سری گروه‌ها

تعریف یک سری نرمال (زیرنرمال یا) از گروه G دنباله‌ای متناهی از زیرگروه‌های $H_0, H_1, H_2, \dots, H_n$ از G است طوری که $H_i \trianglelefteq H_{i+1}$ و $H_0 = \{e\}$ ، $H_n = G$ به عبارت دیگر

$$\{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_{n-1} \trianglelefteq G$$

و یک سری نرمال (یا) از گروه G عبارت است از دنباله‌ای متناهی از زیرگروه‌های نرمال $H_0, H_1, H_2, \dots, H_n$ از G طوری که $H_i \leq H_{i+1}$ و $H_0 = \{e\}$ ، $H_n = G$ به عبارت دیگر

$$\{e\} \trianglelefteq H_1 \leq H_2 \leq \dots \leq H_{n-1} \trianglelefteq G$$

مثال ۱: $\{0\} \lhd 9\mathbb{Z} \lhd 3\mathbb{Z}$ و $\{0\} \lhd 8\mathbb{Z} \lhd 4\mathbb{Z} \lhd 2\mathbb{Z} \lhd \mathbb{Z}$ دو سری نرمال از $\mathbb{Z}$ هستند

توجه: چون هر سری نرمال از یک گروه G یک سری زیرنرمال است پس در مثال ۱ این دو سری زیرنرمال هم در $\mathbb{Z}$ هستند

مثال ۲: $D_4 \geq \{e, \rho_2, \mu_1, \mu_2\} \geq \{e, \rho_2, e, \rho_2\} \geq \{e, \rho_2\} \geq \{e\}$ یک سری زیرنرمال در D_4 است

زیرا $\{e, \rho_2\}$ زیرگروه D_4 است ولی زیرگروه نرمال در D_4 نیست.

همچنین $D_4 \geq \{e, \rho_2, \sigma_1, \sigma_2\} \geq \{e, \rho_2, e, \rho_2\} \geq \{e, \rho_2\} \geq \{e\}$ یک سری زیرنرمال در D_4 است.

همچنین $D_4 \geq \{e, \rho_2, \rho_1, \rho_3\} \geq \{e, \rho_2\} \geq \{e\}$ یک سری زیرنرمال در D_4 است.

تعریف: سری زیرنرمال (نرمال) $\{K_i\}$ یک تظریف سری زیرنرمال (نرمال) $\{H_i\}$ از گروه G است در صورتیکه $H_i \leq K_i$ و به عبارت دیگر هر H_i یکی از K_iها باشد

مثال ۳: سری $\mathbb{Z} \rhd 2\mathbb{Z} \rhd 4\mathbb{Z} \rhd 8\mathbb{Z} \rhd 24\mathbb{Z} \rhd 72\mathbb{Z} \rhd \{0\}$ یک تظریف از سری

$\mathbb{Z} \rhd 2\mathbb{Z} \rhd 8\mathbb{Z} \rhd 24\mathbb{Z} \rhd 72\mathbb{Z} \rhd \{0\}$ است

تعریف: دو سری زیرنرمال (نرمال) $\{H_i\}$ و $\{K_j\}$ از گروه G ایزومورف (یکریخت) نامیم در صورتیکه یک تناظر یک به یک بین گروه‌های خارج قسمتی H_{i+1}/H_i و K_{j+1}/K_j وجود داشته باشد طوری که گروه‌های خارج قسمتی متناظر با هم ایزومورف باشند

توجه: بدیهی است که تعداد گروه‌های دو سری زیرنرمال (نرمال) ایزومورف باید با هم برابر باشد.

مثال ۱۴: در سری $\{0\} \lhd \langle 5 \rangle \lhd \langle 3 \rangle \lhd \langle 15 \rangle \lhd Z_{15}$ و $\{0\} \lhd \langle 5 \rangle \lhd \langle 3 \rangle \lhd \langle 15 \rangle \lhd Z_{15}$ از Z_{15} با هم ایزومورف هستند.

زیرا $\frac{\langle 5 \rangle}{\{0\}} \cong Z_3$ ، $\frac{Z_{15}}{\langle 5 \rangle} \cong Z_5$ ، $\frac{\langle 3 \rangle}{\{0\}} \cong Z_5$ ، $\frac{Z_{15}}{\langle 3 \rangle} \cong Z_3$

بنابراین $\frac{\langle 5 \rangle}{\{0\}} \cong \frac{Z_{15}}{\langle 3 \rangle}$ و $\frac{\langle 3 \rangle}{\{0\}} \cong \frac{Z_{15}}{\langle 5 \rangle}$

قضیه (شرایط) هر دو سری زیر نرمال (نرمال) از گروه G دارای تظریف های ایزومورف هستند

مثال ۵: تظریف های ایزومورف $\{0\} \lhd \langle 7 \rangle \lhd \langle 7^2 \rangle \lhd \langle 7^3 \rangle \lhd Z_{7^4}$ و $\{0\} \lhd \langle 7^2 \rangle \lhd \langle 7 \rangle \lhd Z_{7^4}$ را بیابید. حل: در مثال ۳ دیدیم که سری ① $\{0\} \lhd \langle 7^4 \rangle \lhd \langle 7^3 \rangle \lhd \langle 7^2 \rangle \lhd \langle 7 \rangle \lhd Z_{7^4}$ تظریف سری $\{0\} \lhd \langle 7^4 \rangle \lhd \langle 7^3 \rangle \lhd \langle 7^2 \rangle \lhd Z_{7^4}$ است. سری ② $\{0\} \lhd \langle 7^4 \rangle \lhd \langle 7^2 \rangle \lhd \langle 7 \rangle \lhd Z_{7^4}$ یک تظریف سری $\{0\} \lhd \langle 7^2 \rangle \lhd \langle 7 \rangle \lhd Z_{7^4}$ است.

دو سری ① و ② با هم ایزومورف هستند زیرا

$$\frac{\langle 7^2 \rangle}{\{0\}} \overset{①}{\cong} \langle 7^2 \rangle \overset{②}{\cong} \frac{\langle 7^3 \rangle}{\{0\}}$$

$$\frac{\langle 7^3 \rangle}{\langle 7^4 \rangle} \overset{①}{\cong} Z_7 \overset{②}{\cong} \frac{\langle 7 \rangle}{\langle 7^2 \rangle} \quad , \quad \frac{\langle 7 \rangle}{\langle 7^2 \rangle} \overset{①}{\cong} Z_7 \overset{②}{\cong} \frac{\langle 7^2 \rangle}{\langle 7^3 \rangle}$$

تعریف: گروه G را ساده نامیم هرگاه هیچ زیرگروه نرمال واقعی و ناپدیهی نداشته باشد به عبارت دیگر گروه G بجز خود G و $\{e\}$ زیرگروه نرمال دیگری نداشته باشد

مثال ۶: اگر p عددی اول باشد Z_p یک گروه ساده است.

قضیه ۱: گروه متناوب A_n برای $n \geq 5$ ساده است.

تعریف: زیرگروه نرمال M از گروه G را یک زیرگروه نرمال ماکسیمال نامیم هرگاه $M \neq G$ و G زیرگروه نرمال واقعی ما نند N نداشته باشد که شامل M باشد به عبارت دیگر اگر $M \leq N \lhd G$ آنگاه $N = G$ یا $N = M$.

مثال ۷: $2Z$ ، $3Z$ ، $5Z$ و $7Z$ زیرگروه های نرمال ماکسیمال Z هستند زیرا هیچ زیرگروه نرمال ما نند N از Z وجود ندارد که $7Z < N < Z$ و یا $3Z$ ، $5Z$ ، $7Z$ هم به همین صورت.

البته طبق قضیه زیر این مثال بدیهی است

قضیه ۲: M زیرگروه نرمال ماکسیمال گروه G است اگر و فقط اگر G/M ساده باشد

اثبات: فرض کنید که M زیرگروه نرمال ماکسیمال G است. همومورفیسم طبیعی $\sigma : G \longrightarrow G/M$ با ضابطه $\sigma(a) = aM$ موجود است که $\sigma(a) = aM$. حال اگر $N \lhd G/M$ باشد آنگاه $\sigma^{-1}(N) \lhd G$ و $M \leq \sigma^{-1}(N)$

چون M زیرگروه نرمال ماکسیمال G است پس $\bar{\sigma}(N)=G$ یا $\bar{\sigma}(M)=M$ که در این صورت $N=G$ یا $N=M$ یعنی $\frac{G}{M}$ ساده است.

برعکس اگر $\frac{G}{M}$ ساده باشد و T زیرگروه نرمال G باشد که $M \subset T$ در این صورت چون $\bar{\sigma}: G \to \frac{G}{M}$ یک همومورفیسم پوشا است پس $\bar{\sigma}(T) \trianglelefteq \frac{G}{M}$ حال اگر $T \neq G$ باشد آنگاه $\bar{\sigma}(T) \neq \frac{G}{M}$ و $\bar{\sigma}(T) \neq \{M\}$ حال چون $\frac{G}{M}$ ساده است چنین T وجود ندارد که $\bar{\sigma}(T) \trianglelefteq \frac{G}{M}$ باشد.

تعریف: سری زیرنرمال $\{H_i\}$ از گروه G را یک سری ترکیبی نامیم هرگاه گروههای خارج قسمتی $\frac{H_{i+1}}{H_i}$ ساده باشند.
سری نرمالی مانند $\{H_i\}$ از گروه G را یک سری اصلی (عمده) نامیم در صورتیکه گروههای خارج قسمتی $\frac{H_{i+1}}{H_i}$ ساده باشند.

توجه: در گروههای آبلی چون هر زیرگروه نرمال است پس مفاهیم سری ترکیبی و سری عمده (اصلی) یکی هستند.
همچنین چون هر سری نرمال یک سری زیرنرمال هم هست پس اعم از اینکه یک گروه آبلی باشد یا آبلی نباشد هر سری اصلی آن یک سری ترکیبی هم هست.

مثال ۸: گروه جمعی $\mathbb{Z}$ هیچ سری ترکیبی (و بنابر هیچ سری اصلی) ندارد زیرا اگر سری $\{H_i\}$ یعنی

$$\{0\}=H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{n-1} \lhd H_n=\mathbb{Z}$$

یک سری زیرنرمال باشد چون هر زیرگروه $\mathbb{Z}$ به صورت $n\mathbb{Z}$ است پس $\frac{H_1}{H_0} \cong n\mathbb{Z}$ که خود یک گروه دوری نامتناهی است و بنابراین زیرگروه نرمال نامتناهی دارد (مثلاً $2n\mathbb{Z}$) پس گروه ساده نیست.
پس گروه $\mathbb{Z}$ هیچ سری ترکیبی (و بنابر سری اصلی) ندارد.

مثال ۹: برای هر $n \geq 5$ سری $\{e\} \lhd A_n \lhd S_n$ یک سری ترکیبی (و بنابر یک سری اصلی) از S_n است زیرا $\frac{A_n}{\{e\}} \cong A_n$ گروه ساده است و بنابر $\frac{S_n}{A_n} \cong Z_2$ که ساده است

مثال ۱۰: در مثال ۴ دیدیم دوسری $\mathbb{Z}_{15} \lhd \langle \bar{5} \rangle \lhd \{\bar{0}\}$ و $\mathbb{Z}_8 \lhd \langle \bar{2} \rangle \lhd \langle \bar{4} \rangle \lhd \{\bar{0}\}$ از دو سری هستند این دو سری هم سری ترکیبی (سری اصلی) هستند

نتیجه: دیدیم که در یک سری زیرنرمال چون $\{H_i\}$ از گروه G اگر $\frac{H_{i+1}}{H_i}$ گروه ساده باشد آنگاه H_i زیر گروه نرمال ماکسیمال H_{i+1} است بنابراین برای ساختن یک سری ترکیبی هر H_i باید زیرگروه نرمال ماکسیمال H_{i+1} باشد پس برای ساختن یک سری ترکیبی از گروه G، ابتدا باید زیرگروه نرمال ماکسیمال H_{n-1} ی

H_{n-1} از G می‌گردیم سپس زیرگروه نرمال ماکسیمالی برای H_{n-1} را پیدا می‌کنیم. اگر این فرایند طی تعداد متناهی مرحله پایان یابد به آنگاه یک سری ترکیبی از گروه G را بدست آورده‌ایم. طبق قضیه ۳ یک سری ترکیبی نمی‌تواند تظریفی غیر خودش داشته باشد. برای متکامل یک سری اصلی، ابتدا یک زیرگروه نرمال ماکسیمال چون H_{n-1} از G را می‌یابیم، سپس زیرگروه نرمال ماکسیمالی برای H_{n-1} پیدا می‌کنیم که زیرگروه نرمال G باشد و این روند را ادامه می‌دهیم اگر این روند طی تعداد متناهی مرحله پایان پذیرد آنگاه یک سری اصلی را برای گروه G پیدا کرده‌ایم.

قضیه ۴ (زوردان - هولدر) هر دو سری ترکیبی (اصلی) از یک گروه G ایزومورف هستند.

اثبات: فرض کنید $\{H_i\}$ و $\{K_j\}$ دو سری ترکیبی (اصلی) از G باشند. بنابراین طبق قضیه مشابه این دو سری دو تظریف ایزومورف دارند. حال چون تمام گروه‌های خارج قسمت خود ساده هستند پس طبق قضیه ۳ هر دو سری بدست آمده تظریفی جز خود ندارند. بنابراین $\{H_i\}$ و $\{K_j\}$ خود باید ایزومورف باشند.

قضیه ۵: اگر G یک سری ترکیبی (اصلی) داشته باشد و N یک زیرگروه واقعی (محض) نرمال از G باشد آنگاه یک سری ترکیبی (اصلی) شامل N هم وجود دارد.

اثبات: سری $G \rhd N \rhd \{e\}$ هم زیرنرمال است و هم نرمال، چون G دارای یک سری ترکیبی ما شد $\{H_i\}$ است بنابراین طبق قضیه مشابه این تظریفی از $G \rhd N \rhd \{e\}$ به صورت یک سری زیرنرمال وجود دارد که با تظریفی از $\{H_i\}$ ایزومورف است. ولی به عنوان یک سری ترکیبی، $\{H_i\}$ تظریفی جز خودش نمی‌تواند داشته باشد بنابراین $G \rhd N \rhd \{e\}$ تظریفی با یک سری زیرنرمال دارد که تمام گروه‌های خارج قسمت آن ساده هستند، یعنی این تظریف یک سری ترکیبی است. اگر به جای $\{H_i\}$ با یک سری اصلی $\{K_j\}$ از G آغاز کنیم، استدلال مشابه برقرار خواهد بود.

مثال ۱۱: یک سری ترکیبی (و نیز یک سری اصلی) از $H = \langle (0\,1)(2\,3),\ (0\,2)(1\,3) \rangle$ که شامل $Z_4 \times Z_2$ باشد عبارت است از

$$Z_4 \times Z_2 = \langle \overline{1} \rangle \times \langle \overline{1} \rangle \rhd \langle \overline{2} \rangle \times \langle \overline{1} \rangle \rhd \langle (0,2) \rangle \rhd \langle (0,1)(2,3) \rangle \rhd \{(0,0)\}$$

تعریف: گروه G را حل‌پذیر نامیم اگر یک سری ترکیبی مانند $\{H_i\}$ داشته باشد طوری که تمام گروه‌های خارج قسمت H_{i+1}/H_i آبلی باشند.

توجه: با توجه به قضیه زوردان - هولدر، ملاحظه می‌کنیم که برای یک گروه حل‌پذیر در هر سری ترکیبی $\{H_i\}$، تمام گروه‌های خارج قسمت H_{i+1}/H_i باید آبلی باشند.

مثال ۱۲: گروه S_4 حل‌پذیر است زیرا سری ترکیبی $S_4 \rhd A_4 \rhd \{e\}$ دارای گروه‌های خارج قسمتی ایزومورف با Z_2 و Z_3 دارد که هر دو آبلی هستند.

A

مثال ۱۳: گروه S_5 حل پذیر نیست چون A_5 ساده است سری $\{e\} \lhd A_5 \lhd S_5$ یک سری نرمالی است و $A_5/\{e\} \cong A_5$ آبلی نیست. ولی S_4 و S_3 و S_2 حل پذیر هستند

توجه: گروه A_5 که مرتبه آن ۶۰ است کوچکترین گروهی است که حل ناپذیر است. این واقعیت بستگی تردیکی دارد به این که بطور کلی معادلات چند جمله‌ای درجه ۵ توسط رادیکالها حلشان پذیر است. اما معادلات چند جمله‌ای از درجات کوچکتر یا مساوی ۴ حل پذیرند

قضیه ۹ مرکز هر گروه زیر گروه نرمالی از آن گروه است

اثبات: دیدیم که مرکز گروه G عبارت است از $Z(G) = \{x \in G \mid ax = xa \ \forall a \in G\}$.

$Z(G)$ ناتهی است زیرا $e \in Z(G)$ چون $ea = ae = a$ ، $\forall a \in G$

$\forall a \in G \Rightarrow y^{-1}a = ay^{-1}$ ، $ya = ay$ ، $xa = ax$ ، $\forall x, y \in Z(G)$

پس $(xy^{-1})a = a(xy^{-1})$ زیرا $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = a(xy^{-1})$

یعنی $xy^{-1} \in Z(G)$ پس $Z(G) \leq G$. برای نرمال بودن

$\forall x \in Z(G), \forall g \in G) : gxg^{-1} \in Z(G)$

$gxg^{-1} = xgg^{-1} = x \in Z(G)$ با فرض $a = g$ $\forall a \in G$ $xa = ax$

توجه: اگر جمله مثالهای G در دست باشد، پیدا کردن مرکز آن ساده خواهد بود زیرا: $a \in Z(G)$ اگر و فقط اگر اعضای که در سطر مربوط به a قرار دارد دقیقاً به همان ترتیبی باشد که اعضای ستون مربوط به a.

توجه: فرض کنید که G یک گروه باشد پس $Z(G) \trianglelefteq G$ حال $G/Z(G)$ یک گروه خارج قسمتی است و مرکز آن یعنی $Z\left(G/Z(G)\right)$ را پیدا می‌کنیم چون $Z\left(G/Z(G)\right)$ در $G/Z(G)$ نرمال است. اگر $\gamma : G \longrightarrow G/Z(G)$ نگاشت طبیعی باشد آنگاه طبق قضیه‌ای $\gamma^{-1}\left[Z(G/Z(G))\right] = Z_1(G)$ زیر گروه نرمال از G است که آنگاه می‌گیریم گروه خارج قسمتی $G/Z_1(G)$ و مرکز آن را تشکیل می‌دهیم و اگر γ_1 برای $Z_2(G)$ استفاده می‌کنیم و $\gamma_1 : G \longrightarrow G/Z_1(G)$.

ولین روند را ادامه می دهیم.

تعریف: سری $\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$ را سری مرکزی فضایی گروه G می نامیم.

مثال ۱۴: $Z(S_3) = \{e\}$ بنابراین سری مرکزی فضایی گروه S_3 عبارت است از

$$\{e\} \leq \{e\} \leq \{e\} \leq \cdots$$

مثال ۱۵: مرکز D_4 عبارت است از $\{e, \rho_2\}$ حالتهای $G/\{e, \rho_2\}$ گروه از مرتبه ۴ است بنابراین آبلی است پس مرکز آن تمام $G/\{e, \rho_2\}$ است پس سری مرکزی فضایی D_4 عبارت است از

$$\{e\} \leq \{e, \rho_2\} \leq D_4 \leq D_4 \leq \cdots$$

تمرین:

۱- تظیرهای ایزومورف دوسری نرمال $\mathbb{Z}_7 \times \mathbb{Z}_{20} \times \mathbb{Z}_{50} \times \{0\}$ و $\mathbb{Z}_7 \times \mathbb{Z}_{49} \times \mathbb{Z}_{245} \times \{0\}$ از $\mathbb{Z}$ را پیدا کنید.

۲- تمام سریهای ترکیبی گروه Z_{40} را پیدا کنید و نشان دهید که در واقع همه با هم ایزومورف هستند.

۳- تمام سریهای ترکیبی $Z_5 \times Z_5$ را پیدا کنید.

۴- تمام سریهای ترکیبی $S_4 \times Z_2$ را پیدا کنید.

۵- یک سری ترکیبی برای $S_3 \times S_3$ پیدا کنید. آیا $S_3 \times S_3$ حل پذیر است؟

۶- مرکز گروه $S_4 \times Z_4$ را پیدا کنید.

تعریف: یک سری نرمال $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$ برای گروه G را یک سری مرکزی برای گروه G می نامیم اگر برای هر i که $0 \leq i \leq n$ گروه خارج قسمتی G_{i+1}/G_i در مرکز G/G_i قرار داشته باشد یعنی $G_{i+1}/G_i \leq Z(G/G_i)$.

تعریف: گروه G را پوچتوان نامیم هرگاه دارای یک سری مرکزی باشد.

تعریف: فرض کنید که G یک گروه و p عددی اول باشد. G را یک p-گروه نامیم هرگاه هر عضو از G مرتبه p^i داشته باشد یعنی $\forall g \in G \; o(g) = p^i$

قضیه ۱: گروه متناهی G یک p-گروه است $\iff$ $|G|$ توانی از p باشد.

قضیه ۲: اگر p عددی اول باشد، آنگاه هر p-گروه متناهی پوچتوان است.

مثال: S_3 گروه پوچتوان نیست زیرا p گروه نیست (زیرا $|S_3|=6$ توانی از یک عدد اول مانند p نیست)

مثال: گروه D_4 یک گروه پوچتوان است زیرا یک ۲ گروه است چون $|D_4|=8=2^3$. $p=2$

قضیه ۳: هر p گروه حل پذیر است.

مثال: گروه D_4 طبق قضیه قبل حل پذیر است.

قضیه ۴: اگر G یک p گروه باشد آنگاه $Z(G)\neq\{e\}$.

قضیه ۵: اگر p عددی اول باشد آنگاه هر گروه G از مرتبه p^2 آبلی است.

قضیه ۶: هر گروه پوچتوان حل پذیر است.

توضیح: عکس قضیه ۶ برقرار نیست زیرا S_3 و S_4 حل پذیر است ولی پوچتوان نیستند.

مثال: $\mathbb{Z}_2$ و $\mathbb{Z}_3$ و $\mathbb{Z}_4$ و $\mathbb{Z}_9$ و $\mathbb{Z}_8$ و D_4 و $\mathbb{Z}_{16}$ و $\mathbb{Z}_{27}$ و ... همگی p گروه هستند.
زیرا $p=2$ و $p=3$

تمرین

۱- قضیه ۵ را ثابت کنید.

۲- نشان دهید که عکس قضیه ۲ برقرار نیست (مثال نقض معرفی کنید).

۳- نشان دهید اگر p و q دو عدد اول متمایز باشند آنگاه هر گروهی از مرتبه pq ساده نیست.

۴- مرکز گروه D_4 را بدست آورید (از روی جدول گروه مشابه G).

Scanned with CamScanner

عمل گروه روی یک مجموعه

تعریف: فرض کنید که G یک گروه و X یک مجموعهٔ غیرتهی باشد. گوییم که G روی X عمل می‌کند، اگر یک تابع $f: G \times X \longrightarrow X$ موجود باشد بطوریکه $f(g,x) = gx$ یا $f(g,x) \in X$ یا gx را با $f(g,x)$ نمایش می‌دهیم و این تابع در شرط زیر صدق کند:

۱) $\forall a,b \in G \ , \ \forall x \in X \quad (ab)x = a(bx)$

۲) $ex = x$: اگر e عضو خنثی گروه G باشد آنگاه

به عبارت دیگر تحت شرایط بالا G از سمت چپ روی مجموعه X عمل می‌کند. با همین خصوصیات می‌توان عمل راست G روی X را تعریف کرد.

$$f: X \times G \longrightarrow X$$
$$f(x,g) = xg$$
$$\forall a,b \in G, \forall x \in X$$
$$x(ab) = (xa)b \quad , \quad xe = x$$

قرارداد: از این پس هرگاه صحبت از عمل یک گروه روی یک مجموعه می‌شود (در این مبحث) منظور عمل چپ است.

مثال ۱: فرض کنید که $\{1,2,3,\dots,n\} = X$ و $G = S_n$. یک عمل از گروه S_n روی مجموعه X عبارت است از $f: S_n \times X \longrightarrow X$. بدیهی است که $f(\sigma, x) = \sigma(x)$ و $\forall \sigma \in S_n \ \forall x \in X$

$$\forall x \in X : \sigma\rho(x) = \sigma(\rho(x)) \ , \ e(x) = x \quad \forall \sigma, \rho \in S_n$$

مثال ۲: می‌توان مثال ۱ را کلیتر در نظر گرفت. X یک مجموعهٔ ناتهی و $G = S_X$. در این صورت S_X روی X عمل می‌کند. در این مثال و مثال قبل $\sigma(\rho(x)) = \sigma\rho(x)$ همان ترکیب توابع است.

این عمل را عمل طبیعی گروه S_X روی مجموعه X می‌نامیم.

قرارداد: در تعریف بالا X یک G-مجموعه نامیده می‌شود.

مثال ۳: فرض کنید که G یک گروه باشد و $H \leq G$. تحت ضرب چپ G بر یک H-مجموعه می‌باشد. به عبارت دیگر

$$f: H \times G \longrightarrow G$$
$$f(h,g) = hg$$

زیرا $\forall h_1, h_2 \in H, \forall g \in G : (h_1h_2)g = h_1(h_2g)$

$\forall g \in G : eg \in G$

مثال ۴: فرض کنید که G یک گروه و $H \leq G$. تحت مزدوج‌گیری G یک H-مجموعه می‌باشد. به عبارت دیگر

$$f: H \times G \longrightarrow G$$
$$f(h,g) = hgh^{-1}$$

زیرا $\forall h \in H, \forall g \in G$.

$$\forall h_1,h_2 \in H, \forall g \in G$$
$$f(h_1h_2, g) = (h_1h_2)g(h_1h_2)^{-1} = (h_1h_2)g(h_2^{-1}h_1^{-1}) = h_1(h_2gh_2^{-1})h_1^{-1} = f(h_1, f(h_2,g))$$
$$f(e,g) = ege^{-1} = g$$

توجه: در این مثال به جای hg از عبارت hgh^{-1} برای $f(h,g)$ استفاده کرده‌ایم.

تعریف: عمل به کار گرفته شده در مثال ۴ عمل $h \in H$ روی G را مزدوجی با h می‌گوییم و عنصر hxh^{-1} را مزدوج x می‌نامیم که در آن $x \in G$ دلخواه است.

توجه: در مثال قبل اگر K زیرگروه دلخواهی از G غیر از H باشد و hKh^{-1} آنگاه h زیرگروهی از G است؟ و یا K است؟ از این H روی مجموعه S متشکل از تمام زیرگروه‌های G به چند جزء؟

جواب: $f(h,K)=hKh^{-1}$ عمل می‌کند. گروه hKh^{-1} مزدوج K می‌نامند.

مثال ۵ - فرض کنید که G یک گروه و $H \leq G$ و L مجموعه تمام همدسته‌های چپ K در G باشد که $K \leq G$ و $L=\{aK \mid a \in G\}$ در این صورت اگر

$f: H \times L \longrightarrow L$

$f(h, aK) = h(aK)$

$\forall h_1, h_2 \in H, \forall aK \in L$

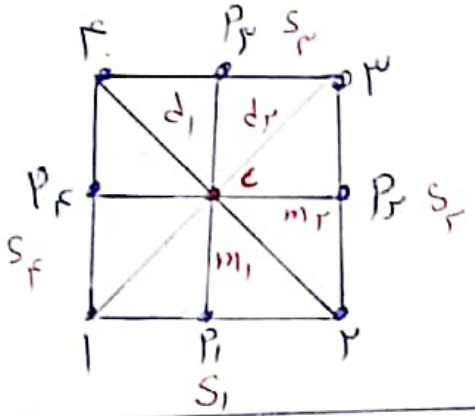
$(h_1 h_2)(aK) = h_1(h_2(aK))$ و $e(aK) = aK$

آنگاه L یک H - مجموعه است زیرا

مثال ۶: فرض کنید که $G = D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, m_1, m_2, d_1, d_2\}$ و

$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, c\}$ و P_1, P_2, P_3, P_4

که در آن اعداد ۱ و ۲ و ۳ و ۴ راس مربع و s_1 و s_2 و s_3 و s_4 ضلع‌های مربع و d_1 و d_2 قطرهای مربع و c مرکز مربع (محل برخورد قطرها) و P_1 و P_2 و P_3 و P_4 وسط ضلع‌های مربع می‌باشند. شکل زیر



و m_1 و m_2 محورهای افقی و عمودی مربع هستند.

در این صورت X یک D_4 - مجموعه است و عمل D_4 روی مجموعه X به صورت جدول زیر است.

	۱ ۲ ۳ ۴	s_1 s_2 s_3 s_4	m_1 m_2 d_1 d_2 c	P_1 P_2 P_3 P_4
ρ_0	۱ ۲ ۳ ۴	s_1 s_2 s_3 s_4	m_1 m_2 d_1 d_2 c	P_1 P_2 P_3 P_4
ρ_1	۲ ۳ ۴ ۱	s_2 s_3 s_4 s_1	m_2 m_1 d_2 d_1 c	P_2 P_3 P_4 P_1
ρ_2	۳ ۴ ۱ ۲	s_3 s_4 s_1 s_2	m_1 m_2 d_1 d_2 c	P_3 P_4 P_1 P_2
ρ_3	۴ ۱ ۲ ۳	s_4 s_1 s_2 s_3	m_2 m_1 d_2 d_1 c	P_4 P_1 P_2 P_3
m_1	۲ ۱ ۴ ۳	s_1 s_4 s_3 s_2	m_1 m_2 d_2 d_1 c	P_1 P_4 P_3 P_2
m_2	۴ ۳ ۲ ۱	s_3 s_2 s_1 s_4	m_1 m_2 d_2 d_1 c	P_3 P_2 P_1 P_4
δ_1	۳ ۲ ۱ ۴	s_2 s_1 s_4 s_3	m_2 m_1 d_1 d_2 c	P_2 P_1 P_4 P_3
δ_2	۱ ۴ ۳ ۲	s_4 s_3 s_2 s_1	m_2 m_1 d_1 d_2 c	P_4 P_3 P_2 P_1

قضیه ۱: فرض کنید که X یک G مجموعه باشد (یعنی G روی X عمل می‌کند)

الف) برای هر x از X مجموعه $G_x = \{g \in G \mid gx = x\}$ زیرگروه G است.

ب) برای هر x_1 و x_2 از X قرار می‌دهیم $x_1 \sim x_2$ اگر و فقط اگر عضوی چون g در G موجود باشد بطوریکه $gx_1 = x_2$ در این صورت $\sim$ رابطه هم‌ارزی روی X است.

اثبات: الف) بسته بودن

$\forall g_1, g_2 \in G_x \quad g_1 x = x, g_2 x = x$

طبق شرط ۱ عمل G بر مجموعه X: $(g_1 g_2)x = g_1(g_2 x) = x$ داریم $g_1 g_2 \in G_x$ پس $\forall x \in X: ex = x$ و طبق شرط ۲

پس $e \in G_x$ و همچنین

$\forall g \in G_x : gx = x \Rightarrow x = g^{-1}x \Rightarrow g^{-1} \in G_x$

پس $G_x \leq G$.

اثبات ب) انعکاسی: چون $\forall x \in X: ex = x$ پس $x \sim x$

تقارنی: اگر $x_1 \sim x_2$ پس $g \in G$ وجود دارد که $gx_1 = x_2$ و چون $x_1 = g^{-1}x_2$ پس $x_2 \sim x_1$

تعدی: اگر $x_1 \sim x_2$ و $x_2 \sim x_3$ آنگاه $\exists g_1, g_2 \in G$ که $g_1 x_1 = x_2$ و $g_2 x_2 = x_3$

$(g_2 g_1)(x_1) = g_2(g_1 x_1) = g_2 x_2 = x_3 \Longrightarrow x_1 \sim x_3$

تعریف: در قضیه قبل (G-مجموعه X) زیرگروه $G_x = \{g \in G \mid gx = x\}$ را ثابت ساز x می‌نامیم و با $\mathrm{Stab}_G(x)$ نمایش می‌دهیم و همچنین کلاسهای هم‌ارزی رابطه $\sim$ روی X را مدارهای عمل G روی X می‌نامیم و مدار عضو $x \in X$ را با $\bar{x}$ نمایش می‌دهیم.

$\bar{x} = \{y \in X \mid x \sim y\}$.

