بعض خواص الأعداد الصحيحة $\mathbb{Z}$

تعريف : ليكن $a,b\in\mathbb{Z}$ بحيث $b\neq 0$ نقول عن b إنه يقسم a إذا وجد $c\in\mathbb{Z}$ بحيث : $a=b\cdot c$

نسمي a بـ المقسوم , b المقسوم عليه , c ناتج القسمة .

القسمة ليست عملية وإنما خوارزمية .

مبرهنة , خوارزمية القسمة :

ليكن $a,b\in\mathbb{Z}$ بحيث $b>0$ عندئذٍ يوجد $q,r\in\mathbb{Z}$ بحيث :

$$a=q\cdot b+r$$

حيث $0\leq r<b$ ، زد على ذلك فإنَّ q,r يتعينان بشكل وحيد .

نسمي a بـ المقسوم , b المقسوم عليه , c ناتج القسمة , r باقي القسمة .

البرهان : لنأخذ المجموعة :

$$S=\{a-b\cdot k\geq 0\ :\ k\in\mathbb{Z}\}$$

نميز حالتين :

1 - $0\in S$ ومنه $S\neq\emptyset$ إذن يوجد $k\in\mathbb{Z}$ بحيث $a=k_0$

في هذه الحالة نختار $k_0=q$ وَ $r=0$ ويتم المطلوب .

2 - $0\notin S$ لنبرهن على أن : $S\neq\emptyset$ ونميز ثلاث حالات :

عندما $a>0$: نختار $k=0$ فيكون $a-b\cdot k=a>0$

ومنه $a=k\cdot b>0$ أي أنّ $S\neq\emptyset$.

عندما $a = 0$: نختار $k = -1$ فنجد :

$$a - k \cdot b = b > 0 \Rightarrow a - k \cdot b \in S \Rightarrow S \neq \emptyset$$

عندما $a < 0$: نختار $k = 2a$ فنجد :

$$a - k \cdot b = a - (2a) \cdot b \Rightarrow a - k \cdot b > 0 \Rightarrow S \neq \emptyset$$

وبما أن $S \subset \mathbb{N}^*$ فيوجد في S عنصر أصغر وليكن r , وبما أنّ $r \in S$ فإنّ :

$$r = a - q \cdot b \ : \ q \in \mathbb{Z}$$

وأنّ $r > 0$ ومنه : $a = q \cdot b + r$:

نفرض جدلا أنّ $r > b$ عندئذٍ

$$r - b > 0 \overset{r=a-q\cdot b}{\Rightarrow} a - q \cdot b - b > 0 \Rightarrow a - b \cdot (q + 1) > 0$$

ومنه : $r - b = a - b \cdot (q + 1) \in S$

ولكن $r - b < r$ وهذا يناقض كون r عنصر أصغر في S ومنه لا يمكن أن يكون $r > b$

لنفرض جدلاً أنّ $r = b$:

$$a - q \cdot b = b \Rightarrow a - b \cdot (q + 1) = 0$$

وهذا يناقض كون $0 \notin S$, وبما أنّ $r \neq b$ وَ $r \not> b$ يكون $r < b$

وبذلك يكون $0 < r < b$, وبدمج الحالتين معاً نجد أنّ $0 \leq r < b$.

لنبرهن الآن وحدانية q, r : لنفرض أنّ العنصر a يكتب بالشكلين :

$$a = q \cdot b + r \qquad a = q_1 \cdot b + r_1$$

$$0 \leq r < b \qquad 0 \leq r_1 < b$$

ومن جهة أخرى كل من r, r_1 أصغر من b وأولى بفرقهما أن يكون أصغر من b وهذا يبين أنّ : $r_1 - r = 0$ وبالتالي $r_1 = r$ وينتج عن ذلك $q_1 = q$.

ملاحظة : إن المبرهنة الأخيرة تعتبر صحيحة عندما $b < 0$ ويصبح النص على النحو التالي :

ليكن $a, b \in \mathbb{Z}$ بحيث $b \neq 0$ عندئذٍ يوجد $q, r \in \mathbb{Z}$ بحيث :

$$a = q \cdot b + r$$

حيث $0 \leq r < |b|$ ، زد على ذلك فإنَّ q, r يتعينان بشكل وحيد .

القاسم المشترك الأعظم :

تعريف : ليكن $a, b \neq 0$ أعداد صحيحة موجبة , نسمي أكبر عدد صحيح موجب يقسم العددين a, b بالقاسم المشترك الأعظم للعددين a, b , ونرمز لذلك بـ $gcd(a, b)$.

إذا كان $gcd(a, b) = 1$ نقول إنَّ العددين a, b أوليان نسبياً (فيما بينهما) .

