فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۵ (پاییز ۱۳۷۹)، صص. ۲۳ تا ۳۷

حلقهٔ چهارگانها

منصور معتمدی

مقدمه: نخستین مثال حلقه‌های تقسیمی تعویض‌ناپذیر به نام چهارگانها یا چهارگانهای حقیقی توسط ویلیام راون همیلتن کشف شد. روش ساختن چهارگانهای حقیقی به گونه‌ای است که به جای هیأت اعداد حقیقی می‌توان از هر حلقهٔ تعویض‌پذیر A استفاده کرد. حلقهٔ حاصل را حلقهٔ چهارگانها روی A می‌نامیم. حالت‌های کلاسیک با انتخاب هیأت اعداد حقیقی، حلقهٔ اعداد صحیح یا هر زیر حلقهٔ دیگر اعداد گویا به دست می‌آید. هدف این نوشتار که در سه بخش تنظیم شده است مطالعهٔ مقدماتی حلقهٔ چهارگانها است. در بخش اوّل به معرفی بعضی ویژگی‌های عمومی این گونه حلقه‌ها می‌پردازیم. در بخش دوّم A را یک هیأت دلخواه فرض می‌کنیم. در بخش پایانی چهارگانهای صحیح و ایده‌آل‌های آن، مورد نظر هستند. مرکز حلقهٔ A را با $C(A)$، حلقهٔ ماتریس‌ها با درآیه‌ها در حلقهٔ A را با $M_n(A)$ و تعداد اعضای مجموعهٔ X را با $|X|$ نشان می‌دهیم.

۱. خواص مقدماتی $H(A)$

گزارهٔ ۱. فرض کنیم A حلقه‌ای تعویض‌پذیر است. اگر حاصلضرب دکارتی $A \times A \times A \times A$ را تشکیل داده، عمل جمع و ضرب دلخواه (a_0, a_1, a_2, a_3) و (b_0, b_1, b_2, b_3) را در آن با تساوی‌های زیر تعریف کنیم:

$$(a_0, a_1, a_2, a_3) + (b_0, b_1, b_2, b_3) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3)$$
$$(a_0, a_1, a_2, a_3) \times (b_0, b_1, b_2, b_3) = (c_0, c_1, c_2, c_3)$$

که در آن

$$c_0 = a_1 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3$$
$$c_1 = a_0 b_2 + b_0 a_1 + a_2 b_3 - a_3 b_2$$
$$c_2 = a_0 b_2 + b_0 a_2 + a_3 b_1 - a_1 b_3$$
$$c_3 = a_0 b_3 + b_0 a_3 + a_1 b_2 - a_2 b_1$$

در این صورت $A \times A \times A \times A$ با این دو عمل یک حلقهٔ واحددار است.

اثبات. اثبات قضیه شبیه اثبات در مورد چهارگانهای حقیقی است، و در اینجا به ذکر چند نکته بسنده می‌کنیم. عضو صفر این حلقه برابر با $(0, 0, 0, 0)$ و قرینهٔ (a, b, c, d) عبارتست از $(-a, -b, -c, -d)$. واحد این حلقه برابر است با $(1, 0, 0, 0)$. □

تعریف. حلقهٔ مذکور در گزارهٔ ۱ را حلقهٔ چهارگانها روی A می‌نامیم و آن را با $H(A)$ نشان می‌دهیم.

گزارهٔ ۲: برای هر حلقه A، $H(A)$ یک توسیع A است.

اثبات. کافی است توجّه کنیم تابع $f : A \to H(A)$ که با ضابطهٔ $f(a) = (a, 0, 0, 0)$ تعریف می‌شود، یک تکریختی حلقه‌ها است و لذا A را در $H(A)$ می‌نشاند. □

اگر در حلقهٔ $H(A)$ قرار دهیم

$$i = (0, 1, 0, 0), \quad j = (0, 0, 1, 0), \quad k = (0, 0, 0, 1)$$

مشاهده می‌شود که

$$i^2 = j^2 = k^2 = (-1, 0, 0, 0)$$
$$ij = k = -ji$$
$$jk = i = -kj$$
$$ki = j = -ik$$

با این قرارداد و یکی دانستن -1 و $(-1, 0, 0, 0)$ در واقع می‌توان $H(A)$ را یک $A-$ مدول آزاد با پایهٔ $\{1, i, j, k\}$ تعریف کرد که در آن ۱ همان واحد حلقهٔ A است. اکنون با توجّه به قوانین ضرب فوق این $A-$ مدول آزاد به یک حلقه تبدیل می‌شود. از این رو $H(A)$ یک $A-$ جبر است. بنابر این

$$H(A) = \{a + bi + cj + dk : a, b, c, d \in A\}$$

گزارهٔ ۳: فرض‌کنیم A یک حوزهٔ صحیح است. اگر مشخصهٔ A برابر با ۲ نباشد، آن‌گاه $C\big(H(A)\big) = A$.

اثبات. بدیهی است که $A \subseteq C\big(H(A)\big)$. فرض‌کنیم $x = a+bi+cj+dk$ یک عضو $C\big(H(A)\big)$

باشد. از آنجا که باید تساوی $xi = ix$ برقرار باشد داریم $ai - b + ck - dj = ai - b - ck - dj$ پس $c = -c$ و $d = -d$. امّا A یک حوزه صحیح است و لذا $c = d = 0$. به همین نحو از لزوم تساوی $jx = xj$ نتیجه می‌شود که $b = 0$، از این رو $x = a$ و $x \in A$. بنابر این $C(H(A)) = A$. $\square$

نتیجه. اگر A یک حلقهٔ تعویض‌پذیر باشد، آن گاه $H(A)$ تعویض‌پذیر است اگر و تنها اگر مشخصهٔ A برابر با ۲ باشد.

