

Vorlesung Diskrete Strukturen

Die natürlichen Zahlen

Bernhard Ganter

Institut für Algebra
TU Dresden
D-01062 Dresden
bernhard.ganter@tu-dresden.de

WS 2009/10

Alles ist Zahl?

Wenn in der modernen Mathematik alles auf Mengen aufgebaut ist, woher kommen dann die Zahlen? Sind Zahlen etwa auch Mengen?

Die Antwort ist „ja“. In einem sorgfältigen Aufbau der Mathematik werden auch die Zahlbereiche, von den natürlichen bis zu den komplexen Zahlen und darüber hinaus, aus dem Mengenbegriff entwickelt.

Informatiker müssen das nicht lernen, außer für den Fall der natürlichen Zahlen, denn der wird gern bei den **abstrakten Datentypen** als Beispiel genommen.

Eine Mengenkonstruktion

Als Modell der natürlichen Zahlen könnte man eine Folge von Mengen nehmen, die $0, 1, 2, \dots$ Elemente haben. Um eine solche Folge zu erhalten, definieren wir für beliebige Mengen S

$$S^+ := S \cup \{S\}.$$

Wir nennen S^+ den **Nachfolger** von S .

Zum Beispiel ist der Nachfolger der Menge $S := \{a, b, c\}$ gleich

$$\{a, b, c\}^+ = \{a, b, c, \{a, b, c\}\}.$$

Ein Modell der natürlichen Zahlen

Man betrachtet nun, ausgehend von der leeren Menge $S := \emptyset$, die Folge $\emptyset, \emptyset^+, (\emptyset^+)^+, \dots$, also

$$\begin{aligned}\emptyset & \\ \emptyset^+ &= \{\emptyset\} \\ \emptyset^{++} &= \{\emptyset, \{\emptyset\}\} \\ \emptyset^{+++} &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ &\dots\end{aligned}$$

Man kann diesen Mengen abkürzend die vertrauten Namen geben

$$0 := \emptyset, \quad 1 := \emptyset^+, \quad 2 := \emptyset^{++}, \quad 3 := \emptyset^{+++}, \dots$$

und setzt

$$\mathbb{N} := \{\emptyset, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, \dots\}.$$

Die Axiome von Giuseppe Peano

Für die auf der vorigen Folie konstruierte Menge \mathbb{N} mit der Operation $+$ gelten folgende Gesetze:

- 1 Zu jeder natürlichen Zahl n gibt es genau eine natürliche Zahl n^+ , genannt der **Nachfolger** von n .
- 2 Aus $m^+ = n^+$ folgt stets $m = n$, d.h., jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.
- 3 Es gibt eine natürliche Zahl 0 , die nicht Nachfolger einer natürlichen Zahl ist. Es gibt also keine natürliche Zahl n mit $0 = n^+$.
- 4 Ist S eine Menge von natürlichen Zahlen, die die Zahl 0 enthält und die die Eigenschaft hat, dass für jedes $n \in S$ auch $n^+ \in S$ gilt, dann ist S die Menge aller natürlichen Zahlen.

Die axiomatische Methode

Man untersucht nun nur noch, welche Gesetze aus diesen Axiomen folgen. Jede Struktur, die diese Axiome erfüllt, wird als ein Modell der natürlichen Zahlen angesehen. Die Frage nach der „wahren Natur“ der natürlichen Zahlen erübrigt sich dadurch.

Das vierte Axiom wird auch das **Induktionsaxiom** genannt. Betrachte irgendeine Aussage $A(n)$, die für natürliche Zahlen n gelten kann, aber von n abhängt. Es sei S die Menge derjenigen natürlichen Zahlen, für die diese Aussage gilt. Das Induktionsaxiom sagt: Enthält S die Zahl 0 und ist mit jeder Zahl, die zu S gehört, auch deren Nachfolger in S , dann enthält S alle natürlichen Zahlen.

