دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

چه زمانی یک حلقه ماتریسی ۲ × ۲ روی یک حلقه موضعی جابجایی قویاً تمیز است ؟

پایان‌نامه کارشناسی ارشد رشته ریاضی محض

گلی جدی

استاد راهنما

دکتر محمدرضا ودادی

۱۳۸۶

دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد رشته ریاضی محض خانم گلی جدی

تحت عنوان

چه زمانی یک حلقه ماتریسی ۲ × ۲ روی یک حلقه موضعی جابجایی قویاً تمیز است ؟

در تاریخ ۱۳۸۶/۸/۱۲ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهائی قرار گرفت.

۱ــ استاد راهنمای پایان‌نامه	دکتر محمدرضا ودادی
۲ــ استاد مشاور پایان‌نامه	دکتر احمد حقانی
۳ــ استاد داور ۱	دکتر عاطفه قربانی ()
۴ــ استاد داور ۲	دکتر حسین خبازیان

سرپرست تحصیلات تکمیلی دانشکده دکتر رسول نصر اصفهانی

$w \in J(R)$، در R نسبت به x حلپذیر است.

(۲) هرگاه $2 \in J(R)$ و $R/J(R) \ncong \mathbb{Z}_2$، آنگاه $\mathbb{M}_2(R)$ قویاً تمیز است اگر و تنها اگر معادله $x^2 + (1 + w_1)x = w_2$ برای هر $w_1, w_2 \in J(R)$، در R نسبت به x حلپذیر است.

(۳) شرایط زیر با هم معادلند:

(الف) $\mathbb{M}_2(R)$ قویاً تمیز است.

(ب) $\mathbb{M}_2(R[[x]])$ قویاً تمیز است.

(ج) $\mathbb{M}_2(R[x]/(x^n))$ قویاً تمیز است.

(د) $\mathbb{M}_2(RC_2)$ قویاً تمیز است (هرگاه C_2 گروه دوری ازمرتبه ۲ باشد).

فهرست مطالب

چکیده:

یک حلقه یکدار R قویاً تمیز نامیده می‌شود اگر هر عضو $a \in R$ به صورت $a = e + u$ باشد که در آن $e^2 = e$، $u^{-1} \in R$ و $eu = ue$. اگر p یک عدد اول باشد، حلقه ماتریسی $\mathbb{M}_2(\hat{\mathbb{Z}}_p)$ که در آن $\hat{\mathbb{Z}}_p$ حلقه اعداد صحیح $p-adic$ است، قویاً تمیز است، اما $\mathbb{M}_2(\mathbb{Z}_{(p)})$ که در آن $\mathbb{Z}_{(p)}$ موضعی سازی $\mathbb{Z}$ در ایدآل اول تولید شده توسط p است، قویاً تمیز نیست. اگر R یک حلقه موضعی جابجایی باشد، یک مشخصه‌سازی برای R در حالتی که حلقه ماتریسی $\mathbb{M}_2(R)$ قویاً تمیز باشد، بدست آمده است. فرض کنید R هر حلقه جابجایی باشد. اگر $\mathbb{M}_2(R)$ قویاً تمیز باشد آنگاه معادله $x^2 - x = w$ برای هر $w \in J(R)$، در R نسبت به x حلپذیر است. بعلاوه فرض کنید که R یک حلقه موضعی جابجایی باشد، در این صورت

(۱) هرگاه $\frac{1}{2} \in R$ یا $R/J(R) \cong \mathbb{Z}_2$، آنگاه $\mathbb{M}_2(R)$ قویاً تمیز است اگر و تنها اگر معادله $x^2 - x = w$ برای هر $w \in J(R)$، در R نسبت به x حلپذیر است.

(۲) هرگاه $2 \in J(R)$ و $R/J(R) \ncong \mathbb{Z}_2$، آنگاه $\mathbb{M}_2(R)$ قویاً تمیز است اگر و تنها اگر معادله $x^2 + (1 + w_1)x = w_2$ برای هر $w_1, w_2 \in J(R)$، در R نسبت به x حلپذیر است.

(۳)شرایط زیر با هم معادلند:

(الف) $\mathbb{M}_2(R)$ قویاً تمیز است.

(ب) $\mathbb{M}_2(R[[x]])$ قویاً تمیز است.

(ج) $\mathbb{M}_2(R[x]/(x^n))$ قویاً تمیز است.

(د) $\mathbb{M}_2(RC_2)$ قویاً تمیز است(هرگاه C_2 گروه دوری ازمرتبه ۲ باشد).

