درسنامه نظریه گروه، درس اول : آشنایی مقدماتی با گروه

وحیدکریمی پور– دانشکده فیزیک – دانشگاه صنعتی شریف

۳۱ فروردین ۱۳۹۵

۱ مقدمه

درزندگی روزمره اغلب از لفظ تقارن استفاده می کنیم. می گوییم که یک گل ، یک منظره، یک تابلوی نقاشی، طرح یک فرش، یک مجسمه، طرح کاشیکاری یک مسجد، و یا معماری یک ساختمان متقارن است و دیگری نیست. یا یکی تقارن بیشتری نسبت به دیگری دارد. درتوصیف دقیق طبیعت آنچنان که در فیزیک با آن روبرو هستیم، تقارن نقش مهم تر و بنیادی تری ایفا می کند و اثر آن تنها یک اثر زیبایی شناسی نیست. درسطوح مختلف طبیعت به تقارن های متعدد و متفاوت بر می خوریم. فضای سه بعدی مطلق یعنی فضای خالی دارای تقارن انتقالی و دورانی است یا به عبارت بهتر قوانین طبیعت نسبت به انتقال و دوران در فضای سه بعدی یکسان هستند. تکرار یک آزمایش دریک نقطه همان نتایجی را بدست می دهد که درنقطه دیگر و یا در جهت دیگر. این یک خاصیت بنیادی و مهم فضاست. فضا زمان چهاربعدی تقارن های بازهم بیشتر و عمیق تری دارد. قوانین طبیعت در دستگاه های لختی که نسبت به یکدیگر در حال حرکت مستقیم الخط یکنواخت هستند یکسان هستند وبه همین جهت با هیچ آزمایش فیزیکی و با مشاهده هیچ پدیده طبیعی نمی توانیم از حرکت دستگاه لختی که بر آن سوار هستیم آگاه شویم.

اطمینان ما به این تقارن ها چنان است که از آنها به عنوان محکی برای سنجیدن درستی قوانین جدیدی که می خواهیم برای پدیده های ناشناخته وضع کنیم استفاده می کنیم و آن دسته از قوانین را که با این تقارن ها سازگار نباشند درهمان مرحله

اول کنار می گذاریم. تقارن های قوانین فیزیکی تنها خاصیت های انتزاعی نیستند بلکه این تقارن ها باعث می شوند که اشیای فیزیکی ای که لاجرم تحت تسلط این قوانین هستند به نوبه خود تقارن هایی پیداکنند. یک ستاره که از تراکم گازهای درون کهکشانی بوجود می آید دراثر تقارن دورانی، خود به شکل یک کره درمی آید و نه مثلا به صورت یک بیضی گون. حالت پایه اتم هیدروژن نیز یک شکل کروی دارد و شکل دیگر اربیتال ها نیز تقارن های مخصوص به خود دارند. از پیوند اتم ها مولکول هایی با تقارن های مختلف بوجود می آید. تقارن انتقالی باعث می شود که بلور ها از تکرار سلول های یکسانی درفضا ایجاد شوند. قیودی که ناشی از سازگاری تقارن های انتقالی برای یک بلور و تقارن های سلول واحد آن است، باعث می شود که تنها بلورهایی با شکل های معین درطبیعت یافت شوند. این تقارن نهایتاً به ابعاد ماکروسکوپی و به دنیای گل ها و پروانه ها راه می یابد.

درسطح عمیق تر و میکروسکوپی تر تقارن های دیگری وجود دارند که براستی شگفت انگیزند. این تقارن ها مثل تقارن های یک گلبرگ و یا یک شکل هندسی ساده ملموس نیستند. بااین وجود به همان معنادقیق هستند و اثرات فیزیکی مهم دارند. به عنوان مثال نیروی هسته ای قوی نسبت به تعویض پروتون و نوترون کاملاً متقارن است. این تقارن یک تقارن گسسته است که باگروه Z_2 توصیف می شود. می توانیم بگوییم که نیروی هسته ای قوی تنها روی یک هستک [1] اثر می کند واین هستک می تواند دریکی از دو حالت که آن را پروتون و یا نوترون می گوییم قرار گیرد درست مثل اسپین الکترون که می تواند دریکی از دو حالت بالا یا پایین قرارگیرد. به همین علت این تقارن را تقارن ایزواسپین می گوییم.

اما ازانجا که مکانیک کوانتومی به ما آموخته است که حالات فیزیکی یک ذره با بردارهای یک فضای خطی متناظر هستند می توانیم بگوییم که یک هستک می تواند دریک حالت دلخواه $|\phi\rangle = a|proton\rangle + b|neutron\rangle$ قرارگیرد. درنتیجه حالت یک هستک که با یک بردار دو تایی $|\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ توصیف می شود می تواند تحت تبدیلات گسترده تری مثل تبدیلات $U(2)$ [2] قرار بگیرد بدون اینکه نیروی هسته ای قوی متوجه این تغییرات بشود. درنتیجه تقارن ایزواسپین با گروه $U(2)$ توصیف می شود. دراینجا برای اولین بار با تقارنی مواجه می شویم که تقارن فضا یا فضازمان ملموس نیست بلکه تقارن یک فضای مجرد و درونی مربوط به ذرات موسوم به فضای ایزواسپین است . این تقارن تنها تقارنی نیست که دردنیای ذرات وجود دارد و فضای

---

[1] Nucleon

[2] این گروه ، گروه تبدیلات ماتریس های یکانی با بعد ۲ است.

ایزواسپین نیز تنها فضای درونی مربوط به ذرات نیست. دردنیای میکروسکوپی باتقارن هایی مواجه می شویم مثل تقارن رنگ و یا تقارن پیمانه ای . توصیف دقیق این تقارن هانیاز به حداقلی از دانش ذرات بنیادی دارد و درمحدوده این درس نیست.

نظریه گروه شاخه ای از ریاضیات است که به توصیف تقارن به صورت دقیق می پردازد. با استفاده از نظریه گروه ما می توانیم توصیف خیلی دقیق و مشخصی از تقارن بدست آوریم. درکلی ترین تعریف معنای تقارن آن است که بعضی از خواص یک دستگاه تحت اثر مجموعه معینی از اعمال تغییر نمی کند. بعنوان مثال انبساط همسانگرد کره جغرافیایی نسبت مساحت بین کشور ها را روی کره دست نخورده باقی می گذارد و حال آنکه مساحت مطلق آنها را تغییر می دهد. هم چنین دراثر این انبساط تمام زوایا و نسبت های طولی ناوردا باقی می مانند. منظور از ذکر این مثال آن است که تاکید کنیم عمل تقارنی لازم نیست تمامی یک شی را ناوردا باقی بگذارد بلکه تنها کافی است که خاصیت هایی در شی ناوردا باقی بمانند اگر چه درگفتار ها معمولا ذکری از خاصیت های مورد نظر نمی رود و با تسامح از تقارن خود شی صحبت می شود.

اگر شی را با O وعمل انجام شده را با g نمایش دهیم آنگاه شی بعد از عمل را با $O' = g(O)$ نشان می دهیم. هرگاه خاصیت مورد نظر را با P نشان دهیم آنگاه بنا برتعریف بالا داریم :

$$P(O') = P(O) \qquad \longrightarrow \qquad P(g(O)) = P(O) \tag{۱}$$

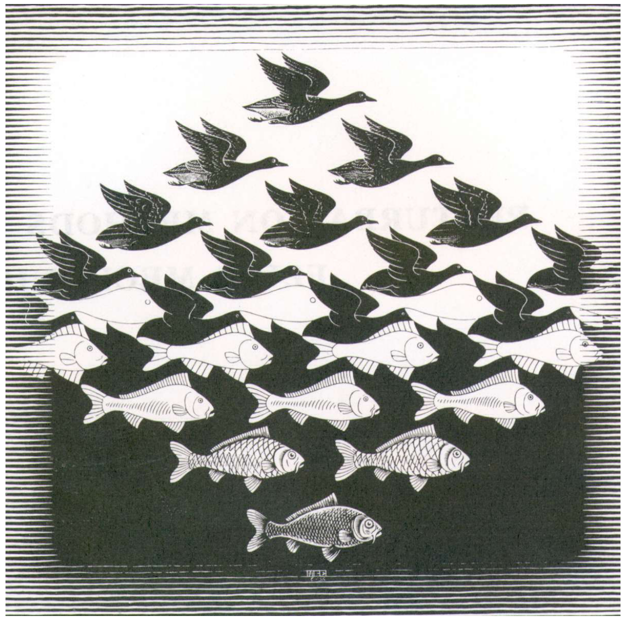
دراین حالت g را یک عمل تقارنی می نامیم. حال فرض کنید که g_1 و g_2 دو عمل تقارنی باشند آنگاه خواهیم داشت:

$$O' = g_1(O), \quad O'' = g_2(O') \longrightarrow O'' = g_2(g_1(O)) =: (g_2g_1)(O) \tag{۲}$$

می خواهیم ببینیم که آیا g_2g_1 نیز یک عمل تقارنی هست یا نه ؟ منظور از g_2g_1 این است نخست عمل g_1 و سپس عمل g_2 را انجام دهیم. این کار را می توان ضرب دو عمل g_1 و g_2 نامید. برای این کار تست می کنیم که آیارابطه $P(O") = P(O)$ برقراراست یا نه؟

$$P(O") = P((g_2g_1)(O)) = P(g_2(g_1(O)) = P(g_1(O)) = P(O) \tag{۳}$$

بنابراین g_2g_1 نیز یک عمل تقارنی است.



شکل ۱: تابلوی نقاشی اثر موریس اشر Maurice Escher

به این ترتیب متوجه می شویم که مجموعه عمل های تقارنی یک شی نسبت به این عمل ضرب بسته است. هم چنین می دانیم که اگر هیچ کاری روی شی انجام ندهیم خاصیت مورد نظر آن دست نخورده باقی می ماند. اگر این عمل را با e نشان دهیم به این معناست که $e(O)=O$ و واضح است که

$$eg = ge = g.$$

و نهایتاً اگر عمل g^{-1} را به عنوان عملی تعریف کنیم که عمل g را خنثی می کند یعنی

$$g^{-1}g = g^{-1}g = e,$$

آنگاه به این معناست که اگر g یک عمل تقارنی باشد، آنگاه g^{-1} نیز یک عمل تقارنی است.

