مرور جبر کارشناسی

تعریف ۱.۱ نیم‌گروه

فرض کنید S مجموعه‌ای ناتهی باشد و یک عمل دوتایی $\cdot$ روی S را در نظر بگیرید. اگر این عمل شرکت‌پذیر باشد یعنی:

$$\forall a, b, c \in S \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

آنگاه S را همراه با عمل $\cdot$ یک **نیم‌گروه** [a] می‌نامند.

[a] Semigroup

تعریف ۲.۱ گروه

فرض کنید مجموعه ناتهی G همراه با عمل دوتایی $\cdot$ در شرایط زیر صدق کند:

$$\forall a, b, c \in G \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

$$\exists e \in G \; \forall a \in G \quad a \cdot e = e \cdot a = a$$ (وجود عنصر همانی)

$$\forall a \in G \; \exists b \in G \quad a \cdot b = b \cdot a = e$$ (وجود عنصر وارون)

در این صورت $(G, \cdot)$ را یک **گروه** می‌نامند.

تذکر ۳.۱

غالبا بجای $a \cdot b$ می‌نویسیم ab.

تعریف ۴.۱ گروه آبلی

اگر به ازای هر $a, b \in G$ داشته باشیم:

$$a \cdot b = b \cdot a$$

گروه را **آبلی یا جابجایی** می‌نامند.

تعریف ۵.۱ زیرگروه

اگر $(G, \cdot)$ یک گروه باشد و $H \subseteq G$ زیرمجموعه‌ای ناتهی از G باشد که خودش نیز تحت عمل $\cdot$ یک گروه باشد، آنگاه H را یک **زیرگروه** G می‌نامند و می‌نویسیم:

$$H \leq G$$

قضیه ۶.۱ محک فشرده

زیرمجموعه ناتهی $H \subseteq G$ زیرگروه G است اگر و تنها اگر:

$$\forall a, b \in H \quad a \cdot b^{-1} \in H$$

مثال ۷.۱

$(\mathbb{Z}, +)$، گروه اعداد صحیح با عمل جمع را در نظر بگیرید. زیرمجموعه‌ی $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ یعنی اعداد زوج، با همان عمل جمع، یک زیرگروه از $\mathbb{Z}$ است، بنابراین:

$$(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$$

اثبات. برای اثبات اینکه $(2\mathbb{Z}, +)$ زیرگروه است، از محک فشرده استفاده می‌کنیم: باید نشان دهیم اگر $a, b \in 2\mathbb{Z}$ باشند، آنگاه $a - b \in 2\mathbb{Z}$. ازآنجا که $a = 2m$ و $b = 2n$ به ازای $m, n \in \mathbb{Z}$، آنگاه:

$$a - b = 2m - 2n = 2(m - n)$$

که چون $m - n \in \mathbb{Z}$، پس $a - b \in 2\mathbb{Z}$. بنابراین، $a + (-b) \in 2\mathbb{Z}$ و با استفاده از محک فشرده نتیجه می‌گیریم که $(2\mathbb{Z}, +)$ زیرگروه $(\mathbb{Z}, +)$ است.

□

مثال ۸.۱

$(\mathbb{Z},+)$، گروه اعداد صحیح با عمل جمع را در نظر بگیرید. برای هر $n \in \mathbb{N}$، مجموعه $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ با همان عمل جمع، زیرگروه $\mathbb{Z}$ است:

$$(n\mathbb{Z},+) \leq (\mathbb{Z},+)$$

اثبات. برای $a, b \in n\mathbb{Z}$، داریم $a = nk$، $b = nl$ به ازای $k, l \in \mathbb{Z}$، پس:

$$a - b = nk - nl = n(k-l) \in n\mathbb{Z}$$

بنابراین، $n\mathbb{Z}$ تحت تفاضل بسته است و زیرگروه $\mathbb{Z}$ می‌باشد.

□

مثال ۹.۱

$(\mathbb{N}, \times)$ گروه نیست.
زیرا برای مثال عدد $2 \in \mathbb{N}$ هیچ عضو معکوسی نسبت به ضرب در $\mathbb{N}$ ندارد. یعنی عدد طبیعی‌ای وجود ندارد که $2 \times x = 1$ را برآورده کند.
بنابراین، شرط وجود عنصر معکوس برای همه اعضا برقرار نیست و $(\mathbb{N}, \times)$ گروه نیست.

تعریف ۱۰.۱

برای هر میدان F، مجموعه‌ی F^* به صورت زیر تعریف می‌شود:

$$F^* = F \setminus \{0\}$$

یعنی مجموعه‌ی تمام اعضای ناصفر F. این مجموعه تحت عمل ضرب، یک گروه تشکیل می‌دهد. به طور خاص:

- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$: اعداد گویا ناصفر
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$: اعداد حقیقی ناصفر
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$: اعداد مختلط ناصفر

هر یک از این مجموعه‌ها با عمل ضرب، یک گروه ضربی می‌سازند.

تعریف ۱۱.۱

اگر F یک میدان [a] باشد، آنگاه $M_n(F)$ مجموعه‌ی تمام ماتریس‌های $n \times n$ با درایه‌هایی از F است:

$$M_n(F) = \{A = (a_{ij}) \mid 1 \leq i, j \leq n,\ a_{ij} \in F\}$$

روی $M_n(F)$ می‌توان اعمال مختلفی تعریف کرد، مانند جمع ماتریسی و ضرب ماتریسی.
معمولاً $(M_n(F), +)$ یک گروه آبلی است (نسبت به جمع ماتریسی) و $(M_n(F), \cdot)$ یک نیم‌گروه است (نسبت به ضرب ماتریسی، ولی بسته به F و n ممکن است گروه نباشد زیرا ماتریس‌های ناتبدیل وارون ندارند).

[a] Field

مثال ۱۲.۱

در ادامه چند مثال از زیرگروه‌ها آورده شده است:

$$(\mathbb{Z},+) \leq (\mathbb{Q},+)$$
$$(\mathbb{Q},+) \leq (\mathbb{R},+)$$
$$(\mathbb{Q}^*,\cdot) \leq (\mathbb{R}^*,\cdot)$$
$$(M_n(\mathbb{Q}),+) \leq (M_n(\mathbb{R}),+)$$

مثال ۱۳.۱ گروه

مثال‌هایی از گروه

$(\mathbb{C},+)$ (گروه جمعی اعداد مختلط)

$(\mathbb{C}^*,\cdot)$ (گروه ضربی اعداد مختلط ناصفر)

$(M_n(\mathbb{C}),+)$ (گروه ماتریس‌های $n \times n$ مختلط با جمع)

تعریف ۱۴.۱

برای عدد صحیح $n \geq 2$، مجموعه‌ی باقیمانده‌های صحیح پیمانه‌ای را به صورت زیر تعریف می‌کنیم:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

که در آن $\overline{a}$ نمایانگر کلاس پیمانه‌ای a نسبت به n است، یعنی:

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$$

عمل جمع روی $\mathbb{Z}_n$ به صورت زیر تعریف می‌شود:

$$\overline{i} + \overline{j} := \overline{i+j}$$

به این ترتیب، $(\mathbb{Z}_n, +)$ یک گروه آبلی متناهی است.

اثبات خوش‌تعریف بودن عمل جمع. فرض کنید $\bar{i} = \overline{i'}$ و $\bar{j} = \overline{j'}$. آنگاه به ازای $k, \ell \in \mathbb{Z}$ داریم:

$$i = i' + kn \quad \text{و} \quad j = j' + \ell n$$

بنابراین:

$$i + j = i' + j' + (k + \ell)n \Rightarrow i + j \equiv i' + j' \pmod{n}$$

یعنی:

$$\overline{i + j} = \overline{i' + j'}$$

پس:

$$\bar{i} + \bar{j} = \overline{i + j} = \overline{i' + j'} = \overline{i'} + \overline{j'}$$

بنابراین، عمل جمع خوش‌تعریف است.

تعریف ۱۵.۱ زیرگروه نرمال

زیرگروه N از گروه G را **نرمال** گویند اگر:

$$\forall g \in G \quad gNg^{-1} \subseteq N$$

که معادل است با:

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} \subseteq N$$

در این صورت می‌نویسیم $N \trianglelefteq G$.

مثال ۱۶.۱

تمام زیرگروه‌های آبلی نرمال هستند.

مثال ۱۷.۱

گروه دیهدرال $D_n = \langle a, b \mid a^n = b^2 = e,\ bab^{-1} = a^{-1} \rangle$ را در نظر بگیرید.
اعضای این گروه عبارت‌اند از:

$$\{e, a, a^2, \dots, a^{n-1},\ b, ab, a^2b, \dots, a^{n-1}b\}$$

زیرگروه مولد a که برابر است با:

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

یک زیرگروه نرمال در D_n است، یعنی:

$$\langle a \rangle \trianglelefteq D_n$$

اثبات. کافی است نشان دهیم که $b\langle a \rangle b^{-1} \subseteq \langle a \rangle$. برای هر $a^k \in \langle a \rangle$ داریم:

$$ba^kb^{-1} = (bab^{-1})^k = (a^{-1})^k = a^{-k} \in \langle a \rangle$$

پس $b\langle a \rangle b^{-1} \subseteq \langle a \rangle$ و از آنجا که D_n توسط a و b تولید شده، برای همه عناصر $g \in D_n$ داریم $g\langle a \rangle g^{-1} \subseteq \langle a \rangle$. بنابراین، $\langle a \rangle$ زیرگروه نرمال در D_n است.

قضیه ۱.۱۸

اگر $G \leq H$ و $[G:H]=2$ آنگاه $H \trianglelefteq G$.

اثبات. چون اندیس برابر ۲ است، G دقیقاً دو هم‌دسته‌ی راست دارد: H و $G \setminus H$. حال اگر $g \in H$ باشد، آنگاه $gH = H = Hg$. و اگر $g \in G \setminus H$ باشد، آنگاه $gH = G \setminus H = Hg$. پس برای همه $g \in G$ داریم $gH = Hg$، یعنی همه‌ی هم‌دسته‌های چپ و راست با هم برابرند و H نرمال است.

تعریف ۱۹.۱ هم‌دستهٔ راست

اگر $G \geq H$ و $g \in G$، هم‌دستهٔ راست H نسبت به g به صورت زیر تعریف می‌شود:

$$Hg = \{hg \mid h \in H\}$$

مثال ۲۰.۱

مثال. در گروه D_{2n} با فرض $H = \langle a \rangle$ دو هم‌دستهٔ متمایز داریم:

$$H \quad \text{و} \quad Hb$$

که در واقع دو مجموعهٔ متمایزند:

$$\{e, a, \dots, a^{n-1}\} \neq \{e, a, \dots, a^{n-1}\}b$$

اثبات. هر عضو از D_{2n} یا به صورت دوران a^k است یا به صورت بازتاب $a^k b$ برای $0 \leq k \leq n-1$، بنابراین:

$$D_{2n} = H \dot{\cup} Hb.$$

در نتیجه، $[D_{2n} : H] = 2$ و بنابراین حداکثر دو هم‌دستهٔ راست داریم: H و Hb.
برای بررسی اینکه این دو هم‌دسته متفاوتند، فرض کنید $Hb = H$. آنگاه $b \in H$ و در نتیجه $b = a^m$ برای عددی صحیح m خواهد بود. اما در این صورت:

$$bab^{-1} = a^m a a^{-m} = a$$

که این با رابطهٔ تعریف‌شده‌ی گروه یعنی $bab^{-1} = a^{-1}$ در تضاد است، مگر اینکه $n = 2$ باشد. بنابراین $b \notin H$ و $Hb \neq H$.
(برای مورد خاص $n = 2$ داریم $D_4 = \{e, a, b, ab\}$ با روابط $a^2 = b^2 = e$ و $ab = ba$؛ در این حالت $H = \{e, a\}$ و $Hb = \{b, ab\}$ هستند که به‌وضوح متمایزند.)

لم ۲۱.۱

اگر $G \triangleleft N$ باشد، آنگاه برای هر $g \in G$ داریم:

$$gN = Ng$$

اثبات. از آنجا که $G \triangleleft N$ است، برای هر $g \in G$ داریم $gNg^{-1} = N$.
ابتدا نشان می‌دهیم $gN \subseteq Ng$: برای هر $n \in N$، داریم

$$gn = gn1 = gn(g^{-1}g) = (gng^{-1})\, g \in Ng$$

چون $gng^{-1} \in N$ است.
برعکس، نشان می‌دهیم $Ng \subseteq gN$: برای هر $n \in N$، داریم

$$ng = g\,(g^{-1}ng) \in gN$$

چون $g^{-1}ng \in N$ است.
در نتیجه، برای هر $g \in G$ داریم $gN = Ng$.

تذکر ۲۲.۱

برای هر $a, b \in G$ داریم:

$$Ha = Hb \iff ab^{-1} \in H$$

اثبات. $(\Rightarrow)$ اگر $Ha = Hb$، آنگاه $a \in Hb$، بنابراین $a = hb$ برای عضوی $h \in H$. پس:

$$ab^{-1} = h \in H.$$

$(\Leftarrow)$ اگر $ab^{-1} \in H$، بنویسید $ab^{-1} = h$ با $h \in H$. آنگاه $a = hb$، و در نتیجه:

$$Ha = Hhb = Hb$$

چون برای هر $h \in H$ داریم $Hh = H$.

تعریف ۲۳.۱ گروه خارج‌قسمتی

فرض کنید $N \lhd G$. در این صورت، مجموعهٔ تمام همدسته‌های راست N در G را با نماد G/N نمایش می‌دهیم و روی مجموعهٔ همدسته‌های N در G عمل زیر را تعریف می‌کنیم:

$$Na \cdot Nb := Nab$$

عنصر همانی همدستهٔ N برابر است با:

$$N = Ne = Nn \quad (n \in N)$$

خوش‌تعریفی عمل ضرب. فرض کنید $Na = Na'$ و $Nb = Nb'$. آنگاه عناصری $n, m \in N$ وجود دارند به‌طوری‌که $a' = na$ و $b' = mb$. پس:

$$Na'b' = N(na)(mb) = N\,n\,(ama^{-1})\,ab.$$

از آنجا که $N \lhd G$، داریم $ama^{-1} \in N$، و در نتیجه $N\,n\,(ama^{-1}) = N$. بنابراین:

$$Na'b' = Nab.$$

پس عمل $Na \cdot Nb := Nab$ مستقل از نماینده‌های انتخاب‌شده است، و لذا خوش‌تعریف است.

تعریف ۲۴.۱ همریختی

فرض کنید G و H دو گروه باشند و تابع $f: G \to H$ را در نظر بگیرید.
می‌گوییم f **همریختی** است اگر:

$$\forall\, a, b \in G \quad f(ab) = f(a)f(b)$$

در این صورت، مفاهیم زیر تعریف می‌شوند:

- **هستهٔ همریختی**:
$$ker(f) = \{a \in G \mid f(a) = e_H\}$$
- **برد همریختی**:
$$Im(f) = \{f(a) \mid a \in G\}$$
- اگر f یک‌به‌یک باشد، آن‌را **تک‌ریختی** [a] می‌نامند.
- اگر f پوشا باشد، آن‌را **بروریختی** [b] می‌نامند.
- اگر f هم‌تک‌ریختی و هم بروریختی باشد، آن‌را **ایزومورفیسم** یا **یکریختی** [c] می‌نامند. در این صورت می‌نویسیم $G \cong H$.

[a] monomorphism
[b] epimorphism
[c] isomorphism

مثال ۲۵.۱

اگر G گروهی دوری از مرتبهٔ n باشد یعنی $G = \langle a \mid a^n = e \rangle$، آنگاه $G \cong \mathbb{Z}_n$ ؛ یعنی گروه G با گروه $\mathbb{Z}_n$ ایزومورف است.

مثال ۲۶.۱

اگر G گروه دوران‌های حول مبدا صفحه در جهت مثلثاتی به اندازهٔ $\frac{2\pi k}{n}$ باشد که $k \in \mathbb{Z}$، این گروه G با $\mathbb{Z}_n$ ایزومورف است.

مثال ۲۷.۱

هر گروه دوری نامتناهی با $\mathbb{Z}$ ایزومورف است.

تعریف ۲۸.۱

اگر G گروهی متناهی باشد، $|G|$ را تعداد اعضای گروه G تعریف می‌کنیم و آن را **مرتبهٔ گروه** می‌نامند.

مثال ۲۹.۱

هر گروه از مرتبهٔ p با گروه دوری $(\mathbb{Z}_p, +)$ ایزومورف است.

قضیه ۳۰.۱ قضایای یکریختی

قضیهٔ اول یکریختی: فرض کنید $f: G \to H$ یک همریختی گروهی باشد. در این صورت داریم:

$$\frac{G}{ker(f)} \cong Im(f)$$

قضیهٔ دوم یکریختی: اگر $H \leq G$ و $G \trianglelefteq N$، آنگاه:

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

قضیهٔ سوم یکریختی: اگر $H, K \trianglelefteq G$ و $H \leq K$، آنگاه:

$$\frac{G/H}{K/H} \cong G/K$$

مثال ۳۱.۱

به ازای هر $n \in \mathbb{Z}$ داریم،

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$$

اثبات. تابع $f : \mathbb{Z} \to \mathbb{Z}_n$ را به‌صورت $f(k) = \overline{k}$ تعریف می‌کنیم که همریختی پوشاست، زیرا:

$$f(i+j) = \overline{i+j} = \overline{i} + \overline{j} = f(i) + f(j)$$

در نتیجه $ker(f) = n\mathbb{Z}$، و چون f پوشاست، طبق قضیهٔ اول یکریختی داریم:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$$

کلاس‌های هم‌ریختی در $\mathbb{Z}/n\mathbb{Z}$ عبارتند از:

$$\{n\mathbb{Z},\ n\mathbb{Z}+1,\ n\mathbb{Z}+2,\ \dots,\ n\mathbb{Z}+(n-1)\}$$

تذکر ۳۲.۱ یادآوری مفهوم گروه‌های خارج‌قسمتی

اعضا: همدسته ها

در گروه $(\mathbb{Z},+)$ همدسته های زیرگروه $n\mathbb{Z}$ به شکل زیر هستند:

$$n\mathbb{Z}+m=\{nk+m \mid k\in\mathbb{Z}\} \quad (m\in\mathbb{Z})$$

برای نمونه:

$$\begin{aligned} n\mathbb{Z}+0 &= n\mathbb{Z}=\{\dots,-3n,-2n,-n,0,n,2n,3n,\dots\} \\ n\mathbb{Z}+1 &= \{\dots,-3n+1,-2n+1,-n+1,1,n+1,2n+1,3n+1,\dots\} \\ &\vdots \\ n\mathbb{Z}+(n-1) &= \dots \\ n\mathbb{Z}+n &= \{nk+n \mid k\in\mathbb{Z}\}=\{n(k+1) \mid k\in\mathbb{Z}\}=n\mathbb{Z} \end{aligned}$$

تعریف ۳۳.۱ گروه خودریختی‌ها

گروه خودریختی‌های G برابر است با:

$$Aut(G) = \{\varphi\colon G \to G \mid \varphi \text{ همریختی یک به یک و پوشا}\}$$

تعریف ۳۴.۱ خودریختی‌های درونی

گروه خودریختی‌های داخلی G برابر است با:

$$Inn(G) = \{I_g\colon G \to G \mid g \in G\}$$

که در آن نگاشت I_g به‌صورت زیر تعریف می‌شود:

$$I_g(x) = gxg^{-1}$$

تعریف ۳۵.۱ مرکز گروه

مرکز گروه G برابر است با:

$$Z(G) = \{g \in G \mid gx = xg \quad (\forall x \in G)\}$$

تذکر ۳۶.۱

G **آبِلی** است اگر و تنها اگر $G = Z(G)$.

