Mathematik für Wirtschaftsinformatik I

von
J.B. Cooper
(mit Ergänzungen von K. Kiener)

WS 1998/99/00/01

Inhaltsverzeichnis

Kapitel 1

Zahlen & Logik

1.1 Natürliche Zahlen

Wir verwenden den Buchstaben $\mathbf{N}$, um die Menge der natürlichen Zahlen zu bezeichnen, d.h.

$$\mathbf{N} = \{1, 2, 3, \dots\}.$$

$n \in \mathbf{N}$ bedeutet: n ist eine natürliche Zahl. Mit $\mathbf{N}_0$ bezeichnen wir die Menge $\{0, 1, 2, \dots\}$. Die relevanten Eigenschaften von $\mathbf{N}$ sind Konsequenzen der folgenden Axiome von Peano:

a) 1 ist eine natürliche Zahl und jede Zahl n besitzt einen **Nachfolger** geschrieben n'. Weiters gilt:

b) Der Nachfolger von $n \in \mathbf{N}$ ist eindeutig bestimmt;

c) jedes $n \neq 1$ aus $\mathbf{N}$ ist Nachfolger von genau einem $m \in \mathbf{N}$;

d) falls A eine Teilmenge von $\mathbf{N}$ ist, sodaß $1 \in A$ und der Nachfolger von jedem $n \in A$ auch in A ist, dann gilt $A = \mathbf{N}$.

Die letzte Aussage heißt **Prinzip der vollständigen Induktion** (auch Prinzip der mathematischen Induktion).
Die Menge $\mathbf{N}_0$ besitzt eine Addition und eine Multiplikation d.h. Operationen

$$(m, n) \mapsto m + n \text{ bzw. } (m, n) \mapsto mn.$$

Das folgt aus den Axiomen wie folgt: Für jedes m definieren wir $m + 1 = m'$. Wir setzen dann $m + n' = (m + n)'$. Es folgt aus dem Prinzip der mathematischen Induktion, daß $m + n$ wohl definiert ist. Ähnlicherweise kann man die Axiome von Peano verwenden, um Multiplikation zu definieren (Aufgabe für den Leser). (Dies ist ein Beispiel einer **rekursiven Definition**. Solche Methoden sind gerade in der Informatik äußerst wichtig.)
Es gilt:

$$\begin{aligned} m + n &= n + m, \quad (m + n) + p = m + (n + p) \\ m + 0 &= m \\ mn &= nm, \quad (mn)p = m(np), m \cdot 1 = m \\ m(n + p) &= mn + mp \quad (m, n, p \in \mathbf{N}_0). \end{aligned}$$

BEISPIELE. Zeige: $1+2+\cdots+n=\frac{n}{2}(n+1)$.
Sei A die Menge aller $n\in\mathbf{N}$, für die die Formel gilt: d.h.

$$A=\left\{n: 1+2+\cdots+n=\frac{1}{2}n(n+1)\right\}.$$

Es ist klar, daß $1\in A$, und wir zeigen, daß aus $n\in A$ folgt $n+1\in A$. $n\in A$ bedeutet, daß die Formel $1+2+\cdots+n=\frac{1}{2}n(n+1)$ gilt. Dann:

$$\begin{aligned}1+\cdots+n+(n+1) &= (1+\cdots+n)+n+1\\ &= \frac{1}{2}n(n+1)+(n+1)\\ &= (n+1)\left(\frac{n}{2}+1\right)\\ &= \frac{n+1}{2}((n+1)+1)\end{aligned}$$

d.h. $n+1\in A$. Daraus folgt, daß $A=\mathbf{N}$, d.h. die Formel gilt für jedes $n\in\mathbf{N}$.

Die Ordnungsstruktur: $\mathbf{N}$ hat zusätzlich eine Ordnungsstruktur: Wir definieren

$$m<n \Leftrightarrow \text{ es existiert } p\in\mathbf{N} \text{ mit } m+p=n.$$

Identifizieren wir die Elemente aus $\mathbf{N}$ mit den Gitterpunkten einer Zahlengerade, dann bedeutet $m<n$, daß m links von n liegt. Dann gilt: Aus $m<n$ folgt $mp<np$, $m+p<n+p$ $(m,n,p\in\mathbf{N})$.

Der Divisionsalgorithmus (Euklidischer Algorithmus): Seien $m,n\in\mathbf{N}$. Dann existieren $q,r\in\mathbf{N}_0$ sodaß

$$m=nq+r \text{ mit } 0\le r<n.$$

Dabei sind q,r eindeutig bestimmt.
Falls $r=0$, dann ist n **ein Teiler** von m (geschrieben $n|m$). m ist eine **Primzahl**, falls m und 1 die einzigen Teiler von m sind.

BEISPIEL. Berechne alle Primzahlen ≤ 100. Wir benutzen das sogenannte **Sieb von Eratosthenes** d.h. wir streichen sukzessive die Vielfachen von $2,3,5,7,\ldots$ durch. Die Zahlen, die übrigbleiben, sind prim:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100.

Die gesuchten Primzahlen sind daher $2,3,5,7,11,13,17,19,23,29,31,37,41,43,$
$47,53,59,61,67,71,73,79,83,89,97$.

Schon Euklid hat bewiesen, daß es unendlich viele Primzahlen gibt. Der Beweis lautet wie folgt: Wir nehmen an, daß nur endlich viele Primzahlen $p_1, \ldots, p_n$ existieren und führen diese Annahme zu einem Widerspruch. Sei N die Zahl $p_1 p_2 \cdots p_n + 1$. Die Primzahlen $p_1, \ldots, p_n$ sind keine Teiler von N, N hat aber mindestens *eine* Primzahl als Teiler. Daher können wir unsere Liste um mindestens eine Primzahl erweitern, und das ist schon der gesuchte Widerspruch.

Darstellungen von natürlichen Zahlen: Als Anwendung des Divisionsalgorithmus haben wir folgende Aussage: Sei $n \in \mathbf{N}$, $n > 1$. Dann hat jedes $m \in \mathbf{N}$ eine eindeutige Darstellung

$$m = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_0,$$

wobei $0 \leq a_i < n$ (und $a_k \neq 0$).
Diese Darstellung heißt die **n-are Entwicklung von** m. Die wichtigsten Fälle in der Praxis sind

$n = 10$ – Dezimalentwicklung;

$n = 2$ – Dyadische Entwicklung;

$n = 16$ – Hexadezimalentwicklung.

Die Koeffizienten $a_0, a_1, \ldots, a_k$ sind die Restglieder nach sukzessiven Divisionen wie im folgenden Schema:

$$\begin{aligned} m &= q_0 n + a_0 \\ q_0 &= q_1 n + a_1 \\ &\vdots \\ q_{k-1} &= q_k n + a_k \text{ (wobei } q_k = 0). \end{aligned}$$

Beispiel. Stelle die Dezimalzahl 27 in dyadischer Form dar

$$\begin{aligned} 27 &= 2.13 + 1 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

Daher ist die dyadische Darstellung 11011.

Eine wichtige Zahl ist $n! = 1 \cdot 2 \cdot 3 \cdots n$, das Produkt der ersten n natürlichen Zahlen. $n!$ (gesprochen "n Fakultät" oder "n faktorielle") ist die Anzahl der möglichen Anordnungen von n verschiedenen Elementen.
$n!$ wächst sehr schnell mit n $(1, 2, 6, 24, 120, 750, 5040, 40320, 362880, 3628800 (= 10!)$,
$15! \sim 1.3 \times 10^{12}, 20! \sim 2.43 \times 10^{18}, 30! \sim 2.65 \times 10^{32}, 40! \sim 8.16 \times 10^{47})$.
Diese Zahlen stehen in enger Beziehung zu dem sogenannten Pascalschen Dreieck, wobei jedes Element die Summe der zwei oberen Elemente ist. Wir bezeichnen mit $\binom{n}{r}$ das Element in der n-ten Reihe und r-ten Diagonale. $\binom{n}{r}$ ist die Anzahl der Möglichkeiten, aus einer Menge von n unterschiedlichen Elementen r Objekte auszuwählen, wobei die Reihenfolge nicht entscheidend ist.

Es gilt dann

$$\binom{n}{r} = \frac{n!}{(n-r)!r!}.$$

Eine wichtige Formel ist:

$$\binom{n}{r} + \binom{n}{r+1} = \binom{n+1}{r+1}.$$

Die Koeffizienten $\binom{n}{r}$ spielen eine wichtige Rolle in der Mathematik, z.B. in dem

Binomialsatz:

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r.$$

1.2 Rationale Zahlen & Reelle Zahlen

Rationale Zahlen

(Positive) Rationalzahlen sind diejenigen der Gestalt $\frac{p}{q}$ $(p, q \in \mathbf{N})$. Wir bezeichnen die Menge solcher Zahlen mit $\mathbf{Q}^+$, – $\mathbf{Q}_0^+$ ist die Menge $\mathbf{Q}^+ \cup \{0\}$.
Wir können die Strukturen von $\mathbf{N}$ verwenden, um entsprechende Strukturen auf $\mathbf{Q}^+$ zu definieren:
Addition:

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}$$

Multiplikation:

$$\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$$

Ordnung:

$$\frac{p}{q} < \frac{r}{s} \Leftrightarrow ps < qr.$$

Die gewöhnlichen Rechenregeln gelten.
Jede Rationalzahl hat eine Darstellung der Gestalt

$$m + \frac{a_1}{10} + \cdots + \frac{a_r}{10^r} + \frac{1}{10^r}\left(\frac{b_1}{10} + \cdots + \frac{b_s}{10^s} + \frac{b_1}{10^{s+1}} + \cdots + \frac{b_s}{10^{2s}} + \frac{b_1}{10^{2s+1}} + \ldots\right)$$

(geschrieben $m, a_1 a_2 \ldots a_r \overline{b_1 \ldots b_s}$). (Die Koeffizienten liegen zwischen 0 und 9.)
Beispiel. $0, \overline{365} = 0,365365365365365\cdots = \frac{365}{999}$.

Reelle Zahlen

Schon die alten Griechen haben erkannt, daß es Zahlen gibt, die nichtrational sind z.B. gibt es kein $r \in \mathbf{Q}$, sodaß $r^2 = 2$. (Denn gäbe es p, q, sodaß $(\frac{p}{q})^2 = 2$, dann wäre $p^2 = 2q^2$. Daraus folgt, daß p^2 und daher auch p gerade sind. Setzen wir $p = 2p'$, so sehen wir, daß $q^2 = 2p'^2$. Daher ist auch q gerade. p und q haben also den gemeinsamen Faktor 2, den wir wegkürzen können. Aber das gleiche Argument erlaubt uns noch einmal einen Faktor 2 zu kürzen – und so weiter ad infinitum. Diese Situation ist offensichtlich unmöglich – also gibt es keine solchen p, q).

Daher führen wir den Begriff der (positiven) reellen Zahlen ein. Das sind diejenigen Zahlen, die Dezimalentwicklungen der Gestalt

$$m + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots \quad (m \in \mathbf{N}, 0 \leq a_i \leq 9)$$

(geschrieben $m, a_1 a_2 \ldots$) haben.
Wir bezeichnen die Menge solcher Zahlen mit $\mathbf{R}^+$.

Negative Zahlen

$\mathbf{R}$ bezeichnet die Menge aller Zahlen mit einer Darstellung

$$m, a_1 a_2 \ldots$$

oder

$$-m, a_1 a_2 \ldots$$

Z.B. $-1,41421\ldots, -3,14159\ldots$

$\mathbf{Z}$ bezeichnet die ganzen Zahlen $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

$\mathbf{Q}$ bezeichnet die rationalen Zahlen $\{\pm\frac{p}{q} : p \in \mathbf{N}_0, q \in \mathbf{N}\}$.

Auf $\mathbf{R}$ definieren wir

- eine Addition $(x, y) \mapsto x + y$
- eine Multiplikation $(x, y) \mapsto xy$
- eine Ordnungstruktur $x < y \Leftrightarrow y - x \in \mathbf{R}^+$.

