البنى الجبرية 1

الدكتور: حمزة الحاكمي

المحاضرة : السابعة عشر

التاريخ : ٢١/١١/٢٠١٦

إعداد : أحمد أبو التوت

Web: www.syriamath.net group: Improve our mathematics

((من أهم تطبيقات التماثل الأولى))

حيث وجدنا سابقا لأجل كل عدد صحيح توجد زمرتين الأولى هي nZ والثانية هي z_n حيث :

$$nZ = \{m.n \ \ : m \in Z\}$$

$$Z_n = \{0,1,\dots\dots,n-1\}$$

فهل توجد علاقة بين هاتين الزمرتين ؟ سندرس العلاقة من خلال المبرهنة التالية :

مبرهنة : ليكن $n \geq 1$ عدد صحيح عندئذ $\frac{Z}{<n>} \cong Z_n$

الإثبات :

بما أن زمرة الأعداد الصحيحة تبديلية فإن nZ ناظمية في Z إذاً nZ معرفة وبالتالي أيضاً $< n >$ معرفة .

ولدينا z_n زمرة بالنسبة لعملية الجمع بالمقاس n لنعرف العلاقة :

$$\varphi : Z \to Zn$$

بالشكل الاتي :

$$\forall x \in Z \ ; \ \varphi(x) = \underbrace{x \ mod - n}_{\text{باقي قسمة } x \text{ على } n} = r$$

لان $x = qn + r : 0 \leq r < n$ أي أن r وحيدة وموجود في Z_n . وبالتالي

واضح أن φ تطبيق .

وإن φ تشاكل لأنه إذا كان $x, y \in Z$ فإن :

$$\varphi(x+y) = (x+y)mod - n$$

$$= (x \ mod - n) + (y \ mod - n)$$

$$= \varphi(x) + \varphi(y) \ \ \Rightarrow \ \ \varphi \text{ تشاكل}$$

إن φ غامر لأن :

$$\forall \ a \in Z_n \qquad ; \qquad a \in Z$$

نأخذ الصورة المباشرة لـ a :

$$\varphi(a) = a.mod - n$$

$$\varphi(a) = a$$

وحسب مبرهنة التماثل الأولى فإن

$$\frac{Z}{\ker(\varphi)} \cong Z_n$$

حتى يتم المطلوب يجب ان نبرهن أن $<n>= \ker\varphi$

ليكن $x \epsilon \ker\varphi$ عندئذ $x \epsilon Z$

نأخذ الصورة المباشرة له :

$$\varphi(x) = x.mod - n = \underbrace{0}_{\text{محايد}}$$

حسب الخوارزمية $x = qn + r$ حيث :

$$r = x.mod - n = 0$$

وهذا يبين أن $x = qn \epsilon nZ$ حيث $q \epsilon Z$

ومنه $\ker\varphi \subseteq nZ$

الاحتواء المعاكس :

ليكن $y \epsilon nZ$ عندئذ $y = nt : t \epsilon Z$

$$\varphi(y) = y.mod - n = 0$$

وبالتالي $y \epsilon \ker\varphi$ ومنه فإن : $nZ \subseteq \ker f$

ومن الاحتوائين نجد : $<n>= nZ = \ker\varphi$

سنأخذ الأن مبرهنتين تفيدان في حل بعض التمارين التي تتعلق بالزمر المتماثلة وبشكل خاص بالزمر الدوارة .

مبرهنة : القضايا التالية صحيحة.

١) كل زمرة دوارة وغير منتهية تماثل الزمرة Z .
٢) جميع الزمر الدوارة وغير المنتهية متماثلة .

البرهان :

١) لتكن G زمرة دوارة غير منتهية عندئذ :

يوجد $a \in G$ حيث $G = < a >$

وجدنا سابقا أن العلاقة : $\varphi : Z \to G$ المعرفة بالشكل :

$$\forall\, n \in Z \;;\; \varphi(n) = a^n$$

وجدنا سابقا أن φ غامر و قد تم إثبات ذلك في محاضرات سابقة وإن φ متباين لأن G غير منتهية

لنبرهن أن φ تشاكل : ليكن $n, m \in Z$

$$\varphi(n+m) = a^{n+m} = a^n . a^m = \varphi(n).\varphi(m)$$

وهذا يبين أن φ تماثل أي ان $Z \cong G$

٢) لتكن G, G' زمرتين دوارتين غير منتهية عندئذ حسب ١ يوجد

$$f : Z \to G$$
$$g : Z \to G'$$

كلاً منهما تماثل ومنه

$$g^{-1} : G' \to Z$$

ايضا تماثل لآنه تقابل وايضاً هو تشاكل (اثبات التشاكل وظيفة وإليك حلها :)

ليكن $x, y \in G'$ فإن

$$g^{-1}(x.y) = n + m = a^n + a^m = g^{-1}(n) + g^{-1}(m)$$

لنركب تطبيقين كما يلي :

$$f.g^{-1} : G' \to G$$

ان التطبيق $f.g^{-1}$ هو تماثل لآنه تقابل وايضا هو تشاكل (اثبات التشاكل وظيفة و إليك حلها)

ليكن $x, y \in G'$ عندئذٍ:

$$f.g^{-1}(x.y) = f\big(g^{-1}(x.y)\big)$$

و لما كان كلاً من g^{-1}, f تشاكل فإن :

$$fg^{-1}(x.y) = f\big(g^{-1}(x.y)\big) = f\big(g^{-1}(x).g^{-1}(y)\big) = f\big(g^{-1}(x)\big).f\big(g^{-1}(y)\big)$$
$$= fg^{-1}(x).fg^{-1}(y)$$

و منه fg^{-1} تماثل و بالتالي $G \cong G'$

و هو المطلوب .

مبرهنة :

١) كل زمرة دوارة ومنتهية ومرتبتها n تماثل الزمرة Z_n .
٢) جميع الزمر الدوارة والمنتهية التي لها نفس المرتبة متماثلة .

البرهان :

١) لتكن G زمرة دوارة ومنتهية ومرتبتها n عندئذ يوجد :

$G = < a >$ حيث $a \in G$

وعندئذٍ $G = \{e, a, \dots \dots \dots, a^{n-1}\}$ وهذه العناصر مختلفة مثنى مثنى

لنعرف العلاقة $\varphi : Z_n \to G$ بالشكل :

$$\forall\, k \in Z_n \quad ; \quad \varphi(k) = a^k$$

واضح أن φ تطبيق ومتباين لان عناصر G مختلفة مثنى مثنى

وهو تشاكل لأن : $\forall\, t, s \in Z_n;$

$$\varphi(t + s) = a^{t+s} = a^t . a^s = \varphi(t).\varphi(s)$$

إن φ غامر لأنه من أجل $y \in G$ فإن $y = a^k$ حيث $0 \le k < n$

نأخذ الصورة المباشرة $\varphi(k) = a^k = y$ وبالتالي φ تماثل ومنه $Z_n \cong G$

٢) ينتج مباشرةً من (١).

أمثلة :

أي من هذه الزمر متماثلة : Z_4 , $U(10)$, $U(5)$

نعلم سابقا أن Z_4 زمرة دوارة ومرتبتها 4

$$Z_4 = \{0,1,2,3\} =< 1 >=< 3 >$$

$$U(10) = \{1,3,7,9\} \quad \Rightarrow \quad U(10) =< 3 >$$

$$3^0 = 1 \quad , \quad 3^1 = 3 \quad , 3^2 = 9 \;\; , \;\; 3^3 = 7 \;\; , \;\; 3^4 = 1$$

ومنه $U(10) \cong Z_4$

وايضاً

$$U(5) = \{1,2,3,4\} \qquad U(5) =< 2 >$$

$$2^0=1 \quad , \quad 2^1=2 \quad , 2^2=4 \ , \ 2^3=3 \ , \ 2^4=1$$

ومنه $U(5)\cong Z_4$

$U(5)\cong U(10)$ ومنه $U(5)\cong Z_4\cong U(10)$

مثال٢):

ادرس التماثل بين الزمرتين $U(10)$, $U(12)$ ؟

$$U(12)=\{1,5,7,11\}$$

$$5^0=1 \quad , \quad 5^1=5 \quad , 5^2=1$$

$$7^0=1 \quad , \quad 7^1=7 \quad , 7^2=1$$

$$11^0=1 \quad , \quad 11^1=11 \quad , 11^2=1$$

لا يمكن أن نستفيد من النص السابق في هذه الحالة كون الزمرة $U(12)$ ليست دوارة.لذلك سنلجأ لطريقة اخرى

