2 Zahlen

1 Die Körper $\mathbb{R}$ und $\mathbb{Q}$

Da wir es in diesem und in den nächsten Semestern sehr viel mit reellen Zahlen zu tun haben werden, wollen wir zunächst unser hoffentlich vorhandenes Wissen hierüber auffrischen. Welche Rechenregeln für reelle und rationale Zahlen sind uns bekannt?

- Die Addition oder Multiplikation reeller bzw. rationaler Zahlen a, b ergibt stets eine reelle bzw. rationale Zahl $a + b$ oder $a \cdot b$.
- Es gelten die *Assoziativgesetze*: $a + (b + c) = (a + b) + c, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Es gelten die *Kommutativgesetze*: $a + b = b + a, \quad a \cdot b = b \cdot a$
- Es gilt das *Distributivgesetz*: $a \cdot (b + c) = a \cdot b + a \cdot c$ [5]
- Es existieren *neutrale Elemente*: $a + 0 = a$ und $a \cdot 1 = a$ für jede Zahl a. 0 ist das neutrale Element der Addition, 1 das der Multiplikation.
- Es existieren *inverse Elemente*: Zu jeder reellen bzw. rationalen Zahl a gibt es eine reelle bzw. rationale Zahl b mit $a + b = 0$. Zu jeder reellen bzw. rationalen Zahl $a \neq 0$ gibt es eine reelle bzw. rationale Zahl $c \neq 0$ mit $a \cdot c = 1$. Es ist $b = -a$ und $c = \frac{1}{a}$.

Jetzt gehen wir axiomatisch vor, d.h., wir geben Axiome an, durch die die Menge, deren Elemente wir in der Schule als reelle Zahlen kennengelernt haben, letztendlich eindeutig bestimmt ist. Vergleichen Sie die folgenden Axiome mit den oben angeführten Rechenregeln!

Def 1.1 (Körperaxiome)

Auf einer beliebigen Menge $\mathbb{K}$ seien zwei binäre Verknüpfungen + (Addition) und $\cdot$ (Multiplikation) erklärt. $(\mathbb{K}, +, \cdot)$ heißt *Körper* : $\Longleftrightarrow$

$$
\begin{aligned}
&(K1) \quad a + (b + c) = (a + b) + c, \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall\, a, b, c \in \mathbb{K} \\
&(K2) \quad a + b = b + a, \qquad a \cdot b = b \cdot a \qquad \forall\, a, b \in \mathbb{K} \\
&(K3) \quad a \cdot (b + c) = a \cdot b + a \cdot c \qquad \forall\, a, b, c \in \mathbb{K} \\
&(K4) \quad \exists\, 0, 1 \in \mathbb{K}\ (0 \neq 1)\ :\ a + 0 = a, \qquad a \cdot 1 = a \qquad \forall\, a \in \mathbb{K} \\
&(K5) \quad \forall\, a \in \mathbb{K} \quad \exists - a \in \mathbb{K}\ :\ a + (-a) = 0, \\
&\qquad\quad \forall\, a \in \mathbb{K} \backslash \{0\} \quad \exists\, a^{-1} \in \mathbb{K} \backslash \{0\}\ :\ a \cdot a^{-1} = 1
\end{aligned}
$$

Bei den Verknüpfungen + und $\cdot$ muss es sich nicht um die bekannte Addition und Multiplikation von Zahlen handeln. Wenn es eindeutig klar ist, welche Verknüpfungen zu Grunde liegen, spricht man auch kurz von dem Körper $\mathbb{K}$ an Stelle von $(\mathbb{K}, +, \cdot)$. Die Gesetze $(K1)$–$(K3)$ heißen Assoziativ–, Kommutativ– und Distributivgesetz. Die Forderung nach der Kommutativität der Addition ist eigentlich überflüssig, da sie aus den anderen Axiomen gefolgert werden kann (eventuell Übung). Die Elemente 0 und 1 werden

[5] Mit der Vereinbarung Punktrechnung vor Strichrechnung

neutrale Elemente bezüglich der jeweiligen Verknüpfung oder auch Null– bzw. Einselement genannt. Analog spricht man in $(K5)$ von den *inversen Elementen*. Bei einer beliebigen Menge $\mathbb{K}$ sind die neutralen Elemente in der Regel nicht die Zahlen 0 und 1!

Beispiele: Neben den reellen Zahlen bilden auch die rationalen Zahlen mit der normalen Addition und Multiplikation einen Körper, weitere Beispiele für Körper werden wir in den Übungen kennenlernen.

Die natürlichen bzw. die ganzen Zahlen genügen nicht allen Axiomen eines Körpers.

Frage: Welche Axiome werden nicht erfüllt?

Die ganzen Zahlen sind „beinahe“ ein Körper, es scheitert lediglich an der fehlenden Existenz von inversen Elementen bezüglich der Multiplikation: So findet man beispielsweise zur ganzen Zahl 2 keine ganze Zahl z mit $2 \cdot z = 1$.

Def 1.2 (Ringaxiome)

Auf einer beliebigen Menge R seien binäre Verknüpfungen $+$ und $\cdot$ erklärt. $(R, +, \cdot)$ heißt (kommutativer) *Ring* (mit Eins) $:\Longleftrightarrow$ Außer den Körperaxiomen (K1) –(K4) gilt

$$(R5) \qquad \forall\, a \in R \quad \exists - a \in R \;:\; a + (-a) = 0$$

Jeder Körper ist gleichzeitig ein Ring. Bezüglich der üblichen Addition und Multiplikation bilden die ganzen Zahlen einen Ring, aber keinen Körper. Die natürlichen Zahlen bilden keinen Ring und damit erst recht keinen Körper. Andere wichtige Beispiele für Zahlenringe mit nur endlich vielen Elementen werden wir später untersuchen.

Erfüllt eine Menge mit nur *einer* binären Verknüpfung die entsprechenden Bedingungen $(K1), (K4)$ und $(K5)$, so spricht man von einer *Gruppe*, gilt zusätzlich für diese Verknüpfung $(K2)$, von einer *kommutativen* oder *abelschen Gruppe*.

Beispiele: $(\mathbb{R}, +)$ und $(\mathbb{R}\backslash\{0\}, \cdot)$ sind abelsche Gruppen. $(\mathbb{Z}, +)$ ist eine Gruppe, $(\mathbb{N}, +)$ nicht. Bezüglich der Multiplikation ist auch $\mathbb{Q}\backslash\{0\}$ eine Gruppe. Was ist mit $\mathbb{Z}\backslash\{0\}$?

Ist der Gruppenbegriff bekannt, kann ein Körper auch so definiert werden:

Def 1.3 $(K, +, \cdot)$ ist ein Körper $:\Longleftrightarrow$

1) $(K, +)$ ist abelsche Gruppe
2) $(K^*, \cdot)$ ist abelsche Gruppe mit $K^* := K\backslash\{0\}$
3) Es gilt das Distributivgesetz $(K3)$

In Gruppen und Körpern gelten viele Rechengesetze, die wir von den reellen Zahlen bereits aus der Schulzeit kennen (sollten). Wir werden einige dieser Regeln beweisen. Ab jetzt sei $(\mathbb{K}, +, \cdot)$ stets ein beliebiger Körper, $\mathbb{K}^* := \mathbb{K}\backslash\{0\}$. Wem dies zu abstrakt ist, darf sich unter $\mathbb{K}$ die rationalen oder besser die reellen Zahlen vorstellen. Ferner werden wir häufig statt $a \cdot b$ kürzer ab schreiben.

Satz 1.1 (Kürzungsregel)

Seien $a, b, x \in \mathbb{K},\ c, d, y \in \mathbb{K}^*$ beliebig. Dann gelten

$$\begin{array}{lll} 1) & a + x = b + x & \Longrightarrow \quad a = b \\ 2) & cy = dy & \Longrightarrow \quad c = d \end{array}$$

Beweis: 1): $a = a+0 = a+(x+(-x)) = (a+x)+(-x) = (b+x)+(-x) = b+(x+(-x)) = b+0 = b$. Der Beweis zu 2) verläuft analog (Übung!).

Mit Hilfe der Kürzungsregel können wir weitere einfache Aussagen beweisen.

Satz 1.2 Seien $a, b \in \mathbb{K},\ c \in \mathbb{K}^*$ beliebig. Dann gelten

$$\begin{array}{lrcl} 1) & 0 \cdot a & = & 0 \\ 2) & -(-a) & = & a, \qquad (c^{-1})^{-1} \ = \ c \\ 3) & a \cdot (-b) & = & (-a) \cdot b \ = \ -ab \\ 4) & (-a)(-b) & = & ab \end{array}$$

Beweis: 1): $0a + 0 = 0a = (0+0)a = 0a + 0a \implies 0 = 0a$

2): $(-a) + a = a + (-a) = 0 = (-a) + (-(-a)) \implies$ Behauptung

3): $a(-b) + ab = a((-b) + b) = a \cdot 0 = 0 \cdot a = 0 \implies a(-b) = -ab$

Die fehlenden Beweisteile werden eventuell in den Übungen erledigt.

Zur Erinnerung: $-x$ ist das additiv inverse Element zu $x \in \mathbb{K}$ und hat zunächst nichts mit positiv oder negativ zu tun. Andererseits gibt es reelle Zahlen, die wir in der Schule als positiv oder negativ bezeichnet haben, ferner haben wir gelernt, Zahlen der Größe nach zu vergleichen.

Def 1.4 (Anordnungsaxiome)

Ein Körper $(\mathbb{K}, +, \cdot)$ heißt *angeordnet* : $\Longleftrightarrow$ Es existiert eine Relation $<$ auf $\mathbb{K}$ mit

$$\begin{array}{ll} (A1) & \forall\, (a,b) \in \mathbb{K} \times \mathbb{K} \text{ gilt genau eine der Möglichkeiten } a < b \ \vee \ a = b \ \vee \ b < a \\ (A2) & a < b \ \wedge \ b < c \implies a < c \qquad \forall\, a, b, c \in \mathbb{K} \\ (A3) & a < b \implies a + c < b + c \qquad \forall\, a, b, c \in \mathbb{K} \\ (A4) & a < b \ \wedge \ 0 < c \implies ac < bc \qquad \forall\, a, b, c \in \mathbb{K} \end{array}$$

In (A2) wird die Transitivität gefordert. Gilt $a < b$ oder $a = b$, schreibt man zusammenfassend $a \leq b$. An Stelle von $a < b$ oder $a \leq b$ werden wir auch die Schreibweisen $b > a$ oder $b \geq a$ verwenden.

Beispiel: Die rationalen Zahlen und die reellen Zahlen bilden jeweils angeordnete Körper. Später werden wir sehen, dass die komplexen Zahlen einen Körper bilden, der nicht angeordnet werden kann.

Wir wollen einige Rechenregeln für Ungleichungen in angeordneten Körpern beweisen. Zur besseren Übersicht werden wir das multiplikativ inverse Element zu x nicht x^{-1}, sondern $\frac{1}{x}$ schreiben. Wegen der Kommutativität der Multiplikation hat das einen angenehmen Nebeneffekt; denn wegen

$$a \cdot b^{-1} \ = \ a \cdot \frac{1}{b} \ = \ \frac{1}{b} \cdot a \ = \ b^{-1} \cdot a$$

dürfen wir einfach

$$a \cdot b^{-1} \ = \ b^{-1} \cdot a \ = \ \frac{a}{b}$$

schreiben – wie aus Schulzeiten gewohnt.

Satz 1.3 Sei $(\mathbb{K}, +, \cdot)$ ein angeordneter Körper, seien $a, b, c, d \in \mathbb{K}$. Dann gelten

1) $a < b \ \wedge \ c < d \implies a + c < b + d$
2) $a < b \ \wedge \ c < 0 \implies ac > bc$
3) $0 < 1$
4) $0 < a < b \implies 0 < \frac{1}{b} < \frac{1}{a}$

Beweis: 1): Aus Axiom $(A3)$ folgt $a + c < b + c$ und $c + b < d + b$, mit $(K2)$ und $(A2)$ folgt dann die Behauptung $a + c < b + d$.

2): Für $c < 0$ folgt aus $(A3)$ $c + (-c) < 0 + (-c)$, damit gilt $0 < -c$. Wenn wir jetzt $(A4)$ auf $a < b$ und $0 < -c$ anwenden, erhalten wir $a(-c) < b(-c)$. Dies ist nach 3) aus Satz 1.2 gleichbedeutend mit $-ac < -bc$. Addiert man auf beiden Seiten $ac+bc$, folgt die Behauptung aus $(A3)$ und den Körperaxiomen.

3): Nach $(A1)$ und $(K4)$ wissen wir, dass $0 < 1$ oder $1 < 0$ gelten muss. Wäre $1 < 0$, so würde aus 2) (setze dort $a = c = 1$ und $b = 0$) sofort auch $1 = 1 \cdot 1 > 0 \cdot 1 = 0$ folgen, ein Widerspruch.

4): Beweis als Übung.

Eine einfache Folgerung aus $0 < 1$ ist $-1 < 0$. Versuchen Sie dies zu beweisen, indem Sie das Gegenteil $0 < -1$ annehmen und mit Hilfe von Satz 1.3 zu dem Widerspruch $0 < 0$ gelangen!

In den folgenden Sätzen und Definitionen sei $(\mathbb{K}, +, \cdot)$ stets ein angeordneter Körper und $a, b, c, d \in \mathbb{K}$. Ohne Beweis geben wir analog zu Satz 1.3 einige Regeln für $\leq$ an:

Satz 1.4

1) $a \leq b \ \wedge \ b \leq c \implies a \leq c$
2) $a \leq b \ \wedge \ c \leq d \implies a + c \leq b + d$
3) $a \leq b \ \wedge \ c > 0 \implies ac \leq bc$
4) $a \leq b \ \wedge \ c < 0 \implies ac \geq bc$

Def 1.5

$$|a| := \begin{cases} a & \text{falls} \quad a \geq 0 \\ -a & \text{falls} \quad a < 0 \end{cases}$$

heißt der *(Absolut)betrag* von a.

Beispiel: $|-5| = -(-5) = 5$. Spätestens jetzt sollte klar sein, dass $-x$ nicht automatisch eine negative Zahl ist!

Wegen $0 < 1$ gilt $1 = |1|$ und wegen $-1 < 0 < 1$ gilt $-1 < 1 = |1|$, also insgesamt $1, -1 \leq |1|$. Man kann sogar für jedes $x \in \mathbb{K}$ zeigen, dass $x \leq |x|$ und $-x \leq |x|$ immer beide erfüllt sind.

Satz 1.5

1) Es gilt stets $|a| \geq 0$ und es ist $|a| = 0 \iff a = 0$
2) $|a\,b| \ = \ |a|\,|b|$
3) $|\frac{a}{b}| \ = \ \frac{|a|}{|b|}$ falls $b \neq 0$
4) $|a + b| \ \leq \ |a| + |b|$ (sogenannte *Dreiecksungleichung*)
5) $|a - b| \ \geq \ |a| - |b|$

Beweis: 1): Für $a > 0$ ist $|a| = a$, für $a < 0$ ist $|a| = -a > 0$.

