گروههای ماتیو

محمدرضا درفشه، غلامرضا برادران خسروشاهی*

۱. مقدمه

نظریهٔ گروهها با مطالعهٔ گروههای جایگشتی آغاز شد. اول‌بار، اواریست گالوا به‌هنگام کوشش برای حل معادلات درجهٔ پنج به‌بالا به‌وسیلهٔ رادیکالها، چنین گروههایی را به‌کار گرفت، هرچند وی آنها را گروه ننامید. گالوا به‌هرچندجمله‌ای تحویل‌ناپذیر $f(x)$ روی اعداد گویا مجموعه‌ای مانند G نسبت داد به‌طوری‌که عناصر آن ریشه‌های $f(x)$ را به‌یکدیگر تبدیل می‌کرد. به‌علاوه مجموعهٔ G دارای ویژگیهای دیگری‌نیز بود که باعث می‌شد، به‌زبان امروزی، دارای ساختار گروهی باشد.

یک **گروه جایگشتی** روی مجموعهٔ Ω عبارت است از زیرمجموعه‌ای از نگاشتهای وارونپذیر Ω در Ω به طوری که تحت قانون ترکیب نگاشتها دارای ساختار گروهی باشد. درحالت خاص، مجموعهٔ تمام نگاشتهای وارونپذیر Ω در Ω دارای ساختار یک گروه است که گروه متقارن مجموعهٔ Ω نامیده و با S_Ω نمایش داده می‌شود. درحالتی که Ω یک مجموعهٔ متناهی است و $|\Omega|=n$، گروه متقارن روی Ω را با S_n نمایش می‌دهند. درواقع می‌توان گفت که یک گروه جایگشتی عبارت است از زیرگروهی از S_Ω. اگر G یک گروه جایگشتی روی Ω باشد، یعنی $G\leqslant S_\Omega$، آنگاه عمل G روی Ω را با $(G|\Omega)$ نشان می‌دهیم و به‌جای اینکه بگوییم G یک گروه جایگشتی روی Ω است زوج (G,Ω) را یک گروه جایگشتی می‌نامیم. هر عنصر Ω یک حرف نامیده می‌شود. به ازای $\omega\in\Omega$ و $g\in G$ اثر g بر ω را به‌صورت ω^g نمایش می‌دهیم و توجه‌داریم که $\omega^g\in\Omega$. هر عنصر G یک جایگشت روی Ω نامیده می‌شود و معمول است که ترکیب جایگشتها از چپ به‌راست نوشته شود. یعنی اگر $\omega\in\Omega$ و $g,h\in G$، آنگاه $(\omega^g)^h=\omega^{gh}$. عضو خنثای G را با ۱ نمایش می‌دهیم و توجه‌داریم که $\omega^1=\omega$ به‌ازای تمام $\omega\in\Omega$.

برخی از مفاهیم اساسی مربوط به گروههای جایگشتی را که دراین مقاله از آنها صحبت خواهد شد در اینجا می‌آوریم ولی خواننده را برای مطالعهٔ مفصلتر به‌مرجع [۱۷] ارجاع می‌دهیم. فرض کنیم (G,Ω) یک گروه جایگشتی است. به‌ازای $\omega\in\Omega$ و $g\in G$ اگر $\omega^g=\omega$، آنگاه می‌گوییم g پایدارساز ω است. مجموعهٔ K متشکل از عناصر $g\in G$ به‌طوری‌که تمام عناصر $\omega\in\Omega$ را پایدار می‌سازند، هستهٔ عمل $(G|\Omega)$ نامیده می‌شود. K زیرگروهی از G است و اگر $K=\{1\}$، آنگاه عمل G بر Ω وفادار نامیده می‌شود. مجموعهٔ عناصر G را که عنصر داده شدهٔ $\omega\in\Omega$ را پایدار می‌سازند، با G_ω نمایش می‌دهیم و پایدارساز ω می‌نامیم. واضح است که G_ω زیرگروهی از G است. به‌طور کلی اگر Δ زیرمجموعه‌ای ناتهی از Ω باشد، آنگاه دو نوع پایدارساز برای Δ درنظر می‌گیریم. یکی پایدارساز مجموعه‌ای Δ، یعنی مجموعهٔ عناصر $g\in G$ به‌طوری‌که $\Delta^g=\Delta$ و دیگری پایدارساز نقطه به نقطهٔ Δ، یعنی مجموعهٔ عناصر $g\in G$ به‌طوری که $\omega^g=\omega$ به‌ازای هر $\omega\in\Delta$. اولی را با $G_{(\Delta)}$ و دومی را با $G_{[\Delta]}$ نمایش می‌دهیم. در اینجا منظور از Δ^g اینست: $\Delta=\{\alpha,\beta,\dots,\gamma\}$ یک $\Delta^g=\{\omega^g|\omega\in\Delta\}$. درحالتی که مجموعهٔ متناهی است قرار می‌دهیم $G_{[\Delta]}=G_{\alpha,\beta,\dots,\gamma}$.

اکنون اگر $\omega\in\Omega$، آنگاه $\omega^G=\{\omega^g|g\in G\}$ یک مدار G روی Ω نامیده می‌شود. واضح است که ω^G زیرمجموعه‌ای از Ω است. اگر فقط یک مدار داشته باشیم، آنگاه گروه جایگشتی (G,Ω) را متعدی می‌نامیم و می‌گوییم عمل G روی Ω متعدی است. مدار ω^G دارای این ویژگی است که اگر دو عنصر ω^g و ω^h، $g,h\in G$، را در آن درنظر بگیریم آنگاه داریم

$$(\omega^g)^{g^{-1}h}=(\omega^{gg^{-1}})^h=\omega^h$$

که دراینجا $g^{-1}h \in G$. بنابراین می‌توان گفت که گروه جایگشتی (G, Ω) متعدی است اگر و فقط اگر به‌ازای هردوعنصر ω_1 و ω_2 از Ω، عنصر $g \in G$ وجود داشته باشد به‌طوری که $\omega_2 = \omega_1^g$. مفهوم متعدی‌بودن را می‌توان به‌مفهوم k-متعدی‌بودن تعمیم داد. فرض کنید G روی Ω عمل کند و k عددی طبیعی باشد به‌طوری که $k \leqslant |\Omega|$. مجموعهٔ زیرمجموعه‌های مرتب k عضوی Ω را با Δ نمایش می‌دهیم. واضح است که عمل G بر Ω یک‌عمل G بر Δ القا می‌کند به‌این‌صورت که اگر $X \in \Delta$ و $g \in G$، آنگاه $X^g = \{x^g | x \in X\}$. اگر (G, Δ) یک گروه جایگشتی متعدی باشد آنگاه (G, Ω)را یک‌گروه جایگشتی k-متعدی می‌نامیم. درحالت خاص $k = 1$، گروه ۱-متعدی همان گروه متعدی است. به‌این‌ترتیب اگر (G, Ω) یک گروه k-متعدی باشد آنگاه به‌ازای هردو kتایی $(\alpha_1, \dots, \alpha_k)$ و $(\beta_1, \dots, \beta_k)$، α_iها متمایز و β_iها متمایز، عنصر $g \in G$ وجود دارد به‌طوری‌که $\alpha_i^g = \beta_i$، $1 \leqslant i \leqslant k$. اکنون اگرمجموعهٔ تمام زیر مجموعه‌های kعضوی Ω را با Γ نمایش دهیم (توجه داشته باشید که در این حالت زیر مجموعه‌های kعضوی متعلق به Γ مرتب نیستند) آنگاه گروه G روی Γ عمل می‌کند. دراین‌حالت، اگر (G, Γ) متعدی باشد، می‌گوییم (G, Ω) یک گروه جایگشتی k-همگن است.

گروههای S_n به ازای تمام nها روی مجموعهٔ nعضوی Ω به‌طور n-متعدی عمل می‌کنند درصورتی که گروههای متناوب A_n، $n \geqslant 3$، متشکل از تمام‌جایگشتهای زوج در S_n، روی Ω به‌طور $(n-2)$-متعدی عمل می‌کنند. اینها دومثال‌از گروههای‌جایگشتی‌اند که درجهٔ متعدی بودن آنها اصطلاحاً بالاست. هرگروه k-متعدی، $k \geqslant 2$، را یک گروه چندمتعدی می‌نامیم. گروههای S_n و A_n گروههای چندمتعدی بدیهی نامیده می‌شوند.

ای. ماتیو هنگامی‌که در سال ۱۸۶۰ مشغول مطالعهٔ گروههای جایگشتی چندمتعدی بود دو گروه ۵-متعدی روی ۱۲ حرف و ۲۴ حرف کشف کرد [۱۳، ۱۴ و ۱۵] و توانست جایگشتهایی بنویسد که دو گروه فوق‌الذکر را تولید کنند. بعدها این گروهها موردمطالعهٔ بیشتری قرار گرفتند و ای. ویت [۱۸] روش‌هماهنگی برای‌ساختن این گروهها ارائه‌کرد. او گروه ۵-متعدی روی ۱۲ حرف را با M_{12} و گروه ۵-متعدی روی ۲۴ حرف‌را با M_{24} حرف نشان‌داد. درطول بیش از صد سال، ریاضیدانان کوشش کردند گروههای ۵-متعدی دیگری بجز اینها کشف کنند ولی‌موفق نشدند. هنگامی‌که قضیهٔ رده‌بندی گروههای سادهٔ متناهی ثابت‌شد، ریاضیدانان به‌این نتیجه رسیدندکه این دو گروه ماتیو تنها گروههای ۵-متعدی غیربدیهی‌اند.

