



Lineare Algebra

2., aktualisierte Auflage

Theo de Jong

Aufgaben



Lösung

Aufgabe 3.17 Zeichnen Sie die komplexen Zahlen z , welche eine der nachfolgenden Gleichungen erfüllen.

- | | | |
|----------------------------|--------------------|------------------------|
| 1. $z^2 = i$ | 2. $(z + 1)^2 = i$ | 3. $(z + 2 - i)^2 = i$ |
| 4. $z^2 = -2\sqrt{3} + 2i$ | 5. $z^3 = 1$ | 6. $z^4 = 1$ |
| 7. $z^6 - 2z^3 + 1 = 0$ | 8. $(z - i)^4 = 1$ | 9. $z^6 = 1$ |

Aufgabe 3.18 Lösen Sie die nachfolgenden Gleichungen.

- | | |
|-----------------------|---|
| 1. $z^2 - 2z + 2 = 0$ | 2. $z^2 + 4z + 6 = 0$ |
| 3. $z^2 + 4z - 8 = 0$ | 4. $z^4 + 8 - 8\sqrt{3}i = 0$ |
| 5. $z^2 + iz + 2 = 0$ | 6. $z^2 + (2 - 2i)z - 2 - 2(1 + \sqrt{3})i = 0$ |

Aufgabe 3.19 Bestimmen Sie die komplexen Zahlen a , sodass die Gleichung

$$iz^2 + (a - 3 + i)z - 12 + 5i = 0$$

genau eine Lösung hat.

Aufgabe 3.20 Bestimmen Sie die reellen Zahlen a , sodass die Gleichung

$$(3 + 4i)z^2 - (a + 5)z + (2 - 4i) = 0$$

eine reelle Lösung hat und lösen Sie dann diese Gleichung.

Aufgabe 3.21 (cardanische Formel) Betrachten Sie die Gleichung $x^3 = px + q$ in x mit p, q in \mathbb{C} und $p \neq 0$. Seien z, u komplexe Zahlen mit

$$z^2 = \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^2 \quad \text{und} \quad u^3 = \frac{q}{2} + z.$$

Zeigen Sie, dass $x = u + p/(3u)$ eine Lösung der Gleichung $x^3 = px + q$ ist.

Tipp: Berechnen Sie $x^3 - px$ und zeigen Sie, dass $u^6 - qu^3 + p^3/27 = 0$.

Aufgabe 3.22 Finden Sie mithilfe der cardanischen Formel eine Lösung für:

- | | |
|--------------------|--------------------|
| 1. $x^3 = 9x + 28$ | 2. $x^3 = -3x + 4$ |
|--------------------|--------------------|

Was fällt bei der zweiten Gleichung auf?

3.5 Polynome

1. Ein Polynom mit Koeffizienten in einem Körper K ist ein Ausdruck der Form $f = f(x) = a_0 + a_1x + \dots + a_nx^n$ mit $a_1, \dots, a_n \in K$. Ist $a_n \neq 0$, so nennt man n den **Grad** von f , Notation $\deg(f)$. Dem Nullpolynom geben wir den Grad $-\infty$. Ein Polynom f wie oben heißt *normiert*, wenn $a_n = 1$. Die Menge der Polynome bezeichnen wir mit $K[x]$.
2. Für Polynome $f = a_0 + \dots + a_nx^n$ und $g = b_0 + \dots + b_nx^n$ definieren wir

$$f + g := (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n,$$

$$f \cdot g := a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0)x + \dots + (a_{n-1} \cdot b_n + a_n \cdot b_{n-1})x^{2n-1} + a_n \cdot b_nx^{2n}.$$
3. Ist $f = a_0 + a_1x + \dots + a_nx^n$ und $\lambda \in K$, so ist $f(\lambda) := a_0 + a_1\lambda + \dots + a_n\lambda^n$.
4. Eine Zahl $\alpha \in K$ heißt **Nullstelle** von f , wenn $f(\alpha) = 0$.

Satz 3.5 (Polynomdivision) Seien $f(x), g(x)$ Polynome. Dann gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, sodass

$$g(x) = q(x) \cdot f(x) + r(x), \quad \deg(r) < \deg(f).$$

Existenz. Beweis mit Induktion nach $\deg(g)$. Ist $\deg(g) < \deg(f)$, so nehmen wir $q = 0$ und $r = g$. Sei $g = b_mx^m + \dots + b_0$ und $f = a_nx^n + \dots + a_0$ mit $m \geq n$ und $a_n \neq 0$. Dann ist der Grad von $\tilde{g} := g - \frac{b_m}{a_n} \cdot x^{m-n}f$ kleiner als m , deshalb gilt nach Induktionsannahme $\tilde{g} = \tilde{q} \cdot f + r$ für gewisse \tilde{q} und r . Nimm nun $q = \tilde{q} + \frac{b_m}{a_n}x^{m-n}f(x)$.