اثبات. بدیهی است. $\square$

تعریف (مزدوج): فرض کنیم $x = a + bi + cj + dk$ یک عضو $H(A)$ باشد مزدوج x که آن را با x^* نشان می‌دهیم با $x^* = a - bi - cj - dk$ تعریف می‌شود.

گزارهٔ ۴. اگر A حلقه‌ای تعویض‌پذیر باشد برای هر $u, v \in A$ و برای هر $x, y \in H(A)$ تساوی‌های زیر برقرارند:

آ) $(x^*)^* = x^*$

ب) $(ux + vy)^* = ux^* + vy^*$

پ) $(xy)^* = y^*x^*$

اثبات. قسمت‌های (آ) و (ب) به سادگی اثبات می‌شوند. برای اثبات قسمت (پ)، با توجّه به قسمت (ب) کافی است درستی تساوی برای i، j و k تحقیق شوند که آن نیز به سادگی انجام می‌شود. $\square$

توجه: ازگزارهٔ قبل چنین نتیجه می‌شود که تابع $* : H(A) \rightarrow H(A)$ که هر عضو x در $H(A)$ را به مزدوج آن x^* می‌نگارد در واقع یک بازگشت روی $H(A)$ است. بنابر این $H(A)$ حلقه‌ای با بازگشت است.

گزارهٔ ۵: اگر $x = a + bi + cj + dk$ یک عضو $H(A)$ باشد، آن گاه

$$xx^* = x^*x = a^2 + b^2 + c^2 + d^2$$

اثبات. محاسبهٔ مستقیم نتیجه را آشکار می‌سازد. $\square$

تعریف (نرم): فرض کنیم $x = a + bi + cj + dk$ یک عضو $H(A)$ است. نرم x که با $N(x)$ نشان داده می‌شود چنین تعریف می‌شود:

$$N(x) = xx^* = x^*x = a^2 + b^2 + c^2 + d^2$$

گزارهٔ ۶: اگر u یک عضو حلقهٔ تعویض‌پذیر A باشد برای هر $x, y \in H(A)$،

آ) $N(u) = u^2$

ب) $N(ux) = u^2 N(x)$

پ) $N(xy) = N(x)N(y)$

اثبات.قسمت‌های (آ) و (ب) بدیهی‌اند، برای اثبات (پ) توجّه می‌کنیم که برای هر $x \in H(A)$، $N(x) \in A$ و لذا $N(x) \in C\big(H(A)\big)$ پس

$$N(xy) = (xy)(xy)^* = (xy)(y^*x^*) = xyy^*x^*$$
$$= xN(y)x^* = xx^*N(y) = N(x)N(y).\square$$

گزارهٔ ۷: اگر x یک عضو $H(A)$ باشد. آن گاه x در $H(A)$ وارون‌پذیر است اگر و تنها اگر $N(x)$ در A وارون‌پذیر باشد. در این حالت $x^{-1} = \big(N(x)\big)^{-1}x^*$.

اثبات. اگر $x \in H(A)$ وارون‌پذیر باشد و $xy = 1$ پس

$$1 = N(1) = N(xy) = N(x)N(y)$$

و لذا $N(y) \in A$ در A، وارون $N(x)$ است. به عکس اگر $N(x)$ در A وارون‌پذیر باشد، $\big(N(x)\big)^{-1}x^* \in H(A)$، $x^*\big(N(x)\big)^{-1}$. اکنون تساوی‌های

$$\big(N(x)\big)^{-1}x^*x = \big(N(x)\big)^{-1}N(x) = 1$$
$$xx^*\big(N(x)\big)^{-1} = N(x)\big(N(x)\big)^{-1} = 1$$

نشان می‌دهند که x در $H(A)$ وارون‌پذیر است. $\square$

تعریف (اثر): اگر $x = a + bi + cj + dk$ یک عضو $H(A)$ باشد اثر x را با $x + x^* = 2a$ تعریف می‌کنیم و آن را با $Tr(x)$ نشان می‌دهیم.

گزارهٔ ۸: برای هر v و u در حلقه A و برای هر $x, y \in H(A)$ داریم:

آ) $Tr(u) = 2u$

ب) $Tr(ux + vy) = uTr(x) + uTr(y)$

پ) $Tr(xy) = Tr(yx)$

ت) $x^2 - Tr(x)x - N(x) = 0$

اثبات.تمام تساوی‌ها مستقیماً از تعریف نتیجه می‌شوند. $\square$

۲. چهارگانها روی یک هیأت

در این بخش F یک هیأت است.

گزارهٔ ۹: فرض کنیم A یک زیرحلقهٔ هیأت اعداد مختلط یعنی $\mathbb{C}$ است. در این صورت $H(A)$ با یک زیرحلقهٔ $M_2(\mathbb{C})$ یکریخت است.

