بسم الله الرحمن الرحیم

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

معرفی یک ارزیابی هنسلی تعریف‌پذیر با پیچیدگی سوری بالا

پایان‌نامه کارشناسی ارشد ریاضی محض

نجمه زمانی

استاد راهنما

دکتر محسن خانی

۱۴۰۱

دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد ریاضی محض خانم نجمه زمانی

تحت عنوان

معرفی یک ارزیابی هنسلی تعریف‌پذیر با پیچیدگی سوری بالا

در تاریخ ۳۰ شهریور ۱۴۰۱ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت

۱- استاد راهنمای پایان‌نامه	دکتر محسن خانی
۲- اســـــــــتاد داور ۱	دکتر علیرضا مفیدی
۳- اســـــــــتاد داور ۲	دکتر مجید سلامت
سرپرست تحصیلات تکمیلی دانشکده	دکتر اعظم اعتماد

تقدیم به:

مادرم

فهرست مطالب

چکیده:

هدف این پایان‌نامه پاسخ دادن به این سوال است که آیا یک فرمولِ $\exists\forall$ و یا یک فرمولِ $\forall\exists$ در زبان حلقه‌ها وجود دارد که حلقهٔ ارزیابِ یک میدان ارزیابیِ هنسلی را بدون پارامتر تعریف کند؟ این سوال توسط پِرستِل [1] در مقالهٔ [۱۲] مطرح شده است. در پاسخ دادن به این سوال یک میدان ارزیابی هنسلی به صورت $K = k((\Gamma_1))((\Gamma_2))$ معرفی می‌کنیم که حلقهٔ ارزیاب آن با هیچ فرمول $\forall\exists$ و یا $\exists\forall$ بدون پارامتر در زبان حلقه‌ها تعریف نمی‌شود. منظور از $k((\Gamma_1))$ میدان سری‌های هان با گروه ارزیاب Γ_1 است. مهم‌ترین ایده‌های به کار رفته برای پاسخ به این سوال، محکی از پرستل برای تعریف پذیری یک حلقهٔ ارزیاب با فرمول‌های $\exists\forall$ و $\forall\exists$ و همچنین قضیهٔ اکس–کوچن و ارشوف [2] است که هر دو در پایان‌نامه آورده شده است.

مقالهٔ زیر منبع اصلی این پایان‌نامه است.

Halupczok, I and Jahnke, F.: *A definable Henselian valuation with high quantifier complexity.* Mathematical Logic Quarterly Bull. 61 (4-5). pp. 362-366. ISSN 0942-5616 (2015).

رده بندی موضوعی: 03C40 (13F30)

واژگان کلیدی: میدان ارزیابی هنسلی، حلقهٔ ارزیاب، قضیهٔ اکس–کوچن و ارشوف، تعریف‌پذیری.

[1]Perestel [2]Ax-Kochen and Eršov

پیشگفتار

یک نگاشت ارزیابی، نگاشتی از یک دامنهٔ صحیحِ A به یک گروه آبلی مرتبِ Γ به صورت $v : A^{\times} \longrightarrow \Gamma$ است که دو ویژگی زیر را داراست:

$$\forall a, b \in A \quad v(ab) = v(a) + v(b)$$

$$\forall a, b \in A \quad v(a+b) \geq \min\{v(a), v(b)\}.$$

به جفت (A, v) یک حلقهٔ ارزیابی گوییم. اگر K یک میدان باشد، به جفت (K, v) یک میدان ارزیابی، به Γ گروه ارزیاب و به $O_v = \{x \in K : v(x) \geq ۰\}$ حلقهٔ ارزیاب گوییم. در فصل دو نشان خواهیم داد حلقهٔ ارزیاب، حلقه‌ای موضعی است یعنی تنها یک ایده‌آل ماکسیمال دارد که آن را با m_v می‌نشان دهیم و حلقهٔ خارج قسمتیِ $k_v := \dfrac{O_v}{m_v}$ یک میدان است که آن را میدان باقی‌مانده‌ها نامیم.

برای مثال فرض کنید p یک عدد اول باشد و $a \in \mathbb{Z}$. اگر $a = p^m a'$ به طوری که $p \nmid a'$. نگاشت ارزیابیِ v_p از دامنهٔ صحیح $\mathbb{Z}$ به گروه $\mathbb{Z}$ به صورت

$$v_p : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$v_p(a) = n$$

تعریف می‌شود که به آن نگاشت ارزیابی p–ادیک گویند. بنابراین به جفت $(\mathbb{Z}, v_p)$ حلقهٔ ارزیابی p–ادیک گویند که گروه ارزیاب آن $\mathbb{Z}$ است. میدان باقی‌مانده‌ها $\mathbb{F}_p$ می‌باشد که جلوتر به آن می‌پردازیم. منظور از میدان هنسلی یک دامنهٔ موضعی A با ایده آل ماکسیمال m می‌باشد که هرگاه برای هر $f(x) \in A[X]$ و برای هر $a \in A$ به طوری که $f(a) \in m$ و $f'(a) \notin m$ آنگاه $\alpha \in A$ موجود باشد به طوری که $f(\alpha) = ۰$ و $\alpha \equiv a \ (mod\ m)$.

اگر زبان حلقه‌ها $\mathcal{L}_{\mathrm{r}} = \{+, -, ., ۰, ۱\}$ را در نظر بگیریم، مجموعهٔ تعریف‌پذیر در زبان به این معناست که بتوانیم فرمولی در زبان ارائه دهیم به طوری که عناصری که در فرمول صدق می‌کنند برابر مجموعه باشد. به عنوان مثال می‌توانیم مجموعهٔ $A = \{i, -i\}$ را در زبان حلقه‌ها با استفاده از فرمولِ $x^۲ + ۱ = ۰$ تعریف کنیم در این صورت گوییم مجموعهٔ A در زبان تعریف‌پذیر است.

در مقالات [۱۲، ۹، ۸، ۷، ۶، ۵، ۳، ۲] مثال‌های زیادی وجود دارند که تعریف‌پذیری حلقه‌های ارزیاب را در زبان حلقه‌ها با فرمول‌های ساده (فرمول‌های با سور کم) بیان می‌کنند. در ادامه مروری بر چکیده‌های این مقالات می‌کنیم.

اَنسکوب [۳] و کونیگزمن [۴] در منبع [۲] نشان داده‌اند که هرگاه $\mathbb{F}_q$ میدانی متناهی باشد، حلقه ارزیاب سری‌های توانی

[3] Anscombe
[4] Koenigsmann

$\mathbb{F}_q[[t]]$ در میدان $\mathbb{F}_q((t))$ در زبان حلقه‌ها به طور وجودی و بدون پارامتر تعریف‌پذیر است. روش اثبات آن‌ها به این صورت است که با استفاده از تعریف توپولوژی هنسلی، در ادامه کار پرستل و زیگلر [5]، یک همسایگی F_q– تعریف‌پذیر حول صفر پیدا کرده‌اند و با استفاده از لم هنسل یک تعریف با فرمول‌های به صورت $\exists$ برای زیرمجموعه‌ای از $\mathbb{F}_q[[t]]$ شامل $t\mathbb{F}_q[[t]]$ معرفی کرده‌اند. در نهایت با استفاده از این حقیقت که $\mathbb{F}_q$ با فرمول $x^q - x = ۰$ تعریف‌پذیر است، تعریف‌پذیری را حول $\mathbb{F}_q[[t]]$ گسترش داده‌اند و تعریفی بدون پارامتر معرفی کرده‌اند.
بعد از آن‌ها، آرنو فهن [6] در مقالهٔ [۵] روش استفاده شدهٔ آن‌ها را گسترش داد و تعریف‌پذیری میدان‌های هنسلیِ ارزیابی با میدان باقی ماندهٔ متناهی یا میدان سودو بستهٔ جبری را بررسی کرد. میدان‌های سودو بسته جبری در فصل دوم معرفی شده است. در واقع در این مقاله قضیهٔ زیر اثبات شده است:

قضیه ۱. فرض کنید K یک میدان ارزیابی هنسلی و O_v و k_v به ترتیب حلقهٔ ارزیاب و میدان باقی‌ماندهٔ آن باشند. اگر k_v متناهی و یا سودو بستهٔ جبری باشد و بخش جبری k_v بستهٔ جبری نباشد، آنگاه یک فرمول به صورت $\exists$ وجود دارد که حلقهٔ ارزیاب O_v را در میدان ارزیابی هنسلی K تعریف می‌کند.

یانکه [7] و کونیگزمن در مقالهٔ [۹] به این سوال پاسخ داده‌اند که چه زمانی حلقهٔ ارزیاب یک میدان ارزیابی ِهنسلی در زبان حلقه‌ها $\varnothing$– تعریف‌پذیر است. آن‌ها به این نتیجه رسیدند که این امکان پذیر نیست هرگاه میدان ما جدایی‌پذیر یا بسته حقیقی باشد. در مقالات مختلف پرستل و زیگلر مثال‌های زیادی از میدان‌های ارزیابیِ هنسلی وجود دارد که حلقهٔ ارزیاب آن‌ها $\varnothing$– تعریف‌پذیر نیستند. درمقاله [۹] شرایطی را روی میدان باقی مانده‌ها ارائه می‌دهند که $\varnothing$– تعریف‌پذیر بودن حلقهٔ ارزیاب را تضمین می‌کند. در واقع آن‌ها نشان داده‌اند حلقهٔ ارزیاب یک میدان ارزیابیِ هنسلی $\varnothing$– تعریف‌پذیر است هرگاه میدان باقی ماندهٔ آن بسته جدایی‌پذیر یا غیر هنسلی باشد.
بعد از آن پرستل با ارائهٔ محکی برای تعریف‌پذیری حلقه‌های ارزیاب در مقاله [۱۲] شرایطی را برای تعریف‌پذیری حلقه‌های ارزیابِ هنسلی با استفاده از فرمول‌های با پیچیدگیِ سوری کم را معرفی کرده است. در واقع در منطق برای ما مهم است که تعریف‌پذیری با چه نوع فرمولی باشد و فرمول‌های با سور کم مورد توجه هستند. با توجه به این محک که در فصل ۳ آورده شده است، پِرستل نشان داده است که اکثر تعاریفِ بدونِ پارامتر برای حلقه ارزیابِ هنسلی در زبانِ حلقه‌ها معادل با فرمول‌های بدون پارامترِ $\exists\forall$ یا $\forall\exists$ می‌باشند. سپس پِرستل این سوال را مطرح کرده است که آیا یک فرمولِ بدون پارامتر به صورت $\exists\forall$ یا به صورت $\forall\exists$ وجود دارد که حلقهٔ ارزیاب را در میدان ارزیابی هنسلی تعریف کند؟
در این پایان نامه یک مثالِ نقض برای سوال پرستل فراهم شده است. در واقع ما مثال مشخصِ $k = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})$ را بررسی می‌کنیم. در اینجا منظور از $\mathbb{Q}^{tot\mathbb{R}}$ میدان اعداد حقیقی کامل هستند که توسیعِ ماکسیمال $\mathbb{Q}$ هستند به طوری که تصویرِ هر نشاندن این میدان به اعداد مختلط، زیرمجموعهٔ اعداد حقیقی است.
میدانِ $\mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})$ مثالی از یک میدان سودو بستهٔ جبری است. منظور از میدان سودو بستهٔ جبری میدانی است که در هر توسیع میدانی منتظم به طور وجودی بسته است. در این پایان‌نامه نشان خواهیم داد که $\mathcal{L}_{ring}$– فرمولی وجود دارد که حلقهٔ ارزیاب O_w را در میدان ارزیابیِ $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})((\Gamma_۱))((\Gamma_۲))$ تعریف می‌کند اما O_w با هیچ فرمولِ به صورت $\exists\forall$ یا $\forall\exists$ تعریف‌پذیر نیست. منظور از $K((\Gamma_۱))$ مجموعهٔ سری‌های هان است که اگر روی آن نگاشت ارزیابی

[5] Ziegler [6] Arno Fehn [7] Jahnke

تعریف کنیم، آنگاه حلقهٔ ارزیاب آن $K[[\Gamma_۱]]$ است. در بخش ۸.۲ نشان می‌دهیم $K((\Gamma_۱))$ یک میدان است بنابراین می‌توان میدان ارزیابی سری‌های هان $K = k((\Gamma_۱))((\Gamma_۲))$ را تعریف کرد که حلقهٔ ارزیاب آن $O_w = k((\Gamma_۱))[[\Gamma_۲]]$ است. در ادامه قضیهٔ مهم این پایان‌نامه و اثبات آن به اختصار گفته می‌شود.
در واقع هدف اصلی این پایان‌نامه اثبات قضیهٔ زیر است:

قضیه ۲. گروه‌های آبلی مرتب $\Gamma_۱$ و $\Gamma_۲$ وجود دارند به طوری که برای هر میدان سودو بستهٔ جبری که با بستار جدایی‌پذیرش برابر نباشد($k \neq k^{sep}$) حلقه ارزیابِ $O_w = k((\Gamma_۱))[[\Gamma_۲]]$ در میدان ارزیابی هنسلی $K = k((\Gamma_۱))((\Gamma_۲))$ بدون پارامتر تعریف‌پذیر است، اما O_w با هیچ فرمولِ $\exists\forall$ و $\forall\exists$ در زبان حلقه‌ها تعریف‌پذیر نیست.

برای اثبات قضیهٔ فوق از محکی که پرستل برای تعریف‌پذیری محمول تک‌موضعی O در ساختار (K, O) در منبعِ [۱۲] ارائه کرده است و در فصل آخر این پایان نامه اثبات آن آورده شده، بهره خواهیم برد. در اینجا $K_۱ \prec_\exists K_۲$ به این معنی است که $K_۱$ از نظر وجودی در $K_۲$ بسته است. برای مثال، هر $\mathcal{L}_{ring}$ فرمول وجودی $\rho(x_۱, x_۲, ...)$ در $K_۱$ که در $K_۲$ برآورده می‌شود در $K_۱$ نیز برآورده می‌شود. محک پرستل بیان می‌کند اگر O یک محمول تک موضعی در ساختار (K, O) باشد، آنگاه O توسط یک فرمولِ $\exists\forall$ بدون پارامتر در زبان حلقه‌ها تعریف می‌شود، اگر در تئوری از اینکه $K_۱ \prec_\exists K_۲$ نتیجه بگیریم $O_۱ \subseteq O_۲$. بالعکس اگر $(K_۱, O_۱)$ و $(K_۲, O_۲)$ دو مدل از تئوری باشند، اگر از اینکه $K_۱ \prec_\exists K_۲$ نتیجه بگیریم $O_۱ \subseteq O_۲$ آنگاه در هر مدل (K, O) از این تئوری O توسط یک فرمول ِ$\exists\forall$ تعریف می‌شود. همچنین محک پرستل برای فرمول‌های به صورت $\exists$، $\forall$ و $\forall\exists$ بیان شده است که در این پایان‌نامه، فقط تعریف‌پذیری حلقه‌های ارزیاب با فرمول‌های ِ$\exists\forall$ و $\forall\exists$ بررسی خواهد شد. مانند حالت $\exists\forall$ برای تعریف‌پذیری محمول تک‌موضعی در یک ساختار داریم:

$$\forall\exists \text{ iff } (K_۱ \prec_\exists K_۲ \Rightarrow O_۲ \cap K_۱ \subseteq O_۱)$$

در ادامه مختصری از روند اثبات قضیهٔ ۸۹ را بیان می‌کنیم. گروه‌های آبلی مرتب X و Y را به صورت زیر در نظر بگیرید.

$$X := \mathbb{Z}_{(۲)} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, ۲ \nmid b, (a, b) = ۱\}$$

$$Y := \mathbb{Z}_{(۳)} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, ۳ \nmid b, (a, b) = ۱\}$$

اگر $(\mathbb{N}, <)$ مجموعهٔ اعداد طبیعی با ترتیب معمول و $(\mathbb{N}', <)$ مجموعهٔ اعداد طبیعی با عکس ترتیب معمول باشد، آنگاه گروه‌های $\Gamma_۱$ و $\Gamma_۲$ و Γ را به صورت زیر را تعریف می‌کنیم:

$$\Gamma_۱ := \bigoplus_{\mathbb{N}}((\bigoplus_{\mathbb{N}}) \oplus X)$$

$$\Gamma_۲ := \bigoplus_{\mathbb{N}'}(X \oplus Y)$$

$$\Gamma := \Gamma_۲ \oplus \Gamma_۲$$

با توجه به قضیهٔ اکس-کوچن و ارشف [8] برای اینکه میدان ارزیابی دیگرِ $(K_۱, w, k, \Gamma_۱)$ را در یک میدان ارزیابی $(K_۲, u, k', \Gamma_۲)$ به صورت بستهٔ وجودی بنشانیم، کافی است میدان باقی ماندهٔ k و گروه ارزیاب $\Gamma_۱$ را به ترتیب، به صورت بستهٔ وجودی در k' و گروه ارزیاب $\Gamma_۲$ بنشانیم. بنابراین جهت آنکه نشان دهیم $K \prec_{\exists} K$، دو نشاندن بستهٔ وجودی از گروه ارزیاب در بخش ۴.۳ ارائه می‌دهیم و جهت نشاندن میدان باقی‌مانده k همان نگاشت همانی id_k را در نظر می‌گیریم و در آخر نشان می‌دهیم $O \subsetneq O$ و $O \subsetneq O \cap K$. در نتیجه با توجه به محک پرستل حلقهٔ ارزیاب O_w با هیچ فرمول به صورت $\exists\forall$ و $\forall\exists$ در زبان حلقه‌ها تعریف‌پذیر نیست. اما دقت می‌کنیم که حلقهٔ ارزیاب O_w در میدان ارزیابی مورد نظر، بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است. این حقیقت را با بررسی میدان ارزیابی هنسلیِ $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})((\Gamma_۱))((\Gamma_۲))$ به طور خاص نشان می‌دهیم.

فصل‌بندی پایان‌نامه به صورت زیر است:

در فصل اول مفاهیم مقدماتی مورد نیاز نظریهٔ مدل همچون تعاریف مقدماتی منطق پرداخته شده است. در بخش بعدی محمول تک‌موضعی با ذکر چندمثال توضیح داده شده است که درفصل‌های بعدی به کرات مورد استفاده قرار می‌گیرد. در انتهای فصل به مفاهیم تعریف‌پذیری و تعبیرپذیری پرداخته شده است.

در فصل دوم به مطالعهٔ مفاهیم جبری مورد استفاده شده در روند مطالعهٔ این پایان نامه پرداخته شده است. انواع توسیع‌های میدانی معرفی شده و حلقه‌های نرم‌دار مانند هنسلی و p-ادیک ها آورده شده است.همچنین در بحثی کوتاه در مورد زیرگروه‌های محدب شده است . علاوه بر آن میدان‌های ارزیابی در این فصل مطالعه شده است و گزاره‌هایی در آن مرور شده است.

در آخر در فصل سوم ابتدا مسیر اثبات قضیهٔ ۲ گفته شده است و بعد از آن به مقاله پرداخته شده است و مواردی که پیش‌تر گفتیم مورد بررسی و بحث قرار گرفته است.

[8] Ax-Kochen and Eršov

فصل ۱

مقدماتی بر نظریهٔ مدل‌ها

در این فصل ابتدا به مفاهیم مقدماتی نظریهٔ مدل می‌پردازیم. در ادامه به محمول تک موضعی و مثال‌هایی از آن می‌پردازیم که منظور از افزودن محمول تک موضعی به زبان، جدا کردن بخشی از ساختار در زبان است. همچنین مفاهیمی از قبیل زیرساختار مقدماتی، بستهٔ وجودی، تئوری کامل و رتبه سوری را مرور می‌کنیم و قضایا و گزاره‌های مورد نیاز این پایان نامه را می‌خوانیم. در آخر مفاهیم تعریف‌پذیری و تعبیرپذیری را با ذکر چند مثال تعریف می‌کنیم.

۱.۱ مفاهیم مقدماتی

توجه ۳. جهت مختصر بودن این بخش تعاریفی که برای زبان، ساختار، ترم و فرمول گفته شد تعاریف دقیقی نیستند. خواننده می‌تواند تعاریف دقیق را درکتاب‌های مرجع در نظریهٔ مدل مانند کتاب نظریهٔ مدل از دیوید مارکر [1] مطالعه کند.

یک زبانِ مرتبهٔ اولِ $\mathcal{L}$ یک مجموعهٔ متشکل از نمادهایی برای توابع، نمادهایی برای روابط و نمادهایی برای ثوابت است. اگر F نمادی برای توابع و R نمادی برای روابط C و نمادی برای ثوابت در زبان باشند آنگاه $\mathcal{L} = F \cup R \cup C$. در منطق مرتبهٔ اول جملات باید در ساختارها معنا شوند. منظور از یک $\mathcal{L}-$ ساختار جفتی به صورت زیر است:

$$\mathcal{M} = (M, (\mathcal{Z}^{\mathcal{M}})_{\mathcal{Z}\in\mathcal{L}})$$

که متشکل از یک مجموعهٔ M است به نام جهان آن $\mathcal{L}$ ساختار، و همچنین برای هر نمادِ $\mathcal{Z} \in \mathcal{L}$ یک مابازای $\mathcal{Z}^{\mathcal{M}}$ وجود دارد که به آن تعبیر (معنای)نماد $\mathcal{Z}$ در ساختار $\mathcal{M}$ گفته می‌شود.

[1] David Marker

فرض کنید $\mathcal{L}$ یک زبان مرتبهٔ اول باشد. یک مجموعه $x_1, x_2, \ldots$ 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 $\mathcal{L}$ ترم یا یک $\mathcal{L}$ کلمه گویند. دقت کنید که هر دنبالهٔ دلخواه از ثوابت و توابع و متغیرها ترم نیست. به عنوان مثال در زبان حلقه‌ها $\mathcal{L}_r = \{+, -, ., 0, 1\}$ موارد زیر ترم هستند:

$$1 + 0$$

$$x_1 + x_2 + x_3$$

ما می‌توانیم ترم‌ها را در ساختاری تعبیر کنیم. فرض کنید $\mathcal{M}$ یک $\mathcal{L}-$ ساختار باشد. فرض کنید $t(x_1, \ldots, x_n)$ یک $\mathcal{L}-$ ترم باشد و $a_1, \ldots, a_n \in M$. در این صورت عنصری در جهان ساختارِ $\mathcal{M}$ وجود دارد که آن را با $t^{\mathcal{M}}(a_1, \ldots, a_n)$ (تعبیر ترم t در ساختار $\mathcal{M}$ با جایگذاری a_i به جای x_i) نشان می‌دهیم. به عنوان مثال در زبان حلقه‌ها در ساختار $\mathcal{R} = (\mathbb{R}, +, -, ., 0, 1)$ داریم،

$$(2x_1x_2 + x_3^4)^{\mathcal{R}}(1, 2, 3) = 2(1)(2^2) + 3^4 = 89$$

به بیان واضح‌تر زبان حکم حروف الفبا را دارد و ترم‌ها حکم کلمه‌ها را. بعد از آن، فرمول‌ها دنباله‌هایی متناهی هستند که با استفاده از ترم‌های زبان، علائم منطقی و $\wedge$ و $\exists$ و $\vee$ و علامت تساوی ساخته می‌شوند. برای مثال $\exists x(x.x = -1)$ فرمولی در زبان حلقه‌هاست.
متغیر x را در فرمول φ آزاد گوییم هرگاه تحت تاثیر هیچ سوری نباشد در غیر اینصورت آن را پایبند می‌نامیم. مثلا در فرمول $((\forall x\psi(x)) \wedge R(x, y))$ متغییر x اول پایبند و x دوم و متغیر y آزاد است.

تعریف ۴. فرض کنید $\varphi(x_1, \ldots, x_n)$ یک $\mathcal{L}$–فرمول و $\mathcal{M}$ یک $\mathcal{L}-$ ساختار باشد و $a_1, \ldots, a_n \in M$. منظور از $\varphi(x_1, \ldots, x_n)$ این است که متغیرهای $x_1, \ldots, x_n$ متغیر آزاد هستند. عبارت $\mathcal{M} \models \varphi(a_1, \ldots, a_n)$ برقرار است هرگاه فرمول φ با جایگذاری a_i به جای x_i در ساختار $\mathcal{M}$ درست باشد در اینصورت گوییم $\mathcal{M}$ مدلی برای این فرمول است.

مانند ترم‌ها، فرمول‌ها نیز در ساختارها تعبیر می‌شوند. به عنوان مثال فرمول یکسان $\exists x(x.x = -1)$ در دو $\mathcal{L}_{ring}-$ ساختار $(\mathbb{R}, +, -, ., 0, 1)$ و $(\mathbb{C}, +, -, ., 0, 1)$ تعبیر می‌شود اما در یکی درست و در یکی نادرست است:

$$(\mathbb{C}, +, -, ., 0, 1) \models \exists x(x.x = -1)$$

$$(\mathbb{R}, +, -, ., 0, 1) \not\models \exists x(x.x = -1).$$

مفهوم بعدی که می‌خواهیم در موردش صحبت کنیم $\mathcal{L}-$ جمله است. منظور از یک $\mathcal{L}-$ جمله یک $\mathcal{L}-$ فرمولِ بدون متغیر آزاد است. برای مثال در زبان $\mathcal{L}_r = \{+, -, ., 0, 1\}$ فرمول‌های زیر جمله‌اند.

$$\forall x \exists y(x + y = 0)$$

$$\forall x \exists y (x.y = \circ)$$

همانند فرمول‌ها، جمله‌ها نیز در ساختارها تعبیر می‌شوند. به عنوان مثال فرمول زیر در یک ساختار درست و در ساختاری دیگر نادرست است:

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

در حالی که

$$\mathbb{R} \not\models \exists x (x^{۲} = -۱)$$

یکی از اهداف مهم در نظریهٔ مدل ارائه‌ی اصول موضوعه برای بخش‌هایی از ریاضی است. این کار تحت تئوری‌ها صورت می‌گیرد. منظور از یک $\mathcal{L}$- تئوری مجموعه‌ای از $\mathcal{L}$- جمله‌هاست. برای مثال در زبان حلقه‌ها یعنی $\mathcal{L}_{ring} = \{+, -, , , \circ, ۱\}$، تئوری حلقه‌ها به صورت زیر است.

$$T = \{\forall x\, (x + \circ = \circ + x = x)$$
$$\forall x, y, z\, (x + (y + z) = (x + y) + z)$$
$$\forall x (\exists y\, x + y = \circ)$$
$$\forall x, y\, (x + y = y + x)$$
$$\forall x, y, z\, ((x.y).z = x.(y.z))$$
$$\forall x\, (x \cdot ۱ = x)$$
$$\forall x, y, z\, (x.(y + z) = (x.y) + (x.z))$$
$$\forall x, y, z ((y + z).x = (y.x) + (z.x))\}$$

و تئوری میدان‌ها به صورت زیر است:

$$T_{field} = T_{ring} \cup \{\forall x (x \neq \circ \to \exists y \quad xy = ۱)\}$$

مسالهٔ مهم در تئوری مرتبهٔ اول این است که آیا تئوری ما مدل دارد یا نه. برای مثال در زبان حلقه‌ها تئوری $T = \{\forall x \exists y (x + y = ۱), \forall x \neg (\exists y (x + y = ۱))\}$ هیچ مدلی ندارد زیرا که در هیچ ساختاری این دو جمله همزمان نمی‌توانند درست باشند.