Eindeutigkeit. Ist $q \cdot f + r = \tilde{q}f + \tilde{r}$, so folgt $(q - \tilde{q})f = \tilde{r} - r$. Links steht 0 oder ein Polynom vom Grad $\geq n$, rechts steht 0 oder ein Polynom vom Grad kleiner n . Es folgt $r = \tilde{r}$ und $q = \tilde{q}$. ■

Beispiel

$$\begin{array}{r}
 f(x) = (x^3 \quad +2x^2 \quad -3x \quad +7) : (x^2 - x + 2) = x + 3 \\
 \underline{x^3 \quad -x^2 \quad +2x} \\
 3x^2 \quad -5x \quad +7 \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\
 \quad -3x \quad +6 \quad \quad \quad g(x) \quad \quad \quad q(x) \\
 \underline{ -2x \quad +1} \leftarrow r(x)
 \end{array}$$

Der Beweis der Polynomdivision ist ähnlich dem Beweis der Division mit Rest für die ganzen Zahlen. Diese Division formulieren wir im Folgenden.

Satz 3.6 (Teilung mit Rest) Sind a, b ganze Zahlen mit $b > 0$, so gibt es eindeutig bestimmte $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $a = q \cdot b + r$ und $0 \leq r < b$.

Aufgaben



Lösung

Aufgabe 3.23 Beweisen Sie Satz 3.6.

Aufgabe 3.24 Sei K ein Körper und $f \in K[x]$.

1. α ist eine Nullstelle von f genau dann, wenn $f = (x - \alpha) \cdot q$ für ein Polynom q .
2. f hat höchstens $\deg(f)$ Nullstellen.

Aufgabe 3.25 Führen Sie die Polynomdivision für die nachfolgenden Polynome durch.

1. $g(x) = x^5 + 2x^3 - x^2 + 5x - 7$, $f(x) = x^2 - 2x + 1$
2. $g(x) = 4x^4 + 3x^2 - 5x - 3$, $f(x) = x - 2$
3. $g(x) = x^7 - 1$, $f(x) = x - 1$

Aufgabe 3.26 Es sei $f(x) = a_n x^n + \dots + a_1 x + a_0$ ein Element von $K[x]$. Die Ableitung von f ist gegeben durch

$$f'(x) = n a_n x^{n-1} + \dots + a_1.$$

Zeigen Sie:

1. $(f + g)' = f' + g'$
2. $(cf)' = c \cdot f'$ für $c \in K$
3. $(f \cdot g)' = f' \cdot g + g' \cdot f$
Tipp: Nehmen Sie zunächst $f = x^n$ und $g = x^m$.
4. Ist $f = g^k \cdot h$, so ist $f' = k \cdot g' \cdot g^{k-1} \cdot h + g^k \cdot h'$.

Aufgabe 3.27 (Der Körper der rationalen Funktionen $K(x)$) Eine rationale Funktion ist ein Bruch $\frac{f(x)}{g(x)}$, wobei $f(x), g(x)$ Polynome sind und $g(x) \neq 0$ gilt. Zwei rationale Funktionen $\frac{f_1(x)}{g_1(x)}$ und $\frac{f_2(x)}{g_2(x)}$ sind gleich genau dann, wenn $f_1(x)g_2(x) = g_1(x)f_2(x)$. Betrachten Sie die Menge $K(x)$ der rationalen Funktionen mit der Addition und Multiplikation:

$$\begin{aligned} \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} &= \frac{f_1(x) \cdot g_2(x) + f_2(x)g_1(x)}{g_1(x) \cdot g_2(x)} \\ \frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} &= \frac{f_1(x) \cdot f_2(x)}{g_1(x) \cdot g_2(x)} \end{aligned}$$

Zeigen Sie, dass $K(x)$ ein Körper ist und ein Polynom $f(x)$ als rationale Funktion gesehen werden kann.

3.6 Primzahlen, irreduzible Polynome

1. Seien $a, b \in \mathbb{Z}$. Ist $a \cdot c = b$ für ein $c \in \mathbb{Z}$, so heißt a Teiler von b , Notation $a \mid b$.
2. $p \in \mathbb{N}$ heißt Primzahl, wenn $p \neq 1$ und $\pm 1, \pm p$ die einzigen Teiler von p sind.
3. Eine ganze Zahl $d > 0$ heißt der größte gemeinsame Teiler $\text{ggT}(a, b)$ von $a, b \in \mathbb{Z}$, wenn $d \mid a, d \mid b$ und aus $c > 0, c \mid a, c \mid b$ folgt, dass $c \mid d$.
4. Sei K ein Körper, $f, g \in K[x]$. Dann heißt f Teiler von g , Notation $f \mid g$, wenn $f \cdot h = g$ für ein $h \in K[x]$.
5. Sei K ein Körper. Ein Polynom $f \in K[x]$ heißt irreduzibel, wenn $\deg(f) \geq 1$ und die Polynome $c \in K$ und cf für $c \in K$ die einzigen Teiler von f sind.
6. Ein $d \in K[x]$ heißt der größte gemeinsame Teiler $\text{ggT}(f, g)$ von $f, g \in K[x]$, wenn d normiert ist, $d \mid f, d \mid g$ und aus $e \mid f, e \mid g$ folgt, dass $e \mid d$.

