دانشگاه زنجان

دانشکده علوم - گروه ریاضی

پایان نامه ی کارشناسی ارشد

عنوان:

# مجموع مرتبه ی عناصر گروه های متناهی از مرتبه ی یکسان

نگارش:

سمیه رحمت آبادی

استاد راهنمای اول:

دکتر سید مجید جعفریان امیری

استاد راهنمای دوم:

دکتر حبیب امیری

شهریور ۹۱

بسم الله الرحمن الرحیم

تقدیم به پدر فداکار

و

مادر مهربانم

# تقدیر و تشکر

ناخواسته در مسیری گام نهادم به نام زندگی. مسیری پر پیچ و خم و پر از فراز و نشیب. اما هرگز هراسی نداشتم چون دستانم را محکم در دستان گرم وجودی مهربان به نام پدر و مادر فشرده و آسوده و آرام این مسیر تاریک و بی انتها را طی می کردم. اما تقدیر برای فرصتی هرچند کوتاه، میان این دست ها فرسنگ ها فاصله انداخت و تنها و سرگردان مرا در این مسیر مبهم رها کرد. اما شکر و سپاس بی کران، ایزد یکتا را که در این فرصت، کسانی را در مسیر زندگی من قرار داد که به من آموختند زندگی یعنی گاهی باید فاصله ها را تحمل کرد، گاهی باید صبورانه مشکلات و سختی ها را پشت سر گذاشت و هرگز نباید فراموش کرد که همیشه باید یک انسان بود حتی اگر گاهی خیلی سخت باشد. اینان کسانی هستند که هرگز از یاد و خاطرم فراموش نخواهند شد و برای همیشه در ذهن من حک خواهند شد و این فرصت شاید تنها فرصتی باشد که بتوانم با ذکر نام این عزیزان ذره ای از محبت های بی دریغشان را جبران کنم، اساتید گرانقدر دکتر مسعود آرین نژاد و دکتر مجید حیدرپور که با رفتار و کلام خود به من درس زندگی آموختند. همچنین از اساتید راهنمای بزرگوارم دکتر سید مجید جعفریان امیری و دکتر حبیب امیری کمال تشکر را دارم که بی شک بدون راهنمایی های دلسوزانه ی آنان این پایان نامه هرگز به اتمام نمی رسید. در ادامه صمیمانه از جناب آقای محسن امیری تشکر می کنم که در مدت این دو سال همواره از کمک های بی دریغ ایشان بهره برده ام.

همچنین از خواهر نازنینم و خانواده ی محترمشان که با حضور خود در کنارم رنج دوری از خانواده را برای من آسان نمودند بسیار سپاس گذارم. از هم اتاقی های عزیزم خانم ها: صادق آبادی، سهرابی، اربابیان، شهباز نژاد و محمدی که همواره در تمامی سختی ها و مشکلات در کنارم بودند کمال تشکر را دارم.

# چکیده

فرض کنید $G$ گروهی متناهی و $\psi(G)$ نشان دهنده‌ی مجموع مرتبه‌ی عناصر گروه $G$ باشد. ماکسیمم مقدار $\psi$ روی همه‌ی گروه‌های از مرتبه‌ی $n$، به‌طوری‌که $n$ عدد صحیح مثبتی است در گروه‌های دوری اتفاق می‌افتد. همچنین اگر گروه غیرپوچتوانی از مرتبه‌ی $n$ موجود باشد، آن‌گاه مینیمم مقدار $\psi$ در یک گروه غیرپوچتوان اتفاق می‌افتد. همچنین در ادامه برخی از ویژگی‌های مجموع مرتبه‌ی عناصر گروه‌های آبلی متناهی را بررسی می‌کنیم.

**واژه‌های کلیدی:** *گروه‌های متناهی، مرتبه‌ی عناصر گروه، گروه‌های پوچتوان.*

# فهرست مطالب

# پیشگفتار

مفهوم گروه یکی از مهم‌ترین مفاهیم در ریاضیات است. با وجودی که حتی از زمان‌های گذشته، در قالب تقارن اشکال هندسی و حرکت در فضا، بشر با این مفهوم آشنا بوده است. اما تشخیص آن به‌عنوان یک موضوع جبری از نیمه‌ی اول قرن نوزدهم میلادی میسر شد. نظریه‌ی گروه‌ها بخش مهمی از جبر مجرد را دربر می‌گیرد که در نظریه‌ی تبلور در شیمی، در فیزیک کوانتوم، در نظریه‌ی کنترل و اقتصاد کاربرد دارد. به‌علاوه در چندین شاخه‌ی ریاضیات مانند توپولوژی، هندسه دیفرانسیل، نظریه‌ی نمایش و جبر لی به‌صورت طبیعی و ضروری به‌کار گرفته می‌شود.