مثال ۷: در مثال ۶ یعنی D_4 - مجموعه X داریم:

$G_1 = \{\rho_0, \delta_2\} = G_3$ ، $G_2 = \{\rho_0, \delta_1\}$

$G_{S_1} = G_{S_3} = \{\rho_0, \mu_1\}$ ، $G_{S_2} = G_{S_4} = \{\rho_0, \mu_2\}$ و $G_C = D_4$

$G_{d_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\} = G_{d_2}$ ، $G_{m_1} = G_{m_2} = \{\rho_0, \rho_2, \mu_1, \mu_2\}$

$G_{P_1} = G_{P_3} = \{\rho_0, \mu_1\}$ و $G_{P_2} = G_{P_4} = \{\rho_0, \mu_2\}$

مدارهای (کلاسهای هم‌ارزی) X عبارتند از

$\bar{1} = \bar{2} = \bar{3} = \bar{4} = \{1,2,3,4\}$ ، $\bar{d_1} = \bar{d_2} = \{d_1, d_2\}$ ، $\bar{P_1} = \bar{P_2} = \bar{P_3} = \bar{P_4} = \{P_1, P_2, P_3, P_4\}$

$\bar{c} = \{c\}$ ، $\bar{S_1} = \bar{S_2} = \bar{S_3} = \bar{S_4} = \{S_1, S_2, S_3, S_4\}$

توجه: برای هر $g \in G$ می‌توان $X_g = \{x \in X \mid gx = x\}$ ثابت ساز g در نظر گرفت و در مثال ۶ داریم

$X_{\rho_0} = X$ ، $X_{\rho_1} = \{c\}$ ، $X_{\rho_2} = \{m_1, m_2, d_1, d_2, c\}$ و $X_{\rho_3} = \{c\}$ و $X_{\delta_1} = \{2,4,d_1,d_2,c\}$

$X_{\mu_1} = \{S_1, S_3, m_1, m_2, c, P_1, P_3\}$ ، $X_{\mu_2} = \{S_2, S_4, m_1, m_2, c, P_2, P_4\}$ و $X_{\delta_2} = \{1,3,d_1,d_2,c\}$

مثال ۸: یک گروه G روی مجموعه $X=G$ به صورت مزدوجی عمل می‌کند (یعنی G روی خودش) و به عبارت دیگر G یک G-مجموعه است نسبت به عمل مزدوجی نام‌گذاری زیر را داریم.

$$f: G\times G \longrightarrow G$$
$$\forall x,g\in G : f(g,x)=gxg^{-1}$$

دراین صورت: ۱) مدار x را برده مزدوجی x می‌گوییم. $\bar{x}=\{gxg^{-1} \mid g\in G\}$ $(\forall x\in G)$.

۲) اگر $H\leq G$. $Stab_H(x)=\{h\in H \mid hxh^{-1}=x\}=\{h\in H \mid hx=xh\}$ را مرکز ساز x در H می‌نامیم و با $C_H(x)$ نمایش می‌دهیم. بنابراین $C_H(x)$ مجموعه اعضای از H است که با x جابجا می‌شوند یعنی $hx=xh$.

۳) اگر $H=G$ آنگاه $C_G(x)$ را مرکز ساز x می‌نامیم یعنی مجموعه اعضای از G که $xg=gx$.

اگر H روی مجموعه S یعنی مجموعه تمام زیرگروه‌های G به صورت مزدوجی عمل کند آنگاه به ازای هر $K\in S$ ثابت ساز K یعنی $Stab_H(K)=\{h\in H \mid hKh^{-1}=K\}$ را نرمالساز K در H می‌نامیم و آن را با $N_H(K)$ نمایش می‌دهیم زیرگروه $N_G(K)$ را نرمالساز K می‌گوییم. بدیهی است هر زیرگروه K در $N_G(K)$ نرمال است و $K\trianglelefteq G$ اگر و فقط اگر $N_G(K)=G$ (طبق تعریف $N_G(K)$ بدیهی) $(N_G(K)=\{g\in G \mid gKg^{-1}=K\}$ تعریف نرمالیزور و تعریف نرمال)

قضیه ۲: اگر X یک G مجموعه باشد آنگاه برای هر $x\in X$ $|\bar{x}|=[G:G_x]$.

اثبات: فرض کنید که L مجموعه تمام همدسته‌های چپ G_x در G باشد. تناظر $\phi: L\longrightarrow \bar{x}$ در نظر می‌گیریم $\phi(gG_x)=gx$ نشان می‌دهیم که ϕ یک تابع درست است.

$$gG_x=hG_x \iff g^{-1}h\in G_x \iff (g^{-1}h)x=x \iff gx=hx \iff \phi(gG_x)=\phi(hG_x)$$

خوش‌تعریفی تابع ϕ از $\Longrightarrow$ نتیجه می‌شود و یک به یک بودن تابع ϕ از $\Longleftarrow$ نتیجه می‌شود.

ϕ پوشا است زیرا برای هر $y=gx\in\bar{x}$ آنگاه gG_x در L وجود دارد که $\phi(gG_x)=gx$ پس $|L|=|\bar{x}|$

وچون $[G:G_x]=|L|$ پس $[G:G_x]=|\bar{x}|$

نتیجه: فرض کنید که G یک گروه متناهی باشد و $K\leq G$ دراین صورت

الف) تعداد عناصر برده مزدوجی $x\in G$ برابر است با $[G:C_G(x)]$ که $|G|$ را می‌شمارد.

ب) اگر $\bar{x_1}$ و $\bar{x_2}$ و ... و $\bar{x_n}$ تمام برده‌های مزدوجی متمایز G باشند آنگاه $|G|=\sum_{i=1}^{n}|\bar{x_i}|=\sum_{i=1}^{n}[G:C_G(x_i)]$

ج) تعداد زیرگروه‌های G مزدوج با K برابر است با $[G:N_G(K)]$ که $|G|$ را می‌شمارد.

اثبات الف: طبق قضیه ۱ ($G_x\leq G$) و قضیه لاگرانژ برقرار است. حال چون رابطه مزدوجی یک رابطه هم‌ارزی است لذا اجتماع کلاس‌های هم‌ارزی $\bar{x_1}$ و $\bar{x_2}$ و ... و $\bar{x_n}$ برابر با G است پس با بکارگیری الف) حکم ب) برقرار می‌شود.

چون زیرگروه‌های مزدوج K در G به صورت gKg^{-1} می‌باشند و طبق $N_G(K)=\{g\in G \mid gKg^{-1}=K\}$ و اینکه G روی مجموعه تمام زیرگروه‌های G به صورت مزدوجی عمل می‌کند پس طبق الف) $[G:N_G(K)]$ برابر با تعداد زیرگروه‌های G مزدوج با K است و $|G|$ را می‌شمارد.

قضیه ۳ (برنساید) فرض کنید که G یک گروه متناهی باشد و X یک G-مجموعه متناهی باشد اگر r تعداد (مدارهای) X تحت G

باشد آنگاه ① $|G| = \frac{1}{N}\sum_{g\in G} |X_g|$ که در آن $X_g = \{x \in X \mid gx = x\}$.

اثبات: تمام زوج‌های (x, g) که $gx = x$ را در نظر می‌گیریم و تعداد این زوج‌ها را N می‌نامیم. برای هر g از G، $|X_g|$ تعداد زوج‌هایی با مؤلفه دوم g وجود دارد و بنابراین ② $N = \sum_{g\in G} |X_g|$. از طرف دیگر برای هر x از X، $|G_x|$ تعداد زوج‌هایی با مؤلفه اول x وجود دارد پس داریم $N = \sum_{x\in X} |G_x|$. حال طبق قضیه ۲ داریم $|\bar{x}| = [G : G_x]$ اما می‌دانیم که $[G : G_x] = \frac{|G|}{|G_x|}$

از این رو نتیجه می‌شود که $|G_x| = \frac{|G|}{|\bar{x}|}$ پس $N = \sum_{x\in X} \frac{|G|}{|\bar{x}|} = |G| \sum_{x\in G} \frac{1}{|\bar{x}|}$.

اکنون $\frac{1}{|\bar{x}|}$ برای تمام xهای در یک مدار مقداری ثابت دارد و اگر θ را مدار دلخواهی بگیریم آنگاه $\sum_{x\in\theta} \frac{1}{|\bar{x}|} = 1$

بنابراین داریم ③ $N = |G| \times$ (تعداد مدارهای X تحت G) $= |G| \cdot r$

حال با مقایسه ② و ③ داریم $|G| = \frac{1}{r}\sum_{g\in G} |X_g|$.

چند کاربرد از G-مجموعه در شمارش

① فرض کنید که X مجموعه ۲۰ نقطه گذاری متفاوت و جوه یک مکعب با استفاده از یک تاسی نقلی باشد. (!۶) (بعضی ساختن یک تاس) فرض کنید که G گروه ۲۴ چرخش مکعب باشد (یعنی قرارداد ن یک تاس روی میز) زیرا هر یک از شش وجه مکعب را می‌توان پایین قرار داد آنگاه. هر یک از چهار وجه با چرخاندن در جهار قرار دارد ($۶\times۴ = ۲۴$) تعداد تاس‌های متمایز برابر است با تعداد مدارهای X تحت G. برای هر $g \in G$ که $g \neq e$ آنگاه $|X_g| = ۰$ زیرا هر چرخش غیر از همانی هر یک از $۲۰! = ۶۱$ نقطه گذاری را به دیگری تغییر می‌دهد. چون $|X_e| = ۲۰!$ زیرا عضوهای هر یک از ۲۰ نقطه گذاری را ثابت نگه می‌دارد بنابراین طبق قضیه برنسایید داریم

تعداد مدارها $= \frac{1}{۲۴} \times ۲۰! = ۳۰$

بنابراین ۳۰ تاس متمایز وجود دارد.

توجه: این مسئله را می‌توان از روش مقدماتی حل کرد. برای ساختن تاس‌های متمایز (مختلف) می‌توان فرض کرد که وجه با یک نقطه در پایین قرار داشته باشد برای وجه بالا پنج انتخاب وجود دارد و با دوران تاس وقتی که از بالا به آن نگاه می‌کنیم هر کدام از چهار وجه دیگر می‌تواند به جلو آورده شود. از این رو برای وجه جلو تفاوتی در انتخابها نیست. اما نسبت به عدد روی وجه جلو، به تعداد $۱ \times ۲ \times ۳$ امکان به سه وجه جانبی باقیمانده وجود دارد. بنابراین به تعداد $۵ \times ۳ \times ۲ \times ۱ = ۵ \times ۳! = ۳۰$ امکان تاس متفاوت وجود دارد.

② با چند صورت مختلف هفت شخص می‌توانند دور یک میز گرد بنشینند.

حل: بطور کلی $۷!$ امکان متفاوت برای نشستن افراد روی هفت صندلی متفاوت وجود دارد. X را مجموعه $۷! = ۵۰۴۰$ امکان نشستن‌ها در نظر می‌گیریم. دورانی از افراد که از هر کس خواسته شود یک صندلی به طرف راست (یا چپ) حرکت دهد همان آرایش (دور میز) را نتیجه می‌دهد. چنین دورانی یک گروه دوری G از مرتبه ۷ تولید می‌کند و با طریق طبیعی متوان نشان کرد که این گروه

روی X عمل می‌کند. در اینجا تنها عنصر همانی e هر آرایش را ثابت نگه می‌دارد. بنابراین طبق قضیه برنساید داریم

$$\text{تعداد مدارها} = \frac{1}{7}\times 7! = 6! = 720$$

نتیجه: به $(n-1)!$ طریق می‌توانند n شخص دور میز گرد بنشینند.

(۳) به چند صورت مختلف با هفت مهره هم‌اندازه با رنگهای متفاوت می‌توان یک گردنبند (بدون قلاب) درست کرد؟

حل: برخلاف مثال قبل، گردنبندها علاوه بر دوران می‌توان برگرداند و بنابراین کل گروه D_7 از مرتبه $14 = 2\times 7$ را داریم که روی مجموعه X از $7!$ امکان عمل می‌کند. پس تعداد گردنبندهای متفاوت عبارت است از:

$$\text{تعداد مدارها} = \frac{1}{14}\times 7! = \frac{1}{2}\times 6! = 360$$

نتیجه: به $\frac{1}{2}(n-1)!$ طریق می‌توان با n مهره هم‌اندازه و هم‌رنگ گردنبند درست کرد.

(۴) به چند طریق می‌توان با چهار رنگ متفاوت اضلاع یک مثلث متساوی‌الاضلاع را رنگ‌آمیزی کرد با شرطی که برای هر ضلع فقط از یک رنگ بتوان استفاده کرد و یک رنگ را برای اضلاع مختلف هم بتوان به کار برد.

حل: برای رنگ‌آمیزی ضلعها تعداد $4^3 = 64$ طریق وجود دارد زیرا هر یک از ضلعها را می‌توان با هر چهار رنگ، رنگ‌آمیزی کرد. X را مجموعه این ۶۴ رنگ درنظر بگیریم. گروه G را که روی X عمل می‌کند گروه تقارنهای مثلث یعنی S_3 درنظر بگیریم. باید $|X_g|$ را برای هر عنصر g از S_3 حساب کنیم.

هر مثلث رنگ‌شده توسط ρ_0 ثابت نگه داشته می‌شود. پس داریم:

$$|X_{\rho_0}| = 64$$

برای ثابت ماندن ضلعها تحت ρ_1 باید همه ضلع‌ها از یک رنگ باشند. پس

$$|X_{\rho_1}| = 4 = |X_{\rho_2}|$$

اضلاعی که با هم تعویض می‌شوند باید از یک رنگ باشند (یعنی ۴ امکان) و سایر اضلاع نیز از هر رنگی می‌توانند باشند (پس در ۴ ضرب می‌شوند). پس

$$|X_{\mu_1}| = |X_{\mu_2}| = |X_{\mu_3}| = 16$$

$$\sum_{g\in S_3} |X_g| = 64+4+4+4+16+16+16 = 120$$

۲۰ مثلث رنگ‌شده متمایز وجود دارد. $\Leftarrow$ $\text{تعداد مدارها} = \frac{1}{6}(120) = 20$

(۵) در مسئله قبل اگر بخواهیم اضلاع مثلث را با رنگهای متفاوت رنگ کنیم، تعداد حالتهای ممکن برای رنگ‌آمیزی اضلاع مثلث برابر $4\times 3\times 2 = 24$ است. X را مجموعه ۲۴ مثلث رنگ‌شده درنظر بگیریم. گروهی که روی X عمل می‌کند همان S_3 است. چون رنگ همه اضلاع متفاوت است پس $|X_{\rho_0}| = 24$، در حالی که برای هر g از S_3 غیر از ρ_0 داریم $|X_g| = 0$. پس

$$\text{تعداد مدارها} = \frac{1}{6}\times(24) = 4$$

بنابراین ۴ مثلث متفاوت (متمایز) وجود دارد.

قضیه ۴: فرض کنید که G یک گروه باشد که روی مجموعه X عمل می‌کند. دراین صورت به ازای هر $g\in G$ یک تابع $\rho_g: X\to X$ تعریف می‌شود که به ازای هر $x\in X$ به صورت $\rho_g(x)=gx$ تعریف می‌شود و ρ_g یک جایگشت از X است (یعنی $\rho_g\in S_X$). علاوه بر این تابع $\phi: G\to S_X$ که به ازای هر $g\in G$ به صورت $\phi(g)=\rho_g$ تعریف می‌شود یک هموومورفیسم است. این هموومورفیسم را معرف جایگشتی G متناظر با عمل G روی X نامند.

اثبات: جایگشت بودن ρ_g: طبق تعریف عمل گروه G روی X، ρ_g برای هر $g\in G$ یک تابع از X به X است.

$\forall g_1,g_2\in G,\ \forall x\in X \quad \rho_{g_1}\rho_{g_2}(x)=\rho_{g_1}(g_2x)=g_1(g_2x)=(g_1g_2)x=\rho_{g_1g_2}(x) \Longrightarrow \rho_{g_1}\rho_{g_2}=\rho_{g_1g_2}$ ①

همچنین $\rho_e=I_X\in S_X$ پس $\rho_e(x)=ex=x$ ②.

بنابر ① و ② $\forall g\in G \quad \rho_g\rho_{g^{-1}}=I_X=\rho_{g^{-1}}\rho_g$ بنابراین ρ_g یک تابع دارون پذیر است یعنی یک به یک و پوشا است پس ρ_g یک جایگشت از X به X است یعنی $\rho_g\in S_X$. $(\rho_{g^{-1}}=(\rho_g)^{-1})$

هموومورفیسم بودن ϕ: $\forall g_1,g_2\in G \quad \phi(g_1g_2)=\rho_{g_1g_2}\overset{①}{=}\rho_{g_1}\cdot\rho_{g_2}=\phi(g_1)\phi(g_2)$

قضیه ۵: فرض کنید که G یک گروه و X یک مجموعه غیرتهی و σ یک هموومورفیسم از G به S_X باشد دراین صورت G روی X به طور عمل می‌کند اگر به ازای هر $g\in G$ و برای هر $x\in X$ تعریف کنیم $gx=(\sigma(g))(x)$ و σ معرف جایگشتی G متناظر با این عمل است.

برهان: چون σ هموومورفیسم است پس: $\forall g_1,g_2\in G,\ \forall x\in X$

$(g_1g_2)(x)=(\sigma(g_1g_2)(x))=(\sigma(g_1)\sigma(g_2))(x)=(\sigma(g_1)(\sigma(g_2)(x))=(\sigma(g_1))(g_2x)=g_1(g_2x)$

یعنی شرط اول عمل G روی X برقرار است. همچنین شرط دوم: $ex=(\sigma(e))(x)=I_X(x)=x$

بنابراین عمل $gx=(\sigma(g))(x)$ از گروه G روی مجموعه X خوشتعریف است

فرض کنید که ϕ معرف جایگشتی متناظر با این عمل G باشد. دراین صورت به ازای هر $x\in X$ و هر $g\in G$

$\rho_g(x)=gx=(\sigma(g))(x)$ ولذا به ازای هر $g\in G$، $\rho_g=\sigma(g)$ پس $\phi=\sigma$.

تمرین:

۱) فرض کنید که V یک فضای برداری غیرصفر روی میدان F باشد. نشان دهید که $F^*=F-\{0\}$ (تحت ضرب) روی مجموعه V عمل می‌کند ولی گروه $(F,+)$ روی مجموعه V عمل نمی‌کند.

۲- فرض کنید که G یک گروه و H زیرگروه نرمال آبلی از گروه G باشد. نشان دهید که G/H به صورت مذکور روی H عمل می‌کند و یک هموومورفیسم $\phi: \frac{G}{H}\to Aut(H)$ به دست آورید.

۳- فرض کنید X یک G-مجموعه باشد و σ معرف عمل متناظر با این عمل باشد. ثابت کنید

$$Ker(\sigma) = \bigcap_{x\in X} Stab_G(x).$$

۴- فرض کنید X یک G-مجموعه باشد. عمل G روی X را انتقالی نامیم اگر به ازای هر $x,y\in X$ عضوی مانند $g\in G$ وجود داشته باشد به قسمی که $y=gx$. فرض کنید عمل G روی X انتقالی باشد. ثابت کنید

الف) $\forall x\in X \ , \ \bar{x}=X$

ب) پایدارسازهای هر دو عضو از X (ثابت‌سازهای) در G مزدوجند.

ج) اگر G دارای این خاصیت باشد که $\{e\}=\{g\in G \mid gx=x, \forall x\in X\}$ و اگر $N\trianglelefteq G$ و به ازای عضوی $x\in X$، $N\leq Stab_G(x)$، آنگاه $N=\{e\}$ (مثلاً اگر $G\leq S_n$ به ازای عضوی n و $X=X_n=\{1,2,3,\dots,n\}$).

د) به ازای هر $x\in X$، $|X|=[G:Stab_G(x)]$ و لذا $|X| \mid |G|$.

طبق قضیه برنساید تمرین‌های ۵ تا ۸ را حل کنید.

۵- تعداد مدارهای $\{1,2,3,4,5,6,7,8\}$ تحت زیرگروه دوری $\langle(1,3,5,6)\rangle$ از S_8 را به دست آورید.

۶- تعداد مدارهای $\{1,2,3,4,5,6,7,8\}$ تحت زیرگروه S_8 تولید شده توسط $(1,3)$ و $(2,4,7)$ را به دست آورید.

۷- تعداد تاس‌های متمایز چهاروجهی را که با قرار دادن یک، دو، سه و چهار نقطه روی وجوه یک چهاروجهی منتظم به جای یک مکعب می‌توان به دست آورد.

۸- الف) برای ساختن اسباب بازی، وجوه مکعب‌های چوبی هم‌اندازه را باید با رنگ‌های متفاوت رنگ آمیزی کنیم. اگر ۸ رنگ در اختیارمان باشد، چند مکعب متمایز می‌توانیم بسازیم؟

ب) اگر بخواهیم روی وجوه متفاوت رنگ‌های تکراری هم امکان‌پذیر باشد، چند مکعب متمایز می‌توان ساخت؟

گروه متناهیاً تولید شده

تعریف: فرض کنید G یک گروه باشد و برای هر i از مجموعه I، $a_i\in G$. کوچکترین زیرگروه G شامل $\{a_i \mid i\in I\}$ زیرگروه تولید شده توسط $\{a_i \mid i\in I\}$ نامیده می‌شود. اگر این زیرگروه خود G باشد آنگاه مجموعه $\{a_i \mid i\in I\}$ را مولد گروه G می‌نامیم و این مجموعه G را تولید می‌کند. اگر مجموعه $\{a_i \mid i\in I\}$ متناهی باشد و گروه G را تولید کند آنگاه G را یک گروه متناهیاً تولید شده می‌نامیم.

توجه: مجموعه مولد $\{a_i \mid i\in I\}$ در G وجودی است یعنی اگر چنین مجموعه متناهی در G وجود داشته باشد و G را تولید کند آنگاه G را گروه متناهیاً تولید شده می‌نامیم.

مثال ۱) گروه $\mathbb{Z}\times\mathbb{Z}_2$ به وسیله مجموعه $\{(1,0),(0,1)\}$ تولید می‌شود پس گروه $\mathbb{Z}\times\mathbb{Z}_2$ متناهیاً تولید شده می‌باشد.

قضیه ۱: اگر G یک گروه باشد و برای هر i از I، $a_i\in G$. آنگاه زیرگروه H از G تولید شده به وسیله $\{a_i \mid i\in I\}$ دقیقاً از تمام اعضایی از G تشکیل می‌شود که به صورت حاصلضرب متناهی از توان‌های صحیح a_iها باشند. در اینجا توان‌های یک a_i ثابت می‌تواند چندین بار در حاصلضرب ظاهر شود.

گروه‌های آبلی آزاد:

برای معرفی گروه آبلی آزاد قضیه زیر را بررسی می‌کنیم و سپس از روی این قضیه گروه آبلی آزاد را معرفی می‌کنیم

قضیه ۲: فرض کنید که X زیرمجموعه‌ای از یک گروه آبلی جمعی ناصفر G باشد. شرایط زیر روی X هم ارز هستند.

الف) هر عضو ناصفر a از G را با ازای $n_i \neq 0$ از $\mathbb{Z}$ و x_i های متمایز از X را می‌توان بطور یکتا به صورت $a = \sum_{i=1}^{r} n_i x_i = n_1 x_1 + n_2 x_2 + \cdots + n_r x_r$ نوشت

ب) X گروه G را تولید می‌کند و با ازای $n_i \in \mathbb{Z}$ و x_iهای متمایز از X: $\sum_{i=1}^{r} n_i x_i = 0 \iff n_1 = n_2 = \cdots = n_r = 0$

تعریف: هر گروه آبلی که مجموعه‌ای مولدی ناتهی چون X داشته باشد و واجد شرایط مذکور در قضیه ۱ باشد یک گروه آبلی آزاد نامیده می‌شود و X مبنایی برای گروه آبلی آزاد است.

مثال ۲: گروه $\mathbb{Z}$ آبلی آزاد است و $X = \{(1,0)\}$ یک مبنای آن است.

همچنین $\mathbb{Z} \times \mathbb{Z}$ گروه آبلی آزاد است و $X = \{(1,1),(0,1)\}$ و $\{(1,0),(0,1)\}$ یک مبنای آن است.

بطور کلی حاصلضرب‌های متناهی از گروه $\mathbb{Z}$ با خودش، گروه‌های آبلی آزاد هستند.

دلیل گروه آبلی آزاد بودن $\mathbb{Z} \times \mathbb{Z}$: چون $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z} \Rightarrow (a,b) = a(1,0) + b(0,1)$

یعنی خاصیت الف در قضیه ۱ برقرار است (همینطور خاصیت ب) از قضیه ۱ برای $\mathbb{Z} \times \mathbb{Z}$ برقرار است و زیرا

$$n(1,0) + m(0,1) = (0,0) \Rightarrow (n,m) = (0,0) \Rightarrow n = 0, m = 0$$

مثال ۳: گروه $\mathbb{Z}_n$ آبلی آزاد نیست. زیرا برای هر x از $\mathbb{Z}_n$ و $n \neq 0$ داریم $nx = 0$ که متناقض با خاصیت ب) در قضیه ۱ است.

قضیه ۳: اگر G یک گروه آبلی آزاد ناصفر با مبنایی از r عضوی $X = \{x_1, x_2, \ldots, x_r\}$ باشد آنگاه G با گروه $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r عامل) ایزومورف است.

اثبات: $\phi : G \longrightarrow \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ عامل}}$ با ضابطه $\phi(a) = (n_1, n_2, \ldots, n_r)$

که در آن $a = \sum_{i=1}^{r} n_i x_i$ است طبق قضیه ۲ منحصر بفرد است.

ϕ خوش‌تعریف است. زیرا اگر $a = b$ آنگاه $a = \sum_{i=1}^{r} n_i x_i$ و $b = \sum_{i=1}^{r} m_i x_i$ پس $\sum_{i=1}^{r} n_i x_i = \sum_{i=1}^{r} m_i x_i$ بنابراین $\sum_{i=1}^{r} (n_i - m_i) x_i = 0$ بنابراین $\forall i = 1, \ldots, r : n_i - m_i = 0$

پس $n_i = m_i$ یعنی $\phi(a) = \phi(b)$.

ϕ یک‌یک است:

$$\phi(a) = \phi(b) \Rightarrow (n_1, n_2, \ldots, n_r) = (m_1, m_2, \ldots, m_r)$$

بنابراین $n_i = m_i$ برای هر $i = 1, 2, \ldots, r$ پس $\sum_{i=1}^{r} n_i x_i = \sum_{i=1}^{r} m_i x_i$ یعنی $a = b$.

ϕ پوشا است. زیرا برای هر $(n_1, n_2, \ldots, n_r)$ از $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ آنگاه $a = \sum_{i=1}^{r} n_i x_i \in G$ وجود دارد که $\phi(a) = (n_1, n_2, \ldots, n_r)$.

$\forall a,b \in G: \ a=\sum_{i=1}^{r} n_i x_i$ و $b=\sum_{i=1}^{r} m_i x_i$ ϕ همومورفیسم جمعی است. زیرا

$$\phi(a+b)=\phi\left(\sum_{i=1}^{r} n_i x_i+\sum_{i=1}^{r} m_i x_i\right)=\phi\left(\sum_{i=1}^{r}(n_i+m_i)x_i\right)=(n_1+m_1,\dots,n_r+m_r)$$

$$=(n_1,n_2,\dots,n_r)+(m_1,m_2,\dots,m_r)=\phi(a)+\phi(b)$$

پس ϕ یک اندومورفیسم است.

قضیه ۳: فرض کنید که $G\neq\{0\}$ یک گروه آبلی آزاد با مبنای متناهی باشد. آنگاه هر مبنای G متناهی است، و تعداد اعضای همه مبناها یکی است.

برهان: فرض کنید G مبنایی چون $\{x_1,x_2,\dots,x_r\}$ داشته باشد. آنگاه G مطابق قضیه قبل با $\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}$ (r تا) یکریخت است. قرار دهید $2G=\{2g \mid g\in G\}$. ($2G\leq G$ زیرگروه. تمرین).

$$\frac{G}{2G}\cong\frac{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}{2\mathbb{Z}\times2\mathbb{Z}\times\cdots\times2\mathbb{Z}}\cong\underbrace{\mathbb{Z}_2\times\mathbb{Z}_2\times\cdots\times\mathbb{Z}_2}_{r \text{ عامل}}$$

چون $G\cong\underbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}_{r \text{ تا}}$ داریم

بنابراین $2^r=\left|\frac{G}{2G}\right|$. از این رو تعداد اعضای هر مبنای متناهی X برابر است با $\log_2\left|\frac{G}{2G}\right|$

پس تعداد اعضای هر دو مبنای متناهی یکی است. حال نشان می دهیم که G نمی تواند مبنایی نامتناهی هم داشته باشد.

فرض کنید Y مبنایی دلخواه برای G و $\{y_1,y_2,\dots,y_s,\dots\}$ مجموعه ای از اعضای متمایز Y باشد. فرض کنید H زیرگروه تولید شده با $\{y_1,y_2,\dots,y_s\}$ و K زیرگروه تولید شده با بقیه اعضای Y باشد. با سهولت می توان ملاحظه کرد که $G=H\times K$، از اینرو

$$\frac{G}{2G}\cong\frac{(H\times K)}{(2H\times 2K)}\cong\left(\frac{H}{2H}\right)\times\left(K/2K\right)$$

چون $2^s=\left|\frac{H}{2H}\right|$ می بینیم که $2^s\leq|G/2G|$ یا به صورت معادله $2^r=\left|\frac{G}{2G}\right|$، ملاحظه می کنیم که $s\leq r$

پس Y نمی تواند مجموعه ای نامتناهی باشد، زیرا می توانستیم قرار دهیم $r<s$.

تعریف: اگر G گروه آبلی آزاد باشد، رتبه G را تعداد اعضای مبنایی از G است. (همه مبناها یک تعداد عضو دارند)

مثال ۴ رتبه $\mathbb{Z}\times\mathbb{Z}$ برابر ۲ است. دیدیم که $\{(0,1),(1,0)\}$ یک پایه $\mathbb{Z}\times\mathbb{Z}$ است و همچنین مجموعه $\{(3,1),(1,0)\}$ هم مبنای دیگری برای $\mathbb{Z}\times\mathbb{Z}$ است زیرا اگر $(m,n)\in\mathbb{Z}\times\mathbb{Z}$ دلخواه باشد:

$$(m,n)=x(1,0)+y(3,1)=(x+3y,y)\Rightarrow\begin{cases}m=x+3y\\ n=y\end{cases}\Rightarrow x=m-3y=m-3n$$

بنابراین $x=m-3n$ و $y=n$.

ولی $\{(3,0),(0,1)\}$ یک مبنای $\mathbb{Z}\times\mathbb{Z}$ نیست زیرا عضو $(2,0)$ از $\mathbb{Z}\times\mathbb{Z}$ نمی توان به صورت $n(3,0)+m(0,1)$ نوشت.

$$(2,0)=n(3,0)+m(0,1)=(3n,m)\Rightarrow\begin{matrix}3n=2\\ m=0\end{matrix}\Rightarrow n=\frac{2}{3}\notin\mathbb{Z}$$

قضیه ۵: فرض کنید که G یک گروه آبلی آزاد با رتبه n باشد و فرض کنید K زیرگروه ناصفری از G باشد. آنگاه K آبلی آزاد است و رتبه K برابر s، $s\leq n$.

همچنین بدان G مبنایی چون $\{x_1,x_2,\dots,x_n\}$ و اعداد طبیعی چون d_1 و d_2 و ... و d_s وجود دارند که برای $i=1,2,\dots,(s-1)$، $d_i\mid d_{i+1}$ و $\{d_1x_1,d_2x_2,\dots,d_sx_s\}$ همر مبنایی برای K است.

قضیه ۶: هر گروه آبلی متناهیاً تولید شده یا گروهی با صورت $Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_t} \times Z \times Z \times \cdots \times Z$ ایزومورف است که در آن برای هر $i=1,2,\ldots,t$ عدد m_i عدد m_{i+1} را عاد می‌کند (می‌شمارد).

گروه آزاد:

فرض کنید که A مجموعه‌ای (نه لزوماً متناهی) از اعضای a_i باشد $i \in I$. می‌توان A را با عنوان یک الفبا در نظر گرفت و هر عضو آن مانند a_i ها یک حرف از این الفبا تصور کرد و هر نمادی با صورت a_i^n که در آن $n \in \mathbb{Z}$ است را یک هجا و هر تعداد متناهی هجا را که پشت سر هم نوشته شده‌اند را یک کلمه در نظر گرفت. همچنین کلمه تهی را کلمه‌ای در نظر می‌گیریم که در آن هیچ هجایی وجود ندارد.

مثال ۵: فرض کنید که $A = \{a_1, a_2, a_3\}$ در این صورت a_i همان a_i^1 است و a_3^3 و $a_1 a_2 a_1^2$ و $a_1 a_3^{-4} a_1^2 a_2$ همه کلمه خواهند بود.

توجه: به کمک قانون توان‌ها یعنی $a^n \cdot a^m = a^{n+m}$ و $a^0 = 1$ می‌توان یک کلمه را مختصر کرد.

مثال ۶: شکل مختصر کلمه $a_2^3 a_3^{-1} a_2 a_1^2 a_1^{-7}$ عبارت است $a_2^2 a_2 a_1^{-5}$.

مثال ۷: فرض کنید که $F[A]$ مجموعه تمام کلمه‌های متناهی حاصل از الفبای A باشد. $F[A]$ تحت عمل ضرب یک گروه است و این این گروه را گروه آزاد (تولید شده یا روی) A می‌نامیم.

دلیل گروه بودن $F[A]$: فرض کنید که w_1, w_2 دو عضو دلخواه از $F[A]$ باشند در این صورت $w_1 w_2 \in F[A]$. زیرا می‌توان $w_1 w_2$ را طبق قانون توان ساده کرد (مختصر کرد) مثلاً اگر $w_1 = a_2^3 a_1^{-5} a_3^2$ و $w_2 = a_3^{-2} a_1^2 a_2 a_3^{-2}$ باشد آنگاه

$$w_1 w_2 = a_2^3 a_1^{-5} a_3^2 a_3^{-2} a_1^2 a_2 a_3^{-2} = a_2^3 a_1^{-3} a_2 a_3^{-2} \in F[A]$$

کلمه تهی 1 همان عضو همانی $F[A]$ است و برای هر $w \in F[A]$ بدیهی است که $w^{-1} \in F[A]$.

