المحاضرة الخامس عشر

ألتطابق الجبري

تطابق كثيرة الحدود:

لتكن: $(1) \rightarrow f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in Z[x]$

كثيرة حدود على حلقة الاعداد الصحيحة Z حيث $a_0, a_1, \ldots, a_n \in Z$, $n \geq 0$ فان f

كثيرة حدود من الدرجة n أي: $degf = n$ أو $degreeof = n$

مثال: اوجد حل المتطابقات الجبرية الاتية:

-1 $\boldsymbol{x^2 - 1 \equiv 0(mod\ 3)}$

نلاحظ ان $Z_3 = \{0,1,2\}$،

$0 - 1 \not\equiv 0(mod\ 3)$

$1 - 1 \equiv 0(mod\ 3)$

$4 - 1 \equiv 0(mod\ 3)$

$x_0 = 1, 2$

-2 $\boldsymbol{x^3 - 2x \equiv 0(mod\ 8)}$

$Z_8 = \{0,1,2,3,4,5,6,7\}$

$x_0 = 0, 4$

تعريف:

لتكن $f, g \in Z[x]$ حيث $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$

نقول Z كثيرتا حدود على حلقة الأعداد الصحيحة $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$

ان f تطابق مقياس m ونكتب: $f(x) \equiv g(x)(modm)$

اذا كان: $a_i \equiv b_i(modm)$ لكل $i = 1 . 2 . 3 \ldots . n$

مثال: اذا كان

$$f(x) = x^3 + 2x + 1,\ g(x) = x^3 + 6x + 5$$

بين ان: $f(x) \equiv g(x) \pmod 4$

الحل:

$$m = 4 \quad \deg f = 3 = n$$

$$a_n = 1 \ , \ a_1 = 2 \ , \ a_0 = 1$$

$$b_n = 1 \ , \ b_1 = 6 \ , b_0 = 5$$

نجد ان :

$$1 \equiv 1 \pmod 4$$

$$2 \equiv 6 \pmod{40}$$

$$1 \equiv 5 \pmod 4 \therefore f(x) \equiv g(x) \pmod 4$$

الدوال العددية

الدالة f التي مجالها مجموعة الأعداد الصحيحة الموجبة ومجالها الصاحب مجموعة الحقيقية أو المركبة تسمي دالة عددية .

تعريف:

يقال أن $f \neq 0$ أنها دالة عددية ضربية إذا كان: $f(m\,n) = f(m)f(n)$ حيث $(m\,,n) = 1$

مثال: 1) دالة اويلر دالة ضريبية.

2) الدالة $f(n) = 1$ دالة ضربية لأن إذا كان $(m\,,n) = 1$ فإن $f(m\,n) = 1$

$$f(m\,n) = f(m)f(n) = 1 \cdot 1 = 1$$

تعريف:

تسمى الدالة f دالة عددية ضربية تماما إذا كانت $f(m\,n) = f(m) \cdot f(n)\ , \forall\ m, n \in R$ بدون شرط $(m, n) = 1$.

مثال:

$$\varphi(2\cdot 6)=\varphi(12)=\varphi(3\cdot 4)$$

$$=\varphi(3)\emptyset(4)=2\cdot 2=4$$

أنظمة الرواسب (البواقي) Residue Systems

أثبتنا في المبرهنة (12) أن علاقة التطابق قياس n هي علاقة تكافؤ على المجموعة Z. وحيث أن كل علاقة تكافؤ تجزئ المجموعة المعرفة عليها الى فصول أو صفوف تكافؤ. اذاً

$$Z/\equiv_n=\{[a]/a\in Z\}$$

تجزئة للمجموعة Z. لكن صف أو فصل التكافؤ $[a]$ والذي يحول العنصر a الى مجموعة عن طريق التطابق

$$\bar{a}=[a]=\{b\in Z: b\equiv a\ (mod\ n)\}$$

$$=\{b\in Z: b=a+nr, r\in Z\}$$

$$=\{a+nr: r\in Z\}.$$

$$\therefore\ \bar{0}=[0]=\{nr: r\in Z\}$$

$$\bar{1}=[1]=\{1+nr: r\in Z\}$$

$$\bar{2}=[2]=\{2+nr: r\in Z\},\ \ldots,$$

$$\overline{n-1}=[n-1]=\{n-1+nr: r\in Z\}$$

$$=\{-1+n(1+r): r\in Z\}$$

$$\bar{n}=[n]=\{n+nr: r\in Z\}$$

$$=\{n(1+r): r\in Z\}=[0]$$

$$\overline{n+1}=[n+1]=\{n+1+nr: r\in Z\}$$

$$=\{1+n(1+r): r\in Z\}=[1],\ \ldots,$$

$$\overline{2n-1}=[2n-1]=\{2n-1+nr: r\in Z\}$$

$$=\{-1+n(2+r): r\in Z\}=[n-1]$$

$$2\bar{n}=[2n]=\{2n+nr: r\in Z\}$$

$$=\{n(2+r): r\in Z\}=[0],\ \ldots,$$

$$[2n+1]=[1],[2n+2]=[2],\ \ldots,[3n-1]=[n-1],$$

$[3n] = [0].$

وعليه فاذا رمزنا للمجموعة $Z/\equiv_n$ بالرمز Z_n نجد أن

$Z_n = \{[0], [1], \dots, [n-1]\}.$

والتي تسمى **مجموعة الرواسب قياس n.**

مثال (1):

$Z_4 = \{[0], [1], [2], [3]\}$ حيث ان,

$[0] = \{0, \mp 4, \mp 8, \dots\}$

$[1] = \{1 + nr\} = \{1 + 0, 1 \mp 4, 1 \mp 8, \dots\}$

$= \{\dots, -7, -3, 1, 5, 9, \dots\}$

$[2] = \{2 + nr\} = \{2 + 0, 2 \mp 4, 2 \mp 8, \dots\}$

$= \{\dots, -6, -2, 2, 6, 10, \dots\}$

$[3] = \{3 + 0, 3 \mp 4, 3 \mp 8, \dots\} = \{\dots, -5, -1, 3, 7, 11, \dots\}.$

مبرهنة (37):

كل عدد صحيح يطابق عدداً وحيداً من الاعداد **0, 1, 2, 3, …, n-1** قياس n.

