بسم الله الرحمن الرحیم

دانشگاه قم
دانشکده علوم پایه
گروه ریاضیات

پایان‌نامه کارشناسی‌ارشد

رشته ریاضی محض گرایش جبر

عنوان:

زیرگروه‌های منظم از گروه‌های آفین که هیچ انتقالی ندارند

استاد راهنما:

سید علی موسوی

نگارنده:

فاطمه محمودی

تابستان ۱۴۰۰

چکیده

برای زیرگروه منظم داده شده R از $\mathrm{AGL}_n(\mathbb{F})$، می‌توان این پرسش را مطرح کرد که آیا R شامل انتقال‌های غیر بدیهی است. پاسخ منفی به این سوال توسط لیبک، پرگر و ساکسل برای $\mathrm{AGL}_۲(p)$ (p یک عدد اول)، $\mathrm{AGL}_۳(p)$ (p یک عدد اول فرد) و $\mathrm{AGL}_۴(۲)$ داده شده است. اما پاسخ مثبت به این سوال توسط هگدوس برای $\mathrm{AGL}_n(p)$ که در آن اگر p عددی فرد باشد، $n \geq ۴$ و اگر $p = ۲$ آن‌گاه $n = ۳$ یا $n \geq ۵$، ارائه شده بود. اولین تعمیم روش هگدوس برای میدان‌های متناهی، اخیراً توسط کاتینو، کولازو و استفانلی به دست آورده شده است. در این پایان‌نامه، مثال‌هایی از این زیرگروه‌ها را در $\mathrm{AGL}_n(\mathbb{F})$، برای هر $n \geq ۵$ و هر میدان $\mathbb{F}$ ارائه می‌دهیم. برای $n < ۵$، شرایط لازم و کافی برای وجود این زیرگروه‌ها را ارائه می‌کنیم با این فرض که اگر $\operatorname{char} \mathbb{F} = ۰$، آن‌گاه R را تک‌توان در نظر می‌گیریم.

کلمات کلیدی: زیرگروه منظم، گروه آفین، انتقال.

مقدمه

فرض کنید که $\mathrm{AGL}_n(\mathbb{F})$ گروه آفین از درجه n روی میدان $\mathbb{F}$ باشد که اعضای این گروه را می‌توان آن را به صورت زیر نمایش داد:

$$\mathrm{AGL}_n\left(\mathbb{F}\right)=\left\{\left(\begin{array}{cc}1 & v\\ 0 & A\end{array}\right)\ :v\in\mathbb{F}^n,\ A\in\mathrm{GL}_n(\mathbb{F})\right\}.$$

فرض کنید $\mathbb{F}^n$ فضای برداری n بردارهای سطری از بعد n روی میدان $\mathbb{F}$ باشد. گروه $\mathrm{AGL}_n(\mathbb{F})$ از راست روی مجموعه‌ی $\mathbb{F}^n$ عمل می‌کند.

یک زیرگروه R از گروه $\mathrm{AGL}_n(\mathbb{F})$ را منظم می‌نامیم اگر R به صورت منظم روی مجموعه‌ی نقاط آفین عمل کند، به عبارت دیگر R منظم است اگر به ازای هر $v\in\mathbb{F}^n$ یک عضو منحصر به فرد از R موجود باشد به طوری که نقطه‌ی آفین $(1,v)$ سطر اول آن باشد.

فرض کنید که π تابعی از گروه $\mathrm{AGL}_n\left(\mathbb{F}\right)$ به گروه $\mathrm{GL}_n\left(\mathbb{F}\right)$ باشد که به صورت زیر تعریف می‌شود:

$$\pi:\mathrm{AGL}_n\left(\mathbb{F}\right)\to\mathrm{GL}_n\left(\mathbb{F}\right)$$
$$\left(\begin{array}{cc}1 & v\\ 0 & A\end{array}\right)\mapsto A$$

در این صورت π یک همریختی پوشاست. حال هسته‌ی این به‌روریختی را در نظر می‌گیریم و آن را گروه انتقال $\mathcal{T}$ می‌نامیم. مسئله‌ی وجود زیرگروه‌های منظمی از $\mathrm{AGL}_n(\mathbb{F})$ که دارای

هیچ انتقالی غیر از بدیهی نیستند، اولین بار توسط لیبک[1]، پرگر[2] و ساکسل[3] در سال ۲۰۰۰ در مقاله‌ی [۶] مطرح شد. اگر $\mathbb{F}_p$ را میدان p عضوی در نظر بگیریم، آنگاه نویسندگان فوق نشان دادند که هیچ زیرگروه منظمی با شرایط فوق برای گروه‌های $\mathrm{AGL}_2(\mathbb{F}_p)$ به ازای هر عدد اول p، $\mathrm{AGL}_3(\mathbb{F}_p)$ به ازای عدد اول $p > 2$ و برای $\mathrm{AGL}_4(\mathbb{F}_2)$ وجود ندارد.

اولین مثالی که دارای چنین زیرگروه‌هایی باشد توسط هگدوس درسال ۲۰۰۰ در مقاله‌ی [۴] برای حالت $\mathbb{F} = \mathbb{F}_p$ ساخته شد. به شکل دقیق‌تر هگدوس ثابت کرد که گروه $\mathrm{AGL}_n(\mathbb{F}_p)$ شامل یک زیرگروه منظم بدون هیچ انتقال غیر بدیهی است هرگاه:

الف) $n = 3$ یا $n \geq 5$ اگر $p = 2$ باشد. یا

ب) $n \geq 4$ اگر $p > 2$ باشد.

روش‌هایی که هگدوس استفاده کرد اخیراً توسط کاتینو[4]، کولازو[5] و استفانلی[6] در سال ۲۰۱۶ در مقاله‌ی [۳] مورد استفاده قرار گرفت تا نتایج هگدوس برای $\mathbb{F} = \mathbb{F}_{p^l}$ توسعه داده شود.

در فصل اول این پایان نامه به بیان مفاهیم و تعاریف مقدماتی خواهیم پرداخت که در طول پایان نامه از آنها استفاده می شود.

فصل دوم پایان نامه به بررسی گروههای آفین و زیرگروههای منظم و نتایج به دست آمده اختصاص دارد.

در فصل سوم این پایان نامه ما نتایج بدست آمده در مورد عدم وجود چنین زیرگروه‌هایی منظمی که در [۶] بیان شده است را برای یک میدان دلخواه تعمیم می‌دهیم و همچنین مثالهایی در مورد وجود زیرگروههای منظم ارائه خواهیم داد. مطالب این فصل که فصل اصلی پایان نامه می باشد برگرفته از [۷] است.

[1] Liebeck [2] Praeger [3] Saxl [4] Catino [5] Colazzo [6] Stefanelli

فهرست مطالب

فهرست نمادها

فصل اول

مفاهیم مقدماتی

۱ـ۱ مقدماتی از نظریه گروه‌ها

در این بخش برخی مطالب مقدماتی که در طول پایان نامه از آنها استفاده می کنیم را بیان خواهیم کرد. فرض کنید که G یک گروه باشد. عضو خنثی گروه G را با نماد ۱ و زیرگروه بدیهی را نیز با همان نماد ۱ نمایش میدهیم.

تعریف ۱ـ۱. فرض کنید که G یک گروه باشد و H زیرگروهی از G باشد. مرکزساز H در G را با نماد $C_G(H)$ نمایش داده و به صورت زیر تعریف می شود:

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

در حالت خاص $C_G(G)$ را مرکز گروه G نامیده و آنرا با نماد $Z(G)$ نمایش می‌دهند.

تعریف ۱ـ۲. فرض کنید که G یک گروه باشد و H زیرگروهی از G باشد. نرمال‌ساز H در G را با نماد $N_G(H)$ نمایش داده و به صورت زیر تعریف می شود:

$$N_G(H) = \{g \in G | Hg = gH\}$$

لم ۱ــ۳. *فرض کنید $(G,\star)$ و $(H,\circ)$ گروه‌هایی دلخواه باشند. در این صورت $G\times H$ با تعریف*

$$G\times H=\{(a,b)\ :\ a\in G, b\in H\}$$

همراه با عمل

$$(a,b).(a',b')=(a\star a', b\circ b')$$

یک گروه است.

تعریف ۱ــ۴. گروه $G\times H$ در لم قبل را حاصل ضرب مستقیم خارجی G و H می‌نامیم. هم‌چنین G و H را عامل‌های مستقیم $G\times H$ می‌نامیم.

تعریف ۱ــ۵. فرض کنید G یک گروه باشد و a و b اعضایی از G باشند. در این صورت گوییم a و b مزدوج یکدیگر در G هستند، هرگاه $x\in G$ وجود داشته باشد به طوری که $b=x^{-1}ax$. یعنی اگر a مزدوج b باشد، آن‌گاه b نیز مزدوج a است.

تعریف ۱ــ۶. فرض کنید H زیرگروهی از G باشد. زیرگروه K از G را مزدوج H در G می‌نامیم اگر $g\in G$ وجود داشته باشد به طوری که $K=gHg^{-1}$.

تعریف ۱ــ۷. فرض کنید $(G,\circ)$ و $(H,\star)$ دو گروه دلخواه باشند. در این صورت

الف) تابع $\alpha: G\to H$ را یک همریختی از گروه G به گروه H می‌نامیم هرگاه برای هر $x,y\in G$ داشته باشیم $\alpha(x\circ y)=\alpha(x)\star\alpha(y)$.

ب) یک همریختی از گروه G به گروه H را یک یکریختی از گروه G به گروه H می‌نامیم هرگاه α یک به یک و پوشا (تناظر یک به یک) نیز باشد. هم‌چنین تکریختی به معنای همریختی یک به یک بوده و بروریختی به معنای همریختی پوشا است.

ج) گروه G را با گروه H یکریخت می‌نامیم هرگاه یک یکریختی از G به H موجود باشد و در این حالت با نماد $(G,\circ)\cong(H,\star)$ و یا به طور ساده‌تر با نماد $G\cong H$ نشان می‌دهیم. (اگر G با H یکریخت نباشد، از نماد $G\ncong H$ استفاده می‌کنیم.)

د) یک یکریختی از گروه G به خودش را یک خودریختی از G می‌نامیم.

قضیه ۱ــ۸ (قضیه اول یکریختی). *فرض کنید* $\alpha : G \to H$ *یک همریختی از گروه* G *به گروه* H *باشد. در این صورت* $\operatorname{Im}\alpha \cong \frac{G}{\operatorname{Ker}\alpha}$.

برهان. به قضیه ۳.۵.۱۲ از [۲] مراجعه شود. □

قضیه ۱ــ۹ (قضیه دوم یکریختی). *فرض کنید* G *یک گروه و* $N \trianglelefteq G$ *و* $H \leq G$. *در این صورت*

الف) $HN \leq G$

ب) $N \trianglelefteq HN$.

ج) $H \cap N \trianglelefteq H$.

د) $\frac{HN}{N} \cong \frac{H}{H\cap N}$.

برهان. به قضیه ۳.۵.۱۴ از [۲] مراجعه شود. □

قضیه ۱ــ۱۰ (قضیه سوم یکریختی). *فرض کنید* G *یک گروه و* $N \trianglelefteq G$ *و* $H \trianglelefteq G$ *و* $N \subseteq H$. *در این صورت* $N \trianglelefteq H$، $\frac{H}{N} \trianglelefteq \frac{G}{N}$ *و* $\frac{\frac{G}{N}}{\frac{H}{N}} \cong \frac{G}{N}$.

برهان. به قضیه ۳.۵.۱۶ از [۲] مراجعه شود. □

تعریف ۱ــ۱۱. الف) همان‌گونه که در تعریف ۱ــ۷، بیان شد؛ یک همریختی یک به یک و پوشا از گروه G به خودش را یک خودریختی از G نامیده و مجموعه تمام خودریختی‌های گروه G را با $\operatorname{Aut}(G)$ نشان می‌دهیم.

ب) یک همریختی از گروه G به خودش را یک درون ریختی از G نامیده و مجموعه تمام درون ریختی‌های گروه G را با $\operatorname{End}(G)$ نشان می‌دهیم.

یک خودریختی از گروه G، یک تناظر یک به یک از G نیز است، پس یک جایگشت از G بوده و لذا $\operatorname{Aut}(G) \subseteq S_G$. همچنین مجموعه $\operatorname{Aut}(G)$ همراه با عمل ضرب جایگشت‌ها (ترکیب توابع) یک گروه است.

قضیه ۱ــ۱۲ (قضیه نرمال‌ساز ــ مرکزساز). *فرض کنید H زیرگروهی از گروه G باشد، در این صورت $C_G(H) \trianglelefteq N_G(H)$ و $\frac{N_G(H)}{C_G(H)}$ با زیرگروهی از $\mathrm{Aut}(H)$ یکریخت است.*

برهان. به قضیه ۴.۱.۲۰ از [۲] مراجعه شود. □

تعریف ۱ــ۱۳. فرض کنید a و b عضوهایی از گروه G باشند و A و B زیرگروه‌هایی از G باشند. در این صورت:

الف) جابه‌جاگر a و b که با $[a,b]$ نشان می‌دهیم عبارت است از $[a,b] = a^{-1}b^{-1}ab$.

ب) زیرگروه جابه‌جاگر A و B که با نماد $[A,B]$ نشان می‌دهیم عبارت است از زیرگروه

$$[A,B] = \langle [a,b] \mid a,b \in G \rangle.$$

ج) زیرگروه جابه‌جاگر $[G,G]$ را زیرگروه مشتق G (و یا گروه مشتق G) نامیده و با نماد G' نشان می‌دهیم

$$G' = \langle [a,b] \mid a,b \in G \rangle.$$

به عبارت دیگر زیرگروه تولید شده به وسیله تمام جابه‌جاگرهای اعضای گروه G را با G' نمایش می دهیم.

نکته ۱ــ۱۴ . فرض کنید G یک گروه و a، b و x اعضایی از آن و A و B زیرگروه‌هایی از G باشند. در این صورت:

الف) $[a,b] = e$ اگر و تنها اگر $ab = ba$.

ب) $[b,a] = b^{-1}a^{-1}ba = [a,b]^{-1}$.

جابه‌جاگر سه تایی $[a,b,c]$ را برابر با $[[a,b],c]$ تعریف می‌کنیم؛ هم‌چنین زیرگروه جابه‌جاگر سه تایی $[A,B,C]$ را برابر با $[[A,B],C]$ تعریف می‌کنیم. تعمیم جابه‌جاگرهای nــ تایی در تعریف ذیل آمده است.

تعریف ۱ـ۱۵. فرض کنید G یک گروه، $a_1, a_2, \ldots, a_n \in G$ و $A_1, A_2, \ldots, A_n$ زیرگروه‌هایی از G باشند. در این صورت جابه‌جاگرهای nـ تایی به طور بازگشتی به صورت زیر تعریف می‌شوند:

الف) $[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$.

ب) $[A_1, \ldots, A_{n-1}, A_n] = [[A_1, \ldots, A_{n-1}], A_n]$.

۱ـ۱ـ۱ گروه‌های پوچ‌توان

تعریف ۱ـ۱۶. در گروه G فرض کنید G_iها، $0 \leq i \leq n$، زیرگروه‌هایی از G باشند به طوری که

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G \tag{۱ـ۱}$$

در این صورت (۱ـ۱) را یک سری به طول n از G می‌نامیم. زیرگروه‌های G_i را جملات این سری و گروه‌های خارج قسمتی $\frac{G_i}{G_{i-1}}$ را عوامل این سری می‌نامیم. سری فوق را می‌توانیم به صورت

$$G = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = \{e\}$$

نیز بنویسیم (در حالت کلی نیازی نیست که G_iها در G نرمال باشند).

اگر به ازای هر i، $G_i \trianglelefteq G$، سری (۱ـ۱) را یک سری نرمال از G می‌نامیم.

تعریف ۱ـ۱۷. الف) فرض کنید $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$ یک سری نرمال برای گروه G باشد. در این صورت سری فوق را یک سری مرکزی برای G می‌نامیم هرگاه به ازای هر i، $\frac{G_i}{G_{i-1}} \leq Z\left(\frac{G}{G_{i-1}}\right)$ (همچنین گروه‌های $\frac{G_i}{G_{i-1}}$ را عوامل مرکزی G می‌نامیم).

ب) گروه G را پوچ‌توان می‌نامیم هرگاه G دارای یک سری مرکزی باشد.

تعریف ۱ـ۱۸. برای هر گروه G، زیرگروه‌های $\Gamma_n(G)$ را به طور بازگشتی به صورت زیر تعریف می‌کنیم

$\Gamma_1(G) = G$ و برای هر $n > 1$، $\Gamma_n(G) = [\Gamma_{n-1}, G]$.

دقت می‌کنیم که $\Gamma_n(G) \trianglelefteq G$ و $\Gamma_n(G) \leq \Gamma_{n-1}(G)$. همچنین بنابر تعریف فوق داریم

$$\Gamma_n(G) = \underbrace{[G, G, \dots, G]}_{n\text{ـبار}}.$$

دنباله نزولی $G = \Gamma_1(G) \geq \Gamma_2 \geq \Gamma_3(G) \geq \cdots$ را سری مرکزی پایینی G می‌نامیم.

قضیه ۱ـ۱۹. *فرض کنید که G یک گروه باشد. در اینصورت احکام زیر هم ارزند:*

الف. G پوچ‌توان است.

ب. یک عدد طبیعی مانند n موجود است به طوری که $\Gamma_n(G) = 1$.

برهان. به قضیه ۷.۵۴ از [۹] مراجعه شود. □

۱ـ۱ـ۲ عمل گروه روی مجموعه

تعریف ۱ـ۲۰. فرض کنید G یک گروه و X مجموعه‌ی ناتهی باشد. فرض کنید به ازای هر $g \in G$ و $x \in X$، عضو یکتایی از X که آن را با علامت $x.g$ نشان می‌دهیم وجود داشته باشد به طوری که

۱. به ازای هر $x \in X$ داشته باشیم $x1 = x$ که در آن $1 \in G$ عضو همانی گروه G است.

۲. $x(g_1g_2) = (xg_1)g_2 \quad \forall g_1, g_2 \in G\ ,\ x \in X$.

در این صورت گوییم گروه G روی مجموعه X عمل می‌کند.

تعریف ۱ـ۲۱. اگر $x \in X$ و $g \in G$. آن‌گاه مدار x را با علامت $\mathrm{orb}(x)$ نشان می‌دهیم و به صورت زیر تعریف می کنیم:

$$\mathrm{orb}(x) = \{xg \mid g \in G\}.$$

تعریف ۱ـ۲۲. فرض کنید G بر مجموعه‌ی ناتهی X عمل می‌کند و $x \in X$. در این صورت

$$\mathrm{stab}(x) = \{g \in G \mid xg = x\}$$

را پایدارساز x در G می‌نامند و داریم که $\mathrm{stab}(x) \leq G$.

قضیه ۱ــ۲۳. *فرض کنید G بر مجموعه‌ی X عمل می‌کند و $x \in X$. در این صورت تناظری یک به یک بین $\mathrm{orb}(x)$ و مجموعه‌ی همه‌ی هم‌دسته‌های راست $\mathrm{stab}(x)$ در G وجود دارد به خصوص اگر $\mathrm{orb}(x)$ متناهی باشد، آن‌گاه $|G : \mathrm{stab}(x)| = |\,\mathrm{orb}(x)|$.*

برهان. به قضیه‌ی ۲.۳.۲ از [۱] مراجعه شود. □

تعریف ۱ــ۲۴. فرض کنید G بر مجموعه‌ی X عمل کند. این عمل ترایا نامیده می‌شود اگر X تنها مدار عمل باشد. به عبارت دیگر برای هر $x_1, x_2 \in X$، عنصری از G مانند g وجود داشته باشد به طوری که $x_1 g = x_2$.

تعریف ۱ــ۲۵. عمل G بر مجموعه‌ی X را منظم گوییم اگر این عمل ترایا باشد و به ازای هر $x \in X$، $\mathrm{stab}(x) = 1$.

تعریف ۱ــ۲۶. فرض کنید گروه G روی مجموعه X عمل کند. در این صورت برای هر $g \in G$، تابع $\tau_g : X \to X$ با ضابطه $\tau_g(x) = gx$ یک جایگشت از X است. هم‌چنین تابع $\tau : X \to X$ با ضابطه $\tau(g) = \tau_g$ یک همریختی است که آن را نمایش جایگشتی G متناظر با این عمل می‌نامیم.

تعریف ۱ــ۲۷. فرض کنید G بر مجموعه‌ی X عمل کند. این عمل را صادق (باوفا) گوییم اگر نمایش جایگشتی متناظر با G یک به یک باشد.

۱ــ۱ــ۳ حاصلضرب نیم مستقیم

فرض کنید که H و K دو گروه باشند. گوییم گروه H روی K به عنوان یک گروه عمل می کند هرگاه H روی K به عنوان مجموعه عمل کند (در اینجا عمل عضو h روی عضو k را با نماد k^h نمایش میدهیم) و علاوه بر آن به ازای هر k_1, k_2 از K و هر عضو h از H داشته باشیم:

$$(k_1 k_2)^h = k_1^h k_2^h.$$

تعریف ۱ـ۲۸. فرض کنید که H و K دو گروه باشند و H روی K به عنوان گروه عمل کند. در اینصورت مجموعه

$$H \times K = \{(h,k) | h \in H, k \in K\}$$

همراه با عمل زیر تشکیل یک گروه می دهد:

$$(h_۱, k_۱) \cdot (h_۲, k_۲) = (h_۱ h_۲, k_۱^{h_۲} k_۲)$$

این گروه را حاصلضرب نیم مستقیم K توسط H نامیده و آنرا با نماد $H \ltimes K$ نمایش می دهیم.

۱ـ۲ فضاهای برداری

در این پایان نامه ماتریس همانی $n \times n$ را با نماد I_n و یا در جایی که بیم ابهام نباشد با نماد I نمایش می‌دهیم.

فرض کنید $\mathbb{F}$ یک میدان باشد. بردار سطری که مولفه iام آن برابر ۱ و بقیه مولفه‌ها برابر صفر باشد را با نماد e_i نمایش می‌دهیم. یعنی:

$$e_i = (\circ, \ldots, \circ, \underset{\text{مولفه } i\text{ام}}{\circ}, \circ, \ldots, \circ).$$

مجموعه $\{e_۱, \ldots, e_n\}$ پایه‌ای برای فضای برداری $\mathbb{F}^n$ است که آن را پایه استاندارد (متعارف) $\mathbb{F}^n$ می‌نامند.

ماتریس $n \times n$ که درایه (i,j)ام آن برابر ۱ باشد و بقیه درایه‌های آن برابر صفر باشد را با نماد

$E_{i,j}$ نمایش می‌دهیم. یعنی:

$$E_{i,j} = \begin{array}{c} \text{ستون } j\text{ام} \\ \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} \end{array} \begin{array}{l} \\ \\ \\ \\ \rightarrow \text{سطر } i\text{ام} \\ \\ \\ \\ \end{array}$$

قضیه زیر در مورد ماتریسهای E_{ij} در بسیاری از اثباتهای پایان نامه مورد استفاده قرار خواهد گرفت.

قضیه ۱ــ۲۹. *فرض کنید که E_{ij} ماتریسی باشد که درایه (i,j)ام آن برابر ۱ و بقیه درایه‌های آن برابر صفر باشد. در اینصورت داریم:*

الف. $E_{ij}E_{kl} = \delta_{jk}E_{il}$.

ب. اگر $i \neq j$ *آنگاه* $E_{ij}^2 = 0$ *و اگر* $i = j$ *آنگاه* $E_{ij}^2 = E_{ij}$.

۱ــ۲ــ۱ حاصلضرب تانسوری

تعریف ۱ــ۳۰. فرض کنید A یک ماتریس $m \times n$ و B یک ماتریس $p \times q$ باشد. حاصل‌ضرب کرونکر A در B را با نماد $A \otimes B$ نمایش می‌دهند و یک ماتریس $pm \times qn$ است که به شکل بلوکی زیر است:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

که در آن $A = [a_{ij}]$. به صورت دقیق‌تر اگر $B = [b_{ij}]$ آن‌گاه:

$$A \otimes B = \left[\begin{array}{ccc|c|ccc} a_{11}b_{11} & \cdots & a_{11}b_{1q} & & a_{1n}b_{11} & \cdots & a_{1n}b_{1q} \\ \vdots & & \vdots & \cdots & \vdots & & \vdots \\ a_{11}b_{p1} & \cdots & a_{11}b_{pq} & & a_{1n}b_{p1} & \cdots & a_{1n}b_{pq} \\ \hline \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \hline a_{m1}b_{11} & \cdots & a_{m1}b_{1q} & & a_{mn}b_{11} & \cdots & a_{mn}b_{1q} \\ \vdots & & \vdots & \cdots & \vdots & & \vdots \\ a_{m1}b_{1q} & \cdots & a_{mn}b_{11} & & a_{mn}b_{p1} & \cdots & a_{mn}b_{pq} \end{array}\right]$$

به عنوان مثال داریم:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} = \left[\begin{array}{c|c} 1\begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} & 2\begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} \\ \hline 3\begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} & 4\begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} \end{array}\right] = \begin{bmatrix} 0 & 5 & 0 & 10 \\ 6 & 7 & 12 & 14 \\ 0 & 15 & 0 & 20 \\ 18 & 21 & 24 & 28 \end{bmatrix}.$$

حاصل‌ضرب تانسوری (کرونکر) دارای خواص زیر است:

۱. $A \otimes (B + C) = A \otimes B + A \otimes C$

۲. $(B + C) \otimes A = B \otimes A + C \otimes A$

۳. $(kA) \otimes B = A \otimes (kB) = k(A \otimes B)$

۴. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$

۵. $A \otimes 0 = 0 \otimes A = 0$

۶. $(A \otimes B)(C \otimes D) = (AC \otimes BD)$. در حالت خاص می‌توان نوشت

$$A \otimes B = (A \otimes I_1)(I_2 \otimes B).$$

۷. $A \otimes B$ معکوس‌پذیر است اگر و تنها اگر A و B معکوس‌پذیر باشند و

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

۸. $A \otimes B = ۰$ اگر و تنها اگر $A = ۰$ یا $B = ۰$.

برهان. برای اثبات این خواص به [۱۰] مراجعه شود. □

۱ـ۲ـ۲ فرم‌های ژوردان

تعریف ۱ـ۳۱. فرض کنید T یک عملگر خطی (یا A یک ماتریس $n \times n$) باشد. اسکالر λ را یک مقدار ویژه T (یا A) می‌نامند هرگاه بردار غیر صفری مانند x موجود باشد به طوری که $T(x) = \lambda x$ ($Ax = \lambda x$). هم‌چنین بردار x را یک بردار ویژه متناظر با λ می‌نامند.

تعریف ۱ـ۳۲. فرض کنید A یک ماتریس $n \times n$ باشد. چندجمله‌ای مشخصه A را با نماد $C_A(x)$ نمایش داده و به صورت $C_A(x) = \det(xI - A)$ تعریف می‌شود. ریشه‌های $C_A(x)$ همان مقادیر ویژه A می‌باشند.

تعریف ۱ـ۳۳. فرض کنید λ یک اسکالر باشد. ماتریس J_n به صورت

$$J_n = \begin{bmatrix} \lambda & ۱ & ۰ & \cdots & ۰ \\ ۰ & \lambda & ۱ & \cdots & ۰ \\ ۰ & ۰ & \lambda & \cdots & ۰ \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ ۰ & ۰ & \cdots & ۰ & \lambda \end{bmatrix}$$

را یک بلوک ژوردان می‌نامند. یعنی J_n ماتریسی است که درایه‌های روی قطر اصلی آن λ، درایه‌هایی که بلافاصله بالای قطر اصلی‌اند ۱ و بقیه درایه‌های آن صفر است.

ماتریس J به صورت زیر

$$J = \begin{bmatrix} J_۱ & ۰ & ۰ & \cdots & ۰ \\ ۰ & J_۲ & ۰ & \cdots & ۰ \\ ۰ & ۰ & J_۳ & \cdots & ۰ \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ۰ & ۰ & ۰ & \cdots & J_r \end{bmatrix}$$

(این ماتریس را در بسیاری از موارد به صورت $\mathrm{diag}(J_1, J_2, \dots, J_r)$ نمایش می‌دهند) که در آن J_i یک بلوک ژوردان از اندازه $m_i \times m_i$ باشد را یک ماتریس به صورت نرمال ژوردان می‌نامند.

فرض کنید A یک ماتریس مربعی روی میدان $\mathbb{F}$ باشد. با توجه به قضیه‌ای در جبرخطی، اگر تمام مقادیر ویژه A در $\mathbb{F}$ باشند، آنگاه A دارای یک فرم نرمال ژوردان خواهد بود به این معنی که A با یک ماتریس به فرم نرمال ژوردان متشابه خواهد بود.

در این پایان نامه از نماد J_m برای بلوک ژوردان بالا مثلثی تک‌توان استفاده می‌کنیم. یعنی

$$J_m = I_m + \sum_{i=1}^{m-1} E_{i,i+1}$$

که در حقیقت همان بلوک ژوردان است که درایه‌های روی قطر اصلی آن برابر ۱ می‌باشد. به عنوان مثال

$$J_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad , \quad J_4 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

۱ــ۲ــ۳ فرم‌های دوخطی

تعریف ۱ــ۳۴. فرض کنید V یک فضای برداری روی میدان $\mathbb{F}$ باشد. منظور از یک فرم دوخطی روی V تابعیمانند Q است به طوری که به ازای هر زوج مرتب α و β از بردارهای V یک اسکالر $Q(\alpha, \beta)$ از $\mathbb{F}$ را متناظر می‌کند به طوری که به ازای هر $c \in \mathbb{F}$ و هر $\alpha_1, \alpha_2, \beta_1, \beta_2 \in V$:

$$Q(c\alpha_1 + \alpha_2, \beta) = cQ(\alpha_1, \beta) + Q(\alpha_2, \beta)$$

$$Q(\alpha, c\beta_1 + \beta_2) = cQ(\alpha, \beta_1) + Q(\alpha, \beta_2).$$

به عبارت دیگریک فرم دوخطی روی V تابعی مانند Q است که

$$Q : V \times V \to \mathbb{F}$$

و تابع Q با شرط ثابت بودن هر کدام از مولفه‌هایش، نسبت به مولفه دیگر خطی باشد.

۱ـ۲ـ۴ فرم درجه دوم

تعریف ۱ـ۳۵. منظور از یک فرم درجه دوم تابعی مانند $q: V \to \mathbb{F}$ است به طوری که به ازای هر $a \in \mathbb{F}$ و هر $v \in V$ داشته باشیم

$$q(av) = a^2 q(v)$$

و تابع

$$q_1 : V \times V \to \mathbb{F}$$

$$q_1(u,v) = q(u+v) - q(u) - q(v)$$

دوخطی باشد. به صورت کلی‌تر یک فرم دوخطی nـتایی یک چندجمله‌ای همگن از درجه دو بر حسب n متغیر با ضرایب در میدان $\mathbb{F}$ است. یعنی

$$q(x_1, \dots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j \ , \quad a_{ij} \in \mathbb{F}.$$

این فرمول را می‌توان بر حسب ماتریس‌ها بازنویسی کرد. فرض کنید X یک بردار ستونی با مولفه‌های x_1، ...، x_n باشد و $A = [a_{ij}]$ یک ماتریس $n \times n$ روی $\mathbb{F}$ باشد که درایه‌های آن همان ضرایب q باشد. در این صورت

$$q(x) = X^T A X.$$

تعریف ۱ـ۳۶. گروه ایزومتری‌های یک فرم درجه دوم Q روی $\mathbb{F}^m$ را با نماد $O_m(\mathbb{F}, Q)$ نمایش داده و به صورت زیر است

$$O_m(\mathbb{F}, Q) = \{ A \in \mathrm{GL}_m(\mathbb{F}) \mid Q(vA) = Q(v) \ \ \forall v \in \mathbb{F}^n \} .$$

۱ـ۲ـ۵ ماتریس جایگشتی

تعریف ۱ـ۳۷. فرض کنید α یک جایگشت روی مجموعه $\{۱,\dots,m\}$ باشد. ماتریس جایگشتی $\mathcal{P}_\alpha$ از اندازه $m\times m$ را به صورت $\mathcal{P}_\alpha=(P_{ij})$ تعریف می‌کنیم که

$$\begin{cases} P_{ij}=۱ & \text{اگر } j=\alpha(i) \\ P_{ij}=۰ & \text{در غیر این صورت} \end{cases}$$

در حقیقت هر ماتریس جایگشتی با یک جایگشت روی ستون‌های (سطرهای) ماتریس همانی حاصل می‌شود. چون درایه‌های واقع در سطر iام ماتریس جایگشتی $\mathcal{P}$ همگی به غیر از درایه واقع در ستون $\alpha(i)$ برابر صفرند و درایه واقع در ستون $\alpha(i)$ام برابر ۱ است. بنابراین $\mathcal{P}_\alpha$ را می‌توان به صورت زیر نمایش داد:

$$\mathcal{P}_\alpha=\begin{bmatrix} e_{\alpha(۱)} \\ e_{\alpha(۲)} \\ \vdots \\ e_{\alpha(m)} \end{bmatrix}.$$

به عنوان مثال اگر $\alpha=(۱\ ۲)(۳\ ۴)$، آنگاه

$$\mathcal{P}_\alpha=\begin{bmatrix} e_{\alpha(۱)} \\ e_{\alpha(۲)} \\ e_{\alpha(۳)} \\ e_{\alpha(۴)} \end{bmatrix}=\begin{bmatrix} e_۲ \\ e_۱ \\ e_۴ \\ e_۳ \end{bmatrix}=\begin{bmatrix} ۰ & ۱ & ۰ & ۰ \\ ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ \end{bmatrix}.$$

اگر $\mathcal{P}$ یک ماتریس جایگشتی باشد و A یک ماتریس باشد آنگاه حاصل $\mathcal{P}A$ جایگشتی روی سطرهای A و حاصل $A\mathcal{P}$ جایگشتی روی ستون‌های A خواهد بود.

فصل دوم

گروه‌های آفین و زیرگروه‌های منظم

در این فصل ابتدا به بیان تعاریف لازم در مورد گروه‌های آفین خواهیم پرداخت و سپس زیرگروه‌های منظم را بررسی خواهیم کرد. برخی از کارهایی که در زمینه زیرگروه‌های منظم انجام شده است را در این فصل بیان و اثبات خواهیم کرد.

۲ـ۱ گروه‌های آفین

تعریف ۲ـ۱. مجموعه‌ی تمام ماتریس‌های $n \times n$ با درایه‌هایی در میدان $\mathbb{F}$ که دترمینان آن مخالف صفر است را گروه خطی عمومی یا عام از درجه‌ی n روی میدان $\mathbb{F}$ می‌نامند و با $\mathrm{GL}_n(\mathbb{F})$ نمایش می‌دهند. به صورت مشابه مجموعه تمام عملگرهای خطی معکوس‌پذیر روی فضای برداری V را گروه خطی عام روی فضای برداری V نامیده و آن‌را با نماد $GL(V)$ نمایش می‌دهند.

تعریف ۲ـ۲. مجموعه‌ی تمام ماتریس‌های $n \times n$ معکوس پذیر با درایه‌هایی در میدان $\mathbb{F}$ که دترمینان آن‌ها برابر ۱ باشد را گروه خطی خاص از درجه‌ی n روی میدان $\mathbb{F}$ می‌نامند و با $\mathrm{SL}_n(\mathbb{F})$ نمایش می‌دهند.