درعمل M_{12} روی ۱۲ حرف، پایدارساز یک‌حرف با M_{11} نمایش داده می‌شود و درعمل M_{24} روی ۲۴ حرف، پایدارساز i حرف، $2 \leqslant i \leqslant 1$، با M_{24-i} نمایش داده می‌شود. پنج گروه M_{11}، M_{12}، M_{22}، M_{23}، و M_{24} گروههای‌ماتیو نامیده‌می‌شوند. این گروهها هم درنظریهٔ گروههای ساده و هم درنظریهٔ کدگذاری بسیار با اهمیت هستند. هنگامی‌که کول [۲] مشغول تعیین همهٔ گروههای جایگشتی متعدی‌روی ۱۰ حرف و ۱۱ حرف بود موفق شد ثابت‌کند M_{11} گروهی ساده است. بعدها میلر [۱۶] ثابت‌کرد که چهار گروه دیگرماتیو نیز گروههایی ساده‌اند.

ویت به‌این‌ترتیب گروه M_{24} را ساخت‌که ابتدا مشاهده‌کرد پایدارساز ۳ حرف درعمل M_{24} روی ۲۴ حرف، گروه سادهٔ $PSL(3, 4)$ است که روی ۲۱ حرف باقیمانده به‌طور ۲-متعدی عمل می‌کند. او سپس شرایط کافی‌را برای‌اینکه یک‌گروه ۲-متعدی بتواند دارای توسیع متعدی باشد، ثابت‌کرد و نشان داد که این شرایط می‌توانند سه‌بار روی‌گروه $PSL(3, 4)$ اعمال شوند تا گروههای M_{22}، M_{23}، و M_{24} حاصل گردند. مشابه همین‌شیوه‌را می‌توان برای ساختن گروههای M_{11} و M_{12} نیز به‌کار گرفت.

در این مقاله رهیافت ویت را مناسب تشخیص داده‌ایم و جزئیات ساختن گروههای ماتیو را با استفاده از توسیع متعدی گروههای معلوم شرح خواهیم داد. همچنین ارتباط گروههای ماتیو را با سایر گروههای سادهٔ پراکنده و کادبرد آنها را درنظریهٔ طرحهای بلوکی و نظریه‌کدگذاری تشریح می‌کنیم.

۲. قضیهٔ ویت

قبل از بیان قضیهٔ ویت، تعریف زیر را در ارتباط با گروههای جایگشتی یادآوری می‌کنیم.

تعریف. فرض‌کنیم (G, Ω) یک‌گروه جایگشتی‌است. نیز فرض‌کنیم ∞ حرفی است که در Ω نیست و قرار دهیم $\bar{\Omega} = \Omega \cup \{\infty\}$. گوییم $(\bar{G}, \bar{\Omega})$ توسیع متعدی (G, Ω) است اگر $(\bar{G}, \bar{\Omega})$ متعدی باشد و $G_\infty = G$.

توجه داشته باشید که اگر (G, Ω) یک‌گروه‌جایگشتی k-متعدی باشد، آنگاه $(\bar{G}, \bar{\Omega})$ یک گروه جایگشتی $(k+1)$-متعدی خواهد بود.

قضیهٔ ۱. گیریم (G, Ω) یک‌گروه جایگشتی k-متعدی باشد $(k > 1)$. فرض‌کنیم $\infty \notin \Omega$ و h جایگشتی از مجموعهٔ $\bar{\Omega} = \Omega \cup \{\infty\}$ باشد به‌طوری‌که $\infty^h \in \Omega$. همچنین‌فرض کنیم $g \in G$ و $\omega \in \Omega$ با شرایط زیر وجود داشته باشند

الف) $g \notin G_\omega$

ب) $h^2 = (gh)^3 = 1$

پ) $hG_\omega h = G_\omega$

دراین صورت، گروه $\bar{G}$ وجود دارد به‌طوری‌که $(\bar{G}, \bar{\Omega})$ توسیع متعدی (G, Ω) است؛ و $(\bar{G}, \bar{\Omega})$ یک‌گروه‌جایگشتی $(k+1)$-متعدی است.

برهان. می‌توان عناصر گروه G را به‌عنوان‌جایگشتهایی‌از $\bar{\Omega}$ درنظر گرفت‌که ∞ را پایدار می‌سازند. چون $k > 1$ فرض شده‌است پس $(G|\Omega)$ حداقل ۲-متعدی است و درنتیجه تعداد همدسته‌های مضاعف G_ω در G برابر ۲ است. چون $g \notin G_\omega$ لذا می‌توان نوشت $G = G_\omega \cup G_\omega g G_\omega$. اگر نشان دهیم که $\bar{G} = G \cup GhG$ یک‌گروه است آنگاه به‌سادگی دیده‌می‌شود که $(\bar{G}, \bar{\Omega})$ یک توسیع متعدی (G, Ω) است.

$\bar{G}$ دارای عضوخنثای ۱ است وچون $h = h^{-1}$، لذا به‌ازای هر $y \in \bar{G}$ داریم $y^{-1} \in \bar{G}$. چون عناصر $\bar{G}$ جایگشتهایی از $\bar{\Omega}$ هستند، عمل ترکیب در $\bar{G}$ شرکتپذیر است. بنابراین کافی است

ثابت کنیم $\bar{G}$ تحت عمل ترکیب بسته‌است و برای این کار کافی‌است نشان دهیم $hGh \subseteq \bar{G}$ زیرا دراین‌صورت خواهیم داشت

$$GhG \cdot GhG = G(hGh)G \subseteq G\bar{G}G \subseteq \bar{G}.$$

حال از $(gh)^{۳} = ۱$ نتیجه می‌شود

$$hgh = (ghg)^{-۱} = g^{-۱}hg^{-۱}.$$

و با درنظر گرفتن $hG_{\infty}h = G_{\infty}$ حاصل می‌شود

$$hGh = h(G_{\infty} \cup G_{\infty}gG_{\infty})h = hG_{\infty}h \cup hG_{\infty}gG_{\infty}h$$
$$= G_{\infty} \cup hG_{\infty}hhghhG_{\infty}h$$
$$= G_{\infty} \cup G_{\infty}g^{-۱}hg^{-۱}G_{\infty} \subseteq G \cup GhG = \bar{G}$$

و به‌این‌ترتیب قضیه ثابت می‌شود.

۳. گروههای $PGL(n, q)$

فرض کنید $GF(q)$ هیأت گالوای q عضوی‌است، و $q = p^{l}$ توانی از عدد اول p است. فضای برداری n بعدی روی $GF(q)$ را با $V(n, q)$ نمایش می‌دهیم. مجموعهٔ تمام ماتریسهای وارونپذیر (تبدیلات خطی ناتکین) روی $GF(q)$ را با $GL(n, q)$ نشان‌داده **گروه خطی عام** می‌نامیم. مرکز این گروه Z عبارت است از مجموعهٔ تمام‌ماتریسهای‌اسکالر λI که در آن $\lambda \in GF(q)^{*}$. گروه $PGL(n, q) = \dfrac{GL(n, q)}{Z}$ را **گروه تصویری خطی عام** می‌نامیم.

مجموعهٔ تمام‌ماتریسهای‌وارونپذیر با دترمینان ۱ در $GL(n, q)$ تشکیل زیر گروهی می‌دهدکه آن را با $SL(n, q)$ نمایش‌می‌دهیم و**گروه خطی خاص** می‌نامیم. مرکز این گروه $Z \cap GL(n, q)$ عبارت است ازمجموعهٔ تمام ماتریسهای اسکالر λI، $\lambda \in GF(q)^{*}$ به‌طوری‌که $\lambda^{n} = ۱$، وبنابراین گروهی‌است ازمرتبهٔ $(n, q-۱)$. **گروه تصویری خطی خاص** عبارت است از $\dfrac{SL(n, q)}{Z \cap GL(n, q)}$ که آن‌را با $PSL(n, q)$ نمایش می‌دهیم. گروههای $PSL(n, q)$ ساده هستند مشروط بر اینکه $(n, q) \neq (۲, ۳)$ و $(۲, ۲)$. مرتبهٔ این‌گروهها عبارت است از

$$|PGL(n, q)| = q^{\binom{n}{۲}} \prod_{i=۲}^{n} (q^{i} - ۱)$$

$$|PSL(n, q)| = \frac{۱}{(n, q-۱)} q^{\binom{n}{۲}} \prod_{i=۲}^{n} (q^{i} - ۱)$$

گروههای تصویری فوق روی‌مجموعهٔ تمام زیرفضاهای‌ناصفر $V(n, q)$ عمل‌می‌کنند. مجموعهٔ تمام زیرفضاهای ناصفر $V(n, q)$ همراه با رابطهٔ شمول $\subseteq$ را **هندسهٔ تصویری** $(n-۱)$ **بعدی** می‌نامیم و با $\mathcal{P}(n-۱, q)$ نمایش‌می‌دهیم. تعداد زیرفضاهای یک‌بعدی $V(n, q)$ برابراست با $\dfrac{q^{n}-۱}{q-۱}$ و هرزیرفضای یک‌بعدی یک نقطه نامیده می‌شود. یک خط عبارت است از یک زیرفضای دوبعدی.