Dann gilt:

1. $\mathbf{R}$ ist ein Körper (genaue Definitionen in der Vorlesung);
2. aus $x < y$ folgt $x + z < y + z$;
3. aus $x < y$ folgt $xz < yz$ falls $z > 0$; $xz > yz$ falls $z < 0$;
4. aus $0 < x < y$ folgt $\frac{1}{x} > \frac{1}{y}$, aus $x < y < 0$ folgt $\frac{1}{x} > \frac{1}{y}$, aus $x < 0 < y$ folgt $\frac{1}{x} < \frac{1}{y}$.

1.3 Die komplexen Zahlen

Identifizieren wir die Zahlen aus $\mathbf{R}$ mit Punkten aus der Zahlengeraden, so ist es natürlich, Punkte aus $\mathbf{R}^2$ (d.h. geordnete Paare (x, y)) mit Punkten einer Ebene zu identifizieren. Wir betrachten diese Objekte als Zahlen – die sogenannten "komplexen Zahlen" – und versehen die Menge $\mathbf{C}$ solcher Zahlen mit einer Addition und Multiplikation wie folgt:

$$\begin{aligned} (x_1, y_1) + (x_2, y_2) &= (x_1 + x_2, y_1 + y_2) \\ (x_1, y_1)(x_2, y_2) &= (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1). \end{aligned}$$

Verwenden wir den Buchstaben i für die komplexe Zahl $(0, 1)$ und identifizieren wir die reelle Zahl x mit der komplexen Zahl $(x, 0)$, so sehen wir:

1. daß $i^2 = -1$

2. daß jedes $z \in \mathbf{C}$ eine eindeutige Darstellung

$$z = x + iy$$

($x, y \in \mathbf{R}$) hat.

x heißt der **Realteil** von z (geschrieben $\Re z$). y heißt der **Imaginärteil** von z (geschrieben $\Im z$). Wir führen folgende Bezeichnung ein: $\bar{z} = x - iy$ heißt die zu z **konjugiert komplexe Zahl**; $|z| = \sqrt{(x^2 + y^2)} = \sqrt{z\bar{z}}$ – der **Absolutbetrag** von z. $\arg z =$ der Winkel $\theta \in [0, 2\pi[$, sodaß

$$\cos\theta = \frac{x}{|z|}, \sin\theta = \frac{y}{|z|} \quad (z \neq 0).$$

Wir haben die folgenden einfachen Beziehungen zwischen diesen Größen:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$$

$$\begin{aligned} |z_1 + z_2| &\leq |z_1| + |z_2| \\ |z_1 z_2| &= |z_1||z_2|. \end{aligned}$$

Falls $z \neq 0$, dann gilt $zz^{-1} = 1$ wobei $z^{-1} = \frac{\bar{z}}{|z|^2}$ **die Inverse** von z ist.

Die Polardarstellung: Jedes $z \neq 0$ aus $\mathbf{C}$ hat die Darstellung

$$z = \rho(\cos\theta + i\sin\theta)$$

wobei $\rho = |z|$ (und daher eindeutig bestimmt) und θ ein Winkel ist, mit $\cos\theta = \frac{x}{|z|}, \sin\mathbf{h} = \frac{y}{|z|}$ (d.h. $\theta = \arg z$ bis auf ein ganzzahliges Vielfaches von 2π). In bezug auf diese Darstellung hat die Multiplikation die einfache Gestalt:

$$z_1 z_2 = \rho_1\rho_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$$

wobei $z_1 = \rho_1(\cos\theta_1 + i\sin\mathbf{h}_1)$, $z_2 = \rho_2(\cos\theta_2 + i\sin\mathbf{h}_2)$.

Korollar 1.3.1 *(Gesetz von de Moivre). Für $n \in \mathbf{Z}$ gilt:*

$$(\cos\theta + i\sin\theta)^n = (\cos n\theta + i\sin n\theta).$$

Aus diesen Formeln folgt die wichtige Tatsache: Für jede komplexe Zahl

$$\zeta = \rho(\cos\theta + i\sin\theta)$$

(ungleich Null) und jedes $n \in \mathbf{N}$ existieren genau n komplexe Zahlen z, sodaß $z^n = \zeta$, nämlich

$$z = \rho^{1/n}\left(\cos\left(\frac{2k\pi + \theta}{n}\right) + i\sin\left(\frac{2k\pi + \theta}{n}\right)\right)$$

($k = 0, 1, \ldots, n-1$).

Insbesondere gibt es n komplexe Zahlen z, sodaß $z^n = 1$, nämlich

$$z = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad (k = 0, \ldots, n-1).$$

Sie heißen die n-ten **Wurzeln der Einheit**.
Eine der wichtigsten Eigenschaften der komplexen Zahlen ist der sogenannte

Satz 1.3.2 Fundamentalsatz der Algebra: *Sei p ein komplexes Polynom von Grad $n > 1$, etwa*

$$p(z) = a_0 + a_1 z + \cdots + a_n z^n.$$

Dann hat p genau n Nullstellen $\lambda_1, \ldots, \lambda_n$ d.h.

$$p(z) = a_n(z - \lambda_1)\cdots(z - \lambda_n).$$

Falls p ein reelles Polynom ist, etwa

$$p(t) = a_0 + a_1 t + \cdots + a_n t^n,$$

wobei die a_i reell sind, dann haben die Nullstellen von p die Gestalt:

$$\underbrace{t_1, \ldots, t_r}_{\text{reell}}, \quad \underbrace{\alpha_1 + i\beta_1, \alpha_1 - i\beta_1, \ldots, \alpha_s + i\beta_s, \alpha_s - i\beta_s}_{\text{konjungiert-komplexe Paare.}}, \quad r + 2s = n$$

Es gilt dann

$$p(t) = (t - t_1)\cdots(t - t_r)(t^2 - 2\alpha_1 t + \alpha_1^2 + \beta_1^2)\cdots(t^2 - 2\alpha_s t + \alpha_s^2 + \beta_s^2).$$

Die Zahlen $\exp z, \ln z, z^\alpha$: Für $z \in \mathbf{C}$ definieren wir $\exp(z)$ (oder einfach e^z) bzw. $\ln z$ (für $z \neq 0$) wie folgt

$$\begin{aligned} e^z &= e^x(\cos y + i\sin y) \quad (z = x + iy) \\ \ln z &= \ln|z| + i\mathbf{h}, \text{ wobei } z = |z|(\cos\mathbf{h} + i\sin\mathbf{h}) \end{aligned}$$

(Wegen der Mehrdeutigkeit der Wahl von $\mathbf{h}$ gibt es unendlich viele mögliche Werte für $\ln z$. Normalerweise wählt man $\mathbf{h} = \arg z$ (d.h. den Winkel $\mathbf{h}$, der zwischen 0 und 2π liegt). Der ensprechende Wert von $\ln z$ heißt der **Hauptwert** des Logarithmus. (Für die Funktionen exp, ln auf $\mathbf{R}$, siehe unten).)
Falls $z(\neq 0) \in \mathbf{C}$, $\alpha \in \mathbf{C}$, dann definieren wir $z^\alpha = \exp(\alpha \ln z)$.
Wegen der Mehrdeutigkeit des Logarithmus hat z^α i.a. unendlich viele mögliche Werte. Wählen wir den Hauptwert des Logarithmus, so bekommen wir den **Hauptwert** von z^α.
(N.B. Wenn $\alpha = n$ eine ganze Zahl ist, dann stimmen diese Werte alle überein, sodaß man in Wirklichkeit einen eindeutigen Wert hat. Falls $\alpha = \frac{p}{q}$ rational ist (wobei p und q keine gemeinsamen Faktoren besitzen), dann bekommt man q Werte.)

BEISPIELE. Berechne $e^i, \ln i, i^i$:

$$\begin{aligned} e^i &= \cos 1 + i\sin 1; \\ \ln i &= i\frac{\pi}{2} \text{ (Hauptwert)}; \\ i^i &= \exp(i\ln i) = \exp\left(-\frac{\pi}{2}\right) = e^{-\frac{\pi}{2}} \text{ (Hauptwert)}. \end{aligned}$$

Einfache Eigenschaften der Funktionen exp und ln:

$$\begin{aligned} \exp(z_1 + z_2) &= \exp z_1 \exp z_2; \\ \ln(z_1 z_2) &= \ln z_1 + \ln z_2 + 2i\epsilon\pi \quad (\epsilon = 1, 0, -1). \end{aligned}$$

Wir schließen dieses Kapitel mit einer Liste von Zahlensystemen und ihren charakteristischen Eigenschaften:

N
Division nicht immer möglich d.h. $ax = b$ nicht immer lösbar

$\mathbf{Q}^+$
Wurzel ziehen nicht immer möglich d.h. $x^2 = a$ nicht immer lösbar

$\mathbf{R}^+$
Subtrahieren nicht immer möglich da $x+a = b$ nicht immer lösbar

R
$x^2 = a$ nicht lösbar für a negativ

C
alle Polynomialgleichungen lösbar

1.4 Mengen und Abbildungen

In der Vorlesung haben wir mit "Mengen" und "Abbildungen" gearbeitet, ohne diese Begriffe genau zu erläutern.

BEISPIELE. Die Lösungsmenge des Systems:

$$\begin{aligned} 3x + 2y + z &= 6 \\ x + 3y - 7z &= 1. \end{aligned}$$

Die Menge aller ganzen Zahlen;
Die Menge $\mathbf{R}$ aller reellen Zahlen usw.

Versuchen wir, eine präzise Definition einer Menge zu geben, so kommen wir in Schwierigkeiten (vgl. den Versuch, in der euklidischen Geometrie einen Punkt zu definieren). Da die Feinheiten der Mengentheorie uns in dieser Vorlesung nicht besonders interessieren, werden wir einen eher pragmatischen Standpunkt einnehmen. Unter einer Menge versteht man "eine Zusammenfassung" bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens – welche die Elemente der Menge genannt werden – zu einem "Ganzen" (Originaldefinition von Georg CANTOR). Die Begriffe "Menge" bzw. "Eigenschaft" überdecken sich im großen und ganzen. Jede Eigenschaft bestimmt eine Menge (die Menge aller Dinge, die diese Eigenschaft besitzen) – jede Menge bestimmt eine Eigenschaft (Mitgliedschaft dieser Menge). Eine bequeme Methode, Mengen zu spezifizieren, besteht darin, ihre Elemente zwischen geschwungenen Klammern aufzulisten (falls die Menge sehr viele oder sogar unendlich viele Elemente besitzt, verwendet man Punkte, um fehlende Elemente anzudeuten).

BEISPIELE. $\{1, 2, 3\}$ ist die Menge aller natürlichen Zahlen ≤ 3;
$\{1, 2, 3, \dots\}$ ist die Menge aller natürlichen Zahlen;
$\{2, 4, 6, \dots\}$ ist die Menge aller geraden Zahlen.
Eine andere Möglichkeit verwendet die definierende Eigenschaft der Menge, d.h. $\{x \in A \colon P(x)\}$ ist die Menge aller $x \in A$, die die Eigenschaft P erfüllen.

BEISPIELE. $\{x \in \mathbf{N} \colon x$ ist eine gerade Zahl$\}$ ist die Menge $\{2, 4, 6, \dots\}$.
$\{x \in \mathbf{R} \colon x \geq 0\}$ – die Menge aller nicht-negativen reelen Zahlen.

Wir verwenden Großbuchstaben für Mengen, kleine für Elemente.
$\in$ bedeutet "ist Mitglied von". Die Folgenden Mengen sind so wichtig in der Mathematik, daß man eigene Buchstaben für sie reserviert:
$\mathbf{N}$ – die Menge aller natürlichen Zahlen;
$\mathbf{Z}$ – die Menge aller ganzen Zahlen;
$\mathbf{Q}$ – die Menge aller rationalen Zahlen;
$\mathbf{R}$ – die Menge aller reellen Zahlen;
$\mathbf{C}$ – die Menge der komplexen Zahlen.
Falls A, B Mengen sind, dann bedeutet:
"$A \subseteq B$" – A ist Teilmenge von B (d.h. jedes Element von A ist Element von B).
"$A = B$" – A und B sind identisch (d.h. sie besitzen die gleichen Elemente).
$A \cap B$ – ist die Menge aller Elemente, die sowohl in A als auch in B sind.
$A \cup B$ – ist die Menge aller Elemente, die entweder in A oder in B (oder in beiden) sind.
$A \setminus B$ – ist die Menge aller Elemente, die in A aber nicht in B sind.
$\emptyset$ – (die leere Menge) ist die Menge, die keine Elemente besitzt.
$A \times B$ – ist die Menge aller geordneten Paare (a, b), wobei $a \in A$, $b \in B$ ($A \times B$ heißt das **kartesische Produkt** von A und B).
Diese Bezeichnungen lassen sich mit Hilfe der sogenannten VENN'schen Diagramme veranschaulichen.