تعریف ۵. تئوری T سازگار است هرگاه حداقل یک مدل داشته باشد.

این موضوع برای فرمول‌ها نیز صدق می‌کند. موضوع مهم این ست که یک تئوری نسبت به فرمولی چگونه است یعنی در برخی مدل‌های تئوری فرمول درست و در برخی دیگر نباشد. برای مثال زبان $\mathcal{L}_{ring}$ را در نظر بگیرید. می‌دانیم $\mathbb{R} \models \mathcal{L}_{ring}$ و $\mathbb{C} \models \mathcal{L}_{ring}$ با این حال $\mathbb{C} \models \exists x (x^{۲} = -۱)$ ولی $\mathbb{R} \not\models \exists x (x^{۲} = -۱)$. در این حالت گوییم تئوری نسبت به فرمول بی تفاوت است.

اگر در تئوری هر $\mathcal{L}$ فرمول و یا نقیض آن در تمام مدل‌های تئوری T درست باشد، گوییم تئوری T کامل است.

توجه ۶. فرض کنید $\mathcal{M}$ یک $\mathcal{L}$- ساختار باشد، تئوری $Th(\mathcal{M})$، مجموعه‌ای از جمله‌هایی مانند φ است به طوری که $\mathcal{M} \models \varphi$. اگر $\mathcal{M}$ یک $\mathcal{L}$- ساختار باشد، آنگاه $\mathcal{M}$ مدلی برای تئوری $Th(\mathcal{M})$ است. در واقع همیشه $\mathcal{M} \models Th(\mathcal{M})$ برقرار است.

تعریف ۷ (هم ارز مقدماتی ساختارها). دو $\mathcal{L}$- ساختار $\mathcal{M}$ و $\mathcal{N}$ را هم ارز مقدماتی گوییم و می‌نویسیم $\mathcal{M} \equiv \mathcal{N}$، هرگاه برای هر $\mathcal{L}$- جملهٔ φ داشته باشیم

$$\mathcal{M} \vDash \varphi \Longleftrightarrow \mathcal{N} \vDash \varphi$$

به بیان دیگر دو ساختار $\mathcal{M}$ و $\mathcal{N}$ زمانی هم ارز مقدماتی هستند که

$$Th(\mathcal{M}) = Th(\mathcal{N}).$$

برای مثال زبان حلقه‌ها و عدد ثابت p را در نظر بگیرید. آنگاه $(\mathbb{R}, +, ., ۰, ۱) \not\equiv (\mathbb{F}_p, +, ., \bar{۰}, \bar{۱})$ زیرا اگر جملهٔ $\varphi = \forall x \ \ x + x + \ldots + x = \bar{۰}$ باشد آنگاه داریم $\mathbb{F}_p \models \varphi$ ولی $\mathbb{R} \nvDash \varphi$.

دو تئوری T و T' را معادل می‌نامیم و می‌نویسیم $T \equiv T'$ هرگاه کلاس مدل‌های T دقیقاً همان کلاس مدل‌های T' باشد.
قضیهٔ فشردگی یک محک است برای بررسی این که چه زمانی یک تئوری بزرگ دارای مدل است. قضیهٔ فشردگی در اثبات بسیاری از گزاره‌ها در نظریهٔ مدل استفاده شده است و ما آن را بدون اثبات بیان می‌کنیم.

قضیه ۸ (قضیهٔ فشردگی). فرض کنیم T یک تئوری مرتبه اول باشد، در این صورت T دارای یک مدل است اگر هر زیرمجموعهٔ متناهی $\Delta \subseteq T$ دارای مدل باشد.

تعریف ۹ (نشاندن). فرض کنید $\mathcal{L}$ یک زبان و $\mathcal{M}$ و $\mathcal{N}$ دو $\mathcal{L}$- ساختار باشند. $e : \mathcal{M} \longrightarrow \mathcal{N}$ یک $\mathcal{L}$- نشاندن است هرگاه ویژگی های زیر را داشته باشد:

۱. به ازای هر $f \in F$ نماد تابعی n- متغیر و به ازای هر $a_۱, a_۲, \ldots, a_n \in \mathcal{M}$ داشته باشیم

$$e(f^{\mathcal{M}}(a_۱, a_۲, \ldots, a_n)) = f^{\mathcal{N}}(e(a_۱), \ldots, e(a_n))$$

۲. به ازای هر $R \in \mathcal{R}$ نماد رابطه‌ای m- موضعی و به ازای هر $a_۱, a_۲, \ldots, a_n \in \mathcal{M}$ داشته باشیم

$$(a_۱, a_۲, \ldots, a_n) \in \mathcal{R}^{\mathcal{M}} \longleftrightarrow (e(a_۱), e(a_۲), \ldots, e(a_n)) \in \mathcal{R}^{\mathcal{N}}$$

۳. به ازای هر $c \in \mathcal{C}$ داشته باشیم:

$$e(c^{\mathcal{M}}) = c^{\mathcal{N}}$$

مثلا اگر $\mathcal{L} = \{(*, ۲) \cup \{c\}$ و $\mathcal{L}$- ساختار $(\mathbb{Z}, +, ۰)$ را در نظر بگیریم. تابع

$$e : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$X \longmapsto ۲X$$

یک تابع $\mathcal{L}$ نشاندن است زیرا اگر نماد تابعی $*$ را در $\mathbb{Z}$ برابر $+$ تعبیر کنیم و c را برابر عدد ۰ تعبیر کنیم آنگاه داریم

$$e(a+b) = ۲(a+b) = ۲(a) + ۲(b) = e(a) + e(b)$$

$$e(c^{\mathbb{Z}}) = e(۰) = ۲ \cdot ۰ = ۰$$

تعریف ۱۰ (نشاندن مقدماتی). فرض کنید $\mathcal{M}$ و $\mathcal{N}$ دو $\mathcal{L}$- ساختار باشند. نگاشت $f : \mathcal{M} \longrightarrow \mathcal{N}$ را یک نشاندن مقدماتی می‌نامیم هرگاه برای هر $\bar{m} \in \mathcal{M}$ و هر فرمول φ داشته باشیم:

$$\mathcal{M} \models \varphi(\bar{m}) \Longleftrightarrow \mathcal{N} \models (\varphi(f(\bar{m}))).$$

تعریف ۱۱. (زیرساختار) فرض کنید $\mathcal{M}$ و $\mathcal{N}$ دو $\mathcal{L}$- ساختار باشند، گوییم $\mathcal{M}$ زیرساختار $\mathcal{N}$ است و می‌نویسیم $\mathcal{M} \subseteq \mathcal{N}$، هرگاه نگاشت شمول (یعنی نگاشت همانی) $i : M \longrightarrow N$ یک نشاندن باشد.

همیشه فرمول‌های بدون سور تحت زیرساختارها بسته هستند به بیان دیگر اگر $\mathcal{M} \subseteq \mathcal{N}$ برای هر فرمولِ بدون سور $\varphi(x_۱, \dots, x_n)$ و هر $m_۱, \dots, m_k \in \mathcal{M}$ داریم:

$$\mathcal{M} \models \varphi(m_۱, \dots, m_k) \Longleftrightarrow \mathcal{N} \models \varphi(m_۱, \dots, m_k).$$

اگر $\mathcal{M}$ یک $\mathcal{L}$- ساختار باشد، مجموعهٔ تمام فرمول‌های بدون سور با پارامترهای در $\mathcal{L}$- ساختار $\mathcal{M}$ که در $\mathcal{M}$ برقرارند را با $Diag(\mathcal{M})$ نشان می‌دهیم. به بیان دیگر

$$Diag(\mathcal{M}) = \{\varphi(m_۱, \dots, m_k) | \varphi(x_۱, \dots, x_k) \in \mathcal{L}, m_۱, \dots, m_k \in \mathcal{M}, \mathcal{M} \models \varphi(m_۱, \dots, m_k), \varphi \text{بدون سور}\}$$

$$eDiag(\mathcal{M}) = \{\varphi(m_۱, \dots, m_k) | \varphi(x_۱, \dots, x_k) \in \mathcal{L}, m_۱, \dots, m_k \in \mathcal{M}, \mathcal{M} \models \varphi(m_۱, \dots, m_k)\}.$$

تعریف ۱۲ (زیرساختار مقدماتی). فرض کنید $\mathcal{M}$ و $\mathcal{N}$ دو $\mathcal{L}$- ساختار باشند به طوری که $\mathcal{M} \subseteq \mathcal{N}$، گوییم $\mathcal{M}$ زیرساختار مقدماتی $\mathcal{N}$ است و می‌نویسیم $\mathcal{M} < \mathcal{N}$، هرگاه برای هر $\mathcal{L}$- فرمول $\varphi(\bar{x})$ و هر چندتایی $\bar{a} \in \mathcal{M}$ داشته باشیم:

$$\mathcal{M} \models \varphi(\bar{a}) \Longleftrightarrow \mathcal{N} \models \varphi(\bar{a}).$$

به عنوان مثال می‌دانیم $(\mathbb{Z}, <)$ زیر ساختارِ $(\mathbb{Q}, <)$ است اما $(\mathbb{Z}, <)$ زیرساختارِ مقدماتی $(\mathbb{Q}, <)$ نیست زیرا $(\mathbb{Q}, <) \models \exists x \;\; ۲ < x < ۳$ در حالی که $(\mathbb{Z}, <) \not\models \exists x \;\; ۲ < x < ۳$.
گفتیم که در منطق برای ما وجود تئوری حائز اهمیت است. فرض کنید $\mathbb{K}$ کلاسی از $\mathcal{L}$- ساختارها باشد. می‌گوییم کلاس $\mathbb{K}$ دارای اصل‌بندی است هرگاه یک تئوری مرتبهٔ اول T وجود داشته باشد به طوری که $\mathbb{K} = \{\mathcal{M} | \mathcal{N} \models T\}$. به عنوان مثال میدان‌های با مشخصهٔ صفر دارای اصل‌بندی هستند:

$$T = T_{field} \cup \{۱ + ۱ \neq ۰, ۱ + ۱ + ۱ \neq ۰, \dots\}.$$

دو تئوری T و T' را معادل می‌نامیم و می‌نویسیم $\mathrm{T} \equiv \mathrm{T}'$، هرگاه کلاس مدل‌های T دقیقا همان کلاس مدل‌های T' باشد، یعنی برای هر $\mathcal{L}$- ساختار $\mathcal{M}$ داشته باشیم:

$$\mathcal{M} \models \mathrm{T} \longleftrightarrow \mathcal{M} \models \mathrm{T}'.$$

تعریف ۱۳ (اصل‌بندی عمومی). تئوری T دارای اصل‌بندی عمومی است هرگاه تئوری T' موجود باشد که همه جملات موجود در T' به صورت $\forall x_1, \ldots, x_n \quad \varphi(x_1, \ldots, x_n)$ باشند به طوری که $\varphi(x_1, \ldots, x_n)$ بدون سور باشد و $\mathrm{T} \equiv \mathrm{T}'$.

قضیه ۱۴. تئوری T دارای اصل‌بندی عمومی است اگر و تنها اگر کلاس مدل‌های این تئوری تحت زیرساختارها بسته باشد یعنی هرگاه $\mathcal{N} \models \mathrm{T}$ و $\mathcal{M} \subseteq \mathcal{N}$ آنگاه $\mathcal{M} \models \mathrm{T}$.

اثبات. ($\Leftarrow$) فرض کنید T دارای اصل‌بندی عمومی باشد و $\mathcal{N} \models \mathrm{T}$ و $\mathcal{M} \subseteq \mathcal{N}$ ، نشان می‌دهیم $\mathcal{M} \models \mathrm{T}$. فرض کنید برای هر $x_1, \ldots, x_n$ داریم $\varphi(x_1, \ldots, x_n) \in \mathrm{T}$ که $\varphi(x_1, \ldots, x_n)$ یک فرمول بدون سور است چون $\mathcal{N} \models \forall x_1, \ldots, x_n \, \varphi(x_1, \ldots, x_n)$ پس به ازای هر $n_1, \ldots, n_n \in \mathcal{N}$ داریم $\mathcal{N} \models \varphi(n)$. حال فرض کنید $m \in \mathcal{M}$ داریم $\mathcal{N} \models \varphi(m)$ و φ یک فرمول بدون سور است پس $\mathcal{M} \models \varphi(m)$ و چون m عنصری دلخواه بود پس $\mathcal{M} \models \forall x \, \varphi(x)$.

($\Rightarrow$) برعکس فرض کنید کلاس مدل‌های تئوری T تحت زیرساختارها بسته باشد، نشان می‌دهیم که یک تئوری $\mathrm{T} \equiv \mathrm{T}'$ موجود است به طوری که تمام جملات T' تنها با سور عمومی نوشته شده اند. قرار دهید:

$$\mathrm{T}' = \{\varphi | \mathrm{T} \models \varphi, \text{عمومی است } \varphi\}.$$

فرض کنید $\mathcal{M} \models \mathrm{T}'$ ادعا می‌کنیم $\mathcal{M} \models \mathrm{T}$. مجموعهٔ $Diag(\mathcal{M}) \cup \mathrm{T}$ را در زبان $\mathcal{L}_{\mathcal{M}} = \mathcal{L} \cup \{c_{\mathcal{M}} | c \in M\}$ در نظر بگیرید.

ادعای اول: $Diag(\mathcal{M}) \cup \mathrm{T}$ دارای مدل است.

ادعای دوم: از ادعای اول حکم قضیه نتیجه می‌شود.

اثبات ادعای دوم: اگر $\mathcal{N} \models Diag(\mathcal{M}) \cup \mathrm{T}$ آنگاه $\mathcal{N} \overset{\mathcal{L}}{\models} \mathrm{T}$ و $\mathcal{N} \overset{\mathcal{L}_{\mathcal{M}}}{\models} Diag(\mathcal{M})$ پس $\mathcal{M} \subseteq \mathcal{N} \models \mathrm{T}$ بنابراین کلاس مدل‌های T تحت زیرساختارگیری بسته است نتیجه می‌گیریم که $\mathcal{M} \models \mathrm{T}$.

اثبات ادعای اول: $Diag(\mathcal{M}) \cup \mathrm{T}$ یک تئوری در زبان $\mathcal{L}_{\mathcal{M}}$ است. بنا به قضیه فشردگی برای اثبات این که تئوری فوق دارای مدل است کافی است نشان دهیم که هر بخش متناهی از آن دارای مدل است. فرض کنید $\Delta \subseteq Diag(\mathcal{M}) \cup \mathrm{T}$ متناهی دارای مدل نباشد. بنابراین جملهٔ $\varphi(m) \in Diag(\mathcal{M})$ یافت می‌شود به طوری که $\{\varphi(m)\} \cup \mathrm{T}$ دارای مدل نیست یعنی اگر $\mathcal{M} \models \mathrm{T}$ آن‌گاه $\mathcal{M} \models \neg\varphi(m)$. پس $\mathrm{T} \overset{\mathcal{L}_{\mathcal{M}}}{\models} \neg\varphi(\mathrm{m})$ بنابراین در زبان $\mathcal{L}$ داریم $\mathrm{T} \overset{\mathcal{L}}{\models} \forall \mathrm{x} \, \neg\varphi(\mathrm{x})$ یعنی $\forall x \neg\varphi(x)$ یک نتیجه عمومی از تئوری T است یعنی $\forall x \neg\varphi(x) \in \mathrm{T}'$. از طرفی $\mathcal{M} \models \mathrm{T}'$ پس $\mathcal{M} \models \forall x \neg\varphi(x)$ و این غیر ممکن است زیرا $\varphi(m) \in Diag(\mathcal{M})$. $\square$

به عنوان مثال $Th(\mathbb{C})$ اصل‌بندی عمومی ندارد زیرا $\mathbb{C} \models Th(\mathbb{C})$ و $(\mathbb{R}, +, -, ., ۰, ۱) \subseteq (\mathbb{C}, +, -, ., ۰, ۱)$ اما $\mathbb{R} \nvDash Th(\mathbb{C})$.

گزاره ۱۵ (محک تارسکی). فرض کنید $\mathcal{M}$ و $\mathcal{N}$ دو $\mathcal{L}-$ ساختار باشند به طوری که $\mathcal{M} \subseteq \mathcal{N}$. در این صورت شرایط زیر هم ارزند:

(i) : $\mathcal{M}$ زیر ساختار مقدماتی $\mathcal{N}$ است. ($\mathcal{M} < \mathcal{N}$)

(ii) : به ازای هر $\mathcal{L}-$ فرمول $\varphi(x_1, \ldots, x_n)$ و به ازای هر $a_1, \ldots, a_n \in M$ اگر $\mathcal{N} \models \exists x \ \ \varphi(x, a_1, \ldots, a_n)$ آنگاه عنصر $a \in M$ موجود است به طوری که $\mathcal{N} \models \varphi(a, a_1, \ldots, a_n)$.

تعریف ۱۶ (تئوری میدان‌های مدل‌کامل). تئوری T را مدل‌کامل می‌نامیم هرگاه برای هر $\mathcal{M}, \mathcal{N} \models \mathrm{T}$ اگر $\mathcal{M} \subseteq \mathcal{N}$ باشد آنگاه $\mathcal{M} \leq \mathcal{N}$.

قضیه ۱۷. تئوری T مدل‌کامل است اگر و تنها اگر هر فرمول $\varphi(\bar{x})$ نسبت به T دارای یک معادل عمومی باشد. به بیان دیگر برای هر فرمول $\varphi(x)$ یک فرمول به صورت $\chi(\bar{x}) : \forall \bar{y} \psi(\bar{x}, \bar{y})$ که $\psi(\bar{x}, \bar{y})$ بدون سور است وجود دارد به طوری که $\mathrm{T} \models \varphi(\bar{\mathrm{x}}) \leftrightarrow \chi(\bar{\mathrm{x}})$.

اثبات. فرض کنید تئوری T مدل‌کامل و $\varphi(\bar{x})$ یک فرمول دلخواه باشد. قرار دهید :

$$\Gamma(\bar{x}) = \{\chi(\bar{x}) | \mathrm{T} \vdash \varphi(\bar{\mathrm{x}}) \to \chi(\bar{\mathrm{x}}), \text{یک فرمول عمومی است} \chi(\bar{\mathrm{x}})\}.$$

ادعای اول : $\mathrm{T} \cup \Gamma(\bar{\mathrm{x}}) \models \varphi(\bar{\mathrm{x}})$.

ادعای دوم : از ادعای اول حکم نتیجه می‌شود.

اثبات ادعای دوم: اگر ادعا برقرار باشد، بنابر قضیهٔ فشردگی، فرمول‌های $\chi_1, \ldots, \chi_n \in \Gamma(\bar{x})$ موجودند به طوری که $\mathrm{T} \vdash (\chi_1 \wedge \ldots \wedge \chi_n \Leftrightarrow \varphi)$. توجه کنید که می‌دانیم $\forall x \varphi(x) \wedge \forall \psi(x) \Leftrightarrow \forall x (\varphi(x) \wedge \psi(x))$.

اثبات ادعای اول: فرض کنید $\mathrm{T} \cup \Gamma(\bar{\mathrm{x}}) \cup \{\neg \varphi(\mathrm{x})\}$ سازگار باشد. مثلاً فرض کنید $(\mathcal{M}, \bar{a}) \models \mathrm{T} \cup \Gamma(\mathrm{x}) \cup \{\neg \varphi(\mathrm{x})\}$. هدف پیدا کردن مدلِ $\mathrm{T} \models \mathcal{N} \supseteq \mathcal{M}$ است. نشان می‌دهیم تئوری $\mathrm{Diag}(\mathcal{M}) \cup \mathrm{T} \cup \{\varphi(\bar{\mathrm{a}})\}$ سازگار است. اگر تئوری ناسازگار باشد، بنا به قضیهٔ فشردگی داریم:

$$\mathrm{T} \vdash \varphi(\bar{\mathrm{a}}) \to \neg \psi(\bar{\mathrm{m}}, \bar{\mathrm{a}})$$

$$\Rightarrow \mathrm{T} \vdash \varphi(\bar{\mathrm{x}}) \to \forall \mathrm{y} \ \ \neg \psi(\bar{\mathrm{y}}, \bar{\mathrm{x}})$$

$$\Rightarrow \forall y \ \ \neg \psi(\bar{y}, \bar{x}) \in \Gamma(\bar{x})$$

$$\Rightarrow \mathcal{M} \models \forall \bar{y} \ \ \neg \psi(\bar{y}, \bar{a})$$

اما می‌دانیم $\mathcal{M} \models \psi(\bar{m}, \bar{a})$ پس به تناقض می‌رسیم.

برعکس فرض کنید هر فرمول دارای معادل عمومی است. اگر $\mathcal{M} \subseteq \mathcal{N}$ و $\bar{a} \in M$ و $\varphi(\bar{x})$ دلخواه باشد.

$$\mathcal{M} \models \varphi(\bar{a})$$

$$\Rightarrow \mathcal{M} \models \exists \bar{y} \psi(\bar{a}, \bar{y})$$

$$\Rightarrow \mathcal{N} \models \exists \bar{y} \psi(\bar{a}, \bar{y})$$

$$\Rightarrow \mathcal{N} \models \varphi(\bar{a})$$

و عکس هم به همین صورت ثابت می‌شود. در نتیجه نشان دادیم $\mathcal{M} \models \varphi(\bar{a}) \Leftrightarrow \mathcal{N} \models \varphi(\bar{a})$. □

نتیجه ۱۸. تئوری T مدل کامل است اگر و تنها اگر هر فرمول دارای معادلی وجودی باشد.

اثبات. روند اثبات مانند قضیهٔ قبل است. □

تعریف ۱۹ (بستهٔ وجودی). فرض کنید $\mathcal{M}, \mathcal{N} \models \mathrm{T}$ و $\mathcal{M} \subseteq \mathcal{N}$ می‌گوییم $\mathcal{M}$ در $\mathcal{N}$ به طور وجودی بسته است هرگاه $\mathcal{M} \models \exists \bar{y} \psi(\bar{m}, \bar{y}) \Leftrightarrow \mathcal{N} \models \exists \bar{y} \psi(\bar{m}, \bar{y})$ به طوری که $\psi(\bar{m}, \bar{y})$ بدون سور است.

تعریف ۲۰ (رتبهٔ سوری[2]). اگر φ یک $\mathcal{L}$- فرمول باشد، آنگاه رتبهٔ سوری فرمول φ را به صورت $\mathrm{qr}(\varphi)$ نمایش می‌دهیم و با استقرا به صورت زیر تعریف می‌شود:

$$\begin{cases} \mathrm{qr}(\varphi) = 0 \Leftarrow \text{اگر}\varphi\text{فرمولِ اتمیک باشد} \\ \mathrm{qr}(\varphi_1 \wedge \varphi_2) = \max(\mathrm{qr}(\varphi_1) \wedge \mathrm{qr}(\varphi_1)) \\ \mathrm{qr}(\varphi_1 \vee \varphi_2) = \max(\mathrm{qr}(\varphi_1) \wedge \mathrm{qr}(\varphi_1)) \\ \mathrm{qr}(\varphi_1 \to \varphi_2) = \max(\mathrm{qr}(\varphi_1) \wedge \mathrm{qr}(\varphi_1)) \\ \mathrm{qr}(\neg\varphi) = \mathrm{qr}(\varphi) \\ \mathrm{qr}(\forall \mathrm{x} \varphi) = \mathrm{qr}(\exists \mathrm{x} \varphi) = \mathrm{qr}(\varphi) + 1. \end{cases}$$

به عنوان مثال اگر فرمولِ $\varphi(x, y, z) = \forall x \exists y (x < y) \wedge \exists x \exists z (x = z)$ را در نظر بگیریم آنگاه $qr(\varphi) = ۲$.

۲.۱ محمول تک‌موضعی

فرض کنید $\mathcal{L} = F \cup R \cup C$ یک زبان مرتبهٔ اول باشد و $\mathcal{L}$- ساختارِ $\mathcal{M} = (M, (\mathcal{Z}^{\mathcal{M}})_{\mathcal{Z} \in \mathcal{L}})$ را در نظر بگیرید. حال اگر زبان $\mathcal{L}' = \mathcal{L} \cup \{U\}$ را در نظر بگیریم به طوری که U یک رابطهٔ تک موضعی است، $\mathcal{L}'$ ساختار ما به شکلِ $\mathcal{M} = (M, (\mathcal{Z}^{\mathcal{M}})_{\mathcal{Z} \in \mathcal{L}}, U^{\mathcal{M}})$ در می‌آید که $U^{\mathcal{M}} \subseteq M$ و $U^{\mathcal{M}} = \{x \in M | U(x)\}$. به U یک محمولِ تک‌موضعی گوییم. در واقع $U^{\mathcal{M}}$ باعث می‌شود بخشی از ساختار $\mathcal{M}$ جدا شود. چند مثال از محمول تک‌موضعی را بررسی می‌کنیم.

مثال ۲۱. زبان $\mathcal{L}_{\mathrm{U}} = \mathcal{L}_{ring} \cup \{\mathrm{U}\}$ را در نظر بگیرید. تئوری T را در زبان $\mathcal{L}_{\mathrm{U}}$ می‌توان به‌گونه‌ای نوشت که $(\mathcal{M}, U) \models \mathrm{T}$ هرگاه $\mathcal{M}$ یک حلقه باشد و U با جمع $\mathcal{M}$ یک گروه باشد. با توجه به زبان داریم $\mathcal{L}_U = \{+, ., -, ۰, ۱, U\}$ و تئوری را به صورت زیر می‌نویسیم:

[2] Quantifier rank

$$T=\{\forall x\,(x+\circ=\circ+x=x)\quad \forall x,y,z\,(x+(y+z)=(x+y)+z)\quad \forall x(\exists y\, x+y=\circ)\quad \forall x,y\,(x+y=y+x)$$

$$\forall x,y,z\,((x.y).z=x.(y.z))\quad \forall x\,(x\cdot ۱=x)\quad \forall x,y,z\,(x\cdot(y+z)=(x.y)+(x.z))$$

$$\forall x,y,z((y+z).x=(y.x)+(z.x))\forall x,y\,(U(x)\wedge U(y)\rightarrow U(x+y))\quad U(\circ)$$

$$\forall x\,(U(x)\rightarrow \exists y(U(y)\wedge x+y=\circ)\}.$$

مثال ۲۲. زبان $\mathcal{L}_{\mathrm{U}}=\{<,U\}$ را در نظر بگیرید و همچنین تئوری T در زبان $\mathcal{L}_{\mathrm{U}}$ را به صورت

$$\mathrm{T}=\{\forall \mathrm{x}(\mathrm{x}<\mathrm{x})$$

$$\forall x\forall y(x<y\wedge y<x\rightarrow x=y)$$

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

$$\forall x\forall y(x<y\vee y<x)$$

$$\forall x\forall y(x<y\rightarrow \exists z(U(z)\wedge x<z<y)\}$$

در نظر بگیرید. اگر $(\mathcal{M},U)\models \mathrm{T}$ و $\mathcal{M}$ مجموعه‌ای مرتب خطی باشد آنگاه U یک زیرمجموعهٔ چگال از $\mathcal{M}$ است.

