UNIVERSITÄT LEIPZIG

Vorlesung 14 - Ringe, Körper, Polynome

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

Übersicht

- Ein Ring

- Ein Ring ist eine algebrische Struktur

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
    - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
    - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
    - $\cdot$ ist assoziativ und kommutativ

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).
  - für alle

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).
  - für alle $a, b, c \in M$

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).
  - für alle $a, b, c \in M$ gilt

- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und kommutativ
  - es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).
  - für alle $a, b, c \in M$ gilt $a \cdot (b + c) = a \cdot b + a \cdot c$.

- Körper -

- Körper - ein Ring $(M, +, \cdot)$

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent:

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper,

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper:

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$,

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt,

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert,

- Körper - ein Ring $(M,+,\cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M,+,\cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\},\cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$. $(\mathbb{Z},+,\cdot)$ ist kein Körper.
- In einem Körper $(M,+,\cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - ▶ In der Tat,

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
    - In der Tat, wenn $x \neq 0$

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - In der Tat, wenn $x \neq 0$ dann können wir schreiben

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy =$

- Körper - ein Ring $(M,+,\cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M,+,\cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\},\cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$. $(\mathbb{Z},+,\cdot)$ ist kein Körper.
- In einem Körper $(M,+,\cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
    - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.
- Wenn A und B Ringe sind,

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.
- Wenn A und B Ringe sind, dann ist $A \times B$ ebenfalls ein Ring.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.
- Wenn A und B Ringe sind, dann ist $A \times B$ ebenfalls ein Ring. Wenn A und B jedoch Körper sind, dann ist $A \times B$ kein Körper:

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
  - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.
- Wenn A und B Ringe sind, dann ist $A \times B$ ebenfalls ein Ring. Wenn A und B jedoch Körper sind, dann ist $A \times B$ kein Körper: wir haben $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$

Beispiel

$\mathbb{Z}/m$ ist ein Ring.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist,

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden,

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist,

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper gdw.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper gdw. p ist eine Primzahl.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper gdw. p ist eine Primzahl.

- Der Körper $\mathbb{Q}$

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper gdw. p ist eine Primzahl.

- Der Körper $\mathbb{Q}$ und die Körper $\mathbb{Z}/p$

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper gdw. p ist eine Primzahl.

- Der Körper $\mathbb{Q}$ und die Körper $\mathbb{Z}/p$ werden als Primkörper bezeichnet.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

> **Lemma.** $\mathbb{Z}/p$ ist ein Körper gdw. p ist eine Primzahl.

- Der Körper $\mathbb{Q}$ und die Körper $\mathbb{Z}/p$ werden als Primkörper bezeichnet. Jeder Körper enthält ein Primkörper.

Beispiel

$\mathbb{Z}/m$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m$ kein Körper.

Lemma. $\mathbb{Z}/p$ ist ein Körper gdw. p ist eine Primzahl.

- Der Körper $\mathbb{Q}$ und die Körper $\mathbb{Z}/p$ werden als Primkörper bezeichnet. Jeder Körper enthält ein Primkörper.
- Gibt's andere als $\mathbb{Z}/p$ endliche Körper?

- Sei $(M, +, \cdot)$ ein Ring,

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$.

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p \colon M \to M$.

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p\colon M \to M$. Für alle $x \in M$:

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p \colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p\colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Wir schreiben auch $\operatorname{grad}(p) = n$.

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p \colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Wir schreiben auch $\mathrm{grad}(p) = n$. Das Nullpolynom p mit $p = 0$ hat kein Grad oder Grad $-\infty$.

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p \colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Wir schreiben auch $\operatorname{grad}(p) = n$. Das Nullpolynom p mit $p = 0$ hat kein Grad oder Grad $-\infty$. Ein Element $x \in M$ ist Nullstelle von p

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p\colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Wir schreiben auch $\mathrm{grad}(p) = n$. Das Nullpolynom p mit $p = 0$ hat kein Grad oder Grad $-\infty$. Ein Element $x \in M$ ist Nullstelle von p gdw. $p(x) = 0$.

