حلقه و میدان[1]

● حمید رضا امیری

در برهان ۱ از سال اول مقاله‌ای تحت عنوان «گروه، پیدایش و کاربرد نظریه گروههاء به چاپ رسید. در آنجا از یک دستگاه ریاضی[2] به‌نام گروه صحبت به میان آمد، این دستگاه ریاضی که در مقدمهٔ آن مقاله راجع به کاربردهای عملی و غیرریاضی آن نیز اشاره‌هایی شده است، از یک مجموعه مانند G و یک عمل دوتایی مانند $*$، روی G تشکیل می‌شد، در این مقاله راجع به دستگاههای ریاضی دیگری که هرکدام از یک مجموعه امّا با دو عمل تشکیل شده‌اند صحبت به میان خواهد آمد (در اینجا لازم به تذکر است عزیزان دانش‌آموز و خوانندگان محترمی که قصد مطالعهٔ این مقاله را دارند می‌بایست اطلاعات کافی در مورد گروه و خواص آن داشته‌باشند زیرا همانطور که خواهید دید اساس و مبنای نظریهٔ حلقه‌ها بر گروه استوار است).

فرض کنیم R مجموعه‌ای ناتهی و دو عمل روی این مجموعه تعریف شده باشد. عمل اول را $*$ و عمل دوّم را o می‌نامیم. (تقدم و تأخر این دو عمل مهّم است.) هرگاه مجموعهٔ R همراه با این دو عمل دارای خواص زیر باشد در این صورت آن را یک حلقه نامیده و می‌نویسیم $(R, *, o)$ یک حلقه است.

۱) R توأم با عمل اول $(*)$ یک گروه آبلی باشد ($(R, *)$ گروه آبلی باشد).

۲) R نسبت به عمل دوم (o) بسته باشد.

۳) عمل دوم (o) در R شرکت‌پذیر باشد.

۴) عمل دوم یعنی (o) نسبت به عمل اول یعنی $(*)$ از چپ و راست توزیع‌پذیر باشد یا به‌عبارت دیگر:

$$\forall a, b, c \in R, \quad ao(b * c) = (aob) * (aoc)$$
$$(b * c)oa = (boa) * (coa)$$

قرار داد: از این به‌بعد برای راحتی کار عمل اول در یک حلقه را با نماد $+$ و عمل دوم را با نماد $\times$ نمایش می‌دهیم که این نمادها لزوماً جمع و ضرب معمولی نمی‌باشند.

مثال ۱) مجموعهٔ اعداد حقیقی یعنی IR را با دو عمل جمع و ضرب معمولی درنظر می‌گیریم، در این صورت:

۱) $(IR, +)$ یک گروه جابجایی است.

۲) IR نسبت به ضرب بسته است.

۳) عمل ضرب در IR شرکت‌پذیر است. (اصل موضوعهٔ دستگاه اعداد حقیقی)

۴) عمل ضرب از چپ و راست در عمل جمع توزیع‌پذیر است.

بنابراین $(IR, +, \circ)$ یک حلقه است.

نکته: توجه داریم، هرگاه خاصیتی با یک سور عمومی برای اعضای یک مجموعه برقرار باشد (مانند شرکت‌پذیری، توزیع‌پذیری یا جابجایی)، این خاصیت برای تمام زیر مجموعه‌های آن مجموعه نیز برقرار خواهد بود.

باتوجه به نکتهٔ گفته شده و مثال ۱ واضح است که $(Q, +, \circ)$ و $(Z, +, \circ)$ هرکدام یک حلقه می‌باشند که به‌ترتیب آنها را حلقهٔ اعداد گویا و حلقهٔ اعداد صحیح می‌نامیم.

---

1) Ring and feild

۲) منظور از یک دستگاه ریاضی مجموعه‌ای است همراه با یک یا چند عمل که تعاریف، قضایا و ویژگیهای مخصوص به خود را دارا می‌باشد.

هرگاه مجموعهٔ ماتریسهای مربعی از مرتبهٔ n ($n \times n$) را $M_{n \times n}$ بنامیم در این صورت $M_{n \times n}$ همراه با دوعمل جمع و ضرب ماتریسی یک‌حلقه است یابه‌عبارت دیگر $(M_{n \times n}, +, \times)$ یک حلقه است.

مثال ۲) مجموعهٔ $IR^2 = IR \times IR$ را درنظر می‌گیریم و روی اعضای این مجموعه دو عمل جمع و ضرب را به شکل زیر تعریف می‌کنیم، ثابت کنید $(IR^2, +, \times)$ یک حلقه است.

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \times (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2)$$

الف) شرکت پذیری IR^2 نسبت به $+$ به‌راحتی قابل بررسی است.

ب) زوج مرتب $(0, 0)$ عضو خنثی می‌باشد.

ج) متقابل هرزوج مانند (a, b) به صورت $(-a, -b)$ می‌باشد.

د) جابجایی بودن IR^2 نسبت به $+$ نیز واضح است.

پس $(IR^2, +)$ یک گروه آبلی است.

ه) باتوجه به تعریف $\times$ مشاهده می‌شود که IR^2 نسبت به $\times$ بسته است. (حاصل ضرب دو زوج مرتب، یک زوج مرتب است.)