تعریف ۳۷.۱ حلقه

فرض کنید R مجموعه‌ای ناتهی همراه با دو عمل دوتایی $+$ و $\cdot$ باشد، به‌طوری‌که $(R,+)$ یک گروه آبلی باشد و خواص زیر برقرارند:
برای همهٔ $a,b,c \in R$:

$$a(bc) = (ab)c \tag{۱}$$
$$a(b+c) = ab + ac \tag{۲}$$
$$(b+c)a = ba + ca \tag{۳}$$

در این صورت $(R,+,\cdot)$ را یک **حلقه** می‌نامند. اگر عمل ضرب دارای عضو همانی باشد، یعنی عنصری مانند 1_R وجود داشته باشد چنان‌که:

$$\forall a \in R \quad a1_R = 1_R a = a$$

در این صورت، R را **حلقه یکدار** می‌نامند. اگر عمل $\cdot$ جابجایی باشد، حلقه را **حلقه جابجایی** می‌نامند. زیرمجموعهٔ ناتهی S از حلقهٔ $(R,+,\cdot)$ را **زیرحلقه** می‌نامند اگر S نسبت به دو عمل $+$ و $\cdot$ یک حلقه باشد.

تذکر ۳۸.۱

در این درس همواره فرض براین است که حلقه جابجایی و یکدار باشد، مگر آن‌که خلاف آن بیان شود.

مثال ۳۹.۱

$$(\mathbb{Z},+,\cdot),\quad (\mathbb{Q},+,\cdot),\quad (\mathbb{R},+,\cdot),\quad (\mathbb{C},+,\cdot),\quad (M_n(R),+,\cdot)$$

تعریف ۴۰.۱ محک فشرده

چون $(R,+) \leqslant (S,+)$ زیرمجموعهٔ ناتهی S از حلقهٔ R یک زیرحلقه است اگر و تنها اگر:

$$\forall a,b \in S \quad a-b \in S$$

$$\forall a,b \in S \quad ab \in S$$

تذکر ۴۱.۱

مثال: $(2\mathbb{Z}, +, \cdot)$ یک زیرحلقه از $(\mathbb{Z}, +, \cdot)$ است. زیرا:

$$a - b \in 2\mathbb{Z}, \quad \forall a, b \in 2\mathbb{Z} \quad ab \in 2\mathbb{Z}$$

به طور مشابه $(n\mathbb{Z}, +, \cdot)$ یک زیر حلقه از $(\mathbb{Z}, +, \cdot)$ است. اما این زیرحلقه‌ها هیچ‌گاه یکدار نیستند.

تعریف ۴۲.۱ ایده‌آل

زیرمجموعهٔ ناتهی I از حلقهٔ $(R, +, \cdot)$ را یک **ایده‌آل** راست حلقهٔ R نامند هرگاه $(I, +) \leqslant (R, +)$ و بعلاوه:

$$\forall a \in I \quad \forall r \in R \quad ar \in I$$

به طور مشابه می‌توان ایده‌آل چپ را نیز تعریف کرد. ایده آلی که هم ایده‌آل چپ و هم ایده‌آل راست باشد را **ایده‌آل دوطرفه** یا به‌اختصار **ایده‌آل** می‌نامند.

مثال ۴۳.۱

هر ایده‌آل یک زیرحلقه است اما هر زیرحلقه یک ایده‌آل نیست. به عنوان مثال

- $(2\mathbb{Z}, +, \cdot)$ زیرحلقه‌ای از $(\mathbb{Z}, +, \cdot)$ است ولی ایده‌آل آن نیست.
- $(\mathbb{Z}, +, \cdot)$ زیرحلقه‌ای از $(\mathbb{R}, +, \cdot)$ است ولی ایده‌آل آن نیست. چرا که $\sqrt{2} \cdot n \notin \mathbb{Z}$.

تذکر ۴۴.۱

- در حلقه یکدار R اگر ایده‌آل I عنصر 1_R را دربر داشته باشد، در این‌صورت $I = R$.
- در هر میدان هر ایده‌آل ناصفر دارای عنصر همانی است. لذا یک میدان دارای ایده‌آل نابدیهی نیست.

تعریف ۴۵.۱ حلقه خارج‌قسمتی

اگر I یک ایده‌آل از حلقهٔ R باشد، به ازای هر $r \in R$ تعریف می‌کنیم:

$$r + I := \{r + a \mid a \in I\}$$

مجموعهٔ تمام همدسته ها را با R/I نمایش می‌دهیم. حال عملیات عملیات جمع و ضرب را به صورت تعریف

$$(r + I) + (r' + I) := (r + r') + I$$

$$(r + I)(r' + I) := rr' + I$$

ثابت می‌شود که $(R/I, +, \cdot)$ یک حلقه است که به آن **حلقهٔ خارج‌قسمتی** R گفته می‌شود.

تذکر ۴۶.۱

آیا برای زیرحلقه‌ها می‌توان حلقهٔ خارج‌قسمتی تعریف کرد؟

تعریف ۴۷.۱ حلقهٔ خارج‌قسمتی

اگر $(R,+,\cdot)$ یک حلقه باشد و I یک ایده‌آل از R، آنگاه حلقهٔ خارج‌قسمتی R نسبت به I را به‌صورت $(R/I,+,\cdot)$ تعریف می‌کنیم.

مثال ۴۸.۱

اگر $n \in \mathbb{N}$، آنگاه $(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\cdot)$ یک حلقهٔ خارج‌قسمتی $(\mathbb{Z},+,\cdot)$ است.

تعریف ۴۹.۱ همریختی حلقه

فرض کنید $(R,+,\cdot)$ و $(S,+',\cdot')$ دو حلقه دلخواه باشند و $f\colon R \to S$ یک تابع باشد. f را **همریختی حلقه‌ای** می‌نامند اگر:

$$\forall r_1, r_2 \in R \quad f(r_1 + r_2) = f(r_1) +' f(r_2)$$

$$\forall r_1, r_2 \in R \quad f(r_1 r_2) = f(r_1) \cdot' f(r_2)$$

مشابه بحث‌های گروه، **تکریخی** ، **بروریختی** و **یکریختی** تعریف می‌شود.

تعریف ۵۰.۱ هسته و برد همریختی حلقه

اگر $f: R \to S$ همریختی حلقه باشد، آنگاه:

$$ker(f) = \{r \in R \mid f(r) = 0_S\} \quad \text{(ایده‌آل)}$$
$$Im(f) = \{f(r) \mid r \in R\}$$

قضیه ۵۱.۱ قضایای یکریختی برای حلقه‌ها

- **قضیهٔ اول یکریختی:** اگر $f: R \to S$ همریختی حلقه باشد، آنگاه:

$$\frac{R}{ker(f)} \overset{\text{حلقه‌ای}}{\cong} Im(f)$$

- **قضیهٔ دوم یکریختی:** اگر I و J دو ایده‌آل از R باشند، آنگاه:

$$\frac{I+J}{I} \cong \frac{J}{I \cap J}$$

- **قضیهٔ سوم یکریختی:**اگر $J \subseteq I$ دو ایده‌آل از حلقهٔ R باشند، آنگاه:

$$\frac{R/J}{I/J} \overset{\text{حلقه‌ای}}{\cong} \frac{R}{I}$$

تعریف ۵۲.۱ ایده‌آل اصلی

ایده‌آل I از حلقهٔ جابجایی و یکدار R را **اصلی** نامند هرگاه عنصری چون $a \in R$ موجود باشد به‌طوری‌که:

$$I = Ra = \{ra \mid r \in R\}$$

تعریف ۵۳.۱ حلقه با ایده‌آل‌های اصلی

حلقه‌ای که تمام ایده‌آل‌های آن اصلی باشند را **حلقهٔ ایده‌آل اصلی** یا PIR[a] می‌نامند.

[a] Principal Ideal Ring

تعریف ۵۴.۱ عضو مقسوم‌علیه صفر

عضو $a \in R$ را **مقسوم‌علیه صفر** نامند هرگاه عنصری چون $b \in R$ موجود باشد به‌طوری‌که $ab = 0$

تعریف ۵۵.۱ دامنه صحیح

حلقهٔ جابجایی و یکدار که مقسوم‌علیه صفر ناصفری نداشته باشد را **دامنه صحیح** یا **حوزهٔ صحیح**[a] می‌نامند.

[a] Domain

تعریف ۵۶.۱ حوزه ایده‌آل اصلی

دامنهٔ صحیحی که تمام ایده‌آل‌های آن اصلی باشند را **حوزهٔ ایده‌آل اصلی** یا PID [a] می‌نامند.

[a] Principal Ideal Domain

تعریف ۵۷.۱ ایده‌آل ماکسیمال

در حلقهٔ R ایده‌آل سرهٔ I را ماکسیمال گوییم، هرگاه چنانچه J ایده‌آلی از R باشد که $I \subseteq J \subseteq R$ آنگاه $J = I$ یا $J = R$. مجموعهٔ تمام ایده‌آل های ماکسیمال حلقهٔ R را با $max(R)$ نمایش می دهیم.

مثال ۵۸.۱

$(2\mathbb{Z},+,\cdot) \leqslant (\mathbb{Z},+,\cdot)$ ایده‌آلی ماکسیمال است.

تعریف ۵۹.۱ ایده‌آل اول

در حلقهٔ جابجایی و یکدار R، ایده‌آل P را **ایده‌آل اول** نامند هرگاه برای هر $a,b \in R$ اگر $ab \in P$ آنگاه $a \in P$ یا $b \in P$.

$$\forall a,b\ inR \quad ab \in P \implies a \in P \vee b \in P$$

مجموعهٔ تمام ایده‌آل‌های اول حلقه R را با $Spec(R)$ نمایش می‌دهیم.

تذکر ۶۰.۱

در صورتی که حلقه جابجایی نباشد از شرط زیر استفاده می‌کنیم:

$$IJ \subseteq R \implies I \subseteq R \vee J \subseteq R$$

مثال ۶۱.۱

اگر p عددی اول باشد. آنگاه ایده‌آل $(p) = p\mathbb{Z} = \{pk : k \in \mathbb{Z}\}$ یک ایده‌آل اول در حلقهٔ $\mathbb{Z}$ است. بعلاوه (p) ایده‌آلی ماکسیمال است.

اول بودن. فرض کنید $ab \in p\mathbb{Z}$. پس $p \mid ab$. چون p عدد اول است، دراین صورت $p \mid a$ یا $p \mid b$. معادل با این است که $a \in p\mathbb{Z}$ یا $b \in p\mathbb{Z}$. پس $p\mathbb{Z}$ یک ایده‌آل اول است.

ماکسیمال بودن. هر ایده‌آل در $\mathbb{Z}$ اصلی است؛ یعنی به صورت $n\mathbb{Z}$ برای عددی $0 \leq n \in \mathbb{Z}$ نوشته می‌شود. اگر $p\mathbb{Z} \subseteq I \subsetneq \mathbb{Z}$، آنگاه $I = n\mathbb{Z}$ و $p \mid n$. چون p عدد اول است، مقسوم‌علیه‌هایش فقط 1 و p هستند، و چون $I \neq \mathbb{Z}$، باید $n \neq 1$ باشد؛ در نتیجه $n = p$ و $I = p\mathbb{Z}$.

مثال ۶۲.۱

در هر **دامنه صحیح**، ایده‌آل صفر یعنی (0) یک **ایده‌آل اول** است؛ زیرا اگر $ab = 0$ آنگاه $a = 0$ یا $b = 0$.

مثال ۶۳.۱

در حلقهٔ $\mathbb{Z}_6$، ایده‌آل (0) اول هست اما ماکسیمال نیست.

$$ab \in P = (0) \implies ab = 0 \xRightarrow[\text{ایده‌آل اصلی } \mathbb{Z}]{} a = 0 \vee b = 0 \implies a \in (0) \vee b \in (0)$$

و بعلاوه

$$(0) \subsetneq (2) \subsetneq \mathbb{Z}_6$$

قضیه ۶۴.۱

در هر حلقهٔ جابجایی و یکدار R داریم:

$$max(R) \subseteq Spec(R)$$

یعنی هر ایده‌آل ماکسیمال، ایده‌آل اول نیز هست.

اثبات. فرض کنید M یک ایده‌آل ماکسیمال از R باشد و فرض کنید $a, b \notin M$ اما $ab \in M$. در این صورت، چون $a \notin M$، داریم $M + (a) = R$ و نیز $M + (b) = R$. پس موجودند $m_1, m_2 \in M$ و $r_1, r_2 \in R$ چنان‌که:

$$m_1 + r_1 a = 1_R \quad \text{و} \quad m_2 + r_2 b = 1_R$$

حالا داریم:

$$1_R = (m_1 + r_1 a)(m_2 + r_2 b) = m_1 m_2 + m_1 r_2 b + r_1 a m_2 + r_1 r_2 ab$$

تمام جملات بالا در M قرار دارند زیرا M ایده‌آل است و $ab \in M$. پس $1_R \in M$ که تناقض است، زیرا ایده‌آل شامل 1 کل حلقه می‌شود. در نتیجه، باید داشته باشیم $a \in M$ یا $b \in M$، پس M ایده‌آل اول است.

تذکر ۶۵.۱

در حالت کلی، $max(R) \subsetneq Spec(R)$.

مثال ۶۶.۱

شاید افزودن یک مثال خوب باشه.

تعریف ۶۷.۱ پوچساز

اگر I ایده‌آلی از حلقهٔ R باشد، **پوچساز** I را به‌صورت زیر تعریف می‌کنیم:

$$Ann_R(I) = \{r \in R \mid \forall a \in I \quad ra = 0\}$$

تعریف ۶۸.۱ رابطهٔ ترتیبی

فرض کنید X یک مجموعهٔ ناتهی و $\leq$ یک رابطه بر X باشد. در این صورت، $\leq$ یک رابطهٔ ترتیبی است اگر خواص زیر برقرار باشند:

بازتابی: $\forall x \in X,\ x \leq x$

پادتقارنی: $\forall x_1, x_2 \in X,\ (x_1 \leq x_2$ **و** $x_2 \leq x_1) \Rightarrow x_1 = x_2$

تعدی: $\forall x_1, x_2, x_3 \in X,\ (x_1 \leq x_2$ **و** $x_2 \leq x_3) \Rightarrow x_1 \leq x_3$

تعریف ۶۹.۱ ترتیب کلی

رابطهٔ $\leq$ روی X را **ترتیب کلی** یا **تام** گویند اگر:

$\forall x_1, x_2 \in X \quad x_1 \leq x_2$ **یا** $x_2 \leq x_1$

تعریف ۷۰.۱ زنجیر

مجموعهٔ ناتهی X همراه با رابطهٔ ترتیبی $\leq$ را درنظر بگیرید. زیرمجموعه‌ای از X که کاملاً مرتب باشد را **زنجیر** [a] می‌نامند.

[a] chain

تعریف ۷۱.۱ کران بالا

فرض کنید $Y \subseteq X$ یک زیرمجموعهٔ ناتهی و X مجهز به رابطهٔ ترتیبی $\leq$ باشد. در این صورت، عنصر $\alpha \in X$ را **کران بالای** Y می‌نامیم اگر:

$$\forall a \in Y, \quad a \leq \alpha$$

و عنصر β را یک عنصر ماکسیمال X نامند هرگاه

$$\forall a \in X; \quad \beta \leq a \implies \beta = a$$

قضیه ۷۲.۱ لِم زورن

اگر X یک مجموعهٔ ناتهی و $\leq$ یک رابطهٔ ترتیب جزئی روی X باشد به‌طوری‌که هر زنجیر در X دارای کران بالایی باشد، آنگاه X حداقل دارای یک عنصر ماکسیمال است.

تعریف ۷۳.۱ مجموعه بستهٔ ضربی

زیرمجموعهٔ ناتهی S از حلقهٔ جابجایی و یکدار R را یک **مجموعهٔ بستهٔ ضربی** نامند هرگاه:

$$1_R \in S \quad \text{و} \quad \forall a, b \in S; \quad ab \in S$$

قضیه ۷۴.۱

فرض کنید R حلقه‌ای جابجایی و یکدار است، S یک زیرمجموعهٔ بستهٔ ضربی و I یک ایده‌آل از R باشد، طوری که $I \cap S = \emptyset$ در این صورت، یک **ایده‌آل اول** P از R وجود دارد به‌طوری‌که:

$$I \subseteq P \quad \text{و} \quad P \cap S = \emptyset$$

اثبات. مجموعهٔ زیر را در نظر بگیرید:

$$\mathcal{A} = \{J \subseteq R \mid I \leqslant J \leqslant R,\ J \cap S = \emptyset\}$$

این مجموعه ناتهی است، زیرا $I \in \mathcal{A}$. $\mathcal{A}$همراه با رابطهٔ شمول یک زیرمجموعهٔ جزئاً مرتب است. حال، هر زنجیرهٔ T در $\mathcal{A}$ دارای کران بالایی است:

$$L = \bigcup_{J \in T} J$$

L یک ایده‌آل است (چرا؟)، و داریم:

$$I \subseteq L \quad \text{و} \quad L \cap S = \emptyset$$

پس $L \in \mathcal{A}$ و L کران بالای T است. به کمک لم زورن، $\mathcal{A}$ دارای عضو ماکسیمال P است. نشان می‌دهیم که این عضو ماکسیمال، یک ایده‌آل اول است. فرض کنید $a, b \in R$ و $ab \in P$ ولی $a \notin P$ و $b \notin P$. آنگاه

$$\left.\begin{array}{l} P \subsetneq P + Ra \\ P \subsetneq P + Rb \end{array}\right\} \xrightarrow[\text{ایده‌آلی ماکسیمال } P]{\qquad\qquad} P + Ra \nsubseteq \mathcal{A} \text{ و } P + Rb \nsubseteq \mathcal{A}$$

$P + (a)$ و $P + (b)$ ایده‌آل‌هایی بزرگ‌تر از P و شامل I هستند که حتماً با S اشتراک دارند (به‌خاطر ماکسیمال بودن P). پس موجودند $s_1 \in (P + (a)) \cap S$ و $s_2 \in (P + (b)) \cap S$. بنویسید:

$$s_1 = m_1 + r_1 a, \quad s_2 = m_2 + r_2 b \quad \text{به ازای } m_1, m_2 \in P,\ r_1, r_2 \in R$$

آنگاه:

$$s_1 s_2 = (m_1 + r_1 a)(m_2 + r_2 b) = m_1 m_2 + m_1 r_2 b + r_1 a m_2 + r_1 r_2 ab \in P$$

و چون S بستهٔ ضربی است، $s_1 s_2 \in S$. پس $P \cap S \neq \emptyset$ که تناقض است. بنابراین، P ایده‌آل اول است.

