2. Teil: Diskrete Strukturen

Die nächsten 23 Einheiten betreffen Inhalte aus dem Bereich der diskreten Strukturen – mit Betonung auf Resultaten mit starkem Bezug zur Informatik:

Einheiten 18-22: Algebraische und zahlentheoretische Algorithmen (12.12./18.12./19.12.)

Einheiten 23-25: Graphen (19.12./8.1.)

Einheiten 26-30: RSA, Euler, Fibonacci (9.1./15.1./16.1.)

Einheiten 31-33: Wachstumsabschätzungen (16.1./22.1.)

Einheiten 34-35: Diskrete Wahrscheinlichkeit (23.1.)

Einheiten 36-38: Kombinatorik (29.1./5.2.)

Einheiten 39-41: Satz von Ramsey, Zusammenfassung (5.2./6.2.)

Zahlensysteme

Kenntnis der Zahlenbereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ setzen wir voraus.

Axiomatische Einführung von $\mathbb{N}$ über Peano-Axiome.

$\mathbb{Z}$ aus $\mathbb{N}$ leicht abzuleiten.

Wie wird $\mathbb{Q}$ definiert?

$\mathbb{R}$ ist der erste *überabzählbare* Zahlenbereich.

Von $\mathbb{R}$ gelangt man zu $\mathbb{C}$ durch Hinzunahme von $i = \sqrt{-1}$.

In $\mathbb{N}$ gibt es die wichtige Teilmenge der *Primzahlen*.

Halbgruppen und Monoide

Sei M eine Menge und $\circ$ eine zweistellige Verknüpfung, d.h.

$$\circ : M \times M \to M, \quad (m, n) \mapsto \circ(m, n)$$

Man schreibt dann oft $m \circ n$ statt $\circ(m, n)$.

Wenn $\circ$ eine assoziative Verknüpfung ist, sagen wir:

$(M, \circ)$ bildet eine Halbgruppe.

Hierbei bedeutet *assoziativ*, dass $\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$.

Wenn in einer Halbgruppe $(M, \circ)$ außerdem noch ein neutrales Element existiert, d.h. ein $e \in M$, für das $a \circ e = e \circ a = a$ für alle $a \in M$, dann sagen wir

$(M, \circ)$ bildet ein Monoid.

Manchmal schreibt man auch $(M, \circ, e)$, um das neutrale Element herauszuheben.

Gruppen

Wenn ein Monoid für jedes Element ein sogenanntes *beidseitiges Inverses* enthält, so nennen wir es eine Gruppe:

$$(G, \circ, e)$$

Wir zählen noch einmal alle Bedingungen an die Gruppenstruktur auf, man nennt sie auch *Gruppenaxiome*:

$\circ : G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \circ g_2$

$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ für alle $g_1, g_2, g_3 \in G$

$g \circ e = e \circ g = g$ für alle $g \in G$

Für jedes $g \in G$ gibt es ein $h \in G$ mit $g \circ h = h \circ g = e$

Gilt außerdem $g \circ h = h \circ g$ für alle $g, h \in G$, dann ist G eine kommutative oder abelsche Gruppe.

Ringe und Körper

Ein Ring R besteht aus einer *additiven* Gruppe mit neutralem Element 0, d.h. $(R, +, 0)$ ist eine abelsche Gruppe, sowie einer zusätzlichen Operation $\cdot$ (der Multiplikation), so dass $(R, \cdot, 1)$ mit einem Element $1 \in R$ ein Monoid bildet und die Distributivgesetze gelten:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Ein Körper K ist ein *kommutativer Ring* (also ein Ring, bei dem auch die Multiplikation kommutativ ist, d.h. $a \cdot b = b \cdot a$ für alle a, b), bei dem die Menge $K \setminus \{0\}$ mit der Multiplikation ebenfalls eine Gruppe bildet, d.h. für jedes $a \in K \setminus \{0\}$ gibt es ein Inverses $b \in K \setminus \{0\}$, so dass $a \cdot b = b \cdot a = 1$ gilt.

Unterstrukturen

Wenn X eine algebraische Struktur ist, dann ist eine Teilmenge $Y \subseteq X$ eine Unterstruktur, falls Y ebenfalls die von X geforderten Struktureigenschaften hat.

So gibt es also Untergruppen in Gruppen, Untermonoide in Monoiden, Unterhalbgruppen in Halbgruppen, und natürlich auch Unterringe in Ringen und Unterkörper in Körpern.

Beispiele:

In der Gruppe $(\mathbb{Z}, +, 0)$ ist für festes $n \in \mathbb{N}$ die Menge $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$ eine Untergruppe.

Im Körper $\mathbb{R}$ ist $\mathbb{Q}$ ein Unterkörper.

Im Monoid aller Wörter über dem Alphabet $\{a, b, c\}$ bilden die Wörter, die nur aus a's und b's bestehen, ein Untermonoid.

Homomorphismen

Ein Homomorphismus ist eine *strukturerhaltende Abbildung.*

So ist z.B. ein Monoid-Homomorphismus eine Abbildung φ von einem Monoid $(M_1, \circ_1, e_1)$ in ein Monoid $(M_2, \circ_2, e_2)$ mit der Eigenschaft, dass $\varphi(m \circ_1 m') = \varphi(m) \circ_2 \varphi(m')$ und $\varphi(e_1) = e_2$ gilt.

In ähnlicher Weise gibt es auch Gruppenhomomorphismen, Ringhomomorphismen und Körperhomomorphismen.

Homomorphismen mit zusätzlichen Eigenschaften haben spezielle Namen: Monomorphismus (injektiver Homomorphismus), Epimorphismus (surjektiver Homomorphismus), Isomorphismus (bijektiver Homomorphismus).