منطق پیشرفته

محسن خانی

۲۳ دی ۱۳۹۸

چکیده

هدفهم در درس منطق پیشرفته، اثبات دو قضیه‌ی مهم گودل است: قضیه‌ی تمامیت و قضیه‌ی ناتمامیت. همچنین به بیان مصداقهائی از خوشرفتاری و بدرفتاری منطقی خواهم پرداخت. بنا به قضیه‌ی تمامیت، در منطق مرتبه‌ی اول، اگر حکمی در تمامی مدل های یک تئوری درست باشد، آن حکم با استفاده از اصول آن تئوری اثبات می شود. مثلاً اگر حکمی مرتبه‌ی اول در تمامی گروه‌های آبلی برقرار باشد، آنگاه قطعاً اثباتی برای آن حکم با استفاده از اصول موضوعه‌ی گروه‌های آبلی پیدا می‌شود. ابتدا تمامیت را تحت عنوان قضیه‌ی فشردگی، با رویکردی کاملاً نظریه‌ی مدلی ثابت خواهم کرد و سپس اثباتی برای آن با استفاده از حساب رشته‌ها ارائه خواهم کرد.

در بخش دوم درس، به قضایای ناتمامیت گودل خواهم پرداخت. بنا به ناتمامیت اول گودل، امکان ارائه یک اصل بندی کامل برای حساب توسط یک الگوریتم وجود ندارد. نیز بنا به قضیه‌ی ناتمامیت دوم گودل، یک قضیه‌ای مرتبه‌ی اول درباره اعداد طبیعی وجود دارد که این قضیه (با این که در مورد اعداد طبیعی درست است) از اصول پئانو نتیجه نمی شود. رویکردم در این قسمت از درس، بررسی مدلهای مختلف حساب، به ترتیب پیچیدگی زبان خواهد بود.

سرآخر در بخش سوم، به یک کاربرد جبری منطق خواهم پرداخت و درباره‌ی تئوری میدانهای بسته‌ی حقیقی به عنوان مصداقی از یک تئوری کامل سخن خواهم گفت.

فهم دقیق قضیه‌های بالا، البته نیازمند پشت سر گذاشتن چندین جلسه از درس است. برای خواندن یک مقدمه‌ی مفصل‌تر برای درس منطق، لطفاً به جزوه‌ی درس مبانی منطق و نظریه‌ی مجموعه‌ها، در تارنمای شخصیم مراجعه کنید. [1]

[1] تایپ اولیه‌ی جلسات به ترتیب توسط: ج۱ آرمان عطائی، ج۲ افشین زارعی، ج۳و۴و۵ آرمان عطائی، ج۶ درسا پیری، ج۷ آرمان عطائی، ج۸ گلنوش خورسندی، ج۹و۱۰ آرمان عطائی، ۱۱ نجمه زمانی، ۱۲ علیرضا محمدصالحی، ۱۳ نجمه زمانی، چهار جلسه رویا داوودی و یک جلسه مائده رحمانی صورت گرفته است.

فهرست مطالب

فصل ۱

تمامیت و خوشرفتاری‌ها

۱.۱ الفبا، بدون معانی

مطالعه‌ی هر مفهوم جبری در منطق مرتبه‌ی اول، نخست نیازمند انتخاب یک زبان مناسب است. زبان، حکمِ حروف الفبای فارسی را دارد که کلمات قرار است با استفاده از آنها ساخته شوند.

تعریف ۱ (یک زبان مرتبه‌ی اول). منظور از یک زبان مرتبه اولِ L، یک مجموعه متشکل از **نمادهایی** برای توابع، **نمادهایی** برای روابط و **نمادهایی** برای ثوابت است. برای هر نماد تابعیِ $f \in L$ یک عدد طبیعیِ n_f به نام تعداد مواضع تابع f در نظر گرفته شده است و برای نماد رابطه‌ایِ R نیز یک عدد طبیعیِ n_R به نام تعداد مواضع رابطه‌ی R در نظر گرفته شده است.

توجه ۲.

۱. نماد تابعی با تابع فرق می‌کند. بعداً قرار است متناظر با هر نماد تابعی، یک تابع واقعی پیدا کنیم که ترجمه‌ی آن نماد باشد.

۲. در یک زبانِ مرتبه‌ی اولِ L، نمادهای منطقی مانند $\wedge$ ، $\vee$ ، $\forall$ ، $\exists$ و $\cdots$ قرار ندارند. بعداً درباره‌ی جایگاه اینها در منطق مرتبه‌ی اول سخن خواهیم گفت.

برای مطالعه یک پدیده، باید زبانی را انتخاب کنیم که از پس بیان ویژگی‌های جبری آن پدیده برآید. در درسهای آینده این سخن را روشنتر خواهم کرد. در زیر مثالی از چند زبان مرتبه‌ی اول آورده‌ام.

مثال ۳ (مثالهائی از زبانهای مرتبه‌ی اول).

۱. زبان تهی: $L = \phi$ که شامل هیچ نمادی برای تابع، ثابت یا رابطه نیست.

۲. زبان گروه‌های جمعی آبلی: $L_{AbG} = \{+, -, ۰\}$. در این زبان، $+$ یک نماد تابعی دو موضعی است، $-$ یک نماد تابعی تک موضعی است و ۰ نمادی برای یک ثابت است.

۳. زبان نظریه‌ی گروه‌ها: $L_{Group} = \{\cdot, ^{-۱}, e\}$. در این زبان، $^{-۱}$ یک نماد تابعی تک‌موضعی، $\cdot$ یک نماد تابعی دوموضعی و e یک نماد برای یک ثابت است.

۴. زبان نظریه‌ی گراف: $L_{Graph} = \{R\}$. در این زبان، R یک نماد رابطه‌ای دو موضعی است.

۵. زبان حلقه‌ها: $L_{Ring} = \{+, -, \cdot, ۰, ۱\}$ که در آن $۰, ۱$ دو نماد برای دو ثابت هستند. این زبان در واقع از افزودنِ ۰ و ۱ به زبان گروه‌های جمعی آبلی به دست می‌آید.

۶. زبان نظریه‌ی مجموعه‌ها: $L_{Set} = \{\in\}$. در این زبان، علامت $\in$ یک نماد رابطه‌ای دوموضعی است.

۷. زبان نظریه‌ی اعداد: $L_{\mathbb{N}} = \{+, \cdot, ۰, ۱, s\}$ در این زبان، s یک نماد تابعی تک‌موضعی (برای تابع تالی) است.

۸. زبانِ $L = \{\leq\}$ زبان مطالعه‌ی مجموعه‌های مرتب است؛ در این زبان، $\leq$ یک نماد رابطه‌ای دوموضعی است.

۹. زبان $L_{oring} = L_{Ring} \cup \{\leq\}$ زبانی برای مطالعه‌ی حلقه‌های مرتب است.

طبیعت برخی پدیده‌ها، بخصوص فضاهای توپولوژیک، مرتبه‌ی اول نیست ولی در عین حال برخی فضاهای توپولوژیک که ساختار جبری دارند،مرتبه‌ی اول هستند.

تمرین ۱. برای مطالعه‌ی فضاهای برداری چه زبان مرتبه‌ی اولی را پیشنهاد می‌کنید؟

بحث زبان را فعلاً رها می‌کنم. در جلسات آینده، دوباره به زبان (به بیان بهتر، به نحو) بازخواهیم گشت.

۲.۱ جبر ساختارها

در منطق مرتبه‌ی اول، جملات باید در ساختارها **معنا** شوند. مثلاً این را که «هر عنصری دارای یک وارون ضربی است» باید در یک گروه ضربی معنا کرد. آنچه در منطق (یا بهتر بگویم در نظریه‌ی مدلها) یک ساختار نامیده می‌شود، تعمیمی از تعریف همه‌ی ساختمانهای مرتبه‌ی اول جبری، مانند حلقه و گروه و غیره است.

تعریف ۴ (Lساختار). فرض کنید L یک زبان مرتبه‌ی اول باشد. منظور از یک Lساختار جفتی به صورت زیر است:

$$\mathfrak{M} = (M, (z^{\mathfrak{M}})_{z \in L})$$

که متشکل از یک مجموعه‌ی M است به نام جهان آن Lساختار، و همچنین برای هر نماد $z \in L$ یک مابازای $z^{\mathfrak{M}}$ وجود دارد که به آن تعبیر(معنای) نماد z در ساختار $\mathfrak{M}$ گفته می‌شود. این تعبیر به صورت دقیقِ زیر تعریف می‌شود.

- اگر z یک نماد ثابت باشد آنگاه $z^{\mathfrak{M}} \in M$ یک عنصر است که به آن تعبیر ثابت z گفته می شود.
- اگر z یک نماد تابعی و n تعداد مواضع آن باشد آنگاه

$$z^{\mathfrak{M}} : M^n \to M$$

یک تابع است که به آن تعبیر نماد تابعیِ z گفته می‌شود.

- اگر z یک نماد رابطه‌ای n موضعی باشد آنگاه $z^{\mathfrak{M}} \subseteq M^n$ یک رابطه است که به آن تعبیرِنماد رابطه‌ی z گفته می‌شود.

به طور خاص دقت کنید که جهان یک ساختار مرتبه‌ی اول، تحت تابع‌های تعبیرشده بسته است. همچنین این تابعها بردشان زیرمجموعه‌ی M (و نه M^n) است.

تمرین ۲. برای هر کدام از زبان‌های L در مثالِ ۳ بررسی کنید که L ساختارهای مربوطه چگونه‌اند.

تعریف ۵ (Lهومومرفیسم). فرض کنید $\mathfrak{M}$ و $\mathfrak{N}$ دو Lساختار باشند. تابع $h : M \longrightarrow N$ را یک Lهومومرفیسم می‌نامیم هرگاه حافظ ساختار باشد، به بیان دقیق هرگاه این گونه باشد که

- برای هر نماد ثابت $z \in L$

$$h(z^{\mathfrak{M}}) = z^{\mathfrak{N}}$$

- برای هر نماد تابعی n موضعی $f \in L$ و هر $a_1, \ldots, a_n \in M$

$$h(f^{\mathfrak{M}}(a_1, \cdots, a_n)) = f^{\mathfrak{N}}(h(a_1), \cdots, h(a_n))$$

- وبرای هر نماد رابطه‌ای n موضعی $R \in L$ و هر $a_1, \cdots, a_n \in M$

$$R^{\mathfrak{M}}(a_1, \cdots, a_n) \Rightarrow R^{\mathfrak{N}}(h(a_1), \cdots, h(a_n))$$

به یک طرفه بودن فلشِ بالا دقت کنید. اگر h یک به یک باشد و فلش بالا دو طرفه باشد، آنگاه h را یک نشاندن می‌نامیم. اگر h یک نشاندنِ پوشا باشد، آن را یک ایزومرفیسم می‌نامیم.

تمرین ۳. مفهوم هومومرفیسم بین Lساختارها را برای هر یک از زبانهای مثال ۳ بررسی کنید.

دقت کنید که مفاهیم بالا، تعمیم مفاهیم همنام خود در جبر گروه‌ها، حلقه‌ها، فضاهای برداری و غیره هستند.

تعریف ۶. فرض کنید $\mathfrak{M}$ یک Lساختار باشد. نگاشت $h : M \to M$ را یک اتومرفیسم می‌نامیم هرگاه h یک ایزومرفیسم باشد.

مجموعه‌ی همه‌ی اتومرفیسم‌های یک ساختار $\mathfrak{M}$ تشکیل یک گروه می‌دهد که آن را با $\mathrm{Aut}(\mathfrak{M})$ نشان می‌دهیم.

تعریف ۷. فرض کنید $\mathfrak{M}$ و $\mathfrak{N}$ دو Lساختار باشند. می‌گوییم $\mathfrak{M}$ یک زیرساختار[۱] از $\mathfrak{N}$ است و می‌نویسیم $\mathfrak{M} \subseteq \mathfrak{N}$، هرگاه نگاشت شمول (یعنی نگاشت همانی) $i : M \to N$ یک نشاندن باشد.

دقت کنید که در صورتی که $\mathfrak{M}$ زیر ساختاری از $\mathfrak{N}$ باشد، برای هر تابعِ n موضعیِ $f \in L$ داریم

$$f^{\mathfrak{M}} = f^{\mathfrak{N}} \restriction M$$

همچنین برای هر رابطه‌ی n موضعیِ $R \in L$ داریم

$$R^{\mathfrak{M}} = R^{\mathfrak{N}} \cap M^n$$

همچنین برای هر ثابتِ $c \in L$ داریم

$$c^{\mathfrak{N}} = c^{\mathfrak{M}}$$

همه‌ی عبارتهای بالا بیانگر این هستند که نگاشتِ همانی یک نشاندن است.

[۱] substruture

حال فرض کنید که $\mathfrak{M}$ یک Lساختار باشد و $A \subseteq M$؛ یعنی A یک مجموعه باشد که زیرمجموعه‌ای از جهانِ $\mathfrak{M}$ است. دقت کنید که A خودش یک Lساختار نیست و فقط یک مجموعه است. در ادامه می‌خواهیم بگوییم که در چه صورت A جهان زیرساختار از $\mathfrak{M}$ می‌تواند باشد. یعنی در چه صورتی یک ساختارِ $\mathfrak{A}$ وجود دارد به طوری که $\mathfrak{A} \subseteq \mathfrak{M}$ و جهان $\mathfrak{A}$ مجموعه‌ی A است.

طبیعتاً اگر A جهان یک زیرساختار از $\mathfrak{M}$ باشد، اولاً برای هر ثابت $c \in L$ داریم $c^{\mathfrak{M}} \in A$؛ ثانیاً برای هر تابع n موضعی $f \in L$ و برای هر $a_1, \ldots, a_n \in A$ داریم $f^{\mathfrak{M}}(a_1, \ldots, a_n) \in A$. به بیانی دیگر A باید تحت ثوابت و توابع زبان بسته است.

تمرین ۴. نشان دهید که همین کافی است؛ یعنی اگر $\mathfrak{M}$ یک Lساختار باشد و $A \subseteq M$، آنگاه A جهان یک زیرساختارِ $\mathfrak{A} \subseteq \mathfrak{M}$ است اگروتنهااگر تحت ثوابت و توابعِ $\mathfrak{M}$ بسته باشد.

پس اگر زبان L شامل هیچ نماد تابعی و نماد ثابتی نباشد (یعنی فقط شامل نمادهای رابطه‌ای باشد) آنگاه هر زیرمجموعه‌ی ناتهی $A \subseteq M$ جهان یک زیرساختار از $\mathfrak{M}$ است.

لم ۸. فرض کنید $(\mathfrak{M}_i)_{i\in I}$ خانواده‌ای از زیرساختارهای یک Lساختار $\mathfrak{N}$ باشد. در این صورت $\bigcap M_i$ جهان یک زیرساختار از $\mathfrak{N}$ است (اگر تهی نباشد).

اثبات. برای هر ثابتِ $c \in L$ عنصر $c^{\mathfrak{N}}$ در تمام M_i ها قرار دارد. همچنین برای عناصرِ $(a_1, \ldots, a_n) \in \bigcap M_i$ بنا به زیرساختار بودن تک‌تکِ $\mathfrak{M}_i$ ها می‌دانیم که $f^{\mathfrak{N}}(a_1, \ldots, a_n) \in \bigcap M_i$. همین دوشرط بنا به تمرین بالا کافی است. □

زیرساختاری را که در لم قبل بدان اشاره شد با $\bigcap \mathfrak{M}_i$ نشان می‌دهیم.

گفتیم که اشتراک هر خانواده از زیرساختارها، یک زیرساختار است. اگر $\mathfrak{N}$ یک Lساختار باشد و $A \subseteq N$ (زیرمجموعه) آنگاه زیرساختار تولید شده توسط A در $\mathfrak{N}$ را اشتراک همه‌ی زیرساختارهائي از $\mathfrak{N}$ می‌گیریم که جهانشان شامل A است. به بیان دیگر تعریف می‌کنیم

$$\langle A\rangle^{\mathfrak{N}} = \bigcap\{\mathfrak{M} | \mathfrak{M} \subseteq \mathfrak{N}, A \subseteq M\}$$

به بیان دیگر $\langle A\rangle^{\mathfrak{N}}$ کوچکترین زیرساختاری از $\mathfrak{N}$ است که جهان آن شامل A است. اگر A متناهی باشد و $\mathfrak{M} = \langle A\rangle^{\mathfrak{N}}$ می‌گوییم $\mathfrak{M}$ یک زیرساختار متناهیاًتولید شونده از $\mathfrak{N}$ است. در جلسات آینده اعضای این زیرساختار را به طور صریح مشخص خواهیم کرد.

توجه ۹. اگر زبان L شامل حداقل یک نماد ثابت باشد و $A = \emptyset$ آنگاه

$$\langle\emptyset\rangle^{\mathfrak{N}} = \bigcap_{\mathfrak{M}\subseteq\mathfrak{N}} \mathfrak{M}.$$

یعنی در زبانی که ثابت دارد، ساختار تولید شده توسط تهی، تهی نیست.

لم ۱۰. فرض کنید $A \neq \emptyset$ و $\mathfrak{M} = \langle A\rangle^{\mathfrak{M}}$، (دقت کنید که لزوماً M برابر با A نیست؛ یعنی جهان ساختار تولید شده توسط A شاید از خودِ مجموعه‌ی A بزرگتر باشد) آنگاه هر هومومرفیسم $h : \mathfrak{M} \to \mathfrak{N}$ تنها توسط مقادیر h روی A تعیین می‌شود؛ یعنی اگر $h_1 : \langle A\rangle^{\mathfrak{M}} \to \mathfrak{N}$ و $h_2 : \langle A\rangle^{\mathfrak{M}} \to \mathfrak{N}$ دو هومومرفیسم باشند، در این صورت اگر برای هر $a \in A$ داشته باشیم $h_1(a) = h_2(a)$، آنگاه برای هر $x \in M$ داریم $h_1(x) = h_2(x)$.

اثبات. فرض کنید $h_۱, h_۲ : \langle A \rangle^{\mathfrak{M}} \to \mathfrak{N}$ دو هومورفیسم باشند که روی A مقادیر یکسانی دارند. قرار دهید

$$B = \{x \in M | h_۱(x) = h_۲(x)\}.$$

می‌خواهیم نشان دهیم که $B = M$. (یعنی می‌خواهیم نشان دهیم که روی تمام نقاطِ ساختار تولیدشده، این دو هومورفیسم با هم برابرند). واضح است که $A \subseteq B$ زیرا فرض کرده‌ایم که روی A این دو هومورفیسم مقادیر یکسانی دارند.

ادعا می‌کنیم که مجموعه‌ی B جهان یک زیرساختار از $\mathfrak{M}$ است.

برای اثبات ادعای بالا کافی است نشان دهیم که B تحت ثوابت و روابطِ $\mathfrak{M}$ بسته است.

اولاً برای هر ثابت c داریم $h_۱(c^{\mathfrak{M}}) = h_۲(c^{\mathfrak{M}})$. پس $c^{\mathfrak{M}} \in B$ و همچنین بنا به هومورفیسم بودن داریم $c^{\mathfrak{N}} = c^{\mathfrak{M}}$. ثانیاً برای عناصر $b_۱, \ldots, b_n \in B$ داریم $f^{\mathfrak{M}}(b_۱, \ldots, b_n) \in B$؛ زیرا $h_۱(b_i) = h_۲(b_i)$ و بنابراین

$$h_۱(f^{\mathfrak{M}}(b_۱, \ldots, b_n)) = f^{\mathfrak{N}}(h_۱(b_۱), \ldots, h_۱(b_n)) = f^{\mathfrak{N}}(h_۲(b_۱), \ldots, h_۲(b_n)) = h_۲(f^{\mathfrak{M}}(b_۱, \ldots, b_n)).$$

تا اینجا نشان دادیم که B جهان یک زیرساختار از $\mathfrak{M}$ است. کوچکترین زیرساختار شاملِ A همان $\mathfrak{M}$ است پس $M \subseteq B$. از آنجا که $B \subseteq M$ داریم $M = B$. □

لم ۱۱. فرض کنید $h : \mathfrak{M} \xrightarrow{\sim} \mathfrak{M}'$ یک ایزومرفیسم باشد و $\mathfrak{M} \subseteq \mathfrak{N}$. در این صورت Lساختار $\mathfrak{M}' \subseteq \mathfrak{N}'$ به همراه ایزومرفیسم $h' : \mathfrak{N} \to \mathfrak{N}'$ موجود است به طوری که h' توسیعی از h است.

اثبات. یک مجموعه‌ی $M' \subseteq N'$ و یک تابع یک‌به‌یک و پوشای h' بین N و N' پیدا کنید که توسیع h باشد. آنگاه با استفاده از h' مجموعه‌ی N' را تبدیل به جهان یک Lساختار بکنید. مثلاً تعریف کنید:

$$f^{\mathfrak{N}'}(h'(a_۱), h'(a_۲)) := h'(f^{\mathfrak{N}}(a_۱, a_۲)).$$

□

آنچه که در لم زیر بدان پرداخته‌ایم، تعمیمی از مفاهیم جبری حد مستقیم و حد معکوس [۲] است.

لم ۱۲. فرض کنید $(I, \leq)$ یک مجموعه‌ی مرتب جزئی جهتدار [۳] باشد. همچنین فرض کنید $(\mathfrak{M}_i)_{i \in I}$ یک خانواده‌ی جهتدار از Lساختارها باشد؛ یعنی به گونه‌ای باشد که اگر $i_۱ \leq i_۲$ آنگاه $\mathfrak{M}_i \subseteq \mathfrak{M}_j$. در این صورت $\bigcup M_i$ جهان یک Lساختار است که همه‌ی $\mathfrak{M}_i$ها زیرساختاری از آن هستند.

اثبات. باید بتوانیم تمامی علائم زبانی را در $\bigcup M_i$ تعبیر کنیم. در زیر این کار برای روابط انجام داده‌ام؛ با توابع و ثوابت می‌توان رفتار مشابهی داشت:

فرض کنید $a_۱, \ldots, a_n \in \bigcup M_i$ و $R \in L$. در این صورت $j \in I$ موجود است به طوری که تمام a_i ها در M_j هستند. تعریف می‌کنیم

$$R^{\bigcup \mathfrak{M}_i}(a_۱, \ldots, a_n) \iff R^{\mathfrak{m}_j}(a_۱, \ldots, a_n)$$

[۲] direct/inverse limit

[۳] مجموعه‌ای مرتب به‌طوری که برای هر $i_۱, i_۲ \in I$ عنصر $j \in I$ موجود است به طوری که $j \geq i_۱$ و همچنین $j \geq i_۲$.

تعریف بالا، خوش‌تعریف است؛ یعنی به j بستگی ندارد. زیرا اگر تمام a_i ها در یک $\mathfrak{M}_k$ دیگر باشند، آنگاه ساختاری مانند $\mathfrak{M}_l$ شامل $\mathfrak{M}_k, \mathfrak{M}_j$ در کلاس هست و این موجب می‌شود که تعبیر این رابطه در هر سه‌ی این ساختارها یکسان شود:

$$R^{\mathfrak{M}_j}(a_1, \ldots, a_n) \Leftrightarrow R^{\mathfrak{M}_l}(a_1, \ldots, a_n) \Leftrightarrow R^{\mathfrak{M}_k}(a_1, \ldots, a_n).$$

□

در بالا درباره‌ی زیرساختار بودن سخن گفتیم. دقت کنید که مثلاً

$$(\mathbb{Q}, +, \cdot) \subseteq (\mathbb{R}, +, \cdot)$$

در بالا (یعنی در تعریف زیرساختار) زبانها یکسانند ولی جهانها تغییر کرده‌اند. در مفهوم تعریف‌شده‌ی زیر، جهانها یکسانند ولی زبان بزرگتر شده است.

تعریف ۱۳. فرض کنید $L \subseteq K$ دو زبان مرتبه‌ی اول باشند. در این صورت Kساختار $\mathfrak{N}$ را یک تقلیل از Lساختار $\mathfrak{M}$ می‌نامیم هرگاه جهانهای M و N یکسان باشند و $\mathfrak{N} = \mathfrak{M} \restriction_K$. دقت کنید که در این صورت $\mathfrak{M}$ را بسطی از $\mathfrak{N}$ می‌نامیم. [۴]

در زیر چند مثال از بسط زبان آورده‌ایم.

مثال ۱۴. فرض کنید $\mathfrak{M}$ یک Lساختار و R یک رابطه روی M^n باشد. قرار دهید $L' = L \cup \{R\}$. در این صورت $\mathfrak{M}$ تقلیلی از L'ساختارِ $\mathfrak{M}' = (\mathfrak{M}, R)$ است که در آن $R^{\mathfrak{M}'}$ همان رابطه‌ی R تعبیر شده است.

مثال ۱۵. فرض کنید $\mathfrak{M}$ یک Lساختار باشد و $m_1, \ldots, m_n \in M$. زبان $L' = L \cup \{c_{m_1}, \ldots, c_{m_n}\}$ را در نظر بگیرید که در آن ثوابتی برای این اعضای M وجود دارد. حال $\mathfrak{A} = (\mathfrak{M}, m_1, \ldots, m_n)$ را به عنوان یک L'ساختار در نظر بگیرید که در آن $c_{c_{m_i}}^{\mathfrak{A}} = m_i$.

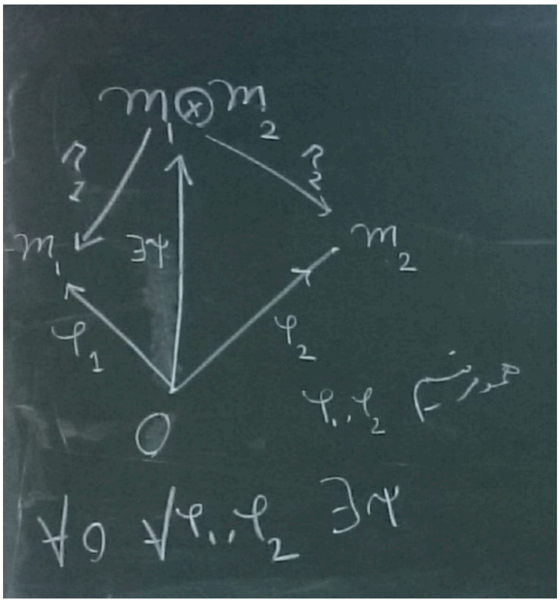
مثال ۱۶. فرض کنید $\mathfrak{M}$ یک Lساختار باشد و $A \subseteq M$. قرار دهید $L \subseteq L_A = L \cup \{c_a | a \in A\}$. در این صورت یک بسط از Lساختارِ $\mathfrak{M}$ به زبان L_A وجود دارد:

$$\mathfrak{M}_A = (\mathfrak{M}, \{a\}_{a\in A}), \qquad c_a^{\mathfrak{M}} = a$$

در این صورت گروه اتومرفیسم‌های روی $\mathfrak{M}_A$ یعنی $\mathrm{Aut}(\mathfrak{M}_A)$ در زبان L_A برابر است با اتومرفیسم‌هایی از M که روی اعضای A ثابت هستند. این گروه را با $\mathrm{Aut}(\frac{\mathfrak{M}}{A})$ نیز نشان می‌دهیم.

تمرین ۵ (حاصل‌ضرب در کاتگوری Lساختارها و Lهومومرفیسم‌ها). فرض کنید $\mathfrak{M}_1$ و $\mathfrak{M}_2$ دو Lساختار باشند. روی $M_1 \times M_2 = \{(x,y) | x \in M_1, y \in M_2\}$ یک Lساختار تعریف کنید (یعنی اجزای زبانِ L را به گونه‌ای تعبیر کنید) که $\mathfrak{M}_1 \otimes \mathfrak{M}_2$ (نامی که شما روی Lساختار جدید گذاشته‌اید) ویژگی جهانی زیر را داشته باشد.

[۴] وقتی که $\mathfrak{N} \subseteq \mathfrak{M}$ در انگلیسی گفته به این نوع گسترش یک *extension* گفته می‌شود. وقتی مانند تعریف بالا، $\mathfrak{M}$ بسطی از $\mathfrak{N}$ باشد، در انگلیسی به این نوع گسترش *expansion* گفته می‌شود. در فارسی شاید خوب باشد اولی را توسیع و دومی را بسط بنامیم.



دقت کنید که π_i نگاشتهای هومرفیسمِ پوشای طبیعیِ

$$\pi_i : \mathfrak{M}_1 \times \mathfrak{M}_2 \to \mathfrak{M}_i$$

هستند. تصویر بیان اگر این است که برای هر Lساختارِ $\mathfrak{D}$ و هومرفیسمهای $\phi_i : \mathfrak{D} \to \mathfrak{M}_i$، هومرفیسمِ $\psi : \mathfrak{D} \to \mathfrak{M}_1 \times \mathfrak{M}_2$ موجود باشد به طوری که دیاگرام کشیده شده جابه‌جائی باشد.

تمرین ۶. فرض کنید $f : \mathfrak{M} \to \mathfrak{M}$ یک نشاندن باشد. نشان دهید که یک Lساختار $\mathfrak{N} \supseteq \mathfrak{M}$ و یک اتومرفیسم $g : \mathfrak{N} \to \mathfrak{N}$ موجود است به طوری که $g|_{\mathfrak{M}} = f$ و $(\mathfrak{N}, g)$ تحت این شرط که N اجتماع زنجیر زیر است و

$$M \subseteq g^{-1}(M) \subseteq g^{-2}(M) \subseteq \ldots$$

یکتاست.

