بسم الله الرحمن الرحیم

۱۳۰۷

دانشگاه صنعتی خواجه نصیرالدین طوسی

نخستین دانشگاه صنعتی ایران

ساختارهای جبری

گروه، حلقه و میدان متناهی

شعبان قلندرزاده

دانشیار دانشکده ریاضی دانشگاه صنعتی خواجه نصیرالدّین طوسی

شماره ۵۵۰

قلندرزاده، شعبان، ۱۳۴۱ -

عنوان و نام پدیدآور: ساختارهای جبری گروه، حلقه و میدان متناهی/ شعبان قلندرزاده.

مشخصات نشر: تهران: دانشگاه صنعتی خواجه نصیرالدین طوسی، انتشارات، ۱۴۰۲.

مشخصات ظاهری: [۳۴۵] ص.: جدول.

شابک: ۸-۳۳-۵۲۳۴-۶۲۲-۹۷۸ ISBN: 978-622-5234-33-8

وضعیت فهرست نویسی: فیپا

یادداشت: واژه‌نامه.

یادداشت: کتابنامه: ص. [۳۴۵]

موضوع: حلقه‌ها (جبر)/ Rings (Algebra)

مدول‌ها (جبر)/ Modules (Algebra)

میدان‌های متناهی/ Finite fields (Algebra)

رده‌بندی کنگره: QA۲۴۷

رده‌بندی دیویی: ۵۱۲/۷۴

شماره کتابشناسی ملی: ۹۵۳۳۶۲۶

ناشر: دانشگاه صنعتی خواجه نصیرالدین طوسی **press.kntu.ac.ir**

عنوان: ساختارهای جبری گروه، حلقه و میدان متناهی

مؤلف: شعبان قلندرزاده

نوبت چاپ: اول

تاریخ انتشار: مرداد ۱۴۰۳

شمارگان: ۲۰۰ جلد

ویراستار: حسین علیقلی‌زاده

چاپ و صحافی: گرنامی

قیمت:

تمام حقوق برای ناشر محفوظ است

خیابان میرداماد غربی– شماره ۴۷۰– انتشارات دانشگاه صنعتی خواجه نصیرالدین طوسی – تلفن: ۸۸۸۸۱۰۵۲

میدان ونک – خیابان ولی‌عصر(عج) – بالاتر از چهارراه میرداماد – شماره ۲۶۲۶– مرکز پخش و فروش انتشارات

تلفن: ۸۸۷۷۲۲۷۷ رایانامه: press@kntu.ac.ir – تارنما (فروش برخط): press.kntu.ac.ir

زمان بی‌کرانه را

تو با شمارگام عمر ما مسنج

به پای او دمی‌ست این درنگ درد و رنج.

به‌سان رود

که در نشیب دره سر به سنگ می زند،

رونده باش.

امید هیچ معجزی ز مرده نیست

زنده باش.

ه.ا.سایه

پیش‌گفتار

جبر مجرد به عنوان شاخه‌ای از دانش ریاضی، در سده گذشته نه تنها در ریاضیات، بلکه در پیشبرد سایر علوم نیز نقشی به‌سزا ایفا کرده است. برای مثال می‌توان از کاربرد مفهوم گروه‌ها در فیزیک و شیمی، میدان‌های متناهی در نظریه کدگذاری و رمزنگاری، مفهوم تکواره‌ها در نظریه اتوماتا و... نام برد. افزون بر نقش جبر در دیگر علوم، این شاخه از دانش ریاضی ایفاگر نقش یک رابط اثر گذار در ایجاد آمیختگی بین شاخه‌های مختلف دانش ریاضی نیز بوده است و موجبات آفرینش شاخه‌های جدیدی در ریاضیات مانند هندسه جبری، نظریه جبری اعداد، آمار جبری و ... شده است.

