
بسم الله الرحمن الرحيم

**دانشکده علوم ریاضی**

**گروه ریاضی محض**

پایان‌نامه کارشناسی ارشد

گرایش جبر

**عنوان**

# گروه‌های متناهی دارای $POS$

پژوهشگر

**مسعود حکمی**

استاد راهنما

**دکتر غلامرضا رضایی‌زاده**

استاد مشاور

**دکتر ندا آهنجیده**

آبان ۱۳۹۲

تقدیم به

خدایی که آفرید

جهان را، انسان را، عقل را، علم را، معرفت را، عشق را،

تقدیم به پدر، مادر، همسر و فرزند دلبندم

و تقدیم به کسانی که عشقشان را در وجودم دمیدند.

«سپاس خدای راکه سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت‌های او ندانند و کوشندگان، حق او را گزاردن نتوانند، و سلام و درود بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...»

بدون شک جایگاه و منزلت معلم، اجل از آن است که در مقام قدردانی از زحمات بی شائبه ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم اما از آنجایی که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تأمین می کند و سلامت امانت هایی را که به دستش سپرده اند، تضمین؛ بر حسب وظیفه و از باب «من لم یشکر المنعم من المخلوقین لم یشکر اللهِ عزّ و جلّ»: از پدر و مادر عزیزم، این دو معلم بزرگوارم که همواره بر کوتاهی و درشتی من، قلم عفو کشیده و کریمانه از کنار غفلت هایم گذشته اند و در تمام عرصه های زندگی یار و یاوری بی چشم داشت برای من بوده اند؛ از استاد با کمالات و شایسته؛ جناب آقای دکتر غلامرضا رضایی زاده که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند؛ و زحمت راهنمایی این رساله را بر عهده گرفتند؛ از استاد صبور و با تقوا، جناب دکتر ندا آهنجیده که زحمت مشاوره این رساله را در حالی متقبل شدند که بدون مساعدت ایشان، این پروژه به نتیجه مطلوب نمی رسید؛ کمال تشکر و قدردانی را دارم. باشد که این خرد ترین، بخشی از زحمات آنان را سپاس گوید.

با آرزوی موفقیت برای تمام عزیزان

مسعود حکمی

آبان ۱۳۹۲

# چکیده

فرض کنید $G$ گروه متناهی و $x$ عضوی از $G$ باشد. مجموعه $OS(x)$، مجموعه‌ای از تمام عناصر گروه $G$ که مرتبه آن‌ها با مرتبه $x$ برابر باشد. گروه متناهی $G$ یک $POS$-گروه است، هرگاه برای هر $x \in G$، کاردینال $OS(x)$ مقسوم علیه‌ای از مرتبه $G$ باشد. در این پایان‌نامه بعضی از خواص $POS$-گروه‌ها بررسی شده و خانواده‌ای از $POS$-گروه‌های غیر آبلی به کمک حاصل‌ضرب نیم مستقیم ارائه می‌شود. در پایان نشان داده می‌شود گروه متناوب $A_n$ ($n \geq ۳$) و گروه متقارن $S_n$ ($n \geq ۴$)، $POS$-گروه نیستند.

**کلمات کلیدی :** گروه‌های متناهی، حاصل‌ضرب نیم مستقیم، بخش‌پذیری، عدد اول.

# فهرست مطالب


**مقدمه** ۲

**۱ مفاهیم مقدماتی و پیش نیازها** ۳

۱.۱ نظریه اعداد . . . . . ۳

۲.۱ قضایای سیلو . . . . . ۵

۳.۱ حاصل‌ضرب گروه‌ها . . . . . ۷

۴.۱ گروه خود ریختی‌ها . . . . . ۱۲

۵.۱ گروه جایگشتی . . . . . ۱۳

**۲ $POS$-گروه‌ها** ۱۷

۱.۲ تعاریف و آشنایی با بعضی از ویژگی‌های $POS$-گروه‌ها . . . . . ۱۷

۲.۲ $POS$-گروه‌ها و حاصل‌ضرب مستقیم . . . . . ۲۹

**۳ $POS$-گروه‌های غیر آبلی** ۳۹

۱.۳ $POS$-گروه‌ها و حاصل‌ضرب نیم مستقیم . . . . . ۳۹

**۴ گروه‌های جایگشتی و $POS$-گروه‌ها** ۵۱

۱.۴ مثال‌هایی از گروه‌هایی که $POS$-گروه نیستند . . . . . ۵۱

**مراجع** ۶۱

**واژه‌نامه انگلیسی به فارسی** ۶۲

**واژه‌نامه فارسی به انگلیسی** ۶۴

**Abstract** ۶۶

# مقدمه

در سال ۲۰۰۲ فینچ [1] و جونز [2] [۴] مفهوم $POS$-گروه‌ها را معرفی کردند. آنها روش‌هایی برای ساختن یک گروه آبلی که $POS$-گروه هستند را ارائه دادند. همچنین در سال ۲۰۰۳ [۵] نشان دادند که تعداد نامتناهی گروه غیر آبلی از این نوع وجود دارد. در این مقاله ثابت کردند که اگر $n$ یا $n-1$ عدد اول باشد، آن‌گاه گروه متناوب $A_n$ برای $n \geq 4$ یک $POS$-گروه نیست. در سال ۲۰۰۳ لیبرا [3] و تلسک [4] [۸] با ارائه مثال‌هایی از گروه‌های غیر آبلی که با دو عضو تولید می‌شوند نشان دادند که گروه $D_{2n}$ یک $POS$-گروه است اگر و تنها اگر $n = 3^a$ که $a \geq 1$.

در سال ۲۰۰۹ داس [5] [۲] به بررسی خواص $POS$-گروه‌ها پرداخت. سپس به کمک حاصل‌ضرب نیم مستقیم و اعداد اول فرما نشان داد که تعداد نامتناهی گروه غیر آبلی از این نوع وجود دارد و در آخر ثابت نمود که $A_n$ برای $n \geq 3$ یک $POS$-گروه نیست. همچنین در سال ۲۰۱۰ توآن [6] [۱۱] ثابت نمود که $S_n$ برای $n \geq 4$ یک $POS$-گروه نیست.

