بسم الله الرحمن الرحيم

دانشگاه یزد

دانشکده ریاضی

پایان‌نامه

برای دریافت درجه‌ی کارشناسی ارشد

ریاضی محض-جبر

ATI-گروه‌ها

استادان راهنما:

دکتر محمدعلی ایرانمنش

دکتر بیژن دواز

پژوهش و نگارش:

مرضیه عموشاهی

مهرماه ۱۳۸۷

تقدیم به سرمایه‌های زندگیم:

پدرم که استواری و آرامش را

و

مادرم که شکیبایی و امید را

در وجودم تداوم بخشیدند!

تقدیر و تشکر

به‌نام آفریننده‌ی بی‌همتا

الهی، کجا باز یابم آن روز که تو ما را بودی و من نبودم، تا باز به آن روز رسم میان آتش و دودم، اگر به دو گیتی آن روز یابم پر سودم ور بود خود را یابم به نبود خود خشنودم.

الهی، آن‌چه ما خود کشتیم به بر میار و آن‌چه تو ما را کشتی آفت ما را از آن بازدار.

الهی، سپاس تو را که بی‌طلب بر من بخشیدی.

سپاس بیکران خداوند را به سبب پدری عزیز و مهربان که بی‌منّت، همواره و بیش از همه، مرا در پناه لطف و مهربانی خویش داشته است.

سپاس و تقدیر ویژه از استاد گرانقدرم، جناب آقای دکتر ایرانمنش، که نظارت و سرپرستی این پایان‌نامه را بر عهده داشته و در تمامی مراحل تحقیق و تدوین این پایان‌نامه مرا یاری نمودند. از جناب آقای دکتر دواز به سبب راهنمایی‌های ارزشمندشان کمال تشکر را دارم. همچنین از اساتید محترم، آقای دکتر معدنشکاف و آقای دکتر انوریه که با وجود مشغله‌ی کاری فراوان، زحمت داوری این پایان‌نامه را پذیرفتند سپاسگزاری می‌کنم.

در خاتمه از الطاف و محبت‌های دلسوزانه‌ی دوستان عزیزم و همچنین سرکار خانم عابدینی، سرکار خانم عباسی‌زاده و سرکار خانم رضایی تشکر می‌کنم.

امید که زحمات همه‌ی این عزیزان را در شادی‌هایشان جبران کنم، هر چند لحظه‌ای، هر چند ذرّه‌ای!

مرضیه عموشاهی

مهرماه ۱۳۸۷

بسمه تعالی

مدیریت تحصیلات تکمیلی	**صورتجلسه دفاعیه پایان نامه دانشجوی دوره کارشناسی ارشد**	شناسه: ب/ک/۳

جلسه دفاعیه پایان نامه تحصیلی خانم مرضیه عموشاهی دانشجوی کارشناسی ارشد

رشته/گرایش: ریاضی محض

تحت عنوان: ATI- گروه‌ها

و تعداد واحد: ۶ درتاریخ ۸۷/۷/۲۸ باحضور اعضای هیأت داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیأت داوران، پایان‌نامه با نمره: به عدد ۱۸ به حروف هجده و درجه عالی مورد تصویب قرارگرفت.

عنوان	نام و نام خانوادگی	امضاء
استاد/ استادان راهنما:	محمد علی ایرانمنش بیژن دواز	
استاد/ استادان مشاور:	-----	
متخصص وصاحبنظرداخلی:	سیدمحمد انوریه	
متخصص و صاحبنظر خارجی:	علی معدنشکاف	

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام ونام خانوادگی: قاسم انصاری پور

امضاء:

فهرست مندرجات

چکیده

در این پایان‌نامه ابتدا CN-گروه‌ها را معرفی می‌کنیم. در واقع یک CN-گروه، گروهی است که مرکزساز هر عضو غیربدیهی آن پوچتوان است. همچنین گروه G یک ATI-گروه نامیده می‌شود اگر برای هر زیرگروه آبلی A از G و برای هر $x \in G$، $A \cap A^x = 1_G$ یا $A \cap A^x = A$. سپس ATI-گروه‌های متناهی را رده‌بندی کرده و ثابت می‌کنیم که اگر G یک ATI-گروه متناهی باشد آن‌گاه G یا یک گروه پوچتوان، یا یک گروه فروبنیوس حل‌پذیر، یا یکریخت با S_4 و یا یکریخت با یکی از گروه‌های ساده‌ی $\mathrm{PSL}(2,4)$، $\mathrm{PSL}(2,7)$ و یا $\mathrm{PSL}(2,9)$ است. به‌علاوه در حالتی‌که G یک گروه فروبنیوس حل‌پذیر با هسته‌ی K و متمم H است هر H-عامل اصلی از K دوری است. در این‌حالت همچنین نشان داده‌ایم که یا H دوری است و یا به‌صورت حاصل‌ضرب مستقیم یک گروه دوری از مرتبه‌ی فرد و گروه کواترنیونی Q_8 است.

مقدمه

مفهوم گروه نخستین بار در اوایل سده‌ی ۱۹ معرفی شد، ولی ریشه‌های آن‌را می‌توان در دوران بسیار گذشته جستجو کرد؛ در واقع، مفهوم گروه به نوعی در موضوع حرکت یا تبدیل که در هندسه‌ی قدیم به‌کار می‌رفت نهفته بود. از اواخر سده‌ی ۱۹ که این مفهوم صورت روشنی به خود گرفت، نقش مهمی را در همه‌ی شاخه‌های ریاضیات ایفا کرد.

در اواخر سده‌ی ۱۸، لاگرانژ، واندرموند و روفینی در مطالعات خود راجع به معادلات جبری به اهمیت گروه جایگشت‌های ریشه‌ها پی برده بودند و آبل با استفاده از این ایده ثابت کرد که یک معادله‌ی کلی از درجه‌ی ناکمتر از ۵ را نمی‌توان به‌طور جبری حل کرد. کشی گروه جایگشت‌های ریشه‌ها را به‌خاطر اهمیتشان مورد مطالعه قرار داد؛ ولی توصیف کامل رابطه‌ی بین گروه‌ها و معادلات جبری را نخستین بار گالوا به‌دست آورد. ژوردان به بسط نظریه‌ی آبل و گالوا پرداخت و شرح مفصلی از آن‌را در رساله‌ی جایگشت‌ها و معادلات جبری خود به سال ۱۸۷۰ آورد. تا آن زمان گروه به معنی گروه جایگشتی به‌کار می‌رفت؛ تعریف گروه به‌صورت اصول موضوعه توسط کیلی (۱۸۵۴) و کرونکر

(۱۸۷۰) ارائه شد. کلاین در برنامه‌ی ارلانگن خود (۱۸۷۲) به اهمیت نظریه‌ی گروه‌ها در مطالعه‌ی هندسه تأکید کرد و سوفوس لی نظریه‌ی گروه‌های لی را در سال ۱۸۸۰ ایجاد نمود. برنساید کتاب نظریه‌ی گروه‌های خود را منتشر ساخت که با گذشت یک سده، چاپ دوم آن (۱۹۱۱) هنوز یک کتاب کلاسیک با ارزش در نظریه‌ی گروه‌های متناهی به‌شمار می‌رود. از سال ۱۸۹۶ فروبنیوس و دیگران نظریه‌ی نمایش گروه‌ها با ماتریس‌ها را بسط دادند. تا آن زمان، نظریه‌ی گروه‌های متناهی اهمیت اساسی خود را کسب کرده بود.

از بین شاخه‌های جبر مجرد، نظریه‌ی گروه‌ها نخستین شاخه‌ای بود که توسعه‌ی آن آغاز گشت و با بسط این شاخه از جبر بود که پیشرفت جبر مجرد در دهه‌ی ۱۹۳۰ شروع شد. از نیمه‌ی دوم این دهه، نظریه‌ی گروه‌ها به پیشرفت‌های بسیار زیادی نایل آمده و توجه بسیاری از ریاضیدانان را به خود معطوف داشته است. از سال ۱۹۵۵ نتایج بسیار مهم و عمیقی در این نظریه به‌دست آمده است که شاخص‌ترین آن‌ها رده‌بندی گروه‌های ساده‌ی متناهی است که بنابر عقیده‌ی بسیاری از صاحب‌نظران ریاضی بزرگ‌ترین دستاورد ریاضی سده‌ی ۲۰ به‌شمار می‌رود.