بصيغة اخرى: اذا كان $a \in Z$ فيوجد عنصر وحيد $r \in Z_n$ بحيث أن

$a \equiv r \ (mod\ n)$

البرهان:

لنفرض أن $a \in Z$ وحسب خوارزمية القسمة، يوجد عددين وحيدين $m, r \in Z$، بحيث ان $a = nm + r, 0 \leq r < n$، وعليهه فأن

$a \equiv r \ (mod\ n), r \in \{0, 1, 2, 3, \dots, n-1\}.$

والان، لإثبات الوحدانية نفرض أن وجود عدد اخر s، بحيث أن

$s \equiv r \ (mod\ n),, s \in \{0, 1, 2, 3, \dots, n-1\}$

اذاً $s \equiv r \ (mod\ n)$، وعليه فأن s=r.

مبرهنة (38): اذا كان $a, b \in Z$ وكان $a \neq b$، فان $a \not\equiv b \ (mod\ n)$.

تعريف: يقال أن $\{a_0, a_1, \dots, a_{n-1}\}$ انها **نظام رواسب تام قياس n** (مكمل قياس n)، اذا كان كل عدد صحيح يطابق عدداً وحيداً من الاعداد $a_0, a_1, \dots, a_{n-1}$ قياس n. اذاً $\{a_0, a_1, \dots, a_{n-1}\}$ نظام رواسب تام قياس n اذا وفقط اذا كان $\{[a_0], [a_1] \dots, [a_{n-1}]\} \in a$ لكل $a \in Z$. يطلق احياناً على المجموعة $\{[a_0], [a_1] \dots, [a_{n-1}]\}$ مجموعة البواقي التامة قياس n.

ملاحظة: لكي نبرهن أن n من الاعداد الصحيحة تمثل نظام رواسي تام قياس n، يكفي ان نثبت ان كل عدد من الاعداد المعطاة يطابق عدداً واحداً فقط من الاعداد $0, 1, 2, \dots, n-1$ قياس n.

مثال:

(أ) أثبت ان المجموعة $C = \{0, -9, 12, 8, 14\}$ تمثل نظام رواسب تام قياس 5.

(ب) أثبت ان المجموعة $D = \{0, \pm 1, \pm 2\}$ تمثل نظام رواسب تام قياس 5.

(ت) هل أن $\{2,4, 6, 8, 11\}$ نظام بواقي تام؟

الحل:

(أ) المجموعة تمثل نظام رواسب تام قياس 5، لان

$0 \equiv 0 \ (mod\ 5)$

$-9 \equiv 1 \ (mod\ 5)$

$12 \equiv 2 \ (mod\ 5)$

$8 \equiv 3 \ (mod\ 5)$

$14 \equiv 4 \ (mod\ 5)$

وبالتالي فان

$S = \{[0], [-9], [12], [8], [14]\}$

هي مجموعة بواقي تامة قياس 5.

(ب) المجموعة تمثل نظام بواقي تامة قياس 5، لان

$0 \equiv 0 \ (mod\ 5)$

$1 \equiv 1 \ (mod\ 5)$

$2 \equiv 2 \ (mod\ 5)$

$-2 \equiv 3 \ (mod\ 5)$

$-1 \equiv 4 \ (mod\ 5)$

(ت) المجموعة لا تمثل نظام بواقي تامة قياس 5، لان

$2 \not\equiv 0 \pmod 5$

$4 \not\equiv 1 \pmod 5$

$6 \not\equiv 2 \pmod 5$

$8 \equiv 3 \pmod 5$

$11 \not\equiv 4 \pmod 5$

نتيجة(14) :

اذا كان $r_1, r_2, \dots, r_n$ نظام رواسب تام قياس n وكان (a, n)=1 حيث أن $a \in Z$، فان:

$ar_1 + b, ar_2 + b, \dots, ar_n + b$ نظام رواسب تام قياس n لكل عدد صحيح b.

نظام الرواسب المختزل قياس n Reduced Residue System

تعريف:

ليكن $S = \{r_1, r_2, \dots, r_n\}$ نظام رواسب تام قياس n. نقول ان المجموعة

$T = \{a \in S: (a, n) = 1\}$ نظام رواسب مختزل قياس n.

مثال:

(أ) اذا كان n=12، فان $\{0,1, 2, \dots, 11\}$ نظام رواسب تام قياس 12. فأن $\{1,5,7, 11\}$ يكون نظام رواسب مختزل قياس 12.

(ب) أذا كان لدينا $\{0, \mp1, \mp2, \mp3, \mp4, \mp5, \mp6\}$ كنظام رواسب تام قياس 12، فعندئذ يكون $\{\mp1, \mp5\}$ نظام رواسب مختزل قياس 12.

ملاحظة:

نلاحظ من المثال اعلاه ان النظامين المختزلين قياس 12 يحتويان على نفس العدد من العناصر لأي عدد n.

وهذا ما سنقدمه بالمبرهنة التالية:
