دسترسی در سایتِ http://jnrm.srbiau.ac.ir
سال هفتم، شماره سی و یکم، مرداد و شهریور ۱۴۰۰
شماره شاپا: ۲۵۸۸-۵۸۸X

پژوهش‌های نوین در ریاضی

دانشگاه آزاد اسلامی، واحد علوم و تحقیقات

روابط چندمجموعه‌ای و چندگروه‌های تحت t_n-نرم

حسین نراقی[۱]، سعید میروکیلی[۲*]، پیمان غیاثوند[۳]

(۱و۲و۳) گروه ریاضی، دانشگاه پیام نور، تهران، ایران

تاریخ ارسال مقاله: ۱۳۹۹/۰۷/۱۱ تاریخ پذیرش مقاله: ۱۳۹۹/۰۹/۱۷

چکیده

در این مقاله پس از بررسی خواص و قضایایی در چندگروه‌ها و نتایجی از یکریختی چندگروه‌ها نشان می‌دهیم که چگونه یک چندگروه می‌تواند به یک چندگروه غیر ثابت دیگر تحت یک عمل دوتایی مناسب که آن را t_n-نرم می‌نامیم، نسبت داده شود. در واقع تحت یک t_n-نرم دلخواه به یک چندگروه، چندگروه دیگری را وابسته نموده و خواص متقابل آن‌ها را بررسی می‌کنیم. از این فرایند برای تولید یک چندگروه غیر ثابت از یک رابطه چندمجموعه‌ای تحت یک t_n-نرم دلخواه بهره می‌بریم. همچنین در پایان کاربردی از مفاهیم ارائه شده برای تولید رمزیکبار مصرف بیان می‌کنیم.

واژه‌های کلیدی: چندمجموعه، رابطه‌ی چندمجموعه‌ای، چندگروه، t_n-نرم.

*. عهده‌دار مکاتبات: Email: saeed_mirvakili@pnu.ac.ir

۱- مقدمه

چندمجموعه‌ها به‌طور کاملاً طبیعی از زمینه‌های خاص در ریاضیات، علوم کامپیوتر، فیزیک و فلسفه برمی‌خیزد، گرچه در ریاضیات کلاسیک نمی‌توان مستقیماً با چندمجموعه‌ها سروکار داشت. ایده‌ی چندمجموعه‌ای برای اولین بار در سال ۱۹۸۸ توسط دِدکیند مطرح گردید که در آن چندمجموعه به صورت تابعی از مجموعه‌ی X به اعداد حسابی تعریف می‌شود. در سال ۲۰۰۹، گریسل مفاهیم ارتباط، عملکرد، ترکیب و هم ارزی در چند مجموعه‌ها را معرفی کرد. برای اطلاعات بیشتر و کارهای انجام شده در رابطه با چند مجموعه‌ها به مراجع [۲]، [۳]، [۴]، [۵]، [۱۲]، [۱۳]، [۱۴]، [۱۵]، [۱۶]، [۱۷] و [۱۸] مراجعه کنید. تلا، دنیل و نازمول در سال ۲۰۱۳ مفهوم چندگروه را مورد مطالعه قرار داده‌اند. مطالعات بسیاری روی چندگروه‌ها شده است که می‌توان به [۱]، [۵]، [۶]، [۷]، [۹]، [۱۰]، [۱۱]، [۱۸] و [۱۹] اشاره کرد.

یک خانواده از اشیاء که هر شیء ممکن است تکرار هم شده باشد (بر خلاف مجموعه) را یک چندمجموعه گوییم. نمایش‌های مختلف یک چندمجموعه مانند $\{a,b,b,c,c,c\}$ را می‌توان به‌صورت‌های $\{a,b,c\}_{۱,۲,۳}$، $\left\{\frac{a}{۱},\frac{b}{۲},\frac{c}{۳}\right\}$، $\{a^۱,b^۲,c^۳\}$ یا $\{a,۲b,۳c\}$ نوشت، که در اینجا a، b و c اشیاء هستند و هر وقوع این اشیاء یک عنصر است. هر رخداد فردی از یک شیء در یک چندمجموعه عنصر آن نامیده می‌شود. به‌عبارت دیگر عناصر متمایز یک چندمجموعه اشیا آن هستند.

تعداد رخدادهای یک شی x در یک چندمجموعه‌ی A را تعدد یا ارزش مشخصه می‌نامند که معمولاً با $C_A(x)$ نشان می‌دهند. در نظریه‌ی مجموعه‌ها به‌جای $C_A(x)$ از $x \in A$ استفاده می‌شود. چندمجموعه را با نماد (A,C_A) نشان داده و اعضای آن را با نماد $x/C_A(x)$ نشان می‌دهیم. در جایی که ابهامی ایجاد نشود، بجای (A,C_A) از A یا C_A استفاده می‌کنیم. اگر ابهامی پیش نیاید بجای C_A از C استفاده می‌کنیم.

مجموعه‌ای از عناصر متمایز از یک چندمجموعه، ریشه یا پشتیبان نامیده می‌شود وآن را با نماد A^* نمایش می‌دهیم. زیرمجموعه‌ی $\{x \in A^* | C_A(x)>0\}$ را با نماد $\operatorname{Supp} C_A$ نمایش می‌دهند. همچنین به ازای هر $t \in \operatorname{Im}(C_A)$، زیرمجموعه‌ی $\{x \in A^* | C_A(x) \geq t\}$ را با نماد C_t نمایش می‌دهیم، که در آن $\operatorname{Im}(C_A)$ تصویر یا برد چند مجموعه‌ی A است. مجموعه‌ی ریشه‌ای از یک چندمجموعه‌ی A، مجموعه‌ی $\{x : x \in A\}$ است، به عنوان مثال مجموعه‌ی ریشه‌ای چند مجموعه‌ی $\{a,a,a,b,c,c\}$، مجموعه‌ی $\{a,b,c\}$ است.

عدد اصلی مجموعه‌ی ریشه‌ای یک چندمجموعه را بعد آن می‌نامند.

دو چندمجموعه‌ی A و B را مساوی گویند و با $A=B$ نشان می‌دهند اگر $C_A(x)=C_B(x)$.

در سراسر این مقاله، مجموعه‌ی اعداد حسابی را با $\mathbb{W}$و مجموعه اعداد طبیعی را با $\mathbb{N}$ نمایش می‌دهیم. همچنین قرارداد می‌کنیم $\mathbb{W}_n=\{0,1,...,n\}$ و $\mathbb{N}_n=\{1,...,n\}$.

در بخش اول این مقاله، مقدماتی از نظریه‌ی چند مجموعه‌ها و چندگروه‌ها از دیدگاه t_n-نرم به طور خلاصه مطرح می‌شود. در این بخش سعی شده است تعاریف و قضایایی که در قسمت‌های بعدی مورد نیاز است، بیان گردد. در بخش سوم به یکریختی چندگروه‌های روی یک مجموعه‌ی t_n-نرم پرداخته و برخی خواص آن‌ها را مورد مطالعه قرار می‌دهیم. در بخش چهارم، با استفاده از تعاریف و مطالب استفاده شده، قضایا و نتایجی از روابط چندمجموعه‌ای روی یک چندمجموعه‌ی را تحت یک t_n-نرم دلخواه بدست می‌آوریم و در بخش پنجم، با توجه به بررسی‌های انجام گرفته، نشان می‌دهیم که به هر رابطه‌ی چند مجموعه‌ای روی

یک چندمجموعه می‌توان یک چندگروه تحت یک t_n-نرم دلخواه نظیر کرد.

۲- چندگروه‌های تولید شده توسط t_n-نرم

تعریف ۲-۱: عمل دوتایی $T_n : \mathbb{W}_n \times \mathbb{W}_n \to \mathbb{W}_n$ را یک t_n-نرم می‌نامیم اگر به ازای هر $a,b,c \in \mathbb{W}_n$ در ویژگی‌های زیرصدق کند:

۱) $T_n(a,b) = T_n(b,a)$،

۲) $T_n(a,n) = a$،

۳) $T_n(a,T_n(b,c)) = T_n(T_n(a,b),c)$،

۴) اگر $a \le b$ و $c \le d$، آنگاه $T_n(a,c) \le T_n(b,d)$.

