Mathematik I für Studierende der Informatik und Wirtschaftsinformatik (Diskrete Mathematik) im Wintersemester 2017/18

9. November 2017

Beispiel 3.6

Wir können die rationalen Zahlen wie folgt konstruieren:
Betrachte zunächst die Menge

$$M = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n \neq 0\}.$$

Ein Paar (m, n) steht dabei für den Bruch $\frac{m}{n}$.
Nun identifizieren wir Brüche, die durch Erweitern oder Kürzen auseinander hervorgehen. Dazu sei $(m, n) \sim (m', n')$, falls $mn' = m'n$ gilt.
Man rechnet leicht nach, dass $\sim$ eine Äquivalenzrelation auf M ist.
Nun definieren wir $\mathbb{Q}$ als die Menge der Äquivalenzklassen der Relation $\sim$ auf M.
Für die Äquivalenzklasse von (m, n) schreiben wir $\frac{m}{n}$.

Die Menge der Äquivalenzklassen einer Äquivalenzrelation $\sim$ auf einer Menge M nennt man auch die *Faktormenge* oder den *Quotienten* von M nach der Relation $\sim$.
Die Menge der Äquivalenzklassen wird mit $M/\sim$ bezeichnet.

Ist M endlich mit m Elementen und haben alle $\sim$-Äquivalenzklassen gleichviele Elemente, zum Beispiel n Stück, so hat $M/\sim$ genau m/n Elemente.

Beispiel 3.7

Auch die ganzen Zahlen können wir als Faktormenge konstruieren:
Betrachte zunächst die Menge

$$M = \mathbb{N}_0 \times \mathbb{N}_0.$$

Ein Paar (m, n) steht dabei für die Differenz $m - n$.
Nun identifizieren wir Paare $(m, n), (m', n') \in M$, die dieselben Differenzen beschreiben.Dazu sei $(m, n) \sim (m', n')$, falls $m + n' = m' + n$ gilt.
Man rechnet leicht nach, dass $\sim$ eine Äquivalenzrelation auf M ist.
Nun definieren wir $\mathbb{Z}$ als die Menge der Äquivalenzklassen der Relation $\sim$ auf M, also als die Faktormenge $M/\sim$.

Die Addition auf $\mathbb{Z}$ wird dann wie folgt definiert:

$$[(m, n)] + [(m', n')] := [(m + m', n + n')]$$

Das entspricht der Rechenregel

$$(m - n) + (m' - n') = (m + m') - (n + n').$$

Ordnungsrelationen

Definition 3.8

Sei A eine Menge und R eine Relation auf A. Dann ist R eine *Ordnungsrelation*, falls R reflexiv, antisymmetrisch und transitiv ist. Ein Ordnungsrelation R auf einer Menge A heißt *lineare Ordnung*, falls für alle $a, b \in A$ mit $a \neq b$ entweder aRb oder bRa gilt.

Ordnungsrelationen werden oft mit $\leq$ oder einem ähnlichen Zeichen bezeichnet, auch wenn es sich nicht um die bekannten Relationen auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$ handelt. Man schreibt dann praktisch immer $a \leq b$ anstelle von $(a, b) \in \leq$.

Beispiel 3.12

(1) Die Relationen, die alle mit $\leq$ bezeichnet werden, sind lineare Ordnungen auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.

(2) Für jede Menge M ist $\subseteq$ eine Ordnungsrelation auf $\mathcal{P}(M)$.

(3) Die Teilbarkeitsrelation $|$ ist eine Ordnungsrelation auf $\mathbb{N}$

Die rationalen Zahlen lassen sich als Punkte auf dem Zahlenstrahl veranschaulichen.
Dabei liegen die rationalen Zahlen *dicht* auf dem Zahlenstrahl.
D.h., zwischen je zwei verschiedenen Punkten auf dem Zahlenstrahl liegt eine rationale Zahl. .
Eine naheliegende Frage ist, ob jeder Punkt auf dem Zahlenstrahl auch einer rationalen Zahl entspricht.

Die reellen Zahlen

Mit $\sqrt{2}$ bezeichnen wir die positive Lösung der Gleichung $x^2 = 2$.
Es stellt sich heraus, dass $\sqrt{2}$ keine rationale Zahl ist.

Lemma 3.16

Sei m eine ganze Zahl. Falls m^2 gerade ist, so ist auch m selbst gerade.

Satz 3.17

Es gibt keine rationale Zahl a mit $a^2 = 2$.

