



دانشگاه شاهرود

مباحثی در نظریه حلقه و مدول

(رشته ریاضی)

دکتر خدیجه احمدی آملی دکتر منصوره معانی شیرازی

بسم الله الرحمن الرحيم

پیشگفتار ناشر

کتاب‌های دانشگاه پیام نور حسب مورد و با توجه به شرایط مختلف یک درس در یک یا چند رشته دانشگاهی، به صورت کتاب درسی، متن آزمایشگاهی، فرادرسی، و کمک درسی چاپ می‌شوند.

کتاب درسی ثمره کوشش‌های علمی صاحب اثر است که براساس نیازهای درسی دانشجویان و سرفصل‌های مصوب تهیه و پس از داوری علمی، طراحی آموزشی، و ویرایش علمی در گروه‌های علمی و آموزشی، به چاپ می‌رسد. پس از چاپ ویرایش اول اثر، با نظرخواهی‌ها و داوری علمی مجدد و با دریافت نظرهای اصلاحی و متناسب با پیشرفت علوم و فناوری، صاحب اثر در کتاب تجدیدنظر می‌کند و ویرایش جدید کتاب با اعمال ویرایش زبانی و صوری جدید چاپ می‌شود.

متن آزمایشگاهی (م) راهنمایی است که دانشجویان با استفاده از آن و کمک استاد، کارهای عملی و آزمایشگاهی را انجام می‌دهند.

کتاب‌های فرادرسی (ف) و **کمک درسی** (ک) به منظور غنی‌تر کردن منابع درسی دانشگاهی تهیه و بر روی لوح فشرده تکثیر می‌شوند و یا در وبگاه دانشگاه قرار می‌گیرند.

مدیریت تولید محتوا و تجهیزات آموزشی

فهرست

نه	پیشگفتار مؤلفین
۱	فصل اول: حلقه‌ها
۲	۱.۱ مقدمه
۲	۲.۱ مفهوم یک حلقه
۴	۳.۱ تعریف یک حلقه
۱۴	۴.۱ زیرحلقه‌ها
۱۷	۵.۱ حوزه‌های صحیح
۲۵	۶.۱ خودآزمایی
۲۷	۷.۱ پاسخ خودآزمایی
۳۱	۸.۱ تمرین
۳۷	فصل دوم: ایده‌آل‌ها و حلقه‌های خارج قسمتی
۳۸	۱.۲ مقدمه
۳۸	۲.۲ ایده‌آل‌ها
۵۱	۳.۲ حلقه‌های خارج قسمتی
۵۴	۴.۲ ایده‌آل‌های اول و ایده‌آل‌های ماکسیمال
۶۱	۵.۲ لم ژرن و ایده‌آل‌های ماکسیمال
۶۵	۶.۲ خودآزمایی
۶۶	۷.۲ پاسخ خودآزمایی
۶۹	۸.۲ تمرین
۷۳	فصل سوم: همریختی‌ها و قضایای یکرینتی حلقه‌ها
۷۴	۱.۳ مقدمه

۷۴	۲.۳ همریختی حلقه‌ها
۸۰	۳.۳ قضایای یکریختی حلقه‌ها
۸۹	۴.۳ حاصل جمع مستقیم حلقه‌ها
۹۷	۵.۳ خودآزمایی
۹۸	۶.۳ پاسخ خودآزمایی
۱۰۲	۷.۳ تمرین

۱۰۵	فصل چهارم: موضعی سازی حلقه‌ها
۱۰۶	۱.۴ مقدمه
۱۰۶	۲.۴ میدان کسرهای یک حوزه صحیح
۱۱۰	۳.۴ حلقه کسرهای کلی
۱۱۲	۴.۴ حلقه‌های کسر ها و موضعی سازی
۱۲۱	۵.۴ خودآزمایی
۱۲۲	۶.۴ پاسخ خودآزمایی
۱۲۶	۷.۴ تمرین

۱۲۹	فصل پنجم: تجزیه یکتا
۱۳۰	۱.۵ مقدمه
۱۳۰	۲.۵ حوزه‌های تجزیه یکتا
۱۳۹	۳.۵ حلقه‌های اقلیدسی
۱۴۲	۴.۵ خودآزمایی
۱۴۳	۵.۵ پاسخ خودآزمایی
۱۴۶	۶.۵ تمرین

۱۴۹	فصل ششم: مدول‌ها
۱۵۰	۱.۶ مقدمه
۱۵۰	۲.۶ مفهوم یک مدول
۱۵۴	۳.۶ زیرمدول‌ها
۱۶۱	۴.۶ مدول‌های خارج قسمتی
۱۶۲	۵.۶ خودآزمایی
۱۶۴	۶.۶ پاسخ خودآزمایی
۱۶۵	۷.۶ تمرین