نتیجه ۷۵.۱

فرض کنید R حلقه‌ای جابجایی و یکدار باشد و I ایده‌آلی سره از R باشد. در این صورت، عضوی چون $M \in max(R)$ موجود است به‌طوری‌که:

$$I \subseteq M$$

اثبات. مجموعهٔ $S := \{1_R\}$ را در نظر بگیرید. S بستهٔ ضربی است و $I \cap S = \emptyset$. پس یک ایده‌آل اول چون P وجود دارد که $I \subseteq P$ و $P \cap S = \emptyset$.

اما چون $P \in \mathcal{A}$، پس در آن عضو ماکسیمال هم هست. در نتیجه اگر $P \subseteq J \subsetneq R$ و J ایده‌آل باشد، آنگاه $J \in \mathcal{A}$ لذا $J = P$ که یعنی P ماکسیمال است.

نتیجه ۷۶.۱

اگر R یک حلقهٔ جابجایی و یک‌دار باشد، آن‌گاه:

$$Spec(R) \neq \emptyset.$$

نتیجه ۷۷.۱

اگر R یک حلقهٔ جابجایی و یک‌دار باشد، آن‌گاه:

$$max(R) \neq \emptyset.$$

02 Zorn's Lemma

قضیه ۱.۲

فرض کنید R حلقه‌ای جابجایی و یکدار باشد و I ایده‌آلی سره از R باشد. در این صورت **ایده‌آل اول** P وجود دارد که شامل I است و به‌علاوه هیچ ایده‌آل اولی بین I و P وجود ندارد.

اثبات. فرض کنید

$$\mathcal{A} = \{Q \mid I \subseteq Q,\ Q \in Spec(R)\}\,.$$

توجه کنید که $\mathcal{A} \neq \emptyset$.

رابطه‌ی $\leq$ را عکس شمول در نظر می‌گیریم یعنی $B \leq C \Leftrightarrow C \subseteq B$، که رابطه‌ای جزئاً مرتب بر $\mathcal{A}$ است.

فرض کنید $\mathcal{T}$ یک زنجیر در $\mathcal{A}$ باشد. ثابت می‌کنیم که $\mathcal{T}$ در $\mathcal{A}$ کران بالا دارد. بگذارید

$$\mathcal{L} = \bigcap_{B\in\mathcal{T}} B.$$

در این صورت $\mathcal{L}$ کران بالای $\mathcal{T}$ است. نشان می‌دهیم که $\mathcal{A} \in \mathcal{L}$ است.
اگر $ab \in \mathcal{L}$ و $a \notin \mathcal{L}$، آنگاه:

$$\exists B \in \mathcal{T}; \quad a \notin B.$$

اما در این صورت

$$\forall C \in \mathcal{T}; \quad b \in C.$$

در نتیجه $b \in \mathcal{L}$ و لذا $\mathcal{L} \in \mathcal{A}$. پس شرایط لم زورن برقرار است، لذا $\mathcal{A}$ دارای عنصری ماکسیمال مانند P است. مفهوم ماکسیمال بودن در این شرایط... $\square$

تعریف ۲.۲

ایده‌آل P در قضیه‌ی قبل را یک **ایده‌آل اول مینیمال** I نامیده و با $Min(I)$ نمایش می‌دهند.

تمرین ۳.۲

فرض کنید R حلقه‌ای جابجایی و یکدار باشد و I ایده‌آلی از R باشد بعلاوه فرض کنید $I \subseteq P$ موجود است که $I \subseteq P$. ثابت کنید ایده‌آل اول مینیمالی از I مانند Q وجود دارد که $I \subseteq Q \subseteq P$.

تذکر ۴.۲

- اگر $\varphi : R \to S$ یک همریختی حلقه‌ای باشد و I ایده‌آلی از S، آنگاه $\varphi^{-1}(I)$ ایده‌آلی از R است.
- اگر J ایده‌آلی از R باشد،لزوما $\varphi(J)$ ایده‌آل S نیست.
- $\varphi^{-1}(I) = I^c$ را **انقباض**[a] I و $J^e = \varphi(J)S$ (ایده‌آل تولید شده توسط $(\varphi(J)$ را **توسیع**[b] J گویند.

[a] contraction
[b] extension

قضیه ۵.۲

اگر $P \in Spec(S)$ آنگاه $P^c \in Spec(R)$.

اثبات. اگر $ab \in P^c$ ولی $a \notin P^c$، آنگاه $b \in P^c$. □

قضیه ۶.۲ Prime Avoidance Theorem

فرض کنید $P_1, \dots, P_n$ $(n \geq 2)$ ایده‌آل‌هایی از حلقه جابجایی و یک‌دار R باشند، به‌طوری‌که حداقل $n-2$ تا از آن‌ها اول باشند. فرض کنید $I \subseteq R$ زیرمجموعه‌ای باشد که تحت جمع و ضرب بسته است و $I \subseteq \bigcup_{i=1}^{n} P_i$. در این صورت، $\exists 1 \leq t \leq n$ چنان‌که $I \subseteq P_t$.

اثبات.

با استقرا بر n حکم ثابت می‌شود.

پایه: اگر $n=2$، فرض کنیم $I \subseteq P_1 \cup P_2$ ولی $I \nsubseteq P_1$ و $I \nsubseteq P_2$، آنگاه $\exists x \in I \setminus P_1$ و $\exists y \in I \setminus P_2$. چون $x+y \in I$ ولی $x+y \notin P_1 \cup P_2$، تناقض.

گام استقرا: فرض کنید حکم برای $n=k$ برقرار است. حال $n=k+1$ را در نظر بگیرید.

فرض کنید $I \subseteq \bigcup_{i=1}^{k+1} P_i$ و حداقل $k-1$ تا از P_i ها اولند. با برهان خلف فرض کنید حکم صحیح نباشد، پس

$$\forall 1 \leq j \leq k+1; \quad I \nsubseteq \bigcup_{\substack{i=1 \\ i \neq j}}^{k+1} P_i$$

برای هر j، عضوی $a_j \in I$ موجود است که

$$a_j \notin \bigcup_{\substack{i=1 \\ i \neq j}}^{k+1} P_i$$

از آنجا که

$$I \subseteq \bigcup_{i=1}^{k+1} P_i$$

پس به ازای هر $1 \leq j \leq k+1$ بایستی $a_j \in P_j$. ضمناً فرض کنید که P_{k+1} اول باشد. حال عنصر

$$b = a_1 a_2 \cdots a_k + a_{k+1}$$

را در نظر بگیرید. نشان می‌دهیم

$$b \notin \bigcup_{i=1}^{k+1} P_i$$

- از آنجا که $a_{k+1} \in P_{k+1}$، اگر $b \in P_{k+1}$ در این صورت

$$a_1 a_2 \cdots a_k = b - a_{k+1} \in P_{k+1}$$

و از آنجا که P_{k+1} اول است، حداقل یک $1 \leq j \leq k$ وجود دارد که $a_j \in P_{k+1}$، تناقض.

- به همین ترتیب، به ازای $1 \leq j \leq k$ از آنجا که $a_j \in P_j$ و P_j یک ایده‌آل است $a_1 a_2 \cdots a_k \in P_j$ ، اگر $b \in P_{k+1}$ در این صورت $a_{k+1} = b - a_1 a_2 \cdots a_k \in P_{k+1}$، تناقض.

پس داریم $b \in I$ ولی $b \notin \bigcup_{i=1}^{k+1} P_i$، که این با فرض اولیه

$$I \subseteq \bigcup_{i=1}^{k+1} P_i$$

در تناقض است.

در نتیجه: باید $I \subseteq P_t$ برای یک $1 \leq t \leq k+1$ باشد. $\square$

تعریف ۷.۲ رادیکال پوچ R

اگه R یک حلقه باشد، در این صورت رادیکال پوچ حلقه R یا نیل‌رادیکال R به صورت زیر تعریف می‌شود:

$$nil(R) = \bigcap_{P \in Spec(R)} P$$

تعریف ۸.۲ جیکبسون رادیکال R

اگه R یک حلقه باشد، در این صورت جیکبسون رادیکال R به صورت زیر تعریف می‌شود:

$$\mathcal{J}(R) = \bigcap_{M \in Max(R)} M$$

تذکر ۹.۲

اگر R حلقه‌ای جابجایی و یکدار باشد، از آنجا که $Max(R) \subseteq Spec(R)$ داریم:

$$nil(R) \subseteq \mathcal{J}(R)$$

قضیه ۱۰.۲

اگر R حلقه‌ای جابجایی و یکدار باشد، در این صورت

$$nil(R) = \{x \in R \mid \exists n \in \mathbb{N};\ x^n = 0\} = R \text{ مجموعهٔ عناصر پوچتوان}$$

اثبات. فرض کنید $x^n = 0$، در این صورت $x^n = 0 \in P$ برای هر $P \in Spec(R)$. از آنجا که P اول است، آنگاه $x \in P$ برای هر $P \in Spec(R)$، پس:

$$x \in \bigcap_{P \in Spec(R)} P = nil(R)$$

بنابراین:

$$nil(R) \subseteq \text{مجموعهٔ عناصر پوچتوان } R$$

حال اگر $x \in nil(R)$، آنگاه $x \in P$ برای هر $P \in Spec(R)$. فرض کنیم $\forall n,\ x^n \neq 0$. بگذارید:

$$S = \{x^n \mid n \in \mathbb{N} \cup \{0\}\}$$

S بستهٔ ضربی است و $0 \notin S$. پس $\{0\} \cap S = \emptyset$. بنابراین ایده‌آل اول Q موجود است که $\{0\} \subseteq Q$ و $S \cap Q = \emptyset$ پس

$$x \notin Q \implies x \notin nil(R)$$

که تناقض است؛ پس وجود دارد n که $x^n = 0$.

$\square$

تمرین ۱۱.۲

فرض کنید R حلقه‌ای جابجایی و یکدار است، در این صورت:

$$x \in \mathcal{J}(R) \iff \forall y \in R, \text{ در } R \text{ یکه است } 1 - xy$$

تمرین ۱۲.۲

فرض کنید R حلقه‌ای جابجایی و یکدار است، در این صورت

$$\frac{R}{nil(R)}$$

هیچ عنصر پوچ‌توان ناصفری ندارد.

03 Introduction

تمرین ۱.۳

فرض کنید R حلقه‌ای جابجایی و یکدار است. ثابت کنید موارد زیر معادلند:

۱. R فقط یک ایده‌آل اول دارد.

۲. هر عنصر R یا یکه است یا عنصری پوچتوان است.

۳. $\frac{R}{nil(R)}$ یک میدان است.

تعریف ۲.۳

حلقه‌ای را که دقیقا یک ایده‌آل ماکسیمال داشته باشد را یک **حلقهٔ موضعی** نامند.

مثال ۳.۳

میدان $\mathbb{F}$ یک حلقهٔ موضعی است، چرا که در هر میدان ایده‌آل نابدیهی وجود ندارد.

مثال ۴.۳

اگر p عددی اول باشد، در این صورت حلقه های زیر نیز موضعی هستند

$$\frac{\mathbb{Z}}{p\mathbb{Z}}, \quad \frac{\mathbb{Z}}{p^2\mathbb{Z}}, \quad \frac{\mathbb{Z}}{p^3\mathbb{Z}}, \quad \ldots, \quad \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

مثال ۵.۳

حلقهٔ $\mathbb{C}[[x]]$، یعنی مجموعهٔ تمام عناصر $\Sigma_{i=0}^{+\infty} c_i x^i$ که در آن $c_i \in \mathbb{C}$ است، با ضرب معمولی موضعی است.

مثال ۶.۳

حلقه زیر:

$$R = \left\{ \frac{m}{n} \in \mathbb{Q} \mid n \text{ فرد است} \right\}$$

حلقه‌ای موضعی است چرا که تنها ایده‌آل ماکسیمال آن ایده‌آل زیر است:

$$\mathfrak{m} = \left\{ \frac{m}{n} \in R \mid m \text{ زوج است} \right\}$$

قضیه ۷.۳

R حلقه ای موضعی است اگر و تنها اگر برای هر $r \in R$ عنصر r یا $1-r$ عنصری یکه باشد.

اثبات. اگر R حلقه‌ای موضعی باشد، فقط یک ایده‌آل اول مانند m دارد، از طرفی هر عنصر $a \notin m$ عنصری یکه است زیرا $R = m + (a) \supsetneq m$. لذا اگر $r \in R$ از آنجا که $r \notin m$ یا $1 - r \notin m$، پس r یا $1 - r$ یکه است.
حال، اگر M و M' دو ایده‌آل ماکسیمال R باشند؛ فرض کنید $a \in M' \setminus M$ پس

$$R = M + (a) \implies \exists m \in M, \exists r \in R; \quad 1 = m + ra \implies m = 1 - ra$$

از طرفی

$$a \in M' \implies ra \in M' \implies 1 - ra \text{ یکه است}$$

پس $m \in M$ عنصری یکه بوده، که در تناقض با ماکسیمال بودن M است. $\square$

نتیجه ۸.۳

حلقه ای $\mathbb{R}[x]$ موضعی نیست، چرا که x و $1-x$ هر دو غیر یکه هستند.

نتیجه ۹.۳

۱. فرض کنید R یک حلقه و $\mathfrak{m} \neq (1)$ ایده‌آلی از R باشد، به طوری که هر $x \in R \setminus \mathfrak{m}$ یکه‌ای از R باشد. در این صورت R موضعی است و $\mathfrak{m}$ ایده‌آل ماکسیمال آن است.

۲. R یک حلقه و $\mathfrak{m}$ ایده‌آل ماکسیمال R باشد، به طوری که به ازای هر عنصر $m \in \mathfrak{m}$، $1+m$ یکه‌ای در R باشد. در این صورت R موضعی است.

اثبات قسمت ۲. اگر $a \in R \setminus \mathfrak{m}$ در این صورت $R = \mathfrak{m} + (a)$ پس

$$\exists t \in \mathfrak{m}, \exists r \in R; \quad t + ra = 1 \implies ra = 1 - t = 1 + (-t) \implies ra \text{ یکه} \implies a \text{ یکه}$$

بنابر قسمت ۱ حلقهٔ R موضعی است. $\square$

تعریف ۱۰.۳

$$\mathcal{N}(R) = \bigcup_{M \in Max(R)} M$$

تذکر ۱۱.۳

اجتماع ۳ ایده‌آل ممکن است یک ایده‌آل نباشد. مثل $\mathbb{Z}_2 \times \mathbb{Z}_2$.

قضیه ۱۲.۳

موارد زیر هم‌ارزند:

۱. $\mathcal{N}(R) = \mathcal{J}(R)$

۲. $\mathcal{N}(R)$ یک ایده‌آل از R است.

۳. R موضعی است.

اثبات.

- (۱) $\Leftarrow$ (۲): واضح ✓
- (۳) $\Leftarrow$ (۱): واضح ✓
- (۲) $\Leftarrow$ (۳): اگر $M \subsetneq \mathcal{N}(R)$ و M ماکسیمال باشد، آنگاه اگر R موضعی نباشد، $R = \mathcal{N}(R) = \mathcal{J}(R)$. از طرفی $R \subseteq M \subseteq \mathcal{J}(R) = R$، بنابر این $R = M$، که در تناقض با ماکسیمال بودن M است.

□

تعریف ۱۳.۳

اگر M یک Rـمدول باشد و $X \subseteq M$ آنگاه کوچکترین Rـزیرمدول M که شامل X باشد را زیرمدول تولیدشده توسط X می‌نامند و آن را با $\langle X\rangle$ نشان می‌دهند. اگر $X = \{a\}$، می‌نویسیم $\langle a\rangle$.
اگر $X = \emptyset$ به‌وضوح $\langle X\rangle = \{0\}$. اگر $X = a$ آنگاه $\langle a\rangle$ یک زیرمدول دوری M نامیده می‌شود.
اگر X متناهی باشد $\langle X\rangle$ با تولید متناهی نامیده می‌شود.

لم ۱۴.۳

با فرضیات فوق داریم:

$$\langle X\rangle = \bigcap_{N\leqslant M, X\subseteq N} N$$

مثال ۱۵.۳

در $\mathbb{Z}$ به‌عنوان $\mathbb{Z}$ـ مدول:

$$\langle n \rangle = n\mathbb{Z}$$

مثال ۱۶.۳

در $\mathbb{Z}_{30}$ به‌عنوان $\mathbb{Z}$ـ مدول:

$$\langle \overline{5} \rangle = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\}$$

$$\langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24}, \overline{28}\}$$

تعریف ۱۷.۳

اگر R حلقه جابجایی و یکدار و M یک Rـمدول باشد، برای $a \in M$ تعریف می‌کنیم:

$$Ra = \{ra \mid r \in R\}$$

که یک زیرمدول از M خواهد بود.

تذکر ۱۸.۳

آیا $Ra = \langle a \rangle$ همواره برقرار است؟

$$Ra = \{ra \mid r \in R\} \qquad , \langle a \rangle = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$$

ولی اگر حلقه یکدار باشد، یکی هستند. به عنوان مثال حلقهٔ غیر یکدار $R = (5\mathbb{Z}, +, \cdot)$ را در نظر بگیرید. به وضوح $\mathbb{Z}$ یک Rـ مدول است. حالا اگر $a = 3$

$$Ra = \{ra \mid r \in R\} = 15\mathbb{Z}$$

در حالی که $\langle 3 \rangle = 3\mathbb{Z}$. البته در ادامه همواره حلقه های را جابجایی و یکدار فرض می‌کنیم.

تذکر ۱۹.۳

با تعریف

$$\varphi : R \to Ra, \quad r \mapsto ra$$

به یک Rـ برویختی می‌رسیم.