گروه $GL(n, q)$ (و همین‌طور گروه $SL(n, q)$) روی مجموعهٔ نقاط هندسهٔ تصویری عمل می‌کند و هستهٔ این‌عمل عبارت است از Z (یا $Z \cap GL(n, q)$ درمورد $SL(n, q)$). بنابراین گروههای $PGL(n, q)$ و $PSL(n, q)$ روی نقاط تصویری دارای‌اعمالی وفادار هستند. بنابه‌قضیهٔ اساسی‌هندسهٔ تصویری[۱] هرعضو $PGL(n, q)$ به‌وسیلهٔ یک ماتریس ناتکین القا می‌شود.

دراینجا حالتهای $n = ۲$ و $n = ۳$ را بیشترمورد بررسی قرارمی‌دهیم. ابتدا فرض می‌کنیم $n = ۲$. یک‌نقطهٔ تصویری در $\mathcal{P}(۱, q)$ را می‌توان به‌صورت $\langle \mathbf{v} \rangle = \{\lambda \mathbf{v} | \lambda \in GF(q)^{*}\}$ نوشت که در آن $\mathbf{v} \in V(۲, q)$ $\mathbf{v} \neq ۰$. اگر $\mathbf{v}$ بردار ناصفر دلخواهی در $V(۲, q)$ باشد آنگاه می‌توان $\mathbf{v}$ را نسبت به پایهٔ معینی مؤلفه‌دار کرد و نوشت $\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix}$، که در آن $a, b \in GF(q)$ و هردو باهم صفر نیستند. اگر $b \neq ۰$، آنگاه

$$\left\langle \begin{pmatrix} a \\ b \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} b^{-۱}a \\ ۱ \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} z \\ ۱ \end{pmatrix} \right\rangle = \begin{bmatrix} z \\ ۱ \end{bmatrix}, \quad z \in GF(q)$$

و اگر $b = ۰$، آنگاه

$$\left\langle \begin{pmatrix} a \\ ۰ \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \right\rangle = \begin{bmatrix} ۱ \\ ۰ \end{bmatrix}$$

پس $q+۱$ نقطهٔ تصویری عبارت‌اند از q نقطهٔ $\begin{bmatrix} z \\ ۱ \end{bmatrix}$ و یک‌نقطهٔ $\begin{bmatrix} ۱ \\ ۰ \end{bmatrix}$. حال حرفی مانند ∞ را کـه در $GF(q)$ نباشد در نظر می‌گیریم و قرارمی‌دهیم $L = GF(q) \cup \{\infty\}$. تناظری یک‌به‌یک بین $\mathcal{P}(۱, q)$ و L چنین برقرار می‌کنیم که به نقطهٔ $\begin{bmatrix} z \\ ۱ \end{bmatrix}$ عنصر z را نسبت می‌دهیم و به $\begin{bmatrix} ۱ \\ ۰ \end{bmatrix}$ عنصر ∞ را. اگر $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ماتریسی وارونپذیر و القاکنندهٔ عضوی از $PGL(۲, q)$ باشد، آنگاه عمل این ماتریس روی نقاط تصویری چنین است

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} z \\ ۱ \end{bmatrix} = \begin{bmatrix} az+b \\ cz+d \end{bmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} ۱ \\ ۰ \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}.$$

با توجه به‌تناظر بین $\mathcal{P}(۱, q)$ و L ملاحظه می‌شود که A به‌عنوان جایگشتی از L، عنصر $z \in GF(q)$ را به‌عنصر $\dfrac{az+b}{cz+d}$ وعنصر ∞ را به $\dfrac{a}{c}$ تبدیل می‌کند. بنابراین می‌توان نوشت

$$PGL(۲, q) = \left\{ x \to \frac{ax+b}{cx+d} \,\middle|\, ad-bc \neq ۰, \right.$$
$$\left. a, b, c, d \in GF(q) \right\}.$$

همین‌طور گروه $PSL(2,q)$ را می‌توان چنین نوشت

$$PSL(2,q)=\left\{x\to\frac{ax+b}{cx+d}\;\middle|\;ad-bc\in GF(q)^{\square},\ a,b,c,d\in GF(q)\right\}$$

که در آن $GF(q)^{\square}$ مجموعهٔ تمام عناصر ناصفر و مربع کامل در $GF(q)$ است.

درمورد $n=3$ یک نقطهٔ تصویری که به وسیلهٔ بردار $\begin{pmatrix}a\\b\\c\end{pmatrix}$ پدید می‌آید با $\begin{bmatrix}a\\b\\c\end{bmatrix}$ نمایش داده می‌شود. اگر $a=b=0$ آنگاه $\begin{bmatrix}0\\0\\c\end{bmatrix}=\begin{bmatrix}0\\0\\1\end{bmatrix}$ و اگر $a=0$ و $b\neq 0$ آنگاه $\begin{bmatrix}0\\b\\c\end{bmatrix}=\begin{bmatrix}0\\1\\b^{-1}c\end{bmatrix}$ که نقطه‌ای است به‌شکل $\begin{bmatrix}0\\1\\x\end{bmatrix}$، $x\in GF(q)$، و درنتیجه برای آن q انتخاب داریم. اگر $a\neq 0$ آنگاه $\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}1\\a^{-1}b\\a^{-1}c\end{bmatrix}$ که نقطه‌ای است به شکل $\begin{bmatrix}1\\x\\y\end{bmatrix}$، $x,y\in GF(q)$، که برای آن q^2 انتخاب داریم. درنتیجه، q^2+q+1 نقطهٔ تصویری همینهایی هستند که نوشتیم. درخاتمهٔ این بخش توضیح می‌دهیم که گروههای $PSL(n,q)$ و $PGL(n,q)$ روی نقاط تصویری به‌طور ۲-متعدی عمل می‌کنند.

۴. گروههای ماتیو

در این قسمت گروههای معینی را درنظر می‌گیریم و ثابت می‌کنیم دارای توسیع متعدی هستند. یعنی در واقع نشان می‌دهیم شرایط قضیهٔ ویت درمورد آنها برقرار است. گروههایی که از توسیع متعدی آنها حاصل می‌شوند در واقع همان گروههای ماتیو هستند. ابتدا گروه معینی را که M_{11} از توسیع متعدی آن به‌دست می‌آید شرح می‌دهیم.

فرض کنید $p>2$ عددی اول باشد و $f=2m$. هیأت گالوای $GF(q)$ با $q=p^f$ عنصر را درنظر می‌گیریم. داریم

$$|PGL(2,q)|=q(q^2-1)$$

$$|PSL(2,q)|=\frac{1}{2}q(q^2-1).$$

در این حالت $\varphi: x\to x^{p^m}$ یک خودریختی مرتبهٔ ۲ از $GF(q)$ است. با توجه به‌شکل عناصر گروه $PGL(2,q)$ که در بخش ۳ به‌آن اشاره کردیم، اگر قرار دهیم $\infty^{\varphi}=\infty$، آنگاه φ جایگشتی از L خواهد بود و در نتیجه $G=PGL(2,q)\langle\varphi\rangle$ یک گروه جایگشتی روی L است که برای آن داریم $PSL(2,q)\trianglelefteq G$. گروه $\frac{G}{PSL(2,q)}$ گروهی است مرتبهٔ ۴ و یکریخت است با $\mathbf{Z}_2\times\mathbf{Z}_2$. بنابراین G شامل ۳ زیرگروه با اندیس ۲ و شامل $PSL(2,q)$ است. دوتا از این زیرگروهها عبارت‌اند از $PGL(2,q)$ و $PSL(2,q)\langle\varphi\rangle$. گروه سوم را با $M(q)$ نمایش می‌دهیم. بنابراین $M(q)$ گروهی است شامل $PSL(2,q)$ و $[G:M(q)]=2$. از آنجا که $PSL(2,q)$ روی خط تصویری L دارای عملی ۲-متعدی است، پس $M(q)$ نیز روی L به‌طور ۲-متعدی عمل می‌کند. درواقع با توجه به‌شکل عناصر $M(q)$ می‌توان ثابت کرد که $M(q)$ روی L به‌طور ۳-متعدی عمل می‌کند. درساختن گروههای M_{11} و M_{12} گروه $M(9)$ مورد استفاده قرار می‌گیرد ($p=3$، $f=2$ و $q=9$) که در این حالت مناسب است قرار دهیم $M(9)=M_{10}$. هیأت $GF(9)$ از توسیع هیأت $\mathbf{Z}_3$ حاصل می‌گردد. چون چندجمله‌ای x^2+x-1 روی $\mathbf{Z}_3$ تحویل‌ناپذیر است می‌توان α را صفری از x^2+x-1 درنظر گرفت و قرارداد

$$GF(q)=\mathbf{Z}_3(\alpha)=\{a+b\alpha\,|\,a,b\in\mathbf{Z}_3\}$$

قضیهٔ ۲. گیریم G گروه ۳-متعدی M_{10} روی

$$L=GF(9)\cup\{\infty\}$$

باشد. نیز فرض کنیم ∞_1 و ∞_2 دوعنصر متمایز باشند به‌طوری که $\infty_1,\infty_2\notin L$. جایگشتهای h_1، h_2، و h_3 روی

$$\bar{L}=L\cup\{\infty_1,\infty_2\}$$

را درنظر می‌گیریم

$$h_1:\begin{cases}z\to z^{-1},\ z\in L\\ \infty_1\to\infty_1\\ \infty_2\to\infty_2\end{cases}$$

$$h_2:\begin{cases}\infty\to\infty_1\\ \infty_1\to\infty\\ \infty_2\to\infty_2\\ a+\alpha b\to a-\alpha b,\ a,b\in\mathbf{Z}_3\end{cases}$$

$$h_3:\begin{cases}\infty\to\infty\\ \infty_1\to\infty_2\\ \infty_2\to\infty_1\\ z\to z^2,\ z\in GF(9)\end{cases}$$

در این‌صورت، $M_{11}'=\langle M_{10},h_2\rangle$ یک گروه ۴-متعدی درجهٔ ۱۱ روی $L=L\cup\{\infty_1\}$ و $M_{12}=\langle M_{11},h_3\rangle$ یک گروه ۵-متعدی درجهٔ ۱۲ روی $\bar{L}$ است.

