حذف سور در میدانهای ارزیابی بستهٔ جبری

تدریس: محسن خانی، محمود بهبودی
(گردآوری: فاطمه اکبری)

۹ بهمن ۱۴۰۰

چکیده

عنوان این درس «پدیدهٔ حذف سور در میدانهای ارزیابی بستهٔ جبری» است و این درس توسط من، محسن خانی، و آقای دکتر بهبودی به طور همزمان ارائه می‌شود. هدف از این ارائه، تقویت همکاری بین رشته‌ای در دانشکدهٔ ریاضی، و سوق دادن دانشجویان تکمیلی به سمت موضوعات نسبتاً جدیدتر در زمینهٔ جبر و نظریهٔ مدل میدانهای ارزیابی است.

برنامهٔ تقریبی کار به صورت زیر خواهد بود:

- ۵ الی ۶ جلسه اول، مقدمات برای آشنائی با نظریهٔ مدلها (توسط من)
- ۴ الی پنج جلسهٔ دوم، مقدمات نظریهٔ گالوا و میدانهای بستهٔ جبری (توسط دکتر بهبودی)
- ۲ جلسه معرفی پدیدهٔ حذف سور (توسط من)
- بقیهٔ جلسات، پرداختن به موضوع اصلی درس، یعنی معرفی حلقه‌های هنسلی، میدانهای ارزیابی و بررسی حذف سور در آنها (توسط من و دکتر بهبودی)

منبع اصلی درس، یادداشتهای مدرسان در هنگام تدریس و جزوهٔ در حال تایپ توسط خانم اکبری است، ولی برخی منابع مفید جانبی به صورت زیر هستند (لینکها قابل کلیک هستند)

برای نظریهٔ مدل میدانهای ارزیابی:

- منبع اصلی درس: یادداشتهای ون دن دریز در مورد میدانهای ارزیابی، فصلِ Lectures on the Model Theory of Valued Fields
  https://www.springer.com/gp/book/9783642549359
- یادداشتهای دیوید مارکر دربارهٔ نظریهٔ مدل میدانهای ارزیابی
  http://homepages.math.uic.edu/~marker/valued_fields.pdf

برای میدانهای ارزیابی:

- میدانهای ارزیابی نوشتهٔ انگلر و پرستل
  https://www.springer.com/gp/book/9783540242215

برای نظریهٔ مدل:

- نظریهٔ مدل، مارکر
  https://www.springer.com/gp/book/9780387987606
- نظریهٔ مدل، تنت و زیگلر
  https://www.cambridge.org/core/books/course-in-model-theory/7A4C7BCF0F243AE31C0923A021A06066
- نظریهٔ مدل جبری، خانی
  https://khani.iut.ac.ir/sites/khani.iut.ac.ir/files//file_basepage/modeltheory.pdf
- نظریهٔ مدل، خانی تدریس ترم قبل
  https://www.aparat.com/v/NOfEn?playlist=601936&%D9%86%D8%B8%D8%B1%DB%8C%D9%87%E2%80%8C%D9%94%E2%80%8C_%D9%85%D8%AF%D9%84%D9%87%D8%A7

برای جبر و نظریهٔ گالوا:

- نظریهٔ گالوا، موراندی
https://www.springer.com/gp/book/9780387947532
- جبر، سرج لنگ
https://www.springer.com/gp/book/9780387953854
- فیلمهای تدریس نظریهٔ گالوا توسط محسن خانی
https://www.aparat.com/playlist/305753/%D9%86%D8%B8%D8%B1%DB%8C%D9%87%26zwnj%3B%DB%8C_%DA%AF%D8%A7%D9%84%D9%88%D8%A7

قدردانی. تایپ جزوه برای درسهای اینچنین موجب ماندگاری آنها و قابل دسترس شدنشان برای همگان است. از خانم «فاطمه اکبری» بابت تقبل زحمت تایپ این جزوه کمال سپاسگزاری را داریم.

مقدمه

تدریس ریاضی گاهی برای پُر کردن خالیگاه‌های ذهنی ریاضیدان است. چیزهائی هست که تنها شانس عمیق شدن در آنها تدریسشان است، و تدریس مطالب این یادداشت برای من چنین وضعی داشت. سالها بود که دربارهٔ میدانهای ارزیابی مطالعات داشتم و نکته‌های فراوان دیده بودم و پی این می‌گشتم که این دانسته‌ها را به کسی منتقل کنم. برای رسیدن به این هدف، چه چیزی بهتر از «مباحث ویژه». در طی سالهای گذشته، چندین بار درس مباحث ویژه تدریس کرده‌ام؛ هر بار برای خودم ابهام‌هایی برطرف شده است و دانشجویان با مطالبی جدید، عمیق و غیرکلیشه‌ای در حوزه‌های گوناگون آشنا شده‌اند. بابت این امکان خداوند را شاکرم.

در نیمسال اول ۱۴۰۰ این فرصت فراهم شد تا با همکار گرامیم، آقای دکتر بهبودی این درس را به صورت مشترک ارائه کنیم، خانم فاطمه اکبری نیز تایپ جزوهٔ آن را به طور داوطلبانه عهده‌دار شدند، و آقای حمزه محمدی در انتخاب و حل تمرینها همکاری کردند. حاصل این همکاری، جزوهٔ پیش رو است.

درس را با نظریهٔ مدل مقدماتی و معرفی قضیهٔ فشردگی آغازیده‌ایم. مفهوم حذف سور را برای تئوری ها تعریف کرده‌ایم و پس از مقدماتی از نظریهٔ گالوا، حذف سور میدانهای بستهٔ جبری را اثبات کرده‌ایم و از مواهب جبری آن گفته‌ایم. سپس وارد حلقه‌های موضعی شده‌ایم و دوباره پس از بسط جبر کافی، از نظریهٔ مدلها برای اثبات قضیهٔ گرین‌لیف و اکس‌کوچن دربارهٔ پی‌ادیکها استفاده کرده‌ایم. آنگاه میدانهای ارزیابی و ارتباط آنها با حلقه‌های موضعی را گفته‌ایم و با اثبات حذف سور برای میدانهای ارزیابی بستهٔ جبری درس را به اتمام رسانده‌ایم.

از دانشجویان گرامی دانشگاه صنعتی اصفهان که در طی تدریس این یادداشت همراه بوده‌اند سپاسگزارم و برایشان آرزوی توفیق دارم.

کلاسهای ضبط شده این کلاس در لینک زیر موجودند. توجه کنید که تنها بخشی که توسط من، محسن خانی، تدریس شده است در لینک زیر قرار داده شده است:

https://www.aparat.com/v/kcfgo?playlist=1448806

محسن خانی

زمستان ۱۴۰۰

فهرست مطالب

فصل ۱

مقدمات نظریهٔ مدلی

تدریس: محسن خانی
گردآوری: فاطمهٔ اکبری

۱.۱ زبان، ترم، فرمول

تعریف ۱. یک مجموعه‌ی L متشکل از سه دسته نماد تابعی، نماد رابطه‌ای و نماد ثابت را یک زبان مرتبه اول[۱] می‌نامیم. متناظر با هر نماد تابعی $f \in L$ یک عدد طبیعی n_f در نظر گرفته می‌شود که آن را تعداد مواضع تابع f می‌نامیم. به طور مشابه، برای هر نماد رابطه‌ای $R \in L$ یک عدد طبیعی n_R در نظر گرفته می‌شود که آن را تعداد مواضع رابطه R می‌نامیم.

به عنوان یک مثال کلی می‌توانیم به زبان $L = \{f, g, c, R\}$ اشاره کنیم که در آن f یک نماد تابعی دو موضعی، g یک نماد تابعی تک موضعی، c نماد ثابت و R یک نماد رابطه‌ای سه موضعی است.

مثال ۱. در این مثال سعی داریم نمونه‌های آشناتر از یک زبان مرتبه اول را معرفی کنیم.

۱) زبان تهی: ابتدایی‌ترین مثال، زبان $L = \emptyset$ است که شامل هیچ نمادی برای تابع، ثابت و رابطه نیست.

۲) زبان گروه‌های جمعی: $L_{group۱} = \{+, -, ۰\}$. در این زبان $+$ نماد تابعی دو موضعی، $-$ نماد تابعی تک موضعی و ۰ نماد ثابت است.

۳) زبان گروه‌های ضربی: $L_{group۲} = \{\cdot, ^{-۱}, ۱\}$. در این زبان $\cdot$ نماد تابعی دو موضعی، $^{-۱}$ نماد تابعی تک موضعی و ۱ نماد ثابت است.

۴) زبان حلقه‌ها: $L_{ring} = \{+, -, \cdot, ۰, ۱\}$. این زبان در واقع از افزودن نماد ثابت ۱ و نماد تابعی دو موضعی $\cdot$ به زبان گروه‌های جمعی به دست می‌آید.

۵) زبان مجموعه‌های مرتب: $L_{order} = \{\leq\}$. در این زبان $\leq$ یک نماد رابطه‌ای دو موضعی است.

۶) زبان حلقه‌های مرتب: $L_{or} = L_{ring} \cup L_{order}$.

همواره در کنار یک زبان مرتبه اول، یک مجموعه از متغیرها مانند $Var = \{v_۱, v_۲, v_۳, \ldots\}$ را در نظر می‌گیریم. در ادامه خواهیم دید که در یک زبان مرتبهٔ اول چگونه می‌توان کلمه‌سازی کرد.

تعریف ۲. فرض کنیم L یک زبان مرتبه اول و Var مجموعه‌ی متغیرها L-ترم‌ها را به صورت استقرایی زیر تعریف می‌کنیم،

۱) هر متغیر $v_i \in Var$ و هر ثابت $c \in L$ یک L-ترم است.

[۱] first-order language

۲) اگر $f \in L$ یک نماد تابعی n موضعی باشد آنگاه $ft_1t_2\cdots t_n$ یک L-ترم است.

مثال ۲. اگر $L=\{+\}$ زبان مرتبه اول و $Var=\{v_0,\ldots,v_n\}$ مجموعه متغیرها باشد آنگاه $+v_0v_0$ یک ترم است. در ریاضیات روزمره این ترم را به صورت v_0+v_0 یا به اختصار به صورت $v_0$۲ نمایش می‌دهند. مشابهاً $+v_0+v_0v_0$ نیز یک ترم است که آن را در ریاضیات روزمره به صورت $(v_0+v_0)+v_0$ نشان دهندهٔ $v_0+(v_0+v_0)$ (و اگر موجب ابهام نشود با $v_0$۳) نشان می‌دهند. دقت کنید که $++v_0v_0v_0$ است. به طور کلی اگر هر متغیر v_i، $m_i\in\mathbb{N}$ بار تحت تابع $+$ قرار بگیرد، L-ترم‌ها به صورت $m_0v_0+\cdots+m_nv_n$ هستند. به طور مشابه اگر $L=\{\cdot\}$ و تاثیر α_i بار تابع را بر روی متغیر v_i به طور اختصار با $v_i^{\alpha_i}$ نمایش دهیم آنگاه ترم‌ها به صورت $v_0^{\alpha_0}\cdots v_n^{\alpha n}$ هستند.

تمرین ۱. در زبان‌های L_{or} و L_{group}۲ معرفی شده در مثال ۱ چند ترم بنویسید.

پس از معرفی زبان و چگونگی ساخت ترم‌ها، می‌توانیم به سراغ معرفی فرمول‌ها برویم. لازم به ذکر است که برای نوشتن L-فرمول‌ها علاوه بر امکانات زبان از متغیرها و نمادهای) ، (، $=$، $\wedge$، $\neg$ و $\exists$ استفاده می‌کنیم. معمولا به نمادهای خارج از زبان که در نوشتن فرمولهای منطقی استفاده می‌شوند، نمادهای منطقی گفته می‌شود.

تعریف ۳. در یک زبان مرتبهٔ اولِ L فرمول‌های اتمی را با دو قانون زیر ساخته می‌شوند.

۱) اگر t_1 و t_2 دو L-ترم باشد آنگاه $t_1=t_2$ یک فرمول اتمی است.

۲) اگر $t_1,t_2,\ldots,t_n$، ترم باشند و $R\in L$ یک نماد رابطه‌ای n موضعی باشد، آنگاه $Rt_1t_2\cdots t_n$ یک فرمول اتمی است.

مثال ۳. زبان مرتبه اول $L=\{+,\leq\}$ و متغیرهای v_0 و v_1 در نظر می‌گیریم. در این صورت موارد زیر فرمول اتمی هستند:

- $\leq v_0v_1$. این فرمول اتمی را برای راحتی می‌توان به صورت $v_0\leq v_1$ نوشت.
- $\leq +v_0v_1++v_2v_3v_0$. این فرمول اتمی را برای راحتی می‌توان به صورت $v_0+v_1\leq v_2+(v_3+v_0)$ نوشت.
- $+v_0v_1=+v_2+v_3v_4$.

به طور کلی عبارتهائی به صورت $m_0v_0+\ldots m_kv_k\leq n_0v_0+\ldots n_kv_k$ را می‌توان به صورت فرمول اتمی در زبان بالا نوشت. همچنین عبارتهائی به صورت $m_0v_0+\ldots+m_kv_k=n_0v_0+\ldots+n_kv_k$ نیز فرمول اتمی در این زبان هستند.

مثال ۴. اگر زبان را L_{ring} در نظر بگیریم و $Var=\{v_0,\ldots,v_n\}$ آنگاه ترم‌ها به صورت $m_0v_0^{\alpha_0}+\cdots+m_nv_n^{\alpha n}$ (چندجمله‌ای‌های $n+$۱ متغیره) هستند که اگر آن‌ها را به اختصار با $f(v_0,\ldots,v_n)$ نمایش دهیم می‌توانیم نتیجه بگیریم که فرمول‌های اتمی در این زبان به صورت $f(v_0,\ldots,v_n)=g(v_0,\ldots,v_n)$ هستند که در آن f,g چند جمله‌ای‌هائی با ضرایب در اعداد طبیعی هستند. به عنوان مثال عبارت $+.v_0v_0..v_1v_2.v_3v_3=0$ یک فرمول اتمی است که در ریاضیات رومزه به صورت $v_0^2+v_1v_2v_3^2=0$ نوشته می‌شود.

توجه داشته باشیم که گستره فرمول‌ها پهناورتر است و فرمول‌های اتمی تنها بخشی از آن هستند. در زیر به طور دقیق‌تر تعریف فرمول در یک زبان مرتبه اول را بیان می‌کنیم.

تعریف ۴. اگر L یک زبان مرتبه اول باشد آنگاه L- فرمول‌ها (ی مرتبهٔ اول) با قوانین استقرائی زیر ساخته می‌شوند.

۱) فرمول‌های اتمی L-فرمول هستند.

۲) اگر ψ یک L-فرمول باشد آنگاه $\neg\psi$ نیز یک L-فرمول است.

۳) اگر ψ_1 و ψ_2 دو L-فرمول باشند آنگاه $(\psi_1\wedge\psi_2)$ یک L-فرمول است.

۴) اگر ψ یک L-فرمول و v_0 یک متغیر باشد آنگاه $\exists v_0\ \ \psi$ یک L-فرمول است.

مثال ۵. زبان مرتبه اول L_{ring} و متغیرهای v_0, v_1, v_2 را در نظر می‌گیریم. همانطور که در مثال قبل مشاهده کردیم می‌توانیم ترم‌های این زبان را به اختصار با $f(v_0, v_1, v_2)$ (چندجمله‌ای‌های سه متغیره) نمایش دهیم. پس

$$\exists v_0 \ \exists v_1 \ \exists v_2 \quad f_1(v_0, v_1, v_2) = 0 \wedge \cdots \wedge f_k(v_0, v_1, v_2) = 0$$

(بیانگر جواب داشتن یک دستگاه معادلات چندجمله‌ای) یک فرمول است. به عنوان تمرین فرمول‌های دیگری را در این زبان بیابید.

تذکر ۱. فرض کنیم ψ یک L-فرمول باشد. در منطق مرتبه اول هیچ فرمولی به صورت $(\exists v_i \in U \quad \psi)$ و یا $(\exists v_i \subseteq U \quad \psi)$ وجود ندارد.

تذکر ۲. اگر ψ_1 و ψ_2 دو L-فرمول باشند آنگاه برای ساده سازی برخی فرمول‌ها می‌توانیم از نمادهای $\vee$، $\forall$، $\longrightarrow$ و $\longleftrightarrow$ به شکل زیر استفاده کنیم،

۱) $\psi_1 \vee \psi_2 := \neg(\neg\psi_1 \wedge \neg\psi_2)$.

۲) $\forall v \ \psi_1 := \neg(\exists v \ \neg\psi_1)$.

۳) $\psi_1 \longrightarrow \psi_2 := \neg\psi_1 \vee \psi_2$.

۴) $\psi_1 \longleftrightarrow \psi_2 := \psi_1 \longrightarrow \psi_2 \wedge \psi_2 \longrightarrow \psi_1$.

تذکر ۳. برای سادگی خوانش فرمول‌ها قوانین اولویت را به ترتیب

۱) پرانتز،

۲) $\neg$، $\exists$ و $\forall$،

۳) $\wedge$ و $\vee$،

۴) $\longrightarrow$ و $\longleftarrow$.

در نظر می‌گیریم. توجه داشته باشیم که هر نماد روی اولین عنصر بعد از خود اثر می‌کند و در نمادهای هم رده هرکدام اول باشد، اولویت دارد.

اولویت بندی‌های بالا اثر سورها بر روی متغیرها را در یک فرمول تحت تاثیر قرار می‌دهند. برای مثال اگر R و S دو نماد رابطه‌ای دو موضعی و $Var = \{x, y, z\}$ باشد آنگاه در فرمول $\exists x \ \ R(x, y) \wedge S(x, z)$ سور وجودی تنها به متغیر x در $R(x, y)$ اثر می‌کند. این در حالی است که اگر فرمول به صورت $\exists x \ \ (R(x, y) \wedge S(x, z))$ باشد سور وجودی بر متغیر x در هر دو رابطه اثر گذار است. در اینجاست که مفهومی به نام متغیر آزاد پدید می‌آید.

تعریف ۵. متغیر x را در فرمول ψ آزاد گوییم هرگاه تحت تاثیر هیچ سوری نباشد. در غیر این صورت آن را متغیر وابسته می‌نامیم.

۲.۱ ساختارهای مرتبهٔ اول

تعریف ۶. فرض کنیم L یک زبان مرتبه اول باشد. یک L-ساختار $\mathfrak{M}$ از موارد زیر تشکیل شده است،

۱) یک مجموعه ناتهی M که به آن جهان L-ساختار $\mathfrak{M}$ گوییم.

۲) متناظر با هر نماد تابعی n موضعی، $f \in L$، یک تابع $f^{\mathfrak{M}} : M^n \longrightarrow M$ وجود دارد که به آن تعبیر نماد تابعی f در $\mathfrak{M}$ می‌گوییم.

۳) متناظر با هر نماد ثابت $c \in L$ یک عنصر مشخص $c^{\mathfrak{M}} \in M$ وجود دارد که به آن تعبیر نماد ثابت c در $\mathfrak{M}$ می‌گوییم.

۴) به ازای هر نماد رابطه‌ای n موضعی، $R \in L$، یک مجموعه $R^{\mathfrak{M}} \subseteq M^n$ وجود دارد که به آن تعبیر نماد رابطه‌ای f در $\mathfrak{M}$ می‌گوییم.

هر L-ساختار $\mathfrak{M}$ را به صورت $\mathfrak{M} = (M, (f^{\mathfrak{M}}, R^{\mathfrak{M}}, c^{\mathfrak{M}})_{f,R,c \in L})$ نمایش می‌دهیم.

مثال ۶. اگر زبان را $L = \{*, e\}$ در نظر بگیریم که در آن $*$ نماد تابعی دو موضعی و e نماد ثابت باشد، $\mathfrak{R} = (\mathbb{R}, \times, ۱)$ یک L-ساختار است که در آن مجموعه اعداد حقیقی جهان، تعبیر نماد تابعی زبان ضرب معمول میان اعداد و تعبیر نماد ثابت e عدد یک است. به عبارت دیگر

$$*^{\mathfrak{R}} = \times, \qquad e^{\mathfrak{R}} = ۱.$$

به همین صورت $\mathfrak{Z} = (\mathbb{Z}, +, ۰)$ نیز یک L-ساختار است.

مثال ۷. فرض کنیم $L = \{f, g, R\}$، که در آن f نماد تابعی دو موضعی، g نماد تابعی تک موضعی و R نماد رابطه‌ای دو موضعی باشد در این صورت

- $\mathfrak{N} = (\mathbb{N}, +, s, <)$ یک L-ساختار است، چرا که $f^{\mathfrak{N}} = +$ (جمع معمول میان اعداد)، $g^{\mathfrak{N}} = s$ (تابع تالی با ضابطه $s(x) = x + ۱$) و $R^{\mathfrak{N}} = \{(x, y) \in \mathbb{N}^۲ \mid x < y\}$.
- $\mathfrak{R} = (\mathbb{R}, \times, exp, >)$ که در آن $f^{\mathfrak{R}} = \times$ (ضرب معمول میان اعداد)، $g^{\mathfrak{R}} = exp$ (تابع نمایی با ضابطه $exp(x) = e^x$) و $R^{\mathfrak{R}} = \{(x, y) \in \mathbb{R}^۲ \mid x > y\}$ یک L-ساختار است.

مثال ۸. برای زبان $L = \{R\}$ (R نماد رابطه‌ای دو موضعی)، $\mathfrak{M} = (\{a, b, c\}, \{(a, b), (a, c)\})$ یک L-ساختار است. در واقع این ساختار را می‌توان گرافی با سه راس $\{a, b, c\}$ در نظر گرفت که تعبیر نماد رابطه‌ای در آن وجود داشتن یال میان راس‌های a, b و a, c است.

تعریف ۷. فرض کنیم L یک زبان مرتبه اول و $\mathfrak{M}$ و $\mathfrak{N}$ دو L-ساختار باشند. یک L-نشاندن[۲] عبارت است از یک تابع یک به یک $\eta : M \longrightarrow N$ که تعابیر نمادهای زبان را حفظ می‌کند. یعنی

۱) برای هر نماد ثابت $c \in L$ داریم $\eta(c^{\mathfrak{m}}) = c^{\mathfrak{N}}$.

۲) برای هر نماد تابعی n موضعی $f \in L$ و هر n-تایی $(a_۱, \ldots, a_n) \in M^n$ داریم

$$\eta(f^{\mathfrak{M}}(a_۱, \ldots, a_n)) = f^{\mathfrak{N}}(\eta(a_۱), \ldots, \eta(a_n)).$$

۳) برای هر نماد رابطه‌ای n موضعی $R \in L$ و هر n-تایی $(a_۱, \ldots, a_n) \in M^n$ داریم

$$(a_۱, \ldots, a_n) \in R^{\mathfrak{M}} \Leftrightarrow (\eta(a_۱), \ldots, \eta(a_n)) \in R^{\mathfrak{N}}.$$

در این صورت می‌نویسیم $\eta : \mathfrak{M} \to \mathfrak{N}$. همچنین L-نشاندن η را یک ایزومرفیسم می‌نامیم هرگاه پوشا نیز باشد.

مثال ۹. فرض کنیم $L = \{f, c\}$ یک زبان مرتبه اول باشد که در آن f یک نماد تابعی دو موضعی و c نماد ثابت است. یک L-نشاندن میان دو L-ساختار $\mathfrak{Z} = (\mathbb{Z}, +, ۰)$ و $\mathfrak{R} = (\mathbb{R}, \times, ۱)$ تابع یک به یک $\eta = e^x : \mathbb{Z} \longrightarrow \mathbb{R}$ است. چرا که

- $\eta(c^{\mathfrak{Z}}) = \eta(۰) = e^۰ = ۱ = c^{\mathfrak{R}}$
- برای $a, b \in \mathbb{Z}$،

$$\eta(f^{\mathfrak{Z}}(a, b)) = \eta(a + b) = e^{a+b} = e^a \times e^b = \eta(a) \times \eta(b) = f^{\mathfrak{R}}(\eta(a), \eta(b)).$$

مثال ۱۰. زبان L_{ring} را در نظر می‌گیریم. در این صورت $\mathfrak{M} = (M_۲(\mathbb{R}), +, \cdot, \begin{bmatrix} ۰ & ۰ \\ ۰ & ۰ \end{bmatrix}, \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix})$ با تعبیر هر یک از نمادهای تابعی دو موضعی به اعمال جمع و ضرب معمول ماتریسی یک L-ساختار است. حال علاوه بر L-ساختار $\mathfrak{M}$، L-ساختار $\mathfrak{R} = (\mathbb{R}, +, \times, ۰, ۱)$ را در نظر می‌گیریم. تابع $\eta : \mathbb{R} \longrightarrow M_۲(\mathbb{R})$ با ضابطه $\eta(x) = \begin{bmatrix} x & ۰ \\ ۰ & x \end{bmatrix}$ یک L-نشاندن است، زیرا

[۲] L-embedding

- $\eta(۰) = \begin{bmatrix} ۰ & ۰ \\ ۰ & ۰ \end{bmatrix}$ و $\eta(۱) = \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix}$.
- $\eta(a+b) = \begin{bmatrix} a+b & ۰ \\ ۰ & a+b \end{bmatrix} = \begin{bmatrix} a & ۰ \\ ۰ & a \end{bmatrix} + \begin{bmatrix} b & ۰ \\ ۰ & b \end{bmatrix}$ به طوری که $a, b \in \mathbb{R}$.
- $\eta(a \times b) = \begin{bmatrix} a \times b & ۰ \\ ۰ & a \times b \end{bmatrix} = \begin{bmatrix} a & ۰ \\ ۰ & a \end{bmatrix} \cdot \begin{bmatrix} b & ۰ \\ ۰ & b \end{bmatrix}$ به طوری که $a, b \in \mathbb{R}$.

تمرین ۲. زبان L_{ring} و دو L-ساختار، $\mathfrak{C} = (\mathbb{C}, +, \times, ۰, ۱)$ (با تعبیر جمع و ضرب معمول اعداد) و $\mathfrak{M} = (M, +, \cdot, \begin{bmatrix} ۰ & ۰ \\ ۰ & ۰ \end{bmatrix}, \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix})$ که در آن $M = \{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} , \quad a, b \in \mathbb{R}\}$، $+$ جمع ماتریس‌ها و $\cdot$ ضرب ماتریس‌ها است را در نظر بگیرید. ثابت کنید که تابع $\eta : \mathbb{C} \longrightarrow M$ با ضابطه $\eta(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ یک L-نشاندن است.

در مثال قبل به نظر می‌رسد که یک کپی از اعداد حقیقی در $M_۲(\mathbb{R})$ وجود دارد. اما گاهی نه یک کپی از مجموعه بلکه با یک نگاشت می‌توان خود مجموعه را در سمت دیگر یافت.

تعریف ۸. فرض کنیم $\mathfrak{M} = (M, (f^{\mathfrak{M}}, R^{\mathfrak{M}}, c^{\mathfrak{M}})_{f,R,c \in L})$ و $\mathfrak{N} = (N, (f^{\mathfrak{N}}, R^{\mathfrak{N}}, c^{\mathfrak{N}})_{f,R,c \in L})$ دو L-ساختار باشند. گوییم $\mathfrak{M}$ زیر ساختار $\mathfrak{N}$ است و می‌نویسیم $\mathfrak{M} \subseteq \mathfrak{N}$ هرگاه نگاشت همانی، $id : M \longrightarrow N$ یک نشاندن باشد.

لازم به ذکر است که اگر $\mathfrak{M} \subseteq \mathfrak{N}$ آنگاه

- $f^{\mathfrak{M}} = f^{\mathfrak{N}}|_M$،
- $R^{\mathfrak{M}} = R^{\mathfrak{N}} \cap M$،
- $c^{\mathfrak{M}} = c^{\mathfrak{N}}$.

برای مثال $(\mathbb{N}, <) \subseteq (\mathbb{Z}, <)$ و $(\mathbb{C}, +, \times, ۰, ۱) \subseteq (\mathbb{R}, +, \times, ۰, ۱) \subseteq (\mathbb{Z}, +, \times, ۰, ۱)$.

۳.۱ تعابیر ترمها و فرمولها

بعد از آشنایی با تعبیر هر نماد زبان L در L-ساختارها، در ادامه سعی داریم به تعبیر L-ترم‌ها و L-فرمول‌ها در ساختارها بپردازیم.

تعریف ۹. فرض کنیم L یک زبان مرتبه اول و $t(v_۱, \ldots, v_n)$ یک L-ترم باشد. اگر $\mathfrak{M}$ یک L-ساختار با جهان M باشد و $a_۱, \ldots, a_n \in M$ آنگاه تعبیر ترم $t(v_۱, \ldots, v_n)$ در ساختار M با جایگذاری $a_۱, \ldots, a_n$ به جای $v_۱, \ldots, v_n$ که آن را با $t^{\mathfrak{M}}(a_۱, \ldots, a_n)$ نمایش می‌دهیم، به صورت استقرایی زیر تعریف می‌شود،

۱) اگر ترم t یک ثابت $c \in L$ باشد آنگاه $t^{\mathfrak{M}}(a_۱, \ldots, a_n) = c^{\mathfrak{M}}$.

۲) اگر $t(v_۱, \ldots, v_n) = v_i$ آنگاه $t(a_۱, \ldots, a_n) = a_i$.

۳) اگر f یک نماد تابعی m موضعی و $t_۱(v_۱, \ldots, v_n), \ldots, t_m(v_۱, \ldots, v_n)$ ترمهایی باشند که $t_۱^{\mathfrak{M}}(a_۱, \ldots, a_n), \ldots, t_m^{\mathfrak{M}}(a_۱, \ldots, a_n)$ دانسته باشند آنگاه $t = f(t_۱, \ldots, t_m)$ به صورت زیر تعبیر می‌شود:

$$t^{\mathfrak{M}}(a_۱, \ldots, a_n) = f^{\mathfrak{M}}(t_۱^{\mathfrak{M}}(a_۱, \ldots, a_n), \ldots, t_m^{\mathfrak{M}}(a_۱, \ldots, a_n)).$$

تذکر ۴. وقتی L یک زبان مرتبه اول است و $Var = \{v_1, \dots, v_n\}$، L-ترم‌ها را به صورت $t(v_1, \dots, v_n)$ می‌نویسیم. یعنی Lترمها صرفا کلمه هستند و معنا ندارند. اما وقتی $\mathfrak{M}$ یک L-ساختار با جهان M است و می‌نویسیم $t^{\mathfrak{M}}(a_1, \dots, a_n)$ به طوری که $a_1, \dots, a_n \in M$، در این صورت دربارهٔ معنا (تعبیر) یک ترم در یک ساختار صحبت می‌کنیم. در واقع $t^{\mathfrak{M}}(v_1, \dots, v_n)$ یک ترم نیست (به تعریف ترمها مراجعه کنید) بلکه یک نگاشت از M^n به M است که می‌توان به جای متغیرهای آن عناصر $a_1, \dots, a_n$ را جایگزین کرد و مقدار این نگاشت را در ساختار حساب کرد.

مثال ۱۱. زبان $L = \{*\}$ که در آن $*$ نماد تابعی دو موضعی است و متغیرهای v_1 و v_2 را در نظر می‌گیریم. ترم $t(v_1, v_2) = *v_1v_2$ در ساختار $\mathfrak{M}_1 = (\mathbb{R}, +)$ به صورت $t^{\mathfrak{M}_1}(a_1, a_2) = a_1 + a_2$ تعبیر می‌شود و در ساختار $\mathfrak{M}_2 = (\mathbb{N}, \times)$ به شکل $t^{\mathfrak{M}_2}(a_1, a_2) = a_1 \times a_2$ است.

مثال ۱۲. فرض کنیم $L = \{f, g, c\}$ که در آن f نماد تابعی تک موضعی، g نماد تابعی دو موضعی و c نماد ثابت باشد. همچنین فرض کنیم $Var = \{v_1, v_2\}$. دو L-ساختار $\mathfrak{M}_1 = (\mathbb{R}, \exp, +, 1)$ ($\exp$ تابع نمایی) و $\mathfrak{M}_2 = (\mathbb{N}, s, \cdot, 0)$ (s تابع تالی) را در نظر می‌گیریم. اگر $a_1 \in \mathbb{R}$ و $b_1 \in \mathbb{N}$ آنگاه تعبیر ترم $t_1(v_1) = gv_1c$ در این L-ساختارها به صورت $t_1^{\mathfrak{M}_1}(a_1) = a_1 + 1$ و $t_1^{\mathfrak{M}_2}(b_1) = b_1 \cdot 0 = 0$ است. به همین شکل، تعبیر ترم $t_2(v_1) = fgcfv_1$ در $\mathfrak{M}_1$ برابر $t_2^{\mathfrak{M}_1}(a_1) = e^{1+e^{a_1}}$ و در $\mathfrak{M}_2$ به صورت $t_2^{\mathfrak{M}_2}(b_1) = 0 \cdot (b_1 + 1) + 1 = 1$ است. به عنوان تمرین تعبیر ترم $t_3(v_1, v_2) = gv_1fgv_2gv_1fv_2$ را در این دو L-ساختار بررسی کنید.

در جلسات قبل دربارهٔ ایزومرفیسمها صحبت کرده بودیم. یکی از ویژگی‌های ایزومرفیسمها این است که تعابیر ترمها را حفظ می‌کنند:

لم ۱. فرض کنیم $\eta : \mathfrak{M} \longrightarrow \mathfrak{N}$ یک ایزومرفیسم بین دو L-ساختار $\mathfrak{M}$ و $\mathfrak{N}$ باشد. اگر $t(v_1, \dots, v_n)$ یک L-ترم باشد آنگاه برای هر $a_1, \dots, a_n \in M$ داریم

$$\eta(t^{\mathfrak{M}}(a_1, \dots, a_n)) = t^{\mathfrak{N}}(\eta(a_1), \dots, \eta(a_n)).$$

اثبات. با استقرا روی پیچیدگی ترم‌ها اثبات می‌کنیم.

۱) اگر $t(v_1, \dots, v_n) = c$ آنگاه

$$\eta(t^{\mathfrak{M}}(a_1, \dots, a_n)) = \eta(c^{\mathfrak{M}}) = c^{\mathfrak{N}} = t^{\mathfrak{N}}(\eta(a_1), \dots, \eta(a_n))$$

۲) اگر $t(v_1, \dots, v_n) = v_i$ آنگاه

$$\eta(t^{\mathfrak{M}}(a_1, \dots, a_n)) = \eta(a_i) = t^{\mathfrak{N}}(\eta(a_1), \dots, \eta(a_n))$$

۳) فرض کنیم f نماد تابعی m موضعی و $t_1, \dots, t_m$ ترم باشند. اگر $t = f(t_1, \dots, t_m)$ آنگاه برای $a_1, \dots, a_n \in M$،

$$\begin{aligned}
\eta(t^{\mathfrak{M}}(a_1, \dots, a_n)) &= \eta(f^{\mathfrak{M}}(t_1^{\mathfrak{M}}(a_1, \dots, a_n), \dots, t_m^{\mathfrak{M}}(a_1, \dots, a_n))) \\
&= f^{\mathfrak{N}}(\eta(t_1^{\mathfrak{M}}(a_1, \dots, a_n)), \dots, \eta(t_m^{\mathfrak{M}}(a_1, \dots, a_n))) \\
&= f^{\mathfrak{N}}(t_1^{\mathfrak{N}}(\eta(a_1), \dots, \eta(a_n)), \dots, t_m^{\mathfrak{N}}(\eta(a_1), \dots, \eta(a_n))) \\
&= t^{\mathfrak{N}}(\eta(a_1), \dots, \eta(a_n))
\end{aligned}$$

□

همانطور که در ابتدا اشاره کردیم در اینجا باید به تعبیر فرمول‌های مرتبه اول در ساختارها بپردازیم. اما پیش از آن باید به عنوان یک قرارداد در نظر داشته باشیم که برای یک فرمول φ منظور از $\varphi(v_1, \dots, v_n)$ این است که متغیرهای آزاد فرمول φ در مجموعه $\{v_1, \dots, v_n\}$ هستند (و لزوما همهٔ متغیرهای موجود در این مجموعه در فرمول φ استفاده نشده‌اند). برای مثال اگر زبان $L = \{\cdot, +, 0\}$ و $Var = \{x, y, z\}$، فرمول $\exists x \quad + \cdot xxy$ (یا به شکل جبری $\exists x \quad x^2 + y$)، را به صورت $\varphi(y)$ (و یا حتی $\varphi(y, z)$) نمایش می‌دهیم.

تعریف ۱۰. فرض کنیم $\varphi(v_1,\dots,v_n)$ یک L-فرمول باشد. اگر $\mathfrak{M}$ یک L-ساختار با جهان M باشد و $a_1,\dots,a_n \in M$، گوییم

$$\mathfrak{M} \models \varphi(a_1,\dots,a_n)$$

(بخوانیم $\mathfrak{M}$ مدلی برای φ است وقتی به جای v_iها، a_i قرار بگیرد) هرگاه $\varphi(a_1,\dots,a_n)$ در $\mathfrak{M}$ برقرار باشد. تعریف دقیق‌تر، تنها به صورت استقرائی زیر ممکن است.