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \dots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \dots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p \colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \dots a_n x^n \in M.$$

- Wir schreiben auch $\mathrm{grad}(p) = n$. Das Nullpolynom p mit $p = 0$ hat kein Grad oder Grad $-\infty$. Ein Element $x \in M$ ist Nullstelle von p gdw. $p(x) = 0$.
- Die Menge von allen Polynomen

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p\colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Wir schreiben auch $\mathrm{grad}(p) = n$. Das Nullpolynom p mit $p = 0$ hat kein Grad oder Grad $-\infty$. Ein Element $x \in M$ ist Nullstelle von p gdw. $p(x) = 0$.
- Die Menge von allen Polynomen mit Koeffizienten aus M

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p\colon M \to M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \ldots a_n x^n \in M.$$

- Wir schreiben auch $\mathrm{grad}(p) = n$. Das Nullpolynom p mit $p = 0$ hat kein Grad oder Grad $-\infty$. Ein Element $x \in M$ ist Nullstelle von p gdw. $p(x) = 0$.
- Die Menge von allen Polynomen mit Koeffizienten aus M wird mit $M[X]$ bezeichnet.

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$.

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:
  - $p(0) \equiv 2$,

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:
  - $p(0) \equiv 2$,
  - $p(1) \equiv 2 + 4 + 1 \equiv 2$,

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:
  - $p(0) \equiv 2$,
  - $p(1) \equiv 2 + 4 + 1 \equiv 2$,
  - $p(2) \equiv 4$,

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:
  - $p(0) \equiv 2$,
  - $p(1) \equiv 2 + 4 + 1 \equiv 2$,
  - $p(2) \equiv 4$,
  - $p(3) \equiv 2 + 2 + 4 \equiv 3$ und

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:
  - $p(0) \equiv 2$,
  - $p(1) \equiv 2 + 4 + 1 \equiv 2$,
  - $p(2) \equiv 4$,
  - $p(3) \equiv 2 + 2 + 4 \equiv 3$ und
  - $p(4) \equiv 2 + 1 + 1 \equiv 4$.

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:
  - $p(0) \equiv 2$,
  - $p(1) \equiv 2 + 4 + 1 \equiv 2$,
  - $p(2) \equiv 4$,
  - $p(3) \equiv 2 + 2 + 4 \equiv 3$ und
  - $p(4) \equiv 2 + 1 + 1 \equiv 4$.

  Offenbar hat p keine Nullstellen.

- Wie schnell

- Wie schnell kann man $p(a)$

- Wie schnell kann man $p(a)$ berechnen?

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$)

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$.

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1X + \ldots + a_nX$ ein Polynom von einem Grad $n \geq 0$.

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M,+,\cdot)$ ein Ring und sei $p = a_0 + a_1X + \ldots + a_nX$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

- Mit Induktion

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

- Mit Induktion beweisen wir dass mit Horner-Schema

- Wie schnell kann man $p(a)$ berechnen?
    - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
    - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
    - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
    - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

- Mit Induktion beweisen wir dass mit Horner-Schema brauchen wir nur $2n$ Operationen.

- Wie schnell kann man $p(a)$ berechnen?
    - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
    - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
    - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
    - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

- Mit Induktion beweisen wir dass mit Horner-Schema brauchen wir nur $2n$ Operationen. Also $C_1 \cdot n$.

- Wie schnell kann man $p(a)$ berechnen?
  - Wie viele Operationen $+$ und $\cdot$ werden gebraucht? .
  - Nicht mehr als: $(n+1)$ (für $a_n a^n$) $+n$ (für $a_{n-1}a^{n-1}$ ...
  - Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2.
  - kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \ldots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

- Mit Induktion beweisen wir dass mit Horner-Schema brauchen wir nur $2n$ Operationen. Also $C_1 \cdot n$. Deutlich besser als $C \cdot n^2$.

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper.

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$.

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$. Dann existieren Polynome

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$. Dann existieren Polynome t und r

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$. Dann existieren Polynome t und r mit

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\operatorname{grad}(q) \geq 0$. Dann existieren Polynome t und r mit

$$p(X) = t(X) \cdot q(X) + r(X)$$

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$. Dann existieren Polynome t und r mit

$$p(X) = t(X) \cdot q(X) + r(X)$$

und $\mathrm{grad}(r) < \mathrm{grad}(q)$.

Satz. (Polynomdivision) Sei $(M,+,\cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$. Dann existieren Polynome t und r mit

$$p(X) = t(X) \cdot q(X) + r(X)$$

und $\mathrm{grad}(r) < \mathrm{grad}(q)$.