گروه‌ها از نظر تعداد اعضای خود، به دو دسته‌ی متناهی و نامتناهی تقسیم بندی می‌شوند. گروه‌های متناهی گروه‌هایی هستند که تعداد اعضای آن‌ها متناهی و گروه‌های نامتناهی گروه‌هایی هستند که تعداد اعضای آن‌ها نامتناهی می‌باشد. هر عضو از گروه نیز دارای ویژگی به‌نام مرتبه می‌باشد که در فصل اول این پایان نامه به‌طور مفصل درباره‌ی مرتبه‌ی یک عضو از گروه توضیح داده شده و مثال‌هایی نیز در این زمینه ارائه شده است.

اکنون اگر از میان تمام گروه‌ها، گروه‌های متناهی را در نظر بگیریم که مرتبه‌ی آن‌ها یکسان می‌باشند و مرتبه‌ی تمامی عناصر هر گروه را با یکدیگر جمع کنیم لزوماً مقادیر یکسانی را به دست نمی‌آوریم. همین مسأله موجب شد که دکترحبیب امیری، دکتر سید مجید جعفریان امیری و پروفسور ایزاک در مقاله‌ای با عنوان « مجموع مرتبه‌ی عناصر گروه‌های متناهی از مرتبه‌ی یکسان » تابعی به‌نام $\psi$ را معرفی کنند. این تابع به ازای هر گروه متناهی، مرتبه‌ی تمامی عناصر گروه را با یکدیگر جمع می‌کند. سپس مقدار تابع $\psi$ را به ازای تعداد زیادی از گروه‌های متناهی هم‌مرتبه محاسبه کردند و به این نتیجه رسیدند که ماکزیمم مقدار تابع $\psi$ از میان گروه‌های متناهی هم‌مرتبه، به ازای گروه‌های دوری اتفاق می‌افتد. به‌عبارتی دیگر اگر $C$ یک گروه دوری از مرتبه‌ی $n$ باشد، آن‌گاه به ازای همه‌ی گروه‌های غیردوری $G$ از مرتبه‌ی $n$ خواهیم داشت $\psi(G) < \psi(C)$.

اکنون به‌طور طبیعی سوال دیگری مطرح می‌شد و آن این بود که از میان گروه‌های متناهی هم‌مرتبه، مینیمم مقدار تابع $\psi$ به ازای چه گروه‌هایی اتفاق می‌افتد؟

برای رسیدن به پاسخی برای این سوال، مجدداً تلاش‌ها ادامه پیدا کرد. تا این‌که پس از بررسی‌های انجام شده روی گروه‌های جدید و همچنین گروه‌های بررسی شده‌ی قبلی سرانجام به این نتیجه دست یافتند که تابع معرفی شده‌ی $\psi$ از میان تمامی گروه‌های متناهی هم‌مرتبه، در صورتی‌که گروهی غیرپوچتوان از آن مرتبه موجود باشد، مینیمم مقدار خود را به ازای گروههای غیرپوچتوان اختیار می‌کند. به‌عبارتی دیگر اگر گروهی غیرپوچتوان از مرتبه‌ی $n$ موجود باشد، آن‌گاه گروهی غیرپوچتوان مانند $K$ موجود است به‌طوری‌که به ازای همه‌ی گروه‌های پوچتوان از مرتبه‌ی $n$ مانند$H$ خواهیم داشت $\psi(K) < \psi(H)$.

تارناوسونو [1] و فودور [2] روشی کلی برای محاسبه‌ی مجموع مرتبه‌ی عناصر $p-$گروه‌های آبلی متناهی ارائه و برخی دیگر از ویژگی‌های تابع معرفی شده‌ی $\psi$ را بیان و اثبات کردند.

در این پایان نامه سعی شده است تا با بیان تمامی جزئیات و با ساده‌ترین روشها همه‌ی مراحل طی‌شده برای دست یافتن به چنین نتایج مهمی را بیان و اثبات کنیم.