تاریخچه

وارفیلد[۱] در سال ۱۹۷۲ [۴۵]، ضمن بررسی مدول هایی که خاصیت تبادل متناهی دارند و بدنبال یافتن پاسخ این پرسش که آیا این خاصیت تحت هم ارزی موریتا پایاست، نشان داد که مدول ${}_RM$ دارای خاصیت تبادل متناهی است اگر و تنها اگر ${}_SS$ دارای خاصیت تبادل متناهی باشد، که در آن $S = End({}_RM)$ (یک $R-$ مدول M دارای خاصیت تبادل‌متناهی است هرگاه برای هر مدول ${}_RA$ و هر دو تجزیه $A = M' \oplus N = \bigoplus_{i=1}^{n} A_i$ که در آن $M \cong M'$، زیرمدول های $A'_i \subset A_i$ وجود دارند به طوری که $A = M' \oplus (\bigoplus_{i=1}^{n} A'_i)$). در سال ۱۹۷۷ نیکلسون[۲] [۳۴] نشان داد که یک حلقه R دارای خاصیت تبادل متناهی است اگر و تنها اگر خودتوان ها به هنگ هر ایدآل سره بالا بروند و اگر خودتوان ها در R مرکزی باشند، آنگاه R دارای خاصیت تبادل متناهی است اگر و تنها اگر حلقه R تمیز باشد، بدین معنی که هر عضو R مجموع یک خودتوان و یک یکه باشد. مقالات متعددی در رابطه با این که چه موقع خاصیت تمیز بودن تحت هم ارزی موریتا پایدار است، نوشته شده است. با توجه به شرط مرکزی بودن خودتوان ها در قضیه نیکلسون، در سال ۱۹۹۹ [۳٦]، مفهوم قویاً تمیز توسط نیکلسون به صورت زیر مطرح شد.
حلقه مفروض R قویاً تمیز نامیده می‌شود، هرگاه هر عضو $a \in R$ به صورت مجموع $e + u$ باشد که در آن $e^2 = e \in R$، $u \in U(R)$ و $eu = ue$. وی در[۳٦] نشان داد که هر حلقه قویاً $\pi-$ منظم، قویاً تمیز است (حلقه R قویاً $\pi-$ منظم است، هرگاه زنجیر $aR \supseteq a^2R \supseteq \dots$ برای هر $a \in R$ متوقف شود)، و پرسش های زیر را مطرح کرد:

(۱) آیا هر حلقه قویاً تمیز مانند R، دارای برد پایدار ۱ است ؟(R دارای برد پایدار ۱ است، هرگاه شرط $aR + bR = R$ ایجاب کند که $a + by \in U(R)$ برای بعضی $y \in R$).

(۲) آیا هر حلقه قویاً تمیز مانند R، ددکیند متناهی است ؟(R ددکیند متناهی نامیده می‌شود، هرگاه $xy = 1$ در R، $yx = 1$ را نتیجه می‌دهد).

(۳) آیا خاصیت قویاً تمیز بودن ، پایدار موریتا است؟

[۱] Warfield
[۲] Nicholson

(۴) آیا هر حلقه منظم یکه، قویاً تمیز است؟(حلقه R منظم یکه نامیده می‌شود، هرگاه برای هر $a \in R$، $a = eu$ که در آن $e^{2} = e \in R$ و $u \in U(R)$).

(۵) آیاهر حلقه نیم کامل ، قویاً تمیز است؟(حلقه R نیم کامل نامیده می‌شود، هرگاه $R/J(R)$ یک حلقه نیمساده باشد و خودتوان ها به هنگ $J(R)$ بالا بروند).

