Mathematik I
Lineare Algebra
WS 2024

1 Logik

Definition 1.1. Logik ist die *Lehre vom Argumentieren*, bzw. die *Lehre vom Schlussfolgern*. Sie hat das Ziel, die Regeln des Argumentierens so streng zu setzen, dass Widersprüche und Paradoxen möglichst ausgeschlossen sind.

1.1 Begriffe in der Logik

Aussage:	Ein Satz, der in einem gegebenen Kontext eindeutig wahr oder falsch ist
Konjunktion:	Eine logische Verknüpfung (z. B. ünd", öder")
Negation:	Umkehrung des Wahrheitswertes einer Aussage
Implikation:	Aus Aussage A folgt Aussage B
Tautologie:	Eine Aussage, die immer wahr ist
Kontradiktion	Eine widersprüchliche Aussage, die immer falsch ist

1.2 Logische Gesetze

De-Morgansche Gesetze:	$\neg(A \wedge B) \iff \neg A \vee \neg B$
	$\neg(A \vee B) \iff \neg A \wedge \neg B$
Kommutativgesetz:	$A \wedge B \iff B \wedge A$
	$A \vee B \iff B \vee A$
Assoziativgesetz:	$A \wedge (B \wedge C) \iff (A \wedge B) \wedge C$
	$A \vee (B \vee C) \iff (A \vee B) \vee C$
Distributivgesetz:	$A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$
	$A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$
Absorptionsgesetz:	$A \wedge (A \vee B) \iff A$
	$A \vee (A \wedge B) \iff A$

1.3 Quantoren

Existenzquantor:	$\exists n \in \mathbb{N}$	Es existiert ein n in der Menge der natürlichen Zahlen, für das gilt ...
Allquantor:	$\forall n \in \mathbb{N}$	Für alle Zahlen n in der Menge der natürlichen Zahlen gilt, ...

1.4 Beweisarten

1.4.1 Direkter und Indirekter Beweis

Direkter Beweis:	$A \longrightarrow B$
Beispiel n ist gerade $\longrightarrow n^2$ ist gerade	$\exists n \in \mathbb{N} : n = 2k \Longrightarrow n^2 = (2k)^2 = 4k^2 = \underbrace{2(2k)}_{\in \mathbb{N}}$

Indirekter Beweis (Widerspruchsbeweis):	$\neg A \longrightarrow$ Widerspruch
Beispiel Behauptung: $\sqrt{2}$ ist irrational	Annahme: $\sqrt{2}$ ist rational
	$\sqrt{2} = \frac{a}{b} \Longrightarrow 2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2$
	$\Longrightarrow a^2$ ist gerade $\Longrightarrow a$ ist gerade
	$\Longrightarrow a = 2k \Longrightarrow 2b^2 = 4k^2 \Longrightarrow b^2 = 2k^2$
	$\Longrightarrow b^2$ ist gerade $\Longrightarrow b$ ist gerade
	$\Longrightarrow$ Widerspruch, da a und b beide gerade sind

1.4.2 Beweis durch vollständige Induktion

Die vollständige Induktion besteht aus folgenden Schritten:

1. Induktionsanfang: Zeige, dass die Aussage für ein beliebiges n gilt (meist $n = 0$ oder $n = 1$).
2. Induktionsvoraussetzung: durch den Induktionsanfang ist bewiesen, dass es mindestens ein n gibt, für das die Aussage stimmt.
3. Induktionsbehauptung: Es wird angenommen, dass wenn die Aussage für n stimmt, dass sie auch für $n + 1$ stimmen muss.
4. Induktionsschritt: Beweis, dass die Induktionsbehauptung richtig ist.

Das genaue Vorgehen beim Induktionsbeweis hängt von der konkreten Aussage ab.

