بسم الله الرحمن الرحيم

دانشگاه تربیت معلم

دانشکدهٔ علوم ریاضی و مهندسی کامپیوتر

(موسسه ریاضی دکتر مصاحب)

پایان نامه:

کارشناسی ارشد ریاضی محض

موضوع

مشخص سازی گروه *PSL(2,q)* به وسیلهٔ مرتبهٔ اعضای آن

استاد راهنما: دکتر علیرضا جمالی

نگارش: پوریا مجد آملی

تیر ۱۳۸۰

تقدیم به همهٔ بزرگانی که حاصل
عمر آنها سعادت رهپویانشان را
رقم می‌زند.

تقدیر و تشکر:

سپاس بی‌منتها خدای را سزاست که هستی را پدید آورد و از روح خود در انسان دمید، خداوند را شکر گزارم که در همهٔ مراحل زندگی پشتیبان من بود. امیدوارم بتوانم بنده‌ای ناشکر نباشم.

از زحمات همهٔ اساتید محترم و همهٔ کسانی که برای من به هر نحو زحمت کشیده‌اند، بالاخص از زحمات استاد عزیزم جناب آقای دکتر علیرضا جمالی تشکر و قدردانی می‌نمایم.

همچنین از اساتید ارجمند جناب آقای دکتر علیرضا زکائی و جناب آقای دکتر حسین دوستی که زحمت مطالعه و داوری این پایان‌نامه را تقبل فرمودند سپاسگزارم.

همینطور از کلیهٔ کارمندان شرکت رهپویان دانش بالاخص سرکار خانم زیرک که زحمت تایپ این پایان‌نامه را برعهده داشتند تشکر و قدردانی می‌نمایم.

تاریخ ....

شماره ....

پیوست ....

واحد ....

بسمه تعالی

دانشکدهٔ علوم ریاضی و مهندسی کامپیوتر

دانشگاه تربیت معلم

صورتجلسهٔ دفاع از پایان نامهٔ کارشناسی ارشد

جلسهٔ دفاع از پایان نامه آقای پوریا مجدآملی دانشجوی دورهٔ کارشناسی ارشد رشتهٔ ریاضی محض تحت عنوان:

مشخص سازی گروه $PSL(۲, q)$ به وسیلهٔ مرتبهٔ اعضایش

در روز شنبه مورخه ۸۰/۴/۲ در دانشکدهٔ علوم ریاضی و مهندسی کامپیوتر تشکیل گردید و نتیجه آزمون به شرح زیر تعیین می‌گردد. نمرهٔ این آزمون ۱۸/۵ (هجده و نیم) می‌باشد.

۱- عالی ☒
۲- بسیار خوب ☐
۳- خوب ☐
۴- قابل قبول ☐
۵- غیر قابل قبول ☐

استاد راهنما — دکتر علیرضا جمالی

داور خارجی — دکتر علیرضا زکائی

داور داخلی — دکتر حسین دوستی

اسماعیل بابلیان

رئیس دانشکدهٔ علوم ریاضی و مهندسی کامپیوتر

تهران، خیابان طالقانی بین بهار و شریعتی، پلاک ۵۹۹ کدپستی ۱۵۶۱۸ تلفن ۷۵۰۷۷۷۲ فاکس ۷۶۲۹۸۸

چکیده

فرض کنیم G گروهی متناهی باشد. مجموعهٔ مرتبهٔ اعضای G را با $\pi_e(G)$ ، و تعداد گروههای متناهی غیر یکریخت با G چون H را به قسمی که $\pi_e(H)=\pi_e(G)$ ، با $h(\pi_e(G))$ نشان می‌دهیم. گوییم گروه G قابل شناسایی به وسیلهٔ مجموعهٔ مرتبهٔ اعضایش است هرگاه $h(\pi_e(G))=0$.

