http://www.fs.tum.de/

FSMPI/Referate/SET

Letztes Mal: Was ist eine Gruppe

Gegeben eine Menge G und einen zweistelligen Operator $\circ : G \times G \to G$

(i) Es ex ein $e \in G$ so daß für alle $g \in G$: $e \circ g = g$

Linksneutrales

(ii) Für alle $g \in G$ gibt es ein $g' \in G$: $g' \circ g = e$

Linksinverses zu g

(iii) Für alle $a, b, c \in G$ gilt

$$(a \circ b) \circ c = a \circ (b \circ c)$$

Assoziativität

Satz 1 Aus $a' \circ a = e$ folgt $a \circ a' = e$

Bew:

$$a \circ a' \overset{(i)}{=} e \circ (a \circ a')$$

$$\overset{(ii)}{=} \big((a')' \circ a'\big) \circ (a \circ a')$$

$$\overset{(iii)}{=} (a')' \circ \big(a' \circ (a \circ a')\big)$$

$$\overset{(iii)}{=} (a')' \circ \big((a' \circ a) \circ a'\big)$$

$$\overset{(ii)}{=} (a')' \circ \big(e \circ a'\big)$$

$$\overset{(i)}{=} (a')' \circ a'$$

$$\overset{(ii)}{=} e$$

q.e.d

Jedes Links-inverse ist auch Rechts inverses.

Satz 2 Aus $e \circ a = a$ für alle a folgt

$$a \circ e = a \text{ für alle } a.$$

Bew: Sei $a \in G$ und a' inverses zu a

Links neutrale sind auch Rechts neutral

$$a \circ e \overset{(ii)}{=} a \circ (a' \circ a)$$

$$\overset{(iii)}{=} (a \circ a') \circ a$$

$$\overset{\text{Satz 1}}{=} e \circ a$$

$$\overset{(i)}{=} a$$

q.e.d

Satz 3/4

Für $a, b \in G$ gibt es genau ein $x \in G$ mit

$$a \circ x = b$$

$y \in G$

$$y \circ a = b$$

Bew: Eindeutigkeit:

Ann: $a \circ x = b$ und $a \circ \bar{x} = b$

$\Rightarrow \quad a \circ x = a \circ \bar{x}$

$\Rightarrow a' \circ (a \circ x) = a' \circ (a \circ \bar{x})$

$\Rightarrow (a' \circ a) \circ x = (a' \circ a) \circ \bar{x}$

$\Rightarrow \quad e \circ x = e \circ \bar{x}$

$\Rightarrow \quad x = \bar{x}$

Existenz:

N: $x = a' \circ b$

$a \circ x = a \circ (a' \circ b)$

$= (a \circ a') \circ b$

$= e \circ b$

$= b$

Folgerungen:

- Neutrales Element ist eindeutig

- Inverses zu a ist Eindeutig

$a \circ x = a$
$\Rightarrow x = e$
ist eindeutig

- Für endl. Gruppen
  In jeder Zeile / Spalte der
  Verknüpfungstabelle jedes Elements aus G
  genau ein Mal.

(A) $(\mathbb{Z}_p, \oplus_p)$ ist Gruppe für alle $p \in \mathbb{N} - \{0\}$

(B) $(\mathbb{Z}_p - \{0\}, \odot_p)$ ist Gruppe wenn p Primzahl.

Bew (A) (0) Abgeschlossenheit von $\oplus_p$

Bildbereich von $\oplus_p$ ist $\{0, 1, 2, \ldots, p-1\} = \mathbb{Z}_p$

(i) Neutrales Element: Sei $a \in \mathbb{Z}_p$

$a \oplus_p 0 = (a+0) \bmod p = a \bmod p = a$

(ii) Inverses Element: Sei $a \in \mathbb{Z}_p$

wähle $a' = (p-a) \bmod p$

$a \oplus_p a' = (a + (p-a)) \bmod p = p \bmod p = 0$

(iii) Assoziativ: Sei $a, b, c \in \mathbb{Z}_p$

$(a \oplus_p b) \oplus_p c = ((a+b) \bmod p) + c) \bmod p = ((a+b)+c) \bmod p$

$= (a + (b+c)) \bmod p = \ldots = a \oplus_p (b \oplus_p c)$

(B): $(\mathbb{Z}_p - \{0\}, \odot_p)$ ist für wenn p eine Primzahl

Bew (O) Abgeschlossenheit: Zeige: Bildbereich vom $\odot_p$ ist $\mathbb{Z}_p - \{0\}$

Zeige $a \cdot b \neq k \cdot p$ für $a, b \in \{1, \ldots, p-1\}$

Andernfalls wäre $a \cdot b = k \cdot p$ für $a < p$ und $b < p$.

