دانشگاه اصفهان

دانشکده علوم

گروه ریاضی

پایان‌نامه‌ی کارشناسی ارشد رشته‌ی ریاضی محض گرایش جبر

گروه‌هایی با گراف ناجابجایی یکسان

اساتید راهنما:

دکتر علی‌اکبر محمدی حسن‌آبادی

دکتر مریم خاتمی

پژوهشگر:

مائده آذریون

بهمن‌ماه ۱۳۹۱

چکیده

موضوع این پایان‌نامه مربوط به بررسی گروه‌هایی با گراف‌های ناجابجایی یکسان می‌باشد. هدف اصلی ما اثبات این مسئله است که اگر H یک گروه ساده غیر آبلی متناهی و G یک گروه متناهی باشد به قسمی که گراف‌های ناجابجایی آن‌ها یکریخت باشد آن‌گاه $|G| = |H|$. به علاوه برای تعدادی از گروه‌های ساده خاص H و همچنین گروه‌هایی که حدس تامپسون برای آن‌ها برقرار است، یکریختی گراف‌های ناجابجایی، یکریختی خود گروه‌ها را نتیجه می‌دهد.

واژه‌های کلیدی: گروه متناهی، گروه ساده، گروه خطی تصویری، گراف ناجابجایی، یکریختی گراف

فهرست مطالب

مقدمه

گراف ناجابجایی Γ_G از یک گروه غیر آبلی G به صورت زیر تعریف می‌شود:

مجموعه رئوس Γ_G برابر $G - Z(G)$ می‌باشد، جایی که $Z(G)$ مرکز گروه G است. دو رأس x و y توسط یک یال متصل می‌شوند اگر و تنها اگر $xy \neq yx$. بنا بر [۲۲] گراف ناجابجایی از یک گروه متناهی G ابتدا توسط اردوش[۱] در ارتباط با مسئله زیر در نظر گرفته شده است.

فرض کنید G یک گروه باشد به طوری که گراف ناجابجایی Γ_G زیرگراف‌های کامل نامتناهی ندارد. آیا این مطلب صحیح است که یک کران متناهی روی اندازه زیرگراف‌های کامل Γ_G وجود دارد؟

نویمن[۲] در [۲۲] به سؤال اردوش جواب مثبت می‌دهد و این مبدأ بسیاری از تحقیقات مشابه در مورد گراف ناجابجایی یک گروه می‌شود. اخیراً در [۱] برخی از خواص گراف ناجابجایی متناظر با یک گروه غیر آبلی مورد مطالعه قرار گرفته است و بحث شناسایی‌پذیری گروه‌ها با گراف ناجابجایی مطرح شده است. گروه متناهی G شناسایی‌پذیر با گراف ناجابجایی نامیده می‌شود، هرگاه هنگامی که H یک گروه دلخواه باشد به طوری که $\Gamma_G \cong \Gamma_H$ بتوانیم نتیجه بگیریم $G \cong H$. در [۱]، شناسایی‌پذیری گروه‌های ساده $PSL_۲(۲^n)$ و $Suz(۲^{۲m+۱})$ با گراف ناجابجایی ثابت شده است.

در [۸، ۲۷] نشان داده شده است که همه گروه‌های ساده متناهی با گراف اول ناهمبند، شناسایی‌پذیر با گراف ناجابجایی هستند، همچنین گروه متناوب $A_{۱۰}$، که گراف اول همبند دارد، شناسایی‌پذیر با گراف ناجابجایی است. لازم به ذکر است که گراف اول گروه متناهی G که آن را با $\nabla(G)$ نمایش می‌دهیم به صورت زیر ساخته می‌شود:

---

[۱] P. Erdos

[۲] Neuman

مجموعه رئوس این گراف برابر $\pi(G)$ می‌باشد، جایی که $\pi(G)$ نمایانگر شمارنده‌های اول $|G|$ می‌باشد. اعداد اول p و q به عنوان رئوس $\nabla(G)$ توسط یک یال متصل می‌شود اگر و تنها اگر G شامل یک عنصر از مرتبه pq باشد.

این پایان‌نامه شامل چهار فصل است.

فصل اول شامل دو بخش است. بخش اول آن به بیان تعاریف و مفاهیم و بعضی قضایا و نتایج مقدماتی و کلیدی می‌پردازد. در بخش دوم به تعاریف مورد نیاز از گروه‌هایی از نوع لی می‌پردازیم.

فصل دوم نیز شامل دو بخش است و مرجع اصلی این فصل [۸] می‌باشد. در این فصل سه حدس زیر را بررسی می‌کنیم:

حدس اول: فرض کنید G و H گروه‌های غیر آبلی متناهی باشند به طوری که $\Gamma_G \cong \Gamma_H$. در این صورت $|G| = |H|$.

حدس دوم: فرض کنید P یک گروه ساده غیر آبلی متناهی باشد و G یک گروه باشد به قسمی که $\Gamma_G \cong \Gamma_P$، در این صورت $G \cong P$. این حدس توسط عبدالهی و دیگر مؤلفان در [۱] بیان شده است و به حدس AAM مشهور است.