زبان و ساختار چندبخشی

تا کنون هر ساختار مرتبه‌ی اولی که مشاهده کردیم دارای یک جهان مشخص بود و توابع و روابط روی همان جهان تعریف شده بودند. اما در بسیاری ساختارهای ریاضی، بیش از یک جهان وجود دارد و میان جهانها توابع و روابطی وجود دارد. این خواسته به راحتی در ساختارهای مرتبه‌ی اول قابل گنجاندن است. در زیر ساختارها و زبانهای چند بخشی را تعریف کرده‌ایم. در درس دوباره به آنها بازنخواهیم گشت ولی هر قضیه‌ای که درس ثابت کنیم درباره‌ی آنها نیز درست است.

تعریف ۱۷. زبان L را یک زبان S بخشی گوییم هرگاه دارای روابط از نوع $(s_1, \ldots, s_n)$ ، توابع از نوع $(s_1, \ldots, s_n, t)$ و ثوابت از نوع s_i باشد. متناظر با یک زبان Sبخشیِ L، Lساختارهای S بخشی به صورت زیر هستند.

$$\mathfrak{M} = ((A_s)_{s \in S}, (z^{\mathfrak{M}})_{z \in L})$$

که در آن هر A_s یک جهان از نوع s نامیده می‌شود و

- اگر $z \in L$ یک نماد ثابت از نوع s_i باشد، $z^{\mathfrak{M}} \in A_{s_i}$.

- اگر $z \in L$ یک نماد تابعی از نوع $(s_1, ..., s_n, t)$ باشد،

$$z^{\mathfrak{M}} : A_{s-1} \times A_{s_2} \times ... \times A_{s_n} \to A_t$$

یک تابع است.

- اگر $z \in L$ یک نماد رابطه‌ای از نوع $(s_1, ..., s_n)$ باشد،

$$z^{\mathfrak{M}} \subseteq A_{s-1} \times A_{s_2} \times ... \times A_{s_n}$$

یک رابطه است.

در نوشتن فرمولهای چندبخشی، سورها و متغیرها می‌توانند مربوط به بخشهای خاصی باشند.

مثال ۱۸. گروه‌های جایگشتی را می‌توان به عنوان ساختارهای دوبخشی در نظر گرفت.

$$(X, G, g : G \times X \to X, e^G, .^G, ()^{-1^G})$$

در یک گروه جایگشتی، یک مجموعه‌ی X داریم که یک گروه G اعضای آن را جابه‌جا می‌کند.

مثال ۱۹. میدان های ارزیابی را می‌توان به عنوان ساختارهای سه‌بخشی در نظر گرفت: [5]

$$(K, \Gamma, k, V : K \to \Gamma)$$

یک میدان ارزیابی از یک میدان K تشکیل شده است و یک گروه Γ و یک نگاشت ارزیابیِ $v : K \to \gamma$. این نگاشت منجر به ایجاد یک میدانِ k به نام میدان پیمانه‌ها می‌شود. [6]

۳.۱ ادامه‌ی مبحث زبان

فرض کنید L یک زبان مرتبه اول باشد.یک مجموعه $x_1, x_2, \cdots$ از متغیرها را در نظر بگیرید. به هر دنباله متناهی‌ای که از علائم زبانیِ تابع، ثابت و با استفاده از این متغیرها، و البته با قوانین خاصی، ساخته شود یک Lترم یا یک Lکلمه گفته می‌شود. هر دنباله‌ی دلخواه از ثوابت و توابع و متغیرها ترم نیست. در زیر به صورت استقرائی بیان کرده‌ایم که دقیقاً کدام دنباله‌ها ترم هستند.

تعریف ۲۰ (تعریف دقیق)**.** مجموعه‌ی Lترم‌ها به صورت استقرایی زیر تعریف می شود.

- هر ثابت $c \in L$ و هر متغیر x_i یک Lترم محسوب می شود.

- هرگاه بدانیم که $t_1, \cdots, t_n$ چند L ترم هستند و $f \in L$ یک تابع n موضعی باشد، آنگاه $f(t_1, \cdots, t_n)$ یک Lترم است.

[5] valued field

[6] انشاءالله زمانی درباره‌ی میدانهای ارزیابی درس خواهم داد!

مثال ۲۱. در زبانِ $L_{AbG}=\{+,(-),۰\}$ موارد زیر Lترم هستند.

- ۰
- $۰+۰$
- $x+\cdots+x$ (گاهی به جای این به طور خلاصه می‌نویسیم nx.)
- $x_۱+x_۲+x_۳$
- $nx_۱+mx_۲+kx_۳$.

دقت کنید که در نوشتن ترمهای بالا ساده‌سازیهای استفاده شده است. مثلاً به جای دنباله‌ی $++x_۱x_۲x_۳$ نوشته‌ایم $x_۱+x_۲+x_۳$.

مثال ۲۲. در زبانِ $L_{ring}=\{+,\cdot,۰,۱,(-)\}$ موارد زیر Lترم هستند.

- $۱+۰$
- $۱\cdot۰$
- $۱+۱+۱$
- $x_۱+x_۲+x_۳$
- $x_۱\cdot x_۲\cdot x_۳$
- $۵x_۱x_۲^۲+۶x_۴x_۷^۳x_۸$ (دقت کنید که عدد ۵ جزو ترم نیست. تنها منظورم پنج بار نوشتن جمع بوده است. توان هم به همین صورت).

تعریف ۲۳ (تعبیرترمهادرساختارها). فرض کنید که $\mathfrak{M}$ یک Lساختار باشد. فرض کنید $t(x_۱,\cdots,x_n)$ یک Lترم باشد و $a_۱,\cdots,a_n\in M$. در این صورت عنصری در جهان ساختارِ $\mathfrak{M}$ ،جود دارد که آنرا با $t^{\mathfrak{M}}(a_۱,\cdots,a_n)$ (تعبیر ترم t در ساختار $\mathfrak{M}$ با جایگذاریِ a_i به جای x_i) نشان می‌دهیم. این عنصر به صورت استقرائی زیر تعریف می‌شود.

- اگر $t=c$ یک ثابت باشد

$$c^{\mathfrak{M}}(a_۱,\cdots,a_n)=c^{\mathfrak{M}}$$

- اگر $t=x_i$ یک متغیر باشد آنگاه

$$x_i^{\mathfrak{M}}(a_۱,\ldots,a_n)=a_i.$$

- اگر $t_i^{\mathfrak{M}}(a_۱,\cdots,a_n)$ دانسته باشند و f یک تابع n موضعی باشد آنگاه تعبیر $f(t_۱,\ldots,t_n)$ در M با جایگذاریِ a_i به جای x_i به صورت زیر تعریف می‌شود:

$$[f(t_۱,\ldots,t_n)]^{\mathfrak{M}}(a_۱,\ldots,a_n)=f^{\mathfrak{M}}(t_۱^{\mathfrak{M}}(a_۱,\cdots,a_n),\ldots,t_n^{\mathfrak{M}}(a_۱,\cdots,a_n))).$$

مثال ۲۴. در زبان $L = L_{ring}$ در ساختار $R = (\mathbb{R}, +, \cdot, -, ۰, ۱)$ داریم

$$[۲x_۱x_۲^۲ + x_۳^۴]^R(۱, ۲, ۳) = ۸۹$$

قبلاً دربارهی ساختار تولید شده توسط یک مجموعه صحبت کردهایم. در لم زیر که اثبات آن جزو تمرینهاست، خواهیم دید که ساختار تولید شده توسط جایگذاری عناصرِ A در ترمها حاصل میشود.

لم ۲۵. فرض کنید $\mathfrak{M}$ یک Lساختار باشد و $A \subseteq M$. آنگاه

$$\langle A\rangle^{\mathfrak{M}} = \bigcap_{A\subseteq N, \mathfrak{N}\subseteq\mathfrak{M}} \mathfrak{N} = \{t^{\mathfrak{M}}(a_۱, \cdots, a_n) | a_۱, \cdots, a_n \in A, \text{یک ترم است } t, n \in \mathbb{N}\}$$

اثبات. تمرین. $\square$

توجه ۲۶. اگر زبان L حاوی ثوابت باشد، آنگاه

$$\emptyset \neq \langle\phi\rangle^{\mathfrak{M}} = \{t^{\mathfrak{M}}(c_۱^{\mathfrak{M}}, \cdots, c_n^{\mathfrak{M}}) | n \in \mathbb{N} \text{ و } c_i \text{ ترم است و } t \text{ ها ثوابت هستند}\}$$

بنا به لم قبلی، حداکثر اندازهی ساختار تولید شده توسط A به صورت زیر تعیین میشود: (با توجه به این که هر ترم یک دنبالهی متناهی از علائم است، در صورتی که زبنا نامتناهی باشد، تعداد ترمهای بیشتر از اندازهی زبان نمیشود)

نتیجه ۲۷. $\langle A\rangle^{\mathfrak{M}} \leq \max\{| L | + \aleph_۰, | A |\}$

گفتیم که زبان حکم حروف الفبا را دارد و ترمها حکم کلمهها را. آخرین چیزی که باید تعریف شود، جملهها (یا فرمولها) هستند. Lفرمولها دنبالههائی متناهی هستند که با استفاده از ترم های زبان و علائم منطقی $\neg$ و $\wedge$ و $\exists$ و
و علامت تساوی ساخته می شوند. دوباره دقت کنید که هر دنبالهی متناهی این چنین یک فرمول نیست. پس باید فرمولها را به صورت دقیقتر تعریف کرد.

تعریف ۲۸ (فرمولها)**.** مجموعه L فرمولها کوچکترین مجموعه ای است که اعضایش از طریق زیر حاصل می شود.

- برای هر دو ترم $t_۱$ و $t_۲$ عبارت $t_۱(x_۱, \cdots, x_n) = t_۲(x_۱, \cdots, x_n)$ یک L فرمول است.
- برای ترم های $t_۱, \cdots, t_n$ و رابطه ی n موضعی R عبارت $R(t_۱, \cdots, t_n)$ یک L فرمول است.
- اگر ϕ فرمول باشد دراینصورت $\neg\phi$ نیز یک فرمول است.
- اگر ϕ و ψ دو L فرمول باشند در این صورت $\phi \wedge \psi$ یک L فرمول است.
- اگر ϕ یک فرمول باشد دراین صورت $\exists x\phi(x)$ نیز یک L فرمول است.

یک سری کوتاهنوشت نیز به صورت زیر داریم:

۱. $\phi \vee \psi \equiv \neg(\neg\phi \wedge \neg\psi)$

۲. $\forall x\psi \equiv \neg(\exists x\neg\psi)$

۳. $\phi \to \psi \equiv \neg\phi \vee \psi$.

تعریف ۲۹ (متغیر های پایبند و آزاد). متغیر x را در فرمول ϕ آزاد گوییم هرگاه تحت تاثیر هیچ سوری نباشد؛ در غیر این صورت آن را پایبند می‌نامیم.

مثال ۳۰. در فرمول زیر

$$\forall x \psi(x) \wedge R(x,y)$$

متغیر x اول پای‌بند است و x دوم آزاد است و y آزاد است. برای تشخیص این نیاز به دانستن ترتیب اولویت نمادهاست. فرمول بالا به صورت زیر پرانتزگذاری می‌شود:

$$((\forall x \psi(x)) \wedge R(x,y))$$

آخرین چیزی که می‌خواهیم تعریف کنیم این است که چه زمانی می‌گوئیم یک فرمول در یک ساختار درست است.

تعریف ۳۱. فرض کنید $\phi(x_۱,\cdots,x_n)$ یک L فرمول و $\mathfrak{M}$ یک L ساختار باشند و $a_۱,\cdots,a_n \in M$. در این صورت عبارت $\mathfrak{M} \models \phi(a_۱,\cdots,a_n)$ (خوانده شود: فرمول ϕ با جایگذاری a_i به جای x_i در ساختارِ $\mathfrak{M}$ درست است، یا $\mathfrak{M}$ مدلی برای این فرمول است) به صورت استقرایی زیر تعریف می شود.

- $\mathfrak{M} \models t_۱(a_۱,\cdots,a_n) = t_۲(a_۱,\cdots,a_n)$ هرگاه $t_۱^{\mathfrak{M}}(a_۱,\cdots,a_n) = t_۲^{\mathfrak{M}}(a_۱,\cdots,a_n)$
- $\mathfrak{M} \models R(t_۱,\cdots,t_n)(a_۱,\ldots,a_n)$ هرگاه $R^{\mathfrak{M}}(t_۱^{\mathfrak{M}}(a_۱,\ldots,a_n),\cdots,t_n^{\mathfrak{M}}(a_۱,\ldots,a_n))$
- $\mathfrak{M} \models \phi \wedge \psi$ هرگاه $\mathfrak{M} \models \phi$ و $\mathfrak{M} \models \psi$
- $\mathfrak{M} \models \neg\phi$ هرگاه $\mathfrak{M} \not\models \phi$
- $\mathfrak{M} \models \exists x \psi(x)$ هرگاه $a \in M$ عنصر در M موجود باشد به طوری که $\mathfrak{M} \models \psi(a)$

توجه ۳۲. دقت کنید که امکان دارد یک L فرمولِ یکسان در یک L ساختار درست باشد ولی در L ساختار دیگر غلط باشد. برای مثال در L_{ring} هم $(\mathbb{R},+,\cdot,-,۰,۱)$ یک L ساختار است و $(\mathbb{C},+,\cdot,-,۰,۱)$. با این حال

$$(\mathbb{C},+,\cdot,-,۰,۱) \models \exists x \quad x\cdot x = ۱$$

ولی

$$(\mathbb{R},+,\cdot,-,۰,۱) \not\models \exists x \quad x\cdot x = ۱$$

۴.۱ تئوریها

تمرین ۷. فرض کنید $h:\mathfrak{M} \longrightarrow \mathfrak{N}$ یک هومومرفیسم باشد. نشان دهید که آنگاه برای هر ترم t داریم:

$$t^{\mathfrak{M}}(a_۱,\cdots,a_n) \longmapsto^{h} t^{\mathfrak{N}}(h(a_۱),\cdots,h(a_n)).$$

تعریف ۳۳. فرض کنید $\phi(x_1,...,x_n)$ و $\psi(x_1,...,x_n)$ دو L فرمول باشند. می‌گوییم ایندو معادلند و می‌نویسیم

$$\phi \equiv \psi$$

هرگاه در هر L ساختار $\mathfrak{M}$ داشته باشیم

$$\{(x_1,...,x_n) \in M^n \mid \phi(x_1,...,x_n)\} = \{(x_1,...,x_n) \in M^n \mid \psi(x_1,...,x_n)\}.$$

برای مثال دو L فرمول $\neg(\exists x \phi(x))$ و $\forall x \neg\phi(x)$ معادلند.

تمرین ۸. فرض کنید $\phi(x_1,...,x_n)$ یک L فرمول باشد که هیچ سوری ندارد. در این صورت نشان دهید که ϕ دارای معادلی به صورت نرمال عطفی و معادلی به صورت نرمال فصلی است. [۷]

تمرین ۹. فرض کنید $\mathfrak{M}$ و $\mathfrak{N}$ دو L ساختار باشند و $h : \mathfrak{M} \longrightarrow \mathfrak{N}$ یک ایزومرفیسم باشد. نشان دهید که در این صورت برای هر Lفرمول $\phi(x_1,\cdots,x_n)$ و هر $a_1,\cdots,a_n \in M$ داریم

$$\mathfrak{M} \models \phi(a_1,\cdots,a_n) \Leftrightarrow \mathfrak{N} \models \phi(h(a_1),\cdots,h(a_n)).$$

تمرین ۱۰. فرض کنید $h : \mathfrak{M} \longrightarrow \mathfrak{N}$ یک نشاندن باشد. نشان دهید که برای هر فرمول وجودی، یعنی هر فرمولی که در ابتدای آن فقط سورهای وجودی آمده است و پس از آن فرمولی بدون سور قرار گرفته است، مانندِ $\phi(x_1,\cdots,x_n)$ و هر $a_1,\cdots,a_n \in M$ داریم

$$\mathfrak{M} \models \phi(a_1,\cdots,a_n) \Leftrightarrow \mathfrak{N} \models \phi(h(a_1),\cdots,h(a_n)).$$

منظور از یک Lجمله یک L فرمولِ بدون متغیر آزاد است. برای مثال در زبان $L_{ring} = \{+,\cdot,(-),0,1\}$ فرمولهای زیر L_{ring} جمله‌اند.

- $\forall x \exists y \quad x+y=0$
- $\forall x \exists y \quad x \cdot y=0$

ممکن است یک Lجمله‌ی ϕ در یک Lساختار درست و در دیگری نادرست باشد، مثلاً

$$\mathbb{C} \models \exists x \quad x^2=-1$$

در حالی که

$$\mathbb{R} \not\models \exists x \quad x^2=-1.$$

با این حال چیزی که برای مهم است ارائه‌ی اصول موضوعه برای بخشهائی از ریاضی است که این کار تحت تئوری‌ها صورت می‌گیرد.

[۷] صورت نرمال عطفی یعنی به صورت $\bigwedge_{i=1}^{n}\bigvee_{j=1}^{m}\psi_{ij}$ و صورت نرمال فصلی یعنی به صورت $\bigvee_{i=1}^{n}\bigwedge_{j=1}^{m}\psi_{ij}$ که در ایندو ψ_{ij} ها فرمولهای اتمی یا نقیض اتمی هستند.

تعریف ۳۴. منظور از یک Lتئوری مجموعه‌ای از L جمله‌هاست.

مثال ۳۵. اگر $L_{AbG} = \{+, -, ۰\}$ زبان گروه های آبلی باشد، آنگاه تئوری گروه‌های آبلی در این زبان، مجموعه‌ای از جملات به شکل زیر است:

$$T_{AbG} = \{\forall xyz \quad x + (y + z) = (x + y) + z, \forall x \quad x + (-x) = x, \forall xy \quad x + y = y + x, \forall x \quad x + ۰ = x\}$$

اگر T یک تئوری مرتبه‌ی اول در زبان L و $\mathfrak{M}$ یک L ساختار باشد، در این صورت می‌گوئیم که $\mathfrak{M}$ مدلی برای T است، و می‌نویسیم $\mathfrak{M} \models T$ هرگاه تمام جملات موجود در T در $\mathfrak{M}$ برقرار باشند. برای مثال $(\mathbb{R}, +, -, ۰) \models T_{AbG}$.

در زیر چند مثال از تئوریها را بررسی کرده‌ایم.

- در زبانِ $L_{ring} = L_{AbG} \cup \{\cdot, ۱\}$ تئوری زیر را تئوری حلقه‌های جابجائی می‌نامیم:

$$T_{ring} = T_{AbG} \cup \{\forall xyz \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x \quad x \cdot ۱ = x, \forall xyz \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$
$$\forall x \quad x \cdot y = y \cdot x\}$$

- در همان زبان تئوری میدانها به صورت زیر است: $T_{field} = T_{ring} \cup \{\forall x (x \neq ۰ \to \exists y x \cdot y = ۱)\}$

تمرین ۱۱ . یک تئوری برای میدانهای بسته جبری بنویسید.

تمرین ۱۲ . یک تئوری در زبان $\{<\}$ برای مجموعه‌های مرتب خطی چگالِ بدون عنصر ابتدا و انتها بنویسید.

برای مثال یک تئوری برای مجموعه های نامتناهی می‌تواند بدین صورت نوشته شود. زبان را تهی می‌گیریم: $L = \emptyset$. و قرار می‌دهیم:

$$T_{inf-set} = \{\exists x_۱ x_۲ \neg(x_۱ = x_۲),$$
$$\exists x_۱ x_۲ x_۳ \neg(x_۱ = x_۲) \wedge \neg(x_۲ = x_۳) \wedge \neg(x_۳ = x_۱)$$
$$\vdots$$
$$\}$$

دقت کنید که اگر $\mathfrak{M}$ یک ساختار باشد که در آن تمام جمله‌های بالا برقرار باشند، آنگاه M نامتناهی است.

تمرین ۱۳ . آیا می توانید یک تئوری T

- الف. برای مجموعه‌های ۵ عضوی بنویسید.
- ب. برای مجموعه‌های متناهی بنویسید.

در تمرین بالا، با اولین نکته درباره‌ی تئوری‌های مرتبه‌ی اول آشنا شده‌ایم، و آن این است که برای چه پدیده‌هائی اصولاً می‌توان یک تئوری نوشت.

دومین نکته‌ای که در مورد یک تئوری مرتبه‌ی اول مهم است، این است که آیا این تئوری هیچ مدلی دارد یا نه. برای مثال، در زبانِ $L = L_{ring}$ تئوریِ $T = \{\forall x \exists y x + y = ۱, \neg(\forall x \exists y x + y = ۱)\}$ هیچ مدلی ندارد؛ زیرا در هیچ L ساختاری این

دو جمله نمی‌توانند همزمان درست باشند. مدل داشتن یک تئوری را تحت عنوان سازگاری می‌شناسیم. به بیان دقیقتر می‌گوئیم گوییم L تئوری T سازگار است هرگاه حداقل یک مدل داشته باشد.

و سومین نکته‌ی مهم این است که آیا یک تئوریِ T می‌تواند نسبت به یک جمله‌ی ϕ بی‌تفاوت باشد؛ بدین معنی که در برخی مدلهای تئوریِ T جمله‌ی ϕ درست باشد و در برخی دیگر نباشد. برای مثال در زبانِ L_{ring} داریم $\mathbb{C} \models T_{ring}$ $\mathbb{R} \models T_{ring}$ با این حال

$\mathbb{C} \models \exists x x^۲ = -۱$

$\mathbb{R} \not\models \exists x x^۲ = -۱$. این سومین نکته را تحت عنوان «کامل بودن» یک تئوری بررسی می‌کنیم که در ادامه تعریف شده است.

تعریف ۳۶. فرض کنید T یک L تئوری و ϕ یک L جمله باشد. می گوییم $T \models \phi$ (جمله ϕ از تئوری T نتیجه می شود) هرگاه ϕ در تمام مدل های T درست باشد؛ به عبارت دیگر هرگاه داشته باشیم

$$\mathfrak{M} \models T \Rightarrow \mathfrak{M} \models \phi.$$

برای مثال

$$T_{AbG} \models \forall x(\exists y_۱ \exists y_۲ (x + y_۱ = ۰ \wedge x + y_۲ = ۰) \rightarrow y_۱ = y_۲)$$

به بیان ساده‌تر، در هرگروه آبلی وارون هر عنصر یکتاست، پس این که وارون هر عنصر یکتاست از تئوری گروه‌های آبلی نتیجه می‌شود. اما جمله‌ی زیر

$$\exists xyz \quad \forall t \quad (t = x \vee t = y \vee t = z)$$

از تئوری گروه‌های آبلی نتیجه نمی‌شود؛ زیرا برخی گروه‌های آبلی حداکثر سه عضو دارند و برخی دیگر بیش از سه عضو دارند. به بیان دیگر، تئوری گروه‌های آبلی هم با جمله‌ی بالا سازگار است و هم با نقیض آن سازگار است.

پس $T \not\models \phi$ هرگاه T مدلی داشته باشد که در آن $\neg\phi$ درست باشد؛ به بیان دیگر $T \not\models \phi$ اگروتنهااگر $T \cup \{\neg\phi\}$ مدل داشته باشد.

تعریف ۳۷. فرض کنید T یک تئوری سازگار باشد، دراین صورت می‌گوییم T یک تئوریِ کامل است، هرگاه برای هر L جمله ϕ یا ϕ در تمام مدل های T برقرار باشد یا $\neg\phi$. به بیان دیگر T کامل است هرگاه برای هر جمله‌ی ϕ یا $T \models \phi$ یا $T \models \neg\phi$ (و این یا مانع جمع است زیرا تئوری مورد نظر ما سازگار است). باز به بیان دیگر، تئوری T کامل است هرگاه برای هر دو مدلِ $\mathfrak{M}, \mathfrak{N} \models T$ و هر جمله‌ی ϕ در زبانِ تئوری، داشته باشیم

$$\mathfrak{M} \models T \Leftrightarrow \mathfrak{N} \models T.$$

پس تئوریِ سازگارِ T کامل نیست هرگاه L جمله ϕ پیدا شود به طوریِ $T \cup \{\phi\}$ و $T \cup \{\neg\phi\}$ هر دو سازگار باشند.

تمرین ۱۴. یک جمله ϕ در زبان گروه‌های آبلی بنویسید به طوری‌که $\mathbb{Z} \models \phi$ و $\mathbb{Z} \oplus \mathbb{Z} \not\models \phi$.

گفته‌های این بخش را خلاصه می‌کنم: برای یک تئوری مرتبه‌ی اول، سازگاری و کامل بودن مهم است. برای هر پدیده‌ای، این امر که بتوان برای آن تئوری نوشت مهم است.

همین سوالات برای تئوری‌هایی که کل ریاضیات بر آنها بنا شده است مانند تئوری مجموعه‌های نیز پرسیده می‌شود: آیا تئوری نظریه‌ی مجموعه‌ها، مثلاً زدافسی سازگار است؟ آیا تئوری زدافسی در صورت سازگار بودن کامل است؟ در مورد سوال

دوم، مثلا از درس مبانی ریاضی می‌دانید که فرضیه‌ی پیوستار، از نظریه‌ی مجموعه‌ها مستقل است؛ بدین معنی که اگر نظریه‌ی مجموعه‌ها سازگار باشد هم با فرضیه‌ی پیوستار و هم با نقیض آن سازگار است.

تعریف ۳۸. دو L تئوری T و T' را معادل می نامیم و می نویسیم $T \equiv T'$ هرگاه مدلهای یکسانی داشته باشند.

تمرین ۱۵. اگر تئوری T کامل باشد آنگاه برای هر $T \subseteq T'$ به طوری که T' سازگار باشد، داریم $T \equiv T'$.

تمرین ۱۶.

$$T \equiv Th(\mathfrak{M}) \Leftrightarrow \text{تئوری } T \text{ کامل است.}$$

که در آن $\mathfrak{M}$ یک L ساختار است و $Th(\mathfrak{M}) = \{\phi \mid \mathfrak{M} \models \phi\}$.

تمرین ۱۷. در زبان $L = \{<\}$ یک تئوری کامل بنویسید که هیچ مدل متناهی نداشته باشد.

تمرین ۱۸. در زبان $L = \{E\}$ که در آن E یک رابطه‌ی دوموضعی است، یک تئوری کامل T بنویسید به طوری که

$$T \supseteq \text{تئوری روابط هم ارزی}$$

و مدلهای T نامتناهی باشند و نامتناهی کلاس هم‌ارزی داشته باشند. آیا تئوری روابط هم‌ارزی با نامتناهی کلاس، کامل است؟

تمرین ۱۹. آیا دو عبارت زیر با هم معادلند؟

$$T \models \phi \Rightarrow T \models \psi \qquad\qquad T \models \phi \to \psi$$

۵.۱ وجود تئوری‌های هنکینی

در ادامه‌ی درس هدفمان اثبات قضیه‌ی فشردگی است که محکی برای سازگاری یک تئوری مرتبه‌ی اول فراهم می‌کند. بنا به این قضیه، اگر بی‌نهایت اتفاق داشته باشیم که هر تعداد متناهی آنها بتوانند با هم رخ دهند، همه‌ی این اتفاقها می‌توانند با هم رخ دهند. به بیان دقیق:

قضیه ۳۹ (فشردگی). L تئوری T دارای مدل است اگر و تنها اگر هر زیرمجموعه متناهی $\Delta \subseteq T$ از آن دارای مدل باشد.

دقت کنید که در این درس، برای اثبات قضیه‌ی فشردگی، از قضیه‌ی تمامیت گودل استفاده نکرده‌ام؛ با این حال اثباتی که برای اثبات این قضیه آمده است کاملاً مشابه همان اثبات است. در واقع اثبات زیر، تنها با استفاده از نظریه‌ی مدل بیان شده است.

منظور از یک تئوری هنکینی، تئوری‌ای است که برای همه‌ی فرمولهای وجودی، شاهدی از نوع ثابت دارد؛ به بیان دقیق:

تعریف ۴۰. فرض کنید L یک زبان مرتبه اول و C یک مجموعه از ثوابت جدید باشد، در این صورت $L(C)$ تئوری T را یک تئوری هنکینی [۸] می نامیم هرگاه برای هر $L(C)$ [۹] فرمول ϕ یک ثابت $c_\phi \in C$ موجود باشد، به طوری که

$$\text{“}\exists x \phi(x) \to \phi(c_\phi)\text{”} \in T$$

[۸] Henkin

[۹] $L \cup \{c \mid c \in C\}$

لم ۴۱. فرض کنید T یک L تئوری باشد که هر زیرمجموعه متناهی از آن دارای مدل باشد، در این صورت یک $L(C)$ تئوری T' با ویژگی های زیر پیدا می شود.

- $T \subseteq T'$
- T' متناهیا سازگار است(یعنی هر زیرمجموعه‌ی متناهی آن دارای مدل است)،
- T' هنکینی است،
- برای هر $L(C)$ جمله‌ی ϕ یا $\phi \in T'$ یا $\neg\phi \in T'$.

