$. حال برای $y=\gamma\cdot\delta^M$ داریم: $u<y<v$ و $\bigwedge\!\!\!\bigwedge_j \neg\Re_{m_j}(y\cdot x_j)$. زیرا در غیر این صورت خواهیم داشت $\Re_{m_j}(y\cdot x_j)$ و در نتیجه $\Re_{m_j}(\gamma\cdot\delta^M\cdot x_j)$؛ بنابراین رابطه‌ی $\Re_{m_j}(\gamma\cdot x_j)$ برقرار خواهد بود و این یک تناقض است.⊠

لم ۹.۴.۴. در نظریه‌ی TQ فرمول‌های زیر

$\exists x[\Re_n(x\cdot t)\wedge \bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(x\cdot s_j)]$,

$\exists x[u<x\wedge\Re_n(x\cdot t)\wedge \bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(x\cdot s_j)]$,

$\exists x[x<v\wedge\Re_n(x\cdot t)\wedge \bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(x\cdot s_j)]$

معادل با:

$$\bigwedge\!\!\!\bigwedge_{m_j|n}\neg\Re_{m_j}(t^{-1}\cdot s_j)$$

بوده و فرمول

$$\exists x[u<x<v\wedge\Re_n(x\cdot t)\wedge\bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(x\cdot s_j)]$$

معادل است با:

$$\bigwedge\!\!\!\bigwedge_{m_j|n}\neg\Re_{m_j}(t^{-1}\cdot s_j)\wedge u<v.$$

برهان. اگر $m_j\mid n$ در این صورت $\Re_n(x\cdot t)$ ایجاب می‌کند که $\Re_{m_j}(x\cdot t)$. حال اگر $\Re_{m_j}(t^{-1}\cdot s_j)$ درست باشد، در این صورت $\Re_{m_j}(x\cdot s_j)$ نیز درست خواهد بود که متناقض با $\bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(x\cdot s_j)$ می‌باشد.

حال فرض کنیم رابطه‌ی $\bigwedge\!\!\!\bigwedge_{m_j|n}\neg\Re_{m_j}(t^{-1}\cdot s_j)$ برقرار باشد. با استفاده از اصل $\mathtt{M}_{11}$، γای

وجود دارد به طوری که $\bigwedge\!\!\!\bigwedge_{m_j\nmid n}\neg\Re_{m_j}(\gamma^n\cdot t^{-1}\cdot s_j)$. با استفاده از اصل $\mathtt{M}_{10}$، δای وجود دارد به طوری که $u\cdot t\cdot\gamma^{-n}<\delta^{M\cdot n}<v\cdot t\cdot\gamma^{-n}$ (اگر $u<v$) و $M=\prod_{j<q}m_j$. برای $x=\delta^{M\cdot n}\cdot\gamma^n\cdot t^{-1}$ داریم: $u<x<v$ و $\Re_n(x\cdot t)$.

حال برای $j<q$ نشان می‌دهیم که $\neg\Re_{m_j}(x\cdot s_j)$. دو حالت در نظر می‌گیریم:

- اگر $m_j\mid n$ در این صورت $\neg\Re_{m_j}(t^{-1}\cdot s_j)$ ایجاب می کند که $\neg\Re_{m_j}(\delta^{M\cdot n}\cdot\gamma^n\cdot t^{-1}\cdot s_j)$.
- اگر $m_j\nmid n$ در این صورت $\neg\Re_{m_j}(\gamma^n\cdot t^{-1}\cdot s_j)$ ایجاب می‌کند که $\neg\Re_{m_j}(\delta^{M\cdot n}\cdot\gamma^n\cdot t^{-1}\cdot s_j)$ (زیرا $m_j\mid M$). ⊠

• بالاخره می‌توانیم نتیجه‌ی اصلی را اثبات کنیم که برای اولین بار در این رساله بررسی شده است.

قضیه ۱۰.۴.۴ . نظریه‌ی نامتناهی TQ به طور کامل نظریه‌ی ساختار $\langle\mathbb{Q}^+;<,\times\rangle$ را اصل‌بندی می‌کند و ساختار $\langle\mathbb{Q}^+;<,\times,\square^{-1},\mathbf{1},\{\Re_n\}_{n>1}\rangle$ حذف سور می‌پذیرد.