مرجع اصلی این پایان‌نامه مرجع [۳] است که در آن ATI-گروه‌های متناهی رده‌بندی می‌شوند. گروه G یک ATI-گروه نامیده می‌شود اگر برای هر زیرگروه آبلی A از G و برای هر $x \in G$، $A \cap A^x = \{1\}$ یا $A \cap A^x = A$.

در فصل ۱ که در ۳ بخش تنظیم گردیده، به بیان تعاریف و قضایایی که در این پایان‌نامه استفاده می‌شود می‌پردازیم.

در فصل ۲ گروه‌های حل‌پذیر، پوچتوان و فروبنیوس را تعریف کرده و هر کدام را در سطحی نسبتاً وسیع مورد بحث قرار می‌دهیم.

در فصل ۳ با معرفی CN-گروه‌ها و ATI-گروه‌ها به بحث و بررسی این گروه‌ها می‌پردازیم و در فصل ۴، ATI-گروه‌های متناهی را رده‌بندی می‌کنیم.

فصل ۱

مفاهیم اساسی نظریه‌ی گروه‌ها

در این فصل مفاهیم مقدماتی نظریه‌ی گروه را مرور خواهیم کرد. هدف ما علاوه بر یادآوری، فراهم آوردن اصطلاحات، علامات و مقدماتی است که در بخش‌های آتی مورد نیاز خواهد بود.

علامات $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{R}$ و $\mathbb{Q}$ را به‌ترتیب برای نشان دادن مجموعه‌های اعداد طبیعی، اعداد صحیح، اعداد حقیقی و اعداد گویا به‌کار خواهیم برد. فرض کنیم X یک مجموعه و A و B زیرمجموعه‌هایی از آن باشند. هرگاه A زیرمجموعه‌ی B باشد، خواهیم نوشت $A \subseteq B$. علامت $A \subset B$ را وقتی به‌کار خواهیم برد که A زیرمجموعه‌ی واقعی B باشد.

هرگاه m و n دو عدد صحیح باشند به‌طوری‌که m مقسوم‌علیهی از n باشد، خواهیم نوشت $m \mid n$. همچنین بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح m و n را با (m,n) نشان خواهیم داد.

حلقه‌ی اعداد صحیح به پیمانه‌ی m را با $\mathbb{Z}_m$ نشان خواهیم داد. به اختصار، اعضای این حلقه را با $۰, ۱, \ldots, m-۱$ نشان می‌دهیم. همچنین به ازای هر عدد اول p، میدان گالوای p عضوی را نیز با علامت $\mathbb{Z}_p$ نشان می‌دهیم.

۱.۱ پیشنیازهای نظریه‌ی گروه

در این بخش تعاریف پایه‌ای، لم‌ها و قضایای مقدماتی نظریه‌ی گروه‌ها را یادآوری می‌کنیم.

۱.۱.۱ تعریف. [۱]

اگر π یک مجموعه از اعداد اول باشد، می‌گوییم عضو x از G یک π-عضو است اگر مرتبه‌ی آن توسط برخی اعداد اول مجموعه‌ی π شمرده شود. به‌ویژه، اگر $\pi = \{p\}$ از p-عضو به‌جای π-عضو استفاده می‌کنیم. به‌طور مشابه، یک گروه G، π-گروه نامیده می‌شود اگر $|G|$ تنها توسط اعداد اول درون π شمرده شود. به‌علاوه، $\pi(G)$ نشان‌دهنده‌ی مجموعه‌ی اعداد اول شمارنده‌ی $|G|$ است. به‌وضوح، G یک $\pi(G)$-گروه است. همچنین اگر G یک π-گروه باشد آن‌گاه $\pi(G) \subseteq \pi$. مکمل مجموعه‌ی اعداد اول π را با π' نشان داده و مشابه فوق، π'-عضو و p'-عضو و همچنین π'-گروه و p'-گروه را تعریف می‌کنیم.

به‌عنوان مثال، یک $۲'$-عضو یک عضو از درجه‌ی فرد است.