کتاب حاضر بر اساس سر فصل درس «جبر» برنامه آموزشی دوره کارشناسی رشته ریاضیات و کاربردها و به‌عنوان در آمدی بر دنیای عظیم جبر نگارش یافته است، با این امید که بتواند مقدمه‌ای کوتاه در ورود به این دانش باشد. کتاب مشتمل بر هفت فصل همراه یک پیوست است. فصل نخست به معرفی حلقه‌ها و مفاهیم مرتبط می‌پردازد که در فصول پنج، شش و هفت استفاده خواهد شد. فصل دوم معرف مفهوم عمل یک گروه روی یک مجموعه به همراه مثال‌های مختلف از کاربرد این مفهوم در جبر خطی و هندسه و جبر است. فصل سوم کتاب شامل بیان قضایای سیلو و برخی کاربردهای این قضیه‌هاست .در فصل چهار به عنوان حسن ختام کتاب در نظریه گروه‌ها، گروه‌های حل‌پذیر و پوچ‌توان به‌همراه برخی خواص آنها ارائه شده است. در فصل پنج کتاب، حلقه خارج قسمتی چندجمله‌ای‌ها روی یک میدان برای بیان میدان‌های شکافنده معرفی شده است. در فصل شش بحثی مختصر در مورد دامنه‌های تجزیه به انجام رسیده و سرانجام در فصل هفت به‌عنوان برآیندی از سه فصل قبل،میدان، توسیع میدان و میدان‌های شکافنده معرفی گردیده است.

سخنی با دانشجو، اینکه:

« ما قواعدی کلی سراغ نداریم که بتواند مفیدترین ضوابط فکر را به تفصیل بیان

کند. حتی اگر بیان چنین قواعدی هم ممکن بود، چندان سودمند نبود. به جای دانستن قواعد صحیح تفکر از جنبه نظری، بهتر آن‌است که شخص این قواعد را در گوشت و خون خود جذب کند، به نحوی که برای استفاده آنی و فطری آماده باشند. بنابراین، برای تربیت قدرت تفکر، آنچه واقعاً مفید است تمرین در فکر کردن است. حل مستقل مسائل مبارزطلب شخص را به مراتب بیشتر از کلمات کوتاهی که به دنبال آنها می‌آید یاری می‌کند، اگر چه به عنوان اولین قدم زیانی از آنها متوجه او نمی‌شود.» **پولیا و سگو**

ازاین‌روی توصیه می‌شود که برای تمرین فکر کردن، به کنجکاوی نقادانه مسائل طرح شده در آخر هر فصل از کتاب پرداخته و به‌طور خلاقانه ایده‌های خود را با دانش ریاضی در حل آنها درآمیزید، به‌سان شاعری که واژه‌ها را با احساس و مانند نقاشی که رنگ‌ها را با بوم در می‌آمیزد. چرا که ریاضی خود هنر است، هنر اندیشیدن .

کلام آخر، کنفوسیوس سخنی دارد با این مضمون که اشتباه کردن و آن را اصلاح نکردن، خود به منزله اشتباهی دیگراست، ازاین‌روی سپاسگزار اندیشمندانی خواهم بود که خطاهای این نوشته را یادآوری نمایند تا نویسنده بر تصحیح آنها همت گمارد.

شعبان قلندرزاده
دانشگاه صنعتی خواجه نصیرالدین طوسی
ghalandarzadeh@kntu.ac.ir

فهرست مطالب

عنوان		صفحه
پیشگفتار		۱
فصل ۱	حلقه‌ها	۳
۱.۱	مثال‌ها و خواص مهم	۳
۲.۱	حوزه‌های صحیح و میدان‌ها	۱۵
۳.۱	ایده‌آل‌ها و حلقه‌های خارج قسمتی	۲۰
۴.۱	همومورفیسم حلقه‌ها	۳۰
۵.۱	میدان کسرها	۴۳
۶.۱	تمرین	۴۸
فصل ۲	عمل گروه	۵۵
۱.۲	عمل گروه	۵۵
۲.۲	مثال‌ها	۵۹
۳.۲	مدارها وپایدارسازها	۷۴
۴.۲	عمل p-گروه‌ها	۹۷
۵.۲	چند اثبات جدید با استفاده از عمل گروه	۹۹
۶.۲	کاربردهای بیشتر از عمل گروه در نظریه گروه‌ها	۱۰۳
۷.۲	کاربردهایی از عمل گروه در نظریه اعداد	۱۰۹
۸.۲	عمل انتقالی گروه	۱۱۰
۹.۲	تمرین	۱۱۶