$\sqrt{2}$ entspricht einem Punkt auf der Zahlengeraden.
Wir können $\mathbb{Q}$ aber so zur Menge $\mathbb{R}$ der *reellen Zahlen* erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden.
Wir können reelle Zahlen addieren und multiplizieren, wobei wir bei Einschränkung dieser Operationen auf $\mathbb{Q}$ genau die bekannten Operationen auf den rationalen Zahlen erhalten.
Mit diesen Operationen bilden die reellen Zahlen einen Körper, wie die rationalen Zahlen auch.

Die Kleiner-Beziehung $<$ zwischen reellen Zahlen ist so erklärt, dass für reelle Zahlen a und b die Beziehung $a < b$ genau dann gilt, wenn der Punkt auf der Zahlengeraden, der a entspricht, links von dem Punkt liegt, der b entspricht.
Es gelten dieselben Rechenregeln für $<$ auf $\mathbb{R}$ wie auf $\mathbb{Q}$.

Es gibt verschiedene Möglichkeiten, die reellen Zahlen ausgehend von den rationalen Zahlen zu konstruieren.
Wir werden allerdings nicht näher auf die Konstruktion eingehen.
Alle reellen Zahlen lassen sich als (eventuell unendliche) Dezimalbrüche darstellen.
Die rationalen Zahlen entsprechen den Dezimalbrüchen, die entweder nach endlich vielen Nachkommastellen abbrechen oder periodisch werden.

Die reellen Zahlen, die nicht rational sind, heißen *irrational*.
Beispiele für irrationale Zahlen sind $\sqrt{2}$, $\sqrt{3}$, e, π und $\sqrt[3]{5}$.

Die Abzählbarkeit von $\mathbb{Q}$ und die Überabzählbarkeit von $\mathbb{R}$

Definition 3.18

Zwei Mengen A und B heißen *gleichmächtig*, wenn es eine Bijektion $f : A \to B$ gibt.

Diese Definition ist auch für unendliche Mengen sinnvoll. So ist

$$f : \mathbb{Z} \to \{a \in \mathbb{Z} : a \text{ ist gerade}\}; a \mapsto 2a$$

eine Bijektion zwischen den ganzen Zahlen und den (positiven sowie negativen) geraden Zahlen. $\mathbb{Z}$ und die Menge aller geraden Zahlen sind also gleichmächtig.

Definition 3.19

Eine Menge M heißt abzählbar, wenn M entweder endlich ist oder es eine Bijektion $f : \mathbb{N} \to M$ gibt.
Eine Menge, die nicht abzählbar ist, heißt überabzählbar.

Man kann leicht zeigen, dass eine Menge genau dann M abzählbar ist, wenn M entweder leer ist oder es eine surjektive Abbildung $f : \mathbb{N} \to M$ gibt. Eine Surjektion $f : \mathbb{N} \to M$ nennt man eine *Aufzählung* von M. Eine Aufzählung f von M kann man einfach in der Form $f(1), f(2), \ldots$ notieren.

Satz 3.20

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.

Wir hatten schon gesehen, dass es reelle Zahlen gibt, die nicht rational sind. Der folgende Satz zeigt, dass es viel mehr reelle Zahlen als rationale Zahlen gibt.

Satz 3.21

Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.

Teilbarkeit, Primzahlen und der euklidische Algorithmus

Definition 3.22

Eine ganze Zahl a ist ein *Teiler* einer ganzen Zahl b, falls eine ganze Zahl c mit $b = a \cdot c$ existiert.
Wenn a ein Teiler von b ist, so nennt man b ein *Vielfaches* von a.
Ist a ein Teiler von b, so schreiben wir $a \mid b$.
Ist a kein Teiler von b, so schreiben wir $a \nmid b$.

Man beachte, dass jede ganze Zahl a die 0 teilt. Es ist nämlich $0 = 0 \cdot a$. Umgekehrt teilt 0 nur sich selber und keine andere ganze Zahl.

Ebenso beachte man, dass für alle ganzen Zahlen a und b Folgendes gilt:

$$a \mid b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b \Leftrightarrow a \mid -b$$

Damit kann man die Teilbarkeitsbeziehung zwischen ganzen Zahlen immer auf die Teilbarkeitsbeziehung zwischen natürlichen Zahlen zurückführen.