تعریف: اگر G گروهی با مجموعه مولدی چون $A = \{a_i \mid i \in I\}$ باشد و اگر $\phi : G \longrightarrow F[A]$ با تعریف $\phi(a_i) = a_i$ یا $F[A]$ ایزومورف باشد آنگاه می‌گوییم G بر $A = \{a_i\}$ آزاد است و a_i ها مولدهای آزاد G هستند. یک گروه را آزاد می‌نامیم اگر بر مجموعه‌ای ناتهی چون $\{a_i\}$ آزاد باشد.

مثال ۸: گروه $\mathbb{Z}$ روی یک مولد (یعنی روی $\{1\}$ یا $\{-1\}$) آزاد است.

توجه: هر گروه آزاد نامتناهی است.

قضیه ۷: اگر گروه G هم بر مجموعه $\{a_i\}$ و هم بر مجموعه $\{b_i\}$ آزاد باشد آنگاه تعداد اعضای $\{a_i\}$ با تعداد اعضای $\{b_i\}$ برابر است یعنی هر دو مجموعه مولدهای آزاد یک گروه آزاد دارای یک عدد اصلی هستند.

تعریف: اگر گروه G بر مجموعه $\{a_i\}$ آزاد باشد آنگاه تعداد اعضای مجموعه $\{a_i\}$ را مرتبه گروه آزاد G می‌نامیم.

قضیه ۸: دو گروه آزاد با هم ایزومورف هستند اگر و فقط اگر دارای یک مرتبه باشند.

قضیه ۹: هر زیر گروه نابدیهی از گروه آزاد خود آزاد است.

قضیه ۱: فرض کنید که G با دستگاه $\{a_i\}_{i\in I}$ تولید شده و G' گروهی دلخواهی باشد اگر a'_i برای $i\in I$ اعضای دلخواه متمایز از G' باشند آنگاه حداکثر یک هموморفیسم $\phi: G \longrightarrow G'$ وجود دارد که $\phi(a_i) = a'_i$.
اگر G بر $\{a_i\}$ آزاد باشد آنگاه دقیقاً یک هموморفیسم بدین صورت وجود دارد.

تمرین:

۱- مبنایی چون $\{(c_1, c_2), (b_1, b_2), (a_1, a_2)\}$ برابری $\mathbb{Z}\times\mathbb{Z}$ پیدا کنید که در آن a_i ها و b_i ها و c_i ها مخالف صفر هستند.

۲- ثابت کنید که اشتراک برای a و b و c و d مجموعه $\{(a,b),(c,d)\}$ مبنایی برای $\mathbb{Z}\times\mathbb{Z}$ باشد.

۳- در قضیه ۴ ثابت کنید که $2G \leq G$

۴- در قضیه ۴ ثابت کنید که $G \cong H \times K$

حلقه ها

تعریف: فرض کنیم R یک مجموعه غیرتهی باشد و دو عمل جمع و ضرب روی R تعریف شود. در این صورت $(R,+,\cdot)$ را یک حلقه می نامیم اگر شرایط زیر برقرار باشند:

الف) $(R,+)$ یک گروه آبلی باشد

ب) عمل ضرب روی R شرکت پذیر باشد یعنی $\forall a,b,c \in R \quad (a\cdot b)\cdot c = a\cdot(b\cdot c)$

به عبارت دیگر $(R,\cdot)$ یک نیم گروه باشد.

ج) عمل ضرب روی جمع توزیع پذیر باشد، یعنی $\forall a,b,c \in R$

$(a+b)\cdot c = a\cdot c + b\cdot c$ (قانون توزیع پذیری راست) ، $a\cdot(b+c) = a\cdot b + a\cdot c$ (قانون توزیع پذیری چپ)

قرارداد و نمادگذاری: بجای حلقه $(R,+,\cdot)$ می گوییم حلقه R و بجای $a\cdot b$ می نویسیم ab.

عمل جمع $+$ و عمل ضرب $\cdot$ می توانند اعمال جمع و ضرب معمولی باشند ولی لزومی ندارد که این دو عمل جمع و ضرب معمولی باشند ها شد گروه ها این دو عمل می توانند جمع و ضرب باقی مانده ای یا جمع و ضرب مولفه ای و ... باشند.

تعریف: اگر عمل ضرب روی R خاصیت جابجایی داشته باشد می گوییم حلقه R یک حلقه جابجایی است و اگر در حلقه R عضوی مانند $e \in R$ وجود داشته باشد بطوریکه $a\cdot e = e\cdot a = a \quad (\forall a \in R)$ یعنی R شامل عضوخنثی ضرب باشد آنگاه حلقه R را یک حلقه یکدار می نامیم.

مثال ۱: $(\mathbb{Z},+,\cdot)$ و $(\mathbb{Q},+,\cdot)$ و $(\mathbb{R},+,\cdot)$ و $(\mathbb{C},+,\cdot)$ حلقه های یکدار و جابجایی هستند که به ترتیب حلقه $\mathbb{Z}$ و $\mathbb{Q}$ و $\mathbb{R}$ و $\mathbb{C}$ می نامیم.

مثال ۲: $(2\mathbb{Z},+,\cdot)$ یک حلقه جابجایی است ولی حلقه یکدار نیست.

مثال ۳: اگر n یک عدد صحیح مثبت باشد آنگاه $(\mathbb{Z}_n,\oplus,\odot)$ یک حلقه جابجایی و یکدار است.

$\oplus$ و $\odot$ به ترتیب عمل جمع و ضرب باقی مانده ای می باشد.

مثال ۴: فرض کنید که A یک مجموعه دلخواه باشد در این صورت $P(A)$ همراه با عمل تفاضل متقارن Δ (یا $\oplus$) و اشتراک $\cap$ یک حلقه است (یعنی $(P(A),\Delta,\cap)$ یک حلقه است.

عمل Δ یا $\oplus$ چه صورت زیر تعریف می شود:

$\forall B,C \in P(A)$:

$B\oplus C = (B-C)\cup(C-B) = (B\cup C)-(B\cap C) \qquad \oplus = \Delta$

حلقه $P(A)$ یک حلقه جابجایی و یکدار است زیرا اشتراک $\cap$ خاصیت جابجایی دارد و مجموعه A عضوخنثی ضرب در $P(A)$ است (توجه: بجای عمل جمع عمل $\oplus$ و بجای عمل ضرب، عمل اشتراک قرار گرفته است)

مثال ۵: $(Mat_{n\times n}(\mathbb{R}),+,\cdot)$ یک حلقه یکدار است ولی حلقه جابجایی نیست که در آن $+$ و $\cdot$ همان جمع و ضرب

ماتریسی است.

مثال ۶: اگر R یک حلقه با شد آنگاه $R \times R$ همراه با جمع و ضرب مولفه یک حلقه است اگر R حلقه‌ای جابجایی با شد آنگاه $R \times R$ هم حلقه جابجایی است و اگر R حلقه‌ای یکدار با شد آنگاه $R \times R$ حلقه‌ای یکدار است

مثال ۷: اگر $R_1, R_2, \dots, R_n$ حلقه با شند آنگاه $R_1 \times R_2 \times \cdots \times R_n$ تحت دو عمل جمع و ضرب مولفه‌ای یک حلقه است و اگر R_i ها جابجایی با شند، حلقه $R_1 \times R_2 \times \cdots \times R_n$ جابجایی است و اگر R_i ها یکدار با شند آنگاه $R_1 \times R_2 \times \cdots \times R_n$ یکدار است.

مثال ۸. $C(\mathbb{R}, \mathbb{R})$ = مجموعه‌ی همه‌ی توابع پیوسته از $\mathbb{R}$ یا $\mathbb{R}$ تحت جمع و ضرب توابع یک حلقه جابجایی و یکدار است.

$$\forall f(x), g(x) \in C(\mathbb{R}, \mathbb{R}) \quad : \quad (f+g)(x) = f(x) + g(x) \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

مثال ۹: فرض کنید که $(G, +)$ یک گروه آبی با شد، یک عمل ضرب روی G به صورت زیر تعریف می‌کنیم:

$$\forall a, b \in G \quad a \cdot b = 0$$

0 عضو همانی جمعی $(G, +)$ است.

در این صورت $(G, +, \cdot)$ یک حلقه جابجایی است ولی یکدار نیست.

قضیه ۱: اگر R حلقه‌ای با عضو همانی جمعی 0 با شد آنگاه برای هر a و b از R داریم:

الف) $0a = a0 = 0$

ب) $a(-b) = (-a)b = -ab$

ج) $(-a)(-b) = ab$

اثبات (الف)

$$a(0) = a(0+0) = a0 + a0 \xrightarrow[\text{حذفی}]{\text{قاعده}} a0 = 0$$

$$0a = (0+0)a = 0a + 0a \Longrightarrow 0a = 0$$

اثبات (ب)

$$a(-b) + ab = a(-b+b) = a0 = 0 \quad \text{و} \quad (-a)b + ab = [-a+a]b = 0b = 0 \Longrightarrow$$

چون عضو قرینه‌ی هر عضو یکتا است پس $a(-b)$ و $(-a)b$ قرینه‌ی ab است پس $a(-b) = (-a)b$

اثبات ج) با استفاده از قسمت (ب) داریم

$$(-a)(-b) = -[a(-b)] = -[-a(b)] = ab$$

قضیه ۲: اگر R حلقه یکدار با عضو همانی ضربی 1 با شد آنگاه، این 1 عضو همانی ضربی است (یعنی عضو همانی ضربی در صورت وجود منحصر به فرد است).

اثبات: فرض کنید که $1'$ هر عضو همانی ضربی حلقه R با شد در این صورت

$$1' = (1)(1') = 1 \Rightarrow 1 = 1'$$

قضیه ۳: در هر حلقه R: برای هر a و b از R و برای هر $m \in \mathbb{Z}$ داریم $m(ab) = (ma)b = a(mb)$

اثبات: اگر $m = 0$ طبق قضیه ۱ حکم برقرار است زیرا: $0 = 0(ab) = (0a)b = a(0b) = 0$

برای $m > 0$ با کمک روش استقرای ریاضی ثابت می‌کنیم که $m(ab) = (ma)b$

شروع استقرا $m=1$: $(a)b = (1a)b = 1(ab) = ab$

فرض استقرا فرض کنید که برای $m=k$ داشته باشیم: $k(ab) = (ka)b$

حکم استقرا: باید ثابت می‌کنیم که: $(k+1)(ab) = [(k+1)a]b$

$(k+1)(ab) = k(ab) + ab \xrightarrow{\text{فرض استقرا}} (ka)b + ab \xrightarrow{\text{توزیع‌پذیری}} [(ka+a)]b = [(k+1)a]b$

پس طبق اصل استقرا حکم برقرار است.

حال برای $m<0$ داریم $-m>0$ و چون $-m = (-1)m$ طبق حالت قبل $m(ab) = (ma)b$

به همین صورت می‌توان نشان داد که $m(ab) = a(mb)$

نتیجه: فرض کنید که R حلقه شامل یک عنصر همانی ضربی e باشد (یعنی حلقه R یکدار باشد) در این صورت بازای هر عدد صحیح m و برای هر $a \in R$، عضوی چون $r \in R$ وجود دارد بطوریکه $ma = r$. یعنی هر مضرب صحیح یک مضرب حلقه‌ای است.

اثبات: چون برای هر a از R، $ea = a$ بنابر قضیه قبل داریم.

$ma = m(ea) = (me)a$ با فرض $r = (me) \in R$ پس $ma = r$

تعریف: فرض کنید که R حلقه‌ای یکدار باشد، عضو a از R یک یکال R است در صورتی که a معکوس ضربی داشته باشد. حلقه یکدار R را یک حلقه تقسیم (میدان چپ) نامیم هرگاه هر عضو ناصفر از R یک یکال باشد یا به عبارت حلقه R یک حلقه تقسیم (میدان چپ) نامیم هرگاه $(R-\{0\}, .)$ یک گروه باشد.

حلقه R را یک میدان نامیم هرگاه $(R-\{0\}, .)$ یک گروه آبلی باشد یا به عبارت دیگر هر حلقه تقسیم جابجایی یک میدان است (معمولاً به میدان، هیات هم گفته می‌شود)

حلقه R را یک میدان چاوله (هیات چاوله) می‌نامیم هرگاه $(R-\{0\}, .)$ یک گروه غیر آبلی باشد

بنابراین یک حلقه تقسیم جابجایی را یک میدان و یک حلقه تقسیم غیر جابجایی را یک میدان چاوله می‌نامیم.

مثال ۱۰: $\mathbb{R}$ و $\mathbb{Q}$ میدان هستند ولی $\mathbb{Z}$ یک میدان نیست. یکال‌های $\mathbb{Z}$ عبارت است از 1 و -1.

توجه: یک حلقه تقسیم R باید حداقل دارای دو عضو باشد زیرا $0 \in R$ و باید $R - \{0\} \neq \phi$ زیرا در غیر این صورت $(R-\{0\})$ گروه نباشد بنابراین یک حلقه R باید حداقل دارای ۲ عضو باشد.

تعریف: فرض کنید که R یک حلقه باشد، یک عضو $a \neq 0$ در R را یک مقسوم علیه صفر چپ گوئیم اگر یک عضو $b \neq 0$ در R وجود داشته باشد بطوریکه $ab = 0$. با همین صورت یک عضو $b \neq 0$ در R را یک مقسوم علیه صفر راست نامیم هرگاه یک عضو $a \neq 0$ در R وجود داشته باشد بطوریکه $ab = 0$. یک مقسوم علیه صفر عضوی است که هم یک مقسوم علیه صفر چپ و هم یک مقسوم علیه صفر راست باشد.

توجه: در یک حلقه جابجایی، مقسوم علیه صفر چپ و راست یکسان هستند.

مثال ۱۱: مقسوم علیه‌های صفر حلقه Z_{12} را بیابید.

حل: مقسوم علیه‌های Z_{12} عبارت است از $Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$

$\bar{2}$ و $\bar{3}$ و $\bar{4}$ و $\bar{6}$ و $\bar{8}$ و $\bar{9}$ و $\bar{10}$ زیرا

$\bar{2}\odot\bar{6} = \bar{0}$ ، $\bar{3}\odot\bar{4} = \bar{0}$ ، $\bar{3}\odot\bar{8} = \bar{0}$ ، $\bar{4}\odot\bar{6} = \bar{0}$

$\bar{6}\odot\bar{10} = \bar{0}$ ، $\bar{9}\odot\bar{4} = \bar{0}$

مثال ۱۲: یکال‌های Z_{12} را بیابید.

حل: یکال‌های Z_{12} عبارت است از $\bar{5}$ و $\bar{7}$ و $\bar{11}$ زیرا

$\bar{5}\odot\bar{5} = \bar{1}$ ، $\bar{7}\odot\bar{7} = \bar{1}$

$\bar{11}\odot\bar{11} = \bar{1}$

مثال ۱۳: حلقه $(Mat_{2\times 2}(\mathbb{R}), +, \cdot)$ دارای مقسوم علیه صفر هستند

$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ مقسوم علیه صفر چپ در $Mat_{2\times 2}(\mathbb{R})$ است $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ مقسوم علیه صفر راست در $Mat_{2\times 2}(\mathbb{R})$ است.

تعریف فرض کنید که R یک حلقه باشد. گوییم R دارای قانون حذف چپ (راست) است هرگاه

$ab = ac \Longrightarrow b = c$ $\quad (ba = ca \Longrightarrow b = c)$: برای $a \neq 0$

قضیه ۴: حلقه R دارای قانون حذف چپ (راست) است اگر و فقط اگر R دارای مقسوم علیه صفر نباشد. اثبات: فرض کنید که R دارای قانون حذف چپ باشد حال فرض کنید که $ab = 0$ که در آن $a, b \in R$ و $a \neq 0$. بنابراین $ab = 0 = a0$ پس طبق قانون حذف چپ داریم $b = 0$ پس a یک مقسوم علیه صفر چپ نیست. به همین صورت می‌توان نشان داد که اگر R دارای قانون حذف راست باشد آنگاه R دارای مقسوم علیه صفر راست نیست.

برعکس: فرض کنید که R دارای مقسوم علیه صفر چپ نیست: فرض کنید که $ab = ac$ و $a \neq 0$.

در این صورت $a(b-c) = 0$ چون R دارای مقسوم علیه صفر چپ نیست پس باید $b-c = 0$ یعنی $b = c$ یعنی R دارای قانون حذف چپ می‌باشد. به همین صورت می‌توان ثابت کرد که اگر R دارای مقسوم علیه صفر راست نیست آنگاه R دارای قانون حذف راست می‌باشد.

تعریف: فرض کنید که R یک حلقه باشد. R را یک دامنه صحیح (حوزه صحیح) می‌نامیم هرگاه الف) R جابجایی باشد ب) $1 \in R$ $(1 \neq 0)$ ج) R دارای مقسوم علیه صفر نباشد (یا R

مثال ۱۴: حلقه های $(\mathbb{Z},+,\cdot)$ و $(\mathbb{Q},+,\cdot)$ و $(\mathbb{R},+,\cdot)$ و $(\mathbb{C},+,\cdot)$ و $(Z_p,\oplus,\odot)$ که p اول است حوزه صحیح هستند.

قضیه ۵: اگر $(R,+,\cdot)$ یک میدان باشد آنگاه R یک حوزه صحیح است.

اثبات: چون R یک میدان است پس حلقه جابجایی و یکدار است برای حوزه صحیح بودن کافی است نشان دهیم که R مقسوم علیه صفر ندارد. فرض کنید که $a,b\in R$ و $a\neq 0$ ، $ab=0$ ثابت می کنیم که $b=0$.

$$ab=0 \Rightarrow a^{-1}(ab)=a^{-1}0 \Rightarrow (a^{-1}a)b=0 \Rightarrow b=0$$

توجه: عکس این قضیه برقرار نیست زیرا $\mathbb{Z}$ یک حوزه صحیح است ولی $\mathbb{Z}$ میدان نیست.

قضیه ۶: مقسوم علیه های صفر حلقه Z_n دقیقاً عبارتند از اعدادی که با n متباین نیستند (یعنی اعضای از Z_n که نسبت به n اول نیستند)

اثبات: فرض کنید که $m\in Z_n$ و $m\neq 0$ و $(m,n)=d$ و $d\neq 1$ (بزرگترین مقسوم علیه مشترک m,n بطریق $d\neq 1$) در این صورت $m\left(\frac{n}{d}\right)=\left(\frac{m}{d}\right)n=0$ و $m\neq 0$ و $\frac{n}{d}\neq 0$ پس m مقسوم علیه صفر است.

از طرف دیگر اگر $(m,n)=1$ اگر برای یک $r\in Z_n$ داشته باشیم $rm=0$ آنگاه $n\mid rm$ چون $(m,n)=1$ پس $n\mid r$ از این رو $r=0$. یعنی مقسوم علیه های صفر Z_n دقیقاً اعضای از Z_n هستند که نسبت به n اول نیستند.

نتیجه: اگر p عدد اول باشد آنگاه Z_p مقسوم علیه صفر ندارد.

توجه: طبق نتیجه قبل برای p اول، حلقه Z_p یک حوزه صحیح است.

قضیه ۷: هر حوزه صحیح متناهی یک میدان است.

اثبات: فرض کنید که D یک حوزه صحیح متناهی باشد $D=\{0,1,a_1,a_2,\dots,a_n\}$ اکنون a را از سمت چپ (یا راست) در اعضای ناصفر D یعنی $a_1,a_2,\dots,a_n$ ضرب می کنیم پس $a1, aa_1, aa_2, \dots, aa_n$ ①

ادعا می کنیم که اعضای ① دو به دو متمایز هستند زیرا اگر $aa_i=aa_j$ طبق قانون حذف $a_i=a_j$.

و هیچ یک از اعضای ① صفر نیستند زیرا D مقسوم علیه صفر ندارد (پس اعضای ① با یک جایگشتی همان اعضای $a_1,a_2,\dots,a_n,1$ هستند از این رو یا $aa_i=1$ پس $a=1$ و یا به ازای یک مقدار i، $aa_i=1$ یعنی a_i وارون ضربی a است.

نتیجه: اگر p عدد اول باشد آنگاه Z_p یک میدان است.

اثبات: زیرا Z_p حوزه صحیح متناهی است.

توجه: کوچکترین میدان از نظر تعداد اعضا Z_2 است.

تمرین:

۱- نشان دهید که $R = \mathbb{Z} \times \mathbb{Z}$ با اعمال زیر یک حلقه است.

$\forall (a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}$

$(a,b) + (c,d) = (a+c, b+d)$ ، $(a,b)(c,d) = (ac+bd, ad+bc)$

۲- نشان دهید که $\mathbb{Q}(\sqrt{2}) = D = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ یک حلقه جابجایی و یکدار است. (با اعمال جمع و ضرب معمولی)

آیا $\mathbb{Q}(\sqrt{2})$ یک میدان است؟ (ادعای خود را ثابت کنید)

۳- اگر R یک حلقه یکدار باشد نشان دهید که مجموعه یکاهای R تحت عمل ضرب یک گروه است.

۴- نشان دهید که حلقه R یک حلقه جابجایی است اگر و فقط اگر $\forall a,b \in R \; ; \; a^2 - b^2 = (a-b)(a+b)$

۵- حلقه R را یک حلقه بولی گوییم اگر به ازای هر $a \in R$، $a^2 = a$. ثابت کنید که در یک حلقه بولی R

الف) $\forall a,b \in R \quad ab = ba \quad (\leftarrow \quad \forall a \in R \quad a + a = 2a = 0$

۶- عضو a از حلقه R را خودتوان نامیم وگاه $a^2 = a$. نشان دهید که هر حوزه صحیح (دقیقاً دو عضو خودتوان دارد.

۷- نشان دهید که مجموعه

$$H = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_1, a_2, a_3, a_4 \in \mathbb{R} \text{ و } i^2 = j^2 = k^2 = -1\}$$

با در عمل جمع معمولی و ضرب زیر یک میدان چپ (حلقه تقسیم) است

$$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 \vec{i} + b_3 \vec{j} + b_4 k) = (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i$$
$$+ (a_1 b_3 - a_2 b_4 - a_3 b_1 + a_4 b_2) \vec{j} + (a_1 b_4 - a_2 b_3 - a_3 b_2 + a_4 b_1) k$$

این حلقه را حلقه کواترنیون‌های حقیقی نامیده می‌شود.

۸- نشان دهید که $G = \{\pm 1, \pm i, \pm j, \pm k\}$ که در آن i و j همان اعضای H در تمرین ۷ هستند تحت ضرب یک گروه است G را گروه کواترنیون‌ها می‌نامیم.

۹- نشان دهید که $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} \mid a,b,c \in \mathbb{Q}\}$ تحت جمع و ضرب معمولی یک میدان است.

۱۱- یکاهای حلقه $\mathbb{Z} \times \mathbb{Z}$ ، $\mathbb{Z} \times \mathbb{Z}_3$ و $\mathbb{Z} \times \mathbb{Q}$ را بیابید.

۱۲- مقسوم علیه‌های صفر حلقه $\mathbb{Z} \times \mathbb{Z}$ را بیابید. آیا $\mathbb{Z} \times \mathbb{Z}$ حوزه صحیح است؟

نتیجه بگیرید که اگر D یک حوزه صحیح باشد آنگاه $D \times D$ حوزه صحیح نیست.

زیر حلقه ها و زیر میدان ها

تعریف: فرض کنید که $(R,+,\cdot)$ یک حلقه باشد زیر مجموعه ناتهی S از R تحت دو عمل $+$ و $\cdot$ یک زیر حلقه R نامیم هرگاه $(S,+,\cdot)$ خودش یک حلقه باشد و می نویسیم $S \leq R$

مثال ۱۵: $2\mathbb{Z} \leq \mathbb{Z}$ ، $\mathbb{Z} \leq \mathbb{R}$ ، $\mathbb{Z} \leq \mathbb{Q}$ و $\mathbb{Q} \leq \mathbb{R}$

تعریف: فرض کنید که $(F,+,\cdot)$ یک میدان باشد زیر مجموعه ناتهی R از F را یک زیر میدان F نامیم هرگاه $(R,+,\cdot)$ خودش یک میدان باشد و می نویسیم $R \leq F$

مثال ۱۶: $\mathbb{Q} \leq \mathbb{R}$ (یعنی $\mathbb{Q}$ زیر میدان $\mathbb{R}$ است). $\mathbb{R} \leq \mathbb{C}$ یعنی $\mathbb{R}$ زیر میدان $\mathbb{C}$ است.

قضیه ۸: زیر مجموعه S از حلقه R زیر حلقه R است اگر و فقط اگر

الف) $0 \in S$ ب) $\forall a,b \in S : (a-b) \in S$ و $\forall a,b \in S : a.b \in S$

اثبات: اگر S زیر حلقه R باشد بنابراین $(S,+,\cdot)$ خود یک حلقه است بنابراین $0 \in S$ و

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

برعکس اگر شرایط الف و ب برای زیر مجموعه S از حلقه R برقرار باشد نشان می دهیم که S زیر حلقه R است. طبق الف و ب و قضیه ای در گروه ها $(S,+) \leq (R,+)$ (S زیر گروه جمعی R است). پس $(S,+)$ یک گروه آبلی است و بنابراین زیر حلقه میدان S با به ضرب روی جمع از چپ و راست توزیع پذیر باشد که این خاصیت از R به S ارث می رسد.

مثال ۱۷: فرض کنید که R یک حلقه باشد و $a \in R$ عضو ثابت دلخواهی باشد. نشان دهید که مجموعه $I_a = \{x \in R \mid ax = 0\}$ زیر حلقه R است.

حل: طبق قضیه قبل نشان می دهیم که $0 \in I_a$ و $\forall b,c \in I_a \quad b-c \in I_a$ و $bc \in I_a$

چون $a0 = 0$ پس $0 \in I_a$. برای هر $b,c \in I_a$ داریم $ab = 0$ ، $ac = 0$ پس

$$a(b-c) = ab - ac = 0 - 0 = 0 \Rightarrow b-c \in I_a$$

$$a(bc) = (ab)c = 0c = 0 \Rightarrow bc \in I_a$$

بنابراین $I_a \leq R$

تمرین:

۱- الف) نشان دهید که اشتراک تعدادی از زیرحلقه های یک حلقه R زیرحلقه ای از R است

ب) نشان دهید که اشتراک تعدادی از زیرمیدانهای میدان F زیرمیدان F است

۲- اگر R یک حلقه باشد، نشان دهید که مرکز حلقه R یعنی $Z(R)=\{c\in R \mid ac=ca, \forall a\in R\}$ زیرحلقه R است

۳- ثابت کنید $S=\{\frac{a}{5} \mid a\in Z\}$ زیرحلقه $\mathbb{Q}$ است؛

۴- نشان دهید که $T=\{\frac{a}{2^n} \mid n\geq 0, a\in Z\}$ زیرحلقه $\mathbb{Q}$ است.

۵- فرض کنید که D یک حوزه صحیح باشد، نشان دهید که $T=\{n.1 \mid n\in Z\}$ زیرحوزه صحیح ای از D است

ایده آل در حلقه خارج قسمتی:

تعریف: فرض کنید که R یک حلقه باشد و I یک زیرحلقه R باشد در این صورت:

الف) I را یک ایده آل چپ حلقه R نامیم اگر ($RI\subseteq I$ یا) $\forall a\in I, \forall r\in R : ra\in I$

ب) I را یک ایده آل راست حلقه R نامیم اگر ($IR\subseteq I$ یا) $\forall a\in I, \forall r\in R : ar\in I$

ج) I را یک ایده آل (ایده آل دوطرفه) حلقه R نامیم هرگاه I هم ایده آل چپ و هم ایده آل راست R باشد.

اگر I یک ایده آل حلقه R باشد می نویسیم $I\trianglelefteq R$.

توجه: ایده آل برای یک حلقه همچون یک زیرگروه نرمال برای گروه است.

مثال ۱: برای هر عدد صحیح مثبت m: $mZ\trianglelefteq Z$ و $\langle m\rangle = mZ$.

توجه: برای هر حلقه R، R همیشه دارای حداقل دو ایده آل $\{0\}$ و R می باشد. ایده آل های R یا R ایده آل سره یا ایده آل بدیهی می نامیم. اگر I یک ایده آل R باشد و $I\neq R$ و $I\neq\{0\}$ آنگاه I را یک ایده آل سره R می نامیم.

توجه: همه زیرحلقه ها یک ایده آل نیستند مثلاً Z یک زیرحلقه $\mathbb{Q}$ است ولی Z ایده آل $\mathbb{Q}$ نیست چون $\frac{1}{2}\in\mathbb{Q}, 1\in Z$ ولی $\frac{1}{2}\times 1=\frac{1}{2}\notin Z$

مثال ۲: ایده آل های Z_{12} عبارتند از $\{\bar{0}\}$ و Z_{12} و $\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\bar{10}\}$ و $\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6},\bar{9}\}$ و $\langle\bar{4}\rangle=\{\bar{0},\bar{4},\bar{8}\}$ و $\langle\bar{6}\rangle=\{\bar{0},\bar{6}\}$

مثال ۳: زیرحلقه ای از $Z\times Z$ بیابید که ایده آل $Z\times Z$ باشد.

حل قراری دهیم که $I = \{(n,n) \mid n \in \mathbb{Z}\}$. I زیرحلقه $\mathbb{Z}\times\mathbb{Z}$ است ولی ایده‌آل $\mathbb{Z}\times\mathbb{Z}$ نیست. برای ایده‌آل نبودن داریم

$(1,3) \in \mathbb{Z}\times\mathbb{Z}$ و $(2,2) \in I$ $\quad (1,3)(2,2) = (2,6) \notin I$

قضیه ۱: اگر R یک حلقه یکدار باشد و N ایده‌آلی از R شامل یک یکال باشد آنگاه $N = R$.

اثبات: فرض کنید که N ایده‌آلی از R باشد که شامل عضوی از R باشد که یکال است و در N قرار دارد. چون N ایده‌آل است پس $\forall r \in R \quad ru \in N$ و $ur \in N$، حال با فرض $u' = r$ بنابراین $u = uu' = u'u \in N$ پس $1 \in N$

بنابراین $\forall a \in R : a = a.1 \in N$ یعنی $R \subseteq N$ پس $N = R$.

نتیجه: یک میدان ایده‌آلی نابدیهی و واقعی (محض - سره) ندارد.

اثبات: چون اعضای ناصفر میدان یکال می‌باشند و بنابراین هر ایده‌آل آن شامل یک یکال است پس این ایده‌آل طبق قضیه قبل برابر میدان می‌شود. (نابدیهی)

قضیه ۲: فرض کنید که $\{I_j \mid j \in J\}$ خانواده‌ای از ایده‌آل‌های حلقه R باشند در این صورت $\bigcap_{j\in J} I_j$ یک ایده‌آل در R است.

اثبات: چون هر I_j برای هر $j \in J$ یک ایده‌آل حلقه R است پس $\bigcap_{j\in J} I_j$ زیرحلقه R هم هست و بنابراین $\bigcap_{j\in J} I_j = I$ زیرحلقه R می‌باشد. برای ایده‌آل بودن $I = \bigcap_{j\in I} I_j$: فرض کنید که $\forall a \in R, \forall b \in I$

$$b \in I \Rightarrow b \in I_j \ (\forall j \in J) \Rightarrow ab \ \& \ ba \in I_j \Rightarrow ab, ba \in \bigcap_{j\in J} I_j \Rightarrow I \trianglelefteq R$$

توجه: فرض کنید که R یک حلقه و I یک ایده‌آل از R باشد فرض کنید که $(R/I, +)$ گروه خارج قسمتی $(R,+)$ بر $(I,+)$ باشد [چون $(R,+)$ یک گروه آبلی است پس $(I,+)$ زیرگروه نرمال $(R,+)$ است و بنابراین $(R/I, +)$ یک گروه خارج قسمتی جبری است] روی مجموعه R/I عمل ضرب را اینطور تعریف می‌کنیم

$$(a+I)(b+I) = ab + I \qquad \forall (a+I), (b+I) \in R/I$$

در این صورت قضیه زیر را داریم:

قضیه ۳: فرض کنید که R یک حلقه باشد و I یک ایده‌آل در R باشد. در این صورت مجموعه R/I نسبت به اعمال جمع همدسته‌ها و ضرب بالا یک حلقه است. اگر R جابجایی باشد آنگاه R/I جابجایی است و اگر R یکدار باشد آنگاه R/I یکدار است. عمل جمع همدسته‌ها به صورت زیر است

$$(a+I) + (b+I) = (a+b) + I \qquad \forall a+I, b+I \in R/I$$

اثبات، میدانیم است که $(R,+)$ یک گروه آبلی است پس گروه خارج قسمتی $(R/I,+)$ نیز گروه آبلی است. باید نشان دهیم که عمل ضرب خوش تعریف است. یعنی با انتخاب نمایندگان مختلف همسته‌ها یکسان نماند. پس فرض کنید $a_1+I=a_2+I$ و $b_1+I=b_2+I$ در این صورت $a_1-a_2\in I$ و $b_1-b_2\in I$ پس عناصری مانند $i_1,i_2\in I$ وجود دارند که $a_1-a_2=i_1$ و $b_1-b_2=i_2$ پس $a_1=a_2+i_1$ و $b_1=b_2+i_2$

$$a_1b_1=(a_2+i_1)(b_2+i_2)=a_2b_2+\underbrace{a_2i_2+i_1b_2+i_1i_2}_{i_3}=a_2b_2+i_3$$

زیرا I ایده‌آل است، $a_2i_2\in I$ و $i_1b_2\in I$ پس $i_1i_2\in I$ بنابراین $i_3=a_2i_2+i_1b_2+i_1i_2\in I$ پس $a_1b_1-a_2b_2\in I$ بنابراین $a_1b_1+I=a_2b_2+I$.