فصل اول این پایاننامه به تعریفها و نتایج بنیادی اختصاص دارد که در فصلهای بعد مورد نیاز خواهند بود. در فصل دوم مفهوم گراف اول وابسته به یک گروه متناهی و قضایا و لمهایی را در این رابطه بیان خواهیم کرد؛ جدول مولفه‌های همبند گراف اول گروههای ساده در این فصل خواهد آمد. همچنین قضیهٔ معروف هیگمن در مورد EPPO- گروههای حل‌پذیر به اثبات خواهد رسید. در فصل سوم با محاسبهٔ مرتبهٔ اعضای PSL(2,q) که q توانی از یک عدد اول فرد است و با استفاده از قضیه‌ها و لمهای اثبات شده در فصول قبل نشان می‌دهیم که PSL(2,q) قابل شناسایی به وسیلهٔ مجموعهٔ مرتبهٔ اعضایش می‌باشد.

واژه‌های کلیدی : قابل شناسائی، گراف اول، مشخص سازی، مولفه‌های همبند گراف اول

فهرست مطالب

عنوان **صفحه**

پیشگفتار

مسائل مربوط به مرتبهٔ اعضای گروههای متناهی همواره یکی از مهمترین موضوعات تحقیقی برای ریاضیدانها بوده است. یکی از این مسائل که تقریباً دو دهه قبل به طور جدی مورد بررسی ریاضیدانهایی که در شاخهٔ نظریه گروهها فعالیت می‌کردند واقع شد، مساله شناسایی یک گروه متناهی به وسیله مجموعه مرتبهٔ اعضایش بود. فرض کنیم G گروهی متناهی باشد. مجموعهٔ مرتبهٔ اعضای G را با $\pi_e(G)$ و مجموعهٔ عوامل اول موجود در تجزیه $|G|$ را با $\pi(G)$ نشان می‌دهیم؛ گوییم G قابل شناسایی به وسیلهٔ مجموعهٔ مرتبهٔ اعضایش است هرگاه به ازای هر گروه متناهی چون H به قسمی که $\pi_e(G)=\pi_e(H)$، داشته باشیم $G\cong H$.

مساله قابل شناسایی بودن یک گروه متناهی به وسیلهٔ مجموعهٔ مرتبهٔ اعضایش با مفهومی بنام گراف اول که به یک گروه متناهی وابسته می‌شود ارتباطی نزدیک دارد. گراف اول یک گروه متناهی به صورت زیر تعریف می‌شود :

گراف اول G، گرافی است که مجموعهٔ رئوس آن $\pi(G)$ است و دوراس p و q توسط یک یال به هم وصل می‌شوند هرگاه $pq\in\pi_e(G)$.

در سال ۱۹۸۱ ویلیامز[1]، جدول مولفه‌های همبند گراف اول گروههای ساده را به دست آورد [۴۲]. در سال ۱۹۸۴ شی[2]، ریاضیدان چینی، با استفاده از مقالهٔ ویلیامز که جدول مولفه‌های همبند گراف اول گروههای ساده را به دست آورده بود و با استفاده از روشهایی که در فصل ۲ پایاننامه خواهد آمد ثابت کرد که A_5 به وسیلهٔ مجموعهٔ مرتبهٔ اعضایش قابل شناسایی است[۳۹].

---

[1] J.S.Williams

[2] W.J.Shi

از سال ۱۹۸٤ به بعد مقالات بسیار زیادی در این مورد و مسائل مرتبط با آن نوشته شده است. در مقدمه تاریخی که در فصل ۲ خواهد آمد،بیشتر تحقیقاتی که در این زمینه انجام شده است معرفی خواهند شد. از جمله این تحقیقات اثبات قابل شناسایی بودن گروه PSL(2,q) است که در آن q توانی از یک عدد اول فرد است. اثبات این حکم که به توسط براندل[1] و شی در ۱۹۹٤ صورت گرفته است[۳] موضوع اصلی این پایاننامه است.

این پایاننامه به سه فصل تقسیم شده است :

فصل اول به تعریفها و قضیه‌ها و لمهایی اختصاص یافته است که در فصلهای بعد مورد نیاز خواهند بود. در فصل دوم مفهوم گراف اول یک گروه متناهی و لمها و قضیه‌های مربوط به آن مورد بررسی قرار خواهند گرفت. همچنین قضیه معروف هیگمن[2] در مورد EPPO- گروههای حل‌پذیر متناهی به اثبات خواهد رسید؛ و نیز جدول مولفه‌های همبند گراف اول گروههای ساده درج خواهد شد. در فصل سوم با محاسبهٔ مرتبهٔ اعضای PSL(2,q) که q توانی از یک عدد اول فرد است و با استفاده از قضیه‌ها و لمهایی که در فصل‌های ۱ و ۲ بیان شد ثابت خواهیم کرد PSL(2,q) به وسیلهٔ مجموعه مرتبهٔ اعضایش قابل شناسایی است.