مثال ۲۳. تئوری زیر را در زبان $\mathcal{L}_U=\mathcal{L}\cup\{U\}$ در نظر بگیرید. می‌خواهیم تئوری T را در زبان $\mathcal{L}_{\mathcal{N}}$ به گونه‌ای می‌نویسیم که $(\mathcal{M},\mathcal{N})\models \mathrm{T}$ هرگاه $\mathcal{N}\leq\mathcal{M}$.

۱. در تئوری باید برای هر $f\in\mathcal{L}$ قرار دهیم:

$$\forall a_۱,\dots,a_n\quad \big(U(a_۱)\wedge U(a_۲)\wedge\ldots\wedge U(a_n)\longrightarrow U(f(a_۱,\dots,a_n))\big).$$

۲. برای هر $c\in\mathcal{L}$ در تئوری قرار دهیم:

$$U(c).$$

۳ با توجه به محک تارسکی ۱۵ برای هر $\mathcal{L}$- فرمول φ در تئوری اصل زیر را قرار دهیم :

$$\forall a_۱,\dots,a_n\quad U(a_۱)\wedge U(a_۲)\wedge\ldots\wedge U(a_n)\longrightarrow \big(\exists x\,\varphi(x,a_۱,\dots,a_n)\longrightarrow \exists x(U(x)\wedge\varphi(x,a_۱,\dots,a_n))\big).$$

مثال ۲۴. فرض کنید زبان $\mathcal{L}_{\mathrm{A}}=\mathcal{L}\cup\{\mathrm{A}\}$ داده شده باشد که $\mathcal{L}$ زبان حلقه‌هاست. می‌خواهیم تئوری T را در زبان $\mathcal{L}_{\mathrm{A}}$ به گونه‌ای بنویسیم که $(\mathcal{M},\mathcal{A})\models \mathrm{T}$ هرگاه $\mathcal{M}$ یک میدان باشد و $\mathcal{A}\subseteq\mathcal{M}$ یک حلقهٔ ارزیاب برای $\mathcal{M}$ باشد. با توجه به زبان داریم $\mathcal{L}_A=\{+,.,-,\circ,۱,A\}$ و تئوری را به صورت زیر می‌نویسیم:

$$T=\{\forall x(x+\circ=\circ+x=x)\quad \forall x,y,z(x+(y+z)=(x+y)+z)\quad \forall x(\exists y\, x+y=\circ)\quad \forall x,y\,(x+y=y+x)$$

$$\forall x, y, z\,((x.y).z = x.(y.z)) \quad \forall x(x \cdot 1 = x) \quad \forall x, y, z(x.(y+z) = (x.y) + (x.z))$$

$$\forall x, y, z((y+z).x = (y.x) + (z.x)) \quad \forall x(\exists y\, xy = 1) \quad \forall x \forall y \quad (A(x) \wedge A(y) \longrightarrow A(x+y) \wedge A(x.y))$$

$$A(0) \quad A(1) \quad \forall x(A(x) \vee A(x^{-1}))\}.$$

ملاحظه ۲۵. فرض کنید $(\mathcal{M}, \mathcal{N}) \subseteq (\mathcal{M}', \mathcal{N}')$. چون $\mathcal{M} \subseteq \mathcal{M}'$ برای هر $a \in \mathcal{M}$ داریم $\mathcal{M} \models U(a) \iff \mathcal{M}' \models U(a)$ در نتیجه $a \in \mathcal{N}' \iff a \in \mathcal{N}$. همچنین $a \in \mathcal{M}$ زیرا داریم $a \in \mathcal{N}' \cap \mathcal{M} \iff a \in \mathcal{N} \cap \mathcal{M}$. در واقع $a \in \mathcal{N}' \cap \mathcal{M} \iff a \in \mathcal{N}$. بنابراین نشان دادیم $\mathcal{M} \cap \mathcal{N}' = \mathcal{N}$.

۳.۱ مجموعه‌های تعریف‌پذیر

تعریف ۲۶ (تعریف‌پذیری). فرض کنید $\mathcal{M}$ یک $\mathcal{L}$- ساختار باشد و $A \subseteq M$. می‌گوییم مجموعهٔ $X \subseteq M^n$ یک مجموعهٔ A- تعریف‌پذیر است هرگاه فرمول $\varphi(x_1, \ldots, x_n, a_1, \ldots, a_m)$ موجود باشد که در آن $a_i \in A$ و

$$X = \{(b_1, \ldots, b_n) \in \mathcal{M}^n \,|\, \mathcal{M} \models \varphi(b_1, \ldots, b_n, a_1, \ldots, a_m)\}.$$

می‌گوییم X، $\emptyset$- تعریف‌پذیر است هرگاه $X = \{\bar{b} \,|\, \varphi(\bar{b})\} = \{(b_1, \ldots, b_n) \,|\, \mathcal{M} \models \varphi(b_1, \ldots, b_n)\}$.

مثال ۲۷. در ساختار $(\mathbb{C}, +, \cdot, 0, 1)$ مجموعهٔ $X = \{i, -i\}$ تعریف‌پذیر است زیرا می‌توان نوشت:

$$X = \{x | \mathbb{C} \models x^2 + 1 = 0\} = \{i, -i\}.$$

مثال ۲۸. در ساختارِ $(\mathbb{Z}, +, \cdot, 0, 1)$ مجموعهٔ $X = \{(x, y) \,|\, x \leq y\}$ تعریف‌پذیر است زیرا بنابر قضیهٔ چهارمربع لاگرانژ عدد $x \in \mathbb{Z}$ مثبت است اگر و تنها اگر حاصل جمع چهار مربع کامل باشد.

$$A = \{x \in \mathbb{Z} | x \geq 0\} = \{x \in \mathbb{Z} | \exists a_1, a_2, a_3, a_4 \;\; x = a_1^2 + a_1^2 + a_3^2 + a_4^2\}$$

و در نتیجه داریم:

$$X = \{(x, y) | y - x \in A\} = \{(x, y) | \exists a \in A; y = x + a\}.$$

تعریف ۲۹ (تعبیرپذیری[3]). گوییم $\mathcal{L}$- ساختار $\mathcal{M}$ در $\mathcal{L}'$- ساختار $\mathcal{N}$ تعبیرپذیر است، اگر جهان M و همچنین همه روابط، ثوابت و توابع در $\mathcal{N}$ تعریف‌پذیر باشد.

مثال ۳۰. فرض کنید K یک میدان و $G = GL_2(K)$ گروهی از ماتریس‌های 2×2 وارون‌پذیر روی میدان K باشند. فرض کنید

$$X = \{(a, b, c, d) \in K^4 : ad - bc \neq 0\}$$

[3] interpretable

و تابع $f : X^۲ \longrightarrow X$ به صورت زیر تعریف می‌کنیم

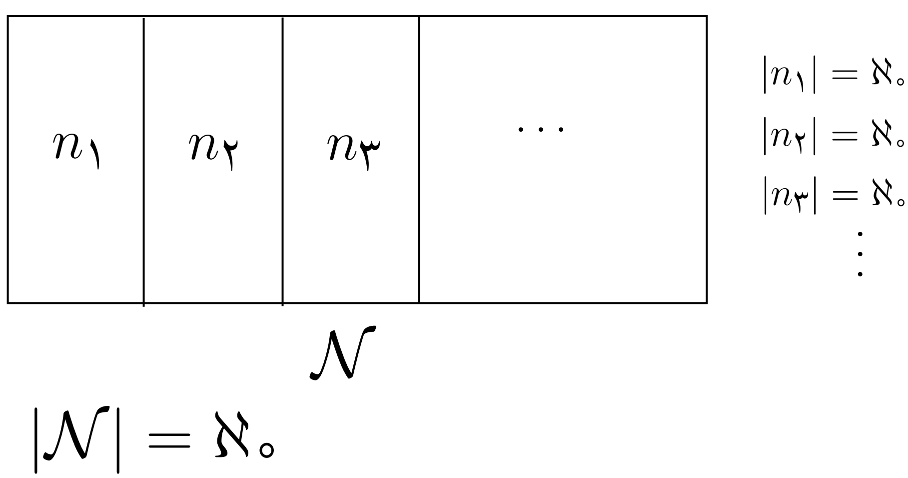
$$f((a_۱, b_۱, c_۱, d_۱), (a_۲, b_۲, c_۲, d_۲)) = (a_۱a_۲ + b_۱c_۲, a_۱b_۲ + b_۱d_۲, c_۱a_۲ + d_۱c_۲, c_۱d_۲ + d_۱d_۲).$$

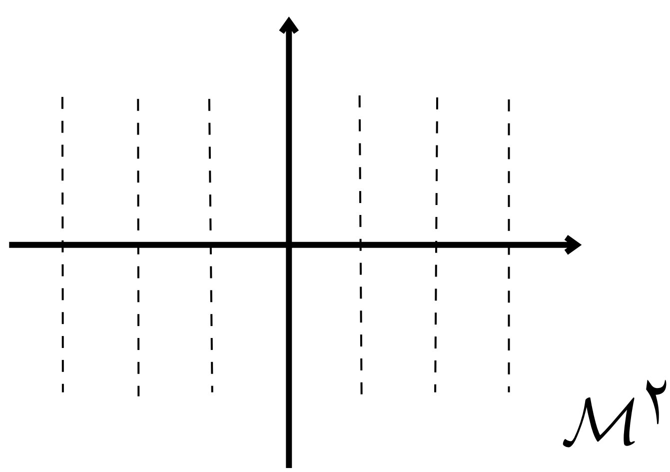
واضح است که X و f در $(K, +, .)$ تعریف‌پذیر است و مجموعهٔ X همراه با تابع f با $GL_۲(K)$ یکریخت است به طوری که عضو همانی آن $(۱, ۰, ۰, ۱)$ می‌باشد. بنابراین $GL_۲(K)$, در $(K, +, ., ۰, ۱)$ تعبیرپذیر است.

مثال ۳۱. فرض کنید $\mathcal{L} = \varnothing$ و $\mathcal{M}$ یک $\mathcal{L}$- ساختار با جهان شمارا باشد یعنی $|M| = \aleph_۰$. همچنین فرض کنید زبانِ $\mathcal{L}_۰ = \{E\}$ که E یک رابطهٔ دو موضعی باشد. اگر $\mathcal{L}_۰$- ساختارِ $\mathcal{N} = (N, E)$ که E یک رابطهٔ هم ارزی با شمارا کلاس هم‌ارزیِ شمارا است، را در نظر بگیرید، آنگاه $\mathcal{L}_۰$- ساختارِ $\mathcal{N}$ در $\mathcal{L}$- ساختارِ $\mathcal{M}$ تعبیرپذیر است زیرا اگر تعریف کنیم:

$$R = \{(x_۱, x_۲)(y_۱, y_۲) \in \mathcal{M}^۲ \times \mathcal{M}^۲ : x_۱ = y_۱\}$$

آنگاه $\mathcal{N} \cong (\mathcal{M}^۲, R)$.





فصل ۲

مقدمات جبری

در این فصل مباحث جبری مورد نیاز برای مطالعهٔ این پایان‌نامه آورده شده است. در ابتدا مروری بر جمع مستقیم و خواص آن شده و در ادامه به بررسی انواع توسیع‌های میدانی نظیر توسیع جبری، جدایی‌پذیر و منتظم پرداخته شده است و ادامه میدان سودو بستهٔ جبری تعریف شده است. همچنین مروری مختصر بر سری‌های توانی و انواع آن شده است. بعد از آن میدان‌های ارزیابی و خواص و گزاره‌هایی در این مبحث گفته شده، که جلوتر در مقاله از آن‌ها استفاده خواهیم کرد. حلقه‌های نرم‌دار، حلقه‌های هنسلی و علاوه بر آن میدان سری‌های هان در آخر فصل مورد مطالعه قرار گرفته است.

۱.۲ جمع مستقیم گروه‌ها

فرض کنید G و H دو گروه باشند. جمع مستقیم این دو گروه به صورت زیر تعریف می‌شود:

$$G \oplus H = \{(g,h) | g \in G, h \in H\}.$$

$G \oplus H$ یک گروه است که اگر $(g_۱, h_۱), (g_۲, h_۲) \in G \oplus H$ جمع این گروه به صورت زیر تعریف می‌شود:

$$(g_۱, h_۱) + (g_۲, h_۲) = (g_۱ +_G g_۲, h_۱ +_H h_۲).$$

ما همچنین می‌توانیم جمع مستقیم را با هر تعداد نامتناهی از جمعوند به صورت زیر تشکیل دهیم:

$$\bigoplus_{i\in I} G_i = \{(g_i)_{i\in I} | g_i \in G_i, \text{متناهی باشد}\{i : g_i \neq ۰\}\}.$$

ملاحظه ۳۲. جمع مستقیم هر تعداد گروه آبلی، گروهی آبلی است.

گروهِ $(G,+,0)$ را تاب‌دار گوییم هرگاه برای هر عنصر $g \in G$ یک $n \in \mathbb{N}$ موجود باشد به طوری که $\underbrace{g+g+\ldots+g}_{n\text{بار}} = 0$. اگر برای هر $n \in \mathbb{N}$ در گروه داشته باشیم $\underbrace{g+g+\ldots+g}_{n\text{بار}} \neq 0$، آنگاه گروه G را بدون تاب گوییم. برای مثال گروه $(\mathbb{Z},+,0)$ یک گروه بدون تاب است زیرا تنها عدد صحیحی که n بار با خودش جمع شود تا برابر صفر شود، خود صفر است.

می‌دانیم ترتیب خطی یک رابطهٔ دوتایی $\leq$ روی مجموعهٔ X است که برای هر $a,b,c \in X$ ویژگی‌های زیر را دارد:

۱. $a \leq a$.

۲.اگر $a \leq b$ و $b \leq c$ آنگاه $a \leq c$.

۳. اگر $a \leq b$ و $b \leq a$ آنگاه $a = b$.

۴. $a \leq b$ یا $b \leq a$.

گوییم $(G,\leq)$ یک گروه مرتب خطی است هرگاه $\leq$ یک ترتیب خطی باشد و برای هر $a,b,c \in G$ ویژگی‌های زیر برقرار باشد:($c > 0$)

$$a \leq b \Longrightarrow ac \leq bc$$

$$a \leq b \Longrightarrow ca \leq cb$$

تعریف ۳۳ (ترتیب قاموسی[1]). فرض کنید A و B دو مجموعه باشند. ترتیب " $\leq$ " یک ترتیب قاموسی است هرگاه برای هر $(a,b),(a',b') \in A \times B$ داریم $(a,b) < (a',b')$ هرگاه $a < a'$ یا اگر $a = a'$ آنگاه $b < b'$.

فرض کنید $(G,<_G)$ و $(H,<_H)$ دو گروه مرتب باشند، برای هر $(g,h),(g',h') \in G \oplus H$، ترتیب قاموسی به این صورت تعریف می‌شود که $(g,h) < (g',h')$ اگر و تنها اگر $g <_G g'$ یا اگر $g = g'$ آنگاه داشته باشیم $h <_H h'$.

تعریف ۳۴ (زیرگروه محدب). فرض کنید G و H گروه‌هایی مرتب باشند به طوری که $H \leq G$. گوییم G در H محدب است هر گاه برای هر $A,B \in G$ داشته باشیم

$$\{X \in H | A \leq X \leq B\} = \{X \in G | A \leq X \leq B\}$$

به عنوان مثال $\mathbb{Q}$ در $\mathbb{R}$ محدب نیست زیرا $1,2 \in \mathbb{Q}$ ولی $\{x \in \mathbb{R} | 1 \leq x \leq 2\} \neq \{x \in \mathbb{Q} | 1 \leq x \leq 2\}$.

گزاره ۳۵. فرض کنید $G := \bigoplus_{i\in I} G_i$. برای هر $k \in I$، $\bigoplus_{i\in I, i>k} G_i$ زیرگروه محدب G است به بیان دیگر هر جمعوند $\bigoplus_{i\in I} G_i$ زیرگروه محدب آن است.

اثبات. در اینجا $\bigoplus_{i\in I, i>k} G_i \subseteq \bigoplus_{i\in I} G_i$ (نشاندن) و $\bigoplus_{i\in I, i>k} G_i$ زیر گروه محدب $\bigoplus_{i\in I} G_i$ است زیرا اگر فرض کنیم $A,B \in \bigoplus_{i\in I, i>k} G_i$ که $A \leq X \leq B$ و $X \in G$ داریم

$$A = (0,\ldots,0,g_{k+1},g_{k+2},\ldots)$$

---

[1] lexicographical order

و

$$B = (\circ, \dots, \circ, g'_{k+1}, g'_{k+2}, \dots)$$

که $g_{K+1} < g'_{k+1}$ یا اگر $g_{K+1} = g'_{k+1}$ آنگاه $g_{K+2} < g'_{k+2}$ یا اگر $g_{K+2} = g'_{k+2}$ آنگاه $g_{K+3} < g'_{k+3}$ و به همین ترتیب الی آخر. چون $X \in G$ آنگاه

$$X = (X_1, X_2, \dots, X_k, X_{k+1}, \dots)$$

و فرض کردیم $A \leq X \leq B$ بنابراین $\begin{cases} X_i = \circ & i \leq k \\ g \leq X_i \leq g' & i \geq k+1 \end{cases}$ در نتیجه $\bigoplus_{i \in I, i>k} G_i$. □

فرض کنید H زیرگروه G باشد. گروه خارج قسمتی $\frac{H}{G}$ به صورت زیر تعریف می‌شود:

$$\frac{H}{G} = \{h + G | h \in H\}.$$

زمانی دو عنصر در گروه خارج قسمتی $\frac{H}{G}$ مساوی‌اند که تفاضل آن‌ها در گروه G باشد یعنی

$$h + G = h' + G \Longleftrightarrow h - h' \in G$$

ملاحظه ۳۶. فرض کنید $G := \bigoplus_{i \in I} G_i$ و $H := \bigoplus_{i \in I, i>k} G_i$. می‌خواهیم گروه خارج قسمتی $\frac{H}{G}$ را به دست آوریم. اگر $A = (a_1, a_2, \dots), B = (b_1, b_2, \dots) \in H$ آنگاه

$$A + G = B + G \Longleftrightarrow A - B \in G \Longleftrightarrow a_i = b_i \quad (i \leq k).$$

بنابراین در گروه خارج قسمتی $\frac{H}{G}$ فقط k عنصر اول تعیین کننده هستند و باعث تمایز عناصر گروه می‌شوند. به بیان دیگر دو عنصر زیر در $\frac{H}{G}$ برابر هستند:

$$(a_1, a_2, \dots, a_k, C) = (a_1, a_2, \dots, a_k, D)$$

در نتیجه داریم

$$\frac{H}{G} = \frac{\bigoplus_{i \in I, i>k} G_i}{\bigoplus_{i \in I} G_i} = \{(a_1, a_2, \dots, a_k, \dots) + G | a_i \in H\}.$$

تعریف ۳۷. گروه آبلی $(G, +)$ بخش‌پذیر است اگر برای هر عدد صحیح مثبت n و هر $g \in G$ یک $y \in G$ یافت شود به طوری که $g = ny = \underbrace{n + n + \dots + n}_{y\text{بار}}$. به بیان دیگر هر عنصرِ G بر هر عدد صحیح مثبت بخش‌پذیر است.

برای مثال گروه جمعیِ اعداد گویا $\mathbb{Q}$ و گروه اعداد حقیقی $\mathbb{R}$ بخش‌پذیرند اما $\mathbb{Z}$ گروهی بخش‌پذیر نیست زیرا هیچ عدد صحیحی وجود ندارد که $2x = 1$.

۲.۲ توسیع میدان‌ها

اگر L یک میدان و K یک زیر میدان آن باشد، گوییم L توسیع K است و به صورت $K \subseteq L$ نشان می‌دهیم. برای مثال $\mathbb{R}$ توسیع میدان $\mathbb{Q}$ است و $\mathbb{C}$ توسیع میدان $\mathbb{R}$ است. قبل از آن که به انواع توسیع‌های میدانی بپردازیم چند مفهوم را در مورد میدان‌ها مرور می‌کنیم. فرض کنید F یک میدان باشد. کوچکترین عدد طبیعی m را که $\underbrace{1_F + 1_F + \ldots + 1_F}_{m\text{ بار}} = 0_F$ مشخصهٔ میدان گوییم. اگر برای هر عدد طبیعی m داشته باشیم $\underbrace{1_F + 1_F + \ldots + 1_F}_{m\text{ بار}} \neq 0_F$ میدان F را یک میدان با مشخصهٔ صفر گوییم. برای مثال $\mathbb{Q}$ و $\mathbb{R}$ و $\mathbb{C}$ مشخصهٔ صفر دارند ولی میدان $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ یک میدان با مشخصهٔ p است زیرا در این میدان

$$\underbrace{\bar{1} + \bar{1} + \ldots + \bar{1}}_{p\text{ بار}} = \bar{0}$$

ملاحظه ۳۸. اگر مشخصهٔ میدان F ناصفر باشد، آنگاه مشخصهٔ F یک عدد اول است، زیرا اگر فرض کنید $m \neq 0$ مشخصهٔ میدان F باشد و عددی اول نباشد، آنگاه $m = ab$ به طوری که $a, b < m$. در نتیجه داریم:

$$m \cdot 1_F = ab \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F) = (\underbrace{1_F + 1_F + \ldots + 1_F}_{a\text{ بار}})(\underbrace{1_F + 1_F + \ldots + 1_F}_{b\text{ بار}}) = 0$$

و به تناقض می‌رسیم چون گفتیم m کوچکترین عدد طبیعی است که $\underbrace{1_F + 1_F + \ldots + 1_F}_{m\text{ بار}}$ و بنابر فرض $a, b < m$.

۱.۲.۲ توسیع جبری

فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. عضو $a \in L$ را روی K **جبری** گوییم هرگاه چند جمله‌ای ناصفر $f(x) \in K[x]$ وجود داشته باشد که $f(a) = 0$. در غیر این صورت a را روی K **متعالی** گوییم. توسیع $K \subseteq L$ را **توسیع جبری** می‌نامیم، هرگاه هر عضو L روی K جبری باشد. برای مثال اگر $a + bi \in \mathbb{C}$ را در نظر بگیریم، آنگاه $a + bi$ یک ریشهٔ چندجمله‌ای زیر است:

$$(x - (a + bi)(x - (a - bi)) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[X]$$

پس $a + bi$ روی $\mathbb{R}$ جبری است بنابراین $\mathbb{C}$ یک توسیع جبری $\mathbb{R}$ اما نه $\mathbb{C}$ و نه $\mathbb{R}$ توسیعی از $\mathbb{Q}$ نیستند زیرا اعدادی گنگ مانند π و e وجود دارند که روی $\mathbb{Q}$ جبری نیستند.

فرض کنید L یک توسیع میدان K است و $f(x) \in K[X]$ یک چندجمله‌ای غیر ثابت با درجهٔ n باشد. اگر $f(x)$ در $L[X]$ به صورت $f(x) = c(x - u_1)(x - u_2) \ldots (x - u_n)$ تجزیه شود آنگاه گوییم که $f(x)$ روی میدان $K[X]$ شکافته می‌شود. کوچکترین توسیع میدانی که تمام ریشه‌های $f(x)$ را شامل می‌شود، در نظر بگیرید. توسیع میدان L از K را میدان شکافندهٔ $f(x)$ روی K گوییم، هرگاه دو شرط زیر برقرار باشد:

۱. $f(x)$ روی L شکافته شود یعنی $f(x) = c(x-u_1)(x-u_2)\dots(x-u_n)$.

۲. $L = k(u_1, u_2, \dots, u_n)$.

به عنوان مثال اگر $x^2 + 1$ به عنوان یک چندجمله‌ای در $\mathbb{R}[X]$ در نظر گرفته شود، آنگاه $\mathbb{C}$ یک توسیع میدان شکافندهٔ $x^2 + 1$ است زیرا اولاً در $\mathbb{C}[X]$ داریم $x^2 + 1 = (x-i)(x+i)$ دوماً $\mathbb{C} = \mathbb{R}(i, -i) = \mathbb{R}(i)$.

تعریف ۳۹ (میدان بسته جبری). میدان L را بستهٔ جبری می‌نامیم هرگاه هر چندجمله‌ای در $K[x]$ همه ریشه‌هایش در خود L باشد. به بیان دیگر به میدانی که روی آن هر چندجمله‌ای غیر ثابت با ضرایب در K شکافته می‌شود، بستهٔ جبری گفته می‌شود.

برای مثال میدان اعداد مختلط $\mathbb{C}$، بستهٔ جبری است زیرا هر چند جمله‌ای در آن ریشه دارد.

تعریف ۴۰ (بستار جبری). میدان $K \subseteq L$ را یک بستار جبری K می‌نامیم، هرگاه اولاً یک توسیع جبری باشد، ثانیاً L خودش بستهٔ جبری باشد. بستار جبری K را با K^{alg} نشان می‌دهیم.

برای مثال $\mathbb{C}$ بستار جبری $\mathbb{R}$ است زیرا $\mathbb{C} = \mathbb{R}[i]$ یک توسیع جبری از $\mathbb{R}$ است که خودش بستهٔ جبری است. با این حال $\mathbb{C}$ بستار جبری $\mathbb{Q}$ نیست زیرا $\mathbb{C}$ روی $\mathbb{Q}$ جبری نیست.

۲.۲.۲ توسیع جدایی‌پذیر

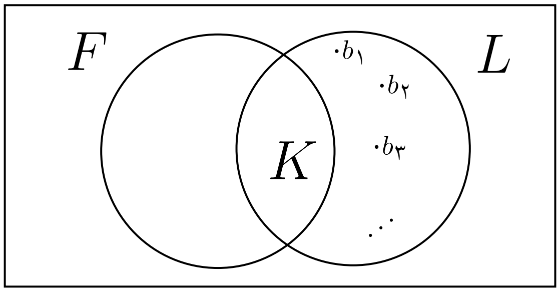
هر چندجمله‌ای دارای یک میدان شکافنده است که تمام ریشه‌هایش را داراست. این ریشه‌ها ممکن است متمایز و یا تکراری باشند. اگر L یک میدان باشد، چندجمله‌ای $f(x) \in [X]$ با درجهٔ n را **چندجمله‌ای جدایی‌پذیر** گوییم هرگاه این چندجمله‌ای دارای n ریشهٔ متمایز در یک میدان شکافنده باشد. به طور معادل $f(x)$ جدایی‌پذیر است اگر این چندجمله‌ای در هر میدان شکافنده ریشهٔ مکرر نداشته باشد. توسیع L از K را **توسیع جدایی‌پذیر** گویند اگر هر عنصر از L ریشهٔ یک چندجمله‌ای جدایی‌پذیر $f \in K[x]$ باشد. بنابراین هر توسیع جدایی‌پذیر لزوماً جبری است. برای مثال چندجمله‌ای $x^2 + 1 \in \mathbb{Q}[X]$ جدایی‌پذیر است زیرا دارای ریشه‌های متمایز $\{i, -i\}$ در $\mathbb{C}$ است ولی $f(x) = x^4 - x^3 - x + 1$ جدایی‌پذیر نیست زیرا به صورت $(x-1)^2(x^2+x+1)$ تجزیه می‌شود و یک ریشه مکرر دارد.

