المحاضرة السادسة　　　　　　　　　　　　　　　　الأحد: 28/3/2015 م

خوارزمية القسمة الحدوديات:

لتكن R حلقة و $R[x]$ حلقة حدوديات معرفة على R ، إذا كانت $f(x), g(x) \in R[x]$

حيث $\mathcal{L}[g]$ (المعامل الرئيسي لـ g) قابل للقلب في R

- فإنه يوجد حدوديتان وحيدتان (تتعينان بشكل وحيد) $r(x), q(x) \in R[x]$

تحققان: $f(x)=g(x)q(x)+r(x)$

- وإنه إما $r(x)=0$ أو $\deg(r(x)) < \deg(g(x))$

الإثبات:

نميز حالتين:

الحالة الأولى:

$f(x)=0$ (الحدودية الصفرية) $\leftarrow$ $\deg(f(x))=\infty$

فعند اختيار $q(x)=0$ و $r(x)=0$ يتحقق $f(x)=g(x).q(x)+r(x)$

$r(x)=0$. ($q(x), r(x)$ تتعينان بشكل وحيد)

فالمبرهنة صحيحة

الحالة الثانية:

$f(x)\neq 0$. يتم الإثبات بالاستقراء الرياضي لدرجة الحدودية $f(x)$.

$\deg(f)=n$. 　$f(x)=\sum_{i=0}^{n} a_i x^i$ 　$a_n\neq 0$

$\deg(g)=m$ 　$g(x)=\sum_{j=0}^{m} b_j x^j$ 　$b_n\neq 0$.

1- من أجل $\boxed{n=0}$

$f(x)=a\neq 0$ (الحدودية الثابتة) $\leftarrow$ $\deg(f)=0$

نختار $q(x)=0$ فيكون $f(x)=r(x)$. تحقق $f(x)=g(x)q(x)+r(x)$

وتحقق $r(x)=0$.

القضية صحيحة من أجل $n=0$

2- نفرض صحة القضية لأجل كل الحدوديات التي درجتها أقل من n

3- لنبرهن صحة هذه القضية من أجل كل الحدوديات ذات الدرجة n

نميز حالتين:

→ الحالة الأولى: $m \le n$

لنعرف الحدودية

$$h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

$$\deg(f(x)) < \deg(h(x))$$

- وبالتالي حسب (1) الفرض الاستقرائي.

يوجد حدوديتان وحيدتان $q_1(x), r_1(x) \in \mathbb{R}[x]$

تحققان $h(x) = g(x)\,q_1(x) + r_1(x)$ *

محققتان إما $r_1(x) = 0$ أو $\deg(r_1(x)) < \deg(g(x))$

نعوض قيمة h في (*)

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x)\,q_1(x) + r_1(x)$$

$$f(x) = \underbrace{(q_1(x) + a_n b_m^{-1} x^{n-m})}_{q(x)} g(x) + r_1(x)$$

$$f(x) = q(x)\,g(x) + r_1(x)$$

ومنه حصلنا على البرهنة.

لماذا اخترنا h بهذا الشكل؟

$$h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

الجواب:

$$h(x) = (a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) - a_n b_m^{-1} x^{n-m}$$
$$(b_m x^m + b_{m-1} x^{m-1} + \dots + b_0)$$

$$a_n b_m^{-1} x^{n-m} \cdot b_m x^m = a_n x_n$$

$$a_n x^n - a_n x^n = 0$$

وهكذا أصبحت لدينا حدودية درجتها أصغر من n

→ الحالة الثانية: $n < m$

أي $\deg(f) < \deg(g(x))$ وهذا يعني أن:

$f(x) = g(x)\,q(x) + r(x) \xrightarrow{\text{نختار}} q(x) = 0$ ، $r(x) = f(x)$

ويحقق $r(x) < g(x)$

عندما $n \ge m$ و $n < m$ إثبات الوحدانية (أي الحدوديتان وحيدتان) $q(x) , r(x)$

نفرض وجود

$$q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{R}[x]$$

حيث يحقق: $\deg(r_1) < \deg(g)$ أو $r_1(x) = 0$ ، $f(x) = g(x)\,q_1(x) + r_1(x)$

$\deg(r_2) < \deg(g)$ أو $r_2(x) = 0$ ، $f(x) = g(x)\,q_2(x) + r_2(x)$

$$f(x) = f(x)$$

$$g(x)\,(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

من مبرهنة سابقة درجة حاصل ضرب الحدوديتين أكبر أو تساوي مجموع الدرجتين

$$\deg(g(x)\cdot(q_1(x) - q_2(x))) \geqslant \deg(g(x)) + \deg(q_1(x) - q_2(x))$$

ومنه

$$\deg g(x) \leqslant \deg(q_1(x) - q_2(x)) = \deg(r_2 - r_1)$$

كيف تحولت العلاقة =

$\deg(g(x)\cdot(q_1(x) - q_2(x)) =$

$\deg(r_2(x) - r_1(x))$

لأنه من مبرهنة سابقة

إذا كان $f[g]$ مثال الحقل

تتحول العلاقة إلى =

وعندنا الشرط $f[g]$ مثال الحقل

(1) إذا كان $r_1(x) = r_2(x) = 0$

يتم المطلوب

(2) في حالة $0 \neq r_1(x) \neq r_2(x)$ (فرضاً)