2): Wir führen eine Fallunterscheidung durch:

$$\begin{aligned} a,b \geq 0 &\implies ab \geq 0 \implies |ab| = ab = |a|\,|b| \\ a \geq 0,\ b < 0 &\implies ab \leq 0 \implies |ab| = -ab = a(-b) = |a|\,|b| \\ a < 0,\ b \geq 0 &\implies ab \leq 0 \implies |ab| = -ab = (-a)b = |a|\,|b| \\ a,b < 0 &\implies ab > 0 \implies |ab| = ab = (-a)(-b) = |a|\,|b| \end{aligned}$$

3): Es ist $a = \frac{a}{b} \cdot b$, also $|a| = |\frac{a}{b} b| = |\frac{a}{b}|\,|b| \implies$ Behauptung

4): Wir benutzen Satz 1.4. 2) und die Tatsache, dass für alle Körperelemente x stets $x \leq |x|$ und $-x \leq |x|$ erfüllt sind. Es folgt $a + b \leq |a| + b \leq |a| + |b|$ und $-(a+b) = (-a) + (-b) \leq |a| + (-b) \leq |a| + |b|$. Es gibt nur die beiden Möglichkeiten:

$$a + b \geq 0 \implies |a+b| = a + b \leq |a| + |b| \quad \text{und} \quad a + b < 0 \implies |a+b| = -(a+b) \leq |a| + |b|$$

5): $|a| = |b + a - b| \leq |b| + |a - b| \implies$ Behauptung

Mit Hilfe vollständiger Induktion kann man die Dreiecksungleichung für $n > 2$ Summanden beweisen:

Satz 1.6 $$\left| \sum_{i=1}^{n} a_i \right| \leq \sum_{i=1}^{n} |a_i| \quad , \quad a_i \in \mathbb{K} \, .$$

Alle Aussagen und Definitionen in diesem Abschnitt galten bisher gleichermaßen für $\mathbb{R}$ und für $\mathbb{Q}$. Dies wird sich nun ändern!

Def 1.6 (Vollständigkeitsaxiom)

Ein angeordneter Körper $(\mathbb{K}, +, \cdot)$ heißt *vollständig* : $\iff$ Seien $A, B \subseteq \mathbb{K}$ nicht leer und es gelte $a < b \ \forall\, a \in A,\, b \in B$. Dann existiert (mindestens) ein $c \in \mathbb{K}$ mit $a \leq c \leq b \ \forall\, a \in A,\, b \in B$.

Jetzt haben wir unser Ziel erreicht, die reellen Zahlen sind eindeutig durch Axiome festgelegt: *Die reellen Zahlen bilden den einzigen vollständigen angeordneten Körper.* Stellt man sich $\mathbb{R}$ auf einer Zahlengeraden in der üblichen Weise vor, besagt das Vollständigkeitsaxiom anschaulich, dass man zwischen jeder „linken“ Menge A und „rechten“ Menge B mindestens eine reelle Zahl c finden kann (die zu A oder B gehören darf), die die Mengen A und B im obigen Sinn „trennt“. Manchmal wird dieses Axiom deshalb auch *Schnittaxiom* genannt. Man kann auch für nicht angeordnete Körper Vollständigkeit definieren, dies ist jedoch wesentlich komplizierter und wird von uns nicht weiter untersucht.

Ohne Beweis geben wir eine weitere wichtige Eigenschaft der reellen Zahlen an:

$$\forall\, r \in \mathbb{R} \quad \exists\, n \in \mathbb{N} \ : \quad 0 \leq |r| < n$$

Wegen Teil 4) von Satz 1.3 gilt dann auch $\quad \forall\, r \in \mathbb{R}^* \quad \exists\, n \in \mathbb{N} \ : \quad 0 < \frac{1}{n} < |r|$.

Mit Hilfe dieser Tatsache zeigen wir

Satz 1.7 $\mathbb{Q}$ ist nicht vollständig.

Beweis: Sei $A := \{a \in \mathbb{Q} \mid a < \sqrt{2}\}$ und $B := \{b \in \mathbb{Q} \mid b > \sqrt{2}\}$. Wäre $\mathbb{Q}$ vollständig, müsste es eine rationale Zahl q geben mit $a \leq q \leq b$ für alle $a \in A$ und $b \in B$. Wegen $\sqrt{2} \notin \mathbb{Q}$ ist $\mathbb{Q} = A \cup B$. Das gesuchte q muss in A oder in B liegen.

1. Fall: $q \in A$, also $\sqrt{2} - q > 0$. Wie oben gesagt, gibt es eine natürliche Zahl n mit $0 < \frac{1}{n} < \sqrt{2} - q \implies q + \frac{1}{n} < \sqrt{2} \implies q < q + \frac{1}{n} \in A$, Widerspruch.

2. Fall: $q \in B \implies q - \sqrt{2} > 0 \implies \exists\, m \in \mathbb{N} : 0 < \frac{1}{m} < q - \sqrt{2} \implies \sqrt{2} < q - \frac{1}{m} < q$. Da $q - \frac{1}{m} \in B$, ist auch dies nicht möglich.

Also ist das Vollständigkeitsaxiom für die rationalen Zahlen nicht erfüllt.

2 Einige ordnungstheoretische Begriffe

Dieser Abschnitt handelt vornehmlich von Maxima, Minima, Suprema und Infima. Wir werden zum ersten Mal dem griechischen Buchstaben ε begegnen, der besonders im dritten Semester eine große Rolle spielen wird. M sei stets eine Teilmenge der reellen Zahlen.

Def 2.1 1) $k \in \mathbb{R}$ heißt *obere Schranke von* $M \ :\Longleftrightarrow\ m \leq k \ \ \forall m \in M$
M heißt *nach oben beschränkt*, falls M eine obere Schranke besitzt.

2) $k \in \mathbb{R}$ heißt *untere Schranke von* $M \ :\Longleftrightarrow\ k \leq m \ \ \forall m \in M$
M heißt *nach unten beschränkt*, falls M eine untere Schranke besitzt.

3) M heißt *beschränkt*, falls M nach unten und nach oben beschränkt ist.

Beispiele: 1) {1,2,3} besitzt – neben unendlich vielen anderen – die unteren Schranken $-11,\ 0$ oder 1 und die oberen Schranken $3,\ \pi$ oder 50 300.

2) $\mathbb{Q} \subseteq \mathbb{R}$ ist nach unten und oben *unbeschränkt*.

3) $\mathbb{R}^+ := \{r \in \mathbb{R} \mid r > 0\}$ besitzt unendlich viele untere, aber keine obere Schranke und ist deshalb nicht beschränkt.

4) a und b sind Schranken der *Intervalle* $]a,b[:= \{r \in \mathbb{R} \mid a < r < b\},\ \ [a,b] := \{r \in \mathbb{R} \mid a \leq r \leq b\}$ und $[a,b[,\ ]a,b]$.

5) *Frage*: Welche Schranken hat $\{q \in \mathbb{Q} \mid q^2 < 2\}$?

Def 2.2 1) $k \in \mathbb{R}$ heißt *Maximum von* M, geschrieben $k = \max M \ :\Longleftrightarrow\ k \in M \ \wedge\ k$ ist obere Schranke.

2) $k \in \mathbb{R}$ heißt *Minimum von* M, geschrieben $k = \min M \ :\Longleftrightarrow\ k \in M \ \wedge\ k$ ist untere Schranke.

Wie wir an den Beispielen sehen, besitzt nicht jede Teilmenge von $\mathbb{R}$ ein Maximum oder ein Minimum, selbst wenn sie beschränkt ist. Falls Maximum oder Minimum existieren, sind sie eindeutig festgelegt:

Angenommen, a und b seien beide Maxima von $M \implies a \leq b$ und $b \leq a \implies (a < b$ oder $a = b)$ und $(a > b$ oder $a = b) \implies a = b$ (siehe (A1) von Def. 1.3)

Wenn $\max M$ existiert, so handelt es sich um die *kleinste obere Schranke*, analog ist $\min M$ die *größte untere Schranke*.

Beispiel: Sei $M := \{\frac{1}{n} \mid n \in \mathbb{N}\}$. M ist beschränkt mit größter unterer Schranke 0 und kleinster oberer Schranke 1. Während 1 gleichzeitig Maximum ist, also $1 = \max M$, existiert kein Minimum.

Größte untere und kleinste obere Schranken interessieren auch, falls sie *nicht* zu der betreffenden Menge gehören.

Def 2.3 1) $s \in \mathbb{R}$ heißt *Supremum von* M, geschrieben $s = \sup M \ :\Longleftrightarrow\ s$ ist kleinste obere Schranke.

2) $t \in \mathbb{R}$ heißt *Infimum von* M, geschrieben $t = \inf M \ :\Longleftrightarrow\ t$ ist größte untere Schranke.

Beispiel: Für $M := \{\frac{1}{n} \mid n \in \mathbb{N}\}$ ist $1 = \max M = \sup M$ und $0 = \inf M$ (Kein Minimum, siehe oben).

Wegen $s = \min\{k \in \mathbb{R} \mid k \text{ ist obere Schranke von } M\}$ sind Infimum und analog Supremum – falls existent – eindeutig bestimmt. Wenn Maximum oder Minimum existieren, ist $\max M = \sup M$ bzw. $\min M = \inf M$.

Satz 2.1 Sei s eine obere Schranke von $M \neq \emptyset$, $M \subseteq \mathbb{R}$. Dann gilt

$$s = \sup M \iff \forall\, \varepsilon > 0 \;\; \exists\, m \in M : \; s - \varepsilon < m$$

Beweis: „⇒“: Angenommen falsch, also $\exists\, \varepsilon > 0 : \; s - \varepsilon \geq m \quad \forall\, m \in M$.

$$\begin{aligned} &\Longrightarrow \quad s - \varepsilon \text{ ist obere Schranke und es gilt } s - \varepsilon < s \\ &\Longrightarrow \quad s \neq \sup M\,, \quad \text{Widerspruch.} \end{aligned}$$

„⇐“: Sei $t \in \mathbb{R}$ beliebig mit $t < s$, also $\varepsilon := s - t > 0$. (Wir haben $s - t > 0$ durch ε abgekürzt.)

$$\begin{aligned} &\Longrightarrow \quad \exists\, m \in M \;: \quad t = s - \varepsilon < m \\ &\Longrightarrow \quad t \text{ ist keine obere Schranke} \\ &\Longrightarrow \quad s = \sup M \end{aligned}$$

Einen analogen Satz kann man für untere Schranken angeben, dies soll in den Übungen geschehen.

Ausdrücke wie $\forall\, \varepsilon > 0$ oder $\exists\, \varepsilon > 0$ werden Ihnen in der Mathematik mit Sicherheit noch oft begegnen – einigen von Ihnen vielleicht zu oft. Der Buchstabe ε bedeutet für Mathematiker immer eine beliebig kleine positive reelle Zahl. Vielleicht verstehen Sie jetzt den kürzesten Witz, über den nur Mathematiker lachen können: *Sei* $\varepsilon \leq 0$.

Wie wir gesehen haben, existieren max und min nicht immer für beschränkte Teilmengen von $\mathbb{R}$. Auf Grund der Vollständigkeit von $\mathbb{R}$ ist dies für sup und inf anders, es gilt – hier ohne Beweis –

Satz 2.2 (Supremumsprinzip für reelle Zahlen)

Jede nichtleere nach oben beschränkte Menge besitzt in $\mathbb{R}$ ein Supremum.

Analog kann man natürlich auch das Infimumsprinzip angeben. Da $\mathbb{Q}$ nicht vollständig ist, gelten diese Aussagen nicht, wenn man nur die rationalen Zahlen betrachtet. (Wer kennt ein Gegenbeispiel?)

3 Folgen und (Über)abzählbarkeit

In einem früheren Kapitel haben wir Abbildungen als spezielle Relationen kennengelernt. Jetzt beschäftigen wir uns mit speziellen Abbildungen.

Def. 3.1 Sei M eine beliebige Menge. Eine Abbildung $a : \mathbb{N} \to M$ oder $a : \mathbb{N}_0 \to M$ heißt eine *Folge*.

Der Funktionswert $a(n)$ wird normalerweise a_n geschrieben, a_n ist also das *n–te Folgenglied*.[6] Man schreibt Folgen im Allgemeinen $(a_n)_{n\in\mathbb{N}}$ oder kürzer (a_n). Wenn klar ist, welche Folge gemeint ist, reicht auch

[6] Wenn nicht ausdrücklich etwas anderes gesagt wird, fangen wir mit a_1 an.

die Angabe der ersten Folgenglieder $a_1, a_2, a_3, \ldots$. In dieser Vorlesung werden wir uns hauptsächlich mit *reellen* Folgen beschäftigen, d.h. $M = \mathbb{R}$.

Zwei Folgen (a_n), (b_n) heißen gleich, wenn alle Folgenglieder übereinstimmen, d.h., wenn $a_n = b_n \ \forall n \in \mathbb{N}$ gilt.

Frage: Sind die Folgen 1,2,1,2,1,2,... und 2,1,2,1,2,1,... gleich?

Beispiele: 1) 1,2,3,.... Gemeint ist die Folge (a_n) mit $a_n := n$. Es handelt sich um die Folge der natürlichen Zahlen.

2) Für ein fest vorgegebenes $q \in \mathbb{R}$ sei $a_n := q^n$. Je nach dem speziellen Wert von q zeigt die Folge unterschiedliches Verhalten:

$q = 1$:	1,1,1,...	*konstante* Folge
$q = -1$:	-1,1,-1,1,...	*alternierende* Folge, das Vorzeichen wechselt ständig. Ferner *beschränkt*, da kein Glied größer als 1 oder kleiner als -1 ist.
$q = -2$:	-2,4,-8,16,...	ebenfalls alternierend, Folgenglieder werden beliebig groß bzw. klein.
$q = \frac{1}{2}$:	$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \ldots$	Folgenglieder nähern sich beliebig nahe der Zahl 0, erreichen sie jedoch nie.

3) Sei $a_1 := 1$, $a_{n+1} := a_n + 1$. Diese Folge ist *rekursiv* definiert: Man gibt das erste Glied konkret an und benennt die Vorschrift, wie die weiteren Glieder zu berechnen sind. Diese Folge kam übrigens bereits unter den anderen Beispielen vor.

4) Sei $a_1 = a_2 := 1$, $a_{n+2} := a_n + a_{n+1}$. Ebenfalls rekursiv definiert. Diese sogenannte *Fibonacci* – Folge, benannt nach *Leonardo von Pisa* (1175 – 1250(?)), kommt an vielen Stellen außerhalb und innerhalb der Mathematik vor. In der Vorlesung werden einige Beispiele hierfür genannt, die hier nicht wiedergegeben werden sollen[7].

5) Weitere Beispiele: $a_n := \left(1 + \frac{1}{n}\right)^n$, $\quad b_{n+1} := \frac{1}{2}\left(b_n + \frac{2}{b_n}\right)$ mit $b_1 = 2$,
$c_n := \frac{1}{2^n\sqrt{5}}\left((1+\sqrt{5})^n - (1-\sqrt{5})^n\right)$.

Wir müssen stets den Unterschied zwischen einer Folge (a_n) (immer unendlich viele Glieder) und der Menge ihrer Folgenglieder (Wertemenge, kann endlich sein) vor Augen haben.

In der ersten Vorlesung haben wir eine Bijektion $f : \mathbb{Z} \to \mathbb{N}$ kennengelernt. Wir wissen inzwischen, dass dann auch $f^{-1} : \mathbb{N} \to \mathbb{Z}$ bijektiv ist. Wir können somit die ganzen Zahlen als Glieder einer Folge auffassen, wegen der Bijektivität sind die Mengen $\mathbb{N}$ und $\mathbb{Z}$ gleichmächtig (siehe Def I.4.5).