یک میدان را **به طور جدایی‌پذیر بسته** گوییم هرگاه توسیع جدایی‌پذیر آن، خودش باشد. میدان $K \subseteq L$ را یک **بستار جدایی‌پذیر** می‌نامیم هرگاه هیچ توسیع جدایی‌پذیر از K شامل خودش وجود نداشته باشد. بستار جدایی‌پذیر K را با K^{sep} نشان می‌دهیم. منظور از $K \neq K^{sep}$ این است که K با بستار جدایی‌پذیر خودش برابر نیست.

۳.۲.۲ توسیع منتظم

در ادامه به تعریف مجزای خطی و جبری می‌پردازیم.

تعریف ۴۱ (مجزای خطی). دو حلقه L و F در یک توسیع میدانی مشترک روی یک زیر میدان مشترک مانند K را به طور خطی مجزا گویند هر گاه اگر $b_1, b_2, b_3, \ldots$ در L روی K مستقل خطی باشند آنگاه روی F هم مستقل خطی باشند یعنی اگر ترکیب خطی $r_1b_1 + r_2b_2 + r_3b_3 + \ldots = 0$ به طوری که $r_i \in K$ آنگاه $r_i = 0$.



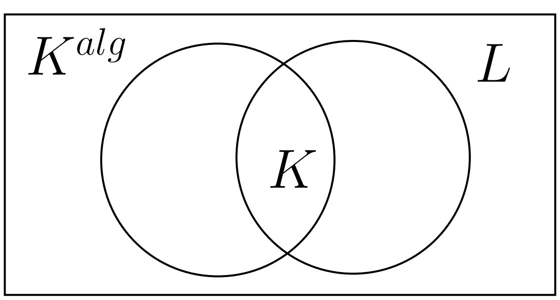
تعریف ۴۲ (مجزای جبری). دو حلقه L و F در یک توسیع میدانی مشترک روی یک زیر میدان مشترک مانند K را به طور جبری مجزا گویند هر گاه اگر $b_1, b_2, b_3, \ldots$ در L روی K مستقل جبری باشند آنگاه روی F هم مستقل جبری باشند یعنی اگر ترکیب جبری $r_1b_1 + r_2b_2^2 + r_3b_2b_3 + \ldots = 0$ و $r_i \in K$ آن گاه $r_i = 0$.

لم ۴۳. مجزای خطی بودن شرط قوی‌تری از مجزای جبری بودن است. به بیان دیگر مجزای جبری بودن از مجزای خطی بودن نتیجه می‌شود.

اثبات. فرض کنید L و F دو حلقهٔ مجزای خطی روی زیر میدان مشترک K باشند. می‌خواهیم نشان دهیم L و F مجزای جبری نیز هستند. فرض کنید L روی K مجزای جبری باشد، یعنی عناصر $b_1, b_2, b_3, \ldots$ در L روی K مستقل جبری باشند آنگاه هر ترکیب جبری آن‌ها ناصفر است، در این صورت توان‌های $b_1, b_2, b_3, \ldots$ روی K مستقل خطی هستند. بنابراین توان‌های $b_1, b_2, b_3, \ldots$ روی F مستقل جبری‌اند. در واقع $b_1, b_2, b_3, \ldots$ مستقل جبری‌اند اگر و تنها اگر توان‌های $b_1, b_2, b_3, \ldots$ مستقل خطی باشند. در نتیجه $b_1, b_2, b_3, \ldots$ روی F مستقل جبری هستند. پس L و F مجزای جبری هستند. □

عکس لم بالا همواره برقرار نیست مگر آنکه F یک توسیع منتظم از K باشد.

تعریف ۴۴. توسیع $K \subseteq L$ یک توسیع میدانی منتظم است هرگاه L و K^{alg} روی K مجزای خطی باشند.



۴.۲.۲ میدان سودو بستهٔ جبری

چندجمله‌ای $f \in K[X_1, \dots, X_n]$ مطلقاً تحویل ناپذیر است هرگاه در هر توسیع جبریِ میدانِ K تحویل ناپذیر باشد. می‌دانیم چندجمله‌ای‌های تک متغیره همگی در اعداد مختلط تجزیه می‌شوند بنابراین چندجمله‌ای‌های تک متغیره مطلقاً تحویل‌ناپذیر نیستند. برای مثال چندجمله‌ای دو متغیره $x^2 + y^2$ در اعداد مختلط به $(x+iy)(x-iy)$ تجزیه می‌شود اما چندجمله‌ای دو متغیره $x^2 + y^2 - 1$ در هیچ توسیعی از میدان تجزیه نمی‌شود یعنی تحویل ناپذیر است در نتیجه یک چندجمله‌ای مطلقاً تحویل ناپذیر است.

تعریف ۴۵ (میدان سودو بسته جبری[2]). میدان K را یک میدان سودو بسته جبری گوییم هرگاه اگر $f(X_1, \dots, X_n, T) \in K[X_1, \dots, X_n, T]$ یک چندجمله‌ای مطلقاً تحویل ناپذیر باشد و توان T از یک بزرگتر باشد و $g \in K[X_1, \dots, X_n]$ آنگاه $(a,b) \in K^n \times K$ وجود داشته باشد به طوری که $f(a,b) = 0$ و $g(a) \neq 0$.

لم ۴۶. میدان K یک میدان سودو بستهٔ جبری است اگر وتنها اگر در هر توسیع میدانی منتظم به طور وجودی بسته باشد.

به عنوان مثال میدان‌های بستهٔ جبری و میدان های بستهٔ جدایی‌پذیر، سودو بستهٔ جبری هستند.

۵.۲.۲ $\mathbb{Q}^{tot\mathbb{R}}$

تعریف ۴۷ (میدان اعداد کاملاً حقیقی [3]). میدان اعداد K را کاملاً حقیقی گویند و با $\mathbb{Q}^{tot\mathbb{R}}$ نمایش می‌دهند، هرگاه تصویر هر نشاندن از K به اعداد مختلط زیر مجموعهٔ اعداد حقیقی باشد و یا به طور معادل K روی $\mathbb{Q}$ توسط یک چندجمله‌ای با ضرایب صحیح که تمام ریشه‌های آن حقیقی هستند تولید شده است. به بیان دیگر میدان K میدان اعداد کاملاً حقیقی است هرگاه، اگر $f : K \longrightarrow \mathbb{C}$ یک نشاندن باشد، آنگاه $f(K) \subseteq \mathbb{R}$.
برای مثال $\mathbb{Q}(\sqrt{2})$ میدان اعداد کاملاً حقیقی است و به طور کلی اگر $r \in \mathbb{R} - \mathbb{Q}$ آنگاه میدان $\mathbb{Q}(r)$ میدان کاملاً حقیقی است.

۳.۲ سری‌های توانی

فرض کنید F یک میدان باشد. حلقهٔ چندجمله‌ای‌های با متغیر X روی میدان F را با $F[X]$ نشان می‌دهیم که از عناصری به شکل زیر تشکیل شده است:

$$F[X] = \{a_0 + a_1X + a_2X^2 + \dots + a_nX^n | n \in \mathbb{N}, a_i \in K\}$$

هر عضو در $F[X]$ یک چندجمله‌ای با ضرایب در F است. اگر $f \in F[X]$ به صورت $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ باشد به طوری که $a_n \neq 0$، گوییم f یک چندجمله‌ای با درجهٔ n است. اگر

[2] pseudo algebraically closed [3] Totally real numbers field

$f=a_0+a_1X+a_2X^2+\ldots+a_nX^n$ و $g=b_0+b_1X+b_2X^2+\ldots+b_nX^n+\ldots+b_mX^m$ آنگاه جمع و ضرب در این حلقه به صورت زیر تعریف می‌شود:

$$f+g=(a_0+b_0)+(a_1+b_1)X+\ldots+(a_n+b_n)X^n+\ldots+b_mX^m$$

$$f.g=c_0+c_1X+c_2X^2+\ldots+c_{n+m}X^{n+m}$$

$$c_0=a_0b_0$$

$$c_1=a_0b_1+a_1b_0$$

$$c_2=a_0b_2+a_1b_1+a_2b_0$$

$$\ldots$$

دقت کنید که $F[X]$ یک حلقه است که عضو همانی و عضو خنثای آن همان عضو همانی و عضو خنثای میدان F است.
در ادامه به مطالعهٔ سری‌های توانی می‌پردازیم.
سری‌های توانی، سری‌هایی نامتناهی به فرم $\sum_{i=0}^{\infty} a_ix_i=a_0+a_1x+a_2x^2+\ldots$ هستند. فرض کنید F یک میدان باشد آنگاه $F[[X]]$، حلقهٔ سری‌های توانی، مجموعه‌ای از چندجمله‌ای‌ها به صورت $\sum_{i=0}^{\infty} a_ix_i=a_0+a_1x+a_2x^2+\ldots$ با ضرایب در F یعنی $a_i\in F$ است. جمع و ضرب در حلقهٔ سری‌های توانی به صورت زیر تعریف می‌شود:

$$(a_n)_{n\in\mathbb{N}}+(b_n)_{n\in\mathbb{N}}=(a_n+b_n)_{n\in\mathbb{N}}$$

$$(a_n)_{n\in\mathbb{N}}\times(b_n)_{n\in\mathbb{N}}=(\sum_{k=0}^{n}a_kb_{n-k})_{n\in\mathbb{N}}$$

تعریف ۴۸. فرض کنیم R یک حلقهٔ جابه جایی و یکدار باشد، زیر مجموعه $S\subseteq R$ را یک مجموعهٔ بسته ضربی می‌نامیم هرگاه:
۱. S شامل عنصر همانی ضرب باشد.
۲. برای هر s_1,s_2 داشته باشیم $s_1s_2\in S$.

فرض کنیم R یک حلقه و S یک مجموعهٔ بسته ضربی باشد. رابطهٔ تساوی را برای مجموعهٔ $S^{-1}R=\{\frac{r}{s}|r\in R,s\in S\}$ به صورت زیر تعریف می‌کنیم:

$$\frac{r_1}{s_1}=\frac{r_2}{s_2}\Longleftrightarrow \exists u\in S\qquad u(r_1s_2-r_2s_1)=0$$

این تساوی یک رابطهٔ هم‌ارزی است. مجموعه $S^{-1}R$ با اعمال جمع و ضرب $\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2}$ و $\frac{r_1}{s_1}.\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}$ یک حلقه است که به آن حلقهٔ کسرها گویند. اگر $S=R-\{0\}$ آنگاه $S^{-1}R$ یک میدان است.
میدان کسرهای $F[X]$ را با $F(X)$ نشان می‌دهیم. این میدان از عناصر به صورت $\dfrac{f(X)}{g(X)}$ تشکیل شده است که $f(X),g(X)\in F[X]$ و $g(X)\neq 0$.

تعریف ۴۹ (سری‌های لوران). سری لوران یک تابع مختلط $f(z)$ یک نمایش از آن تابع به صورت سری توانی است که شامل جملاتی از درجه منفی است. این سری می‌تواند برای نمایش توابع مختلط در حالتی که یک بسط سری تیلور نمی‌توان به کار برد، استفاده شود. سری لوران برای تابع مختلط $f(z)$ حول نقطهٔ c به وسیلهٔ $f(z)=\sum_{n=-\infty}^{\infty} a_n(z-c)^n$ که $a_n=\frac{1}{2\pi i}\oint \frac{f(z)dz}{(z-c)^{c+1}}$ ، تعریف می‌شود.

$F((X))$ میدان کسرهای حلقهٔ سری‌های توانی یعنی $F[[X]]$ است. به بیان دیگر $F((X))$ مجموعه‌ای از عناصر به فرم $\frac{P(X)}{Q(X)}$ است به طوری که $P(X),Q(X)\in F[[X]]$ و $Q(X)\neq 0$.

۴.۲ حلقه‌های موضعی

اگر R حلقه باشد، $I\subset R$ را ایده‌آل چپ (راست) R می‌نامیم هرگاه I همراه با عمل جمع زیر، گروه باشد و برای هر $a\in I$ و هر $r\in R$ داشته باشیم $ra\in I(ar\in I)$. اگر I هم ایده‌آل راست و هم ایده‌آل چپ R باشد آنگاه آن را ایده‌آل می‌نامیم و با $I\trianglelefteq R$ نمایش می‌دهیم. اگر R یک حلقه باشد و $I\trianglelefteq R$ آنگاه مجموعهٔ $\{r+I|r\in R\}$ با اعمال

$$(r_1+I)+(r_2+I)=(r_1+r_2)+I$$

$$(r_1+I).(r_2+I)=((r_1r_2)+I)$$

یک حلقه است و این حلقه را به صورت $\frac{R}{I}$ نشان می‌دهیم و به آن حلقهٔ خارج قسمتی گوییم.
ایده‌آل ناسره I ازحلقهٔ R را ماکسیمال گوییم هرگاه هیچ ایده‌آلی مابین I و R نباشد به بیان دیگر هیچ ایده آل سره ای شامل I وجود نداشته باشد. برای مثال حلقهٔ $\mathbb{Z}$ را در نظر بگیرید و I مجموعهٔ مضارب ۳ یعنی $I=\{0,\pm3,\pm6,\pm9,\ldots\}$ یک زیر حلقه از $\mathbb{Z}$ است زیرا مجموع و حاصل ضرب مضارب ۳، مضارب ۳ هستند. به علاوه چون حاصل ضرب هر عدد صحیح در مضارب ۳، مضربی از ۳ است در نتیجه I یک ایده‌آل حلقهٔ $\mathbb{Z}$ است. به طور کلی تر، اگر R یک حلقهٔ جابه جایی و یکدار باشد و $c\in R$ آنگاه $I=\{rc|r\in R\}$ ایده‌آلی در R است و آن را با $<c>$ نمایش می‌دهیم.
یکی از شروط معادل میدان بودن این است که تنها ایده‌آل ماکزیمال حلقه، ایده‌آل صفر باشد. کمی ضعیف شدهٔ این شرط این است که حلقه، تنها یک ایده‌آل ماکزیمال داشته باشد. به چنین حلقه ای، حلقهٔ موضعی می گوییم. برای مثال میدان‌ها موضعی هستند که ایده آل ماکسیمال آن‌ها $<0>$ است.

قضیه ۵۰. اگر R یک حلقه جابه جایی و یکدار باشد آنگاه R حلقهٔ موضعی است اگر و تنها اگر مجموعهٔ عناصر غیر یکه R تشکیل ایده‌آل ماکسیمال می‌دهند.

اثبات. فرض کنیم R حلقهٔ موضعی و m ایده‌آل ماکسیمال آن باشد. ثابت می‌کنیم $m=R\backslash U(R)$. واضح است که عناصر m وارون ندارند. بنابراین $m\subseteq R\backslash U(R)$. فرض کنیم $a\in R\backslash U(R)$. چون $a\notin U(R)$ نتیجه می‌گیریم ایده‌آل Ra در R سره است. هر ایده‌آل سره زیر مجموعهٔ یک ایده‌آل ماکسیمال است و چون تنها یک ایده‌آل ماکسیمال داریم،

$Ra \subseteq m$ یعنی $a \in m$. در نتیجه $R\backslash U(R) \subseteq m$.

برعکس فرض کنیم $m = R\backslash U(R)$ مجموعهٔ عناصر غیریکه R تشکیل ایده‌آل ماکسیمال می‌دهند. نشان می‌دهیم R حلقهٔ موضعی است. دقت کنید چون $1 \in R$ یکه می‌باشد پس m یک ایده‌آل سره از R است. حال کافی است نشان دهیم m تنها ایده‌آل ماکسیمال R است. فرض کنیم چنین نباشد و m' ایده‌آل ماکسیمال دیگری در این حلقه باشد. چون m' یک ایده‌آل سره از R است درنتیجه هر عضو از آن غیریکه است در نتیجه $m' \subseteq m$ و چون m' یک ایده‌آل ماکسیمال است در نتیجه $m' = m$. □

گزاره ۵۱. فرض کنید m ایده آل ماکسیمال حلقهٔ R باشد آنگاه $\frac{R}{m}$ یک میدان است.

اثبات. فرض کنید m ایده‌آل ماکسیمال R باشد. اگر $a + m$ عنصر غیر صفر $\frac{R}{m}$ باشد، آنگاه $a \notin m$. مجموعهٔ $J = \{m' + ra | r \in R, m' \in m\}$ یک ایده‌آل در R است که m را شامل می‌شود. علاوه بر آن $0_R + 1_R a \in m$ در J قرار دارد، بنابراین $J \neq m$. از آنجا که m ایده‌آل ماکسیمال است در نتیجه باید داشته باشیم $J = R$. از اینکه $J = R$ نتیجه می‌گیریم $1_R \in J$ پس $m' \in m$ وجود دارد به طوری که $1_R = m' + ca$ و $c \in R$. حال نتیجه می‌گیریم $ca - 1_R = m' \in m$ بنابراین $ca + m = 1_R + m$ یعنی هم‌مجموعهٔ $c + M$ وارون $a + m$ است زیرا

$$(c + m)(a + m) = ca + m = 1_R + m$$

□

۵.۲ میدان‌های ارزیابی

تعریف ۵۲. فرض کنید A یک دامنهٔ صحیح و Γ یک گروه مرتب آبلی باشد. نگاشت $v : A^\times \longrightarrow \Gamma$ یک نگاشت ارزیابی است هرگاه برای هر $a, b \in A^\times$ ویژگی‌های زیر را داشته باشد:

۱. $v(ab) = v(a) + v(b)$

۲. $v(a + b) \geq \min\{v(a), v(b)\}$

می‌توان نگاشت ارزیابی را به صورت $v : A^\times \longrightarrow \Gamma \cup \{\infty\}$ نیز در نظر گرفت به طوری که $v(0) = \infty$ تعریف شود. اگر v یک نگاشت ارزیابی روی A باشد، به (A, v) یک حلقهٔ ارزیابی گفته می‌شود و اگر K یک میدان باشد، آنگاه به (K, v) یک میدان ارزیابی گوییم.

مثال ۵۳ (ارزیابی بدیهی). اگر K یک میدان باشد و برای هر $x \in K$ تعریف کنیم $v(x) = 0$، آنگاه v یک نگاشت ارزیابی است که به آن ارزیابی بدیهی گفته می‌شود.

مثال ۵۴ (ارزیابی پی‌اَدیک[4]). فرض کنید p یک عدد اول باشد و $a \in \mathbb{Z}$. همچنین فرض کنید $a = p^m a'$ به طوری که $p \nmid a'$، آنگاه اگر $v_p(a) = m$ را در نظر بگیریم، v_p یک نگاشت ارزیابی است زیرا اولاً اگر $a = p^n a'$ و $b = p^m b'$ آنگاه

[4] P-adic valuation

$v_p(a.b) = n + m = v_p(a) + v_p(b)$. ثانیاً اگر $v_p(a) > v_p(b)$ یعنی $n > m$ آنگاه $v_p(a+b) = m = v_p(b)$.
در نتیجه $(\mathbb{Z}, v_p)$ یک میدان ارزیابی است و به v_p یک ارزیابی pـادیک گویند.

مثال ۵۵. فرض کنید F یک میدان و $F[X]$ حلقهٔ چندجمله‌ای‌ها باشد.اگر $f \in F[X]$ و $f = X^m g$ به طوری که $g(\circ) \neq \circ$، می‌توان یک ارزیابی روی $F[X]$ به صورت زیر تعریف کرد:

$$v_p : F[X] \longrightarrow \mathbb{Z}$$

$$v(f) = m$$

مثال ۵۶. فرض کنید F یک میدان و $F[[T]]$ حلقهٔ دنباله سری‌های توانی روی f باشد. ارزیابی $v : F[[T]] \longrightarrow F$ را به صورت $v(f) = m$ تعریف می‌کنیم هر گاه $f = a_m T^m + a_{m+\text{۱}} T^{m+\text{۱}} + \ldots$ و $a_m \neq \circ$.

لم ۵۷. فرض کنید (K, v) یک میدان ارزیابی است و $x, a, b \in K$. خواص زیر برقرارند:
۱. $v(\text{۱}) = \circ$.
۲. $v(-\text{۱}) = \circ$.
۳. $v(x) = v(-x)$.
۴. $v(\frac{\text{۱}}{x}) = v(x)$.
۵. اگر $v(a) < v(b)$ آنگاه $v(a+b) = v(a)$.

اثبات. ۱.

$$v(\text{۱}) = v(\text{۱} \cdot \text{۱}) = v(\text{۱}) + v(\text{۱}) \Rightarrow v(\text{۱}) = \circ$$

۲.

$$\circ = v(\text{۱}) = v((-\text{۱}).(-\text{۱})) = v(-\text{۱}) + v(-\text{۱})$$

چون گروه‌های مرتب، بدون تاب هستند بنابراین $v(-\text{۱}) = \circ$.
۳.

$$\circ = v(-x) = v(-\text{۱}.x) = v(-\text{۱}) + v(x) = v(x)$$

۴.

$$v(\frac{\text{۱}}{x}) + v(x) = v(\text{۱}) = \circ$$

۵. می‌دانیم $v(a+b) \geq \min\{v(a), v(b)\}$ آنگاه $v(a+b) \geq v(a)$. از طرف دیگر $v(a) = v(a+b-b) \geq \min\{v(a+b), v(b)\}$. چون $v(a) < v(b)$ پس $v(a+b) < v(b)$ و $v(a) \geq v(a+b)$. $\square$

ملاحظه ۵۸. اگر A یک دامنهٔ صحیح و K میدان کسرهای آن باشد و (A,v) یک میدان ارزیابی باشد، آنگاه می‌توان v را روی K به صورت $v(\frac{a}{b}) = v(a) - v(b)$ گسترش داد. بنابراین (K,v) یک میدان ارزیابی است زیرا اولاً

$$v(\frac{a}{b}.\frac{c}{d}) = v(\frac{ac}{bd}) = v(ac) - v(bd) = v(a) + v(c) - v(b) - v(d)$$
$$= v(a) - v(b) + v(c) - v(d) = v(\frac{a}{b}) + v(\frac{c}{d}).$$

ثانیاً اگر فرض کنیم $v(\frac{a}{b}) \leq v(\frac{c}{d})$ داریم

$$v(\frac{a}{b}) \leq v(\frac{c}{d}) \longrightarrow v(a) - v(b) \leq v(c) - v(d) \longrightarrow v(a) + v(d) \leq v(b) + v(c)$$
$$\longrightarrow v(ad) \leq v(bc) \longrightarrow v(ad) \leq v(ad+bc) \longrightarrow v(a) + v(d) \leq v(ad+bc)$$
$$\longrightarrow v(a) \leq v(ad+bc) - v(d) \longrightarrow v(a) - v(b) \leq v(ad+bc) - v(b) - v(d)$$
$$\longrightarrow v(a) - v(b) \leq v(ad+bc) - v(bd) \longrightarrow v(\frac{a}{b}) \leq v(\frac{ad+bc}{bd}) = v(\frac{a}{b} + \frac{c}{d}).$$

نشان می‌دهیم این تنها راه گسترش نگاشت ارزیابی روی K است.

ملاحظه ۵۹. فرض کنیم A یک دامنه باشد و K میدان کسرهای آن باشد و v یک نگاشت ارزیابی روی A باشد. اگر $v_۱$ و $v_۲$ گسترش‌های v روی K باشند، آنگاه داریم:

$$v_۱(\frac{a}{b}) = v_۱(a) - v_۱(b) = v(a) - v(b)$$
$$v_۲(\frac{a}{b}) = v_۲(a) - v_۲(b) = v(a) - v(b).$$

به بررسی چند مثال از توسیع‌های نگاشت‌های ارزیابی می‌پردازیم:

مثال ۶۰. گفتیم نگاشت ارزیابی پی‌ادیک به صورت زیر تعریف می‌شود:

$$v_p : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$a \longmapsto m$$

به طوری که اگر $a = p^m b$ و $p \nmid b$ آنگاه $v_p(a) = m$. از آنجا که $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ می‌توان این ارزیابی را به صورت زیر گسترش داد:

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$$
$$v_p(\frac{a}{b}) = v_p(a) - v_p(b)$$

مثال ۶۱. نگاشت ارزیابی روی حلقهٔ چندجمله‌ای ها $K[X]$ را در نظر بگیرید. اگر $X^n | f$ و $X^{n+۱} \nmid f$ داریم $v(f) = n$. می‌دانیم $\mathrm{Frac(K[X]) = K(X)}$ است و نگاشت ارزیابی توسیع یافته به صورت زیر است:

$$v : K(X) \longrightarrow \mathbb{Z}$$
$$v(\frac{f}{g}) = v(f) - v(g)$$

مثال ۶۲. نگاشت ارزیابی روی سری‌های توانی $v: K[[X]] \longrightarrow \mathbb{Z}$ را در نظر بگیرید. می‌توان این نگاشت را به روی میدان کسرهای $K((X))$ یعنی میدان سری‌های لوران گسترش داد.

تعریف ۶۳. فرض کنید (K,v) یک میدان ارزیابی باشد. به $O_v = \{x \in K : v(x) \geq ۰\}$ یک حلقهٔ ارزیاب گفته می‌شود.

توجه کنید که O_v یک حلقه است زیرا $v(۰) = +\infty \geq ۰$ و $v(۱) = ۰ \geq ۰$ بنابراین $۰, ۱ \in O_v$. همچنین اگر $a, b \in O_v$ آنگاه $a+b \in O_v$ و $ab \in O_v$ زیرا $v(a+b) \geq \min\{v(a), v(b)\} \geq ۰$ و $v(ab) = v(a) + v(b) \geq ۰$. اگر مجموعهٔ $U = \{x : v(x) = ۰\}$ را در نظر بگیریم، آنگاه U مجموعه‌ای از یکه‌ها در O_v است زیرا اگر $x \in U$ پس $v(x) = ۰$ بنابراین $v(x^{-۱}) = ۰$ در نتیجه $x^{-۱} \in U$. همچنین اگر $x, x^{-۱} \in O_v$ داریم $v(x) \geq ۰, v(x^{-۱}) \geq ۰$ بنابراین $v(x) \leq ۰$ پس $v(x) = ۰$ درنتیجه $x \in U$.

لم ۶۴. اگر مجموعهٔ $m_v = \{x \in O_v : v(x) > ۰\}$ را در نظر بگیرید، آنگاه m_v یک ایده‌آل ماکسیمال یکتا از O_v است.