اثبات شرکت پذیری ضرب همسته‌ها I و توزیع پذیری ضرب روی جمع به عنوان تمرین در نظر گرفته می‌شود. بنابراین $(R/I,+,\cdot)$ یک حلقه است. اگر R جابجایی باشد آنگاه

$$\forall\, a+I,b+I\in R/I \qquad (a+I)(b+I)=ab+I=ba+I=(b+I)(a+I)$$

یعنی R/I جابجایی است و اگر $1\in R$ آنگاه $1+I\in R/I$ عضو خنثی ضربی حلقه R/I است زیرا

$$\forall\, a+I\in R/I \qquad (a+I)(1+I)=a.1+I=a+I=1.a+I=(1+I)(a+I)$$

یعنی R/I یکدار است.

تعریف، اگر R یک حلقه باشد و I ایده‌آلی از R باشد آنگاه حلقه R/I را حلقه خارج قسمتی R بر I می‌نامیم

مثال ۳: چون $n\mathbb{Z}\trianglelefteq\mathbb{Z}$ برای هر $n\in\mathbb{N}$ (n عدد صحیح مثبت) پس $\frac{\mathbb{Z}}{n\mathbb{Z}}$ یک حلقه خارج قسمتی است.

مثال ۵: دیدیم که $\langle 6\rangle=\{\dots,-12,-6,0,6,12,\dots\}$ ایده‌آل $\mathbb{Z}_{12}$ است پس $\frac{\mathbb{Z}_{12}}{\langle 6\rangle}$ یک حلقه خارج قسمتی است.

مثال ۶: دیدیم که $\mathbb{Z}$ یک ایده‌آل $\mathbb{Q}$ نیست پس $\frac{\mathbb{Q}}{\mathbb{Z}}$ تعریف نشده است یعنی حلقه خارج قسمتی $\frac{\mathbb{Q}}{\mathbb{Z}}$ تعریف نمی‌شود.

مثال ۷: $\mathbb{Z}\times\{0\}$ و $\{0\}\times\mathbb{Z}$ دو ایده‌آل $\mathbb{Z}\times\mathbb{Z}$ است بنابراین $\frac{\mathbb{Z}\times\mathbb{Z}}{\mathbb{Z}\times\{0\}}$ و $\frac{\mathbb{Z}\times\mathbb{Z}}{\{0\}\times\mathbb{Z}}$ دو حلقه خارج قسمتی است. در آینده ثابت می‌کنیم که این دو حلقه با حلقه $\mathbb{Z}$ ایزومورف هستند.

در این مثال، باقی ایده‌آل‌های $\mathbb{Z}\times\mathbb{Z}$ به صورت $n\mathbb{Z}\times m\mathbb{Z}$ و $\{0\}\times n\mathbb{Z}$ و $n\mathbb{Z}\times\{0\}$ هستند که در آن m و n دو عدد صحیح نامنفی است بنابراین $\frac{\mathbb{Z}\times\mathbb{Z}}{n\mathbb{Z}\times m\mathbb{Z}}$ و $\frac{\mathbb{Z}\times\mathbb{Z}}{\{0\}\times m\mathbb{Z}}$ و $\frac{\mathbb{Z}\times\mathbb{Z}}{n\mathbb{Z}\times\{0\}}$ حلقه‌های خارج قسمتی هستند.

تمرین ۱ (ایده‌آل‌ها و حلقه‌های خارج قسمتی)

۱- فرض کنید که A یک مجموعه باشد و $(\mathcal{P}(A), \Delta, \cap)$ و $B \subseteq A$. ثابت کنید که $(\mathcal{P}(B), \Delta, \cap)$ ایده‌آلی از $(\mathcal{P}(A), \Delta, \cap)$ است.

۲- در تمرین ۱ حلقه خارج قسمتی $\frac{\mathcal{P}(A)}{\mathcal{P}(B)}$ را برای $A = \{1,2,3\}$ و $B = \{2,3\}$ بسازید.

۳- اگر R یک حلقه جابجایی و یکدار باشد و تنها دو ایده‌آل 0 و R داشته باشد ثابت کنید که R یک میدان است (راهنمایی برای هر x از R، مجموعه $\{rx \mid r \in R\}$ را بررسی کنید.)

۴- فرض کنید که R حلقه‌ای جابجایی باشد و $a \in R$. نشان دهید که $I_a = \{x \in R \mid ax = 0\}$ ایده‌آلی از R است.

۵- عضو a از حلقه‌ای چون R را هیچ‌توان (پوچ‌توان) نامیم هرگاه $\exists n \in \mathbb{Z}^+ ; a^n = 0$

نشان دهید که مجموعه تمام اعضای هیچ‌توان (پوچ‌توان) حلقه جابجایی R یک ایده‌آل R است. این ایده‌آل را رادیکال R می‌نامیم و با $\sqrt{R} = Rad(R)$ نمایش می‌دهیم. یعنی $\sqrt{R} = \{a \in R \mid \exists n \in \mathbb{Z}^+ . a^n = 0\}$

۶- با توجه به تمرین ۵، $\sqrt{\mathbb{Z}_{12}}$ و $\sqrt{\mathbb{Z}}$ و $\sqrt{\mathbb{Z}_{32}}$ را بدست آورید.

۷- اگر R حلقه تعویض‌پذیر باشد و $N = \sqrt{R}$. نشان دهید که $\sqrt{R/N} = \{0+N\}$.

۸- فرض کنید که R حلقه‌ای تعویض‌پذیر باشد و I ایده‌آلی از R باشد. نشان دهید که اگر هر عضو I عضو هیچ‌توان باشد و $\sqrt{R/I} = R/I$ آنگاه $\sqrt{R} = R$.

۹- فرض کنید که اگر R حلقه تعویض‌پذیر باشد و I ایده‌آلی از R باشد. نشان دهید که $\sqrt{I}$ شامل تمام اعضای a چون a که به ازای عددی مانند $n \in \mathbb{Z}^+$ و $a^n \in I$ ایده‌آلی از R است یعنی $\sqrt{I} = \{a \in R \mid a^n \in I \ \exists n \in \mathbb{Z}^+\}$

۱۰- اگر R حلقه جابجایی باشد چه رابطه‌ای بین $\sqrt{I}$ و $\sqrt{R/I}$ وجود دارد آن رابطه را بیان کنید. (I ایده‌آلی از R است)

۱۱- فرض کنید که R یک حلقه باشد و A و B دو ایده‌آل R باشند. نشان دهید که $A+B$ ایده‌آلی از R است که در آن $A+B = \{a+b \mid a \in A, b \in B\}$

همچنین نشان دهید که $A \subseteq A+B$ و $B \subseteq A+B$

۱۲- فرض کنید که A و B دو ایده‌آل حلقه R باشند. نشان دهید که AB یک ایده‌آل R است که در آن $AB = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}^+\}$

همچنین نشان دهید که $AB \subseteq A \cap B$.

۱۳- فرض کنید که A و B دو ایده‌آل از حلقه جابجایی R باشند نشان دهید که $A:B$ ایده‌آل R است در آن

$$A:B=\{r\in R \mid rb\in A \ \forall b\in B\}$$

۱۴- نشان دهید که $I=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a,b\in\mathbb{R}\right\}$ یک ایده‌آل راست از $Mat_{2\times 2}(\mathbb{R})$ است ولی ایده‌آل چپ نیست.

۱۵- نشان دهید که حلقه $Mat_{2\times 2}(\mathbb{Z}_2)$ یک حلقه ساده است یعنی $Mat_{2\times 2}(\mathbb{Z}_2)$ ایده‌آل نابدیهی و واقعی ندارد.

۱۶- (در تمرین ۴) اگر R حلقه جابجایی باشد و $a\in R$ نشان دهید که $I_a=\{x\in R \mid ax=0\}$ یک ایده‌آل راست R است و $I_a=\{x\in R \mid xa=0\}$ ایده‌آل چپ راست است.

۱۷- فرض کنید که R یک حلقه باشد و $Z(R)$ مرکز حلقه R باشد نشان دهید که در حالت کلی $Z(R)$ یک ایده‌آل R نیست (راهنمایی $Z(Mat_{2\times 2}(\mathbb{R}))$ را بررسی کنید.)

۱۸- ثابت کنید که $Mat_{2\times 2}(\mathbb{R})$ تنها دارای دو ایده‌آل $\{0\}$ و $Mat_{2\times 2}(\mathbb{R})$ می‌باشد.

۱۹- فرض کنید که R یک حلقه باشد و I ایده‌آلی از R باشد نشان دهید که مجموعه $R(I)=\{x\in R) \ rx\in I, \forall r\in R\}$ یک ایده‌آل R شامل I است.

۲۰- فرض کنید که R یک حلقه با شد که در آن عمل ضرب بصورت $\forall a,b\in R: ab=0$ تعریف می‌شود ثابت کنید که هر زیرگروه $(R,+)$ یک ایده‌آل در R است.

۲۱- فرض کنید که R یک حلقه و a عضو یوچوان از R باشد ثابت کنید که a وارون ضربی ندارد ولی عضو $1-a$ وارون ضربی دارد.

همریختی ها و یکریختی های حلقه (هموومورفیسم ها و ایزومورفیسم های حلقه)

تعریف: فرض کنید که R و R' دو حلقه باشند. تابع $f: R \longrightarrow R'$ را یک همریختی (هموومورفیسم) حلقه‌ای از R به R' نامیم هرگاه: الف) $f(a+b) = f(a) + f(b)$ $\forall a,b \in R$

ب) $f(a \cdot b) = f(a) \cdot f(b)$

به عبارت دیگر تابع f را یک هموومورفیسم جمعی و هم هموومورفیسم ضربی نامند.

مثال ۱: تابع $\phi: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ با ضابطه $\phi(n) = (n, n)$ یک هموومورفیسم است زیرا

$$\forall n,m \in \mathbb{Z} : \phi(n+m) = (n+m, n+m) = (n,n) + (m,m) = \phi(n) + \phi(m)$$

$$\phi(nm) = (nm, nm) = (n,n)(m,m) = \phi(n) \cdot \phi(m)$$

مثال ۲: تابع $f: \mathbb{Z} \longrightarrow \mathbb{Z}_m$ با ضابطه $\forall a \in \mathbb{Z} : f(a) = \overline{a}$ یک هموومورفیسم است. زیرا

$$\forall n,l \in \mathbb{Z} \quad f(n+l) = \overline{n+l} = \overline{n} \oplus \overline{l} = f(n) \oplus f(l)$$

$$f(nl) = \overline{nl} = \overline{n} \odot \overline{l} = f(n) \odot f(l)$$

مثال ۳: تابع $f: \mathbb{C} \longrightarrow Mat_{2\times 2}(\mathbb{R})$ با ضابطه $\forall (a+ib) \in \mathbb{C} \quad f(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ یک هموومورفیسم است زیرا

$$\forall (a+ib), (c+id) \in \mathbb{C}$$

$$f(a+ib+c+id) = f(a+c+i(b+d)) = \begin{bmatrix} a+c & b+d \\ -b-d & a+c \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} =$$

$$= f(a+ib) + f(c+id)$$

$$f((a+ib)(c+id)) = f(ac-bd+i(ad+bc)) = \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix} =$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = f(a+ib)\, f(c+id)$$

قضیه ۱: فرض کنید که I ایده‌آلی از حلقه R باشد. نگاشت طبیعی (کانونی) $\sigma: R \longrightarrow \frac{R}{I}$ با تعریف $\forall a \in R : \sigma(a) = a + I$ یک هموومورفیسم است این هموومورفیسم را هموومورفیسم طبیعی (کانونی) ناظم

اثبات: $\forall a,b \in R \quad \sigma(a+b) = (a+b) + I = (a+I) + (b+I) = \sigma(a) + \sigma(b)$

$$\sigma(ab) = ab + I = (a+I)(b+I) = \sigma(a)\sigma(b)$$

(این هموومورفیسم پوشا است)

تعریف: اگر R و R' دو حلقه باشند و $f: R \longrightarrow R'$ یک هموومورفیسم باشد هسته f یا $\ker f$ را مجموعه $\ker f = \{a \in R \mid f(a) = 0'\}$ که $0'$ صفر جمعی حلقه R' است

قضیه ۲: فرض کنید که $\phi : R \longrightarrow R'$ یک همومورفیسم باشد.

الف) $\phi(0) = 0'$ ب) $\forall a \in R \quad \phi(-a) = -\phi(a)$

ج) اگر S زیرحلقه‌ای از R باشد آنگاه $\phi(S)$ زیرحلقه‌ای از R' است که در آن $\phi(S) = \{\phi(a) \mid a \in S\}$

د) اگر S' زیرحلقه‌ای از R' باشد آنگاه $\phi^{-1}(S')$ زیرحلقه‌ای از R است که در آن $\phi^{-1}(S') = \{a \mid \phi(a) \in S'\}$

ر) اگر I ایده‌آلی از حلقه R باشد آنگاه $\phi(I)$ ایده‌آلی از $\phi(R)$ است

ز) اگر I' ایده‌آلی از $\phi(R)$ باشد آنگاه $\phi^{-1}(I')$ ایده‌آلی از حلقه R است.

س) اگر R میدان باشد و $\phi(1) \neq 0'$ آنگاه $\phi(1) = 1'$ واحد $\phi(R)$ است

اثبات: الف) $\phi(0) = 0'$ جمعی $\Longrightarrow$ قاعده حذف $\phi(0+0) = \phi(0) + \phi(0) = \phi(0)$

ب) یکتایی قرینه جمعی $\Rightarrow \phi(a) = -\phi(a)$

$$\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0)$$
$$\phi(-a) + \phi(a) = \phi(-a + a) = \phi(0)$$

اثبات ج) طبق الف $0 = \phi(0) \in \phi(S)$.

$\forall \phi(a), \phi(b) \in \phi(S)$

$\phi(a) - \phi(b) = \phi(a-b) \Rightarrow \phi(a) - \phi(b) \in \phi(S)$ زیرا $a - b \in S$:

$\phi(a)\phi(b) = \phi(ab) \Longrightarrow \phi(ab) \in \phi(S)$ زیرا $ab \in S$

بنابراین $\phi(S)$ زیرحلقه R' است.

اثبات د): چون $\phi(0) = 0' \in S'$ پس $0 \in \phi^{-1}(S')$

$\forall a, b \in \phi^{-1}(S') \Rightarrow \phi(a), \phi(b) \in S' \Rightarrow \phi(a) - \phi(b) = \phi(a-b) \in S' \Rightarrow a - b \in \phi^{-1}(S')$

$\phi(a)\phi(b) = \phi(ab) \in S' \Rightarrow ab \in \phi^{-1}(S') \Longrightarrow$ $\phi^{-1}(S')$ زیرحلقه R است.

اثبات ر): $\forall \phi(a) \in \phi(I), \forall \phi(r) \in \phi(R) \Rightarrow \phi(a)\cdot\phi(r) = \phi(ar) \in \phi(I)$

چون $ar \in I$: $a \in I, r \in R$ زیرا $\phi(a) \in \phi(I), \phi(r) \in \phi(R)$

$\phi(r)\phi(a) = \phi(ra) \in \phi(I)$ زیرا $ra \in I$ چون $r \in R, a \in I$ پس :

همچنین حلقه بودن $\phi(I)$ از ج نتیجه می‌شود.

اثبات ز) $\forall r \in R, \forall a \in \phi^{-1}(I') \Rightarrow \phi(r) \in \phi(R), \phi(a) \in I' \Longrightarrow$ ایده‌آل بودن I' $\begin{cases} \phi(r)\phi(a) \in I' \\ \phi(a)\phi(r) \in I' \end{cases}$

بنابراین چون $\phi(r)\phi(a) = \phi(ra)$ ، $\phi(a)\phi(r) = \phi(ar)$ پس $ar \in \phi^{-1}(I')$ ، $\forall a$ یعنی $\phi^{-1}(I')$ ایده‌آل R است (زیرحلقه بودن $\phi^{-1}(I')$ از ج) نتیجه می‌شود

اثبات س) اگر حلقه R میدان باشد ، $1 \in R$ ، $\phi(1) \neq 0'$ آنگاه $\phi(1) \in \phi(R)$ عضو خنثی ضرب است زیرا

$\forall \phi(a) \in \phi(R) \quad \phi(a)\phi(1) = \phi(a1) = \phi(a)$

$\phi(1)\phi(a) = \phi(1a) = \phi(a)$

یعنی $\phi(R)$ میدان است.

تبصره ۱: در قضیه قبل در صورت یکدار بودن حلقه R لازم نیست که حلقه R' یکدار باشد. برای نمونه می‌توان

$\phi: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ تحت تابع ϕ یک همومورفیسم است ولی $\phi(1) = (1,0)$ عضو خنثی

$\phi(n) = (n,0) \quad \forall n \in \mathbb{Z}$

ضرب $\phi(\mathbb{Z})$ است ولی عضو خنثی ضرب $\mathbb{Z} \times \mathbb{Z}$ نیست زیرا عضو خنثی ضرب $\mathbb{Z} \times \mathbb{Z}$ عبارت است از $(1,1)$.

تبصره ۲: در قضیه قبل فرض ۱) لازم نیست که $\phi(I)$ ایده‌آلی از R' باشد. برای نمونه می‌توان در مثال (الف) نشان داد که $\phi: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ $\phi(n) = (n,n)$ ایده‌آلی از $\mathbb{Z}$ است ولی $\phi(2\mathbb{Z})$ ایده‌آلی از $\mathbb{Z} \times \mathbb{Z}$ نیست زیرا

$\phi(2\mathbb{Z}) = \{(2n, 2n) \mid n \in \mathbb{Z}\}$

$(1,2)(4,4) = (4,8) \notin \phi(2\mathbb{Z})$

$(4,4) \in \phi(2\mathbb{Z})$ و $(1,2) \in \mathbb{Z} \times \mathbb{Z}$

تبصره ۳: طبق قضیه قبل $\ker\phi$ ایده‌آلی از حلقه R است زیرا طبق قسمت (ب) قضیه قبل $\ker\phi = \phi^{-1}(\{0'\})$ ایده‌آل R است.

البته مورد (ب) با صورت مستقیم هم ثابت می‌شود که $\ker\phi$ ایده‌آلی از R است (مثال زیر)

مثال ۴: اگر $\phi: R \longrightarrow R'$ یک همومورفیسم باشد و R یا R' دو حلقه باشند آنگاه ثابت کنید که $\ker\phi$ ایده‌آلی از R است.

حل: $\ker\phi = \{a \in R \mid \phi(a) = 0'\}$ ثابت می‌کنیم که $\ker\phi$ زیرحلقه R است و

$\forall a \in \ker\phi, \forall r \in R \quad ra, ar \in \ker\phi$

زیرحلقه‌ی است:

$\phi(0) = 0' \Rightarrow 0 \in \ker\phi$.

$\forall a,b \in \ker\phi \Rightarrow \phi(a) = 0, \phi(b) = 0 \Rightarrow 0 = \phi(a) - \phi(b) = \phi(a-b) \Rightarrow a-b \in \ker\phi$

$0 = \phi(a)\phi(b) = \phi(ab) \Rightarrow ab \in \ker\phi$

$\forall a \in \ker\phi, \forall r \in R \quad \phi(a) = 0 \quad 0 = \phi(r)\phi(a) = \phi(ra) \Rightarrow ra \in \ker\phi$

$0 = \phi(a)\phi(r) = \phi(ar) \Rightarrow ar \in \ker\phi$

تعریف: فرض کنید که $f: R \longrightarrow R'$ یک همومورفیسم باشد و R یا R' دو حلقه هستند در این صورت

الف) اگر f یک به یک باشد آنگاه f را یک منومورفیسم (تکریختی) حلقه‌ای می‌نامیم.

ب) اگر f پوشا باشد آنگاه f را یک اپی‌مورفیسم (برورریختی) حلقه‌ای می‌نامیم.

ج) اگر f دوسویی باشد آنگاه f را یک ایزومورفیسم (یکریختی) حلقه‌ای می‌نامیم و می‌نویسیم $R \cong R'$

مثال ۵: در مثال ۱: $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ با ضابطه $\phi(n)=(n,n)$ پوشا نیست پس ϕ یکریختی نیست و در مثال ۲: $f: \mathbb{Z} \longrightarrow \mathbb{Z}_m$ با ضابطه $f(a)=\bar{a}$ یک یک نیست زیرا $f(m)=f(2m)=0$ ولی $m \neq 2m$ پس f ایزومورفیسم حلقه‌ای نیست.

در مثال ۳: تابع $f: \mathbb{C} \longrightarrow M_{2\times 2}(\mathbb{R})$ با ضابطه $f(a+ib)=\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ پوشا نیست پس f یک ایزومورفیسم حلقه‌ای نیست.

قضیه ۳: هومومورفیسم حلقه $\phi: R \longrightarrow R'$ یک منومورفیسم (یکریختی) است اگر و فقط اگر $\ker\phi=\{0\}$

اثبات: فرض کنید که ϕ یک منومورفیسم باشد و $a \in \ker\phi$ پس $\phi(a)=0$ (زیرا عضوی در دامنه است که $\phi(0)=0$) پس $\phi(a)=\phi(0)$ چون ϕ یک یک است پس $a=0$ یعنی $\ker\phi=\{0\}$.

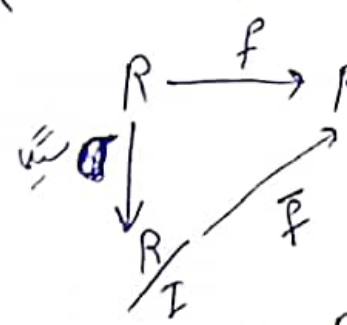
حال فرض کنید که $\ker\phi=\{0\}$ و $f(a)=f(b)$ پس $0=f(a)-f(b)=f(a-b)$ یعنی $a-b \in \ker f$ پس $a-b=0$ یعنی $a=b$.

قضیه ۴: فرض کنید که $f: R \longrightarrow R'$ یک هومومورفیسم حلقه‌ای باشد. فرض کنید که I ایده‌آلی از حلقه R باشد که در هسته f باشد (یعنی $I \subseteq \ker f$). در این صورت هومومورفیسم حلقه‌ای یکتایی مانند $\bar{f}: R/I \longrightarrow R'$ وجود دارد بطوریکه $\forall a \in R \quad \bar{f}(a+I)=f(a)$ و $\operatorname{Im}\bar{f}=R_{\bar{f}}=R_f=\operatorname{Im} f$ و $\ker\bar{f}=\frac{\ker f}{I}$.

بعلاوه $\bar{f}$ یک یکریختی است اگر و فقط اگر f پوشا باشد و $I=\ker f$.

اثبات: (این قضیه را برای حلقه‌ها ثابت می‌کنیم که برای گروه‌ها نیز ثابت شده است)

خوشتعریفی $\bar{f}$: اگر $a+I=b+I$ آنگاه $a-b \in I$ پس چون $I \subseteq \ker f$ پس $a-b \in \ker f$ پس $f(a-b)=0$ بنابراین $f(a)=f(b)$ یعنی $\bar{f}(a+I)=\bar{f}(b+I)$.



$\bar{f}$ هومومورفیسم است زیرا

$\forall a+I, b+I \in \frac{R}{I}$

$\bar{f}((a+I)+(b+I))=\bar{f}((a+b)+I)=f(a+b)=f(a)+f(b)=\bar{f}(a+I)+\bar{f}(b+I)$

$\bar{f}((a+I)\cdot(b+I))=\bar{f}(ab+I)=f(ab)=f(a)f(b) \Rightarrow \bar{f}(a+I)\cdot\bar{f}(b+I)$

بدیهی است که $\operatorname{Im}\bar{f}=\{\bar{f}(a+I) \mid a \in R\}=\{f(a) \mid a \in R\}=\operatorname{Im} f$

$\ker\bar{f} = \{a+I \mid \bar{f}(a+I)=0'\} = \{a+I \mid f(a)=0'\} = \{a+I \mid a\in\ker f\} = \frac{\ker f}{I}$

⊛ $\bar{f}$ یکتا است زیرا کاملاً توسط f معین می‌شود.

⊛ $\bar{f}$ پوشا است اگر و فقط اگر f پوشا باشد و $\bar{f}$ یک‌به‌یک است اگر و فقط اگر $\ker f = \{I\}$ پس طبق مطالب بالا

$\bar{f}$ یک‌به‌یک است اگر و فقط اگر $\ker f = I$، پس می‌توان گفت که $\bar{f}$ یک ایزومورفیسم است اگر و فقط اگر f پوشا باشد و $\ker f = I$.

قضیه ۵ (قضیه اول یکریختی): اگر $f: R \longrightarrow R'$ یک هم‌مورفیسم حلقه‌ای باشد آنگاه f یک یکریختی حلقه‌ای $\frac{R}{\ker f} \cong R_f = \mathrm{Im} f$ القا می‌کند.

اثبات: چون $f: R \longrightarrow R'$ یک هم‌مورفیسم حلقه‌ای است پس $f: R \longrightarrow \mathrm{Im} f$ پوشا است بنابراین طبق قضیه قبل (قسمت علاوه (قسمت آخر قضیه)) این هم‌مورفیسم پوشا یک یکریختی (ایزومورفیسم) $\bar{f}: \frac{R}{\ker f} \longrightarrow R_f$ القا می‌کند (زیرا $I = \ker f$) یعنی $\frac{R}{\ker f} \cong R_f$

$\bar{f}(a+\ker f) = f(a)$

تتمیم: اگر $f: R \longrightarrow R'$ یک هم‌مورفیسم حلقه‌ای باشد و I ایده‌آلی در R باشد و J ایده‌آلی در R' باشد بطوریکه $f(I) \subseteq J$ آنگاه f یک هم‌مورفیسم حلقه‌ای $\bar{f}: \frac{R}{I} \longrightarrow \frac{R'}{J}$ با ضابطه $\bar{f}(a+I) = f(a)+J$ القا می‌کند.

و $\bar{f}$ یک ایزومورفیسم است اگر و فقط اگر $\mathrm{Im} f + J = R'$ و $I \subseteq f^{-1}(J)$.

بویژه اگر f پوشا باشد بطوریکه $f(I) = J$ و $\ker f \subseteq I$ آنگاه $\bar{f}$ یک ایزومورفیسم است.

اثبات: ترکیب هم‌مورفیسم‌های $R \xrightarrow{f} R' \xrightarrow{\sigma} \frac{R'}{J}$ در نظر می‌گیریم که در آن $\sigma: R' \longrightarrow \frac{R'}{J}$ هم‌مورفیسم طبیعی (کانونی) است (قضیه ۱) یعنی هم‌مورفیسم $g: R \longrightarrow \frac{R'}{J}$

$\forall a\in R: \ g(a) = \sigma(f(a)) = f(a)+J$

طبق قضیه ۴ این هم‌مورفیسم g یک هم‌مورفیسم حلقه یکتای $\bar{g}: \frac{R}{I} \longrightarrow \frac{R'}{J}$ یا ضابطه $\bar{g}(a+I) = g(a)$ القا می‌کند یعنی $\forall a+I \in \frac{R}{I}$ $g\cdot\bar{g}(a+I) = g(a) = f(a)+J$

و $\mathrm{Im}\bar{g} = R_{\bar{g}} = R_g = \mathrm{Im} g$. با قرار دادن $\bar{g} = \bar{f}$ قسمت اول قضیه اثبات می‌شود یعنی $\bar{f}: \frac{R}{I} \longrightarrow \frac{R'}{J}$ با ضابطه $\bar{f}(a+I) = f(a)+J$ تحقق می‌شود.

⊛ $\ker g = \ker(\sigma f) = \{a\in R \mid \sigma(f(a)) = J\} = \{a\in R \mid f(a)+J = J\} = \{a\in R \mid f(a)\in J\}$

از طرفی چون $f(I) \subset J$ پس طبق (*) $I \subseteq f^{-1}(J) = \ker(\sigma f)$

حال $\bar{f} = \bar{g}$ یک ایزومورفیسم است اگر و فقط اگر $g = \sigma f$ پوشا باشد (طبق قضیه ۴) و $I = \ker(\sigma f)$

اما $I = \ker(\sigma f)$ اگر و فقط اگر $R' = R_f + J$ و $f^{-1}(J) \subseteq I$ پس قسمت دوم نتیجه هم تحقق می‌شود.

برای قسمت سوم نتیجه (قسمت بویژه) اگر f پوشا باشد و $f(I) = J$ و $\ker f \subseteq I$ در این صورت $\operatorname{Im} f = R'$ چون پوشا است و $f^{-1}(J) \subseteq I$ پس طبق قسمت دوم نتیجه $\bar{f}$ یک ایزومورفیسم می‌شود.

قضیه ۶: فرض کنید که R یک حلقه و I ایده‌آلی از R باشد. در این صورت یک همومورفیسم پوشا (بروریختی ایی‌سورفیسم) $f: R \longrightarrow \frac{R}{I}$ وجود دارد که $\ker f = I$. در قضیه ۱

اثبات: این قضیه همان قضیه ۱ است و f همان σ است. کافی است نشان دهیم که σ پوشا است.

$$\forall a+I \in \frac{R}{I} \quad \exists a \in R \ ; \ \sigma(a) = a+I$$ بدلیل پوشا بودن

قضیه ۷ (قضیه دوم ایزومورفیسم) فرض کنید که I و J دو ایده‌آل از حلقه R باشند در این صورت

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

اثبات: (این قضیه همان قضیه دوم ایزومورفیسم دیگر گروه‌ها است با این تفاوت بجای ضرب I J در گروه‌ها، در حلقه‌ها از جمع $I+J$ استفاده شده است.) طبق تمرین ۱۱ فصل قبل I یک ایده‌آل از $I+J$ است و چنانکه از این $\frac{I+J}{I}$ یک حلقه است. همچنین $I \cap J$ یک ایده‌آل از J است پس $\frac{J}{I \cap J}$ یک حلقه است

حال تابع $f: J \longrightarrow \frac{I+J}{I}$ با ضابطه $\forall a \in J \ ; \ f(a) = a+I$

f یک همومورفیسم حلقه‌ای است زیرا

$$\forall a,b \in J \quad f(a+b) = (a+b)+I = (a+I)+(b+I) = f(a)+f(b)$$
$$f(ab) = ab+I = (a+I)(b+I) = f(a)f(b)$$
$$\ker f = \{a \in J \mid f(a) = I\} = \{a \in J \mid a+I = I\} = \{a \in J \mid a \in I\} = I \cap J$$

$$\forall c \in \frac{I+J}{I} \quad c = (a+b)+I \quad a \in I, b \in J \Rightarrow \exists b \in J \ f(b) = c = b+I$$

زیرا $b+I = a+b+I$ (چون $a \in I$).

حال طبق قضیه اول ایزومورفیسم $\frac{J}{I \cap J} = \frac{J}{\ker f} \cong \frac{I+J}{I}$.

قضیه ۸ (قضیه سوم ایزومورفیسم) فرض کنید که I و J دو ایده‌آل از حلقه R باشند با شرطی که $I \subseteq J$ در این صورت

الف) $\frac{J}{I}$ یک ایده‌آل $\frac{R}{I}$ است ب) $\frac{R/I}{J/I} \cong \frac{R}{J}$.

اثبات الف) چون I و J هر دو ایده‌آل R هستند و $I \subseteq J$ پس I هم یک ایده‌آل از J است بنابراین $\frac{J}{I}$ یک حلقه خارج قسمتی است پس $\frac{J}{I}$ تعریف شده است همچنین $\frac{J}{I}$ زیرحلقه $\frac{R}{I}$ است چون $\frac{J}{I} \subseteq \frac{R}{I}$. برای ایده‌آل بودن:

$$\forall (r+I) \in \frac{R}{I}, \forall (a+I) \in \frac{J}{I}$$

$$(r+I)(a+I) = ra+I \in \frac{J}{I} \quad (ra \in J \text{ چون } J \text{ ایده‌آل } R \text{ است})$$

$$(a+I)(r+I) = ar+I \in \frac{J}{I} \quad (ar \in J \text{ چون } J \text{ ایده‌آل } R \text{ است})$$

حال نگاشت $f: \frac{R}{I} \longrightarrow \frac{R}{J}$ با ضابطه $f(a+I) = a+J$ $\forall (a+I) \in \frac{R}{I}$

در نظر می‌گیریم. f خوش‌تعریف است زیرا برای $a+I, b+I \in \frac{R}{I}$ اگر $a+I = b+I$ آنگاه $a-b \in I \subseteq J$ پس $a-b \in J$ یعنی $a+J = b+J$ و $f(a+I) = f(b+I)$.

f همومورفیسم حلقه‌ای است $\forall a+I, b+I \in \frac{R}{I}$

$$f((a+I)(b+I)) = f(ab+I) = ab+J = (a+J)(b+J) = f(a+I)\cdot f(a+J)$$

$$f((a+I)+(b+I)) = f((a+b)+I) = (a+b)+J = (a+J)+(b+J) = f(a+I)+f(b+J)$$

f پوشا است زیرا $\forall a+J \in \frac{R}{J} \quad \exists a+I \in \frac{R}{I} \ ; \ f(a+I) = a+J$

$$\ker f = \{a+I \mid f(a+I) = J\} = \{a+I \mid a+J = J\} = \{a+I \mid a \in J\} = \frac{J}{I}$$

بنابراین طبق قضیه اول ایزومورفیسم $\frac{R/I}{J/I} = \frac{R/I}{\ker f} \cong \frac{R}{J}$.

