بسم الله الرحمن الرحیم

عدد رده‌ای p—گروه‌ها از مرتبه‌ی داده شده

زکیه اعلایی

دانشکده‌ی علوم

گروه ریاضی

دی ۱۳۸۸

پایان نامه برای دریافت درجه‌ی کارشناسی ارشد

استاد راهنما:

دکتر علی سرباز جانفدا

پایان نامه آقای/خانم زکیه اعدانی به تاریخ ۶ر۱۱ر۸۸

شماره ۱۸. ۱۰-۲ مورد پذیرش هیات محترم داوران با رتبه عالی و نمره ۱۸/- هیجده تمام

قرار گرفت .

۱- استاد راهنما و رئیس هیئت داوران : دکتر علی سربازاحمدی

۲- استاد مشاور : دکتر ——

۳- داور خارجی : دکتر محسن قاسمی

۴- داور داخلی : دکتر هوشنگ بهروش

۵- نماینده تحصیلات تکمیلی : دکتر ساکینه اشدربش

۱

فهرست مندرجات

تقدیم

تقدیم به مهربان فرشتگانی که؛

لحظات ناب باور بودن، لذت و غرور دانستن، جسارت خواستن، شکوه توانستن، عظمت رسیدن و تمام تجربه‌های یکتا و زیبای زندگی‌ام، مدیون حضور سبز آن‌هاست.

پدر بزرگوارم، مادر مهربانم و خواهر عزیزم.

تقدیر و تشکر

سپاس بی‌کران باد خداوند متعال، استاد بی‌همتا را، که قلم به تحریر نرفت جز آن‌که جوهر از کاسه‌ی عشق و علم او برمی‌داشت.

باتشکر فراوان از استاد راهنمای بزرگوارم آقای دکتر سرباز جانفدا که هر وقت به راهنماییها و کمک ایشان نیاز داشتم با برنامه ریزی دقیق همواره حضور داشتند و با دقت و حوصله‌ی کافی وقت زیادی را صرف این پایان‌نامه کردند. همچنین از داور داخلی‌ام آقای دکتر بهروش کمال تشکر را دارم که اگر کمک‌ها و راهنمائیهای ایشان نبود پس از دو ماه کار روی این مقاله و سردرگمی‌های زیاد به دلیل عدم اطلاع کافی از قسمت‌های اوّل مقاله به فکر عوض کردن موضوع پایان‌نامه بودم ولی اکنون خیلی خوشحالم که به کمک راهنمائیهای به موقع و با حوصله‌ی این بزرگوار توانستم با علاقه‌ای فراوان روی این مقاله (هر چند دشوار) ولی بسیار جالب دکتر آیزاک کار کنم. از داور خارجی‌ام آقای دکتر قاسمی نیز به خاطر دقت فراوان ایشان در مطالعه‌ی پایان‌نامه و وقتی که برای مطالعه‌ی تمام صفحات آن صرف کردند، تشکر می‌کنم و موفقیت و شادکامی هر سه بزرگوار را از خداوند متعال خواستارم.

از پدر عزیزم که در تمام دوران تحصیل مشوق اصلی بنده بودند تشکر فراوان دارم. از مادر مهربانم که با محبت‌ها و مهربانی‌هایشان همواره مسیری درست را در زندگی برایمان نشان داده‌اند قدردانی می‌کنم و از خواهر عزیزم که بعد از خدای مهربان تنها کسی است که وجودش را در تمام لحظات سخت در کنارم احساس می‌کردم و همواره آرامش قلبی برایم بوده و هستند، بی‌نهایت سپاسگذارم.

چکیده

در این پایان‌نامه موضوع مورد مطالعه p—گروه‌هایی با نماهای کوچک می‌باشد. می‌خواهیم رفتار تعداد کلاس‌های تزویجی p—گروه‌هایی از مرتبه‌های p^e را وقتی که e تغییر می‌یابد، مطالعه کنیم. به علاوه ارتباطی بین این رفتار و خم‌های بیضوی برقرار خواهیم نمود.

