8. Polynome

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
- Polynome der Form a_0X^0 heißen konstant.

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
- Polynome der Form a_0X^0 heißen konstant.
- Der Körper K läßt sich in $K[X]$ durch $a \mapsto aX^0$ mit den konstanten Polynomen identifizieren und als Teilmenge von $K[X]$ auffassen.

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
- Polynome der Form a_0X^0 heißen konstant.
- Der Körper K läßt sich in $K[X]$ durch $a \mapsto aX^0$ mit den konstanten Polynomen identifizieren und als Teilmenge von $K[X]$ auffassen.
- **Bem.:** Im Allgemeinen werden Polynome oft auch über kommutative Ringe mit 1 (z. B. über $\mathbb{Z}$) betrachtet.

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

mit $n \in \mathbb{N}_0$ und Koeffizienten $a_0, \ldots, a_n \in K$, heißt Polynom (über K).

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
- Polynome der Form a_0X^0 heißen konstant.
- Der Körper K läßt sich in $K[X]$ durch $a \mapsto aX^0$ mit den konstanten Polynomen identifizieren und als Teilmenge von $K[X]$ auffassen.
- **Bem.:** Im Allgemeinen werden Polynome oft auch über kommutative Ringe mit 1 (z. B. über $\mathbb{Z}$) betrachtet.

Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6 \in \mathbb{R}[X]$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht“ man das Minus in die Summe der Terme

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht" man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht" man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6 + X^4$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht“ man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6 + X^4 - 0.01X^2$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht“ man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6 + X^4 - 0.01X^2 + \tfrac{7}{3}X$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte 1 und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht" man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \tfrac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + 0X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6 + X^4 - 0.01X^2 + \tfrac{7}{3}X + 1\,.$$

Polynome über $\mathbb{Z}/p\mathbb{Z}$

- neben den bekannten Polynomen über $\mathbb{R}$ und $\mathbb{Q}$, können wir nun auch Polynome über $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p betrachten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

Polynome über $\mathbb{Z}/p\mathbb{Z}$

- neben den bekannten Polynomen über $\mathbb{R}$ und $\mathbb{Q}$, können wir nun auch Polynome über $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p betrachten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

- Zur Vereinfachung der Notation schreiben wir für die Koeffizienten anstelle der Restklassen einfach den Standardrepräsentanten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 + 3X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]\,,$$

Polynome über $\mathbb{Z}/p\mathbb{Z}$

- neben den bekannten Polynomen über $\mathbb{R}$ und $\mathbb{Q}$, können wir nun auch Polynome über $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p betrachten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

- Zur Vereinfachung der Notation schreiben wir für die Koeffizienten anstelle der Restklassen einfach den Standardrepräsentanten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 + 3X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]\,,$$

wobei

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 - 2X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

auch üblich ist.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$ und wird mit $\mathrm{grad}(p)$ bezeichnet.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$ und wird mit $\operatorname{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \ldots, n\}$, so nennt man p das Nullpolynom und setzt $\operatorname{grad}(p) = -\infty$.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \dots, n\}$ mit $a_i \neq 0$ und wird mit $\operatorname{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \dots, n\}$, so nennt man p das Nullpolynom und setzt $\operatorname{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \dots, n\}$ mit $a_i \neq 0$ und wird mit $\operatorname{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \dots, n\}$, so nennt man p das Nullpolynom und setzt $\operatorname{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\operatorname{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$ und wird mit $\mathrm{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \ldots, n\}$, so nennt man p das Nullpolynom und setzt $\mathrm{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\mathrm{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \dots, n\}$ mit $a_i \neq 0$ und wird mit $\mathrm{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \dots, n\}$, so nennt man p das Nullpolynom und setzt $\mathrm{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\mathrm{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
  - $\mathrm{grad}(p) = \mathrm{grad}(q)$

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$ und wird mit $\mathrm{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \ldots, n\}$, so nennt man p das Nullpolynom und setzt $\mathrm{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\mathrm{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
  - $\mathrm{grad}(p) = \mathrm{grad}(q)$
  - und $a_i = b_i$ für alle $i = 0, \ldots, \mathrm{grad}(p)$.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \dots, n\}$ mit $a_i \neq 0$ und wird mit $\operatorname{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \dots, n\}$, so nennt man p das Nullpolynom und setzt $\operatorname{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\operatorname{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
  - $\operatorname{grad}(p) = \operatorname{grad}(q)$
  - und $a_i = b_i$ für alle $i = 0, \dots, \operatorname{grad}(p)$.

$$0X^3 - X^2 + 0X + 3$$

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$ und wird mit $\mathrm{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \ldots, n\}$, so nennt man p das Nullpolynom und setzt $\mathrm{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\mathrm{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
  - $\mathrm{grad}(p) = \mathrm{grad}(q)$
  - und $a_i = b_i$ für alle $i = 0, \ldots, \mathrm{grad}(p)$.

$$0X^3 - X^2 + 0X + 3 = -X^2 + 0X + 3$$

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom über einem Körper K. Der Grad von p ist das größte $i \in \{0, \ldots, n\}$ mit $a_i \neq 0$ und wird mit $\mathrm{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \ldots, n\}$, so nennt man p das Nullpolynom und setzt $\mathrm{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\mathrm{grad}(p)}$ den Leitkoeffizienten und p heißt normiert, falls der Leitkoffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
  - $\mathrm{grad}(p) = \mathrm{grad}(q)$
  - und $a_i = b_i$ für alle $i = 0, \ldots, \mathrm{grad}(p)$.

$$0X^3 - X^2 + 0X + 3 = -X^2 + 0X + 3 = -X^2 + 3$$

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren die Summe $p + q$ koeffizientenweise

$$p + q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i \,,$$

wobei $b_{m+1} = \ldots = b_n = 0$ (falls $n > m$) b. z. w. $a_{n+1} = \ldots = a_m = 0$ (falls $m > n$).

Somit gilt $\mathrm{grad}(p + q) \leqslant \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$.

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren die Summe $p + q$ koeffizientenweise

$$p + q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i \,,$$

wobei $b_{m+1} = \ldots = b_n = 0$ (falls $n > m$) b. z. w. $a_{n+1} = \ldots = a_m = 0$ (falls $m > n$).
Somit gilt $\operatorname{grad}(p + q) \leqslant \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$.

Beispiel: Für $p = X^4 + 3X^2 + 2$ und $q = 4X^4 + X^3 + 2X^2 - 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p + q = 5X^4 + X^3 + 5X^2 + 1$$

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren die Summe $p + q$ koeffizientenweise

$$p + q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i \,,$$

wobei $b_{m+1} = \ldots = b_n = 0$ (falls $n > m$) b. z. w. $a_{n+1} = \ldots = a_m = 0$ (falls $m > n$).
Somit gilt $\operatorname{grad}(p + q) \leqslant \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$.

Beispiel: Für $p = X^4 + 3X^2 + 2$ und $q = 4X^4 + X^3 + 2X^2 - 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p + q = 5X^4 + X^3 + 5X^2 + 1 = X^3 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren die Summe $p + q$ koeffizientenweise

$$p + q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i \,,$$

wobei $b_{m+1} = \ldots = b_n = 0$ (falls $n > m$) b. z. w. $a_{n+1} = \ldots = a_m = 0$ (falls $m > n$).
Somit gilt $\operatorname{grad}(p + q) \leqslant \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$.

Beispiel: Für $p = X^4 + 3X^2 + 2$ und $q = 4X^4 + X^3 + 2X^2 - 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p + q = 5X^4 + X^3 + 5X^2 + 1 = X^3 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

$\Longrightarrow \operatorname{grad}(p + q) = 3 < 4 = \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$ hier

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren die Summe $p + q$ koeffizientenweise

$$p + q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i \,,$$

wobei $b_{m+1} = \ldots = b_n = 0$ (falls $n > m$) b. z. w. $a_{n+1} = \ldots = a_m = 0$ (falls $m > n$).

Somit gilt $\mathrm{grad}(p + q) \leqslant \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$.

Beispiel: Für $p = X^4 + 3X^2 + 2$ und $q = 4X^4 + X^3 + 2X^2 - 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p + q = 5X^4 + X^3 + 5X^2 + 1 = X^3 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

$\Longrightarrow \mathrm{grad}(p + q) = 3 < 4 = \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$ hier

Im Allgmeinen gilt: $\mathrm{grad}(p + q) < \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$

$\iff \mathrm{grad}(p) = \mathrm{grad}(q)$ und die Leitkoeffizienten sind additive Inverse in K.

Multiplikation von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren das Produkt $p \cdot q$ „durch ausmultiplizieren“

$$p \cdot q := \sum_{i=0}^{m+n} c_i X^i \quad \text{mit} \quad c_i := \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0$$

wobei (ähnlich wie bei der Addition) dafür $b_{m+1} = \ldots = b_{m+n} = 0$ und $a_{n+1} = \ldots = a_{m+n} = 0$ gesetzt wird.

Multiplikation von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren das Produkt $p \cdot q$ „durch ausmultiplizieren“

$$p \cdot q := \sum_{i=0}^{m+n} c_i X^i \quad \text{mit} \quad c_i := \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0$$

wobei (ähnlich wie bei der Addition) dafür $b_{m+1} = \ldots = b_{m+n} = 0$ und $a_{n+1} = \ldots = a_{m+n} = 0$ gesetzt wird.