مقاله اصلی، که نگارش این پایان نامه با توجه به آن تدوین گردیده است، پاسخ پرسش (۳) را بررسی می‌کند[۱۶]. ولی در پایان نامه در مورد بقیه پرسش ها نیز مطالبی آورده شده است. در سال ۲۰۰۱، چن [۳] و لی [۴] [۱۴]، نشان دادند که پاسخ پرسش های (۱) و (۲)، برای حلقه هایی که شرط زنجیر نزولی روی ایدآل های اساسی دارند، مثبت است. در تلاش برای پاسخ دادن به پرسش های (۴) و (۵) در سال ۲۰۰۱، کامیلو [۵] و خورانا[۶] [۹]، نشان دادند که هر حلقه منظم یکه و هر حلقه نیم کامل، تمیز است. مثالی از یک حلقه نیم کامل که قویاً تمیز نیست در سال ۲۰۰۴ توسط وانگ [۷] و چن [۴۴]، ارائه شده است.
اما در مورد پاسخ پرسش (۳)، ثابت شده است که اگر R یک حلقه‌قویاً تمیز باشد و $e^{2} = e \in R$، آنگاه eRe قویاً تمیز است [۱۵]. بنابراین پرسش (۳) به پرسش زیر تقلیل می‌یابد:
آیا اگر حلقه R قویاً تمیز باشد، آنگاه حلقه ماتریسی $\mathbb{M}_{2}(R)$ نیز قویاً تمیز است ؟
از آنجا که هر حلقه موضعی جابجایی، قویاً تمیز است، جواب این پرسش حتی در حالتی که R یک حلقه موضعی جابجایی است نیز به اندازه کافی جای بحث دارد و مطالب زیر در این راستا اثبات شده است :
قضیه [۳۱]: فرض کنید R یک حلقه موضعی جابجایی باشد. احکام زیر معادلند:

(۱) حلقه $\mathbb{M}_{2}(R)$ قویاً تمیز است.

(۲) برای هر $A \in \mathbb{M}_{2}(R)$ که $\det A \in J(R)$ و $\det(A-I) \in J(R)$، معادله مشخصه A، $x^{2} - (trA)x + \det A = 0$ در R نسبت به x حلپذیر است.

(۳) برای هر $A \in \mathbb{M}_{2}(R)$ که $\det A \in J(R)$ و $\det(A-I) \in J(R)$، معادله $x^{2} - x - \frac{\det A}{(trA)^{2} - 4\det A} = 0$ در R نسبت به x حلپذیر است.

(۴) هر $A \in \mathbb{M}_{2}(R)$ که $\det A \in J(R)$ و $\det(A-I) \in J(R)$ در $\mathbb{M}_{2}(R)$ قطری شدنی است.

(۵) برای هر $w \in J(R)$، ماتریس $B = \begin{pmatrix} 1 & 1 \\ -w & 0 \end{pmatrix}$ قویاً تمیز است.

(۶) برای هر $w \in J(R)$، معادله $x^{2} - x + w = 0$ در R نسبت به x حلپذیر است.

(۷) برای هر $w \in J(R)$ و $u \in U(R)$، معادله $x^{2} - ux + w = 0$ در R نسبت به x حلپذیر است.

---
[۳] Chen
[۴] Li
[۵] Camillo
[۶] Khurana
[۷] Wang

قضیه[۱۶]: فرض کنید R یک حلقه موضعی جابجایی باشد.

(۱) اگر $۲ \in U(R)$، آنگاه $\mathbb{M}_۲(R)$ قویاً تمیز است اگر و تنها اگر، برای هر $w \in J(R)$، معادله $x^۲ - x = w$ در R نسبت به x حلپذیر باشد.

(۲) اگر $R/J(R) \cong \mathbb{Z}_۲$، آنگاه $\mathbb{M}_۲(R)$ قویاً تمیز است اگر و تنها اگر، برای هر $w \in J(R)$، معادله $x^۲ - x = w$ در R نسبت به x حلپذیر باشد.

(۳) اگر $۲ \in J(R)$ و $R/J(R) \ncong \mathbb{Z}_۲$، آنگاه $\mathbb{M}_۲(R)$ قویاً تمیز است اگر و تنها اگر، برای هر $w_۱, w_۲ \in J(R)$، معادله $x^۲ + (۱ + w_۱)x = w_۲$ در R نسبت به x حلپذیر باشد.

در سال ۲۰۰۷ بروآ[۸] ، دایسل [۹] و درسی [۱۰] [۷]، یک حلقه موضعی R را شفاف نامیدند(bleached)، اگر برای هر $u \in U(R)$ و هر $j \in J(R)$، گروه آبلی درونریختی های

$$l_u - r_j \quad \text{و} \quad l_j - r_u$$

از R پوشا باشد. به عنوان یک نتیجه از قضیه زیر، ثابت شده است که $\mathbb{T}_n(R)$ (حلقه ماتریس های پایین مثلثی روی R) قویاً تمیز است، هرگاه R یک حلقه موضعی جابجایی باشد.

قضیه [۷]: فرض کنید R یک حلقه موضعی شفاف باشد. آنگاه حلقه $\mathbb{T}_n(R)$ قویاً تمیز است.

---

۸ Borooah

۹ Diesl

۱۰ Dorsey

پرسش های مطرح شده ۵—۱ در تاریخچه را به صورت زیر پاسخ می‌دهیم :

پرسش ۱و۲، صفحه ۸۱.

