البنى الجبرية 1

الدكتور : حمزة الحاكمي

المحاضرة : السابعة

التاريخ : ٢٠١٦/١٠/١٧

إعداد : أحمد أبو التوت

القاسم المشترك الاعظم :

تعريف : ليكن $a, b \epsilon Z$ مغايرة للصفر نسمي أكبر عدد صحيح موجب يقسم كل من a, b القاسم المشترك الأعظم للعددين a, b ونرمز له $\gcd(a, b)$.

_ اذا كان $\gcd(a, b) = 1$ نقول في هذه الحالة أن العددين a, b أوليان فيما بينهما .

مبرهنة : ليكن $z \ni a, b \neq 0$ عندئذ يوجد $s, t \epsilon Z$ تحقق أن :

$$\gcd(a, b) = sa + bt$$

فضلاً عن ذلك فإن $\gcd(a, b)$ هو أصغر عدد طبيعي من الشكل: $sa + tb$.

الإثبات :

لنأخذ المجموعة $S = \{n.a + m.b > 0 : m, n \epsilon Z\}$

واضح أن $\emptyset \neq S \subset N$ ومنه يوجد في S عنصر أصغر

وليكن d وطالما $d \epsilon S$ فله نفس شكل عناصر S ومنه $d = s.a + t.b : s, t \epsilon Z$

وحسب خوارزمية القسمة لأجل العددين a, d نجد أن $a = q.d + r$ حيث $r, q \epsilon Z$ وأن $0 \leq r < d$.

لنفرض جدلا أن $r \neq 0$ ومنه عندئذ $0 < r < d$ ونحسب r من العلاقة $a = q.d + r$

$$r = a - q.d = a - q(sa + t.b) = (1 - q.s)a + (-q.t)b \epsilon S$$

ومنه $d > r$

وهذا يناقض كون d عنصر أصغر في S ومنه الفرض الجدلي خاطئ ومنه $r = 0$ وبالتالي $a = q.d$

وبنفس الطريقة نثبت أن d يقسم b ومنه يكون d قاسم مشترك للعددين a, b

والآن نثبت أن d قاسم مشترك أكبر (أي لا يوجد قاسم أكبر منه):

نفرض وجود قاسم مشترك اخر وليكن $\grave{d}$ عندئذ يوجد $\grave{n}, \grave{m} \epsilon Z$ بحيث

$$a = \grave{n}.\grave{d} \quad \text{و} \quad b = \grave{m}.\grave{d}$$

نعوض في علاقة الـ d ومنه نجد أن :

$$d = s.\grave{m}.\grave{d} + t.\grave{n}.\grave{d}$$

$$\overbrace{\acute{d}}^{\text{موجب}} = \left(\underbrace{s.\acute{m}.+t.\acute{n}}_{\text{موجب}}\right)\overbrace{\acute{d}}^{\text{موجب}}$$

ومنه نجد أن $d \geq \acute{d}$ ومنه يكون d القاسم المشترك الأكبر للعددين a,b وهو المطلوب .

$$\gcd(a,b) = d = s.a + t.b$$

تعريف :

ليكن $p \in Z$ نقول عن p عدد أولي إذا كان $P > 1$ وان مجموعة قواسمه $\{\pm1,\pm P\}$.

تمهيدية اقليدس : لتكن p عدداً أولياً و $a,b \epsilon Z$ إذا كان p يقسم الجداء $a.b$ عندئذ p يقسم a أو b .

الإثبات :

لنفرض أن p يقسم الجداء $a.b$ عندئذ يوجد عدد صحيح $s \epsilon Z$ بحيث $a.b = s.p$

ولنفرض أن p لا يقسم a

توضيح : إذا أخذنا أي عدد مع عدد أولي فإن القواسم هي $(1,p)$ ولو فرضنا أنه لا يقسم عندئذ لا يبقى قواسم أخرى غير الواحد .

عندئذٍ $\gcd(a,p) = 1$ أوليان فيما بينهما ومنه يوجد $m,t \epsilon Z$ بحيث $1 = m.a + t.p$ وحسب النص الأخير $b = m.a.b + t.p.b$ و منه

$$b = s.m.p + t.p.b = (s.m + t.b)p$$

أي أن p يقسم b وهو المطلوب .

تم الانتهاء من اول فصل و هو المجموعات والان سندخل في فصل جديد و هو:

نظرية الزمر

تعريف الزمرة :

لتكن G مجموعة غير خالية نسمي كل تطبيق G :

ملاحظة : (النقطة سنعبر عنها بدل من اشارة الضرب $\times$ كما يلي)

$$\cdot : \quad G \times G \to G$$

$$(a,b) \mapsto a.b$$

عملية ثنائية على G (قانون تشكيل داخلي)

تعريف (٢) :

لتكن G مجموعة غير خالية معرف عليها عملية ثنائية (.)

$$G \times G \to G$$

$$(a, b) \to a.b$$

نسمي الثنائية $(G\,,.)$ زمرة إذا حققت الشروط التالية :

١) $\forall\, a, b \in G;\ \ a.b \in G$

٢) تجميعية $\forall\, a, b \in G;\ \ (a.b).c = a.(b.c)$

٣) يوجد في G عنصر بحيث $e \in G$ بحيث :

نسمي e عنصر محايد $\forall\, a \in G\,; a.e = e.a = a$

٤) $\forall\, a \in G\,; \exists\, b \in G\ :\ a.b = b.a = e$

نسمي العنصر b مقلوب العنصر a ونرمز له a^{-1} .