اثبات. در ابتدا نشان می‌دهیم m_v ایده‌آل است. برای هر $x, y \in m_v$ و $o \in O_v$ داریم $v(x-y) = v(x).v(-y) > ۰$ و $v(x.y) = v(x) + v(y) > ۰$ و $v(ox) = v(o) + v(x) > ۰$. همچنین m_v یک ایده‌آل ماکسیمال از O_v است یعنی هیچ ایده‌آل سره از O_v شامل x وجود ندارد زیرا اگر ایده‌آل سره I موجود باشد که شامل x باشد و $x \notin m$ پس $v(x) \leq ۰$ در نتیجه $v(x^{-۱}) > ۰$ بنابراین $x^{-۱} \in O_v$. داریم $x^{-۱}.x = ۱ \in I$ در نتیجه $I = O_v$ و به تناقض می‌رسیم. در ضمن m_v یکتا نیز است زیرا اگر p یک ایده‌آل ماکسیمال دیگر از O_v باشد که $m \nsubseteq p$ و $p \nsubseteq m$ پس $x \in m - p$ و $y \in p - m$. بدون کاسته شدن از کلیت می‌توان فرض کرد $v(\frac{y}{x}) = v(y) - v(x) \geq ۰$ و $\frac{y}{x} \in O_v$. اما از طرفی $y = (\frac{y}{x})x \in p$ و به تناقض می‌رسیم. □

تا اینجا نشان دادیم O_v دارای یک ایده‌آل ماکسیمال یکتا است یعنی O_v یک حلقهٔ موضعی است.

لم ۶۵. اگر O_v حلقهٔ ارزیابِ میدان ارزیابی (K,v) باشد آنگاه:

۱.برای هر $x \in K^{\times}$ داریم $x \in O_v$ یا $x^{-۱} \in O_v$.

۲.گروه یکه‌ها از O_v برابر $U(O_v) = \{x \in O_v : v(x) = ۰\}$ است.

اثبات. ۱. برای هر $x \in K^{\times}$ داریم $۰ = v(۱) = v(xx^{-۱}) = v(x) + v(x^{-۱})$. بنابراین $v(x) \geq ۰$ یا $v(x^{-۱}) \geq ۰$. در نتیجه $x \in O_v$ یا $x^{-۱} \in O_v$.

۲. فرض کنیم $x \in O_v$ و $x \neq ۰$ پس $v(x) \geq ۰$. $x \in U$ اگر و تنها اگر $x^{-۱} \in O_v$. در نتیجه داریم $v(x^{-۱}) = -v(x) \geq ۰$ اگر و تنها اگر $v(x) = ۰$. □

ملاحظه ۶۶. به دو طریق می‌توانیم یک میدان ارزیابی را تعریف کنیم.

روش اول: طبق تعریف ۵۲ اگر نگاشت ارزیابی $v : K^{\times} \longrightarrow \Gamma$ را درنظر بگیریم، آنگاه به (K,v) یک میدان ارزیابی

گفته می‌شود که حلقهٔ ارزیاب آن به صورت $O_v=\{x\in K : v(x)\geq ۰\}$ است و Γ گروه ارزیاب است.
روش دوم: حلقهٔ ارزیاب از میدان K، زیر حلقهٔ O از میدان K است هرگاه برای هر $x\in K^{\times}$ داشته باشیم یا $x\in O$ یا $x^{-۱}\in O$. اگر گروه خارج قسمتیِ $\Gamma=\dfrac{K^{\times}}{U(O)}$ را در نظر بگیریم، آنگاه نگاشت زیر یک نگاشت ارزیابی است:

$$v: K^{\times}\longrightarrow\Gamma$$

$$v(x)=xU(O).$$

در ادامه نشان می‌دهیم نگاشت تعریف شده در روش دوم یک نگاشت ارزیابی است.

فرض کنید $\Gamma=\dfrac{K^{\times}}{U(O)}$. برای هر $\dfrac{x}{U},\dfrac{y}{U}\in\Gamma$ رابطه زیر را روی Γ تعریف می‌کنیم:

$$\frac{x}{U}\leq\frac{y}{U}\Longleftrightarrow x|y\Longleftrightarrow\frac{y}{x}\in O$$

اولاً این رابطه خوش تعریف است، زیرا اگر $x,y,u,v\in O^{\times}$ و $x=u,y=v$ آنگاه $\dfrac{vy}{ux}\in O\Longleftrightarrow\dfrac{y}{x}\in O$.
ثانیاً $\leq$ یک ترتیب خطی روی Γ است زیرا
۱.داریم $\dfrac{x}{U}\leq\dfrac{x}{U}$ چون $\dfrac{x}{x}=۱\in O$.
۲.اگر $\dfrac{x}{U}\leq\dfrac{y}{U}$ و $\dfrac{y}{U}\leq\dfrac{x}{U}$ بنابراین $\dfrac{x}{y}\in O$ و $\dfrac{y}{x}\in O$ و چون O یک حلقهٔ ارزیابی است در نتیجه $\dfrac{x}{U}=\dfrac{y}{U}$.
۳.اگر $\dfrac{x}{U}\leq\dfrac{y}{U}$ و $\dfrac{y}{U}\leq\dfrac{z}{U}$ پس $a,b\in A$ به طوری که $y=ax$ و $z=by$ حال می‌توان نوشت $z=abx$ در نتیجه $\dfrac{x}{U}\leq\dfrac{z}{U}$.
۴.داریم $\dfrac{x}{U}\leq\dfrac{y}{U}$ یا $\dfrac{y}{U}\leq\dfrac{x}{U}$ زیرا O یک حلقهٔ ارزیاب است.
بنابراین تا اینجا نشان دادیم $(\Gamma,.,<)$ یک گروه آبلی مرتب است.
حال نگاشت ارزیابی را به صورت زیر تعریف می‌کنیم:

$$v: K^{\times}\longrightarrow G$$

$$v(x)=\frac{x}{U}$$

ادعا داریم v یک نگاشت ارزیابی است زیرا:
۱. اگر $x,y\in K^{\times}$ آنگاه $xy^{-۱}\in O$ یا $yx^{-۱}\in O$. واضح است که $v(xy)=\dfrac{xy}{U}=\dfrac{x}{U}\dfrac{y}{U}$.
۲. اگر $min\{v(x),v(y)\}=v(x)$ آنگاه $v(y)\geq v(x)$. بنابراین $\dfrac{y}{x}\in O$. داریم $(x+y)x^{-۱}=۱+yx^{-۱}\in O$ در نتیجه $v(x+y)\geq v(x)=min\{v(x,v(y))\}$.
به بررسی چند مثال از نگاشت‌های ارزیابی می‌پردازیم.
۱.در نگاشت ارزیابی بدیهی روی میدان K، حلقه ارزیاب خود K می باشد و ایده آل ماکسیمال آن $\{۰\}$ و میدان باقی مانده ها K است.
۲.اگر میدان سری های صوری لوران $F((T))$ را در نظر بگیریم که گفتیم $v(f)=m$ هرگاه $f=\sum\limits_{n=m}^{\infty}a_nT^n$ و $a_m\neq ۰$،

حلقه ارزیاب آن $F[[T]]$ و ایده آل ماکسیمال آن تمام سری های به فرم $\sum_{n=m}^{\infty} a_n T^n$ به طوری که $m > \circ$ و میدان باقی مانده ها F است.
در ادامه حلقهٔ pـادیک را معرفی می‌کنیم که آن را با $\mathbb{Z}_{(p)}$ نمایش می‌دهیم. نشان می‌دهیم $\mathbb{Z}_{(p)}$ یک میدان ارزیابی هنسلی است و حلقهٔ ارزیاب و میدان باقی‌ماندهٔ آن را بررسی می‌کنیم.

۶.۲ حلقهٔ pـادیک‌ها

۷.۲ حلقهٔ های نُرم‌دار، هنسلی و pـادیک‌ها

۱.۷.۲ حلقه‌های نُرم‌دار

تعریف ۶۷. فرض کنید R یک حلقهٔ جابه جایی و یکدار باشد. یک نرم روی R، نگاشتی به صورت $|\ | : R \longrightarrow \mathbb{R}^{\geq \circ}$ است، هرگاه ویژگی‌های زیر را داشته باشد:

۱. $|x| = \circ \Leftrightarrow x = \circ$

۲. $|xy| \leq |x||y|$

۳. $|x + y| \leq |x| + |y|$

اگر R یک حلقه باشد و نگاشت $|\ | : R \longrightarrow \mathbb{R}^{\geq \circ}$ یک نرم باشد به $(R, |\ |)$ یک حلقهٔ نرم‌دار گویند.

تعریف ۶۸. اگر نرم خاصیت $|x + y| \leq \max[|x|, |y|] \leq |x| + |y|$ را داشته باشد به آن نرم غیر ارشمیدسی [5] گفته می‌شود.

گزاره ۶۹. فرض کنید $|.|$ یک نرم غیر ارشمیدسی باشد. اگر $x, y \in A$ و $|x| \neq |y|$ آنگاه $|x + y| = \max[|x|, |y|]$.

اثبات. بدون کاسته شدن از کلیت فرض کنید $|x| > |y|$. چون $|x + y| \leq \max[|x|, |y|] = |x|$. از طرفی داریم $|x| = |x + y - y| \leq \max[|x + y|, |y|]$. پس $\max[|x + y|, |y|] = |x + y|$ در نتیجه $|x| \leq |x + y|$. □

تعریف ۷۰. فرض کنیم $(a_n)_{n \in \mathcal{N}}$ یک دنباله در حلقهٔ نرم‌دار $(R, |\ |)$ باشد. این دنباله را کُشی می‌نامیم هرگاه

$$\forall \epsilon > \circ, \exists N \in \mathbb{N}, \forall m, n > N, |a_n - a_m| < \epsilon$$

حلقهٔ $(R, |\ |)$ را کامل می‌نامیم هرگاه هر دنبالهٔ کُشی در آن همگرا باشد.

[5] nonarchimedean

۲.۷.۲ حلقهٔ هنسلی

فرض کنیم R یک حلقهٔ موضعی با ایده‌آل ماکسیمال m باشد. حلقهٔ چندجمله‌ای $R[X]$ را در نظر می‌گیریم. نگاشت زیر موجود است:

$$R \longrightarrow \frac{R}{m} = K$$
$$t \longmapsto \bar{t} = t + m.$$

فرض کنیم $f \in R[X]$ یک چند جمله‌ای باشد. می‌توانیم نگاشت زیر را در نظر بگیریم که هر $f \in R[X]$ را به یک چند جمله‌ای در $k[X]$ می‌برد.

$$f(X) = a_\circ + a_۱ X + \ldots + a_n X^n \in R[X] \longrightarrow \bar{f}(X) = \bar{a}_\circ + \bar{a}_۱ X + \ldots + \bar{a}_n X^n \in k[X]$$

اگر a ریشهٔ چند جمله‌ای $\bar{f}(X)$ باشد آنگاه اگر R یک حلقهٔ هنسلی باشد $\alpha \in A$ موجود است به طوری که $f(\alpha) = \circ$ و $\alpha \equiv a \ (mod\ m)$.
حال به سراغ تعریف حلقهٔ هنسلی می‌رویم.

تعریف ۷۱ (حلقهٔ هنسلی). گوییم دامنهٔ موضعی A با ایده‌آل ماکسیمال m یک حلقهٔ هنسلی است هرگاه برای هر $f(x) \in A[X]$ و برای هر $a \in A$ به طوری که $f(a) \in m$ و $f'(a) \notin m$ آنگاه $\alpha \in A$ موجود باشد به طوری که $f(\alpha) = \circ$ و $\alpha \equiv a \ (mod\ m)$.

با توجه به لم زیر، حلقهٔ نرم‌دار حالت خاصی از حلقه‌های هنسلی است.

لم ۷۲ (لم هنسل). اگر $(R, |.|)$ یک حلقهٔ کامل، مجهز به نرم غیر ارشمیدسی باشد آنگاه حلقهٔ ارزیاب $O_v = \{x \in R : |x| \leq ۱\}$ یک هنسلی است یعنی اگر $f(x) \in R[X]$ یک چندجمله‌ای باشد و $\alpha \in R$ وجود داشته باشد که $|f(\alpha)| < ۱$ و $f'(\alpha) \in U(R)$ آنگاه $a \in R$ وجود دارد به طوری که $f(a) = \circ$ و $|a - \alpha| < ۱$.

اثبات. برای اثبات از روش درون یابی نیوتن استفاده می‌کنیم. در ابتدا $a_\circ = \alpha$ قرار می‌دهیم. داریم $|f(a_\circ)| \leqslant \epsilon < ۱$ و $f'(a_\circ)$ وارون پذیر است. حال قرار می‌دهیم $a_۱ = a_\circ - \frac{f(a_\circ)}{f'(a_\circ)}$ بنابراین $|a_۱ - a_\circ| = |\frac{f(a_\circ)}{f'(a_\circ)}| < \epsilon$.
قرار می‌دهیم $h = -\frac{f(a_\circ)}{f'(a_\circ)}$ بنابراین با استفاده از بسط تیلور داریم

$$f(a_۱) = f(a_\circ + h) = f(a_\circ) + f'(a_\circ)h + h^۲(\ldots) + \ldots$$

در نتیجه $|f(a)| < \epsilon^۲$. مجدداً قرار می‌دهیم $a_۲ = a_۱ - \frac{f(a_۱)}{f'(a_۱)}$. مانند قبل می‌توانیم نتیجه بگیریم $|a_۲ - a_۱| < \epsilon^۲$ و $|f(a_۲)| < \epsilon^۴$. با تکرار این روش به یک دنبالهٔ $a_\circ, a_۱, a_۲, \ldots$ می‌رسیم که فاصلهٔ اعضای دنباله از هم کمتر از $\epsilon^{۲n}$ می‌باشد. پس این دنباله کوشی است و چون حلقه کامل است حد این دنباله وجود دارد. بنابراین $\lim_{n\to\infty} a_n = a \in R$ و

$$f(a) = f(\lim_{n\to\infty} a_n) = lim_{n\to\infty} f(a_n) = \circ$$

لازم به ذکر است که دنباله $(f(a_n))_n \in \mathbb{N}$ همگرا به صفر است زیرا نرم آن‌ها در هر مرحله کوچک و کوچکتر می‌شود. □

۳.۷.۲ حلقهٔ $\mathbb{Z}_p$

برای یک عدد اول p میدان‌های p عضوی (میدان باقی‌مانده‌های p) را با $\mathbb{F}_p$ نشان می‌دهیم.
اگر a عددی صحیح باشد برای عدد اول p تعریف می‌کنیم $v_p(a) = n$ اگر و تنها اگر $p^n|a$ و $p^{n+1} \nmid a$. نگاشت $v_p : \mathbb{Z} \longrightarrow \mathbb{Z}$ یک نگاشت ارزیابی است.

ملاحظه ۷۳. نگاشت $|.|_p : \mathbb{Z} \longrightarrow \mathbb{R}$ با ضابطهٔ $|a|_p = ۲^{-v_p(a)}$ یک نرم غیر ارشمیدسی روی حلقهٔ $\mathbb{Z}$ است.

تعریف ۷۴ (حلقهٔ pـادیک‌ها). برای یک عدد اول p، کامل شدهٔ حلقهٔ $\mathbb{Z}$ نسبت به نرم $|.|_p$ را با $\mathbb{Z}_p$ نمایش می‌دهیم و آن را حلقهٔ اعداد صحیح pـادیک گوییم.

لم ۷۵. هر عنصر a دارای نمایش یکتا به صورت $\sum_{i=o}^{\infty} a_i p^i$ است به طوری که برای هر اندیس i، $a_i \in \{۰, ۱, \dots, p-۱\}$

اثبات. فرض کنیم a عنصری در $\mathbb{Z}_p$ باشد در این صورت دنبالهٔ کشی $(b_n)_n \in \mathbb{N}$ در $\mathbb{Z}$ وجود دارد که به a همگراست. چون دنبالهٔ $(b_n)_n \in \mathbb{N}$ کشی است، برای هر $n \in \mathbb{N}$ عدد $N_n \in \mathbb{N}$ وجود دارد به طوری که برای هر $n, m > N_n$ داریم $|b_n - b_m| < ۲^{-n}$. به بیان دیگر، با توجه به تعریف نرم، برای هر $n, m > N_n$ داریم $b_n \equiv b_m (p^n$به پیمانهٔ$m)$. پس اگر $n, m \geq N_۱$ در این صورت $a_۰ \in \{۰, ۱, \dots, p-۱\}$ وجود دارد که $b_n \equiv b_m \equiv a_۰ (p$به پیمانهٔ$m)$. مشابهاً برای $n, m \geq N_۲$ داریم $b_n \equiv b_m \equiv a'_۱ (p^۲$به پیمانهٔ$m)$ که در آن $a'_۱ \in \{۰, ۱, \dots, p^۲-۱\}$ اما $a'_۱$ را می‌توان به صورت $a_۰ + a_۱ p$ نوشت و $a_۱$ از اینجا حاصل می‌شود. به طور مشابه $a'_۲ \in \{۰, ۱, \dots, p^۳-۱\}$ موجود است که برای هر $n, m \geq N_۳$ داریم $b_n \equiv b_m \equiv a'_۲ (p^۳$به پیمانهٔ$m)$ اما $a'_۲$ را می‌توان به صورت $a_۰ + a_۱ p + a_۲ p^۲$ نوشت.سایز a_i ها به همین طریق به دست می‌آیند. □

لم ۷۶. حلقه $\mathbb{Z}_p$ یک حلقه موضعی هنسلی با ایده‌آل ماکسیمال $p\mathbb{Z}_p$ است.

اثبات. برای اثبات موضعی بودن، کافی است نشان دهیم عناصر وراون پذیر $\mathbb{Z}_p$ دقیقاً آنهائی هستند که نرمشان برابر با یک است تا بتوانیم نتیجه بگیریم ایده‌آل ماکسیمال مجموعه عناصری است که نرم آن‌ها کمتر از یک است. پس فرض کنیم $a = \sum_{i=o}^{\infty} a_i p^i \mathbb{Z}_p$ و $|a| = ۱$. بنابراین $p \nmid a_۰$ و این یعنی $a_۰$ در F_p وارون دارد. اگر b وارون $a_۰$ در F_p باشد آنگاه $q \in \mathbb{Z}$ وجود دارد به طوری که $b.a_۰ b = pq + ۱$ را در a ضرب می‌کنیم،

$$ab = a_۰ b \sum_{i=۱}^{\infty} a_i p^i + b = ۱ + pq + b \sum_{i=۱}^{\infty} a_i p^i$$

واضح است که $|pq + b \sum_{i=۱}^{\infty} a_i p^i| < ۱$ بنابراین ab و در نتیجه a در $\mathbb{Z}_p$ وارون‌پذیر است. پس $p\mathbb{Z}_p$ ایده‌آل ماکسیمال $\mathbb{Z}_p$ است. همچنین بنا به لم هنسل به وضوح $\mathbb{Z}_p$ هنسلی است. □

توجه ۷۷. نگاشت $\varphi : \mathbb{Z}_p \longrightarrow F_p$ با ضابطه $\varphi(\sum_{i=۱}^{\infty} a_i p^i) = a_۰$ همریختی است و $Ker(\varphi) = p\mathbb{Z}_p$. بنابراین $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong F_p$

۴.۷.۲ میدان $\mathbb{Q}_p$

برای هر عدد اول p، مشابه اعداد صحیح، نرم $|.|_p$ را روی اعداد گویا تعریف می‌کنیم. برای هر $x \in \mathbb{Q}$، $|x|_p = ۲^{-v_p(n)}$ به طوری که

$$v_p(x) = n \Longleftrightarrow a = p^n(\frac{r}{s}) \ \ s.t \ \ p \nmid s, p \nmid r$$

به عبارت دیگر اگر $x = \dfrac{a}{b}$ آنگاه $v_p(x) = v_p(a) - v_p(b)$. کامل سازی $\mathbb{Q}$ با نرم $|.|_p$ را با $\mathbb{Q}_p$ نمایش می‌دهیم و به آن میدان p–ادیک‌ها گوییم. پس عناصر $\mathbb{Q}_p$ را می‌توان حد دنباله‌های کشی از اعضای $\mathbb{Q}$ با نرم $|.|_p$ در نظر گرفت. همچنین واضح است که $\mathbb{Z}_p \subseteq \mathbb{Q}_p$.

قضیه ۷۸ (قضیهٔ اَکس–کوچن و ارشف). فرض کنید (K,O) و (K',O') دو میدان ارزیابی هنسلی با میدان باقی‌ماندهٔ k و k' و گروه ارزیابِ Γ و Γ' باشند. فرض کنید k میدانی با مشخصهٔ صفر باشد آنگاه

$$(K,O) \equiv (K',O') \Longleftrightarrow k \overset{\mathcal{L}_{ring}}{\equiv} k', \Gamma \overset{\mathcal{L}_{oag}}{\equiv} \Gamma'$$

به بیان دیگر دو میدان ارزیابی هم ارز مقدماتی هستند هرگاه میدان باقی‌ماندهٔ آن‌ها در زبان حلقه‌ها و گروه ارزیاب آن‌ها در زبان گروه‌های آبلی مرتب هم ارز مقدماتی باشند.

۸.۲ میدان سری‌های هان

فرض کنید K یک میدان و $(\Gamma, +, <)$ یک گروه آبلی مرتب باشد. به $f = \sum\limits_{\gamma \in \Gamma} a_\gamma t^\gamma$ که $a_\gamma \in K$ و $\gamma \in \Gamma$ یک سری هان گوییم هرگاه $supp(f) = \{\gamma | a_\gamma \neq ۰\}$ خوش ترتیب باشد. مجموعهٔ سری‌های هان را با $K((\Gamma))$ نمایش می‌دهیم که به صورت زیر است:

$$K((\Gamma)) = \{f = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma | \text{خوش ترتیب است} \ supp(f)\}$$

یعنی در $supp(f)$ هیچ دنبالهٔ نامتناهی نزولی وجود ندارد.

فرض کنید $f = \sum\limits_{\gamma \in \Gamma} a_\gamma t^\gamma$ و $g = \sum\limits_{\gamma \in \Gamma} b_\gamma t^\gamma$، مجموعهٔ $K((\Gamma))$ همراه با اعمال جمع و ضرب زیر یک حلقه است:

$$f + g = \sum_{\gamma \in \Gamma} (a_\gamma + b_\gamma) t^\gamma$$

$$f.g = (\sum_{\gamma \in \Gamma} a_\gamma t^\gamma)(\sum_{\gamma \in \Gamma} b_\gamma t^\gamma) = \sum_{\gamma \in \Gamma} \sum_{\gamma_۱ + \gamma_۲ = \gamma} a_{\gamma_۱} b_{\gamma_۲} t^\gamma$$

ملاحظه ۷۹. حلقهٔ $K((\Gamma))$ یک میدان است زیرا اگر $f \neq ۰$ آنگاه $f = \sum\limits_{\gamma \in \Gamma} a_\gamma t^\gamma = a_\gamma T^\gamma (۱ - \epsilon)$ به طوری که $\epsilon \in K((\Gamma))$ و $a_\gamma \in K^\times$. می‌دانیم اگر $|\epsilon| < ۱$ آنگاه $\dfrac{۱}{۱ - \epsilon} = ۱ + \epsilon + \epsilon^۲ + \epsilon^۳ + \ldots$. در نظر می‌گیریم $g = \sum_{n=۰}^{\infty} \epsilon^n$. بنابراین g وارون $۱ - \epsilon$ است زیرا $g(۱ - \epsilon) = ۱ + \epsilon + \epsilon^۲ + \epsilon^۳ + \ldots (-\epsilon - \epsilon^۲ - \epsilon^۳ - \ldots) = ۱$

در نتیجه معکوس f به صورت زیر است:

$$f^{-1} = \frac{1}{a}T^{-\gamma}\frac{1}{1-\epsilon} = \frac{1}{a}T^{-\gamma}g.$$

نگاشت ارزیابی روی میدان سری‌های هان به صورت زیر تعریف می‌کنیم:

$$v : K((\Gamma)) \longrightarrow \Gamma$$

$$v(\sum a_\gamma t^\gamma) := min\{\gamma : a_\gamma \neq 0\}.$$

دقت کنید تعریف بالا خوش تعریف است زیرا $supp(f)$ خوش ترتیب است در نتیجه $min\{\gamma\}$ وجود دارد. برای هر $f \in K((\Gamma))$ داریم $v(f) \in \Gamma$. بنابراین گروه ارزیاب v خود Γ است. حلقهٔ ارزیاب $K((\Gamma))$ را به صورت $K[[\Gamma]]$ نشان می‌دهیم و به شکل زیر است:

$$O_v = \{f | v(f) \geq 0\} = \{f \text{هایی که اولین توان آن ها بزرگتر یا مساوی صفر باشد} | f\}$$

$$= \{f \text{هایی که توان منفی نداشته باشند} | f\}$$

میدان باقی‌مانده‌های $K((\Gamma))$ برابر K است. زیرا اگر نگاشت

$$h : O_v \longrightarrow K$$

$$f \longmapsto t^\circ \text{ضریب}$$

را در نظر بگیرید آنگاه $ker(h) = \{f | \text{کوچکترین توان f مثبت است}\}$ که همان $m_v = \{f | v(f) > 0\}$ است در نتیجه

$$\frac{O_v}{ker(h)} \cong \frac{O_v}{m_v} \cong K$$

برای مثال اگر $\Gamma = \mathbb{Z}$ را در نظر بگیریم آنگاه $K((t^\gamma))$ همان میدان سری‌های لوران است یعنی همان $K((t))$ که حلقه ارزیاب آن $K[[t]]$ است.

ملاحظه ۸۰. نشان دادیم $K((\Gamma_1))$ یک میدان است بنابراین اگر Γ_1 و Γ_2 گروه‌های آبلی مرتب باشند، می‌توان میدان $K((\Gamma_1))((\Gamma_2))$ را به صورت زیر تعریف کرد:

$$K((\Gamma_1))((\Gamma_2)) = \{f | f = \sum a_\gamma t^\gamma, a_\gamma \in K((\Gamma_1)), \gamma \in \Gamma_2, \text{خوش ترتیب است} \, supp(f)\}$$

و با توجه به آن چه در بالاتر گفته شد روی میدان $K((\Gamma_1))((\Gamma_2))$ می‌توان یک نگاشت ارزیابی تعریف کرد که حلقه ارزیاب آن به صورت $K((\Gamma_1))[[\Gamma_2]]$ است. در واقع یکی از کاربردهای میدان سرهای هان این است که اگر میدان K و گروه آبلی مرتب Γ را داشته باشیم، می‌توانیم میدان $K((\Gamma))$ را بسازیم که گروه ارزیاب آن Γ و میدان باقی‌ماندهٔ آن K باشد.

