◄ الدكتور: شوقي الراشد

◄المحاضرة: الأولى

عنوان المحاضرة: لمحة عن المقرر

✓ الرجاء منكم أعزائي الطلبة قراءة هذه المحاضرة لما فيها من معلومات وأمور مهمة ذكرها الدكتور.

محتوى المقرر:

١. مفاهيم أساسية: الحلقة، الحقل، الحلقة الجزئية والتشاكل الحلقي

2. المنطقة الصحيحة (التكاملية) *Integral Domain* ومميز الحلقة

3. حلقة كثيرات الحدود:

- القسمة في حلقة كثيرات الحدود.
- كثيرات الحدود وقابلية الاختزال *Eisensteien crition*

4. المثاليات وحلقة القسمة

- المثاليات والعمليات عليها
- حلقة القسمة
- النظرية الأساسية في التماثل الحلقي
- مبرهنة الباقي الصينية *Chinese Remainder Theorem*
- المثاليات الأولية والأعظمية + مبرهنة *Prime Avoidence*
- الحلقات المحلية *Local rings*

5. التحليل:

- العناصر غير قابلة للتحليل والعناصر الأولية
- المناطق الإقليدية والمثاليات الرئيسية ومناطق التحليل الوحيد $(\gcd \_ \ lcm)$

6. الحلقات النوثيرية والآرتينية.

المراجع العلمية:

١) بنى جبرية 2 منشورات جامعة دمشق.

٢) *J.B.Fraleigh: A first course in abstract Algebra 7th eidition university island*

٣) *M.F.Atiyah: Introduction to commutative Algebra, university of onford 1967*

توزيع المحاضرات:

(الزمرة الأولى) الثلاثاء من الساعة الثامنة للساعة العاشرة
الأربعاء من الساعة العاشرة للساعة الثانية عشر
(الزمرة الثانية) الثلاثاء من الساعة العاشرة للساعة الثانية عشر
الأربعاء من الساعة الثامنة للساعة العاشرة

وقت تواجد الدكتور في المكتب لمراجعته

الثلاثاء من الساعة ١١:٣٠ أو من الساعة ١٤:٣٠
الأربعاء من الساعة ١٢:٠٠

ملاحظات مهمة:

- نوه الدكتور إلى أن أسئلة الامتحان ستكون من الشكل:
  من ١ علامة إلى ٧٥ علامة من المحاضرات.
  من ١ علامة إلى ٢٥ علامة سؤال وظيفة أو سؤال للمتميزين.
- كما ذكر الدكتور أنه يفضل امتلاك كتاب البنى ٢ للمقتدر.
- أكد الدكتور على أهمية الحضور والمتابعة والدراسة (مع فهم المقرر). ☺

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة

نظري

◄ الدكتور: شوقي الراشد

◄ المحاضرة: الثانية عنوان المحاضرة: الحلقة والحقل

المحتوى العلمي: سندرس في هذه المحاضرة:

١. مفاهيم أساسية (تعريف الحلقة مع أمثلة).
٢. الحلقة الجزئية مع مبرهنة.
٣. أمثلة عن الحلقة الجزئية.
٤. تعريف الحقل مع أمثلة.

تعريف الحلقة: لتكن $R \neq \emptyset$ مجموعة جزئية وغير خالية ومزودة بقانوني تشكيل داخليين نرمز للأول بالرمز $(+)$ والثاني بالرمز $(.)$، نقول عن النظام الثلاثي أو الثلاثية $(R, +, .)$ أنها حلقة إذا وفقط إذا تحققت الشروط الآتية:

الشرط الأول: $(R, +)$ زمرة تبديلية، أي تحقق الشروط التالية

- القانون $(+)$ قانون تشكيل داخلي أي: $\forall a, b \in R : a + b \in R$
- القانون $(+)$ قانون تشكيل تجميعي أي:
$\forall a, b, c \in R : \quad a + (b + c) = (a + b) + c$
- يوجد عنصر حيادي بالنسبة لعملية الجمع ونرمز له بالرمز (0) يحقق:
$\forall \, a \in R : a + 0 = 0 + a = a$
- لكل عنصر نظير جمعي:

$$\forall \, d \in R : \exists - d \in R : d + (-d) = d - d = 0$$

من الشروط الأربعة السابقة نجد أن $(R, +)$ زمرة.

- وتكون الزمرة تبديلية إذا تحقق: $\forall \, a, b \in R : a + b = b + a$

الشرط الثاني: $(R, .)$ نصف زمرة، أي يتحقق الشرطين:

$$\forall \, a, b, c \in R :$$

- ♦ القانون $(.)$ هو قانون تشكيل داخلي في R أي: $a.b \in R$
- ♦ القانون $(.)$ هو قانون تشكيل تجميعي في R أي: $a.(b.c) = (a.b).c$

الشرط الثالث: الضرب $(.)$ توزيعي على الجمع $(+)$ من اليمين ومن اليسار:

$$\forall\, a,b,c \in R$$

- من اليسار: $a.(b+c) = ab + ac$
- من اليمين: $(b+c).a = ba + ca$

تذكرة: قانون التشكيل: تطبيق منطلقه جداء ديكارتي ومستقره $\mathbb{R}$

ملاحظة ١ : نقول عن الحلقة R أنها تبديلية إذا تحقق الشرط:

$$\forall\, a,b \in R\,;\, a.b = b.a$$

أي نقول عن R أنها تبديلية إذا كانت تبديلية بالنسبة للعملية الثانية في الثلاثية $(R,+,.)$

ملاحظة ٢: إذا وجد عنصر $e \in R$ يحقق:

$$\forall\, a \in R : a.e = e.a = a$$

فإن e يمثل الحيادي (الضربي) ويدعى واحد الحلقة ونرمز له بـ (1) وتسمى R في حال وجوده بالحلقة الواحدية أو ذات عنصر محايد.

- صفر الحلقة دائماً موجود أما واحد الحلقة ليس بالضرورة أن يكون موجود.

ملاحظة ٣: إذا كانت R حلقة واحدية نقول عن العنصر $a \in R$ أنه قابل للقلب في R إذا وفقط إذا تحقق الشرط $\exists\, b \in R : a.b = b.a = 1$

ونرمز لمقلوب a بـ $a^{-1} = b$ ولمجموعة كل العناصر القابلة للقلب في R بالرمز $U(R)$

- وجود عنصر قابل للقلب يعني أن الحلقة واحدية.

أمثلة:

١) $R = (\mathbb{Z},+,.)$ حلقة تبديلية واحدية فيها $U(R) = \{\pm 1\}$

٢) $R = (\mathbb{Z}_n,\oplus,\otimes)$ حلقة تبديلية واحدية بالنسبة لعملية الجمع والضرب بالمقاس n والعنصر المحايد هو ١

حيث $\mathbb{Z}_n = \{0,1,2,3,\dots,n-1\}$

$\forall\, x,y \in \mathbb{Z}_n\,;\, x \oplus y = (x+y) mod\ n$ (باقي قسمة $x+y$ على n)

$x \otimes y = (x.y) mod\ n$ (باقي قسمة $x.y$ على n)

مثال توضيحي: عندما $n = 6$ فإن $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$

$$1 \oplus 2 = 3 < 6$$

$$1 \oplus 5 = 0$$

لأن $(1+5) mod\ 6 = 0$ [يعني باقي قسمة $1+5=6$ على ٦ هو ٠ ومنه ناتج جمع العددين $1, 5$ بالمقاس 6 هو الصفر]

$$2 \oplus 4 = 0$$

لأن $6\ mod\ 6 = 0$ (يعني باقي قسمة 6 على 6 هو (0) فالناتج (0))

$$3 \oplus 4 = 1$$

لأن $7 mod\ 6 = 1$ (باقي قسمة ٧ على ٦ هو ١)

$$4 \oplus 4 = 2$$

لأن $8\ mod\ 6 = 2$ (باقي قسمة ٨ على ٦ هو ٢)

وعلى هذا النمط نستنتج الجدول

⊕	٠	١	٢	٣	٤	٥
٠	٠	١	٢	٣	٤	٥
١	١	٢	٣	٤	٥	٠
٢	٢	٣	٤	٥	٠	١
٣	٣	٤	٥	٠	١	٢
٤	٤	٥	٠	١	٢	٣
٥	٥	٠	١	٢	٣	٤

٣) $R = (M_{m\times n}(\mathbb{R}), +, .)$ حلقة ليست تبديلية (لأن الضرب غير تبديلي في المصفوفات) وليست واحدية.

٤) $(M_{n\times n}, +, .)$ حلقة واحدية وليست تبديلية

٥) $R = \mathbb{Z}(\sqrt{p}) = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$ وهي ممدد مجموعة الأعداد الصحيحة $\mathbb{Z}$ حيث p عدد أولي

$$\forall\, x, y \in \mathbb{Z}(p) : a_1, a_2, b_1, b_2 \in \mathbb{Z}\,; x = a_1 + b_1\sqrt{p}\,, y = a_2 + b_2\sqrt{p}$$

ومنه

$$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{p}$$

$$x.y = (a_1.a_2 + b_1.b_2.p) + (a_1.b_2 + a_2.b_1)\sqrt{p}$$

عندئذٍ $(R, +, .)$ حلقة تبديلية واحدية فيها:

$$U(R) = \{\pm 1\} \quad , \quad 1 = 1 + 0\sqrt{p}$$

حيث

$$(1 + 0\sqrt{p})(1 + 0\sqrt{p})^{-1} = (1 + 0\sqrt{p})^{-1}(1 + 0\sqrt{p}) = 1$$

مبرهنة: لتكن R حلقة وليكن $a,b,c \in R$ عندئذٍ القضايا التالية صحيحة:

١. $0.a = a.0 = 0$
٢. $a(-b) = (-a)b = -ab$
٣. $(-a)(-b) = a.b$
٤. $a(b-c) = ab - ac$

البرهان: -إثبات الطلب (١):

$$a.0 = a(0+0) \Rightarrow a.0 = a.0 + a.0$$

نجمع نظير $(a.0)$ إلى كل من الطرفين ومنه:

$$a.0 - a.0 = a.0 + a.0 - a.0$$

ومنه $\boxed{0 = a.0}$

-إثبات الطلب (٢):

