Diskrete Strukturen

Vorlesung 11: Körper

8. Januar 2019

Organisation

Prüfung:

- Freitag, den 22. Februar 2019 von 10–11 Uhr
  im AudiMax, HS 3, HS 9
- Abmeldungen noch bis zum 14. Januar 2019, 12 Uhr möglich
- schriftlich, 60 min
- Hilfsmittel: nur ein beschriebenes oder bedrucktes DIN-A4-Blatt

Organisation

neue Übungsleiter (der Übungen von Frau Götze):

- mittwochs, 7:30-9:00 Uhr: Martin Böhm
- donnerstags, 7:30-9:00 Uhr: Martin Böhm
- donnerstags, 11:15-12:45 Uhr: Tobias Rosenkranz
- freitags, 9:15-10:45 Uhr: Mirko Schulze

Nächste Termine — Modul “Diskrete Strukturen”

Hörsaalübung (Mo. 9:15)	**Vorlesung (Di. 17:15)**
7.1. —	8.1. Körper (5. Abgabe + 6. Übungsblatt)
14.1. Hörsaalübung 6. Übungswoche	15.1. Graphen und Bäume (Abgabe 1. Bonushalbserie)
21.1. —	22.1. Planarität von Graphen (6. Abgabe + 7. Übungsblatt)
28.1. Hörsaalübung 7. Übungswoche	29.1. Färbbarkeit von Graphen (Abgabe 2. Bonushalbserie)
4.2. Tutorium (Klausurvorbereitung)	5.2. Arithmetik

Vorlesungsstruktur

1. Mathematische Grundlagen
   - Aussagen- und Prädikatenlogik
   - Naive Mengenlehre
   - Relationen und Funktionen

2. Diskrete Strukturen
   - Algebraische Strukturen
   - Bäume und Graphen
   - Arithmetik

Heutige Vorlesung

- Eigenschaften von kommutativen Gruppen
- Definition Körper
- Grundlegende Eigenschaften von Körpern

Bitte Fragen direkt stellen!

Algebraische Strukturen — Kommutative Gruppen

Definition (§10.7 kommutative Gruppe)

Eine algebraische Struktur $(M, \oplus, \cdot^*, e)$ des Typs $(0, 1, 1, 1)$ ist eine kommutative (oder: Abelsche) Gruppe, gdw.

- $\oplus$ kommutativ und assoziativ ist,
  $x \oplus y = y \oplus x$ für alle $x, y \in M$ und
  $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ für alle $x, y, z \in M$
- $e \oplus x = x$ für alle $x \in M$ und (neutrales Element)
- $x \oplus x^* = e$ für alle $x \in M$. (Inverse)

Beispiel (1/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\sim_m \subseteq \mathbb{Z} \times \mathbb{Z}$ durch ('$|$' steht für 'teilt')

$$\sim_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid m \mid (x - y)\}$$

Beispiel (1/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\sim_m \subseteq \mathbb{Z} \times \mathbb{Z}$ durch ('|' steht für 'teilt')

$$\sim_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid m \mid (x - y)\}$$

- $\sim_m$ ist Äquivalenzrelation (reflexiv, symmetrisch, transitiv)
  - reflexiv: $x \sim_m x$ für alle $x \in \mathbb{Z}$, denn $m \mid 0$

Beispiel (1/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\sim_m \subseteq \mathbb{Z} \times \mathbb{Z}$ durch ('$|$' steht für 'teilt')

$$\sim_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid m \mid (x - y)\}$$

- $\sim_m$ ist Äquivalenzrelation (reflexiv, symmetrisch, transitiv)
  - reflexiv: $x \sim_m x$ für alle $x \in \mathbb{Z}$, denn $m \mid 0$
  - symmetrisch: Sei $x \sim_m y$. Dann $m \mid (x - y)$ also existiert $k \in \mathbb{Z}$, so dass $m \cdot k = x - y$. Dann ist $m \cdot (-k) = -(m \cdot k) = -(x - y) = y - x$. Also $y \sim_m x$

Beispiel (1/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\sim_m \subseteq \mathbb{Z} \times \mathbb{Z}$ durch ('$|$' steht für 'teilt')

$$\sim_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid m \mid (x - y)\}$$

- $\sim_m$ ist Äquivalenzrelation (reflexiv, symmetrisch, transitiv)
  - reflexiv: $x \sim_m x$ für alle $x \in \mathbb{Z}$, denn $m \mid 0$
  - symmetrisch: Sei $x \sim_m y$. Dann $m \mid (x - y)$ also existiert $k \in \mathbb{Z}$, so dass $m \cdot k = x - y$. Dann ist $m \cdot (-k) = -(m \cdot k) = -(x - y) = y - x$. Also $y \sim_m x$
  - transitiv: Seien $x \sim_m y$ und $y \sim_m z$. Dann gelten $m \mid (x - y)$ und $m \mid (y - z)$ und es existieren $k, n \in \mathbb{Z}$, so dass $m \cdot k = x - y$ und $m \cdot n = y - z$. Also

$$\begin{aligned} m \cdot (k + n) &= (m \cdot k) + (m \cdot n) = (x - y) + (y - z) \\ &= x - z \end{aligned}$$

  und damit $x \sim_m z$

Beispiel (2/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Sei $\mathbb{Z}_m = (\mathbb{Z}/\sim_m) = \{[x]_{\sim_m} \mid x \in \mathbb{Z}\}$ (Restklassen)
- Wir definieren $+_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch $[x] +_m [y] = [x + y]$ für alle $x, y \in \mathbb{Z}$

Beispiel (2/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Sei $\mathbb{Z}_m = (\mathbb{Z}/\sim_m) = \{[x]_{\sim_m} \mid x \in \mathbb{Z}\}$ (Restklassen)
- Wir definieren $+_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch $[x] +_m [y] = [x + y]$ für alle $x, y \in \mathbb{Z}$
- Repräsentantenunabhängigkeit: Seien $x \sim_m y$ und $u \sim_m v$.
  Z.zg. $x + u \sim_m y + v$. Es gelten $m \mid (x - y)$ und $m \mid (u - v)$ also existieren $k, n \in \mathbb{Z}$, so dass $m \cdot k = x - y$ und $m \cdot n = u - v$.

Beispiel (2/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Sei $\mathbb{Z}_m = (\mathbb{Z}/\sim_m) = \{[x]_{\sim_m} \mid x \in \mathbb{Z}\}$ (Restklassen)
- Wir definieren $+_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch $[x] +_m [y] = [x + y]$ für alle $x, y \in \mathbb{Z}$
- Repräsentantenunabhängigkeit: Seien $x \sim_m y$ und $u \sim_m v$.
  Z.zg. $x + u \sim_m y + v$. Es gelten $m \mid (x - y)$ und $m \mid (u - v)$ also existieren $k, n \in \mathbb{Z}$, so dass $m \cdot k = x - y$ und $m \cdot n = u - v$. Also

$$\begin{aligned} m \cdot (k + n) &= (m \cdot k) + (m \cdot n) = (x - y) + (u - v) \\ &= (x + u) - (y + v) \end{aligned}$$

  und damit $x + u \sim_m y + v$

Beispiel (3/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ ist eine kommutative Gruppe

Beispiel (3/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ ist eine kommutative Gruppe
- kommutativ: $[x] +_m [y] = [x + y] = [y + x] = [y] +_m [x]$ für alle $x, y \in \mathbb{Z}$

Beispiel (3/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ ist eine kommutative Gruppe
- kommutativ: $[x] +_m [y] = [x + y] = [y + x] = [y] +_m [x]$ für alle $x, y \in \mathbb{Z}$
- assoziativ: für alle $x, y, z \in \mathbb{Z}$

$$\begin{aligned}[x] +_m ([y] +_m [z]) &= [x] +_m [y + z] = [x + y + z] \\ &= [x + y] +_m [z] = ([x] +_m [y]) +_m [z]\end{aligned}$$

