Subject: 24/3/2014

« المحاضرة الخامسة »

2.2 .. مميّز الحلقة : Ring's characteristic ..

2.2.1 .. تعريف :

- لتكن $R$ حلقة ، نعرف مميّز الحلقة $R$ بأنه أصغر عدد صحيح موجب $n \in \mathbb{Z}^+$ .. بحيث يحقق :

$$\forall a \in R ; n.a = 0$$

ونرمز له بالرمز : $char(R) = n$ ..

*. ما إذا كان لا يوجد عدد صحيح $n$ يحقق : $\forall a \in R ; n.a = 0$

فإننا نصطلح أن : $char(R) = 0$ ..

*. أمثلة :

[1]. إذا كانت $R = (\mathbb{Z}, +, \cdot)$ ، فإن : $char(R) = 0$

[2]. إذا كانت $R = (\mathbb{Z}_6, \oplus, \otimes)$ ، فإن : $char(R) = 6$

2.2.1 .. مبرهنة :

- لتكن $R$ حلقة ذات عنصر محايد ، عندئذٍ :

$char(R) = n \Leftrightarrow n$ أصغر عدد صحيح موجب يحقق : $1.n = 0$

« الإثبات » .. " $\Leftarrow$ "

إن $1 \in R \Leftarrow 1.n = 0$ « بقي أن نثبت أن $n$ هو min »

- لنفرض جدلاً أن :

$$\exists m \in \mathbb{Z}^+ : 0 < m < n \wedge 1.m = 0$$

$$\Rightarrow \forall a \in R ; a.m = (a.1)m = a(1.m) = a.0 = 0$$

وهذا يناقض تعريف المميز « أي كون $n$ هو أصغر عدد في $\mathbb{Z}^+$ ويحقق أن :

$$\text{«} \ \forall a \in R ; a.n = 0$$

$\Leftarrow$ الفرض الجدلي خاطئ ، ومنه $n$ هو أصغر عدد صحيح موجب يحقق : $1.n = 0$ .. #

Subject:

$r \in \mathbb{Z}^+$ بالعودة لكون $\mathbb{Z}^+ \subset R$
$\wedge r \notin R$

"$\Longrightarrow$"

- لنفرض أن: $n$ هو أصغر عدد صحيح موجب تحقق: $1.n = 0$ ..
عندئذٍ: وحسب تعريف المميز نكون: $char(R) = n$ .. #

2.2.3 .. مبرهنة:
- إذا كانت $R$ هي $ID$، فإن: $char(R) = 0$
أو: $char(R) = P$ حيث: $P$ أولي

«الإثبات»..
- إذا كان: $char(R) = 0$ يتم المطلوب.
- لنفرض جدلاً أن: $char(R) \neq P$ ..
$\Rightarrow \exists r, s \in \mathbb{Z}^+ : 1 < r < P \wedge 1 < s < P$
حيث: « $P = r.s$ »
«وحسب المبرهنة السابقة» نجد أن: $0 = 1.P$ ..
$\Rightarrow 0 = 1.(r.s) = (1.r)(1.s)$
$\Leftarrow$ بما أن $R$ هي $ID$، أي أن $R$ خالية من القواسم الصفرية فإن:
إما $(1.r) = 0 \vee (1.s) = 0$
ولكن: $r < P \wedge s < P$ ..
مما يناقض كون $P$ هو أصغر عدد صحيح موجب يحقق: $1.P = 0$
« حسب المبرهنة السابقة »
$\Leftarrow$ تناقض $\Leftarrow$ الفرض الجدلي خاطئ $\Leftarrow char(R) = P$
حيث: $P$ عدد أولي .. #

مهمة 2.2.4 .. مبرهنة:
- لتكن $R$ منطقة تكاملية $(ID)$، عندئذٍ ما يلي صحيح:

1- إذا كان $char(R) = 0$ ، فإنه يوجد في $R$ حلقة جزئية تقابل $\mathbb{Z}$ .

2- إذا كان $char(R) = p$ ، حيث $p$ عدد أولي ، فإنه يوجد في $R$ حلقة جزئية تقابل $\mathbb{Z}_p$ ..

«الإثبات» ..

- لنعرف المجموعة : $\mathbb{Z}.1_R = \{m.1_R : m \in \mathbb{Z}\}$

عندئذٍ : $\mathbb{Z}.1_R$ حلقة جزئية في $R$ ..