- Die Polynome t und r

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\mathrm{grad}(q) \geq 0$. Dann existieren Polynome t und r mit

$$p(X) = t(X) \cdot q(X) + r(X)$$

und $\mathrm{grad}(r) < \mathrm{grad}(q)$.

- Die Polynome t und r erhält man per Polynomdivision.

$$
\begin{array}{r}
x^3 \phantom{{}-2x^2+4x} - x - 2 \\
x^2+1 \overline{\big)\; x^5 \phantom{{}-x^3} - 2x^2 + 4x + 7} \\
\underline{-x^5 - x^3 \phantom{{}-2x^2+4x+7}} \\
-x^3 - 2x^2 + 4x \phantom{{}+7} \\
\underline{x^3 \phantom{{}-2x^2} + x \phantom{{}+7}} \\
-2x^2 + 5x + 7 \\
\underline{2x^2 \phantom{{}+5x} + 2} \\
5x + 9
\end{array}
$$

$$
\begin{array}{r}
x^3 \qquad\qquad - x - 2 \\
x^2+1 \overline{\smash{)}\, x^5 \qquad - 2x^2 + 4x + 7} \\
\underline{-x^5 - x^3} \qquad\qquad\quad \\
-x^3 - 2x^2 + 4x \quad\; \\
\underline{x^3 \qquad\qquad + x} \quad\; \\
-2x^2 + 5x + 7 \\
\underline{2x^2 \qquad\quad + 2} \\
5x + 9
\end{array}
$$

- $x^5 - 2x^2 + 4x + 7$

$$
\begin{array}{rrrrrr}
 & x^3 & & & -x & -2 \\
\cline{2-6}
x^2+1 \big) & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -x^3 & & & \\
\cline{2-3}
 & & -x^3 & -2x^2 & +4x & \\
 & & x^3 & & +x & \\
\cline{3-5}
 & & & -2x^2 & +5x & +7 \\
 & & & 2x^2 & & +2 \\
\cline{4-6}
 & & & & 5x & +9
\end{array}
$$

- $x^5 - 2x^2 + 4x + 7 =$

$$
\begin{array}{r}
x^3 \qquad\qquad - x - 2 \\
x^2+1 \overline{\big)\; x^5 \qquad - 2x^2 + 4x + 7} \\
\underline{- x^5 - x^3} \qquad\qquad\qquad \\
- x^3 - 2x^2 + 4x \quad \\
\underline{x^3 \qquad\qquad + x} \quad \\
- 2x^2 + 5x + 7 \\
\underline{2x^2 \qquad\quad + 2} \\
5x + 9
\end{array}
$$

- $x^5 - 2x^2 + 4x + 7 = (x^3 - x - 2)(x^2 + 1)$

$$
\begin{array}{rrrrrr}
 & & x^3 & & -x & -2 \\ \cline{2-6}
x^2+1\big) & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -x^3 & & & \\ \cline{2-3}
 & & -x^3 & -2x^2 & +4x & \\
 & & x^3 & & +x & \\ \cline{3-5}
 & & & -2x^2 & +5x & +7 \\
 & & & 2x^2 & & +2 \\ \cline{4-6}
 & & & & 5x & +9
\end{array}
$$

- $x^5 - 2x^2 + 4x + 7 = (x^3 - x - 2)(x^2 + 1) + (5x + 9)$

$$
\begin{array}{r}
\frac{1}{2}x^3 \qquad\qquad - \frac{1}{4}x - 1 \\
2x^2 + 1 \overline{\smash{\big)}\; x^5 \qquad\qquad - 2x^2 \;\; + 4x + 7} \\
\underline{- x^5 - \frac{1}{2}x^3} \qquad\qquad\qquad\qquad\quad \\
- \frac{1}{2}x^3 - 2x^2 \;\; + 4x \qquad \\
\underline{\frac{1}{2}x^3 \qquad\qquad + \frac{1}{4}x} \qquad \\
- 2x^2 + \frac{17}{4}x + 7 \\
\underline{2x^2 \qquad\qquad + 1} \\
\frac{17}{4}x + 8
\end{array}
$$

$$
\begin{array}{rrrrrr}
 & & \frac{1}{2}x^3 & & -\frac{1}{4}x & -1 \\
\cline{2-6}
2x^2+1 \big) & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -\frac{1}{2}x^3 & & & \\
\cline{2-3}
 & & -\frac{1}{2}x^3 & -2x^2 & +4x & \\
 & & \frac{1}{2}x^3 & & +\frac{1}{4}x & \\
\cline{3-5}
 & & & -2x^2 & +\frac{17}{4}x & +7 \\
 & & & 2x^2 & & +1 \\
\cline{4-6}
 & & & & \frac{17}{4}x & +8
\end{array}
$$

