مميز الحلقة

تعريف :

إذا كانت R حلقة فإن أصغر عدد صحيح موجب $n \in Z^+$ يحقق أن

$na=0$ لكل $a \in R$

ويسمى مميز الحلقة R ويكتب $Char\ R = n$.

في هذا التعريف إذا كان لا يوجد عدد صحيح موجب n يحقق أن

$na=0$ لكل $a \in R$

فإن مميز R هو الصفر أي أن $Char\ R = 0$.

فمثلاً :

$$Char\ Z = Char\ Q = Char\ R = Char\ C = 0$$

بينما

$$Char\ Z_n = n$$

خاصية :

إذا كانت R حلقة ذات عنصر محايد فإن

$Char\ R = n > 0$ إذا وفقط إذا كانت n هي أصغر عدد صحيح موجب يحقق أن $n(1)=0$.

البرهان :

إذا كانت Char R =n فإن $n(1)=0$.

وإذا كان $m(1)=0$ حيث $0<m<n$ فإن :

$$ma=(m1)a=0a=0$$

لكل $a \in R$ وهذا يناقض أن Char R =n أي أن n هي أصغر عدد صحيح موجب يحقق أن $n(1)=0$.

ولإثبات العكس

نفرض أن n هي أصغر عدد صحيح موجب وأن $n(1)=0$ فإن :

$$na=(n1)a=0a=0$$

لكل ومن ثم فإن Char R =n .

خاصية :

مميز الحلقة التامة هو صفر أو عدد أولي .

البرهان :

نفرض أن R حلقة تامة وأن Char R =n>0 ، إذا كانت n عدد غير أولي فإن $n=rs$ حيث $0<r,s<n$ وحيث $n1=0$ فإن

$$(r1)(s1)=0$$

وحيث أن R خالية من قواسم الصفر فإن

s1=0 أو r1=0

وهذا يناقض الفرض أن Char R =n>0 بهذا فإن n يجب أن تكون عدداً أولياً .

نظرية :

نفرض أن R حلقة تامة

أ) Z منغمسة في R إذا كان Char R =0 .

ب) منغمسة في Rإذا كان Char R =p حيث p عدد أولي .

البرهان :

(أ) نفرض أن e هو العنصر المحايد في R .

الدالة

$$f:Z \to R \quad , \quad f(n) = ne$$

تشاكل حلقي ،

وهذا التشاكل أحادي لأنه لكل $n,m \in Z$ ونجد أن :

$$f(m) = f(n) \to me = ne$$

وحيث أن R خالية من قواسم الصفر لأنها تامة فإن m=n

أي ان F متباينة (أحادية) بهذا فإن $Z \cong f(Z)$ حيث $f(Z) \le R$.

(ب) نفرض أن e هو العنصر المحايد في R ، الدالة

$f : Z_p \to R \quad , \quad f(n) = ne$

تشاكل حلقي ، هذا التشاكل متباين لأن :

$$
\begin{aligned}
& f(m) = f(n) \\
& \to me = ne \\
& \to (m-n)e = 0
\end{aligned}
$$

و بإستخدام خوارزمية القسمة فإنه يوجد $r,s \in Z$ بحيث :

(m-n)e=(pr+s)e=pre+se

وحيث أن pre=0 فإن se=0 .

وحيث أن 0<s<p فإن هذا يناقض الفرض .

فإن Char R =p بذلك فإن s=0

ومن ثم يكون

m-n=pre=0

أي أن m=n ومن ثم فإن $Z_p \cong f(Z_p)$ حيث

$f(Z_p) \le R$.

حلقات كثيرات الحدود

تعريف :

إذا كانت R حلقة فإن المتتابعة :

$$f=(a_0,a_1,a_2,\dots,a_n,0,\dots)$$

تسمى كثيرة حدود على R إذا كان $a_i \in R$ لكل i ، $a_i=0$ إذا كان $i>n$.

مثال :

كل من

$f=(1,1,12,2,-2,0,0,0,\dots)$

$g=(0,1,1,1,0,0,0,0,0,\dots)$

كثيرتي حدود على Z بينما

$h=(0,1,0,1,0,\dots)$

ليست كثيرة حدود على Z لعدم وجود n بحيث أنه $a_i=0$ لكل $i>n$.

تعريف :

أ- كثيرتي الحدود

$$f=(a_0,a_1,a_2,\dots,a_n,0,\dots)$$

$$g=(b_0,b_1,b_2,\dots,b_n,0,\dots)$$

40

على الحلقة R تسميان متساويتان إذا كان $a_i = b_i$ لكل i
وتكتب f=g.

ب- إذا كان

$$f = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots)$$
$$g = (b_0, b_1, b_2, \ldots, b_n, 0, \ldots)$$

كثيرتي حدود على الحلقة R تعريف جمعهما f+g
وحاصل ضربها f.g كالآتي :

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, 0, \ldots)$$
$$f \cdot g = (c_0, c_1, c_2, \ldots, c_n, 0, \ldots)$$

حيث

$$\begin{aligned} c_k &= \sum_{i+j=k} a_i b_j \\ &= a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \ldots + a_k b_0 \end{aligned}$$

وإذا كان $a_i = 0$ لكل i>n و $b_j = 0$ لكل j>m فإن
$c_k = 0$ لكل k>m+n .

مثال :

إذا كان

f=(1,2,3,3,1,0,...)
g=(2,1,1,3,1,0,...)