۱) اگر $\varphi : t_1(v_1,\dots,v_n) = t_2(v_1,\dots,v_n)$ گوییم $\mathfrak{M} \models \varphi(a_1,\dots,a_n)$ هرگاه $t_1^{\mathfrak{M}}(a_1,\dots,a_n) = t_2^{\mathfrak{M}}(a_1,\dots,a_n)$.

۲) اگر $\varphi : R(t_1,\dots,t_m)(v_1,\dots,v_n)$ گوییم $\mathfrak{M} \models \varphi(a_1,\dots,a_n)$ هرگاه $R^{\mathfrak{M}}(t_1^{\mathfrak{M}}(a_1,\dots,a_n),\dots,t_m^{\mathfrak{M}}(a_1,\dots,a_n))$ یا به عبارت دیگر $t_1^{\mathfrak{M}}(a_1,\dots,a_n),\dots,t_m^{\mathfrak{M}}(a_1,\dots,a_n) \in R^{\mathfrak{M}}$.

۳) اگر $\varphi(v_1,\dots,v_n)$ یک L-فرمول باشد آنگاه $\mathfrak{M} \models \neg\varphi(a_1,\dots,a_n)$ اگر و تنها اگر $\mathfrak{M} \not\models \varphi(a_1,\dots,a_n)$.

۴) اگر $\varphi(v_1,\dots,v_n)$ و $\psi(v_1,\dots,v_n)$ فرمول باشند آنگاه

$$\mathfrak{M} \models (\varphi \wedge \psi)(a_1,\dots,a_n) \iff \mathfrak{M} \models \varphi(a_1,\dots,a_n) \quad \& \quad \mathfrak{M} \models \psi(a_1,\dots,a_n).$$

۵) اگر $\varphi(w,v_1,\dots,v_n)$ فرمول باشد آنگاه $\mathfrak{M} \models (\exists w \ \ \varphi)(a_1,\dots,a_n)$ اگر عنصر $a \in M$ وجود داشته باشد که $\mathfrak{M} \models \varphi(a,a_1,\dots,a_n)$.

مثال ۱۳. در زبان L_{ring} با $Var = \{x,y,z\}$ داریم

۱) اگر $\mathfrak{M}_1 = (\mathbb{C},+,\cdot,0,1)$ آنگاه $\mathfrak{M}_1 \models \exists x \ \ x^2 + 1$.

۲) اگر $\mathfrak{M}_2 = (\mathbb{R},+,\cdot,0,1)$، $\psi(x,y) : \exists z \ \ y = x + z^2$ و $\chi(x,y) : \exists z \ \ y = x \cdot z + y = 0$ آنگاه $\mathfrak{M}_2 \models \psi(2,3)$ اما $\mathfrak{M}_2 \not\models \chi(2,3)$.

مثال ۱۴. زبان معرفی شده در مثال ۱۲ را در نظر می‌گیریم. اگر $\mathfrak{M}_1 = (\mathbb{R},\exp,\cdot,1)$ و $\mathfrak{M}_2 = (\mathbb{N},s,+,0)$ دو ساختار در این زبان و فرمول $\varphi : \exists x \ \ fx = c$، آنگاه $\mathfrak{M}_1 \models \varphi$ اما $\mathfrak{M}_2 \not\models \varphi$.

در قضیهٔ بعدی خواهیم دید که ایزومرفیسمها، همهٔ ویژگی‌های مرتبهٔ اول ساختارها را حفظ می‌کنند.

قضیه ۱. فرض کنیم $\mathfrak{M}$ و $\mathfrak{N}$ دو L-ساختار و $\varphi(v_1,\dots,v_n)$ یک فرمول مرتبه اول در زبان L باشند. اگر $\eta : \mathfrak{M} \longrightarrow \mathfrak{N}$ یک L-ایزومرفیسم باشد آنگاه برای هر $a_1,\dots,a_n \in M$ داریم

$$\mathfrak{M} \models \varphi(a_1,\dots,a_n) \iff \mathfrak{N} \models \varphi(\eta(a_1),\dots,\eta(a_n))$$

اثبات. تمرین. □

تعریف ۱۱. L-فرمول φ را یک L-جمله[۳] می‌نامیم هرگاه هیچ متغیر آزادی نداشته باشد.

برای مثال، در زبان L_{ring}، $\varphi : \exists x \ \ x^2 + 1 = x$ یک L-جمله است در حالی که $\psi : \exists x \ \ x^2 + 1 = y$، L-جمله نیست.

تعریف ۱۲. گوییم دو L-ساختار $\mathfrak{M}$ و $\mathfrak{N}$ هم ارز مقدماتی[۴] هستند هرگاه برای هر L-جمله φ داشته باشیم

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

در این صورت می‌نویسیم $\mathfrak{M} \equiv \mathfrak{N}$.

[۳] L-sentence

[۴] elenentary equivalent

مثال ۱۵. زبان L_{ring} و دو ساختار $\mathfrak{M}_۱$ و $\mathfrak{M}_۲$ در مثال ۱۴ را در نظر می‌گیریم. در این صورت $\mathfrak{M}_۱ \not\equiv \mathfrak{M}_۲$ چون برای L-جمله $\varphi : \exists x \;\; x^۲ + ۱ = ۰$ داریم $\mathfrak{M}_۱ \models \varphi$ و $\mathfrak{M}_۲ \not\models \varphi$.

مثال ۱۶. زبان L_{order} و دو L-ساختار $\mathfrak{M}_۱ = (\mathbb{Z}, \leq)$ و $\mathfrak{M}_۲ = (\mathbb{Q}, \leq)$ را در نظر می‌گیریم. همانطور که می‌دانیم ترتیب در مجموعه اعداد گویا دارای خاصیت چگال بودن است اما مجموعه اعداد صحیح چنین نیست. این خاصیت را به صورت L-جمله

$$\varphi : \forall x \;\; \forall y \;\; (x < y \longrightarrow \exists z \;\; (z \neq x \wedge z \neq y \wedge x < z < y))$$

نمایش می‌دهیم. بنابراین $\mathfrak{M}_۱ \not\models \varphi$ و $\mathfrak{M}_۲ \models \varphi$. پس $\mathfrak{M}_۱ \not\equiv \mathfrak{M}_۲$.

همانطور که از مثال‌ها هم مشخص است اثبات هم ارز نبودن دو ساختار به نظر ساده‌تر است و کافی است یکی از تفاوت‌های بنیادین ساختارها را به صورت جمله مرتبه اول بنویسیم. اما برای اثبات هم ارز بودن دو ساختار به مطالعه مفاهیم بیشتری از منطق نیاز است که در این درس فرصت پرداختن به آن را نداریم!

تذکر ۵. وقتی φ یک جمله باشد باز هم می‌توانیم بنویسیم $\varphi(v_۱, \ldots, v_n)$. در این حالت اگر $\mathfrak{M}$ یک ساختار باشد و $a_۱, \ldots, a_n, b_۱, \ldots, b_n \in M$ داریم $\mathfrak{M} \models \varphi(a_۱, \ldots, a_n) \iff \mathfrak{M} \models \varphi(b_۱, \ldots, b_n)$. برای مثال اگر زبان L_{ring}، $\mathfrak{M}_۱ = (\mathbb{C}, \cdot, +, ۰, ۱)$ و $\varphi(y) : \exists x \;\; x^۲ + ۱ = ۰$ باشد، آنگاه

$$\mathfrak{M}_۱ \models \varphi \iff \mathfrak{M}_۱ \models \varphi(۱۵) \iff \mathfrak{M}_۱ \models \varphi(۲i + ۳).$$

اما در مورد فرمول‌ها بحث متفاوت است. برای مثال اگر ساختار $\mathfrak{M}_۲ = (\mathbb{R}, \cdot, +, ۰, ۱)$ و $\varphi(y) : \exists x \;\; x^۲ = y$ آنگاه $\mathfrak{M}_۲ \models \varphi(۲)$ اما $\mathfrak{M}_۲ \not\models \varphi(-۱)$.

از آنچه در تذکر بالا گفتیم نتیجه زیر حاصل می‌شود.

نتیجه ۱. اگر دو ساختار $\mathfrak{M}$ و $\mathfrak{N}$ ایزومرف باشند (می‌نویسیم $\mathfrak{M} \cong \mathfrak{N}$) آنگاه $\mathfrak{M}$ و $\mathfrak{N}$ هم ارز مقدماتی هستند.

مثال ۱۷. هر دو میدان بسته جبری با مشخصه صفر هم ارز مقدماتی هستند (این گفته را در بخشهای آینده درس اثبات خواهیم کرد). می‌دانیم $\mathbb{C}$ یک میدان بسته جبری با مشخصه صفر است، بنابراین اگر φ یک جمله باشد و $(\mathbb{C}, +, \cdot, ۰, ۱) \models \varphi$ آنگاه در تمام میدان‌های بسته جبری دیگر مانند K نیز داریم $(K, +, \cdot, ۰, ۱) \models \varphi$. به همین صورت هر مجموعه مرتب خطی چگال بدون ابتدا و انتها با $(\mathbb{Q}, \leq)$ هم ارز مقدماتی است. برای مثال $(\mathbb{R}, \leq) \equiv (\mathbb{Q}, \leq)$.

۴.۱ تعریف‌پذیری

تعریف ۱۳. فرض کنیم $\mathfrak{M}$ یک ساختار مرتبه اول با جهان M باشد. یک مجموعه $X \subseteq M^n$ را تعریف پذیر توسط فرمول $\varphi(x_۱, \ldots, x_n, y_۱, \ldots, y_m)$ با پارامترهای $b_۱, \ldots, b_m$ می‌نامیم هرگاه

$$X = \{(a_۱, \ldots, a_n) \in M^n \mid \mathfrak{M} \models \varphi(a_۱, \ldots, a_n, b_۱, \ldots, b_m)\}.$$

اگر $b_۱, \ldots, b_m \in A \subseteq M$، می‌گوییم X تعریف پذیر با پارامتر A است.

مثال ۱۸. فرض کنیم زبان L_{ring} و $\mathfrak{M} = (R, +, \cdot, ۰, ۱)$ باشد که جهان M یعنی R، یک حلقه است. فرض کنیم $p(x) \in R[x]$ (چندجمله‌ای‌های تک متغیره با ضرایب متعلق به R)، در این صورت مجموعه $Y = \{x \in R \mid p(x) = ۰\}$ (مجموعه ریشه‌های یک چندجمله‌ای) یک مجموعه تعریف پذیر است. به طور دقیق‌تر، مثلا فرمول زیر را در نظر بگیرید:

$$\varphi(x, y_۰, y_۱, y_۲) : y_۰ + y_۱ x + y_۲ x^۲ = ۰$$

حال مجموعهٔ

$$X = \{x \in M : ۳ + ۲x + ۵x^۲ = ۰\}$$

یک مجموعهٔ تعریف‌پذیر (با استفاده از پارامترهای $۲, ۳, ۵$) است؛ زیرا

$$X = \{x \in M : \mathfrak{M} \models \varphi(x, ۳, ۲, ۵)\}.$$

به همین صورت مجموعه

$$X = \{(x_۱, \ldots, x_n) \in R^n \mid f_۱(x_۱, \ldots, x_n) = ۰ \wedge \cdots \wedge f_k(x_۱, \ldots, x_n)\}$$

(مجموعه جواب‌های یک دستگاه معادلات چندجمله‌ای) تعریف پذیر است. در همین ساختار مجموعه $\{x \mid x \cdot x + x + x + ۱ = ۰\}$ (یا به شکل ساده‌تر $\{x \mid x^۲ + ۲x + ۱ = ۰\}$) تعریف پذیر بدون استفاده از پارامتر است.

مثال ۱۹. زبان L_{ring} و ساختار $\mathfrak{M} = (\mathbb{R}, +, \cdot, ۰, ۱)$ را در نظر می‌گیریم. با اینکه نماد رابطه‌ای $<$ در زبان وجود ندارد، مجموعه

$$X = \{(x, y) \in \mathbb{R}^۲ \mid x < y\}$$

(منظور از $<$ ترتیب معمول اعداد حقیقی است) تعریف پذیر توسط فرمول $\varphi : \exists z \ (z \neq ۰ \wedge y = x + z^۲)$ است. به طور مشابه، مجموعه $Y = \{(x, y) \in \mathbb{Z}^۲ \mid x < y\}$ در ساختار $\mathfrak{N} = (\mathbb{Z}, +, \cdot, ۰, ۱)$ نیز تعریف پذیر است. چرا که بر اساس قضیه لاگرانژ هر عدد صحیح مثبت حاصل جمعی از چهار مربع کامل است که در منطق مرتبه اول فرمولی به صورت $\psi(x, y) : \exists t_۱ \ \exists t_۲ \ \exists t_۳ \ \exists t_۴ \quad y = x + t_۱^۲ + t_۲^۲ + t_۳^۲ + t_۴^۲$ است. پس

$$Y = \{(x, y) \in \mathbb{Z}^۲ \mid x < y\} = \{(x, y) \in \mathbb{Z}^۲ \mid \mathfrak{N} \models \psi(x, y)\}.$$

مثال ۲۰. اگر F یک میدان و $\mathfrak{M} = (F[x], +, \cdot, ۰, ۱)$ (منظور از $F[x]$ مجموعه همه چندجمله‌ای‌های تک متغیره با ضرایب متعلق به F است) یک L_{ring}-ساختار باشد، آنگاه $F \subseteq F[x]$ تعریف پذیر است. زیرا تنها عناصر وارون پذیر $F[x]$ اعضای F هستند و

$$F = \{x \mid \mathfrak{M} \models x = ۰ \vee \exists y \ \ x \cdot y = ۱\}.$$

در بحث تعریف پذیری مجموعه‌ها مثال‌های جدی‌تری نیز وجود دارند که برای پرداختن به آن‌ها به ابزارها و اطلاعات بیشتری نیاز است. برای مثال پاسخ دادن به این سوال که آیا $\mathbb{Z} \subseteq \mathbb{Q}$ در ساختار $(\mathbb{Q}, +, \cdot, ۰, ۱)$ تعریف پذیر است، چندان ساده نیست و به ظاهر فرمولی در منطق مرتبه اول وجود ندارد که بتوان توسط آن این مجموعه را تعریف کرد. اما جولیا رابینسون به این سوال پاسخ مثبت می‌دهد که البته از پرداختن به آن صرف نظر می‌کنیم. در واقع یک سوال کلی در مطالعهٔ مدل‌تئورتیک وجود دارد که مجموعه‌های تعریف پذیر در میدان‌های خاص، مدول‌های خاص و یا حلقه‌های خاص چه شکلی دارند.

تمرین ۳. مجموعه $\mathbb{C}$ در ساختار $(\mathbb{C}, +, \cdot, ۰, ۱)$ تعریف پذیر است. در واقع با مطالعه برخی مباحث در خم‌های بیضوی در می‌یابیم vهایی که در فرمول $\varphi : \exists x \ \exists y \ \ v = y^۲ \wedge v = x^۳ + ۱$ صدق می‌کنند همان اعداد مختلط هستند. به عنوان یک پروژه درسی بررسی کنید که چرا اعضای $\mathbb{C}$ را می‌توان به این صورت نوشت.

برای دست یابی به ابزارهای بیشتری پیرامون اثبات تعریف پذیری یک مجموعه گزاره زیر را بیان می‌کنیم. توجه کنیم که این گزاره به صورت خیلی کلی بیان شده است.

گزاره ۱. ساختار $\mathfrak{M}$ با جهان M را در نظر می‌گیریم،

۱) فرض کنیم X و Y دو مجموعه تعریف پذیر در $\mathfrak{M}$ باشند در این صورت مجموعه‌های $X \cup Y$، $X \cap Y$ و X^c نیز تعریف پذیر هستند.

۲) فرض کنیم $X \subseteq M^n \times M^m$ در ساختار $\mathfrak{M}$ قابل تعریف باشد در این صورت تصویر X روی M^n قابل تعریف است.

اثبات. تمرین. □

تمرین ۴. فرض کنیم $X \subseteq \mathbb{R}^n$ در $(\mathbb{R}, +, \cdot, ۰, ۱, <)$ قابل تعریف باشد. ثابت کنید بستار توپولوژیک X هم قابل تعریف است.

قضیه ۲. فرض کنیم $\mathfrak{M}$ یک L-ساختار باشد و $X \subseteq M^n$ یک مجموعه A-تعریف پذیر باشد. در این صورت برای هر $\sigma \in Aut(\frac{\mathfrak{M}}{A})$ داریم $\sigma(X) = X$. به عبارت دیگر، برای هر اتومرفیسم $\sigma : \mathfrak{M} \longrightarrow \mathfrak{M}$ اگر برای هر $a \in A$ داشته باشیم $\sigma(a) = a$ آنگاه $\sigma(X) = X$.

اثبات. می‌دانیم X تعریف پذیر است، پس برای $\overline{x} = (x_۱, \ldots, x_n) \in M^n$ و $\overline{a} = (a_۱, \ldots, a_m) \in A^m$ داریم

$$X = \{\overline{x} \mid \mathfrak{M} \models \varphi(\overline{x}, \overline{a})\}.$$

بنا به قضیه ۱،

$$\begin{aligned} \mathfrak{M} \models \varphi(\overline{x}, \overline{a}) &\iff \mathfrak{M} \models \varphi(\sigma(\overline{x}), \sigma(\overline{a})) \\ &\iff \mathfrak{M} \models \varphi(\sigma(\overline{x}), \overline{a}) \\ &\iff \sigma(\overline{x}) \in X. \end{aligned}$$

□

مثال ۲۱. مجموعه $\mathbb{R}$ در ساختار $(\mathbb{C}, +, \cdot, ۰, ۱)$ قابل تعریف نیست، ثابت می‌کنیم اتومرفیسم σ وجود دارد که $\sigma(\mathbb{R}) \neq \mathbb{R}$. فرض کنیم دو عنصر $r \in \mathbb{R}$ و $s \notin \mathbb{R}$ به گونه‌ای باشند که هر دو روی $\mathbb{Q}$ متعالی باشند. در این صورت $\mathbb{Q}(r) \cong \mathbb{Q}(s)$ (جلوتر و در مباحث جبری درس به چرایی و چگونگی این یکریختی خواهیم پرداخت) و یک اتومرفیسم $\sigma \in Aut(\frac{\mathbb{C}}{\mathbb{Q}})$ وجود دارد که $\sigma(r) = s$. پس $\mathbb{R}$ تعریف پذیر نیست.

۵.۱ تئوری‌های مرتبهٔ اول

در جلسات قبل گفتیم که یک Lفرمول را که هیچ متغیر آزادی ندارد، یک Lجمله می‌نامیم.

تعریف ۱۴. فرض کنیم L یک زبان مرتبه اول باشد،

۱) منظور از یک L-تئوری مرتبه اول T، مجموعه‌ای از L-جملات است.

۲) فرض کنیم T یک L-تئوری باشد و $\mathfrak{M}$ یک L-ساختار باشد می‌گوییم $\mathfrak{M} \models T$ ($\mathfrak{M}$ مدلی برای تئوری T است) هرگاه برای هر جمله $\varphi \in T$ داشته باشیم $\mathfrak{M} \models \varphi$.

۳) فرض کنیم $\mathbb{K}$ یک کلاس از L-ساختارها باشد. می‌گوییم $\mathbb{K}$ یک کلاس مقدماتی است هرگاه یک تئوری T موجود باشد به طوری که

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

لازم به ذکر است که در زبان ریاضی روزمره تئوری را گاهی نظریه و گاهی اصول موضوعه می‌نامند.

مثال ۲۲. زبان $L = \emptyset$ را در نظر می‌گیریم. ساختار $\mathfrak{M}$ مدلی برای جمله $\varphi_۲ : \exists x_۱ \; \exists x_۲ \; (x_۱ \neq x_۲)$ است هرگاه $\mathfrak{M}$ حداقل دارای دو عضو باشد. به همین صورت ساختار $\mathfrak{M}$ مدلی برای جمله

$$\varphi_۳ : \exists x_۱ \; \exists x_۲ \; \exists x_۳ \; (x_۱ \neq x_۲ \wedge x_۱ \neq x_۳ \wedge x_۲ \neq x_۳)$$

است هرگاه حداقل سه عضو داشته باشد. به همین ترتیب می‌توان بی‌نهایت جمله φ_i نوشت. در این صورت می‌توانیم تئوری مجموعه‌های نامتناهی را مجموعه $T_{infset} = \{\varphi_۲, \varphi_۳, \ldots\}$ در نظر بگیریم. بنابراین اگر $\mathfrak{M} \models T$ آنگاه $\mathfrak{M}$ یک مجموعه نامتناهی است. همچنین نتیجه می‌گیریم که کلاس مجموعه‌های نامتناهی یک کلاس مقدماتی است.

مثال ۲۳. در زبان $L = \emptyset$، $T = \{\psi_۳\}$ به طوری که

$$\psi_۳ : \exists x_۱ \ \exists x_۲ \ \exists x_۳ \ \ (x_۱ \neq x_۲ \wedge x_۱ \neq x_۳ \wedge x_۲ \neq x_۳) \wedge (\forall y \ (y = x_۱ \vee y = x_۲ \vee y = x_۳))$$

تئوری مجموعه‌های سه عضوی است. در این صورت $\mathfrak{M} \models T$ اگر و تنها اگر جهانِ ساختار $\mathfrak{M}$ سه عضوی باشد.

تذکر ۶. یک سوال مناسب در این جای درس این است که آیا مجموعه‌های متناهی را می‌توان اصل‌بندی کرد؟ به عبارت دیگر آیا می‌توان یک تئوری مانند T در زبانِ $L = \emptyset$ بنویسیم به طوری که $\mathfrak{M} \models T$ اگروتنهااگر M متناهی باشد؟

مثال ۲۴. در زبان $L = \{<\}$،

۱) تئوری $T_{or} = \{\varphi_۱, \varphi_۲, \varphi_۳\}$ که

$$\varphi_۱ : \forall x \ \neg(x < x)$$

$$\varphi_۲ : \forall x \ \forall y \ \forall z \ \neg(x < y \wedge y < z \longrightarrow x < z)$$

$$\varphi_۳ : \forall x \ \forall y \ \neg(x < y \vee y < x \vee x = y)$$

تئوری مجموعه‌های مرتب خطی است. برای مثال $(\mathbb{Q}, <), (\mathbb{Z}, <) \models T_{or}$. به طور کلی اگر $\mathfrak{M} = (M, <^{\mathfrak{M}}) \models T$ آنگاه $(M, <^{\mathfrak{M}})$ یک مجموعه مرتب خطی است.

۲) اگر بخواهیم تئوری مجموعه‌های مرتب خطی گسسته را بنویسیم کافی است که جمله

$$\varphi_۴ : \forall x \ \exists y \ \ (y > x \wedge \neg(\exists z \ (x < z < y)))$$

را به تئوری T_{or} اضافه کنیم. بنابراین $T' = T_{or} \cup \{\varphi_۴\}$ تئوری مجموعه‌های مرتب خطی گسسته است. پس $(\mathbb{Z}, <) \models T'$ اما $(\mathbb{Q}, <) \not\models T'$.

مثال ۲۵. فرض کنیم $L = \{E\}$ که E یک نماد رابطه‌ای دو موضعی است.

۱) تئوری T شامل جملات

$$\varphi_۱ : \forall x \ \ E(x, x)$$

$$\varphi_۲ : \forall x \ \forall y \ \ (E(x, y) \longrightarrow E(y, x))$$

$$\varphi_۳ : \forall x \ \forall y \ \forall z \ \ (E(x, y) \wedge E(y, z) \longrightarrow E(x, z))$$

تئوری روابط هم ارزی است. به عبارت دیگر اگر $\mathfrak{M} = (M, E^{\mathfrak{M}}) \models T$ آنگاه $E^{\mathfrak{M}}$ یک رابطه هم ارزی روی M است.

۲) تئوری $T' = T \cup \{\psi\}$ که در آن

$$\forall x \ \exists y \ \ \Big(y \neq x \wedge E(x, y) \wedge \forall z \ \ (E(z, x) \longrightarrow (z = x \vee z = y))\Big)$$

تئوری روابط هم ارزی‌ای است که در آن‌ها هر کلاس هم ارزی دقیقاً دو عضو دارد.

مثال ۲۶. زبان L_{group} را در نظر می‌گیریم.

۱) تئوری گروه‌ها را با T_{group} نمایش می‌دهیم که شامل جملات $\varphi_۱$، $\varphi_۲$ و $\varphi_۳$ به صورت زیر است:

$$\varphi_۱ : \forall x \ \ \circ + x = x + \circ = x$$

$$\varphi_۲ : \forall x \ \exists y \ \ x + y = \circ$$

$$\varphi_۳ : \forall x \ \forall y \ \forall z \ \ (x + (y + z) = (x + y) + z).$$

۲) منظور از گروه‌های بخش پذیر این است که برای هر عنصر x و هر $n \in \mathbb{N}$، عنصر y وجود داشته باشد که $ny = x$. (منظور از ny عنصری از گروه است که با n بار جمع کردن عنصر y به دست می‌آید). به ترتیب جملات $\psi_۲ : \forall x\ \exists y\ \ y + y = x$ و $\psi_۳ : \forall x\ \exists y\ \ y + y + y = x$ و ... را در نظر می‌گیریم. در این صورت $T = T_{group} \cup \{\psi_۲, \psi_۳, \ldots\}$ تئوری گروه‌های بخش پذیر است.

۳) در زبان $L_{group_۱} \cup \{<\}$ تئوری گروه‌های آبلی مرتب به شکل

$$T = T_{group} \cup T_{or} \cup \{\forall x\ \forall y\ \ x + y = y + x\} \cup \{\forall x\ \forall y\ \forall z\ \ (x < y \longrightarrow x + z < y + z)\}$$

است.

۴) منظور از گروه بدون تاب گروهی است که برای هر عنصر ناصفر x در گروه و برای هر $n \in \mathbb{N}$ داریم $nx \neq ۰$. بنابراین با اضافه کردن جملات

$$\varphi_۲ : \forall x\ \ (x \neq ۰ \longrightarrow x + x \neq ۰)$$
$$\varphi_۳ : \forall x\ \ (x \neq ۰ \longrightarrow x + x + x \neq ۰)$$
$$\vdots$$

به T_{group}، تئوری گروه‌های بدون تاب به دست می‌آید. بنابراین $T_{torsion-free-groups} = T_{group} \cup \{\varphi_۲, \varphi_۳, \ldots\}$.

مثال ۲۷. فرض کنیم زبان مورد نظر L_{ring} باشد،

۱) تئوری حلقه‌ها به صورت $T_{ring} = T_{group} \cup \{\varphi_۱, \varphi_۲, \varphi_۳, \varphi_۴, \varphi_۵\}$ است که

$$\varphi_۱ : \forall x\ \ x \cdot ۰ = ۰ \cdot x = ۰$$
$$\varphi_۲ : \forall x\ \forall y\ \forall z\ \ x \cdot (y \cdot z) = (x \cdot y) \cdot z$$
$$\varphi_۳ : \forall x\ \ x \cdot ۱ = ۱ \cdot x = x$$
$$\varphi_۴ : \forall x\ \forall y\ \forall z\ \ x \cdot (y + z) = x \cdot y + x \cdot z$$
$$\varphi_۵ : \forall x\ \forall y\ \forall z\ \ (x + y) \cdot z = x \cdot z + y \cdot z$$

۲) در همان زبان بالا، تئوری میدان‌ها به صورت

$$T_{field} = T_{ring} \cup \{\forall x\ \forall y\ \ x \cdot y = y \cdot x\} \cup \{\forall x\ \ (x \neq ۰) \longrightarrow (\exists y\ \ x \cdot y = ۱)\}$$

است.

۳) میدان‌های بسته جبری میدان‌هایی هستند که هر چندجمله‌ای در آن ریشه داشته باشد (برای مثال $\mathbb{C}$ یک میدان بسته جبری است در صورتی که $\mathbb{R}$ بسته جبری نیست زیرا $x^۲ + ۱$ در آن ریشه ندارد). تئوری این میدان‌ها به صورت زیر است

$$T = T_{field} \cup \{\forall a_۰\ \forall a_۱\ \exists x\ \ a_۰ + a_۱x = ۰, \forall a_۰\ \forall a_۱\ \forall a_۲ \exists x\ \ a_۰ + a_۱x + a_۲x^۲ = ۰, \ldots\}$$

۴) در زبان $L_{ring} \cup \{<\}$،

$$T = T_{field} \cup \{\forall x\ \forall y\ \forall z\ \ (x < y \longrightarrow x + z < y + z)\} \cup \{\forall x\ \forall y\ \forall z\ \ (x < y \wedge z > ۰ \longrightarrow x \cdot z < y \cdot z)\}$$

تئوری میدان‌های مرتب است.

تعریف ۱۵. فرض کنیم T یک L-تئوری و φ یک L-جمله باشد می‌گوییم T مستلزم φ است و به صورت $T \models \varphi$ نمایش می‌دهیم هرگاه برای هر مدل $\mathfrak{M} \models T$ داشته باشیم $\mathfrak{M} \models \varphi$.

مثال ۲۸. نشان می‌دهیم تئوری گروه‌های آبلی مرتب (مثال ۲۶) مستلزم $\varphi : \forall x \ (x \neq 0 \longrightarrow x + x \neq 0)$ است. فرض کنیم ساختار $\mathfrak{M}$ یک گروه آبلی مرتب باشد. باید نشان دهیم $\mathfrak{M} \models \varphi$. فرض کنیم $x \neq 0$ در این صورت یا $x > 0$ و یا $x < 0$. اگر $x > 0$ آنگاه $x + x > x > 0$ پس $x + x \neq 0$. به طور مشابه اگر $x < 0$ آنگاه $x + x \neq 0$.

همانطور که گفتیم $T \models \varphi$ هر گاه برای L-ساختار $\mathfrak{M}$ اگر مدلی برای T باشد داشته باشیم $\mathfrak{M} \models \varphi$. بنابراین اگر $T \not\models \varphi$ آنگاه یک ساختار وجود دارد که $\mathfrak{M} \models T$ اما $\mathfrak{M} \models \neg\varphi$؛ به بیان دیگر $T \not\models \varphi$ هرگاه $T \cup \{\neg\varphi\}$ دارای مدل باشد. اما سوالی که پیش می‌آید این است که آیا یک تئوری می‌تواند نه مستلزم یک جمله مانند φ باشد و نه مستلزم نقیض آن؟ پاسخ مثبت است. برای مثال تئوری گروه‌ها و جمله $\varphi : \forall x \ \forall y \ \ x + y = y + x$ را در نظر می‌گیریم. واضح است که برای این تئوری مدلهائی هستند که φ در آن‌ها صدق می‌کند (گروه‌های آبلی) و هم ساختارهایی هستند که نقیض φ در آن‌ها برقرار است (گروه‌های غیر آبلی). بنابراین $T \not\models \varphi$ و $T \not\models \neg\varphi$. (توجه کنید که اگر $\mathfrak{M}$ یک ساختار و φ یک جمله باشد، یا $\mathfrak{M} \models \varphi$ و یا $\mathfrak{M} \models \neg\varphi$. مثلاً یک گروه نمی‌تواند هم آبلی باشد و هم آبلی نباشد.)

گزاره ۲. تئوری T مدل ندارد اگر و تنها اگر یک جمله φ موجود باشد که $T \models \varphi \wedge \neg\varphi$. به عبارت دیگر تئوری T هیچ مدلی ندارد اگروتنهااگر مستلزم تناقض باشد. به عبارت دیگر تئوری T دارای مدل است اگروتنهااگر مستلزم تناقض نباشد.

اثبات. فرض کنیم T مدل ندارد به انتفای مقدم $T \models \varphi \wedge \neg\varphi$. حال فرض کنیم $T \models \varphi \wedge \neg\varphi$. در این صورت اگر $\mathfrak{M} \models T$ آنگاه $\mathfrak{M} \models \varphi$ و $\mathfrak{M} \not\models \varphi$ که این یک تناقض است. □

تعریف ۱۶. تئوری T را کامل می‌نامیم هرگاه برای هر جمله φ داشته باشیم $T \models \varphi$ یا $T \models \neg\varphi$.

پس وقتی تئوری T کامل است، یک جملهٔ دلخواه φ یا همزمان در همهٔ مدلهای آن برقرار است یا همزمان نقیض آن در همهٔ مدلها برقرار است. پس مثلا تئوری گروه‌ها، کامل نیست، زیرا جملهٔ آبلی بودن در برخی گروه‌ها برقرار است و در برخی دیگر برقرار نیست. در واقع اگر تئوری T کامل باشد و $\mathfrak{M}$ مدلی برای آن باشد، هر ویژگی‌ای که $\mathfrak{M}$ داشته باشد، همهٔ مدلهای دیگر T هم دارند.

تعریف ۱۷. فرض کنیم $\mathfrak{M}$ یک L-ساختار باشد در این صورت

$$Th(\mathfrak{M}) = \{\varphi \mid \ \mathfrak{M} \models \varphi\}.$$

به راحتی می‌توان دید که تئوری T کامل است اگروتنهااگر مدلهای آن با مدلهای $Th(\mathfrak{M})$، برای هر $\mathfrak{M} \models T$ یکی باشد.
مثال زیر، ربطی به تئوری‌های کامل ندارد!

مثال ۲۹. فرض کنیم $L = \{H\}$ یک نماد رابطه‌ای تک موضعی باشد. در این صورت

$$\emptyset \models \exists x \ (H(x) \longrightarrow \forall y \ H(y)).$$

این جمله در همه ساختارها صحیح است و آن را در زبان روزمره می‌توان به این صورت معنا کرد که یک نفر هست که اگر او کلاه داشته باشد همه کلاه دارند!
برای اثبات فرض کنیم $\mathfrak{M} = (M, H^{\mathfrak{M}})$ یک L-ساختار باشد. اگر $a \in M$ وجود داشته باشد که $\neg H^{\mathfrak{M}}(a)$ (به زبان دیگر یعنی یک نفر باشد که کلاه نداشته باشد) آنگاه به انتفای مقدم

$$\mathfrak{M} \models \exists x \ (H(x) \longrightarrow \forall y \ H(y)).$$

اگر $H^{\mathfrak{M}}(a)$ برای هر $a \in M$ برقرار باشد (همه کلاه داشته باشند) آنگاه به وضوح

$$\mathfrak{M} \models \exists x \ (H(x) \longrightarrow \forall y \ H(y)).$$

تذکر ۷. اگر $\emptyset \models \varphi$ می‌نویسیم $\models \varphi$، پس جمله مثال قبل را می‌توان به این صورت نشان داد $\models \exists x \ (H(x) \longrightarrow \forall y \ H(y))$.

۶.۱ قضیهٔ فشردگی

قضیهٔ فشردگی یک محک است برای بررسی این که چه زمانی یک تئوری بزرگ دارای مدل است.

قضیه ۳. (قضیه فشردگی). فرض کنیم T یک تئوری مرتبه اول باشد در این صورت T دارای یک مدل است اگر هر زیرمجموعه متناهی $\Delta \subseteq T$ دارای مدل باشد. به عبارت دیگر T مستلزم تناقض نیست اگروتنهااگر هیچ زیرمجموعهٔ متناهی از آن مستلزم تناقض نباشد.

اثبات. برای مشاهده اثبات می‌توانید به جزوه درس منطق کارشناسی مراجعه کنید. □

نتیجه ۲. اگر $T \models \varphi$ آنگاه مجموعه متناهی $\Delta \subseteq T$ وجود دارد که $\Delta \models \varphi$.

اثبات. اگر $T \models \varphi$ آنگاه $T \cup \{\neg\varphi\}$ مدل ندارد بنا به قضیه فشردگی یک زیرمجموعه متناهی Δ وجود دارد که $\Delta \cup \{\neg\varphi\}$ مدل ندارد یعنی $\Delta \models \varphi$. □

در ادامه سعی داریم در قالب چند مثال کاربردهایی از قضیه فشردگی را بیان کنیم.