- In $\mathbb{Q}$:

$$
\begin{array}{r|rrrrr}
 & & \frac{1}{2}x^3 & & -\frac{1}{4}x & -1 \\
\hline
2x^2+1 & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -\frac{1}{2}x^3 & & & \\
\cline{2-3}
 & & -\frac{1}{2}x^3 & -2x^2 & +4x & \\
 & & \frac{1}{2}x^3 & & +\frac{1}{4}x & \\
\cline{3-5}
 & & & -2x^2 & +\frac{17}{4}x & +7 \\
 & & & 2x^2 & & +1 \\
\cline{4-6}
 & & & & \frac{17}{4}x & +8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7$

$$
\begin{array}{r}
\frac{1}{2}x^3 \qquad\qquad - \frac{1}{4}x - 1 \\
2x^2+1 \overline{\big) \; x^5 \qquad\qquad - 2x^2 \;\; + 4x + 7} \\
\underline{- x^5 - \frac{1}{2}x^3 \qquad\qquad\qquad\qquad\qquad} \\
- \frac{1}{2}x^3 - 2x^2 \;\; + 4x \qquad \\
\underline{\frac{1}{2}x^3 \qquad\qquad + \frac{1}{4}x} \qquad \\
- 2x^2 + \frac{17}{4}x + 7 \\
\underline{2x^2 \qquad\qquad + 1} \\
\frac{17}{4}x + 8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7 =$

$$
\begin{array}{r|rrrrr}
 & & \tfrac{1}{2}x^3 & & -\tfrac{1}{4}x & -1 \\
\hline
2x^2+1 & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -\tfrac{1}{2}x^3 & & & \\
\cline{2-3}
 & & -\tfrac{1}{2}x^3 & -2x^2 & +4x & \\
 & & \tfrac{1}{2}x^3 & & +\tfrac{1}{4}x & \\
\cline{3-5}
 & & & -2x^2 & +\tfrac{17}{4}x & +7 \\
 & & & 2x^2 & & +1 \\
\cline{4-6}
 & & & & \tfrac{17}{4}x & +8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7 = (\frac{1}{2}x^3 - \frac{1}{4}x - 1)(2x^2 + 1) + (\frac{17}{4}x + 8)$

$$
\begin{array}{r}
 \tfrac{1}{2}x^3 \qquad\qquad - \tfrac{1}{4}x - 1 \\
2x^2+1 \overline{\Big)\; x^5 \qquad\quad - 2x^2 + 4x + 7} \\
-x^5 - \tfrac{1}{2}x^3 \qquad\qquad\qquad\qquad\quad \\
\hline
-\tfrac{1}{2}x^3 - 2x^2 + 4x \qquad \\
\tfrac{1}{2}x^3 \qquad\quad + \tfrac{1}{4}x \qquad \\
\hline
-2x^2 + \tfrac{17}{4}x + 7 \\
2x^2 \qquad\qquad + 1 \\
\hline
\tfrac{17}{4}x + 8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7 = (\frac{1}{2}x^3 - \frac{1}{4}x - 1)(2x^2 + 1) + (\frac{17}{4}x + 8)$
- In $\mathbb{Z}/5$:

$$
\begin{array}{rrrrrr}
 & & \frac{1}{2}x^3 & & -\frac{1}{4}x & -1 \\ \cline{2-6}
2x^2+1\big) & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -\frac{1}{2}x^3 & & & \\ \cline{2-3}
 & & -\frac{1}{2}x^3 & -2x^2 & +4x & \\
 & & \frac{1}{2}x^3 & & +\frac{1}{4}x & \\ \cline{3-5}
 & & & -2x^2 & +\frac{17}{4}x & +7 \\
 & & & 2x^2 & & +1 \\ \cline{4-6}
 & & & & \frac{17}{4}x & +8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7 = (\frac{1}{2}x^3 - \frac{1}{4}x - 1)(2x^2 + 1) + (\frac{17}{4}x + 8)$
- In $\mathbb{Z}/5$: $x^5 - 2x^2 + 4x + 2$