برهان. ثابت می‌کنیم شرایط قضیهٔ ویت برقرار است. قرار

می‌دهیم $\Omega = L = GF(9) \cup \{\infty\}$ و $\bar{\Omega} = \Omega \cup \{\infty_1\}$ و $G = M_{10}$ و $\bar{G} = \langle M_{10}, h_2 \rangle$. واضح است که h_2 جایگشتی از $\bar{\Omega}$ است که برای آن داریم $\infty_1^{h_2} = \infty \in \Omega$. اما دترمینان h_1 برابر است با -1 که در هیأت $GF(9)$ مربع کامل است و در نتیجه $h_1 \in G$. حال تجزیه‌های دوری h_1، h_2 و h_1h_2 روی $\bar{\Omega}$ چنین‌اند

$$h_1 = (\infty_1)(1)(-1)(0\ \infty)(\alpha\ \alpha+1)(-\alpha\ -\alpha-1)(\alpha-1\ -\alpha+1)$$

$$h_2 = (0)(1)(-1)(\infty\ \infty_1)(\alpha\ -\alpha)(\alpha+1\ -\alpha+1)(\alpha-1\ -\alpha-1)$$

$$h_1h_2 = (1)(-1)(0\ \infty_1\ \infty)(\alpha\ -\alpha+1\ -\alpha-1)(-\alpha\ \alpha-1\ \alpha+1)$$

بنابراین دیده می‌شود که $h_2^2 = (h_1h_2)^3 = 1$. چون $\infty^{h_1} = 0$ پس $h_1 \notin G_\infty$. ازطرف دیگر داریم

$$\infty^{h_2 G_\infty h_2} = (\infty^{h_2})^{G_\infty h_2} = \infty_1^{G_\infty h_2} = \infty_1^{h_2} = \infty.$$

بنابراین $h_2 G_\infty h_2 = G_\infty$. به‌این‌ترتیب تمام شرایط قضیهٔ ویت برقرار است و درنتیجه $(\bar{G}, \bar{\Omega})$ توسیع متعدی (G, Ω) است. چون (G, Ω) به‌طور ۳-متعدی عمل می‌کند لذا $(\bar{G}|\bar{\Omega})$، ۴-متعدی است و باتوجه به‌مرتبهٔ G داریم: $|\bar{G}| = 7920 = |M_{11}|$. گروه ۴-متعدی $\bar{G}$ را M_{11} می‌نامیم.

برای ساختن گروه M_{12} گروه‌جایگشتی ۴-متعدی $(\bar{G}, \bar{\Omega})$ را درنظرمی‌گیریم و ثابت‌می‌کنیم شرایط قضیهٔ ویت درمورد توسیع متعدی‌این گروه‌برقراراست. باتوجه به‌قراردادهای‌فوق‌قرارمی‌دهیم $\bar{\Omega} = \bar{\Omega} \cup \{\infty_2\}$ و $\bar{G} = \langle G, h_2 \rangle$. تجزیهٔ دوری عناصر h_2 و h_1h_2 به‌عنوان جایگشتهایی از $\bar{\Omega}$ چنین است

$$h_2 = (\infty)(0)(1)(-1)(\infty_1\ \infty_2)(\alpha\ -\alpha-1)(-\alpha\ \alpha+1)(\alpha-1\ -\alpha+1)$$

$$h_1h_2 = (0)(1)(-1)(\infty\ \infty_2\ \infty_1)(\alpha\ \alpha+1\ \alpha-1)(-\alpha\ -\alpha-1\ -\alpha+1).$$

داریم $h_2 \in \bar{G}$ و $\infty_2^{h_2} = \infty_1 \in \bar{\Omega}$ و $h_2^2 = (h_1h_2)^3 = 1$.

چون $\infty_1^{h_2} = \infty$ پس $h_2 \notin \bar{G}_{\infty_1}$. همچنین

$$\infty_1^{h_2 \bar{G}_{\infty_1} h_2} = (\infty_1^{h_2})^{\bar{G}_{\infty_1} h_2} = \infty_2^{\bar{G}_{\infty_1} h_2} = \infty_2^{G_\infty h_2}$$
$$= \infty_2^{h_2} = \infty_1.$$

درنتیجه $h_2 \bar{G}_{\infty_1} h_2 = \bar{G}_{\infty_1}$ و لذا تمام شرایط قضیهٔ ویت برقرار است. بنابراین گروه جایگشتی $(\bar{G}, \bar{\Omega})$ وجود دارد به‌طوری‌که توسیع‌متعدی $(\bar{G}, \bar{\Omega})$ باشد. گروه ۵-متعدی $\bar{G}$ را M_{12} می‌نامیم. مرتبهٔ این گروه برابر است با

$$|M_{12}| = 12 \times |M_{11}| = 95040.$$

حال‌که چگونگی ساختن گروههای M_{11} و M_{12} را با استفاده ازقضیهٔ ویت دیدیم، طرز ساختن دیگر گروههای ماتیو یعنی M_{22}، M_{23} و M_{24} را شرح می‌دهیم؛ شیوهٔ ساختن گروههای اخیر را نیز با استفاده ازقضیهٔ ویت بیان می‌کنیم. گروهی که با آن شروع کرده و M_{22} را می‌سازیم عبارت است ازگروه خطی $PSL(3, 4)$ از مرتبهٔ ۲۵۱۶۰. می‌دانیم‌که این‌گروه روی ۲۱ نقطهٔ تصویری‌در $\mathcal{P}(2, 4)$ به‌طور ۲-متعدی عمل‌می‌کند. همان‌طور که قبلا توضیح دادیم نقطهٔ تصویری را که به‌وسیلهٔ بردار $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ پدید می‌آید با $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$ نمایش‌می‌دهیم. چون چندجمله‌ای x^2+x+1 روی Z_2 تحویل‌ناپذیر است لذا می‌توان α را صفری از این چندجمله‌ای فرض‌کرد و قرارداد $GF(4) = Z_2(\alpha)$.

قضیهٔ ۳. فرض می‌کنیم $G = PSL(3, 4)$ و Ω مجموعهٔ ۲۱ نقطهٔ تصویری در $\mathcal{P}(2, 4)$ باشد. قرارمی‌دهیم

$$\bar{\Omega} = \Omega \cup \{\infty_1, \infty_2, \infty_3\}$$

که ∞_1، ∞_2 و ∞_3 سه حرف متمایز در خارج Ω اند، و جایگشتهای زیردوی $\bar{\Omega}$ را درنظرمی‌گیریم

$$h_1 : \begin{cases} \infty_1 \to \infty_1 \\ \infty_2 \to \infty_2 \\ \infty_3 \to \infty_3 \\ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \to \begin{bmatrix} y \\ x \\ z \end{bmatrix} \end{cases}$$

$$h_2 : \begin{cases} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \to \infty_1 \\ \infty_1 \to \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \\ \infty_2 \to \infty_2 \\ \infty_3 \to \infty_3 \\ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \to \begin{bmatrix} x^2+yz \\ y^2 \\ z^2 \end{bmatrix}, \quad \begin{bmatrix} x \\ y \\ z \end{bmatrix} \neq \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \end{cases}$$

$$h_2:\begin{cases}\infty_1 \to \infty_2\\ \infty_2 \to \infty_1\\ \infty_3 \to \infty_3\\ \begin{bmatrix}x\\y\\z\end{bmatrix} \to \begin{bmatrix}x^2\\y^2\\\alpha z^2\end{bmatrix}\end{cases}$$

$$h_4:\begin{cases}\infty_1 \to \infty_1\\ \infty_2 \to \infty_3\\ \infty_3 \to \infty_2\\ \begin{bmatrix}x\\y\\z\end{bmatrix} \to \begin{bmatrix}x^2\\y^2\\z^2\end{bmatrix}\end{cases}$$

دراین‌صورت

الف) $M_{22}=\langle G, h_2\rangle$ یك‌گروه ۳-متعدی روی ۲۲ حرف $\bar{\Omega}=\Omega\cup\{\infty_1\}$ است و $|M_{22}|=443520$.

ب) $M_{23}=\langle M_{22}, h_3\rangle$ یك گروه ۲-متعدی روی ۲۳ حرف $\bar{\bar{\Omega}}=\Omega\cup\{\infty_1,\infty_2\}$ است و $|M_{23}|=10200960$.

