UNIVERSITÄT
LEIPZIG

Vorlesung 13 - Kommutative Gruppen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

Kommutative Gruppen - zwei äquivalente Definitionen.

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen:

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M,+)$ ist eine kommutative Gruppe, gdw.

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen:
$(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$,

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$, so dass

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M,+)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x+y)+z = x+(y+z)$
- für alle $x, y \in M$ gilt $x+y = y+x$
- es gibt $0 \in M$, so dass für alle $x \in M$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen:
$(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$, so dass für alle $x \in M$ gilt

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$
- für alle $x \in M$

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$
- für alle $x \in M$ gibt es y

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen: $(M, +)$ ist eine kommutative Gruppe, gdw.

- für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- für alle $x, y \in M$ gilt $x + y = y + x$
- es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$
- für alle $x \in M$ gibt es y so dass $x + y = 0$.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \dots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
    - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
    - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi\colon M \to N$,

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi\colon M \to N$, so dass für alle $a, b \in M$ gilt

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist "Addition modulon n". Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi\colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
    - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi\colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
    - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi\colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi\colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$ und

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi \colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$ und für alle $x \in M$ gilt

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.

- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.

- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.

  - Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.

- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi \colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$ und für alle $x \in M$ gilt $\varphi(-x) = -\varphi(x)$

- Beispiele von Gruppenhomomorphismen:

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n$,

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n,\ f(x) := x \mod n.$

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n,\ f(x) := x \mod n.$
  - $f : \mathbb{Z}/m \to \mathbb{Z}/n,$

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n,\ f(x) := x \mod n$.
  - $f : \mathbb{Z}/m \to \mathbb{Z}/n$, wenn $n \mid m$.

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n,\ f(x) := x \mod n.$
  - $f : \mathbb{Z}/m \to \mathbb{Z}/n,$ wenn $n \mid m.$ $f(x) := x \mod n.$

- Beispiele von Gruppenhomomorphismen:
  - $f: \mathbb{Z} \to \mathbb{Z}/n$, $f(x) := x \mod n$.
  - $f: \mathbb{Z}/m \to \mathbb{Z}/n$, wenn $n \mid m$. $f(x) := x \mod n$.
  - $n \mid m$ ist nötig

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n$, $f(x) := x \mod n$.
  - $f : \mathbb{Z}/m \to \mathbb{Z}/n$, wenn $n \mid m$. $f(x) := x \mod n$.
  - $n \mid m$ ist nötig um einen Homomorpphismu zu haben.

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n,\ f(x) := x \mod n$.
  - $f : \mathbb{Z}/m \to \mathbb{Z}/n$, wenn $n \mid m$. $f(x) := x \mod n$.
  - $n \mid m$ ist nötig um einen Homomorpphismu zu haben. Z.B. $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/3$ mit $f(x) := x \mod 3$ ist kein Homomorphismus:

- Beispiele von Gruppenhomomorphismen:
  - $f : \mathbb{Z} \to \mathbb{Z}/n$, $f(x) := x \mod n$.
  - $f : \mathbb{Z}/m \to \mathbb{Z}/n$, wenn $n \mid m$. $f(x) := x \mod n$.
  - $n \mid m$ ist nötig um einen Homomorppphismu zu haben. Z.B. $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/3$ mit $f(x) := x \mod 3$ ist kein Homomorphismus: $f(3+3) = f(6) = f(1) = 1$, aber $f(3) + f(3) = 0 + 0 = 0$.

- Beispiele von Gruppenhomomorphismen:
  - $f: \mathbb{Z} \to \mathbb{Z}/n$, $f(x) := x \mod n$.
  - $f: \mathbb{Z}/m \to \mathbb{Z}/n$, wenn $n \mid m$. $f(x) := x \mod n$.
  - $n \mid m$ ist nötig um einen Homomorpphismu zu haben. Z.B. $f: \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/3$ mit $f(x) := x \mod 3$ ist kein Homomorphismus: $f(3+3) = f(6) = f(1) = 1$, aber $f(3) + f(3) = 0 + 0 = 0$.
  -

Sei $(M, +)$ eine kommutative Gruppe.

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe,

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die “triviale Untergruppe” von M.

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die “triviale Untergruppe” von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe,

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$.

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$,

Sei $(M,+)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x,0) \colon x \in \mathbb{Z}\}$, $\{(x,x) \colon x \in \mathbb{Z}\}$, $\{(5x,7x) \colon x \in \mathbb{Z}\}$.

