دانشگاه زنجان

دانشکده علوم - گروه ریاضی

پایان نامه کارشناسی ارشد

عنوان:

مجموع مرتبه ی عناصر زیرگروه های ماکسیمال گروه متقارن S_n

نگارش:

محمد مهدوی گلوجه

اساتید راهنما:

دکتر حبیب امیری

و

دکتر سید مجید جعفریان امیری

تیر ۱۳۹۱

بسم الله الرحمن الرحیم

تقدیم به

روح پاک شهیدان،

آنان که از جان خود گذشتند تا ما در آرامش باشیم.

قدردانی

خدای متعال را شاکرم که توفیقاتی را نصیب این بنده ی حقیر نمود در حالی که شایسته ی آنها نبودم. اکنون که با لطف الهی، پس از ما ه ها تلاش، کار تهیه ی پایان نامه را به اتمام می رسانم، برخود لازم می دانم از تمام کسانی که مرا در تهیه ی آن یاری کردند، تشکر و قدر دانی کنم.

از استاد بزرگوار، جناب آقای دکتر حبیب امیری، که زحمت های فراوانی را از سوی بنده متحمل شدند و با کمال اخلاق و آرامش، سوالات و اشکالات بنده را برطرف کردند، صمیمانه تشکر و قدردانی می نمایم.

همچنین از استاد راهنمای دوم، جناب آقای دکتر سید مجید جعفریان امیری، که افتخار دادند تربیت و راهنمایی این شاگرد حقیر را به عهده بگیرند و با پیشنهادات ارزنده ی خود، باعث بهبود این پایان نامه شدند، کمال تشکر را دارم.

از اساتید بزرگوار ریاضی، جناب آقای دکتر مسعود آرین نژاد و جناب آقای دکتر محمد علی اسم خانی، که زحمت مطالعه و داوری این پایان نامه را تقبل فرمودند، کمال امتنان را دارم.

از سایر اساتید گروه ریاضی نیز که زحمت های زیادی را در خصوص تربیت دانشجویان ریاضی متحمل می شوند، تشکر و قدر دانی می کنم.

از همکلاسی و دوست بسیار صمیمی، جناب آقای یونس عابدی و همسر بزرگوار ایشان، خانم عطایی، که در این سال ها، زحمت های زیادی را از سوی بنده متحمل شدند، صمیمانه تشکر و قدردانی می کنم. همچنین از همکلاسی بزرگوار، خانم فاضلی، که در تهیه، نصب و آموزش نرم افزار زیپرشین، زحمت های زیادی کشیدند، تشکر و قدردانی می نمایم.

از دوستان بسیار گرامی، آقای علیرضا کیوان، سعید حاجی و محمد نادری نیز کمال تشکر و قدردانی را دارم.

همچنین از زحمات بی دریغ پدر و مادرم تشکر می نمایم و بر دستان پر مهر آنها بوسه می زنم.

در پایان برای همه ی اساتید بزرگوار، دوستان عزیز و پدر و مادر مهربانم، آرزوی سربلندی و سلامتی دارم و از خدای کریم، پاداشی در خور کرم خویش برای آنان مسئلت دارم.

محمد مهدوی گلوجه

تیر ۱۳۹۱

چکیده

فرض کنید G یک گروه متناهی باشد و $\Psi(G)$ را مجموع مرتبه ی عناصر گروه G در نظر بگیرید.
قضیه ی اصلی ما در این پایان نامه، این است که برای زیرگروه سره ی H از گروه متقارن S_n، که H متمایز از گروه متناوب A_n می باشد، نشان دهیم، $\Psi(H) < \Psi(A_n)$. برای این کار نشان خواهیم داد که برای هر زیرگروه ماکسیمال H از S_n، که H متمایز از گروه متناوب A_n باشد، همواره داریم، $\Psi(H) < \Psi(A_n)$.
طبق قضیه ی اسکات، هر زیرگروه ماکسیمال M از S_n، در یکی از سه دسته ی، غیر انتقالی، انتقالی اولیه و انتقالی غیر اولیه، قرار می گیرد.
ابتدا نشان خواهیم داد که اگر H یک زیرگروه غیر انتقالی ماکسیمال از S_n باشد، آنگاه $\Psi(H) < \Psi(A_n)$ و در گام دوم نشان می دهیم که اگر H زیرگروه ماکسیمال انتقالی از S_n باشد که متمایز از گروه متناوب A_n است، آنگاه $\Psi(H) < \Psi(A_n)$.