Aus der Definition folgt direkt:

$$\operatorname{grad}(p \cdot q) \leqslant \operatorname{grad}(p) + \operatorname{grad}(q) \quad \text{mit} \quad c_{\operatorname{grad}(p)+\operatorname{grad}(q)} = a_{\operatorname{grad}(p)} \cdot b_{\operatorname{grad}(q)}$$

Multiplikation von Polynomen

Definition

Seien $p = \sum_{i=0}^{n} a_i X^i$ und $q = \sum_{i=0}^{m} b_i X^i$ Polynome über dem gleichen Körper K. Wir definieren das Produkt $p \cdot q$ „durch ausmultiplizieren“

$$p \cdot q := \sum_{i=0}^{m+n} c_i X^i \quad \text{mit} \quad c_i := \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$$

wobei (ähnlich wie bei der Addition) dafür $b_{m+1} = \ldots = b_{m+n} = 0$ und $a_{n+1} = \ldots = a_{m+n} = 0$ gesetzt wird.

Aus der Definition folgt direkt:

$$\operatorname{grad}(p \cdot q) \leqslant \operatorname{grad}(p) + \operatorname{grad}(q) \quad \text{mit} \quad c_{\operatorname{grad}(p)+\operatorname{grad}(q)} = a_{\operatorname{grad}(p)} \cdot b_{\operatorname{grad}(q)}$$

Da in Körpern das Produkt $a_{\operatorname{grad}(p)} \cdot b_{\operatorname{grad}(q)}$ zweier von Null verschiedener Elemente niemals Null ist, folgt somit auch

$$\operatorname{grad}(p \cdot q) = \operatorname{grad}(p) + \operatorname{grad}(q)$$

für Polynome über einem Körper K.

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 8$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 8$$

und zusammenfassen und umrechnen in Standardrepräsentanten führt zu

$$= 2X^5 + 5X^4 + X^3 + 16X^2 - 2X + 8$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 8$$

und zusammenfassen und umrechnen in Standardrepräsentanten führt zu

$$= 2X^5 + 5X^4 + X^3 + 16X^2 - 2X + 8 = 2X^5 + X^3 + X^2 + 3X + 3\,.$$

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 8$$

und zusammenfassen und umrechnen in Standardrepräsentanten führt zu

$$= 2X^5 + 5X^4 + X^3 + 16X^2 - 2X + 8 = 2X^5 + X^3 + X^2 + 3X + 3\,.$$

Es gilt in $(\mathbb{Z}/5\mathbb{Z})[X]$ also

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3.$$

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

$$p \cdot q$$

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

$$p \cdot q = 6X^5 + 2X^3$$

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

$$p \cdot q = 6X^5 + 2X^3 = 2X^3 \in (\mathbb{Z}/6\mathbb{Z})[X]$$

Verwirrender Abstecher

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

$$p \cdot q = 6X^5 + 2X^3 = 2X^3 \in (\mathbb{Z}/6\mathbb{Z})[X]$$

$\Longrightarrow \mathrm{grad}(p \cdot q) = 3 < 5 = \mathrm{grad}(p) + \mathrm{grad}(q)$

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n} (-a_i) X^i \in K[X]$

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n} (-a_i) X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n}(-a_i)X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K
- konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n}(-a_i)X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K
- konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation

$\Rightarrow$ $(K[X], \cdot)$ ist ein kommutatives Monoid

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n}(-a_i)X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K
- konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation

$\Rightarrow$ $(K[X], \cdot)$ ist ein kommutatives Monoid

- Distributivgesetzte kann man nachrechnen

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n} (-a_i) X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K
- konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation

$\Rightarrow$ $(K[X], \cdot)$ ist ein kommutatives Monoid

- Distributivgesetzte kann man nachrechnen $\square$

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein kommutativer Ring mit 1, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen Polynomring (über K).

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
- Nullpolynom ist offensichtlich neutral bezüglich der Addition
- $p = \sum_{i=0}^{n} a_i X^i \in K[X] \Longrightarrow -p := \sum_{i=0}^{n} (-a_i) X^i \in K[X]$

$\Rightarrow$ $(K[X], +)$ ist eine abelsche Gruppe

- Assoziativität und Kommutativität von $\cdot$ vererbt sich von K
- konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation

$\Rightarrow$ $(K[X], \cdot)$ ist ein kommutatives Monoid

- Distributivgesetzte kann man nachrechnen $\square$

Auch Polynome $R[X]$ über kommutative Ringe R mit 1 bilden einen solchen.

Teilbarkeit für Polynome

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m \,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) =$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3\,.$$

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein Vielfaches von q, falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m\,.$$

Wir schreiben dafür $q \mid p$ und sagen q teilt p, oder q ist ein Teiler von p.

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q, dann ist r ein gemeinsamer Teiler von p und q.

Das Polynom r ist ein größter gemeinsamer Teiler von p und q ($\neq$ Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p, insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3\,.$$

$\Rightarrow X^3 + 3X^2 + 2$ und $2X^2 - X + 4$ sind Teiler von $2X^5 + X^3 + X^2 + 3X + 3$.

Einheiten in $K[X]$

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt
- $\operatorname{grad}(1) = 0$ und da K ein Körper ist, gilt

$$\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q$$

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt
- $\operatorname{grad}(1) = 0$ und da K ein Körper ist, gilt

$$\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q$$

$\Rightarrow$ nur die konstanten Polynome mit Grad 0 können Einheiten sein

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt
- $\operatorname{grad}(1) = 0$ und da K ein Körper ist, gilt

$$\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q$$

$\Rightarrow$ nur die konstanten Polynome mit Grad 0 können Einheiten sein

- tatsächlich gibt es für jedes $a \in K \setminus \{0\}$ ein multiplikativ Inverses $a^{-1} \in K \setminus \{0\}$ und für die konstanten Polynome $p = aX^0$ und $q = a^{-1}X^0$ gilt
$$p \cdot q = (a \cdot a^{-1})X^0 = 1X^0$$

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt
- $\mathrm{grad}(1) = 0$ und da K ein Körper ist, gilt

$$\mathrm{grad}(p \cdot q) = \mathrm{grad}\, p + \mathrm{grad}\, q$$

$\Rightarrow$ nur die konstanten Polynome mit Grad 0 können Einheiten sein

- tatsächlich gibt es für jedes $a \in K \setminus \{0\}$ ein multiplikativ Inverses $a^{-1} \in K \setminus \{0\}$ und für die konstanten Polynome $p = aX^0$ und $q = a^{-1}X^0$ gilt

$$p \cdot q = (a \cdot a^{-1})X^0 = 1X^0$$

Satz

Für jeden Körper K sind die Einheiten des Polynomrings $K[X]$ genau die konstanten Polynome vom Grad 0, d. h.

$$(K[X])^\times = \left\{aX^0 \colon a \in K \setminus \{0\}\right\}.$$

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit a, $b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit a, $b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler
- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

$$m \mid p_1 \quad \text{und} \quad m \mid p_2 \qquad \Longrightarrow \qquad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

für alle m, p_1, $p_2 \in K[X]$ und $a \in K \setminus \{0\}$

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit $a, b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler
- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

$$m \mid p_1 \quad \text{und} \quad m \mid p_2 \qquad \Longrightarrow \qquad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

  für alle $m, p_1, p_2 \in K[X]$ und $a \in K \setminus \{0\}$
- ein größter gemeinsamer Teiler zweier Polynome läßt sich wie der ggT zweier ganzer Zahlen mit dem EUKLIDischen Algorithmus bestimmen

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit $a, b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler
- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

  $$m \mid p_1 \quad \text{und} \quad m \mid p_2 \qquad \Longrightarrow \qquad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

  für alle $m, p_1, p_2 \in K[X]$ und $a \in K \setminus \{0\}$
- ein größter gemeinsamer Teiler zweier Polynome läßt sich wie der ggT zweier ganzer Zahlen mit dem EUKLIDischen Algorithmus bestimmen
- EUKLIDischer Algorithmus in $\mathbb{Z}$ beruht auf der Division mit Rest

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit a, $b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler
- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

$$m \mid p_1 \quad \text{und} \quad m \mid p_2 \qquad \Longrightarrow \qquad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

  für alle $m, p_1, p_2 \in K[X]$ und $a \in K \setminus \{0\}$
- ein größter gemeinsamer Teiler zweier Polynome läßt sich wie der ggT zweier ganzer Zahlen mit dem EUKLIDischen Algorithmus bestimmen
- EUKLIDischer Algorithmus in $\mathbb{Z}$ beruht auf der Division mit Rest
- analog führen wir die Division mit Rest in $K[X]$ ein

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit a, $b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler
- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

$$m \mid p_1 \quad \text{und} \quad m \mid p_2 \qquad \Longrightarrow \qquad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

  für alle m, p_1, $p_2 \in K[X]$ und $a \in K \setminus \{0\}$
- ein größter gemeinsamer Teiler zweier Polynome läßt sich wie der ggT zweier ganzer Zahlen mit dem EUKLIDischen Algorithmus bestimmen
- EUKLIDischer Algorithmus in $\mathbb{Z}$ beruht auf der Division mit Rest
- analog führen wir die Division mit Rest in $K[X]$ ein

$\longrightarrow$ Polynomdivision

Polynomdivision

Satz

Sei K ein Körper und seien $p,\ m \in K[X]$ Polynome mit $m \neq 0$,

Polynomdivision

Satz

Sei K ein Körper und seien p, $m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome q, $r \in K[X]$ mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m)$.

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m)$.

Beweis:

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\mathrm{grad}(p) = n$ und $\mathrm{grad}(m) = k$.