مجموعه ی این اعمال همراه با عمل ضرب ساختاری را تعریف می کند که در ریاضیات به آن گروه می گویند. در این درس ما نخست به چند مفهوم ابتدایی در ریاضیات می پردازیم و سپس به معرفی مفهوم گروه و مثال هایی از آن می پردازیم.

دراین درس نخست به تعریف میدان و سپس به تعریف فضای برداری روی یک میدان و نهایتاً به تعریف گروه می پردازیم. پس از مرور خواص مقدماتی از یک گروه و اثبات چند قضیه ساده در این باره، به ارایه مثال هایی از گروه ها می پردازیم. نخست لازم است که دو ساختار مهم ریاضی یعنی میدان و فضای برداری را معرفی کنیم. این دو ساختار برای معرفی گروه لازم

۲ میدان

معروف ترین مثالی که از میدان [۳] می شناسیم میدان اعداد حقیقی است که همواره با آن سروکار داریم. این میدان مجموعه‌ای است از اعداد با دو عمل جمع و ضرب که دارای خواص معینی هستند. به طور کلی میدان به هر مجموعه‌ای از اشیا گفته می شود که بین آنها دو عمل موسوم به عمل جمع و ضرب تعریف شده باشد که این دو عمل همان خواص اشنای اعداد را داشته باشند. به طور دقیق تر میدان به شکل زیر تعریف می شود:

تعریف: یک دستگاهِ $\{F,+,\cdot\}$ شاملِ یک مجموعه‌ی F به همراه دو نگاشتِ جابجایی و شرکت پذیرِ $+ : F\times F \longrightarrow F$ و $\cdot : F\times F \longrightarrow F$ یک میدان [۴] خوانده می شود هرگاه خواص زیر برقرار باشند:

$$\begin{aligned} A1: &\quad \exists \quad 0\in F \quad | \quad \forall \alpha\in F, \quad 0+\alpha=\alpha+0=\alpha, \\ A2: &\quad \forall \quad \alpha\in F, \quad \exists \quad (-\alpha)\in F, \quad | \quad \alpha+(-\alpha)=(-\alpha)+\alpha=0, \end{aligned} \tag{۴}$$

$$\begin{aligned} M1: &\quad \exists 1 \quad \in F \quad | \quad \forall \alpha\in F, \quad 1\cdot\alpha=\alpha\cdot 1=\alpha, \\ M2: &\quad \forall \quad \alpha\neq 0\in F \quad \exists\,(\alpha^{-1}) \quad | \quad \alpha\cdot(\alpha^{-1})=(\alpha^{-1})=1, \end{aligned} \tag{۵}$$

و

$$AM: \quad \forall \quad \alpha,\beta,\gamma\in F, \quad \alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma. \tag{۶}$$

[۳] Field

[۴] Field

دربسیاری اوقات برای سادگی بجای نمادِ $\alpha \cdot \beta$ از نمادِ $\alpha\beta$ استفاده می کنیم. هرگاه خاصیت جابجایی برای ضرب در یک میدان برقرارنباشد آن را یک میدان ناجابجایی [5] می گوییم.

۱.۲ مثال هایی از میدان ها

- **مثال :** مجموعه های اعداد گویا Q، اعداد حقیقی R و اعداد مختلط C به همراه جمع و ضرب متعارفی که از آن ها می شناسیم مثال های مهمی از میدان هستند.

- **مثال :** میدان ناجابجاییِ کواترنیون ها[6] تعمیمی از اعداد مختلط است که به ترتیب زیر تعریف می شود: سه نماد i, j, k درنظرمی گیریم که درخاصیت های زیر صدق می کنند:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \tag{۷}$$

مجموعه کواترنیون ها H به شکل زیرتعریف می شود:

$$H := \{q | q = q_0 + q_1 i + q_2 j + q_3 k, q_0, q_1, q_2, q_3 \in R\}. \tag{۸}$$

دو کواترنیون p و qبه شکل زیر با هم جمع می شوند:

$$p + q := (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k. \tag{۹}$$

هم چنین ضرب این دو کواترنیون نیز با توجه به رابطه‌ی ؟؟ صورت می گیرد. این ضرب شرکت پذیراست ولی جابجایی نیست.

---

[5] Non-Commutative Field

[6] Quaternion

مزدوج یک کواترنیون q با $\overline{q}$ نشان داده می شود و برابراست با:

$$\overline{q} := q_0 - q_1 i - q_2 j - q_3 k. \tag{۱۰}$$

حاصلضرب یک کواترنیون q درمزدوج آن برابراست با:

$$q\overline{q} = q_0^2 + q_1^2 + q_2^2 + q_3^2. \tag{۱۱}$$

اندازه یک کواترنیون q با $|q|$ نشان داده می شود وبرابراست با:

$$|q| := \sqrt{q\overline{q}}. \tag{۱۲}$$

هرکواترنیون غیرصفر یک وارون ضربی دارد که برابراست با:

$$q^{-1} := \frac{\overline{q}}{|q|^2}. \tag{۱۳}$$

- **مثال:** میدان $GF(p)$: یا میدان Z_p.

به ازای هر عددِ اول مثل p ، مجموعه‌ی

$$Z_p = \{0, 1, 2, \cdots p - 1\} \tag{۱۴}$$

که درآن جمع و ضرب به سنجِ p صورت می گیرند، یک میدان تشکیل می دهد. دراین میدان عضو خنثی جمع و ضرب به ترتیب 0 و 1 هستند. دقت کنید که اول بودن عددِ p لازم است. این میدان را با $GF(p)$ هم نمایش می دهند که به معنای میدان متناهی گالوا [۷] با مرتبه ی p است. **مرتبه یک میدان** [۸] مرتبه یک میدان تعداد اعضای آن میدان است. به عنوان مثال مرتبه میدان Z_p برابر است با p.

[۷] Finite Galois Field

[۸] Order of a Field

۲.۲ طبقه بندی میدان ها

بنابر یک قضیه مهم در جبر، نشان داده می شود که مرتبه یک میدان همواره عبارت است از یک عدد اول مثل p یا توانی از یک عدد اول مثلِ p^n. این مطالب را بهتراست در یک قضیه که اثبات آن خارج از موضوع این درس است بیان کنیم.

- **قضیه‌ی طبقه بندی میدان ها:**

الف: مرتبه یک میدان همواره عددی است به صورت p^n که درآن p یک عدد اول و n عددی مثبت یا صفراست.

ب: به ازای هرعددِ p^n حتماً یک میدان با آن مرتبه وجود دارد.

ج: هر دو میدانی که یک مرتبه داشته باشند حتماً با هم یکسان هستند.

بنابر قضیه فوق کافی است هر میدان را با مرتبه‌ی آن نشان دهیم. به همین مناسبت معمولاً از نمادِ $GF(p^n)$ برای نشان دادن یک میدان استفاده می شود. علامتِ GF مخففِ $Galois\ Field$ یعنی میدان گالوا است.

در حالتی که n برابر با یک است $GF(p)$ همان Z_p است. بنابراین داریم

$$GF(p) = Z_p = \{0, 1, 2, \cdots p-1\}.$$

برای وقتی که n بزرگ تر از ۱ است، میدان گالوا به ترتیب زیر ساخته می شود: مجموعه تمام چندجمله ای های از یک متغیر x که ضرایب آن از Z_p انتخاب می شوند را با $P_{Z_p}[x]$ نشان می دهیم. سپس در این فضا یک چند جمله ای کاهش ناپذیر[۹] از مرتبه n انتخاب می کنیم. می بایست همه ضرب ها را به سنج یک چندجمله ای کاهش ناپذیر چند جمله ای کاهش ناپذیر روی Z_p چندجمله ایست که روی این میدان هیچ گونه ریشه ای ندارد. به عنوان مثال چندجمله ای

[۹] Irreducible polynomial

x^2+1 روی میدان اعداد حقیقی کاهش ناپذیر است ولی روی میدان اعداد مختلط کاهش پذیر است و به همین دلیل می توان آن را به صورت حاصلضرب دو چندجمله ای کوچکتر یعنی $(x+i)(x-i)$ نوشت یا به اصطلاح کاهش داد. ریشه اصطلاح کاهش پذیری نیز از همین جا می آید. به عنوان یک مثال دیگر چندجمله ای $1+x+x^2$ روی میدان Z_2 کاهش ناپذیر است، زیرا هیچ ریشه ای در این میدان ندارد. قضیه ای که گالوا ثابت کرده است این است که هر گاه تمام ضرب ها و جمع ها را در مجموعه تمام چندجمله ای های $F_{Z_p}[x]$ به سنج یک چندجمله ای کاهش ناپذیر درجه n انجام دهیم، آنگاه مجموعه حاصل یک مجموعه متناهی است و یک میدان از مرتبه p^n است. این میدان را با $GF(p^n)$ نمایش می دهیم. نکته مهم این است که میدان های حاصل از چندجمله ای های کاهش ناپذیر که همگی یک درجه دارند با یکدیگر معادل اند. دقت کنید که هیچ میدانی با مرتبه مثلاً ۶ یا ۱۲ وجود ندارد، زیرا این دوعدد توانی از یک عدد اول نیستند.

- مثال: اگر $n=2$ و $p=2$ چندجمله ای کاهش ناپذیر را به صورت $1+x+x^2$ می گیریم . دراین صورت خواهیم داشت:

$$GF(2^2)=\{0,1,x,1+x\} \tag{۱۵}$$

- تمرین: جدول جمع و ضرب را برای GF_4 تشکیل دهید و نشان دهد که GF_4 واقعا یک میدان است.

- تمرین: میدان $GF(8)$ را مشخص کنید.

- تمرین: میدان $GF(9)$ را مشخص کنید.

۳ فضای برداری

در این قسمت تنها به یاداوری تعریف یک فضای برداری می پردازیم. هدف این بخش تنها یادآوری تعریف اساسی است. خواننده علاقمند برای مطالعه بیشتر می بایست به یک کتاب جبر خطی مراجعه کند.