واژه‌های کلیدی: *گروه متقارن، مرتبه ی عنصر، زیرگروه ماکسیمال.*

فهرست مطالب

پیشگفتار

فرض کنیم G یک گروه متناهی باشد. برای زیرمجموعه ی ناتهی S از G، تابع Ψ را به صورت

$$\Psi(S) = \sum_{g\in S} o(g)$$

تعریف می کنیم که در آن، $o(g)$، مرتبه ی عنصر g از گروه G است. از آنجایی که یکریختی مرتبه ی عناصر را حفظ می کند، بنابراین برای دو گروه یکریخت و متناهی H و G، داریم $\Psi(G) = \Psi(H)$. بنابراین اگر H گروهی متناهی باشد که با یک زیرگروه سره از G یکریخت است، آنگاه $\Psi(H) < \Psi(G)$.

در [۱] اثبات شده است که بیشترین مقدار Ψ، در بین گروههای هم مرتبه، در گروه دوری اتفاق می افتد؛ یعنی اگر C یک گروه دوری متناهی و G گروه متناهی غیردوری از مرتبه ی یکسان باشند، آنگاه $\Psi(G) < \Psi(C)$.

در [۲] ثابت شده است که اگر n یک عدد صحیح غیرپوچ توان و گروهی مانند K از مرتبه ی n وجود داشته باشد، بطوریکه $\Psi(K) = min\{\Psi(G) :| G |= n\}$، آنگاه K غیر پوچ توان است.

همچنین طبق لم ۲.۱ از [۲]، اگر G و H دو گروه متناهی باشند، آنگاه $\Psi(G \times H) \leq \Psi(G)\Psi(H)$.

همچنین در مورد حالت تساوی می توان نوشت:

$\Psi(G \times H) = \Psi(G)\Psi(H)$، اگر و فقط اگر $(| G |, | H |) = 1$.

توجه داریم که اگر H و K دو زیرگروه از گروه متناهی G باشند به طوری که $H \leq K$، آنگاه $\Psi(H) \leq \Psi(K)$.

حال این سوال به ذهن می رسد که آیا در بین زیرگروههای یک گروه، بیشترین مقدار Ψ در زیرگروهی رخ می دهد که بزرگترین مرتبه را داشته باشد؟ جواب این سوال منفی است؛ یعنی برای دو زیرگروه متناهی H و K از گروه متناهی G، که $| H |<| K |$، همواره نمی توان گفت، $\Psi(H) < \Psi(K)$.

ما این مطلب را با بیان مثالی از گروه های $\mathbb{Z}_n$ نشان خواهیم داد.

همچنین بیان خواهیم کرد که زیرگروه ماکسیمال M از S_n، در یکی از سه دسته ی، غیرانتقالی، انتقالی اولیه و انتقالی غیراولیه، قرار می گیرد.

قضیه ی اصلی دراین پایان نامه، این است که می خواهیم اثبات کنیم، برای زیرگروه سره ی H از گروه متقارن S_n، که H متمایز از گروه متناوب A_n باشد، همواره داریم $\Psi(H) < \Psi(A_n)$. برای اثبات این قضیه، با توجه به مطالب بیان شده، کافیست نشان دهیم که برای زیرگروه ماکسیمال H از S_n، که در یکی از سه دسته ی بیان شده قرار می گیرد و متمایز از گروه متناوب A_n می باشد، همواره داریم، $\Psi(H) < \Psi(A_n)$.

