2.3 Primitive Elemente

Definition 128

Sei K ein endlicher Körper. Ein Element a, das die multiplikative Gruppe $K^* = K \setminus \{0\}$ erzeugt, nennt man primitives Element.

Beispiel 129

In $\mathbb{Z}_5^*$ sind sowohl 2 als auch 3 primitive Elemente:

$$\begin{array}{ll} 2^0 = 1 & 3^0 = 1 \\ 2^1 = 2 & 3^1 = 3 \\ 2^2 = 4 & 3^2 = 4 \\ 2^3 = 3 & 3^3 = 2 \\ (2^4 = 1 & 3^4 = 1) \end{array}$$

Bemerkung: $\langle \mathbb{Z}_4, +_4, \cdot_4, 0, 1 \rangle$ ist kein Körper!

Beispiel 130

Setzt man $K = \{0, 1, a, b\}$ und definiert eine Addition und Multiplikation wie folgt:

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

so bildet $\langle K, \oplus, \odot, 0, 1 \rangle$ einen Körper (Übung!).

3. Polynome

3.1 Definition und Grundlagen

Definition 131
Sei R ein (kommutativer) Ring. Ein Polynom über R in der Variablen x ist eine Funktion p der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

wobei $n \in \mathbb{N}_0$, $a_i \in R$ und $a_n \neq 0$.
n heißt der Grad des Polynoms, $a_0, \ldots, a_n$ seine Koeffizienten.
Die Funktion p ordnet jedem Wert $x_0 \in R$ den Wert $p(x_0) \in R$ zu, ist also eine Funktion von R nach R.
$R[x]$ bezeichnet die Menge der Polynome über dem Ring R in der Variablen x.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel 132

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

Berechnung des Funktionswertes

Um den Wert eines Polynoms an einer bestimmten Stelle $x_0 \in R$ zu bestimmen, verwendet man am besten das sogenannte Hornerschema:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ &= ((\ldots(((a_n x + a_{n-1})x + a_{n-2})x + ...)x + a_1)x + a_0. \end{aligned}$$

Hat man die Koeffizienten in einem Array $a[0..n]$ abgespeichert, kann man den Funktionswert $p(x_0)$ daher wie folgt berechnen:

```
begin
  p ← a[n]
  for i = n-1 downto 0 do
    p ← p · x_0 + a[i]
  end
  return(p)
end
```

Beobachtung:
Für die Auswertung eines Polynoms vom Grad n genügen damit $O(n)$ Multiplikationen und Additionen.

Addition

Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ ist (sei o.B.d.A. $m \leq n$) definiert durch

$$(a+b)(x) = c_n x^n + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i \ .$$

Bemerkungen:

- An sich fehlende Koeffizienten sind gleich 0 gesetzt.
- Für den Grad des Summenpolynoms gilt

$$\mathrm{grad}(a+b) \leq \max\{\mathrm{grad}(a), \mathrm{grad}(b)\} \ .$$

Beispiel 133

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich $(a + b)(x) = x^2 + x + 7$. Hier gilt $\text{grad}(a + b) = 2 = \text{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen $(a + b)(x) = 2$ und somit $\text{grad}(a + b) = 0 < 3 = \max\{\text{grad}(a), \text{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\leq n$ lässt sich in $O(n)$ arithmetischen Schritten berechnen.

Multiplikation

Das Produkt zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ erhält man durch Ausmultiplizieren und anschliessendes Sortieren und Zusammenfassen der Koeffizienten. Also

$$(a \cdot b)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Für den Grad des Produktpolynoms gilt

$$\operatorname{grad}(a \cdot b) = \operatorname{grad}(a) + \operatorname{grad}(b) \ ,$$

falls R nullteilerfrei sowie $a \neq 0 \neq b$ ist, ansonsten

$$\operatorname{grad}(a \cdot b) \leq \operatorname{grad}(a) + \operatorname{grad}(b) \ .$$

Beispiel 134

Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + \\ &\qquad ((-3) \cdot 2 + 5 \cdot 4)x + 5 \cdot 2 \\ &= 4x^3 - 10x^2 + 14x + 10\,.\end{aligned}$$

Man sagt auch, dass die Koeffizienten

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

des Produktpolynoms durch Faltung der Koeffizientenfolgen von $a(x)$ und $b(x)$ entstehen.