■ **تعریف:** مجموعه V را یک فضای برداری روی میدان غ F می گوییم هرگاه دو عمل زیر تعریف شده

$$+\ : V\times V\longrightarrow V \qquad \text{و} \qquad .: F\times V\longrightarrow V \tag{۱۶}$$

دارای خاصیت های زیر باشند:

$$\begin{aligned}
A1: &\quad x+y=y+x\\
A2: &\quad (x+y)+z=x+(y+z)\\
A3: &\quad \exists 0\in V\ | \qquad 0+x=x\\
A4: &\quad \forall x\in V \qquad \exists -x\in V\ | \qquad -x+x=0,
\end{aligned}$$

$$\begin{aligned}
M1: &\quad \alpha(x+y)=\alpha x+\alpha y\\
M2: &\quad (\alpha+\beta)x=\alpha x+\beta x\\
M1: &\quad \alpha(\beta x)=(\alpha\beta)x\\
M1: &\quad 1x=x.
\end{aligned} \tag{۱۷}$$

به ازای هر دو بردار u و v و هر عدد $\alpha\in F$، $u+v$ جمع دو بردار و $\alpha\ u$ ضرب اسکالر α در بردار v نامیده می شود. بسته به این که F میدان اعداد حقیقی R یامیدان اعداد مختلط C باشد، فضای برداری V را فضای برداری حقیقی یا مختلط می گوییم.

■ **مثال ها:** مجموعه های زیر هرکدام یک فضای برداری هستند. در اغلب این مثال ها تعریف جمع + و ضرب اسکالر بدیهی است و خواننده می تواند خود تعریف طبیعی مورد نظر را پیشنهاد کند.

۱ ـ R^n یا مجموعه n تایی های مرتب حقیقی یک فضای برداری حقیقی است.

۲ ـ C^n یامجموعه n تایی مرتب مختلط، یک فضای برداری مختلط است.

۳ ـ $M_{m\times n}(F)$ یامجموعه ماتریس های $m \times n$ که درایه های آن عناصریک میدان F هستند، نیز یک فضای برداری است.

۴ ـ F^n یا مجموعه n تایی های مرتب که درایه های آن عناصر یک میدانِ F هستند نیز یک فضای برداری تشکیل می دهد. هرگاه مرتبه‌ی F محدود و برابر با q باشد، آنگاه تعداد اعضای فضای برداری F^n نیز محدود و برابر با q^n خواهد شد. دلیل این امر هم ساده است زیرا هر عضو $v \in F^n$ به صورتِ $v = (f_1, f_2, \cdots f_n)$ است و هر درایه‌ی f_i می تواند q مقدار مختلف را اختیار کند. به عنوان مثال بردار های Z_2^2 عبارتند از:

$$Z_2^2 = \{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}\} \tag{۱۸}$$

۴ گروه

■ **تعریف:** یک گروه عبارت است از یک مجموعه G بهمراه یک عمل دوتایی $* : G \times G \longrightarrow G$ و یک عنصر $e \in G$ به نحوی که خاصیت های زیررا داشته باشند:

الف : شرکت پذیری :

$$\forall a, b, c \in G \quad (a * b) * c = a * (b * c) \tag{۱۹}$$

ب : عضو خنثی

$$\forall a \in G \quad a * e = e * a = a \tag{۲۰}$$

ج : عضو وارون

$$\forall a \in G \quad \exists a^{-1} \mid a^{-1} * a = a * a^{-1} = e \tag{۲۱}$$

ازاین به بعد از نوشتن نماد $*$ صرف نظر می کنیم و ضرب دوعنصر مثل a و b را به صورت ab می نویسیم.

هرگاه که خاصیت اضافه $ab = ba$ درگروه وجود داشته باشد، گروه آبلی [۱۰] خوانده می شود و در غیر این صورت گروه غیرآبلی [۱۱] خوانده می شود.

قضیه:

الف: عضو خنثی گروه یکتاست.

ب : وارون یک عضو گروه یکتاست.

ج : به ازای هر $g \in G$ ، $(g^{-1})^{-1} = g$.

د : به ازای هر $a, b \in G$، $(ab)^{-1} = b^{-1}a^{-1}$.

---

[۱۰] Abellian Group

[۱۱] Non-Abellian Group

اثبات:

الف: فرض کنید که e و e' هردو عضو خنثی باشند. دراین صورت خواهیم داشت :

$$e' = ee' = e \tag{۲۲}$$

که درتساوی اول از خنثی بودن e و درتساوی دوم از خنثی بودن e' استفاده کرده ایم.

ب: فرض کنید که x و x' هردو وارون عضو a باشند. دراین صورت داریم

$$ax = e, \quad ya = e \tag{۲۳}$$

اگر تساوی اول رااز چپ درy ضرب کنیم خواهیم داشت:

$$y(ax) = ye, \longrightarrow \quad (ya)x = y, \quad ex = y, \quad x = y. \tag{۲۴}$$

اثبات قسمت های ج و د آسان است.

قضیه: اگر $ab = ac$ آنگاه $b = c$.

اثبات: طرفین را از چپ در وارون a ضرب می کنیم و از شرکت پذیری استفاده می کنیم. این قاعده، قاعده حذف نامیده می شود و مشابه آن برای حذف از راست نیز وجود دارد.

برای یک گروه می توان جدول ضربی به همان معنای متعارف که می شناسیم تشکیل داد. قواعد حذف نشان می دهند که در جدول ضرب گروه درهیچ سطریا ستونی نمی بایست عضو تکراری وجود داشته باشد.

تمرین جدول ضرب گروه های با ۲ تا ۵ عضو را تشکیل دهید و آنهاراطبقه بندی کنید.

تعریف: مرتبه یک گروه تعداد اعضای یک گروه مثل G را مرتبه آن گروه می نامند و با نمادِ $|G|$ نشان می دهند. گروهی که مرتبه آن یک عددِ متناهی است گروه متناهی [12] نامیده می شود. در فصل های ابتدایی این درس بیشتر به گروه های متناهی می پردازیم ولی در بقیه فصل ها به مطالعه گروه های نامتناهی بخصوص گروه های پیوسته می پردازیم. در ادامه این فصل با چند مثال از گروه ها آشنا می شویم. در این جا نمی خواهیم خواص این گروه ها را به تفصیل بررسی کنیم و تنها به تعاریف کلی آنها بسنده می کنیم.

---

۵ گروه تبدیلات وارون پذیر روی یک مجموعه

هرگاه S یک مجموعه دلخواه و $Aut(S)$ مجموعه تمام نگاشت های وارون پذیر روی S باشند، آنگاه $Aut(S)$ با عمل ترکیب نگاشت ها یک گروه تشکیل می دهد. این گروه گروه خودسانی های [13] های S خوانده می شود. اگر $f,\ g \in Aut(S)$ دو عضو از این گروه باشند ضرب آنها به شکل زیر تعریف می شود:

$$(fg)(x) := f(g(x)), \qquad \forall x \in S \tag{۲۵}$$

از آنجا که ترکیب دو نگاشت وارون پذیر یک نگاشت وارون پذیر است، درمی یابیم که $fg \in Aut(S)$. هم چنین نگاشت همانی با تعریف $x \in S \qquad e(x) = x,$ عضو خنثی این گروه را تشکیل می دهد. می توان با افزودن قید یا قیدهایی به این توابع زیر مجموعه هایی از توابع وارون پذیر روی S را بدست آورد که خود نیز گروه باشند.

- **مثال:** هرگاه S یک مجموعه متناهی با n عضو باشد، از آنجا که هرنگاشت وارون پذیر چیزی جز یک جایگشت بین این اعضا نیست، $Aut(S)$ عبارت خواهد بود از گروه جایگشت های بین n شی که با S_n نشان داده می شود.

---

[12] Finite Group

[13] Automorphisms

۶ مثال هایی از گروه های متناهی

- گروه دوره ای : [۱۴] گروه دوره ای Z_n به صورت زیر تعریف می شود:

$$Z_n := \{0, 1, 2, \cdots n-1\}$$

که در آن جمع به سنجه n انجام می شود. این گروه یک گروه دوری ای نامیده می شود که مرتبه آن نیز برابر است با n.

- گروه دوره ای : [۱۵] گروه دوره ای Z_p که در آن p یک عدد اول است، به صورت زیر تعریف می شود:

$$Z_p := \{1, 2, \cdots p-1\}$$

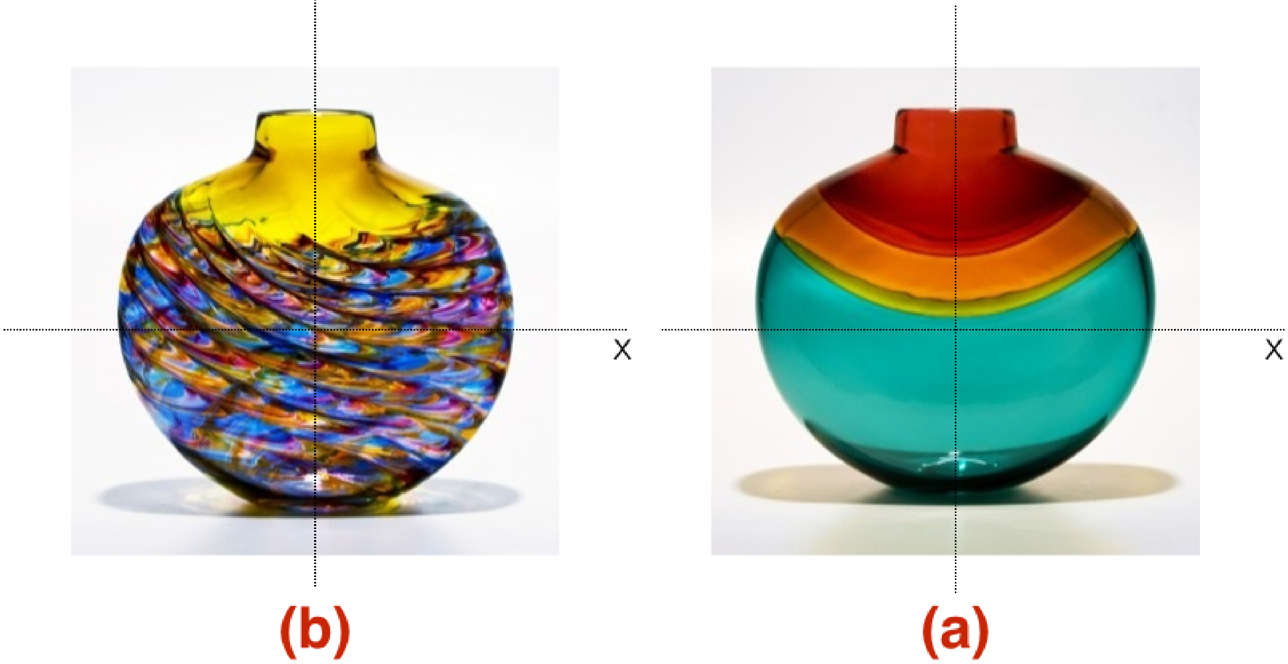
که در آن ضرب به سنجه p انجام می شود. این گروه یک گروه دوری ای نامیده می شود که مرتبه آن نیز برابر است با p.