این پایان نامه شامل ۵ فصل به شرح زیر است:

در فصل اول مروری بر تعاریف مقدماتی خواهیم داشت و مفاهیمی از گروه و گروه متقارن را بیان خواهیم کرد. همچنین مختصر نگاهی بر تعریف عمل گروه و عمل انتقالی و غیر انتقالی خواهیم داشت و پس از بیان تعریف بلوک، تعریف گروه اولیه و غیر اولیه را بیان خواهیم کرد. همچنین مفاهیمی از حاصلضرب گروه ها را بیان خواهیم کرد و بعد از بیان تعریف حاصل ضرب مستقیم خارجی و داخلی، به بیان مفاهیمی از حاصل ضرب نیم مستقیم و حاصل ضرب حلقوی خواهیم پرداخت.

در فصل دوم، زیرگروه ها و مجموع مرتبه ی عناصر گروه متقارن از درجه ی حداکثر ۴ را بیان کرده و درستی قضیه ی اصلی را در مورد این گروه ها بررسی می کنیم.

فصل سوم ، مشتمل بر مباحثی از زیرگروه ها ی S_n، اعم از انتقالی و غیر انتقالی و قضیه ی اسکات در مورد زیرگروه های ماکسیمال گروه متقارن S_n است.

در فصل چهارم، مجموع مرتبه ی عناصر زیرگروه های ماکسیمال غیر انتقالی S_n را بررسی کرده و درستی قضیه ی اصلی را در مورد این زیرگروه ها بیان می کنیم. ما این کار را در دو مرحله انجام می دهیم.

ابتدا نشان می دهیم که اگر H یکریخت با S_{n-1} باشد، آن گاه $\Psi(H) < \Psi(A_n)$. سپس نشان می دهیم که اگر H زیر گروه ماکسیمال غیر انتقالی از S_n باشد که با S_{n-1} یکریخت نیست، آن گاه $\Psi(H) < \Psi(A_n)$.

در فصل پنجم، که آخرین فصل این پایان نامه است،تابع لاندائو را معرفی می کنیم و مطالبی را در مورد این تابع بیان می کنیم. سپس این تابع و نتایجی از آن را با تکنیک خاصی به کار می گیریم و برای زیرگروه ماکسیمال انتقالی H از S_n، که $H \neq A_n$، نشان می دهیم $\Psi(H) < \Psi(A_n)$.

بنابراین در فصل پنجم، اثبات قضیه ی اصلی را تمام می کنیم.

ما این پایان نامه را با یک حدس در مورد مجموع مرتبه ی عناصر گروه متناوب A_n و مجموع مرتبه ی عناصر مجموعه ی جایگشت های فرد گروه متقارن S_n؛ یعنی B_n، به پایان می رسانیم.

فصل ۱

تعاریف و قضایای اولیه

۱.۱ مروری بر نظریه ی اعداد

تعریف ۱.۱.۱. *گیریم $a, b \in \mathbb{Z}$ و $a \neq ٠$، آن گاه a را مقسوم علیه ای از b می نامیم و می نویسیم $a \mid b$، و می خوانیم a، عدد b را عاد می کند، چنان چه اگر $m \in \mathbb{Z}$ وجود داشته باشد به طوری که $b = ma$.*

قضیه ۲.۱.۱. الگوریتم تقسیم: *اگر $a, b \in \mathbb{Z}$ و $a > ٠$، آن گاه اعداد منحصر به فرد $q, r \in \mathbb{Z}$ وجود دارند به طوری که*

$$b = aq + r, \qquad ٠ \leqslant r < a.$$

برهان. به قضیه ی ۱.۱ از [۳۵] رجوع شود.