و) توزیع پذیری $\times$ نسبت به $+$ را بررسی می‌کنیم یعنی ثابت می‌کنیم:

$$(a_1, b_1) \times [(a_2, b_2) + (a_3, b_3)] = (a_1, b_1) \times (a_3, b_3) + (a_1, b_1) \times (a_2, b_2)$$

$$\text{سمت چپ} = (a_1, b_1) \times (a_2 + a_3, b_2 + b_3)$$
$$= (a_1 (a_2 + a_3) - b_1 (b_2 + b_3) \text{ و } a_1 (b_2 + b_3) + b_1 (a_2 + a_3))$$
$$= (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3, a_1b_2 + a_1b_3 + b_1a_2 + b_1a_3)$$

$$\text{سمت راست} = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2) + (a_1a_3 - b_1b_3 \text{ و } a_1b_3 + b_1a_3)$$

و

$$= (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3, a_1b_2 + a_1b_3 + b_1a_2 + b_1a_3)$$

که دو طرف باهم برابر بوده و تساوی برقرار است.

ز) آخرین خاصیت (باتوجه به تعریف حلقه) که به اثبات آن می‌پردازیم خاصیت شرکت‌پذیری IR^2 نسبت به $\times$ است یعنی باید ثابت کنیم:

$$(a_1, b_1) \times [(a_2, b_2) \times (a_3, b_3)]$$
$$= [(a_1, b_1) \times (a_2, b_2)] \times (a_3, b_3)$$

(اثبات به‌عهدهٔ خواننده)

بیان چند تعریف و معرفی حلقه‌هایی خاص

تعریف : حلقهٔ $(R, +, \times)$ را یک حلقهٔ جابجایی می‌نامیم هرگاه R نسبت به عمل دوم یعنی $\times$ خاصیت جابجایی داشته‌باشد.

مثال : حلقه‌های زیر همگی جابجایی هستند.

$(IR, +, \circ)$ و $(Q, +, \circ)$ و $(Z, +, \circ)$ و $(IR^2, +, \times)$

چون مجموعهٔ $M_{n \times n}$ نسبت به عمل ضرب ماتریسها خاصیت جابجایی ندارد لذا حلقهٔ $(M_{n \times n}, +, \times)$ ، حلقهٔ جابجایی نیست.

تعریف : حلقهٔ $(R, +, \times)$ را یک حلقهٔ یکدار[1] می‌نامیم هرگاه حلقهٔ R دارای عضو خنثی نسبت به عمل دوم یعنی $\times$ باشد.

مثال : حلقه‌های $(IR, +, \circ)$ ، $(Q, +, \circ)$ و $(Z, +, \circ)$ حلقه‌هایی جابجایی و یکدارند. حلقهٔ $(M_{n \times n}, +, \times)$ یک حلقهٔ

۱) در حلقهٔ $(R, +, \times)$ عضو خنثی نسبت به عمل $+$ را صفر حلقه و عضو خنثی نسبت به عمل $\times$ را یکِ حلقه می‌نامیم.

غیرجابجایی ولی یکدار است که یکِ حلقه همان ماتریس واحد یا I_n است.

در حلقهٔ $(IR^2, +, \times)$ زوج مرتب $(0, 1)$ عضو خنثی نسبت به $\times$ است زیرا:

$$(a, b) \times (1, 0) = (a \times 1 - b \times 0 \text{ و } a \times 0 + b \times 1)$$
$$= (a, b)$$

پس $(IR^2, +, \times)$ یک حلقهٔ جابجایی و یکدار است.

نکته : وقتی می‌گوییم متقابل ضربی یا وارون یک عضو دریک حلقه، منظور از این متقابل یا وارون نسبت به عمل دوم یعنی ضرب است و مثلاً اگر $(R, +, \times)$ یک حلقه باشد و در ضمن حلقه‌ای یکدار باشد و $a \in R$، منظور از وارون یا متقابل ضربیِ a، عضوی است چون $a^{-1} \in R$ به قسمی که :

$$a \times a^{-1} = a^{-1} \times a = 1$$

تعریف میدان : اگر $(R, +, \times)$ یک حلقهٔ جابجایی و یکدار باشد و نیز هر عضو مخالفِ صفر آن متقابل ضربی داشته باشد در این صورت این حلقه با چنین شرایطی، دستگاهی ریاضی به نام میدان تشکیل می‌دهد.

نتیجه : باتوجه به تعریف حلقه و تعریف میدان می‌توان میدان را به‌صورت زیر تعریف کرد: هرگاه F مجموعه‌ای ناتهی و دو عمل $*$ و o روی آن تعریف شده باشد در این صورت $(F, *, o)$ یک میدان است، وقتی که شرایط زیر برقرار باشند:

۱) $(F, *)$ گروه آبلی باشد.

۲) $(F - \{0\}, o)$ گروه آبلی باشد.

۳) عمل o از چپ و راست در عمل $*$ توزیع‌پذیر باشد.

مثال ۳) باتوجه به تعریف میدان و خواص دو عمل جمع و ضرب معمولی واضح است که، $(0, +, \times)$ و $(IR, +, \times)$ و $(Q, +, \times)$ هرکدام میدان‌می‌باشند. ازطرفی چون هرعضو در Z (به جز ۱ و ۱−) فاقد وارون یا متقابل ضربی در Z است لذا، $(Z, +, \times)$ میدان نمی‌باشد.

مثال ۴) باتوجه به‌اینکه اگر دترمینانِ یک ماتریس صفرباشد، آن ماتریس فاقد وارون خواهدبود، واضح‌است‌که $(M_{n \times n}, +, \times)$ درحالت کلّی ممکن است میدان نباشد.