اثبات. ریشهٔ دوّم ۱− در $\mathbb{C}$ را با w نشان می‌دهیم تابع

$$f : H(A) \to M_2(\mathbb{C})$$

را برای هر $a + bi + cj + dk$ چنین تعریف می‌کنیم

$$f(a+bi+cj+dk) = \begin{bmatrix} a+bw & c+dw \\ \frac{1}{2}(c-dw) & a-bw \end{bmatrix}$$

می‌توان نشان داد که f یک تکریختی حلقه‌ها است. □

گزارهٔ ۱۰: $H(F)$ یک حلقهٔ تقسیمی است اگر و تنها اگر v و u در F وجود نداشته باشد که $u^2 + v^2 = -1$.

اثبات. ابتدا فرض کنیم u و v در F چنان باشند که $u^2+v^2 = -1$. اگر قرار دهیم $x = 1+ui+vj$، آن گاه $N(x) = 1 + u^2 + v^2 = 0$. از گزارهٔ ۷ نتیجه می‌شود که x در $H(F)$ وارون‌پذیر نیست. به عکس فرض کنیم $H(F)$ یک حلقهٔ تقسیمی نباشد. پس بنابر گزارهٔ ۷، $x = a + bi + cj + dk$ مخالف صفر در $H(F)$ وجود دارد که $N(x) = a^2 + b^2 + c^2 + d^2 = 0$. می‌توان فرض کرد که $a \neq 0$. اگر $a^2 + b^2 = 0$ پس $(ba^{-1})^2 + 0^2 = -1$ و اثبات تمام است، پس فرض می‌کنیم $a^2 + b^2 \neq 0$ و قرار می‌دهیم $y = c + di$ و $z = a + bi$ لذا $N(z) = a^2 + b^2 \neq 0$ و بنابر گزارهٔ ۷، z در $H(F)$ وارون‌پذیر است. اکنون با توجّه به اینکه $a^2 + b^2 + c^2 + d^2 = 0$ داریم:

$$N(yz^{-1}) = N(y)\big(N(z)\big)^{-1} = (c^2+d^2)(a^2+b^2)^{-1} = -1$$

همچنین

$$yz^{-1} = (yz^*)\big(N(z)\big)^{-1} = (c+di)(a-bi)\big(N(z)\big)^{-1} = u+iv$$

که در آن u و v عناصری در F هستند. بنابر این

$$-1 = N(yz^{-1}) = N(u+iv) = u^2+v^2$$

و اثبات تمام است. □

نتیجه. اگر F یک زیرهیأت اعداد حقیقی باشد، آن گاه $H(F)$ یک حلقهٔ تقسیمی است.
اثبات. بدیهی است. □

برای اثبات گزارهٔ بعد به لم زیر که در اکثر کتاب‌های درسی جبر به عنوان مسأله عنوان می‌شود، نیاز است. [ر. ک ۶]

لم: فرض کنیم p یک عدد اوّل فرد است. در این صورت هر عضو هیأت $\frac{z}{pz}$ مجموع دو مربع کامل است.

اثبات. قرار می‌دهیم $F = \frac{z}{pz}$. اگر $x, y \in F$ آن گاه $x^۲ = y^۲$ اگر و تنها اگر $x = y$ یا اینکه $x = -y$، لذا اگر مجموعهٔ عناصری در F را که مربع کامل هستند S بنامیم S دارای $\frac{p-۱}{۲}$ عنصر ناصفر است و $|S| = \frac{p+۱}{۲}$. فرض کنیم $a \in F$، قرار می‌دهیم $T = \{a - s : s \in S\}$ در این صورت $|S| = |T| = \frac{p+۱}{۲}$ پس $S \cap T = \varnothing$ و به ازای $x, y \in F$، $a - x^۲ = y^۲$ بنابر این $a = x^۲ + y^۲$. □

گزارهٔ ۱۱: اگر p یک عدد اوّل فرد باشد و قرار دهیم $F = \frac{z}{pz}$ آن گاه

$$H(F) \cong M_۲(F)$$

اثبات. بنابر لم قبل $u, v \in F$ وجود دارند که $-۱ = u^۲ + v^۲$، اکنون قرار می‌دهیم

$$e = \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix} \qquad x = \begin{bmatrix} ۰ & ۱ \\ -۱ & ۰ \end{bmatrix} \qquad y = \begin{bmatrix} u & v \\ v & -u \end{bmatrix} \qquad z = \begin{bmatrix} v & -u \\ -u & -v \end{bmatrix}$$

به سادگی مشاهده می‌شود که $x^۲ = y^۲ = z^۲ = -e$

$$xy = z = -yx \quad \text{و} \quad yz = x = -zy \quad \text{و} \quad zx = y = -xy$$

اگر $a + bi + cj + dk$ یک عضو F باشد تابع

$$f : H(F) \to M_۲(F)$$

را چنین تعریف می‌کنیم

$$f(a + bi + cj + dk) = ae + bx + cy + dz$$

f یک همریختی حلقه‌ها است. مجموعه $\{e, x, y, z\}$ یک پایه برای فضای برداری $M_۲(F)$ روی F است و علاوه بر آن

$$\{e, x, y, z\} \subseteq f\big(H(F)\big)$$

بنابر این $f\big(H(F)\big) = M_{2}(F)$. امّا، بُعد $H(F)$ و نیز بُعد $M_{2}(F)$ روی F برابر ۴ است. بنابر این f یک یکریختی است. □

پیش از بیان گزارهٔ بَعد یادآوری می‌کنیم که مجموع عناصر پوچ‌توان هر حلقهٔ تعویض‌پذیر A یک ایده‌آل حلقهٔ A و برابر اشتراک تمام ایده‌آل‌های اوّل آن است. این ایده‌آل را رادیکال اوّل A می‌نامیم و با $N(A)$ یا N نشان می‌دهیم.