فصل ۳

یک میدان ارزیابی هنسلی تعریف‌پذیر با پیچیدگی سوری بالا

منظور از $(K_۱, O_۱)$ یک میدان ارزیابی هنسلی $K_۱$ با حلقهٔ ارزیاب $O_۱$ است که مانند مثال ۲۴، $O_۱$ به عنوان یک محمول تک موضعی در ساختار $K_۱$ در نظر گرفته شد. در این فصل ابتدا قضیهٔ مورد نظر پایان نامه و مسیر اثبات آن را شرح می‌دهیم و در بخش بعدی به اثبات قضیه و بررسی مثال مشخص $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})((\Gamma_۱))((\Gamma_۲))$ می‌پردازیم.

۱.۳ مسیر اثبات

همان طور که گفته شد در این پایان‌نامه به این سوال پرستل [1] پاسخ دهیم که:

سوال ۸۱. آیا یک فرمولِ $\forall\exists$ و یا یک فرمولِ $\exists\forall$ در زبان حلقه‌ها وجود دارد که حلقهٔ ارزیابِ یک میدان ارزیابیِ هنسلی را بدون پارامتر تعریف کند؟

در پاسخ به این سوال، به اثبات قضیهٔ زیر می‌پردازیم:

قضیه ۸۲. گروه‌های آبلی مرتب $\Gamma_۱$ و $\Gamma_۲$ وجود دارند به طوری که برای هرمیدان سودو بستهٔ جبری که $k \neq k^{sep}$ (یعنی میدان k با بستار جدایی‌پذیرش برابر نیست)حلقه ارزیابِ هنسلی $k((\Gamma_۱))[[\Gamma_۲]]$ در میدان $K = k((\Gamma_۱))((\Gamma_۲))$ بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است، اما با هیچ فرمول به صورت $\exists\forall$ و $\forall\exists$ تعریف‌پذیر نیست.

---
[1] Perestel

بنابر محکی از پرستل (که در بخش بعدی دربارهٔ آن خواهیم نوشت)، حلقهٔ ارزیاب در میدانِ ارزیابی هنسلی با فرمول $\exists\forall$ تعریف‌پذیر است اگر و تنها اگر از بستهٔ وجودی بودن $K_۱$ و $K_۲$ نتیجه شود که $O_۱ \subseteq O_۲$. همچنین این حلقهٔ ارزیاب با فرمول $\forall\exists$- تعریف‌پذیر است اگر و تنها اگر اگر از بستهٔ وجودی بودن $K_۱$ و $K_۲$ نتیجه شود که $O_۱ \subseteq O_۲$.
بنابراین جهت ارائه مثال نقض سوال پرستل ۸۱ کافی است یک نشاندنِ بستهٔ وجودی از $K_۱$ به $K_۲$ بیابیم به طوری که $O_۱ \nsubseteq O_۲$. علاوه بر آن یک نشاندنِ بستهٔ وجودی از $K_۱$ به $K_۲$ معرفی کنیم که $O_۲ \cap K_۱ \nsubseteq O_۱$. با توجه به قضیه اکس-کوشن و ارشوف، برای اینکه یک میدان ارزیابی $(K_۱, w, k, \Gamma_۱)$ را در یک میدان ارزیابی $(K_۲, u, k', \Gamma_۲)$ به صورت بستهٔ وجودی بنشانیم کافی است میدان باقی‌ماندهٔ k و گروه ارزیاب آن $\Gamma_۱$ را به ترتیب در k' و گروه ارزیاب $\Gamma_۲$ به صورت بستهٔ وجودی به صورت بستهٔ وجودی بنشانیم. بنابراین به همین جهت نشاندن‌های (۳-۱) و (۳-۲) را ارائه می‌دهیم. مثال خاصی که در این مقاله به آن پرداخته می‌شود میدان ارزیابی هنسلیِ $K := k((\Gamma_۱))((\Gamma_۲))$ برای گروه‌های ارزیاب $\Gamma_۱$ و $\Gamma_۲$ است که در ادامه به دو طریق در خودش می نشانیم.

۲.۳   محکی برای تعریف‌پذیری محمول تک‌موضعی

در این بخش به اثبات قضیهٔ زیر [2] که پرستل در مرجع [۱۲]، آورده است، می‌پردازیم. این قضیه، محکی برای تعریف‌پذیری محمول تک موضعی در یک ساختار در زبان حلقه‌ها است. در ادامه ابتدا صورت قضیه را بیان می‌کنیم و بعد از آن به زبان ساده آن را شرح می‌دهیم.

قضیه ۸۳. فرض کنید $\sum$ یک سیستمِ اصل موضوعه‌ای مرتبهٔ اول در زبان حلقه‌ها به همراه یک محمول تک‌موضعیِ O باشد. در این صورت فرمولِ $\phi(x)$ در زبان حلقه‌ها موجود است به طوری که مجموعهٔ O را در همهٔ مدل‌های $(K, O) \models \sum$ تعریف می‌کند و نوع سوری آن، برای هر دو مدل $(K_۱, O_۱)$ و $(K_۲, O_۲)$ از $\sum$ به شرح زیر است:

$$\exists \text{ iff } (K_۱ \subseteq K_۲ \Rightarrow O_۱ \subseteq O_۲)$$

$$\forall \text{ iff } (K_۱ \subseteq K_۲ \Rightarrow O_۲ \cap K_۱ \subseteq O_۱)$$

$$\exists\forall \text{ iff } (K_۱ \prec_\exists K_۲ \Rightarrow O_۱ \subseteq O_۲)$$

$$\forall\exists \text{ iff } (K_۱ \prec_\exists K_۲ \Rightarrow O_۲ \cap K_۱ \subseteq O_۱)$$

در اینجا $K_۱ \prec_\exists K_۲$ به این معنی است که $K_۱$ از نظر وجودی در $K_۲$ بسته است. برای مثال، هر $\mathcal{L}_{ring}$ فرمول وجودی $\rho(x_۱, x_۲, ...)$ در $K_۱$ که در $K_۲$ برآورده می‌شود در $K_۱$ نیز برآورده می‌شود.

در واقع این قضیه بیان می‌کند که اگر O یک محمولِ تک موضعی در ساختار K باشد آن گاه O توسط یک فرمول $\exists\bar{x}\varphi(\bar{x}, \bar{a})$ (که φ یک فرمول بدون سور است) تعریف می‌شود، هرگاه ما در تئوری از اینکه $K_۱ \subseteq K_۲$ نتیجه بگیریم $O_۱ \subseteq O_۲$. بالعکس اگر $(K_۱, O_۱) \models \sum$ و $(K_۲, O_۲) \models \sum$ اگر از اینکه $K_۱ \subseteq K_۲$ نتیجه بگیریم $O_۱ \subseteq O_۲$ آنگاه

[2] Characterization Theorem

برای هر $\sum \models (K,O)$، O توسط یک فرمول وجودی تعریف می‌شود. همچنین محمول تک‌موضعی O توسط یک فرمول به صورت $\forall$ در زبان حلقه‌ها تعریف می‌شود هرگاه ما در تئوری از اینکه $K_۱ \subseteq K_۲$ نتیجه بگیریم $O_۲ \cap K_۱ \subseteq O_۱$. بالعکس اگر $\sum \models (K_۱,O_۱)$ و $\sum \models (K_۲,O_۲)$ اگر از اینکه $K_۱ \subseteq K_۲$ نتیجه بگیریم $O_۲ \cap K_۱ \subseteq O_۱$، آنگاه برای هر $\sum \models (K,O)$، O توسط یک فرمول به صورت $\forall$ در زبان حلقه‌ها تعریف می‌شود. قضیه ۸۳ نیز بیان می‌کند محمول تک‌موضعی O در ساختار (K,O) با یک فرمول به صورت $\exists\forall$ در زبان حلقه‌ها تعریف می‌شود هرگاه از اینکه $K_۱ \prec_{\exists} K_۲$ یعنی $K_۱$ به طور وجودی در $K_۲$ بسته باشد، نتیجه بگیریم $O_۱ \subseteq O_۲$. بالعکس اگر برای هر $\sum \models (K_۱,O_۱)$ و $\sum \models (K_۲,O_۲)$ اگر از اینکه $K_۱ \prec_{\exists} K_۲$ نتیجه بگیریم $O_۱ \subseteq O_۲$ آنگاه برای هر $\sum \models (K,O)$، O توسط یک فرمولِ $\exists\forall$ تعریف می‌شود. همچنین این قضیهٔ برای حالت $\forall\exists$ می‌گوید، اگر از اینکه $K_۱ \prec_{\exists} K_۲$ نتیجه بگیریم $O_۲ \cap K_۱ \subseteq O_۱$ محمول تک‌موضعی O توسط یک فرمول $\forall\exists$ در ساختار (K,O) در زبان حلقه‌ها تعریف‌پذیر است. در نهایت اگر $\sum \models (K_۱,O_۱)$ و $\sum \models (K_۲,O_۲)$ اگر از اینکه $K_۱ \prec_{\exists} K_۲$ نتیجه بگیریم $O_۲ \cap K_۱ \subseteq O_۱$، آنگاه برای هر $\sum \models (K,O)$، محمول تک‌موضعی O توسط یک فرمولِ $\forall\exists$ در زبان حلقه‌ها تعریف می‌شود.

قبل از پرداختن به اثبات قضیهٔ ۸۳ ، توجه شود که، اگر $(K_۱,O_۱,a_۱)$ و $(K_۲,O_۲,a_۲)$ دو $\mathcal{L}(O,c)$− ساختار و Φ مجموعه‌ای از $\mathcal{L}(O,c)$− فرمول‌ها باشند، منظور از $(K_۱,O_۱,a_۱) \overset{\Phi}{\rightsquigarrow} (K_۲,O_۲,a_۲)$ این است که هر فرمولِ $\phi \in \Phi$ که در $(K_۱,O_۱,a_۱)$ برقرار است در $(K_۲,O_۲,a_۲)$ نیز برقرار باشد. به علاوه در اثبات قضیه ۸۳ از قضیهٔ زیر که بدون اثبات آن را می‌پذیریم، استفاده می‌کنیم:

قضیه ۸۴. [۱۲، قضیه۱] فرض کنید در تمام مدل‌های (K_i,O_i,a_i) از تئوری $\sum$ داشته باشیم:

$$(K_۱,O_۱,a_۱) \overset{\Phi}{\rightsquigarrow} (K_۲,O_۲,a_۲) \Longrightarrow (K_۱,O_۱,a_۱) \overset{\{c \in O\}}{\rightsquigarrow} (K_۲,O_۲,a_۲)$$

آنگاه $c \in O$ توسط یک فرمول در Φ قابل تعریف است. به بیان دیگر اگر از این که مدل‌های تئوری نسبت به همهٔ فرمول‌های موجود در Φ هم‌نظر هستند، نتیجه شود که نسبت به حضورِ c در O نیز هم‌نظر هستند آنگاه، $c \in O$ توسط یک فرمول در Φ قابل تعریف است. یعنی هرگاه بتوانیم از این که فرمول‌های موجود در Φ که در $K_۱$ درست هستند، درست بودن آن‌ها در $K_۲$ را نتیجه بگیریم آنگاه

$$K_۱ \models a_۱ \in O_۱ \Rightarrow K_۲ \models a_۲ \in O_۲$$

اثبات. قضیه۸۳ (حالت $\exists$): Φ را مجموعهٔ تمام فرمول‌هایی در $\mathcal{L}(c)$ در نظر می‌گیریم که به صورت $\exists$ باشند. همچنین فرض کنیم برای همهٔ مدل‌های تئوری $\sum$ داشته باشیم $K_۱ \subseteq K_۲ \Rightarrow O_۱ \subseteq O_۲$. اگر $(K_۱,O_۱)$ و $(K_۲,O_۲)$ دو مدل از $\sum$ باشند به طوری که $(K_۱,O_۱,a_۱) \overset{\Phi}{\rightsquigarrow} (K_۲,O_۲,a_۲)$. نشان می‌دهیم اگر $a_۱ \in O_۱$ آنگاه $a_۲ \in O_۲$. فرض کنیم $a_۲ \notin O_۲$. حال مجموعهٔ $\prod = Diag(K_۱,a_۱,(b)_{b\in K_۱}) \cup Th(K_۲,O_۲,a_۲)$ را در زبان حلقه‌ها در نظر بگیرید. نشان می‌دهیم $\prod$ دارای مدل است. بنابر قضیهٔ فشردگی برای اثبات این که تئوری فوق دارای مدل است کافی است اثبات کنیم که هر بخشِ متناهی از آن دارای مدل است. فرض کنید $\Delta \subseteq \prod$ متناهی و دارای مدل نباشد یعنی $b_۱,\ldots,b_n \in K_۱$ و $\mathcal{L}$− فرمول χ موجود است که $\chi(a_۱,b_۱,\ldots,b_n) \in Diag(K_۱)$ به طوری که $\{\chi\} \cup Th(K_۲,O_۲,a_۲)$ سازگار

نیست. بنابراین فرمول $\varphi(c) \equiv \exists b_۱, \ldots, b_n \chi(c, \bar{b})$ در زبان $\mathcal{L}(c)$ موجود است که در $(K_۱, O_۱)$ برقرار است و $Th(K_۲, O_۲, a_۲) \vdash \forall b_۱, \ldots, b_n \neg\chi(c, \bar{b})$ و این غیر ممکن است زیرا $\varphi(c)$ یک فرمول وجودی است و بنابر فرض اگر در $(K_۱, a_۱)$ صدق می‌کند آنگاه در $(K_۲, a_۲)$ نیز صدق می کند. در نتیجه $\prod$ دارای مدل است برای مثال این مدل را $(K_۲^*, O_۲^*, a_۲^*)$ در نظر می‌گیریم. داریم $K_۱ \subseteq K_۲^*$ و $a_۱ \in O_۱$ و $a_۱ = a_۲^* \notin O_۲^*$ در نتیجه $O_۱ \nsubseteq O_۲^*$ و با توجه به فرض به تناقض می‌رسیم.

(حالت $\exists\forall$): برای این حالت فرض کنیم برای همهٔ مدل‌های (K_i, O_i) از تئوری $\sum$ داشته باشیم $K_۱ \overset{\exists}{\subseteq} K_۲ \to O_۱ \subseteq O_۲$. اکنون تئوری $\prod_\forall = Th_\forall(K_۱, a_۱, (b)_{b \in K_۱}) \cup Th(K_۲, O_۲, a_۲)$ که $Th_\forall(K_۱, a_۱, (b)_{b \in K_۱})$ مجموعهٔ تمام فرمول‌های به صورت $\forall$ یعنی به شکل $\varphi(x, \bar{b}) \equiv \forall y_۱, \ldots, y_n \chi(c, \bar{y}, \bar{b})$ (که χ فرمولی بدون سور است)را در نظر می‌گیریم و مانند حالت قبل نشان می‌دهیم این تئوری دارای مدل است.

(حالت $\forall\exists$ و $\forall$): در حالت‌های $\forall\exists$ و $\forall$ به ترتیب تئوری‌های

$$\prod = Diag(K_۲, a_۲, (b)_{b \in K_۲}) \cup Th(K_۱, O_۱, a_۱)$$

و

$$\prod_\forall = Th_\forall(K_۲, a_۲, (b)_{b \in K_۱}) \cup Th(K_۱, O_۱, a_۱)$$

را در نظر گرفته و مانند حالت‌های قبل نشان می‌دهیم این تئوری‌ها دارای مدل هستند. $\square$

۳.۳ ساخت میدان ارزیابی هنسلی مورد نظرِ پایان‌نامه

در این بخش جهت اثبات قضیهٔ ۸۹ به ساخت یک میدان ارزیابی هنسلی $k((\Gamma_۱))((\Gamma_۲))$ با استفاده از گروه‌های $\Gamma_۱$ و $\Gamma_۲$ و میدان باقی‌ماندهٔ k که در واقع مثال نقضی برای سوال پرستل ۸۱ خواهد بود، می‌پردازیم.

گروه‌های آبلی مرتب زیر را در نظر بگیرید:

$$X := \mathbb{Z}_{(۲)} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, ۲ \nmid b, (a, b) = ۱\}$$

و

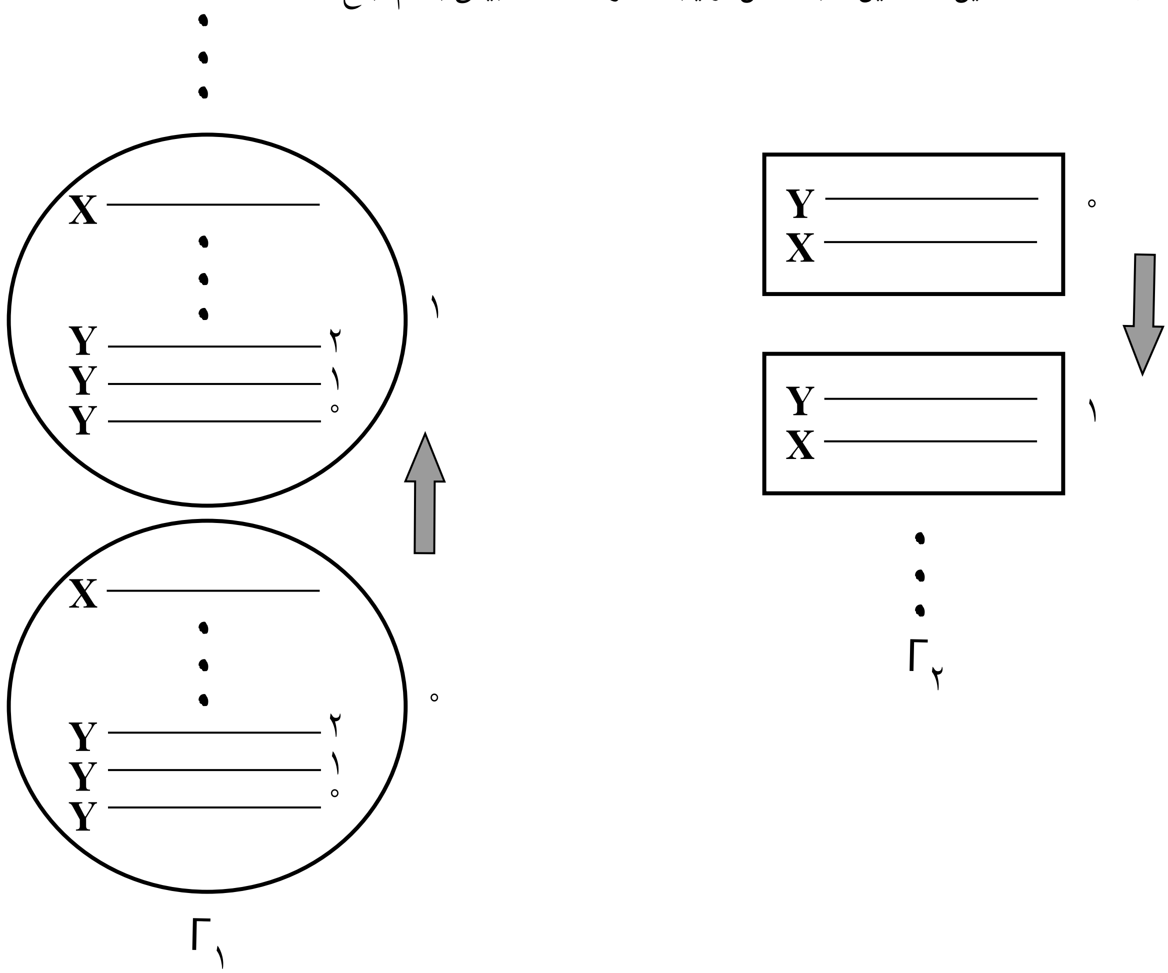
$$Y := \mathbb{Z}_{(۳)} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, ۳ \nmid b, (a, b) = ۱\}$$

فرض کنید $(\mathbb{N}, <)$ مجموعهٔ اعداد طبیعی با ترتیب معمول باشد و $(\mathbb{N}', <)$ مجموعهٔ اعداد طبیعی با عکس ترتیب معمول باشد، آنگاه گروه‌های $\Gamma_۱$ و $\Gamma_۲$ را به صورت زیر تعریف می‌کنیم:

$$\Gamma_۱ := \bigoplus_{\mathbb{N}}((\bigoplus_{\mathbb{N}} Y) \oplus X)$$

$$\Gamma_۲ := \bigoplus_{\mathbb{N}'}(X \oplus Y).$$

گروه‌های Γ_1 و Γ_2 را می‌توانیم توسط تصویرهای صفحهٔ بعد تصور کنیم. در واقع هر دایره در تصویر Γ_1 نشان دهندهٔ $X \oplus (\bigoplus Y)$ است یعنی در هر دایره شمارا تا $\mathbb{Z}_{(3)}$ به علاوه یک $\mathbb{Z}_{(2)}$ با ترتیب معمول روی اعداد طبیعی در نظر گرفته شده است. در نهایت در Γ_1 شمارا تا از این دایره‌ها با ترتیب معمول اعداد طبیعی با هم جمع شده‌اند. همچنین هر مستطیل در تصویر Γ_2 نشان دهندهٔ $X \oplus Y$ است یعنی در هر مستطیل یک $\mathbb{Z}_{(3)}$ با یک $\mathbb{Z}_{(2)}$ در نظر گرفته شده است که در نهایت در Γ_2 شمارا تا از این مستطیل‌ها با عکس ترتیب معمول اعداد طبیعی با هم جمع شده‌اند.

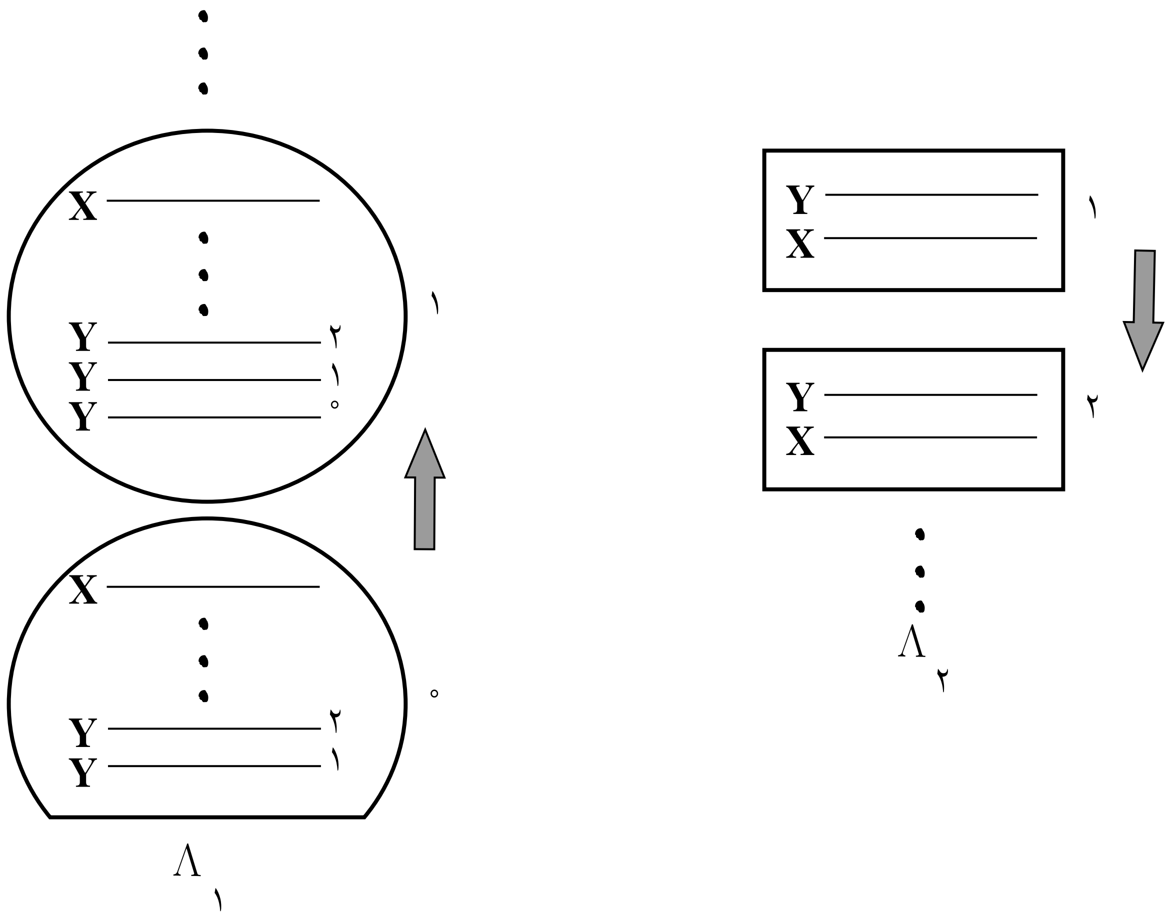


زیرگروه Λ_1 از گروه Γ_1 و زیرگروه Λ_2 از گروه Γ_2 را به صورت زیر در نظر می‌گیریم:

$$\Lambda_1 := ((\bigoplus_{\mathbb{N}-\{0\}}) \oplus X) \oplus (\bigoplus_{\mathbb{N}-\{0\}} (\bigoplus_{\mathbb{N}} Y) \oplus X))$$

$$\Lambda_2 := \bigoplus_{\mathbb{N}'-\{0\}} (X \oplus Y).$$

با توجه به گزارهٔ ۳۵ زیرگروه‌های Λ_1 و Λ_2 به ترتیب زیرگروه‌هایی محدب در Γ_1 و Γ_2 هستند که در ادامه تصویر آنها را قرار دادیم. در واقع Λ_1 مثل این است که یک $\mathbb{Z}_{(3)}$ از پایین دایرهٔ اول برداشته‌ایم و Λ_2 به این صورت است که، کلاً مستطیل اول از Γ_2 را برداشته‌ایم.

