بسم الله الرحمن الرحیم

دانشکده علوم ریاضی

گروه ریاضی محض

پایان‌نامه کارشناسی ارشد

بیش‌ترین تعداد یال در گراف‌های توانی گروه‌های متناهی

الهام محمودی

استاد راهنما

دکتر سید حیدر جعفری

آبان ۱۳۹۵

تقدیم به

پدر و مادر مهربانم

اولین معلّمان زندگی من...

سپاس گزاری...

سپاس بی کران پروردگار یکتا را که هستیمان بخشید و به طریق علم و دانش رهنمونمان شد و به همنشینی رهروان علم و دانش مفتخرمان نمود و خوشه چینی از علم و معرفت را روزیمان ساخت.
در آغاز بر خود لازم می‌دانم از کسانی که مرا در دوران تحصیل و هم‌چنین در به پایان رساندن این پایان‌نامه یاری کردند، تشکر و قدردانی کنم. نخست بوسه می‌زنم بر دستان پدر فداکار و مادر دلسوزم و بعد از خدا ستایش می‌کنم وجود مقدسشان را که همواره حامی و مشوق من در راه تحصیل علم بودند و امیدوارم با اتمام این مجموعه توانسته باشم ذره‌ای از زحمات بی‌دریغشان را جبران نمایم.
سپاس بی‌پایان از استاد راهنمای ارجمندم، دکتر سید حیدر جعفری که همواره با صبر و شکیبایی پاسخگوی پرسش‌های من بودند و قطعاً بدون راهنمایی‌های ارزنده ایشان این مجموعه به انجام نمی‌رسید.
و در آخر از اساتید گرامی، دکتر ابراهیم هاشمی و دکتر مهدی رضا خورسندی که زحمت داوری این پایان‌نامه را بر عهده گرفتند و مرا در بهتر به پایان رساندن آن راهنمایی کردند، صمیمانه تشکر می‌کنم.

الهام محمودی
آبان ۱۳۹۵

تعهد نامه

اینجانب **الهام محمودی** دانشجوی کارشناسی ارشد رشته **ریاضی محض** **دانشکده علوم ریاضی** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان **بیش‌ترین تعداد یال در گراف‌های توانی گروه‌های متناهی** ، تحت راهنمایی **دکتر سید حیدر جعفری** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های دیگر پژوهش‌گران، به مرجع مورد استفاده استناد شده است.
- مطالب این پایان‌نامه، تاکنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ‌جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود تعلق دارد، و مقالات مستخرج با نام “ دانشگاه شاهرود “ یا “ Shahrood University of Technology “ به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آوردن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده) شده است، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

الهام محمودی

آبان ۱۳۹۵

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان‌نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

گراف توانی نیم‌گروه S، $\mathcal{P}(S)$، گرافی با مجموعه رئوس S است که دو رأس $a,b \in S$ مجاورند اگروتنها اگر $a \neq b$ و برای برخی اعداد صحیح مثبت m، $a^m = b$ یا $b^m = a$. گراف توانی گروه G، $\mathcal{P}(G)$، نیز به‌طور مشابه تعریف می‌شود. در این پایان‌نامه، رده همه نیم‌گروه‌های S را، که $\mathcal{P}(S)$ همبند یا کامل است، مشخص می‌کنیم. به عنوان نتیجه ثابت می‌کنیم که $\mathcal{P}(G)$ برای هر گروه متناهی G، همبند بوده و $\mathcal{P}(G)$ کامل است اگروتنها اگر برای عدد اول p و $m \in \mathbb{N}$، G یک گروه دوری از مرتبه ۱ یا p^m باشد. سپس تعداد یال‌های $\mathcal{P}(G)$ را برای گروه متناهی G محاسبه می‌کنیم و نشان می‌دهیم در میان همه گروه‌های متناهی از مرتبه داده شده، گروه دوری از آن مرتبه، بیش‌ترین تعداد یال را در گراف توانی‌اش دارد.
هم‌چنین درباره مسطح بودن و همبندی رأسی گراف‌های توانی گروه‌های دوری متناهی، دووجهی و دودوری به بحث می‌پردازیم.

کلمات کلیدی : نیم‌گروه، گروه، گروه دوری، p–گروه، گراف توانی، گراف همبند، همبندی، گروه دووجهی، گروه دودوری.

فهرست مطالب

پیشگفتار

در سال ۱۹۶۴، بوساک [1] [۵] به مطالعه گراف‌های خاصی روی نیم‌گروه‌ها پرداخت. مطالعه گراف توانی نیم‌گروه‌ها و گروه‌ها توسط چندین نویسنده انجام شد. کلارو و کویین [2] [۱۴]، گراف توانی جهت‌دار نیم‌گروه S، $\overrightarrow{\mathcal{P}}(S)$، را گرافی تعریف کردند که همه عناصر S، رأس هستند و برای $u, v \in S$ و عدد صحیح مثبت m، یال جهت‌دار از u به v وجود دارد زمانی‌که $u \neq v$ و $v = u^m$.
در [۶] کامرون[3] ثابت کرد که برای یک گروه دوری متناهی G از مرتبه توانی از یک عدد غیراول n، مجموعه رئوس T از $\mathcal{P}(G)$، که با همه رئوس دیگر $\mathcal{P}(G)$ مجاورند، همانی و مولدهای G هستند لذا

$$|T| = ۱ + \phi(n)$$

که $\phi(n)$ تابع فی اویلر [4] است.
این پایان‌نامه شامل چهار فصل است که فصل اول را تعاریف پایه تشکیل می‌دهد.
در فصل دوم به تعریف گراف توانی نیم‌گروه‌ها و مفهوم خودتوان در نیم‌گروه‌ها می پردازیم و نشان می‌دهیم که گراف توانی نیم‌گروه متناهی S، $\mathcal{P}(S)$، همبند است اگروتنهااگر S شامل یک خودتوان واحد باشد.
در ادامه گراف توانی نیم‌گروه ضربی $\mathbb{Z}_n$ از اعداد صحیح به پیمانه n، $\mathcal{P}(\mathbb{Z}_n)$، را در نظر می‌گیریم و مولفه‌های همبندی آن را مشخص می‌کنیم.
در فصل سوم این پایان‌نامه، به مفهوم گراف توانی جهت‌دار و گراف توانی گروه‌ها می‌پردازیم.
در ادامه این فصل به بررسی گراف‌های توانی گروه‌های متناهی و گروه دوری از همان مرتبه می‌پردازیم و با درنظر گرفتن حالت‌های مختلف، پیرامون تعداد یال‌ها در گراف‌های توانی گروه‌های متناهی و گروه دوری از همان مرتبه بحث می‌کنیم.
از آنجایی‌که در فصل دوم این پایان‌نامه اشاره شد که برای هر گروه متناهی G، $\mathcal{P}(G)$، همبند است، زیرا عنصر همانی G با همه رئوس دیگر $\mathcal{P}(G)$ مجاور است، فصل چهارم این پایان‌نامه مربوط به این مسئله است که اگر عنصر همانی از $\mathcal{P}(G)$ حذف شود، دراین‌صورت گراف به‌دست آمده همبند است یا خیر و اگر همبند باشد دراین‌صورت حذف کدام رئوس، گراف را ناهمبند می‌کند؟
به عبارت دیگر مسئله اصلی، همبندی $\mathcal{P}(G)$ است. در این پایان‌نامه، نشان می‌دهیم که گراف توانی گروه‌های دودوری،۲ -همبند است درحالی‌که گراف توانی گروه‌های دووجهی، ۱-همبند است.

[1] J. Bosak

[2] A.V. Kelarev , S.J. Quinn

[3] P.J. Cameron

[4] Euler phi function

هم‌چنین در این فصل، شرط لازم و کافی برای مسطح بودن گراف‌های توانی گروه‌های دووجهی و گروه‌های دودوری را می‌یابیم.
مطالب این پایان‌نامه برگرفته از سه مقاله زیر است:

- I. Chakrabarty, S. Ghosh and M.K. Sen, *Undirected power graphs of semigroups*, Semigroup Forum, **78**, 410–426, 2009.

- S. Chattopadhyay and P. Panigrahi, *Connectivity and planarity of power graphs of finite cyclic, dihedral and dicyclic groups*, J. Algebra and Discrete Mathematics, **18**, 1, 42–49, 2014.

- B. Curtin and G.R. Pourgholi, *Edge-maximality of power graphs of finite cyclic groups*, J. Algebra Comb, 313–330, 2014.

فصل ۱

تعاریف و مفاهیم پایه

۱.۱ مفاهیم اولیه نظریه گروه‌ها

تعریف ۱.۱.۱. فرض کنیم G یک گروه باشد. مرکز گروه G را با نماد $Z(G)$ نشان داده و به‌صورت

$$Z(G) = \{a \in G \mid \forall b \in G, ab = ba\}$$

تعریف می‌کنیم.

تعریف ۲.۱.۱. گروه G را متناهی مولد گوییم درصورتی‌که زیرمجموعه‌ای متناهی مانند X داشته باشد به‌طوری‌که $G = \langle X \rangle$. دراین‌صورت X را یک مولد G می‌نامیم و می‌گوییم X، گروه G را تولید می‌کند. گروه G را دوری خوانیم هرگاه، G با یک عضو تولید شود.

تعریف ۳.۱.۱. فرض کنیم H یک زیرگروه G باشد و $x \in G$. رده هم‌ارزی شامل عضو x، عبارت است از $\{hx \mid h \in H\}$. این مجموعه را با علامت Hx نشان می‌دهیم و آن را همدسته راست H (در G) شامل x می‌نامیم.

از هر همدسته راست H، یک و تنها یک عضو مانند t انتخاب می‌کنیم و مجموعه چنین اعضایی را T می‌نامیم. واضح است که هرگاه $t_۱$ و $t_۲$ دو عضو متمایز T باشند، آن‌گاه $Ht_۱ \neq Ht_۲$ و $Ht_۱ \cap Ht_۲ = \emptyset$ و در نتیجه $G = \bigcup\limits_{t \in T} Ht$. مجموعه T را یک تراگرد راست H در G می‌نامیم.

تعریف ۴.۱.۱. فرض کنیم X زیرمجموعه‌ای از گروه G باشد. هسته X عبارت است از زیرگروه نرمال تولیدشده با همه زیرگروه‌های نرمال G که جزء X اند. هسته X را با $\mathrm{Core}_G(X)$ (یا به اختصار با $\mathrm{Core}(X)$) نشان می‌دهیم.

درصورتی‌که X حاوی هیچ زیرگروه نرمال G نباشد، برطبق قرارداد، $\mathrm{Core}(X) = ۱$.

تعریف ۵.۱.۱. فرض کنیم G و H دو گروه باشند. تابع $f : G \to H$ را یک همریختی نامیم هرگاه به ازای هر x و y از G،

$$(xy)f = (x)f(y)f.$$

مجموعه همه همریختی‌های از G به H را با $\mathrm{Hom}(G,H)$ نشان می‌دهیم.

اگر $f : G \to H$ یک همریختی باشد، تصویر f و هسته f، که به‌ترتیب با علامت‌های $\mathrm{Im}f$ و $\mathrm{Ker}f$ نشان داده می‌شوند، به صورت زیر تعریف می‌کنیم :

$$\mathrm{Im}f = \{xf \mid x \in G\},$$
$$\mathrm{Ker}f = \{x \in G \mid xf = ۱\}.$$

تعریف ۶.۱.۱. فرض کنیم G یک گروه باشد و $U \subseteq G$. مرکزساز U در G را به صورت زیر تعریف می‌کنیم :

$$\{g \in G \mid \forall u \in U,\ ug = gu\}$$

و آن را با علامت $C_G(U)$ نشان می‌دهیم. (یا مختصرا $C(U)$)

تعریف ۷.۱.۱. فرض کنیم G یک گروه باشد و $H \leq G$. زیرگروه H را یک زیرگروه مشخصه G می‌نامیم درصورتی‌که به ازای هر خودریختی G مانند τ، $H\tau \leq H$ که در آن $H\tau = \{h\tau \mid h \in H\}$. هرگاه H زیرگروه مشخصه G باشد، می‌نویسیم $H \ \mathrm{ch}\ G$.

گزاره ۸.۱.۱. *فرض کنیم H و K دو زیرگروه از گروه G باشند و $H \ \mathrm{ch}\ K$.*

(الف) اگر $K \ \mathrm{ch}\ G$، آن‌گاه $H \ \mathrm{ch}\ G$.

(ب) اگر $K \lhd G$، آن‌گاه $H \lhd G$.

برهان. به گزاره ۵.۸.۲ مرجع [۲۱] مراجعه شود. □

تعریف ۹.۱.۱. فرض کنیم X مجموعه‌ای ناتهی باشد. هر تناظر دوسویی مانند $f : X \to X$ را یک جایگشت X می‌گوییم.
مجموعه همه جایگشت‌های X با عمل ترکیب توابع، تشکیل یک گروه می‌دهد. این گروه را گروه متقارن بر X می‌خوانیم و آن را با S_X نشان می‌دهیم.

قضیه ۱۰.۱.۱. *فرض کنیم G یک گروه باشد و $H \leq G$. به‌علاوه فرض کنیم X مجموعه همه همدسته‌های راست (چپ) H در G باشد. دراین‌صورت یک همریختی مانند $\varphi : G \to S_X$ وجود دارد به‌طوری‌که $\mathrm{Ker}\varphi = \mathrm{Core}_G(H)$. بنابراین،*

$$\frac{G}{\mathrm{Core}_G(H)} \hookrightarrow S_X.$$

برهان. به قضیه ۴.۱.۲ مرجع [۲۰] مراجعه شود. □

نتیجه ۱۱.۱.۱. *فرض کنیم $G \leq H$ و $|G:H| = n$، که در آن n عددی طبیعی است. دراین‌صورت G زیرگروه نرمالی مانند N دارد به‌طوری‌که $N \leq H$ و $|\frac{G}{N}||n!$.*

نتیجه ۱۲.۱.۱. *فرض کنیم G گروهی متناهی و p کوچک‌ترین عدد اولی باشد که $|G|$ را عاد کند. دراین‌صورت، اگر H زیرگروهی از G باشد به‌طوری‌که $|G:H| = p$، آن‌گاه $H \lhd G$.*

برهان. به موجب نتیجه ۱۱.۱.۱، G زیرگروه نرمالی مانند N دارد که $N \leq H$ و $|\frac{G}{N}||p!$. بنابر فرض $|G| = p|H|$. پس

$$|\frac{H}{N}||(p-۱)!$$

از اینجا لازم می‌آید که $|\frac{H}{N}| = ۱$، زیرا درغیراین‌صورت $|H|$ و درنتیجه $|G|$ عامل اولی مانند q دارد که بنابر فرض باید از p ناکمتر باشد و این متناقض است با $q \mid (p-۱)!$. □

تعریف ۱۳.۱.۱. فرض کنیم H زیرگروه دلخواهی از G باشد. مجموعه

$$N_G(H) = \{g \in G \mid H^g = H\}$$

نرمال‌ساز H در G نامیده می‌شود.

دو قضیه زیر برگرفته از قضایای ۴.۳.۲ و ۵.۳.۲ مرجع [۲۰] هستند.

قضیه ۱۴.۱.۱. *فرض کنیم G یک گروه باشد و $H, K \leq G$. با فرض $H \leq K$، $H \lhd K$ اگروتنها اگر $K \leq N_G(H)$. به عبارت دیگر، $N_G(H)$ بزرگ‌ترین زیرگروه G است که H در آن نرمال است. به‌خصوص $H \lhd G$ اگروتنها اگر $G = N_G(H)$.*

قضیه ۱۵.۱.۱. *فرض کنیم G یک گروه باشد و $H \leq G$. دراین‌صورت*

(الف) $C_G(H) \leq N_G(H)$،

(ب) $Z(G) \leq C_G(H)$.

قضیه ۱۶.۱.۱. *(قضیه نرمال‌ساز-مرکزساز) فرض کنیم G یک گروه باشد و $H \leq G$. دراین‌صورت*

(الف) $C_G(H) \lhd N_G(H)$،

(ب) $\frac{N_G(H)}{C_G(H)} \hookrightarrow \mathrm{Aut}(H)$.

برهان. به قضیه ۶.۳.۲ مرجع [۲۰] مراجعه شود. □

تعریف ۱.۱.۱۷. فرض کنیم G یک گروه متناهی و حاصل‌ضرب مستقیم زیرگروه‌های نرمال U و V باشد. دراین‌صورت، علامت زیر را به کار می‌بریم.

$$G = U \times V = \{uv \mid u \in U, v \in V\}.$$

تعریف ۱.۱.۱۸. گروه G حاصل‌ضرب نیم‌مستقیم داخلی زیرگروه نرمال U و زیرگروه V است هرگاه $G = UV$ و $U \cap V = \{e\}$.

تعریف ۱.۱.۱۹. فرض کنیم H و K دو گروه دلخواه و $\varphi : H \to \mathrm{Aut}(K)$ یک همریختی باشد. (به ازای هر h از H، تصویر h تحت φ را با φ_h نشان می‌دهیم.) در حاصل‌ضرب دکارتی $H \times K$ عمل دوتایی زیر را تعریف می‌کنیم:

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

مجموعه $H \times K$ با عمل فوق تشکیل یک گروه می‌دهد. این گروه را حاصل‌ضرب نیم‌مستقیم خارجی H و K با عمل φ می‌نامیم و آن را با علامت $H \ltimes_\varphi K$ نشان می‌دهیم.

قضیه ۱.۱.۲۰. *فرض کنیم $G = H \ltimes_\varphi K$ که در آن H و K دو گروه و $\varphi : H \to \mathrm{Aut}(K)$ یک همریختی است. دراین‌صورت G زیرگروه نرمالی مانند N و زیرگروهی مانند M دارد که $H \cong M$ و $N \cong K$ به‌طوری‌که $G = MN$ و $M \cap N = 1$.*

برهان. کافی است M و N را به صورت زیر تعریف کنیم :

$$M = \{(h, 1) \mid h \in H\}, \quad N = \{(1, k) \mid k \in K\}.$$

$\square$

لم ۱.۱.۲۱. *(قضیه شور- زاسنهاوس) [1] فرض کنیم G یک گروه متناهی و K یک زیرگروه نرمال آن باشد که $(|K|, |G : K|) = 1$. دراین‌صورت G، حاصل‌ضرب نیم‌مستقیم خارجی K و $\frac{G}{K}$ است. بویژه، یک زیرگروه H از G با مرتبه $|G : K|$ وجود دارد به طوری که در $G = HK$ و $H \cap K = \{e\}$ صدق می‌کند.*

برهان. به قضیه ۱۰.۳۰ مرجع [۱۷] مراجعه شود. $\square$

تعریف ۱.۱.۲۲. فرض کنیم G یک گروه و p یک عدد اول باشد. گروه G را یک p-گروه می‌نامیم درصورتی‌که مرتبه هر عضو G، توانی صحیح و نامنفی از p باشد.
زیرگروه H از G را یک p- زیرگروه G گوییم درصورتی‌که H یک p-گروه باشد.

نتیجه ۱.۱.۲۳. *اگر G یک p-گروه متناهی باشد، آن‌گاه مرتبه G به صورت p^α است که در آن α یک عدد صحیح نامنفی است.*

---
[1] The Schur-Zassenhaus theorem

تعریف ۲۴.۱.۱. p-گروه آبلی متناهی G را آبلی مقدماتی (یا مختصرا مقدماتی) می‌گوییم درصورتی‌که مرتبه هر عضو نابدیهی G، عدد اول p باشد.

لم ۲۵.۱.۱. *فرض کنیم p یک عدد اول فرد و P یک p-گروه ناآبلی با زیرگروه دوری از اندیس p باشد. دراین‌صورت $P \cong \mathbb{Z}_{p^{\alpha-1}} \rtimes_{\varphi} \mathbb{Z}_p$.*
مرتبه مرکز P، $p^{\alpha-2}$ است و P نمایش زیر را دارد :

$$P \cong M_{p^\alpha} = \langle a, b \mid a^{p^{\alpha-1}} = b^p = 1, b^{-1}ab = a^{1+p^{\alpha-2}} \rangle.$$

برهان. به قضیه ۲.۱ مرجع [۴] مراجعه شود. □

قضیه ۲۶.۱.۱. *(کوشی) فرض کنیم G یک گروه متناهی باشد و $p||G|$، که در آن p یک عدد اول است. دراین‌صورت G عضوی از مرتبه p دارد.*

برهان. به قضیه ۱.۱.۴ مرجع [۲۰] مراجعه شود. □

تعریف ۲۷.۱.۱. فرض کنیم G یک گروه متناهی از مرتبه n باشد و $n = p^\alpha n'$ که در آن α یک عدد صحیح نامنفی است و p عدد اولی است که $p \nmid n'$. دراین‌صورت هر زیرگروه G از مرتبه p^α را یک p-زیرگروه سیلوی G می‌نامند.

قضیه ۲۸.۱.۱. *(قضیه اول سیلو) فرض کنیم G گروهی از مرتبه $p^n m$ باشد که در آن p عددی اول است، $n \geq 1$ و $(p, m) = 1$. دراین‌صورت برای هر عدد صحیح $1 \leq i \leq n$، G زیرگروهی از مرتبه p^i دارد و هر زیرگروه از مرتبه p^i $(0 \leq i < n)$ در یک زیرگروه از مرتبه p^{i+1} نرمال است.*

برهان. به قضیه ۳.۹.۲ مرجع [۲۱] مراجعه شود. □

تعریف ۲۹.۱.۱. فرض کنیم G یک گروه متناهی و p یک عدد اول باشد. دراین‌صورت مجموعه همه p-زیرگروه‌های سیلوی G را با $\mathrm{Syl}_p(G)$ نشان می‌دهیم و تعداد اعضای مجموعه اخیر را با $n_p(G)$ (یا مختصرا با n_p) نمایش می‌دهیم.

در لم و نتیجه بعدی، G را یک گروه متناهی در نظر می‌گیریم و برای زیرمجموعه ناتهی B از G قرار می‌دهیم $\psi(B) = \sum_{x \in B} o(x)$ که $o(x)$ مرتبه عنصر x است.

لم ۳۰.۱.۱. *فرض کنیم P یک p-زیرگروه سیلوی دوری نرمال G باشد. $x \in G$ را در نظر می‌گیریم و فرض می‌کنیم همدسته Px یک عنصر از $\frac{G}{P}$ از مرتبه m باشد. دراین‌صورت*

$$\psi(Px) \leq m\psi(P),$$

به‌علاوه تساوی برقرار است اگروتنها اگر x، با عناصر P جابه‌جا شود.