مبرهنة : ليكن $a, b > 0$ أعداد صحيحة , عندئذٍ يوجد $s, t \in Z$ تحقق أنَ :

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

بالإضافة لذلك فإنَّ $gcd(a, b)$ هو أصغر عدد طبيعي من الشكل $a \cdot s + b \cdot t$

الإثبات : لنأخذ المجموعة : $S = \{n \cdot a + m \cdot b > 0 \quad n, m \in \mathbb{Z}\}$

إنَّ $S \neq \emptyset$, ومنه $S \subset \mathbb{N}$ أي S تحوي عنصر أصغر وليكن d

$$d = s \cdot a + t \cdot b \quad : s, t \in \mathbb{Z}$$

وحسب خوارزمية القسمة لعددين a, d يوجد $q, r \in \mathbb{Z}$ بحيث

$$a = q \cdot d + r \qquad 0 \leq r < d$$

لنفرض جدلا أنَ $r \neq 0$ عندئذٍ $0 < r < d$

$$r = a - q \cdot d = a - q \cdot s \cdot a - q \cdot t \cdot b$$

$$r = a \cdot (1 - q \cdot s) + (-q \cdot t)b \in S$$

r أصغر من d وها يناقض كون d عنصر أصغر في S , ومنه الفرض الجدلي خاطئ أي أنَ $r = 0$

وبالتالي : $a = q \cdot d$

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

ليكن d_0 قاسم مشترك آخر للعددين a, b عندئذٍ يوجد $h, k \in \mathbb{Z}$ بحيث :

$$a = d_0 \cdot h \qquad , \qquad b = d_0 \cdot k$$

ومنه نجد أنّ :

$$d = s \cdot a + t \cdot b = s \cdot d_0 \cdot h + t \cdot d_0 \cdot k = d_0 \cdot (s \cdot h + t \cdot k)$$

وبالتالي $d \geq d_0$ ومنه يكون d القاسم المشترك الأكبر للعددين a, b أي : $gcd(a, b) = d$

تعريف :

ليكن $p > 1$ عدد صحيح , نقول إنّ p عدد أولي إذا كانت مجموعة قواسمه $\{\pm 1, \pm p\}$

تمهيدية إقليدس : ليكن $a, b \in \mathbb{Z}$ وليكن p عدد أولي إذا كان p يقسم الجداء $a \cdot b$ فإن p يقسم a أو b

ليكن $a, b \in \mathbb{Z}$ وليكن p عدد أولي يقسم الجداء $a \cdot b$ عندئذٍ يوجد $t \in \mathbb{Z}$ بحيث : $a \cdot b = p \cdot t$

لنفرض أنّ p لايقسم a عندئذٍ :

$$gcd(a, p) = 1$$

ومنه يوجد $h, k \in \mathbb{Z}$ بحيث :

$$1 = a \cdot h + p \cdot k$$

$$b = a \cdot b \cdot h + p \cdot k \cdot b = p \cdot t \cdot h + p \cdot k \cdot b = p \cdot (t \cdot h + k \cdot b)$$

ملاحظة : في خوارزمية القسمة سنرمز لباقي القسمة r بالشكل : $r = a \bmod -b$

الزمـــــــــرة

تعريف : لتكن G مجموعة غير خالية , نسمي التطبيق :

$$\cdot : G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

عملية ثنائية على G , على سبيل المثال " جمع وضرب الأعداد ، جمع وضرب المصفوفات ،..... " .

الزمرة : وهي مجموعة غير خالية G معرف عليها عملية ثنائية.

$$\cdot : G \times G \longrightarrow G$$

$$(a,b) \longmapsto a \cdot b$$

ويحققان " أي المجموعة والعملية " معاً.

1) $\forall\, a,b \in G \;\; : a \cdot b \in G$

2) $\forall\, a,b,c \in G \;:\; (a \cdot b) \cdot c = a \cdot (b \cdot c)$ تجميعية

3) $\exists\, e \in G \;;\; \forall\, a \in G \;: a \cdot e = e \cdot a = a$ يدعى e بالمحايد

4) $\forall\, a \in G \;:\; \exists\, a^{-1} \in G \;; a \cdot a^{-1} = a^{-1} \cdot a = e$

ونقول عن الزمرة إنها تبديلية إذا حققت الشرط التالي : $\forall\, a,b \in G \;: a \cdot b = b \cdot a$

ونسمي الثنائية $(G,\cdot)$ زمرة .

أمثلة على الزمر :

زمرة الأعداد الصحيحة $\mathbb{Z}$ بالنسبة لعملية جمع الأعداد المألوفة $(\mathbb{Z},+)$ تشكل زمرة جمعية .

مجموعة المصفوفات المعرفة على الأعداد الصحيحة من المرتبة (2) بالنسبة لعملية الجمع تشكل زمرة تبديلية

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

مجموعة الأعداد المركبة بالنسبة لعملية جمع الأعداد $(\mathbb{C},+)$ تشكل زمرة جمعية .

$(\mathbb{R}^*,\cdot)$ تشكل زمرة ضربية .

المجموعة : $\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\; detA = ad - bc \neq 0 \right\}$ بالنسبة لعملية ضرب المصفوفات تشكل زمرة .

إنَّ الخصائص السابقة تتعلق بالزمرة الضربية أما الزمرة الجمعية تختلف بكل ما يأتي:

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

ملاحظة : لتكن G زمرة , $a\in G$ وَ $n\in\mathbb{Z}$:

$$a^n=\begin{cases}\overbrace{a\cdot a\cdot\ldots\cdot a}^{\text{مرة }(n)} & n>0\\ e & n=0\\ \underbrace{a^{-1}\cdot a^{-1}\cdot\ldots\cdot a^{-1}}_{\text{مرة }(-n)} & n<0\end{cases}$$

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

... انتهت المحاضرة ...