Satz 3.7

1. Sind $a, b \in \mathbb{Z}$, beide ungleich 0, so existiert der $\text{ggT}(a, b) =: d$ und es gilt $d = xa + yb$ für gewisse $x, y \in \mathbb{Z}$.
2. Sei p eine Primzahl und $p \mid a \cdot b$. Dann ist $p \mid a$ oder $p \mid b$.
3. Für jedes $a \in \mathbb{N}$ mit $a > 1$ gilt: $a = \pm p_1 \cdot \dots \cdot p_s$, wobei $p_1 \leq \dots \leq p_s$ eindeutig bestimmte Primzahlen sind.
4. Ist K ein Körper, $f, g \in K[x]$, beide ungleich 0. Dann existiert der $\text{ggT}(f, g) = d$ und es gilt $d = Af + Bg$ für gewisse $A, B \in K[x]$. A und B werden die Bézoutkoeffizienten von f und g genannt.
5. Ist $f \in K[x]$ mit $\deg(f) \geq 1$, so gibt es normierte irreduzible Polynome f_1, \dots, f_s und $c \in K$ mit $f = c \cdot f_1 \cdot \dots \cdot f_s$. Bis auf die Reihenfolge sind die f_i eindeutig bestimmt.

1. Sei $D = \{ma + nb : m, n \in \mathbb{Z}\}$. Weil $\pm a, \pm b$ Elemente von D sind, enthält D positive Elemente. Sei $d = xa + yb$ das kleinste positive Element von D . Es ist $a = qd + r$ mit $0 \leq r < d$. Dann gilt $r = (1 - qx)a + (-qy)b \in D$ und es folgt $r = 0$. Also $d \mid a$ und analog $d \mid b$. Ist $e \mid a$ und $e \mid b$, dann $e \mid d = xa + yb$. Also ist d der größte gemeinsame Teiler von a und b .
2. Gilt $p \nmid a$, so ist $\text{ggT}(p, a) = 1$ und es existieren x, y mit $1 = xa + yp$. Multiplizieren mit b ergibt $b = xab + ybp$. Aus $p \mid xab$ und $p \mid ybp$ folgt $p \mid b$.
3. Induktion nach $a > 1$. Ist a eine Primzahl, so ist $s = 1$ und $p_1 = a$. Sonst ist $a = b \cdot c$ mit $b, c < a$. Nach Induktionsannahme sind b, c Produkte von Primzahlen. Also ist a ein Produkt $p_1 \cdot \dots \cdot p_s$ von Primzahlen. Zum Nachweis der Eindeutigkeit sei $p_1 \cdot \dots \cdot p_s = q_1 \cdot \dots \cdot q_t$. Es folgt $p_s \mid q_1 \cdot \dots \cdot q_t$. Mit Induktion folgt $p_s \mid q_i$ für ein i . Analog gilt $q_i \mid p_j$ für ein j . Also folgt $p_s \mid p_j$ und $p_s = p_j = q_j$. O.B.d.A. gilt $p_s = q_t$ und $p_1 \cdot \dots \cdot p_{s-1} = q_1 \cdot \dots \cdot q_{t-1}$. Mit Induktion folgt die Behauptung.
4. und 5. zeigt man analog. ■

Aufgaben



Lösung

Aufgabe 3.28 Beweisen Sie die Aussagen 4. und 5. des Satzes 3.7.

Aufgabe 3.29 (Euklidischer Algorithmus zur ggT-Berechnung) Seien $a, b \in \mathbb{N}$ mit $a > b$. Wir definieren $a_0 = a, a_1 = b$ und induktiv durch Teilung mit Rest $a_{n-1} = q_n a_n + a_{n+1}$.