Beobachtung:
Das Produkt zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Es gibt dafür aber auch schnellere Algorithmen!

Division

Für diesen Abschnitt setzen wir voraus, dass der Koeffizientenring ein Körper ist.

Betrachte das Schema

$$
\begin{array}{rl}
 & 2x^4 + x^3 + x + 3 \ \text{ div } \ x^2 + x - 1 \ = \ 2x^2 - x + 3 \\
\underline{-(2x^4 + 2x^3 - 2x^2)} & \\
 & -x^3 + 2x^2 + x + 3 \\
\underline{-(-x^3 - x^2 + x)} & \\
 & 3x^2 + 3 \\
\underline{-(3x^2 + 3x - 3)} & \\
 & -3x + 6
\end{array}
$$

Satz 135

Zu je zwei Polynomen $a(x)$ und $b(x)$, $b \neq 0$, gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, so dass

$$a(x) = q(x)b(x) + r(x) \text{ und } r = 0 \text{ oder } \operatorname{grad}(r) < \operatorname{grad}(b).$$

Beispiel 136

Im vorhergehenden Schema war das

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)} \cdot \underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}$$

Beweis:
Gilt $\mathrm{grad}(a) < \mathrm{grad}(b)$, so kann man $q = 0$ und $r = a$ setzen. Sei also $\mathrm{grad}(a) \geq \mathrm{grad}(b)$.

Induktion über $\mathrm{grad}(a)$:
Ist $\mathrm{grad}(a) = 0$, so folgt aus $\mathrm{grad}(a) \geq \mathrm{grad}(b)$, dass a und b beides konstante Funtionen sind. Also $a(x) = a_0$ und $b(x) = b_0$ mit $b_0 \neq 0$. Wir können daher $q(x) = a_0/b_0$ und $r(x) = 0$ setzen.

Beweis (Forts.):

Ist $\text{grad}(a) = n > 0$ und $\text{grad}(b) = m$, $m \leq n$, und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m)x^{n-m} \cdot b(x) \; .$$

Dann gilt $\text{grad}(\tilde{a}) < \text{grad}(a)$.

Nach Induktionsannahme gibt es daher Polynome $\tilde{q}(x)$ und $\tilde{r}(x)$ mit $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$, mit $\tilde{r}(x) = 0$ oder $\text{grad}(\tilde{r}) < \text{grad}(b)$ (falls $m = n$, wird $\tilde{q}(x) = 0$ und $\tilde{r}(x) = \tilde{a}(x)$). Es gilt

$$a(x) \; = \; (a_n/b_m)x^{n-m}b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \; =: \; q(x)b(x) + r(x) \; .$$

Beweis (Forts.):

Um die Eindeutigkeit zu beweisen, nehmen wir an, es gäbe für Polynome a und b zwei Darstellungen wie im Satz angegeben. Also $q \cdot b + r = a = \hat{q} \cdot b + \hat{r}$ und somit auch

$$(q - \hat{q}) \cdot b = (\hat{r} - r).$$

Falls $q \neq \hat{q}$, ist die linke Seite ein Polynom vom Grad $\geq \mathrm{grad}(b)$. Da die rechte Seite aus der Differenz zweier Polynome vom Grad kleiner als $\mathrm{grad}(b)$ besteht, Widerspruch! Also ist $q = \hat{q}$ und damit auch $r = \hat{r}$.

□

Beobachtung:
Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 135 wie im Beispiel bestimmen. Da sich der Grad des Polynoms in jeder Zeile verringert, benötigen wir also höchstens n Multiplikationen von Polynomen mit Konstanten und n Subtraktionen von Polynomen vom Grad höchstens n.

Insgesamt ergibt sich:

Die Division zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Beobachtung:
Falls der führende Koeffizient des Divisorpolynoms gleich 1 ist, lässt sich die Division auch über einem Ring R durchführen.