این پایان‌نامه شامل چهار فصل است که برگرفته از مقالات [۲]، [۴] و [۱۱] می‌باشد. در فصل اول مفاهیم مقدماتی که در طول پایان‌نامه مورد استفاده قرار می‌گیرد بیان خواهد شد. فصل دوم که شامل دو بخش می‌باشد. در بخش اول به بررسی بعضی از ویژگی‌ها و خواص $POS$-گروه‌ها خواهیم پرداخت و در بخش دوم با ارائه قضایایی طریقه ساختن یک گروه با مرتبه کوچک از روی یک گروه با مرتبه بزرگ که هر دو $POS$-گروه هستند (یا بر عکس) را به کمک حاصل‌ضرب مستقیم بیان خواهیم کرد. در فصل سوم با $POS$-گروه‌های غیر آبلی که به کمک حاصل‌ضرب نیم مستقیم و اعداد اول فرما به دست می‌آیند آشنا خواهیم شد. در فصل چهارم مثال‌هایی از گروه‌هایی که $POS$-گروه نیستند را ارائه می‌دهیم در این فصل نشان خواهیم داد که گروه متقارن $S_n$ برای $n \geq 4$ و گروه متناوب $A_n$ برای $n \geq 3$ $POS$-گروه نیستند.

1. Finch
2. Jones
3. Libera
4. Tlucek
5. Das
6. Tuan

# فصل ۱

# مفاهیم مقدماتی و پیش نیازها

## ۱.۱ نظریه اعداد

در این بخش ابتدا به معرفی تابع فی اویلر و بعضی از خواص آن پرداخته و در ادامه به معرفی مرتبه اعداد صحیح به پیمانه (مد) $n$ و ریشه‌های اولیه اعداد می‌پردازیم و در آخر به معرفی اعداد اول فرما خواهیم پرداخت.

**تعریف ۱.۱.۱.** تابع فی اویلر ($\phi$ اویلر) یک تابع با دامنه $N$ (مجموعه اعداد صحیح مثبت) است که چنین تعریف می‌شود. به ازای هر $m \geq ۱$، $\phi(m)$ برابر با تعداد اعداد صحیح نابیشتر از $m$ که نسبت به $m$ اولند می‌باشد.

**قضیه ۱.۱.۲.** *به ازای $n > ۲$، $\phi(n)$ عدد صحیح زوجی است.*

***برهان.*** مرجع [الف] صفحه ۱۷۰. □

**قضیه ۱.۱.۳.** *فرض کنید $m$ و $n$ دو عدد طبیعی باشند. اگر $m \mid n$، آنگاه $\phi(m) \mid \phi(n)$.*

***برهان.*** فرض کنید تجزیه $m, n$ به عوامل اول به صورت $n = p_۱^{\alpha_۱} ... p_k^{\alpha_k}$ و $m = q_۱^{\beta_۱} ... q_s^{\beta_s}$ باشد بطوریکه $q_۱, q_۲, ..., q_s \in \{p_۱, ..., p_k\}$ حال بدون اینکه از کلیت مسئله چیزی کم شود فرض می‌کنیم :

$$m = p_۱^{\beta_۱} ... p_s^{\beta_s}$$

بطوریکه $s \leq k$ و برای هر $۱ \leq i \leq s$ داشته باشیم $\beta_i \leq \alpha_i$ حال نشان می‌دهیم حاصل $\frac{\phi(n)}{\phi(m)}$ یک عدد

صحیح است:

$$\frac{\phi(n)}{\phi(m)} = \frac{n(1-\frac{1}{p_1})...(1-\frac{1}{p_k})}{m(1-\frac{1}{p_1})...(1-\frac{1}{p_s})} = \frac{n(p_{s+1}-1)(p_{s+2}-1)...(p_k-1)}{m(p_{s+1}p_{s+2}...p_k)}$$
$$= \frac{p_1^{\alpha_1}...p_s^{\alpha_s}...p_k^{\alpha_k}(p_{s+1}-1)...(p_k-1)}{p_1^{\beta_1}...p_s^{\beta_s}...p_{s+1}p_{s+2}...p_k}$$
$$= p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}...p_s^{\alpha_s-\beta_s}p_{s+1}^{\alpha_{s+1}-1}...p_k^{\alpha_k-1}(p_{s+1}-1)...(p_k-1) \in Z.$$

□

**قضیه ۴.۱.۱.** *(اویلر) اگر $n$ عدد صحیح مثبت و بزرگترین مقسوم علیه مشترک $a,n$ برابر یک باشد، آن‌گاه $a^{\phi(n)} \equiv 1 \pmod n$.*

***برهان.*** مرجع [الف] صفحه ۱۷۴. □

**تعریف ۵.۱.۱.** اگر $n > 1$ و $(a,n) = 1$، آن‌گاه کوچک‌ترین عدد صحیح مثبت $k$ به طوری که $a^k \equiv 1 \pmod n$، مرتبه $a$ به پیمانه (مد) $n$ نامیده می‌شود.

**تعریف ۶.۱.۱.** اگر $(a,n) = 1$ و مرتبه $a$ به پیمانه $n$ برابر $\phi(n)$ باشد، آن‌گاه $a$ ریشه اولیه‌ای از $n$ نامیده می‌شود. به بیان دیگر $a$ ریشه اولیه‌ای از $n$ است هرگاه $a^{\phi(n)} \equiv 1 \pmod n$، ولی به ازای هر عدد صحیح مثبت $k < \phi(n)$، $a^k \not\equiv 1 \pmod n$.
به آسانی می‌توان ملاحظه کرد که ۳ ریشه اولیه‌ای از ۷ است زیرا $\phi(7) = 6$ و
$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1$ (به پیمانه ۷).

**قضیه ۷.۱.۱.** *اگر $n$ ریشه اولیه‌ای داشته باشد، آن‌گاه $n$ دقیقا $\phi(\phi(n))$ ریشه اولیه دارد.*

***برهان.*** مرجع [الف] صفحه ۲۰۰. □

**قضیه ۸.۱.۱.** *الف) هر عدد اول ریشه اولیه دارد.*

*ب) اگر $p$ یک عدد اول فرد باشد و $\alpha \in N$ در این صورت عدد $p^\alpha$ ریشه‌ی اولیه دارد.*

*پ) فقط اعداد ۲,۴ و اعداد طبیعی به صورت $p^\alpha$ و $2p^\alpha$ که در آن‌ها $p$ یک عدد اول فرد و $\alpha$ عدد طبیعی است ریشه اولیه دارد.*

*ت) هر ریشه اولیه $r$ از $p^\alpha$ ریشه اولیه $p$ نیز می باشد.*

***برهان.*** مرجع [الف] صفحه ۲۱۵. □

**لم ۹.۱.۱.** *اگر $m$ یک عدد طبیعی و $2^m + 1$ عدد اول باشد، آن‌گاه $m$ توانی از ۲ است.*

***برهان.*** فرض کنیم $m$ توانی از ۲ نباشد و دارای مقسوم علیه فردی به صورت $۲k+۱ > ۱$ باشد. پس

$$\exists\, r \in Z \; s.t \; m = (۲k+۱)r,$$

$$۲^m + ۱ = ۲^{(۲k+۱)r} + ۱ = (۲^r)^{۲k+۱} + ۱ = (۲^r + ۱)(۲^{۲kr} - ۲^{(۲k-۱)r} + \ldots + ۲^{۲r} - ۲^r + ۱)$$

که این خلاف اول بودن $۲^m + ۱$ است. پس باید $m$ توانی از ۲ باشد. □

**تعریف ۱.۱.۱۰.** هر عدد صحیح به صورت $F_n = ۲^{۲^n} + ۱ \; (n \geq ۰)$ عدد فرما نامیده می‌شود.
اگر $F_n$ یک عدد اول باشد، آن را "عدد اول فرما" می‌نامیم.
فرما با ملاحظه اعداد اول $F_۰ = ۳ \, , F_۱ = ۵ \, , F_۲ = ۱۷ \, , F_۳ = ۲۵۷۲ \, , F_۴ = ۶۵۵۳۷$ تصور کرد که سایر اعداد از این دنباله اولند ولی اویلر در سال ۱۷۳۲ دریافت که $F_۵$ بر ۶۴۱ بخش‌پذیر است زیرا

$$F_۵ = ۲^{۲^۵} + ۱ = ۲^{۳۲} + ۱ = ۲^۴ \times ۲^{۲۸} + ۱ = (۶۴۱ - ۵^۴)۲^{۲۸} + ۱$$

$$= ۶۴۱ \times ۲^{۲۸} - (۵ \times ۲^۷)^۴ + ۱ = ۶۴۱ \times ۲^{۲۸} - (۶۴۱ - ۱)^۴ + ۱ \equiv -۱ + ۱ = ۰ \pmod{۶۴۱}$$

اویلر شکل عوامل اول فرما را نیز تعیین و در سال ۱۷۴۷ ثابت کرد که وقتی $m \geq ۲$ هر عامل اول $F_m$ به صورت $۲^{m+۱} \times n + ۱$ است. لوکاس در سال ۱۸۷۹ نشان داد که $n$ زوج است و حکم اویلر را به صورتی که در قضیه زیر ملاحظه می‌کنید کامل کرد.

**قضیه ۱.۱.۱۱.** *اگر $m \geq ۲$، هر عامل اول $F_m$ به صورت $۲^{m+۲} \times n + ۱$ است.*

***برهان.*** مرجع [الف] صفحه ۲۹۳. □

**قضیه ۱.۱.۱۲.** *به ازای $n \geq ۱$، عدد فرمای $F_n = ۲^{۲^n} + ۱$ اول است اگر و تنها اگر*
$$۳^{\frac{(F_n - ۱)}{۲}} \equiv -۱ \pmod{F_n}$$

***برهان.*** مرجع [الف] صفحه ۲۹۱. □

**قضیه ۱.۱.۱۳.** *هر عدد صحیح مثبت بجز ۱، ۲، ۴، ۶ و ۹ را به صورت مجموع چند عدد اول فرد متمایز می‌توان نوشت.*

***برهان.*** مرجع [۳] صفحه ۲۲۶. □

## ۲.۱ قضایای سیلو

**قضیه ۱.۲.۱.** (کوشی). *فرض کنیم $G$ یک گروه متناهی باشد و $p \,||G|$، که در آن $p$ یک عدد اول است. در این صورت $G$ عضوی از مرتبه $p$ دارد.*

***برهان.*** مرجع [ج] صفحه ۶۹. □

**تعریف ۲.۲.۱.** فرض کنیم $G$ یک گروه، و $p$ یک عدد اول باشد. گروه $G$ را یک $p$-گروه می‌نامیم در صورتی که مرتبه هر عضو $G$ توان مثبتی از $p$ باشد. زیر گروه $H$ از $G$ را یک $p$-زیر گروه $G$ گوییم در صورتی که $H$ یک $p$-گروه باشد.

**نتیجه ۳.۲.۱.** *اگر $G$ یک $p$-گروه متناهی باشد، آن‌گاه مرتبه $G$ به صورت $p^a$ است که در آن $a$ یک عدد صحیح نامنفی است.*

***برهان.*** اگر مرتبه $G$ توانی از عدد اول $p$ باشد، در این صورت چون مرتبه هر عنصر، مرتبه گروه را می‌شمارد پس مرتبه هر عضو $G$ توانی از عدد اول $p$ است. حال فرض کنید $G$ یک $p$-گروه متناهی است. اگر $q \neq p$ عدد اول باشد و $q \mid |G|$، آن‌گاه بنا به قضیه کوشی $G$ باید عضوی از مرتبه $q$ داشته باشد که متناقض با $p$-گروه بودن $G$ است. بنابراین مرتبه $G$ باید توانی از عدد اول $p$ باشد. □

**مثال ۴.۲.۱.** گروه کواترنیون. گروه تولید شده توسط عناصر $a$ و $b$ که فقط در روابط $b^{-1}ab = a^{-1}$ و $a^4 = 1$ و $a^2 = b^2$ صدق کند، گروه کواترنیون مرتبه ۸ نامیده می‌شود و با $Q_8$ نمایش داده می‌شود. این گروه یک مثال از ۲-گروه می‌باشد.