مثال ۵) هرگاه مجموعهٔ باقیمانده‌های حاصل از تقسیم اعداد صحیح بر عدد صحیح m را Z_m بنامیم، خواهیم داشت :

$$Z_m = \{0, 1, 2, \ldots, m-1\}$$

حال روی این مجموعه دو عملِ $\oplus$ و $\otimes$ به صورت زیر تعریف می‌کنیم:

$\forall x, y \in Z_m$، $x \oplus y =$ باقیماندهٔ تقسیم $x + y$ بر m

$\forall x, y \in Z_m$، $x \otimes y =$ باقیمانده تقسیم xy بر m

به‌عنوان مثال دو مجموعهٔ $Z_5 = \{0, 1, 2, 3, 4\}$ و $Z_6 = \{0, 1, 2, 3, 4, 5\}$ را درنظر می‌گیریم و خواهیم داشت:

در Z_5 ←
- ۲ = باقیماندهٔ تقسیم ۴ + ۳ بر ۵ = ۳ ⊕ ۴
- ۲ = باقیماندهٔ تقسیم ۴ × ۳ بر ۵ = ۳ ⊗ ۴
- ۳ = باقیماندهٔ تقسیم ۱ × ۳ بر ۵ = ۳ ⊗ ۱
- ۳ = باقیماندهٔ تقسیم ۰ + ۳ بر ۵ = ۳ ⊕ ۰
- ۱ = باقیماندهٔ تقسیم ۳ × ۲ بر ۵ = ۲ ⊗ ۳

در Z_6 ←
- ۱ = باقیماندهٔ تقسیم ۴ + ۳ بر ۶ = ۳ ⊕ ۴
- ۰ = باقیماندهٔ تقسیم ۴ × ۳ بر ۶ = ۳ ⊗ ۴

با توجه به تعاریف دو عمل فوق روی Z_m به سادگی قابل بررسی است که $(Z_m, \oplus, \otimes)$ یک حلقه است که این حلقه جابجایی و یکدار است.

در حالت کلّی ممکن است $(Z_m, \oplus, \otimes)$ میدان نباشد، زیرا

ممکن است بعضی از اعضای Z_m فاقد متقابل نسبت به $\otimes$ باشند مثلاً در Z_6 عددِ ۲ فاقدِ متقابلِ ضربی است (نسبت به $\otimes$) زیرا:

$$۲ \otimes ۰ = ۰ \quad و \quad ۲ \otimes ۱ = ۲ \quad و \quad ۲ \otimes ۲ = ۴ \quad و \quad ۲ \otimes ۳ = ۰$$
$$۲ \otimes ۴ = ۲ \quad و \quad ۲ \otimes ۵ = ۴$$

یعنی ترکیب عدد ۲ با هیچ‌یک از اعضای Z_6 نسبت به عمل $\otimes$ مساوی با ۱ نمی‌باشد.

در اینجا به ذکر قضیه‌ای در این مورد می‌پردازیم.

قضیه: در حلقهٔ $(Z_m, \oplus, \otimes)$ هرگاه $a \in Z_m$ و a نسبت به m اول باشد (بزرگترین مقسوم علیه مشترک a و m، یک باشد) در این صورت a وارون پذیراست (a دارای متقابل ضربی است).

اثبات: (برای اثبات ناگزیریم از قضیه‌ای در هم‌نهشتی ها استفاده کنیم) چون $(a, m) = ۱$ پس معادلهٔ هم‌نهشتی $ax \overset{m}{\equiv} ۱$ همواره در Z_m دارای جواب است یعنی عددی صحیح در Z_m چون $x_۰$ یافت می‌شود به قسمی که $ax_۰ \overset{m}{\equiv} ۱$ (باقیماندهٔ تقسیم $ax_۰$ بر m مساوی با ۱ است). به عبارت دیگر $a \times x_۰ = ۱$ یعنی $x_۰$ متقابل a می‌باشد.

نکتهٔ ۱) می‌دانیم هرگاه P عددی اول باشد تمام اعداد صحیح و مثبت که کوچکتر از P باشند نسبت به P اولند حال اگر حلقهٔ $(Z_p, \oplus, \otimes)$ را درنظر بگیریم که P اول باشد، چون همهٔ اعضا در Z_p از P کوچکترند پس نسبت به P اولند و طبق قضیهٔ قبل همهٔ اعضای مخالف صفر در Z_p وارون پذیرند یعنی: $(Z_p, \oplus, \otimes)$ یک میدان است.

نکتهٔ ۲) باتوجه به قضیهٔ قبل هرگاه بخواهیم تعداد اعضای وارون‌پذیر در حلقهٔ Z_m را محاسبه کنیم، کافی است تعداد اعدادی در Z_m که نسبت به m اولند را بشماریم که در این رابطه به معرفی فرمول اولر که به تابع فی ـ اولر معروف است می‌پردازیم:

هرگاه m عددی صحیح، مثبت و مخالف یک باشد و آن را به‌صورت استاندارد به حاصل ضرب عاملهای اول تجزیه کنیم، یعنی داشته‌باشیم:

$$m = P_۱^{a_۱} P_۲^{a_۲} \dots P_k^{a_k}$$

که $P_۱$ ، $P_۲$ ، ... ، P_k اعداد اول هستند.

دراین صورت تعداد اعداد صحیح مثبت و کوچکتر از m که نسبت به m اولند برابر است با $\varphi(m)$ که از دستور زیر محاسبه می‌شود:

$$\varphi(m) = m\left(۱ - \frac{۱}{P_۱}\right)\left(۱ - \frac{۱}{P_۲}\right)\dots\left(۱ - \frac{۱}{P_k}\right)$$

به‌عنوان مثال تعداد وارون‌پذیرهای حلقهٔ $Z_{۱۸}$ برابر است با:

$$۱۸ = ۲ \times ۳^۲ \Rightarrow \varphi(۱۸) = ۱۸ \times \left(۱ - \frac{۱}{۲}\right)\left(۱ - \frac{۱}{۳}\right)$$
$$\Rightarrow \varphi(۱۸) = ۱۸ \times \frac{۱}{۲} \times \frac{۲}{۳} = ۶$$

یعنی در $Z_{۱۸}$، ۶ عضو وارون‌پذیر وجود دارد.

