الأحد: 2015/5/17 — المحاضرة 16

ملاحظة:

إذا كانت $\mathbb{R}$ هي UFD "وحيدة التحليل" فإن لأي مجموعة منتهية من العناصر الغير صفرية في $\mathbb{R}$ يكون لها قاسم مشترك أعظم ومضاعف مشترك أصغر.

مبرهنة:

لتكن $\mathbb{R}$ حلقة تبديلية (موسعة أحادية أولاً) لتكن $a_1, a_2, \dots, a_n \in \mathbb{R}$ عناصر غير صفرية

إن القضايا التالية صحيحة:

1. $g = \gcd(a_1, a_2, \dots, a_n) \in \mathbb{R}$ وليكن $\exists r_1, r_2, \dots, r_n \in \mathbb{R}$

وتحقق: $g = \sum_{i=1}^{n} r_i a_i$

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

2. إن $g = \gcd(a_1, a_2, \dots, a_n) \in \mathbb{R}$ $\quad l = \operatorname{lcm}(a_1, a_2, \dots, a_n) \in \mathbb{R}$

$\longleftrightarrow$ تحقق: $\langle l \rangle = \bigcap_{i=1}^{n} \langle a_i \rangle$

الإثبات:

رقم 1 $\longleftarrow$

$\rightarrow \ g \mid a_i \ : \forall i \in \{1, \dots, n\}$ (الاحتواء الأول)

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

$\exists r_1, \dots, r_n \in \mathbb{R} \ : g = \sum_{i=1}^{n} r_i a_i \in \langle a_1, a_2, \dots, a_n \rangle$ (الاحتواء العكسي)

$\rightarrow \langle g \rangle \subseteq \langle a_1, \dots, a_n \rangle$

ومنه: $\langle g \rangle = \langle a_1, \dots, a_n \rangle$

$\rightarrow \ \forall i \in \{1, \dots, n\} : a_i \in \langle a_1, \dots, a_n \rangle = \langle g \rangle \ \rightarrow$

$\rightarrow \forall i \in \{1, \dots, n\} \ : g \mid a_i$ ؛

$\rightarrow \exists t \in \mathbb{R}$ ؛ $t \mid a_i \quad \forall i \in \{1, \dots, n\}$

من ثبت أن t يقسم g ،

$\rightarrow \forall i \in \{1,2,\dots,n\} \quad : a_i \in \langle t \rangle$

$\rightarrow \langle g \rangle = \langle a_1, a_2, \dots, a_n \rangle \subseteq \langle t \rangle$

$\rightarrow t \mid g$

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

$\forall i \in \{1,\dots,n\} \quad : a_i \mid f$ ← رقم 2

$\rightarrow f \in \langle a_i \rangle \quad \forall i \in \{1,\dots,n\}$

$\rightarrow f \in \bigcap_{i=1}^{n} \langle a_i \rangle$

(الاحتواء الأول) $\rightarrow \langle f \rangle \subseteq \bigcap_{i=1}^{n} \langle a_i \rangle$

$\forall x \in \bigcap_{i=1}^{n} \langle a_i \rangle \longrightarrow x \in \langle a_i \rangle$

$\forall i \in \{1,2,\dots,n\} \longrightarrow a_i \mid x$

$\forall i \in \{1,2,\dots,n\} \longrightarrow f \mid x$

$\rightarrow x \in \langle f \rangle$

(الاحتواء المعاكس) $\rightarrow \bigcap_{i=1}^{n} \langle a_i \rangle \subseteq \langle f \rangle$

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

$\rightarrow f \in \langle a_i \rangle \;, \forall i \in \{1,2,\dots,n\}$ ←

$\rightarrow a_i \mid f \quad \forall i \in \{1,2,\dots,n\}$

$t \in \mathbb{R} \quad ; a_i \mid t \qquad \forall i \in \{1,\dots,n\}$

$\rightarrow t \in \langle a_i \rangle \qquad \forall i \in \{1,2,\dots,n\}$

$\rightarrow t \in \bigcap_{i=1}^{n} \langle a_i \rangle = \langle f \rangle$

$\rightarrow f \mid t.$

برهنة:

لتكن $\mathbb{R}$ حلقة واحدية غير تبديلية:

1- $\mathbb{R}$ Id في $\longleftrightarrow$ $\mathbb{R}[x]$ Id في

2- $\mathcal{U}(\mathbb{R}) = \mathcal{U}(\mathbb{R}[x])$

3- $r \in \mathbb{R}$ غير قابلة للتحليل في $\mathbb{R}$ $\leftarrow$ r غير قابلة للتحليل في $\mathbb{R}[x]$

4- $p \in \mathbb{R}$ أولي في $\mathbb{R}$ $\leftarrow$ p عنصر أولي في $R[x]$

إمكانية (٢-٣-٤) Id بيناني (١) غير ضرورية.