- **مثال :** هرگاه عددِ n اول نباشد آنگاه مجموعه‌ی $Z_n^* = \{x | 0 < x < n, gcd(x, n) = 1\}$ با عمل ضرب تشکیل یک گروه می دهد. در اینجا منظور از gcd بزرگترین مقسوم علیه مشترک است. در واقع این مجموعه در بردارنده ی تمام اعدادی است که از n کوچکترند و نسبت به آن اول هستند.

- مثال: شکل (؟؟) را در نظر بگیرید. بر روی این شکل دو عمل زیر را می توان انجام داد: یکی عمل e که هیچ کاری نمی کند و عمل دیگر π_y که شکل را حول محور π_y منعکس می کند. شکل تحت این دو عمل به خودش تبدیل می شود. بنابراین می گوییم که گروه تقارنی این شی گروه $Z_2 = \{e, \pi_y\}$ است . دقت کنید که یک شکل ممکن است تحت یک گروه از اعمال متقارن باشد یا نباشد. شکل (؟؟)

[۱۴] Cyclic Group

[۱۵] Cyclic Group



شکل ۲: گلدان سمت راست تحت گروه Z_2 متقارن است. اما گلدان سمت چپ تحت این گروه (لااقل تحت اعمالی که روی گلدان اول انجام می دهیم) تقارن ندارد. البته در نگاه دقیق تر متوجه می شویم که هر دو گلدان تقارن های بیشتر و البته متفاوتی دارند.

- تمرین : مجموعه اعمال زیر را در نظر بگیرید. $G = \{e, \pi_x, \pi_y, R\}$ اعمال π_x و π_y تعاریف مشابهی دارند (رجوع کنید به مثال قبل) و عمل R چیزی نیست جز انعکاس نسبت به مبدا مختصات. این مجموعه اعمال یک گروه تشکیل می دهند. جدول ضرب این گروه را تشکیل دهید. شکل دوبعدی ای را رسم کنید که تحت این گروه تقارن دارد.

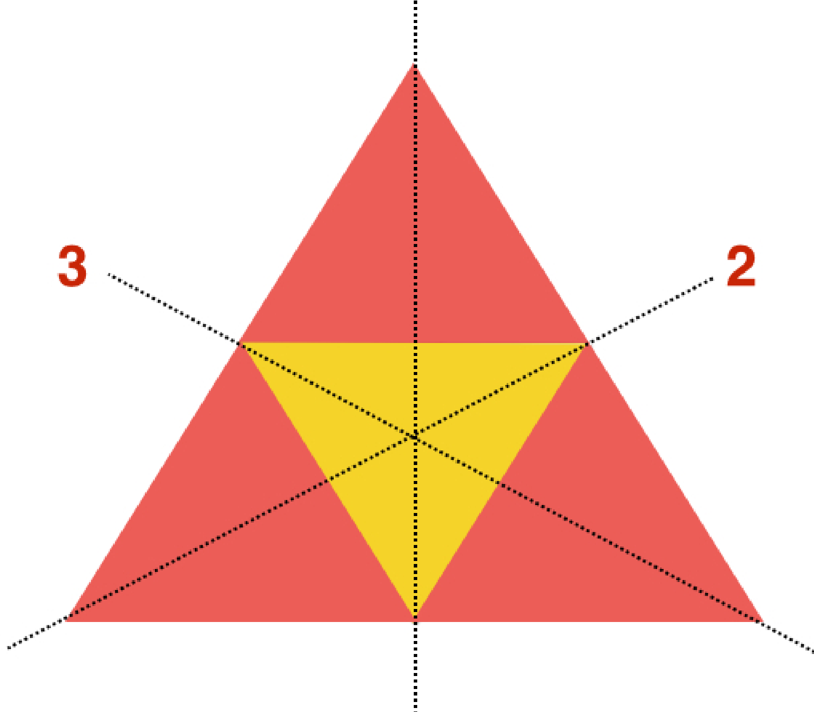
- تمرین: با توجه به شکل () مجموعه اعمال زیر را در نظر می گیریم: $\Delta = \{e,\ R,\ R^2,\ \pi_1,\ \pi_2,\ \pi_3\}$ این اعمال کارهای زیر را انجام می دهند:

$$\begin{aligned} R &= \text{Clockwise rotation by}120^\circ, \\ \pi_i &= I\text{Inversion with respect to the axis}i. \end{aligned} \tag{۲۶}$$

الف: ثابت کنید که مجموعه این اعمال تشکیل یک گروه می دهند.

ب: شکلی را رسم کنید که تحت این گروه متقارن باشد. شکلی را رسم کنید که تحت این گروه متقارن نباشد.

پ: شکلی را رسم کنید که تحت یکی از مجموعه گروه های $G_i = \{e, \pi_i\}$ متقارن باشد، اما تحت گروه کامل G تقارن نداشته باشد.



شکل ۳: شکلی که تحت مجموعه اعمال Δ تقارن دارد.

پ: شکلی را رسم کنید که تحت گروه $Z_3 := \{e,\ R, R^2\}$ متقارن باشد اما تحت کل گروه G متقارن نباشد.

ت: آیا می توانید شکلی رسم کنید که تحت مجموعه اعمال $\{\pi_1,\ \pi_2,\ \pi_3\}$ متقارن باشد اما تحت کل گروه G متقارن نباشد؟

■ **مثال: گروه پاوولی:** این گروه در نظریه تصحیح خطاهای کوانتومی در رایانش کوانتومی اهمیت دارد. ماتریس های دو بعدی مربعی موسوم به ماتریس های پاوولی را درنظر بگیرید:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{۲۷}$$

این ماتریس ها دررابطه زیر صدق می کنند:

$$\sigma_k\sigma_l = i\epsilon_{klm}\sigma_m, \tag{۲۸}$$

که درآن ϵ_{klm} تانسورکاملاً پادمتقارن است و $\epsilon_{123} = 1$. با توجه به ا ین رابطه می توان نشان داد که مجموعه زیر یک گروه غیرآبلی با مرتبه 8 تشکیل می دهد.

$$G_0 = \{\pm I, \pm\sigma_1, \pm\sigma_2, \pm i\sigma_3\}. \qquad (۲۹)$$

هم چنین گروه زیر یگ گروه غیرآبلی بامرتبه 16 است.

$$G_1 = \{\pm I, \pm\sigma_1, \pm\sigma_2, \pm\sigma_3, \pm iI, \pm i\sigma_1, \pm i\sigma_2, \pm i\sigma_3\} \qquad (۳۰)$$

- تمرین: می دانیم که $Z_2 = \{0,1\}$ یک میدان است. این میدان را با $GF(2)$ نشان می دهند. هرگاه مجموعه دوتایی مرتب را در نظر بگیریم این مجموعه روی این میدان تشکیل یک فضای برداری می دهد. این فضای برداری را با $V := (Z_2)^2 = GF(2)^2$ نشان می دهیم. اعضای این فضای برداری متناهی هستند و عبارتند از:

$$V = \{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}\} \qquad (۳۱)$$

مجموعه تبدیلات خطی وارون پذیر روی این فضا را بنویسید. این مجموعه تشکیل یک گروه می دهد.

- تمرین: میدان $GF(3)$ و فضای برداری $V = GF(3)^2$ را در نظر بگیرید. گروه تبدیلات وارون پذیر روی این فضای برداری را بنویسید. مرتبه این گروه چند است؟

- تمرین: میدان $GF(4)$ و فضای برداری $V = GF(4)^2$ را در نظر بگیرید. گروه تبدیلات وارون پذیر روی این فضای برداری را بنویسید. مرتبه این گروه چند است؟

می دانیم که گروه S_n یعنی گروه جایگشت های n شی مثالی از یک گروه متناهی است. درواقع این گروه چیزی نیست جز گروه خودسانی های یک مجموعه‌ی n عضوی. ولی به دلیلی که بعداً خواهیم دید این گروه از اهمیت ویژه‌ای برخوردار است که مطالعه مستقل آن را ضروری می سازد. به همین دلیل است که آن را در یک بخش جداگانه مورد مطالعه قرار می دهیم.

۱.۶ گروه جایگشت

یک مجموعه از n شی که آنهارا بابرچسب های $1,2,\cdots n$ مشخص می کنیم، درنظر می گیریم. یک جایگشت از این مجموعه یک نگاشت یک به یک و پوشا از این مجموعه روی خودش است. مجموعه تمام این جایگشت هارا با S_n نمایش می دهیم. می توان یک جایگشت $\alpha \in S_n$ را به شکل زیر نشان داد:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}. \tag{۳۲}$$

اگر $\alpha, \beta \in S_n$ دو جایگشت باشند، ضرب آن دو به صورت زیرتعریف می شود:

$$(\alpha\beta)(k) := \alpha(\beta(k)), \tag{۳۳}$$

که درواقع به این معناست که $\alpha\beta$ همان ترکیب دو نگاشت α و β است. ازآنجا که ترکیب دو نگاشت یک به یک و پوشا خودیک نگاشت یک به یک و پوشاست، پس $\alpha\beta$ نیز یک جایگشت است . درنتیجه S_n تحت این ضرب بسته است. هم چنین عضو واحد دراین مجموعه وجود دارد که همان نگاشت همانی است:

$$e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}. \tag{۳۴}$$

ازآنجایی که وارون یک نگاشت یک به یک و پوشا خود یک نگاشت یک به یک و پوشاست ، وارون هرعضو $\alpha \in S_n$، نیز عضوی در S_n است که آن را با α^{-1} نشان می دهیم.