مثال ۳۰. میدان اعداد حقیقی یک میدان ارشمیدسی است یعنی

$$\forall x, y > ۰ \ \ \exists m \in \mathbb{N} \ \ x < my.$$

به کمک قضیه فشردگی ثابت می‌کنیم خاصیت ارشمیدسی بودن یک میدان را نمی‌توان با یک فرمول مرتبه اول در زبان حلقه‌های مرتب نوشت. برای این منظور در زبان $L_{ring} \cup \{<\}$ یک ساختار (میدان مرتب) را پیدا می‌کنیم که همهٔ ویژگی‌های مرتبهٔ اول ساختار اعداد حقیقی، $\mathfrak{R} = (\mathbb{R}, +, \cdot, ۰, ۱, <)$ را دارد ولی غیر ارشمیدسی است. $Th(\mathfrak{R})$ را در نظر می‌گیریم بنابراین اگر $\mathfrak{M}$ یک L-ساختار باشد و $\mathfrak{M} \models Th(\mathfrak{R})$ آنگاه $\mathfrak{M} \equiv \mathfrak{R}$. تئوری T^* را در زبان $L \cup \{c_۱, c_۲\}$ را به صورت زیر در نظر می‌گیریم،

$$T^* = Th(\mathfrak{R}) \cup \{c_۱ > c_۲, c_۱ > c_۲ + c_۲, \ldots\}.$$

از قضیه فشردگی نتیجه می‌شود که T^* دارای مدل است زیرا هر بخش متناهی از آن مدل دارد و در واقع خود $\mathfrak{R}$ با تعبیر ثوابت جدید اضافه شده به زبان در آن، مدل هر بخش متناهی است. به طور دقیق‌تر، فرض کنیم $\Delta = \Delta_{\mathfrak{R}} \cup \{c_۱ > c_۲, c_۱ > c_۲ + c_۲, \ldots, c_۱ > \underbrace{c_۲ + \cdots + c_۲}_{N}\}$ زیر مجموعه متناهی از T است که $\Delta_{\mathfrak{R}} \subseteq Th(\mathfrak{R})$ (متناهی). ساختار $\mathfrak{M}_\Delta = (\mathbb{R}, +, \cdot, ۰, ۱, <, c_۱^{\mathfrak{M}_\Delta}, c_۲^{\mathfrak{M}_\Delta})$ که در آن $c_۱^{\mathfrak{M}_\Delta} = ۱۰$ و $c_۲^{\mathfrak{M}_\Delta} = ۱۰N + ۱$ مدل Δ است. بنابراین ساختار $\mathfrak{R}^*$ وجود دارد که $\mathfrak{R}^* \models T^*$ و $\mathfrak{R}^*$ تمام ویژگی‌های ساختار $\mathfrak{R}$ را دارد اما ارشمیدسی نیست. و از این نتیجه می‌شود که ارشمیدسی بودن یک میدان، جزو ویژگی‌های مرتبهٔ اول اعداد حقیقی نبوده است.

مثال ۳۱. هیچ فرمول $\varphi(v)$ در زبان نظریه گروه‌ها وجود ندارد که عناصر با مرتبه متناهی را تعریف کند. برای اثبات از قضیه فشردگی استفاده می‌کنیم. فرض کنید فرمول $\varphi(v)$ عناصر با مرتبهٔ متناهی را تعریف کند. در زبان $L = L_{group۱} \cup \{c\}$ تئوری

$$T^* = T_{group} \cup \{c + c \neq ۰, c + c + c \neq ۰, \ldots\} \cup \{\varphi(c)\}$$

را در نظر می‌گیریم. فرض کنیم

$$\Delta = T_{group} \cup \{c + c \neq ۰, \ldots, \underbrace{c + \cdots + c}_{N} \neq ۰\} \cup \{\varphi(c)\}$$

در این صورت این تئوری دارای مدل است (میدان‌های $\mathbb{Z}_p$ که $p > N$ و $\varphi(c)$ در آن‌ها برقرار است می‌توانند با تعبیر یک ثابت c مدلی برای Δ باشند.) بنابراین طبق قضیه فشردگی T^* دارای مدل است. اما در یک مدل تئوری T^* تعبیر ثابت c عنصری است که در فرمول φ صدق می‌کند ولی مرتبه‌اش نامتناهی است.

تمرین ۵. فرض کنیم $L = \{+, \cdot, <, ۰, ۱\}$. در این زبان $\mathfrak{N} = (\mathbb{N}, +, \cdot, <, ۰, ۱)$ یک ساختار است. نشان دهید که یک L-ساختار $\mathfrak{M}$ وجود دارد که $\mathfrak{M} \equiv \mathfrak{N}$ ولی $\mathfrak{M}$ دارای یک عدد است که از همه اعداد طبیعی بزرگتر است.

مثال ۳۲. در میدان‌ها کوچکترین عدد $n \in \mathbb{N}$ که اگر هر عضور ناصفر را n بار با خودش جمع کنیم حاصل صفر (عضو خنثی عمل جمع) شود را مشخصه می‌نامیم. نشان می‌دهیم اگر یک ویژگی مانند φ در میدان‌های بسته جبری با مشخصه متناهی به اندازه کافی بزرگ برقرار باشد آنگاه در یک میدان بسته جبری با مشخصه صفر نیز برقرار است.

بنابراین، فرض کنیم φ یک جمله در L_{ring} باشد. اگر T تئوری میدان‌های بسته جبری باشد (مثال ۲۷) آنگاه

$$T^* = T \cup \{۱ + ۱ \neq ۰, ۱ + ۱ + ۱ \neq ۰, \ldots\} \cup \{\varphi\}$$

تئوری میدان‌های بسته جبری با مشخصه صفر است که φ در آن‌ها برقرار است. هر بخش متناهی از این تئوری مانند

$$T^* = T \cup \{۱ + ۱ \neq ۰, \ldots, \underbrace{۱ + \cdots + ۱}_{N} \neq ۰\} \cup \{\varphi\}$$

دارای مدل است (یک میدان بسته جبری با مشخصه بیشتر از N یافت می‌شود که φ در آن برقرار است. F_p^{alg}ها می‌توانند مدلی برای Δ باشند). پس بر اساس قضیه فشردگی T^* دارای مدل است و φ در این مدل که یک میدان بسته جبری با مشخصه صفر است صدق می‌کند.

مثال ۳۳. فرض کنیم T یک تئوری در زبان L باشد که مدل‌های متناهی به اندازه دلخواه بزرگ دارد در این صورت T دارای مدل‌های نامتناهی با هر کاردینال دلخواه است. برای اثبات این موضوع از قضیه فشردگی استفاده می‌کنیم. فرض کنیم κ کاردینال دلخواه باشد. به زبان L به اندازه κ ثابت اضافه می‌کنیم. بنابراین $L' = L \cup \{c_\lambda \mid \lambda < \kappa\}$. بنا به قضیه فشردگی در این زبان تئوری $T' = T \cup \{c_\lambda \neq c_{\lambda'} \mid \lambda, \lambda' < \kappa\}$ دارای مدلی است که به اندازه κ عضو دارد (زیرا مطابق فرض هر زیرمجموعهٔ متناهی از T' دارای مدل است).

۷.۱ حذف سور

تعریف ۱۸. فرض کنیم $\mathfrak{M}$ یک L-ساختار با جهان M باشد و $A \subseteq M$. ساختار تولید شده توسط A در $\mathfrak{M}$ به صورت زیر است،

$$\langle A \rangle_{\mathfrak{M}} = \bigcap_{\substack{\mathfrak{N} \subseteq \mathfrak{M} \\ A \subseteq N}} \mathfrak{N} = \{t^{\mathfrak{M}}(a_۱, \ldots, a_n) \mid t(v_۱, \ldots, v_n) \in Term \ \& \ a_۱, \ldots, a_n \in A\}.$$

در بالا منظورمان از $Term$ مجموعهٔ همهٔ ترمها است.

تذکر ۸. اگر $\mathfrak{M}$ و $\mathfrak{N}$ دو L-ساختار باشند به طوری که $\mathfrak{M} \subseteq \mathfrak{N}$ و $\varphi(v_۱, \ldots, v_n)$ یک L-فرمول بدون سور باشد آنگاه برای هر $a_۱, \ldots, a_n \in M$،

$$\mathfrak{M} \models \varphi(a_۱, \ldots, a_n) \iff \mathfrak{N} \models \varphi(a_۱, \ldots, a_n).$$

اما اگر φ دارای سور باشد ممکن است چنین نباشد. برای مثال $(\mathbb{R}, +, \cdot, ۰, ۱) \subseteq (\mathbb{C}, +, \cdot, ۰, ۱)$، $(\mathbb{C}, +, \cdot, ۰, ۱) \models \exists x \ x^۲ + ۱$ اما $(\mathbb{R}, +, \cdot, ۰, ۱) \not\models \exists x \ x^۲ + ۱$.

برخی فرمول‌ها معادل بدون سور دارند. برای مثال فرمول $\varphi : \exists x \ ax^۲ + bx + c = ۰$ (وجود جواب برای معادله $ax^۲ + bx + c = ۰$) را می‌توان به صورت $\psi : (b^۲ - ۴ac \geq ۰) \vee (a = b = c \neq ۰)$ نمایش داد. همچنین شرط وجود جواب برای دستگاه $\begin{cases} a_۱x + a_۲y = c \\ a'_۱x + a'_۲y = c' \end{cases}$ این است که دترمینان ماتریس $\begin{bmatrix} a_۱ & a_۲ \\ a'_۱ & a'_۲ \end{bmatrix}$ مخالف صفر باشد. به عبارت دیگر

$$\exists x \ \exists y \ (a_۱x + a_۲y = c \ \wedge \ a'_۱x + a'_۲y = c') \iff a_۱a'_۲ - a_۲a'_۱ \neq ۰.$$

تذکر ۹. فرمول‌های بدون سور به شکل $\psi : (\beta_۱^۱ \wedge \cdots \wedge \beta_n^۱) \vee \cdots \vee (\beta_۱^m \wedge \cdots \wedge \beta_n^m)$ هستند که β_j^iها فرمول‌های اتمی یا نقیض اتمی هستند.

به طور کلی یک فرمول بدون سور یک دستگاه معادله است. مثال بعدی به طور دقیق‌تر این موضوع را نشان می‌دهد.

مثال ۳۴. در زبان L_{ring} فرمول‌های بدون سور از فصل یا عطف‌های فرمول‌های اتمی $f(x_1,\dots x_n)=g(x_1,\dots x_n)$ (و یا نقیض این فرمول‌ها) حاصل می‌شوند.

تعریف ۱۹. گوییم تئوری T حذف سور دارد (سورها را حذف می‌کند) هرگاه برای هر L-فرمول $\varphi(v_1,\dots v_n)$ یک L-فرمول بدون سور $\psi(v_1,\dots v_n)$ وجود داشته باشد که $T\models\varphi\longleftrightarrow\psi$. به بیان دیگر به طور هم زمان در همه مدل‌های T، φ و فرمول بدون سور ψ با هم معادل باشند.

برای مثال، تئوری میدان‌های بسته جبری با مشخصه صفر حذف سور دارد. این موضوع را پس از بیان مقدمات جبری درس اثبات خواهیم کرد.

تذکر ۱۰. فرض کنیم تئوری T برای فرمول‌های $\exists x\ \varphi(x,v_1,\dots,v_n)$ معادل بدون سور داشته باشد در این صورت T سورها را حذف می‌کند.

قضیه ۴. فرض کنیم $\varphi(v_1,\dots v_n)$ یک فرمول مرتبه اول باشد. این فرمول در تئوری T دارای یک معادل بدون سور است اگر و تنها اگر برای هر دو مدل $\mathfrak{M},\mathfrak{N}\models T$ و هر زیر ساختار مشترک $\mathfrak{A}\subseteq\mathfrak{M},\mathfrak{N}$ و هر چندتایی $a_1,\dots,a_n\in A$ داشته باشیم

$$\mathfrak{M}\models\varphi(a_1,\dots,a_n)\iff\mathfrak{N}\models\varphi(a_1,\dots,a_n).$$

اثبات. فرض کنیم فرمول $\varphi(v_1,\dots,v_n)$ دارای یک معادل بدون سور مانند $\psi(v_1,\dots,v_n)$ باشد، برای $\mathfrak{M}\models T$ و $a_1,\dots,a_n\in A$ داریم

$$\begin{aligned}\mathfrak{M}\models\varphi(a_1,\dots,a_n)&\iff\mathfrak{M}\models\psi(a_1,\dots,a_n)\\&\iff\mathfrak{A}\models\psi(a_1,\dots,a_n)\\&\iff\mathfrak{N}\models\psi(a_1,\dots,a_n)\\&\iff\mathfrak{N}\models\varphi(a_1,\dots,a_n).\end{aligned}$$

حال فرض کنیم برای هر $a_1,\dots,a_n\in A$، $\mathfrak{M}\models\varphi(a_1,\dots,a_n)\iff\mathfrak{N}\models\varphi(a_1,\dots,a_n)$. باید ثابت کنیم یک معادل بدون سور $\psi(v_1,\dots,v_n)$ موجود است که $T\models\varphi(v_1,\dots,v_n)\longleftrightarrow\psi(v_1,\dots,v_n)$. مجموعه زیر را در نظر می‌گیریم

$$\Gamma(v_1,\dots,v_n)=\{\psi(v_1,\dots,v_n)\mid\psi\in QF\ \&\ T\models\varphi(v_1,\dots,v_n)\longleftrightarrow\psi(v_1,\dots,v_n)\}$$

منظورمان از QF مجموعهٔ همهٔ فرمولهای بدون سور است. پس $\Gamma(v_1,\dots,v_n)$ در واقع مجموعه همه نتایج بدون سور فرمول φ نسبت به تئوری T است.

ادعا می‌کنیم $T\cup\Gamma(v_1,\dots,v_n)\models\varphi$. اگر این ادعا درست باشد آنگاه قضیه اثبات می‌شود. زیرا در این صورت بنا به قضیه فشردگی تعداد متناهی فرمول $\psi\in\Gamma$ وجود دارد که $T\cup\{\psi_1,\dots,\psi_k\}\models\varphi$. یعنی $T\cup\psi_1\wedge\dots\wedge\psi_k\models\varphi$ و

$$T\models\psi_1\wedge\dots\wedge\psi_k\longleftrightarrow\varphi.$$

بنابراین به اثبات ادعا می‌پردازیم. فرض کنیم $T\cup\Gamma(v_1,\dots,v_n)\not\models\varphi$ (برهان خلف)، در این صورت $T\cup\Gamma(v_1,\dots,v_n)\cup\{\neg\varphi\}$ دارای مدلی مانند $(\mathfrak{M},\bar{a})$ است. قرار می‌دهیم $\mathfrak{A}=\langle\overline{a}\rangle_{\mathfrak{M}}$. مجموعه همه فرمول‌های بدون سور که در $\mathfrak{A}$ برقرار هستند را $Diag(\mathfrak{A})$ می‌نامیم. اگر تئوری $T^*=Diag(\mathfrak{A})\cup T\cup\varphi(\overline{a})$ دارای مدلی مانند $\mathfrak{N}$ باشد آنگاه به تناقض می‌رسیم چون $\mathfrak{A}$ زیر ساختار مشترک $\mathfrak{M}$ و $\mathfrak{N}$ است و $\mathfrak{M}\models\neg\varphi$ و $\mathfrak{N}\models\varphi$. بنابراین برای پایان دادن به این اثبات کافی است ثابت کنیم T^* دارای مدل است. اگر چنین نباشد، آنگاه فرمول بدون سوری مانند $\chi(\overline{a})\in Diag(\mathfrak{A})$ وجود دارد که $T\models\varphi(\overline{a})\longrightarrow\neg\chi(\overline{a})$. بنابراین $\neg\chi\in\Gamma$ و $\mathfrak{M}\models\neg\chi$. از طرفی $\neg\chi$ عضوی از $Diag(\mathfrak{A})$ است و $\mathfrak{M}\models\chi$ که تناقض است. □

به عنوان یک کاربرد از قضیه بالا نتیجه زیر را بیان می‌کنیم.

نتیجه ۳. تئوری میدان‌های بسته جبری با مشخصه صفر کامل است. یعنی اگر T تئوری میدان‌های بسته جبری با مشخصه صفر باشد آنگاه برای هر جمله φ یا $T\models\varphi$ و یا $T\models\neg\varphi$.

صورت نتیجه را به این شکل نیز می‌توان معنا کرد که اگر φ جمله‌ای در زبان L_{ring} باشد یا φ به طور همزمان در همه میدان‌های بسته جبری با مشخصهٔ صفر درست و یا همزمان در همه میدان‌های بسته جبری با مشخصهٔ صفر غلط است! به بیان دیگر هر جمله‌ای که در میدان اعداد مختلط درست باشد، در همهٔ میدانهای بستهٔ جبری دیگر درست است. برای اثبات نتیجه از این تعبیر کمک می‌گیریم.

اثبات. فرض کنیم ساختارهای $\mathfrak{M}_1$ و $\mathfrak{M}_2$ دو میدان بسته جبری با مشخصه صفر باشند. هر میدان با مشخصه صفر شامل $\mathbb{Q}$ و در نتیجه شامل بستار جبری $\mathbb{Q}$ (به صورت $\mathbb{Q}^{ac}$ نمایش می‌دهیم) است. بنابراین $\mathfrak{M}_1$ و $\mathfrak{M}_2$ نیز شامل $\mathbb{Q}^{ac}$ هستند. بنا به قضیه قبل اگر φ جمله‌ای باشد که $\mathfrak{M}_1 \models \varphi$ آنگاه چون φ دارای معادل بدون سور است (میدان‌های بسته جبری حذف سور دارند!) بنابراین تحت زیر ساختارها حفظ می‌شود و $\mathbb{Q}^{ac} \models \varphi$ و از این رو $\mathfrak{M}_2 \models \varphi$. □

ترکیب نتیجهٔ بالا با مثال ۳۲ نشان می‌دهد که جملاتی در میدان اعداد مختلط برقرارند که در میدانهای بستهٔ جبری با مشخصهٔ متناهی به اندازهٔ کافی برقرار باشند.

تذکر ۱۱. اگر تئوری T سورها را حذف کند آنگاه هر مجموعه تعریف پذیر A با یک فرمول بدون سور تعریف می‌شود، یعنی A ترکیب بولی از مجموعه جواب معادلات مختلف است.

همانطور که گفتیم ثابت می‌کنیم تئوری میدان‌های بسته جبری سورها را حذف می‌کند بنابراین اگر $\mathfrak{K} = (K, +, \cdot, ۰, ۱)$ یک میدان بسته جبری باشد و $A \subseteq K^n$ یک مجموعه تعریف پذیر باشد آنگاه A یک مجموعه ساخته شدنی است. یعنی ترکیب بولی از مجموعه‌های بسته زاریسکی است (مجموعه بسته زاریسکی همان مجموعه جواب‌های یک دستگاه معادله است).

گزاره ۳ (قضیهٔ شوالی). فرض کنیم $\mathfrak{K} = (K, +, \cdot, ۰, ۱)$ یک میدان بسته جبری باشد. اگر $A \subseteq K^{n+m}$ یک مجموعه ساخته شدنی باشد آنگاه تصویر A روی K^n نیز یک مجموعه ساخته شدنی است.

اثبات. A ساخته شدنی است بنابراین تعریف پذیر است یعنی برای هر $\overline{x} = (x_1, \ldots, x_n) \in K^n$ و $\overline{y} = (y_1, \ldots, y_m) \in K^m$ داریم

$$A = \{(\overline{x}, \overline{y}) \mid \mathfrak{K} \models \varphi(\overline{x}, \overline{y})\}.$$

تابع تصویر $\pi : K^{n+m} \longrightarrow K^n$ را اثر می‌دهیم،

$$A = \{\overline{x} \mid \mathfrak{K} \models \exists \overline{y} \ \varphi(\overline{x}, \overline{y})\}.$$

فرمول $\exists \overline{y} \ \varphi(\overline{x}, \overline{y})$ دارای معادل بدون سور مانند $\psi(\overline{x}, \overline{y})$ است. بنابراین $A = \{\overline{x} \mid \mathfrak{K} \models \psi(\overline{x}, \overline{y})\}$ یک مجموعه ساخته شدنی است. □

از گزاره بالا نتیجه می‌گیریم که کلاس مجموعه‌های ساخته شدنی علاوه بر ترکیبات بولی، تحت تصویرگیری هم بسته است. دقت کنید که اثبات این قضیه با تکنیک‌های جبری، به این سادگی نیست!

فصل ۲

مقدمات جبری

تدریس: محمود بهبودی
گردآوری: فاطمهٔ اکبری

برای ادامه درس لازم است به بیان برخی تعاریف و قضایای جبری مورد نیاز بپردازیم. برای اطلاع از جزئیات بیشتر (مثال و اثبات قضایا) می‌توانید به جزوه جبر ۲ مراجعه کنید. لازم به ذکر است که به دلیل تکرار تعاریف حلقه (جا به جایی و یکدار) و میدان در جلسات گذشته در ادامه از بیان این تعاریف خودداری می‌کنیم.

۱.۲ یادآوری تعاریف و قضایای مقدماتی

تعریف ۲۰. در یک حلقه دلخواه مانند R، عنصر $a \in R$ دارای وارون راست (چپ) است اگر $b \in R$ وجود داشته باشد به طوری که $a \cdot b = 1_R$ $(b \cdot a = 1_R)$. همچنین اگر a دارای وارون راست و چپ باشد که با هم برابر باشند آنگاه گوییم a وارون پذیر است. مجموعه همه عناصر وارون پذیر R را با $U(R)$ نمایش می‌دهیم. حلقه یکدار R که هر عنصر ناصفر آن وارون داشته باشد را حلقه تقسیم می‌نامیم. اگر R یک حلقه باشد، $S \subset R$ را زیر حلقه می‌نامیم هرگاه S با همان اعمال معرفی شده روی R خود یک حلقه باشد.

تذکر ۱۲. اگر حلقه R یکدار باشد آنگاه معمولا زیر حلقه S را نیز یکدار در نظر می‌گیریم. توجه داشته باشیم که $1_S = 1_R$.

تذکر ۱۳. هر حلقه دلخواه در یک حلقه یکدار می‌نشیند، لذا معمولا به طور پیش فرض حلقه را یکدار در نظر می‌گیریم. به عنوان تمرین نشان دهید هر حلقه غیر یکدار زیر حلقه یک حلقه یک حلقه یکدار است. (راهنمایی: برای حلقه دلخواه R، اعمال جمع و ضرب را به گونه‌ای روی $R \times \mathbb{Z}$ تعریف کنید که یک حلقه باشد و $R \subseteq R \times \mathbb{Z}$.)

تعریف ۲۱. 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 a عنصری در R باشد آنگاه ایده‌آل تولید شده توسط a را با $\langle a \rangle$ نمایش می‌دهیم و آن را کوچکترین ایده‌آلی که شامل a است تعریف می‌کنیم. در این صورت اگر R جا به جایی و یکدار باشد آنگاه $\langle a \rangle = \{ra \mid r \in R\}$ اما اگر R یکدار نباشد آنگاه خود a در $\langle a \rangle$ وجود ندارد و بنابراین تعریف می‌کنیم $\langle a \rangle = \{na + ra \mid n \in \mathbb{Z},\ r \in R\}$.

فرض کنیم R یک حلقه باشد و $I \trianglelefteq R$. مجموعه $\{r + I \mid r \in R\}$ با اعمال

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

یک حلقه است. این حلقه را به صورت $\frac{R}{I}$ نمایش می‌دهیم و آن را حلقه خارج قسمتی می‌نامیم.

تعریف ۲۲. در حلقه R، $P \trianglelefteq R$ را ایده‌آل اول گوییم هرگاه P سره نباشد ($P \neq R$) و برای هر دو عنصر a و b در R اگر $ab \in P$ آنگاه یا $a \in P$ و یا $b \in P$.

در حلقه R ایده‌آل ناسره M را ایده‌آل ماکسیمال گوییم هرگاه هیچ ایده‌آلی بین M و R نباشد.

تمرین ۶.

- ثابت کنید در حلقه‌های یکدار هر ایده‌آلی زیر مجموعه یک ایده‌آل ماکسیمال است. (با استفاده از لم زرن به این سوال پاسخ دهید. همچنین به این سوال نیز فکر کنید که آیا ایده‌آل ماکزیمال یکتاست).

تعریف ۲۳. نگاشت $f : R \longrightarrow R'$ که R و R' حلقه هستند را در نظر می‌گیریم. اگر این نگاشت حافظ اعمال میان حلقه‌ها باشد آن را همریختی بین حلقه‌ها می‌نامیم. اگر این همریختی یک به یک باشد تک ریختی و اگر پوشا باشد آن را برون ریختی می‌نامیم. در صورتی که هم یک به یک و هم پوشا باشد به آن یکریختی بین حلقه‌های R و R' گوییم. اگر f یکریختی باشد آنگاه R و R' یکریخت هستند و آن را به صورت $R \cong R'$ نمایش می‌دهیم.

اگر $f : R \longrightarrow R'$ یک همریختی باشد، هسته f به صورت زیر تعریف می‌شود،

$$Ker(f) = \{x \in R \mid \ f(x) = o_{R'}\}.$$

هسته f یک ایده‌آل در R است.

قضیه ۵. (قضیه اول یکریختی). اگر $f : R \longrightarrow R'$ یک همریختی باشد آنگاه $\frac{R}{Ker(f)} \cong Im(f)$. پس اگر f پوشا باشد آنگاه $\frac{R}{Ker(f)} \cong R'$.

تعریف ۲۴. یکریختی $f : R \longrightarrow R$ را خود ریختی می‌نامیم.

تعریف ۲۵. حلقه جا به جایی R یک دامنه صحیح است هرگاه ضرب دو عنصر ناصفر آن صفر نباشد.

تذکر ۱۴. اگر R دامنه جا به جایی و یکدار باشد نگاشت $\psi : \mathbb{Z} \longrightarrow R$ با ضابطه

$$\psi(n) = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n} & n > 0 \\ 0 & n = 0 \\ -\underbrace{(1_R + \cdots + 1_R)}_{-n} & n < 0 \end{cases}$$

یک همریختی بین حلقه‌ها است. هسته ψ در $\mathbb{Z}$ یک ایده‌آل است و چون $\mathbb{Z}$، PID است داریم $Ker(\mathbb{Z}) = \langle c \rangle$. عدد صحیح c را مشخصه حلقه R می‌نامیم. ثابت می‌شود که (در صورت وجود) c کوچکترین عددی است که $\underbrace{1_R + \cdots + 1_R}_{c} = 0_R$.

تذکر ۱۵. هر دامنه صحیح جا به جایی و یکدار شامل یک زیر حلقه‌ای است که یا با $\mathbb{Z}$ یکریخت است و یا با $\mathbb{Z}_p$ به طوری که p یک عدد اول است.

تذکر ۱۶. هر میدان شامل زیر میدانی است که یا با $\mathbb{Q}$ یکریخت است و یا با $\mathbb{Z}_p$ به طوری که p یک عدد اول است.

تعریف ۲۶.

- عنصر ناصفر $r \in R$ را تحویل ناپذیر گوییم هرگاه $r \notin U(R)$ و اگر $r = ab$ آنگاه $a \in U(R)$ یا $b \in U(R)$.
- عنصر ناصفر $r \in R$ را اول گوییم هرگاه $r \notin U(R)$ و اگر $r \mid ab$ آنگاه $r \mid a$ یا $r \mid b$.

تعریف ۲۷. مجموعه همه چندجمله‌ای‌ها تک متغیره که ضرایب آن‌ها متعلق به حلقه R است را با $R[x]$ نمایش می‌دهیم. اعضای $R[x]$ به صورت $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ هستند. n را درجه و a_n را ضریب پیشرو $f(x)$ می‌نامیم.

قضیه ۶. عنصر ناصفر $f(x)$ را در $K[x]$ در نظر می‌گیریم به طوری که K یک میدان باشد. در این صورت موارد زیر با هم معادل هستند.

۱) $\langle f(x) \rangle$ یک ایده‌آل ماکسیمال است.

۲) $\langle f(x) \rangle$ یک ایده‌آل اول است.

۳) $f(x)$ در $K[x]$ اول است.

۴) $f(x)$ در $K[x]$ تحویل ناپذیر است.

تذکر ۱۷. تنها عناصر وارون پذیر $K[x]$ اعضای K هستند. به عبارت دیگر $U(K[x]) = K$.

قضیه ۷. فرض کنیم $g(x)$ یک چندجمله‌ای ناصفر در $K[x]$ باشد. برای هر $f(x) \in K[x]$، چندجمله‌ای‌های یکتای $q(x)$ و $r(x)$ متعلق به $K[x]$ وجود دارند به طوری که $f(x) = q(x)g(x) + r(x)$ که در آن یا $r(x) = 0$ و یا درجه $r(x)$ از $g(x)$ اکیدا کمتر باشد.

تعریف ۲۸. اگر D یک دامنه صحیح باشد آنگاه میدان $F = \{\frac{a}{b} \mid a, b \in D,\ b \neq 0\}$ را میدان کسرهای D می‌نامیم.

در ادامه دو محک برای تشخیص تحویل‌ناپذیری چندجمله‌ایها روی اعداد گویا ارائه کرده‌ایم (اولی لم گاوس و دومی محک آیزن‌اشتاین نام دارد).

قضیه ۸. فرض کنیم $f(x) \in \mathbb{Z}(x)$ به گونه‌ای باشد که عدد اول p ضریب پیشروی آن را عاد نکند. در این صورت اگر $\overline{f}(x) \in \mathbb{Z}_p[x]$ در $\mathbb{Z}_p[x]$ تحویل ناپذیر باشد آنگاه $f(x)$ در $\mathbb{Q}[x]$ هم تحویل ناپذیر است.

قضیه ۹. اگر $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ باشد و p عدد اولی باشد که برای $1 \leq i \leq n-1$ داشته باشیم $p \mid a_i$ و همچنین $p \nmid a_n$ و $p^2 \nmid a_0$ آنگاه $f(x)$ در $\mathbb{Q}[x]$ تحویل ناپذیر است.

نتیجه ۴. (تعمیم محک آیزنشتاین). اگر F میدان کسرهای دامنه تجزیه یکتای D باشد در این صورت اگر $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$ یک چندجمله‌ای اولیه غیر ثابت باشد و $p \in D$ عنصری تحویل ناپذیر باشد که $p \nmid a_n$ و $p^2 \nmid a_0$ آنگاه $f(x)$ در $F[x]$ تحویل ناپذیر است.

۲.۲ تعریف توسیع‌های میدانی

تعریف ۲۹. اگر K و F دو میدان باشند و $\alpha : K \longrightarrow F$ یک تکریختی میدان‌ها باشد آنگاه (F, α) (به اختصار F) را توسیع میدان K می‌نامیم.

برای مثال $\mathbb{R}$ توسیع میدان $\mathbb{Q}$ است و $\mathbb{C}$ توسیع میدان $\mathbb{R}$ است.

تعریف ۳۰. اگر K، E و F میدان باشند به طوری که $K \leq E \leq F$ (منظور از این علامت گذاری این است که E توسیعی از K و F توسیعی از E است.) آنگاه E را توسیع میانی F روی K می‌نامیم.

گزاره ۴. اگر مشخصه میدان F صفر باشد آنگاه F توسیعی از میدان $\mathbb{Q}$ است.

اثبات. تکریختی $\alpha : \mathbb{Z} \longrightarrow F$ را با ضابطه $\alpha(n) = \underbrace{1_F + \cdots + 1_F}_{n}$ در نظر می‌گیریم. به کمک α نگاشت $\alpha' : \mathbb{Q} \longrightarrow F$ را با ضابطه $\alpha'(\frac{m}{n}) = \alpha(m)\alpha(n)^{-1}$ معرفی می‌کنیم. α' تکریختی است و بنابراین (F, α') توسیعی از $\mathbb{Q}$ است. □

۳.۲ یافتن ریشه برای چندجمله‌ایها در توسیعهای میدانی

قضیه ۱۰. اگر K یک میدان و $p(x) \in K[x]$ تحویل ناپذیر باشد آنگاه $E = \frac{K[x]}{\langle p(x) \rangle}$ (حلقه تقسیم بر ایده‌آل ماکسیمال) یک توسیع از K است و به علاوه $p(x)$ در E دارای ریشه است، یعنی در E تجزیه می‌شود.

اثبات. نگاشت $\alpha : K \longrightarrow \frac{K[x]}{\langle p(x)\rangle}$ با ضابطه $\alpha(a) = a + \langle p(x)\rangle$ یکریختی است. بنابراین $E = \frac{K[x]}{\langle p(x)\rangle}$ یک توسیع از K است. حال ثابت می‌کنیم $p(x)$ در E ریشه دارای ریشه $u = x + \langle p(x)\rangle$ است. داریم

$$p(u) = p(x + \langle p(x)\rangle) = p(x) + \langle p(x)\rangle$$

چون $p(x) \in \langle p(x)\rangle$ آنگاه $p(u) = \langle p(x)\rangle$ که $\langle p(x)\rangle$ همان صفر میدان E است. بنابراین u ریشه $p(x)$ در E است. □

سعی داریم در مثال زیر به یکی از معروف‌ترین توسیع میدان‌ها از چند منظر متفاوت نگاه کنیم.

مثال ۳۵. چندجمله‌ای $x^۲ + ۱ \in \mathbb{R}[x]$ در $\mathbb{R}$ تحویل ناپذیر است. بنا به قضیه قبل $E = \frac{\mathbb{R}[x]}{\langle x^۲ + ۱\rangle}$ توسیع میدان $\mathbb{R}$ است. این میدان همان میدان اعداد مختلط یعنی $\mathbb{C}$ است.

۱) می‌دانیم $\frac{\mathbb{R}[x]}{\langle x^۲ + ۱\rangle} = \{f(x) + \langle x^۲ + ۱\rangle \mid f(x) \in \mathbb{R}[x]\}$. بنا به قضیه تقسیم باقی مانده تقسیم هر $f(x)$ به $x^۲ + ۱$ چندجمله‌ای درجه به صورت $r(x) = a + bx$ است (یعنی درجه $r(x)$ یا صفر است و یا یک). از آنجایی که $f(x) - r(x) \in \langle x^۲ + ۱\rangle$ داریم $f(x) + \langle x^۲ + ۱\rangle = r(x) + \langle x^۲ + ۱\rangle$ و این یعنی توسیع میدان $\mathbb{R}$ به صورت زیر است،

$$\mathbb{C} = \{a + bx + \langle x^۲ + ۱\rangle \mid a, b \in \mathbb{R}\}.$$

لازم به ذکر است که بنا به قضیه قبل ریشه $x^۲ + ۱$ در $\mathbb{C}$ برابر $x + \langle x^۲ + ۱\rangle$ است.

۲) از زاویه‌ای دیگر $\mathbb{C} = \frac{\mathbb{R}[x]}{\langle x^۲ + ۱\rangle}$ مجموعه همه چندجمله‌ای‌های متعلق به $\mathbb{R}[x]$ با شرط $x^۲ + ۱ = ۰$ است. این تساوی به این معنی است که $x^۲ = -۱$، پس می‌توانیم در چندجمله‌ای‌های دیگر به جای $x^۲$، قرار دهیم -۱. برای مثال $x^۳$ را می‌توان همان $-x$ در نظر گرفت. بنابراین توان‌هایی بالاتر از توان یک نداریم و این یعنی

$$\mathbb{C} = \{a + bx + \langle x^۲ + ۱\rangle \mid a, b \in \mathbb{R}\}.$$

۳) می‌خواهیم بدانیم شناسایی اعضای $\mathbb{C}$ در مورد یک و دو چه رابطه‌ای با میدان مختلطی که با آن آشنا هستیم دارد؟ بنا به دو مورد قبل،

$$\begin{aligned}\mathbb{C} &= \{a + bx + \langle x^۲ + ۱\rangle \mid a, b \in \mathbb{R}\} \\ &= \{(a + \langle x^۲ + ۱\rangle) + (b + \langle x^۲ + ۱\rangle)(x + \langle x^۲ + ۱\rangle) + \langle x^۲ + ۱\rangle \mid a, b \in \mathbb{R}\}\end{aligned}$$

قرار می‌دهیم $a' = (a + \langle x^۲ + ۱\rangle)$، $b' = (b + \langle x^۲ + ۱\rangle)$ و $i = x + \langle x^۲ + ۱\rangle$. بنابراین اعضای $\mathbb{C}$ به صورت $a' + b'i$ هستند که $i = \sqrt{-۱}$ زیرا

$$\begin{aligned}i^۲ = (x + \langle x^۲ + ۱\rangle)^۲ &= x^۲ + \langle x^۲ + ۱\rangle \\ &= -۱ + x^۲ + ۱ + \langle x^۲ + ۱\rangle \\ &= -۱ + \langle x^۲ + ۱\rangle \\ &= -۱ \mod \langle x^۲ + ۱\rangle\end{aligned}$$

۴) فرض کنیم $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i^۲ = -۱\}$. نگاشت $\psi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ با ضابطه $\psi(f(x)) = f(i)$ یک همریختی است. می‌دانیم $Ker(\psi) \trianglelefteq \mathbb{R}[x]$. از آنجایی که $\mathbb{R}[x]$ دامنه ایده‌آل اصلی است، نتیجه می‌گیریم $Ker(\psi)$ تنها با یک عنصر تولید می‌شود. به سادگی ثابت می‌شود که $Ker(\psi) = \langle x^۲ + ۱\rangle$. بنا به قضیه یکریختی $\frac{\mathbb{R}[x]}{\langle x^۲ + ۱\rangle} \cong \mathbb{C}$.