كثيرتي حدود على Z فإن :

41

$$f+g=(3,3,4,6,2,0,\ldots)$$
$$f\cdot g=(1\times2,1\times1+2\times2,1\times1+2\times1+3\times2,$$
$$1\times3+2\times1+3\times1+3\times2,1\times1+2\times3+3\times1+3\times1+1\times2,0,\ldots.)$$
$$=(2,5,9,14,15,0,\ldots)$$

تعريف :

إذا كانت $(R,+,\cdot)$ حلقة وكانت P(R) مجموعة جميع كثيرات الحدود على R فإن :

أ) $(P(R),+,\cdot)$حلقة حيث + , . هما عمليتي الجمع والضرب على الترتيب P(R) .

ب) $(P(R),+,\cdot)$ ذات عنصر محايد إذا وفقط إذا كانت R كذلك .

جـ) $R\cong S\leq P(R)$ أي أن R منغمسة في P(R) .

د) $(P(R),+,\cdot)$ حلقة إبدالية إذا وفقط إذا كانت R كذلك .

البرهان :

أ) (i) (P(R),+) زمرة إبدالية لأن :

١- لكل $f,g,h\in P(R)$ نجد أن:

42

١- لأي $f,g \in P(R)$ فإن $f+g \in P(R)$

٢- لكل $f,g,h \in P(R)$ نجد أن:

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

٣- المتتابعة الصفرية $0=(0,0,0,0,...)$.

توجد في $P(R)$ وتحقق أن :

$$f+0=0+f=f \quad , \quad \forall f \in P(R)$$

٤- لكل $f=(a_0,a_1,a_2,...,a_n,0,...)$ يوجد

$$-f=(-a_0,-a_1,-a_2,...,-a_n,0,0,...)$$

هو معكوس f الجمعي لأنه يحقق أن :

$$f+(-f)=-f+f=0$$

٥- لكل $f,g \in P(R)$ نجد أن $f+g=g+f$.

(ii) $(P(R),\cdot)$ نصف زمره لأن

$$(f\cdot g)\cdot h = f\cdot(g\cdot h) \quad , \quad \forall f,g,h \in P(R)$$

(iii) لكل $f,g,h \in P(R)$ يحقق أن :

$$f\cdot(g+h)=f\cdot g+f\cdot h$$

$$(g+h)\cdot f = g\cdot f+h\cdot f$$

بهذا فإن $(P(R),+,\cdot)$ حلقة .

ب) نفرض أن 1 هو العنصر المحايد في R فإن :

e=(1,0,0,...)

هو العنصر المحايد في P(R) لأنه لكل

$$f=(a_0,a_1,,...,a_n,0,0,...)$$

نجد أن

$$f.e = e.f = f$$

والعكس إذا كان

$$e = (b_0, b_1, \dots, b_n, 0, \dots)$$

عنصر محايد في P(R) فيكون لكل $a \in R$ يتحقق أن :

$$\begin{aligned}(a,0,0,\dots) &= (a,0,0,\dots)e \\ &= (ab_0, 0b_1, \dots, 0b_n, 0, \dots) \\ &= ab_0\end{aligned}$$

$$\begin{aligned}(a,0,0,\dots) &= e(a,0,0,\dots) \\ &= (b_0a, b_10, \dots, b_n0, 0, \dots) \\ &= b_0a\end{aligned}$$

$$\therefore a = ab_0 = b_0a \quad , \quad \forall a \in R$$

أي أن b_0 هو العنصر المحايد في R .

جـ) نفرض أن

$$S = \{(a,0,0,\dots); a \in R\}$$

فإن $S \leq P(R)$

ونجد أن

$$\theta : R \to S \quad , \quad \theta(a) = (a,0,0,\dots)$$

تماثل حلقي $R \cong S \leq P(R)$ أي أن R منغمسة في P(R) .

د) نفرض ان R إبدالية ونفرض أن :

$$f = (a_0, a_1, \dots, a_n, 0, 0, \dots)$$

$$g = (b_0, b_1, \dots, b_m, 0, \dots)$$

فإن

$$f\cdot g=(a_0b_0,a_0b_1+a_1b_0,a_0b_2+a_1b_1+a_2b_0,\ldots$$
$$,a_0b_k+a_1b_{k-1}+\ldots+a_kb_0,0,0,\ldots..)$$
$$=(b_0a_0,b_0a_1+b_1a_0,b_0a_2+b_1a_1+b_2a_0,\ldots$$
$$,b_0a_k+b_1a_{k-1}+\ldots+b_ka_0,0,0,\ldots..)$$
$$=g\cdot f$$

لإثبات العكس نجد أن $R\cong S\le P(R)$ ،

فإذا كانت P(R) إبدالية فكذلك S ومن ثم تكون R حلقة إبدالية

.

نظرية :

إذا كانت R حلقة ذات عنصر محايد 1 وكانت

$$x=(0,1,0,0,\ldots,0,\ldots)\in P(R)$$

كثيرة حدود فإن :

أ- $x^n=(0,0,\ldots,0,1,0,\ldots)$ حيث الواحد يظهر في الموقع (n+1).

ب- إذا كانت $f=(a_0,a_1,\ldots,a_m,0)\in P(x)$ فإن :

$$f=\sum_{i=0}^{n}a_ix^i$$

تعريف :

إذا كانت

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

كثيرة حدود غير صفرية وكانت $a_n \neq 0$ فإن a_n يسمى المعامل الرئيسي أو القيادي ويرمز له بالرمز L(f) وتسمى n درجة كثيرة الحدود ويرمز له بالرمز deg f وتسمى كثيرة الحدود f(x) واحدية إذا كان L(f)=1 .