**مثال ۵.۲.۱.** گروه دو وجهی. گروه $G$ با مولدهای $a$، $b$ و روابط $a^n = b^2 = 1$ و $b^{-1}ab = a^{-1}$ گروه دو وجهی مرتبه $2n$ نامیده می‌شود و با $D_{2n}$ نمایش داده می‌شود. گروه دو وجهی $D_{2n}$ از مرتبه ۸ یک مثال از ۲-گروه می‌باشد.

**تعریف ۶.۲.۱.** زیر گروه سیلو: فرض کنیم $G$ یک گروه متناهی است و $p$ یک مقسوم علیه اول مرتبه $G$ است. می‌توان نوشت $|G| = p^n.m$ که $m$ و $n$ اعداد طبیعی‌اند به طوری که $(p, m) = 1$. در این صورت هر زیر گروه $G$ از مرتبه $p^n$ یک سیلو $p$-زیرگروه $G$ و یا یک $p$-سیلو زیرگروه $G$ نامیده می‌شود. مجموعه تمام سیلو $p$-زیرگروه‌های $G$ را با $\mathrm{Syl_p}(G)$ نمایش می‌دهیم و تعداد اعضای مجموعه اخیر را با $n_p(G)$ (یا $n_p$) نمایش می‌دهیم.
به عبارت دیگر $P$ یک سیلو $p$-زیرگروه، گروه متناهی $G$ است هرگاه $P$ یک $p$-زیر گروه بوده و $[G : P]$ نسبت به $p$ اول باشد.

در قضیه زیر وجود زیرگروه‌های سیلو در یک گروه متناهی و نیز خواص این زیرگروه‌ها و تعداد آنها بیان می‌شود.

**قضیه ۷.۲.۱.** *فرض کنیم $G$ یک گروه متناهی از مرتبه $n$ باشد که در آن $n = p^\alpha.m$، $\alpha \geq 0$ و $p$ عدد اولی است که $p \nmid m$. در این صورت،*

۱) *$G$ حداقل یک $p$-زیرگروه سیلو دارد.*

۲) *هر $p$-زیرگروه $G$ جزء یک $p$-زیرگروه سیلوی $G$ است.*

۳) *هر دو $p$-زیرگروه $G$ مزدوج‌اند.*

۴) *تعداد همه $p$- زیرگروه‌های سیلو $G$ همنهشت ۱ به پیمانه $p$ است.*

***برهان.*** مرجع [پ] صفحه ۷۲. □

**قضیه ۸.۲.۱.** *اگر همه سیلو- زیرگروه‌های $G$ دوری باشد، آن‌گاه گروه $G$ نمایشی بصورت زیر دارد.*

$$G =< a, b : a^m = ۱ = b^n \ , b^{-۱}ab = a^r >$$

*که در آن $۰ \leq r < m$، $r^n \equiv ۱ \pmod m$، $m$ فرد و $(m, n(r-۱)) = ۱$ است.*

***برهان.*** مرجع [۹] صفحه ۲۹۰. □

**لم ۹.۲.۱.** *برای هر مقسوم علیه مثبت $d$ از $n$، گروه دوری از مرتبه $n$ به تعداد $\phi(d)$ عنصر از مرتبه $d$ دارد.*

***برهان.*** فرض کنید $G$ یک گروه دوری از مرتبه $n$ باشد و $d \mid n$. در این‌صورت $G$ یک و فقط یک زیرگروه مانند $H$ از مرتبه $d$ دارد که $H =< x : x^d = ۱ >$ به عبارت دیگر تمام عناصر $G$ که از مرتبه $d$ هستند در $H$ قرار دارند. از طرفی تعداد مولدهای گروه دوری $H$ عبارت از $\phi(d)$ است. لذا تعداد عناصر از مرتبه $d$ برابر با $\phi(d)$ است. □

**لم ۱۰.۲.۱.** *اگر در گروه متناهی $G$ به ازای هر عدد صحیح $n$ حداکثر $n$ عنصر $x \in G$ وجود داشته باشد به گونه‌ای که $x^n = ۱$ ، آنگاه $G$ گروهی دوری است.*

***برهان.*** مرجع [ب] صفحه ۶۹. □

**لم ۱۱.۲.۱.** (*قضیه فروبنیوس*) *فرض کنیم $G$ یک گروه متناهی باشد که $n \mid |G|$ و $X = \{g \in G \ : g^n = ۱\}$. در این صورت $n \mid |X|$.*

***برهان.*** مرجع [۶] صفحه ۱۳۶. □

## ۳.۱ حاصل‌ضرب گروه‌ها

یکی از مباحث نظریه گروه‌ها، موضوع ساختن گروه‌ها از گردایه‌ای از گروه‌های مفروض و نیز موضوع تجزیه گروهی مفروض به مولفه‌هایی از گروه‌هایی معلوم است. یکی از ساده‌ترین روش‌های ساختن و تجزیه معرفی حاصل‌ضرب مستقیم گروه‌هاست.