Beispiel (Gaußsche Summenformel):

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Induktionsanfang (IA): $n = 1 \quad 1 = \frac{2}{2} \quad \checkmark$

Induktionsvoraussetzung (IV): $\exists n \in \mathbb{N} : \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

Induktionsbehauptung (IB): $\sum_{k=1}^{n+1} k = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$

Induktionsschritt (IS):

$$\sum_{k=1}^{n+1} k = \underbrace{\sum_{k=1}^{n} k}_{\text{IV}} + (n+1)$$

$$= \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1)+2(n+1)}{2}$$

$$= \frac{n^2+n+2n+2}{2}$$

$$= \frac{(n+1)(n+2)}{2} \qquad \square$$

2 Mengenlehre

Definition 2.1. Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

2.1 Beispiele von Mengen

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$	(Natürliche Zahlen)
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$	(Ganze Zahlen)
$\mathrm{M} = \{1, \pi, a\}$	
$\mathrm{N} = \{x \in \mathbb{Z} \mid x = k^2\}$	
$\mathrm{O} = \emptyset$ oder $\{\}$	(Leere Menge)

2.2 Definitionen

Eine Menge M ist eine **Teilmenge** von N, wenn jedes Element von M auch in N enthalten ist.

$$M \subseteq N \Longleftrightarrow \forall x (x \in M \Longrightarrow x \in N)$$

Die **Schnittmenge** von M und N ist die Menge aller Elemente, die sowohl Teil von M als auch Teil von N sind.

$$M \cap N = \{x \mid x \in M \wedge x \in N\}$$

Wenn $M \cap N = \emptyset$, dann heißen M und N **disjunkt**.

Die **Vereinigungsmenge** von M und N ist die Menge aller Elemente, die in M oder in N enthalten sind.

$$M \cup N = \{x | x \in M \vee x \in N\}$$

Sind $M, N, C \subseteq$	gilt:	
Kommutativgesetz:	$M \cap N = N \cap M$	$M \cup N = N \cup M$
Assoziativgesetz:	$M \cap (N \cap C) = (M \cap N) \cap C$	$M \cup (N \cup C) = (M \cup N) \cup C$
Distributivgesetz:	$M \cap (N \cup C) = (M \cap N) \cup (M \cap C)$	$M \cup (N \cap C) = (M \cup N) \cap (M \cup C)$
Absorptionsgesetz:	$M \cap (M \cup N) = M$	$M \cup (M \cap N) = M$

Die **Differenzmenge** von M und N besteht aus allen Elementen der Menge M, die nicht in N enthalten sind.

$$M \setminus N = \{x | x \in M \wedge x \notin N\}$$

Die **Menge aller Teilmengen** einer Menge M wird als $P(M)$ angegeben.

$$M = \{1, a, \pi\}$$
$$P(M) = \emptyset, M, \{1\}, \{a\}, \{\pi\}, \{1, a\}, \{1, \pi\}, \{a, \pi\}$$

Die Anzahl der Elemente in einer Menge bezeichnet man als **Kardinalität** oder **Mächtigkeit**. Geschrieben wird sie als

$$|M| = ...$$

Die Anzahl der möglichen Teilmengen ist

$$|P(M)| = 2^{|M|}$$

Anmerkung 2.1. Die Kardinalität der Menge der natürlichen Zahlen ist $|\mathbb{N}| = \aleph_0$, welche als kleinste abzählbare Unendlichkeit bekannt ist.

2.3 Kartesisches Produkt

Das **kartesische Produkt** einer Menge M und einer Menge N ist definiert als

$$M \times N := \{(a, b) | a \in M, b \in N\}$$

Die Kardinalität des kartesischen Produkts ist definiert als

$$|M \times N| = |M| \cdot |N|$$

2.4 Relationen

Eine **Relation** R zwischen einer Menge M und einer Menge N ist eine Beziehung zwischen Elementen von M und N, geordnet in Paare (m, n) mit $m \in M$ und $n \in N$. Daraus folgt, dass jede Relation zwischen zwei Mengen eine Teilmenge des kartesischen Produkts ebendieser ist. Eine Relation wird geschrieben als $\sim_R$. Gilt $M = N$, so heißt die Relation **homogen**.

Betrachtet man eine Funktion $f : D \longrightarrow \mathbb{R}$ mit $D \subseteq \mathbb{R}$, so ist diese Funktion eine Relation R zwischen D und $\mathbb{R}$ mit der Eigenschaft:

$$\forall x \in D \; \exists^{=1} y \in \mathbb{R} : (x, y) \in R$$

Daraus lässt sich allgemein feststellen, dass eine Funktion $f : D \longrightarrow N$ eine Relation R zwischen D und N ist, für die gilt:

$$\forall x \in D \; \exists^{=1} y \in N : (x, y) \in R$$

2.5 Eigenschaften von homogenen Relationen

Reflexiv:	$\forall m \in M : m \sim_R m$
Transitiv:	$m_1 \sim_R m_2 \wedge m_2 \sim_R m_3 \Longrightarrow m_1 \sim_R m_3$
Symmetrisch:	$m_1 \sim_R m_2 \Longrightarrow m_2 \sim_R m_1$
Antisymmetrisch:	$m_1 \sim_R m_2 \wedge m_2 \sim_R m_1 \Longrightarrow m_1 = m_2$
Asymmetrisch :	$m_1 \sim_R m_2 \Longrightarrow \neg(m_2 \sim_R m_1)$

