م.ح 2016/3/23

تجزئة مجموعة إلى عدة مجموعات: لنفرض A مجموعة معينة عدد عناصرها r وأن $r_1, r_2, \ldots, r_n$ أعداد طبيعية تحقق $r = r_1 + r_2 + \ldots + r_n$ فيمكن تجزئة A إلى n مجموعة $A_1, \ldots, A_n$

حيث $|A_1| = r_1$ ، $|A_2| = r_2$ ، ... ، $|A_n| = r_n$

تحقق التجزئة: $A = \bigcup_{i=1}^{n} A_i$

مجموعات منفصلة $A_i \cap A_j = \phi \quad i \neq j$

وعليه عدد طرائق اختيار الأجزاء يساوي

$$\binom{r}{r_1, r_2, \ldots, r_n} = \frac{r!}{r_1!\, r_2! \cdots r_n!}$$

$r = 10$ ، $r_1 = 5$ ، $r_2 = 3$ ، $r_3 = 2$

$$= \binom{10}{5}\binom{5}{3}\binom{2}{2} = \frac{10!}{5!\,5!} \cdot \frac{5!}{3!\,2!} \cdot \frac{2!}{2!\,0!}$$

من هنا استنتجنا القانون السابق

مثال: بكم طريقة يمكن توزيع 7 جوائز على ثلاث أطفال إذا كان يريد أن نعطي الطفل الأول 3 جوائز و الطفلين الآخرين جائزتين

$$\binom{7}{3\ 2\ 2} = \frac{7!}{3!\,2!\,2!}$$

مثال: بكم طريقة يمكن توزيع أوراق اللعب على أربع أشخاص بالتساوي

$$\binom{52}{13\ 13\ 13\ 13} = \frac{52!}{(13!)^4}$$

يكفي جواب إلى هنا

التباديل: هو التقابل من المجموعة $A=\{1,2,\ldots,n\}$ مجموعة كل
إلى نفسها ونرمز لها بـ S_n.

$$f: A \longrightarrow A \;:\; f(i)=j$$

أي الـ 3 أماكن
(2) لها 2 مكان
(3) له مكان واحد

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\ldots\right\}$$

$$|S_3|=3!=6$$

ملاحظة: $|S_n|=n!$

مقلوب تباديل: هو تبديل بين سطري مصفوفة.

$$\sigma=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$$

$$\sigma^{-1}=\begin{pmatrix}3&4&2&1\\1&2&3&4\end{pmatrix}$$

بالترتيب ومحافظة على صورة العدد $=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$

التبديل المطابق: $f(i)=i$

$$id=\begin{pmatrix}1&2&3&\ldots&n\\1&2&3&\ldots&n\end{pmatrix}$$

تركيب تباديل: $\pi\circ\tau=\pi\cdot\tau$

تركيب التباديل توابع فيمكن تركيبها

مع العلم: $\pi\tau\neq\tau\pi$ من الأخر للأول.

$$\pi=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$1\longrightarrow1\longrightarrow2$

$2\longrightarrow3\longrightarrow3$

$3\longrightarrow2\longrightarrow1$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\pi\circ\tau$$

ب

تعريف: يمكن كتابة عناصر S_n باستخدام ترميز الحلقات

إذا كان: $a_1 \to a_2, a_2 \to a_3, \dots$ تكتب،

$a_k \to a_1$

$$(a_1 \quad a_2 \quad \dots \quad a_k)$$

أي الحلقة ستكون:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_k \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$$

عندما يرتبط العنصر مع نفسه فإننا لا نكتبه بصيغة حلقة

مثال: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ← عنصر مرتبط مع نفسه

$= (2,3)$

بتركيب توابع نحصل $(3,2)$.

ملاحظة: إن الحلقة الأحادية لا تكتب.

مثال:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 \end{pmatrix}$$

$1 \to 2 \to 3 \to 4$

$= (1 \quad 2 \quad 3 \quad 4)(5 \quad 6)$ حلقة أحادية (7)

مثال: من أجل $n = 9$

$$(2 \quad 3 \quad 5 \quad 1)(7 \quad 8)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 5 & 4 & 1 & 6 & 8 & 7 & 9 \end{pmatrix}$$

كل عدد لم يذكر فهو أحادي مرتبط مع نفسه

مثال:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 4 & 1 & 8 & 7 & 6 \end{pmatrix}$$

$1 \to 3 \to 5 \to 1$ $6 \to 8 \to 6$

(عناصر أحادية .