Polynomdivision

Satz

Sei K ein Körper und seien p, $m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome q, $r \in K[X]$ mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\text{grad}(p) = n$ und $\text{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\operatorname{grad}(p) = n$ und $\operatorname{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\mathrm{grad}(p) = n$ und $\mathrm{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\operatorname{grad}(p) = n$ und $\operatorname{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \operatorname{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:

Polynomdivision

Satz

Sei K ein Körper und seien p, $m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome q, $r \in K[X]$ mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\text{grad}(p) = n$ und $\text{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \text{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
   - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\text{grad}(p) = n$ und $\text{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \text{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
   - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.
   - Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.

Polynomdivision

Satz

Sei K ein Körper und seien p, $m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome q, $r \in K[X]$ mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\mathrm{grad}(p) = n$ und $\mathrm{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \mathrm{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
   - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.
   - Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.
4. Gib $r = s$ und $q = \sum_{i=0}^{n-k} c_i X^i$ aus.

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\text{grad}(p) = n$ und $\text{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \text{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
   - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.
   - Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.
4. Gib $r = s$ und $q = \sum_{i=0}^{n-k} c_i X^i$ aus.

Algorithmus terminiert, da sich in jedem Durchlauf von 3 der Grad von s um mindestens 1 verringert und $k \geqslant 0$ gilt.

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\operatorname{grad}(p) = n$ und $\operatorname{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \operatorname{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
    - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.
    - Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.
4. Gib $r = s$ und $q = \sum_{i=0}^{n-k} c_i X^i$ aus.

Algorithmus terminiert, da sich in jedem Durchlauf von 3 der Grad von s um mindestens 1 verringert und $k \geqslant 0$ gilt. Tatsächlich hat $c_{\ell-k} X^{\ell-k} \cdot m$ Leitkoeffizienten $c_{\ell-k} \cdot b_k = d_\ell$ und Grad ℓ genau wie s.

Polynomdivision

Satz

Sei K ein Körper und seien p, $m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome q, $r \in K[X]$ mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^{n} a_i X^i$ und $m = \sum_{i=0}^{k} b_i X^i$ mit $\operatorname{grad}(p) = n$ und $\operatorname{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1. Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.
2. Initialisiere $s = p$
3. Solange $\ell := \operatorname{grad}(s) \geqslant k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:
   - Setze $c_{\ell-k} = \frac{d_\ell}{b_k}$.
   - Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.
4. Gib $r = s$ und $q = \sum_{i=0}^{n-k} c_i X^i$ aus.

Algorithmus terminiert, da sich in jedem Durchlauf von 3 der Grad von s um mindestens 1 verringert und $k \geqslant 0$ gilt. Tatsächlich hat $c_{\ell-k} X^{\ell-k} \cdot m$ Leitkoeffizienten $c_{\ell-k} \cdot b_k = d_\ell$ und Grad ℓ genau wie s. Somit hat das Polynom $s - c_{\ell-k} X^{\ell-k} \cdot m$ einen geringeren Grad.

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \qquad (*)$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n:

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen.

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert **1** eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt **2** q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$p =$

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m$$

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m \overset{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m =$$

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m \overset{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m = \left(q - \frac{a_n}{b_k} X^{n-k}\right) \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m\,.$$

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m \overset{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m = \left(q - \frac{a_n}{b_k} X^{n-k}\right) \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m\,.$$

$$\Longrightarrow p = q \cdot m - \frac{a_n}{b_k} X^{n-k} \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m$$

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m \overset{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m = \left(q - \frac{a_n}{b_k} X^{n-k}\right) \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m\,.$$

$$\Longrightarrow p = q \cdot m - \frac{a_n}{b_k} X^{n-k} \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m = q \cdot m + r$$

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

1. Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
2. Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m, sodass
$$p' = q' \cdot m + r \qquad \text{und} \qquad \operatorname{grad}(r) < k = \operatorname{grad}(m)\,. \tag{$*$}$$
3. Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert 1 eine Lösung, da dann $\operatorname{grad}(p) = n < k = \operatorname{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n: Da $\operatorname{grad}(p') < \operatorname{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt 2 q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m \overset{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m = \left(q - \frac{a_n}{b_k} X^{n-k}\right) \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m\,.$$

$$\Longrightarrow p = q \cdot m - \tfrac{a_n}{b_k} X^{n-k} \cdot m + r + \tfrac{a_n}{b_k} X^{n-k} \cdot m = q \cdot m + r \qquad \square$$

Bemerkungen zur Polynomdivision

- die im Beweis angegebenen Algorithmen der Polynomdivison lassen sich effizient implementieren, wenn die Division im entsprechenden Körper K effizient realisierbar ist

Bemerkungen zur Polynomdivision

- die im Beweis angegebenen Algorithmen der Polynomdivison lassen sich effizient implementieren, wenn die Division im entsprechenden Körper K effizient realisierbar ist
- bei der Berechnung der Koeffizienten von q wird durch den Leitkoeffizienten von m geteilt, was in Polynomringen über Körpern immer möglich ist

Bemerkungen zur Polynomdivision

- die im Beweis angegebenen Algorithmen der Polynomdivison lassen sich effizient implementieren, wenn die Division im entsprechenden Körper K effizient realisierbar ist
- bei der Berechnung der Koeffizienten von q wird durch den Leitkoeffizienten von m geteilt, was in Polynomringen über Körpern immer möglich ist
- in Polynomringen $R[X]$ über kommutativen Ringen R mit 1 müßte man zusätzlich fordern, dass der Leitkoeffizient b_k von m eine Einheit ist, d. h. $b_k \in R^\times$

Bemerkungen zur Polynomdivision

- die im Beweis angegebenen Algorithmen der Polynomdivison lassen sich effizient implementieren, wenn die Division im entsprechenden Körper K effizient realisierbar ist
- bei der Berechnung der Koeffizienten von q wird durch den Leitkoeffizienten von m geteilt, was in Polynomringen über Körpern immer möglich ist
- in Polynomringen $R[X]$ über kommutativen Ringen R mit 1 müßte man zusätzlich fordern, dass der Leitkoeffizient b_k von m eine Einheit ist, d. h. $b_k \in R^\times$
- mithilfe der Polynomdivision lässt sich der EUKLIDische Algorithmus von $\mathbb{Z}$ direkt auf Polynomringe $K[X]$ übertragen, um einen größten gemeinsamen Teiler von zwei gegebenen Polynomen $p_1, p_2 \in K[X]$ zu berechnen

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m)$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m) = 1$.

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$X^4 \qquad - 3X^2 + 5X - 3 = \big(X - 1\big)\big(\qquad\qquad\qquad \big)$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$X^4 \qquad - 3X^2 + 5X - 3 = \big(X - 1\big)\big(X^3 \qquad\qquad\qquad \big)$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$\begin{array}{rl} X^4 \qquad - 3X^2 + 5X - 3 &= \big(X-1\big)\big(X^3 \qquad\qquad\qquad\big) \\ \underline{-X^4 + X^3} & \end{array}$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rl}
X^4 \qquad\quad & - 3X^2 + 5X - 3 = \big(X-1\big)\big(X^3 \qquad\qquad\qquad\quad \big) \\
\underline{- X^4 + X^3} & \\
X^3 & - 3X^2
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$\begin{array}{rrrrl} X^4 & & -3X^2 & +5X-3 & = (X-1)\big(X^3 + X^2 \qquad\qquad\big) \\ \underline{-X^4} & \underline{+X^3} & & & \\ & X^3 & -3X^2 & & \end{array}$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -\,3X^2 & +\,5X - 3 & = \big(X-1\big)\big(X^3 + X^2 \qquad\qquad\big) \\
\underline{-\,X^4} & \underline{+\,X^3} & & & \\
 & X^3 & -\,3X^2 & & \\
 & \underline{-\,X^3} & \underline{+\,X^2} & & \\
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -\,3X^2 & +\,5X - 3 & = \big(X-1\big)\big(X^3 + X^2 \qquad\qquad \big) \\
-\,X^4 & +\,X^3 & & & \\
\hline
 & X^3 & -\,3X^2 & & \\
 & -\,X^3 & +\,X^2 & & \\
\hline
 & & -\,2X^2 & +\,5X &
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -\,3X^2 & +\,5X - 3 & = \big(X-1\big)\big(X^3 + X^2 - 2X \qquad\big) \\
-\,X^4 & +\,X^3 & & & \\
\hline
& X^3 & -\,3X^2 & & \\
& -\,X^3 & +\,X^2 & & \\
\hline
& & -\,2X^2 & +\,5X & \\
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -\,3X^2 & +\,5X & -\,3 = \big(X-1\big)\big(X^3 + X^2 - 2X \qquad\big) \\
-\,X^4 & +\,X^3 & & & \\
\hline
& X^3 & -\,3X^2 & & \\
& -\,X^3 & +\,X^2 & & \\
\hline
& & -\,2X^2 & +\,5X & \\
& & 2X^2 & -\,2X & \\
\cline{3-4}
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -\,3X^2 & +\,5X & -\,3 = \big(X-1\big)\big(X^3 + X^2 - 2X \qquad\big) \\
-\,X^4 & +\,X^3 & & & \\
\hline
& X^3 & -\,3X^2 & & \\
& -\,X^3 & +\,X^2 & & \\
\hline
& & -\,2X^2 & +\,5X & \\
& & 2X^2 & -\,2X & \\
\hline
& & & 3X & -\,3
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -3X^2 & +5X-3 & = (X-1)\big(X^3+X^2-2X+3\big) \\
\underline{-X^4} & \underline{+X^3} & & & \\
 & X^3 & -3X^2 & & \\
 & \underline{-X^3} & \underline{+X^2} & & \\
 & & -2X^2 & +5X & \\
 & & \underline{2X^2} & \underline{-2X} & \\
 & & & 3X-3 &
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrr}
X^4 & & -\,3X^2 & +\,5X & -\,3 = (X-1)(X^3 + X^2 - 2X + 3) \\
-\,X^4 & +\,X^3 & & & \\
\hline
 & X^3 & -\,3X^2 & & \\
 & -\,X^3 & +\,X^2 & & \\
\hline
 & & -\,2X^2 & +\,5X & \\
 & & 2X^2 & -\,2X & \\
\hline
 & & & 3X & -\,3 \\
 & & & -\,3X & +\,3 \\
\hline
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3 + X^2 - 2X + 3\big) \\
-X^4 & +X^3 & & & & \\
\hline
 & X^3 & -3X^2 & & & \\
 & -X^3 & +X^2 & & & \\
\hline
 & & -2X^2 & +5X & & \\
 & & 2X^2 & -2X & & \\
\hline
 & & & 3X & -3 & \\
 & & & -3X & +3 & \\
\hline
 & & & & 0 &
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
-X^4 & +X^3 & & & & \\
\hline
 & X^3 & -3X^2 & & & \\
 & -X^3 & +X^2 & & & \\
\hline
 & & -2X^2 & +5X & & \\
 & & 2X^2 & -2X & & \\
\hline
 & & & 3X & -3 & \\
 & & & -3X & +3 & \\
\hline
 & & & & 0 &
\end{array}
$$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -\,3X^2 & +\,5X & -\,3 & = \big(X-1\big)\big(X^3 + X^2 - 2X + 3\big) \\
-\,X^4 & +\,X^3 & & & & \\
\hline
& X^3 & -\,3X^2 & & & \\
& -\,X^3 & +\,X^2 & & & \\
\hline
& & -\,2X^2 & +\,5X & & \\
& & 2X^2 & -\,2X & & \\
\hline
& & & 3X & -\,3 & \\
& & & -\,3X & +\,3 & \\
\hline
& & & & 0 &
\end{array}
$$