Def 3.2 Eine beliebige Menge M heißt *abzählbar* : $\iff$ M ist endlich oder es gibt eine bijektive Abbildung von $\mathbb{N}$ bzw. $\mathbb{N}_0$ nach M. M heißt *überabzählbar* : $\iff$ M ist nicht abzählbar.

Unser Wissen aus der ersten Vorlesung können wir jetzt folgendermaßen als Satz formulieren:

Satz 3.1 $\mathbb{Z}$ ist abzählbar.

Für jede unendliche abzählbare Menge M gilt $|M| = |\mathbb{N}|$. Die Menge der Glieder einer beliebigen Folge ist stets abzählbar.

[7] In diesem Zusammenhang soll eventuell von Kaninchenvermehrung, Vorfahren einer Drohne, der Ananasfrucht, Sonnenblumen, einer beliebig langen Treppe und einem zerschnittenen Quadrat die Rede sein.

Beispiel: Die Menge $M = \{2, 4, 6, \ldots\}$ der geraden natürlichen Zahlen ist abzählbar. Um dies nachzuweisen, müssen wir eine bijektive Abbildung $f : \mathbb{N} \to M$ angeben; mit anderen Worten: Wir müssen die Elemente von $M = \{2, 4, 6, \ldots\}$ „durchnummerieren“.

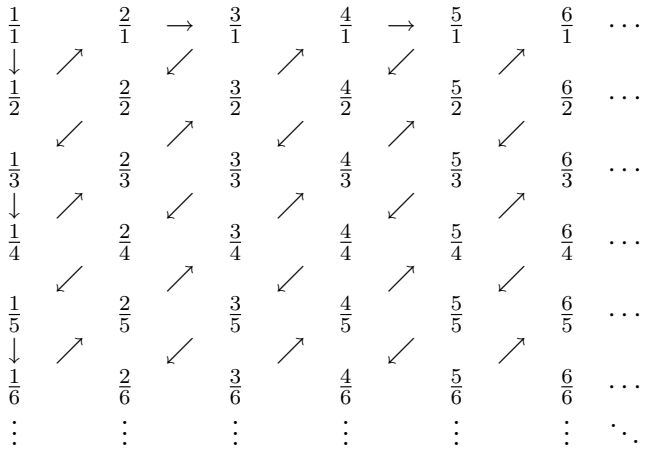
n	1	2	3	4	5	6	7	$\cdots$
$f(n)$	2	4	6	8	10	12	14	$\cdots$

oder $f(n) := 2n$.

Es gibt also genau so viele ganze wie natürliche Zahlen, obwohl $\mathbb{N}$ eine echte Teilmenge von $\mathbb{Z}$ ist. Noch überraschender ist die nächste Aussage:

Satz 3.2 $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$ ist abzählbar.

Beweis (nach *G. Cantor*): Wir zeigen zunächst, dass die Menge $\mathbb{Q}^+$ der positiven rationalen Zahlen (d.h., $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$) abzählbar ist. Wir machen dies mit dem sog. *ersten Cantorschen Diagonalverfahren* und ordnen die Elemente aus $\mathbb{Q}^+$ in dem folgenden Schema an. Wir folgen bei der Nummerierung der Elemente von $\mathbb{Q}^+$ (dies entspricht einer Bijektion $\mathbb{N} \to \mathbb{Q}^+$) den Pfeilen. Dabei überspringen wir alle Zahlen, die in der Nummerierung schon einmal (in anderer Darstellung) aufgetreten sind.



Auf diese Art erhält man eine bijektive Abbildung $\mathbb{N} \to \mathbb{Q}^+$, nämlich

$q_1 = 1$, $q_2 = \frac{1}{2}$, $q_3 = 2$, $q_4 = 3$, $q_5 = \frac{1}{3}$, $q_6 = \frac{1}{4}$, ...

Hieraus kann man dann nach folgendem Schema eine Abzählung aller Elemente von $\mathbb{Q}$ gewinnen:

0, q_1, $-q_1$, q_2, $-q_2$, q_3, $-q_3$, ...

Analog zum letzten Beweis können wir die Abzählbarkeit von Mengen wie $\mathbb{Q} \times \mathbb{Q}$ oder $\mathbb{Z}^n$ nachweisen. Die endliche Vereinigung von abzählbaren Mengen ist ebenfalls abzählbar. Es gibt aber auch Mengen, die man nicht mehr durchnummerieren kannn.

Satz 3.3 $\mathbb{R}$ ist überabzählbar.

Beweis: Wir argumenmtieren mit dem sog. *zweiten Cantorschen Diagonalverfahren* und zeigen, dass bereits die Menge I aller reeller Zahlen zwischen 0 und 1 nicht mehr abzählbar ist. Wir führen einen Widerspruchsbeweis und nehmen an, dass I doch abzählbar ist. Die Folge $r_1, r_2, r_3, \ldots$ sei das Resultat einer möglichen bijektiven Abbildung $\mathbb{N} \to I$.

Wir stellen die Zahlen $r_1, r_2, r_3, \ldots$ als unendliche Dezimalbrüche dar:

$$\begin{array}{lcll} r_1 & = & 0.s_{11}s_{12}s_{13}s_{14}s_{15} & \dots \\ r_2 & = & 0.s_{21}s_{22}s_{23}s_{24}s_{25} & \dots \\ r_3 & = & 0.s_{31}s_{32}s_{33}s_{34}s_{35} & \dots \\ r_4 & = & 0.s_{41}s_{42}s_{43}s_{44}s_{45} & \dots \\ \vdots & & & \ddots \end{array}$$

Allgemein:

$$r_i = 0.s_{i1}s_{i2}s_{i3}s_{i4}s_{i5} \quad \dots$$

Es bezeichnet $s_{ij} \in \{0, 1, 2, \dots, 9\}$ die j-te Stelle der Dezimalbruchdarstellung von r_i. Es sei vorausgesetzt, dass in diesen Dezimaldarstellungen nicht alle Ziffern von einer bestimmten Stelle an 9 sind, zum Beispiel schreiben wir $0.2000\dots$ anstelle von $0.19999\dots$.

Es sei nun $r \in]0, 1[$ die Zahl mit der Dezimaldarstellung $r = 0.s_1s_2s_3s_4s_5\dots$, wobei für $i \in \mathbb{N}$ gelte

$$s_i = \begin{cases} 1, & \text{falls } s_{ii} \neq 1 \\ 2, & \text{falls } s_{ii} = 1 \end{cases}$$

Es gilt $r \in I$, aber r kommt unter den Zahlen r_1, r_2, ... garantiert nicht vor, da sich r und r_i für jedes i an der i-ten Stelle unterscheiden ($i = 1, 2, \dots$). Dies ist ein Widerspruch, und Satz 3.3 ist somit bewiesen.

Frage: Warum kann man mit dem Beweis von Satz 3.3 nicht analog die „Überabzählbarkeit“ von $\mathbb{Q}$ nachweisen?

Aufgrund des letzten Satzes wissen wir, dass es mehr irrationale als rationale Zahlen gibt. Wäre $\mathbb{R}\backslash\mathbb{Q}$ nämlich abzählbar, müsste auch $\mathbb{R} = \mathbb{R}\backslash\mathbb{Q} \cup \mathbb{Q}$ abzählbar sein. Unmathematisch formuliert können wir sagen, dass bereits die Anzahl der irrationalen Zahlen zwischen 0 und 1 größer ist als die aller rationalen Zahlen.

In den Übungen wird die Gleichmächtigkeit von zwei beliebigen echten reellen Intervallen gezeigt. Jedes noch so kleine Intervall enthält also überabzählbar viele reelle Zahlen. Trotzdem ist jede Menge paarweise disjunkter echter Intervalle höchstens abzählbar, da es in jedem Intervall eine rationale Zahl gibt und $\mathbb{Q}$ abzählbar ist! Kaum vorstellbar ist ferner, dass man in beliebiger Nähe jeder der überabzählbar vielen reellen Zahlen stets auch unendlich viele rationale Zahlen findet, obwohl es hiervon „nur“ abzählbar viele gibt!

Satz 3.4 Sei $r \in \mathbb{R}$ beliebig. Dann gilt: $\forall\, \varepsilon > 0 \;\; \exists\, q \in \mathbb{Q} : \;\; r - \varepsilon < q < r + \varepsilon$

Beweis: Wir haben am Ende von §1 festgestellt, dass es zu jeder positiven reellen Zahl, also auch zu jedem $\varepsilon > 0$, ein $m \in \mathbb{N}$ gibt mit $\frac{1}{m} < \varepsilon$. Wir suchen ein $q \in \mathbb{Q}$ mit $q - \frac{1}{m} \leq r \leq q + \frac{1}{m}$, denn dann gilt auch $r - \varepsilon < r - \frac{1}{m} \leq q \leq r + \frac{1}{m} < r + \varepsilon$.

1. Fall: $r \geq 0$. Zu dem Produkt mr gibt es natürliche Zahlen k mit $mr < k$: Sei oBdA k die kleinste natürliche Zahl mit dieser Eigenschaft, also es gelte $k - 1 \leq mr < k$.

Beh.: $q := \frac{k}{m}$ ist die gesuchte rationale Zahl.

Bew.: $q - \frac{1}{m} \leq r < \frac{k}{m} = q \leq q + \frac{1}{m}$.

2.Fall: $r < 0$. Dann ist $-r > 0$, nach dem 1. Fall existiert ein $q \in \mathbb{Q}$ mit $-r - \varepsilon < q < -r + \varepsilon \iff r + \varepsilon > -q > r - \varepsilon$. Also ist $-q \in \mathbb{Q}$ die gesuchte Zahl.

Aufgrund dieser Tatsache sagt man auch, dass die rationalen Zahlen *dicht* in der Menge der reellen Zahlen liegen.

Zum Schluss stellen wir fest, dass es auch verschiedenmächtige überabzählbare Mengen gibt.

Satz 3.5 Sei M eine beliebige Menge. Dann gilt $|M| \neq |\mathrm{Pot}\, M|$.

Beweis: Für endliche Mengen folgt die Behauptung aus Satz I.5.3: $|M| = n \neq 2^n = |\mathrm{Pot}\, M|$.

Für unendliche Mengen argumentieren wir indirekt. Angenommen, es gibt eine Bijektion $f : M \to \mathrm{Pot}\, M$, bei der jedem Element $x \in M$ eine Teilmenge $f(x) \subset M$ zugeordnet wird. Wir interessieren uns für diejenigen $x \in M$, die nicht in ihrem Bild $f(x)$ liegen. Sei $A := \{x \in M \mid x \notin f(x)\} \subseteq M$. Da f nach Annahme bijektiv ist, hat auch die Menge A ein Urbild $a \in M$. Wir untersuchen, ob a in A liegt.

1. Fall $a \in A$: Geht nicht wegen $a \in A = f(a) \implies a \notin A$

2. Fall $a \notin A$: Geht nicht wegen $a \notin A = f(a) \implies a \in A$

Damit ist die Annahme der Existenz einer Bijektion zwischen M und ihrer Potenzmenge ad absurdum geführt, diese Mengen sind nicht gleichmächtig.

Dieser Beweis erinnert an das Dilemma des Friseurs, der genau die Personen rasieren soll, die sich nicht selbst rasieren!

Wir beenden diesen Abschnitt mit einer Bemerkung, die in der Vorlesung eventuell nicht zur Sprache kommen wird. Wir haben festgestellt, dass $\mathbb{N}$ abzählbar unendlich und $\mathbb{R}$ überabzählbar unendlich ist, und dass es nach Satz 3.5, angewandt auf $M = \mathbb{R}$, überabzählbare Mengen verschiedlicher Mächtigkeiten gibt. Die interessante Frage ist nun: Gibt es Mengen, deren Mächtigkeit zwischen der von $\mathbb{N}$ und $\mathbb{R}$ liegt?[8] Je nach Ihrer Gemütslage ist die Antwort hierauf spannend oder frustrierend: Die *Kontinuumshypothese* besagt: Solche Mengen gibt es nicht, aber dies kann man im Rahmen der üblichen Mengenlehre weder beweisen, noch widerlegen!

4 Über $\mathbb{Z}$: Teilbarkeit, Primzahlen und Euklidischer Algorithmus

In diesem Abschnitt sollen einige Dinge, die wir bisher als „Schulwissen“ bezeichnet haben, näher untersucht werden. Mit kleinen lateinischen Buchstaben sind stets ganze Zahlen gemeint.

Def 4.1 Man nennt a einen *Teiler von* $b :\iff \exists\, c \in \mathbb{Z} \,:\, b = c \cdot a \quad (a, b, c \in \mathbb{Z})$.

Ist a ein Teiler von b so sagt man auch a *teilt* b, geschrieben $a \mid b$. $a \nmid b$ bedeutet, dass a kein Teiler von b ist.

Beispiel: $5 \mid 15, \quad 5 \nmid -7$

Einige Eigenschaften der Teilbarkeitsbeziehung $\mid$ sind:

Satz 4.1
(1) Gilt $a \mid b$ und $b \mid c$, dann 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 $c \cdot a \mid c \cdot b$ mit $c \neq 0$ folgt $a \mid b$.
(4) Aus $a \mid b_1$ und $a \mid b_2$ folgt $a \mid c_1 \cdot b_1 + c_2 \cdot b_2$ für beliebige ganze Zahlen c_1, c_2.

[8] Man kann zeigen, dass das im Beweis von Satz 3.3 benutzte Intervall gleichmächtig zu $\mathbb{R}$ ist.

Von der Richtigkeit der Aussagen (1) – (4) kann man sich leicht überzeugen; (1) sieht man beispielsweise so ein: $a \mid b$ bedeutet, dass $b = d \cdot a$ für ein $d \in \mathbb{Z}$ gilt; $b \mid c$ bedeutet, dass $c = e \cdot b$ für ein $e \in \mathbb{Z}$ gilt. Durch Einsetzen erhält man $c = e \cdot d \cdot a$; also gilt $a \mid c$. Wenn Sie sich an den Abschnitt über Relationen erinnern: Die Teilbarkeitsbeziehung ist eine Ordnungsrelation auf $\mathbb{Z}$.

Die sogenannten *trivialen Teiler* jeder ganzen Zahl a sind $1, -1, a$ und $-a$.

Def 4.2 Eine natürliche Zahl $n \geq 2$ heißt *Primzahl*, wenn n nur die trivialen Teiler $1, -1, n$ und $-n$ besitzt.

Ist $n \geq 2$ eine natürliche Zahl und ist p eine Primzahl, für die $p \mid n$ gilt, so heißt p ein *Primteiler* von n. Jede natürliche Zahl $n \geq 2$ besitzt mindestens einen Primteiler, da die kleinste natürliche Zahl $p \geq 2$, die n teilt, ein solcher Primteiler ist.

Die ersten zwölf Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, eine etwas größere Primzahl ist 845 100 400 152 152 934 331 135 470 251.

Wieviele Primzahlen gibt es insgesamt? Schon seit langem ist die Antwort bekannt:

Satz 4.2 (*Euklid*, um 300 v.Chr.)
Es gibt unendlich viele Primzahlen.