Vier schwerwiegende Fragen

- 1 Ist es (bis auf Isomorphie) das einzige Modell der Peano-Axiome, oder gibt es vielleicht mehrere verschiedene Arten natürlicher Zahlen? (Fachausdruck: Ist das Axiomensystem **kategorisch**?)
- 2 Kann das Induktionsaxiom durch ein einfacheres Axiom ersetzt werden? (Können die natürlichen Zahlen in der **Logik erster Stufe** axiomatisiert werden?)
- 3 Kann man noch Axiome hinzunehmen, die aus den obigen weder folgen noch zu ihnen im Widerspruch stehen? (**Vollständigkeit** des Axiomensystems)
- 4 Reichen die natürliche Zahlen für das Zählen aus?

... und Antworten

- 1 Man kann (leicht) beweisen, dass das System der Peano-Axiome kategorisch ist, was bedeutet, dass je zwei seiner Modelle isomorph sind. Damit ist die Frage nach der Eindeutigkeit der Arithmetik positiv beantwortet: Das Standardmodell ist bis auf Isomorphie das einzige Modell der Peano-Axiome.
- 2 Nach dem Satz von Skolem aus der mathematischen Logik gibt es zu jeder unendlichen Struktur eine, die zu ihr elementar äquivalent, aber nicht isomorph ist. Das bedeutet, dass das Induktionsaxiom nicht durch ein Axiom in der Logik erster Stufe ersetzt werden kann, ohne dass die Eindeutigkeit des Modells verloren geht. Man erhält bei einer Axiomatisierung in der Logik erster Stufe stets sogenannte „Nichtstandardmodelle“ der Arithmetik.
- 3 Die Arithmetik ist (nach K. Gödel) in der Prädikatenlogik erster Stufe **unentscheidbar**. Es gibt Aussagen, die weder bewiesen noch widerlegt werden können.
- 4 Die Frage „Wieviele natürliche Zahlen gibt es“ hat als Antwort jedenfalls keine natürliche Zahl. G. Cantor hat gezeigt, dass man sinnvoll und mathematisch korrekt *unendliche* Zahlen einführen und damit auch rechnen kann.

Die arithmetischen Operationen

Auf die Axiome kann man die Definitionen der Addition und der Multiplikation aufbauen, z.B. so:

Addition

- 1 $n + 0 := n,$
- 2 $n + m^+ := (n + m)^+.$

Multiplikation

- 1 $n \cdot 0 := 0,$
- 2 $n \cdot m^+ := n \cdot m + n.$

Auch die \leq -Ordnung lässt sich so präzise beschreiben.

Die natürlichen Zahlen bilden mit diesen Operationen einen geordneten **kommutativen Semiring**.

Die natürlichen Zahlen sind wohlgeordnet

Man kann auch beweisen, dass die Ordnung der natürlichen Zahlen eine besondere Eigenschaft hat, die man **Wohlordnung** nennt:

Theorem

Jede nichtleere Menge natürlicher Zahlen hat ein kleinstes Element.

Die Wohlordnungseigenschaft kann man als alternative Beweisform zum Induktionsbeweis verwenden. Man spricht scherzhaft vom *Prinzip des kleinsten Verbrechers*:

Wenn eine Behauptung $A(n)$ nicht für alle natürlichen Zahlen gilt, dann muss es ein *kleinstes* Gegenbeispiel geben. Kann man also die Existenz eines kleinsten Gegenbeispiels widerlegen, muss $A(n)$ für alle natürlichen Zahlen gelten.

Wir definieren auf \mathbb{N} die **Teilbarkeitsrelation** durch

$$a \mid b : \iff \exists_{k \in \mathbb{N}} \quad a \cdot k = b$$

und erhalten dadurch eine (weitere) Ordnungsrelation.

Eine natürliche Zahl p ist eine **Primzahl**, wenn sie größer als 1 ist und nur durch 1 und sich selbst teilbar ist.

Beachte:

- 1 ist keine Primzahl.
- Jede natürliche Zahl teilt 0.
- Wenn a ein Teiler von b ist und $b > 0$, dann ist $a \leq b$.
- Teilt a sowohl b_1 als auch b_2 , dann teilt a auch $b_1 + b_2$ und $b_1 - b_2$ (vorausgesetzt $b_1 \geq b_2$).
- $a \mid b$ ist gleichbedeutend zu $a \bmod b = 0$.