تعریف ۳.۱.۱. *فرض کنید $a, b \in \mathbb{Z}$ به طوری که هر دو با هم صفر نیستند. عدد $d \in \mathbb{Z}$ را* **بزرگترین مقسوم علیه مشترک (ب.م.م)** *a, b نامیده و با (a, b) یا $gcd(a, b)$ نشان می دهیم، چنان چه اگر داشته باشیم:*

الف). $d > ٠$،

ب). $d \mid a$ و $d \mid b$،

ج). اگر $a \mid c$ و $b \mid c$، آن گاه $c \mid d$.

تعریف ۴.۱.۱. *فرض کنید $a, b \in \mathbb{Z}$ به طوری که هر دوی آن ها صفر نیستند. عدد $m \in \mathbb{Z}$ را* **کوچکترین مضرب مشترک(ک.م.م)** *a, b می نامیم و می نویسیم $m = [a, b]$ یا $m = lcm\{a, b\}$، هرگاه داشته باشیم:*

۱). $a \mid m$ و $b \mid m$،

۲). اگر $a \mid c$ و $b \mid c$، آن گاه $m \mid c$،

۳). $m > 0$.

قضیه ۵.۱.۱. *هر عدد صحیح $n > 1$ را می توان به صورت $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ تجزیه کرد، که p_i ها مقسوم علیه های اول n می باشند و این تجزیه منحصر به فرد است مگر در ترتیب نوشتن p_i ها.*

برهان. به قضیه ی ۴.۱ از [۳۵] رجوع شود.

قضیه ۶.۱.۱. *برای عدد صحیح $k > 1$، $(2k)! > 2(k!)^2$.*

برهان:

با توجه به اینکه داریم

$$2(k!)^2 = 2k! \times k!$$

و

$$(2k)! = 2k \times (2k-1) \times (2k-2) \times ...(k+1) \times k!$$

بنابراین با حذف $2(k!)$ از هر دو طرف داریم

$$k \times (2k-1) \times (2k-2) \times ...(k+1) \quad \square \quad k \times (k-1) \times ... \times 1$$

در هر دو طرف به تعداد k تا جمله وجود دارد که $k = k$، ولی در بقیه ی آنها داریم

$$۲k - i > k - i, \quad ۱ \leqslant i \leqslant k - ۱$$

بنابراین سمت چپ مربع بزرگتر از سمت راست است، در نتیجه $(۲k)! > ۲(k!)^۲$. ■

۲.۱ مقدمه ای بر گروه

تعریف ۱.۲.۱. عمل دوتایی: *فرض کنید S یک مجموعه ی ناتهی و $f : S \times S \longrightarrow S$ یک تابع باشد، آن گاه f را یک عمل دوتایی می گویند و به علت تعدد توابع، f ها را با نمادهای $*$، $\Box$، $\bullet$ و ... نشان می دهند.*

تعریف ۲.۲.۱. *با شرایط تعریف بالا، زوج مرتب $(S, *)$ را یک دستگاه جبری می گویند.*

تعریف ۳.۲.۱. عنصر همانی: *اگر $(A, *)$ یک دستگاه جبری باشد و $e \in A$ وجود داشته باشد،بطوریکه به ازای هر عضوی مانند x که از A اختیار کنیم، داشته باشیم $e * x = x * e = e$. آن گاه e را عنصر همانی A با عمل $*$ می گویند و برای راحتی،گاهی فقط با ۱ نشان می دهیم.*

تعریف ۴.۲.۱. عنصر وارون یا معکوس: *اگر در دستگاه جبری $(A, *)$، که دارای عنصر همانی e است، به ازای هر $x \in A$، عنصری مانند $y \in A$ وجود داشته باشد، بطوریکه $x * y = y * x = e$، در اینصورت y را معکوس x یا x را معکوس y می گویند.*

تعریف ۵.۲.۱. گروه: *اگر دستگاه جبری $(A, *)$ در شرایط زیر صدق نماید:*

۱). *A دارای عنصر همانی با عمل $*$ باشد،*

۲). *هر عضو A، دارای معکوس با عمل $*$ باشد،*

۳). *قانون شرکت پذیری $(y * z) * x = y * (z * x)$، به ازای هر x، y و z از A برقرار باشد،*

در این صورت می گویند A با عمل $*$ یک گروه است. یا به صورت ساده تر، A یک گروه است.