Beweis: Wir nehmen an, es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$, und führen dies zu einem Widerspruch. Sei $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Die Zahl $a+1$ hat, wie jede natürliche Zahl ≥ 2, einen Primteiler p. Da $p_1, p_2, \ldots, p_n$ nach unserer Annahme die einzigen Primzahlen sind, muss $p = p_i$ für ein i gelten, d.h., $p_i \mid a+1$. Wegen $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ gilt $p_i \mid a$. Es ist aber unmöglich, dass p_i sowohl $a+1$ als auch a teilt. Damit haben wir aus unserer Annahme, es gebe nur endlich viele Primzahlen, einen Widerspruch hergeleitet.

Leider ist dies ein reiner *Existenzbeweis*: Wir wissen zwar, dass es unendlich viele Primzahlen gibt, Satz und Beweis helfen aber nicht weiter, wenn wir eine konkrete Primzahl suchen. Primzahlen gehören zu den willkürlichsten Objekten in der Mathematik. So schreibt der bekannte Mathematiker *D. Zagier*: „Sie wachsen wie Unkraut unter den natürlichen Zahlen, scheinbar keinem anderen Gesetz als dem Zufall unterworfen, und kein Mensch kann voraussagen, wo wieder eine sprießen wird, noch einer Zahl ansehen, ob sie prim ist oder nicht“.[9] Vor dem Einsatz elektronischer Rechenanlagen war die größte bekannte Primzahl $2^{127} - 1$, bestehend aus 39 Ziffern, gefunden im Jahr 1876. Erst 75 Jahre später wurde sie übertroffen. Beim Schreiben dieser Zeilen (September 2009) ist die größte bekannte Primzahl $2^{43112609} - 1$. Sie wurde im letzten Jahr entdeckt und besteht aus 12 978 189 Ziffern.

Der Exponent 43 112 609 ist übrigens selbst eine Primzahl. Primzahlen von der Gestalt $2^p - 1$ heißen *Mersennesche Primzahlen*. Für $p = 2, 3, 5$ erhält man so die Primzahlen $3, 7, 31$. *Frage*: Was gilt für $p = 7$ oder $p = 11$?

Ohne Beweis merken wir uns folgenden grundlegenden Satz über die Existenz und Eindeutigkeit der Primfaktorzerlegung:

Satz 4.3 Jede natürliche Zahl $n \geq 2$ ist bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellbar:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m \qquad (m \geq 1)$$

[9] Zitat entnommen aus D. Zagier: Die ersten 50 Millionen Primzahlen, Basel 1977

Hierbei sind die Primfaktoren $p_1, p_2, \ldots, p_m$ in der Regel nicht alle verschieden.

Beispiel: $6600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11, \quad 126 = 2 \cdot 3 \cdot 3 \cdot 7$

Zur besseren Übersicht fasst man gleiche Faktoren zusammen: $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$, $126 = 2 \cdot 3^2 \cdot 7$. Das Ergebnis von Satz 4.3 lautet somit:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$$

Hierbei sind die p_i *verschiedene* Primzahlen ($\alpha_1, \ldots, \alpha_s \in \mathbb{N}$).

Wir wollen uns nun mit den Begriffen *größter gemeinsamer Teiler* (ggT) und *kleinstes gemeinsames Vielfaches* (kgV) beschäftigen.

Gilt $c \mid a$ und $c \mid b$, so heißt c ein *gemeinsamer Teiler* von a und b. Als eine Folgerung aus Satz 4.3 lässt sich zeigen: Zu je zwei natürlichen Zahlen a, b gibt es immer einen gemeinsamen Teiler $t \in \mathbb{N}$ derart, dass für jeden gemeinsamen Teiler d von a und b gilt: $d \mid t$. Man nennt t den *größten gemeinsamen Teiler* von a und b, geschrieben $\mathrm{ggT}(a, b)$.

Ist die Primfaktorzerlegung von a und b gegeben, so kann man den $\mathrm{ggT}(a, b)$ leicht bestimmen.

Beispiel: $a = 2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13^4$, $b = 2^2 \cdot 5 \cdot 7^2 \cdot 13^3 \cdot 17 \cdot 23$, $\mathrm{ggT}(a, b) = 2^2 \cdot 5 \cdot 7 \cdot 13^3$.

Gilt $a \mid c$ und $b \mid c$, so heißt c ein *gemeinsames Vielfaches* von a und b. Ebenfalls als Folgerung aus Satz 4.3 erhält man: Zu je zwei natürlichen Zahlen a, b gibt es immer ein gemeinsames Vielfaches $v \in \mathbb{N}$ derart, dass für jedes andere gemeinsame Vielfache w von a und b gilt: $v \mid w$. Man nennt v das *kleinste gemeinsame Vielfache* von a und b, geschrieben $\mathrm{kgV}(a, b)$.

Beispiel: Für a und b wie vorhin ist $\mathrm{kgV}(a, b) = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 13^4 \cdot 17 \cdot 23$.

Es gilt allgemein

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b \qquad (*)$$

Sind a und b gegeben, so genügt es, $\mathrm{ggT}(a, b)$ zu berechnen, $\mathrm{kgV}(a, b)$ kann dann aus $(*)$ bestimmt werden.

Wir kommen zum *Euklidischen Algorithmus*, mit dem man relativ einfach den größten gemeinsamen Teiler $\mathrm{ggT}(m, n)$ berechnen kann, auch wenn keine Primfaktorzerlegung von m oder n bekannt ist. Hierzu benötigen wir die folgende Feststellung über die „Division mit Rest“:

Satz 4.4 Zu $m \in \mathbb{Z}$ und $n \in \mathbb{N}$ gibt es immer eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < n$, so dass $m = q \cdot n + r$ gilt. (Man nennt q den *Quotienten* und r den *Rest*.)

Beweis: 1. *Existenz*: Sei $q := \max\{z \in \mathbb{Z} \mid z \leq \frac{m}{n}\} =: \lfloor \frac{m}{n} \rfloor$, also $q \leq \frac{m}{n} < q + 1$. Damit ist $nq \leq m < nq + n \iff 0 \leq m - nq < n$. Für $r := m - nq$ folgt $0 \leq r < n$ und $m = nq + r$.

2. *Eindeutigkeit*: Sei $m = nq' + r'$ mit $q', r' \in \mathbb{Z}$ und $0 \leq r' < n$, also $\frac{m}{n} = q' + \frac{r'}{n}$ mit $0 \leq \frac{r'}{n} < 1$. Dies geht nur für $q' = \lfloor \frac{m}{n} \rfloor = q$, und damit ist auch $r' = m - nq = r$.

Beispiele: 1) $m = 27$, $n = 12$: Es ist $27 = 2 \cdot 12 + 3$, d.h. $q = 2$ und $r = 3$.

2) $m = -8$, $n = 3$: Es ist $-8 = (-3) \cdot 3 + 1$, d.h. $q = -3$ und $r = 1$.

Dem Euklidischen Algorithmus liegt die folgende einfache Beobachtung zu Grunde:

Satz 4.5 Für $m = q \cdot n + r \quad (0 \le r < n)$ folgt $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r)$.

Beweis: Es gelte $m = q \cdot n + r$. Ist t ein gemeinsamer Teiler von n und r, so auf Grund von Satz 4.1 (4) auch von m und n.

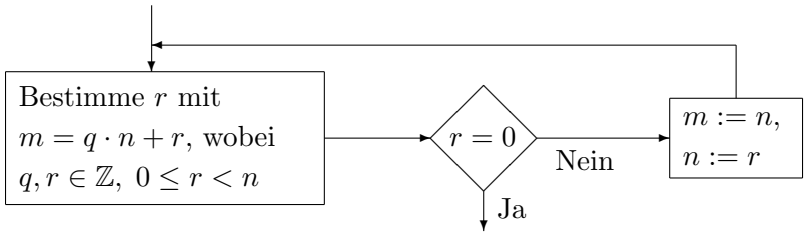
Ist umgekehrt t ein gemeinsamer Teiler von m und n, so ist wegen $r = m - q \cdot n$ gemäß (4) t auch ein gemeinsamer Teiler von n und r. Die Menge der gemeinsamen Teiler von n und r ist gleich der Menge der gemeinsamen Teiler von m und n; insbesondere gilt $\mathrm{ggT}(n, r) = \mathrm{ggT}(m, n)$.

Es folgt ein „Kochrezept“ zur Anwendung des *Euklidischen Algorithmus*, es sei oBdA $m \ge n$:

1. Teile m durch n und bestimme den Rest r (d.h., bestimme r, so dass gilt $m = q \cdot n + r$, wobei $q, r \in \mathbb{Z},\ 0 \le r < n$).

2. Im Fall $r = 0$ ist man fertig, n ist der gesuchte Wert.

3. Andernfalls setze man $m := n$, $n := r$ und gehe nach **1.**



Beispiel: $m = 816, n = 294$:

$$\begin{aligned} 816 &= 2 \cdot 294 + 228 \\ 294 &= 1 \cdot 228 + 66 \\ 228 &= 3 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \end{aligned} \qquad \Rightarrow\ \mathrm{ggT}(816, 294) = 6$$

Der Algorithmus endet nach endlich vielen Schritten, da bei jeder Ausführung der Anweisung $n := r$ der Wert von n verkleinert wird.

Dass der Euklidische Algorithmus tatsächlich den $\mathrm{ggT}(m, n)$ berechnet, lässt sich wie folgt einsehen: Ist $r > 0$, so wird in **3.** die Anweisung $m := n$, $n := r$ ausgeführt und anschließend nach **1.** gegangen. Dies bedeutet, dass man die Aufgabe, den $\mathrm{ggT}(m, n)$ zu berechnen, durch die Aufgabe, den $\mathrm{ggT}(n, r)$ zu berechnen, ersetzt hat; wegen Satz 4.5 gilt aber $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r)$. Ist $r = 0$, so gilt $m = q \cdot n$, d.h., n ist ein Teiler von m; also ist in diesem Fall n der größte gemeinsame Teiler von m und n.

Exkurs: Modulare Arithmetik

Die Berechnung der Reste bei der Division einer natürlichen oder ganzen Zahl a durch eine natürliche Zahl n ist in der Grundschule ganz wichtig. Wie ein solches Ergebnis notiert wird, ist umstritten. Eine Möglichkeit ist $a : n = q$ Rest r. Manchmal interessiert der ganzzahlige Anteil q nicht, dann schreibt man einfach

$$r = a \bmod n \qquad \text{oder} \qquad r \equiv a \bmod n \quad \text{(wie im Abschnitt über Relationen)}$$

Beispiel: Für $n = 7$ und $a = 12$ erhalten wir wegen $12 = 1 \cdot 7 + 5$ den Rest 5, also $5 = 12 \bmod 7$, genauso wie für $b = -9$: Hier ist wegen $-9 = (-2) \cdot 7 + 5$ ebenfalls $5 = -9 \bmod 7$.

Verschiedene Zahlen können bei der Division durch n den gleichen Rest hinterlassen. Unter Beachtung von Satz 4.4 wissen wir, dass die Menge der möglichen Reste „mod n“ genau der Menge $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ entspricht.

Auf dieser Menge führen wir eine Addition $+_n$ und eine Multiplikation $\cdot_n$ wie folgt ein:

$$a +_n b := (a + b) \bmod n\,, \qquad a \cdot_n b := (a \cdot b) \bmod n$$

Beispiele: $4 +_6 5 = 3$, $4 \cdot_6 5 = 2$.

Diese Rechnungen kann man auch folgendermaßen notieren: $4 + 5 \equiv_6 3$, $4 \cdot 5 \equiv_6 2$.

Ohne Beweis halten wir folgenden Satz fest:

Satz 4.6 Für jedes $n \in \mathbb{N}$ ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein Ring.

Falls n eine Primzahl ist, handelt es sich sogar um einen Körper.

Moduloaddition und –multiplikation sind zum Glück recht einfach zu bewerkstelligen, da man bei jedem einzelnen Rechenschritt „modulo n reduzieren“ darf, wir wollen dies lediglich an einem Beispiel vorführen:

Beispiel: Welcher Rest entsteht beim Dividieren von 5^4 durch 7? Mit anderen Worten: Wie berechnet man $5^4 \bmod 7$?

$$\begin{aligned} 5^4 \bmod 7 &= (5^2 \cdot 5^2) \bmod 7 = (5^2 \bmod 7) \cdot (5^2 \bmod 7) \\ &= (25 \bmod 7) \cdot (25 \bmod 7) = (4 \bmod 7) \cdot (4 \bmod 7) \\ &= (4 \cdot 4) \bmod 7 = 16 \bmod 7 = 2 \end{aligned}$$

Unter Verwendung der abkürzenden Schreibweise $a \equiv_n b :\iff b = a \bmod n$ sieht unsere Rechnung bei einem anderen Zahlenbeispiel wie folgt aus:

$$2^{10} = 2^4 \cdot 2^4 \cdot 2^2 = 16 \cdot 16 \cdot 4 \equiv_5 1 \cdot 1 \cdot 4 = 4$$

Teilt man 2^{10} durch 5, erhält man der Rest 4.

5 Teilbarkeitskriterien und g–adische Darstellung

Zunächst sollen aus der Schule bekannte Teilbarkeitsregeln bewiesen werden, dann werden wir uns mit anderen Zahlsystemen als dem Dezimalsystem beschäftigen.

Beispiel: Ist 26 333 384 durch 7, 8, 9 oder 11 teilbar?

Im vorherigen Kapitel haben wir für Teilbarkeit unter anderen folgende Eigenschaft angegeben (hier in Kurzform wiedergegeben):

$$a \mid b \text{ und } a \mid c \implies a \mid (\alpha b + \beta c) \qquad (*)$$

Bevor wir mit den Kriterien beginnen, rufen wir uns ins Gedächtnis, dass beispielsweise $n = 123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$ bedeutet.

Satz 5.1 Sei $n = \sum_{i=0}^{r} a_i \cdot 10^i$ mit $a_i \in \{0, 1, 2, \ldots, 9\}$ und $r \in \mathbb{N}$. Dann ist

(1) $2 \mid n \iff 2 \mid a_0$

(2) $4 \mid n \iff 4 \mid (10a_1 + a_0)$

(3) $8 \mid n \iff 8 \mid (100a_2 + 10a_1 + a_0)$

(4) $5 \mid n \iff 5 \mid a_0$

Beweis: (1) Für $b_i \in \{0, 1, 2, \ldots, 9\}$ und $r \in \mathbb{N}$ folgt wegen $2 \mid 10$ aus $(*)$ $\quad 2 \mid \sum_{i=1}^{r} b_i \cdot 10^i$.

„$\Rightarrow$“: Wir wenden $(*)$ auf $2 \mid n$ und $2 \mid \sum_{i=1}^{r} a_i \cdot 10^i$ an und erhalten $2 \mid \left(n - \sum_{i=1}^{r} a_i \cdot 10^i = a_0\right)$.

„$\Leftarrow$“: Wir wenden $(*)$ auf $2 \mid a_0$ und $2 \mid \sum_{i=1}^{r} a_i \cdot 10^i$ an und erhalten $2 \mid \left(a_0 + \sum_{i=1}^{r} a_i \cdot 10^i = n\right)$.

Die Beweise zu (2) – (4) verlaufen analog, man beachte nur $2^i \mid 10^i$ für alle $i \in \mathbb{N}$ (Übung).