**قضیه ۱.۳.۱.** *فرض کنیم $G_۱$ ، $G_۲$ ،...، $G_n$ گروه‌اند. حاصل‌ضرب دکارتی $\prod_{i=۰}^{n} G_i = G_۱ \times ... \times G_n$ تحت قانون ترکیب زیر یک گروه است که حاصل‌ضرب مستقیم خارجی $G_۱$ ، $G_۲$ ، ...، $G_n$ نامیده می‌شود.*

$$(x_۱, x_۲, ..., x_n)(y_۱, y_۲, ..., y_n) = (x_۱y_۱, x_۲y_۲, ..., x_ny_n)$$

$$x_i, y_i \in G_i \qquad ۱ \leq i \leq n$$

***برهان.*** مرجع [ب] صفحه ۱۱۶. □

**قضیه ۲.۳.۱.** *فرض کنیم $G_۱$ ، $G_۲$ ، ... ، $G_n$ گروه و $G = \prod_{i=۱}^{n}$ حاصل‌ضرب مستقیم خارجی آن‌هاست. قرار می‌دهیم $\bar{G}_i = \{(۱, ۱, ..., g_i, ..., ۱) : g_i \in G_i\}$ که $g_i$ در مکان $i$ام قرار دارد. در این صورت شرایط زیر برقرار است :*

*الف)* $\bar{G}_i \trianglelefteq G$ *برای هر* $۱ \leq i \leq n$ ،

ب) $G = \bar{G}_۱\bar{G}_۲...\bar{G}_n$ ،

پ) $\bar{G}_i \cap (\bar{G}_۱\bar{G}_۲...\bar{G}_{i-۱}^{-}) = ۱$ *برای هر* $۲ \leq i \leq n$ .

***برهان.*** مرجع [ب] صفحه ۱۱۶. □

**تعریف ۳.۳.۱.** فرض کنیم $G$ گروه و $G_۱$ ، $G_۲$ ، ... ، $G_n$ زیر گروه‌هایی از آن هستند. گوییم $G$ حاصل‌ضرب مستقیم داخلی زیرگروه‌های $G_۱$ ، $G_۲$ ، ... ، $G_n$ است هرگاه شرایط زیر را داشته باشیم :

الف) $G_i \trianglelefteq G$ برای هر $۱ \leq i \leq n$ ،

ب) $G = G_۱G_۲...G_n$ ،

پ) $G_i \cap (G_۱G_۲...G_{i-۱}) = ۱$ برای هر $۲ \leq i \leq n$ .

**قضیه ۴.۳.۱.** *فرض کنید $G$ حاصل‌ضرب مستقیم داخلی زیرگروه‌های $G_۱$ ، $G_۲$ ، ... ، $G_n$ است در این صورت :*

*الف) اگر* $g_۱g_۲...g_n = ۱$ *که* $g_i \in G_i$ $(۱ \leq i \leq n)$ *آن‌گاه* $g_i = ۱$ *برای هر* $i$ .

ب) $G_i \cap G_j = ۱$ ، $i \neq j$ .

پ) *هر عضو* $g \in G$ *را می‌توان به طور منحصر بفردی به صورت* $g = g_۱g_۲...g_n$ *نوشت که* $g_i \in G_i$ ، $۱ \leq i \leq n$ .

***برهان.*** مرجع [ب] صفحه ۱۱۷. □

**قضیه ۵.۳.۱.** *فرض کنید $G$ حاصل‌ضرب مستقیم داخلی زیرگروه‌های $G_۱$ ، $G_۲$ ، ... ، $G_n$ است. در این‌صورت داریم :*

$$G \cong G_۱ \times G_۲ \times ... \times G_n.$$

***برهان.*** مرجع [ب] صفحه ۱۱۸. □

**قضیه ۶.۳.۱.** *هر گروه آبلی متناهی با حاصل‌ضرب مستقیم داخلی زیرگروه‌های سیلویش یکریخت است.*

***برهان.*** مرجع [ب] صفحه ۲۲۹. □

**تعریف ۷.۳.۱.** عمل گروه . گوییم گروه $G$ بر مجموعه $\Omega$ عمل می‌کند هرگاه نگاشت

$$\Omega \times G \longrightarrow \Omega$$

$$(w\ ,\ g) \longmapsto w^g\ ,\ \forall\ w \in \Omega\ ,\ \forall\ g \in G$$

وجود داشته باشد، به طوری که داشته باشیم :

الف) برای هر $w \in \Omega$ $w = w^1$،

ب) برای هر $w \in \Omega$ و هر $g, h \in G$ $(w^g)^h = w^{gh}$.

۱ عضو خنثی گروه $G$ است و $w = w^1$ به این معناست که اثر عضو خنثی بر هر عضو $\Omega$ تغییری در آن عضو ایجاد نمی‌کند.

**تعریف ۸.۳.۱.** عمل گروه بر گروه. فرض کنیم $G$ و $H$ گروه‌اند. گوییم $G$ روی $H$ عمل می‌کند و یا اینکه $G$ یک گروه عملگر روی $H$ است، هرگاه $G$ روی $H$ به عنوان مجموعه عمل کند (یعنی شرایط تعریف (۷.۳.۱) برقرار باشند) و به علاوه داشته باشیم:

$$(xy)^g = x^g y^g\ ,\ \forall\ x, y \in H\ ,\ \forall\ g \in G.$$

اگر به ازای هر $x \in H$ و هر $g \in G$ داشته باشیم $x^g = x$، آن‌گاه این را عمل بدیهی $G$ بر $H$ می‌نامیم.