۱۶۹	فصل هفتم: همریختی‌ها و قضایای یکریختی مدول‌ها
۱۶۹	۱.۷ مقدمه
۱۷۰	۲.۷ همریختی مدول‌ها
۱۷۵	۳.۷ قضایای یکریختی مدول‌ها
۱۸۱	۴.۷ خودآزمایی
۱۸۲	۵.۷ پاسخ خودآزمایی

۱۸۵	۶.۷ تمرین
۱۸۹	فصل هشتم: مدول‌های آزاد
۱۸۹	۱.۸ مقدمه
۱۹۰	۲.۸ حاصل جمع مستقیم مدول‌ها
۱۹۷	۳.۸ مدول‌های آزاد
۲۰۴	۴.۸ خودآزمایی
۲۰۴	۵.۸ پاسخ خودآزمایی
۲۰۶	۶.۸ تمرین
۲۱۱	فصل نهم: مدول‌های کسرها
۲۱۱	۱.۹ مقدمه
۲۱۲	۲.۹ مدول‌های کسرها
۲۱۷	۳.۹ زیرمدول‌های مدول‌های کسرها
۲۲۲	۴.۹ خودآزمایی
۲۲۳	۵.۹ پاسخ خودآزمایی
۲۲۶	۶.۹ تمرین
۲۲۹	فصل دهم: شرط‌های زنجیری
۲۲۹	۱.۱۰ مقدمه
۲۳۰	۲.۱۰ شرط‌های زنجیری
۲۳۴	۳.۱۰ مدول‌های نوتری و مدول‌های آرتینی
۲۴۰	۴.۱۰ خودآزمایی
۲۴۱	۵.۱۰ پاسخ خودآزمایی
۲۴۲	۶.۱۰ تمرین
۲۴۵	فهرست نمایه
۲۴۷	مراجع

پیشگفتار مؤلفین

کتاب حاضر در باب نظریه حلقه‌ها و مدول‌ها نگارش شده است. مؤلفین سعی بر آن داشته‌اند این کتاب را به صورت یک کتاب درسی و خودخوان برای دانشجویان مقطع کارشناسی به نحوی ارائه دهند که خواننده تنها با دانستن مبانی نظریه گروه‌ها بتواند مطالب کتاب را به راحتی دنبال نماید. البته کتب بسیاری (برای نمونه [Sh]، [AM] و [Ka]) در باب نظریه حلقه‌ها و مدول‌ها، در سطح پیشرفته‌تر نگارش شده است که خواننده را ترغیب به مطالعه آن‌ها در کنار این کتاب می‌کنیم. لیست کتب بیشتر، در انتهای کتاب در بخش مراجع آورده شده است.

ویژگی‌های این کتاب:

کتاب در دو قسمت نگارش شده است. قسمت اول شامل فصول یک تا پنج می‌شود و در خصوص نظریه حلقه‌ها است. در این قسمت مؤلفین سعی کرده‌اند مطالب را با نگرشی بنیادی و اصولی بیان دارند تا دانشجو با دریافت دیدی جبری بتواند قسمت دوم کتاب، فصول شش تا ده، را که مربوط به نظریه مدول‌ها است شخصاً و به طور ساختاری درک و دنبال نماید.

در پایان هر فصل مسائلی تحت عنوان خودآزمایی و متعاقباً پاسخ آن‌ها آورده شده است تا خواننده بتواند با حل آن‌ها از یادگیری خود اطمینان خاطر حاصل نماید. توصیه می‌گردد ابتدا خواننده برای حل مسائل خودآزمایی تا حد امکان تأمل کرده و وقت

صرف نماید و سپس پاسخ خود را با حل خودآزمایی بسنجد. در این صورت به پیشرفت‌ها و کاستی‌های خود در درک مفاهیم و کاربرد آنها پی خواهد برد. همچنین در انتهای هر فصل متناسب با موضوع و مباحث آن فصل تمرین‌هایی نیز داده شده است. در متن درس برای هر اصطلاح ریاضی که معرفی می‌گردد، هم‌زمان معادل لاتین آن به صورت زیر نویس درج شده است که این امر، موجب افزودن گنجینه لغات و اصطلاحات زبان تخصصی ریاضی دانشجویان می‌گردد. لذا انتظار می‌رود دانشجویان هم‌زمان با مطالعه این کتاب، کتب دیگری از جمله کتب معرفی شده در مراجع را نیز به عنوان مکمل این کتاب، مرور نمایند.

از آنجا که این کتاب تنها برای درس نظریه حلقه و مدول در سطح کارشناسی به ارزش سه واحد نگارش شده است، مجال معرفی و بیان مباحث گسترده‌تر در این کتاب مقدور نبوده و لذا فقط به ارائه رئوس مطالب بنیادی بسنده شده است.