BEISPIELE. Die Aussagen $2 \in \mathbf{N}$, $-7 \in \mathbf{Z}$, $\frac{7}{2} \in \mathbf{Q}$, $\sqrt{2} \in \mathbf{R}$ sind richtig;
Die Aussagen $-7 \in \mathbf{N}$, $\frac{7}{2} \in \mathbf{Z}$, $\sqrt{2} \in \mathbf{Q}$, $3 + \sqrt{-1} \in \mathbf{R}$ sind falsch. $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$, $\mathbf{N} \subseteq \mathbf{Z}$, $\mathbf{Z} \subseteq \mathbf{Q}$, $\mathbf{Q} \subseteq \mathbf{R}$ (richtig);
$\mathbf{Q} \subseteq \mathbf{Z}$, $\{1, 2, 3, 4\} \subseteq \{1, 3, 4, 5\}$ (falsch); $\mathbf{N} = \{1, 2, 3, 4 \dots\}$ (richtig);
$\{x \in \mathbf{R} \colon x \geq 0\} = \{x \in \mathbf{R} \colon$ es existiert $y \in \mathbf{R} \quad$ mit $\quad x = y^2\}$ (richtig);
$\{1, 2, 3, 4\} \cap \{1, 2, 5\} = \{1, 2\}$ (richtig);
$\{1, 2, 3, 4, \} \cup \{1, 2, 5\} = \{1, 2, 3, 4, 5\}$ (richtig). $\mathbf{R} \setminus \mathbf{Q}$ ist die Menge der irrationalen Zahlen, (richtig).
$\emptyset = \{x \in \mathbf{R} \colon x^2 = -1\} = \{1, 3, 5, \dots\} \cap \{2, 4, 6, \dots\}$ (richtig). Die Mengenoperationen erfüllen die folgenden Rechenregeln, wie man sich leicht überzeugt:

1. $A \cup A = A, A \cap A = A$;
2. $(A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C)$;
3. $A \cup B = B \cup A, A \cap B = B \cap A$;
4. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
6. $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C), (A \setminus B) \cup (A \setminus C) = A \setminus (B \cap C)$

(Die Gesetze von de MORGAN.)

Abbildungen: Eine informale Definition wäre etwa: Eine Abbildung f von einer Menge A in eine Menge B (in Symbolen $f \colon A \to B$) ist eine Vorschrift, die jedem $x \in A$ *ein* Element $f(x)$ in B zuordnet. A heißt die **Definitionsmenge** (oder **Definitionsbereich**), B die **Bildmenge** von f.

BEISPIEL. Die Vorschrift $f(x) = x^2$ definiert eine Abbildung von $\mathbf{R}$ in $\mathbf{R}$. Wir benutzen folgende Schreibweise:

$$\begin{aligned} f\colon \mathbf{R} &\to \mathbf{R} \\ x &\mapsto x^2 \end{aligned}$$

oder $f\colon x \mapsto x^2 \quad (x \in \mathbf{R})$. Um Anthropomorphismen wie "Vorschrift" zu vermeiden, können wir etwa die folgende formale Definition geben: eine Abbildung $f\colon A \to B$ ist eine Teilmenge M von $A \times B$ mit den Eigenschaften:
a) für jedes $x \in A$ existiert ein $y \in B$ mit $(x, y) \in M$;
b) $(x, y) \in M$ und $(x, z) \in M$ impliziert $y = z$.
(M ist der **Graph** der Abbildung.)

NOTATION. Id_A ist die Identitätsabbildung $x \mapsto x$ auf einer Menge A: Falls $f\colon A \to B$ und $A_1 \subseteq A$, dann ist $f(A_1) = \{f(x)\colon x \in A_1\}$ das **Bild** von A_1 bzgl. f.
Für $B_1 \subseteq B$ ist

$$f^{-1}(B_1) = \big\{x \in A\colon f(x) \in B_1\big\}$$

das **Urbild** von B_1 bzgl. f. Eine Abbildung $f\colon A \to B$ ist
injektiv, falls $x \neq y$ impliziert $f(x) \neq f(y)$;
surjektiv, falls $f(A) = B$ (d.h. jedes Element in B ist das Bild eines Elements aus A);
bijektiv, falls injektiv und surjektiv.
(Entsprechende Hauptwörter: Injektion, Surjektion, Bijektion.)

BEISPIELE. Die Abbildung

$$f\colon x \mapsto x^2 \quad \text{von} \quad \mathbf{R} \quad \text{in} \quad \mathbf{R}$$

ist weder injektiv noch surjektiv. Es gilt:

$$\begin{aligned} f(\mathbf{R}) &= \{x\colon x \geq 0\} \\ f^{-1}(y) &= \{\sqrt{y}, -\sqrt{y}\} \quad (y \geq 0) \\ f^{-1}(B) &= \{\sqrt{y}, -\sqrt{y}\colon y \in B, y \geq 0\}. \end{aligned}$$

$g\colon \mathbf{R} \to \mathbf{R}$, wobei $g\colon x \mapsto x^3$, ist surjektiv und injektiv – daher bijektiv.
$h\colon x \mapsto \sin x$ von $\mathbf{R}$ in $[-1, 1]$ ist surjektiv.

Zusammensetzung von Abbildungen:
Eine Abbildung kann man betrachten als eine mathematische Abstraktion eines "Input-Ouput Systems". Der Zusammensetzung (Verknüpfung) zweier Abbildungen entspricht die reihenweise Koppelung von zwei Systemen. Damit die Zusammensetzung möglich ist, muß der Output von S_1 ein mögliches Input von S_2 sein. In unserer Sprache heißt das, daß die Abbildungen $f\colon A \to B$, $g\colon C \to D$ zusammensetzbar sind, falls $B \subseteq C$. Die Abbildungen $g \circ f$ von A in D ist dann die Abbildung

$$x \mapsto g\big(f(x)\big).$$

Falls eine Abbildung $f\colon A \to B$ bijektiv ist, dann existiert *eine* Abbildung $g\colon B \to A$, sodaß $f \circ g = \mathrm{Id}_A$, $g \circ f = \mathrm{Id}_B$. g heißt die **Inverse** von f. (Geschrieben f^{-1}.)

BEISPIELE. Die Zusammensetzung der Abbildungen

$$\begin{aligned} f\colon (\xi_1, \xi_1) &\mapsto (a_{11}\xi_1 + a_{12}\xi_2, a_{21}\xi_1 + a_{22}\xi_2) \\ g\colon (\xi_1, \xi_2) &\mapsto (b_{11}\xi_1 + b_{12}\xi_2, b_{21}\xi_1 + b_{22}\xi_2) \end{aligned}$$

ist die Abbildung

$$g \circ f\colon (\xi_1, \xi_2) \;\mapsto\; \big((b_{11}a_{11} + b_{12}a_{21})\xi_1 + (b_{11}a_{12} + b_{12}a_{22})\xi_2,\\ (b_{21}a_{11} + b_{22}a_{21})\xi_1 + (b_{21}a_{12} + b_{22}a_{22})\xi_2\big).$$

(Alle Abbildungen von $\mathbf{R}^2$ in sich selbst.)

1.5 Gruppen

Sei A eine Menge. Wir betrachten die Menge aller Bijektionen von A als ein algebraisches System, mit Zusammensetzung als "Multiplikation". Wie man leicht sieht, erfüllt dieses System folgende Bedingungen.

G1) $h \circ (g \circ f) = (h \circ g) \circ f$ (Assoziativität);

G2) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$ (Existenz eines Einselements);

G3) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$ (Existenz von Inversen).

Wir bezeichnen diese Menge mit $\mathrm{Per}(A)$. Jede Teilmenge $G(\neq \emptyset)$ von $\mathrm{Per}(A)$, sodaß $g \circ f$ und $f^{-1} \in G$, wenn $f, g \in G$, heißt eine **Transformationsgruppe** von A.

Beispiele. **Symmetriegruppen:** Sei A eine Teilmenge von $\mathbf{R}^2$. Die **Symmetriegruppe von** A ist die Menge aller Isometrien $T\colon \mathbf{R}^2 \to \mathbf{R}^2$ sodaß $T(A) = A$.

Beispiele: Die Symmetriegruppe von

I. dem Quadrat besteht aus 8 Elementen (die Identität, drei Drehungen, vier Spiegelungen).

II. dem Kreis $\big\{(\xi_1, \xi_2)\colon \xi_1^2 + \xi_2^2 = 1\big\}$ ist unendlich (jede Rotation um 0, Spiegelung an jeder Geraden durch 0).

Eine bequeme Art, Transformationsgruppen zu charakterisieren, ist die Angabe eines Systems Erzeugender, d.h. einer Menge S von Transformationen, sodaß jedes Element der Gruppe darstellbar als ein Produkt von Elementen aus S ist. Z.B. haben die Gruppen oben folgende erzeugende Systeme:

I. Die Drehung um 90 Grad plus eine Spiegelung an der x-Achse.

II. Die Menge aller Spiegelungen.

Wir führen jetzt den allgemeinen Begriff einer Gruppe ein. Eine **Gruppe** ist eine Menge G zusammen mit einer Multiplikation, d.h. eine Abbildung $(x, y) \mapsto xy$ von $G \times G$ in G, sodaß

1. $x(yz) = (xy)z \qquad (x, y, z \in G)$ (Assoziativität);

2. es existiert $e \in G$ mit $ex = xe = x \qquad (x \in G)$;

3. für $x \in G$ existiert $y \in G$, sodaß $xy = yx = e$.

   Das Element $e \in G$ mit Eigenschaft 2) ist eindeutig bestimmt und heißt die **Einheit** von G. Ähnlicherweise ist das Element y von 3) eindeutig durch x bestimmt und heißt die **Inverse** von x (geschrieben x^{-1}).

   Eine **Teilgruppe** von einer Gruppe G ist eine nichtleere Teilmenge G_1 von G, sodaß

4. G_1 ist geschlossen bzgl. Multiplikation, d.h. $x, y \in G_1$ impliziert $xy \in G_1$;

5. $x \in G_1$ impliziert $x^{-1} \in G_1$.
   G_1 ist dann selber eine Gruppe.

In der Praxis werden Teilgruppen oft folgendermaßen bestimmt: $\{x_1, \ldots, x_n\}$ sei eine Teilmenge von einer Gruppe G. Die Menge aller Elemente, die darstellbar als Produkte von Elementen aus $\{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}, e\}$ (wobei jedes Element öfters vorkommen kann) sind, ist eine Teilgruppe von G. Sie heißt die von $\{x_1, \ldots, x_n\}$ **erzeugte Teilgruppe** und wird mit $\langle x_1, \ldots, x_n \rangle$ bezeichnet. $\{x_1, \ldots, x_n\}$ heißen **Erzeugende** der Teilgruppe.
Besonders wichtig sind die sogenannten **zyklischen Teilgruppen** – das sind die Teilgruppen, die von *einem* Element erzeugt sind, d.h. sie haben die Gestalt $\{x^n : n \in \mathbf{Z}\}$.
Im allgemeinen ist die Gruppenmultiplikation nicht kommutativ d.h. es kann Elemente x, y geben, mit $xy \neq yx$.
Eine Grupe G heißt **kommutativ** (oder **abel'sch**), falls alle Elemente kommutieren d.h. $xy = yx\,(x, y \in G)$ (die Multiplikationstabelle ist symmetrisch bzgl. der Diagonale). Beispiele von kommutativen Gruppen sind: $\mathbf{R}$ mit Addition, $\mathbf{C} \setminus \{0\}$ mit Multiplikation.
Wegen der Nichtkommutativität ist die Aussage $(xy)^{-1} = x^{-1}y^{-1}$ im allgemeinen falsch. Allerdings gilt der folgende Satz:

Satz 1.5.1 *Seien x, y Elemente einer Gruppe G. Dann gilt:*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Beweis. Es gilt:

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = (xe)x^{-1} = xx^{-1} = e$$

Ähnlicherweise gilt $(y^{-1}x^{-1})xy = e$.