3.3 Nullstellen von Polynomen

Definition 137
Eine Nullstelle eines Polynoms p ist ein Wert x_0 mit $p(x_0) = 0$.

Lemma 138
Sei $p \in R[x]$, $x_0 \in R$ eine Nullstelle von p. Dann ist $p(x)$ ohne Rest durch $x - x_0$ teilbar.

Beweis:
Nach Satz 135 gibt es Polynome q und r mit $p(x) = q(x) \cdot (x - x_0) + r(x)$ und $\text{grad}(r) < \text{grad}(x - x_0) = 1$, also $\text{grad}(r) = 0$, d.h. $r(x) = r_0$. Wegen $p(x_0) = q(x_0) \cdot (x_0 - x_0) + r_0 = r_0$ muss also r_0 gleich Null sein. D.h., $p(x) = q(x) \cdot (x - x_0)$. □

Satz 139 (Fundamentalsatz der Algebra)

Jedes Polynom $p \neq 0$ mit Grad n hat höchstens n Nullstellen.

Beweis:

Wir zeigen den Satz durch Induktion über den Grad des Polynoms. Ist p ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme $p \neq 0$ offenbar richtig.
Ist p ein Polynom mit Grad $n > 0$, so hat p entweder keine Nullstelle (und die Aussage ist somit trivialerweise richtig) oder p hat mindestens eine Nullstelle a. Dann gibt es nach Lemma 138 eine Darstellung $p(x) = q(x) \cdot (x - a)$ mit $\mathrm{grad}(q) = n - 1$. Nach Induktionsannahme hat q höchstens $n - 1$ und somit p höchstens n Nullstellen. □

Beispiele 140

- Das Polynom $x^2 - 1 = (x + 1)(x - 1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

3.4 Partialbruchzerlegung

Beispiel 141

Finde zu $\frac{g}{f} = \frac{x^2+1}{(x-1)^2(x-2)}$ Polynome p, q mit $\operatorname{grad}(p) < 2$, $\operatorname{grad}(q) < 1$ und

$$\frac{x^2+1}{(x-1)^2(x-2)} = \frac{p}{(x-1)^2} + \frac{q}{x-2}. \qquad (*)$$

Die r.S. von (*) heißt Partialbruchzerlegung von $\frac{g}{f}$.

Ansatz: $p(x) = ax + b$, $q(x) = c$.

$$\frac{p}{(x-1)^2} + \frac{q}{x-2} = \frac{(x-2)\cdot p + (x-1)^2 \cdot q}{(x-1)^2(x-2)}.$$

Durch Vergleich mit (*) erhält man

$$\begin{aligned} x^2+1 &= (ax+b)(x-2)+c(x-1)^2 \\ &= (a+c)x^2+(b-2a-2c)x+c-2b. \end{aligned}$$

Koeffizientenvergleich liefert folgendes lineares Gleichungssystem:

$$\begin{aligned} a+c &= 1 \\ b-2a-2c &= 0 \\ c-2b &= 1 \end{aligned}$$

Dieses hat die eindeutige Lösung $a=-4, \quad b=2, \quad c=5$. Somit gilt:

$$\frac{x^2+1}{(x-1)^2(x-2)} = \frac{-4x+2}{(x-1)^2}+\frac{5}{x-2}.$$

Satz 142 (Partialbruchzerlegung)

Seien $f, g \in K[x]$ *(*$K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$*) Polynome mit* $\operatorname{grad}(g) < \operatorname{grad}(f)$*, und es gelte*

$$f(x) = (x - \alpha_1)^{m_1} \cdot \ldots \cdot (x - \alpha_r)^{m_r}$$

mit $\mathbb{N} \ni m_i \geq 1$ *und paarweise verschiedenen* $\alpha_i \in K$ *(*$i = 1, \ldots, r$*). Dann gibt es eindeutig bestimmte Polynome* $g_1, \ldots, g_r \in K[x]$ *mit* $\operatorname{grad}(g_i) < m_i$*, so dass gilt:*

$$\frac{g}{f} = \frac{g_1}{(x - \alpha_1)^{m_1}} + \cdots + \frac{g_r}{(x - \alpha_r)^{m_r}}.$$