بما أن $-(ab) + (ab) = 0 \quad \dots (1)$

وأن $a(-b) + ab = a(-b+b) = a.0 = 0 \quad \dots (2)$

ومن 1 , 2 نجد: $-(ab) + (ab) = a(-b) + ab \quad \dots (3)$

وبإضافة نظير العنصر ab إلى الطرفين في العلاقة (3) نجد أن

$$\boxed{-ab = a(-b)}$$

-إثبات الطلب (٣):

$$(-a)(-b) = -\big(a(-b)\big) = -\big(-(ab)\big) = ab$$

ومنه: $\boxed{(-a)(-b) = ab}$

-إثبات الطلب (٤):

$$a(b-c) = a\big(b + (-c)\big) = ab + a(-c) = ab - ac$$

مبرهنة: لتكن R حلقة و $a,b \in R$ وليكن n,m أعداد صحيحة عندئذٍ:

١. $(ma)b = a(mb) = m(ab)$
٢. $(ma)(nb) = mn(ab)$

٣. $\forall\, m,n \in \mathbb{Z}^+ \,;\, (a^m)^n = a^{m.n} \quad , \quad a^m.a^n = a^{m+n}$

البرهان: -إثبات الطلب (١):

البرهان على أن $(ma)b = m(ab)$ نميز حالتين:

الحالة الأولى: إذا كان $m \geq 0$ عندئذٍ:

$$(ma)b = \underbrace{(a + a + \cdots + a)}_{m \text{ مرة}}\, b = \underbrace{ab + ab + \cdots + ab}_{m \text{ مرة}} = m(ab)$$

الحالة الثانية: إذا كان $m < 0$ عندئذ:

$$(ma)b = [(-m)(-a)]b = (-m)[(-a)b] = (-m)[-(ab)] = m(ab)$$

وبشكل مشابه نجد أن $m(ab) = a(mb)$

-إثبات الطلب (٢):

نميز حالتان:

الحالة الأولى: العددان m,n موجبان عندئذٍ:

$$(ma)(nb) = \underbrace{(a + a + \cdots + a)}_{m \text{ مرة}}\underbrace{(b + b + \cdots + b)}_{n \text{ مرة}}$$

$$= \underbrace{a\underbrace{(b + b + \cdots + b)}_{n \text{ مرة}} + a\underbrace{(b + b + \cdots + b)}_{n \text{ مرة}} + \cdots + a\underbrace{(b + b + \cdots + b)}_{n \text{ مرة}}}_{m \text{ مرة}}$$

$$= \underbrace{\underbrace{(ab + ab + \cdots + ab)}_{n \text{ مرة}} + \underbrace{(ab + ab + \cdots + ab)}_{n \text{ مرة}} + \cdots + \underbrace{(ab + ab + \cdots + ab)}_{n \text{ مرة}}}_{m \text{ مرة}}$$

$$= \underbrace{ab + ab + \cdots + ab}_{mn \text{ مرة}} = (mn)(ab)$$

الحالة الثانية: كل من m,n أعداد سالبة، عندئذٍ:

$$(ma)(nb) = [(-m)(-a)][(-n)(-b)] = [(-m)(-n)][(-a)(-b)]$$
$$= (mn)(ab)$$

الحالة الثالثة: العددان n,m من إشارتين مختلفتين، ولنفرض أن $n < 0$ ، $m > 0$ عندئذٍ:

$$(ma)(nb) = (ma)[(-n)(-b)] = [m(-n)][a(-b)] = [-(mn)][-(ab)]$$
$$= (mn)(ab)$$

إثبات الطلب (٣):

$$\forall\, m,n \in \mathbb{Z}^+ \,;\, (a^m)^n = \underbrace{a^m . a^m . \dots . a^m}_{n \text{ مرة}}$$

$$= \underbrace{\underbrace{(a.a.\dots.a)}_{m \text{ مرة}}\underbrace{(a.a.\dots.a)}_{m \text{ مرة}}.\dots.\underbrace{(a.a.\dots.a)}_{m \text{ مرة}}}_{n \text{ مرة}} = a^{mn}$$

$$a^m . a^n = \underbrace{(a.a.\dots.a)}_{m \text{ مرة}}\underbrace{(a.a.\dots.a)}_{n \text{ مرة}} = \underbrace{(a.a.\dots.a)}_{m+n \text{ مرة}} = a^{m+n}$$

مثال(١): لتكن R حلقة واحدية أثبت أن $(U(R),+,.)$ زمرة.

-إن $1 \in U(R) \Leftarrow U(R) \neq \emptyset$

-لنتحقق من شروط الزمرة:

$$\forall\, a,b \in U(R)\,;\exists\, c,d \in R : ac = ca = 1\,, bd = db = 1$$

١) من اليمين: $(ab)(dc) = a(bd)c = ac = 1$

من اليسار: $(dc)(ab) = d(ca)b = db = 1$

ومنه فإن $(.)$ داخلي.

٢) التجميعية:

$$\forall\, a,b,c \in U(R) \subseteq R : (ab)c = a(bc)$$

حيث الضرب في R تجميعي.

٣) الحيادي: $1 \in U(R)$ حيث $\forall\, a \in U(R) : 1.a = a.1 = a$

٤) النظير الضربي (المقلوب)

$$\forall\, a \in U(R) : \exists\, b \in R\,; ab = ba = 1$$

ومما سبق نجد أن $U(R)$ زمرة تبديلية.

مثال(٢): حلقة بول: لتكن R حلقة تحقق:

$$\forall\, a \in R : a = a^2$$

عندئذٍ R تبديلية.

الحل: $\forall\, a,b \in R : a + b = (a+b)^2 = a^2 + b^2 + \underline{a.b + b.a}$

لم نكتب $2ab$ لأن الضرب هنا ليس تبديلي

ومنه: $a + b = a^2 + b^2 + ab + ba$

بما أن $a = a^2$ و $b = b^2$ فإن: $0 = ab + ba$

ومنه $ab = -ba$

$$\forall\, x \in R : x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2$$

بما أن $x = x^2$ فإن $0 = x^2 + x^2 \quad \Leftarrow \quad x^2 = -x^2$

ومنه $x = -x$ وبالتالي: من أجل $x = b.a$

$$\forall\, a, b \in R : ab = -x = x = ba$$

ومنه R تبديلية.

تعريف الحقل: لتكن $F \neq \emptyset$ مجموعة غير خالية مزودة بقانوني تشكيل داخلين $(+)$ و $(.)$ نقول عن النظام الثلاثي $(F, +, .)$ أنه حقل إذا وفقط إذا تحققت الشروط التالية:

١- $1 \neq 0$

٢- $(F, +)$ زمرة تبديلية.

٣- $(F \backslash \{0\}, .)$ زمرة تبديلية.

٤- $(.)$ الضرب توزيعي على الجمع $(+)$:

$$\forall\, a, b, c \in F : a.(b + c) = ab + ac$$

موجز: نقول عن هذا النظام الثلاثي $(F, +, .)$ أنه حقل إذا كانت $(F, +, .)$ أنه حقل إذا كانت $(F, +, .)$ حلقة تبديلية واحدية وكل عنصر مغاير للصفر له مقلوب في F و $1 \neq 0$

أمثلة:

- $(\mathbb{Q}, +, .)$ حقل
- $(\mathbb{R}, +, .)$ حقل
- $(\mathbb{C}, +, .)$ حقل
- $(\mathbb{Q}\sqrt{p}, +, .)$ حقل

كل حقل هو حلقة ولكن ليست كل حلقة هي حقل مثال على ذلك $\mathbb{Z}$ هي حلقة وليست حقل لأن $2 \in \mathbb{Z}$ نظيرها $\frac{1}{2}$ و $\frac{1}{2}$ لا ينتمي للزمرة.

الحلقات الجزئية:

تعريف: لتكن $(R, +, .)$ حلقة و $\emptyset \neq S \subseteq R$ نقول عن S أنها حلقة جزئية في R إذا وفقط إذا كانت $(S, +, .)$ حلقة بحد ذاتها ونرمز بـ $S \leq R$

أمثلة:

١) إذا كانت R حلقة فإن كل حلقة هي حلقة جزئية من نفسها أي $R \leq R$ والصفر حلقة جزئية لكل حلقة $\{0\} \leq R$

٢) $R = (\mathbb{Z}, +, .)$ فإن $S = 2\mathbb{Z} \leq R$

٣) $R = (\mathbb{Z}_6, \oplus, \otimes)$ فإن $S = 2\mathbb{Z}_6 = \{0,2,4\} \leq R$

وظيفة: ((تترك للطالب كتفصيل))

تمرين (١): بين أياً من الأنظمة الرياضية التالية:

حلقة ، حلقة جزئية ، حلقة واحدية ، حقل

١- $(n\mathbb{Z}, +, .) \Leftarrow$ حلقة تبديلية ليست واحدية.
٢- $(\mathbb{Z}^+, +, .) \Leftarrow$ حلقة تبديلية وواحدية.
٣- $(2\mathbb{Z} \times \mathbb{Z}, +, .) \Leftarrow$ حلقة تبديلية وليست واحدية.
٤- $(\mathbb{Z}\sqrt{2}, +, .) \Leftarrow$ حلقة تبديلية واحدية.
٥- $(\mathbb{Q}\sqrt{3}, +, .) \Leftarrow$ حقل

تمرين (٢): أوجد العناصر القابلة للقلب في كل من الحلقات التالية:

١- $(\mathbb{Z}_4, \oplus, \otimes) \Leftarrow U(\mathbb{Z}_4) = \{1,3\}$
٢- $(\mathbb{Z}_{12}, \oplus, \otimes) \Leftarrow U(\mathbb{Z}_{12}) = \{1,5,7,11\}$
٣- $(\mathbb{Z} \times \mathbb{Z}, +, .) \Leftarrow U(\mathbb{Z} \times \mathbb{Z}) = \{\pm 1, \pm 1\}$
٤- $(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}, +, .) \Leftarrow U(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}) = \{\pm 1, \mathbb{Q}^+, \pm 1\}$

ملاحظة: $x \in U(\mathbb{Z}_n) \Leftrightarrow gcd(x, n) = 1$

مثال على ذلك في $\mathbb{Z}_6$ نجد أن $U(\mathbb{Z}_6) = \{1,5\}$

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة

◄ دكتور المادة: شوقي الراشد

◄ المحاضرة: الثالثة عنوان المحاضرة: تعريف الحلقة

المحتوى العلمي: سندرس في هذه المحاضرة.