در [۱] نشان داده شده است که حدس AAM به حدس تامپسون[۳] مربوط می‌شود، که در سال ۱۹۸۷ به صورت زیر بیان کرده است:

حدس سوم: اگر G یک گروه متناهی باشد به طوری که $Z(G) = ۱$ و M یک گروه ساده متناهی غیر آبلی باشد به قسمی که $N(G) = N(M)$، آن‌گاه $G \cong M$، جایی که $N(G)$ مجموعه اندازه کلاس‌های مزدوجی G را نشان می‌دهد.

فصل سوم نیز شامل دو بخش است و مرجع اصلی این فصل [۷] می‌باشد. گروه G را قابل تجزیه می‌نامیم اگر G یکریخت با حاصلضرب مستقیم از زیرگروه‌های سره‌اش باشد. در این فصل نشان خواهیم داد که اگر G و H دو گروه با مرکز بدیهی باشند و $\Gamma_G \cong \Gamma_H$، آن‌گاه G قابل تجزیه است اگر و تنها اگر H قابل تجزیه باشد، به علاوه اگر

$$G \cong G_۱ \times G_۲ \times \ldots \times G_n,$$

[۳] Thompson

آن‌گاه زیرگروه‌هایی از H مانند H_1، H_2،...، H_n وجود دارند به طوری که

$$H \cong H_1 \times H_2 \times ... \times H_n.$$

در ادامه این فصل اثبات خواهیم کرد که اگر G_1، G_2،...، G_n گروه‌های متناهی باشند به طوری که به ازای هر $i = 1, 2, ..., n$ داشته باشیم $Z(G_i) = 1$ و گروه G_i با گراف ناجابجایی شناسایی‌پذیر باشد، آن‌گاه $G_1 \times G_2 \times ... \times G_n$ با گراف ناجابجایی شناسایی‌پذیر است.

در فصل چهارم که شامل دو بخش است و مرجع اصلی آن [30] می‌باشد، شناسایی‌پذیری گروه ساده خطی خاص تصویری $L_4(9)$ را با گراف ناجابجایی بررسی می‌کنیم. لازم به ذکر است که این گروه ساده دارای گراف اول همبند است. در حقیقت در این فصل ثابت می‌کنیم که اگر G یک گروه متناهی باشد که $\Gamma_G \cong \Gamma_{L_4(9)}$، آن‌گاه $G \cong L_4(9)$.

فصل ۱

مفاهیم اولیه

بر این باوریم که خواننده با مفاهیم اولیه نظریه گروه‌ها آشناست. در این فصل برخی تعاریف و قضایایی که در فصول بعد مورد نیاز می‌باشد را با استفاده از مراجع [۲، ۳، ۲۳، ۳۲، ۳۳، ۳۴] بیان می‌کنیم.

۱.۱ تعاریف و قضایای مورد نیاز

تعریف ۱.۱.۱. فرض کنید G یک گروه باشد. عنصر $g \in G$ را یک عنصر مرکزی G نامند، اگر به ازای هر $a \in G$ داشته باشیم $ag = ga$. مجموعه‌ی تمام چنین عناصری را مرکز G گویند و آن را با $Z(G)$ نمایش می‌دهند. به سادگی نتیجه می‌شود که $Z(G) \leq G$.

تعریف ۲.۱.۱. فرض کنید $(G, .)$ یک گروه غیر آبلی باشد. گراف ناجابجایی G، که آن را با Γ_G نمایش می‌دهیم، به صورت زیر ساخته می‌شود. مجموعه رئوس Γ_G که با $V(\Gamma_G)$ نمایش داده می‌شود برابر $G - Z(G)$ می‌باشد. دو رأس x و y توسط یک یال به هم متصل می‌شوند اگر و تنها اگر $xy \neq yx$. مجموعه یال‌های Γ_G را با $E(\Gamma_G)$ نمایش می‌دهیم.

تعریف ۳.۱.۱. فرض کنید G و H دو گروه باشند. گوییم گراف‌های ناجابجایی Γ_G و Γ_H یکریخت است هرگاه یک تابع دوسویی $\phi : V(\Gamma_G) \longrightarrow V(\Gamma_H)$ وجود داشته باشد به طوری که x و y در گراف

ناجابجایی Γ_G توسط یک یال متصل می‌شوند اگر و تنها اگر $\phi(x)$ و $\phi(y)$ در گراف ناجابجایی Γ_H توسط یالی متصل شوند، یعنی اگر $x, y \in G - Z(G)$، آن‌گاه $xy \neq yx$ اگر و تنها اگر $\phi(x)\phi(y) \neq \phi(y)\phi(x)$.

تعریف ۴.۱.۱. مجموعه $\pi(n)$ را مجموعه شمارنده‌های اول عدد طبیعی n در نظر می‌گیریم. حال فرض کنید G یک گروه متناهی است، مجموعه شمارنده‌های اول $|G|$ را با $\pi(G)$ نمایش می‌دهیم.