برهان. چون m، $o(x)$ را عاد می‌کند، عدد صحیح q وجود دارد که $o(x) = mq$. دراین‌صورت $q = o(x^m)$ و چون $x^m \in P$، می‌توان دید که q توانی از p است. اما m، $|\frac{G}{P}|$ را، که به p بخش‌پذیر نیست، عاد می‌کند لذا، q و m نسبت به هم اول هستند و یک عدد صحیح n وجود دارد به‌طوری‌که $qn \equiv ۱$ (به پیمانه m). حال $o(x^q) = m$ و می‌نویسیم $y = (x^q)^n$ لذا چون n نسبت به m اول است، $o(y) = m$. هم‌چنین

$$Py = Px^{qn} = (Px)^{qn} = Px$$

و به‌علاوه چون P آبلی است، y، با عناصر P جابه‌جا می‌شود اگروتنها اگر x، با عناصر P جابه‌جا شود. بنابراین می‌توانیم x را به‌جای y قرار دهیم و فرض کنیم $o(x) = m$.
برای هر $u \in P$، ادعا می‌کنیم که $o(ux) \leq mo(u)$ و تساوی برقرار است اگروتنها اگر x، با u جابه‌جا شود. چون P دوری است، $\langle u \rangle$ در P مشخصه است و بنابراین $\langle u \rangle \lhd G$ و $\langle u \rangle\langle x \rangle$ یک زیرگروه است. حال ux یک عنصر $\langle u \rangle\langle x \rangle$ است و لذا

$$o(ux) \leq |\langle u \rangle\langle x \rangle| = mo(u)$$

همان‌طور که می‌خواستیم.
هم‌چنین اگر تساوی برقرار باشد دراین‌صورت، $\langle u \rangle\langle x \rangle$ یک گروه دوری است و لذا x، با u جابه‌جا می‌شود. به عکس اگر x، با u جابه‌جا شود آن‌گاه، چون $o(x)$ و $o(u)$ نسبت به هم اول هستند، داریم

$$o(ux) = o(u)o(x) = mo(u).$$

حال

$$\psi(Px) = \sum_{u \in P} o(ux) \leq \sum_{u \in P} mo(u) = m \sum_{u \in P} o(u) = m\psi(P).$$

هم‌چنین تساوی برقرار است اگروتنها اگر برای هر $u \in P$، x با u جابه‌جا شود یا معادلاً x، با عناصر P جابه‌جا شود. $\square$

نتیجه ۳۱.۱.۱. *فرض کنیم P یک p-زیرگروه سیلوی دوری نرمال G باشد. دراین‌صورت*

$$\psi(G) \leq \psi(P)\psi(\frac{G}{P}),$$

تساوی برقرار است اگروتنها اگر P در G مرکزی باشد.

برهان. فرض کنیم همدسته Px، عنصری از $\frac{G}{P}$ باشد. با بکار بردن لم قبل، برای هر همدسته P در G داریم

$$\psi(G) = \sum_{Px \in \frac{G}{P}} \psi(Px) \leq \sum_{Px \in \frac{G}{P}} o(Px)\psi(P) = \psi(P) \sum_{Px \in \frac{G}{P}} o(Px) = \psi(P)\psi(\frac{G}{P}).$$

بنابراین $\psi(G) \leq \psi(P)\psi(\frac{G}{P})$ و طبق لم قبل، تساوی برقرار است اگروتنهااگر هر عنصر $x \in G$، با عناصر P جابه‌جا شود. $\square$

لم ۳۲.۱.۱. *فرض کنیم G یک گروه و H زیرگروهی از آن باشد که $|G:H| = n$. قرار می‌دهیم $\Omega = \{1, 2, \cdots, n\}$. فرض کنیم $\{x_1, \ldots, x_n\}$ و $\{y_1, \ldots, y_n\}$ دو تراگرد راست H در G باشند و $a \in G$. دراین‌صورت به ازای هر i از Ω، یک و تنها یک j از Ω، و نیز یک و تنها یک h_i از H وجود دارد به‌طوری‌که*

$$y_i a = h_i x_j.$$

به‌علاوه تابع $\sigma : \Omega \to \Omega$ با ضابطه $i\sigma = j$، یک جایگشت Ω است.

برهان. عضو دلخواه ولی ثابت i را از Ω درنظر می‌گیریم. چون همدسته‌های راست H در G، گروه G را افراز می‌کنند، $y_i a$ به یک و تنها یک همدسته راست مانند Hx_j تعلق دارد. درنتیجه H عضوی مانند h_i دارد به‌طوری‌که

$$y_i a = h_i x_j.$$

به آسانی دیده می‌شود که h_i یکتاست. حال فرض کنیم $i, k \in \Omega$ و $i\sigma = k\sigma = j$. بنابراین برای $u_i \in H$، $y_k a = u_i x_j$. از اینجا،

$$u_i^{-1} y_k a = h_i^{-1} y_i a$$

و درنتیجه $u_i h_i^{-1} = y_k y_i^{-1}$. بنابراین $y_k y_i^{-1} \in H$ یعنی $Hy_k = Hy_i$.
حال چون $\{y_1, \ldots, y_n\}$ یک تراگرد راست H در G است، $k = i$. یعنی σ یک‌به‌یک است. بنابراین $\sigma \in S_n$. $\square$

تعریف ۳۳.۱.۱. فرض کنیم G یک گروه و H زیرگروهی از آن باشد که $|G:H| = n$. فرض کنیم $\{x_1, \ldots, x_n\}$ یک تراگرد راست H در G باشد، تابع $T : G \to \frac{H}{H'}$ با ضابطه

$$aT = \prod_{i=1}^{n} H' h_i$$

را که در آن $x_i a = h_i x_j$ (مطابق لم قبل)، انتقال می‌گوییم.

قضیه ۳۴.۱.۱. *با فرض‌ها و علامت‌های تعریف فوق،*

(الف) *T مستقل از انتخاب تراگرد راست H در G است،*

(ب) *T یک همریختی است.*

برهان. به قضیه ۲.۱.۱۲ مرجع [۲۰] مراجعه شود. $\square$

قضیه ۳۵.۱.۱. *فرض کنیم G یک گروه و H زیرگروهی از آن باشد که $|G:H|=n$. فرض کنیم $a\in G$. دراین‌صورت اعدادی طبیعی مانند $r_۱$، ...، r_m و اعضایی از G مانند $g_۱$، ...، g_m موجودند به‌طوری‌که*

(الف) $\sum_{t=۱}^{m} r_t = n$،

(ب) به ازای هر t که $۱\le t\le m$، $g_t a^{r_t} g_t^{-۱}\in H$،

(ج) $aT=\prod_{t=۱}^{m} H'(g_t a^{r_t} g_t^{-۱})$.

برهان. ابتدا $\{x_۱,\ldots,x_n\}$ را یک تراگرد راست H در G می‌گیریم. پس $\sigma\in S_n$ و $h_۱,\cdots,h_n\in H$ وجود دارند که $x_i a = h_i x_{i\sigma}$. فرض کنیم $\sigma=\sigma_۱\ldots\sigma_m$ تجزیه σ به دورهای جدا از هم باشد (با ملحوظ داشتن دورهای به طول ۱).

فرض کنیم $۱\le t\le m$ و $\sigma_t=(j_{t_۱}\ldots j_{t_{r_t}})$. معلوم است که $\sum_{t=۱}^{m} r_t=n$. برای اختصار و سهولت در نوشتن، فرض می‌کنیم $\sigma_t=(j_۱\ldots j_r)$. با این قرارداد، داریم

$$\begin{aligned}
x_{j_۱}a &= h_{j_۱}x_{j_۱\sigma}=h_{j_۱}x_{j_۲},\\
x_{j_۲}a &= h_{j_۲}x_{j_۲\sigma}=h_{j_۲}x_{j_۳},\\
&\vdots\\
x_{j_{r-۱}}a &= h_{j_{r-۱}}x_{j_r},\\
x_{j_r}a &= h_{j_r}x_{j_۱}.
\end{aligned}$$

اینک به آسانی می‌بینیم که

$$\begin{aligned}
x_{j_۱}a^r x_{j_۱}^{-۱} &= x_{j_۱}a x_{j_۲}^{-۱} x_{j_۲} a^{r-۱} x_{j_۱}^{-۱}\\
&= h_{j_۱} x_{j_۲} a x_{j_۳}^{-۱} x_{j_۳} a^{r-۲} x_{j_۱}^{-۱}\\
&= h_{j_۱} h_{j_۲}\ldots x_{j_r} a x_{j_۱}^{-۱}\\
&= h_{j_۱} h_{j_۲}\ldots h_{j_r}.
\end{aligned}$$

بنابراین، $x_{j_۱}a^r x_{j_۱}^{-۱}\in H$. حال به ازای هر t که $۱\le t\le m$، قرار می‌دهیم : $g_t=x_{j_۱}=x_{j_{t_۱}}$. ملاحظه می‌کنیم که

$$\begin{aligned}
aT &= \prod_{i=۱}^{n} H'h_i=\prod_{i=۱}^{n} H'h_{i\sigma}\\
&= H'(\ldots)\ldots(h_{j_۱}h_{j_۲}\ldots h_{j_r})\ldots(\ldots),
\end{aligned}$$

که در آن عوامل داخل پرانتزها به ترتیب مربوط به جایگشت‌های σ_1، …، σ_t، …، σ_mاند. از آن‌جا

$$aT = H'(g_1a^{r_1}g_1^{-1})\dots(g_ta^{r_t}g_t^{-1})\dots(g_ma^{r_m}g_m^{-1}),$$

و حکم ثابت می‌شود. $\square$

قضیه ۳۶.۱.۱. *فرض کنیم G یک گروه باشد و $H \leq Z(G)$. دراین‌صورت اگر $|G:H| = n$، آن‌گاه به ازای هر $a \in G$، $aT = a^n$.*

برهان. چون H آبلی است، $\frac{H}{H'} \cong H$. بنابراین $\frac{H}{H'}$ را با H یکسان می‌گیریم و درنتیجه انتقال T را می‌توان از G به H درنظر گرفت.
فرض کنیم $a \in G$. طبق لم ۳۵.۱.۱، اعدادی طبیعی مانند r_1، …، r_m و اعضایی از G مانند g_1، …، g_m موجودند به‌طوری‌که $\sum_{t=1}^{m} r_t = n$ و به ازای هر t که $1 \leq t \leq m$، $g_ta^{r_t}g_t^{-1} \in H$ و $aT = \prod_{t=1}^{m}(g_ta^{r_t}g_t^{-1})$. حال فرض کنیم t عدد طبیعی دلخواهی باشد به‌طوری‌که $1 \leq t \leq m$. چون H نرمال است، $g_t^{-1}(g_ta^{r_t}g_t^{-1})g_t \in H$. یعنی $a^{r_t} \in H$. ولی چون H زیرگروه مرکزی است، $g_ta^{r_t}g_t^{-1} = a^{r_t}$. بنابراین $aT = \prod_{t=1}^{m} a^{r_t} = a^n$. $\square$

نتیجه ۳۷.۱.۱. *فرض کنیم G یک گروه باشد و $H \leq Z(G)$. دراین‌صورت اگر $|G:H| = n$، آن‌گاه تابع $T: G \to H$ با ضابطه $aT = a^n$ یک همریختی است.*

تعریف ۳۸.۱.۱. فرض کنیم p یک عدد اول، G یک گروه متناهی و P یک p-زیرگروه سیلوی G باشد. یک p-متمم در G، یک زیرگروه با اندیس برابر با مرتبه p-زیرگروه سیلو است.

قضیه ۳۹.۱.۱. *فرض کنیم G یک گروه متناهی از مرتبه mn باشد که در آن m و n نسبت به هم اول‌اند. به‌علاوه فرض می‌کنیم $H \leq Z(G)$ به‌طوری‌که $|H| = m$. دراین‌صورت، H یک متمم نرمال در G مانند K دارد و $G = H \times K$.*

برهان. به موجب نتیجه ۳۷.۱.۱، تابع $T: G \to H$ با ضابطه $aT = a^n$ یک همریختی است. چون $(m,n) = 1$، اعداد صحیحی مانند λ و μ موجودند به‌طوری‌که $\lambda n + \mu m = 1$. اینک به ازای هر h از H داریم

$$h = h^{\lambda n + \mu m} = (h^\lambda)^n = (h^\lambda)T.$$

یعنی T یک برو‌ریختی است. درنتیجه $\frac{G}{K} \cong H$، که در آن $K = \mathrm{Ker}T$. واضح است که $|K| = n$ و چون $(m,n) = 1$، $H \cap K = 1$. از اینجا حکم ثابت می‌شود. $\square$

لم ۴۰.۱.۱. *(برنساید) فرض کنیم P یک زیرگروه سیلوی گروه متناهی G باشد و $a, b \in C_G(P)$. دراین‌صورت اگر a و b در G مزدوج باشند، آن‌گاه در $N_G(P)$ مزدوج‌اند.*

برهان. به لم ۲.۲.۱۲ مرجع [۲۰] مراجعه شود. $\square$

قضیه ۴۱.۱.۱. *(قضیه انتقال برنساید)* [۲] *با توجه به نمادگذاری تعریف ۳۸.۱.۱، اگر $P \subseteq Z(N_G(P))$، آن‌گاه G یک p-متمم نرمال دارد.*

برهان. ابتدا از $P \subseteq Z(N_G(P))$ نتیجه می‌شود که P آبلی است. بنابراین $P' = ۱$. بنابراین انتقال $T : G \to \frac{P}{P'}$ را می‌توان از G به P در نظر گرفت، که در آن $|G : P| = n$. ثابت می‌کنیم $\mathrm{Ker}T$ متمم نرمال P در G است. ابتدا ثابت می‌کنیم که به ازای هر a از P، $aT = a^n$.
فرض کنیم $a \in P$. طبق لم ۳۵.۱.۱، اعدادی طبیعی مانند $r_۱$، ...، r_m و اعضایی از G مانند $g_۱$، ...، g_m موجودند به‌طوری‌که

$$\sum_{t=۱}^{m} r_t = n$$

و به ازای هر t که $۱ \leq t \leq m$، $g_t a^{r_t} g_t^{-۱} \in P$ و

$$aT = \prod_{t=۱}^{m} g_t a^{r_t} g_t^{-۱}.$$

حال چون P آبلی است، $P \leq C_G(P)$. بنابراین به ازای هر t که $۱ \leq t \leq m$، داریم $a^{r_t} \in C_G(P)$ و

$$g_t a^{r_t} g_t^{-۱} \in C_G(P).$$

از لم ۴۰.۱.۱، $N_G(P)$ عضوی مانند c دارد به‌طوری‌که

$$g_t a^{r_t} g_t^{-۱} = c^{-۱} a^{r_t} c.$$

ولی چون $a^{r_t} \in P$ و $P \subseteq Z(N_G(P))$، خواهیم داشت $c^{-۱} a^{r_t} c = a^{r_t}$ و درنتیجه $g_t a^{r_t} g_t^{-۱} = a^{r_t}$. پس

$$aT = \prod_{t=۱}^{m} a^{r_t} = a^n.$$

اینک با توجه به این‌که $(|P|, |G : P|) = ۱$، مانند استدلالی که در قضیه ۳۹.۱.۱ دیدیم، معلوم می‌شود که T یک برور یختی است. به موجب قضیه اول یکریختی، $\frac{G}{\mathrm{Ker}T}$ با P یکریخت است و حکم با $K = \mathrm{Ker}T$ ثابت می‌شود. □

نتیجه ۴۲.۱.۱. *فرض کنیم G یک گروه متناهی و P یک زیرگروه سیلوی آن باشد. دراین‌صورت اگر $C_G(P) = N_G(P)$، آن‌گاه P یک متمم نرمال در G دارد.*

برهان. چون $P \leq N_G(P) = C_G(P)$، P آبلی است و در نتیجه $P \leq Z(C_G(P)) = Z(N_G(P))$. اینک کافی است قضیه برنساید را به کار بندیم. □

نتیجه ۴۳.۱.۱. *فرض کنیم P یک p-زیرگروه سیلوی گروه متناهی G باشد که در آن p کوچکترین عدد اولی است که $|G|$ را عاد می‌کند. دراین‌صورت اگر P دوری باشد، آن‌گاه P یک متمم نرمال در G دارد.*

[۲] Burnside's transfer theorem

برهان. طبق نتیجه قبل کافی است ثابت کنیم که $C_G(P) = N_G(P)$. به موجب قضیه نرمال‌ساز-مرکزساز،

$$\frac{N_G(P)}{C_G(P)} \hookrightarrow \mathrm{Aut}(P).$$

چون P دوری است، با فرض $|P| = p^m$، خواهیم داشت

$$|\mathrm{Aut}(P)| = p^{m-۱}(p-۱).$$

از طرفی از آبلی بودن P معلوم می‌شود که $P \leq C_G(P)$. در نتیجه، $p \nmid |\frac{N_G(P)}{C_G(P)}|$. از آن‌جا، $(p^{m-۱}, |\frac{N_G(P)}{C_G(P)}|) = ۱$. بنابراین، $|\frac{N_G(P)}{C_G(P)}|\,|p-۱$. چون p کوچک‌ترین عامل اول $|G|$ است، باید داشته باشیم

$$|\frac{N_G(P)}{C_G(P)}| = ۱.$$

در نتیجه، $C_G(P) = N_G(P)$ و حکم ثابت می‌شود. $\square$

قضیه ۴۴.۱.۱. *هر گروه متناهی شامل یک زیرگروه دوری از اندیس عدد اول، یک زیرگروه سیلوی نرمال دارد.*

برهان. فرض کنیم G یک گروه متناهی و C یک زیرگروه دوری از اندیس عدد اول p در G باشد. با استقرا روی تعداد عوامل اول متمایز $|G|$، حکم را ثابت می‌کنیم. اگر G یک p-گروه باشد، دراین‌صورت G خودش یک p-زیرگروه سیلوی نرمال است. فرض کنیم عدد اول r متمایز از p وجود داشته باشد که $|G|$ را عاد می‌کند.

فرض کنیم R یک r-زیرگروه سیلوی C باشد. حال $|G:R| = p.|C:R|$ به r بخش‌پذیر نیست، لذا R یک r-زیرگروه سیلوی G است. اگر R در G نرمال باشد، آن‌گاه حکم برقرار است. فرض می‌کنیم R در G نرمال نباشد. حال R در زیرگروه دوری C نرمال است لذا $C \leq N_G(R) < G$.

چون C از اندیس عدد اول در G است، باید $N_G(R) = C$. به ویژه، $R \leq Z(N_G(R))$، لذا بنا به قضیه انتقال برنساید، G یک r-متمم نرمال N دارد. بنابراین $RN = G$ و لذا $CN = G$.

حال چون C دوری است، $N \cap C$ دوری است و

$$|N : N\cap C| = |CN : C| = |G : C| = p.$$

فرض کنیم $N \cap C$ نابدیهی باشد. دراین‌صورت بنا به استقرا، N یک زیرگروه سیلوی نرمال نابدیهی S دارد. در واقع، S در N مشخصه است، لذا S در G نرمال است. مشاهده می‌کنیم چون $|G:N|$ و $|N|$ نسبت به هم اول هستند لذا، S یک زیرگروه سیلوی G است .

فرض کنیم $N\cap C = ۱$. دراین‌صورت

$$|G| = |NC| = \frac{|N||C|}{|N\cap C|} = \frac{(\frac{|G|}{|R|})(\frac{|G|}{p})}{۱},$$

لذا برای توان مثبت α، $|G| = pr^{\alpha}$. حال R و P زیرگروه‌های دوری G هستند لذا، نتیجه ۴۳.۱.۱ ایجاب می‌کند که اگر $r < p$، آنگاه G یک r–متمم نرمال دارد و اگر $p < r$، آنگاه G یک p–متمم نرمال دارد. در هر دو مورد، یک زیرگروه سیلوی نرمال G وجود دارد. □

۲.۱ مفاهیمی از گراف‌ها

در این پایان‌نامه منظور از گراف‌ها، گراف‌های ساده هستند.

تعریف ۱.۲.۱. فرض کنیم V یک مجموعه باشد و $E \subseteq V \times V = \{(a,a) \mid a \in V\}$. دراین‌صورت (V,E) را یک گراف جهت‌دار می‌نامیم.
اگر $(a,b) \in E$، آنگاه از نماد $a \to b$ استفاده می‌کنیم.

تعریف ۲.۲.۱. گراف کامل ، گراف ساده‌ای است که در آن، هر دو رأس مجاورند. یک گراف کامل از مرتبه n با K_n نشان داده می‌شود.
درجه هر رأس در گراف کامل برابر $n - ۱$ و لذا تعداد یال‌ها برابر $\binom{n}{۲}$ است.

تعریف ۳.۲.۱. اگر گراف A زیرگرافی از گراف B باشد، آنگاه گراف B را زبرگراف گراف A می‌نامیم.

تعریف ۴.۲.۱. فرض کنیم $n \geq ۲$ و $V = \{v_۱, \ldots, v_n\}$. یک مسیر از مرتبه n، گراف ساده‌ای با مجموعه رئوس V و مجموعه یال‌های $\{\{v_۱,v_۲\},\{v_۲,v_۳\},\ldots,\{v_{n-۱},v_n\}\}$ است که با P_n نشان می‌دهیم.

تعریف ۵.۲.۱. فرض کنیم $n \geq ۳$. یک دور از مرتبه n، گرافی با مجموعه رئوس $\{v_۱,\ldots,v_n\}$ و مجموعه یال‌های $\{\{v_۱,v_۲\},\{v_۲,v_۳\},\ldots,\{v_{n-۱},v_n\},\{v_n,v_۱\}\}$ است که با C_n نشان می‌دهیم.

تعریف ۶.۲.۱. رأس برشی یک گراف، رأسی است که حذف آن، تعداد مولفه‌های همبندی را افزایش می‌دهد.

تعریف ۷.۲.۱. یک یال برشی در گراف G، یالی است که با حذف آن، تعداد مولفه‌های همبندی گراف حاصل، بیش‌تر می‌شود.

تعریف ۸.۲.۱. فرض کنیم G گرافی از مرتبه n باشد. اگر G یک گراف غیرکامل باشد، آنگاه کم‌ترین تعداد رئوسی که حذف آن‌ها، گراف G را ناهمبند می‌کند، همبندی (رأسی) G نامیده و با $\kappa(G)$ نشان می‌دهیم.
درصورت کامل بودن G، همبندی آن را $n - ۱$ تعریف می‌کنیم.