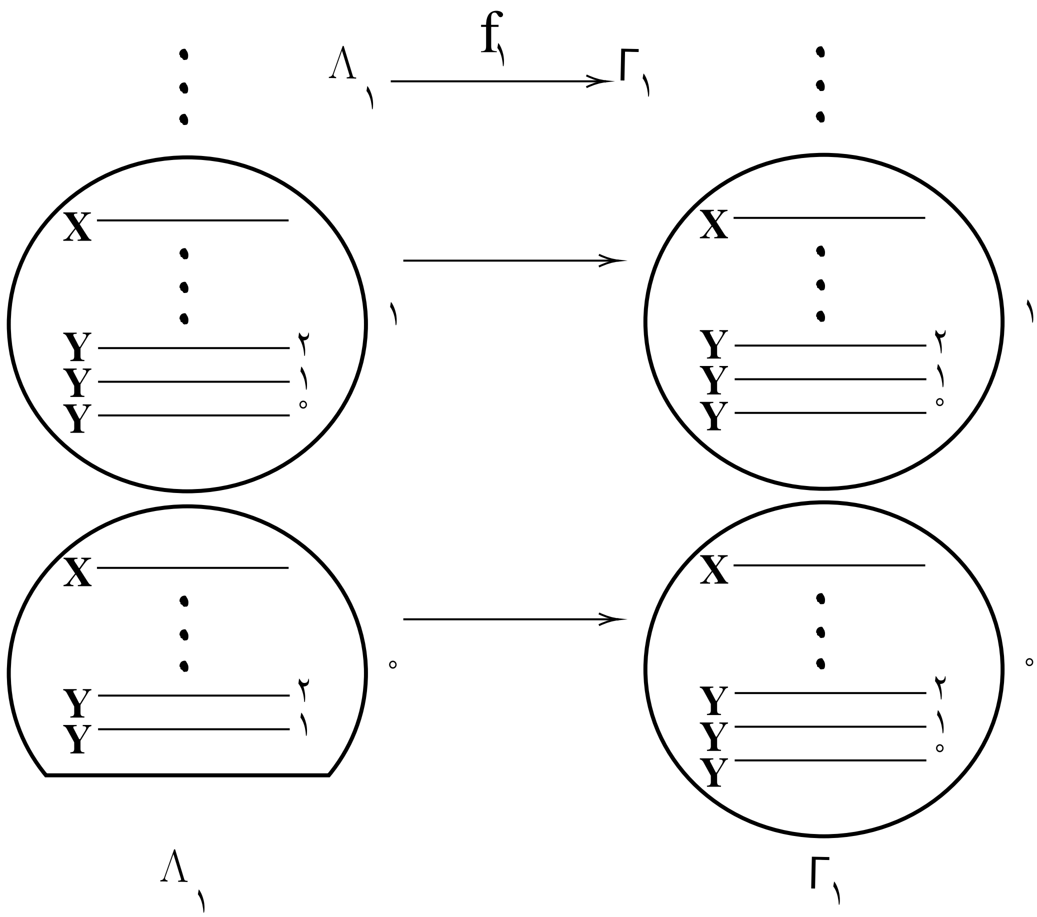


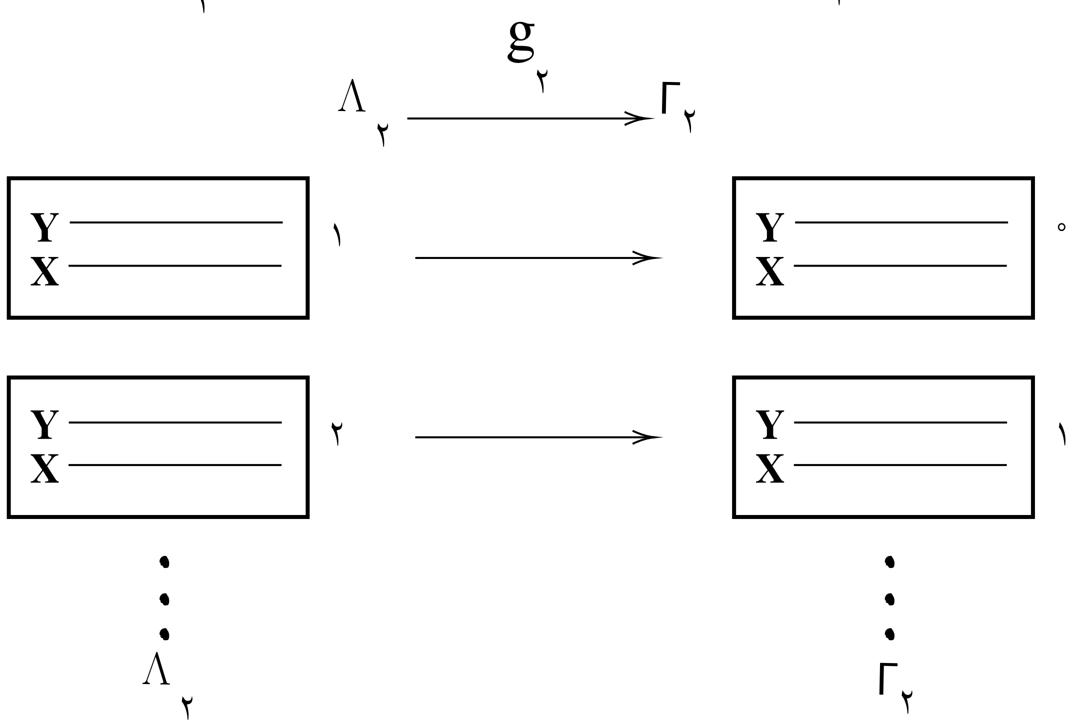
از Λ_1 به Γ_1 ایزومرف f_1 را داریم. تنها کافی است نگاشت همانی را در نظر بگیریم که هر طبقه از Λ_1 را به یک طبقهٔ Γ_1 می‌برد. ایزومرف g_2 نیز به همین صورت است که هر مستطیل در Λ_2 به یک مستطیل در Γ_2 به صورت ایزومرف می‌برد. بنابراین

$$f_1 : \Lambda_1 \xrightarrow{\sim} \Gamma_1$$

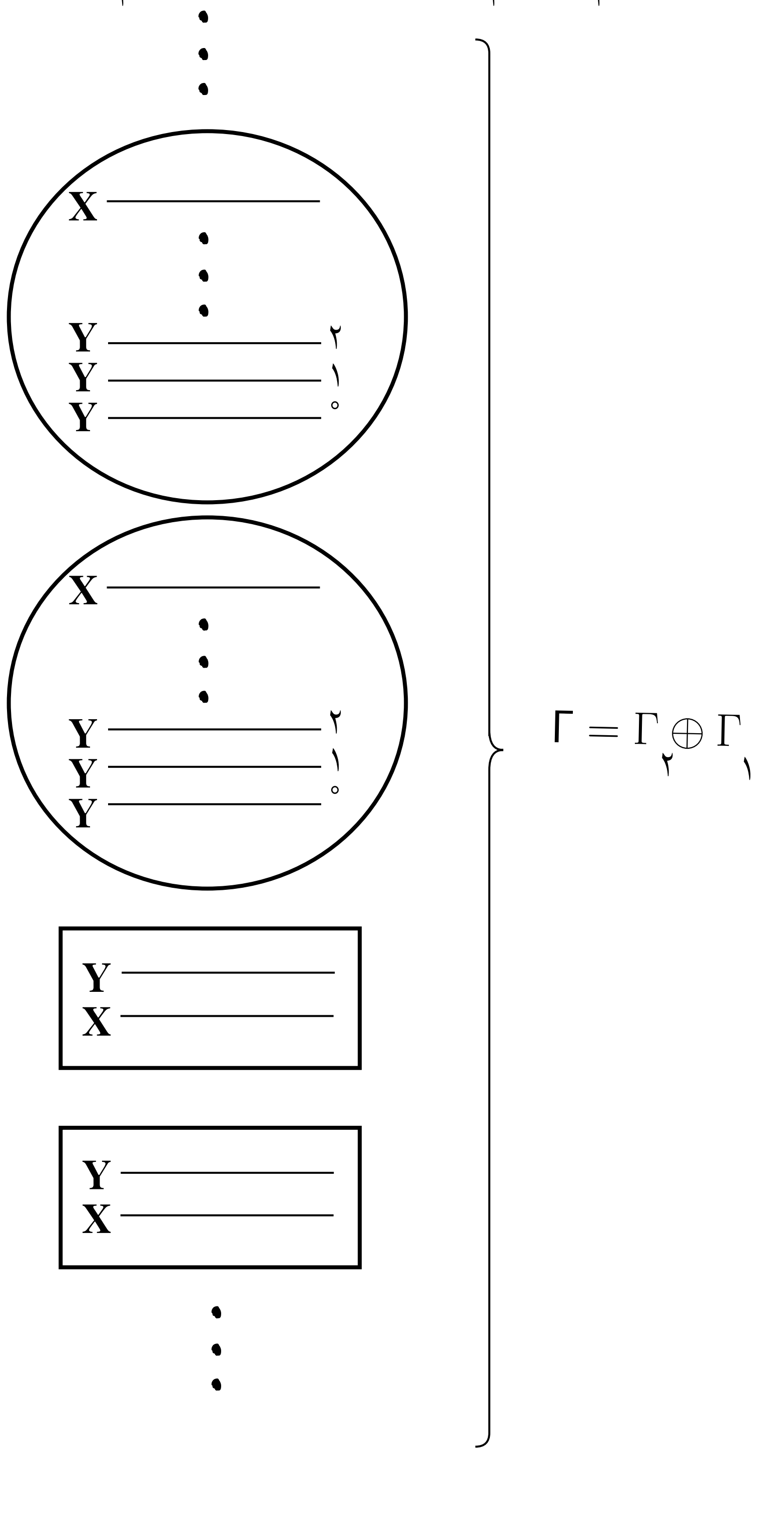
$$g_2 : \Lambda_2 \xrightarrow{\sim} \Gamma_2$$

در ادامه می‌توانیم f_1 و g_2 را به این صورت تصور کنیم.


f۱
Λ۱
Γ۱
X
Y۲
Y۱
Y۰
۱
۰


g۲
Λ۲
Γ۲
Y
X
۱
۲
۰

گروه Γ را به صورت $\Gamma := \Gamma_2 \oplus \Gamma_1$ تعریف می‌کنیم. می‌توانیم شکل Γ را به صورت زیر تصور کنیم.



یکی از نکات جالب و مهم گروه‌های تعریف شده تا اینجا این است که $\Gamma_۱$ در Γ تعریف‌پذیر است که در ادامه اثبات می‌کنیم $\Gamma_۱$ در Γ اولین جایی است که دو تا Y پشت سرهم می‌آیند و آن را با فرمولی در زبان گروه‌های آبلی مرتب تعریف می‌کنیم. در ادامه به طور دقیق‌تر این مطلب را بررسی می‌کنیم.

لم ۸۵. $\Gamma_۱$ در Γ بدون پارامتر در زبانِ $\mathcal{L}_{oag}$، تعریف‌پذیر است.

اثبات. می‌دانیم زبانِ گروه‌های آبلی مرتب $\mathcal{L}_{oag} = \{+, -, ., <\}$ است. بنا به آنچه در بخش ۳.۳ گفته شد، اگر گروه‌های آبلی مرتب X و Y را به صورت

$$X := \mathbb{Z}_{(۲)} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, ۲ \nmid b, (a, b) = ۱\}$$

و

$$Y := \mathbb{Z}_{(۳)} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, ۳ \nmid b, (a, b) = ۱\}$$

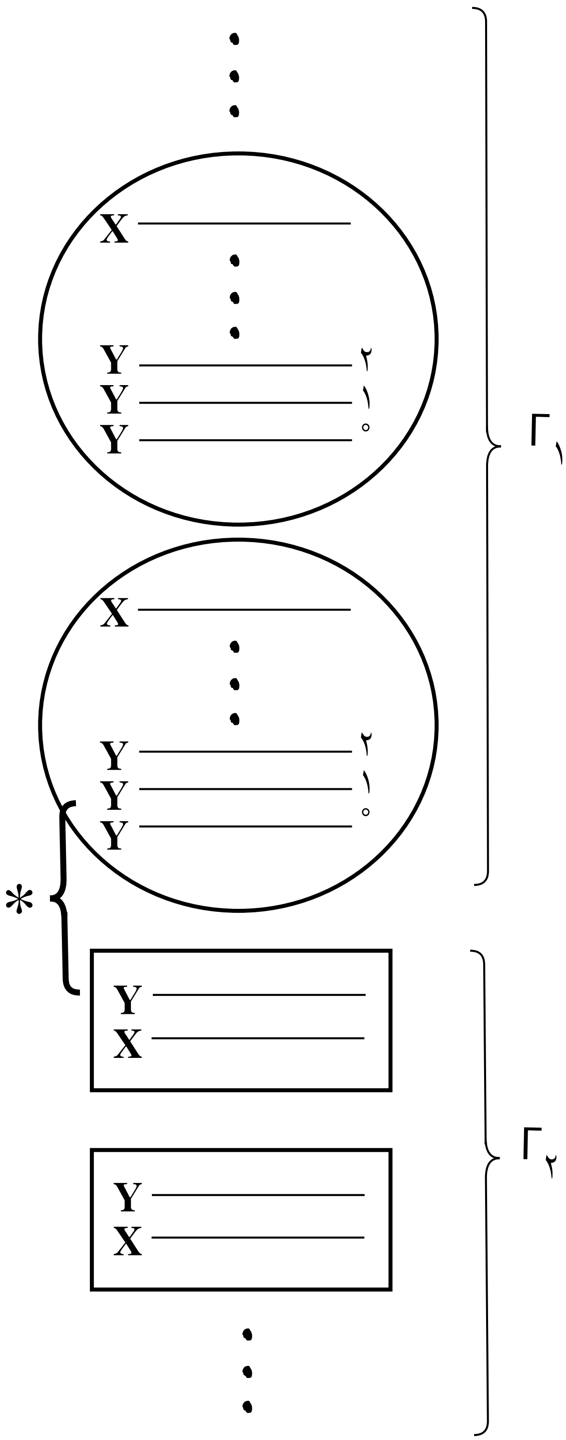
در نظر بگیریم آنگاه گروه Γ را می‌توانیم به صورت $\Gamma = \bigoplus_{j \in J} G_j$ بنویسیم به طوری که $G_j \in \{X, Y\}$ باشد. در واقع چون گروه $\Gamma := \Gamma_۲ \oplus \Gamma_۱$ تعریف شده است و $\Gamma_۱$ و $\Gamma_۲$ جمع مستقیم X ها و Y ها بودند، آنگاه $\Gamma = \bigoplus_{j \in J} G_j$ ، یعنی X و Y ها را پشت سر هم بنویسیم. کوچکترین اندیس $k \in J$ وجود دارد که بلافاصله بعد از آن اندیس k' است که $G_k = G_{k'} = Y$. در واقع اندیس k اولین جایی که دو تا Y پشت سرهم می‌آیند. بنابراین اولین جایی که دو تا Y پشت سر هم می‌آیند گروه $\Gamma_۱$ شروع می‌شود. به بیان دیگر $\Gamma_۱ = \bigoplus_{j \in J, j > k} G_j$. به شکل صفحهٔ بعد دقت کنید. اولین جایی که دو تا Y پشت سرهم می‌آیند را با $*$ نشان دادیم.
ایدهٔ اثبات این است که این موضوع را با یک فرمول بیان کنیم. در واقع نشان دهیم مجموعهٔ اندیس‌ها یعنی $(J, <)$ در Γ تعبیرپذیر است. در ادامه این تعبیرپذیری را به طور مختصر می‌آوریم. فرض کنید $r \in \mathbb{N}$ عنصر ثابت باشد. برای $x \in \Gamma \setminus r\Gamma$، فرض کنید $F_r(x)$ بزرگترین زیر گروه محدب Γ باشد که از $x + r\Gamma$ مجزا باشد. برای عنصر ثابتِ r، بنا به [۱۳، لم۲۰۱۱] یا [۴، لم۲۰۱] $F_r(x)$ به طور یکنواخت در x تعریف‌پذیر است. به بیان دقیق‌تر:

$$y \in F_r(x) \iff [۰, max\{-y, y\}] \cap x + r\Gamma = \phi$$

بنا به [۱۳، مثال۱۲] چون تمام G_jها ارشمیدسی هستند، آنگاه مجموعهٔ گروه‌های به فرم $F_r(x)$ که $x \in \Gamma \setminus r\Gamma$ دقیقاً برابر مجموعهٔ گروه‌های به فرم $\bigoplus_{j \in J, j > j_۰} G_j$ است که G_j، r- بخش‌پذیر نیست. بنابراین تعبیرپذیری $J := (\Gamma \setminus ۶\Gamma)/ \sim_۶$، را که $x \sim_r x' \iff F_r(x) = F_r(x')$ برقرار است. علاوه بر آن داریم

$$J_Y := (\Gamma \setminus ۳\Gamma)/ \sim_۳ = \{j \in J | G_j = Y\}.$$

ترتیب روی J نیز تعریف‌پذیر است زیرا $x/ \sim_۶ \leq x'/ \sim_۶ \iff F_۶(x) \supseteq F_۶(x')$. در نتیجه اندیس $k \in J$ بنابر آنچه گفته شد، $\varnothing$- تعریف‌پذیر است و داریم $F_۶(x) = \Gamma_۱$ برای هر $x \in \Gamma \setminus ۶\Gamma$ که $k = x/ \sim_۶$. □


X
Y ۲
Y ۱
Y ۰
X
Y ۲
Y ۱
Y ۰
*
Y
X
Y
X
$\Gamma_۱$
$\Gamma_۲$

ملاحظه ۸۶. می‌دانیم $\frac{G_1 \oplus G_2}{G_1} \cong G_2$ بنابراین داریم

$$\frac{\Gamma_1}{\Lambda_1} = Y = \mathbb{Z}_{(3)}$$

و

$$\frac{\Gamma_2}{\Lambda_2} = Y = X \oplus Y = \mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(3)}$$

۴.۳ نشاندن‌های گروه ارزیاب

در این بخش گروه Γ را به دو طریق به صورت بستهٔ وجودی در خودش می‌نشانیم. در این روند از قضیهٔ زیر بهره می‌بریم.

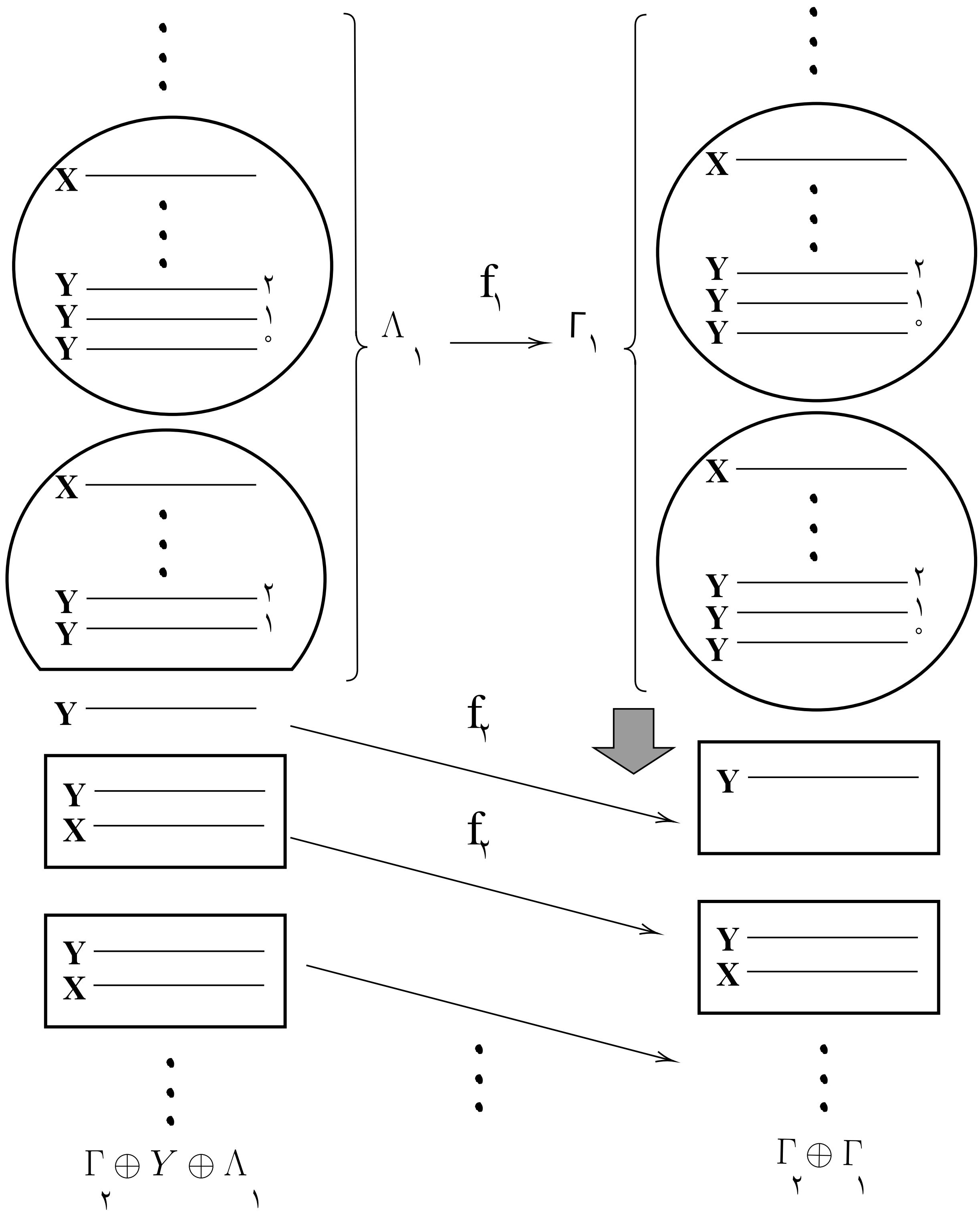
قضیه ۸۷. [۱۴، نتیجه۴.۱و۷.۱] فرض کنید G_1 و G_2 دو گروه آبلی مرتب باشند.
۱.اگر G_1 زیرگروه محدبِ G_2 باشد، آنگاه G_1 در G_2 به طور وجودی بسته است.
۲.جمع مستقیمِ $G = G_1 \oplus G_2$ را در نظر بگیرید. فرض کنید G'_1 (به ترتیب G'_2) زیرگروه مرتبِ G_1 (به ترتیب G_2) که به طور وجودی در G_1 (به ترتیب G_2) بسته است . اگر $G' := G'_2 \oplus G'_1$، آنگاه G' در G به طور وجودی بسته است.
در واقع قضیه بیان می‌کند اگر $G = G_1 \oplus G_2$ و اگر G'_1 در G_1 بسته باشد و G'_2 در G_2 بسته باشد آنگاه جمع آنها یعنی $G' := G'_2 \oplus G'_1$ نیز در G بسته است.

در ادامه دو نشاندن از Γ به خودش ارائه می‌دهیم.
(نشاندن اول): می‌دانیم $\Gamma = \Gamma_2 \oplus \Gamma_1$. برای آنکه Γ را در خودش به صورت بستهٔ وجودی بنشانیم، بنا به تعریف $\Gamma_1 = Y \oplus \Lambda_1$، می‌توان Γ را به صورت $\Gamma_2 \oplus Y \oplus \Lambda_1$ در نظر گرفت یعنی:

$$\Gamma = \Gamma_2 \oplus \Gamma_1 = \Gamma_2 \oplus Y \oplus \Lambda_1$$

نشاندن $f_3 : \Gamma \longrightarrow \Gamma$ ترکیبی ازنشاندن‌های $f_1 : \Lambda_1 \longrightarrow \Gamma_1$ و $f_2 : \Gamma_2 \oplus \longrightarrow \Gamma_2$ است. نشاندن f_1 همان نشاندن همانی که در بخش ۳.۳ دربارهٔ آن بحث کردیم، است و نشاندن f_2 به این صورت عمل می‌کند که Γ_2 را یک طبقه به پایین فرو می‌کشاند و در طبقهٔ خالی Y را می‌نشاند و بقیهٔ طبقه‌ها را نظیر به نظیر می‌نشاند. در نتیجه داریم:

$$f_3 : \Gamma_2 \oplus \Gamma_1 = \Gamma_2 \oplus Y \oplus \Lambda_1 \cong \underbrace{f_2(\Gamma_2 \oplus Y)}_{\prec_\exists} \oplus \underbrace{f_1(\Lambda_1)}_{=\Gamma_2} \prec_\exists \Gamma_2 \oplus \Gamma_1 \qquad (۱-۳)$$

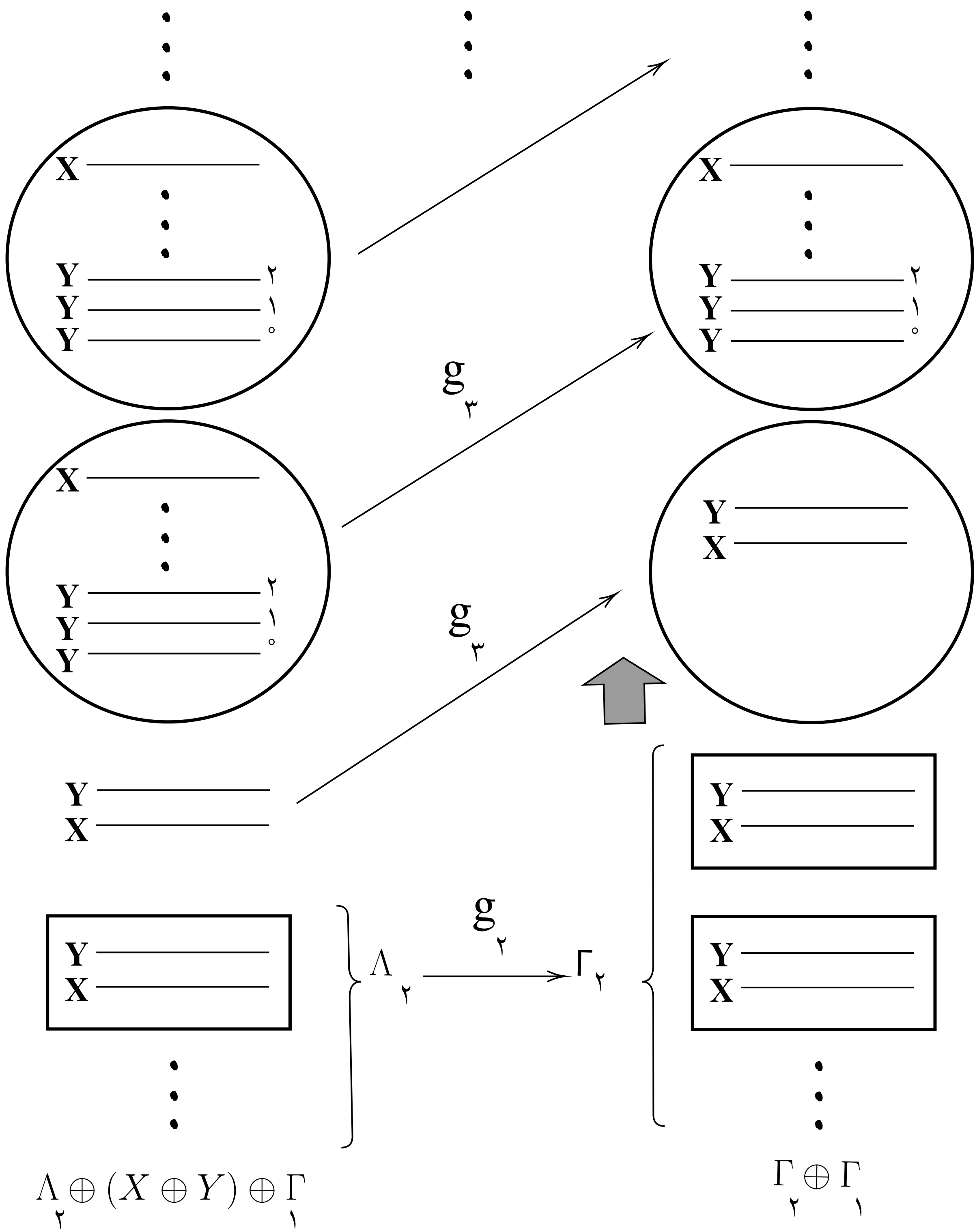

X
Y۲
Y۱
Y۰
f۱
Λ۱
Γ۱
Y
f۲
Γ۲ ⊕ Y ⊕ Λ۱
Γ۲ ⊕ Γ۱

(نشاندن دوم): مانند روش قبل می‌دانیم $\Gamma = \Gamma_۲ \oplus \Gamma_۱$. برای آنکه Γ را در خودش به صورت بستهٔ وجودی بنشانیم، بنا به تعریف $\Gamma_۲ = \Lambda_۲ \oplus (X \oplus Y)$، می‌توان Γ را به صورت $\Lambda_۲ \oplus (X \oplus Y) \oplus \Gamma_۱$ در نظر گرفت یعنی:

$$\Gamma = \Gamma_۲ \oplus \Gamma_۱ = \Lambda_۲ \oplus (X \oplus Y) \oplus \Gamma_۱$$

نشاندن $g_۳ : \Gamma \longrightarrow \Gamma$ ترکیبی ازنشاندن‌های $g_۲ : \Lambda_۲ \longrightarrow \Gamma_۲$ و $g_۱ : (X \oplus Y) \oplus \Gamma_۱ \longrightarrow \Gamma_۱$ است. نشاندن $g_۲$ همان نشاندن همانی که در بخش ۳.۳ دربارهٔ آن بحث کردیم، است و نشاندن $g_۱$ به این صورت عمل می‌کند که $\Gamma_۱$ را یک طبقه به بالا می‌کشاند و در طبقهٔ خالی $X \oplus Y$ را می‌نشاند و بقیهٔ طبقه‌ها را نظیر به نظیر می‌نشاند. در نتیجه داریم:

$$g_۳ : \Gamma_۲ \oplus \Gamma_۱ = \Lambda_۲ \oplus (X \oplus Y) \oplus \Gamma_۱ \cong \underbrace{g_۲(\Lambda_۲)}_{\prec_\exists} \oplus \underbrace{g_۱((X \oplus Y) \oplus \Gamma_۱)}_{=\Gamma_۲} \prec_\exists \Gamma_۲ \oplus \Gamma_۱ \qquad (۲-۳)$$


X
Y ۲
Y ۱
Y ۰
X
Y ۲
Y ۱
Y ۰
g ۳
X
Y ۲
Y ۱
Y ۰
Y
X
g ۳
Y
X
Y
X
Y
X
Y
X
Λ ۲
g ۲
Γ۲
Λ ۲ ⊕ (X ⊕ Y) ⊕ Γ ۱
Γ ۲ ⊕ Γ ۱

۵.۳ میدان باقی‌مانده‌ها

در فصل دوم، مفاهیم میدان سودو بستهٔ جبری در ۴.۲.۲ و بستار جدایی‌پذیر در ۲.۲.۲ توضیح داده شده است. فرض کنید k یک میدان سودو بستهٔ جبری باشد به طوری که بستهٔ جدایی‌پذیر نیست یعنی بستار جدایی‌پذیر آن با خودش برابر نباشد ($k^{sep} \neq k$)، آنگاه با توجه به [۹، لم۳.۵و قضیه۳.۶] هر ارزیابی هنسلی با میدان باقی‌ماندهٔ k، در زبان حلقه‌ها بدون پارامتر تعریف‌پذیر است. همچنین فرض کنید k یک میدان سودو بستهٔ جبری با مشخصهٔ صفر باشد که، بخش جبری $k_\circ$ در k بستهٔ جبری نیست یعنی $k_\circ = \mathbb{Q}^{alg} \cap k \subsetneq \mathbb{Q}^{alg}$. (توجه کنید که هر میدانی شامل $\mathbb{Q}$ است و در واقع می‌خواهیم k شامل بستار جبری $\mathbb{Q}$ نباشد به بیان دیگر k شامل $\mathbb{Q}^{alg}$ نباشد). با توجه به [۵، قضیهٔ ۳.۵] و اثبات آن، که در ادامه به آن اشاره می‌کنیم، هر میدان ارزیابی هنسلی با میدان باقی‌ماندهٔ k، با فرمول‌های به صورت $\exists$ بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است.