تبصره: هرگاه عدد صحیح a را بر عدد صحیح $b \neq ۰$ تقسیم کنیم اصطلاحاً b را مقسوم علیه a می‌نامند و اگر باقیمانده صفر باشد می‌نویسند $a = bq$ (در این حالت q نیز می‌تواند مقسوم علیه a باشد).

تعریف مقسوم‌علیه صفر: درحلقهٔ $(R, +, \times)$ عضو $a \neq ۰$ را یک مقسوم علیه صفر می‌نامند هرگاه عضوی چون $b \neq ۰$ در این حلقه یافت شود به قسمی که $a \times b = ۰$.

نکته ۱) باتوجه به تبصرهٔ قبل همانطور که حتماً پی برده‌اید اصطلاح مقسوم علیه صفر از همان اصطلاح جاری در اعداد صحیح ناشی شده زیرا دیدید که اگر حاصل ضرب دو عدد مساوی با عددی دیگر باشد هریک از آن دو عدد مقسوم علیه عددِ حاصل است در این تعریف نیز حاصل ضرب a و b مساوی با صفر شده و بنابراین هریک مقسوم علیه صفر هستند.

نکته ۲) باتوجه به اینکه اگر a و b دو عدد حقیقی باشند و $ab = 0$ در این صورت، $a = 0$ یا $b = 0$، واضح است که حلقهٔ اعداد حقیقی و کلیهٔ حلقه‌های عددی همراه با اعمال جمع و ضرب معمولی فاقد مقسوم علیه صفر می‌باشند.

مثال ۱) در حلقهٔ Z_6 دیدیم که $3 \otimes 4 = 0$ درصورتی که $3 \neq 0$ و $4 \neq 0$ پس ۳ و ۴ در Z_6 هریک مقسوم علیه صفر می‌باشند.

مثال ۲) در حلقهٔ ماتریسهای 2×2 داریم:

$$\underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}}_{B} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

یعنی دو ماتریس A و B هر دو مخالف با ماتریس صفرند ولی حاصلِ AB مساوی با ماتریس صفراست پس A و B هریک مقسوم علیه صفرند.

در این قسمت نیز به بیان و اثبات قضیه‌ای بسیار مهّم می‌پردازیم که به نوعی ارتباط بین مقسوم علیه‌های صفر یک حلقه و وارون‌پذیرهای آن حلقه را نشان می‌دهد.

قضیه: در حلقهٔ یکدار $(R, +, \times)$ هرگاه a عضوی از این حلقه بوده و وارون‌پذیر باشد مقسوم‌علیه صفر نیست. (عکس این قضیه در حالت کلّی برقرار نمی‌باشد.)

اثبات: فرض‌کنیم $(R, +, \times)$ یک حلقهٔ یکدار و $a \in R$ و a وارون‌پذیر باشد. ثابت می‌کنیم a مقسوم‌علیه صفر نیست. در جهت نیل به این مقصود، برای bای دلخواه در R فرض می‌کنیم $ab = 0$ و ثابت می‌کنیم $b = 0$.

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

همانطور که قید شد عکس قضیهٔ فوق درحالت کلّی برقرار نیست یعنی همواره نمی‌توان از اینکه عضوی دریک حلقه مقسوم علیه صفر نیست، نتیجه گرفت که وارون‌پذیر است. مثلاً در حلقهٔ اعداد صحیح همراه با جمع و ضرب معمولی عدد ۲ مقسوم علیه صفر نیست ولی وارون‌پذیر نیز نمی‌باشد $(\frac{1}{2} \notin Z)$.

نتیجه: عکس نقیض قضیهٔ فوق که با خود قضیه هم ارز است به‌صورت زیر بیان می‌شود:

در حلقهٔ یکدار $(R, +, \times)$، اگر a مقسوم علیه صفر باشد، وارون‌پذیر نیست.

تذکر: عکس قضیهٔ قبل در مورد دو حلقهٔ $M_{n \times n}$ و Z_m، صادق است یعنی مثلاً در حلقهٔ Z_m، a مقسوم‌علیه صفر است اگر و فقط اگر وارون‌پذیر نباشد.

بنابراین در حلقه Z_m، مقسوم‌علیه‌های صفر عبارتند از اعدادی که نسبت به m اول نیستند (چرا؟). یعنی باتوجه به تابع فی ـ اولر و اینکه عدد صفر نیز نمی‌تواند مقسوم علیه صفر باشد داریم:

$$\text{تعداد مقسوم علیه‌های صفر در } Z_m = m - \varphi(m) - 1$$

مثال: تعداد مقسوم‌علیه‌های صفر حلقهٔ Z_{18} را محاسبه می‌کنیم، که باتوجه به مطالب قبل خواهیم داشت:

$$\text{تعداد مقسوم علیه‌های صفر در } Z_{18} = 18 - \varphi(18) - 1 = 18 - 6 - 1 = 11$$

نتیجه: دیدیم که در Z_p (p اول است) همهٔ اعضایِ مخالف صفر نسبت به p اول و در نتیجه وارون‌پذیرند، لذا Z_p فاقد مقسوم علیه صفر است.

$$p \text{ اول است} \Rightarrow \varphi(p) = p(1 - \frac{1}{p}) = (p-1)$$ تعداد وارون‌پذیرهای Z_p

$$\text{تعداد مقسوم‌علیه‌های صفر در } Z_p = p - \varphi(p) - 1 = p - (p-1) - 1 = 0$$

تعریف حوزهٔ صحیح یا میدان درست:

هرگاه R یک حلقهٔ جابجایی و یکدار باشد، که فاقد مقسوم‌علیه صفر است، در این صورت R یک میدان درست نامیده می‌شود.

