باب 6

حلقة كثيرات الحدود

1.6 تعاريف

تعريف 1.6: كثير الحدود

كثير الحدود ذات المعاملات في $\mathbb{K}$ هو تعبير على الشكل:

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0,$$

حيث $n \in \mathbb{N}$ و $a_0, a_1, \ldots, a_n \in \mathbb{K}$.
مجموعة جميع كثيرات الحدود يرمز لها بـ $\mathbb{K}[X]$.

- a_i تسمى معاملات كثير الحدود.
- إذا كانت جميع المعاملات a_i منعدمة، يسمى P كثير الحدود المنعدم، ويرمز له بـ 0.
- نسمى درجة P أكبر عدد صحيح i بحيث $a_i \neq 0$؛ ونرمز لها بـ $\deg P$. لدرجة كثير الحدود المنعدم نضع حسب الاصطلاح $\deg(0) = -\infty$.
- كثير الحدود من الشكل $P = a_0$ حيث $a_0 \in \mathbb{K}$ يسمى كثير حدود ثابت. إذا كان $a_0 \neq 0$، فإن درجته هي 0.

مثال 1.6: أمثلة على كثيرات الحدود

- $X^3 - 5X + \frac{3}{4}$ هو كثير حدود من الدرجة 3.
- $X^n + 1$ هو كثير حدود من الدرجة n.
- 2 هو كثير حدود ثابت، من الدرجة 0.

تعريف 2.6: المساواة

ليكن $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$
و $Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$
كثيري حدود معاملاتهما في $\mathbb{K}$.

$P = Q \iff \forall i \; a_i = b_i$ ونقول أن P و Q متساويان.

تعريف 3.6: الجمع

ليكن $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$
و $Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$.

نعرف:

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \cdots + (a_1 + b_1)X + (a_0 + b_0)$$

تعريف 4.6: الضرب

ليكن $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$
و $Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$.

نعرف:

$$P \times Q = c_rX^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0$$

حيث $r = n + m$ و $c_k = \sum_{i+j=k} a_ib_j$ من أجل $k \in \{0, \ldots, r\}$.

تعريف 5.6: الضرب سلمي

إذا كان $\lambda \in \mathbb{K}$ فإن $\lambda \cdot P$ هو كثير الحدود الذي معامله i هو λa_i.

مبرهنة 1.6: خصائص الجمع والضرب

لـ $P, Q, R \in \mathbb{K}[X]$ يكون:

- $0 + P = P$، $P + Q = Q + P$، $(P + Q) + R = P + (Q + R)$
- $1 \cdot P = P$، $P \times Q = Q \times P$، $(P \times Q) \times R = P \times (Q \times R)$
- $P \times (Q + R) = P \times Q + P \times R$

مبرهنة 2.6: خصائص الدرجة

ليكن P و Q كثيري حدود معاملاتهما في $\mathbb{K}$.

- $\deg(P \times Q) = \deg P + \deg Q$
- $\deg(P + Q) \le \max(\deg P, \deg Q)$

نرمز $\mathbb{R}_n[X] = \{P \in \mathbb{R}[X] \mid \deg P \le n\}$. إذا كان $P, Q \in \mathbb{R}_n[X]$ فإن $P + Q \in \mathbb{R}_n[X]$.

تعريف 6.6: مصطلحات إضافية

- كثيرات الحدود التي تحتوي على حد واحد غير منعدم (من الشكل $a_k X^k$) تسمى أحادية الحد.
- ليكن $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$، كثير حدود مع $a_n \neq 0$. نسمى أحادية الحد $a_n X^n$ الحد الرئيسي. المعامل a_n يسمى المعامل الرئيسي لـ P.
- إذا كان المعامل الرئيسي هو 1، نقول أن P هو كثير حدود أحادي .

مثال 2.6: الجمع والضرب في $\mathbb{K}[x]$

لنأخذ كثيرَي الحدود:

$$p(x) = 2 + 3x - x^2, \qquad q(x) = 1 - 4x + 2x^3.$$

أولاً: جمع كثيرَي الحدود نحسب:

$$p(x) + q(x) = (2 + 3x - x^2) + (1 - 4x + 2x^3).$$

نجمع الحدود ذات الدرجات المتناظرة:

$$p(x) + q(x) = (2 + 1) + (3x - 4x) + (-x^2) + 2x^3,$$

ومن ثم:

$$p(x) + q(x) = 3 - x - x^2 + 2x^3.$$

ثانياً: ضرب كثيرَي الحدود نحسب:

$$p(x)q(x) = (2 + 3x - x^2)(1 - 4x + 2x^3).$$

وبالتالي:

$$p(x)q(x) = -2x^5 + 6x^4 + 8x^3 - 13x^2 - 5x + 2.$$

نظرية 1.6: خاصية الحلقة $\mathbb{K}[x]$

$\mathbb{K}[x]$ تشكّل حلقة تبديلية.