1- لنعرف العلاقة : $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}.1_R$

بحيث :

$$\forall m \in \mathbb{Z} \; ; \; \varphi(m) = m.1_R$$

* $\varphi$ تطبيق لأن :

$\forall m_1, m_2 \in \mathbb{Z} : m_1 = m_2 \; ; \; m_1.1 = m_2.1 \Rightarrow \varphi(m_1) = \varphi(m_2)$ #

** $\varphi$ متباين لأن :

$\forall m_1, m_2 \in \mathbb{Z} : \varphi(m_1) = \varphi(m_2) \Rightarrow m_1.1 = m_2.1$

$\Rightarrow (m_1 - m_2).1 = 0 \Rightarrow m_1 = m_2$ #

*** $\varphi$ غامر لأن :

$\forall m.1 \in \mathbb{Z}.1_R \; ; \; \exists m \in \mathbb{Z} : \varphi(m) = m.1$ #

**** $\varphi$ تشاكل لأن :

- $\forall m_1, m_2 \in \mathbb{Z} \; ; \; \varphi(m_1.m_2) = (m_1.m_2).1 = (m_1.1).(m_2.1)$

$= \varphi(m_1).\varphi(m_2)$

- $\forall m_1, m_2 \in \mathbb{Z} \; ; \; \varphi(m_1 + m_2) = (m_1 + m_2).1 = (m_1.1) + (m_2.1)$

$= \varphi(m_1) + \varphi(m_2)$ #.

$\Leftarrow$ $\varphi$ تقابل $\Leftarrow$ $\mathbb{Z} \simeq \mathbb{Z}.1_R$

$: \mathbb{Z}.1_R \leq R$ #

$\boxed{2}$ ـ لنعرف العلاقة : $\varphi : \mathbb{Z}_p \longrightarrow \mathbb{Z}.1_R$

بحيث :

$$\forall m \in \mathbb{Z}_p \; ; \; \varphi(m) = m.1_R$$

* ـ $\varphi$ تطبيق لأن :

$$\forall m_1, m_2 \in \mathbb{Z}_p : m_1 = m_2 \Rightarrow m_1.1 = m_2.1$$
$$\Rightarrow \varphi(m_1) = \varphi(m_2) \quad \#$$

** ـ $\varphi$ تشاكل لأن :

$\forall m_1, m_2 \in \mathbb{Z}_p$ ؛

1)- $\varphi(m_1 + m_2) = (m_1 + m_2).1 = (m_1.1) + (m_2.1)$
$= \varphi(m_1) + \varphi(m_2)$

2)- $\varphi(m_1 . m_2) = (m_1 . m_2).1 = (m_1.1).(m_2.\cancel{m}1)$
$= \varphi(m_1).\varphi(m_2) \quad \#$

✓ *** ـ $\varphi$ متباين لأن :

$$\forall m_1, m_2 \in \mathbb{Z}_p : \varphi(m_1) = \varphi(m_2) \Rightarrow m_1.1 = m_2.1$$
$$\Rightarrow (m_1 - m_2).1 = 0$$
$$\Rightarrow m_1 = m_2 \rightarrow \underline{\underline{in\, \mathbb{Z}}}$$

ـ ولإثبات ذلك في $\mathbb{Z}_p$ نقوم بما يلي :

ـ حسب خوارزمية القسمة لأجل العددين $(m_1 - m_2) \wedge p$ فإنه :

ـ بما أن R هي ID فهي خالية من قواسم الصفر ← لابد من أن يكون $(m_1 - m_2) = 0$

$$\exists r, ك \in \mathbb{Z} : (m_1 - m_2) = ك.p + r \quad : \quad 0 \leq r < p$$

ـ لنفرض جدلاً أن $(r \neq 0)$ ..

$$\Rightarrow 0 = (m_1 - m_2).1 = ك.p + r = ك.(\underbrace{p.1}_{0}) + r$$

$$\Rightarrow 0 = ك.0 + r = 0 + (r.1) \Rightarrow (r.1) = 0 \Rightarrow \boxed{r = 0}$$

حسب ... ID ... $\mathbb{Z}_p$

$char(R) = p$

فرضاً

⇐ تناقض ⇐ الفرض الجدلي خاطئ ⇐ «$r = 0$»

$$\Rightarrow m_1 - m_2 = s.p \Rightarrow (m_1 - m_2) = s.(p.1) = 0$$
$$\Rightarrow m_1 = m_2 \longrightarrow \text{in } \mathbb{Z}_p$$
$\Rightarrow$ تم المطلوب #

**. $\varphi$ غامر لأن:

$$\forall m.1 \in \mathbb{Z}.1_R \ ; \ \exists m \in \mathbb{Z}_p : \varphi(m) = m.1 \quad \#$$

$$\Rightarrow (S = \mathrm{Im}\,\varphi) \leqslant \mathbb{Z}.1_R \leqslant R$$
$$\wedge \ \mathbb{Z}.1_R \cong \mathbb{Z}_p$$

#

5.2.2. مبرهنة:

- لتكن $R$ حقل، عندئذٍ:

1- إذا كان $char(R) = 0$، فإنه يوجد ضمن $R$ حقل جزئي يماثل $Q$.