پ) $M_{24}=\langle M_{23}, h_4\rangle$ یك گروه ۵-متعدی روی ۲۴ حرف $\bar{\bar{\bar{\Omega}}}$ است و

$$|M_{24}|=244823040.$$

برهان. ابتدا مرتبهٔ جایگشتهای h_i، $1\leqslant i\leqslant 4$، را پیدا می‌کنیم. واضح است که مرتبهٔ h_1 برابر ۲ است. با توجه به‌تعریف h_2 دیده می‌شود که h_2^2، عناصر $\begin{bmatrix}1\\0\\0\end{bmatrix}$، ∞_1، ∞_2 و ∞_3 را به خودشان تبدیل می‌کند و $\begin{bmatrix}x\\y\\z\end{bmatrix}$ را به $\begin{bmatrix}x^4\\y^4\\z^4\end{bmatrix}$ مبدل می‌سازد. چون به‌ازای هر $x\in GF(4)$ داریم $x^4=x$ لذامرتبهٔ h_2 نیز ۲ است. همین‌طور، مرتبهٔ h_4 برابر ۲ می‌باشد. اما جایگشت h_2^2، عناصر ∞_1، ∞_2 و ∞_3 را پایدار می‌سازد و $\begin{bmatrix}x\\y\\z\end{bmatrix}$ را به $\begin{bmatrix}x^4\\y^4\\\alpha^3 z^4\end{bmatrix}$ تبدیل می‌کند که چون $\alpha^3=1$، نتیجه‌می‌شود که مرتبهٔ h_2، دو است. پس ثابت کرده‌ایم $h_i^2=1$، $1\leqslant i\leqslant 4$. عملیات مشابهی نشان می‌دهد که $(h_1h_2)^3=(h_2h_4)^3=(h_1h_4)^3=1$. حال به بررسی شرایط قضیهٔ ویت درهرمورد می‌پردازیم.

الف) قرار می‌دهیم $G=PSL(3,4)$، $\bar{\Omega}=\Omega\cup\{\infty_1\}$ و $\bar{G}=\langle G, h_2\rangle$. h_2 جایگشتی از $\bar{\Omega}$ است و داریم

$$\infty_1^{h_2}=\begin{bmatrix}1\\0\\0\end{bmatrix}\in\Omega.$$

h_1 جایگشتی روی Ω است و به‌وسیلهٔ ماتریس $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$ القا می‌شود که ماتریسی است با درایه‌های در $GF(4)$ و دترمینان ۱ پس $h_1\in G$. چون $\begin{bmatrix}1\\0\\0\end{bmatrix}^{h_1}=\begin{bmatrix}0\\1\\0\end{bmatrix}$ پس $h_1\notin G_{\begin{bmatrix}1\\0\\0\end{bmatrix}}$. حال از

$$\begin{bmatrix}1\\0\\0\end{bmatrix}^{h_1 G_{\begin{bmatrix}1\\0\\0\end{bmatrix}} h_2}=\infty_1^{G_{\begin{bmatrix}1\\0\\0\end{bmatrix}} h_2}=\infty_1^{h_2}=\begin{bmatrix}1\\0\\0\end{bmatrix}$$

نتیجه می‌شود $h_2 G_{\begin{bmatrix}1\\0\\0\end{bmatrix}} h_2=G_{\begin{bmatrix}1\\0\\0\end{bmatrix}}$. و چون داریم

$$h_2^2=(h_1h_2)^3=1$$

پس تمام شرایط قضیهٔ ویت برقرار است و درنتیجه $\bar{G}$ یك‌توسیع متعدی G است. یعنی $\bar{G}$ یك‌گروه ۳-متعدی روی ۲۲ حرف است و $|\bar{G}|=22\times|PSL(3,4)|=443520$. گروه ۳-متعدی $\bar{G}$ را M_{22} می‌نامیم.

ب) قرارمی‌دهیم $\bar{\bar{G}}=\langle \bar{G}, h_3\rangle$ و $\bar{\bar{\Omega}}=\bar{\Omega}\cup\{\infty_2\}$. در این حالت h_3 جایگشتی از $\bar{\bar{\Omega}}$ است و $\infty_1^{h_3}=\infty_1\in\bar{\Omega}$. چون $h_3\in\bar{G}$ و $\begin{bmatrix}1\\0\\0\end{bmatrix}^{h_3}=\infty_1$ پس $h_3\notin\bar{G}_{\infty_1}$. روابط

$$h_3^2=(h_2h_3)^3=1$$

و $h_4\bar{G}_{\infty_1}h_4=\bar{G}_{\infty_1}$ نیز برقرارند و درنتیجه تمام شرایط قضیهٔ ویت صادق است. پس $\bar{\bar{G}}$ گروهی ۴-متعدی روی ۲۳ حرف است که M_{23} نامیده می‌شود و داریم

$$|M_{23}|=23\times|M_{22}|=10200960.$$

پ) قرار می‌دهیم $\bar{\bar{\bar{G}}}=\langle\bar{\bar{G}},h_4\rangle$ و $\bar{\bar{\bar{\Omega}}}=\bar{\bar{\Omega}}\cup\{\infty_3\}$. h_4 جایگشتی از $\bar{\bar{\bar{\Omega}}}$ است و $\infty_1^{h_4}=\infty_3\in\bar{\bar{\Omega}}$. چون $h_4\in\bar{\bar{G}}$ و $h_2\notin\bar{\bar{G}}_{\infty_3}$ لذا $\infty_2^{h_4}=\infty_1$. چون روابط $h_4^2=(h_3h_4)^3=1$ و $h_4\bar{\bar{G}}_{\infty_3}h_4=\bar{\bar{G}}_{\infty_3}$ برقرارند پس تمام شرایط قضیهٔ ویت صادق است. درنتیجه $\bar{\bar{\bar{G}}}$ گروهی ۵-متعدی روی $\bar{\bar{\bar{\Omega}}}$ است که M_{24} نامیده می‌شود و

$$|M_{24}|=24\times|M_{23}|=244823040.$$

به‌این‌ترتیب ساختن ۵ گروه ماتیو تکمیل می‌شود. چون این گروهها از توسیع متعدی گروههای معینی حاصل می‌شوند می‌توان پرسید که آیا M_{12} و M_{24} دارای توسیع متعدی هستند؟ جواب این سؤال منفی است. یعنی نمی‌توان گروههای M_{12} و M_{24} را

به‌طور متعدی توسعه داد و از آنها گروههای دیگری به‌دست‌آورد. پنج گروه ماتیو ساده هستند یعنی دارای زیر گروه نرمال غیر بدیهی نمی‌باشند. این دوقضیه را بدون اثبات در زیر می‌آوریم

قضیهٔ ۴. گروههای ۵-متعدی M_{12} و M_{24} دارای توسیع متعدی نیستند.

قضیهٔ ۵. گروههای M_{11}، M_{12}، M_{22}، M_{23} و M_{24} ساده هستند.

۵. دستگاههای اشتاینر

برخی از گروههای سادهٔ پراکنده با استفاده از ویژگیهای ترکیبیاتی گروههای ماتیو ساخته شده‌اند. در این بخش به تشریح این ویژگیها می‌پردازیم. فرض کنید Ω مجموعه‌ای است متناهی با $|\Omega|=v$ عضو و $\mathcal{B}$ مجموعه‌ای از زیرمجموعه‌های k عضوی Ω است. عناصر Ω را نقطه و عناصر $\mathcal{B}$ را بلوک می‌نامیم. زوج $(\Omega, \mathcal{B})$ یک t-(v,k,λ) طرح نامیده می‌شود اگر هر t نقطه در دقیقاً λ بلوک ظاهر شود. درحالتی که $\lambda=1$، $(\Omega, \mathcal{B})$ یک دستگاه اشتاینر نامیده می‌شود و آن را $S(t,k,v)$ نمایش می‌دهیم. دستگاههای اشتاینر برای اولین بار به‌وسیلهٔ وول‌هاوس [۱۹] مطرح شدند. او این سؤال را طرح کرد: به‌ازای چه‌مقادیری از پارامترهای t، v و k دستگاه اشتاینر $S(t,k,v)$ وجود دارد؟ اولین جواب به‌سؤال فوق توسط کرکمن ارائه شد [۱۰]. او دستگاه اشتاینر $S(3,4,2^n)$ را ساخت و نشان داد که $S(2,3,v)$ وجود دارد اگر و فقط اگر $v\equiv 1$ یا $3 \pmod 6$. به‌ازای $t\leqslant 3$ خانواده‌های نامتناهی از دستگاههای اشتاینر وجود دارد درصورتی‌که به‌ازای $t\geqslant 4$ برای مدتهای مدیدی فقط تعداد متناهی دستگاه اشتاینر شناخته‌شده بوده. این دستگاههای اشتاینر که به‌طرحهای ویت نیز معروفند عبارت‌اند از $S(4,5,11)$، $S(5,6,12)$، $S(4,7,23)$ و $S(5,8,24)$ که با گروههای ماتیو ارتباط نزدیک دارند. اخیراً دستگاههای اشتاینر دیگری به‌ازای $t\geqslant 4$ پیدا شده‌اند که از ذکر آنها خودداری می‌کنیم.