1. **الحلقة والحقل.**
2. **التشاكل الحلقي.**

مبرهنة الحلقات الجزئية: لتكن $(R,+.)$ حلقة و $\emptyset \neq S \subseteq R$ إن $S \leq R$ إذا وفقط إذا تحقق الشرطان:

- $\forall\, a, b \in S : a - b \in S$
- $\forall\, a, b \in S : a.b \in S$

البرهان:

➢ لزوم الشرط: لنفرض أن $s \leq R$ أي لنفرض أن S حلقة جزئية من R عندئذٍ S تحقق جميع شروط الحلقة ومنه:

$$\forall\, a, b \in S \;;\; a, -b \in S : a - b = a + (-b) \in S$$
$$\forall\, a, b \in S : a.b \in S$$

فالشرطان محققان.

➢ كفاية الشرط: لنفرض الشرطان محققان ولنثبت أن S حلقة.

- الحيادي: $\forall\, a \in S : 0 = a - a \in S$
- النظير الجمعي: $\forall\, a \in S : 0 \in S\,,\; -a = 0 - a \in S$
- قانون داخلي: $\forall\, a, b \in S :\; -b \in S \;\Rightarrow a + b = a - (-b) \in S$
- تجميعي: $\forall\, a, b, c \in S \subseteq R : (a + b) + c = a + (b + c)$
- تبديلي: $\forall\, a, b \in S \subseteq R : a + b = b + a$

- مما سبق نجد أن $(s,+)$ زمرة تبديلية.

- الضرب داخلي: $\forall\, a, b \in S : a.b \in S$
- الضرب تجميعي: $\forall\, a, b, c \in S \subseteq R : a.(b.c) = (a.b).c$

- ومنه $(S,.)$ نصف زمرة.

- من اليسار $\forall\ a,b,c \in S \subseteq R : a.(b+c) = a.b + a.c$
- من اليمين $\forall\ a,b,c \in S \subseteq R : (b+c).a = b.a + c.a$

- ومنه الضرب توزيعي على الجمع

ومما سبق نجد أن $(S,+,.)$ حلقة.

ملاحظة: لتكن R حلقة تبديلية و $R \le S$ فإن S تبديلية.

سؤال (١): إذا كانت R حلقة و $S \le R$ ويوجد في R حيادي (ضربي) هل من الضروري أن تحوي S حيادي؟؟

لا، مثال على ذلك:

$R = (\mathbb{Z},+,.)$ و $S = (2\mathbb{Z},+,.)$ حيث $S \le R$ الحيادي في R هو (1) ولكن غير موجود في S

سؤال (٢): هل من الممكن وجود الحيادي في S وعدم وجوده في R حيث $S \le R$ ؟

نعم، مثال على ذلك:

$$R = \left(\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in R\right\},+,.\right)\ ,S = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R\right\}$$

حيث $S \le R$ و $1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

سؤال (٣): هل من الممكن وجود في R حيادي و S حيادي مختلف؟

نعم، مثال على ذلك:

$$R = (M_{2\times 2}(\mathbb{R}),+,.)\ ,S = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R\right\}$$

حيث $S \le R$ ، $1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

سؤال (٤): هل تقاطع الحلقات الجزئية هي حلقة جزئية؟

مبرهنة: إذا كانت R حلقة فإن تقاطع أي مجموعة غير خالية من الحلقات الجزئية في R هو حلقة جزئية في R .

البرهان:

لنفرض أن $\{S_i \,:\, \forall\, i \in I\}$ هي أسرة من الحلقات الجزئية في R

- بما أن $0 \in S_i : \forall\, i \in I$ فإن $0 \in \cap_{i\in I} S_i = S$ ومنه $S \neq \emptyset$
- ليكن $x, y \in \cap_{(i\in I)} S_i$ وعندئذ بما أن $\forall\, i \in I : x, y \in S_i$

وبما أن S_i حلقة جزئية في R فإن:

$$\forall\, i \in I\,; x - y \in S_i \ \Rightarrow x - y \in \cap_{i\in I} S_i = S$$

وبالتالي الشرط الأول محقق.

وأيضاً لما كانت S_i حلقة جزئية في R فإن:

$$x.y \in S_i : \forall\, i \in I \ \Rightarrow x.y \in \cap_{(i\in I)} S_i = S$$

ومنه S هي حلقة جزئية من الحلقة R أي $S \leq R$.

سؤال (٥): هل الاجتماع حلقة جزئية ؟

تمرين: لتكن R حلقة و $S_1, S_2 \leq R$

١. بين أن ليس بالضرورة أن يكون $S = S_1 \cup S_2 \leq R$
٢. $S = S_1 \cup S_2 \leq R$ إذا وفقط إذا $S_1 \subseteq S_2$ أو $S_2 \subseteq S_1$

الحل:

١. اجتماع حلقتين جزئيتين من الحلقة ليس بالضرورة أن يكون حلقة جزئية.
مثال على ذلك: لنأخذ $R = \mathbb{Z}$ ولنأخذ حلقتين جزئيتين من حلقة الأعداد الصحيحة ولتكن
$$S_1 = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$$
$$S_2 = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$$
نجد أن $2{,}3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ ولكن $3 - 2 = 1 \ \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ ومنه فإن $2\mathbb{Z} \cup 3\mathbb{Z}$ ليست حلقة جزئية في حلقة الأعداد الصحيحة $\mathbb{Z}$

٢. لنفرض $R = \mathbb{Z} = \{0, \pm 1, \pm 2 \pm 3, \dots\}$ ولتكن $S_1 \leq R$ و $S_2 \leq R$ حيث
$$S_1 = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \dots\}$$

$$S_2 = 4\mathbb{Z} = \{0, \pm 4, \pm 8, \pm 12, \dots\}$$

نجد أن $S_2 \subseteq S_1$ حيث $4\mathbb{Z} \subseteq 2\mathbb{Z}$ ومنه:

$$S = S_1 \cup S_2 = 2\mathbb{Z} \cup 4\mathbb{Z} = 2\mathbb{Z}$$

وبالتالي $S = 2\mathbb{Z} \leq R$

وبالتالي نجد أن اجتماع حلقتين جزئيتين من الحلقة R هو عبارة عن حلقة جزئية في R بشرط أن تكون إحدى الحلقتين الجزئيتين محتواه في الأخرى.

التشاكل الحلقي:

تعريف: لتكن $(S, +, .)$ و $(R, +, .)$ حلقات عندئذٍ نقول عن التطبيق $\varphi: R \to S$ أنه تشاكل حلقي (Homomorphism) إذا تحققت الشروط التالية:

$$\forall\, a, b \in R$$

$$1)\;\; \varphi(a + b) = \varphi(a) + \varphi(b)$$

$$2)\;\; \varphi\left(a \underset{\text{الضرب معرف على } R}{\cdot} b\right) = \varphi(a) \underset{\text{الضرب معرف على } S}{\cdot} \varphi(b)$$

تعريف النواة: ليكن $\varphi: R \to S$ تشاكل حلقي نسمي المجموعة:

$$\ker \varphi = \{a : a \in R\, ; \varphi(a) = o_S\}$$

بنواة التشاكل φ حيث 0 هو الحيادي الجمعي في S .

تعريف المستقر الفعلي: ليكن $\varphi: R \to S$ تشاكل حلقي نسمي المجموعة:

$$Im(\varphi) = \varphi(R) = \{\varphi(r) \in S : r \in R\}$$

المستقر الفعلي أو الصورة المباشرة لـ R (وهو جزء من S)

مبرهنة: ليكن $\varphi: R \to S$ تشاكل حلقي عندئذ القضايا التالية صحيحة:

١) $\varphi(0_R) = 0_S$

٢) $\forall\, a \in R : \varphi(-a) = -\varphi(a)$

٣) $B \leq S\, ;\, \varphi^{-1}(B) \leq R$

٤) $A \leq R\, ; \varphi(A) \leq S$

٥) $\ker \varphi \leq R \quad , \quad Im(\varphi) \leq S$

٦) φ متباين $\Leftrightarrow \ker \varphi = \{0_R\}$

البرهان:

١) إن $\varphi(0)$ يمكن أن تكتب بالشكل: $\varphi(0) = \varphi(0+0)$
وبما أن φ تشاكل حلقي فإن: $\varphi(0) = \varphi(0) + \varphi(0)$
نطرح من الطرفين $\varphi(0)$ ومنه نجد: $0_S = \varphi(0_R)$

٢) ليكن $a \in R$ عندئذ $-a \in R \Leftarrow -a + a = 0$ حسب الطلب (1) وبما أن φ تشاكل حلقي يكون لدينا

$$\varphi(-a+a) = \varphi(-a) + \varphi(a) = \varphi(0) = 0$$

نطرح من الطرفين $-\varphi(a)$ فنجد:

$$\varphi(-a) = -\varphi(a)$$

٣) لنعرف المجموعة $\varphi^{-1}(B) = \{a \in R : \exists\, b \in B\,,\ b = \varphi(a)\}$

$$\exists\, 0_S \in B\,; 0_S = \varphi(0_R) \Rightarrow 0_R \in \varphi^{-1}(B) \Rightarrow \varphi^{-1}(B) \neq \emptyset$$

$$\forall\, a_1, a_2 \in \varphi^{-1}(B) : \exists\, b_1, b_2 \in B$$

بحيث $b_1 = \varphi(a_1) \quad , \quad b_2 = \varphi(a_2)$

الشرط الأول من شروط الحلقة الجزئية:

$$\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) = b_1 - b_2 \in B$$

$$\Rightarrow a_1 - a_2 \in \varphi^{-1}(B)$$

الشرط الثاني:

$$\varphi(a_1 . a_2) = \varphi(a_1).\varphi(a_2) = b_1 . b_2 \in B$$

$$\Rightarrow a_1 . a_2 \in \varphi^{-1}(B)$$

وبالتالي $\varphi^{-1}(B)$ حلقة جزئية في R أي أن $\varphi^{-1}(B) \leq R$

٤) بفرض أن A حلقة جزئية في R فإن $\varphi(A) = \{\varphi(0) : a \in A\}$
وبما أن $0 \in A$ عندئذٍ $\varphi(0) \in \varphi(A)$ إذاً $\varphi(A) \neq \emptyset$
ليكن $x, y \in \varphi(A)$ عندئذ يوجد $a, b \in A$ بحيث $\varphi(a) = x \ , \ \varphi(b) = y$

$$x - y = \varphi(a) - \varphi(b) = \varphi(a) + \varphi(-b) = \varphi(a-b) \in \varphi(A)$$

فالشرط الأول محقق:

$$x.y = \varphi(a).\varphi(b) = \varphi(a.b) \in \varphi(A)$$

والشرط الثاني محقق:
ومنه $\varphi(A)$ حلقة جزئية في S .