1. Zeigen Sie: $a_0 > a_1 > \dots > a_k > a_{k+1} = 0$ für ein k .
2. Zeigen Sie, dass für diese Zahl k gilt: $\text{ggT}(a, b) = a_k$.
3. Seien $x_0 = y_1 = 1, x_1 = y_0 = 0$ und x_{n+1} und y_{n+1} induktiv definiert durch: $x_{n-1} = q_n x_n + x_{n+1}, y_{n-1} = q_n y_n + y_{n+1}$. Zeigen Sie, dass $x_n a + y_n b = a_n$. Mit $x_n = x$ und $y_n = y$ gilt deshalb $\text{ggT}(a, b) = xa + yb$ (erweiterter euklidischer Algorithmus).
4. Seien $a = 2003$ und $b = 1812$. Berechnen Sie a_n, q_n, x_n und y_n in der nachfolgenden Tabelle. Zeigen Sie, dass $a_8 = 0$.

n	0	1	2	3	4	5	6	7	8
a_n	2003	1812							
x_n	1	0							
y_n	0	1							
q_n									

5. Führen Sie den erweiterten euklidischen Algorithmus für die nachfolgenden Zahlen durch.
 1. $a = 313, b = 217$
 2. $a = 1767, b = 533$
 3. $a = 1891, b = 1273$
6. Formulieren Sie einen euklidischen und einen erweiterten euklidischen Algorithmus für Polynome. Beweisen Sie die Aussagen 1.–3. aus dieser Aufgabe.

Aufgabe 3.30

1. Sei K ein Körper, $f \in K[x]$ mit $\deg(f) = 2$ oder $\deg(f) = 3$. Zeigen Sie, dass f irreduzibel ist genau dann, wenn f keine Nullstelle in K hat.
2. Warum ist diese Aussage im Allgemeinen falsch für $\deg(f) = 4$?

Aufgabe 3.31

1. Eine rationale Zahl p/q mit $\text{ggT}(p, q) = 1$ sei Lösung einer Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$$

mit $a_i \in \mathbb{Z}$ und $a_0, a_n \neq 0$. Zeigen Sie, dass $p \mid a_0$ und $q \mid a_n$.

2. Sei $n > 2$ und p eine Primzahl. Zeigen Sie, dass $\sqrt[n]{p} \notin \mathbb{Q}$.

Aufgabe 3.32

1. Es sei $\text{ggT}(a, c) = 1$ und $c \mid (ab)$. Zeigen Sie, dass $c \mid b$.
2. Sei $\text{ggT}(a, b) = 1$ und $a \mid c, b \mid c$. Zeigen Sie: $(ab) \mid c$.

Aufgabe 3.33 Zeigen Sie, dass es unendlich viele Primzahlen gibt (Euklid).

3.7 Die Körper \mathbb{F}_p und $K[x]/\langle f \rangle$

1. Seien $a, b \in \mathbb{N}$. Ist $a = qb + r$ mit $0 \leq r < b$, so schreiben wir $r = a \bmod b$. Analoges gilt für Polynome $f, g \in K[x]$.

2. Sei p eine Primzahl und $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. Wir definieren für $a, b \in \mathbb{F}_p$:

$$a +_p b := a + b \bmod p, \quad a \cdot_p b := a \cdot b \bmod p.$$

3. Sei K ein Körper, $f \in K[x]$ irreduzibel und $n = \deg(f)$. Sei $K[x]/\langle f \rangle = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_1, \dots, a_{n-1} \in K\}$. Wir definieren für $a, b \in K[x]/\langle f \rangle$:

$$a +_f b := a + b, \quad a \cdot_f b := a \cdot b \bmod f.$$

Satz 3.8 **1.** Ist p eine Primzahl, so ist \mathbb{F}_p zusammen mit der Addition $+_p$ und der Multiplikation \cdot_p ein Körper.

2. Ist K ein Körper und $f \in K[x]$ irreduzibel, so ist $K[x]/\langle f \rangle$ zusammen mit der Addition $+_f$ und der Multiplikation \cdot_f ein Körper.

Wir beweisen **1.** Die Aussage **2.** zeigt man analog. Sei $\bar{a} := a \bmod p$ für $a \in \mathbb{Z}$.

$$\overline{a+b} = a+b - q_3p = \bar{a} + \bar{b} + (q_1 + q_2 - q_3)p = (q_4 + q_1 + q_2 - q_3)p + \bar{a} + \bar{b}$$

für gewisse q_3 und q_4 . Wegen der Eindeutigkeit der Teilung mit Rest folgt $\overline{a+b} = \bar{a} + \bar{b}$. Analog gilt $\overline{a \cdot b} = \bar{a} \cdot \bar{b}$.