در بخش قبل طرز ساختن گروههای ماتیو را شرح دادیم و در این بخش شرح خواهیم‌داد که چگونه طرحهای فوق با استفاده از گروههای ماتیو به‌دست می‌آیند. ابتدا گروه خودریختی‌های یک t-(v,k,λ) طرح را شرح می‌دهیم. فرض کنید $D=(\Omega, \mathcal{B})$ یک t-(v,k,λ) طرح است. یک خودریختی از D عبارت‌است از جایگشتی مانند π از Ω به‌طوری که به‌ازای هر $B\in\mathcal{B}$ داشته باشیم $B^\pi\in\mathcal{B}$. مجموعهٔ تمام خودریختی‌های D تشکیل یک گروه می‌دهد که آن را گروه خودریختی‌های D نامیده و آن را با $\mathrm{Aut}\,D$ نمایش می‌دهیم. هر زیر گروه $\mathrm{Aut}\,D$ را یک گروه خودریختی‌های D می‌نامیم. به‌این ترتیب گروههای خودریختی‌های D، که جایگشتهایی از Ω هستند، روی مجموعهٔ $\mathcal{B}$ یک گروه جایگشتی القا می‌کنند. ارتباط گروه خودریختی‌های D با خود D از قضیهٔ زیر که دارای اثباتی ساده است مشهود است.

قضیهٔ ۶. فرض کنید (G,Ω) یک گروه جایگشتی t-همگن است و $|\Omega|=v$، $v\geqslant t$ و $B\subseteq\Omega$ و $k=|B|\geqslant t$. آنگاه $D=(\Omega, B^G)$ یک t-(v,k,λ) طرح است که λ عبارت است از

$$\lambda=|G|\binom{k}{t}/|G_B|\binom{v}{t}.$$

درقضیهٔ فوق G_B پایدار ساز مجموعهٔ B است. مجموعهٔ B را یک بلوک پایه می‌نامیم. واضح است که در این حالت داریم $G\leqslant \mathrm{Aut}\,D$، یعنی G یک گروه خودریختی‌های D است.

حال مفهوم توسیع یک طرح را شرح می‌دهیم. طبق معمول فرض می‌کنیم $D=(\Omega, \mathcal{B})$ یک t-(v,k,λ) طرح است. همچنین فرض می‌کنیم $\omega\in\Omega$ نقطهٔ ثابتی است. نقطهٔ ω را از Ω و تمام بلوکهای $\mathcal{B}$ که ω را دربردارند حذف می‌کنیم و قرار می‌دهیم $\Omega'=\Omega-\{\omega\}$ و $\mathcal{B}'=\{B-\{\omega\}\mid B\in\mathcal{B}, \omega\in B\}$. در این حالت واضح است که $D_\omega=(\Omega', \mathcal{B}')$ یک

$$(t-1)\text{-}(v-1,k-1,\lambda)$$

طرح است که آن‌را طرح مشتق‌شده در ω می‌نامیم. D یک توسیع طرح D_ω نامیده می‌شود. قضیهٔ زیر منسوب به‌هیوز [۸] است که بیان کنندهٔ ارتباطی است بین توسیع طرحها و توسیع گروهها.

قضیهٔ ۷. فرض کنید $D=(\Omega, \mathcal{B})$ یک t-(v,k,λ) طرح است و $G\leqslant \mathrm{Aut}\,D$. همچنین فرض کنید (G,Ω) یک گروه جایگشتی t-متعدی و $(G,\mathcal{B})$ یک گروه جایگشتی متعدی است. به‌علاوه قرار می‌دهیم $\bar\Omega=\Omega\cup\{\infty\}$ و فرض می‌کنیم $(\bar G, \bar\Omega)$ یک توسیع متعدی (G,Ω) است. به‌ازای بلوک ثابت $B\in\mathcal{B}$ قرار می‌دهیم $\bar B=B\cup\{\infty\}$ و $\bar{\mathcal{B}}=B^{\bar G}$. آنگاه $(\bar\Omega, \bar{\mathcal{B}})$ یک

$$(t+1)\text{-}(v+1,k+1,\bar\lambda)$$

طرح است که در آن

$$\bar\lambda=\frac{\lambda(k+1)|G_B|}{|\bar G_{\bar B}|}.$$

به‌علاوه طرح $(\bar\Omega, \bar{\mathcal{B}})$ یک توسیع طرح $(\Omega, \mathcal{B})$ است اگر و فقط اگر $\bar\lambda=\lambda$ و این درحالتی که $\bar G_{\bar B}$ روی $\bar B$ به‌طور متعدی عمل کند برقرار است.

حال گروه M_{10} را که در بخش ۴ از آن صحبت شد در نظر می‌گیریم. می‌توان ثابت کرد که عناصر این گروه عبارت‌اند از تبدیلات $x\to\dfrac{ax+b}{cx+d}$، $ad-bc\in GF(9)^\square$، و

$$x\to\frac{ax^3+b}{cx^3+d}$$

a، b، c و d عناصری از $GF(9)$ هستند. قبلا توضیح دادیم که M_{10} روی خط تصویری $\Omega=GF(9)\cup\{\infty\}$ به‌طور ۳-متعدی عمل می‌کند و $|M_{10}|=720$. عمل M_{10} روی زیر مجموعه‌های ۲ عضوی Ω را درنظر گرفته و $B=\{\infty, 0, 1, -1\}$ را به‌عنوان بلوک پایه انتخاب می‌کنیم. بنابه‌قضیهٔ ۶ زوج $(\Omega, B^{M_{10}})$ یک 3-$(10,4,\lambda)$ طرح است. از آنجایی که شکل عناصر M_{10} مشخص است، می‌توان پایدارساز B یعنی $M_{10(B)}$ را پیدا کرد. ما جزئیات محاسبه را نمی‌نویسیم ولی توضیح می‌دهیم که $|M_{10(B)}|=24$

و گروه $M_{10(B)}$ وقتی که روی B عمل می‌کند همریخت است با S_3. بنابه‌قضیهٔ ۶ داریم

$$\lambda=\frac{|M_{10}|\binom{4}{3}}{|M_{10(B)}|\binom{10}{3}}=10$$

بنابراین $(\Omega, B^{M_{10}})$ یك $(10,4,1)$-۳ طرح است و به‌عبارت دیگر یك دستگاه اشتاینر $S(3,4,10)$ است.

بنابه‌قضیهٔ ۲ می‌دانیم $M_{11}=\langle M_{10}, h_2\rangle$ و اگر قراردهیم $\bar{\Omega}=\Omega\cup\{\infty_1\}$، آنگاه $(M_{11}, \bar{\Omega})$ یك توسیع متعدی (M_{10}, Ω) است. بنابراین اگر قراردهیم $\bar{B}=B\cup\{\infty_1\}$ آنگاه بنابه‌قضیهٔ ۷، زوج $(\bar{\Omega}, B^{M_{11}})$ یك $(11,5,\bar{\lambda})$-۴ طرح است، اما گروه $M_{11(\bar{B})}$ گروه $M_{10(B)}$ را دربردارد و لذا $M_{11(\bar{B})}$ هردونقطهٔ دلخواه B را به یکدیگر تبدیل می‌کند. با توجه به‌ساختمان گروه M_{11} درقضیهٔ ۲ دیده‌می‌شود که $h_2\in M_{11(\bar{B})}$. اما $\infty^{h_2}=\infty_1$ و در نتیجه $M_{11(\bar{B})}$ روی $\bar{B}$ به‌طور متعدی عمل می‌کند. بنابه‌قضیهٔ ۷ باید داشته‌باشیم $\bar{\lambda}=\lambda=1$ و درنتیجه $(\bar{\Omega}, B^{M_{11}})$ یك توسیع طرح $(\Omega, B^{M_{10}})$ است. به‌این‌ترتیب $(\bar{\Omega}, B^{M_{11}})$ یك دستگاه اشتاینر $S(4,5,11)$ است. به‌همین‌روش، دستگاه اشتاینر فوق‌را درنظر می‌گیریم و با توجه به اینکه M_{12} یك توسیع متعدی M_{11} است با استفاده از قضیهٔ ۷ دستگاه اشتاینر $S(5,6,12)$ را می‌سازیم که در اینجا از ذکر جزئیات آن خودداری می‌کنیم.

حال گروه $M_{21}=PSL(3,4)$ را درنظر بگیرید. این گروه روی ۲۱ نقطهٔ تصویری به‌طور ۲-متعدی عمل می‌کند. اگر B یك خط تصویری باشد آنگاه $|B|=5$ و بنابه‌قضیهٔ ۶، زوج $(\Omega, B^{M_{21}})$ یك $(21,5,1)$-۲ طرح است. علت $\lambda=1$ این است که هردونقطهٔ تصویری روی یك خط تصویری یکتا هستند. به‌این ترتیب دستگاه اشتاینر $S(2,5,21)$ را داریم که گروه خودریختی‌های آن M_{21} است. بنابه‌قضیهٔ ۳ گروه M_{21} را می‌توان به گروه M_{22} توسعه داد و لذا اگر قرار دهیم $\bar{B}=B\cup\{\infty_1\}$ آنگاه $(\bar{\Omega}, \bar{B}^{M_{22}})$ یك $(22,6,\bar{\lambda})$-۳طرح است که می‌توان نشان‌داد $\bar{\lambda}=1$. بنابراین دستگاه‌اشتاینر $S(3,6,22)$ حاصل می‌شود که توسیع $S(2,5,21)$ است. مشابهاً دستگاه اشتاینر $S(3,6,22)$ قابل توسیع به $S(4,7,23)$ و دستگاه اخیر قابل توسیع به $S(5,8,24)$ است.