Beispiel (3/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ ist eine kommutative Gruppe
- kommutativ: $[x] +_m [y] = [x + y] = [y + x] = [y] +_m [x]$ für alle $x, y \in \mathbb{Z}$
- assoziativ: für alle $x, y, z \in \mathbb{Z}$

$$\begin{aligned}[x] +_m ([y] +_m [z]) &= [x] +_m [y + z] = [x + y + z] \\ &= [x + y] +_m [z] = ([x] +_m [y]) +_m [z]\end{aligned}$$

- neutrales Element: $[0] +_m [x] = [0 + x] = [x]$ für alle $x \in \mathbb{Z}$

Beispiel (3/3)

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ ist eine kommutative Gruppe
- kommutativ: $[x] +_m [y] = [x + y] = [y + x] = [y] +_m [x]$ für alle $x, y \in \mathbb{Z}$
- assoziativ: für alle $x, y, z \in \mathbb{Z}$

$$\begin{aligned}[x] +_m ([y] +_m [z]) &= [x] +_m [y + z] = [x + y + z] \\ &= [x + y] +_m [z] = ([x] +_m [y]) +_m [z]\end{aligned}$$

- neutrales Element: $[0] +_m [x] = [0 + x] = [x]$ für alle $x \in \mathbb{Z}$
- Inverse: für alle $x \in \mathbb{Z}$ gilt $[x] +_m [-x] = [x - x] = [0]$

§11.1 Theorem

Sei $(M, \oplus, \cdot^*, e)$ eine kommutative Gruppe und $x, y \in M$. Dann existiert genau ein $z \in M$, so dass $x \oplus z = y$.

§11.1 Theorem

Sei $(M, \oplus, \cdot^*, e)$ eine kommutative Gruppe und $x, y \in M$. Dann existiert genau ein $z \in M$, so dass $x \oplus z = y$.

Beweis (direkt).

Seien $x, y \in M$ beliebig. Wir wählen $z = x^* \oplus y$. Dann gilt offenbar

$$x \oplus z = x \oplus (x^* \oplus y) = (x \oplus x^*) \oplus y = e \oplus y = y \ ,$$

womit ein geeignetes z existiert.

§11.1 Theorem

Sei $(M, \oplus, \cdot^*, e)$ eine kommutative Gruppe und $x, y \in M$. Dann existiert genau ein $z \in M$, so dass $x \oplus z = y$.

Beweis (direkt).

Seien $x, y \in M$ beliebig. Wir wählen $z = x^* \oplus y$. Dann gilt offenbar

$$x \oplus z = x \oplus (x^* \oplus y) = (x \oplus x^*) \oplus y = e \oplus y = y \ ,$$

womit ein geeignetes z existiert. Sei $m \in M$, so dass $x \oplus m = y$.
Z.zg. $m = x^* \oplus y$.

$$m = e \oplus m = \underbrace{(x \oplus x^*)}_{e} \oplus m = (x^* \oplus x) \oplus m$$

$$= x^* \oplus \underbrace{(x \oplus m)}_{y} = x^* \oplus y$$

□

§11.2 Konsequenzen

- Gleichungen $x \oplus m = y$ lassen sich in der kommutativen Gruppe $(M, \oplus, (-\cdot), e)$ lösen
- wir dürfen kürzen: $m \oplus x = m \oplus y$ impliziert $x = y$

§11.3 Definition (Untergruppe)

Sei $(M, \odot, \cdot^{-1}, i)$ eine kommutative Gruppe und $U \subseteq M$.
Dann bildet U eine (kommutative) Untergruppe, gdw.

- $i \in U$,
- $u \odot v \in U$ für alle $u, v \in U$ und
- $u^{-1} \in U$ für alle $u \in U$.

§11.3 Definition (Untergruppe)

Sei $(M, \odot, \cdot^{-1}, i)$ eine kommutative Gruppe und $U \subseteq M$.
Dann bildet U eine (kommutative) Untergruppe, gdw.

- $i \in U$,
- $u \odot v \in U$ für alle $u, v \in U$ und
- $u^{-1} \in U$ für alle $u \in U$.

Beispiele

- M bildet eine Untergruppe der kommutativen Gruppe $(M, \odot, \cdot^{-1}, i)$
- $\mathbb{N}$ bildet keine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$
  (denn $2 \in \mathbb{N}$, aber für das Inverse -2 gilt $-2 \notin \mathbb{N}$)

Notiz:

- Menge U bildet Untergruppe gdw.
  man Menge U nicht mit den Operationen verlassen kann

§11.4 Theorem

Sei $(M, \odot, \cdot^{-1}, i)$ eine kommutative Gruppe.
Dann bildet $\{i\}$ eine Untergruppe.

Notiz:

- Menge U bildet Untergruppe gdw.
  man Menge U nicht mit den Operationen verlassen kann

§11.4 Theorem

Sei $(M, \odot, \cdot^{-1}, i)$ eine kommutative Gruppe.
Dann bildet $\{i\}$ eine Untergruppe.

Beweis (direkt).

- neutrales Element (Konstante): $i \in \{i\}$

Notiz:

- Menge U bildet Untergruppe gdw.
  man Menge U nicht mit den Operationen verlassen kann

§11.4 Theorem

Sei $(M, \odot, \cdot^{-1}, i)$ eine kommutative Gruppe.
Dann bildet $\{i\}$ eine Untergruppe.

Beweis (direkt).

- neutrales Element (Konstante): $i \in \{i\}$
- binäre Operation: $i \odot i = i \in \{i\}$

Notiz:

- Menge U bildet Untergruppe gdw.
  man Menge U nicht mit den Operationen verlassen kann

§11.4 Theorem

Sei $(M, \odot, \cdot^{-1}, i)$ eine kommutative Gruppe.
Dann bildet $\{i\}$ eine Untergruppe.

Beweis (direkt).

- neutrales Element (Konstante): $i \in \{i\}$
- binäre Operation: $i \odot i = i \in \{i\}$
- Inverse (unäre Operation): Es gilt $i \odot i^* = i \odot i$.
  Nach Kürzen bleibt $i^* = i \in \{i\}$. □

Beispiele

- $\mathbb{Z}$ bildet eine Untergruppe von $(\mathbb{Q}, +, (-\cdot), 0)$
- $\mathbb{Q}$ bildet eine Untergruppe von $(\mathbb{R}, +, (-\cdot), 0)$
- $\mathbb{Q} \setminus \{0\}$ bildet eine Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$

Beispiele

- $\mathbb{Z}$ bildet eine Untergruppe von $(\mathbb{Q}, +, (-\cdot), 0)$
- $\mathbb{Q}$ bildet eine Untergruppe von $(\mathbb{R}, +, (-\cdot), 0)$
- $\mathbb{Q} \setminus \{0\}$ bildet eine Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$

Notiz:

- Untergruppe = Unterstruktur einer Gruppe $(M, \odot, \cdot^{-1}, i)$

§11.5 Beobachtung

In der total geordneten Menge $(\mathbb{N}, \leq)$ existiert für jede nichtleere Teilmenge $N \subseteq \mathbb{N}$ das kleinste Element von N.

§11.5 Beobachtung

In der total geordneten Menge $(\mathbb{N}, \leq)$ existiert für jede nichtleere Teilmenge $N \subseteq \mathbb{N}$ das kleinste Element von N.

Beweis (direkt).

1. $i \leftarrow 0$ (setze i auf 0)
2. falls $i \in N$, liefere i (Element gefunden)
3. sonst $i \leftarrow i + 1$ und zu 2 (probiere nächste Zahl)

Terminiert mit $i \in N$ und für alle $n \in \mathbb{N}$ mit $n < i$ gilt $n \notin N$. Also $i \leq n$ für alle $n \in N$, womit i das kleinste Element von N ist. □

§11.6 Theorem

Sei $n \in \mathbb{Z}$. Dann bildet $n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$.

§11.6 Theorem

Sei $n \in \mathbb{Z}$. Dann bildet $n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$.

Beweis (direkt).