در صورتی‌که $\otimes_n$ یک t_n-نرم باشد، برخی مواقع به جای $\otimes_n(a,b)$ می‌نویسیم $a \otimes_n b$. به‌سادگی می‌توان نشان داد به ازای هر $a,b \in \mathbb{W}_n$ داریم:

۱) $a = a \otimes_n n \ge a \otimes_n a$،

۲) $b = b \otimes_n n \ge b \otimes_n a = a \otimes_n b$

لذا $\min\{a,b\} \ge a \otimes_n b$.

به عنوان مثال $\oplus_n : \mathbb{W}_n \times \mathbb{W}_n \to \mathbb{W}_n$ با ضابطه $a \oplus_n b = \begin{cases} 0 & a+b \le n \\ a+b-n & a+b > n \end{cases}$ یک t_n-نرم است.

در ادامه قصد تعریف چندگروه روی یک گروه G را داریم. در اینجا یادآوری می‌کنیم منظور از چند مجموعه C_G روی مجموعه G زوج مرتب (G,C_G) است که در آن $C_G : G \to \mathbb{W}$ می‌باشد.

تعریف ۲-۲: [۹] فرض کنید $C_G : G \to \mathbb{W}$ یک چندمجموعه از گروه G باشد. در این صورت C_G یک چندگروه روی G نامیده می‌شود، هرگاه

برای هر x و y در G، $C_G(xy) \ge \min\{C_G(x), C_G(y)\}$

برای هر x در G، $C_G(x^{-1}) \ge C_G(x)$.

توجه شود در تعریف ۲-۲ نامساوی در قسمت (۲) تساوی را نتیجه می‌دهد، یعنی همیشه در چندگروه‌ها برای هر $x \in G$ داریم $C_G(x^{-1}) = C_G(x)$.

چندگروه C_G روی G را غیرثابت گوییم هرگاه برد آن به‌عنوان تابع بیش از یک عضو داشته باشد، به عبارت دیگر $|\mathrm{Im}(C_G)| \ge 2$.

تعریف ۲-۳: فرض کنید $C_G : G \to \mathbb{W}$ یک چند مجموعه از گروه G باشد که در آن $\mathrm{Max}_{x \in G} C_G(x) \le n$ و $\otimes_n$ یک t_n-نرم باشد، در این صورت C_G را یک چندگروه t_n-نرم تحت $\otimes_n$ از G می‌نامیم، هرگاه برای هر x و y در G،

$C_G(xy) \ge C_G(x) \otimes_n C_G(y)$

۱) برای هر x در G، $C_G(x^{-1}) \ge C_G(x)$.

قرارداد: اگر C یک چندگروه t_n-نرم تحت $\otimes_n$ از $G = \{a_1, a_2, \ldots, a_n\}$ باشد $C(a_1) \otimes_n C(a_2) \otimes_n \cdots \otimes_n C(a_n)$ را با نماد $\otimes_n \sum_{a \in G} C(a)$ نمایش می‌دهیم.

لم ۲-۴: فرض کنید G گروه متقارن $\mathbb{S}_n$ و $\mathbb{A}_n$ مجموعه جایگشت‌های زوج باشد. $C : G \to \mathbb{W}$ را به صورت زیر تعریف می‌کنیم:

$$C(f) = \begin{cases} n & f \in \mathbb{A}_n \\ 0 & f \notin \mathbb{A}_n \end{cases}$$

در این صورت داریم:

الف) C یک چندگروه از G است.

ب) اگر $\otimes_n$ یک t_n-نرم باشد، به ازای هر $r \in \{0,1,\cdots,n\}$، $C_r : G \to \mathbb{W}$ با ضابطه‌ی $C_r(f) = C(f) \otimes_n r$ یک چندگروه t_n-نرم تحت $\otimes_n$ از G است.

اثبات: برای اثبات دو حالت زیر را در نظر می‌گیریم:

حالت اول: $f,g \in G$ هردو جایگشت‌هایی زوج یا هر دو فرد باشند بنابراین $f \circ g$ نیز جایگشتی زوج است، لذا

$C(f \circ g) = n \ge \min\{C(f), C(g)\}$

حالت دوم: برای $f,g\in G$، یکی از جایگشت‌ها زوج و دیگری فرد باشد، بنابراین $f\circ g$ نیز جایگشتی فرد است، بنابراین

$$C(f\circ g)=0\geq \min\{C(f),C(g)\}$$

از طرفی به ازای $f\in G$، f و f^{-1} هردو جایگشت باهم یا زوجند یا فرد هستند بنابراین $C(f^{-1})=C(f)$، پس C یک چندگروه است.

برای اثبات (ب) در هر دو حالت داریم:

$$\min\{C(f),C(g)\}\geq C(f)\otimes_n C(g)$$

لذا

$$C(f\circ g)\geq C(f)\otimes_n C(g)$$

پس داریم:

$$\begin{aligned}&C_r(f\circ g)\\&=C(f\circ g)\otimes_n r\\&\geq (C(f)\otimes_n C(g))\otimes_n r\\&=C(f)\otimes_n (C(g)\otimes_n r)\\&\geq (C(f)\otimes_n r)\otimes_n (C(g)\otimes_n r)\\&=C_r(f)\otimes_n C_r(g)\end{aligned}$$

این نشان می‌دهد که C_r یک چندگروه t_n-نرم تحت $\otimes_n$ از G است.

گزاره ۲-۵: فرض کنید G یک گروه باشد، اگر C_G یک چندگروه باشد، آنگاه به ازای هر t_n-نرم مانند $\otimes_n$، C_G یک چندگروه t_n-نرم تحت $\otimes_n$ از G است.

اثبات: به‌ازای هر $a,b\in G$، همواره داریم:

$$\min\{C_G(a),C_G(b)\}\geq C_G(a)\otimes_n C_G(b)$$

بنابراین اگر C_G یک چندگروه باشد، آنگاه C_G یک چندگروه t_n-نرم تحت $\otimes_n$ از G است.

مثال ۲-۶: فرض کنید $G=K_4=\{e,a,b,c\}$ گروه چهارتایی کلاین و $C_G=\{\frac{e}{3},\frac{a}{3},\frac{b}{2},\frac{c}{2}\}$ با جدول زیر بیان شود:

$\wedge$	e/3	a/3	b/2	c/2
e/3	e/3	a/3	b/2	c/2
a/3	a/3	e/3	c/2	b/2
b/2	b/2	c/2	e/2	a/2
c/2	c/2	b/2	a/2	e/2

که در آن $\frac{x}{C_G(x)}\wedge\frac{y}{C_G(y)}$ برابر با $\frac{xy}{\min\{C_G(x),C_G(y)\}}$ است. واضح است که در این مثال همواره برای هر x و y در G، $C_G(x^{-1})\geq C_G(x)$ و $C_G(xy)\geq\min\{C_G(x),C_G(y)\}$ پس C_G یک چندگروه از G است. حال با توجه به این‌که $\oplus_4$ با ضابطه‌ی زیر یک t_4-نرم است،

$$r\oplus_4 s=\begin{cases}0 & r+s\leq 4\\ r+s-4 & r+s>4\end{cases}$$

لذا بنا بر گزاره قبل، C_G یک چندگروه t_4-نرم تحت $\oplus_4$ از G است.

مثال زیر نشان می‌دهد که اگر C_G چندگروه t_n-نرم تحت $\otimes_n$ از گروه G باشد آنگاه C_G لزوما یک چندگروه از G نیست.