تعریف ۵.۱.۱. گراف اول متناظر با یک گروه متناهی G را با $\nabla(G)$ نمایش می‌دهیم. مجموعه رئوس این گراف برابر $\pi(G)$ می‌باشد. اعداد اول p و q به عنوان رئوس $\nabla(G)$ توسط یک یال متصل می‌شود اگر و تنها اگر G شامل یک عنصر از مرتبه pq باشد.

تعریف ۶.۱.۱. فرض کنید G یک گروه باشد. دنباله‌ی ناتهی $W = v.e_۱v_۱e_۲v_۲...e_kv_k$ را یک گشت از $v.$ به v_k در Γ_G گوییم، هرگاه جمله‌های آن رأس‌ها و یال‌ها باشند به قسمی که به ازای $۱ \leq i \leq k$، دو انتهای یال e_i، رأس‌های $v_{i-۱}$ و v_i می‌باشند.

اگر یال‌های $e_۱, e_۲, ..., e_K$ از گشت W متمایز باشند، W را گذر می‌نامند؛ اگر علاوه بر این رأس‌های $v., v_۱... , v_k$ متمایز باشند، W را مسیر می‌نامند.

تعریف ۷.۱.۱. گوییم گراف Γ_G همبند است، اگر بین هر دو رأس آن مسیری وجود داشته باشد؛ در غیر این صورت گراف Γ_G را ناهمبند گوییم.

قضیه ۸.۱.۱. (لاگرانژ[۱]) اگر G یک گروه متناهی باشد و $H \leq G$، آن‌گاه $|G| \mid |H|$.

اثبات. به قضیه ۷.۷.۳ از [۳۳] رجوع شود. □

گزاره ۹.۱.۱. اگر a و b اعداد صحیحی باشند به طوری که $a \mid (b - ۱)$، آن‌گاه a و b نسبت به هم اولند.

اثبات. فرض کنید $d = (a, b)$ و $d \neq ۱$. می‌دانیم $d \mid a$ و $d \mid b$، از طرفی $a \mid (b - ۱)$ لذا داریم $d \mid (b - ۱)$ و از آنجا که $d \mid b$، لذا باید داشته باشیم $d = ۱$. پس به تناقض می‌رسیم و نتیجه می‌گیریم a و b نسبت به هم اولند. □

[۱] Lagrange

تعریف ۱۰.۱.۱. فرض کنید $(G, .)$ و $(H, *)$ دو گروه باشند. تابع $f : G \longrightarrow H$ را یک همریختی از گروه G به گروه H می‌نامند اگر به ازای هر $a, b \in G$ داشته باشیم

$$f(a.b) = f(a) * f(b).$$

همریختی f را یک یکریختی گویند اگر f پوشا و یک‌به‌یک باشد.

تعریف ۱۱.۱.۱. فرض کنید G یک گروه باشد.

(الف) هر همریختی $f : G \longrightarrow G$ را یک درونریختی از G می‌نامند.

(ب) هر یکریختی $f : G \longrightarrow G$ یک خودریختی از G نامیده می‌شود.

فرض کنید $a \in G$. در این صورت تابع $\phi_a : G \longrightarrow G$ که به ازای هر $x \in G$ به صورت $\phi_a(x) = axa^{-1}$ تعریف می‌شود یک خودریختی از G می‌باشد. ϕ_a را خودریختی داخلی متناظر با a از G گویند. مجموعه‌ی تمام خودریختی‌های یک گروه G را با $Aut(G)$ و مجموعه‌ی تمام خودریختی‌های داخلی آن را با $Inn(G)$ نشان می‌دهند. در این صورت $Aut(G)$ با عمل ترکیب توابع یک گروه می‌باشد و آن را گروه خودریختی‌های گروه G می‌نامند. به سادگی می‌توان دید که $Inn(G) \trianglelefteq Aut(G)$، همچنین $G/Z(G) \cong Inn(G)$. حال قرار می‌دهیم $Out(G) = \frac{Aut(G)}{Inn(G)}$ و به آن گروه خودریختی‌های خارجی G گوییم.

تعریف ۱۲.۱.۱. فرض کنید G یک گروه و X یک مجموعه غیر تهی باشد. فرض کنید به ازای هر g از G و هر x از X، عضو یکتایی از X که آن را با علامت $x.g$ نشان می‌دهیم وجود داشته باشد به طوری که

$$\forall x \in X : x \cdot ۱ = x,$$

$$\forall g_۱, g_۲ \in G, x \in X : x.(g_۱ g_۲) = (x.g_۱).g_۲$$

در این صورت گوییم G بر X عمل می‌کند و . را عمل G بر X گویند.

تعریف ۱۳.۱.۱. فرض کنید G یک گروه باشد و $H \leq G$. یک عمل از گروه H روی مجموعه G به صورت $hxh^{-۱} \longrightarrow (h, x)$ تعریف می‌شود. این عمل $h \in H$ روی G را مزدوجی با h گویند و عنصر $hxh^{-۱}$ را مزدوج x می‌نامند.