پیش گفتار

نظریه گروه‌ها و خم‌های بیضوی دو شاخه‌ی مهمی در گرایش جبر می‌باشند. از جمله مباحث مهم در نظریه گروه‌ها بحث رده‌بندی گروه‌ها بر اساس عدد رده‌ای آن‌ها می‌باشد.

مهمترین و پرکاربردترین بحث خم‌های بیضوی که در مسائل رمز نگاری نیز استفاده‌ی زیادی دارد بحث رتبه‌ی خم‌های بیضوی یا به عبارتی تعداد نقاط روی یک خم بیضوی می‌باشد.

ما در این پایان‌نامه، که کار روی مقاله[۳]، مقاله‌ای بسیار جالب از دکتر آیزاک و ناقل بوستون در سال (۲۰۰۴) می‌باشد، ارتباطی بین این دو مبحث مهم از نظریه گروه‌ها و خم‌های بیضوی ایجاد خواهیم کرد.

در حقیقت خم‌های بیضوی شاخه‌ای از ریاضیات است که علاوه بر نظریه گروه‌ها می‌توان گرایش‌های مختلف دیگری از ریاضیات مانند جبرجابجایی، هندسه‌ی جبری، آنالیز حقیقی، آنالیز مختلط، نظریه اعداد، آنالیز عددی و $\cdots$ را با آن مرتبط ساخت.

هدف اصلی در این پایان‌نامه اثبات قضیه مهمی در ارتباط با p−گروه‌هایی از مرتبه p^9 می‌باشد. p−گروه‌ها ویژگی‌های خاص مفیدی دارند و نقش مهمی در تحلیل گروه‌های متناهی ایفا می‌کنند و تحقیق در مورد اعداد رده‌ای p−گروه ها حداکثر به دو دهه قبل برمی‌گردد.

اثبات این قضیه در نظریه گروه‌ها کار دشواری است به همین علت برای اثبات آن، دو مبحث مهم از نظریه گروه‌ها و خم‌های بیضوی را که در بالا اشاره شد به یکدیگر مرتبط ساخته و با ساختن پل ارتباطی بین عدد رده‌ای p−گروه‌ها و تعداد نقاط روی

یک خم‌بیضوی، این قضیه‌ی اساسی از نظریه گروه‌ها را به خم‌های بیضوی ارتباط داده و به کمک قضایای مهمی از خم‌ها آن را اثبات خواهیم کرد.

در بخش اوّل یک سری تعاریفی از این دو شاخه می‌آوریم. در بخش دوّم در مورد عدد رده‌ای p-گروه‌هایی از مرتبه‌های p، p^2، p^3، p^4، p^5 و p^6 بحث خواهیم کرد. برای ساختن این پل ارتباطی به یک سری گروه‌ها و فضایی از ماتریس‌ها نیاز خواهیم داشت؛ که گروه‌های مورد نیاز را در بخش سوّم و ماتریس‌های ضروری را در بخش چهارم تعریف خواهیم کرد.

در حقیقت با تعریف این گروه‌ها و ماتریس‌ها به ازای هر p داده شده یک گروهی از مرتبه‌ی p^9 و یک خم بیضوی خواهیم ساخت به طوری‌که عدد رده‌ای این گروه ساخته شده با تعداد نقاط خم بیضوی به‌دست آمده رابطه‌ای مستقیم داشته باشد. بالاخره در بخش آخر چگونگی این ارتباط را توضیح داده و قضیه را اثبات خواهیم کرد.

پیشنهاد: در بخش دوّم پایان‌نامه که در رابطه با p-گروه‌ها است و همچنین در بخش آخر که در رابطه با خم‌های بیضوی می‌باشد، مطالب خوب زیادی برای باز کردن و توضیح بیشتر حتی مطالبی برای تغییر دادن وجود دارد. شاید بتوان با یک سری تغییرات p-گروهی جدید تعریف کرد و خم بیضوی جدیدی ساخته و مسئله را به روش دیگری نتیجه گرفت.

۱ تعاریف اوّلیه

ابتدا تعاریفی در رابطه با مباحث نظریه‌ی گروهها می‌آوریم که در قسمت مقدمه و بخش گروهها از آن‌ها استفاده خواهیم کرد.