گزاره ۹.۲.۱. *(الف) $\kappa(G)$ برابر است با کم‌ترین تعداد رئوسی که با حذف آن‌ها، یک گراف ناهمبند یا بدیهی بدست می‌آید.*

(ب) $\kappa(G) = 0$ *اگروتنها‌اگر G ناهمبند باشد یا بدیهی.*

(ج) $\kappa(G) = 1$ *اگروتنها‌اگر $G = K_2$ یا G یک‌گراف همبند و دارای رأس برشی باشد.*

تعریف ۱۰.۲.۱. گراف G را k-همبند می‌نامیم هرگاه $\kappa(G) \geq k$.
در یک گراف k-همبند، اگر کم‌تر از k رأس حذف شود، گراف حاصل همبند است اما با حذف k رأس، ممکن است گراف حاصل، همبند باشد یا نباشد.

گزاره ۱۱.۲.۱. *(الف) گراف بدیهی، ۰-همبند است ؛ اما برای $k \geq 1$، k-همبند نیست.*

(ب) هر گراف نابدیهی ۰-همبند است. علاوه بر آن، اگر همبند باشد، آن‌گاه ۱-همبند نیز هست.

تعریف ۱۲.۲.۱. گراف G و H را یکریخت گوییم هرگاه تابع دوسویی $\theta : V_G \to V_H$ وجود داشته باشد به‌طوری‌که برای $u, v \in V_G$ داشته باشیم

$$uv \in E_G \iff \theta(u)\theta(v) \in E_H$$

دراین‌صورت می‌نویسیم $G \cong H$. θ را نیز یک یکریختی بین G و H می‌نامیم.

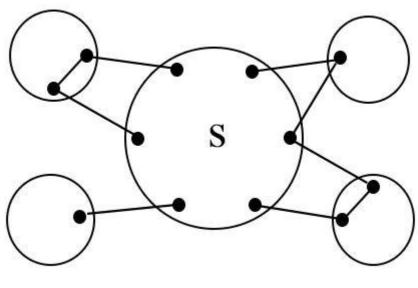
تعریف ۱۳.۲.۱. گراف G را مسطح می‌نامیم هرگاه بتوان آن را در صفحه طوری رسم کرد که یال‌هایش تنها در رئوس انتهایی همدیگر را قطع کنند.

تعریف ۱۴.۲.۱. یک دور هامیلتونی در گراف G، دوری است که همه رئوس G را دارد.
اگر G دارای دور هامیلتونی باشد، آن‌گاه G را یک گراف هامیلتونی می‌نامیم.

قضیه ۱۵.۲.۱. *(کوراتوفسکی) یک گراف G مسطح است اگروتنها‌اگر G شامل K_5 یا $K_{3,3}$ یا هر گراف همسانریخت با آن‌ها به عنوان یک زیرگراف نباشد.*

گزاره ۱۶.۲.۱. *اگر G یک دور هامیلتونی داشته باشد، آن‌گاه برای هر مجموعه ناتهی $S \subseteq V$، گراف $G - S$، حداکثر $|S|$ مولفه دارد.*

برهان. در حین خروج از یک مولفه $G - S$، دور هامیلتونی تنها می تواند به S برود و ورودی‌های به S باید به رئوس متمایز S بروند. بنابراین S باید حداقل به اندازه مولفه‌های $G - S$، رأس داشته باشد.



□

فصل ۲

گراف توانی نیم‌گروه‌ها

۱.۲ گراف توانی نیم‌گروه‌ها و گروه‌ها

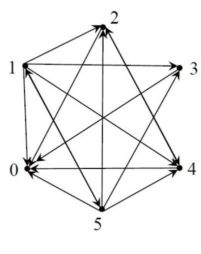
تعریف ۱.۱.۲. گراف توانی نیم‌گروه S، $\mathcal{P}(S)$، گرافی است که مجموعه رئوس آن، S است و دو رأس a و b مجاورند اگروتنها اگر $a \neq b$ و برای برخی عدد صحیح مثبت m، $a^m = b$ یا $b^m = a$.

تعریف ۲.۱.۲. فرض کنیم G یک گروه متناهی باشد و $g \in G$.

(الف) گراف توانی جهت‌دار گروه G، $\overrightarrow{\mathcal{P}}(G)$، گرافی با مجموعه رئوس G و مجموعه یال

$$\overrightarrow{E}(G) = \{(g,h) |\, g, h \in G, h \in \langle g \rangle - \{g\}\}$$

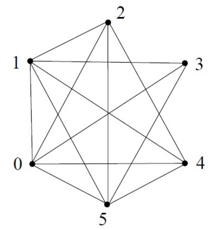
است به عبارت دیگر، یک یال جهت‌دار از یک عنصر گروه به عنصر دیگری زمانی وجود دارد که دومی توان مثبتی از اولی و متمایز از آن باشد.
شکل زیر گراف توانی مستقیم گروه $\mathbb{Z}_6$ را نشان می‌دهد:



(ب) گراف توانی گروه G، $\mathcal{P}(G)$، گرافی با مجموعه رئوس G و مجموعه یال

$$E(G) = \{\{g,h\} | (g,h) \in \overrightarrow{E}(G) \text{ یا } (h,g) \in \overrightarrow{E}(G)\}$$

است که دو عنصر متمایز گروه مجاورند اگر، یکی از آن‌ها توان مثبتی از دیگری باشد.
شکل زیر گراف توانی گروه $\mathbb{Z}_6$ را نشان می‌دهد:



فرض کنیم S یک نیم‌گروه متناهی باشد. عنصر $e \in S$ خودتوان گفته می‌شود اگر $e^{۲} = e$. مجموعه همه خودتوان‌های S را با $E(S)$ نشان می‌دهیم. چون S متناهی است، برای هر $a \in S$، $m \in \mathbb{N}$ وجود دارد به‌طوری‌که a^m یک خودتوان است. هم‌چنین به راحتی بررسی می‌شود برای $e, f \in E(S)$، اگر $a^m = e$ و $a^n = f$، آن‌گاه

$$e = a^m \Rightarrow e = e^n = (a^m)^n = (a^n)^m = f^m = f.$$

رابطه دوتایی ρ روی S را به صورت زیر تعریف می‌کنیم:

$$a\rho b \Leftrightarrow \exists m \in \mathbb{N}, \quad a^m = b^m. \tag{۱.۲}$$

واضح است که ρ یک رابطه هم‌ارزی روی S است. در ادامه نشان می‌دهیم که برای هر زوج عناصر متمایز $a, b \in S$، $a\rho b$ اگروتنها‌اگر a و b توسط یک مسیر در گراف $\mathcal{P}(S)$ به هم وصل شوند. بنابراین رده‌های هم‌ارزی تحت ρ، دقیقاً مولفه‌های $\mathcal{P}(S)$ هستند.

تعریف ۳.۱.۲. فرض کنیم $\rho \subseteq S \times S$ یک رابطه هم‌ارزی روی نیم‌گروه S باشد. دراین‌صورت ρ رابطه هم‌نهشتی روی S نامیده می‌شود اگر برای هر $s, t, u \in S$ که $s\rho t$، آن‌گاه

$$(su)\rho(tu) \qquad \text{و} \qquad (us)\rho(ut).$$

رابطه هم‌ارزی ρ روی نیم‌گروه S هم‌نهشتی است اگروتنها‌اگر برای هر $s, t, u, v \in S$،

$$s\rho t\ ,\ u\rho v\ \Rightarrow\ (su)\rho(tv).$$

لم ۴.۱.۲. *فرض‌کنیم S یک نیم‌گروه متناهی و ρ یک رابطه دوتایی تعریف‌شده توسط معادله ۱.۲ باشد. دراین‌صورت برای هر $a, b \in S$، $a\rho b$ اگروتنها‌اگر برای برخی $m_۱, m_۲ \in \mathbb{N}$ و $e \in E(S)$،*

$$a^{m_۱} = b^{m_۲} = e.$$

برهان. فرض کنیم $a\rho b$، $(a, b \in S)$. دراین‌صورت $m \in \mathbb{N}$ وجود دارد که $a^m = b^m$. چون S متناهی است، $n_۱, n_۲ \in \mathbb{N}$ وجود دارند به‌طوری‌که برای $e, f \in E(S)$، $a^{n_۱} = e$ و $b^{n_۲} = f$. دراین‌صورت

$$e = a^{mn_۱n_۲} = b^{mn_۱n_۲} = f.$$

بنابراین برای $m_۱ = m_۲ = mn_۱n_۲$، $a^{m_۱} = b^{m_۲} = e \in E(S)$.
عکس : فرض کنیم $a, b \in S$ به‌طوری‌که برای برخی $m_۱, m_۲ \in \mathbb{N}$ و $e \in E(S)$، $a^{m_۱} = b^{m_۲} = e$. دراین‌صورت $a^m = b^m$ که $m = m_۱m_۲$ یعنی $a\rho b$. □

قضیه ۵.۱.۲. *فرض کنیم S یک نیم‌گروه متناهی باشد و $a, b \in S$ به‌طوری‌که $a \neq b$. دراین‌صورت a و b توسط یک مسیر در گراف $\mathcal{P}(S)$ به هم وصل می‌شوند اگروتنها اگر $a\rho b$.*

برهان. فرض کنیم $a, b \in S$ که توسط مسیر $(a, c_1, c_2, \ldots, c_k, b)$ در گراف $\mathcal{P}(S)$ به هم متصل هستند. حال چون c_1 با a در $\mathcal{P}(S)$ مجاور است لذا به ازای برخی $m \in \mathbb{N}$، $a^m = c_1$ یا $c_1^m = a$. دراین‌صورت در هر دو حالت، طبق لم ۴.۱.۲ داریم $a\rho c_1$. بنابراین، با استقرا روی طول مسیر برای هر $i = 1, 2, \ldots, k-1$ داریم $c_i\rho c_{i+1}$ و $c_k\rho b$. لذا بنا به تعدی ρ، داریم $a\rho b$.
عکس : فرض کنیم $a\rho b$. دراین‌صورت $m \in \mathbb{N}$ وجود داردکه $a^m = b^m$. دراین‌صورت طبق لم ۴.۱.۲، برای برخی $n \in \mathbb{N}$

$$a^n = e = b^n.$$

که ایجاب می‌کند a و b هر دو با e مجاور باشند. بنابراین a و b با یک مسیر به هم متصل هستند. $\square$

حال از مطلب فوق واضح است که هر رأس در $\mathcal{P}(S)$ با یک و تنها یک خودتوان در S مجاور است و هیچ دو خودتوانی توسط یک مسیر متصل نیستند، یعنی هر مولفه $\mathcal{P}(S)$ شامل یک خودتوان منحصربه‌فرد، که با هر رأس دیگر آن مولفه مجاور است، می‌شود. این نکته را در نتیجه زیر خلاصه می‌کنیم. رده هم‌ارزی $e \in E(S)$ تحت ρ را با C_e نمایش می‌دهیم یعنی

$$C_e = \{a \in S \mid a\rho e\} = \{a \in S \mid \exists m \in \mathbb{N},\ a^m = e\}.$$

نتیجه ۶.۱.۲. *مولفه‌های گراف $\mathcal{P}(S)$، دقیقاً $\{C_e \mid e \in E(S)\}$ هستند به‌علاوه اگر S جابه‌جایی باشد، آن‌گاه برای هر $e \in E(S)$، C_e یک زیرنیم‌گروه S است.*

طبق خصوصیات مولفه‌های گراف $\mathcal{P}(S)$، نتیجه زیر بدست می‌آید.

نتیجه ۷.۱.۲. *فرض کنیم S یک نیم‌گروه متناهی باشد. دراین‌صورت $\mathcal{P}(S)$ همبند است اگروتنها اگر S شامل یک خودتوان واحد باشد.*

بر این اساس، نتیجه زیر را برای گروه‌ها داریم.

نتیجه ۸.۱.۲. *اگر G یک گروه متناهی باشد، آن‌گاه $\mathcal{P}(G)$ همیشه همبند است.*

در حالت کلی، به گزاره زیر می‌رسیم.

گزاره ۹.۱.۲. *فرض کنیم S یک نیم‌گروه باشد به‌طوری‌که $\mathcal{P}(S)$ همبند است. دراین‌صورت S شامل حداکثر یک خودتوان است.*

برهان. فرض کنیم e و f دو عنصر متمایز در $E(S)$ باشند و $(e, a_1, a_2, \ldots, a_n, a_{n+1} = f)$ یک مسیر بین e و f باشد. دراین‌صورت $m \in \mathbb{N}$ وجود دارد که $a_1^m = e$ (چون برای هر $t \in \mathbb{N}$، $e^t = e \neq a_1$).

حال فرض کنیم $n_1 \in \mathbb{N}$ وجود دارد که $a_2^{n_1} = a_1$. لذا $a_2^{mn_1} = e$. درغیراین‌صورت $n_2 \in \mathbb{N}$ وجود دارد که $a_1^{n_2} = a_2$ که ایجاب می‌کند

$$a_2^m = a_1^{mn_2} = e.$$

با استقرا روی طول مسیر، $k \in \mathbb{N}$ وجود دارد که $a_{n+1}^k = e$. بنابراین $e = a_{n+1}^k = f^k = f$، که تناقض است. لذا نتیجه حاصل می‌شود. □

عکس گزاره بالا برقرار نیست زیرا $(\mathbb{Z}, +)$ یک نیم‌گروه (گروه) با خودتوان واحد است اما می‌بینیم که $\mathcal{P}(\mathbb{Z}, +)$ ناهمبند است.

تعریف ۱۰.۱.۲. نیم‌گروه S را منظم می‌نامیم اگر برای هر $a \in S$، یک عنصر $x \in S$ وجود داشته باشد به‌طوری‌که $axa = a$.

نیم‌گروه منظم S شامل عنصر خودتوان است و S یک گروه است اگروتنهااگر S شامل یک خودتوان واحد باشد. بنابراین داریم

نتیجه ۱۱.۱.۲. *فرض کنیم S یک نیم‌گروه منظم باشد. اگر $\mathcal{P}(S)$ همبند باشد، آن‌گاه S گروه است.*

قضیه ۱۲.۱.۲. *فرض کنیم G یک گروه باشد. دراین‌صورت $\mathcal{P}(G)$ همبند است اگروتنهااگر هر عنصر G، از مرتبه متناهی باشد (یعنی G یک گروه تاب‌دار باشد).*

برهان. فرض کنیم $\mathcal{P}(G)$ همبند باشد. فرض کنیم $a \neq e$ یک عنصر از G باشد. دراین‌صورت مسیر $(e = a_0, a_1, \ldots, a_k = a)$ در $\mathcal{P}(G)$ وجود دارد. چون $a_1 \neq e$، برای برخی $n \in \mathbb{N}$ داریم $a_1^n = e$.
چون a_1 و a_2 در $\mathcal{P}(G)$ مجاورند، $m \in \mathbb{N}$ $(m > 1)$ وجود دارد که

$$a_1^m = a_2 \qquad \text{یا} \qquad a_2^m = a_1.$$

اگر $a_1^m = a_2$، دراین‌صورت $a_2^n = a_1^{mn} = e$.
درغیراین‌صورت $a_2^{mn} = a_1^n = e$. لذا در هر دو حالت $o(a_2)$ متناهی است. با استقرا روی طول مسیر می‌توانیم نشان دهیم که $o(a)$ متناهی است.
برای عکس قضیه، درمی‌یابیم که هر رأس با e مجاور است. لذا $\mathcal{P}(G)$ همبند است. □

نتیجه ۱۳.۱.۲. *اگر G یک گروه دوری نامتناهی باشد، آن‌گاه $\mathcal{P}(G)$ همبند نیست.*

با توجه به نتیجه قبل $\mathcal{P}(\mathbb{Z}, +)$ همبند نیست. اما

$$(\mathbb{Z}_5[x], +), (\mathbb{Z}_3[x], +), (\mathbb{Z}_5[x] \times \mathbb{Z}_3[x], +)$$

گروه‌های تاب‌دار نامتناهی هستند و لذا گراف توانی آن‌ها همبند است که $(\mathbb{Z}_m[x], +)$ گروه جمعی حلقه چندجمله‌ای $\mathbb{Z}_m[x]$ است.
مطلب بعدی، رده نیم‌گروه‌های S، که $\mathcal{P}(S)$ کامل است، را مشخص می‌کند.

گزاره ۱۴.۱.۲. *فرض کنیم S یک نیم‌گروه باشد. دراین‌صورت $\mathcal{P}(S)$ کامل است اگر و تنها اگر زیرنیم‌گروه‌های دوری S با توجه به رابطه شمول، خطی مرتب باشند (یعنی برای هر دو زیرنیم‌گروه دوری $S_۱, S_۲ \in S$، $S_۱ \subseteq S_۲$ یا $S_۲ \subseteq S_۱$).*

برهان. فرض کنیم گراف توانی نیم‌گروه S، کامل باشد. فرض کنیم $S_۱ = \langle a \rangle$ و $S_۲ = \langle b \rangle$، دو زیرنیم‌گروه دوری S باشند. چون $\mathcal{P}(S)$ کامل است، a و b مجاورند و لذا

$$\langle a \rangle \subseteq \langle b \rangle \qquad \text{یا} \qquad \langle b \rangle \subseteq \langle a \rangle,$$

یعنی $S_۱ \subseteq S_۲$ یا $S_۲ \subseteq S_۱$. لذا زیرنیم‌گروه‌های دوری S با توجه به رابطه شمول، خطی مرتب هستند.
به‌عکس، فرض کنیم S یک نیم‌گروه باشد که زیرنیم‌گروه‌های دوری S با توجه به رابطه شمول، خطی مرتب باشند. فرض کنیم a و b در S باشند. دراین‌صورت

$$\langle a \rangle \subseteq \langle b \rangle \qquad \text{یا} \qquad \langle b \rangle \subseteq \langle a \rangle,$$

که ایجاب می‌کند a با b در $\mathcal{P}(S)$ مجاور باشد. بنابراین گراف $\mathcal{P}(S)$ کامل است. □

قضیه ۱۵.۱.۲. *فرض کنیم G یک گروه متناهی باشد. دراین‌صورت $\mathcal{P}(G)$ کامل است اگر و تنها اگر برای عدد اول p و $m \in \mathbb{N}$، G یک گروه دوری از مرتبه ۱ یا p^m باشد.*

برهان. اگر $|G| = ۱$، آنگاه $\mathcal{P}(G)$ یک گراف کامل با یک رأس است. فرض کنیم برای عدد اول p و $m \in \mathbb{N}$، G یک گروه دوری متناهی از مرتبه $n = p^m$ باشد. دراین‌صورت برای هر مقسوم‌علیه d از n، یک زیرگروه منحصربه‌فرد از مرتبه d وجود دارد و زیرگروه‌های (دوری) G، به صورت زیر هستند:

$$G_۰ \subseteq G_۱ \subseteq G_۲ \subseteq \cdots \subseteq G_m (= G),$$

که $|G_i| = p^i$. بنابر گزاره ۱۴.۱.۲، $\mathcal{P}(G)$ کامل است.
به‌عکس، فرض کنیم G یک گروه متناهی باشد که $|G| > ۱$ و $\mathcal{P}(G)$ کامل باشد. ابتدا ادعا می‌کنیم که G دوری است. اگر نباشد، دراین‌صورت G حداقل دو عنصر a و b دارد به‌طوری‌که

$$a \notin \langle b \rangle \qquad \text{و} \qquad b \notin \langle a \rangle,$$

که ایجاب می‌کند a و b در $\mathcal{P}(G)$ مجاور نباشند که متناقض است با این‌که $\mathcal{P}(G)$ کامل است.
در آخر فرض کنیم p و q دو عامل اول متمایز $|G|$ باشند. دراین‌صورت G شامل عناصر a و b با مرتبه‌های به ترتیب p و q است. اما دراین‌صورت

$$\langle a \rangle \nsubseteq \langle b \rangle \qquad \text{و} \qquad \langle b \rangle \nsubseteq \langle a \rangle.$$

لذا هیچ یالی بین a و b در $\mathcal{P}(G)$ وجود ندارد و بنابراین $\mathcal{P}(G)$ کامل نیست که تناقض است. لذا برای عدد اول p و $m \in \mathbb{N}$، $|G| = p^m$. □

۲.۲ گراف توانی نیم‌گروه $(\mathbb{Z}_n, .)$

در این بخش، گراف روی یک نیم‌گروه متناهی خاص، $(\mathbb{Z}_n, .)$، نیم‌گروه اعداد صحیح به پیمانه n تحت ضرب کلاس‌های هم‌ارزی، را مطالعه می‌کنیم. در ادامه برخی ویژگی‌های گراف $\mathcal{P}(\mathbb{Z}_n)$ را مشاهده می‌کنیم که به ما در توصیف گراف $\mathcal{P}(\mathbb{Z}_n)$ کمک خواهد کرد. چون مولفه‌های $\mathcal{P}(S)$ کاملاً توسط خودتوان‌های نیم‌گروه متناهی S مشخص شدند (نتیجه ۶.۱.۲ را ببینید)، می‌خواهیم همه خودتوان‌های $\mathbb{Z}_n$ را کاملاً مشخص کنیم.

لم ۱.۲.۲. *فرض کنیم برای عدد اول p و $m \in \mathbb{N}$، $n = p^m$. دراین‌صورت تنها خودتوان‌های $\mathbb{Z}_n$، $\bar{۰}$ و $\bar{۱}$ هستند.*

برهان. فرض کنیم $\bar{e} \in \mathbb{Z}_n$ یک خودتوان باشد. دراین‌صورت $e^۲ \equiv e$ (به پیمانه p^m). دراین‌صورت

$$p^m \mid (e^۲ - e) = e(e - ۱)$$

که ایجاب می‌کند $p^m \mid e$ یا $p^m \mid e - ۱$. لذا $\bar{e} = \bar{۰}$ یا $\bar{e} = \bar{۱}$، همان‌طور که می‌خواستیم. □

برای ادامه بخش، برای $n > ۱$، n را به صورت $n = p_۱^{n_۱} p_۲^{n_۲} \dots p_k^{n_k}$ در نظر می‌گیریم که p_iها اعداد اول متمایز هستند و برای هر $i = ۱, ۲, \dots, k$ $(k \in \mathbb{N})$، $n_i \in \mathbb{N}$. دراین‌صورت از [۱۲] می‌دانیم که به عنوان حلقه

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_۱^{n_۱}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

بنابراین به عنوان نیم‌گروه (تحت ضرب) یکریختی

$$f : \mathbb{Z}_n \to \mathbb{Z}_{p_۱^{n_۱}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

با ضابطه زیر تعریف می‌شود :

$$f([a]_n) = ([a]_{p_۱^{n_۱}}, [a]_{p_۲^{n_۲}}, \dots, [a]_{p_k^{n_k}}). \quad (۲.۲)$$

تعریف ۲.۲.۲. فرض کنیم $n = p_۱^{n_۱} p_۲^{n_۲} \dots p_k^{n_k}$. تعریف می‌کنیم

$$\mathrm{PFS}[n] = \{p_۱, p_۲, \dots, p_k\} \qquad \text{و} \qquad \pi[n] = p_۱ p_۲ \dots p_k.$$

و قرارداد می‌کنیم $\mathrm{PFS}[۱] = \emptyset$ و $\pi[۱] = ۱$.