Beweis:
Induktion nach r. Für $r = 1$ ist nichts zu zeigen. Es gelte $r > 1$. Sei $\tilde{f} = (x - \alpha_2)^{m_2} \cdot \ldots \cdot (x - \alpha_r)^{m_r}$. Dann gilt $f = (x - \alpha_1)^{m_1} \tilde{f}$. Sei $d = \mathrm{grad}(f)$ und $\tilde{d} = \mathrm{grad}(\tilde{f})$. Es genügt nun, Folgendes zu zeigen:
Zwischenbehauptung: Es gibt eindeutig bestimmte Polynome $A, B \in K[x]$ mit $\mathrm{grad}(A) < m_1$, $\mathrm{grad}(B) < \tilde{d}$, so dass

$$\frac{g}{f} = \frac{A}{(x - \alpha_1)^{m_1}} + \frac{B}{\tilde{f}} \tag{1}$$

gilt.
(Wendet man auf $\frac{B}{\tilde{f}}$ die Induktionsbehauptung an, so folgt die Behauptung des Satzes.)

Gleichung (1) ist äquivalent zu

$$A\tilde{f} + B(x-\alpha_1)^{m_1} = g. \tag{2}$$

Wir machen den Ansatz: $A = \sum_{i=0}^{m_1-1} a_i x^i$, $B = \sum_{j=0}^{\tilde{d}-1} b_j x^j$.
Durch Koeffizientenvergleich mit (2) erhalten wir folgendes inhomogene lineare Gleichungssystem bestehend aus d Gleichungen in den Unbestimmten $a_{m_1-1}, \ldots, a_0, b_{\tilde{d}-1}, \ldots, b_0$:

$$M \cdot \begin{pmatrix} a_{m_1-1} \\ \vdots \\ a_0 \\ b_{\tilde{d}-1} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} c_{d-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ c_0 \end{pmatrix}, \tag{3}$$

wobei M eine $d \times d$-Matrix ist, und $g = \sum_{i=0}^{d-1} c_i x^i$. Wir haben die Zwischenbehauptung bewiesen, wenn wir zeigen können, dass die Matrix M invertierbar ($\det M \neq 0$) ist. Dazu benötigen wir das folgende Lemma.

Lemma 143

Seien $\tilde{A}, \tilde{B} \in K[x]$ *Polynome mit* $\operatorname{grad}(\tilde{A}) \geq 1$ *und* $\operatorname{grad}(\tilde{B}) \geq 1$. *Gibt es dann Polynome* $A, B \in K[x]$, $A \neq 0$ *oder* $B \neq 0$, *mit* $\operatorname{grad}(A) < \operatorname{grad}(\tilde{A})$, $\operatorname{grad}(B) < \operatorname{grad}(\tilde{B})$ *und*

$$A\tilde{B} + B\tilde{A} = 0,$$

so sind $\tilde{A}$ *und* $\tilde{B}$ *nicht teilerfremd.*

Beweis:

Dies folgt sofort aus der Eindeutigkeit der Primfaktorzerlegung. □

Beweis (Forts.):

Nun zurück zum Beweis von Satz 142. Angenommen $\det(M) = 0$. Dann würde es einen Vektor $y = (a_{m_1-1}, \ldots, a_0, b_{\tilde{d}-1}, \ldots, b_0)^t \neq 0$ mit $M \cdot y = 0$ geben, d.h. es würde Polynome $A = \sum_{i=0}^{m_1-1} a_i x^i$ und $B = \sum_{j=0}^{\tilde{d}-1} b_j x^j$, $A \neq 0$ oder $B \neq 0$, geben mit $\mathrm{grad}(A) < m_1$, $\mathrm{grad}(B) < \tilde{d} = \mathrm{grad}(\tilde{f})$ und $A\tilde{f} + B(x - \alpha_1)^{m_1} = 0$.

Nach Lemma 143 wären dann $\tilde{f}$ und $(x - \alpha_1)^{m_1}$ nicht teilerfremd. Dies ist jedoch ein Widerspruch zur Voraussetzung. Damit ist Satz 142 bewiesen. □