Außerdem heißt R **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

2.6 Äquivalenzklassen

Betrachtet man eine Äquivalenzrelation $\sim_R$ auf eine Menge M mit zwei Elementen $m, n \in M$, so heißen diese **äquivalent**, wenn $m \sim_R n$.

Eine Teilmenge $a \subseteq M$ heißt **Äquivalenzklasse**, wenn gilt

- Sind $m, n \in A,$ so ist $m \sim_R n$
- Ist $m \in A \wedge n \in M$ mit $n \sim_R m,$ so ist $n \in A$

Das bedeutet, die Äquivalenzklasse $[a]$ enthält alle Elemente, die mit a in Relation stehen. Existiert eine Äquivalenzrelation $\sim_R$ auf M und sind $m, n \in M$, dann gilt entweder $[m] = [n]$ oder $[m]$ und $[n]$ sind disjunkt.

2.7 Repräsentantensystem

Ein **Repräsentant** einer Äquivalenzklasse $[a]$ ist ein Element $a \in [a]$, das die Klasse repräsentiert.

Ein **Repräsentantensystem** ist eine Teilmenge $N \subseteq M$ die genau einen Repräsentanten jeder Äquivalenzklasse enthält.

Beispiel 2.1. Gegeben ist die Relation "modulo 3äuf der Menge $\mathbb{Z}$. Zwei Zahlen a, b sind äquivalent bezüglich dieser Relation, wenn sie bei der Division durch 3 den gleichen Rest haben. Mathematisch bedeutet das:

$$a \equiv b (\mathrm{mod}\, 3) \quad \text{wenn} \quad 3 \mid a - b$$

Die Äquivalenzklassen für diese Äquivalenzrelation sind die Menge aller Elemente, die zueinander äquivalent sind. In diesem Fall existieren drei Äquivalenzklassen, nämlich für jeden möglichen Rest (0, 1, 2) der Division jeweils eine.

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

Nun kann man ein Repräsentantensystem für diese Äquivalenzrelation aufstellen. Dafür nimmt man aus jeder Äquivalenzklasse ein beliebiges Element (da die Elemente alle untereinander äquivalent sind, repräsentiert ein beliebiges Element die gesamte Klasse).

Ein mögliches Repräsentantensystem für diese Relation ist:

$$\{0, 1, 2\}$$

3 Algebraische Strukturen

3.1 Halbgruppen, Monoide, Gruppen

Definition 3.1. Gegeben ist eine Menge M. Verknüpft man zwei Elemente $m_1, m_2 \in M$ und ist das Ergebnis ebenfalls ein Element aus M, so spricht man von einem **Magma**.

Die innere Verknüpfung wird oft als $\circ$ gekennzeichnet und ist formal definiert ist:

$$\circ : M \times M \longrightarrow M$$

Beispiele für die innere Verknüpfung sind die Addition oder die Multiplikation.

Die Schreibweise eines Magmas ist $(M, \circ)$.

Definition 3.2. Gilt für das Magma das **Assoziativgesetz**, also gilt für alle $a, b, c \in M$:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

so heißt das Magma $(M, \circ)$ eine **Halbgruppe**.

Beispiel 3.1. Folgende Beispiele sind Halbgruppen: $(\mathbb{Z}, +)$, $(\mathbb{R}, \cdot)$

Existiert in der Halbgruppe zusätzlich ein **neutrales Element** $e \in M$, sodass gilt

$$\forall a \in M : a \circ e = e \circ a = a$$

so heißt die Halbgruppe eine **Monoid**.

Beispiel 3.2. Folgende neutrale Elemente existieren als Beispiel: $(\mathbb{Z}, +)$: 0, $(\mathbb{R}, \cdot)$: 1, $(P(M), \cup)$: $\emptyset$

Existiert in der Monoid zusätzlich zu dem neutralen Element ein **inverses Element** $a^{-1} \in M$, sodass gilt

$$a \circ a^{-1} = a^{-1} \circ a = e$$

so heißt die Monoid eine **Gruppe**.