---

[1] R.Brandl

[2] G.Higman

فصل اول

پیشنیازها

از تمامی قضایا و لمهای بیان شده در این فصل در فصول بعد استفاده خواهیم کرد و حتی‌الامکان از اثبات قضایا و لمهای متعارف خودداری می‌شود.

۱-۱. **تعریف** . فرض کنیم G یک گروه و Ω مجموعه‌ای غیر تهی باشد(عضو بی اثر G را با علامت 1 نمایش می‌دهیم). نگاشت $f : \Omega \times G \to \Omega$ را یک *عمل* G روی Ω می‌نامیم هرگاه :

1) $(\omega, 1) f = \omega , \quad \forall\, \omega \in \Omega ,$

2) $((\omega,g)f, h)f = (\omega, gh)f , \forall\, \omega\in \Omega , \forall\, g,h \in G.$

در حالت کلی که نوشتن قانون عمل یعنی f ایجاد ابهام ننماید بـه جـای $(\omega,g)\ f$ مختصـراً می‌نویسیم ω^g. بنابراین شرایط ۱ و ۲ تعریف ۱-۱ به این صورت نوشته خواهند شد.

1) $\omega^1 = \omega , \forall\, \omega \in \Omega,$

2) $(\omega^g)^h = \omega^{gh}, \forall\, \omega\in\Omega, \ \forall\, g,h\in G.$

در این صورت گوییم G روی Ω عمل می‌کند.

۱-۲. لم . فرض کنیم G یک گروه و Ω یک مجوعه باشد و G روی Ω عمل می‌کنـد. در این صورت $\sim$ که در زیر تعریف می‌شود یک رابطهٔ هم‌ارزی در Ω است

$$\alpha\sim\beta \Leftrightarrow \exists\, g\in G \ni \alpha^g=\beta\ ,\ \alpha,\beta\in\Omega .$$

۱-۳. تعریف . فرض کنیم G یک گروه و Ω مجموعه‌ای ناتهی باشد و G روی Ω عمـل کند. همچنین فرض کنیم $\sim$ رابطهٔ هم‌ارزی تعریف‌شده در لم ۱-۲ باشد. برای $\alpha\in\Omega$ مجموعهٔ

$$\Delta(\alpha)=\{\beta\in\Omega \mid \alpha\sim\beta\}$$

را که ردهٔ هم‌ارزی α است یک *مدار* G می‌نامیم.

۱-٤. تعریف . فرض کنیم G یک گروه باشد و H و K زیـر گروهـهایی از G باشـند بـه طوری که :

الف) $H\lhd G$،

ب) $H\cap K=\{1\}$،

ج) $G=HK$.

در این صورت G را *حـاصلضرب نیم‌مستقیم H و K* می‌نـامیم و می‌نویسـیم $G=H.K$. بـا توجه به شرایط (ب) و (ج) هر $g\in G$ به طور منحصر بفردی به شکل $g=hk$ نوشـته می‌شـود، به طوری که $h\in H$ و $k\in K$.

۱-۵. تعریف . اگر G و H و K گروه باشند، آنگاه دنبالهٔ

$$1\to H\xrightarrow{g} G\xrightarrow{f} K\to 1$$

متشکل از همریختی گروهها، یک *دنبالهٔ دقیق کوتاه* نامیده می‌شود هرگاه Im(g)=Ker(f) و g یک به یک و f پوشا باشد. در این صورت گوییم G ، *توسیع H به وسیلهٔ K* می‌باشد. همچنین گوییم توسیع G روی H *شکافته* می‌شود هرگاه همریختی $h : K \to G$ وجود داشته باشد به طوری که fh=i ، که در آن i همریختی همانی از k به K می‌باشد.