٥) إثبات أن $\ker\varphi \leq R$ ، نعلم أن: $\ker\varphi = \{a : a \in R\,;\ \varphi(a) = 0_S\}$
نعلم أن $0_R \in R$ وبما أن $\varphi(0_R) = 0_S$ فإن $0_R \in \ker\varphi$ وبالتالي $\ker\varphi \neq \emptyset$
لنبرهن أن $\ker\varphi$ حلقة جزئية في R
ليكن $a, b \in \ker\varphi$ عندئذ $\varphi(b) = 0_S \ , \ \varphi(a) = 0_S$
الشرط الأول

$$\varphi(a-b) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b) = 0_s - 0_s = 0_s$$

الشرط الثاني $\varphi(\mathrm{a.b}) = \varphi(a).\varphi(b) = 0_S.0_S = 0_S$

وبالتالي نجد أن $\ker\varphi \leq R$

- إثبات أن $Im(\varphi) \leq S$ نعلم أن:

$$Im(\varphi) = \varphi(R) = \{\varphi(r) \in S : r \in R\}$$

- بما أن $0_R \in R$ فإن $\varphi(0_R) = 0_S \in S$ ومنه $\varphi(0_R) \in Im\,\varphi$ ومنه $Im(\varphi) \neq \emptyset$
- لنثبت أن $Im(\varphi)$ حلقة جزئية في S

ليكن $x, y \in Im(\varphi)$ عندئذ يوجد $a, b \in R$ بحيث:

$$x = \varphi(a) \quad , \quad y = \varphi(b)$$

$$x - y = \varphi(a) - \varphi(b)$$
$$= \varphi(a) + \varphi(-b)$$
$$= \varphi(a - b) \in Im(\varphi)$$

$$x.y = \varphi(a).\varphi(b) = \varphi(a.b) \in Im(\varphi)$$

ومنه $Im(\varphi)$ هي حلقة جزئية من S

٦) نريد إثبات أن φ متباين $\Leftrightarrow \ker\varphi = \{0\}$

$\Rightarrow$ لنفرض أن $\ker\varphi = \{0\}$ ولنثبت أن φ متباين.

$$\forall x, y \in R : \varphi(x) = \varphi(y) \Rightarrow \varphi(x) - \varphi(y) = 0_S$$
$$\Rightarrow \varphi(x) + \varphi(-y) = 0_S \Rightarrow \varphi(x - y) = 0_S \Rightarrow x - y \in \ker\varphi = \{0_R\}$$
$$\Rightarrow x - y = 0_R \Rightarrow x = y$$

ومنه φ متباين.

$\Leftarrow$ لنفرض أن $\varphi: R \to S$ متباين وبما أن $\ker\varphi$ حلقة جزئية من R فإن $0_R \in \ker\varphi$

ومنه $\{0_R\} \subseteq \ker\varphi$

ولنثبت الاحتواء المعاكس ليكن $x \in \ker\varphi$ بالتالي $\varphi(x) = 0_S$ وبما أن φ تشاكل حلقي وأن $\varphi(0_R) = 0_S$ بالتالي $\varphi(x) = \varphi(0_R)$ ومنه $x = 0_S$ لأن φ متباين.

ومنه $\ker\varphi \subseteq \{0_R\}$

ومن الإحتوائين نجد أن $\ker\varphi = \{0\}$

أمثلة عن التشاكل:

١) لدينا $R = (\mathbb{Z}, +, .)$ و $S = (\mathbb{Z}_n, \oplus, \otimes)$ حلقات $\varphi : R \to S$ تطبيق معرف بالشكل:

$$\forall\, r \in R\, ; \varphi(r) = r(mod\ n)$$

$$\forall\, a, b \in R:$$

$$(1) \quad \varphi(a+b) = (a+b)\ mod\ n = a\ mod\ n + b\ mod\ n = \varphi(a) + \varphi(b)$$

$$(2) \quad \varphi(a.b) = (a.b)\ mod\ n = (a\ mod\ n)(b\ mod\ n) = \varphi(a).\varphi(b)$$

ومنه φ تشاكل حلقي

٢) $R = (\mathbb{Z}, +, .)$ و $S = (2\mathbb{Z}, +, .)$ حلقتين.

ولدينا التطبيق $\varphi : R \to S$ المعرف بالشكل: $\forall\, r \in R : \ \varphi(r) = 2r$

هل φ تشاكل حلقي؟

$$\forall\, r_1, r_2 \in R$$

$$(1) \quad \varphi(r_1 + r_2) = 2(r_1 + r_2) = 2r_1 + 2r_2 = \varphi(r_1) + \varphi(r_2)$$

$$(2) \quad \varphi(r_1.r_2) = 2(r_1.r_2)$$

$$\varphi(r_1) = 2r_1 \ , \ \ \varphi(r_2) = 2r_2 \ \Rightarrow \varphi(r_1).\varphi(r_2) = 4r_1r_2$$

وبالتالي الشرط الثاني يختل حيث: $\varphi(r_1.r_2) = 2(r_1.r_2) \neq 4r_1r_2 = \varphi(r_1)\varphi(r_2)$

٣) $R = (\mathbb{Z}_4, +, .)$ و $S = (\mathbb{Z}_6, +, .)$ حلقتين

ولدينا التطبيق $\varphi : R \to S$ المعرف بالشكل:

$$\forall\, r \in R : \ \varphi(r) = 3r$$

هل φ تشاكل حلقي؟

$$\forall\, r_1, r_2 \in R$$

$$(1) \quad \varphi(r_1 + r_2) = 3(r_1 + r_2) = 3r_1 + 3r_2 = \varphi(r_1) + \varphi(r_2)$$

$$(2) \quad \varphi(r_1.r_2) = \overbrace{3(r_1.r_2) = 9}^{\text{9 نفسها 3 بالمقاس 6}}(r_1.r_2) = 3r_1.3r_2 = \varphi(r_1).\varphi(r_2)$$

ومنه φ تشاكل حلقي ونواته هي $\ker\varphi = \{0,2\}$

٤) R حلقة تبديلية واحدية $a \in U(R)$

ولدينا التطبيق $\varphi_a : R \to R$

معرف بالشكل: $\forall\, x \in R : \ \varphi_a(x) = axa^{-1}$

هل هي تشاكل حلقي؟ وهل هو تماثل؟

$$\forall\, x, y \in R;$$

$$(1) \quad \varphi_a(x+y) = a(x+y)a^{-1} = (ax+ay)a^{-1} = axa^{-1} + aya^{-1} = \varphi_a(x) + \varphi_a(y)$$

$$(2)\quad \varphi(x.y) = a(x.y)a^{-1} = a(x.1s.y)a^{-1} = ax(a^{-1}.a)ya^{-1}$$
$$= (axa^{-1}).(aya^{-1}) = \varphi_a(x).\varphi_a(y)$$

ومن φ_a تشاكل حلقي.

لنثبت أنه تماثل: (بما أن φ_a تشاكل بقي إثبات أنه متباين وغامر ليكون تماثل)

$$(1)\quad \forall\, x,y \in R : \varphi_a(x) = axa^{-1} \;\;,\;\; \varphi_a(y) = aya^{-1}$$

بحيث $\varphi_a(x) = \varphi_a(y)$

نضرب بـ a من اليمين $ax = ay$

نضرب بـ a^{-1} من اليسار $x = y$

ومنه φ_a متباين

(2) ليكن $Z \in R$ عندئذٍ يوجد $z \in R$ بحيث: $Z = aza^{-1}$

$\varphi_a(z) = aza^{-1} = Z \Leftarrow$ φ_a غامر $\Leftarrow$ φ_a تماثل

سؤال: ما هي علاقة c بـ R^2 ؟؟ إن c هي نفسها R^2

٥) لتكن $R = (\mathbb{R}^2, +, .)$ حلقة حيث

$$\forall\, x = (a_1, b_1)\,, y = (a_2, b_2) \in R\,;$$
$$x + y = (a_1 + a_2, b_1 + b_2)$$
$$x.y = (a_1.a_2 - b_1.b_2\,, a_1.b_1 + b_1a_2)$$

و $S = (\mathbb{C}, +, .)$ حلقة.

وليكن $\varphi\colon \mathrm{R} \to \mathrm{C}$ تطبيق معرف بالشكل:

$$\forall\, x = (a,b) \in R :\; \varphi(x) = a + b_i$$

φ تماثل.

٦) $R = (\mathbb{Z}_6, +, .)$ و $S = (\mathbb{Z}_2 \times \mathbb{Z}_3, +, .)$ حلقات.

$\varphi\colon R \to S$ تطبيق معرف بالشكل:

$$\forall\, r \in R : \varphi(r) = (r,r) = (r \bmod 2, r \bmod 3)$$

φ تماثل.

مبرهنة: ليكن $\varphi\colon \mathrm{R} \to \mathrm{S}$ تشاكل حلقي غامر حيث R,S حلقات واحدية عندئذ ما يلي صحيح:

١- $\varphi(1_R) = 1_S$

٢- إذا كانت R تبديلية فإن S تبديلية.

البرهان:

١. $\forall\, b \in S\,; \exists\, a \in R : b = \varphi(a)$

$$b.\varphi(1_R) = \varphi(a)\varphi(1_R) = \varphi(a.1_R) = \varphi(a) = b$$
$$\varphi(1_R).b = \varphi(1_R).\varphi(a) = \varphi(1_R.a) = \varphi(a) = b$$

ومنه $\varphi(1_\mathrm{R}) = 1_\mathrm{S}$

٢. $\forall\, b_1, b_2 \in S\,; \exists\, a_1, a_2 \in R\,, b_1 = \varphi(a_1), b_2 = \varphi(a_2)$

$$b_1.b_2 = \varphi(a_1)\varphi(a_2) = \varphi(a_1.a_2) = \varphi(a_2a_1) = \varphi(a_2)\varphi(a_1) = b_2b_1$$

ومنه S تبديلية.