تذکر ۱۸. فرض کنیم K یک میدان و $f(x)$ در $k[x]$ تحویل ناپذیر باشد. یک توسیع از K مانند $E_۱$ را می‌یابیم که $f(x)$ حداقل یک ریشه داشته باشد. فرض کنیم $\alpha_۱, \ldots, \alpha_t$ ریشه‌های $f(x)$ در $E_۱$ باشند. بنابراین می‌توان نوشت

$$f(x) = (x - \alpha_۱) \cdots (x - \alpha_t) f_۱(x) \cdots f_k(x)$$

به طوری که برای هر $1 \leq i \leq k$، $f_i(x)$ در E_1 تحویل ناپذیر است. بنابراین توسیعی برای E_1 می‌یابیم که $f_1(x)$ در آن ریشه داشته باشد. به همین صورت می‌توانیم توسیعی برای K بیابیم که همه ریشه‌های $f(x)$ در آن وجود داشته باشد.

تذکر ۱۹. فرض کنیم F یک توسیع میدان K باشد و $S \subseteq F$. اشتراک تمام زیرمیدان‌های F که شامل $S \cup K$ هستند را با $K_F(S)$ نشان می‌دهیم. همچنین کوچکترین زیر حلقه F که شامل S و K است را به صورت $K_F[S]$ نمایش می‌دهیم. در حالت کلی $K_F[S] \subseteq K_F(S)$.

لازم به ذکر است که منظور از $K[U,V]$ همان $K[U][V]$ است. به همین صورت $K(U,V) = K(U)(V)$.

مثال ۳۶. چندجمله‌ای $x^3 + x^2 + 1 = 0$ در $\mathbb{Q}[x]$ تحویل ناپذیر است. بنابراین

$$\frac{\mathbb{Q}[x]}{\langle x^3 + x^2 + 1 \rangle} = \{a + bx + cx^2 \mid a, b, c \in \mathbb{Q},\ x^3 = -x^2 - 1\}.$$

اگر قرار دهیم $\omega = \sqrt[3]{3}$ آنگاه مطابق مورد ۴ در مثال قبل، همریختی وجود دارد که $\frac{\mathbb{Q}[x]}{\langle x^3 + x^2 + 1 \rangle} \cong \mathbb{Q}[\omega]$. از تذکر ۱۹ داریم $\mathbb{Q}[\omega]$ کوچکترین زیر حلقه $\mathbb{R}$ است که شامل $\mathbb{Q}$ و ω است. همچنین $\mathbb{Q}(\omega)$ اشتراک تمام زیر میدان‌های $\mathbb{R}$ است که شامل $\mathbb{Q}$ و ω است. واضح است که $\mathbb{Q}[\omega] \subseteq \mathbb{Q}(\omega)$. از آنجایی که $\frac{\mathbb{Q}[x]}{\langle x^3 + x^2 + 1 \rangle} \cong \mathbb{Q}[\omega]$ پس $\mathbb{Q}[\omega]$ میدان است و این یعنی $\mathbb{Q}(\omega) \subseteq \mathbb{Q}[\omega]$. بنابراین در این حالت $\mathbb{Q}(\omega) = \mathbb{Q}[\omega]$.

تذکر ۲۰. در حالت کلی $\mathbb{Q}[x]$ میدان نیست زیرا x وارون ندارد.

تذکر ۲۱. بین دو میدان $\mathbb{Q}$ و $\mathbb{R}$ بی‌نهایت میدان مانند $\mathbb{Q}[\omega]$ وجود دارد.

تذکر ۲۲. با آنچه تا اینجا آموخته‌ایم می‌توانیم میدان‌های p^n عضوی بسازیم به طوری که p یک عدد اول و n یک عدد طبیعی است. برای مثال اگر بخواهیم یک میدان $2^2 = 4$ عضوی بسازیم چندجمله‌ای تحویل ناپذیری با توان دو را در $\mathbb{Z}_2[x]$ میابیم. مانند $f(x) = x^2 + x + 1$. بنابراین میدان $\frac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1 \rangle}$ به صورت

$$\frac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1 \rangle} = \{a + bx + \langle x^2 + x + 1 \rangle \mid a, b \in \mathbb{Z}_2[x]\}$$

۴ عضوی است. به طور کلی، اگرچه میدان‌های متناهی ممکن است به شکل‌های متفاوتی باشند اما چیزی به جز فاکتورهای $\mathbb{Z}_p[x]$ نیستند. به عبارت دیگر هر میدان متناهی F که $|F| = p^n$ با $\frac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}$ که $f(x)$ یک چندجمله‌ای تحویل ناپذیر از درجه n است، یکریخت است.

۴.۲ توسیعهای میدانی به عنوان فضاهای برداری

تعریف ۳۱. اگر F یک توسیع برای میدان K باشد و $\alpha : K \longrightarrow F$ تکریختی باشد آنگاه $(F, +)$ یک K-فضای برداری با ضرب اسکالر $K \times F \longrightarrow F$ به صورت $(k, f) \longrightarrow \alpha(k)f$ است. اگر K زیر میدان F باشد، ضرب اسکالر به صورت $(k, f) \longrightarrow kf$ تعریف می‌شود.

مثال ۳۷. هر میدان F یک F-فضای برداری است. $\mathbb{C}$ یک $\mathbb{R}$-فضای برداری است. همچنین $\mathbb{R}$ و $\mathbb{C}$ هر دو $\mathbb{Q}$-فضای برداری هستند.

مثال ۳۸. فرض کنیم K یک میدان و $f(x) \in K[x]$ یک چندجمله‌ای تحویل ناپذیر باشد. از میدان $F = \frac{K[x]}{\langle f(x) \rangle}$ و تکریختی $\alpha : K \longrightarrow F$ با ضابطه $\alpha(k) = k + \langle f(x) \rangle$ نتیجه می‌گیریم F یک K-فضای برداری است. همانطور که گفتیم اگر $p(x)$ یک چندجمله‌ای تحویل ناپذیر در $K[x]$ باشد آنگاه میدان توسیع K، یعنی $\frac{K[x]}{\langle p(x) \rangle}$ یک K-فضای برداری است. بنابراین لازم است به بررسی این توسیع از این منظر بپردازیم. به عنوان یک مقدمه از مباحث پیش رو می‌توانیم به تفاوت دو مبحث استقلال خطی و استقلال جبری اشاره کنیم. در واقع استقلال خطی با همان تعریف آشنا در جبر خطی در مقابل تعریف استقلال جبری قرار می‌گیرد که هر کدام بعدی جداگانه را روی فضاهای مورد بررسی معرفی می‌کنند. در ابتدا و در قضیه زیر به ارتباط میان بعد میدان توسیع K و درجه چدجمله‌ای $p(x)$ می‌پردازیم.

قضیه ۱۱. فرض کنیم E توسیع میدان K و $p(x) \in K[x]$ یک چندجمله‌ای از درجه n و تحویل ناپذیر در $K[x]$ باشد. اگر $u \in E$ ریشه $p(x)$ باشد آنگاه

$$K(u) = K[u] \cong \frac{K[x]}{\langle p(x) \rangle}$$

و $\{۱, u, u^۲, \ldots, u^{n-۱}\}$ یک پایه برای $K[u]$ روی K است. به عبارت دیگر

$$K[u] = \{\sum_{i=۰}^{n-۱} k_i u^i \mid k_i \in K\}.$$

اثبات. اگر ثابت شود $K[u] \cong \frac{K[x]}{\langle p(x)\rangle}$ آنگاه واضح است که $K(u) = K[u]$. به عنوان تمرین ثابت کنید نگاشت $\varphi : K[x] \longrightarrow K[u]$ با ضابطه $\varphi(f(x)) = f(u)$ یکریختی است و $Ker(\varphi) = \langle p(x)\rangle$. □

تعریف ۳۲. اگر E توسیع میدان K باشد آنگاه $\dim_K E$ را با $[E : K]$ نمایش داده و آن را درجه توسیع E روی K می‌نامیم. همچنین اگر $[E : K]$ متناهی باشد، گوییم E توسیع متناهی است.

مثال ۳۹. $p(x) = x^۴ + x + ۱$ روی $\mathbb{Z}_۲[x]$ تحویل ناپذیر است. فرض کنیم $E = \frac{\mathbb{Z}_۲[x]}{\langle p(x)\rangle}$. $u + \langle p(x)\rangle \in E$ یک ریشه برای $p(x)$ در میدان E است. بنابراین طبق قضیه قبل

$$\mathbb{Z}_۲[x] = \{a_۳u^۳ + a_۲u^۲ + a_۱u + a_۰ \mid a_۰, a_۱, a_۲, a_۳ \in \mathbb{Z}_۲\}.$$

به عبارت دیگر $\{۱, u, u^۲, u^۳\}$ یک پایه برای E است و $[E : K] = ۴$.

تعریف ۳۳. اگر E یک توسیع برای میدان K باشد و $S = \{a_۱, \ldots, a_n\} \subseteq E$ به گونه‌ای باشد که $K(S) = E$ آنگاه E را توسیع متناهیا تولید شده روی K می‌نامیم. برای یک عنصر u در E اگر $K(u) = E$، گوییم E توسیع ساده است.

مثال ۴۰. اگر میدان را $\mathbb{Q}$ در نظر بگیریم آنگاه $\mathbb{Q}(e)$ (e عدد نپر) یک توسیع ساده برای $\mathbb{Q}$ است (در واقع بعد جبری $\mathbb{Q}$ یک است). از آنجایی که مجموعه $B = \{۱, e, e^۲, \ldots\}$ یک مجموعه مستقل خطی است نتیجه می‌گیریم $[\mathbb{Q}(e) : \mathbb{Q}] = \infty$.

بنا به آنچه گفته شد اگر u ریشه یک چندجمله‌ای تحویل ناپذیر $p(x) \in K[x]$ باشد آنگاه درجه توسیع $K[u] = \frac{K[x]}{\langle p(x)\rangle}$ برابر با درجه چندجمله‌ای $p(x)$ است. این در حالی است که بعد جبری $K[u]$ یک است. در واقع $K[u]$ توسط یک عنصر تولید می‌شود.

قضیه ۱۲. فرض کنیم E توسیع میدان K باشد و $a_۱, \ldots, a_n \in E$. در این صورت میدان کسرهای $K(a_۱, \ldots, a_n)$ برابر است با $K[a_۱, \ldots, a_n]$.

اثبات. واضح است که $K[a_۱, \ldots, a_n] \subseteq K(a_۱, \ldots, a_n)$. از طرفی، همه میدان‌ها شامل میدان کسرها هستند و بنابراین

$$K(a_۱, \ldots, a_n) \subseteq K[a_۱, \ldots, a_n].$$

□

تعریف ۳۴. دو حلقه R و S را در نظر می‌گیریم به طوری که شامل میدان K باشند. اگر در همریختی $\varphi : R \longrightarrow S$ برای هر $k \in K$، داشته باشیم $\varphi(k) = k$ آنگاه φ را K-همریختی می‌نامیم. اگر φ دو سویی باشد گوییم φ، K-یکریختی است.

مقدار دهی یک چندجمله‌ای مفهوم ساده‌ای است که با آن آشنا هستیم اما به طور دقیق می‌توانیم آن را به این صورت تعریف کنیم: اگر R یک حلقه شامل میدان K باشد و $f(x) = \sum_{i=۱}^n a_i x^i \in K[x]$ آنگاه برای هر عنصر $r \in R$ عبارت $\sum_{i=۱}^n a_i r^i \in R$ را مقدار (ارزش) چندجمله‌ای $f(x)$ در نقطه r گوییم.

قضیه ۱۳. فرض کنیم حلقه R شامل میدان K باشد. برای $r \in R$، K-همریختی یکتای $\varphi_r : K[x] \longrightarrow R$ وجود دارد به طوری که $\varphi_r(x) = r$.

اثبات. قرار می‌دهیم $\varphi_r(f(x)) = f(r)$ (هر نگاشت با این ضابطه را نگاشت مقدار دهی گوییم). φ_r همریختی است. ثابت می‌کنیم یکتاست. اگر $\psi : K[x] \longrightarrow R$ یک همریختی باشد به طوری که $\psi(x) = r$ آنگاه برای هر $f(x) = \sum_{i=۱}^n a_i x^i \in K[x]$ بنا به همریختی ψ داریم

$$\psi(f(x)) = \sum_{i=۱}^n a_i r^i = f(r) = \varphi_r(f(x)).$$

□

قضیه ۱۴. اگر K-همریختی $\varphi_r : K[x] \longrightarrow R$ یک نگاشت مقدار دهی بین دو حلقه $K[x]$ و R و R دامنه صحیح باشد، آنگاه یکی از دو حالت زیر رخ می‌دهد؛

۱) φ_r یک به یک است. در این صورت طبق قضیه اول یکریختی داریم $K[x] \cong K[r] \leq R$.

۲) φ_r یک به یک نیست. در این صورت چندجمله‌ای تحویل ناپذیر $p(x) \in K[x]$ وجود دارد که $Ker(\varphi) = \langle p(x) \rangle$. بنابراین $K[r]$ یک میدان است و $p(r) = 0$. همچنین برای هر $g(x) \in K[x]$ داریم

$$g(r) = 0 \iff p(x) \mid g(x). \tag{۱.۲}$$

اثبات. برای اثبات تنها باید ثابت کنیم $p(x)$ تحویل ناپذیر و (۱.۲) برقرار است. چون $\langle p(x) \rangle$ یک ایده‌آل اول است نتیجه می‌گیریم $p(x)$ تحویل ناپذیر است. اگر $g(r) = 0$ آنگاه $g(x) \in \langle p(x) \rangle$ و این یعنی $p(x) \mid g(x)$. برعکس، اگر $p(x) \mid g(x)$ آنگاه $q(x) \neq 0$ وجود دارد که $g(x) = q(x) \cdot p(x)$ و $g(r) = q(r)p(r) = q(x) \cdot 0 = 0$. □

به طور خلاصه، قضیه قبل به این موضوع اشاره دارد که تصویر φ_r یا با $K[x]$ ایزومرف است و یا با $\frac{K[x]}{\langle p(x) \rangle}$ که $p(x)$ یک چندجمله‌ای تحویل ناپذیر است. به کمک قضیه بالا عنصر متعالی و جبری را به صورت زیر تعریف می‌کنیم.

۵.۲ توسیعهای جبری و متعالی

تعریف ۳۵. اگر E توسیع میدان K باشد آنگاه $\alpha \in E$ روی میدان K متعالی است اگر ریشه هیچ چندجمله‌ای ناصفر در $K[x]$ نباشد. همچنین گوییم $\omega \in E$ روی میدان K جبری است اگر ω ریشه یک چندجمله‌ای ناصفر مانند $p(x) \in K[x]$ باشد.

نتیجه ۵. فرض کنیم E توسیع میدان K و $\omega \in E$ روی K جبری باشد. در این صورت یک چندجمله‌ای تکین تحویل ناپذیر و یکتای $p(x) \in K[x]$ موجود است که $p(\omega) = 0$ و همریختی $\psi_\omega : \frac{K[x]}{\langle p(x) \rangle} \longrightarrow K[\omega]$ با ضابطه $\psi_\omega(f(x) + \langle p(x) \rangle) = f(\omega)$ یک یکریختی است. چندجمله‌ای $p(x)$ را چندجمله‌ای مینیمال ω روی K می‌نامیم.

نتیجه ۶. اگر ω روی K جبری باشد آنگاه بعد میدان $[K(\omega) : K]$ برابر با درجه چندجمله‌ای مینیمال ω روی K است.

تمرین ۷. با فرض نمادگذاری‌های نتیجه ۵، نشان دهید که چندجمله‌ای مینیمال ω روی K یک چندجمله‌ای با حداقل درجه در $K[x]$ است که ω ریشه آن است و برعکس.

تعریف ۳۶. توسیع E روی میدان K را جبری نامیم هرگاه هر عنصر $\omega \in E$ روی K جبری باشد.

قضیه ۱۵. هر توسیع متناهی، جبری است.

اثبات. فرض کنیم E توسیع متناهی روی K باشد. یعنی $[E : K] = n$. فرض کنیم عنصر $\alpha \in E$ روی K متعالی باشد. در این صورت α ریشه هیچ چندجمله‌ای در $K[x]$ نیست. مجموعه $B = \{1, \alpha, \alpha^2, \ldots\} \subseteq E$ مستقل خطی است زیرا اگر مستقل خطی نباشد آنگاه ترکیب خطی متناهی $\sum_{i=0}^{k} r_i \alpha^i$ وجود دارد که حداقل یکی از ضرایب α^iها مخالف صفر است اما $\sum_{i=0}^{k} r_i \alpha^i = 0$. بنابراین α ریشه چندجمله‌ای مانند $f(x) = \sum_{i=0}^{k} r_i x^i$ است و این تناقض با متعالی بودن α است. بنابراین B یک پایه برای E است و $[E : K] = \infty$ که در تناقض با فرض قضیه است. □

تذکر ۲۳. اگر K و L دو میدان و $\sigma : K \longrightarrow L$ یکریختی میدان‌ها باشد آنگاه $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ در $K[x]$ تحویل ناپذیر است اگر و تنها اگر $\sigma(a_0)x + \cdots + \sigma(a_n)x^n$ در $L(x)$ نحویل ناپذیر باشد.

قضیه ۱۶. فرض کنیم E و F دو توسیع از میدان K باشند. همچنین فرض کنیم عناصر $\alpha \in E$ و $\beta \in F$ جبری روی K با چندجمله‌ای مینیمال $p(x)$ باشند. در این صورت یک K-یکریختی یکتایی مانند $\varphi : K_F[\beta] \longrightarrow K_E[\alpha]$ وجود دارد که $\varphi(\beta) = \alpha$.

اثبات. به سادگی و با استفاده از دو یکریختی $K_F[\beta] \cong \frac{K[x]}{\langle p(x)\rangle}$ و $K_E[\alpha] \cong \frac{K[x]}{\langle p(x)\rangle}$ می‌توانیم یکریختی مورد نظر را بیابیم. □

قضیه ۱۷. فرض کنیم K، E و F میدان باشند و $K < E < F$. در این صورت

۱) $[F : K] < \infty$ اگر و تنها اگر $[F : E] < \infty$ و $[E : K] < \infty$.

۲) اگر $[F : K] < \infty$ آنگاه $[F : K] = [F : E] \cdot [E : K]$.

اثبات. فرض کنید $e_1, \ldots, e_m$ پایه‌ای برای E روی K باشند و $f_1, \ldots, f_n$ پایه‌ای برای F روی E باشند. نشان دهید که $e_i f_j$ ها پایه‌ای برای F روی K هستند. (تمرینها). □

مثال ۴۱. واضح است که $\mathbb{Q} < \mathbb{Q}(\sqrt{2}) < \mathbb{Q}(\sqrt{2}, \sqrt{3})$. بنا به قضیه بالا، $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$ زیرا $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2})] = 2$ (برابر با درجه چندجمله‌ای مینیمال $p(x) = x^2 - 3$) و $[\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2$ (برابر با درجه چندجمله‌ای مینیمال $q(x) = x^2 - 2$). یعنی

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}), \mathbb{Q}].$$

به همین صورت می‌توان $[\mathbb{Q}(\sqrt{2}, i), \mathbb{Q}]$ را محاسبه کرد.

مثال ۴۲. فرض کنیم $\alpha = \sqrt[5]{2}$ و $\beta = e^{2\pi i/7}$. می‌خواهیم $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ را محاسبه کنیم. چندجمله‌ایهای مینیمال نظیر α و β روی $\mathbb{Q}$ به ترتیب برابر است با $p(x) = x^5 - 2$ و $q(x) = 1 + x + x^2 + \cdots + x^6$. چندجمله‌ای $q(x)$ ممکن است روی $\mathbb{Q}[\alpha]$ تحویل ناپذیر نباشد بنابراین $6 \leq [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}[\alpha]]$ پس طبق قضیه $30 \leq [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$. از طرفی $5 = \mathbb{Q}[\alpha] \mid [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ و $6 = \mathbb{Q}[\beta] \mid [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ و این یعنی $30 \mid [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ بنابراین $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 30$.

نتیجه ۷. فرض کنیم K میدان و $F = K(\alpha_1, \ldots, \alpha_n)$ به طوری که $\alpha_1, \ldots, \alpha_n$ روی K جبری باشند. در این صورت $[F : K] < \infty$. (به بیان دیگر، هر توسیع جبری با تعداد متناهی عنصر، یک توسیع متناهی است. توجه کنید که قبل نشان داده‌ایم که هر توسیع متناهی نیز جبری است).

قضیه ۱۸. اگر میدان F روی میدان E جبری و میدان E روی میدان K جبری باشد آنگاه F روی K نیز جبری است.

اثبات. اگر $[F : E]$ و $[E : K]$ متناهی باشند آنگاه $[F : K] < \infty$ و F روی K جبری است. فرض کنیم چنین نباشد و $\alpha \in F$. ثابت می‌کنیم α روی K جبری است. F روی E جبری است، پس چندجمله‌ای $f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$ وجود دارد که $f(\alpha) = 0$. از طرفی $f(x) \in K(a_0, \ldots, a_n)[x] \subseteq E[x]$. بنابراین α روی $K(a_0, \ldots, a_n)$ هم جبری است. پس $[K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)]$ برابر با درجه چندجمله‌ای مینیمال α روی $K(a_0, \ldots, a_n)$ است. به طور دقیق‌تر $[K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)] < \infty$. از آنجایی که برای هر $0 \leq i \leq n$، $a_i \in E$ طبق فرض a_iها روی K جبری هستند. بنابراین $K(a_0, \ldots, a_n)$ روی K توسیع متناهی است. با توجه به آنچه گفته شد و قضیه ۱۷ داریم

$$[K(a_0, \ldots, a_n)(\alpha) : K] = [K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)] \cdot [K(a_0, \ldots, a_n) : K] < \infty.$$

پس $K(a_0, \ldots, a_n)(\alpha)$ روی K توسیع متناهی و α روی K جبری است. □

قضیه ۱۹. فرض کنیم F و K میدان باشند به طوری که $K < F$. قرار دهید $E = \{u \in F : u \text{ روی } K \text{ جبری است }\}$ آنگاه $K \subseteq E$ و E میدان است.

اثبات. $K \subseteq E$ است زیرا هر عنصر K مانند k با چندجمله‌ای $p(x) = x - k \in K[x]$ در K جبری است. فرض کنیم $u, v \in E$. چون u و v روی K جبری هستند، پس طبق نتیجه ۷، $[K(u, v) : K] < \infty$. پس $K(u, v)$ روی K جبری است. از طرفی $u + v$، $u \cdot v$ و u^{-1} همگی در $K(u, v)$ هستند و بنابراین روی K جبری هستند. بنابراین $u + v$، $u \cdot v$ و u^{-1} در E هستند و این یعنی E میدان است. □

تذکر ۲۴. عناصری از $\mathbb{R}$ که روی $\mathbb{Q}$ جبری هستند را با $\mathbb{R}^{alg}$ و عناصری از $\mathbb{C}$ که روی $\mathbb{Q}$ جبری هستند را با $\mathbb{Q}^{alg}$ نمایش می‌دهیم. واضح است که $\mathbb{R}^{alg}$ و $\mathbb{Q}^{alg}$ متفاوت از هم هستند و $\mathbb{Q} \leq \mathbb{R}^{alg} \leq \mathbb{C}^{alg} \leq \mathbb{C}$. به $\mathbb{R}^{alg}$ میدان بسته حقیقی و به $\mathbb{C}^{alg}$ بسته جبری گوییم. ثابت می‌کنیم $[\mathbb{R}^{alg} : \mathbb{Q}] = \infty$. فرض کنیم چنین نباشد. یعنی $[\mathbb{R}^{alg} : \mathbb{Q}] = n$. همچنین فرض کنیم α روی $\mathbb{Q}$ متعالی باشد. چندجمله‌ای $f(x) = x^{n+1} - \alpha \in \mathbb{Q}[x]$ تحویل ناپذیر و $f(\alpha) = 0$. بنابراین طبق قضیه ۱۷ داریم

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{R}^{alg} : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{R}^{alg} : \mathbb{Q}]$$

و این یعنی $n \leq n + 1$ که تناقض است.

تعریف ۳۷. توسیع جبری E روی K را نرمال گوییم هرگاه هر چندجمله‌ای تحویل ناپذیر در $K[x]$ که در E ریشه داشته باشد به صورت حاصلضرب عوامل خطی در $E[x]$ تجزیه می‌شود. به عبارت دیگر هر چندجمله‌ای تحویل ناپذیر در $K[x]$ یا هیچ ریشه‌ای در E ندارد و یا همه ریشه‌هایش در E است.

مثال ۴۳. اگر $\alpha = \sqrt[3]{2}$ آنگاه $\mathbb{Q}(\alpha)$ روی $\mathbb{Q}$ نرمال نیست. زیرا چندجمله‌ای تحویل ناپذیر $f(x) = x^3 - 2$ را نمی‌توان در $\mathbb{Q}(\alpha)[x]$ به صورت حاصلضرب عوامل خطی نوشت. به عبارت دیگر تنها ریشه $f(x)$ در $\mathbb{Q}(\alpha)$ خود α است و دو ریشه دیگر آن در میدان‌های بالاتر (یا به طور کلی در $\mathbb{C}$) قرار دارند.

فصل ۳

میدانهای بستهٔ جبری، حذف سور و قضیهٔ ریشه‌ها

مدرس: محسن خانی
گردآوری: فاطمهٔ اکبری

۱.۳ معرفی میدانهای بستهٔ جبری

لم ۲. (لم زرن). فرض کنیم $(X, <)$ یک مجموعه مرتب جزئی و ناتهی باشد. همچنین فرض کنیم هر زنجیر $A \subset X$ دارای یک کران بالا در X باشد؛ در این صورت X دارای یک عنصر ماکسیمال است.

لم ۳. برای هر میدان K یک توسیع جبری مانند $K \subseteq L$ وجود دارد به طوری که هر چندجمله‌ای $f(x) \in K[x]$ تمام ریشه‌هایش در L است.

اثبات. $\mathcal{A}$ را به صورت زیر در نظر می‌گیریم،

$$\mathcal{A} = \{E \in Field \mid K \subseteq_{alg} E, \ \}$$

که در بالا منظورمان از $K \subseteq_{alg} E$ این است که E یک توسیع جبری K است و منظورمان از $Field$ کلاس همه میدان‌ها است. $\mathcal{A}$ ناتهی است و می‌توان ترتیب توسیع میدانی را روی آن تعریف کرد. به طور دقیق‌تر برای هر $E_1, E_2 \in \mathcal{A}$، داریم $E_1 \subseteq E_2$ اگر و تنها اگر E_2 شامل E_1 باشد و نشاندن $\varphi : E_1 \longrightarrow E_2$ موجود باشد. فرض کنیم A یک زنجیر در $\mathcal{A}$ باشد. یعنی

$$A = \{E_i\}_{i \in I}$$

و

$$i < j \Leftrightarrow E_i \subseteq E_j.$$

در این صورت $\bigcup_{E \in A} E$ یک میدان است (چرا؟) که توسیع جبری K است. زیرا اگر $a \in \bigcup_{E \in A} E$ آنگاه $E_i \in A$ روی K وجود دارد که $a \in E_i$ و بنابراین a روی K جبری است. $\bigcup_{E \in A} E$ کران بالای زنجیر A است و این یعنی هر زنجیر صعودی در $\mathcal{A}$ دارای کران بالا است. بنا به لم زرن $\mathcal{A}$ دارای یک عنصر ماکسیمال مانند L است. به بیان دیگر یک میدان L در $\mathcal{A}$ وجود دارد که توسیع جبری K است و هیچ توسیع جبری ندارد. همچنین همه ریشه‌های هر چندجمله‌ای دلخواه $f(x) \in K[x]$ در L است. زیرا در غیر این صورت ریشه‌ای از $f(x)$ در یک توسیع از L قرار دارد که این در تناقض با ماکسیمال بودن L است. □

گزاره ۵. فرض کنیم میدان L توسیع جبری میدان K باشد. اگر همه چندجمله‌ای‌های $f(x) \in K[x]$ در L ریشه داشته باشند آنگاه همه چندجمله‌ای‌های $g(x) \in L[x]$ هم در L ریشه دارند.

اثبات. فرض کنیم α ریشه $g(x) \in L[x]$ باشد که در یک توسیع جبری L مانند L' قرار دارد. L' روی K جبری است یعنی α ریشه یک چندجمله‌ای مانند $f(x) \in K[x]$ است. پس $\alpha \in L$. □

تا به اینجا، بنا به آنچه گفته شد اگر K یک میدان باشد آنگاه یک توسیع جبری L برای K موجود است که همه چندجمله‌ای‌های متعلق به $K[x]$ در L ریشه دارند و این دقیقا معادل است با این که همه ریشه‌های همه چندجمله‌ای‌های در $L[x]$ در L قرار دارند.

تعریف ۳۸. اگر میدان L یک توسیع جبری برای میدان K باشد به طوری که همه چندجمله‌ای‌های متعلق به $K[x]$ در آن ریشه داشته باشند آنگاه به L یک بستار جبری K می‌گوییم.

در یک بستار جبری تمام نقاط جبری وجود دارند و اگر قرار باشد توسیع دیگری شامل این بستار ارائه دهیم آنگاه این توسیع تنها با اضافه‌کردن عناصر متعالی حاصل می‌شود. بنابراین یک بستار جبری هیچ توسیع جبری غیر بدیهی ندارد.

قضیه ۲۰. فرض کنیم L_1 و L_2 دو بستار جبری K باشند در این صورت K-یکریختی وجود دارد که L_1 و L_2 تحت آن یکریخت هستند. به عبارت دیگر، میدان‌های بسته جبری تحت یکریختی یکتا هستند.

اثبات. قرار می‌دهیم،

$$\mathcal{A} = \{f : E_1 \longrightarrow E_2 \mid f : \text{یکریختی} - K, \quad K \subseteq E_1 \subseteq L_1,\ K \subseteq E_2 \subseteq L_2\}.$$

$\mathcal{A}$ ناتهی است. ترتیب $\subseteq$ را روی $\mathcal{A}$ به این صورت تعریف می‌کنیم: برای هر f_1و f_2 در $\mathcal{A}$ قرار می‌دهیم $f_1 \subseteq f_2$ اگر و تنها اگر f_2 حافظ انتقال‌های f_1 باشد. فرض کنیم

$$\{f_i\}_{i\in I} \tag{۱.۳}$$

یک زنجیر از اعضای $\mathcal{A}$ باشد در این صورت برای مجموعه اندیس I،

$$F = \bigcup_{i\in I} f_i : \bigcup_{i\in I} Dom(f_i) \longrightarrow \bigcup_{i\in I} Rang(f_i)$$

یک K-یکریختی است. همچنین F یک کران بالا برای زنجیر (۱.۳) و بنابراین $\mathcal{A}$ دارای عنصر ماکسیمال است. اگر عنصر ماکسیمال $\mathcal{A}$، K-یکریختی g باشد آنگاه دامنه g برابر با L_1 است. زیرا در غیر این صورت عنصری مانند α در دامنه g وجود دارد که جبری نیست و بنابراین K-یکریختی، $h : Dom(g)(\alpha) \longrightarrow Rang(h)$ وجود دارد که این در تناقض با ماکسیمال بودن g است. به طور مشابه ثابت می‌شود که برد g برابر با L_2 است. بنابراین L_1 و L_2 تحت g یکریخت هستند. □

تذکر ۲۵. بستار جبری میدان K (که تحت یکریختی یکتاست) را با K^{ac} نمایش می‌دهیم.

تعریف ۳۹. میدان K را بسته جبری نامیم هرگاه بستار جبری K خودش باشد ($K^{ac} = K$). به بیان دیگر، K بسته جبری است اگر هیچ توسیع جبری سره‌ای نداشته باشد.

تکنیکی که در اثبات‌های لم ۳ و قضیه ۲۰ به کار بردیم بسیار کاربردی است. در ادامه خواهیم دید که برای اثبات نتیجه زیر و گزاره پس از آن نیز می‌توان از این تکنیک استفاده کرد.

نتیجه ۸. فرض کنیم L بستار جبری K باشد و $f \in K[x]$ یک چندجمله‌ای تحویل ناپذیر باشد. اگر α و β دو ریشه متمایز f در L باشند در این صورت خودریختی $\sigma : L \longrightarrow L$ وجود دارد که $\sigma(\alpha) = \beta$.

اثبات. می‌دانیم که یک یکریختی بین $K(\alpha), K(\beta)$ وجود دارد. بین ایزومرفیسمهای بین زیرمیدانهای L که شامل این یکریختی هستند ترتیب شمول را در نظر بگیرید و نشان دهید که ایزمرفیسم ماکزیمال، همان خودریختی مورد نظر ماست. □

نتیجه بالا را می‌توان به این صورت نیز تعبیر کرد. دقت کنید که اگر $\sigma : L \longrightarrow L$ یک K-خودریختی باشد آنگاه برای هر α که ریشه $f(x) \in K[x]$ در L باشد، $\sigma(\alpha)$ نیز ریشه‌ای از $f(x)$ در L است. یعنی خودریختی‌ها ریشه‌های چندجمله‌ای را جابه‌جا می‌کنند. اما از طرفی برای دو ریشه متخلف یک خودریختی وجود دارد که یکی را به دیگری ببرد. بنابراین در توسیع K توسط ریشه‌های f تعداد خودریختی‌ها مرتبط با تعداد ریشه‌های f است.

اما گزاره بعدی به مباحث تعریف پذیری در جلسات گذشته برمی‌گردد. پیش‌تر گفتیم که مجموعه $\mathbb{R}$ در $\mathbb{C}$ تعریف ناپذیر است و اشاره کوتاهی به اثبات این موضوع داشتیم. در اثبات گزاره زیر به طور دقیق‌تر به چرایی آنچه پیرامون این گزاره گفته شد می‌پردازیم.

گزاره ۶. مجموعه اعداد حقیقی در ساختار $(\mathbb{C}, +, \cdot, ۰, ۱)$ با پارامترهای در $\mathbb{Q}$ تعریف ناپذیر است.

اثبات. اگر $r \in \mathbb{R} \setminus \mathbb{Q}$ و $s \in \mathbb{C} \setminus \mathbb{Q}$ دو عنصر متعالی روی $\mathbb{Q}$ باشند آنگاه $\mathbb{Q}(r) \cong \mathbb{Q}(s)$. مشابه تکنیک اثبات‌های گذشته خودریختی σ وجود دارد که $\sigma(r) = s$. این نتیجه در تناقض است با اینکه اگر $\mathbb{R}$ تعریف پذیر باشد آنگاه برای هر $\mathbb{Q}$-خودریختی، $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ داریم $\sigma(\mathbb{R}) = \mathbb{R}$. □

در اینجا به عنوان مقدمه اشاره کوتاهی به میدان کسرها خواهیم داشت. از آنجایی که دوباره وارد مباحث منطقی در جبر خواهیم شد از نمادگذاری‌هایی که در بخش مقدمات منطق در نظر گرفتیم استفاده می‌کنیم. اگر حوزه صحیح A زیر مجموعه‌ای از میدان‌های M و N باشد آنگاه می‌توان میدان کسرهای A را به صورت جداگانه روی M و N ساخت. این میدان کسرها را به ترتیب با $Frac_M(A)$ و $Frac_N(A)$ نمایش می‌دهیم. ثابت می‌شود که $Frac_M(A) \cong Frac_N(A)$. اما نکته دیگری که قبل از قضیه زیر باید به آن اشاره کنیم این است که میدان‌های بسته جبری نامتناهی هستند. در واقع اگر یک میدان متناهی مانند $K = \{\alpha_۱, \ldots, \alpha_n\}$ داشته باشیم آنگاه چندجمله‌ای $f(x) = (x - \alpha_n) + \cdots + (x - \alpha_۱) + ۱ \in K[x]$ تحویل ناپذیر و بنابراین K بسته جبری نیست.

۲.۳ حذف سور در میدانهای بستهٔ جبری

قضیه ۲۱. تئوری میدان‌های بسته جبری حذف سور دارد.

اثبات. فرض کنیم T تئوری میدان‌های بسته جبری باشد و $\mathfrak{M}, \mathfrak{N} \models T$. همچنین فرض کنیم $\mathfrak{A}$ یک زیرساختار مشترک از $\mathfrak{M}$ و $\mathfrak{N}$ باشد. اگر A جهان $\mathfrak{A}$ باشد، A یک حوزه است (در واقع هر زیرساختار میدان حوزه صحیح است). میدان کسرهای A را روی M (جهان $\mathfrak{M}$) می‌سازیم، یعنی $Frac_M(A) = \{\frac{a}{b} \mid a, b \in A\}$. فرمول زیر را در نظر می‌گیریم،

$$\psi : \quad \exists x \;\; f_۱(x) = ۰ \wedge \cdots \wedge f_k(x) = ۰ \wedge g_۱(x) \neq ۰ \wedge \cdots \wedge g_t(x) \neq ۰ \qquad (۲.۳)$$

به طوری که f_iها و g_jها به $A[x]$ تعلق دارند. می‌خواهیم نشان دهیم اگر این دستگاه معادله روی M جواب داشته باشد ($\mathfrak{M} \models \psi$) آنگاه روی N نیز جواب دارد ($\mathfrak{N} \models \psi$). دو حالت در نظر می‌گیریم،

۱) دستگاه (۲.۳) حداقل دارای یک معادله تساوی باشد. در این صورت $a \in M$ وجود دارد که a روی A جبری است. بنابراین $a \in (Frac_M(A))^{ac}$. یکریختی $\varphi : (Frac_M(A))^{ac} \longrightarrow (Frac_N(A))^{ac}$ وجود دارد که $\varphi(a) = b$ به طوری که $b \in N$. پس b جواب دستگاه (۲.۳) در N است.