فرض کنید V یک فضای برداری باشد و $\mathrm{GL}(V)$ گروه خطی عام V باشد. در این صورت $\mathrm{GL}(V)$ به طور طبیعی روی V عمل می‌کند. بنابراین حاصلضرب نیم مستقیم V توسط $\mathrm{GL}(V)$ را

می‌توان تشکیل داد. این حاصلضرب نیم مستقیم را گروه آفین V نامیده و با نماد $\mathrm{AGL}(V)$ نمایش می‌دهند. در حالت خاص که V را فضای برداری $\mathbb{F}^n$ از بعد n روی میدان $\mathbb{F}$ در نظر بگیریم آن را با نماد $\mathrm{AGL}_n(\mathbb{F})$ نمایش می‌دهند، بنابراین:

$$\mathrm{AGL}_n(\mathbb{F}) = \mathbb{F}^n \rtimes \mathrm{GL}_n(\mathbb{F}).$$

اعضای گروه $\mathrm{AGL}_n(\mathbb{F})$ را می‌توان به شکل ماتریسی بلوکی نیز نمایش داد که در این حالت هر عضو از $\mathrm{AGL}_n(\mathbb{F})$ به شکل زیر است:

$$\left(\begin{array}{c|c} ۱ & v \\ \hline ۰ & A \end{array}\right)\ ,\ v \in \mathbb{F}^n\ ,\ A \in \mathrm{GL}_n(\mathbb{F}).$$

بنابراین با این نمایش ماتریسی داریم:

$$\mathrm{AGL}_n(\mathbb{F}) = \left\{ \begin{pmatrix} ۱ & v \\ ۰ & A \end{pmatrix} \quad \Big| \quad v \in \mathbb{F}^n\ ,\ A \in \mathrm{GL}_n(\mathbb{F}) \right\}.$$

عمل ضرب در گروه $AGL_n(F)$ به صورت بلوکی به شکل زیر است:

$$\begin{pmatrix} ۱ & v \\ ۰ & A \end{pmatrix} \cdot \begin{pmatrix} ۱ & v' \\ ۰ & B \end{pmatrix} = \begin{pmatrix} ۱ & v' + vB \\ ۰ & AB \end{pmatrix}$$

همچنین معکوس یک عضو به صورت زیر است:

$$\begin{pmatrix} ۱ & v \\ ۰ & A \end{pmatrix}^{-۱} = \begin{pmatrix} ۱ & -vA^{-۱} \\ ۰ & A^{-۱} \end{pmatrix}$$

برای هر $v \in \mathbb{F}^n$، تابع T_v را به صورت زیر تعریف می‌کنیم:

$$T_v = x + v.$$

و قرار می‌دهیم

$$\mathcal{T} = \{T_v \mid v \in \mathbb{F}^n\}.$$

در این صورت $\mathcal{T}$ زیرگروهی از گروه $\mathrm{AGL}_n(\mathbb{F})$ است که آن را زیرگروه انتقال می‌نامند.

فرض کنید

$$\Omega = \{(۱, v) \mid v \in \mathbb{F}^n\}.$$

در این صورت $\mathrm{AGL}_n(\mathbb{F})$ با ضرب معمولی ماتریس‌ها از راست روی مجموعه Ω عمل می‌کند، یعنی به ازای هر $x \in \Omega$ و هر $\mathcal{A} \in \mathrm{AGL}_n(\mathbb{F})$، عمل به صورت زیر تعریف می‌شود:

$$x\mathcal{A} = xA.$$

واضح است که تعریف فوق واقعاً یک عمل $\mathrm{AGL}_n(\mathbb{F})$ بر Ω را مشخص می‌کند زیرا:

۱. به ازای هر x از Ω داریم

$$x \begin{pmatrix} ۱ & ۰ \\ ۰ & I \end{pmatrix} = x.$$

۲. به ازای هر $\mathcal{A}_۱, \mathcal{A}_۲ \in \mathrm{AGL}_n(\mathbb{F})$ و هر $x \in \Omega$، با توجه به ضرب ماتریس‌ها داریم

$$x.(\mathcal{A}_۱\mathcal{A}_۲) = x(\mathcal{A}_۱\mathcal{A}_۲) = (x\mathcal{A}_۱)\mathcal{A}_۲ = (x.\mathcal{A}_۱).\mathcal{A}_۲.$$

۲ــ۲ زیرگروه‌های منظم

تعریف ۲ــ۳. زیرگروه R از گروه $\mathrm{AGL}_n(\mathbb{F})$ را یک زیرگروه منظم گوییم هرگاه R به صورت منظم روی مجموعه Ω عمل کند، به عبارت دیگر R روی Ω انتقالی باشد و اعضای غیربدیهی R هیچ نقطه‌ای را ثابت نگه ندارند.

قضیه ۲ــ۴. *زیرگروه R از $\mathrm{AGL}_n(\mathbb{F})$ منظم است اگر و تنها اگر به ازای هر $v \in \mathbb{F}^n$، عضو منحصر به فردی از R موجود باشد به طوری که $(۱, v)$ سطر اول آن باشد.*

برهان. ابتدا فرض کنید که R منظم است. فرض کنید $v \in \mathbb{F}^n$ دلخواه باشدد. چون R منظم است پس عمل R روی Ω انتقالی است. لذا عضوی از R مانند $\mathcal{A}$ موجود است که

$$(۱, ۰, \ldots, ۰)\mathcal{A} = (۱, v).$$

با توجه به عمل ضرب ماتریس‌ها واضح است که در این صورت سطر اول $\mathcal{A}$ به صورت $(1, v)$ خواهد بود. پس به ازای هر $v \in \mathbb{F}^n$، عضوی از R موجود است که $(1, v)$ سطر اول آن است. حال نشان می‌دهیم که این عضو منحصر به فرد است. فرض کنید که $\mathcal{B}$ عضو دیگری از R باشد که $(1, v)$ سطر اول آن است. در این صورت

$$(1, 0, \dots, 0)\mathcal{A} = (1, v) = (1, 0, \dots, 0)\mathcal{B}.$$

بنابراین $\mathcal{A}\mathcal{B}^{-1}$ عضو $(1, 0, \dots, 0)$ را ثابت نگه می‌دارد که با توجه به منظم بودن R باید داشته باشیم $\mathcal{A}\mathcal{B}^{-1} = I$. بنابراین $\mathcal{A} = \mathcal{B}$. پس به ازای هر $v \in \mathbb{F}^n$ عضو منحصر به فردی از R موجود است که $(1, v)$ سطر اول آن است.

برعکس، فرض کنید که به ازای هر $v \in \mathbb{F}^n$ عضو منحصر به فردی از R موجود است که $(1, v)$ سطر اول آن است. نشان می‌دهیم R منظم است. اگر $(1, v) \in \Omega$ دلخواه باشد طبق فرض عضو منحصر به فردی مانند $\mathcal{A} = \left(\begin{smallmatrix} 1 & V \\ 0 & A \end{smallmatrix}\right) \in R$ موجود است. پس

$$(1, 0, \dots, 0)\mathcal{A} = (1, v).$$

بنابراین هر عضو Ω عضوی از مدار عضو $(1, 0, \dots, 0)$ است و لذا عمل R روی Ω انتقالی است. علاوه بر این اگر $\mathcal{A} = \left(\begin{smallmatrix} 1 & V \\ 0 & A \end{smallmatrix}\right)$ عضوی غیر بدیهی از R باشد که عضوی از Ω مانند $(1, x)$ را ثابت نگه می‌دارد در این صورت داریم $(1, x)\mathcal{A} = (1, x)$. بنابراین

$$(1, x) \begin{pmatrix} 1 & v \\ 0 & A \end{pmatrix} = (1, v + xA) = (1, x) \Rightarrow v + xA = x. \tag{2-1}$$

از طرفی می‌دانیم که عضوی منحصر به فرد از R موجود است که $(1, x)$ سطر اول آن است. فرض کنیم این عضو $\mathcal{B} = \left(\begin{smallmatrix} 1 & x \\ 0 & B \end{smallmatrix}\right)$ باشد. حال حاصل ضرب $\mathcal{B}\mathcal{A}$ را در نظر می‌گیریم:

$$\mathcal{B}\mathcal{A} = \begin{pmatrix} 1 & x \\ 0 & B \end{pmatrix} \begin{pmatrix} 1 & v \\ 0 & A \end{pmatrix} = \begin{pmatrix} 1 & v + xA \\ 0 & BA \end{pmatrix} \overset{(2-1)}{=} \begin{pmatrix} 1 & x \\ 0 & BA \end{pmatrix}.$$

پس عضو دیگری از R یافتیم که $(1, x)$ سطر اول آن است. اگر $\mathcal{B}\mathcal{A}$ همان $\mathcal{B}$ باشد آن‌گاه خواهیم داشت $\mathcal{A} = I$ که متناقض با این است که $\mathcal{A}$ عضوی غیر بدیهی از R است. پس $\mathcal{B}\mathcal{A}$ عضو دیگری

از R است که $(۱, x)$ سطر اول آن است و این هم متناقض با این است که به ازای هر $x \in \mathbb{F}^n$ عضو منحصر به فردی از R موجود است که $(۱, x)$ سطر اول آن است. پس هیچ عضو غیر بدیهی از R نقطه ثابت ندارد و چون عمل R هم انتقالی بود پس R یک زیرگروه منظم است. $\square$

نکته ۲ـ۵. فرض کنید R یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ باشد. با توجه به قضیه‌ی قبل به ازای هر $v \in \mathbb{F}^n$ عضو منحصر به فردی از R موجود است که $(۱, v)$ سطر اول آن است. اگر این عضو منحصر به فرد به صورت $\begin{pmatrix} ۱ & v \\ ۰ & R(v) \end{pmatrix}$ باشد آن‌گاه می‌توانیم R را در حقیقت تابعی از $\mathbb{F}^n$ به $\mathrm{GL}_n(\mathbb{F})$ در نظر بگیریم که هر عضو v را به $R(v)$ می‌برد.

مثال ۲ـ۶. فرض کنید که R زیرمجموعه متشکل از تمام ماتریس‌هایی باشد که به صورت زیر است:

$$R = \left\{ \begin{bmatrix} ۱ & v \\ ۰ & I \end{bmatrix} \mid v \in \mathbb{F}^n \right\}.$$

در این صورت با توجه به تعریف حاصل‌ضرب دو عضو در $\mathrm{AGL}_n(\mathbb{F})$ داریم:

$$\begin{bmatrix} ۱ & v \\ ۰ & I \end{bmatrix} \begin{bmatrix} ۱ & -v' \\ ۰ & I \end{bmatrix} = \begin{bmatrix} ۱ & -v'+v \\ ۰ & I \end{bmatrix} \in R$$

که نشان می‌دهد R یک زیرگروه است.

هم‌چنین باتوجه به تعریف اعضای R، به ازای هر عضو $v \in \mathbb{F}^n$، عضو منحصر به فردی از R موجود است که $(۱, v)$ سطر اول آن است و لذا طبق قضیه ؟؟، R زیرگروه منظمی از $\mathrm{AGL}_n(\mathbb{F})$ است. زیرگروه R در حقیقت همان زیرگروه انتقال است.

مثال ۲ـ۷. فرض کنید که $U = U_{n+۱}(\mathbb{F})$ گروه ماتریس‌های بالا مثلثی تک‌توان از درجه $n+۱$ روی میدان $\mathbb{F}$ باشد. هم‌چنین فرض کنید که $J \in U$ یک بلوک ژوردان $(n+۱) \times (n+۱)$ با چندجمله‌ای مینیمال $(x-۱)^{n+۱}$ باشد. در این صورت در [۱۱] نشان داده شده است که $\mathbf{C}_U(J)$ یک زیرگروه آبلی منظم از $\mathrm{AGL}_n(\mathbb{F})$ است.

توجه کنید که در مثال‌های بالا زیرگروه‌های منظم بیان شده آبلی هستند.

مثال ۲ـ۸. فرض کنید که R زیرمجموعه متناهی $\mathrm{AGL}_2(\mathbb{R})$ متشکل از ماتریس‌های به صورت زیر باشد:

$$R = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & e^y & 0 \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; x, y \in \mathbb{R} \right\}.$$

در این صورت اولاً R زیرگروهی از $\mathrm{AGL}_2(\mathbb{R})$ است. زیرا اولاً R بسته است، چون

$$\begin{pmatrix} 1 & x & y \\ 0 & e^y & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & e^{y'} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x' + xe^y & y' + y \\ 0 & e^{y+y'} & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (2-2)$$

و هم‌چنین معکوس هر عضو R به صورت زیر است.

$$\begin{pmatrix} 1 & x & y \\ 0 & e^y & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -xe^y & -y \\ 0 & e^{-y} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in R$$

حال چون به ازای هر $(x, y) \in \mathbb{R}^2$، عضو منحصر به فردی از R موجود است که $(1, x, y)$ سطر اول آن است پس طبق قضیه ؟؟، R زیرگروه منظمی از $\mathrm{AGL}_2(\mathbb{R})$ است (توجه کنید که منحصر به فردی به این دلیل است که وقتی سطر اول مشخص باشد تنها درایه متغیر دیگر ماتریس که درایه $(2, 2)$ام یعنی e^y است بلافاصله از روی سطر اول مشخص می‌شود). این زیرگروه R غیر آبلی است زیرا به عنوان مثال داریم:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & e & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & e & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & e^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

اما

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & e & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & e & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & e & 2 \\ 0 & e^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

پس R یک زیرگروه منظم غیر آبلی از $\mathrm{AGL}_2(\mathbb{R})$ است. هم‌چنین R شامل انتقال‌های غیر بدیهی هم هست، مثلاً اگر

$$A=\begin{pmatrix}1 & 1 & 0\\ 0 & e^{0} & 0\\ 0 & 0 & 1\end{pmatrix}\in R$$

آن‌گاه A یک انتقال غیر بدیهی است.

مثال ۲ـ۹. فرض کنید $n\geq 3$ و $i\neq j$ و قرار می‌دهیم:

$$R=\left\{\begin{pmatrix}1 & v & x\\ 0 & I+xE_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix}\quad\Big|\quad v\in\mathbb{F}^{n-1},\ x\in\mathbb{F}\right\}.$$

در این صورت R زیرگروهی از $\mathrm{AGL}_n(\mathbb{F})$ است، زیرا اولاً R بسته است چون

$$\begin{pmatrix}1 & v & x\\ 0 & I+xE_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & v' & x'\\ 0 & I+x'E_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix}=\begin{pmatrix}1 & v'+v+x'vE_{ij} & x'+x\\ 0 & I+(x'+x)E_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix}.$$

هم‌چنین معکوس هر عضو R به صورت زیر است

$$\begin{pmatrix}1 & v & x\\ 0 & I+xE_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}0 & v(-I+xE_{i,j}) & -x\\ 0 & I-xE_{ij} & 0\\ 0 & 0 & 1\end{pmatrix}\in R$$

هم‌چنین به ازای هر $(v,x)\in\mathbb{F}^n$ سطرهای دوم به بعد بلافاصله از روی سطر اول مشخص می‌شوند که نشان می‌دهد عضو منحصر به فردی از R موجود است که $(1,v,x)$ سطر اول آن است. پس طبق قضیه ؟؟، R منظم است. هم‌چنین اگر v برداری باشد که مولفه iام آن مخالف صفر باشد (که آن را v_i می‌نامیم) و قرار دهیم

$$A=\begin{pmatrix}1 & v & 1\\ 0 & I+E_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix},\qquad B=\begin{pmatrix}1 & v & 0\\ 0 & I & 0\\ 0 & 0 & 1\end{pmatrix}$$

آن‌گاه

$$AB = \begin{pmatrix} 1 & 2v & 1 \\ 0 & I + E_{i,j} & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2v + vE_{ij} & 1 \\ 0 & I + E_{i,j} & 0 \\ 0 & 0 & 1 \end{pmatrix} = BA$$

زیرا در صورت برابری باید داشته باشیم $2v = 2v + vE_{ij}$ که نتیجه می‌دهد $vE_{ij} = 0$ و لذا $v_i = 0$ که تناقض است. بنابراین زیرگروه R یک زیرگروه غیر آبلی است. هم‌چنین اگر قرار دهیم

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & I & 0 \\ 0 & 0 & 1 \end{pmatrix} \in R$$

آن‌گاه A یک انتقال غیر بدیهی از R است و لذا R شامل تمام انتقال‌های غیر بدیهی است.