Um Teilbarkeitsregeln für 3, 9 und 11 angeben zu können, führen wir eine Hilfsbetrachtung durch.

Satz 5.2 Für $n \in \mathbb{N}$ gilt

(1) $3 \mid (10^n - 1)$

(2) $9 \mid (10^n - 1)$

(3) $11 \mid (10^n - (-1)^n)$

Beweis durch vollständige Induktion:

Zu (1): $n = 1$: Es gilt $3 \mid 9$. $\quad n \mapsto n + 1$: Sei $10^n - 1 = a \cdot 3$, dann ist
$10^{n+1} - 1 = (9 + 1) \cdot 10^n - 1 = 9 \cdot 10^n + 10^n - 1 = 3 \cdot (3 \cdot 10^n) + a \cdot 3 = (3 \cdot 10^n + a) \cdot 3$.
(Oder $\quad 10^{n+1} - 1 = 10 \cdot 10^n - 1 = 10 \cdot (10^n - 1) + 10 - 1 = 10 \cdot a \cdot 3 + 9 = (10 \cdot a + 3) \cdot 3$)

Zu (2): Eine fast wörtliche Übertragung des Beweises von (1), einfache Übung.

Zu (3): $n = 1$: Es gilt $11 \mid 11$. $\quad n \mapsto n + 1$: Sei $10^n - (-1)^n = a \cdot 11$, dann ist
$10^{n+1} - (-1)^{n+1} = 10 \cdot (10^n - (-1)^n) + 10 \cdot (-1)^n - (-1)^{n+1} = 10 \cdot a \cdot 11 + (-1)^n \cdot 11 = b \cdot 11$

Jetzt können wir die bekannten *Quersummenregeln* für 3 und 9 und die weniger bekannte *alternierende Quersummenregel* für 11 beweisen:

Satz 5.3 Sei $n = \sum_{i=0}^{r} a_i \cdot 10^i$ mit $a_i \in \{0, 1, 2, \ldots, 9\}$ und $r \in \mathbb{N}$. Dann ist

(1) $3 \mid n \iff 3 \mid \sum_{i=0}^{r} a_i$

(2) $9 \mid n \iff 9 \mid \sum_{i=0}^{r} a_i$

(3) $11 \mid n \iff 11 \mid \sum_{i=0}^{r} (-1)^i \cdot a_i$

Beweis: (1): „⇒“: Nach Voraussetzung ist 3 ein Teiler von $n = \sum_{i=0}^{r} a_i \cdot 10^i$. Da 3 nach Satz 5.2 für $i = 1, 2, \ldots, r$ ein Teiler von $10^i - 1$ ist, folgt aus $(*)$ (Seite 36), dass 3 auch ein Teiler von $\sum_{i=1}^{r} a_i \cdot \left(10^i - 1\right)$ ist. Erneut $(*)$ angewandt, erhalten wir

$$3 \mid \left(n - \sum_{i=1}^{r} a_i \cdot (10^i - 1) = \sum_{i=0}^{r} a_i \right)$$

„⇐“: Wir wenden $(*)$ auf $3 \mid \sum_{i=1}^{r} a_i \cdot \left(10^i - 1\right)$ und $3 \mid \sum_{i=0}^{r} a_i$ an und erhalten

$$3 \mid \left(\sum_{i=1}^{r} a_i \cdot (10^i - 1) + \sum_{i=0}^{r} a_i = \sum_{i=1}^{r} a_i \cdot 10^i + a_0 = n \right)$$

Mit den analogen Beweisen von (2) und (3) beschäftigen wir uns in den Übungen.

Auch für 7 kann man ein Teilbarkeitskriterium angeben. Wir verzichten auf die formale Wiedergabe der Beweise und geben nur die Ergebnisse an:

Satz 5.4 Für $n \in \mathbb{N}$ gilt $7 \mid \left(10^{3n} - (-1)^n\right)$

Diesen Satz beweist man wie Satz 5.2 durch vollständige Induktion. Um die Aussage des folgenden Teilbarkeitskriteriums für 7 zu verstehen, muss man sich die Bedeutung von $\lfloor \frac{r}{3} \rfloor$ (kam im Beweis von Satz 4.4 vor) ins Gedächtnis zurückrufen.[10]

Satz 5.5 Sei $n = \sum_{i=0}^{r} a_i \cdot 10^i$ mit $a_i \in \{0, 1, 2, \ldots, 9\}$ und $r \in \mathbb{N}$. Dann ist

$$7 \mid n \quad \Longleftrightarrow \quad 7 \mid \sum_{i=0}^{\lfloor \frac{r}{3} \rfloor} (-1)^i \cdot \left(a_{3i+2} \cdot 10^2 + a_{3i+1} \cdot 10 + a_{3i} \right)$$

(Falls nötig, setze man $a_{r+1} = a_{r+2} = 0$)

Beispiele: 1) $7 \mid 12\,208$: Es ist $\lfloor \frac{r}{3} \rfloor = \lfloor \frac{4}{3} \rfloor = 1$, also
$\sum_{i=0}^{1} (-1)^i \cdot \left(a_{3i+2} \cdot 10^2 + a_{3i+1} \cdot 10 + a_{3i} \right) = (2 \cdot 10^2 + 0 \cdot 10 + 8) - (0 \cdot 10^2 + 1 \cdot 10 + 2) = 208 - 12 = 196,$
und diese Zahl ist ein Vielfaches von 7.

2) $7 \nmid 1\,204\,208$, denn $208 - 204 + 1$ ist kein Vielfaches von 7

3) *Frage*: Für welche Ziffer x gilt $7 \mid 23\,304\,10x$?

Teilbarkeitsregeln für 7 können bei der Zuordnung von Wochentagen zu Datumsangaben (wer ist ein Sonntagskind?) nützlich sein.

Jetzt können wir die eingangs gestellte Frage nach der Teilbarkeit von $n = 26\,333\,384$ durch 7, 8, 9 oder 11 beantworten:

[10] Um Ihnen mühsames Zurückblättern zu ersparen: $\lfloor a \rfloor := \max\{z \in \mathbb{Z} \mid z \leq a\}$.

$8 \mid n$, denn $384 = 48 \cdot 8$

$9 \nmid n$, denn $2+6+3+3+3+3+8+4 = 32$ ist kein Vielfaches von 9

$11 \mid n$, denn $4-8+3-3+3-3+6-2 = 0$ ist ohne Rest durch 11 teilbar

$7 \mid n$, denn $384 - 333 + 26 = 77$ ist ohne Rest durch 7 teilbar.

Bei den Überlegungen zu den Teilbarkeitskriterien haben wir eine Zahlendarstellung mit Hilfe von Zehnerpotenzen benutzt: $n = \sum_{i=0}^{r} a_i \cdot 10^i = \sum_{i=0}^{r} a_{r-i} \cdot 10^{r-i}$

Beispiel: $n = 345 = 3 \cdot 10^2 + 4 \cdot 10 + 5 \cdot 10^0$

Diese Darstellung an Hand des Dezimalsystems ist nicht selbstverständlich. In früheren Kulturkreisen (Maya, Babylonier) wurden andere Zahlen als 10 zur Grundzahl von Rechnungen gewählt. Computer rechnen intern mit Zahlen, die aus Zweierpotenzen zusammengesetzt sind. Es gibt also gute Gründe, sich zumindest kurz mit anderen Darstellungen zu beschäftigen und vor allem zu klären, wie man Zahlen in andere Systeme umformen kann.

In den folgenden Aussagen bis zum Ende dieses Kapitels steht der Buchstabe $g \in \mathbb{N}\backslash\{1\}$ für die verschiedenen Grundzahlen. Zunächst etwas Theorie:

Satz 5.6 Sei x eine beliebige reelle Zahl und $g \in \mathbb{N}\backslash\{1\}$. Dann gibt es $m \in \mathbb{N}$ mit $x < g^m$.

Beweis: Wie wir wissen, gibt es zu jeder reellen Zahl eine größere natürliche Zahl, also auch ein $n \in \mathbb{N}$ mit $n > \frac{x}{g-1}$. Wir zeigen, dass n die von m verlangte Eigenschaft besitzt:

$$\frac{x}{g-1} < n \quad \Longleftrightarrow \quad x < n(g-1) < 1 + n(g-1)$$

Auf $g-1$ können wir die Bernoullische Ungleichung (Satz I.5.6) anwenden und erhalten

$$x < 1 + n(g-1) \leq (1 + (g-1))^n = g^n$$

Ohne Beweis halten wir fest:

Korollar Sei $r \in \mathbb{N}$ und $g \in \mathbb{N}\backslash\{1\}$. Dann gibt es genau ein $n \in \mathbb{N}_0$ mit $g^n \leq r < g^{n+1}$.

Bei den folgenden Aussagen sei $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$, beispielsweise ist $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

Satz 5.7 Seien $r, m \in \mathbb{N}_0$ und $g \in \mathbb{N}\backslash\{1\}$ mit $r < g^{m+1}$. Dann existiert genau ein $z_m \in \mathbb{Z}_g$ und genau ein $r_m \in \mathbb{Z}_{g^m}$ mit $r = z_m \cdot g^m + r_m$.

Beweis: Da aus Satz 4.4 die eindeutige Existenz von $z_m, r_m \in \mathbb{Z}$ und $r_m < g^m$ folgt, ist nur noch $z_m \in \mathbb{Z}_g$ zu zeigen. Dies geschieht indirekt:

Angenommen, $z_m < 0 \quad \Rightarrow \quad r_m = r - z_m \cdot g^m \geq g^m$, Widerspruch zu Satz 4.4.

Angenommen, $z_m \geq g \quad \Rightarrow \quad r = z_m \cdot g^m + r_m \geq g^{m+1}$, Widerspruch zur Voraussetzung.

Beispiel: $r = 123,\ g = 5,\ m = 2$ erfüllen die Voraussetzung $123 < 5^3$. Die eindeutig bestimmten Zahlen z_2 und r_2 sind 4 bzw. 23: $\quad 123 = 4 \cdot 5^2 + 23$.

Sehen wir uns Satz 5.7 etwas genauer für den interessanten Fall $g^m \le r < g^{m+1}$ mit $m > 1$ an. Da in der gefundenen Darstellung $r = z_m \cdot g^m + r_m$ auch $r_m < g^m$ gilt, können wir den Satz erneut anwenden, und zwar auf r_m, $m-1$ und g. Wir erhalten eindeutig bestimmte Zahlen $z_{m-1} \in \mathbb{Z}_g$ und $r_{m-1} \in \mathbb{Z}_{g^{m-1}}$ mit $r_m = z_{m-1} \cdot g^{m-1} + r_{m-1}$. Falls $m - 1 > 0$ ist, können wir das Spiel fortsetzen. Den gleichen Satz auf r_{m-1}, $m-2$, g angewandt ergibt $r_{m-1} = z_{m-2} \cdot g^{m-2} + r_{m-2}$ mit $r_{m-2} \in \mathbb{Z}_{g^{m-2}}$, usw.

Beispiel (Fortsetzung): $123 = 4 \cdot 5^2 + 23, \qquad 23 = 4 \cdot 5^1 + 3, \qquad 3 = 3 \cdot 5^0 + 0$

Wir fassen zusammen: Sind r und g gegeben, gibt es genau ein n mit $g^n \le r < g^{n+1}$. Mehrfache Anwendung von Satz 5.7 liefert $n+1$ Zahlen $z_n, z_{n-1}, \ldots, z_0 \in \mathbb{Z}_g$ mit $r = \sum_{i=0}^{n} z_{n-i} \cdot g^{n-i}$.

Beispiel (Fortsetzung): $123 = 4 \cdot 5^2 + 4 \cdot 5^1 + 3 \cdot 5^0$

Als Satz formuliert lauten unsere Erkenntnisse

Satz 5.8 Sei $r \in \mathbb{N}$, $n \in \mathbb{N}_0$ und $g \in \mathbb{N}\backslash\{1\}$ mit $g^n \le r < g^{n+1}$. Dann existieren eindeutig bestimmte Zahlen $z_i \in \mathbb{Z}_g$ mit

$$r = \sum_{i=0}^{n} z_{n-i} \cdot g^{n-i}$$

Def. 5.1 Sei $g \in \mathbb{N}\backslash\{1\}$ und $z_i \in \mathbb{Z}_g$. Dann heißt

$$(z_n z_{n-1} \ldots z_1 z_0)_g := \sum_{i=0}^{n} z_{n-i} \cdot g^{n-i} = r$$

die *g–adische Darstellung* der Zahl r, man setzt außerdem $(0)_g := 0$.

Beispiel (Fortsetzung): $123 = (443)_5$

Im Fall $g = 10$, also der bei uns üblichen Dezimaldarstellung von Zahlen, verzichtet man auf die Wiedergabe des unteren Index, *Beispiel* $(1203)_{10} = 1203$.

So weit die Theorie, nun zur Praxis! Die Umrechnung vom Dezimalsystem in ein g–adisches System führt man am Einfachsten mit einer Variante des Euklidischen Algorithmus durch.

Beispiele: 1) 350 soll in eine 6–adische Zahl umgewandelt werden:

$$\begin{array}{rcrcl@{\qquad}c@{\qquad}rcl} 350:6 & = & 58 & \text{Rest} & 2 & \Longleftrightarrow & 350 & = & 58 \cdot 6 + 2 \\ 58:6 & = & 9 & \text{Rest} & 4 & \Longleftrightarrow & 58 & = & 9 \cdot 6 + 4 \\ 9:6 & = & 1 & \text{Rest} & 3 & \Longleftrightarrow & 9 & = & 1 \cdot 6 + 3 \\ 1:6 & = & 0 & \text{Rest} & 1 & \Longleftrightarrow & 1 & = & 0 \cdot 6 + 1 \end{array}$$

$$\Longrightarrow \quad 350 = 58 \cdot 6 + 2 = (9 \cdot 6 + 4) \cdot 6 + 2 = \ldots = 1 \cdot 6^3 + 3 \cdot 6^2 + 4 \cdot 6^1 + 2 \cdot 6^0 = (1342)_6$$

2) $r = 345 = 2 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5^1 + 0 \cdot 5^0 = (2340)_5$.

3) $r = 100, \quad g = 2: \quad 100 = (?\ldots?)_2$

Die Umrechnung von g–adisch in dezimal ist wesentlich einfacher.

Beispiel: $(123)_7 = 1 \cdot 7^2 + 2 \cdot 7 + 3 = 66 = (66)_{10} = (?\ldots?)_4$

Wenn man Zeit und Muße hat, kann man mit jeder Grundzahl g Arithmetik betreiben (Addition, Subtraktion, Multiplikation, Division, ...), dies ist weniger schwierig als gewöhnungsbedürftig. Wir wollen uns hier auf ein Beispiel beschränken und verweisen für weitere Rechnungen auf die Übungen.

Beispiel: $(203)_4 \cdot (33)_4 = ??$ Wir rechnen schriftlich modulo 4:

2	0	3	·	3	3
	1	2	2	1	
		1	2	2	1
	2	0	0	3	1

Damit ist $(203)_4 \cdot (33)_4 = (20031)_4$

Wir hätten natürlich auch die gegebenen Zahlen in das Zehnersystem umrechnen, sie dort multiplizieren und dann das Ergebnis zurück in das Vierersystem übertragen können.