گزارهٔ ۱۲: قرار می‌دهیم $S = H\left(\frac{z}{2z}\right)$ و فرض می‌کنیم N رادیکال اوّل S است:

آ) S یک حلقهٔ تعویض‌پذیر با ۱۶ عضو است.

ب) $N^{2} \neq (0)$ امّا $N^{3} = (0)$

پ) $\frac{S}{N} \cong \frac{z}{2z}$

اثبات. بنابر نتیجهٔ گزارهٔ ۳، S حلقه‌ای تعویض‌پذیر است و بدیهی است که S دارای ۱۶ عضو است. بنابر گزارهٔ ۷، $x \in S$ وارون‌پذیر است و تنها اگر $N(x) = 1$. بنابراین مجموعهٔ عناصر وارون‌پذیر S برابر است با

$$\{1, i, j, k, 1+j+k, 1+j+k, 1+i+k, 1+i+j\}$$

اگر $x \in S$ وارون‌پذیر باشد محاسبه مستقیم نشان می‌دهد که $x^{2} = 0$ بنابراین

$$N = \{0, 1+i, 1+j, 1+k, 1+j, i+k, 1+i+j+k\}$$

و برای هر $x \in N$، $x^{2} = 0$. از آنجا که $(1+i)(1+j) \neq (0)$، $N^{2} \neq 0$. امّا محاسبه مستقیم نشان خواهد داد که $N^{3} = (0)$. به علّت اینکه $\frac{S}{N}$ دارای دو عضو است، با $\frac{z}{2z}$ یکریخت است. □

۳. چهارگانهای لیپشیتز

در این بخش حلقهٔ $H(Z)$ را مطالعه می‌کنیم. این حلقه به چهارگانهای لیپشیتز موسوم است و به همین جهت آن را با L نشان می‌دهیم. ابتدا به بیان تعریفی که در گزارهٔ ۱۳ به آن نیاز داریم می‌پردازیم.

تعریف. فرض کنیم A یک حلقه باشد که لزوماً تعویض‌پذیر نیست. حلقهٔ خارج‌قسمت‌های راست حلقه‌ای است مانند S به طوری که $A \subseteq S$ و

آ) هر عضو A که مقسوم‌علیه صفر نیست در S وارون‌پذیر است.

ب) هر عضو S را می‌توان به شکل ab^{-1} نوشت که در آن $a, b \in A$ و b مقسوم‌علیه صفر نیست.

توجه: اگر A حلقه‌ای تعویض‌پذیر باشد حلقهٔ خارج‌قسمت‌های آن وجود دارد، در غیر این صورت حلقهٔ خارج‌قسمت‌های راست و حلقهٔ خارج‌قسمت‌های چپ جداگانه تعریف می‌شوند. وجود آنها منوط به برقراری شرطی به نام شرط اور است. [ر. ک۳]

گزارهٔ ۱۳: حلقهٔ L فاقد مقسوم‌علیه صفر است و حلقهٔ خارج‌قسمت‌های راست آن حلقهٔ تقسیمی $H(Q)$ می‌باشد.

اثبات. به علت اینکه L یک زیرحلقهٔ $H(Q)$ است، در نتیجه مقسوم علیه صفر ندارد. حال فرض می‌کنیم $x = a + bi + cj + dk$ یک عضو $H(Q)$ باشد. عدد صحیح و ناصفر z وجود دارد به طوری که za, zb, zc, zd اعداد صحیح‌اند. بنابر این $xz \in L$ و به ازای یک $l \in L$، $x = lz^{-۱}$. از آنجا که هر عضو ناصفر $H(Q)$ وارون‌پذیر است نتیجه می‌گیریم که $H(Q)$ حلقهٔ خارج‌قسمت‌های H می‌باشد. $\square$

گزارهٔ ۱۴: گروه عناصر وارون‌پذیر L برابر است با

$$\{۱, i, j, k, -۱, -i, -j, -ki\}$$

که با گروه چهارگانها یکریخت است.

اثبات. محاسبه مستقیم نتیجه را آشکار می‌سازد. $\square$

گزارهٔ ۱۵: گروه خودریختی‌های L، ۲۴ عضو دارد.

اثبات. فرض کنیم f یک خودریختی L باشد. قرار می‌دهیم $x = f(i)$. از اینکه

$$x^۲ = f(i)f(i) = f(i^۲) = f(-۱) = -۱$$

نتیجه می‌گیریم که x یک عضو وارون‌پذیر H و $x-$ وارون آن است. به لحاظ اینکه f یک خودریختی است $f(i) \neq ۱$ همچنین $f(i) \neq ۱$، لذا $x \in S$ و ۶ انتخاب برای x وجود دارد متشابهاً $f(j) \in S$. امّا برای $f(j)$ چهار انتخاب وجود دارد چون که با $f(i)$ و $f(i)-$ متمایزند. از آنجا که $f(k) = f(i)f(j)$، عمل f روی h کاملاً با مقادیر $f(i)$ و $f(j)$ مشخص می‌شود به عکس با انتخاب یکی از اعضای S برای $f(i)$ و انتخاب یکی از چهار عنصر غیر از $f(i)$ و $f(i)-$ توسیع آن به تمامی L یک خودریختی H به دست می‌آید. بنابر این گروه خودریختی‌های L شامل ۲۴ عضو است. $\square$

تعریف. عضو $x \in L$ را یک عضو نرمال می‌نامیم هرگاه $xL = Lx$.