تابع π را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned} \pi : \mathrm{AGL}_n(\mathbb{F}) &\to \mathrm{GL}_n(\mathbb{F}) \\ \begin{pmatrix} 1 & v \\ 0 & A \end{pmatrix} &\mapsto A \end{aligned}$$

واضح است که π یک همریختی از $\mathrm{AGL}_n(\mathbb{F})$ به $\mathrm{GL}_n(\mathbb{F})$ است زیرا،

$$\begin{aligned} \pi\left(\begin{pmatrix} 1 & v \\ 0 & A \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & B \end{pmatrix}\right) &= \pi\left(\begin{pmatrix} 1 & u + vB \\ 0 & AB \end{pmatrix}\right) = AB \\ &= \pi\left(\begin{pmatrix} 1 & v \\ 0 & A \end{pmatrix}\right)\pi\left(\begin{pmatrix} 1 & u \\ 0 & B \end{pmatrix}\right). \end{aligned}$$

هم‌چنین π پوشاست زیرا اگر $A \in \mathrm{GL}_n(\mathbb{F})$ دلخواه باشد، آن‌گاه

$$\pi\left(\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}\right) = A.$$

بنابراین π یک بروریختی است. هسته این همریختی به صورت زیر است:

$$\begin{aligned}\ker(\pi) &= \{\mathcal{A} \in \mathrm{AGL}_n(\mathbb{F}) \mid \pi(\mathrm{A}) = I\}\\ &= \left\{ A_1 \begin{pmatrix} 1 & v \\ 0 & A \end{pmatrix} \;\middle|\; A = I \right\}\\ &= \left\{ \begin{pmatrix} 1 & v \\ 0 & I \end{pmatrix} \;\middle|\; v \in \mathbb{F}^n \right\}.\end{aligned}$$

پس هسته همان زیرگروه انتقال یعنی $\mathcal{T}$ است. با توجه به قضیه اول یکریختی داریم:

$$\frac{\mathrm{AGL}_n(\mathbb{F})}{\mathcal{T}} \cong \mathrm{GL}_n(\mathbb{F}).$$

نکته ۲ـ۱۰ . در این پایان نامه به بررسی زیرگروه‌های منظمی از $\mathrm{AGL}_n(\mathbb{F})$ خواهیم پرداخت که شامل هیچ انتقالی غیر از عضو همانی نباشند. اگر R چنین زیرگروهی باشد بنابراین داریم $R \cap \mathcal{T} = 1$. بنابراین اگر همریختی π را به R محدود کنیم آنگاه $R \cap \ker \pi = 1$ و لذا با توجه به قضیه اول یکریختی برای چنین زیرگروه‌هایی داریم:

$$R \cong \pi(R).$$

مسئله‌ی وجود زیرگروه‌های منظمی از $\mathrm{AGL}_n(\mathbb{F})$ که دارای هیچ انتقالی غیر از بدیهی نیستند، اولین بار توسط لیبک[7]، پرگر[8] و ساکسل[9] در سال ۲۰۰۰ در مقاله‌ی [۶] مطرح شد. اگر $\mathbb{F}_p$ را میدان p عضوی در نظر بگیریم، آنگاه نویسندگان فوق احکام زیر را در مورد عدم وجود چنین زیرگروه‌های ثابت کردند:

قضیه ۲ـ۱۱. *فرض کنید $\mathbb{F} = \mathbb{F}_p$ میدان p عضوی باشد. در اینصورت $AGL_2(\mathbb{F})$ هیچ زیرگروه منظمی ندارد به طوری که شامل انتقال غیربدیهی نباشد.*

برهان. به بخش ۷ از [۶] مراجعه شود. □

[7] Liebeck [8] Praeger [9] Saxl

قضیه ۲ــ۱۲. *فرض کنید p یک عدد اول فرد باشد و $\mathbb{F} = \mathbb{F}_p$ میدان p عضوی باشد. در اینصورت $AGL_3(\mathbb{F})$ هیچ زیرگروه منظم R ندارد به طوری که $R \cap \mathcal{T} = 1$.*

برهان. به قضیه ۱.۷ از [۶] مراجعه شود. □

قضیه ۲ــ۱۳. *فرض کنید $\mathbb{F} = \mathbb{F}_2$ میدان ۲ عضوی باشد. در اینصورت هیچ زیرگروه منظم R از*

$AGL_4(\mathbb{F})$

وجود ندارد به طوری که $R \cap \mathcal{T} = 1$.

برهان. به لم ۲.۷ از [۶] مراجعه شود. □

در فصل سوم این پایان نامه ما به تعمیم قضایای عدم وجود فوق خواهیم پرداخت.

تعریف ۲ــ۱۴. زیرگروه U از $\mathrm{GL}_n(\mathbb{F})$ را تک‌توان گویند هرگاه هر عضو U دارای مقدار ویژه ۱ باشد و عدد ۱ تنها مقدار ویژه آن باشد، به عبارت دیگر هر عضو U عدد ۱ را به عنوان مقدار ویژه منحصر به فرد داشته باشد. مجموعه تمام ماتریس‌های تک‌توان بالا مثلثی روی میدان $\mathbb{F}$ را با نماد $U_n(\mathbb{F})$ نمایش می‌دهیم.

قضیه ۲ــ۱۵. *فرض کنید که G یک زیرگروه تک‌توان از $\mathrm{GL}_n(\mathbb{F})$ باشد. در این صورت G با زیرگروهی از $U_n(\mathbb{F})$ مزدوج است. به ویژه G پوچ‌توان است.*

برهان. به نتیجه بخش ۱۷.۵ از [۵] مراجعه شود. □

قضیه ۲ــ۱۶. *فرض کنید R یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ باشد. اگر R آبلی باشد آن‌گاه R تک‌توان است.*

برهان. به قضیه ۳.۱ از [۱۱] مراجعه شود. □

قضیه ۲ــ۱۷. *فرض کنید $\mathbb{F}$ یک میدان باشد که $\mathrm{char}\,(\mathbb{F}) = p > 0$. اگر R یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ باشد آن‌گاه R تک‌توان است.*

برهان. به قضیه ۳.۲ از [۱۱] مراجعه شود. $\square$

قضیه ۲ــ۱۸. *فرض کنید که R زیرگروه منظمی از $\mathrm{AGL}_n(\mathbb{F})$ باشد. فرض کنید $R \leq U_{n+1}(\mathbb{F})$ آبلی باشد و $\{e_1, \ldots, e_n\}$ پایه استاندارد $\mathbb{F}$ باشد. در این صورت داریم $R(e_n) = I$.*

برهان. به لم ۵.۲ از [۱۱] مراجعه شود. $\square$

با توجه به قضیه فوق اگر R زیرگروه منظم آبلی از $\mathrm{AGL}_n(\mathbb{F})$ باشد آنگاه $R(e_n) = I$. این به این معنی است که وقتی R به عنوان تابعی از $\mathbb{F}^n$ به $\mathrm{GL}_n(\mathbb{F})$ در نظر گرفته می‌شود این تابع e_n را به عضو همانی می‌برد. بنابراین عضو

$$\begin{pmatrix} 1 & e_n \\ 0 & R(e_n) \end{pmatrix}$$

در هسته همریختی π قرار دارد که همان زیرگروه انتقال است. این موضوع نشان می‌دهد $R \cap \mathcal{T} \neq 1$. بنابراین قضیه زیر را ثابت کرده‌ایم.

قضیه ۲ــ۱۹. *فرض کنید که R یک زیرگروه منظم آبلی از $\mathrm{AGL}_n(\mathbb{F})$ باشد. در این صورت R شامل یک انتقال غیر بدیهی است.*

برهان. با توجه به مطلب قبل از قضیه داریم $R \cap \mathcal{T} \neq 1$. حال هر عضو غیر بدیهی از $R \cap \mathcal{T}$ یک انتقال غیر بدیهی است. $\square$

لم ۲ــ۲۰. *هر زیرگروه منظم تک‌توان R از $\mathrm{AGL}_2(\mathbb{F})$ شامل انتقال غیر بدیهی است.*

برهان. فرض کنید R زیرگروه منظم تک‌توانی از $\mathrm{AGL}_2(\mathbb{F})$ باشد. فرض کنید R شامل هیچ انتقال غیر بدیهی نباشد. در این صورت با توجه به نکته ۲ــ۱۰ داریم $R \cong \pi(R)$. چون R تک‌توان است پس $\pi(R)$ هم تک‌توان است و لذا طبق قضیه ۲ــ۱۵، $\pi(R)$ با زیرگروهی از $U_2(\mathbb{F})$ مزدوج است. چون $U_2(\mathbb{F})$ آبلی است پس $\pi(R)$ و در نتیجه R آبلی خواهد بود و در نتیجه طبق قضیه ۲ــ۱۹ شامل انتقال غیر بدیهی است که متناقض با فرض است. پس R شامل هیچ انتقال غیر بدیهی نیست. $\square$

قضیه ۲ـ۲۱. *فرض کنید R یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ باشد و $z \neq I_n$ عضوی از مرکز R یعنی $Z(R)$ باشد. در این صورت در حد تزویج R تحت $\mathrm{AGL}_n(\mathbb{F})$ می‌توانیم z را با فرم ژوردان آن یعنی $J_z = \mathrm{diag}(J_{n_۱}, J_{n_۲}, \ldots, J_{n_k})$ که دارای بلوک‌های ژوردان به ترتیب از اندازه $n_i \geq n_{i+۱}$ (به ازای هر $i \geq ۱$)، یکی در نظر بگیریم.*

برهان. به قضیه ۴.۴ از [۸] مراجعه شود. □

قضیه ۲ـ۲۲. *فرض کنید که R زیرگروه تک‌توانی از $\mathrm{AGL}_۴(\mathbb{F})$ باشد به طوری که $R \cap \mathcal{T} = \{I_۵\}$ و $\mathrm{char}\,(\mathbb{F}) = ۲$. در این صورت به ازای هر $r \in R$ داریم $r^۴ = I$.*

برهان. اگر $r = I$ آن‌گاه واضح است که $r^۴ = I$. پس فرض کنیم که $r \neq I$. چون R تک‌توان است لذا به ازای هر عضو r از R، تنها مقدار ویژه r برابر با ۱ است و لذا تنها عامل چندجمله‌ای مشخصه آن برابر $(x - ۱)$ است که چون r ماتریسی ۵×۵ است پس چندجمله‌ای مشخصه آن برابر $(x - ۱)^۵$ می‌باشد. فرض کنیم که

$$r = \begin{pmatrix} ۱ & v \\ ۰ & A \end{pmatrix}$$

در این صورت داریم

$$r^۴ = \begin{pmatrix} ۱ & v + vA + vA^۲ + vA^۳ \\ ۰ & A^۴ \end{pmatrix}$$

چون هر ماتریس در چندجمله‌ای مشخصه خود صدق می‌کند بنابراین داریم $(r - I)^۵ = ۰$. پس داریم:

$$\begin{aligned} ۰ = (r - I)^۵ &= \begin{pmatrix} ۰ & v \\ ۰ & A - I \end{pmatrix}^۵ \\ &= \begin{pmatrix} ۰ & v + v(A-I) + v(A-I)^۲ + v(A-I)^۳ + v(A-I)^۴ \\ ۰ & (A-I)^۵ \end{pmatrix} \end{aligned}$$

بنابراین $(A-I)^۵ = ۰$. بنابراین $m_A(x) \mid (x-۱)^۵$ که چون ماتریسی ۴×۴ است و درجه چندجمله‌ای مشخصه A برابر ۴ است پس $m_A(x) \mid (x - ۱)^۴$ و لذا $(A - I)^۴ = ۰$ که چون $\mathrm{char}\,(\mathbb{F}) = ۲$،

نتیجه می‌دهد که

$$0 = (A - I)^4 = A^4 - I$$

پس $A^4 = I$. بنابراین داریم:

$$r^4 = \begin{pmatrix} 1 & v + vA + vA^2 + vA^3 \\ 0 & A^4 \end{pmatrix} = \begin{pmatrix} 1 & v + vA + vA^2 + vA^3 \\ 0 & I \end{pmatrix}$$

اگر $r^4 \neq I$ باشد آن‌گاه $v+vA+vA^2+vA^3 \neq 0$ لذا r^4 عضوی از $\mathcal{T}$ است که عضو R نیز می‌باشد. پس $I \neq r^4 \in R \cap \mathcal{T} = \{I_5\}$ که تناقض است. بنابراین حتما باید داشته باشیم $r^4 = I$. $\square$

۲ـ۳ زیرگروه‌های منظم گروه آفین بدون انتقال غیربدیهی

همانطور که قبلا اشاره شد هدف ما در این پایان نامه بررسی زیرگروه‌های منظمی از گروه‌های آفین است که شامل هیچ انتقال غیربدیهی نباشند. در این بخش، زیرگروه‌های منظمی از گروه آفین $\mathrm{AGL}_n(\mathbb{F}_1)$ خواهیم ساخت که فقط شامل انتقال بدیهی هستند.

قضیه ۲ـ۲۳. *فرض کنیم p یک عدد اول باشد. اگر $p = 2$، آن‌گاه $n = 3$ یا $n \geq 5$ را در نظر می‌گیریم و اگر p یک عدد فرد باشد، آن‌گاه فرض می‌کنیم $n \geq 4$. در این صورت گروه آفین $\mathrm{AGL}_n(\mathbb{F}_p)$ دارای یک زیرگروه منظم است که شامل هیچ انتقالی به جز همانی نیست.*

برهان. فرض کنیم $f(v)$ یک فرم درجه دوم نامولد روی $\mathbb{F}_p^{n-1}$ باشد (برای $p = 2$ و nهای زوج، چنین fای وجود ندارد) و فرض کنیم X ماتریس متناظر با فرم دوخطی متناظر با فرم درجه دوم

$$f(u + w) = f(v) + f(w) + vxw^T, \qquad v, w \in \mathbb{F}_p^{n-1} \tag{۲ـ۳}$$

باشد. به ازای هر v در $\mathbb{F}_p^{n-1}$ قرار می دهیم:

$$g_v = \left(\begin{array}{c|c|c} I & Xv^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline v & f(v) & 1 \end{array}\right)$$

در این صورت g_v یک ماتریس با $n+1$ سطر و $n+1$ ستون در یک شکل بلوکی است. منظور از 0 در بالا بردار صفر $\mathbb{F}_p^{n-1}$ است. طبق رابطه‌ی (۲ـ۳) نتیجه می‌گیریم برای هر بردار $u, v \in \mathbb{F}_p^{n-1}$ داریم

$$g_v g_w = g_w g_v = g_{v+w}$$

زیرا

$$g_v g_u = \left(\begin{array}{c|c|c} I & Xv^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline v & f(v) & 1 \end{array}\right)\left(\begin{array}{c|c|c} I & Xu^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline u & f(u) & 1 \end{array}\right) \quad (۲ـ۴)$$

$$= \left(\begin{array}{c|c|c} I & X(v^T+u^T) & 0^T \\ \hline 0 & 1 & 0 \\ \hline v+u & vxu^T + f(v) + f(u) & 1 \end{array}\right) \quad (۲ـ۵)$$

$$= \left(\begin{array}{c|c|c} I & X(v^T+u^T) & 0^T \\ \hline 0 & 1 & 0 \\ \hline v+u & f(v+u) & 1 \end{array}\right) \quad (۲ـ۶)$$

$$= g_{v+u} = g_{u+v} = g_u g_v \quad (۲ـ۷)$$

بنابراین اگر قرار دهیم

$$H = \{g_v \mid v \in \mathbb{F}_p^{n-1}\}$$

آنگاه H یک گروه آبلی است. همچنین با توجه به رابطه فوق نتیجه می‌شود که

$$(g_v)^p = g_{pv} = g_0$$

که نتیجه می‌دهد H آبلی مقدماتی است (توجه می‌کنیم که g_0 همان عضو خنثی گروه می باشد). همچنین واضح است که مرتبه H برابر با p^{n-1} می‌باشد. اگر X نامنفرد باشد، آنگاه فقط انتقال

بدیهی مشمول در H می‌باشد. فرض کنیم

$$h=\left(\begin{array}{c|c|c} A & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & 1 & 1 \end{array}\right)$$

یک ماتریس دیگر با شکل بلوکی یکسان باشد که ماتریس A یک ماتریس $(n-1)\times(n-1)$ نامنفرد باشد. در این صورت اگر به ازای هر $v\in\mathbb{F}_p^{n-1}$ داشته باشیم $h^{-1}g_vh\in H$، آنگاه h عضوی از نرمالساز H است. اما با محاسبه‌ی درایه‌های ماتریس مزدوج داریم:

$$\begin{aligned} h^{-1}g_vh &= \left(\begin{array}{c|c|c} A^{-1} & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & -1 & 1 \end{array}\right)\left(\begin{array}{c|c|c} I & Xv^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline v & f(v) & 1 \end{array}\right)\left(\begin{array}{c|c|c} A & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & 1 & 1 \end{array}\right) \\ &= \left(\begin{array}{c|c|c} A^{-1} & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & -1 & 1 \end{array}\right)\left(\begin{array}{c|c|c} A & Xv^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline vA & 1+f(v) & 1 \end{array}\right) \\ &= \left(\begin{array}{c|c|c} I & A^{-1}Xv^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline vA & f(v) & 1 \end{array}\right) \end{aligned}$$

مشاهده می‌شود که برای نرمال بودن باید شرایط زیر برقرار باشد:

(الف) $XA^T=A^{-1}X$.

(ب) برای هر v داشته باشیم $f(v)=f(vA)$.

طبق رابطه‌ی (۲ـ۳)، شرط (ب)، (الف) را نتیجه می‌دهد. زیرا اگر (ب) برقرار باشد آنگاه:

$$\begin{aligned} f(v)+f(w)+vXw^T &= f(v+w) \\ &= f((v+w)A)=f(vA+wA) \\ &= f(vA)+f(wA)+(vA)X(A^Tw^T) \end{aligned}$$

بنابراین داریم:

$$vAXA^Tw^T = vXw^T \longrightarrow v(AXA^T - X)w^T = 0$$

که چون v و w دلخواه هستند نتیجه میدهد که

$$AXA^T = X \longrightarrow XA^T = A^{-1}X$$

همچنین داریم:

$$h^k = \left(\begin{array}{c|c|c} A^k & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & k & 1 \end{array}\right)$$

بنابراین اگر A از مرتبه p باشد، آنگاه h نیز از مرتبه p است زیرا

$$h^p = \left(\begin{array}{c|c|c} A^k & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & p & 1 \end{array}\right) = \left(\begin{array}{c|c|c} I & 0^T & 0^T \\ \hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

بنابراین چون H از مرتبه p^{n-1} است و h عضوی از نرمالساز H است که دارای مرتبه p است بنابراین گروه $G = < h, H >$ از مرتبه p^n است. به علاوه

$$g_vh^k = \left(\begin{array}{c|c|c} A^k & \star & 0^T \\ \hline 0 & 1 & 0 \\ \hline vA^k & \star & 1 \end{array}\right)$$

حال با توجه به معکوس‌پذیر بودن A سطر آخر فقط در حالتی می‌تواند بدیهی باشد که $v = 0$. در این حالت سطر آخر برابر $(0|k|1)$ است. بنابراین لازم است که $k = 0$، و در نتیجه خواهیم داشت $g_vh^k = g_0h^0 = I$. به عبارت دیگر اعضای غیربدیهی g_0 را ثابت نگه نمی‌دارند.