Wichtiges über Primzahlen

Satz

Jede natürliche Zahl $n > 1$ ist durch eine Primzahl teilbar.

Beweis durch vollständige Induktion.

Satz

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Satz

Teilt eine Primzahl ein Produkt natürlicher Zahlen, dann teilt sie einen der Faktoren.

Satz (Fundamentalsatz der Arithmetik)

Jede natürliche Zahl $n > 0$ kann auf genau eine Weise als ein Produkt

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

geschrieben werden, wobei k eine natürliche Zahl ist,

$p_1 < p_2 < \dots < p_k$ Primzahlen und $\alpha_1, \dots, \alpha_k$ positive natürliche Zahlen sind.

Man nennt dieses Produkt die **kanonische Darstellung** der natürlichen Zahl n . Für das leere Produkt (also den Fall $k = 0$) hat man dabei den Wert 1 vereinbart.

Hilfssatz

Die Teiler einer natürlichen Zahl n mit der kanonischen Darstellung

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

sind genau die Zahlen t der Form

$$t = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k},$$

wobei die β_i natürliche Zahlen sind mit $0 \leq \beta_i \leq \alpha_i$ für alle $i \in \{1, \dots, k\}$.

Wieviele Teiler?

Korollar

Die Anzahl der Teiler einer natürlichen Zahl mit der kanonischen Darstellung

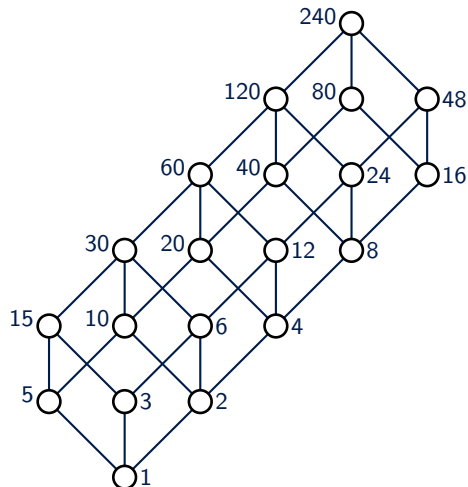
$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

ist

$$\prod_{i=1}^k (\alpha_i + 1) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1).$$

Beispiel: Die Zahl $240 = 2^4 \cdot 3 \cdot 5$ hat genau $(4 + 1) \cdot (1 + 1) \cdot (1 + 1)$ Teiler.

Ein Teilerdiagramm der Zahl 240



Der Teilverband als Begriffsverband

Die Teiler einer beliebigen Zahl $n \geq 1$ können als Begriffe eines formalen Kontextes dargestellt werden.

- Als Gegenstände wählt man diejenigen Primzahlpotenzen, die Teiler von n sind:

$$G := \{q \mid q \text{ Primzahlpotenz, die } n \text{ teilt}\},$$

- Merkmale sind die Teiler $\frac{n}{q}$, wobei q Primzahlpotenz ist:

$$M := \left\{ \frac{n}{q} \mid q \in G \right\},$$

- und die Inzidenzrelation ist die Teilbarkeit.

Beispiel $n = 240$

T_{240}	120	60	30	15	80	48
2	×	×	×		×	×
4	×	×			×	×
8	×				×	×
16					×	×
3	×	×	×	×		×
5	×	×	×	×	×	

Diese formalen Kontexte haben genau so viele Begriffe, wie es Teiler der Zahl n gibt. Zu jedem Teiler t gehört der Begriff (A_t, B_t)

- mit dem Umfang $A_t = \{g \in G \mid g \text{ teilt } t\}$
- und dem Inhalt $B_t = \{m \in M \mid t \text{ teilt } m\}$.

Man erhält

$$\text{kgV}(A_t) = t = \text{ggT}(B_t).$$

Je zwei natürliche Zahlen n und m (nicht beide Null) besitzen

- einen größten gemeinsamen Teiler $\text{ggT}(m, n)$ und
- ein kleinstes gemeinsames Vielfaches $\text{kgV}(m, n)$.

