◄ دكتور المادة: حزة الحاكمي

◄ المحاضرة: الخامسة ◄ عنوان المحاضرة: المجموعات

المحتوى العلمي : أهلاً بكم أصدقائي سندرس في هذه المحاضرة :

١ـالمجموعات القابلة للعد ومبرهنات عنها.

٢ـ خوارزمية القسمة ومبرهنات عنها.

٣ـ القاسم المشترك الأعظم ومبرهنتان عنه.

تعريف المجموعات القابلة للعد: وجدنا سابقاً ان علاقة التساوي بين القدرات تعرّف لنا علاقة تكافؤ، ولنرمز لصف التكافؤ الناتج عن مجموعة الاعداد الطبيعية بالشكل $[\mathbb{N}]$ نقول عن المجموعة A انها قابلة للعد إذا كانت $A \in [\mathbb{N}]$

أي ان $A \in [\mathbb{N}] \Leftrightarrow \text{card A} = card\ \mathbb{N}$

- ينتج من التعريف ان كل مجموعة قابلة للعد هي مجموعة غير منتهية.

مبرهنة: كل مجموعة غير منتهية في $\mathbb{N}$ قابلة للعد.

البرهان:

لنفرض ان D مجموعة غير منتهية في $\mathbb{N}$ولنفرض أن a_1 هو العنصر الأصغر في D . عندئذٍ:

$D \setminus \{a_1\}$ مجموعة جزئية في $\mathbb{N}$ وغير خالية ولنفرض أن a_2 هو العنصر الأصغر فيها .

ولنفرض انه تم تعيين العنصر a_n الذي هو عنصر اصغر في المجموعة

$$D\setminus \{ a_1, a_2 \dots \dots \dots . a_{n-1}\}$$

ولنفرض ان a_{n+1} عنصر أصغر في

$$D\setminus \{ a_1, a_2 \dots \dots \dots . a_n\}$$

لنعرف العلاقة

بالشكل: $f : N^* \to D$

: $\forall\, m \in N^* \quad ; f(m) = a_m$

حيث a_m هو العنصر الأصغر في المجموعة:

$$D \backslash \{ a_1 , a_2 \ldots \ldots \ldots . a_{m-1} \}$$

وبما ان العنصر الأصغر وحيد ((هنا نربط كل a_m مع $f(m)$))

$\Leftarrow$ f تطبيق $\Leftarrow$ f متباين .

لأنه اذا كان $n , m \in \mathbb{N}^*$ حيث $f(n) = f(m) \Leftarrow a_n = a_m$

لنفرض جدلاً أن $n \neq m$ وان $n > m$ عندئذ تكون

$$\{ a_1 , a_2 , a_3 \ldots \ldots , a_{m-1} \} \subset \{ a_1 , a_2 , a_3 \ldots \ldots , a_{n-1} \}$$

ومنه تكون $D \ \backslash \{ a_1 , a_2 , a_3 \ldots \ldots , a_{n-1} \} \subset D \ \backslash \{ a_1 , a_2 , a_3 \ldots \ldots , a_{m-1} \}$

حيث $a_m \in D \ \backslash \{ a_1 , a_2 , a_3 \ldots \ldots , a_{m-1} \}$

$$a_n \in D \ \backslash \{ a_1 , a_2 , a_3 \ldots \ldots , a_{n-1} \}$$

وأن $a_n < a_m$ وهذا يتناقض كون a_m عنصر أصغر في المجموعة $D \ \backslash \{ a_1 , a_2 , a_3 \ldots \ldots , a_{m-1} \}$ مما سبق نجد ان $n = m$ اي أن f متباين .

من جهة اخرى لدينا $D \subset N^*$ عندئذ العلاقة ((تاو)) $\daleth : D \to N^*$

$$\forall x \in D ; \daleth(x) = x$$

فالعلاقة هي تطبيق متباين

وحسب مبرهنة **((كانتور – برنشتاين))** يوجد تقابل بين المجموعتين N^* و D ومنه:

$$card\ D = card\ N^*$$

ومنه D قابلة للعد.

وهو المطلوب

ملاحظة : كل مجموعة جزئية وغير منتهية من مجموعة قابلة للعد تكون أيضاً قابلة للعد

امثلة:

- ان مجموعة الاعداد الأولية هي مجموعة قابلة للعد .
- ان مجموعة الاعداد التي تقبل القسمة على 2 هي مجموعة قابلة للعد.
- كل منهما مجموعة جزئية من $\mathbb{N}$ وغير منتهية.

