15. Vorlesung 16.11.2020

Notiztitel 16.11.2020

Aus der 14. Vorlesung:

Definition: Eine Menge M, $M \neq \emptyset$, mit zwei Verknüpfungen $\oplus : M \times M \to M$ und $\otimes : M \times M \to M$ heißt **Körper**, falls gilt

1) $(M, \oplus, \otimes)$ ist ein kommutativer Ring mit Eins
2) $e \in M$ ist das neutrale Element in $(M, \oplus)$ also $a \oplus e = e \oplus a = a \; \forall a \in M$, dann ist $M^* = M \setminus \{e\}$ und $(M^*, \otimes)$ ist eine **kommutative (abelsche) Gruppe**.

Merke: Ein Körper $(M, \oplus, \otimes)$ ist gekennzeichnet durch die 5 Körperaxiome, nämlich

Name	$\oplus$	$\otimes$
Assoziativgesetz	$a \oplus (b \oplus c) = (a \oplus b) \oplus c$	$a \otimes (b \otimes c) = (a \otimes b) \otimes c$
Kommutativgesetz	$a \oplus b = b \oplus a$	$a \otimes b = b \otimes a$
Distributivgesetz	$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$	
Existenz neutraler Elemente	$\exists! \, 0 \in M : a \oplus 0 = a \; \forall a \in M$	$\exists! \, 1 \in M : a \cdot 1 = a \; \forall a \in M$
Existenz inverser Elemente	$\forall a \in M \; \exists (-a) \in M : a + (-a) = 0$	$\forall a \in M \setminus \{0\} \; \exists a^{-1} \in M : a \cdot a^{-1} = 1$

Beispiele:

① $K = \{0, 1\}$ mit $\oplus : K \times K \to K$

Verknüpfungstabelle

$\oplus$	0	1
0	0	1
1	1	0

Kommutativ $\hat{=}$ Spiegeln an der Diagonale lässt die Tabelle gleich!

$\odot : K \times K \to K$

$\odot$	0	1
0	0	0
1	0	1

$K = \{0, 1\}$ mit $\oplus, \odot$ laut Verknüpfungstabelle ist der kleinste

mögliche Körper (Hinweis: 4. Übung → $0 \neq 1$ in einem Körper)

② $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

③ $K = \{0, 1, a, b\}$ mit folgenden Verknüpfungen

$\oplus : K \times K \to K$

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Spiegelsymmetrisch zur Diagonalen, also Kommutativ, 0 neutrales Element für $\oplus$, in jeder Zeile steht genau einmal die 0, d.h. zu jedem Element gibt es genau ein inverses Element bezüglich $\oplus$

$\odot : K \times K \to K$

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Spiegelsymmetrisch zur Diagonalen also Kommutativ, 1 neutrales Element für $\odot$

$K^* = K \setminus \{0\}$ mit $\odot$ ← in jeder Zeile steht genau einmal die 1, d.h. zu jedem Element $\neq 0$ gibt es genau ein inverses Element bezüglich $\odot$!

Exemplarisch (an einem Beispiel) das Distributivgesetz

$a \odot (b \oplus 1) = a \odot a = b$

$(a \odot b) \oplus (a \odot 1) = 1 \oplus a = b$

$\Rightarrow a \odot (b \oplus 1) = b = (a \odot b) \oplus (a \odot 1)$

das Distributivgesetz ist erfüllt!

Elementare Zahlentheorie → Zahlentheorie beschäftigt sich mit $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}$ und Rechenoperationen für diese Mengen

Definition:

Gegeben sind $a, b \in \mathbb{Z}$, $a \neq 0$. Dann gilt:

① **a teilt b** (geschrieben $a \mid b$), falls gilt: $\exists k \in \mathbb{Z} : b = k \cdot a$.
Man sagt dann auch: b ist ein (ganzzahliges) Vielfaches von a

② $\tilde{T}(b) = \{a \in \mathbb{Z} \mid a \mid b\}$ **Teilermenge von b** (Menge aller (ganzzahligen) Teiler von b

Beispiele:

① $5 \mid 15$ denn $15 = 3 \cdot 5$

$5 \mid -50$ denn $-50 = (-10) \cdot 5$

$5 \nmid 7$ denn $7 \neq k \cdot 5 \ \forall k \in \mathbb{Z}$

↳ $\nmid$ steht für „teilt nicht (ganzzahlig)"

$\cdot \mid$ ← „Spiegelsymmetrie"

② $\tilde{T}(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\} \subseteq [-12, 12]$

↳ denn $12 = (-3) \cdot (-4) = k \cdot (-4)$ mit $k = -3$

Es gilt folgende Symmetrie: $a \in \tilde{T}(12) \Leftrightarrow (-a) \in \tilde{T}(12)$