توجه کنید که چون h عضوی از نرمالساز H است بنابراین هر عضو G را میتوان به صورت g_vh^k نمایش داد. اگر g_vh^k یک انتقال باشد، آنگاه داریم $A^k = I$ و بنابراین $k = mp = 0$ ، بنابراین g_v باید یک انتقال باشد. ولی اگر $v \neq 0$ باشد، آنگاه $g(v)$ یک انتقال نیست. پس G شامل هیچ انتقال غیربدیهی نیست.

بنابراین G منظم و بدون انتقال غیربدیهی است، و این همان چیزی است که میخواستیم ثابت کنیم.

حال اگر $n-1 > 2$ و $p > 2$ آنگاه یک فرم درجه دوم نامولد موجود است که ماتریس متناظر با آن ماتریس نامنفرد X است و هم‌چنین ماتریس A با خواص (ب) و از مرتبه p وجود دارد. بنابراین روش ساخت قابل انجام است. اگر $n-1 \geq 2$ زوج باشد و $p = 2$ بازهم روش ساخت قابل انجام است.

اگر $p = 2$ و $n = 2l \geq 6$، آنگاه n مجموع دو عدد فرد می‌باشد. (هر کدام از این اعداد بزرگتر از ۱ هستند) و حاصل‌ضرب مستقیم متناظر با دو گروه آفین یکی از درجه n را نتیجه می دهد.

محاسبات انجام شده در [۶] نشان می‌دهد برای $p = 2$ و $n = 4$ و برای $p > 2$ و $n = 3$ این زیرگروه‌های منظم وجود ندارند. بدیهی است که این حکم برای $n \leq 2$ و عدد p دلخواه برقرار است. □

فصل سوم

نتایج عدم وجود و مثال‌هایی از زیرگروه‌های منظم

۳ـ۱ تعمیم قضایای عدم وجود زیرگروه‌های منظم بدون انتقال غیربدیهی

همانطور که در فصل دوم اشاره شد ما در این فصل به تعمیم نتایج وجود زیرگروه‌های منظمی که شامل هیچ انتقال غیربدیهی نباشند خواهیم پرداخت. در [۶] نویسندگان نشان دادند که هیچ زیرگروه منظمی که شامل انتقال غیربدهی نباشد برای گروه‌های $\mathrm{AGL}_2(\mathbb{F}_p)$ به ازای هر عدد اول p، $\mathrm{AGL}_3(\mathbb{F}_p)$ به ازای عدد اول $p > 2$ و برای $\mathrm{AGL}_4(\mathbb{F}_2)$ وجود ندارد که احکام فوق در فصل دوم بیان شد. اولین تعمیم که با شرط تک توان بودن زیرگروه منظم اثبات شده است در مورد وجود چنین زیرگروه‌های برای $\mathrm{AGL}_3(\mathbb{F}_2)$ است.

قضیه ۳ـ۱. *گروه آفین $\mathrm{AGL}_3(\mathbb{F})$ شامل یک زیرگروه منظم تک‌توان مانند R است به طوری که $R \cap \mathcal{T} = \{I_4\}$ اگر و تنها اگر $|\mathbb{F}| = 2$.*

برهان. ابتدا فرض کنید که R یک زیرگروه منظم تک‌توان از $\mathrm{AGL}_3(\mathbb{F})$ باشد به طوری که $R \cap \mathcal{T} =$

$\{I_۴\}$. نشان می‌دهیم که $|\mathbb{F}| = ۲$. در ابتدا توجه می‌کنیم که R نمی‌تواند آبلی باشد زیرا اگر R آبلی باشد، آنگاه با توجه به قضیه ۲ــ۱۵، R شامل یک انتقال غیر بدیهی خواهد بود که متناقض با فرض است. پس R غیر آبلی است. همچنین چون R شامل انتقال غیر بدیهی نیست پس با توجه به نکته ۲ــ۱۰ داریم $R \cong \pi(R)$. با توجه به قضیه ۲ــ۲۱، می‌توانیم فرض کنیم که $\mathbf{Z}(R)$ شامل یک عضو $\tilde{z}$ است که به یکی از فرم‌های ژوردان $J_۴$، $\mathrm{diag}(J_۳, J_۱)$، $\mathrm{diag}(J_۲, J_۲)$ و یا $\mathrm{diag}(J_۲, J_۱, J_۱)$ است. توجه می‌کنیم که چون $\tilde{z}$ ماتریسی ۴×۴ است و اندازه بلوک‌های ژوردان را طبق قضیه ۲ــ۲۱ به صورت نزولی در نظر گرفتیم فقط حالت‌های فوق امکان پذیر است. اگر $\tilde{z} = J_۴$ آنگاه با توجه به لم ۵.۲ از [۵]، چون $\mathbf{C}_{\mathrm{AGL}_۴(\mathbb{F})}(J_۴)$ آبلی است و $R \subseteq \mathbf{C}_{\mathrm{AGL}_۴(\mathbb{F})}(\tilde{z})$ پس R هم خواهد بود که متناقض با فرض است. پس $\tilde{z} \neq J_۴$. به همین صورت اگر $\tilde{z} = \mathrm{diag}(J_۳, J_۱)$ آنگاه باز هم با توجه به مطالب بخش ۵ از [۵]، هر زیرگروه تک‌توان از $\pi(\mathbf{C}_{\mathrm{AGL}_۴(\mathbb{F})}(\mathrm{diag}(J_۳, J_۱)))$ آبلی است و چون در این حالت $R \leq \mathbf{C}_{\mathrm{AGL}_۴(\mathbb{F})}(\tilde{z})$ پس $\pi(R) \leq \pi(\mathbf{C}_{\mathrm{AGL}_۴(\mathbb{F})}(\mathrm{diag}(J_۳, J_۱)))$ که چون R تک‌توان است پس $\pi(R)$ هم زیرگروه تک‌توانی از $\pi(\mathbf{C}_{\mathrm{AGL}_۴(\mathbb{F})}(\mathrm{diag}(J_۳, J_۱)))$ است. بنابراین با توجه به این‌که $R \cong \pi(R)$ پس R هم آبلی است که باز هم متناقض با فرض است. پس $\tilde{z} \neq \mathrm{diag}(J_۳, J_۱)$. اگر $\tilde{z} = \mathrm{diag}(J_۲, J_۱, J_۱)$ آنگاه

$$\tilde{z} = \left[\begin{array}{cc|c|c} ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ \\ \hline ۰ & ۰ & ۱ & ۰ \\ \hline ۰ & ۰ & ۰ & ۱ \end{array}\right].$$

بنابراین $\tilde{z}$ یک انتقال غیر بدیهی از R است که باز هم متناقض با این است که $R \cap \mathcal{T} = \{I_۴\}$. پس $\tilde{z} \neq \mathrm{diag}(J_۲, J_۱, J_۱)$. بنابراین تنها حالتی که برای $\tilde{z}$ امکان پذیر است این است که

$$\tilde{z} = \mathrm{diag}(J_۲, J_۲).$$

بنابراین

$$\tilde{z} = \left[\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right].$$

برای راحتی کار $\tilde{z}$ را با مزدوجی از آن توسط یک ماتریس جایگشتی تعویض می‌کنیم. فرض کنیم که α روی جایگشت روی مجموعه $\{1,2,3,4\}$ به صورت $\alpha = (2\ 3)$ باشد و $\mathcal{P}$ ماتریس جایگشتی متناظر با α باشد . با توجه به مطالب فصل اول داریم

$$\mathcal{P} = \begin{bmatrix} e_{\alpha(1)} \\ e_{\alpha(2)} \\ e_{\alpha(3)} \\ e_{\alpha(4)} \end{bmatrix} = \begin{bmatrix} e_1 \\ e_3 \\ e_2 \\ e_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

بنابراین

$$\mathcal{P}^{-1}\tilde{z}\mathcal{P} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

حال به جای $\tilde{z}$ از $z = \mathcal{P}^{-1}z\mathcal{P}$ استفاده می‌کنیم. پس می‌توانیم فرض کنیم

$$z = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in \mathbf{Z}(R).$$

حال فرض کنید

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix} \in \mathbf{C}_{\mathrm{AGL}_3(\mathbb{F})}(z).$$

در این از رابطه $cz = zc$ خواهیم داشت:

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ 0 & 0 & a_1 & a_2 \\ 0 & 0 & b_1 & b_2 \end{bmatrix}$$

که با توجه به این‌که $c \in \mathrm{AGL}_3(\mathbb{F})$ باید داشته باشیم $b_1 = 0$ که از آن نتیجه می‌شود c باید به صورت بالا مثلثی باشد.

$$b_1 = 0 \implies c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & b_2 & b_3 & b_4 \\ 0 & 0 & a_1 & a_2 \\ 0 & 0 & 0 & b_2 \end{bmatrix}. \tag{۳ـ۱}$$

از طرفی چون $z \in \mathbf{Z}(R)$ پس $R \leq \mathbf{C}_{\mathrm{AGL}_3(\mathbb{F})}(z)$. چون R تک‌توان است پس اعضای R با توجه به این‌که $R \leq \mathbf{C}_{\mathrm{AGL}_3(\mathbb{F})}(z)$ و تک‌توان بودن R و رابطه (۳ـ۱) شامل ماتریس‌های به شکل زیر خواهد بود.

$$r_{(x_1,x_2,x_3)} = \begin{bmatrix} 1 & x_1 & x_2 & x_3 \\ 0 & 1 & a(X) & b(X) \\ 0 & 0 & 1 & x_1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad , \quad X = (x_1, x_2, x_3).$$

رابطه فوق با توجه به این‌که R منظم است لذا به ازای هر $X \in \mathbb{F}^3$ عضو منحصر به فردی از R موجود است که $(1, X)$ سطر اول آن است که درایه‌های این عضو منحصر به فرد در سطر دوم را به خاطر وابستگی به X با $a(X)$ و $b(X)$ نمایش داده‌ایم. حال به ازای هر $x \in \mathbb{F}$ قرار می‌دهیم

$t_x = r_{(}۰,۰,x)$، $\tilde{a}(x) = a(۰,۰,x)$ و $\tilde{b}(x) = b(۰,۰,x)$. در این صورت داریم

$$t_x t_y = \begin{bmatrix} ۱ & ۰ & ۰ & x \\ ۰ & ۱ & a(X) & b(X) \\ ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ \end{bmatrix} \begin{bmatrix} ۱ & ۰ & ۰ & y \\ ۰ & ۱ & a(Y) & b(Y) \\ ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ \end{bmatrix}$$

$$= \begin{bmatrix} ۱ & ۰ & ۰ & x+y \\ ۰ & ۱ & a(X)+a(Y) & b(X)+b(Y) \\ ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ \end{bmatrix}.$$

حال می‌دانیم که به ازای هر $x \in \mathbb{F}^۳$ عضو منحصر به فردی از R موجود است که $(۱,x)$ سطر اول آن است و $t_x t_y$ عضوی از R است که $(۱,۰,۰,x+y)$ سطر اول آن است و

$$t_{x+y} = \begin{bmatrix} ۱ & ۰ & ۰ & x+y \\ ۰ & ۱ & a(X+Y) & b(X+Y) \\ ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ \end{bmatrix}$$

نیز عضو دیگری از R است که $(۱,۰,۰,x+y)$ سطر اول آن است پس منحصر به فردی نتیجه می‌دهد که

$$t_x t_y = t_{x+y}.$$

بنابراین داریم:

$$\tilde{b}(x+y) = \tilde{b}(x) + \tilde{b}(y), \quad \forall x,y \in \mathbb{F}.$$

حال فرض کنید به ازای هر $x \in \mathbb{F}$ داشته باشیم $\tilde{a} = ۰$. در این صورت جابه‌جاگر $[r_{(۱,۰,۰)}, t_x]$ برابر

است با (فرض کنیم $X=(1,0,0)$ و $Y=(0,0,x)$):

$$
\begin{aligned}
[r_{(1,0,0)},t_x] &= r_{(1,0,0)}^{-1}t_x^{-1}r_{(1,0,0)}t_x \\
&= \begin{bmatrix} 1 & -1 & a(X) & -a(X)+b(X) \\ 0 & 1 & -a(X) & a(X)-b(X) \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & -x \\ 0 & 1 & -a(Y) & -b(Y) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\
&\times \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & a(X) & b(X) \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & x \\ 0 & 1 & a(Y) & b(Y) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & -1 & a(Y)+a(X) & -x+b(Y)-a(X)+b(X) \\ 0 & 1 & -a(Y)-a(X) & -b(Y)+a(X)-b(X) \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\
&\times \begin{bmatrix} 1 & 1 & a(Y) & x+b(Y) \\ 0 & 1 & a(X)+a(Y) & b(X)+b(Y) \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & a(Y) & a(Y)+b(Y) \\ 0 & 1 & 0 & -a(Y) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.
\end{aligned}
$$

از طرفی طبق فرض داریم

$$a(Y)=a(0,0,x)=\tilde{a}(x)=0\ ,\ b(Y)=b(0,0,x)=\tilde{b}(x).$$

پس حاصل به صورت زیر است:

$$[r_{(1,0,0)}, t_x] = \begin{bmatrix} 1 & 0 & 0 & \tilde{b}(x) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4 + \tilde{b}(x)E_{1,4}.$$

از طرفی چون $r_{(1,0,0)}$ و t_x هر دو اعضای R هستند و R زیرگروه است پس $[r_{(1,0,0)}, t_x]$ هم عضوی از R است یعنی

$$I_4 + \tilde{b}(x)E_{1,4} \in R.$$

هم‌چنین با توجه به تعریف $\mathcal{T}$ واضح است که $I_4 + \tilde{b}E_{1,4} \in \mathcal{T}$. پس

$$I_4 + \tilde{b}E_{1,4} \in R \cap \mathcal{T} = \{I_4\}.$$

بنابراین $\tilde{b} = 0$. در نتیجه با توجه به تعربف t_x و مجموعه انتقال $\mathcal{T}$ داریم $t_x \in \mathcal{T}$ و باز هم با توجه به این‌که $R \cap \mathcal{T} = \{I_4\}$ خواهیم داشت $t_x = \{I_4\}$ که نتیجه می‌دهد $x = 0$. پس اگر $\tilde{a}(x) = 0$ آن‌گاه $x = 0$. بنابراین اگر $x \neq 0$ آن‌گاه $\tilde{a}(x) \neq 0$. لذا برای هر عضو $x \neq 0$ با توجه به این‌که $\tilde{a}(x) \neq 0$ می‌توانیم عضو $r_{(\tilde{a}(x)^{-1},0,0)}$ را در نظر بگیریم. با محاسبه‌ای همانند قسمت قبل می‌توان نشان داد که:

$$[r_{(\tilde{a}(x)^{-1},0,0)}, t_x] = I_4 + 2E_{1,3} + \frac{\tilde{b}(x)+1}{\tilde{a}(x)} + E_{1,4}. \qquad (۳-۲)$$

حال اگر $\operatorname{char}(\mathbb{F}) \neq 2$، عضو فوق یک انتقال غیر بدیهی است که عضو R هم می‌باشد که متناقض با فرض است. پس حتما باید داشته باشیم $\operatorname{char}(\mathbb{F}) = 2$. در این حالت نیز اگر $\frac{\tilde{b}(x)+1}{\tilde{a}(x)} \neq 0$ آن‌گاه یک انتقال غیر بدیهی در R داریم که باز هم تناقض است. پس باید داشته باشیم $\tilde{b}(x) + 1 = 0$ که چون $\operatorname{char}(\mathbb{F}) = 2$ پس داریم $\tilde{b}(x) = -1 = 1$. حال نشان می‌دهیم $|\mathbb{F}| = 2$. فرض کنید $|\mathbb{F}| > 2$ و فرض کنید $w \in \mathbb{F}$ به طوری که $w \neq 0, 1$. با توجه به خاصیت جمعی $\tilde{b}$ و این‌که $\tilde{b}(x) = 1$ (به ازای هر $x \neq 0$) داریم:

$$1 = \tilde{b}(1 + w) = \tilde{b}(1) + \tilde{b}(w) = 1 + 1 = 0$$

که تناقض است. بنابراین $|\mathbb{F}| = 2$ و حکم ثابت شد.

برعکس، فرض کنید که $|\mathbb{F}| = 2$ یعنی $\mathbb{F} = \mathbb{F}_2$. در این صورت زیرگروه

$$R = \langle (I_4 + E_{1,2} + E_{2,3} + E_{3,4}), (I_4 + E_{1,4} + E_{2,3} + E_{2,4}) \rangle$$

یک زیرگروه منظم از $\mathrm{AGL}_3(2)$ است به طوری که $R \cap \mathcal{T} = \{I_4\}$. □

قضیه ۲ــ۱۳ در [۶] برای میدان دو عضوی ثابت شده است. ما در اینجا تعمیمی از این قضیه را برای حالتی که مشخصه میدان برابر ۲ باشد را ارائه می کنیم.

قضیه ۳ــ۲. *فرض کنید $\mathbb{F}$ یک میدان از مشخصه ۲ باشد. در این صورت هر زیر گروه منظم R از $\mathrm{AGL}_4(\mathbb{F})$ شامل انتقال غیر بدیهی است.*

برهان. فرض کنید که R یک زیرگروه منظم از $\mathrm{AGL}_4(\mathbb{F})$ باشد. چون $\mathrm{char}\,\mathbb{F} = 2 > 0$، پس طبق قضیه ۲ــ۱۷، R تک‌توان است. با استفاده از قضیه ۲ــ۲۱، در حد تزویج تحت $\mathrm{AGL}_4(\mathbb{F})$ می‌توانیم فرض کنیم که $\mathbf{Z}(R)$ شامل یک عضو $\tilde{z}$ است که به یکی از شکل‌های زیر است:

J_5، $\mathrm{diag}(J_4, J_1)$، $\mathrm{diag}(J_3, J_2)$، $\mathrm{diag}(J_3, J_1, J_1)$، $\mathrm{diag}(J_2, J_2, J_1)$ یا $\mathrm{diag}(J_2, J_1, J_1, J_1)$.