لم تذكر) $(1\ 3\ 5)\ (6\ 8)$

ممكن أن يأتي تركيب تبادل بالشكل:

$(1\ 2)(2\ 3) = (1\ 2\ 3$

ليست حلقات لأنه يوجد عنصر مشترك (2)

(1) مرتبط مع (2) و (2) مرتبط مع (3) و (3) عنصر أحادي

مرتبط مع (3)

ملاحظة: التبديل المطابق في الحلقات يكتب بالشكل:

$id = (1)(2) \ldots (n)$

تعريف: أي عنصر في S_n يقال إنه زوجي أو فردي ويقال عن جميع العناصر الزوجية من S_n بـ A_n.

- إن لدينا تبديل المطابق زوجي $\forall\ n \geq 2$

- n الحلقة $(a_1, a_2, \ldots, a_k)$ تكون زوجية إذا كان k فردي

عدد عناصر

وبالعكس

- إن التبديل $(c_1, \ldots, c_m)\ (b_1, b_2, \ldots b_n)\ (a_1, \ldots, a_k)$

$(k-1)(n-1)(m-1)$ زوجي ← تبديل زوجي

فردي ← تبديل فردي

ملاحظة: تطبق هذه ~~الخواص~~ الخواص على تبديل الواحد (أي لا يوجد تقاطعات بين الحلقات)

تبديل واحد مثل $(1\ 2\ 3)(5\ 6)$

لكن $(1\ 2)(2\ 3)$ هذا ليس تبديل لأن (2) مشترك في حلقتين

بهذه الحالة نطلع نتيجة التبديل ونطبق الخواص.

ملاحظة:

في S_n نصف عناصرها زوجي ونصفها فردي.

$$|A_n| = \frac{n!}{2} \in \mathbb{N}$$

2016 / 3 / 24 م.3

الزمرة: هي عبارة عن بنية $\langle G, \sim \rangle$ حيث G مجموعة غير خالية مع قانون تشكيل $\sim$ يحقق الشروط التالية

1) $\sim$ مغلق في G: $\forall x,y \in G : x \sim y \in G$

2) $\sim$ تجميعي: $\forall x,y,z \in G,\ (x \sim y) \sim z = x \sim (y \sim z)$

3) يوجد في G حيادي بالنسبة لـ $\sim$ وليكن e_G

$$\forall x \in G,\ e_G \sim x = x \sim e_G = x$$

4) لكل عنصر نظير في G بالنسبة لـ $\sim$

$$\forall x \in G : y \sim x = x \sim y = e_G$$

وندعو y بنظير x ونرمز له بـ x^{-1}

مثال:

$\langle \mathbb{R}, + \rangle$ زمرة ، $\langle \mathbb{R}, \cdot \rangle$ ليست زمرة ، $\langle \mathbb{R}^*, \cdot \rangle$ زمرة

$\langle Z, + \rangle$ زمرة و $\langle Z, \cdot \rangle$ ليست زمرة

* أثبت أن $\langle S_2, \circ \rangle$ زمرة باستخدام جدول كيلي. (جدول قانون تشكيل)

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$id = (1)(2)$ $(1\ 2)$

مثال عن جدول كيلي: هل البنية $\langle A, + \rangle$ زمرة حيث $A = \{0, 1, 2\}$

جدول كيلي هو:

+	0	1	2
0	0	1	2
1	1	2	3
2	2	3	4

ليست زمرة لأنها ليست مغلقة بالنسبة لـ $(+)$.