2.6 القسمة الاقليدية

تعريف 7.6

لِنعتبر $A, B \in K[X]$. نقول إنّ B يقسم A إذا وُجد كثير حدود $Q \in K[X]$ بحيث

$$A = BQ.$$

وفي هذه الحالة نكتب:

$$B \mid A.$$

نقول أيضاً إنّ A مضاعف لـ B، أو أنّ A قابل للقسمة على B. وإضافةً إلى الخواصّ البديهية مثل:

$$A \mid A, \qquad 1 \mid A, \qquad A \mid 0,$$

نملك النتائج التالية:

مبرهنة 3.6

لِنعتبر $A, B, C \in K[X]$. إذن:

1. إذا كان $B \mid A$ و$A \mid B$، فإنّه يوجد عدد غير منعدم $\lambda \in K^*$ بحيث
$$A = \lambda B.$$
2. إذا كان $B \mid A$ و$C \mid B$، فإنّه عندئذٍ $C \mid A$.
3. إذا كان $C \mid A$ و$C \mid B$، فإنّ
$$C \mid (AU + BV),$$
وذلك لأي $U, V \in K[X]$.

نظرية 2.6

(القسمة الإقليدية لكثيرات الحدود) لِنعتبر $A, B \in K[X]$ حيث $B \neq 0$. عندئذٍ يوجد كثير حدود وحيد Q ويوجد كثير حدود وحيد R بحيث

$$A = BQ + R,$$

مع تحقق الشرط:

$$\deg(R) < \deg(B).$$

يُسمّى Q حاصل القسمة وتُسمّى R باقي القسمة، وتُسمّى هذه الكتابة القسمة الإقليدية لـ A على B.

لاحظ أنّ الشرط

$$\deg(R) < \deg(B)$$

يعني أنّ $R = 0$ أو

$$0 \le \deg(R) < \deg(B).$$

وأخيراً، لدينا:

$$R = 0 \quad \iff \quad B \mid A.$$

مثال 3.6

لنأخذ:

$$A = 2X^4 - X^3 - 2X^2 + 3X - 1, \qquad B = X^2 - X + 1.$$

نجد بالقسمة الإقليدية:

$$Q = 2X^2 + X - 3, \qquad R = -X + 2.$$

والتحقّق:

$$A = BQ + R.$$

وتمثيل القسمة العمودية يكون كما يلي:

$$\begin{array}{r|l}
2X^4 - X^3 - 2X^2 + 3X - 1 & \begin{array}{l} X^2 - X + 1 \\ \hline 2X^2 + X - 3 \end{array} \\
-\left(2X^4 - 2X^3 + 2X^2\right) & \\
\hline
X^3 - 4X^2 + 3X - 1 & \\
-\left(X^3 - X^2 + X\right) & \\
\hline
-3X^2 + 2X - 1 & \\
-\left(-3X^2 + 3X - 3\right) & \\
\hline
-X + 2 &
\end{array}$$

مثال 4.6

نعتبر كثير الحدود

$$A = X^4 - 3X^3 + X + 1,$$

وكثير الحدود

$$B = X^2 + 2.$$

نقوم بإجراء القسمة الإقليدية لـ A على B، فنجد أن:

$$Q = X^2 - 3X - 2 \quad (\text{حاصل القسمة}),$$

$$R = 7X + 5 \quad (\text{باقي القسمة}).$$

وبالتالي يتحقق:

$$A = BQ + R.$$

3.6 القاسم المشترك الاكبر

مبرهنة 4.6: القاسم المشترك الأكبر

ليكن $A, B \in K[X]$، حيث $A \neq 0$ أو $B \neq 0$. يوجد كثير حدود وحيد أحادي (المعامل الرئيسي (أمام أعلى قوة) يساوي 1) ذو أكبر درجة يقسم كلاً من A و B.

تعريف 8.6: القاسم المشترك الأكبر

يُسمى كثير الحدود الوحيد هذا **القاسم المشترك الأكبر** لـ A و B، ونرمز له بـ $\gcd(A, B)$.