مثال: عناصر وارون‌پذیر و مرکزی L نرمال هستند، همچنین هر یک از عناصر $۱ + i$، $۱ + j$، $۱ - i$ و $۱ + j$، $۱.k$ نرمال‌اند.

پیش از بیان گزارهٔ بعد یادآوری می‌کنیم که جبر A روی هیأت F را مرکزی می‌نامیم هرگاه مرکز A برابر با $F۱ = \{a۱ : a \in F\}$ باشد. در اثبات گزارهٔ ۱۶ به قضیه اسکولم ـ نویتر نیاز است.

قضیه (اسکولم ـ نویتر): هر خودریختی یک جبر مرکزی متناهی ـ بعد که مرکز را ثابت نگاه دارد داخلی است. **اثبات.** [ر. ک۴]. □

گزارهٔ ۱۶. هر خودریختی L مرکزی است یعنی عضو نرمال $x \in L$ وجود دارد به طوری که برای $l \in L$، $f(l) = x^{-1}lx$.

اثبات. فرض کنیم $w \in H(Q)$، همان طور که در گزارهٔ ۱۲ دیدیم $l \in L$ و $z \in Z$ وجود دارند که $w = lz^{-1}$. قرار می‌دهیم $f(w) = f(l)z^{-1}$. بدین ترتیب می‌توانیم f را به یک خودریختی $H(Q)$ بسط دهیم که باز هم آن را با f نشان می‌دهیم. می‌دانیم $C\big(H(Q)\big) = Q$ و لذا f مرکز $H(Q)$ را عضو به عضو ثابت نگاه می‌دارد. بنابر قضیه اسکولم نویتر $u \in H(Q)$ وجود دارد که برای هر $w \in H(Q)$، $f(w) = u^{-1}wu$، امّا به ازای یک $n \in Z$ و یک $x \in L$ $x \neq \circ$ داریم $u = xn^{-1}$. از اینجا می‌توان نتیجه گرفت که برای هر $l \in L$، $f(l) = x^{-1}lx$. همچنین $f(L) = L$، یعنی $Lx = xL$ و x در L نرمال است. □

توجه. اگر I یک ایده‌آل راست (چپ) L باشد به سادگی دیده می‌شود که

$$I^* = \{x^* : x \in I\}$$

یک ایده‌آل چپ (راست) L است. بنابر این برای مطالعهٔ ایده‌آلهای یک طرفهٔ L کافی است فقط ایده‌آلهای راست یا ایده‌آلهای چپ L را مطالعه کنیم.

گزارهٔ ۱۷. هر ایده‌آل ناصفر و یک طرفهٔ L شامل یک عدد صحیح مثبت است.

اثبات. فرض کنیم I یک ایده‌آل ناصفر و راست L باشد و $x \in L$ $x \neq \circ$ پس I شامل $xx^* = N(x)$ می‌باشد که عددی است صحیح و مثبت. □

گزارهٔ ۱۸. فرض کنیم I یک ایده‌آل ناصفر راست L باشد، در این صورت گروه خارج‌قسمتی $\frac{L}{I}$ متناهی است.

اثبات. فرض کنیم $x \in I$ $x \neq \circ$، پس I شامل عدد صحیح $N(x)$ می‌باشد. اکنون $\frac{L}{I}$ روی حلقهٔ متناهی $\frac{z}{N(x)z}$ یک مدول متناهی تولید شده است و لذا متناهی است. □

نکته: توجّه می‌کنیم که هر کدام از گزاره‌های ۱۷ و ۱۸ در مورد حلقهٔ اعداد صحیح و نیز حلقهٔ اعداد گاوسی برقرارند. یادآوری می‌کنیم که حلقهٔ اعداد صحیح گاوسی مجموعهٔ تمام اعداد مختلط $a + bw$ هستند که در آن a و b اعداد صحیح‌اند. در این راستا می‌توان گزارهٔ زیر را بیان کرد که اثبات آن را به عهده خواننده می‌گذاریم.

گزارهٔ ۱۹. هر همریختی $f : L \to L$ یک خودریختی است. (همریختی حلقه‌ها ۱ را به ۱ می‌نگارد).

قضیه ۱. فرض کنیم M یک ایده‌آل دو طرفهٔ ماکسیمال L باشد. در این صورت یکی از دو حالت

زیر برقرار است:

آ) به ازای یک عدد اوّل و فرد p، $M = pL$.

ب) M تنها ایده‌آل ماکسیمال L است که $۲L \subseteq M$ و همچنین $M^۳ \subseteq ۲L$.