مثال ۱) حلقهٔ $(Z, +, \cdot)$ میدان درست است.

مثال ۲) » $(\mathbb{R}, +, \circ)$ » » » . »

مثال ۳) » $(\mathbb{Q}, +, \circ)$ » » » . »

مثال ۴) » $(Z_p, \oplus, \otimes)$ » » » . (P اول است)

مثال ۵) اگر m اول نباشد در حلقهٔ $(Z_m, \oplus, \otimes)$ مقسوم‌علیه صفر موجود است لذا Z_m میدان درست نیست.

مثال ۶) حلقهٔ ماتریسهای مربع $n \times n$ میدان درست نیست.

تذکر : در حلقهٔ $(M_{n\times n}, +, \times)$ هر ماتریس مانند A که $|A| = \circ$ وارون‌پذیر نیست لذا مقسوم علیه صفر است.

در این قسمت نیز به بیان و اثبات قضیه‌ای می‌پردازیم که بیانگر رابطهٔ بین برقراری قاعدهٔ حذف در یک حلقه و وجود مقسوم علیه صفر در آن حلقه است.

قضیه : شرط لازم و کافی برای آنکه در حلقهٔ R قاعدهٔ حذف برقرار باشد آن است که R فاقد مقسوم علیه صفر باشد.

اثبات : فرض کنیم در R قانون حذف برقرار باشد یعنی

$$\forall a, b, c \in R \ , \ ab = ac \Rightarrow b = c$$

ثابت می‌کنیم R فاقد مقسوم علیه صفر است. برای این کار فرض می‌کنیم $ab = \circ$ و ثابت می‌کنیم $a = \circ$ یا $b = \circ$. اگر $a \neq \circ$، در این صورت،

قانون حذف

$$ab = \circ \Rightarrow ab = a\circ \Longrightarrow b = \circ$$

عکس قضیه : فرض کنیم R فاقد مقسوم علیه صفر باشد ثابت می‌کنیم قانون حذف در R برقرار است برای این کار فرض می‌کنیم $a \neq \circ$ و $ab = ac$ ثابت می‌کنیم $b = c$.

$$ab = ac \Rightarrow ab - ac = \circ \Rightarrow a(b - c) = \circ$$
$$a \neq \circ$$
$$\Longrightarrow (b - c) = \circ \Rightarrow b = c$$

R فاقدمقسوم‌علیه صفر

نتیجه : باتوجه به تعریف میدان درست و قضیهٔ قبل داریم:

«شرط لازم و کافی برای آنکه حلقهٔ جابجایی و یکدار R میدان درست باشد آن است که قانون حذف در آن برقرار باشد.»

تذکر : استفاده از قضیهٔ قبل، در حلقه‌هایی که فاقد مقسوم علیه صفر می‌باشند منجر به استفاده از قانون حذف در این حلقه‌ها می‌باشد که در همنهشتی‌ها و حل معادلات همنهشتی در حلقه‌های Z_p به چشم می‌خورد، مثلاً در Z_{11} داریم:

$$7x \overset{11}{\equiv} 1 \Rightarrow 7x \overset{11}{\equiv} 1 + 11 \Rightarrow 7x \overset{11}{\equiv} 7 \times 2 \Rightarrow$$
$$x \overset{11}{\equiv} 2$$

نتیجه : ثابت می‌کنیم هر میدان مانند F، میدان درست است.

روش اول : بنابر نتیجهٔ قبل چون هر میدان یک حلقهٔ جابجایی و یکدار است، کافی است ثابت کنیم در F قانون حذف برقرار است و این باتوجه به وارون‌پذیربودنِ همهٔ اعضای غیرصفر در F آسان است.

$$ab = ac \Rightarrow a^{-1}ab = a^{-1}ac \Rightarrow 1b = 1c \Rightarrow b = c$$

روش دوم : در میدان F همهٔ اعضا وارون‌پذیرند لذا طبق قضیه هیچ کدام مقسوم‌علیه صفر نیستند یعنی F فاقد مقسوم علیه صفر است و طبق قضیه قانون حذف در آن برقرار است لذا F میدان درست است.

در این قسمت به تعریف و بررسی خواص و قضایای مربوط به زیر حلقه‌ها و ایده‌آلها می‌پردازیم:

تعریف زیر حلقه : هرگاه $(R, +, \times)$ یک حلقه و R' زیر مجموعه‌ای ناتهی از R باشد و با همان دو عمل تعریف شده روی R، تشکیل یک حلقه دهد، در این صورت حلقهٔ R' را زیر حلقهٔ، حلقهٔ R می‌نامیم.

تذکر ۱) همان طور که از تعریف زیر حلقه مشخص است، هر زیر حلقه به تنهایی یک حلقه است.

تذکر ۲) در بسیاری اوقات در حل مسائل مربوط به حلقه و میدان،

برای اثبات حلقه یا حتّی میدان بودنِ یک مجموعه، با توجه به قضیه‌ای که خواهیم‌گفت، ابتدا ثابت می‌کنیم آن مجموعه همراه با دو عمل تعریف شده روی آن، زیر حلقهٔ یک حلقهٔ شناخته شده است و بلافاصله نتیجه می‌گیریم که حلقه است.