توجه می‌کنیم که چون $\tilde{z}$ ماتریسی 5×5 است و اندازه بلوک‌های ژوردان نزولی است فقط همین حالت‌ها را داریم. می‌خواهیم نشان دهیم R شامل انتقال غیر بدیهی است. فرض کنید چنین نباشد و $R \cap \mathcal{T} = \{I_5\}$. اولاً توجه می‌کنیم که R غیر آبلی است زیرا اگر R آبلی باشد آنگاه طبق قضیه ۲ــ۱۹، شامل انتقال غیر ببدیهی است که تناقض است. همچنین توجه کنید که چون R شامل انتقال غیر بدیهی نیست با توجه به نکته ۲ــ۱۰ داریم $R \cong \pi(R)$. با توجه به قضیه ۲ــ۲۲ برای هر $r \in R$ داریم $r^4 = I_5$. اگر $\tilde{z} = J_5$ آنگاه خواهیم داشت

$$\tilde{z}^4 = \begin{bmatrix} 1 & 4 & 6 & 4 & 1 \\ 0 & 1 & 4 & 6 & 4 \\ 0 & 0 & 1 & 4 & 6 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \neq I_5$$

که متناقض با این است که $\tilde{z} \in R$. پس $\tilde{z} \neq J_5$. اگر $\tilde{z} = \mathrm{diag}(J_3, J_2)$ آنگاه داریم

$$\tilde{z}^2 = \left(\mathrm{diag}(J_3, J_2)\right)^2 = \begin{bmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xlongequal{\mathrm{char}\,(\mathbb{F})=2} \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + E_{1,4}.$$

بنابراین $\tilde{z}^2$ یک انتقال غیر بدیهی است که چون $\tilde{z}^2 \in R$ متناقض با فرض است. پس $\tilde{z} \neq \mathrm{diag}(J_3, J_2)$. اگر $\tilde{z} = \mathrm{diag}(J_3, J_1, J_1)$ آنگاه مانند حالت قبل داریم $\tilde{z} = I_5 + E_{1,3}$ که باز هم مانند حالت قبل یک تناقض است. پس $\tilde{z} \neq \mathrm{diag}(J_3, J_1, J_1)$. اگر $\tilde{z} = \mathrm{diag}(J_2, J_1, J_1, J_1)$ آنگاه خود $\tilde{z}$ یک انتقال غیر بدیهی است که باز هم متناقض با این است که $R \cap \mathcal{T} = \{I_5\}$. پس $\tilde{z} \neq \mathrm{diag}(J_2, J_1, J_1, J_1)$. اگر $\tilde{z} = \mathrm{diag}(J_4, J_1)$ آنگاه با توجه به مطلب بخش ۵ از [۵] هر زیرگروه تک‌توان از $\pi(\mathbf{C}_{\mathrm{AGL}_4(\mathbb{F})}(\tilde{z}))$ آبلی است. حال چون $R \leq \mathbf{C}_{\mathrm{AGL}_4(\mathbb{F})}(\tilde{z})$ پس $\pi(R) \leq \pi(\mathbf{C}_{\mathrm{AGL}_4(\mathbb{F})}(\tilde{z}))$ که چون R تک‌توان است پس $\pi(R)$ زیرگروه تکتوانی از $\pi(\mathbf{C}_{\mathrm{AGL}_4(\mathbb{F})}(\tilde{z}))$ است و در نتیجه آبلی است. چون $R \cong \pi(R)$ پس R هم آبلی خواهد بود که تناقض است (چون گفتیم R غیر آبلی است). بنابراین تنها حالتی که برای $\tilde{z}$ امکان‌پذیر است این است که $\tilde{z} = \mathrm{diag}(J_2, J_2, J_1)$.

همانند قضیه ؟؟، برای راحتی کار $\tilde{z}$ را با مزدوجی از آن تحت یک ماتریس جایگشتی جایگزین می‌کنیم. فرض کنید که α جایگشت (۲ ۴ ۵ ۳) روی مجموعه $\{1, 2, 3, 4, 5\}$ باشد و $\mathcal{P}$ ماتریس

جایگشتی متناظر با α باشد. پس

$$\mathcal{P} = \begin{bmatrix} e_{\alpha(1)} \\ e_{\alpha(2)} \\ e_{\alpha(3)} \\ e_{\alpha(4)} \\ e_{\alpha(5)} \end{bmatrix} = \begin{bmatrix} e_1 \\ e_4 \\ e_2 \\ e_5 \\ e_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

در این صورت داریم:

$$\mathcal{P}^{-1}\tilde{z}\mathcal{P} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + E_{1,4} + E_{2,5}.$$

قرار می‌دهیم $z = \mathcal{P}^{-1}\tilde{z}\mathcal{P} = I_5 + E_{1,4} + E_{2,5} \in \mathbf{Z}(R)$. هم‌چنین با توجه به تک‌توان بودن R طبق ...... می‌توان نوشت:

$$R \leq \left\{ \begin{bmatrix} 1 & \rho_1 & \rho_2 & \rho_3 & \rho_4 \\ 0 & 1 & 0 & \rho_2 & 0 \\ 0 & \rho_5 & 1 & \rho_6 & \rho_7 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & \rho_8 & 0 & \rho_9 & 1 \end{bmatrix} \ : \ \rho_i \in \mathbb{F} \right\}$$

و با مزدوج سازی تحت ماتریس جایگشتی $\mathcal{P}$ هر عضو r از R را می‌توان به صورت زیر نوشت:

$$r = \begin{bmatrix} 1 & x_1 & x_2 & x_3 & x_4 \\ 0 & 1 & \alpha_1(X) & \alpha_2(X) & \alpha_3(X) \\ 0 & 0 & 1 & \alpha_4(X) & \alpha_5(X) \\ 0 & 0 & 0 & 1 & x_1 \\ 0 & \rho_8 & 0 & \rho_9 & 1 \end{bmatrix}, \qquad X = (x_1, x_2, x_3, x_4). \qquad (۳-۳)$$

بنابراین هر عضو R تحت تزویج بالا مثلثی خواهد بود و لذا می‌توانیم فرض کنیم که $R \cong \pi(R) \leq U_4(\mathbb{F})$.

بنابراین با توجه به اینکه $U_4(F)$ پوچ‌توان از کلاس ۴ است بنابراین با توجه به قضیه ۱ــ۱۹ داریم $\Gamma_4(U_4)=1$ و لذا $\Gamma_3(U_4)\leq Z(G)$. بنابراین به ازای هر r_1، r_2 و r_3 از R داریم $[[r_1,r_2],r_3]\in\mathbf{Z}(R)$. در ادامه اثبات عضوی از R را که سطر اول آن $(1,1,0,0,0)$ است را s می‌نامیم. فرض کنید که $g=I_5+\alpha_5(1,0,0,0)E_{3,4}$ در این صورت داریم

$$\begin{aligned} gz &= (I_5+\alpha_5(1,0,0,0)E_{3,4})\,(I_5+E_{1,4}+E_{2,5}) \\ &= I_5+E_{1,4}+E_{2,5}+\alpha_5(1,0,0,0)E_{3,4}=zg. \end{aligned}$$

پس g و z با هم جابجا می‌شوند. هم‌چنین داریم (با فرض $\alpha_i=\alpha_i(1,0,0,0)$):

$$g^{-1}sg=g^{-1}\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2 & \alpha_3 \\ 0 & 0 & 1 & \alpha_4 & \alpha_5 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} g=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2+\alpha_1\alpha_5 & \alpha_3 \\ 0 & 0 & 1 & \alpha_4 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

بنابراین $z=g^{-1}zg\in\mathbf{Z}(R^g)$ و gsg^{-1} هم عضوی از R^g است که $(1,1,0,0,0)$ سطر اول آن است و مولفه $(3,5)$ام آن برابر با صفر است. لذا به جای R می‌توانیم از R^g که یکریخت با R است استفاده کنیم. برای راحتی کار بدون تغییر نماد فرض کنیم

$$z=\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}\in\mathbf{Z}(R),\qquad s=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & \beta_1 & \beta_2 & \beta_3 \\ 0 & 0 & 1 & \beta_4 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}\in R. \tag{۳ــ۴}$$

ادعا می‌کنیم که عضوی از R موجود است به طوری که در آن $\alpha_1(x)\neq 0$. فرض کنیم چنین نباشد و به ازای هر $x\in\mathbb{F}^4$ داشته باشیم $\alpha_1(x)=0$. (به ویژه در عضو s هم داریم $\beta_1=0$). فرض کنیم که R_0 پایدارساز زیرفضای V_0 در R باشد که V_0 زیرفضای پدید آمده توسط بردارهای e_1، e_2، e_4 و

e_5 است یعنی

$$V_0 = \langle e_1, e_2, e_4, e_5\rangle = \{(a_0, a_1, 0, a_2, a_3) \mid a_i \in \mathbb{F}\}.$$

در این صورت با اثر دادن اعضای R روی اعضای V_0 مشخص است که اعضای R_0 متشکل از ماتریس‌هایی هستند که در آن‌ها $x_2 = 0$. حال طبق قضیه .... ، R_0 یک زیرگروه منظم $\tilde{R}$ از $\mathrm{AGL}_3(\mathbb{F})$ القا می‌کند. حال چون $R_0 \cap \mathcal{T} \subset R \cap \mathcal{T} = \{I_5\}$، پس $R_0 \cap \mathcal{T} = \{I_5\}$ و در نتیجه $\tilde{R}$ شامل هیچ انتقالی غیر از همانی نیست. بنابراین با توجه به قضیه ؟؟ باید داشته باشیم $\mathbb{F} = \mathbb{F}_2$. حال دو عضو زیر از R را در نظر می‌گیریم:

$$v = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & v_2 & v_3 \\ 0 & 0 & 1 & v_4 & v_5 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad t = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & \xi_2 & \xi_3 \\ 0 & 0 & 1 & \xi_4 & \xi_5 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

در این صورت داریم

$$v^2 = \begin{bmatrix} 1 & 0 & 0 & v_4 & v_5 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + v_4 E_{1,4} + v_5 E_{1,5}.$$

چون $v^2 \in R$ و R شامل انتقال غیر بدیهی نیست پس باید داشته باشیم $v_4 = v_5 = 0$. هم‌چنین خواهیم داشت:

$$[v,t] = v^{-1}t^{-1}vt = \begin{bmatrix} 1 & 0 & 0 & \xi_4 & \xi_5 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + \xi_4 E_{1,4} + \xi_5 E_{1,5}.$$

که باز هم چون $[v,t]\in R$ و R شامل انتقال غیر بدیهی نیست بنابراین $\xi_4=\xi_5=0$. اگر $\xi_2=0$ آن‌گاه داریم

$$[s,t]=s^{-1}t^{-1}st=\begin{bmatrix}1&0&0&0&\xi_3\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}=I_5+\xi_3E_{1,5}.$$

باز هم چون $[s,t]\in R$ و R شامل انتقال غیر بدیهی نیست نتیجه می‌شود که $\xi_3=0$. پس خواهیم داشت $\xi_2=\xi_3=\xi_4=\xi_5=0$ که به این معنی است که t یک انتقال غیر بدیهی است که عضو R نیز می‌باشد که تناقض است. بنابراین $\xi_2\neq 0$ و لذا $\xi_2=1$. اما در این صورت داریم

$$z[s,t]=z(s^{-1}t^{-1}st)=\begin{bmatrix}1&0&0&0&(1+\xi_3)\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}=I_5+(1+\xi_3)E_{1,5}.$$

اگر $\xi_3=0$ آن‌گاه عضو فوق یعنی $z[s,t]$ یک انتقال غیر بدیهی است که عضو R هم می‌باشد که تناقض است. پس $\xi_3=1$. با محاسبات مشابه با توجه به این‌که هیچ کدام از اعضای v، vz، vt و vtz نمی‌توانند انتقال‌های غیر بدیهی باشند (چون در این صورت R شامل انتقال غیر بدیهی است که تناقض است) بنابراین نتیجه می‌شود که

$$(v_3,v_4)\neq(0,0),(0,1),(1,1),(1,0)$$

که باز هم تناقض است (زیرا $v_3,v_4\in\mathbb{F}_2$). بنابراین با فرض این‌که $X\in\mathbb{F}^4$ داشته باشیم $\alpha_1(X)=0$ باطل است و در نتیجه عضوی از R خواهیم داشت که $\alpha_1(X)\neq 0$. فرض کنیم این عضو به

صورت

$$u = \begin{bmatrix} 1 & y_1 & y_2 & y_3 & y_4 \\ 0 & 1 & \gamma_1 & \gamma_2 & \gamma_3 \\ 0 & 0 & 1 & \gamma_4 & \gamma_5 \\ 0 & 0 & 0 & 1 & y_1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \in R$$

باشد که $\gamma_1 \neq 0$. فرض کنید که s همان عضو رابطه (۳ـ۴) باشد. چون $[[s,u],s] \in \mathbf{Z}(R)$ بنابراین داریم:

$$s[[s,u],s] = [[s,u],s]s$$

که از روی آن خواهیم داشت

$$\beta_k = \frac{\beta_1\gamma_k}{\gamma_1}.$$

فرض کنید که $\gamma_4 \neq 0$. در این صورت داریم:

$$s^4 = \begin{bmatrix} 1 & 0 & 0 & 0 & \beta_1\beta_4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + \beta_1\beta_4 E_{1,5} = I_5 + \frac{\beta_1^2\gamma_4}{\gamma_1}E_{1,5}.$$

چون باید داشته باشیم $s^4 = I_5$ پس

$$\frac{\beta_1^2\gamma_4}{\gamma_1} = 0 \xRightarrow{\gamma_4 \neq 0} \beta_1 = 0.$$

از طرفی داریم

$$[s,u]^2 = [s,u][s,u] = \begin{bmatrix} 1 & 0 & 0 & 0 & \gamma_1\gamma_4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + \gamma_1\gamma_4 E_{1,5}$$

که چون γ_1 و γ_4 هر دو مخالف صفرند پس یک انتقال غیر بدیهی در R داریم که تناقض است. پس $\gamma_4 = 0$ و لذا $\beta_4 = 0$. حال خواهیم داشت (چون $\beta_4 = \gamma_4 = 0$):

$$[[s,u],u] = \begin{bmatrix} 1 & 0 & 0 & 0 & \gamma_1\gamma_5 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + \gamma_1\gamma_5 E_{1,5}.$$

باز هم با توجه به این‌که R شامل انتقال غیر بدیهی نیست باید داشته باشیم $\gamma_1\gamma_5 = 0$ که چون $\gamma_1 \neq 0$ پس $\gamma_5 = 0$. حال فرض کنید $r \in R$ به شکل (۳ـ۳) باشد، چون $[[s,r],u] \in \mathbf{Z}(R)$ پس

$$s[[s,r],u] = [[s,r],u]s$$

که از آن نتیجه می‌شود $\alpha_4(X) = 0$ به ازای هر $X \in \mathbb{F}^4$. بنابراین

$$[[u,r],s] = \begin{bmatrix} 1 & 0 & 0 & 0 & \gamma_1\alpha_5(X) \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5 + \gamma_1\alpha_5(X)E_{1,5}.$$

دوباره با توجه به این‌که R شامل انتقال غیر بدیهی نیست و $\gamma_1 \neq 0$ پس به ازای هر $X \in \mathbb{F}^4$ باید داشته باشیم $\alpha_5(X) = 0$. بنابراین تا این مرحله به این نتیجه رسیدیم که هر عضو $r \in R$ به شکل زیر است:

$$r = \begin{bmatrix} 1 & x_1 & x_2 & x_3 & x_4 \\ 0 & 1 & \alpha_1(X) & \alpha_2(X) & \alpha_3(X) \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & x_1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad X = X(x_1,x_2,x_3,x_4). \qquad (۵ـ۳)$$

حال قرار می‌دهیم $m_x = r_{(x,0,0,0)}$ و $t_{(x_2,x_4)} = r_{(0,x_2,0,x_4)}$. هم‌چنین قرار می‌دهیم $\tilde{\alpha}_i(x_2,x_4) = \tilde{\alpha}_i(0,x_2,0,x_4)$ به ازای هر $i = 1,2,3$. در این صورت داریم:

$$t_{(x_2,x_4)}t_{(y_3,y_4)} = \begin{bmatrix} 1 & 0 & x_2+y_2 & 0 & x_4+y_4 \\ 0 & 1 & \alpha_1(X)+\alpha_1(Y) & \alpha_2(X)+\alpha_2(Y) & \alpha_3(X)+\alpha_3(Y) \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

از طرفی $t_{(x_2+y_2,x_4+y_4)}$ نیز سطر اول یکسان با ماتریس فوق دارد که با توجه به منظم بودن R باید داشته باشیم

$$t_{(x_2,x_4)}t_{(y_2,y_4)} = t_{(x_2+x_4,y_2+y_4)}.$$

بنابراین با مقایسه سطر دوم این دو ماتریس نتیجه می‌شود که (به ازای هر $i = 1,2,3$):

$$\alpha_i(0,x_2+y_2,0,x_4+y_4) = \alpha_i(0,x_2,0,x_4) + \alpha_i(0,y_2,0,y_4).$$

در نتیجه به ازای هر $x_2,x_4,y_2,y_4 \in \mathbb{F}$ داریم:

$$\tilde{\alpha}_i(x_2+y_2,x_4+y_4) = \tilde{\alpha}_i(x_2,x_4) + \tilde{\alpha}_i(y_2,y_4), \quad i = 1,2,3 \qquad (۳\text{–}۶)$$