ملاحظة 1.6: ملاحظات حول القاسم المشترك الأكبر

- $\gcd(A, B)$ كثير حدود أحادي
- إذا كان $B \mid A$ و $A \neq 0$، فإن $\gcd(A, B) = \frac{1}{\lambda}A$، حيث λ المعامل الرئيسي لـ A
- لكل $\lambda \in K^*$، $\gcd(\lambda A, B) = \gcd(A, B)$
- كما في حالة الأعداد الصحيحة: إذا كان $A = BQ + R$ فإن $\gcd(A, B) = \gcd(B, R)$. وهذا يُبرر خوارزمية إقليدس.

خوارزمية 1.6: خوارزمية إقليدس

ليكن A و B حدوديين، حيث $B \neq 0$. نحسب القسمات الإقليدية المتتالية:

$$\begin{aligned}
A &= BQ_1 + R_1 & \deg R_1 &< \deg B \\
B &= R_1Q_2 + R_2 & \deg R_2 &< \deg R_1 \\
R_1 &= R_2Q_3 + R_3 & \deg R_3 &< \deg R_2 \\
&\vdots \\
R_{k-2} &= R_{k-1}Q_k + R_k & \deg R_k &< \deg R_{k-1} \\
R_{k-1} &= R_kQ_{k+1}
\end{aligned}$$

درجة الباقي تتناقص في كل قسمة. نوقف الخوارزمية عندما يصبح الباقي مساوياً للصفر. القاسم المشترك الأكبر هو آخر باقي غير منعدم R_k (بعد جعله أحادي القياس).

مثال 5.6: حساب القاسم المشترك الأكبر

لنحسب $\gcd(A, B)$ حيث $A = X^4 - 1$ و $B = X^3 - 1$. نطبق خوارزمية إقليدس:

$$\begin{aligned}
X^4 - 1 &= (X^3 - 1) \times X + (X - 1) \\
X^3 - 1 &= (X - 1) \times (X^2 + X + 1) + 0
\end{aligned}$$

القاسم المشترك الأكبر هو آخر باقي غير منعدم، إذن:

$$\gcd(X^4 - 1, X^3 - 1) = X - 1$$

مثال 6.6: حساب قاسم مشترك أكبر آخر

لنحسب $\gcd(A, B)$ حيث $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ و $B = X^4 + 2X^3 + X^2 - 4$:

$$\begin{aligned}
X^5 + X^4 + 2X^3 + X^2 + X + 2 &= (X^4 + 2X^3 + X^2 - 4) \times (X - 1) + 3X^3 + 2X^2 + 5X - 2 \\
X^4 + 2X^3 + X^2 - 4 &= (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}(X^2 + X + 2) \\
3X^3 + 2X^2 + 5X - 2 &= (X^2 + X + 2) \times (3X - 1) + 0
\end{aligned}$$

إذن:

$$\gcd(A,B) = X^2 + X + 2$$

تعريف 9.6: كثيرات حدود أولية فيما بينها

ليكن $A, B \in K[X]$. نقول أن A و B أوليان فيما بينها إذا كان $\gcd(A,B) = 1$.
لأي A, B يمكن الاختزال إلى كثيرات حدود أولية فيما بينها: إذا كان $\gcd(A,B) = D$ فإن A و B يكتبان:

$$A = DA' \quad , \quad B = DB'$$

حيث $\gcd(A', B') = 1$.

نظرية 3.6: نظرية بيزو

ليكن $A, B \in K[X]$ كثيرا حدود حيث $A \neq 0$ أو $B \neq 0$. نضع $D = \gcd(A,B)$.
يوجد كثيار حدود $U, V \in K[X]$ بحيث:

$$AU + BV = D$$

ملاحظة 2.6: استنتاج نظرية بيزو

هذه النظرية تنتج من خوارزمية إقليدس وتحديداً من عملية "الرجوع إلى الخلف" كما يتبين في المثال التالي.

مثال 7.6: تطبيق نظرية بيزو

لقد حسبنا $\gcd(X^4 - 1, X^3 - 1) = X - 1$. نرجع في خوارزمية إقليدس، هنا كان هناك سطر واحد فقط:

$$X^4 - 1 = (X^3 - 1) \times X + (X - 1)$$

لنستنتج أن:

$$X - 1 = (X^4 - 1) \times 1 + (X^3 - 1) \times (-X)$$

إذن $U = 1$ و $V = -X$ يحققان النظرية.

مثال 8.6: تطبيق نظرية بيزو على مثال معقد

لـ $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ و $B = X^4 + 2X^3 + X^2 - 4$ وجدنا $D = \gcd(A, B) = X^2 + X + 2$.