قضیه : شرط لازم و کافی برای آنکه یک زیر مجموعهٔ ناتهی مانند R'، از حلقهٔ R زیر حلقهٔ آن باشد، آن است که:

الف) $\forall a, b \in R' \ , (a - b) \in R'$

ب) $\forall a, b \in R' \ , (ab) \in R'$

اثبات : شرط الف) زیر گروه[1] جمعی بودن R' نسبت به $(R, +)$ را می‌رساند و شرط ب) بسته بودن نسبت به عمل دوم یا ضرب را اثبات می‌کند و بقیهٔ شروط حلقه با توجه به زیر مجموعه بودنِ R'، از R به R' القاء می‌شود. اگر R' زیر حلقهٔ R باشد که طبق تعریف خودش حلقه است و نسبت به تفاضل و ضرب بسته خواهدبود.

$$\forall a, b \in R' \Rightarrow a, (-b) \in R' \Rightarrow a + (-b) \in R'$$

بنابراین برای اثبات زیر حلقه بودنِ یک مجموعه کافی است دو شرط الف) و ب) را برای آن بررسی کنیم و بلافاصله به قضیه استناد کرده و نتیجه بگیریم که زیر حلقه است.

مثال : نشان‌دهیدکه مجموعهٔ $R_1 = \{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in IR \}$ یک زیر حلقهٔ حلقهٔ ماتریسهای 2×2 است:

$$0 \in IR \Rightarrow \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R_1 \Rightarrow R_1 \neq \phi$$

و واضح است که $R_1 \subset M_{2\times 2}$. پس R_1 یک زیر مجموعهٔ ناتهی از $M_{2\times 2}$ است. حال به بررسی دو شرط زیر حلقه می‌پردازیم:

$$\begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} \overbrace{a_1 - a_2}^{a_3} & 0 - 0 \\ 0 - 0 & \underbrace{a_1 - a_2}_{a_3} \end{bmatrix} = \begin{bmatrix} a_3 & 0 \\ 0 & a_3 \end{bmatrix} \in R_1$$

$$\begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} \overbrace{a_1 a_2}^{a} & 0 \\ 0 & \underbrace{a_1 a_2}_{a} \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in R_1$$

مسأله ۱) ثابت کنید اشتراک دو زیر حلقه از حلقهٔ R، زیر حلقه‌ای از حلقهٔ R است.

فرض کنیم R_1 و R_2 هردو زیر حلقهٔ، حلقهٔ R باشند ثابت می‌کنیم $(R_1 \cap R_2)$ نیز زیرحلقهٔ R است.

$$0 \in R_1 \wedge 0 \in R_2 \Rightarrow 0 \in (R_1 \cap R_2) \Rightarrow (R_1 \cap R_2) \neq \phi$$
$$(R_1 \cap R_2) \subset R_1 \wedge R_1 \subset R \Rightarrow (R_1 \cap R_2) \subset R$$

پس $(R_1 \cap R_2)$ یک زیر مجموعهٔ ناتهیِ حلقهٔ R است. حال دو شرط زیر حلقه را بررسی می‌کنیم:

$$\forall x,y \in (R_1 \cap R_2) \Rightarrow \text{تعریف اشتراک} \Rightarrow \begin{cases} x,y \in R_1 \xrightarrow{\text{زیرحلقه } R_1} x - y \in R_1 \\ x,y \in R_2 \xrightarrow{\text{زیر حلقه } R_2} x - y \in R_2 \end{cases}$$

$$(x - y) \in (R_1 \cap R_2)$$

$$\forall x,y \in (R_1 \cap R_2) \Rightarrow \text{تعریف اشتراک} \Rightarrow \begin{cases} x,y \in R_1 \xrightarrow{\text{زیرحلقه } R_1} xy \in R_1 \\ x,y \in R_2 \xrightarrow{\text{زیر حلقه } R_2} xy \in R_2 \end{cases}$$

$$(x\,y) \in (R_1 \cap R_2)$$

۱) اگر $(*, G)$ یک گروه باشد و G' زیر مجموعهٔ ناتهی G، شرط لازم و کافی برای آنکه G' زیر گروه G باشد آن است که: $a * b' \in G'$، $\forall a, b \in G'$. (در این جا $*$ همان $+$ است پس b' به‌صورت $-b$ درآمده است.)

مسألهٔ ۲) نشان دهید مجموعهٔ $Q\sqrt{۳} = \{a + b\sqrt{۳} \mid a,b \in Q\}$ یک میدان است (همراه با دو عمل جمع و ضرب معمولی).

ابتدا ثابت می‌کنیم $Q\sqrt{۳}$ یک زیر حلقهٔ $(IR , + , ۰)$ است

الف) $(a_۱ + b_۱\sqrt{۳}) - (a_۲ + b_۲\sqrt{۳}) = (a_۱ - a_۲) + (b_۱ - b_۲)\sqrt{۳} = (a_۳ + b_۳\sqrt{۳}) \in Q\sqrt{۳}$

ب) $(a_۱ + b_۱\sqrt{۳})(a_۲ + b_۲\sqrt{۳}) = \underbrace{(a_۱a_۲ + ۳b_۱b_۲)}_{a} + \underbrace{(a_۱b_۲ + b_۱a_۲)}_{b}\sqrt{۳} = (a + b\sqrt{۳}) \in Q\sqrt{۳}$

پس $Q\sqrt{۳}$ یک زیر حلقهٔ حلقهٔ IR است لذا طبق تعریف زیر حلقه $Q\sqrt{۳}$ یک حلقه است و چون $۱ = ۱ + ۰\sqrt{۳} \in Q\sqrt{۳}$ پس یکدار است و جابجایی بودن را از IR به ارث می‌برد بنابراین یک حلقهٔ جابجایی و یکدار است، کافی است ثابت کنیم هر عضوِ مخالف صفر آن متقابل ضربی دارد.

$$(a + b\sqrt{۳}) \times ۱ = ۱ \Rightarrow ۱ = \frac{۱}{a + b\sqrt{۳}} = \frac{a - b\sqrt{۳}}{a^۲ - ۳b^۲}$$
$$= \frac{a}{a^۲ - ۳b^۲} + \frac{(-b)}{a^۲ - ۳b^۲}\sqrt{۳}$$
$$\Rightarrow ۱ \in Q\sqrt{۳}$$

تعریف ایده‌آل: هرگاه I زیر مجموعه‌ای ناتهی از حلقهٔ R باشد و شرایط زیر را نیز دارا باشد در این صورت I را یک ایده‌آل دو طرفه حلقهٔ R می‌نامند.