نتیجه ۳.۲.۲. *هر خودتوان (ضربی) $\bar{e}$ از $\mathbb{Z}_n$ به صورت*

$$\bar{e} = (\bar{e_۱}, \bar{e_۲}, \dots, \bar{e_k}) \in \mathbb{Z}_{p_۱^{n_۱}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

است که برای هر $i = ۱, ۲, \dots, k$، $\bar{e_i} = \bar{۰}$ یا $\bar{e_i} = \bar{۱}$ و $e \equiv e_i$ (به پیمانه $p_i^{n_i}$). به‌علاوه تعداد کل خودتوان‌های (ضربی) $\mathbb{Z}_n$ برابر است با $۲^{|\mathrm{PFS}[n]|}$.

برهان. اثبات از لم ۱.۲.۲ و این حقیقت که $(\bar{e_1}, \bar{e_2}, \dots, \bar{e_k})$ یک خودتوان از

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

است، اگروتنها اگر برای هر $i = 1, 2, \dots, k$، $\bar{e_i}$ یک خودتوان در $\mathbb{Z}_{p_i^{n_i}}$ باشد، نتیجه می‌شود. □

نتیجه ۴.۲.۲. *فرض کنیم $\bar{e}$ یک خودتوان در $\mathbb{Z}_n$ باشد که*

$$\mathrm{PFS}[(n, e)] = \{p_1, p_2, \dots, p_r\}.$$

(که منظور از (n, e)، بزرگ‌ترین مقسوم‌علیه مشترک n و e است.) دراین‌صورت $\bar{e} = (\bar{e_1}, \bar{e_2}, \dots, \bar{e_k})$ که برای هر $1 \leq i \leq r$، $\bar{e_i} = \bar{0}$ و برای هر $r + 1 \leq i \leq k$، $\bar{e_i} = \bar{1}$.

برهان. به‌وضوح $(e, p_i^{n_i}) = 1$ اگروتنها اگر $i \in \{r + 1, r + 2, \dots, k\}$. لذا اثبات از نتیجه ۳.۲.۲ بدست می‌آید. □

نتیجه ۵.۲.۲. *فرض کنیم $\bar{e}$ و $\bar{f}$ خودتوان‌های $\mathbb{Z}_n$ باشند به‌طوری‌که*

$$\mathrm{PFS}[(n, e)] = \mathrm{PFS}[(n, f)].$$

دراین‌صورت $e \equiv f$ (به پیمانه n).

برهان. از نتیجه ۴.۲.۲ بدست می‌آید. □

لم ۶.۲.۲. *فرض کنیم برای عدد صحیح $n > 1$، $\bar{a}, \bar{b} \in \mathbb{Z}_n$. دراین‌صورت*

$$\bar{a}\rho\bar{b} \Leftrightarrow \mathrm{PFS}[(n, a)] = \mathrm{PFS}[(n, b)].$$

برهان. فرض کنیم $\bar{a}\rho\bar{b}$. دراین‌صورت طبق تعریف برای $m \in \mathbb{N}$، $a^m \equiv b^m$ (به پیمانه n).
فرض کنیم $p \in \mathrm{PFS}[(n, b)]$ دراین‌صورت $p \mid b^m$. لذا $p \mid a^m$ که نتیجه می‌دهد $p \mid a$.
لذا $p \in \mathrm{PFS}[(n, a)]$. بنابراین

$$\mathrm{PFS}[(n, b)] \subseteq \mathrm{PFS}[(n, a)]$$

به طور مشابه $\mathrm{PFS}[(n, a)] \subseteq \mathrm{PFS}[(n, b)]$. لذا نتیجه برقرار است.
عکس، فرض کنیم $\mathrm{PFS}[(n, a)] = \mathrm{PFS}[(n, b)]$. $m_1, m_2 \in \mathbb{N}$ و $e, f \in E(\mathbb{Z}_n)$ را در نظر می‌گیریم به‌طوری‌که $a^{m_1} = e$ و $b^{m_2} = f$. دراین‌صورت

$$\mathrm{PFS}[(n, a)] = \mathrm{PFS}[(n, e)]$$

و

$$\mathrm{PFS}[(n, b)] = \mathrm{PFS}[(n, f)]$$

نتیجه می‌دهد

$$\mathrm{PFS}[(n, e)] = \mathrm{PFS}[(n, f)]$$

لذا بنا به نتیجه ۵.۲.۲، $\bar{e} = \bar{f}$. بنابراین $\bar{a}^{m_1} = \bar{b}^{m_2}$. لذا $\bar{a}\rho\bar{b}$. □

چون $(\mathbb{Z}_n, .)$، یک نیم‌گروه جابه‌جایی متناهی است، طبق نتیجه ۶.۱.۲ می‌دانیم که مولفه‌های $\mathcal{P}(\mathbb{Z}_n)$، دقیقاً رده‌های همنهشتی ρ هستند که هر رده همنهشتی $C_{\bar{e}}$، یک زیرنیم‌گروه $\mathbb{Z}_n$ است و شامل یک خودتوان منحصربه‌فرد $\bar{e}$ می‌شود. حال از نتیجه ۵.۲.۲ و لم ۶.۲.۲ داریم که هر چنین رده همنهشتی $C_{\bar{e}}$، منحصراً توسط زیرمجموعه $\mathrm{PFS}[(n,e)]$ از $\mathrm{PFS}[n]$ مشخص می‌شود. لذا در ادامه از نماد C_S به جای $C_{\bar{e}}$ استفاده می‌کنیم که $S = \mathrm{PFS}[(n,e)]$. در زیر، نتایجی پیرامون نیم‌گروه خاص $(\mathbb{Z}_n, .)$ را توضیح می‌دهیم. گروه یکه‌های حلقه $\mathbb{Z}_n$ را با U_n نمایش می‌دهیم. در حقیقت،

$$U_n = \{\bar{a} \in \mathbb{Z}_n \mid (n,a) = ۱\}.$$

نتیجه ۷.۲.۲. *مولفه‌های گراف $\mathcal{P}(\mathbb{Z}_n)$، دقیقاً مجموعه زیرنیم‌گروه‌های $\{C_S \mid S \subseteq \mathrm{PFS}[n]\}$ از $\mathbb{Z}_n$ است که*

$$C_S = \{\bar{a} \in \mathbb{Z}_n \mid \mathrm{PFS}[(n,a)] = S\}.$$

به‌ویژه $C_\emptyset$، گروه $(U_n, .)$ است.

لم ۸.۲.۲. *فرض کنیم*

$$n = p_۱^{n_۱} p_۲^{n_۲} \dots p_k^{n_k} \quad ، \quad S = \{p_۱, p_۲, \dots, p_r\} \quad \text{و} \quad m = p_{r+۱}^{n_{r+۱}} p_{r+۲}^{n_{r+۲}} \dots p_k^{n_k}.$$

دراین‌صورت

$$\bar{x} = (\bar{x_۱}, \dots, \bar{x_r}, \bar{x'}) \in C_S$$

(که $\bar{x_i} \in \mathbb{Z}_{p_i^{n_i}}$ و $\bar{x'} \in \mathbb{Z}_m$) اگروتنها اگر برای هر $i = ۱,۲,\dots,r$، $p_i \mid x_i$ و $(x',m) = ۱$.

برهان. فرض کنیم $n = p_۱^{n_۱} p_۲^{n_۲} \dots p_r^{n_r} \dots p_k^{n_k}$. دراین‌صورت

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_۱^{n_۱}} \times \dots \times \mathbb{Z}_{p_r^{n_r}} \times \mathbb{Z}_m$$

که $m = p_{r+۱}^{n_{r+۱}} p_{r+۲}^{n_{r+۲}} \dots p_k^{n_k}$. فرض کنیم $\bar{x} \in C_S$. دراین‌صورت $\mathrm{PFS}[(n,x)] = \{p_۱, p_۲, \dots, p_r\}$.
فرض کنیم $\bar{x} = (\bar{x_۱}, \dots, \bar{x_r}, \bar{x'})$ که $\bar{x_i} \in \mathbb{Z}_{p_i^{n_i}}$ و $\bar{x'} \in \mathbb{Z}_m$ به‌طوری‌که $x \equiv_{p_i^{n_i}} x_i$ و $x \equiv x'$ (به پیمانه m). حال برای هر $i = ۱,۲,\dots,r$، $p_i \mid x$ و لذا برای هر $i = ۱,۲,\dots,r$، $p_i \mid x_i$.
$x \equiv x'$ (به پیمانه m) لذا $k \in \mathbb{N}$ وجود دارد که $x = x' + km$.
فرض کنیم $d = (x',m)$. دراین‌صورت $d \mid x'$ و $d \mid m$ بنابراین $d \mid x$ که نتیجه می‌دهد $d \mid (m,x)$.
اما $(m,x) = ۱$. دراین‌صورت $d = ۱$ و لذا $(m,x') = ۱$.
به‌عکس، فرض کنیم برای هر $i = ۱,۲,\dots,r$، $p_i \mid x_i$ و $(x',m) = ۱$. لذا برای هر $i = ۱,۲,\dots,r$، $p_i \mid x$. همچنین چون $x \equiv x'$ (به پیمانه m)، داریم $(m,x) = ۱$. لذا

$$\mathrm{PFS}[(n,x)] = \{p_۱, p_۲, \dots, p_r\}$$

بنابراین $\bar{x} \in C_S$. □

قضیه زیر، خصوصیات کاملی از مولفه‌های C_S فراهم می‌آورد. برای عدد اول p و $n \in \mathbb{N}$، $p\mathbb{Z}_{p^n}$ زیرنیم‌گروه دوری $\mathbb{Z}_{p^n}$ تولید شده توسط $\bar{p} \in \mathbb{Z}_{p^n}$ است یعنی

$$p\mathbb{Z}_{p^n} = \{\overline{pk} \in \mathbb{Z}_{p^n} \mid k = ۰, ۱, ۲, \dots, p^{n-۱} - ۱\}.$$

قضیه ۹.۲.۲. *فرض کنیم* $n = p_۱^{n_۱} p_۲^{n_۲} \dots p_k^{n_k}$ *و* $S = \{p_۱, p_۲, \dots, p_r\}$. *دراین‌صورت*

$$C_S \cong p_۱\mathbb{Z}_{p_۱^{n_۱}} \times p_۲\mathbb{Z}_{p_۲^{n_۲}} \times \cdots \times p_r\mathbb{Z}_{p_r^{n_r}} \times U_m,$$

که $m = p_{r+۱}^{n_{r+۱}} p_{r+۲}^{n_{r+۲}} \dots p_k^{n_k}$ *و برای هر* $a \in C_S$، $|C_S| = \dfrac{\phi(n)}{\phi(\pi[(n,a)])}$.

برهان. توجه داشته باشیم که

$$\begin{aligned}\bar{x} =&(\bar{x_۱}, \dots, \bar{x_r}, \bar{x'}) \in C_S\\ &\Leftrightarrow p_i \mid x_i \quad i = ۱, ۲, \dots, r \text{ و برای هر } (m, x') = ۱ \qquad (\text{طبق لم } ۸.۲.۲)\\ &\Leftrightarrow \bar{x_i} \in p_i\mathbb{Z}_{p_i^{n_i}} \quad i = ۱, ۲, \dots, r \text{ و برای هر } \bar{x'} \in U_m\\ &\Leftrightarrow (\bar{x_۱}, \dots, \bar{x_r}, \bar{x'}) \in p_۱\mathbb{Z}_{p_۱^{n_۱}} \times p_۲\mathbb{Z}_{p_۲^{n_۲}} \times \cdots \times p_r\mathbb{Z}_{p_r^{n_r}} \times U_m.\end{aligned}$$

بنابراین $C_S \cong p_۱\mathbb{Z}_{p_۱^{n_۱}} \times p_۲\mathbb{Z}_{p_۲^{n_۲}} \times \cdots \times p_r\mathbb{Z}_{p_r^{n_r}} \times U_m$. لذا

$$\begin{aligned}|C_S| &= |p_۱\mathbb{Z}_{p_۱^{n_۱}} \times p_۲\mathbb{Z}_{p_۲^{n_۲}} \times \cdots \times p_r\mathbb{Z}_{p_r^{n_r}} \times U_m|\\ &= |p_۱\mathbb{Z}_{p_۱^{n_۱}}| \times |p_۲\mathbb{Z}_{p_۲^{n_۲}}| \times \cdots \times |p_r\mathbb{Z}_{p_r^{n_r}}| \times |U_m|\\ &= p_۱^{n_۱-۱} p_۲^{n_۲-۱} \dots p_r^{n_r-۱}\phi(m) = \frac{\phi(n)}{\phi(p_۱p_۲\dots p_r)} = \frac{\phi(n)}{\phi(\pi[(n,a)])},\end{aligned}$$

همانطورکه نیاز داشتیم. □

گزاره ۱۰.۲.۲. *فرض کنیم* $n = p_۱^{n_۱} p_۲^{n_۲} \dots p_k^{n_k}$، $S = \{p_۱, p_۲, \dots, p_r\}$ *و* $\bar{x} \in C_S$. *دراین‌صورت اگر* $l = |C_S|$ *و* $\bar{e}_S$ *خودتوان منحصربه‌فرد* C_S *باشد، آن‌گاه* $\bar{x}^l = \bar{e}_S$.

برهان. طبق لم ۱.۲.۲، داریم برای هر i، تنها خودتوان در $p_i\mathbb{Z}_{p_i^{n_i}}$، $\bar{۰}$ است (توجه کنیم که برای $n_i = ۱$، $\bar{p}_i = \bar{۰}$). بنابراین خودتوان منحصربه‌فرد $\bar{e}_S$ در

$$C_S \cong p_۱\mathbb{Z}_{p_۱^{n_۱}} \times p_۲\mathbb{Z}_{p_۲^{n_۲}} \times \cdots \times p_r\mathbb{Z}_{p_r^{n_r}} \times U_m$$

برابر $(\bar{۰}, \bar{۰}, \dots, \bar{۰}, \bar{۱})$ است. حال فرض کنیم $\bar{x} \in C_S$ دراین‌صورت $\bar{x} = (\bar{x}_۱, \bar{x}_۲, \dots, \bar{x}_r, \bar{x'})$. حال برای $n_i = ۱$، $p_i\mathbb{Z}_{p_i^{n_i}} = \{\bar{۰}\}$ و برای $n_i > ۱$، داریم $p_i^{n_i-۱} \geq n_i$ که ایجاب می‌کند برای هر $i = ۱, ۲, \dots, r$، $x_i^{p_i^{n_i-۱}} \equiv ۰$ (به پیمانه $p_i^{n_i}$).
چون $(x', m) = ۱$، $(x')^{\phi(m)} \equiv ۱$ (به پیمانه m). حال چون $l = p_۱^{n_۱-۱} p_۲^{n_۲-۱} \dots p_r^{n_r-۱}\phi(m)$، داریم $x_i^l \equiv ۰$ (به پیمانه $p_i^{n_i}$) برای $i = ۱, ۲, \dots, r$ و $(x')^l \equiv ۱$ (به پیمانه m). بنابراین $\bar{x}^l = \bar{e}_S$، همان‌طورکه نیاز داشتیم. □

فصل ۳

بیش‌ترین تعداد یال در گراف‌های توانی گروه‌های متناهی

۱.۳ یال‌ها در گراف‌های توانی

فرض کنیم G یک گروه متناهی باشد. برای هر $g \in G$، فرض کنیم $\mathrm{o}(g)$ مرتبه g را به عنوان یک عنصر گروه و $\deg(g)$، درجه g را به عنوان یک راس $\mathcal{P}(G)$ مشخص می‌کند.
$g \in G$ را در نظر می‌گیریم. مشاهده می‌کنیم که g، درجه خروجی $\mathrm{o}(g) - ۱$ را دارد، زیرا یک یال جهت‌دار از $g \in G$ به هر عنصر $\langle g\rangle - \{g\}$ وجود دارد. یک یال جهت‌دار از هر $h \in G - \{g\}$ به g برای $g \in \langle h\rangle$ وجود دارد. بنابراین درجه ورودی g، $|\{h \in G - \{g\} \mid g \in \langle h\rangle\}|$ است.

تعریف ۱.۱.۳. فرض کنیم G یک گروه متناهی باشد. مجموعه یال دوطرفه $\overleftrightarrow{E}(G)$ از $\overleftrightarrow{\mathcal{P}}(G)$، به صورت

$$\{\{g,h\} \mid \ (g,h) \in \overrightarrow{E}(G) \ , \ (h,g) \in \overrightarrow{E}(G)\}$$

تعریف می‌شود.
به عبارت دیگر $\overleftrightarrow{E}(G)$ متشکل از زوج عناصر متمایز است که هر کدام توان مثبتی از دیگری است.

لم ۲.۱.۳. *فرض کنیم G یک گروه متناهی، g و h عناصر متمایزی از G باشند. دراین‌صورت $\{g,h\} \in \overleftrightarrow{E}(G)$ اگروتنها اگر $\langle g\rangle = \langle h\rangle$.*

برهان. مستقیماً از تعریف مجاورت در گراف توانی جهت‌دار نتیجه می‌شود. $\square$

لم ۳.۱.۳. *فرض کنیم G یک گروه متناهی از مرتبه n باشد. دراین‌صورت*

$$|\overrightarrow{E}(G)| = \sum_{g\in G}(\mathrm{o}(g) - ۱), \qquad (۱.۳)$$

$$|\overleftrightarrow{E}(G)| = \frac{۱}{۲}\sum_{g\in G}(\phi(\mathrm{o}(g)) - ۱), \tag{۲.۳}$$

$$|E(G)| = |\overrightarrow{E}(G)| - |\overleftrightarrow{E}(G)| = \frac{۱}{۲}\sum_{g\in G}(۲\mathrm{o}(g) - \phi(\mathrm{o}(g)) - ۱). \tag{۳.۳}$$

برهان. در معادله ۱.۳ درجه خروجی رئوس را جمع می‌کنیم و لذا هر یال جهت‌دار را یک بار می‌شماریم. حال از لم ۲.۱.۳ و اینکه یک گروه دوری از مرتبه $\mathrm{o}(g)$، $\phi(\mathrm{o}(g))$ تا مولد دارد، معادله ۲.۳ نتیجه می‌شود. درحقیقت $\phi(\mathrm{o}(g)) - ۱$ یال از چنین یال‌هایی، از g خارج می‌شوند و با جمع همه یال‌های G، این یال‌ها دوبار شمارش می‌شوند. برای تساوی اول در معادله ۳.۳، یال‌ها در گراف توانی جهت‌دار را شمارش می‌کنیم و برای هر زوج از یال‌های جهت‌دار خلاف جهت، برای اجتناب از دوبار شمردن، یکی را کم می‌کنیم. تساوی دوم در معادله ۳.۳، از معادلات ۱.۳ و ۲.۳ نتیجه می‌شود. □

برای محاسبه تعداد یال‌ها در گراف توانی $\mathbb{Z}_n$، از ملاحظه زیر استفاده می‌کنیم.