الوسيلة الوحيدة إلى النجاح هي الاستمرار بقوة حتى النهاية

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة

نظري

◄ دكتور المادة: شوقي الراشد

◄ المحاضرة: الرابعة ◄ عنوان المحاضرة: المنطقة الصحيحة ومميز الحلقة

المحتوى العلمي: سندرس في هذه المحاضرة.

١. المناطق الصحيحة $(\boldsymbol{Integral\ Domain})$
٢. مميز الحلقة $(\boldsymbol{character})$

المناطق الصحيحة:

- قواسم الصفر:

لتكن R حلقة و $0 \neq a$ بحيث $a \in R$:

١) يسمى العنصر a قاسم أيمن للصفر إذا وفقط إذا تحقق أنه:
$$\exists\, 0 \neq b \in R : b.a = 0$$
٢) يسمى العنصر a قاسم أيسر للصفر إذا وفقط إذا تحقق أنه:
$$\exists\, 0 \neq b \in R : a.b = 0$$
٣) يسمى العنصر a قاسم للصفر إذا وفقط إذا تحقق:
$$\exists\, 0 \neq b \in R : b.a = a.b = 0$$

أمثلة:

١. لتكن $R = (M_2(\mathbb{R}),+,.)$ و $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ عندئذ:
$$\exists\, 0 \neq b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in R : a.b = b.a = 0_R$$
٢. وليكن $R = (M_2(\mathbb{R}),+,.)$ و $x = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ ومنه:
$$\exists\, 0 \neq y = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} : x.y = 0$$
أي x قاسم أيسر و y قاسم أيمن

٣. إذا كانت $R = (\mathbb{Z}_6,\oplus,\otimes)$ فإن: $\{2,3,4\}$ قواسم للصفر في R

المنطقة الصحيحة أو التكاملية:

لتكن R حلقة واحدية تبديلية نقول عن R أنها منطقة صحيحة (تكاملية) إذا وفقط إذا كانت لا تحوي قواسم للصفر وترمز بـ ID

أمثلة عن الـ ID

(١) $(\mathbb{Z},+,.)$

(٢) $(\mathbb{Z}_p,\oplus,\otimes)$ حيث p عدد أولي.

ليكن $x,y \in \mathbb{Z}_p$ بحيث: $x.y = 0$

ومنه $p\backslash xy$ ومنه: إما $p\backslash x$ أو $p\backslash y$

وبالتالي: إما $x = 0$ أو $y = 0$

ومنه $\mathbb{Z}_p$ لا تحوي قواسم للصفر

مبرهنة: لتكن R حلقة إذا كان $a,b,c \in R$

R لا تحوي قواسم الصفر إذا وفقط إذا تحقق:

$(1)\quad a.b = a.c \;\;,\;\; a \neq 0 \Rightarrow b = c$ من اليسار

$(2)\quad b.a = c.a \;\;,\;\; a \neq 0 \Rightarrow b = c$ من اليمين

ملاحظة: في حال كانت R تبديلية يصبح الشرطان عبارة عن شرط واحد.

البرهان:

$\Leftarrow$ لنفرض R لا تحوي قواسم الصفر ولنثبت الشرطين:

$$(1)\quad a.b = a.c \;\;,\;\; a \neq 0 \Rightarrow a(b-c) = 0 \;\;,\;\; a \neq 0 \Rightarrow b = c$$

$$(2)\quad b.a = c.a \;\;,\;\; a \neq 0 \Rightarrow (b-c)a = 0 \;\;,\;\; a \neq 0 \Rightarrow b = c$$

$\Leftarrow$ لنفرض الشرطين محققين ولنثبت أن R لا تحوي قواسم الصفر:

$$\forall\, x,y \in R : x.y = 0 \;\;,\;\; x \neq 0$$

$$x.y = 0 = x.\underbrace{0}_{c} \;\;,\;\; x \neq 0 \;\underbrace{\Rightarrow}_{1\text{ حسب}}\; y = 0$$

سؤال (١): نعلم أن كل ID لا تحوي قواسم الصفر، هل كل ما ليست ID تحوي قواسم الصفر؟

الجواب: $2\mathbb{Z}$ حلقة تبديلية لا تحوي قواسم الصفر وليست ID لأنها لا تحوي 1

ملاحظة: الحلقة التامة هي حلقة تبديلية وواحدية والـ ID حلقة تامة لا تحوي قواسم الصفر.

سؤال (٢): أثبت أن كل حقل هو ID وبين أن العكس ليس صحيح بالضرورة.

الجواب: لتكن R حقل وبالتالي R حلقة تبديلية واحدية ليتم المطلوب يكفي أن نبرهن أن R لا تحوي قواسم الصفر.

لنفرض جدلاً أن R تحوي قواسم الصفر ومنه:

$$\exists\, a,b \in R \;\;,\;\; a.b = 0 \;\;,\;\; a \neq 0 \;\;,\;\; b \neq 0$$

نضرب بـ $a^{-1} \Leftarrow$ $\qquad b = a^{-1}ab = a^{-1}0 = 0$

ومنه $b = 0$ وهذا تناقض ومنه الفرض الجدلي خاطئ ومنه كل حقل هو ID

والعكس ليس صحيح بالضرورة مثال على ذلك:

$R = (\mathbb{Z}, +, .)$ هي ID ولكن ليست حقل

سؤال (٣): متى ID تصبح حقل؟

الجواب: إذا كانت ID منتهية تصبح حقل.

مبرهنة: كل منطقة صحيحة منتهية هي حقل.

البرهان: لتكن R هي ID وبالتالي هي حلقة تبديلية واحدية وبالتالي يكفي أن نبرهن أنه من أجل $\forall\, 0 \neq a \in R$ يجب أن يكون له مقلوب.

لنعرف العلاقة: $\forall\, 0 \neq a \in R : \varphi_a : R \to R$

بالشكل: $\forall\, r \in R : \varphi_a(r) = ar$

φ_a تطبيق لأنه: $\forall\, r_1, r_2 \in R : r_1 = r_2 \Rightarrow ar_1 = ar_2$

$$\Rightarrow \varphi_a(r_1) = \varphi_a(r_2)$$

φ_a متباين لأنه: $\forall\, r_1, r_2 \in R : \varphi_a(r_1) = \varphi_a(r_2)$

$$\Rightarrow ar_1 = ar_2 \Rightarrow r_1 = r_2$$

ملاحظة: كل تطبيق بين منتهية ومنتهية هو غامر.

ومنه بما أن R منتهية فإن φ_a غامر.

$$1 \in R \,;\, \exists\, b \in R : ab = \varphi_a(b) = 1 \Rightarrow ab = ba = 1$$

ومنه a قابل للقلب في R وبالتالي R حقل

مثال: إذا كان p عددا أولياً فإن $\mathbb{Z}_p$ حقل.

مميز الحلقة:

لتكن R حلقة نعرف مميز الحلقة R (إن وجد) بأنه أصغر عدد صحيح موجب $n \in \mathbb{Z}^+$ يحقق الشرط:

$$\forall\, a \in R : na = 0$$

وفي حال كان غير موجود نضع المميز يساوي الصفر (اصطلاحاً) ونرمز له بالرمز

$$char(R) = n$$

أمثلة:

١- $R=(\mathbb{Z}_n,\oplus,\otimes)$ فيها $char(R)=n$
٢- $R=(\mathbb{Z},+,.)$ ومنه اصطلاحاً $char(R)=0$

مبرهنة:

لتكن R حلقة واحدية و $0<char(R)=n \Leftrightarrow n$ أصغر عدد صحيح موجب يحقق $1.n=0$

البرهان:

$\Leftarrow \quad 1\in R: 1.n=0$

لنفرض جدلاً أنه يوجد $m\in\mathbb{Z}^+$ بحيث $m<n\ ,\ 1.m=0$

$$\forall\, a\in R\,;\ a.m=a.(1.m)=a.0=0$$

وهذا يناقض تعريف المميز وبالتالي الفرض الجدلي خاطئ ومنه n أصغر عدد صحيح موجب يحقق:

$$1.n=0$$

$$\Rightarrow \quad \forall\ a\in R\ :\ \ a.n=a(1.n)=0$$

وحسب الفرض n أصغر عدد صحيح ومنه $n=char(R)>0$

مبرهنة:

إذا كانت R هي ID فإن: إما $char(R)=0$ أو $char(R)=p$ حيث p عدد أولي.

البرهان:

- إذا كان $char(R)=0$ يتم المطلوب.
- وفي حالة $char(R)=n>0$ نفرض جدلاً أن n ليس أولي

$$\exists\, m,s\in\mathbb{Z}\ :1<m<n\,,1<s<n,\quad n=m.s$$

$$0=1.n=1(m.s)=(1m)(1s)\Rightarrow\begin{cases}1.m=0\\1.s=0\end{cases}$$

وهذا تناقض كون n أصغر عدد صحيح موجب يحقق $1.n=0$

ومنه الفرض الجدلي خاطئ و n عدد أولي.