Sei $(M,+)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x,0) : x \in \mathbb{Z}\}$, $\{(x,x) : x \in \mathbb{Z}\}$, $\{(5x,7x) : x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x, 0) : x \in \mathbb{Z}\}$, $\{(x, x) : x \in \mathbb{Z}\}$, $\{(5x, 7x) : x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \ldots, n-k\}$

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x, 0) \colon x \in \mathbb{Z}\}$, $\{(x, x) \colon x \in \mathbb{Z}\}$, $\{(5x, 7x) \colon x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \ldots, n - k\}$ ist eine Untergruppe von $\mathbb{Z}/n$

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x, 0) \colon x \in \mathbb{Z}\}$, $\{(x, x) \colon x \in \mathbb{Z}\}$, $\{(5x, 7x) \colon x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \ldots, n-k\}$ ist eine Untergruppe von $\mathbb{Z}/n :=$

Sei $(M,+)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die “triviale Untergruppe” von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x,0) \colon x \in \mathbb{Z}\}$, $\{(x,x) \colon x \in \mathbb{Z}\}$, $\{(5x,7x) \colon x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \dots, n-k\}$ ist eine Untergruppe von $\mathbb{Z}/n := \{0, 1, 2, \dots, n\}$.

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x, 0) \colon x \in \mathbb{Z}\}$, $\{(x, x) \colon x \in \mathbb{Z}\}$, $\{(5x, 7x) \colon x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \ldots, n-k\}$ ist eine Untergruppe von $\mathbb{Z}/n := \{0, 1, 2, \ldots, n\}$. Diese Untergruppe

Sei $(M,+)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die "triviale Untergruppe" von M.
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.
- $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x,0) \colon x \in \mathbb{Z}\}$, $\{(x,x) \colon x \in \mathbb{Z}\}$, $\{(5x,7x) \colon x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \ldots, n-k\}$ ist eine Untergruppe von $\mathbb{Z}/n := \{0, 1, 2, \ldots, n\}$. Diese Untergruppe ist isomorph zu $\mathbb{Z}/\frac{n}{k}$.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \dots, n-1\}$ definiert,

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \dots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$,

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$,

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
    - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$,

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ...,

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, …, $\{\ldots -1, n-1, \ldots\}$

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots -1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n - 1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n - 1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
  - Die Addition

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n - 1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
  - Die Addition ist dann definiert als $[x] + [y] := [x + y]$.

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
  - Die Addition ist dann definiert als $[x] + [y] := [x+y]$.
  - Der Homomorphismus

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
  - Die Addition ist dann definiert als $[x] + [y] := [x + y]$.
  - Der Homomorphismus $\mathbb{Z} \to \mathbb{Z}/n$

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
    - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
    - Die Addition ist dann definiert als $[x] + [y] := [x+y]$.
    - Der Homomorphismus $\mathbb{Z} \to \mathbb{Z}/n$ ist dann definiert als

- Wir haben $\mathbb{Z}/n$ als $\{0, 1, 2, \ldots, n-1\}$ definiert, mit addition modulo n.
- Etwas abstraktere Perspektive:
  - wir haben eine Äquivalenzrelation auf $\mathbb{Z}$, gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, 1, n+1, \ldots\}$, ..., $\{\ldots - 1, n-1, \ldots\}$
- Wir können alternativ $\mathbb{Z}/n$ als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
  - Die Addition ist dann definiert als $[x] + [y] := [x + y]$.
  - Der Homomorphismus $\mathbb{Z} \to \mathbb{Z}/n$ ist dann definiert als $f(x) := [x]$.

- Sei nun p eine Primzahl.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten:

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^*$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten:
  $\mathbb{Z}/p^* :=$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \dots, p-1\}$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.
  - In $\mathbb{Z}/7^*$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
    - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
    - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
    - Assoziativität, Kommutativität - klar

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element:

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
  - Inversen:

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: $1. \quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist:

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende:

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
    - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
    - Assoziativität, Kommutativität - klar
    - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
    - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \bmod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
    - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
    - Assoziativität, Kommutativität - klar
    - Neutrales Element: $1. \quad 1 \cdot x \equiv x \mod p$.
    - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
    - Betrachten wir die Funktion

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: $1. \quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - ▶ Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - ▶ Betrachten wir die Funktion $f\colon \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \dots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: $1. \quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - ▶ Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - ▶ Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - ▶ Diese Funktion ist injektiv:

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
    - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
    - Assoziativität, Kommutativität - klar
    - Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
    - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
    - Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
    - Diese Funktion ist injektiv: Wenn $ax \equiv ay$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: 1. $\quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - ▶ Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - ▶ Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$, d.h. $p \mid a(x-y)$.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
    - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
    - Assoziativität, Kommutativität - klar
    - Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
    - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
    - Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
    - Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$, d.h. $p \mid a(x-y)$. Also entweder $p \mid a$