۲) فرض کنیم در (۲.۳) هیچ معادله تساوی وجود ندارد و a یک جواب این دستگاه در M باشد. از آنجایی که تعداد ریشه‌های یک چندجمله‌ای متناهی است، بنابراین عنصر b در N وجود دارد که در هیچ یک از g_jها صفر نشود.

به همین صورت ثابت می‌شود که اگر (۲.۳) روی N جواب داشته باشد ($\mathfrak{N} \models \psi$) آنگاه روی M نیز جواب دارد ($\mathfrak{M} \models \psi$) و این یعنی تئوری میدان‌های بسته جبری سورها را حذف می‌کند. □

تعریف ۴۰. فرض کنیم K میدان و $K[x_۱, \ldots, x_n]$ حلقه چندجمله‌ای‌های n متغیره باشد. برای هر $S \subseteq K[x_۱, \ldots, x_n]$ مجموعه

$$V(S) = \{(a_۱, \ldots, a_n) \in K^n \mid \forall f \in S, \;\; f(a_۱, \ldots, a_n) = ۰\}$$

را ورایتی یا چندگونای S می‌نامیم.

اگر $I \subseteq K[x_۱, \ldots, x_n]$ یک ایده‌آل باشد آنگاه بوسیله $V(I)$ها یک توپولوژی روی K^n تعریف می‌شود. در این حالت مجموعه‌های $V(I)$ را مجموعه‌های بسته زاریسکی می‌گویند.

گزاره ۷. اگر I و J دو ایده‌آل در $K[x_۱, \ldots, x_n]$ باشند به طوری که $I \subseteq J$ آنگاه $V(J) \subseteq V(I)$.

اثبات. برای هر $\overline{a} = (a_1, \ldots, a_n) \in V(J)$ و هر $f \in J$ داریم $f(\overline{a}) = 0$ چون $I \subseteq J$ بنابراین برای هر $g \in I$ نیز داریم $g(\overline{a}) = 0$. یعنی $\overline{a} \in V(I)$. □

تعریف ۴۱. ایده‌آل I را در حلقه R ایده‌آل رادیکال می‌نامیم هرگاه برای هر $n \in \mathbb{N}$ که $r^n \in I$ آنگاه $r \in I$.

تمرین ۸. ثابت کنید ایده‌آل I یک ایده‌آل رادیکال است هرگاه برای $r \in R$، اگر $r^2 \in I$ آنگاه $r \in I$.

۳.۳ اثبات قضیهٔ ریشه‌های هیلبرت

دو لم مورد نیاز زیر را بدون اثبات بیان می‌کنیم.

لم ۴. اگر $I \subseteq K[x_1, \ldots, x_n]$ یک ایده‌آل رادیکال باشد آنگاه ایده‌آل‌های اول $P_1, \ldots, P_n$ وجود دارند به طوری که $I = P_1 \cap \cdots \cap P_n$.

لم ۵. اگر I یک ایده‌آل در $K[x_1, \ldots, x_n]$ باشد آنگاه I متناهیا تولید می‌شود. یعنی $f_1, \ldots, f_k \in I$ وجود دارند که $I = \langle f_1, \ldots, f_k \rangle$.

قضیه ریشه‌ها را به وسیله حذف سور اثبات کنیم.

قضیه ۲۲. (قضیه ریشه‌ها)[1]. فرض کنیم I و J دو ایده‌آل رادیکال در $K[x_1, \ldots, x_n]$ باشند به طوری که K یک میدان بسته جبری است. در این صورت اگر I زیر مجموعه سره J باشد آنگاه $V(J)$ زیر مجموعه سره $V(I)$ است.

اثبات. I یک تجزیه از ایده‌آل‌های اول به صورت $I = P_1 \cap \cdots \cap P_n$ دارد. همچنین $f_1, \ldots, f_k \in I$ وجود دارند که $I = \langle f_1, \ldots, f_k \rangle$. فرض کنیم $g \in J \setminus I$. بنابراین اندیس i وجود دارد که $g \notin P_i$. اگر $\overline{x} = (x_1, \ldots, x_n)$، فرمول

$$\psi(\overline{x}) : \ \exists x \ \ (g(\overline{x}) \neq 0) \wedge (\bigwedge_{i=1}^{k} f_i(\overline{x}) = 0)$$

در حوزه صحیح

$$F = \frac{K[x_1, \ldots, x_n]}{P_i}$$

درست است. پس می‌توان نوشت

$$F \models \exists \overline{a} \ \ \psi(\overline{a}).$$

(در واقع $\overline{a}$ همان جواب معادله $g(\overline{x}) \neq 0$ در F است.) همچنین، $(F)^{ac} \models \exists x \ \ \psi(\overline{x})$. اما $(F)^{ac}$ یک میدان بسته جبری شامل K است، پس بنا به حذف سور $K \models \exists \bar{x} \ \ \psi(\overline{x})$ و این یعنی در K^n عنصری وجود دارد که به $V(I)$ تعلق دارد اما در $V(J)$ قرار ندارد. □

لم ۶. برای هر دو ایده‌آل I, J داریم

$$V(I \cap J) = V(I) \cup V(J).$$

اثبات. واضح است که هم $V(I)$ و هم $V(J)$ زیرمجموعهٔ $V(I \cap J)$ هستند و از این رو $\supseteq$ برقرار است.

حال فرض کنید a نه در $V(I)$ و نه در $V(J)$ باشد. در این صورت $f \in I$ و $g \in J$ موجودند که a ریشهٔ آنها نیست. پس a ریشهٔ $f.g$ نیست؛ اما $f.g \in I \cap J$. □

نتیجه ۹. فرض کنیم I و J دو ایده‌آل رادیکال در $K[x_1, \ldots, x_n]$ باشند به طوری $I \neq J$ در این صورت $V(I) \neq V(J)$.

اثبات. اگر $I \neq J$ آنگاه $I \cap J \neq I$. پس $V(I \cap J) \neq V(I)$. اما اگر قرار بود $V(I) = V(J)$ آنگاه می‌داشتیم

$$V(I \cap J) = V(I) \cup V(J) = V(I).$$

□

[1] Nullstellensatz

تعریف ۴۲. اگر $X \subseteq K^n$، ایده‌آل نظیر مجموعه X را به صورت زیر تعریف می‌کنیم:

$$I(X) = \{f \in K[x_1, \dots x_n] \mid \forall (a_1, \dots a_n) \in X, \quad f(a_1, \dots a_n) = 0\}$$

تمرین ۹. نشان دهید $I(X)$ در بالا یک ایده‌آل اولیه است.

تمرین ۱۰. با عضوگیری نشان دهید که

$$V(I(V(I)) = V(I).$$

نتیجه ۱۰. اگر I یک ایده‌آل اولیه $K[x_1, \dots x_n]$ باشد آنگاه $I(V(I)) = I$.

اثبات. بنا به قضیهٔ قبل اگر $I(V(I)) \neq I$ آنگاه

$$V(I(V(I)) \neq V(I)$$

اما این بنا به تمرین بالا امکان‌پذیر نیست. □

فصل ۴

معرفی حلقه‌های موضعی

تدریس: محمود بهبودی
گردآوری: فاطمهٔ اکبری

۱.۴ حلقه‌های موضعی

یکی از شروط معادل میدان بودن این است که تنها ایده‌آل ماکزیمال حلقه، ایده‌آل صفر باشد. کمی ضعیفتر شده‌ی این شرط این است که حلقه، تنها یک ایده‌آل ماکزیمال داشته باشد. به چنین حلقه‌ای، حلقهٔ موضعی می‌گوییم.

تعریف ۴۳. حلقه جابه جایی و یکدار R را موضعی می‌نامیم هرگاه تنها یک ایده‌آل ماکسیمال داشته باشد. اگر m ایده‌آل ماکسیمال R باشد آنگاه این حلقه را به صورت (R, m) نمایش می‌دهیم.

برای مثال میدان‌ها موضعی با ایده‌آل ماکسیمال $\langle ۰ \rangle$ هستند. در قضیه زیر نشان می‌دهیم اعضای ایده‌آل ماکسیمال یک حلقه موضعی وارون ندارند.

قضیه ۲۳. اگر R یک حلقه جابه جایی و یکدار باشد آنگاه موارد زیر با هم معادلند.

۱) R موضعی است،

۲) مجموعه عناصر غیر یکان R تشکیل ایده‌آل ماکزیمال می‌دهند،

۳) مجموعه عناصر غیر یکان R تحت عمل جمع بسته است.

اثبات. (۱ $\Leftarrow$ ۲) فرض کنیم m ایده‌آل ماکسیمال حلقه R باشد. ثابت می‌کنیم $m = R \setminus U(R)$. واضح است که عناصر m وارون ندارند، بنابراین $m \subseteq R \setminus U(R)$. فرض کنیم $a \in R \setminus U(R)$. چون $a \notin U(R)$ نتیجه می‌گیریم ایده‌آل Ra در R سره است. هر ایده‌آل سره زیرمجموعهٔ یک ایده‌آل ماکزیمال است و چون در اینجا فقط یک ایده‌آل ماکزیمال داریم، $Ra \subseteq m$ یعنی $a \in M$. این یعنی $R \setminus U(R) \subseteq M$.
(۲ $\Leftarrow$ ۳) واضح است.
(۳ $\Leftarrow$ ۱) فرض کنیم برای هر $a, b \in R \setminus U(R)$ داریم $a+b \in R \setminus U(R)$. ثابت می‌کنیم $R \setminus U(R)$ یک ایده‌آل است. فرض کنیم $a \in R \setminus U(R)$ و $b \in R$ در این صورت $a \cdot b \in R \setminus U(R)$. زیرا اگر چنین نباشد آنگاه $a \cdot b \in U(R)$ و این یعنی a وارون پذیر است که تناقض است. از طرفی برای هر عنصر دلخواه $a \in U(R)$ چون a وارون پذیر است، نمی‌تواند شامل یک ایده‌آل ماکسیمال باشد بنابراین $R \setminus U(R)$ تنها ایده‌آل ماکسیمال R است و R موضعی است. □

می‌خواهیم مثال‌هایی از حلقه‌های موضعی را بررسی کنیم. اما قبل از آن دو نکته از ایده‌آل‌های اول و ماکسیمال یادآوری می‌کنیم.

- اگر ایده‌آل I در حلقه R ماکسیمال باشد آنگاه اول هم هست.

- از تعریف اول بودن ایده‌آل‌ها می‌توانیم نتیجه بگیریم برای هر دو ایده‌آل $I, J \subseteq R$ و ایده‌آل اول P، اگر $IJ \subseteq P$ آنگاه یا $I \subseteq P$ و یا $J \subseteq P$.

قضیه ۲۴. اگر R یک حلقه جابه جایی و یکدار و M یک ایده‌آل ماکسیمال در R باشد آنگاه برای هر $k \in \mathbb{N}$، $(\frac{R}{M^k}, \frac{M}{M^k})$ یک حلقه موضعی است.

اثبات. فرض کنیم ایده‌آل $\frac{J}{M^k}$ در $\frac{R}{M^k}$ وجود داشته باشد که

$$\frac{M}{M^k} < \frac{J}{M^k} < \frac{R}{M^k}.$$

در این صورت $M \subset J$. اما M در R ماکسیمال است پس $J = R$ و $\frac{J}{M^k} = \frac{R}{M^k}$. پس $\frac{M}{M^k}$ در $\frac{R}{M^k}$ ماکسیمال است. ثابت می‌کنیم یکتاست. فرض کنیم ایده‌آل ماکسیمال دیگری مانند $\frac{M'}{M^k}$ وجود داشته باشد. در R، M' ماکسیمال است و این یعنی M' اول هم هست. پس از $MM \subseteq M'$ نتیجه می‌گیریم $M \subseteq M'$. بنابراین $M = M'$ و $\frac{M}{M^k}$ تنها ایده‌آل ماکسیمال $\frac{R}{M^k}$ است. □

پس بنا به قضیه بالا برای یک حلقه دلخواه R و هر ایده‌آل ماکسیمال M در R می‌توانیم یک دسته از حلقه‌های موضعی به شکل $\frac{R}{M^k}$ را بدست آوریم.

مثال ۴۴. فرض کنیم K میدان و $p(x) \in K[x]$ تحویل ناپذیر باشد. $\langle x \rangle$ یک ایده‌آل ماکسیمال در $K[x]$ است. بنابراین طبق قضیه قبل $(\frac{K[x]}{\langle p(x) \rangle^n}, \frac{\langle x \rangle}{\langle p(x) \rangle^n})$ یک حلقه موضعی است.

مثال ۴۵. ایده‌آل $\langle x \rangle$ در $\mathbb{Z}_۴[x]$ ماکسیمال است. پس طبق قضیه قبل $(\frac{\mathbb{Z}_۴[x]}{\langle x^۲ \rangle}, \frac{\langle x \rangle}{\langle x^۲ \rangle})$ یک حلقه موضعی با مشخصه ۳ است که $(\frac{\langle x \rangle}{\langle x^۲ \rangle})^۲ = ۰$.

تذکر ۲۶. اگر R یک حلقه موضعی باشد، نمی‌توانیم نتیجه بگیریم که $R[x]$ موضعی است (حتی اگر R میدان باشد). زیرا در $R[x]$، عناصر x و $۱ - x$ وارون ندارند اما $۱ - x + x = ۱$ وارون دارد که این یعنی عناصر یکه نسبت به جمع بسته نیستند و $R[x]$ موضعی نیست.

مثال ۴۶. اگر (R, M) یک حلقه موضعی باشد، آنگاه $R[[x]]$ موضعی با ماکسیمال

$$\langle M, x \rangle = \{r_۰ + r_۱x + r_۲x^۲ + \cdots \mid r_۰ \in M,\ r_i \in R\}$$

است. این نتیجه از این نکته حاصل می‌شود که $f(x) \in R[[x]]$ یکه است اگر و تنها اگر $r_۰$ در R یکه باشد (به عنوان تمرین این نکته را ثابت کنید). بنابراین در حالت خاص اگر K میدان باشد آنگاه $(K[[x]], \langle x \rangle)$ موضعی است. این مثال را در جلسات آینده اثبات خواهیم کرد.

گزاره ۸. حلقه جابه جایی و یکدار R موضعی است اگر و تنها اگر $R[[x]]$ موضعی باشد.

اثبات. در مثال قبل نشان دادیم اگر R موضعی باشد آنگاه $R[[x]]$ موضعی است. برعکس، ثابت می‌کنیم اگر $R[[x]]$ موضعی باشد آنگاه R هم موضعی است. اگر M و M' دو ایده‌آل ماکسیمال مجزا در R باشند آنگاه $\langle M, x \rangle$ و $\langle M', x \rangle$ دو ایده‌آل ماکسیمال مجزا در $R[[x]]$ هستند که این در تناقض با موضعی بودن آن است. بنابراین $M = M'$. □

۲.۴ موضعی سازی

در ادامه به دسته مهمی از حلقه‌ای موضعی می‌پردازیم که با روش **موضعی سازی** به دست می‌آیند.

تعریف ۴۴. فرض کنیم R یک حلقه جابه جایی و یکدار باشد، زیر مجموعه $S \subseteq R$ را یک مجموعه بسته ضربی می‌نامیم هرگاه:

۱) S شامل عنصر همانی ضرب باشد.

۲) برای هر $s_۱, s_۲ \in S$ داشته باشیم $s_۱s_۲ \in S$.

فرض کنیم R یک حلقه و S یک مجموعه بسته ضربی باشد. رابطه تساوی را برای مجموعه

$$S^{-۱}R = \{\frac{r}{s} \mid r \in R,\ s \in S\}$$

به صورت زیر تعریف می‌کنیم،

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \iff \exists u \in S \qquad u(r_1 s_2 - r_2 s_1) = 0.$$

این تساوی یک رابطه هم ارزی است. مجموعه $S^{-1}R$ با اعمال جمع و ضرب به صورت

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\ , \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

یک حلقه است(این حلقه را حلقه کسرها می‌نامیم). همچنین نگاشت همانی $i : R \longrightarrow S^{-1}R$ یک همریختی است. اگر R دامنه صحیح باشد آنگاه i نشاندن است.

تذکر ۲۷. اگر $S = R \setminus \{0\}$ آنگاه $S^{-1}R$ میدان است.

تذکر ۲۸. توجه داشته باشیم که نوشتن اعضای $S^{-1}R$ به صورت $\frac{r}{s}$ به این معنا نیست که وارونی مانند $\frac{s}{r}$ دارد! اما $S^{-1}R$ کوچکترین حلقه‌ای است که عناصر $s \in S$ در آن وارون دارند. برای مثال، اگر بخواهیم کوچکترین حلقه شامل $\mathbb{Z}$ که ۲ در آن وارون دارد را بسازیم به این صورت عمل می‌کنیم: قرار می‌دهیم $S = \{2^i \mid i \in \mathbb{N}\}$. S بسته ضربی است. بنابراین $S^{-1}R = \{\frac{n}{2^i} \mid n \in \mathbb{Z},\ i \in \mathbb{N}\}$ کوچکترین حلقه شامل $\mathbb{Z}$ است که ۲ در آن وارون دارد.

لم ۷. در حلقه جابه جایی و یکدار R، ایده‌آل سره P اول است اگر و تنها اگر $S = R \setminus P$ بسته ضربی باشد.

اثبات. فرض کنیم P اول باشد و $s_1, s_2 \in S$،

$$s_1, s_2 \notin P \Rightarrow s_1 \notin P \ \&\ s_2 \notin P$$
$$\Rightarrow s_1 s_2 \notin P \Rightarrow s_1 s_2 \in S.$$

برعکس، فرض کنیم S بسته ضربی باشد، برای هر دو عنصر $a, b \notin P$ داریم:

$$a \in S,\ \ b \in S \Rightarrow ab \in S \Rightarrow ab \notin P$$

بنابراین P اول است. □

قضیه ۲۵. فرض کنیم R یک حلقه و P یک ایده‌آل اول در آن باشد. قرار می‌دهیم $S = R \setminus P$. در این صورت $S^{-1}R$ یک حلقه موضعی است.

اثبات. مجموعه $M = \{\frac{r}{s} \mid r \in P,\ s \in S\}$ یک ایده‌آل ماکسیمال در $S^{-1}R$ است. در واقع ثابت می‌کنیم هر عنصر خارج از این ایده‌آل وارون دارد. فرض کنیم $\frac{r}{s} \notin M$، بنابراین $r \notin P$. پس $r \in S$ و این یعنی $\frac{s}{r}$ وارون $\frac{r}{s}$ است. بنابراین $(S^{-1}R, M)$ موضعی است. □

تعریف ۴۵. حلقهٔ $S^{-1}R$ در قضیهٔ بالا را موضعی سازیِ R در ایده‌آل اول P می‌نامیم.

مثال ۴۷. فرض کنیم K یک میدان باشد. ایده‌آل $P = \langle x \rangle$ در $K[x]$ اول است. بنابراین

$$S = K[x] \setminus P = \{f(x) \in K[x] \mid f(0) \neq 0\}$$

بسته ضربی است و $S^{-1}K[x] = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ \ f(x) \neq 0\}$ حلقه موضعی است. به طور کلی اگر $f(x)$ در $K[x]$ تحویل ناپذیر باشد آنگاه $P = \langle f(x) \rangle$ اول است و بنابراین $S^{-1}K[x]$ که $S = K[x] \setminus P$ موضعی است.

اگر در مثال قبل مجموعه بسته ضربی $S = \{x^i \mid i \in \mathbb{N}\}$ را در نظر بگیریم، آنگاه $S^{-1}K[x]$ کوچکترین حلقه موضعی شامل $K[x]$ است که عنصر x در آن وارون دارد.

گزاره ۹. اگر (R', M') کوچکترین حلقه موضعی شامل حلقه جابه جایی و یکدار R باشد و $\alpha : R \longrightarrow R'$ یک نشاندن باشد آنگاه ایده‌آل اول P در R وجود دارد که $S^{-1}R \cong R'$ به طوری که $S = R \setminus P$.

اثبات. به سادگی ثابت می‌شود ایده‌آل $P = \alpha^{-1}(M') = \{r \in R \mid \alpha(r) \in M'\}$ در R اول است. قرار می‌دهیم $S = R \setminus P$. نگاشت $\varphi : S^{-1}R \longrightarrow R'$ با ضابطه $\varphi(\frac{r}{s}) = \alpha(r)\alpha(s)^{-1}$ همریختی است و $Ker(\varphi) = \{0\}$ (توجه داشته باشیم که φ خوشتعریف است زیرا وارون $\alpha(s)$ وجود دارد). پس بنا به قضیه اول یکریختی داریم $S^{-1}R \cong R'$. □

فصل ۵

حلقه‌های نُرمدار، پی‌ادیکها و قضیهٔ گرین‌لیف و اکس‌کوچن

تدریس: محسن خانی
گردآوری: فاطمهٔ اکبری

۱.۵ حلقه‌های نرم‌دار

برای یک عدد اول p، از اینجا به بعد، میدان‌های p عضوی (میدان باقی مانده‌های p) را با F_p، حلقه موضعی حاصل از موضعی سازی $\mathbb{Z}$ در ایده‌آل اول $p\mathbb{Z}$ را با $\mathbb{Z}_{p\mathbb{Z}}$ و حلقه جدیدی به نام p-ادیک‌ها که در ادامه با آن آشنا خواهیم شد را با $\mathbb{Z}_p$ نمایش می‌دهیم. p-ادیک‌ها یکی از مثال‌های مهم حلقه‌های نرم دار هستند.

تعریف ۴۶. فرض کنیم R حلقه جابه جایی و یکدار باشد. منظور از یک نُرم روی R تابعی به صورت $|.| : \mathbb{R} \longrightarrow \mathbb{R}^+$ است که

۱) برای هر x داریم $|x| = ۰ \Leftrightarrow x = ۰$ و $|۱| = |-۱| = ۱$.

۲) برای هر دو عنصر x و y، $|x+y| \leq |x| + |y|$.

۳) برای هر دو عنصر x و y، $|x \cdot y| \leq |x| \cdot |y|$.

اگر شرط زیر را جایگزین شرط دوم در تعریف اصلی نرم کنیم، آنگاه این نرم را فرا نرم یا نرم غیر ارشمیدسی می‌نامیم.

۲*) $|x+y| \leq \max(|x|, |y|)$.

حلقه R همرا با نرم $|.|$ را به صورت $(R, |.|)$ نمایش می‌دهیم.

تذکر ۲۹. به طور مستقیم می‌توانیم از تعریف بالا نتیجه بگیریم برای هر $x \in R$، $|x| = |-x|$.

لم ۸. فرض کنیم $(R, |.|)$ یک حلقه دارای فرا نرم باشد. در این صورت اگر $|x| \neq |y|$ آنگاه $|x+y| = \max(|x|, |y|)$.

اثبات. فرض کنیم $|x| < |y|$، یعنی $\max(|x|, |y|) = |x|$. بنا به تعریف $|x+y| \leq |x|$. بنابراین

$$|x+y| \leq |x| = |x+y-y| \leq \max(|x+y|, |y|) = |x+y|.$$

برای تساوی آخر دقت کنید، از آنجا که $|x| < |y|$ و $|x| \leq \max\{|x+y|, |y|\}$ نتیجه گرفته‌ایم که $\max\{|x+y|, |y|\} = |x+y|$. □

تعریف ۴۷. فرض کنیم $(a_n)_{n\in\mathbb{N}}$ یک دنباله در حلقه نرم دار $(R,|.|)$ باشد. این دنباله را کوشی نامیم هرگاه

$$\forall \epsilon > ۰ \quad \exists N \in \mathbb{N} \qquad \forall m,n > N \quad |a_n - a_m| < \epsilon.$$

حلقه $(R,|.|)$ را کامل می‌نامیم هرگاه هر دنباله کوشی در آن همگرا باشد.

لم ۹. فرض کنیم حلقه R نسبت به فرا نرم $|.|$ کامل باشد در این صورت برای هر دنباله دلخواه $(a_n)_{n\in\mathbb{N}}$ در R داریم

$$\sum_{n=۰}^{\infty} a_n \in R \iff \lim_{n\to\infty} |a_n| = ۰.$$

اثبات. قرار می‌دهیم $S_n = a_۰ + a_۱ + \cdots + a_n$. اگر $\lim_{n\to\infty} S_n = \sum_{n=۰}^{\infty} a_n$ موجود باشد آنگاه $\lim_{n\to\infty} S_n = \lim_{n\to\infty} S_{n+۱}$، پس $\lim_{n\to\infty}(S_n - S_{n+۱}) = \lim_{n\to\infty} a_{n+۱} = ۰$. برعکس، فرض کنیم $(|a_n|)_{n\in\mathbb{N}}$ همگرا به صفر باشد. کافی است نشان دهیم دنباله $(S_n)_{n\in\mathbb{N}}$ کوشی است. برای هر $m,n \in \mathbb{N}$ که $m < n$ داریم

$$|S_n - S_m| = |a_{m+۱} + a_{m+۲} + \cdots + a_{n-۱}| \le \max_{m+۱\le i\le n-۱}(|a_i|)$$

و چون حد $(|a_n|)_{n\in\mathbb{N}}$ صفر است پس $(S_n)_{n\in\mathbb{N}}$ کوشی و همگرا به صفر است. □

لم بالا برای نرم‌های غیر ارشمیدسی برقرار نیست. برای مثال دنباله $(\frac{۱}{n})_{n>۰}$ در $\mathbb{R}$ با در نظر گرفتن نرم قدر مطلق همگرا به صفر است. اما $\sum_{n=۰}^{\infty} \frac{۱}{n}$ واگراست.

مثال ۴۸. فرض کنیم R یک حلقه غیر بدیهی و $R[[x_۱,\ldots,x_n]]$ حلقه سری‌های توانی n متغیره با ضرایب متعلق به R باشد. هر یک از عناصر $R[[x_۱,\ldots,x_n]]$ را به صورت

$$f = \sum_{(i_۱,\ldots,i_n)\in\mathbb{N}^n} a_{(i_۱,\ldots,i_n)} x_۱^{i_۱}\cdots x_n^{i_n}$$

نمایش می‌دهیم و مرتبه آن را به صورت زیر تعریف می‌کنیم،

$$\operatorname{ord}(f) = \begin{cases} \min(\{i_۱ + \cdots + i_n \mid a_{(i_۱,\ldots,i_n)} \neq ۰\}) & f \neq ۰ \\ \infty & f = ۰ \end{cases}$$

پس $\operatorname{ord}(۱) = ۰$ و

$$\operatorname{ord}(f+g) \ge \min(\operatorname{ord}(f),\operatorname{ord}(g)), \quad \operatorname{ord}(f\cdot g) \ge \operatorname{ord}(f) + \operatorname{ord}(g).$$

روی حلقه $R[[x_۱,\ldots,x_n]]$ برای هر عنصر دلخواه f نرم را به صورت $|f| = ۲^{-\operatorname{ord}(f)}$ تعریف می‌کنیم (اثبات نرم بودن آن بسیار ساده است). به علاوه، در ادامه ثابت کرده‌ایم که $R[[x_۱,\ldots,x_n]]$ تحت این نرم کامل است. برای ساده‌تر شدن بحث، تعداد متغیرها را یکی گرفته‌ایم. فرض کنید f,g دو سری تک متغیره باشند. دقت کنید که $|f-g| < ۲^{-N}$ بدین معنی است که سریهای f_n, f_m تا قبل از توان N شبیه به هم هستند:

$$f = a_۰ + a_۱x + \cdots + a_{N-۱}x^{N-۱} + a_N x^N + \cdots$$

$$g = a_۰ + a_۱x + \cdots + a_{N-۱}x^{N-۱} + b_N x^N + \cdots$$

حال اگر (f_n) یک دنبالهٔ کشی باشد، فاصلهٔ جملات آن رفته رفته کمتر از ۲^{-N} ها می‌شود؛ یعنی میزان جملات شبیه به هم سریها بیشتر و بیشتر می‌شود. سری‌ای که از کنار هم نوشتن این جملات مشابه ایجاد می‌شود، حد f_n هاست.

لم ۱۰. فرض کنیم حلقه R با فرا نرم $|.|$ کامل باشد. اگر برای هر $x \in R$ داشته باشیم $|x| \le ۱$ آنگاه $M = \{x \in R \mid |x| < ۱\}$ یک ایده‌آل سره است (یعنی عناصری که در آن قرار دارند یکه نیستند).

اثبات. فرض کنیم $x \in M$ وارونی مانند $x^{-۱}$ داشته باشد. در این صورت $|xx^{-۱}| = |۱| = ۱$ که در تناقض با $|xx^{-۱}| \le |x||x^{-۱}| < ۱$ است. □

توجه داشته باشیم که لم قبل به این معنا نیست که تمام عناصر وارون ناپذیر حلقه R در M قرار دارند. در واقع ادعا نکردیم M ماکسیمال است.

۲.۵ لم هنسل

لم ۱۱. (لم هنسل). فرض کنیم R یک حلقه باشد که نسبت به فرا نرم $|.|$ کامل است. همچنین فرض کنیم برای هر عنصر $x \in R$ داشته باشیم $|x| \leq ۱$. اگر $f \in R[x]$ یک چندجمله‌ای باشد و $\alpha \in R$ وجود داشته باشد که

$$|f(\alpha)| < ۱ \ , \quad f'(\alpha) \in U(R)$$

(منظور از f' همان مشتق f است)، آنگاه $a \in R$ وجود دارد به طوری که $f(a) = ۰$ و $|a - \alpha| < ۱$.

اثبات. (مشابه روش درون‌یابی نیوتون) ابتدا قرار می‌دهیم $a_۰ = \alpha$. پس $|f(a_۰)| \leq \epsilon < ۱$ و $f'(a_۰)$ وارون پذیر است. اگر قرار دهیم $a_۱ = a_۰ - \frac{f(a_۰)}{f'(a_۰)}$ (دقت کنید که این عبارت را می‌توان نوشت زیرا $f'(a_۰)$ وارون‌پذیر است) آنگاه $|a_۱ - a_۰| < \epsilon$ (زیرا $|f'(a_۰)| = ۱$ و $|f(a_۰)| \leq \epsilon$). و با قرار دادن $h = -\frac{f(a_۰)}{f'(a_۰)}$ داریم

$$f(a_۱) = f(a_۰ + h) = f(a_۰) + f'(a_۰)h + h^۲(\ldots) + \cdots \quad (*)$$

برای توجیه این بسط تمرینی از کتاب سرج لنگ (صفحهٔ ۲۱۳) را در اینجا نوشته‌ام:

فرض کنید که f یک چندجمله‌ای تک متغیره روی یک میدان k باشد. فرض کنید X, Y دو متغیر باشند. در این صورت بسط تیلور

$$f(X + Y) = f(X) + \sum_{i=۱}^{n} \varphi(X)Y^i$$

را داریم که در آن $\varphi_i(X)$ یک چندجمله‌ای بر حسب X با ضرایب در k است. اگر مشخصهٔ k صفر باشد آنگاه

$$\varphi_i(X) = f^{(i)}(X)/i!.$$

به ادامهٔ اثبات می‌پردازیم: از آنجا که

$$f(a_۰ + h) = f(a_۰) + f'(a_۰)h = ۰$$

از عبارت $(*)$ نتیجه می‌گیریم $|f(a_۱)| < \epsilon^۲$. در مرحله دوم قرار می‌دهیم $a_۲ = a_۱ - \frac{f(a_۱)}{f'(a_۱)}$. توجه کنید که $f'(a_۱)$ وارون پذیر است، زیرا $a_۱ \equiv_M a_۰$ و از این رو $f'(a_۱) \equiv_M f'(a_۰)$ که $M = R - U(R)$. در واقع هر توانی از $a_۱$ هم‌ارز با همان توان از $a_۰$ به پیمانهٔ ایده‌آل M است و از این رو چندجمله‌های بر حسب $a_۱$ با چندجمله‌ایهای بر حسب $a_۰$ هم‌ارز هستند.

مانند قبل می‌توانیم نتیجه بگیریم $|a_۲ - a_۱| < \epsilon^۲$ و $|f(a_۲)| < \epsilon^۴$. با تکرار این روش به یک دنباله $a_۰ \ a_۱ \ a_۲ \ \cdots$ می‌رسیم که فاصله اعضای دنباله از هم کمتر از $\epsilon^{۲n}$ است. 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

$$f(a) = f(\lim_{n\to\infty} a_n) = \lim_{n\to\infty} f(a_n) = ۰.$$

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. □

لم ۱۲. فرض کنیم $(R, |.|)$ یک حلقه نرم دار غیر ارشمیدسی باشد. اگر R کامل و $a \in R$ به گونه‌ای باشد که $|a| < ۱$، آنگاه $۱ - a$ وارون پذیر است.

اثبات. قرار می‌دهیم $S_n = \sum_{i=۰}^{n} a^i$. چون $\lim_{n\to\infty} |a|^n = ۰$، نتیجه می‌گیریم عنصر $\sum_{i=۰}^{\infty} a^i$ در حلقه موجود است. (قبلا نشان داده بودیم که $\sum a_n$ موجود است اگروتنهااگر $\lim a_n = ۰$.) از طرفی

$$(\sum_{i=۰}^{\infty} a^i) \cdot (۱ - a) = ۱$$

□

قضیه ۲۶. فرض کنیم R یک حلقه و $R[[x_۱, \ldots, x_n]]$ حلقه سری‌های توانی n-متغیره نظیر آن باشد. در این صورت عناصری در $R[[x_۱, \ldots, x_n]]$ معکوس پذیراند که جمله ثابت آن‌ها در R معکوس پذیر باشد.

اثبات. برای سادگی، اثبات را تنها در سری‌های توانی تک متغیره بیان می‌کنیم. فرض کنیم $f = \sum_{i=0}^{n} a_i x^i \in R[[x]]$، چون a_0 وارون پذیر است می‌توانیم از آن فاکتور بگیریم. بنابراین $f = a_0(1 + g)$ به طوری که $g \in R[[x]]$. با توجه به به نرم تعریف شده روی حلقه سری‌های توانی داریم $|g| < 1$. پس بنا به لم قبل $1 + g$ وارون پذیر است و این یعنی f وارون پذیر است. □

پس به طور خاص می‌توان گفت، اگر K یک میدان باشد آنگاه تمامی عناصر $K[[x_1, \ldots, x_n]]$ که دارای جمله ثابت هستند وارون پذیراند. به بیان دیگر عناصری در $K[[x_1, \ldots, x_n]]$ وارون پذیر هستند که نرم آن‌ها برابر با یک باشد. پس $K[[x_1, \ldots, x_n]]$ یک حلقه موضعی با ایده‌آل ماکسیمال $M = \{f \in K[[x_1, \ldots, x_n]] \mid |f| < 1\}$ است.

تعریف ۴۸. (حلقه هنسلی). فرض کنید (R, M) یک حلقهٔ موضعی باشد و $k = R/M$. می‌گوییم R یک حلقهٔ موضعی هنسلی است هرگاه برای هر $f \in R[x]$ اتفاق زیر رخ دهد: اگر $\alpha \in R$ موجود باشد به طوری که $f(\alpha) \in M$ و $f'(\alpha) \notin M$، آنگاه $a \in R$ موجود باشد که $f(a) = 0$ و $\bar{a} = \alpha$ به پیمانه M.

در ادامه در مورد p-ادیک‌ها صحبت خواهیم کرد که مثال‌های مهمی از حلقه‌های نرم دار هنسلی هستند.

۳.۵ حلقهٔ پی‌ادیکها

در جلسات قبل دیدیم که هر $\mathbb{Z}/p^k\mathbb{Z}$ یک حلقهٔ موضعی است. به $\lim_{k\to\infty} \mathbb{Z}/\mathbb{Z}_k$ حلقهٔ پی‌ادیکها گفته می‌شود. در این فصل این مفهوم را به طور دقیق توضیح داده‌ایم.

تعریف ۴۹. فرض کنیم a یک عدد صحیح باشد. در این صورت برای عدد اول p قرار می‌دهیم $V_p(a) = n$ اگر و تنها اگر $p^n \mid a$ و $p^{n+1} \nmid a$.

برای مثال اگر $a = a_0 + a_1 p$ آنگاه $V_p(a) = 0$ و در صورتی که $a = a_2 p^2 + a_3 p^3$ قرار می‌دهیم $V_p(a) = 2$.

لم ۱۳. فرض کنیم p یک عدد اول باشد. نگاشت $V_p : \mathbb{Z} \longrightarrow \mathbb{Z}$ با ضابطه معرفی شده در تعریف بالا دارای ویژگی‌های زیر است،

۱) $V_p(a + b) \geq \min\{V_p(a), V_p(b)\}$

۲) $V_p(a \cdot b) = V_p(a) + V_p(b)$

۳) $V_p(1) = 0$.

همچنین نگاشت $|.|_p : \mathbb{Z} \longrightarrow \mathbb{R}$ با ضابطه $|a|_p = 2^{-V_p(a)}$، یک نرم غیر ارشمیدسی روی حلقه $\mathbb{Z}$ است.

می‌دانیم که میدان $\mathbb{R}$ کامل شده میدان $\mathbb{Q}$ است. به طور دقیق‌تر، $\mathbb{R}$ اجتماعی از $\mathbb{Q}$ و حد دنباله‌های کشی موجود در آن است. در تعریف زیر به طور مشابه برای حلقه $\mathbb{Z}$ به همراه نُرم پی‌ادیک بالا، یک حلقه کامل شده ارائه می‌دهیم.

تعریف ۵۰. برای یک عدد اول p، کامل شده حلقه $\mathbb{Z}$ نسبت به نرم $|.|_p$ را با $\mathbb{Z}_p$ نمایش می‌دهیم و آن را حلقه اعداد صحیح p-ادیک می‌نامیم.

لم ۱۴. هر عنصر $\mathbb{Z}_p$ دارای یک نمایش یکتا به صورت $\sum_{i=0}^{\infty} a_i p^i$ است به طوری که برای هر اندیس i، $a_i \in \{0, 1, \ldots, p-1\}$.

اثبات. فرض کنیم a عنصری در $\mathbb{Z}_p$ باشد. در این صورت دنباله کُشی $(b_n)_{n\in\mathbb{N}}$ در $\mathbb{Z}$ وجود دارد که به a همگراست. از آنجا که $(b_n)_{n\in\mathbb{N}}$ یک دنبالهٔ کشی است، برای هر $n \in \mathbb{N}$ دلخواه عدد $N_n \in \mathbb{N}$ وجود دارد که

$$|b_n - b_m| < 2^{-n}$$

برای هر $n, m > N_n$. به بیان دیگر، با توجه به تعریف نُرم، برای هر $n, m > N_n$ داریم

$$b_n \overset{p^n}{\equiv} b_m.$$

پس اگر $m,n \geq N_1$ در این صورت $a_0 \in \{0,1,\dots,p-1\}$ وجود دارد که $b_n \overset{p}{\equiv} b_m \overset{p}{\equiv} a_0$. مشابهاً برای $m,n > N_2$ داریم $b_n \overset{p^2}{\equiv} b_m \overset{p^2}{\equiv} a'_1$ که در آن $a'_1 \in \{0,1,\dots,p^2-1\}$. اما a'_1 را می‌توان به صورت $a_0 + a_1 p$ نوشت و a_1 از اینجا حاصل می‌شود. به طور مشابه، $a'_2 \in \{0,\dots,p^3-1\}$ موجود است که برای هر $n,m > N_3$ داریم $b_n \overset{p^3}{\equiv} b_m \overset{p^3}{\equiv} a'_2$. اما a'_2 را نیز می‌توان به صورت $a_0+a_1p+a_2p^2$ نوشت. سایر a_i ها به همین طریق به دست می‌آیند. □

لم ۱۵. 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 وارون پذیر $\mathbb{Z}_p$ دقیقا 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 $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ و $|a| = 1$. بنابراین $p \nmid a_0$ و این یعنی a_0 در F_p وارون دارد. اگر b وارون a_0 در F_p باشد آنگاه $q \in \mathbb{Z}$ وجود دارد به طوری که $a_0 b = pq + 1$. b را در a ضرب می‌کنیم،

$$ab = a_0 b + b\sum_{i=1}^{\infty} a_i p^i = 1 + pq + b\sum_{i=1}^{\infty} a_i p^i$$

.

واضح است که $|pq + b\sum_{i=1}^{\infty} a_i p^i| < 1$، بنابراین ab و در نتیجه a در $\mathbb{Z}_p$ وارون پذیر است. پس $p\mathbb{Z}_p$ ایده‌آل ماکسیمال $\mathbb{Z}_p$ است. همچنین بنا به لم هنسل به وضوح، حلقه موضعی $\mathbb{Z}_p$ هنسلی است. □

تذکر ۳۰. نگاشت $\varphi : \mathbb{Z}_p \longrightarrow F_p$ با ضابطه $\varphi(\sum_{i=1}^{\infty} a_i p^i) = a_0$ همریختی است و $Ker(\varphi) = p\mathbb{Z}_p$. بنابراین $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong F_p$.

۴.۵ برکشیدنِ میدان پیمانه‌ها در حلقه‌های هنسلی

تمرین ۱۱. اگر مشخصه میدان K صفر باشد، $f \in K[x]$ تحویل ناپذیر و a در یک توسیع از K باشد به طوری که $f(a) = 0$ آنگاه $f'(a) \neq 0$.

فرض کنیم (R, M) یک حلقه موضعی هنسلی باشد و $E \subset R$ و E یک میدان باشد. همچنین فرض کنیم مشخصه میدان $K = \frac{R}{M}$ صفر باشد. در این صورت اگر $\overline{E}$ تصویر E تحت همریختی $i : E \longrightarrow \frac{R}{M}$ با ضابطه $i(a) = \overline{a} = a + M$ باشد آنگاه $\overline{E}$ را می‌توان به صورت زیر توسیع داد. فرض کنیم $\overline{E} \neq K$ و $y \in K \setminus \overline{E}$ دو حالت داریم:

۱) y روی $\overline{E}$ متعالی باشد. می‌دانیم که عنصر a در R وجود دارد که $\overline{a} = y$. a روی E متعالی است، زیرا اگر a جبری باشد آنگاه y نیز جبری می‌شود و این تناقض است. از آنجایی که $E \cong \overline{E}$ داریم $E(a) \cong \overline{E}(y)$. یعنی می‌توان تصویر E را بزرگتر کرد.

۲) y روی $\overline{E}$ جبری باشد. اگر $\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n$ چندجمله‌ای تحویل ناپذیر باشد که $\overline{f}(y) = 0$. از تمرین قبل نتیجه می‌گیریم $\overline{f'}(y) \neq 0$. بنا به هنسلی بودن R عنصر a در آن وجود دارد که $\overline{a} = y$ و $f(a) = 0$ پس $E(a) \cong \overline{E}(y)$.

قضیه ۲۷. فرض کنیم (R, M) هنسلی و $K = \frac{R}{M}$ دارای مشخصه صفر باشد. در این صورت برداشتی از K در R موجود است. یعنی یک میدانِ $E \subseteq R$ موجود است به طوری که $\bar{E} = K$.

اثبات. مجموعه

$$\mathcal{A} = \{f : E \longrightarrow K \mid f \text{ : نشاندن}, \ E \subseteq R, \ E \text{ : میدان}\}$$

ناتهی است. برای مثال نشاندن $f : \mathbb{Q} \longrightarrow K$ با ضابطه $f(n) = n \cdot 1_K$ به $\mathcal{A}$ تعلق دارد. مشابه اثبات‌های گذشته، ترتیب شمول را روی مجموعه $\mathcal{A}$ در نظر می‌گیریم. تحت این ترتیب هر زنجیر صعودی در $\mathcal{A}$ دارای کران بالا و بنابراین $\mathcal{A}$ دارای یک عنصر ماکسیمال مانند $F : E_1 \longrightarrow K$ است. اگر F پوشا نباشد، آنگاه $y \in K \setminus \overline{E_1}$ وجود دارد و بنا به قضیه قبل E_1 توسیع می‌یابد. در واقع یک نشاندن مانند $G : E_1(a) \longrightarrow K$ وجود دارد که این در تناقض با ماکسیمال بودن F است. بنابراین $\overline{E_1} = K$. □

نتیجه ۱۱. فرض کنیم (R, M) یک حلقه هنسلی و مشخصه میدان $K = \frac{R}{M}$ صفر باشد. اگر $X = (x_1, \ldots, x_n)$ و $f_1, \ldots, f_k \in R[X]$ آنگاه هر جواب دستگاه

$$\overline{f}_1(X) = 0 \ \wedge \ \cdots \ \wedge \ \overline{f}_k(X) = 0 \tag{۱.۵}$$

در K دارای یک برداشت به یک جواب در R است.

اثبات. فرض کنید $E \subseteq R$ به گونه‌ای باشد که $E \cong K$ (مطابق قضیهٔ قبل). پس اگر $\overline{y}$ جواب دستگاه (۱.۵) در K باشد آنگاه تصویر $\overline{y}$ در E همان جواب دستگاه در R است. □

۵.۵ قضیهٔ گرین‌لیف، اکس، کوچن

قضیه ۲۸ (گرین‌لیف، اکس‌کوچن). فرض کنیم $X = (x_1, \ldots, x_n)$ و $f_1, \ldots, f_k \in \mathbb{Z}[X]$. در این صورت برای همه اعداد اول p (مگر تعدادی متناهی) هر جواب برای تصویر دستگاه

$$f_1(X) = 0 \ \wedge \ \cdots \ \wedge \ f_k(X) = 0 \tag{۲.۵}$$

در F_p قابل ارتقاء به یک جواب در $\mathbb{Z}_p$ است.

توجه کنیم که در این قضیه اگرچه F_p با $\frac{\mathbb{Z}_1}{p\mathbb{Z}_1}$ یکریخت است اما مشخصه آن ناصفر است و بنابراین نمی‌توان برای اثبات آن از نتیجه قبل استفاده کرد. تکنولوژی این اثبات، به کارگیری قضیهٔ فشردگی در نظریهٔ مدلهاست.

اثبات. در زبان L_{ring}، تئوری حلقه‌های موضعی هنسلی با مشخصه پیمانه‌ای صفر به صورت

$$T = T_{ring} \cup T_{local} \cup T_H \cup \{(\neg\exists a \quad a \cdot 1 = 1), (\neg\exists a \quad a \cdot (1 + 1) = 1), \ldots\}$$

است که در آن

- منظور از T_{local}، تئوری حلقه‌های موضعی به شکل

$$T_{local} = T_{ring} \cup \{\forall x \ \forall y \ \ (\neg\exists z \quad x \cdot z = 1) \wedge (\neg\exists z \quad y \cdot z = 1) \longrightarrow (\neg\exists z \quad (x + y) \cdot z = 1)\}$$

- و منظور از T_H تئوری حلقه‌های هنسلی به صورت زیر است

$$T_H = T_{ring} \cup \{\forall a_0 \ \forall a_1 \ \ (\exists \alpha \ (\neg\exists b \ \ b \cdot (a_0 + a_1\alpha) = 1 \ \wedge \ \exists b \ \ b \cdot a_1 = 1) \to \exists a \ a_0 + a_1 a = 0 \ \wedge \ \neg\exists b \cdot (\alpha - a) = 1),$$
$$\forall a_0 \ \forall a_1 \ \forall a_2 \ \ (\exists \alpha \ (\neg\exists b \ \ b \cdot (a_0 + a_1\alpha + a_2\alpha^2) = 1 \ \wedge \ \exists b \ \ b \cdot (a_1 + a_2\alpha) = 1) \longrightarrow$$
$$\exists a \ a_0 + a_1 a + a_2 a^2 = 0 \ \wedge \ \neg\exists b \cdot (\alpha - a) = 1), \ldots\}$$

اگر

$$\varphi : \exists a \ \ (\neg\exists b \ b \cdot f_1(a) = 1) \ \wedge \cdots \wedge \ (\neg\exists b \ b \cdot f_k(a) = 1) \Longrightarrow \exists a \ \ f_1(a) = 0 \ \wedge \ \cdots \ \wedge f_k(a) = 0$$

(در واقع جمله بالا می‌گوید اگر دستگاه (۲.۵) در $\frac{R}{M}$ جواب داشته باشد آنگاه یک جواب در R دارد) آنگاه $T \models \varphi$. بنا به فشردگی یک زیرمجموعه متناهی Δ از T وجود دارد که $\Delta \models \varphi$. پس یعنی اگر Δ' تئوری حلقه‌های هنسلی با مشخصه پیمانه‌ای p باشد هم $\Delta' \models \varphi$. بنابراین برای pهای به اندازه کافی بزرگ داریم $\mathbb{Z}_p \models \varphi$. □

قضیه ۲۹ (اکس ـ کوچن). فرض کنیم φ یک جمله در زبان L_{ring} باشد. در این صورت برای همه pهای اول (مگر تعدادی متناهی) داریم،

$$\mathbb{Z}_p \models \varphi \Longleftrightarrow F_p \models \varphi.$$

اثبات. برای مشاهده اثبات می‌توانید به منبع اصلی درس مراجعه کنید. □

۶.۵ توضیحی کوتاه دربارهٔ توسیعهای جدائی‌پذیر

تعریف ۵۱. فرض کنیم K یک میدان باشد. توسیع $K \subseteq L$ را یک توسیع جدایی پذیر می‌نامیم هرگاه هر عنصر $a \in L \setminus K$ روی K جبری باشد و چندجمله‌ای مینیمال a روی K در K^{ac} به عوامل درجهٔ ۱ تجزیه شود. یعنی چندجمله‌ای مورد نظر دارای ریشهٔ تکراری نباشد.

لم ۱۶. فرض کنیم K میدان باشد و $f \in K[x]$. عنصر $a \in K^{ac}$ یک ریشه مضاعف برای f است اگر و تنها اگر $f(a) = f'(a) = ۰$.

اثبات. اگر a یک ریشه مضاعف f باشد آنگاه $f = (x-a)^۲ + g(x)$ و به وضوح $f(a) = f'(a) = ۰$. برعکس، چون $f(a) = ۰$ پس $f = (x-a)g(x)$. بنابراین $f' = g(x) + (x-a)g'(x)$ و از آنجایی که $f'(a) = ۰$ نتیجه می‌گیریم $g(a) = ۰$. پس f باید شامل عامل $(x-a)^۲$ باشد. □

گزاره ۱۰. فرض کنیم K یک میدان با مشخصه صفر و f یک چندجمله‌ای تحویل ناپذیر در $K[x]$ باشد. در این صورت f در K^{ac} ریشه مضاعف ندارد. به عبارت دیگر اگر مشخصه K صفر باشد و L توسیع جبری K باشد آنگاه توسیع L جدایی پذیر است.

اثبات. فرض کنیم a ریشه چندجمله‌ای تحویل ناپذیر f در $K[x]$ باشد. در واقع f یک چندجمله‌ای با حداقل درجه در $K[x]$ است که $f(a) = ۰$. اگر a ریشه مضاعف f باشد آنگاه $f'(a) = ۰$. اما درجه f' از درجه f کمتر است (چون مشخصه میدان صفر است) و این در تناقض با مینیمال بودن f است. □

۷.۵ میدان $\mathbb{Q}_p$

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

$$V_p(x) = n \iff a = p^n(\frac{r}{s}) \quad s.t \quad p \nmid r,\ p \nmid s.$$

به عبارت دیگر اگر $x = \frac{a}{b}$ 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 آن را میدان p-ادیک‌ها می‌نامیم. پس عناصر $\mathbb{Q}_p$ را می‌توان حد دنباله‌های کوشی از اعضای $\mathbb{Q}$ با نرم $|.|_p$ در نظر گرفت. همچنین واضح است که $\mathbb{Z}_p \subset \mathbb{Q}_p$.

فرض کنیم $x \in \mathbb{Q}_p$ عنصری در $\mathbb{Q}$ باشد. اگر $V_p(x) = n$ مطابق آنچه گفته شد $x = p^n\frac{r}{s}$ که $p \nmid r$ و $p \nmid s$. r و s دارای تجزیه در $\mathbb{Z}_p$ به صورت

$$r = a_۰ + a_۱x + \cdots + a_nx^n, \qquad s = b_۰ + b_۱x + \cdots + b_mx^m$$

هستند. بنابراین r و s و در نتیجه $\frac{r}{s}$ وارون پذیر است. یعنی $x = p^nu$ است که در آن u عنصری وارون پذیر در $\mathbb{Z}_p$ است. همین، برای هر عنصر متعلق به $\mathbb{Q}_p$ نیز برقرار است:

لم ۱۷. اگر x عنصری ناصفر در $\mathbb{Q}_p$ باشد آنگاه $x = p^nu$ به طوری که u در $\mathbb{Z}_p$ وارون پذیر است.

اثبات. اگر $x \in \mathbb{Q}_p$ عنصری ناصفر باشد آنگاه حد یک دنباله از عناصرِ $\mathbb{Q}$ مانند $(x_i)_{i\in\mathbb{N}}$ با نرم $|.|_p$ است. با توجه به گفتهٔ بالا، هر عنصر x_i را می‌توان به صورت $x_i = p^{k_i}u_i$ نوشت که در آن $u_i \in \mathbb{Z}_p$ عنصری وارون پذیر است. چون x حد این دنباله است، نرم عناصر این دنباله باید در نزدیکی نرمِ x باشد. دقت کنید که نرم u_i ها برابر با یک است. پس $N \in \mathbb{N}$ وجود دارد که برای $i \geq N$ اعضای دنباله در یک توان مانند k مشترک هستند. پس $x = p^k \lim_{i\to\infty} u_i$. اگر $u = \lim_{i\to\infty} u_i$ آنگاه $x = p^ku$ که u در $\mathbb{Z}_p$ وارون پذیر است.

□

نتیجه ۱۲.

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq ۱\}.$$

۸.۵ تعریف‌پذیری $\mathbb{Z}_p$ در $\mathbb{Q}_p$.

قضیه ۳۰. مجموعه $\mathbb{Z}_p$ در $\mathbb{Q}_p$ تعریف پذیر است.

اثبات. برای $p \neq 2$ نشان می‌دهیم

$$\forall x \in \mathbb{Q}_p \qquad x \in \mathbb{Z}_p \iff \exists y \quad 1 + px^2 = y^2.$$

اگر رابطه بالا ثابت شود علاوه بر اینکه فرمولی که به وسیله آن می‌توان مجموعه $\mathbb{Z}_p$ را تعریف کرد پیدا کرده‌ایم، به نوعی ترتیب در $\mathbb{Q}_p$ دست پیدا می‌کنیم.

- (اثبات $\Rightarrow$) ابتدا نشان می‌دهیم اگر $x \in \mathbb{Z}_p$ آنگاه x در معادله صدق می‌کند. قرار می‌دهیم $f(y) = y^2 - (1 + px^2)$. در میدان پیمانه‌های F_p داریم $\overline{f}(y) = y^2 - 1$. چون $\overline{f}(1) = 0$ و $\overline{f}(1) \neq 0$ بنا به هنسلی بودن $\mathbb{Z}_p$ عنصر y وجود دارد که $y^2 = 1 + px^2$.
- (اثبات $\Leftarrow$) فرض کنیم x در معادله بالا صدق کند. نشان می‌دهیم $|x|_p \leq 1$. اگر چنین نباشد، یعنی $|x|_p > 1$ یا به عبارت دیگر $V_p(x) < 0$، آنگاه از معادله بالا و ویژگی‌های نگاشت V_p تساوی $1 + 2V_p(x) = 2V_p(y)$ حاصل می‌شود که تناقض است.

پس در حالتی که $p \neq 2$، مجموعه $\mathbb{Z}_p$ با فرمول $\varphi(x) : \exists y \ 1 + px^2 = y^2$ در $\mathbb{Q}_p$ تعریف پذیر است. اثبات تعریف پذیری $\mathbb{Z}_p$ را در حالت $p = 2$ به عنوان تمرین رها می‌کنیم. □

فصل ۶

میدانهای ارزیابی

تدریس: محسن خانی
گردآوری: فاطمه اکبری

تعریف ۵۲. فرض کنیم Γ یک گروه مرتب آبلی باشد. اگر K یک میدان باشد نگاشت $V : K \longrightarrow \Gamma$ را یک نگاشت ارزیابی می‌نامیم هرگاه برای هر $x, y \in K$،

۱) $V(x+y) \geq \min\{V(x), V(y)\}$

۲) $V(x \cdot y) = V(x) + V(y)$

۳) $x = ۰ \Leftrightarrow V(x) = \infty$

تذکر ۳۱. اگر V یک نگاشت ارزیابی باشد، موارد زیر به طور مستقیم از تعریف نتیجه می‌شوند،

- $V(۱) = V(-۱) = ۰$
- برای هر x، $V(x) = V(-x)$
- برای هر x، $V(x^{-۱}) = -V(x)$

لم ۱۸. فرض کنیم Γ یک گروه مرتب آبلی، K یک میدان و $V : K \longrightarrow \Gamma$ یک نگاشت ارزیابی باشد. اگر برای $x, y \in K$ داشته باشیم $V(x) \neq V(y)$ آنگاه $V(x+y) = \min\{V(x), V(y)\}$.

اثبات. فرض کنیم $V(x) > V(y)$ در این صورت

$$V(x+y) \geq V(y) = V(x+y-x) \geq \min\{V(x+y), V(x)\} = V(x+y).$$

بنابراین $V(x+y) = V(y)$.

□

۱.۶ حلقه‌های ارزیاب و ارتباط ارزیابی با حلقه‌های موضعی

تعریف ۵۳. فرض کنیم K یک میدان، Γ یک گروه آبلی مرتب و $V : K \longrightarrow \Gamma$ یک نگاشت ارزیابی باشد. حلقه ارزیاب نظیر نگاشت V را با O_V نمایش داده و به صورت زیر تعریف می‌کنیم،

$$O_V = \{x \in K \mid V(x) \geq ۰\}.$$

تذکر ۳۲. واضح است که برای هر عنصر $x \in K$، یا $x \in O_V$ و یا $x^{-1} \in O_V$. زیرا اگر $V(x) < 0$ آنگاه $V(x^{-1}) > 0$.

لم ۱۹. حلقه ارزیاب $O_V \subseteq K$ معرفی شده در تعریف بالا، یک حلقه موضعی است و ایده‌آل ماکسیمال آن برابر است با

$$M_V = \{x \in K \mid V(x) > 0\}.$$

اثبات. اثبات زیرحلقه بودن O_V در K و ایده‌آل بودن M_V در O_V، از ویژگی‌های نگاشت V به سادگی حاصل می‌شود. ثابت می‌کنیم M_V تنها ایده‌آل ماکسیمال O_V است. اگر $x \in O_V$ به گونه‌ای باشد که $V(x) = 0$ آنگاه $V(x^{-1})$ نیز صفر است و این یعنی x^{-1} به O_V تعلق دارد. اما اگر $V(x) > 0$ آنگاه $V(x^{-1}) < 0$ و بنابراین x^{-1} در O_V نیست. پس عناصر غیر وارون پذیر O_V عناصری هستند که مقدار نگاشت ارزیابی در آن‌ها اکیدا بزرگتر از صفر باشد. □

تعریف ۵۴. میدان $K_V = \frac{O_V}{M_V}$ را میدان پیمانه‌های نگاشت ارزیابی V می‌نامیم.

در ادامه به بیان مثال‌هایی از نگاشت ارزیابی می‌پردازیم.

مثال ۴۹. فرض کنیم $K = \mathbb{C}(t)$. برای هر $\frac{g(t)}{h(t)} \in K$، قرار می‌دهیم $V(\frac{g(t)}{h(t)}) = n$ اگر و تنها اگر $f = t^n \cdot \frac{g'(t)}{h'(t)}$ به طوری که $g'(0), h'(0) = 0$ (در واقع $V : \mathbb{C}(t) \longrightarrow \mathbb{Z}$ یک نگاشت ارزیابی است). در این صورت

$$O_V = \{\frac{g}{h} \mid g, h \in \mathbb{C}(t), \quad h(0) \neq 0\}.$$

به عبارت دیگر O_V همان موضعی سازی $\mathbb{C}(t)_{t\mathbb{C}(t)}$ است. همچنین

$$M_V = \{\frac{g}{h} \mid g, h \in \mathbb{C}(t), \quad h(0) \neq 0, \ g(0) = 0\}.$$

در واقع M_V برابر است با $t\mathbb{C}(t)_{t\mathbb{C}(t)}$. نگاشت $\varphi : O_V \longrightarrow \mathbb{C}$ با ضابطه $\varphi(\frac{g(t)}{h(t)}) = \frac{g(0)}{h(0)}$ همریختی است و $Ker(\varphi) = M_V$. پس بنا به قضیه اول یکریختی، $K_V = \frac{O_V}{M_V} \cong \mathbb{C}$.

مثال ۵۰. برای یک عدد اول p، فرض کنیم $K = \mathbb{Q}_p$. نگاشت ارزیابی $V_p : K \longrightarrow \mathbb{Z}$ را با ضابطه $V_p(x) = n$ تعریف می‌کنیم هرگاه $x = p^n u$ به طوری که $u \in U(\mathbb{Z}_p)$. در این صورت

$$O_{V_p} = \{x \in \mathbb{Q}_p \mid V_p(x) \geq 0\} = \mathbb{Z}_p$$

و

$$M_{V_p} = \{x \in \mathbb{Q}_p \mid V_p(x) > 0\} = p\mathbb{Z}_p.$$

همچنین $K_{V_p} = \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong F_p$.

مثال ۵۱. فرض کنیم $K = \mathbb{Q}$ و p یک عدد اول باشد. نگاشت ارزیابی $V_p : K \longrightarrow \mathbb{Z}$ را باضابطه $V_p(\frac{a}{b}) = n$ تعریف می‌کنیم هرگاه $\frac{a}{b} = p^n \cdot \frac{a'}{b'}$ به طوری که $p \nmid a'$ و $p \nmid b'$. به عنوان تمرین O_{V_p}، M_{V_p} و K_{V_p} را برای این مثال بیابید.

تعریف ۵۵. حلقه A در میدان K را یک حلقه ارزیاب برای K می‌نامیم هرگاه برای هر $x \in K$، یا $x \in A$ و یا $x^{-1} \in A$.

مثال ۵۲. اگر یک نگاشت ارزیابی V روی میدان K تعریف کنیم، آنگاه O_V مثالی از یک حلقه ارزیاب است.

قضیه ۳۱. هر حلقه ارزیاب ناشی از یک نگاشت ارزیابی است. به طور دقیق‌تر، اگر K یک میدان شامل حلقه ارزیاب A باشد، آنگاه یک گروه مرتب مانند Γ و یک ارزیابی $V : K \longrightarrow \Gamma$ وجود دارد که $A = O_V$.

اثبات. روی عناصر K رابطه هم ارزی زیر را در نظر می‌گیریم،

$$x \sim y \Leftrightarrow xy^{-1} \in A \ \& \ yx^{-1} \in A$$

یا به عبارت دیگر $x \sim y$ اگر و تنها اگر $xy^{-1} \in U(A)$. مجموعه $\Gamma = \{[x] \mid x \in K\}$ همراه با عمل ضرب میدان یک گروه است. در واقع $\Gamma = \frac{K \setminus \{0\}}{U(A)}$. روی Γ ترتیب را به صورت زیر تعریف می‌کنیم،

$$[x] > [y] \Leftrightarrow xy^{-1} \in A \ \& \ yx^{-1} \notin A$$

و

$$[x] = [y] \Leftrightarrow xy^{-1} \in A \ \& \ yx^{-1} \in A.$$

در این صورت نگاشت $V : K \longrightarrow \Gamma$ با ضابطه $V(x) = [x]$ یک نگاشت ارزیابی است و $A = O_V = \{x \in K \mid V(x) \geq 0_\Gamma\}$. □

تذکر ۳۳. نگاشت ارزیابی که در قضیه قبل معرفی کردیم یکتاست.

نتیجه ۱۳. اگر K یک میدان و $A \subseteq K$ یک حلقه ارزیاب باشد آنگاه A یک حلقه موضعی است.

تعریف ۵۶. به زوج (K, A) یک میدان ارزیابی گوییم هرگاه $A \subseteq K$ یک حلقه ارزیاب باشد.

تعریف ۵۷. فرض کنیم (K, A) یک میدان ارزیابی باشد. همچنین فرض کنیم $K \subseteq L$ یک توسیع میدانی و B یک حلقه ارزیاب برای L باشد. گوییم B بر A چیره است اگر $A = B \cap K$.

تذکر ۳۴. تحت مفروضات تعریف بالا، اگر B بر A چیره باشد آنگاه نتایج زیر به طور مستقیم حاصل می‌شوند،

- $U(A) = K \cap U(B)$.
- $M_A = K \cap M_B$. (منظور از M_A و M_B به ترتیب ایده‌آل‌ها ماکسیمال A و B است).
- نگاشت ارزیابی $V_B : K \longrightarrow \Gamma_B$ توسیع نگاشت ارزیابی $V_A : K \longrightarrow \Gamma_A$ است.
- نگاشت‌های $\varphi_1 : \Gamma_1 \longrightarrow \Gamma_2$ و $\varphi_2 : \frac{A}{M_A} \longrightarrow \frac{B}{M_B}$ نشاندن هستند.

۲.۶ قضیهٔ چیرگی به همراه مقدماتی از جبر جابه‌جائی

تعریف ۵۸. فرض کنیم A و B دو دامنه صحیح باشند که $A \subseteq B$. عنصر $b \in B$ را روی A صحیح می‌نامیم هرگاه $a_0, a_1, \ldots, a_{n-1} \in A$ موجود باشند به طوری که

$$b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0.$$

همچنین گوییم B روی A صحیح است هرگاه هر عنصر B روی A صحیح باشد.

لم ۲۰. فرض کنیم A و B دو دامنه صحیح باشند که $A \subseteq B$ و $b \in B$. در این صورت موارد زیر با هم معادل هستند.

۱) b روی A صحیح است.

۲) $A[b]$ (حلقه تولید شده توسط A و b) یک A-مدول متناهیا تولید شده است.

۳) $A[b]$ زیر مدول یک A-مدول متناهیا تولید شده است.

(باید توجه داشته باشیم که در حالت کلی، زیر مدول‌های یک مدول متناهیا تولید شده لزوما متناهیا تولید شده نیستند. برای مثال، هر حلقه R یک R-مدول است که توسط 1_R تولید می‌شود. اما هر ایده‌آل R که زیر مدولی از آن است لزوما متناهیا تولید شده نیست).

اثبات. اثبات (۲ ⇒ ۱) بسیار ساده و اثبات (۳ ⇒ ۲) واضح است. برای بیان اثبات (۱ ⇒ ۳) در این درس مجالی نیست. بنابراین آن را بدون اثبات می‌پذیریم! □

نتیجه ۱۴. فرض کنیم A، B و C دامنه صحیح باشند به طوری که C روی B و B روی A صحیح باشد. در این صورت C روی A صحیح است.

اثبات. فرض کنیم $c \in C$. C روی B صحیح است، پس عناصر $b_0, b_1, \ldots, b_{n-1} \in B$ وجود دارند که

$$c^n = b_{n-1}c^{n-1} + \cdots + b_1 c + b_0.$$

بنابراین $A[c] \subseteq A[b_0, \ldots, b_{n-1}, c, c^2, \ldots, c^n]$. از طرفی B روی A صحیح است. یعنی هر یک از b_iها دارای نمایش خطی از عناصر A هستند. بنابراین یک A-مدول متناهیا تولید شده وجود دارد که $A[b_0, \ldots, b_{n-1}, c, c^2, \ldots, c^n]$ و در نتیجه $A[c]$ زیر مدول آن است. پس طبق لم قبل C روی A صحیح است. □

لم ۲۱. فرض کنیم B یک دامنه صحیح و شامل دامنه صحیح A باشد. اگر B روی A صحیح باشد، آنگاه B میدان است اگر و تنها اگر A میدان باشد.

اثبات. فرض کنیم B میدان باشد. اگر a عنصری در A باشد آنگاه چون B میدان است، a^{-1} در B قرار دارد. از طرفی B روی A صحیح است، یعنی عناصر $c_0, c_1, \ldots, c_{n-1} \in A$ وجود دارند که

$$a^{-n} = c_{n-1}a^{-n+1} + \cdots + c_1 a^{-1} + c_0.$$

دو طرف تساوی بالا را در a^n ضرب می‌کنیم. بنابراین

$$a^{-1} = c_{n-1}a + \cdots + c_1 a^{n-1} + c_0 a^n.$$

سمت راست این تساوی به A تعلق دارد و بنابراین a^{-1} در A است. برعکس، فرض کنیم A میدان باشد. اگر $b \in B$، آنگاه b روی A صحیح و بنابراین $A[b]$ یک A-مدول متناهیا تولید شده است. از طرفی چون A میدان است $A[b]$ یک فضای برداری متناهیا تولید شده است. پس نگاشت $\varphi : A[b] \longrightarrow A[b]$ با ضابطه $\varphi(z) = bz$ یک تبدیل خطی پوشاست. بنابراین $c \in A[b]$ وجود دارد که $bc = 1$ و این یعنی B میدان است. □

تعریف ۵۹. فرض کنیم دامنه صحیح B شامل دامنه صحیح A باشد. اگر P یک ایده‌آل اول در A و Q یک ایده‌آل اول در B باشد، گوییم Q بر P چیره است هرگاه $A \cap Q = P$.

قضیه ۳۲. فرض کنیم دامنه صحیح B شامل دامنه صحیح A و B روی A صحیح باشد، P یک ایده‌آل اول در A و Q یک ایده‌آل اول در B باشد. اگر Q بر P چیره باشد آنگاه Q ماکسیمال در B است اگر و تنها اگر P در A ماکسیمال باشد.

اثبات. چون Q بر P چیره است، نگاشت $\varphi : \frac{A}{P} \longrightarrow \frac{B}{Q}$ یک نشاندن است. همچنین $\frac{B}{Q}$ بر $\frac{A}{P}$ صحیح است، زیرا اگر $b \in B$ آنگاه $a_0, a_1, \ldots, a_{n-1} \in A$ وجود دارند به طوری که

$$b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$$

و

$$b^n + Q = (a_{n-1}b^{n-1} + \cdots + a_1 b + a_0) + Q.$$

بنا به لم قبلی $\frac{A}{P}$ میدان است اگر و تنها اگر $\frac{B}{Q}$ میدان باشد و این یعنی P ماکسیمال است اگر و تنها اگر Q ماکسیمال باشد. □

لم ۲۲. فرض کنیم A و B دو دامنه صحیح باشند که $A \subseteq B$. همچنین فرض کنیم B روی A صحیح است و P یک ایده‌آل اول در A است. قرار دهید $S = A - P$. در این صورت $S^{-1}B$ روی A_P (موضعی سازی A در ایده‌آل اول P)، صحیح است.

اثبات. مجموعه $S = A \setminus P$ در A بسته ضربی است. بنابراین S در B نیز بسته ضربی است و می‌توانیم $S^{-1}B$ را تشکیل دهیم. این حلقه را با BA_p نشان می‌دهیم. BA_P [1] روی A_P یک توسیع صحیح است، زیرا اگر $\frac{b}{t}$ عنصری در BA_P باشد آنگاه $b \in B$ روی A صحیح است، یعنی $a_0, a_1, \ldots, a_{n-1} \in A$ وجود دارند به طوری که

$$b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$$

و بنابراین

$$(\frac{b}{t})^n = a_{n-1}t^{n-1}(\frac{b}{t})^{n-1} + \cdots + a_1 t(\frac{b}{t}) + a_0.$$

توجه داشته باشیم که در تساوی بالا برای هر اندیس i، $a_i t^i$ عناصری در A_P هستند. □

قضیه ۳۳. (قضیه چیرگی). فرض کنیم A و B دو دامنه صحیح باشند که $A \subseteq B$. همچنین فرض کنیم B روی A صحیح است و P یک ایده‌آل اول در A است. در این صورت ایده‌آل اول Q در B وجود دارد به طوری که $Q \cap A = P$.

اثبات. حلقه A را به کمک P موضعی سازی می‌کنیم و آن را با A_P نمایش می‌دهیم. بنا به قضیه قبل BA_P یک توسیع صحیح بر A_P است. بنابراین یک ایده‌آل Q از BA_P موجود است که $Q \cap A_P = PA_P$. قرار می‌دهیم $Q_0 = Q \cap B$. در این صورت $Q_0 \cap A = P$. □

لم ۲۳. فرض کنیم (A, M) حلقه موضعی و K میدان باشد به طوری که $A \subseteq K$. اگر x یک عنصر ناصفر در K باشد و

$$1 = a_0 + \frac{a_1}{x} + \frac{a_2}{x} + \cdots + \frac{a_n}{x^n}$$

به طوری که $a_0 \in M$ و برای هر اندیس $1 \leq i \leq n$، $a_i \in A$، آنگاه x روی A صحیح است. (یعنی اگر $\frac{1}{x}$ به همراه ایده‌آل ماکزیمال M در A عنصر یک را تولید کند، x روی A صحیح است).