پرسش ۳، که همان طور که دیدیم به بررسی ماتریس های ۲ × ۲ تقلیل می یابد برای حلقه های موضعی به طور مفصل در فصل ۲ مورد بررسی قرار می‌گیرد.

پرسش ۵، صفحه ۸۲.

فصل ۱

مقدمه ای بر حلقه و مدول

در سر تا سر مقاله تمام حلقه ها یکدار و شرکت پذیر و تمام مدول ها یکانی اند، مگر خلاف آن ذکر شود.

تعریف ۱.۱ عضو a در حلقه R را خودتوان گویند، هرگاه $a^۲ = a$.
واضح است که در هر حلقه یکدار عناصر ۰ و ۱ خودتوان هستند، آن ها را خودتوان های بدیهی گویند.

تعریف ۲.۱ فرض کنید R یک حلقه ای یکدار باشد. عناصر معکوس پذیر در R را یکه نامند و در صورتی که هر عضو ناصفر R یکه باشد R یک میدان چپ یا یک حلقه تقسیم گویند.

۱—۱ حوزه تجزیه یکتا (UFD) و حوزه اقلیدسی

تعریف ۳.۱ فرض کنید D یک حلقه باشد. دو عضو $a, b \in D$ در D شریک هستند، در صورتی که به ازای یکه ای مانند u از D داشته باشیم $a = bu$.
دامنه صحیحی چون D یک حوزه تجزیه یکتا (UFD) است، در صورتی که شرایط زیر برقرار باشد.
(الف) هر عضو D را که نه صفر و نه یکه ای از D است، بتوان به حاصل ضربی از تعداد متناهی تحویل ناپذیر تجزیه کرد.(در اینجا تحویل ناپذیر عضوی است که در هر تجزیه یکی از عوامل یکه باشد.)

(ب) اگر $p_1 \cdots p_r$ و $q_1 \cdots q_s$ دو تجزیه تحویل ناپذیرها از یک عضو D باشند، آن گاه $r = s$ و q_j ها را بتوان طوری تجدید شماره گذاری کرد که هر p_i و q_i شریک باشند.

لم ۴.۱ در یک UFD مانند D یک عضو مربع کامل است اگر و تنها اگر تعداد مقسوم علیه‌های آن فرد باشد.

اثبات. فرض کنید $0 \neq a \in D$. بنا به تعریف UFD، a تجزیه ای به صورت حاصل ضرب متناهی از تحویل ناپذیرها دارد. یعنی

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$

که در آن $p_1, \ldots, p_t$ عناصر تحویل ناپذیر D و $\alpha_1, \ldots, \alpha_t$ اعداد صحیح مثبتی هستند.اگر $d(a)$ نمایانگر تعداد مقسوم علیه های a باشد، می دانیم که $d(kl) = d(k)d(l)$ هرگاه $\gcd(k,l) = 1$.حال چون p_i ها تحویل ناپذیرند، داریم

$$\begin{aligned} d(a) &= d(p_1^{\alpha_1}) \ldots d(p_t^{\alpha_t}) \\ &= (\alpha_1 + 1) \ldots (\alpha_t + 1) \end{aligned}$$

بنابراین اگر تعداد مقسوم علیه های a زوج باشد، یعنی $d(a)$ عددی زوج باشد، حداقل برای یک i، $(\alpha_i + 1)$ زوج است. پس α_i فرد است و این نتیجه می دهد که a مربع کامل نیست. این نشان می دهد که اگر a مربع کامل باشد، آنگاه تعداد مقسوم علیه های آن فرد است.
بر عکس، فرض کنید تعداد مقسوم علیه های a فرد باشد، در نتیجه برای هر i، $(\alpha_i + 1)$ فرد است و یا به عبارت معادل ، هر α_i زوج است. از این رو a یک مربع کامل است. ■
میدان کسر یک دامنه جابجایی D با $Q(D)$ نمایش داده می‌شود.

گزاره ۵.۱ فرض کنید D یک UFD و $0 \neq a \in D$. معادله $x^2 = a$ در D نسبت به x حلپذیر است اگر و تنها اگر معادله $x^2 = a$ در $Q(D)$ نسبت به x حلپذیر باشد.

اثبات. $(\Leftarrow)$. واضح است، زیرا $D \subseteq Q(D)$.
$(\Rightarrow)$. فرض کنید معادله $x^2 = a$ در $Q(D)$ نسبت به x حلپذیر باشد، بنابراین

$$\exists\ \frac{m}{n} \in Q(D) \quad : \quad (\frac{m}{n})^2 = a \Rightarrow m^2 = an^2$$

هرگاه $\gcd(m,n)=1$.