تعريف :

نقول عن الزمرة $(G,.)$ إنها تبديلية إذا حققت الشرط :

$$\forall\, a, b \in G;\ \ a.b = b.a$$

إن الخصائص السابقة تتعلق بالزمر الضربية أما الزمر الجمعية تختلف

	الزمرة الجمعية	الزمرة الضربية
العملية الثنائية	$+$	$-$
العنصر المحايد	0	$1, e$
المقلوب أو النظير	نظير a هو $-a$	مقلوب a هو a^{-1}
التشكيل	$a + (-b)$	$a.b^{-1}$
المضاعف أو القوة	مضاعف a هو $n.a : n \epsilon Z$	قوة a هي $a^{n} : n \epsilon z$

ملاحظة :

لتكن G زمرة و $a \in G$ و $n \in Z$

$$a^n = \begin{cases} \overbrace{a.a.a.a....a}^{n\ \text{مرة}} & n > 0 \\ 1, e & n = 0 \\ \underbrace{a^{-1}.a^{-1}......a^{-1}}_{-n\ \text{مرة}} & n < 0 \end{cases}$$

$$n.a = \begin{cases} \overbrace{a + a + a + a....a}^{n\ \text{مرة}} & n > 0 \\ 0\ \text{محايد في زمرة} & n = 0 \\ \underbrace{(-a) + (-a)......+(-a)}_{-n\ \text{مرة}} & n < 0 \end{cases}$$

أمثلة عن الزمر بالنسبة للأعداد:

١) مجموعة الأعداد الصحيحة Z بالنسبة لعملية الجمع هي الأعداد $(Z,+)$ تشكل زمرة جمعية تبديلية .

ولكن $(Z,.)$ ليست زمرة بالنسبة لعملية ضرب الاعداد لأنها لا تحقق هذا الشرط :

$$\forall\, a \in G:\ \exists\, a^{-1} \in Z$$

لو كان لدينا $2 \in Z\,, 2^{-1} = \frac{1}{2} \notin Z$

٢) مجموعة الأعداد الحقيقية R بالنسبة لجمع الأعداد تشكل أيضا زمرة جمعية تبديلية $(R,+)$

٣) مجموعة الأعداد الحقيقية المغايرة للصفر R^* تشكل زمرة ضربية تبديلية $(R^*\,,\,.)$

((استثنينا الصفر لأن الصفر ليس له مقلوب))

بالنسبة للمصفوفات المربعة

$$M_2(Z) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a,b,c,d \in Z\right\}$$

تشكل زمرة بالنسبة لعملية جمع المصفوفات

بينما $M_2(Z) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} a,b,c,d \in Z\,, a.d - c.b \neq 0\right\}$

تشكل زمرة بالنسبة لعملية ضرب المصفوفات .

(لأنه لكي تكون للمصفوفة المربعة مقلوب فإن هذا يقتضي أن يكون محدد هذه المصفوفة غير معدوم)

تمهيدية :

لتكن G زمرة عندئذ :

١) العنصر المحايد في G وحيد .

٢) مقلوب أي عنصر في G وحيد .

٣) قانون الاختصار محقق أي إذا كان $a.b = b.c \quad : \quad \forall a,b,c \in G$

فإن $b = c$

٤) $\forall a \in G \; ; (a^{-1})^{-1} = a$

٥) $\forall \; a_1, a_2, a_3, \ldots \ldots . . a_n \in G$

$$(a_1, a_2, a_3, \ldots \ldots . . a_n)^{-1} = a_n{}^{-1}, a_{n-1}{}^{-1}, a_{n-2}{}^{-1} \ldots \ldots . . a_1{}^{-1}$$

الإثبات :

١) ليكن $e_1, e_2 \in G$ كل منهما عنصر محايد لنأخذ الجداء لهذ بين العنصريين

$$e_2 = e_2 . e_1 = e_1$$

٢) ليكن $a \in G$ ولنفرض أن $b \, , c \in G$ كل منهما مقلوب للعنصر a

طالما b هو المقلوب ل a فإن : $a . b = b . a = e$

طالما c هو مقلوب العنصر a فإن : $a . c = c . a = e$

ولنبرهن أن $b = c$:

طالما الزمرة تبديلية فلدينا محايد فإن :

$$b = e . b = \underbrace{c . (a . b)}_{\text{الخاصة التجميعية محققة}} = c . e = c$$

ومنه $b = c$.