③ $\tilde{T}(7) = \{-7, -1, 1, 7\}$

Es gilt folgender Satz: $\forall a, b \in \mathbb{Z}, a \neq 0$

1) $\tilde{T}(b) = \tilde{T}(-b)$

2) $a \in \tilde{T}(b) \Leftrightarrow (-a) \in \tilde{T}(b)$

} es ist ausreichend alle Überlegungen zur (ganzzahligen) Teilbarkeit für $a, b \in \mathbb{N}$ durchzuführen

Beweisidee:

↳ 1) $a \in T(b) \Leftrightarrow \exists k \in \mathbb{Z} : b = k \cdot a \quad | \cdot (-1)$

$\Leftrightarrow \exists -k \in \mathbb{Z} : -b = (-k) \cdot a$

$\Leftrightarrow a \in T(-b)$

2) $a \in T(b) \Leftrightarrow \exists k \in \mathbb{Z} : b = k \cdot a \quad | \cdot 1 = (-1) \cdot (-1)$

$\Leftrightarrow b = (-k) \cdot (-a)$

$\Leftrightarrow (-a) \in T(b)$

Ab jetzt: $T(b) = \tilde{T}(b) \cap \mathbb{N}$ ← wir betrachten nur nicht negative Teiler

↳ $T(b) = \{a \in \mathbb{N} \mid b = k \cdot a \text{ für ein } k \in \mathbb{Z}\}$

↳ $T(7) = \tilde{T}(7) \cap \mathbb{N} = \{1, 7\}$

Definition: $p \in \mathbb{N}$ heißt Primzahl, falls gilt $T(p) = \{1, p\}$, d.h.

p hat (außer 1 und p) keine ganzzahligen Teiler!

Bemerkung: 2 ist die einzige gerade Primzahl

Es gilt: $\forall b \in \mathbb{Z}$ ist $\tilde{T}(b) \subseteq [-|b|, |b|]$ und $\underbrace{\tilde{T}(b)}_{=T(b)} \cap \mathbb{N} \subseteq [1, |b|]$

Im Intervall $[-|b|, |b|]$ liegen nur endlich viele ganze Zahlen, d.h. $\tilde{T}(b)$ ist eine endliche Menge!

$T(a,b) = T(a) \cap T(b)$; es gilt $T(a) \cap T(b) \subseteq T(b)$ und $T(a) \cap T(b) \subseteq T(a)$

Menge der gemeinsamen Teiler von a und b

$\Rightarrow$ $T(a,b)$ ist als Teilmenge endlicher Mengen ebenfalls eine endliche Menge

$\Rightarrow$ jede endliche Menge (Menge mit endlich vielen Zahlen als Element) kann nach Größe der Zahlen sortiert werden und es gibt ein größtes Element in $T(a,b)$.

Definition:

Das größte Element in $T(a,b) = T(a) \cap T(b)$ heißt größter gemeinsamer Teiler von a und b, man schreibt dafür $ggT(a,b)$.

Beispiel:

$\tilde{T}(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$

$\tilde{T}(8) = \{-8, -4, -2, -1, 1, 2, 4, 8\}$

$\rightarrow \tilde{T}(12) \cap \mathbb{N} = \{1, 2, 3, 4, 6, 12\} = T(12)$

$\rightarrow \tilde{T}(8) \cap \mathbb{N} = \{1, 2, 4, 8\} = T(8)$

$\Rightarrow T(12,8) = T(12) \cap T(8) = \{1, 2, 4\} \Rightarrow ggT(8,12) = 4$

Gibt es einen Algorithmus zur Berechnung von $ggT(a,b)$ ohne $T(a)$ und $T(b)$ einzeln zu ermitteln, $T(a,b) = T(a) \cap T(b)$ zu bilden, die Zahlen in $T(a,b)$ der Größe nach anzuordnen und dann das größte

Element anzugeben? Antwort: Ja → euklidischer Algorithmus

Vorbereitung: Division mit Rest

Gegeben sind $a, b \in \mathbb{Z}$, $a \neq 0$ dann existieren $k \in \mathbb{Z}$ und $m \in \mathbb{Z} \cap \mathbb{N}_0$ mit $b = k \cdot a + m$; $0 \leq m < |b|$

Reste sind immer nicht negativ

↳ (ganzzahliges) Teilen von b durch a mit Rest m

Beispiel: $a = 8, b = 21 \Rightarrow 21 = \underset{\uparrow k=2}{2} \cdot 8 + \underset{\uparrow m=5}{5}$

$a = 8, b = -27 \Rightarrow -27 = \underset{\uparrow k=-4}{(-4)} \cdot 8 + \underset{\uparrow m=5}{5}$

Behauptung: $ggT(a,b) = ggT(a,m)$ falls gilt $b = k \cdot a + m$, $0 \leq m < |b|$

Beweisidee: $ggT(a,b)$ ist das größte Element in $T(a,b) = T(a) \cap T(b)$

$ggT(a,m)$ ist das größte Element in $T(a,m) = T(a) \cap T(m)$

Wir zeigen (morgen) $\boxed{T(a,b) = T(a,m)}$

da die Mengen gleich sind,

sind die größten Elemente in beiden Mengen gleich!