تعریف: یک عضو α از گروه جایگشت S_n، یک دوره یا سیکل[۱۶] k تایی خوانده می شود هرگاه این عضو k شی از مجموعه‌ی n تایی را در یک سیکل جابجا کند. بهترین راه برای فهم این تعریف توجه به چند مثال است. عضو $\alpha \in S_3$ به شکل زیر یک سیکل سه تایی است:

[۱۶] Cycle

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad (۳۵)$$

به عبارت دیگر

$$\alpha(1) = 2, \quad \alpha(2) = 3, \quad \alpha(3) = 1. \qquad (۳۶)$$

هم چنین عضو $\beta \in S_5$ یک سیکل چهارتایی است:

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \qquad (۳۷)$$

به عبارت دیگر

$$\beta(1) = 3, \quad \beta(3) = 4, \quad \beta(4) = 5, \quad \beta(5) = 1. \qquad (۳۸)$$

دقت کنید که β نقطه‌ی ۲ را ثابت نگاه می دارد.

تعریف: یک جابجایی [۱۷] یک سیکل دوتایی است. به عنوان مثال در S_3، $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ یک جابجایی است. می توان ثابت کرد که هر عضو از گروه جایگشت را می توان به صورت حاصل ضربی از سیکل های دوتایی نوشت.

■ گروه S_3.

ساده ترین گروه جایگشت S_2 است که دو عضو دارد و آبلی است. ساده ترین گروه جایگشت غیرآبلی S_3 است که ۶ عضو دارد:

$$S_3 = \{e, \alpha, \beta, \gamma, \delta, \eta\}. \qquad (۳۹)$$

[۱۷] Transposition

این اعضا عبارتند از:

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \gamma &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \eta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \end{aligned} \quad (۴۰)$$

خواننده می تواند براحتی جدول ضرب این گروه راتشکیل دهد. قبل ازآنکه گروه جایگشت n عضو را مطالعه کنیم بهتر است که مفهوم مولد های یک گروه را مرور کنیم.

---

۷ مولد ها ی یک گروه و رابطه بین آنها

گروه اعداد صحیح با عمل جمع یعنی Z را در نظر می گیریم. عناصر این گروه عبارتند از:

$$Z = \{\cdots - 2,\ -1,\ 0,\ 1,\ 2,\ \cdots\}. \quad (۴۱)$$

تمام عناصر این گروه را می توان از جمع عنصر 1 یا وارون آن بدست آورد به این معنا که داریم:

$$2 = 1 + 1, \qquad 3 = 1 + 1 + 1, \qquad -4 = -1 - 1 - 1 - 1, \cdots. \quad (۴۲)$$

می گوییم که گروه بالا توسط یک عنصر یعنی 1 تولید شده است و عنصر 1 مولد [۱۸] آن است. یک گروه می تواند بیش از یک مولد داشته باشد. در حالت کلی تعریف زیر را داریم:

- تعریف: گروه آزاد [۱۹] به گروهی گفته می شود که توسط یک مجموعه متناهی مولد مثل $\{a, b, \cdots c\}$ بدون اینکه هیچ رابطه ای بین آنها قائل شویم بوجود می آید. اعضای این گروه حاصلضرب تمام توان های صحیح این عناصرند. بنابراین عناصری مثل $\cdots a^{n_1}b^{n_2}c^{n_3}a^{m_1}b^{m_2}c^{m_3}\cdots$ عضو این گروه هستند.

[۱۸] Generator

[۱۹] Free Group

طبیعی است که گروه های آزاد بی نهایت عضو دارند. اما می توان روی مولدهای یک گروه آزاد قیدها یا رابطه هایی اعمال کرد. به عنوان مثال هرگاه در گروه $\mathcal{Z}$ قید $0 = \underbrace{1+1+\cdots 1}_{n}$ را اعمال کنیم، گروهی که بوجود می آید همان گروه Z_n است.
به طور کلی هرگاه گروهی مثل G توسط یک مجموعه مولد مثل $\{a, b, \cdots c\}$ و یک مجموعه رابطه مثل $R_1, R_2, \cdots R_k$ تولید شود می نویسیم:

$$G = \frac{\langle a, b, \cdots c\rangle}{R_1, R_2, \cdots R_k}. \tag{۴۳}$$

در ادامه با مثال های دیگری از مولدهای یک گروه و رابطه های بین آنها آشنا می شویم.

براحتی می توان تحقیق کرد که همه عناصر گروه S_3 از ضرب دو عنصر α و β بدست می آیند. یعنی

$$S_3 = \{e, \alpha, \beta, \alpha\beta\alpha, \beta\alpha, \alpha\beta\}. \tag{۴۴}$$

دراین صورت می گوییم که α و β مولد های گروه S_3 هستند، یعنی تمام عناصراین گروه از ضرب توان های دلخواه از این دو عضو بدست می آیند یابه اصطلاح تولید می شوند. البته باید دقت کرد که بین این دو عنصر رابطه های زیر برقرارند:

$$\alpha^2 = e, \qquad \beta^2 = e, \qquad \alpha\beta\alpha = \beta\alpha\beta, \tag{۴۵}$$

که درنتیجه آن هرنوع حاصلضرب قابل تصور ازتوان های مولد ها چیزی بجزهمان ۶ عضو گروه S_3 تولید نمی کند.
هم چنین خواننده می تواند نشان دهد که گروه G_0 از عناصر $\{I, \sigma_1, \sigma_2\}$ تولید می شود و گروه G_1 از عناصر $\{I, \sigma_1, \sigma_2, \sigma_3\}$ تولید می شود. دقت کنیدکه انتخاب مولدهایکتانیست. به عنوان مثال برای گروه G_1 می توان مولدهای $\{I, iI, \sigma_1, \sigma_2\}$ را نیز انتخاب کرد.

■ **تعریف:** دریک گروه G زیر مجموعه ای ازعناصرمثل $S = \{g_1, g_2, \cdots g_n\}$ را مولد های گروه می گوییم هرگاه هر عضو گروه را بتوان به صورت حاصلضربی از توان های مثبت و منفی اعضای S نوشت . به عنوان مثال گروه $\{Z, +\}$ توسط $S = \{1\}$ تولید می شود. هم چنین گروه $\{nZ, +\}$ توسط $S = \{n\}$ تولید می شود. دراین حالت ها می نویسیم $G = \langle S\rangle$ و یا $G = \langle g_1, g_2, \cdots g_n\rangle$.

دربعضی موارد بین مولدهارابطه هایی وجود دارد مثل رابطه هایی که درمورد مولد های گروه S_3 دیدیم. اگر این رابطه هارا مجموعاً با R نشان دهیم، دراین صورت می نویسیم $G = \langle S \rangle / R$. به عنوان مثال داریم

$$S_3 = \langle \alpha, \beta \rangle / \{ \alpha^2 = \beta^2 = e, \alpha\beta\alpha = \beta\alpha\beta \}. \tag{۴۶}$$

■ تعریف : اگر یک گروه G تنها توسط یک عضو تولید شود، آن گروه یک گروه دوری $Cyclic\ \ Group$ خوانده می شود. دریک چنین گروهی می توان همه اعضا را به صورت توان های متوالی از یک عضو نوشت. مثالی از یک گروه دوری نامتناهی $Infinite\ \ Cyclic\ \ Group$ عبارت است از:

$$G = \{ e, a, a^2, a^3, a^4, \cdots \} \tag{۴۷}$$

یک گروه دوری متناهی شکل زیر رادارد:

$$G = \{ e, a, a^2, \cdots, a^{n-1} \}, \tag{۴۸}$$

که درآن $a^n = e$.

هرگروه دوری مسلماً آبلی است، اما هرگروه آبلی الزاماً دوری نیست مثل گروهی باجدول ضرب زیر:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(49)

۱.۷ مولد های گروه جایگشت

مولدهای گروه جایگشت S_n، عبارتنداز:

$$S = \{ \alpha_1, \alpha_2, \cdots \alpha_{n-1} \}, \tag{۵۰}$$

که درآن α_i جایگشتی است که تنها جای i و $i+1$ را عوض می کند. به عبارت دیگر:

$$\alpha_i = \begin{pmatrix} 1 & 2 & 3 & \cdots & i & i+1 & \cdots & n \\ 1 & 2 & 3 & \cdots & i+1 & i & \cdots & n \end{pmatrix}. \qquad (۵۱)$$

می توان نشان داد که تمام اعضای S_n از این جایگشت ها تولید می شوند. براحتی می توان دید که بین این مولد ها رابطه های زیر وجود دارد.

$$\begin{aligned} \alpha_i^2 &= e, \\ \alpha_i\alpha_{i+1}\alpha_i &= \alpha_{i+1}\alpha_i\alpha_{i+1}, \\ \alpha_i\alpha_j &= \alpha_j\alpha_i \quad if \quad |i-j| > 1. \end{aligned} \qquad (۵۲)$$

۸ مثالهایی از گروه های نامتناهی

مجموعه ی اعداد صحیح تحت عمل جمع که آن را با $\mathcal{Z}$ نشان می دهیم، مجموعه اعداد گویا تحت عمل جمع که آن را با $\mathcal{Q}$ نشان می دهیم، نمونه هایی از گروه های نامتناهی هستند. نمونه های دیگری از مجموعه های اعداد که تحت عمل ضرب گروه های نامتناهی تشکیل می دهند این ها هستند: $\mathcal{Q}-\{0\}$ یا $\mathcal{R}-\{0\}$ که اولی مجموعه اعداد گویا و دومی مجموعه اعداد حقیقی است که در هر دو مورد عدد صفر را از آنها کنار گذاشته ایم. به عنوان مثال دیگر می توانیم به مجموعه توابع وارون پذیر روی هر مجموعه ای از اعداد نگاه کنیم. به عنوان مثال $F[0,1]$ مجموعه توابع وارون پذیر روی فاصله ی $[0,1]$ است. این مجموعه دارای بی نهایت عضو است و یک گروه تشکیل می دهد. همه این گروه ها به طور طبیعی و بدیهی در فیزیک اهمیت پیدا می کنند. به خصوص گروه های ماتریسی که دسته بسیار مهمی از گروه ها هستند در فیزیک اهمیت و کاربرد دارند و در ادامه این درس به معرفی آنها خواهیم پرداخت. اما اکنون توجه خود را معطوف به یک گروه موسوم به گروه گیسو می کنیم تا نشان دهیم چگونه تغییری در یک رابطه بین مولدهای یک گروه می تواند نتایج و معنای بسیار مهم داشته باشد.