Nun zeigen wir zum Beispiel die Distributivität.

$$\begin{aligned} a \cdot_p (b +_p c) &= a \cdot_p (\bar{b} + \bar{c}) = \overline{a \cdot (\bar{b} + \bar{c})} = \overline{a \cdot \bar{b} + a \cdot \bar{c}} = \overline{\bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}} \\ &= \overline{\bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}} = \overline{\bar{a} \cdot_p \bar{b} + \bar{a} \cdot_p \bar{c}} = \bar{a} \cdot_p \bar{b} +_p \bar{a} \cdot_p \bar{c} \end{aligned}$$

Die anderen Rechenregeln – bis auf die Existenz des Inversen – zeigt man analog. Zum Beweis der Existenz des Inversen: Ist $a \in \mathbb{F}_p$ mit $a \neq 0$, so ist $\text{ggT}(a, p) = 1$, weil p eine Primzahl ist. Es existieren deshalb x, y mit $xa + yp = 1$. Sei $x = sp + b$ mit $0 < b < p$. Dann gilt $a \cdot b = (-as - y)p + 1$, es folgt $a \cdot_p b = 1$. ■

Wir werden ab jetzt einfach $a+b$ statt $a+_pb$ oder $a \cdot b$ statt $a \cdot_p b$ schreiben. Analog für $+_f$ und \cdot_f .

Beispiele

1. Das Polynom $x^2 + 1 \in \mathbb{R}[x]$ ist irreduzibel. Somit ist $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ ein Körper, welcher eine äquivalente Beschreibung des Körpers \mathbb{C} ist.

2. Betrachte den Körper mit 2 Elementen $\mathbb{F}_2 = \{0, 1\}$ und $f = x^2 + x + 1$. Dann ist f irreduzibel, weil $\deg(f) = 2$ und f keine Nullstellen hat. Es folgt, dass $\mathbb{F}_2[x]/\langle f \rangle = \{a + bx : a, b \in \{0, 1\}\}$ ein Körper mit vier Elementen ist, siehe Aufgabe 3.3.

Aufgaben



Lösung

Aufgabe 3.34 Wenn wir in der Definition von \mathbb{F}_p bzw. $K[x]/\langle f \rangle$ nicht annehmen, dass p eine Primzahl bzw. f ein irreduzibles Polynom ist, warum liegt dann kein Körper vor?

Aufgabe 3.35

1. Zeigen Sie, dass 101 und 127 Primzahlen sind.
2. Berechnen Sie $45 \cdot 14$ in \mathbb{F}_{101} und in \mathbb{F}_{127} .
3. Berechnen Sie den Kehrwert von 23 in \mathbb{F}_{101} und in \mathbb{F}_{127} .
4. Berechnen Sie den Kehrwert von 10 in \mathbb{F}_{101} und in \mathbb{F}_{127} .

Aufgabe 3.36

1. Welche irreduziblen Polynome in $\mathbb{F}_2[x]$ vom Grad zwei gibt es?
2. Konstruieren Sie ein irreduzibles Polynom in $\mathbb{F}_2[x]$ vom Grad drei.
3. Konstruieren Sie irreduzible Polynome vom Grad vier und fünf in $\mathbb{F}_2[x]$.

Aufgabe 3.37 Sei $f = x^2 + 3x + 5 \in \mathbb{F}_7[x]$.

1. Zeigen Sie, dass $\mathbb{F}_7[x]/\langle f \rangle$ ein Körper ist.
2. Wie viel Elemente hat $\mathbb{F}_7[x]/\langle f \rangle$?
3. Berechnen Sie $(x+2) \cdot (3x+4) \in \mathbb{F}_7[x]/\langle f \rangle$.
4. Berechnen Sie den Kehrwert von x und von $3x+1$ in $\mathbb{F}_7[x]/\langle f \rangle$.

Aufgabe 3.38

1. Sei $x \in \mathbb{F}_p$ mit $x \neq 0$. Zeigen Sie, dass $x^{p-1} = 1$ (kleiner Satz von Fermat).
Tipp: Zeigen Sie, dass $\mathbb{F}_p \setminus \{0\} = \{x, 2x, \dots, (p-1)x\}$, und betrachten Sie $N = 1 \cdot 2 \cdot \dots \cdot (p-1)$.
2. Sei K ein Körper mit q Elementen und $x \in K$ mit $x \neq 0$. Zeigen Sie, dass $x^{q-1} = 1$.
3. Sei p eine Primzahl und $1 \leq k \leq p-1$. Zeigen Sie, dass $\binom{p}{k}$ eine durch p teilbare natürliche Zahl ist.
4. (Falsche binomische Formel) Sind $f, g \in \mathbb{F}_p[x]$, so zeigen Sie, dass $(f+g)^p = f^p + g^p$.

Aufgabe 3.39 Warum gibt es keinen Körper mit sechs Elementen?

Aufgabe 3.40

1. Bestimmen Sie den Kehrwert von 2 in \mathbb{F}_p für $p = 3, 5, 7, 11, 13, 17$.
2. Bestimmen Sie ein $a \in \mathbb{F}_p$ mit $\{a, a^2, \dots, a^{p-1}\} = \mathbb{F}_p \setminus \{0\}$ für $p = 3, 5, 7, 11$.
3. Sei K der Körper $\mathbb{F}_3[x]/\langle x^2+1 \rangle$ mit neun Elementen. Bestimmen Sie ein $a \in K$ mit $\{a, a^2, \dots, a^8\} = K \setminus \{0\}$.