- $0 \in n\mathbb{Z}$, da $n \cdot 0 = 0$
- $(n \cdot x) + (n \cdot y) = n \cdot (x + y) \in n\mathbb{Z}$ für alle $x, y \in \mathbb{Z}$
- $-(n \cdot x) = n \cdot (-x) \in n\mathbb{Z}$ für alle $x \in \mathbb{Z}$

Also bildet $n\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$. □

§11.7 Theorem

Sei $U \subseteq \mathbb{Z}$, so dass U eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$ bildet.
Dann existiert $n \in \mathbb{Z}$, so dass $U = n\mathbb{Z}$.

§11.7 Theorem

Sei $U \subseteq \mathbb{Z}$, so dass U eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$ bildet.
Dann existiert $n \in \mathbb{Z}$, so dass $U = n\mathbb{Z}$.

Beweis (direkt und Fallunterscheidung; 1/2).

- Sei $U = \{0\}$. Dann ist $U = 0\mathbb{Z}$.

§11.7 Theorem

Sei $U \subseteq \mathbb{Z}$, so dass U eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$ bildet.
Dann existiert $n \in \mathbb{Z}$, so dass $U = n\mathbb{Z}$.

Beweis (direkt und Fallunterscheidung; 1/2).

- Sei $U = \{0\}$. Dann ist $U = 0\mathbb{Z}$.
- Sei $U \neq \{0\}$. Da $0 \in U$, folgt $V = U \setminus \{0\} \neq \emptyset$. Weiterhin gilt auch $V \cap \mathbb{N} \neq \emptyset$, denn für jedes $v \in V$ mit $v < 0$ gilt auch $-v \in V$. Also existiert gemäß §11.4 ein kleinstes Element n von $V \cap \mathbb{N}$.

§11.7 Theorem

Sei $U \subseteq \mathbb{Z}$, so dass U eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$ bildet.
Dann existiert $n \in \mathbb{Z}$, so dass $U = n\mathbb{Z}$.

Beweis (direkt und Fallunterscheidung; 1/2).

- Sei $U = \{0\}$. Dann ist $U = 0\mathbb{Z}$.
- Sei $U \neq \{0\}$. Da $0 \in U$, folgt $V = U \setminus \{0\} \neq \emptyset$. Weiterhin gilt auch $V \cap \mathbb{N} \neq \emptyset$, denn für jedes $v \in V$ mit $v < 0$ gilt auch $-v \in V$. Also existiert gemäß §11.4 ein kleinstes Element n von $V \cap \mathbb{N}$. Z.zg. $U = n\mathbb{Z}$.

§11.7 Theorem

Sei $U \subseteq \mathbb{Z}$, so dass U eine Untergruppe von $(\mathbb{Z}, +, (-\cdot), 0)$ bildet.
Dann existiert $n \in \mathbb{Z}$, so dass $U = n\mathbb{Z}$.

Beweis (direkt und Fallunterscheidung; 1/2).

- Sei $U = \{0\}$. Dann ist $U = 0\mathbb{Z}$.
- Sei $U \neq \{0\}$. Da $0 \in U$, folgt $V = U \setminus \{0\} \neq \emptyset$. Weiterhin gilt auch $V \cap \mathbb{N} \neq \emptyset$, denn für jedes $v \in V$ mit $v < 0$ gilt auch $-v \in V$. Also existiert gemäß §11.4 ein kleinstes Element n von $V \cap \mathbb{N}$. Z.zg. $U = n\mathbb{Z}$.

  ($\supseteq$) Sei $n \cdot x \in n\mathbb{Z}$. Falls $x = 0$, dann ist $n \cdot x = 0 \in U$. Zunächst

  $$|n \cdot x| = n \cdot |x| = \underbrace{n + \cdots + n}_{|x| \text{ mal}} \in U$$

  denn $n \in V$, $V \subseteq U$ und U bildet Untergruppe. Damit sind $n \cdot x$ und $-(n \cdot x)$ Elemente von U.

Beweis (direkt und Fallunterscheidung; 2/2).

Per Fallunterscheidung:

- Sei $U \neq \{0\}$. Z.zg. $U = n\mathbb{Z}$.
  - ($\subseteq$) Sei $u \in U$. Falls $u = 0$, dann gilt $u \in n\mathbb{Z}$.

Beweis (direkt und Fallunterscheidung; 2/2).

Per Fallunterscheidung:

- Sei $U \neq \{0\}$. Z.zg. $U = n\mathbb{Z}$.
  - ($\subseteq$) Sei $u \in U$. Falls $u = 0$, dann gilt $u \in n\mathbb{Z}$. Sei nun $u \neq 0$. Wir teilen nun u durch n mit Rest. Sei also

$$u = n \cdot x + r \qquad \text{mit} \quad x \in \mathbb{Z},\ 0 \leq r < n$$

Beweis (direkt und Fallunterscheidung; 2/2).

Per Fallunterscheidung:

- Sei $U \neq \{0\}$. Z.zg. $U = n\mathbb{Z}$.
  - ($\subseteq$) Sei $u \in U$. Falls $u = 0$, dann gilt $u \in n\mathbb{Z}$. Sei nun $u \neq 0$. Wir teilen nun u durch n mit Rest. Sei also

$$u = n \cdot x + r \qquad \text{mit} \quad x \in \mathbb{Z},\ 0 \leq r < n$$

Offensichtlich ist $n \cdot x \in n\mathbb{Z} \subseteq U$. Zusammen mit $u \in U$ haben wir $r = u - (n \cdot x) \in U$. Da aber $r \in U \cap \mathbb{N}$ mit $r < n$ und n das kleinste Element von $V \cap \mathbb{N}$ ist, muss $r = 0$ gelten. Also ist $u = n \cdot x$ und ist damit in $n\mathbb{Z}$. □

§11.8 Definition (Körper)

Eine algebraische Struktur $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ des Typs $(0, 2, 2, 2)$ ist ein Körper, gdw.

- $(M, \oplus, (-\cdot), e)$ eine kommutative Gruppe ist,
- $M \setminus \{e\}$ bildet eine Unterstruktur von $(M, \odot, \cdot^{-1}, i)$, die eine kommutative Gruppe ist, und
- $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ für alle $x, y, z \in M$. (Distributivität)

§11.8 Definition (Körper)

Eine algebraische Struktur $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ des Typs $(0, 2, 2, 2)$ ist ein Körper, gdw.

- $(M, \oplus, (-\cdot), e)$ eine kommutative Gruppe ist,
- $M \setminus \{e\}$ bildet eine Unterstruktur von $(M, \odot, \cdot^{-1}, i)$, die eine kommutative Gruppe ist, und
- $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ für alle $x, y, z \in M$. (Distributivität)

Notizen:

- Körper = 2 distributiv verbundene kommutative Gruppen
- mult. Inverses e^{-1} von e üblicherweise undefiniert; wir setzen $e^{-1} = e$
- $(M, \oplus, (-\cdot), e)$ = additive kommutative Gruppe
- $(M \setminus \{e\}, \odot, \cdot^{-1}, i)$ = multiplikative kommutative Gruppe
- nur $\odot$ distributiv über $\oplus$ (wie in der Arithmetik)

Algebraische Strukturen — Körper

Beispiele

- $(\mathbb{Q}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist ein Körper
- $(\mathbb{R}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist ein Körper
- $(\mathbb{Z}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist kein Körper
  denn $(\mathbb{Z} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$ ist keine kommutative Gruppe

Beispiele

- $(\mathbb{Q}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist ein Körper
- $(\mathbb{R}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist ein Körper
- $(\mathbb{Z}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist kein Körper
  denn $(\mathbb{Z} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$ ist keine kommutative Gruppe

§11.9 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Dann gilt $e \odot x = e$ für alle $x \in M$.

Beispiele

- $(\mathbb{Q}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist ein Körper
- $(\mathbb{R}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist ein Körper
- $(\mathbb{Z}, +, \cdot, (-\cdot), \cdot^{-1}, 0, 1)$ ist kein Körper
  denn $(\mathbb{Z} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$ ist keine kommutative Gruppe

§11.9 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Dann gilt $e \odot x = e$ für alle $x \in M$.