برهان. کافی است فرمول زیر حذف سور شود:

$$\exists x\Big(\bigwedge\!\!\!\bigwedge_{i<p}\Re_{n_i}(x^{a_i}\cdot t_i)\ \wedge\ \bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(x^{b_j}\cdot s_j)\ \wedge\ \bigwedge\!\!\!\bigwedge_{k<f}u_k<x^{c_k}\ \wedge\ \bigwedge\!\!\!\bigwedge_{\ell<g}x^{d_\ell}<v_\ell\ \wedge\ \bigwedge\!\!\!\bigwedge_{\iota<h}x^{e_\iota}=w_\iota\Big).\tag{۱.۴}$$

با توجه به روابط

$$(i)\qquad a^n<b^n\leftrightarrow a<b$$
$$(ii)\qquad \Re_{m\cdot n}(a^n)\leftrightarrow\Re_m(a)$$

که از اصول نتیجه می‌شوند، می‌توانیم همه‌ی a_iها، b_jها، c_kها، d_ℓها و e_lها را برابر فرض کرده و به همان شیوه‌ی اثبات قضیه‌ی ۳.۴.۳ برابر یک بگیریم. همچنین می‌توانیم فرض کنیم $h=0$ و $f,g\leqslant 1$. و نیز با توجه به لم ۶.۴.۴، می‌توان فرض کرد که $p\leqslant 1$.

ـ اگر $q=\circ$، در این صورت لم **۷.۴.۴** ایجاب می‌کند که سور فرمول (**۱.۴**) حذف شود. بنابراین فرض می‌کنیم که $q>\circ$.

ـ اگر $p=\circ$، در این صورت سور فرمول (**۱.۴**) توسط لم **۸.۴.۴** حذف می‌شود.

ـ سرانجام با فرض $p=۱$، $h=\circ\neq q$ و $f,g\leqslant ۱$، لم **۹.۴.۴** ایجاب می‌کند که فرمول (**۱.۴**) حذف سور شود. ⊠

نتیجه ۱۱.۴.۴ . نظریه‌ی نامتناهی زیر به طور کامل نظریه‌ی $\langle\mathbb{Q};<,\times\rangle$ را اصل‌بندی می‌کند:

$$(\mathtt{O}_۱)\quad \forall x,y(x<y\rightarrow y\not< x)$$

$$(\mathtt{O}_۲)\quad \forall x,y,z(x<y<z\rightarrow x<z)$$

$$(\mathtt{O}_۳)\quad \forall x,y(x<y\vee x=y\vee y<x)$$

$$(\mathtt{M}_۱)\quad \forall x,y,z\,(x\cdot(y\cdot z)=(x\cdot y)\cdot z)$$

$$(\mathtt{M}^\circ_۲)\quad \forall x(x\cdot\mathbf{1}=x\ \ \wedge\ \ x\cdot\mathbf{0}=\mathbf{0}=-\mathbf{0})$$

$$(\mathtt{M}^\circ_۳)\quad \forall x(x\neq\mathbf{0}\rightarrow x\cdot x^{-۱}=\mathbf{1})$$

$$(\mathtt{M}_۴)\quad \forall x,y(x\cdot y=y\cdot x)$$

$$(\mathtt{M}^\circ_۵)\quad \forall x,y,z(x<y\wedge\mathbf{0}<z\rightarrow x\cdot z<y\cdot z)$$

$$(\mathtt{M}^\bullet_۵)\quad \forall x,y,z(x<y\wedge z<\mathbf{0}\rightarrow y\cdot z<x\cdot z)$$

$$(\mathtt{M}^\circ_۶)\quad \exists y(-\mathbf{1}<\mathbf{0}<\mathbf{1}<y)$$

$$(\mathtt{M}_۸)\quad \forall x(x^{۲n}=\mathbf{1}\longleftrightarrow x=\mathbf{1}\vee x=-\mathbf{1})$$

$$(\mathtt{M}^\circ_{۱\circ})\quad \forall x,z\exists y(\mathbf{0}<x<z\rightarrow x<y^n<z)\qquad n\in\mathbb{N}$$

$$(\mathtt{M}_{۱۱})\quad \forall\{x_j\}_{j<q}\,\exists y\forall z\bigwedge\nolimits_{m_j\nmid n\,(j<q)}(y^n\cdot x_j\neq z^{m_j})$$ برای $n\geqslant ۱$ و $(m_j>۱)$