تعریف ۱.۱ فرض کنیم G یک گروه باشد. G را p—گروه[۱] نامیم هرگاه مرتبه‌ی هر عضو آن توانی از عدد اول p باشد.

تعریف ۲.۱ فرض می‌کنیم $x, y \in G$. گوییم x مزدوج[۲] y در G است اگر به ازای عضوی مانند $g \in G$ داشته باشیم $y = g^{-1}xg$.

تعریف ۳.۱ مجموعه‌ی تمام عناصری از G که با x مزدوج هستند کلاس تزویجی[۳] x در G نامیده می‌شود. این مجموعه را به صورت زیر نمایش می‌دهیم:

$$x^G = \{g^{-1}xg \mid g \in G\}.$$

تعریف ۴.۱ اگر x عضوی از گروه G باشد، مجموعه‌ی عناصری از G را که ضربشان در x تعویض پذیر است مرکز ساز x در G نامیده و با نماد $C_G(x)$ نمایش می‌دهیم.

تعریف ۵.۱ فرض کنیم G یک گروه باشد. مجموعه

$$\{g \in G \mid xg = gx \quad \forall x \in G\}$$

را مرکز گروه G نامیده و با نماد $Z(G)$ نشان می‌دهیم.

---

[۱] p-group
[۲] conjugate
[۳] conjugacy class

تعریف ۶.۱ اگر G یک گروه باشد، تعداد کلاس‌های تزویجی G را عدد رده‌ای [۴] G نامیده و با نماد $K(G)$ نمایش می‌دهیم.

تعریف ۷.۱ گوییم گروه G دارای نمای [۵] e است، اگر e کوچکترین عدد صحیح مثبتی باشد که به ازای هر x عضو G داشته باشیم $x^e = ۱$.

تعریف ۸.۱ گروه آبلی A را مقدماتی [۶] گوییم هرگاه یک عدد اوّل، مانند p، موجود باشد به‌طوری‌که به‌ازای هر a عضو A، داشته باشیم $a^p = ۱$.

تعریف ۹.۱ گروه ماتریس‌های وارون پذیر $n \times n$ روی F را گروه خطی عام نامیده و با $GL(n, F)$ [۷] نمایش می‌دهیم. زیر گروهی از اعضای $GL(n, F)$ را که دترمینان [۸] آن‌ها برابر یک باشد، گروه خطی خاص نامیده و با $SL(n, F)$[۹] نمایش می‌دهیم.

تعریف ۱۰.۱ گوییم گروه G بر مجموعه‌ی ناتهی X از راست عمل می‌کند (یا G ترتیب اعضای X را عوض می‌کند) اگر به هر $g \in G$ و هر $x \in X$؛ عضو یکتای $xg \in X$، طوری متناظر شود که به ازای هر $x \in X$ و $g_۱, g_۲ \in G$؛ دو تساوی زیر را داشته باشیم:

$$(xg_۱)g_۲ = x(g_۱g_۲)$$

$$x \cdot ۱ = x.$$

---

[۴] class number
[۵] exponent
[۶] elementary ablian group
[۷] general linear group
[۸] determinant
[۹] special linear group

تعریف ۱۱.۱ فرض می‌کنیم H و K دو گروه دلخواه و $\varphi : H \to K$، یک همریختی باشد. در حاصل‌ضرب دکارتی $H \times K$ عمل دوتایی زیر را تعریف می‌کنیم:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, (k_1 \varphi_{h_2}) k_2) \ .$$

مجموعه‌ی $H \times K$ باعمل فوق تشکیل یک گروه می‌دهد. این گروه را حاصل‌ضرب نیم مستقیم [10] H و K با عمل φ می‌نامیم و آن را با علامت $H \ltimes K$ نشان می‌دهیم، و می‌گوییم گروه H بر گروه K با φ عمل می‌کند.