Zur Bestimmung des ggT kann man den Algorithmus der *Wechselwegnahme* benutzen:

Algorithmus Wechselwegnahme

```
while  $m \neq n$  do
begin
    if  $m < n$  then  $n := n - m$ 
    if  $n < m$  then  $m := m - n$ 
end
output(''ggT ='', m).
```

Beispiel zur Wechselwegnahme

		n	m
Input:		154	238
$238 - 154 = 84$	also:	154	84
$154 - 84 = 70$	also:	70	84
$84 - 70 = 14$	also:	70	14
$70 - 14 = 56$	also:	56	14
$56 - 14 = 42$	also:	42	14
$42 - 14 = 28$	also:	28	14
$28 - 14 = 14$	also:	14	14
	stop.		

Ergebnis: Der ggT von 154 und 238 ist 14.

Der ggT ändert sich nicht

Beobachtung Sind $m \neq n$ natürliche Zahlen und sind m_1, n_1 die Zahlen, die aus m, n nach einem Schritt des Algorithmus Wechselwegnahme entstehen, dann gilt $\text{ggT}(m_1, n_1) = \text{ggT}(m, n)$.

Beweis O.B.d.A. sei $m < n$. Dann ist $m_1 = m$ und $n_1 = n - m$. Jede Zahl, die m und n teilt, teilt auch $n - m$, und jede Zahl, die m und $n - m$ teilt, teilt auch n .

Die Zahlen m und n haben also genau die gleichen gemeinsamen Teiler wie die Zahlen m und $n - m$.

Insbesondere haben sie den gleichen größten gemeinsamen Teiler. □

Hilfssatz

Der Algorithmus **Wechselwegnahme** berechnet den größten gemeinsamen Teiler (ggT).

Beweis Der Algorithmus bricht nach endlich vielen Schritten ab, weil bei jedem Schritt eine der beiden Zahlen echt kleiner wird.

Nach der Beobachtung bleibt der ggT bei jedem Schritt erhalten, er muss also auch der gleich sein, wenn der Algorithmus terminiert.

Der Algorithmus terminiert, wenn die beiden Zahlen gleich sind. Der ggT von n und n ist aber n . □

Zweite Beobachtung Es seien $m \neq n$ natürliche Zahlen und m_1, n_1 die Zahlen, die aus m, n nach einem Schritt des Algorithmus Wechselwegnahme entstehen.

Außerdem seien a_1, b_1 beliebige ganze Zahlen und

$$d := a_1 \cdot m_1 + b_1 \cdot n_1.$$

Dann gibt es ganze Zahlen a, b mit

$$d = a \cdot m + b \cdot n.$$

Beweis O.B.d.A. sei $m_1 = m$ und $n_1 = n - m$, also

$$\begin{aligned} d &= a_1 \cdot m_1 + b_1 \cdot n_1 \\ &= a_1 \cdot m + b_1 \cdot (n - m) \\ &= (a_1 - 1) \cdot m + b_1 \cdot n. \quad \square \end{aligned}$$

Der ggT als Linearkombination

Aus der zweiten Beobachtung können wir einen nützlichen Satz ableiten:

Satz

Zu je zwei natürlichen Zahlen m, n existieren ganze Zahlen α, β mit

$$\text{ggT}(m, n) = \alpha \cdot m + \beta \cdot n.$$

Diese Zahlen α, β kann man durch „Rückwärtseinsetzen“ beim Algorithmus „Wechselwegnahme“ leicht bestimmen.

Der Euklidische Algorithmus ...

Am Beispiel erkennt man eine Möglichkeit, den Algorithmus zu beschleunigen: Die letzten vier Schritte kann man zu einem einzigen zusammenfassen.

Statt die kleinere Zahl von der größeren nur einmal abzuziehen, zieht man sie gleich mehrfach ab, aber immer so, dass das Ergebnis nicht negativ wird:

Euklidischer Algorithmus

Input: Natürliche Zahlen n, m mit $n \geq m \geq 0$

```
WHILE  $m \neq 0$  do  
     $(n, m) := (m, n \bmod m);$ 
```

```
output('ggT =', m).
```

... berechnet den ggT

Der Euklidische Algorithmus führt offenbar zum gleichen Ergebnis wie die Wechselwegnahme. Wir haben also:

Satz

Der Euklidische Algorithmus berechnet den ggT .