$\Rightarrow$ zu p ist Primzahl

(i) Neutrales Element: sei $a \in \mathbb{Z}_p - \{0\}$

$a \odot_p 1 = (a \cdot 1) \bmod p = a$

(ii) Inverses El: $\rightarrow$ Nächste Tafeln

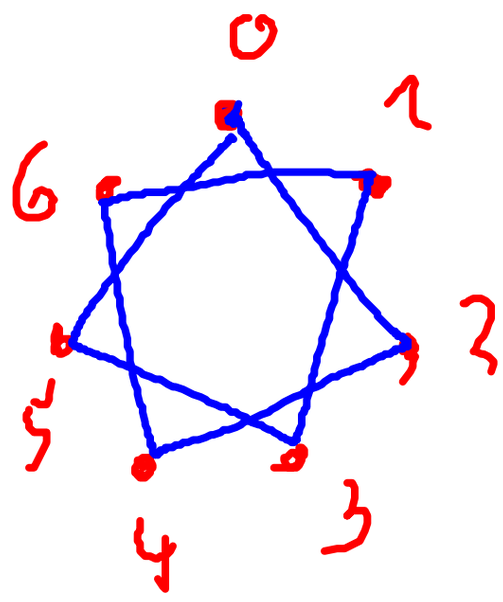
(iii) Assoziativität: Schreibarbeit, aber einfach.

Die eigentliche Schwierigkeit:

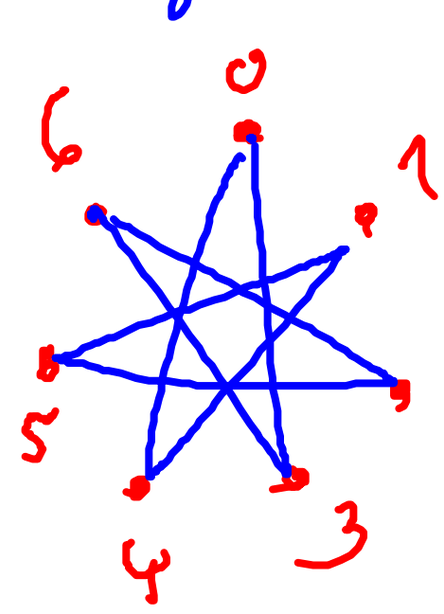
Sei p eine Primzahl und $a \in \{1, \dots, p-1\}$

Zeige es gibt ein $b \in \mathbb{Z}_p$ mit $(a \cdot b) \bmod p = 1$

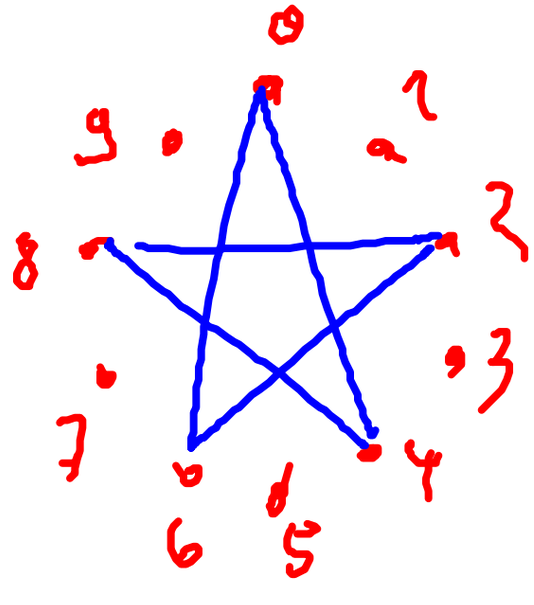
Bild haftes Diagramm für die Vielfachen von a



$p = 7, \quad a = 2$



$p = 7, \quad a = 3$



$p = 10, \quad a = 4$

Beobachtungen:

(1) jede getroffene Ecke sieht gleichaus

(2) bei p = Prim werden alle Ecken getroffen

Formalen Beweis: Es sei p eine Primzahl
und $a < p$, $a \neq 0$

Betrachte: $\{0 \odot_p a, 1 \odot_p a, 2 \odot_p a \dots (p-1) \odot_p a\} = M_a$

Zeige $M_a = \mathbb{Z}_p$! Bew durch Widerspruch

Annahme: $M_a \neq \mathbb{Z}_p \Rightarrow$ Es ex. $i, j < p$ mit

$i \odot_p a = j \odot_p a = \quad i > j$

$\Rightarrow (i \cdot a) \bmod p = (j \cdot a) \bmod p$

$\Rightarrow (i \cdot a - j \cdot a) \bmod p = 0$

$\Rightarrow ((i-j) \cdot a) \bmod p = 0$

$\Rightarrow (i-j) \cdot a = k \cdot p \Rightarrow$ p ist Primz.

$i-j \neq 0$, $i-j < p$; $a \neq 0$, $a < p$

Also gilt

$M_a = \mathbb{Z}_p$

$\Rightarrow 1 \in M_a$

$\Rightarrow$ Es ex b

mit $b \odot_p a = 1$