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \dots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - Betrachten wir die Funktion $f\colon \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$, d.h. $p \mid a(x-y)$. Also entweder $p \mid a$ oder $p \mid (x-y)$,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - ▶ Assoziativität, Kommutativität - klar
  - ▶ Neutrales Element: $1.\quad 1 \cdot x \equiv x \mod p$.
  - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - ▶ Betrachten wir die Funktion $f\colon \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - ▶ Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$, d.h. $p \mid a(x-y)$. Also entweder $p \mid a$ oder $p \mid (x-y)$, aber das ist nicht möglich.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: 1. $1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - Betrachten wir die Funktion $f : \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$, d.h. $p \mid a(x-y)$. Also entweder $p \mid a$ oder $p \mid (x-y)$, aber das ist nicht möglich.
  - Somit ist f auch surjektiv,

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten: $\mathbb{Z}/p^* := \{1, 2, \ldots, p-1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \mod p$.
  - In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
  - Assoziativität, Kommutativität - klar
  - Neutrales Element: $1. \quad 1 \cdot x \equiv x \mod p$.
  - Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: für ein gegebenes $a \in \mathbb{Z}/p^*$ müssen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \mod p$.
  - Betrachten wir die Funktion $f\colon \mathbb{Z}/p^* \to \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
  - Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x-y) \equiv 0 \mod p$, d.h. $p \mid a(x-y)$. Also entweder $p \mid a$ oder $p \mid (x-y)$, aber das ist nicht möglich.
  - Somit ist f auch surjektiv, und somit $ab \equiv 1$ für irgendein b.

- In Anwendungen

- In Anwendungen ist es äußerst wichtig,

- In Anwendungen ist es äußerst wichtig, diese "multiplikative Inversen modulo p"

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p

- In Anwendungen ist es äußerst wichtig, diese "multiplikative Inversen modulo p" zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
    - Wenn p 1000 Ziffern hat

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1 000$

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1 000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\, in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1 000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen, etwas komplizierteren Beweis,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1 000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen, etwas komplizierteren Beweis, dass multiplikative Inverse

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1 000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen, etwas komplizierteren Beweis, dass multiplikative Inverse modulo p

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a\ in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen, etwas komplizierteren Beweis, dass multiplikative Inverse modulo p existieren,

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
  - Wenn p 1000 Ziffern hat und wir ein Element $a in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^1 000$ verschiedene Elemente von $\mathbb{Z}/p^*$ überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen, etwas komplizierteren Beweis, dass multiplikative Inverse modulo p existieren, der einen effektiven Algorithmus liefert.

- Wir führen den euklidischen Algorithmus durch,

- Wir führen den euklidischen Algorithmus durch, mit p und a,

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
    - $p = q_1 a + r_1$
    - $a = q_2 r_1 + r_2$

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\ldots$

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\dots$
  - $r_{k-2} = q_k r_{k-1} + r_k$

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\dots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\ldots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\dots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$,

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
    - $p = q_1 a + r_1$
    - $a = q_2 r_1 + r_2$
    - $r_1 = q_3 r_2 + r_3$
    - $\dots$
    - $r_{k-2} = q_k r_{k-1} + r_k$
    - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\ldots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen,

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\ldots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*:

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\dots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*: $xp + ya = r_k = 1$ für einige x, y.

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\dots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*: $xp + ya = r_k = 1$ für einige x, y. Jetzt ist y die multiplikative Inverse von a.

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\ldots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*: $xp + ya = r_k = 1$ für einige x, y. Jetzt ist y die multiplikative Inverse von a.
- Die Anzahl der Zeilen

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
    - $p = q_1 a + r_1$
    - $a = q_2 r_1 + r_2$
    - $r_1 = q_3 r_2 + r_3$
    - $\ldots$
    - $r_{k-2} = q_k r_{k-1} + r_k$
    - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*: $xp + ya = r_k = 1$ für einige x, y. Jetzt ist y die multiplikative Inverse von a.
- Die Anzahl der Zeilen im euklidischen Algorithmus

- Wir führen den euklidischen Algorithmus durch, mit p und a, das wir invertieren wollen.
  - $p = q_1 a + r_1$
  - $a = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\ldots$
  - $r_{k-2} = q_k r_{k-1} + r_k$
  - $r_{k-1} = q_{k+1} r_k$.
- Dann ist r_k gleich zu $ggt(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*: $xp + ya = r_k = 1$ für einige x, y. Jetzt ist y die multiplikative Inverse von a.
- Die Anzahl der Zeilen im euklidischen Algorithmus ist vergleichbar mit $\log(p)$.