Für Grundzahlen $g > 10$ erfindet man zur eindeutigen Darstellung weitere Ziffern, zum Beispiel setzt man für $g = 11$ (diese Grundzahl kommt im Buchhandel vor) $\mathbb{Z}_{11} = \{0, 1, \ldots, 9, X\}$.

Frage: Wie lautet $(230)_{11}$ im Zwölfersystem?

g–adische Darstellung beschränkt sich nicht auf natürliche Zahlen. So wie es im Dezimalsystem Brüche oder „Kommazahlen“ gibt, kann man Ausdrücke wie $\left(\frac{2}{5}\right)_6$ oder $(0.2\overline{1})_3$ bilden[11]. Wir beschränken uns im Wesentlichen auf die Angabe von „Kochrezepten“, wie man zu solchen Zahlen kommt. Hierzu ein letzter Satz:

Satz 5.9 Sei $r \in [0,1[:= \{r \in \mathbb{R} \mid 0 \leq r < 1\}$, $g \in \mathbb{N}\backslash\{1\}$. Dann gibt es für jedes $n \in \mathbb{N}$ eine eindeutige Darstellung

$$r = \sum_{i=1}^{n} z_{-i} \cdot g^{-i} + r_n \cdot g^{-n} \qquad \text{mit } z_{-i} \in \mathbb{Z}_g \quad \text{und} \quad r_n \in [0,1[$$

Beweisskizze: Mit Induktion zeigt man

$n = 1$: Für $r \in [0,1[$ ist $0 \leq r \cdot g < g$ und damit $r \cdot g = z_{-1} + r_1$ mit $z_{-1} \in \mathbb{Z}_g$ und $r_1 \in [0,1[$, also $r = z_{-1} \cdot g^{-1} + r_1 \cdot g^{-1}$.

$n \mapsto n+1$: Sei $r = \sum_{i=1}^{n} z_{-i} \cdot g^{-i} + r_n \cdot g^{-n}$ mit $z_{-i} \in \mathbb{Z}_g$ und $r_n \in [0,1[$. Dann gilt $r_n \cdot g^{-n} = (r_n \cdot g) \cdot g^{-(n+1)}$ mit $r_n \cdot g < g$, also $r_n \cdot g = z_{-(n+1)} + r_{n+1}$ mit $z_{-(n+1)} \in \mathbb{Z}_g$ und $r_{n+1} \in [0,1[$.

Insgesamt folgt

$$r = \sum_{i=1}^{n} z_{-i} \cdot g^{-i} + r_n \cdot g^{-n} = \sum_{i=1}^{n} z_{-i} \cdot g^{-i} + (z_{-(n+1)} + r_{n+1}) \cdot g^{-(n+1)} = \sum_{i=1}^{n+1} z_{-i} \cdot g^{-i} + r_{n+1} \cdot g^{-(n+1)}.$$

Interessanter als der Beweis ist die Anwendung: Wie kommt man bei beliebigen $n \in \mathbb{N}$ zu den gesuchten Ziffern z_{-i}? Die Antwort, die wir nicht formal nachweisen werden, lautet

$$z_{-1} = \lfloor r \cdot g \rfloor \quad \text{und für } i > 1 \quad z_{-i} = \lfloor r_{i-1} \cdot g \rfloor.$$ [12]

Beispiel: Gesucht ist die 5–adische Darstellung von $\frac{3}{50} = (0.06)_{10}$:

[11] Wir benutzen wie international üblich an Stelle des Kommas einen Punkt.

[12] Erneut zur Erinnerung: $\lfloor x \rfloor := \max\{z \in \mathbb{Z} \mid z \leq x\}$

$$\begin{array}{lllllll} \frac{3}{50} & \cdot\ 5 & = & 0 & + & \frac{3}{10} & \Rightarrow \quad z_{-1} = 0 \\ \frac{3}{10} & \cdot\ 5 & = & 1 & + & \frac{1}{2} & \Rightarrow \quad z_{-2} = 1 \\ \frac{1}{2} & \cdot\ 5 & = & 2 & + & \frac{1}{2} & \Rightarrow \quad z_{-3} = 2 \\ \frac{1}{2} & \cdot\ 5 & = & 2 & + & \frac{1}{2} & \Rightarrow \quad z_{-4} = 2 = z_{-5} = z_{-6} = \ldots \end{array} .$$

Damit ist $\frac{3}{50} = (0.01\overline{2})_5$.

Wie bereits gesehen, ist die Umwandlung einer gegebenen g–adischen Zahl in das Dezimalsystem einfach zu bewerkstelligen, zumindest solange keine Periode vorkommt:

Beispiel: $(0.122)_3 = 1 \cdot 3^{-1} + 2 \cdot 3^{-2} + 2 \cdot 3^{-3} = \frac{17}{27}$

Zur Umwandlung periodischer Zahlen wie beispielsweise $(0.1\overline{2})_3$ benötigt man Hilfsmittel aus der Analysis (Stichwort unendliche Reihen), hiermit werden wir uns aber erst im dritten Semester beschäftigen. Trotzdem soll an dieser Stelle das Ergebnis verraten werden: $(0.1\overline{2})_3 = 1 \cdot 3^{-1} + 2 \cdot \frac{1}{3 \cdot 2} = \frac{2}{3}$.

Zum Schluss geben wir an, wie man zu einer beliebigen reellen Zahl r eine g–adische Darstellung findet:

1. Fall $r \geq 0$: Es gilt $r = m + s$ mit $m \in \mathbb{N}_0$ und $s \in [0, 1[$. Die g–adische Darstellungen von m und s sind bekannt: $m = (z_n z_{n-1} \ldots z_0)_g$, $s = (z_{-1} z_{-2} \ldots)_g$

$\Rightarrow \quad r = (z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots)_g$

2. Fall $r < 0$: Es ist $-r = m + s > 0$. Wie im ersten Fall folgt $r = -(z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots)_g$.

6 Elementare Kombinatorik

Am Ende dieses Abschnitts können Sie (hoffentlich) folgende *Fragen* beantworten:

Wieviele Möglichkeiten gibt es

a) fünf Studierende auf drei Arbeitsgruppen aufzuteilen, wenn jede Arbeitsgruppe aus mindestens einer Person bestehen muss?

b) fünf nicht unterscheidbare Bonbons auf drei Kinder aufzuteilen, wenn jedes Kind mindestens ein Bonbon erhalten soll?

c) Drei Exemplare eines Lehrbuchs unter fünf Studierende aufzuteilen, wenn kein Studierender mehr als ein Buch benötigt?

d) die drei Medaillen (Gold, Silber, Bronze) eines Wettbewerbs unter fünf Nationen aufzuteilen, wenn jede Nation mit drei Sportlern vertreten ist?

Wir beginnen mit einer einfachen Überlegung und erinnern an den Begriff *kartesisches Produkt* aus dem Grundlagenkapitel.

Frage: Wieviel verschiedene k–Tupel $(b_1, \ldots, b_k) \in A_1 \times \ldots \times A_k$ gibt es, wenn jede Menge A_i aus n_i Elementen besteht ?

Antwort: Für jedes b_i gibt es n_i Wahlmöglichkeiten, also gibt es $n_1 \cdot n_2 \cdot \ldots \cdot n_k =: \prod_{i=1}^{k} n_i$ viele k–Tupel. Dieses einfache Ergebnis wird auch *Multiplikationsregel* genannt.

Beispiele: 1) $A_1 = \{a, b\}$, $A_2 = \{b, c, d\} \implies A_1 \times A_2 = \{(a,b), (a,c), (a,d), (b,b), (b,c), (b,d)\}$, es ist $|A_1 \times A_2| = 2 \cdot 3 = 6$.

2) Fridolin darf von seinen sechs Stoffhunden, vier Plüschhasen und fünf Märchenbüchern insgesamt nur drei Dinge mit in den Urlaub nehmen. Wieviele Wahlmöglichkeiten hat Fridolin, wenn er auf jeden Fall drei wesentlich verschiedene Dinge mitnehmen will? Wieviele Wahlmöglichkeiten hat er, wenn ihm nur die Mitnahme von zwei Sachen erlaubt wird?

Frage: Wieviele verschiedene k–Tupel kann man aus einer n–elementigen Menge bilden?

Antwort: Wende die Multiplikationsregel auf $n_1 = \ldots = n_k = n$ an, die gesuchte Anzahl ist $\prod_{i=1}^{k} n = n^k$.

Beispiele: 1) Die Anzahl aller möglichen Tripel aus $A = \{a, b\}$ ist acht. (Man beachte, dass z.B. $(a, b, a) \neq (a, a, b)$ gilt.)

2) Wieviele Bücher kann eine Bibliothekarin katalogisieren, wenn jedes Buch durch drei Buchstaben und drei Ziffern gekennzeichnet wird?

Unsere Frage nach der Anzahl aller k–Tupel einer n–elementigen Menge kann auch als *Urnenproblem* gedeutet werden:

Gegeben sei eine Urne mit n Kugeln, aus der k–mal eine Kugel gezogen wird.

- *Mit* Beachtung der Reihenfolge und *mit* Zurücklegen gibt es n^k viele Möglichkeiten.

Bei den bisher untersuchten k–Tupel $(b_1, \ldots, b_k)$ war natürlich $b_i = b_j$ erlaubt.

Frage: Wieviele verschiedene k–Tupel kann man aus einer n–elementigen Menge A bilden, wenn in keinem Tupel Elemente mehrfach auftreten dürfen?

Antwort: Die gesuchte Zahl ist $n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$. Man kann jedes dieser k–Tupel als injektive Abbildung der k–elementigen Menge $\{1, \ldots, k\}$ auf A deuten.

Beispiele: 1) Sei $A = \{a, b, c\}$. Es gibt genau $3 \cdot 2 = 6$ erlaubte 2–Tupel (ohne Wiederholungen). Dem Tupel (a, c) entspricht die injektive Abbildung $\{1, 2\} \to \{a, b, c\}$ mit $1 \mapsto a$ und $2 \mapsto c$. Übertragen auf das Urnenmodells kann man sagen, dass beim ersten Ziehen die Kugel a und beim zweiten Ziehen die Kugel b erwischt wurde.

2) In der Fußballbundesliga gibt es pro Saison 306 Spiele. Dies ist die Zahl aller aus den Mannschaften gebildeten 2–Tupel. Da jeweils Hin– und Rückspiel ausgetragen wird, kommt es auch auf die Reihenfolge der Vereine an.

3) Wieviele (sinnvolle oder sinnlose) Worte mit drei oder vier Buchstaben können aus der Buchstabenmenge $\{A, B, D, E, G, R, S, T, U\}$ gebildet werden, wenn kein Buchstabe pro Wort mehrfach benutzt werden darf?

Als Urnenproblem formuliert lautet unser Ergebnis (n Kugeln, k Ziehungen):

- *Mit* Beachtung der Reihenfolge und *ohne* Zurücklegen gibt es $\frac{n!}{(n-k)!}$ viele Möglichkeiten.

Die folgende Definition hätte in diesem Skript auch an anderer Stelle auftauchen können.

Def 6.1 Jede Bijektion einer endlichen Menge auf sich heißt *Permutation*.

Weil jeder Permutation eine Anordnung von Elementen einer endlichen Menge M in einer bestimmten Reihenfolge entspricht und damit jeder Permutation eine bijektive Abbildung auf M zugeordnet ist, gibt es $n!$ viele Permutationen einer n–elementigen Menge auf sich.

Frage: Wieviele verschiedene k–elementige Teilmengen enthält eine n–elementige Menge?

Beispiel: Die zweielementigen Teilmengen von $\{a, b, c, d\}$ sind $\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$. Es gibt vier dreielementige Teilmengen.

Allgemeine Antwort: 1) Eine n–elementige Menge besitzt $\frac{n!}{(n-k)!}$ viele k–Tupel (ohne Zurücklegen).

2) Jeweils $k!$ viele k–Tupel gehören zur gleichen k–elementigen Teilmenge (es gibt $k!$ viele Umordungen).

3) Die gesuchte Anzahl ist daher $\frac{n!}{(n-k)!k!} =: \binom{n}{k}$.

Def 6.2 Seien $n, k \in \mathbb{N}$ mit $n \geq k$. Dann heißt

$$\binom{n}{k} := \frac{n!}{k!(n-k)!} \qquad \textit{Binomialkoeffizient}$$

$\binom{n}{k}$ wird üblicherweise „n über k“ gesprochen, eine andere Möglichkeit ist „k aus n“. Man kann Binomialkoeffizienten auch für $n = 0$ oder $k = 0$ berechnen. Es ist beispielsweise $\binom{n}{0} = 1$ (auch für $n = 0$) und $\binom{4}{2} = 6$ (siehe vorheriges Beispiel). [13]

Wir haben folgenden Satz bewiesen

Satz 6.1 Die Anzahl aller k–elementigen Teilmengen einer n–elementigen Menge ist $\binom{n}{k}$.

Auch dieser Fall kann im Urnenmodell beschrieben werden (n Kugeln, k Ziehungen):

- *Ohne* Beachtung der Reihenfolge und *ohne* Zurücklegen gibt es $\binom{n}{k}$ viele Möglichkeiten.

Beispiel: Will man im Lotto genau x Treffer erzielen ($0 \leq x \leq 6$, ohne Zusatzzahl) und sind $a_1, \ldots a_6$ die korrekten Zahlen, so muss man aus den möglichen $\binom{49}{6}$ Kombinationen eine Menge A tippen mit $|A \cap \{a_1, \ldots, a_6\}| = x$ und $|A \cap (\{1, \ldots, 49\} \backslash \{a_1, \ldots, a_6\})| = 6 - x$.

Hierfür gibt es $\binom{6}{x}$ bzw. $\binom{49-6}{6-x}$ Möglichkeiten. Nach der Multiplikationsregel sind $\binom{6}{x} \cdot \binom{43}{6-x}$ Kombinationen erfolgreich (von insgesamt $\binom{49}{6}$).

Die Chancen für einen Volltreffer liegen damit bei 1:13 983 816, genau „3 Richtige“ kann man circa in einem von 57 Fällen erwarten.

Frage: Wie groß ist die Chance für „5 Richtige mit Zusatzzahl“?

Wir wollen uns etwas intensiver mit Binomialkoeffizienten beschäftigen.

[13] Eine mögliche Interpretation von $\binom{n}{0} = 1$: Kein Element aus einer Menge von n Elementen liegt genau im Fall der leeren Menge vor.