مؤلفین از اساتید ارجمند و دانشجویان عزیز جهت ارائه نقطه نظرات تکمیلی استقبال می‌نمایند تا بتوانند در چاپ‌های بعدی به رفع نقایص و تکمیل مطالب اقدام نمایند.

دکتر خدیجه احمدی آملی

دکتر منصوره معانی شیرازی

بهار ۱۳۹۱

فصل اول

حلقه‌ها

هدف کلی

هدف کلی از ارائه این فصل معرفی مفهوم مجرد حلقه و زیرحلقه با در نظر گرفتن وجه تشابه بین مجموعه‌ی اعداد و مجموعه‌ی چندجمله‌ای‌ها می‌باشد.

اهداف آموزشی

دانشجو پس از مطالعه و فراگیری این فصل باید:

۱. انگیزه تجرید مفهوم حلقه را به کمک وجه تشابه بین اعداد و چندجمله‌ای‌ها درک نماید.
۲. بتواند تعریف یک حلقه را بیان نماید.
۳. بتواند تشخیص دهد که مجموعه‌ای با دو عمل داده شده یک حلقه است یا خیر، سپس ادعای خود را ثابت نماید.
۴. بتواند عناصر یکه برخی از حلقه‌ها را به دست آورد.
۵. بتواند مقسوم علیه صفر برخی از حلقه‌ها را به دست آورد.
۶. بتواند ثابت کند که مجموعه‌ای زیرحلقه‌ی حلقه‌ی داده شده است یا خیر.
۷. با مثال‌هایی از حوزه‌های صحیح آشنا باشد.
۸. ارتباط بین حوزه‌های صحیح و میدان‌ها را بداند.
۹. فرق بین یک حلقه تقسیمی و یک میدان را بداند.
۱۰. قادر به حل مسائل خودآزمایی و تمرینات آخر فصل باشد.

۱.۱ مقدمه

در این فصل ابتدا به کمک ویژگی‌های اعداد و چندجمله‌ای‌ها و شباهت بین آن‌ها به معرفی مفهوم حلقه و زیرحلقه می‌پردازیم. مثال‌های متنوعی بیان و برخی از خواص حلقه‌ها و زیرحلقه‌ها را اثبات می‌نماییم. سپس به کمک خواص آشنای اعداد صحیح حوزه‌های صحیح، حلقه‌های تقسیم و میدان‌ها را معرفی می‌نماییم.

۲.۱ مفهوم یک حلقه



دیوید هیلبرت (۱۸۶۲-۱۹۴۳)

تعریف مجرد حلقه ابتدا توسط فرانکل^۱ در سال ۱۹۱۴ به صورت فرموله درآمد $[K]$. هرچند که قبل از آن، مفهوم "حلقه" توسط هیلبرت^۲ معرفی شده بود.

در سال ۱۸۸۸- هنگامی که ۲۶ سال بیشتر نداشت- دیوید هیلبرت مسأله معروفی را در نظریه ناورداها حل کرد. این مسأله به نام "مسأله گردان"^۳ معروف بود زیرا گردان ۲۰ سال پیش‌تر از هیلبرت نشان داد که فرم‌های دوتایی دارای پایه‌ای متناهی هستند.

راه حل گردان طولانی و از نقطه نظر محاسباتی خیلی پیچیده بود به طوری که بعید به نظر می‌رسید بتوان آن را به فرم‌های سه‌تایی تعمیم داد. در این مختصر نمی‌خواهیم به جزئیات مسأله گردان و یا حتی به نظریه‌ی ناورداها بپردازیم، اما هیلبرت با راه حلی که ارائه کرد نشان داد که در واقع یک پایه متناهی برای تمام ناورداها، هرچقدر هم از درجه بالایی برخوردار باشند، وجود دارد.

ساختار اثبات هیلبرت بسیار ساده و با ارزش است. ابتدا او نشان داد که اگر یک حلقه R دارای خاصیتی مانند $\mathcal{P}$ باشد، آن‌گاه حلقه چندجمله‌ای‌ها برحسب یک متغیر

1. Frankel

2. David Hilbert

3. Gordan's Problem

x با ضرایب از حلقه R (که آن را با $R[x]$ نمایش می‌دهند) نیز دارای همان خاصیت $\mathcal{P}$ است. لذا اولین قدم هیلبرت را می‌توان به صورت زیر خلاصه کرد:

"اگر حلقه R دارای خاصیت $\mathcal{P}$ باشد آن گاه حلقه $R[x]$ نیز چنین خواهد بود."