تعریف ۱۲.۱ فرض کنیم G یک گروه باشد. جابجاگرِ [11] یک زوج مرتب g_1, g_2 از اعضای G به صورت زیر تعریف می‌شود:

$$[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2 \in G \ .$$

تعریف ۱۳.۱ فرض کنیم H زیرگروه G باشد و $a \in G$. مجموعه

$$aH = \{ah \mid h \in H\}$$

را هم‌دسته‌ی [12] چپ H در G، شامل a می‌نامیم. به طور مشابه، مجموعه

$$Ha = \{ha \mid h \in H\}$$

را هم‌دسته‌ی راست H در G شامل a می‌نامیم.

---
[10] semidirect Product
[11] commutator
[12] coset

حال تعاریفی در رابطه با جبرخطی که بیشتر در بخش ماتریس‌ها و خم‌های بیضوی به کار خواهیم برد، می‌آوریم.

تعریف ۱۴.۱ ماتریس $A = [a_{ij}]_{m\times n}$ را در نظر می‌گیریم، بردارهای:

$$r_1 = (a_{11}, a_{12}, \dots, a_{1n}),\ r_2 = (a_{21}, a_{22}, \dots, a_{2n})\,, \dots, r_m = (a_{m1}, a_{m2}, \dots, a_{mn})$$

را که از سطرهای ماتریس A تشکیل شده‌اند، بردارهای سطری ماتریس A، و بردارهای:

$$c_1 = (a_{11}, a_{21}, \dots, a_{m1}),\ c_2 = (a_{12}, a_{22}, \dots, a_{m2})\,, \dots, c_n = (a_{1n}, a_{2n}, \dots, a_{mn})$$

را بردارهای ستونی ماتریس A گوییم. زیر فضایی از R^n را که توسط بردارهای سطری ماتریس A تولید می‌شود، فضای سطری ماتریس A، و زیر فضایی از R^m را که توسط بردارهای ستونی ماتریس A تولید می‌شود فضای ستونی ماتریس A می‌نامیم.

تعریف ۱۵.۱ بعد فضای سطری ماتریس A را، که طبق قضیه‌ای در جبرخطی برابر با بعد فضای ستونی ماتریس A می‌باشد، رتبه‌ی ماتریس A نامیده و با $\mathrm{rank}A$ نمایش می‌دهیم.

تعریف ۱۶.۱ اگر در ماتریس A جای سطرها و ستون‌ها را عوض کنیم ماتریس به‌دست آمده را ترانهاده‌ی [۱۳]ماتریس A نامیده، و با نماد A^T نمایش می‌دهیم.

تعریف ۱۷.۱ اگر $A = [a_{ij}]_n$ و $X^T = [x_1\ x_2\ \dots\ x_n]$، X^TAX را فرم درجه‌ی دوّم ماتریس A می‌نامیم. داریم:

$$X^TAX = \Sigma_i\Sigma_j x_i x_j a_{ij} = \Sigma_i x_i^2 a_{ij} + 2\Sigma_i\Sigma_{j>i} x_i x_j (a_{ij} + a_{ji}).$$

[۱۳] transpose

تعریف ۱۸.۱ اگر X^TAX تنها زمانی صفر شود که $X = \circ$، آن‌گاه آن را، فرم درجه‌ی دوّم معین مثبت [۱۴] می‌نامیم.

[۱۴] positive-definite quadratic form

حال چند تعریف از نظریه اعداد جبری می آوریم.

تعریف ۱.۱۹ فرض کنیم R دامنه‌ی صحیح و K میدان کسرهای آن باشد. یک R–زیر مدول a از میدان K را ایده‌ال کسری[۱۵] R می‌نامیم هرگاه $0 \neq c \in R$ وجود داشته باشد به‌طوری‌که $ca \subset R$. به عبارت دیگر $b = ca$ یک ایده‌ال از R است. بنابراین ایده‌ال‌های کسری R زیرمجموعه‌هایی از K به شکل $c^{-1}b$ هستند، به‌طوری‌که b یک ایده‌ال R و c عضو ناصفری از R می‌باشد.

