المحاضرة الخامسة :

مبرهنة : كل مجموعة جزئية وغير منتهية في المجموعة $\mathbb{N}^*$ تكون قابلة للعد.

البرهان:

- لتكن $A \subset \mathbb{N}^*$ وغير منتهية (وكما نعلم أن كل مجموعة جزئية في $\mathbb{N}$ تحوي عنصر أصغر)
- ولنفرض أنّ a_1 هو العنصر الأصغر في المجموعة $A \setminus \{a_1\}$
- ولنفرض أنّ a_2 هو العنصر الأصغر في المجموعة $A \setminus \{a_1, a_2\}$
- ولنعرف التطبيق f :

$$f : \mathbb{N}^* \longrightarrow A$$

بالشكل التالي : $f(n) = a_n$

- a_n هو العنصر الأصغر في المجموعة $A \setminus \{a_1, a_2, \dots, a_{n-1}\}$
- إنّ التطبيق f متباين وغامر (وذلك حسب العنصر الأصغر) وبالتالي يكون تقابل ومنه : $\text{Card}\,\mathbb{N} = \text{card}\,A$
- وبالتالي المجموعة A قابلة للعد.

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 : $a = b.c$ ونسمي :

a : 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.

$$a = q.b + r$$

بحيث : $0 \leq r < b$ زد على ذلك فإنّ r ، q يتعينان بشكل وحيد.

الإثبات: لنأخذ المجموعة: $S=\{a-bk\geqslant 0 : k\in\mathbb{Z}\}$

نميز حالتين:

1) $0\in S$ ومنه $S\neq\emptyset$ إذن يوجد $k_0\in\mathbb{Z}$ بحيث:

$a-b.k_0=0$

ومنه: $a=b.k_0$

ومنه: b قاسم لـ a:

في هذه الحالة نختار: $k_0=q$ ، $r=0$ وتم المطلوب.

2) $0\notin S$ ومنه لنبرهن أنّ: $S\neq\emptyset$

ومنه نميز ثلاث حالات:

عندما $a>0$ نختار $k=0$ فيكون:

$a-bk=a-b.0=a>0$

$\Rightarrow a-bk>0\Rightarrow a-b.k\in S\Rightarrow S\neq\emptyset$

عندما $a=0$ نختار $k=-1$ فنجد:

$a-k.b=0-(-1).b=b>0$

$\Rightarrow a-kb>0\Rightarrow a-kb\in S\Rightarrow S\neq\emptyset$

عندما $a<0$ نختار $k=2a$ فنجد:

$a-k.b=a-(2a).b$

$\Rightarrow a-kb=\underbrace{a}_{\text{سالب}}.\underbrace{(1-2b)}_{\text{سالب}}>0$

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

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

$r=a-q.b\ ;\ q\in\mathbb{Z}$

وبالتالي:

$a=q.b+r\ ;\ r>0$

ولنبرهن أن: $r<b$

نفرض جدلاً أن $r > b$ عندئذٍ:

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

ومنه:

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

ولكن: $r - b < r$ وهذا يناقض كون r عنصر أصغري S ومنه لا يمكن أن يكون $r > b$.

لنفرض جدلاً أنّ: $r = b$ عندئذٍ:

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

وهذا يناقض كون $0 \notin S$ وبما أنّ: $r \neq b$ ؛ $r \not> b$ فإنّ: $r < b$.

وبذلك يكون: $0 < r < b$.

وبدمج الحالتين (1) و (2) يكون: $0 \leq r < b$

لنبرهن وحدانية q ، r ، لنفرض أنّ العنصر a يكتب بالشكلين

$$a = q_1.b + r_1 \qquad a = q.b + r$$
$$0 \leq r_1 < b \qquad 0 \leq r < b$$

$$q.b + r = q_1.b + r_1 \Rightarrow r_1 - r = q.b - q_1.b$$
$$\Rightarrow r_1 - r = b(q - q_1)$$

أي أن b قاسم لـ: $r_1 - r$ ومنه: $b \leq r_1 - r$

ومن جهة أخرى كل من r_1 ، r أصغر من b وأولى بفرقهما أن يكون أصغر من b أي: $r_1 - r < b$

وهذا يعني أنّ: $r_1 - r = 0 \Leftarrow r_1 = r$

وينتج عن ذلك: $q_1 = q$.