قضیه ۹: فرض کنید I یک ایده‌آل در حلقه R باشد. در این صورت یک تناظر یک به یک بین ایده‌آل‌های R که شامل I هستند و مجموعه ایده‌آل‌های $\frac{R}{I}$ (یعنی $J \longmapsto \frac{J}{I}$) وجود دارد. از این رو هر ایده‌آل در $\frac{R}{I}$ به صورت $\frac{J}{I}$ می‌باشد که در آن J ایده‌آلی در R است به قسمی که $I \subseteq J$.

اثبات. تابع $f: A \longrightarrow B$ با ضابطه $f(J) = \frac{J}{I}$ $\forall J \in A$ را در نظر می‌گیریم. [که در آن A = مجموعه تمام ایده‌آل‌های R شامل I و B = مجموعه تمام ایده‌آل‌های $\frac{R}{I}$ است]

f یک به یک است زیرا اگر $f(J) = f(L)$ که در آن L و J دو ایده‌آل از R هستند که شامل I هستند یعنی $I \subseteq J$ و $I \subseteq L$. بنابراین $\frac{J}{I} = \frac{L}{I}$ می‌توان نشان داد که $J = L$ (تمرین ۳۰) یعنی f یک به یک است. برای پوشا بودن f:

$$\forall \frac{J}{I} \in B \quad \exists J \in A : f(J) = \frac{J}{I}$$

پس f یک تابع دوسویی است پس دو مجموعه A و B هم‌اندازه هستند. یعنی A و B از نظر یک به یک هستند.

تمرین:

۱- فرض کنید که $Z(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in Z\}$ الف) نشان دهید که $Z(\sqrt{2})$ تحت جمع و ضرب معمولی یک حلقه است. ب) نشان دهید که $f: Z(\sqrt{2}) \longrightarrow Z(\sqrt{2})$ با ضابطه $f(a+b\sqrt{2}) = a-b\sqrt{2}$ یک هموومورفیسم پوشا است. ج) آیا f یک هموومورفیسم حلقه‌ای است.

۲- فرض کنید که $F = C(\mathbb{R}, \mathbb{R})$ مجموعه تمام توابع پیوسته حقیقی (یعنی از $\mathbb{R}$ تا $\mathbb{R}$) باشد:

الف) نشان دهید که $\phi: F \longrightarrow \mathbb{R}$ با ضابطه $\phi(f) = f(\frac{1}{2})$ $\forall f \in F$ یک هموومورفیسم حلقه‌ای است. ب) $\ker\phi$ را حساب کنید.

۳- فرض کنید که R یک حلقه باشد و I و J ایده‌آل‌های R باشند که $I \subseteq J \subseteq R$. اگر $\frac{R}{I} = \frac{R}{J}$ نشان دهید که $I = J$.

۴- یک حوزه صحیح R را با مشخصه صفر گوییم، اگر رابطه $ma = 0$ برای هر عضو a غیر صفر از R و عدد صحیح m تنها وقتی برقرار باشد که $m = 0$. و R را با مشخصه غیر صفر نامند اگر با ازای یک عضو غیر صفر a از R و عدد صحیح غیر صفر m وجود داشته باشد بقسمی که $ma = 0$، در این صورت کوچکترین عدد صحیح مثبت n را بطوری که $na = 0$ با ازای یک عضو غیر صفر a از R، مشخصه R می نامند.

الف) ثابت کنید که اگر R با مشخصه n باشد، آنگاه با ازای هر a از R $na = 0$ (راهنمایی: از الگوریتم تقسیم استفاده کنید که $n = qn + r$ $0 \le r < n$).

ب) ثابت کنید که مشخصه یک حوزه صحیح یا صفر است یا عددی اول می باشد.

۵- فرض کنید که k یک عدد صحیح ثابت بزرگتر از ۱ باشد. اگر $f: Z \longrightarrow Z$ با ضابطه $f(n) = kn$ $\forall n \in Z$ ثابت کنید که f یک هموومورفیسم حلقه‌ای نیست.

۶- اگر $f: Z \longrightarrow Z$ یک هموومورفیسم حلقه‌ای باشد، ثابت کنید که یا f هموومورفیسم صفر است یا هموومورفیسم همانی.

۷- الف) نشان دهید که $L = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a,b \in \mathbb{R} \right\}$ یک حلقه است.

ب) اگر $f: L \longrightarrow \mathbb{R}$ با ضابطه $f\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = a$ ثابت کنید که f یک هموومورفیسم حلقه‌ای است. ج) هسته f را پیدا کنید.

۸- فرض کنید R یک حلقه جابجایی یکدار با مشخصه عدد اول p باشد، ثابت کنید که تابع $f: R \longrightarrow R$ با ضابطه $f(r) = r^p$ برای هر $r \in R$ یک هموومورفیسم حلقه‌ای است.

۹- فرض کنید که F یک میدان و R یک حلقه باشد. فرض کنید $f: F \longrightarrow R$ یک هموومورفیسم پوشا حلقه‌ای باشد، ثابت کنید که $R = \{0\}$ و $R = F$.

۱۰- فرض کنید $f: Z \longrightarrow F$ یک هموومورفیسم پوشا باشد که F یک میدان است، ثابت کنید که F با میدانی از مرتبه عددی اول یکریخت است.

۱۱- فرض کنید که R حلقه‌ای یکدار با واحد ۱ باشد، آنگاه نگاشت $\phi: Z \longrightarrow R$ با تعریف $\phi(n) = n \cdot 1$ $\forall n \in Z$ یک هموومورفیسم حلقه‌ای است. (نشان دهید)

ایده‌آل‌های اول و ماکسیمال و میدان‌های اول

تعریف: فرض کنید که R یک حلقه باشد. ایده‌آل M از حلقه R را یک ایده‌آل ماکسیمال نامیم هرگاه ایده‌آل واقعی (محض) مانند N از R وجود نداشته باشد که طور واقعی شامل M باشد. یا عبارت دیگر ایده‌آلی از R مانند N موجود نباشد که $M \subset N \subset R$. اگر $M \subseteq N \subseteq R$ آنگاه $N = R$ یا $N = M$.

مثال ۱) $2\mathbb{Z}$ یک ایده‌آل ماکسیمال $\mathbb{Z}$ است زیرا $\mathbb{Z}$ هیچ ایده‌آلی بین $\mathbb{Z}$ و $2\mathbb{Z}$ ندارد. یا همین صورت $3\mathbb{Z}$ و $5\mathbb{Z}$ ایده‌آل‌های ماکسیمال $\mathbb{Z}$ است. ولی $4\mathbb{Z}$ ایده‌آل ماکسیمال $\mathbb{Z}$ نیست زیرا $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$ یعنی بین $\mathbb{Z}$ و $4\mathbb{Z}$ ایده‌آل محض $2\mathbb{Z}$ از $\mathbb{Z}$ وجود دارد.

توجه: با کمک قضیه زیر می‌توان ایده‌آل‌های ماکسیمال از یک حلقه جابجایی و یکدار R را شناخت. ایده‌آل ماکسیمال در حلقه‌ها مانند زیرگروه نرمال ماکسیمال در گروه‌ها است.

قضیه ۱: فرض کنید که R حلقه تعویض‌پذیر و یکدار باشد. در این صورت M ایده‌آل ماکسیمال از R است اگر و فقط اگر $\frac{R}{M}$ یک میدان باشد.

اثبات: فرض کنید که M ایده‌آل ماکسیمال از حلقه جابجایی و یکدار R باشد. در این صورت $\frac{R}{M}$ یک حلقه جابجایی و یکدار است (یکال است.) پس فرض کنید که $\frac{R}{M}$ برای میدان بودن $\frac{R}{M}$ باید نشان دهیم که هر عضو ناصفر دارون ضربی دارد. فرض کنید که $a + M \neq M$ (یعنی $a \notin M$) و $(a+M) \in \frac{R}{M}$

$$N = \{ ra + m \mid r \in R, m \in M \}$$

$(N, +, \cdot)$ یک زیر حلقه R است زیرا $0 = 0a + 0 \in M$

$$\forall r_1a + m_1, r_2a + m_2 \in N \quad (r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in N$$

$$(r_1a + m_1)(r_2a + m_2) = r_1ar_2a + r_1am_2 + m_1r_2a + m_1m_2 = \underbrace{(r_1ar_2)}_{r_3}a + \underbrace{(r_1am_2 + r_2am_1 + m_1m_2)}_{m_3} = r_3a + m_3 \in N$$

$$\forall r_1 \in R, \forall (ra+m) \in N \Rightarrow r_1(ra+m) = r_1ra + r_1m = \underbrace{(r_1r)}_{r_2}a + \underbrace{r_1m}_{m_2} \in N$$

N ایده‌آل R است. چون R جابجایی است پس $r_1 \in N$ ؛ از طرفی $(ra+m) \in N$ (یعنی $a \in N$) $a = (1a + 0) \in N$ و $m = (0a + m) \in N$ چون $M \subset N \subseteq R$ و M یک ایده‌آل ماکسیمال از R است پس $N = R$ یعنی $\forall m \in M$ بنابراین $1 \in N$ بنابراین $\exists r \in R, \exists m \in M \quad 1 = ra + m$

$1 + M = ra + M = (r + M)(a + M)$ یعنی $a + M$ دارون ضربی دارد و دوارون آن $r + M$ است

برعکس: فرض کنید که $\frac{R}{M}$ یک میدان باشد و N ایده‌آلی از R باشد بطوریکه $M \subset N \subset R$، σ را همومورفیسم کانونی (طبیعی) $\sigma : R \to \frac{R}{M}$ ؛ طبق قضیه (۶) فصل قبل پوشا است و طبق قضیه ۳ فصل قبل $\sigma(N)$ ایده‌آلی از $\frac{R}{M}$ است و $\{(0 + M)\} \subset \sigma(N) \subset \frac{R}{M}$ و این متناقض با میدان بودن $\frac{R}{M}$ است زیرا $\frac{R}{M}$ باید ایده‌آل واقعی و غیر بدیهی نداشته باشد. بنابراین $M \subset N \subset R$ نادرست است و M ایده‌آل ماکسیمال R است.

نتیجه: یک حلقه جابجایی و یکدار یک میدان است اگر و فقط اگر ایده‌آل واقعی و نابدیهی نداشته باشد.

تعریف: ایده‌آل $N \neq R$ در حلقه جابجایی و یکدار R یک ایده‌آل اول نامیم در صورتی که با ازای هر $ab \in R$ از $ab \in N$ نتیجه شود $a \in N$ یا $b \in N$.

مثال ۲: ایده‌آل $2\mathbb{Z}$ در $\mathbb{Z}$ یک ایده‌آل اول است زیرا $2\mathbb{Z} \neq \mathbb{Z}$ و برای هر $m, n \in \mathbb{Z}$ اگر $mn \in 2\mathbb{Z}$ آنگاه mn زوج است و یا m زوج است یا n زوج است یعنی $m \in 2\mathbb{Z}$ یا $n \in 2\mathbb{Z}$.

با کمک قضیه زیر می‌توان ایده‌آل‌های اول حلقه خارج قسمتی جابجایی و یکدار R را شناخت.

قضیه ۲: فرض کنید که R حلقه‌ای جابجایی و یکدار باشد و فرض کنید $N \neq R$ ایده‌آلی در R باشد. در این صورت $\frac{R}{N}$ حوزه صحیح است اگر و فقط اگر N ایده‌آل اول در R باشد.

اثبات: فرض کنید که $\frac{R}{N}$ یک حوزه صحیح باشد و برای هر a و b از R اگر $ab \in N$ باشد آنگاه $ab + N = N$ بنابراین $(a+N)(b+N) = N$ چون $\frac{R}{N}$ مقسوم علیه صفر ندارند پس $a+N = N$ یا $b+N = N$ یعنی $a \in N$ یا $b \in N$ یعنی N ایده‌آل اول از حلقه R است.

برعکس اگر $N \neq R$ ایده‌آل اول از R باشد آنگاه $\frac{R}{N}$ یک حلقه است حال چون R جابجایی و یکدار است پس $\frac{R}{N}$ هم حلقه‌ای جابجایی و یکدار است برای حوزه صحیح بودن $\frac{R}{N}$ باید $\frac{R}{N}$ مثال مقسوم علیه صفر نباشد فرض کنید $(a+N)(b+N) = N$ و $a+N \neq N$ در این صورت $ab + N = N$ پس $ab \in N$ حال چون $a \notin N$ پس $a+N \neq N$ و چون N ایده‌آل اول است پس باید $b \in N$ یعنی $b+N = N$ یعنی $\frac{R}{N}$ مقسوم علیه صفر ندارد. (توجه N نقش صفر در حلقه $\frac{R}{N}$ دارد)

نتیجه: هر ایده‌آل ماکسیمال در حلقه جابجایی و یکدار ما شده R یک ایده‌آل اول است.

اثبات: اگر M در R یک ایده‌آل ماکسیمال باشد و طبق قضیه (۱) $\frac{R}{M}$ یک میدان است و چون هر میدان حوزه صحیح است پس $\frac{R}{M}$ حوزه صحیح است پس M یک ایده‌آل اول است (طبق قضیه (۲)).

توجه: عکس نتیجه قبل برقرار نیست یعنی لازم نیست که هر ایده‌آل اول در حلقه جابجایی و یکدار یک ایده‌آل ماکسیمال باشد برای مثونه $\mathbb{Z} \times \mathbb{Z}$ را در نظر می‌گیریم. ایده‌آل $\{0\} \times \mathbb{Z}$ ایده‌آل اول در $\mathbb{Z} \times \mathbb{Z}$ است زیرا $\frac{\mathbb{Z} \times \mathbb{Z}}{\{0\} \times \mathbb{Z}} \cong \mathbb{Z}$ حوزه صحیح است ولی $\mathbb{Z} \times \{0\}$ ایده‌آل ماکسیمال $\mathbb{Z} \times \mathbb{Z}$ نیست.

قضیه ۳: اگر R حلقه‌ای یکدار با مشخصه $n \neq 1$ باشد آنگاه R زیر حلقه‌ای ایزومورف با $\mathbb{Z}_n$ دارد و اگر R دارای مشخصه صفر باشد آنگاه R زیر حلقه‌ای ایزومورف با $\mathbb{Z}$ دارد.

اثبات: نگاشت $\phi : \mathbb{Z} \longrightarrow R$ با تعریف $\phi(m) = m \cdot 1$: $\forall m \in \mathbb{Z}$ طبق تمرین ۱۱ فصل قبل یک هموومورفیسم حلقه‌ای است. $\ker \phi$ ایده‌آلی از $\mathbb{Z}$ است. چون ایده‌آل‌های $\mathbb{Z}$ به صورت $n\mathbb{Z}$ هستند پس عدد $n \in \mathbb{N}$ وجود دارد که $\ker \phi = n\mathbb{Z}$. حال اگر مشخصه R عددی مانند $n \neq 0$ باشد آنگاه $\phi(\mathbb{Z}) \leq R$ با $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$ ایزومورف است و اگر مشخصه R صفر باشد آنگاه برای هر $m \neq 0$ از $\mathbb{Z}$ داریم $m \cdot 1 \neq 0$ و از این رو هسته ϕ عبارت است از $\{0\}$ یعنی $\ker \phi = \{0\}$. پس تصویر $\phi(\mathbb{Z}) \leq R$ با $\mathbb{Z}$ ایزومورف است یعنی با $\mathbb{Z} \cong \frac{\mathbb{Z}}{\{0\}}$ ایزومورف است.

قضیه ۴: هر میدان F یا دارای مشخصه اول p است و دارای زیر میدان ایزومورف با $\mathbb{Z}_p$ (است) یا دارای مشخصه صفر است و زیر میدانی ایزومورف با $\mathbb{Q}$ دارد.

اثبات: اگر مشخصه F صفر نباشد، قضیه قبل می‌گوید که F زیر حلقه‌ای ایزومورف با $\mathbb{Z}_n$ دارد. دراین صورت n باید عدد اولی چون p باشد یا در غیر این صورت F مضروب صحیح صفر دارد (چون $\mathbb{Z}_n$ برای nهای غیر اول مقسوم علیه صفر دارد). اگر F دارای مشخصه صفر باشد آنگاه F باید زیر حلقه‌ای ایزومورف با $\mathbb{Z}$ داشته باشد. دراین صورت F باید شامل میدانی از خارج قسمتهای این زیر حلقه باشد (درآینده، با میدان خارج قسمت‌های یک حوزه صحیح یا میدان کسرها آشنا می‌شوید) و این میدان خارج قسمتها باید با $\mathbb{Q}$ ایزومورف باشد.

تعریف: میدانهای $\mathbb{Z}_p$ و $\mathbb{Q}$ میدانهای اول هستند.

تعریف: اگر R حلقه‌ای تعویضی یکدار باشد و $a \in R$، ایده‌آل $\{ra \mid r \in R\}$ متشکل از تمام مضربهای a را ایده‌آل اصلی تولید شده توسط a می‌نامیم و با $\langle a \rangle$ نمایش می‌دهیم. و ایده‌آلی چون N از R را یک ایده‌آل اصلی است در صورتی که عضوی چون a از R موجود باشد که $N = \langle a \rangle$.

و حوزه صحیح چون D را یک حوزه ایده‌آل اصلی (یا P.I.D) نامیم در صورتی که هر ایده‌آل آن اصلی باشد

P.I.D مخفف principal ideal domain است

مثال ۳: $\mathbb{Z}$ یک P.I.D حوزه ایده‌آل اصلی است زیرا هر ایده‌آل آن با صورت $n\mathbb{Z} = \langle n \rangle$ اصلی است.

$\{0\} = 0\mathbb{Z}$ و $\langle 1 \rangle = 1\mathbb{Z}$ و $n\mathbb{Z} = \langle n \rangle$

مثال ۴: برای هر عدد صحیح مثبت n، حلقه $\mathbb{Z}_n$ یک حوزه ایده‌آل اصلی است زیرا هر ایده‌آل آن اصلی است

تمرین:

۱- تمام ایده‌آل‌های اول و ماکسیمال $\mathbb{Z}_{12}$ را معین کنید.

۲- ایده‌آل واقعی از $\mathbb{Z} \times \mathbb{Z}$ را بدست آورید که اول نباشد.

۳- اگر R یک حوزه ایده‌آل اصلی باشد، ثابت کنید که هر حلقه خارج قسمتی از آن نیز حوزه ایده‌آل اصلی است.

۴- فرض کنید که R حلقه جابجایی یکدار و متناهی است، ثابت کنید هر ایده‌آل اول R یک ایده‌آل ماکسیمال R است.

میدان کسرهای (میدان خارج قسمتهای) یک حوزه صحیح

می دانیم که $\mathbb{Z}$ یک حوزه صحیح است و $\mathbb{Q}$ یک میدان است که اعضای آن معمولاً با صورت $\frac{m}{n}$ معرفی می شوند که $n \neq 0$ و $m, n \in \mathbb{Z}$ یعنی $\mathbb{Q} = \{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \}$. همچنین می دانیم که $\mathbb{Z} \subseteq \mathbb{Q}$ و $\mathbb{Q}$ کوچکترین میدانی است که شامل $\mathbb{Z}$ است و $\mathbb{Q}$ را میدان کسرهای حوزه صحیح $\mathbb{Z}$ نامیده می شود.
در این فصل روش ساختن میدان کسرهای یک حوزه صحیح دلخواه را شرح می دهیم.

فرض کنید که D یک حوزه صحیح باشد. قرار می دهیم $S = \{ (a,b) \mid a,b \in D \text{ و } b \neq 0 \}$
به عبارت دیگر $S = D \times (D - \{0\})$. می خواهیم زوج (a,b) را به عنوان معرفی برای خارج قسمت (کسر) $\frac{a}{b}$ تصور کنیم. اگر $D = \mathbb{Z}$ آنگاه، زوج $(3,4)$ را می توان $\frac{3}{4}$ معرفی کرد.

تعریف: در عضو (a,b) و (c,d) از S هم ارز نامیم و می نویسیم $(a,b) \sim (c,d)$ اگر و فقط اگر $ad = bc$

قضیه ۱: نسبت $\sim$ روی S یک رابطه هم ارزی است.
اثبات این قضیه یعنی نشان دادن اینکه رابطه $\sim$ انعکاسی و متقارن و متعدی است با عنوان تمرین در نظر گرفته می شود (تمرین ۱).

توجه: کلاسهای (ردههای) هم ارزی این رابطه هم ارزی را با $[(a,b)] = \overline{(a,b)}$ نمایش می دهیم و

$$[(a,b)] = \{ (c,d) \in S \mid (a,b) \sim (c,d) \} = \{ (c,d) \in S \mid ad = bc \}$$

می دانیم که این کلاس های هم ارزی مجموعه S را افراز می کند این افراز یعنی $\frac{S}{\sim}$ را با F نمایش می دهیم و قصد داریم که F را یک میدان که همان میدان کسرهای حوزه صحیح D است تبدیل کنیم.
توجه: مجموعه تمام کلاسهای هم ارزی $= F = \{ [(a,b)] \mid (a,b) \in S \}$
قضیه ۲: با ازای هر $[(a,b)]$ و $[(c,d)]$ از F، ساده ترین عمل های جمع و ضرب خوشتعریفی در F را ارائه می کنند.

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$
$$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

برای درک اثبات این قضیه می توان بجای $[(a,b)]$ نوشت کسر $\frac{a}{b}$ در این صورت دو عمل جمع و ضرب ذکر شده همان جمع و ضرب دو کسر $\frac{a}{b}$ و $\frac{c}{d}$ است یعنی

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = [(ad+bc, bd)]$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = [(ac, bd)]$$

اثبات قضیه ۲: برای خوشتعریفی جمع و ضرب باید نشان دهیم که الف) $[(ac, bd)] \in F$ و $[(ad+bc, bd)]$ ب) جمع و ضرب مستقل از انتخاب نماینده های کلاس های هم ارزی است.

الف: چون $[(a,b)]$ و $[(c,d)]$ عضو F هستند پس $(a,b), (c,d) \in S$ پس $b \neq 0$ و $d \neq 0$ و چون D حوزه صحیح است پس $bd \neq 0$ چون D مفروض علی الصفر است پس
$(ad+bc, bd) \in S$ و $(ac, bd) \in S$ یعنی : $[(ac, bd)]$ و $[(ad+bc, bd)]$

ب) فرض کنید که $[(a_1,b_1)] \in [(a,b)]$ و $[(c_1,d_1)] \in [(c,d)]$. باید نشان دهیم که

$[(a_1d_1+b_1c_1, b_1d_1)] \in [(ad+bc, bd)]$ و $[(a_1c_1, b_1d_1)] \in [(ac, bd)]$

اکنون $[(a_1,b_1)] \in [(a,b)]$ بدین معنی است $(a_1,b_1) \sim (a,b)$، یعنی که $a_1b = b_1a$ ①

مشابهاً، $[(c_1,d_1)] \in [(c,d)]$ نتیجه می دهد که $c_1d = d_1c$ ②

با ضرب طرفین ① در d_1d و با ضرب طرفین ② در b_1b و جمع تساویهای حاصل، تساوی زیر را در D بدست می آوریم:

$$a_1b\,d_1d + c_1d\,b_1b = b_1a\,d_1d + d_1c\,b_1b \Rightarrow (a_1d_1+b_1c_1)bd = b_1d_1(ad+bc) \Rightarrow$$

$$(a_1d_1+b_1c_1, b_1d_1) \sim (ad+bc, bd)$$

یعنی $[(a_1d_1+b_1c_1, b_1d_1)] \in [(ad+bc, bd)]$ یعنی جمع مستقل از انتخاب نماینده در کلاس هم ارزی است

برای ضرب کافی است با ضرب کردن تساوی ① و ② در هم $a_1b\,c_1d = b_1a\,d_1c$ پس $a_1c_1\,bd = b_1d_1\,ac$

که نتیجه می دهد $(a_1c_1, b_1d_1) \sim (ac, bd)$ پس $[(a_1c_1, b_1d_1)] \in [(ac, bd)]$ یعنی ضرب در F مستقل از انتخاب نماینده در کلاس هم ارزی است.

قضیه ۳: $(F, +, \cdot)$ میدان است

اثبات: باید نشان دهیم که $(F, +)$ یک گروه آبلی است و $(F-\{[(0,1)]\}, \cdot)$ یک گروه آبلی است که در آن $[(0,1)] = 0$ عضو خنثی جمعی است. همچنین باید نشان دهیم که ضرب روی جمع توزیع پذیر است.

برای گروه آبلی بودن $(F, +)$: $[(0,1)]$ عضو خنثی جمعی F است زیرا $\forall [(a,b)] \in F$

$$[(a,b)] + [(0,1)] = [(a\cdot1+b\cdot0, b\cdot1)] = [(a,b)] = [(0,1)] + [(a,b)]$$

جمع خاصیت جابجایی دارد زیرا $\forall [(a,b)], [(c,d)] \in F$

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)] = [(cb+da, db)] = [(c,d)] + [(a,b)]$$

جمع خاصیت شرکت پذیری دارد زیرا

$$[(a,b)], [(c,d)] \text{ و } [(e,f)] \in F$$

$$([(a,b)] + [(c,d)]) + [(e,f)] = [(ad+bc, bd)] + [(e,f)] = [(adf+bcf+bde, bdf)]$$

$$= [(a,b)] + [(cf+de, df)] = [(a,b)] + ([(c,d)] + [(e,f)])$$

قدرینه $[(-a,b)]$ در F است زیرا $[(a,b)]$

$$[(a,b)] + [(-a,b)] = [(ab-ab, b^2)] \overset{(*)}{=} [(0,b^2)] = [(0,1)]$$

دلیل برابری (*): چون $(0,b^2) \sim (0,1)$ زیرا $0 \cdot 1 = b^2 \cdot 0$ پس $[(0,b^2)] = [(0,1)]$.

پس $(F, +)$ یک گروه آبلی است.

برای گروه آبلی بودن $(F-\{[(0,1)]\}, \cdot)$: ضرب در $F-\{[(0,1)]\}$ شرکت پذیر است؛

$$\forall [(a,b)], [(c,d)], [(e,f)] \in F-\{[(0,1)]\}$$

$$([(a,b)]\cdot[(c,d)])\cdot[(e,f)] = [(ac,bd)]\cdot[(e,f)] = [(ace, bdf)] = [(a,b)]\cdot[(ce,df)] =$$

$$= [(a,b)]\cdot([(c,d)]\cdot[(e,f)])$$

$[(1,1)]$ عضو خنثی ضربی در F است زیرا $\forall [(a,b)] \in F : [(a,b)][(1,1)] = [(a,b)][(1,1)] = [(a,b)]$

اگر $[(a,b)] \in F$ آنگاه $[(a,b)] \neq [(0,1)]$ پس $a \neq 0$ و وارون ضربی $[(a,b)]$ است زیرا

$$[(a,b)][(b,a)] = [(ab,ba)] = [(1,1)]$$

بدین است که $[(ab,ba)] = [(1,1)]$ زیرا $(ab,ba) \sim (1,1)$ چون $ab = ba$.

پس $(F - \{[(0,1)]\}, \cdot)$ یک گروه است آبلی یعنی ضرب میدان است چون D آبلی است.

ضرب روی جمع توزیع پذیر است (تمرین) بنابراین $(F, +, \cdot)$ یک میدان است.

قضیه ۴: نگاشت $f: D \longrightarrow F$ با تعریف $\forall a \in D : f(a) = [(a,1)]$ ایزومورفیسی از D با زیر حلقه‌ای از F است. (یعنی f هموومورفیسم یک به یک است.)

اثبات: $\forall a,b \in D :$

$$f(a+b) = [(a+b,1)] = [(a,1)] + [(b,1)] = f(a) + f(b)$$

$$f(ab) = [(ab,1)] = [(a,1)][(b,1)] = f(a) \cdot f(b)$$

f یک به یک است

$$f(a) = f(b) \Rightarrow [(a,1)] = [(b,1)] \Leftrightarrow (a,1) \sim (b,1) \Leftrightarrow a = b$$

پس f ایزومورفیسمی از D با زیر حلقه $f(D)$ از F است.

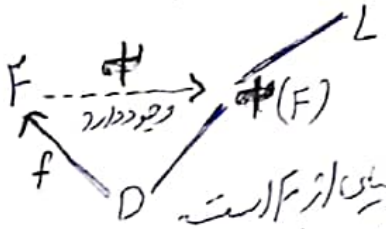
توجه: در قضیه قبل داریم:

$$[(a,b)] = [(a,1)][(1,b)] = [(a,1)] / [(b,1)] = \frac{f(a)}{f(b)}$$

بنابراین قضیه زیر را خواهیم داشت.

قضیه ۵: هر حوزه صحیح D را می‌توان توسعه داد (یا شاید در) میدانی مانند F طوری که هر عضو F را بتوان به صورت خارج قسمتی از دو عضو D بیان کرد. (میدان F را یک میدان کسرها (خارج قسمتهای) D می‌نامیم.)

قضیه ۶: فرض کنید که F میدانی از خارج قسمتهای D باشد و L میدانی شامل D. در این صورت نگاشتی چون $\forall a \in D \cdot \Psi(a) = a$ وجود دارد که ایزومورفیسمی از F با زیر میدانی از L ارائه می‌کند، طوری که



اثبات: برای راحتی هر عضو F را به صورت $\frac{a}{b}_F$ نمایش می‌دهیم علامت F نشان دهنده خارج قسمت a بر b (که $a,b \in D$) به عنوان اعضایی از F است. هدف این است که $\frac{a}{b}_F$ را به $\frac{a}{b}_L$ بنگاریم و $\frac{a}{b}_L$ خارج قسمت اعضا در L است.

بنابراین نگاشت $\Psi : F \longrightarrow L$ را به صورت $\Psi(a) = a$ برای هر a از D و همچنین برای اعضای F به صورت $\forall \frac{a}{b}_F \in F \; \Psi\left(\frac{a}{b}_F\right) = \frac{\Psi(a)}{\Psi(b)}$ تعریف می‌کنیم که در آن $b \neq 0$

ابتدا نشان می‌دهیم که نگاشت Ψ با معنی و خوش تعریف است چون Ψ بر D نگاشت همانی است و برای هر $b \in D$ داریم $\Psi(b) \neq 0$ از این رو کسر $\frac{\Psi(a)}{\Psi(b)}$ تعریف شده است اگر F را گردد داشته باشیم

$\frac{a}{b}_F = \frac{c}{d}_F$ آنگاه در D داریم $ad = bc$ بنابراین $\Psi(ad) = \Psi(bc)$

$\varphi(ab)=\varphi(a)\varphi(b)$ و $\varphi(bc)=\varphi(b)\varphi(c)$ چون φ بر D یکریختی است پس

پس در L داریم $\frac{\varphi(a)}{\varphi(b)}=\frac{\varphi(c)}{\varphi(d)}$ یعنی φ خوشتعریف است

نشان می‌دهیم که φ همومورفیسم حلقه‌ای است: $\forall \frac{a}{F b}, \frac{c}{F d} \in F$

$$\varphi\left(\frac{a}{F b}+\frac{c}{F d}\right)=\varphi\left(\frac{ad+bc}{F bd}\right)=\frac{\varphi(ad+bc)}{\varphi(bd)}=\frac{\varphi(ad)+\varphi(bc)}{\varphi(b)\varphi(d)}=$$

$$\frac{\varphi(a)\varphi(d)+\varphi(b)\varphi(c)}{\varphi(b)\varphi(d)}=\frac{\varphi(a)}{\varphi(b)}+\frac{\varphi(c)}{\varphi(d)}=\varphi\left(\frac{a}{F b}\right)+\varphi\left(\frac{c}{F d}\right)$$

$$\varphi\left(\frac{a}{F b}\cdot\frac{c}{F d}\right)=\varphi\left(\frac{ac}{F bd}\right)=\frac{\varphi(ac)}{\varphi(bd)}=\frac{\varphi(a)\varphi(c)}{\varphi(b)\varphi(d)}=\frac{\varphi(a)}{\varphi(b)}\cdot\frac{\varphi(c)}{\varphi(d)}$$

$$=\varphi\left(\frac{a}{F b}\right)\varphi\left(\frac{c}{F d}\right)$$

φ یک به یک است زیرا اگر $\varphi\left(\frac{a}{F b}\right)=\varphi\left(\frac{c}{F d}\right)$ آنگاه

$$\frac{\varphi(a)}{\varphi(b)}=\frac{\varphi(c)}{\varphi(d)} \Rightarrow \varphi(a)\varphi(d)=\varphi(b)\varphi(c) \Rightarrow \varphi(ad)=\varphi(bc)$$

چون φ روی D یکریختی است پس $ad=bc$ بنابراین $\frac{a}{F b}=\frac{c}{F d}$.

نتیجه ۱: هر میدان L که شامل یک حوزه صحیح‌اند شامل میدانی از خارج قسمتهای (کسرهای) D می‌باشد.