حال فرض کنید $x_2,x_4 \in \mathbb{F}$ موجود باشند به طوری که $\tilde{\alpha}_2(x_2,x_4) = 0$. در این صورت داریم

$$[s,t_{(x_2,x_4)}] = \begin{bmatrix} 1 & 0 & \tilde{\alpha}_1(x_2,x_4) & 0 & \tilde{\alpha}_3(x_2,x_4) \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$
$$= I_5 + \tilde{\alpha}_1(x_2,x_4)E_{1,3} + \tilde{\alpha}_3(x_2,x_4)E_{1,5}.$$

یعنی $[s,t_{(x_2,x_4)}] \in \mathcal{T}$ که چون R شامل انتقال غیر بدیهی نیست بنابراین باید داشته باشیم:

$$\tilde{\alpha}_1(x_2,x_4) = \tilde{\alpha}_3(x_2,x_4) = 0.$$

اما در این حالت خواهیم داشت $t_{(x_2,x_4)} \in \mathcal{T}$ که باز هم چون R شامل انتقال غیر بدیهی نیست نتیجه می‌شود که $x_2 = x_4 = 0$. پس اگر $\tilde{\alpha}_2(x_2,x_4) = 0$ آنگاه داریم $x_2 = x_4 = 0$. به عبارت دیگر اگر $(x_2,x_4) \neq (0,0)$ آنگاه $\tilde{\alpha}_2(x_2,x_4) \neq 0$ و لذا می‌توانیم عضو $m_{\tilde{\alpha}_2(x_2,x_4)^{-1}}$ را در نظر بگیریم. داریم:

$$z[m_{\tilde{\alpha}_2(x_2,x_4)^{-1}}, t_{(x_2,x_4)}] = I_5 + \frac{\tilde{\alpha}_1(x_2,x_4)}{\tilde{\alpha}_2(x_2,x_4)}E_{1,3} + \frac{\tilde{\alpha}_3(x_2,x_4)+1}{\tilde{\alpha}_2(x_2,x_4)}E_{1,5}.$$

که باز هم چون R شامل انتقال غیر بدیهی نیست پس باید داشته باشیم $\alpha_1(x_2,x_4) = 0$ و $\tilde{\alpha}_3(x_2,x_4) + 1 = 0$ که چون $\mathrm{char}\,(\mathbb{F}) = 2$ نتیجه می‌دهد $\tilde{\alpha}_3(x_2,x_4) = 0$. بنابراین برای هر $(x_2,x_4) \neq (0,0)$ داریم $\tilde{\alpha}_1(x_2,x_4) = 0$ و $\tilde{\alpha}_3(x_2,x_4) = 0$. بنابراین با قرار دادن $(x_2,x_4) = (1,1)$ با توجه به رابطه (۳ـ۶) داریم:

$$1 = \tilde{\alpha}_3(1,1)\tilde{\alpha}_3(1+0,0+1) = \tilde{\alpha}_3(0,1) = 1+1 = 0.$$

پس $0 = 1$ که تناقض نهایی به دست آمد. بنابراین فرض $R \cap \mathcal{T} = \{I_5\}$ باطل است و R حتماً شامل انتقال غیر بدیهی است و حکم قضیه به دست می‌آید. □

قضیه زیر در حقیقت یک جمع بندی از نتایج عدم وجود به دست آمده را بیان می کند.

قضیه ۳ـ۳. *فرض کنید که R یک زیرگروه منظم از $\mathrm{AGL}_n\,(\mathbb{F})$ باشد و فرض کنید که R تک‌توان باشد هرگاه $\mathrm{char}\,(\mathbb{F}) = 0$. فرض کنید که یکی از شرایط زیر برقرار است:*

الف. $n \leq 2$.

ب. $n = 3$ و $\mathbb{F} \neq \mathbb{F}_2$.

پ. $n = 4$ و $\mathrm{char}\,\mathbb{F} = 2$.

در این صورت R شامل یک انتقال غیر بدیهی است.

برهان. اگر $n = 1$ آنگاه $\mathcal{T} = \mathrm{AGL}_1(\mathbb{F})$. بنابراین در این حالت حکم بدیهی است، زیرا با توجه به این‌که در این حالت مجموعه $\Omega = \{(1,x) \mid x \in \mathbb{F}\}$ دارای حداقل دو عضو است پس برای منظم

بودن، زیرگروه R حتماً باید غیر بدیهی باشد که در نتیجه شامل انتقال غیر بدهی خواهد بود. فرض کنیم $n = ۲$. اگر $\mathrm{char}\,(\mathbb{F}) = ۰$، طبق فرض R تک‌توان است و لذا طبق لم ؟؟ شامل یک انتقال غیر بدیهی است. اگر $\mathrm{char}\,(\mathbb{F}) > ۲$ باشد آن‌گاه طبق قضیه ۲ـ۱۷، R تک‌توان است و باز هم طبق لم ؟؟ شامل انتقال غیر بدیهی خواهد بود. اگر $n = ۳$ آن‌گاه طبق فرض داریم $\mathbb{F} \neq \mathbb{F}_۲$ و لذا طبق قضیه ؟؟، R شامل انتقال غیر بدیهی خواهد بود. بالاخره اگر $n = ۴$ آن‌گاه طبق فرض داریم $\mathrm{char}\,(\mathbb{F}) = ۲$ و در نتیجه طبق قضیه ۳ـ۲، R شامل انتقال غیر بدیهی است و اثبات حکم تمام می‌شود. □

۳ـ۲ تعمیم وجود زیرگروه‌های منظم بدون هیچ انتقال غیربدیهی

در این بخش پس از اثبات یک لم و با استفاده از آن زیرگروه‌های منظمی که شامل هیچ انتقال بدیهی نباشند را خواهیم ساخت.

لم ۳ـ۴. *فرض کنید $m, k \geq ۱$ و d یک بردار سطری ثابت از $\mathbb{F}^k$ باشد. فرض کنید Q یک فرم درجه دوم روی $\mathbb{F}^m$ با فرم قطبی J و فرض کنید که $\varphi : (\mathbb{F}^k, +) \to \mathrm{O}_m(\mathbb{F}, Q)$ یک همریختی گروهی باشد. در این صورت احکام زیر برقرار است:*

الف. مجموعه

$$N = \left\{ \begin{bmatrix} ۱ & v & Q(v)d \\ ۰ & I_m & Jv^T \otimes d \\ ۰ & ۰ & I_k \end{bmatrix} \quad \Big| \quad v \in \mathbb{F}^m \right\}$$

زیرگروهی از $\mathrm{AGL}_{m+k}(\mathbb{F})$ است.

ب. مجموعه

$$M = \left\{ \begin{bmatrix} ۱ & ۰ & a \\ ۰ & \varphi(a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix} \quad \Big| \quad a \in \mathbb{F}^k \right\}$$

زیرگروهی از $\mathrm{AGL}_{m+k}(\mathbb{F})$ است به طوری که $M \leq N_{\mathrm{AGL}_{m+k}(\mathbb{F})}(N)$.

پ. گروه $R = M \ltimes N$ یک زیر گروه منظم از $\mathrm{AGL}_{m+k}(\mathbb{F})$ است و اگر Q نامولد باشد و $d \neq 0$، آن‌گاه داریم $R \cap \mathcal{T} \cong \ker(\varphi)$.

برهان. ابتدا توجه می‌کنیم که اعضای N ماتریس‌هایی $(m+k+1)\times(m+k+1)$ هستند. هم‌چنین در عبارت $Jv^T \otimes d$، J ماتریسی $m \times m$ است و $v \in \mathbb{F}^n$ و لذا v^T یک ماتریس $m \times 1$ است، پس Jv^T یک ماتریس $m \times d$ است که با ساختار بلوکی بیان شده سازگار است. حال به اثبات بخش‌های مختلف می‌پردازیم.

الف. ابتدا توجه می‌کنیم که حاصل‌ضرب اعضای N به شکل بلوکی زیر است:

$$\begin{bmatrix} 1 & v & Q(v)d \\ 0 & I_m & Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix} \begin{bmatrix} 1 & v' & Q(v')d \\ 0 & I_m & J(v')^T \otimes d \\ 0 & 0 & I_v \end{bmatrix}$$
$$= \begin{bmatrix} 1 & v'+v & Q(v')d + vJ(v')^T \otimes d + Q(v)d \\ 0 & I_m & Jv'^T \otimes d + Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix}$$
$$= \begin{bmatrix} 1 & v'+v & Q(v'+v)d \\ 0 & I_m & J(v'^T + v^T) \otimes d \\ 0 & 0 & I_k \end{bmatrix}$$

که نشان می دهد N بسته است. همچنین با توجه به عمل حاصلضرب، معکوس اعضای N به صورت زیر است:

$$\begin{bmatrix} 1 & v & Q(v)d \\ 0 & I_m & Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -v & Q(-v)d \\ 0 & I_m & J(-v)^T \otimes d \\ 0 & 0 & I_k \end{bmatrix} \in N$$

بنابراین N زیرگروهی از $\mathrm{AGL}_{m+k}(\mathbb{F})$ می‌باشد.

ب. توجه می‌کنیم که حاصل‌ضرب اعضای M به شکل بلوکی زیر است:

$$\begin{bmatrix} ۱ & ۰ & a \\ ۰ & \varphi(a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix} \begin{bmatrix} ۱ & ۰ & b & ۰ & \varphi(b) & ۰ \\ ۰ & ۰ & I_k & & & \end{bmatrix} = \begin{bmatrix} ۱ & ۰ & b+a \\ ۰ & \varphi(a)\varphi(b) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix}$$

$$= \begin{bmatrix} ۱ & ۰ & b+a \\ ۰ & \varphi(b+a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix}$$

که در رابطه فوق از همریختی بودن $\varphi : (\mathbb{F}^k, +) \to \mathrm{O}_m(\mathbb{F}, Q)$ استفاده کرده‌ایم (که نتیجه می‌دهد $\varphi(a)\varphi(b) = \varphi(a+b)$). بنابراین حاصل‌ضرب هر دو عضو از M دوباره عضوی از M است و هم‌چنین واضح است که

$$\begin{bmatrix} ۱ & ۰ & a \\ ۰ & \varphi(a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix}^{-۱} = \begin{bmatrix} ۱ & ۰ & -a \\ ۰ & \varphi(-a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix} \in M$$

پس M زیرگروهی از $\mathrm{AGL}_{m+k}(\mathbb{F})$ می‌باشد. حال نشان می‌دهیم M زیرگروهی از نرمال‌ساز N در $\mathrm{AGL}_{m+k}(\mathbb{F})$ می‌باشد. فرض کنید که

$$A = \begin{bmatrix} ۱ & v & Q(v)d \\ ۰ & I_m & Jv^T \otimes d \\ ۰ & ۰ & I_k \end{bmatrix} \in N, \quad B = \begin{bmatrix} ۱ & ۰ & a \\ ۰ & \varphi(a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix} \in M.$$

در این صورت داریم:

$$B^{-۱}AB = \begin{bmatrix} ۱ & ۰ & -a \\ ۰ & \varphi(a)^{-۱} & ۰ \\ ۰ & ۰ & I_k \end{bmatrix} \begin{bmatrix} ۱ & v & Q(v)d \\ ۰ & I_m & Jv^T \otimes d \\ ۰ & ۰ & I_k \end{bmatrix} \begin{bmatrix} ۱ & ۰ & a \\ ۰ & \varphi(a) & ۰ \\ ۰ & ۰ & I_k \end{bmatrix}$$

$$= \begin{bmatrix} ۱ & v\varphi(a) & Q(v)d \\ ۰ & I_m & \varphi(a)^{-۱}Jv^T \otimes d \\ ۰ & ۰ & I_k \end{bmatrix} = \begin{bmatrix} ۱ & v\varphi(a) & Q(v\varphi(a))d \\ ۰ & I_m & J(v\varphi(a))^T \otimes d \\ ۰ & ۰ & I_k \end{bmatrix}.$$

در رابطه فوق دقت می‌کنیم که چون $\varphi(a) \in \mathrm{O}_m(\mathbb{F}, Q)$ پس طبق تعریف $Q(v\varphi(a)) = Q(v)$.
هم‌چنین با توجه به خواص فرم درجه دوم Q و شکل قطبی آن داریم:

$$J(v\varphi(a))^T = J\varphi(a)^T v^T = \varphi(a)^{-1}\varphi(a)J\varphi(a)^T v^T = \varphi(a)^{-1}Jv^T.$$

بنابراین با توجه به شکل $B^{-1}AB$ می‌بینیم که $B^{-1}AB \in N$ و لذا $M \leq N_{\mathrm{AGL}_{m+k}(\mathbb{F})}(N)$.

پ. چون $M \leq N_{\mathrm{AGL}_{m+k}(\mathbb{F})}(N)$ بنابراین M روی N با مزدوج سازی عمل می‌کند و لذا می‌توان حاصل‌ضرب نیم مستقیم $M \ltimes N$ را تشکیل داد. قرار می‌دهیم $R = M \ltimes N$. با توجه به شکل اعضای M و N واضح است که $M \cap N = 1$. لذا به جای استفاده از زوج مرتب برای نمایش اعضای R می‌توانیم هر عضو R را به صورت حاصل‌ضرب عضوی از M در عضوی از N نمایش دهیم. بنابراین هر عضو R مانند r را می‌توان به صورت یکتای $r = AB$ نوشت که $A \in M$ و $B \in N$ و لذا r دارای نمایشی به صورت زیر است:

$$\begin{aligned} r = AB &= \begin{bmatrix} 1 & 0 & a \\ 0 & \varphi(a) & 0 \\ 0 & 0 & I_k \end{bmatrix} \begin{bmatrix} 1 & v & Q(v)d \\ 0 & I_m & Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix} \\ &= \begin{bmatrix} 1 & v & a + Q(v)d \\ 0 & \varphi(a) & \varphi(a)Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix} \end{aligned}$$

بنابراین

$$\begin{aligned} R &= \left\{ \begin{bmatrix} 1 & v & a + Q(v)d \\ 0 & \varphi(a) & \varphi(a)Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix} \;\middle|\; v \in \mathbb{F}^m, a \in \mathbb{F}^k \right\} \\ &= \left\{ \begin{bmatrix} 1 & v & a \\ 0 & \varphi(a - Q(v)d) & \varphi(a - Q(v)d)Jv^T \otimes d \\ 0 & 0 & I_k \end{bmatrix} \;\middle|\; v \in \mathbb{F}^m, a \in \mathbb{F}^k \right\} \end{aligned}$$

که در رابطه آخر به جای a از $a = \varphi(v)d$ استفاده شده است. این امر هیچ اشکالی ایجاد نمی‌کند

زیرا می‌توان نوشت

$$\mathbb{F}^k = \left\{a - \varphi(v)d \mid a \in \mathbb{F}^k\right\} \quad (۳\text{–}۷)$$

درستی رابطه (۳ـ۷) واضح است زیرا اولاً به ازای هر $a \in \mathbb{F}^k$ داریم $a - \varphi(v)d \in \mathbb{F}^k$ که نشان می‌دهد

$$\left\{a - \varphi(v)d \mid a \in \mathbb{F}^k\right\} \subseteq \mathbb{F}^k$$

و ثانیاً اگر $b \in \mathbb{F}^k$ دلخواه باشد، آنگاه $b + \varphi(v)d \in \mathbb{F}^k$، مثلاً اگر قرار دهیم $a = b + \varphi(v)d$ آنگاه $b = a - \varphi(v)d$ که نشان می‌دهد $\mathbb{F}^k \subseteq \{a - \varphi(v)d \mid a \in \mathbb{F}^k\}$. پس رابطه (۳ـ۷) برقرار است.

لذا نشان دادیم که هر عضو R به صورت یکتایی به شکل

$$\begin{bmatrix} ۱ & v & a \\ ۰ & \varphi(a - Q(v)d) & \varphi(a - Q(v)d)Jv^T \otimes d \\ ۰ & ۰ & I_k \end{bmatrix}, \quad v \in \mathbb{F}^m, a \in \mathbb{F}^k$$

نوشت. دلیل یکتایی این است که درایه‌های سطرهای بعد کاملاً ازروی v و a مشخص می‌شوند. چون هر عضو $x \in \mathbb{F}^{m+k}$ را می‌توان به صورت $x = (v, a)$ نوشت که $v \in \mathbb{F}^m$ و $a \in \mathbb{F}^k$، بنابراین به ازای هر $x \in \mathbb{F}^{m+k}$ عضو منحصر به فردی از R موجود است که x سطر اول آن است و لذا R منظم است.

حال فرض کنید که Q نامولد باشد و r عضوی از R باشد که $(۱, v, a)$ سطر اول آن است. می‌خواهیم نشان دهیم که اگر $d \neq ۰$، آنگاه $R \cap \mathcal{T} \cong \ker \varphi$. با توجه به تعریف $r \in R \cap \mathcal{T}$ اگر و تنها اگر $\varphi(a - \varphi(v)d) = I_m$ و $Jv^T \otimes d = ۰$. از $Jv^T \otimes d = ۰$ نتیجه می‌شود که یا $d = ۰$ و یا $Jv^T = ۰$. چون $d \neq ۰$ پس $Jv^T = ۰$. چون Q نامولد است اگر $v \neq ۰$ آنگاه $Q(v) \neq ۰$ و لذا حتماً باید داشته باشیم $v = ۰$. بنابراین $\varphi(a) = \varphi(a - \varphi(v)d) = I_m$. پس $I_m = \varphi(a)$ و لذا

$a \in \ker\varphi$. حال کافی است تابع ψ را به صورت زیر تعریف کنیم:

$$\psi : R \cap \mathcal{T} \longrightarrow \ker\varphi$$

$$\psi(r) = a$$

در این صورت با توجه به موارد بالا φ یکریختی است و لذا خواهیم داشت $R \cap \mathcal{T} \cong \ker\varphi$. □

یادآوری می‌شود که اگر $\mathbb{F}$ یک میدان باشد، آنگاه اشتراک همه‌ی زیرمیدان‌های $\mathbb{F}$، زیرمیدان اول $\mathbb{F}$ نامیده می‌شود.