فصل ۳ قضایای سیلو و کاربردهای آنها ۱۲۱

۱.۳ قضایای سیلو ۱۲۱

۲.۳ نتایجی از قضایای سیلو ۱۳۲

۳.۳ جابجایی‌پذیری و ساده بودن یک گروه ۱۴۱

۴.۳ سیلو زیرگروه‌های گروه خارج قسمتی ۱۴۹

۵.۳ نرمال‌ساز سیلو زیرگروه‌ها ۱۵۳

۶.۳ تمرین ۱۵۶

فصل ۴ گروه‌های حل‌پذیر و گروه‌های پوچ‌توان ۱۵۹

۱.۴ گروه‌های حل‌پذیر ۱۵۹

۲.۴ گروه‌های پوچ‌توان ۱۸۱

۳.۴ تمرین ۱۸۷

فصل ۵ حلقه چندجمله‌ای‌ها ۱۸۹

۱.۵ حلقه‌چندجمله‌ای‌ها ۱۸۹

۲.۵ تجزیه چندجمله‌ای‌ها روی یک میدان ۲۰۴

۳.۵ حلقه خارج‌قسمتی چندجمله‌ای‌ها روی یک میدان ۲۲۰

۴.۵ تمرین ۲۳۳

فصل ۶ دامنه‌های صحیح ۲۳۹

۱.۶ دامنه‌های تجزیه‌یکتا ۲۳۹

۲.۶ دامنه‌های ایده‌آل اصلی ۲۵۷

۳.۶ دامنه‌های اقلیدسی ۲۶۱

۴.۶ تمرین ۲۶۶

فصل ۷ میدان‌ها ۲۶۹

۱.۷ مروری مختصر بر جبرخطی ۲۶۹

۲.۷ توسیع میدان ۲۷۲

۳.۷ عناصر جبری ۲۷۶
۴.۷ میدان‌های شکافنده ۲۹۷
۵.۷ میدان‌های متناهی ۳۰۹
۶.۷ ترسیم‌های هندسی ۳۲۰
۷.۷ تمرین ۳۲۹

پیوست ۳۳۳

واژه‌نامه و نمایه ۳۴۷

مراجع ۳۵۵

۱

حلقه‌ها

در این فصل به معرفی یکی از موضوعات اصلی کتاب یعنی حلقه‌ها خواهیم پرداخت. ابتدا حلقه را تعریف کرده و سپس چند مثال مهم از حلقه‌ها ارائه و در ادامه بعضی خواص آنها را ثابت خواهیم کرد. سپس به بررسی کلاس مهمی از حلقه‌ها که حوزه های صحیح هستند، خواهیم پرداخت. سرانجام در مورد ایده‌آل‌های یک حلقه و مفاهیم مرتبط با آن و هم‌چنین در باره همومورفیسم حلقه‌ها مطالبی بیان خواهیم کرد.

۱.۱ مثال‌ها و خواص مهم

تعریف ۱.۱.۱. یک حلقه یک مجموعه ناتهی مانند R همراه با دو عمل روی R- که به‌طورمعمول جمع و ضرب نامیده می‌شوند - است که در اصول زیر صادقند:

$(R_۱)$ برای هر $a,b \in R$، $a+b=b+a$؛

$(R_۲)$ برای هر $a,b,c \in R$، $(a+b)+c=a+(b+c)$؛

$(R_۳)$ عنصر $\circ \in R$ موجود است، به‌گونه‌ای که برای هر $a \in R$، $a+\circ=\circ+a=a$؛

$(R_۴)$ برای هر $a \in R$، $-a \in R$ موجود است، به‌طوری‌که: $a+(-a)=(-a)+a=\circ$؛

$(R_۵)$ برای هر $a,b,c \in R$، $(a\cdot b)\cdot c=a\cdot(b\cdot c)$؛

$(R_۶)$ عنصر ۱ از R موجود است، به‌طوری‌که برای هر $a \in R$، $a\cdot ۱=۱\cdot a=a$؛

$(R_۷)$ برای هر a,b,c عضو R، $a\cdot(b+c)=a\cdot b+a\cdot c$ و $(a+b)\cdot c=a\cdot c+b\cdot c$.

حلقه R را جابجایی نامیم، هرگاه برای هر $a,b \in R$ داشته باشیم $a \cdot b = b \cdot a$. معمولاً در نمایش عناصر همانی دو عمل جمع و ضرب وقتی به‌خواهیم به حلقه R نیز اشاره کنیم از نمادهای ۰_R و ۱_R به‌جای ۰ و ۱ استفاده خواهیم کرد.