سپس هیلبرت بر آن شد که نشان دهد حلقه چندجمله‌ای‌ها برحسب دو متغیر x و y با ضرایب از حلقه R (که آن را با نماد $R[x, y]$ نشان می‌دهند) نیز دارای خاصیت $\mathcal{P}$ است. اعضای $R[x, y]$ کاملاً شبیه چندجمله‌ای‌های معمولی، مانند $x^2 + 6$ و $3y^2 - 6y + 5$ ، بودند، که در آن دو متغیر x و y با هم در یک چندجمله‌ای می‌توانند ظاهر شوند. به عنوان مثال چندجمله‌ای

$$3x^2 + 4xy + 2y^2 + 7x - 5y + 12$$

که در آن ضرایب اعداد صحیح می‌باشند. هیلبرت متوجه شد که حلقه چندجمله‌ای‌های $R[x, y]$ برحسب دو متغیر x و y با ضرایب از R ، را می‌توان به صورت زیر نیز دسته‌بندی کرد:

$$3x^2 + 4xy + 2y^2 + 7x - 5y + 12 = 2y^2 + (4x - 5)y + (3x^2 + 7x + 12)$$

ملاحظه می‌گردد که چندجمله‌ای سمت چپ به عنوان یک چندجمله‌ای در حلقه $R[x, y]$ است؛ در حالی که سمت راست یک چندجمله‌ای برحسب یک متغیر y است که ضرایب آن خودشان چندجمله‌ای‌هایی برحسب x هستند. برای حلقه دوم که اشاره شد از نماد $(R[x])[y]$ ، یا ساده تر $R[x][y]$ ، استفاده می‌کنیم.

هیلبرت از این ایده بسیار ساده کمک گرفت و نتیجه گرفت که حلقه چندجمله‌ای‌های $R[x, y]$ نیز دارای خاصیت $\mathcal{P}$ است. استدلال او چنین بود: چون R خاصیت $\mathcal{P}$ را دارد، پس حلقه $R[x]$ نیز این خاصیت را دارد؛ اما دوباره چون حلقه $R[x]$ دارای این خاصیت است، حلقه $R[x][y]$ نیز چنین است؛ و همان‌طور که در بالا دیدیم حلقه‌ی همان حلقه $R[x, y]$ است.

بدین ترتیب هر بار با افزودن یک متغیر، هیلبرت نشان داد که حلقه چندجمله‌ای‌ها با هر تعداد متناهی متغیر دارای خاصیت $\mathcal{P}$ است. مثلاً می‌توانیم نشان دهیم که حلقه

$R[x, y, z]$ دارای خاصیت $\mathcal{P}$ است، زیرا این حلقه همان حلقه $R[x, y][z]$ است و قبلاً هم دیدیم که حلقه $R[x, y]$ دارای خاصیت $\mathcal{P}$ است.

گردان این مطلب را برای حالت دوتایی با ساختن یک پایه اثبات کرد در حالی که همان‌طور که دیدیم، هیلبرت در اثبات خود هیچ‌گونه پایه‌ای نساخت. او نشان داد که اگر هیچ پایه‌ی متناهی وجود نداشته باشد، آنگاه تناقضی ایجاد می‌شود از این رو باید پایه‌ای متناهی وجود داشته باشد. امروزه با نحوه‌ی چنین استدلالی تحت عنوان "برهان خلف" آشنا هستیم. در واقع هیلبرت این تکنیک را به روش جدیدی به‌کار برد: او وجود چیزی را بدون ساختن آن به اثبات رساند.

در عمق اثبات جنجال برانگیز هیلبرت، مفهوم مجرد یک حلقه نهفته است، اگر چه چندین سال بعد، هیلبرت اصطلاح حلقه (Zahlring) - به معنای واقعی کلمه، حلقه اعداد) را به نحوی که اکنون آن را به‌کار می‌بریم، عنوان کرد. او چنین فکر می‌کرد که اگر چه چندجمله‌ای‌ها ظاهراً با اعداد صحیح متفاوت به‌نظر می‌آیند، اما به انحایی می‌توان چندجمله‌ای‌ها و اعداد صحیح را شبیه هم در نظر گرفت: مثلاً، شما می‌توانید اعداد صحیح را با هم جمع و یا در هم ضرب کنید و نیز چندجمله‌ای‌ها را می‌توانید با هم جمع و یا در هم ضرب نمایید. آنچه اغلب ما به آن توجه داریم تفاوت بین اعداد صحیح و چندجمله‌ای‌ها است در حالی که هیلبرت به شباهت‌های آن‌ها پرداخت. بنابراین این وجه تشابه بین اعداد صحیح، اعداد گویا، اعداد حقیقی، اعداد مختلط، چندجمله‌ای‌ها با ضرایب مختلط و نیز توابع پیوسته (هر چند که از نظر ما بسیار متفاوت‌اند) در پشت تعریف یک حلقه نهفته است. این شباهت‌ها پایه و اساس اصول موضوعه تعریف‌مان از یک حلقه را تشکیل می‌دهند.