3.8 *Der chinesische Restsatz*

Ist $n \in \mathbb{N}$, so können wir auf $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$ eine Addition und eine Multiplikation durchführen, genauso wie wir es für $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ im Falle einer Primzahl getan haben. Ist n zusammengesetzt, so ist $n = a \cdot b$ mit $0 < a, b < n$, also $a \cdot b = 0 \in \mathbb{Z}/n\mathbb{Z}$, aber $a, b \neq 0$ als Elemente von $\mathbb{Z}/n\mathbb{Z}$. Dies kann in einem Körper nicht vorkommen. Ist $a \cdot b = 0$ und $a \neq 0$, so folgt $b = a^{-1}ab = a^{-1} \cdot 0 = 0$. Deshalb ist $\mathbb{Z}/n\mathbb{Z}$, wenn n keine Primzahl ist, kein Körper.

Ähnliches gilt für Polynome $f \in K[x]$ (nicht notwendigerweise irreduzibel). Ist $n = \deg(f)$, so können wir auf der Menge

$$K[x]/\langle f \rangle = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_0, \dots, a_{n-1} \in K\}$$

eine Addition und Multiplikation einführen. Genau dann ist $K[x]/\langle f \rangle$ ein Körper, wenn f irreduzibel ist.

Satz 3.9 (Chinesischer Restsatz)

1. Seien $n = p \cdot q$ mit p, q teilerfremde natürliche Zahlen. Dann ist

$$\begin{aligned} \varphi: \mathbb{Z}/(pq)\mathbb{Z} &\rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ a &\rightarrow (a \bmod p, a \bmod q) \end{aligned}$$

bijektiv.

2. Es sei K ein Körper und $g, h \in K[x]$ teilerfremde Polynome. Dann ist

$$\begin{aligned} \varphi: K[x]/\langle g \cdot h \rangle &\rightarrow K[x]/\langle g \rangle \times K[x]/\langle h \rangle \\ f &\rightarrow (f \bmod g, f \bmod h) \end{aligned}$$

bijektiv.

1. Wir zeigen, dass die Abbildung φ injektiv ist. Ist $\varphi(a) = \varphi(b)$ mit o.E. $a \geq b$ so ist $(a-b)$ sowohl durch p , als auch durch q teilbar. Also pq teilt $a-b$ und es folgt $a = b \bmod n = pq$.

Für die Surjektivität bestimme $c, d \in \mathbb{Z}$ mit $c \cdot p + d \cdot q = 1$ (Zum Beispiel mit dem erweiterten euklidischen Algorithmus). Ist $(a, b) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, dann gilt mit

$$x = adq + bcp,$$

dass $x = a \bmod p$ und $x = b \bmod q$. Also ist φ surjektiv.

2. Analog. ■

Beispiel Es sei $p = 13$ und $q = 11$. Wir bestimmen eine Zahl a mit $a = 4 \bmod 13$ und $a = 5 \bmod 11$.

Mit dem erweiterten euklidischen Algorithmus erhalten wir $-5 \cdot 13 + 6 \cdot 11 = 1$. Also ist $-65 = 0 \bmod 13$, $-65 = 1 \bmod 11$ und $66 = 0 \bmod 13$, $66 = 0 \bmod 11$. Die Lösung ist deshalb $a = 4 \cdot 66 + 5 \cdot (-65) \bmod 143$. Man rechnet nach, dass $a = 82$.

13	11	2	1
1	0	1	-5
0	1	-1	6
	1	5	

Aufgaben



Lösung

Aufgabe 3.41 Geben Sie einen viel einfacheren Beweis für die Bijektivität von $\varphi: \mathbb{Z}/(pq)\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, wenn $\text{ggT}(p, q) = 1$.

Aufgabe 3.42

- Es seien $p_1, \dots, p_s \in \mathbb{N}$ mit $p_i \geq 2$ und alle teilerfremd. Sei $n = p_1 \cdot \dots \cdot p_s$. Zeigen Sie, dass die nachfolgende Abbildung bijektiv ist.

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_s\mathbb{Z} \\ x &\mapsto (x \bmod p_1, \dots, x \bmod p_s) \end{aligned}$$

- Analog: Sei K ein Körper und $f_1, \dots, f_s \in K[x]$ mit $\deg(f_i) \geq 1$ und alle teilerfremd. Sei $f = f_1 \cdot \dots \cdot f_s$. Zeigen Sie, dass die nachfolgende Abbildung bijektiv ist.

$$\begin{aligned} K[x]/\langle f \rangle &\rightarrow K[x]/\langle f_1 \rangle \times \dots \times K[x]/\langle f_s \rangle \\ g &\mapsto (g \bmod f_1, \dots, g \bmod f_s) \end{aligned}$$

Aufgabe 3.43 Lösen Sie die folgenden Gleichungssysteme.