اثبات لم. قراردهید

$$
\begin{aligned}
&C_0 = \emptyset \\
&C_1 = \{c_\phi \mid \phi \text{ یک } L \text{ فرمول است}\} \\
&\vdots \\
&C_{n+1} = \{c_\phi \mid \phi \text{ یک } L(C_n) \text{ فرمول است}\} \\
&\vdots
\end{aligned}
$$

در هر مرحله در بالا، به تعداد فرمولهای موجود، به زبان ثابت جدید افزوده‌ایم. حال قرار دهید $C = \bigcup_{n\in\mathbb{N}} C_n$. تئوری T^H را (در زبان $L(C)$) به صورت زیر درنظر بگیرید.

$$T^H = \{\exists x\phi \to \phi(c_\phi)\}.$$

دقت کنید که $T \cup T^H$ متناهیا سازگار است: فرض کنید $\Delta \cup \Delta' \subseteq T \cup T^H$ متناهی باشد به طوری که $\Delta \subseteq T$ و $\Delta' \subseteq T^H$. فرض کنید $\text{“}\exists x\phi(x) \to \phi(c_\phi)\text{”} \in \Delta'$ و (برای راحت شدن بحث) فرض کنید که فرمول ذکر شده در $L(C_1)$ باشد. در این صورت اگر $\mathfrak{M}$ یک مدل از Δ باشد به طوری که $\mathfrak{M} \models \exists x\phi(x)$ آنگاه $a \in M$ موجود است به طوری که $\mathfrak{M} \models \phi(a)$. تعبیر کنید $c_\phi^{\mathfrak{M}} = a$. دراین صورت داریم.

$$(\mathfrak{M}, c_\phi) \models \Delta \cup \{\exists x\phi(x) \to \phi(c_\phi)\}$$

مجموعه $\mathcal{A}$ را به صورت زیر درنظر بگیرید (دقت کنید که این مجموعه، از تئوریها تشکیل شده است):

$$\mathcal{A} = \{T' \mid T \cup T^H \subseteq T' \text{ و } T' \text{ متناهیا سازگار باشد}\}$$

اولاً $\mathcal{A} \neq \phi$ و ثانیاً اگر $T_1 \subseteq T_2 \subseteq \cdots$ زنجیری از تئوری‌های موجود در $\mathcal{A}$ باشد آنگاه $\bigcup T_i \in \mathfrak{A}$ (بررسی کنید که چرا این گونه است.) پس بنابر لم زرن یک تئوری $T^* \in \mathcal{A}$ موجود است که نسبت به $\subseteq$ ماکزیمال است. ادعا می‌کنیم که T^* تمام ویژگی های مورد نظر ما را دارد.

اولاً T^* متناهیا سازگار است. ثانیاً T^* هنکینی است زیرا در زبانِ $L(C)$ نوشته شده است و شاملِ T^H است.

همچنین برای هر جمله‌ی ϕ یا T^* با ϕ متناهیاً است و یا با $\neg\phi$. زیرا اگر ϕ یک $L(C)$ جمله باشد، و همزمان $T^* \cup \{\phi\}$ و $T^* \cup \{\neg\phi\}$ متناهیاً ناسازگار باشند، مجموعه‌های $\Delta, \Delta' \subseteq T^*$ یافت می‌شوند به طوری که

$\Delta \cup \{\phi\}$ناسازگار است.

$\Delta' \cup \{\neg\phi\}$ناسازگار است.

$\Delta \cup \Delta' \cup \{\phi\}$ناسازگار است.

$\Delta \cup \Delta' \cup \{\neg\phi\}$ناسازگار است.

بنابراین $\Delta \cup \Delta'$ ناسازگار است و این خلاف متناهیاً سازگار بودن T^* است.

از طرفی $T^* \cup \{\phi\}$ و $T^* \cup \{\neg\phi\}$ نیز نمی‌توانند هر دو سازگار باشند، زیرا (همان طور که در زیر توضیح داده شده است) هر جمله‌ای که با T^* سازگار است در این تئوری قرار دارد (و این تئوری متناهیاً سازگار است).

فرض کنید $T^* \cup \{\phi\}$ سازگار باشد، در این صورت اگر $\phi \notin T^*$ ماکزیمال بودن T^* نقض می‌شود، پس $\phi \in T^*$. به طور مشابه برای $T^* \cup \{\neg\phi\}$ می‌توان بحث کرد. $\square$

یک نکته‌ی مهم در اثبات بالا این است که تئوری هنکینی‌ای که در نهایت ساخته می‌شود از لحاظ تعداد جملات هم‌اندازه‌ی تئوریِ اولیه است. هم‌چنین زبانی که تئوری هنکینی ساخته شده در آن نوشته شده است، دارای اندازه‌ی $\aleph_0 + |L|$ است.

۶.۱ تکمیل اثبات قضیه‌ی فشردگی

قضیه ۴۲. فرض کنید T یک تئوری هنکینیِ متناهیاً سازگار در زبانِ $L(C)$ باشد به طوری که برای هر Lجمله‌ی φ یا $\varphi \in T$ یا $\neg\varphi \in T$؛ در این صورت T دارای مُدِل است. (به بیان دقیقتر، تئوری یاد شده، یک مدل دارد که اعضای آن مجموعه C است و با این شرط، این مدل تحت ایزومرفیسم یکتاست.)

اثبات. قرار دهید $M = \{a_c | c \in C\}$ روی M رابطه‌ی تساوی را به صورت زیر تعریف کنید.

$$a_c = a_d \Leftrightarrow c = d \in T$$

نخست جهانِ M را تبدیل به یک $L(C)$ساختار می‌کنیم. برای این کار باید اجزای زبانِ $L(C)$ در M تعبیر شوند. اساس این تعبیر، واگذاری همه چیز به تئوریِ T است.

تعبیر ثوابت مشخص است:

$$c^M = a_c.$$

فرض کنید f یک نماد تابع تابعی دو موضعی در L باشد (اگر n موضعی باشد هم همین روش کار می‌کند). قرار دهید:

$$f^M(a_c, a_d) = a_e \Leftrightarrow \underbrace{f(c,d) = e}_{\text{جمله}L(C)} \in T$$

توجه کنید که از آنجا که T متناهیاًسازگار است،

$$\text{“}\exists x \quad f(c,d) = x\text{”} \in T$$

زیرا در غیر این صورت نقیض جمله‌ی بالا در T است؛ اما نقیض جمله‌ی بالا نمی‌تواند مدل داشته باشد زیرا در هر $L(C)$ساختاری که ثوابتِ c,d تعبیر شوند، $f(c,d)$ نیز تعبیر می‌شود. حال از آنجا که تئوریِ T هنکینی است ثابت e وجود دارد به طوری که $f(c,d)=e\in T$. بنابراین تابعِ f^M قابل تعریف است. خوش‌تعریفی این تابع را به عنوان تمرین چک کنید.

تمرین ۲۰. حال که توابع و ثوابت در M تعریف شده‌اند، پس تعبیر ترمها نیز به صورت استقرائی ممکن می‌شود. نشان دهید که

$$t^M(a_{c_1},\dots,a_{c_n})=c^a_\circ \Leftrightarrow T\models t(c_1,\dots,c_n)=c_\circ$$

تعبیر روابط زبان نیز به صورت زیر صورت می‌گیرد:

$$R^M(a_{c_1},\dots,a_{c_n})\Leftrightarrow R(c_1,\dots,c_n)\in T$$

بنابراین M با تعبیرهای صورت گرفته در بالا، یک Lساختار است که آن را با $\mathfrak{M}$ نشان می‌دهیم.

در ادامه‌ی کار هدفمان اثباتِ این است که $T\models\mathfrak{M}$. در واقع می‌خواهیم نشان دهیم که برای هر $L(C)$جمله‌ی φ داریم

$$\varphi\in T\Leftrightarrow\mathfrak{M}\models\varphi$$

(به بیان دیگر، ثابت خواهیم کرد که $(T=Th(\mathfrak{M})$. این حکم را با استقراء روی پیچیدگی جملاتِ φ اثبات می‌کنیم.

الف) فرض کنید φ یک جمله‌ی اتمی به صورت زیر است.

$$t_1(c_1,\dots,c_n)=t_2(c_1,\dots,c_n)$$

اگر $``t_1(c_1,\dots,c_n)=t_2(c_1,\dots,c_n)"\in T$ آنگاه باید نشان دهیم که

$$\mathfrak{M}\models t_1^{\mathfrak{M}}(a_{c_1},\dots,a_{c_n})=t_2^{\mathfrak{M}}(a_{c_1},\dots,a_{c_n})$$

دقت کنید که بنا به سازگاری T داریم

$$\exists x\quad t_1(c_1,\dots,c_n)=x\in T$$

و بنا به هنکینی بودن آن داریم

$$"t_1(c_1,\dots,c_n)=c_\circ"\in T$$

دوباره بنا به سازگاری و هنکینی بودن T داریم

$$``t_2(c_1,\dots,c_n)=c_\circ"\in T$$

و از اینها نتیجه می‌شود که

$$\mathfrak{M}\models t_1^{\mathfrak{M}}(a_{c_1},\dots,a_{c_n})=t_2^{\mathfrak{M}}(a_{c_1},\dots,a_{c_n})$$

همچنین روند بالا قابل بازگشت است.

تمرین ۲۱. به طور مشابه ثابت کنید که

$$\mathfrak{M}\models R(t_1^M(a_{c_1},\dots,a_{c_n}),\dots,t_n^M(a_{c_1},\dots,a_{c_n}))\Leftrightarrow R(t_1(c_1,\dots,c_n),\dots,t_n(c_1,\dots,c_n))\in T.$$

ب. فرض کنید ادعا برای جمله‌ی φ درست باشد. آنگاه

$$\mathfrak{M} \models \neg\varphi \Leftrightarrow$$

$$\mathfrak{M} \not\models \varphi \Leftrightarrow$$

$$T \not\models \varphi (\varphi \notin T) \Leftrightarrow$$

$$\neg\varphi \in T$$

ج. اگر ادعا برای φ و ψ درست باشد آنگاه

$$\mathfrak{M} \models \varphi \wedge \psi \Leftrightarrow$$

$$\mathfrak{M} \models \varphi \text{و} \mathfrak{M} \models \psi \Leftrightarrow$$

$$\varphi \in T \text{و} \psi \in T \Leftrightarrow$$

$$\varphi \wedge \psi \in T$$

فرض کنید φ به صورت $\exists x \quad \psi$ باشد و ادعا برای ψ برقرار باشد.

$$T \models \exists x \quad \psi \Leftrightarrow$$

$$\exists x \quad \psi \in T \Leftrightarrow$$

$$\psi(c_\psi) \in T \Leftrightarrow$$

$$\mathfrak{M} \models \psi(c_\psi) \Leftrightarrow$$

$$\mathfrak{M} \models \exists x \quad \psi(x) \Leftrightarrow$$

$$\mathfrak{M} \models \varphi$$

چند کاربرد ساده از قضیه‌ی فشردگی

از قضیه‌ی فشردگی گاهی برای تشخیص این استفاده می‌شود که برای چه کلاسهائی از Lساختارها می‌توان تئوری نوشت. در مثال گذشته، یک تئوری T برای مجموعه‌های نامتناهی نوشتیم. در زیر نشان داده‌ایم که نمی‌توان برای مجموعه‌های متناهی تئوری نوشت. به بیان دیگر نمی‌توان یک تئوری T نوشت به طوری که همه‌ی مجموعه‌های متناهی مدل آن باشند و هر چیزی که مدل آن باشد یک مجموعه‌ی متناهی باشد.

به برهان خلف، فرض کنید T یک تئوری برای مجموعه‌های متناهی باشد. تئوری T' را به صورت زیر در نظر بگیرید:

$$T' = T \cup \{\exists x_1, x_2 \quad x_1 \neq x_2, \exists x_1, x_2, x_3 \quad x_1 \neq x_2 \quad x_2 \neq x_3 \quad x_1 \neq x_3, \ldots, \exists x_1, \ldots, x_n \quad \bigwedge x_i \neq x_j, \ldots\}$$

تئوری T' متناهیاً سازگار است؛ زیرا اگر

$$\underbrace{\Delta}_{\text{متناهی}} \subseteq T'$$

آنگاه اگر فرض کنیم n بزرگترین عددی باشد که جمله‌ی $\exists x_1, \ldots, x_n \bigwedge x_i \neq x_j \in \Delta$ آنگاه T دارای یک مدل $\mathfrak{M}$ با حداقل n عضو هست، پس

$$\mathfrak{M} \models \Delta$$

از این که هر بخش متناهیِ T' دارای مدل است، بنا به قضیه‌ی فشردگی نتیجه می‌شود که T' دارای مُدِل است. حال اگر

$$\mathfrak{N} \models T'$$

آنگاه از یک طرف $\mathfrak{N}$ متناهی است، زیرا مدلی برای T است؛ و از طرف دیگر نامتناهی است زیرا تمام جملاتی که وجود n عنصر را بیان می‌کنند در آن برقرار هستند؛ و این تناقض است. ↯ □

می‌گوییم یک میدان دارای مشخصه‌ی n است هرگاه n کوچکترین عددی باشد به طوری که برای عنصرِ x در آن میدان داشته باشیم $nx = ۰$. مشخصه‌ی یک میدان در صورت وجود یک عدد اول است (بررسی کنید که چرا). اگر چنین عدد n برای میدانی وجود نداشته باشد، آن میدان را میدانی با مشخصه‌ی صفر می‌نامیم.

در زیر نشان داده‌ایم که برای میدانهای با مشخصه‌ی ناصفر نمی‌توان یک تئوری نوشت. اگر فرض کنیم که T تئوری میدانهای با مشخصه‌ی ناصفر در یک زبانِ L است؛ آنگاه تئوریِ T' را به صورت زیر در نظر بگیرید:

$$T' = T \cup \{c + c \neq ۰, c + c + c \neq ۰, \ldots, \underbrace{c + c + \ldots + c}_{n\text{بار}} \neq ۰, \ldots\}$$

تئوریِ بالا در یک زبانِ $L \cup \{c\}$ نوشته شده است که c یک ثابت جدید است. دقت کنید که T' یک تئوری متناهیاًسازگار است. مثلا برای اثبات این که

$$T \cup \{c + c \neq ۰, c + c + c \neq ۰\}$$

مدل دارد کافی است یک مدل از T انتخاب کنیم که مشخصه‌ی آن بیش از ۳ است و در آن c را عنصری تعبیر کنیم که اگر سه بار با خودش جمع شود صفر نشود؛ این کار به آسانی در $\mathbb{Z}_۵$ میسر است. از آنجا که هر قسمت متناهی از T' دارای مدل است، پس T' دارای مدل است. این مدل، از یک طرف یک میدان با مشخصه‌ی ناصفر است، و از طرفی حاوی یک عنصر (تعبیر c) است که هر چه با خودش جمع شود صفر نمی‌شود؛ و این تناقض است.

به عنوان مثالی دیگر در زیر نشان داده‌ایم که برای گرافهای هم‌بند نمی‌توان یک تئوری نوشت. منظور از یک گراف همبند، گرافی است که بین هر دو راس آن یک مسیر متناهی وجود داشته باشد.

فرض کنید T یک تئوری برای گرافهای همبند باشد (در زبانی که یک رابطه‌ی دوتائی R برای وجود یال بین دو راس دارد). دو ثابتِ c, d به زبان اضافه کنید و تئوریِ T' را اجتماعِ T با نامتناهی جمله‌ی ϕ_n در نظر بگیرید که هر ϕ_n بیانگر این است که بین c, d مسیری به طول n وجود ندارد (یعنی فاصله‌ی بین آنها بیش از n است). نشان دهید که هر زیرمجموعه‌ی متناهی از این تئوری دارای مدل است؛ بنا به فشردگی، خودِ این تئوری دارای مدل است و در این مدل، میان تعبیرهای c, d فاصله‌ی نامتناهی وجود دارد.

مثال زیر و راه‌حل جالب آن توسط خانم سمنانی ارائه شد.

مثال ۴۳. نشان دهید که برای گروه‌های دوری نمی‌توان یک تئوری نوشت. منظور از یک گروه دوری، گروهی است که توسط یک مجموعه‌ی تک‌عضوی تولید شده است.

اثبات. فرض کنید که T یک تئوری برای گروه‌های دوری باشد. تئوریِ T' را به صورت زیر در نظر بگیرید:

$$T' = T \cup T_{inf-set} \cup \{\forall x \exists y \quad x = y + y\}$$

اگر تئوری T' دارای مدل باشد، آنگاه، بنا به قضیه‌ای که در درس آینده بدان خواهم پرداخت، دارای مدلی شماراست. اگر $\mathfrak{N}$ مدلی شمارا برای T' باشد، از یک طرف این مدل با $\mathbb{Z}$ ایزومرف است (زیرا دوری است) و از یک طرف تمام عناصر آن زوج هستند (بنا به اصل آخر) و این غیر ممکن است.

اما تئوری T' به دلیل زیر، متناهیاً سازگار است. هر بخش متناهی از این تئوری بیانگر وجود تعداد متناهی عنصر در در یک گروه که تمام عناصر آن گروه زوج هستند. $\mathbb{Z}_p$ ها برای p های به اندازه‌ی کافی، مدلهائی برای این تئوری هستند. زیرا در $\mathbb{Z}_p$ همه‌ی عناصر زوج هستند.

اگر $x \in \mathbb{Z}_p$ از دو حالت خارج نیست؛ یا x خود به عنوان عنصری از $\mathbb{Z}$ زوج است که مطلوب ماست. یا این که x به عنوان عنصری از $\mathbb{Z}$ فرد است که در این صورت $x + p = x$ زوج است. □

۷.۱ ادامه‌ی کاربردهای قضیه‌ی فشردگی

یک حکم داده شده در صورتی از یک تئوری T نتیجه می‌شود (یعنی در همه‌ی مدلهای آن درست است) که از بخشی متناهی از آن تئوری نتیجه شود:

نتیجه ۴۴. $T \models \phi$ اگروتنهااگر $\Delta \models \phi$ برای یک زیرمجموعه‌ی متناهیِ $\Delta \subseteq T$.

اثبات. اثباتِ از راست به چپ. اگر برای هر زیرمجموعه‌ی متناهی $\Delta \subseteq T$ داشته باشیم $\Delta \not\models \phi$ آنگاه برای هر زیرمجموعه‌ی متناهیِ $\Delta \subseteq T$ مجموعه‌ی $\Delta \cup \{\neg\phi\}$ سازگار است. بنابراین $T \cup \{\neg\phi\}$ متناهیاًسازگار است. پس بنا به فشردگی $T \cup \{\neg\phi\}$ دارای مدل است؛ یعنی $T \not\models \phi$. □

یکی از مهمترین نتیجه‌های قضیه‌ی فشردگی، لم لُوِنهایم‌اسکولم است. بنا به این لم، هر تئوری‌ای که دارای مدل باشد، دارای مدلهائی با هر سایز دلخواهِ ماست.

نتیجه ۴۵. فرض کنید L یک زبان مرتبه اول شمارا و T یک L تئوری مرتبه اول باشد که دارای حداقل یک مدل نامتناهی است. آنگاه برای هر کاردینال نامتناهی κ، تئوریِ T دارای مدلی با اندازه‌ی دقیقاً برابر با κ است.

اثبات. اگر $\kappa = \aleph_0$ آنگاه با استفاده از روش هنکینی، برای T یک مدل به اندازه κ وجود دارد. علت این است که در روش هنکینی، جهانِ‌مدلی که حاصل می‌شود، متشکل از ثابتهائی است که ما اضافه کرده‌ایم و این ثابتها به تعداد فرمولهای موجود در زبان هستند؛ پس وقتی زبان شماراست، سایز مدل به دست آمده نیز شمارا خواهد بود.

حال فرض کنید $\kappa > \aleph_0$. یک مجموعه از ثوابت $\{c_\lambda\}_{\lambda \leq \kappa}$ به زبان اضافه کنید (یعنی به تعدادِ κ ثابت جدید به زبان اضافه کنید) و تئوری T' را به صورت زیر درنظر بگیرید.

$$T' = T \cup \{c_\lambda \neq c_{\lambda'} \mid \lambda, \lambda' < \kappa\}$$

تئوری T' متناهیاًسازگار است (زیرا هر بخش متناهی آن دارای مدل است؛ مدل هر بخش متناهیِ این تئوری، همان مدل نامتناهی‌ای است که در فرض قضیه آمده است) و در زبانی به اندازه κ نوشته شده است. بنا به روش هنکینی در اثبات قضیه‌ی فشردگی، این تئوری دارای مدلی است که از ثوابت تشکیل شده است و مساوی بودن یا نبودن این ثوابت را تئوری تعیین می‌کند. پس این تئوری دارای مدلی با اندازه‌ی κ است. □

قضیه‌ی فشردگی منجر به بروز پارادوکسهای جذابی در نظریه‌ی مجموعه‌ها می‌شود که به یکی ازآنها، به نام پارادوکس اسکولم اشاره می‌کنم. می‌دانیم که در نظریه‌ی مجموعه‌ها ثابت می‌شود که یک مجموعه‌ی ناشمارا وجود دارد. از طرفی زبان نظریه‌ی مجموعه‌ها حداکثر شماراست؛ پس خود نظریه‌ی مجموعه‌ها دارای مدلی شماراست که همه‌ی مجموعه‌ها در این مدل شمارا قرار دارند. حال در این مدل شمارا، این جمله درست است که مجموعه‌ای ناشمارا وجود دارد (که اعضای آن در این مدل شمارا هستند)!

یکی دیگر از کاربردهای قضیه‌ی فشردگی، استفاده از آن برای بررسی نحوه‌ی اصل‌پذیری کلاسهای مختلف است.

تعریف ۴۶. فرض کنید $\mathbb{K}$ کلاسی از Lساختارها باشد. می‌گوییم کلاس $\mathbb{K}$ دارای اصل‌بندی است هرگاه یک تئوری مرتبه اول T وجود داشته باشد به طوری که

$$\mathbb{K} = \{\mathfrak{M} \mid \mathfrak{M} \models T\}$$

تعریف ۴۷. می گوییم تئوری T **دارای اصل‌بندی متناهی** است هرگاه یک تئوری مرتبه اول T با متناهی جمله وجود داشته باشد به طوری که

$$\mathbb{K} = \{\mathfrak{M} \mid \mathfrak{M} \models T\}$$

لم ۴۸. کلاس $\mathbb{K}$ از Lساختارها دارای اصل‌بندی متناهی است اگر و تنها اگر هر دو کلاسِ $\mathbb{K}$ و $\mathbb{K}^c$ دارای اصل‌بندی باشند.

اثبات. در اینجا از راست به چپ را فقط ثابت کرده‌ام. فرض کنید $\mathbb{K}$ و $\mathbb{K}^c$ هر دو دارای اصل‌بندی‌های زیر باشند:

$$\mathbb{K} = \{\mathfrak{M} \mid \mathfrak{M} \models T\}$$

$$\mathbb{K}^c = \{\mathfrak{M} \mid \mathfrak{M} \models T'\}$$

در این صورت $T \cup T'$ ناسازگار است. بنابراین یک زیرمجموعه متناهی $\Delta \cup \Delta' \subseteq T \cup T'$ وجود دارد که ناسازگار است. با فرضِ این که $\Delta' = \{\psi_1, \cdots, \psi_n\}$ قرار دهید

$$T'' = \Delta \cup \{\neg\psi_1 \vee \cdots \vee \neg\psi_n\}.$$

دقت کنید که T'' یک تئوریِ متناهی است.

اگر $\mathfrak{N}$ مدلی برای T'' باشد، آنگاه در کلاسِ $\mathbb{K}$ است؛ زیرا در غیر این صورت باید همه‌ی ψ_i ها در آن برقرار باشد. از طرفی اگر $\mathfrak{N}$ در کلاسِ $\mathbb{K}$ باشد، مدلی برای T'' است؛ زیرا تمام جملات موجود در Δ در آن درست است و تمام جملات موجود در Δ' نمی‌تواند در آن درست باشد (زیرا $\Delta \cup \Delta'$ هیچ مدلی ندارد). $\square$

تمرین ۲۲. نشان دهید که

- کلاس مجموعه‌های نامتناهی دارای اصل‌بندی متناهی نیست.
- کلاس میدانهای با مشخصه‌ی صفر دارای اصل‌بندی متناهی نیست.

تمرین ۲۳. فرض کنید ثابتهای $c_1, \ldots, c_n$ در زبان L نباشند و داشته باشیم

$$T \models \phi(c_1, \ldots, c_n).$$

نشان دهید که

$$T \models \forall x_1, \ldots, x_n \quad \phi(x_1, \ldots, x_n).$$

تمرین ۲۴. کلاس $\mathbb{K}$ از Lساختارها دارای اصل‌بندی عمومی است هرگاه یک تئوری T وجود داشته باشد که تنها از جملات به صورت $\forall x_1, \cdots, x_n \phi(x_1, \cdots, x_n)$ (ϕ بدون سور) تشکیل شده است، به طوری که

$$\mathbb{K} = \{\mathfrak{M} \mid \mathfrak{M} \models T\}$$

نشان دهید که $\mathbb{K}$ دارای اصل‌بندی عمومی است اگر و تنها اگر تحت زیرساختارها بسته باشد. (راهنمائی: از تمرین بالا استفاده کنید). [10]

گفتیم که در مورد تئوری‌ها، علاوه بر سازگار بودن آنها، کامل بودنشان نیز مهم است. قضیه‌ی فشردگی در این زمینه هم کمک می‌کند:

نتیجه ۴۹. فرض کنید تئوری T در زبان L هیچ مدل متناهی نداشته باشد و دارای این ویژگی باشد که کاردینالِ $\kappa \geq |L| + \aleph_0$ وجود داشته باشد به طوری هر دو مدل T که دارای سایزِ κ هستند باهم ایزومرفند (به بیان دیگر، T تنها دارای یک مدل از سایزِ κ باشد). در این صورت T یک تئوریِ کامل است.

اثبات. فرض کنید $\mathfrak{M}, \mathfrak{N}$ دو مدل برای T باشند و ϕ یک Lجمله باشد. می‌خواهیم نشان دهیم که

$$\mathfrak{M} \models \phi \Leftrightarrow \mathfrak{N} \models \phi.$$

فرض کنید که $\mathfrak{M} \models \phi$. در این صورت $T \cup \{\phi\}$ یک تئوری متناهیاً سازگار است. بنا به لونهایم اسکولم، این تئوری دارای مدلی مانند $\mathfrak{M}'$ از سایز κ است. از طرفی $\mathfrak{M}' \models T$. پس در تنها مدل T از سایزِ κ جمله‌ی ϕ درست است.

حال اگر $\mathfrak{N} \models \neg\phi$ آنگاه $T \cup \{\neg\phi\}$ سازگار است و از این رو دارای مدلی مانند $\mathfrak{N}'$ از سایزِ κ است (که مدل T نیز هست). پس در $\mathfrak{N}'$ هم ϕ و هم $\neg\phi$ باید برقرار باشند و این تناقض است. □

در ادامه چند نمونه از کاربردهای قضیه‌ی بالا را نشان داده‌ام.

مثال ۵۰. تئوری فضاهای برداری نامتناهی روی $\mathbb{Q}$ را در زبانِ

$$L = \{+, -, \{f_\lambda\}_{\lambda \in \mathbb{Q}}, 0\}$$

می‌نویسیم که در آن هر f_λ یک تابع است که ضرب در اسکالرِ λ را نشان می‌دهد. تئوری مورد نظر اجتماع تئوریها و جملات زیر است:

- T_{Abg}

[10] $\mathfrak{M} \in \mathbb{K}, \mathfrak{N} \subseteq \mathfrak{M} \Rightarrow \mathfrak{N} \in \mathbb{K}$

- $T_{inf-set}$

- $f_\lambda(a+b) = f_\lambda(a) + f_\lambda(b)$ که این جمله برای هر $\lambda \in \mathbb{Q}$ به طور جداگانه نوشته شده است.

- $\forall a \times ۰ \times a = ۰$

- $f_\lambda(f_{\lambda'}(a)) = f_{\lambda\cdot\lambda'}(a)$ که این جمله برای هر $\lambda, \lambda' \in \mathbb{Q}$ یک بار نوشته شده است.

- $f_{\lambda+\lambda'}(a) = f_\lambda(a) + f_{\lambda'}(a)$ که این جمله برای هر $\lambda, \lambda' \in \mathbb{Q}$ یک بار نوشته شده است.

تئوری بالا را با T_{VS} نشان دهید.

ادعا می‌کنم که T_{VS} یک تئوری کامل است.

اولاً دقت کنید که T_{VS} هیچ مدل متناهی ندارد. حال ادعا می‌کنم هر دو مدلِ T_{VS} از سایزِ $۲^{\aleph_۰}$ با هم ایزومرفند.

دقت کنید که دو فضای برداری روی یک میدان یکسان، در صورتی با هم ایزومرفند که پایه‌های هم‌اندازه داشته باشند. از طرفی اگر یک فضای برداری روی $\mathbb{Q}$ دارای سایزِ $۲^{\aleph_۰}$ داشته باشد باید سایز پایه‌اش نیز $۲^{\aleph_۰}$ باشد (زیرا ترکیب‌های خطی متناهی کمتر از این تعداد عنصر، منجر به ایجاد این تعداد عنصر نمی‌شود).

پس هر دو فضای برداری روی $\mathbb{Q}$ که دارای سایز $۲^{\aleph_۰}$ هستند دارای پایه‌های هم‌سایز و از این رو با هم ایزومرفند.

تمرین ۲۵.

- یک تئوری برای گروههای آبلیِ‌بدون تاب بنویسید.

- نشان دهید که هر گروه آبلی بدون تاب را می‌توان به صورت یک فضای برداری روی $\mathbb{Q}$ دید.

- نشان دهید که تئوری گروه‌های آبلی بدون تاب، یک تئوری کامل است.