ادعا می کنیم $\gcd(a,n^2)=1$. فرض کنید چنین نباشد لذا

$$\exists\, p \;:\; p|a, p|n^2 \Rightarrow p|m^2 \Rightarrow p|m \Rightarrow \gcd(m,n)\neq 1$$

که تناقض است. بنابراین طبق لم ۴.۱

$$d(m^2)=d(a)d(n^2)$$

چون m^2 و n^2 مربع کامل می باشند پس تعداد مقسوم علیه هایشان فرد است. پس ناگزیر تعداد مقسوم علیه های a نیز فرد است. و لذا a نیز در D یک مربع کامل است. یعنی

$$\exists\, y\in D \;:\; y^2=a$$

بنابراین معادله $x^2=a$ در D نسبت به x حلپذیر است.

■

تعریف ۶.۱ یک ارزیابی اقلیدسی بر حوزه صحیحی مانند D تابعی است چون v که اعضای ناصفر D را بتوی اعداد صحیح نامنفی بنگارد، به طوری که شرایط زیر برقرار باشند.

(۱) به ازای هر $a,b\in D$، با $b\neq 0$، اعضای q و r در D وجود داشته باشند به طوری که $a=bq+r$ و $r=0$ یا $v(r)<v(b)$.

(۲) به ازای هر $a,b\in D-\{0\}$، $v(a)\geq v(ab)$.

حوزه D یک حوزه اقلیدسی است در صورتی که یک ارزیابی اقلیدسی بر D وجود داشته باشد.

۱—۲ ایدآل بیشین و ایدآل کمین

تعریف ۷.۱ حلقه R مفروض است.

(الف) یک ایدال (راست) بیشین از حلقه R عبارتست از ایدال (راست) چون M متفاوت با R به طوری که هیچ ایدال (راست) از R به طور سره بین M و R نباشد.

(ب) یک ایدآل (راست) کمین از حلقه R عبارتست از ایدال (راست) چون L متفاوت با (0) به طوری که هیچ ایدال (راست) از R به طور سره بین L و (0) نباشد.

ایدال های چپ بیشین و کمین نیز به طور مشابه تعریف می‌شوند.

تعریف ۸.۱ برای یک حلقه R، جیکوبسن رادیکال R ($J(R)$)، به صورت اشتراک تمام ایدال های راست بیشین R تعریف می شود.

گزاره ۹.۱ یک عضو $x \in R$ معکوس پذیر چپ (معکوس پذیر) است اگر و تنها اگر $x + J(R)$ در $R/J(R)$ معکوس پذیر چپ(معکوس پذیر) باشد.

اثبات. کافیست حالت معکوس پذیری چپ را بررسی کنیم. قرار دهید $\bar{R} = R/J(R)$ و عناصر $\bar{R}$ را به $\bar{x}$ نشان دهید.

($\Leftarrow$) واضح است.

($\Rightarrow$) گیریم $y \in R$ به طوری که $\bar{y}\bar{x} = ۱$. آنگاه $yx - ۱ \in J(R)$، بنابراین

$$yx \in ۱ + J(R) \subseteq U(R).$$

این نتیجه می دهد که x یک معکوس چپ در R دارد. ■

۱—۳ حلقه های موضعی

قضیه ۱۰.۱ برای یک حلقه R، گزاره‌های زیر معادلند:

(۱) R یک ایدال بیشین چپ یکتا دارد.

(۲) R یک ایدال بیشین راست یکتا دارد.

(۳) $R/J(R)$ حلقه تقسیم است.

(۴) $R \setminus U(R)$ یک ایدآل در R است.

(۵) $R \setminus U(R)$ تحت جمع یک گروه است.

(۶) برای هر n، شرط $a_۱ + \cdots + a_n \in U(R)$ نتیجه می دهد که حداقل یک a_i در $U(R)$ است.

(۷) $a + b \in U(R)$ نتیجه می دهد که $a \in U(R)$ یا $b \in U(R)$.

اگر هر یک از این شرایط برقرار باشد گوییم R یک حلقه موضعی است. در این حالت بوضوح $m = J(R)$، یک ایدآل (راست) بیشین است. و به طور مختصر می گوییم (R, m) یک حلقه موضعی است.