تذکر ۶.۲.۱. توجه شود که در تعریف فوق، شرط بسته بودن، در تعریف دستگاه جبری وجود دارد؛ یعنی می گوییم A به عمل $*$ بسته است، هرگاه به ازای هر a و b دلخواه از A داشته باشیم، $a * b \in A$.

تعریف ۷.۲.۱. گروه متناهی: گوییم گروه G متناهی است، اگر تعداد متناهی عنصر داشته باشد.

تعریف ۸.۲.۱. مرتبه ی گروه: تعداد عناصر گروه متناهی G را مرتبه ی گروه G می نامند و با $o(G)$ یا $| G |$ نشان می دهند.

تعریف ۹.۲.۱. مرتبه ی یک عنصر: اگر G یک گروه و $x \in G$، آن گاه کوچکترین عدد صحیح و مثبت n را که برای آن داشته باشیم $x^n = e$، مرتبه ی x می نامیم و می نویسیم $o(x) = n$. اگر چنین n ای موجود نباشد، آن گاه x را از مرتبه ی نامتناهی نامیده و می نویسیم $o(x) = \infty$.

لم ۱۰.۲.۱. اگر $o(x) = n$ و داشته باشیم $x^m = e$، آن گاه $n \mid m$.

برهان: مطابق الگوریتم تقسیم داریم

$$m = nq + r, \qquad \circ \leq r < n.$$

بنابراین،

$$x^m = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = x^r$$

در نتیجه $x^r = e$. چون $o(x) = n$، پس $r = \circ$؛ یعنی $n \mid m$. $\blacksquare$

تعریف ۱۱.۲.۱. زیرگروه: زیرمجموعه ی ناتهی H از گروه G را یک زیرگروه G می نامیم، اگر که H نیز تحت عمل گروه G، خود یک گروه تشکیل دهد. در چنین حالتی می نویسیم $H \leq G$.

تعریف ۱.۲.۱۲. زیرگروه بدیهی: اگر e عنصر همانی گروه G فرض شود، آن گاه واضح است که $\{e\}$ و خود G زیرگروه هایی از گروه G هستند، که زیرگروه های بدیهی G نامیده می شوند.

تذکر ۱.۲.۱۳. ما در بیان مطالب این پایان نامه، گاهی زیرگروه بدیهی $\{e\}$ را فقط با ۱ نشان می دهیم.

تعریف ۱.۲.۱۴. زیرگروه سره (حقیقی): اگر H زیرگروهی از G باشد و $H \neq G$، آن گاه H را یک زیرگروه حقیقی(سره) G می نامیم و می نویسیم $H < G$.

لم ۱.۲.۱۵. زیرمجموعه ی ناتهی H از گروه G یک زیرگروه G است، اگر و فقط اگر به ازای هر $x, y \in H$، داشته باشیم $x^{-1}y \in H$.

برهان. به قضیه ی ۱.۱ از [۳۵] رجوع شود.

تعریف ۱.۲.۱۶. فرض کنید G یک گروه باشد و $a \in G$، در این صورت $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ را **زیرگروه دوری** تولید شده توسط a می نامیم.

قضیه ۱.۲.۱۷. فرض کنید G یک گروه باشد و $a \in G$. در این صورت مرتبه ی زیرگروه $\langle a \rangle$ با مرتبه ی a برابر است. به عبارت دیگر $o(a) = |\langle a \rangle|$.