۹ گروه گیسو

یک تعمیم جالب و عمیق از گروه جایگشت، گروه گیسو یا گروه $Braid$ است. این گروه اهمیت زیادی درمطالعه توپولوژی گره ها دارد. فرض کنید که دریک صفحه n نقطه ی $p_1, p_2, \cdots, p_n$ قرارگرفته اند. صفحه ای به موازات این صفحه باهمان نقاط درروی آن درنظربگیرید. حال یک مجموعه منحنی درنظر بگیرید که نقاط پایینی را به نقاط بالایی وصل می کنند. این منحنی ها نباید یکدیگررا قطع کنند ولی می توانند هرشکل دلخواهی داشته باشند ویابه دوریکدیگر پیچ وتاب بخورند. ضمناً هردو مجموعه منحنی که به طور پیوسته به یکدیگر قابل تبدیل باشند باهم یکسان درنظر گرفته می شوند. اصطلاحاً می گوییم که فقط کلاس هموتوپی منحنی هاست که برای ما اهمیت دارند و نه خود منحنی ها. هرمجموعه منحنی یا کلاس هموتوپی آن یک عضو گروه گیسوخواهد بود. به طور دقیق ترداریم:

$$\gamma : [0,1] \longrightarrow R^2 \times [0,1], |\gamma(t) = (\gamma_1(t), \gamma_2(t), \cdots, \gamma_n(t)) \qquad (۵۳)$$

که درآن $\gamma_1, \gamma_2, \cdots \gamma_n$ هامنحنی های پیوسته غیرمتقاطع هستند و عبارت بالا نشان دهنده این است که پارامتراین منحنی ها یعنی t بین صفر و یک تغییرمی کند. این منحنی ها از نقاط پایینی شروع می شوند، به عبارت دیگر

$$\gamma_1(0) = p_1, \quad \gamma_2(0) = p_2, \cdots, \gamma_n(0) = p_n, \qquad (۵۴)$$

و انتهای منحنی ها می توانند جایگشتی از نقاط ابتدایی آنها باشند،به عبارت دیگر نقاط $(\gamma_1(1), \gamma_2(1), \cdots, \gamma_n(1))$ جایگشتی از نقاط $(\gamma_1(0), \gamma_2(0), \cdots, \gamma_n(0))$ است.

هرعضو گروه گیسو یک مجموعه منحنی یا کلاس هموتوپی آن است. اعضای گروه را با حروف $\alpha, \beta, \gamma, \cdots$ نمایش می دهیم. حال باید برای این عناصر یک ضرب تعریف کنیم. نخست ضرب دو منحنی منفرد را به ترتیب زیر تعریف می کنیم. فرض کنید که $a : [0,1] \longrightarrow R^3$ و $b : [0,1] \longrightarrow R^3$ دومنحنی باشند. دراین صورت ضربِ ab به لحاظ شهودی یعنی این که اول منحنی a را طی کنیم و بعد منحنی b را. حال می خواهیم ضرب دوعضو گروه گیسو یعنی $\alpha = (\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n)$ و $\beta = (\beta_1, \beta_2, \beta_3, \cdots, \beta_n)$ را تعریف کنیم. برای این کار منحنی های α را ابتدا طی می کنیم و سپس منحنی های β را طی می کنیم و کلاس هموتوپی منحنی های حاصل را در نظر می گیریم. به عبارت دقیق تر می توانیم بگوییم که اگر منحنی های α نقاط $(1, 2, \cdots n)$ را به نقاط $(\pi(1), \pi(2), \cdots \pi(n))$ بنگارند که در آن π یک جایگشت است آنگاه حاصل ضرب $\alpha\beta$ عبارت خواهد بود از: [۲۰]

[۲۰] در ویراست قبلی این درسنامه یک اشتباه بنیادی در این رابطه وجود داشت . از خانم سبا امین الرعایا دانشجوی دانشگاه امیر کبیر که این اشتباه را به من

$$\alpha\beta = (\alpha_1\beta_{\pi(1)}, \alpha_2\beta_{\pi(2)}, \cdots, \alpha_n\beta_{\pi(n)}). \quad (۵۵)$$

اگر $a : [0,1] \longrightarrow R^3$ یک منحنی باشد،منحنی ای که درجهت برعکس طی می شود به شکل زیرتعریف می شود:

$$a^{-1}(t) := a(1-t). \quad (۵۶)$$

حال می توان وارون یک عضو گروه گیسو را به شکل زیر تعریف می کنیم که البته درهمه موارد منظورما کلاس هموتوپی منحنی هاست.

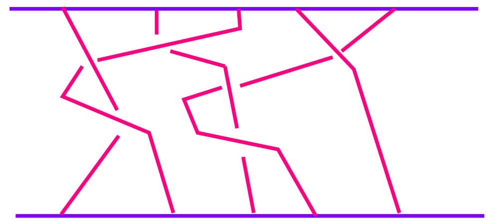
$$\alpha^{-1} = (\alpha_1^{-1}, \alpha_2^{-1}, \cdots, \alpha_n^{-1}). \quad (۵۷)$$

این ملاحظات تعریف گروه گیسو را کامل می کند. ضمناً عنصرواحد کلاس هموتوپی دسته منحنی ای است که بدون هیچ نوع پیچ وتابی نقاط پایینی را به نقاط بالایی وصل می کند.

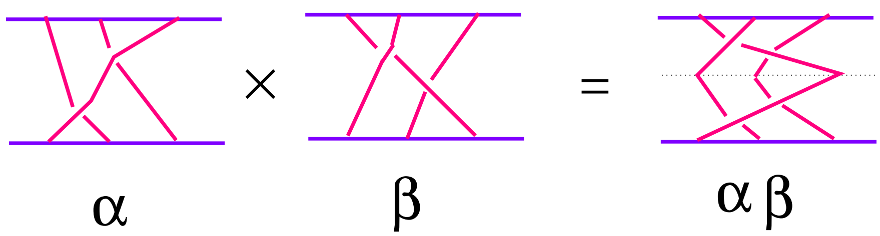
شکل (??) یک عضو ازگروه گیسوی 5 نقطه ای یعنی B_5 را نشان می دهد.

شکل های ?? و ?? نیز نشان می دهند که ضرب دو عضو از گروه گیسو و معکوس یک عضو از گروه گیسو چگونه تعریف می شوند.

تذکر دادند تشکر می کنم. ضمنا املای اسم کوچک ایشان به تایید خودشان رسیده است که از ملکه «سبا» در قصه های قرآن گرفته شده و با باد «صبا» فرق دارد.



شکل ۴: یک عضو از گروه گیسوی B_5.



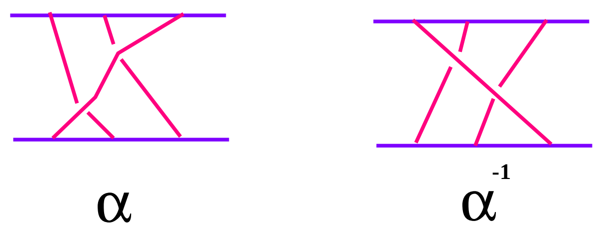
شکل ۵: ضرب دو عضو از گروه B_3.

۱.۹ مولد های گروه گیسو

گروه گیسوی n نقطه ای دارای $n-1$ مولد است . این مولدهارا با $\sigma_1, \sigma_2, \sigma_3, \cdots, \sigma_{n-1}$ نشان می دهیم. شکل ؟؟ مولد σ_3 و وارون آن را درگروه B_7 نشان می دهد. بین این مولدها رابطه های زیربرقرارند:

$$\begin{aligned} &\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \\ &\sigma_i\sigma_j = \sigma_j\sigma_i \qquad if \quad |i-j| > 1. \end{aligned} \tag{۵۸}$$

برخلاف گروه S_n دیگر رابطه $\sigma_i{}^2 = 1$ برقرارنیست. همین موضوع گروه گیسو را به یک گروه بی نهایت عضوی تبدیل می کند. روابط ؟؟ حاوی یک هم ارزی توپولوژیک بین گیسوهاست که خواننده خود می تواند صحت آنها را تحقیق کند. اهمیت



شکل ۶: وارون یک عضو از گروه B_3.

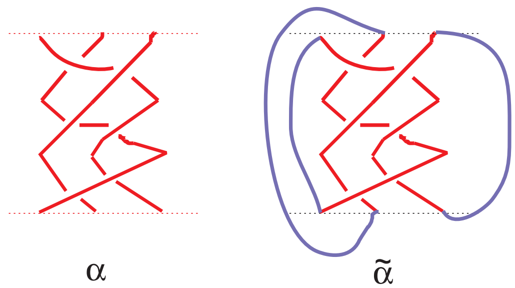
شکل ۷: مولد σ_3 درگروه B_7(شکل دست راست) و وارون آن .

گروه گیسو در ارتباطی است که با نظریه گره ها [۲۱] دارد.

نظریه گره به مطالعه کلاس های هم ارزی توپولوژیک گره ها در فضای سه بعدی می پردازد. دو گره K_1 و K_2 را هم ارز می گوییم هرگاه بتوان بدون پاره کردن یکی را به دیگری تبدیل کرد. گره بدیهی [۲۲] به گرهی گفته می شود که در فضای ۳ بعدی مثل یک دایره نشسته است. می توان گره های بسیار پیچیده‌ای را در فضا تصور کرد که براحتی نتوان در باره هم ارز بودن یا نبودن آنها قضاوت کرد. نظریه گره مفاهیم و روش هایی را پیشنهاد می کند که بوسیله آنها بتوانیم این کار را انجام دهیم.