Satz 3.23

Die Teilbarkeitsbeziehung $|$ hat folgende Eigenschaften:

1. *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
2. *Aus $a_1 \mid b_1$ und $a_2 \mid b_2$ folgt $a_1 \cdot a_2 \mid b_1 \cdot b_2$.*
3. *Aus $a \cdot b \mid a \cdot c$ und $a \neq 0$ folgt $b \mid c$.*
4. *Aus $a \mid b_1$ und $a \mid b_2$ folgt für alle $c_1, c_2 \in \mathbb{Z}$ die Beziehung $a \mid b_1 \cdot c_1 + b_2 \cdot c_2$.*

Definition 3.24

Eine natürliche Zahl $n \geq 2$ heißt *Primzahl*, wenn n nur durch -1, 1, n und $-n$ teilbar ist.
Die Zahlen ± 1 und $\pm n$ nennt man die *trivialen* Teiler von n.

Satz 3.25 (Euklid)

Es gibt unendlich viele Primzahlen.

Satz 3.26

Jede natürliche Zahl $n \geq 2$ ist ein Produkt der Form $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ wobei k eine natürliche Zahl ≥ 1 ist, $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen sind und $\alpha_1, \ldots, \alpha_k$ natürliche Zahlen sind.
Dabei ist die Produktdarstellung $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ bis auf die Reihenfolge der Faktoren eindeutig.

Korollar 3.27

Teilt eine Primzahl p ein Produkt $a \cdot b$ natürlicher Zahlen, so teilt p eine der beiden Zahlen a und b.

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition 3.28

Seien a und b natürliche Zahlen. Der *größte gemeinsame Teiler* von a und b ist die größte natürliche Zahl c, die sowohl a als auch b teilt.
Der größte gemeinsame Teiler von a und b wird mit $\mathrm{ggT}(a, b)$ bezeichnet.

Das *kleinste gemeinsame Vielfache* von a und b ist die kleinste natürliche Zahl, die sowohl von a als auch von b geteilt wird.
Das kleinste gemeinsame Vielfache von a und b wird mit $\mathrm{kgV}(a, b)$ bezeichnet.

Sei $\{p_1, \ldots, p_n\}$ die Menge der Primzahlen, die sowohl a als auch b teilen.
Für jedes $i \in \{1, \ldots, n\}$ sei α_i die größte natürliche Zahl, so dass $p_i^{\alpha_i}$ sowohl a als auch b teilt.
Dann ist $p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ der größte gemeinsame Teiler von a und b.

Sei nun $\{q_1, \ldots, q_m\}$ die Menge der Primzahlen, die a oder b teilen.
Für jedes $i \in \{1, \ldots, m\}$ sei β_i die größte natürliche Zahl, so dass $q_i^{\beta_i} \mid a$ oder $q_i^{\beta_1} \mid b$ gilt.
Dann ist $q_1^{\beta_1} \cdot \ldots \cdot q_m^{\beta_n}$ das kleinste gemeinsame Vielfache von a und b.

Es gilt die Beziehung $\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b$.

Satz 3.30

Für alle $m \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen q und r mit $0 \leq r < n$ und $m = q \cdot n + r$.

In der Darstellung $m = q \cdot n + r$ nennt man q den *Quotienten* von m und n und r den *Rest*.
Die Funktion, die m und n den Quotienten q zuordnet wird mit div bezeichnet.
Die Funktion, die m und n den Rest r zuordnet heißt mod.
Es gilt also für alle $m \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ die Gleichung

$$m = (m \operatorname{div} n) \cdot n + (m \bmod n).$$

Für ganze Zahlen m und n gilt $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, m \mod n)$.
Für jede natürliche Zahl n ist $\mathrm{ggT}(n, 0) = n$.

Der euklidische Algorithmus zur Bestimmung des ggT.
Seien $m, n \in \mathbb{N}_0$ mit $m > n$.

1. Falls $n = 0$ ist, so gib m als den größten gemeinsamen Teiler aus.
2. Falls $n \neq 0$ ist, so bestimme ganze Zahlen q und r mit $0 \leq r < n$ und $m = q \cdot n + r$.
3. Setze $m := n$ und $n := r$ gehe zurück zu 1.

Der Algorithmus endet also, wenn $n = 0$ erreicht wird. Die dann ausgegebene Zahl ist der größte gemeinsame Teiler der ursprünglichen Werte von m und n.

Modulare Arithmetik

Definition 3.33

Es sei m eine natürliche Zahl. Zwei ganze Zahlen a und b sind *kongruent modulo* m, falls a und b denselben Rest bei Division durch m haben.

Ist a kongruent zu b modulo m, so schreiben wir $a \equiv b \,(\mathrm{mod}\, m)$.

$a \equiv b \,(\mathrm{mod}\, m)$ gilt genau dann, wenn $a - b$ durch m teilbar ist.