۳.۱ تعریف یک حلقه

قبل از اینکه واقعاً به تعریف یک حلقه بپردازیم، ابتدا مختصری در خصوص اینکه یک حلقه چیست، صحبت می‌کنیم. خیلی ساده می‌گوییم یک حلقه مجموعه‌ای از عناصر (مثلاً مجموعه‌ای از اعداد از نوعی خاص، یا مثلاً مجموعه‌ای متشکل از نوعی خاص از توابع) به همراه دو عمل روی عناصر آن به‌نام‌های جمع و ضرب می‌باشد. بسیار مهم

است که از یک حلقه به‌عنوان یک شیء متشکل از دو چیز، یک مجموعه زمینه و دو عمل، تصور شود نه فقط به‌عنوان یک مجموعه به خودی خود.

به‌علاوه این اعمال چنان رفتار کنند که ما انتظار داریم. مثلاً اگر a و b دو عنصر در یک حلقه باشند، انتظار داریم $a+b$ و $b+a$ مساوی بوده، یا مثلاً انتظار داریم $a+0$ با a برابر باشد، یا مثلاً می‌خواهیم $a(a+b)$ مساوی a^2+ab شود. این انتظارات را بدون در نظر گرفتن اینکه a و b عدد هستند یا خیر، چندجمله‌ای‌اند یا ماتریس، داریم.

ابتدا چند نمونه از حلقه به شرح زیر را ملاحظه کنید. در هر حالت، توجه شود که هم مجموعه و هم دو عمل روی آن مجموعه را برای توصیف حلقه ارائه می‌دهیم.

۱.۳.۱ مثال. مسلماً اساسی‌ترین مثال از یک حلقه، حلقه‌ای است که روی اعداد $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$ بنا نهاده شده است. این حلقه را حلقه اعداد صحیح^۱ یا ساده‌تر اعداد صحیح^۲ خواهیم نامید و با نماد $\mathbb{Z}$ نشان خواهیم داد. ممکن است انتخاب این حرف برای اعداد صحیح عجیب به‌نظر برسد، اما این حرف از *zahl*، کلمه آلمانی برای عدد، گرفته شده است. حلقه $\mathbb{Z}$ مجموعه‌ی اعداد صحیح به همراه اعمال دوتایی جمع و ضرب می‌باشد.

۲.۳.۱ مثال. طبیعی‌ترین حلقه بعد از مثال ۱.۳.۱، حلقه متشکل از کسرهای اعداد صحیح است، از قبیل $1/3$ و $22/7$. بنابراین، اعداد گویا را به‌عنوان یک حلقه با اعمال دوتایی جمع و ضرب کسرها در نظر خواهیم گرفت. این حلقه را با $\mathbb{Q}$ نشان خواهیم داد. این حرف از Quotients^۳ آمده است.

۳.۳.۱ مثال. به‌طور مشابه اعداد حقیقی به همراه اعمال جمع و ضرب معمول، تشکیل یک حلقه می‌دهد که آن را با $\mathbb{R}$ نشان خواهیم داد. (آیا می‌توانید بگویید که چرا

1. ring of integers
2. the integers

ریاضی دانان تصمیم گرفتند از این حرف بخصوص، برای اعداد حقیقی استفاده کنند؟

۴.۳.۱ مثال. مجموعه اعداد مختلط با جمع و ضرب معمول، تشکیل یک حلقه داده که آن را با $\mathbb{C}$ نمایش می دهیم. این اعمال عبارتند از:

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

$$(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i$$

برای هر $a, b, c, d \in \mathbb{R}$.

۵.۳.۱ مثال. مجموعه چندجمله ای ها با ضرایب اعداد صحیح به همراه اعمال جمع و ضرب معمول چندجمله ای ها تشکیل یک حلقه می دهد. این حلقه را با نماد $\mathbb{Z}[x]$ نشان می دهیم. لذا برای نمونه

$$(1+x+x^2) + (-2+3x-x^3) = -1+4x+x^2-x^3$$

و

$$(1+x+x^2) \cdot (-2+3x-x^3) = -2+x+x^2+2x^3-x^4-x^5.$$

۶.۳.۱ مثال. مجموعه ماتریس های 2×2 در 2 که درایه های آن اعداد حقیقی اند به همراه اعمال جمع و ضرب معمول ماتریس ها تشکیل یک حلقه می دهد. این حلقه را با $M_2(\mathbb{R})$ نشان می دهیم. این اعمال عبارتند از:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

برای هر $a, b, c, d, f, g, h \in \mathbb{R}$.