أمثلة :

١)إذا كانت f(x) كثيرة حدود

$$f(x)=2-3x+5x^2+7x^3 \in Z[x]$$

فإن deg f(x)=3 وهي كثيرة حدود ليست واحدية لأن $L(f) \neq 1$.

٢)إذا كانت

$$f(x)=1-\frac{1}{2}x+\frac{1}{3}x^2-4x^5+x^6 \in Q[x]$$

فإن deg f(x)=6 وهي كثيرة حدود واحدية لأن L(f)=1 .

٣)نفرض أن

f(x)=1+2x , g(x)=1+3x

كثيرتي حدود في Z_6

deg f(x)= deg g(x)=1

ونجد أن :

f(x).g(x)=1+5x

أي أن :

46

$$\deg\left[f(x)+g(x)\right]=1\neq\deg f(x)+\deg g(x)$$
$$\deg\left[f(x)\cdot g(x)\right]=1\neq\deg f(x)+\deg g(x)$$

٤)نفرض أن

f(x)=1+2x , g(x)=3+4x

كثيرتي حدود في Z_6

deg f(x)= deg g(x)=1

بينما

f(x)+g(x)=4

deg[f(x)+ g(x)]=0

أيضاً

$f(x).\ g(x)=3+4x+2x^2$, $\deg[\ f(x).\ g(x)]=2$

أي أن

deg[f(x). g(x)]= deg[f(x)]+ deg[g(x)]

نظرية :

إذا كان كل من f(x) ، g(x) كثيرة حدود غير صفرية على الحلقة R فإن :

47

أ) $\deg\left[f(x)\cdot g(x)\right]\le \deg\left(f(x)\right)+\deg\left(g(x)\right)$.

ب) $\deg\left[f(x)\cdot g(x)\right]=\deg\left(f(x)\right)+\deg\left(g(x)\right)$.

إذا كان L(f) أو L(g) قابل للإنعكاس .

جـ) $\deg\left[f(x)\cdot g(x)\right]=\deg\left(f(x)\right)+\deg\left(g(x)\right)$

إذا كان R خالية من القواسم الصفرية .

د) إما f(x)+g(x)=0 أو

$\deg\left[f(x)+g(x)\right]\le \max\left\{\deg\left(f(x)\right),\deg\left(g(x)\right)\right\}$.

البرهان :

نفرض أن

$$\deg(f(x))=n \quad , \quad \deg(g(x))=m$$

أي أن :

$$f(x)=\sum_{i=0}^{m}a_i x^i \quad , \quad a_m\ne 0$$

$$g(x)=\sum_{j=0}^{n}b_j x^j \quad , \quad b_n\ne 0$$

فيكون :

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}c_k x^k$$

حيث:

$$c_k = \sum_{i+j=k} a_i b_j$$

ومن ثم يكون :

$$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + a_2 b_{m+n-2} + \dots + a_m b_n + \dots + a_{m+n} b_0$$

لكن $a_i = 0$ لكل i>m ، $b_j = 0$ لكل j>n .

ومن ثم يكون $c_{m+n} = a_m \cdot b_n$.

أ) إذا وجد في الحلقة R قاسم للصفر فقد يكون $a_m b_n = 0$ ومن ثم يكون

$\deg[f(x) \cdot g(x)] \le \deg(f(x)) + \deg(g(x))$.

ب) نلاحظ أن $a_m b_n \ne 0$ في هذه الحالة لأنه إذا كان $a_m b_n = 0$ وكان b_n لها معكوس b_n^{-1} فهذا يؤدي إلى أن $a_m = 0$ وهذا يناقض الفرض deg(f(x))=m .

وكذلك إذا كان a_m لها معكوس فإن ذلك يؤدي إلى $b_n = 0$ وهذا يناقض الفرض أن

deg g(x)=n

حيث $a_m b_n \ne 0$ ومن ثم فإن :

$$\deg[f(x) \cdot g(x)] = \deg(f(x)) + \deg(g(x))$$

جـ) في هذا الحالة يكون $a_m b_n \neq 0$ ومن ثم يكون

$$\deg\left[f(x)\cdot g(x)\right]=\deg\left(f(x)\right)+\deg\left(g(x)\right)$$

د) $f(x)+g(x)\neq 0$ فإن

$$f(x)+g(x)=\sum_{i=0}\left(a_i+b_j\right)x^i$$

إذا كانت r=max{m,n}

فإن $a_i=b_j=0$ لكل i>r .

ومن ثم يكون :

$$f(x)+g(x)=\sum_{i=0}^{r}\left(a_i+b_i\right)x^i$$

ومن ثم فإن :

$$\begin{aligned}\deg\left[f(x)+g(x)\right]&\le r\\&=\max\{m,n\}\end{aligned}$$

خاصية :

إذا كانت الحلقة R تامة فكذلك R[x] .

البرهان :

نفرض ان f(x) ، g(x) كثيرتي حدود غير الصفرية فإن :

$$\deg[f(x)] \neq 0 \quad , \quad \deg[g(x)] \neq 0$$

ومن ثم يكون

$$\deg[f(x)\cdot g(x)] = \deg(f(x)) + \deg(g(x))$$

ومن ثم يكون

$$f(x)\cdot g(x) \neq 0$$

إذن خالية من قواسم الصفر .