Beweis (direkt).

$$\begin{aligned}(e \odot x) \oplus e = e \odot x = x \odot e = x \odot (e \oplus e)\\ = (x \odot e) \oplus (x \odot e) = (e \odot x) \oplus (e \odot x)\end{aligned}$$

Da $(M, \oplus, (-\cdot), e)$ eine kommutative Gruppe ist, können wir "kürzen" ($e \odot x$ subtrahieren; siehe §11.6) und erhalten $e = e \odot x$. □

Beispiel

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch $[x] \cdot_m [y] = [x \cdot y]$ für alle $x, y \in \mathbb{Z}$

Beispiel

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch $[x] \cdot_m [y] = [x \cdot y]$ für alle $x, y \in \mathbb{Z}$
- Repräsentantenunabhängigkeit: Seien $x \sim_m y$ und $u \sim_m v$.
  Z.zg. $x \cdot u \sim_m y \cdot v$. Es gelten $m \mid (x - y)$ und $m \mid (u - v)$ also existieren $k, n \in \mathbb{Z}$, so dass $m \cdot k = x - y$ und $m \cdot n = u - v$.

Beispiel

Sei $m \in \mathbb{N}$ mit $m \geq 1$.

- Wir definieren $\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch $[x] \cdot_m [y] = [x \cdot y]$ für alle $x, y \in \mathbb{Z}$
- Repräsentantenunabhängigkeit: Seien $x \sim_m y$ und $u \sim_m v$.
  Z.zg. $x \cdot u \sim_m y \cdot v$. Es gelten $m \mid (x - y)$ und $m \mid (u - v)$ also existieren $k, n \in \mathbb{Z}$, so dass $m \cdot k = x - y$ und $m \cdot n = u - v$. Also

$$\begin{aligned} & (x \cdot u) - (y \cdot v) \\ = \; & (x \cdot u) \underbrace{- (x \cdot v) + (x \cdot v)}_{=0} - (y \cdot v) \\ = \; & x \cdot (u - v) + (x - y) \cdot v \\ = \; & x \cdot m \cdot n + m \cdot k \cdot v = m \cdot \big((x \cdot n) + (k \cdot v)\big) \end{aligned}$$

  und damit $x \cdot u \sim_m y \cdot v$

§11.10 Theorem

Sei $m \in \mathbb{N}$ eine Primzahl. Dann ist $(\mathbb{Z}_m, +_m, \cdot_m, (-\cdot), \cdot^{-1}, [0], [1])$ ein Körper.

§11.10 Theorem

Sei $m \in \mathbb{N}$ eine Primzahl. Dann ist $(\mathbb{Z}_m, +_m, \cdot_m, (-\cdot), \cdot^{-1}, [0], [1])$ ein Körper.

Beweis (direkt; 1/2).

- Wir wissen, dass $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ eine kommutative Gruppe ist.

§11.10 Theorem

Sei $m \in \mathbb{N}$ eine Primzahl. Dann ist $(\mathbb{Z}_m, +_m, \cdot_m, (-\cdot), \cdot^{-1}, [0], [1])$ ein Körper.

Beweis (direkt; 1/2).

- Wir wissen, dass $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ eine kommutative Gruppe ist.
- Offensichtlich gilt für alle $x, y, z \in \mathbb{Z}$

$$\begin{aligned}[x] \cdot_m ([y] +_m [z]) &= [x] \cdot_m [y + z] = [x \cdot (y + z)] \\ &= [(x \cdot y) + (x \cdot z)] = [x \cdot y] +_m [x \cdot z] \\ &= ([x] \cdot_m [y]) +_m ([x] \cdot_m [z])\end{aligned}$$

§11.10 Theorem

Sei $m \in \mathbb{N}$ eine Primzahl. Dann ist $(\mathbb{Z}_m, +_m, \cdot_m, (-\cdot), \cdot^{-1}, [0], [1])$ ein Körper.

Beweis (direkt; 1/2).

- Wir wissen, dass $(\mathbb{Z}_m, +_m, (-\cdot), [0])$ eine kommutative Gruppe ist.
- Offensichtlich gilt für alle $x, y, z \in \mathbb{Z}$

$$\begin{aligned}[x] \cdot_m ([y] +_m [z]) &= [x] \cdot_m [y + z] = [x \cdot (y + z)] \\ &= [(x \cdot y) + (x \cdot z)] = [x \cdot y] +_m [x \cdot z] \\ &= ([x] \cdot_m [y]) +_m ([x] \cdot_m [z])\end{aligned}$$

- Z.zg. $(\mathbb{Z}_m \setminus \{[0]\}, \cdot_m, \cdot^{-1}, [1])$ ist eine kommutative Gruppe
  - kommutativ: $[x] \cdot_m [y] = [x \cdot y] = [y \cdot x] = [y] \cdot_m [x]$ für alle $x, y \in \mathbb{Z}$
  - assoziativ: für alle $x, y, z \in \mathbb{Z}$

$$\begin{aligned}[x] \cdot_m ([y] \cdot_m [z]) &= [x] \cdot_m [y \cdot z] = [x \cdot y \cdot z] \\ &= [x \cdot y] \cdot_m [z] = ([x] \cdot_m [y]) \cdot_m [z]\end{aligned}$$

Beweis (direkt; 2/2).

- Z.zg. $(\mathbb{Z}_m \setminus \{[0]\}, \cdot_m, \cdot^{-1}, [1])$ ist eine kommutative Gruppe
  - neutrales Element: $[1] \cdot_m [x] = [1 \cdot x] = [x]$ für alle $x \in \mathbb{Z}$

Beweis (direkt; 2/2).

- Z.zg. $(\mathbb{Z}_m \setminus \{[0]\}, \cdot_m, \cdot^{-1}, [1])$ ist eine kommutative Gruppe
  - neutrales Element: $[1] \cdot_m [x] = [1 \cdot x] = [x]$ für alle $x \in \mathbb{Z}$
  - Inverse: Sei $n < m$ mit $n \neq 0$. Wir werden noch beweisen (Euklidischer Algorithmus), dass $x, y \in \mathbb{Z}$ existieren, so dass $\mathrm{ggT}(n, m) = nx + my$. Da m prim ist und $n < m$, gilt $\mathrm{ggT}(n, m) = 1 = nx + my$. Des Weiteren gilt für jedes $k \in \mathbb{Z}$

$$nx + my = nx + \underbrace{nkm - nkm}_{0} + my = n(x + km) + m(y - kn)$$

Beweis (direkt; 2/2).

- Z.zg. $(\mathbb{Z}_m \setminus \{[0]\}, \cdot_m, \cdot^{-1}, [1])$ ist eine kommutative Gruppe
  - neutrales Element: $[1] \cdot_m [x] = [1 \cdot x] = [x]$ für alle $x \in \mathbb{Z}$
  - Inverse: Sei $n < m$ mit $n \neq 0$. Wir werden noch beweisen (Euklidischer Algorithmus), dass $x, y \in \mathbb{Z}$ existieren, so dass $\mathrm{ggT}(n, m) = nx + my$. Da m prim ist und $n < m$, gilt $\mathrm{ggT}(n, m) = 1 = nx + my$. Des Weiteren gilt für jedes $k \in \mathbb{Z}$

$$nx + my = nx + \underbrace{nkm - nkm}_{0} + my = n(x + km) + m(y - kn)$$

Wähle k, so dass $z = x + km \in \{0, \ldots, m-1\}$. Dann gilt

$$1 = nx + my = nz + m(y - kn)$$

womit $1 - nz = m(y - kn)$ und damit $1 \sim_m nz$ also $[1] = [nz]$. Es folgt $[n] \cdot_m [z] = [nz] = [1]$. □

§11.11 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper.
Für beliebige $x, y \in M$ mit $x \odot y = e$ gilt $e \in \{x, y\}$.