قضیه ۳ـ۵. *فرض کنید که $\mathbb{F}$ یک میدان باشد و W زیرفضایی از $\mathbb{F}$ باشد که به عنوان یک فضای برداری روی زیرمیدان اول $\mathbb{F}_{۰}$ در نظر گرفته می‌شود. فرض کنید که یکی از شرایط زیر برقرار است:*

الف. $n = ۳$ و $\mathbb{F} = \mathbb{F}_{۲}$،

ب. $n \geq ۴$ و $\operatorname{char}\mathbb{F} \neq ۲$،

پ. $n \geq ۵$ و $\operatorname{char}\mathbb{F} = ۲$.

در این صورت یک زیرگروه منظم R_W از $\mathrm{AGL}_n(\mathbb{F})$ موجود است به طوری که $R_W \cap \mathcal{T} \cong (W, +)$.
به ویژه زیرگروه منظم $R_{\{۰\}}$ موجود است به طوری که $R_{\{۰\}} \cap \mathcal{T} = \{I_{n+۱}\}$.

برهان. اگر n زوج باشد و $\operatorname{char}\mathbb{F} = ۲$ آنگاه در اثبات لم ۳ـ۴، قرار می‌دهیم $(m, k) = (n - ۲, ۲)$ و در بقیه حالت‌ها در لم ۳ـ۴ قرار می‌دهیم $(m, k) = (n - ۱, ۱)$. در این صورت با توجه به فصل ۱۱ از [۱۲] یک فرم درجه دوم نامولد Q روی $\mathbb{F}^m$ موجود است به طوری که $\mathrm{O}_m(\mathbb{F}, Q)$ شامل یک زیر گروه یکریخت با $(\mathbb{F}^k, +)$ است. فرض کنید که

$$\psi : (\mathbb{F}^k, +) \to \mathrm{O}_m(\mathbb{F}, Q)$$

همان یکریختی بین $(\mathbb{F}^k, +)$ و زیرگروه بیان شده از $Q_m(\mathbb{F}, Q)$ باشد. همچنین فرض کنید که U متممی برای W در $\mathbb{F}^k$ باشد، یعنی $\mathbb{F}^k = U \oplus W$. چون $\mathbb{F}^k = U \oplus W$ پس هر عضو a از $\mathbb{F}^k$ را

می‌توان به صورت منحصر به فردی به شکل زیر نوشت:

$$a = u_a + w_a, \quad u_a \in U,\ w_a \in W.$$

فرض کنید که ϖ تابع تصویر از $\mathbb{F}^k$ به روی U باشد یعنی

$$\varpi : \mathbb{F}^k \longrightarrow \mathbb{F}^k$$

$$\varpi(u_a + w_a) = u_a$$

در این صورت تابع $\psi\varpi = \varpi$ یک همریختی گروهی از $(\mathbb{F}^k, +)$ به $\mathrm{O}_m(\mathbb{F}, Q)$ است، زیرا

$$\begin{aligned}\psi\varpi(a+b) &= \psi\varpi\big((u_a + w_a) + (u_a + w_b)\big) = \psi\varpi\big((u_a + u_a) + (w_a + w_b)\big)\\ &= \psi(u_a + u_b) \xlongequal{\text{همریختی } \psi} \psi(u_a) + \psi(u_b) = \psi\varpi(a) + \psi\varpi(b).\end{aligned}$$

هسته همریختی $\psi\varpi$ برابر است با:

$$\begin{aligned}\ker(\psi\varpi) &= \{a \in \mathbb{F}^k \mid \psi\varpi(a) = I\}\\ &= \{a \in \mathbb{F}^k \mid \psi(u_a) = I\}\\ &\xlongequal{\text{همریختی شمول } \psi} \{a \in \mathbb{F}^k \mid u_a = 0\} = W.\end{aligned}$$

پس هسته همریختی $\psi\varpi$ برابر با W است. حال فرض کنید که M و N زیرگروه‌های معرفی شده در لم ۳ـ۴ باشند. در این صورت $R = M \ltimes N$ یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ می‌باشد. همچنین با توجه به قسمت سوم لم ۳ـ۴ داریم: $R \cap \mathcal{T} \cong \ker(\psi\varpi) = (W, +)$. پس قسمت اول اثبات می‌شود. در حالت خاص اگر قرار دهیم $W = \{0\}$ در این صورت $R \cap \mathcal{T}$ گروه بدیهی یعنی همان $\{I_{n+1}\}$ خواهد بود. $\square$

مثال ۳ـ۶. فرض کنید $\mathrm{char}\,\mathbb{F} \neq 2$، $n \geq 4$، و فرم درجه دوم Q روی $\mathbb{F}^{n-1}$ را به صورت

$$Q(x_1, \ldots, x_{n-1}) = x_1 x_3 - x_2^2 + \frac{1}{2}\sum_{i=4}^{n-1} x_i^2.$$

در نظر می‌گیریم. شکل قطبی Q به صورت $J = \mathrm{diag}(A, I_{n-4})$ است که $J \in \mathrm{GL}_{n-1}(\mathbb{F})$ و

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

تابع $\varphi : \mathbb{F} \to \mathrm{GL}_{n-1}(\mathbb{F})$ را به صورت زیر تعریف می‌کنیم:

$$\varphi : \mathbb{F} \longrightarrow \mathrm{GL}_{n-1}(\mathbb{F})$$

$$\varphi(a) = I_{n-1} + 2aE_{2,1} + a^2E_{3,1} + aE_{3,2}$$

در این صورت φ یک تکریختی از $(\mathbb{F}, +)$ به $\mathrm{O}_{n-1}(\mathbb{F}, Q)$ است. زیرا اولاً φ همریختی است چون

$$\begin{aligned}\varphi(a+b) &= I_{n-1} + 2(a+b)E_{2,1} + (a+b)^2E_{3,1} + (a+b)E_{3,2} \\ &= (I_{n-1} + 2aE_{2,1} + a^2E_{3,1} + aE_{3,2})(I_{n-1} + 2bE_{2,1} + b^2E_{3,1} + bE_{3,2}) \\ &= \varphi(a)\varphi(b)\end{aligned}$$

و همچنین φ یک به یک است چون

$$\varphi(a) = I_{n-1} \to 2a = 0 \to a = o \to \ker\varphi = \{0\}.$$

پس φ تکریختی است. حال با توجه به لم ۳ـ۴، زیرگروه R به صورت

$$R = \left\{ \begin{bmatrix} 1 & v & a + Q(v) \\ 0 & \varphi(a) & \varphi(a)Jv^T \\ 0 & 0 & 1 \end{bmatrix} \quad \middle| \quad v \in \mathbb{F}^{n-1}, a \in \mathbb{F} \right\}$$

یک زیر گروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ است که شامل هیچ انتقال غیر بدیهی نیست زیرا

$$R \cap \mathcal{T} \cong \ker\varphi = \{0\}.$$

مثال ۳ـ۷. فرض کنید $\mathrm{char}\,\mathbb{F} = 2$، $n = 2t + 1 \geq 3$ و فرم درجه دوم Q روی $\mathbb{F}^{2t}$ را به صورت

$$Q(x_1, \ldots, x_{2t}) = \sum_{i=1}^{t} x_i x_{t+i}$$

در نظر می‌گیریم. شکل قطبی Q ماتریس به شکل $\left(\begin{smallmatrix} 0 & I_t \\ I_t & 0 \end{smallmatrix}\right)$ دارد. اگر $n \geq 5$ (که در نتیجه $t \geq 2$)، تابع

$$\varphi : \mathbb{F} \longrightarrow \mathrm{GL}_{2t}(\mathbb{F})$$

$$\varphi(a) = I_{2t} + a(E_{1,t} + E_{2t,t+1})$$

یک همریختی از $(\mathbb{F}, +)$ به $\mathrm{O}_{2t}(\mathbb{F}, Q)$ است. زیرا:

$$\begin{aligned}\varphi(a+b) &= I_{2t} + (a+b)(E_{1,t} + E_{2t,t+1}) \\ &= \big(I_{2t} + a(E_{1,t} + E_{2t,t+1})\big)\big(I_{2t} + b(E_{1,t} + E_{2t,t+1})\big) = \varphi(a)\varphi(b)\end{aligned}$$

که نشان می‌دهد φ همریختی است. هم‌چنین داریم:

$$a \in \ker\varphi \to \varphi(a) = I_{2t} \to a = 0 \to \ker\varphi = \{0\}.$$

بنابراین با توجه به لم ۳ـ۴، زیرگروه R به صورت

$$R = \left\{ \begin{bmatrix} 1 & v & a + Q(v) \\ 0 & \varphi(a) & \varphi(a)Jv^t \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; v \in \mathbb{F}^{2t},\ a \in \mathbb{F}^k \right\}$$

یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ است که باز هم با توجه به این‌که $R \cap \mathcal{T} \cong \ker\varphi = \{0\}$، R شامل هیچ انتقال غیر بدیهی نیست. در حالتی که $n = 3$ (و لذا $t = 1$) و $\mathbb{F} = \mathbb{F}_2$، تابع φ را به صورت

$$\varphi : \mathbb{F}_2 \longrightarrow \mathrm{O}_2(\mathbb{F}_2)$$

$$\varphi(1) = E_{1,2} + E_{2,1}$$

تعریف می‌کنیم. در این صورت باز هم طبق لم ۳ـ۴،

$$R = \left\{ \begin{bmatrix} 1 & v & a + Q(v) \\ 0 & \varphi(a) & \varphi(a)Jv^T \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; v \in \mathbb{F}^{2},\ a \in \mathbb{F} \right\}$$

یک زیر گروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ است که شامل هیچ انتقال غیر بدیهی نیست.

مثال ۳ــ۸. فرض کنید $\operatorname{char}\mathbb{F} = ۲$ و $n = ۲t + ۲ \geq ۶$ و فرض کنید Q فرم درجه دوم روی $\mathbb{F}^{۲t}$ باشد که به صورت زیر باشد.

$$\varphi : \mathbb{F}^{۲} \longrightarrow \mathrm{GL}_{۲t}(\mathbb{F})$$

$$\varphi(a,b) = I_{۲t} + a(E_{۱,t} + E_{۲t,t+۱}) + b(E_{۱,۲t} + E_{t,t+۱}) + abE_{۱,t+۱}$$

در این صورت φ یک همریختی است که

$$\ker\varphi = \{(a,b) \mid \varphi(a,b) = I_{۲t}\} = \{(a,b) \mid a = ۰,\ b = ۰\} = \{(۰,۰)\}.$$

بنابراین باز هم طبق لم ۳ــ۴ زیرگروه R که به صورت زیر است یک زیرگروه منظم از $\mathrm{AGL}_n(\mathbb{F})$ که شامل هیچ انتقال غیر بدیهی نیست.

$$R = \left\{ \begin{bmatrix} ۱ & v & a + Q(v)d \\ ۰ & \varphi(a) & \varphi(a)Jv^T \\ ۰ & ۰ & ۱ \end{bmatrix} \;\middle|\; v \in \mathbb{F}^{n-۱}, a \in \mathbb{F} \right\}$$

توجه می‌کنیم که باز هم طبق لم ۳ــ۴ داریم $R \cap \mathcal{T} \cong \ker\varphi = \{(۰,۰)\}$.

جمع بندی مطالب و گزاره‌های به دست آمده در مورد وجود زیرگروه‌های منظم بدون انتقال غیربدیهی و عدم وجود چنین زیرگروه‌هایی را می‌توان در قالب نتایج زیر بیان کرد.

نتیجه ۳ــ۹. *فرض کنید که $\mathbb{F}$ یک میدان از مشخصه عددی مثبت باشد. در این صورت گروه $AGL_n(F)$ شامل یک زیرگروه منظم بدون انتقال غیربدیهی است اگر و تنها اگر یکی از احکام زیر برقرار باشد:*

الف. $n = ۳$ و $|\mathbb{F}| = ۲$؛

ب. $n = ۴$ و $char(\mathbb{F}) > ۲$؛

پ. $n \geq ۵$.

برهان. با توجه به قضایای ۳ــ۳ و ۳ــ۵ حکم واضح است. □

نتیجه ۳ـ۱۰. *فرض کنید که* $\mathbb{F}$ *یک میدان از مشخصه صفر باشد. در این صورت گروه* $AGL_n(F)$ *شامل یک زیرگروه منظم بدون انتقال غیربدیهی است اگر و تنها اگر* $n \geq ۴$.

برهان. با توجه به قضایای ۳ـ۳ و ۳ـ۵ حکم واضح است. □

کتاب‌نامه

[۱] جمالی، علیرضا. *مقدمه‌ای بر نظریه‌ی گروه‌های متناهی*. انتشارات مبتکران، تهران، ۱۳۹۱.

[۲] فقیهی، سید احمد. *مبانی جبر*. انتشارات پوران پژوهش، تهران، ۱۳۹۳.

[3] Catino, F., Colazzo, I., and Stefanelli, P. Regular subgroups of the affine group and asymmetric product of radical braces. *J. Algebra*, **455**:164–182, 2016.

[4] Hegedus, P. Regular subgroups of the affine group. *J. Algebra*, **225**(2):740–742, 2000.

[5] Humphreys, J. E. *Linear algebraic groups*. New York-Heidelberg, 1975.

[6] Liebeck, M. W., Praeger, C. E., and Saxl, J. Transitive subgroups of primitive permutation groups. *J. Algebra*, **234**(2):291–361, 2000.

[7] Pellegrini, M. A. and Tamburini, Bellani M. C. Regular subgroups of the affine group with no translations. *J. Algebra*, **478**:410–418, 2017.

[8] Pellegrini, M. A. and Tamburini Bellani, M. C. More on regular subgroups of the affine group. *Linear Algebra and its Applications*, **505**:126–151, 2016.

[9] Rosse, J. S. *A course on group theory*. Cambridge University Press, 1978.

[10] Taboga, M. Properties of the kronecker product. *Lectures on matrix algebra*, 2021.

[11] Tamburini, Bellani M. C. Some remarks on regular subgroups of the affine group. *International Journal of group theory*, 2012.

[12] Taylor, D. E. *The geometry of the classical groups*, volume **9**. Heldermann Verlag, 1992.

واژه‌نامه فارسی به انگلیسی

آ

آبلی .... Abelian

انتقال .... Translation

آفین .... Affine

ب

بالا مثلثی .... Upper triangular

پ

پایه .... Basis

پایه کانونی .... Canonical basis

ت

تصویر .... Projection

تک‌توان .... Unipotent

تکریختی .... Monomorphism

ج

جایگشت .... Permutation

د

درجه دوم .... Quadratic

ز

زیرگروه .... Subgroup

ف

فضای برداری .... Vector space

ق

قطری .... Diagonal

گ

گروه .... Group

گروه آفین .... Affine group

گروه جمعی .... Additive group

گروه متعامد .... Orthogonal group

م

ماتریس .... Matrix

متناهی .... Finite

مرکزساز .... Centralizer

مزدوج .... Conjugate

مزدوج سازی .... Conjugation

مشخصه .... Characteristic

منظم .... Regular

میدان . . . . Field

میدان اول . . . . Prime field

ن

نامولد . . . . Non-degenerate

ه

همریختی . . . . Homomorphism

ی

یکریخت . . . . Isomorphic

یکریختی . . . . Isomorphism

واژه‌نامه انگلیسی به فارسی

A

Abelian .... آبلی

Additive group .... گروه جمعی

Affine .... آفین

Affine group .... گروه آفین

B

Basis .... پایه

C

Canonical basis .... پایه کانونی

Centralizer .... مرکزساز

Characteristic .... مشخصه

Conjugate .... مزدوج

Conjugation .... مزدوج سازی

D

Diagonal .... قطری

F

Field .... میدان

Finite .... متناهی

G

Group .... گروه

H

Homomorphism .... همریختی

I

Isomorphic .... یکریخت

Isomorphism .... یکریختی

M

Matrix .... ماتریس

Monomorphism .... تکریختی

N

Non-degenerate .... ناموِلد

O

Orthogonal group .... گروه متعامد

P

Permutation .... جایگشت

Prime field .... میدان اول

Projection .... تصویر

Q

Quadratic .... درجه دوم

R

Regular .... منظم

S

Subgroup .... زیرگروه

T

Translation .... انتقال

U

Unipotent .... تک‌توان

Upper triangular .... بالا مثلثی

V

Vector space .... فضای برداری

Abstract

Given a regular subgroup R of $\mathrm{AGL}_n(\mathbb{F})$, one can ask if R contains nontrivial translations. A negative answer to this question was given by Liebeck, Praeger and Saxl for $\mathrm{AGL}_2(p)$ (p a prime), $\mathrm{AGL}_3(p)$ (p odd prime) and for $\mathrm{AGL}_4(2)$. A positive answer was given by Hegedus for $\mathrm{AGL}_n(p)$ when $n \leq 4$ if p is odd and for $n = 3$ or $n \leq 5$ if $p = 2$. A first generalization to finite fields of Hegedus' construction was recently obtained by Catino, Colazzo and Stefanelli. In this thesis we give examples of such subgroups in $\mathrm{AGL}_n(\mathbb{F})$ for any $n \leq 5$ and any field $\mathbb{F}$. For $n < 5$ we provide necessary and sufficient conditions for their existence, assuming R to be unipotent if $\operatorname{char} \mathbb{F} = 0$.

Keywords: Regular subgroup, Affine group, Translations.

The University of Qom
Faculty of Science
Department of Mathematics

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Pure Mathematics

Title:

Regular subgroups of the affine group with no translations

Supervisor:
Seyyed Ali Moosavi

By:
Fatemeh Mahmoudi

Summer 2021