Satz 6.2 Für $1 \leq k \leq n-1$ gilt

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Beweis:

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{(n-1)!(n-k) + (n-1)!k}{k!(n-k)!} \\ &= \frac{(n-1)!(n-k+k)}{k!(n-k)!} = \binom{n}{k}\end{aligned}$$

Satz 6.3 (Binomischer Lehrsatz)

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Beweis: Vollständige Induktion[14]

$n = 1:\quad (a+b)^1 = 1 \cdot a \cdot 1 + 1 \cdot 1 \cdot b = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = \sum_{i=0}^{1} \binom{1}{i} a^{1-i} b^i.$

$n \mapsto n+1$:

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n \cdot (a+b) \\ &= \left(\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i\right)(a+b) \\ &= \sum_{i=0}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^{i+1} \\ &= \binom{n}{0} a^{n+1} b^0 + \sum_{i=1}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^{n-1} \binom{n}{i} a^{n-i} b^{i+1} + \binom{n}{n} a^0 b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} b^0 + \sum_{i=1}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=1}^{n} \binom{n}{i-1} a^{n-(i-1)} b^{i-1+1} + \binom{n}{n} a^0 b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} b^0 + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1}\right) a^{n+1-i} b^i + \binom{n+1}{n+1} a^0 b^{n+1} \\ &= \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i} b^i\end{aligned}$$

Beispiele: $(a+b)^2 = a^2 + 2ab + b^2, \qquad (a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3.$

[14] Man hätte auch mit $n = 0$ starten können: $(a+b)^0 = 1, \quad \binom{0}{0} a^{0-0} b^0 = \frac{0!}{0! \cdot 0!} a^0 b^0 = \frac{1}{1 \cdot 1} \cdot 1 \cdot 1 = 1.$

Das *Pascalsche Dreieck* liefert eine Anordnung der Binomialkoeffizienten. Man erhält $\binom{n}{k}$ für $k = 0, \ldots, n$, indem man die beiden versetzt über $\binom{n}{k}$ stehenden Zahlen addiert.

$$\begin{array}{ll}
n=0 & \qquad\qquad\qquad\qquad 1 \\
n=1 & \qquad\qquad\qquad 1 \qquad 1 \\
n=2 & \qquad\qquad 1 \qquad 2 \qquad 1 \\
n=3 & \qquad\qquad 1 \qquad 3 \qquad 3 \qquad 1 \\
n=4 & \qquad 1 \qquad 4 \qquad 6 \qquad 4 \qquad 1 \\
\vdots & \qquad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots
\end{array}$$

Mit Hilfe der Binomialkoeffizienten können wir Satz I.5.3 (Sei $|M| = n \implies |\mathrm{Pot}\, M| = 2^n$) auf eine weitere elegante Weise beweisen:

Wir sortieren alle Teilmengen von M nach der Anzahl ihrer Elemente.

$|\mathrm{Pot}\, M| = \binom{n}{0} + \ldots + \binom{n}{n} = \sum_{i=0}^{n} \binom{n}{i} \cdot 1^{n-i} \cdot 1^i = (1+1)^n = 2^n.$

In unserem Urnenmodell fehlt uns noch eine Formel für den Fall einer Ziehung *ohne* Reihenfolge, *mit* Zurücklegen. Wir stellen uns zunächst die

Frage: Wieviele n–Tupel kann man aus Elementen der Menge $\{a_1, \ldots, a_r\}$ bilden, wenn jedes Element a_i genau n_i–mal vorkommen soll? Hierbei muss $n = \sum_{i=1}^{r} n_i$ gelten.

Beispiele: 1) $r = 2,\ n = 3,\ n_1 = 2, n_2 = 1$: 3 Möglichkeiten

2) $r = 2,\ n = 4,\ n_1 = n_2 = 2$: 6 Möglichkeiten

3) $r = 3,\ n = 3,\ n_i = 1$ für $i = 1, 2, 3$: 6 Möglichkeiten

Allgemeine *Antwort*: Sei $(a_1, \ldots, a_1, a_2, \ldots a_2, \ldots \ \ldots, a_r)$ eine mögliche Lösung. Es gibt insgesamt $n!$ viele Umordnungen dieses n–Tupels. Nichts Neues erhält man hierbei, wenn jeweils die a_i untereinander vertauscht werden. Dies ist genau $n_1! \cdot n_2! \cdot \ldots \cdot n_r!$ mal möglich. Somit ist die gesuchte Anzahl

$$\frac{n!}{n_1! \cdot \ldots \cdot n_r!}$$

Beispiele: 1) Gesucht sind alle sinnvollen und sinnlosen Buchstabenkombinationen, die aus den Wörtern

a) RAUM, b) KLASSE, c) ANANAS gebildet werden können.

2) Wieviele verschiedene Wahlergebnisse sind möglich, wenn k Wähler zwischen n Parteien (oder Personen) wählen können? (Jeder Wähler habe genau eine Stimme, Stimmenthaltung sei nicht erlaubt.)

Lösung: Fassen wir die k Stimmen als k–fache Wiederholung eines Elementes a auf, entspricht jeder mögliche Wahlausgang einer Zuordnung der Art

$$a, \ldots, a, t, a, \ldots, a, t, \ldots \ \ldots, t, a, \ldots, a,$$

wobei die a's zwischen zwei „Trennern" t jeweils die Stimmen für eine Partei wiedergeben. Da es k Stimmen gibt und zwischen n Parteien $n-1$ Trenner stehen, existiert zu jedem möglichen Wahlausgang genau ein $n+k-1$–Tupel aus Elementen der Menge $\{a, t\}$, genauer aus k–fachem Auftreten der a's und $n-1$–fachem Vorkommen der t's. Die gesuchte Anzahl ist also

$$\frac{(n+k-1)!}{k!(n-1)!} = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Zusatzfrage: Wieviele Wahlausgänge sind möglich, wenn Stimmenthaltung erlaubt ist?

Wir übertragen die Wahlproblematik auf das Urnenmodell: Jeder der k Wähler zieht eine von n Parteien, wobei es nicht auf die Reihenfolge der Stimmen ankommt. Da Parteien mehrfach gewählt werden können, liegt der Fall *mit* Zurücklegen vor:

- *Ohne* Beachtung der Reihenfolge und *mit* Zurücklegen gibt es $\binom{n+k-1}{k}$ viele Möglichkeiten.

Jetzt sollte man in der Lage sein, die zu Beginn dieses Abschnitts gestellten Fragen zu beantworten, auch mit anderen Zahlen als 3 und 5. Wir schließen mit einem Beispiel, zu dessen Lösung ein wenig Wahrscheinlichkeitsrechnung benötigt wird.

Wie groß ist die Wahrscheinlichkeit, dass die Hörer–Geburtstags–Funktion aus Abschnitt 4 des ersten Kapitels nicht injektiv ist, dass also mehrere Personen am gleichen Tag Geburtstag feiern können?

Wir gehen von n Personen, einem Jahr mit 365 Tagen und der Annahme aus, dass jeder Tag im Jahr als Geburtstag gleich wahrscheinlich ist. Jede Verteilung der Geburtstage entspricht einer Abbildung der Hörer auf die durchnummerierten Tage $\{1, \ldots, 365\}$. Hiervon gibt es 365^n verschiedene, davon sind $365 \cdot \ldots \cdot (365 - n + 1) = \frac{365!}{(365-n)!}$ injektiv.

Die Wahrscheinlichkeit, dass alle Geburtstage an verschiedenen Tagen liegen, berechnet man aus dem Quotienten der Anzahl der injektiven zu allen Abbildungen. Summiert man alle möglichen Wahrscheinlichkeiten zu 1, ist die gesuchte Zahl

$$1 - \frac{\frac{365!}{(365-n)!}}{365^n}$$

Will man eine Prozentangabe, muss man diese Zahl mit 100 multiplizieren.

Erstaunlicherweise liegt bereits bei nur 23 Personen die Wahrscheinlichkeit für mindestens eine gemeinsame Feier mehrerer Personen bei über 50 Prozent; ab 57 Personen ist es extrem unwahrscheinlich, dass keine Geburtstage zusammenfallen (Wahrscheinlichkeit unter einem Prozent).

7 Einiges über die Menge der komplexen Zahlen $\mathbb{C}$

Zu Beginn dieses Kapitels wurde der abstrakte Begriff *Körper* eingeführt. Wir haben als Beispiele den Körper der reellen Zahlen und den der rationalen Zahlen kennengelernt. Jetzt wird ein weiterer wichtiger Körper untersucht.

Auch die Menge der *komplexen Zahlen* $\mathbb{C} := \{a + ib \mid a, b \in \mathbb{R}\}$ mit der Festsetzung $i^2 = -1$ ($i \notin \mathbb{R}$) bildet einen Körper, wenn man mit der *imaginären Einheit* i wie mit einer reellen Zahl rechnet. Da die Multiplikation in $\mathbb{R}$ kommutativ ist, spielt es für uns keine Rolle, ob die imaginäre Einheit i von rechts oder von links mit einer reellen Zahl (oder mit i) multipliziert wird.

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$
$$(a + ib) \cdot (c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc).$$

Beispiele: $(5 + 2i) - (1 - 7i) = 4 + 9i$, $(5 + 2i) \cdot (1 - 7i) = 19 - 33i$

Der Nachweis der Körperaxiome erfordert einige Schreibarbeit, wir geben hier nur die inversen Elemente zu $a+ib$ bezüglich Addition und Multiplikation an:

Additiv invers zu $z=a+ib$ ist $-z=-(a+ib)=-a-ib$.

Multiplikativ invers zu $z=a+ib\neq 0$ und damit $a^2+b^2\neq 0$ ist $z^{-1}=\frac{a}{a^2+b^2}-i\frac{b}{a^2+b^2}$.

Wozu werden komplexe Zahlen benötigt? In dem empfehlenswerten Lehrbuch *Analysis I* schreibt der Autor *H. Heuser*, dass *Geronimo Cardano* (1501–1576) bei der Aufgabe, eine Strecke der Länge 10 so in zwei Stücke zu zerlegen, dass das aus ihnen gebildete Rechteck die Fläche 40 hat, auf die für ihn absurde Lösung $x_{1,2}=5\pm\sqrt{-15}$ kommt und nur durch rein formales Rechnen tatsächlich $x_1+x_2=10$ und $x_1\cdot x_2=40$ erhält.

Der Körper der komplexen Zahlen ist somit der erste Rechenbereich, in dem alle Grundrechenarten uneingeschränkt möglich sind (natürlich bis auf Division durch Null).

Beispiel: Es gibt keine natürliche Zahl n mit $n+3=2$, es gibt keine ganze Zahl z mit $z\cdot 3=2$, es gibt keine rationale Zahl q mit $q\cdot q=2$ und es gibt keine reelle Zahl r mit $r\cdot r=-1$.

Sei $C:=\{(a,b)\mid a,b\in\mathbb{R}\}$. Definiert man auf C die komponentenweise Addition und folgende Multiplikation:

$$(a,b)\cdot(c,d):=(ac-bd,ad+bc)$$

erhält man eine weitere Darstellung der komplexen Zahlen. Um dies einzusehen, betrachtet man die Abbildung $f:\mathbb{C}\to C,\ \ z=a+ib\mapsto(a,b)$. f ist bijektiv (leicht einzusehen) und *strukturerhaltend*; denn man kann nachprüfen, dass für alle $z_1,z_2\in\mathbb{C}$ gilt

$$f(z_1+z_2)=f(z_1)+f(z_2),\qquad f(z_1\cdot z_2)=f(z_1)\cdot f(z_2)$$

Alle Körpereigenschaften von $\mathbb{C}$ werden so auf C übertragen. Später werden wir für eine bijektive und strukturerhaltende Abbildung den Namen *Isomorphismus* kennenlernen.

Frage: Was sind die Bilder von 1 bzw. i unter f?

Def 7.1 a) Es sei $z=a+ib\in\mathbb{C}$. Dann heißt a *Realteil* von z, b *Imaginärteil* von z,

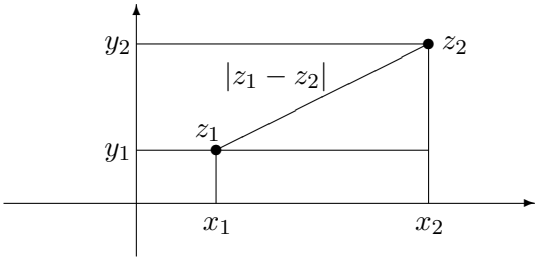
$|z|:=\sqrt{a^2+b^2}$ *absoluter Betrag* von z, $\bar{z}:=a-ib$ *konjugiert komplexe Zahl* zu z.

b) Es seien $z_1,z_2\in\mathbb{C}$. Dann heißt $|z_1-z_2|$ der *Abstand* von z_1 und z_2.

Diese Definition ist in Einklang mit der gewohnten Definition des Abstands zweier Punkte in der Ebene, es gilt nämlich für $z_1=x_1+iy_1$, $z_2=x_2+iy_2$:

$$|z_1-z_2|=|x_1-x_2+i(y_1-y_2)|=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}\,,$$

und dies ist genau die übliche Abstandsdefinition zweier Punkte (x_1,y_1), (x_2,y_2) in der Ebene („Lehrsatz des Pythagoras“).



Wie Sie ganz leicht selbst nachrechnen können, besteht folgender Zusammenhang zwischen z, $|z|$ und $\bar{z}$:

Satz 7.1 Sei $z = a + ib \in \mathbb{C}$. Dann ist $z \cdot \bar{z} \;=\; a^2 + b^2 = |z|^2$.

Damit ist auch klar, dass für jedes $z \in \mathbb{C}$ das Produkt $z \cdot \bar{z}$ eine reelle Zahl ist.

Für den Quotienten zweier komplexer Zahlen $a + ib$ und $c + id \neq 0$ gilt:

$$\frac{a+ib}{c+id} \;=\; \frac{(a+ib)(c-id)}{(c+id)(c-id)} \;=\; \frac{(ac+bd)+i(bc-ad)}{c^2+d^2} \;=\; \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}.$$

Besser als das Ergebnis auswendig zu lernen ist es, sich den ersten Rechenschritt der Herleitung zu merken: *Man erweitert $\frac{a+ib}{c+id}$ mit der konjugiert komplexen Zahl des Nenners.* Im Nenner steht dann die reelle Zahl $c^2 + d^2$ und man benötigt nur noch eine Multiplikation im Zähler.

Beispiel: $z = \frac{3+4i}{2+3i} = \frac{(3+4i)(2-3i)}{(2+3i)(2-3i)} = \frac{6-9i+8i+12}{4+9} = \frac{18}{13} - \frac{1}{13}i$.

Wir stellen Rechenregeln für den Übergang zur konjugiert komplexen Zahl zusammen:

Satz 7.2 Es seien $z_1, z_2 \in \mathbb{C}$. Dann gilt:

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}\,, \qquad \overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}\,, \qquad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}\,, \qquad \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}\,, \qquad \overline{\overline{z_1}} = z_1 \quad .$$

Beweis: Wir zeigen nur $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$, der Rest sei als einfache Übungsaufgabe empfohlen:

$\overline{z_1 \cdot z_2} = \overline{(a+ib)(c+id)} = \overline{(ac-bd)+i(ad+bc)} = (ac-bd) - i(ad+bc)$

$\overline{z_1} \cdot \overline{z_2} = (a-ib)(c-id) = ac - iad - ibc - bd = (ac-bd) - i(ad+bc)$.

Im folgenden Satz werden ohne Beweis Eigenschaften des absoluten Betrags für komplexe Zahlen genannt. Es sind natürlich genau die Eigenschaften, die wir bereits aus Satz 1.5 für reelle Zahlen kennen, da es sich bei den Beträgen um reelle Zahlen handelt.

Satz 7.3 Für alle $z_1, z_2 \in \mathbb{C}$ gilt:

1. $|z_1| \geq 0$; $|z_1| = 0$ gilt genau dann, wenn $z_1 = 0$.
2. $|z_1 z_2| = |z_1|\,|z_2|$
3. $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|} \quad (z_2 \neq 0)$
4. $|z_1 + z_2| \leq |z_1| + |z_2|$ (*Dreiecksungleichung*)
5. $|z_1 - z_2| \geq |z_1| - |z_2|$.