ساختار $\langle\mathbb{Q};<,\times,\square^{-۱},-\mathbf{1},\mathbf{0},\mathbf{1},\{\Re_n\}_{n>۱}\rangle$ حذف سور می‌پذیرد و بنابراین نظریه‌ی آن تصمیم‌پذیر است.

برهان. حذف سور ساختار $\langle \mathbb{Q}; <, \times, \square^{-1}, -\mathbf{1}, \mathbf{0}, \mathbf{1}, \{\Re_n\}_{n>1} \rangle$ از قضیه‌ی اصلی (۱۰.۴.۴) نتیجه می‌شود: کافی است علامت‌ها را متمایز کنیم؛ برای هر متغیر x، یکی از حالت‌های $-x > \mathbf{0}$ یا $x = \mathbf{0}$ یا $x > \mathbf{0}$ برقرار است. ⊠

گزاره ۱۲.۴.۴ . نظریه‌ی ساختار $\langle \mathbb{Q}; +, \times \rangle$ تصمیم‌ناپذیر است.

برهان. با توجه به اینکه مجموعه‌ی اعداد صحیح در ساختار $\langle \mathbb{Q}; +, \times \rangle$ تعریف‌پذیر است [۱۶]، تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{Q}; +, \times \rangle$ تصمیم‌پذیری نظریه ساختار $\langle \mathbb{Z}; +, \times \rangle$ را نتیجه می‌دهد که متناقض با گزاره‌ی ۱.۲.۴ می‌باشد. ⊠

نتیجه ۱۳.۴.۴ . عمل جمع در ساختار $\langle \mathbb{Q}; <, \times \rangle$ تعریف‌پذیر نیست.

برهان. اگر $+$ در ساختار $\langle \mathbb{Q}; <, \times \rangle$ تعریف‌پذیر باشد، آنگاه $\langle \mathbb{Q}; +, \times \rangle$ شامل $\langle \mathbb{Q}; <, \times \rangle$ می‌بود. در این صورت با توجه به تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{Q}; <, \times \rangle$، نظریه‌ی ساختار $\langle \mathbb{Q}; +, \times \rangle$ نیز تصمیم‌پذیر می‌شد که متناقض با گزاره‌ی ۱۲.۴.۴ است. ⊠

۲.۴.۴ اصل‌ناپذیری متناهی ساختار $\langle \mathbb{Q}; <, \times \rangle$

قضیه ۱۴.۴.۴ . ساختار $\langle \mathbb{Q}^{+}; <, \times \rangle$ به طور متناهی اصل‌پذیر نیست.

برهان. برای اینکه نشان دهیم ساختار $\langle \mathbb{Q}^{+}; <, \times \rangle$ نمی‌تواند به طور متناهی اصل‌پذیر باشد، یک ساختار ضربی مرتب می‌سازیم که هر تعداد به اندازه‌ی کافی زیاد از اصول نظریه‌ی TQ اما نه همه‌ی آن اصول را ارضاء کند. $\mathfrak{p}$ را یک عدد اول به اندازه‌ی کافی بزرگ می‌گیریم. همان طور که قبلاً دیدیم، مجموعه‌ی زیر

$$\mathbb{Q}/\mathfrak{p} = \{m/\mathfrak{p}^k \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$$