ملاحظه ۴.۱.۳. *فرض کنیم n یک عدد صحیح مثبت باشد. برای اعداد اول $p_۱ < p_۲ < \cdots < p_k$، می‌نویسیم $n = p_۱^{\alpha_۱}p_۲^{\alpha_۲}\dots p_k^{\alpha_k}$. فرض کنیم $q = p_۱$، $p = p_k$، $\beta = \alpha_۱$ و $\alpha = \alpha_k$.* *می‌دانیم*

$$\phi(n) = p_۱^{\alpha_۱-۱}(p_۱ - ۱)\, p_۲^{\alpha_۲-۱}(p_۲ - ۱)\dots p_k^{\alpha_k-۱}(p_k - ۱). \tag{۴.۳}$$

به عنوان نتیجه داریم

$$\phi(nm) = \phi(n)\phi(m)\frac{(n,m)}{\phi((n,m))}. \tag{۵.۳}$$

لم ۵.۱.۳. *فرض کنیم $n > ۱$. دراین‌صورت درگروه $\mathbb{Z}_n$ داریم*

$$\sum_{z\in\mathbb{Z}_n}\mathrm{o}(z) = \sum_{d|n}\phi(d)d = \prod_{h=۱}^{k}\frac{p_h^{۲\alpha_h+۱}+۱}{p_h+۱}, \tag{۶.۳}$$

$$\sum_{z\in\mathbb{Z}_n}\phi(\mathrm{o}(z)) = \sum_{d|n}\phi(d)^۲ = \prod_{h=۱}^{k}\frac{p_h^{۲\alpha_h}(p_h-۱)+۲}{p_h+۱}. \tag{۷.۳}$$

برهان. برای هر $z \in \mathbb{Z}_n$، $o(z)$ یک مقسوم‌علیه از n است. برای هر مقسوم علیه d ، $\phi(d)$ عنصر از $\mathbb{Z}_n$ با مرتبه یکسان d وجود دارد. لذا تساوی اول در معادله ۶.۳ برقرار می‌باشد. به طور مشابه برای هر عنصر از $\mathbb{Z}_n$ با مرتبه d مانند z، $\phi(\mathrm{o}(z)) = \phi(d)$ و بنابراین تساوی اول در معادله ۷.۳ برقرار است. حال تساوی‌های دوم روابط ۶.۳ و ۷.۳ را ثابت می‌کنیم. فرض کنیم که n، $k \geq ۱$ مقسوم علیه اول متمایز داشته باشد و هر دو تساوی برای همه n ها با حداکثر $k - ۱$ مقسوم علیه اول متمایز برقرار باشد. مقسوم علیه‌های n را بر اساس بالاترین توان q که آن را عاد می‌کند، تفکیک می‌کنیم. از آنجایی‌که d، n را عاد می‌کند، داریم $d = fq^l$ که $q^l \mid d$ و $q^{l+۱} \nmid d$. لذا $\frac{n}{q^\beta} \mid f$. چون $q \nmid \frac{n}{q^\beta}$، از معادله ۴.۳ داریم

$\phi(fq^l) = q^{l-1}(q-1)\phi(f)$.
محاسبه می‌کنیم

$$\begin{aligned}\sum_{d|n} \phi(d)d &= \sum_{l=0}^{\beta} \sum_{f|\frac{n}{q^\beta}} \phi(q^l f) f q^l \\ &= \sum_{l=0}^{\beta} \phi(q^l) q^l \sum_{f|\frac{n}{q^\beta}} \phi(f) f \\ &= \left(1 + \sum_{l=1}^{\beta} q^{l-1}(q-1)q^l\right) \sum_{f|\frac{n}{q^\beta}} \phi(f) f,\end{aligned}$$

و

$$\begin{aligned}\sum_{l=1}^{\beta} q^{2l-1}(q-1) = \sum_{l=0}^{\beta-1}(q-1)q^{2l+1} &= q(q-1)\sum_{l=0}^{\beta-1}(q^2)^l \\ &= q(q-1)\frac{(q^{2\beta}-1)}{q^2-1} \\ &= q\frac{q^{2\beta}-1}{q+1} = \frac{q^{2\beta+1}+1}{q+1} - 1.\end{aligned}$$

لذا تساوی دوم در معادله ۶.۳ بنا به استقرا برقرار است.
به طور مشابه،

$$\begin{aligned}\sum_{d|n} \phi(d)^2 &= \sum_{l=0}^{\beta} \sum_{f|\frac{n}{q^\beta}} \phi(q^l f)^2 \\ &= \sum_{l=0}^{\beta} \phi(q^l)^2 \sum_{f|\frac{n}{q^\beta}} \phi(f)^2 \\ &= \left(1 + \sum_{l=1}^{\beta} \left(q^{l-1}(q-1)\right)^2\right) \sum_{f|\frac{n}{q^\beta}} \phi(f)^2,\end{aligned}$$

و

$$\begin{aligned}\sum_{l=1}^{\beta} \left(q^{l-1}(q-1)\right)^2 &= (q-1)^2 \sum_{l=0}^{\beta-1} q^{2l} \\ &= (q-1)^2 \frac{q^{2\beta}-1}{q^2-1} = \frac{(q-1)(q^{2\beta}-1)}{q+1}.\end{aligned}$$

بنابراین تساوی دوم در معادله ۷.۳ بنا به استقرا نتیجه می‌شود. □

نتیجه ۶.۱.۳. *برای $n > ۱$ در گروه $\mathbb{Z}_n$، داریم:*

$$|E(\mathbb{Z}_n)| = \sum_{d|n} \phi(d)\left(d - \frac{\phi(d)}{۲}\right) - \frac{n}{۲}$$
$$= \prod_{h=۱}^{k} \frac{p_h^{۲\alpha_h+۱}+۱}{p_h+۱} - \frac{۱}{۲}\prod_{h=۱}^{k}\frac{p_h^{۲\alpha_h}(p_h-۱)+۲}{p_h+۱} - \frac{n}{۲}.$$

لم ۷.۱.۳. *فرض کنیم $n > ۱$ و $z \in \mathbb{Z}_n$. قرار می‌دهیم $e = \mathrm{o}(z)$. در این‌صورت*

$$\deg(z) = e - ۱ - \phi(e) + \sum_{d|\frac{n}{e}} \phi(de)$$
$$= e - \phi(e) - ۱ + \phi(e)\sum_{d|\frac{n}{e}} \phi(d)\frac{(d,e)}{\phi((d,e))}. \qquad (۸.۳)$$

برهان. عبارت $\mathrm{o}(z) - ۱ = e - ۱$، درجه خروجی z است. یک یال جهت‌دار از هر عنصر $x \in \mathbb{Z}_n$ به z وجود دارد هنگامی‌که $\mathrm{o}(z) \mid \mathrm{o}(x)$. برای چنین x ای، $\mathrm{o}(x)$، حاصل‌ضرب $o(z)$ در یک مقسوم علیه از $\frac{n}{\mathrm{o}(z)}$ است. $\phi(k\mathrm{o}(z))$ مولد از $\langle x\rangle$ وجود دارد. بنابراین درجه ورودی z، $\sum_{d|\frac{n}{e}} \phi(de)$ است. ضمناً برای اجتناب از دوبار شمردن حین حذف جهت، باید عناصر با مرتبه یکسان مانند z را بیرون نگه داریم یعنی در حالت $k = ۱$، $\phi(ke) = \phi(e)$. بنابراین تساوی اول برقرار می‌شود. تساوی دوم از معادله ۵.۳ نتیجه می‌شود زیرا، جمعوند برای $d = ۱$، ۱ است. □

لم ۸.۱.۳. *فرض کنیم G یک گروه و H زیرگروهی از G باشد.*

(الف) $\overrightarrow{\mathcal{P}}(H)$ یک زیرگراف القا شده از $\overrightarrow{\mathcal{P}}(G)$ است.

(ب) هر یال خروجی از یک عنصر H، به یکی از عناصر H منتهی می‌شود.

(ج) $\mathcal{P}(H)$ یک زیرگراف القا شده از $\mathcal{P}(G)$ است.

به ویژه، مجاورت‌ها و غیرمجاورت‌ها بین عناصر H در $\overrightarrow{\mathcal{P}}(H)$ و $\overrightarrow{\mathcal{P}}(G)$ و به طور مشابه برای $\mathcal{P}(H)$ و $\mathcal{P}(G)$ یکسان هستند.

برهان. مستقیماً از تعاریف نتیجه می‌شوند. □

لم ۹.۱.۳. *فرض کنیم G یک گروه متناهی باشد. در این‌صورت گزاره‌های زیر برقرار است:*

(الف) $|G| \le |E(G)| + ۱$. تساوی برقرار است اگروتنها اگر G یک ۲-گروه آبلی مقدماتی باشد.

(ب) $|E(G)| \le |\overrightarrow{E}(G)|$. تساوی برقرار است اگروتنها اگر G یک ۲-گروه آبلی مقدماتی باشد.

(ج) $۲|\overleftrightarrow{E}(G)| \le |\overrightarrow{E}(G)| - |G| + ۱$. تساوی برقرار است اگروتنها اگر G یک ۲-گروه آبلی مقدماتی باشد یا برای عدد اول p، $G \cong \mathbb{Z}_p$.

برهان. (الف) هر عنصر غیرهمانی G با همانی مجاور است لذا $|G| \leq |E(G)| + ۱$. تساوی برقرار است اگروتنها اگر هر عنصر غیرهمانی G، از مرتبه ۲ باشد.

(ب) هر یال بدون جهت، از یک یال جهت‌دار بوجود می‌آید بنابراین نامساوی برقرار است. بنا به معادله ۳.۳، $|E(G)| = |\overrightarrow{E}(G)|$ اگروتنها اگر هیچ یال دوطرفه‌ای وجود نداشته باشد اگروتنها اگر برای هر $g \in G$، g تنها مولد $\langle g \rangle$ باشد اگروتنها اگر برای هر $g \in G$، یک تنها عددی باشد که هم کمتر از $o(g)$ و هم نسبت به آن اول باشد اگروتنها اگر هر عنصر G، از مرتبه ۲ باشد.

(ج) $(|G| - ۱)$ یال به عنصر همانی، دوطرفه نیست و یال‌های دوطرفه از جفت یال‌های جهت‌دار پدید می‌آیند. بنابراین $۲|\overleftrightarrow{E}(G)| \leq |\overrightarrow{E}(G)| - |G| + ۱$. اگر برخی $g \in G$، مرتبه مرکب داشته باشند، یعنی برای عدد اول p و $m > ۱$، $o(g) = pm$، دراین‌صورت یال بین g و g^p دوطرفه نیست. حال فرض کنیم $|\overleftrightarrow{E}(G)| \neq ۰$. در این‌صورت تساوی در (ج) برقرار است اگروتنها اگر هر یال غیرمتصل به همانی، دوطرفه باشد اگروتنها اگر هر عنصر غیرهمانی، G را تولید کند اگروتنها اگر برای اعداد اول $p > ۲$، $G \cong \mathbb{Z}_p$. اما $|\overleftrightarrow{E}(G)| = ۰$ اگروتنها اگر G، هیچ عنصری از مرتبه بزرگ‌تر از ۲ نداشته باشد اگروتنها اگر G، یک ۲-گروه آبلی مقدماتی باشد.

□

نامساوی‌های باقیمانده در این بخش با $\mathbb{Z}_n$ مرتبط هستند و لذا دارای طبیعت نظریه اعدادی هستند.

لم ۱۰.۱.۳. *فرض کنیم $n > ۱$ و p بزرگ‌ترین مقسوم‌علیه اول n باشد. دراین‌صورت*

$$\phi(n) \geq \frac{n}{p} \tag{۹.۳}$$

و تساوی برقرار است اگروتنها اگر برای $\alpha \geq ۱$ و $\beta \geq ۰$، $n = ۲^\alpha ۳^\beta$.

برهان. اگر $n = p^\alpha$، آن‌گاه

$$\phi(p^\alpha) = p^{\alpha-۱}(p-۱) \geq p^{\alpha-۱} = \frac{p^\alpha}{p}.$$

در این مورد نامساوی برقرار است. تساوی برقرار است اگروتنها اگر $p = ۲$. حال فرض کنیم n، $k \geq ۲$ عامل اول متمایز داشته باشد. بنا به معادله ۴.۳،

$$\frac{\phi(n)}{n} = \frac{(p_۱ - ۱)(p_۲ - ۱)\cdots(p_k - ۱)}{(p_۱ p_۲ \cdots p_k)}.$$

توجه کنیم که $p_{i-۱} \geq p_{i+۱} - ۱$ $(۱ \leq i \leq k-۱)$، با بررسی عبارت‌های میانی داریم :

$$\frac{\phi(n)}{n} \geq \frac{(p_۱ - ۱)}{p_k} = \frac{(q-۱)}{p} \geq \frac{۱}{p},$$

تساوی زمانی برقرار است که $k = ۲$ ، $p_۱ = ۲$ و $p_۲ = ۳$.

قسمت عکس واضح است.

□

نتیجه ۱۱.۱.۳. *فرض کنیم $n > 1$ و p بزرگ‌ترین مقسوم‌علیه اول n باشد. دراین‌صورت*

$$\sum_{z \in \mathbb{Z}_n} o(z) > \frac{n^2}{p}.$$

برهان. می‌دانیم $\phi(n)$ عنصر، از مرتبه n در $\mathbb{Z}_n$ وجود دارد و بنابراین $\sum_{z\in\mathbb{Z}_n} o(z) > n\phi(n) \geq \frac{n^2}{p}$، که نامساوی اول اکید است زیرا عنصر همانی $\mathbb{Z}_n$ را درنظر نگرفته‌ایم. □

لم ۱۲.۱.۳. *فرض کنیم G یک گروه غیردوری از مرتبه متناهی n باشد. دراین‌صورت*

$$\sum_{g \in G} o(g) < \sum_{z \in \mathbb{Z}_n} o(z).$$

برهان. فرض کنیم G یک گروه متناهی از مرتبه n باشد که $\sum_{g\in G} o(g) \geq \sum_{z\in\mathbb{Z}_n} o(z)$. قرار می‌دهیم $\psi(G) = \sum_{g\in G} o(g)$. باید نشان دهیم G دوری است. اگر $n = 1$، G دوری است. پس $n > 1$ را در نظر می‌گیریم و روی n استقرا می‌کنیم.
طبق نتیجه قبل، میانگین مرتبه‌های عناصر G به صورت زیر است

$$\frac{\psi(G)}{|G|} \geq \frac{\psi(\mathbb{Z}_n)}{n} > \frac{n^2/p}{n} = \frac{n}{p}.$$

چون ممکن نیست که همه عناصر G، دارای مرتبه کمتر از میانگین باشند، پس یک عنصر $x \in G$ وجود دارد به‌طوری‌که مرتبه آن بیش‌تر از میانگین است و لذا $o(x) > \frac{n}{p}$. دراین‌صورت $|G : \langle x\rangle| < p$ و بنابراین $\mathrm{Core}(\langle x\rangle)$ شامل یک p-زیرگروه سیلوی P از G است و P دوری است. چون $\mathrm{Core}(\langle x\rangle)$ دوری است پس P در $\mathrm{Core}(\langle x\rangle)$ مشخصه است و لذا P در G نرمال است. طبق نتیجه ۳۱.۱.۱، $\psi(G) \leq \psi(P)\psi(\frac{G}{P})$ و تساوی برقرار است اگروتنهااگر P در G مرکزی باشد.
فرض کنیم Q، p-زیرگروه سیلوی $\mathbb{Z}_n$ باشد. توجه کنیم که P و Q گروه‌های دوری با مرتبه‌های مساوی هستند و لذا $P \cong Q$ و $\psi(P) = \psi(Q)$. داریم

$$\psi(P)\psi(\frac{G}{P}) \geq \psi(G) \geq \psi(\mathbb{Z}_n) = \psi(Q)\psi(\frac{\mathbb{Z}_n}{Q}),$$

که تساوی به کار برده شده در بالا، بنا به نتیجه ۳۱.۱.۱، برقرار است. با حذف $\psi(P) = \psi(Q)$، داریم $\psi(G/P) \geq \psi(\mathbb{Z}_n/Q)$. اما $\mathbb{Z}_n/Q$ دوری است و G/P دارای مرتبه یکسان با $\mathbb{Z}_n/Q$ است که کم‌تر از n است لذا، G/P دوری است. دراین‌صورت $G/P \cong \mathbb{Z}_n/Q$ و بنابراین $\psi(G/P) = \psi(\mathbb{Z}_n/Q)$.
این ایجاب می‌کند که تساوی در نامساوی‌های بالا برقرار و لذا P در G مرکزی باشد.
چون P مرکزی و G/P دوری است، ایجاب می‌کند که G آبلی باشد و چون P یک زیرگروه سیلوی G است، می‌توانیم بنویسیم $G = P \times B$ که $B \cong G/P$ و دوری است. بنابراین G حاصل‌ضرب مستقیم گروه‌های دوری از مرتبه‌های نسبت به هم اول است و لذا G دوری است. □

قضیه ۱۳.۱.۳. *در میان همه گروه‌های متناهی از مرتبه داده شده، گروه دوری از آن مرتبه، بیش‌ترین تعداد یال را در گراف توانی جهت‌دار خود داراست.*

برهان. از لم ۱۲.۱.۳ و معادله ۱.۳ نتیجه می‌شود. □

هدف بعدی بهبود کران $\sum_{d|n}\phi(d)d > \frac{n^{۲}}{p}$ داده شده در [۲] است.

نتیجه ۱۴.۱.۳. *اگر $n > ۱$، به صورت تجزیه عوامل اول $۲^{\alpha_۱}$، $۲^{\alpha_۱}۳^{\alpha_۲}$، $۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}$ یا $۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}۷^{\alpha_۴}$ نباشد که $\alpha_۱$، $\alpha_۲$، $\alpha_۳$ و $\alpha_۴$ اعداد مثبتی هستند، آن‌گاه*

$$\sum_{d|n}\phi(d)d \geq \left(\prod_{h=۱}^{k}\frac{p_h+۱}{p_h}\right).\frac{n^{۲}}{p}. \tag{۱۰.۳}$$

اگر n توانی از ۲ نباشد، آن‌گاه

$$\sum_{d|n}\phi(d)d \geq \left(\frac{q+۱}{q}\right).\frac{n^{۲}}{p}. \tag{۱۱.۳}$$

برهان. رابطه ۱۰.۳ را با استقرا روی k مقسوم‌علیه اول متمایز ثابت می‌کنیم. می‌نویسیم

$$S(n)=\sum_{d|n}\phi(d)d, \quad R(n)=\left(\prod_{h=۱}^{k}\frac{p_h+۱}{p_h}\right).\frac{n^{۲}}{p}$$

بنابراین

$$\frac{S(n)}{R(n)} = p.\prod_{h=۱}^{k}\frac{p_h^{۲}+\frac{۱}{p_h^{۲\alpha_h-۱}}}{(p_h+۱)^{۲}}.$$

توجه می‌کنیم رابطه ۱۰.۳ زمانی برقرار است که $\frac{S(n)}{R(n)} \geq ۱$. عبارت $\frac{۱}{p_h^{۲\alpha_h-۱}}$ یک تابع نزولی از α_h است و α_h می‌تواند مقدار بزرگی باشد. قرار می‌دهیم

$$T(n) := p.\prod_{h=۱}^{k}\frac{p_h^{۲}}{(p_h+۱)^{۲}}.$$

چون $\frac{S(n)}{R(n)} \geq T(n)$، لذا برای اثبات رابطه ۱۰.۳، کافیست نشان دهیم $T(n) \geq ۱$. توجه می‌کنیم که $T(n)$ به توان‌ها بستگی ندارد. ابتدا فرض می‌کنیم n، به‌گونه‌ای باشد که به جز عوامل اول $۲^{\alpha_۱}$، $۲^{\alpha_۱}۳^{\alpha_۲}$، $۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}$ یا $۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}۷^{\alpha_۴}$، عامل اول ۱۱ را نیز داشته باشد. پس

$$T(۲^{\alpha_۱}۱۱^{\alpha_۲})=\frac{۵۳۲۴}{۱۲۹۶}, \qquad T(۲^{\alpha_۱}۳^{\alpha_۲}۱۱^{\alpha_۳})=\frac{۴۷۹۱۶}{۲۰۷۳۶},$$
$$T(۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}۱۱^{\alpha_۴})=\frac{۳۳۲۷۵}{۲۰۷۳۶}, \; T(۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}۷^{\alpha_۴}۱۱^{\alpha_۵})=\frac{۱۶۳۰۴۷۵}{۱۳۲۷۱۰۴}.$$

چون برای $p > ۱$، $\frac{p^{۳}}{(p+۱)^{۲}}$ صعودی است لذا اگر به جای ۱۱، عامل اول p قرار دهیم، آن‌گاه $T(n) \geq ۱$.

حال فرض کنیم برای $k \geq ۲$، $n = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_k^{\alpha_k}$ و $n' = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_{k-۱}^{\alpha_{k-۱}}$. فرض کنیم برای n' حکم برقرار باشد بنابراین بنا به استقرا داریم $p_k \geq p_{k-۱} + ۲$ و $S(n') \geq R(n')$. مشاهده می‌کنیم

$$S(n) = S(n').\frac{p_k^{۲\alpha_k+۱}+۱}{p_k+۱}, \quad R(n) = R(n').p_{k-۱}.\frac{p_k+۱}{p_k}.\frac{p_k^{۲\alpha_k}}{p_k}.$$

چون $p_{k-۱} \leq p_k - ۲$، محاسبه می‌کنیم

$$\frac{S(n)}{R(n)} = \frac{S(n')}{R(n')}\left(\frac{p^۲(p+p^{-۲\alpha_k})}{(p+۱)^۲ p_{k-۱}}\right) \geq \frac{S(n')}{R(n')}\left(\frac{p^۳+p^{-۲\alpha_k+۲}}{p^۳-۳p-۲}\right) \geq ۱.$$

لذا رابطه ۱۰.۳ بنا به استقرا برقرار است.

چون $\frac{p_h+۱}{p_h} > ۱$، رابطه ۱۱.۳ برای غیر از تجزیه‌هایی که در فرض ذکر شد، برقرار است. چون n توانی از ۲ نیست، بنابراین تنها نیاز داریم سه حالت را برای رابطه ۱۱.۳ در نظر بگیریم. می‌نویسیم

$$Q(n) = (\frac{q+۱}{q}).\frac{n^۲}{p}, \quad U(n) = \frac{pq}{q+۱}\prod_{h=۱}^{k}\frac{p_h}{p_h+۱}.$$

بنابراین

$$\frac{S(n)}{Q(n)} = \frac{pq}{q+۱}\prod_{h=۱}^{k}\frac{p_h+\frac{۱}{p_h^{۲\alpha_h}}}{p_h+۱} \geq U(n).$$

برای اثبات رابطه ۱۱.۳، کافیست نشان دهیم برای nهایی که توانی از ۲ نیستند، $U(n) \geq ۱$. داریم

$$U(۲^{\alpha_۱}۳^{\alpha_۲}) = ۱,\ U(۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}) = \frac{۲۵}{۱۸},\ U(۲^{\alpha_۱}۳^{\alpha_۲}۵^{\alpha_۳}۷^{\alpha_۴}) = \frac{۲۴۵}{۱۸}.$$

لذا حکم برای همه nها زمانی که n توانی از ۲ نباشد، برقرار است. $\square$

لم ۱۵.۱.۳. *فرض کنیم $z \in \mathbb{Z}_n$ و $e = o(z)$. دراین‌صورت*

$$\deg(z) \geq e - ۱ + \phi(e)(\frac{n}{e} - ۱),$$

و تساوی برقرار است اگروتنها اگر e و $\frac{n}{e}$ نسبت به هم اول باشند.

برهان. معادله ۸.۳ را در نظر می‌گیریم. عبارت $\frac{(d,e)}{\phi((d,e))}$، حداقل یک است و تساوی زمانی برقرار است که $(d,e) = ۱$. اگر $\frac{n}{e}$ هیچ مقسوم علیه اولی، که نسبت به e اول باشد، نداشته باشد، در این‌صورت نامساوی باید اکید باشد. $\square$

لم ۱۶.۱.۳. *فرض کنیم برای $\alpha > ۱$، n با ۲^α برابر نباشد. دراین‌صورت*

$$\begin{cases} \sum_{z\in\mathbb{Z}_n} \deg(z) \geq ۲\frac{n^۲}{p} + \frac{n}{p} - ۱, & \phi(n) \leq \frac{n}{q} \\ \sum_{z\in\mathbb{Z}_n} \deg(z) > (n-۱)\left(\frac{n}{q}+۱\right), & \phi(n) > \frac{n}{q} \end{cases}$$

برهان. برای هر عدد اول p (به غیر از ۲)، بنا به معادله ۴.۳،

$$\phi(p^\alpha) = p^{\alpha-1}(p-1) > \frac{p^\alpha}{p}$$

و بنا به قضیه ۱۵.۱.۲ داریم

$$|E(\mathbb{Z}_{p^\alpha})| = \frac{p^\alpha(p^\alpha-1)}{2} > \frac{p^\alpha}{p}$$

بنابراین فرض می‌کنیم n، توانی از یک عدد اول نیست.