مثال ۵۱. ساختار $(\mathbb{Q}, <)$ را در نظر بگیرید. مجموعه‌ی اصول زیر را در زبان $L = \{<\}$ تئوری T بنامید.

$$\forall x \;\; \neg(x < x) \tag{۱.۱}$$

$$\forall x, y \;\; (x \leq y) \vee (y \leq x) \tag{۲.۱}$$

$$\forall x, y, z \;\; ((x < y) \wedge (y < z) \longrightarrow (x < z)) \tag{۳.۱}$$

$$\forall x, y \;\exists z \;\; x < z < y \tag{۴.۱}$$

$$\forall x \;\exists y \;\; x < y \tag{۵.۱}$$

$$\forall x \;\exists y \;\; y < x \tag{۶.۱}$$

ادعا می‌کنم که اگر L ساختارهای $(M, <)$ و $(N, <)$ دو مدل شمارا برای T باشند آنگاه

$$(M, <) \cong (N, <).$$

برای اثبات این ادعا شمارش‌های $M = (a_i)_{i\in\mathbb{N}}$ و $N = (b_i)_{i\in\mathbb{N}}$ از اعضای M و N را در نظر بگیرید. دقت کنید که این شمارشها، صعودی نیستند.

تابعِ

$$f_۰ = (a_۰, b_۰)$$

را در نظر بگیرید.

در زیر یک دنباله از توابعِ

$$f_۰ \subseteq f_۱ \subseteq \dots$$

ساخته‌ایم به طوری که هر تابع f_n دارای ویژگی‌های زیر باشد:

- $a_n \in \mathrm{dom} f_n$ و $b_n \in \mathrm{range} f_n$،
- دامنه و بردِ هر f_n متناهی است و f_n حافظ ترتیب است یعنی :

$$x < y \to f(x) < f(y).$$

فرض کنید که تابع f_n به گونه‌ای ساخته شده باشد ویژگی‌های بالا را دارد. برای ساختن $f_{n+۱}$ به صورت زیر عمل می کنیم:

عنصر $a_{n+۱}$ را با همه‌ی اعضای دامنه‌ی f_n مقایسه می‌کنیم. آنگاه، اگر مثلاً $t_۱ < a_{n+۱} < t_۲ < t_۳ < t_۴$ قرار می‌دهیم $f_{n+۱} = b$ به طوری که

$$f_n(t_۱) < b < f_n(t_۲) < f_n(t_۳) < f_n(t_۴).$$

قرار می‌دهیم $f'_{n+۱} = f_n \cup \{(a_{n+۱}, b)\}$. به همین ترتیب $b_{n+۱}$ را به برد تابعِ $f'_{n+۱}$ با پیدا کردن عنصر a در دامنه، اضافه می‌کنیم و تابع حاصل را $f_{n+۱}$ می‌نامیم؛ یعنی

$$f_{n+۱} = f_n \cup \{(a_{n+۱}, b)\}, \{(a, b_{n+۱})\}.$$

حال تابع

$$f^* : M \to N$$

که به صورت

$$f^* = \bigcup_{n \in \mathbb{N}} f_n$$

تعریف می‌شود

- حافظ ترتیب است.
- دامنه‌ی f^* کل M است و برد آن کل N است.
- یک به یک و پوشاست.

پس هر دو مدل تئوری T از سایز $\aleph_۰$ با هم ایزومرف هستند. پس T کامل است.

بنابراین هر جمله‌ی φ که در $(\mathbb{Q}, <)$ درست باشد در $(\mathbb{R}, <)$ نیز درست است و برعکس:

$$(\mathbb{Q}, <) \models T$$

$$(\mathbb{R},<) \models T$$

به بیان دیگر، از آنجا که T کامل است و $(\mathbb{Q},<) \models T$ هر چه که در ساختارِ $\mathbb{Q},<$ درست باشد، دقیقا همان است که از تئوریِ T نتیجه می‌شود.

مثال ۵۲. فرض کنید φ یک جمله در زبان حلقه‌ها باشد. اگر φ در میدانهای با مشخصه‌ی متناهی به اندازه کافی بزرگ درست باشد آنکاه φ در یک میدان با مشخصه‌ی صفر برقرار است.

تئوریِ

$$T_{field} \cup \{۱+۱ \neq ۰, ۱+۱+۱ \neq ۰, \cdots\} \cup \{\varphi\}$$

را در نظر بگیرید. تئوری بالا متناهیاً سازگار است پس مدل دارد و این مدل یک میدان با مشخصه‌ی صفر است که φ در آن برقرار است.

به عنوان کاربرد دیگری از قضیه‌ی فشردگی، در ادامه به آنالیز نااستاندارد پرداخته‌ام.

۸.۱ آنالیز نااستاندارد

میدان مرتب اعداد حقیقی $\mathbb{R}$ را در نظر بگیرید. روشهای مختلفی برای ساخت این میدان وجود دارد ولی یکی از مهمترین ویژگی‌های این میدان آن است که اصل کمال در آن برقرار است (یعنی هر زیر مجموعه ی از بالا کراندار از $\mathbb{R}$ دارای کوچکترین کران بالاست).

نتیجه ۵۳. میدان اعداد حقیقی دارای ویژگی ارشمیدسی است؛ یعنی

$$\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N} \quad n > x$$

اثبات. فرض کنید یک عدد حقیقی وجود داشته باشد که از تمام اعداد طبیعی بیشتر است. آنگاه $\mathbb{N}$ در $\mathbb{R}$ دارای کران بالاست. پس، بنا به اصل کمال، دارای کوچکترین کران بالایی چون $x_۰$ است:

$$x_۰ = \sup \mathbb{N}$$

پس $x_۰ - ۱$ کران بالای $\mathbb{N}$ نیست. پس داریم

$$\exists n \in \mathbb{N} \quad n > x_۰ - ۱$$

بنابراین

$$\underbrace{n+۱}_{\in \mathbb{N}} > x_۰$$

و عبارت بالا با کران بالا بودنِ $x_۰$ تناقض دارد.

نتیجه ۵۴.

$$\bigcap_{n \in \mathbb{N}} (۰, \frac{۱}{n}) = \emptyset$$

اثبات. به برهان خلف فرض کنیم عنصری چون $t \in \bigcap_{n\in\mathbb{N}}(۰, \frac{۱}{n})$ وجود دارد. آنگاه

$$\forall n \in \mathbb{N} \quad t < \frac{۱}{n}$$

پس

$$\forall n \in \mathbb{N} \quad \frac{۱}{t} > n$$

و این ویژگی ارشمیدسی را نقض می‌کند.

بنابراین در اعداد حقیقی عناصر بینهایت بزرگ و بی‌نهایت کوچک وجود ندارند و این همان ویژگی ارشمیدسی است.

تعریف لایبنیتز برای حد تابع به صورت زیر است که

$$\lim_{x\to a} f(x) = l$$

هرگاه «وقتی x بی‌نهایت به a نزدیک شود، $f(x)$ بی‌نهایت به l نزدیک شود.» و این در حالیست که می‌دانیم عناصر بینهایت بزرگ و بی‌نهایت کوچک در اعداد حقیقی وجود ندارند. پس در واقع x و $f(x)$ نمی‌توانند بینهایت به a و l نزدیک شوند!

در حساب، روش بیان تعریف حد بدین گونه است که $f(x)$ به هر **اندازه‌ی دلخواه** به l نزدیک شود به شرطی که x به **اندازه‌ی کافی** به a نزدیک شده باشد:

$$\lim_{x\to a} f(x) = l \Leftrightarrow \forall \epsilon > ۰ \quad \exists \delta > ۰ \quad \forall x \quad (|x-a| < \delta \to |f(x) - l| < \epsilon).$$

اما در زیر، به بررسی مفاهیم آنالیزی در ساختاری نااستاندارد پرداخته‌ام. ساختاری که از لحاظ منطق مرتبه‌ی اول کاملاً شبیه اعداد حقیقی است ولی غیرارشمیدسی است.

فرض کنید

$$T = Th(\mathbb{R}, +, \cdot, ۰, ۱, <) = \{\phi | (\mathbb{R}, +, ., ۰, ۱, <) \models \phi\}.$$

تئوری T' را در زبان $L \cup \{c\}$ به صورت زیر در نظر بگیرید:

$$T' = T \cup \{c > ۱, c > ۱ + ۱, c > ۱ + ۱ + ۱, ...\}$$

از قضیه ی فشردگی نتیجه می شود که T' دارای مدل است (زیرا متناهیاً سازگار است و مدل هر بخش متناهی آن خودِ اعداد حقیقی است). نام این مدل را $\mathbb{R}^*$ می گذاریم. پس $\mathbb{R}^*$ دارای ویژگی‌های زیر است:

- یک میدان مرتب است.
- همه‌ی ویژگی‌های مرتبه‌ی اول اعداد حقیقی را داراست.
- دارای یک عنصر c است که بی‌نهایت بزرگ است و از این رو دارای عنصر $\frac{۱}{c}$ است که بی‌نهایت کوچک است.
- هر ویژگی مرتبه‌ی اولی که $\mathbb{R}^*$ داشته باشد اعداد حقیقی هم دارند.

می‌توان $\mathbb{R}^*$ را به گونه‌ای یافت که $\mathbb{R} \subseteq \mathbb{R}^*$. برای این منظور کافی است برای هر عدد حقیقی یک ثابت به زبان اضافه می‌کردیم. بدین طریق می‌شود هر موجودی را که در اعداد حقیقی در نظر داریم به مدل نااستاندارد ببریم و در آنجا آن را با علامت ستاره نشان دهیم. برای مثال اگر $f : \mathbb{R} \to \mathbb{R}$ یک تابع باشد، می‌توان آن را به زبان اضافه کرد و به تابعِ f^* در مدل نااستاندارد رسید که همه‌ی ویژگی‌های مرتبه‌ی اول f را داراست.

تمرین ۲۶ . نشان دهید که یک میدان شمارا وجود دارد که همه‌ی ویژگی‌های اعداد حقیقی را داراست و دارای عناصر بی‌نهایت بزرگ و بی‌نهایت کوچک است.

تعریف ۵۵.

$$\mu(\mathbb{R}^*) = \{x \in \mathbb{R}^* | \forall y \in \mathbb{R}^+ \quad |x| < y\}$$

$$Fin(\mathbb{R}^*) = \{x \in \mathbb{R}^* | \exists y \in \mathbb{R}^+ \quad |x| < y\}$$

منظور از $\mathbb{R}^+$ عناصر مثبت حقیقی است. مجموعه‌ی اول را مجموعه‌ی بی‌نهایت کوچکها و دومی را مجموعه‌ی عناصر متناهی در $\mathbb{R}^*$ می‌نامیم.

تمرین ۲۷ . نشان دهید که حاصل جمع و ضرب عناصر بی‌نهایت کوچک، بی‌نهایت کوچک هستند.

تمرین ۲۸ . نشان دهید که هر عنصر **متناهی** در $\mathbb{R}^*$ به صورت زیر است:

$$x^* = x + dx$$

که در آن dx یک عنصر بی‌نهایت کوچک است $x \in \mathbb{R}$ به طور یکتا تعیین می‌شود. می‌گوییم x بخش استاندارد x^* است و آن را با $st(x^*)$ نیز نمایش می دهیم. (راهنمائی: مجموعه‌ی زیر را در نظر بگیرید:

$$\{x \in \mathbb{R} | x < x^*\}$$

نشان دهید این مجموعه، به عنوان زیرمجموعه‌ای از $\mathbb{R}$ از بالا کراندار، و از این رو، دارای کوچکترین کران بالاست.)

توجه ۵۶. در $\mathbb{R}^*$ داریم:

$$\bigcap_{n \in \mathbb{N}} (۰, \frac{۱}{n}) \neq \varnothing$$

تمرین ۲۹ . نشان دهید $\mathbb{N}$ در $\mathbb{R}^*$ دارای کوچک ترین کران بالا نیست (یعنی کوچکترین بی‌نهایت بزرگ وجود ندارد).

حال می‌توان مفهوم حد را در اعداد حقیقی را با کمک گرفتن از آنالیز نااستاندارد به صورت زیر تعریف کرد.

قضیه ۵۷. فرض کنید $f : \mathbb{R} \to \mathbb{R}$ یک تابع باشد در این صورت در اعداد حقیقی

$$\lim_{x \to a} f(x) = l$$

اگروتنهااگر در $\mathbb{R}^*$ هرگاه $|x - a|$ بی‌نهایت کوچک باشد آنگاه $|f^*(x) - l|$ بی‌نهایت کوچک باشد.

اثبات. فرض کنید بدانیم در $\mathbb{R}^*$ هرگاه فاصله‌ی x از a بی‌نهایت کوچک شود، فاصله‌ی f^* از l بی‌نهایت کوچک می‌شود. برای نشان دادن این که

$$\lim_{x \to a} f(x) = l$$

باید نشان دهیم

$$\mathbb{R} \models \forall \epsilon > ۰ \exists \delta > ۰ \quad (|x - a| < \delta \to |f(x) - l| < \epsilon)$$

برای $\epsilon < \frac{۱}{n}$ در نظر گرفته شده، عبارت زیر در $\mathbb{R}^*$ برقرار است.

$$\mathbb{R}^* \models \exists \delta > ۰ \quad (|x-a| < \delta \to |f^*(x) - l| < \frac{۱}{n}) \qquad (*)$$

زیرا کافی است که δ بی‌نهایت کوچک در نظر گرفته شود. پس از آنجا که $\mathbb{R}^* \models Th(\mathbb{R})$ در $\mathbb{R}$ نیز عبارت (*) برقرار است. پس عنصر مورد نظرِ δ در $\mathbb{R}$ نیز موجود است.

تمرین ۳۰. جهت عکس قضیه‌ی بالا را ثابت کنید.

حد تابع $f(x)$

$$\lim_{x\to a} f(x) = l \Leftrightarrow (x \sim a \Rightarrow f(x) \sim l)$$

پس تابع f در $x=a$ پیوسته است اگر و تنها اگر در $\mathbb{R}^*$ داشته باشیم:

$$x \sim a \Rightarrow f^*(x) \sim f^*(a)$$

درواقع $\lim_{x\to a} f(x) = l$ یعنی اگر $x \sim a$ آن گاه $st(f(x)) = f(a)$

مشتق در آنالیز استاندارد و نااستاندارد

- آنالیز استاندارد

$$\begin{aligned} f'(a) &= \lim_{h\to ۰} \frac{f(a+h)-f(a)}{h} \\ &= \lim_{x\to a} \frac{f(x)-f(a)}{x-a} \end{aligned}$$

- آنالیز نااستاندارد

$f'(a)$ موجود است هرگاه وقتی $x \sim a$ آنگاه $f'(a) \sim \frac{f^*(x)-f^*(a)}{x-a}$

به بیان دیگر، تابع f در نقطه‌ی a مشتق‌پذیر است و مشتق آن عدد استانداردِ $f'(a)$ است هرگاه برای هر مقدار بی‌نهایت کوچکِ dx داشته باشیم $f'(a) \sim \frac{f^*(a+dx)-f^*(a)}{dx}$؛ یا به بیان بهتر هرگاه: $f'(a) \sim \frac{dy}{dx}$. دقت کنید که وقتی f در a مشتق‌پذیر است، در واقع $f'(a) = st(\frac{f^*(a+dx)-f^*(a)}{dx})$.

مثال ۵۸. نشان دهید که اگر تابع f در نقطه‌ی a مشتق پذیر باشد آنگاه f در a پیوسته است.

داریم

$$\frac{f^*(a+dx)-f^*(a)}{dx} \sim f'(a)$$

پس

$$f^*(a+dx) - f^*(a) \sim dx f'(a)$$

به بیان دیگر $f^*(a+dx) - f^*(a)$ بی‌نهایت کوچک است و این یعنی $\lim_{x\to a} f(x) = f(a)$.

مثال ۵۹. فرض کنید $f(x) = x^۲$ در این صورت $f'(a)$ را حساب کنید.

$$f'(a) = st(\frac{(a+dx)^۲ - a^۲}{dx}) = st(\frac{dx^۲ + ۲adx}{dx}) = st(dx + ۲a) = ۲a$$

تمرین ۳۱. نشان دهید $\mathbb{N} \subset \mathbb{R}^*$ از بالا کران دار است ولی دارای کوچکترین کران بالا نیست.

تمرین ۳۲.

- نشان دهید که هر عنصر در $\mathbb{R}^*$ بینهایت نزدیک به یک عنصر در $\mathbb{Q}^*$ است.
- نتیجه بگیرید که

$$| \mathbb{Q}^* | \geqslant 2^{\aleph_0}$$

$$| \mathbb{N}^* | \geqslant 2^{\aleph_0}$$

تمرین ۳۳. نشان دهید

$$A \text{ متناهی است} \Leftrightarrow A = A^*$$

تمرین ۳۴ (مقدار میانی)**.** فرض کنید $A \subseteq \mathbb{R}$ نامتناهی و کراندار باشد. نشان دهید $p \in \mathbb{R}$ موجود است به طوری که p بینهایت نزدیک به یک عنصر از A^* است ولی با آن مساوی نیست. با استفاده از این، قضیه‌ی مقدار میانی را ثابت کنید.

تمرین ۳۵ (قضیه فشردگی)**.** قرار دهید

$$S = \{Th(\mathfrak{M}) \mid \mathfrak{M} \text{ یک } L\text{ساختار است}\}$$

که در آن $Th(\mathfrak{M})$ تئوریِ کامل $\mathfrak{M}$ است. تعریف کنید

$$[\phi] = \{T \in S \mid \phi \in T\}$$

نشان دهید که $[\phi]$ پایه‌ای برای یک توپولوژی روی S است و قضیه فشردگی بیانگر فشردگی S است.

۹.۱ حساب رشته

تعریف ۶۰. فرض کنید $\Delta = \{\delta_1, \cdots, \delta_n\}$ و $\Gamma = \{\gamma_1, \cdots, \gamma_m\}$ مجموعه‌های متناهی از جمله‌ها در یک زبان $L(C)$ باشد. می گوییم رشته‌ی $\Gamma \succ \Delta$ دارای مدل است هرگاه $\delta_1 \wedge \cdots \wedge \delta_n \to \gamma_1 \vee \cdots \vee \gamma_m$ دارای مدل باشد؛ یعنی $L(C)$ ساختار $\mathfrak{M}$ موجود باشد به طوری که $\mathfrak{M} \models \delta_1 \wedge \cdots \wedge \delta_n \to \gamma_1 \vee \cdots \vee \gamma_m$. می‌گوییم رشته $\Gamma \succ \Delta$ همواره‌درست است هرگاه به ازای هر $L(C)$ ساختارِ $\mathfrak{M}$ داشته باشیم

$$\mathfrak{M} \models \delta_1 \wedge \cdots \wedge \delta_n \to \gamma_1 \vee \cdots \vee \gamma_m$$

تعریف ۶۱. می‌گوییم رشته $\Gamma \succ \Delta$ قابل اثبات است هرگاه با متناهی بار استفاده از قواعدی که در ادامه (در سیستم حساب رشته‌ای) می آیند به دست آید.

قوانین حساب رشته‌ای

- $$\frac{}{\Delta \cup \{\phi\} \succ \Gamma \cup \{\phi\}} \quad \text{اصول}$$

- $$\frac{\Delta \succ \Gamma \cup \{\phi\}}{\Delta \cup \{\neg\phi\} \succ \Gamma} \quad \neg\text{چپ}$$

- $$\frac{\Delta \cup \{\phi\} \succ \Gamma}{\Delta \succ \Gamma \cup \{\neg\phi\}} \quad \neg\text{راست}$$

- $$\frac{\Delta \cup \{\phi_1\} \succ \Gamma}{\Delta \cup \{\phi_1 \wedge \phi_2\} \succ \Gamma} \quad \wedge\ \text{چپ}$$

- $$\frac{\Delta \cup \{\phi_2\} \succ \Gamma}{\Delta \cup \{\phi_1 \wedge \phi_2\} \succ \Gamma} \quad \wedge\ \text{چپ}$$

- $$\frac{\Delta \succ \Gamma \cup \{\phi_1\} \quad \Delta \succ \Gamma\phi_2\}}{\Delta \succ \Gamma \cup \{\phi_1 \wedge \phi_2\}} \quad \wedge\ \text{راست}$$

- $$\frac{\Delta \cup \phi(c) \succ \Gamma}{\Delta \cup \{\exists x\phi(x)\} \succ \Gamma} \quad \exists\text{چپ}$$

  در صورتی که ثابتِ $c \in C$ در Δ و Γ استفاده نشده باشد.

- $$\frac{\Delta \succ \Gamma \cup \phi(c)}{\Delta \succ \Gamma \cup \{\exists x\phi(x)\}} \quad \exists\text{راست}$$

تمرین ۳۶. نشان دهید که گزاره زیر قابل اثبات است.

$$\exists x\forall y \quad R(x,y) \rightarrow \forall y\exists x \quad R(x,y)$$

به بیان دیگر نشان دهید که رشته‌ی

$$\emptyset \succ \{\exists x\forall y \quad R(x,y) \rightarrow \forall y\exists x \quad R(x,y)\}$$

قابل اثبات است.

قضیه ۶۲ (تمامیت). رشته $\Delta \succ \Gamma$ قابل اثبات است اگر و تنها اگر همواره درست باشد.

اثبات. دقت کنید که قوانینی که در بالا نوشته شد، در همه‌ی $L(C)$ ساختارها درست هستند. پس اگر رشته‌ای قابل اثبات باشد در تمام $L(C)$ ساختارها درست است.

در ادامه نشان می‌دهیم که اگر رشته‌ی $\Gamma \succ \Delta$ غیر قابل اثبات باشد، آنگاه یک $L(C)$ ساختارِ $\mathfrak{M}$ چنان یافت می‌شود که برای هر جمله‌ی $\delta \in \Delta$ داریم $\mathfrak{M} \models \delta$ و برای هر جمله‌ی $\gamma \in \Gamma$ داریم $\mathfrak{M} \models \neg\gamma$؛ به بیان دیگر رشته‌ی یادشده در ساختار یادشده درست نیست.

فرض کنید $\Gamma \succ \Delta$ رشته‌ی غیرقابل اثبات ما باشد. قرار دهید $\Delta_0 = \Delta$ و $\Gamma_0 = \Gamma$ و مجموعه‌های

$$\Delta_0 \subseteq \Delta_1 \subseteq \dots$$

و

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \dots$$

را به گونه‌ای که در زیر خواهم گفت بسازید به طوری که هر رشته‌ی

$$\Delta \succ \Gamma$$

غیر قابل اثبات باشد.

یک شمارشِ $(\epsilon_i, \phi_i, c_i)$ از علامتهای $\epsilon_i \in \{l, r\}$ و ϕ_i یک فرمول، و $c_i \in C$ را به گونه‌ای در نظر بگیرید که در این شمارش تمامی فرمولها و ثوابت و علامتهای چپ و راست، بی‌نهایت بار ظاهر شوند و هر حالت ممکن از بروز سه‌تائی آنها نیز بی‌نهایت بار رخ دهد. دقت کنید که به جای کلمه‌های چپ و راست از حروف l, r استفاده کرده‌ام. همچنین دقت کنید که همچنان این شمارش (یعنی شمارا بودن) امکان‌پذیر است.

حال فرض کنید که رشته‌ی $\Gamma_i \succ \Delta_i$ را در اختیار داریم و می‌دانیم که این رشته غیرقابل اثبات است. برای ساختنِ رشته‌ی غیرقابل اثباتِ $\Gamma_{i+1} \succ \Delta_{i+1}$ نخست به عنصرِ $(\epsilon_i, \phi_i, c_i)$ نگاه می‌کنیم و بنا به یکی از حالات زیر عمل می‌کنیم.

۱. اگر $\epsilon_i = l$ و $\neg\phi_i \in \Delta_i$ آنگاه قرار دهید $\Delta_{i+1} = \Delta_i$ و $\Gamma_{i+1} = \Gamma_i \cup \{\phi_i\}$. در این صورت رشته‌ی $\Gamma_{i+1} \succ \Delta_{i+1}$ غیر قابل اثبات است؛ زیرا اگر اثبات شود، آنگاه بنا به قانونِ نقیض‌چپ رشته‌ی $\Gamma_i \succ \Delta_i$ اثبات خواهد شد:

$$\frac{\Delta_i \succ \Gamma_i \cup \{\phi_i\}}{\Delta_i \cup \{\neg\phi_i\} \succ \Gamma_i}$$

خط بالائی برابر با رشته‌ی $\Gamma_{i+1} \succ \Delta_{i+1}$ است و خط پائینی همان رشته‌ی $\Gamma_i \succ \Delta_i$ است.

۲. اگر $\epsilon_i = r$ و $\neg\phi_i \in \Gamma_i$ آنگاه قرار دهید $\Delta_{i+1} = \Delta_i \cup \{\phi_i\}$ و $\Gamma_{i+1} = \Gamma_i$. بنا به قانونِ نقیض‌راست، این رشته‌ی جدید غیرقابل‌اثبات است.

۳. اگر $\epsilon_i = l$ و $\phi_i = \psi_1 \wedge \psi_2 \in \Delta_i$ آنگاه قرار دهید $\Delta_{i+1} = \Delta_i \cup \{\psi_1, \psi_2\}$ و $\Gamma_{i+1} = \Gamma_i$. بنا به قانون عطف‌چپ، رشته‌ی $\Gamma_{i+1} \succ \Delta_{i+1}$ قابل اثبات نیست.

۴. اگر $\epsilon_i = r$ و $\phi_i = \psi_1 \wedge \psi_2 \in \Gamma_i$ آنگاه قرار دهید $\Delta_{i+1} = \Delta_i$ و $\Gamma_{i+1} = \Gamma_i \cup \{\psi_1, \psi_2\}$.

۵. اگر $\epsilon_i = l$ و $\phi_i = \exists x \quad \psi$ آنگاه قرار دهید $\Delta_{i+1} = \Delta_i \cup \{\psi(c_i)\}$ و $\Gamma_{i+1} = \Gamma_i$.

۶. اگر $\epsilon_i = r$ و $\phi_i = \exists x \quad \psi$ آنگاه قرار دهید $\Delta_{i+1} = \Delta_i$ و $\Gamma_{i+1} = \Gamma_i \cup \{\psi(c_i)\}$.

۷. اگر هیچ‌کدام از حالات بالا برقرار نباشد، قرار دهید $\Delta_{i+1} = \Delta_i$ و $\Gamma_{i+1} = \Gamma_i$.

دنباله‌ی $\Delta_i \succ \Gamma_i$ که در بالا ساخته شد دارای ویژگی زیر است:

- هیچ Δ_i با هیچ Γ_i اشتراکی ندارد؛ زیرا Δ_0 با Γ_0 اشتراکی نداشت (در غیر این صورت بنا به اصل، رشته‌ی $\Delta_0 \succ \Gamma_0$ قابل اثبات می‌شد).

حال قرار دهید $\Delta^* = \bigcup \Delta_i$ و $\Gamma^* = \bigcup \Gamma_i$. در این صورت Δ^* و Γ^* ویژگی‌های زیر را دارا هستند:

- $\Delta^* \cap \Gamma^* = \emptyset$.
- اگر $\phi \in \Delta_i$ آنگاه $\neg\phi \in \Gamma_i$.
- اگر $\phi \in \Gamma_i$ آنگاه $\neg\phi \in \Delta_i$.
- اگر $\exists x\phi \in \Delta_i$ آنگاه ثابت c موجود است به طوری که $\phi(c) \in \Delta$.
- اگر $\exists x\phi \in \Gamma$ آنگاه برای هر ثابتِ $c \in C$ جمله‌ی $\phi(c)$ در Γ است.
- اگر $\phi_1 \wedge \phi_2 \in \Delta^*$ آنگاه ϕ_1 و ϕ_2 هر دو در Δ^* هستند.
- اگر $\phi_1 \wedge \phi_2 \in \Gamma^*$ آنگاه ϕ_1 یا ϕ_2 در Γ^* هستند.

در زیر یک ساختارِ $\mathfrak{M}$ معرفی کرده‌ام که در آن تمام جملات موجود در Δ^* برقرار هستند ولی هیچ‌یک از جملاتِ موجود در Γ^* برقرار نیست. به طور خاص، در ساختاری که معرفی خواهم کرد، رشته‌ی $\Delta_0 \succ \Gamma_0$ درست نیست.

جهان ساختارِ $\mathfrak{M}$ را همان مجموعه‌ی C از ثوابت در نظر بگیرید. حال روابط زبان را به صورت زیر در $\mathfrak{M}$ تعبیر کنید:

$$R^{\mathfrak{M}}(c_1, \ldots, c_n) \Leftrightarrow R(c_1, \ldots, c_n) \in \Delta^*$$

توجه کنید که در این اثبات، فرض کرده‌ام که زبان، تنها از روابط تشکیل شده است، و اثبات برای حالتی که زبان دارای توابع و ثوابت باشد، مشابه است. حتی می‌توان هر تابع را به عنوان یک رابطه در نظر گرفت.

حال با استقراء روی ساخت فرمولها نشان می‌دهم که اگر $\phi \in \Delta^*$ آنگاه $\mathfrak{M} \models \phi$ و اگر $\phi \in \Gamma^*$ آنگاه $\mathfrak{M} \not\models \phi$.

۱. اگر $\phi = R(c_1, \ldots, c_n)$. در این صورت بنا به تعریف اگر $\phi \in \Delta^*$ آنگاه $\mathfrak{M} \models \phi$. همچنین اگر $\phi \in \Gamma^*$ آنگاه $\neg\phi \in \Delta^*$ پس $\mathfrak{M} \models \neg\phi$.

۲. اگر $\phi = \neg\psi$ و حکم برای ψ ثابت شده باشد. آنگاه اگر $\phi \in \Delta^*$ آنگاه $\neg\phi \in \Gamma^*$ پس $\mathfrak{M} \models \neg\neg\phi$. مشابهاً برای وقتی که $\phi \in \Gamma^*$ عمل کنید.

۳. اگر $\phi = \psi_1 \wedge \psi_2 \in \Delta^*$. آنگاه ψ_1 و ψ_2 هر دو در Δ^* هستند و بنا به فرض استقرا داریم $\mathbb{M} \models \phi_1$ و $\mathfrak{M} \models \phi_2$.