**قضیه ۹.۳.۱.** *فرض کنیم گروه $G$ بر گروه $H$ عمل می‌کند. در این صورت حاصل‌ضرب دکارتی $H \times G$ با قانون ترکیب زیر یک گروه است:*

$$(x, g)(y, h) = (x^h y, gh) \quad \forall\ x, y \in H\ ,\ \forall\ g, h \in G$$

*گروه بالا را حاصل‌ضرب نیم مستقیم $H$ و $G$ نسبت به عمل داده شده $G$ بر $H$ می‌نامند و با $H \rtimes G$ یا $H : G$ نمایش می‌دهند.*

***برهان.*** مرجع [ب] صفحه ۱۴۳. □

**نتیجه ۱۰.۳.۱.** *اگر $G$ روی $H$ به طور بدیهی عمل کند. در این صورت*

$$H \rtimes G \cong H \times G$$

**تعریف ۱۱.۳.۱.** فرض کنیم $H$ و $K$ دو گروه دلخواه و $\phi : H \longrightarrow \mathrm{Aut}(K)$ یک همریختی باشد. به ازای هر $h$ از $H$ ، تصویر $h$ با $\phi$ را با $\phi_h$ نشان می‌دهیم. در حاصل‌ضرب دکارتی $H \times K$ عمل دوتایی زیر را تعریف می‌کنیم :

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, (k_1 \phi_{h_2}) k_2).$$

مجموعه $H \times K$ با عمل فوق تشکیل یک گروه می‌دهد. این گروه را حاصل‌ضرب نیم مستقیم $H$ و $K$ با عمل $\phi$ می‌نامند و آن را با علامت $H \ltimes_\phi K$ نشان می‌دهند که اصطلاحا می‌گویند $H$ بر گروه $K$ با $\phi$ عمل می‌کند. در حالتی که ابهامی در مورد $\phi$ پیش نیاید، یا مشخص کردن آن مورد نیاز نباشد، به جای علامت مذکور، از علامت $H \ltimes K$ استفاده می‌شود.
توضیح اینکه عضو همانی گروه $H \ltimes_\phi K$ عبارت است از $(1_H, 1_K)$ و عضو معکوس $(h,k)$، که در آن $h \in H$ و $k \in K$، عضو $(h^{-1}, k^{-1}\phi_{h^{-1}})$ است.

**مثال ۱۲.۳.۱.** فرض کنیم $H$ و $K$ به ترتیب گروه‌هایی دوری از مرتبه ۲ و ۳ باشند. مولدهای $H$ و $K$ را به ترتیب $x$ و $y$ می‌نامیم. بنابراین $H = \{1, x\}$ و $K = \{1, y, y^2\}$. اینک می‌دانیم $\mathrm{Aut}(K)$ دارای دو عضو است یکی $\varepsilon$، (خود ریختی همانی $K$)، و دیگری که آن را با $\sigma$ نشان می‌دهیم که هر عضو $K$ را معکوس می‌کند.
حال $\phi : H \longrightarrow \mathrm{Aut}(K)$ را با ضابطه $\phi_1 = \varepsilon$ و $\phi_x = \sigma$ در نظر می‌گیریم. داریم :

$$H \ltimes_\phi K = \{(1,1), (1,y), (1,y^2), (x,1), (x,y), (x,y^2)\}$$

با فرض $a = (x,1)$ و $b = (1,y)$،

$$ab = (x\ 1)(1\ ,\ y) = (x\ ,\ y),$$

$$ba = (1\ y)(x\ ,\ 1) = (x\ ,\ y\phi_x) = (x\ ,\ y\sigma) = (x\ ,\ y^{-1}) = (x\ ,\ y^2)$$

بنابراین $ab \neq ba$. یعنی گروه شش عضوی $H \ltimes_\phi K$ غیر آبلی است و در نتیجه با $S_3$ یکریخت است.

**قضیه ۱۳.۳.۱.** *فرض کنیم $H \ltimes_\phi K$ که در آن $H$ و $K$ دو گروه و $\phi : H \longrightarrow \mathrm{Aut}(K)$ یک همریختی است. در این صورت $G$ زیر گروه نرمالی مانند $N$ و زیر گروهی مانند $M$ دارد که $M \cong H$ و $N \cong K$ به طوری که $G = MN$ و $M \cap N = 1$.*

***برهان.*** مرجع [پ] صفحه ۱۸۱. □

**قضیه ۱۴.۳.۱.** *فرض کنیم $G = H \ltimes_\phi K$، که در آن $H$ و $K$ دو گروه و $\phi : H \longrightarrow \mathrm{Aut}(K)$ یک همریختی است. به علاوه فرض کنیم $\tilde{H} = \{(h,1) : h \in H\}$. در این صورت $\tilde{H} \lhd G$ اگر و تنها اگر $\phi$ همریختی بدیهی باشد.*

***برهان.*** مرجع [پ] صفحه ۱۸۲. □

**نتیجه ۱۵.۳.۱.** *فرض کنیم $G = H \ltimes_\phi K$، که در آن $\phi : H \longrightarrow \mathrm{Aut}(K)$ یک همریختی غیر بدیهی است. در این صورت $G$ غیر آبلی است.*

***برهان.*** مرجع [پ] صفحه ۱۸۲. □

**مثال ۱۶.۳.۱.** فرض کنیم $G$ گروهی مرتبه ۳ و $H$ گروه دوری مرتبه ۷ است. قرار می‌دهیم :

$$G =< g \ : \ g^{۳} = ۱ > \ , \ H =< x \ : \ x^{۷} = ۱ >$$

برای تعریف عمل $G$ روی $H$ کافی است $x^g$ را تعریف کنیم. اگر قرار دهیم $x^g = x$ آن‌گاه عمل $G$ روی $H$ بدیهی است (خود ریختی همانی است) پس داریم $G \ltimes H = G \times H$. برای تعریف عمل دیگری از $G$ روی $H$ باید $x^g$ عضو دیگری از $H$ به جز $x$ باشد.
قرار می‌دهیم $x^g = x^n$ که $۱ < n < ۷$. بنا به تعریف باید داشته باشیم $x = x^{۱}$ و در نتیجه

$$x^{g^{۲}} = (x^g)^g = (x^n)^g = x^{n^{۲}}$$
$$x^{g^{۳}} = (x^{g^{۲}})^g = (x^{n^{۲}})^g = x^{n^{۳}}$$

$$\Rightarrow \ x^{۱} = x^{n^{۳}} \ \Rightarrow \ x = x^{n^{۳}} \ \Rightarrow \ x^{n^{۳}-۱} = ۱ \ \Rightarrow \ ۷ \mid (n^{۳} - ۱) \ \Rightarrow \ n = ۲, ۴.$$

بنابراین با تعریف $x^g = x^{۲}$ یا $x^g = x^{۴}$ یا

$$f \ : \ H \longrightarrow H \qquad f \ : \ H \longrightarrow H$$
$$x \longmapsto x^{۴} \qquad x \longmapsto x^{۲}$$

می‌توان حاصل‌ضرب نیم مستقیم $G \ltimes H$ را تشکیل داد که در هر دو حالت، گروه ناآبلی از مرتبه ۲۱ حاصل می‌شود.