■

Permutationen:

Eine sehr wichtige Klasse von Gruppen sind die Permutationsgruppen von endlichen Mengen. Wir bezeichnen die Gruppe der Permutationen der Menge $\{1, 2, \ldots, n\}$ mit S_n. S_n hat bekanntlich $n!$ Elemente.

Es ist bequem, eine Permutation π folgendermaßen zu bezeichen:

$$\begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ \pi(1) & \pi(2) & \ldots\ldots & \pi(n) \end{pmatrix}$$

Z.B.

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

ist die Permutation $1 \mapsto 4, 2 \mapsto 3 \quad 3 \mapsto 2, 4 \mapsto 1$.

Beispiele von wichtigen Permutationen:

I. **Transpositionen:** Permutationen, die zwei Zahlen austauschen. Sie haben die Gestalt:

$$\begin{pmatrix} 1 & 2 & \ldots\ldots & i & \ldots\ldots & j & \ldots\ldots & n \\ 1 & 2 & \ldots\ldots & j & \ldots\ldots & i & \ldots\ldots & n \end{pmatrix}$$

Wir bezeichnen diese Permutation mit $(i\,j)$. Z.B. in S_7 bezeichnet $(2\,3)$ die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

II. **Zyklen:** Der Zyklus $(i_1\, i_2 \ldots i_k)$ in S_n ist die Permutation, die i_1 in i_2, i_2 in $i_3, \ldots, i_{k-1}$ in i_k und i_k in i_1 überführt.

Z.B. in S_7 bezeichnet $(2\,3\,6)$ die Permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 6 & 4 & 5 & 2 & 7 \end{pmatrix}$$

Zwei Zyklen $(i_1, \ldots, i_k)$, $(j_1, \ldots, j_r)$ sind **disjunkt**, falls sie keine gemeinsamen Elemente haben. Z.B. sind $(2\,3\,6)$, $(4\,5\,7)$ disjunkt in S_7, $(2\,3\,6)$, $(2\,4\,5)$ nicht.

Wir werden jetzt beweisen, daß jede Permutation als Produkt von disjunkten Zyklen darstellbar ist. Betrachten wir zunächst die Permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 10 & 9 & 4 & 6 & 8 & 2 & 1 & 3 \end{pmatrix}$$

Wir fangen mit dem Element 1 an und wenden wiederholt die Permutation an. Das liefert den Zyklus $(1\,5\,4\,9)$. Diese Prozedur wird wiederholt, indem wir mit einer Zahl (z.B. 2), die nicht in $(1\,5\,4\,9)$ vorkommt, anfangen. Wir bekommen den Zyklus $(2\,7\,8)$. Ähnlicherweise bekommen wir die Zyklen $(3\,10)$, (6). Das liefert die Faktorisierung

$$(1\,5\,4\,9) \quad (2\,7\,8) \quad (3\,10) \quad (6)$$

(Bemerkung: disjunkte Zyklen kommutieren.)

Satz 1.5.2 *Jede Permutation in S_n ist darstellbar als ein Produkt von disjunkten Zyklen.*

Korollar 1.5.3 *Jede Permutation ist darstellbar als Produkt von Transpositionen.*

BEWEIS. Nach dem letzten Satz genügt es, zu zeigen, daß jeder Zyklus diese Eigenschaft hat. Aber

$$(i_1 \dots i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \dots (i_1\, i_2).$$

In der Sprache der Gruppentheorie heißt dieses Ergebnis, daß die Transpositionen die ganze Gruppe S_n erzeugen.

N.B. Die obige Darstellung einer Permutation als Produkt von Transpositionen ist nicht eindeutig!

■

BEISPIEL. Bestimme eine Darstellung der Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 10 & 9 & 4 & 6 & 8 & 2 & 1 & 3 \end{pmatrix}$$

als Produkt von Transpositionen.
Die Permutation $= (1\,5\,4\,9)(2\,7\,8)(3\,10)(6) = (1\,9)(1\,4)(1\,5)(2\,8)(2\,7)(3\,10)$.

Definition 1.5.4 *Der* **Charakter** ε_π *einer Permutation* π *ist* $(-1)^r$, *wobei* r *die Anzahl der Transpositionen in einer Darstellung wie oben ist.*
π *heißt* **gerade**, *falls* $\varepsilon_\pi = 1$, **ungerade**, *falls* $\varepsilon_\pi = -1$; *Es gilt:*

a) $\varepsilon_{\pi\circ\pi_1} = \varepsilon_\pi \varepsilon_{\pi_1}$;

b) falls $\pi = (i_1, \dots, i_r)$ *ein Zyklus ist, dann gilt* $\varepsilon_\pi = (-1)^{r-1}$ *(denn*

$$(i_1, \dots, i_r) = (i_1\, i_r)(i_1 \dots i_{r-1}).$$

Daher gilt $\varepsilon_\pi = -\varepsilon_{\pi_1}$ *wobei* $\pi_1 = (i_1 \dots i_{r-1})$*).*

BEISPIEL. Berechne ε_π, wobei

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 10 & 9 & 4 & 6 & 8 & 2 & 1 & 3 \end{pmatrix}.$$

Es gilt: $\pi = (1\,5\,4\,9)(2\,7\,8)(3\,10)$.
Daher gilt: $\varepsilon_\pi = (-1)^3(-1)^2(-1) = 1$.
Oder: $\pi = (1\,9)(1\,4)(1\,5)(1\,8)(2\,7)(3\,10)$.
Das sind 6 Zyklen – also gilt $\varepsilon_\pi = 1$.

1.6 Logik

1.6.1 Grundbegriffe der Logik

Wir stellen im folgenden einige Begriffe der Logik zusammen, die notwendig sind, um eine gewisse Abklärung und Normierung des Gebrauchs der Umgangssprache sowie eine Stilisierung der Schreibweise mathematischer Sätze zu erreichen.

Aussagenlogik: Wir verstehen unter einer Aussage ein (schrift-) sprachliches Gebilde, für welches es einen Sinn hat, zu fragen, ob es wahr oder falsch ist. Eine Aussage soll stets entweder wahr oder falsch (jedoch nichts Drittes, insgesondere nicht wahr und falsch zugleich) sein (zweitwertige Logik). Es spielt dabei keine Rolle, ob wir tatsächlich feststellen können, ob eine Aussage wahr oder falsch ist.
Symbole für Aussagen: $A, B, C, \ldots$ oder $p, q, r, \ldots$

Definition 1.6.1 *A, B seien Aussagen. Dann definieren wir den Wahrheitswert $|A|$ von A wie folgt:*
$|A| = W :\Leftrightarrow A$ *ist wahr,*
$|A| = F :\Leftrightarrow A$ *ist falsch,*
$A \equiv B$ *(oder $|A| = |B|$)* $:\Leftrightarrow A$ *und B haben denselben Wahrheitswert.*

Beispiele. **für Aussagen:**
"Paris liegt in Frankreich", "4 ist eine Primzahl" sind Aussagen. Keine Aussagen sind: "Wie spät ist es?", "Komm her!".
Die "Aussagenlogik" gestattet, aus gegebenen Aussagen A, B neue Aussagen zu bilden, nämlich:
$\neg A$, (lies "nicht A"), die **Negation** von A,
$A \wedge B$, (lies "A und B"), die **Konjunktion** von A und B,
$A \vee B$, (lies "A oder B"), die **Disjunktion** von A und B,
$A \Rightarrow B$, (lies "wenn A so B" oder "A impliziert B"), die **Implikation** von A auf B,
$A \Leftrightarrow B$, (lies "A genau dann, wenn B" oder "A äquivalent B"), die **Äquivalenz** von A und B.
Diese Aussagen sind definiert durch die folgende "**Wahrheitstafel**" (das ist eine Tabelle, in der der Wahrheitswert von Aussagen angegeben wird):

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
W	W	F	W	W	W	W
W	F	F	F	W	F	F
F	W	W	F	W	W	F
F	F	W	F	F	W	W

Zusätze:

- Wie die Tabelle zeigt, ist $A \vee B$ genau dann wahr, wenn wenigstens eine der beiden Aussagen A, B wahr ist, die Disjunktion "$\vee$" entspricht also dem nichtausschließenden "oder".
- Bei der Implikation "$A \Rightarrow B$" nennt man A die **Prämisse**, B die **Konklusion**. Die Implikation ist definitionsgemäß genau dann falsch (siehe Wahrheitstafel), wenn A wahr und B falsch ist. Im Sinne der Aussagenlogik ist demnach der in der Umgangssprache als Unsinn empfundene Satz "Wenn der Schnee grün ist, dann ist Paris die Hauptstadt von England" eine wahre Aussage.

Vereinbarung:
Um Klammern zu sparen, vereinbart man:
"$\neg$" bindet stärker als "$\wedge$", "$\vee$", "$\Rightarrow$", "$\Leftrightarrow$";

"$\wedge$", "$\vee$" binden stärker als "$\Rightarrow$", "$\Leftrightarrow$".
Wir schreiben demnach z.B.
$\neg A \wedge B$ statt $(\neg A) \wedge B$ oder $A \wedge B \Rightarrow C$ statt $(A \wedge B) \Rightarrow C$.

Definition 1.6.2 *Eine Verknüpfung von Aussagen $A, B, C, \ldots$, die unabhängig von den Wahrheitswerten von $A, B, C, \ldots$ stets wahr (falsch) ist, heißt* **Tautologie** *(***Kontradiktion***).*

Regeln des logischen Schließens:

Satz 1.6.3 *A, B, C seien beliebige Aussagen, T sei eine Tautologie und K eine Kontradiktion, dann gilt:*

a) $\neg(\neg A) \equiv A$

b) $\neg(A \wedge B) \equiv \neg A \vee \neg B$ *(De MORGANsche Regel)*

c) $\neg(A \vee B) \equiv \neg A \wedge \neg B$ *(De MORGANsche Regel)*

d) $A \Rightarrow B \equiv \neg(A \wedge \neg B) \equiv \neg A \vee B$

e) $A \Rightarrow B \equiv (\neg B \Rightarrow \neg A)$ *(Kontrapositionsregel)*

f) $A \Rightarrow B \equiv (A \wedge \neg B \Rightarrow K)$ *(reductio ad absurdum)*

g) $\big((A \Rightarrow B) \wedge (A \Rightarrow \neg B) \Rightarrow \neg A\big) \equiv T$ *(reductio ad absurdum)*

h) $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C) \equiv T$

i) $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

j) $A \wedge (A \Rightarrow B) \Rightarrow B \equiv T$ *(modus ponens)*

k) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ *(Distributivgesetze)*

l) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ *(Distributivgesetze)*

m) $(A \vee B) \vee C \equiv A \vee (B \vee C) \quad (=: A \vee B \vee C)$ *(Assoziativgesetze)*

n) $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C) \quad (=: A \wedge B \wedge C)$ *(Assoziativgesetze)*

Bemerkung.

- Die Beziehungen des voranstehenden Satzes beweist man mit Hilfe von Wahrheitstafeln.
- Die in voranstehendem Satz zusammengestellten Beziehungen heißen **Regeln des logischen Schließens**; sie werden beim Beweis mathematischer Sätze benutzt.

Aussageformen und Quantoren:

Definition 1.6.4 *Eine* **einstellige Aussageform** $A(\dots)$ *ist ein sprachlicher Ausdruck mit einer "Leerstelle" und einer Klasse M von Objekten, sodaß gilt: Durch Einsetzen eines Objektes a aus der Klasse M entsteht eine Aussage $A(a)$. (Statt der Leerstelle kann auch ein Buchstabe als Platzhaltersymbol stehen.)*
Mit Hilfe einer einstelligen Aussageform bildet man die Aussagen

$$\bigwedge_{a\in M} A(a) \quad \textit{(Generalisierung)}$$

$$\bigvee_{a\in M} A(a) \quad \textit{(Partikularisierung)},$$

deren Wahrheitswert definiert ist durch

a) $$\left|\bigwedge_{a\in M} A(a)\right| = W :\Leftrightarrow \textit{ für alle } a \in M \textit{ ist } A(a) \textit{ wahr}$$

b) $$\left|\bigvee_{a\in M} A(a)\right| = W :\Leftrightarrow \textit{ es existiert ein } a \in M, \textit{ so daß } A(a) \textit{ wahr ist.}$$

Bemerkung.