حل التمرين: جدول كيلي هو:

o تركيب	id	$(1\ 2)$
id	id	$(1\ 2)$
$(1\ 2)$	$(1\ 2)$	id

$1 \to 2 \to 1$
$2 \to 1 \to 2$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = id$$

من الجدول: 1) مغلقة 2) الحيادي هو id 3) $(1\ 2)^{-1} = (1\ 2)$

4) تركيب توابع تجميعي

مثال. هل $\langle A_3, \circ \rangle$ زمرة ولماذا؟ زمرة زوجية من S_3.

$$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$$

عدد عناصرها

$1 \to 2 \to 3 \to 1$ $1 \to 3 \to 2 \to 1$

$$\frac{n!}{2} = \frac{3!}{2} = 3$$

A_3 زوجية لأن: id زوجية $\forall n \geq 2$

$(1\ 2\ 3)$, $(1\ 3\ 2)$ ← عددها فردي لأن دورات زوجية

$\circ$	id	$(1\ 2\ 3)$	$(1\ 3\ 2)$
id	id	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	id
$(1\ 3\ 2)$	$(1\ 3\ 2)$	id	$(1\ 2\ 3)$

$(1\ 2\ 3)(1\ 2\ 3)$

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}$$

$$= (1\ 3\ 2)$$

زمرة لأن من جدول 1) $\circ$ مغلقة

2) يوجد محايد وهو id

3) لكل عنصر نظير

$(1\ 3\ 2)^{-1} = (1\ 2\ 3)$

$(1\ 2\ 3)^{-1} = (1\ 3\ 2)$

تمرين: هل البنية $\langle A, \Delta \rangle$ زمرة ولماذا؟

حيث $A = \{0, 1, 2\}$

باقي قسمة $(x+y)$ على 3 $x \Delta y = (x+y) \pmod 3$

- هل البنية $\langle G_n, \cdot \rangle$ زمرة ولماذا؟

حيث: $G_n = \{1, g^1, \_\_\_, g^{n-1}\}$

حيث $g^i \cdot g^j = g^{i+j}$, $g^n = 1$

حل وظيفة 3.3

نشكل جدول كيلي :

Δ	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$0+0=0$ باقي قسمة على 3 هو صفر

إذاً (Δ , Z_3) مغلقة

- حيادي موجود وهو صفر
- ولكل عنصر نظير $2^{-1}=1$ و $1^{-1}=2$
- وتحقق خاصية تجميعية

$2=1+1$

$$G_5=\{g^0 \quad g^1 \quad g^2 \quad g^3 \quad g^4\}$$

نشكل جدول كيلي :

$\sim$	g^0	g^1	g^2	g^3	g^4
g^0	$g^0=1$	g^1	g^2	g^3	g^4
g^1	g^1	g^2	g^3	g^4	$g^5=1$
g^2	g^2	g^3	g^4	$g^5=1$	g^1
g^3	g^3	g^4	$g^5=1$	g^1	g^2
g^4	g^4	$g^5=1$	g^1	g^2	g^3

$g^2 \sim g^4 = g^{2+4} = g^6 = \underbrace{g^5}_{1} . g^1 = g^1$

$g^3 \sim g^3 =$

$g^3 \sim g^4 = g^4 \sim g^3 = g^{4+3} = g^7$

$= g^5 . g^2 = g^2$

$g^{3} \sim g^4 = g^2 = g^5 . g^2 = g^2$

وبالتالي هي زمرة ومغلقة وتبديلية ... g^1 ولكل نظير

م 4 2016/13/30

..الأعداد صحيحة..

باقي القسمة : $a \equiv b (\mod m)$ باقي قسمة العدد a على m هو عدد b.

ويرمز للصف $[x]$ لصف البواقي وهي مجموعة الأعداد الصحيحة والتي يكون باقيها مشتركا على m يساوي x

مثال: ليكن $m=5$ فإن $t = x (\mod 5)$ وهي:

$[5]=[0]=0+5\mathbb{Z}=\{\dots,-10,-5,0,5,10,\dots\}$

عدد 5 قوائم $[6]=[1]=1+5\mathbb{Z}$

$[2]=2+5\mathbb{Z}$

$[3]=3+5\mathbb{Z}$

$[4]=4+5\mathbb{Z}$

ويرمز بـ $\mathbb{Z}/n\mathbb{Z}=\{[0],[1],[2],[3] \dots [n-1]\}$ n مقام

مبرهنة: ليكن $a,b \in \mathbb{Z}$ و $b>0$ عندها يوجد عددين صحيحين $q,r \in \mathbb{Z}$ بحيث