٣) لتكن $a, b, c \in G$ تحقق : $a . b = a . c$

$a^{-1} . (a . b) = a^{-1} . (a . c) \implies$ تجميعية محققة

$$\underbrace{(a^{-1} . \text{a})}_{e} . \text{b} = \underbrace{(a^{-1} . a)}_{e} . c$$

$$e . b = e . c$$

٤) ليكن $a \in G$ عندئذ :

$$\underbrace{a^{-1}}_{\text{عنصر}} . \underbrace{(a^{-1})^{-1}}_{\text{مقلوبه}} = e$$

نضرب الطرفين ب a

$$(a^{-1})^{-1} = a$$

٥) يتم اثباته من خلال الاستقراء :

نثبته من أجل $n = 2$

ولنبرهن أن $a, b \in G$ $\quad (a . b)^{-1} = b^{-1} . a^{-1}$

وبما أن $a, b \in G$ فإن $a . b \in G$ ومنه لكل عنصر مقلوب أي : $(a . b)^{-1} \in G$ ويحقق أي عنصر .

مع المقلوب له يعطي المحايد أي أن : $(a.b).(a.b)^{-1} = e$.

$$. a(b.(a.b)^{-1}) = e$$

نضرب بـ a^{-1} من اليسار

$$. b.(a.b)^{-1} = a^{-1}$$

نضرب بـ b^{-1} من اليسار

$$(a.b)^{-1} = b^{-1}a^{-1}$$

لنفرض أن $n = k$ محققة : $\forall k \in N^*$

$$(a_1.a_2.a_3 \dots \dots .a_k)^{-1} = a_k{}^{-1}.a_{k-1}{}^{-1} \dots .a_2{}^{-1}.a_1{}^{-1} \ (*)$$

لنثبت صحة العلاقة من أجل $k+1 \in N^*$

$$(a_1.a_2.a_3 \dots \dots .a_{k+1})^{-1} = a_{k+1}{}^{-1}.a_k{}^{-1} \dots .a_2{}^{-1}.a_1{}^{-1} \ (**)$$

بفرض أن $(a_1.a_2.a_3 \dots \dots .a_k) = b$

بالتعويض في $(**)$ نجد :

$$(b.a_{k+1})^{-1} = a_{k+1}{}^{-1}.b^{-1} = a_{k+1}{}^{-1}.(a_1.a_2.a_3 \dots \dots .a_k)^{-1}$$

نلاحظ أن العلاقة $(*)$ محققة ومنه يكون :

$$= a_{k+1}{}^{-1}.a_k{}^{-1} \dots .a_2{}^{-1}.a_1{}^{-1}$$

وبالتالي : $(a_1.a_2.a_3 \dots \dots .a_{k+1})^{-1} = a_{k+1}{}^{-1}.a_k{}^{-1} \dots .a_2{}^{-1}.a_1{}^{-1}$ محققة .

تعريف الزمرة الجزئية :

لتكن $(G,.)$ زمرة و H مجموعة جزئية في G نقول عن $(H,.)$ إنها زمرة جزئية من Gإذا كانت $(H,.)$ زمرة بحد ذاتها .

مبرهنة :

لتكن $(G,.)$ زمرة و H مجموعة جزئية وغير خالية في G فإن الشروط الاتية متكافئة :

١) H زمرة جزئية في G .
٢) H تحقق الشروط الاتية :

- $\forall a,b \in H ; a.b \in H$ **(a)**
- $\forall c \in H ; \ c^{-1} \in H$ **(b)**

٣)

- $\forall\, a,b \in H\,;\, a.b^{-1} \in H$

الاثبات :

$(1 \leftarrow 2)$

لنفرض أن H زمرة جزئية عندئذ الشروط **a,b** محققة .

$(2 \leftarrow 3)$

ليكن $a,b \in H$ عندئذ $b \in H$ فإن $b^{-1} \in H$ وحسب الفرض $a,b^{-1} \in H$ وحسب الشرط a فإن $a.b^{-1} \in H$.

$(3 \leftarrow 1)$

لدينا في الفرض $H \neq \emptyset$ فهي تحوي عنصر على الأقل

- ليكن $a \in H$ وحسب الفرض $e = a.a^{-1} \in H$
- ليكن $b \in H$ اصبح لدينا $e,b \in H$ فإن : $b^{-1} = e.b^{-1} \in H$ وأن الضرب تجميعي على عناصر H
- ليكن $a,b \in H$ عندئذ $a\,,b^{-1} \in H$ ومنه حسب الفرض $a.b = a.(b^{-1})^{-1} \in H$

وهذا يبين ان الضرب عملية داخلية لـ G وواضح ان التجميعية محققة مما سبق نجد أن $(H,.)$ زمرة وبالتالي $(H,.)$ زمرة جزئية في G .

" انتهت المحاضرة "