تحت جمع و عمل $x\mapsto x/\mathfrak{p}$ بسته می‌باشد و رابطه‌ی $\mathbb{Z}\subset\mathbb{Q}/\mathfrak{p}\subset\mathbb{Q}$ برقرار است. فرض کنیم $\rho_0,\rho_1,\rho_2,\cdots$ دنباله‌ی همه‌ی اعداد اول ($2,3,5,\cdots$) را نشان دهد. $(\mathbb{Q}/\mathfrak{p})^*$ را مجموعه‌ی $\{\prod_{i<\ell}\rho_i^{r_i}\mid \ell\in\mathbb{N}, r_i\in\mathbb{Q}/\mathfrak{p}\}$ قرار می‌دهیم؛ این مجموعه تحت ضرب و عمل $x\mapsto x^{1/\mathfrak{p}}$ بسته می‌باشد و رابطه‌ی $\mathbb{Q}^+\subset(\mathbb{Q}/\mathfrak{p})^*\subset\mathbb{R}^+$ برقرار است. بنابراین مجموعه‌ی $(\mathbb{Q}/\mathfrak{p})^*$، اصول $\mathtt{O}_1$، $\mathtt{O}_2$، $\mathtt{O}_3$، $\mathtt{M}_1$، $\mathtt{M}_2$، $\mathtt{M}_3$، $\mathtt{M}_4$، $\mathtt{M}_5$ و $\mathtt{M}_6$ از گزاره‌ی **۲.۳.۴**، و همچنین اصل $\mathtt{M}_{10}$ را ارضاء می‌کند. با این حال، این مجموعه اصل $\mathtt{M}_{11}$ را برای $n=x_j=1$ و $m_j=\mathfrak{p}$ ارضاء نمی‌کند زیرا $(\mathbb{Q}/\mathfrak{p})^*\models\forall y\Re_{\mathfrak{p}}(y)$. نشان می‌دهیم که $(\mathbb{Q}/\mathfrak{p})^*$ اصل $\mathtt{M}_{11}$ را برای حالتی که $1<m_j<\mathfrak{p}$، ارضاء می‌کند (برای هر n و q دلخواه و هر $j<q$). بنابراین تعداد متناهی از موارد اصل $\mathtt{M}_{11}$ (به همراه بقیه‌ی اصول نظریه‌ی TQ) نمی‌توانند همه‌ی موارد آن را اثبات کنند. فرض کنیم x_j از $(\mathbb{Q}/\mathfrak{p})^*$ به صورت $x_j=\prod_{i<\ell_j}\rho_i^{r_{i,j}}$ داده شده باشد؛ می‌توانیم فرض کنیم که $\ell_j\geqslant q$. قرار می‌دهیم $r_{j,j}=u_j/\mathfrak{p}^{v_j}$ که $u_j\in\mathbb{Z}$ و $v_j\in\mathbb{N}$ (برای هر $j<q$). عدد t_j را برای حالتی که $m_j\mid u_j$، برابر ۱ و برای حالتی که $m_j\nmid u_j$، برابر m_j تعریف می‌کنیم. فرض کنیم

$$y=\prod_{i<q}\rho_i^{(t_i/\mathfrak{p}^{v_i+1})}\ (\in(\mathbb{Q}/\mathfrak{p})^*)$$

و نشان می‌دهیم که وقتی $\bigwedge\!\!\!\bigwedge_{j<q} m_j\nmid n$، رابطه زیر برقرار است:

$$\bigwedge\!\!\!\bigwedge_{j<q}\neg\Re_{m_j}(y^n\cdot x_j).$$

عدد $k<q$ را در نظر می‌گیریم و فرض می‌کنیم که $\Re_{m_k}(y^n\cdot x_k)$ (فرض خلف). در این صورت رابطه‌ی $\Re_{m_k}(\rho_k^{nt_k/\mathfrak{p}^{v_k+1}}\cdot\rho_k^{u_k/\mathfrak{p}^{v_k}})$ برقرار می‌شود. اعداد صحیح a و b باید وجود

داشته باشند به طوری که

$$\rho_k^{(nt_k+\mathfrak{p}u_k)/\mathfrak{p}^{v_k+1}} = \rho_k^{(m_k\cdot a)/\mathfrak{p}^b}.$$