قضیه ۱۴.۱.۱. فرض کنید G یک گروه باشد که روی مجموعه X عمل می‌کند. در این صورت

(الف) رابطه $\sim$ روی G که به صورت زیر تعریف می‌شود یک رابطه هم‌ارزی است:

$x \sim x'$ اگر و تنها اگر عنصری مانند $g \in G$ وجود داشته باشد به قسمی که $x.g = x'$.

(ب) به ازای هر $x \in X$، $G_x = \{g \in G : x.g = x\}$ زیرگروهی از G است.

اثبات. به [۳۳] رجوع شود. $\square$

رده‌های هم‌ارزی رابطه فوق را مدارهای عمل G روی X گویند، و مدار $x \in X$ را با $\overline{x}$ نشان می‌دهند. زیرگروه G_x را ثابت‌ساز x می‌نامند و آن را با $stab_G(x)$ نشان می‌دهند.

تعریف ۱۵.۱.۱. یک گروه G روی مجموعه G به صورت مزدوجی عمل می‌کند. نسبت به این عمل، مدار $\overline{x} = \{gxg^{-۱} | \; g \in G\}$ از x را رده مزدوجی x گویند. یک زیرگروه H از یک گروه G روی مجموعه G به صورت مزدوجی عمل می‌کند.

نسبت به این عمل، ثابت‌ساز

$$stab_H(x) = \{h \in H : \; hxh^{-۱} = x\} = \{h \in H : \; hx = xh\}$$

از x را مرکزساز x در H می‌نامند و آن را با $C_H(x)$ نشان می‌دهند. اگر $H = G$ آن‌گاه $C_G(x)$ را مرکزساز x می‌نامند.

اگر زیرگروه H از یک گروه G روی مجموعه S از تمام زیرگروه‌های G به صورت مزدوجی عمل کند، آن‌گاه به ازای هر $K \in S$، ثابت‌ساز K یعنی

$$stab_H(K) = \{h \in H | \; hKh^{-۱} = K\}$$

را نرمال‌ساز K در H می‌نامند و آن را با $N_H(K)$ نشان می‌دهند.

زیرگروه $N_G(K)$ را نرمال‌ساز K گویند. بوضوح هر زیرگروه K در $N_G(K)$ نرمال است و $K \trianglelefteq G$ اگر و تنها اگر $N_G(K) = G$. به راحتی می‌توان نشان داد که $H \trianglelefteq N_G(H) \leq G$.

حال به ازای $H \leq G$ مرکزساز H در G را به صورت زیر تعریف می‌کنیم:

$$C_G(H) = \{g \in G : \; gh = hg \qquad \forall h \in H\}$$

آن‌گاه به راحتی می‌توان نشان داد که $Z(G) \leq C_G(H) \leq G$.

گزاره ۱۶.۱.۱. اگر $A \subseteq B$، آن‌گاه داریم $C_G(B) \subseteq C_G(A)$.

اثبات. فرض کنید $x \in C_G(B)$. در این صورت به ازای هر $b \in B$ داریم $xb = bx$. چون که $A \subseteq B$ نتیجه می‌گیریم که به ازای هر $a \in A$ داریم $xa = ax$. لذا $x \in C_G(A)$ و بنابراین $C_G(B) \subseteq C_G(A)$. □

تعریف ۱۷.۱.۱. فرض کنید X یک مجموعه غیر تهی باشد، یک تابع دوسویی $\pi : X \longrightarrow X$ یک جایگشت از X نامیده می‌شود. مجموعه همه جایگشت‌های X گروه متقارن روی X نامیده می‌شود و آن را با $SymX$ نمایش می‌دهند. یک زیرگروه G از گروه متقارن $SymX$ یک گروه جایگشتی روی X نامیده می‌شود.

گروه جایگشتی G متعدی نامیده می‌شود، اگر به ازای هر جفت عناصر مفروض x و y در X، یک جایگشت π از G وجود داشته باشد به طوری که $\pi(x) = y$.

گروه جایگشتی G نیم‌منظم گفته می‌شود اگر $stab_G(x) = ۱$، به ازای تمامی $x \in X$ و گروه جایگشتی G منظم است اگر متعدی و نیم‌منظم باشد.

عمل گروه G بر X یک همریختی $\gamma : G \longrightarrow SymX$ معین می‌کند که به این همریختی γ، یک نمایش جایگشتی G روی X گفته می‌شود. گفته می‌شود γ متعدی (منظم) است اگر $Im\gamma$ یک گروه جایگشتی متعدی (منظم) باشد.

گزاره ۱۸.۱.۱. اگر G گروهی با مرکز بدیهی باشد آن‌گاه $C_{Aut(G)}(Inn(G)) = ۱$ و در نتیجه $Aut(G)$ مرکز بدیهی دارد.

