Subject:

29/4/2014

«المحاضرة الثانية عشرة»

6-5. مبرهنة:

- لتكن R هي ID ، عندئذٍ ما يلي من قضايا هو صحيح:

$\boxed{1}$ - $R\{x\}$ هي ID ..

$\boxed{2}$ - $U(R) = U(R\{x\})$ ..

$\boxed{3}$ - r غير قابل للتحليل في R $\Leftarrow$ r غير قابل للتحليل في $R\{x\}$ ..

$\boxed{4}$ - r عنصر أولي في R $\Leftarrow$ r عنصر أولي في $R\{x\}$ ..

«الإثبات» ..

$\boxed{1}$ - «تعريف سابق».

$\boxed{2}$ - «$U(R) \subseteq U(R\{x\})$» لأن:

$$\forall r \in U(R) ; \exists a \in R \subseteq R\{x\} : a.r = 1 \Rightarrow r \in U(R\{x\})$$

كذلك: «$U(R\{x\}) \subseteq U(R)$» لأن:

$$\forall f \in U(R\{x\}) ; \exists g \in R\{x\} : f.g = 1 \Rightarrow$$ (لأن R هي ID)

فإن: $deg(f) = deg(g) = 0 \Leftarrow deg(f) + deg(g) = 0$

وعليه «$f.g=1$» $\Leftarrow f \in U(R)$

ومن الاحتواءين ينتج: $U(R) = U(R\{x\})$ ..

#

$\boxed{3}$ - (r عنصر غير قابل للتحليل في R) .. أي أن:

$r \notin U(R) = U(R\{x\})$ ، $r \neq 0$ ، وليكن:

$$f, g \in R\{x\} : r = f.g$$

$$0 = deg(f) + deg(g) \Rightarrow f, g \in R$$

ولكن: «$r = f.g$» وإن r غير قابل للتحليل في R .. عندئذٍ:

$$\left\{ \begin{array}{l} f \in U(R) = U(R\{x\}) \\ g \in U(R) = U(R\{x\}) \end{array} \right\} \Rightarrow$$ r غير قابل للتحليل في $R\{x\}$

#

Subject:

[14] - (r عنصر أولي في R) .. أي أن:

$0 \neq r \notin U(R) = U(R\{x\})$ ، ولكن:

$r \mid f.g$: $f, g \in R\{x\}$

حيث:

$f = \sum_{i=0}^{n} a_i . x^i \;\wedge\; g = \sum_{j=0}^{m} b_j . x^j$

$\Rightarrow f.g = \sum_{k=0}^{n+m} c_k . x^k \quad , \sum_{i+j=k} a_i . b_j = c_k$

عندئذٍ:

$r \mid f.g \Rightarrow \forall k \in \{0, 1, \dots, n+m\} \; ; r \mid c_k$

★- نفرض جدلاً أن: $\underset{\text{لا تقسم}}{r \nmid g}$ ، $\underset{\text{لا تقسم}}{r \nmid f}$ .. وبالتالي:

ليكن j_0 أصغر عدد صحيح موجب يحقق: $r \nmid b_{j_0}$

وليكن i_0 أصغر عدد صحيح موجب يحقق: $r \nmid a_{i_0}$

$\Leftarrow \quad r \nmid a_{i_0} . b_{j_0}$ «لأن r عنصر أولي» .

ومنه نوجد: «$k_0 = i_0 + j_0$» يحقق: $r \nmid c_{k_0}$ ، ولنبيّن ذلك

نفرض جدلاً أن: «$r \mid c_{k_0}$» ..

$\Rightarrow c_{k_0} = a_0 b_{k_0} + a_1 b_{k_0 - 1} + \dots + a_{i_0} . b_{j_0} + \dots + a_{k_0} b_0$

$\Rightarrow \underbrace{c_{k_0}}_{r \text{ تقسم}} - (\underbrace{a_0 b_{k_0} + \dots + a_{i_0} b_{j_0} + a_{i_0 - 1} b_{j_0 + 1} + a_{i_0 + 1} b_{j_0 - 1} + \dots + a_{k_0} b_0}_{r \text{ تقسم}}) = \underbrace{a_{i_0} b_{j_0}}_{r \text{ لا تقسم}}$

لا يمكن أن تقسم على r

هذا تناقض كون: «$r \nmid a_{i_0} b_{j_0}$» ، ومنه «$r \nmid c_{k_0}$»

وهنا تناقض كون: $\forall k \in \{0, 1, \dots, n+m\} \; ; r \mid c_k$

وبالتالي الفرض الجدلي خاطئ ، أي أن : $r\mid f$ أو $r\mid g$)
ومنه يكون r عنصر أولي في $R[x]$.

#

5-7. مبرهنة :

- لتكن R هي ID ، عندئذ القضايا التالية صحيحة :

1- R هي UFD ..

2- إذا كان $0\neq r\in R/U(R)$ فإن : $r=\prod_{i=1}^{n} p_i$
«حيث p_i عنصر غير قابل للتحليل» و كل عنصر غير قابل للتحليل في R هو عنصر أولي.