أي أن : R[x] خالية من قواسم الصفر وحيث أن R[x]حلقة إبدالية ذات عنصر محايد لأن R كذلك فإن R[x] حلقة تامة .

ملاحظة :

إذا كانت F حقلاً فإن F[x] ليست حقل لأنه إذا كانت F[x] حقل وكانت f(x) كثيرة حدود غير صفرية في F[x] فإنه توجد كثيرة حدود غير صفرية g(x) في F[x] بحيث أن

$$f(x).g(x)=1$$

أي أن

$$\deg[f(x).g(x)]=0$$

ومن ثم فإن :

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

وهذا غير ممكن .

خاصية :

إذا كانت R حلقة إبدالية ذات عنصر محايد وكانت

$f(x), g(x) \in R[x]$ وكان $L(g) \neq 0$ قابل للإنعكاس في R

فإنه توجد كثيرتي حدود وحيدتين

$$p(x), r(x) \in R[x]$$

بحيث أن

$$f(x)=p(x)g(x)+r(x)$$

حيث

$$r(x)=0 \quad \vee \quad \deg(r(x)) < \deg(g(x))$$

في هذه النظرية تسمى f(x) مقسوم وg(x) مقسوم عليه p(x) خارج القسمة ، r(x) الباقي

وإذا كانت r(x)=0 قيل عن f(x) أنها تقبل القسمة على g(x) أو أن g(x) قاسم لـ f(x) وتكتب كذلك g(x)|f(x) ولنفي ذلك نكتب $g(x) \nmid f(x)$ **.**

أمثلة :

١)إذا كانت

$$f(x)= x^3+x^2+x+3$$
$$g(x)= x^2+x+1$$

كثيرتي حدود في Z فإن

$$f(x)=xg(x)+3$$

فإن

$p(x)=x$ ، $r(x)=3$.

ونلاحظ أن

$\deg(r(x))=0 < \deg(g(x))=2$.

٢)إذا كانت

$$f(x)= 2x^5+3x^4+7x^3+x^2+2x+1$$

$$g(x)= x^3+2x^2+3x+1$$

كثيرتي حدود في Z_{11} فإن :

$$f(x)= \left(2x^2+10x+3\right)g\left(x\right)+\left(7x^2+5x+9\right)$$

توضيح :

$$\begin{array}{r|l}
 & 2x^2+10x+3 \\
\hline
x^3+2x^2+3x+1 & 2x^5+3x^4+7x^3+x^2+2x+1 \\
 & 2x^5+4x^4+6x^3+2x^2 \\
\cline{2-2}
 & 10x^4+x^3+10x^2+2x+1 \\
 & 10x^4+9x^3+8x^2+10x \\
\cline{2-2}
 & 3x^3+2x^2+3x+1 \\
 & 3x^3+6x^2+9x+3 \\
\cline{2-2}
 & 7x^2+5x+9
\end{array}$$

53

ونجد أن

. $deg(r(x))=2<deg(g(x))=3$

٣)إذا كانت

$$f(x)= x^4 - 3x^2 - 4$$

$$g(x)= x^2 + 1$$

كثيرتي حدود في Q[x] فإن f(x) تقبل القسمة على g(x)

وذلك لأن :

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

حيث

$$h(x) = x^2 - 4$$

تعريف :

إذا كانت R حلقة وكانت f(x) كثيرة حدود في R[x] حيث $r \in R$ تسمى جذر (root) لكثيرة الحدود f(x) إذا كان $f(r)=0$.

مثال :

١)كل من 1,-1 جذر لكثيرة الحدود

$$Z[x] = f(x) = x^2 - 1$$

٢)$f(x) = x^2 - 1$ ليس لها جذر في R .

٣)كثيرة الحدود $f(x) = x^2 + 2x + 3$ في Z_6 لها جذران هما 1,3 لأن $f(1)=f(3)=0$.

54

نظرية :(نظرية الباقي)

إذا كانت R حلقة إبدالية ذات عنصر محايد وكان

$a \in R$, $f(x) \in R[x]$ فإنه توجد كثيرة حدود وحيدة

$P(x) \in R[x]$ تحقق أن :

$$f(x)=(x-a)P(x)+f(a).$$

البرهان :

حيث أن :

$$f(x)=(x-a)P(x)+r(x)$$

و $r(x)=0$ أو $\deg(r(x))<\deg(x-a)=1$

أي أن $\deg(r(x))=0$ ومن ثم $r(x)=c \in R$

ومن ثم فإن :

$$f(x) = (x-a)P(x)+ c$$

وحيث أن $f(a)=c$ فإن :

$$f(x)=(x-a)P(x)+f(a).$$

نتيجة :

إذا كانت R حلقة إبدالية ذات عنصر محايد فإن $f(x)$ تقبل القسمة على $(x-a)$ إذا وفقط إذا كانت $a \in R$ جذرا لكثيرة الحدود $f(x)$.

55

البرهان :

حيث أن f(a)=0 إذا وفقط إذا كان

. f(x)=(x-a)P(x)

فإن (x-a)|f(x) إذا وفقط إذا كانت $a \in R$ جذرا لكثيرة الحدود

. f(x)

نظرية :

إذا كانت R حلقة تامة وكان $a_1, a_2, \ldots, a_n$ جذور مختلفة لكثيرة الحدود $f(x) \in R[x]$ فإن f(x) تقبل القسمة على $\prod_{i=1}^{n}(x-a_i)$ حيث $i = 1, 2, ..n$.