۴. اگر $\phi = \psi_1 \wedge \psi_2 \in \Gamma^*$ آنگاه مثلا $\psi_1 \in \Gamma^*$. پس $\mathfrak{M} \models \neg\psi_1$ و از این رو $\mathfrak{M} \models \neg\psi_1 \vee \neg\psi_2$.

۵. بررسی دو حالت باقی‌مانده را به عنوان تمرین رها می‌کنم.

□

آنچه در تمرین زیر بیان کرده‌ام ویژگی درونیابی نام دارد. اثبات این تمرین، با استفاده از حساب رشته‌ها آسان است؛ با این حال اگر به جای نظریه‌ی اثبات بخواهیم از نظریه‌ی مدل استفاده کنیم، من راهی برای اثبات آن نمی‌دانم.

بنا به تمرین زیر، اگر عبارتی از عبارتی دیگر نتیجه شود، اطلاعاتی در یک زبان مشترک در این میان هست که به کار آمده است؛ باقی اطلاعات اضافه بوده‌اند. مثلاً وقتی می‌خواهیم به عنوان قاضی، به دعوای دو نفر رسیدگی کنیم، باید سرنخ را میان جملاتی بیابیم که درباره‌ی موضوعات مشترک هستند!

تمرین ۳۷. فرض کنید ϕ یک جمله در زبانِ L_1 باشد و ψ یک جمله در زبانِ L_2. فرض کنید که

$$\phi \to \psi$$

همواره درست باشد. نشان دهید که یک جمله‌ی ξ در زبانِ $L_1 \cap L_2$ وجود دارد به طوری که $\phi \to \xi$ و $\xi \to \psi$ هر دو همواره درست هستند.

راهنمائی. به طور کلی‌تر نشان دهید که اگر $\Delta_1 \cup \Delta_2 \succ \Gamma_1 \cup \Gamma_2$ یک رشته‌ی همواره درست باشد و Δ_i در زبان L_i باشد، آنگاه جمله‌ی ξ در زبان $L_1 \cap L_2$ یافت می‌شود به طوری که

$$\Delta_1 \succ \Gamma_1 \cup \{\xi\}$$

و

$$\{\xi\} \cup \Delta_2 \succ \Gamma_2$$

هر دو رشته‌های همواره درست هستند. برای اثبات این گفته نیز، از استقراء روی طول اثبات استفاده کنید.

۱۰.۱ اثبات قضیه‌ی فشردگی با استفاده از حساب رشته‌ها

می‌گوییم جمله‌ی ϕ قابل اثبات است، و می‌نویسیم $\vdash \phi$، هرگاه رشته‌ی $\emptyset \succ \phi$ قابل اثبات باشد. در قضیه‌ی تمامیت ثابت کردیم که

$$\vdash \phi \Leftrightarrow \models \phi.$$

می‌گوییم فرمول ϕ با استفاده از اصول تئوریِ T قابل اثبات است و می‌نویسیم $T \vdash \phi$ هرگاه هر وقت که تمام فرمولهای موجود در T اثبات شوند آنگاه ϕ نیز اثبات شود. به بیان دیگر، هرگاه اثباتی برای ϕ وجود داشته باشد که در آن از اصول موجود در T استفاده شده است. **دقت کنید که اگر $T \vdash \phi$ آنگاه بنا بر طبیعت اثبات‌پذیری، تنها متناهی جمله از T هستند که در اثباتِ ϕ استفاده شده‌اند و خودِ اثبات نیز طبق تعریف، متناهی مرحله دارد. به بیان دیگر، $T \vdash \phi$ اگروتنهااگر یک زیرمجموعه‌ی متناهیِ $T \supseteq \Delta$ موجود باشد به طوری که $\Delta \vdash \phi$.**

تمرین ۳۸. نشان دهید که

$$T \models \phi \Leftrightarrow T \vdash \phi.$$

تئوریِ T مدل ندارد هرگاه $T \models \perp$ (به انتفاء مقدم). پس T مدل ندارد هرگاه $T \vdash \perp$. پس T مدل ندارد هرگاه یک زیرمجموعه‌ی متناهی از T مانند Δ یافت شود به طوری که $\Delta \vdash \perp$. پس T مدل ندارد هرگاه یک زیرمجموعه‌ی متناهی Δ از آن

پیدا شود به طوری که $\Delta \models \perp$. آنچه گفته شد، همان قضیه‌ی فشردگی است: T دارای مدل است اگروتنهااگر هر زیرمجموعه‌ی متناهی از آن دارای مدل باشد.

به بیان کوتاه‌تر یک تئوری زمانی مدل ندارد که تناقضی از جملات آن نتیجه شود؛ و بنا به طبیعت اثباتها، در این صورت، حتماً تناقض از بخشی متناهی از T به دست می‌آید. پس اگر هر بخش متناهی از T تناقض ندهد، T تناقض نمی‌دهد.

گفتیم که $T \models \phi$ هرگاه اثباتی برای ϕ با استفاده از جملات T وجود داشته باشد. از طرفی گفتیم که قوانین اثبات متناهی و ساده هستند. بنابراین به جای تولید کردن ریاضی، چرا اصول یک تئوری ریاضی T را به همراه روشهای متناهی ساده‌ی استدلال به یک رایانه ندهیم تا خود این اصول و قوانین را با هم ترکیب کند و همه‌ی قضیه‌های ریاضی را بسازد؟ در بخش آینده درس به این موضوع خواهیم پرداخت.

۱۱.۱ تصمیم‌پذیری

فرض کنید $\mathfrak{M}$ یک L ساختار باشد و T یک تئوری کامل باشد به طوری که $\mathfrak{M} \models T$. در این صورت برای هر جمله φ داریم

$$\mathfrak{M} \models \varphi \Leftrightarrow T \models \varphi \Leftrightarrow T \vdash \varphi$$

حال فرض کنید جمله‌های موجود در تئوریِ کاملِ T را بتوان با یک روش کارا تولید کرد (یعنی، یک الگوریتم، با هر تعریف شهودی‌ای که برای الگوریتم دارید، وجود داشته باشد که جملات تئوریِ T را لیست کند). در این صورت، بنا به این که روشهای اثبات در روش حساب رشته‌ها قابل ورود به یک الگوریتم هستند، یک الگوریتم داریم که می‌تواند تمامی جملات موجود در تئوریِ T را به همراه تمامی نتایج این تئوری، لیست کند. در این صورت برای هر جمله‌ی φ داریم

$$\mathfrak{M} \models T \Leftrightarrow T \vdash \varphi \Leftrightarrow \text{الگوریتم مورد نظر } \varphi \text{ را تولید کند}$$

در اینجا با یک سوال فلسفی ـ ریاضی مهم رو به رو می‌شویم: اگر امکان داشته باشد که یک سری اصول اولیه برای ریاضیات نوشت به صورتی که

۱. این مجموعه از اصول کامل باشد

۲. این مجموعه از اصول قابل لیست شدن توسط یک الگوریتم باشد

آنگاه الگوریتمی که اصول اولیه‌ی ریاضیات را تولید می‌کند قادر به تولید تمامی نتایج ریاضی این اصول است. بنابراین هر قضیه‌ای در ریاضی اگر قابل اثبات باشد، توسط این اصول تولید می‌شود؛ و اگر قابل اثبات نباشد، از آنجا که تئوری ما کامل است، نقیض آن از این اصول نتیجه می‌شود. پس ماشین می‌تواند تمام ریاضیات بشری را تولید کند و نیازی به ریاضیدان نیست!

در ادامه‌ی درس می‌خواهیم به روشن کردن موضوع بالا بپردازیم. در واقع هدف ما اثبات قضیه‌ی مهم زیر است:

قضیه ۶۳. با هیچ الگوریتمی نمی‌توان اصول کاملی برای نظریه‌ی اعداد (یعنی برای ساختار $(\mathbb{N}, +, \cdot)$) تولید کرد.

قضیه‌ی بالا را (به صورتی که نوشته شده است) قضیه‌ی ناتمامیت اول گودل می‌خوانند. البته این قضیه محتوای مفصل‌تر زیر را نیز دارد که بیان زیر از آن را قضیه‌ی ناتمامیت دوم گودل می‌خوانند. به این قضیه نیز تا پایان ترم خواهیم پرداخت.

قضیه ۶۴. در صورتی که T یک تئوری برای نظریه‌ی اعداد باشد که توسط یک الگوریتم لیست شده است، یک جمله‌ی φ وجود دارد به طوری که $(\mathbb{N}, +, \cdot) \models \varphi$ اما $T \not\vdash \varphi$.

توجه ۶۵. از کلمه‌ی الگوریتم، یا روش کارا، درادامه‌ی درس بسیار استفاده خواهم کرد، بی‌آنکه تعریف دقیقی از آن ارائه دهم. پس فعلاً تعریف ما از روش کارا، روشی است که با یک ماشین برنامه‌نویس قابل اجراست.

برای این که یک تئوری بتواند تصمیم بگیرد، لزوماً نیازی نیست که کامل باشد:

تعریف ۶۶.

- فرض کنید T یک تئوری مرتبه اول باشد می گوئیم تئوری T تصمیم پذیر است هرگاه یک الگوریتم وجود داشته باشد که برای هر جمله φ اگر $T \models \varphi$ الگوریتم پاسخ بله بدهد و اگر $T \not\models \varphi$ الگوریتم پاسخ خیر بدهد.
- ساختار $\mathfrak{M}$ را تصمیم پذیر نامیم هرگاه الگوریتمی وجود داشته باشد که برای هر جمله φ تصمیم بگیرد که $\mathfrak{M} \models \varphi$ یا $\mathfrak{M} \not\models \varphi$.

تمرین ۳۹. اگر T یک تئوری کامل باشد که توسط یک روش کارا لیست شده باشد، آنگاه T تصمیم‌پذیر است.

در ادامه‌ی درس، نخست با چند بخشِ تصمیم‌پذیر از حساب، آشنا می‌شویم و پس از آن به سمت قضایای ناتمامیت خواهیم رفت.

۱۲.۱ ساختارِ $\mathfrak{N}_s$

ساختارِ $(\mathbb{N}, s, ۰)$ را با $\mathfrak{N}_s$ نشان می‌دهیم. در این ساختار، ۰ یک ثابت است که نقش صفر اعداد طبیعی را بازی می‌کند و $s(x) = x + ۱$ تابع تالی است.

تئوری زیر را در نظر بگیرید

$$
\begin{gathered}
T_s = \{\forall x \quad s(x) \neq ۰, \\
\forall x \quad (x \neq ۰ \to \exists y \quad s(y) = x), \\
\forall x, y \quad (s(x) = s(y) \to x = y), \\
\forall x \quad s(x) \neq x, \\
\forall x \quad s^{۲}(x) \neq x, \\
\forall x \quad s^{۳}(x) \neq x, \\
\cdots\}
\end{gathered}
$$

تمرین ۴۰. نشان دهید که خواسته‌ی جمله‌ی زیر را نمی توان در یک تئوری مرتبه‌ی اول برای $\mathfrak{N}_s$ گنجاند.

$$\forall x \exists n \in N \quad s^n(۰) = x$$

لم ۶۷. تئوری T دارای یک مدل شماراست که درآن عنصری وجود دارد که

$$\forall n \in N \quad x \neq s^n(۰)$$

اثبات. تئوریِ

$$T' = T_s \cup \{c \neq ۰, x \neq s(۰), x \neq s^۱(۰), x \neq s^۲(۰), \cdots, x \neq s^n(۰), \cdots\}$$

متناهیا سازگار، و از این رو بنا به فشردگی سازگار است، و بنا به لونهایم اسکولم دارای مدلی شماراست. □

همچنین به آسانی می‌توان ثابت کرد که:

لم ۶۸. هر مدل تئوری T_s شامل $\mathbb{N}$ است.

اما دو لم بالا به حقیقت عجیبی درباره‌ی مدلهای شمارای T_s اشاره دارند: هر مدل شمارای T_s لزوماً مجموعه‌ی اعداد طبیعی نیست. یعنی T_s یک مدل شمارا دارد که در آن عنصری نااستاندارد (یعنی غیر از تالی متناهی صفر) وجود دارد. دقت کنید که اگر x یک عنصر ناااستاندارد باشد، تمامی عناصری که در فاصله‌ی استاندارد آن قرار دارند، یعنی تمام عناصری که با متناهی بار اعمال تابع s و $s^{-۱}$ به x ایجاد می‌شوند، باز هم ناااستاندارد هستند. پس حول هر عنصر ناااستاندارد یک $\mathbb{Z}$ زنجیر وجود دارد.

تمرین ۴۱. چند مدلِ غیرایزومرف از سایز $\aleph_۰$ برای این تئوری وجود دارد؟

قضیه ۶۹. برای هر $\kappa > \aleph_۰$ تئوری T_s یک تئوریِ κ جازم است.

اثبات. فرض کنید $\mathfrak{M}_۱$ و $\mathfrak{M}_۲$ دو مدل این تئوری باشند. در این صورت هر دوی این مدلها دارای κ طبقه‌اند. (یعنی از κ تا $\mathbb{Z}$ زنجیر تشکیل شده‌اند). در این صورت با نظیر کردن هریک از طبقات این دو مدل با هم توسط یک تابع f که دو بخش $\mathbb{N}(\mathfrak{M}_۱)$ و $\mathbb{N}(\mathfrak{M}_۲)$ را به هم نظیر کند، این دو ساختار با هم ایزومرف می‌شوند. □

نتیجه ۷۰. تئوری T_s سازگار و κ جازم است، بنابراین T یک تئوری کامل است.

نتیجه ۷۱. ساختارِ $(\mathbb{N}, s, ۰)$ یک ساختارِ تصمیم‌پذیر است.

اثبات. ازآنجا که تئوری T_s قابل تولید توسط یک روش کاراست، مجموعه‌ی همه‌ی نتایجِ T قابل تولید توسط یک روش کاراست. از آنجا که T_s کامل است و $(\mathbb{N}, s, ۰)$ مدل آن است، همه‌ی ویژگی‌های مرتبه‌ی اول این ساختار، توسط الگوریتمی که نتایج تئوری را تولید می‌کند، تولید می‌شود. □

تعریف ۷۲. می گوییم تئوری T سورها را حذف می‌کند هرگاه برای هر فرمول $\phi(x_۱, \cdots, x_n)$ با متغیرهای آزادِ $x_۱, \ldots, x_n$ یک فرمولِ بدون سور $\psi(x_۱, \cdots, x_n)$ با متغیرهای آزادِ $x_۱, \ldots, x_n$ پیدا شود به طوری که

$$T \vdash \forall x_۱, \cdots, x_n \quad (\phi(x_۱, \cdots, x_n) \leftrightarrow \psi(x_۱, \cdots, x_n)).$$

یک مصداق آشنای معادل بدون سور برای یک فرمول را در ریاضیات دبیرستانی دیده‌اید: در میدان اعداد حقیقی فرمولِ

$$\phi(a, b, c) : \exists x \quad ax^۲ + bx + c = ۰$$

معادل با فرمول زیر است:

$$((b^۲ - ۴ac \geq ۰) \vee (a = b = c = ۰))).$$

لم ۷۳. فرض کنید تئوری T به گونه‌ای باشد که هر فرمول به صورت زیر نسبت به T دارای معادل بدون سور باشد، در این صورت تئوری T سورهارا حذف می کند.

$$\exists x(\beta_1 \wedge \cdots \wedge \beta_n) \qquad (\beta_i(x, y_1, \ldots, y_n) \text{ اتمی یا نقیض اتمی})$$

اثبات. با استقرا روی ساخت ترمها نشان می‌دهیم که همه‌ی فرمول‌ها دارای معادل بدون سورند. فرض کنید فرمول φ به صورت $t_1 = t_2$ و $R(t_1, ..., t_n)$ باشد، در این صورت φ دارای معادل بدون سور است. فرض کنید ψ_1 و ψ_2 معادل بدون سور داشته باشند.در این صورت $\psi_1 \wedge \psi_2 \equiv {\psi'}_1 \wedge {\psi'}_2$ (که در آن ${\psi'}_1$و${\psi'}_2$ معادل‌های بدون سور ψ_1وψ_2 هستند) نیز دارای معادل بدون سور است. همچنین واضح است که اگر φ دارای معادل بدون سور باشد، آنگاه $\neg\varphi$ نیز دارای معادل بدون سور است.
حال فرض کنید ψ دارای معادل بدون سور باشد، در این صورت $\psi \equiv \exists x \underbrace{\psi'}_{\text{بدون سور}}$ از آن جا که $\exists x \quad \psi'$ بدون سور است:

$$\psi' = \underbrace{({\beta^1}_1 \wedge \cdots \wedge {\beta^1}_n)}_{\chi_1} \vee ... \vee ({\beta^m}_1 \wedge \cdots \wedge {\beta^m}_n) \quad (\text{صورت نرمال عطفی})$$

پس در این حالت نیز سور، بنا به مشاهده‌ی زیر، حذف می‌شود.

مشاهده ۷۴.

$$\exists x(p(x) \vee q(x)) \Leftrightarrow \exists x p(x) \vee \exists x q(x)$$

پس

$$\exists x \psi' \Leftrightarrow (\exists x \chi_1) \vee ... \vee (\exists x \chi_m)$$

تک تک فرمول های بالا دارای معادل بدون سور می باشند.

□

حذف سور روی جبر مدلهای یک تئوری، تأثیر زیر را می‌گذارد:

مشاهده ۷۵. فرض کنید تئوری T سورها را حذف کند و $\mathfrak{M}_1, \mathfrak{M}_2 \models T$ و $A \subseteq \mathfrak{M}_1, \mathfrak{M}_2$ (زیرساختار مشترک دو مدل فوق) و φ یک فرمول دلخواه باشد. در این صورت برای هر $\bar{a} \in A$ داریم

$$\mathfrak{M}_1 \models \varphi(\bar{a}) \Leftrightarrow \mathfrak{M}_2 \models \varphi(\bar{a})$$

تمرین ۴۲. مشاهده‌ی فوق را اثبات کنید.

قضیه ۷۶. T_s سورها را حذف می‌کند.

اثبات. برای اثبات این قضیه کافی است (مشابه لم قبل) فرمول‌های به صورت

$$\exists x(\beta_1 \wedge \cdots \wedge \beta_n) \qquad (\beta_i \text{ اتمی یا نقیض اتمی})$$

را بررسی کنیم و مطمئن شویم که معادل بدون سور دارند.

فرمول های اتمی و نقیض اتمی (با متغیرهای $x_۱, ..., x_n$) در زبان این تئوری همگی به یکی از صورتهای زیر هستند:

$$s^m ۰ = s^n ۰$$

$$s^m x_i = s^n x_j$$

$$s^m x_i = x_j$$

$$s^m x_i = s^n ۰$$

با تسامح، به جای $s^n(x) = s^m ۰$ می‌نویسیم $x + n = m$. پس با دستگاهی از معادلات به صورت زیر مواجه هستیم:

$$\exists x \begin{cases} \{x + n_j = x_j + m_j\}_{j=۱,...,k} \\ ... \\ \text{و چند فرمول در صورت نقیض فرمولهای بالا} \end{cases}$$

اگر دستگاه بالا شامل یک فرمول دارای تساوی باشد، مثلاً فرمولِ

$$x + m = y + n$$

در آن باشد، مثلا به صورت

$$\exists x \quad (x + m = y + n) \wedge \psi(x, \bar{y})$$

باشد، آنگاه فرمول بالا معادل با فرمول بدون سور زیر است:

$$\psi(y + n - m)$$

هر چند در زبان، نماد منفی نداریم، اما از آنجا که ψ خود مجموعه‌ای از معادلات است، با جمع کردن طرفین با عباراتی مناسب می‌توانیم به فرمول بدون سور در زبان اصلی برسیم.

فرض کنید دستگاه بالا شامل تساوی نباشد؛ در این صورت، با کم و زیاد کردن اعداد طبیعی، می‌توان دستگاه را به صورت زیر نوشت:

$$\exists x \{x \neq u_j(y_۱, \ldots, y_m)\}_{j=۱,...,k}$$

باشد، دراین صورت از آنجا که مدلهای T نامتناهی هستند دستگاه یادشده قابل حل است. پس فرمول بالا، معادل با فرمول بدون سورِ $x = x$ است. $\square$

تمرین ۴۳. نشان دهید که هر زیرمجموعه‌ی $\mathbb{N}$ که توسط یک فرمولِ $\phi(x)$ در ساختارِ $(\mathbb{N}, s, ۰)$ تعریف شود، یا متناهی است یا متممتناهی. اگر $\mathfrak{M}$ یک مدل دلخواه از T_s باشد، آیا این گفته درباره‌ی آن صادق است؟

تمرین ۴۴. نشان دهید که ترتیب اعداد طبیعی در ساختار $(\mathbb{N}, s, ۰)$ قابل تعریف نیست. یعنی هیچ فرمولِ $\phi(x, y)$ در این زبان وجود ندارد به طوری که

$$\{(x, y) \in \mathbb{N}^۲ | x < y\} = \{(x, y) \in \mathbb{N}^۲ | \varphi(x, y)\}$$

تمرین ۴۵. نشان دهید که T_s دارای اصل‌بندی متناهی نیست.

حذف سور بالا، اثبات دیگری برای کامل بودن تئوریِ T_s فراهم می‌کند. فرض کنید φ یک جمله باشد. بنا به حذف سور، این جمله دارای یک معادل بدون سور است و از آنجا که هیچ متغیر آزادی ندارد، به صورت عطف و فصلهائی از فرمولهایی به صورت زیر یا نقیض آنهاست:

$$s^m \cdot = s^n \cdot$$

تئوری به سادگی درستی یا غلطی فرمولهای به فرم بالا را تصمیم‌گیری می‌کند.

۱۳.۱ ساختارِ $\mathfrak{N}_l$

در این بخش به ساختارِ

$$\mathfrak{N}_l = (\mathbb{N}, +, \cdot, <)$$

پرداخته‌ایم. دقت کنید که ترتیب در ساختارِ $\mathfrak{N}_s$ قابل تعریف نبود، پس ساختارِ $\mathfrak{N}_l$ حاوی بخش بزرگتری از حساب است.

تئوری T_l را به صورت زیر در نظر بگیرید

$$\forall y \quad (y \neq \cdot \rightarrow y = s(x))$$

$$\forall x, y \quad x < s(y) \rightarrow x \leq y$$

$$\forall x \neg (x < \cdot)$$

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

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

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

تمرین ۴۶. نشان دهید که از T_l نتیجه می‌شود که s یک تابع اکیدا صعودی است.

قضیه ۷۷. T_l سورها راحذف می‌کند.

اثبات. کافی است نشان دهیم که فرمولهای به صورت $\exists x(\varphi(x, y_۱, \cdots, y_n))$ که در آن φ عطفی از فرمول های اتمی و نقیض اتمی است، دارای معادلی بدون سور هستند. صورت کلی فرمول های اتمی به صورت زیر است:

$$x < t(y, \ldots, y_n)$$

$$x = t(y_۱, \ldots, y_n)$$

که در آنها t ترمی در زبان است (که ممکن است شامل علامت $-$ نیز باشد.) □

پس شکل کلی فرمول مورد نظر چندین معادله به یکی از صورتهای زیر است:

$$\exists x$$

$$(\{x = t_i(y_۱, \ldots, y_n)$$

$$x \neq t_i(y_۱, \ldots, y_n)$$

$$\{x + n_i < y_i + m_i$$

$$\{u_i(y_۱, \ldots, y_n) < x < t_i(y_۱, \ldots, y_n)$$

که باز هم در t_i از علامت منفی هم استفاده شده است.

می‌توان فرض کرد فرمولهای حاوی $\neq$ وجود ندارند. زیرا

$$T_l \vdash x \neq y \leftrightarrow (x < y \vee y < x)$$

پس می توان فرض کرد که فرمولهای اتمی تنها دارای نمادهای $<$ و $=$ هستند.

اگر در معادلات بالا تساویِ $x = t(y_۱, \ldots, y_n)$ وجود داشته باشد معادل بدون سور مورد نظر به راحتی با قرار دادن $t(y_۱, \ldots, y_n)$ به جای x در معادلات دیگر به دست می‌آید.

فرض کنید که علامت تساوی در فرمول های یاد شده وجود ندارد. در این صورت فرمول مورد نظر بیانگر حدود بالایی و پایینی برای x است.در این فرمول φ معادل با فرمولی است که بیان کند ماکزیمم کران های پایین از مینیموم کران های بالا کمتر است.

اثبات زمانی کامل می‌شود که با جمع کردن عبارتها با اعداد مناسب، تمام ظهورهای علامت منفی را از بین ببریم.

نتیجه ۷۸. تئوری T_l کامل است.

اثبات. فرض کنید φ یک جمله در زبان $L(T_l)$ باشد. بنا به آنچه گفته شد، φ دارای یک معادل بدون سور است و همچنین هیچ متغیر آزادی ندارد. پس عطف و فصلی از فرمولهای به صورت زیر است:

$$s^n(۰) < s^m(۰)$$

اما به راحتی می‌توان دید که

$$T_L \vdash ۰ < ۱ < ۲ < ۳ < \cdots$$

پس تئوری T_l می تواند نسبت به زیرفرمولهای φ و در نتیجه نسبت به خودِ φ تصمیم بگیرد. □

نتیجه ۷۹. ساختار $(\mathbb{N}, s, ۰, <)$ تصمیم پذیر است.

اثبات. حکم از این نتیجه می‌شود که T_l به صورت کارا تولید می‌شود و کامل است. □

تمرین ۴۷. نشان دهید که هر زیر مجموعه از $\mathbb{N}$ که در ساختار $(\mathbb{N}, s, ۰, <)$ تعریف پذیر باشد یا متناهی است یا متمم آن متناهی است. آیا این گفته برای هر مدلِ $\mathfrak{N} \models T_l$ نیز درست است؟

نتیجه ۸۰. جمع اعداد طبیعی در ساختار $(\mathbb{N}, s, ۰, <)$ قابل تعریف نیست. یعنی هیچ فرمولِ $\phi(x, y, z)$ وجود ندارد به طوری که

$$\{(x, y, z) \in \mathbb{N}^۳ | x + y = z\} = \{(x, y, z) \in \mathbb{N}^۳ | \varphi(x, y, z)\}$$

اثبات. فرض کنید فرمول بالا وجود داشته باشد در این صورت

$$X = \{x | \exists y \quad y + y = x\}$$

یک مجموعه تعریف‌پذیر است اما نه X متناهی است و نه $\mathbb{N} - X$ متناهی است. □

تمرین ۴۸. جازمیتِ T_l را بررسی کنید.

۱۴.۱ حساب پرسبرگر

متاسفانه جزوه‌ی این جلسه درست تایپ نشده است. آنچه به دست من رسیده است بسیار ناقص است و متاسفانه وقت آن را ندارم که خودم کامل جزوه‌ی این جلسه را بنویسم. بنابراین حساب پرسبرگر در امتحان خواهد آمد، اما خود دانشجو موظف است تا آن را در کتابها مطالعه کند (کتاب اندرتون مرجع خوبی است).

۱۵.۱ ساختار جمعی و ضربی اعداد طبیعی

هدفمان در ادامه‌ی درس پرداختن به ساختار زیر است:

$$\mathfrak{N}_E = (\mathbb{N}, ۰, s, <, +, \cdot, \exp)$$

که در آن $\exp(x, y) = x^y$.

تمرین ۴۹. نشان دهید که در ساختارِ $(\mathbb{N}, +, \cdot)$ مجموعه‌ی تک‌عضویِ $\{۰\}$ و تابعِ s و رابطه‌ی $<$ و تابع $\exp$ همه قابل تعریف هستند (قسمت مربوط به تعریف تابع $\exp$ شاید نیاز به پیش بردن بیشتر درس داشته باشد).

بنا به تعریف بالا، آنچه در ساختارِ $\mathfrak{N}_E$ داریم همه در ساختارِ $(\mathbb{N}, +, \cdot)$ نیز رخ می‌دهد. با این حال، برای راحتی به کار گیری فرمولها، همچنان این نمادهای اضافه را در زبان نگه می‌داریم.

دقت کنید که اگر ساختار $\mathfrak{N}_E$ دارای یک تئوریِ تصمیم‌پذیر باشد، باید این تئوری بتواند درباره‌ی مفاهیم مهمی از جمله‌ی قضیه‌ی فرما تصمیم بگیرد: باید تئوری یادشده تصمیم بگیرد که چه معادلات دیوفانتی‌ای در اعداد طبیعی دارای جواب هستند و چه معادلاتی دارای جواب نیستند. هدف ما در ادامه‌ی درس پرداختن به قضیه‌ی زیر است:

قضیه ۸۱. هر تئوریِ کارائی که برای ساختارِ $\mathfrak{N}_E$ نوشته شود، ناکامل است. در واقع ساختار یادشده تصمیم‌پذیر نیست.

فعلاً یک تئوری طبیعی به نام T_E در نظر می‌گیریم و حکم بالا را، که قضیه‌ی ناتمامیت گودل نام دارد، درباره‌ی آن ثابت می‌کنیم. نشان خواهیم داد که هر چقدر هم که تئوری T_E را غنی کنیم، باز هم حکم بالا برقرار است.

تئوریِ T_E

مجموعه‌ی اصول زیر را T_E می‌نامیم:

۱. $\forall x \quad sx \neq ۰$

۲. $\forall x, y \quad (sx = sy \to x = y)$

۳. $\forall x, y \quad (x < sy \to x \leq y)$.

۴. $\forall x \quad x \not< ۰$

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

۶. $\forall x \quad x + ۰ = x$

۷. $\forall x, y \quad (x + sy = s(x + y))$.