Beispiel

a	b	
238	154	$238 \bmod 154 = 84$

Beispiel

a	b	
238	154	$238 \bmod 154 = 84$
154	84	$154 \bmod 84 = 70$

Beispiel

a	b	
238	154	$238 \bmod 154 = 84$
154	84	$154 \bmod 84 = 70$
84	70	$84 \bmod 70 = 14$

Beispiel

a	b	
238	154	$238 \bmod 154 = 84$
154	84	$154 \bmod 84 = 70$
84	70	$84 \bmod 70 = 14$
70	14	$70 \bmod 14 = 0$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	
84	70	$84 \bmod 70 = 14$	
70	14	$70 \bmod 14 = 0$	$\text{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	
84	70	$84 \bmod 70 = 14$	$14 = 84 - 70$
70	14	$70 \bmod 14 = 0$	$\text{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	$70 = 154 - 84$
84	70	$84 \bmod 70 = 14$	$14 = 84 - 70$
70	14	$70 \bmod 14 = 0$	$\text{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	$84 = 238 - 154$
154	84	$154 \bmod 84 = 70$	$70 = 154 - 84$
84	70	$84 \bmod 70 = 14$	$14 = 84 - 70$
70	14	$70 \bmod 14 = 0$	$\text{ggT}(238, 154) = 14$

Beispiel

a	b	
238	154	$84 = 238 - 154$
154	84	$70 = 154 - 84$
84	70	$14 = 84 - 70$
70	14	$\text{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$84 = 238 - 154$	$\text{ggT} = 84 - 70$
154	84	$70 = 154 - 84$	
84	70	$14 = 84 - 70$	
70	14	$\text{ggT}(238, 154) = 14$	

Beispiel

a	b		
238	154	$84 = 238 - 154$	
154	84	$70 = 154 - 84$	$\text{ggT} = 2 \cdot 84 - 154$
84	70	$14 = 84 - 70$	$\text{ggT} = 84 - 70$
70	14	$\text{ggT}(238, 154) = 14$	

Beispiel

a	b		
238	154	$84 = 238 - 154$	$\text{ggT} = 2 \cdot 238 - 3 \cdot 154$
154	84	$70 = 154 - 84$	$\text{ggT} = 2 \cdot 84 - 154$
84	70	$14 = 84 - 70$	$\text{ggT} = 84 - 70$
70	14	$\text{ggT}(238, 154) = 14$	

Teilerfremde Zahlen

Zwei natürliche Zahlen heißen **teilerfremd**, wenn ihr größter gemeinsamer Teiler gleich 1 ist.

Ein wichtiger Spezialfall des oben formulierten Satzes ist folgender:

Satz

Zwei natürliche Zahlen m und n sind genau dann teilerfremd, wenn es ganze Zahlen α und β gibt mit

$$\alpha \cdot m + \beta \cdot n = 1.$$

Zu gegebenen teilerfremden Zahlen m und n kann man Zahlen α und β mit $\alpha \cdot m + \beta \cdot n = 1$ über den euklidischen Algorithmus berechnen.

Wieviele zu n teilerfremde Zahlen sind kleiner als n ?

Die Anzahl der zu n teilerfremden Zahlen in $\{0, 1, 2, \dots, n-1\}$ wird mit $\varphi(n)$ bezeichnet. Man nennt die Funktion $n \mapsto \varphi(n)$ die **eulersche φ -Funktion** oder **Totient-Funktion**.

Die ersten Werte der φ -Funktion sind:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
φ	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Eine Formel für die eulersche φ -Funktion

Hilfssatz

Hat die Zahl n die kanonische Darstellung

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k},$$

dann gilt

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right).$$

Beispiel:

$$\varphi(240) = \varphi(2^4 \cdot 3 \cdot 5) = 240 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 64.$$