۱-۶. **تذکر** . اگر G، K و H گروه باشند و G توسیع H به وسیله K باشد، در این صورت H دارای زیر گروه نرمال یکریخت با H است و $G / H \cong K$.

۱-۷. **قرارداد** . فرض کنیم G یک گروه متناهی باشد. مجموعهٔ همهٔ شمارنده‌های اول |G| را با π (G) نمایش می‌دهیم.

۱-۸ . **تعریف** . فرض کنیم G یک گروه متناهی و π زیر مجموعه‌ای از اعداد اول باشد، گوییمG یک π-گروه است هرگاه $\pi (G) \subseteq \pi$.

۱-۹. **تعریف** . فرض کنیم G یک گروه باشد. گوییم G *حل‌پذیر* است هرگاه سری زیر نرمالی از G مانند

$$G_0 = \{1\} \lhd G_1 \lhd \ldots \lhd G_n = G$$

وجود داشته باشد به قسمی که برای هر $1 \le i \le n$ ، G_i / G_{i-1} آبلی باشد.

۱-۱۰. **تعریف** . یک سری از زیر گروههای G مانند :

$$G_0 = \{1\} \lhd G_1 \lhd \ldots \lhd G_n = G$$

را یک *سری ترکیبی* برای G می‌نامیم هرگاه برای هر $1 \le i \le n$ ، G_{i-1} زیر گروه نرمال ماکسیمال G_i باشد.

در ایـن صورت G_i / G_{i-1} سـاده می‌باشد، به هر یک از گروههای خارج قسمتی G_i / G_{i-1} (برای هر $1 \leq i \leq n$)، *عاملی ترکیبی G* می‌گوییم.

۱-۱۱. تعریف . گوییم گروه G ، *π- حل‌پذیر* است اگر یک سری ترکیبی داشته باشد که همه عاملهای آن π'- گروه (π' زیر مجموعـــه‌ای از مجموعـهٔ اعـداد اول اسـت بـه قسـمی کـه $\pi' \cap \pi = \varnothing$) یا p- گروه باشد، به ازای برخی اعداد p در π.

۱-۱۲. لم . اگر گروه متناهی G حل‌پذیر باشد آنگاه به ازای هر عــدد اول p، گروه G، p- حل‌پذیر می‌باشد.

۱-۱۳. قضیه . فرض کنیم G یک گروه متناهی باشد. در این صورت :

الف) اگر G حل‌پذیر باشد آنـگاه تمـام زیـرگروهـها و گروهـهای خـارج قسـمتی G نـیز حل‌پذیر هستند.

ب) فرض کنیم $K \lhd G$. هرگاه K و G / K حل‌پذیر باشد آنگاه G حل‌پذیر است.

ج) هرگاه G متناهی و حل‌پذیر باشد آنگاه G دارای π- زیر گروه هال می‌باشد. (زیـر گروه H از G را زیر گروه *هال* گوییم هرگاه $(|G : H| , |H|) = 1$ و $(\pi(H) \subseteq \pi)$.

۱-۱٤. قرارداد . اگر H و K دو π- زیـر گروه نرمـال از گروه متنـاهی G باشـند در ایـن صورت HK نیز π- زیر گروه نرمال G است، در نتیجه G دارای π- زیر گروه نرمال ماکســیمال منحصر بفرد می‌باشد که آن را با $O_\pi(G)$ نمایش می‌دهیم.

۱-۱۵. تعریــف . فـرض کنیـم G یـک گروه متنـاهی باشـد. زیـر گروه H از G را یــک زیرگروه مشخصه G می‌نامیم هرگاه

$$\forall \varphi \in Aut(G), \varphi(H) \subseteq H$$

و می‌نویسیم H Char G به وضوح اگر H Char G ، آنگاه $H \lhd G$.

با این تعریف واضح است که $O_\pi(G)$ Char G ؛ همچنین با استفاده از تعریف $O_\pi(G)$ نتیجه می‌شود $O_\pi(G / O_\pi(G)) = \{1\}$.

۱-۱۶. لم . فرض کنیم G یک گروه باشد و $H \leq G$ در این صورت

الف) $C_G(H) \lhd N_G(H)$ ،

ب) $N_G(H) / C_G(H)$ با زیر گروهی از $Aut(H)$ یکریخت است.