نبدأ من السطر قبل الأخير في خوارزمية إقليدس:

$$B = (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}D$$

إذن:

$$-\frac{14}{9}D = B - (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4)$$

السطر السابق في الخوارزمية كان:

$$A = B \times (X - 1) + 3X^3 + 2X^2 + 5X - 2$$

نعوض الباقي لنحصل على:

$$-\frac{14}{9}D = B - [A - B \times (X - 1)] \times \frac{1}{9}(3X + 4)$$

نستنتج أن:

$$-\frac{14}{9}D = -A \times \frac{1}{9}(3X + 4) + B \left[1 + (X - 1) \times \frac{1}{9}(3X + 4)\right]$$

إذن بوضع $U = \frac{1}{14}(3X+4)$ و $V = -\frac{1}{14}\left[9 + (X - 1)(3X + 4)\right] = -\frac{1}{14}(3X^2 + X + 5)$ نحصل على $AU + BV = D$.

نتيجة 1.6: معيار أولية كثيرات الحدود

ليكن A و B كثيرا حدود. A و B أوليان فيما بينهما إذا وفقط إذا وجد كثيرا حدود U و V بحيث:

$$AU + BV = 1$$

نتيجة 2.6: خاصية القاسم المشترك

ليكن $A, B, C \in K[X]$ حيث $A \neq 0$ أو $B \neq 0$. إذا كان $C \mid A$ و $C \mid B$ فإن $C \mid \gcd(A, B)$.

نتيجة 3.6: توطئة غاوس

ليكن $A, B, C \in K[X]$. إذا كان $A \mid BC$ و $\gcd(A, B) = 1$ فإن $A \mid C$.

4.6 جذر كثير حدود

تعريف 10.6: دالة كثير الحدود

ليكن $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$. من أجل عنصر $x \in \mathbb{K}$، نرمز $P(x) = a_n x^n + \cdots + a_1 x + a_0$. بهذا نربط بكثير الحدود P دالة كثيرة الحدود (نرمز لها أيضاً بـ P):

$$P : \mathbb{K} \to \mathbb{K}, \quad x \mapsto P(x) = a_n x^n + \cdots + a_1 x + a_0.$$

تعريف 11.6: جذر كثير الحدود

ليكن $P \in \mathbb{K}[X]$ و $\alpha \in \mathbb{K}$. نقول أن α هو جذر (أو صفر) لـ P إذا كان $P(\alpha) = 0$.

مبرهنة 5.6: علاقة الجذر بالقسمة

$$P(\alpha) = 0 \iff X - \alpha \text{ يقسم } P$$

برهان 1.6: برهان العلاقة

عند كتابة القسمة الإقليدية لـ P على $X - \alpha$ نحصل على $P = Q \cdot (X - \alpha) + R$ حيث R ثابت لأن $\deg R < \deg(X - \alpha) = 1$. إذن:

$$P(\alpha) = 0 \iff R(\alpha) = 0 \iff R = 0 \iff X - \alpha \mid P$$

تعريف 12.6: تضاعف الجذر

ليكن $k \in \mathbb{N}^*$. نقول أن α هو جذر مضاعف من الرتبة k لـ P إذا كان $(X-\alpha)^k$ يقسم P بينما $(X-\alpha)^{k+1}$ لا يقسم P. عندما $k=1$ نتحدث عن جذر بسيط، وعندما $k=2$ نتحدث عن جذر مزدوج، وهكذا.

مبرهنة 6.6: تكافؤات تعدد الجذر

هناك تكافؤ بين:

(i) α هو جذر من الرتبة k لـ P

(ii) يوجد $Q \in \mathbb{K}[X]$ بحيث $P=(X-\alpha)^k Q$، مع $Q(\alpha) \neq 0$

(iii) $P(\alpha)=P'(\alpha)=\cdots=P^{(k-1)}(\alpha)=0$ و $P^{(k)}(\alpha) \neq 0$

ملاحظة 3.6: مشتق كثير الحدود

قياساً على مشتق الدالة، إذا كان $P(X)=a_0+a_1X+\cdots+a_nX^n \in \mathbb{K}[X]$ فإن كثير الحدود

$$P'(X)=a_1+2a_2X+\cdots+na_nX^{n-1}$$

هو مشتق كثير الحدود P.

نظرية 4.6: نظرية دالمبير-غاوس

كل كثير حدود معاملاته مركبة ودرجته $n \geq 1$ له على الأقل جذر واحد في $\mathbb{C}$. وله بالضبط n جذراً إذا أحصينا كل جذر مع تعدده.