بنابراین

$$m_k \mid nt_k + \mathfrak{p}u_k,$$

حال با بررسی دو حالت زیر به تناقض می‌رسیم:

(i) اگر $m_k \mid u_k$ در این صورت $t_k = 1$ و بنابراین $m_k \mid n + \mathfrak{p}u_k$ و از آنجا $m_k \mid n$، که متناقض با فرض $\bigwedge\!\!\!\bigwedge_{j<q} m_j \nmid n$ است؛

(ii) اگر $m_k \nmid u_k$ در این صورت $t_k = m_k$ و بنابراین $m_k \mid nm_k + \mathfrak{p}u_k$ و از آنجا $m_k \mid \mathfrak{p}u_k$ که با $(m_k, \mathfrak{p}) = 1$، نتیجه می‌دهد $m_k \mid u_k$، که متناقض با فرض $m_k \nmid u_k$ می‌باشد. ⊠

فصل ۵

جمع‌بندی و مسایل باز

۱.۵ جمع‌بندی

در جدول زیر، ساختارهای تصمیم‌پذیر با Δ_1 و ساختارهای تصمیم‌ناپذیر با $\not\Delta_1$ نشان داده شده‌اند:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1
$\{<,+\}$	Δ_1	Δ_1	Δ_1	Δ_1
$\{<,\times\}$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1
$\{+,\times\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1

- تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{Q}; <, \times \rangle$ و همچنین اصل‌بندی صریح برای نظریه‌ی ساختار تصمیم‌پذیر $\langle \mathbb{R}; <, \times \rangle$ از نتایج جدید این رساله می‌باشند.

- برای نظریه‌ی ساختارهای تصمیم‌پذیر دیگر، برهان‌های قدیمی و جدید (نحوی) همراه با اصل‌بندی‌های صریح ارایه شده‌اند.

- جالب توجه است که

— تصمیم‌ناپذیری نظریه‌ی ساختارهای $\langle \mathbb{N}; <, \times \rangle$ و $\langle \mathbb{Z}; <, \times \rangle$ از تصمیم‌ناپذیری نظریه‌ی ساختارهای $\langle \mathbb{N}; +, \times \rangle$ و $\langle \mathbb{Z}; +, \times \rangle$ (و تعریف‌پذیری $+$ در زبان $<$ و $\times$ در $\mathbb{N}$ و $\mathbb{Z}$)، نتیجه می‌شوند و

— تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{R}; <, \times \rangle$ از تصمیم‌پذیری نظریه‌ی ساختار $\langle \mathbb{R}; +, \times \rangle$ (و تعریف‌پذیری $<$ در زبان $+$ و $\times$ در $\mathbb{R}$)، نتیجه می‌شود.

— با این وجود، تصمیم‌ناپذیری نظریه‌ی ساختار جمعی و ضربی $\langle \mathbb{Q}; +, \times \rangle$ به نظریه‌ی ساختار ضربی (تصمیم‌پذیر) $\langle \mathbb{Q}; <, \times \rangle$ مربوط نمی‌باشد؛ در واقع $+$ در ساختار ضربی $\langle \mathbb{Q}; <, \times \rangle$ تعریف‌پذیر نیست در حالی که $<$ در $\langle \mathbb{Q}; +, \times \rangle$ تعریف‌پذیر است.

۲.۵ مسایل باز

بین $\mathbb{Q}$ و $\mathbb{R}$ مجموعه‌های بسیار زیادی وجود دارند که قابل توجه‌اند. مثلاً

— $\mathbb{Q}[\sqrt{۲}]$.

— $\mathbb{Q}[\sqrt{۲}, \sqrt{۳}, \sqrt{۵}, \cdots]$.

— مجموعه‌ی اعداد حقیقی که با خط‌کش و پرگار قابل ساختن هستند $= \mathfrak{Q}$.

— میدان حاصل از رادیکال‌های اعداد گویا (وقتی در اعداد حقیقی وجود دارند).