قضیه ۲۰.۳

فرض کنید R حلقه‌ای یکدار باشد. در این صورت، Rـمدول یکانی M دوری است اگر و تنها اگر $M \cong \frac{R}{I}$ که در آن I یک ایده‌آل چپ R است. [در واقع $I = Ann_R(a) = \{r \in R \mid ra = 0\}$]

$$M = \langle a \rangle \Rightarrow \frac{R}{Ann_R(a)} \overset{\text{مدولی}}{\cong} M = Ra$$

اثبات. چون R یکدار است و M یکانی است، پس

$$\exists a \in R, \quad M = Ra$$

در این صورت

$$\varphi : R \longrightarrow M = Ra, \quad r \longmapsto ra$$

φ یک Rـ بروریختی است. بنابراین:

$$\frac{R}{ker\varphi} \overset{\text{مدولی}}{\cong} Im\varphi = M$$

و واضح است که

$$ker\varphi = Ann_R(a)$$

برعکس. اگر $M \cong \frac{R}{I}$ که I یک ایده‌آل چپ از R باشد، فرض کنید:

$$\varphi : \frac{R}{I} \longrightarrow M, \quad \varphi(r+I) = \varphi(r)$$

Rـ یکریختی موردنظر باشد. در این صورت با فرض $a = \varphi(1+I)$ داریم

$$\varphi(r+I) = \varphi(r(1+I)) = r\varphi(1+I) = ra$$

و لذا M توسط $\{a\}$ تولید می‌شود.

تعریف ۲۱.۳

اگر M یک Rـ مدول و $\{M_i\}_{i\in I}$ زیرمدول‌های آن باشند، مجموع زیرمدول‌ها را به‌صورت زیر تعریف می‌کنیم:

$$\sum_{i\in I} M_i := \left\{a_1 + a_2 + \cdots + a_n \mid n \in \mathbb{N},\ a_j \in M_{i_j}\right\}$$

لم ۲۲.۳

واضح است که

$$\sum_{i\in I} M_i = \left\langle \bigcup_{i\in I} M_i \right\rangle$$

تعریف ۲۳.۳

فرض کنید $\{M_i\}_{i\in I}$ خانواده‌ای از Rـمدول‌ها باشند. در این صورت دنباله‌هایی به شکل $\{m_i\}_{i\in I}$ را در نظر می‌گیریم که در آن $m_i \in M_i$. سپس عملیات‌های زیر را تعریف می‌کنیم:

$$\{m_i\}_{i\in I} + \{m'_i\}_{i\in I} := \{m_i + m'_i\}_{i\in I} \quad ; \quad r \cdot \{m_i\}_{i\in I} = \{rm_i\}_{i\in I}$$

با این جمع و ضرب تعریف‌شده، یک Rـمدول بدست می‌آید که آن را حاصل‌ضرب مستقیم M_iها می‌خوانند و با نماد

$$\prod_{i\in I} M_i$$

نمایش می‌دهیم.

حال اگر فقط دنباله‌هایی به شکل $\{M_i\}_{i\in I}$ را در نظر بگیریم که فقط تعداد متناهی از عناصر آن‌ها ناصفرند، به زیرمجموعه‌ای از قبلی می‌رسیم که خود یک Rــ مدول است و آن را حاصل‌جمع مستقیم M_i ها گویند و با علامت $\bigoplus_{i\in I} M_i$ نمایش داده می‌شود.

واضح است که $\bigoplus_{i\in I} M_i$ زیرمدولی از $\prod_{i\in I} M_i$ است. اگر I متناهی باشد:

$$\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i.$$

تذکر ۲۴.۳

حال اگر فرض کنیم $\{M_i\}_{i\in I}$ خانواده‌ای از زیرمدول‌های یک Rـ مدول M باشند، در این صورت با تعریف

$$\varphi : \bigoplus_{i\in I} M_i \longrightarrow \sum_{i\in I} M_i \ , \ \{m_i\}_{i\in I} \longmapsto \sum_{i\in I} m_i$$

یک Rـ همریختی پوشا می‌رسیم و لذا:

$$\sum_{i\in I} M_i \ \cong_{R-\text{همریختی}} \ \frac{\bigoplus_{i\in I} M_i}{ker\varphi}.$$

اما در این صورت $ker\varphi = \{0\}$ به چه معنا است؟

$$\begin{aligned} ker\varphi = \{0\} \quad &\Longleftrightarrow \text{نمایش منحصر بفرد} \\ &\Longleftrightarrow \left(m_{i_1} + \cdots + m_{i_k} = 0 \ \Rightarrow \ \forall j : m_i = 0\right) \\ &\Longleftrightarrow \quad M_i \ \cap \sum_{\substack{j\in I \\ j\neq i}} m_j \ = \ \{0\}. \end{aligned}$$

قضیه ۲۵.۳ Internal direct sum

فرض کنید M یک Rـ مدول است و $\{M_i\}_{i\in I}$ خانواده‌ای از زیرمدول‌های M باشند. در این صورت M را **مجموع مستقیم** زیرمدول‌های M_i می‌نامند هرگاه:

$$M = \sum_{i\in I} M_i$$

و هر عنصر M را بتوان به‌صورت منحصر بفردی به شکل مجموع عناصری از M_i نوشت. در این صورت می‌نویسیم

$$M = \bigoplus_{i\in I} M_i.$$

نتیجه ۲۶.۳

اگر $\{M_i\}_{i\in I}$ خانواده‌ای از Rـزیرمدول‌های M باشند، گزاره‌های زیر معادلند:

(۱)

$$M = \bigoplus_{i\in I} M_i$$

(۲)

$$M_i \ \cap \ \sum_{\substack{j\in I\\ j\neq i}} M_j \ = \ \{0\} \quad (\forall i \in I)$$

اثبات. اگر

$$a \in M_i \ \cap \ \sum_{\substack{j\in I\\ j\neq i}} M_j$$

پس

$$a = m_i = m_{t_1} + m_{t_2} + \cdots + m_{t_k}$$

در این صورت:

$$m_i - m_{t_1} - m_{t_2} - \cdots - m_{t_k} = 0 + 0 + \cdots + 0$$

و با توجه به نمایش یکتا

$$a = m_i = 0$$

برعکس، اگر نمایش یک عنصر به دو صورت توشته شود:

$$m_{t_1} + m_{t_2} + \cdots + m_{t_k} \ = \ m'_{s_1} + m'_{s_2} + \cdots + m'_{s_r}$$

با یکی گرفتن این اندیس‌ها نتیجه می‌گیریم که

$$m_{t_1} - m'_{t_1} = (m'_{t_2} - m_{t_2}) + \cdots + (m'_{t_k} - m_{t_k})$$

که

$$m_{t_1} - m'_{t_1} \in M_{t_1}, \quad (m'_{t_2} - m_{t_2}) + \cdots + (m'_{t_k} - m_{t_k}) \in \sum_{\substack{j \in I \\ j \neq t_1}} M_j$$

لذا صفر می‌شود و پس $m_{t_1} = m'_{t_1}$ و همین‌طور برای بقیهٔ اعضا.

تذکر ۲۷.۳

فرض کنید R حلقه‌ای جابجایی و یک‌دار است. اگر M یک Rـمدول و X یک مجموعهٔ مولد M باشد آنگاه خواهیم داشت:

$$M = \sum_{x \in X} Rx.$$

تعریف ۲۸.۳

زیرمدول N از Rـمدول M را **ماکسیمال** گوییم هرگاه $N \neq M$ و اگر

$$N \subseteq K \subseteq M$$

که K یک Rـزیرمدول M است، آنگاه

$$K = N \quad \text{یا} \quad K = M.$$

مثال ۲۹.۳

$\mathbb{Z}$ به عنوان $\mathbb{Z}$ـ مدول و

$$N = p\mathbb{Z}$$

که p عددی اول است.

05 Maximal submodule

قضیه ۱.۴

فرض کنید M یک Rـمدول ناصفر و مولد متناهی باشد. در این صورت هر زیرمدول سرهٔ M مشمول در یک زیرمدول ماکسیمال M خواهد بود. لذا هر Rـمدول با تولید متناهی حداقل یک زیرمدول ماکسیمال دارد.

اثبات. فرض کنید K زیرمدولی سره از M باشد. فرض کنید:

$$\mathcal{A} = \{N \mid K \subseteq N \subsetneq M\}$$

و آن را با رابطهٔ شمول در نظر بگیرید. واضح است که $K \in \mathcal{A}$، پس $\mathcal{A} \neq \emptyset$.
چنانچه $\mathcal{T} \neq \emptyset$ یک زنجیر از اعضای $\mathcal{A}$ باشد، بوضوح

$$\mathcal{L} = \bigcup_{N \in \mathcal{T}} N$$

یک کران بالای $\mathcal{T}$ در $\mathcal{A}$ است (چرا؟).

اگر $M = \mathcal{L}$ آنگاه چون M با تولید متناهی است پس مثلاً

$$M = \langle \alpha_1, \alpha_2, \dots, \alpha_r \rangle$$

و لذا $N_1, \dots, N_r$ از اعضای $\mathcal{T}$ یافت می‌شود که $\alpha_i \in N_i$ در نتیجه $\exists j$ که

$$\forall i; \quad \alpha_i \in N_j$$

(چرا؟).

پس $M = N_j$، که تناقض است. بنابراین A دارای عنصر ماکسیمال است. یعنی زیرمدول ماکسیمال برای M وجود دارد.

نتیجه ۲.۴

قبلاً دیده بودیم که در حلقه جابجایی و یک‌دار هر ایده‌آل مشمول در یک ایده‌آل ماکسیمال است. چون $R = (1)$ پس با تولید متناهی است و لذا از حکم فوق نتیجه به‌دست می آید.

تذکر ۳.۴

قرارداد. از این پس، همواره Rـ مدول‌ها را Rـ مدول چپ و یک‌دار درنظر می‌گیریم.

تعریف ۴.۴

Rـ مدول $(0) \neq M$ را **ساده** یا تحویل‌ناپذیر نامند هرگاه تنها زیرمدول‌های آن (0) و M باشند.

مثال ۵.۴

میدان $\mathbb{F}$ به عنوان $\mathbb{F}$ـ مدول.

تذکر ۶.۴

درمورد مدول‌های (با طول متناهی؟)، مدولهای ساده بلوک‌های سازندهٔ آنهاهستند. چیزی شبیه به گروه‌های ساده در نظریه گروه‌ها.

تذکر ۷.۴

واضح است اگر M یک Rـ مدول ساده باشد و $0 \neq a \in M$ آنگاه

$$M = Ra.$$

مثال ۸.۴

- $\mathbb{Z}_p$ به عنوان $\mathbb{Z}_p$ـ مدول ساده است.
- $\mathbb{Z}_p$ به عنوان $\mathbb{Z}$ـ مدول.

مثال ۹.۴

در حلقهٔ جابجایی و یک‌دار R، ایده‌آل مینیمال I به عنوان یک Rـ مدول ساده است. چون هر Rـ زیر مدول زیر مدول آن در واقع یک ایده‌آل است.

مثال ۱۰.۴

در حلقهٔ R اگر I یک ایده‌آل ماکسیمال باشد، $\frac{R}{I}$ به‌عنوان Rـ مدول یک Rـ مدول ساده است.

تذکر ۱۱.۴

هر Rـمدول لزوماً شامل یک Rـزیر مدول ساده نیست، مانند $\mathbb{Z}$ به عنوان $\mathbb{Z}$ـمدول.

قضیه ۱۲.۴

فرض کنید M یک Rـمدول ساده (تحویل‌ناپذیر) باشد. در این صورت ایده‌آل چپ ماکسیمال I از R موجود است که:

$$M \cong \frac{R}{I} \quad (\text{مدولی}\text{ـ}R)$$

اثبات. اگر $0 \neq a \in M$، آنگاه $M \leqslant Ra \in a$ پس $M = Ra$ چون M ساده است. اما چون $M = Ra$ پس M دوری است. و لذا $M \cong \frac{R}{I}$ که $I = Ann_R(a)$. اما M، زیرمدول غیربدیهی ندارد، پس $\frac{R}{I}$ هم به‌عنوان Rـمدول ساده است و لذا ایدآلی مانند J وجود ندارد که $I \lneqq J \lneqq R$ یعنی I ایدآلی ماکسیمال R است.

تذکر ۱۳.۴

اگر N زیرمدول ماکسیمال M باشد آنگاه $\frac{M}{N}$ یک Rـمدول ساده است. چرا که بنابر قضیهٔ تناظر، تنها زیرمدول‌های $\frac{M}{N}$ به شکل $\frac{K}{N}$ هستند که $N \subseteq K \subseteq M$.

قضیه ۱۴.۴

فرض کنید $M = \sum_{i\in I} M_i$ که در آن M_iها Rـمدول‌های ساده M هستند. اگر K زیرمدولی از M باشد در این صورت زیرمجموعهٔ $J \subseteq I$ وجود دارد به طوری که $\sum_{j\in J} M_j$ یک مجموع مستقیم است و بعلاوه:

$$M = K \oplus \sum_{j\in J} M_j.$$

اثبات. فرض کنید

$$\mathcal{A} = \left\{ I' \subseteq I \;\middle|\; \begin{array}{c} \sum_{i\in I'} M_i \text{ مجموعهٔ مستقیم} \\ \sum_{i\in I'} M_i \cap K = \{0\} \end{array} \right\}.$$

توجه که اگر $I' = \emptyset$ آنگاه $\sum_{i\in I'} M_i = 0$. پس به‌وضوح $\mathcal{A} \neq \emptyset$ زیرا $\emptyset \in \mathcal{A}$. رابطهٔ ترتیبی را شمول درنظر می‌گیریم که رابطه‌ای جزئاً مرتب می‌شود. حالا زنجیر ناتهی $\mathcal{T}$ را در $\mathcal{A}$ درنظر بگیرید. پس $\mathcal{T}$ کاملاً مرتب است. قرار می‌دهیم

$$S = \bigcup_{I' \in \mathcal{T}} I'$$

به وضوح $\forall I' \in \mathcal{T}$، $I' \subseteq S$. پس کران بالایی برای $\mathcal{T}$ است. ثابت می‌کنیم که S در $\mathcal{A}$ قرار دارد.

شرط اول.
اگر

$$\sum_{i\in S} M_i$$

مجموعهٔ مستقیم نباشد، پس

$$m_{i_1}, \dots, m_{i_n}$$

با

$$i_1 \in I_1 \cdots i_n \in I_n$$

وجود دار که

$$m_{i_1} + \cdots + m_{i_n} = 0$$

و

$$\{i_1, \cdots, i_n\} \subseteq S$$

اما چون در زنجیر هستیم αای هست که

$$\{i_1, \cdots, i_n\} \subseteq I_\alpha$$

و I_α در $\mathcal{A}$ است. پس از $m_{i_1} + \cdots + m_{i_n} = 0$ نتیجه می‌شود تمام m_{i_j} ها صفرند.

شرط دوم.

$$K \cap \sum_{i\in S} M_i = 0.$$

چنانچه

$$x \in \left(\sum_{i\in S} M_i\right) \cap K$$

دراین‌صورت

$$\exists m_{i_j}; \quad x = m_{i_1} + \cdots + m_{i_n}.$$

و دقیقا شبیه بحث بالا به تناقض می‌رسیم. پس بنابر لم زورن $\mathcal{A}$ دارای عنصری ماکسیمال مانند J است.

ادعا ۱۵.۴

I. $\sum_{i\in J} M_i$ مجموع مستقیم است.

II. $M = K \oplus \sum_{i\in J} M_i$.

به وضوح چون $K \cap \sum_{i\in J} M_i = 0$ پس مجموع این دو، مجموع مستقیم است.

نهایتاً ثابت می‌کنیم به ازای هر $\beta \in I$،

$$M_\beta \subseteq N = K \oplus \sum_{i \in J} M_i.$$

برای هر $\beta \in I$ دقت می‌کنیم که چون M_β ساده است و $M_\beta \cap N$ یک Rـزیرمدول M_β است، پس $M_\beta \cap N = (0)$ یا $M_\beta \cap N = M_\beta$. چنانچه $M_\beta \cap N = M_\beta$ یعنی $M_\beta \subseteq N$. اما خواهیم دید که $M_\beta \cap N = (0)$ امکان‌پذیر نیست.

چنانچه β ای باشد که $M_\beta \cap N = (0)$ نشان می‌دهیم که $J \cup \beta$ نیز در $\mathcal{A}$ قرار داد که با ماکسیمال بودن J در تناقض است.

دقت کنیم که

$$M_\beta \cap N = (0)$$

نتیجه می‌دهد که

$$M_\beta \cap K = (0)$$

و بعلاوه

$$M_\beta \cap \sum_{i \in J} M_i = 0$$

از طرف دیگر چنانچه

$$\left(\sum_{i \in J \cup \{\beta\}} M_i \right) \cap K \neq 0.$$

فرض کنید x در اشتراک باشد، در این‌صورت $x \in K$ و ضمناً

$$x \in \sum_{i \in J \cup \{\beta\}} M_i = \left(\sum_{i \in J} M_i \right) + M_\beta$$

پس $x = y + m_\beta$ که در آن $y \in \sum_{i\in J} M_i$ و $m_\beta \in M_\beta$ اما در این صورت

$$m_\beta = x - y \in K \oplus \sum_{i\in J} M_i = N$$

پس

$$m_\beta \in N \cap M_\beta = (0)$$

و لذا

$$m_\beta = 0$$

پس

$$x = y \in \Sigma_{i\in J} M_i$$

و

$$x \in K$$

یعنی

$$x \in \sum_{i\in J} M_i \cap K = (0)$$

یعنی $x = 0$، پس حکم ثابت شد.

نتیجه ۱۶.۴

اگر $M = \sum_{i\in I} M_i$ مجموع خانواده‌ای از زیرمدول‌های سادهٔ M باشد آنگاه زیرمجموعهٔ $J \subseteq I$ وجود دارد که:

$$M = \bigoplus_{i\in I} M_i.$$

اثبات. در قضیهٔ قبل فرض کنید $k = (0)$.

تعریف ۱۷.۴

فرض کنید M یک Rـمدول باشد. در این صورت زیرمدول M_1 از M را یک جمعوند مستقیم M نامیم، هرگاه زیرمدول M_2 از M موجود باشد که $M = M_1 \oplus M_2$ (اصطلاحاً گوییم M_1 در M مکمل دارد و M_2 را یک مکمل M_1 در M می‌نامیم).

تعریف ۱۸.۴

مدول M را *مکمل‌پذیر* نامیم هرگاه هر زیرمدول آن دارای مکمل باشد.

مثال ۱۹.۴

فضاهای برداری مکمل‌پذیرند.

مثال ۲۰.۴

K_4 به‌عنوان $\mathbb{Z}$ـ مدول مکمل‌پذیر است.

مثال ۲۱.۴

در $\mathbb{Q}$ به‌عنوان $\mathbb{Z}$ـ مدول، $\mathbb{Z}$ مکمل ندارد (چرا؟)

مثال ۲۲.۴

در $\mathbb{Q}$ به‌عنوان $\mathbb{Z}$ـ مدول، هیچ زیرمدول ناصفر مکمل ندارد. (چرا؟)

$$Q = M \oplus N \qquad \ldots$$

06 simple and semisimple modules

قضیه ۱.۵

فرض کنید M یک Rـمدول مکمل‌پذیر باشد و N زیرمدولی از M باشد. در این صورت N و M/N هر دو مکمل‌پذیرند.