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

$$a=qb+r$$

حيث:

حيث أنّ: $0\leq r<|b|$، زد على ذلك فإنّ: q,r يتعيّنان بشكل وحيد.

الإثبات:

في المبرهنة السابقة تكون هذه المبرهنة صحيحة من أجل $b>0$.

لنفرض أن $b<0$ عندئذٍ $-b>0$ وحسب المبرهنة الأخيرة يكون.

يوجد $q_1,r\in\mathbb{Z}$ بحيث:

$$a=q_1(-b)+r \quad ; \quad 0\leq r<-b$$

$$a=-q_1 b+r=q_0 b+r \quad ; \quad q_0=-q_1$$

$$0\leq r<b,$$

القاسم المشترك الأعظم:

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

إذا كان: $gcd(a,b)=1$ نقول عندها إنّ العددين a,b أوليان نسبياً (فيما بينهما)

مبرهنة: ليكن: $a,b>0$ أعداد صحيحة، عندئذٍ يوجد $s,t\in\mathbb{Z}$

تحقق أنّ: $gcd(a,b)=a.s+b.t$

بالإضافة لذلك فإنّ $gcd(a,b)$ هو أصغر عدد طبيعي من الشكل:

$$a.s+b.t$$

الإثبات:

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

إنّ $S\neq\emptyset$، ومنه $S\subset\mathbb{N}^*$ أي أنّ S تحوي عنصر أصغر وليكن d

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

وحسب خوارزمية القسمة لعددين a , d فإنه :
يوجد $q, r \in \mathbb{Z}$ حيث
$$a = q.d + r \quad : 0 \leq r < d$$
لنفرض جدلاً أنّ $r \neq 0$ عندئذٍ : $0 < r < d$
$$r = a - q.d = a - q(s.a + t.b)$$
$$= a - q.s.a - q.t.b$$
$$\Rightarrow r = a(1 - q.s) + (-q.t).b$$
ولكن $r < d$ وهذا يناقض كون d عنصر أصغري S.
ومنه الفرض الجدلي خاطئ أي أنّ : $r = 0$.
وبالتالي : $a = q.d$
وبنفس الطريقة نثبت أنّ d يقسم b.
ومنه يكون d قاسم مشترك للعددين.

ليكن d_0 قاسم مشترك للعددين a, b عندئذٍ يوجد $h, K \in \mathbb{Z}$ بحيث :
$$a = d_0.h \quad , b = d_0.K$$
ومنه نجد أنّ :
$$d = s.a + t.b$$
$$= s.d_0.h + b.d_0.K$$
$$d = d_0(s.h + b.K)$$
ومنه نجد أنّ :
$d_0 \nmid d$ ، ومنه يكون d القاسم المشترك الأكبر
أي $gcd(a, b) = d$ للعددين a, b

تعريف: ليكن $P>1$ عدد صحيح، إنّ P عدد أولي إذا كانت مجموعة قواسمه في $\mathbb{Z}$ هي: $\{\pm 1, \pm P\}$.

تمهيدية إقليدس: ليكن $a,b\in\mathbb{Z}$ وليكن P عدد أولي، إذا كان P يقسم الجداء $a.b$ فيكون: P يقسم a أو يقسم P

البرهان:

ليكن: $a,b\in\mathbb{Z}$ وليكن P عدد أولي يقسم الجداء $a.b$ عندئذٍ

يوجد $t\in\mathbb{Z}$ بحيث: $a.b=P.t$

لنفرض أنّ P لا يقسم a عندئذٍ: $gcd(a,P)=1$.

ومنه يوجد $h,K\in\mathbb{Z}$ بحيث:

$$1=a.h+P.K$$

$$b=\underline{a.b}\,h+P.b.K$$

بضرب الطرفين بـ b ومنه:

$$=P.t.h+P.b.K=P\underbrace{(th+K.b)}_{\in\mathbb{Z}}$$

أي أنّ: P يقسم b. (فرضنا أنه لا يقسم الأول ووصلنا إلى أنه يقسم الثاني).

انتهت المحاضرة الخامسة.