الف) $\forall a , b \in I ، (a - b) \in I$

ب) $\forall r \in R , \forall a \in I ، ra \in I , ar \in I$

(حاصل‌ضرب هرعضو حلقهٔ R در هر عضو I، چه از چپ و چه از راست عضوی از I باشد.)

نکته: همانطور که مشاهده می‌شود شرط اولِ ایده‌آلها با شرط اول زیر حلقه‌ها برابر می‌باشد و توسط شرط دوم ایده‌آلها می‌توان به شرط دوم زیر حلقه‌ها (بسته‌بودن نسبت به ضرب) دست یافت. بنابراین هر ایده‌آل یک حلقه، زیر حلقهٔ آن حلقه نیز هست ولی عکس این مطلب در حالت کلّی برقرار نیست. مثلاً $(Z , + , ۰)$ یک زیر حلقهٔ $(IR , + , ۰)$ است ولی ایده‌آل آن نیست زیرا:

$$\frac{۲}{۳} \in IR , ۱ \in Z \quad \text{ولی} \quad \frac{۲}{۳} \times ۱ = \frac{۲}{۳} \notin Z$$

مساله ۱) ثابت کنید اشتراکِ دو ایده‌آلِ حلقهٔ R، ایده‌آل حلقهٔ R است.

اثبات: فرض کنیم $I_۱$ و $I_۲$ هر دو ایده‌آلِ حلقهٔ R باشند برای اثبات ایده‌آل بودنِ $(I_۱ \cap I_۲)$ فقط به اثبات شرط ب) می‌پردازیم: (شرطِ الف) در اثبات زیر حلقه بودنِ اشتراک دو زیر حلقه قبلاً ثابت شده)

$$\forall r \in IR, \forall x \in (I_۱ \cap I_۲) \Rightarrow \left.\begin{array}{l} x \in I_۱ \xrightarrow{I_۱ \text{ ایده‌آل}} rx, xr \in I_۱ \\ x \in I_۲ \xrightarrow{I_۲ \text{ ایده‌آل}} rx, xr \in I_۲ \end{array}\right\} \xrightarrow{\text{تعریف اشتراک}} \Rightarrow$$

$$rx , xr \in (I_۱ \cap I_۲)$$

مسألهٔ ۲) ثابت کنید مجموعهٔ $mZ = \{mx \mid x \in Z\}$ یک ایده‌آل حلقهٔ Z است.

اثبات: فرض کنیم $mx_۱ , mx_۲ \in mZ$

$$mx_۱ - mx_۲ = m\overbrace{(x_۱ - x_۲)}^{x_۳} = mx_۳ \in mZ$$

$$\forall r \in Z , \forall mx \in mZ ، r(mx) = (rm)x = (mr)x = m\overbrace{(rx)}^{x_۱} = (mx_۱) \in mZ$$

$$(mx)r = m\overbrace{(xr)}^{x_۲} = (mx_۲) \in mZ$$

مسألهٔ ۳) ثابت کنید هرگاه I ایده‌آل حلقهٔ R باشد و $۱ \in I$ ، آنگاه $I = R$. (هر ایده‌آلِ یکدار از حلقهٔ R، با خود حلقهٔ R برابر است.)

اثبات: فرض کنیم I یک ایده‌ال حلقهٔ R باشد و $۱ \in I$. چون I ایده‌آلِ حلقهٔ R می‌باشد، لذا $I \subset R$ (۱).

حال ثابت می‌کنیم $R \subset I$،

$$\forall x \in R \Rightarrow x \in R \wedge \underset{\text{ایده‌آل } I}{۱ \in I} \Rightarrow ۱x \in I \Rightarrow x \in I \Rightarrow$$

$$R \subset I \ (۲) \overset{(۱) \text{ و } (۲)}{\Rightarrow} I = R$$

مسألهٔ ۴) هرگاه I و J هر دو ایده‌آل حلقهٔ R باشند و $(I \cap J) = \{ ۰ \}$، ثابت کنید: $\forall a \in I, \forall b \in J, ab = ۰$

اثبات:

$$\forall a \in I, \forall b \in J \overset{I \subset R}{\Rightarrow} a \in R, b \in \underset{\text{ایده‌آل } J}{J} \Rightarrow ab \in J \ (۱)$$

$$\forall a \in I, \forall b \in J \overset{J \subset R}{\Rightarrow} a \in \underset{\text{ایده‌آل } I}{I}, b \in R \Rightarrow ab \in I \ (۲)$$

$$\overset{(۱) \text{ و } (۲)}{\Rightarrow} ab \in (I \cap J) \Rightarrow ab \in \{ ۰ \} \Rightarrow ab = ۰$$

مسألهٔ ۵) ثابت کنید تنها ایده‌آلهای هر میدان مانند F عبارتند از F و $\{ ۰ \}$.