برای هر مجموعه‌ی A که $\mathbb{Q} \subseteq A \subseteq \mathbb{R}$، قضیه‌ی **۱.۲.۳** نظریه‌ی ساختار $\langle A; <, + \rangle$ را وقتی مجموعه‌ی A تحت عمل جمع و توابع $x \mapsto x/n$ $(n \in \mathbb{N})$ بسته باشد، اصل‌بندی می‌کند. ولی نظریه‌ی ساختار $\langle A; <, \times \rangle$ وقتی مجموعه‌ی A تحت عمل $\times$ بسته باشد، ممکن است متفاوت باشد (یا اصلاً اصل‌پذیر بازگشتی نباشد یا با مجموعه‌ای کاملاً متفاوت اصل‌بندی گردد). مثلاً هنوز معلوم نیست که آیا نظریه‌ی ساختار $\langle \Omega; <, \times \rangle$ تصمیم‌پذیر هست یا نه؟!

از طرف دیگر، بررسی تصمیم‌پذیری ساختارهای جمعی یا ضربی مجموعه‌های چندجمله‌ای (که تحت جمع یا ضرب بسته هستند) می‌توانند نتایج جالبی در جبر نظریه‌ی مدلی داشته باشند. به عنوان مثال ساختارهای جمعی یا ضربی یا جمعی و ضربی حلقه‌های $\mathbb{Z}[X]$، $\mathbb{Q}[X]$ و $\mathbb{R}[X]$ با در نظر گرفتن رابطه‌ی ترتیب یا بدون آن از مسایل قابل توجه می‌باشند. بررسی هر کدام از این مسایل می‌تواند نتایج شگفت‌آوری را در زمینه‌ی منطق، علوم کامپیوتر و ریاضیات به همراه داشته باشد.

مراجع

[۱] Zofia Adamowicz & Pawel Zbierski, *Logic of Mathematics: a modern course of classical logic*, Wiley (1997), ISBN: 9780471060260.

[۲] Ziba Assadi & Saeed Salehi, `On Decidability and Axiomatizability of Some Ordered Structures`, *Soft Computing* 23:11 (2019) 3615–3626. DOI: 10.1007/s00500-018-3247-1.

[۳] George S. Boolos & John P. Burgess & Richard C. Jeffrey, *Computability and Logic*, Springer (5th ed. 2007), ISBN: 9780521701464.

[۴] Jacek Bochnak & Michel Coste & Marie–Françoise Roy, *Real Algebraic Geometry*, Springer (1998), ISBN: 9783642084294.

[۵] Saugata Basu & Richard Pollack & Marie–Françoise Roy, *Algorithms in Real Algebraic Geometry*, Springer (2nd ed. 2006), ISBN: 9783540330981.

[۶] Patrick Cégielski, "`Théorie Élémentaire de la Multiplication des Entiers Naturels`", in: C. Berline, K. McAloon, J.-P. Ressayre (eds.) *Model Theory and Arithmetic*, Comptes Rendus d'une Action Thématique Programmée du C.N.R.S. sur la Théorie des Modèles et l'Arithmétique, Paris, France, 1979/80, Lecture Notes in Mathematics 890, Springer (1981), ISBN: 9783540111597, pp. 44–89. DOI: 10.1007/BFb0095657.

[۷] Herbert B. Enderton, *A Mathematical Introduction to Logic*, Academic Press (2nd ed. 2001), ISBN: 9780122384523.

[۸] Aviezri S. Fraenkel, `New Proof of the Generalized Chinese Remainder Theorem`, *The Proceedings of the American Mathematical Society* 14:5 (1963) 790–791. DOI: 10.2307/203499.

[۹] Peter G. Hinman, *Fundamentals of Mathematical Logic*, CRC Press (2005), ISBN: 9781568812625.

[۱۰] Georg Kreisel & Jean Louis Krivine, *Elements of Mathematical Logic: Model Theory*, North–Holland (1971), ISBN: 9780720422658.

[۱۱] David Marker, *Model Theory: An Introduction*, Springer (2002), ISBN: 9781441931573.

[۱۲] J. Donald Monk, *Mathematical Logic*, Springer (1976), ISBN: 9780387901701.