در واقع دستگاههای اشتاینر فوق یکتا هستند و می‌توان گروه خودریختی‌های آنها را به‌عنوان تعریف گروههای ماتیو درنظر گرفت. داریم

$$\mathrm{Aut}\,S(4,5,11)=M_{11}$$
$$\mathrm{Aut}\,S(5,6,12)=M_{12}$$
$$\mathrm{Aut}\,S(3,6,22)=M_{22}$$
$$\mathrm{Aut}\,S(4,7,23)=M_{23}$$
$$\mathrm{Aut}\,S(5,8,24)=M_{24}.$$

در بالا M_{22} گروه خودریختی‌های M_{22} است و

$$[M_{22}:M_{22}]=2.$$

از دیگرویژگیهای ترکیبیاتی گروههای ماتیو ارتباط آنها با نظریهٔ جبری کدگذاری است. کد خارق‌العادهٔ $(11,23)$ و توسیع آن $(12,24)$ که به‌کدهای گولای معروف‌اند با گروههاتیوی M_{24} ارتباط دارند. همچنین کد $(5,11)$ و توسیع آن $(6,12)$ با گروه M_{12} مرتبط‌اند. در اینجا کد $(12,24)$ را شرح می‌دهیم و از رهیافتی که در [۳] آمده است استفاده می‌کنیم. یك کد عبارت است از زیرمجموعه‌ای مانند C ازفضای برداری $V(n,q)$. اگر C زیرفضایی از $V(n,q)$ باشدآن‌را یك کد خطی می‌نامیم. هیأت گالوای $GF(23)$ را درنظر می‌گیریم و قرارمی‌دهیم

$$\Omega=GF(23)\cup\{\infty\}, Q=\{x^2\mid x\in GF(23)\}, N=\Omega\backslash Q.$$

$\mathcal{P}(\Omega)$، مجموعهٔ تمام زیرمجموعه‌های Ω، با جمع متقارن، یك گروه آبلی است که به طور معمول دارای ساختار یك فضای برداری روی $GF(2)$ است. بنابراین $\mathcal{P}(\Omega)$ یك‌فضای برداری با بعد ۲۴ روی $GF(2)$ می‌باشد. واضح است که M_{24} روی $\mathcal{P}(\Omega)$ عمل می‌کند. کانوی‌در [۳] نشان‌داده‌است که درعمل M_{24} روی $\mathcal{P}(\Omega)$، یك‌زیرفضای ۱۲ بعدی $\mathcal{C}$ ناورداست که همان کد دوتایی گولای است. این کد به‌وسیلهٔ ۲۴ مجموعهٔ N_i، $i\in\Omega$، تولید می‌شود

$$N_i=N-i=\{n-i\mid n\in N\},\quad N_\infty=\Omega$$

عناصر $\mathcal{C}$ که آنها را $\mathcal{C}$-مجموعه می‌نامیم عبارت‌اند از ۷۵۹ زیرمجموعهٔ ۸عضوی Ω که اکتاد نامیده می‌شوند، ۷۵۹ زیرمجموعهٔ ۱۶ عضوی Ω که مکمل اکتادها هستند، ۲۵۷۶ زیر مجموعهٔ ۱۲عضوی Ω بنام دودکاد، مجموعهٔ ϕ، ومجموعهٔ Ω. درواقع ۷۵۹ اکتاد $\mathcal{C}$ تشکیل دستگاه اشتاینر $S(5,8,24)$ را می‌دهند.

۶. ارتباط گروههای ماتیو با سایرگروههای پراکنده

گروههای متناوب A_n، $n\geq 5$، همگی ساده هستند. می‌گوییم که گروههای سادهٔ A_n، $n\geq 5$، تشکیل یك خانوادهٔ نامتناهی از گروههای سادهٔ متناهی می‌دهند. گروه ساده‌ای که عضو هیچ خانوادهٔ نامتناهی از گروههای سادهٔ متناهی نباشد **گروه سادهٔ پراکنده** نامیده می‌شود. گروههای سادهٔ ماتیو پراکنده‌اند و قریب به یك قرن تنها گروههای سادهٔ پراکندهٔ شناخته شده بودند. دراهمیت این گروهها همین‌بس که بگوییم اولین گروه سادهٔ پراکنده، بجز گروههای‌ماتیو، با استفاده از تشابه ساختار داخلی گروه ماتیوی M_{12} ساخته شد. امروزه ثابت شده است که تنها ۲۶ گروه سادهٔ پراکنده وجود دارد [۵]. در این بخش برخی گروههای ساده را که مستقیماً با گروههای ماتیو ارتباط دارند ذکر می‌کنیم.

در گروه‌ماتیوی M_{12} یك‌عضو مرتبهٔ دووجود داردبه‌طوری که مرکزساز آن، گروهی است یکریخت با S_3. (Q_8*Q_8)، که در اینجا Q_8 گروه کواترنیون مرتبهٔ ۸، و $*$ و . به‌ترتیب حاصلضربهای مرکزی و نیم‌مستقیم دوگروه است. یانکو این‌سؤال را مطرح کرد که آیا یك گروه سادهٔ متناهی‌وجود دارد به‌طوری که مرکزساز یك عضو مرتبهٔ ۲ی آن مشابه مرکزساز عضوی مرتبهٔ ۲ در گروه ماتیو باشد؟ به‌زبان دقیق، او به‌عنوان مرکزساز عضومرتبهٔ

۲، گروهی به‌شکل $\mathbf{A}_5 . (Q_8 * Q_8)$ را انتخاب کرد و قضیهٔ زیر را ثابت نمود.

قضیهٔ ۸ [۹]. اگر G گروهی ساده باشد و مرکزساز عضوی مرتبهٔ ۲ در G یکریخت باشد با گروه $\mathbf{A}_5 . (Q_8 * Q_8)$، آنگاه

الف) G دارای ۲ کلاس تزویج اعضای مرتبهٔ ۲ است و $|G| = ۲^۷ . ۳^۳ . ۵^۲ . ۷$.

ب) G دارای یک کلاس تزویج اعضای مرتبهٔ ۲ است و $|G| = ۲^۷ . ۳^۵ . ۵ . ۱۷ . ۱۹$.

بعداً هلد با در نظر گرفتن مشابه عضوی مرتبهٔ ۲ در گروه $M_{۲۴}$ قضیهٔ زیر را ثابت کرد.

قضیهٔ ۹ [۶]. اگر G گروهی ساده و متناهی باشد و مرکزساز عضوی مرتبهٔ ۲ در آن یکریخت باشد با گروه

$$(D_8 * D_8 * D_8) . GL(۳, ۲)$$

آنگاه

الف) G یکریخت است با $M_{۲۴}$ یا $GL(۵, ۲)$.

ب) G دارای دو کلاس تزویج اعضای مرتبهٔ ۲ است و $|G| = ۲^{۱۰} . ۳^۳ . ۵^۲ . ۷^۳ . ۱۷$.

می‌دانیم گروه ماتیوی $M_{۲۴}$ روی نقاط و بلوکهای دستگاه اشتاینر $S(۳, ۶, ۲۲)$ به‌طور متعدی عمل می‌کند. اگر مجموعهٔ نقاط را Ω و مجموعهٔ بلوکها را $\mathcal{B}$ فرض کنیم آنگاه $|\Omega| = ۲۲$ و $|\mathcal{B}| = ۷۷$. به‌این ترتیب $M_{۲۴}$ روی مجموعهٔ $\Omega \cup \mathcal{B}$ دارای عمل غیرمتعدی است. هیگمن و سیمز [۷] ثابت کردند $M_{۲۴}$، در عمل روی $\Omega \cup B$، دارای یک توسیع متعدی چون G است. G گروهی است ساده و درجهٔ آن عبارت است از $۱۰۰ = ۷۷ + ۲۲ + ۱$. مرتبهٔ G برابر است با ۱۰۰ برابر مرتبهٔ $M_{۲۴}$. این گروه ساده، گروه هیگمن-سیمز نامیده می‌شود و آن را با HS نمایش می‌دهند.

اما گروههای دیگری که با استفاده از ویژگیهای ترکیباتی گروههای ماتیو پیدا شدند، گروههای سادهٔ کانوی هستند. در سال ۱۹۶۹ کانوی [۴] سه گروه سادهٔ پراکنده با استفاده از گروه خودریختی‌های شبکهٔ لیچ پیدا کرد. در اینجا مختصری از رهیافت کانوی را شرح می‌دهیم.