مثال ۲-۷: فرض کنید $G=K_4=\{e,a,b,c\}$ گروه چهارتایی کلاین و $C_G=\{\frac{e}{4},\frac{a}{3},\frac{b}{2},\frac{c}{1}\}$ با جدول زیر بیان شود: ($\wedge$ در مثال قبل تعریف شده است)

$\wedge$	e/4	a/3	b/2	c/1
e/4	e/4	a/3	b/2	c/1
a/3	a/3	e/3	c/2	b/1
b/2	b/2	c/2	e/2	a/1
c/1	c/1	b/1	a/1	e/1

آنگاه C_G یک چندگروه از G نیست، زیرا

$$\begin{aligned}C_G(ab) &= C_G(c)\\&= 1\\&< \min\{C_G(a),C_G(b)\}\\&= 2\end{aligned}$$

حال t_4-نرم $\oplus_4$ را با جدول زیر در نظر بگیرید:

$\oplus_4$	e/4	a/3	b/2	c/1
e/4	e/4	a/3	b/2	c/1
a/3	a/3	e/2	c/1	b/1
b/2	b/2	c/1	e/2	a/0
c/1	c/1	b/0	a/0	e/0

که در آن $\frac{x}{C_G(x)}\oplus_4\frac{y}{C_G(y)}$ برابر با $\frac{xy}{C_G(x)\oplus_4 C_G(y)}$ است. در این صورت C_G یک چندگروه t_4-نرم تحت $\oplus_4$ از G است.

۳- یکریختی چندگروه‌ها

فرض کنید C و C' به ترتیب دوچند گروه از گروه‌های G و G' باشند. همریختی گروهی $h:G\to G'$ را همریختی چندگروهی از C به C' گوییم هرگاه $C=C'\circ h$، به عبارت دیگر به ازای هر $x\in G$، $C'(h(x))=C(x)$.

تعریف ۳-۱: فرض کنید C و C' به ترتیب دو چندگروه از گروه‌های G و G' باشند. همریختی چندگروهی $h:G\to G'$ را یکریختی چندگروهی گوییم هرگاه h تابع دوسویی باشد و می‌نویسیم $C\cong C'$.

همچنین اگر C یک چندگروه از G باشد، یکریختی $f:G\to G$ را یک خودریختی چندگروهی روی G نامیم، اگر برای هر x در G، $C(f(x))=C(x)$.

گزاره ۳-۲: فرض کنید C و C' به ترتیب دو چندمجموعه از گروه‌های G و G' باشند و $f:G\to G'$ یک یکریختی گروهی باشد که ازای به هر $x\in G$ داریم $C'(f(x))=C(x)$. اگر C یک چندگروه از گروه G باشد، آنگاه C' یک چندگروه از گروه G' است.

اثبات: فرض کنید x' و y' دو عضو از G' باشند. بنابراین اعضایی مانند x و y در G وجود دارند که $f(x)=x'$ و $f(y)=y'$. بنابراین

$$\begin{aligned}C'(x'y') &= C'\big(f(x)f(y)\big)\\ &= C'\big(f(xy)\big)\\ &= C(xy)\\ &\geq \min\{C(x),C(y)\}\\ &= \min\{C'(f(x)),C'(f(y))\}\\ &= \min\{C'(x'),C'(y')\}\end{aligned}$$

و

$$\begin{aligned}C'\big((x')^{-1}\big) &= C'\Big(f(x)^{-1}\Big)\\ &= C'\Big(f\big(x^{-1}\big)\Big)\\ &= C\big(x^{-1}\big)\\ &= C(x)\\ &= C'\big(f(x)\big)\\ &= C'(x')\end{aligned}$$

گزاره ۳-۳: فرض کنید C و C' به‌ترتیب دو چندگروه یکریخت از گروه‌های متناهی G و G' تحت یکریختی f باشند، آنگاه:

الف) $\mathrm{Im}C=\mathrm{Im}C'$ (بردهای چندگروه‌های C و C' با هم برابرند).

ب) C_t و C'_t به ترتیب زیرگروه‌های G و G' هستند.

ج) به ازای هر $t\in\mathrm{Im}C$، $C_t\cong C'_t$ و $f(C_t)=C'_t$.

د) $\mathrm{Supp}C'=f(\mathrm{Supp}C)$.

اثبات: الف) فرض کنید t عضوی دلخواه از $\mathrm{Im}C$ باشد. بنابراین عضوی مانند x از G وجود دارد به قسمی که $C(x)=t$. از طرفی، $C(x)=C'(f(x))$. بنابراین $t=C(x)\in\mathrm{Im}C'$، لذا $\mathrm{Im}C\subseteq\mathrm{Im}C'$. حال فرض کنید t' عضوی دلخواه از $\mathrm{Im}C'$ باشد، بنابراین عضوی مانند x' از G' وجود دارد که

$C'(x')=t'$ و همچنین عضوی مانند x از G موجود است به‌طوری‌که $t'=C'(x')=C'(f(x))=C(x)$.

لذا، $C'(x')\in \operatorname{Im}C$. بنابراین $\operatorname{Im}C'\subseteq \operatorname{Im}C$.

ب) فرض کنید $x,y\in C_t$، آنگاه

$$\begin{aligned} C(xy^{-1}) &\geq \min\{C(x),C(y^{-1})\} \\ &= \min\{C(x),C(y)\} \\ &\geq t \end{aligned}$$

پس $xy^{-1}\in C_t$ و در نتیجه C_t زیرگروه G است. به طریق مشابه C'_t زیرگروه G' است.

ج) تابع $f_t:C_t\to C'_t$ را با ضابطه $f_t(x)=f(x)$ در نظر بگیرید. f_t خوش‌تعریف است زیرا f خوش‌تعریف است و فرض کنید x عضوی دلخواه از C_t باشد. بنابراین $C(x)\geq t$. از طرفی $C(x)=C'(f(x))$، پس $f(x)\in C'_t$. پس f_t پوشا است، زیرا اگر $y\in C'_t$ پس $x\in G$ وجود دارد به قسمی که $y=f(x)$ و $C(x)=C'(f(x))=C'(y)\geq t$، در نتیجه $x\in C_t$ و $y=f_t(x)$. یک به یک بودن و همریختی بودن f_t از یکریختی بودن f نتیجه می‌شود، بنابراین $C_t\cong C'_t$.

د) به سادگی اثبات می‌شود.

لم ۳-۴: فرض کنید $\operatorname{Aut}(G)$ مجموعه‌ی همه‌ی خودریختی‌های چندگروهی C روی G باشد. در این صورت $\operatorname{Aut}(G)$ تحت عمل ترکیب توابع، تشکیل یک گروه می‌دهد.

اثبات: واضح است که ترکیب توابع دارای خاصیت شرکت‌پذیری است. برای اثبات بسته بودن فرض کنید f و g دو عضو از $\operatorname{Aut}(G)$ باشند. از طرفی دیگر برای هر x در G داریم:

$$\begin{aligned} C(f\circ g(x)) &= C(f(g(x)) \\ &= C(g(x)) \\ &= C(x) \end{aligned}$$

به این ترتیب $f\circ g$ عضوی از $\operatorname{Aut}(G)$ است. خواص دیگر گروه به سادگی قابل بررسی است. بنابراین $\operatorname{Aut}(G)$ همراه با ترکیب توابع یک گروه است.

گزاره ۳-۵: فرض کنید C و C' به ترتیب دو چندگروه یکریخت روی گروه‌های یکریخت G و G' باشد، دراین‌صورت $\operatorname{Aut}(G)\cong \operatorname{Aut}(G')$.

اثبات: از آنجایی که C و C' یکریخت هستند، یکریختی مانند $\pi:G\to G'$ موجود است که به ازای هر عضو دلخواه $f\in \operatorname{Aut}(G)$، $\pi\circ f\circ\pi^{-1}\in \operatorname{Aut}(G')$، زیرا به ازای هر $x\in G$،

$$\begin{aligned} C'\left(\pi\circ f\circ\pi^{-1}(x)\right) &= C\left(f\circ\pi^{-1}(x)\right) \\ &= C\left(\pi^{-1}(x)\right) \\ &= C'\left(\pi\circ\pi^{-1}(x)\right) \\ &= C'(x) \end{aligned}$$

همچنین به سادگی می‌توان نشان داد تابع

$$\varphi:\operatorname{Aut}(G)\to\operatorname{Aut}(G')$$
$$\varphi(f)=\pi\circ f\circ\pi^{-1}$$

یک یکریختی بین گروه‌ها است. پس داریم $\operatorname{Aut}(G)\cong \operatorname{Aut}(G')$.