$$
\begin{array}{r|rrrrr}
 & & \frac{1}{2}x^3 & & -\frac{1}{4}x & -1 \\
\hline
2x^2+1 & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -\frac{1}{2}x^3 & & & \\
\cline{2-3}
 & & -\frac{1}{2}x^3 & -2x^2 & +4x & \\
 & & \frac{1}{2}x^3 & & +\frac{1}{4}x & \\
\cline{3-5}
 & & & -2x^2 & +\frac{17}{4}x & +7 \\
 & & & 2x^2 & & +1 \\
\cline{4-6}
 & & & & \frac{17}{4}x & +8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7 = (\frac{1}{2}x^3 - \frac{1}{4}x - 1)(2x^2 + 1) + (\frac{17}{4}x + 8)$
- In $\mathbb{Z}/5$: $x^5 - 2x^2 + 4x + 2 \equiv$

$$
\begin{array}{r|rrrrr}
 & & \frac{1}{2}x^3 & & -\frac{1}{4}x & -1 \\
\hline
2x^2+1 & x^5 & & -2x^2 & +4x & +7 \\
 & -x^5 & -\frac{1}{2}x^3 & & & \\
\cline{2-3}
 & & -\frac{1}{2}x^3 & -2x^2 & +4x & \\
 & & \frac{1}{2}x^3 & & +\frac{1}{4}x & \\
\cline{3-5}
 & & & -2x^2 & +\frac{17}{4}x & +7 \\
 & & & 2x^2 & & +1 \\
\cline{4-6}
 & & & & \frac{17}{4}x & +8
\end{array}
$$

- In $\mathbb{Q}$: $x^5 - 2x^2 + 4x + 7 = (\frac{1}{2}x^3 - \frac{1}{4}x - 1)(2x^2+1) + (\frac{17}{4}x + 8)$
- In $\mathbb{Z}/5$: $x^5 - 2x^2 + 4x + 2 \equiv (3x^3 + x - 1)(2x^2+1) + (3x+3)$

- Folgerung:

- Folgerung: Wenn M ist ein Körper,

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p, q) = 1$,

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p, q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$.

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p, q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p, q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p,q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p,q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
  - Z.B.

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p, q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p, q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
  - Z.B.
  - $p = x^4 - 2x^2 - 3x - 2$

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p,q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p,q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
  - Z.B.
  - $p = x^4 - 2x^2 - 3x - 2 \;\; q = x^3 + 4x^2 + 4x + 1$

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p,q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p,q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
  - Z.B.
  - $p = x^4 - 2x^2 - 3x - 2 \;\; q = x^3 + 4x^2 + 4x + 1$
  - Euklidischer Algorithmus:

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p,q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p,q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
  - Z.B.
  - $p = x^4 - 2x^2 - 3x - 2 \quad q = x^3 + 4x^2 + 4x + 1$
  - Euklidischer Algorithmus: $ggt(p,q) = x + 1$

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
    - Wenn $p, q \in M[X]$ und $ggt(p, q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p, q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
    - Z.B.
    - $p = x^4 - 2x^2 - 3x - 2 \;\; q = x^3 + 4x^2 + 4x + 1$
    - Euklidischer Algorithmus: $ggt(p, q) = x + 1$
    - Bezout-identiät:

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
  - Wenn $p, q \in M[X]$ und $ggt(p, q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($ggt(p, q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
  - Z.B.
  - $p = x^4 - 2x^2 - 3x - 2 \;\; q = x^3 + 4x^2 + 4x + 1$
  - Euklidischer Algorithmus: $ggt(p, q) = x + 1$
  - Bezout-identiät:

$$x + 1(5x^2/22 - 3x/11 - 3/11)p + (-5x/22 - 7/11)q$$

- Wir sagen, dass ein Polynom f

- Wir sagen, dass ein Polynom f irreduzibel ist,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung:

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
    - Das heißt,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
    - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft.

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \nmid a$, dann $f \mid b$.
  - Beweis.

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - Beweis. Wir schreiben $sf + ta = 1$,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
    - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
    - Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt,

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt, und deshalb teilt es auch die rechte Seite.