اثبات. بنابر گزارهٔ ۱۸، M شامل یک عدد صحیح مثبت $n \neq ۱$ می‌باشد. از آنجا که $\frac{L}{M}$ یک حلقهٔ ساده و لذا یک حلقهٔ اوّل است نتیجه می‌گیریم M شامل یک عدد اوّل مانند p می‌باشد، p تنها عدد اوّلی است که به M تعلق دارد، زیرا اگر $q \neq p$ عدد اوّل دیگری باشد، $pz + qz = z$ و لذا $pL + qL = L$ که تناقض است زیرا $pL \subseteq M$ و نیز $qL \subseteq M$. اکنون

$$H\left(\frac{z}{pz}\right) \cong \frac{L}{pL}$$

ابتدا فرض کنیم p عددی فرد است، بنابر گزارهٔ ۱۱

$$\frac{L}{pL} \cong M_۲\left(\frac{z}{pz}\right)$$

که از آن نتیجه می‌شود $\frac{L}{pL}$ حلقه‌ای ساده است، لذا pL یک ایده‌آل ماکسیمال L است و $M = pL$ بنابر این (آ) برقرار است. اگر $p = ۲$ از گزارهٔ ۱۲ نتیجه می‌شود که $\frac{M}{۲L}$ رادیکال اوّل $\frac{L}{۲L}$ است و $\left(\frac{M}{۲L}\right)^۳ = (۰)$. بنابر این M یگانه ایده‌آل L است که $۲L \subseteq M$ و همچنین $M^۳ \subseteq ۲L$. $\square$

با استفاده از مطالب بیان شده در قضیهٔ بعد عناصر نرمال L مشخص می‌شوند.

قضیه ۲. هر عنصر نرمال و ناصفر L حاصلضرب عناصری است که یا به مرکز L تعلق دارند یا وارون‌پذیرند یا اینکه نرم آنها برابر ۲ است.

اثبات. مجموعه‌ای را که هر عضو آن حاصلضرب عناصری است که به مرکز L تعلق دارند یا وارون‌پذیر و یا اینکه نرم آنها برابر ۲ است S می‌نامیم. ابتدا نشان می‌دهیم که هر عضو S نرمال است. اگر $x \in L$ و $N(x) = ۲$، پس $۲L \subseteq xL$ زیرا که $xx^* = N(x) = ۲$ و $۲ \in xL$، همچنین $۲L \subseteq Lx$. از آنجا که $\frac{L}{۲L}$ تعویض‌پذیر است نتیجه می‌گیریم که $xL = Lx$ یعنی x یک عضو نرمال L است. اکنون باید آشکار باشد که هر عضو S یک عضو نرمال است.

به عکس فرض کنیم $۰ \neq x \in L$ نرمال باشد. باید نشان دهیم $x \in S$. بدیهی است که اگر x وارون‌پذیر باشد، x نرمال است، پس فرض کنیم $xL \neq L$. همچنین می‌توان فرض کرد که تنها عدد صحیح n که $x \in nL$ برابر ۱ و ۱− است. از این رو برای هر عدد اوّل و فرد p، $x \notin pL$. از قضیهٔ ۱ نتیجه می‌شود که تنها ایده‌آل ماکسیمال L که شامل ایده‌آل دو طرفهٔ xL است ایده‌آلی است که شامل $۲L$ می‌باشد. بنابر گزارهٔ ۱۷، $\frac{L}{xL}$ متناهی است. می‌دانیم xL شامل حاصلضرب چند ایده‌آل ماکسیمال L است. بنابر این به ازای یک صحیح مثبت r، $M^r \subseteq xL$ لذا $۲^{۲r} \in xL$، از این رو

$xy = 2^r$ که $y \in L$. پس $N(x)N(y) = N(2^r) = 2^{2r}$ و بدین ترتیب $N(x)$ توانی از ۲ است. اگر $N(x) = 1$ یا $N(x) = 2$، آن گاه $x \in S$ و اثبات تمام است، پس فرض کنیم $N(x) = 2^t$ و $t > 2$. اگر $x = a + bi + cj + dk$، داریم $a^2 + b^2 + c^2 + d^2 = 2^t$. به لحاظ اینکه $t > 2$، $a^2 + b^2 + c^2 + d^2$ بر ۴ بخش‌پذیر است، امّا باقی‌ماندهٔ هر عدد طبیعی بر ۴ برحسب اینکه n زوج یا فرد باشد برابر با ۰ یا ۱ است، لذا تمام اعداد a^2 و b^2، c^2 و d^2 زوج یا تمام آنها فردند. به علّت اینکه $x \notin 2L$ تمام آنها فرد هستند. اکنون می‌توان نتیجه گرفت که $x \in L$ $\frac{1}{2}(1-i)$، یعنی $x \in L$ $(1+i)^{-1}$، یعنی $x \in (1+i)L$، پس به ازای یک $x' \in L$، $x = (1+i)x'$. چون $N(1+i) = 2$ می‌دانیم که $1 + i$ در L نرمال است، پس x' نیز در S است و $N(x') < (x)$. می‌توان فرض کرد که $x' \in S$ بنابر این $x \in S$ و اثبات تمام است. $\square$

گزارهٔ ۲۰. فرض کنیم K یک ایده‌آل ماکسیمال راست L باشد. در این صورت K ایده‌آل یگانه ماکسیمال L است که $2L \subseteq K$ یا اینکه به ازای یک عدد اوّل و فرد p، $pL \subseteq K$.

اثبات. بنابر گزارهٔ ۱۶، K شامل یک عدد صحیح $n \neq 1$ است. فرض کنیم $a, b \in Z$، امّا $a, b \notin Z$، به علّت اینکه K یک ایده‌آل ماکسیمال راست L است خواهیم داشت:

$$L = aL + k = bK + K$$

پس

$$L = a(bL + k) + K = ab + L$$

که نشان می‌دهد $ab \notin L$. از اینجا نتیجه می‌شود که دست کم یکی از عوامل اوّل n مانند q وجود دارد که $p \in L$. در واقع p یگانه عدد اوّل متعلق به L است. اگر $p = b$، $L/2L$ تعویض‌پذیر است و K یک ایده‌آل دو طرفه L و لذا یک ایده‌آل ماکسیمال K می‌باشد که $2L \subseteq K$.

گزارهٔ ۲۱. هر ایده‌آل ماکسیمال راست L مانند K که شامل یک عدد اوّل فرد p باشد یک ایده‌آل راست اصلی است. در واقع $K = xL$ که $x \in L$ و $N(x) = p$.

اثبات. فرض کنیم $a \in K$ امّا $a \notin pL$. دست کم یکی از a_iها بر p بخش‌پذیر نیست. برای هر i، عدد صحیح b_i وجود دارد که $-\frac{p-1}{2} \leqslant b_i \leqslant \frac{p-1}{2}$ و $a_i \equiv b_i \pmod p$ $(i = 0, 1, 2, 3)$ قرار می‌دهیم $b = b_0 + b_1 i + b_2 j + b_3 k$، در این صورت $b \in K$ و $N(b) \leqslant 4\big((p-1)/2\big)^2 < p^2$ همچنین $b \neq 0$ زیرا که $a \notin pL$. بنابر این می‌توان عنصر $x \in K$ $\neq 0$ را که $N(x)$ تا حد امکان کوچک باشد انتخاب کرد. می‌دانیم که $N(x) < p^2$. اعداد گویای c_0، c_1، c_2 و c_3 وجود دارند که $x^{-1}p = c_0 + c_1 i + c_2 j + c_3 k$، برای هر i $(i = 0, 1, 2, 3)$ فرض کنیم d_i عدد صحیحی باشد که تا حد امکان به c_i نزدیک است در این صورت $(c_i - d_i)^2 \leqslant \frac{1}{4}$. قرار می‌دهیم

اکنون $r \in K$ و $d \in L$ پس $r = p - xd$ و $d = (d_۰ + d_۱ i + d_۲) + d_۳ K$

$$\begin{aligned} N(x) &= N(p - xd) = N\big(x(x^{-1}p - d)\big) = N(x)(x^{-1}p - d) \\ &= N(x)N\big(c_۰ - d_۰ + (c_۱ - d_۱)i + (c_۲ - d_۲)j + (c_۳ - d_۳)k\big) \\ &\leqslant N(x)\big(\frac{۱}{۴} + \frac{۱}{۴} + \frac{۱}{۴} + \frac{۱}{۴}\big) = N(x) \end{aligned}$$

تساوی برقرار است اگر و تنها اگر برای هر i، $(c_i - d_i)^۲ = \frac{۱}{۴}$ بنابر انتخاب x داریم $r = ۰$ یا اینکه $N(r) = N(x)$.

حالت اوّل: اگر $r = ۰$، پس $p = xd$ و لذا

$$p^۲ = N(p) = N(xd) = N(x)N(d)$$

که $۰ < N(x) < p^۲$ بنابر این $N(x) = p$.

حالت دوّم: $N(r) = N(x)$ آنگاه برای هر $(c_i - d_i)^۲ = \frac{۱}{۴}$ یعنی $c_i = \frac{n_i}{۲}$ که در آن n_i یک عدد صحیح فرد است، پس

$$x^{-1}p = (n_۰ + n_۱ i + n_۲) + n_۳ K/۲$$

یعنی

$$۲p = x(n_۰ + n_۱ i + n_۳) + n_۳ K$$

با نرم گرفتن از طرفین نتیجه می‌شود:

$$۴p^۲ = N(x)(n_۰^۲ + n_۱^۲ + n_۲^۲ + n_۳^۲)$$

امّا n_iها فردند، لذا به ازای یک $z \in Z$، $n_۰^۲ + n_۱^۲ + n_۲^۲ + n_۳^۲ = ۴z$ از این رو $۴p^۲ = ۴N(x)z$ که از آن نتیجه می‌شود $N(x) = p$. بنابراین در هر حالت $N(x) = p$. پس $p = xx^* \in xL$ و از آن نتیجه می‌شود که $pL \subsetneq xL \subseteq K$. به لحاظ اینکه K/pL یک مدول ساده است نتیجه می‌گیریم که $xL = K$. $\square$

نتیجه (لاگرانژ): هر عدد صحیح مثبت n مجموع چهار مربع کامل است.
اثبات. کافی است نشان دهیم که به ازای یک $x \in L$، $N(x) = n$ چون N ضربی است کافی است حالتی را که در آن n یک عدد اوّل است در نظر بگیریم و گزارهٔ ۲۱ را به کار بریم. $\square$

۴. چهارگانهای هرویتس

یکی از زیرحلقه‌های چهارگانهای حقیقی که شامل چهارگانهای لیپشیتز می‌باشد حلقه‌ای است موسوم به چهارگانهای هرویتس که آن را با H نشان خواهیم داد. این حلقه بیشتر در نظریهٔ اعداد مطرح می‌شود و به تعبیری یک نوع حوزهٔ اقلیدسی تعویض‌ناپذیر است و در نتیجه هر ایده‌آل راست یا چپ آن اصلی است. [ر. ک۹]. در اینجا به شرح کوتاهی از این چهارگانها می‌پردازیم.

تعریف و نمادگذاری: قرار می‌دهیم

$H = \{x \in H(Q) : x = \frac{1}{2}(a+bi+cj+dk)$ ‏ a، b، c و d همگی زوج یا همگی فردند$\}$

گزارهٔ ۲۲. H یک زیرحلقهٔ $H(Q)$ و L یک زیرحلقهٔ H است.