Beispiel 3.3. Folgende Beispiele sind Gruppen: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$

Anmerkung 3.1. Ist eine Gruppe zusätzlich noch kommutativ, also wenn

$$\forall a, b \in M : a \circ b = b \circ a$$

gilt, so spricht man von einer **abelschen Gruppe**.

3.1.1 Permutationsgruppen

Eine **Permutation** ist eine bijektive Abbildung von einer Menge auf sich selbst. Das bedeutet, dass die Permutation die gleichen Elemente wie die Ausgangsmenge beinhaltet und lediglich die Reihenfolge verändert wird. Diese permuttierten Elemente werden als $\sigma \in S_N$ bezeichnet.

Betrachtet man die Zahlen, die vertauscht wurden, so spricht man von **Transpositionen**.

Beispiel 3.4. Gegeben ist

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Vertauscht wurden unter anderem die Zahlen 1 und 2, also spricht man von der Transposition $\tau_{12} = \langle 1\ 2 \rangle$

Die Verknüpfung, bei der die Permutation die gleiche Reihenfolge wie die Ausgangsmenge abbildet, nennt man id.

Ist $\tau = \langle i\ k \rangle$, so gilt:

$$\tau \circ \tau = \mathrm{id}$$

Eine wichtige Eigenschaft von Permutationen ist außerdem die **Signatur**. Die Signatur $\mathrm{sign}(\sigma)$ ist die Anzahl der Fehlstände, also der Anzahl an Vertauschungen, bei denen $i < j$ aber $\sigma(i) > \sigma(j)$ gilt.

Die Signatur ist definiert als:

$$\text{sign}(\sigma) = \begin{cases} +1 & \text{für gerade Anzahl an Vertauschungen} \\ -1 & \text{für ungerade Anzahl an Vertauschungen} \end{cases}$$

Um die Signatur zu bestimmen kann man entweder alle Fehlstände zählen oder die folgende Formel verwenden:

$$\text{sign}(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

3.1.2 Endliche Gruppen

Eine Gruppe G heißt **endlich**, wenn $|G| < \infty$, also wenn G nur endlich viele Elemente hat.

Die Ordnung der Gruppe G ist die Anzahl der Elemente in G, also $\text{ord}(G) = |G| = n$. Die Ordnung eines Elements $g \in G$ ist das kleinste $n \geq 1$ für das gilt: $g^n = e$. Also in anderen Worten, es muss ein $g^n \in G$ existieren, für das am Ende das neutrale Element e herauskommt und das kleinste n, für das dies gilt, bezeichnet man als Ordnung der Gruppe.

Anmerkung 3.2. Die Ordnung eines Elements g ist immer ein Teiler der Ordnung der Gruppe G.

$$\text{ord}(g) \mid \text{ord}(G)$$

Beispiel 3.5. Gegeben ist die Gruppe $(\mathbb{Z}\backslash 7\mathbb{Z}, \cdot, 1)$. Die gegebene Menge ist die Restklasse von $\mathbb{Z} \mod 7$ und somit endlich, da sie nur aus den Elementen $\{1, 2, 3, 4, 5, 6\}$ besteht. Das bedeutet, $\text{ord}(G) = 6$. Somit muss jedes $g \in G$ die Ordnung $1, 2, 3$ oder 6 haben.

Um die Ordnung für ein Element $g \in G$ zu bestimmen, multipliziert man es solange mit sich selbst, bis das neutrale Element e (in diesem Fall 1) herauskommt. Für beispielsweise $g = 3$ ergibt sich dadurch:

$$\begin{aligned} 3^1 &\equiv 3 \\ 3 \cdot 3 = 3^2 &\equiv 2 \\ 3 \cdot 3 \cdot 3 = 3^3 &\equiv 6 \\ 3 \cdot 3 \cdot 3 \cdot 3 = 3^4 &\equiv 4 \\ 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^5 &\equiv 5 \\ 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6 &\equiv 1 \\ \text{ord}(3) &= 6 \end{aligned}$$

3.2 Ringe

Ein **Ring** ist ein Tripel $(R, +, \cdot)$, mit einer nicht leeren Menge R und zwei Verknüpfungen $+$ und $\cdot$, für das gilt:

- $(R, +, 0)$ ist eine abelsche Gruppe
- $(R, \cdot, 1)$ ist eine Halbgruppe
- Es gilt das Distributivgesetz

Ist $(R, \cdot, 1)$ ein Monoid, so spricht man von einem **unitären Ring**. Ist das Monoid $(R, \cdot, 1)$ zusätzlich ein kommutatives Monoid, spricht man von einem kommutativen unitären Ring.