- $x = 3 \bmod 7, x = 6 \bmod 11$.
- $x = 3 \bmod 7, x = 6 \bmod 11, x = 4 \bmod 13$.
- $x = 43 \bmod 101, x = 57 \bmod 127$.

Aufgabe 3.44 Es sei $g = x^2 + x + 1 \in \mathbb{F}_2[x]$ und $h = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Finden Sie ein Polynom $f \in \mathbb{F}_2[x]$, sodass $f = x \bmod g$ und $f = x^2 + 1 \bmod h$.

Aufgabe 3.45

- Es sei p eine Primzahl. Zeigen Sie, dass aus $x^2 = 1 \bmod p$ folgt, dass $x = \pm 1 \bmod p$.
- Angenommen $n = p_1 \cdot \dots \cdot p_s$ mit verschiedenen ungeraden Primzahlen p_i . Zeigen Sie, dass die Menge

$$\{x \in \mathbb{Z}/n\mathbb{Z} : x^2 = 1 \bmod n\}$$

genau 2^s Lösungen hat.

- Es sei $f \in \mathbb{F}_p[x]$ und $f = f_1 \cdot \dots \cdot f_s$ mit $f_i \in \mathbb{F}_p[x]$ verschiedene normierte Polynome. Zeigen Sie, dass die Menge

$$\{g \in \mathbb{F}_p[x]/\langle f \rangle : g^p = g\}$$

genau p^s Elemente hat.

3.9 *Mehrfache Nullstellen und sturmsche Ketten*

Satz 3.10 Es sei $f = f_1^{n_1} \cdot \dots \cdot f_s^{n_s} \in \mathbb{Q}[x], \mathbb{R}[x]$ oder $\mathbb{C}[x]$, sodass die Polynome f_i irreduzibel und paarweise verschieden sind. Dann gilt

$$\frac{f}{\text{ggT}(f, f')} = f_1 \cdot \dots \cdot f_s.$$

Aus der Produktformel folgt $f' = \sum_{i=1}^s n_i \frac{f}{f_i} f'_i$. Ist $n_i \geq 2$, so kommt der $f_i^{n_i-1}$ als echter Faktor in jedem Summand vor, aber $f_i^{n_i}$ nicht, denn sonst muss f_i das Polynom f'_i teilen, was aus Gradgründen nicht möglich ist. ■

1. Sei K ein Körper und $f \in K[x]$. Ist $f = cf_1 \cdot \dots \cdot f_s$ mit f_i verschiedenen irreduziblen Faktoren, so nennt man f quadratfrei.

2. Ist $f \in \mathbb{R}[x]$ quadratfrei, so ist die **sturmsche Kette** f_0, \dots, f_s definiert durch:

$$f_0 = f, f_1 = f', f_{i+1} = -f_{i-1} \bmod f_i, \quad i \geq 1, f_s = c \neq 0.$$

3. Ist $f \in \mathbb{R}[X]$ gegeben und $a \in \mathbb{R}$, so definieren wir $v(a) = v_f(a)$ als die Anzahl der Vorzeichenwechsel in der Folge $f_0(a), \dots, f_s(a)$. (Hierbei werden evtl. Nullen ignoriert.)

Satz 3.11 Sei $f \in \mathbb{R}[x]$ quadratfrei und für $a < b$ $f(a) \cdot f(b) \neq 0$, so ist die Anzahl der Nullstellen von f im Intervall (a, b) gleich $v(a) - v(b)$ ($a = -\infty$ und $b = \infty$ sind erlaubt).

Die Aussage ist wahr, wenn a sehr groß und $b = \infty$, denn die Anzahl von Vorzeichenwechsel für a und b sind gleich. Wir brauchen deshalb nur zu schauen, was passiert, wenn a eine Nullstelle einer f_i überquert. Es sei $f_i(a) = 0$ für ein $i > 0$. Aus $f_{i-1} = q_i f_i - f_{i+1}$ folgt durch Einsetzen von a , dass $f_{i-1}(a) = -f_{i+1}(a)$. Sie können nicht null sein, dann sonst wäre (mit dem gleichen Argument) $f_{i+2}(a) = f_{i+3}(a) = \dots = f_s(a) = 0$. Jedoch ist $f_s = \text{ggT}(f, f')$ eine Konstante ungleich 0, weil f und f' keine gemeinsamen Faktoren haben. Die Anzahl von Vorzeichenwechsel von $f_{i-1}(x), f_i(x), f_{i+1}(x)$ ist deshalb für x in der Nähe von a konstant, unabhängig vom Vorzeichen von $f_i(x)$. Es sei nun $f(a) = f_0(a) = 0$. Weil f nur einfache Nullstellen hat, ist $f'(a) \neq 0$. Es gilt: Ist $f'(a) < 0$, so ist $f(x) > 0$ für $x < a$ und nahe bei a und $f'(x) < 0$. Also gibt es einen Vorzeichenwechsel für $x < a$. Ist $x > a$, so ist $f(x) < 0$ und $f'(x) < 0$ ebenfalls. Wir haben beim Überqueren von a (von rechts nach links) genau einen Vorzeichenwechsel gewonnen. Der Fall $f'(a) > 0$ ist analog. ■