2- إذا كان $char(R) = p$، حيث: $p$ عدد أولي، فإنه يوجد ضمن $R$ حقل جزئي يماثل $\mathbb{Z}_p$.

«الإثبات»:

1- (لأن $char(R)=0 \wedge n \neq 0$ أيضاً)

$$\forall n \neq 0 : n \in \mathbb{Z} \ ; \ n.1 \neq 0 \in R \Rightarrow$$
$$n.1 \in U(R)$$ ← «لأن كل عنصر $\neq 0$ له معكوس»

- عندئذٍ يستطيع أن نعرف المجموعة:

$$E = \left\{ \frac{m.1}{n.1} : m, n \in \mathbb{Z} \wedge n \neq 0 \right\} \longrightarrow$$ $E$ حقل جزئي من $R$

- بعبارة أخرى : $E = \{ (m.1).(n.1)^{-1} : m, n \in \mathbb{Z} \wedge n \neq 0 \}$

ولنعرف العلاقة : $\varphi : Q \longrightarrow E$

بحيث :

$$\forall \frac{m}{n} \in Q \; ; \; \varphi\left(\frac{m}{n}\right) = \frac{m.1}{n.1}$$ $\longrightarrow$ « لا داعي لذكر أن $n \neq 0$ لأنه من تعريف عناصر $Q$ - $n \neq 0$ - »

- $\varphi$ تطبيق لأن :

$$\forall \frac{m_1}{n_1}, \frac{m_2}{n_2} \in Q : \frac{m_1}{n_1} = \frac{m_2}{n_2} \; ; \; \frac{m_1.1}{n_1.1} = \frac{m_2.1}{n_2.1}$$

$$\Rightarrow \varphi\left(\frac{m_1}{n_1}\right) = \varphi\left(\frac{m_2}{n_2}\right) \quad \#$$

- $\varphi$ تشاكل لأن :

$$*) - \varphi\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) = \varphi\left(\frac{m_1.n_2 + m_2.n_1}{n_1.n_2}\right) = \frac{(m_1.n_2 + m_2.n_1).1}{(n_1.n_2).1}$$

$$= \frac{(m_1 n_2).1 + (m_2.n_1).1}{(n_1.n_2).1} = \frac{(m_1 n_2).1}{(n_1.n_2).1} + \frac{(m_2.n_1).1}{(n_1.n_2).1}$$

$$= \frac{m_1.1}{n_1.1} + \frac{m_2.1}{n_2.1} = \varphi\left(\frac{m_1}{n_1}\right) + \varphi\left(\frac{m_2}{n_2}\right)$$

$$**) - \varphi\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) = \varphi\left(\frac{m_1.m_2}{n_1.n_2}\right) = \frac{(m_1.m_2).1}{(n_1.n_2).1}$$

$$= \frac{m_1.1}{n_1.1} \cdot \frac{m_2.1}{n_2.1} = \varphi\left(\frac{m_1}{n_1}\right) \cdot \varphi\left(\frac{m_2}{n_2}\right) \quad \#$$

- $\varphi$ متباين لأن :

$$\forall \frac{m_1}{n_1}, \frac{m_2}{n_2} \in Q : \varphi\left(\frac{m_1}{n_1}\right) = \varphi\left(\frac{m_2}{n_2}\right) \Rightarrow \frac{m_1.1}{n_1.1} = \frac{m_2.1}{n_2.1}$$

$$\Rightarrow (m_1.n_2).1 = (m_2.n_1).1 \Rightarrow (m_1.n_2 - m_2.n_1).1 = 0$$

Subject:

$$\Rightarrow m_1 \cdot n_2 = m_2 \cdot n_1 \Rightarrow \frac{m_1}{n_1} = \frac{m_2}{n_2} \qquad \#$$

- $\varphi$ غامر لأن :

$$\forall \frac{m \cdot 1}{n \cdot 1} \in E \; ; \; \exists \frac{m}{n} \in Q : \varphi\left(\frac{m}{n}\right) = \frac{m \cdot 1}{n \cdot 1} \qquad \#$$

$$\Rightarrow E \cong Q \quad \wedge \; E \overset{\text{déf}}{\leq} R .$$

النتيجة الجاهزة

$\#$