اکنون زمان مناسبی است که به این نکته اشاره کنیم که در نماد گذاری ها (همان طور که در مثال ۶.۳.۱ ملاحظه کردید)، از نماد یکسان به علاوه (+) برای نمایش

هر دو عمل جمع ماتریسی و عمل جمع اعداد حقیقی استفاده کردیم و نیز به‌طور معمول، به هر دو این اعمال "جمع" گفتیم. (به همین ترتیب در مثال ۴.۳.۱).
حال با در دست داشتن این شش مثال آماده‌ایم که تعریف یک حلقه را به‌طور رسمی بیان نماییم. این تعریف مشتمل بر اصول موضوعه است که اگر هر مجموعه‌ای با دو عمل در آن‌ها صدق کند، یک حلقه نامیده می‌شود. از خواننده می‌خواهیم که به محض خواندن هر اصل موضوع تأمل کند و درباره اینکه آن اصل موضوع در مورد شش مثال مطرح شده در متن چه می‌گوید، بیاندیشد.

۷.۳.۱ تعریف. یک حلقه^۱ مجموعه‌ای است مانند R به همراه دو عمل دوتایی روی R (جمع $+$ و ضرب $\cdot$) که در اصول موضوع زیر صدق کند:
(ح ۱) جمع شرکت‌پذیر است. یعنی، برای هر $a, b, c \in R$

$$a + (b + c) = (a + b) + c ;$$

(ح ۲) جمع جابجایی است. یعنی، برای هر $a, b \in R$

$$a + b = b + a ;$$

(ح ۳) R دارای عنصر صفر است. یعنی عنصری مانند 0 در R وجود دارد به‌طوری که برای هر $a \in R$

$$a + 0 = a ;$$

(ح ۴) برای هر $a \in R$ عنصری مانند $-a$ در R وجود دارد به‌طوری که

$$a + (-a) = 0 ;$$

(ح ۵) ضرب شرکت‌پذیر است. یعنی، برای هر $a, b, c \in R$

$$a.(b.c) = (a.b).c ;$$

(ح ۶) ضرب نسبت به جمع توزیع پذیر است. یعنی، برای هر $a, b, c \in R$

$$a.(b+c) = ab+ac \quad \text{و} \quad (a+b)c = ac+bc$$

چهار اصل موضوع اول بدین معنی است که $(R, +)$ یک گروه آبدی است. هرگاه R علاوه بر شش اصل موضوع فوق در اصل موضوع زیر نیز صدق کند، گوییم $(R, +, \cdot)$ یک حلقه جابجایی^۱ است

(ح ۷) ضرب جابجایی است. یعنی، برای هر $a, b \in R$

$$ab = ba$$

همچنین، هرگاه اصل موضوع زیر در حلقه R برقرار باشد، $(R, +, \cdot)$ را یک حلقه یکدار^۲ می نامیم

(ح ۸) R دارای عنصر همانی^۳ ضربی است. یعنی، عنصری مانند 1 در R وجود دارد به طوری که برای هر $a \in R$

$$a \cdot 1 = a.$$

در مثال های بالا، به جز مثال ۶.۳.۱، همه حلقه هایی جابجایی و یکدار بودند. اما حلقه $M_2(\mathbb{R})$ جابجایی نیست. زیرا به عنوان مثال

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

در حالی که

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

1. commutative ring
2. unitary ring
3. identity element

حلقه‌هایی مانند $M_2(\mathbb{R})$ که جابجایی نیستند را حلقه‌های غیرجابجایی^۱ می‌نامند.

۸.۳.۱ ملاحظات. (الف) همان‌طور که می‌دانید، منظور از یک عمل دوتایی^۲ روی یک مجموعه ناتهی R عبارت است از یک تابع از $R \times R$ به توی R . در این صورت گوییم R تحت آن عمل بسته است.

(ب) عنصر صفر در اصل موضوع (ح ۳)، شکل‌های متفاوتی در حلقه‌های مورد بحث دارد. مثلاً در حلقه‌های $\mathbb{Z}$ ، $\mathbb{Q}$ و $\mathbb{R}$ عنصر صفر دقیقاً عدد ۰ است. در حلقه $\mathbb{C}$ ، عنصر صفر عدد مختلط $0+i$ است. در حلقه چندجمله‌ای‌ها با ضرایب صحیح، $\mathbb{Z}[x]$ ، عنصر صفر چندجمله‌ای ثابت صفر است و در حلقه $M_2(\mathbb{R})$ ، عنصر صفر ماتریس صفر $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ می‌باشد. به هر حال عنصر صفر در هر حلقه منحصر به فرد است. (چرا؟) از این رو، عنصر صفر در یک حلقه R را با نماد ۰ (گاهی برای تأکید بر حلقه با 0_R) نشان می‌دهیم.

(ج) در حلقه R ، به ازای هر عنصر $a \in R$ دقیقاً یک عنصر مانند $-a$ در R وجود دارد به طوری که در (ح ۴) صدق کند. (چرا؟) به همین دلیل این عنصر منحصر به فرد را با $-a$ نمایش داده و آن را قرینه^۳ a می‌خوانیم.