§11.11 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper.
Für beliebige $x, y \in M$ mit $x \odot y = e$ gilt $e \in \{x, y\}$.

Beweis (direkt).

O.B.d.A. sei $x \neq e$. Dann gilt

$$y = i \odot y = \underbrace{(x \odot x^{-1})}_{i} \odot y = (x^{-1} \odot x) \odot y$$
$$= x^{-1} \odot \underbrace{(x \odot y)}_{e} = x^{-1} \odot e = e$$

□

§11.12 Definition (Polynom)

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Jede Wahl $a_0, \ldots, a_n \in M$ mit $a_n \neq e$ definiert ein Polynom $p = (a_0, \ldots, a_n)$ vom Grad n. Dieses Polynom p definiert eine Funktion $f_p \colon M \to M$ für alle $x \in M$ durch

$$f_p(x) = a_0 \oplus (a_1 \odot x) \oplus (a_2 \odot x \odot x) \oplus \cdots \oplus (a_n \odot \underbrace{x \odot \cdots \odot x}_{n \text{ mal}})$$

§11.12 Definition (Polynom)

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Jede Wahl $a_0, \ldots, a_n \in M$ mit $a_n \neq e$ definiert ein Polynom $p = (a_0, \ldots, a_n)$ vom Grad n. Dieses Polynom p definiert eine Funktion $f_p \colon M \to M$ für alle $x \in M$ durch

$$f_p(x) = a_0 \oplus (a_1 \odot x) \oplus (a_2 \odot x \odot x) \oplus \cdots \oplus (a_n \odot \underbrace{x \odot \cdots \odot x}_{n \text{ mal}})$$

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

§11.12 Definition (Polynom)

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Jede Wahl $a_0, \ldots, a_n \in M$ mit $a_n \neq e$ definiert ein Polynom $p = (a_0, \ldots, a_n)$ vom Grad n. Dieses Polynom p definiert eine Funktion $f_p \colon M \to M$ für alle $x \in M$ durch

$$f_p(x) = a_0 \oplus (a_1 \odot x) \oplus (a_2 \odot x \odot x) \oplus \cdots \oplus (a_n \odot \underbrace{x \odot \cdots \odot x}_{n \text{ mal}})$$

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

§11.12 Definition (Polynom)

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Jede Wahl $a_0, \ldots, a_n \in M$ mit $a_n \neq e$ definiert ein Polynom $p = (a_0, \ldots, a_n)$ vom Grad n. Dieses Polynom p definiert eine Funktion $f_p \colon M \to M$ für alle $x \in M$ durch

$$f_p(x) = a_0 \oplus (a_1 \odot x) \oplus (a_2 \odot x \odot x) \oplus \cdots \oplus (a_n \odot \underbrace{x \odot \cdots \odot x}_{n \text{ mal}})$$

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

Beispiel

Im Körper $(\mathbb{Z}_5, +_5, \cdot_5, (-\cdot), \cdot^{-1}, [0], [1])$ ist $p = ([2], [4], [1])$ ein Polynom vom Grad 2. Es gilt

$$f_p([2]) = [2] +_5 ([4] \cdot_5 [2]) +_5 ([2] \cdot_5 [2]) = [2] +_5 [3] +_5 [4] = [4]$$

§11.13 Definition (Nullstelle)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin sei p ein Polynom.
Ein Element $x \in M$ ist Nullstelle von p gdw. $f_p(x) = e$.

§11.13 Definition (Nullstelle)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin sei p ein Polynom.
Ein Element $x \in M$ ist Nullstelle von p gdw. $f_p(x) = e$.

Beispiel

Nullstellen des Polynoms $p = ([2], [4], [1])$ in $(\mathbb{Z}_5, +_5, \cdot_5, (-\cdot), \cdot^{-1}, [0], [1])$

- $f_p([0]) = [2]$
- $f_p([2]) = [4]$

§11.13 Definition (Nullstelle)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin sei p ein Polynom.
Ein Element $x \in M$ ist Nullstelle von p gdw. $f_p(x) = e$.

Beispiel

Nullstellen des Polynoms $p = ([2], [4], [1])$ in $(\mathbb{Z}_5, +_5, \cdot_5, (-\cdot), \cdot^{-1}, [0], [1])$

- $f_p([0]) = [2]$
- $f_p([1]) = [2] +_5 [4] +_5 [1] = [2]$
- $f_p([2]) = [4]$

§11.13 Definition (Nullstelle)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin sei p ein Polynom.
Ein Element $x \in M$ ist Nullstelle von p gdw. $f_p(x) = e$.

Beispiel

Nullstellen des Polynoms $p = ([2], [4], [1])$ in $(\mathbb{Z}_5, +_5, \cdot_5, (-\cdot), \cdot^{-1}, [0], [1])$

- $f_p([0]) = [2]$
- $f_p([1]) = [2] +_5 [4] +_5 [1] = [2]$
- $f_p([2]) = [4]$
- $f_p([3]) = [2] +_5 [2] +_5 [4] = [3]$

§11.13 Definition (Nullstelle)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin sei p ein Polynom.
Ein Element $x \in M$ ist Nullstelle von p gdw. $f_p(x) = e$.

Beispiel

Nullstellen des Polynoms $p = ([2], [4], [1])$ in $(\mathbb{Z}_5, +_5, \cdot_5, (-\cdot), \cdot^{-1}, [0], [1])$

- $f_p([0]) = [2]$
- $f_p([1]) = [2] +_5 [4] +_5 [1] = [2]$
- $f_p([2]) = [4]$
- $f_p([3]) = [2] +_5 [2] +_5 [4] = [3]$
- $f_p([4]) = [2] +_5 [1] +_5 [1] = [4]$

§11.14 Theorem (Horner-Schema)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Weiterhin sei $p = (a_0, \ldots, a_n)$ ein Polynom vom Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$f_p(x) = a_0 \oplus \Big(x \odot \Big(a_1 \oplus \big(x \odot \big(a_2 \oplus (x \odot \cdots (x \odot a_n) \cdots)\big)\big)\Big)\Big)$$

§11.14 Theorem (Horner-Schema)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Weiterhin sei $p = (a_0, \ldots, a_n)$ ein Polynom vom Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$f_p(x) = a_0 \oplus \Big(x \odot \Big(a_1 \oplus \big(x \odot \big(a_2 \oplus (x \odot \cdots (x \odot a_n) \cdots)\big)\big)\Big)\Big)$$

Beweis.

Einfaches Ausklammern □

§11.14 Theorem (Horner-Schema)

Seien $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper und $n \in \mathbb{N}$. Weiterhin sei $p = (a_0, \ldots, a_n)$ ein Polynom vom Grad $n \geq 0$. Dann gilt für alle $x \in M$

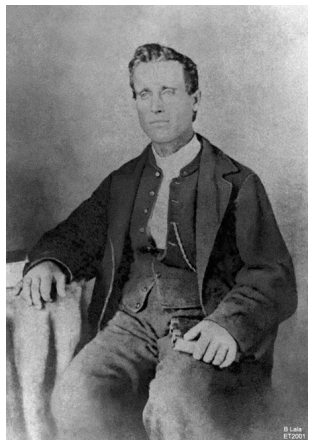
$$f_p(x) = a_0 \oplus \Big(x \odot \Big(a_1 \oplus \big(x \odot \big(a_2 \oplus (x \odot \cdots (x \odot a_n) \cdots)\big)\big)\Big)\Big)$$

Beweis.