مبرهنة: *(وظيفة)*

كل مجموعة جزئية و غير منتهية من مجموعة قابلة للعد تكون ايضاً قابلة للعد.

البرهان

لتكن D مجموعة قابلة للعد ولتكن S مجموعة جزئية منها وغير منتهية بما أن D قابل للعد وحسب مبرهنة سابقة يوجد تقابل بينها وبين N^* وليكن $f : D \to N^*$
ولنعرف التطبيق $g: S \to D$ بالشكل $\forall a \in S \quad : \quad g(a) = a$
وهو تطبيق متباين وايضاً هذا يبين أن $fog: S \to N^*$ ايضاً متباين وبما أن المجموعة $fog(S)$ غير منتهية ومحتواة في N^* نستنتج أن المجموعة $fog(S)$ قابلة للعد ومنه S قابلة للعد .

تعريف خوارزمية القسمة

ليكن $a, b \in \mathbb{Z}$ بحيث $b \neq 0$ نقول ان b يقسم a في $\mathbb{Z}$ اذا وجد $d \in \mathbb{Z}$ بحيث $a = b.d$

ملاحظة: لنفرض ان $a = b.d$ و $a = b.d_1$

$$\Rightarrow b.d = b.d_1 \Rightarrow d = d_1$$

ومنه نجد ان d عنصر وحيد.

مبرهنة: ليكن $a, b \in Z$ بحيث $b > 0$ عندئذ يوجد $q, r \in Z$ يحققان $a = q.b + r$ حيث $0 \leq r < b$

فضلاً عن ذلك. كلاًّ من q, r يتعينان بشكل وحيد .

حيث: q ناتج القسمة و r باقي القسمة.

البرهان :

لنعرّف المجموعة : $S = \{a - k.b : k \epsilon Z \; ; \; a - k.b \geq 0\}$

١) اذا كان $0 \epsilon S$ وهنا واضح أن $S \neq \emptyset$

وبالتالي يوجد $k \epsilon Z$ بحيث $0 = a - k.b$ أي أن $a = k.b$

بطريقة علمية: $\Rightarrow \exists d \in Z \; : a - b.d = 0 \Rightarrow a = d.b$

٢) اذا كان $0 \notin S$ ((لنتأكد اذا كانت S غير خالية)).

إذا لنبرهن أن $S \neq \emptyset$ سنميز ثلاث حالات :

١) عندما $a > 0$ عندئذٍ لأجل $k = 0$ نجد ان : $a - b.k = a \in S$

٢) عندما $a < 0$ عندئذٍ لأجل $k = -2a$ نجد أن :

$$a - k.b = a - (2a.b) \in S$$

نأخذ k اختياري

٣) عندما $a = 0$ عندئذٍ لأجل $k = -1$ نجد ان :

$$a - k.b = b \in S$$

في جميع الحالات S ليست خالية.

أي إن $S \subset N$ عندئذٍ يوجد في S عنصر أصغر وليكن r حيث أن $r \epsilon S$ ومنه :

$$\exists q \epsilon Z : \quad a - q.b = r$$

أي أن : $a = q.b + r \Leftarrow r > 0$

((الأن لنبرهن على أن $r < b$)):

الحالة الاولى : لنفرض جدلاً أن $r > b$ عندئذ: $r - b > 0$ و لنأخذ :

$$a - (1 + q)b = \underbrace{a - qb}_{r} - b = \overbrace{r}^{\text{موجب}} - \overbrace{b}^{\text{موجب}} > 0$$

وايضاً $a - (1 + q)b \epsilon S$

$$a - (1 + q)b = r - b < r$$

وهذا يناقض كون r عنصر أصغر في S .

الحالة الثانية : لنفرض أن $r = b$ عندئذ:

$$a-(1+q).b = \underbrace{a-qb}_{r} - b = r - b = 0$$

$$a-(1+q)b \in S$$

لكن $0 \notin S$ وهذا تناقض.