[۱۳] Andrzej Mostowski, `On Direct Products of Theories`, *The Journal of Symbolic Logic* 17 (1952) 1–31. DOI: 10.2307/2267454.

[۱۴] Oystein Ore, `The General Chinese Remainder Theorem`, *The American Mathematical Monthly* 59:6 (1952) 365–370. DOI: 10.2307/2306804.

[۱۵] Abraham Robinson & Elias Zakon, `Elementary Properties of Ordered Abelian Groups`, *Transactions of the American Mathematical Society* 96:2 (1960) 222–236. DOI: 10.2307/199346.

[۱۶] Julia Robinson, `Definability and Decision Problems in Arithmetic`, *The Journal of Symbolic Logic* 14:2 (1949) 98–114. DOI: 10.2307/2266510.

[۱۷] Saeed Salehi, "`Axiomatizing Mathematical Theories: Multiplication`", in: A. Kamali-Nejad (ed.) *Proceedings of Frontiers in Mathematical Sciences*, Sharif University of Technology, Tehran, Iran (2012), pp. 165–176. URL: https://arxiv.org/pdf/1612.06525.pdf

[۱۸] Saeed Salehi, "`Computation in Logic and Logic in Computation`", in: B. Sadeghi-Bigham (ed.) *Proceedings of the Third International Conference on Contemporary Issues in Computer and Information Sciences* (CICIS 2012), Brown Walker Press, USA (2012), pp. 580–583. URL: https://arxiv.org/pdf/1612.06526.pdf

[۱۹] Craig Smorynski, *Logical Number Theory I: An Introduction*, Springer (1991), ISBN: 9783540522362.

[۲۰] Albert Visser, `On Q`, *Soft Computing* 21:1 (2017) 39–56. DOI: 10.1007/s00500-016-2341-5.

واژه‌نامه فارسی به انگلیسی

اتحاد تارسکی	Tarski's Identity
ارضاء کردن	Satisfy
اصل موضوعه	Axiom
اصل‌بندی	Axiomatization
اصل‌پذیری	Axiomatizablity
اصل‌پذیری نامتناهی	Infinite Axiomatizablity
الگوریتم تقسیم	Division Algorithm
اول	Prime
بدیهی	Trivial
برهان نحوی	Syntactic Proof
بزرگ‌ترین مقسوم علیه مشترک	Greatest Common Divisor
تالی	Successor
تجزیه	Factorization
ترتیب	Order
ترکیب عطفی	Conjunction

ترکیب فصلی .... Disjunction
تصمیم‌پذیر .... Decidable
تصمیم‌پذیری .... Decidability
تصمیم‌ناپذیر .... Undecidable
تصمیم‌ناپذیری .... Undecidability
تعبیر .... Interpretation
تعریف‌پذیر .... Definable
تعمیم .... Generalization
توسیع .... Extension
جمعی .... Additive
چگال .... Dense
حذف سور .... Quantifier Elimination
حساب اسکولم .... Skolem Arithmetic
حساب پرسبورگر .... Presburger Arithmetic
دوگان .... Dual
رابطه‌ی دوتایی .... Binary Relation
ریشه .... Root
زبان .... Language
ساختار .... Structure
شمارش‌پذیر .... Enumerable
صریح .... Explicit

صورت کسر .... Numerator
ضربی .... Multiplicative
فرمول .... Formula
فرمول اتمی .... Atomic Formula
فرمول بدون سور .... Quantifier-Free Formula
کوچک‌ترین مضرب مشترک .... Least Common Multiplier
گروه آبلی .... Abelian Group
گروه بخش‌پذیر .... Divisible Group
گسسته .... Discrete
متغیر .... Variable
مخرج کسر .... Denominator
معادل .... Equivalent
منطق گزاره‌ای .... Propositional Logic
منطق مرتبه‌ی اول .... First-order Logic
ناتمامیت .... Incompleteness
نسبی سازی .... Relativization
نظریه .... Theory
نقیض .... Negation
هم‌نهشتی .... Congruence
یکریخت .... Isomorphic
یکریخت جبری .... Algebraically Isomorphic