۲.۱.۱ تعریف. [۷]

فرض کنیم G یک گروه و $x \in G$. مرکزساز x در G را که با $\mathrm{C}_G(x)$ نشان می‌دهیم مجموعه‌ی همه‌ی اعضای G است که با x تعویض می‌شوند، یعنی

$$\mathrm{C}_G(x) = \{g \in G \mid xg = gx\}.$$

به‌طور کلی، اگر X یک زیرمجموعه‌ی دلخواه و ناتهی از G باشد مرکزساز X در G عبارت است از:

$$\mathrm{C}_G(X) = \{g \in G \mid \forall\ x \in X : xg = gx\}.$$

همچنین اگر H و K دو زیرگروه دلخواه G باشند گوییم H، K را مرکزی می‌کند اگر

.$H \subseteq \mathrm{C}_G(K)$

۳.۱.۱ تعریف. [۷]

مرکز G عبارت است از $\mathrm{C}_G(G)$ که آن‌را با $\mathrm{Z}(G)$ نشان می‌دهیم، به‌عبارت دیگر،

$$\mathrm{Z}(G) = \{g \in G \mid \forall\ x \in G : xg = gx\}.$$

با توجه به تعریف $\mathrm{C}_G(x)$ و $Z(G)$ به‌سادگی نتیجه می‌شود که:

$$\mathrm{Z}(G) = \bigcap_{x \in G} \mathrm{C}_G(x).$$

۴.۱.۱ تعریف. [۷]

فرض کنیم G یک گروه و X یک زیرمجموعه‌ی دلخواه و ناتهی از G است. نرمال‌ساز X در G عبارت است از:

$$\mathrm{N}_G(X) = \{g \in G \mid gX = Xg\}.$$

همچنین اگر H و K دو زیرگروه دلخواه G باشند گوییم H، K را نرمال می‌کند اگر .$H \subseteq \mathrm{N}_G(K)$

۵.۱.۱ مثال.

در گروه Q_8 و زیرگروه $H =< i >$ از آن داریم:

$$jHj^{-1} =< jij^{-1} >=< -jij >=< -i >=< i >= H,$$

$$kHk^{-1} =< kik^{-1} >=< -kik >=< -i >=< i >= H.$$

پس $jHj^{-1} = H$ و $kHk^{-1} = H$. از طرفی برای هر $h \in H$، $hHh^{-1} = H$. از این‌رو، برای هر $a \in \mathrm{Q}_8$ داریم $aHa^{-1} = H$. بنابراین $H \trianglelefteq \mathrm{Q}_8$. با برهانی مشابه ثابت می‌شود که هر زیرگروه Q_8 در Q_8 نرمال است. □

۶.۱.۱ قضیه.

برای هر مجموعه S از G و هر عضو g از G داریم:

۱) $< S^g >=< S >^g$؛

۲) $\mathrm{N}_G(S^g) = \mathrm{N}_G(S)^g$؛

۳) $\mathrm{C}_G(S^g) = \mathrm{C}_G(S)^g$.

اثبات. به [۷، صفحه ۱۴] مراجعه شود. □

۷.۱.۱ لم.

فرض کنیم G یک گروه و $V \leq \mathrm{Z}(G)$ است. اگر $\frac{G}{V}$ دوری باشد آن‌گاه G آبلی است.

اثبات. به [۱، صفحه ۱۱] مراجعه شود. □

۸.۱.۱ قضیه. (نرمال‌ساز– مرکزساز)

فرض کنیم G یک گروه و $H \leq G$، در این‌صورت:

۱) $\mathrm{C}_G(H) \trianglelefteq \mathrm{N}_G(H)$؛

۲) $\frac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)} \cong\leq \mathrm{Aut}(H)$.

اثبات. به [۱۰، صفحه ۳۷] مراجعه شود. □

۹.۱.۱ قضیه.

۱) اگر G دوری باشد آن‌گاه $\mathrm{Aut}(G)$ آبلی است.

۲) اگر G دوری و از مرتبه‌ی p باشد آن‌گاه $\mathrm{Aut}(G)$ دوری و از مرتبه‌ی $p-1$ است.