- "$\bigwedge$" heißt **Allquantor** (A ohne Querstrich, Gedächtnisstütze!),
  "$\bigvee$" heißt **Existenzquantor**.
- Falls kein Mißverständnis möglich ist hinsichtlich der zugrundeliegenden Klasse von Objekten, schreibt man einfach $\bigwedge_a A(a)$ und $\bigvee_a A(a)$ statt $\bigwedge_{a\in M} A(a)$ und $\bigvee_{a\in M} A(a)$.
- Ist $A(\dots)$ eine einstellige Aussageform mit der Leermenge als zugehöriger Klasse von Objekten, dann definiert man

$$\bigwedge_{a\in\emptyset} A(a) \quad \text{ist eine Tautologie und}$$

$$\bigvee_{a\in\emptyset} A(a) \quad \text{ist eine Kontradiktion.}$$

Satz 1.6.5 *Sei B eine Aussage, $A(\dots)$ eine Aussageform, dann gilt:*

a) $\neg(\bigwedge_a A(a)) \equiv \bigvee_a(\neg A(a))$ *(De MORGANsche Regeln)*

b) $\neg(\bigvee_a A(a)) \equiv \bigwedge_a(\neg A(a))$ *(De MORGANsche Regeln)*

c) $B \wedge (\bigwedge_a A(a)) \equiv \bigwedge_a(B \wedge A(a))$

d) $B \vee (\bigwedge_a A(a)) \equiv \bigwedge_a(B \vee A(a)) \qquad B \wedge (\bigvee_a A(a)) \equiv \bigvee_a(B \wedge A(a))$ *(Distributivgesetz)*

e) $B \vee (\bigvee_a A(a)) \equiv \bigvee_a(B \vee A(a))$

f) $\left[B \Rightarrow \bigwedge_a A(a)\right] \equiv \bigwedge_a (B \Rightarrow A(a))$

g) $\left[B \Rightarrow \bigvee_a A(a)\right] \equiv \bigvee_a (B \Rightarrow A(a))$

h) $[(\bigwedge_a A(a)) \Rightarrow B] \equiv \bigwedge_a (A(a) \Rightarrow B)$

i) $[(\bigvee_a A(a)) \Rightarrow B] \equiv \bigvee_a (A(a) \Rightarrow B)$

Definition 1.6.6 *Eine* **zweistellige Aussageform** $A(\ldots', \ldots'')$ *ist ein sprachlicher Ausdruck mit einer "ein-gestrichenen" und einer "zwei-gestrichenen" Leerstelle zusammen mit zwei Klassen M' und M'' von Objekten, sodaß folgende zwei Bedingungen gelten:*

(1) Durch Einsetzen eines Objektes a aus M' in die eingestrichene Leerstelle von $A(\ldots', \ldots'')$ entsteht eine einstellige Aussageform $A(a, \ldots'')$, deren Leerstelle die zweigestrichene Leerstelle von $A(\ldots', \ldots'')$ ist und deren Einsetzungsklasse M'' ist.

(2) Durch Einsetzen eines Objektes b aus M'' in die zwei-gestrichene Leerstelle von $A(\ldots', \ldots'')$ entsteht eine einstellige Aussageform $A(\ldots', b)$, deren Leerstelle die eingestrichene Leerstelle von $A(\ldots', \ldots'')$ ist und deren Einsetzungsklasse M' ist.

Bemerkung.

- Drei- und mehrstellige Aussageformen werden analog der voranstehenden Definition erklärt.
- Mit einer zweistelligen Aussageform lassen sich durch Kombination von Generalisierung und Partikularisierung folgende 8 Aussagen bilden:

$$\bigwedge_a \bigwedge_b A(a,b), \quad \bigwedge_b \bigwedge_a A(a,b), \quad \bigwedge_a \bigvee_b A(a,b), \quad \bigvee_b \bigwedge_a A(a,b),$$
$$\bigvee_a \bigwedge_b A(a,b), \quad \bigwedge_b \bigvee_a A(a,b), \quad \bigvee_a \bigvee_b A(a,b), \quad \bigvee_b \bigvee_a A(a,b).$$

  Dabei ist z.B. die Aussage $\bigvee_a \bigwedge_b A(a,b)$ genau dann wahr, wenn es mindestens ein Objekt a der Klasse M' gibt, sodaß für alle Objekte b der Klasse M'' die Aussage $A(a,b)$ wahr ist.

- Für eine zweistellige Aussageform gelten folgende Beziehungen:

$\alpha)$ $$\bigwedge_a \bigwedge_b A(a,b) \equiv \bigwedge_b \bigwedge_a A(a,b)$$

$\beta)$ $$\bigvee_a \bigvee_b A(a,b) \equiv \bigvee_b \bigvee_a A(a,b)$$

$\gamma)$ $$\neg \left(\bigwedge_a \bigwedge_b A(a,b) \right) \equiv \bigvee_a \bigvee_b \neg A(a,b)$$

$\delta)$ $$\neg \left(\bigwedge_a \bigvee_b A(a,b) \right) \equiv \bigvee_a \bigwedge_b \neg A(a,b)$$

- Ist $A(\ldots', \ldots'')$ eine zweistellige Aussageform, für die die erste und zweite Einsetzungsklasse miteinander übereinstimmen ($M' = M'' := M$), dann schreibt man:

$$\bigwedge_{a,b\in M} A(a,b) \text{ statt } \bigwedge_{a\in M}\bigwedge_{b\in M} A(a,b)$$

und

$$\bigvee_{a,b\in M} \text{ statt } \bigvee_{a\in M}\bigvee_{b\in M} A(a,b).$$

Vorsicht:

$$\bigvee_{a}\bigwedge_{b} A(a,b) \text{ und } \bigwedge_{b}\bigvee_{a} A(a,b)$$

sind im allgemeinen nicht wahrheitsgleich!

Beispiele. Wir setzen einige der Definitionen bzw. Aussagen der Vorlesung mit Hilfe dieser Schreibweise um:
Das Prinzip der mathematischen Induktion:

$$\left[A(1) \wedge \left(\bigwedge_{n\in\mathbf{N}} A(n) \Rightarrow A(n+1)\right)\right] \Rightarrow \bigwedge_{n\in\mathbf{N}} A(n).$$

Die Folge (x_n) konvergiert gegen x: $\bigwedge_{\epsilon>0}\bigvee_{N\in\mathbf{N}}\bigwedge_{n\geq N} |x_n - x| \leq \epsilon$.
Die Folge (f_n) konvergiert punktweise auf $[a,b]$ gegen f:

$$\bigwedge_{\epsilon>0}\bigwedge_{x\in[a,b]}\bigvee_{N\in\mathbf{N}}\bigwedge_{n\geq N} |f_n(x) - f(x)| \leq \epsilon.$$

Die Folge (f_n) konvergiert gleichmäßig auf (a,b) gegen f:

$$\bigwedge_{\epsilon>0}\bigvee_{N\in\mathbf{N}}\bigwedge_{x\in[a,b]}\bigwedge_{n\geq N} |f_n(x) - f(x)| \leq \epsilon.$$

(Die letzten 3 Begriffe werden später behandelt.)

Zusammenfassung und Ergänzung

Aus konkreten Aussagen $A, B, C, \ldots$ entstehen durch die Verknüpfungen $\wedge$, $\vee$, $\neg$ neue, zusammnegesetzte Aussagen, deren Wahrheitswert nicht vom konkreten Inhalt der ursprünglichen Aussagen, sondern nur von deren Wahrheitswert abhängt.
Sehen wir vom konreten Inhalt der Aussagen ab, und fassen $A, B, C, \ldots$ (oder $x_1, x_2, \ldots x_n$) als Aussagen–Variable auf, welche die Wahrheitswerte W, F (oder 1, 0) annehmen, so entsprechen den zusammengesetzten Aussagen die Aussage–Formen $p(x_1, x_2, \ldots x_n)$, welche ihrereseits auch wieder nur die Werte W, F annehmen (oder 1, 0). Wir können also Aussage–Formen als Abbildungen interpretieren, deren Argumente alle möglichen $0, 1$–Folgen der Länge n sind und deren Werte wieder $0, 1$ sind.
Jene Aussage–Form, die immer der Wert 0 bzw. 1 annimmt, entspricht allen möglichen Kontradiktionen bzw Tautologien in n Aussage–Variablen.
Bei vorgebenem n gibt es für $(x_1, x_2, \ldots x_n)$ insgesamt 2^n mögliche Belegungen mit den Werten $0, 1$ und wir erhalten daher:

Satz 1.6.7 *Es gibt 2^{2^n} Aussage–Formen $p(x_1, x_2, \ldots x_n)$ in n Aussage–Variablen $x_1, x_2, \ldots x_n$. Diese Aussage–Formen können wir wieder durch $\wedge$, $\vee$, $\neg$ miteinander verknüpfen zu Aussage–Formen der gleichen Art.*
Bezeichne **1** *jene Form, die nur den Wert 1 annimt und* **0** *jene, die nur den Wert 0 annimmt. Seien p, q, r beliebige Aussage–Formen (in n Variablen), dann gelten folgende Beziehungen:*

$a)$ $p \vee p = p$	$b)$ $p \wedge p = p$
$c)$ $p \vee q = q \vee p$	$d)$ $p \wedge q = q \wedge p$
$d)$ $(p \vee q) \vee r = p \vee (q \vee r)$	$e)$ $(p \wedge q) \wedge r = p \wedge (q \wedge r)$
$f)$ $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$	$g)$ $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
$h)$ $p \vee \mathbf{0} = p$	$i)$ $p \wedge \mathbf{1} = p$
$j)$ $p \vee \mathbf{1} = \mathbf{1}$	$k)$ $p \wedge \mathbf{0} = \mathbf{0}$
$l)$ $p \vee \neg p = \mathbf{1}$	$m)$ $p \wedge \neg p = \mathbf{0}$
$n)$ $\neg(\neg p) = p$	$o)$ $\neg\mathbf{1} = \mathbf{0}$, $\neg\mathbf{0} = \mathbf{1}$
$q)$ $\neg(p \vee q) = \neg p \wedge \neg q$	$r)$ $\neg(p \wedge q) = \neg p \vee \neg q$
$s)$ $p \wedge (p \vee q) = p$	$t)$ $p \vee (p \wedge q) = p$

Diese Gesetze beschreiben den sg. Aussagenkalkül und beinhalten die Regeln des logischen Schließens in Satz 1.6.3. Obgleich überaus nützlich (praktische Anwendung: Schaltalgebra), sind diese Regeln und der Aussagenkalkül weder ausreichend für die „ Logik des täglichen Lebens“ noch für die Bedürfnisse der Mathematik. Insbesondere für die Formulierung von Sätzen über die Mitglieder, Objekte, Elemente udgl. von Gesamtheiten, Klassen, Mengen, welche aus praktischen oder grunsätzlichen Gründen nicht einzeln aufzählbar sind, benötigt man die Einführung der Quantoren $\bigvee$, $\bigwedge$, deren wichtigste Eigenschaften in Satz 1.6.5 zusammengefaßt sind.
Besondere Bedeutung haben dabei die de MORGAN'schen Regeln

$$\neg(\bigwedge_a A(a)) \equiv \bigvee_a (\neg A(a))$$
$$\neg(\bigvee_a A(a)) \equiv \bigwedge_a (\neg A(a)).$$

Insbesondere die erste dient in der Mathematik oft zur Widerlegung einer Behauptung (Vermutung) durch Angabe eines Gegenbeispiels. (Im täglichen Leben ist diese Methode jedoch selten erfolgreich zur Beseitigung von Vorurteilen.)