$\Longrightarrow q =$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = (X-1)(X^3+X^2-2X+3) \\
-X^4 & +X^3 & & & & \\
\hline
& X^3 & -3X^2 & & & \\
& -X^3 & +X^2 & & & \\
\hline
& & -2X^2 & +5X & & \\
& & 2X^2 & -2X & & \\
\hline
& & & 3X & -3 & \\
& & & -3X & +3 & \\
\hline
& & & & 0 &
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrl}
X^4 & & -3X^2 & +5X & -3 = (X-1)(X^3+X^2-2X+3) \\
\underline{-X^4} & \underline{+X^3} & & & \\
& X^3 & -3X^2 & & \\
& \underline{-X^3} & \underline{+X^2} & & \\
& & -2X^2 & +5X & \\
& & \underline{2X^2} & \underline{-2X} & \\
& & & 3X & -3 \\
& & & \underline{-3X} & \underline{+3} \\
& & & & 0
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r =$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
\underline{-X^4} & \underline{+X^3} & & & & \\
 & X^3 & -3X^2 & & & \\
 & \underline{-X^3} & \underline{+X^2} & & & \\
 & & -2X^2 & +5X & & \\
 & & \underline{2X^2} & \underline{-2X} & & \\
 & & & 3X & -3 & \\
 & & & \underline{-3X} & \underline{+3} & \\
 & & & & 0 &
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\operatorname{grad}(r) < \operatorname{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
-X^4 & +X^3 & & & & \\
\hline
 & X^3 & -3X^2 & & & \\
 & -X^3 & +X^2 & & & \\
\hline
 & & -2X^2 & +5X & & \\
 & & 2X^2 & -2X & & \\
\hline
 & & & 3X & -3 & \\
 & & & -3X & +3 & \\
\hline
 & & & & 0 &
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
-X^4 & +X^3 & & & & \\
\hline
& X^3 & -3X^2 & & & \\
& -X^3 & +X^2 & & & \\
\hline
& & -2X^2 & +5X & & \\
& & 2X^2 & -2X & & \\
\hline
& & & 3X & -3 & \\
& & & -3X & +3 & \\
\hline
& & & & 0 &
\end{array}$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$
- unter den Strichen steht der aktuell relevante Teil von s

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrr}
X^4 & & -\,3X^2 & +\,5X & -\,3 = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
\underline{-\,X^4} & \underline{+\,X^3} & & & \\
 & X^3 & -\,3X^2 & & \\
 & \underline{-\,X^3} & \underline{+\,X^2} & & \\
 & & -\,2X^2 & +\,5X & \\
 & & \underline{2X^2} & \underline{-\,2X} & \\
 & & & 3X & -\,3 \\
 & & & \underline{-\,3X} & \underline{+\,3} \\
 & & & & 0
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$
- unter den Strichen steht der aktuell relevante Teil von s
- unter dem letzten Strich (wenn $\mathrm{grad}(s) < \mathrm{grad}(m)$) steht das Restpolynom r

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
\underline{-X^4} & \underline{+X^3} & & & & \\
 & X^3 & -3X^2 & & & \\
 & \underline{-X^3} & \underline{+X^2} & & & \\
 & & -2X^2 & +5X & & \\
 & & \underline{2X^2} & \underline{-2X} & & \\
 & & & 3X & -3 & \\
 & & & \underline{-3X} & \underline{+3} & \\
 & & & & 0 &
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$
- unter den Strichen steht der aktuell relevante Teil von s
- unter dem letzten Strich (wenn $\mathrm{grad}(s) < \mathrm{grad}(m)$) steht das Restpolynom r
- auf der rechten Seite steht $m \cdot (c_{n-k}X^{n-k} + \dots + c_{\ell-k}X^{\ell-k} \dots)$ und am Ende der Rechnung $m \cdot q$

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\mathrm{grad}(r) < \mathrm{grad}(m) = 1$.

$$
\begin{array}{rrrrrl}
X^4 & & -3X^2 & +5X & -3 & = \big(X-1\big)\big(X^3+X^2-2X+3\big) \\
\underline{-X^4} & \underline{+X^3} & & & & \\
 & X^3 & -3X^2 & & & \\
 & \underline{-X^3} & \underline{+X^2} & & & \\
 & & -2X^2 & +5X & & \\
 & & \underline{2X^2} & \underline{-2X} & & \\
 & & & 3X & -3 & \\
 & & & \underline{-3X} & \underline{+3} & \\
 & & & & 0 &
\end{array}
$$

$\Longrightarrow q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$
- unter den Strichen steht der aktuell relevante Teil von s
- unter dem letzten Strich (wenn $\mathrm{grad}(s) < \mathrm{grad}(m)$) steht das Restpolynom r
- auf der rechten Seite steht $m \cdot (c_{n-k}X^{n-k} + \cdots + c_{\ell-k}X^{\ell-k} \dots)$ und am Ende der Rechnung $m \cdot q$
- wegen dem „=“ muß am Ende der Rechnung auf der rechten Seite noch $+r$ ergänzt werden (entfällt oben, da hier $r = 0$)

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$X^4 \qquad - X^2 + 3X + 2 = \big(X^2 - 2X + 1\big)\big(\qquad \big)$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$X^4 \qquad\qquad - X^2 + 3X + 2 = \left(X^2 - 2X + 1\right)\left(X^2 \qquad\qquad\right)$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$\begin{array}{rrrl} X^4 & & -X^2 + 3X + 2 = & \big(X^2 - 2X + 1\big)\big(X^2 \qquad\qquad\qquad \big) \\ -X^4 & +2X^3 & -X^2 & \\ \hline \end{array}$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rl}
X^4 \qquad\qquad - X^2 + 3X + 2 & = \big(X^2 - 2X + 1\big)\big(X^2 \qquad\qquad\quad \big) \\
\underline{-X^4 + 2X^3 \;\; - X^2} & \\
2X^3 - 2X^2 + 3X &
\end{array}
$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrl}
X^4 & & - X^2 & + 3X + 2 & = \big(X^2 - 2X + 1\big)\big(X^2 + 2X \qquad\big) \\
- X^4 & + 2X^3 & - X^2 & & \\
\hline
 & 2X^3 & - 2X^2 & + 3X &
\end{array}
$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrrl}
X^4 & & -X^2 & +3X & +2 & = \big(X^2 - 2X + 1\big)\big(X^2 + 2X \qquad\big) \\
-X^4 & +2X^3 & -X^2 & & & \\
\hline
 & 2X^3 & -2X^2 & +3X & & \\
 & -2X^3 & +4X^2 & -2X & & \\
\hline
\end{array}
$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$\begin{array}{rrrrrl}
X^4 & & -X^2 & +3X & +2 & = \big(X^2 - 2X + 1\big)\big(X^2 + 2X \qquad\big) \\
-X^4 & +2X^3 & -X^2 & & & \\
\hline
 & 2X^3 & -2X^2 & +3X & & \\
 & -2X^3 & +4X^2 & -2X & & \\
\hline
 & & 2X^2 & +X & +2 &
\end{array}$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