اثبات. به [۱، صفحه ۱۲] مراجعه شود. □

۱۰.۱.۱ تعریف. [۵]

فرض کنیم $G \trianglelefteq K$ و $K \leq H \leq G$. مرکزساز $\frac{H}{K}$ در G، زیرگروه J از G است به‌طوری‌که $K \leq J$ و $\frac{J}{K} = \mathrm{C}_{\frac{G}{K}}(\frac{H}{K})$. می‌نویسیم $J = \mathrm{C}_G(\frac{H}{K})$. بنابراین

$$\mathrm{C}_G(\frac{H}{K}) = \{g \in G \mid [g,h] \in K \;:\; \forall\, h \in H\}.$$

با توجه به تعریف فوق، اگر $H \trianglelefteq G$ آن‌گاه $\mathrm{C}_G(\frac{H}{K}) \trianglelefteq G$ و $\frac{G}{\mathrm{C}_G(\frac{H}{K})} \cong\leq \mathrm{Aut}(\frac{H}{K})$.

۱۱.۱.۱ تعریف. [۵]

فرض کنیم G گروهی متناهی و $p \mid |G|$. بزرگ‌ترین p–زیرگروه نرمال G را با $\mathrm{O}_p(G)$ نشان می‌دهیم. به‌عبارت دیگر،

$$\mathrm{O}_p(G) = \langle\, A : A \trianglelefteq G,\ A \text{ ، } p\text{–گروه} \,\rangle.$$

۱۲.۱.۱ مثال. [۵]

$\mathrm{O}_۲(\mathbb{S}_۳) = \{۱_{\mathbb{S}_۳}\}$ و $\mathrm{O}_۳(\mathbb{S}_۳) = \mathbb{A}_۳$. □

۱۳.۱.۱ تعریف. [۱]

فرض کنیم G گروهی متناهی است. بزرگ‌ترین π–زیرگروه نرمال G را با $\mathrm{O}_\pi(G)$ نشان می‌دهیم.

۱۴.۱.۱ لم.

$$\frac{G}{\mathrm{Z}(G)} \cong \mathrm{Inn}(G).$$

اثبات. بنابر قضیه‌ی اول یکریختی، نتیجه حاصل می‌شود. □

۱۵.۱.۱ لم.

فرض کنیم G یک گروه ساده‌ی ناآبلی است، در این‌صورت هر خودریختی از $\mathrm{Aut}(G)$، خودریختی داخلی است.

اثبات. به [۶، صفحه ۳۹۹] مراجعه شود. □

۱۶.۱.۱ تعریف. [۱۲]

فرض کنیم G یک گروه است و $H \leq G$. گوییم H در G به‌طور کامل ناوردا است هرگاه تحت درون‌ریختی‌های G ناوردا باشد، یعنی برای هر $\alpha \in \mathrm{End}(G)$، $\alpha(H) \subseteq H$.

۱۷.۱.۱ تعریف. [۱۲]

گوییم H در G مشخصه است و می‌نویسیم $H \text{ char } G$، هرگاه تحت خودریختی‌های G

ناوردا باشد، یعنی برای هر $\alpha \in \mathrm{Aut}(G)$، $\alpha(H) \subseteq H$.

گروه نابدیهی G را به‌طور مشخص ساده گوییم هرگاه زیرگروه مشخصه‌ی نابدیهی نداشته باشد.

۱۸.۱.۱ لم.

$\mathrm{O}_\pi(G)$، در صورت وجود، مشخصه است.

اثبات. اگر $\sigma \in \mathrm{Aut}(G)$ آن‌گاه $(\mathrm{O}_\pi(G))^\sigma$ یک π−زیرگروه نرمال از G است. بنابراین $(\mathrm{O}_\pi(G))^\sigma \subseteq \mathrm{O}_\pi(G)$. پس $\mathrm{O}_\pi(G)$ مشخصه است. □

حال اگر π را برابر با مجموعه‌ی تک عضوی $\{p\}$ قرار دهیم نتیجه می‌گیریم که $\mathrm{O}_p(G)$ نیز در صورت وجود، مشخصه است.

۱۹.۱.۱ قضیه. [۱۲]

اگر H زیرگروه مینیمال نرمال G باشد آن‌گاه H به‌طور مشخص ساده است.