- Wenn $n \mid m$,

- Wenn $n \mid m$, dann haben wir

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$,

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.
- Der folgende Satz ist als “Chinesischer Restsatz” bekannt.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$.

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.
- Der folgende Satz ist als “Chinesischer Restsatz” bekannt.

> **Satz.** Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.
- Der folgende Satz ist als “Chinesischer Restsatz” bekannt.

> **Satz.** Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

- Dieser Satz ist extrem häufig benutzt.

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.
- Der folgende Satz ist als “Chinesischer Restsatz” bekannt.

> **Satz.** Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

- Dieser Satz ist extrem häufig benutzt. Anders gesagt:

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.
- Der folgende Satz ist als “Chinesischer Restsatz” bekannt.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

- Dieser Satz ist extrem häufig benutzt. Anders gesagt: Gegeben sind $k, l \in \mathbb{Z}$.

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomomorphismus $\varphi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \mod n$.
- Der folgende Satz ist als "Chinesischer Restsatz" bekannt.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

- Dieser Satz ist extrem häufig benutzt. Anders gesagt: Gegeben sind $k, l \in \mathbb{Z}$. Wir wollen die Gleichungs-system $x \equiv k \mod a$, $x \equiv l \mod b$ lösen.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) :=$

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \dots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.
- Dann $a \mid y - x$ und $b \mid y - x$.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.
- Dann $a \mid y - x$ und $b \mid y - x$. Da aber a und b teilfremd sind,

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.
- Dann $a \mid y - x$ und $b \mid y - x$. Da aber a und b teilfremd sind, bedeutet dies, dass $n \mid y - x$.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.
- Dann $a \mid y - x$ und $b \mid y - x$. Da aber a und b teilfremd sind, bedeutet dies, dass $n \mid y - x$. Widerspruch zu der Tatsache, dass $0 < y - x < n$.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomoprhismus $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \mod a, x \mod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.
- Dann $a \mid y - x$ und $b \mid y - x$. Da aber a und b teilfremd sind, bedeutet dies, dass $n \mid y - x$. Widerspruch zu der Tatsache, dass $0 < y - x < n$. $\square$

- Was für eine Gruppe ist $\mathbb{Z}/p^*$? Ist sie zu $\mathbb{Z}/(n-1)$ isomorph?

- Natürlich gibt es für Zahlenmengen

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen,

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation.

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings*

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- Ein Ring

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder "kommutativen Rings mit Eins").
- Ein Ring ist eine algebrische Struktur

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder "kommutativen Rings mit Eins").
- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
    - $(M, +)$ ist eine kommutative Gruppe

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass
  - $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
  - $\cdot$ ist assoziativ und

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder "kommutativen Rings mit Eins").
- 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

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- 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 $1_M \in M$

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- 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 $m \in M$

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- 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 $1_M \cdot m = m$

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder "kommutativen Rings mit Eins").
- 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).

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder "kommutativen Rings mit Eins").
- 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

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).

- 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 $a, b, c \in M$

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- 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

- Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- 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 $a \cdot (b + c) = a \cdot b + a \cdot c$.

- Wie bei Gruppen

- Wie bei Gruppen könnten wir Ringe

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring,

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x.

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x.
  - Tatsächlich:

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x.
  - Tatsächlich: $0 \cdot x = (0 + 0) \cdot x =$

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x.
  - Tatsächlich: $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$,

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x.
    - Tatsächlich: $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, und da $(M, +)$ eine kommutative Gruppe ist,

- Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ is ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x.
    - Tatsächlich: $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, und da $(M, +)$ eine kommutative Gruppe ist, folgt $0 \cdot x = 0$.

- 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

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

Beispiel

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

Beispiel

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

Beispiel

$\mathbb{Z}/m\mathbb{Z}$ 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

$\mathbb{Z}/m\mathbb{Z}$ 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

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

Beispiel

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

Beweis.

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass,

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist,

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p ist eine Primzahl,

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p ist eine Primzahl, dann die multiplikative Inversen existieren,

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p ist eine Primzahl, dann die multiplikative Inversen existieren, also $\mathbb{Z}/p$ ist ein Körper.

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p ist eine Primzahl, dann die multiplikative Inversen existieren, also $\mathbb{Z}/p$ ist ein Körper. □

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p ist eine Primzahl, dann die multiplikative Inversen existieren, also $\mathbb{Z}/p$ ist ein Körper. □

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

Beispiel

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

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p ist eine Primzahl, dann die multiplikative Inversen existieren, also $\mathbb{Z}/p$ ist ein Körper. $\square$

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

UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski
Mathematisches Institut

grabowski@math.uni-leipzig.de