قضیه ۱.۲.۱۸. فرض کنید $G = \langle a \rangle$ از مرتبه ی n باشد، در این صورت

$$o(a^k) = \frac{n}{(n, k)}.$$

گروه های $\mathbb{Z}$ و $\mathbb{Z}_n$ با اعمال جمع، مثال هایی از گروه دوری اند و دارای ساختاری قابل فهم تر می باشند، به همین دلیل ما در بیان مثالی از گروه $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ استفاده خواهیم کرد.

نتیجه ۱.۲.۱۹. مرتبه ی عنصر t از $\mathbb{Z}_n$ به صورت زیر به دست می آید.

$$o(t) = \frac{n}{(n,t)}.$$

برهان: چون $t = 1.t$ ، پس طبق قضیه ی ۱.۲.۱۷ ، داریم

$$o(t) = o(\langle t \rangle) = o(\langle 1.t \rangle).$$

بنابراین کافیست که در قضیه ی ۱۸ .۲ .۱، $k = t$ در نظر بگیریم. ■

تعریف ۱.۲.۲۰. هم دسته : فرض کنید G یک گروه و $H \leq G$ و $g \in G$، آن گاه مجموعه ی $Hg = \{hg : h \in H\}$ را یک هم دسته ی راست H در G و مجموعه ی $gH = \{gh : h \in H\}$ را یک هم دسته چپ H در G می نامند.

تعریف ۱.۲.۲۱. فرض کنید G یک گروه و $H \leq G$، تعداد هم دسته های راست یا چپ (متناهی یا نامتناهی) H در G را **اندیس** H در G نامیده و با $[G : H]$ نمایش می دهیم. در صورتی که G متناهی باشد، آن گاه

$$[G : H] = \frac{\mid G \mid}{\mid H \mid}.$$

قضیه ۱.۲.۲۲. هر گاه H، K و G، گروه هایی با خاصیت $H < K < G$ باشند، آن گاه

$$[G : K] = [G : H][H : K]$$

و هرگاه $[G : H]$ و $[H : K]$ متناهی باشند، آن گاه $[G : K]$ متناهی است.

قضیه ۱.۲.۲۳. قضیه ی لاگرانژ: فرض کنید G یک گروه و $H \leq G$، در این صورت داریم

$$\mid G \mid = [G : H] \mid H \mid .$$

نتیجه ۲۴.۲.۱. فرض کنید G یک گروه متناهی باشد. در این صورت

۱). اگر $H \leq G$، آن گاه $|H| \mid |G|$ (مرتبه ی H، مرتبه ی G را عاد می کند)؛

۲). اگر $g \in G$، آن گاه $o(g) \mid |G|$ (مرتبه ی g، مرتبه ی G را عاد می کند)؛

۳). اگر $g \in G$، آن گاه $g^{|G|} = e$.

تعریف ۲۵.۲.۱. اگر H و K زیرمجموعه های ناتهی از گروه G باشند، آن گاه حاصل ضرب HK به صورت زیر تعریف می شود:

$$HK = \{hk : h \in H, k \in K\}.$$

لم ۲۶.۲.۱. فرض کنید H و K دو زیرگروه متناهی از گروه G باشند، ثابت کنید HK زیرگروهی از G است، اگر و فقط اگر $HK = KH$.

برهان).

ابتدا فرض می کنیم که $HK = KH$؛ یعنی، هر گاه $h \in H$ و $k \in K$، آن گاه به ازای دو عنصر مانند $k_1 \in K$ و $h_1 \in H$، $hk = k_1h_1$. برای اثبات زیرگروه بودن HK، باید تحقیق شود که بسته است و معکوس هر عنصر HK در HK باشد. ابتدا بسته بودن را نشان می دهیم؛ پس فرض کنیم که $x = hk \in HK$ و $y = h'k' \in HK$. در این صورت، $xy = hkh'k'$. اما، چون $kh' \in KH = HK$، پس دو عنصر مثل $h_2 \in H$ و $k_2 \in K$ وجود دارند، به طوری که $kh' = h_2k_2$. در نتیجه داریم

$$xy = h(h_2k_2)k' = (hh_2)(k_2k') \in HK.$$

در نتیجه HK بسته خواهد بود. همچنین،

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK.$$

لذا، HK زیرگروهی از G است.