Kapitel 2

Lineare Algebra

2.1 Lineare Gleichungssysteme

Um die Methoden zur Lösung von linearen Gleichungssystemen zu illustrieren, beginnen wir mit einigen Beispielen:

Beispiel.

$$\begin{array}{rcrcrcl} 3x & + & 2y & = & 7 & \quad (A) \\ 5x & + & y & = & 7 & \quad (B) \end{array}$$

ist ein System von 2 Gleichungen in 2 Unbekannten.
Um es zu lösen, eliminieren wir x

$$\begin{array}{rcrcrcl} 3x & + & 2y & = & 7 & \quad (A') & = & (A) \\ & & 7y & = & 14. & \quad (B') & = & 5(A) - 3(B) \end{array}$$

Das ergibt: $y = 2$, $3x + 4 = 7$, also $x = 1$.

Beispiel. Betrachte das System

$$\begin{array}{rcrcrcrl} & & 7y & + & 2z & = & -22 & \quad (A) \\ 4x & + & 9y & + & z & = & -7 & \quad (B) \\ 3x & + & y & - & z & = & 0. & \quad (C) \end{array}$$

Hier funktioniert die obige Methode nicht, da x in (A) nicht vorkommt. Es genügt aber, Gleichungen (A) und (B) zu vertauschen.

Beispiel.

$$\begin{array}{rcrcrcrl} 2x & - & y & & & = & 3 & \quad (A) \\ 3x & - & 5y & + & 2z & = & 7 & \quad (B) \\ 2x & + & 2y & - & 3z & = & 5. & \quad (C) \end{array}$$

Schritt 1: Wir erreichen, daß der Koeffizient von x in (A) gleich 1 ist (PIVOT eins).

$$\begin{array}{rcrcrcrl} \boxed{1}x & - & \frac{1}{2}y & & & = & \frac{3}{2} & \quad (A') \\ 3x & - & 5y & + & 2z & = & 7 & \quad (B') \\ 2x & + & 2y & - & 3z & = & 5. & \quad (C') \end{array}$$

Schritt 2: Wir eliminieren x von (B') und (C'):

$$\begin{array}{rcrcrcrl} x & - & \frac{1}{2}y & & & = & \frac{3}{2} & \quad (A'') \\ & - & \frac{7}{2}y & + & 2z & = & \frac{5}{2} & \quad (B'') = (B') - 3 \cdot (A') \\ & & 3y & - & 3z & = & 2. & \quad (C'') = (C') - 2 \cdot (A') \end{array}$$

Schritt 3:

$$\begin{array}{rcrcrcr} x & - & \frac{1}{2}y & & & = & \frac{3}{2} \\ & & \boxed{1}y & - & \frac{4}{7}z & = & -\frac{5}{7} \\ & & 3y & - & 3z & = & 2. \end{array}$$

Wir können jetzt die Prozedur (mit y statt x) wiederholen und bekommen die Lösung: $x = \frac{2}{9}$, $y = -\frac{23}{9}$, $z = -\frac{29}{9}$.

Um zu sehen, warum diese Methode nicht immer funktioniert, betrachten wir weitere Beispiele:

BEISPIEL.

$$\begin{array}{rcrcrcr} x & + & 3y & + & 2z & = & 1 \\ 2x & + & 6y & + & 9z & = & -1 \\ 4x & + & 12y & + & 13z & = & 1 \end{array}$$

Wenden wir die obige Methode an, so bekommen wir das äquivalente System:

$$\begin{array}{rcrcrcr} x & + & 3y & + & 2z & = & 1 \\ & & & & 5z & = & -3 \\ & & & & 5z & = & -3 \end{array}$$

In diesem Fall hat das System unendlich viele Lösungen (das System ist *unterdeterminiert*).

BEISPIEL.

$$\begin{array}{rcrcrcr} x & + & 3y & + & 2z & = & 1 \\ 2x & + & 6y & + & 9z & = & -1 \\ 4x & + & 12y & + & 13z & = & 2 \end{array}$$

In diesem Fall bekommen wir:

$$\begin{array}{rcrcrcr} x & + & 3y & + & 2z & = & 1 \\ & & & & 5z & = & -3 \\ & & & & 5z & = & -2 \end{array}$$

Dieses System ist *inkompatibel* – damit hat das ursprüngliche System keine Lösung.

Wir bringen jetzt eine systematischere Darstellung der allgemeinen Methode. Das allgemeine System (m Ungleichungen, n Unbekannte) hat die Gestalt

$$\begin{array}{rcrcl} a_{11}x_1 & + \cdots + & a_{1n}x_n & = y_1 & \\ \vdots & & \vdots & & (*) \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = y_m & \end{array}$$

Das Zahlenschema

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}$$

(kurz $A = [a_{ij}]$) heißt **die Matrix des Systems**.

A hat m Zeilen und n Spalten – ist daher eine $m \times n$ **Matrix**. Das Element a_{ij} ist in der i-ten **Zeile** und der j-ten **Spalte**.

Die Gleichung $(*)$ löst man mit Hilfe des sogenannten **Gaußschen Eliminationsverfahrens**, d.h. man ersetzt die Matrix A durch eine Matrix B der Gestalt

$$\tilde{A} = \begin{bmatrix} 0 & 0 & \dots & 1 & \tilde{a}_{1,j_1+1} & \dots & & & & \tilde{a}_{1n} \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 & \tilde{a}_{2,j_2+1} & & \tilde{a}_{2n} \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \dots & & & 0 & \dots & 1 & \tilde{a}_{r,j_r+1} \dots & \tilde{a}_{rn} \\ 0 & \dots & & & & & & & & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \dots & & & & & & & & 0 \end{bmatrix}$$

Das macht man wie folgt:

Schritt 1: Falls $a_{11} \neq 0$ ersetzt man A durch

$$\begin{bmatrix} 1 & \frac{a_{12}}{a_{11}} & \dots & \frac{a_{1n}}{a_{11}} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & & & a_{mn} \end{bmatrix}$$

Falls $a_{11} = 0$ sucht man ein i, sodaß $a_{i1} \neq 0$ und vertauscht die Gleichung 1 mit Gleichung i. Dann zurück zu Schritt 1.

Falls die erste Spalte null ist, dann wendet man Schritt 1 auf die Matrix

$$\begin{bmatrix} a_{12} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m2} & \dots & a_{mn} \end{bmatrix}$$

an.

Schritt 2: Man subtrahiert entsprechende Vielfache der 1. Gleichung von den anderen und bekommt dann eine Matrix der Gestalt

$$\begin{bmatrix} 1 & b_{12} & b_{13} & \dots & b_{1n} \\ 0 & b_{22} & & & \\ \vdots & \vdots & & & \vdots \\ 0 & b_{m2} & \dots & \dots & b_{mn} \end{bmatrix}$$

Jetzt wenden wir dieselbe Methode auf die $(m-1) \times (n-1)$ Matrix

$$\begin{bmatrix} b_{22} & \dots & b_{2n} \\ \vdots & & \vdots \\ b_{m2} & \dots & b_{mn} \end{bmatrix} \text{ an.}$$

Die Prozedur endet, wenn die übrigen Zeilen alle Null sind.

Die Matrix $\tilde{A}$ heißt eine **hermitesche Normalform** von A. Die Zahl r der nicht verschwindenden Zeilen von $\tilde{A}$ heißt der **Rang** von A, geschrieben $r(A)$.

Es gilt: Falls $r < m$, dann ist die Gleichung nicht immer lösbar. Falls $r < n$, dann ist die Lösung (falls existent) nicht eindeutig, sondern enthält $n - r$ freie Parameter. Falls $r = n = m$, dann ist das Gleichungssystem eindeutig lösbar.

BEISPIEL. Berechne eine hermitesche Normalform bzw. den Rang von A wobei

$$\begin{aligned} A &= \begin{bmatrix} 2 & -2 & 1 & 4 \\ 3 & 5 & -1 & 0 \\ 2 & -2 & 1 & 1 \end{bmatrix} \\ &\downarrow \\ &\begin{bmatrix} 1 & -1 & \frac{1}{2} & 2 \\ 3 & 5 & -1 & 0 \\ 2 & -2 & 1 & 1 \end{bmatrix} \\ &\downarrow \\ &\begin{bmatrix} 1 & -1 & \frac{1}{2} & 2 \\ 0 & 8 & -\frac{5}{2} & -6 \\ 0 & 0 & 0 & -3 \end{bmatrix} \\ &\downarrow \\ &\begin{bmatrix} 1 & -1 & \frac{1}{2} & 2 \\ 0 & 1 & -\frac{5}{16} & -\frac{3}{4} \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{– Rang 3} \end{aligned}$$

BEISPIEL. Bestimme Koeffizienten a, b, c, d, sodaß

$$1^2 + 2^2 + \cdots + n^2 = an^3 + bn^2 + cn + d.$$

Wir setzen $n = 0, 1, 2, 3$ und bekommen das System

$$\begin{array}{rcrcrcrcr} & & & & & & d & = & 0 \\ a & + & b & + & c & + & d & = & 1 \\ 8a & + & 4b & + & 2c & + & d & = & 5 \\ 27a & + & 9b & + & 3c & + & d & = & 14, \end{array}$$

das man einfach lösen kann. Man bekommt damit die bekannte Formel:

$$\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1).$$

BEISPIEL. Für welche Werte von a hat das System

$$\begin{array}{rcrcrcr} x & + & y & + & z & = & 1 \\ 2x & + & 3y & + & az & = & 3 \\ x & + & ay & + & 3z & = & 2 \end{array}$$

a) keine Lösung;

b) genau eine Lösung;

c) mehrere Lösungen?

Die Matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 3 & a \\ 1 & a & 3 \end{bmatrix}$$

hat hermitesche Form

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & a-2 \\ 0 & 0 & 2-(a-1)(a-2) \end{bmatrix}$$

Der Rang ist 3 falls $2-(a-1)(a-2) \neq 0$, d.h. $a \neq 0$ und $a \neq 3$. Dann gibt es genau eine Lösung.
$a = 3$: Das System ist äquivalent zum System

$$\begin{array}{rcrcrcll} x & + & y & + & z & = & 1 & \\ & & y & + & z & = & 1 & \text{– keine Lösung} \\ & & & & 0 & = & -1 & \end{array}$$

$a = 0$: keine Lösung.

2.2 Matrizen

Die folgenden speziellen Matrizen bzw. Matrizentypen sind wichtig.

1. Die $m \times n$ **Nullmatrix**

$$\begin{bmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{bmatrix}$$

   geschrieben $0_{m,n}$ oder einfach 0.

2. Die $m \times m$ **Einsmatrix** oder **Eiheitsmatrix**

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & 0 \\ \vdots & & & \vdots \\ 0 & \dots & \dots & 1 \end{bmatrix}$$

   geschrieben I_m oder einfach I.

3. **Diagonalmatrizen**

$$\begin{bmatrix} \lambda_1 & 0 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & & \lambda_n \end{bmatrix}$$

4. **Dreiecksmatrizen**

$$\begin{bmatrix} a_{11} & \dots & \dots & a_{1n} \\ 0 & a_{22} & & a_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & a_{nn} \end{bmatrix}$$

   (d.h. Matrizen mit $a_{ij} = 0$, falls $i > j$).

2.2.1 Matrizenaddition und Multiplikation

1. **Addition:** Falls $A = [a_{ij}]$, $B = [b_{ij}]$ $m \times n$ Matrizen sind, dann ist $A + B$ die Matrix $[a_{ij} + b_{ij}]$, z.B.
$$\begin{bmatrix} 3 & 4 & 8 \\ 2 & 7 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 3 \\ 4 & -5 & 6 \end{bmatrix} = \begin{bmatrix} 4 & 6 & 11 \\ 6 & 2 & 9 \end{bmatrix}$$
Eigenschaften:
   (i) $A + 0 = 0 + A = A$;
   (ii) $A + B = B + A$;
   (iii) $A + (B + C) = (A + B) + C$;
   (iv) $A + (-A) = 0$ ($-A$ ist die Matrix $[-a_{ij}]$).