فرض کنید $\mathbf{R}^n$ فضای اقلیدسی nبعدی با حاصلضرب داخلی $(,)$ است. یک شبکهٔ Λ در $\mathbf{R}^n$ عبارت است از مجموعهٔ تمام ترکیبات خطی، با ضرایب در $\mathbf{Z}$، از بردارهای $\mathbf{v}_1, \ldots, \mathbf{v}_n$ در $\mathbf{R}^n$ به‌طوری که $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ پایه‌ای از $\mathbf{R}^n$ باشد و $(\mathbf{v}_i, \mathbf{v}_j)$ به‌ازای تمام i و jها اعداد صحیحی باشند. حال فرض کنید $\{e_i \mid 1 \leqslant i \leqslant ۲۴\}$ یک پایهٔ متعامد برای $\mathbf{R}^n$ است. شبکهٔ Λ یک شبکهٔ صحیح نامیده می‌شود اگر مؤلفه‌های $\mathbf{v}_i$، $1 \leqslant i \leqslant ۲۴$، نسبت به‌پایهٔ فوق اعداد صحیح باشند. گروه خودریختی‌های شبکهٔ Λ، که با $\mathrm{Aut}\,\Lambda$ نمایش داده می‌شود، عبارت است از مجموعهٔ تمام دورانهای $\mathbf{R}^n$ به‌طوری که Λ را پایدار سازند. لیچ در ارتباط با کره‌بندی فضای اقلیدسی $\mathbf{R}^{۲۴}$ شبکهٔ خارق‌العاده‌ای پیدا کرد که به‌شبکهٔ لیچ معروف است [۱۲ و ۱۱] و آن را می‌توان چنین توضیح داد.

فرض می‌کنیم Ω یک مجموعهٔ ۲۴ عضوی است و $\mathcal{C} \subseteq \mathcal{P}(\Omega)$ کدگولای است. دستگاه اشتاینر $S(۵, ۸, ۲۴)$ را که بلوکهای آن اکتادهای $\mathcal{C}$ هستند در نظر می‌گیریم. همچنین فرض می‌کنیم $\{\mathbf{v}_i \mid i \in \Omega\}$ یک پایهٔ متعامد یکانی برای $\mathbf{R}^{۲۴}$ است و مؤلفه‌های بردارها را نسبت به‌این پایهٔ ثابت می‌نویسیم. به‌ازای هر عدد صحیح m و هر زیرمجموعهٔ S از Ω قرار می‌دهیم

$$[S, m] = \left\{(x_1, \ldots, x_{۲۴}) \mid x_i \in \mathbf{Z},\ \sum_{i=1}^{۲۴} x_i = ۴m,\right.$$
$$\left. x_i \equiv m \pmod ۴ \text{ اگر } i \notin S,\ x_i \equiv (m+۲) \pmod ۴ \text{ اگر } i \in S\right\}$$

شبکهٔ لیچ عبارت است از $\Lambda = \cup [S, m]$، که در آن، اجتماع روی تمام $m \in \mathbf{Z}$ و $S \in \mathcal{C}$ در نظر گرفته می‌شود. به‌سادگی می‌توان بررسی کرد که به‌ازای هر $x \in \Lambda$ داریم $(x, x) \in ۱۶\mathbf{Z}$. اگر $(x, x) = ۱۶n$ آنگاه x را یک بردار از نوع n می‌نامیم. مجموعهٔ بردارهای نوع یک تهی است و بردارهای نوع دو عبارت‌اند از:

$۲^۲ \times ۷۵۹$ بردار به‌شکل $(۲^۸, ۰^{۱۶})$، که در آن هشت مؤلفهٔ ناصفر درمکان یک اکتاد جا دارند و تعداد ۲ها عددی زوج است.

$۲^{۱۲} \times ۲۴$ بردار به‌شکل $(۳, ۱^{۲۳})$، که در آن، مؤلفه‌هایی که همنهشت با ۱ — به‌پیمانهٔ ۴ هستند در مکان یک $\mathcal{C}$-مجموعه قرار دارند.

$۲^۲ \times \binom{۲۴}{۲}$ بردار به‌شکل $(۴^۲, ۰^{۲۲})$.

مجموعهٔ تمام بردارهای نوع n را با Λ_n نمایش می‌دهیم. بنابراین، در بالا بردارهای $\Lambda_۲$ نوشته شده‌است و داریم $|\Lambda_۲| = ۱۹۶۵۶۰$.

کانوی در مرحلهٔ بعدی گروه خودریختی‌های Λ را با «۰» نمایش داد و ثابت کرد که گروهی متناهی است. اما ابتدا زیر گروههایی از ۰ به ترتیب زیر ساخت. اگر S یک $\mathcal{C}$-مجموعه باشد آنگاه دوران ϵ_S که در زیر تعریف می‌شود عضوی از ۰ است

$$\epsilon_S(\mathbf{v}_i) = \begin{cases} -۱ & i \in S \\ ۱ & i \notin S \end{cases}$$

مجموعهٔ تمام ϵ_Sها یک گروه آبلی مرتبهٔ $۲^{۱۲}$ را تشکیل می‌دهد که با گروه جمعی $\mathcal{C}$ یکریخت است. این گروه را با D نمایش می‌دهیم. هر عضو π از $M_{۲۴}$ به ترتیب زیر عضوی از ۰ القا می‌کند: $\pi(\mathbf{v}_i) = \mathbf{v}_{(i)\pi}$. به‌این ترتیب $M_{۲۴}$ در ۰ نشانده می‌شود. به‌راحتی می‌توان نشان داد که رابطهٔ $DM_{۲۴} = M_{۲۴}D$ برقرار است و در نتیجه $M = D . M_{۲۴}$ زیر گروهی از ۰ است. او نشان داد M یک زیر گروه سرهٔ ۰ است و قضیهٔ زیر را ثابت کرد.

قضیهٔ ۱۰ [۴]. گروه ۰ روی $\Lambda_۲$ به طور متعدی عمل می‌کند و اگر $\mathbf{x}$ و $\mathbf{y}$ دو بردار متعامد در $\Lambda_۲$ باشند آنگاه $|\mathrm{St}_{\mathbf{x}, \mathbf{y}}| = ۰$، پایدارساز $\mathbf{x}$ و $\mathbf{y}$ در ۰، گروهی است متناهی به‌شکل $۲^{۱۰} . M_{۲۴}$ و بنابراین ۰ گروهی است متناهی و

$$|۰| = ۱۹۶۵۶۰ \times ۹۳۱۵۰ \times ۲^{۱۰} \times |M_{۲۴}| .$$

گروه ۰ ساده نیست زیرا $\langle \epsilon_\Omega \rangle = Z(۰)$ یک زیر گروه

نرمال آن است اما گروه $\frac{\cdot^{\circ}}{Z(\cdot^{\circ})}$ ساده است که کانونی آن را با ۱. نشان داد. گروه ۰. روی Λ_{γ} و Λ_{γ} به طور متعدی عمل می‌کند و پایدارساز یک‌حرف در هرمورد گروهی ساده است که به‌ترتیب با ۲. و ۳. نمایش داده می‌شوند. گروههای ۱. و ۲. و ۳. گروههای سادهٔ پراکنده هستند.

مراجع

1. E. Artin, *Geometric Algebra*, Interscience Publishers, Inc., New York (1957).
2. F. N. Cole, "List of the transitive substitution groups of ten and of eleven letters," *Quart. J. Pure Appl. Math.*, **27** (1895) 39-50.
3. J. H. Conway, "Three lectures on exceptional groups," *Finite Simple Groups*, ed. M. B. Powel and G. H. Higman, Academic Press, London, New York (1971).
4. J. H. Conway, "A group of order 8315553613086720000," *Bull. London Math. Soc.*, **1** (1969) 79-88.
5. D. Gorenstein, *Finite Simple Groups*, Plenum Press, New York and London (1982).
6. D. Held, "The simple groups related to M_{24}," *J. alg.*, **13** (1969) 253-296.
7. D. Higman, S. Sims, "A simple group of order 44352000," *Math Z.*, **105** (1968) 110-113.
8. D. R. Hughes, "Combinatorial analysis, t-designs and permutation groups," *Proc. Symp. Pure Math.*, **6** (1962) 39-41.
9. Z. Janko, "Some new finite simple groups of finite order," *First Naz. Alta Math. Symposia Math.*, **1** (1968)25-65.
10. T. P. Kirkman, "On a problem in combinatorics," *Cambridge and Dublin Math. J.*, **2** (1947) 191-204.
11. J. Leech, "Some sphere packings in higher space," *Canad. J. Math.*, **16** (1964) 657-682.
12. J. Leech, "Notes on sphere packings," *Canad. J. Math.*, **19** (1967) 251-267.
13. E. Mathieu, "Memoire sur le nombre de valeurs que peut acquerir une fonction quand on y permut ses variables de toutes les manieres possibles," *Crelle J.*, **5** (1860) 9-42.
14. E. Mathieu, "Memoire sur l'etude des fonctions des plusieures quantites, sur la maniera de les formes, et sur les substitutions qui les laissent invariables," *Crelle J.*, **6** (1861).
15. E. Mathieu, "Sur la fonction cinq fois transitive des 24 quantities," *Crelle J.*, **18** (1873) 25-46.
16. J. A. Miller, "On the simple groups which can be represented as substitution groups that contain cyclical substitutions of a prime degree," *Amer Math. Monthly*, **6** (1899) 102-103.
17. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London (1964).
18. E. Witt, "Die 5-fach transitiven Gruppen von Mathieu," *Abh. Math. Sem. Univ. Hamburg*, **12** (1938) 256-264.
19. W. S. B. Woolhouse, Prize questions 1733, *Lady's and Gentleman's Diary* (1844).

* محمدرضا درفشه و غلامرضا برادران خسروشاهی، بخش ریاضی دانشکدهٔ علوم دانشگاه تهران؛ مرکز فیزیک تئوری و ریاضی سازمان انرژی اتمی ایران