Der Name *Dreiecksungleichung* hat einen geometrischen Hintergrund, denn in einem Dreieck ist die Summe der Längen zweier Seiten immer mindestens so groß wie die Länge der dritten Seite. Daher findet man die Dreiecksungleichung auch in der Gestalt $|z_1 - z_3| \leq |z_1 - z_2| + |z_2 - z_3|$ (für alle $z_1, z_2, z_3 \in \mathbb{C}$) vor. Ebenso wird die Ungleichung $\big|\,|z_1| - |z_2|\,\big| \leq |z_1 - z_2|$ (für alle $z_1, z_2 \in \mathbb{C}$) manchmal als Dreiecksungleichung bezeichnet.

Wie wir wissen, bilden $\mathbb{Q}$ und $\mathbb{R}$ *angeordnete* Körper, wobei $\mathbb{R}$ vollständig ist und $\mathbb{Q}$ nicht. Was gilt für den Körper der komplexen Zahlen $\mathbb{C}$?

Satz 7.4 Es gibt keine Relation auf $\mathbb{C}$, die die Anordnungsaxiome erfüllt.

Beweis: Angenommen, $<$ ist eine Relation auf $\mathbb{C}$, die die Anordnungsaxiome erfüllt (Def 1.3). Wir vergleichen die verschiedenen Elemente 0 und i und zeigen, dass beide theoretische Möglichkeiten $0 < i$ und $i < 0$ jeweils zu einem Widerspruch führen. Als Hilfsmittel benutzen wir Teile des Satzes 1.3: In angeordneten Körpern gilt stets $0 < 1$, und aus $a < b,\ c < 0$ folgt $ac > bc$.

1. Fall: Angenommen $0 < i$. Dann ist $0 \cdot i < i \cdot i \iff 0 < -1$.

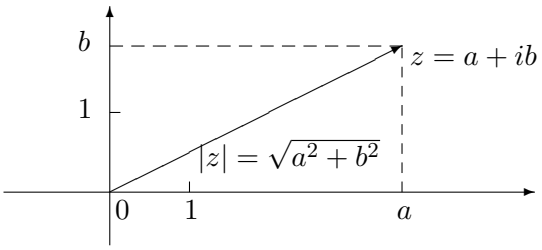
2. Fall: Angenommen $i < 0$. Dann ist $i \cdot i > 0 \cdot i \iff -1 > 0$.

Stets ist $0 < -1$. Da aber auch $0 < 1$ gilt, folgt der Widerspruch $0 + 0 < (-1) + 1 = 0$.

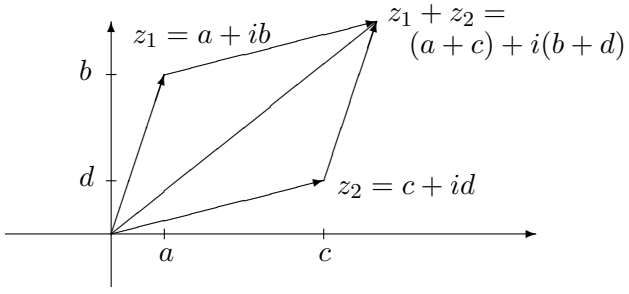
$\mathbb{C}$ ist also kein angeordneter Körper. Die Frage nach der Vollständigkeit von $\mathbb{C}$ beantworten wir ohne Beweis:

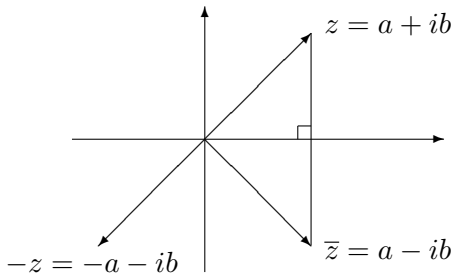
Satz 7.5 $\mathbb{C}$ ist ein vollständiger Körper.

Wir können die komplexen Zahlen als Punkte der Anschauungsebene (*Gaußsche Zahlenebene*) interpretieren. Hierzu legt man auf die übliche Art ein rechtwinkliges, kartesisches[15] Koordinatensystem in der Zeichenebene zu Grunde. Komplexe Zahlen $z = a + ib$ und Punkte mit den Koordinaten (a, b) entsprechen sich dann umkehrbar eindeutig. Manchmal stellt man eine komplexe Zahl $a + ib$ durch einen Pfeil (Vektor) vom Punkt $(0, 0)$ zum Punkt (a, b) dar. Man nennt die x–Achse *reelle Achse* und die y–Achse *imaginäre Achse*. Der Betrag $|z|$ einer komplexen Zahl entspricht dann dem Abstand zwischen $z = a + ib$ und dem Punkt $(0, 0)$ („Lehrsatz des Pythagoras“).



Die Addition komplexer Zahlen lässt sich als Vektoraddition („Parallelogramm der Kräfte“) veranschaulichen. Die konjugiert komplexe Zahl $\bar{z}$ zu z erhält man durch Spiegelung von z an der x–Achse, die negative Zahl $-z$ durch Punktspiegelung am Ursprung:





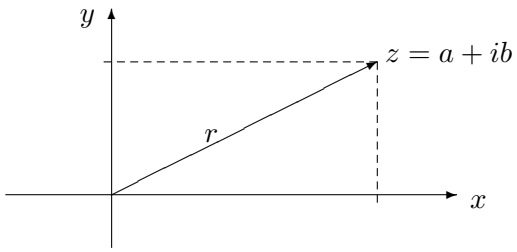
[15] „kartesisch“ bedeutet, dass auf beiden Achsen dieselbe Längeneinheit gewählt ist, d.h., der Punkt $(1, 0)$ hat in der Zeichnung denselben Abstand vom Ursprung wie der Punkt $(0, 1)$.

Zur zeichnerischen Deutung der Multiplikation komplexer Zahlen holen wir etwas weiter aus.

Es sei $z = a + ib \neq 0$ eine komplexe Zahl, $r = |z|$ sei der Betrag von z, d.h., der Abstand von z zum Koordinatenursprung. Mit φ bezeichnen wir den Winkel zwischen der positiven x–Achse und dem „Vektor“ z, gemessen im mathematisch positiven Sinn, d.h., entgegen dem Uhrzeigersinn. Wir können φ in Grad oder im *Bogenmaß* angeben. Falls Sie es nicht aus Ihrer Schulzeit wissen: Das Bogenmaß eines jeden Winkels α zwischen 0° und 360° ist die Länge des zugehörigen Einheitskreisbogens.

Beispiel: Zum Winkel 90° gehört das Bogenmaß $\frac{\pi}{2}$, welcher Gradzahl gehört zu 2π?

Ab jetzt werden wir Winkel weitgehend im Bogenmaß angeben.



(Diese Zeichnung wird in der Vorlesung ergänzt.)

Zwischen φ, r, a und b besteht der Zusammenhang $\cos\varphi = \frac{a}{r}$ und $\sin\varphi = \frac{b}{r}$.[16]

$$\Rightarrow \quad z = a + ib = r\cos\varphi + i\,r\sin\varphi = r(\cos\varphi + i\sin\varphi)$$

Diese Beziehung gilt für alle $a, b \in \mathbb{R}$ (nicht beide Null).

Beispiele: 1) $z = 4 - 3i$: Es ist $r = 5$, $\cos\varphi = \frac{4}{5}$, $\sin\varphi = -\frac{3}{5} \implies \varphi \approx 323^\circ$ bzw. $\varphi \approx 5.637$.

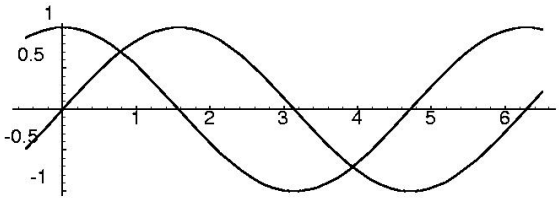
2) $\varphi = \frac{3}{4}\pi$, $r = 2\sqrt{2}$: Es ist $a = r\cos\varphi = 2\sqrt{2} \cdot \left(-\frac{\sqrt{2}}{2}\right) = -2$ und $b = r\sin\varphi = 2\sqrt{2} \cdot \frac{\sqrt{2}}{2} = 2$, damit ist $z = -2 + 2i$.

Man nennt $z = r(\cos\varphi + i\sin\varphi)$ die *Polarkoordinatendarstellung* von z, der Winkel φ wird auch das *Argument* von z genannt.

Koordinatenangaben durch Winkelgrößen sind beispielsweise in der Geografie üblich, die Lage eines Ortes wird durch zwei Winkel festgelegt.

Beispiel: Berlin hat die Koordinaten 13.4° östliche Länge und 52.5° nördliche Breite.

Da der Einheitskreis in beiden Richtungen auch mehrfach durchlaufen werden kann (Winkel modulo 2π), sind die Winkelfunktionen Sinus und Cosinus für jede reelle Zahl definiert, als Bilder kommen nur Werte aus dem Intervall $[-1, 1]$ in Frage, also $\sin, \cos : \mathbb{R} \to [-1, 1]$.



[16] Wir verzichten auf eine exakte Einführung der Winkelfunktionen und benutzen die in der Schule übliche Definition.

Fragen: Welche der beiden Kurven stellt die Sinusfunktion dar? Ist sie injektiv oder surjektiv?

Für alle $x \in \mathbb{R}$ gilt $\cos(-x) = \cos x,\ \cos(\pi + x) = -\cos x,\ \sin(-x) = -\sin x,\ \sin(\pi + x) = -\sin x.$

In der linearen Algebra werden wir die *Additionstheoreme* für Sinus und Cosinus beweisen:

$$\begin{aligned} \sin(\alpha + \beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta \\ \cos(\alpha + \beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{aligned}$$

Zurück zur Multiplikation komplexer Zahlen!

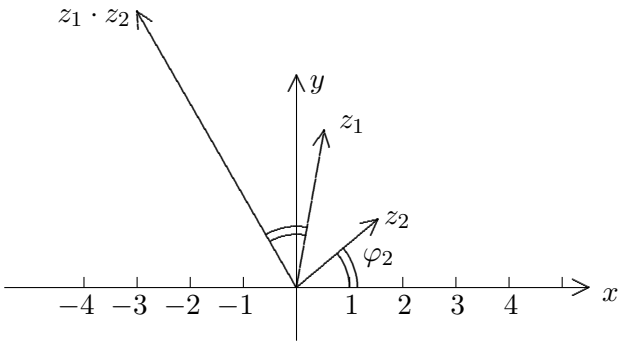
Satz 7.6 Es sei $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ und $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Für das Produkt $z_1 z_2$ gilt dann:

$$z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$$

Beweis: Der Beweis folgt direkt aus den Additionstheoremen.

$$\begin{aligned} z_1 z_2 &= r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) \\ &= r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)) \\ &= r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)) \end{aligned}$$

Formuliert man das Ergebnis in Worten, so erhält man die *geometrische Interpretation der Multiplikation komplexer Zahlen*: Bei der Multiplikation komplexer Zahlen werden die Beträge multipliziert und die Winkel addiert. (Siehe Zeichnung: Dort ist $|z_1| = 3$, $|z_2| = 2$, also $|z_1 z_2| = 6$.)



Wie im Reellen werden in $\mathbb{C}$ die Potenzen mit ganzzahligen Exponenten erklärt, für $n \in \mathbb{N}$ und $z \in \mathbb{C}$ definiert man $z^n := z \cdot \ldots \cdot z$, $\quad z^{-n} := \frac{1}{z^n}$ (nur für $z \neq 0$) und $z^0 := 1$.

Satz 7.7: Es sei $z \in \mathbb{C}$, $z \neq 0$, und $m \in \mathbb{Z}$. Es gelte $z = r(\cos\varphi + i\sin\varphi)$. Dann ist

$$z^m = r^m(\cos(m\varphi) + i\sin(m\varphi)).$$

Beweis: Für $m = 0$ und $m = 1$ ist die Behauptung klar; $m \geq 2$ folgt direkt aus Satz 6.

Es sei nun $m < 0$. Wir setzen $n = -m$. Dann gilt $n \in \mathbb{N}$ und es folgt

$$\begin{aligned} z^m &= z^{-n} = \tfrac{1}{z^n} = \tfrac{1}{r^n(\cos(n\varphi)+i\sin(n\varphi))} \\ &= r^{-n}\,\tfrac{\cos(n\varphi)-i\sin(n\varphi)}{(\cos(n\varphi)+i\sin(n\varphi))(\cos(n\varphi)-i\sin(n\varphi))} = r^{-n}\,\tfrac{\cos(n\varphi)-i\sin(n\varphi)}{\cos^2(n\varphi)+\sin^2(n\varphi)} \\ &= r^{-n}(\cos(n\varphi) - i\sin(n\varphi)) = r^m(\cos(-m\varphi) - i\sin(-m\varphi)) \\ &= r^m(\cos(m\varphi) + i\sin(m\varphi)) \end{aligned}$$

Für $r = 1$ ist dieser Satz als *Moivresche Formel* bekannt.

Jetzt können wir alle komplexen Lösungen von $z^n = 1$ konstruieren: Man zeichne in den Einheitskreis ein regelmäßiges n–Eck mit einer Ecke in $(1, 0)$. Genau jede der n Ecken liefert uns eine Lösung.

Beispiel: $n = 4 \Rightarrow z_1 = 1,\ z_2 = i,\ z_3 = -1,\ z_4 = -i.$

Das Verfahren funktioniert auch bei Gleichungen der Art $z^n = a + ib$.

Aufgabe: Sei $n \in \mathbb{N}$ und $z = a + ib \in \mathbb{C}$ gegeben, gesucht sind alle z_k mit $z_k^n = z$.

Lösung: Wir suchen $z_k = r_k(\cos\varphi_k + i\sin\varphi_k)$ mit $z_k^n = r_k^n(\cos(n\varphi_k) + i\sin(n\varphi_k)) = z = r(\cos\varphi + i\sin\varphi)$

1. Alle Lösungen haben die gleiche Länge $r_k = \sqrt[n]{r}$.

2. Eine Lösung ist einfach anzugeben: $z_0 = \sqrt[n]{r}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)$.

3. Sämtliche Lösungen sind Ecken eines regelmäßigen n–Ecks, eingezeichnet in den Kreis um den Ursprung mit Radius $\sqrt[n]{r}$ und einer Ecke in z_0 .

4. Die Lösungen sind $z_k = \sqrt[n]{r}\left(\cos(\frac{\varphi}{n} + k\frac{2\pi}{n}) + i\sin(\frac{\varphi}{n} + k\frac{2\pi}{n})\right)$ für $k = 0, \ldots, n-1$.

Beispiel: $z^3 = 2i = 2\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$. Gemäß 2. ist $z_0 = \sqrt[3]{2}\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right) = \sqrt[3]{2}\left(\frac{1}{2}\sqrt{3} + \frac{1}{2}i\right)$.
Als weitere Lösungen erhält man $z_1 = \sqrt[3]{2}\left(\cos(\frac{\pi}{6} + \frac{2\pi}{3}) + i\sin(\frac{\pi}{6} + \frac{2\pi}{3})\right) = \sqrt[3]{2}\left(-\frac{1}{2}\sqrt{3} + \frac{1}{2}i\right)$ und
$z_2 = \sqrt[3]{2}\left(\cos(\frac{\pi}{6} + 2\cdot\frac{2\pi}{3}) + i\sin(\frac{\pi}{6} + 2\cdot\frac{2\pi}{3})\right) = -\sqrt[3]{2}\cdot i.$