3- إذا كان $0\neq r\in R/U(R)$ فإن : r يكتب كجداء منتهي (لعناصر غير قابلة للتحليل في R) بشكل وحيد ، أي :

$$\left.\begin{array}{l} r=\prod_{i=1}^{k} p_i \\ r=\prod_{j=1}^{l} q_j \end{array}\right\} \Rightarrow \begin{cases} k=l \\ \forall i\in\{1,\dots,k\} \;;\; \exists j\in\{1,\dots,l\} \\ p_i=u\cdot q_j \;:\; u\in U(R) \end{cases}$$

أي أن : p_i , q_j مترادفان .

«الإثبات» .. «تقبل دون إثبات» .

5-8. تعريف :

- لتكن R هي UFD و $a_1,a_2,\dots,a_n\in R\setminus\{0\}$ ، عندئذ :

* $g\in R$ قاسم مشترك أعظم للعناصر $a_1,\dots,a_n$ .. إذا كانت :

1)- $g\mid a_i \;:\; \forall i\in\{1,\dots,n\}$

2)- $t\in R \,,\, t\mid a_i \;:\; \forall i\in\{1,\dots,n\} \Rightarrow t\mid g$

ونرمز لذلك بالرمز :

$g=\gcd(a_1,a_2,\dots,a_n)$

Greatest common divisor

Subject:

تعريف: $\mathcal{L} \in R$ مضاعف مشترك أصغر للعناصر $a_1, a_2, \ldots, a_n$ ، إذا تحقق:

1)- $a_i | \mathcal{L} \quad : \forall i \in \{1, \ldots, n\}$

2)- $t \in R \ , \ a_i | t \ : \forall i \in \{1, \ldots, n\} \Rightarrow \mathcal{L} | t$

ونرمز لذلك بالرمز:

$\mathcal{L} = \mathcal{L}cm(a_1, \ldots, a_n)$ Least common multiplication

- أمثلة:

[1]- $R = (\mathbb{Z}_{12}, \oplus, \otimes)$ ، $a = 6 \wedge b = 8$

$\mathcal{L}cm(a, b) = ؟؟؟$

[2]- $R = (\mathbb{Z}(\sqrt{-3}), +, \cdot)$ ، $a = -2 + 2\sqrt{-3} \wedge b = 4$

$gcd(a, b) = ؟؟؟$

- تمرين: - مرفقة -

- لتكن R حلقة تبديلية واحدية ، عندئذٍ:

[1]- بين أنه ليس بالضرورة أن يكون لأي مجموعة منتهية من عناصر R قاسم مشترك أعظم (مضاعف مشترك أصغر).

[2]- إذا كانت R هي PID ، فإن أي مجموعة منتهية $\{a_1, \ldots, a_n\} \in R$ من عناصر R لها قاسم مشترك أعظم $g \in R$ يكتب بالشكل:

$g \wedge r_i \in R \ : \ « g = \sum_{i=1}^{n} r_i \cdot a_i »$

حل: تتعلق بالمبرهنة 5-و

- 5 - و - مبرهنة:

- لتكن R حلقة تبديلية واحدية ، ولتكن $\{a_1, \ldots, a_n\} \in R$ عندئذٍ ، فإن

[1]- $g \in R$ هو قاسم مشترك أعظم للعناصر $a_1, \ldots, a_n$ بحيث:

$g = \sum_{i=1}^{n} r_i \cdot a_i \quad : r_i \in R$

Subject:

إذا وفقط إذا كان المثالي : $\langle g \rangle = \langle a_1, a_2, \dots, a_n \rangle$ رئيسياً

$\boxed{2}$ - يكون ، $\ell = lcm(a_1, \dots, a_n) \in R$

إذا وفقط إذا تحقق :

$$\langle \ell \rangle = \bigcap_{i=1}^{n} \langle a_i \rangle$$

«الإثبات»

$\boxed{1}$ - « $\Leftarrow$ »

- لدينا $g = gcd(a_1, \dots, a_n)$ ، وهذا يعني أن :

$$g \mid a_i : \forall i \in \{1, \dots, n\} \Rightarrow \forall i \in \{1, \dots, n\} ; \langle a_i \rangle \subseteq \langle g \rangle$$
$$\Rightarrow \langle a_1, a_2, \dots, a_n \rangle \subseteq \langle g \rangle$$

- ومن جهة ثانية لدينا :

$$g = \sum_{i=1}^{n} r_i \cdot a_i \Rightarrow g \in \langle a_1, \dots, a_n \rangle \Rightarrow \langle g \rangle \subseteq \langle a_1, \dots, a_n \rangle$$

ومن الاحتواءين ينتج أن :

$$\langle g \rangle = \langle a_1, a_2, \dots, a_n \rangle$$

#

« $\Rightarrow$ »

- لدينا $g \in \langle g \rangle = \langle a_1, a_2, \dots, a_n \rangle$ ، وذلك يعني أن :

$$\forall i \in \{1, 2, \dots, n\} ; a_i \in \langle g \rangle = \langle a_1, a_2, \dots, a_n \rangle$$
$$\Rightarrow \forall i \in \{1, 2, \dots, n\} ; g \mid a_i$$

