Brückenkurs – Tag 5 – 2016-10-10

In der letzten Ausgabe

In der letzten Vorlesung behandelt: Primfaktorzerlegung. Weiterhin ist unbekannt, wie viele Primzahlen existieren. Ist ihre Zahl unbeschränkt?

6 Primzahlen

Satz (Euklid) Es gibt undendlich viele Primzahlen.

Beweis Seien $p_0, \dots p_{n-1}$ Primzahlen.
Dann können wir eine Primzahl p_n konstruieren mit $p_n \notin \{p_0, \dots, p_{n-1}\}$: Dazu betrachte: $e := p_0 \dots p_{n-1} + 1 = q_1 \dots q_s$ mit Primzahlen $q_1, \dots, q_s$ (PFZ)
Da die $P - i$ jeweils e nicht teilen (Rest 1!), die q_j aber e teilen, sind die q_j von p_i verschieden. Damit ist $p_n := q_i$ die gesuchte Primzahl.

Beispiel

$$\begin{array}{rcccl}
\emptyset & \rightsquigarrow & 1+1 & = & 2 = 2^1 \\
2 & \rightsquigarrow & 2+1 & = & 3 = 3^1 \\
2,3 & \rightsquigarrow & 2\cdot 3+1 & = & 7 = 7^1 \\
2,3,7 & \rightsquigarrow & 2\cdot 3\cdot 7+1 & = & 43 = 43^1 \\
2,3,7,43 & \rightsquigarrow & 2\cdot 3\cdot 7\cdot 43+1 & = & 1807 = 13\cdot 139
\end{array}$$

Primzahlsatz Sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Dann gilt: $\pi(x) \approx \frac{x}{\ln x}$, d.h.

$$\lim_{x\to\infty} {}^{\pi(x)}/_{x/_{\log x}} = 1$$

$$\pi(1) = 0, \pi(2) = 1, \pi(3) = 2, \pi(4) = 2, \pi(5) = 3, \pi(7,5) = 4, \cdots$$

Riemannsche Vermutung: $\Sigma_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$
Sei p_n die n-te Primzahl ($p_0 = 2, p_1 = 3, \cdots$).

Behauptung $p_n < e^{2^n}$ (Konvention [1])

Beweis per Induktion über n **n=0**
$p_0 = 2; e^{2^0} = e^1 = e > 2$
$n \implies n+1$

$$p_{n+1} \overset{\text{Euklid}}{\leq} p_0 \dots p_n + 1 = e^{2^0+2^1+\dots+2^n} + 1 = e^{2^{n+1}-1} + 1 = e^{2^{n+1}}(\frac{1}{e} + \frac{1}{e^{2^{n+1}}}) < e^{2^{n+1}} \quad \square$$

7 Algebraische Strukturen

7.1 Definition: Gruppe

Eine Gruppe ist eine Menge G zusammen mit einem ausgezeichneten Element $e \in G$ und einer Verknüpfung $\circ : G \times G \to G, (g,h) \mapsto g \circ h$, so dass folgende Axiome gelten:

(G1) Die Verknüpfung ist assoziativ: $g \circ (h \circ k) = (g \circ h) \circ k$ für $g, h, k \in G$

(G2) Das Element e ist neutrales Element: $e \circ g = g = g \circ e$ für $g \in G$

(G3) Jedes Element besitzt ein Inverses: Für alle $g \in G$ existiert ein $h \in G$ mit $g \circ h = e = h \circ g$

Die Gruppe heißt kommutativ (oder *abelsch*), falls zusätzlich gilt:

(G4) Die Verknüpfung ist kommutativ: $g \circ h = h \circ g$ für alle $g, h \in G$.

[1] $(a^b)^c = a^{b\cdot c}$, $a^{b^c} =: a^{b^c}$

7.1.1 Beispiele

Beispiel $G = \mathbb{Z}, e = 0 \in \mathbb{Z}, \circ = + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

(G1) $g + (h + k) = (g + h) + k$ für alle $g, h, k \in \mathbb{Z}$

(G2) $0 + g = g = g + 0$ für alle $g \in \mathbb{Z}$

(G3) $g + (-g) = 0 = (-g) + g$ für alle $g \in \mathbb{Z}$

(G4) $g + h = h + g$

Beispiel $(\mathbb{Q}, 0, +)$ ist genauso eine abelsche Gruppe.

Beispiel $(\mathbb{N}_0, 0, +)$ ist **keine Gruppe**.

Beispiel $(\mathbb{Z}, 1, \cdot)$ ist **keine Gruppe**, da G3 nicht erfüllt (z.B. existiert kein $n \in \mathbb{Z} mit 2 \cdot n = 1$).

Beispiel $(\mathbb{Q}, 1, \cdot)$ ist keine Gruppe, da G3 nicht erfüllt (Es existiert kein $x \in \mathbb{Q}\text{mit}0 \cdot x = 1$)

Beispiel $(\mathbb{Q}*, 1, \cdot)$, wobei $\mathbb{Q}* := \mathbb{Q} \setminus 0$ ist eine Gruppe

Beispiel $(\mathbb{Q} \setminus \mathbb{Z}, 1, \cdot)$ ist alles, aber keine Gruppe

7.1.2 Aussage

Sei G eine Gruppe mit zwei neutralen Elementen e, e'. Dann gilt $e = e'$.

Beweis $e = e \circ e' = e'$, da e neutral und e' neutral. □

Bemerkung Analog zeigt sich, dass das Inverse zu einem Element eindeutig bestimmt ist.