هر $\phi(n)$ تا مولد $\mathbb{Z}_n$ مانند عنصر همانی، درجه $n-1$ دارد. بنابراین از جمع درجه‌های مولدها و عنصر همانی داریم

$$\sum_z \deg(z) = \phi(n)(n-1) + n - 1 = \big(\phi(n)+1\big)(n-1).$$

اگر $\phi(n) > \frac{n}{q}$، آن‌گاه

$$\sum_{z\in\mathbb{Z}_n} \deg(z) > (n-1)\Big(\frac{n}{q}+1\Big) > \frac{n^2}{q}.$$

بنا به معادله ۸.۳، برای $z \in \mathbb{Z}_n$،

$$\deg(z) = \mathrm{o}(z) - 1 - \phi(\mathrm{o}(z)) + \sum_{d|\frac{n}{\mathrm{o}(z)}} \phi(d\mathrm{o}(z)). \qquad (۱۲.۳)$$

در تساوی فوق، جمعوند متناظر با $d=1$، $\phi(\mathrm{o}(z))$ و جمعوند متناظر با $d=\frac{n}{\mathrm{o}(z)}$، $\phi(n)$ است. بنا به رابطه ۹.۳ داریم

$$\phi(n) \geq \frac{n}{p}.$$

بنابراین $\deg(z) \geq \mathrm{o}(z) - 1 + \frac{n}{p}$. ادعا می‌کنیم تساوی برای همه عناصر غیرمولد و غیرهمانی برقرار است اگروتنها اگر $n=6$. فرض کنیم $x \in \mathbb{Z}_n$ یک عنصر غیرهمانی و غیرمولد از مرتبه p باشد. با توجه به تساوی ۱۲.۳، تساوی زمانی برقرار است که $\frac{n}{o(x)}$، اول باشد. پس برای عدد اول q، $n=pq$. اگر $p=q$، داریم

$$\phi(n) = \phi(p^2) = p(p-1)$$

لذا طبق لم ۷.۱.۳،

$$\begin{aligned}\deg(x) &= p - 1 - \phi(p) + \sum_{d|\frac{n}{p}=p} \phi(dp)\\ &= p-1-\phi(p)+\phi(p)+\phi(p^2) = p-1+p(p-1)\end{aligned}$$

در نتیجه داریم

$$\begin{aligned} p-۱+p(p-۱) &= \deg(x) = p-۱+p \\ &\Rightarrow p(p-۱)=p \;\Rightarrow\; p=۲ \end{aligned}$$

بنابراین n توانی از ۲ است که تناقض است. لذا باید $p \neq q$. دراین‌صورت طبق معادله ۴.۳ داریم

$$\phi(n)=\phi(pq)=(p-۱)(q-۱)$$

و لذا

$$\begin{aligned} \deg(x) &= p-۱-\phi(p)+\sum_{d|\frac{n}{p}=q}\phi(dp) \\ &= p-۱-\phi(p)+\phi(p)+\phi(pq)=p-۱+(p-۱)(q-۱) \end{aligned}$$

در نتیجه داریم

$$\begin{aligned} p-۱+(p-۱)(q-۱) &= \deg(x)=p-۱+\frac{n}{p} \\ &\Rightarrow \quad (p-۱)(q-۱)=q \\ &\Rightarrow \quad \begin{cases} q=۲ \\ p=۳ \end{cases} \quad \Rightarrow n=۶ \end{aligned}$$

حال

$$\begin{aligned} \sum_{z\in\mathbb{Z}_n}\deg(z) &\geq \left(\sum_{z\in\mathbb{Z}_n}\mathrm{o}(z)\right)-n+(n-\phi(n)-۱)\frac{n}{p}+n-۱ \\ &\geq \left(\sum_{z\in\mathbb{Z}_n}\mathrm{o}(z)\right)+\frac{n^۲}{p}-(\phi(n)-۱)\frac{n}{p}-۱. \end{aligned}$$

اگر $\phi(n)\leq\frac{n}{q}$، در این‌صورت بنا به نتیجه ۱۴.۱.۳ ،

$$\sum_{z\in\mathbb{Z}_n}\deg(z)\geq\frac{q+۱}{q}\frac{n^۲}{p}+\frac{n^۲}{p}-\left(\frac{n}{q}-۱\right)\frac{n}{p}-۱=۲\frac{n^۲}{p}+\frac{n}{p}-۱.$$

□

برای هر گراف بدون جهت Γ داریم

$$|E(\Gamma)|=\frac{۱}{۲}\sum_{g\in\Gamma}\deg(g).$$

لم ۱۷.۱.۳. *فرض کنیم $\phi(n)>\frac{n}{q}$. دراین‌صورت n فرد است.*

برهان. با توجه به معادله ۴.۳، $\phi(n) > \frac{n}{q}$ اگروتنها اگر

$$(p_1 - 1)\cdots(p_k - 1) > p_2 \cdots p_k.$$

فرض کنیم $q = p_1 = 2$، بنابراین $p_1 - 1 = 1$. دراین‌صورت از نامساوی فوق داریم:

$$(p_2 - 1)\cdots(p_k - 1) > p_2 \cdots p_k$$

که یک تناقض است. لذا n فرد است. □

لم ۱۸.۱.۳. *فرض کنیم r و s اعداد طبیعی باشند به طوری که $r \mid s$. در این‌صورت*

$$2r - \phi(r) - 1 \geq 2s - \phi(s) - 1$$

و تساوی برقرار است اگروتنها اگر $r = s$.

برهان. می‌نویسیم $r = st$ و می‌دانیم $\phi(st) \leq \phi(s)t$. در این‌صورت

$$2r - \phi(r) - 1 \geq 2st - \phi(s)t - 1 = t\big(2s - \phi(s)\big) - 1 \geq 2s - \phi(s) - 1.$$

واضح است که اگر $t > 1$، آن‌گاه این نامساوی اکید است. □

۲.۳ حاصل‌ضرب مستقیم و نیم‌مستقیم

فرض کنیم G حاصل‌ضرب مستقیم زیرگروه‌های نرمال U و V باشد، $u \in U$ و $v \in V$. دراین‌صورت عناصر G را با uv نمایش می‌دهیم.

لم ۱.۲.۳. *فرض کنیم G حاصل‌ضرب مستقیم زیرگروه‌های نرمال U و V باشد و*

$$\begin{aligned} D =& \{(uv, u'v') \mid uu' \in \overrightarrow{E}(U), vv' \in \overrightarrow{E}(V)\} \\ & \cup \{(uv, u'v) \mid uu' \in \overrightarrow{E}(U), v \in V\} \\ & \cup \{(uv, uv') \mid u \in U, vv' \in \overrightarrow{E}(V)\}, \end{aligned}$$

$$\begin{aligned} B =& \{(uv, u'v') \mid uu' \in \overleftrightarrow{E}(U), vv' \in \overleftrightarrow{E}(V)\} \\ & \cup \{(uv, u'v) \mid uu' \in \overleftrightarrow{E}(U), v \in V\} \\ & \cup \{(uv, uv') \mid u \in U, vv' \in \overleftrightarrow{E}(V)\}. \end{aligned}$$

در این‌صورت

$$\overrightarrow{E}(U \times V) \subseteq D, \tag{۱۳.۳}$$

$$\overleftrightarrow{E}(U \times V) \subseteq B. \tag{۱۴.۳}$$

برهان. فرض کنیم $u, u' \in U$ و $v, v' \in V$ و $uv \to u'v'$ در $\overrightarrow{\mathcal{P}}(U \times V)$ باشد. بنابراین برای برخی عدد صحیح مثبت c، $u'v' = (uv)^c = u^c v^c$. لذا $u' = u^c$ و $v' = v^c$. بنابراین یکی از شرایط زیر برقرار است :

(۱) $u \to u'$ در $\overrightarrow{\mathcal{P}}(U)$ و $v \to v'$ در $\overrightarrow{\mathcal{P}}(V)$ باشد،

(۲) $u = u'$ و $v \to v'$ در $\overrightarrow{\mathcal{P}}(V)$ باشد یا

(۳) $u \to u'$ در $\overrightarrow{\mathcal{P}}(U)$ و $v' = v$ باشد.

بنابراین عبارت ۱۳.۳ برقرار است. حال فرض کنیم $uv \leftrightarrow u'v'$ در $\overleftrightarrow{\mathcal{P}}(U \times V)$ باشد. همانند مبحث بالا، یکی از شرایط زیر برقرار است :

(۱′) $u \leftrightarrow u'$ در $\overleftrightarrow{\mathcal{P}}(U)$ و $v \leftrightarrow v'$ در $\overleftrightarrow{\mathcal{P}}(V)$ باشد،

(۲′) $u = u'$ و $v \leftrightarrow v'$ در $\overleftrightarrow{\mathcal{P}}(V)$ باشد یا

(۳′) $u \leftrightarrow u'$ در $\overleftrightarrow{\mathcal{P}}(U)$ و $v' = v$ باشد.

بنابراین عبارت ۱۴.۳ برقرار است. □

لم ۲.۲.۳. *با مفروضات لم ۱.۲.۳ ، شرایط زیر برقرار است :*

(الف) $D = \overrightarrow{E}(U \times V)$ *اگروتنها اگر* $(|U|, |V|) = ۱$،

(ب) اگر $(|U|, |V|) = ۱$، *آن‌گاه* $B = \overleftrightarrow{E}(U \times V)$.

برهان. (الف) فرض کنیم $(|U|, |V|) = ۱$، $u \to u'$ در $\overrightarrow{\mathcal{P}}(U)$ و $v \to v'$ در $\overrightarrow{\mathcal{P}}(V)$ باشند. دراین‌صورت $uv \to u'v'$ در $\overrightarrow{\mathcal{P}}(U \times V)$ است. همچنین برای هر $u \in U$ و $v \in V$، $uv \to uv'$ در $\overrightarrow{\mathcal{P}}(U \times V)$ و $uv \to u'v$ در $\overrightarrow{\mathcal{P}}(U \times V)$ قرار می‌گیرند. بنابراین $D \subseteq \overrightarrow{E}(U \times V)$ ولذا تساوی برقرار است.
حال نشان می‌دهیم که تساوی در شرایط دیگر برقرار نیست. فرض کنیم عدد اول p وجود داشته باشد که $(|U|, |V|)$ را عاد کند. دراین‌صورت U و V شامل به ترتیب عناصر u و v از مرتبه p می‌شوند. مشاهده می‌کنیم یال $uv \to ue$ وجود ندارد، ولی در زیرمجموعه سوم در تعریف D، ظاهر شده است. بنابراین $D \nsubseteq \overrightarrow{E}(U \times V)$.

(ب) اثبات مشابه اثبات (الف) است.

□

نتیجه ۳.۲.۳. *فرض‌کنیم* $G = U \times V$ *و* $(|U|, |V|) = ۱$. *دراین‌صورت*

(الف) مجموعه یال‌های گراف توانی جهت‌دار G *برابر است با*

$$|\overrightarrow{E}(G)| = |\overrightarrow{E}(U \times V)| = |\overrightarrow{E}(U)|.|\overrightarrow{E}(V)| + |\overrightarrow{E}(U)|.|V| + |U|.|\overrightarrow{E}(V)|.$$

(ب) مجموعه یال‌های دوطرفه گراف توانی جهت‌دار G برابر است با

$$|\overleftrightarrow{E}(G)| = |\overleftrightarrow{E}(U\times V)| = ۲|\overleftrightarrow{E}(U)|.|\overleftrightarrow{E}(V)| + |\overleftrightarrow{E}(U)|.|V| + |U|.|\overleftrightarrow{E}(V)|.$$

برهان. با مراجعه به اثبات رابطه ۱۳.۳، تعداد $|\overrightarrow{E}(U)|.|\overrightarrow{E}(V)|$ یال در مورد (۱)، $|U|.|\overrightarrow{E}(V)|$ یال در مورد (۲) و $|\overrightarrow{E}(U)|.|V|$ یال در مورد (۳) وجود دارند. بنابراین (الف) برقرار است. با مراجعه به اثبات رابطه ۱۴.۳، تعداد $۲|\overleftrightarrow{E}(U)|.|\overleftrightarrow{E}(V)|$ یال در مورد (۱′) وجود دارد زیرا برای هر $\{u,u'\}\in\overleftrightarrow{\mathcal{P}}(U)$ و $\{v,v'\}\in\overleftrightarrow{\mathcal{P}}(V)$، داریم $u'v'\leftrightarrow uv$ و $u'v\leftrightarrow uv'$، که یال‌های دوطرفه متمایز در $\overleftrightarrow{E}(G)$ هستند. تعداد $|U|.|\overleftrightarrow{E}(V)|$ یال در مورد (۲′) و $|\overleftrightarrow{E}(U)|.|V|$ یال در مورد (۳′) وجود دارند. بنابراین (ب) برقرار است. □

لم ۴.۲.۳. *فرض کنیم U، V و V' گروه‌های متناهی باشند که $|V'|=|V|$ و $(|U|,|V|)=۱$. دراین‌صورت*

$$\begin{aligned}|E(U\times V)|-|E(U\times V')| &= (|\overrightarrow{E}(U)|-۲|\overleftrightarrow{E}(U)|)(|\overrightarrow{E}(V)|-|\overrightarrow{E}(V')|)\\ &\quad+(۲|\overleftrightarrow{E}(U)|+|U|)(|E(V)|-|E(V')|).\end{aligned}$$

برهان. با استفاده از معادله ۳.۳، $|E(U\times V)|-|E(U\times V')|$ را بسط می‌دهیم :

$$\begin{aligned}|E(U\times V)|-|E(U\times V')| =&(|\overrightarrow{E}(U\times V)|-|\overrightarrow{E}(U\times V')|)\\ &-(|\overleftrightarrow{E}(U\times V)|-|\overleftrightarrow{E}(U\times V')|).\end{aligned}$$

چون $|V'|=|V|$، از نتیجه ۳.۲.۳ داریم

$$|\overrightarrow{E}(U\times V)|-|\overrightarrow{E}(U\times V')| = (|\overrightarrow{E}(U)|+|U|)(|\overrightarrow{E}(V)|-|\overrightarrow{E}(V')|),$$
$$|\overleftrightarrow{E}(U\times V)|-|\overleftrightarrow{E}(U\times V')| = (۲|\overleftrightarrow{E}(U)|+|U|)(|\overleftrightarrow{E}(V)|-|\overleftrightarrow{E}(V')|).$$

در خط دوم، از معادله ۳.۳، برای نوشتن $|\overleftrightarrow{E}(V)|=|\overrightarrow{E}(V)|-|E(V)|$ و به طور مشابه برای $|\overleftrightarrow{E}(V')|$ استفاده می‌کنیم. لذا

$$|\overleftrightarrow{E}(U\times V)|-|\overleftrightarrow{E}(U\times V')| = (۲|\overleftrightarrow{E}(U)|+|U|)(|\overleftrightarrow{E}(V)|-|\overleftrightarrow{E}(V')|).$$

با ساده کردن رابطه فوق، نتیجه مطلوب بدست می‌آید. □

نتیجه ۵.۲.۳. *فرض کنیم U، V و V' گروه‌های متناهی باشند که $|V'|=|V|$ و $(|U|,|V|)=۱$. فرض کنیم $|E(V)|\geq|E(V')|$ و $|\overrightarrow{E}(V)|\geq|\overrightarrow{E}(V')|$. دراین‌صورت*

$$|E(U\times V)|\geq|E(U\times V')|,$$

و تساوی برقرار است اگروتنها اگر $|E(V)|=|E(V')|$ و $|\overrightarrow{E}(V)|=|\overrightarrow{E}(V')|$.

برهان. واضح است که $|\overrightarrow{E}(U)| > ۲|\overleftrightarrow{E}(U)|$، زیرا هر یال دوطرفه در $\overrightarrow{E}(U)$ دوبار شمرده می‌شود و همچنین $\overrightarrow{E}(U)$، شامل یال‌های یک طرفه از هر عنصر U به عنصر همانی است.
بوضوح، $۲|\overleftrightarrow{E}(U)| + |U| > ۰$. از لم ۴.۲.۳ داریم

$$|E(U \times V)| - |E(U \times V')| \geq ۰$$

بنابراین نتیجه حاصل می‌شود.
تساوی برقرار است اگروتنها اگر $|E(V)| = |E(V')|$ و $|\overrightarrow{E}(V)| = |\overrightarrow{E}(V')|$. چون همه عبارت‌های سمت راست مثبت هستند لذا، سمت راست صفر است اگروتنها اگر این تساوی‌ها برقرار باشد. □

عناصر $G = U \rtimes_\varphi V$ می‌توانند درست همانند حاصل‌ضرب مستقیم، با حاصل‌ضرب دکارتی مجموعه‌های U و V، معرفی شوند. از $*$، برای حاصل‌ضرب گروه روی $U \rtimes_\varphi V$ استفاده می‌کنیم.
در حاصل‌ضرب مستقیم و نیم‌مستقیم برای نمایش توان c ام uv به ترتیب، از $(uv)^c$ و $(uv)^{*c}$ استفاده می‌کنیم. همچنین مرتبه uv مرتبط با ضرب متناظر، را با $o.(uv)$ و $o_*(uv)$ ومعکوس‌های متناظر، را با $(uv)^{-۱}$ و $(uv)^{*-۱}$ نشان می‌دهیم.
با این تذکر،

$$\begin{aligned}(uv)^{*c} &= \left(uu^{\varphi v}u^{\varphi v^۲}\cdots u^{\varphi v^{c-۲}}u^{\varphi v^{c-۱}}\right)\left(v^c\right),\\ (uv)^{*-۱} &= \left(u^{-۱}\right)^{\varphi v^{-۱}}\left(v^{-۱}\right).\end{aligned} \qquad (۱۵.۳)$$

لم ۶.۲.۳. *فرض کنیم G یک گروه متناهی و $G = U \rtimes_\varphi V$ حاصل‌ضرب نیم‌مستقیم زیرگروه دوری نرمال U و زیرگروه V باشد. $u \in U$ و $v \in V$ را در نظر می‌گیریم. دراین‌صورت برای برخی r،*

$$u^{\varphi v} = u^r$$

و

$$(uv)^{*c} = u^t v^c$$

که $t = ۱ + r + r^۲ + \cdots + r^{c-۱}$.

برهان. زیرگروه $\langle u\rangle$ از U را، در نظر می‌گیریم. چون U دوری است و $\langle u\rangle$ زیرگروه منحصربه‌فردی از U از مرتبه خودش است، $\langle u\rangle$ باید زیرگروه مشخصه U باشد. بنابراین برای برخی r، $u^{\varphi v} = u^r$.
حال $u^{\varphi v^b} = u^{r^b}$. بنابراین، محاسبه می‌کنیم

$$\begin{aligned}(uv)^{*c} &= \left(uu^{\varphi v}u^{\varphi v^۲}\cdots u^{\varphi v^{c-۲}}u^{\varphi v^{c-۱}}\right)\left(v^c\right)\\ &= \left(u^۱u^ru^{r^۲}\cdots u^{r^{c-۱}}\right)\left(v^c\right)\\ &= \left(u^{۱+r+r^۲+\cdots+r^{c-۱}}\right)\left(v^c\right) = u^tv^c.\end{aligned}$$

□

لم ۷.۲.۳. *فرض کنیم G یک گروه متناهی و $G = U \rtimes_\varphi V$ حاصل‌ضرب نیم‌مستقیم زیرگروه دوری نرمال U و زیرگروه V باشد. دراین‌صورت*

$$\overrightarrow{E}(U \rtimes_\varphi V) \subseteq D, \tag{۱۶.۳}$$

$$\overleftrightarrow{E}(U \rtimes_\varphi V) \subseteq B. \tag{۱۷.۳}$$

به ویژه، اگر $(|U|, |V|) = ۱$، آن‌گاه

$$E(U \rtimes_\varphi V) \subseteq E(U \times V),$$
$$\overleftrightarrow{E}(\mathbb{Z}_{|U|} \rtimes_\varphi \mathbb{Z}_{|V|}) \subseteq \overleftrightarrow{E}(\mathbb{Z}_{|U|} \times \mathbb{Z}_{|V|}).$$

برهان. $u, u' \in U$ و $v, v' \in V$ را در نظر می‌گیریم و قرار می‌دهیم $u^{\varphi v} = u^r$. فرض کنیم $uv \to u'v'$ در $\overrightarrow{\mathcal{P}}(U \rtimes_\varphi V)$ باشد. دراین‌صورت همانند لم ۶.۲.۳ برای برخی t،

$$u'v' = (uv)^{*c} = u^t v^c.$$

چون حاصل‌ضرب، نیم‌مستقیم است، $u' = u^t$ و $v' = v^c$. مانند اثبات لم ۱.۲.۳، به نتیجه یکسان می‌رسیم. □

لم ۸.۲.۳. *فرض کنیم G یک گروه متناهی و $G = U \rtimes_\varphi V$ حاصل‌ضرب نیم‌مستقیم زیرگروه نرمال آبلی U و زیرگروه V باشدکه مرتبه‌های U و V نسبت به هم اول هستند. دراین‌صورت برای هر $u \in U$ و $v \in V$،*

$$o_*(uv) \mid o.(uv).$$

برهان. برای اثبات نشان می‌دهیم $(uv)^{*o.(uv)}$، همانی $U \rtimes_\varphi V$ است. توجه کنیم که

$$o.(uv) = \frac{o(u)o(v)}{(o(u), o(v))} = o(u)o(v).$$

بنا به معادله ۱۵.۳،

$$\begin{aligned}(uv)^{*o(v)} &= \left(uu^{\varphi v}u^{\varphi v^۲} \cdots u^{\varphi v^{o(v)-۲}} u^{\varphi v^{o(v)-۱}}\right)\left(v^{o(v)}\right)\\ &= \left(uu^{\varphi v}u^{\varphi v^۲} \cdots u^{\varphi v^{o(v)-۲}} u^{\varphi v^{o(v)-۱}}\right)(e).\end{aligned}$$

بنابراین چون U آبلی است، داریم

$$\begin{aligned}(uv)^{*o.(uv)} &= \left[\left(uu^{\varphi v}u^{\varphi v^۲} \cdots u^{\varphi v^{o(v)-۲}} u^{\varphi v^{o(v)-۱}}\right)(e)\right]^{*o(u)}\\ &= \left(u^{o(u)}\left(u^{\varphi v}\right)^{o(u)}\left(u^{\varphi v^۲}\right)^{o(u)} \cdots \left(u^{\varphi v^{o(v)-۲}}\right)^{o(u)}\left(u^{\varphi v^{o(v)-۱}}\right)^{o(u)}\right)(e)\\ &= (e)(e).\end{aligned}$$