گزاره ۳-۶: اگر H یک زیرگروه از گروه G و C یک چندگروه از G باشد، آنگاه $C\big|_H$ یک چندگروه تحت t_n-نرم از H است.

اثبات: به ازای هر h و h' در H داریم:

$$\begin{aligned} C\big|_H(hh') &= C(hh') \\ &\geq C(h)\otimes_n C(h') \\ &= C\big|_H(h)\otimes_n C\big|_H(h') \end{aligned}$$

و به ازای هر $h \in H$،
$C|_H(h^{-1}) = C(h^{-1}) = C(h) = C|_H(h)$.

نتیجه ۳-۷: فرض کنید C یک چندگروه روی گروه متناهی $G = \mathbb{Z}_n$ باشد که $\mathrm{Max}_{x \in G} C(x) \le n$ و $\mathrm{Aut}(G)$ همراه با ترکیب توابع گروه همه‌ی خودریختی‌ها روی G باشد، نگاشت $C^* : \mathrm{Aut}(G) \to \mathbb{W}$ را به‌صورت زیر تعریف می‌کنیم:

$$C^*(f) = \begin{cases} n & f \in \mathbb{A}_n \\ 0 & f \notin \mathbb{A}_n \end{cases}$$

آنگاه:

الف) C^* یک چندگروه از $\mathrm{Aut}(G)$ است.

ب) اگر $\otimes_n$ یک t_n-نرم باشد، به ازای هر $r \in \{0,1,\cdots,n\}$، $C_r : G \to \mathbb{W}$ با ضابطه‌ی $C_r(f) = C(f) \otimes_n r$ یک چندگروه t_n-نرم تحت $\otimes_n$ از G است.

اثبات: می دانیم $\mathrm{Aut}(G)$ زیرگروهی از گروه متقارن $\mathbb{S}_n$ است. لذا بنا به لم ۲-۴ و گزاره‌ی ۳-۶ به سادگی نتیجه حاصل می‌شود.

مثال ۳-۸: اگر $G = \mathbb{Z}_6$ و

$$C(x) = \begin{cases} 4 & x = 0 \\ 2 & x \in \{2,4\} \\ 1 & x \in \{1,3,5\} \end{cases}$$

آنگاه

$$\mathrm{Aut}(G) = \{(2\ 4), (1\ 3), (1\ 5), (3\ 5), (1\ 3\ 5)\ (2\ 4)(1\ 3), (2\ 4)(1\ 5), (2\ 4)(3\ 5), \text{و}\ (2\ 4)(1\ 3\ 5), \mathrm{id}\}$$

$$C^*(f) = \begin{cases} 4 & f \in \mathbb{A}_n \\ 0 & f \notin \mathbb{A}_n \end{cases},$$

آنگاه C^* یک چندگروه از $\mathrm{Aut}(G)$ است.

۴- نتایجی از روابط چندمجموعه‌ای روی یک چندگروه

تعریف ۴-۱: فرض کنید S یک مجموعه‌ی غیر تهی متناهی، $C : S \to \mathbb{W}$ یک چندمجموعه روی S، در این‌صورت $R : S \times S \to \mathbb{W}$ را یک رابطه چندمجموعه‌ای روی چندمجموعه C نامند اگر و فقط اگر برای هر $x, y \in S$، $R(x,y) \le \min\{C(x), C(y)\}$ و برای هر $x, y \in S$ داشته باشیم $R(x,y) = R(y,x)$.

همچنین اگر R یک چندمجموعه از $S \times S$ باشد آنگاه (R, C_R) یک رابطه‌ی چندمجموعه‌ای است که در آن $C_R(x) = \mathrm{Max}_{y \in S} R(x,y)$، زیرا
$R(x,y') \le \mathrm{Max}_{y \in S} R(x,y)$,

و $R(x,y) \le \min\{C_R(x), C_R(y)\}$. لذا (R, C_R) یک رابطه چندمجموعه‌ای است.

تذکر: فرض کنید S یک مجموعه‌ی غیر تهی متناهی، $C : S \to \mathbb{W}$ یک چندمجموعه روی S باشد و $\mathrm{Max}_{x \in S} C(x) \le n$ و $R : S \times S \to \mathbb{W}$

الف) به ازای هر $x, y \in S$، اگر
$R(x,y) \le \min\{C(x), C(y)\}$

آنگاه $R(x,y) \le n$.

ب) به ازای هر $x, y \in S$، اگر
$R(x,y) \le C(x) \otimes_n C(y)$

آنگاه $R(x,y) \le n \otimes_n n = n$.

تعریف ۴-۲: فرض کنید S یک مجموعه‌ی غیر تهی متناهی، $C : S \to \mathbb{W}$ یک چندمجموعه روی S باشد و $\mathrm{Max}_{x \in S} C(x) \le n$. اگر $\otimes_n$ یک t_n-نرم باشد، در این‌صورت $R : S \times S \to \mathbb{W}$ را یک رابطه‌ی چندمجموعه‌ای t_n-نرم روی چندمجموعه‌ی C می‌نامند اگر و فقط اگر برای هر $x, y \in S$،
$R(x,y) \le C(x) \otimes_n C(y)$

و برای هر $x, y \in S$ داشته باشیم:
$R(x, y) = R(y, x)$.

توجه: همواره نمی‌توان گفت (R, C) یک رابطه‌ی چندمجموعه‌ای t_n-نرم روی چندمجموعه‌ی S است. به مثال زیر توجه کنید.

مثال ۴-۳: فرض کنید $C: S = \{۰,۱,۲\} \to \mathbb{W}$، $R: S \times S \to \mathbb{W}$ با ضابطه‌های زیر تعریف شده باشند:

$$R(x,y) = \begin{cases} x & x = y \\ ۲ & \{x,y\} = \{۱,۲\} \\ ۳ & \{x,y\} = \{۱,۰\} \\ ۳ & \{x,y\} = \{۰,۲\} \end{cases},$$

$$C(x) = \begin{cases} ۳ & x = ۰ \\ ۳ & x = ۱ \\ ۳ & x = ۲ \end{cases}$$

و $\oplus_۴$ t_4-نرم تعریف شده در مثال ۲-۶ باشد. در این صورت

$$\begin{aligned} ۳ &= R(۰,۲) \\ &\geq C(۲) \oplus_۴ C(۰) \\ &= ۳ \oplus_۴ ۳ \\ &= ۲ \end{aligned}$$

و در نتیجه (R, C) یک رابطه چندمجموعه‌ای t_n-نرم نیست.

یک رابطه‌ی چندمجموعه‌ای R روی چندمجموعه‌ی C تحت مجموعه‌ی پشتیبان S را با نمادهای (S, C, R) نمایش می‌دهیم.

لم ۴-۴: اگر یک رابطه‌ی چندمجموعه‌ای R روی چندمجموعه‌ی C تحت مجموعه‌ی پشتیبان S باشد، آنگاه:

الف) $R^* \subseteq S^* \times S^*$،

ب) $R_t \leq C_t \times C_t$.

اثبات: الف) اگر $(x, y) \in R^*$ آنگاه

$$\min\{C(x), C(y)\} \geq R(x, y) > ۰$$

بنابراین $C(x) > 0$ و $C(y) > 0$، پس $x \in S^*$ و $y \in S^*$. در این صورت $R^* \subseteq S^* \times S^*$.