[۲۱] Knot Theory

[۲۲] Trivial Knot



شکل ۸: یک عضو از گروه گیسوی B_3 به نام α و بستار آن که یک گره به نام $\tilde{\alpha}$ است.

یک قضیه مهم در نظریه گره بیان می کند که هر گره چیزی نیست جز بستار یک عضو از گروه گیسو. مفهوم بستار و محتوی این قضیه در شکل ؟؟ نشان داده شده است.

اهمیت نظریه گره به نوبه خود در آن است که فهم گره های هم ارز و یا طبقه بندی گره های هم ارز گام مهمی در راه طبقه بندی خمینه‌های توپولوژیک سه بعدی است که یک مسئله مهم در ریاضیات به شمار می رود. اهمیت دیگر گروه گیسو در مطالعه فیزیک بعضی از سیستم های دو بعدی است. حالت های برانگیخته ی این سیستم ها را می توان به صورت مجموعه ای از شبه ذرات توصیف کرد. هرگاه n شبه ذره در یک حالت وجود داشته باشد و این شبه ذرات که به آنها انیون [۲۳] می گوییم حرکت کنند جهان خط آنها یک عضو از گروه گیسو را بوجود می آورد. توصیف دقیق مکانیک کوانتومی این شبه ذرات نیازمند دانستن خواص گروه گیسو و نمایش های آن دارد. بحث بیشتر در این مورد خارج از محدوده ی این درس است.

---

[۲۳] Anyon

۱۰ مثالهایی از گروه های پیوسته

در درسهای آینده با تفصیل بیشتر گروه های پیوسته [۲۴] یا گروه های توپولوژیک [۲۵] را بررسی خواهیم کرد. در این جا تنها به ذکر نمونه های ساده ای از این گروه ها اکتفا می کنیم. تنها کافی است بدانیم که گروه پیوسته گروهی است که اگر چه تعداد عناصرش بی نهایت است اما این تعداد شمارش پذیر نیست. به عنوان مثال گروه توابع وارون پذیر روی فاصله $[0,1] \in R$ یک گروه پیوسته است.

۱.۱۰ گروه تبدیلات خطی

یک دسته وسیع و بسیار مهم از گروه ها به صورت تبدیلات خطی روی یک فضای برداری تعریف می شوند. درواقع این گروه ها زیر گروه هایی از گروه های خودسانی روی فضاهای برداری هستند که درآن نگاشت های مورد نظر دارای خاصیت اضافی بودن خطی بودن هستند. از این به بعد برای تطابق با نمادگزاری های رایج مجموعه مورد نظر را بابه جای S با V نمایش می دهیم که روی ساختار خطی آن تاکید کرده کنیم. علامت V چنانکه می دانیم معمولاً برای نشان دادن یک فضای برداری به کار می رود. مجموعه‌ی تبدیل های خطی وارون پذیر روی یک فضای برداری V را با $GL(V)$ نشان می دهیم و آن را گروه تبدیلات عمومی خطی روی V [۲۶] می خوانیم. عمومی بودن این تبدیلات به این معناست که هیچ قید دیگری به جز خطی بودن ندارند.

هرگاه T و T' دو عضو از $GL(V)$ باشند، آنگاه ضرب دو عضو هم چنان به صورت ترکیب دو نگاشت تعریف می شود یعنی $TT'(x) = T(T'(x))$. با انتخاب یک پایه برای فضای برداری V می توانیم هر نگاشت خطی را با ماتریس آن نشان دهیم که در این صورت ترکیب دو نگاشتِ T و T' متناظر با ضرب ماتریس های وابسته به این دو نگاشت خواهد شد. بنابراین اگر فضای برداری V n بعدی باشد و این فضا روی میدانِ F تعریف شده باشد، ماتریس وابسته به نگاشتِ T که آن را با $\hat{T}$ نشان

---

[۲۴] Continuous Group

[۲۵] Topological Groups

[۲۶] General Linear Transformations on V

می دهیم یک ماتریس مربعی با درایه های متعلق به F خواهد شد. دراین شرایط مجموعه ماتریس های مربعی و n بعدیِ $\hat{T}$ یک گروه تشکیل می دهند که آن را با نمادِ $GL_n(F)$ نمایش می دهیم. این گروه با همان گروه اول یعنی $GL(V)$ یکسان است. البته مفهوم شهودی یکسانی را بعداً به صورت دقیق تر بیان خواهیم کرد. دقت کنید که هرگاه F یک میدان متناهی با مرتبه‌ی q باشد $GL_n(F)$ نیز یک گروه متناهی خواهد بود که مرتبه‌ی آن از q^{n^2} کمتراست.

تمرین: اگر $F = Z_2$ باشد، عناصر گروه $GL_2(F)$ را بنویسید.

تمرین: اگر $F = Z_3$ باشد، عناصر گروه $GL_2(F)$ را بنویسید.

مثال: هرگاه فضای برداری V یک فضای برداری حقیقی n بعدی باشد، گروه تبدیلات خطی روی آن یک گروه نامتناهی است که آن را با $GL_n(R)$ نشان می دهیم. هرعنصر این گروه یک ماتریس وارون پذیر $n \times n$ با درایه های حقیقی است. به عنوان مثال داریم

$$GL_2(R) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad | \quad a,\ b,\ c,\ d,\ \in R, \quad ad - bc \neq 0\}. \qquad (۵۹)$$

این گروه گروه تبدیلات روی صفحه دو بعدی است. هر عضو از این گروه یک تبدیل خطی است که بردار $\begin{pmatrix} x \\ y \end{pmatrix}$ را به بردار $\begin{pmatrix} x' \\ y' \end{pmatrix}$ می نگارد که در آن

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}. \qquad (۶۰)$$

مثال: زیر مجموعه ای از ماتریس های $GL_2(R)$ که متعامد باشند یعنی در شرطِ $AA^T = I$ صدق کنند، گروه ماتریس

های متعامد دو بعدی حقیقی را تشکیل می دهند که با نمادِ $O_2(R)$ نشان داده می شود. به عبارت دیگر

$$O_2(R) = \{A \in GL_2(R), \quad | \quad AA^T = I\}. \tag{۶۱}$$

از این که $AA^T = I$ می توان نتیجه گرفت که $det(A) = \pm 1$. زیر مجموعه‌ای از این ماتریس ها که دترمینان آنها برابر با یک است خود تشکیل یک گروه می دهند. این گروه با نماد $SO_2(R)$ نمایش داده می شود. خواننده براحتی می تواند نشان دهد که هرماتریسِ A متعلق به گروه $SO_2(R)$ را می توان به شکل زیر نمایش داد:

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \qquad \theta \in [0, \ 2\pi]. \tag{۶۲}$$

گروه $SO_2(R)$ را گروه دوران های صفحه دوبعدی نیز می نامند، زیرا هر عضو از این گروه یک دوران به شکل زیر در صفحه دو بعدی القا می کند:

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{۶۳}$$

مثال: مجموعه ماتریس های سه بعدی و حقیقی متعامد تشکیل یک گروه می دهند. این گروه با نماد $O_3(R)$ نمایش داده می شود که درآن R به معنای حقیقی بودن درایه های ماتریس و O به معنای متعامد بودن این ماتریس هاست. به زبان دیگر داریم

$$O_3(R) = \{A \in GL_3(R), \quad | \quad AA^T = I\}. \tag{۶۴}$$

از این که $AA^T = I$ می توان نتیجه گرفت که $det(A) = \pm 1$. زیر مجموعه‌ای از این ماتریس ها که دترمینان آنها برابر با یک است خود تشکیل یک گروه می دهند. این گروه با نماد $SO_3(R)$ نمایش داده می شود. در درسهای آینده نشان می دهیم که هر عضو از این گروه یک دوران در فضای سه بعدی القا می کند. به این معنی که هرگاه r یک بردار در فضای سه بعدی باشد، انگاه به ازای هر $A \in SO_3(R)$ بردارِ $r' = Ar$ دوران یافته‌ی بردار r حول یک محور و به اندازه یک زاویه مشخص است. محور دوران و زاویه دوران را می توان از روی ماتریس A بدست آورد. این موضوع را در درس های آینده یاد خواهیم گرفت.

مثال: هرگاه فضای برداری V یک فضای برداری مختلط n بعدی باشد، گروه تبدیلات خطی روی آن یک گروه نامتناهی است که آن را با $GL_n(C)$ نشان می دهیم. هرعنصر این گروه یک ماتریس وارون پذیر $n\times n$ با درایه های مختلط است. به عنوان مثال داریم

$$GL_2(C)=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad | \quad a,\ b,\ c,\ d,\ \in C, \quad ad-bc\neq 0\}. \tag{۶۵}$$

این گروه، گروه تبدیلات خطی روی یک فضای مختلط دو بعدی است.

مثال: زیر مجموعه ای از ماتریس های $GL_n(C)$ که یکانی باشند یعنی در شرطِ $UU^\dagger=I$ صدق کنند، گروه ماتریس های یکانی n را تشکیل می دهند که با نمادِ $U_n(C)$ نشان داده می شود. به عبارت دیگر

$$U_n(C)=\{U\in GL_n(C), \quad | \quad UU^\dagger=I\}. \tag{۶۶}$$

از این که $UU^\dagger=I$ می توان نتیجه گرفت که $|det(U)|=1$ یا $det(U)=e^{i\phi}$. زیر مجموعه‌ای از این ماتریس ها که دترمینان آنها برابر با یک است خود تشکیل یک گروه می دهند. این گروه با نماد $SU_n(C)$ نمایش داده می شود. خواننده می تواند نشان دهد که هر عضو از گروهِ $SU_2(C)$ را می توان به شکل زیر نمایش داد:

$$U\in SU_2(C)\longrightarrow U=\{\begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}, \qquad |a|^2+|b|^2=1. \tag{۶۷}$$

هم چنین واضح است که هر عضو از گروه $U_1(C)$ چیزی نیست جز یک عدد که به صورت فاز خالص است یعنی

$$U_1(C)=\{e^{i\phi}, \qquad {}^{\phi\in[0,2\pi]}\}. \tag{۶۸}$$

۱۱ حاصلضرب دکارتی دو گروه

هرگاه دو گروه A و B داشته باشیم می توانیم گروه بزرگتری بسازیم که حاصلضرب دکارتی دو گروه نامیده می شود. بنابرتعریف داریم:

$$A \times B = \{(a,b)|a \in A, \quad b \in B\}. \qquad (۶۹)$$

ضرب دراین گروه به شکل زیر تعریف می شود:

$$(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2). \qquad (۷۰)$$

عضو خنثی این گروه عبارت است از (e,e') که درآن e عضو خنثی A و e' عضو خنثی B است. هم چنین داریم

$$(a,b)^{-1} = (a^{-1}, b^{-1}). \qquad (۷۱)$$

به این ترتیب می توان ازگروه های $Z_n \times Z_m$ یا $GL_2(R) \times GL_3(R)$ سخن گفت.