۸. $\forall x \quad x \times ۰ = ۰$

۹. $\forall x, y \quad x \times sy = x \times y + x$

۱۰. $\forall x \quad x^۰ = s۰$

۱۱. $\forall x, y \quad (x^{sy} = x^y \times x)$

لم ۸۲. برای هر ترم بدون متغیر آزادِ t عدد طبیعیِ n موجود است به طوری که

$$T_E \vdash t = s^n ۰$$

اثبات. با استقراء روی ساخت ترم‌ها. اگر حکم برای ترمهای $t_۱, t_۲$ درست باشد، یعنی

$$T_E \vdash t_۱ = m_۱ \quad T_E \vdash t_۲ = m_۲$$

در این صورت،

$$T_E \vdash t_۱ + t_۲ = m + n$$

مشابه همین برای ترمهای شامل ضرب و توان نیز برقرار است. □

تمرین ۵۰.

۱. فرض کنید که τ یک جمله‌ی بدون سور باشد به طوری که $\mathfrak{N}_E \models \tau$. نشان دهید که در این صورت

$$T_E \vdash \tau.$$

۲. فرض کنید که τ یک جمله‌ی وجودی باشد به طوری که $\mathfrak{N}_E \models \tau$. نشان دهید که

$$T_E \vdash \tau.$$

بنا به تمرین بالا، اگر τ یک جمله‌ی وجودی باشد که در اعداد طبیعی درست است، این جمله توسط الگوریتمی که تئوریِ T_E و نتایج آن را را تولید می‌کند، تولید می‌شود. اما اگر جمله‌ی وجودیِ τ در مورد اعداد طبیعی درست نباشد، آن الگوریتم چه خواهد کرد؟ پیش از پاسخ دادن به این پرسش، کمی بیشتر مفهوم شهودی الگوریتم را در زیر کاویده‌ایم.

فصل ۲

ناتمامیت و بدرفتاریها

۱.۲ تِزِ چرچ

تزِ چرچ، یک قضیه‌ی شهودی است میان دو دسته ترمینولوژی زیر رابطه برقرار می‌کند:

دسته‌ی اول تصمیم‌پذیر، به طور کاراشمارش‌پذیر، محاسبه‌پذیر

دسته‌ی دوم بازگشتی، به طور بازگشتی شمارش‌پذیر، بازگشتی

دسته‌ی اول

فرض کنید که $A \subseteq \mathbb{N}^n$. می‌گوییم که A یک مجموعه‌ی **تصمیم‌پذیر** است، هرگاه یک الگوریتم (با هر تعریف شهودی‌ای که برای الگورتیم در نظر گرفته باشیم) موجود باشد به طوری که برای هر n تائیِ $(a_۱, \ldots, a_n) \in \mathbb{N}^n$ این الگوریتم مشخص کند که آیا $(a_۱, \ldots, a_n) \in A$ یا خیر. به بیان دیگر، الگوریتم ما چندتائی $(a_۱, \ldots, a_n)$ را می‌گیرد، اگر این چندتائی در مجموعه‌ی A باشد، پاسخ بله می‌دهد و اگر نباشد، پاسخ خیر می‌دهد. دقت کنید که تعداد الگوریتمهای رایانه‌ای شماراست و تعداد زیرمجموعه‌ی اعداد طبیعی ناشمارا، پس زیرمجموعه‌های زیادی از اعداد طبیعی وجود دارد که غیرتصمیم‌پذیر هستند.

مجموعه‌ی A را یک مجموعه‌ی **به طور کارا شمارش‌پذیر** می‌نامیم هرگاه الگوریتمی وجود داشته باشد که تمام اعضای A را به صورت یک لیست چاپ کند.

تمرین ۵۱. نشان دهید که اگر $A \subseteq \mathbb{N}^n$ تصمیم‌پذیر باشد، آنگاه به طور کارا شمارش‌پذیر است.

فرض کنید که A به طور کارا شمارش پذیر باشد و $(a_۱, \ldots, a_n)$ یک n تائی باشد. اگر این n تائی در مجموعه‌ی A باشد، آنگاه الگوریتمی که اعضای A را لیست می‌کند، پس از متناهی مرحله این عنصر را در لیست قرار می‌دهد. پس اگر A به طور کارا شمارش پذیر باشد، می‌توان الگوریتم را به گونه‌ای تنظیم کرد که برای هر عنصر $(a_۱, \ldots, a_n)$ اگر این عنصر در A باشد، الگوریتم بایستد و پاسخ بله بدهد. مشکل اینجاست که اگر ندانیم که عنصر مورد نظر در A نیست، شاید هر چه منتظر الگوریتم شویم بیهوده باشد؛ چون از پیش نمی‌دانیم که الگوریتم چه عناصری را چاپ نمی‌کند. در واقع الگوریتم مورد نظر را می‌توان با کمی تغییر به الگوریتمی تبدیل کرد که متوقف می‌شود اگروتنهااگر عنصر مورد نظر ما در A باشد.

تمرین ۵۲. نشان دهید که کلاس مجموعه‌های به طور کارا شمارش‌پذیر، از کلاس مجموعه‌های تصمیم‌پذیر بزرگتر است. به بیان دیگر، یک مجموعه‌ی به طور کارا شمارش‌پذیر معرفی کنید که تصمیم‌پذیر نباشد.

رابطه‌ی $R \subseteq \mathbb{N}^n$ را یک رابطه‌ی **محاسبه‌پذیر** می‌نامیم هرگاه به عنوان یک زیرمجموعه از $\mathbb{N}^n$ تصمیم‌پذیر باشد. پس رابطه‌ی R محاسبه‌پذیر است هرگاه الگوریتمی وجود داشته باشد که وقتی چندتائی $(a_1, \ldots, a_n)$ را بدان بدهیم، دقیقاً تعیین کند که آیا این چندتائی در رابطه‌ی R هست یا نه.

به طور مشابه، رابطه‌ی R را به طور کارا شمارش‌پذیر می‌نامیم هرگاه الگوریتمی وجود داشته باشد که تمام عناصری را که با هم در رابطه هستند، چاپ کند.

وقتی بحث به توابع کشانده می‌شود، موضوع پیچیدگی جذابی پیدا می‌کند: تابعِ $f : \mathbb{N}^n \to \mathbb{N}$ را یک تابع **محاسبه‌پذیر (یا تصمیم‌پذیر)** می‌نامیم هرگاه یک الگوریتم وجود داشته باشد که هرگاه عنصر $(a_1, \ldots, a_n)$ را به آن بدهیم، $f(a_1, \ldots, a_n)$ را به ما برگرداند. برای مثال، توابع جمع و ضرب، توابعی محاسبه‌پذیر هستند.

بنابراین هر مجموعه‌ی به طور کارا شمارش‌پذیر در واقع بُردِ یک تابع محاسبه‌پذیر است. همچنین نکته‌ی مهم (و کمی گیج‌کننده‌ی) تمرین زیر را داریم:

تمرین ۵۳. تابعِ f به عنوان یک تابع، محاسبه‌پذیر است اگروتنهااگر تابعِ f به عنوان یک رابطه، تصمیم‌پذیر باشد اگروتنهااگر تابعِ f به عنوان یک رابطه، به طور کارا شمارش‌پذیر باشد.

دسته‌ی دوم

رابطه‌ی $R \subseteq \mathbb{N}^n$ را **بازگشتی** می‌نامیم هرگاه **قابل نمایش** در یک تئوری متناهی (یعنی دارای متناهی جمله) سازگار برای اعداد طبیعی در زبانی شامل $\{0, s\}$ باشد؛ به بیان دیگر، هر گاه یک تئوری متناهیِ سازگارِ T به همراه یک فرمولِ $\phi(x_1, \ldots, x_n)$ داشته باشیم به طوری که برای هر $(a_1, \ldots, a_n) \in \mathbb{N}^n$

۱. یا $T \vdash \phi(s^{a_1}0, \ldots, s^{a_n}0)$ یا $T \vdash \neg\phi(s^{a_1}0, \ldots, s^{a_n}0)$.

۲. $R(a_1, \ldots, a_n)$ برقرار است اگروتنهااگر $T \vdash \phi(s^{a_1}0, \ldots, s^{a_n}0)$.

رابطه‌ی R را **به طور بازگشتی شمارش‌پذیر** می‌نامیم هرگاه به صورت زیر باشد:

$$R = \{\bar{a} | \exists b \quad (\bar{a}, b) \in Q\}$$

که در آن Q یک رابطه‌ی بازگشتی است.

تمرین ۵۴. نمایش‌پذیر بودن یک رابطه با قابل‌تعریف‌بودن آن چه فرقی دارد؟

تزچرچ

تز چرچ یک قضیه‌ی دقیق ریاضی نیست. بنا به تز چرچ مفهوم شهودیِ تصمیم‌پذیری معادل با مفهوم قابل تعریف بازگشتی بودن در بالاست.

اثبات این که یک رابطه‌ی بازگشتی، تصمیم‌پذیر است ساده است؛ (چرا؟) اما اثبات این که تصمیم‌پذیر بودن همان بازگشتی بودن است، تقریباً بی‌معنی است. با این حال، برای مدلهای آشنای تصمیم‌پذیری، مثلاً ماشین‌های تورینگ، اثبات این گفته آسان

است. **به این مطالب در بخش دیگری از درس دوباره باز خواهیم گشت. فعلاً، تز چرچ را درست فرض می‌کنیم. در ادامه‌ی درس توجه‌مان را به تئوریِ T_E معطوف کرده‌ایم.**

ادامه‌ی درس در تئوری T_E

تعریف ۸۳. فرمولِ $\phi(x_1,\ldots,x_m)$ توسط تئوریِ T_E **در اعداد طبیعی معین می‌شود** هرگاه برای هر m تائیِ $(a_1,\ldots,a_m)\in\mathbb{N}^m$ یا $T_E\vdash\phi(s^{a_1}0,\ldots,s^{a_m}0)$ یا $T_E\vdash\neg\phi(s^{a_1}0,\ldots,s^{a_m}0)$.

قضیه ۸۴.

۱. فرمولهای اتمی توسط T_E در اعداد طبیعی معین می‌شوند.

۲. اگر ϕ و ψ در اعداد طبیعی معین شوند، فرمولهای $\neg\phi$ و $\phi\to\psi$ نیز در اعداد طبیعی معین می‌شوند.

۳. اگر ϕ در اعداد طبیعی معین باشد، آنگاه فرمولهای زیر نیز در اعداد طبیعی معین هستند:

$$\forall x\quad (x<y\to\phi)$$

$$\exists x\quad (x<y\wedge\phi)$$

تعریف ۸۵. فرض کنید $f:\mathbb{N}^m\to\mathbb{N}$ یک تابع باشد. می‌گوئیم فرمولِ $\phi(x_1,\ldots,x_{m+1})$ نماینده‌ی تابعِ f (به صورت تابعی و نه به صورت رابطه‌ای) است هرگاه برای هر $a_1,\ldots,a_m\in\mathbb{N}$ داشته باشیم

$$T_E\vdash\forall x_{m+1}\big(\phi(s^{a_1}0,\ldots,s^{a_m}0,x_{m+1})\leftrightarrow x_{m+1}=s^{f(a_1,\ldots,a_m)}0\big)$$

به راحتی می‌توان دید که توابعی که توسط ترمهای زبان به دست می‌آیند، قابل نمایش توسط فرمولها هستند؛ به طور خاص:

لم ۸۶.

- تابع تالی (روی اعداد طبیعی) قابل نمایش توسط یک فرمول است.
- هر تابع ثابت (روی اعداد طبیعی) قابل نمایش توسط یک فرمول است.
- توابع، تصویر، یعنی توابع زیر قابل نمایش هستند:

$$f(a_1,\ldots,a_m)=a_i$$

- توابع جمع و ضرب و توان، قابل نمایش هستند.
- اگر g یک تابع n موضعی قابل نمایش باشد و $h_1,\ldots,h_n$ توابع m موضعی قابل نمایش باشند، آنگاه $f=g(h_1,\ldots,h_n)$ قابل نمایش است.

• فرض کنید که تابعِ $m+۱$ موضعی g قابل نمایش باشد و داشته باشیم

$$\forall a_۱,\ldots,a_m \quad \exists b \quad g(a_۱,\ldots,a_m,b)=۰$$

در این صورت تابعِ m موضعی f که به صورت زیر تعریف می‌شود، قابل نمایش است:

$$f(a_۱,\ldots,a_m)=\min\{b|g(a_۱,\ldots,a_m,b)=۰\}.$$

(تابع f را به صورت

$$f(\bar{a})=\mu b[g(\bar{a},b)=۰]$$

نشان می‌دهیم).

۲.۲ لمهای لازم برای نمایش‌پذیری کُدهای دنباله‌ها

۱. هر رابطه‌ای که در $\mathfrak{N}_E$ بدون سور قابل تعریف باشد، قابل نمایش است. کلاس روابط نمایش‌پذیر تحت اجتماع و اشتراک و متمم‌گیری بسته است. اگر R قابل نمایش باشد، دو رابطه‌ی زیر نیز قابل نمایش هستند:

$$\{(\bar{a},b)|\forall c<b \quad (\bar{a},c)\in R\}$$

$$\{(\bar{a},b)|\exists c<b \quad (\bar{a},c)\in R\}.$$

۲. رابطه‌ی R قابل نمایش است اگروتنها اگر تابع مشخصه‌ی آن قابل نمایش باشد.

۳. اگر رابطه‌ی R قابل نمایش باشد و f,g دو تابع قابل نمایش باشند، آنگاه رابطه‌ی زیر قابل نمایش است:

$$\{\bar{a}|(f(\bar{a}),g(\bar{a}))\in R\}.$$

۴. اگر R قابل نمایش باشد، رابطه‌ی زیر قابل نمایش است:

$$\{(a,b)|\exists c\leq b \quad (a,c)\in R\}.$$

۵. رابطه‌ی عاد کردن، یعنی رابطه‌ی زیر، قابل نمایش است:

$$R=\{(a,b):a|b\}$$

۶. مجموعه‌ی اعداد اول قابل نمایش است.

۷. مجموعه‌ی جفتهای مجاور اول، قابل نمایش است. (زوج (a,b) را یک جفت مجاور اول می‌نامیم هرگاه $a<b$ اول باشند و بین a,b هیچ عدد اولی وجود نداشته باشد).

۸. تابعی که a را به $n+۱$ اُمین عدد اول می‌برد قابل نمایش است. $a+۱$ امین عدد اول را با p_a نشان می‌دهیم. پس $p_۰=۲, p_۱=۳,\ldots$.

اثبات. نخست نیاز به یک مشاهده‌ی نظریه‌ی اعدادی داریم. دقت کنید که $p_a = b$ اگروتنهااگر b یک عدد اول باشد و هرگاه که حاصلضربی به صورت زیر بنویسیم:

$$۲^k \times \ldots \times \text{عدد اول قبل از آن}^{a-۲} \times \text{عدد اول قبلی}^{a-۱} \times p^a$$

آنگاه توان ۲ در این حاصلضرب برابر با صفر باشد. برای یافتن فرمول مربوطه به صورت زیر عمل می‌کنیم:

فرض کنید که $p_a = b$. در این صورت عدد $c = ۲^۰۳^۱ \ldots b^a$ دارای ویژگی‌های زیر است:

(آ) $c < b^{a^۲}$.

(ب) $b^a | p$ و $b^{a+۱} \not| c$.

(ج) اگر r یک عدد اول باشد به طوری $r \leq b$ و q عدد اول قبل از r باشد، در این صورت

$$q^j | c \Leftrightarrow r^{j+۱} | c.$$

(د) $۲ \not| c$.

از طرفی اگر یک عدد c وجود داشته باشد که شرطهای سه‌گانه‌ی بالا را برآورده کند، آن عدد به صورت زیر است:

$$c = (۲^۰۳^۱ \ldots b^a) \times \text{توانهائی از برخی اعداد اول بزرگتر}$$

یعنی توان b در آن برابر با a است. پس b برابر با $a + ۱$ امین عدد اول است.

بنا بر آنچه گفته شد، $p_a = b$ اگروتنهااگر عدد c با شرایط بالا وجود داشته باشد؛ و این شرایط قابل نوشتن در یک زبان مرتبه‌ی اول هستند.

□

۹. برای هر m، تابعی که $(a_۰, \ldots, a_m)$ را به $\langle a_۰, \ldots, a_m \rangle$ می‌برد قابل نمایش است، که در آن

$$\langle a_۰, \ldots, a_m \rangle = \prod_{i \leq m} p_i^{a_i + ۱}$$

اثبات. داریم $f(a_۱, \ldots, a_n) = b$ هرگاه b برابر با حاصلضرب اعداد اول $a_{i+۱}$ ام باشد. یافتن این اعداد اول بنا به قسمت قبل ممکن است. □

۱۰. تابعی که کدها را می‌شکند قابل نمایش است:

$$((\langle a_۱, \ldots, a_m \rangle), b) \stackrel{f}{\mapsto} a_b \quad b \leq m$$

تابع بالا را برای راحتی، به صورت $(\langle \bar{a} \rangle)_b$ نشان می‌دهیم.

اثبات. $f(x, b)$ برابر است با توانی از عدد اول $b + ۱$ ام که x را عاد می‌کند؛ یعنی اولین جائی که توان بعد از آن x را عاد نکند. □

۱۱. مجموعه‌ی همه‌ی کدهای دنباله‌ها، یعنی مجموعه‌ی زیر، قابل نمایش است:

$$A = \{\langle a_{۰}, \dots, a_m\rangle | m \geq -۱\}$$

که در آن تعریف کرده‌ایم:

$$\langle\rangle = ۱.$$

اثبات. $x \in A$ اگروتنهااگر x کد یک دنباله باشد؛ یعنی اعداد اول کمتر از x و توانهائی از آنها موجود باشند که حاصلضربشان برابر با x شود. □

۱۲. تابع محدود کننده‌ی کدها، قابل نمایش است:

$$(\langle a_{۰}, \dots, a_m\rangle, b) \mapsto \langle a_{۰}, \dots, a_{b-۱}\rangle \quad b \leq m + ۱$$

اثبات. $f(\langle \bar{a}\rangle, b)$ برابر است با کوچکترین عدد n که دارای ویژگی زیر است: هر توانی از اعداد اول کوچکتر از p_b عدد $\langle a\rangle$ را عاد می‌کند اگروتنهااگر n را عاد می‌کند. □

۱۳. تابعی که طول کدها را می‌دهد قابل نمایش است:

$$\mathrm{lh}(\langle a_{۰}, \dots, a_m\rangle) = m + ۱.$$

اثبات. $f(\langle \bar{a}\rangle) = m$ اگروتنهااگر تا عدد اول m ام $\langle \bar{a}\rangle$ را عاد کند و اعداد اول p_b برای $b > m$ عدد m را عاد نکنند. □

۱۴. (توابع بازگشتی اولیه) فرض کنید که f یک تابعِ $k + ۱$ موضعی باشد. تابع $\bar{f}$ را به صورت زیر تعریف کنید:

$$\bar{f}(a, \bar{b}) = \langle f(۰, \bar{b}), \dots, f(a - ۱, \bar{b})\rangle$$

حال فرض کنید که g یک تابعِ $k + ۲$ موضعی باشد. در این صورت تابعِ یکتای f موجود است به طوری که

$$f(a, \bar{b}) = g(\bar{f}(a, \bar{b}), a, \bar{b}).$$

قضیه ۸۷. اگر تابعِ g قابل نمایش باشد، آنگاه تابع f که به صورت زیر تعریف می‌شود، قابل نمایش است:

$$f(a, \bar{b}) = g(\bar{f}(a, \bar{b}), a, \bar{b}).$$

اثبات. اولاً تابعِ $\bar{f}$ قابل نمایش است؛ زیرا $\bar{f}(a, b)$ برابر است با کوچکترین عدد s که s کد یک دنباله به طول a است به طوری که هر درایه‌ی $i < a$ آن به صورت $(s)_i = g(s \restriction i, a, \bar{b})$ است. پس تابع f قابل نمایش است زیرا

$$f(a, \bar{b}) = g(\bar{f}(a, \bar{b}), a, \bar{b}).$$

□

تمرین ۵۵ (بازگشت اولیه). فرض کنید که g, h توابعی نمایش‌پذیر باشند و تابع f به صورت زیر باشد:

$$f(a,b) = g(b)$$

$$f(a+۱,b) = h(f(a,b),a,b)$$

در این صورت نشان دهید که تابع f نیز نمایش‌پذیر است.

۱۵. اگر F یک تابع قابل نمایش باشد، آنگاه توابع زیر قابل نمایش هستند:

$$(a,\bar{b}) \mapsto \prod_{i<a} F(i,\bar{b}).$$

$$(a,\bar{b}) \mapsto \sum_{i<a} F(i,\bar{b}).$$

اثبات. اگر تابع بالا را G بنامیم داریم

$$G(۰,\bar{b}) = ۱$$

$$G(a+۱,\bar{b}) = F(a,\bar{b}) \times G(a,b)$$

□

۱۶. تابعی که کدها را به هم می‌چسباند، قابل نمایش است:

$$\langle a_۱,\ldots,a_m\rangle * \langle b_۱,\ldots,b_n\rangle = \langle a_۱,\ldots,a_m,b_۱,\ldots,b_n\rangle.$$

۱۷. تعریف کنید:

$$\circledast_{i<a} f(i) = f(۰) * \ldots * f(a-۱).$$

اگر F قابل نمایش باشد، آنگاه تابع زیر قابل نمایش است:

$$(a,\bar{b}) \mapsto \circledast_{i<a} F(i,\bar{b}).$$

۳.۲ کدهای گودل

هدفمان در ادامه‌ی درس اثبات این است که مجموعه‌ی همه‌ی فرمولهای اثبات‌پذیر، قابل نمایش است. برای اثبات این گفته، باید نشان دهیم که تمامی اصول منطقی و دنباله‌های متناهی اثبات، قابل نمایش هستند.

در این قسمت اثبات‌پذیری را بر اساس سیستم هیلبرتی در نظر گرفته‌ام.

سیستم هیلبرت برای استنتاج، به صورت زیر تعریف می‌شود:

یک استنتاج برای فرمولِ ϕ از Γ دنباله‌ی متناهی به صورت $\langle\alpha_۰,\ldots,\alpha_n\rangle$ است که هر α_i یا یکی از اصول منطقی (در زیر) است یا توسط MP از دو فرمول قبل از خود به دست آمده است. منظور از به دست آمدن با استفاده از MP این است که در صورتی که $\phi \to \psi$ و ϕ استنتاج شده باشند، ψ نیز استنتاج می‌شود.

اصول منطقی در دستگاه هیلبرت به صورت زیر هستند:

- نتایجی که از تاتولوژیهای منطق گزاره‌ها حاصل می‌شوند.

- در صورتی که x در α نسبت به t آزاد باشد: $\forall x \alpha \to \alpha(t/x)$.

دقت کنید که زمانی x در α نسبت به ترم t آزاد است که هیچ حضوری از x در α تحت تأثیر هیچ سوری نباشد که متغیرهای t را در بردارد. مثلاً در فرمول زیر، x نسبت به $t = y$ آزاد نیست

$$\exists y \quad (y \neq x)$$

دقت کنید که از فرمول زیر:

$$\forall x \quad \exists y \quad y \neq x$$

نتیجه نمی‌شود که

$$\exists y \quad y \neq y.$$

- $\forall x(\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta)$

- در صورتی که x در α آزاد نباشد: $\alpha \to \forall x \alpha$

به نمادها کدهای زیر را اختصاص دهید:

(۱	$\forall$ ۰
) ۳	۰ ۲
$\neg$ ۵	s ۴
$\to$ ۷	$<$ ۶
$=$	$+$ ۸
v_1 ۱۱	$\cdot$ ۱۰
v_2 ۱۳	E ۱۲

در جدول بالا، کدهای متغیرها به همان روال ادامه می‌یابد. اگر $\epsilon = s_0 \ldots s_n$ یک عبارت منطقی باشد (مثلاً یک ترم)، کد گودل آن را به صورت زیر تعریف می‌کنیم:

$$\sharp(\epsilon) = \sharp(s_1, \ldots, s_n) = \langle h(s_0), \ldots, h(s_n) \rangle$$

که در آن h تابعی است که هر علامت را به کد آن (مطابق جدول بالا) می‌برد.

اگر Φ یک مجموعه از عبارات باشد آنگاه تعریف می‌کنیم:

$$\sharp\Phi = \{\sharp(\epsilon) : \epsilon \in \Phi\}$$

اگر $(\alpha_0, \ldots, \alpha_n)$ یک دنباله از عبارات باشد، مثلاً یک استنتاج باشد، به آن کد زیر را نسبت می‌دهیم:

$$\mathfrak{F}(\alpha_0, \ldots, \alpha_n) = \langle \sharp\alpha_0, \ldots, \sharp\alpha_n \rangle$$

موارد زیر برقرارند:

۱. مجموعه‌ی کدهای گودل تمامی متغیرها قابل نمایش است.

اثبات. مجموعه‌ی یادشده به صورت زیر است:

$$\{a : \exists b < a \quad a = \langle ۱۱ + ۲b \rangle\}.$$

$\square$

۲. مجموعه‌ی متشکل از کدهای گودل تمامی ترمها، قابل نمایش است.

اثبات. فرض کنید که f تابع مشخصه‌ی مجموعه‌ی همه‌ی ترمها باشد. در این صورت، $f(a)$ برابر با یک است اگروتنهااگر a کد گودل یک متغیر باشد، یا اتفاق زیر رخ دهد:

اعداد $i, k < a$ وجود داشته باشند به طوری که i کد یک دنباله به صورت $\langle \ldots \rangle$ باشد به طوری که برای هر $j < \mathrm{lh}(i)$ داشته باشیم ۱ $f((i)_j) =$؛ و k کد جدولیِ یک نماد تابعی به‌اندازه‌ی‌طولِ iموضعی (در زبان) باشد و

$$a = \langle k \rangle \star \circledast_{j < \mathrm{lh}\, i} (i)_j$$

در غیرِ دو صورت بالا، ۰ $f(a) =$. اما دقت کنید که $f(a) = g(\bar{f}(a), a))$ که در آن تابع $g(s, a)$ به گونه‌ای تعریف می‌شود که $g(s, a)$ در دو صورت زیر برابر یک است و در غیر این دو صورت برابر با صفر است.

صورت اول. اگر a کُدِ گودل یک متغیر باشد.

صورت دوم. اعداد $i, k < a$ وجود داشته باشند به طوری که i یک کد یک دنباله باشد و برای هر j که از طول i کمتر است داشته باشیم ۱ $(s)_{(i)_j} =$ و k کد جدولی یک تابع i متغیره باشد و

$$a = \langle k \rangle * \circledast_{j < \mathrm{lh}\, i} (i)_j$$

$\square$

۳. مجموعه‌ی کدهای گودل فرمولهای اتمی قابل نمایش است.

۴. مجموعه‌ی کُدهای گودلِ تمامی فرمولها قابل نمایش است.

۵. یک تابع قابل نمایشِ sb موجود است به طوری که برای هر فرمول α و متغیر x و ترم t داریم

$$sb(\sharp\alpha, \sharp x, \sharp t) = \sharp\alpha(t/x).$$

۶. تابع زیر قابل نمایش است:

$$n \mapsto \sharp(s^n ۰)$$

۷. یک رابطه‌ی قابل نمایشِ Fr موجود است به طوری که

$\langle \sharp\alpha, \sharp x \rangle \in Fr \Leftrightarrow$ متغیرِ x در فرمولِ α به صورت آزاد ظاهر شود.

۸. مجموعه‌ی کدهای گودل جمله‌ها قابل نمایش است.

۹. یک رابطه‌ی قابل نمایشِ sbl وجود دارد به طوری که

$$\langle\sharp\alpha, \sharp x, \sharp t\rangle \in sbl \Leftrightarrow$$ متغیرِ x در فرمولِ α نسبت به ترم t آزاد باشد.

۱۰. رابطه‌ی زیر قابل نمایش است:

$$(a,b) \in G \Leftrightarrow$$ a کد گودل یک فرمولِ ϕ و b کد گودل یک فرمول به صورت $\forall\bar{x}\phi$ است.

۱۱. مجموعه‌ی کدهای گودل تمامی تاتولوژی‌ها قابل نمایش است. (اثبات این گفته نیاز به اثبات تصمیم‌پذیر بودن تمامی جداول صفر و یکی دارد).

۱۲. مجموعه‌ی کدهای گودل فرمولهای به صورتِ $\forall x(\alpha \to \beta) \to (\forall x\alpha \to \forall x\beta)$ قابل نمایش است.

۱۳. مجموعه‌ی کدهای گودل فرمولهای به صورت $\forall x\alpha \to \alpha(t/x)$ وقتی x در α آزاد نباشد، قابل نمایش است.

۱۴. مورد بالا در مورد فرمولهای به صورت $\alpha \to \forall x\alpha$ که در آن x در α آزاد نیست، برقرار است.

۱۵. مجموعه‌ی کدهای گودل تمامی اصول منطقی (دستگاه هیلبرت)قابل نمایش است.

۱۶. اگر A یک مجموعه‌ی متناهی از فرمولها باشد آنگاه مجموعه‌ی

$$\{\mathcal{F}(D):$$ D یک استنتاجِ منطقیِ از A است $\}$

قابل نمایش است. در بالا، D یک دنباله است که با روشهای استنتاج به دست آمده است و ما را به اثبات فرمولی در انتهای دنباله می‌رساند.

۱۷. هر رابطه‌ی بازگشتی قابل نمایش در T_E است.