Definition 3.36

Für jede natürliche Zahl m und jede ganze Zahl a heißt die Menge $[a]_m := \{b \in \mathbb{Z} : b \bmod m = a \bmod m\}$ die *Restklasse von a modulo m*.

Für jede natürliche Zahl m gibt es genau m verschiedene Restklassen modulo m, nämlich $[0]_m, \ldots, [m-1]_m$.
Diese Restklassen sind paarweise disjunkt und es gilt $\mathbb{Z} = [0]_m \cup \cdots \cup [m-1]_m$.

Satz 3.37

Für alle $m \in \mathbb{N}$ *und alle* $a, b, c, d \in \mathbb{Z}$ *gilt:*

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
4. $a \equiv b \pmod{m} \Rightarrow -a \equiv -b \pmod{m}$
5. $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$
6. *Gilt* $\mathrm{ggT}(c, m) = 1$, *so folgt aus* $c \cdot a \equiv c \cdot b \pmod{m}$ *die Kongruenz* $a \equiv b \pmod{m}$.

Definition 3.39

Für eine reelle Zahl r ist $\lceil r \rceil$ die kleinste ganze Zahl $\geq r$.
Analog ist $\lfloor r \rfloor$ die größte ganze Zahl $\leq r$.
Man nennt $\lceil \quad \rceil$ die *obere Gaußklammer* und $\lfloor \quad \rfloor$ die *untere Gaußklammer*.

Für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt $m \operatorname{div} n = \lfloor \frac{m}{n} \rfloor$ sowie $m \bmod n = m - n \cdot \lfloor \frac{m}{n} \rfloor$.

Elementare Kombinatorik

Satz 4.2

1. (Additionsregel) M sei eine endliche Menge und $M_1, \ldots, M_n$ seien disjunkte Teilmengen von M mit $M = M_1 \cup \cdots \cup M_n$. Dann gilt

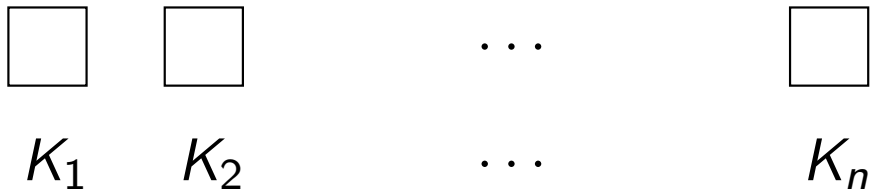
$$|M| = \sum_{i=1}^{n} |M_i|.$$

2. (Multiplikationsregel) Seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot \ldots \cdot |A_n| = \prod_{i=1}^{n} |A_i|.$$

3. (Gleichheitsregel) Seien A und B zwei endliche Mengen. Dann gilt $|A| = |B|$ genau dann, wenn es eine Bijektion $f : A \to B$ gibt.

Eine typische Anwendung der Multiplikationsregel ist die folgende:
Für ein $n \in \mathbb{N}$ betrachten wir n Kästchen $K_1, \ldots, K_n$.



In das erste Kästchen K_1 legen wir ein Objekt a_1, in das zweite Kästchen K_2 ein Objekt a_2 und so weiter.
Wenn wir k_1 Möglichkeiten haben, das erste Kästchen K_1 zu belegen, k_2 Möglichkeiten, das zweite Kästchen K_2 zu belegen und so weiter, dann gibt es insgesamt $k_1 \cdot k_2 \cdot \ldots \cdot k_n$ Möglichkeiten, die n Kästchen zu belegen.

Beispiel 4.3

1. Eine Kennziffer bestehe aus drei Buchstaben und vier darauffolgenden Ziffern, wie *FAB*3447 oder *ARR*5510. Wieviele derartige Kennziffern gibt es?
Nach der Multiplikationsregel gibt es

$$26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 26^3 \cdot 10^4 = 175760000$$

Kennziffern.
2. Wieviele Kennziffern wie in (1) gibt es, in denen kein Buchstabe und keine Ziffer doppelt vorkommen?
Nach der Multiplikationsregeln ergibt sich

$$26 \cdot 25 \cdot 24 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 78624000.$$

3. Gegeben seien 15 unterschiedliche Bücher, von denen 8 auf Englisch, 3 auf Deutsch und 4 auf Russisch sind. Auf wie viele Arten kann man zwei Bücher in verschiedenen Sprachen auswählen?
Nach Additions- und Multiplikationsregel ergibt sich

$$8 \cdot 3 + 8 \cdot 4 + 3 \cdot 4 = 68.$$