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

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

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

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrrl}
X^4 & & -X^2 & +3X & +2 & = \big(X^2 - 2X + 1\big)\big(X^2 + 2X + 2\big) \\
-X^4 & +2X^3 & -X^2 & & & \\
\hline
& 2X^3 & -2X^2 & +3X & & \\
& -2X^3 & +4X^2 & -2X & & \\
\hline
& & 2X^2 & +X & +2 & \\
& & -2X^2 & +4X & -2 & \\
\hline
& & & 5X & &
\end{array}
$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrrl}
X^4 & & -X^2 & +3X & +2 & = \left(X^2 - 2X + 1\right)\left(X^2 + 2X + 2\right) + 5X \\
-X^4 & +2X^3 & -X^2 & & & \\
\hline
 & 2X^3 & -2X^2 & +3X & & \\
 & -2X^3 & +4X^2 & -2X & & \\
\hline
 & & 2X^2 & +X & +2 & \\
 & & -2X^2 & +4X & -2 & \\
\hline
 & & & 5X & & \\
\end{array}
$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrr}
X^4 & & -X^2 & +3X & +2 = \left(X^2 - 2X + 1\right)\left(X^2 + 2X + 2\right) + 5X \\
-X^4 & +2X^3 & -X^2 & & \\
\hline
& 2X^3 & -2X^2 & +3X & \\
& -2X^3 & +4X^2 & -2X & \\
\hline
& & 2X^2 & +X & +2 \\
& & -2X^2 & +4X & -2 \\
\hline
& & & 5X &
\end{array}
$$

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$
\begin{array}{rrrrrl}
 X^4 & & -X^2 & +3X & +2 & = \big(X^2 - 2X + 1\big)\big(X^2 + 2X + 2\big) + 5X \\
 -X^4 & +2X^3 & -X^2 & & & \\
\hline
 & 2X^3 & -2X^2 & +3X & & \\
 & -2X^3 & +4X^2 & -2X & & \\
\hline
 & & 2X^2 & +X & +2 & \\
 & & -2X^2 & +4X & -2 & \\
\hline
 & & & 5X & &
\end{array}
$$

Hier ist der Quotient $q = X^2 + 2X + 2$ und der Rest $r = 5X$.

EUKLIDischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDischen Algorithmus berechnen

Euklidischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des Euklidischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$

EUKLIDischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$
- dabei teilt man ausgehend von p_1 und p_2, also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r

Euklidischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des Euklidischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$
- dabei teilt man ausgehend von p_1 und p_2, also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r
- sobald p_2 das Nullpolynom ist, ist p_1 ein größter gemeinsamer Teiler gefunden

EUKLIDischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$
- dabei teilt man ausgehend von p_1 und p_2, also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r
- sobald p_2 das Nullpolynom ist, ist p_1 ein größter gemeinsamer Teiler gefunden
- im Unterschied zur Situation bei ganzen Zahlen, kann es bei Polynomen passieren, dass die beiden gegebenen Polynome p_1 und p_2 denselben Grad haben, ohne dass die beiden Polynome einander teilen

EUKLIDischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$
- dabei teilt man ausgehend von p_1 und p_2, also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r
- sobald p_2 das Nullpolynom ist, ist p_1 ein größter gemeinsamer Teiler gefunden
- im Unterschied zur Situation bei ganzen Zahlen, kann es bei Polynomen passieren, dass die beiden gegebenen Polynome p_1 und p_2 denselben Grad haben, ohne dass die beiden Polynome einander teilen
- in diesem Falle ist es egal, ob man zunächst das eine Polynom durch das andere teilt oder umgekehrt

EUKLIDischer Algorithmus in Polynomringen

- wie in $\mathbb{Z}$ kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDischen Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in $\mathbb{Z}$
- dabei teilt man ausgehend von p_1 und p_2, also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r
- sobald p_2 das Nullpolynom ist, ist p_1 ein größter gemeinsamer Teiler gefunden
- im Unterschied zur Situation bei ganzen Zahlen, kann es bei Polynomen passieren, dass die beiden gegebenen Polynome p_1 und p_2 denselben Grad haben, ohne dass die beiden Polynome einander teilen
- in diesem Falle ist es egal, ob man zunächst das eine Polynom durch das andere teilt oder umgekehrt
- die Korrektheit diese Verfahrens beweist man ebenso wie die Korrektheit des EUKLIDischen Algorithmus in $\mathbb{Z}$, mit Induktion nach $\operatorname{grad}(p_1) + \operatorname{grad}(p_2)$, kombiniert mit der Proposition, dass für $p_1 = q \cdot p_2 + r$ mit $\operatorname{grad}(r) < \operatorname{grad}(p_2)$ jeder größte gemeinsame Teiler von p_2 und r auch ein größter gemeinsamer Teiler von p_1 und p_2 ist

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen.

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$X^3 - 3X^2 + 5X - 3 = \left(X^3 - 1\right)$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$X^3 - 3X^2 + 5X - 3 = \big(X^3 - 1\big)1$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$
\begin{array}{rl}
X^3 - 3X^2 + 5X - 3 & = \big(X^3 - 1\big)1 \\
\underline{- X^3 \qquad\qquad\qquad + 1} &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$
\begin{array}{r}
X^3 - 3X^2 + 5X - 3 = \big(X^3 - 1\big)1 \\
\underline{-\,X^3 \qquad\qquad\qquad + 1} \\
-\,3X^2 + 5X - 2
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.

Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$\begin{array}{rl} X^3 - 3X^2 + 5X - 3 & = \big(X^3 - 1\big)1 - 3X^2 + 5X - 2 \\ -\,X^3 \qquad\qquad\qquad + 1 & \\ \hline -\,3X^2 + 5X - 2 & \end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.

Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$\begin{array}{rl} X^3 - 3X^2 + 5X - 3 & = \big(X^3 - 1\big)1 - 3X^2 + 5X - 2 \\ -\,X^3 \qquad\qquad\qquad + 1 & \\ \hline -\,3X^2 + 5X - 2 & \end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$\begin{array}{r}
X^3 - 3X^2 + 5X - 3 = \big(X^3 - 1\big)1 - 3X^2 + 5X - 2 \\
\underline{- X^3 \qquad\qquad\qquad + 1} \qquad\qquad\qquad\qquad\qquad\qquad\quad \\
- 3X^2 + 5X - 2 \qquad\qquad\qquad\qquad\qquad\qquad\quad
\end{array}$$

Der Rest ist

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$\begin{array}{rl} X^3 - 3X^2 + 5X - 3 & = \big(X^3 - 1\big)1 - 3X^2 + 5X - 2 \\ - X^3 \qquad\qquad\qquad + 1 & \\ \hline - 3X^2 + 5X - 2 & \end{array}$$

Der Rest ist $r_1 = -3X^2 + 5X - 2$

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.
Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2:

$$\begin{array}{rl} X^3 - 3X^2 + 5X - 3 & = \big(X^3 - 1\big)1 - 3X^2 + 5X - 2 \\ -\,X^3 + 1 & \\ \hline -\,3X^2 + 5X - 2 & \end{array}$$

Der Rest ist $r_1 = -3X^2 + 5X - 2$ und im nächsten Schritt teilen wir p_2 durch r_1.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$X^3 \qquad\qquad\qquad - 1 = \big(- 3X^2 + 5X - 2\big)\big(\qquad\qquad \big)$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$X^3 \qquad\qquad\qquad\qquad - 1 = \big(-3X^2 + 5X - 2\big)\big(-\tfrac{1}{3}X \qquad \big)$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$\begin{array}{l}
\quad X^3 \qquad\qquad\qquad\qquad -1 = \big(-3X^2 + 5X - 2\big)\big(-\tfrac{1}{3}X \qquad \big) \\
\underline{-X^3 + \tfrac{5}{3}X^2 - \tfrac{2}{3}X}
\end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$\begin{array}{rrrrl} X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\tfrac{1}{3}X \qquad\big) \\ -X^3 & +\tfrac{5}{3}X^2 & -\tfrac{2}{3}X & & \\ \hline & \tfrac{5}{3}X^2 & -\tfrac{2}{3}X & -1 & \end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrr}
X^3 & & & -1 = \big(-3X^2+5X-2\big)\big(-\tfrac{1}{3}X-\tfrac{5}{9}\big) \\
-X^3 + & \tfrac{5}{3}X^2 & -\tfrac{2}{3}X & \\
\hline
 & \tfrac{5}{3}X^2 & -\tfrac{2}{3}X & -1
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\tfrac{1}{3}X-\tfrac{5}{9}\big) \\
\underline{-X^3} & \underline{+\tfrac{5}{3}X^2} & \underline{-\tfrac{2}{3}X} & & \\
 & \tfrac{5}{3}X^2 & -\tfrac{2}{3}X & -1 & \\
 & \underline{-\tfrac{5}{3}X^2} & \underline{+\tfrac{25}{9}X} & \underline{-\tfrac{10}{9}} &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\tfrac{1}{3}X-\tfrac{5}{9}\big) \\
-X^3 & +\frac{5}{3}X^2 & -\frac{2}{3}X & & \\
\hline
 & \frac{5}{3}X^2 & -\frac{2}{3}X & -1 & \\
 & -\frac{5}{3}X^2 & +\frac{25}{9}X & -\frac{10}{9} & \\
\hline
 & & \frac{19}{9}X & -\frac{19}{9} &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\frac{1}{3}X-\frac{5}{9}\big)+\frac{19}{9}X-\frac{19}{9} \\
-X^3 & +\frac{5}{3}X^2 & -\frac{2}{3}X & & \\
\hline
 & \frac{5}{3}X^2 & -\frac{2}{3}X & -1 & \\
 & -\frac{5}{3}X^2 & +\frac{25}{9}X & -\frac{10}{9} & \\
\hline
 & & \frac{19}{9}X & -\frac{19}{9} &
\end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\frac{1}{3}X-\frac{5}{9}\big)+\frac{19}{9}X-\frac{19}{9} \\
-X^3 & +\frac{5}{3}X^2 & -\frac{2}{3}X & & \\
\hline
 & \frac{5}{3}X^2 & -\frac{2}{3}X & -1 & \\
 & -\frac{5}{3}X^2 & +\frac{25}{9}X & -\frac{10}{9} & \\
\hline
 & & \frac{19}{9}X & -\frac{19}{9} &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\frac{1}{3}X-\frac{5}{9}\big)+\frac{19}{9}X-\frac{19}{9} \\
-X^3 & +\frac{5}{3}X^2 & -\frac{2}{3}X & & \\
\hline
 & \frac{5}{3}X^2 & -\frac{2}{3}X & -1 & \\
 & -\frac{5}{3}X^2 & +\frac{25}{9}X & -\frac{10}{9} & \\
\hline
 & & \frac{19}{9}X & -\frac{19}{9} &
\end{array}$$