نتيجة ١:

إذا كانت R حلقة تامة و $f(x) \in R[x]$ حيث deg(f(x))=n فإن لكثيرة الحدود f(x) على الأكثر n من الجذور في الحلقة R .

نتيجة ٢:

إذا كانت R حلقة تامة غير منتهية و E مجموعة جزئية غير منتهية من R وكان $f(x) \in R[x]$ وكان f(a)=0 لكل $a \in E$ فإن f(x)=0

.

البرهان :

نفرض أن $f(x)\neq 0$ و deg(f(x))=n>0 فإن f(x) لها على الأكثر n من الجذور وعليه فإن لبعض قيم $a\in E$ وهذا يناقض الفرض بهذا فإن f(x)=0 .

نتيجة ٣:

إذا كانت R حلقة تامة غير منتهية و Eمجموعة جزئية غير منتهية من Rوكان$f(x),g(x)\in R[x]$ وكان f(a)=g(a) لكل $a\in E$ فإن f(x)=g(x) .

البرهان :

نفرض أن h(x)=f(x)-g(x) فإن h(a)=0 لكل $a\in E$ ومن ثم h(x)=0 ومن ثم فإن f(x)=g(x) .

ملاحظات :

١)إذا كانت الحلقة R ليست تامة فإن نتيجة١ ليست صحيحة <u>كما في المثال الآتي</u> :

نفرض أن

$$f(x)=x^2+3x+2\in Z_6[x]$$

فإننا نعلم أن Z_6 حلقة ليست تامه و deg(f(x))=2
ولكن لكثيرة الحدود f(x) اربعة جذور في Z_6 وهي
. 1,2,4,5

٢)إذا كانت R حلقة تامة منتهية فإن نتيجة ٣ ليست صحيحة كما في المثال الآتي :

نفرض أن :

$$f(x)=x^3\in Z_3[x] \quad , \; g(x)=x\in Z_3[x]$$

فإن f(a)=g(a) لكل $a\in Z_3$ ولكن $f(x)\neq g(x)$ لأن
. $\deg(f(x))\neq\deg(g(x))$

نظرية :

إذا كان $z\in C$ جذر لكثيرة الحدود f(x) فإن $\overline{z}$ جذراً لها .

البرهان :

نفرض أن :

$$f(x)=\sum_{i=0}^{n}a_i x^i$$

فإن :

$$f(z)=\sum_{i=0}^{n} a_i z^i = 0$$

ومن ثم فإن :

$$f(\bar{z})=\sum_{i=0}^{n} a_i (\bar{z})^i = \overline{\sum_{i=0}^{n} a_i z^i} = \bar{0} = 0$$

أي أن $\bar{z}$ جذر لكثيرة الحدود f(x) .

نتيجة :

إذا كانت f(x) كثيرة حدود وكان deg(f(x))=n عددا فرديا فإنه يوجد على الأقل جذر حقيقي واحد.

البرهان :

نفرض أن جميع جذور f(x) مركبة وهي $r_1, r_2, ..., r_n \in C$ وهذا يعني أن $r_i \neq \bar{r_i}$ لكل i ،

وحيث أن $\bar{r_i}$ جذر لكثيرة الحدود فإن $(r_i\ ,\ \bar{r_i})$ زوج من الجذور المختلفة لكثيرة الحدود f(x) لكل i ،

وهذا يعني أن n عدد زوجياً وهذا يناقض الفرض ومن ثم فإنه يوجد على الأقل جذر حقيقي واحد لكثيرة الحدود f(x) .

59

تعريف :

إذا كانت R حلقة تامة فإن كثيرة الحدود الواحدية $d(x) \in R[x]$
تسمى قاسم مشترك أعظم (**greatest common divisor**)
لكثيرتي الحدود غير الصفريتين $f(x), g(x) \in R[x]$ إذا كان :

أ) $d(x) | g(x)$, $d(x) | f(x)$.

ب) إذا كانت $c(x) | f(x)$, $c(x) | g(x)$
فإن $c(x) | d(x)$ وتكتب كذلك :

$$d(x) = gcd(f(x), g(x))$$

أمثلة :

١)إذا كانت
$$f(x) = x^3 + 1 \ , \ g(x) = x^2 - 1$$
كثيرتي حدود في $Z(x)$ فإن :
$$f(x) = (x+1)(x^2 - x + 1)$$
$$g(x) = (x+1)(x-1)$$
ومن ثم فإن
$d(x) = (x+1) = gcd(f(x), g(x))$.

٢)إذا كانت

$$g(x) = x^3 + 4x^2 + 7x + 6 \in Q[x]$$
$$f(x) = x^4 + 2x^3 + 2x^2 - 2x - 3 \in Q[x]$$

فإن $f(1)=f(-1)=0$ ومن ثم فإن :

$$(x-1)(x+1) \mid f(x)$$

أي أن :

$$f(x) = (x-1)(x+1)(x^2 + 2x + 3)$$

أيضا

$(x+2) \mid g(x)$ لأن $g(-2)=0$ ومن ثم

$$g(x) = (x+2)(x^2 + 2x + 3)$$

ومن ثم فإن

$$\gcd(f(x), g(x)) = x^2 + 2x + 3$$

نظرية :

إذا كانت F حقلاً فإنه لأي كثيرتي حدود غير صفريتين $f(x), g(x) \in F[x]$ قاسم مشترك أعظم وحيد $d(x) \in F[x]$ كما توجد كثيرتي حدود $s(x), t(x) \in F[x]$

بحيث أن :

$$d(x)=s(x)f(x)+t(x)g(x)$$

البرهان :