همان‌طور که نیاز داشتیم. □

لم ۹.۲.۳. *فرض کنیم G یک گروه متناهی از مرتبه n باشد که n توانی از ۲ نیست و $r > 2$ یک مقسوم‌علیه اول n است. فرض کنیم G شامل یک r−متمم دوری و یک r−سیلو زیرگروه نرمال، که خودش شامل یک زیرگروه دوری از اندیس r است، باشد. دراین‌صورت دوسویی $\lambda : G \to \mathbb{Z}_n$ وجود دارد به‌طوری‌که برای هر $g \in G$،*

$$o(g) \big| o(\lambda(g)).$$

برهان. فرض کنیم U یک r−متمم دوری G و R یک r−زیرگروه سیلوی نرمال G، که شامل یک زیرگروه دوری C از اندیس r است، باشند. قرار می‌دهیم $|R| = r^{\alpha}$. با درنظر گرفتن مرتبه گروه، $G = RU$ و $R \cap U = \{e\}$. چون R در G نرمال است، $G = R \rtimes_{\varphi} U$ و $\frac{G}{R} \cong U$.
فرض کنیم R ناآبلی باشد. طبق لم ۲۵.۱.۱، مرکز R، $(Z(R))$، مرتبه $r^{\alpha-2}$ دارد. حال $Z(R) \subseteq C$، چون درغیراین‌صورت، از $R = Z(R)C$، ایجاب می‌شود که R آبلی باشد و این متناقض با فرض است. بنابراین $Z(R)$ دوری و علاوه براین زیرگروه منحصربه‌فرد C از اندیس r، است. حال $Z(R)$ یک زیرگروه مشخصه زیرگروه (مشخصه) نرمال R، است لذا $Z(R)$ در G نرمال است. چون $Z(R)$ یک زیرگروه دوری نرمال G است، از لم ۸.۲.۳ داریم

$$\forall ab \in Z(R) \rtimes_{\varphi} U, \qquad o_*(ab) \mid o.(ab).$$

می‌بینیم که $Z(R) \times U$ دوری است بنابراین، می‌توانیم λ را تحدید به $Z(R) \rtimes_{\varphi} U$ بگیریم که یک دوسویی از $Z(R) \rtimes_{\varphi} U$ به $Z(R) \times U \cong \mathbb{Z}_{|Z(R)|} \times \mathbb{Z}_{|U|} \subseteq \mathbb{Z}_n$ باشد زمانی‌که

$$\forall x \in Z(R) \rtimes_{\varphi} U, \qquad o(x) \mid o(\lambda(x)).$$

حال چون $G = RU$، می‌توانیم بنویسیم

$$G = Z(R)U \cup (R - Z(R))U.$$

فرض کنیم $x \in (R - Z(R))U$. دراین‌صورت برای $r \in R - Z(R)$ و $u \in U$، $x = ru$. چون R دوری نیست پس شامل عنصری از مرتبه r^{α} نمی‌باشد. بنابراین مرتبه x، به $r^{\alpha-1}o(u)$، بخش‌پذیر است. $\mathbb{Z}_{|U|}$ بر اساس U معرفی می‌شود. بنابراین

$$\mathbb{Z}_n = \mathbb{Z}_{|Z(R)|}U \cup (\mathbb{Z}_{r^{\alpha}} - \mathbb{Z}_{|Z(R)|})U.$$

چون عناصر $\mathbb{Z}_{r^{\alpha}} - \mathbb{Z}_{|Z(R)|}$ از مرتبه $r^{\alpha-1}$ یا r^{α} هستند، داریم

$$\forall z \in \mathbb{Z}_{r^{\alpha}} - \mathbb{Z}_{|Z(R)|}, \qquad r^{\alpha-1}o(u) \mid o(z)o(u).$$

بنابراین هر دوسویی از $G - (Z(R) \rtimes_{\varphi} U)$ به $\mathbb{Z}_n - \mathbb{Z}_{|Z(R)|}\mathbb{Z}_{|U|}$، λ را به کل G با خواص مطلوب، بسط خواهد داد.

حال فرض کنیم R آبلی باشد. اگر R دوری باشد، آن‌گاه بنا به لم ۸.۲.۳، چیزی برای اثبات باقی نمی‌ماند. فرض کنیم R دوری نباشد. دراین‌صورت از لم ۸.۲.۳ داریم

$$\forall ab \in R \rtimes_\varphi U, \qquad o_*(ab) \mid o.(ab).$$

حال کافیست نشان دهیم که یک دوسویی از $R \times U$ به $\mathbb{Z}_n$ با خاصیت مطلوب وجود دارد. بنا به فرض، R یک زیرگروه دوری از اندیس r دارد. لذا

$$R \cong \mathbb{Z}_{r^{\alpha-1}} \times \mathbb{Z}_r$$

و

$$R \times U \cong \mathbb{Z}_{r^{\alpha-1}} \times \mathbb{Z}_r \times U.$$

حال اگر بنویسیم $R \times U = (R - \mathbb{Z}_{r^{\alpha-1}})U \cup \mathbb{Z}_{r^{\alpha-1}}U$، آن‌گاه از استدلال بالا به نتیجه یکسان می‌رسیم. □

لم ۱۰.۲.۳. *فرض کنیم G یک گروه متناهی باشد و دوسویی $\lambda : G \to \mathbb{Z}_n$ وجود داشته باشد به‌طوری‌که برای هر $g \in G$، $o(g) \mid o(\lambda(g))$. دراین‌صورت $|E(G)| = |E(\mathbb{Z}_n)|$ اگروتنها اگر $G \cong \mathbb{Z}_n$.*

برهان. فرض کنیم $|E(G)| = |E(\mathbb{Z}_n)|$. بنا به لم ۱۸.۱.۳، برای هر $g \in G$،

$$2o(g) - \phi(o(g)) - 1 \leq 2o(\lambda(g)) - \phi(o(\lambda(g))) - 1.$$

طبق معادله ۳.۳ و چون λ یک دوسویی است،

$$|E(G)| = \sum_{g \in G} 2o(g) - \phi(o(g)) - 1 = \sum_{g \in G} 2o(\lambda(g)) - \phi(o(\lambda(g))) - 1 = |E(\mathbb{Z}_n)|$$

این تساوی و نامساوی قبل ایجاب می‌کند که برای هر $g \in G$،

$$2o(g) - \phi(o(g)) = 2o(\lambda(g)) - \phi(o(\lambda(g))).$$

مولد z از $\mathbb{Z}_n$ را درنظر می‌گیریم و قرار می‌دهیم $g = \lambda^{-1}(z)$. دراین‌صورت

$$2o(g) - \phi(o(g)) = 2o(\lambda(g)) - \phi(o(\lambda(g))) = 2o(z) - \phi(o(z)) = 2n - \phi(n).$$

فرض کنیم G دوری نباشد. دراین‌صورت $o(g) < n$ و $o(g)$، $n = o(z)$ را عاد می‌کند. از لم ۱۸.۱.۳ داریم $2o(g) - \phi(o(g)) < 2n - \phi(n)$ که با تساوی بالا در تناقض است بنابراین، G باید دوری و لذا یکریخت با $\mathbb{Z}_n$ باشد. عکس واضح است. □

۳.۳ بیش‌ترین تعداد یال در گراف‌های توانی

ملاحظه ۱.۳.۳. *فرض کنیم G یک گروه متناهی از مرتبه n باشد و قرارداد ملاحظه ۴.۱.۳ را برای عوامل اول n درنظر می‌گیریم.*

لم ۲.۳.۳. *تعداد یال‌های گراف توانی گروه متناهی G از مرتبه توانی از یک عدد اول، از تعداد یال‌های گراف توانی یک گروه دوری از همان مرتبه، بیش‌تر نیست.*

برهان. برهان از قضیه ۱۵.۱.۲ نتیجه می‌شود. □

لم ۳.۳.۳. *فرض کنیم G یک گروه متناهی از مرتبه n و حاصل‌ضرب نیم‌مستقیم زیرگروه سیلو دوری نرمال P و زیرگروه T باشد که مرتبه‌های P و T نسبت به هم اولند. دراین‌صورت تعداد یال‌های گراف توانی G از تعداد یال‌های گراف توانی گروه دوری از همان مرتبه، کم‌تر است.*

برهان. فرض کنیم G گروهی از کم‌ترین مرتبه باشد که تعداد یال‌های گراف توانی آن از تعداد یال‌های گراف توانی گروه دوری از همان مرتبه، کم‌تر نباشد. طبق لم ۷.۲.۳،

$$|E(P\times T)|\geq|E(P\rtimes_{\varphi}T)|=|E(G)|\geq|E(\mathbb{Z}_n)|.$$

در نظر داریم که P یکریخت با $\mathbb{Z}_{|P|}$ است. بنا به فرض باید، $(|P|,|T|)=۱$. قرار می‌دهیم $T'=\mathbb{Z}_{|T|}$ و می‌بینیم $P\times T'$ یکریخت با $\mathbb{Z}_n$ است. $\mathbb{Z}_n$ و $P\times T'$ را یکی در نظر می‌گیریم.
فرض کنیم T دوری نباشد. چون $|T|<|G|$ و چون فرض شد که G گروهی از کم‌ترین مرتبه باشد که تعداد یال‌های گراف توانی آن از تعداد یال‌های گراف توانی گروه دوری از آن مرتبه، بیش‌تر باشد، پس $|E(T)|<|E(T')|$. هم‌چنین طبق قضیه ۱۳.۱.۳، $|\overrightarrow{E}(T)|<|\overrightarrow{E}(T')|$. حال بنا به نتیجه ۵.۲.۳،

$$|E(P\times T)|<|E(P\times T')|=|E(\mathbb{Z}_n)|.$$

این ایجاب می‌کند $|E(\mathbb{Z}_n)|>|E(\mathbb{Z}_n)|$ که تناقض است.
فرض کنیم T دوری باشد. دراین‌صورت G حاصل‌ضرب نیم‌مستقیم زیرگروه‌های دوری از مرتبه‌های نسبت به هم اول است. چون $(|P|,|T|)=۱$، $P\times T$ یکریخت با $\mathbb{Z}_n$ است. بنابراین

$$|E(\mathbb{Z}_n)|\leq|E(G)|\leq|E(\mathbb{Z}_n)|=|E(P\times T)|.$$

لذا $|E(G)|=|E(\mathbb{Z}_n)|$. چون T، یک p-متمم دوری و P، یک p-زیرگروه سیلوی دوری است، طبق لم ۸.۲.۳، یک دوسویی $\theta:G\to\mathbb{Z}_n$ وجود دارد به‌طوری‌که

$$\forall g\in G,\qquad o(g)\big|o(\theta(g)).$$

حال از لم ۱۰.۲.۳ به این نتیجه می‌رسیم که G دوری است. این تناقض ایجاب می‌کند که G کوچکترین مثال نقضی برای حکم نباشد. پس حکم برقرار است. □

لم ۴.۳.۳. *فرض کنیم G یک گروه متناهی از مرتبه n و p بزرگ‌ترین مقسوم‌علیه اول n باشد. اگر $g\in G$ وجود داشته باشد که $o(g)>\dfrac{n}{p}$، آن‌گاه تعداد یال‌های گراف توانی گروه G، از تعداد یال‌های گراف توانی گروه دوری از همان مرتبه، کم‌تر است.*

برهان. چون $o(g) > \frac{n}{p}$، داریم

$$|G:\langle g\rangle| = \frac{|G|}{o(g)} < p.$$

بنابراین $\langle g\rangle$ شامل یک p-زیرگروه سیلوی P از G است. حال، P در $\langle g\rangle$ مشخصه و $\langle g\rangle$ در G نرمال است بنابراین، $P \lhd G$. طبق لم ۲۱.۱.۱، $G = P \rtimes_{\varphi} T$. حکم از لم ۳.۳.۳ نتیجه می‌شود. $\square$

لم ۵.۳.۳. *فرض کنیم G یک گروه متناهی از مرتبه n و q کوچک‌ترین مقسوم‌علیه اول n باشد. اگر $\phi(n) \leq \frac{n}{q}$، آن‌گاه تعداد یال‌های گراف توانی G از تعداد یال‌های گراف توانی گروه دوری از همان مرتبه، کم‌تر است.*

برهان. فرض کنیم حکم برقرار نباشد و G کوچک‌ترین مثال نقض برای آن باشد. دراین‌صورت $|E(G)| \geq |E(\mathbb{Z}_n)|$. در نظر داریم که طبق لم ۲.۳.۳، G دوری و n توانی از یک عدد اول نیست. به‌ویژه، n توانی از ۲ نیست.
بنا به فرض و لم ۳.۱.۳ و لم ۱۶.۱.۳،

$$\begin{aligned}\sum_{g\in G} ۲o(g) - \phi(o(g)) - ۱ &= \sum_{g\in G}\deg(g) = ۲|E(G)| \geq ۲|E(\mathbb{Z}_n)|\\ &= \sum_{z\in\mathbb{Z}_n}\deg(z) \geq ۲\frac{n^۲}{p} + \frac{n}{p} - ۱.\end{aligned}$$

-۱ را از سمت راست و $-\phi(o(e)) = -۱$ را از سمت چپ حذف می‌کنیم و سپس بقیه $-\phi(o(g))$ باقی‌مانده در چپ را حذف می‌کنیم. به دو طرف، $n = \sum_{g\in G} ۱$ را برای رسیدن به معادله زیر، اضافه می‌کنیم

$$\sum_{g\in G} ۲o(g) > ۲\frac{n^۲}{p} + \frac{n}{p} + n.$$

لذا حداقل یک $g \in G$ وجود دارد که $o(g) > \frac{n}{p}$. حکم از لم ۴.۳.۳ نتیجه می‌شود. $\square$

لم ۶.۳.۳. *فرض کنیم G یک گروه متناهی از مرتبه n و q کوچک‌ترین مقسوم‌علیه اول n باشد. اگر $\phi(n) > \frac{n}{q}$، آن‌گاه تعداد یال‌های گراف توانی G از تعداد یال‌های گراف توانی گروه دوری از همان مرتبه، کم‌تر است.*

برهان. فرض کنیم حکم برقرار نباشد و G مثال نقضی برای آن، از کم‌ترین مرتبه باشد. دراین‌صورت، مانند اثبات لم ۵.۳.۳، داریم

$$\sum_{g\in G} ۲o(g) - \phi(o(g)) - ۱ \geq (n-۱)\left(\frac{n}{q} + ۱\right).$$

مقدار هر عبارت $\phi(o(g))$، حداقل یک است لذا می‌توانیم $2n$ را به دو طرف اضافه کنیم و سپس همه $\phi(o(g))$−های باقی‌مانده را حذف می‌کنیم. هم‌چنین برای $g = e$، ۲ را از دو طرف کم می‌کنیم :

$$\sum_{g\in G-\{e\}} 2o(g) \geq (n-1)\left(\frac{n}{q}+1\right) + 2n - 2.$$

بنابراین در بین $n-1$ عبارت در سمت چپ، حداقل یک عنصر غیرهمانی g وجود دارد که

$$o(g) \geq \frac{n}{2q} + \frac{1}{2} + 1.$$

به‌ویژه، $o(g) > \frac{n}{2q}$.

فرض کنیم $p > 2q$. دراین‌صورت $\frac{n}{2q} < \frac{n}{p}$ و لذا $o(g) > \frac{n}{2q} > \frac{n}{p}$. در این مورد، طبق لم ۴.۳.۳، حکم برقرار است. توجه کنیم که $p \neq 2q$، چون p اول است.

حال فرض کنیم $p < 2q$. پس $o(g) > \frac{n}{2q}$، لذا

$$|G:\langle g\rangle| = \frac{|G|}{o(g)} < \frac{n}{(\frac{n}{2q})} = 2q.$$

توجه می‌کنیم که بنا به لم ۱۷.۱.۳، n فرد است و بنابراین $|G:\langle g\rangle|$ یک عدد اول است که آن را s می‌نامیم. حال بنا به قضیه ۴۴.۱.۱، برای عدد اول r، G یک r−سیلو زیرگروه نرمال R دارد. طبق لم ۲۱.۱.۱، G شامل یک r−متمم U است. لذا $G = R \rtimes_{\varphi} U$.

توجه می‌کنیم که برای $s \neq t$، $\langle g\rangle$ شامل همه t−زیرگروه‌های سیلوی G است. اگر $s \neq r$، آن‌گاه $R \subseteq \langle g\rangle$، بنابراین دوری است. R و U در فرض لم ۳.۳.۳ صدق می‌کنند لذا، نتیجه می‌گیریم G کوچک‌ترین مثال نقضی برای حکم نیست.

فرض کنیم $s = r$. قرار می‌دهیم $|R| = r^{\beta}$. چون $|G:\langle g\rangle| = r$، زیرگروه $H = \langle g^{r^{\beta-1}}\rangle$ از مرتبه $\frac{|G|}{r^{\beta}}$، وجود دارد. بنابراین H یک r−متمم دوری است. طبق لم ۱۷.۱.۳، $q > 2$.

حال بنا به لم ۹.۲.۳، یک دوسویی λ، از G به $\mathbb{Z}_n$ وجود دارد و برای هر $g \in G$، $o(g) \mid o(\lambda(g))$. بنابر لم ۱۰.۲.۳، G دوری است. این تناقض ایجاب می‌کند G کوچک‌ترین مثال نقضی برای حکم نباشد و لذا حکم برقرار است. □

حال آماده‌ایم تا قضیه اساسی را ثابت کنیم.

قضیه ۷.۳.۳. *در میان همه گروه‌های متناهی از مرتبه داده شده، گروه دوری از آن مرتبه بیش‌ترین تعداد یال را در گراف توانی‌اش دارد.*

برهان. چون لم‌های ۵.۳.۳ و ۶.۳.۳ در مورد احتمالات بحث کردند، هیچ مثال نقضی از کمترین مرتبه برای این قضیه، وجود ندارد لذا در حالت کلی مثال نقضی وجود ندارد. بنابراین این قضیه برای همه گروه‌های متناهی از همه مرتبه‌ها برقرار است. □

قضیه ۷.۳.۳، سبب می‌شود که قسمت (ب)، قسمت (ج) را در نتیجه زیر ایجاب کند. بقیه بدیهی هستند.

نتیجه ۸.۳.۳. *فرض کنیم G یک گروه متناهی باشد. در این‌صورت برای هر $n \geqslant 1$، گزاره‌های زیر هم‌ارزند :*

(الف) $\mathcal{P}(G) \cong \mathcal{P}(\mathbb{Z}_n)$،

(ب) $|E(G)| = |E(\mathbb{Z}_n)|$،

(ج) $G \cong \mathbb{Z}_n$.

فصل ۴

همبندی و مسطح بودن گراف‌های توانی گروه‌های دوری متناهی، دووجهی و دودوری

۱.۴ گراف توانی گروه‌های دوری متناهی

همبندی رأسی یک گراف، کم‌ترین تعداد رئوسی است که حذف آن‌ها، گراف را ناهمبند می‌کند.

قضیه ۱.۱.۴. *برای هر گروه دوری متناهی G از مرتبه n، همبندی رأسی گراف توانی G، $\kappa(\mathcal{P}(G))$، در شرایط زیر صدق می‌کند:*

(الف) $\kappa(\mathcal{P}(G)) = n - ۱$ *زمانی‌که برای عدد اول p و $m \in \mathbb{N}$،* $n = ۱$ *یا* $n = p^m$.

(ب) $\kappa(\mathcal{P}(G)) \geq \phi(n) + ۱$ *زمانی‌که n توانی از یک عدد اول نباشد. تساوی برای $n = pq$ برقرار است که p و q اعداد اول متمایز هستند.*

برهان. (الف) چون برای عدد اول p و $m \in \mathbb{N}$، G یک گروه دوری از مرتبه ۱ یا p^m است، دراین‌صورت $\mathcal{P}(G)$ یک گراف کامل روی n رأس است. بنابراین

$$\kappa(\mathcal{P}(G)) = n - ۱.$$

(ب) تعداد مولدهای G، $\phi(n)$ است. لذا زمانی‌که n توانی از یک عدد اول نباشد، $\phi(n) + ۱$ رأس از $\mathcal{P}(G)$، با همه رئوس دیگر $\mathcal{P}(G)$ مجاور است. بنابراین

$$\kappa(\mathcal{P}(G)) \geq \phi(n) + ۱.$$

فرض کنیم $n = pq$ که p و q اعداد اول متمایز هستند. هر گروه دوری متناهی G از مرتبه n، با گروه جمعی $\mathbb{Z}_n$ یکریخت است. بنابراین تساوی را فقط برای گروه جمعی $\mathbb{Z}_n = \mathbb{Z}_{pq}$ ثابت می‌کنیم.
دقیقاً $(p - ۱) + (q - ۱) = pq - \phi(pq) - ۱$ عنصر از $\mathbb{Z}_n = \mathbb{Z}_{pq}$، وجود دارند که نه همانی هستند

و نه مولد. فرض کنیم برای $1 \leq r \leq q-1$ و $1 \leq s \leq p-1$، $r\bar{p}$ با $s\bar{q}$ مجاور باشد. دراین‌صورت برای برخی اعداد صحیح مثبت m_1 و m'_1،

$$r\bar{p} = m_1 s\bar{q} \quad \text{یا} \quad s\bar{q} = m'_1 r\bar{p},$$

ابتدا $r\bar{p} = m_1 s\bar{q}$ را درنظر می‌گیریم. این ایجاب می‌کند $m_2 \in \mathbb{Z}$ وجود داشته باشد که

$$rp = m_1 sq + m_2 pq.$$

دراین‌صورت $q \mid rp$. چون q یک عدد اول است و $q \mid rp$، دراین‌صورت $q \mid r$ یا $q \mid p$. اما چون $1 \leq r < q$، لذا $q \nmid r$. هم‌چنین طبق فرض، $q \nmid p$ که تناقض است. لذا $r\bar{p} \neq ms\bar{q}$. به‌طورمشابه می‌توان ثابت کرد که $s\bar{q} \neq mr\bar{p}$.