Der Rest ist

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\frac{1}{3}X-\frac{5}{9}\big)+\frac{19}{9}X-\frac{19}{9} \\
-X^3 & +\frac{5}{3}X^2 & -\frac{2}{3}X & & \\
\hline
 & \frac{5}{3}X^2 & -\frac{2}{3}X & -1 & \\
 & -\frac{5}{3}X^2 & +\frac{25}{9}X & -\frac{10}{9} & \\
\hline
 & & \frac{19}{9}X & -\frac{19}{9} &
\end{array}$$

Der Rest ist $r_2 = \frac{19}{9}(X-1)$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\tfrac{1}{3}X-\tfrac{5}{9}\big)+\tfrac{19}{9}X-\tfrac{19}{9} \\
-X^3 & +\tfrac{5}{3}X^2 & -\tfrac{2}{3}X & & \\
\hline
& \tfrac{5}{3}X^2 & -\tfrac{2}{3}X & -1 & \\
& -\tfrac{5}{3}X^2 & +\tfrac{25}{9}X & -\tfrac{10}{9} & \\
\hline
& & \tfrac{19}{9}X & -\tfrac{19}{9} &
\end{array}
$$

Der Rest ist $r_2 = \frac{19}{9}(X-1)$ und im nächsten Schritt teilen wir $r_1 = -3X^2 + 5X - 2$ durch r_2.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$
\begin{array}{rrrrl}
X^3 & & & -1 & = \big(-3X^2+5X-2\big)\big(-\frac{1}{3}X-\frac{5}{9}\big)+\frac{19}{9}X-\frac{19}{9} \\
\underline{-X^3} & \underline{+\frac{5}{3}X^2} & \underline{-\frac{2}{3}X} & & \\
& \frac{5}{3}X^2 & -\frac{2}{3}X & -1 & \\
& \underline{-\frac{5}{3}X^2} & \underline{+\frac{25}{9}X} & \underline{-\frac{10}{9}} & \\
& & \frac{19}{9}X & -\frac{19}{9} &
\end{array}
$$

Der Rest ist $r_2 = \frac{19}{9}(X-1)$ und im nächsten Schritt teilen wir $r_1 = -3X^2 + 5X - 2$ durch r_2. Da das Polynom $\frac{19}{9}(X-1)$ genau dieselben Teiler wie $X - 1$ hat und auch genau dieselben Polynome teilt, können wir aber einfach auf $r_2' = X - 1$ übergehen.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$-3X^2 + 5X - 2 = \big(X - 1\big)\big(\qquad\qquad\big)$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$-3X^2 + 5X - 2 = \big(X - 1\big)\big(-3X \qquad\big)$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{aligned} -3X^2 + 5X - 2 &= \big(X - 1\big)\big(-3X \qquad\big) \\ \underline{\;\;3X^2 - 3X\;} & \end{aligned}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{l} -3X^2 + 5X - 2 = \big(X - 1\big)\big(-3X \qquad\big) \\ \quad\; 3X^2 - 3X \\ \hline \qquad\qquad 2X - 2 \end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{rl} -3X^2 + 5X - 2 = \big(X - 1\big)\big(-3X + 2\big) \\ \underline{3X^2 - 3X \phantom{{}-2}} & \\ 2X - 2 & \end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$
\begin{array}{rl}
-3X^2 + 5X - 2 &= \big(X - 1\big)\big(-3X + 2\big) \\
\underline{3X^2 - 3X\phantom{{}-2}} & \\
2X - 2 & \\
\underline{-2X + 2} &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$
\begin{array}{rl}
-3X^2 + 5X - 2 & = \big(X - 1\big)\big(-3X + 2\big) \\
\underline{3X^2 - 3X\phantom{{}-2}} & \\
2X - 2 & \\
\underline{-2X + 2} & \\
0 &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$
\begin{array}{rl}
-\,3X^2 + 5X - 2 &= \big(X-1\big)\big(-3X+2\big) \\
\underline{3X^2 - 3X\phantom{{}-2}} & \\
2X - 2 & \\
\underline{-\,2X + 2} & \\
0 &
\end{array}
$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{rl} -\,3X^2 + 5X - 2 &= \big(X-1\big)\big(-3X+2\big) \\ \underline{3X^2 - 3X\phantom{{}-2}} & \\ 2X - 2 & \\ \underline{-\,2X + 2} & \\ 0 & \end{array}$$

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{rl}
-\,3X^2 + 5X - 2 & = \big(X - 1\big)\big(-\,3X + 2\big) \\
\underline{3X^2 - 3X\phantom{{}-2}} & \\
2X - 2 & \\
\underline{-\,2X + 2} & \\
0 &
\end{array}$$

Der Rest ist 0,

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{rl} -3X^2 + 5X - 2 = & (X-1)(-3X+2) \\ 3X^2 - 3X \phantom{{}-2} & \\ \hline 2X - 2 & \\ -2X + 2 & \\ \hline 0 & \end{array}$$

Der Rest ist 0, also ist $X - 1$ ein größter gemeinsamer Teiler von den Ausgangspolynomen $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r_2' = X - 1$ ergibt:

$$\begin{array}{rl}
-3X^2 + 5X - 2 & = \big(X-1\big)\big(-3X+2\big) \\
3X^2 - 3X \phantom{{}-2} & \\
\hline
2X - 2 & \\
-2X + 2 & \\
\hline
0 &
\end{array}$$

Der Rest ist 0, also ist $X - 1$ ein größter gemeinsamer Teiler von den Ausgangspolynomen $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$. Tatsächlich ist $X - 1$ ein gemeinsamer Teiler:

$$p_1 = X^3 - 3X^2 + 5X - 3 = (X-1) \cdot (X^2 - 2X + 3)$$

und

$$p_2 = X^3 - 1 = (X-1) \cdot (X^2 + X + 1)\,.$$

Polynomfunktionen

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet
- im Folgenden betrachten wir Polynome (wie aus der Schule bekannt) als Funktionen von K nach K

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet
- im Folgenden betrachten wir Polynome (wie aus der Schule bekannt) als Funktionen von K nach K

Definition (Polynomfunktion)

Sei K ein Körper und $p = \sum_{i=0}^{n} a_i X^i$ ein Polynom in $K[X]$. Die Polynomfunktion $f_p\colon K \to K$ ist gegeben durch

$$x \mapsto \sum_{i=0}^{n} a_i x^i \in K \quad \text{für alle } x \in K\,.$$

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet
- im Folgenden betrachten wir Polynome (wie aus der Schule bekannt) als Funktionen von K nach K

Definition (Polynomfunktion)

Sei K ein Körper und $p = \sum_{i=0}^{n} a_i X^i$ ein Polynom in $K[X]$. Die Polynomfunktion $f_p \colon K \to K$ ist gegeben durch

$$x \mapsto \sum_{i=0}^{n} a_i x^i \in K \quad \text{für alle } x \in K\,.$$

- Üblicherweise wird das Polynom p und die Polynomfunktion f_p gleichgesetzt und wir schreiben einfach $p(x)$ für $f_p(x)$.

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet
- im Folgenden betrachten wir Polynome (wie aus der Schule bekannt) als Funktionen von K nach K

Definition (Polynomfunktion)

Sei K ein Körper und $p = \sum_{i=0}^{n} a_i X^i$ ein Polynom in $K[X]$. Die Polynomfunktion $f_p \colon K \to K$ ist gegeben durch

$$x \mapsto \sum_{i=0}^{n} a_i x^i \in K \quad \text{für alle } x \in K\,.$$

- Üblicherweise wird das Polynom p und die Polynomfunktion f_p gleichgesetzt und wir schreiben einfach $p(x)$ für $f_p(x)$.
- In diesem Fall ist aber x ein Element aus dem Körper K, welches **NICHT** mit der Unbekannten X des Polynomrings zu verwechseln ist.