7.1.3 Aussage

Sei G eine Gruppe. Seien $a, b \in G$ mit Inversen a^{-1} bzw. $b^{-1} \in G$. Dann ist $b^{-1} \cdot a^{-1}$ invers zu $(a \circ b)$
$=: (a \circ b)^{-1}$

Beweis

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ b = e$$

Analog

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = \cdots = e$$

Schreibweise Auch in abstrakten Gruppen schreiben wir häufig $\cdot$ statt $\circ$ für die Verknüpfung und 1 für das neutrale Element. **Abkürzung** $ab := a \cdot b, a^{-1} :=$ Inverses zu a.

Aussage Sei G eine (multiplikativ geschriebene) Gruppe. Für $a \in G$ gilt dann $(a^{-1})^{-1} = a$

Beweis $a \cdot a^{-1} = 1 = a^{-1} \cdot a$ □

Beispiel [Gleichseitiges Dreieck mit gegen den Urzeigersinn nummerierten Ecken 1 - 3]
Symmetrien in der Ebene: $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} =: G$
mit e, τ, σ.
Seien $g, h \in G$. Dann sei $g \cdot h$ die Hintereinanderausführung von h und danach g.

Beispiel

$$\begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}$$

$\tau \circ \sigma = e$

Gruppentafel:

a \ b	e	σ	τ
e	e	σ	τ
σ	σ	τ	e
τ	τ	e	σ

Beispiel [Gleichseitiges Dreieck mit gegen den Urzeigersinn nummerierten Ecken 1 - 3]
Symmetrien im Raum:

$$\left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}\right\}$$

mit e, τ, σ, α_1, α_2, α_3.

$\alpha_1 \circ \sigma = \alpha_2$, $\sigma \circ \alpha_1 = \alpha 3 \neq \alpha_2 = \alpha 1 \circ \sigma$ Also nicht abelsch / kommutativ.

$$\alpha_1^2 = \alpha_1 \circ \alpha_1 = e \implies \alpha_1^{-1} = \alpha_1$$

Definition: symmetrische Gruppe Die **symmetrische Gruppe in n Buchstaben** ist die Gruppe der Permutationen von $1, \ldots, n$, geschrieben S_n, d.h. $S_n = \left\{\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma_1 & \sigma_2 & \cdots & \sigma_n\end{pmatrix} |(\sigma_1, \cdots, \sigma_n) \text{ Permutationen von } (1, \cdots, n)\right\}$

Beispiel {Dreiecks-Symmetrie im Raum} $= S_3$

7.1.4 Definition: Untergruppe

Eine Teilmenge $U \subseteq G$ einer Gruppe G heißt **Untergruppe**, falls (U1) $e \in U$, (U2) $g, h \in U \implies g \circ h \in U$, (U3) $g \in U \implies g^{-1} \in U$

Beispiel {Dreiecks-Symmetrien in der Ebene} $\subseteq \{Dreiecks-SymmetrienimRaum\}$

Beispiel $\mathbb{Z} \subseteq (\mathbb{Q}, 0, +)$ ist Untergruppe

Beispiel $\mathbb{N}_0 \subseteq (\mathbb{Z}, 0, +)$ ist keine Untergruppe.

7.1.5 Definition: Kommutative Ringe

Ein **kommutativer Ring** ist eine Menge R zusammen mit zwei ausgezeichneten Elementen 0 und $1 \in R$ und zwei Verknüpfungen $+ : R \times R \mapsto R$ und $\cdot : R \times R \mapsto R$ so dass gilt:

(R1) $\forall x, y, z \in R : x + (y + z) = (x + y) + z$

(R2) $\forall x \in R : x + 0 = x = 0 + x$

(R3) $\forall x \in R \; \exists \; y \in R : x + y = 0 = y + x$

(R4) $\forall x, y \in R : x + y = y + x$

(R5) $\forall x, y, z \in R : x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(R6) $\forall x \in R : x \cdot 1 = x = 1 \cdot x$

(R7) $\forall x, y \in R : x \cdot y = y \cdot x$

(R8) $\forall x, y, z \in R : x \cdot (y + z) = x \cdot y + x \cdot z \land (y + z) \cdot x = y \cdot x + u \cdot x$

Beispiel $(\mathbb{Z}, 0, 1, +, \cdot)$

Beispiel $(\mathbb{Q}, 0, 1, +, \cdot)$

Beispiel

Menge der Polynome bis X aus $\mathbb{Z}$ $\mathbb{Z}[X] = \{a_n X^n + \cdots + a_1 X + a_0 \;\mid\; a_0, \cdots, a_n \in \mathbb{Z}\}$

Beispiel $(\mathbb{Z}[X], 0, 1, +, \cdot)$
$(R[X], 0, 1, +, \cdot)$ falls R kommutativer Ring.

Bemerkung Ist $(R, 0, 1, +, \cdot)$ ein kommutativer Ring, so ist $(R, 0, +)$ eine abelsche Gruppe.

Definition Ist R ein kommutativer Ring, so $R* := \{x \in R \mid \exists\, y \in R : x \cdot y = 1 = y \cdot x\}$ Es ist $(R*, 1, \cdot)$ eine kommutative Gruppe, die **Einheitengruppe von** R.

Beispiel $\mathbb{Z}* = \{\pm 1\}, \mathbb{Q}* = \mathbb{Q} \setminus \{0\}$

Definition: Körper Ein **Körper** K der Menge ist ein kommutativer Ring für den Multiplikation und Addition abelsch definiert sind. Somit gelten für ihn die Axiome der abelschen Gruppen $(K, +, 0)$ und $(K, \cdot, 1)$ und das Distributivgesetz. Außerdem ist definiert: $K* = K \setminus \{0\}$

Beispiel $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.

Beispiel $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ ist ein Unterkörper.

$$0 = 0 + 0\sqrt{2}\,,\; 1 = 1 + 0\sqrt{2}$$

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} -$$