بعضی موارد می‌توان خاصیت $(R_۶)$ را از خواص حلقه حذف کرد. دراین‌صورت R را یک حلقه بدون عنصر همانی ضرب می‌نامند ولی اگر $(R_۶)$ برقرار باشد آنگاه R را یک حلقه یکدار می‌نامند. لازم به ذکر است که در این کتاب فرض بر این است که همه حلقه‌ها در $(R_۶)$ صادقند. یعنی همه حلقه‌ها یکدار فرض می‌شوند. خواص $(R_۱)$ تا $(R_۴)$ بیان می‌کنند که $(R,+)$ یک گروه آبلی است. خواص $(R_۵)$ و $(R_۶)$ بیانگر این مطلب است که $(R,.)$ یک تکواره است. بنابراین عضو همانی عمل ضرب یعنی ۱_R حلقه منحصربه فرد است. به‌طور مشابه ۰_R نیز منحصر به فرد است.

مثال ۱.۱. مجموعه‌های $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ با جمع و ضرب معمولی و مجموعه $\mathbb{C}$ با جمع و ضرب اعداد مختلط حلقه‌های جابجایی و یکدار بوده و مجموعه $۲\mathbb{Z}$ با عمل جمع وضرب اعداد صحیح یک حلقه جابجایی فاقد عضو همانی ضرب است.

مثال ۲.۱. فرض کنید n یک عدد صحیح مثبت باشد و فرض کنید $\mathbb{Z}_n = \{\bar{۰}, \bar{۱}, \cdots, \overline{n-۱}\}$. آنگاه مجموعه $\mathbb{Z}_n$ با جمع و ضرب به پیمانه n که به شکل

$$a \bigotimes b = n \text{ مانده تقسیم } a \cdot b \text{ بر}$$

$$a \bigoplus b = n \text{ مانده تقسیم } a + b \text{ بر}.$$

تعریف می‌شود یک حلقه جابجایی است.

مثال ۳.۱. فرض کنید $M_n(\mathbb{Q})$ مجموعه ماتریس‌های $n \times n$ با درایه‌های عضو $\mathbb{Q}$ باشند. آنگاه $M_n(\mathbb{Q})$ با جمع و ضرب ماتریس‌ها یک حلقه است و بدیهی است که برای $n \geq ۲$، $M_n(\mathbb{Q})$ جابجایی نیست. در حالت کلی اگر R یک حلقه باشد، آنگاه $M_n(R)$ نیز با جمع و ضرب ماتریس‌ها یک حلقه است.

مثال ۴.۱. (حلقه چندجمله‌ای‌ها) فرض کنید R یک حلقه باشد. قرار دهید:

$$R[x] = \{a_\circ + a_1 x + \cdots + a_m x^m \mid a_\circ, \cdots, a_m \in R, m \in \mathbb{N}\}$$

که x یک مجهول خواهد بود. هر عضو این مجموعه را یک چندجمله‌ای با ضرائب در R و a_n را ضریب جمله پیشرو می‌نامند و هرگاه ضریب جمله پیشرو مساوی 1_R باشد، چندجمله‌ای را تکین می‌نامند. لازم به ذکر است که جمع بین جملات یک چندجمله‌ای وهم چنین ضرب عناصر a_i از R در مجهول x صوری است.

روی مجموعه $R[x]$ تساوی ، جمع و ضرب چندجمله‌ای‌ها را به شکل زیر تعریف می‌کنیم که چندجمله‌ای‌های $p(x) = a_\circ + a_1 x + \cdots + a_n x^n$ و $q(x) = b_\circ + b_1 x + \cdots + b_m x^m$ مساوی هستند اگر و فقط اگر برای هر $i \geq \circ$، $a_i = b_i$.

ازاین‌روی $p(x) = q(x)$ ایجاب می کند که $m = n$ و برای هر $\circ \leq i \leq n$، $a_i = b_i$.
قبل از تعریف جمع چندجمله‌ای‌ها این نکته قابل ذکر است که هرگاه $n \geq m$ می‌توان جملاتی که در آنها $b_{m+1} = \cdots = b_n = \circ$ به چندجمله‌ای $q(x)$ اضافه کرد. حال با توجه به نکته اشاره شده اگر $s = Max(m,n)$، آنگاه

$$p(x) + q(x) = \sum_{i=\circ}^{s} (a_i + b_i) x^i = (a_\circ + b_\circ) + (a_1 + b_1)x + \cdots + (a_s + b_s)x^s.$$

باید این نکته را بیان کرد که عمل جمع داخل هر کدام از پرانتزها همان عمل جمع حلقه R و عمل جمع بین پرانتزها صوری است.

حال عمل ضرب دو چندجمله‌ای را تعریف می‌کنیم:

$$p(x) \cdot q(x) = c_\circ + c_1 x + \cdots + c_t x^t,$$

$$c_k = a_k b_\circ + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_\circ b_k = \sum_{i=\circ}^{k} a_i b_{k-i},$$

برای هر $\circ \leq k \leq t \leq m + n$.