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt, und deshalb teilt es auch die rechte Seite.
  - Zum Beispiel:

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
  - ▶ Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - ▶ Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt, und deshalb teilt es auch die rechte Seite.
  - ▶ Zum Beispiel: in $\mathbb{Z}/5$

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: "Unreduzierbare Polynome sind prim"
  - Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt, und deshalb teilt es auch die rechte Seite.
  - Zum Beispiel: in $\mathbb{Z}/5$ das Polynom $p = X^2 + 4X + 2$

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf, C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
  - ▶ Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \not| a$, dann $f \mid b$.
  - ▶ Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt, und deshalb teilt es auch die rechte Seite.
  - ▶ Zum Beispiel: in $\mathbb{Z}/5$ das Polynom $p = X^2 + 4X + 2$ ist irreduzibel.

- Folgerung:

- Folgerung: (“Eindeutigkeit der Faktorisierung”)

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$,

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden.

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
    - Beweis.

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an,

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k$

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k =$

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$.

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$,

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist,

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i.

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung:

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$,

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent:

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
   - Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f gdw

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f gdw $(X - a) \mid f$.

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f gdw $(X - a) \mid f$.
  - ▶ In der Tat:

- Folgerung: ("Eindeutigkeit der Faktorisierung") Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
  - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f gdw $(X - a) \mid f$.
  - ▶ In der Tat: Wir schreiben $f = q(X - a) + r$,

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \ldots \cdot p_k$ geschrieben werden. Die Polynome $p_1, \ldots, p_k$ sindp bis zur Multiplikation mit einer Konstanten eindeutig.
    - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \ldots \cdot p_k = r_1 \ldots r_l$. Dann teilt p_1 das Produkt $r_1 \ldots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i. Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f gdw $(X - a) \mid f$.
    - ▶ In der Tat: Wir schreiben $f = q(X - a) + r$, mit $\deg r < 1$.

- Folgerung:

- Folgerung: Ein Polynom f in $M[X]$

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
    - Die Polynome $(X - a)$

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel,

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
    - ▶ Die Polynome $(X - a)$ sind irreduzibel, wenn also a

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist,

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f.

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe,

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe, die keine Körper sind,

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe, die keine Körper sind, gilt dies nicht.

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe, die keine Körper sind, gilt dies nicht.
  - In $\mathbb{Z}/8$

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X-a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X-a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe, die keine Körper sind, gilt dies nicht.
  - In $\mathbb{Z}/8$ hat das Polynom x^3

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
  - Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f. Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe, die keine Körper sind, gilt dies nicht.
  - In $\mathbb{Z}/8$ hat das Polynom x^3 die Wurzeln $0, 2, 4, 6$.

- Wir können nun Körper

- Wir können nun Körper mit p^k Elementen

- Wir können nun Körper mit p^k Elementen konstruieren.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit x^2+x+2 beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2+x+2)$, die aus allen Polynomen vom Grad höchstens $k-1$ besteht. In unserem Beispiel also $ux+v$,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2)$

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv$

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit x^2+x+2 beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2+x+2)$, die aus allen Polynomen vom Grad höchstens $k-1$ besteht. In unserem Beispiel also $ux+v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x+3)(x+2) \equiv x^2+1$

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv$

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x+3)(x+2) \equiv x^2 + 1 \equiv -x - 3$.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit x^2+x+2 beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2+x+2)$, die aus allen Polynomen vom Grad höchstens $k-1$ besteht. In unserem Beispiel also $ux+v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x+3)(x+2) \equiv x^2+1 \equiv -x-3$.
  - ▶ Die Irreduzibilität von F

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
    - Die Irreduzibilität von F wird benutzt,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
    - Die Irreduzibilität von F wird benutzt, um zu zeigen,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit x^2+x+2 beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2+x+2)$, die aus allen Polynomen vom Grad höchstens $k-1$ besteht. In unserem Beispiel also $ux+v$, mit $u,v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x+3)(x+2) \equiv x^2+1 \equiv -x-3$.
  - Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit x^2+x+2 beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2+x+2)$, die aus allen Polynomen vom Grad höchstens $k-1$ besteht. In unserem Beispiel also $ux+v$, mit $u,v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x+3)(x+2) \equiv x^2+1 \equiv -x-3$.
    - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
    - ▶ In der Tat:

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit x^2+x+2 beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2+x+2)$, die aus allen Polynomen vom Grad höchstens $k-1$ besteht. In unserem Beispiel also $ux+v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x+3)(x+2) \equiv x^2+1 \equiv -x-3$.
  - Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - In der Tat: Wenn $g \in M[X]/(x^2+x+2)$,

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - ▶ In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir mitte Bezout-Identität

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - ▶ In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir mitte Bezout-Identität $ag + bF = 1$ für einige Polynome a, b

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - ▶ In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir mitte Bezout-Identität $ag + bF = 1$ für einige Polynome a, b schreiben.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - ▶ In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir mitte Bezout-Identität $ag + bF = 1$ für einige Polynome a, b schreiben. Dann ist a die multiplikative Inverse von g

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irrreduzierbaren Polynom F vom Grad k. Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F. Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
  - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
  - ▶ In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir mitte Bezout-Identität $ag + bF = 1$ für einige Polynome a, b schreiben. Dann ist a die multiplikative Inverse von g modulo F.

Satz. [Moore]

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt).

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim,

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M|$

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| =$

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ endliche Körper

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ endliche Körper mit gleich vielen Elementen.

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ endliche Körper mit gleich vielen Elementen. Dann sind

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ endliche Körper mit gleich vielen Elementen. Dann sind $\mathcal{K}$ und $\mathcal{N}$ isomorph.

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ endliche Körper mit gleich vielen Elementen. Dann sind $\mathcal{K}$ und $\mathcal{N}$ isomorph.

- Insbesondere:

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Kórper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ endliche Körper mit gleich vielen Elementen. Dann sind $\mathcal{K}$ und $\mathcal{N}$ isomorph.

- Insbesondere: kein Körper mit 6 Elemente.

- Sei $(M, +, \cdot)$ ein Ring.

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen,

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist,

- Sei $(M,+,\cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
    - I eine Untergruppe von $(M, +)$ ist

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
    - I eine Untergruppe von $(M, +)$ ist und

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - I eine Untergruppe von $(M, +)$ ist und
  - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - I eine Untergruppe von $(M, +)$ ist und
  - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M.

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
    - I eine Untergruppe von $(M, +)$ ist und
    - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M. Jedes andere Ideal heißt echt.

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - I eine Untergruppe von $(M, +)$ ist und
  - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M. Jedes andere Ideal heißt echt. Ein Ideal ist echt,

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - I eine Untergruppe von $(M, +)$ ist und
  - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M. Jedes andere Ideal heißt echt. Ein Ideal ist echt, wenn es 1_M nicht als Element enthält.

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - ▶ I eine Untergruppe von $(M, +)$ ist und
  - ▶ für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M. Jedes andere Ideal heißt echt. Ein Ideal ist echt, wenn es 1_M nicht als Element enthält.
- $\{0\} \subset M$ ist ein Ideal.

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - I eine Untergruppe von $(M, +)$ ist und
  - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M. Jedes andere Ideal heißt echt. Ein Ideal ist echt, wenn es 1_M nicht als Element enthält.
- $\{0\} \subset M$ ist ein Ideal.
- $n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal für jede natürliche Zahl n.

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein Ideal ist, wenn
  - I eine Untergruppe von $(M, +)$ ist und
  - für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M. Jedes andere Ideal heißt echt. Ein Ideal ist echt, wenn es 1_M nicht als Element enthält.
- $\{0\} \subset M$ ist ein Ideal.
- $n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal für jede natürliche Zahl n.
- $fM[X] \subset M[X]$ ist ein Ideal für jedes Polynomi f.

- Ist $I \subset M$ ein Ideal,

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring,

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an,

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$. Daraus folgt, dass

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$. Daraus folgt, dass $n'(m - m') + m(n - n') = mn - n'm' \in I$

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$. Daraus folgt, dass $n'(m - m') + m(n - n') = mn - n'm' \in I$ und somit tatsächlich $[mn] = [m'n']$.

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$. Daraus folgt, dass $n'(m - m') + m(n - n') = mn - n'm' \in I$ und somit tatsächlich $[mn] = [m'n']$. □

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I.

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$. Daraus folgt, dass $n'(m - m') + m(n - n') = mn - n'm' \in I$ und somit tatsächlich $[mn] = [m'n']$. □
- Spezieller Fall: $\mathbb{Z}/5[X]/(x^2 + x + 2)$.

UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski
Mathematisches Institut

grabowski@math.uni-leipzig.de