حسب ما فرضنا $\deg(r_1) < \deg(g)$

$$\deg(r_2) < \deg(g)$$

$$\deg(r_2 - r_1) < \deg(g)$$

ولكن بينا سابقاً من نظرية سابقة $\deg(g(x)) \leqslant \deg(r_2(x) - r_1(x))$

وهكذا حصلنا على تناقض

ومنه الفرض الجدلي خاطئ وبالتالي $r_1(x) = r_2(x)$ ← $q_1(x) = q_2(x)$

وهكذا نجد الحدوديتان وحيدتان

[إذاً يوجد حدوديتان وحيدتان تحققان كلا المبرهنة]

تم المطلوب

مثال:

لتكن الحدودية $f(x) = x^3 + x^2 + x + 3 \in \mathbb{Z}[x]$

$\exists g(x) = x^2 + x + 1$ تحقق $f(x) = g(x).q(x) + r(x)$

حيث $q(x) = x$ $r(x) = 3 \in \mathbb{Z}[x]$

ويتحقق $\deg(r(x)) = 0 < \deg(g) = 2$

مبرهنة: (معيار آيزنشتاين) Eisenstein :

لتكن الحدودية $f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0=\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$

حدودية معرفة على $\mathbb{Z}$

- p: عدد أولي يحقق:

$a_n \not\equiv 0 \pmod p$

$a_0 \not\equiv 0 \pmod{p^2}$

$a_i \equiv 0 \pmod p \quad i \in [0,1,\dots,n-1]$

فإن $f(x)$ غير قابلة للاختزال (غير قابلة للتحليل) على $\mathbb{Q}$

تعريف الحدودية الغير قابلة للتحليل

لتكن $f(x)$ حدودية معرفة على حلقة $\mathbb{R}[x]$; $\deg(f(x))=n$

- نقول أن $f(x)$ غير قابلة للتحليل (الاختزال):

إذا كان لا يوجد حدوديتان $h(x), g(x) \in \mathbb{R}[x]$ تحققان:

$f(x)=g(x).h(x)$

$0<\deg h(x)<\deg f(x) \quad <\deg(f(x))$

الإثبات

نفرض جدلاً أن f قابلة للاختزال على $\mathbb{Q}$ أي يوجد حدوديتان

$\exists q(x), g(x) \longrightarrow f(x)=(b_0+b_1x+\dots+b_rx^r)(c_0+c_1x+\dots+c_sx^s)$

$0<r<n \qquad 0<s<n$

[illegible] $a_0=b_0c_0 \equiv 0 \pmod p \longrightarrow p \mid b_0c_0$

[illegible]

[illegible]

$a_0=b_0c_0 \not\equiv 0 \pmod{p^2} \longrightarrow p^2 \nmid b_0c_0$

$b_0 \equiv 0 \pmod p \quad \vee \quad c_0 \equiv 0 \pmod p$

نفرض: $b_0 \equiv 0 \pmod p$; $c_0 \not\equiv 0 \pmod p$

$f(x)=2x-6$

$=2(x-3)$

$\uparrow$

$\deg(g(x)) \neq 0$ حيث

ولاحظ أن جميع المعاملات

قابلة للاختزال

[أي أن $f(x)$ غير قابل للاختزال

لأن $g(x)=2$

$\deg(g(x))=0$

ليكن m أصغر عدد موجب صحيح تحقق

$$b_m \neq 0 \pmod p$$

حسب تعريف جداء باليف $a_m = c_0 b_m + c_1 b_{m-1} + \dots + c_m b_0$

$\underbrace{c_0 b_m}_{\text{لا يقبل القسمة على } p}$ $\underbrace{c_1 b_{m-1}}_{\text{يقبل القسمة}}$ $\underbrace{c_m b_0}_{\text{يقبل القسمة على } p}$

حسب الفرض: $a_m \neq 0 \pmod p$ m موجود لأن a_n لا يقبل 1

$m < n$ فيكون $c_0 b_m$ لا يقبل القسمة لأن 1 لا تقبل القسمة على p

وهذا يناقض كون

$a_i = 0 \pmod p$ $i \in [0, 1, \dots, n-1]$

ومنه يناقض الفرض الجدلي

فيكون $f(x)$ غير قابل للاختزال على Q

مثال: سؤال دورات أكبير (5 علامات).

$f(x) = 9x^3 + 8x^2 + 2x + 6$

من أجل $p = 2$

$r_3 = 9$ $r_2 = 8$ $r_1 = 2$ $r_0 = 6$

$r_3 \neq 0 \pmod p$

$r_0 \neq 0 \pmod{p^2}$

$r_i = 0 \pmod p$ $i \in [0, 1, 2]$

f غير قابلة للاختزال.

نختار p بحيث:

a_n لا يقبل القسمة على

ومربعه لا يقسم a_0