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen,

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \setminus \{a\}} \frac{X - b}{a - b}$$

  eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \smallsetminus \{a\}} \frac{X-b}{a-b}$$

  eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

$\Rightarrow$ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \smallsetminus \{a\}} \frac{X-b}{a-b}$$

  eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

$\Rightarrow$ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben $\longrightarrow$ Schubfachprinzip

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \smallsetminus \{a\}} \frac{X - b}{a - b}$$

  eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

$\Rightarrow$ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben $\longrightarrow$ Schubfachprinzip

Beispiel: $p = X$ und $q = X^3$ in $(\mathbb{Z}/3\mathbb{Z})[X]$

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \setminus \{a\}} \frac{X - b}{a - b}$$

eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

$\Rightarrow$ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben $\longrightarrow$ Schubfachprinzip

Beispiel: $p = X$ und $q = X^3$ in $(\mathbb{Z}/3\mathbb{Z})[X]$

$$p(0) = 0\,, \qquad p(1) = 1\,, \qquad p(2) = 2$$

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g\colon K \to K$ gibt

  Bemerkung: tatsächlich hat für eine gegebene Funktion $g\colon K \to K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \setminus \{a\}} \frac{X - b}{a - b}$$

  eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

$\Rightarrow$ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben $\longrightarrow$ Schubfachprinzip

Beispiel: $p = X$ und $q = X^3$ in $(\mathbb{Z}/3\mathbb{Z})[X]$

$$p(0) = 0\,, \qquad p(1) = 1\,, \qquad p(2) = 2$$

und

$$q(0) = 0\,, \qquad q(1) = 1\,, \qquad q(2) = 2$$

Nullstellen

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$,

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte q, $r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\mathrm{grad}(r) < \mathrm{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$.

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\mathrm{grad}(r) < \mathrm{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a)$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\mathrm{grad}(r) < \mathrm{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a)$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\text{grad}(r) < \text{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r'$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\mathrm{grad}(r) < \mathrm{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\text{grad}(r) < \text{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$,

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$ und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$ und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$“) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$.

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$“) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a)$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' \,.$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$“) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a) = q(a) \cdot 0$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$“) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$“) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$ und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r'\,.$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$“) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

und somit ist a eine Nullstelle.

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt Nullstelle von (der Polynomfunktion) p, falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p, wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („$\Longrightarrow$") Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$und wegen $\operatorname{grad}(r) < \operatorname{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r' .$$

$\Rightarrow r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„$\Longleftarrow$") Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

und somit ist a eine Nullstelle. □

Nullstellen und Grad

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K$

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \smallsetminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \smallsetminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$) $\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n+1$: Sei $p \in K[X]$ mit Grad $n+1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n+1$: Sei $p \in K[X]$ mit Grad $n+1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\operatorname{grad}(q) = n$.

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \smallsetminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n+1$: Sei $p \in K[X]$ mit Grad $n+1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\operatorname{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen.

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \smallsetminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle $\checkmark$

Induktionsschritt $n \to n+1$: Sei $p \in K[X]$ mit Grad $n+1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\operatorname{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen. Für jede Nullstelle $b \in K \smallsetminus \{a\}$ von p gilt wegen $0 = p(b) = q(b) \cdot (b - a)$ auch $q(b) = 0$,

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n + 1$: Sei $p \in K[X]$ mit Grad $n + 1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a) .$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\operatorname{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen. Für jede Nullstelle $b \in K \setminus \{a\}$ von p gilt wegen $0 = p(b) = q(b) \cdot (b - a)$ auch $q(b) = 0$, d. h. b ist auch eine Nullstelle von q.

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \smallsetminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n + 1$: Sei $p \in K[X]$ mit Grad $n + 1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\operatorname{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen. Für jede Nullstelle $b \in K \smallsetminus \{a\}$ von p gilt wegen $0 = p(b) = q(b) \cdot (b - a)$ auch $q(b) = 0$, d. h. b ist auch eine Nullstelle von q.
$\Rightarrow p$ hat neben a höchstens n weitere Nullstellen (die von q)

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geqslant 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)
$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle ✓

Induktionsschritt $n \to n+1$: Sei $p \in K[X]$ mit Grad $n+1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a)\,.$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\operatorname{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen. Für jede Nullstelle $b \in K \setminus \{a\}$ von p gilt wegen $0 = p(b) = q(b) \cdot (b - a)$ auch $q(b) = 0$, d. h. b ist auch eine Nullstelle von q.
$\Rightarrow p$ hat neben a höchstens n weitere Nullstellen (die von q) □

Nullstellen bestimmen

- für Polynome $p = a_1X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen

Nullstellen bestimmen

- für Polynome $p = a_1X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist

$$a = -a_0 a_1^{-1}$$

die Nullstelle der Polynomfunktion p

Nullstellen bestimmen

- für Polynome $p = a_1X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel

Nullstellen bestimmen

- für Polynome $p = a_1 X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind

Nullstellen bestimmen

- für Polynome $p = a_1 X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt

Nullstellen bestimmen

- für Polynome $p = a_1X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt
- es gibt aber numerische Verfahren zur Approximation von Nullstellen für beliebige Polynome aus $\mathbb{R}[X]$

Nullstellen bestimmen

- für Polynome $p = a_1X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt
- es gibt aber numerische Verfahren zur Approximation von Nullstellen für beliebige Polynome aus $\mathbb{R}[X]$
- für Polynome $p \in K[X]$ von beliebigen Grade kann man mithilfe des Satzes, nachdem eine Nullstelle $a \in K$ gefunden wurde, mithilfe der Polynomdivision das Polynom q mit
$$p = q \cdot (X - a)$$
bestimmt werden und dann können die Nullstellen für q gesucht werden

Nullstellen bestimmen

- für Polynome $p = a_1 X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt
- es gibt aber numerische Verfahren zur Approximation von Nullstellen für beliebige Polynome aus $\mathbb{R}[X]$
- für Polynome $p \in K[X]$ von beliebigen Grade kann man mithilfe des Satzes, nachdem eine Nullstelle $a \in K$ gefunden wurde, mithilfe der Polynomdivision das Polynom q mit
$$p = q \cdot (X - a)$$
bestimmt werden und dann können die Nullstellen für q gesucht werden

Nullstellen bestimmen

- für Polynome $p = a_1 X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist
$$a = -a_0 a_1^{-1}$$
die Nullstelle der Polynomfunktion p
- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p-q-Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (Cardano-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt
- es gibt aber numerische Verfahren zur Approximation von Nullstellen für beliebige Polynome aus $\mathbb{R}[X]$
- für Polynome $p \in K[X]$ von beliebigen Grade kann man mithilfe des Satzes, nachdem eine Nullstelle $a \in K$ gefunden wurde, mithilfe der Polynomdivision das Polynom q mit
$$p = q \cdot (X - a)$$
bestimmt werden und dann können die Nullstellen für q gesucht werden
$\longrightarrow$ hilftreich da $\mathrm{grad}(q) < \mathrm{grad}(p)$

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

Beweis: Sei a eine Nullstelle von $X^2 + pX + q$. Dann gilt

$$0 = a^2 + pa + q$$

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

Beweis: Sei a eine Nullstelle von $X^2 + pX + q$. Dann gilt

$$0 = a^2 + pa + q = a^2 + 2\frac{p}{2}a + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q\,.$$

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

Beweis: Sei a eine Nullstelle von $X^2 + pX + q$. Dann gilt

$$0 = a^2 + pa + q = a^2 + 2\frac{p}{2}a + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q\,.$$

Die ersten drei Terme können wir mit der binomischen Formel zusammenfassen und nach Umstellen erhalten wir

$$\left(a + \frac{p}{2}\right)^2 = \left(\frac{p}{2}\right)^2 - q\,.$$

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

Beweis: Sei a eine Nullstelle von $X^2 + pX + q$. Dann gilt

$$0 = a^2 + pa + q = a^2 + 2\frac{p}{2}a + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q\,.$$

Die ersten drei Terme können wir mit der binomischen Formel zusammenfassen und nach Umstellen erhalten wir

$$\left(a + \frac{p}{2}\right)^2 = \left(\frac{p}{2}\right)^2 - q\,.$$

Da die linke Seite nicht negativ ist, muss $q \leqslant p^2/4$ gelten

p-q-Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leqslant p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \qquad \text{oder} \qquad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

Beweis: Sei a eine Nullstelle von $X^2 + pX + q$. Dann gilt

$$0 = a^2 + pa + q = a^2 + 2\frac{p}{2}a + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q\,.$$

Die ersten drei Terme können wir mit der binomischen Formel zusammenfassen und nach Umstellen erhalten wir

$$\left(a + \frac{p}{2}\right)^2 = \left(\frac{p}{2}\right)^2 - q\,.$$

Da die linke Seite nicht negativ ist, muss $q \leqslant p^2/4$ gelten und Wurzelziehen und Auflösen nach a ergibt die Behauptung. $\square$

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten.

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$:

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$**:** Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$.

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \cdots + a_1 \cdot \left(\frac{y}{z}\right) + a_0\,. \qquad (*)$$

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \cdots + a_1 \cdot \left(\frac{y}{z}\right) + a_0\,. \qquad (*)$$

Wir multiplizieren die Gleichung mit z^n, stellen nach y^n um und erhalten

$$y^n = z \cdot \big(-a_{n-1}y^{n-1} - \cdots - a_1 yz^{n-2} - a_0 z^{n-1}\big)\,.$$

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \cdots + a_1 \cdot \left(\frac{y}{z}\right) + a_0\,. \qquad (*)$$

Wir multiplizieren die Gleichung mit z^n, stellen nach y^n um und erhalten

$$y^n = z \cdot \left(- a_{n-1}y^{n-1} - \cdots - a_1 yz^{n-2} - a_0 z^{n-1}\right).$$

Da alle Koeffizienten $a_{n-1}, \ldots, a_0$ sowie y und z ganzzahlig sind, ist die rechte Seite ein ganzzahliges Vielfaches von z.