61

نعلم أنه توجد كثيرتي حدود وحيدتين $p_1(x), r_1(x) \in F[x]$ بحيث أن

$$f(x) = p_1(x)g(x) + r_1(x)$$

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

إذا كان $r_1(x) = 0$ فإن $d(x) = g(x)$

أما إذا كان $r_1(x) \neq 0$ فإننا نقسم g(x) على $r_1(x)$ فيكون

$$g(x) = p_2(x)r_1(x) + r_2(x)$$

حيث $r_2(x) = 0$ أو $\deg(r_2(x)) < \deg(r_1(x))$

فإذا كانت $r_2(x) = 0$ فإن $d(x) = c^{-1}r_1(x)$

حيث $c = 1.(r_1(x))$

أما إذا كان $r_2(x) \neq 0$:

نكرر عملية القسمة السابقة عدة مرات وحيث :

$$\deg(g(x)) > \deg(r_1(x)) > \ldots\ldots$$

ونجد أن :

$$f(x) = p_1(x)g(x) + r_1(x)$$
$$g(x) = p_2(x)r_1(x) + r_2(x)$$
$$r_1(x) = p_3(x)r_2(x) + r_3(x)$$

.

.

وهكذا حتى يكون :

$$r_{m-2}(x) = p_m(x) r_{m-1}(x) + r_m(x)$$

و

$$\deg(r_m(x)) < \deg(r_{m-1}(x))$$

و أخيراً

$$r_{m-1}(x) = p_{m+1}(x) r_m(x)$$

ومن ثم نجد أن $r_m(x)$ هو القاسم المشترك لكثيرتي الحدود f(x),g(x) وإذا كان $L(r_m(x)) = c_m$ فإن

. $d(x) = c_m^{-1} r_m(x)$

و بإستخدام المعادلات السابقة بالتعويض من أسفل إلى أعلى يمكن إيجاد $s(x), t(x) \in F[x]$.

بحيث أن

$$d(x)=s(x)f(x)+t(x)g(x)$$

نفرض أن e(x) قاسم مشترك أعظم لكثيرتي الحدود f(x),g(x) فإن e(x) | d(x) وايضاً d(x) | e(x) ومن ثم فإن :

$$d(x)=h(x)e(x)$$

و

$$e(x)=k(x)d(x)$$

حيث $h(x), k(x) \in F[x]$ ومن ثم فإن

$d(x)=h(x)k(x)\ d(x)$

ومن ثم فإن $k(x)h(x)=1$ وذلك لأن $F[x]$ خالية من قواسم الصفر بهذا فإن

$$k(x)=b\in F\ ,\ h(x)=a\in F$$

ولكن $L(d(x))=L(e(x))=1$ أي أن $a=b$ ومن ثم فإن $d(x)=e(x)$.

أمثلة :

١-نفرض أن

$$f(x)=2x^4-3x^3-x^2+21x+10$$
$$g(x)=2x^3-5x^2+7x+5$$

كثيرتي حدود في $R[x]$ بقسمة $f(x)$ على $g(x)$ نجد أن

$$f(x)=(x+1)g(x)+3(x^2-3x+5)$$

أي أن:

$$r_1(x)=3(x^2-3x+5)\quad ,\quad p_1(x)=x+1$$

وحيث أن

$$2=\deg(r_1(x))<\deg(g(x))=3$$

فإننا نقسم $g(x)$ على $r(x)=x^2-3x+5$

فيكون $g(x)=(2x+1)r(x)$

فإن :

64

$$d(x)=x^2-3x+5$$

ولإيجاد $s(x),t(x)\in R[x]$ نلاحظ أن :

$$f(x)=(x+1)g(x)-3d(x)$$

ومن ثم فإن

$$d(x)=\frac{-1}{3}f(x)+\left(\frac{x+1}{3}\right)g(x)$$

ومن ثم فإن

$$s(x)=\frac{-1}{3} \quad , \quad t(x)=\frac{x+1}{3}$$

٢-إذا كان

$$f(x)=x^4-3x^3+x^2+1$$
$$g(x)=x^3-1$$

كثيرتي حدود في Q[x] بقسمة f(x) على g(x) نجد أن

$$f(x)=(x^3-1)(x-1)+(-x^2+x)$$

أي أن

$$r_1(x)=-x^2+x \quad , \quad p_1(x)=x-1$$

وحيث أن

$$2=\deg(r_1(x))<\deg(g(x))=3$$

فإننا نقسم g(x) على $r_1(x)$ فنجد أن

$$g(x)=r_1(x)(-x-1)+(x-1)$$

ويكون

$$1=\deg\left(r_2(x)\right)<\deg\left(r_1(x)\right)=2$$

ومن ثم نقسم $r_1(x)$ على $r_2(x)$ فيكون

$$r_1(x)=-xr_2(x)$$

ومن ثم d(x)=x-1 ولإيجاد $s(x),t(x)\in Q[x]$

نلاحظ أن

$$-x^2+x=f(x)-g(x)(x-1)$$

لكن

$$d(x)=(x-1)=g(x)-\left(-x^2+1\right)(-x-1)$$

$$=g(x)-\left[f(x)-g(x)(x-1)\right](-x-1)$$

$$=f(x)(x+1)+g(x)\left[1-\left(x^2+1\right)\right]$$

$$=f(x)(x+1)+g(x)\left(2-x^2\right)$$

أي أن

$$s(x)=x+1 \quad , \quad t(x)=2-x^2$$

٣-إذا كانت

$$f(x)=x^5+2x^3+x^2+2x$$

$$g(x)=x^4+x^3+x^2$$

كثيرتي حدود في $Z_3[x]$ فإن

$$f(x)=g(x)(x+2)+2\left(x^3+x^2+x\right)$$

$$g(x)=x\left(x^3+x^2+x\right)$$

ومن ثم فإن

$$d(x)=x^3+x^2+x$$

66

و نلاحظ أن

$$2^{-1} = 2 \in Z_3$$

ولإيجاد t(x),s(x) نلاحظ أن :

f(x)=g(x)(x+2)+2d(x)