ولكن لدينا أيضاً :

$$t \in R : t \mid a_i : \forall i \in \{1, \dots, n\}$$
$$\Rightarrow \langle a_1, \dots, a_n \rangle \subseteq \langle t \rangle \Rightarrow g \in \langle t \rangle \Rightarrow t \mid g$$
$$\Rightarrow g = gcd(a_1, \dots, a_n)$$

#

$\boxed{2}$ - « $\Leftarrow$ »

- لدينا : $\ell = lcm(a_1, \dots, a_n)$ ، أي أن :

Alamal Notebook

$$\forall i\in\{1,\dots,n\}\ ;\ a_i \mid \ell \Rightarrow \forall i\in\{1,\dots,n\}\ ;\ \langle \ell\rangle \subseteq \langle a_i\rangle$$

$$\Rightarrow \langle \ell\rangle \subseteq \bigcap_{i=1}^{n} \langle a_i\rangle$$

وبالعكس :

$$\forall x\in \bigcap_{i=1}^{n}\langle a_i\rangle \Rightarrow \forall i\in\{1,\dots,n\}\ ;\ a_i\mid x$$

$$\Rightarrow \ell\mid x \Rightarrow x\in\langle\ell\rangle \Rightarrow \bigcap_{i=1}^{n} \langle a_i\rangle\subseteq\langle \ell\rangle$$

ومنه : $\langle\ell\rangle = \bigcap_{i=1}^{n}\langle a_i\rangle$

#

«$\Longrightarrow$»

لدينا : $\langle \ell\rangle=\bigcap_{i=1}^{n}\langle a_i\rangle$

$$\Rightarrow \forall i\in\{1,\dots,n\}\ ;\ a_i\mid \ell$$

ليكن $\Rightarrow t\in\langle a_i\rangle : \forall i\in\{1,\dots,n\} \Rightarrow t\in\bigcap_{i=1}^{n}\langle a_i\rangle=\langle\ell\rangle$

$$\Rightarrow \ell\mid t$$

ومنه ينتج أن : $\ell = \mathrm{lcm}(a_1,\dots,a_n)$

#

تعريف : ـ ملاحظة ـ

ـ إذا كانت R هي « PID » ، فإن :

$\boxed{1}$ ـ كل سلسلة متزايدة من المثاليات في R ($I_1\subseteq I_2\subseteq \dots$) تتقطع أي أن :

$$\exists i\in\mathbb{N} : \forall j\geq i\ ;\ I_i = I_j$$

$\boxed{2}$ ـ أي مثالي $I \trianglelefteq R$ ، $\neq\langle 0\rangle$ ، يكتب على شكل جداء منتهي لمثاليات أولية في R ، أي :

$$I=\prod_{i=1}^{n} P_i \ :\ P_i\in \mathrm{Spec}(R)$$

lcm ← نأخذ العناصر المشتركة والغير مشتركة بأكبر أس . } سيصاغ هذا الكلام في البرهنة
gcd ← نأخذ العناصر المشتركة فقط بأصغر أس .

Subject:

10 - 5 - مبرهنة :

- إذا كانت R هي UFD ، فإن أي عنصرين : $a, b \in R / \{0\}$
يكون لهما قاسم مشترك أعظم و مضاعف مشترك أصغر في R .

« الإثبات » :

- بما أن R هي UFD ، فإن :

$$a = \prod_{i=1}^{n} P_i^{\alpha_i} \quad : \quad P_i \text{ عناصر أولية}$$

$$b = \prod_{j=1}^{m} q_j^{\beta_j} \quad : \quad q_j \text{ عناصر أولية}$$

فيكون القاسم المشترك الأعظم لهما هو :

$$g = gcd(a, b) = \prod_{k=1}^{t} \eta_k^{\gamma_k} \quad :$$

$$\exists i \in \{1, \dots, n\} \wedge \exists j \in \{1, \dots, m\} : \eta_k = P_i = q_j \quad \wedge$$

$$\gamma_k = \min\{\alpha_i, \beta_j\} \quad \text{« العناصر المشتركة بأصغر أس »}$$

و يكون المضاعف المشترك الأصغر لهما هو :

$$l = lcm(a, b) = \prod_{k=1}^{\cancel{s}\,t} \eta_k^{\gamma_k}$$

حيث أن : η_k سيكون لها إحدى القيم التالية :

1) - $\exists i \in \{1, \dots, n\} \wedge j \in \{1, \dots, m\}$:

$$\eta_k = P_i = q_j \quad \wedge \quad \gamma_k = \max\{\alpha_i, \beta_j\}$$

2) - $\exists i \in \{1, \dots, n\} : \forall j \in \{1, \dots, m\}$;

$$\eta_k = P_i \neq q_j \quad \wedge \quad \gamma_k = \alpha_i$$

Subject:

3) - $\forall i \in \{1, \dots, n\} ; \exists j \in \{1, \dots, m\}$:

$$m_k = q_j \neq p_i \wedge \gamma_k = \beta_j$$

#

//