Einfaches Ausklammern □

William George Horner (* 1786; † 1837)

- engl. Mathematiker
- Lösung algebraischer Gleichungen
- eigentlich bereits 500 Jahre vorher von Zhu Shijie entdeckt



§11.15 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin seien p, q Polynome mit $\text{grad}(q) \geq 0$. Dann existieren Polynome t und r, so dass für alle $x \in M$

$$f_p(x) = f_t(x) \odot f_q(x) \oplus f_r(x)$$

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

§11.15 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Weiterhin seien p, q Polynome mit $\text{grad}(q) \geq 0$. Dann existieren Polynome t und r, so dass für alle $x \in M$

$$f_p(x) = f_t(x) \odot f_q(x) \oplus f_r(x)$$

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

Beweis.

normale Polynomdivision; Training in der Übung □

§11.16 Definition (Galois-Körper)

Ein Körper $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ist endlich (oder ein Galois-Körper) gdw. M endlich ist

Évariste Galois (* 1811; † 1832)

- franz. Mathematiker
- löste als Jugendlicher ein 350 Jahre altes Problem
- verstarb leider bereits mit 20 in einem Duell

§11.17 Theorem (Moore 1893)

- Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Galois-Körper (endlicher Körper). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.

Eliakim Hastings Moore (* 1862; † 1932)

- amer. Mathematiker
- Vorreiter der abstrakten Algebra
- studierte Mathematik in Berlin

§11.17 Theorem (Moore 1893)

- Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Galois-Körper (endlicher Körper). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien $\mathcal{K}$ und $\mathcal{N}$ Galois-Körper mit gleich vielen Elementen. Dann sind $\mathcal{K}$ und $\mathcal{N}$ isomorph.

Eliakim Hastings Moore (* 1862; † 1932)

- amer. Mathematiker
- Vorreiter der abstrakten Algebra
- studierte Mathematik in Berlin

Notizen:

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Galois-Körper.

- für $p = |M|$ prim, ist $\mathcal{M}$ isomorph zu $(\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, 0, 1)$
- die weiteren Galois-Körper ergeben sich mit Hilfe von Polynomen (siehe Ausblick)

Notizen:

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Galois-Körper.

- für $p = |M|$ prim, ist $\mathcal{M}$ isomorph zu $(\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, 0, 1)$
- die weiteren Galois-Körper ergeben sich mit Hilfe von Polynomen (siehe Ausblick)
- $|M| \neq 6$ (kein Körper hat 6 Elemente)
- wichtig in der Kodierungstheorie und Kryptographie

Notizen:

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Galois-Körper.

- für $p = |M|$ prim, ist $\mathcal{M}$ isomorph zu $(\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, 0, 1)$
- die weiteren Galois-Körper ergeben sich mit Hilfe von Polynomen (siehe Ausblick)
- $|M| \neq 6$ (kein Körper hat 6 Elemente)
- wichtig in der Kodierungstheorie und Kryptographie

- wir zeigen noch den ersten Anstrich von §11.17

§11.18 Definition (Charakteristik)

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Die Charakteristik von $\mathcal{M}$ ist die kleinste Zahl $c \in \mathbb{N} \setminus \{0\}$, so dass

$$\underbrace{i \oplus \cdots \oplus i}_{c \text{ Summanden } i} = e \ .$$

Falls keine solche Zahl existiert, dann ist die Charakteristik 0.

§11.18 Definition (Charakteristik)

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein Körper. Die Charakteristik von $\mathcal{M}$ ist die kleinste Zahl $c \in \mathbb{N} \setminus \{0\}$, so dass

$$\underbrace{i \oplus \cdots \oplus i}_{c \text{ Summanden } i} = e \ .$$

Falls keine solche Zahl existiert, dann ist die Charakteristik 0.

Notiz:

- Wir schreiben $\underline{c}$ für das Element $\underbrace{i \oplus \cdots \oplus i}_{c \text{ Summanden } i}$

§11.19 Lemma

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper.
Die Charakteristik von $\mathcal{M}$ ist eine Primzahl.

Beweis (direkt; 1/2).

Da M endlich ist, existieren $m, n \in \mathbb{N}$ mit $m < n$, so dass

$$\underbrace{i \oplus \cdots \oplus i}_{m \text{ Summanden } i} = \underline{m} = \underline{n} = \underbrace{i \oplus \cdots \oplus i}_{n \text{ Summanden } i} .$$

§11.19 Lemma

Sei $\mathcal{M} = (M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper.
Die Charakteristik von $\mathcal{M}$ ist eine Primzahl.

Beweis (direkt; 1/2).

Da M endlich ist, existieren $m, n \in \mathbb{N}$ mit $m < n$, so dass

$$\underbrace{i \oplus \cdots \oplus i}_{m \text{ Summanden } i} = \underline{m} = \underline{n} = \underbrace{i \oplus \cdots \oplus i}_{n \text{ Summanden } i} .$$

Also gilt auch

$$\underline{m} \oplus \underbrace{(-i) \oplus \cdots \oplus (-i)}_{m \text{ Summanden } -i} = e = \underline{n} \oplus \underbrace{(-i) \oplus \cdots \oplus (-i)}_{m \text{ Summanden } -i} = \underline{(n-m)}$$

womit die Charakteristik nicht 0 ist.

Beweis (direkt; 2/2).

Sei $p \neq 0$ die Charakteristik und seien $m, n \in \mathbb{N}$, so dass $p = m \cdot n$. Dann ist

$$e = \underline{p} = \underline{(m \cdot n)} = \underline{m} \odot \underline{n} \ .$$

Beweis (direkt; 2/2).

Sei $p \neq 0$ die Charakteristik und seien $m, n \in \mathbb{N}$, so dass $p = m \cdot n$. Dann ist

$$e = \underline{p} = \underline{(m \cdot n)} = \underline{m} \odot \underline{n} \ .$$

Gemäß §11.11 gilt daher $e \in \{\underline{m}, \underline{n}\}$.

Beweis (direkt; 2/2).

Sei $p \neq 0$ die Charakteristik und seien $m, n \in \mathbb{N}$, so dass $p = m \cdot n$. Dann ist

$$e = \underline{p} = \underline{(m \cdot n)} = \underline{m} \odot \underline{n} \ .$$

Gemäß §11.11 gilt daher $e \in \{\underline{m}, \underline{n}\}$.
Da $m \leq p$ und $n \leq p$ muss $m = p$ oder $n = p$ gelten. Daraus folgt, dass p eine Primzahl ist. □

§11.20 Theorem

Jeder endliche Körper $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ der Charakteristik p enthält einen Unterkörper, der isomorph zu $\mathcal{Z}_p = (\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, [0], [1])$ ist.

Beweis (direkt).

Der Unterkörper wird von den Elementen $S = \{\underline{m} \mid 1 \leq m \leq p\}$ gebildet und der Isomorphismus $\varphi\colon S \to \mathbb{Z}_p$ ist durch $\varphi(\underline{m}) = [m]$ gegeben.

Die Nachweise der Unterstruktur und der Isomorphie sind einfache Übungen. □

§11.20 Theorem

Jeder endliche Körper $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ der Charakteristik p enthält einen Unterkörper, der isomorph zu $\mathcal{Z}_p = (\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, [0], [1])$ ist.

Beweis (direkt).

Der Unterkörper wird von den Elementen $S = \{\underline{m} \mid 1 \leq m \leq p\}$ gebildet und der Isomorphismus $\varphi\colon S \to \mathbb{Z}_p$ ist durch $\varphi(\underline{m}) = [m]$ gegeben.

Die Nachweise der Unterstruktur und der Isomorphie sind einfache Übungen. □

Notizen:

- Elemente von S nennen wir auch Skalare
- wir nutzen im Folgenden immer die Menge S für die Skalare

§11.21 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper und S die Menge der Skalare (siehe §11.20). Wenn $S \subseteq U \subseteq M$ eine additive Untergruppe bildet, dann ist

$$\equiv_U = \{(x, y) \in M \times M \mid x \oplus (-y) \in U\} \ ,$$

eine Äquivalenzrelation mit Äquivalenzklassen der Größe $|U|$.

§11.21 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper und S die Menge der Skalare (siehe §11.20). Wenn $S \subseteq U \subseteq M$ eine additive Untergruppe bildet, dann ist

$$\equiv_U = \{(x, y) \in M \times M \mid x \oplus (-y) \in U\} \ ,$$

eine Äquivalenzrelation mit Äquivalenzklassen der Größe $|U|$.