الإثبات:

رقم (٢):

(الاتجاه الأول)

$$r \in \mathcal{U}(\mathbb{R}) \rightarrow \exists b \in \mathbb{R} : b.r = 1$$

$$r \in \mathbb{R} \subseteq \mathbb{R}[x] \ , \exists b \in \mathbb{R} \subseteq \mathbb{R}[x]$$

$$r.b = 1 \rightarrow r \in \mathcal{U}(\mathbb{R}[x])$$

(الاتجاه المعاكس)

$$\forall f \in \mathcal{U}(R[x]) : \exists g \in \mathbb{R}[x] \ , \ f.g = 1$$

(Id في $\mathbb{R}[x], \mathbb{R}$ مقبولة كي في العلاقة

$$\deg(f.g) = \deg(1) = 0.$$

(= لـ

$$\rightarrow \deg(f) + \deg(g) = 0.$$

$$\rightarrow \deg(f) = \deg(g)$$

باقي البرهنة

$$\rightarrow f.g \in \mathbb{R} \ , \ f.g = 1$$

غير مطلوب

$$\rightarrow f \in \mathcal{U}(R)$$

عندنا حالتين:

- الحالة الأولى:

f غير قابلة للتحليل في $R[x]$

كما أن $d \in \mathbb{R}$ و $\mathbb{R}$ هي UFD

تمهيدية غاوس (Gauss's lemma) (سيتم ذكر اسم المبرهنة في الامتحان لا نصها)

إذا كان R هي UFD فإن $R[x]$ هي UFD

"ومعناها: R حلقة وحيدة التحليل فإن حلقة الحدوديات وحيدة التحليل"

الإثبات:

ليكن $0 \neq f(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus U(R)$

$U(R) = U(R[x])$ حسب مبرهنة سابقة

- سنثبت أن هذه الحدودية تكتب على شكل جداء منتهي لعناصر غير قابلة التحليل في $R[x]$

وذلك بالاستقراء الرياضي على درجة الحدودية على $[n]$

- ليكن $d = \gcd(a_1, \dots, a_n) \in R$ موجودة حسب مبرهنة سابقة.

← نعرف $a_i' = \frac{a_i}{d} \in R$ $\forall i \in \{0, 1, 2, \dots, n\}$ $\frac{a_i}{d} \in R$ يقبل القسمة

$f = d \cdot f'$

$f'(x) = \sum_{i=0}^{n} a_i' x^i \in R[x]$

- يتم الإثبات بالاستقراء الرياضي:

← $n = 0$ الحدودية الثابتة

$f \in R$ - بما أن R حلقة تحليل وحيد يمكن كتابة f على شكل جداء منتهي لعناصر

غير قابلة للتحليل في $R[x]$ حسب مبرهنة سابقة.

← نفرض أن كل الحدوديات درجتها أصغر من n معرفة على R تكتب على شكل جداء منتهي

من العناصر الغير قابلة للتحليل في $R[x]$

← ولنبرهن صحتها من أجل حدودية f درجتها n

نميز حالتين:

- الحالة الأولى:

f' غير قابلة للتحليل في $R[x]$

كما أن $d \in R$ و R هي UFD

غير قابلة للتحليل p_i $d = \prod_{i=1}^{t} p_i$ تكتب على شكل جداء منتهي من العناصر الغير قابلة للتحليل.

$f = d \cdot f' = \left(\prod_{i=1}^{t} p_i\right) f'$

وبالتالي تكون f جداء منتهي لعناصر غير قابلة للتحليل في $R[x]$

الحالة الثانية:

f' قابلة للتحليل في $R[x]$

منه يوجد: $\exists h, g \in R[x] \setminus U(R) = U(R[x])$ مثال:

تحقق: $f' = h.g$ $f' = 2x^2+6$

$\underbrace{2}_{h}\underbrace{(x^2+3)}_{g}$

نفرض جدلاً: $\deg(h)=0$ $h \in R$ (عدد ثابتة)

$\to h \mid a_i' \quad \forall i \in \{1, \dots, n\}$

$\to h \mid \gcd(a_0', a_1', \dots, a_n') = 1$ (لأنه f' بدائية الأمثال)

$\to h \in U(R)$

وهذا تناقض، ومنه الفرض الجدلي خاطئ. ($h \notin U(R)$)

$\deg(g) \neq 0 \quad \deg(h) \neq 0$

ومنه: $0 < \deg(h) < n \quad 0 < \deg(g) < n$

حسب الفرض الاستقرائي:

$h = \prod_{i=1}^{m} s_i(x) \quad g = \prod_{i=m+1}^{k} s_i(x)$

حيث $s_i(x)$ غير قابلة للتحليل في $R[x]$ $\forall i \in [1, \dots, k]$

كما أن: $d \in R$

$d = \prod_{i=1}^{t} p_i$

p_i: غير قابلة للتحليل في $R[x]$ $\forall i \in [1, \dots, t]$

$f = d.f' = d.h.g = (\prod_{i=1}^{t} p_i)(\prod_{i=1}^{k} s_i(x))$

- وبالتالي تكون حلقة الحدوديات $R[x]$ هي UFD

نتيجة:

إذا كانت R هي UFD فإن $R[x_1, x_2, \dots, x_n]$ هي UFD

UFD $R[x_1][x_2]$ $\longleftarrow$ $R[x_1]$ UFD حسب نظرية غاوس.