اثبات. فرض کنیم $\phi \in C_{Aut(G)}(Inn(G))$، آن‌گاه به ازای هر $g \in G$ داریم $\phi\phi_g = \phi_g\phi$، به طوری که ϕ_g یک خودریختی داخلی می‌باشد. بنابراین به ازای هر $x \in G$ و هر $g \in G$ داریم

$$\phi\phi_g(x) = \phi_g\phi(x).$$

بنا بر تعریف خودریختی داخلی می‌توان نوشت:

$$\phi(gxg^{-۱}) = g\phi(x)g^{-۱}$$

و چون ϕ یک خودریختی است داریم

$$g^{-1}\phi(g)\phi(x)\phi(g)^{-1}g = \phi(x) \qquad , \forall x \in G.$$

با استفاده از تعریف $Z(G)$، نتیجه می‌گیریم $g^{-1}\phi(g) \in Z(G)$ و چون $Z(G) = 1$ به ازای هر $g \in G$ نتیجه می‌شود $\phi(g) = g$. بنابراین ثابت کردیم $C_{Aut(G)}(Inn(G)) = 1$ و بنا بر تعریف مرکزیساز می‌دانیم $Z(Aut(G)) \leq C_{Aut(G)}(Inn(G))$، لذا نتیجه می‌شود $Z(Aut(G)) = 1$. $\square$

تعریف ۱۹.۱.۱. فرض کنید F یک مجموعه باشد که روی آن دو عمل دوتایی تعریف شده است به طوری که:

۱. F نسبت به یکی از این اعمال دوتایی یک گروه آبلی است. این عمل دوتایی را جمع گویند و آن را با $+$ نشان می‌دهند. عنصر همانی گروه آبلی $(F, +)$ را با ۰ نشان می‌دهند و آن را صفر می‌نامند.

۲. $F - \{0\}$ نسبت به عمل دوم یک گروه آبلی است. عمل دوم را ضرب گویند. عنصر همانی $(F - \{0\}, .)$ را معمولاً با ۱ نشان می‌دهند.

۳. عمل ضرب نسبت به عمل جمع توزیع‌پذیر است.

$$\forall a, b, c \in F: \qquad (b + c)a = ba + ca, \qquad a(b + c) = ab + ac$$

در این صورت مجموعه F نسبت به اعمال جمع و ضرب فوق را یک میدان گویند و آن را با نماد $(F, +, .)$ نمایش می‌دهند.

تعریف ۲۰.۱.۱. یک خودریختی میدانی روی میدان F یک تابع یک‌به‌یک و پوشای

$$\theta : F \longrightarrow F$$

می‌باشد به طوری که:

$$\theta(x + y) = \theta(x) + \theta(y),$$

$$\theta(x.y) = \theta(x).\theta(y).$$

تعریف ۲۱.۱.۱. اگر F یک میدان و V گروه آبلی جمعی باشد و یک ضرب عددی برای هر عضو c از F در هر عضو α از V تعریف شده باشد، به طوری که عضو منحصر به فرد $c\alpha$ از V را نتیجه دهد و به ازای هر

c_1 و c_2 از F و هر α و β از V داشته باشیم:

۱. $c_1(\alpha+\beta)=c_1\alpha+c_1\beta$

۲. $(c_1+c_2)\alpha=c_1\alpha+c_2\alpha$

۳. $(c_1c_2)\alpha=c_1(c_2\alpha)$

در این صورت V یک فضای برداری بر روی میدان F نامیده می‌شود.

تعریف ۲۲.۱.۱. فرض کنید V یک فضای برداری روی یک میدان F باشد. بردارهای α_1، α_2،...، α_n عضو V را وابسته خطی می‌نامیم هرگاه اسکالرهای c_1، c_2،...، c_n که همگی صفر نیستند موجود باشند به طوری که

$$c_1\alpha_1+c_2\alpha_2+\ldots+c_n\alpha_n=0.$$

در غیر این صورت بردارهای α_1، α_2،...،α_n را مستقل خطی می‌نامیم.

تعریف ۲۳.۱.۱. فرض کنید V یک فضای برداری روی یک میدان F باشد. زیرمجموعه B از V را یک پایه V گوییم، هرگاه B مستقل خطی باشد و فضای V را تولید کند. بعد فضای V عبارت است از تعداد بردارهای یک پایه V که آن را با نماد $dimV$ نمایش می‌دهند.

تعریف ۲۴.۱.۱. فرض کنید U و V دو فضای برداری روی یک میدان F باشند. تابع $T:U\to V$ را یک تبدیل خطی گوییم، هرگاه به ازای هر x و y از U و هر c در F داشته باشیم:

$$T(cx+y)=cT(x)+T(y)$$

و هر تبدیل خطی از یک فضا به خودش را یک عملگر خطی گویند.

تبدیل خطی T را نامنفرد نامیم هرگاه $T(\gamma)=0$ ایجاب کند $\gamma=0$. بدیهی است که T یک به یک است اگر و تنها اگر T نامنفرد باشد. به آسانی می‌توان دید که تبدیل‌های خطی نامنفرد آن‌هایی هستند که استقلال خطی را حفظ می‌کنند.

تعریف ۲۵.۱.۱. فرض کنید F یک میدان باشد. به ازای یک خودریختی میدانی θ از F، تابع f از U به V بین دو فضای برداری U و V روی F یک θ-نیم‌خطی یا به طور ساده نیم‌خطی است اگر به ازای هر

$x, y \in U$ و $l \in F$ داشته باشیم:

$$f(x+y) = f(x) + f(y),$$
$$f(lx) = l^{\theta} f(x),$$

جایی که l^{θ} تصویر l تحت θ را نمایش می‌دهد.