در فصل اول به بیان همه‌ی تعاریف و قضایای استفاده شده جهت یادآوری و همچنین اثبات برخی از قضایای مقدماتی اما مهم و اساسی می‌پردازیم. در فصل دوم به بررسی این مطلب می‌پردازیم که تابع معرفی شده‌ی $\psi$، ماکزیمم مقدار خود را از میان گروه‌های متناهی هم‌مرتبه به ازای کدام گروه‌ها اختیار خواهد کرد. در فصل سوم از این پایان نامه به این سوال پاسخ خواهیم داد که مینیمم مقدار $\psi$، از میان همه‌ی گروه‌های متناهی هم‌مرتبه به ازای کدام گروه‌ها اتفاق خواهد افتاد. در فصل چهارم، فرمولی کلی برای محاسبه‌ی مجموع مرتبه‌ی عناصر $p-$گروه‌های آبلی متناهی ارائه و برخی دیگر از ویژگی‌های $\psi$ را برای این گروه‌ها بیان می‌کنیم.

سمیه رحمت آبادی

شهریور ۱۳۹۱

[1] Tarnauceanu
[2] fodor

# فصل ۱

# تعاریف و قضایای مقدماتی

**تعریف ۱.۱.** *فرض کنید $G$ یک گروه باشد. اگر $G$ شامل تعداد متناهی عضو باشد، آن‌گاه تعداد اعضای $G$ را مرتبه‌ی $G$ می‌نامیم. در غیر این‌صورت $G$ را از مرتبه‌ی نامتناهی گوییم. مرتبه‌ی $G$ را معمولاً با نماد $|G|$ نمایش می‌دهیم.*

**مثال ۱.** گروه جمعی $(\mathbb{Z}_n, \oplus)$ گروهی متناهی و از مرتبه‌ی $n$ می‌باشد و گروه‌های $(\mathbb{Z}, +)$، $(\mathbb{Q}, +)$، $(\mathbb{R}, +)$ و $(\mathbb{C}, +)$ گروه‌هایی نامتناهی هستند.

**تعریف ۲.۱.** *فرض کنید $G$ یک گروه و $x \in G$ باشد.کوچک‌ترین عدد صحیح مثبت $n$ که در رابطه‌ی $x^n = e$ صدق می‌کند را مرتبه‌ی $x$ می‌نامیم و با نماد $o(x) = n$ نمایش می‌دهیم. اگر چنین $n$ای موجود نباشد، گوییم $x$ از مرتبه‌ی نامتناهی است و با نماد $o(x) = \infty$ نمایش می‌دهیم.*

**مثال ۲.** اگر گروه $(\mathbb{Z}, +)$ را در نظر بگیریم، آن‌گاه $o(۱) = \infty$. زیرا

$$۱ \neq ۰ \ , \ \ ۱ + ۱ \neq ۰ \ , \ \ ۱ + ۱ + ۱ \neq ۰ \ , \ \ \ldots$$

**قضیه ۳.۱.** فرض کنید $G$ یک گروه و $x \in G$ باشد. در این‌صورت

الف) اگر $o(x) = n$ و $x^m = e$، آن‌گاه $n \mid m$.

ب) اگر $o(x) = n$ و $(m, n) = d$، آن‌گاه $o(x^m) = \frac{n}{d}$.

**برهان .** به قضیه‌ی (۴.۴) از مرجع [۱۲] مراجعه کنید. □

**تعریف ۴.۱.** فرض کنید $H$ زیر گروهی از گروه $G$ و $a \in G$ باشد. در این‌صورت

$$aH = \{ah \mid h \in H\}$$

هم‌مجموعه‌ی[۱] چپ $H$ در $G$ نامیده می‌شود. به‌طور مشابه

$$Ha = \{ha \mid h \in H\}$$

هم‌مجموعه‌ی راست $H$ در $G$ نامیده می‌شود.

**قضیه ۵.۱.** فرض کنید $H$ زیرگروهی از گروه $G$ باشد و $a, b \in G$. در این‌صورت عبارت‌های زیر معادل می‌باشند.

الف) $Ha = Hb$.

ب) $h \in H$ وجود دارد به‌طوری‌که $b = ha$.

ج) $b \in Ha$.

د) $ba^{-1} \in H$.

**برهان .** به قضیه‌ی (۱۵.۴) از مرجع [۱۲] مراجعه کنید. □

**تذکر ۶.۱.** فرض کنید $H$ زیر گروهی از گروه $G$ باشد. در این‌صورت هم‌مجموعه‌های راست (چپ) $H$ در $G$ یا برابر هستند و یا اشتراک آن‌ها تهی است. به‌عبارت دیگر افرازی برای $G$ می‌باشند.