از سوی دیگر، هرگاه HK زیرگروه G باشد، آن گاه به ازای هر $h \in H$ و $k \in K$، $h^{-1}k^{-1} \in HK$. و در نتیجه

$$kh = (h^{-1}k^{-1})^{-1} \in HK.$$

پس $KH \subset HK$. حال اگر x عنصری از HK باشد، $x^{-1} = hk \in HK$ و در نتیجه داریم

$$x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$$

پس $HK \subset KH$. بنابراین، $HK = KH$. ■

تعریف ۲۷.۲.۱. فرض کنیم G یک گروه و M زیرمجموعه ی ناتهی از G باشد، برای $g \in G$، مجموعه ی M^g را چنین تعریف می کنیم

$$M^g = \{g^{-1}mg : m \in M\}$$

مجموعه ی M^g را **مزدوج** M در G می نامیم. در حالتی که M ، مجموعه ای تک عضوی باشد؛ یعنی $M = \{m\}$، آن گاه به جای $\{m\}^g$ می نویسیم m^g . بنابراین، $m^g = g^{-1}mg$.

تعریف ۲۸.۲.۱. **زیرگروه نرمال:** فرض کنید G یک گروه و N زیرگروهی از آن باشد، N را زیرگروه نرمال G می نامند، اگر به ازای هر $g \in G$ ، داشته باشیم، $N^g \subseteq N$؛ یعنی برای تمام $g \in G$ و تمام $n \in N$، داریم $g^{-1}ng \in N$ ، در اینصورت می نویسیم $N \trianglelefteq G$.

تعریف ۲۹.۲.۱. **زیرگروه ماکسیمال :** فرض کنیم G یک گروه و M زیرگروهی از آن باشد. M را زیرگروه ماکسیمال G می گوییم هرگاه داشته باشیم:

الف). $M \neq G$ ،

ب). به ازای هر زیرگروه G مانند K که $M \subseteq K \subseteq G$، آن‌گاه $M = K$ یا $M = G$.

اکنون قضیه ای را بیان می کنیم که در بیان مثال نقضی، آن را به کار خواهیم گرفت.

قضیه ۱.۲.۳۰. اگر $M < G$ و $[G : M] = p$، که p یک عدد اول است، آن‌گاه M یک زیرگروه ماکسیمال G است.

برهان. فرض کنیم که M زیرگروه ماکسیمال G نباشد، پس زیرگروهی مانند K وجود دارد به طوری که $M < K < G$. اکنون طبق قضیه ی قبلی داریم

$$[G : K][K : M] = [G : M] = p$$

چون p یک عدد اول است، پس دو حالت زیر را داریم

حالت اول: $[K : M] = 1$ و $[G : K] = p$

حالت دوم: $[K : M] = p$ و $[G : K] = 1$

در حالت اول داریم $M = K$ و در حالت دوم، $K = G$، در نتیجه طبق تعریف ۱.۲.۲۹، M یک زیرگروه ماکسیمال است. ■

تعریف ۱.۲.۳۱. تابع φ از گروه G به گروه H $(\varphi : G \longrightarrow H)$ را یک **همریختی (هومومرفیسم)** گوییم اگر برای هر a و b از G داشته باشیم، $\varphi(ab) = \varphi(a)\varphi(b)$.

تعریف ۱.۲.۳۲. یکریختی : فرض کنید G و H دو گروه باشند. تابع $\varphi : G \longrightarrow H$ یک یکریختی (ایزومرفیسم) نامیده می شود اگر

۱). φ یک به یک و پوشا باشد،

۲). برای هر a و b در G، $\varphi(ab) = \varphi(a)\varphi(b)$.