اثبات: فرض کنیم I ایده‌آل میدان F باشد و $I \neq \{ ۰ \}$، ثابت می‌کنیم $I = F$. برای اثبات اینکه $I = F$، طبق مسألهٔ ۳) کافی است ثابت کنیم، I یک ایده‌آل یکدار است یا $۱ \in I$.

$$I \neq \{ ۰ \} \Rightarrow \exists x \neq ۰ \in I \overset{I \subset F}{\Rightarrow} x \in \underset{\text{میدان است } F}{F} \Rightarrow x^{-۱} \in F$$

$$\Rightarrow x \in I \wedge x^{-۱} \in F \overset{\text{ایده‌آل } I}{\Rightarrow} xx^{-۱} \in I \Rightarrow ۱ \in I \Rightarrow I = F$$

طرح یک تست: هرگاه I یک ایده‌آل حلقهٔ $(\mathbb{Q}, +, ۰)$ (حلقهٔ اعداد گویا یا اعداد مُنْطِق) باشد، و $۹ \in I$ ، در این صورت I کدام است؟

۱) $I = Z$ ۲) $I = Q^{+}$ ۳) $I = Q$ ۴) $I = Z^{+}$

حل) گزینهٔ ۳) صحیح است زیرا:

Q میدان است و طبق مسألهٔ ۵) فقط می‌تواند دو ایده‌آل داشته باشد یکی $\{ ۰ \}$ و دیگری خودش یعنی Q، بنابراین $I = \{ ۰ \}$ یا $I = Q$ و چون $۹ \in I$ پس $I \neq \{ ۰ \}$ و لذا $I = Q$.

مسألهٔ ۶) ثابت کنید هرگاه H و K هر دو ایده‌آل حلقهٔ R باشند، در این صورت $H + K = \{(h + k) \mid h \in H, k \in K\}$ نیز یک ایده‌آل R است (جمع دو ایده‌آل، ایده‌آل است).

اثبات: $۰ \in H \wedge ۰ \in K \Rightarrow ۰ + ۰ \in H + K \Rightarrow ۰ \in H + K$

$$\Rightarrow (H + K) \neq \phi$$

$$\text{اگر } (h+k) \in (H+K) \begin{cases} h \in H \Rightarrow h \in R \\ k \in K \Rightarrow k \in R \end{cases} \Rightarrow (h + k) \in R$$

$$\Rightarrow (H + K) \subset R$$

بنابراین ثابت کردیم $(H + K)$ یک زیر مجموعهٔ ناتهی از حلقهٔ R است. حال کافی است دو شرط ایده‌آل را بررسی کنیم:

$$(h_۱ + k_۱), (h_۲ + k_۲) \in (H+K) \begin{cases} h_۱, h_۲ \in H \\ k_۱, k_۲ \in K \end{cases} \Rightarrow$$

$$\begin{cases} (h_۱ - h_۲) \in H \\ (k_۱ - k_۲) \in K \end{cases} \Rightarrow (h_۱ - h_۲) + (k_۱ - k_۲) \in H + K \ (۱)$$

$$(h_۱ + k_۱) - (h_۲ + k_۲) = (h_۱ + k_۱) + [-h_۲ + (-k_۲)]$$

$$= [(h_۱ + k_۱) - h_۲] - k_۲ = [h_۱ + (k_۱ - h_۲)] - k_۲$$

$$= [h_۱ + (-h_۲ + k_۱)] - k_۲ = [(h_۱ - h_۲) + k_۱] - k_۲$$

$$= (h_۱ - h_۲) + (k_۱ - k_۲) \in h + k \leftarrow \text{طبق } (۱)$$

فرض کنیم $r \in R, h+k \in H+K \Rightarrow$ $\begin{cases} h \in H \Rightarrow rh, hr \in H \\ k \in K \Rightarrow rk, kr \in K \end{cases} \Rightarrow$

$$(rh + rk) \in H + K$$

(۲)

$$(hr + kr) \in H + K$$

$$r(h + k) = rh + rk \in H + K$$

طبق (۲) ←

$$(h + k)r = hr + kr \in H + K$$

لذا $H + K$ یک ایده‌آل R است.

نکته ۱: ثابت می‌شود ایده‌آلهای حلقهٔ اعداد صحیح یعنی $(Z, +, \circ)$ فقط به صورت mZ هستند که:

$$mZ = \{mx \mid x \in Z\}$$

مانند $2Z$ و $3Z$ و ... (مضارب ۲ و مضارب ۳ و ...)

نکته ۲: برای هر دو عدد صحیح مثبت مانند a و b داریم:

$$aZ + bZ = dZ$$

که d بزرگترین مقسوم‌علیه مشترکِ اعداد a و b است. در حقیقت این نکته با این قضیه در تئوری اعداد هم ارز است:

«بزرگترین مقسوم‌علیه مشترک دو عدد بر هر مقسوم علیه مشترک آن دو عدد بخش‌پذیر است.»

واضح است که اگر a و b نسبت به هم اول باشند یعنی $d = 1$ در این صورت $aZ + bZ = Z$.

نکته ۳: به ازای هر دو عدد صحیح و مثبت مانند a و b داریم:

$$aZ \cap bZ = mZ$$

که m کوچکترین مضرب مشترک a و b است.

این نکته نیز با قضیهٔ زیر در تئوری اعداد هم ارز است.

«هر مضرب مشترک دو عدد بر کوچکترین مضرب مشترک آن دو عدد بخش‌پذیر است.»

به مثالهای زیر توجه کنید:

۱) $2Z + 3Z = Z$

۲) $2Z \cap 3Z = 6Z$

۳) $2Z \cap 4Z = 4Z$

۴) $2Z + 4Z = 2Z$

در خاتمهٔ این مقاله با امید به اینکه مطالب فوق تا حدودی مشکلات و مسائل مربوط به این قسمت از کتاب را برطرف کرده باشد متذکر می‌شوم که، نظریه حلقه‌ها و میدانها بسیار وسیع و پیشرفته‌تر از آن است که بتوان همه را در یک مقاله جمع‌آوری نمود و در این مقاله سعی شده در حد نیاز به آن پرداخته شود.

والسلام.