2. **Multiplikation:** Falls A eine $m \times \mathbf{n}$ Matrix $[a_{ij}]$, B eine $\mathbf{n} \times p$ Matrix $[b_{jk}]$ ist, dann ist AB die $m \times p$ Matrix $[c_{ik}]$, wobei $c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$.

BEISPIEL. Berechne c_{35} wobei
$$A = \begin{bmatrix} 1 & 2 & 3 & -1 & 2 & -3 & 1 \\ 0 & -1 & 1 & 0 & -1 & 1 & 0 \\ -1 & -2 & -3 & -4 & -5 & -6 & -7 \\ 1 & 2 & 3 & 5 & 7 & 1 & 13 \\ 2 & 4 & 6 & 6 & -2 & -4 & -6 \end{bmatrix}$$
$$B = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 2 \\ -1 & -2 & -3 & -4 & -5 & -6 & -7 & -8 \\ 2 & 4 & 2 & 4 & 2 & 8 & 2 & 4 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 5 & -5 & 3 & 2 & 1 & 6 & 7 & 8 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$$
$c_{35} = 0 + 10 - 6 - 4 - 5 - 6 + 7 = -4$.

Eigenschaften:

1. $(AB)C = A(BC)$
2. $A(B + C) = AB + AC$
3. $(A + B)C = AC + BC$
4. $I_m A = A = A I_n$.

Im allgemeinen ist die Multiplikation nicht kommutativ, d.h. $AB \neq BA$.
BEISPIEL. Für
$$A = \begin{bmatrix} 3 & 2 \\ -1 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ gilt } AB = \begin{bmatrix} 5 & 1 \\ 0 & -2 \end{bmatrix}, BA = \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}.$$

BEISPIEL. Betrachte die Systeme

$$\begin{array}{rcrcrcrcl} 3x & + & 6y & + & 4z & + & 2w & = & a \\ x & + & 7y & + & 8z & + & 9w & = & b \\ -4x & - & y & + & 2z & + & 3w & = & c \end{array} \qquad \text{I}$$

$$\begin{array}{rcrcl} u & & & = & x \\ 2u & + & 4v & = & y \\ 6u & - & v & = & z \\ 2u & + & v & = & w \end{array} \qquad \text{II}$$

(d.h. das "Output" von I ist das "Input" von II).
Substituierend bekommen wir das System

$$\begin{array}{rcrcrcrcl} 3u & + & 6(2u+v) & + & 4(6u-v) & + & 2(2u+v) & = & a \\ u & + & 7(2u+4v) & + & 8(6u-v) & + & 9(2u+v) & = & b \\ -4y & - & (2u+4v) & + & 2(6u-v) & + & 3(2u+v) & = & c \end{array}$$

d.h.

$$\begin{array}{rcrcl} 43u & + & 22v & = & a \\ 81u & + & 29v & = & b \\ 12u & - & 3v & = & c \end{array} .$$

In Matrizenschreibweise:

$$X = \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}, \quad A = \begin{bmatrix} 3 & 6 & 4 & 2 \\ 1 & 7 & 8 & 9 \\ -4 & -1 & 2 & 3 \end{bmatrix}, \quad AX = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

$$Z = \begin{bmatrix} u \\ v \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 2 & 4 \\ 6 & -1 \\ 2 & 2 \end{bmatrix}, \quad BZ = X.$$

Aus

$$AX = \begin{bmatrix} a \\ b \\ c \end{bmatrix}, \quad BZ = X \text{ folgt formal } A(BZ) = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

d.h.

$$(AB)Z = \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

(Kontrolle:

$$\begin{bmatrix} 3 & 6 & 4 & 2 \\ 1 & 7 & 8 & 9 \\ -4 & -1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 4 \\ 6 & -1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 43 & 22 \\ 81 & 29 \\ 12 & -3 \end{bmatrix}).$$

Inverse: Eine Inverse für eine $n \times n$ Matrix ist eine Matrix B, sodaß $AB = BA = I$. Nicht jede $n \times n$ Matrix hat eine Inverse, aber die Inverse, falls existent, ist eindeutig. Es gilt

Satz 2.2.1 *Falls A invertierbar ist, dann hat das System $AX = Y$ die eindeutige Lösung $X = A^{-1}Y$. Die $n \times n$ Matrix A ist genau dann invertierbar, wenn der Rang von A gleich n ist.*

Beispiel.

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

hat keine Inverse. Denn für

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \text{ gilt } AB = \begin{bmatrix} b_{11} & b_{12} \\ 0 & 0 \end{bmatrix},$$

und diese Matrix ist nie die Einsmatrix.

Um die Matrix A zu invertieren, betrachten wir die $n \times 2n$ Matrix $[A \quad I_n]$. Durch Zeilenumformungen reduzieren wir A auf eine hermitesche Normalform. Falls alle Diagonalelemente ungleich null sind, dann ist A invertierbar. Wir reduzieren A weiter auf die Einsmatrix – dann steht A^{-1} rechts in der erweiterten Matrix.

Beispiel. Ist die Matrix

$$\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

invertierbar? Falls ja, bestimme die Inverse dazu und löse damit das System

$$\begin{array}{rcrcrcl} 2x & + & y & + & z & = & 8 \\ x & + & 2y & + & z & = & 9 \\ x & + & y & + & 2z & = & 7. \end{array}$$

Wir bilden die erweiterte Matrix

$$\begin{bmatrix} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

und berechnen eine hermitesche Form wie folgt:

$$\begin{bmatrix} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & \frac{1}{2} & -\frac{1}{2} & 1 & 0 \\ 0 & \frac{1}{2} & \frac{3}{2} & -\frac{1}{2} & 0 & 1 \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & \frac{1}{2} & -\frac{1}{2} & 1 & 0 \\ 0 & 0 & \frac{4}{3} & -\frac{1}{3} & -\frac{1}{3} & 1 \end{bmatrix}$$

Hermitesche Normalform: $\begin{bmatrix} 2 & 1 & 1 \\ 0 & \frac{3}{2} & \frac{1}{2} \\ 0 & 0 & \frac{6}{7} \end{bmatrix}$ – invertierbar.

Wir berechnen weiter

$$\begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ 0 & 1 & 0 & -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ 0 & 0 & 1 & -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{bmatrix}$$

Daher gilt:

$$A^{-1} = \frac{1}{4} \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

Die Lösung des Systems ist: $x = 2, y = 3, z = 1$.

Beispiel. Bestimme eine hermitesche Normalform für

$$A = \begin{bmatrix} 2 & -2 & 1 & 4 \\ 3 & 5 & -1 & 0 \\ 2 & -2 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & -2 & 1 & 4 \\ 3 & 5 & -1 & 0 \\ 2 & -2 & 1 & 1 \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 1 & -1 & \frac{1}{2} & 2 \\ 3 & 5 & -1 & 0 \\ 2 & -2 & 1 & 1 \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 1 & -1 & \frac{1}{2} & 2 \\ 0 & 1 & -\frac{5}{16} & -\frac{3}{4} \\ 0 & 0 & 0 & -3 \end{bmatrix}$$

Beispiel. Löse das System

$$\begin{array}{rcrcrcrcl} 2x & - & 2y & + & z & + & 4w & = & 7 \\ 3x & + & 5y & - & z & & & = & 2 \\ 2x & - & 2y & + & z & + & w & = & 0. \end{array}$$

Wir wiederholen die obige Berechnung, diesmal mit der zusätzlichen Spalte

$$\begin{matrix} 7 \\ 2 \\ 0. \end{matrix}$$

Das führt zur Matrix

$$\begin{bmatrix} 1 & -1 & \frac{1}{2} & 2 & \frac{7}{2} \\ 0 & 1 & -\frac{5}{16} & -\frac{3}{4} & -\frac{17}{16} \\ 0 & 0 & 0 & 1 & \frac{7}{3} \end{bmatrix}$$

und liefert damit das äquivalente System

$$\begin{array}{rcrcrcl} x & - & y & + & \frac{1}{2}z & 2w & = & \frac{7}{2} \\ & & y & - & \frac{5}{16}z & - \frac{3}{4}w & = & -\frac{17}{6} \\ & & & & & w & = & \frac{7}{3}. \end{array}$$

(Sofort lösbar.) Diese Gleichung kann man sukssezive von hinten lösen.

Beispiel. Falls

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

mit $ad - bc \neq 0$, dann gilt

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Z.B. für

$$A = \begin{bmatrix} 3 & 2 \\ -2 & 1 \end{bmatrix}, \qquad A^{-1} = \frac{1}{7} \begin{bmatrix} 1 & -2 \\ 2 & 3 \end{bmatrix}.$$

(Denn

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}.)$$

Beispiel. Berechne A^{-1} (falls existent), wobei

$$A = \begin{bmatrix} -1 & 2 & -2 \\ 3 & -2 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\left[\begin{array}{ccc|ccc} -1 & 2 & -2 & 1 & 0 & 0 \\ 3 & -2 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$\downarrow$$

$$\left[\begin{array}{ccc|ccc} 1 & -2 & 2 & -1 & 0 & 0 \\ 0 & 4 & -5 & 3 & 1 & 0 \\ 0 & 2 & -1 & 1 & 0 & 1 \end{array}\right]$$

$$\downarrow$$

$$\left[\begin{array}{ccc|ccc} 1 & -2 & 2 & -1 & 0 & 0 \\ 0 & 1 & -\frac{5}{4} & \frac{3}{4} & \frac{1}{4} & 0 \\ 0 & 0 & 3 & -1 & -1 & 2 \end{array}\right]$$

$$\downarrow$$

$$\left[\begin{array}{ccc|ccc} 1 & -2 & 2 & -1 & 0 & 0 \\ 0 & 1 & -\frac{5}{4} & \frac{3}{4} & \frac{1}{4} & 0 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{array}\right]$$

$$\downarrow$$

$$\begin{bmatrix} 1 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 1 & -\frac{5}{4} & \frac{3}{4} & \frac{1}{4} & 0 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & 1 & 0 & \frac{1}{3} & -\frac{1}{6} & \frac{5}{6} \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}.$$

BEISPIEL. Untersuche die Gleichung

$$\begin{array}{rcrcrcl} 2x & + & 4y & + & z & = & 1 \\ 3x & + & 5y & & & = & 1 \\ 5x & + & 13y & + & 7z & = & 5. \end{array}$$

$$A = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 5 & 0 \\ 5 & 13 & 7 \end{bmatrix}$$

hat Rang 2 (Gauß'sche Eliminierung) und wir bekommen das äquivalente System

$$\left[\begin{array}{ccc|c} 2 & 4 & 1 & 1 \\ 3 & 5 & 0 & 1 \\ 5 & 13 & 7 & 5 \end{array}\right] \to \left[\begin{array}{ccc|c} 2 & 4 & 1 & 1 \\ 0 & -2 & -3 & -1 \\ 0 & 0 & 0 & 2 \end{array}\right]$$

– also keine Lösung.

BEISPIEL. Wir betrachten die homogene Gleichung

$$\begin{array}{rcrcrcl} 2x & & +4y & & +z & = & 0 \\ 3x & & +5y & & & = & 0 \\ 5x & & +13y & & +7z & = & 0 \end{array}$$

Diese hat immer die triviale Lösung $x = y = z = 0$.
Da aber $r(A) < 3$, bekommen wir weitere Lösungen aus der äquivalenten Gleichung:

$$\begin{array}{rcrcrcl} 2x & + & 4y & + & z & = & 0 \\ & - & 2y & - & 3z & = & 0 \end{array}$$

nämlich $x = \frac{5}{2}\lambda$, $y = -\frac{3\lambda}{2}$, $z = \lambda$ (λ willkürlich) – eine einparametrige Lösungsschar.

2.3 Determinanten

Sei

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

eine 2×2 Matrix. Die **Determinante** $\det A$ von A ist die Zahl $a_{11}a_{22} - a_{21}a_{12}$.
Es gilt:

a) A ist invertiervar $\Leftrightarrow \det A \neq 0$, und

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}.$$

b) Das System $AX = Y$ ist genau dann immer lösbar, wenn $\det A \neq 0$, und die Lösung ist

$$x_1 = \frac{\det \begin{bmatrix} y_1 & a_{12} \\ y_2 & a_{22} \end{bmatrix}}{\det A}, x_2 = \frac{\det \begin{bmatrix} a_{11} & y_1 \\ a_{21} & y_2 \end{bmatrix}}{\det A}.$$

Falls

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

eine 3×3 Matrix ist, definieren wir

$$\begin{aligned} \det A &= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\ &\quad -a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33} - a_{11}a_{23}a_{32}. \end{aligned}$$

Beispiel.