اثبات: در قضیه قبل هر عضو میدان $\varphi(F)$ از L خارج قسمتی از اعضای D از L است

نتیجه ۲: هر دو میدان از خارج قسمتهای یک حوزه صحیح D ایزومورف هستند.

اثبات: در قضیه قبل فرض کنید که L میدانی از خارج قسمتهای D باشد. بنابراین هر عضو از L را می‌توان به صورت $\frac{a}{b}$ که $a \in D$ و $0 \neq b \in D$. نوشت. در این صورت L همان میدان $\varphi(F)$ می‌باشد و لذا با F ایزومورف است.

توجه: اگر $D=\mathbb{Z}$ در نظر بگیریم در این صورت $F=\mathbb{Q}$ است و قبلاً دیدیم که

$\mathbb{Q}=\left\{\frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0\right\}$ میدان اعداد گویا (کسری‌های $\mathbb{Z}$) است.

و $\mathbb{Q}$ کوچکترین میدانی از اعداد است که $\mathbb{Z}$ را در بردارد و در قضیه قبل اگر L میدانی شامل $\mathbb{Z}$ مثلاً $\mathbb{R}$ و یا $\mathbb{Q}(\sqrt{2})$ و $\mathbb{Q}(\sqrt{3})$ و ... باشد آنگاه $\varphi: \mathbb{Q} \longrightarrow L$ برای هر $a \in \mathbb{Z}$ و $\varphi(a)=\frac{a}{1}$

$\forall \frac{a}{b} \in \mathbb{Q}: \varphi\left(\frac{a}{b}\right)=\frac{a}{b} \in L$ است.

تمرین

۱- قضیه ۱ (رابطه هم‌ارزی بودن $\sim$) را ثابت کنید.

۲- در قضیه ۳: توزیع پذیری ضرب روی جمع در F را بررسی کنید.

۳- میدان F متشکل از خارج قسمت‌های زیرحوزه صحیح $D=\{n+mi \mid n,m\in\mathbb{Z}\}$ از $\mathbb{C}$ را توصیف کنید که در آن $n+mi$ یک عدد مختلف است و $i=\sqrt{-1}$ و $m,n\in\mathbb{Z}$.

۴- میدان F متشکل از خارج قسمت‌های زیرحوزه صحیح $D=\{n+m\sqrt{2} \mid m,n\in\mathbb{Z}\}$ از $\mathbb{R}$ را توصیف کنید.

۵- فرض کنید که R یک حلقه باشد. نشان دهید که R در یک حلقه یکدار R' شاملی است.

(راهنمایی اگر $1\in R$ آنگاه $R=R'$ جواب است وگرنه $1\notin R$ آنگاه روی $R'=\{(r,m) \mid r\in R, m\in\mathbb{Z}\}$ کار کنید.)

۶- با قرار دادن $\mathbb{C}=\mathbb{R}\times\mathbb{R}$ و جمع و ضرب روی $\mathbb{C}$ را چنین در نظر بگیرید: $\forall (a,b),(c,d)\in\mathbb{C}$

$(a,b)\cdot(c,d)=(ac-bd, ad+bc)$ و $(a,b)+(c,d)=(a+c,b+d)$

نشان دهید که $(\mathbb{C},+,\cdot)$ یک میدان است.

(راهنمایی: اگر $(a,b)\neq(0,0)$ آنگاه $(a,b)^{-1}=\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$ در نظر بگیرید)

حلقه چند جمله ایها

تعریف: فرض کنید که R یک حلقه باشد. یک چندجمله‌ای $f(x)$ با ضرایب در حلقه R حاصل جمعی و صوری و نامتناهی به صورت $\sum_{i=0}^{+\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$ است که در آن $a_i \in R$ و به ازای جمیع مقادیر i، مگر تعدادی متناهی از آنها $a_i = 0$. این a_iها ضرایب $f(x)$ هستند. درصورتیکه عددی مانند i_0 باشد که $a_i \neq 0$ آنگاه بزرگترین مقدار چنین i را درجه $f(x)$ می‌نامیم. درصورتیکه چنین iای موجود نباشد درجه $f(x)$ را صفر در نظر می‌گیریم و در واقع $f(x) = 0$ است.

قرارداد: اگر در چندجمله‌ای $f(x) = a_0 + a_1 x + \cdots + a_n x^n + \cdots$ اگر برای هر $i > n$ مقدار a_i صفر باشد (یعنی $a_i = 0$) در این صورت می‌نویسیم $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ (یعنی درجه $f(x)$ برابر با n است) و عضو a از R هم یک چندجمله‌ای ثابت در نظر می‌گیریم که $a_0 = a$ و برای هر $i > 0$ $a_i = 0$ است یعنی $f(x) = a$.

مجموعه تمام چندجمله‌ایها با ضرایب در R را با $R[x]$ نمایش می‌دهیم و $R \subseteq R[x]$.

جمع و ضرب دو چندجمله‌ای در $R[x]$ را به صورت زیر تعریف می‌کنیم

$$f(x) = \sum_{i=0}^{+\infty} a_i x^i, \quad g(x) = \sum_{j=1}^{+\infty} b_j x^j \qquad \forall f(x), g(x) \in R[x]$$

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots = \sum_{k=0}^{+\infty} c_k x^k$$

که در آن $c_k = a_k + b_k$ است و $l = \max\{n, m\}$ است.

$$f(x) \cdot g(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_l x^l + \cdots$$

که در آن $d_l = \sum_{i=0}^{l} a_i b_{l-i}$ است.

اگر حلقه R جابجایی نباشد لازم نیست که $\sum_{i=0}^{l} a_i b_{l-i}$ و $\sum_{i=0}^{l} b_i a_{l-i}$ با هم مساوی باشند.

قضیه ۱: مجموعه $R[x]$ تحت جمع و ضرب بالا (جمع ضرب چندجمله‌ایها) یک حلقه است. اگر R جابجایی باشد آنگاه حلقه $R[x]$ جابجایی است و اگر R یکدار باشد آنگاه $R[x]$ یکدار است (واحد ضربی R یعنی ۱ همان واحد ضربی $R[x]$ است)

اثبات: اینکه $(R[x], +)$ یک گروه آبلی است به عنوان تمرین در نظر می‌گیریم. (توجه: قبلاً دیدیم که $C(R,R)$ یک حلقه است و چون هر چندجمله‌ای بیدسته است پس $C(R,R)$ زیرحلقه $R[x]$ است بخصوص وقتی که $R = \mathbb{R}$.)

همچنین توزیع پذیری ضرب روی جمع چون وقت گیر و خسته کننده است به عنوان تمرین در نظر می‌گیریم. (تمرین ۱)

ضرب شرکت پذیر است، فرض کنید که $f(x) = \sum_{i=0}^{+\infty} a_i x^i$ و $g(x) = \sum_{j=0}^{+\infty} b_j x^j$ و $h(x) = \sum_{k=0}^{+\infty} c_k x^k$ سه عضو دلخواه از $R[x]$ باشند. در این صورت:

$$[f(x)g(x)]h(x) = \left(\sum_{i=0}^{+\infty} a_i x^i \cdot \sum_{j=0}^{+\infty} b_j x^j\right) \sum_{k=0}^{+\infty} c_k x^k = \left(\sum_{n=0}^{+\infty} \left(\sum_{i=0}^{n} a_i b_{n-i}\right) x^n\right) \sum_{k=0}^{+\infty} c_k x^k$$

ادامه صفحه بعد

$$= \sum_{s=0}^{+\infty} \left[\sum_{n=0}^{s} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) c_{s-n} \right] x^s = \sum_{\beta=0}^{+\infty} \left(\sum_{i+j+k=\beta} a_i b_j c_k \right) x^\beta =$$

$$= \sum_{s=0}^{+\infty} \left[\sum_{m=0}^{s} a_{s-m} \left(\sum_{j=0}^{m} b_j c_{m-j} \right) \right] x^s = \left(\sum_{i=0}^{+\infty} a_i x^i \right) \left[\sum_{m=0}^{+\infty} \left(\sum_{j=0}^{m} b_j c_{m-j} \right) x^m \right] =$$

$$= \left(\sum_{i=0}^{+\infty} a_i x^i \right) \left[\sum_{j=0}^{+\infty} b_j x^j \cdot \sum_{k=0}^{+\infty} c_k x^k \right] = f(x) \left(g(x) \cdot h(x) \right)$$

مثال ۱ اگر در $\mathbb{Z}[x]$ داشته باشیم $\deg f(x) = 2$ ، $\deg g(x) = 2$ ، $\deg h(x) = 2$ آنگاه $\deg\left((f(x)\, g(x)) h(x) \right) = 6$ است.

مثال ۲ فرض کنید که در $\mathbb{Z}_4[x]$ داشته باشیم

$$f(x) = 1 + x^2$$
$$g(x) = 2 + x + 2x^2 \quad \text{و} \quad h(x) = 3x + 2x^2$$

آنگاه

$$[f(x)\, g(x)]\, h(x) = [(1+x^2)(2+x+2x^2)](3x+2x^2) = [2+x+2x^2+2x^3+2x^4](3x+2x^2)$$
$$= [2+x+2x^2+3x^3+2x^4](3x+2x^2) = 6x+3x^2+6x^3+2x^4+3x^5+2x^6+6x^7+4x^8$$
$$= 6x+3x^2+2x^3+2x^4+3x^5+2x^6 \Rightarrow \deg\left([f(x)\, g(x)]\, h(x) \right) = 6$$

چون حلقه $\mathbb{Z}$ بدون مقسوم علیه صفر است (چون حوزه صحیح است) درجه این سه چندجمله‌ای در $\mathbb{Z}[x]$ با هم جمع شده ولی اگر این چندجمله‌ای‌ها در $\mathbb{Z}_8[x]$ بودند آنگاه

$$[f(x)\, g(x)]\, h(x) = 6x + 3x^3 + 3x^4 + 2x^5 \Rightarrow \deg\left[(f(x)\, g(x)) h(x) \right] = 5$$

مثال ۳ : در $\mathbb{Z}_2[x]$

$$(1+x)^2 = (1+x)(1+x) = 1+2x+x^2 = 1+x^2$$
$$(1+x) + (1+x) = 2+2x = 0$$

نتیجه: طبق تعریف اگر R یک حلقه باشد آنگاه $R[x]$ یک حلقه است بنابراین $(R[x])[y]$ هم یک حلقه چندجمله‌ای برحسب y است که ضرایب هم چندجمله‌ای برحسب x است.
می‌توان ثابت کرد که حلقه $(R[x])[y]$ با حلقه $(R[y])[x]$ با هم ایزومورف هستند (تمرین ۱)
با توجه به ایزومورفیسم یاد شده $(R[x])[y]$ یا $(R[y])[x]$ این دو را یکی در نظر می‌گیریم و با $R[x,y]$ نیز همین‌طور و به همین صورت می‌توان حلقه $R[x_1, x_2, \ldots, x_n]$ ساخت.
اگر R یک حوزه صحیح باشد می‌توان نشان داد که $R[x]$ حوزه صحیح است (تمرین ۲).
اگر R یک میدان باشد آنگاه $R[x]$ نمی‌تواند میدان باشد زیرا $x \in R[x]$ در $R[x]$ وارون ندارد (وارون نمی‌تواند ثابت باشد)
حال R میدان باشد چون حوزه صحیح است پس $R[x]$ یک حوزه صحیح است. بنابراین می‌توان میدان خارج قسمتی‌های $R[x]$ را ساخت و این میدان را می‌توان با $R(x)$ نمایش داد و به همین صورت می‌توان میدان $R(x_1, x_2, \ldots, x_n)$ ساخت.

قبصره ۲: در این فصل می خواهیم به چند سؤال اساسی جواب دهیم:

سؤال ۱: در حلقه چند جمله ای ها ریشه های معادله $f(x)=0$ در چه حلقه ای قرار دارند و چگونه این ریشه ها را پیدا کنیم؟

سؤال ۲: ایده آل های در حلقه $R[x]$ چگونه هستند؟

سؤال ۳: ایده آل های ماکسیمال و ایده آل های اول در $R[x]$ چگونه هستند؟ زیرا که می خواهیم خوب بدانیم حلقه خارج قسمتی چیست.

سؤال ۴: یک چند جمله ای در $R[x]$ چگونه تجزیه می شوند؟

قضیه ۲: (هموومورفیسم ارزیابی نظریه میدان) فرض کنید که E یک میدان باشد و F زیر میدانی از E باشد. فرض کنید که $\alpha \in E$ دلخواه باشد. نگاشت $\phi_\alpha : F[x] \longrightarrow E$ با ضابطه $\forall f(x) \in F[x] \quad \phi_\alpha(f(x)) = f(\alpha)$ یک هموومورفیسم از $F[x]$ بتوی E است. همچنین $\phi_\alpha(x)=\alpha$، و $\forall c \in F \quad \phi_\alpha(c)=c$.

هموومورفیسم ϕ_α را ارزیابی در α می نامیم.

اثبات: اگر $f(x) \in F[x]$ یک چند جمله ای دلخواه باشد و

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

آنگاه

$$f(\alpha) = a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_n \alpha^n$$

بنابراین برای هر $f(x), g(x) \in F[x]$ اگر

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m = \sum_{i=0}^{m} b_i x^i \Rightarrow f(x)+g(x) = \sum_{k=0}^{l} c_k x^k$$

$$\phi_\alpha(f(x)+g(x)) = \phi_\alpha\left(\sum_{k=0}^{l} c_k x^k\right) = \sum_{k=0}^{l} c_k \alpha^k = f(\alpha)+g(\alpha) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$$

$$f(x)\cdot g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{t=0}^{s} d_t x^t \qquad (s \le m+n)$$

و $d_t = \sum_{i=0}^{t} a_i b_{t-i}$.

$$\phi_\alpha(f(x)g(x)) = \phi_\alpha\left(\sum_{t=0}^{s} d_t x^t\right) = \sum_{t=0}^{s} d_t \alpha^t = \left(\sum_{i=0}^{n} a_i \alpha^i\right)\left(\sum_{j=0}^{m} b_j \alpha^j\right) =$$

$$= f(\alpha)\cdot g(\alpha) = \phi_\alpha(f(x))\cdot\phi_\alpha(g(x))$$

بدیهی است $\phi_\alpha(x)=\alpha$، و $\forall c \in F : \phi_\alpha(c)=c$

مثال ۴: فرض کنید که $F=\mathbb{Q}$، $E=\mathbb{R}$، و $\alpha=0$. در این صورت $\phi_0 : \mathbb{Q}[x] \longrightarrow \mathbb{R}$

$$\phi_0(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1(0) + \cdots + a_n(0)^n = a_0$$

$\ker \phi_0 = \{ f(x) \in \mathbb{Q}[x] \mid \phi_0(f(x)) = 0 \} =$ مجموعه تمام چند جمله ای با ضرایب گویا که ثابت صفر $= I$

در این صورت $\frac{\mathbb{Q}[x]}{I} \cong \phi_0(\mathbb{Q}[x]) = \mathbb{Q}$ (طبق قضیه اول ایزومورفیسم)

اعضای حلقه $\frac{\mathbb{Q}[x]}{I}$ را توصیف کنید (تمرین ۳)

مثال ۵ همومورفیسم ارزیابی $\phi_2 : \mathbb{Q}[x] \longrightarrow \mathbb{R}$ در نظر می‌گیریم $\phi_2(f(x)) = f(2)$

$\phi_2(x^2+x-6) = 4+2-6 = 0 \Rightarrow (x^2+x-6) \in \ker\phi_2$

از طرفی $x^2+x-6 = (x-2)(x+3)$.

$\ker\phi_2 = \{ f(x) \in \mathbb{Q}[x] \mid \phi_2(f(x)) = 0 \} = \{ f(x) \in \mathbb{Q}[x] \mid f(2) = 0 \}$

در آینده خواهیم دید که $\ker\phi_2$ این مثال متشکل از تمام چندجمله‌ای‌های $\mathbb{Q}[x]$ به شکل $(x-2)g(x)$ است که $g(x) \in \mathbb{Q}[x]$

در این مثال هم $\frac{\mathbb{Q}[x]}{\ker\phi_2} \cong \phi_2(\mathbb{Q}[x]) \cong \mathbb{Q}$.

مثال ۶: با فرض $\alpha = i$ $(i = \sqrt{-1})$ همومورفیسم $\phi_i : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ در نظر می‌گیریم

$\phi_i(f(x)) = f(i)$; $\phi_i(x^2+1) = i^2+1 = 0 \Rightarrow (x^2+1) \in \ker\phi_i$

$\ker\phi_i$ = مجموعه تمام چندجمله‌ای‌هایی به صورت $(x^2+1)g(x)$ است که $g(x) \in \mathbb{Q}[x]$.

در آینده خواهیم دید که $\frac{\mathbb{Q}[x]}{\ker\phi_i} \cong \phi_i(\mathbb{Q}[x]) = \mathbb{Q}(i)$ که $\mathbb{Q}(i) = \{ p+iq \mid p,q \in \mathbb{Q} \}$

و $\mathbb{Q}(i)$ زیرمیدانی از $\mathbb{C}$ است

مثال ۷: $\phi_\pi : \mathbb{Q}[x] \longrightarrow \mathbb{R}$ در نظر می‌گیریم، در این صورت $\ker\phi_\pi = \{0\}$ یعنی ϕ_π یک‌به‌یک است

پس $\frac{\mathbb{Q}[x]}{\{0\}} = \frac{\mathbb{Q}[x]}{\ker\phi_\pi} \cong \phi_\pi(\mathbb{Q}[x])$ یعنی π جای x را می‌گیرد $\phi_\pi(\mathbb{Q}[x]) = \mathbb{Q}(\pi)$ توجه $\mathbb{Q}[x] \cong \frac{\mathbb{Q}[x]}{\{0\}}$.

تعریف: فرض کنید F زیرمیدانی از میدان E باشد و α عضوی از E. فرض کنید که $f(x) = a_0 + a_1x + \cdots + a_nx^n$ یک چندجمله‌ای از $F[x]$ باشد. $\phi_\alpha : F[x] \longrightarrow E$ همومورفیسم ارزیابی باشد $\phi_\alpha(f(x)) = f(\alpha)$.

اگر $f(\alpha)=0$ آنگاه α را یک صفر $f(x)$ می‌نامیم. (ریشه معادله $f(x)=0$)

در مثال ۵ دیدیم که ۲ و ۳- صفرهای $f(x) = x^2+x-6$ است.

$\{ \alpha \in \mathbb{R} \mid \phi_\alpha(x^2+x-6) = 0 \} = \{ \alpha \in \mathbb{R} \mid \alpha^2+\alpha-6 = 0 \} = \{ 2, -3 \}$

هدف اساسی: نشان دادن این که برای هر میدان F، هر چندجمله‌ای غیرثابت $f(x) \in F[x]$ دارای صفر است.

قضیه ۳ (الگوریتم تقسیم برای $F[x]$) فرض کنید که F یک میدان باشد و $f(x) = \sum_{i=0}^{n} a_ix^i$ و $g(x) = \sum_{j=0}^{m} b_jx^j$ دو عضو از $F[x]$ باشند، با این شرط که a_n و b_m هر دو اعضایی ناصفر از F باشند و $m > 0$. در این صورت چندجمله‌ای‌های منحصربفرد $q(x)$ و $r(x)$ در $F[x]$ وجود دارند بطوریکه $f(x) = g(x)q(x) + r(x)$ و $\deg r(x) < \deg g(x)$.

برهان: مجموعه $S = \{ f(x) - g(x)s(x) \mid s(x) \in F[x] \}$ را در نظر بگیرید. فرض کنید $r(x)$ یک چندجمله‌ای دلخواه در S باشد. بنابراین $r(x)$ به ازای یک چندجمله‌ای $q(x) \in F[x]$، $f(x) = g(x)q(x) + r(x)$.

باید نشان دهیم که $\deg r(x) < m$.

فرض کنید که $r(x)=\sum_{k=0}^{t} c_k x^k$ و $c_k\in F$ و اگر $t\neq 0$ آنگاه $c_t\neq 0$. اگر $t\geq m$ آنگاه

$$f(x)-g(x)q(x)-\left(\frac{c_t}{b_m}\right)x^{t-m}g(x)=r(x)-\left(\frac{c_t}{b_m}\right)x^{t-m}g(x) \quad (1)$$

و طرف دوم به صورت $r(x)-(c_t x^t+$ (جملاتی از درجات کمتر$)$ است که یک چندجمله‌ای از درجه‌ای کمتر از t، یعنی درجه $r(x)$ می‌باشد. چندجمله‌ای تساوی (1) را می‌توان به صورت $f(x)-g(x)\left[q(x)+\frac{c_t}{b_m}x^{t-m}\right]$ نوشت و از این رو عضوی از S است. و این امر با این واقعیت که $r(x)$ با درجه می‌نیمال از S انتخاب شده است متناقض است. پس درجه $r(x)$ کوچکتر است از $m = \deg g(x)$.

برای یکتایی، اگر $f(x)=g(x)q_1(x)+r_1(x)$ و $f(x)=g(x)q_2(x)+r_2(x)$، آنگاه با تفریق این دو تساوی خواهیم داشت

$$g(x)\left[q_1(x)-q_2(x)\right]=r_2(x)-r_1(x)$$

چون $\deg\left[r_2(x)-r_1(x)\right] < \deg\left(g(x)\right)$. این تساوی تنها به شرطی برقرار است که $q_2(x)-q_1(x)=0$ یا $q_2(x)=q_1(x)$ در این صورت باید داشته باشیم $r_2(x)-r_1(x)=0$ یا $r_1(x)=r_2(x)$.

نتیجه ۱: عضو $a\in F$ صفری از $f(x)\in F[x]$ است اگر و فقط اگر $x-a$ عاملی از $f(x)$ در $F[x]$ باشد.

اثبات: فرض کنید که به ازای a از F داشته باشیم $f(a)=0$. بنابر قضیه قبل چندجمله‌ای‌های $r(x)$ و $q(x)$ از $F[x]$ وجود دارند بطوری که $f(x)=(x-a)q(x)+r(x)$ که در آن $\deg r(x)<1$، پس به ازای عضوی مانند c از F باید داشته باشیم $r(x)=c$ بنابراین $f(x)=(x-a)q(x)+c$ با بکاربردن هومومورفیسم ارزیابی $\phi_a: F[x]\to F$ $0=f(a)=0q(a)+c$ پس باید $c=0$ پس $f(x)=(x-a)q(x)$. از این رو $(x-a)$ عاملی از $f(x)$ است.

به عکس اگر $x-a$ عاملی از $f(x)$ در $F[x]$ باشد که $a\in F$، آنگاه با بکاربردن هومومورفیسم ارزیابی ϕ_a به $f(x)=(x-a)q(x)$ خواهیم داشت $f(a)=0q(a)=0$.

نتیجه ۲: هر چندجمله‌ای ناصفر $f(x)\in F[x]$ از درجه n حداکثر می‌تواند n صفر در میدان F داشته باشد.

اثبات: طبق نتیجه قبل اگر $a_1\in F$ صفری از $f(x)$ باشد آنگاه $f(x)=(x-a_1)q_1(x)$ که $\deg q_1(x)=n-1$. صفری چون $a_2\in F$ از $q_1(x)$ به تجزیه‌ای به صورت $f(x)=(x-a_1)(x-a_2)q_2(x)$ منجر می‌شود.

با ادامه این روند سرانجام به تجزیه‌ای به صورت $f(x)=(x-a_1)(x-a_2)\cdots(x-a_r)q_r(x)$ می‌رسیم. که دیگر $q_r(x)$ صفری در F نداشته باشد. واضح است که $r\leq n$. همچنین اگر $b\in F$ و برای $i=1,2,\ldots,r$ داشته باشیم $b\neq a_i$ آنگاه $f(b)=(b-a_1)(b-a_2)\cdots(b-a_r)q_r(b)\neq 0$ زیرا که F مقسوم علیه صفر ندارد و هیچکدام از $b-a_i$ها و $q_r(b)$ صفر نیستند. بنابراین a_iها برای $i=1,2,\ldots$ و $r\leq n$ تمام صفرهای $f(x)$ در F است.

مثال ۸: حلقه $\mathbb{Z}_5[x]$ را در نظر می‌گیریم و $f(x)=x^4-3x^3+2x^2+4x-1$ و $g(x)=x^2-2x+3$

در این صورت $f(x) = (x^2 - x - 3)\,g(x) + (x+3)$

$x^4 - 3x^3 + 2x^2 + 5x - 1 \;\big|\; x^2 - 2x + 3$

$x^4 - 2x^3 + 3x^2$ | $x^2 - x - 3$

$-x^3 - x^2 + 5x$

$-x^3 + 2x^2 - 3x$

$-3x^2 + 8x - 1$

$-3x^2 + 2x - 3$

$x + 2$

بنابراین $g(x) = x^2 - x - 3$

$r(x) = (x+3)$

$1 = \deg r(x) \leq \deg g(x) = 2$

مثال ۹: اگر $f(x) = x^4 + 3x^3 + 2x + 4 \in Z_5[x]$ باشد $f(x)$ را در این حلقه تجزیه کنید.

حل: بدیهی است که $f(1) = 1 + 3 + 2 + 4 = 10$ یعنی در Z_5 داریم $f(1) = 0$ پس طبق قضیه ۱ داریم (با تقسیم)

$f(x) = (x-1)(x^3 + 4x^2 + 4x + 1)$ همچنین $1 \in Z_5$ صفر از $x^3 + 4x^2 + 4x + 1$ است پس

با تقسیم داریم $f(x) = (x-1)^2(x^2 + 4)$

$f(x) = (x-1)^3(x+1)$

$x^4 + 3x^3 + 2x + 4 \;\big|\; x - 1$

$x^4 - x^3$ | $x^3 + 4x^2 + 4x + 1$

$4x^3 + 2x + 4$

$4x^3 - 4x^2$

$4x^2 + 2x + 4$

$4x^2 - 4x$

$4x + 4 = x + 4$

$x - 1$

$+5 = 0$

Z_5

$x^3 + 4x^2 + 4x + 1 \;\big|\; x - 1$

$x^3 - x^2$ | $x^2 + 4$

$5x^2 + 4x + 1$

$5x^2 - 5x$

$0 + 4x + 1$

$4x - 4$

0

Z_5

$5x^2 = 0$

$x^2 + 4 \;\big|\; x - 1$

$x^2 - x$ | $x + 1$

$x + 4$

$x - 1$

0

مثال ۱۰: در $Z_5[x]$ چندجمله‌ای $f(x) = x^2 + 3x + 2$ قابل تجزیه نیست زیرا در Z_5 صفر ندارد

$f(0) = 2,\ f(1) = 1,\ f(2) = 1,\ f(3) = 2,\ f(4) = 3$

مثال ۱۱: چندجمله‌ای $f(x) = x^2 + 1$ روی $\mathbb{R}[x]$ و $\mathbb{Q}[x]$ و $Z_3[x]$ دارای صفر نیست ولی روی $\mathbb{C}[x]$ و $Z_2[x]$ و $Z_5[x]$ دارای صفر است

$(x^2+1) \in Z_5[x]$ $\quad x^2 + 1 = 0 \begin{cases} x = 2 \\ x = 3 \end{cases}$

$(x^2+1) \in \mathbb{C}[x]$ $\quad x^2 + 1 = 0 \begin{cases} x = i \\ x = -i \end{cases}$

$(x^2+1) \in Z_2[x]$ $\quad x^2 + 1 = 0 \longrightarrow x = 1$

چند جمله‌ایهای تحویل ناپذیر

تعریف: چندجمله غیرثابت $f(x) \in F[x]$ بروی F تحویل ناپذیر (یا یک چندجمله‌ای تحویل ناپذیر در $F[x]$ است) است درصورتی که نتوان $f(x)$ را به حاصل ضرب چندین $g(x)h(x)$ تجزیه کرد که درجه هر دوی $g(x)$ و $h(x)$ از درجه $f(x)$ کمتر باشد.

توجه: ممکن است یک چندجمله‌ای روی میدان F تحویل ناپذیر باشد ولی روی میدانی مانند E که $F \subseteq E$ تحویل پذیر باشد. مثال ۱۲ $f(x) = x^2+1$ روی $\mathbb{R}$ تحویل ناپذیر است ولی روی $\mathbb{C}$ تحویل پذیر است. یا $f(x) = x^2-2$ روی $\mathbb{Q}$ تحویل ناپذیر است ولی روی $\mathbb{R}$ تحویل پذیر است.

مثال ۱۳ $f(x) = x^3+3x+2$ در $Z_5[x]$ تجزیه می‌شود (مثال ۱۰) بنابراین $f(x)$ روی Z_5 تحویل ناپذیر است

قضیه ۴: اگر $f(x)$ در $F[x]$ از درجه ۲ یا ۳ باشد در این صورت $f(x)$ بروی F تحویل پذیر است $\Leftrightarrow$ صفری در F داشته باشد.

اثبات: فرض کنید که $f(x)$ روی F تحویل پذیر باشد پس $f(x) = g(x)h(x)$ و درجه $g(x)$ و $h(x)$ کمتر از درجه $f(x)$ (یعنی کمتر از ۲ یا ۳) است. پس یکی از $g(x)$ یا $h(x)$ باید از درجه ۱ باشد. فرض کنید که $\deg h(x) = 1$ پس $h(x) = x-a$ بنابراین $h(a) = 0$ یعنی a صفری از h است درنتیجه چون $f(a) = g(a)h(a) = 0$ پس a صفری از $f(x)$ هم است. برعکس اگر $f(x)$ صفری در F مانند a داشته باشد طبق نتیجه ۱ از قضیه ۳ آنگاه $x-a$ عاملی از $f(x)$ است بنابراین $f(x)$ تحویل پذیر است.

قضیه ۵: اگر $f(x) \in Z[x]$ آنگاه $f(x)$ با حاصلضربی از دو چندجمله‌ای از درجات r و s در $\mathbb{Q}[x]$ تجزیه می‌شود اگر و فقط اگر تجزیه‌ای با حاصلضرب دو چندجمله‌ای از همان درجات r و s در $Z[x]$ داشته باشد.

اثبات: اگر $f(x)$ در $Z[x]$ با حاصل ضرب دو چندجمله‌ای از درجات r و s مانند $g(x)$ و $h(x)$ تجزیه شود آنگاه $f(x) = g(x)h(x)$ روی $\mathbb{Q}[x]$ هم برقرار است یعنی روی $\mathbb{Q}[x]$ هم تجزیه می‌شود و درجات $g(x)$ و $h(x)$ همان درجه r و s است.

حال اگر $h(x) = g(x)h(x) \in \mathbb{Q}[x]$ که در آن $f(x) = g(x)h(x)$. با یکسان کردن مخرج ضرایب و سپس خارج کردن بزرگترین مقسوم علیه‌های مشترک صورت ضرایب می‌توان $f(x) = \left(\frac{a}{b}\right) g_1(x)h_1(x)$ نوشت که در آن a و b در Z است و $g_1(x), h_1(x) \in Z[x]$ و $\deg g_1(x) = \deg g(x)$ ، $\deg h_1(x) = \deg h(x)$.

این قضیه درحالت کلی تر اثبات می‌شود که در مباحث بعد به آن می‌پردازیم (لم ۶).

نتیجه: اگر $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ در $Z[x]$ باشد و $a_0 \neq 0$. و اگر $f(x)$ صفری در $\mathbb{Q}[x]$ داشته باشد. آنگاه صفری چون m در $Z[x]$ دارد و m باید a_0 را عاد کند.

اثبات: اگر $f(x)$ صفری چون a در $\mathbb{Q}$ داشته باشد. آنگاه بنابر نتیجه ۱ از قضیه ۳، $x-a$ عاملی از $f(x)$ در $\mathbb{Q}[x]$ است. در این صورت بنابر قضیه ۵، $f(x)$ تجزیه‌ای شامل یک عامل خطی در $Z[x]$ دارد، درنتیجه با ازای یک $m \in Z$، باید داشته باشیم $f(x) = (x-m)\left(x^{n-1} + \cdots + \frac{a_0}{m}\right)$ پس $\frac{a_0}{m}$ در Z است از این رو $m \mid a_0$.

مثال ۱۴: نشان دهید که $f(x)=x^4-2x^3+11x+1$ روی $\mathbb{Q}$ تحویل ناپذیر است.

حل: اگر $f(x)$ عاملی خطی در $\mathbb{Q}[x]$ داشته باشد، آنگاه صفری در $\mathbb{Z}$ دارد و طبق نتیجه قبل این صفر باید در ± 1 باشد، یعنی کسری از ± 1 باشد، اما $f(1)=11$ و $f(-1)=-15$ بنابراین چنین تجزیه‌ای ممکن است. اگر $f(x)$ در $\mathbb{Q}[x]$ به دو عامل درجه دوم تجزیه شود آنگاه بنابر قضیه قبل تجزیه‌ای در $\mathbb{Z}[x]$ به صورت $f(x)=x^4-2x^3+11x+1=(x^2+ax+b)(x^2+cx+d)$ دارد، یعنی

$$\begin{cases} bd=1 & (1)\\ ad+bc=11 & (2)\\ ac+b+d=-2 & (3)\\ a+c=0 & (4)\end{cases}$$

با مساوی قرار دادن ضرایب دو طرف مساوی با استفاده از دستگاه مقابل می‌رسیم که در آن a,b,c,d در $\mathbb{Z}$ در نظر گرفته شده است. اگر این دستگاه حل داشته باشد به تناقض می‌رسیم، زیرا از معادله (1) داریم $bd=1$ یا $b=d=1$ یا $b=d=-1$

اگر $b=d=1$ در نظر بگیریم آنگاه معادله (3) نتیجه می‌دهد $a+c=-2$ از طرفی طبق معادله (4) نتیجه می‌دهد $a=-c=2$ یا $a=-c=-2$ با توجه به معادله (2) داریم $ad+bc=2-2=0$ یا $ad+bc=-2+2=0$ که قابل قبول نیست اگر $b=d=-1$ باشد طبق معادله (1) $ac=0$ و طبق معادله (4) $a=-c=0$ که در این صورت هم طبق معادله (2) $0=11$ که تناقض است.