نقبل هذه النظرية بدون برهان.

مثال 9.6: مثال على كثير حدود من الدرجة الثانية

ليكن $P(X)=aX^2+bX+c$ كثير حدود من الدرجة 2 معاملاته حقيقية: $a,b,c \in \mathbb{R}$ و $a \neq 0$.

- إذا كان $\Delta=b^2-4ac>0$ فإن P يقبل جذرين حقيقيين متميزين $\frac{-b+\sqrt{\Delta}}{2a}$ و

$\frac{-b-\sqrt{\Delta}}{2a}$.

- إذا كان $\Delta < 0$ فإن P يقبل جذرين مركبين متميزين $\frac{-b+i\sqrt{|\Delta|}}{2a}$ و $\frac{-b-i\sqrt{|\Delta|}}{2a}$.
- إذا كان $\Delta = 0$ فإن P يقبل جذراً حقيقياً مزدوجاً $\frac{-b}{2a}$.

بأخذ الاعتبار لتعدد الجذور، لدينا دائماً بالضبط جذرين.

نظرية 5.6: عدد جذور كثير الحدود

ليكن $P \in \mathbb{K}[X]$ من الدرجة $n \geq 1$. فإن P يقبل على الأكثر n جذراً في $\mathbb{K}$.

مثال 10.6: تأثير مجال المعاملات

$P(X) = 3X^3 - 2X^2 + 6X - 4$. باعتباره كثير حدود معاملاته في $\mathbb{Q}$ أو $\mathbb{R}$، فإن P له جذر وحيد (بسيط) $\alpha = \frac{2}{3}$ ويتحلل إلى:

$$P(X) = 3\left(X - \frac{2}{3}\right)(X^2 + 2)$$

إذا اعتبرنا P الآن كثير حدود معاملاته في $\mathbb{C}$ فإن:

$$P(X) = 3\left(X - \frac{2}{3}\right)(X - i\sqrt{2})(X + i\sqrt{2})$$

ويقبل 3 جذور بسيطة.

5.6 كثيرات الحدود غير القابلة للاختزال

تعريف 13.6: كثيرات الحدود غير القابلة للاختزال

ليكن $P \in \mathbb{K}[X]$ كثير حدود من درجة $n \geq 1$، نقول أن P غير قابل للاختزال إذا كان لكل $Q \in \mathbb{K}[X]$ يقسم P، إما $Q \in \mathbb{K}^*$، أو يوجد $\lambda \in \mathbb{K}^*$ بحيث $Q = \lambda P$.

ملاحظة 4.6: ملاحظات حول كثيرات الحدود غير القابلة للاختزال

- كثير الحدود غير القابل للاختزال P هو إذاً كثير حدود غير ثابت قواسمه الوحيدة هي الثوابت أو P نفسه (إلى within ثابت مضاعف).
- مفهوم كثير الحدود غير القابل للاختزال في حسابيات $\mathbb{K}[X]$ يقابل مفهوم العدد الأولي في حسابيات $\mathbb{Z}$.
- في الحالة المعاكسة، نقول أن P قابل للاختزال؛ يوجد حينئذ كثيرا حدود A, B من $\mathbb{K}[X]$ بحيث $P = AB$، مع $\deg A \geq 1$ و $\deg B \geq 1$.

مثال 11.6: أمثلة على كثيرات الحدود القابلة وغير القابلة للاختزال

- جميع كثيرات الحدود من الدرجة 1 غير قابلة للاختزال. وبالتالي هناك عدد لا نهائي من كثيرات الحدود غير القابلة للاختزال.
- $X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$ قابل للاختزال.
- $X^2 + 1 = (X-i)(X+i)$ قابل للاختزال في $\mathbb{C}[X]$ ولكنه غير قابل للاختزال في $\mathbb{R}[X]$.
- $X^2 - 2 = (X-\sqrt{2})(X+\sqrt{2})$ قابل للاختزال في $\mathbb{R}[X]$ ولكنه غير قابل للاختزال في $\mathbb{Q}[X]$.

مبرهنة 7.6: توطئة إقليدس لكثيرات الحدود

ليكن $P \in \mathbb{K}[X]$ كثير حدود غير قابل للاختزال وليكن $A, B \in \mathbb{K}[X]$. إذا كان $P \mid AB$ فإن $P \mid A$ أو $P \mid B$.

برهان 2.6: برهان توطئة إقليدس

إذا كان P لا يقسم A فإن $\gcd(P, A) = 1$ لأن P غير قابل للاختزال. إذن، بواسطة توطئة غاوس، P يقسم B.