Beispiel Sei $f_0(x) = x^3 - 3x + 1$. Dann ist $f_1(x) = 3x^2 - 3$, $f_2(x) = 2x - 1$ und $f_3(x) = 9/4$. In ∞ gibt es keine Vorzeichenwechsel, in $-\infty$ drei. Deshalb gibt es drei reelle Nullstellen.

Aufgaben



Lösung

Aufgabe 3.46 Ist $f \in \mathbb{F}_p[x]$, $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, so haben wir die Ableitung von f definiert durch (siehe Aufgabe 3.26)

$$f' = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1 \in \mathbb{F}_p[x].$$

Zeigen Sie:

1. $f' = 0 \iff f = x^{kp} + b_{k-1}x^{(k-1)p} + \dots + b_1x^p + b_0$ für gewisse $b_i \in \mathbb{F}_p$.
2. $f' = 0 \iff f = g^p$ für ein $g \in \mathbb{F}_p[x]$.
3. f ist quadratfrei $\iff \text{ggT}(f, f') = 1$.

Aufgabe 3.47 Ist $f = f_1^{n_1} \cdot \dots \cdot f_s^{n_s}$ mit $n_i \geq 1$ und f_i irreduzibel und $\text{ggT}(f_i, f_j) = 1$, so nennt man $f_1 \cdot \dots \cdot f_s$ den quadratfreien Teil von f .

Berechnen Sie den quadratfreien Teil der nachfolgenden Polynome in $\mathbb{Q}[x]$.

1. $f = x^2 - 2x + 1$.
2. $f = x^3 - x^2 - 8x + 12$.
3. $f = x^3 - 4x^2 + 2x - 1$.
4. $f = x^6 - 3x^5 - 3x^4 + 11x^3 + 6x^2 - 12x - 8$.

Aufgabe 3.48 Wir haben den Satz über die Anzahl der reellen Nullstellen einer polynomialen Gleichung bewiesen unter der Annahme, dass f quadratfrei ist. Zeigen Sie, dass der Satz auch für nicht quadratfreie Polynome gilt.

Tipp: Teilen Sie durch $\text{ggT}(f, f')$.

Aufgabe 3.49 Bestimmen Sie mit den sturmschen Ketten die Anzahl der reellen Nullstellen der nachfolgenden Polynome.

1. $x^2 + px + q$. Unterscheiden Sie den Fall $p \neq 0$ und $p = 0$.
2. $x^3 + px + q$.
3. $x^4 - 1$.
4. $x^4 - 3x^2 + 2$.

Aufgabe 3.50 Bestimmen Sie die Anzahl der positiven Nullstellen von

1. $x^4 - 3x + 2$
2. $x^4 + x - 1$

Copyright

Daten, Texte, Design und Grafiken dieses eBooks, sowie die eventuell angebotenen eBook-Zusatzdaten sind urheberrechtlich geschützt. Dieses eBook stellen wir lediglich als **persönliche Einzelplatz-Lizenz** zur Verfügung!

Jede andere Verwendung dieses eBooks oder zugehöriger Materialien und Informationen, einschließlich

- der Reproduktion,
- der Weitergabe,
- des Weitervertriebs,
- der Platzierung im Internet, in Intranets, in Extranets,
- der Veränderung,
- des Weiterverkaufs und
- der Veröffentlichung

bedarf der **schriftlichen Genehmigung** des Verlags. Insbesondere ist die Entfernung oder Änderung des vom Verlag vergebenen Passwort- und DRM-Schutzes ausdrücklich untersagt!

Bei Fragen zu diesem Thema wenden Sie sich bitte an: **info@pearson.de**

Zusatzdaten

Möglicherweise liegt dem gedruckten Buch eine CD-ROM mit Zusatzdaten oder ein Zugangscode zu einer eLearning Plattform bei. Die Zurverfügungstellung dieser Daten auf unseren Websites ist eine freiwillige Leistung des Verlags. **Der Rechtsweg ist ausgeschlossen.** Zugangscodes können Sie darüberhinaus auf unserer Website käuflich erwerben.

Hinweis

Dieses und viele weitere eBooks können Sie rund um die Uhr und legal auf unserer Website herunterladen:

<https://www.pearson-studium.de>