ب) برای هر عضو دلخواه $(x, y) \in R_t$، داریم $R_t(x, y) \geq ۰$. از طرفی

$$R_t(x, y) \leq C(x) \otimes_n C(y)$$

بنابراین

$$C(x) \geq C(x) \otimes_n C(y) \geq ۰,$$
$$C(y) \geq C(x) \otimes_n C(y) \geq ۰$$

این نشان می‌دهد که $(x, y) \in C_t \times C_t$. حال اگر به ازای هر $x, y \in S$، داشته باشیم $C(x) = ۱$ و $R(x, y) = ۱$ آنگاه $R \subseteq S \times S$. که این نشان می‌دهد، تعریف ارایه شده برای رابطه‌ی چند مجموعه‌ای روی چندمجموعه‌ی تحت مجموعه‌ی پشتیبان تعمیمی از رابطه‌ی مجموعه معمولی است.

گزاره ۴-۵: فرض کنید (C, G) یک چندگروه از گروه G باشد و $\text{Max}_{x \in G} C(x) \leq n$. اگر $\otimes_n$ یک t_n-نرم باشد، آنگاه R_C یک چندگروه t_n-نرم از گروه $G \times G$ است که در آن

$$R_C(x, y) = C(x) \otimes_n C(y)$$

اثبات: به ازای هر $a, b, c, d \in G$، بنا بر تعریف R_C و قضیه ۲-۵ داریم:

$$\begin{aligned} R_C(ac, bd) &= C(ac) \otimes_n C(bd) \\ &\geq (C(a) \otimes_n C(c)) \otimes_n (C(b) \otimes_n C(d)) \\ &= (C(a) \otimes_n C(b)) \otimes_n (C(c) \otimes_n C(d)) \\ &= R_C(a, b) \otimes_n R_C(c, d) \end{aligned}$$

بقیه‌ی اثبات به سادگی نتیجه می‌شود.

گزاره ۴-۶: اگر $R: G\times G \to \mathbb{W}$ یک چندگروه از $G\times G$ باشد، آنگاه C_R یک چندگروه از گروه G است.

اثبات: به ازای هر $a,b,y \in G$،

$$C_R(ab)=\mathrm{Max}_{y\in G} R(ab,y)$$

برای هر $x,y \in G$ داریم

$$C_R(ab) \geq R(ab,xy) \geq R(a,x)\otimes_n R(b,y)$$

بنابراین چون x,y دلخواه است لذا

$$\begin{aligned} & C_R(ab) \\ & \geq \mathrm{Max}_{x\in S} R(a,x)\otimes_n \mathrm{Max}_{y\in S} R(b,y) \\ & \geq C_R(a)\otimes_n C_R(b) \end{aligned}$$

همچنین برای هر $x \in S$ داریم

$$\begin{aligned} C_R(a^{-1}) &\geq \mathrm{Max}_{y\in S}(a^{-1},y) \\ &\geq R(a^{-1},x^{-1}) \\ &= R(a,x) \end{aligned}$$

لذا $C_R(a^{-1}) \geq C_R(a)$.

دو مثال زیر، نیز نشان می‌دهند از چندگروه بودن t_n-نرم C از گروه G، چندگروه بودن t_n-نرم R از $G\times G$ نتیجه نمی‌شود و برعکس:

مثال ۴-۷: در رابطه‌ی چندمجموعه‌ی (G,R,C)، C چندگروه از $G=\mathbb{Z}_3$ است اما R چندگروه از $G\times G$ نیست، که در آن $C: G\to \mathbb{W}$ و $R: G\times G \to \mathbb{W}$ به‌صورت زیر تعریف شده‌اند:

$$C(x)=\begin{cases} 4 & x=0 \\ 3 & x=1,2 \end{cases}$$

و

$$R(x,y)=\begin{cases} x & x=y \\ 2 & \{x,y\}=\{1,2\} \\ 3 & \{x,y\}=\{1,0\} \\ 3 & \{x,y\}=\{0,2\} \end{cases}$$

مثال ۴-۸: در رابطه‌ی چندمجموعه‌ای (G,C,R)، R یک چندگروه از $\mathbb{Z}_3\times\mathbb{Z}_3$ است اما C چندگروه از $\mathbb{Z}_3$ نیست، که در آن $C:\mathbb{Z}_3\to\mathbb{W}$ و $R:\mathbb{Z}_3\times\mathbb{Z}_3\to\mathbb{W}$ با ضابطه‌های زیر در نظر گرفته شده‌اند:

$$C(x)=\begin{cases} 6 & x=0 \\ 2 & x=1 \\ 3 & x=2 \end{cases}$$

و

$$R(x,y)=\begin{cases} 2 & x=y \\ 1 & x\neq y \end{cases}.$$

تعریف ۴-۹: فرض کنید $G=(S,C,R)$ و $G'=(S',C',R')$ روابط چندمجموعه‌ای باشند. یک یکریختی از روابط چندمجموعه‌ای روی یک چند مجموعه به‌صورت $f: S\to S'$ نگاشتی دوسویی است که در شرط‌های زیر صدق کند:

۱) برای هر x در S، $C(x)=C'(f(x))$.

۲) برای هر x در S، $R(x,y)=R'(f(x),f(y))$.

گزاره ۴-۱۰: فرض کنید $G=(S,C,R)$ رابطه چندمجموعه‌ای و $h: S\to S'$ نگاشت دوسویی باشد. قرار دهید

۱) برای هر x در S'، $C'(x)=C\left(h^{-1}(x)\right)$،

۲) برای هر x,y در S'، $R'(x,y)=R(h^{-1}(x),h^{-1}(y))$.

در این‌صورت

الف) $G'=(S',C',R')$ رابطه چندمجموعه‌ای است.

ب) $G=(S,C,R)$ و $G'=(S',C',R')$ یکریخت هستند.

اثبات: الف) برای هر x,y در S' داریم

$$\begin{aligned} & R'(x,y) \\ & = R(h^{-1}(x),h^{-1}(y)) \\ & \geq \min\left\{C(h^{-1}(x)),C(h^{-1}(y))\right\} \\ & = \min\left\{C'(x),C'(y)\right\} \end{aligned}$$

ب) در تعریف ۴-۹ قرار دهید $f=h$.

گزاره ۴-۱۱: فرض کنید (H,C,R) و (H',C',R') دو رابطه‌ی چندمجموعه‌ای روی H و H' باشند و $h:H\to H'$ یک یکریختی گروهی بین H و H' باشد که در شرط‌های زیر صدق کند:

۱) برای هر x در H، $C(x)=C'\big(h(x)\big)$،

۲) برای هر x,y در H، $R(x,y)=R'\big(h(x),h(y)\big)$.

در این صورت:

الف) اگر C یک چندگروه از H باشد، آنگاه C' یک چندگروه از H' است.

ب) اگر R یک چندگروه از $H\times H$ باشد آنگاه R' یک چندگروه از $H'\times H'$ است.

اثبات: همانند گزاره‌ی ۲-۳ اثبات می شود.

اینک فرض کنید دو رابطه‌ی چندمجموعه‌ای (G,C,R) و (G',C',R') یکریخت باشند، با دو مثال زیر می‌توان نشان داد:

الف) اگر C یک چندگروه از G باشد ممکن است C' یک چندگروه از G' نباشد.

ب) اگر R یک چندگروه $G\times G$ باشد ممکن است R' یک چندگروه از $G'\times G'$ نباشد.