[۱] Coset

**لم ۷.۱.** فرض کنید $H$ زیر گروهی از گروه متناهی $G$ باشد. در این‌صورت تعداد عناصر متمایز در هر هم‌مجموعه‌ی $H$ در $G$ دقیقاً برابر است با تعداد اعضای $H$. به‌عبارتی دیگر اگر $G$ یک گروه و $a \in G$ و $H$ زیر گروهی از گروه $G$ باشد، آن‌گاه

$$|H| = |Ha| = |aH|.$$

**برهان .** به قضیه‌ی (۳.۹) از مرجع [۱۲] مراجعه کنید. □

**قضیه ۸.۱.** (لاگرانژ[۱]) فرض کنید $H$ زیرگروهی از گروه متناهی $G$ باشد. در این‌صورت مرتبه‌ی $H$، مرتبه‌ی گروه $G$ را عاد می‌کند. در واقع

$$|G| = |G:H||H|.$$

به‌عبارتی دیگر اگر $G$ گروهی متناهی باشد، آن‌گاه مرتبه‌ی $G$ برابر است با حاصل‌ضرب شاخص $H$ در $G$، در مرتبه‌ی $H$.

**برهان .** به قضیه‌ی (۱۰.۴) از مرجع [۱۰] مراجعه کنید. □

**تذکر ۹.۱.** عکس قضیه‌ی لاگرانژ لزوماً برقرار نیست. به‌عبارتی دیگر اگر $G$ گروهی متناهی باشد و عدد صحیح مثبت $m$ موجود باشد به‌طوری‌که $m \mid |G|$، آن‌گاه $G$ لزوماً زیر گروهی از مرتبه‌ی $m$ ندارد.

**مثال ۳.** فرض کنید $G = A_۴$. در این‌صورت $|G| = |A_۴| = ۱۲$ و $۶ \mid ۱۲$. در صورتی‌که $A_۴$ زیرگروهی از مرتبه‌ی ۶ ندارد.

**تذکر ۱۰.۱.** عکس قضیه‌ی لاگرانژ در مورد گروه‌های آبلی برقرار می‌باشد.

**قضیه ۱۱.۱.** فرض کنید $G$ یک گروه آبلی متناهی و $k$ عدد صحیح مثبتی باشد به‌طوری‌که $k \mid |G|$. در این‌صورت $G$ دارای زیرگروهی از مرتبه‌ی $k$ می‌باشد.

**برهان .** به قضیه‌ی (۵.۲۰) از مرجع [۸] مراجعه کنید. □

[۱] Lagrange

**تعریف ۱.۱۲.** گروه $G$ را یک گروه دوری می‌نامیم، هرگاه $G$ توسط یکی از اعضای خود تولید شده باشد. به‌عبارتی دیگر $x \in G$ موجود باشد به‌طوری‌که $G = \langle x \rangle$.

**تعریف ۱.۱۳.** فرض کنید $G$ یک گروه و $M$ زیرمجموعه‌ای غیرتهی از $G$ باشد. در این‌صورت کوچک‌ترین زیرگروه $G$ که $M$ را دربر داشته باشد، زیرگروه تولیدشده توسط $M$ می‌نامیم و با نماد $\langle M \rangle$ نمایش می دهیم. در حالتی‌که $G = \langle M \rangle$، آن‌گاه $M$ را یک مجموعه‌ی مولد $G$ می‌نامیم.

**قضیه ۱.۱۴.** فرض کنید $G$ یک گروه و $M$ زیرمجموعه‌ای غیرتهی از $G$ باشد. در این‌صورت

$$\langle M \rangle = \{x_۱^{\alpha_۱} x_۲^{\alpha_۲} ... x_n^{\alpha_n} \mid x_i \in M, \alpha_i \in \mathbb{Z}, n = ۱, ۲, ...\}.$$

**برهان .** به قضیه‌ی (۶.۴) از مرجع [۱۰] مراجعه کنید. □

**قضیه ۱.۱۵.** هر زیرگروه از یک گروه دوری، دوری می‌باشد.

**برهان .** به قضیه‌ی (۲.۵) از مرجع [۱۲] مراجعه کنید. □

**قضیه ۱.۱۶.** اگر $G$ گروهی دوری باشد، آن‌گاه $G$ آبلی است.

**برهان .** به قضیه‌ی (۷.۴) از مرجع [۱۲] مراجعه کنید. □

**تذکر ۱.۱۷.** عکس قضیه‌ی فوق لزوماً برقرار نیست. به عنوان مثال گروه $(\mathbb{Q}, +)$ گروهی آبلی است. اما دوری نمی‌باشد.