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \cdots + a_1 \cdot \left(\frac{y}{z}\right) + a_0 \,. \qquad (*)$$

Wir multiplizieren die Gleichung mit z^n, stellen nach y^n um und erhalten

$$y^n = z \cdot \big(- a_{n-1}y^{n-1} - \cdots - a_1 y z^{n-2} - a_0 z^{n-1} \big) \,.$$

Da alle Koeffizienten $a_{n-1}, \ldots, a_0$ sowie y und z ganzzahlig sind, ist die rechte Seite ein ganzzahliges Vielfaches von z. Somit muss y^n ein ganzzahliges Vielfaches von z sein.

Ganzzahlige Nullstellen

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \in \mathbb{Z}$**:** Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geqslant 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \cdots + a_1 \cdot \left(\frac{y}{z}\right) + a_0 \,. \qquad (*)$$

Wir multiplizieren die Gleichung mit z^n, stellen nach y^n um und erhalten

$$y^n = z \cdot \big(- a_{n-1}y^{n-1} - \cdots - a_1 y z^{n-2} - a_0 z^{n-1}\big) \,.$$

Da alle Koeffizienten $a_{n-1}, \ldots, a_0$ sowie y und z ganzzahlig sind, ist die rechte Seite ein ganzzahliges Vielfaches von z. Somit muss y^n ein ganzzahliges Vielfaches von z sein. Da $y \neq 0$ und $z \geqslant 1$ teilerfremd sind, kann z nur 1 sein. Insbesondere ist $b = y$ also ganzzahlig.

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist.

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist.

Ausgangspunkt ist wieder $(*)$. Da wir aber bereits wissen, dass $z = 1$ ist und somit $b = y \neq 0$ ist, erhalten wir nun

$$0 = b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0\,.$$

Lemma von Gauss – Beweis von $b \mid a_0$

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist.

Ausgangspunkt ist wieder $(*)$. Da wir aber bereits wissen, dass $z = 1$ ist und somit $b = y \neq 0$ ist, erhalten wir nun

$$0 = b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \,.$$

Diesmal stellen wir nach a_0 um und Klammern b aus. Somit gilt

$$a_0 = b\big(-b^{n-1} - a_{n-1}b^{n-2} - \cdots - a_2 b - a_1\big)\,.$$

Lemma von Gauss – Beweis von $b \mid a_0$

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist.

Ausgangspunkt ist wieder $(*)$. Da wir aber bereits wissen, dass $z = 1$ ist und somit $b = y \neq 0$ ist, erhalten wir nun

$$0 = b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 \,.$$

Diesmal stellen wir nach a_0 um und Klammern b aus. Somit gilt

$$a_0 = b\big(- b^{n-1} - a_{n-1}b^{n-2} - \dots - a_2 b - a_1\big) \,.$$

Nun folgt aus der Ganzzahligkeit von $b = y$ und $a_{n-1}, \dots, a_1$, dass die rechte Seite ein ganzahliges Vielfaches von b ist.

Lemma von Gauss – Beweis von $b \mid a_0$

Satz (Lemma von Gauss)

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0.

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist.

Ausgangspunkt ist wieder $(*)$. Da wir aber bereits wissen, dass $z = 1$ ist und somit $b = y \neq 0$ ist, erhalten wir nun

$$0 = b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \,.$$

Diesmal stellen wir nach a_0 um und Klammern b aus. Somit gilt

$$a_0 = b\big(- b^{n-1} - a_{n-1}b^{n-2} - \cdots - a_2 b - a_1\big) \,.$$

Nun folgt aus der Ganzzahligkeit von $b = y$ und $a_{n-1}, \ldots, a_1$, dass die rechte Seite ein ganzahliges Vielfaches von b ist.

Da $a_0 \in \mathbb{Z}$ folgt somit auch, dass a_0 ein ganzzahliges Vielfaches von b ist. $\square$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$.

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von GAUSS ganzzahlige Teiler des konstanten Terms -6,

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\} .$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$X^3 - 6X^2 + 11X - 6 = \big(X - 1\big)\big(\qquad\qquad\big)$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von GAUSS ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$X^3 - 6X^2 + 11X - 6 = \big(X - 1\big)\big(X^2 \qquad\qquad \big)$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von GAUSS ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{l} X^3 - 6X^2 + 11X - 6 = \big(X - 1\big)\big(X^2 \qquad\qquad \big) \\ \underline{-X^3 \;\; + X^2} \end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rl}
X^3 - 6X^2 + 11X - 6 & = (X-1)(X^2 \qquad\qquad) \\
\underline{-X^3 \;\; + X^2} \qquad\qquad & \\
-5X^2 + 11X \qquad &
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rl} X^3 - 6X^2 + 11X - 6 & = \big(X-1\big)\big(X^2 - 5X \qquad\big) \\ \underline{-X^3 \;\; + X^2} \qquad\qquad & \\ -5X^2 + 11X \qquad & \end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -6X^2 & +11X & -6 & = \big(X-1\big)\big(X^2 - 5X \qquad\big) \\
\underline{-X^3} & \underline{+X^2} & & & \\
 & -5X^2 & +11X & & \\
 & \underline{5X^2} & \underline{-5X} & & \\
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von GAUSS ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -\,6X^2 & +\,11X & -\,6 & = (X-1)(X^2 - 5X \qquad) \\
\underline{-\,X^3} & \underline{+\,X^2} & & & \\
 & -\,5X^2 & +\,11X & & \\
 & \underline{5X^2} & \underline{-\,5X} & & \\
 & & 6X & -\,6 &
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von GAUSS ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -\,6X^2 & +\,11X & -\,6 & = \big(X-1\big)\big(X^2 - 5X + 6\big) \\
\underline{-\,X^3} & \underline{+\,X^2} & & & \\
 & -\,5X^2 & +\,11X & & \\
 & \underline{5X^2} & \underline{-\,5X} & & \\
 & & 6X & -\,6 &
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -6X^2 & +11X & -6 & = \big(X-1\big)\big(X^2 - 5X + 6\big) \\
\underline{-X^3} & \underline{+X^2} & & & \\
 & -5X^2 & +11X & & \\
 & \underline{5X^2} & \underline{-5X} & & \\
 & & 6X & -6 & \\
 & & \underline{-6X} & \underline{+6} &
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -\,6X^2 & +\,11X & -\,6 & = \big(X-1\big)\big(X^2 - 5X + 6\big) \\
-\,X^3 & +\,X^2 & & & \\
\hline
& -\,5X^2 & +\,11X & & \\
& 5X^2 & -\,5X & & \\
\hline
& & 6X & -\,6 & \\
& & -\,6X & +\,6 & \\
\hline
& & & 0 &
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -\,6X^2 & +\,11X & -\,6 & = \big(X-1\big)\big(X^2-5X+6\big) \\
-\,X^3 & +\,X^2 & & & \\
\hline
 & -\,5X^2 & +\,11X & & \\
 & 5X^2 & -\,5X & & \\
\cline{2-3}
 & & 6X & -\,6 & \\
 & & -\,6X & +\,6 & \\
\cline{3-4}
 & & & 0 &
\end{array}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\} .$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -6X^2 & +11X & -6 & = (X-1)(X^2-5X+6) \\
-X^3 & +X^2 & & & \\
\hline
 & -5X^2 & +11X & & \\
 & 5X^2 & -5X & & \\
\hline
 & & 6X & -6 & \\
 & & -6X & +6 & \\
\hline
 & & & 0 &
\end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p-q-Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rl}
X^3 - 6X^2 + 11X - 6 & = \big(X-1\big)\big(X^2 - 5X + 6\big) \\
\underline{-X^3 + X^2 } & \\
-5X^2 + 11X & \\
\underline{5X^2 - 5X } & \\
6X - 6 & \\
\underline{-6X + 6} & \\
0 &
\end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p-q-Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6} = \frac{5}{2} \pm \sqrt{\frac{1}{4}}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rrrrl}
X^3 & -\,6X^2 & +\,11X & -\,6 & = (X-1)(X^2-5X+6) \\
-\,X^3 & +\,X^2 & & & \\
\hline
 & -\,5X^2 & +\,11X & & \\
 & 5X^2 & -\,5X & & \\
\hline
 & & 6X & -\,6 & \\
 & & -\,6X & +\,6 & \\
\hline
 & & & 0 &
\end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p-q-Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6} = \frac{5}{2} \pm \sqrt{\frac{1}{4}} = \frac{5}{2} \pm \frac{1}{2}$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rl}
X^3 - 6X^2 + 11X - 6 & = (X-1)(X^2 - 5X + 6) \\
\underline{-X^3 + X^2 } & \\
-5X^2 + 11X & \\
\underline{5X^2 - 5X } & \\
6X - 6 & \\
\underline{-6X + 6} & \\
0 &
\end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p-q-Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6} = \frac{5}{2} \pm \sqrt{\frac{1}{4}} = \frac{5}{2} \pm \frac{1}{2} \quad \Longrightarrow \quad \text{Nullstellen } 2 \text{ und } 3\,.$$

Ein letztes Beispiel

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von Gauss ganzzahlige Teiler des konstanten Terms -6, d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}\,.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.
Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{rl}
X^3 - 6X^2 + 11X - 6 & = (X-1)(X^2 - 5X + 6) \\
\underline{-X^3 + X^2} \qquad\qquad & \\
-5X^2 + 11X \qquad & \\
\underline{5X^2 - 5X} \qquad & \\
6X - 6 & \\
\underline{-6X + 6} & \\
0 &
\end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p-q-Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6} = \frac{5}{2} \pm \sqrt{\frac{1}{4}} = \frac{5}{2} \pm \frac{1}{2} \quad \Longrightarrow \quad \text{Nullstellen } 2 \text{ und } 3\,.$$

Das Polynom p vom Grad 3 hat also genau die drei Nullstellen 1, 2 und 3.