مثال ۴-۱۲: الف) دو رابطه‌ی چندمجموعه‌ای $G=(\mathbb{Z}_۳,C,R)$ و $G'=(\mathbb{Z}_۳,C',R')$ یکریختند و C با تعریف زیر یک چندگروه از G است ولی C' یک چندگروه از G' نیست.

$$C(x)=\begin{cases}۱۰۰ & x=۰\\ ۵۰ & x=۱\\ ۵۰ & x=۲\end{cases}$$

R	۰	۱	۲
۰	۰	۴۵	۴۵
۱	۴۵	۰	۳۰
۲	۴۵	۳۰	۰

و

$$f:G\to G$$

$$f(x)=\begin{cases}۲ & x=۰\\ ۱ & x=۱\\ ۰ & x=۲\end{cases}$$

$$C'(x)=\begin{cases}۵۰ & x=۰\\ ۵۰ & x=۱\\ ۱۰۰ & x=۲\end{cases}$$

R'	۰	۱	۲
۰	۰	۳۰	۴۵
۱	۳۰	۰	۴۵
۲	۴۵	۴۵	۰

ب) دو رابطه‌ی چندمجموعه‌ای $G=(\mathbb{Z}_{۱۲},C,R)$ و $G'=(\mathbb{Z}_{۱۲},C',R')$، یکریختند و R یک چندگروه $G\times G$ است ولی R' یک چندگروه از $G'\times G'$ نیست که $C:\mathbb{Z}_{۱۲}\to\mathbb{W}$، $C':\mathbb{Z}_{۱۲}\to\mathbb{W}$، $R:\mathbb{Z}_{۱۲}\times\mathbb{Z}_{۱۲}\to\mathbb{W}$، $R':\mathbb{Z}_{۱۲}\times\mathbb{Z}_{۱۲}\to\mathbb{W}$ و $f:G\to G'$ با ضوابط زیر تعریف شده‌اند:

$$C(i)=i+۱۵,\quad C'(i)=f^{-۱}(i)+۱۵$$

$$R(x,y)=\begin{cases}۱۵ & i=j=۰\\ ۱۵ & \{i,j\}=\{۴,۸\},\\ ۱۳ & else\end{cases}$$

$$R'(i,j)=\begin{cases}۱۵ & i=j=۰\\ ۱۵ & \{i,j\}=\{۱۱,۸\}\\ ۱۳ & else\end{cases}$$

و

$$f(x)=\begin{cases}۱۱ & x=۴\\ ۴ & x=۱۱\\ x & else\end{cases}.$$

۵- تولید چندگروه توسط رابطه‌ی چندمجموعه‌ای

تعریف ۵-۱: فرض کنید (S,C,R) که در آن C یک چندمجموعه روی S و R یک رابطه‌ی

چندمجموعه‌ای روی C است، نگاشت یک به یک و پوشای $f:S\to S$ را یک خودریختی چند مجموعه‌ای روی S نامیم، اگر برای هر $x,y\in S$،

$$R(f(x),f(y))=R(x,y),$$
$$C\big(f(x)\big)=C(x).$$

نتیجه ۵-۲: فرض کنید $\mathrm{Aut}(G)$ مجموعه‌ی همه‌ی خودریختی‌های (S,C,R) باشد. در این صورت $\mathrm{Aut}(G)$ تحت عمل ترکیب توابع تشکیل یک گروه می‌دهد.

اثبات: واضح است که ترکیب توابع دارای خاصیت شرکت‌پذیری است. برای اثبات بسته بودن بودن فرض کنید f,g دو عضو از $\mathrm{Aut}(G)$ باشند آنگاه برای هر x,y در S داریم:

$$\begin{aligned}&R(f\circ g(x),f\circ g(y))\\&=R(f(g(x)),f(g(y))\\&=R(g(x),g(y))\\&=R(x,y)\end{aligned}$$

از طرفی دیگر برای هر x در S داریم:

$$\begin{aligned}C(f\circ g(x)) &= C(f(g(x))\\&= C(g(x))\\&= C(x)\end{aligned}$$

به این ترتیب $f\circ g$ عضوی $\mathrm{Aut}(G)$ است خواص دیگر گروه به سادگی قابل بررسی است. بنابراین $\mathrm{Aut}(G)$ همراه با ترکیب توابع یک گروه است.

گزاره ۵-۳: فرض کنید R و R' به ترتیب دو رابطه چندمجموعه‌ای روی چندمجموعه‌های C و C' باشند. اگر $G=(S,C,R)$ و $G'=(S,C',R')$ یکریخت باشند در این صورت $\mathrm{Aut}(G)\cong\mathrm{Aut}(G')$.

اثبات: از آنجایی که $G=(S,C,R)$ و $G'=(S,C',R')$ یکریخت هستند تابع $\pi:S\to S$ وجود دارد که به ازای هر $f\in\mathrm{Aut}(G)$، $\pi\circ f\circ\pi^{-1}\in\mathrm{Aut}(G')$، زیرا به ازای هر $x\in S$،

$$\begin{aligned}&R'\big(\pi\circ f\circ\pi^{-1}(x),\pi\circ f\circ\pi^{-1}(y)\big)\\&=R\big(f\circ\pi^{-1}(x),f\circ\pi^{-1}(y)\big)\\&=R\big(\pi^{-1}(x),\pi^{-1}(y)\big)\\&=R'\big(\pi\circ\pi^{-1}(x),\pi\circ\pi^{-1}(y)\big)\\&=R'(x,y)\end{aligned}$$

همچنین به سادگی می‌توان نشان داد تابع

$$\varphi:\mathrm{Aut}(G)\to\mathrm{Aut}(G')$$
$$\varphi(f)=\pi\circ f\circ\pi^{-1}$$

یک یکریختی بین گروه‌ها است. پس داریم

$$\mathrm{Aut}(G)\cong\mathrm{Aut}(G').$$

گزاره ۵-۴: فرض کنید $G=(S,C,R)$ یک رابطه چندمجموعه‌ای روی C تحت مجموعه‌ی پشتیبان $S=\{1,2,\ldots,n\}$ باشد، نگاشت $C':\mathrm{Aut}(G)\to\mathbb{W}$ به‌صورت زیر تعریف می‌شود:

$$C'(f)=\begin{cases}\min\{f(i)\mid f(i)\neq i\} & f\neq id\\ n & f=id\end{cases}$$

به‌طوری‌که $\mathrm{Max}_{i\in\mathbb{N}_n}C(a_i)\le n$. آنگاه

الف) C' یک چندگروه غیرثابت از $Aut(G)$ است.

ب) اگر $\otimes_n$ یک t_n-نرم دلخواه باشد آنگاه به ازای هر $r\in\{0,1,..,n\}$، $C'_r(f)=r\otimes_n C'(f)$، یک چندگروه t_n-نرم تحت $\otimes_n$ از $Aut(G)$ است.

اثبات: الف) به ازای هر $\mathrm{id}\neq f\in G$ قرار می‌دهیم

$$C'(f)=\min\{f(i)\mid f(i)\neq i\}$$

فرض کنید $f,g\in Aut(G)$ و $f\circ g\neq \mathrm{id}$، آنگاه $C'(f\circ g)=\min\{f\circ g(i)\,|\,f\circ g(i)\neq i\}$ لذا عضوی مانند r وجود دارد که

$$C'(f\circ g)=f\circ g(r)$$

و

$$f\circ g(r)\neq r$$

حالت اول: $f\circ g(r)\neq g(r)$، بنابراین

$$\begin{aligned}C'(f\circ g)&=f(g(r))\\&\geq \min\{f(i)\,|\,f(i)\neq i\}\\&=C'(f)\\&\geq \min(C'(f),C'(g))\end{aligned}$$

حالت دوم: $f\circ g(r)=g(r)$، بنابراین $g(r)\neq r$ و

$$\begin{aligned}C'(f\circ g)&=f(g(r))=g(r)\\&\geq \min\{g(i)\,|\,g(i)\neq i\}\\&=C'(g)\\&\geq \min(C'(f),C'(g))\end{aligned}$$

فرض کنید $\mathrm{id}\neq f\in A_{\bullet}ut(G)$. آنگاه $s\in S$ وجود دارد به قسمی که:

$$C'(f)=\min\{f(i)\,|\,f(i)\neq i\}=f(s)$$

قرار می‌دهیم $f(f(s))=k$. بنابراین $C'(f)=f(s)=f^{-1}(k)$ و $f^{-1}(k)\neq k$، در نتیجه $C'(f)\geq C'(f^{-1})$. پس C' یک چندگروه از $Aut(G)$ است.