اثبات. فرض کنید $K \leq M$ زیرمدولی از N باشد و چون M مکمل‌پذیر است، پس

$$\exists \mathcal{L} \leq M \text{ که } M = K \oplus \mathcal{L}.$$

در این صورت

$$N = N \cap M = N \cap (K \oplus \mathcal{L}) \stackrel{?}{=} (N \cap K) \oplus (N \cap \mathcal{L}).$$

ثابت می‌کنیم: فرض کنید

$$x \in (N \cap K) \oplus (N \cap L),$$

در این صورت

$$x = x_1 + x_2, s.t \left.\begin{matrix} x_1 \in N \cap K \\ x_2 \in N \cap L \end{matrix}\right\} \implies \begin{cases} x = x_1 + x_2 \in N, \\ x = x_1 + x_2 \in K \oplus L \end{cases} \implies x \in N \cap (K \oplus L).$$

برعکس: اگر

$$x \in N \cap (K \oplus L),$$

در این صورت $x \in N$ و $x = k + \ell$ که $k \in K$، $\ell \in L$. از آنجا که $x \in N$، و $K \leqslant N$، $k \in K$، لذا

$$\ell = x - k \in N \implies \ell \in N \cap L$$

$$\implies k \in N \cap K = K, \quad \ell \in N \cap L \implies x \in (N \cap K) \oplus (N \cap L)$$

پس این دو مجموعه برابرند، لذا

$$N = (K \cap N) \oplus (L \cap N) = K \oplus (L \cap N)$$

یعنی K در N مکمل‌پذیر است.

اما بجای اینکه نشان دهیم M/N مکمل‌پذیر است، با توجه به مکمل‌پذیری M زیرمدول N' وجود دارد که

$$M = N \oplus N'.$$

تعریف می‌کنیم

$$\varphi : M \to N', \quad m = n + n' \longmapsto n'.$$

در این صورت φ یک Rـ همریختی است و $ker\varphi = N$ پس

$$M/N \overset{\text{مدولی}}{\cong} N'$$

حالا چون N' مکمل‌پذیر است، نتیجه می‌گیریم M/N مکمل‌پذیر است. □

سوال ۲.۵

اگر N و M/N مکمل‌پذیر باشند، آیا الزاماً نتیجه می‌دهد M مکمل‌پذیر است؟

مثال نقض.
حلقه‌ی زیر را در نظر بگیرید:

$$S = \frac{R[x]}{\langle x^2 \rangle}$$

مدول $\frac{S}{(x)}$ ساده است، و (x) هر دو Sـ‌مدول‌های تحویل‌ناپذیرند . اما S به‌عنوان Sـ‌مدول نیمه‌ساده نیست چون $\langle x \rangle$ تنها زیرمدول ماکسیمال آن است.

□

قضیه ۳.۵

هر مدول مکمل‌پذیر ناصفر شامل یک زیرمدول ساده است.

اثبات. درواقع کافی است که حکم را برای Rـمدول‌های دوری ثابت کنیم زیرا

$$0 \neq a \in M \implies 0 \neq Ra \leqslant M.$$

و ضمناً Ra هم مکمل‌پذیر است. اما می‌دانیم

$$Ra \overset{\text{مدولی}}{\cong} \frac{R}{Ann(a)} = \frac{R}{I}$$

که I یک ایده‌آل چپ R است. پس در ادامه فرض کنید $M = Ra$ بنابر بحث‌های قبل ایده‌آل ماکسیمال چپ J از R یافت می‌شود که $I \subseteq J$ و لذا $\frac{J}{I} \lneqq \frac{R}{I}$ که نتیجه می‌دهد $\frac{J}{I}$ یک Rـزیرمدول ماکسیمال $\frac{R}{I}$ است، پس M هم زیرمدولی نظیر $\frac{J}{I}$ دارد (مانند N) ولی M مکمل‌پذیر است. پس

$$\exists N' \leq M \quad \text{و} \quad M = N \oplus N'$$

اما $M/N \cong N'$ و M/N ساده است. پس N' ساده است.

$\square$

قضیه ۴.۵

فرض کنید M یک Rـمدول و $M = \sum_{i\in I} M_i$ که M_iها زیرمدول‌های ساده M هستند. اگر $N \leqslant M$ ثابت کنید که $I \subseteq J$ یافته می‌شود که

$$N = \bigoplus_{j\in J} M_j$$

اثبات.

$$\exists J_0 \subseteq I \quad s.t \quad M = \bigoplus_{i\in J_0} M_i.$$

بعلاوه $M \leqslant N$ پس وجود دارد $J_1 \subseteq J_0$ که

$$M = N \oplus \left(\bigoplus_{i \in J_1} M_i \right)$$

اما از طرفی

$$M = \left(\bigoplus_{i \in J_1} M_i \right) \oplus \left(\bigoplus_{i \in J_0 \setminus J_1} M_i \right)$$

و شبیه بحث قبل

$$N \cong \frac{M}{\bigoplus_{i \in J_1} M_i} \cong \bigoplus_{i \in J_0 \setminus J_1} M_i$$

$\square$

با توجه به بحث‌های بالا داریم:

قضیه ۵.۵

M یک Rـمدول است. موارد زیر معادلند:

۱. $M = \sum_{i\in I} M_i$ که M_iها ساده‌اند.

۲. $M = \bigoplus_{i\in J} M_i$ و M_iها ساده‌اند.

۳. M مکمل‌پذیر است.

اثبات.

(۱) $\Leftarrow$ (۲) قبلاً بحث شد.

(۲) $\Leftarrow$ (۳) قبلاً بحث شد.

(۳) $\Leftarrow$ (۱) اگر $M \neq 0$ چون مکمل‌پذیر، بنابراین حتماً یک زیرمدول ساده دارد.
تعریف می‌کنیم:

$$N = \sum_{\substack{P \leqslant M \\ P \text{ ساده}}} P,$$

ادعا ۶.۵

$$N = M$$

برهان خلف: اگر $N \lneq M$، آنگاه

$$\exists N' \leqslant M \quad \text{و} \quad M = N \oplus N'$$

اما N' مکمل‌پذیر (چرا؟) و بنابراین شامل زیرمدول ساده P' است. در این صورت $P' \leqslant N \cap N'$، پس $N = M$. □

تعریف ۷.۵

Rـمدول M را نیم‌ساده (*یا کاملاً تجزیه‌پذیر*) می‌نامیم هرگاه در یکی از شرایط قضیه‌ی قبل صدق کند.

قضیه ۸.۵

حلقه‌ی یک‌دار R را در نظر بگیرید که به عنوان Rـمدول نیم‌ساده است. در این صورت هر R-مدول نیم‌ساده است.

اثبات. اگر M دوری باشد،

$$R\text{نیم‌ساده} \implies \text{مکمل‌پذیر} \implies \exists I' \leqslant R;\ R = I \oplus I' \implies \frac{R}{I} \cong I'$$

$$\exists a; \quad M = Ra \implies M \cong \frac{R}{I}$$

بنابراین

$$M \cong I' \text{مکمل‌پذیر} \implies M \text{نیمه‌ساده}$$

اما در حالت کلی

$$M = \sum_{a \in M} Ra \implies M \text{نیمه‌ساده}$$

چرا که Ra مجموعی از ساده‌ها و $\sum_{a\in M} Ra$ مجموعی از ساده‌ها است.

$\square$

تعریف ۹.۵

حلقه R را *نیمه‌ساده‌ی* گوییم هرگاه بعنوان Rـمدول نیمه‌ساده باشد.

قضیه ۱۰.۵

حلقه‌ی ناتهی و نیمه‌ساده‌ی R با جمع مستقیم تعداد متناهی ایده‌آل چپ مینیمال یکتاست.

اثبات. یک Rـزیرمدول سادهٔ R بعنوان Rـمدول در واقع همان ایده‌آل چپ مینیمال است، پس

$$R = \bigoplus_{i \in J} I_i$$

که I_iها ایده‌آل چپ مینیمال R هستند. اما $1 \in R$

$$1 = r_1 + r_2 + \cdots + r_n$$

که

$$\forall m;\ r_m \in I_{j_m}$$

پس

$$\forall r \in R;\ r = rr_1 + rr_2 + \cdots + rr_n$$

به طوری که $rr_1 \in I_{i_1}, \cdots, rr_n \in I_{i_n}$، پس

$$R = \sum_{m=1}^{n} I_{j_m}$$

و بعلاوه جمع مستقیم است(چرا؟) و لذا حکم ثابت شد.

□

07 Hom

قضیه ۱.۶

فرض کنید R حلقه‌ای یک‌دار و نیم‌ساده است. در این‌صورت R با جمع مستقیم تعداد متناهی ایده‌آل چپ مینیمال برابر است.

اثبات. دقت کنید که R بعنوان Rـ‌مدول نیم‌ساده است و ضمناً هر زیرمدولی از R ایده‌آل چپ R درواقع یک است. بعلاوه، زیرمدول ساده است، هرگاه ایده‌آل چپ مینیمال باشد. اما R نیم‌ساده است، پس

$$R = \bigoplus_{j \in J} I_j$$

که I_jها ایده‌آل‌های چپ مینیمال R هستند. اما چون $1_R \in R$ پس

$$\exists n : 1_R = r_1 + r_2 + \cdots + r_n \quad (r_j \in I_{i_j})$$

در نتیجه هر $r \in R$ داریم

$$r = r1_R = rr_1 + rr_2 + \cdots + rr_n \in \sum_{j=1}^{n} I_{i_j}$$

و چون $\oplus$ جمع مستقیم است(چرا؟)، پس

$$R = \bigoplus_{j=1}^{n} I_{i_j}.$$

□

تعریف ۲.۶

فرض کنید M و N دو Rـمدول باشند. در این‌صورت مجموعه‌ی تمام Rـهمریختی‌ها از M به N را با نماد

$$Hom(M,N)$$

نشان می‌دهیم.

تذکر ۳.۶

$Hom(M,N)$ با جمع معمولی Rـهمریختی‌ها یک گروه آبلی است، زیرا

$$f, g \in Hom(M,N) \implies f+g \in Hom(M,N).$$

اما اگر R حلقه‌ای جابجایی باشد، آنگاه $Hom(M,N)$ یک Rـمدول چپ نیز خواهد بود که ضرب اسکالر را به شکل زیر تعریف می‌کنیم:

$$\forall r \in R, \quad f \in Hom(M,N) \implies rf : M \to N, \quad (rf)(m) := rf(m)$$

و چون R جابجایی است، به ازای هر $rf \in Hom(M,N)$ و $r' \in R$ داریم

$$(rf)(r'm) = rf(r'm) = rr'f(m) = r'rf(m) = r'(rf)(m).$$

تعریف ۴.۶

اگر $M = N$ باشد، آنگاه

$$End_R(M) := Hom(M, M)$$

حلقه‌ی Rـ‌خودریختی‌های M نامیده می‌شود.

تذکر ۵.۶

$End_R(M)$ با عمل جمع و ترکیب توابع تشکیل یک حلقه می‌دهد.

لم ۶.۶ لم شُر:

۱. اگر M یک Rـمدول ساده باشد، در این‌صورت $End_R(M)$ یک حلقه‌ی تقسیم است.

۲. فرض کنید M و N دو Rـمدول ساده باشند، در این‌صورت:

$$M \cong N \iff Hom(M,N) \neq \{0\}.$$

اثبات.

۱. فرض کنید

$$0 \neq f \in End_R(M)$$

دراین‌صورت $ker(f) \leqslant M$ و چون M ساده است، $ker(f)=\{0\}$ یا $ker(f)=M$ که دومی ممکن نیست. پس $ker(f)=\{0\}$ و f یک‌به‌یک است. از طرفی $Im(f) \leqslant M$ و چون M ساده است، $Im(f)=M$، پس f وارون‌پذیر است. بعلاوه f^{-1} یک Rـهمریختی است. پس $End_R(M)$ یک حلقهٔ تقسیم است.

۲. با استدلال مشابه بالا.(چرا؟)

قضیه ۷.۶

فرض کنید M_1 و M_2 و N سه Rـ مدول باشند، در این صورت

۱.

$$Hom(N, M_1 \oplus M_2) \cong Hom(N, M_1) \oplus Hom(N, M_2)$$

که این همریختی، یک همریختی $\mathbb{Z}$ـ مدولی است، و درصورتی که R حلقه‌ای جابجایی باشد، یک همریختی Rـ مدولی است.

۲.

$$Hom(M_1 \oplus M_2, N) \cong Hom(M_1, N) \oplus Hom(M_2, N)$$

که این همریختی، یک همریختی $\mathbb{Z}$ـ مدولی است، و درصورتی که R حلقه‌ای جابجایی باشد، یک همریختی Rـ مدولی است.

اثبات ۱. تعریف می‌کنیم:

$$\psi : Hom(N, M_1 \oplus M_2) \to Hom(N, M_1) \oplus Hom(N, M_2)$$

$$f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$$

که در آن π_1, π_2 توابع تصویر روی مؤلفه‌ی اول و دوم هستند، یعنی:

$$\pi_1 : Hom(N, M_1) \oplus Hom(N, M_2) \to Hom(N, M_1), \quad (a, b) \mapsto a$$

$$\pi_2 : Hom(N, M_1) \oplus Hom(N, M_2) \to Hom(N, M_2), \quad (a, b) \mapsto b$$

واضح است که π_1 و π Rـ همریختی هستند. چرا خوش‌تعریف است؟ و می‌توان دید که π_1, π_2 Rـ همریختی هستند. (چرا؟)

Rـ همریختی:

$$\begin{aligned}\psi(f+g) =&(\pi_1(f+g),\pi_2(f+g))\\ =&(\pi_1(f)+\pi_1(g),\pi_2(f)+\pi_2(g))\\ =&\psi(f)+\psi(g)\end{aligned}$$

$$\left.\begin{aligned}\pi_1(rf)=r\pi_1(f),\\ \pi_2(rf)=r\pi_2(f)\end{aligned}\right\} \implies \psi(rf)=r\psi(f)$$

یک‌به‌یک بودن: اگر $f \in ker\psi$ آنگاه

$$\psi(f) = 0 \implies \begin{cases} \pi_1 f = 0, \\ \pi_2 f = 0. \end{cases}$$

اگر $f \neq 0$ یعنی

$$\exists n \in N : f(n) = (m_1, m_2) \neq (0, 0)$$

پس

$$\pi_1 f \neq 0 \text{ یا } \pi_2 f \neq 0$$

پس $f = 0$، تناقض.

پوشا بودن: فرض کنید

$$(g_1, g_2) \in Hom(N, M_1) \oplus Hom(N, M_2).$$

تعریف می‌کنیم:

$$\forall n;\ f(n) := (g_1(n), g_2(n)),$$

ثابت می‌شود که $f \in Hom(N, M_1 \oplus M_2)$ و $\psi(f) = (g_1, g_2)$.(چرا؟)

اثبات ۲. توابع زیر را تعریف می‌کنیم:

$$\iota_1 : M_1 \to M_1 \oplus M_2, \quad m_1 \mapsto (m_1, 0)$$

$$\iota_2 : M_2 \to M_1 \oplus M_2, \quad m_2 \mapsto (0, m_2)$$

$$\psi : Hom(M_1 \oplus M_2, N) \to Hom(M_1, N) \oplus Hom(M_2, N)$$

$$f \mapsto (f \circ \iota_1, f \circ \iota_2)$$

$\square$

تمرین ۸.۶

ادامه حل را کامل کنید.

تمرین ۹.۶

اگر $\{M_i\}_{i\in I}$ ها Rـمدول باشند و N هم Rـمدول باشد:

۱.

$$Hom\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} Hom(M_i, N)$$

۲.

$$Hom\left(N, \prod_{i\in I} M_i\right) \cong \prod_{i\in I} Hom(N, M_i)$$

(همریختی‌ها $\mathbb{Z}$ـمدولی و اگر R جابجایی باشد Rـمدولی‌اند)

تذکر ۱۰.۶

اگر M یک Rـ مدول باشد، $Hom(R, M)$ یک Rـ مدول چپ است (بدون نیاز به جابجایی R). با تعریف ضرب زیر:

$$\forall r \in R,\ f \in Hom(R, M), \quad (r \cdot f)(a) := f(ar) \quad (\forall a \in R)$$

به ازای هر $a_1, a_2, r, s, a \in R$ داریم:

$$(r \cdot f)(a_1 + a_2) = f((a_1 + a_2)r) = f(a_1 r) + f(a_2 r) = (r \cdot f)(a_1) + (r \cdot f)(a_2)$$

$$(r \cdot f)(sa) = f((sa)r) = f(s(ar)) = sf(ar) = s(r \cdot f)(a)$$

بررسی خواص Rـ مدولی بودن $Hom(R, M)$ ...

قضیه ۱۱.۶

اگر R حلقه‌ی یک‌دار و M یک Rـمدول یکانی باشد آنگاه

$$M \overset{\text{مدولی}}{\cong} Hom(R,M)$$

اثبات. تعریف می‌کنیم:

$$\psi : Hom(R,M) \to M, \quad f \mapsto f(1)$$

ψ یک Rـهمریختی است:

$$\psi(f+g) = (f+g)(1) = f(1) + g(1) = \psi(f) + \psi(g)$$

$$\psi(rf) = (rf)(1) = f(1r) = f(r) \overset{?}{=} rf(1) = r\psi(f)$$

ψ یک‌به‌یک است: اگر

$$f \in ker(\psi) \implies \psi(f) = 0$$

آنگاه

$$f(1) = 0 \implies \forall r \in R, f(r) = rf(1) = 0 \implies f = 0.$$

ψ پوشا است: برای هر $m \in M$، تعریف می‌کنیم:

$$\left.\begin{array}{r} f_m(1) := m, \\ f_m(r) := rm \end{array}\right\} \implies \begin{cases} f_m(r + r') = f_m(r) + f_m(r') \\ f_m(sr) = sf(r) \end{cases}$$

بنابراین $f_m \in Hom(R, M)$ و $\psi(f_m) = m$.

$\square$

08 direct sum

قضیه ۱.۷

فرض کنید R حلقه‌ای نیمه‌ساده و یک‌دار باشد. در این صورت هر Rـمدول ساده با ایده‌آل مینیمالی از R یکریخت است.

اثبات. اگر M یک Rـمدول مدول باشد، در این صورت $M \ni a$ وجود دارد که

$$M = Ra \cong \frac{R}{Ann_R(a)} \cong \frac{R}{I}$$

اما چون R نیمه‌ساده است، پس مکمل پذیر است. ولذا

$$\exists I' \leqslant R; \quad R = I \oplus I' \implies I \overset{\text{مدولی}}{\cong} \frac{R}{I'} \overset{\text{مدولی}}{\cong} M$$

روش دوم. با استفاده از قضایای قبل. فرض کنید $R = \bigoplus_{i=1}^{n} I_i$ که I_iها ایده‌آل‌های مینیمال R هستند و فرض کنید M یک Rـ مدول ساده باشد. آنگاه بنابر قضیهٔ قبل

$$M \cong Hom_R(R, M) = Hom_R\left(\bigoplus_{i=1}^{n} I_i, M\right) = \bigoplus_{i=1}^{n} Hom_R(I_i, M)$$

اما M و I_iها ساده‌اند پس بنابر لم شور هر یک از $Hom_R(I_i, M)$ یا صفر است یا $M \cong I_i$. نتیجه اینکه اگر همه صفر باشند $M = 0$ (چرا؟). در غیر این صورت $M \cong I_i$ که I_i یک ایده‌آل مینیمال R است.