پس تجزیه $f(x)$ با حاصل ضرب دو چندجمله‌ای از درجه ۲ غیرممکن است پس $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.

قضیه ۶ (محک اینزنشتاین): فرض کنید $f(x)=a_nx^n+\cdots+a_1x+a_0$ و $p\in\mathbb{Z}$ عددی اول باشد. فرض کنید یک چندجمله‌ای از درجه n در $\mathbb{Z}[x]$ باشد و $a_n\not\equiv 0 \pmod p$ اما برای هر $i<n$ داشته باشیم $a_i\equiv 0 \pmod p$ و همچنین $a_0\not\equiv 0 \pmod{p^2}$ در این صورت $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.

برهان: طبق قضیه قبل کافی است نشان دهیم که $f(x)$ به چندجمله‌ای از درجه کمتر در $\mathbb{Z}[x]$ تجزیه نمی‌شود. اگر $f(x)=(b_rx^r+\cdots+b_0)(c_sx^s+\cdots+c_0)$ تجزیه‌ای در $\mathbb{Z}[x]$ باشد و $b_r\neq 0$، $c_s\neq 0$ و $r,s<n$ آنگاه چون $a_0\not\equiv 0 \pmod{p^2}$ آنگاه هردو b_0 و c_0 با هنگ p با صفر همنهشت نیستند. فرض کنید $b_1\not\equiv 0 \pmod p$ و $c_0\equiv 0 \pmod p$. اکنون چون $a_n\not\equiv 0 \pmod p$ نتیجه می‌دهد که $b_r,c_s\not\equiv 0 \pmod p$ زیرا $a_n=b_rc_s$. فرض کنید که m کوچکترین عضو $\{1,2,\dots,n-1\}$ باشد به طوری که $c_m\not\equiv 0 \pmod p$ در این صورت با ازای مقادیری از i که $0<i<m$ داریم

$$a_m=b_0c_m+b_1c_{m-1}+\cdots+b_{m-i}c_i.$$

اکنون از این که هیچکدام از $c_{i+1},\dots,c_{m-1}$ و c_i همگی با هنگ p با 0 همنهشت نیستند و اعداد b_0 و c_m با هنگ p با 0 همنهشت نیستند نتیجه می‌شود که $a_m\not\equiv 0 \pmod p$ از این رو $m=n$ و در نتیجه $s=n$. و این متناقض با فرض $s<n$ است. بنابراین $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.

مثال ۱۵: نشان دهید که $f(x)=25x^5-9x^4+3x^2-15$ روی $\mathbb{Q}$ تحویل ناپذیر است.

حل: قرار می دهیم که $p=3$ (در قضیه قبل) چون $a_0 = -12 \not\equiv 0 \pmod{3^2}$ و همچنین 9 و 3 و $12-$ با هنگ 3 با عبور و $a_0 = -12 \not\equiv 0 \pmod{9}$ پس طبق محک اینزنشتاین $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.

نتیجه: چند جمله ای $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+x+1$ برای هر عدد اول p روی $\mathbb{Q}$ تحویل ناپذیر است.

اثبات: طبق قضیه ۳ کافی است که نشان دهیم که $\Phi_p(x)$ برای هر عدد اول p در $\mathbb{Z}[x]$ تجزیه نمی شود. فرض کنید که

$$g(x) = \Phi_p(x+1) = \frac{(x+1)^p-1}{x+1-1} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + px}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + p$$

$g(x)$ با ازای عدد اول p در محک اینزنشتاین صدق می کند بنابراین روی $\mathbb{Q}$ تحویل ناپذیر است.

اما اگر $\Phi_p(x) = h(x)\,r(x)$ تجزیه ای ناپدیدی از $\Phi_p(x)$ در $\mathbb{Z}[x]$ باشد آنگاه

$g(x) = \Phi_p(x+1) = h(x+1)\,r(x+1)$ تجزیه ای ناپدیدی در $\mathbb{Z}[x]$ دارد که یک تناقض است.

ایده آل های $F[x]$ چگونه هستند؟

در قضیه زیر نشان می دهیم که هر ایده آل از $F[x]$ که در آن F یک میدان است ایده آل اصلی است یعنی برای هر میدان F، $F[x]$ یک حوزه ایده آل اصلی یعنی P.I.D است.

قضیه ۷: اگر F میدان باشد آنگاه هر ایده آل $F[x]$ اصلی است.

اثبات: فرض کنید که N یک ایده آل از $F[x]$ باشد. اگر $N = \{0\}$ آنگاه $N = \langle 0 \rangle$ پس ایده آل اصلی است حال فرض کنید که $N \neq \{0\}$ و فرض کنید که $g(x)$ عضو ناصفر از N با درجه می نیمال باشد اگر درجه $g(x)$ صفر باشد آنگاه $c = g(x) \in F$ و در نتیجه $c^{-1} \in F$ و $1 = c^{-1}c \in N$ پس $N = F[x] = \langle 1 \rangle$ (قضیه ادغام ایده آل ها)، پس N ایده آل اصلی است.

اگر درجه $g(x)$ بزرگتر یا مساوی یک باشد ($\deg g(x) \geq 1$) فرض کنید که $f(x) \in N$ دلخواه باشد در این صورت طبق قضیه الگوریتم تقسیم داریم $f(x) = g(x)q(x) + r(x)$ که $\deg r(x)$ کوچکتر از $\deg g(x)$ و $q(x) \in N$ و $r(x) \in N$ چون N یک ایده آل است پس $r(x) = f(x) - g(x)q(x) \in N$. چون $g(x)$ عضو ناصفر از درجه می نیمال فرض شده است پس باید $r(x) = 0$ یعنی $f(x) = g(x)q(x)$ پس $N = \langle g(x) \rangle$.

قضیه ۸: ایده آل $\langle p(x) \rangle \neq \{0\}$ از $F[x]$ ماکسیمال است $\iff$ $p(x)$ روی F تحویل ناپذیر باشد (F میدان)

اثبات: فرض کنید که $\langle p(x) \rangle \neq \{0\}$ ایده آل ماکسیمالی از $F[x]$ باشد در این صورت $\langle p(x) \rangle \neq F[x]$ پس $p(x) \notin F$. فرض کنید که $p(x) = f(x)\cdot g(x)$ تجزیه ای از $p(x)$ در $F[x]$ باشد چون $\langle p(x) \rangle$ ایده آل ماکسیمال و در نتیجه ایده آل اصلی است (زیرا $F[x]$ حوزه ای ایده آل اصلی است) پس $f(x) \in \langle p(x) \rangle$ یا $g(x) \in \langle p(x) \rangle$ یعنی که یکی از $f(x)$ یا $g(x)$ چند جمله ای $p(x)$ را به عنوان یک عامل دارد. اما در این صورت می توان گفت که

درجات $f(x)$ و $g(x)$ هر دو از $p(x)$ کمتر است بنابراین $p(x)$ تحویل ناپذیر است

برعکس: فرض کنید که $p(x)$ در F تحویل ناپذیر باشد و N یک ایده‌آل از $F[x]$ باشد بطوریکه $\langle p(x)\rangle \subseteq N \subseteq F[x]$

طبق قضیه قبل چون N یک ایده‌آل اصلی است پس $N=\langle g(x)\rangle$; $\exists g(x)\in N$

از $p(x)\in N$ نتیجه می‌شود که $\exists q(x)\in F[x]$ بطوریکه $p(x)=g(x)q(x)$ اما $p(x)$ تحویل ناپذیر است و از این رو یا یکی از $g(x)$ و $q(x)$ از درجه صفر باشند. اگر $\deg g(x)=0$ یعنی $g(x)=a\in F$ آنگاه $g(x)$ یکی از $F[x]$ است و نتیجه می‌شود که $N=\langle g(x)\rangle = F[x]$. اگر $\deg q(x)=0$ آنگاه $q(x)=c$ $c\in F$

و در نتیجه $g(x)=\frac{1}{c}p(x)$ در $\langle p(x)\rangle$ قرار دارد پس $N=\langle p(x)\rangle$ بنابراین $\langle p(x)\rangle \subset N \subset F[x]$ غیرممکن است پس $\langle p(x)\rangle$ ایده‌آل ماکسیمال است

مثال ۱۶: طبق مثال‌های قبل الف) $\langle 25x^5-9x^4+3x^2-12\rangle$ یک ایده‌آل ماکسیمال از $\mathbb{Q}[x]$ است

ب) $\langle x^4-2x^3+2x^2+1\rangle$ یک ایده‌آل ماکسیمال از $\mathbb{Q}[x]$ است

ج) $\langle x^3+3x+2\rangle$ یک ایده‌آل ماکسیمال از $\mathbb{Z}_5[x]$ است.

د) $\langle x^2+1\rangle$ و $\langle x^2+4\rangle$ ایده‌آل ماکسیمال در $\mathbb{R}[x]$ و $\mathbb{Q}[x]$ هستند.

بنابراین $\frac{\mathbb{R}[x]}{\langle x^2+1\rangle}$ و $\frac{\mathbb{Q}[x]}{\langle x^2+1\rangle}$ و $\frac{\mathbb{R}[x]}{\langle x^2+4\rangle}$ و $\frac{\mathbb{Q}[x]}{\langle x^2+5\rangle}$ و $\frac{\mathbb{Z}_5[x]}{\langle x^3+3x+2\rangle}$ میدان هستند

همچنین $\frac{\mathbb{Q}[x]}{\langle x^5-2x^2+4x+1\rangle}$ و $\frac{\mathbb{Q}[x]}{\langle 25x^5-9x^4+3x^2-12\rangle}$ میدان هستند

تعریف: عضو ناصفر p از حوزه صحیح D که یکای D نیست را یک عنصر تحویل ناپذیر از D می‌نامیم به شرطی که در هر تجزیه $p=ab$ در D یکی از a و b یکا باشد یا به عبارت دیگر p به حاصل ضرب دو یا چند عنصر یکا تجزیه نشود.

مثال ۱۷: اعداد اول در رده عناصر تحویل ناپذیر هستند و اگر F میدان باشد هر چند جمله‌ای $p(x)\in F[x]$ در $F[x]$ تحویل ناپذیر است اگر و فقط اگر $\langle p(x)\rangle$ ایده‌آل ماکسیمال $F[x]$ باشد

تعریف: در حوزه صحیح D دو عضو $a,b\in D$ را شریک نامیم هرگاه یکی از D مانند u موجود باشد که $a=bu$.

توجه: هر شریک یک تحویل ناپذیر در حوزه صحیح D خود تحویل ناپذیر است.

تعریف: حوزه صحیح D را یک حوزه تجزیه یکتا (U.F.D) است در صورتیکه

۱- هر عضو ناصفر و ناوکای D متوان یا حاصل ضربی از تعداد متناهی تحویل ناپذیر تجزیه کرد

۲- اگر $P_1 P_2 \cdots P_r = q_1 q_2 \cdots q_s$ دو تجزیه به تحویل ناپذیرها از یک عضو D باشند آنگاه $r = s$ و q_i ها را بتوان طوری مجدداً شماره گذاری کرد که P_i و q_i شریک باشند.

مثال ۱۸: $\mathbb{Z}$ یک حوزه تجزیه یکتا (یا UFD) است و در $\mathbb{Z}$ داریم $24 = 2 \times 12 = 3 \times 8 = (-2)(-3)(2)(2) = 24$
۲ و ۲- در $\mathbb{Z}$ شریک هستند و ۳ و ۳- در $\mathbb{Z}$ شریک هستند.

تعریف: برای $f(x), g(x) \in F[x]$ بزرگترین در $F[x]$ چندجمله‌ای $d(x)$ را چندجمله‌ای $f(x)$ را عاد می‌کند در صورتی که یک چندجمله‌ای مانند $h(x)$ در $F[x]$ موجود باشد بطوریکه $f(x) = g(x) h(x)$.

قضیه ۹: ثابت کنید که $P(x) \in F[x]$ یک چندجمله‌ای تحویل ناپذیر باشد اگر برای $S(x), r(x) \in F[x]$ داشته باشیم $P(x) \mid r(x)s(x)$ آنگاه $P(x) \mid r(x)$ یا $P(x) \mid s(x)$.
زیرا $\exists f(x) \in F[x] : r(x)s(x) = P(x)f(x)$

اثبات: فرض کنید که $P(x) \mid r(x)s(x)$ در این صورت $r(x)s(x) \in \langle P(x) \rangle$ حیث $\langle P(x) \rangle$ ایده‌آل اصلی است بس طبق قضیه‌ای در مورد ایده‌آل اول است بنابراین $r(x) \in \langle P(x) \rangle$ یا $s(x) \in \langle P(x) \rangle$ که نتیجه می‌دهد $P(x) \mid r(x)$ یا $P(x) \mid s(x)$.

نتیجه: اگر $P(x)$ در $F[x]$ تحویل ناپذیر باشد و $P(x)$ حاصل ضرب $r_1(x) r_2(x) \cdots r_n(x)$ عاد کند که در آن $r_i(x) \in F[x]$ $\forall i = 1, 2, 3, \ldots, n$ آنگاه برای یک مقدار i: $P(x) \mid r_i(x)$.

اثبات (با روش استقرای ریاضی)

قضیه ۱۰: اگر F یک میدان باشد آنگاه $F[x]$ یک حوزه تجزیه یکتا یعنی UFD است. به عبارت دیگر هر چندجمله‌ای غیرثابت $f(x) \in F[x]$ را می‌توان یا حاصل ضربی از چندجمله‌ای‌های تحویل ناپذیر در $F[x]$ تجزیه کرد و این تجزیه چندجمله‌ای‌های تحویل ناپذیر یکتا هستند، مگر در صورت ترتیب آنها و وجود عوامل یکال (یعنی ثابت‌های ناصفر) از F.

اثبات: فرض کنید که $f(x) \in F[x]$ یک چندجمله‌ای غیرثابت باشد اگر $f(x)$ تحویل ناپذیر باشد آنگاه $f(x) = g(x) h(x)$ که در آن $g(x)$ و $h(x)$ کمتر از درجه $f(x)$ هستند اگر $g(x)$ و $h(x)$ هر دو تحویل ناپذیر باشند که مسئله حل است و اثبات تمام می‌شود، در غیر این صورت حداقل یکی از آنها یا حاصل ضرب چندجمله‌ای‌هایی از درجه کوچکتر تجزیه می‌شود با ادامه این روند می‌توان نوشت $f(x) = P_1(x) P_2(x) \cdots P_r(x)$ که $P_i(x)$ ها تحویل ناپذیر هستند. برای یکتایی! فرض کنید که $f(x) = P_1(x) P_2(x) \cdots P_r(x) = q_1(x) q_2(x) \cdots q_s(x)$

حوزه تجزیه $f(x)$ یا چندجمله‌ای‌های تحویل ناپذیر باشد اکنون طبق قضیه قبل $P_1(x)$ یکی از چندجمله‌ای‌های $q_j(x)$ عاد می‌کند، می‌توان فرض کرد که $P_1(x) \mid q_1(x)$ چون $q_1(x)$ تحویل ناپذیر است پس $q_1(x) = u_1 P_1(x)$ که $u_1 \neq 0$ چون F یک میدان است. اکنون با جایگزینی $u_1 P_1(x)$ بجای $q_1(x)$ و حذف عوامل مساوی داریم

$$P_2(x) P_3(x) \cdots P_r(x) = u_1 q_2(x) q_3(x) \cdots q_s(x)$$

با استدلال مشابه حالت قبل $q_1(x) = u_2 p_2(x)$ و بنابراین $p_1(x) \cdots p_r(x) = u_1 u_2 q_1(x) \cdots q_s(x)$

با ادامه این روند سرانجام می رسیم به $1 = u_1 u_2 \cdots u_r q_{s-1}(x) \cdots q_s(x)$ *

این عبارت * وقتی درست است که $s = r$ و از این رو این یکه ها به صورت $1 = u_1 u_2 \cdots u_r$ است

بنابراین عوامل $p_i(x)$ و $q_j(x)$ در تجزیه های $f(x)$ یکی هستند مگر در ترتیب آنها و عوامل یکال ها.

مثال ۱۹: در $Z_5[x]$ برای $f(x) = x^4 + 3x^3 + 2x + 4$ داریم $f(x) = (x-1)^2(x+1)$

یعنی می توان نوشت $f(x) = x^4 + 3x^3 + 2x + 4 = (x-1)^2(x+1) = (x-1)^2(3x-2)(3x+3)$

زیرا $3, 2 \in Z_5$ و وارون ضربی هم هستند در Z_5 یکال می باشند.

توجه: در ادامه این بخش ثابت می کنیم ۱) هر P.I.D یک U.F.D است.

۲) اگر D یک U.F.D باشد آنگاه $D[x]$ یک U.F.D است.

بالبات این دو گزاره با ثبات تعدادی از قضیه های جبر کمپرس $F[x]$ ثابت کردیم در حالت کلی ثابت می شود.

از مباحث ریاضی تعریف زیر را یادآوری می کنیم (اجتماع خانواده ها).

تعریف: اگر $\{A_i \mid i \in I\}$ گردایه ای از مجموعه ها باشد آنگاه اجتماع مجموعه های A_i یعنی $\bigcup_{i \in I} A_i$ عبارت است از مجموعه تمام x هایی که حداقل با ازای $i \in I$ داشته باشیم $x \in A_i$ یا عبارت دیگر

$$\bigcup_{i \in I} A_i = \{ x \mid \exists i \in I \ \ x \in A_i \}$$

لمر ۱: (شرط زنجیر صعودی برای یک P.I.D): فرض کنید که D یک حوزه ایده آل اصلی یعنی P.I.D باشد اگر $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ یک زنجیر صعودی یکنواخت از ایده آلهای N_i در D باشد، آنگاه عددی صحیح و مثبت چون n وجود دارد بطوریکه برای هر $s \geq n$ ، $N_s = N_n$ به عبارت دیگر هر زنجیر صعودی ایده آل (که در آن تمام جزء شمولها اکید باشند) از ایده آلهای یک P.I.D به طول متناهی است. مختصراً در هر P.I.D شرط زنجیر صعودی (بس نرص) برقرار است.

اثبات: فرض کنید که $N_1 \subseteq N_2 \subseteq \cdots$ زنجیر صعودی و یکنواخت از ایده آل های N_i در D باشد قرار می دهیم $N = \bigcup_{i \in I} N_i$ و واضح $N \subseteq D$ ادعا می کنیم که N ایده آلی از D است. فرض کنید که $a, b \in N$ در این صورت ایده آل های N_1 و N_2 وجود دارند که بطوریکه $a \in N_1$ و $b \in N_2$ اما $N_1 \subseteq N_2$ یا $N_2 \subseteq N_1$ فرض کنید که $N_1 \subseteq N_2$ (بدون اینکه از کلیت بحث خللی وارد شود) از این رو $a, b \in N_2$ چون N_2 ایده آل است پس $a - b \in N_2$ و $ab \in N_2$ یعنی $a - b \in N$ و $ab \in N$. چون $a \in N_i$ برای هر i پس $0 \in N$ یعنی N زیر حلقه D است و به همین صورت برای هر $a \in N$ و $d \in D$، $da \in N$.

چون N_r ایده‌آل D است پس $ad=da\in N_r$ پس $ad=da\in N$ یعنی N یک ایده‌آل D است.

چون D یک P.I.D است پس هر ایده‌آل آن اصلی است. پس $\exists c\in N$ که $N=\langle c\rangle$. با توجه به اینکه $N=\bigcup_{i\in I} N_i$ باید به ازای یک $r\in\mathbb{Z}^+$ داشته باشیم $c\in N_r$. به ازای هر $s\geq r$ داریم.

$$\langle c\rangle\subseteq N_r\subseteq N_s\subseteq N=\langle c\rangle$$

پس به ازای هر $s\geq r$، $N_s=N_r$. هم‌ارزی با آنچه خواسته بدیهی است.

تبصره: برای هر $a,b\in D$ که D یک P.I.P است داریم 1) $\langle a\rangle\subseteq\langle b\rangle$ اگر و فقط اگر $b\mid a$.

2) $\langle a\rangle=\langle b\rangle$ اگر و فقط اگر a و b شریک باشند.

زیرا: برای (1) اگر $\langle a\rangle\subseteq\langle b\rangle$ آنگاه $a\in\langle b\rangle$ پس $\exists c\in D$ بطوریکه $a=bc$ پس $b\mid a$.

برای 2) اگر $\langle a\rangle=\langle b\rangle$ آنگاه $\langle b\rangle\subseteq\langle a\rangle$ و $\langle a\rangle\subseteq\langle b\rangle$ و طبق (1) $b\mid a$ و $a\mid b$ پس وجود دارد $d_1,d_2\in D$ بطوریکه $a=bd_1$ و $b=ad_2$ در نتیجه $a=ad_1d_2$ حالت $a=0$ بدیهی است و برای حالت $a\neq 0$ نتیجه می‌شود $d_1d_2=1$ بنابراین d_1 و d_2 یکال هستند، پس a و b شریک هستند.

قضیه ۱۱: فرض کنید که D یک P.I.P باشد، هر عضو ناصفر و غیریکال مانند a از D حاصلضربی از تحویل ناپذیرها است.

اثبات: فرض کنید که $a\in D$ و $a\neq 0$ و a یکال نباشد. اگر a خودش تحویل ناپذیر باشد که کار انجام شده است در غیر این صورت می‌توان نوشت $a=ba_1$ که هیچکدام از a_1 و b یکال نباشد، اکنون $\langle a\rangle<\langle a_1\rangle$.

اگر $\langle a\rangle=\langle a_1\rangle$ آنگاه a و a_1 شریک می‌شوند و در نتیجه b یکال می‌شود که با فرض متناقض است با ادامه این فرایند برای a_1 (یا برای b) و الی آخر به یک زنجیر صعودی آیده به صورت $\langle a\rangle<\langle a_1\rangle<\langle a_2\rangle<\cdots$ می‌رسیم بنابراین طبق لم الشرط زنجیر صعودی، این زنجیر در یک $\langle a_n\rangle$ پایان می‌یابد و باید a_n تحویل ناپذیر باشد.

پس a حاصل تحویل ناپذیری چون a_n دارد حال با فرض $p_1=a_n$ داریم $a=p_1c_1$ که c_1 یکال است بنابراین $\langle a\rangle<\langle c_1\rangle$ اگر c_1 تحویل ناپذیر باشد آنگاه می‌توان قرار داد $c_1=p_2c_2$ که در آن p_2 تحویل ناپذیری در D است و c_2 یکال نیست. با ادامه این روند به یک زنجیر صعودی آیده $\langle a\rangle\subset\langle c_1\rangle\subset\langle c_2\rangle\subset\cdots$ می‌رسیم و طبق لم الشرط زنجیر صعودی باید این زنجیر توسط عضوی چون c_r یعنی یک تحویل ناپذیر خاتمه یابد در این صورت

پایان یابد

$$a=p_1p_2\cdots p_r$$

لم ۲: (تعمیم تمرین ۸) ایده‌آل $\langle p\rangle$ در یک P.I.D یک ایده‌آل ماکسیمال است اگر و فقط اگر p تحویل ناپذیر باشد.

اثبات: فرض کنید که D یک P.I.P باشد و $\langle p\rangle$ ایده‌آل ماکسیمالی از آن باشد و در D داشته باشیم $p=ab$ بدیهی است که $\langle p\rangle\subseteq\langle a\rangle$ اگر $\langle p\rangle=\langle a\rangle$ آنگاه p و a با هم شریک می‌شوند و بنابراین b یکال است. اگر $\langle p\rangle\neq\langle a\rangle$ آنگاه باید $\langle a\rangle=\langle 1\rangle=D$ زیرا $\langle p\rangle$ ماکسیمال است اما در این صورت

در این صورت a و b شریک می‌شوند و در نتیجه a یکای از D می‌شود. بنابراین اگر $p=ab$ آنگاه یکی از a و b یکال می‌شوند پس p تحویل ناپذیری از D است.

برعکس: فرض کنید که p تحویل ناپذیری از D باشد در صورتی که $\langle p\rangle \subseteq \langle a\rangle \subseteq D$ در این صورت $p=ab$ حال اگر a یکال باشد آنگاه $\langle a\rangle = \langle 1\rangle = D$، اگر a یکال نباشد آنگاه با توجه به اینکه p تحویل ناپذیر است پس عضوی $u\in D$ وجود دارد که $bu=1$ در این صورت $pu=abu=a$ از این رو $\langle p\rangle \subseteq \langle a\rangle$ و در نتیجه $\langle a\rangle = \langle p\rangle$ بنابراین $\langle p\rangle$ یک ایده‌آل ماکسیمال است (توجه $\langle p\rangle \neq D$ چون p یکال نیست).

لم ۳: (تعمیم قضیه ۹) در یک P.I.D اگر p تحویل ناپذیر باشد و $p\mid ab$ آنگاه $p\mid a$ یا $p\mid b$.

اثبات: فرض کنید که D یک P.I.D باشد و p عضو تحویل ناپذیری از D باشد و $p\mid ab$ پس $ab \in \langle p\rangle$ چون هر ایده‌آل ماکسیمال یک ایده‌آل اول است از $ab\in\langle p\rangle$ نتیجه می‌شود $a\in\langle p\rangle$ یا $b\in\langle p\rangle$. بنابراین $p\mid a$ یا $p\mid b$.

نتیجه: اگر p عضو تحویل ناپذیری از یک P.I.D مانند D باشد و $p\mid a_1a_2\cdots a_n$ آنگاه حداقل برای یک i ای $p\mid a_i$.

اثبات: طبق روش استقرا ریاضی ثابت می‌شود

تعریف: عضو ناصفر و ناکال p از یک حوزه صحیح D یک عضو اول است در صورتی که همواره از $p\mid ab$ نتیجه شود $p\mid a$ یا $p\mid b$.

تبصره: در تمرین ۱۷ نشان داده می‌شود که الف) هر عضو اول در یک حوزه صحیح همواره یک تحویل ناپذیر است. و همچنین ب) در یک U.F.D هر تحویل ناپذیری یک عضو اول است.

بنابراین در یک U.F.D عضو اول و تحویل ناپذیر یکی هستند.

در مثال زیر نشان می‌دهیم که حوزه صحیحی وجود دارد که شامل تحویل ناپذیرهایی است که اول نیستند.

مثال ۱۹: فرض کنید که F یک میدان باشد و D زیر حوزه $F[x,y]$ باشد که توسط $F+xyf(x,y)$ از x^2 و xy و y^2 تولید می‌شود در این صورت x^2 و xy و y^2 تحویل ناپذیرهایی در D هستند اما

$$(x^2)(y^2)=(xy)(xy)$$

چون xy عادی که x^2y^2 اما xy عضو x^2 یا y^2 را عاد نمی‌کند ولی xy عضو اول در D نیست با استدلالی مشابه می‌توان نشان داد که x^2 و y^2 هم اول نیستند.

قضیه ۱۲ (تعمیم قضیه ۱۰) هر P.I.D یک U.F.D است.

اثبات: طبق قضیه ۱۱ اگر در یک P.I.D باشد آنگاه هر $a\in D$ که $a\neq 0$ و a یکال نیست، تجزیه‌ای با صورت زیر دارد $a=p_1p_2\cdots p_r$ که $p_1,p_2,\dots,p_r$ تحویل ناپذیر هستند برای یکتایی به صورت زیر عمل می‌کنیم.

فرض کنید که $a=q_1q_2\cdots q_s$ تجزیه دیگری با تحویل ناپذیرهای در D باشد اکنون $p_1\mid q_1q_2\cdots q_s$ پس $p_1\mid q_{i_1}$ به ازای یک i_1 با تعویض ترتیب q_i ها در صورت لزوم، فرض کنید که $i=1$ و در نتیجه $p_1\mid q_1$ و چون q_1 یک تحویل ناپذیر است پس u_1 با p_1 یکال باشد پس p_1 و q_1 شریک هستند پس داریم $q_1=p_1u_1$.

بنابراین طبق مطالب فوق داریم $p_1p_2\cdots p_r = p_1u_1p_2\cdots q_s$ یا $p_2\cdots p_r = u_1q_2\cdots q_s$

با ادامه این روند و با شروع از p_2 و ادامه آن سرانجام به تساوی $1 = u_1u_2\cdots u_r q_{r+1} \cdots q_s$ می‌رسیم. چون q_j ها تحویل ناپذیر هستند باید داشته باشیم $s=r$ یعنی تجزیه a یکتا است.

—>——<—

نتیجه: (قضیه اساسی حساب) حوزه صحیح $\mathbb{Z}$ یک حوزه تجزیه یکتا (U.F.D) است.

اثبات: چون $\mathbb{Z}$ یک P.I.D است پس طبق قضیه قبل $\mathbb{Z}$ یک U.F.D می‌شود.

—>——<—

تعریف: فرض کنید که D یک U.F.D باشد. چند جمله‌ای غیرثابت $f(x) = \sum_{i=0}^{n} a_i x^i$ از $D[x]$ را یک چند جمله‌ای اولیه نامیم اگر و فقط اگر تنها مقسوم علیه مشترک‌های تمام a_i ها یکال‌های D باشند و اگر $a_n = 1$ باشد چند جمله‌ای $f(x)$ را یک چند جمله‌ای تکین در $D[x]$ می‌نامیم.

مثال ۲۰: در $\mathbb{Z}[x]$، $f(x) = 2+3x+4x^2$ یک چند جمله‌ای اولیه است ولی $g(x) = 2+6x+4x^2$ یک چند جمله‌ای اولیه نیست و $h(x) = 3+2x^2+x^3$ را یک چند جمله‌ای تکین در $\mathbb{Z}[x]$ ...

توجه: بدیهی است که هر تحویل ناپذیر غیرثابت در $D[x]$ باید یک چند جمله‌ای اولیه باشد زیرا یکال‌های D همان یکال‌های $D[x]$ است.

لم ۴: اگر D یک U.F.D باشد آنگاه به ازای هر چند جمله‌ای غیرثابت $f(x) \in D[x]$ داریم $f(x) = (c)g(x)$ که در آن $c \in D$ و $g(x) \in D[x]$ و $g(x)$ یک چند جمله‌ای اولیه است. عضو c در حد وجود یک عامل یکال در D منحصر به فرد است و محتوای $f(x)$ نامیده می‌شود. همچنین $g(x)$ در حد وجود عامل یکالی از D منحصر به فرد است.

اثبات: فرض کنید $f(x) \in D[x]$ و $f(x)$ غیرثابت باشد. چون D یک U.F.D است، هر یک از ضرایب $f(x)$ را می‌توان در حد ترتیب و عامل یکال به حاصل ضرب متناهی از تحویل ناپذیرهای D تجزیه کرد. c را بزرگترین مقسوم علیه مشترک ضرایب $f(x)$ در D در نظر می‌گیریم و با توجه به آن داریم $f(x) = c\,g(x)$ که در آن $g(x)$ یک چند جمله‌ای اولیه است و $g(x) \in D[x]$. برای منحصر به فردی، اگر به ازای $d \in D$ و $h(x) \in D[x]$ داشته باشیم $f(x) = d\,h(x)$ و $h(x)$ یک چند جمله‌ای اولیه باشد آنگاه هر عامل تحویل ناپذیر c باید d را عاد کند و بالعکس. با قرار دادن $c\,g(x) = d\,h(x)$ و حذف تمام تحویل ناپذیرهای c و d به یک تساوی به صورت $u\,g(x) = v\,h(x)$ می‌رسیم که در آن $u \in D$ یک یکال است. اما در این صورت v هم یکالی از D است. مگر آن که بتوانیم عوامل تحویل ناپذیر v را از h جداسازی کنیم. پس u و v هر دو یکال هستند. از این رو c در حد یک عامل یکال منحصر به فرد است. از $f(x) = c\,g(x)$ مشاهده می‌کنیم که چند جمله‌ای اولیه $g(x)$ هم در حد عاملی یکال منحصر به فرد است.

—>——<—

مثال ۲۱: در $\mathbb{Z}[x]$، $f(x) = 4x^2+6x-8 = 2(2x^2+3x-4)$ و $2x^2+3x-4$ یک چند جمله‌ای اولیه است.

لم ۵ (گاوس) اگر D یک U.F.D باشد آنگاه حاصل ضرب هر دو چند جمله‌ای اولیه از $D[x]$ باز یک چند جمله‌ای اولیه است.