اثبات. چون $a_0 \in M$ آنگاه $1 - a_0$ وارون پذیر است و تساوی $x^n = \frac{a_1}{1-a_0}x^{n-1} + \cdots + \frac{a_n}{1-a_0}$ به سادگی حاصل می‌شود. □

قضیه ۳۴. فرض کنیم (A, M) یک حلقه موضعی و K یک میدان شامل A باشد. در این صورت یک حلقه ارزیاب B در K وجود دارد که B روی A چیره است.

اثبات. بین حلقه‌های موضعی درون K که شامل A هستند ترتیب چیرگی را در نظر می‌گیریم. به عنوان تمرین نشان دهید که این مجموعه تحت زنجیرها بسته است. بنابراین یک حلقه موضعی ماکسیمال در K و شامل A مانند B موجود است. ادعا می‌کنیم B همان حلقه ارزیاب برای K است. فرض کنیم $x \in K$،

۱) اگر x روی B صحیح باشد آنگاه $B[x]$ (که یک مدول متناهیا تولید شده است) روی B یک توسیع صحیح است. بنا به قضیه چیرگی ایده‌آل ماکسیمال موضعی سازی $B[x]$ موجود است که به ایده‌آل ماکسیمال B چیره است که با ماکسیمال بودن B در تناقض است. بنابراین $B = B[x]$ و $x \in B$.

۲) اگر x روی B صحیح نباشد آنگاه بنا به لم قبل $1 \notin B[x^{-1}]$. پس ایده‌آل ماکسیمال موضعی سازی $B[x^{-1}]$ به ایده‌آل ماکسیمال B چیره است. بنابراین (مانند حالت قبل) ماکسیمال بودن B نقض می‌شود. پس $B = B[x^{-1}]$ و $x^{-1} \in B$.

بنا به دو حالت بالا B یک حلقه ارزیاب است. □

[1] به عنوان تمرین نشان دهید که BA_p واقعا حاصلضرب B, A_p است!

فصل ۷

ادامهٔ مقدمات جبری: توسیع‌های نُرمال

تدریس: محمود بهبودی
گردآوری: فاطمه اکبری.

۱.۷ توسیعهای نرمال

تعریف ۶۰. توسیع جبری F روی E را یک توسیع نرمال می‌نامیم هرگاه هر چندجمله‌ای تحویل ناپذیر $f(x) \in E[x]$ که ریشه‌ای در F داشته باشد به صورت حاصلضرب عوامل خطی در $F[x]$ نوشته شود.

تمرین ۱۲. ثابت کنید توسیع جبری F روی E نرمال است اگر وتنها اگر چندجمله‌ای مینیمال هر عنصر F روی E در $F[x]$ به صورت حاصلضرب عوامل خطی نوشته شود.

تذکر ۳۵. فرض کنیم R یک حلقه و $f(x) \in R[x]$. مجموعه ریشه‌های $f(x)$ در R را با $Z_R(f(x))$ نمایش می‌دهیم. با این نماد، اگر میدان F توسیع نرمال E باشد آنگاه یک چندجمله‌ای تکین $f(x) \in E[x]$ که در F ریشه داشته باشد به صورت زیر تجزیه می‌شود،

$$f(x) = \prod_{\alpha_i \in Z_F(f(x))} (x - \alpha_i)^{m_i}$$

هرگاه هر ریشه α_i، m_i-بار تکرار شود.

مثال ۵۳. توسیع $\mathbb{Q}(\sqrt[۳]{۲})$ روی $\mathbb{Q}$ نرمال نیست. زیرا تنها ریشه چندجمله‌ای تحویل ناپذیر $f(x) = x^۳ - ۲ \in \mathbb{Q}[x]$ در $\mathbb{Q}(\sqrt[۳]{۲})$ عنصر $\sqrt[۳]{۲}$ است و ریشه‌های دیگر $f(x)$ در F قرار ندارند.

تمرین ۱۳. چندجمله‌ای $f(x) = x^۴ - ۱۱$ در $\mathbb{Q}[x]$ تحویل ناپذیر است. توسیع F را برای $\mathbb{Q}$ بیابید که $f(x)$ روی F به صورت حاصلضربی از عوامل خطی تجزیه شود و روی هیچ زیر میدان سره‌اش به صورت حاصلضرب عوامل خطی نوشته نشود (راهنمایی: از قضیه کرونکر استفاده کنید).

تعریف ۶۱. فرض کنیم F توسیع میدان E باشد و $f(x) \in E[x]$. F را یک میدان شکافنده $f(x)$ روی E می‌نامیم هرگاه در شرایط زیر صدق کند،

۱) $f(x)$ روی F به ضرایب خطی تجزیه شود،

۲) اگر K یک توسیع میانی سره باشد ($E < K < F$) آنگاه $f(x)$ روی K به عوامل خطی تجزیه نشود.

به عبارت دیگر، F میدان شکافنده $f(x)$ است هرگاه $F = E(\alpha_۱, \alpha_۲, \dots \alpha_n)$ که α_i ها همهٔ ریشه‌های f هستند.

قضیه ۳۵. اگر K میدان و $f(x) \in K[x]$ غیر ثابت باشد آنگاه یک توسیع میدانی E_f برای K موجود است که درجه E_f روی K بیشتر از $\deg(f(x))$ نیست و $f(x)$ روی E_f به عوامل خطی شکافته می‌شود.

اثبات. فرض کنیم $f = f_1^{m_1} f_2^{m_2} \cdots f_k^{m_k}$ که برای هر اندیس i، چندجمله‌ای‌های f_i در $K[x]$ تحویل ناپذیر باشند. به کمک قضیه کرونکر نظیر هر چندجمله‌ای f_i توسیع E_i را می‌یابیم که همه ریشه‌های f_i در آن باشد. بنابراین با این روش می‌توانیم میدان شکافنده f را پیدا کنیم. اما توجه داشته باشیم که درجه این توسیع روی میدان K برابر است با ضرب درجه توسیع‌های E_i روی K. چون درجه f_iها از f کمتر است، درجه توسیع E_f روی K حتما کوچکتر از درجه چندجمله‌ای f است. □

مثال ۵۴. چندجمله‌ای $f(x) = \frac{x^p - 1}{x - 1}$ در $\mathbb{Q}[x]$ را در نظر می‌گیریم. اگر $\alpha \in \mathbb{C}$ یک ریشه $f(x)$ باشد، به عنوان تمرین نشان دهید بقیه ریشه‌ها عبارت اند از α^2، α^3، ...، α^{p-1} و لذا $\mathbb{Q}(\alpha)$ یک میدان شکافنده $f(x)$ در $\mathbb{Q}$ است. همچنین $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ را محاسبه کنید.

مثال ۵۵. فرض کنیم $f(x) = x^4 - 11$ در $\mathbb{Q}[x]$ باشد. به عنوان تمرین نشان دهید $\mathbb{Q}(i, \sqrt[4]{11})$ یک میدان شکافنده $f(x)$ روی $\mathbb{Q}$ است و $\mathbb{Q} \leq \mathbb{Q}(i, \sqrt[4]{11}) \leq \mathbb{C}$. از طریق کرونکر می‌توان توسیع دیگری به غیر از $\mathbb{Q}(i, \sqrt[4]{11})$ یافت به طوری که میدان شکافنده $f(x)$ باشد. بنابراین میدان شکافنده یکتا نیست.

در ادامه می‌خواهیم نشان دهیم میدان‌های شکافنده تحت یکرختی یکتا هستند.

تذکر ۳۶. فرض کنیم $\sigma : K \longrightarrow L$ یک همریختی بین دو میدان K و L باشد. به صورت طبیعی می‌توانیم σ را به $\overline{\sigma} : K[x] \longrightarrow L[x]$ با ضابطه $\overline{\sigma}(\sum_{i=1}^{n} k_i x^i) = \sum_{i=1}^{n} \sigma(K_i) x^i$ توسیع دهیم.

قضیه ۳۶. فرض کنیم $\sigma : K \longrightarrow L$ یک همریختی بین دو میدان K و L باشد. همچنین فرض کنیم $f(x) \in K[x]$ و F میدان شکافنده $f(x)$ روی K باشد. در این صورت اگر L شامل یک میدان شکافنده $\overline{\sigma}(f(x))$ روی $\sigma(K)$ باشد آنگاه می‌توان σ را به هم ریختی $\varphi : F \longrightarrow L$ توسیع داد. پس $\varphi|_K = \sigma$.

اثبات. با استقرا روی شاخص $[F : K]$ ثابت می‌کنیم. اگر $[F : K] = 1$ یعنی $F = K$ و لذا $\varphi = \sigma$. حال چون F میدان شکافنده است داریم $F = K(\alpha_1, \ldots, \alpha_n)$ که $\alpha_i \in F$ ریشه‌ای از $f(x)$ هستند. حال فرض کنیم حکم برای تمام میدان شکافنده‌های F_1 از هر چندجمله‌ای روی K_1 که $[F_1 : K_1]$ از $[F : K]$ کمتر است درست باشد. بدون کاستن از کلیت فرض کنیم که ریشه α_1 در K نباشد. اگر $g(x)$ چندجمله‌ای مینیمال α_1 روی K باشد آنگاه $g(x) \mid f(x)$. اما L شامل یک میدان شکافنده $\overline{\sigma}(f(x))$ روی $\sigma(K)$ است، لذا چندجمله‌ای $\overline{\sigma}(g(x))$ دارای ریشه‌ای مانند β در L است و همریختی $\sigma_1 : K(\alpha_1) \longrightarrow L$ وجود دارد که $\sigma_1|_K = \sigma$. چون $[F : K(\alpha_1)] < [F : K]$ و F میدان شکافنده $f(x) \in K(\alpha_1)[x]$ روی $K(\alpha_1)$ است بنا به فرض استقرا همریختی $\varphi : F \longrightarrow L$ وجود دارد که یک توسیع σ_1 است و چون σ_1 هم توسیع σ است پس φ یک توسیع σ است. □

نتیجه ۱۵. فرض کنیم K و L دو میدان و $\sigma : K \longrightarrow L$ همریختی باشد. اگر E میدان شکافنده $f(x)$ روی K و F یک میدان شکافنده $\overline{\sigma}(f(x))$ روی L باشند آنگاه σ را می‌توان به یک یکریختی $\varphi : E \longrightarrow F$ توسیع داد که $\varphi|_K = \sigma$.

اثبات. بنا به قضیه قبل همریختی $\varphi : E \longrightarrow F$ به طوری که $\varphi|_K = \sigma$ وجود دارد. باید ثابت کنیم این نگاشت پوشا است. فرض کنیم $|Z_E(f(x))| = k$ و $|Z_F(\overline{\sigma}(f(x))| = n$. اگر $r \in E$ یک ریشه $f(x)$ باشد آنگاه $\varphi(r) \in F$ نیز ریشه $\overline{\sigma}(f(x))$ است. بنابراین $k \leq n$. به طور مشابه چون σ^{-1} تکریختی است می‌توان نتیجه گرفت $n \leq k$. پس $n = k$ و این یعنی φ پوشاست. □

نتیجه ۱۶. اگر E و F میدان‌های شکافنده $f(x)$ روی K باشند آنگاه E و F، K-یکریخت هستند.

اثبات. کافی است در نتیجه قبل L را همان K و σ را تابع همانی در نظر بگیریم. □

قضیه ۳۷. فرض کنیم F میدان شکافنده $f(x) \in K[x]$ روی K باشد اگر F زیر میدانی از میدان L و $\sigma : F \longrightarrow L$ یک K-همریختی باشد آنگاه $\sigma(F) = F$.

اثبات. فرض کنیم $n = |Z_F(f(x))|$. بنابراین K یک توسیع متناهی است. اگر α ریشه چندجمله‌ای $f(x)$ باشد آنگاه $\sigma(\alpha)$ نیز ریشه $f(x)$ است و درنتیجه $\sigma|_{Z_F(f(x))}$ یک تابع یک به یک و پوشا است. در نتیجه $Z_F(f(x)) \cup K = \sigma(F)$. اما F میدان شکافنده $f(x)$ در K است. پس $F \subseteq \sigma(F)$. از طرفی

$$[\sigma(F) : K] = [\sigma(F) : F] \cdot [F : K] \Rightarrow [\sigma(F) : K] = [F : K]$$

و این یعنی $F = \sigma(F)$. در واقع ثابت کردیم σ ریشه‌ها را جا به جا می‌کند. □

تعریف ۶۲. فرض کنیم F توسیع میدان K باشد. دو عنصر α و β در F را روی K مزدوج نامیم هرگاه یک K-یکریختی، $\sigma : K(\alpha) \longrightarrow K(\beta)$ وجود داشته باشد که $\sigma(\alpha) = \beta$.

نتیجه ۱۷. فرض کنیم F توسیع میدان K و α و β روی K جبری باشند. در این صورت α و β روی K مزدوج هستند اگر و تنها اگر چندجمله‌ای‌های مینیمال α و β روی K یکی باشند.

اثبات. تمرین. □

قضیه ۳۸. توسیع F را روی میدان K در نظر می‌گیریم، F روی K توسیع نرمال و متناهی است اگر و تنها اگر F میدان شکافنده یک چندجمله‌ای در $K[x]$ باشد.

اثبات. فرض کنید F میدان شکافندهٔ چندجمله‌ای $f(x)$ روی K باشد. اگر $g(x) \in K[x]$ ریشه‌ای مانند α_1 در F و ریشه‌ای مانند α_2 خارج از F داشته باشد، اتومرفیسمی مانند σ از بستار جبری F پیدا می‌شود که α_1 را به α_2 ببرد، یعنی $\sigma(F) \neq F$ و این با قضایای قبلی مغایرت دارد.

برعکس فرض کنیم F روی K توسیع نرمال و متناهی باشد. پس $\alpha_1, \ldots, \alpha_n$ وجود دارند که $F = K(\alpha_1, \ldots, \alpha_n)$. همچنین فرض کنیم $f_1, \ldots, f_n \in K[x]$ چندجمله‌ای‌های مینیمال نظیر $\alpha_1, \ldots, \alpha_n$ باشند. قرار می‌دهیم $f = f_1 \cdots f_n$. بنا به فرض‌ها برای هر اندیس i، چندجمله‌ای f_i روی F به صورت حاصلضرب عوامل خطی تجزیه می‌شود، پس f به حاصلضرب عوامل خطی روی F تجزیه می‌شود. بنابراین همه ریشه‌های $f(x)$ در F است. اما هر زیر میدان سره F که شامل K باشد حداقل یکی از α_iها را شامل نیست. پس بنا به تعریف، F میدان شکافنده $f(x)$ روی K است. □

مثال ۵۶. چندجمله‌ای $f(x) = x^3 - 5$ در $\mathbb{Q}[x]$ تحویل ناپذیر است (بررسی کنید). اگر $\omega = \exp(\frac{2\pi i}{3})$ آنگاه $F = \mathbb{Q}(\sqrt[3]{5}, \omega\sqrt[3]{5})$ یک میدان شکافنده $f(x)$ روی $\mathbb{Q}$ است. اگر $K = \mathbb{Q}(\sqrt[3]{5})$، آنگاه تحویل ناپذیری $f(x)$ در $\mathbb{Q}[x]$ ایجاب می‌کند که $f(x)$ چندجمله‌ای مینیمال $\sqrt[3]{5}$ روی $\mathbb{Q}$ باشد. پس $[K : \mathbb{Q}] = 3$. اگر $p(x) = (x - \omega\sqrt[3]{5})(x - \omega\sqrt[3]{5})$ آنگاه $p(x)$ در $K[x]$ تحویل ناپذیر است، در واقع $p(x)$ چندجمله‌ای مینیمال $\omega\sqrt[3]{5}$ روی K است. بنابراین $[F : K] = 2$ و می‌توانیم نتیجه بگیریم

$$[F : \mathbb{Q}] = [F : K][K : \mathbb{Q}] = 6.$$

قضیه ۳۹. فرض کنیم E توسیعی از میدان F و F توسیع میدان K باشد. همچنین فرض کنیم E روی K توسیع متناهی و نرمال باشد. در این صورت اگر $\sigma : F \longrightarrow E$ یک K-همریختی باشد آنگاه σ را می‌توان به یک خودریختی $\eta : E \longrightarrow E$ توسیع داد.

اثبات. نتیجه مورد نظر به سادگی از نتیجه ۱۵ حاصل می‌شود. □

نتیجه ۱۸. فرض کنیم E روی K یک توسیع متناهی و نرمال و $f(x) \in K[x]$ چندجمله‌ای مینیمال $\alpha \in E$ باشد. اگر $\beta \in E$ ریشه دیگری از f باشد آنگاه همریختی همانی روی K را می‌توان به یک خودریختی $\eta : E \longrightarrow E$ توسیع داد که $\eta(\alpha) = \beta$.

اثبات. همریختی $\xi : K(\alpha) \longrightarrow K(\beta)$ توسیع تابع همانی روی K است و $\xi(\alpha) = \beta$. بنا به قضیه قبل همریختی $\sigma : K(\alpha) \longrightarrow E$ با ضابطه $\sigma(x) = \xi(x)$ را می‌توان به یک خودریختی $\eta : E \longrightarrow E$ توسیع داد به طوری که $\eta(\alpha) = \sigma(\alpha) = \beta$. □

فصل ۸

توسیعهای جبری و متعالی میدانهای ارزیابی و حذف سور در میدانهای ارزیابی بستهٔ حبری

تدریس: محسن خانی

گردآوری: فاطمه اکبری

۱.۸ توسیع‌های صحیح و رابطهٔ آنها با توسیع ارزیابی

قضیه ۴۰. حلقه‌های ارزیاب به طور صحیح بسته هستند. یعنی، اگر A یک حلقه ارزیاب میدان K باشد و $x \in K$ روی A صحیح باشد، آنگاه $x \in A$.

اثبات. فرض کنیم $x \in K$ روی A صحیح باشد. در این صورت عناصر $a_0, \dots, a_{n-1} \in A$ وجود دارند که $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$.
اگر V نگاشت ارزیابی نظیر حلقه ارزیاب A باشد، آنگاه

$$V(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = V(0) = \infty. \tag{۱.۸}$$

فرض کنیم $x \notin A$. در این صورت $V(x) < 0$ و

$$V(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = V(x^n) = nV(x) < 0$$

که این در تناقض با تساوی (۱.۸) است. علت عبارت بالا به شرح زیر است.
اگر $V(x) < 0$ آنگاه تک تک جمع‌وندها در چندجمله‌ای بالا ارزیابی بیشتر از ارزیابی جملهٔ اول دارند زیرا

$$V(a_i x^i) = V(a_i) + iV(x) \geq iV(x) > nV(x)$$

دقت کنید که $V(a_i)$ ها نامنفی است زیرا $a_i \in A$. □

تعریف ۶۳. فرض کنیم A یک حلقه موضعی در K باشد. منظور از بستار صحیح A، مجموعه کلیه عناصر موجود در K است که روی A صحیح‌اند. این مجموعه را با A_K^{int} نمایش می‌دهیم.

قضیه ۴۱. فرض کنیم K میدان و شامل زیر حلقه موضعی A باشد. در این صورت بستار صحیح A در K برابر است با اشتراک تمام حلقه‌های ارزیاب K که بر A چیره هستند. به عبارت دیگر

$$A_K^{int} = \bigcap_{B \subseteq K} B$$

که Bها ارزیاب و چیره بر A هستند.

اثبات. اگر $x \in K$ روی A صحیح باشد آنگاه x در تمام حلقه‌های ارزیاب شامل A قرار دارد. زیرا بنا به اثبات قبل اگر V نگاشت ارزیابی باشد آنگاه $V(x)$ نمی‌تواند منفی باشد. در واقع $V(x)$ در تمامی ارزیابی‌ها مثبت است. حال فرض کنیم $x \in K$ روی A صحیح نباشد. در این صورت

$[A[x^{-1}] \not\in M_A A[x^{-1}]$ ۱ (M_A ایده‌آل ماکسیمال A است). یعنی ایده‌آل ماکسیمال موضعی سازی $A[x^{-1}]$ وجود دارد که شامل M_A و x^{-1} است. پس (از اثبات‌های جلسات گذشته) نتیجه می‌گیریم یک حلقه ارزیاب شامل موضعی سازی $A[x^{-1}]$ وجود دارد. اما x به این حلقه ارزیاب تعلق ندارد، زیرا x^{-1} در ایده‌آل ماکسیمال است. پس به طور خلاصه ثابت کردیم اگر x عنصری صحیح نباشد آنگاه حلقه ارزیابی شامل A وجود دارد که x در آن نیست. □

لم ۲۴. فرض کنیم L یک توسیع نرمال متناهی روی K باشد. در این صورت کاردینال مجموعه $Aut(\frac{L}{K})$ برابر است با $[L : K]$.

اثبات. L یک توسیع نرمال متناهی است، یعنی $\alpha_1, \ldots, \alpha_n$ در L وجود دارند که $L = K[\alpha_1, \ldots, \alpha_n]$ و

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq L.$$

تعداد K-خودریختی‌های، $\sigma : K(\alpha_1) \longrightarrow K(\alpha_1)$ برابر است با درجه چندجمله‌ای مینیمال نظیر α_1. زیرا خودریختی‌ها ریشه‌ها را جا به جا می‌کنند و بنابراین به اندازه تعداد ریشه‌ها خودریختی وجود دارد. به طور مشابه تعداد $K(\alpha_1)$-خودریختی‌ها ی، $\sigma : K(\alpha_1, \alpha_2) \longrightarrow K(\alpha_1, \alpha_2)$ برابر است درجه چندجمله‌ای مینیمال نظیر α_2. به همین صورت اگر ادامه دهیم به این نتیجه می‌رسیم که تعداد K-خودریختی‌ها برابر است با

$$[L : K] = [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots [L : K(\alpha_1, \ldots, \alpha_{n-1})].$$

□

در اینجا خیلی مختصر و برای کسب اطلاعات بیشتر، کمی توسیع‌های گالوایی را تعریف و قضیه اساسی گالوا را بدون اثبات بیان می‌کنیم.

تعریف ۶۴. فرض کنیم L یک توسیع میدانی روی K باشد. در این صورت اگر $Fix(Aut(\frac{L}{K})) = K$ آنگاه توسیع مورد نظر را گالوایی می‌نامیم. توجه کنید که

$$Fix(Aut(\frac{L}{K})) = \{x \in L \mid \forall \sigma \in \frac{L}{K},\ \sigma(x) = x\}.$$

تذکر ۳۷. در مشخصه صفر هر توسیع نرمال متناهی یک توسیع گالوایی است. در مشخصهٔ کلی، گالوائی بودن توسیع معادل نرمال و جدائی‌پذیر بودن آن است.

قضیه ۴۲. (قضیه اساسی گالوا). اگر توسیع L روی K یک توسیع گالوایی باشد (که در مشخصه صفر همان توسیع‌های نرمال هستند) آنگاه یک تناظر یک به یک میان میدان‌های میانی $K \subseteq E \subseteq L$ و زیرگروه‌های گروه $Aut(\frac{L}{K})$ وجود دارد.

لم ۲۵. در مشخصهٔ صفر، فرض کنیم L روی K یک توسیع میدانی نرمال و متناهی و $\alpha \in L$ روی K جبری باشد. در این صورت

$$\prod_{\sigma \in Aut(L/K)} \sigma(\alpha) \in K.$$

اثبات. فرض کنید x ریشهٔ چندجمله‌ای $a_n x^n + \cdots + a_1 x + a$ باشد. در این صورت جملهٔ ثابت این چندجمله‌ای، یعنی a_0 حاصل‌ضرب ریشه‌های آن است. ریشه‌های این چندجمله‌ای همان $\sigma(x)$ ها هستند. □

قضیه ۴۳. (قضیه باقی مانده چینی). اگر A یک گروه آبلی (جمعی) باشد و B_1، ...، B_n زیرگروه‌های A باشند به طوری که برای هر دو اندیس $1 \leq i < j \leq n$، $B_j + B_i = A$ آنگاه برای هر $a_1, \ldots, a_n \in A$ عنصر $a \in A$ وجود دارد که برای هر i، $a \overset{B_i}{\equiv} a_i$ (یا $a - a_i \in B_i$).

قضیه ۴۴. فرض کنیم A یک دامنه موضعی در میدان K باشد که در میدان کسرهایش بسته صحیح است (یعنی عناصری که در میدان کسرهای A هستند و روی A صحیح‌اند در خود A قرار دارند). اگر L توسیع نرمال متناهی K باشد و B بستار صحیح A در L باشد آنگاه برای هر دو ایده‌آل ماکسیمال N و N' در B یک $\sigma \in Aut(\frac{L}{K})$ موجود است به طوری که $\sigma(N) = N'$.

اثبات. فرض کنیم برای هر $\sigma \in Aut(\frac{L}{K})$ داشته باشیم $\sigma(N) \neq N'$. بنابراین ایده‌آل‌های ماکسیمال

$$\{\sigma(N) \mid \sigma \in Aut(\frac{L}{K})\}, \quad \{\sigma(N') \mid \sigma \in Aut(\frac{L}{K})\}$$

در B، مجزا و متناهی هستند زیرا طبق لم ۲۴ تعداد خودریختی‌ها متناهی است. بنا به قضیه باقی‌مانده چینی عنصر x در B موجود است که $x \overset{\sigma(N)}{\equiv} ۰$ و $x \overset{\sigma(N')}{\equiv} ۱$. به عبار دیگر $x \in \sigma(N)$ و $x \notin \sigma(N')$. پس می‌توانیم نتیجه بگیریم برای هر K-خودریختی، σ، عنصر $\sigma(x)$ در N است اما $\sigma(x)$ در N' نیست. (در واقع مشابه همین جمله برای $\sigma^{-۱}(x)$ درست است و هر $\sigma^{-۱}$ یکی از σ هاست!) قرار می‌دهیم $p = \prod_{\sigma \in Aut(L/K)} \sigma(x)$. پس بنا به آنچه تا به اینجا گفته شد $p \in N$ اما $p \notin N'$. از طرفی طبق لم ۲۵، p در K است. چون $x \in B$ و B روی A صحیح است نتیجه می‌گیریم $p \in A$. از آنجایی که همه ایده‌آل‌های ماکسیمال B به M_A (ایده‌آل ماکسیمال A) چیره هستند داریم $p \in A \cap N = M_A$. اما $M_A \subseteq N'$ و $p \in N'$ که تناقض است. □

قضیه ۴۵. فرض کنیم A یک حلقه ارزیاب درون میدان K و L توسیع جبری K باشد. در این صورت هر حلقه ارزیاب L که بر A چیره باشد به صورت موضعی سازی یک بستار صحیح A در L است. به طور دقیق‌تر، حلقه‌های ارزیاب L که بر A چیره‌اند به صورت B_Nهایی هستند که B بستار صحیح A در L و N یک ایده‌آل ماکسیمال در B است.

اثبات. فرض کنیم C یک حلقه ارزیاب برای میدان L باشد. بنابراین C بسته صحیح است و $B \subseteq C$. قرار می‌دهیم $N = M_C \cap B$ که M_C ایده‌آل ماکسیمال C است. ثابت می‌کنیم موضعی سازی B توسط N، B_N، برابر است با C. چون هر عنصر B_N دارای ارزیابی مثبت است بنابراین در C نیز قرار دارد. پس $B_N \subseteq C$. حال فرض کنیم $x \in C$. x روی K جبری است پس عناصر $a'_n, \ldots, a'_۱, a'_۰ \in K$ موجوداند که $a'_n \neq ۰$ و

$$a'_n x^n + \cdots + a'_۱ x + a'_۰ = ۰.$$

اگر دو طرف تساوی بالا را در یک عنصر با ارزیابی به اندازه کافی بزرگ ضرب کنیم آنگاه عناصر $a_n, \ldots, a_۱, a_۰$ حاصل می‌شوند که ارزیابی آن‌ها مثبت است وبنابراین در A قرار دارند. همچنین

$$a_n x^n + \cdots + a_۱ x + a_۰ = ۰. \tag{۲.۸}$$

اگر V نگاشت ارزیابی باشد آنگاه اندیس $۱ \leq j \leq n$ وجود دارد که $V(a_j) = \min\{V(a_n), \ldots, V(a_۰)\}$. دو طرف تساوی (۲.۸) را به $a_j x^j$ تقسیم می‌کنیم. یعنی

$$\frac{a_n}{a_j} x^{n-j} + \cdots + \frac{a_{j+۱}}{a_j} + ۱ + \frac{a_{j-۱}}{a_j} x^{-۱} + \cdots + \frac{a_۰}{a_j} x^{-j} = ۰.$$

قرار می‌دهیم $y = \frac{a_n}{a_j} x^{n-j} + \cdots + \frac{a_{j+۱}}{a_j} + ۱$ و $z = \frac{a_{j-۱}}{a_j} + \cdots + \frac{a_۰}{a_j} x^{-j+۱}$. بنابراین $y + x^{-۱} z = ۰$ یا $z = -xy$. از طرفی برای هر $i \geq j$، داریم

$$V(\frac{a_i}{a_j}) = V(a_i) - V(a_j) > ۰$$

و بنابراین در این حالت برای هر i، $\frac{a_i}{a_j}) \in M_C$. پس $y \notin M_C$ و $y \in U(C)$. بنابراین می‌توانیم بنویسیم $x = \frac{z}{y}$. پس اگر نشان دهیم y و z به B تعلق دارند آنگاه چون $y \notin N$ نتیجه می‌گیریم $x \in B_N$ و اثبات کامل می‌شود. در قضیه ۴۱ گفتیم که بستار صحیح A در L، یعنی B، برابر با اشتراک همه حلقه‌های ارزیاب چیره بر A است. پس کافی است نشان دهیم y و z در همه حلقه‌های ارزیاب L قرار دارند. فرض کنیم D یک حلقه ارزیاب شامل A در L باشد. چه در حالتی که x در D باشد و چه در حالتی که x در D نباشد نتیجه می‌گیریم y و z در D هستند. □

قضیه ۴۶. فرض کنیم A یک حلقه ارزیاب درون میدان K و L توسیع جبری K باشد. اگر B بستار صحیح A در L و N یک ایده‌آل ماکسیمال در B باشد آنگاه موضعی سازی B_N یک حلقه ارزیاب برای L است.

اثبات. اگر B_N یک حلقه ارزیاب نباشد آنگاه یک حلقه ارزیاب شامل B_N وجود دارد که بنا به قضیه قبل به شکل $B_{N'}$ است. یعنی $B_{N'}$ بر B_N چیره است و تنها در صورتی چیرگی اتفاق می‌افتد که $N = N'$. □

نتیجه ۱۹. فرض کنیم A یک حلقه ارزیاب در میدان K و L توسیع نرمال روی K باشد. برای هر دو حلقه ارزیاب C و C' از L که بر A چیره هستند K-خودریختی مانند σ وجود دارد که $\sigma(C) = C'$.

اثبات. بنا به قضیه ۴۵، داریم $C = B_N$ و $C' = B_{N'}$. طبق قضیه ۴۴، K-خودریختی، σ چنان وجود دارد که $\sigma(N) = N'$. بنابراین عناصری که در (L, C) دارای ارزیابی مثبت باشند در (L, C') هم مثبت هستند. در واقع σ حافظ ارزیابی‌ها است. پس $\sigma(C) = C'$. □

نتیجه ۲۰. فرض کنیم A یک حلقه ارزیاب در میدان K و K^{ac} بستار جبری K باشد. همچنین فرض کنیم B_1 و B_2 دو توسیع A در K^{ac} باشند. در این صورت $\sigma \in Aut(\frac{K^{ac}}{K})$ وجود دارد که $\sigma(B_1) = B_2$ (به تقریب خودریختی‌ها یکتا هستند).

اثبات. واضح است. □

۲.۸ توسیعهای جبری و متعالی میدانهای ارزیابی

قضیه ۴۷. فرض کنیم (L, B) توسیع متناهی میدان ارزیابی (K, A) باشد. در این صورت

$$[L : K] \geq [K_B : K_A] \cdot [\Gamma_A : \Gamma_B].$$

(منظور از K_A همان میدان پیمانه‌های نظیر نگاشت ارزیابی V_A است که پیش‌تر آن را با K_{V_A} نمایش می‌دادیم به طوری که V_A نگاشت ارزیابی نظیر حلقه ارزیاب A است.)

اثبات. فرض کنیم $b_1, \ldots, b_p$ عناصری در L باشند که $\overline{b_1}, \ldots, \overline{b_p}$ در K_B مستقل خطی هستند. همچنین فرض کنیم $c_1, \ldots, c_q \in L$ ناصفر و به گونه‌ای باشند که $V(c_1), \ldots, V(c_q)$ هم مجموعه‌های متفاوتی روی Γ_A دارند (به عبارت دیگر، برای هر دو اندیس $1 \leq i < j \leq q$، $V(c_i) - V(c_j) \notin \Gamma_A$). بنابراین $[K_B : K_A] = p$ و $[\Gamma_A : \Gamma_B] = q$، پس باید ثابت کنیم $[L : K] \geq p \cdot q$. برای این منظور نشان خواهیم داد مجموعه

$$B = \{b_i c_j \mid 1 \leq i \leq p,\ 1 \leq j \leq q\}$$

یک مجموعه مستقل خطی روی K است. اگر $\sum_{i,j} a_{ij} b_i c_j$ یک ترکیب خطی از عناصر B باشد به طوری که برای هر i, j، $a_{ij} \in K$، آنگاه

$$V(\sum_{i,j} a_{ij} b_i c_j) = \min_{i,j}\{V(a_{ij} b_i c_j)\} = \min_{i,j}\{V(a_{ij}) + V(c_j)\} \tag{۳.۸}$$

و بنابراین ترکیب خطی مورد نظر هیچگاه صفر نمی‌شود. برای اثبات تساوی (۳.۸) ابتدا ثابت می‌کنیم برای هر $a_1, \ldots, a_p \in K$ داریم

$$V(a_1 b_1 + \cdots + a_p b_p) = \min_i\{V(a_i)\}.$$

فرض کنیم a_t، $1 \leq t \leq p$، کوچکترین ارزیابی را داشته باشد. همچنین بدون کاستن از کلیت فرض کنیم $V(a_t) = 0$ و $V(a_i) \geq 0$، برای هر اندیس $i \neq t$. در این صورت

$$V(a_t(\frac{a_1}{a_t} b_1 + \cdots + \frac{a_p}{a_t} b_p)) = V(a_1 b_1 + \cdots + a_p b_p) = 0$$

زیرا $\overline{b_1}, \ldots, \overline{b_p}$ مستقل خطی هستند و $\overline{a_1 b_1} + \cdots + \overline{a_p b_p} \neq 0$. پس

$$\begin{aligned} V(\sum_i a_{ij} b_i c_j) &= V(\sum_i (a_{ij} b_i) c_j) \\ &= V(\sum_i (a_{ij} b_i)) + V(c_j) \\ &= \min_i\{V(a_{ij})\} + V(c_j) \end{aligned}$$

و بنابراین برای هر دو اندیس $j_1 \neq j_2$ داریم $V(\sum_i a_{ij_1}b_ic_{j_1}) \neq V(\sum_i a_{ij_2}b_ic_{j_2})$ چون در غیر این صورت $V(c_{j_1}) - V(c_{j_2}) \in \Gamma_A$ که در تناقض با فرض اولیه اثبات است. در نهایت،

$$V(\sum_{i,j} a_{ij}b_ic_j) = \min_j\{\min_i\{V(a_{ij})\} + V(c_j)\} = \min_{i,j}\{V(a_{ij}) + V(c_j)\}.$$

□

نتیجه ۲۱. فرض کنیم (L, B) یک توسیع میدان‌های ارزیابی برای (K, A) باشد به طوری که $[L : K] < \infty$. در این صورت بنا به قضیه قبل $[K_A, K_B] < \infty$ و این یعنی K_B روی K_A جبری است. همچنین داریم $[\Gamma_A : \Gamma_B] < \infty$. اگر $[\Gamma_A : \Gamma_B] = m$ آنگاه $m\Gamma_B \subset \Gamma_A$.

تمرین ۱۴. در نتیجه بالا، نشان دهید اگر L بستار جبری K باشد آنگاه K_B بستار جبری K_A و Γ_B هسته بخش پذیر Γ_A است (یعنی $\Gamma_A \subseteq \Gamma_A$ به گونه‌ای است که هر معادله $mx = \gamma \in \Gamma_A$ در Γ_B جواب دارد).

لم ۲۶. فرض کنیم (K, A) یک میدان ارزیابی باشد و $\beta \in K_A^{alg}$. همچنین فرض کنیم $p(x) \in A[x]$ به گونه‌ای باشد که $\overline{p}(x) \in K_A[x]$ چندجمله‌ای مینیمال نظیر β باشد. اگر b یک ریشه $p(x)$ در K^{ac} باشد آنگاه V_A به طور یکتا به $V' : K(b) \longrightarrow \Gamma_A$ گسترش می‌یابد به طوری که K' (میدان باقی‌مانده‌های نظیر نگاشت ارزیابی V') با $K_A(\beta)$ یکریخت است (یعنی می‌توان ارزیابی را به نحوی توسیع داد که گروه Γ_A تغییر نکند و میدان K_A به میدان $K_A(\beta)$ گسترش یابد.)