تعریف ۲۶.۱.۱. اگر H و K دو گروه باشند، آن‌گاه روی حاصلضرب دکارتی

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

عمل زیر را تعریف می‌کنیم:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

در این صورت $H \times K$ نسبت به عمل تعریف شده یک گروه است و آن را گروه حاصلضرب مستقیم خارجی H و K می‌نامیم.

مفهوم حاصلضرب مستقیم دو گروه H و K را می‌توان به هر تعداد متناهی از گروه‌ها تعمیم داد.

قضیه ۲۷.۱.۱. فرض کنید $H_1, H_2, ..., H_n \trianglelefteq G$ به طوری که $G = H_1 H_2 ... H_n$ و برای هر i برابر $1, ..., n$ داشته باشیم

$$H_i \cap H_1 H_2 ... H_{i-1} H_{i+1} ... H_n = \{1\},$$

در این صورت داریم

$$G \cong H_1 \times H_2 \times ... \times H_n = Dr \prod_{i=1}^{n} (H_i).$$

اثبات. به مرجع [۲۳] رجوع شود. □

تعریف ۲۸.۱.۱. فرض کنید H و K دو گروه دلخواه و $\phi : H \longrightarrow Aut(K)$ یک همریختی باشد به طوری که $\phi(h) = \phi_h$. در حاصلضرب دکارتی $H \times K$ عمل دوتایی زیر را تعریف می‌کنیم:

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

مجموعه‌ی $H \times K$ با عمل فوق تشکیل یک گروه می‌دهد. این گروه را حاصلضرب نیم‌مستقیم H و K با عمل ϕ می‌نامند و آن را با علامت $K \rtimes_\phi H$ نشان می‌دهند. در حالتی که ابهامی در مورد ϕ پیش نیاید، یا مشخص کردن آن مورد نیاز نباشد، به جای علامت مذکور، از علامت $K \rtimes H$ استفاده می‌شود.

تذکر ۲۹.۱.۱. اگر $n > ۳$ و $n \neq ۶$، آن‌گاه $Aut(A_n) \cong S_n$.

اثبات. فرض کنید $x \in S_n$. در این صورت خودریختی $f_x : A_n \longrightarrow A_n$ به صورت $f_x(a) = x^{-۱}ax$، به ازای هر $a \in A_n$ تعریف می‌شود، یعنی $f_x \in Aut(A_n)$. لذا همریختی $\phi : S_n \longrightarrow Aut(A_n)$ یک‌به‌یک می‌باشد چون که هسته این همریختی برابر عضو همانی گروه می‌باشد.

حال می‌دانیم $Inn(A_n) \cong \frac{A_n}{Z(A_n)}$ و چون A_n ساده است داریم $Z(A_n) = ۱$، بنابراین نتیجه می‌شود

$$A_n \cong Inn(A_n) \trianglelefteq Aut(A_n).$$

با توجه به این که $Out(A_n) = \frac{Aut(A_n)}{Inn(A_n)}$، داریم $|Aut(A_n)| = |Out(A_n)||Inn(A_n)|$، پس نتیجه می‌گیریم که $|Aut(A_n)| = ۲|A_n|$ و چون می دانیم $|S_n| = ۲|A_n|$ لذا داریم

$$|S_n| = |Aut(A_n)|.$$

در بالا اشاره کردیم که تابع ϕ یک همریختی یک‌به‌یک است، یعنی $S_n \lesssim Aut(A_n)$. چون نشان دادیم $|S_n| = |Aut(A_n)|$، لذا ϕ یک همریختی یک‌به‌یک و پوشاست. بنابراین $Aut(A_n) \cong S_n$. $\square$

تعریف ۳۰.۱.۱. فرض کنید G یک گروه و n عدد طبیعی مفروضی باشد. همچنین فرض کنید $\Gamma \leq S_n$ و $\beta \in \Gamma$. قرار دهید $K = \underbrace{G \times ... \times G}_{n}$، و تابع $\beta^* : K \to K$ را با ضابطه‌ی

$$\beta^* : (x_۱, ..., x_n) \to (x_{\beta^{-۱}(۱)}, ..., x_{\beta^{-۱}(n)})$$

تعریف می‌کنیم. به سهولت معلوم می‌شود که $\beta^* \in Aut(K)$، و تابع $\phi : \Gamma \to Aut(K)$ با ضابطه‌ی $\beta \to \beta^*$ یک تکریختی است . حاصلضرب نیم‌مستقیم $K \rtimes_\phi \Gamma$ را حاصلضرب حلقوی G و Γ می‌نامند و آن را با علامت $GW_r\Gamma$ نشان می‌دهند.

حال تعریف زیر را می‌آوریم:

فرض کنید G یک گروه دلخواه و H یک گروه متناهی باشد. با در نظر گرفتن نمایش جایگشتی H (با عمل ضرب از راست)، $\Gamma \cong H$ که در آن $\Gamma \leq S_{|H|}$. حاصلضرب حلقوی GW_rH را حاصلضرب حلقوی

G و H می‌نامیم و آن را با علامت $G \wr H$ نشان می‌دهیم.