**قضیه ۱.۱۸.** فرض کنید $G = \langle x \rangle$. در این‌صورت خواهیم داشت $|G| = o(x)$.

**برهان .** به قضیه‌ی (۳.۱۶) از مرجع [۸] مراجعه کنید. □

**تعریف ۱.۱۹.** گروه دووجهی [۱] از مرتبه‌ی $n$، یک گروه غیرآبلی از مرتبه‌ی $2n$ به‌صورت زیر می‌باشد.

$$D_n = \langle \alpha, \beta \mid \alpha^n = \beta^2 = 1, \beta\alpha\beta = \alpha^{-1} \rangle.$$

**تعریف ۱.۲۰.** گروه کواترنیون [۲] یک گروه غیرآبلی از مرتبه‌ی ۸ به‌صورت زیر می‌باشد.

$$Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = -1, ijk = -1 \rangle.$$

**تعریف ۱.۲۱.** فرض کنید $H$ و $K$ دو گروه آبلی باشند و $G = Q_8 \times H \times K$. در این‌صورت اگر هر عضو غیربدیهی $H$ از مرتبه‌ی ۲ و هر عضو غیربدیهی $K$ از مرتبه‌ی فرد باشد، آن‌گاه هر زیرگروه $G$ نرمال است. چنین گروه‌هایی را همیلتنی [۳] می‌نامیم.

**تعریف ۱.۲۲.** فرض کنید $G$ یک گروه و $H$ زیر مجموعه‌ای ناتهی از $G$ باشد. در این‌صورت مجموعه‌ی زیر را مرکزساز $H$ در $G$ می‌نامیم.

$$C_G(H) = \{g \in G \mid \forall x \in H, \quad gx = xg\}.$$

در حالتی‌که $H = \{h\}$ زیرمجموعه‌ای تک عضوی از $G$ باشد، آن‌گاه به‌جای $C_G(\{h\})$ به اختصار می‌نویسیم $C_G(h)$ و آن را مرکز ساز $h$ در $G$ می‌نامیم. بنابراین $C_G(h)$ شامل همه‌ی اعضایی از $G$ می‌باشد که با $h$ جابه‌جا می‌شوند.

**قضیه ۱.۲۳.** اگر $G$ یک گروه و $H \subseteq G$ و $H \neq \varnothing$ باشد، آن‌گاه $C_G(H)$ زیرگروهی از $G$ است.

**برهان .** به قضیه‌ی (۴.۴) از مرجع [۱۰] مراجعه کنید. $\square$

[۱] Dihedral Group

[۲] Quaternion Group

[۳] Hamiltonian Group

**تعریف ۲۴.۱.** اگر $G$ یک گروه باشد، آن‌گاه مجموعه‌ی زیر را مرکز گروه $G$ می‌نامیم.

$$Z(G) = C_G(G) = \{g \in G \mid \forall x \in G, \quad gx = xg\}.$$

**قضیه ۲۵.۱.** فرض کنید $G$ گروهی دلخواه و $Z(G)$ مرکز آن باشد. در این‌صورت اگر گروه خارج‌قسمتی $G/Z(G)$ دوری باشد، آن‌گاه $G$ گروهی آبلی است.

**برهان .** به تمرین (۲ .۴۳) از مرجع [۱۱] مراجعه کنید. □

**تعریف ۲۶.۱.** اگر $G$ یک گروه و $H$ زیرمجموعه‌ای غیرتهی از $G$ باشد، آن‌گاه مجموعه‌ی زیر را نرمال‌ساز $H$ در $G$ می‌نامیم.

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

در حالتی‌که $H = \{x\}$ زیر مجموعه‌ای تک عضوی از $G$ باشد، واضح است که $N_G(H) = C_G(H)$ می‌باشد.

**تعریف ۲۷.۱.** فرض کنید $G$ یک گروه و $p$ عددی اول باشد. در این‌صورت اگر مرتبه‌ی هر عضو $G$ به صورت توانی از عدد اول $p$ باشد، آن‌گاه $G$ را یک $p-$گروه می‌نامیم.

**تعریف ۲۸.۱.** گوییم $p-$گروه آبلی متناهی $G$، آبلی مقدماتی است، درصورتی‌که مرتبه‌ی هر عضو غیربدیهی گروه $G$، عدد اول $p$ باشد.

**تعریف ۲۹.۱.** فرض کنید $G$ گروهی متناهی باشد به‌طوری‌که $|G| = p^\alpha m$ که در آن $p$ عددی اول، $m \geq 1$، $\alpha \geq 0$ و $(p, m) = 1$ باشند. در این‌صورت هر زیرگروه از مرتبه‌ی $p^\alpha$ یک $p-$زیرگروه سیلوی[1] $G$ نامیده می‌شود. در واقع تعریف فوق ایجاب می‌کند که اگر $P$ یک $p-$زیرگروه سیلوی $G$ باشد، آن‌گاه $|G : P|$

[1] sylow

نسبت به $p$ اول و مرتبه‌ی $P$ نیز توانی از عدد اول $p$ باشد. این به آن معنا است که مرتبه‌ی $P$ بزرگ‌ترین توانی از عدد اول $p$ می‌باشد که مرتبه‌ی گروه $G$ را عاد می‌کند. مجموعه‌ی تمام $p-$زیرگروه‌های سیلوی گروه $G$ را با نماد $Syl_p(G)$ نمایش می‌دهیم.