برای اثبات (ب) در هر دو حالت داریم:

$$\min\{C'(f),C'(g)\}\geq C'(f)\otimes_n C'(g)$$

لذا $C'(fg)\geq C'(f)\otimes_n C'(g)$، پس داریم:

$$\begin{aligned}C'_r(fg)&=C'(fg)\otimes r\\&\geq (C'(f)\otimes_n C'(g))\otimes r\\&\geq (C'(f)\otimes_n r)\otimes_n (C'(g)\otimes_n r)\\&=C'_r(f)\otimes_n C'_r(g)\end{aligned}$$

و این نشان می‌دهد که C'_r یک چندگروه t_n-نرم تحت $\otimes_n$ از $Aut(G)$ است.

حال نشان می‌دهیم C' غیرثابت است. فرض کنید $f(\alpha)=\min\{f(i)\,|\,f(i)\neq i\}$.

اگر $f(\alpha)=n$ آنگاه دوحالت زیر را داریم:

الف) $f(n)=n$ در این صورت از $f(\alpha)=n$ و یک به یک بودن نتیجه می‌گیریم $\alpha=n$. در نتیجه $f(n)\neq n$ و این تناقض است.

ب) $f(n)\neq n$ آنگاه $f(n)\geq f(\alpha)$. از $f(\alpha)=n$ داریم $f(n)\geq n$. از طرفی $f(n)\leq n$. پس $f(n)=n$ و این تناقض است.

در نتیجه $f(\alpha)\neq n$ و این نشان می‌دهد C' غیرثابت است.

نتیجه ۵-۵: فرض کنید $G=(S,C,R)$ یک رابطه چندمجموعه‌ای روی C تحت مجموعه‌ی متناهی S باشد. $G^{\alpha}=(\mathbb{N}_n,C^{\alpha},R^{\alpha})$ را به‌صورت زیر تعریف می‌کنیم:

۱) تابع $\alpha:S\to\mathbb{N}_n$ یک به یک و پوشا است.

۲) $C^{\alpha}:\mathbb{N}_n\to\mathbb{W}$ و $C^{\alpha}(i)=C(\alpha^{-1}(i))$.

۳) $R^{\alpha}(i,j)=R(\alpha^{-1}(i),\alpha^{-1}(j))$.

همچنین به ازای هر $f\in \mathrm{Aut}(G)$،

$$f_{\alpha}:\mathbb{N}_n\to\mathbb{N}_n$$
$$f_{\alpha}(i)=\alpha\circ f\circ\alpha^{-1}(i)$$

در این صورت:

الف) اگر $f_{\alpha}\in \mathrm{Aut}(G^{\alpha})$، آنگاه $(f\circ g)_{\alpha}=f_{\alpha}\circ g_{\alpha}$.

ب) چندمجموعه‌ی d با ضابطه‌ی

$$d:\mathrm{Aut}(G)\to\mathbb{W}$$
$$d(f)=C'_r(f_{\alpha})$$

یک چندگروه t_n-نرم تحت $\otimes_n$ از $\mathrm{Aut}(G)$ است.

اثبات: اگر $f \in \mathrm{Aut}(G)$، آنگاه برای هر $i \in \mathbb{N}_n$ داریم:

$$\begin{aligned} C^{\alpha}\left(f_{\alpha}(i)\right) &= C(\alpha^{-1}\left(f_{\alpha}(i)\right) \\ &= C\left(\alpha^{-1}\circ\alpha\circ f\circ\alpha^{-1}(i)\right) \\ &= C\left(f\circ\alpha^{-1}(i)\right) \\ &= C\left(\alpha^{-1}(i)\right) \end{aligned}$$

به طور مشابه به ازای هر $i, j \in \mathbb{N}_n$ داریم:

$$R^{\alpha}(f_{\alpha}(i), f_{\alpha}(j)) = R^{\alpha}(i,j)$$

اینک فرض می‌کنیم $f_{\alpha} \in \mathrm{Aut}(G^{\alpha})$. لذا به ازای هر $i \in N_n$:

$$\begin{aligned} (f\circ g)_{\alpha}(i) &= \alpha\circ f\circ g\circ\alpha^{-1}(i) \\ &= (\alpha\circ f\circ\alpha^{-1})\circ(\alpha\circ g\circ\alpha^{-1}(i)) \\ &= f_{\alpha}\circ g_{\alpha}(i) \end{aligned}$$

بنابراین $(f\circ g)_{\alpha} = f_{\alpha}\circ g_{\alpha}$.

۲) فرض کنید $f, g \in \mathrm{Aut}(G)$، بنابراین:

$$\begin{aligned} d(f\circ g) &= C'_r((f\circ g)_{\alpha}) \\ &= C'_r(f_{\alpha}\circ g_{\alpha}) \\ &\geq C'_r(f_{\alpha})\otimes_n C'_r(g_{\alpha}) \\ &= d(f)\otimes_n d(g) \end{aligned}$$

و این نشان می‌دهد d یک چندگروه t_n-نرم تحت $\otimes_n$ از $\mathrm{Aut}(G)$ است.

۶- تولید رمز یکبار مصرف با استفاده از خودریختی روابط چند مجموعه‌ای

در این بخش با توجه به مفاهیم بالا به یکی از کاربردهای چندگروه اشاره می‌کنیم. در حال حاضر رمزهای یکبار مصرف برای بانکداری اینترنتی یا تایید هویت واقعی اشخاص در شبکه‌های اجتماعی استفاده می‌شود[۲۱-۲۲]. در اینجا مشابه شبیه سازی تولید اعداد تصادفی و شبه تصادفی در آمار به کمک چندگروه و خودریختی‌های آن، اعداد تصادفی را تولید می‌کنیم و از آن رمز یکبار مصرف می‌سازیم. با توجه به زمان ورود فرد برای دریافت رمز یکبار مصرف ، رمز تولید می‌شود و می‌توان به راحتی رمز را بر اساس مولفه‌های اضافه بر زمان تولید کرد. به طور مثال بر اساس زمان ورود و کدملی و ... می‌توان رمز یکبار مصرف را تولید کنیم. ابتدا الگوریتم زیر را بیان می‌کنیم و سپس با یک مثال رمز را تولید می‌کنیم:

✓ **الگوریتم تولید رمز یکبار مصرف**

۱. ساعت (h)،دقیقه (m)،ثانیه (s)، روز (a) و ماه (b) را به صورت $m_1 = hmsab$ وارد کنید.

۲. به ازای $2 \leq i \leq 8$، $m_i = m_1 + 8(i-1)$ و $m = \sum_{i=1}^{8} m_i$

را در نظر بگیرید. حال قرار دهید $\varepsilon = \frac{1 - \frac{m_8}{m}}{2}$.

۳. به ازای هر $1 \leq i \leq 8$، $\sigma_i = \frac{m_i}{m} + \frac{\varepsilon}{2^{8-i}}$.

۴. با در نظر گرفتن یک رابطه چندمجموعه‌ای مناسب، $\mathrm{Aut}(G)$ را بدست آورده و قرار بده $\alpha = (\frac{|\mathrm{Aut}G|}{|\mathrm{Aut}G|+2} + \sigma_8) + \sum_{i=1}^{i=8}\sigma_i$.

۵. به ازای هر $1 \leq i \leq 8$، $P_i = \frac{\sigma_i}{\alpha}$.

۶. به ازای هر $\phi \in \mathrm{Aut}(G)$، $C'_r(\phi)$ را بدست آورده و قرار بده $sd = \frac{\varepsilon + \frac{1}{8}(\oplus_8 \sum_{\phi\in AutG} C'_r(\phi))}{|\mathrm{Aut}G|+3}$.

۷. اگر بخواهیم رمز براساس روز iام انتخاب شود قرار دهید $\mathrm{Password} = 10^{10}(\mathrm{sd}+\mathrm{p}_i)$.

۸. اگر بخواهیم رمز براساس ارقام ۱ تا ۸ انتخاب شود عدد k را وارد کن و قرار دهید $\mathrm{Password} = 10^{10}(\mathrm{sd}+\mathrm{p}_k)$.