اثبات. بدیهی است که H تحت عمل جمع بسته است. اگر قرار دهیم $w = \frac{1}{2}(1+i+j+k)$ به سادگی دیده می‌شود که H اجتماع L و $w + L = \{w + l : l \in L\}$ است. بسادگی می‌توان نشان داد هر یک از عناصر wi، jw، wj، Kw و wK عناصر H هستند. اکنون نتیجه می‌شود که H تحت عمل ضرب بسته است. تساوی

$$a + bi + cj + dk = \frac{1}{2}(2a + 2bi + 2cj + 2dk)$$

نشان می‌دهد که L یک زیرحلقهٔ H است. بدیهی است که H یک زیرحلقهٔ $H(Q)$ است. □

گزارهٔ ۲۳. مرکز حلقهٔ H برابر حلقهٔ اعداد صحیح است یعنی $C(H) = Z$.

اثبات. بدیهی است. □

گزارهٔ ۲۴. اگر $x \in H$ آن گاه $tr(x), N(x) \in Z$.

اثبات. فرض کنیم $x = \frac{1}{2}(a + bi + cj + dk)$ که در آن a، b، c و d همگی زوج یا همگی فردند. می‌دانیم که $tr(x) = a$ و $N(x) = a^2 + b^2 + c^2 + d^2/4$ در هر دو حالت $N(x) \in Z$. □

گزارهٔ ۲۵. اگر S یک زیرحلقهٔ $H(Q)$ باشد به طوری که $S \subseteq L$ و برای هر $x \in S$، $tr(x), N(x) \in Z$، در این صورت $S = L$ یا $S = HC$.

اثبات. بنابر آنچه در اثبات آمد به عنوان یک زیرگروه، اندیس H در L برابر ۲ است. فرض کنیم $x \in S$. پس $x = \frac{1}{2}(a + bi + cj + dk)$ که $a, b, c, d \in Q$. اکنون $tr(x) = a$ و $a \in Z$، امّا $i \in S$ نشان می‌دهد که $i \in S$ و $tr(xi) = b$. بنابر این $b \in Z$ به همین ترتیب $c, b \in Z$. همچنین $N(x) \in Z$ یعنی $(a^2 + b^2 + c^2 + d^2) \in 4Z$. بنابر این d, c, b, a همگی زوج یا همگی فردند. □

گزارهٔ ۲۶. گروه عناصر وارون‌پذیر H، ۲۴ عضو دارد.

اثبات. فرض کنیم $x \in H$. به سادگی دیده می‌شود که x در H وارون‌پذیر است اگر و تنها اگر $N(x) = ۱$. $x = \frac{۱}{۲}(a + bi + cj + dk)$ پس x در H وارون‌پذیر است اگر و تنها اگر $a^۲ + b^۲ + c^۲ + d^۲ = ۴$ بنابر این تمام اعداد صحیح $a^۲$، $b^۲$، $c^۲$ و $d^۲$ برابرند یا اینکه یکی از آنها ۴ و بقیه برابر صفرند. بدین ترتیب ۱۶ عنصر وارون‌پذیر به شکل $\frac{۱}{۲}(a + bi + cj + dk)$ به دست می‌آید که هر کدام از اعداد صحیحی a، b، c و d برابر با ۱ یا ۱− هستند. به این ۱۶ عنصر باید ۸ عنصر وارون‌پذیر L را نیز اضافه کرد. □

گزارهٔ ۲۷. هر ایده‌آل یک طرفهٔ H شامل یک عدد صحیح مثبت است.

اثبات. کافی است به گزارهٔ ۲۱ توجّه کنیم. □

نتیجه ۱: اگر I یک ایده‌آل ناصفر دو طرفهٔ H باشد آن گاه $\frac{H}{I}$ متناهی است.

اثبات: شبیه گزارهٔ ۱۷. □

نتیجه ۲: اگر M یک ایده‌آل ماکسیمال H باشد، آنگاه M شامل عدد اوّل یگانه است.

اثبات: ازگزارهٔ ۲۳ و اثبات قسمت اوّل قضیهٔ ۱ استفاده می‌کنیم. □

مراجع

[1] A. W. Chatters, "Matrices, Idealizers and Integer quaternions" J. of algebra, 150 (1992) 45-56.

[2] L. E. Dickson "Arithmetic of quaternions" proc. Lond. Math. Soc. 9(2), (1920) 225-232.

[3] K.R. Goodearl and R. Bwarfield. JR. An introduction to Non commutative Noetherian Rings. London Mathematical Society Student Texts 16. Cambridge University Press 1989.

[4] Pierce, R. S. Associative Algebra, Graduate texts in Mathematics, 88, Springer-Verlag 1982.

[۵] جان ب فرالی ـ نخستین درس در جبر مجرد جلد دوّم ترجمه دکتر مسعود فرزان.

[۶] منصور معتمدی ـ آشنایی با نظریه حلقه‌ها (چاپ دوّم) انتشارات دانشگاه شهید چمران اهواز.

[۷] منصور معتمدی ـ اعداد چهار برگی.فرهنگ و اندیشه ریاضی.شماره چهارم (۱۳۶۳) ۷۱ـ۶۰.

[۸] ا. ن. هرشتاین مباحثی در جبر ترجمه دکتر علی‌اکبر عالم‌زاده.

منصور معتمدی
دانشگاه شهید چمران اهواز، دانشکده علوم ریاضی و کامپیوتر
پست الکترونیک: motamedi_m@cua.ac.ir