اثبات. فرض کنیم $V' : K(b) \longrightarrow \Gamma$ توسیعی از نگاشت ارزیابی V_A باشد و $\Gamma_A \subseteq \Gamma$. b روی K جبری است پس روی A صحیح است (با ضرب عناصری با ارزیابی‌های به اندازه کافی بزرگ در چندجمله‌ای مینیمال نظیر b به چندجمله‌ای می‌رسیم که نشان می‌دهد b صحیح است). بنابراین $V'(b) \geq 0$. چون $p(b) = 0$ پس $\overline{p}(\overline{b}) = 0$. اما $\overline{p}$ چندجمله‌ای مینیمال β روی K نیز هست و بنابراین $K_A(\overline{b}) \cong K_A(\beta)$. (نکته مهمی که باید به آن توجه کنیم این است که هرگز ادعا نکردیم $\overline{b} = \beta$). فرض کنیم $\deg(p) = n$، از این یکریختی نتیجه می‌گیریم که $1, \overline{b}, \overline{b}^2, \ldots, \overline{b}^{n-1}$ روی K_A مستقل خطی هستند و بنا به اثبات قضیه ۴۷، برای هر $a_1, \ldots, a_n \in K$ داریم

$$V'(\sum_{i=0}^{n-1} a_ib^i) = \min_i\{V_A(a_i)\} \in \Gamma_A.$$

از این تساوی نتیجه می‌گیریم، اولا $\Gamma' = \Gamma_A$ (بنابراین V' یکتاست)، ثانیا عناصر $1, b, b^2, \ldots, b^{n-1}$ نیز روی K مستقل خطی هستند و p چندجمله‌ای مینیمال نظیر b است. از طرفی $[K_A(\overline{b}) : K_A] \leq [K' : K_A]$ زیرا $\overline{b} \in K'$ و بنا به قضیه ۴۷،

$$[K' : K_A] \leq [K(b) : K] = [K_A(\overline{b}) : K_A].$$

پس $[K_A(\overline{b}) : K_A] = [K' : K_A]$ و $K_A(\overline{b}) \cong K'$ که نشان می‌دهد حکم برقرار است. □

لم ۲۷. فرض کنیم (K, A) یک میدان ارزیابی و $L = K(x)$ یک توسیع متعالی از K باشد (یعنی عنصر x روی K متعالی باشد). در این صورت یک حلقه ارزیاب یکتا B از L چیره بر A موجود است به طوری که $x \in B$ و $\overline{x}$ روی K_A متعالی است. همچنین برای این توسیع داریم $K_B = K_A(\overline{x})$ و $\Gamma_A = \Gamma_B$.

اثبات. فرض کنیم B یک حلقه ارزیاب برای $K(x)$ باشد به طوری که $x \in B$ و $\overline{x}$ روی K_A متعالی است. بنابراین برای هر $a_0, \ldots, a_n \in K$ داریم

$$V_B(a_0 + a_1x + \cdots + a_nx^n) = \min_i\{V_A(a_i)\} \in \Gamma_A.$$

بنابراین در صورت وجود این ارزیابی یکتاست. برای اثبات وجود B به این صورت عمل می‌کنیم. نگاشت $V : K(x) \longrightarrow \Gamma_A$ را با ضابطه

$$V(a_0 + a_1x + \cdots + a_nx^n) = \min_i\{V_A(a_i)\}$$

تعریف می‌کنیم. ثابت می‌کنیم V یک نگاشت ارزیابی است. اگر $f = a_۰ + a_۱x + \cdots + a_nx^n$ و $g = b_۰ + b_۱x + \cdots + b_nx^n$ دو عنصر $K(x)$ باشند، به وضوح $V(f+g) = \min\{V(f), V(g)\}$. حال فرض کنیم اندیس‌های $i_۰$ و $j_۰$ به گونه‌ای باشند که $a_{i_۰}$ و $b_{j_۰}$ به ترتیب کمترین ارزیابی را بین ضرایب f و g داشته باشند. چون

$$f \cdot g = \sum_n (\sum_{i+j=n} a_ib_j)x^n$$

باید ارزیابی $\sum_{i+j=n} a_ib_j$ را محاسبه کنیم. برای هر n،

$$V_A(\sum_{i+j=n} a_ib_j) \geq \min_{i+j}\{V_A(a_i) + V_A(b_j)\} \geq V_A(a_{i_۰}) + V_A(b_{j_۰}).$$

از طرفی

$$\sum_{i+j=i_۰+j_۰} a_ib_j = a_{i_۰}b_{j_۰} + \sum_{i\neq i_۰, j\neq j_۰} a_ib_j$$

که برای هر اندیس $i \neq i_۰$ و $j \neq j_۰$ داریم، $V_A(a_ib_j) > V_A(a_{i_۰}) + V_A(b_{j_۰})$. بنابراین،

$$V_A(\sum_{i+j=i_۰+j_۰} a_ib_j) = V_A(a_{i_۰}) + V_A(b_{j_۰}) = V(f) + V(g).$$

قرار می‌دهیم $B = O_V$. در این صورت، $x \in B$ (زیرا طبق تعریف $V(x) = V(۱) = ۰$) و $\overline{x}$ روی K_A متعالی است (زیرا هیچ ترکیب خطی $\overline{x}^n + \overline{a_{n-۱}}\,\overline{x}^{n-۱} + \cdots + \overline{a_۰}$ صفر نمی‌شود.) در آخر باید ثابت کنیم $K_B = K_A(\overline{x})$. فرض کنیم $b \in B$ به گونه‌ای باشد که $V(b) = ۰$. بنابراین $b = \dfrac{f(x)}{g(x)}$ به طوری که $f(x), g(x) \in K[x]$. چون $V(b) = ۰$ نتیجه می‌گیریم $V(f(x)) = V(g(x))$. می‌توانیم فرض کنیم $V(f(x)) = V(g(x)) = ۰$. پس $\overline{f}(\overline{x}) \neq ۰$ و $\overline{g}(\overline{x}) \neq ۰$. از $bg(x) = f(x)$ نتیجه می‌گیریم $\overline{b}\overline{g}(\overline{x}) = \overline{f}(\overline{x})$ و

$$\overline{b} = \frac{\overline{g}(\overline{x})}{\overline{f}(\overline{x})} \in K_A(x).$$

□

لم ۲۸. فرض کنیم $V : K \longrightarrow \Gamma_A$ یک نگاشت ارزیابی و $L = K(x)$ یک توسیع متعالی باشد. همچنین فرض کنیم δ در یک گروه شامل Γ_A باشد به گونه‌ای که برای هر $n \in \mathbb{N}$، $n\delta \notin \Gamma_A$. در این صورت، ارزیابی V به طور یکتا به ارزیابی $W : L \longrightarrow \Gamma + \mathbb{Z}\delta$ توسیع می‌یابد به طوری که $W(x) = \delta$ و $K_V = K_W$.

اثبات. برای مشاهده اثبات می‌توانید به مرجع اصلی درس (کتاب کنفرانس چترارو) صفحات ۹۱ و ۹۲ مراجعه کنید. □

۳.۸ حذف سور در میدانهای ارزیابی بستهٔ جبری

تعریف ۶۵. فرض کنیم T یک تئوری مرتبه اول باشد. یک مدل $\mathfrak{M} \models T$ را κ-اشباع می‌نامیم هرگاه هر مجموعه از فرمول‌ها به صورت $\varphi(x, \overline{a})$ که در آن $\overline{a} \in A \subseteq M$ (M جهان $\mathfrak{M}$) و $|A| < \kappa$، اگر متناهیا در $\mathfrak{M}$ برآورده شود آنگاه در $\mathfrak{M}$ برآورده شود. به عبارت دیگر، اگر هر تعداد متناهی از فرمول‌ها به صورت بالا در M جواب داشته باشد آنگاه کل دستگاه در M جواب دارد.

نتیجه ۲۲. اگر تئوری T دارای مدل باشد آنگاه (بنا به قضیه فشردگی) دارای مدل‌های به اندازه دلخواه اشباع است.

مثال ۵۷. میدان‌های بسته جبری مدل‌های اشباع برای تئوری میدان‌های بسته جبری هستند (البته این نیاز به اثبات دارد!)

در تعریف زیر یک محک جدید برای حذف سور ارائه می‌دهیم.

محک. فرض کنیم T یک تئوری مرتبه اول، $\mathfrak{M}_۱$ مدل T و $\mathfrak{M}_۲$ یک مدل به اندازه کافی اشباع برای T باشند. همچنین فرض کنیم $\mathfrak{A}$ یک زیرساختار مشترک برای $\mathfrak{M}_۱$ و $\mathfrak{M}_۲$ باشد. در این صورت تئوری T سورها را حذف می‌کند اگر برای هر دو نشاندن $f : \mathfrak{A} \longrightarrow \mathfrak{M}_۱$ و $g : \mathfrak{A} \longrightarrow \mathfrak{M}_۲$ بتوانیم f را به نشاندن $h : \mathfrak{M}_۱ \longrightarrow \mathfrak{M}_۲$ گسترش دهیم به طوری که $hof = g$.

اثبات. فرض کنیم برای یک دستگاه معادله جواب x در M_1 (جهان $\mathfrak{M}_1$) و y در M_2 (جهان $\mathfrak{M}_2$) باشد. اگر A جهان $\mathfrak{A}$ باشد آنگاه به راحتی می‌توانیم یک نشاندن میان $A[x]$ و $A[y]$ تعریف کنیم. به همین ترتیب اگر هر یک از ریشه‌های دستگاه را در M_1 به A اضافه کنیم می‌توانیم یک ما به ازا در M_2 بیابیم (چون $\mathfrak{M}_2$ اشباع است) و نشاندن را تشکیل دهیم. به کمک لم زرن می‌توانیم به نشاندن h برسیم که دامنه آن $\mathfrak{M}_1$ و برد آن $\mathfrak{M}_2$ است. □

در ادامه می‌خواهیم ثابت کنیم تئوری میدان‌های ارزیابی بسته جبری دارای حذف سور است. برای رسیدن به این منظور ابتدا باید میدان‌های ارزیابی را در منطق مرتبه اول توصیف کنیم.

تذکر ۳۸. زبان $L_{Val} = \{0, 1, +, -, \cdot, |\}$ زبان میدان‌های ارزیابی است به طوری که در آن $|$ یک نماد رابطه‌ای دو موضعی است. تعبیر این نماد رابطه‌ای دو موضعی در ساختار (K, A) به شکل زیر است،

$$x \mid y \iff V_A(x) \leq V_A(y).$$

اگر T تئوری میدان‌های بسته جبری باشد (که در ابتدای درس آن را به طور کامل معرفی کردیم) آنگاه تئوری میدان‌های بسته جبری ارزیابی به صورت

$$T_{Val} = T \cup \{\neg\ (0 \mid 1), \forall x\ \forall y\ \ (x \mid y \vee y \mid x), \forall x\ \forall y\ \forall z\ \ (x \mid y \leftrightarrow xz \mid yz),$$
$$\forall x\ \forall y\ \forall z\ \ (x \mid y \wedge y \mid z \rightarrow x \mid z)\}$$

است.

قضیه ۴۸. تئوری میدان‌های بسته جبری ارزیابی در زبان بالا سورها را حذف می‌کند.

اثبات. فرض کنیم (E, A) یک مدل تئوری T_{Val} و (F, B) یک مدل اشباع برای T_{Val} باشد که هر دو شامل زیرساختار (K, C) هستند. برای اثبات از محک جدید حذف سور کمک می‌گیریم و به دنبال یافتن نشاندن $h : (E, A) \longrightarrow (F, B)$ هستیم. بدون کاستن از کلیت می‌توانیم فرض کنیم (K, C) یک میدان بسته جبری است. زیرا طبق اثبات‌های جلسات گذشته می‌توانیم هر ارزیابی را به حلقه کسرها گسترش دهیم و به طور یکتا آن را به میدان‌های بسته جبری ببریم. پس هر عنصر $x \in E \setminus K$ متعالی است.

در یک حالت خاص، فرض کنیم گروه ارزیابی و میدان پیمانه‌های (E, A) با (K, C) برابر باشند $(K_C = K_A, \Gamma_C = \Gamma_A)$. اگر $x \in E \setminus K$ عنصر دلخواه (x متعالی است) و $f(x) \in K[x]$ یک چندجمله‌ای باشد آنگاه چون K بسته جبری است می‌توان $f(x)$ را به صورت $f(x) = \alpha \prod_i (x - a_i)$ تجزیه کرد. از طرفی

$$V_A(f) = V_A(\alpha) + \sum_i (V_A(x - a_i)) \in \Gamma_A = \Gamma_C.$$

بنابراین اگر بخواهیم یک عنصر متعالی مانند y به گونه‌ای بیابیم که نشاندن $h_1 : K[x] \longrightarrow K[y]$ حافظ ارزیابی‌ها باشد باید دستگاه معادله

$$\begin{cases} V_A(x - a_1) = V_A(y - a_1) \\ \vdots \\ V_A(x - a_n) = V_A(y - a_n) \end{cases}$$

را حل کنیم. جالب این است که ما جواب دستگاه بالا در خود K پیدا خواهیم کرد.

حل این دستگاه معادله می‌تواند به یافتن یک عنصر $y \in K$ که $V_A(y - x) > V_A(x - a)$ تقلیل یابد چرا که در این صورت

$$V_A(y - a_i) = V_A(y - x + x - a_i) = V_A(x - a_i).$$

بدون کاستن از کلیت فرض کنیم $V_A(x - a_1)$ از بقیه ارزیابی‌ها بیشتر باشد. همچنین فرض کنیم $b \in K$ به گونه‌ای باشد که $V_A(x - a_1) = V_A(b)$. بنابراین $V_A(\frac{x - a_1}{b}) = 0$ و

$$\frac{x - a_1}{b} \in K_A = K_C.$$

پس عناصر $c \in C$ (به طوری که $V(c) = 0$) و $\epsilon \in M_C$ وجود دارند که $\frac{x - a_1}{b} = c + \epsilon$ و یا $x = bc + b\epsilon + a_1$. به عنوان تمرین نشان دهید اگر $y := bc + a_1$ آنگاه $V_A(y - x) > V_A(x - a_1)$ و به نتیجه مورد نظر می‌رسیم.

پس در این حالت خاص، به نگاشت h دست پیدا کنیم. اما نکته مهم این است که اگر این حالت خاص برقرار نباشد به کمک قضایا و لم‌های جلسات گذشته می‌توانیم ساختاری را جایگزین ساختار (K, C) کنیم که $K_C = K_A$ و $\Gamma_C = \Gamma_A$.

به طور دقیق‌تر، فرض کنیم $K_A \neq K_C$. پس $x \in E$ چنان وجود دارد که $\overline{x} \in K_A \setminus K_C$. چون K_C جبری است پس $\overline{x}$ روی K_C متعالی است. پس می‌توان ارزیابی را به $K[x]$ به نحوی گسترش داد که $\overline{x}$ به K_C اضافه شود اما گروه Γ_C تغییر نکند. بنابراین اگر در F عنصر y به گونه‌ای باشد که $\overline{y}$ روی K_C متعالی باشد آنگاه $K[x] \cong K[y]$ و می‌توان K را بزرگتر کرد. همچنین فرض کنیم $\Gamma_A \neq \Gamma_C$. پس $x \in E$ چنان وجود دارد که $V_A(x) \notin \Gamma_C$. در این صورت می‌توانیم V_A را به $K[x]$ گسترش دهیم به نحوی که گروه ارزیابی برابر با $\Gamma_A + \mathbb{Z}V_A(x)$ شود. اگر $y \in F$ را به گونه‌ای در نظر بگیریم که $V_B(y)$ در هسته بخش‌پذیر Γ_A نباشد آنگاه $K[x] \cong K[y]$ و می‌توان K را بزرگتر کرد به طوری که $K_C = K_A$. □

به هر مجموعهٔ به صورت

$$\{x : v(x - a) > r\}$$

یک گوی به شعاع گفته می‌شود. منظور از یک پنیر سوئیسی، یک گوی به شکل بالاست که از داخل آن متناهی گوی کوچکتر برداشته شده است. قضیهٔ زیر نتیجهٔ ساده‌ای از حذف سور اثبات شده در این جلسه است، با این حال از ارائهٔ اثبات آن صرف نظر کرده‌ایم.

نتیجه ۲۳. فرض کنیم (K, A) یک میدان ارزیابی بستهٔ جبری باشد. اگر مجموعه X در (K, A) تعریف پذیر باشد آنگاه X اجتماعی متناهی از پنیرهای سوئیسی است.

فصل ۹

تمرینها

۱.۹ تمرینهای نوبت اول، مهلت تحویل پنج‌شنبه ۱۵ مهر ساعت ۲۴

در نوشتن جملات خواسته شده در تمرینهای زیر به نحوهٔ صحیح فرمول نویسی دقت کنید. مثلا ننویسید

$$\forall x, \forall y,\ x < y$$

زیرا در تعریف فرمولها، علامت کاما نداشتیم. همچنین به پرانتزگذاری توجه کنید. مثلاً

$$\exists x \exists y\ (x < y \wedge x < y + ۱)$$

با

$$\exists x \exists y\ x < y \wedge x < y + ۱$$

تفاوت دارد. همچنین توجه کنید که تحویل سه تمرین الزامی است.

تمرین. زبانِ $L = \{f, g, c\}$ را در نظر بگیرید که در آن f یک نماد تابعی دو موضعی، g یک نماد تابعی تک موضعی و c یک نماد ثابت هستند. فرض کنید $t = fgfv_۱v_۲ggfcv_۳$. فرض کنید $\mathfrak{M}_۱ = (\mathbb{R}, +, e^x, ۱۰)$ و $\mathbb{M}_۲ = (\mathbb{N}, \cdot, ۳ \cdot x, ۱)$. تابعهای $t^{\mathfrak{M}_۱}(a, b, c)$ و $t^{\mathfrak{M}_۲}(a, b, c)$ را محاسبه کنید.

تمرین. زبانِ $L = \{\times, e\}$ را برای گروه‌ها در نظر بگیرید. یک جملهٔ φ پیدا کنید به طوری که اگر $\mathfrak{M} \models \varphi$ آنگاه $\mathfrak{M} \cong \mathbb{Z}_۲ \otimes \mathbb{Z}_۲$.

تمرین. در زبانِ $L = \{+, ۰\}$ نشان دهید که $\mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z}$.

تمرین. در زبانِ $L = \{E\}$ که در آن E یک نماد رابطه‌ای دو موضعی است، یک تئوری T بنویسید به طوری که اگر $\mathfrak{M} = (M, E^{\mathfrak{M}}) \models T$ آنگاه $E^{\mathfrak{M}}$ یک رابطهٔ هم‌ارزی باشد که تنها دو کلاس دارد و هر دوی این کلاسها نامتناهی هستند.

تمرین. فرض کنید $\mathfrak{M}, \mathfrak{N}$ دو L ساختار باشند و $\eta : \mathfrak{M} \to \mathfrak{N}$ یک L ایزومرفیسم باشد (با استفاده از استقرا روی ساخت فرمولها) نشان دهید که برای هر L فرمولِ $\varphi(x_۱, \ldots, x_n)$ و هر $a_۱, \ldots, a_n \in M$ داریم

$$\mathfrak{M} \models \varphi(a_۱, \ldots, a_n) \Leftrightarrow \mathfrak{N} \models \varphi(\eta(a_۱), \ldots, \eta(a_n))$$

۲.۹ تمرینهای نوبت دوم، تحویل پنج‌شنبه ۲۹ مهرماه

تمرین. فرض کنیم $X \subseteq \mathbb{R}^n$ در $(\mathbb{R}, +, \cdot, ۰, ۱, <)$ قابل تعریف باشد. ثابت کنید بستار توپولوژیک X هم قابل تعریف است.

تمرین. در زبان $\mathcal{L} = \{+, \cdot, <, ۰, ۱\}$، ساختار $\mathcal{N} = (\mathbb{N}, +, \cdot, <, ۰, ۱)$ را در نظر بگیرید. نشان دهید که یک $\mathcal{L}$-ساختارِ $\mathcal{M}$ وجود دارد به‌طوری‌که $\mathcal{M} \equiv \mathcal{N}$ ولی $\mathcal{M}$ دارای یک عدد است که از همه اعداد طبیعی $(۱, ۱ + ۱, ۱ + ۱ + ۱, \ldots)$ بزرگتر است.

تمرین. در زبانِ $\mathcal{L} = \{<\}$ که $<$ یک نماد رابطه‌ای دو موضعی است، فرض کنید تئوری T توسیعی از تئوریِ مجموعه‌های مرتب خطی است به‌طوری‌که T دارای مدل‌های نامتناهی است. نشان دهید $\mathcal{M} \models T$ و یک نشاندنِ حافظ ترتیب $\sigma : \mathbb{Q} \to \mathcal{M}$ وجود دارند.
برای مثال اگر $T = \text{Th}(\mathbb{Z}, <)$، آنگاه $\mathcal{M} \models T$ و نشاندن $\sigma : \mathbb{Q} \to \mathcal{M}$ وجود دارند. (اگر $\mathcal{M}$ یک $\mathcal{L}$-ساختار باشد، آنگاه $\text{Th}(\mathcal{M}) = \{\phi : \mathcal{M} \models T$ و ϕ یک جمله است$\}$)

تمرین. در زبان $\mathcal{L} = \{E\}$ که E یک نماد رابطه‌ای دو موضعی است، فرض کنید T تئوری یک رابطه هم‌ارزی است که نامتناهی کلاسِ نامتناهی دارد. به سوالات زیر پاسخ دهید.

الف) اصول تئوری T را بنویسید.

ب) تئوری T چند مدل از اندازه‌های $\aleph_۰$، $\aleph_۱$، $\aleph_۲$ و $\aleph_{\omega_۱}$ دارد.

ج) آیا تئوری T کامل است؟ (تئوری T را کامل می‌نامند هرگاه برای هر جمله‌ی φ، $T \models \varphi$ یا $T \models \neg\varphi$).

۳.۹ تمرینهای نوبت سوم، تاریخ تحویل: حداکثر تا پنجشنبه ۶ آبان

تمرین. در حلقه‌ی $\frac{R}{I}$، ایده‌آل تولید شده توسط یک عنصر مانند $a + I$ چگونه است؟

تمرین. فرض کنید R یک حلقه جابجایی و یکدار و I ایده‌آلی از R است. عبارت‌های زیر را ثابت کنید.

۱. $\frac{R}{I}$ دامنه است اگر و تنها اگر I اول باشد.

۲. $\frac{R}{I}$ میدان است اگر و تنها اگر I ماکسیمال باشد.

تمرین. ثابت کنید مشخصه‌ی هر دامنه جابجایی و یکدار یا صفر است یا عددی اول است.

تمرین. فرض کنید K یک حلقه جابجایی و یکدار است به طوری که $۰_K \neq ۱_K$. نشان دهید K یک میدان است اگر و تنها اگر هر همریختی مانند $f : K \to R$، که R یک حلقه دلخواه باشد، تکریختی است.

۴.۹ تمرینهای نوبت چهارم زمان تحویل: ۲۵ آبان

تمرین اول فرض کنید $\mathbb{C}$ میدان اعداد مختلط باشد. نشان دهید

$$\mathbb{C} \cong \frac{\mathbb{R}[x]}{\langle x^۲ + ۱ \rangle}.$$

تمرین دوم فرض کنید $K \subseteq L$ یک توسیع میدانی باشد و $\alpha \in L$. فرض کنید که $p(x) \in K[x]$ یک چندجمله ای با حداقل درجه باشد به طوری که $p(\alpha) = ۰$.

۱. نشان دهید که اگر $q(\alpha) = ۰$ آنگاه $p(x) | q(x)$.

۲. نشان دهید که میدان تولید شده توسط K, α در داخل L ایزومرف است با $\frac{K[x]}{\langle p(x) \rangle}$.

تمرین سوم فرض کنید $p(x)$ یک چندجمله ای تحویل ناپذیر با درجهٔ ۳ در $K[x]$ باشد. معکوس یک عنصرِ $(ax^۲ + bx + c) + \langle p(x) \rangle$ در میدان $\frac{K[x]}{\langle p(x) \rangle}$ را محاسبه کنید.

تمرین چهارم نشان دهید چندجمله ای $x^۴ + x + ۱ \in \mathbb{Z}_۲[x]$ تحویل ناپذیر است.

تمرین پنجم آیا جملهٔ زیر درست است:
چندجمله ای $f[x] \in K[x]$ تحویل ناپذیر است اگروتنهااگر ریشه ای در K نداشته باشد.

۵.۹ تمرینهای نوبت پنجم زمان تحویل پنج‌شنبه ۱۲ آذر

تمرین اول فرض کنید K یک میدان بستهٔ جبری و $V \subseteq K^n$ یک مجموعهٔ بستهٔ زاریسکی باشد (یعنی مجموعهٔ ریشه‌های مشترک تعدادی متناهی چندجمله‌ای). همچنین فرض کنید $f : K[x_۱, \ldots, x_n] \to K[x_۱, \ldots, x_n]$ یک نگاشت چندجمله‌ای باشد؛ یعنی

$$f(x_۱, \ldots, x_n) = (f_۱(x_۱, \ldots, x_n), \ldots, f_n(x_۱, \ldots, x_n))$$

که در آن f_i ها چندجمله‌ای هستند. نشان دهید که $f(V)$ یک مجموعهٔ ساخته‌شدنی است. (راهنمایی: از حذف سور استفاده کنید).

تمرین دوم فرض کنید $K \leq E \leq F$ توسیعهای میدانی باشد. همچنین فرض کنید $e_۱, \ldots, e_k$ پایه‌ای برای E به عنوان یک فضای برداری روی K باشند و $f_۱, \ldots, f_m$ پایه‌ای برای F به عنوان یک فضای برداری روی E باشند. نشان دهید $e_i f_j$ ها پایه‌ای برای F به عنوان یک فضای برداری روی K هستند.

تمرین سوم نشان دهید که حلقهٔ R یک میدان است اگروتنهااگر $\langle ۰ \rangle$ یک ایده‌آل ماکزیمال در آن باشد. (بررسی کنید که در این حالت، R ایده‌آل ماکزیمال دیگری ندارد).

تمرین چهارم یک تئوری مرتبهٔ اول برای حلقه‌های موضعی بنویسید.

تمرین پنجم نشان دهید $V(I \cap J) = V(I) \cup V(J)$.

راهنمایی. سمت $\supseteq$ به راحتی قابل اثبات است. برای اثباتِ $\subseteq$ فرض کنید x نه در $V(I)$ و نه در $V(J)$ باشد. بنابراین یک چندجمله‌ای f در I هست به طوری که $f(\bar{x}) \neq ۰$ و یک چندجمله‌ای g در J هست به طوری که $g(\bar{x}) \neq ۰$. یک چندجمله‌ای در $I \cap J$ پیدا کنید که در $\bar{x}$ صفر نمی‌شود.

۶.۹ تمرینهای نوبت ششم، زمان تحویل دوشنبه ۲۹ آذر

تمرین اول فرض کنید R یک حلقهٔ ارزیاب باشد. نشان دهید برای دو ایده‌آلِ I, J از R یا $I \subseteq J$ یا $J \subseteq I$ (به بیان دیگر، ایده‌آلها در حلقه‌های موضعی تشکیل یک زنجیر می‌دهند).

تمرین دوم فرض کنید $I \subseteq K[\bar{x}]$ یک ایده‌آل باشد. نشان دهید که

$$V(I(V(I)) = V(I).$$

تمرین سوم نشان دهید که حلقهٔ $K[x_۱, \ldots, x_n]$ در حلقهٔ $K[[x_۱, \ldots, x_n]]$ چگال است.

تمرین چهارم نشان دهید که $I(X)$ (تعریف ۴۲) یک ایده‌آل اولیه است.

۷.۹ ،تمرینات سری هفتم تاریخ تحویل: پنجشنبه ۱۶ دی

تمرین ۱۵. نشان دهید که توسیع میدان $K \subset M$ نرمال است اگر و تنها اگر برای هر $\sigma : L \to L$ (یعنی $\sigma \in Aut(\frac{L}{K})$ خودریختی است و σ روی K به صورت نقطه‌وار ثابت است) داشته باشیم: $\sigma(M) = M$.

تمرین ۱۶. می‌دانیم که هر عنصر $a \in \mathbb{Z}_p$ دارای نمایش یکتایی به صورت $a = \sum_{i=0}^{\infty} a_i p^i$ است که $a_i \in \{0, \dots, p-1\}$. وارون عنصر $a = a_0$ که $a_0 \neq 0$ را در حلقه‌ی $\mathbb{Z}_p$ حساب کنید.

تمرین ۱۷. فرض کنید (K, A) یک میدان ارزیابی باشد. فرض کنید $\bar{b_1}, \dots, \bar{b_n}$ روی k_A مستقل خطی‌اند. نشان دهید که $V(\sum_{i=1}^{n} a_i b_i) = \min\{V(a_i)\}$.

تمرین ۱۸. فرض کنید $(R, |\cdot|)$ یک حلقه نرم‌دار باشد به طوری $|x| \leq 0$ برای هر $x \in R$. و $x \in R$. نشان دهید که اگر $|x| < 1$، آنگاه x وارون‌پذیر نیست.

تمرین ۱۹. ارزشیابی V_p را روی Q در نظر بگیرید. حلقه‌ی ارزیاب و ایده‌آل ماکزیمال آن و میدان پیمانه‌ها را مشخص کنید.

۸.۹ امتحان پایان‌ترم

قوانین

۱. اگر به جای تهیه اسلاید روی کاغذ جواب سوالها را می‌نویسید، کاغذ را به طور افقی قرار دهید و حاصل نهائی را به صورت تنها یک فایل پی‌دی‌اف درآورید.

۲. برای اسلایدهائی که با نرم‌افزار تهیه شود ارزش قائل خواهیم بود.

۳. اگر مدعی کسب نمرهٔ n هستید باید پرسشهای مربوط به بخش ۱ تا n را کامل پاسخ دهید.

۴. اگر برای سوالی اسلاید تهیه نشود، نمرهٔ آن سوال کسر خواهد شد.

۵. امتحان در روز قانونی خود با شروع از ساعت ۸ برگزار خواهد شد. برنامهٔ زمان‌بندی شرکت در امتحان متعاقبا اعلام خواهد شد.

۶. ساعت ۱۲ روز قبل از امتحان، باید اسلایدها به من ایمیل شده باشند.

۷. در حین پاسخگوئی به سوالات صادق باشید. صرف نوشتن چیزها به منزلهٔ دانستن آنها نیست. مدرس با پرسیدن جزئیات سطح دانش شما را به چالش خواهش کشید.

۸. در پاسخ یک سوال باید قضایا و لمهائی را که بدان مربوط هستند نیز بدانید.

۹. سه نمره از درس به تمرینها اختصاص داده شده است.

۱۰. امتحان در همان سامانهٔ کلاس درس گرفته خواهد شد (بیگ‌بلوباتن).

۱۵-۱۸

تمرین ۲۰. نشان دهید که تئوری میدانهای بستهٔ جبری ارزیابی در زبان مناسب سورها را حذف می‌کند.

تمرین ۲۱. فرض کنید $(K, A) \subseteq (L, B)$، $(K, A) \subseteq (L', B')$ دو توسیع از میدانهای ارزیابی بستهٔ جبری باشد به طوری که $k_A = k_B$ و $\Gamma_A = \Gamma_B$ و L' به اندازهٔ کافی اشباع باشد. فرض کنید $x \in L - K$. نشان دهید که $y \in L' - K$ چنان یافت می‌شود که $K(x)$ و $K(y)$ به عنوان میدانهای ارزیابی با هم ایزومرف باشند.

تمرین ۲۲. فرض کنید (K, A) یک میدان ارزیابی باشد و $L = K(x)$ یک توسیع متعالی از K باشد. نشان دهید که ارزیابی را به طور یکتا می‌توان از K به L گسترش داد به گونه‌ای که $v(x) \geq 0$ و $\bar{x}$ روی K متعالی باشد.

تمرین ۲۳. فرض کنید $(K, A) \subseteq (L, B)$ توسیعی از میدانهای ارزیابی باشد. نشان دهید که

$$[L : K] \geq [k_B : k_A] \times [\Gamma_B : \Gamma_A].$$

تمرین ۲۴. فرض کنید (K, A) یک میدان ارزیابی باشد و β عنصری جبری روی k_A باشد و $\bar{p}(x)$ چندجمله‌ای مینی مال آن باشد. فرض کنید b یک ریشهٔ $p(x)$ در یک میدان شامل K باشد. نشان دهید که ارزیابی به طور یکتا به $K(b)$ گسترش می‌یابد و میدان پیمانه‌های حاصل ایزومرف با $k(\beta)$ است.

۱۲-۱۵

تمرین ۲۵. فرض کنید (K, A) یک میدان ارزیابی باشد و L توسیعی جبری از K یاشد. نشان دهید که هر حلقه‌ی ارزیاب L که بر A چیره باشد به صورت B_n است که B بستار صحیح A در L و n یک ایده‌آل ماکزیمال آن است.

تمرین ۲۶. نشان دهید که حلقه‌های ارزیاب بستهٔ صحیح هستند.

تمرین ۲۷. فرض کنید K یک میدان و $A \subseteq K$ یک حلقهٔ موضعی باشد. نشان دهید که بستار صحیح A در K برابر با اشتراک تمام حلقه‌های ارزیاب K است که بر A چیره هستند.

تمرین ۲۸. فرض کنید A یک دامنه موضعی باشد که در میدان کسرهای خود بستهٔ صحیح است و $A \subseteq K$ یک میدان باشد. همچنین فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد و B بستار صحیح A در L باشد. نشان دهید که برای هر دو ایده‌آل ماکزیمال $n, n' \subseteq B$ یک اتومرفیسم $\sigma \in Aut(L/K)$ موجود است که $\sigma(n) = n'$.

۱۰-۱۲

تمرین ۲۹. فرض کنید $A \subseteq B$ دو دامنه و B روی A صحیح باشد و p یک ایده‌آل اول از A باشد. نشان دهید که B یک ایده‌آل اول دارد که بر p چیره است.

تمرین ۳۰. فرض کنید K یک میدان و $A \subseteq K$ یک حلقهٔ موضعی باشند. نشان دهید که K یک حلقهٔ ارزیاب دارد که بر A چیره است.

تمرین ۳۱. فرض کنید $A \subseteq B$ دو دامنه باشند به طوری که B روی A صحیح است. نشان دهید که B میدان است اگروتنهااگر A میدان باشد.

تمرین ۳۲. نشان دهید که هر حلقهٔ ارزیاب از یک نگاشت ارزیابی ناشی می‌شود.

تمرین ۳۳. فرض کنید v یک ارزیابی روی میدان K باشد. نشان دهید O_v یک حلقهٔ موضعی ارزیاب است و ایده‌آل ماکزیمال آن از عناصر با ارزیابی اکیدا مثبت تشکیل شده است.

تمرین ۳۴. نگاشت ارزیابی را روی $\mathbb{C}((t))$ و $\mathbb{Q}_p$ با تمامی اجزای آنها مشخص کنید.

تمرین ۳۵. نشان دهید که $\mathbb{Z}_p$ در $\mathbb{Q}_p$ قابل تعریف است.

تمرین ۳۶. حلقهٔ پی‌ادیکها $(\mathbb{Z}_p)$ را تعریف کنید. نشان دهید که یک حلقهٔ موضعی است و ایده‌آل ماکزیمال آن را مشخص کنید.

تمرین ۳۷. فرض کنید $f \in K[x]$ یک چند جمله‌ای تحویل‌ناپذیر باشد و مشخصهٔ K صفر باشد. نشان دهید که f ریشهٔ مضاعف ندارد.

تمرین ۳۸. فرض کنید (R, m) یک حلقهٔ موضعی هنسلی و $k = \frac{R}{m}$. نشان دهید که برداشتی از k در داخل R موجود است.

تمرین ۳۹. قضیهٔ گرین‌لیف و اکس-کوچن را بیان و اثبات کنید.

تمرین ۴۰. لم هنسل را دربارهٔ حلقه‌های نرمدار کامل بیان و اثبات کنید.

۰ تا ۱۰

تمرین ۴۱. نشان دهید که $K[X]$ حلقهٔ موضعی نیست ولی $K[[X]]$ حلقهٔ موضعی است.

تمرین ۴۲. نشان دهید که $\frac{\mathbb{Z}}{p^{۲}\mathbb{Z}}$ یک حلقهٔ موضعی است و ایده‌آل ماکزیمال آن را مشخص کنید.

تمرین ۴۳. قضیهٔ ریشه‌های هیلبرت را با استفاده از مفهوم حذف سور در میدان‌های بستهٔ جبری ثابت کنید.

تمرین ۴۴. نشان دهید که تئوری میدانهای بستهٔ جبری سورها را حذف می‌کند.

تمرین ۴۵. نشان دهید که هر میدان دارای یک بستار جبری یکتاست.

تمرین ۴۶. قضیهٔ فشردگی در نظریهٔ مدل را بیان کنید.