بنابراین هیچ‌کدام از رئوس $\{\bar{p}, 2\bar{p}, \cdots, (q-1)\bar{p}\}$ با هیچ رأسی از $\{\bar{q}, 2\bar{q}, \cdots, (p-1)\bar{q}\}$ مجاور نیستند. لذا بعد از حذف همانی و همه مولدهای $\mathbb{Z}_n = \mathbb{Z}_{pq}$، به زیرگرافی از $\mathcal{P}(\mathbb{Z}_{pq})$ می‌رسیم که یک گراف ناهمبند با دو مولفه است یعنی،

(الف) گراف القاشده توسط $\{\bar{p}, 2\bar{p}, \cdots, (q-1)\bar{p}\}$، که یک گراف کامل روی $q-1$ رأس است و

(ب) گراف القاشده توسط $\{\bar{q}, 2\bar{q}, \cdots, (p-1)\bar{q}\}$، که یک گراف کامل روی $p-1$ رأس است.

بنابراین $\kappa(\mathcal{P}(\mathbb{Z}_{pq})) = \phi(pq) + 1$ و لذا اثبات را کامل می‌کند.

□

قضیه ۲.۱.۴. *فرض کنیم $G = \langle a \rangle$ یک گروه دوری متناهی از مرتبه n باشد. دراین‌صورت $\mathcal{P}(G)$ غیرمسطح است اگروتنها اگر $n \geq 5$.*

برهان. فرض کنیم $G = \langle a \rangle$ یک گروه دوری متناهی از مرتبه $n \geq 5$، باشد. برای هر عدد صحیح $n \geq 5$ (به جز ۶ و ۱۲)، می‌توانیم n را به صورت $p^r q$ بنویسیم که $p^r \geq 5$، p یک عدد اول، r و q اعداد صحیح مثبت هستند و $(p, q) = 1$.

حالت ۱ : فرض کنیم $n \neq 6, 12$. دراین‌صورت $n = p^r q$ که $p^r \geq 5$ و p، q و r در شرایط بالا صدق می‌کنند. بنا به اولین قضیه سیلو، G یک زیرگروه C از مرتبه p^r دارد. چون هر زیرگروه یک گروه دوری، دوری است لذا، C یک زیرگروه دوری G از مرتبه $p^r \geq 5$، است. بنابراین $\mathcal{P}(C) = K_{p^r}$ یک زیرگراف یکریخت با K_5 دارد. لذا طبق قضیه کوراتوفسکی، $\mathcal{P}(C)$ و درنتیجه $\mathcal{P}(G)$، غیرمسطح است.

حالت ۲ : فرض کنیم ۱۲ یا $n = 6$.

برای $n = 6$، $G = \langle a \rangle$ دقیقا دو مولد دارد که آن‌ها را a و a^5 می‌نامیم و سه عنصری که آن‌ها را a^2، a^3 و a^4 در نظر می‌گیریم، نه همانی هستند و نه مولد. رئوس e، a و a^5 با همه رئوس دیگر $\mathcal{P}(G)$، یعنی با رئوس $\{a^2, a^3, a^4\}$، مجاور هستند. بنابراین گراف توانی القاشده توسط

$$\{e, a, a^5\} \cup \{a^2, a^3, a^4\}$$

که همان $\mathcal{P}(G)$ است، یک زبرگراف از $K_{۳,۳}$ است. لذا طبق قضیه کوراتوفسکی، $\mathcal{P}(G)$ غیرمسطح است.

برای $n = ۱۲$، $\langle a^۲ \rangle$ یک زیرگروه دوری G از مرتبه ۶ است و بنابراین طبق قسمت قبل، گراف توانی $\langle a^۲ \rangle$ غیرمسطح است. لذا $\mathcal{P}(G)$، که یک زبرگراف از گراف توانی $\langle a^۲ \rangle$ است، غیرمسطح است.

برای قسمت عکس، کافی است ثابت کنیم که برای $n < ۵$، $\mathcal{P}(G)$ مسطح است. اما برای $n < ۵$، $\mathcal{P}(G)$ زبرگرافی از $K_۵$ یا $K_{۳,۳}$ نیست لذا حکم ثابت شده است. □

۲.۴ گراف توانی گروه‌های دووجهی

برای هر عدد صحیح $n \geq ۳$، گروه دووجهی $D_n = \langle a, b \rangle$، یک گروه ناآبلی از مرتبه $۲n$ است که مولدهای آن، a و b بوده و در شرایط زیر صدق می‌کنند :

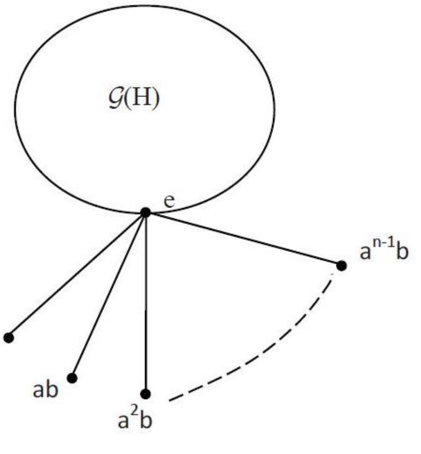
$$o(a) = n, o(b) = ۲$$
$$ba = a^{-۱}b = a^{n-۱}b.$$

۱.۲.۴ ساختار گراف توانی D_n

چون $o(a) = n$، $H = \langle a \rangle$ یک زیرگروه دوری از D_n است که $|H| = n$، لذا $\mathcal{P}(H)$، یک زیرگراف همبند $\mathcal{P}(D_n)$ است. چون $a^n = e = b^۲$، پس برای هر $۱ \leq i \leq n - ۱$، داریم

$$(a^ib)^۲ = a^iba^ib = a^i(b^{-۱}ab)^i = a^ia^{-i} = e.$$

بنابراین برای $۱ \leq k \leq n - ۱$، b و a^kb، فقط با e مجاور هستند. لذا گراف $\mathcal{P}(D_n)$ به فرم شکل ۱ است.



شکل ۱. گراف توانی D_n برای $n \geq ۳$

قضیه ۱.۲.۴. *عنصر همانی e از D_n، یک رأس برشی $\mathcal{P}(D_n)$ است و لذا $\kappa(\mathcal{P}(D_n)) = ۱$. همچنین $\mathcal{P}(D_n)$ هامیلتونی نیست.*

برهان. از ساختار $\mathcal{P}(D_n)$ (شکل ۱) واضح است که حذف عنصر همانی e، تعداد مولفه‌های $\mathcal{P}(D_n)$، که باعث ناهمبندی گراف $\mathcal{P}(D_n)$ می‌شوند، را افزایش می‌دهد. بنابراین e یک رأس برشی $\mathcal{P}(D_n)$ است و لذا $\kappa(\mathcal{P}(D_n)) = ۱$.
چون هر گراف هامیلتونی ۲-همبند است [۱۸]، $\mathcal{P}(D_n)$ هامیلتونی نیست. □

قضیه ۲.۲.۴. *$\mathcal{P}(D_n)$ غیرمسطح است اگروتنها اگر $n \geq ۵$.*

برهان. از ساختار $\mathcal{P}(D_n)$ (شکل ۱) واضح است که $\mathcal{P}(D_n)$ غیرمسطح است اگروتنها اگر $\mathcal{P}(H)$ غیرمسطح باشد. طبق قضیه ۲.۱.۴، $\mathcal{P}(H)$ غیرمسطح است اگروتنها اگر $n \geq ۵$. □

۳.۴ گراف توانی گروه‌های دودوری

برای هر عدد صحیح $n \geq ۲$، گروه دودوری $Q_n = \langle a, b\rangle$ یک گروه ناآبلی از مرتبه $۴n$ است که مولدهای آن، a و b بوده و در شرایط زیر صدق می‌کنند :

$$a^{2n} = e, a^n = b^2$$
$$ab = ba^{-1} = ba^{2n-1}.$$

هر عنصر خارج از زیرگروه دوری $A = \langle a\rangle$ از Q_n، از مرتبه ۴ و عنصر a^n، تنها عنصر از مرتبه ۲ است.

۱.۳.۴ ساختار گراف توانی Q_n

برای $1 \leq k \leq 2n - 1$،

$$\begin{aligned}(a^kb)^2 &= a^kba^kb = a^kb^2b^{-1}a^kb = a^kb^2(b^{-1}ab)^k\\ &= a^kb^2a^{-k} = a^ka^{-k}b^2 = b^2 = a^n. \qquad (۱.۴)\end{aligned}$$

همچنین

$$(a^kb)^3 = (a^kb)^2(a^kb) = a^{n+k}b, \qquad (۲.۴)$$

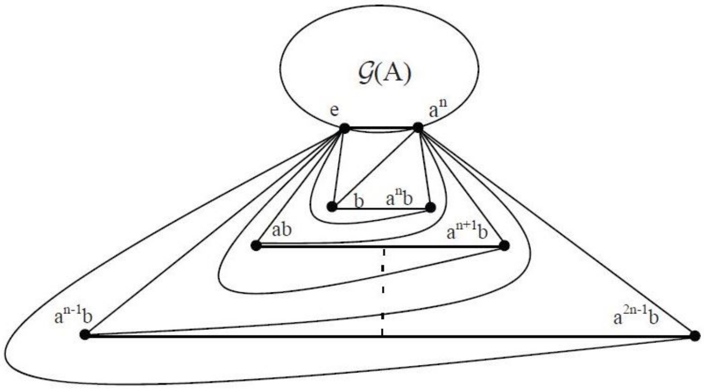
$$(a^nb)^4 = b^4 = e. \qquad (۳.۴)$$

لذا

$$H_1 = \{e, b, a^n, a^nb\}, H_2 = \{e, ab, a^n, a^{n+1}b\}, \cdots ,$$
$$H_n = \{e, a^{n-1}b, a^n, a^{2n-1}b\}$$

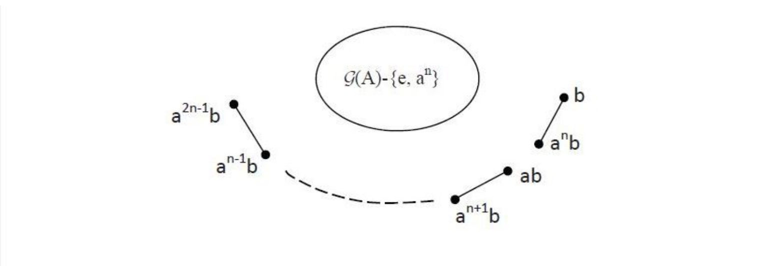
و $A = \langle a \rangle$ تنها زیرگروه‌های دوری Q_n هستند که برای هر $n \leq i \leq$ ۱، ۴ $= |H_i|$ و ۲n $= |A|$.
بنابراین برای $n \leq i \leq$ ۱، هر $\mathcal{P}(H_i)$ (که گراف کامل $K_۴$ است) و $\mathcal{P}(A)$، زیرگراف‌های $\mathcal{P}(Q_n)$، به ترتیب روی ۴ و ۲n رأس هستند. چون برای ۱ $-$ ۲n $\leq k \leq$ ۱، a^kها ، توانی از a هستند که هیچ‌کدام از $\{b, a^k b\}$ نیستند، لذا از تساوی‌های ۱.۴ ، ۲.۴ و ۳.۴، ایجاب می‌شود که هیچ زوج دیگری از رئوس $\mathcal{P}(Q_n)$ مجاور نباشند. بنابراین $\mathcal{P}(Q_n)$، به فرم داده شده در شکل ۲ است.

قضیه ۱.۳.۴. *برای هر ۲ $n \geq$، ۲ $= \kappa(\mathcal{P}(Q_n))$.*



شکل ۲. گراف توانی Q_n برای ۲ $n \geq$

برهان. عناصر e و b از Q_n، با هر رأس دیگری از $\mathcal{P}(Q_n)$ مجاور است و با حذف این دو رأس از $\mathcal{P}(Q_n)$، گراف حاصل به فرم شکل ۳ خواهد بود. به‌وضوح



شکل ۳. گراف توانی $Q_n - \{e, a^n\}$ برای ۲ $n \geq$

زیرگراف $\mathcal{P}(Q_n) - \{e, a^n\}$ از $\mathcal{P}(Q_n)$ دارای ۱ $+$ n مولفه، ناهمبند است. بنابراین

$$\kappa(\mathcal{P}(Q_n)) = ۲.$$

□

قضیه ۲.۳.۴. *برای هر ۲ $n \geq$، $\mathcal{P}(Q_n)$ هامیلتونی نیست.*

برهان. بنا به گزاره ۱۶.۲.۱، اگر G یک گراف هامیلتونی باشد دراین‌صورت، برای هر مجموعه ناتهی $S \subseteq V(G)$، گراف $G - S$ حداکثر $|S|$ مولفه دارد. با در نظر گرفتن $S = \{e, a^n\}$، می‌دانیم که تعداد مولفه‌ها در $\mathcal{P}(Q_n) - S$، $n + ۱$ است که برای هر $n \geq ۲$، بزرگ‌تر از $|S| = ۲$ است. لذا برای هر $n \geq ۲$، $\mathcal{P}(Q_n)$ هامیلتونی نیست. □

قضیه ۳.۳.۴. *$\mathcal{P}(Q_n)$ غیرمسطح است اگروتنها اگر $n > ۲$.*

برهان. از ساختار $\mathcal{P}(Q_n)$ (شکل ۲) واضح است که $\mathcal{P}(Q_n)$ غیرمسطح است اگروتنها اگر $\mathcal{P}(A)$ غیرمسطح باشد. به هر حال $A = \langle a \rangle$ یک گروه دوری از مرتبه $۲n$ است و لذا، طبق قضیه ۲.۱.۴، $\mathcal{P}(A)$ غیرمسطح است اگروتنها اگر $۲n > ۴$ اگروتنها اگر $n > ۲$. □

مراجع

[1] J. Abawajy, A. Kelarev and M. Chowdhury, *Power graphs: A survey*, Electronic J. of Graph Theory and Appl, **1**, **2**, 125–147, 2013.

[2] H. Amiri, S.M. Jafarian Amiri and I.M. Isaacs, *Sums of element orders in finite groups*, Commun. in Algebra®, **37**, 2978–2980, 2009.

[3] T.M. Apostol, *Introduction to analytic number theory*, Springer, Berlin, 1976.

[4] Y. Berkovich, *Groups of Prime Power Order*, **1**, Walter de Gruyter, Berlin, 2008.

[5] J. Bosak, *The graphs of semigroups*, Theory of Graphs and Application, 119–125, Academic Press, New York, 1964.

[6] P.J. Cameron, *The power graph of a finite group II*, J. Group Theory, **13**, 779–783, 2010.

[7] P.J. Cameron and S. Ghosh, *The power graph of a finite group*, Discrete Mathematics, **311**, 1220–1222, 2011.

[8] I. Chakrabarty, S. Ghosh and M.K. Sen, *Undirected power graphs of semigroups*, Semigroup Forum, **78**, 410–426, 2009.

[9] S. Chattopadhyay and P. Panigrahi, *Connectivity and planarity of power graphs of finite cyclic, dihedral and dicyclic groups*, J. Algebra and Discrete Mathematics, **18**, 1, 42–49, 2014.

[10] B. Curtin and G.R. Pourgholi, *Edge-maximality of power graphs of finite cyclic groups*, J. Algebra Comb, 313–330, 2014.

[11] J.M Howie, *An introduction to semigroup theory*, 1976.

[12] T.W. Hungerford, *Algebra*, Berlin, 1974.

[13] A.V. Kelarev and S.J. Quinn, *A combinatorial property and power graphs of groups*, Contributions to General Algebra 12, Proceedings of the Vienna Conference, 229–236, 2000.

[14] A.V. Kelarev and S.J. Quinn, *Directed graphs and combinatorial properties of semigroups*, J. Algebra, **251**, 16–26, 2002.

[15] A.V. Kelarev and S.J. Quinn, *A combinatorial property and power graphs of semigroups*, Comment. Math. Univ. Carol., **45**, 1–7, 2004.

[16] A.V. Kelarev, S.J. Quinn and R. Smolikova, *Power graphs and semigroups of matrices*, Bull. Aust. Math. Soc., **63**, 341–344, 2001.

[17] J.S. Rose, *A course on group theory*, 1994.

[18] D.B. West, *Introduction to graph theory*, Prentice-Hall, New Delhi, 2003.

[19] B. Zelinka, *Intersection graphs of finite abelian groups*, Czech. Math. J., **25**, 171–174, 1975.

[۲۰] ع. جمالی، مقدمه‌ای بر نظریه گروه‌های متناهی، انتشارات مبتکران، ۱۳۹۱.

[۲۱] و. ساهای و و.بیست، جبر، انتشارات دانشگاه صنعتی شاهرود، (ترجمه دکتر ابراهیم هاشمی)، ۱۳۸۷.

واژه‌نامه فارسی به انگلیسی

[هم‌ریختی] انتقال	transfer
اندیس	index
بدیهی	trivial
بزرگ‌ترین مقسوم‌علیه اول	greatest prime divisors
تراگرد	transversal
تعدی	transitivity
جایگشت	permutation
حاصل‌ضرب دکارتی	cartesian product
حاصل‌ضرب مستقیم	direct product
حاصل‌ضرب نیم‌مستقیم	semidirect product
حلقه	ring
خطی مرتب	linearly ordered
خودتوان	idempotent
خودریختی	automorphism
درجه	degree
درجه ورودی	in-degree
درجه خروجی	out-degree
دور	cycle
دوسویی	bijection
رابطه دوتایی	binary relation
رابطه شمول	containment relation
رابطه هم‌ارزی	equivalence relation
رأس	vertex
رأس برشی	cut-vertex
زبرگراف	supergraph

زیرگراف	subgraph
p–زیرگروه	p-subgroup
p–زیرگروه سیلو	Sylow p-subgroup
زیرگروه مشخصه	characteristic subgroup
زیرنیم‌گروه	subsemigroup
کوچک‌ترین مقسوم‌علیه اول	least prime divisors
گراف توانی	power graph
گراف توانی جهت‌دار	directed power graph
گروه	group
p–گروه	p-group
گروه آبلی	abelian group
گروه آبلی مقدماتی	elementary abelian group
گروه تاب‌دار	torsion group
گروه دودوری	dicyclic group
گروه دوری	cyclic group
گروه دووجهی	dihedral group
گروه متقارن	symmetric group
p–متمم	p-complement
گروه متناهی	finite group
گروه متناهی مولد	finitely generated group
مجاور	adjacent
مرتبه	order
مرکز	center
مرکزساز	centralizer
مسطح	planar
مسیر	path
هسته	core
منظم	regular
مولد	generator
نرمال‌ساز	normalizer
نیم‌گروه	semigroup
هامیلتونی	Hamiltonian

همانی .... identity

k–همبند .... k-connected

همبندی .... connectivity

همبندی رأسی .... vertex connectivity

همدسته .... coset

همریختی .... homomorphism

همسانریختی .... homeomorphism

یال .... edge

یال دوطرفه .... bidirectional edge

یکریختی .... isomorphism

واژه‌نامه انگلیسی به فارسی

abelian group .... گروه آبلی
adjacent .... مجاور
automorphism .... خودریختی
bidirectional edge .... یال دوطرفه
bijection .... دوسویی
binary relation .... رابطه دوتایی
cartesian product .... حاصل‌ضرب دکارتی
centralizer .... مرکزساز
center .... مرکز
characteristic subgroup .... زیرگروه مشخصه
connectivity .... همبندی
containment relation .... رابطه شمول
core .... هسته
coset .... همدسته
cut-vertex .... رأس برشی
cycle .... دور
cyclic group .... گروه دوری
degree .... درجه
dicyclic group .... گروه دودوری
dihedral group .... گروه دووجهی
direct product .... حاصل‌ضرب مستقیم
directed power graph .... گراف توانی جهت‌دار
edge .... یال
elementary abelian group .... گروه آبلی مقدماتی
equivalence relation .... رابطه هم‌ارزی

finite group .... گروه متناهی
finitely generated group .... گروه متناهی مولد
generator .... مولد
greatest prime divisors .... بزرگ‌ترین مقسوم‌علیه اول
group .... گروه
Hamiltonian .... هامیلتونی
homeomorphism .... همسانریختی
homomorphism .... همریختی
idempotent .... خودتوان
identity .... همانی
in-degree .... درجه ورودی
index .... اندیس
isomorphism .... یکریختی
k-connected .... k-همبند
least prime divisors .... کوچک‌ترین مقسوم‌علیه اول
linearly ordered .... خطی مرتب
normalizer .... نرمال‌ساز
order .... مرتبه
out-degree .... درجه خروجی
p-complement .... p-متمم
p-group .... p-گروه
p-subgroup .... p-زیرگروه
path .... مسیر
permutation .... جایگشت
planar .... مسطح
power graph .... گراف توانی
regular .... منظم
ring .... حلقه
semidirect product .... حاصل‌ضرب نیم‌مستقیم
semigroup .... نیم‌گروه
subgraph .... زیرگراف
subsemigroup .... زیرنیم‌گروه

زبرگراف .... supergraph

p–زیرگروه سیلو .... Sylow p-subgroup

گروه متقارن .... symmetric group

گروه تاب‌دار .... torsion group

[هم‌ریختی] انتقال .... transfer

تعدی .... transitivity

تراگرد .... transversal

بدیهی .... trivial

رأس .... vertex

همبندی رأسی .... vertex connectivity

نمایه

Abstract

The power graph $\mathcal{P}(S)$ of a semigroup S is a graph whose vertex set is S and two vertices $a, b \in S$ are adjacent if and only if $a \neq b$ and $a^m = b$ or $b^m = a$ for some positive integer m. The power graph $\mathcal{P}(G)$ of a group G is defined similarly. In this thesis, we characterize the class of semigroups S for which $\mathcal{P}(S)$ is connected or complete. As a consequence, we prove that $\mathcal{P}(G)$ is connected for any finite group G and $\mathcal{P}(G)$ is complete if and only if G is a cyclic group of order 1 or p^m, for some prime number p and for some $m \in \mathbb{N}$. Then we compute the number of edges of $\mathcal{P}(G)$ for finite group G and we show that among all finite groups of any given order, the cyclic group of that order has the maximum number of edges in its power graphs.
Also we discuss the planarity and vertex connectivity of the power graphs of finite cyclic, dihedral and dicyclic groups.

Keywords Semigroup, Group, Cyclic group, p-Group, Power graph, Connected graph, Connectivity, Dihedral group, Dicyclic group.

Shahrood University of Technology

Faculty Of Mathematical Sciences

Edge-maximality of power graphs of finite groups

Elham Mahmoodi

Supervisor

Dr. Seyyed Heydar Jafari

November 2016