(د) عنصر همانی ضربی در هر حلقه R (در صورت وجود) منحصر به فرد است. (چرا؟) از این رو آن را با ۱ (گاهی برای تأکید بر حلقه با 1_R) نشان داده و آن را با نام‌هایی متعددی از قبیل یک حلقه، واحد^۴ R و یا عنصر همانی R می‌خوانند.

۹.۳.۱ نمادگذاری. به منظور راحتی در نوشتار، از این پس برای هر $a, b \in R$ ، از نماد ab بجای $a.b$ و از نماد $a-b$ به جای $a+(-b)$ استفاده می‌کنیم.

همان‌طور که ملاحظه شد، اصول موضوع عنوان شده در تعریف، به واسطه‌ی آنچه که ما به‌طور جبری از یک حلقه انتظار داشتیم بیان شدند. لذا تعجب آور نیست

1. non-commutative rings
2. binary operation
3. inverse
4. unit

که قوانین جبری آشنای زیر (که به عمل جمع مربوط می‌شوند)، نیز برای یک حلقه دلخواه R برقرار باشد.

۱۰.۳.۱ قضیه. فرض کنیم R یک حلقه و $a, b, c \in R$ باشند. در این صورت

(الف) هرگاه $a + b = a + c$ آن‌گاه $b = c$ (قانون حذف جمعی^۱).

(ب) معادله $a + x = b$ و $(x + a = b)$ دارای جوابی منحصر به فرد است.

(ج) $-(-a) = a$.

(د) $-(a + b) = (-a) + (-b)$.

(ه) به ازای هر دو عدد صحیح m و n داریم

$$(m + n)a = ma + na, \quad m(a + b) = ma + mb, \quad m(na) = (mn)a$$

$$nab = a(nb) = n(ab)$$

(توجه شود که تعریف na در حلقه R ، همان تعریف na در گروه جمعی $(R, +)$ است.)

(و) اگر حلقه R یک‌دار باشد، $n \in \mathbb{N}$ و $n1 = 0$ آن‌گاه $na = 0$ برای هر $a \in R$.

(ز) اگر $1 \neq 0$ ، آن‌گاه R تنها از یک عنصر صفر تشکیل شده است. (در این حالت R

را حلقه بدیهی^۲ نامیم و می‌نویسیم $R = 0$ ، اگر $1 \neq 0$ را حلقه نابدیهی^۳ می‌نامیم.)

برهان. از آنجا هر حلقه به‌همراه عمل جمع خود یک گروه آبلی است، خواص (الف)–

(ه) نیز در گروه آبلی $(R, +)$ برقرار است. لذا فقط (و) را ثابت می‌کنیم.

(و) فرض کنیم R یک‌دار و $n1 = 0$ ($n \in \mathbb{N}$). عنصر $a \in R$ را دلخواه در نظر

می‌گیریم. در این صورت بنا بر اصل موضوع (ح ۸)، با توجه به خاصیت (ه) در بالا و

فرض (به ترتیب)، خواهیم داشت:

$$na = n(1a) = (n1)a = 0a = 0.$$

1. additive cancelation law

2. trivial ring

3. non-trivial ring

(ز) فرض کنیم R یک‌دار و $1 = 0$ باشد. در این صورت به ازای هر $a \in R$ ، بنا بر اصل موضوع (ح ۸) و فرض خواهیم داشت:

$$a = 1a = 0a = 0$$



لذا $R = 0$.

برخی دیگر از ویژگی‌های یک حلقه را که به عمل ضرب مربوط می‌شود، در قضیه زیر بیان می‌کنیم.

۱۱.۳.۱ قضیه. فرض کنیم R یک حلقه و $a, b, c \in R$ باشند. در این صورت

$$(الف) \quad a \circ 0 = 0a = 0$$

$$(ب) \quad (-a)b = a(-b) = -(ab)$$

$$(ج) \quad (-a)(-b) = ab$$

$$(د) \quad (a-b)c = ac - bc \quad \text{و} \quad a(b-c) = ab - ac$$

برهان. (الف) با توجه به اصول موضوع (ح ۶) و (ح ۳) داریم

$$0a + 0a = (0 + 0)a = 0a = 0a + 0$$

با حذف a از طرفین تساوی فوق خواهیم داشت $0a = 0$. اثبات $a0 = 0$ مشابه است.

(ب) به‌وضوح $x = -(ab)$ جوابی از معادله $x + ab = 0$ است. اما بنا به (ح ۶)، (ح ۴) و (الف) داریم

$$a(-b) + ab = a(-b + b) = a0 = 0.$$

از این‌رو $x = a(-b)$ جوابی دیگر از معادله است. بنا به ۱۰.۳.۱ (ب)، باید $a(-b) = -(ab)$. اثبات $(-a)b = -(ab)$ مشابه است.