لنفرض أن $U(10)\cong U(12)$ عندئذ يوجد تطبيق تشاكل وتباين وغامر

$$\varphi : U(10) \to U(12)$$

وان

$\varphi\big(U(10)\big)=U(12)$ أي انها دوارة وهذا غير ممكن لان $U(12)$ ليست دوارة أي أن

$$U(12)\ncong U(10)$$

تمرين : لتكن G زمرة غير تبديلية و منتهية مرتبتها P^3 حيث P عدد أولي اذا كان $Z(G)\neq<e>$ عندئذ

$$(Z(G):1)=P$$

البرهان: لما كنت G منتهية و $Z(G)$ زمرة جزئية في G فإنه حسب لاغرانج فإن مرتبة $Z(G)$ تقسم مرتبة G

$$(Z(G):1)\in\{1,P,P^2,P^3\}$$

ولما كانت $Z(G)\neq<e>$ فإن $(Z(G):1)\neq 1$

ولما كانت$Z(G)$ تبديلية فأن $Z(G)\neq P^3$ لان G زمرة غير تبديلية

لنفرض جدلاً أن $Z(G)=P^2$ ولنأخذ زمرة الخارج $G/Z(G)$ فإن

$$(G/Z(G):1)=(G:Z(G))=\frac{(G:1)}{(Z(G):1)}=\frac{P^3}{P^2}=P$$

وهذه يبين أن زمرة الخارج دوارة وبالتالي الزمرة G تكون تبديلية وهذه مرفوض فرضاً مما سبق نجد أن $(Z(G):1)=P$

تمرين : ليكن $n>1$ عدد صحيح و k قاسم موجب للعدد n عندئذ يوجد تشاكل زمري

$\varphi:U(n)\to U(k)$ نواته $U_k(n)$

البرهان : لدينا $U(n)=\{x\ ;x\in Z:\ 1\le x<n\ \ :\gcd(x,n)=1\}$

وحسب خوارزمية القسمة لأجل x,k فإن $0\le r<k$ $x=qk+r:q,r\in Z$

لنفرض أن $r=0$ عندئذ $x=qk$ وهذه يبين أن k يقسم x ولما كان k يقسم n نجد ان k

قاسم مشترك للعددين x,n وهذه يناقض كون $\gcd(x,n)=1$ اي أن $r\neq 0$ ومنه $1\le r<k$

لنفرض على ان $\gcd(r,k)=d>1$ عندئذ $s,t\in z$: $r=sd,\quad k=td$

$$x=qtd+sd=(qt+s)d$$

ومنه d يقسم x

من جهة اخرى لما كان d يقسم k و k يقسم n فإن d يقسم n وهذه يناقض كون $\gcd(x,n)=1$

مما سبق نجد ان $\gcd(r,k)=1$ ومنه $r\in U(n)$ والأن لنعرف العلاقة :

$$\varphi:U(n)\to U(k)$$

بالشكل الأتي $\forall x\in U(n):\varphi(x)=x\ mod-k=r$

واضح أن φ تطبيق

وإن φ تشاكل لأنه إذا كان $x,y\in U(n)$ فإن :

$$\varphi(x.y)=(x.y)mod-k$$

$$=(x\ mod-k).(y\ mod-k)$$

$$=\varphi(x).\varphi(y)\quad\Longrightarrow\quad \text{تشاكل}\ \varphi$$

لدينا $U_k(n)=\{x:x\in U(n)\ :x\ mod-k=1\}$

ليكن $x\in\ker(\varphi)$ عندئذ $x\in U(n)$

$$\varphi(x) = x \bmod -k = 1 \Longrightarrow x \in U_k(n)$$

ومنه $\ker(\varphi) \subseteq U_k(n)$

ليكن $y \in U_k(n)$ عندئذ $y \in U(n)$ وأن $y \bmod -k = 1$ وبالتالي $\varphi(y) = 1$

ومنه $y \in \ker(\varphi)$ عندئذ $U_k(n) \subseteq \ker(\varphi)$ من الاحتوائين نجد أن $U_k(n) = \ker(\varphi)$

"انتهت المحاضرة"

Syria Math