مما سبق نجد ان $r < b$ ومنه فإن $0 \le r < b$

لنبرهن ان r, q وحيد:

ليكن $q_1, r_1 \in Z$ حيث $a = q_1.b + r_1 \ : \ 0 \le r_1 < b$

عندئذٍ: $q.b + r = q_1.b + r_1$

$$q.b - q_1.b = r_1 - r$$

$$b(q-q_1) = r_1 - r$$

لنفرض جدلاً ان $r_1 - r \neq 0$ وان $r_1 > r \Leftarrow r_1 - r \ge b$

ولدينا ايضاً ان $r_1 - r < b$

وهذا غير ممكن . ومنه $r = r_1$ وبالتالي $(q_1 - q) = 0 \Longleftarrow q_1 = q$

وهو المطلوب.

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

بحيث $a = q.b + r$ و $0 \le r < |b|$. فضلاً عن ذلك ان كلاً q, r يتعينان بشكل وحيد .

البرهان :

نميز حالتين : $b > 0$ البرهان ينتج من المبرهنة السابقة .

لنفرض $b < 0$ عندئذ $|b| > 0$ و حسب المبرهنة السابقة $\exists q_0, r \in Z$ بحيث :

$a = q_0.|b| + r$ وأن $0 \le r < |b|$ وذلك بفرض $q = -q_0$

ومنه : $a = q.b + r$: $0 < r < |b|$ ومنه q, r وحيدين

ويتم المطلوب

تعريف القاسم المشترك الأعظم: ليكن $a, b \in Z$ اعداد صحيحة مغايرة للصفر نسمي أكبر عدد صحيح موجب يقسم كل من a, b بالقاسم 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 $0 \neq a, b \in z$ اعداد صحيحة مغايرة للصفر عندئذ يوجد $s, t \in Z$ تحقق أن :

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

فضلاً عن ذلك ان $sa + tb$ هو أصغر عدد صحيح موجب لأجله يتحقق

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

الإثبات :

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

أن $S \subset N$ و $S \neq 0$ وبالتالي يوجد في S عنصر اصغر

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

وحسب خوارزمية القسمة $a = q.d + r : r, q \in Z \,; 0 \leq r < d$

حتى اثبت العدد d هو القاسم المشترك يجب ان يكون $r = 0$

لنفرض جدلا أن $r \neq 0$ عندئذ((نعوض d في a))

$$a = q(sa + bt) + r \quad = q.sa + q.tb + r$$

$$\Rightarrow 0 < r = (1 - qs)a + (-qt)b \quad \text{حيث} \quad \begin{cases} 1 - qs \\ -qt \end{cases} \in Z$$

و هذا يبين ان $r \in S$ ولما كان $r < d$ نحصل على تناقض بسبب ان d هو العنصر الأصغر في S ومنه $r = 0 \quad \Rightarrow \quad a = qd$ أي ان d يقسم a

وبطريقة مناسبة نجد ان d يقسم b

ليكن d_0 قاسم مشترك آخر للعددين a, b عندئذٍ:

$$a = d_0\ \lambda \quad \text{و} \quad b = d_0\ \mu \quad : \lambda, \mu \in Z$$

وإن

$$d = sa + tb = sd_0\ \lambda + td_0\ \mu$$

$$= d_0(s\lambda + t\mu)$$

$$\Rightarrow d \geq d_0$$

$$\Rightarrow \gcd(a,b) = d = sa + tb$$

تعريف : ليكن a عدد صحيح حيث $a > 1$ نقول ان a أولي في Z اذا كانت مجموعة قواسمه $\{ \pm 1 , \pm a \}$.

تمهيدية اقليدس : لتكن p عدد أولي و $a, b \in Z$ اعداد صحيحة إذا كان p يقسم الجداء $a.b$ عندئذ p إما يقسم a أو b .

الإثبات :

لنفرض أن p يقسم الجداء $a.b$ عندئذ يوجد عدد صحيح $t \in Z$ بحيث $a.b = t.p$ ولنفرض أن p لا يقسم a ولنبرهن أن p يقسم b .

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

$$\Rightarrow \exists\, k, S \in Z : 1 = s.a + k.p$$

$$\Rightarrow b = b.s.a + b.k.p$$

$$a.b = p.t \text{ لأن } \Rightarrow b = s.p.t + k.b.p$$

$$\Rightarrow b = (s.t + k.b)p \in Z$$

و هو المطلوب..

تم الانتهاء من اول فصل وهو المجموعات .. :)

انتهت المحاضرة

إعداد: ناريمان جلو – ولاء الأخضر – هلا هميج