Beweis (direkt; 1/2).

Wir weisen zunächst die Eigenschaften einer Äquivalenzrelation nach.

- reflexiv: Sei $x \in M$. Dann ist $x \oplus (-x) = e \in U$ und damit gilt $x \equiv_U x$.

§11.21 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper und S die Menge der Skalare (siehe §11.20). Wenn $S \subseteq U \subseteq M$ eine additive Untergruppe bildet, dann ist

$$\equiv_U = \{(x, y) \in M \times M \mid x \oplus (-y) \in U\} \ ,$$

eine Äquivalenzrelation mit Äquivalenzklassen der Größe $|U|$.

Beweis (direkt; 1/2).

Wir weisen zunächst die Eigenschaften einer Äquivalenzrelation nach.

- reflexiv: Sei $x \in M$. Dann ist $x \oplus (-x) = e \in U$ und damit gilt $x \equiv_U x$.
- symmetrisch: Sei $x \equiv_U y$. Dann gilt $x \oplus (-y) \in U$. Also gilt $-(x \oplus (-y)) = y \oplus (-x) \in U$ und damit $y \equiv_U x$.

§11.21 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper und S die Menge der Skalare (siehe §11.20). Wenn $S \subseteq U \subseteq M$ eine additive Untergruppe bildet, dann ist

$$\equiv_U = \{(x, y) \in M \times M \mid x \oplus (-y) \in U\} \ ,$$

eine Äquivalenzrelation mit Äquivalenzklassen der Größe $|U|$.

Beweis (direkt; 1/2).

Wir weisen zunächst die Eigenschaften einer Äquivalenzrelation nach.

- reflexiv: Sei $x \in M$. Dann ist $x \oplus (-x) = e \in U$ und damit gilt $x \equiv_U x$.
- symmetrisch: Sei $x \equiv_U y$. Dann gilt $x \oplus (-y) \in U$. Also gilt $-(x \oplus (-y)) = y \oplus (-x) \in U$ und damit $y \equiv_U x$.
- transitiv: Seien $x \equiv_U y$ und $y \equiv_U z$. Also $x \oplus (-y) \in U$ und $y \oplus (-z) \in U$. Also gilt auch $x \oplus (-y) \oplus y \oplus (-z) = x \oplus (-z) \in U$ und damit $x \equiv_U z$.

Beweis (direkt; 2/2).

Sei $y \in M$. Die Äquivalenzklasse von y ist

$$[y] = \{x \in M \mid x \oplus (-y) \in U\} = \{u \oplus y \mid u \in U\}$$

Damit ist $|[y]| \leq |U|$ direkt klar.

Beweis (direkt; 2/2).

Sei $y \in M$. Die Äquivalenzklasse von y ist

$$[y] = \{x \in M \mid x \oplus (-y) \in U\} = \{u \oplus y \mid u \in U\}$$

Damit ist $|[y]| \leq |U|$ direkt klar. Angenommen $u \oplus y = u' \oplus y$ für $u, u' \in U$. Dann addieren wir $(-y)$ von rechts auf beiden Seiten und erhalten

$$u \oplus y \oplus (-y) = u = u' = u' \oplus y \oplus (-y)$$

womit $u = u'$ folgt. Also $|[y]| = |U|$. □

Wir betrachten immer die Äquivalenzrelation $\equiv_U$

§11.22 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper. Weiterhin bilde $S \subseteq U \subseteq M$ eine additive Untergruppe und es sei $x \in M \setminus U$. Für alle $s, s' \in S$:

1. $[s \odot x] \cap U \neq \emptyset$ genau dann, wenn $s = e$
2. $[s \odot x] \cap [s' \odot x] \neq \emptyset$ genau dann, wenn $s = s'$

Beweis (direkt und per Widerspruch).

Die Richtungen von rechts nach links sind trivial, da $e \in [e] \cap U$.

Wir betrachten immer die Äquivalenzrelation $\equiv_U$

§11.22 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper. Weiterhin bilde $S \subseteq U \subseteq M$ eine additive Untergruppe und es sei $x \in M \setminus U$. Für alle $s, s' \in S$:

1. $[s \odot x] \cap U \neq \emptyset$ genau dann, wenn $s = e$
2. $[s \odot x] \cap [s' \odot x] \neq \emptyset$ genau dann, wenn $s = s'$

Beweis (direkt und per Widerspruch).

Die Richtungen von rechts nach links sind trivial, da $e \in [e] \cap U$. Für 1 sei nun $(s \odot x) \oplus u \in U$ für ein $u \in U$ und $s \neq e$. Also $s \odot x \in U$ und sogar $x = s^{-1} \odot s \odot x = \underbrace{(s \odot x) \oplus \cdots \oplus (s \odot x)}_{s^{-1} \text{ Summanden}} \in U$, da $s^{-1} \in S$. Widerspruch.

Algebraische Strukturen — Körper

Wir betrachten immer die Äquivalenzrelation $\equiv_U$

§11.22 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper. Weiterhin bilde $S \subseteq U \subseteq M$ eine additive Untergruppe und es sei $x \in M \setminus U$. Für alle $s, s' \in S$:

1. $[s \odot x] \cap U \neq \emptyset$ genau dann, wenn $s = e$
2. $[s \odot x] \cap [s' \odot x] \neq \emptyset$ genau dann, wenn $s = s'$

Beweis (direkt und per Widerspruch).

Die Richtungen von rechts nach links sind trivial, da $e \in [e] \cap U$. Für 1 sei nun $(s \odot x) \oplus u \in U$ für ein $u \in U$ und $s \neq e$. Also $s \odot x \in U$ und sogar $x = s^{-1} \odot s \odot x = \underbrace{(s \odot x) \oplus \cdots \oplus (s \odot x)}_{s^{-1} \text{ Summanden}} \in U$, da $s^{-1} \in S$. Widerspruch.

Für 2 sei o.B.d.A. $(s \odot x) \oplus u = (s' \odot x) \oplus u'$ für $s < s'$ und $u, u' \in U$. Wir subtrahieren $(s \odot x)$ und erhalten $u = (s' \oplus (-s)) \odot x \oplus u'$ und damit $[(s' \oplus (-s)) \odot x] \cap U \neq \emptyset$. Mit 1 folgt $s' \oplus (-s) = e$ und damit $s' = s$. □

Wir betrachten immer die Äquivalenzrelation $\equiv_U$

§11.23 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper der Charakteristik p und $S \subseteq U \subseteq M$ eine additive Untergruppe und $x \in M \setminus U$. Dann bildet $V = \bigcup_{s \in S}[s \odot x]$ eine additive Untergruppe der Größe $|V| = p \cdot |U|$.

Beweis (direkt).

Wir zeigen zunächst die Untergruppeneigenschaften:

- $((s \odot x) \oplus u) \oplus ((s' \odot x) \oplus u') = ((s \oplus s') \odot x) \oplus u \oplus u' \in V$ für alle $s, s' \in S$ und $u, u' \in U$

Wir betrachten immer die Äquivalenzrelation $\equiv_U$

§11.23 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper der Charakteristik p und $S \subseteq U \subseteq M$ eine additive Untergruppe und $x \in M \setminus U$. Dann bildet $V = \bigcup_{s \in S}[s \odot x]$ eine additive Untergruppe der Größe $|V| = p \cdot |U|$.

Beweis (direkt).

Wir zeigen zunächst die Untergruppeneigenschaften:

- $\big((s \odot x) \oplus u\big) \oplus \big((s' \odot x) \oplus u'\big) = \big((s \oplus s') \odot x\big) \oplus u \oplus u' \in V$ für alle $s, s' \in S$ und $u, u' \in U$
- $-\big((s \odot x) \oplus u\big) = \big((-s) \odot x\big) \oplus (-u)$ für alle $s \in S$ und $u \in U$

Wir betrachten immer die Äquivalenzrelation $\equiv_U$

§11.23 Lemma

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper der Charakteristik p und $S \subseteq U \subseteq M$ eine additive Untergruppe und $x \in M \setminus U$. Dann bildet $V = \bigcup_{s \in S}[s \odot x]$ eine additive Untergruppe der Größe $|V| = p \cdot |U|$.