نکته‌ای که به ضرورت باید ذکر کرد، این است که اگر R یک حلقه یکدار و جابجایی باشد، $R[x]$ نیز چنین است. پس این مطلب را به شکل لم زیر بیان می‌کنیم.

لم ۱.۱.۱. اگر R حلقه‌ای یکدار و جابجایی باشد، آنگاه $R[x]$ یک حلقه جابجایی و یکدار است و به‌علاوه $1_{R[x]} = 1_R$.

اثبات. در گام نخست نشان می‌دهیم که $R[x]$ تحت عمل جمع چندجمله‌ای‌ها یک گروه آبلی است. به سادگی می‌توان دید که چندجمله‌ای $f(x) = 0$ عنصر همانی عمل جمع است. هم‌چنین بدیهی است که برای هر چندجمله‌ای مانند $p(x) = \sum_{i=0}^{n} a_i x^i$، چندجمله‌ای $-p(x)$ که به شکل $-p(x) = -\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (-a_i) x^i$ تعریف می‌شود، وارون جمعی $p(x)$ خواهد بود. جابجایی و شرکت‌پذیری عناصر این مجموعه نسبت به عمل جمع از تعریف جمع چندجمله‌ای‌ها و جابجایی و شرکت‌پذیری حلقه R به دست می‌آید. برای اثبات شرکت‌پذیری عمل ضرب فرض کنید

$$p(x) = \sum_{i=0}^{m} a_i x^i, \qquad q(x) = \sum_{i=0}^{n} b_i x^i, \qquad r(x) = \sum_{i=0}^{p} c_i x^i.$$

بنابراین

$$\begin{aligned}
[p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right) c_{i-j}\right] x^i \\
&= \sum_{i=0}^{m+n+p}\left(\sum_{j+k+l=i} a_j b_k c_l\right) x^i \\
&= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right] x^i
\end{aligned}$$

$$\begin{aligned} &= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n+p}\left(\sum_{j=0}^{i} b_j c_{i-j}\right)x^i\right] \\ &= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\left(\sum_{i=0}^{n} b_i x\right)\left(\sum_{i=0}^{p} c_i x^i\right)\right] \\ &= p(x)[q(x)r(x)]. \end{aligned}$$

خواص جابجایی و توزیع‌پذیری ضرب چندجمله‌ای‌ها به روش مشابه قابل اثبات است و به‌عنوان یک تمرین محاسباتی واگذار می‌شود. □

حلقه $R[x]$ را حلقه چندجمله‌ای‌های روی حلقه R می‌نامند. به‌عنوان مثال، برای محاسبه ضرب چندجمله‌ای‌ها در حلقه چندجمله‌ای‌های $\mathbb{Z}_3[x]$ داریم:

$$\begin{aligned} (x+1)^3 &= (x+1)(x+1)(x+1) = (x^2+2x+1)(x+1) \\ &= x^3+3x^2+3x+1 = x^3+1. \end{aligned}$$

زیرا در حلقه $\mathbb{Z}_3$ داریم $3 \equiv 0 \pmod 3$.

هم‌چنین این مطلب مهم است که بیان کنیم در ضرب چندجمله‌ای‌ها فرض بر این است که برای هر $a \in R$، $a \cdot x = x \cdot a$.

حلقه چندجمله‌ای‌ها در فصل پنج به‌طور دقیق‌تر مورد بحث و بررسی قرار خواهد گرفت.

مثال ۵.۱. فرض کنید X یک مجموعه ناتهی و $F(X,\mathbb{R})$ مجموعه همه توابع $f : X \to \mathbb{R}$ باشد. می‌توان نشان داد که $F(X,\mathbb{R})$ با عمل جمع و ضرب نقطه‌ای تعریف شده در زیر یک حلقه یکدار است:

$$\begin{aligned} (f \cdot g)(a) &= f(a) \cdot g(a), \quad a \in X \\ (f+g)(a) &= f(a)+g(a), \quad a \in X. \end{aligned}$$

بدیهی است که تابع $0 : X \to \mathbb{R}$ با ضابطه $0(a) = 0_{\mathbb{R}}$ برای هر $a \in X$ و تابع $1 : X \to \mathbb{R}$ با ضابطه $1(a) = 1_{\mathbb{R}}$ برای هر $a \in X$ عناصر همانی عمل جمع و ضرب این حلقه خواهندبود.