اثبات. فرض کنیم L زیرگروه مشخصه‌ای از H است. چون $L \text{ char } H \trianglelefteq G$، $L \trianglelefteq G$. به‌علاوه چون $L \leq H$ و H زیرگروه مینیمال نرمال G است، یا $L = \{1_G\}$ و یا $L = H$. بنابراین H مشخصاً ساده است. □

۲۰.۱.۱ تعریف. [۵]

فرض کنیم G یک گروه و $K \trianglelefteq G$. گوییم G روی K شکافته می‌شود هرگاه زیرگروهی از G مانند H موجود باشد به‌طوری‌که $G = HK$ و $H \cap K = \{1_G\}$.

۲۱.۱.۱ تعریف. [۵]

فرض کنیم G یک گروه است و $H, K \leq G$. H را متمم K در G گوییم هرگاه داشته باشیم $G = HK$ و $H \cap K = \{1_G\}$.

۲۲.۱.۱ مثال. [۵]
به ازای هر عدد طبیعی n که $n > ۱$، $\mathbb{S}_n$ روی $\mathbb{A}_n$ با متمم $H =< (۱\ ۲) >$ شکافته می‌شود. $\square$

۲۳.۱.۱ قضیه.
اگر K یک زیرگروه نرمال غیربدیهی از p–گروه G باشد آن‌گاه $K \cap \mathrm{Z}(G) \neq \{۱_G\}$.

اثبات. به [۱، صفحه ۳۱] مراجعه شود. $\square$

۲۴.۱.۱ تعریف. [۱]
فرض کنیم G یک گروه از مرتبه‌ی زوج است، در این‌صورت G حداقل دارای یک عضو از مرتبه‌ی ۲ است، به هر چنین عضوی یک برگشت گویند.

۲۵.۱.۱ تعریف. [۱۰]
فرض کنیم $\mathbb{F}$ یک میدان است، در این‌صورت مجموعه‌ی همه‌ی ماتریس‌های $n \times n$ با درایه‌های متعلق به $\mathbb{F}$، تحت جمع و ضرب ماتریسی یک حلقه‌ی یک‌دار تشکیل می‌دهند که آن‌را با $\mathrm{M}(n, \mathbb{F})$ نشان می‌دهیم. همچنین مجموعه‌ی همه‌ی ماتریس‌های وارون‌پذیر $n \times n$ با درایه‌های متعلق به $\mathbb{F}$، تحت ضرب ماتریسی یک گروه تشکیل می‌دهند که آن‌را با $\mathrm{GL}(n, \mathbb{F})$ نشان می‌دهیم و گروه خطی عام از درجه‌ی n روی $\mathbb{F}$ گوییم. در صورتی‌که میدان $\mathbb{F}$، q عضوی باشد $\mathrm{GL}(n, \mathbb{F})$ را با $\mathrm{GL}(n, q)$ نیز نشان می‌دهیم. همچنین به $\mathrm{PGL}(n, \mathbb{F}) = \dfrac{\mathrm{GL}(n, \mathbb{F})}{\mathrm{Z}(\mathrm{GL}(n, \mathbb{F}))}$ گروه خطی عمومی تصویری می‌گوییم.
مجموعه همه‌ی تبدیلات متعلق به $\mathrm{GL}(n, \mathbb{F})$ که دترمینان آن‌ها ۱ است را گروه خطی خاص گفته و آن‌را با $\mathrm{SL}(n, \mathbb{F})$ نشان می‌دهیم. همچنین به $\mathrm{PSL}(n, \mathbb{F}) = \dfrac{\mathrm{SL}(n, \mathbb{F})}{\mathrm{Z}(\mathrm{SL}(n, \mathbb{F}))}$ گروه خطی خاص تصویری می‌گوییم.

۲۶.۱.۱ تعریف. [۱۲]

فرض کنیم n عدد صحیح مثبت است. تعداد اعداد کوچک‌تر یا مساوی n که نسبت به n اول‌اند را با $\Phi(n)$ نشان می‌دهیم، یعنی

$$\Phi(n) = |\{m \in \mathbb{N} \mid m \leq n \ , \ (m,n) = ۱\}|.$$

Φ را تابع فی اویلر می‌نامیم.

به‌سادگی مشاهده می‌شود که اگر p یک عدد اول باشد و $n \in \mathbb{N}$، آن‌گاه $\Phi(p^n) = p^{n-۱}(p-۱)$.