اثبات. اگر بتوانیم (۳) $\Leftrightarrow$ (۱) را ثابت کنیم، آنگاه بنا به تقارن خواهیم داشت (۲) $\Leftrightarrow$ (۱).
(۱) $\Rightarrow$ (۳). هر ایدال بیشین چپ M از R شامل $J(R)$ است. اگر $R/J(R)$ یک حلقه تقسیم باشد، آنگاه بوضوح $M = J(R)$ و بنابراین (۱) بدست می آید.
(۳) $\Rightarrow$ (۱). (۱) نتیجه می دهد که $J(R)$ ایدال بیشین چپ یکتای R است. اما $R/J(R)$ تنها دو ایدال چپ دارد (یعنی (۰) و خودش)، بنابراین حلقه تقسیم است.
(۴) $\Rightarrow$ (۳). بنا به گزاره ۹.۱، (۳) نتیجه می دهد که هر $a \notin J(R)$ در R یکه است. بنابراین $R \setminus U(R) = J(R)$، که یک ایدال R است.
(۷) $\Rightarrow$ (٦) $\Rightarrow$ (۵) $\Rightarrow$ (۴) بدیهی اند.
(۳) $\Rightarrow$ (۷). فرض کنید $a \notin J(R)$. ایدال بیشین چپ M را به گونه ای در نظر می گیریم که $a \notin M$. آنگاه $M + Ra = R$، نتیجه می دهد که برای بعضی $m \in M$ و $b \in R$، $۱ = m + ba$. چون $m \notin U(R)$، (۷) نتیجه می دهد که $ba \in U(R)$. بویژه، $\bar{a}$ در $\bar{R} = R/J(R)$ معکوس چپ دارد. بنابراین $\bar{R} \setminus \{۰\}$ تحت ضرب گروه است و لذا $\bar{R}$ یک حلقه تقسیم است. ■

قضیه **۱۱.۱** هر حلقه R حداقل یک ایدال بیشین دارد.

اثبات. این یک کاربرد استاندارد لم زرن است. فرض کنید

$$\Sigma = \{I | I \subsetneqq R\}.$$

Σ را با شمول مرتب می کنیم. Σ ناتهی است، زیرا $۰ \in \Sigma$. برای به کار بردن لم زرن باید نشان دهیم که هر زنجیر در Σ دارای کران بالا در Σ است ؛ گیریم (I_α) یک زنجیر در Σ باشد، بنابراین برای هر زوج α و β یکی از شرایط زیر را داریم :

$$I_\alpha \subseteq I_\beta \text{ یا } I_\beta \subseteq I_\alpha.$$

فرض کنید $I = \bigcup_\alpha I_\alpha$. آنگاه I یک ایدال است و $۱ \notin I$ زیرا برای هر α، $۱ \notin I_\alpha$. بنابراین $I \in \Sigma$، و I یک کران بالای زنجیر است. بنابراین طبق لم زرن Σ یک عضو بیشین دارد. ■

نتیجه **۱۲.۱** اگر $I \neq (۱)$ یک ایدال R باشد، یک ایدال بیشین R شامل I وجود دارد.

اثبات. قضیه ۱۱.۱ را برای R/I به کار می بریم. ■

نتیجه ۱۳.۱ هر عضو غیر یکه R، در یک ایدال بیشین قرار دارد.

گزاره ۱۴.۱ $x \in J(R) \Leftrightarrow \forall y \in R : 1 - xy \in U(R)$.

اثبات. $(\Rightarrow)$. فرض کنید $1 - xy$ یکه نباشد. بنا به نتیجه ۱۳.۱، در یک ایدال بیشین M قرار می گیرد؛ اما $x \in J(R) \subseteq M$، بنابراین $xy \in M$ و لذا $1 \in M$، که تناقض است.
$(\Leftarrow)$. فرض کنید برای یک ایدال بیشین M از R، $x \notin M$. آنگاه $(1) = (x) + M$، بنابراین برای یک $u \in M$ و $y \in R$، داریم $u + xy = 1$. و لذا $1 - xy \in M$ و بنابراین یکه نیست. ■

لم ۱۵.۱ فرض $f : A \longrightarrow B$ یک همریختی حلقه ای پوشا باشد. در این صورت اگر $a \in J(A)$ آنگاه $f(a) \in J(B)$.

اثبات.

$$a \in J(A) \quad \Leftrightarrow \quad 1 - xa \in U(A); \quad \forall x \in A$$
$$\Rightarrow \quad f(1) - f(x)f(a) \in U(B); \quad \forall x \in A$$

چون $B = \{f(x) | x \in A\}$، اگر قرار دهیم $b = f(x)$، داریم

$$a \in J(A) \Rightarrow 1 - bf(a) \in U(B); \quad \forall b \in B$$

که معادل است با $f(a) \in J(B)$. ■

تعریف ۱۶.۱ حلقه R را ددکیند متناهی گویند، هرگاه شرط $ab = 1$ در R، نتیجه دهد $ba = 1$.