۱-۱۷. لم . فرض کنیم G یک گروه باشد. اگر G دوری باشد آنگاه $Aut(G)$ آبلی است.

۱-۱۸. تعریف . فرض کنیم G یک گروه باشد. یک سری از زیر گروههای نرمال G مانند

$$G_0 = \{1\} \leq G_1 \leq \ldots \leq G_n = G$$

را یک *سری مرکزی* برای G می‌نامیم هرگاه

$$G_i / G_{i-1} \leq Z(G/G_{i-1}) \quad (\forall\ 1 \leq i \leq n).$$

گروه G را *پوچ توان* گوییم هرگاه دارای یک سری مرکزی باشد.

۱-۱۹. قضیه . فرض کنیم G یک گروه متناهی باشد، احکام زیر معادل هستند :

الف) G یک گروه پوچ توان است.

ب) G را می‌توان به شکل حاصل ضرب مستقیم p- زیر گروههای سیلوی آن نوشت.

۱-۲۰. تعریف . گروه Q_{2^n} $(n\geq 3)$ را که به شکل زیر نمایش داده می‌شود، گروه *کواترنیون تعمیم یافته* می‌نامیم

$$Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1} \rangle .$$

۱-۲۱. لم . $Z(Q_{2^n}) = \langle y^2 \rangle$

برهان) واضح است که $\langle y^2 \rangle \subseteq Z(Q_{2^n})$ نشان می‌دهیم $Z(Q_{2^n}) \subseteq \langle y^2 \rangle$

فرض کنیم $x^i y^j \in Z(Q_{2^n})$ که در آن $0 \le j \le 3$ و $0 \le i \le 2^n-1$. حال می‌توان نوشت :

$$
\begin{aligned}
&[x^i y^j, x] = 1 \Rightarrow y^{-j}x^{-i}x^{-1}x^i y^j x = 1 \Rightarrow y^{-j}x^{-1}y^j x = 1\\
&y^{-1}xy = x^{-1} \Rightarrow y^{-j}xy^j = (-1)^j \Rightarrow x^{-1}y^{-j}xy^j = x^{(-1)^j-1}\\
&\Rightarrow x^{(-1)^j-1} = 1 \Rightarrow 2^{n-1} \mid (-1)^j - 1 \Rightarrow j = 0 \quad \text{یا} \quad j = 2\\
&[x^i y^j, y] = 1 \Rightarrow y^{-j}x^{-i}y^{-1}x^i y^j y = 1 \Rightarrow x^{-i}y^{-1}x^i y = 1\\
&y^{-1}xy = x^{-1} \Rightarrow y^{-1}x^i y = x^{-i} \Rightarrow x^{-i}y^{-1}x^i y = x^{-2i} \Rightarrow x^{-2i} = 1\\
&\Rightarrow x^{n-1} \mid 2i \Rightarrow 2^{n-1} \mid i \Rightarrow i = 0 \text{ یا } i = 2^{n-2}.
\end{aligned}
$$

جدول زیر را برای مقادیر مختلف i و j داریم

j	0	2	0	2
i	0	0	2^{n-2}	2^{n-2}

$$
\begin{aligned}
&j = 0, i = 0 \Rightarrow x^i y^j = x^0 y^0 = 1 \in \langle y^2 \rangle\\
&j = 2, i = 0 \Rightarrow x^i y^j = x^0 y^2 = y^2 \in \langle y^2 \rangle\\
&j = 0, i = 2^{n-2} \Rightarrow x^i y^j = x^{2^{n-2}} y^0 = x^{2^{n-2}} = y^2 \in \langle y^2 \rangle\\
&j = 2, i = 2^{n-2} \Rightarrow x^i y^j = x^{2^{n-2}} y^2 = y^2 y^2 = y^4 = 1 \in \langle y^2 \rangle.
\end{aligned}
$$

در نتیجه $x^i y^j \in Z(Q_{2^n})$ و در نهایت $Z(Q_{2^n}) = \langle y^2 \rangle$.

۱-۲۲. تعریف . فرض کنیم G یک گروه باشد. $\alpha \in \mathrm{Aut}(G)$ را *خالی از نقطهٔ ثابت* گوییم اگر