ومنه، .... $R[x_1, x_2]$

$ED \rightarrow PID \rightarrow UFD$ (ولكن بالاتجاه المعاكس ليس بالضرورة صحيح).

في أحد الدورات لسنوات سابقة:

كان السؤال: $R = (\mathbb{Z}, +, \cdot)$ أثبت انه $\mathbb{Z}$ إقليدية ثم بين هي ED

بين انه $\mathbb{Z}$ هي UFD ثم بين $\mathbb{Z}[x]$ هي UFD

أثبت $\mathbb{Z}$ حلقة نوثرية ، $\mathbb{Z}[x]$ مونوثرية.؟

الحل:

سابقاً تم إثبات انه $\mathbb{Z}$ هي ED وحسب العلاقة السابقة $\mathbb{Z}$ هي PID

$$ED \longrightarrow PID \longrightarrow UFD$$

حسب تمهيدية غاوس.

$\mathbb{Z}[x]$ هي UFD

هل $\mathbb{Z}[x]$ إقليدية.؟

لا (مثال معاكس) $g = x^2 \quad f(x) = 2x+1 \in \mathbb{Z}[x]$

$\nexists\, q, r \in \mathbb{Z}[x]$ ف $g = qf + r$

حيث، $r = 0 \;\vee\; \deg(r) < 1$

وبالتالي $\mathbb{Z}[x]$ ليست Ed وليست منطقة مثاليات رئيسة.

لأن: $\mathbb{Z}[x]$ هي $UFD \leftarrow \mathbb{Z}[x, y]$ هي UFD

(تمهيدية غاوس)

لكن $\mathbb{Z}[x, y]$ ليست PId

$I = \langle x, y \rangle \trianglelefteq \mathbb{Z}[x, y]$

مثال (على انه العكس صحيح)

$UFD \leftarrow PID$

ولكن العكس صحيح عندما $0 \neq a, b \in R$

$\langle a, b \rangle = \langle g \rangle$

سؤال أولمبياد:

ما حلول هذه المعادلة. $x^2+2=y^3$ $\quad x,y\in \mathbb{Z}^+$

$13=2^2+3^2$, $5=2^2+1$, $17=4^2+1$

حسب نظرية فيرما الوسطى:

اذا ما وجد عددان n,m صحيحان ويوجد عدد يكتب على شكل n^2+m^2

فيكون عدد أولي:

مثال: $1001=(100)^2+1$ ـ اولي.

R حقل $\longleftrightarrow$ $R[x]$ PID $\qquad$ حيث R P Id

مثال $R=(\mathbb{Z}(\sqrt{-2}),+,\cdot)$ اثبت انها Ed

الحل: نعرف العلاقة. $\varepsilon: R\setminus\{0\}\longrightarrow N$

$$x=a+b\sqrt{-2}\in R\setminus\{0\}$$

$$\varepsilon(x)=[a^2-2b]$$

$$\rightarrow x.y^{-1}\in \mathbb{Q}(\sqrt{-2})$$

$$x.y^{-1}=a+b\sqrt{-2}\in \mathbb{Q}(\sqrt{-2})$$

$$a,b\in \mathbb{Q}$$

$$\exists\, n,m\in \mathbb{Z}^+ ;$$

$$|a-n|\leq \frac{1}{2} \qquad |b-n|\leq \frac{1}{2}$$

$$x.y^{-1}=(a-n)+(b+m)\sqrt{-2} \qquad (n+m\sqrt{-2})$$

$a+b\sqrt{-2}$ $\qquad (n+m(\sqrt{-2}))$

$$x=\underbrace{((a+n)+(b-m)\sqrt{2})}_{r}y.+\underbrace{((m+n)\sqrt{-2})}_{q}y$$

$$x=qy+r$$

$$\varepsilon(r) \leq |(a-n)^2 - 2(b-m)^2|\,\varepsilon(y)$$

$$\leq |(a-n)^2 - 2(b-m)^2|\,\varepsilon(y) \leq$$

$$|\tfrac{1}{4} - 2\tfrac{1}{4}|\,\varepsilon(y)$$

$$= \tfrac{1}{4}\varepsilon(y) < \varepsilon(y)$$

هل هي اقليدية $R = (\mathbb{Z}(i), +, \cdot)$

نفس الإثبات السابق

نعرف العلاقة: $\varepsilon : R \setminus \{0\} \longrightarrow N$

$$x = ab + i \in R \setminus \{0\}$$

$$\ldots \quad \varepsilon(x) = |a^2 - b^2|$$

تمرين (من السنة الماضية):

نتيجة:

$d \in \{-1, -2\} \longleftrightarrow$ UFD هي $R(\mathbb{Z}\sqrt{d}, +, \cdot)$