فرض کنیم m یک عدد طبیعی بزرگ‌تر از یک است، در این‌صورت مجموعه‌ی همه‌ی اعداد طبیعی مانند n که $n < m$ و m و n متباین هستند را با $\mathrm{U}(m)$ نشان می‌دهیم. مجموعه‌ی $\mathrm{U}(m)$ با عمل ضرب اعداد طبیعی به پیمانه‌ی m گروهی آبلی تشکیل می‌دهد. این گروه را با همان علامت $\mathrm{U}(m)$ نشان می‌دهیم. بنابراین

$$|\mathrm{U}(m)| = \Phi(m).$$

همچنین اگر G یک گروه دوری غیربدیهی از مرتبه‌ی m باشد آن‌گاه $\mathrm{Aut}(G) \cong \mathrm{U}(m)$.

۲۷.۱.۱ تعریف. [۱۰]

فرض کنیم V یک فضای برداری با بعد n روی میدان $\mathbb{F}$ است، در این‌صورت مجموعه‌ی همه‌ی تبدیلات خطی V، تحت عمل جمع و ترکیب توابع، یک حلقه‌ی یک‌دار تشکیل می‌دهند که آن‌را با $\mathrm{End}(V)$ نشان می‌دهیم. همچنین مجموعه‌ی همه‌ی تبدیلات خطی وارون‌پذیر V، تحت عمل ترکیب توابع یک گروه تشکیل می‌دهند که آن‌را با $\mathrm{GL}(V)$ نشان می‌دهیم و گروه خطی عام V روی $\mathbb{F}$ گوییم.

۲۸.۱.۱ لم.

فرض کنیم V یک فضای برداری با بعد n روی میدان $\mathbb{F}$ است، در این‌صورت

$\mathrm{GL}(V) \cong \mathrm{GL}(n, \mathbb{F})$.

اثبات. کافی است پایه‌ای برای V انتخاب کنیم و هر تبدیل خطی V را به ماتریس آن تبدیل خطی در پایه‌ی انتخاب شده تصویر کنیم. □

فرض کنیم G یک گروه آبلی مقدماتی است، در این‌صورت عدد اول p وجود دارد که به ازای هر $a \in G$، $pa = 0$. فضای برداری V روی $\mathbb{Z}_p$ را به‌صورت زیر تعریف می‌کنیم:

۱) عناصر V همان عناصر G هستند؛

۲) حاصل‌جمع دو عضو V را همان حاصل‌جمع‌شان در G تعریف می‌کنیم؛

۳) به ازای هر $\bar{m} \in \mathbb{Z}_p$ و $a \in G$، حاصل‌ضرب اسکالر $\bar{m}a$ را برابر عضو $ma \in G$ تعریف می‌کنیم.

این حاصل‌ضرب اسکالری خوشتعریف است. زیرا اگر $\bar{m} = \bar{n}$ آن‌گاه $p \mid (m-n)$. پس $(m-n)a = 0$ و $ma = na$، یعنی $\bar{m}a = \bar{n}a$. اکنون به‌سادگی می‌توان تحقیق کرد که V یک فضای برداری روی $\mathbb{Z}_p$ است و به‌وضوح $G \cong (V, +)$. برعکس، اگر V یک فضای برداری روی $\mathbb{Z}_p$ باشد و $G \cong (V, +)$ آن‌گاه $(V, +)$ یک گروه آبلی است. به‌علاوه چون به ازای هر $v \in V$، $pv = 0$ پس $(V, +)$ آبلی مقدماتی است. چون $G \cong (V, +)$، G نیز آبلی مقدماتی است. بنابراین لم زیر برقرار است:

۲۹.۱.۱ لم.

فرض کنیم G یک p-گروه آبلی مقدماتی از مرتبه‌ی p^n است، در این‌صورت یک فضای برداری مانند V روی میدان $\mathbb{Z}_p$ از بعد n وجود دارد به‌طوری‌که $G \cong V^+$، که در آن V^+ گروه جمعی فضای برداری V است. به‌علاوه، $\mathrm{Aut}(G) \cong \mathrm{GL}(V)$.

۳۰.۱.۱ قضیه.

فرض کنیم n یک عدد طبیعی مفروض و q توان مثبتی از یک عدد اول است، در