اثبات. اگر R بازگشتی باشد، یک تئوریِ متناهی A وجود دارد که R در آن توسط یک فرمول ϕ قابل نمایش است. قرار دهید

$$H = \{\mathcal{F}(D)|$$ D یک استنتاج منطقی از A است. $\}$

فرض کنید a یک عدد طبیعی باشد. نخست تابع زیر را در نظر بگیرید:

$$f(a) = \min\{d | d \in H,$$ آخرین بخشِ d یا $\phi(a)$ یا $\neg\phi(a)$ است. $\}$

داریم

$$a \in R \Leftrightarrow$$ آخرین قسمتِ $f(a)$ برابر با $\phi(a)$ باشد.

□

نتیجه ۸۸. یک رابطه‌ی R بازگشتی است اگروتنهااگر قابل نمایش در T_E باشد.

نتیجه ۸۹. هر رابطه‌ی بازگشتی در $\mathfrak{N}_E$ قابل تعریف است.

۱۸. اگر $\sharp A$ بازگشتی باشد و $cn(A)$ یک تئوری کامل باشد، آنگاه $\sharp cn(A)$ بازگشتی است. منظور از $cn(A)$ تئوری کامل متشکل از تمامی جمله‌هائی است که با شروع از A اثبات می‌شوند.

قضیه ۹۰ (لم نقطه‌ی ثابت). برای هر فرمولِ β که تنها متغیر آزادِ آن $v_۱$ است، می‌توان یک جمله‌ی σ چنان یافت که

$$T_E \vdash \big(\sigma \leftrightarrow \beta(\sharp\sigma)\big).$$

اثبات. فرمولی را که کد آن برابر با v است با ϕ_v نشان دهید. تابع زیر یک تابع نمایش‌پذیر است:

$$v_۳ = \sharp(\phi_{v_۱}(v_۲)).$$

حال فرمول زیر را در نظر بگیرید:

$$\forall v_۳ \quad \big(v_۳ = \sharp(\phi_{v_۱}(v_۱)) \to \beta(v_۳)\big)$$

فرض کنید کد فرمول بالا برابر با q باشد. قرار دهید $\sigma = \phi_q(q)$. □

تمرین ۵۶. نشان دهید که فرمول σ شرط خواسته شده در قضیه را برآورده می‌کند.

نتیجه ۹۱ (عدم تعریف‌پذیری تارسکی). مجموعه‌ی $\sharp Th(\mathfrak{N}_E)$ (یعنی مجموعه‌ی متشکل از کدهای همه‌ی فرمولهای درست در اعداد طبیعی) قابل تعریف در $\mathfrak{N}_E$ نیست.

اثبات. فرض کنید فرمول β مجموعه‌ی یادشده را تعریف کند. قضیه‌ی قبل را به فرمولِ $\neg\beta$ اعمال کنید.

به بیان دقیق‌تر، بنا به قضیه‌ی تارسکی، یک جمله‌ی σ وجود دارد به طوری که

$$T_E \vdash \sigma \leftrightarrow \neg\beta(\sharp(\sigma)).$$

جمله‌ی بالا بیانگر این است که از نظر T_E جمله‌ی σ زمانی درست است که در $\mathbb{N}_E$ درست نباشد.

حال اگر $\sharp\sigma \in \sharp Th(\mathbb{N}_E)$ در این صورت $\beta(\sharp\sigma)$ برقرار است و بنابراین $T_E \vdash \neg\sigma$ پس $\mathfrak{N}_E \vdash \neg\sigma$؛ و این تناقض است.

اگر $\sharp\sigma \not\in \sharp Th(\mathbb{N}_E)$ در این صورت $\neg\beta(\sharp\sigma)$ برقرار است پس $T_E \vdash \sigma$ پس $\mathfrak{N}_E \models \sigma$؛ و این تناقض است. □

نتیجه ۹۲. $\sharp Th(\mathfrak{N}_E)$ بازگشتی نیست.

نتیجه ۹۳ (قضیه‌ی ناتمامیت اول گودل). اگر $A \subseteq Th(\mathfrak{N}_E)$ و $\sharp A$ بازگشتی باشد، آنگاه $cn(A)$ یک تئوری ناکامل است.

اثبات قضیه‌ی ناتمامیت را می‌توان به صورت زیر نیز نگاه کرد. فرض کنید $A \subseteq Th(\mathfrak{N}_E)$ یک مجموعه‌ی بازگشتی باشد. در این صورت، $cn(A)$، یعنی مجموعه‌ی همه‌ی نتایجِ A، یک مجموعه‌ی بازگشتی است و از این رو توسط یک فرمولِ β تعریف می‌شود. برای فرمولِ $\neg\beta$ یک جمله‌ی σ وجود دارد به طوری که

$$T_E \vdash \sigma \leftrightarrow \neg\beta(\sharp\sigma).$$

جمله‌ی بالا بیانگر این است که σ در $cn(A)$ است اگروتنهااگر در آن نباشد!

نتیجه ۹۴ (بدون اثبات). اگر T یک تئوری سازگار با T_E باشد، آنگاه T بازگشتی نیست.

۴.۲ ناتمامیت اول و مسئله‌ی توقف

۵.۲ ناتمامیت دوم و نظریه‌ی مجموعه‌ها

اصول نظریه‌ی مجموعه‌ها در زبانِ $L = \{\in\}$ نوشته می‌شوند آنها را با st نشان می‌دهیم. در اینجا st را همان اصول زرملو فرانکل برای نظریه‌ی مجموعه‌ها گرفته‌ام. از اصول نظریه‌ی مجموعه‌ها نتیجه می‌شود که کوچکترین مجموعه‌ی استقرائی وجود دارد. این مجموعه را مجموعه‌ی اعداد طبیعی می‌نامیم. روی مجموعه‌ی اعداد طبیعی می‌توان جمع و ضرب و توان را به صورت استقرائی تعریف کرد. بنابراین در صورتی که اصول نظریه‌ی مجموعه‌ها سازگار باشند؛ یعنی در صورتی که جهانی برای مجموعه‌ها وجود داشته باشد، در آن جهان اعداد طبیعی نیز وجود دارند. پس با فرض سازگاری نظریه‌ی مجموعه‌ها، یک کپی (تعریف‌پذیر) از $\mathbb{N}$ و توابع آن در نظریه‌ی مجموعه‌ها وجود دارد. به بیان دیگر، حساب در نظریه‌ی مجموعه‌ها تعبیر می‌شود.

قضیه ۹۵. فرض کنید T یک تئوری در زبان نظریه‌ی مجموعه‌ها باشد، به طوری که $T \cup st$ سازگار است. در این صورت $\sharp T$ بازگشتی نیست.

نتیجه ۹۶. اگر st سازگار باشد، کامل نیست.

فرض کنید که D رابطه‌ی سه‌تائی زیر روی اعداد طبیعی باشد:

a کد گودل یک فرمولِ α در نظریه‌ی اعداد باشد و c کد گودل یک استنتاج برای $\alpha(b)$ در st باشد. $\Leftrightarrow$ $(a, b, c) \in D$

رابطه‌ی D یک رابطه‌ی بازگشتی است، پس با یک فرمول داده می‌شود. برای راحتی، این رابطه را با فرمولی که نمایش‌دهنده‌ی آن است یکسان فرض می‌کنیم. فرض کنید کُدگودلِ فرمول زیر، r باشد:

$$\forall v_۳ \quad \neg D(v_۱, v_۱, v_۳)$$

فرمول بالا بیانگر این است که هیچ اثباتی برای فرمول $\phi_{v_۱}(v_۱)$ وجود ندارد.

فرمول زیر را در نظر بگیرید:

$$\sigma : \forall v_۳ \quad \neg D(r, r, v_۳).$$

فرمول بالا بیانگر این است که اثباتی برای فرمول $\phi_r(r)$ وجود ندارد. یعنی فرمول σ بیانگر این است که اثباتی برای فرمول σ وجود ندارد. همچنین بنا به تعریف فرمولِ $\phi_r(r)$ فرمول σ بیانگر این است که اثباتی برای این که اثباتی برای $\phi_r(r)$ وجود ندارد، وجود ندارد.

ادعا. اگر st سازگار باشد، آنگاه $st \nvdash \sigma$.

تمرین ۵۷. ادعای بالا را ثابت کنید.

فرض کنید $cons(st)$ فرمولی باشد که می‌گوید اثباتی برای تناقض (مثلا برای فرمول $x \neq x$ وجود ندارد).

قضیه ۹۷ (ناتمامیت دوم گودل). $cons(st)$ در st ثابت نمی‌شود؛ مگر این که st ناساگاز باشد.

اثبات. بنا به لم قبل $cons(st) \to \sigma$ در st اثبات می‌شود (زیرا σ جمله‌ای است که می‌گوید که σ ثابت نمی‌شود!). پس اگر $cons(st)$ اثبات شود، آنگاه σ ثابت می‌شود. □

فصل ۳

میدانهای بسته‌ی حقیقی، مصداقی از یک تئوری کامل خوشرفتار

در این بخش به خوش‌رفتاری تئوری جبری میدان اعداد حقیقی خواهم پرداخت. نشان خواهم داد که بر خلافِ $(\mathbb{N}, +, \cdot)$ که در بخش قبل مورد مطالعه قرار گرفت، ساختار $(\mathbb{R}, +, \cdot)$ را می‌توان به صورت بازگشتی و به صورت کامل اصل‌بندی کرد. بنابراین الگوریتمی وجود دارد که هر قضیه‌ی در مورد اعداد حقیقی را تولید می‌کند. نخست همه‌ی پیشنیازهای جبری درس را خواهم گفت و سپس به بررسی‌های مدل‌تئورتیک خواهم پرداخت.

تعریف ۹۸. میدان K را یک میدان حقیقی می‌نامیم هرگاه $-1 \in K$ را نتوان به صورت یک مجموع متناهی از مربعات نوشت.

به‌طور خاص اگر K یک میدان مرتب باشد آن‌گاه K حقیقی است؛ زیرا در یک میدان مرتب، هر عنصر مربع نامنفی است.

لم ۹۹. اگر F حقیقی باشد و $a \in F$ عنصری ناصفر باشد، دراین‌صورت حداکثر یکی از a یا $-a$ مجموع مربعات است. (یعنی هر دو نمی‌توانند مجموع مربعات باشند؛ شاید هیچ‌یک مجموع مربعات نباشند).

اثبات. فرض کنید a و b دو عنصر دلخواه باشند. اگر هر دو مجموع مربعات باشند در این‌صورت $\frac{a}{b}$ نیز مجموع مربعات است:

$$\frac{a}{b} = \frac{ab}{b^2} = \frac{(\sum c_i^2)(\sum d_i^2)}{b^2}$$

بنابراین اگر a و $-a$ هر دو مجموع مربعات باشند، آن‌گاه -1 مجموع مربعات خواهد بود. □

لم ۱۰۰. فرض کنید F حقیقی باشد و $-a$ مجموع مربعات نباشد، در این‌صورت $F(\sqrt{a})$ یک میدان حقیقی است. (منظور از $F(\sqrt{a})$ توسیع جبری میدانِ F توسط یک ریشه‌ی دوم برای عنصر a است. دقت کنید که این ریشه‌ی دوم در خودِ میدانِ F نیست.)

اثبات. توجه کنید که

$$F(\sqrt{a}) = \{c + d\sqrt{a} | c, d \in F\}.$$

فرض کنید در $F(\sqrt{a})$ عدد -1 مجموع مربعات شود؛ دراین صورت داریم:

$$(\sum c_i + d_i\sqrt{a})^2 = -1$$

$$\sum c_i^۲ + d_i^۲ a + ۲c_i d_i \sqrt{a} + ۱ = ۰$$

توجه کنید که $\sqrt{a}$ و ۱ پایه‌های $F(\sqrt{a})$ روی F (به عنوان یک فضای برداری) هستند. رابطه‌ی بالا به صورت زیر قابل تبدیل است:

$$\sqrt{a}(\sum ۲c_i d_i) + ۱(\sum c_i^۲ + d_i^۲ a + ۲c_i d_i^۲ a + ۱) = ۰$$

ضریب ۱ در بالا باید صفر شود. پس -۱ مجموع مربعات است. $\square$

لم ۱۰۱. فرض کنید F حقیقی باشد و $f(x) \in F[X]$ یک چندجمله‌ای تحویل‌ناپذیر با درجه‌ی فرد باشد و α ریشه‌ی f در یک توسیع میدانی باشد و $\alpha \notin F$. در این صورت $F(\alpha)$ حقیقی است.

اثبات. اگر $F(\alpha)$ حقیقی نباشد آنگاه -۱ در این میدان مجموع مربعات است؛ یعنی چندجمله‌ایهای g_i با درجه‌ی کمتر از n موجودند به طوری که:

$$\sum g_i^۲(\alpha) = -۱$$

از آنجا که $F(\alpha) = F[X]/\langle f\rangle$ عبارت بالا در میدان $F[X]/\langle f\rangle$ به معنی وجود یک چندجمله‌ای q است که در شرط زیر صدق می‌کند:

$$\sum g_i^۲(x) + f(x)q(x) = -۱$$

درجه‌ی q فرد و کمتر از درجه f است.

فرض کنید β یک ریشه از $q(x)$ باشد. بنابه فرض استقرا (استقراء روی درجه‌ی f) $F(\beta)$ حقیقی است. اما داریم

$$\sum g_i^۲(\beta) + f(\beta)q(\beta) = -۱$$

یعنی در میدان $F(\beta)$ داریم: $\sum g_i^۲(\beta) = -۱$ که تناقض با فرض استقرا است. $\square$

توجه ۱۰۲. فرض کنید $f \in F[X]$ یک چندجمله‌ای تحویل ناپذیر باشد. در این‌صورت $F(\alpha) \cong \frac{F[X]}{\langle f\rangle}$ که در آن $F(\alpha)$ میدان تولید شده توسط F و ریشه‌ی f است. از طرفی دیگر

$$F(\alpha) = \{g(\alpha) | \deg g < \deg f, g \in F[X]\}.$$

تعریف ۱۰۳. میدان R را **بسته‌ی حقیقی** می‌نامیم هرگاه R حقیقی باشد، اما هیچ توسیع جبری حقیقی نداشته باشد.

بنابراین اگر R بسته‌ی حقیقی باشد، در هر توسیع جبری از آن، -۱ مجموع مربعات است. (بعداً نشان خواهیم داد که اگر R بسته‌ی حقیقی باشد، تنها یک توسیع جبری دارد و آن $R(\sqrt{-۱})$ است. این توسیع جبری، یک میدانِ بسته‌ی جبری است).

اگر R بسته‌ی حقیقی باشد و $-a$ مجموع مربعات نباشد، در این صورت $F(\sqrt{a})$ یک توسیع جبری حقیقی از F است که بنا به بسته‌ی حقیقی بودن داریم $F(\sqrt{a}) = F$. یعنی اگر R بسته‌ی حقیقی باشد و $-a$ مجموع مربعات نباشد، آنگاه a یک مربع کامل است. بنابراین در یک میدان بسته‌ی جبری دقیقاً یا $-a$ مجموع مربعات است یا a. بنابراین در یک میدان بسته‌ی جبری R برای هر $a \in R$ یا a مربع کامل است یا $-a$.

بنا بر گفته‌ی بالا، هر میدان بسته‌ی حقیقی را می‌توان به‌صورت یکتا مرتب کرد. در هر ترتیبی، عناصری که مربع کامل هستند را باید نامنفی بگیریم.

نتیجه ۱۰۴. اگر F بسته‌ی حقیقی باشد و $f \in F[X]$ یک چندجمله‌ای با درجه‌ی فرد باشد در این‌صورت f دارای ریشه در F است.

در واقع اگر f تحویل‌ناپذیر و از درجه‌ی فرد باشد، آنگاه اگر α ریشه‌ی F باشد و $\alpha \notin F$ در این‌صورت $F(\alpha)$ یک توسیع جبری حقیقی است که تناقض است. اگر f تحویل‌پذیر و از درجه‌ی فرد باشد، در این صورت با تجزیه‌ی f یک عامل تحویل‌ناپذیر از درجه‌ی فرد می‌رسیم که α ریشه‌ی آن است.

قضیه ۱۰۵. اگر F یک میدان حقیقی باشد، آنگاه یک میدان بسته‌ی حقیقی $R \supseteq F$ که توسیع جبری F است. (R را یک بستار حقیقیِ F می‌نامیم.)

اثبات. قرار دهید:

$$A = \{K | \text{توسیع جبری است } F \subseteq K \text{ حقیقی و } K\}$$

دقت کنید که A ناتهی و با رابطه‌ی شمول یک مجموعه‌ی مرتب جزئی است. اجتماع یک زنجیر از میدان‌های حقیقی، میدانی حقیقی است. طبق لم زرن A دارای عضو ماکسیمالی مانند R است. نشان دهید که R میدان مورد نظر ماست. □

نتیجه ۱۰۶. اگر F حقیقی باشد، آنگاه می‌توان F را مرتب کرد.

اثبات. ترتیبِ میدانِ بسته‌ی حقیقی شاملِ F را به F محدود کنید. □

دقت کنید که اگر F حقیقی باشد در این صورت یا $F(\sqrt{a})$ حقیقی است یا $F(\sqrt{-a})$ حقیقی است و یا هر دوی آنها حقیقی هستند. بنابراین امکان دارد که دو توسیع بسته‌ی حقیقی متفاوت برای F پیدا شود که در یکی از آنها a مثبت باشد و در دیگری a منفی باشد. به بیان دیگر، بستار حقیقی یکتا نیست. اما اگر F حقیقی باشد و مرتب باشد، در این صورت بستاری از آن که ترتیب یکسانی با F دارد، یکتاست. این گفته را در جلسات آینده ثابت خواهیم کرد. در واقع اگر F یک میدان حقیقی مرتب باشد و $-a$ مجموع مربعات نباشد، آنگاه در بستار حقیقیِ $F(\sqrt{a})$ عدد a مثبت است. پس در F هم عدد a مثبت است.

در ادامه‌ی درس، ثابت خواهم کرد که میدانهای بسته‌ی حقیقی، دقیقاً همان میدانهائی هستند که اگر ریشه‌ی -۱ به آنها اضافه شود، بسته‌ی جبری می‌شوند. این در واقع صورتی از قضیه‌ی اساسی جبر است.

قضیه ۱۰۷ (قضیه‌ی اساسی جبر). فرض کنید R یک میدان حقیقی باشد به طوری که

(۱) هر چندجمله‌ای با درجه‌ی فرد در R ریشه داشته باشد.

(۲) برای هر $\alpha \in R$ یا $\sqrt{\alpha} \in R$ یا $\sqrt{-\alpha} \in R$ (یعنی یا a ریشه‌ی دوم دارد یا $-a$)

در این‌صورت $K = R(i)$ بسته‌ی جبری است.

تمرین ۵۸. نشان دهید که $\mathbb{C} = \mathbb{R}(i)$ بسته‌ی جبری است. یعنی نشان دهید که میدان اعداد حقیقی شرایط قضیه را داراست.

(در ادامه‌ی درس خواهیم دید که از نتایج قضیه‌ی اساسی این است که $\mathbb{R}$ و $\mathbb{R}^{alg}$ هر دو میدانهای بسته‌ی حقیقی هستند. دومی میدان متشکل از ریشه‌های حقیقی همه‌ی چندجمله‌ایهای با ضرایب در اعداد گویا است.)

برای اثبات قضیه‌ی اساسی جبر نیاز است مفاهیمی در نظریه‌ی گالوا را یادآوری کنم.

یادآوری مبانی نظریه‌ی گالوا و قضایای سیلو

فرض کنید $L \supseteq K$ یک توسیع میدانی باشد. در این صورت، تعریف می‌کنیم:

$$Aut(\frac{L}{K}) = \{\sigma : L \to L | \forall x \in K \quad \sigma(x) = x\}$$

هر σ در بالا یک اتومرفیسمِ L است. به راحتی می‌توان تحقیق کرد که $Aut(L/K)$ یک گروه است. اگر G یک زیرگروه از آن باشد، تعریف می‌کنیم:

$$Fix(G) = \{x \in L | \forall \sigma \in G \quad \sigma(x) = x\}.$$

پس

$$K \subseteq FixAut(\frac{L}{K}) = \{x \in L | \forall \sigma Aut(\frac{L}{K}) \quad \sigma(x) = x\}$$

مشاهده ۱۰۸. فرض کنید $\sigma: L \to L$ یک اتومرفیسم باشد که K را نقطه وار حفظ می‌کند و فرض کنید که $f \in K[X]$. فرض کنید $\alpha \in L$ به‌طوری باشد که $f(\alpha) = ۰$. در این‌صورت $f(\sigma(\alpha)) = ۰$. یعنی هر اتومرفیسم میدانی که ضرایب چندجمله‌ایها را حفظ کند، مجموعه‌ی ریشه‌های چندجمله‌ای را مجموعه‌وار حفظ می‌کند.

تعریف ۱۰۹. توسیع متناهی $L \supseteq K$ را یک توسیع گالوایی می‌نامیم هرگاه $Fix(Aut(\frac{L}{K}) = K$. در این‌صورت می‌نویسیم:

$$Aut(\frac{L}{K}) = Gal(\frac{L}{K}).$$

تمرین ۵۹. نشان دهید که $L \supseteq K$ یک توسیع گالوایی است اگر و تنها اگر نرمال و جدایی‌پذیر باشد.

قضیه ۱۱۰ (قضیه‌ی اساسی نظریه‌ی گالوا).

(الف) فرض کنید $L \supseteq K$ و $\frac{L}{K}$ یک توسیع گالوایی باشد. دراین‌صورت یک تناظر یک به یک میان میدان‌های E که $L \supseteq E \supseteq K$ و زیرگروه‌های $G \subseteq Aut(\frac{L}{K})$ وجود دارد. (که توسط نگاشت $G \to Fix(G)$ داده می‌شود).

(ب) اگر $L \supseteq E_۲ \supseteq E_۱ \supseteq K$ در این‌صورت $[E_۲ : E_۱] = \frac{|G_۱|}{|G_۲|}$

(ج) به‌طور خاص

$$[L : K] = |Gal(L/K)|$$

و تعداد میدانهای میان L, K برابر است با تعداد زیرگروههای گروه گالوا.

قضیه‌ی اساسی گالوا را در درس نظریه‌ی گالوا در ترم آینده اثبات خواهم کرد. برای اثبات قضیه‌ی اساسی جبر همچنین نیاز به یادآوری قضایای سیلو دارم.

قضیه ۱۱۱ (لاگرانژ). اگر $G_۱ \leq G_۲$ دو گروه متناهی باشند آنگاه $|G_۱| \mid |G_۲|$

قضیه ۱۱۲ (سیلو).

(الف) فرض کنید G یک گروه متناهی باشد و $P \mid |G|, \cdots, P^n \mid |G|, P^{n+۱} \nmid |G|$ در این‌صورت G دارای یک P زیرگروه سیلوی ماکزیمال است. (یعنی یک زیرگروه H که مرتبه‌ی هر عنصر آن توانی از p است و $H = P^n$.)

(ب) در واقع از هر سایز p^i یک زیرگروه داریم.

۱.۳ اثبات قضیه‌ی اساسی جبر

در این بخش به اثبات قضیه‌ی ۱۰۷ پرداخته‌ام.

فرض کنید $R \subseteq K \subseteq L$ و L یک توسیع گالوائی از R باشد. نشان خواهیم داد که $L = K$.

قرار دهید $G_1 = Gal(\frac{L}{R})$. در این صورت $|G_1| = [L : R] = [L : K][K : L]$ بنابراین $2 \mid [L : R]$. در نتیجه $2 \mid |G_1|$ و G_1 دارای یک زیرگروه ۲ـ سیلو به نام H است.

ادعا می‌کنیم $H = G_1$ (در نتیجه $G_1 = 2^n$)

فرض کنید $F = FixH$ کافی است نشان دهیم که $F = R$.

اگر $F \neq R$ در این‌صورت $[F : R] = |G_1|/|H|$ یک عدد فرد است؛ پس $F = R(\alpha)$ که در آن α ریشه‌ی چند جمله‌ای درجه‌ی فرد است. اما در این صورت $\alpha \in R$.

تا اینجا نشان داده‌ایم که $R \subseteq K \subseteq L$ و $|Gal(\frac{L}{R})| = 2^n$ و $|Aut(\frac{L}{K})| = [L : K] = 2^{n-1}$.

پس $G_2 = Aut(\frac{L}{K})$ یک زیرگروه با اندیس ۲ به نام H_2 دارد. همچنین

$$R(i) = K \subseteq FixH_2 \subseteq L$$

اما در K هر چندجمله‌ای درجه ۲ ریشه دارد؛ پس $Fix(H_2)$ نمی‌تواند وجود داشته باشد.

۲.۳ ادامه‌ی بحث میدانهای بسته‌ی حقیقی

نتیجه ۱۱۳. در $\mathbb{R}$ همه‌ی چندجمله‌ای‌ها به عوامل تحویل‌ناپذیر درجه اول و درجه دوم تجزیه می‌شوند.

هر میدان بسته‌ی حقیقی شرطهای قضیه را داراست. پس اگر R بسته‌ی حقیقی باشد آنگاه $R(i)$ بسته‌ی جبری است. اگر $f \in R[X]$ یک چندجمله‌ای باشد و $a + bi$ ریشه‌ی f باشد آنگاه $a - bi$ هم ریشه‌ی f است. ضرب $x - (a + bi)$ در $x - (a - bi)$ یک چندجمله‌ای درجه‌ی ۲ می‌دهد. بنابراین اگر R بسته‌ی حقیقی باشد، هر چندجمله‌ای در آن به عوامل تحویل‌ناپذیرِ درجه‌ی ۱ و ۲ تجزیه می‌شود.

نتیجه ۱۱۴. فرض کنید R یک میدان حقیقی باشد. دراین‌صورت R بسته‌ی حقیقی است اگر و تنها اگر $R(i)$ بسته‌ی جبری باشد.

اثبات. اگر R بسته‌ی جبری باشد آنگاه دو شرط قضیه‌ی ۱۰۷ را داراست؛ پس $R(i)$ بسته‌ی جبری است.

فرض کنید R حقیقی باشد و $R(i)$ بسته جبری باشد.

ادعا می‌کنیم R هیچ توسیع جبری حقیقی ندارد. اگر $R \subseteq F$ یک توسیع جبری توسط یک چندجمله‌ی f باشد، آنگاه چندجمله‌ای f در $R(i)$ به عوامل با درجه‌ی ۱ تجزیه می‌شود. پس تنها توسیع جبری R همان $R(i)$ است که آن هم حقیقی نیست. $\square$

در ادامه نشان خواهیم داد که بسته‌ی حقیقی بودن معادل با داشتن ویژگی مقدار میانی است.

تعریف ۱۱۵. فرض کنید R یک میدان مرتب باشد. گوییم $(R, <)$ دارای ویژگی مقدار میانی است هرگاه برای هر چندجمله‌ای $f \in R[X]$ اگر $f(a)f(b) < 0$ آنگاه $\exists c \in (a, b) f(c) = 0$.

لم ۱۱۶. اگر $(R,<)$ ویژگی مقدار میانی داشته باشد، آنگاه R بسته‌ی حقیقی است.

اثبات.

۱) فرض کنید f یک چند جمله‌ای با درجه فرد باشد. در این صورت اعداد $M, -M$ موجودند به‌طوری‌که $f(M) > ۰$ و $f(-M) < ۰$. بنا به ویژگی مقدار میانی، f دارای یک ریشه در R است.

۲) فرض کنید $a > ۰$. معادله‌ی $p(x) = x^۲ - a$ را در نظر بگیرید. داریم $P(۰) < ۰, p(a+۱) > ۰$. بنابراین این معادله دارای ریشه است.

پس $R(i)$ بسته‌ی جبری است و از این‌رو R بسته‌ی حقیقی است. $\square$

قضیه ۱۱۷. فرض کنید R بسته‌ی حقیقی باشد. در این‌صورت $(R,<)$ با ترتیب یکتای خود دارای ویژگی مقدار میانی است.

اثبات. فرض کنید $f(x)$ یک چندجمله‌ای باشد به‌طوری‌که $f(a) < ۰$ و $f(b) > ۰$. چندجمله‌ای f به عوامل درجه اول و دوم قابل تجزیه است. در این‌صورت یکی از عوامل تحویل ناپذیر f در a, b علامت‌های متفاوت دارد، پس فرض می‌کنیم که f تحویل پذیر است. اگر f درجه‌ی اول باشد f دارای ریشه است. اگر f درجه‌ی دوم و تحویل‌ناپذیر باشد آنگاه $f = x^۲+cx+d$ که در آن $c^۲ - ۴d < ۰$. پس $f = (x+\frac{c}{۲})^۲ + (d - \frac{c^۲}{۴})$ و $f > ۰$. $\square$

نتیجه ۱۱۸. موارد زیر باهم معادلند:

۱) R یک میدان بسته‌ی حقیقی است.

۲) برای هر $a \in R$ یا a یا $-a$ دارای ریشه دوم است و چند جمله‌ایهای با درجه فرد در R ریشه دارند.

۳) $R(i)$ بسته‌ی جبری است.

۴) R دارای یک ترکیب یکتاست و با آن ترتیب دارای ویژگی مقدار میانی است.

۳.۳ یکتائی بستار حقیقی

اگر F یک میدان حقیقی باشد در این‌صورت یک میدان بسته‌ی حقیقی $\underbrace{F \subseteq R}_{\text{جبری}}$ موجود است که به آن یک بستار حقیقی برای F گفته می‌شود. بر خلاف بستار جبری، بستار حقیقی یک میدان حقیقی، یکتا نیست. در زیر مثالی برای این عدم یکتائی آورده‌ایم.