**قضیه ۱۷.۳.۱.** *فرض کنیم $H$ و $K$ زیر گروه‌هایی از گروه $G$ باشند به طوری که $K \lhd G$ ، $G = HK$ و $H \cap K = ۱$. در این صورت $G \cong H \ltimes_\phi K$ ، که در آن $\phi \ : \ H \longrightarrow \mathrm{Aut}(K)$ یک همریختی است.*

***برهان.*** مرجع [پ] صفحه ۱۸۵. □

**قضیه ۱۸.۳.۱.** *فرض کنیم $H$ یک گروه دوری از مرتبه عدد اول $p$ و $K$ یک گروه دلخواه باشد. به علاوه فرض کنیم $\phi$ و $\psi$ دو همریختی از $H$ بتوی $\mathrm{Aut}(K)$ باشند به طوری‌که $Im\phi$ و $Im\psi$ در $\mathrm{Aut}(K)$ مزدوج باشند. در این‌صورت*

$$H \ltimes_\phi K \cong H \ltimes_\psi K.$$

***برهان.*** مرجع [پ] صفحه ۱۸۶. □

**قضیه ۱۹.۳.۱.** *فرض کنیم $H$ یک گروه دوری و $K$ یک گروه دلخواه باشد. به علاوه فرض کنیم $\phi \ : \ H \longrightarrow \mathrm{Aut}(K)$ و $\psi \ : \ H \longrightarrow \mathrm{Aut}(K)$ دو تکریختی باشند. در این صورت اگر $\mathrm{Im}\phi = \mathrm{Im}\psi$ ، آن‌گاه $H \ltimes_\phi K \cong H \ltimes_\psi K$.*

***برهان.*** مرجع [پ] صفحه ۱۸۷. □

**قضیه ۲۰.۳.۱.** *فرض کنیم $p$ و $q$ دو عدد اول باشند به طوری که $p < q$. در این صورت*

*الف) اگر* $p \nmid (q-1)$، *آن‌گاه تنها یک گروه از مرتبه* $pq$ *وجود دارد که دوری است.*

*ب) اگر* $p \mid (q-1)$، *آن‌گاه تنها دو گروه از مرتبه* $pq$ *وجود دارد. گروه دوری از مرتبه* $pq$ *و گروه* $G$ *با نمایش* $< x, y \ : \ x^p = y^q = 1 \ , \ x^{-1}yx = y^r >$ *که در آن* $r$ *عدد طبیعی که* $1 < r < q$، $(r,p) = 1$ *و* $r^p \equiv 1 \pmod{q}$.

***برهان.*** مرجع [پ] صفحه ۱۹۰. □

**قضیه ۲۱.۳.۱.** *فرض کنیم* $G$ *گروهی متناهی و* $K$ *زیرگروه نرمال از آن باشد، به طوری‌که* $(|K| \ , \ [G \ : \ K]) = 1$، *در این صورت* $G$ *زیرگروهی از مرتبه* $[G \ : \ K]$ *دارد.*

***برهان.*** مرجع [پ] صفحه ۱۹۵. □

**نتیجه ۲۲.۳.۱.** *اگر* $G$ *یک گروه متناهی و* $K$ *زیرگروهی نرمال از آن باشد به طوری‌که* $(|K| \ , \ [G \ : \ K]) = 1$، *آن‌گاه* $G$ *زیرگروهی مانند* $H$ *دارد به طوری‌که*

$$G \cong H \ltimes K.$$

***برهان.*** مرجع [پ] صفحه ۱۹۸. □

## ۴.۱ گروه خود ریختی‌ها

در این بخش خواصی از خود ریختی‌ها بخصوص خود ریختی گروه‌های دوری را مورد مطالعه قرار می‌دهیم.

**قضیه ۱.۴.۱.** *فرض کنیم* $G = H \times K$ *تجزیه‌ای از* $G$ *به حاصل‌ضرب مستقیم دو زیرگروه نرمالش باشد. اگر* $G$ *متناهی باشد و* $(|H| \ , \ |K|) = 1$، *آن‌گاه*

$$\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(G)$$

***برهان.*** در مرجع [ب] صفحه ۱۴۲. □

**قضیه ۲.۴.۱.** *فرض کنیم* $G$ *یک گروه متناهی باشد و* $\{P_1, ..., P_n\}$ *مجموعه همه زیرگروه‌های سیلو دو به دو متمایز* $G$ *باشد. در این‌صورت اگر* $G = P_1 \times ... \times P_n$، *آنگاه* $\mathrm{Aut}(G) \cong \mathrm{Aut}(P_1) \times ... \times \mathrm{Aut}(P_n)$.

***برهان.*** مرجع [ب] صفحه ۱۴۳. □

**ملاحظه ۳.۴.۱.** *فرض کنیم* $G$ *یک گروه دوری از مرتبه* $n$ *باشد و* $n = p_1^{k_1} ... p_m^{k_m}$ *که در آن* $p_i$*ها اعداد اول دو به دو متمایزند و* $k_i$*ها اعداد طبیعی‌اند. به موجب قضیه قبل داریم :*

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(C_{p_1^{k_1}}) \times ... \mathrm{Aut}(C_{p_m^{k_m}}).$$

**تعریف ۴.۴.۱.** فرض کنیم $m$ یک عدد طبیعی بزرگتر از یک باشد. در این‌صورت مجموعه همه اعداد طبیعی مانند $n$ را که $n < m$ و $n$ ، $m$ متباین‌اند $U(m)$ می‌نامیم.
مجموعه $U(m)$ با عمل ضرب اعداد طبیعی به پیمانه $m$ یک گروه آبلی تشکیل می‌دهد. این گروه را با همان علامت $U(m)$ نشان می‌دهیم. مرتبه این گروه برابر است با $\phi(m)$ که در آن $\phi$ تابع ضربی اویلر است.