ومن ثم

d(x)= 2f(x)+g(x)(x+2)

أي أن :

t(x)=x+2 , s(x)=2

تعريف :

تسمى كثيرة الحدود $f(x) \in R[x]$ قابلة للتحليل على R إذا كانت f(x)=g(x)h(x) حيث $g(x),h(x) \in R[x]$

و

0<deg(g(x))<deg(f(x))

0<deg(h(x))<deg(f(x))

وإذا لم تكن f(x) قابلة للتحليل فإنها تسمى غير قابلة للتحليل (**irreducible**) .

أمثلة :

١-إذا كانت R حلقة خالية من قواسم الصفر وكان $f(x) \in R[x]$ حيث deg(f(x))=1 فإن f(x) غير قابلة للتحليل على R

67

لأنه إذا كانت $f(x)=g(x)h(x)$ فإن

$$deg(g(x))<deg(f(x))=1$$

$$deg(h(x))<deg(f(x))=1$$

ومن ثم فإن

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

وحيث أن :

$$deg(f(x))=deg(g(x))+deg(h(x))=0$$

أي أن $deg(f(x))=0$

وهذا يناقض الفرض بذلك فإن $f(x)$ غير قابلة للتحليل على R .

٢-كثيرة الحدود

$$f(x)=x^2-1\in Z[x]$$

قابلة للتحليل على Z لأن $f(x)=g(x)h(x)$ حيث

$$h(x)=x+1 \quad , \quad g(x)=x-1$$

٣-إذا كانت

$$f(x)=x^2-2\in Q[x]$$

فإن $f(x)$ غير قابلة للتحليل على Q لأن ذلك يعني وجود $a,b\in Q$ بحيث أن

$$f(x)=(x-a)(x-b)$$

ومن ثم

$ab=-2$ ، $a+b=0$

ومن ثم $a^2=2$ أي أن $a=\sqrt{2}\in Q$ وهذا غير ممكن .

نظرية :

إذا كان F حقلاً و $f(x)\in F[x]$ حيث

$deg(f(x))=2$ أو $deg(f(x))=3$

فإن f(x) قابلة للتحليل على F إذا كان لكثيرة الحدود f(x) جذرا في F .

البرهان :

نفرض أن f(x) قابلة للتحليل على F فإنه توجد كثيرتي حدود غير ثابتتين $f(x),g(x)\in F[x]$ بحيث أن :

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

و $deg(g(x))<deg(f(x))$ ، $deg(h(x))<deg(f(x))$

وحيث أن

$deg(f(x))=2$ أو $deg(f(x))=3$

فيكون إما أن

$deg(g(x))=1$ أو $deg(h(x))=1$

وفي كلتا الحالتين يكون لكثيرة الحدود f(x) جذرا واحداً في F .

المثاليات وحلقات الباقي

Ideals and quotient ringes

تعريف :

المجموعة الجزئية غير الخالية A من الحلقة R تسمى مثالية من R ونكتب $A \lhd R$ إذا كان :

أ) $a-b \in A$ لكل $a,b \in A$.

ب) $ar\ ,ra \in A$ لكل $r \in R\ ,\ a \in A$.

أمثلة :

١-كل من R,{0} مثالية لكل حلقة R .

٢- nz مثالية في الحلقة Z لكل $n \in Z$ لأنه لكل $a,b \in nZ$ نجد أن a=nx , b=ny حيث $x,y \in Z$ ومن ثم

$$a-b=nx-ny=n(x-y)\in nZ$$

كذلك

$$ra=r(nx)=n(rx)\in nZ$$

$$ar=(nx)r\in nZ$$

وذلك لكل $r \in Z$.

خاصية :

إذا كان كل من A وb مثالية من الحلقة R فكذلك $A \bigcap B$.

خاصية :

إذا كانت الحلقة R ذات عنصر محايد وكانت A مثالية في R تحتوي على العنصر المحايد فإن A=R .

البرهان :

تتحقق هذه العلاقة لأن

$$r \in R \rightarrow r = r1 \in A$$

أي أن $R \subseteq A$ ومن ثم A=R .

نتيجة :

نفرض أن Rحلقة ذات عنصر محايد . إذا كانت المثالية A من R تحتوي على عنصر قابل للانعكاس فإن A=R .

البرهان :

إذا كان $a \in A$ قابل للانعكاس فإن $aa^{-1} = 1 \in A$ وتحقق النتيجه من الخاصية السابقة .

خاصية :

الحلقة الإبدالية ذات العنصر المحايد R تكون حقلاً إذا كانت لا تحتوي على مثالية غير R,{0} .

البرهان :

نفرض أن R حقلاً وأن $\varphi \neq A \lhd R$ فإنه $0 \neq a \in A$ حيث a قابل للانعكاس فإن A=R .