$a=bq+\underset{\text{باقي قسمة}}{r}$

حيث $0 \le r < b$

ملاحظات: 1) $\forall n \in N$ حيث $n \geq 2$ فإن باقي قسمة a على n وحيد

2) إن $[a]+[b]=[a+b]$

3) يمكن إيجاد $a \neq b$ بحيث $[a]=[b]$

4) إذا كان $a \neq c$ و $b \neq d$ بحيث $[a]=[c]$ و $[b]=[d]$

فإن $[a+b]=[c+d]$ سنستخدم بدلاً من $[i]$ مقدارا

$n = 5$

$[2]+[3] = [2+3] = [5] = [0]$

$[-3]+[1] = [-3+1] = [-2] = [3]$

$\Rightarrow \forall\, g \in \mathbb{Z} : \quad [g] \in \mathbb{Z}/5\mathbb{Z} = \{[0], \dots [4]\}$

إذا كان عدد موجب نطرح

إذا كان عدد سالب نتعامل له (n)

ونضيف عدد حتى نقدر

نطلع عدد يقبل قسمة (n)

$[123] = [123 - 3] = [3]$

$[-123] = [-123 + 2] = [-125] = [2]$

$\to 123 \equiv 3 \pmod 5$

$\to -123 \equiv \underset{\downarrow}{-3} \pmod 5$

$[-3] = [2]$

نطرح عدد 5 $\quad 129 \equiv 4 \pmod 5$

نجمع عدد ① مع تعامل الاشارة $\quad -129 \equiv 1 \pmod 5$

إن البنية $(\mathbb{Z}/n\mathbb{Z}, +)$ هي زمرة تبديلية حياديها $[0]$

حيادي نظير $[x] = [-x]$ يجب إرجاعة لعنصر زمرة من $\mathbb{Z}/n\mathbb{Z}$

مع $n - 0 =$ $[x] + [\ ]$ لها

مثال:

هل البنية $(\mathbb{Z}/3\mathbb{Z}/\{0\}, \cdot)$ زمرة ولماذا ؟

$\cdot$	1
1	1
2	2

مغلقة الحيادية 1

نظير $[2]$ هو $[2]^{-1} = [2]$

هل البنية $(\mathbb{Z}/4\mathbb{Z}/\{0\}, \cdot)$

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

ليست زمرة لأنها ليست مغلقة

و $0 \notin \mathbb{Z}/4\mathbb{Z}/\{0\}$ $[2]$ ليس لها نظير

أي $[2]\cdot[?] \neq 1$

أي عنصر

ملاحظة: $(\mathbb{Z}/n\mathbb{Z}\setminus\{0\}, \cdot)$ ليس بالضرورة زمرة في حال

كان n عدد أولي فتكون تلك البنية زمرة.

تعريف: من أجل $2 \le n \in \mathbb{N}$ المجموعة:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[q] : 1 \le q \le n-1 : \gcd(n,q) = 1\}$$

القاسم المشترك الأكبر

نلاحظ: $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ هي زمرة.

مثال: $(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\}$

هي زمرة لأن:

	1	3
1	1	3
3	3	1

مغلقة بالنسبة لـ (.)

حيادي هو (1)

$[3] = [3]^{-1}$.

أيضاً $(\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\}$

ملاحظة: نجد أن $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})\setminus\{0\}$ في حال n أولي.

مثال: $n = 5$ أولي

$$(\mathbb{Z}/5\mathbb{Z})^* = \{1,2,3,4\} = \mathbb{Z}/5\mathbb{Z}\setminus\{[0]\}$$

تعريف: لتكن $(G, \cdot)$ زمرة ما و $g \in G$ يعرف $\langle g\rangle$

بالزمرة الدائرية (المولدة) بالعنصر g وتعرف:

$\langle g\rangle = \{g^k : k \in \mathbb{Z}\} \rightarrow g \cdot g \cdots g$ مرة k

$\langle g\rangle = \{kg : k \in \mathbb{Z}\} \rightarrow g + g + \cdots + g$ مرة k