**قضیه ۵.۴.۱.** *فرض کنیم $G$ یک گروه دوری غیر بدیهی از مرتبه $m$ باشد. در این‌صورت $\mathrm{Aut}(G) \cong U(m)$.*

***برهان.*** مرجع [ب] صفحه ۱۴۵. □

**قضیه ۶.۴.۱.** *به ازای هر عدد اول $p$، گروه $U(p)$ دوری از مرتبه $p-1$ است.*

***برهان.*** مرجع [ب] صفحه ۱۴۵. □

**قضیه ۷.۴.۱.**

*الف) اگر $P$ یک عدد اول فرد باشد آن‌گاه به ازای هر $k$ طبیعی،*

$$\mathrm{Aut}(C_{p^k}) \cong U(p^k) \cong C_{p^{k-1}(p-1)}$$

*ب) به ازای $k$ طبیعی که $k > 1$،*

$$\mathrm{Aut}(C_{2^k}) \cong U(2^k) \cong C_2 \times C_{2^{k-2}}.$$

***برهان.*** مرجع [ب] صفحه ۱۴۶. □

**مثال ۸.۴.۱.** ساختار گروه $Aut(C_{60})$ به صورت زیر است.

$$\mathrm{Aut}(C_{60}) \cong \mathrm{Aut}(C_{22}) \times \mathrm{Aut}(C_3) \times \mathrm{Aut}(C_5) \cong C_2 \times C_2 \times C_2 \times C_{20}$$

**قضیه ۹.۴.۱.** *فرض کنیم $G$ یک گروه آبلی متناهی باشد. در این‌صورت $\mathrm{Aut}(G)$ آبلی است اگر وتنها اگر $G$ دوری باشد.*

***برهان.*** مرجع [ب] صفحه ۱۴۷. □

## ۵.۱ گروه جایگشتی

**تعریف ۱.۵.۱.** جایگشت. فرض کنید $\Omega$ یک مجموعه است. هر نگاشت دو سویی از $\Omega$ به $\Omega$ یک جایگشت روی $\Omega$ نامیده می‌شود.
اگر $f$ و $g$ نیز جایگشت‌هایی از $\Omega$ فرض شوند، آن‌گاه ترکیب آن‌ها یعنی $gof$ نیز جایگشتی از $\Omega$ است.
مجموعه همه جایگشت‌های $\Omega$ با ترکیب توابع تشکیل یک گروه می‌دهند. این گروه را گروه تقارن مجموعه $\Omega$ نامیده با $S_\Omega$ نمایش می‌دهیم.

در حالتی که $\Omega$ یک مجموعه متناهی $n$ عضوی باشد به منظور سادگی، $S_\Omega$ را با $S_n$ نمایش می‌دهیم و آن را گروه متقارن درجه $n$ می‌نامیم.

**قضیه ۲.۵.۱.** *اگر $\Omega$ و $\Gamma$ مجموعه‌های هم کاردینال باشند، آن‌گاه $S_\Omega \cong S_\Gamma$ .*

***برهان.*** مرجع [ب] صفحه ۸۸.

□

**تعریف ۳.۵.۱.** فرض کنید $\alpha \in S_n$.

الف) گوییم $w \in \Omega$ توسط $\alpha$ ثابت نگه داشته می‌شود هرگاه $(w)\alpha = w$،

ب) اگر برای $w \in \Omega$ داشته باشیم $(w)\alpha \neq w$، آن‌گاه گوییم $w$ توسط $\alpha$ حرکت داده می‌شود،

پ) جایگشت‌های $\alpha$ و $\beta$ از $S_n$، مجزا نامیده می‌شوند، هرگاه هیچ عضو $\Omega$ توسط هر دوی $\alpha$ و $\beta$ حرکت داده نشود.

**قضیه ۴.۵.۱.** *هر دو جایگشت مجزای $S_n$ با هم جابجا می‌شوند.*

***برهان.*** مرجع [ب] صفحه ۸۹. □

**قضیه ۵.۵.۱.** *هر جایگشت در $S_n$ مساوی حاصل‌ضربی از دورهای دو به دو مجزا است و این حاصل‌ضرب قطع نظر از وجود دورهای به طول ۱ و ترتیب دورها، منحصر به فرد است.*

***برهان.*** مرجع [ب] صفحه ۹۱. □

**تعریف ۶.۵.۱.** اگر $a, b \in \Omega$ و $a \neq b$، آن‌گاه دور $(ab)$ به طول ۲ یک ترانهش نامیده می‌شود.

**قضیه ۷.۵.۱.** *هر جایگشت مانند $\alpha$ از $S_n$ را می‌توان به حاصل‌ضربی (متناهی) از ترانهش‌ها تجزیه نمود.*

***برهان.*** مرجع [پ] صفحه ۱۱. □

**تعریف ۸.۵.۱.** جایگشت $\pi$ از $S_n$ را زوج نامیم، هرگاه تعداد ترانهش‌هایی که در هر تجزیه $\pi$ به ترانهش ظاهر می‌شود زوج باشد.

**تعریف ۹.۵.۱.** مجموعه کلیه جایگشت‌های زوج $S_n$ $(n \geq ۲)$ یک گروه از مرتبه $\frac{n!}{۲}$ تشکیل می‌دهد. این گروه را گروه متناوب درجه $n$ نامیده و با $A_n$ نمایش می‌دهیم.

**تعریف ۱۰.۵.۱.** افراز یک عدد. یک افراز عدد طبیعی عبارت از دنباله $(\lambda_۱, \lambda_۲, ..., \lambda_k)$ از اعداد طبیعی به طوری که:

$$\lambda_۱ + \lambda_۲ + ... + \lambda_k = n,$$

$$\lambda_۱ \geq \lambda_۲ \geq ... \geq \lambda_k.$$