قضیه ۸۸. [۵، قضیهٔ ۳.۵] فرض کنید K یک میدان ارزیابی هنسلی با حلقهٔ ارزیاب O_v و میدان باقی‌ماندهٔ k است. اگر F یک میدان سودو بستهٔ جبری باشد به طوری که بستهٔ جبری نیست، آنگاه حلقهٔ ارزیاب O_v در میدان K با فرمول‌های به صورت $\exists$ در زبان حلقه‌ها بدون پارامتر تعریف‌پذیر است.

در واقع بنا به [۵، بخش۳] برای هر چندجمله‌ای تکین و تحویل‌ناپذیر $f \in k_\circ[X]$، به طوری که $deg(f) > ۱$، یک $\mathcal{L}_{ring}$− فرمول، وابسته به چندجمله‌ای f ارائه می‌دهد که حلقهٔ ارزیاب O_v را در هر میدان ارزیابی هنسلی (K, v) با میدان باقی‌ماندهٔ k بدون پارامتر تعریف می‌کند.
همان طور که گفته شد، علاوه بر اثبات قضیهٔ ۸۳، ما به بررسی مثال مشخصِ $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})((\Gamma_۱))((\Gamma_۲))$ می‌پردازیم. فرض کنید $\mathbb{Q}^{tot\mathbb{R}}$، توسیع ماکسیمال میدان اعداد کاملاً حقیقی در $\mathbb{Q}$ باشد. در واقع $\mathbb{Q}^{tot\mathbb{R}}$ یک توسیع از $\mathbb{Q}$ است که وقتی این توسیع را در اعداد مختلط بنشانیم از اعداد حقیقی فراتر نمی‌رود. فصل دوم در بخش ۵.۲.۲ توضیح بیشتری داده شده است. بنا به [۱۰، مثال ۵.۱۰.۷] $k = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})$ یک میدان بستهٔ جبری سودو است. چون $\sqrt[۳]{۲}$ عدد حقیقی کامل نیست و $f = X^۳ - ۲$ یک چندجمله‌ای تکین و تحویل‌ناپذیر است با ضرایبی در بخش جبری $k_\circ$ در k است بنابراین، بنا به [۵، قضیهٔ ۳.۵] که در قضیهٔ ۸۸ صورت آن آورده شده است، فرمول زیر میدان ارزیاب O_v را در هر میدان ارزیابی هنسلی (K, v) با میدان باقی ماندهٔ k بدون پارامتر در زبان حلقه‌ها تعریف می‌کند.

$$\eta(x) \equiv (\exists u, t)(x = u + t \wedge (\exists y, z, y_۱ z_۱)(u = y_۱ - z_۱ \wedge y_۱(y^۳ - ۲) = ۱ \wedge z_۱(z^۳ - ۲) = ۱$$

$$\wedge(\exists y, z, y_۱, z_۱)(t = \circ \vee (t = y_۱ z_۱ \wedge y_۱(y^۳ - ۲) = ۱) \wedge z_۱(z^۳ - ۲) = ۱)))$$

۶.۳ میدان سری‌های هان مورد نظر پایان‌نامه

میدان $K := k((\Gamma_1))((\Gamma_2)) = k((\Gamma_2 \oplus \Gamma_1))$ که k یک میدان سودو بستهٔ جبری است و بستهٔ جدایی‌پذیر نیست ($k^{sep} \neq k$) را در نظر بگیرید، آنگاه با توجه به بخش ۵.۳ حلقهٔ ارزیاب O_v در میدان ارزیابی هنسلی (K, v)، با گروه ارزیاب $\Gamma_2 \oplus \Gamma_1$ و میدان باقی ماندهٔ k، بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است.
علاوه بر آن در مثال مشخصِ مورد نظر پایان‌نامه $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-1})((\Gamma_1))((\Gamma_2))$، در بخش قبل گفتیم حلقهٔ ارزیاب O_v در میدان ارزیابی هنسلی $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-1})((\Gamma_1))((\Gamma_2))$ با گروه ارزیاب $\Gamma_2 \oplus \Gamma_1$ و میدان باقی‌ماندهٔ $k = \mathbb{Q}^{tot\mathbb{R}}$ توسط فرمول $\eta(x)$، بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است.

۷.۳ اثبات قضیهٔ مورد نظر پایان‌نامه

گفتیم هدف این پایان‌نامه پاسخ دادن به این سوال است که آیا یک فرمولِ $\forall\exists$ و یا یک فرمولِ $\exists\forall$ در زبان حلقه‌ها وجود دارد که حلقهٔ ارزیابِ یک میدان ارزیابیِ هنسلی را بدون پارامتر تعریف کند؟ این سوال توسط پِرستِل در مقالهٔ [۱۲] مطرح شده است. در پاسخ به این سوال یک میدان ارزیابی هنسلی به صورت $K = k((\Gamma_1))((\Gamma_2))$ معرفی می‌کنیم که حلقهٔ ارزیاب آن با هیچ فرمول $\forall\exists$ و یا $\exists\forall$ بدون پارامتر در زبان حلقه‌ها تعریف نمی‌شود. در واقع هدف ما اثبات قضیهٔ زیر است:

قضیه ۸۹. گروه‌های آبلی مرتب Γ_1 و Γ_2 وجود دارند به طوری که برای هر میدان سودو بستهٔ جبری k که با بستار جدایی‌پذیرش برابر نیست ($k \neq k^{sep}$)، حلقه ارزیابِ $O_w = k((\Gamma_1))[[\Gamma_2]]$ در میدان ارزیابی هنسلی $K = k((\Gamma_1))((\Gamma_2))$، بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است، اما O_w با فرمول‌های به صورت $\exists\forall$ و $\forall\exists$ بدون پارامتر تعریف‌پذیر نیست.

فرض کنید w یک نگاشت ارزیابی (تحدید شدهٔ نگاشت ارزیابی v) با گروه ارزیاب Γ_2 و میدان باقی‌ماندهٔ $k((\Gamma_1))$ است. بنا به لم (۸۵) زیر گروه محدبِ Γ_1 در گروه آبلی مرتبِ $\Gamma_2 \oplus \Gamma_1$، در زبان گروه‌های آبلی مرتب، بدون پارامتر تعریف‌پذیر است. در نتیجه نگاشت ارزیابیِ w روی میدان ارزیابی K، بدون پارامتر تعریف‌پذیر است.
اکنون دو نشاندن بستهٔ وجودی از میدان ارزیابی هنسلی K به خودش ارائه می‌دهیم که با استفاده از محکی از پرستل برای تعریف‌پذیری حلقه‌های ارزیاب که در قضیهٔ (۸۳) در بخش ۲.۳ به طور مفصل آورده شده است، نشان می‌دهیم w نه با فرمول‌های به صورت $\forall\exists$ و نه به صورت $\exists\forall$ بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر نیست. بنا به قضیهٔ اکس–کوچن و ارشف که در ادامه صورت دقیق آن آورده شده است، اگر بخواهیم یک میدان ارزیابی هنسلی را در توسیعی از آن به صورت بسته وجودی بنشانیم، کافی است گروه ارزیاب و میدان باقی‌ماندهٔ آن را در گروه ارزیاب و میدان باقی‌ماندهٔ توسیع آن به صورت بسته وجودی بنشانیم. خواننده می‌تواند برای مطالعه اثبات قضیهٔ اکس–کوچن و ارشف به [۱۱، صفحهٔ۱۸۳] مراجعه کند.

قضیه ۹۰ (اکس–کوچن و ارشف). فرض کنید (K, w, Γ_w, k_w) یک میدان ارزیابی هنسلی با گروه ارزیاب Γ و میدان باقی‌ماندهٔ k_w است که مشخصهٔ صفر باشد. همچنین فرض کنید (L, u, Γ_u, k_u) یک توسیع از میدان (K, w, Γ, k_w) باشد. اگر گروه ارزیابِ Γ_w و میدان باقی‌ماندهٔ k_w به ترتیب در گروه ارزیابِ Γ_u و میدان باقی‌ماندهٔ k_u به ترتیب در زبان گروه‌های مرتب و زبان حلقه‌ها، بستهٔ وجودی باشد، آنگاه میدان ارزیابی هنسلی (K, w, Γ_w, k_w) بستهٔ وجودی در (L, u, Γ_u, k_u) است.

جهت اثبات قضیهٔ ۸۹، میدان ارزیابی هنسلی $K := k((\Gamma_۱))((\Gamma_۲))$ را در نظر می‌گیریم به طوری که $\Gamma_۱$ و $\Gamma_۲$ همان طور که در بخش ۳.۳ به طور مفصل گفته شد، به صورت زیر هستند:

$$\Gamma_۱ := \bigoplus_{\mathbb{N}}((\bigoplus_{\mathbb{N}} Y) \oplus X)$$

$$\Gamma_۲ := \bigoplus_{\mathbb{N}'}(X \oplus Y)$$

نگاشت ارزیابی هنسلی w را روی میدان ارزیابی هنسلی K، نگاشت ارزیابی تعریف شده روی سری‌های هان، که در فصل دوم در بخش ۸.۲ به آن پرداختیم، در نظر بگیرید. بنابراین حلقه ارزیاب آن $k((\Gamma_۱))[[\Gamma_۲]]$ و گروه ارزیاب $\Gamma_۲$ است. در واقع (K, w) یک میدان ارزیابی هنسلی است که w را نگاشت ارزیابی تعریف شده بر روی سری‌های هان در نظر می‌گیریم. اکنون بنا به قضیهٔ اکس–کوچن و ارشف برای آنکه میدان ارزیابی هنسلی (K, w, Γ_w, k_w) را در خودش به صورت بستهٔ وجودی بنشانیم، کافی است گروه ارزیاب Γ_w و میدان باقی‌ماندهٔ k_w را به صورت بستهٔ وجودی در خودشان بنشانیم.

۱. جهت آنکه میدان باقی‌ماندهٔ k_w را به صورت بستهٔ وجودی در خودش بنشانیم، می‌توانیم نگاشت همانیِ $f_۰ = id_k$ که یک نشاندن بسته وجودی است را در نظر بگیریم. همچنین در بخش ۴.۳ نشاندنِ ۳–۱ ارائه داده شد که گروه ارزیاب Γ را در خودش به صورت بستهٔ وجودی می‌نشاند. در نتیجه بنا به قضیهٔ اکس–کوچن و ارشف یک نشاندن بستهٔ وجودی مانند $f : K \longrightarrow K$ وجود دارد یعنی $K \prec_{\exists} K$. اکنون بنا به محکی که پرستل برای تعریف‌پذیری حلقه‌های ارزیاب در میدان‌های ارزیابی هنسلی در منبع [۱۲] ارائه داد، اگر بخواهیم حلقهٔ ارزیاب O_w در میدان ارزیابی هنسلی (K, w) با فرمول‌های به صورت $\forall\exists$ بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر باشد، باید از اینکه $K \prec_{\exists} K$ نتیجه شود $O_w \subseteq O_w$. اما در میدان ارزیابی هنسلی مورد نظر ما $K = k((\Gamma_۱))((\Gamma_۲))$ که حلقهٔ ارزیاب آن $O_w = k((\Gamma_۱))[[\Gamma_۲]]$ است داریم $O_w \subsetneq O_w$ زیرا با توجه به نشاندن ۳–۱ چیزی بیشتر از $\Gamma_۲$ به $\Gamma_۲$ تصویر می‌شود بنابراین $f(O_w) \supsetneq O_w$. ۲. جهت آنکه میدان باقی‌ماندهٔ k_w را به صورت بستهٔ وجودی در خودش بنشانیم، می‌توانیم نگاشت همانیِ $g_۰ = id_k$ که یک نشاندن بسته وجودی است را در نظر بگیریم. همچنین در بخش ۴.۳ نشاندنِ ۳–۲ ارائه داده شد که گروه ارزیاب Γ را در خودش به صورت بستهٔ وجودی می‌نشاند. در نتیجه بنا به قضیهٔ اکس–کوچن و ارشاف یک نشاندن بستهٔ وجودی مانند $g : K \longrightarrow K$ وجود دارد یعنی $K \prec_{\exists} K$. اکنون بنا به محکی که پرستل برای تعریف‌پذیری حلقه‌های ارزیاب در میدان‌های ارزیابی هنسلی در منبع [۱۲] ارائه داد، که به طور مفصل در بخش ۲.۳ به آن پرداخته شده است، اگر بخواهیم حلقهٔ ارزیاب O_w در میدان ارزیابی هنسلی (K, w) با فرمول‌های به صورت $\forall\exists$ بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر باشد، باید از اینکه $K \prec_{\exists} K$ نتیجه شود $O_w \subseteq O_w$. اما در میدان ارزیابی هنسلی مورد نظر ما $K = k((\Gamma_۱))((\Gamma_۲))$

که حلقهٔ ارزیاب آن $k((\Gamma_{۱}))[[\Gamma_{۲}]]$ است داریم $O_w = k((\Gamma_{۱}))[[\Gamma_{۲}]]$ زیرا با توجه به نشاندن ۳-۲ چیزی بیشتر از $\Gamma_{۱}$ به $\Gamma_{۱}$ تصویر می‌شود بنابراین $f(O_w) \subsetneq O_w$ و $g(O_w) \subsetneq O_w$.

اگر میدان ارزیابی هنسلی $K = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})((\mathit{\Gamma}_{۱}))((\mathit{\Gamma}_{۲}))$ را در نظر بگیریم، آنگاه بنا به آنچه در بخش ۶.۳ گفتیم، حلقهٔ ارزیاب $O_w = \mathbb{Q}^{tot\mathbb{R}}(\sqrt{-۱})((\mathit{\Gamma}_{۱}))[[\mathit{\Gamma}_{۲}]]$ در میدان ارزیابی هنسلی (K, w) با گروه ارزیاب $\Gamma_{۲}$ بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است، اما O_w با هیچ فرمول به صورت $\exists\forall$ و $\forall\exists$ در زبان حلقه‌ها تعریف‌پذیر نیست زیرا از ۱ و ۲ نتیجه گرفتیم اگر $K \prec_{\exists} K$ آنگاه $f(O_w) \subsetneq O_w$ و $O_w \cap K \subsetneq O_w$. در نتیجه بنا به قضیهٔ ۸۳ حلقهٔ ارزیاب $O_w = k((\Gamma_{۱}))[[\Gamma_{۲}]]$ در میدان ارزیابی هنسلی $K = k((\Gamma_{۱}))((\Gamma_{۲}))$ بدون پارامتر تعریف‌پذیر است اما با هیچ فرمول به صورت $\exists\forall$ و $\forall\exists$ در زبان حلقه‌ها تعریف‌پذیر نیست. بنابراین قضیهٔ مورد نظر پایان‌نامه که در ادامه دوباره آن را آوردیم، اثبات شد.

> گروه‌های آبلی مرتب $\mathit{\Gamma}_{۱}$ و $\mathit{\Gamma}_{۲}$ وجود دارند به طوری که برای هر میدان سودو بستهٔ جبری k که با بستار جدایی‌پذیرش برابر نیست ($k \neq k^{sep}$)، حلقه ارزیابِ $O_w = k((\mathit{\Gamma}_{۱}))[[\mathit{\Gamma}_{۲}]]$ در میدان ارزیابی هنسلی $K = k((\mathit{\Gamma}_{۱}))((\mathit{\Gamma}_{۲}))$، بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است، اما O_w با فرمول‌های به صورت $\exists\forall$ و $\forall\exists$ بدون پارامتر تعریف‌پذیر نیست.

منابع

[1] Halupczok, I and Jahnke, F.: *A definable Henselian valuation with high quantifier complexity.* Mathematical Logic Quarterly Bull. 61 (4-5). pp. 362-366. ISSN 0942-5616 (2015).

[2] Anscombe, W and Koenigsmann, J.: ”An existential $\varnothing$-definition of Fq[[t]] in Fq((t)).” J. Symb. Log. 79(4), 1336-1343 (2014).

[3] Cluckers, R, Derakhshan, J, Leenknegt, E, and Macintyre, A.: ”Uniformly defining valuation rings in Henselian valued fields with finite or pseudo-finite residue fields.” Ann. Pure Appl. Log. 164(12), 1236-1246 (2013).

[4] Cluckers, R and Halupczok, I.: ”Quantifier elimination in ordered abelian groups.” Confluentes Math. 3(4),587-615 (2011).

[5] Fehm,A.: ”Existential ϕ-definability of Henselian valuation rings.” J. Symb. Log. 80(1), 301–307, (2015).

[6] Fehm, A and Jahnke, F.: ” On the quantifier complexity of definable canonical henselian valuations.” Math. Log. Q.61(4-5), 347-361 (2015).

[7] Fehm.A and Prestel. A.: ” Uniform definability of henselian valuation rings in the Macintyre language.” to appear in Bull. Lond. Math. Soc.

[8] Hong, J.: ” Definable non-divisible Henselian valuations.” Bull. Lond. Math. Soc. 46(1), 14–18 (2014).

[9] Jahnke, F and Koenigsmann, J.: ” Definable Henselian valuations.” J. Symb. Log. 80(1), 85–99 (2015).

[10] Jarden, M.: ” Algebraic Patching.” Springer Monographs in Mathematics (Springer-Verlag, 2011).

[11] Kuhlmann, F.-V and Prestel, A.: " On places of algebraic function fields." J. Reine Angew. Math. 353, 181-195 (1984).

[12] Prestel, A.: " Definable Henselian valuation rings." to appear in J. Symb. Log.

[13] Schmit, P.H.: " Model theory of ordered abelian groups." Habilitationsschrift (Universität Heidelberg, 1982)

[14] Weispfenning, V.: " Exitential equivalence of ordered abelian groups with parameters." Arch. Math. Log. 29(4), 237-248 (1990).

واژه‌نامه‌ی فارسی به انگلیسی

الف

ارزیابی .... valuation
ایده‌آل ماکسیمال .... maximal ideal
اعداد کاملاً حقیقی .... totally real numbers

ب

به طور جبری .... algebraically
بدیهی .... trivial
بستار جبری .... algebraic closure
بخش‌پذیر .... divisible

پ

pـ ادیک .... p-adic

ت

ترتیب قاموسی .... lexicographical order
توسیع میدان .... field extension
توسیع منظم .... regular extension
توسیع جبری .... algebraic extension
توسیع جدایی‌پذیر .... separable extension
تعبیرپذیر .... interpretable

ث

ج

چ

ح

ز

س

ف

ق

ک

گ

گروه ارزیابی .... valued group
گروه بدون تاب .... torsion free group

م

مجزای خطی .... linearly disjoint
مجزای جبری .... algebraicalyy disjoint
میدان ارزیابی .... valued field
میدان باقی‌مانده‌ها .... residue field
مجموعهٔ تعریف‌پذیر .... definable set
منتظم .... regular
مطلقاً تحویل‌ناپذیر .... absolutely irreducible
میدان هان .... Hahn field
میدان جدایی‌پذیر .... separable field
محمول تک‌موضعی .... unary predicate
مرتب خطی .... linearly ordered
معادل .... equivalent
مقدماتی .... elementary
ن نشاندن .... embedding
نشاندن بستهٔ وجودی .... existentially closed embedding
نرم .... norm
و ه هنسلی .... henselian

ی یکتا .... unique

فهرست نمادها

A definable Henselian valuation with high quantifier complexity

NAJME ZAMANI
zamaninajme@math.iut.ac.ir
September 21 , 2022
Master of Science Thesis (in Farsi)
Department of Mathematical Sciences
Isfahan University of Technology, Isfahan 84156-8311, Iran

Supervisor: Dr. Mohsen Khani, `mohsen.khani@iut.ac.ir`
2000 MSC: 03C40 (13F30)
Keywords: Henselian valuation field, valuation ring, Ax-Kochen and Eršov theorem, definability .

Abstract:
The aim of this thesis is to answer the question of whether there is a parameter-free $\exists\forall$- formula or a parameter-free $\forall\exists$- formula that defines the valuation ring of a Henselian valued field in the language of rings. This question has been raised by Prestel in [12] The aim of this note is to provide a counterexample to Prestel's question. More precisely, we show the theorem below:
There are ordered abelian groups Γ_1 and Γ_2 such that for any PAC field k with $k \neq k^{sep}$ the Henselian valuation ring $O_w = k((\mathit{\Gamma}_1))[[\mathit{\Gamma}_2]]$ is $\varnothing$ -definable in the field $K = k((\mathit{\Gamma}_1))((\mathit{\Gamma}_2))$. However, O_w is neither definable by a $\varnothing - \forall\exists$ -formula nor by a $\varnothing - \exists\forall$ -formula in K.
In answering this question, the Henselian valued field $K = k((\mathit{\Gamma}_1))((\mathit{\Gamma}_2))$ is introduced where its valuation ring is not defined by any $\exists\forall$- formula or $\forall\exists$- formula without parameters in the language of rings. By $k((\Gamma_1))$ we mean the field of Hann series with the valued group Γ_1. The main ideas that we rely on are the Characterization Theorem for definability given by Prestel in [12] and also the Ax-Kochen and Eršov theorem. These two ideas are given in detail in the thesis. Let Σ be a first order axiom system in the ring language $\mathcal{L}_{ring}$ together with a unary predicate O and let $(K_1, O_1) \models \Sigma$ and $(K_2, O_2) \models \Sigma$. Due to the Characterization Theorem the valuation ring of a Henselian valued field defines with an $\exists\forall$- formula if and only if

$$K_1 \prec_{\exists} K_2 \Rightarrow O_1 \subseteq O_2.$$

In other words if we get from $K_1 \prec_{\exists} K_2$ the conclusion $O_1 \subseteq O_2$ then O can be defined with an $\exists\forall$- formula in the language of rings. So for that the valuation ring of a Henselian valued field is not defined with an $\exists\forall$- formula we give an embedding $f : K \longrightarrow K$ such that $f(O) \nsubseteq O$. To give this embedding we use the Ax-Kochen and Eršov theorem.
Let (K, w, Γ_w, k_w) be a Henselian valued field with value group Γ_w and residue field k_w. Let $(K, w, \Gamma, k_w) \subseteq (L, u, \Gamma_u, k_u)$ be an extension of valued fields. If the value group Γ_w and residue field k_w respectively are existentially closed in the value group Γ_u and residue field k_u in the language of ordered group and in the langage of rings ، then heselian valuation field is (K, w, Γ_w, k_w) existentially closed in (L, u, Γ_u, k_u).
In this thesis we consider two embedding for value group and identity embedding for reside field.

Isfahan University of Technology
Department of Mathematical Sciences

A definable Henselian valuation with high quantifier complexity

A Thesis
Submitted in Partial Fulfillment of the Requirements
for the Master of Science

By
Najme Zamani

Evaluated and approved by the thesis committee, on 21/9/2022

1- Dr. Mohsen Khani, Assistant Professor (Supervisor)

2- Dr. Alireza Mofidi, Associate Professor (Examiner)

3- Dr. Majid Salamat, Assistant Professor (Examiner)

Dr. Azam Etemad, Professor (Department graduate coordinator)

Isfahan University of Technology
Department of Mathematical Sciences

Thesis Submitted for the Award of Master of Science in Mathematics

A definable Henselian valuation with high quantifier complexity

Najme Zamani

Supervisor: Dr. Mohsen Khani

September 2022