تعریف ۱.۲۰ یک ایده‌ال کسری از حلقه‌ی صحیح[۱۶] O را اصلی گوییم هرگاه به‌صورت $c^{-1}a$ ای باشد که در آن $c \in O \neq 0$ و a یک ایده‌ال اصلی O است. مجموعه‌ی چنین ایده‌ال‌هایی یک گروه تشکیل می‌دهند. (برای اطلاع بیشتر به [۱۴] مراجعه کنید.)

تعریف ۱.۲۱ فرض کنیم F گروه تمام ایده‌ال‌های کسری و P زیر گروه ایده‌ال‌های کسری اصلی از F باشد. در این‌صورت گروه $H = F/P$ را گروه رده‌ای، و مرتبه‌ی آن را عدد رده‌ای می‌نامیم.

---

[۱۵] fractionl ideal
[۱۶] ring of integer

از بحث خم‌های بیضوی به‌طور مختصر مطالب زیر را یاد آوری می‌کنیم.

تعریف ۲۲.۱ فرض کنیم K یک میدان باشد و $a_1, a_2, a_3, a_4, a_6 \in K$. در این‌صورت معادله‌ای به فرم

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

را یک فرم نرمال وایراشتراس [۱۷] طولانی می‌نامیم.

تعریف ۲۳.۱ معادله‌ای به فرم نرمال وایراشتراس طولانی با ضرایب $a_1, a_2, a_3, a_4, a_6 \in K$ را در نظر می‌گیریم. مقادیر تیِّت به‌صورت زیر تعریف می‌شوند:

$$b_2 = a_1^2 + 4a_2 \qquad b_4 = a_1a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6 \qquad b_8 = b_2b_6 - a_1a_3a_4 + a_2a_4^2 - a_4^2$$

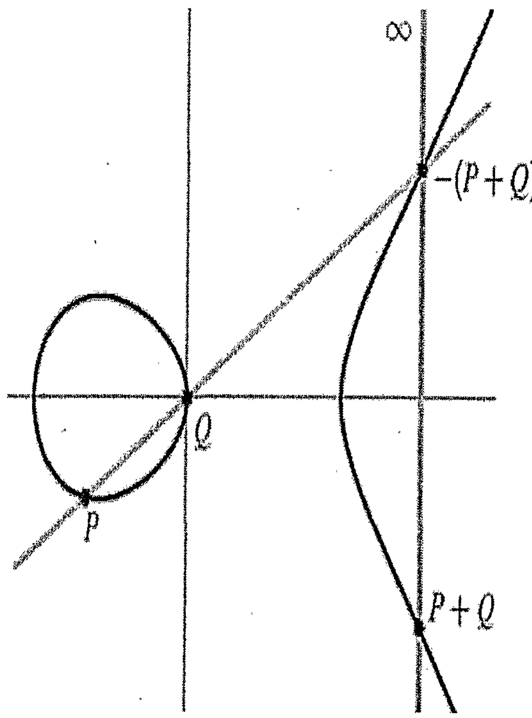
$$c_4 = b_2^2 - 24b_4 \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \qquad j = \frac{c_4^3}{\Delta}$$

Δ به‌دست آمده از روابط بالا را مبین [۱۸]، و j به‌دست آمده را j–پایا [۱۹] می‌نامند.

---

[۱۷] Weierstrass Normal Form
[۱۸] discriminant
[۱۹] j-invariant



تعریف ۲۴.۲ یک خم بیضوی روی K، زوج مرتب (E,O) است که E یک خم با فرم نرمال وایراشتراس طولانی (وایراشتراس تعمیم یافته) با $\Delta \neq 0$ و O نقطه در بی‌نهایت می‌باشد. (برای اطلاع بیشتر از نقطه در بی‌نهایت به [۱۲] مراجعه کنید.)

تعریف ۲۵.۲ اگر دو خم وجود داشته باشند به‌طوری‌که بتوان با یک تغییر متغیر از یکی، دیگری را نتیجه گرفت. در این‌صورت گوییم این دو خم یکریخت هستند. (برای اطلاع بیشتر به [۱٦] مراجعه کنید.)

از ویژگی‌های خم‌های بیضوی این است که بر مجموعه‌ی نقاط این خم‌ها عملی می‌توانیم تعریف کنیم که آن را تبدیل به یک گروه آبلی جمعی می‌کند. اساس تعریف این عمل بر خصوصیات هندسی خم استوار است.