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة

◄ دكتور المادة: شوقي الراشد

نظري

◄المحاضرة: الخامسة العنوان: حل مبرهنات

المحتوى العلمي: سنقوم في هذه المحاضرة بحل مبرهنتين

مبرهنة: لتكن R هي ID

١) إذا كان $char(R) = 0$ فإنه يوجد حلقة جزئية في R تماثل $\mathbb{Z}$
٢) إذا كان $char(R) = p$ حيث p عدد أولي فإنه يوجد حلقة جزئية في R تماثل $\mathbb{Z}$

البرهان:

١) لنعرف $T = \{m.1_R : m \in \mathbb{Z}\} \leq R$

ولنعرف العلاقة $\varphi : \mathbb{Z} \to R$ بالشكل:

$$\forall\, m \in \mathbb{Z} \;;\varphi(m) = m.1$$

φ تطبيق لأنه:

$$\forall\, m,n \in \mathbb{Z} \;: m = n \;\Rightarrow m.1 = n.1 \Rightarrow \varphi(m) = \varphi(n)$$

φ تشاكل لأنه:

$$\forall\, m,n \in \mathbb{Z}$$

$$(1)\quad \varphi(m+n) = (m+n)1 = (m.1) + (n.1) = \varphi(m) + \varphi(n)$$

$$(2)\quad \varphi(m.n) = (m.n).1 = (m.1)(n.1) = \varphi(m).\varphi(n)$$

φ متباين لأنه:

$$\forall\, m,n \in \mathbb{Z} : \varphi_m = \varphi_n \Rightarrow m.1 = n.1 \Rightarrow m.1 - n.1 = 0 \Rightarrow (m-n)1 = 0$$

$$\Rightarrow m - n = 0 \Rightarrow m = n$$

φ غامر لأنه:

ليكن $m \in T$ عندئذ يوجد $m \in \mathbb{Z}$ بحيث $M = m.1_R$

$$\varphi(m) = m.1 = M \Rightarrow \varphi \text{ غامر}$$

وبالتالي φ تماثل

٢) لنعرف $T = \{m.1_R : m \in \mathbb{Z}\} \leq R$

ولنعرف العلاقة: $\varphi : \mathbb{Z}_p \to T$ بالشكل:

$$\forall\, m \in \mathbb{Z}_p \,;\, \varphi(m) = m.1$$

φ تطبيق لأنه:

$$\forall\, m,n \in \mathbb{Z}_p : m = n \Rightarrow m.1 = n.1 \Rightarrow \varphi(m) = \varphi(n)$$

φ تشاكل لأنه:

$$\forall\, m,n \in \mathbb{Z}_p;$$

$$(1) \quad \varphi(m+n) = (m+n)1 = (m.1) + (n.1) = \varphi(m) + \varphi(n)$$

$$(2) \quad \varphi(m.n) = (m.n)1 = (m.1)(n.1) = \varphi(m).\varphi(n)$$

φ متباين لأنه:

$$\forall\, m,n \in \mathbb{Z}_p : \varphi(m) = \varphi(n) \Rightarrow m.1 = n.1 \Rightarrow m.1 - n.1 = 0$$

$$\Rightarrow (m-n)1 = 0$$

وحسب خوارزمية القسمة سنثبت أن: $m - n$ هي من مضاعفات الـ p

$$\exists\, r,s \in \mathbb{Z} \;:\; m - n = rp + s \;,\; 0 \leq s < p \quad \dots *$$

$$\Rightarrow \varphi(m-n) = \varphi(rp+s) = \varphi(rp) + \varphi(s)$$

$$\Rightarrow (m-n)1 = (rp+s)1 = (rp)1 + s.1 = (r.1)(p.1) + (s.1)$$

بما أن $(m-n)1 = 0$ فإن $0 = (r.1)(p.1) + (s.1)$

وبما أن $char(R) = p \Rightarrow 1.p = 0$

$$\Rightarrow s.1 = 0 \Rightarrow s = 0$$

((لأن $char(R) = p$ أصغر عدد صحيح موجب يحقق $1.p = 0$))

ومنه نعوض $s = 0$ في *

$$\Rightarrow m - n = rp$$

وبما أن rp هي من مضاعفات p فإن:

$$m - n = 0 \Rightarrow m = n \Rightarrow$$ φ متباين

φ غامر لأنه: إذا أخذنا مقصور φ بالشكل:

$$\varphi : \mathbb{Z}_p \to Im\,\varphi \subseteq T$$

وحسب الملاحظة التي تقول كل تطبيق بين منتهية وغير منتهية هو غامر نجد أن φ غامر

وبالتالي: $\mathbb{Z}_p \cong Im\,\varphi$

كما أن $Im\,\varphi \leq T$ ومنه $Im\,\varphi \leq R$

مبرهنة:

ليكن R حقل عندئذ:

١) إذا كان $char(R)=0$ فإنه يوجد حقل جزئي في R يماثل $\mathbb{Q}$
٢) إذا كان $char(R)=p$ عدد أولي فإنه يوجد حقل جزئي في R يماثل $\mathbb{Z}_p$

البرهان: $\mathbb{Z}\cong\mathbb{Z}_{1.R} \Leftarrow char(R)=0$

١) حيث $\mathbb{Z}_{1.R}=T=\{1.m : m\in\mathbb{Z}\}$

$$\forall\, 0\neq m\in\mathbb{Z} : 0\neq 1.m\in R \Rightarrow (1.m)^{-1}=\frac{1}{1.m}\in R \Rightarrow 1.m\in U(R)$$

لنعرف المجموعة:

$$S=\left\{\frac{m.1}{n.1} : m,n\in\mathbb{Z}\ ,n\neq 0\right\}\leq R$$

أي S حقل جزئي في R

ولنعرف العلاقة: $\varphi:\mathbb{Q}\to S$ بالشكل:

$$\forall\,\frac{m}{n}\in\mathbb{Q} : \varphi\left(\frac{m}{n}\right)=\frac{m.1}{n.1}$$

φ تطبيق لأنه:

$$\forall\frac{m_1}{n_1},\frac{m_2}{n_2}\in\mathbb{Q} : \frac{m_1}{n_1}=\frac{m_2}{n_2}\Rightarrow\frac{m_1.1}{n_1.1}=\frac{m_2.1}{n_2.1}\Rightarrow\varphi\left(\frac{m_1}{n_1}\right)=\varphi\left(\frac{m_2}{n_2}\right)$$

φ تشاكل لأنه:

$$\forall\frac{m_1}{n_1},\frac{m_2}{n_2}\in\mathbb{Q};$$

$$(1)\quad \varphi\left(\frac{m_1}{n_1}+\frac{m_2}{n_2}\right)=\varphi\left(\frac{m_1n_2+m_2n_1}{n_1n_2}\right)=\frac{(m_1n_2+m_2n_1).1}{(n_1n_2).1}$$
$$=\frac{(m_1n_2).1}{(n_1n_2).1}+\frac{(m_2n_1).1}{(n_1n_2).1}=\frac{m_1.1}{n_1.1}+\frac{m_2.1}{n_2.1}=\varphi\left(\frac{m_1}{n_1}\right)+\varphi\left(\frac{m_2}{n_2}\right)$$
$$(2)\quad \varphi\left(\frac{m_1}{n_1}.\frac{m_2}{n_2}\right)=\varphi\left(\frac{m_1m_2}{n_1n_2}\right)=\frac{(m_1m_2)1}{(n_1n_2)1}=\frac{m_1.1}{n_1.1}.\frac{m_2.1}{n_2.1}$$
$$=\varphi\left(\frac{m_1}{n_1}\right).\varphi\left(\frac{m_2}{n_2}\right)$$

φ متباين لأنه:

$$\forall \frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q} : \varphi\left(\frac{m_1}{n_1}\right) = \varphi\left(\frac{m_2}{n_2}\right) \Rightarrow \frac{m_1.1}{n_1.1} = \frac{m_2.1}{n_2.1}$$

$$\frac{m_1.1}{n_1.1} - \frac{m_2.1}{n_2.1} = 0 \Rightarrow \frac{(m_1 n_2 - m_2 n_1)1}{(n_1 n_2)1} = 0$$

$$\Rightarrow (m_1 n_2 - m_2 n_1)1 = 0$$

وبما أن المميز فرضاً يساوي الصفر نجد أن:

$$\Rightarrow m_1 n_2 - m_2 n_1 = 0 \Rightarrow m_1 n_2 = m_2 n_1$$

نقسم على n_1, n_2 نجد:

$$\frac{m_1 n_2}{n_1 n_2} = \frac{m_2 n_1}{n_1 n_2} \Rightarrow \frac{m_1}{n_1} = \frac{m_2}{n_2} \Rightarrow$$ متباين φ

φ غامر لأن :

$$\forall \frac{m.1}{n.1} \in S : \frac{m}{n} \in \mathbb{Q} ;$$

$$\mathbb{Q}\left(\frac{m}{n}\right) = \frac{m.1}{n.1} \Rightarrow$$ غامر φ

وبالتالي φ تماثل أي $S \cong \mathbb{Q}$

٢) R حقل $\Leftarrow$ R هي ID و $p = char(R)$ عدد أولي ومنه:

حسب المبرهنة السابقة:

$$\exists\, S \leq R : S \cong \mathbb{Z}_p$$

وبما أن $\mathbb{Z}_p$ حقل (منطقة تكاملية منتهية) فتكون S حقل جزئي في R

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة

◄ دكتور المادة: شوقي الراشد

◄ المحاضرة: السادسة العنوان: حلقة كثيرات الحدود

المحتوى العلمي: سنقوم في هذه المحاضرة بحل مبرهنتين

حلقة كثيرات الحدود *polynomial ring*

تعريف

لتكن R حلقة وليكن x متغير ما، نسمي المجموع المنتهي

$$f(x) = a_n.x^n + a_{n-1}.x^{n-1} + \cdots + a_1.x + a_0 = \sum_{i=0}^{n} a_i.x^i$$

انه كثيرة حدود معرفة على R حيث $n \in \mathbb{N}$ عدد طبيعي و

$$\forall\, i = \{0,1,\ldots\ldots n\} : a_i \in R$$

- يسمى a_n المعامل الرئيسي للحدودية $f(x)$ ونرمز له بـ:

$$l\big(f(x)\big) = a_n$$

- اذا كان $a_n \neq 0$ فإن درجة الحدودية تكون $deg(f) = n$.
- إذا كانت R حلقة واحدية و $l\big(f(x)\big) = 1$ فإن f تسمى حدودية واحدية *monic*،
  مثال: الحدودية المميزة
- إذا كانت $0 \neq f(x) \in R$ (لا تحوي متغير x) فإن f تسمى كثيرة حدود ثابتة وتكون $deg(f) = 0$.
- إذا كانت $f(x) = 0$ كثيرة حدود صفرية:

$$f(x) = 0 \Leftrightarrow a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$
$$; a_i \in R\,, n \in \mathbb{N}\,, \forall\, i \in \{0,1,2,\ldots,n\}$$

فإن $\deg(f) = \infty$ ((اصطلاحا))

- نرمز لمجموعة كل كثيرات الحدود المعرفة على الحلقة R بالرمز:

$$R[x] = \left\{ f(x) = \sum_{i=0}^{n} a_i . x^i \ ; n \in \mathbb{N} \ , \ a_i \in R \quad \forall \quad i \in \{0,1, \dots \dots n\} \right\}$$

نعرف على هذه المجموعة قانوني تشكيل داخليين الأول هو$(+)$ والثاني هو $(.)$ المعرفان بالشكل التالي:

$$\forall f(x), g(x) \in R[x] \ : \begin{cases} f(x) = \sum_{i=0}^{m} a_i . x^i \ ; a_i \neq 0 \\ g(x) = \sum_{j=0}^{n} b_j . x^j \ ; b_j \neq 0 \end{cases}$$

$$(1) \qquad f(x) + g(x) = \sum_{k=0}^{t} (a_k + b_k) . x^k \ ; \quad t = max(m,n)$$

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

$$a_i = 0 \ ; i > m \qquad , \qquad b_j = 0 \ ; j > n$$

$$(2) \qquad f(x) . g(x) = \sum_{k=0}^{m+n} c_k . x^k \ : c_k = \sum_{i+j=k} a_i . b_j$$

عندئذ: $(R[x], +, .)$ تشكل حلقة وتسمى حلقة كثيرات الحدود المعرفة على R.