گزاره ۱۷.۱ فرض کنید R یک حلقه موضعی باشد. آنگاه :
(۱) R ددکیند متناهی است. (یعنی اگر $a \in R$ معکوس پذیر چپ باشد آنگاه $a \in U(R)$)
(۲) R خودتوان های نابدیهی ندارد.(تنها خودتوان های R، ۰ و ۱ می باشند.)

اثبات. (۱) اگر $a \in R$ معکوس چپ داشته باشد پس $a \notin J(R)$ و لذا a باید یکه باشد طبق ۱۳.۱
(۲) فرض کنید $e \in R$ یک خودتوان باشد و فرض $f = 1 - e$. از قضیه۱۰.۱(۷)، نتیجه می شود $e \in U(R)$ یا $f \in U(R)$. چون $ef = 0$، این نتیحه می دهد $e = 0$ یا $f = 0$. ■

گزاره ۱۸.۱ اگر $a \in J(R)$ و $b \in U(R)$، آنگاه $b - a \in U(R)$.

اثبات. قرار می دهیم $t = b - a$. باید نشان دهیم که $t \in U(R)$. یعنی، برای یک $y \in R$، $ty = ۱$.

$$t = b - a \Rightarrow t + a = b \overset{b\in U(R)}{\Rightarrow} \exists z \in R \ : \ (t+a)z = ۱$$
$$\Rightarrow \quad tz + az = ۱$$
$$\Rightarrow \quad tz = ۱ - az.$$

از طرفی طبق ۱۴.۱، $۱ - az \in U(R)$. بنابراین $tz \in U(R)$، آنگاه :

$$\exists p \in R \ : \ (tz)p = ۱ \Rightarrow t(zp) = ۱.$$

قرار می دهیم $zp = q \in R$. پس $tq = ۱$. یعنی، $t = b - a \in U(R)$. ■

۱—۴ حلقه سریهای توانی صوری

گزاره ۱۹.۱ اگر $f : R \longrightarrow S$ یک همریختی حلقه ای باشد و J ایدالی در S باشد، آنگاه $J^c := f^{-۱}(S)$ که انقباض J نامیده می شود ایدالی در R است.

اثبات. واضح است. ■

تعریف ۲۰.۱ اگر R یک حلقه باشد، $R[[x]]$ حلقه سری های توانی صوری نامیده می شود و به صورت $R[[x]] = \{\sum_{i=۰}^{\infty} a_i x^i | a_i \in R\}$ تعریف می شود.

گزاره ۲۱.۱ فرض کنید $f(x) = a_۰ + a_۱x + \cdots \in R[[x]]$. آنگاه

(الف) $f \in J(R[[x]]) \Leftrightarrow a_۰ \in J(R)$.

(ب) f در $R[[x]]$ یکه است $\Leftrightarrow a_۰$ در R یکه باشد.

(ج) انقباض یک ایدآل بیشین m از $R[[x]]$، یک ایدآل بیشین در R است، و $m = m^c + (x)$.

اثبات. (الف)($\Rightarrow$). بنا به گزاره ۱۴.۱،

$$f \in J(R[[x]]) \Leftrightarrow \forall g \in R[[x]] \ : \ \text{یکه باشد } ۱ - fg$$

فرض کنید $a \in R$ دلخواه باشد و $g = a$. آنگاه

$$۱ - fa = ۱ - (a_\circ a + a_۱ ax + \cdots) = (۱ - a_\circ a) + (-a_۱ a)x + \cdots$$

برای هر $a \in R$، $۱ - a_\circ a$ یکه است و بنابراین $a_\circ \in J(R)$.

$(\Leftarrow)$.

$$a_\circ \in J(R) \Leftrightarrow \forall a \in R \ : \ ۱ - a_\circ a \text{ یکه باشد}$$

$$\forall g \in R[[x]] \ : \ ۱ - fg = (۱ - a_\circ b_\circ) - (a_۱ b_\circ + a_\circ b_۱)x + \cdots$$

$$\Rightarrow \ ۱ - fg \text{ یکه است} \Rightarrow f \in J(R[[x]]).$$

هرگاه $g(x) = b_\circ + b_۱ x + \cdots$.

(ب) $(\Rightarrow)$. فرض کنید $f \in R[[x]]$ یکه باشد، بنابراین $g(x) = b_\circ + b_۱ x + \cdots$ در $R[[x]]$ موجود است، به طوری که

$$fg = ۱ \Rightarrow [a_\circ b_\circ + (a_\circ b_۱ + a_۱ b_\circ)x + \cdots] = ۱ \Rightarrow a_\circ b_\circ = ۱ \Rightarrow \ a_\circ \text{ یکه است}.$$

$(\Leftarrow)$. باید نشان دهیم که $g(x) = b_\circ + b_۱ x + \cdots$ در $R[[x]]$ وجود دارد به طوری که

$$fg = ۱ \Leftrightarrow \begin{cases} a_\circ b_\circ = ۱ \qquad , b_\circ := a_\circ^{-۱} \\ a_\circ b_۱ + a_۱ b_\circ = \circ \Rightarrow a_۱ a_\circ^{-۱} + b_۱ b_\circ^{-۱} = \circ \Rightarrow b_۱ := a_۱ a_\circ^{-۱} b_\circ^{-۱} = a_۱ \\ \vdots \end{cases}$$

به این ترتیب تمام ضرایب g مشخص می شود.

(ج). می دانیم که $R[[x]] = R \oplus (x)$ و $f^{-۱}(m) = m^c = R \cap m$، به عنوان $R-$ مدول ها. ثابت می کنیم $(x) \subseteq m$:

برهان خلف : فرض $(x) \not\subseteq m$. چون m بیشین است داریم $R[[x]] = (x) + m$، و لذا

$$\begin{aligned} \exists f_\circ \in R[[x]] \ : \ ۱ = xf_\circ + g_\circ \quad &\Rightarrow \quad ۱ = b_\circ + (a_\circ + b_۱)x + \cdots \\ &\Rightarrow \quad b_\circ = ۱ \\ &\Rightarrow \quad g_\circ \text{ یکه است} \\ &\Rightarrow \quad m = R[[x]]. \end{aligned}$$

که متناقض با بیشین بودن m است. هرگاه $f_\circ(x) = a_\circ + a_\backslash x + \cdots$ و $g_\circ(x) = b_\circ + b_\backslash x + \cdots$.
بنابراین

$$m = R[[x]] \cap m = (R \oplus (x)) \cap m = (R \cap m) \oplus (x) = m^c \oplus (x).$$

حال نشان می دهیم m^c در R بیشین است. فرض می کنیم چنین نباشد، پس ایدآل سره I در R موجود است که $m^c \subseteq I$. در نتیجه $m = m^c + (x) \subset I + (x)$. چون m یک ایدآل بیشین در $R[[x]]$ است ، پس باید

$$\begin{aligned} I + (x) = R[[x]] \;\; &\Rightarrow \;\; \exists b \in I, f \in (x) \;:\; 1 = b + xf = b + a_\circ x + a_1 x^2 + \cdots \\ &\Rightarrow \;\; b = 1 \\ &\Rightarrow \;\; I = R. \end{aligned}$$

که متناقض با فرض است. ■

۱–۵ حلقه اعداد صحیح $p-adic$

فرض کنید

$$(\mathbb{Z}, p) = \{\{x_n\}_{n=\circ}^{\infty} | x_n \in \mathbb{Z}, x_n \overset{p^n}{\equiv} x_{n-1}\}$$

رابطه زیر را روی $(\mathbb{Z}, p)$ تعریف می کنیم (برای سادگی x_n را به جای $\{x_n\}_{n=\circ}^{\infty}$ می‌نویسیم)

$$x_n \sim y_n \Leftrightarrow x_n \overset{p^{n+1}}{\equiv} y_n, \;\; \forall n \geq \circ$$

واضح است که اگر $x_n' \sim y_n'$ آن گاه $(x_n + x_n') \sim (y_n + y_n')$ و $x_n y_n \sim x_n' y_n'$.

تعریف ۲۲.۱ حلقه $\hat{\mathbb{Z}}_p$ متشکل از تمام کلاس‌های هم‌ارزی روی $(\mathbb{Z}, p)$ را با عمل

$$[x_n] + [y_n] = [x_n + y_n] \quad \text{و} \quad [x_n][y_n] = [x_n y_n]$$

را حلقه اعداد صحیح $p-adic$ گویند.

لم ۲۳.۱ (الف) اگر دو دنباله x_n و y_n در $(\mathbb{Z}, p)$ در t جمله اول اختلاف داشته باشند آن گاه $[x_n] = [y_n]$.