واژه نامه انگلیسی به فارسی

Abelian Group	گروه آبلی
Additive	جمعی
Algebraically Isomorphic	یکریخت جبری
Atomic Formula	فرمول اتمی
Axiom	اصل موضوعه
Axiomatizablity	اصل‌پذیری
Axiomatization	اصل‌بندی
Binary Relation	رابطه‌ی دوتایی
Congruence	هم‌نهشتی
Conjunction	ترکیب عطفی
Decidability	تصمیم‌پذیری
Decidable	تصمیم‌پذیر
Definable	تعریف‌پذیر
Dense	چگال
Denominator	مخرج کسر

Discrete .... گسسته
Disjunction .... ترکیب فصلی
Divisible Group .... گروه بخش‌پذیر
Division Algorithm .... الگوریتم تقسیم
Dual .... دوگان
Enumerable .... شمارش‌پذیر
Equivalent .... معادل
Explicit .... صریح
Extension .... توسیع
Factorization .... تجزیه
First-order Logic .... منطق مرتبه‌ی اول
Formula .... فرمول
Generalization .... تعمیم
Greatest Common Divisor .... بزرگ‌ترین مقسوم علیه مشترک
Incompleteness .... ناتمامیت
Infinite Axiomatizablity .... اصل‌پذیری نامتناهی
Interpretation .... تعبیر
Isomorphic .... یکریخت
Language .... زبان
Least Common Multiplier .... کوچک‌ترین مضرب مشترک
Multiplicative .... ضربی

Negation .... نقیض
Numerator .... صورت کسر
Order .... ترتیب
Presburger Arithmetic .... حساب پرسبورگر
Prime .... اول
Propositional Logic .... منطق گزاره‌ای
Quantifier Elimination .... حذف سور
Quantifier-Free Formula .... فرمول بدون سور
Relativization .... نسبی سازی
Root .... ریشه
Satisfy .... ارضاء کردن
Skolem Arithmetic .... حساب اسکولم
Structure .... ساختار
Successor .... تالی
Syntactic Proof .... برهان نحوی
Tarski's Identity .... اتحاد تارسکی
Theory .... نظریه
Trivial .... بدیهی
Undecidability .... تصمیم‌ناپذیری
Undecidable .... تصمیم‌ناپذیر
Variable .... متغیر

نمایه

Surname: Assadi **Name:** Ziba

Title: Decidability of Multiplicative and Order Theory of Numbers

Supervisor: Saeed Salehi

Advisor: Jafar Sadegh Eivazloo

Degree: Ph.D. **Subject:** Pure Mathematics

Field: Mathematical Logic **University of Tabriz**

Faculty of Mathematical Sciences **Date:** 2019

Number of Pages: 74

Keywords: Decidability, Undecidability, Completeness, Incompleteness, First-Order Theory, Quantifier Elimination, Ordered Structures.

Abstract

The ordered structures of natural, integer, rational and real numbers are studied in this thesis. The theories of these numbers in the language of order are decidable and finitely axiomatizable. Also, their theories in the language of order and addition are decidable and infinitely axiomatizable. For the language of order and multiplication, it is known that the theories of $\mathbb{N}$ and $\mathbb{Z}$ are not decidable (and so not axiomatizable by a computably enumerable set of sentences). By Tarski's theorem, the multiplicative ordered structure of $\mathbb{R}$ is decidable also. In this thesis we prove this result directly by quantifier elimination and present an explicit infinite axiomatization. The structure of $\mathbb{Q}$ in the language of order and multiplication seems to be missing in the literature. We show the decidability of its theory by the technique of quantifier elimination and after presenting an infinite axiomatization for this structure we prove that it is not finitely axiomatizable.

University of Tabriz

Faculty of Mathematical Sciences

DOCTORAL THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY (Ph.D.) IN PURE MATHEMATICS,

MATHEMATICAL LOGIC

Decidability of Multiplicative and Order Theory of Numbers

Supervisor

Saeed Salehi

Advisor

Jafar Sadegh Eivazloo

by

Ziba Assadi

2019