(ج) به کمک قسمت (ب) و قضیه ۱۰.۳.۱ (ج)، داریم

$$(-a)(-b) = -((-a)b) = ab.$$

(د) به کمک (ح ۶) و قسمت (ب) می‌توان نوشت

$$a(b-c) = a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac$$



اثبات $(a-b)c = ac - bc$ مشابه است.

در ادامه، مثال دیگری از یک حلقه ارائه می‌دهیم که در این کتاب به کرار با آن سروکار خواهیم داشت. برای مشاهده مثال‌های دیگر به بخش خودآزمایی مراجعه نمایید. توجه شود که برای اثبات اینکه مجموعه‌ای با اعمال داده شده یک حلقه است یا خیر، می‌بایست هر شش اصل موضوع ذکر شده در تعریف را بررسی نمود (که کار خسته کننده‌ای است). در بخش ۴.۱، با معرفی مفهوم زیرحلقه، اشاره خواهیم کرد که این کار با بررسی اصول موضوع کمتری نیز امکان‌پذیر است.

۱۲.۳.۱ مثال. فرض کنیم n یک عدد صحیح مثبت دلخواه باشد. در زیر نشان می‌دهیم مجموعه اعداد صحیح به پیمانه n ، $\mathbb{Z}_n$ ، با اعمال جمع و ضرب به پیمانه n یک حلقه جابجایی و یک‌دار است. به عنوان یادآوری، اگر به ازای هر عدد صحیح a ، باقی‌مانده تقسیم a بر n را با $\bar{a}$ نشان دهیم آن‌گاه $\bar{a} = \bar{b}$ است اگر و فقط اگر $a - b$ مضربی از n باشد. در این صورت بنا به الگوریتم تقسیم خواهیم داشت:

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

برای هر $\bar{a}, \bar{b} \in \mathbb{Z}_n$ ، تعریف می‌کنیم

$$\bar{a} + \bar{b} = \overline{a+b}$$

و

$$\bar{a} \bar{b} = \overline{ab}$$

(اعمال جمع و ضرب در سمت راست تساوی‌های فوق همان اعمال جمع و ضرب معمول بین اعداد صحیح است.)

اعمال تعریف شده در بالا خوش تعریف بوده و به علاوه $(\mathbb{Z}_n, +)$ یک گروه آبدلی است. (تمرین ۵.۸.۱)

در زیر مابقی اصول موضوع را بررسی می‌کنیم. فرض کنیم $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ دلخواه باشند.

بررسی (ح ۵):

$$\begin{aligned}
 \overline{a(\overline{b\overline{c}})} &= \overline{a(\overline{bc})} && \text{تعریف ضرب در } \mathbb{Z}_n \\
 &= \overline{a(bc)} && \text{تعریف ضرب در } \mathbb{Z}_n \\
 &= \overline{(ab)c} && \text{شرکت پذیری ضرب در اعداد صحیح} \\
 &= \overline{(ab)c} && \text{تعریف ضرب در } \mathbb{Z}_n \\
 &= \overline{(ab)c} && \text{تعریف ضرب در } \mathbb{Z}_n
 \end{aligned}$$

بررسی (ح ۶):

$$\begin{aligned}
 \overline{a(\overline{b+c})} &= \overline{a(\overline{b+c})} && \text{تعریف جمع در } \mathbb{Z}_n \\
 &= \overline{a(b+c)} && \text{تعریف ضرب در } \mathbb{Z}_n \\
 &= \overline{ab+ac} && \text{توزیع پذیری ضرب نسبت به جمع در اعداد صحیح} \\
 &= \overline{ab+ac} && \text{تعریف جمع در } \mathbb{Z}_n \\
 &= \overline{ab+ac} && \text{تعریف ضرب در } \mathbb{Z}_n
 \end{aligned}$$

اثبات $\overline{(a+b)c} = \overline{ac} + \overline{bc}$ مشابه است.

بررسی (ح ۷):

$$\begin{aligned}
 \overline{ab} &= \overline{ab} && \text{تعریف ضرب در } \mathbb{Z}_n \\
 &= \overline{ba} && \text{جابجایی ضرب در اعداد صحیح} \\
 &= \overline{ba} && \text{تعریف ضرب در } \mathbb{Z}_n
 \end{aligned}$$

بررسی (ح ۸):

$$\overline{a \setminus} = \overline{a \setminus} = \overline{a}$$

تعریف ضرب در $\mathbb{Z}_n$

بنابراین $\mathbb{Z}_n$ به همراه اعمال جمع و ضرب تعریف شده در بالا یک حلقه جابجایی است.