واضح است، در حالتی که G متناهی است، $|G \wr H| = |H||G|^{|H|}$.

تعریف ۳۱.۱.۱. فرض کنید π یک مجموعه از اعداد اول باشد و $\pi' = \{p : p \notin \pi\}$.گروه G را یک π-گروه نامیم هرگاه همه شمارنده‌های اول $|G|$ در π باشند. زیرگروه H از G را یک π-هال[۲] زیرگروه از G گویند هرگاه $|H|$ یک π-عدد باشد، بدین معنی که تمام اعداد اولی که در تجزیه $|H|$ ظاهر می‌شوند در π باشند و $[G : H]$ یک π'-عدد باشد، بدین معنی که تمام اعداد اولی که در تجزیه $[G : H]$ ظاهر می‌شوند در π' باشند.

تعریف ۳۲.۱.۱. حاصلضرب همه π-زیرگروه‌های نرمال G یک π-زیرگروه نرمال G است که آن را با $O_\pi(G)$ نمایش می‌دهیم. همچنین $O^\pi(G)$ کوچکترین زیرگروه نرمال G است به طوری که $\frac{G}{O^\pi(G)}$ یک π-گروه است. اگر $\pi = \{p\}$، آن‌گاه به جای نماد $O_\pi(G)$ از نماد $O_p(G)$ و اگر $\pi = \{q : q \neq p\}$، آن‌گاه از نماد $O_{p'}(G)$ استفاده می‌کنیم.

تعریف ۳۳.۱.۱. فرض کنید G یک گروه باشد. G را کاملاً تحویلپذیر گویند اگر $G = \{۱\}$ یا G حاصلضرب مستقیم تعداد متناهی گروه‌های ساده باشد. واضح است که هر گروه ساده کاملاً تحویلپذیر است. یک گروه کاملاً تحویلپذیر را یک CR-گروه می‌نامند.

اگر G کاملاً تحویلپذیر باشد و $G = Dr\prod_{i=۱}^{n}(K_i)$ به طوری که K_iها ساده هستند، آن‌گاه داریم $Z(G) = Dr\prod_{i=۱}^{n}(Z(K_i))$. اگر K_i آبلی باشد آن‌گاه K_i دوری از مرتبه عدد اول است لذا داریم $Z(K_i) = K_i$، از این رو نتیجه می‌شود $Z(G) = G$. اگر K_i آبلی نباشد آن‌گاه $Z(K_i) = ۱$، لذا نتیجه می‌گیریم $Z(G) = ۱$. ممکن است بعضی از K_iها آبلی و بعضی دیگر غیر آبلی باشند در این صورت داریم $Z(G) \neq ۱$ لذا یک CR-گروه یک گروه با مرکز بدیهی می‌باشد اگر و تنها اگر CR- گروه یک حاصلضرب مستقیم از گروه‌های ساده غیر آبلی باشد.

تعریف ۳۴.۱.۱. فرض کنید G یک گروه باشد و $H \leq G$. در این صورت منظور از یک سری از H به G

[۲] Hall

عبارت است از

$$H = H_\circ \trianglelefteq H_۱ \trianglelefteq H_۲ \trianglelefteq ... \trianglelefteq H_n = G.$$

در این صورت به ازای هر i، $\frac{H_i}{H_{i-۱}}$ را یک عامل از سری گویند.

حال منظور از یک سری برای گروه G عبارت است از یک سری بین $\{e\}$ و G.

تعریف ۳۵.۱.۱. یک سری برای یک گروه G را آبلی گویند اگر همه‌ی عوامل سری آبلی باشد.

گروه G را حل‌پذیر گویند اگر G دارای یک سری آبلی باشد.

قضیه ۳۶.۱.۱. فرض کنید G یک گروه حل‌پذیر باشد. در این صورت هر زیرگروه و هر گروه خارج‌قسمتی از G حل‌پذیر است.

اثبات. به [۲۳] رجوع شود. □

قضیه ۳۷.۱.۱. فرض کنید گروه خارج‌قسمتی G/K حل‌پذیر باشد. در این صورت اگر K حل‌پذیر باشد آن‌گاه G نیز حل‌پذیر است.

اثبات. به [۲۳] رجوع شود. □

قضیه ۳۸.۱.۱. (هال) فرض کنید G یک گروه حل‌پذیر و ω یک مجموعه از اعداد اول باشد. در این صورت G یک ω-هال زیرگروه دارد.

اثبات. به [۲۳] رجوع شود. □

قضیه ۳۹.۱.۱. فرض کنید p و q دو عدد اول باشند به طوری که $p < q$. در این صورت اگر $p \nmid (q-۱)$ آن‌گاه تنها یک گروه از مرتبه pq وجود دارد که دوری می‌باشد.

اثبات. به قضیه ۳.۲.۸ از [۳۲] رجوع شود. □

قضیه ۴۰.۱.۱. (استدلال فراتینی[۳]) فرض کنید G یک گروه متناهی باشد و $H \trianglelefteq G$. در این صورت اگر $P \in Syl_p(H)$ آن‌گاه $G = N_G(P)H$.