اثبات: فرض کنید که $f(x) = \sum_{i=0}^{n} a_i x^i$ و $g(x) = \sum_{j=0}^{m} b_j x^j$ چند جمله‌ای‌های اولیه‌ای در $D[x]$ باشند و فرض کنید $h(x) = f(x)g(x)$. اگر p تحویل ناپذیری از D باشد آنگاه p نه تمام a_i ها را عاد می‌کند و نه تمام b_j ها را زیرا $f(x)$ و $g(x)$ اولیه هستند. فرض کنید برای هر $i<r$، $p|a_i$ و $p\nmid a_r$. به همین منوال، فرض کنید برای هر $j<s$، $p|b_j$ و $p \nmid b_s$. ضریب x^{r+s} در $h(x) = f(x)g(x)$ عبارت است از:

$$c_{r+s} = (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0) = \sum_{i=0}^{r+s} a_i b_{r+s-i}$$

اکنون از این که برای هر $i<r$ ، $p|a_i$ نتیجه می‌شود $p \mid (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1})$ و همچنین از اینکه برای هر $j<s$ ، $p|b_j$ نتیجه می‌شود $p \mid (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0)$ اما p هیچ‌کدام از a_r و b_s را عاد نمی‌کند نتیجه $p \nmid a_r b_s$ پس $p \nmid c_{r+s}$. این نشان می‌دهد که به ازای هر تحویل ناپذیر $p \in D$ ، ضریبی از $f(x)g(x)$ هست که بر p بخش‌پذیر نیست پس $f(x)g(x)$ یک چندجمله‌ای اولیه است

نتیجه: اگر D یک U.F.D باشد، آنگاه هر حاصلضرب متناهی از چندجمله‌ای‌های اولیه در $D[x]$ هم یک چندجمله‌ای اولیه است
اثبات: با روش استقرای ریاضی ثابت می‌شود

لم ۶: فرض کنید D یک U.F.D باشد و F میدان متشکل از خارج قسمت‌های D باشد. فرض کنید که $f(x) \in D[x]$ و $\deg f(x) > 0$ ، اگر $f(x)$ تحویل ناپذیری در $D[x]$ باشد آنگاه $f(x)$ تحویل ناپذیری در $F[x]$ هم هست.
همچنین، اگر $f(x)$ چندجمله‌ای اولیه در $D[x]$ و تحویل ناپذیری در $F[x]$ باشد آنگاه تحویل ناپذیری در $D[x]$ هم هست

اثبات: فرض کنید که یک چندجمله‌ای غیرثابت $f(x) \in D[x]$ با چندجمله‌ای‌ها از درجه کمتر در $F[x]$ تجزیه شود یعنی $f(x) = r(x)s(x)$ که $r(x), s(x) \in F[x]$. چون F میدان خارج قسمت‌های D است. هر یک از ضرایب $r(x)$ و $s(x)$ به صورت $\frac{a}{b}$ است که $a,b \in D$. با ضرب کردن طرفین در مضرب مشترک، بدست می‌آوریم $d f(x) = r_1(x) s_1(x)$ که در آن $d \in D$ و $r_1(x), s_1(x) \in D[x]$ ، و به علاوه درجات $r_1(x)$ و $s_1(x)$ به ترتیب با درجات $r(x)$ و $s(x)$ برابرند.
طبق لم ۴ به ازای چندجمله‌ای‌های اولیه چون $g(x)$ و $r_2(x)$ و $s_2(x)$ و $c \in D$ و c_1, c_2 خواهیم داشت
$f(x) = c\,g(x)$ و $r_1(x) = c_1 r_2(x)$ و $s_1(x) = c_2 s_2(x)$ بنابراین

$$(dc)\,g(x) = (c_1c_2)\,r_2(x)s_2(x)$$

و طبق لم ۵، چندجمله‌ای $r_2(x)s_2(x)$ اولیه است و طبق یکتایی به ازای یکانی مانند u از D ، $c_1c_2 = dcu$
اما در این صورت $(dc)\,g(x) = (dcu)\,r_2(x)s_2(x)$ در نتیجه

$$f(x) = c\,g(x) = (cu)\,r_2(x)s_2(x)$$

بدیهی است که چندجمله‌ای غیرثابتی چون $f(x) \in D[x]$ که در $D[x]$ اولیه است در $F[x]$ تحویل ناپذیر و در $D[x]$ هم تحویل ناپذیر است زیرا $D[x] \subseteq F[x]$.

نتیجه: اگر D یک U.F.D باشد و F میدان متشکل از خارج قسمت‌های D باشد آنگاه یک چندجمله‌ای غیرثابت $f(x)$ از $D[x]$ در $F[x]$ به حاصل ضربی از دو چندجمله‌ای از درجات کمتر r و s تجزیه می‌شود اگر و فقط اگر تجزیه‌ای به حاصلضرب دو چندجمله‌ای از همان درجات r و s در $D[x]$ داشته باشد.

اثبات: در لم قبل دیدیم که اگر $f(x)$ به حاصلضربی از دو چندجمله‌ای از درجات کمتر در $F[x]$ تجزیه شود آنگاه تجزیه‌ای به دو چندجمله‌ای از همان درجات در $D[x]$ دارد. عکس آن بدیهی است زیرا $D[x] \subseteq F[x]$.

قضیه ۱۳: اگر D یک U.F.D باشد آنگاه $D[x]$ هم یک U.F.D است.

اثبات: فرض کنید که $0 \neq f(x) \in D[x]$ و $f(x)$ یکال نباشد. اگر $\deg f(x) = 0$ آنگاه $f(x) = a$ در D به صورت یکتا به حاصلضرب تعداد متناهی تحویل ناپذیر تجزیه می‌گردد و کار انجام شده است. فرض کنید که $\deg f(x) > 0$.

$f(x)$ را عضوی از $F[x]$ در نظر می‌گیریم که در آن F میدان خارج قسمت‌های D است. طبق قضیه ۱، چون $F[x]$ یک U.F.D است می‌توان فرض $f(x)=p_1(x)p_2(x)\cdots p_r(x)$ که $p_i(x)$ها در $F[x]$ تحویل‌ناپذیر هستند. چون F میدان خارج قسمت‌های D است، هر یک از ضرایب $p_i(x)$ها به صورت $\frac{a}{b}$ است که $a,b\in D$. با فرض مخرج مشترک‌گیری و فاکتورگیری به شکل $(d)f(x)=q_1(x)q_2(x)\cdots q_r(x)$ می‌رسیم که در آن $q_i(x)\in D[x]$ و d. چون هر $p_i(x)$ در $F[x]$ تحویل‌ناپذیر است ملاحظه می‌کنیم که $q_i(x)$ که عبارت است از حاصلضرب $p_i(x)$ در یک ثابتی از F، هم در $F[x]$ تحویل‌ناپذیر است. طبق لم ۴ به ازای چندجمله‌ای اولیه $g(x)$ و $q_i'(x)$ در $D[x]$ داریم $f(x)=(c)g(x)$ و $q_i(x)=c_iq_i'(x)$.

پس

$$(dc)g(x)=(c_1\cdots c_r)q_1'(x)\cdots q_r'(x)$$

و طبق لم ۵ حاصل ضرب $q_1'(x)q_2'(x)\cdots q_r'(x)$ یک چندجمله‌ای اولیه است. پس طبق یکتایی لم ۴ به ازای یکالی چون u از D، $c_1\cdots c_r=dcu$. پس $(dc)g(x)=(dcu)q_1'(x)\cdots q_r'(x)$.

اکنون cu را می‌توان به تحویل‌ناپذیرهایی از D تجزیه کرد. همچنین $q_1'(x)$، ... و $q_r'(x)$ تحویل‌ناپذیرهایی در $D[x]$ هستند زیرا اولیه‌اند و نیز در $F[x]$ تحویل‌ناپذیر هستند.

برای یکتایی تجزیه $f(x)\in D[x]$ در حالتی که $f(x)\in D$ و ناصفر و نایکال باشد واضح است. اگر $\deg f(x)>0$ آنگاه طبق لم ۶ هر تجزیه به تحویل‌ناپذیرها در $D[x]$ را می‌توان به عنوان تجزیه‌ای در $F[x]$ در نظر گرفت. بنابر قضیه ۱۰ این چندجمله‌ایها یکتا هستند مگر احیاناً برای وجود عوامل ثابتی از F. اما به عنوان چندجمله‌ای تحویل‌ناپذیری در $D[x]$، هر چندجمله‌ای از درجه بزرگتر از صفر که در تجزیه $f(x)$ در $D[x]$ پدید آید اولیه است. بنابر لم ۴ این چندجمله‌ایها در حد وجود عوامل یکال، یعنی شرکایشان در $D[x]$ یکتا هستند. حاصل‌ضرب تحویل‌ناپذیرهای D در تجزیه $f(x)$ عبارت است از محتوای $f(x)$ که آن هم بنابر لم ۴ در حد وجود یک عامل یکال منحصر به فرد است. پس تمام تحویل‌ناپذیرهایی در $D[x]$ که در تجزیه پدید می‌آیند در حد ترتیب آنها و وجود شریکها منحصر به فرد هستند.

نتیجه: اگر F یک میدان باشد و x_1، x_2، ... و x_n مجهولهایی باشند، آنگاه $F[x_1,\dots,x_n]$ یک U.F.D است.

اثبات: طبق قضیه ۱۰ $F[x_1]$ یک U.F.D است. اکنون $F[x_1,x_2]=(F[x_1])[x_2]$ یک U.F.D است (طبق قضیه قبل). با ادامه این روند به استقراء داریم $F[x_1,x_2,\dots,x_n]$ یک U.F.D است.

توضیح: در حالت کلی نمی‌توان گفت که هر U.F.D یک P.I.D است زیرا $Z[x]$ یک U.F.D است ولی P.I.D نیست. همچنین $F[x,y]$ یک U.F.D است ولی P.I.D نیست زیرا مجموعه تمام چندجمله‌ایها برحسب x و y در $F[x,y]$ را که جمله ثابت آنها صفر است یک ایده‌آل $F[x,y]$ است ولی ایده‌آل اصلی نیست.

تمرین:

۱- خاصیت توزیع پذیری ضرب روی جمع در حلقه $R[x]$ را بررسی کنید.

۲- اگر R یک حوزه صحیح باشد نشان دهید که $R[x]$ یک حوزه صحیح است.

۳- اگر $\phi_0 : \mathbb{Q}[x] \longrightarrow \mathbb{R}$ همومورفیسم ارزیابی باشد (مثال ۴) اعضای حلقه خارج قسمتی $\frac{\mathbb{Q}[x]}{Ker\phi_0}$ را توصیف کنید.

۴- همومورفیسم ارزیابی $\phi_5 : \mathbb{Q}[x] \longrightarrow \mathbb{R}$ را در نظر بگیرید. شش عضو $Ker\phi_5$ را بنویسید.

۵- تمام صفرهای $f(x) = x^5 + 3x^3 + x^2 + 2x$ در Z_5 را بیابید.

۶- اگر F یک میدان باشد، نشان دهید که تمام چند جمله‌ایهای با جمله ثابت $a_0 = 0$ تشکیل ایده‌آل $\langle x \rangle$ از $F[x]$ را می‌دهند و نشان دهید که $F[x]/\langle x \rangle$ میدانی ایزومورف با F است.

۷- چند جمله‌ای $x^4 + 4$ را در $Z_5[x]$ به عوامل خطی (چند جمله‌ای درجه اول) تجزیه کنید.

۸- نشان دهید که $f(x) = x^2 + 1x - 2$ روی $\mathbb{Q}$ تحویل ناپذیر است.

۹- ثابت کنید که اگر F یک میدان باشد، هر ایده‌آل اول دلخواهی از $F[x]$ ماکسیمال است.

۱۰- نشان دهید که چند جمله $x^p + a$ از $Z_p[x]$ با ازای هیچ $a \in Z_p$ تحویل ناپذیر نیست.

۱۱- اگر F یک میدان باشد و $a \neq 0$ صفری از $f(x) = a_0 + a_1x + \cdots + a_nx^n$ در $F[x]$ باشد نشان دهید که $\frac{1}{a}$ صفری $a_n + a_{n-1}x + \cdots + a_0x^n$ است.

۱۲- آیا $\frac{\mathbb{Q}[x]}{\langle x^2 - 5x + 6 \rangle}$ یک میدان است؟ چرا؟ آیا $\frac{\mathbb{Q}[x]}{\langle x^2 - 4x + 6 \rangle}$ میدان است؟

۱۳- فرض کنید که F یک میدان باشد و $f(x), g(x) \in F[x]$. نشان دهید که $f(x) \mid g(x)$ اگر و فقط اگر $g(x) \in \langle f(x) \rangle$

۱۴- در هر حوزه صحیح ما شدال، نشان دهید که نسبت $a \sim b$ به معنی a شریک b است یک رابطه هم ارزی در D است.

۱۵- اگر R و R' در حلقه ایزومورف باشند نشان دهید که حلقه‌های $R[x]$ و $R'[x]$ نیز ایزومورف هستند.

۱۶- فرض کنید که K یک میدان و F زیر میدان K باشد. فرض کنید که $f(x)$ و $g(x) \in F[x]$ در $F[x]$ نسبت به هم اول باشند. ثابت کنید که $f(x)$ و $g(x)$ در $K[x]$ هم نسبت به هم اول هستند.

۱۷- الف) در یک حوزه صحیح هر عضو اول، تحویل ناپذیر است ب) در یک UFD هر عضو تحویل ناپذیر یک عضو اول است. ثابت کنید

ثابت کنید.

حلقه اقلیدسی و حلقه گوسی (حلقه گاوسی)

تعریف: حلقه جابجایی R را یک حلقه اقلیدسی نامیم هرگاه یک تابع $\varphi: R-\{0\} \to \mathbb{N}\cup\{0\}$ با نام ارزیابی اقلیدسی وجود داشته باشد بطوریکه دو شرط زیر را داشته باشد:

۱) برای هر $a,b \in R$ با $b\neq 0$، اعضای $q, r \in R$ وجود داشته باشند بطوریکه $a=bq+r$ و یا $r=0$ یا $\varphi(r) < \varphi(b)$.

۲) برای هر دو عضو ناصفر a و b از R $\varphi(a) \leq \varphi(ab)$.

مثال ۱: هر یک حلقه اقلیدسی (حوزه اقلیدسی) است زیرا $\varphi: \mathbb{Z}-\{0\} \to \mathbb{N}\cup\{0\}$ با ضابطه $\varphi(n)=|n|$ وجود دارد که شرط ۱ و ۲ برای آن برقرار است. شرط (۱) همان الگوریتم تقسیم روی $\mathbb{Z}$ است زیرا

$\forall a,b \in \mathbb{Z}, b\neq 0 \quad \exists r,q \in \mathbb{Z} \quad a=bq+r, \ r=0$ یا $|r|<|b|$ $(\varphi(r)<\varphi(b))$

شرط (۲) $\forall a,b \in \mathbb{Z}-\{0\} \quad \varphi(a)=|a| \leq |ab| = |a||b| = \varphi(ab)$

توجه: در این مثال بدیهی است که $|ab| = \varphi(ab) = \varphi(a)\varphi(b) = |a||b|$

مثال ۲: اگر F یک میدان باشد آنگاه $F[x]$ یک حوزه اقلیدسی است زیرا $\varphi: F[x]-\{0\} \to \mathbb{N}\cup\{0\}$

$\varphi(f(x)) = \deg f(x) \quad \forall f(x) \in (F[x]-\{0\})$

همانند مثال ۱ شرط (۱) الگوریتم تقسیم در $F[x]$ است و

$\forall f(x), g(x) \in (F[x]-\{0\}) \quad \exists q(x), r(x) \in F[x]$

$f(x) = q(x)g(x) + r(x), r(x)=0$ یا $\varphi(r(x)) = \deg r(x) < \deg g(x) = \varphi(g(x))$

توجه: در این مثال $\deg(f(x)g(x)) = \varphi(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) \Rightarrow$

$\varphi(f(x)g(x)) = \varphi(f(x)) + \varphi(g(x))$

مثال ۳: حوزه صحیح $\mathbb{Z}[i] = \{m+in \mid m,n \in \mathbb{Z}, i=\sqrt{-1}\}$ یک حوزه اقلیدسی است.

زیرا $\varphi: \mathbb{Z}[i]-\{0\} \to \mathbb{N}\cup\{0\}$ با ضابطه

$\varphi(m+in) = m^2+n^2$

$\forall m+in \in (\mathbb{Z}[i]-\{0\})$

تعریف می‌شود هر دو شرط ۱ و ۲ را داراست.

شرط (۱): $\forall \alpha = m_1+in_1, \beta = m_2+in_2 \in (\mathbb{Z}[i]-\{0\}) \quad \exists r,q \in \mathbb{Z}[i]:$

$\alpha = \beta q + r, \ r=0$ یا $\varphi(r) < \varphi(\beta)$

اگر عبارت $\frac{\alpha}{\beta} = \frac{m_1+in_1}{m_2+in_2}$ را گویا کنیم q, r بدست می‌آیند.

$$\frac{\alpha}{\beta} = \frac{m_1+in_1}{m_2+in_2} \times \frac{m_2-in_2}{m_2-in_2} = \frac{(m_1m_2+m_1n_2)+i(n_1m_2-m_1n_2)}{m_2^2+n_2^2} =$$

ادامه صفحه بعد

$$\frac{m_1m_2+n_1n_2}{m_2^2+n_2^2}+i\,\frac{n_1m_2-m_1n_2}{m_2^2+n_2^2}=(q_1+iq_2)+\frac{r_1+ir_2}{m_2^2+n_2^2}\qquad (*)$$

چون $m_1m_2+n_1n_2$ و $m_2^2+n_2^2$ نسبت به هم اول است پس طبق الگوریتم تقسیم در $\mathbb{Z}$ داریم:

$$\frac{m_1m_2+n_1n_2}{m_2^2+n_2^2}=q_1+\frac{r_1}{m_2^2+n_2^2}\Rightarrow m_1m_2+n_1n_2=q_1(m_2^2+n_2^2)+r_1 \quad \text{و} \quad r_1=0 \text{ یا } |r_1|^2<m_2^2+n_2^2$$

و همین صورت

$$\frac{n_1m_2-m_1n_2}{m_2^2+n_2^2}=q_2+\frac{r_2}{m_2^2+n_2^2}\Rightarrow n_1m_2-m_1n_2=q_2(m_2^2+n_2^2)+r_2 \quad \text{و} \quad r_2=0 \text{ یا } |r_2|^2<m_2^2+n_2^2$$

که در آن q_1, r_1, q_2, r_2

طبق * داریم $\alpha=(q_1+iq_2)\beta+(r_1+ir_2)$ و $r_1+ir_2=0$ یا $\nu(r)<\nu(\beta)$

یعنی $r_1^2+r_2^2<m_2^2+n_2^2$ پس شرط (۱) برقرار است.

شرط (۲):

$\forall \alpha=m_1+in_1,\ \beta=m_2+in_2\in(\mathbb{Z}[i]-\{0\})$

چون $\nu(\alpha)=\nu(\beta)$ آنگاه $\nu(\alpha\beta)=(m_1^2+n_1^2)(m_2^2+n_2^2)=\nu(\alpha)\nu(\beta)$

پس بنابراین داریم $\nu(\alpha\beta)>\nu(\alpha)$ آنگاه $(m_1^2+n_1^2)<(m_1^2+n_1^2)(m_2^2+n_2^2)$

تعریف: حلقه $\mathbb{Z}[i]$ را حلقه گوسی (حلقه "گاوسی") می نامیم. بنابراین طبق مثال ۳۵ حلقه گوسی یک حوزه اقلیدسی است.

قضیه ۱: هر حوزه اقلیدسی یک P.I.D است.

اثبات: فرض کنید که D یک حوزه اقلیدسی باشد و ν یک ارزیاب اقلیدسی روی D باشد و I ایده آلی در D باشد اگر $I=\{0\}$ که مسئله حل است زیرا $I=\langle 0\rangle$، پس فرض کنید که $I\neq\{0\}$ در این صورت $\exists b\in I$ ، این عضو b از I را طوری انتخاب می کنیم که $\nu(b)$ در بین تمام مقادیر $\nu(a)$: $\forall a\in I$ می نیمال باشد. (وجود می کنیم $I=\langle b\rangle$

طبق شرط (۱) ارزیاب اقلیدسی ν وجود دارد r و q از D طوری که $a=bq+r$ که $r=0$ یا $\nu(r)<\nu(b)$.

اکنون چون I ایده آل است پس $r=a-bq\in I$ و با انتخاب b (روش انتخاب b) نامساوی $\nu(r)<\nu(b)$ غیرممکن است پس $r=0$ یعنی $a=bq$ بنابراین $I=\langle b\rangle$.

نتیجه: هر حوزه اقلیدسی یک U.F.D است. زیرا طبق قضیه قبل هر حوزه اقلیدسی یک P.I.D است و هر P.I.D یک U.F.D است پس با عدی هر حوزه اقلیدسی یک U.F.D است.

توجه: هر P.I.D لزوماً یک حوزه اقلیدسی نیست (تمرین ۱)

قضیه ۲: هر حوزه اقلیدسی D با ارزیاب اقلیدسی ν همواره $\nu(1)$ در بین تمام مقادیر $\nu(a)$ برای

هر عضو ناصفر D می‌یکال است. بیان: $u \in D^\times$ یکال است $\iff \nu(u) = \nu(1)$

اثبات: طبق شرط (۲) از ارزیاب اقلیدسی بیان هر $a \in D$، $a \neq 0$ $\nu(a) = \nu(1a) \geq \nu(1)$ یعنی $\nu(1)$ می‌یکال است.

اگر u یکال باشد آنگاه $\nu(1) = \nu(uu^{-1}) \geq \nu(u)$ پس با ازای هر یکال در D $\nu(u) = \nu(1)$.

برعکس: فرض کنید عضو ناصفر $u \in D$ چنان باشد که $\nu(u) = \nu(1)$ بنابراین طبق الگوریتم تقسیم، اعضای $r, q \in D$ وجود دارند به طوری که $1 = uq + r$ به طوری که $r = 0$ یا $\nu(r) < \nu(u)$. اما چون $\nu(u) = \nu(1)$ در بین تمام مقادیر $\nu(d)$ به ازای هر $d \in D^\times$ می‌یکال است نامساوی $\nu(r) < \nu(u)$ غیرممکن است، پس $r = 0$ و $uq = 1$. از این رو u یکال است. $\#$

مثال ۱: در مثال (۱) یعنی $\mathbb{Z}$ با $\nu(n) = |n|$ چون یکال‌های $\mathbb{Z}$ عبارتند از 1 و -1 پس $\nu(1) = \nu(-1) = 1$.

و در مثال ۲ یعنی $F[x]$ با $\nu(f(x)) = \deg f(x)$، یکال‌های $F[x]$ عبارتند از اعضای ناصفر F یعنی تمام چندجمله‌ای‌های ثابت و ناصفر از $F[x]$ که $\nu(c) = 1$؛ $c \neq 0, c \in F$ (توجه باید F میدان باشد)

تعریف: فرض کنید که D یک حوزه تجزیه یکتا (U.F.D) باشد. عضو $d \in D$ را یک بزرگترین مقسوم علیه مشترک (ب.م.م) از اعضای a و b از D (ناصفر مثلاً ۱) $d \mid a$ و $d \mid b$ و ۲) بیان هر عضو c از D اگر c هر دو عضو a و b را عاد کند آنگاه $c \mid d$

مثال ۵: بدیهی است که ب.م.م دو عدد ۱۲ و ۱۸ عدد ۶ است و معمولاً می‌نویسیم $6 = (12, 18)$ و همچنین $-6 = (12, 18)$ یعنی -6 ب.م.م دیگری از این دو عدد است.

در $\mathbb{Q}[x]$ $1 = x - 1 = (x^2 - 2x + 1, x^2 + x - 2)$ همچنین $2(x-1) = (x^2 - 2x + 1, 2x^2 + 2x - 4)$ و نیز $-(x-1) = (x^2 + x - 2, x^2 - 2x + 1)$ یکی از $\mathbb{Q}[x]^\times$ است، اما در $\mathbb{Z}[x]$ داریم $x - 1 = (x^2 - 2x + 1, 2x^2 + 2x - 4)$ و $-(x-1) = (x^2 + x - 2, x^2 - 2x + 1)$

در $\mathbb{Q}[x]$ $\forall a \in \mathbb{Q} - \{0\}$: $a(x-1) = (x^2 - 2x + 1, ax^2 + ax - 2a)$

قضیه ۳: اگر D یک P.I.D باشد و a و b اعضای ناصفری از D باشند آنگاه یک ب.م.م از a و b وجود دارد.

بیان: هر ب.م.م از a و b را می‌توان به صورت $\lambda a + \mu b$ نوشت که در آن $\exists \lambda, \mu \in D$:

اثبات: مجموعه $N = \{r_1 a + s_1 b \mid r_1, s_1 \in D\}$ را در نظر می‌گیریم. چون $\forall r_1 a + s_1 b, r_2 a + s_2 b \in N$

$(r_1 a + s_1 b) - (r_2 a + s_2 b) = (r_1 - r_2) a + (s_1 - s_2) b \in N$ و $0 = 0a + 0b \in N$

پس N زیرحلقه D است زیرا $(r_1 a + s_1 b)(r_2 a + s_2 b) = (r_1 r_2 a^2 + r_1 s_2 ab + s_1 r_2 ba + s_1 s_2 b^2) =$

$= (r_1 r_2 a) a + (r_1 s_2 a + r_2 s_1 a + s_1 s_2 b) b \in N$. $r_1 r_2 a \in D$, $r_1 s_2 a + r_2 s_1 a + s_1 s_2 b \in D$

$r(r_1 a + s_1 b) = (r r_1) a + (r s_1) b \in N$ و $\forall r \in D$ و $\forall r_1 a + s_1 b \in N$ چون

پس N یک ایدئال D است.

اکنون به ازای یک $d\in D$ داریم $\langle d\rangle = N$ چون D یک P.I.D است، پس به ازای هر $r,s\in D$: $d|(ra+sb)$
با انتخاب $s=0$ و $r=1$ و $r=0$ و $s=1$ می‌بینیم که $d|a$ و $d|b$. حال اگر $c|a$ و $c|b$ آنگاه به ازای هر $ra+sb$ داریم $c|(ra+sb)$ یعنی $\forall n\in N:\ c|n$ بنابراین $c|d$ پس d یک ب.م.م a و b است پس
اگر d_1 یک ب.م.م a و b باشد آنگاه $d|d_1$ و $d_1|d$ پس $d_1=kd=(k\lambda)a+(k\mu)b=\lambda_1 a+\mu_1 b$

قضیه ۱۴: (الگوریتم اقلیدسی) فرض کنید که D حوزه اقلیدسی باشد و φ یک ارزیاب اقلیدسی روی D باشد. فرض کنید a و b اعضای ناصفری از D باشند. فرض کنید که r_1 چنان باشد که در شرط (۱) ارزیاب اقلیدسی φ صدق می‌کند یعنی $a=bq_1+r_1$ که در آن $r_1=0$ و $\varphi(r_1)<\varphi(b)$. اگر $r_1\neq 0$ فرض کنید که r_2 چنان باشد که $b=r_1q_2+r_2$ که $r_2=0$ یا $\varphi(r_2)<\varphi(r_1)$. به طور کلی فرض کنید که r_{i+1} چنان باشد که $r_{i-1}=r_iq_{i+1}+r_{i+1}$ که $r_{i+1}=0$ یا $\varphi(r_{i+1})<\varphi(r_i)$. در این صورت دنباله $r_1, r_2, \ldots$ باید در جایی با $r_s=0$ خاتمه یابد. اگر $r_1=0$ آنگاه b یک ب.م.م a و b است. اگر $r_1\neq 0$ و r_s اولین r_i مساوی صفر باشد آنگاه r_{s-1} یک ب.م.م a و b است.

اثبات: چون $\varphi(r_i)<\varphi(r_{i-1})$ و $\varphi(r_i)$ عدد صحیح نامنفی است، واضح است که باید بعد از تعداد متناهی مرحله به یک $r_s=0$ برسیم. اگر $r_1=0$ آنگاه $a=bq_1$ و بنابراین b یک ب.م.م از a و b است. فرض کنید که $r_1\neq 0$. در این صورت اگر $d|a$ و $d|b$ آنگاه $d|(a-bq_1)$، از این رو $d|r_1$. اگر $d_1|r_1$ و $d_1|b$ آنگاه $d_1|(bq_1+r_1)$ پس $d_1|a$. پس مجموعه مقسوم علیه‌های مشترک a و b همان مجموعه مقسوم علیه‌های مشترک b و r_1 است. با استدلال مشابه اگر $r_2\neq 0$ مجموعه مقسوم علیه‌های مشترک b و r_1 همان مجموعه مقسوم علیه‌های مشترک r_1 و r_2 است. با ادامه این روند سرانجام می‌بینیم که مجموعه مقسوم علیه‌های مشترک a و b همان مجموعه مقسوم علیه‌های مشترک r_{s-2} و r_{s-1} است که در آن r_s اولین r_i مساوی صفر است. پس هر ب.م.م r_{s-2} و r_{s-1} یک ب.م.م از a و b هم هست. اما تساوی $r_{s-2}=q_sr_{s-1}+r_s=q_sr_{s-1}$ نشان می‌دهد که r_{s-1} یک ب.م.م r_{s-2} و r_{s-1} است.

توجه: الگوریتم اقلیدسی در قضیه قبل همان روش یافتن ب.م.م دو عدد از راه تقسیم است.

مثال ۶: ب.م.م دو عدد ۳۰ و ۱۸ در $\mathbb{Z}$ با ارزیاب $\varphi(n)=|n|$ را بیابید.

حل:

۳۰ ÷ ۱۸: خارج قسمت ۱، باقیمانده ۱۲ ، ۱۸ ÷ ۱۲: خارج قسمت ۱، باقیمانده ۶ ، ۱۲ ÷ ۶: خارج قسمت ۲، باقیمانده ۰

$۳۰=۱\times ۱۸+۱۲$

$۱۸=۱\times ۱۲+۶$

$۱۲=۲\times ۶+۰$

پس ۶ یک ب.م.م ۱۸ و ۳۰ است همچنین ۶- هم یک ب.م.م دو عدد ۱۸ و ۳۰ است

تمرین

۱- با یک مثال نشان دهید که هر P.I.D یک حوزه اقلیدسی نیست. ($R = \{a + \frac{1}{2}b(1+i\sqrt{19}) \mid a,b \in \mathbb{Z}\}$ حقیقتاً بررسی شود.)

۲- نشان دهید که الف) تابع $\varphi(n) = n^2$ روی $\mathbb{Z}$ یک ارزیاب اقلیدسی است. $\varphi: \mathbb{Z}-\{0\} \to \mathbb{N}\cup\{0\}$

ب) تابع φ با ضابطه $\varphi(a) = 50$ روی $\mathbb{Q}$ یک ارزیاب اقلیدسی است. $\varphi: \mathbb{Q}-\{0\} \to \mathbb{N}\cup\{0\}$

۳- الف) آیا $\mathbb{Z}[x]$ یک U.F.D است (چرا؟)

ب) نشان دهید $I = \{a + f(x) \mid a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ ایده‌آلی از $\mathbb{Z}[x]$ است.

ج) آیا $\mathbb{Z}[x]$ یک P.I.D است (قسمت ب را بررسی کنید)

د) آیا $\mathbb{Z}[x]$ یک حوزه اقلیدسی است؟

۴- فرض کنید که D یک حوزه اقلیدسی با بزرگ و φ یک ارزیاب اقلیدسی بر D باشد. نشان دهید که اگر a و b در D شریک باشند آنگاه $\varphi(a) = \varphi(b)$

۵- نشان دهید که هر میدان یک حوزه اقلیدسی است. (تابع $\varphi: F-\{0\} \to \mathbb{N}\cup\{0\}$ با ضابطه $\varphi(a) = 1$ بررسی کنید)

۶- نشان دهید $\mathbb{Z}[\sqrt{-5}] = \{a+ib\sqrt{5} \mid a,b \in \mathbb{Z}\}$ یک حوزه صحیح است ولی یک U.F.D نیست. (راهنمایی $(1-2i\sqrt{5})(1+2i\sqrt{5}) = 3\times 7 = 21$.)

۷- فرض کنید که D حوزه صحیح باشد یک نرم (نورم) مرئی φ در D عبارت است تابع $\varphi: D \to \mathbb{Z}$ بطوریکه

۱) $\forall a \in D \quad \varphi(a) \geq 0$ ۲) $a = 0 \iff \varphi(a) = 0$

۳) $\forall a,b \in D \quad \varphi(ab) = \varphi(a)\cdot\varphi(b)$

الف) نشان دهید که تابع $\varphi: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ با ضابطه $\varphi(a+ib\sqrt{5}) = a^2+5b^2$ یک نرم مرئی روی $\mathbb{Z}[\sqrt{-5}]$ است.

ب) اگر F یک میدان باشد آیا تابع $\varphi: F[x] \to \mathbb{Z}$ با ضابطه $\varphi(f(x)) = \deg f(x)$ $\forall f(x) \in (F[x]-\{0\})$ یک نرم مرئی است؟

ج) اگر F یک میدان باشد آیا تابع $\varphi: F[x] \to \mathbb{Z}$ با ضابطه $\varphi(f(x)) = \begin{cases} 2^{\deg f(x)} & f(x) \neq 0 \\ 0 & f(x) = 0 \end{cases}$ یک نرم مرئی است؟

۸- فرض کنید R یک حوزه اقلیدسی باشد و فرض کنید $\varphi(0) = 0$ و اگر $a \in F \Rightarrow a+b \in F$ $\forall a,b \in F$ ثابت کنید که $F = \{a \in R \mid \varphi(a) \leq 1\}$ یک میدان است.