میدان Q حقیقی است و در آن -۲ مجموع مربعات نیست. پس میدان $Q(\sqrt{۲})$ حقیقی است. دقت کنید که

$$Q(\sqrt{۲}) = \{a + b\sqrt{۲} | a, b \in Q\}$$

نگاشتِ

$$a + b\sqrt{۲} \mapsto a - b\sqrt{۲}$$

یک اتومرفیسم از میدان بالاست؛ بنابراین $\sqrt{2}$ در میدان $\mathbb{Q}(\sqrt{2})$ مجموع مربعات نیست (اگر باشد، $-\sqrt{2}$ نیز مجموع مربعات می‌شود و این با حقیقی بودن این میدان تناقض دارد). به بیان دیگر هیچکدام از $\sqrt{2}, -\sqrt{2}$ مجموع مربعات نیستند. پس میدانِ $\mathbb{Q}(\sqrt{2})$ دارای یک توسیع حقیقی است که در آن $\sqrt{2}$ عددی مثبت است و دارای یک توسیع حقیقی است که در آن $\sqrt{2}$ عددی منفی است. این دو توسیع حقیقی با همدیگر ایزومرف (میدانی) نیستند.

در ادامه هدفمان اثبات این است اگر ترتیب را حفظ کنیم، بستار حقیقی یکتا خواهد بود. به بیان دیگر، در ادامه‌ی درس قضیه‌ی زیر را ثابت خواهیم کرد.

قضیه ۱۱۹. اگر $(F, <)$ یک میدان حقیقی باشد. در این‌صورت اگر R_0 و R_1 دو بستار حقیقی حافظ ترتیب از F باشند، آن‌گاه $R_0 \cong R_1$.

تعریف ۱۲۰. دنباله‌ی $f_0, \ldots, f_n$ از چندجمله‌ایها را را یک دنباله اشتورم می‌نامیم هرگاه

- $f_1 = f_0'$
- $\neg(\exists x \quad f_i(x) = 0 \wedge f_{i+1}(x) = 0)$
- $f_i(z) = 0 \rightarrow f_{i-1}(z)f_{i+1}(z) < 0$
- f_n یک ثابت ناصفر است.

مثال ۱۲۱. فرض کنید F یک میدان حقیقی باشد و $f \in F[X]$ یک چندجمله‌ای باشد. دنباله‌ای که به صورت زیر ساخته می‌شود یک دنباله‌ی اشتورم است:

$$f_0 = f$$

$$f_1 = f_0'$$

$$f_{i-1} = gf_i + (-f_{i+1}).$$

به بیان دیگر f_{i+1} باقی‌مانده‌ی تقسیمِ f_{i-1} بر f_i است که در منهای یک ضرب شده است.

تعریف ۱۲۲. فرض کنید $f_0 \ldots f_n$ یک دنباله‌ی اشتورم باشد و $c \in F$. در این صورت تعداد تغییر علامتها در دنباله‌ی $f_0(c), f_1(c), \ldots, f_n(c)$ را با $v(c)$ نشان می‌دهیم.

قضیه ۱۲۳ (الگوریتم اشتورم). اگر R یک میدان بسته حقیقی باشد و $f \in R[X]$ ریشه‌ی تکراری در بازه‌ی (c, d) نداشته باشد و $f_0, \ldots, f_n$ یک دنباله اشتورم باشد که با f شروع شده است، دراین‌صورت تعداد ریشه های f در بازه‌ی (c, d) برابر است با $\nu(c) - \nu(d)$.

اثبات. فرض کنید که تمامی ریشه‌های تمامی f_i ها در بازه‌ی (c, d) به صورت زیر مرتب شده باشند:

$$z_0 < z_1 < \ldots < z_{n-1} < z_n.$$

بین z_i ها عناصر c_i را به صورت زیر انتخاب کنید:

$$c_0 = c < z_0 < c_1 < z_1 < c_2 < z_3 < \ldots < z_{n-1} < c_n < z_n < c_{n+1} = d.$$

دقت کنید که

$$v(c)-v(d)=v(c_0)-v(c_1)+v(c_1)-v(c_2)+\ldots+v(c_{n-1})-v(c_n)+v(c_n)-v(c_{n+1})$$

کافی است نشان دهیم که در هر بازه‌ی (c_i,c_{i+1}) اگر z_i ریشه‌ی f باشد، آنگاه $v(c_i)-v(c_{i+1})=1$ و اگر z_i ریشه‌ی f نباشد، آنگاه $v(c_i)-v(c_{i+1})=0$.

برای سادگی، بازه‌ی مورد نظر را به صورت (c,d) در نظر می‌گیریم و فرض می‌کنیم $z\in(c,d)$ یکی از ریشه‌های یکی از f_i ها باشد.

فرض کنید که z ریشه‌ی f_i باشد که $i\neq 0$. از آنجا که $f_i(z)=0$ بنا به تعریف دنباله‌ی اشتورم، $f_{i-1}(z)$ و $f_{i+1}(z)$ علامتهای متفاوت دارند. فرض کنید اولی منفی و دومی مثبت باشد. از طرفی f_{i-1} و f_{i+1} در بازه‌ی (c,d) ریشه‌ای ندارند، پس علامتها به صورت زیر خواهند بود. (یک حالت نمونه)

$$\begin{array}{ccc} f_{i-1}(c)- & f_{i-1}(z)- & f_{i-1}(d)- \\ f_i(c)- & f_i(z)=0 & f_i(d)+ \\ f_{i+1}(c)+ & f_{i+1}(z)+ & f_{i+1}(d)+ \end{array}$$

پس تعداد تغییر علامتها در چپ و راست با هم برابر است؛ یعنی $v(c)=v(d)$.

حال اگر z ریشه‌ی f باشد، آنگاه f' در بازه‌ی (c,d) ناصفر است. پس f یکنواست و علامتها به صورت زیر خواهد بود: (یک حالت نمونه)

$$\begin{array}{ccc} f_0(c)- & f_0(z)=0 & f_0(d)+ \\ f_1(c)+ & f_1(z)+ & f_1(d)+ \\ f_{i+1}(c)+ & f_{i+1}(z)+ & f_{i+1}(d)+ \end{array}$$

همانطور که در بالا مشاهده می‌کنید $v(c)-v(d)=1$. دقت کنید که در اشکال بالا، تنها یکی از حالتهای ممکن را در نظر گرفته‌ام، و بررسی حالات دیگر را به عنوان تمرین رها کرده‌ام. □

نتیجه ۱۲۴. فرض کنید $(F,<)$ یک میدان حقیقی مرتب و f یک چندجمله‌ای تحویل‌ناپذیر در $F[x]$ باشد. اگر R_0 و R_1 دو بستار حقیقی F با حفظ ترتیب باشند در این‌صورت تعداد ریشه‌های f (بدون شمارش تکرار) در R_0,R_1 برابر است.

اثبات. یک بازه $[-M,M]$ پیدا می‌شود به طوری که تمامی ریشه‌های f در آن هستند و $M\in F$. تعداد ریشه‌های f در R_0 برابر است با $\nu(-M)-\nu(M)$ و آن برابر است با تعداد ریشه‌های f در R_1. □

نتیجه ۱۲۵. اگر R_1,R_2 دو بستار حقیقی F با حفظ ترتیب باشند، دراین‌صورت $R_1\cong R_2$.

تمرین ۶۰. نتیجه‌ی بالا را (چه با استفاده از لم زرن و چه با یک سامانه‌ی رفت‌وبرگشتی) اثبات کنید.

۴.۳ نگاهی جبری به حذف سور

در درسهای گذشته با مفهوم حذف سور آشنا شدیم. تعریف آن را در زیر یادآوری کرده‌ام:

تعریف ۱۲۶. فرض کنید T یک تئوری مرتبه اول باشد. T سورها را حذف می‌کند هرگاه برای هر فرمول $\phi(\bar{x})$ یک فرمول بدون سور $\psi(\bar{x})$ پیدا شود به‌طوری‌که $T \models \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$

حذف سور در واقع یک ویژگی جبری برای تئوری‌ها است. قضیه‌ی زیر این گفته را روشن می‌کند:

قضیه ۱۲۷. در تئوری T فرمول $\varphi(\bar{x})$ دارای معادل بدون سور است، اگروتنهااگر برای هر دو مدل $\mathfrak{M}_1, \mathfrak{M}_2$ از این تئوری و هر زیرساختار مشترک A از این دو مدل برای هر $\bar{a} \in A$ داشته باشیم: $\mathfrak{M}_1 \models \varphi(\bar{a}) \Leftrightarrow \mathfrak{M}_2 \models \varphi(\bar{a})$

اثبات. فرض کنید فرمول φ نسبت به T دارای یک معادل بدون سور ψ باشد. در این صورت
فرض کنید

$$T \models \varphi(\bar{x}) \leftrightarrow \psi(\bar{x})$$
$$\mathfrak{M}_1 \models \varphi(\bar{a}) \Leftrightarrow$$
$$\mathfrak{M}_1 \models \psi(\bar{a}) \Leftrightarrow$$
$$A \models \psi(\bar{a}) \Leftrightarrow$$
$$\mathfrak{M}_2 \models \psi(\bar{a}) \Leftrightarrow$$
$$\mathfrak{M}_2 \models \varphi(\bar{a}).$$

جهت عکس این قضیه، یکی از نتایج قضیه‌ی فشردگی است:
نخست همه‌ی نتایجِ بدونِ سورِ فرمول φ را در یک مجموعه بریزید؛ به بیان دیگر، مجموعه زیر را درنظر بگیرید(ثابت $\bar{c}$ را به زبان اضافه کنید)

$$\Gamma(\bar{c}) = \{\psi(\bar{c}) \mid \psi \text{بدون سور}, T \models \phi(\bar{c}) \to \psi(\bar{c})\}$$

ادعای اول. $T \cup \Gamma(\bar{c}) \models \phi(\bar{c})$.
اگر ادعای اول درست باشد، قضیه اثبات می‌شود؛ زیرا در این صورت بنا به قضیه‌ی فشردگی تعداد متناهی فرمولِ $\psi_i \in \Gamma$ موجودند به طوری که

$$T \cup \{\psi_1 \wedge \ldots \wedge \psi_n\} \models \phi(\bar{c})$$

$T \vdash \psi_1 \wedge \ldots \wedge \psi_n(\bar{c}) \leftrightarrow \phi(\bar{c})$ زیرا بنا به تعریف، ψ_i ها نتایجِ ϕ هستند

$$T \vdash \forall \bar{x} \quad (\psi_1 \wedge \ldots \wedge \psi_n(\bar{x}) \leftrightarrow \phi(\bar{x})).$$

اثبات ادعای اول.
اگر $T \cup \Gamma(\bar{c}) \not\models \phi(\bar{c})$ آنگاه $T \cup \Gamma(\bar{c}) \cup \neg\phi(\bar{c})$ سازگار است بنابراین مدلی مانند $(\mathfrak{M}, \bar{a})$ دارد:

$$\mathfrak{M} \models T \cup \Gamma(\bar{a}) \cup \neg\phi(\bar{a})$$

قرار دهید: $A = \langle \bar{a} \rangle^{\mathfrak{M}}$. ادعا می‌کنیم $Diag(A) \cup T \cup \phi(\bar{\{a\}})$ سازگار است. منظور از $Diag(A)$ مجموعه‌ی همه‌ی فرمولهای بدونِ سورِ $\chi(\bar{a})$ است که در A برقرارند. اگر این ادعا ثابت شود به تناقض می‌رسیم زیرا A یک زیرساختار مشترک از $\mathfrak{M}, \mathfrak{N}$ است و $\mathfrak{M} \models \phi(\bar{a})$ و $\mathfrak{N} \models \neg\phi(\bar{a})$.

اگر ادعا درست نباشد، دراین‌صورت فرمول بدون سوری مانند $\chi(\bar{a}) \in Diag(A)$ یافت می‌شود به طوری که

$$T \models \phi(\bar{a}) \to \neg\chi(\bar{a})$$

بنابراین

$$\neg\chi(\bar{a}) \in \Gamma$$

پس

$$\mathfrak{M} \models \neg\chi(\bar{a})$$

اما $\neg\chi(\bar{a})$ یک فرمولِ بدون سور است و داریم

$$A \models \chi(\bar{a})$$

. $\square$

۵.۳ حذف سور در تئوری میدانهای بسته‌ی حقیقی و کامل بودن تئوری میدانهای بسته‌ی حقیقی

تعریف ۱۲۸ (تئوری میدانهای بسته‌ی حقیقی). در زبانِ $L = \{+, -, \cdot, ۰, ۱, <\}$ تئوری RCF را تئوری شامل اصول زیر در نظر می‌گیریم:

- اصول میدانهای حقیقی مرتب
- $\forall a \ \ [(\exists x \ \ x^۲ = a) \vee (\exists x \ \ x^۲ = -a)]$
- $\{\forall a_۰, \ldots, a_{۲n+۱} \ \ \exists x \ \ a_{۲n+۱}x^{۲n+۱} + \cdots + a_۰ = ۰\}_{n \in \mathbb{N}}$ (به عبارت دیگر، هر چندجمله‌ای با درجه فرد دارای ریشه باشد.)

دقت کنید که تعریف میدانهای بسته‌ی حقیقی، تعریفی کاملاً غیر مرتبه‌ی اول است؛ ولی قضایائی که در درسهای گذشته ثابت کردیم امکان اصل‌بندی بالا را برای میدانهای بسته‌ی حقیقی فراهم کرده است. یک اصل بندی مرتبه‌ی اول معادل نیز، بیان ویژگی مقدار میانی برای چندجمله‌ای‌هاست.

توجه ۱۲۹. تئوری RCF سازگار است زیرا $\overline{\mathbb{R}} = (\mathbb{R}, +, \cdot, -, ۰, ۱)$ یک مدل برای آن است.

در ادامه ثابت خواهیم کرد که RCF یک تئوری کامل است. از این نتیجه خواهد شد که $\mathrm{RCF} \equiv \mathrm{Th}(\overline{\mathbb{R}})$. به بیان دیگر، یک میدان در صورتی بسته‌ی حقیقی است که هم‌ارز مقدماتی با میدان اعداد حقیقی باشد (یعنی همه‌ی ویژگی‌های مرتبه‌ی اول میدان اعداد حقیقی را داشته باشد).

دقت کنید که اصول RCF قابل تولید توسط یک الگوریتم هستند. پس اگر کامل بودن این اصول ثابت شود، این گفته اثبات می‌شود که الگوریتمی وجود دارد که تمامی حقایق درست در مورد اعداد حقیقی را تولید می‌کند (در زبان یادشده). به بیان دیگر، هر قضیه‌ای در مورد اعداد حقیقی با استفاده از آن الگوریتم، از اصول RCF نتیجه خواهد شد.

پیش از اثبات کامل بودن، حذف سور را برای RCF ثابت می‌کنیم.

قضیه ۱۳۰. RCF در زبان $L = \{+, -, ., 0, 1, <\}$ سورها را حذف می‌کند.

اثبات. فرض کنیم $\mathfrak{M}_1 = (M_1, +, -, ., 0, 1, <)$ و $\mathfrak{M}_2 = (M_2, +, -, ., 0, 1, <)$ دو مدل برای RCF باشند. همچنین فرض کنیم A یک زیرساختار مشترک از $\mathfrak{M}_1$ و $\mathfrak{M}_2$ باشد. توجه کنید که A لزوماً مدلی برای RCF نیست و تنها چیزی که از آن می‌دانیم این است که A یک حوزه صحیح مرتب است. یادآوری می‌کنیم که حلقه R را حوزه صحیح می‌نامند هرگاه

$$\forall x, y \in R \quad x.y = 0 \ \rightarrow x = 0 \ \vee y = 0.$$

فرض کنید که $D_1(A), D_2(A)$ به ترتیب میدان کسرهای حوزه‌ی صحیحِ A در M_1 و M_2 باشند. یعنی

$$D_1(A) = \{\frac{m}{n} \in M_1 | m, n \in A\}$$

در این صورت $D_1(A)$ و $D_2(A)$ به عنوان دو میدان، با یکدیگر ایزومرف هستند. در واقع هر دوی آنها ایزومرف با میدان کانونی کسرهای A هستند که از اعضای $\frac{m}{n}$ تحت رابطه‌ی هم‌ارزی زیر تشکیل شده است:

$$\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow mn' = nm'$$

تمرین ۶۱. نشان دهید که هر $D_i(A)$ دارای ترتیبی است که توسیع ترتیبِ A است و نشان دهید که A'_1, A'_2 به عنوان میدانهای مرتب نیز با هم ایزومرف هستند.

همچنین دقت کنید که $D_i(A)$ هر دو میدان حقیقی هستند. پس دیاگرام زیر را داریم:

$$\begin{tikzcd}
\mathfrak{M}_1 & & \mathfrak{M}_2 \\
D_1(A) \arrow[u] \arrow[rr, phantom, "\cong"] & & D_2(A) \arrow[u] \\
& A \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

فرض کنید $rcl_1(D_1(A))$ و $rcl_2(D_2(A))$ به ترتیب بستار حقیقیِ $D_1(A)$ و $D_2(A)$ در داخل M_1 و M_2 با حفظ ترتیب باشند. بنا به آنچه در بخشهای گذشته ثابت کردیم، آندو با هم ایزومرفند. پس دیاگرام زیر را داریم:

$$\begin{tikzcd}
\mathfrak{M}_1 & & \mathfrak{M}_2 \\
rcl_1(D_1(A)) \arrow[u] \arrow[rr, phantom, "\cong"] & & rcl_2(D_2(A)) \arrow[u] \\
D_1(A) \arrow[u] \arrow[rr, phantom, "\cong"] & & D_2(A) \arrow[u] \\
& A \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

حال فرض کنید ψ یک فرمول بدون سور باشد و $\bar{a} \in A$. فرمول $\varphi : \exists x \quad \psi(x, \bar{a})$ را در نظر بگیرید. می‌خواهیم نشان دهیم اگر

$$\exists c \in M_1 \quad \mathfrak{M}_1 \vDash \psi(c, \bar{a})$$

آنگاه

$$\exists d \in M_2 \quad \mathfrak{M}_2 \vDash \psi(d, \bar{a}).$$

از آنجایی که $\psi(x, \bar{a})$ بدون سور است می‌توان آن را به صورت نرمال عطفی نوشت (یعنی فصل عطفهای اتمی). هر فرمول اتمی در این زبان به صورت $f(\bar{x}) > 0$ است که در آن f یک چندجمله‌ای است. پس فرمولِ ψ را می‌توان به صورت زیر فرض کرد:

$$\psi \ : \ \bigvee \bigwedge (f_i(x) > 0 \wedge h_i(x) = 0)$$

که در آن f_iها و h_iها چندجمله‌ای‌هایی با پارامتر در A هستند. همانطور که از فرمول بالا مشخص است کافی است برای ادامه اثبات تنها $\bigwedge_{i\in I}(f_i(x) > 0 \wedge h_i(x) = 0)$ را در نظر بگیریم. فرض کنیم عنصر c در M_1 وجود داشته باشد که

$$\bigwedge_{i\in I}(f_i(c) > 0 \wedge h_i(c) = 0)$$

دو حالت زیر را در نظر می‌گیریم

۱) در فرمول بالا تساوی وجود داشته باشد. فرض کنیم چندجمله‌ای $h[x] \in A[x]$ یکی از آنها باشد. پس $h(c) = 0$. با توجه به اینکه ریشه چندجمله‌ای‌ها در $rcl_1(D_1(A))$ وجود دارد می‌توان نتیجه گرفت متناظر c عنصر d در $rcl_2(D_2(A))$ وجود دارد که $h(d) = 0$ و حکم ثابت می‌شود.

۲) تساوی در فرمول بالا نباشد. چندجمله‌ای $f[x] \in A[x]$ را در نظر می‌گیریم که $f(c) > 0$. می‌دانیم که f در M_1 تعداد متناهی ریشه دارد. از آنجایی که c ریشه نیست پس می‌توان در نظر گرفت که c بین دو ریشه f باشد. با توجه به اینکه ریشه‌های f در $rcl_1(D_1(A))$ قرار دارند پس یک عنصر مانند c' در $rcl_1(D(A))$ وجود دارد که بین دوریشه f است و $f(c') > 0$. تصویر این عنصر در $rcl_1(D_2(A))$ همان عنصر d مورد نظر ماست. همین اثبات را برای حالتی که بیش از یک چندجمله‌ای داشته باشیم توسعه ببخشید.

$\square$

توجه ۱۳۱. RCF در زبان $L = \{+, -, ., 0, 1\}$ سورها را حذف نمی‌کند. (در واقع ترتیب نقش بسیار مهمی را در اثبات قضیه بالا ایفا می‌کند.) برای درک بهتر این موضوع تمرین زیر را بیان می‌کنیم.

تمرین ۶۲. نشان دهید که فرمول

$$\exists y \quad x = y^2$$

در RCF معادل بدون سور ندارد. برای این کار کافی است دو مدل برای RCF بسازید که یک عنصر مشترک، در یکی از آنها مثبت باشد و در دیگری منفی.

توجه ۱۳۲. مجموعه‌های تعریف پذیر در یک مدل RCF در زبان‌های دارای ترتیب و بدون ترتیب یکسان هستند زیرا

$$x < y \iff \exists z \quad y - x = z^2.$$

تمرین ۶۳. با توجه به اینکه RCF در زبان دارای ترتیب حذف سور دارد، ثابت کنید در زبان بدون ترتیب هر فرمول دارای یک معادل وجودی است.

با توجه به قضیه ۱۳۰ و ویژگی‌های حذف سور به نتایج زیر می‌رسیم.

نتیجه ۱۳۳. RCF کامل است؛ یعنی اگر $\mathfrak{M}_۱, \mathfrak{M}_۲ \models \mathrm{RCF}$ آنگاه $\mathfrak{M}_۱ \equiv \mathfrak{M}_۲$.

اثبات. فرض کنیم $\mathfrak{M}_۱$ و $\mathfrak{M}_۲$ دو مدل برای RCF باشند. این دو مدل، میدان و شامل Q نیز هستند. پس هر دو، شاملِ بستار حقیقی $\mathbb{Q}$ هستند.

تمرین ۶۴. بستار حقیقیِ $\mathbb{Q}$ را با $\mathbb{R}^{alg}$ نشان می‌دهیم. نشان دهید که $\mathbb{R}_{alg}$ دقیقاً میدان متشکل از اعداد حقیقیِ جبری است (یعنی اعداد حقیقی‌ای که ریشه‌ی چندجمله‌ایهای با ضرایب در $\mathbb{Q}$ هستند). به بیان دیگر نشان دهید که میدانی که بدین صورت تعریف می‌شود، بسته‌ی حقیقی است.

حال برای هر جمله‌ی ϕ از آنجا که ϕ دارای معادل بدون سور است، تحت زیرساختارها حفظ می‌شود و

$$M_۱ \models \varphi \Rightarrow \mathbb{R}^{alg} \models \varphi \Rightarrow M_۲ \models \varphi.$$

□

نتیجه ۱۳۴. $\mathrm{RCF} \equiv \mathrm{Th}(\overline{\mathbb{R}})$. بنابراین برای جمله φ داریم، $\varphi \in \mathrm{Th}(\overline{\mathbb{R}})$ اگر و تنها اگر $\mathrm{RCF} \vdash \varphi$.

نتیجه ۱۳۵. R یک میدان بسته حقیقی است اگر و تنها اگر $R \equiv \overline{\mathbb{R}}$. (زیرا در یک تئوری کامل هر دو مدل ویژگی‌های کاملا یکسانی دارند.)

نتیجه ۱۳۶. $\mathrm{Th}(\overline{\mathbb{R}})$ تصمیم پذیر است. یعنی الگوریتمی داریم که همه‌ی جملات درست در مورد اعداد حقیقی را تولید کند.

۶.۳ چند نتیجه‌ی جذاب جبری

تعریف ۱۳۷. مجموعه $X \subseteq \mathbb{R}^n$ را شبه جبری[۱] نامیم هرگاه X یک ترکیب بولی متناهی از مجموعه‌های به صورت زیر باشد

$$\{\overline{x} \mid f(\overline{x}) > ۰\}$$

برای مثال مجموعه $\{x \mid ax^۲ + bx < ۰ , cx^۳ + dx^۵ = ۰\}$ شبه جبری است.

پس یک مجموعه‌ی $X \subseteq \mathbb{R}^n$ شبه‌جبری است اگروتنهااگر یک فرمولِ بدون سورِ $\phi(\bar{x})$ در زبان تئوریِ $\overline{\mathbb{R}}$ وجود داشته باشد به طوری که

$$X = \{\bar{a} | \overline{\mathbb{R}} \models \phi(\bar{a}).\}$$

از طرفی هر فرمول در $\overline{\mathbb{R}}$ معادل یک فرمول بدون سور است. پس یک مجموعه‌ی $X \subseteq \mathbb{R}^n$ شبه‌جبری است اگروتنهااگر تعریف‌پذیر توسط یک فرمول (با پارامتر) باشد. این مشاهده‌ی ساده، اثباتی برای قضیه‌ی جبری فراهم می‌آورد.

[۱] Semialgebraic

قضیه ۱۳۸. (تارسکی_سایدنبرگ [۲]) اگر $X \subseteq \mathbb{R}^n \times \mathbb{R}^m$ شبه جبری باشد در این صورت $\pi(X)$ (تصویر X روی $\mathbb{R}^n$) شبه جبری است.

اثبات. فرض کنید $X \subseteq \mathbb{R}^n \times \mathbb{R}^m$ شبه جبری باشد، در این صورت

$$\pi(X) = \{\overline{x} \in \mathbb{R}^n \mid \exists \overline{y} \in \mathbb{R}^m \quad (\overline{x}, \overline{y}) \in X\}.$$

فرض کنیم X با فرمول $\varphi(\overline{x}, \overline{y})$ تعریف شده باشد در این صورت

$$X = \{(\bar{x}, \bar{y} \in \mathbb{R}^{n+m} : \overline{\mathbb{R}} \models \phi(\bar{x}, \bar{y})\}$$

همچنین

$$\pi(X) = \{\overline{x} \in \mathbb{R}^n \mid \exists \overline{y} \in \mathbb{R}^m \quad \varphi(\overline{x}, \overline{y})\}.$$

اما فرمول $\exists \overline{y} \quad \varphi(\overline{x}, \overline{y})$ دارای معادل بدون سور است، یعنی یک مجموعه‌ی شبه‌جبری تعریف می‌کند؛ پس $\pi(X)$ شبه جبری است. $\square$

قضیه ۱۳۹. (مسأله ۱۷ هیلبرت) فرض کنیم R یک میدان بسته حقیقی باشد و $\overline{x} = (x_۱, \ldots, x_n)$. فرض کنید $f \in R(\overline{x})$ یک تابع گویا باشد (یعنی به صورت کسر چندجمله‌ای‌های چندمتغیره مانند $g(\overline{x})/k(\overline{x})$ باشد) به طوری که برای هر عنصر $\overline{a}$ در R داشته باشیم $f(\overline{a}) \geq ۰$. در این صورت توابع گویای $h_۱, \ldots, h_n$ وجود دارند به طوری که $f = h_۱^۲ + \cdots + h_n^۲$.

اثبات. فرض کنیم f مجموع مربعات توابع گویا نباشد. در این صورت در میدان $R(\overline{x})$ عنصر f مجموع مربعات نیست. بنابراین $R(\overline{x})$ دارای یک بستار حقیقی است که در آن f منفی است. پس اگر F این بستار حقیقی $R(\overline{x})$ باشد، در میدان F داریم $f < ۰$. بنابراین

$$F \models f < ۰.$$

دقت کنید که عنصر f در میدانِ F را می‌توان به صورت عنصر $f(\overline{x})$ در نظر گرفت که در آن $\bar{x} \in F$ و $f \in R(\overline{x})$. با این نگاه داریم:

$$F \models \exists \overline{x} \quad f(\overline{x}) < ۰.$$

عنصر $\bar{x}$ در بالا، همان متغیر x است!

از طرفی R, F هر دو مدلهایی برای RCF هستند و $R \subseteq F$. بنا به حذف سور، هر فرمولی که با پارامترهای R در F درست باشد، در R نیز درست است (زیرا هر فرمول دارای معادل بدون سور است و فرمولهای بدون سور تحت زیرساختارها حفظ می‌شوند). بنابراین $R(\overline{x}) \models \exists \overline{x} \quad f(\overline{x}) < ۰$ و این در تناقض با فرض مثبت بودن f به ازای تمامی مقادیر در $R(\overline{x})$ است. $\square$

با ایده‌ای مشابه می‌توان قضیه‌ی اشاره شده در تمرین زیر را ثابت کرد.

ایده‌آل $J \subseteq F[\bar{X}]$ را یک ایده‌آل حقیقی می‌نامیم هرگاه $\sum_{i=۱}^{m} p_i^۲ \in J$ نتیجه دهد که هر p_i در J است. برای یک ایده‌آلِ دلخواه J رادیکال حقیقیِ J برابر است با کوچکترین ایده‌آل حقیقی شامل J.

[۲] Tarski-Seidenberg

تمرین ۶۵. (قضیه ضعیف حقیقی ریشه‌ها[۳]) فرض کنید F بسته حقیقی باشد و I ایده‌آلی در $F[\bar{X}]$ باشد. در این صورت $V_F(I)$ ناتهی است اگروتنهااگر رادیکالِ حقیقیِ I یک ایده‌آل سره باشد (یعنی ناتهی باشد و برابر با کل حلقه نباشد).

تمرین ۶۶. قضیه حقیقی ریشه‌ها را بیان کنید (تناظر میان ایده‌آلهای حقیقیِ $F[\bar{X}]$ و چندگوناها در F).

[۳] Weak Real Nullstellensatz