[۳] Frattini

اثبات. به [۳۲] رجوع شود. □

گزاره ۴۱.۱.۱. فرض کنید G یک گروه باشد. اگر $H, K \leq G$، آن‌گاه لزوماً HK زیرگروه G نیست. اما اگر یکی از آنها مانند H در G نرمال باشد آن‌گاه $HK \leq G$ و یا اگر $HK = KH$ آن‌گاه $HK \leq G$.

تعریف ۴۲.۱.۱. یک زیرگروه K از گروه G را نرمال مینیمال در G گویند اگر

(۱) $K \neq ۱$،

(۲) $K \trianglelefteq G$،

(۳) اگر $N \leq K$ و $N \trianglelefteq G$، آن‌گاه $N = K$ یا $N = \{۱\}$.

تعریف ۴۳.۱.۱. یک زیرگروه K از گروه G را مشخصه گویند اگر

$$\forall \alpha \in Aut(G): \qquad K^{\alpha} = K.$$

تعریف ۴۴.۱.۱. گروه غیر بدیهی G را مشخصاً ساده گویند اگر و تنها اگر زیرگروه‌های مشخصه G عبارت باشند از $\{۱\}$ و G.

قضیه ۴۵.۱.۱. فرض کنید G یک گروه متناهی غیر بدیهی باشد. در این صورت G مشخصاً ساده است اگر و تنها اگر G به حاصلضرب مستقیم تعداد متناهی از زیرگروه‌های ساده خود که دو به دو یکریخت‌اند تجزیه شود.

اثبات. به قضیه ۵.۲.۵ از [۳۲] رجوع شود. □

گزاره ۴۶.۱.۱. اگر مرتبه گروه G عدد اول p باشد، آن‌گاه $|Aut(G)| = p - ۱$.

قضیه ۴۷.۱.۱. (نرمال‌ساز- مرکزساز) فرض کنید G یک گروه باشد و $H \leq G$. در این صورت:

(۱) $C_G(H) \trianglelefteq N_G(H)$؛

(۲) $N_G(H)/C_G(H) \lesssim Aut(H)$.

اثبات. به قضیه ۶.۳.۲ از [۳۲] رجوع شود. □

لم ۴۸.۱.۱. (برنساید[۴]) اگر G یک گروه ساده غیر آبلی متناهی باشد، آن‌گاه $|G|$ بر حداقل دو عدد اول متمایز بخش‌پذیر است. در حقیقت مرتبه یک گروه متناهی غیر آبلی ساده بر حداقل سه عدد اول متمایز بخش‌پذیر است.

اثبات. به [۳۳] رجوع شود. □

۲.۱ مقدماتی از جبرهای ساده از نوع لی

تعریف ۱.۲.۱. فرض کنید R حلقه‌ای یکدار و M مجموعه‌ای ناتهی باشد. M را همراه با عمل جمع $+ : M \times M \to M$ و ضرب در اسکالر $. : R \times M \to M$، R-مدول چپ می‌نامیم اگر

۱. $(M, +)$ گروهی آبلی باشد،

۲. به ازای هر دو عضو از M مثل x و y و هر عضو از R مثل r، $r(x+y) = rx + ry$،

۳. به ازای هر عضو از M مثل x و هر دو عضو از R مثل r و s، $(r+s)x = rx + sx$،

۴. به ازای هر عضو از M مثل x و هر دو عضو از R مثل r و s، $(rs)x = r(sx)$،

۵. به ازای هر عضو از M مثل x داشته باشیم $1x = x$;

مانند تعریف R-مدول چپ، می‌توانیم R-مدول راست را نیز تعریف کنیم. اگر R حلقه‌ای جابجایی باشد و M، R-مدول چپ، آن‌گاه M با تعریف ضرب در اسکالر $. : M \times R \to M$ به صورت $m.r = rm$ به طور طبیعی به R-مدولی راست تبدیل می‌شود.

فرض کنید M و N دو مجموعه ناتهی باشند. $\mathbb{Z}^{(M \times N)}$ را مجموعه تمام حاصل جمع‌های صوری مثل $\Sigma_{i=1}^{t} n_i(x_i, y_i)$ در نظر می‌گیریم به طوری که

$$\mathbb{Z}^{(M \times N)} = \{\Sigma_{i=1}^{t} n_i(x_i, y_i) : t \geq 1, n_i \in \mathbb{Z}, (x_i, y_i) \in M \times N\}.$$

برای راحتی کار، $1(x,y)$ را با (x,y) و $0(x,y)$ را با ۰ نمایش می‌دهیم. هر دو عضو دلخواه از $\mathbb{Z}^{(M \times N)}$ را می‌توانیم به صورت $\Sigma_{i=1}^{t} n_i(x_i, y_i)$ و $\Sigma_{i=1}^{t} n'_i(x_i, y_i)$ در نظر بگیریم. تساوی دو عضو از $\mathbb{Z}^{(M \times N)}$

[۴] Burnside