مثال ۶-۱: رابطه چندمجموعه‌ای $G = (S, C, R)$ که در آن $C : S \to \mathbb{W},\ C(x) = a$

و رابطه R مطابق با جدول زیر در نظر بگیرید:

R	۱	۲	۳	۴	۵	۶	۷	۸
۱	۰	$a^{۳}$	۰	۰	۰	۰	۰	۰
۲	$a^{۳}$	۰	$a^{۲}$	۰	$a^{۲}$	۰	۰	۰
۳	۰	$a^{۲}$	۰	$a^{۴}$	۰	۰	$a^{۲}$	۰
۴	۰	۰	$a^{۴}$	۰	۰	۰	۰	۰
۵	۰	$a^{۲}$	۰	۰	۰	$a^{۴}$	۰	۰
۶	۰	۰	۰	۰	$a^{۴}$	۰	$a^{۲}$	۰
۷	۰	۰	$a^{۲}$	۰	$a^{۲}$	۰	۰	$a^{۳}$
۸	۰	۰	۰	۰	۰	۰	$a^{۳}$	۰

$a = \min\{C(a_i)\}_{i=۱}^{۸}$,

$a^{۲} = a \oplus_{۸} a$,

$a^{۳} = a \oplus_{۸} a \oplus_{۸} a$ و

$a^{۴} = a \oplus_{۸} a \oplus_{۸} a \oplus_{۸} a$.

الگوریتمی برای تولید یک رمز یک بار مصرف به شکل زیر به کمک مفاهیم گفته شده خواهیم داشت:

$$\mathrm{Aut}(G) = \{\mathrm{id}, (۱\ ۸)(۲\ ۷), (۳\ ۵)(۴\ ۶), (۱\ ۸)(۲\ ۷)(۳\ ۵)(۴\ ۶)\}$$

همچنین به ازای $r = a^{۲}$ داریم:

$$C'_r(f) = \begin{cases} ۳ \oplus_{۸} a^{۲} & f = (۳\,۵)(۴\,۶) \\ ۱ \oplus_{۸} a^{۲} & f = (۱\,۸)(۲\,۷)(۳\,۵)(۴\,۶) \\ ۱ \oplus_{۸} a^{۲} & f = (۱\,۸)(۲\,۷) \\ ۸ \oplus_{۸} a^{۲} & f = \mathrm{id} \end{cases}$$

با استفاده از الگوریتم بالا به عنوان مثال به ازای $a = ۷$ برای روز چهارشنبه، ۱۷ خرداد، ساعت ۱۲:۲۰:۳۰، داریم:

$m_{۱} = ۱۲۲۰۳۰۱۷۳$

$\oplus_{۸} \sum_{\phi \in AutG} C'_r(\phi) =$

$(۳ \oplus_{۸} ۶) \oplus_{۸} (۱ \oplus_{۸} ۶) \oplus_{۸} (۱ \oplus_{۸} ۶) \oplus_{۸} (۸ \oplus_{۸} ۶)$

$= ۷.$

$$sd = \frac{\varepsilon + \frac{۱}{۸}(\oplus_{۸} \sum_{\phi \in AutG} C'_r(\phi))}{|\mathrm{Aut}G| + ۳}$$

$$= \frac{۰.۴۳۷۴۹۹۹۸۶ + \frac{۷}{۸}}{۷}$$

$$= ۰.۱۸۷۴۹۹۹۹۸$$

لذا طبق جدول زیر رمز مربوطه برابر ۲۴۵۴۴۹۷۱۳ می‌باشد.

جدول(۱): جدول رمز یکبار مصرف

ردیف	روز	P_i	$Sd + P_i$
۱	شنبه	۰,۰۴۱۴۱۵۱۴	۰,۲۲۸۹۱۵۱۳۸
۲	یکشنبه	۰,۰۴۲۵۱۷۴۴۷	۰,۲۳۰۰۱۷۴۴۵
۳	دوشنبه	۰,۰۴۴۷۲۲۰۵۸	۰,۲۳۲۲۲۲۰۵۶
۴	سه شنبه	۰,۰۴۹۱۳۱۲۷۸	۰,۲۳۶۶۳۱۲۷۶
۵	چهارشنبه	۰,۰۵۷۹۴۹۷۱۵	۰,۲۴۵۴۴۹۷۱۳
۶	پنجشنبه	۰,۰۷۵۵۸۶۵۸۷	۰,۲۶۳۰۸۶۵۸۵
۷	جمعه	۰,۱۱۰۸۶۰۳۲۷	۰,۲۹۸۳۶۰۳۲۵
۸	------	۰,۱۸۱۴۰۷۸۰۶	۰,۳۶۸۹۰۷۸۰۴

فهرست منابع

[1] J. A. Awolola and A.M. Ibrahim, Some results on multigroups, Quasi. Related Systems 24(2): 169- 177(2016)

[2] W.D. Blizard, Multiset theory, Notre Dame J. of Formal Logic, 30:36-66(1989)

[3] W.D. Blizard, The development of multiset theory, Modern Logic, 1: 319-352(1991)

[4] C. Brink, Multisets and the Algebra of Relevance Logic. The Journal of Non-Classical Logic, 5(1): 1-21 (1988)

[5] M. Dresher and O. Ore, Theory of multigroups, American J. Math., 60: 705-733(1938)

[6] A.M. Ibrahim and P.A. Ejegwa, A survey on the concept of multigroup theory, J. Nigerian Asso. Mathl. Physics 38: 75- 89(2016)

[7] L. Mao, Topological multigroups and multifields, Int. J. Math. Combin., 1: 8-17(2009)

[8] R. K. Meyer, and M. A. McRobbie, On multisets and relevant implication I and II. Australasian Journal of Philosophy, 60: 107-139(1982)

[9] S. K. Nazmul, P. Majumdar and S.K. Samantha, On Multisets and Multigroups, Annals of Fuzzy Mathematics and Informatics, 6(3): 643-656(2013)

[10] W. Penowitz, Projective geometries as multigroups, American J. Math., 65: 235-256:(1943)

[11] B.M. Schein, Multigroups, J. Algebra 111: 114-132(1987)

[12] D. Singh, A.M. Ibrahim, T. Yohanna, and J.N. Singh, An overview of the applications of multisets, Novi Sad J. Math. 37(2): 73- 92 (2007)

[13] G. Silvia, J. Pantovic and V. Gradimir, Binary relations and algebras on multisets. Publications de L'Institute Mathematique, Nouvelle serie, tome 95(109): 111-117(2014)

[14] D. Singh, A Note on the Development of Multiset Theory. Modern Logic, 4: 405-406(1994)

[15] D. Singh, A. M. Ibrahim, T. Yohanna and J.N. Singh, An Overview of Applications of Multisets. Novi Sad Journal of Mathematics, 37(2): 73-92(2007)

[16] D. Singh, A. M. Ibrahim, T. Yohanna and J.N. Singh, A Systemization of Fundamentals of Multiset. Lecturas Matematicas, 29:33-48(2008)

[17] A. Syropoulous, Mathematics of multisets, Springer-Verlag Berlin Heidelberg (2001)

[18] Y. Tella and S. Daniel, A study of group theory in the context of multiset theory, Int. J. Sci. Tech. 2(8): 609-615(2013)

[19] Y. Tella and S. Daniel, Symmetric groups under multiset perspective, IOSR J. Math. 7 (5), 47-52(2013)

[20] N.J. Wildberger, A new look at multisets, School of Mathematics, UNSW Sydney 2052, Australia, (2003)

[۲۱] نظام الدین فقیه، سیستم‌های پویا: اصول و تعین هویت، شابک ۷-۸۰۶-۴۵۹-۹۶۴-۹۷۸، (۱۳۹۳)

[۲۲] نظام الدین فقیه، مبانی شبیه سازی سیستم‌ها، شابک ۹۶۴-۶۸۱۰-۰۶-۳، (۱۳۷۸)