ملاحظات:

- ❖ إذا كانت R حلقة واحدية فإن $R[x]$ حلقة واحدية واحدها 1_R .
- ❖ إذا كانت R حلقة تبديلية فإن $R[x]$ حلقة تبديلية.

مثال:

لتكن $R = \mathbb{Z}$ حلقة و $R[x] = \mathbb{Z}[x]$ أي:

$$R[x] = \mathbb{Z}[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in \mathbb{Z}, n \in \mathbb{N}, \forall\, i \in \{0,1,2,\dots,n\} \right\}$$

$$f(x) = 2x^2 - x + 3 \quad \& \quad g(x) = x^3 + 2x - 1 \ \in R[x]$$

$$m = deg(f) = 2 \quad , \quad n = \deg(g) = 3$$

$$a_0 = 3 \qquad , \qquad a_1 = -1 \qquad , \qquad a_2 = 3$$

$$b_0 = -1 \qquad , \qquad b_1 = 2 \qquad , \qquad b_2 = 0 \qquad , \qquad b_3 = 1$$

$$t = max\{m,n\} = max\{2,3\} = 3$$

$$(1) \quad f(x) + g(x) = \sum_{k=0}^{t} (a_k + b_k).x^k = \sum_{k=0}^{3} (a_k + b_k).x^k$$

$$= (a_0.b_0)x^0 + (a_1.b_1)x^1 + (a_2.b_2)x^2 + (a_3 + b_3)x^3$$

$$= (3-1) + (-1+2)x + (2+0)x^2 + (0+1)x^3$$

$$= 2 + x + 2x^2 + x^3$$

$$(2) \quad f(x).g(x) = \sum_{k=0}^{m+n=5} c_k.x^k \ \text{حيث}\ c_k = \sum_{k=i+j} a_i.b_j$$

$$c_0 = (a_0.b_0) = (+3)(-1) = -3$$

$$c_1 = (a_0.b_1 + a_1.b_0) = (3)(2) + (-1)(-1) = 6 + 1 = 7$$

$$c_2 = (a_0.b_2 + a_1.b_1 + a_2.b_0) = (3)(0) + (-1)(2) + (2)(-1)$$
$$= 0 - 2 - 2 = -4$$

$$c_3 = (a_0.b_3 + a_1.b_2 + a_2.b_1 + a_3.b_0)$$
$$= (3)(1) + (-1)(0) + (2)(2) + (0)(-1)$$
$$= 3 + 0 + 4 + 0 = 7$$

$$c_4 = a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0 = -1$$

$$c_5 = a_0b_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_0 = 2$$

وبالتالي:

$$f(x).g(x) = c_0x^0 + c_1x^1 + c_2x^2 + c_3x^3 + c_4x^4 + c_5x^5$$
$$= -3 + 7x - 4x^2 + 7x^3 - x^4 + 2x^5$$

$\deg(f.g) = \deg(f) + \deg(g) \Rightarrow \deg(f.g) = 5$ (لأن $\mathbb{Z}$ لا تحوي قواسم الصفر)

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\} \Rightarrow \deg(f+g) \leq 3$$

مثال آخر:

إذا كان $f(x) = 2x^2 - 1 \ , \ g(x) = 3x + 4 \in \mathbb{Z}_6$

$$\deg(f.g) \leq 3$$

$$\deg(f+g) \leq \max\{2,1\} = 2$$

مبرهنة:

إذا كانت R حلقة وكان $0 \neq f(x), g(x) \in R[x]\backslash\{0\}$ عندئذ القضايا التالية صحيحة:

١) $\deg(f.g) \leq \deg(f) + \deg(g)$

وتكون المساواة $\deg(f.g) = \deg(f) + \deg(g)$ محققة في إحدى الحالات التالية:

١. R لا تحوي قواسم الصفر.

٢. إما $l(g)$ قابل للقلب.

٣. أو $l(f)$ قابل للقلب.

(٢ و٣) يعني إذا كانت R واحدية

٢) إذا كان $f + g = 0$ فإن $\deg(f+g) = \infty$

إذا كان $f + g \neq 0$ فإن $\deg(f+g) \leq \max\{\deg(f) + \deg(g)\}$

الإثبات:

ليكن $f(x).g(x) \in R[x]$ حيث:

$$f(x)=\sum_{i=0}^{m} a_i.x^i \;; a_i\neq 0 \quad \& \quad g(x)=\sum_{j=0}^{n} b_j.x^j \;; b_j\neq 0$$

$$\deg(f)=m \quad , \quad l(f)=a_m$$

$$\deg(g)=n \quad , \quad l(g)=b_n$$

$$h(x)=f(x).g(x)=\sum_{k=0}^{m+n} c_k.x^k \;;\; c_k=\sum_{k=i+j} a_i.b_j$$

$$c_{m+n}=a_0.b_{m+n}+a_1.b_{m+n-1}+\ldots\ldots\ldots+a_{m+n}.b_0=a_mb_n$$

$$c_{m+n}=a_mb_n$$

لكن:

$$h=f.g=c_{m+n}x^{m+n}+c_{m+n-1}x^{m+n-1}+\cdots+c_1x+c_0$$

$$\deg(f(x).g(x))=\deg(h)\leq m+n=\deg(f)+\deg(g)$$

وتتحقق المساواة في حالة $a_mb_n=c_{m+n}\neq 0$

نفرض جدلاً أن:

$$c_{m+n}=a_mb_n=0$$

وأن $l(g)=b_n\in U(R)$ ومنه

$$0=0.b_n^{-1}=a_m.b_n.b_n^{-1}=a_m\Rightarrow a_m=0$$

وهذا غير ممكن أي أن $c_{m+n}\neq 0$ وبالتالي:

$$\deg(f.g)=m+n$$

٢- إذا كان $f(x)+g(x)=0$ يتم المطلوب ، أما إذا كان $f+g\neq 0$ فإن:

$$f(x)+g(x)=\sum_{k=0}^{t}(a_k+b_k).x^k$$

حيث $t = max(m,n)$, $b_j = 0; j > n$, $a_i = 0;\ i > m$

$$\Rightarrow deg(f+g) \le t = max(m,n) = max(deg(f), deg(g))$$

سؤال (١): إذا كانت R هي $\boldsymbol{ID}$ أثبت أن $R[x]$ هي $\boldsymbol{ID}$

سؤال (٢): إذا كانت R حقل بين أنه ليس بالضرورة أن تكون $R[x]$ حقل.

الحل:

١- R هي $\boldsymbol{ID}$ $\Leftarrow$ $R[x]$ هي $\boldsymbol{ID}$

لنفرض جدلاً أن $R[x]$ ليست $\boldsymbol{ID}$ أي:

$$\exists\ f(x) + g(x) \in R[x] : f(x) \neq 0\ ,\ g(x) \neq 0\ ,\ f.g = 0$$

نأخذ الدرجة للطرفين:

$$\underbrace{deg(f)}_{<\infty} + \underbrace{deg(g)}_{<\infty} = deg(f.g) = deg(0) = \infty$$

وهذا مستحيل ومنه الفرض الجدلي خاطئ و $R[x]$ هي ID

٢- لنثبت أن $R[x]$ ليست حقل.

لنفرض جدلاً أن $R[x]$ هي حقل أي:

$$\exists\ 0 \neq f, g \in R[x], f, g \notin R : f.g = 1$$

$$\underbrace{deg(f)}_{<0} + \underbrace{deg(g)}_{<0} = deg(f.g) = deg(1) = 0$$

وهذا غير ممكن ومنه الفرض الجدلي خاطئ ومنه $R[x]$ ليست حقل

_مبرهنة خوارزمية القسمة Division Algorithm :

لتكن R حلقة واحدية تبديلية وليكن $f(x), g(x) \in R[x]$ بحيث أن $g \neq 0$ إذا كان $l(g) \in U(R)$، عندئذ **توجد** كثيرتا حدود **وحيدتان** $r(x), q(x) \in R[x]$ تحققان:

$$f(x) = g(x).\ \underbrace{q(x)}_{\text{ناتج القسمة}} + \underbrace{r(x)}_{\text{باقي القسمة}} \qquad (*)$$

حيث $r(x) = 0$ أو $deg(r(x)) < deg(g(x))$

الإثبات: نميز حالتين:

الحالة الأولى: إذا كانت $deg(f) = n < deg(g) = m$ فإنه نأخذ :

نأخذ $q(x) = 0$ و $r(x) = f(x)$ فنجد أن $f(x) = 0.g(x) + r(x)$

فيكون: $f(x) = g(x).q(x) + r(x)$ و $deg(r) = deg(f) < deg(g)$

وبالتالي يتم المطلوب

الحالة الثانية: إذا كانت $deg(f) \geq deg(g)$ يتم الاثبات باستخدام الاستقراء الرياضي (بحسب العدد n درجة الحدودية f)

ليكن: $f = \sum_{i=0}^{n} a_i.x^i \quad , \quad l(f) = a_n \ , \ \deg(f) = n$

$$g = \sum_{j=0}^{m} b_j.x^j \quad , \quad l(g) = b_m \quad , \quad \deg(g) = m$$

- من أجل $n = 0$ نجد :

$$m = \deg(g) \leq \deg(f) = 0$$

$$\Rightarrow \deg(g) = \deg(f) = 0 \Rightarrow f, g \in R$$

$$g = l(g) = b \in U(R)$$

محققة $f = (f.g^{-1})g + r \quad : r = 0 \quad , \quad q = f.g^{-1}$

ومنه من أجل $n = 0$ القضية صحيحة.

- نفرض صحة القضية من أجل كل الحدوديات التي درجتها أصغر تماما من n . ولنثبت صحتها من أجل n .