نتیجه: تعداد متناهی ایده‌آل مینیمال از هر حلقهٔ نیمه‌ساده وجود دارد که در هر Rـ مدول ساده، با یکی از آن‌ها یک‌ریخت است.

تذکر ۲.۷

واضح است اگر M، N دو Rـمدول باشند، داریم:

$$Hom_R(\{0\}, N) = \{0\}, \quad Hom_R(M, \{0\}) = \{0\}$$

سوال ۳.۷

اگر $Hom_R(M, N) = \{0\}$، آیا M یا N حتماً باید صفر باشند؟

قضیه ۴.۷

فرض کنید M یک Rـمدول و $\{M_i\}_{i\in I}$ خانواده‌ای از Rـمدول‌ها باشد.

$$M \cong \bigoplus_{i\in I} M_i$$

اگر و تنها اگر به‌ازای هر $i \in I$، Rـهمریختی های $\lambda_i : M_i \to M$ موجود باشند، به‌طوری که، برای هر Rـمدول $\mathcal{X}$ و هر Rـهمریختی $f_i : M_i \to \mathcal{X}$ $(\forall i \in I)$ بتوان Rـهمریختی یکتای $\varphi : M \to \mathcal{X}$ را یافت، به طوری که به ازای هر $i \in I$، داشته باشیم $\varphi\lambda_i = f_i$.

$$\begin{tikzcd}
M_i \arrow[r, "\exists\lambda_i"] \arrow[d, "f_i"'] & M \arrow[dl, dashed, "\exists!\varphi"] \\
\mathcal{X} &
\end{tikzcd}$$

اثبات. ابتدا فرض کنید $M \cong \bigoplus_{i\in I} M_i$. در این وضعیت به ازای هر $i \in I$ نگاشت‌های طبیعی

$$\lambda_i : M_i \to M, \quad m_i \mapsto \{m'_j\}\ s.t \begin{cases} m'_j = m_i & j = i \\ m'_j = 0 & j \neq i \end{cases}$$

را درنظر بگیرید که به‌وضوح یک به یک هستند. نشان می‌دهیم شرط طرف دوم برقرار است.
پس فرض کنید $\mathcal{X}$ یک Rـمدول دلخواه و برای هر $i \in I$، Rـهمریختی های $f_i : M_i \to \mathcal{X}$ مفروض باشند. نگاشت‌های $\pi_i : M \to M_i$ را تصویر روی مؤلفهٔ iـام در نظر بگیرید:

$$\pi_i : M \to M_i, \quad \{m_j\} \mapsto m_i$$

و نگاشت φ را به صورت زیر تعریف می‌کنیم:

$$\varphi : M = \bigoplus_{i\in I} M_i \to \mathcal{X}, \quad \varphi = \sum_{i\in I} f_i \circ \pi_i$$
$$\forall m \in M; \quad \varphi(m) := \sum_{i\in I} f_i(\pi_i(m))$$

آیا تعریف مشکل دار؟ خیر، چون فقط تعداد متناهی تا از مؤلفه‌ها می‌توانند ناصفر باشند.
اما در این صورت برای هر $a_j \in M_j$ و $j \in I$ داریم:

$$\varphi(\lambda_j(a_j)) = \sum_{i\in I} f_i \circ \pi_i(\lambda_j(a_j)) = f_j(a_j)$$

یعنی

$$\forall j \in I, \quad \varphi \circ \lambda_j = f_j$$

یکتایی؟ فرض کنید Rـ همریختی ψ هم همین شرایط را داشته باشد،یعنی

$$\forall j \in I, \quad \psi \circ \lambda_j = f_j$$

از آن‌جا که

$$\sum_{i \in I} \lambda_i \circ \pi_i = \mathsf{id}_M$$

داریم

$$\psi \left(\sum_{i \in I} \lambda_i \circ \pi_i \right) = \psi(\mathsf{id}_M) = \psi$$

از طرفی ψ یک Rـ همریختی است، لذا

$$\psi = \psi \left(\sum_{i \in I} \lambda_i \circ \pi_i \right) = \sum_{i \in I} \psi(\lambda_i \circ \pi_i) = \sum_{i \in I} \psi \circ \lambda_i(\pi_i) = \sum_{i \in I} f_i \circ \pi_i = \varphi$$

برعکس: فرض کنید Rـهمریختی های $\lambda_i : M_i \to M$ موجودند، به‌طوری که خواص مطرح شده را دارند. چون برای هر Rـمدول، (X) شرط قضیه برقرار است، فرض می‌کنیم $\mathcal{X} = \oplus_{i\in I} M_i$ و Rـهمریختی های $f_i : M_i \to \mathcal{X}$ را هم نگاشت طبیعی درنظر می‌گیریم.

$$\begin{tikzcd}
M_i \arrow[r, "\lambda_i"] \arrow[d, "f_i"'] \arrow[dd, bend right, "\lambda_i"'] & M \arrow[dl, dashed, "\exists!\varphi"] \arrow[ddl, bend left, "\mathrm{id}_M"] \\
\mathcal{X} = \oplus_{i\in I} M_i \arrow[d, dashed, "\exists!\psi"] & \\
M &
\end{tikzcd}$$

$$
\begin{tikzcd}
& M_i \arrow[r, "\lambda_i"] \arrow[d, "f_i"] \arrow[ddl, "\lambda_i"'] & M \arrow[dl, dashed, "\exists!\varphi"] \arrow[ddll, bend left, "\mathrm{id}_M"] \\
& \mathcal{X} = \bigoplus_{i\in I} M_i \arrow[dl, dashed, "\exists!\psi"] & \\
M & &
\end{tikzcd}
$$

از عبارات فوق:

$$
\begin{cases} \varphi \circ \lambda_i = f_i & \forall i \\ \psi \circ f_i = \lambda_i & \forall i \end{cases} \implies \psi \circ \varphi \circ \lambda_i = \lambda_i \quad \forall i
$$

چون $\mathrm{id}_M \circ \lambda_i = \lambda_i$ برای هر i، بنابراین از یکتایی داریم $\psi \circ \varphi = \mathrm{id}_M$ و در نتیجه ψ وارون‌پذیر و در نتیجه یک Rـ یک‌ریختی است. یعنی:

$$
M \cong \bigoplus_{i\in I} M_i
$$

$\square$

به‌صورت مشابه ثابت می‌شود که:

قضیه ۵.۷

فرض کنید M یک Rـمدول و $\{M_i\}_{i\in I}$ خانواده‌ای از Rـمدول‌ها باشد. آنگاه

$$M \cong \bigoplus_{i\in I} M_i$$

اگر و تنها اگر به‌ازای هر $i \in I$، Rـهمریختی های $\pi_i : M_i \to M$ موجود باشند، به‌طوری که، برای هر Rـمدول $\mathcal{X}$ و هر Rـهمریختی $f_i : M_i \to \mathcal{X}$ $(\forall i \in I)$ بتوان Rـهمریختی یکتای $M \to \mathcal{X} : \varphi$ را یافت، به طوری که به ازای هر $i \in I$، داشته باشیم $\pi_i\varphi = f_i$.

$$\begin{tikzcd} & M \arrow[d, "\pi_i"] \\ \mathcal{X} \arrow[ur, dashed, "\exists!\varphi"] \arrow[r, "f_i"'] & M_i \end{tikzcd}$$

اثبات. (تمرین) □

09 Free modules

مدول‌های آزاد

تعریف ۱.۹

اگر M یک Rـمدول و $\mathcal{X} \subseteq M$ باشد، $\mathcal{X}$ را *مستقل خطی* گوییم هرگاه

$$\forall x_1, x_2, \dots, x_n \in \mathcal{X}, \quad r_1x_1 + \cdots + r_nx_n = 0 \implies r_1 = r_2 = \cdots = r_n = 0.$$

در این حالت گوییم $\mathcal{X}$ نسبت به حلقه R مستقل خطی است. $\mathcal{X}$ را وابستهٔ خطی گوییم، هرگاه مستقل خطی نباشد.

تعریف ۲.۹

زیرمجموعه $\mathcal{X}$ از M را یک *پایه* برای M گوییم هرگاه $M = \langle \mathcal{X} \rangle$ و $\mathcal{X}$ مستقل خطی باشد.

تعریف ۳.۹

Rـمدول M را *آزاد* (Free) نامیم هرگاه دارای یک پایه باشد.

مثال ۴.۹

$M=\{0\}$ آزاد است زیرا $M=\langle\emptyset\rangle$ و $\emptyset$ مستقل خطی است.

مثال ۵.۹

حلقه‌ی یک‌دار R به عنوان Rـ مدول $R=\langle 1\rangle$ آزاد است.

مثال ۶.۹

به عنوان $\mathbb{Z}$ـ مدول، $\mathbb{Z}_n$ آزاد نیست چرا که

$$\begin{cases} \mathbb{Z}_n=\langle\overline{1}\rangle \\ \mathbb{Z}_n=\langle\overline{a}\rangle \quad (a,n)=1 \end{cases}$$

پس آزاد نیست (چرا؟).

مثال ۷.۹

$\mathbb{Q}$ به عنوان $\mathbb{Z}$ـ مدول آزاد نیست.

فرض. $Q = \langle X \rangle$

اگر $|X| \geq 2$ آنگاه $\frac{a}{b}, \frac{c}{d} \in X$، اما در این صورت:

$$bc\left(\frac{a}{b}\right) + (-da)\left(\frac{c}{d}\right) = 0$$

که تناقض است. حال اگر $|\mathcal{X}| = 1$ آنگاه $\{\frac{M}{n}\} = \mathcal{X}$. ولی در اینصورت $\frac{m}{2n} \notin \langle X \rangle$.

تذکر ۸.۹

اگر Rـمدول M با تولید متناهی باشد، آنگاه الزاما هر زیرمدول آن با تولید متناهی نیست.

مثال ۹.۹

حلقهٔ $R = \mathbb{Z}[x_1, x_2, x_3, \dots]$ را در نظر بگیرید. R به عنوان Rـمدول با تولید متناهی است ($R = \langle 1 \rangle$) ولی ایده‌آل

$$I = \langle x_1, x_2, x_3, \dots \rangle \lneq R$$

که یک Rـزیرمدول است با تولید متناهی نیست (چرا؟) (راهنمایی: چندجمله‌ای ثابت صفر و هر چندجمله‌ای متناهی متغیر.). [اگر حلقه نوتری باشد هر زیرمدول یک Rـمدول با تولید متناهی است. پس باید حلقه را غیر نوتری بگیریم.]

تذکر ۱۰.۹

واضح است اگر M با تولید متناهی یاشد، آنگاه $\frac{M}{N}$ نیز با تولید متناهی است.

قضیه ۱۱.۹

اگر Rـمدول M نوتری باشد، آنگاه N و $\frac{M}{N}$ با تولید متناهی باشند، آنگاه M نیز با تولید متناهی است.

اثبات. فرض کنید

$$N = \langle n_1, n_2, \dots, n_k \rangle, \quad \frac{M}{N} = \langle m_1 + N, \dots, m_t + N \rangle.$$

اگر $m \in M$ دلخواه باشد، می‌توان نوشت:

$$\begin{aligned} m + N &= r_1(m_1 + N) + \cdots + r_t(m_t + N) = r_1 m_1 + \cdots + r_t m_t + N \\ &\implies m - (r_1 m_1 + \cdots + r_t m_t) \in N \\ &\implies m - (r_1 m_1 + \cdots + r_t m_t) = r'_1 n_1 + \cdots + r'_k n_k \\ &\implies m \in \langle m_1, \dots, m_t, n_1, \dots, n_k \rangle \end{aligned}$$

تذکر ۱۲.۹

Rـمدول M می‌تواند با تولید متناهی باشد ولی پایه‌ای متناهی نداشته باشد. (چرا؟)

مثال ۱۳.۹

$\mathbb{Z}_n$ به عنوان $\mathbb{Z}$ـمدول (مستقل خطی؟).

تذکر ۱۴.۹

اگر M آزاد باشد و $N \leqslant M$ آنگاه لزوماً $\frac{M}{N}$ آزاد نیست.

مثال ۱۵.۹

- $\mathbb{Z}$ به عنوان $\mathbb{Z}$ـ مدول ،
- $n\mathbb{Z}$ به عنوان $\mathbb{Z}$ـ مدول ، و
- $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

تذکر ۱۶.۹

اگر M آزاد باشد و $N \leqslant M$ آنگاه لزوماً N آزاد نیست.

مثال ۱۷.۹

$\mathbb{Z}_6$ به عنوان $\mathbb{Z}$ـمدول آزاد است، اما

$$\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}\}$$

به عنوان $\mathcal{Z}_6$مدول آزاد نیست زیرا $\overline{0} = \overline{3}\cdot\overline{4} = \overline{3}\cdot\overline{2}$.
بعداً در بحث دنباله‌های دقیق خواهیم دید که اگر N و $\frac{M}{N}$ آزاد باشند، آنگاه M هم آزاد است.

مثال ۱۸.۹

$R = \mathbb{R}[x,y]$، در این صورت R به عنوان Rـ مدول آزاد است. نشان دهید $N = \langle x, y \rangle$ آزاد نیست.

اثبات. $R = \langle 1 \rangle$
اگر N آزاد باشد و فرض کنیم A پایه آن باشد، در این صورت بایستی $|A| > 1$ چرا که x, y نمی‌توانند با تنها یک چندجمله‌ای تولید شوند. حال اگر

$$f(x), g(x) \in A \implies g(x)f(x) + (-f(x))g(x) = 0$$

پس مستقل خطی نیستند. پس N به عنوان Rـ مدول آزاد نیست.

10 Notherian and Artinian modules

تذکر ۱.۱۰ خارج از درس

$\mathbb{R}$ به‌عنوان $\mathbb{Z}$ـمدول آزاد نیست. (چرا که $\mathbb{Q}$ به‌عنوان $\mathbb{Z}$ـمدول آزاد نیست.) [با کمک قضیهٔ ددکیند یا قضیهٔ Nielsen - Schreier] (زیرگروه هر گروه آبلی آزاد، آزاد است.) $\mathbb{R}$ به‌عنوان $\mathbb{Q}$ـمدول آزاد است. (پایهٔ Hammel)

لم ۲.۱۰

اگر M یک Rـمدول آزاد با پایه‌ای n عضوی مانند $\{m_1, \dots, m_n\}$ باشد آنگاه:

$$M \overset{\text{مدولی}}{\cong} R^n$$

اثبات.

$$\psi : R^n \to M, \quad (\alpha_1, \dots, \alpha_n) \mapsto \sum_{i=1}^{n} \alpha_i m_i$$

$$\dots$$

$\square$

قضیه ۳.۱۰

فرض کنید M یک Rـمدول آزاد و با تولید متناهی باشد. در این صورت هر پایه M تعداد متناهی عضو دارد.

اثبات. فرض کنید $\{e_i\}_{i\in I}$ یک پایه برای M باشد، اما چون M با تولید متناهی است، پس

$$\exists m_1, \dots, m_n; \quad M = \langle m_1, \dots, m_n \rangle$$

هر m_j را می‌توان به صورت ترکیب خطی متناهی از e_iها نوشت:

$$m_1 = r_{11}e_{i_1} + r_{12}e_{i_2} + \cdots + r_{1k_1}e_{i_{k_1}}$$

$$\vdots$$

$$m_n = r_{n1}e_{n_1} + r_{n2}e_{n_2} + \cdots + r_{nk_n}e_{n_{k_n}}$$

مجموعهٔ تمام e_iهای ظاهر شده را به صورت T در نظر بگیرید. T متناهی است و $M = \langle T \rangle$. چون $\{e_i\}$ پایه است، T مستقل خطی است و پس T یک پایه متناهی است.

$\square$

قضیه ۴.۱۰

فرض کنید M یک Rـمدول آزاد و با تولید متناهی باشد. در این صورت هر دو پایهٔ M تعداد برابری عضو دارد.

اثبات. فرض کنید:

$$S_1 = \{e_i\}_{i=1}^{n}, \quad S_2 = \{e'_j\}_{j=1}^{m}$$

دو پایه برای M باشند. آنگاه:

$$M \cong R^n, \quad M \cong R^m \quad \Longrightarrow R^n \overset{\text{مدولی}}{\cong} R^m$$

در این صورت Rـهمریختی یک به یک و پوشا $\varphi : R^m \to R^n$ و Rـهمریختی یک به یک و پوشا $\psi : R^n \to R^m$ وجود دارد به‌نحوی که

$$\left.\begin{aligned} A_{n\times m} &= [\varphi]_{S_1,S_2} \\ B_{m\times n} &= [\psi]_{S_2,S_1} \end{aligned}\right\} \ s.t \quad \begin{aligned} AB &= I_{n\times n}, \\ BA &= I_{m\times m} \end{aligned}$$

حال $\bar{A} = \begin{bmatrix} A & 0 \end{bmatrix}$ و $\bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$ را تعریف می‌کنیم. آنگاه:

$$\left.\begin{aligned} \bar{A}\bar{B} = AB = I_n, \\ \bar{B}\bar{A} = \begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix} \end{aligned}\right\} \implies det(\bar{A}\bar{B}) = det(\bar{B}\bar{A}) \implies 0 = 1$$

$\square$

مدول‌های نوتری و آرتینی

تعریف ۱.۱۱

Rـ مدول M را یک *مدول نوتری* نامیم هرگاه هر زنجیر صعودی از Rـ زیرمدول‌های M متوقف شود.

مثال. $\mathbb{Z}$ به عنوان $\mathbb{Z}$ـ مدول نوتری است زیرا تمام زیرمدول‌های آن به شکل $\langle m \rangle$ هستند و:

$$n \mid m \;\Leftrightarrow\; \langle m \rangle \subseteq \langle n \rangle$$

ولذا هر زنجیر صعودی از زیرمدول‌ها متوقف می‌شود.

تعریف ۲.۱۱

Rـ مدول M را یک *مدول آرتینی* نامیم هرگاه هر زنجیر نزولی از زیرمدول‌های M متوقف شود.

مثال ۳.۱۱

$\mathbb{Z}$ به عنوان $\mathbb{Z}$ـ مدول آرتینی نیست زیرا:

$$\mathbb{Z} \supsetneq \langle 2 \rangle \supsetneq \langle 4 \rangle \supsetneq \langle 8 \rangle \supsetneq \dots$$

و هیچگاه متوقف نمی‌شود.

مثال ۴.۱۱

هر گروه آبلی متناهی به عنوان $\mathbb{Z}$ـ مدول هم نوتری است و هم آرتینی.

مثال ۵.۱۱

به عنوان $\mathbb{Z}$ـمدول، $\mathbb{Q}$ نه نوتری است و نه آرتینی زیرا:

$$\mathbb{Q} \supsetneq \langle 2 \rangle \supsetneq \langle 4 \rangle \supsetneq \langle 8 \rangle \supsetneq \dots$$

و

$$\langle \tfrac{1}{2} \rangle \subsetneq \langle \tfrac{1}{4} \rangle \subsetneq \langle \tfrac{1}{8} \rangle \subsetneq \dots$$

مثال ۶.۱۱

هر فضای برداری با بعد متناهی هم نوتری است و هم آرتینی.

تعریف ۷.۱۱

فرض کنید p عددی اول باشد. تعریف کنید:

$$M = \left\{ \frac{a}{p^n} \,\middle|\, n \in \mathbb{N},\ a \in \mathbb{Z} \right\}$$

$(M, +)$ یک گروه آبلی است. بعلاوه:

$$(\mathbb{Z}, +) \subsetneq M \subsetneq (\mathbb{Q}, +)$$

گروه خارج‌قسمتی $\frac{M}{\mathbb{Z}}$ را در نظر بگیرید. این گروه را $\mathbb{Z}_{p^\infty}$ می‌نامیم.

مثال ۸.۱۱

$\mathbb{Z}_{p^\infty}$ به عنوان $\mathbb{Z}$ـمدول آرتینی است ولی نوتری نیست.

اثبات. برای اثبات، تعریف کنید:

$$G_n = \left\{ \frac{a}{p^n} + \mathbb{Z} = \overline{\frac{a}{p^n}} \in \mathbb{Z}_{p^\infty} \;\middle|\; a \in \mathbb{Z} \right\}$$

ادعا:

۱. هر G_n زیرگروهی از $\mathbb{Z}_{p^\infty}$ است،

۲. به‌ازای هر n داریم، $G_n \subsetneq G_{n+1}$،

۳. $\mathbb{Z}_{p^\infty} = \bigcup_{n=1}^{\infty} G_n$،

۴. هر زیرمدول ناصفر $\mathcal{N} \leqslant \mathbb{Z}_{p^\infty}$ برابر با G_n برای یک n است.

برای این منظور ابتدا ثابت می‌کنیم که اگر $\overline{\frac{a}{p^n}} \in \mathcal{N}$ هرگاه $p \nmid a$ در این صورت $\overline{\frac{1}{p^n}} \in \mathcal{N}$

$$
\begin{aligned}
(a,p)=1 \quad &\Longrightarrow \quad (a,p^n)=1 \\
&\Longrightarrow \quad \exists r,s \in \mathbb{Z},\ ra+sp^n=1 \\
&\Longrightarrow \quad \overline{\frac{a}{p^n}} \in \mathcal{N} \\
&\Longrightarrow \quad r\cdot\overline{\frac{a}{p^n}} \in \mathcal{N} \\
&\Longrightarrow \quad \overline{\frac{1-sp^n}{p^n}} \in \mathcal{N} \\
&\Longrightarrow \quad \overline{\frac{1}{p^n}} - s \in \mathcal{N} \\
&\Longrightarrow \quad \overline{\frac{1}{p^n}} \in \mathcal{N} \\
&\Longrightarrow \quad G_n \subseteq \mathcal{N}.
\end{aligned}
$$

اگر بزرگ‌ترین n را در نظر بگیریم که به‌ازای یک a، $\overline{\frac{a}{p^n}} \in \mathcal{N}$ آنگاه $G_n \subseteq \mathcal{N}$ و اگر $G_n \neq \mathcal{N}$، آنگاه:

$$\exists m > n; \quad \overline{\frac{a}{p^m}} \in \mathcal{N}, \quad (a,p)=1$$

که تناقض است. و اگر چنین nای وجود نداشته‌باشد

$$\mathcal{N} = \mathbb{Z}_{p^\infty}.$$

نتیجه: فقط زنجیر زیر در $\mathbb{Z}_{p^\infty}$ وجود دارد:

$$G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \dots$$

که نشان می‌دهد نوتری نیست ولی آرتینی هست.

□

قضیه ۹.۱۱

اگر M یک Rـمدول یکانی باشد، گزاره‌های زیر معادل‌اند:

۱. M یک Rـمدول نوتری است.

۲. هر زیرمدول M با تولید متناهی است.

۳. هر مجموعهٔ ناتهی از زیرمدول‌های M دارای یک عضو ماکسیمال است.

اثبات: (۱) $\Longleftarrow$ (۲) فرض کنید $M \leq N$. اگر $N = 0$ آنگاه نتیجه برقرار است. اگر $N \neq 0$، آنگاه $x_1 \in N$ ناصفر وجود دارد به طوری که اگر $N = \langle x_1 \rangle$ تمام است. در غیر این صورت $x_2 \in N \setminus \langle x_1 \rangle$ ناصفر وجود دارد. به همین ترتیب اگر $N = \langle x_1, x_2 \rangle$، تمام است وگرنه $\exists x_3 \in N \setminus \langle x_1, x_2 \rangle$ و ادامه دادن این فرآیند:

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \dots$$

زنجیر صعودی بی‌نهایت می‌دهد که با نوتری بودن در تناقض است، پس این فرآیند متوقف می‌شود.

(۲) $\Longleftarrow$ **(۳)**: فرض کنید $\{M_i\}_{i\in I}$ مجموعه‌ای از زیرمدول‌های M باشد. اگر M_1 ماکسیمال نباشد، $M_1 \subsetneq M_2$ وجود دارد و به همین ترتیب:

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \dots$$

قرار دهید

$$\mathcal{N} = \bigcup_{i=1}^{+infty} M_i$$

در این صورت $\mathcal{N}$ زیر مدولی از M و کران بالای تمام M_i ها است. طبق فرض $n_k, \cdots, n_1$ وجود دارد به‌نحوی که

$$\mathcal{N} = \langle n_1, \cdots, n_k \rangle$$

لذا هر n_i در M_{j_i} قرار خواهد گرفت. اگر قرار دهید

$$k = max\{j_i \mid 1 \leqslant i \leqslant n\}$$

در این صورت $\mathcal{N} = M_k$.

(۳) $\Longleftarrow$ **(۱)**: فرض کنید
$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$$
یک زنجیر صعودی از زیرمدول‌ها باشد. اگر
$$\bigcup_{i=1}^{\infty} M_i$$
را در نظر بگیریم، این یک زیرمدول M است که ماکسیمال در این زنجیر وجود دارد، پس زنجیر متوقف می‌شود. $\square$

تعریف ۱۰.۱۱

Rـمدول M را **متناهیاً تولید شده** گوییم هرگاه چنانچه برای Rـزیرمدول‌های $\{M_i\}_{i\in I}$ داشته باشیم $M = \sum_{i\in I} M_i$ بتوان زیرمجموعهٔ متناهی $J \subseteq I$ را یافت به‌نحوی که $M = \sum_{i\in J} M_i$. (معادل بودن با تعریف قبل؟)

تعریف ۱۱.۱۱

Rـمدول M را **متناهیاً هم‌تولید شده** گوییم هرگاه چنانچه برای Rـزیرمدول‌های $\{M_i\}_{i\in I}$ داشته باشیم $\bigcap_{i\in I} M_i = 0$ بتوان زیرمجموعهٔ متناهی $J \subseteq I$ را یافت به‌نحوی که $\bigcap_{i\in J} M_i = 0$.

11 Notherian and Artinian modules (2)

مثال ۱.۱۲

$\mathbb{Z}$ به عنوان $\mathbb{Z}$ـ مدول با تولید متناهی است. ولی متناهیاًهم‌تولید شده نیست.

$$\bigcap_{p \text{ اول}} pZ = 0 \quad \Longrightarrow \quad ?$$

مثال ۲.۱۲

$\mathbb{Z}_p^{\infty}$ متناهیاًهم‌تولید شده است ولی با تولید متناهی نیست.

قضیه ۳.۱۲

برای هر Rـمدول M موارد زیر معادلند:

۱. M آرتینی است.

۲. هر مدول خارج‌قسمتی M متناهیاًهم‌تولید شده است.

۳. هر مجموعهٔ ناتهی از زیرمدول‌های M دارای عنصر مینیمالی است.

اثبات. (۱) $\Longleftarrow$ (۲): فرض کنید $M \leqslant N$ و $\frac{M}{N}$ را در نظر بگیرید. اگر

$$\bigcap_{i\in I} \frac{M_i}{N} = 0 \implies \bigcap_{i\in I} M_i = N.$$

ثابت می‌کنیم تعدادی متناهی از اعضای I هستند که

$$\bigcap_{1\leqslant i\leqslant k} M_i = N$$

ادامهٔ اثبات

برای این منظور دقت کنید:

$$M_1 \supsetneqq M_1 \cap M_2 \supsetneqq M_1 \cap M_2 \cap M_3 \supsetneqq \dots$$

ولی در این صورت چون M آرتینی است پس:

$$\exists k \quad s.t \quad \bigcap_{i=1}^{k} M_i = \bigcap_{i \in I} M_i = N$$

پس حکم ثابت شد یعنی $\frac{M}{N}$ متناهیاًهم‌تولیدشده‌است.

ادامهٔ اثبات

(۲) $\Longleftarrow$ (۳): خانواده $\{M_i\}_{i\in I}$ از زیرمدول‌های Rـ‌مدول M را در نظر بگیرید.

اگر M_1 مینیمال باشد.✓

در غیر این‌صورت، $M_2 \subsetneq M_1$ وجود دارد. اگر M_2 مینیمال باشد.✓

در غیر این‌صورت، $M_3 \subsetneq M_2$ وجود دارد. اگر M_3 مینیمال باشد.✓

$$\vdots$$

با تکرار این فرایند، زنجیرهٔ

$$\cdots \subsetneq M_3 \subsetneq M_2 \subsetneq M_1$$

بدست می‌آید.

قرار دهید
$$N = \bigcap_{i=1}^{k} M_i \leqslant M.$$
در این صورت در $\frac{M}{N}$ داریم $\bigcap_{i\in I} \frac{M_i}{N} = 0$. و چون $\frac{M}{N}$ متناهیاًهم تولیدشده است، پس
$$\exists k \quad s.t \quad \bigcap_{i=1}^{k} \frac{M_i}{N} = 0$$
یعنی $N = M_k$ چون تو در تو بود و لذا $N = M_k = M_{k+1}$

(۳) $\Longleftarrow$ (۱): واضح است.

قضیه ۴.۱۲

اگر $M \leqslant N$،

$$M \text{ نوتری است } \iff N \text{ و } \frac{M}{N} \text{ نوتری باشند.}$$

اثبات. اگر M نوتری باشد، در اینصورت زنجیرهٔ

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$$

از زیرمدول‌های N در واقع زنجیره‌ای از زیرمدول‌های M هم هستند. پس متوقف می‌شود.
به صورت مشابه هر زنجیره از زیرمدول‌های $\frac{M}{N}$ به شکل

$$\frac{M_1}{N} \subsetneq \frac{M_2}{N} \subsetneq \frac{M_3}{N} \subsetneq \dots$$

است که از نوتری بودنِ M متوقف می‌شود.

ادامهٔ اثبات

برعکس. N و $\frac{M}{N}$ نوتری هستند. ثابت می‌کنیم هر زیرمدول K از M با تولید متناهی است.
از آنجا که $\frac{K+N}{N}$ زیر مدولی از $\frac{M}{N}$ است و $\frac{M}{N}$ نوتری است، $\frac{K+N}{N}$ با تولید متناهی است. با کمک قضیهٔ دوم یکریختی:

$$\frac{K+N}{N} \cong \frac{K}{K\cap N}$$

و درنتیجه بهَ‌عنوان Rـ مدول

$$\frac{K}{K\cap N} = \langle k_1 + K\cap N, \dots, k_\ell + K\cap N\rangle \implies K = \langle k_1, \dots, k_\ell\rangle + K\cap N$$

از آنجا که $K\cap N$ زیرمدولی از N است، پس با تولید متناهی است. لذا

$$K\cap N = \langle n_1, \dots, n_m\rangle$$

و بنابراین

$$K = \langle n_1, \dots, n_m, k_1, \dots, k_\ell\rangle$$

با تولید متناهی است و M نوتری است. M نوتری $\implies$ نتیجه واضح است. $\square$

قضیه ۵.۱۲

اگر $M \leq N$، از آرتینی بودنِ M نتیجه می‌شود N و $\frac{M}{N}$ آرتینی‌اند (دقیقاً همان اثباتِ قبل).

برعکس نیز برقرار است، ولی ابتدا یک لم را ثابت می‌کنیم.

لم ۶.۱۲

فرض کنید N_1, N_2, N_3 زیرمدول‌های یک Rـمدولِ M باشند به‌طوری‌که

$$\left.\begin{aligned} N_2 &\subseteq N_1, \\ N_1 + N_3 &= N_2 + N_3, \\ N_1 \cap N_3 &= N_2 \cap N_3. \end{aligned}\right\} \implies N_1 = N_2.$$

اثبات.

$$N_1 = N_1 \cap (N_1 + N_3) = N_1 \cap (N_2 + N_3) = (N_1 \cap N_2) + (N_1 \cap N_3) = N_1 + (N_1 \cap N_3) = N_2$$

□

قضیه ۷.۱۲

اگر $M \leqslant N$ و N و $\dfrac{M}{N}$ آرتینی باشند، آنگاه M آرتینی است.

اثبات. یک زنجیرهٔ نزولی از زیرمدول‌های M را در نظر بگیرید

$$M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \cdots .$$

در این‌صورت

$$M_1 + N \supsetneq M_2 + N \supsetneq M_3 + N \supsetneq \cdots .$$

و لذا

$$\frac{M_1 + N}{N} \supsetneq \frac{M_2 + N}{N} \supsetneq \frac{M_3 + N}{N} \supsetneq \cdots$$

در $\dfrac{M}{N}$ نزولی است؛

چون $\dfrac{M}{N}$ آرتینی است، $\exists k$ به‌طوری‌که برای هر $i \geq 0$

$$\frac{M_k+N}{N} = \frac{M_{k+i}+N}{N} \qquad \Longrightarrow \qquad M_k+N = M_{k+i}+N.$$

از طرفی زنجیرهٔ

$$M_1 \cap N \ \supsetneqq\ M_2 \cap N \ \supsetneqq\ M_3 \cap N \ \supsetneqq\ \cdots$$

در N نزولی است؛ چون N آرتینی است، $\exists t$ به‌طوری‌که برای هر $j \geq 0$

$$M_t \cap N = M_{t+j} \cap N.$$

اکنون اگر $s \geq max\{k,t\}$ ، برای هر $i \geq 0$ داریم

$$\left.\begin{aligned} M_{s+i} \subseteq M_s, \\ M_{s+i}+N = M_s+N, \\ M_{s+i} \cap N = M_s \cap N. \end{aligned}\right\} \xrightarrow{\text{از لم قبل}} \forall i;\ M_s = M_{s+i} \implies M \text{ آرتینی است}.$$

$\square$

قضیه ۸.۱۲

اگر $\{M_i\}_{i\in I}$ خانواده‌ای از Rـمدول‌های ناصفر باشد، آنگاه:

$$\bigoplus_{i\in I} M_i \text{ نوتری (آرتینی) است.} \iff \left\{ \begin{array}{l} I \text{ متناهی است،} \\ \text{هر } M_i \text{ نوتری (آرتینی) است.} \end{array} \right.$$

اثبات. اگر $\bigoplus_{i\in I} M_i$ آرتینی باشد و I نامتناهی باشد، دنبالهٔ

$$\bigoplus_{i\in I} M_i \supsetneq \bigoplus_{i\in I\setminus\{i_1\}} M_i \supsetneq \bigoplus_{i\in I\setminus\{i_1,i_2\}} M_i \supsetneq \cdots$$

بی‌نهایت نزولی تشکیل می‌دهد که متوقف نمی‌شود، تناقض.
اگر $\bigoplus_{i\in I} M_i$ نوتری و I نامتناهی باشد، می‌توان نوشت

$$\{0\} \subsetneq M_1 \subsetneq M_1 \oplus M_2 \subsetneq \cdots$$

که تناقض است.

برعکس.
حال اگر I متناهی و هر M_i نوتری (آرتینی) باشد، داریم:

$$\frac{M_1 \oplus M_2}{M_1} \overset{\text{مدولی}}{\cong} M_2$$

پس اگر M_1 و M_2 نوتری (آرتینی) باشد، در این‌صورت $M_1 \oplus M_2$ نوتری (آرتینی) خواهد بود. با تکرار k مرحله، حکم ثابت می‌شود:

$$\bigoplus_{i=1}^{k} M_i = \left(\bigoplus_{i=1}^{k-1} M_i \right) \bigoplus M_k$$

□

قضیه ۹.۱۲

فرض کنید $M = \sum_{i\in I} M_i$ که I متناهی و M_iها زیرمدول‌های M هستند. آنگاه:

M_i نوتری (آرتینی) است. $\forall i; \iff$ M نوتری (آرتینی) است.

اثبات. اگر M نوتری (آرتینی) باشد، چون $M \leqslant M_i$، نتیجه می‌شود M_i نوتری (آرتینی) است.

برعکس، فرض کنید هر M_i نوتری (آرتینی) باشد. در این صورت نگاشت

$$\begin{aligned} \varphi : \bigoplus_{i=1}^{n} M_i &\rightarrow \sum_{i=1}^{n} M_i \\ (m_1, m_2, \dots, m_n) &\mapsto m_1 + m_2 + \cdots + m_n \end{aligned}$$

یک هم‌ریختی پوشا است و داریم

$$\frac{\bigoplus_{i=1}^{n} M_i}{ker(\varphi)} \cong \sum_{i=1}^{n} M_i.$$

اگر هر M_i نوتری (آرتینی) باشد، حاصل‌جمع مستقیم متناهی $\bigoplus_{i=1}^{n} M_i$ نیز نوتری (آرتینی) است. چون خارج‌قسمت یک مدول نوتری (آرتینی) نیز نوتری (آرتینی) است، نتیجه می‌شود $\sum_{i=1}^{n} M_i$ نوتری (آرتینی) است.

$\square$

قضیه ۱۰.۱۲

اگر M یک Rـمدول ساده باشد، موارد زیر معادلند:

۱. M با تولید متناهی است.

۲. M آرتینی است.

۳. M نوتری است.

اثبات. (۱) $\Longleftarrow$ (۲): بدیهی است چون هر مدول با بُعد متناهی آرتینی است.

(۲) $\Longleftarrow$ (۱): اگر M آرتینی باشد و ساده، داریم

$$\left.\begin{array}{r} M=\bigoplus_{i\in I} M_i \ (M_i \text{ ساده}) \\ M=\langle \alpha_1,\alpha_2,\cdots,\alpha_k\rangle \end{array}\right\} \Longrightarrow I \text{ متناهی است.(چرا؟)} \quad M \Longrightarrow \text{نیمه‌ساده است.}$$

هر α_i مجموعی متناهی از تعدادی عناصر ناصفر M_i ها است، بنابر این اندیس‌های ظاهر شده (؟)
اما

$$M\text{نوتری و آرتینی} \Longrightarrow I\text{متناهی} \Longrightarrow M_i\text{نوتری و آرتینی} \Longrightarrow M_i\text{ساده}$$

(۲) $\Leftarrow$ (۳)

$$\left.\begin{array}{r} \text{(ساده } M_i) \; M = \bigoplus_{i\in I} M_i \\ \text{.آرتینی است } M \end{array}\right\} \Longrightarrow \text{متناهی } I \Longrightarrow \text{نوتری } M.$$

(۳) $\Leftarrow$ (۱) واضح است.(قضیه)

$\square$

قضیه ۱۱.۱۲

هر Rـمدول آرتینی ناصفر دارای حداقل یک زیرمدول ساده است.

اثبات. یک زنجیرهٔ نزولی از زیرمدول‌ها بگیرید:

$$M_1 \supsetneqq M_2 \supsetneqq M_3 \supsetneqq \dots$$

به‌علت آرتینی بودن، این زنجیره متوقف می‌شود و مینیمم به‌دست می‌آید که ساده است. $\square$

قضیه ۱۲.۱۲

اگر R یک حلقهٔ یک‌دار باشد، موارد زیر معادلند:

۱. R به عنوان Rـمدول چپ، نوتری (آرتینی) است.

۲. هر Rـمدول با تولید متناهی، نوتری (آرتینی) است.

اثبات. (۱) $\Longleftarrow$ (۲): اگر $M = \langle m_1, \dots, m_n \rangle$، نگاشت

$$\varphi : R^n \to M, \quad (r_1, \dots, r_n) \mapsto r_1 m_1 + \dots + r_n m_n$$

یک همریختی پوشا است، بنابراین $M \cong R^n / ker(\varphi)$. چون R نوتری (آرتینی) است، بنابراین R^n نوتری (آرتینی) است و خارج‌قسمت یک مدول نوتری (آرتینی) نیز نوتری (آرتینی) است، M نوتری (آرتینی) خواهد بود.

(۲) $\Longleftarrow$ (۱): با قرار دادن $R = 1$ حکم بدست می‌آید. $\square$

قضیه ۱۳.۱۲

اگر R حلقه‌ای یک‌دار و به‌عنوان Rـ مدول چپ آرتینی است. اگر $M = 0$ یکریختی Rـ مدول دلخواه باشد، آنگاه M حداقل یک زیرمدول ساده دارد.

اثبات. چون $M \neq 0$، یک $x \in M$ انتخاب کنید و بگذارید $N = Rx$. این N یک زیرمدول غیرصفر و با تولید متناهی است و به‌علت آرتینی بودن، زنجیرهٔ نزولی از زیرمدول‌های N متوقف می‌شود، بنابراین یک زیرمدول مینیمم (ساده) دارد. $\square$

12 Noetherian and Artinian rings

حلقهٔ نوتری (آرتینی)

تعریف ۱.۱۳ حلقهٔ نوتری (آرتینی)

فرض کنید R یک حلقه باشد. در این صورت R را **نوتری چپ (آرتینی چپ)** گوییم هرگاه هر زنجیر صعودی (نزولی) از ایده‌آل‌های چپ متوقف شود. **حلقه** R **را نوتری (آرتینی) گوییم هرگاه هم نوتری (آرتینی) چپ و هم نوتری (آرتینی) راست باشد.**

قضیه ۲.۱۳

فرض کنید R حلقه‌ای یک‌دار باشد. در این صورت R نوتری چپ (آرتینی چپ) است اگر و تنها اگر برای هر $1 \geqslant n$، $M_n(R)$ نوتری چپ (آرتینی چپ) باشد.

اثبات. $M_n(R)$ با تولید متناهی به عنوان Rـ مدول چپ (چرا؟) پس نوتری (آرتینی) است. اما هر ایده‌آل چپ $M_n(R)$ خود یک Rـ مدول چپ هم هست (چرا؟) پس هر زنجیر از ایده‌آل‌های چپ $M_n(R)$ زنجیری از Rـ زیرمدول‌های $M_n(R)$ است و لذا متوقف می‌شود.
برعکس. فرض کنید $n = 1$. □

تذکر ۳.۱۳

اگر حلقه $M_n(R)$ حتی برای یک n هم نوتری (آرتینی) چپ باشد، نتیجه می‌شود که R نوتری (آرتینی) چپ است. چرا که

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \Rightarrow M_n(I_1) \subsetneq M_n(I_2) \subsetneq M_n(I_3) \subsetneq \cdots$$

قضیهٔ اساسی هیلبرت

قضیه ۴.۱۳ قضیهٔ اساسی هیلبرت

حلقهٔ R نوتری و یک‌دار $\iff$ حلقهٔ $R[x]$ نوتری چپ است.

اثبات. فرض کنید که R نوتری چپ باشد و زنجیر

$$A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \cdots$$

از ایده‌آل‌های $R[x]$ را در نظر بگیرید.

اثبات قضیهٔ اساسی هیلبرت

ابتدا برای هر ایده‌آل I از $R[x]$ و هر $n \in \mathbb{N}$ تعریف می‌کنیم:

$$\varphi_n(I) = \{a \in R \mid a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in I \text{ و } a = a_n \neq 0\} \cup \{0\}.$$

واضح است که $\varphi_n(I)$ یک ایده‌آلِ R است. بعلاوه چون I ایده‌آل $R[x]$ است، پس

$$\varphi_n(I) \subseteq \varphi_{n+1}(I).$$

بعلاوه اگر I و J دو ایده‌آل $R[x]$ باشند که $I \subseteq J$ و بعلاوه به‌ازای هر $n \in N$

$$\varphi_n(I) = \varphi_n(J)$$

آنگاه $I = J$. برای اثبات این مطلب فرض کنید

$$f(x) \in J \setminus I.$$

اثبات قضیهٔ اساسی هیلبرت

در این صورت اگر درجهٔ $f(x)$ برابر با n باشد و چون

$$\varphi_n(I) = \varphi_n(J)$$

پس

$$g_n(x) \in I$$

هست که ضریب x^n آن با $f(x)$ یکسان است. (چرا؟) و لذا

$$f(x) - g_n(x)$$

یا صفر است یا درجهٔ آن کمتر یا مساوی x^{n-1} می‌باشد. نتیجه ایکنه چون

$$\varphi_{n-1}(I) = \varphi_{n-1}(J)$$

با استدلال مشابه $g_{n-1}(x)$ در I هست که

$$f(x) - g_n(x) - g_{n-1}(x)$$

یا صفر است یا درجهٔ حداکثر $n-2$ و با ادامه دادن این فرآیند نهایتاً به صفر می‌رسیم(چرا؟) پس $f(x)$ مجموعی از عناصر I است و لذا $I = J$. که تناقض است.

اثبات قضیهٔ اساسی هیلبرت

حال به اثبات برمی‌گردیم:

$$A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \cdots$$

ابتدا تمام ایده‌آل‌ها به شکل

$$\varphi_t(A_s)$$

را که $t, s \in \mathbb{N}$ در یک مجموعه قرار می‌دهیم. بنابر فرض چون R نوتری است، این مجموعه عناصر ماکسیمالی مانند $\varphi_k(A_l)$ دارد که $k, q \in \mathbb{N}$. پس برای هر $t, s \in \mathbb{N}$،

$$\varphi_t(A_l) \subseteq \varphi_k(A_l)$$

و اما چون $\varphi_k(A_q) \subseteq \varphi_k(A_{q+i})$ برای هر $i \in \mathbb{N}$، پس

$$\forall k' \geq k \quad \varphi_{k'}(A_l) = \varphi_k(A_l).$$

یعنی

$$\forall i \in \mathbb{N} \quad \varphi_k(A_l) = \varphi_{k+i}(A_l).$$

اثبات قضیهٔ اساسی هیلبرت

بعلاوه $\forall j \in \mathbb{N}$ داریم $A_l \subseteq A_{l+j}$ و در نتیجه

$$\varphi_k(A_l) \subseteq \varphi_{k+i}(A_{l+j}) \quad \forall i, j \in \mathbb{N}.$$

بنابراین فقط $\varphi_1, \varphi_2, \dots, \varphi_{k-1}$ بررسی نشده‌است. اما

$$\varphi_1(A_l) \subseteq \varphi_1(A_{l+1}) \subseteq \varphi_1(A_{l+2}) \subseteq \dots$$

و از نوتری بودن R مرتبه‌ای مانند $l + t_1$ هست که

$$\varphi_1(A_{l+t_1}) = \varphi_1(A_{l+t_1+i}) \quad \forall i \in \mathbb{N}.$$

به همین صورت برای φ_2 مقداری مانند $l + t_2$ هست که

$$\varphi_2(A_{l+t_2}) = \varphi_2(A_{l+t_2+i}) \quad \forall i \in \mathbb{N},$$

و همین‌طور برای φ_{k-1} یک مرتبهٔ $q + t_{k-1}$ وجود دارد.

اثبات قضیهٔ اساسی هیلبرت

حال با در نظر گرفتن

$$m \geq \max\{\ l+t_1, l+t_2, \ldots, l+t_{k-1}\}$$

نتیجه می‌شود که

$$\forall n \in \mathbb{N} \quad \varphi_n(A_m) = \varphi_n(A_{m+i}) \quad \forall i.$$

و بنابراین ادعا ثابت شده:

$$A_m = A_{m+i} \quad \forall i \in \mathbb{N}.$$

یعنی $R[x]$ نوتری چپ است. $\square$

تذکر ۵.۱۳

حکم برای آرتینی صحیح نیست.

قضیه ۶.۱۳

اگر $M = \bigoplus_{i=1}^{n} M_i$ که M_iها Rـمدول می‌باشند، در این‌صورت

$$Hom_R(M,M) \overset{\text{حلقه‌ای}}{\cong} \begin{bmatrix} Hom_R(M_1,M_1) & Hom_R(M_2,M_1) & \cdots & Hom_R(M_k,M_1) \\ Hom_R(M_1,M_2) & Hom_R(M_2,M_2) & \cdots & Hom_R(M_k,M_2) \\ \vdots & \vdots & \ddots & \vdots \\ Hom_R(M_1,M_k) & Hom_R(M_2,M_k) & \cdots & Hom_R(M_k,M_k) \end{bmatrix}$$

اثبات.

$$\sigma : Hom_R(M,M) \longrightarrow [\ldots]$$

به‌طوری که

$$\sigma(\varphi) = \left[\pi_i \varphi \iota_j\right]_{(i,j)}$$

ادامهٔ اثبات

حال

$$\sigma(\varphi_1+\varphi_2)=\left[\pi_i(\varphi_1+\varphi_2)\iota_j\right]=\sigma(\varphi_1)+\sigma(\varphi_2)$$

$$\sigma(\varphi_1)\,\sigma(\varphi_2)=\left[\pi_i\varphi_1\iota_j\right]\left[\pi_i\varphi_2\iota_j\right]=\left[\sum_{k=1}^{n}\pi_i\varphi_1\iota_k\,\pi_k\varphi_2\iota_j\right]$$

$$=\left[\pi_i\varphi_1\left(\sum_{k=1}^{n}\iota_k\pi_k\right)\varphi_2\iota_j\right]=\left[\pi_i\varphi_1\varphi_2\iota_j\right]=\sigma(\varphi_1\varphi_2)$$

پس σ همریختی حلقه‌ای است.

ادامهٔ اثبات

یک به یک بودن:

$$\sigma(\varphi) = 0 \quad \Longleftrightarrow \quad \varphi \in \ker \sigma$$

اگر $0 \neq \varphi$، آنگاه

$$\exists (m_1, \dots, m_n) \in M \quad s.t. \quad \varphi(m_1, \dots, m_n) \neq 0$$

پس

$$\exists j; \quad \varphi(0, \dots, 0, m_j, 0, \dots, 0) \neq 0$$

یعنی این عبارت که یک بردار است مولفهٔ j آن ناصفر است. بنابراین

$$\exists i \quad \pi_i \varphi \iota_j (m_j) \neq 0$$

و لذا $\pi_i \varphi \iota_j \neq 0$ که با $\sigma(\varphi) = [0]$ تناقض دارد. پس σ یک‌به‌یک است.

ادامهٔ اثبات

پوشا بودن: فرض کنید $[f_{ij}]$ عنصری در طرف راست عبارت بالا باشد، تعریف می‌کنیم:

$$\varphi = \sum_{r} \sum_{s} \iota_r f_{rs} \pi_s$$

که عنصری از $Hom_R(M, M)$ است. آنگاه:

$$\sigma(\varphi) = \left[\pi_i \left(\sum_{r,s} \iota_r f_{rs} \pi_s \right) \iota_j \right]$$

حال می‌دانیم که اگر $i \neq j$ آنگاه $\pi_i \iota_j = 0$ و $\pi_i \iota_i = \mathrm{id}$. پس

$$\sigma(\varphi) = [f_{ij}] \, .$$

□

تعریف ۷.۱۳ حلقهٔ متضاد

اگر R یک حلقه باشد، در این صورت

$$R^{op}$$

همان مجموعهٔ اعضای R است، جمع همان جمع حلقهٔ R است، اما ضرب به صورت

$$a * b := ba \quad (R \text{ ضرب در })$$

تعریف می‌شود که مجدداً یک حلقه می‌سازد.

لم ۸.۱۳

اگر R یک حلقه باشد

$$M_n(R)^{op} \overset{\text{حلقه‌ای}}{\cong} M_n(R^{op})$$

به‌صورت حلقه‌ای.

اثبات. تعریف می‌کنیم

$$\varphi : M_n(R)^{op} \longrightarrow M_n(R^{op}), \quad A \longmapsto A^t.$$

از نظر مجموعه $R^{op} = R$ پس $M_n(R^{op}) = M_n(R)^{op}$ به عنوان مجموعه یا گروه جمعی. داریم:

$$\varphi(A+B) = (A+B)^t = A^t + B^t = \varphi(A) + \varphi(B).$$

ضرب: در $M_n(R)^{op}$ داریم

$$\varphi(A * B) = \varphi(BA) = (BA)^t = A^t B^t = \varphi(A)\varphi(B).$$

و به وضوح φ یک به یک و پوشا است.

□

قضیه ۹.۱۳

اگر R یک‌دار باشد

$$R^{op} \overset{\text{حلقه‌ای}}{\cong} Hom_R(R,R)$$

به‌صورت حلقه‌ای.

اثبات. تعریف می‌کنیم

$$\varphi : R^{op} \longrightarrow Hom_R(R,R), \quad a \longmapsto f_a : R \to R, \quad f_a(r) := ra.$$

واضح است که

$$f_a(r_1 + r_2) = f_a(r_1) + f_a(r_2),$$
$$f_a(rr') = rr'a = r(r'a) = rf_a(r'),$$

پس $f_a \in Hom_R(R,R)$.

ادامهٔ اثبات

بعلاوه φ همریختی حلقه‌ای است:

$$\varphi(a_1 + a_2) = f_{a_1+a_2} = f_{a_1} + f_{a_2} = \varphi(a_1) + \varphi(a_2),$$

$$\varphi(a_1 * a_2) = \varphi(a_2 a_1) = f_{a_2 a_1} = f_{a_2} f_{a_1} = \varphi(a_1)\varphi(a_2),$$

زیرا

$$f_{a_2} f_{a_1}(r) = f_{a_2}(ra_1) = (ra_1)a_2 = ra_1 a_2.$$

φ یک‌به‌یک و پوشا است:

یک‌به‌یک بودن: $ker(\varphi) = \{0\}$ واضح است.

پوشا بودن: اگر $g \in Hom_R(R, R)$، آنگاه

$$g(r) = rg(1) \quad \Longrightarrow \quad g = f_{g(1)}.$$

پس یک‌ریخت است. $\square$

قضیه ۱۰.۱۳ قضیهٔ آرتین–ودربرن

فرض کنید R حلقه‌ای نیم‌ساده باشد. در این صورت اعداد طبیعی $n_1, \dots, n_k$ و حلقه‌های تقسیم $D_1, D_2, \dots, D_k$ موجودند به‌طوری‌که

$$R \overset{\text{حلقه‌ای}}{\cong} M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

اثبات. R حلقه‌ای نیم‌ساده است، پس جمع مستقیم تعدادی متناهی زیرمدول ساده (ایده‌آل مینیمال) خودش است:

$$R = \bigoplus_{i=1}^{n} M_i.$$

می‌نویسیم

$$R = \bigoplus_{i=1}^{k} n_i M_i$$

که $M_i \ncong M_j$ هرگاه $i \neq j$. و

$$n_iM_i = \bigoplus_{t=1}^{n_i} M_i.$$

حال می‌توان نوشت

$$R^{op} \overset{\text{حلقه‌ای}}{\cong} Hom_R(R,R) \overset{\text{حلقه‌ای}}{\cong} Hom_R\left(\bigoplus_{i=1}^{k} n_iM_i, \bigoplus_{i=1}^{k} n_iM_i\right)$$

$$\cong \begin{bmatrix} Hom_R(n_1M_1, n_1M_1) & \cdots & Hom_R(n_kM_k, n_1M_1) \\ \vdots & \ddots & \vdots \\ Hom_R(n_1M_1, n_kM_k) & \cdots & Hom_R(n_kM_k, n_kM_k) \end{bmatrix}$$

اگر $i \neq j$ آنگاه

$$Hom_R(n_iM_i, n_jM_j) \cong \bigoplus_{t=1}^{n_in_j} Hom_R(M_i, M_j) = 0$$

که در آن همریختی ها $\mathbb{Z}$ـمدولی هستند. از آنجا که به‌عنوان $\mathbb{Z}$ـمدول برابر با صفر شد، پس به‌عنوان Rـمدولی هم صفر می‌شود.
و دقت کنید که

$$Hom_R(n_iM_i, n_iM_i) \cong \begin{bmatrix} Hom_R(M_i, M_i) & \cdots & \\ \vdots & \ddots & \end{bmatrix}$$

در تمام درایه‌ها $Hom_R(M_i, M_i)$ ظاهر می‌شود که چون M_i ساده است، بنابر لم شُور $Hom_R(M_i, M_i) = D_i$ یک حلقهٔ تقسیم می‌شود. پس

$$Hom_R(n_iM_i, n_iM_i) \cong M_{n_i}(D_i).$$

با جمع‌بندی داریم:

$$R^{op} \cong \begin{bmatrix} M_{n_1}(D_1) & 0 & \cdots & 0 \\ 0 & M_{n_2}(D_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_{n_k}(D_k) \end{bmatrix} \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

آخرین گام: اگر op بگیریم و دقت کنیم که D_i^{op} خودش هم یک حلقهٔ تقسیم است، حکم ثابت می‌شود. $\square$