<u>ولإثبات العكس</u> :

نفرض أن R حلقة إبدالية ذات عنصر محايد وأنه لا يوجد مثالية في R غير R,{0} نفرض أن $0 \neq a \in R$ فإن
$aR = \{ar = ra : r \in R\}$ مثالية في R .

فإذا كانت R لا تحتوي على مثاليات غير R,{0} فإن aR=R وحيث أن $1 \in R$ فإنه يوجد $x \in R$ يحقق أن ax=1 ومن ثم فإن a قابل للانعكاس ومن ثم تكون R حقلا .

تعريف :

نفرض أن S مجموعة غير خالية من الحلقة R فإن تقاطع جميع المثاليات في R والتي تحتوي على S ، ويرمز لها بالرمز <S> يسمى المثالية المولدة بالمجموعة S . وإذا كانت

$$S = \{x_1, x_2, \ldots, x_n\}$$

فإن <S> تسمى <u>*مثالية ذات مولدات منتهية*</u>

. (<u>Finitely generatail ided</u>)

تعريف :

إذا كانت $S=\{x\}$ مجموعة جزئية من الحلقة R فإن $<S>$ يسمى *مثالية رئيسية* (Principle ideal).

تعريف :

إذا كان كل مثالية في الحلقة R مثالية رئيسية يسمى R حلقة مثاليات رئيسية (Principle ideal ring).

من التعريفات السابقة نستنتج أن :

$$<S>=\left\{\sum_{i=1}^{n}a_i x_i b_i : a_i, b_i \in R, x_i \in S\right\}$$

وإذا كانت R حلقة إبدالية فإن

$$<x_1, x_2, \ldots, x_n>=\left\{\sum_{i=1}^{n}x_i r_i : r_i \in R\right\}$$

وإذا كانت $S=\{x\}$ فإن :

$$<x>=\{xr+nx : r \in R, n \in Z\}$$

وإذا كانت $1 \in R$ فإن :

$$<x>=\{xr : r \in R\}$$

73

أمثلة :

١-الحلقة التامة Z هي حلقة مثاليات رئيسية تامة لأنه إذا كانت $A \lhd Z$ فإن :

أ) إذا كانت A={0} فإن A=<0>.

ب) إذا كانت $A \neq \{0\}$ فإن A تحتوي على عدداً صحيحاً موجباً .

٢-كل حقل F هو حلقة مثاليات رئيسية تامة فإذا كانت $A \lhd F$ فإن :

أ) إذا كانت A={0} فإن A=<0>.

ب) إذا كانت $A \neq \{0\}$ وكان $0 \neq r \in A$ فإن $r \in F$ ومن ثم فإن r قابلة للانعكاس ومن ثم فإن A=F=<r> وذلك لأن

$$< r >= \{ar : a \in F\} = rF = F$$

٣-إذا كان $A, B \lhd F$ فإن $A \cup B$ قد لا يكون مثالية في R فمثلاً في Z نجد أن كل من A=<2> و B=<3> مثالية في Z بينما $A \cup B \not\lhd F$ لأنه مثلاً $2,3 \in A \cup B$ بينما $2+3 \notin A \cup B$.

تعريف :

إذا كان كل من A,B مثالية في الحلقة R فيعرف مجموعهما A+B وضربهما AB كالآتي :

$$A+B=\{a+b : a\in A \wedge b\in B\}$$

$$AB=\left\{\sum_{i=1}^{n} a_i b_i : a_i \in A \wedge b_i \in B\right\}$$

$A=\{a,b\}$, $B=\{x,y\}$

$A+B=\{a+x,a+y,b+x,b+y\}$

$$AB=\{ax,ay,bx,by,ax+ay,ax+bx,ax+by,\\ ay+bx,ay+by,bx+by,ax+ay+bx,\\ ax+by+ay,ax+bx+by,ay+bx+by,\\ ax+ay+bx+by\}$$

أمثلة :

١- نعلم أن <2>=A و <3>=B مثاليتين في الحلقة Z ونجد أن

$A=\{0,\pm 2,\pm 4,\pm 6,...\}$

$B=\{0,\pm 3,\pm 6,\pm 9,...\}$

$A+B=\{0,\pm 1,\pm 2,\pm 3,\pm 4,\pm 5,\pm 6,...\}$

$\therefore A+B=Z$

$AB=\{0,\pm 6,\pm 12,\pm 18,\pm 24,...\}$

$\therefore AB=\langle 6\rangle$

٢-نعلم أن <4>=A و <6>=B مثاليتين في الحلقة Z ونجد أن

75

$$A=\{0,\pm 4,\pm 8,\pm 12,\ldots\}$$
$$B=\{0,\pm 6,\pm 12,\pm 18,\ldots\}$$
$$A+B=\{0,\pm 2,\pm 4,\ldots\}$$
$$A+B=\langle 2\rangle$$
$$\therefore AB=\langle 24\rangle$$

٣-في الحلقة Z_{12} نجد ان كل من :

$$A=\langle 4\rangle=\{0,4,8\}$$
$$B=\langle 3\rangle=\{0,3,6,9\}$$

مثالية ونجد أن :

$$A+B=Z_{12} \quad , AB=\{0\}$$

٤- نفرض أن $A=\langle x\rangle$ مثالية في $Z[x]$ فإن :

$$A+A=A \quad , AA=A^2=\langle x^2\rangle$$

نظرية :

إذا كان كل من A, B مثالية في الحلقة R فإن :

أ- $A+B \lhd R$, $A\subseteq A+B$, $B\subseteq A+B$.

ب- $AB \lhd R$.

76