تعریف ۲۶.۱ فرض کنیم $E|K$ یک خم بیضوی روی K باشد. و $P, Q \in E(K)$ دو نقطه (نه لزوماً متمایز) باشند. خط گذرا از P و Q را L می‌نامیم. این خط خم بیضوی را در نقطه‌ی R قطع می‌کند. حال اگر خط گذرا از R و O را L' در نظر بگیریم، دراین‌صورت $P+Q$ را نقطه‌ی تقاطع دیگر خط L' و خم بیضوی E تعریف می‌کنیم. (اگر $P=Q$، باید خط مماس در E در نقطه P را در نظر بگیریم.)

گزاره ۲۷.۱ قانون جمع تعریف شده توسط تعریف ۲۶.۱ (که شکل آن را نیز آوردیم) در خواص زیر صدق می‌کند:

(۱) اگر P، Q و R نقاط تقاطع (نه لزوماً متمایز) خط L و خم جبری E باشند آنگاه

$$(P+Q)+R=O.$$

(۲) برای هر $P \in E$، $P+O=P$.

(۳) برای هر $P, Q \in E$، $P+Q=Q+P$.

(۴) برای هر $P \in E$، یک نقطه‌ی $P' \in E$ وجود دارد که $P+P'=O$. این نقطه را به‌صورت $-P$ نشان می‌دهیم.

(۵) برای هر $P, Q, R \in E$، $(P+Q)+R = P+(Q+R)$.

(۶) به‌ازای هر خم بیضوی $E|K$ مجموعه‌ی

$$E(K) = \Big\{(x,y) \in K \times K \mid y^{2} + a_{1}xy + a_{3}y = x^{3} + a_{2}x^{2} + a_{4}x + a_{6}\Big\} \cup \{O\},$$

یک زیر گروه از E می‌باشد که نقاط Kـ گویای روی E گفته می‌شوند.

اثبات : به [۱۳] مراجعه کنید.

به‌طور خلاصه می‌توان گفت که این قانون جمع، مجموعه‌ی نقاط روی خم جبری E را به یک گروه آبلی تبدیل می‌کند و عنصر همانی این گروه نقطه‌ی O است.

۲ مفاهیم مقدماتی

از بحث‌های مهم در نظریه‌ی گروه‌های متناهی، دسته بندی گروه‌ها بر حسب تعداد کلاس‌های تزویجی می‌باشد. تا کنون این دسته بندی برای گروه‌هایی با مرتبه‌ی کمتر یا مساوی دو هزار بررسی شده است.

اگر G یک گروه متناهی باشد، تعداد کلاس‌های تزویجی G را با $K(G)$ نمایش می‌دهیم.

نماد $D(m)$ را برای نمایش تعداد $K(G)$ های متفاوتی که در آن G گروهی از مرتبه‌ی m می‌باشد، به کار می‌بریم.

در این مقاله سر و کار ما با $p-$ گروههایی خواهد بود که در آن‌ها p عددی اول است. همچنین رفتار $D(p^e)$ هایی را مطالعه خواهیم کرد که در آن p متغیر است و e را ثابت می‌گیریم.

ابتدا با توان‌های کوچک شروع می‌کنیم. با توجه به تعریف $K(G)$ و آبلی بودن گروه‌هایی از مرتبه‌ی p، داریم $K(G) = p$ در نتیجه $D(p) = ۱$.

حال گروههایی از مرتبه‌ی $p^۲$ را بررسی می کنیم. دو نوع دسته بندی گروهی از مرتبه‌ی $p^۲$ داریم؛ نوع اول به صورت $C_{p^۲}$ و نوع دوم به صورت $C_p \times C_p$، ولی می‌دانیم هر گروهی از مرتبه‌ی $p^۲$ آبلی است، بنابراین با توجه به تعریف $K(G)$، برای همه‌ی گروهها از مرتبه‌ی $p^۲$ داریم $K(G) = p^۲$، یعنی $D(p^۲) = ۱$.