لنستفيد من الفرض الاستقرائي ولنعرف حدودية $h(x)$ بالشكل التالي

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

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

نلاحظ أن:

$$a_n x^n - a_n . b_m^{-1} . x^{n-m} . b_m x^m = a_n x^n - a_n x^n = 0$$

بالتالي $\deg\big(h(x)\big) < n$ وحسب الفرض الاستقرائي:

توجد حدوديتان وحيدتان تحققان:

$$\deg\big(r(x)\big) < \deg\big(g(x)\big) \quad \text{أو} \quad r(x) = 0$$

$$r(x), p(x) \in R[x] \quad \text{حيث}$$

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

$$\Rightarrow f(x) = \big(a_n . b_m^{-1} . x^{n-m} + p(x)\big) . g(x) + r(x)$$

$$\Rightarrow \exists\, q(x) = a_n . b_m^{-1} . x^{n-m} + p(x) \,, r(x) \in R[x] \quad \text{حيث}$$

$$f(x) = q(x) . g(x) + r(x) \quad : \text{عندئذ}$$

لنبرهن الوحدانية:

لنفرض وجود $q_1(x), q_2(x), r_1(x), r_2(x) \in R[x]$ بحيث :

$$f(x) = q_1 g + r_1 \;,\; r_1 = 0 \quad \text{أو} \quad deg(r) < deg(g)$$

$$deg\big((r_1(x)\big) < deg\big(g(x)\big) \quad \text{أو} \quad r_1(x) = 0 \quad \text{حيث}$$

$$deg\big((r_2(x)\big) < deg\big(g(x)\big) \quad \text{أو} \quad r_2(x) = 0 \quad \text{حيث}$$

نفرض جدلا أن $r_1(x) \neq r_2(x)$.

من العلاقة $(*)$ نجد:

$$\Rightarrow g(x) . q_1(x) + r_1(x) = g(x) . q_2(x) + r_2(x)$$

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

$$deg\Big(\big(q_2(x) - q_1(x)\big) . g(x)\Big) = deg\big(r_1(x) - r_2(x)\big)$$

حسب مبرهنة سابقا وكون $\ell(g)$ قابل للقلب فإن :

$$deg\left(\left(q_2(x)-q_1(x)\right).g(x)\right)=deg\left(\left(q_2(x)-q_1(x)\right)\right)+deg\left(g(x)\right)$$

$$\Rightarrow\ deg\left(g(x)\right)\leq deg\left(\left(q_2(x)-q_1(x)\right)\right)+deg\left(g(x)\right)$$

$$=deg\left(\left(q_2(x)-q_1(x)\right).g(x)\right)$$

$$=deg\left(r_1(x)-r_2(x)\right)\leq max\{deg\left(r_1(x)\right),deg\left(r_2(x)\right)\}<deg\left(g(x)\right)$$

لأن $deg\left(r_1(x)\right)<deg\left(g(x)\right)$

$deg\left(r_2(x)\right)<deg\left(g(x)\right)$

وهذا تناقض حيث لا يمكن أن يكون $deg(g)<deg(g)$

ومنه الفرض الجدلي خاطئ ومنه :

$$r_1(x)=r_2(x)$$

$$\left(q_2(x)-q_1(x)\right).g(x)=r_1(x)-r_2(x)$$

$$\left(q_2(x)-q_1(x)\right).g(x)=0$$

وكون g لا يساوي الصفر فرضاً فإن: $\left(q_2(x)-q_1(x)\right)=0 \Leftarrow q_1=q_2$

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة

◄ دكتور المادة: شوقي الراشد

◄ المحاضرة: السابعة العنوان: حلقة كثيرات الحدود

المحتوى العلمي: سنقوم في هذه المحاضرة بحل مبرهنة الباقي ودراسة بعض النتائج.

مبرهنة الباقي: (Remainder theorem)

لتكن R حلقة تبديلية واحدية و $a \in R$ إذا كانت $f(x) \in R[x]$ فإنه يوجد حدودية وحيدة

$q(x) \in R[x]$ تحقق:

$$f(x) = (x-a)q(x) + f(a)$$

الإثبات:

حسب خوارزمية القسمة للحدوديتان f و $(x-\mathrm{a})$:

يوجد حدوديتان وحيدتان

$$\exists\ r(x), q(x) \in R[x]$$

تحققان

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

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

ومنه $r(x) = 0$ أو $r(x) \in R$

لنثبت الان أن $f(a) = r(x)$ نميز حالتين :

١) $r = 0$ فإن $f(a) = 0$ لأن

$$f(a) = (a-a)q(x) + 0 \Longrightarrow f(a) = r(x) = 0$$

٢) $0 \neq r(x) \in R$ فإن:

$$f(a) = (a-a)q(x) + r(x) \Longrightarrow f(a) = r(x)$$

وفي كلا الحالتين $f(a) = r(x)$ ومنه:

$$f(x) = (x-a)q(x) + f(a)$$

تعريف:

لتكن R حلقة و $r \in R[x]$ و $f(x), g(x) \in R[x]$

١) إن r صفرا للحدودية $f(x) \in R[x]$ إذا كان $f(x) = 0$ ونرمز لمجموعة أصفار الحدود $f(x)$ بالرمز $Z(f)$

٢) نقول أن $g(x)$ يقسم $f(x)$ إذا وفقط إذا كان:

$$\exists\, h(x) \in R[x] : f(x) = h(x).\,g(x)$$

ونرمز لذلك بالشكل: $g\backslash f$

نتائج:

نتيجة (١): لتكن R حلقة واحدية تبديلية و $f(x) \in R[x]$ و $f(x)$ يقبل القسمة على $(x-r)$ إذا وفقط إذا كان r صفراً لـ $f(x)$ في R .

الاثبات : (حسب مبرهنة الباقي)

$$r \text{ صفراً لـ } f \Leftrightarrow f(r) = 0 \Leftrightarrow \exists\, q(x) \in R[x] : f(x) = (x-r)q(x)$$
$$\Leftrightarrow (x-r)\backslash f(x)$$

نتيجة (٢) **مبرهنة التعميم:**

لتكن R هي ID و $r_1, r_2, \dots \dots \dots r_n \in R$ اذا كانت $r_1, r_2, \dots, r_n$ أصفارا مختلفة مثنى مثنى للحدودية و $f(x) \in R[x]$ فإن $f(x)$ يقبل القسمة على $\prod_{i=1}^{n}(x-r_i)$.

الاثبات:

يتم الاثبات بالاستقراء الرياضي على n

من أجل $n = 1$ صحيحة حسب النتيجة (١).

نفرض صحتها من أجل $n-1$ أي:

$f(x)$ تقبل القسمة على $\prod_{i=1}^{n-1}(x-r_i)$

من أجل n حسب الفرض الاستقرائي.

$$\exists\ g(x) \in R[x] : f(x) = \prod_{i=1}^{n-1}(x - r_i)\,.\,g(x)$$

حسب الفرض r_n صفرا للحدودية $f(x)$ فإن:

$$0 = f(r_n) = \prod_{i=1}^{n-1}(r_n - r_i)\,.\,g(r_n)$$

$$\forall\ i \in \{1,2 \dots\dots.., n-1\} \quad ; r_i \neq r_n$$

وكون R هي ID فإن $g(r_n) = 0$ وكون $r_1, r_2, \dots, r_n$ مختلفة مثنى مثنى ومنه $\prod_{i=1}^{n-1}(r_n - r_i) \neq 0$ ومنه حسب النتيجة (١) فإن $(x - r_n)$ يقسم $g(x)$ أي:

$$\exists\ h(x) \in R[x] : g(x) = (x - r_n).\,h(x)$$

$$\Rightarrow \exists\ h(x) \in R[x] : f(x) = \prod_{i=1}^{n}(x - r_i).\,h(x)$$

أي $\prod_{i=1}^{n}(x - r_i) \backslash f(x)$

ملاحظة :

نطلق كلمة الجذور للمعادلة والأصفار للحدودية.

نتيجة (٣):

R هي ID و $f(x) \in R[x]$ إذا كان $0 < \deg(f) = n$ فإن الحدودية $f(x)$ لها n صفرا على الأكثر $card(Z(f)) \leq n$.

الاثبات: يتم الاثبات بالاستقراء الرياضي على n

▫ من أجل $n = 1$:

$$a \neq 0 \quad , \quad a, b \in R \quad , \quad f(x) = ax + b$$

في هذه الحالة إذا كان a قابل للقلب في R فإنه يوجد صفر وحيد :

الصفر هو $Z(f) = \{-\frac{b}{a}\}$ وإن $card(Z(f)) \leq 1$

▪▪ لنفرض أن أي كثير حدود درجته تساوي $n-1$ يملك $n-1$ صفراً على الأكثر.

▪▪▪ من أجل n :

لتكن r صفراً لـ f حسب النتيجة (١) فإنه:

$$\exists\, g(x) \in R[x] : f(x) = (x-r)g(x)$$

ومنه $\deg(g) < n$ و $\deg(g) = n-1$

ومنه حسب الفرض الاستقرائي.

$$card(Z(g)) \leq n-1$$

وبما أن أصفار $g(x)$ هي ذاتها أصفار $f(x)$ وبالتالي:

$$card(Z(f)) \leq n$$

نتيجة (٤):

إذا كانت R هي ID غير منتهية وكانت $f(x) \in R[x]$ إذا كان:

$$\forall r \in R \;:\; f(r) = 0 \;\Longrightarrow\; f(x) = 0$$

الإثبات:

نفرض جدلا أن $f(x) \neq 0$ وليكن $\deg(f) = n$ حسب النتيجة السابقة :

$$card(Z(f)) \leq n$$

بما أن R غير منتهية فإنه:

$$\exists\, r \in R \;,\; r \notin Z(f)$$

أي $f(r) \neq 0$ وهذا يناقض الفرض وبالتالي الفرض الجدلي خاطئ $f(x) = 0$.

نتيجة (٥):

اذا كانت R هي ID غير منتهية وكانت $f(x), g(x) \in R[x]$ حدوديتان ليست ثابتتان

$$\forall\, r \in R \quad \text{حيث} \quad f(r) = g(r) \quad \Longrightarrow \quad f(x) = g(x)$$

نعرف الدالة $h(x)$:

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

$$\forall\, r \in R \quad \text{فإن} \quad h(r) = f(r) - g(r) = 0$$

حسب نتيجة ٤ فإن :

$$h(x) = f(x) - g(x) = 0 \;\Longrightarrow f(x) = g(x)$$

انتهت المحاضرة

إعداد: راما جوهر & مرح غريّب & رشا القرصة