**مثال ۴.** گروه متناوب[۱] $A_۴$ را در نظر بگیرید. $|A_۴| = ۲^۲ \times ۳$. بنابراین مرتبه‌ی یک ۲$-$زیرگروه سیلوی $A_۴$ در صورت وجود چهار و مرتبه‌ی یک ۳$-$زیرگروه سیلوی $A_۴$ در صورت وجود سه است.

حال اگر مجموعه‌ی زیر را در نظر بگیریم

$$P = \{e, (۱\ ۲)(۳\ ۴), (۱\ ۳)(۲\ ۴), (۱\ ۴)(۲\ ۳)\},$$

آن‌گاه $P$ زیرگروهی از $A_۴$ و $|P| = ۴$ می‌باشد. بنابراین $P \in Syl_p(A_۴)$. همچنین اگر قرار دهیم

$$Q = \{e, (۱۲۳), (۱۴۲)\},$$

آن‌گاه $Q$ زیرگروهی از $A_۴$ و $|Q| = ۳$ می‌باشد. در نتیجه $Q$ یک ۳$-$زیرگروه سیلوی $A_۴$ است.

**قضیه ۳۰.۱.** به ازای هر عدد اول $p$، گروه متناهی و دلخواه $G$ دارای حداقل یک $p-$زیرگروه سیلو می‌باشد.

**قضیه ۳۱.۱.** (کشی[۲]) اگر $G$ گروهی متناهی و $p$ عددی اول باشد به‌طوری‌که $p \mid |G|$، آن‌گاه $G$ عضوی از مرتبه‌ی $p$ دارد.

**برهان .** به نتیجه‌ی (۲.۹) از مرجع [۱۰] مراجعه کنید. □

**قضیه ۳۲.۱.** (قضیه‌ی سوم سیلو) فرض کنید $G$ گروهی متناهی و $p$ عددی اول باشد به‌طوری‌که $p \mid |G|$. در این‌صورت اگر $n_p(G)$ تعداد $p-$زیرگروه‌های سیلوی $G$ باشد، آن‌گاه

الف) $p \mid n_p(G) - ۱$.

ب) $n_p(G) \mid |G|$.

**برهان .** به قضیه‌ی (۱.۹) از مرجع [۱۰] مراجعه کنید. □

[۱] Alternating Group

[۲] Cauchy

**قضیه ۳۳.۱.** فرض کنید $G$ گروهی متناهی، $p \mid |G|$ و $p$ عددی اول باشد. دراین‌صورت $G$ تنها دارای یک $p-$زیرگروه سیلو مانند $P$ می‌باشد، اگر و تنها اگر $P \trianglelefteq G$ باشد.

**برهان .** به نتیجه‌ی (۵.۹) از مرجع [۱۰] مراجعه کنید. □

**تعریف ۳۴.۱.** اگر $G$ یک گروه و $x, y \in G$ باشند، آن‌گاه $[x, y] = x^{-۱}y^{-۱}xy$ را جابه‌جاگر $x, y$ می‌نامیم. زیرگروه $G$ تولید شده به‌وسیله‌ی تمام جابه‌جاگرهای اعضای $G$ را زیرگروه جابه‌جاگر $G$ می‌نامیم و آن را با نماد $G'$نمایش می‌دهیم. گاهی نیز $G'$ را زیر گروه مشتق شده از $G$ یا زیر گروه مشتق $G$ نیز می‌نامیم. به‌عبارت دیگر

$$G' = \langle\{[x, y] \mid x, y \in G\}\rangle.$$

**تعریف ۳۵.۱.** فرض کنید $G$ یک گروه و $H \leqslant G$ باشد. در این‌صورت $H$ را زیرگروه مشخصه‌ی $G$ می‌نامیم، هرگاه به ازای تمام خودریختی‌های $\varphi$ از $G$ داشته باشیم $\varphi(H) \leqslant H$.

**لم ۳۶.۱.** اگر $H$ زیرگروه مشخصه ای از گروه $G$ باشد، آن‌گاه به ازای تمام خودریختی‌های $\varphi$ از $G$ خواهیم داشت

$$\varphi(H) = H.$$

**برهان .** طبق فرض $H$ زیرگروه مشخصه‌ای از گروه $G$ می‌باشد، بنابراین $\varphi \in Aut(G)$ وجود دارد به‌طوری‌که

$$\varphi(H) \leqslant H. \qquad (۱.۱)$$

اکنون به دلیل این‌که $\varphi \in Aut(G)$ بنابراین $\varphi^{-۱} \in Aut(G)$. درنتیجه طبق تعریف زیرگروه مشخصه خواهیم داشت $\varphi^{-۱}(H) \leqslant H$. بنابراین به‌وضوح داریم $\varphi\varphi^{-۱}(H) \leqslant \varphi(H)$. درنتیجه

$$H \leqslant \varphi(H). \qquad (۲.۱)$$

بنابراین طبق روابط (۱.۱) و (۲.۱) داریم $\varphi(H) = H$. □

**قضیه ۱.۳۷.** اگر $G$ یک گروه باشد، آن‌گاه $Z(G)$ و $G'$ زیرگروه‌های مشخصه‌ی $G$ می‌باشند.

**برهان .** ابتدا ثابت می‌کنیم $Z(G)$ زیرگروه مشخصه‌ی $G$ است. برای این منظور چون $Z(G)$ و $\varphi(Z(G))$ زیرگروه‌هایی از $G$ می‌باشند، بنابراین کافی است ثابت کنیم $\varphi(Z(G)) \subseteq Z(G)$ است.
فرض کنید $\varphi \in Aut(G)$ و $g \in \varphi(Z(G))$. در این‌صورت می‌توان نوشت $g = \varphi(z)$ به طوری‌که $z \in Z(G)$. اگر $h \in G$ باشد، آن‌گاه به دلیل این‌که $\varphi$ پوشا است $k \in G$ وجود دارد به‌طوری‌که $\varphi(k) = h$. اکنون با توجه به این‌که $\varphi$ یک خودریختی از $G$ می‌باشد، بنابراین

$$gh = \varphi(z)\varphi(k) = \varphi(zk) = \varphi(kz) = \varphi(k)\varphi(z) = hg.$$

این به آن معنا است که $g$ با تمام اعضای $G$ جابه‌جا می‌شود. بنابراین $g \in Z(G)$. به این ترتیب ثابت می‌شود که $\varphi(Z(G)) \leqslant Z(G)$. یعنی $Z(G)$ زیرگروه مشخصه‌ی $G$ است
. اکنون ثابت می‌کنیم $G'$ زیرگروه مشخصه‌ی $G$ است. برای این منظور کافی است ثابت کنیم $\varphi(G') \subseteq G'$ است. فرض کنید $\varphi \in Aut(G)$ و $x \in G'$ باشد. در این‌صورت داریم

$$x = (x_۱^{-۱}y_۱^{-۱}x_۱y_۱)(x_۲^{-۱}y_۲^{-۱}x_۲y_۲)...(x_n^{-۱}y_n^{-۱}x_ny_n).$$

همچنین به دلیل همریختی بودن تابع $\varphi$ خواهیم داشت

$$\varphi(x) = \varphi(x_۱^{-۱})\varphi(y_۱^{-۱})\varphi(x_۱)\varphi(y_۱)...\varphi(x_n^{-۱})\varphi(y_n^{-۱})\varphi(x_n)\varphi(y_n).$$

بنابراین $\varphi(x) \in G'$ می‌باشد. در نتیجه $\varphi(G') \subseteq G'$. به این ترتیب حکم ثابت می‌شود. $\square$

**قضیه ۱.۳۸.** فرض کنید $G$ یک گروه و $H \leqslant K \trianglelefteq G$ باشد. در این‌صورت اگر $H$ زیرگروه مشخصه‌ی $K$ باشد، آن‌گاه $H \trianglelefteq G$.

**برهان .** به قضیه‌ی (۳.۱۴) از مرجع [۱۰] مراجعه کنید. $\square$

**قضیه ۱.۳۹.** فرض کنید $G$ گروهی دوری از مرتبه‌ی $n$ باشد و عدد طبیعی $m$ وجود داشته باشد به‌طوری‌که $m \mid n$. در این‌صورت $G$ فقط یک زیرگروه از مرتبه‌ی $m$ دارد.

**برهان .** فرض کنید $a \in G$ و $G = \langle a \rangle$ باشد. در این‌صورت $|G| = o(a) = n$ می‌باشد. همچنین چون طبق فرض $n \mid m$، بنابراین عدد صحیحی مانند $q$ وجود دارد به‌طوری‌که

$$n = mq. \tag{۳.۱}$$

اکنون چون $a^q \in G$ است، بنابراین $H = \langle a^q \rangle$ می‌باشد. در نتیجه خواهیم داشت

$$|H| = o(a^q) = \frac{o(a)}{(o(a), q)} = \frac{n}{(n, q)} = m.$$

اکنون منحصر به فرد بودن این زیرگروه را اثبات می‌کنیم. فرض کنید $K$ زیرگروه دیگری از $G$ و از مرتبه‌ی $m$ باشد. در این‌صورت چون زیرگروه هر گروه دوری، دوری می‌باشد بنابراین $K$ نیز دوری است. فرض کنید $s$ کوچک‌ترین عدد صحیح مثبتی باشدکه $a^s \in K$ باشد. در این‌صورت $K = \langle a^s \rangle$ می‌باشد. درنتیجه به ازای هر عدد صحیحی مانند $r$ که $a^r \in K$ باشد داریم $s \mid r$. به دلیل این‌که $a^n = e \in K$ می‌باشد، بنابراین $s \mid n$. در نتیجه خواهیم داشت

$$|K| = o(a^s) = \frac{o(a)}{(o(a), s)} = \frac{n}{(n, s)} = \frac{n}{s}.$$

چون طبق فرض $|K| = m$، بنابراین داریم

$$n = ms. \tag{۴.۱}$$

از روابط (۳.۱) و (۵.۳) نتیجه می‌گیریم که $q = s$ می‌باشد. بنابراین خواهیم داشت

$$K = \langle a^s \rangle = \langle a^q \rangle = H.$$

به این ترتیب حکم مورد نظر اثبات می‌شود. $\square$

**نتیجه ۴۰.۱.** هر زیرگروه یک گروه دوری متناهی، مشخصه است.

**برهان .** فرض کنید $f \in Aut(G)$ و $H$ زیرگروه دلخواهی از گروه دوری $G$ باشد. در این‌صورت به دلیل همریختی بودن تابع $f$، $f(H)$ نیز زیرگروهی از $G$ می‌باشد. همچنین چون $f$ تابعی دوسویی است، بنابراین

$$|H| = |f(H)|.$$

از طرفی طبق قضیه‌ی لاگرانژ مرتبه‌ی هر زیرگروه، مرتبه‌ی گروه را عاد می‌کند بنابراین

$$|H| \mid |G|. \tag{۵.۱}$$

$$|f(H)| \mid |G|. \tag{۶.۱}$$

در نتیجه طبق روابط (۵.۱) و (۶.۱) و قضیه‌ی (۳۹.۱) خواهیم داشت

$$f(H) = H.$$

این همان نتیجه‌ی دلخواه است. □

**تعریف ۴۱.۱.** فرض کنید $\{G_i\}_{1\leq i\leq n}$ خانواده‌ای متناهی از گروه‌ها باشد. حاصل‌ضرب دکارتی $\prod_{i=1}^{n} G_i$ با عمل ترکیب مؤلفه‌وار، حاصل‌ضرب مستقیم خارجی خانواده‌ی $\{G_i\}_{1\leq i\leq n}$ نامیده می‌شود.

**تعریف ۴۲.۱.** فرض کنید $G$ یک گروه و $\{G_i\}_{1\leq i\leq n}$ خانواده‌ای متناهی از زیرگروه‌های $G$ باشد. در این‌صورت $G$ حاصل‌ضرب مستقیم داخلی $G_i$ها نامیده می‌شود هرگاه شرایط زیر برقرار باشد

الف) $G_i \trianglelefteq G$ باشد، به ازای تمام $1 \leq i \leq n$.

ب) هر عضو $g \in G$ به‌طور منحصر به فردی به‌صورت $g = g_1 g_2 \ldots g_n$ نوشته شود. به‌طوری‌که به ازای هر $1 \leq i \leq n$، $g_i \in G_i$ باشد.

**قضیه ۴۳.۱.** فرض کنید $\{G_i\}_{1\leq i\leq n}$ خانواده‌ای متناهی از گروه‌ها باشد. اگر $G = \prod_{i=1}^{n} G_i$ حاصل‌ضرب مستقیم خانواده‌ی فوق باشد، آن‌گاه زیرگروه‌های $H_i$ از $G$ به‌طوری‌که $1 \leq i \leq n$ وجود دارند که $G$ حاصل‌ضرب مستقیم داخلی $H_i$ها می‌باشد و به ازای هر $1 \leq i \leq n$ داریم $H_i \cong G_i$.

**برهان .** به قضیه‌ی (۱.۱۰) از مرجع [۱۰] مراجعه کنید. □