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).

Euklidischer Algorithmus

Ermitteln des größten gemeinsamen Teilers mit Euklid:

function $ggT(m, n)$ Hierbei ist $m \geq 0$ und $n \geq 0$ vorausgesetzt.
begin
  if $m = 0$ **then return** n
  else return $ggT(n \bmod m, m)$ **fi**
end

Man sieht leicht, dass die folgende Gleichheit gilt:

$$ggT(n \bmod m, m) = ggT(m, n)$$

Denn jeder Teiler von m und n teilt auch $n \bmod m$, und jeder Teiler von m und $n \bmod m$ teilt auch n.

Daraus folgt unmittelbar die Korrektheit des Algorithmus.

(Die Termination des Algorithmus ist klar, da die Zahlen immer kleiner werden.)

Beispiele

Wir illustrieren die Arbeit des Euklidischen Algorithmus bei der Berechnung des ggT von 68 und 171:

$$\begin{aligned} 171 &= 2 \cdot 68 + 35 \\ 68 &= 1 \cdot 35 + 33 \\ 35 &= 1 \cdot 33 + 2 \\ 33 &= 16 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 171 &= 3 \cdot 68 - 33 \\ 68 &= 2 \cdot 33 + 2 \\ 33 &= 16 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Rechts die Variante mit negativen Zahlen – der ggT ist 1 und wird in beiden Varianten korrekt berechnet.

Zur Übung berechnen wir noch $ggT(210, 78)$:

$$\begin{aligned} 210 &= 2 \cdot 78 + 54 \\ 78 &= 1 \cdot 54 + 24 \\ 54 &= 2 \cdot 24 + 6 \\ 24 &= 4 \cdot 6 + 0 \end{aligned}$$

Also: $ggT(210, 78) = 6$

Lemma von Bézout

Das Lemma von Bézout besagt, dass man $ggT(m,n)$ immer als Linearkombination von m und n darstellen kann:

Lemma: Für alle $m, n \in \mathbb{Z}$ existieren $a, b \in \mathbb{Z}$, so dass

$$ggT(m,n) = am + bn$$

Beweis: Es sei ohne Einschränkung $m > n > 0$.

Mit Euklids Algorithmus erhalten wir Reste $r_0 > r_1 > \cdots > r_k$, so dass $r_0 = m$, $r_1 = n$, $r_k = 0$, $r_{k-1} = ggT(m,n)$ und für alle $1 \leq i < k$:

$$r_{i-1} = q_i r_i + r_{i+1}$$

Damit ist r_{k-1} eine Linearkombination von r_{k-2} und r_{k-3}, und man kann induktiv schließen, dass r_{k-1} auch eine Linearkombination von $r_1 = n$ und $r_0 = m$ ist. Da aber $r_{k-1} = ggT(m,n)$ ist, erhalten wir die Behauptung.

Zwei Aufgaben

Aufgabe 1.1: Zeige, dass $\log_{10}(p) \notin \mathbb{Q}$ für beliebige Primzahl p.

Lösung: Wir führen einen Widerspruchsbeweis.
Angenommen, $\log_{10}(p) = \frac{a}{b}$ mit $a, b \in \mathbb{N}$.
Dann folgt: $p^b = (10^{\log_{10}(p)})^b = 10^a = 2^a \cdot 5^a$.
Damit müssten sowohl 2, als auch 5 Teiler von p^b, und damit von p sein, ein Widerspruch, da ja p eine Primzahl ist!

Aufgabe 1.2:

a) Berechne $x, y \in \mathbb{Z}$ mit $ggT(35, 56) = x \cdot 35 - y \cdot 56$.

b) Und jetzt dasselbe für $x, y \in \mathbb{N}$.

Bitte selbst lösen. Zur Kontrolle die Ergebnisse: $7 = (-3) \cdot 35 - (-2) \cdot 56$
und $7 = 53 \cdot 35 - 33 \cdot 56$.

Eindeutige Primfaktorzerlegung

Die folgende Aussage ist eine Folge von Bézout's Lemma:

$$ggT(n, m_1) = 1 \ \wedge \ ggT(n, m_2) = 1 \quad \Longrightarrow \quad ggT(n, m_1 m_2) = 1$$

Denn: Aus $an + bm_1 = 1 = cn + dm_2$ folgt

$$1 = (an + bm_1)(cn + dm_2) = (anc + bm_1 c + adm_2)n + bd(m_1 m_2)$$

Also ist jeder Teiler von n und $m_1 m_2$ auch Teiler der 1, d.h. $ggT(n, m_1 m_2) = 1$.

Satz: Sei $n \in \mathbb{N}$ und $n > 0$. Dann lässt sich n eindeutig darstellen als

$$n = \prod_{p \text{ Primzahl}} p^{n_p}$$

Dabei ist $n_p \neq 0$ genau dann, wenn p Teiler von n ist.