۱۲ ضمیمه

این فصل را با یک ضمیمه در مورد اعداد به پایان می بریم.

قضیه: اگر یک عدد اول p حاصلضرب دوعدد a و b را بشمرد ، آنگاه p یا a را می شمرد و یا b را.

اثبات: هرگاه ab را به عامل های اول آن تجزیه کنیم عدد p که خود اول است یاجزء عامل های a است و یا جزء عامل های b، بنابراین یا a را می شمارد و یا b را.

قضیه: اگر $ab = ac \quad mod \ \ p$ و $0 \leq a < p$ ، آنگاه $b = c \quad mod \ \ p$.

اثبات:

$$ab = ac \quad mod \ \ p \longrightarrow p|a(b-c) \longrightarrow p|(b-c) \longrightarrow b-c = 0 \quad mod \ \ p. \tag{۷۲}$$

دراین عبارت ازقضیه قبلی استفاده کرده ایم و این حقیقت که عدد p نمی تواند a را بشمارد، چون از a بزرگتراست.

قضیه: به ازای هر عدد اول p مجموعه $Z_p^* := \{1, 2, 3, \cdots p-1\}$ با ضرب درپیمانه p یک گروه تشکیل می دهد.

اثبات: عضو خنثی به طور بدیهی همان 1 است. این که برای هرعضو یک عضووارون وجود دارد از این جا معلوم می شود که بنابرقضیه قبلی درجدول ضرب این مجموعه درهیچ سطر یا ستونی عضو تکراری نمی تواند وجود داشته باشد، درنتیجه درهرسطر حتماً می بایست عنصر 1 در جایی از سطر یا ستون مربوطه پدیدارشود و همین به معنای وجود عضو وارون است.

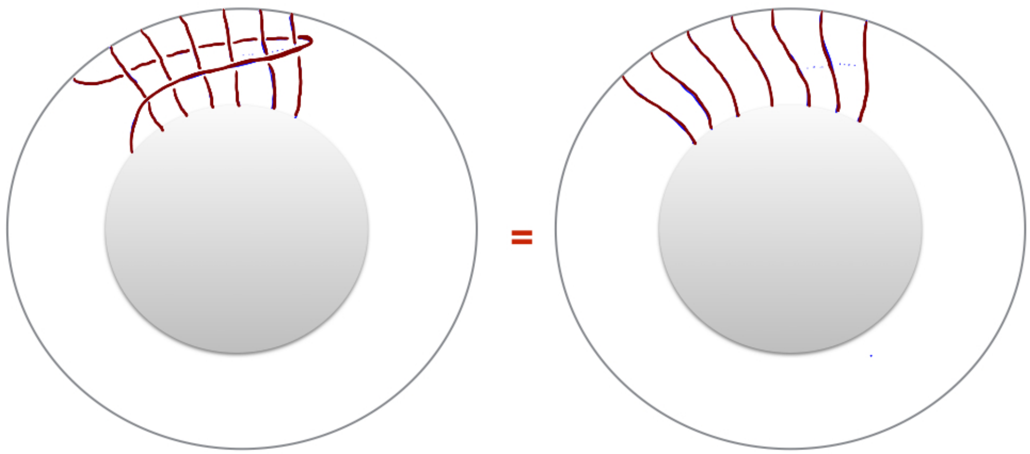
هم چنین خواننده می تواند قضیه زیر را ثابت کند.

قضیه: هرگاه a یک عدد صحیح باشد ${Z_a}^*$ مجموعه تمام اعداد صحیح مثبت کوچک تراز a است که نسبت به آن اول باشند. این مجموعه تشکیل یک گروه می دهد.

■ **مثال:** $Z_{12}^* = \{1, 5, 7, 11\}$. جدول ضرب این گروه عبارت است از:

(73)

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1



شکل ۹: در روی کره این دو گیسو با هم معادل هستند.

۱۳ تمرین های اضافه:

- ۱ـ عناصر گروه S_4 را بر حسب مولدهای آن بنویسید.

- ۲ ـ در گروه گیسوی B_n همه منحنی ها بین دو نسخه از صفحه ی R_2 تعریف شده اند. به عبارت دیگر به ازای هر منحنی $\gamma_i(t)$ داریم $\gamma_i : [0,1] \longrightarrow R^2 \times [0,1]$. حال تعمیمی از گروه گیسو را در نظر بگیرید که در آن همه منحنی ها بین دو نسخه از کره دوبعدی S_2 تعریف شده اند، یعنی

$$\gamma_i : [0,1] \longrightarrow S^2 \times [0,1].$$

مولدهای این گروه هم چنان عبارتند از $\sigma_1,\ \sigma_2,\ \cdots \gamma_{n-1}$. اما به دلیل خاصیت توپولوژیک کره که یک سطح بدون مرز است یک رابطه اضافه بین این مولدها برقرار است. این رابطه را پیدا کنید. (راهنمایی: به شکل ؟؟ توجه کنید.)

■ ۳ـ جدول ضرب تمام گروه های با ۴ عنصر را بسازید. چند گروه متفاوت پیدا می کنید؟ چند تا از این گروه ها آبلی هستند؟ کدام یک از آنها با گروه Z_4 یکسان است؟ کدام یک از آنها با گروه $Z_2 \times Z_2$ یکسان است.؟

■ ۴ ـ فرض کنید که G یک گروه است که درآن خاصیت زیر برقراراست:

$$a^2b^2 = (ab)^2 \qquad \forall \ \ a, \ b \in G \tag{۷۴}$$

نشان دهید که این گروه آبلی است.

■ ۵ـ فرض کنید که G یک گروه است که درآن خاصیت زیر برای سه عدد متوالی (مثلا ۵ و ۴ و ۳) برقراراست:

$$a^ib^i = (ab)^i \qquad \forall \ \ a, \ b \in G \tag{۷۵}$$

نشان دهید که این گروه آبلی است.

■ ۶ـ نشان دهید که درگروه S_3 چهار عنصر وجود دارد که مربع آنها برابر با عنصر واحد است. هم چنین نشان دهید که سه عنصر وجود دارد که مکعب آنها عنصر واحد است.

■ ۷ـ نشان دهید که اگر دریک گروه هر عضو وارون خودش باشد آن گروه حتما یک گروه آبلی است.

■ ۸ ـاگر مرتبه یک گروه زوج باشد نشان دهید که حتما یک عنصر مخالف عضو واحد مثل a وجوددارد که دارای خاصیت $a^2 = e$ است. e دراینجا عنصر وارون گروه است.

■ ۹ ـ میدانِ F به صورت $Z/3Z(x^2+1)$ نوشته می شود. این نماد گذاری به این معناست که اعضای میدان F عبارت اند از چندجمله‌ای هایی از متغیر x که ضرایب آن ها تنها اعدادِ $0, 1, 2$ هستند و جمع این اعداد نیز به سنج ۳ انجام می گیرد.

هم چنین عبارت x^2+1 به این معناست که در جمع و ضرب این چند جمله‌ای ها همواره x^2+1 را معادل با 0 می گیریم. عناصر این میدان و مرتبه آن را پیدا کنید. هم چنین در یک جدول وارون جمعی و وارون ضربی هر عنصر را مشخص کنید.

■ ۱۰ ـ الف : نشان دهید که گروه های با مرتبه ۳ حتماً آبلی هستند.
ب : قسمت الف را برای وقتی که مرتبه گروه ۴ باشد تحقیق کنید.
ج : قسمت الف را برای وقتی که مرتبه گروه ۵ باشد تحقیق کنید.

■ ۱۱ ـ فرض کنید که مجموعه ناتهی مثل G تحت یک ضرب شرکت پذیر بسته باشد و نیز خواص اضافی زیر را داراباشد:
الف : عضوی مثل $e \in G$ وجود داشته باشد به قسمی که $\forall \;\; a \in G, \;\; a\dot{e} = a$ و
ب : به ازای هرعضو a، عضوی مثل $x(a) \in G$ وجود داشته باشد به قسمی که $a \cdot x(a) = e$.
نشان دهید که دراین صورت این مجموعه یک گروه است.

■ ۱۲ ـ فرض کنید که G مجموعه ای متناهی باشد که تحت یک ضرب شرکت پذیر بسته باشد. بعلاوه فرض کنید که دراین مجموعه هم قانون حذف از چپ و هم قانون حذف از راست برقرارباشند. ثابت کنید که دراین صورت G یک گروه است.

■ ۱۳ ـ به ازای هر $n > 2$ گروهی بسازید ناآبلی که ازمرتبه $2n$ باشد. (راهنمایی: از روابط موجود درS_3 تقلید کنید.)

■ ۱۴ ـ اگرp یک عدد اول و $F = Z_p$ باشد. ثابت کنید که $G = GL_2(F)$ یک گروه است. مرتبه این گروه را پیدا کنید.

■ ۱۵ ـ درمسئله قبل زیرگروهی را درنظر بگیرید که اعضای آن دارای شرط $ad-bc = 1 \quad mod \;\; p$ هستند. این زیر گروه با نماد $SL_2(F)$ مشخص می شود که درآن SL از لفظ $SpecialLinearGroup$ آمده است. مرتبه این زیرگروه را تعیین کنید.