Beweis (direkt).

Wir zeigen zunächst die Untergruppeneigenschaften:

- $\big((s \odot x) \oplus u\big) \oplus \big((s' \odot x) \oplus u'\big) = \big((s \oplus s') \odot x\big) \oplus u \oplus u' \in V$ für alle $s, s' \in S$ und $u, u' \in U$
- $-\big((s \odot x) \oplus u\big) = \big((-s) \odot x\big) \oplus (-u)$ für alle $s \in S$ und $u \in U$
- $e \in [e] \subseteq V$

Gemäß §11.22 sind die Äquivalenzklassen disjunkt und §11.21 zeigt, dass jede Klasse die Größe $|U|$ hat. Da $|S| = p$ folgt $|V| = p \cdot |U|$. □

§11.24 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper der Charakteristik p. Dann existiert $n \in \mathbb{N}$, so dass $|M| = p^n$.

§11.24 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper der Charakteristik p. Dann existiert $n \in \mathbb{N}$, so dass $|M| = p^n$.

Beweis (direkt).

Gemäß §11.20 bildet S einen Unterkörper der Größe p. Sei $U = S$.
Falls $U \neq M$, dann existiert $x \in M \setminus U$ und wir wenden Lemma §11.23 an und erhalten eine Menge $U \subsetneq V$ der Größe p^2, die eine additive Untergruppe bildet.

§11.24 Theorem

Sei $(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i)$ ein endlicher Körper der Charakteristik p. Dann existiert $n \in \mathbb{N}$, so dass $|M| = p^n$.

Beweis (direkt).

Gemäß §11.20 bildet S einen Unterkörper der Größe p. Sei $U = S$. Falls $U \neq M$, dann existiert $x \in M \setminus U$ und wir wenden Lemma §11.23 an und erhalten eine Menge $U \subsetneq V$ der Größe p^2, die eine additive Untergruppe bildet. Danach setzen wir $U = V$ und wiederholen den Vorgang. Da M endlich ist, stoppt der Prozess und wir erhalten eine additive Untergruppe M der Größe p^{n+1}, wobei n die Anzahl der Anwendungen von Lemma §11.23 ist. □

Ausblick:

- Wie sehen die Körper der Größe p^n mit p prim aus?
- Wir betrachten Polynome über dem Körper $\mathcal{Z}_p$.
- Polynom r mit $\text{grad}(r) \geq 1$ ist irreduzibel gdw. $r \neq t \cdot q$ für alle Polynome t und q mit $\text{grad}(t) \geq 1$ und $\text{grad}(q) \geq 1$
  (d.h. nicht in nicht-konstante Polynome faktorisierbar)

Algebraische Strukturen — Körper

Ausblick:

- Wie sehen die Körper der Größe p^n mit p prim aus?
- Wir betrachten Polynome über dem Körper $\mathcal{Z}_p$.
- Polynom r mit $\text{grad}(r) \geq 1$ ist irreduzibel gdw. $r \neq t \cdot q$ für alle Polynome t und q mit $\text{grad}(t) \geq 1$ und $\text{grad}(q) \geq 1$ (d.h. nicht in nicht-konstante Polynome faktorisierbar)
- Wir wählen ein irreduzibles Polynom r mit $\text{grad}(r) = n$.
- Dann bilden die Polynome q mit $\text{grad}(q) < n$ einen Körper der Größe p^n, wobei wir Polynome wie erwartet addieren und multiplizieren, aber die Ergebnisse jeweils modulo r rechnen.

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

$\odot$	a	b	c	d	e
a	b	a	e	d	c
b	a	b	c	d	e
c	e	c	a	d	b
d	d	d	d	d	d
e	c	e	b	d	a

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

$\odot$	a	b	c	d	e
a	b	a	e	d	c
b	a	b	c	d	e
c	e	c	a	d	b
d	d	d	d	d	d
e	c	e	b	d	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

$\odot$	a	b	c	d	e
a	b	a	e	d	c
b	a	b	c	d	e
c	e	c	a	d	b
d	d	d	d	d	d
e	c	e	b	d	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

$\odot$	a	b	c	d	e
a	b	a	e	d	c
b	a	b	c	d	e
c	e	c	a	d	b
d	d	d	d	d	d
e	c	e	b	d	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	b	c	0	e
a	c	0	e	a	b
b	0	e	a	b	c
c	e	a	b	c	0
0	a	b	c	0	e
e	b	c	0	e	a

$\odot$	a	b	c	0	e
a	b	a	e	0	c
b	a	b	c	0	e
c	e	c	a	0	b
0	0	0	0	0	0
e	c	e	b	0	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	b	c	0	e
a	c	0	e	a	b
b	0	e	a	b	c
c	e	a	b	c	0
0	a	b	c	0	e
e	b	c	0	e	a

$\odot$	a	b	c	0	e
a	b	a	e	0	c
b	a	b	c	0	e
c	e	c	a	0	b
0	0	0	0	0	0
e	c	e	b	0	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	1	c	0	e
a	c	0	e	a	1
1	0	e	a	1	c
c	e	a	1	c	0
0	a	1	c	0	e
e	1	c	0	e	a

$\odot$	a	1	c	0	e
a	1	a	e	0	c
1	a	1	c	0	e
c	e	c	a	0	1
0	0	0	0	0	0
e	c	e	1	0	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	a	1	c	0	e
a	c	0	e	a	1
1	0	e	a	1	c
c	e	a	1	c	0
0	a	1	c	0	e
e	1	c	0	e	a

$\odot$	a	1	c	0	e
a	1	a	e	0	c
1	a	1	c	0	e
c	e	c	a	0	1
0	0	0	0	0	0
e	c	e	1	0	a

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	4	1	c	0	e
4	c	0	e	4	1
1	0	e	4	1	c
c	e	4	1	c	0
0	4	1	c	0	e
e	1	c	0	e	4

$\odot$	4	1	c	0	e
4	1	4	e	0	c
1	4	1	c	0	e
c	e	c	4	0	1
0	0	0	0	0	0
e	c	e	1	0	4

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	4	1	c	0	e
4	c	0	e	4	1
1	0	e	4	1	c
c	e	4	1	c	0
0	4	1	c	0	e
e	1	c	0	e	4

$\odot$	4	1	c	0	e
4	1	4	e	0	c
1	4	1	c	0	e
c	e	c	4	0	1
0	0	0	0	0	0
e	c	e	1	0	4

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	4	1	c	0	2
4	c	0	2	4	1
1	0	2	4	1	c
c	2	4	1	c	0
0	4	1	c	0	2
2	1	c	0	2	4

$\odot$	4	1	c	0	2
4	1	4	2	0	c
1	4	1	c	0	2
c	2	c	4	0	1
0	0	0	0	0	0
2	c	2	1	0	4

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"

Algebraische Strukturen — Körper

Frage: Zeigen Sie, dass die folgenden Operationen auf $\{a, b, c, d, e\}$ einen Körper bilden.

$\oplus$	4	1	3	0	2
4	3	0	2	4	1
1	0	2	4	1	3
3	2	4	1	3	0
0	4	1	3	0	2
2	1	3	0	2	4

$\odot$	4	1	3	0	2
4	1	4	2	0	3
1	4	1	3	0	2
3	2	3	4	0	1
0	0	0	0	0	0
2	3	2	1	0	4

Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen $\mathcal{Z}_5$ zu "identifizieren"
- dies sind Tafeln von $\mathcal{Z}_5 \rightarrow$ isomorph zu $\mathcal{Z}_5$ und damit Körper

Zusammenfassung

- Definition und Eigenschaften von kommutativen Gruppen
- Definition und Eigenschaften von Körpern
- Charakterisierung der Galois-Körper

Sechste Aufgabenserie bereits im AlmaWeb verfügbar