3.3 Körper

Ein **Körper** ist im Endeffekt nichts anderes als ein Ring, bei dem $(R\backslash\{0\}, \cdot, 1)$ eine abelsche Gruppe ist.

4 Zahlentheorie

4.1 Teilbarkeit

Definition 4.1. Gegeben ist ein Ring $(R, +, \cdot)$ mit den neutralen Elementen 0 (bzgl. der Addition) und 1 (bzgl. der Multiplikation).

Nimmt man drei Zahlen $a, b, q \in R$, so heißt a genau dann **Teiler** von b, wenn es ein q gibt, sodass gilt:

$$b = a \cdot q$$

In diesem Fall schreibt man auch $a \mid b$. Existiert kein q, für das diese Gleichung erfüllt wird, ist a kein Teiler von b und wir schreiben $a \nmid b$.

Beispiel 4.1. Folgende Beispiele zeigen die Teilbarkeit von verschiedenen Zahlen

- $3 \mid 9$, da $9 = 3 \cdot 3$
- $3 \nmid 10$, da $10 = 3 \cdot 3 + 1$
- $a \mid 0$, da $0 = a \cdot 0$
- $a \mid a$, da $a = a \cdot 1$

4.2 gT und gV

Ist a ein Teiler von b und ein Teiler von c, so ist a ein gemeinsamer Teiler (gT) von b und c. Also wenn gilt:

$$a \mid b \wedge a \mid c \Longrightarrow c = \mathrm{gT}(a, b)$$

Analog dazu gilt, wenn b ein Teiler von a und c ein Teiler von a ist, dann ist a ein gemeinsames Vielfaches von b und c:

$$b \mid a \wedge c \mid a \Longrightarrow a = \mathrm{gV}(b, c)$$

Außerdem wird der größte gemeinsame Teiler als ggT bezeichnet und das kleinste gemeinsame Vielfache als kgV.

4.3 Teilbarkeitsregeln

TO DO

4.4 Primzahlen

Davon ausgehend lassen sich ebenfalls **Primzahlen** definieren. Eine Zahl p ist genau dann eine Primzahl, wenn sie lediglich 1 und sich selbst als Teiler hat.

Die Menge aller Primzahlen wird als $\mathbb{P}$ bezeichent. Wenn $d(n)$ die Anzahl an Teilern von n ist, ist die Menge $\mathbb{P}$ definiert als:

$$\mathbb{P} = \{n \in \mathbb{N} \mid d(n) = 2\}$$

Außerdem gilt nach dem **Lemma von Euklid**, dass wenn das Produkt zweier natürlicher Zahlen durch eine Primzahl teilbar ist, dann ist mindestens einer der Faktoren durch die Primzahl teilbar. Das bedeutet, dass für alle $p \in \mathbb{P}$ gilt:

$$p \mid a \cdot b \Longrightarrow p \mid a \vee p \mid b$$

4.5 Hauptsatz der Arithmetik

Der Haupsatz der Arithmetik besagt, dass jede natürliche Zahl n als Produkt von Primzahlen dargestellt werden kann. Diese Darstellung nennt man auch Primfaktorzerlegung.

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

Beispiel 4.2. Einige Zahlen in ihre Primfaktoren zerlegt:

- $120 = 2^3 \cdot 3^1 \cdot 5^1$
- $144 = 2^4 \cdot 3^1$
- $250 = 2^1 \cdot 5^3$

Diesen Haupsatz kann man anwenden, um den ggT und das kgV von zwei Zahlen zu berechnen. Im ersten Schritt zerlegt man die Zahlen in ihre Primfaktoren und als Potenzen aufschreibt. Anschließend betrachtet man die Exponenten (also die Anzahl, wie oft eine Primzahl vorkommt) und entsprechend, ob man den ggT oder das kgV betimmen möchte, nimmt man:

- ggT:Die kleinste Potenz, die in beiden Zerlegungen vorkommt
- kgV:Die größte Potenz, die in beiden Zerlegungen vorkommt

Beispiel 4.3. Gegeben sind die Zahlen 4620 und 9100. Im ersten Schritt zerlegen wir die beiden Zahlen in ihre Primfaktoren:

$$4620 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1$$
$$9100 = 2^2 \cdot 5^2 \cdot 7^1 \cdot 13^1$$

Aus den Exponenten der Primfaktoren lassen sich nun der ggT und das kgV bestimmen.

$$\text{ggT}(4620, 9100) = 2^2 \cdot 5^1 \cdot 7^1 = 140$$
$$\text{kgV}(4620, 9100) = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 11^1 \cdot 13^1 = 300300$$

4.6 Lemma von Bézout

Das **Lemma von Bézout** besagt, dass der ggT zweier ganzen Zahlen a und b als Linearkombination der Form

$$\text{ggT}(a, b) = s \cdot a + t \cdot b$$

mit $s, t \in \mathbb{Z}$ dargestellt werden kann.

Formell ausgedrückt heißt das

$$\forall a, b \in \mathbb{Z} : \exists s, t \in \mathbb{Z} : \text{ggT}(a, b) = s \cdot a + t \cdot b$$

Dabei bezeichnet man s und t als **Bézout-Koeffizienten**.

4.7 Erweiterter Euklidischer Algorithmus

Die Berechnung des ggT durch die Primfaktorzerlegung ist zwar recht einfach, jedoch auch relativ aufwendig, gerade wenn wir mit größeren Zahlen arbeiten. Zur Berechnung des ggT gibt es daher ein Verfahren, das bereits in der Antike entdeckt wurde: den **Euklidischen Algorithmus**. Dieser hat die Form:

$$a = q \cdot b + r$$

wobei a der größere Wert ist, b der kleinere Wert, q der Faktor, wie oft der kleinere Wert in den größeren passt und r der Rest, der übrig bleibt.

Beispiel 4.4. Die Bestimmung des ggT von 4620 und 9100 mit dem erweiterten euklidischen Algorithmus sieht folgendermaßen aus:

$$9100 = 1 \cdot 4620 + 4480 \quad (1)$$
$$4620 = 1 \cdot 4480 + 140 \quad (2)$$
$$4480 = 32 \cdot 140 + 0 \quad (3)$$

Ausgehend davon lassen sich ebenfalls die sogenannen Bézout-Koeffizienten bestimmen. Dazu wenden wir den **erweiterten Euklidischen Algorithmus** an. Zunächst starten wir in der Zeile, in der der ggT als Rest steht. Für das obige Beispiel ist das Zeile (2).

Diese Zeile stellen formen wir nun so um, dass auf der einen Seite der Rest (bzw. der ggT) und auf der anderen Seite der restliche Teil der Gleichung steht. In unserem Beispiel also:

$$140 = 4620 - 1 \cdot 4480$$

Betrachten wir nun die vorherigen Zeilen, so lässt sich feststellen, dass (für das obige Beispiel) 4480 wiederum nichts anderes als der Rest der vorherigen Zeile ist. Diese können wir also ebenfalls umformen und für 4480 einsetzen:

$$140 = 4620 - 1 \cdot (9100 - 1 \cdot 4620)$$

Nun lässt sich diese Gleichung noch ausmultiplizieren, sodass die Gleichung die Form:

$$140 = 2 \cdot 4620 - 1 \cdot 9100$$

annimmt. Dieses Vorgehen wiederholen wir solange, bis wir bei der ersten Zeile angekommen sind (was für unser Beispiel jetzt der Fall ist). Die Koeffizienten, die vor den beiden Zahlen stehen, sind die sogenannten **Bézout-Koeffizienten**.

4.8 Kleiner Satz von Fermat

Der kleine Satz von Fermat besagt: *Es sei p eine Primzahl. Dann gilt für jede Zahl $k \in \mathbb{Z}_p^*$*

$$k^{p-1} \equiv 1 \pmod{p}$$

5 Komplexe Zahlen

Betrachten wir eine Gleichung

$$x^2 + 1 = 0$$

so können wir in der Menge der reellen Zahlen keine Lösung für x finden, da $x = \sqrt{-1}$ wäre und die Wurzel einer negativen Zahl nicht in den reellen Zahlen definiert ist.