(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 :

$$f(m) = f(n)$$
$$\to me = ne$$
$$\to (m-n)e = 0$$

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

$$f(Z_p) \leq R .$$

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

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

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

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

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

$$= a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \ldots + a_k b_0$$

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 :

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

تعريف :

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

أ) $(P(R),+,\cdot)$ حلقة حيث $+$, $\cdot$ 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:

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

$$e = (b_0, b_1, ,..., b_n, 0, ...)$$

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

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

$$\begin{aligned}(a,0,0,...) &= e(a,0,0,...) \\ &= (b_0a, b_1 0, ,..., b_n 0, 0, ...) \\ &= b_0a\end{aligned}$$

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

أي أن b_0 هو العنصر المحايد في R .

جـ) نفرض أن

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

فإن $S \leq P(R)$

ونجد أن

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

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

د) نفرض ان R إبدالية ونفرض أن :

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

$$g = (b_0, b_1, ,..., b_m, 0, ...)$$

فإن

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

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

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

كثيرة حدود فإن :

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

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

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

تعريف :

إذا كانت

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

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 :

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

٤)نفرض أن

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

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

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

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 :

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 , deg (g(x))=m

أي أن :

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

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

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 :

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

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

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

ب) نلاحظ أن $a_m b_n \neq 0$ 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 $a_m b_n \neq 0$ ومن ثم فإن :

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

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 :

$$\deg\left[f(x)+g(x)\right]\leq r$$
$$=\max\left\{m,n\right\}$$

خاصية :

إذا كانت الحلقة R تامة فكذلك R[x] .

البرهان :

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

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

ومن ثم يكون

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

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 و g(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 :

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

توضيح :

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

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.

نظرية :(نظرية الباقي)

إذا كانت R حلقة إبدالية ذات عنصر محايد وكان
$f(x)\in R[x]$, $a\in R$ 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) .

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 كما في المثال الآتي :

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 :

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

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 $\bar{z}$ جذراً لها .

البرهان :

نفرض أن :

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

فإن :