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{array}{l} 1 \cdot 1 + 2 \cdot 1 \cdot 4 + 1 \cdot 2 \cdot 1 - \\ -(1 \cdot 1 \cdot 4 + 2 \cdot 2 \cdot 1 + 1 \cdot 1 \cdot 1) = 2. \end{array}$$

Satz 2.3.1 *(Cramersche Regel). Das System*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= y_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= y_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= y_3 \end{aligned}$$

ist genau dann immer lösbar, wenn $\det A \neq 0$. *Die Lösung ist dann*

$$x_1 = \frac{\det A_1}{\det A}, \quad x_2 = \frac{\det A_2}{\det A}, \quad x_3 = \frac{\det A_3}{\det A}$$

$$\textit{wobei} \quad A_1 = \begin{bmatrix} y_1 & a_{12} & a_{13} \\ y_2 & a_{22} & a_{23} \\ y_3 & a_{32} & a_{33} \end{bmatrix} \quad \textit{usw.}$$

Beispiel. Löse

$$\begin{array}{rcrcrcl} x_1 & - & 2x_2 & + & 2x_3 & = & 2 \\ -x_1 & - & x_2 & + & 3x_3 & = & 0 \\ 2x_1 & - & x_2 & + & x_3 & = & 3 \end{array}$$

$$
\begin{aligned}
A &= \begin{bmatrix} 1 & -2 & 2 \\ -1 & -1 & 3 \\ 2 & -1 & 1 \end{bmatrix}, \quad \det A = -6 \\
A_1 &= \begin{bmatrix} 2 & -2 & 2 \\ 0 & -1 & 3 \\ 3 & -1 & 1 \end{bmatrix}, \quad \det A_1 = -8 \\
A_2 &= \begin{bmatrix} 1 & 2 & 2 \\ -1 & 0 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \det A_2 = -1 \\
A_3 &= \begin{bmatrix} 1 & -2 & 2 \\ -1 & -1 & 0 \\ 2 & -1 & 3 \end{bmatrix}, \quad \det A_3 = -3.
\end{aligned}
$$

Die Lösung ist daher

$$x_1 = \frac{4}{3}, \quad x_2 = \frac{1}{6}, \quad x_3 = \frac{1}{2}.$$

Die allgemeine Definition der Determinante einer $n \times n$ Matrix ist

$$\det A = \sum_{\pi \in S_n} \varepsilon_\pi a_{1\pi(1)} \cdots a_{n\pi(n)}$$

wobei S_n die Menge aller Permutationen von $\{1, \ldots, n\}$ ist und $\varepsilon_\pi = 1$ (bzw. -1) falls π gerade (bzw. ungerade) ist (siehe oben).

Eigenschaften:

1. Wenn man zwei Zeilen oder Spalten einer Determinante vertauscht, so ändert sich das Vorzeichen

$$\det \begin{bmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{bmatrix} = -\det \begin{bmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_n \end{bmatrix}.$$

2. Multipliziert man eine Zeile oder Spalte mit einer Zahl, so wird die Determinante mit dieser Zahl multipliziert:

$$\det \begin{bmatrix} A_1 \\ \vdots \\ \lambda A_i \\ \vdots \\ A_n \end{bmatrix} = \lambda \det \begin{bmatrix} A_1 \\ \vdots \\ A_n \end{bmatrix}.$$

3. Addiert man ein Vielfaches einer Zeile (oder Spalte) zu einer anderen, so ändert sich nichts:
$$\det \begin{bmatrix} A_1 \\ \vdots \\ A_i + \lambda A_j \\ \vdots \\ A_n \end{bmatrix} = \det \begin{bmatrix} A_1 \\ \vdots \\ A_n \end{bmatrix}.$$

4. Falls
$$A = \begin{bmatrix} a_{11} & \dots & \dots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$
eine Dreiecksmatrix ist, dann gilt $\det A = a_{11}a_{22}\dots a_{nn}$.

5. $\det AB = \det A \det B$

6. **Lagrange Entwicklung**:
$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$$
wobei A_{ij} die Matrix ist, die man durch Weglassen der i-ten Zeile und j-ten Spalte bekommt.

7. A ist genau dann invertierbar, wenn $\det A \neq 0$. Es gilt dann
$$A^{-1} = \frac{1}{\det A}[(-1)^{i+j} \det A_{ji}].$$

Da immer $Ao = o$ gilt, ist dies gleichwertig zu: Die Gleichung $Ax = o$ besitzt genau dann eine nichttriviale Lösung, wenn $\det A = 0$.

Beispiel.
$$\det \begin{bmatrix} 2 & 3 & 4 \\ 1 & 1 & 1 \\ -3 & 1 & 2 \end{bmatrix} = 2 \det \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} - \det \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} - 3 \det \begin{bmatrix} 3 & 4 \\ 1 & 1 \end{bmatrix}$$
$$= 2 - 2 + 3 = 3$$
$$\det \begin{bmatrix} 2 & 4 & 0 & 1 \\ 3 & 1 & 0 & -2 \\ 2 & 4 & 1 & -3 \\ -1 & -1 & 0 & 2 \end{bmatrix} = \det \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & -2 \\ -1 & -1 & 2 \end{bmatrix}.$$

Beispiel. Berechne
$$\det \begin{bmatrix} 2 & 4 & 1 \\ 3 & 5 & 0 \\ 5 & 13 & 7 \end{bmatrix}$$

$$\begin{aligned}\det &= 2\det\begin{bmatrix}1 & 2 & \frac{1}{2}\\ 3 & 5 & 0\\ 5 & 13 & 7\end{bmatrix}\\ &= 2\det\begin{bmatrix}1 & 2 & \frac{1}{2}\\ 0 & -1 & -\frac{3}{2}\\ 0 & 3 & \frac{3}{2}\end{bmatrix} = -2\det\begin{bmatrix}1 & \frac{3}{2}\\ 3 & \frac{9}{2}\end{bmatrix} = 0.\end{aligned}$$

Beispiel.

$$\det\begin{bmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\\ 1 & 0 & 1 & 0\\ 2 & 1 & 2 & 1\end{bmatrix} = \det\begin{bmatrix}3 & 2 & 1\\ 0 & 1 & 0\\ 1 & 2 & 1\end{bmatrix} - 2\det\begin{bmatrix}4 & 2 & 1\\ 1 & 1 & 0\\ 2 & 2 & 1\end{bmatrix} + 3\det\begin{bmatrix}4 & 3 & 1\\ 1 & 0 & 0\\ 2 & 1 & 1\end{bmatrix} - 4\det\begin{bmatrix}4 & 3 & 2\\ 1 & 0 & 1\\ 2 & 1 & 2\end{bmatrix}$$

etc. (besser

$$\det\begin{bmatrix}2 & 3 & 4\\ 3 & 2 & 1\\ 1 & 2 & 1\end{bmatrix} + \det\begin{bmatrix}1 & 2 & 4\\ 4 & 3 & 1\\ 2 & 1 & 1\end{bmatrix}).$$

2.4 Das Eigenwertproblem

Sei A eine $n \times n$ Matrix. Ein $\lambda \in \mathbf{R}$ heißt ein **Eigenwert** für A, falls es eine $n \times 1$ Matrix (also einen Vektor) $X(\neq 0)$ gibt, sodaß

$$AX = \lambda X.$$

Das ist genau dann der Fall, wenn λ eine Lösung der Polynomgleichung

$$\det(A - \lambda I) = 0$$

ist. X heißt dann **Eigenvektor** von A (bzgl. λ). Das **Eigenwertproblem** für A besteht darin, alle Eigenvektoren und die entsprechenden Eigenvektoren zu finden.
Nehmen wir an, daß die Gleichung

$$\det(A - \lambda I) = 0$$

die reellen Lösungen $\lambda_1, \ldots, \lambda_k$ besitzt (wir werden hier die komplexen Nullstellen nicht berücksichtigen), wobei λ_i die Vielfachheit r_i hat. Das homogene System

$$AX = \lambda_i X$$

hat dann mindestens **eine** nichttriviale Lösung und dies liefert einen Eigenvektor. Im allgemeinen hat die Gleichung eine k_i-parametrige Lösung, wobei $1 \leq k_i \leq r_i$.
Falls $k_i = r_i$ für jedes i ist, dann kann man für jedes i, r_i unabhängige Eigenwerte finden. Das liefert $r_1 + \cdots + r_k$ unabhängige Lösungen. Falls die Gleichung $\det(A - \lambda I) = 0$ keine komplexe Nullstelle besitzt, dann gilt $r_1 + \cdots + r_k = n$. In diesem Fall haben wir n unabhängige Eigenvektoren $X_1, \ldots, X_n$ und die Matrix

$$P = [X_1, \ldots, X_n]$$

ist invertierbar. Dann gilt: $P^{-1}AP$ ist eine Diagonalmatrix (die Diagonalelemente sind die Eigenwerte von A) und heißt eine **Diagonalisierung** von A.

Bemerkungen: A ist daher genau dann diagonalisierbar, wenn die Nullstellen von $\det(A - \lambda I) = 0$ alle reell sind und jede Nullstelle λ_i (mit Vielfachheit r_i) r_i unabhängige Eigenvektoren besitzt. Dies ist automatisch der Fall, wenn

a) die Gleichung $\det(A - \lambda I) = 0$ n verschiedene reelle Nullstellen besitzt, oder

b) A symmetrisch ist, d.h. $a_{ij} = a_{ji}$.

BEISPIEL. Ist $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ bzw. $A = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$ diagonalisierbar?
Für $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ gilt $\det(A - \lambda I) = \det \begin{bmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{bmatrix} = (1-\lambda)^2$

$$(1-\lambda)^2 = 0 \Leftrightarrow \lambda = 1.$$

A besitzt daher einen Eigenwert mit Vielfachheit 2. Die Eigenvektoren sind Lösungen des Systems

$$\begin{array}{rcrcrcrcl} 0 & \cdot & \xi_1 & + & & & \xi_2 & = & 0 \\ 0 & \cdot & \xi_1 & + & 0 & \cdot & \xi_2 & = & 0 \end{array}$$

d.h. $\xi_2 = 0$, ξ_1 willkürlich.
Das liefert nur einen unabhängigen Eigenvektor, etwa $(1, 0)$. Daher ist A nicht diagonalisierbar.
Für $A = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$ gilt

$$\det(A - \lambda I) = \det \begin{bmatrix} 1-\lambda & 3 \\ 3 & 1-\lambda \end{bmatrix} = 1 - 2\lambda + \lambda^2 - 9 = (\lambda - 4)(\lambda + 2).$$

A hat zwei verschiedene reelle Eigenwerte $4, -2$ und ist daher diagonalisierbar. Wir berechnen eine Diagonalisierung wie folgt: Für $\lambda = 4$ bekommen wir die Gleichung $-3\xi_1 + 3\xi_2 = 0$ mit Eigenvektor $(1, 1)$, für $\lambda = -2$ die Gleichung $3\xi_1 + 3\xi_2$ mit Eigenvektor $(1, -1)$.
Damit gilt:

$$P^{-1}AP = \begin{bmatrix} 4 & 0 \\ 0 & -2 \end{bmatrix}, \text{ wobei } P = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Wir bringen zwei Beispiele von Anwendungen von Diagonalisierungen:

1. Löse die Differenzengleichung

$$f_{n+2} = f_{n+1} + f_n$$

mit den Anfangswerten $f_0 = 0, f_1 = 1$. Die Lösung ist die sogenannte FIBONACCI-Folge $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$. Wir führen die Matrizen

$$X_n = \begin{bmatrix} f_{n+1} \\ f_n \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad X_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

ein. Es gilt: $X_{n+1} = AX_n$. Daraus folgt: $X_n = A^n X_0$. Um die Lösung zu bekommen, müssen wir A^n berechnen. Das macht man mit Hilfe einer Diagonalisierung. Es gilt:

$$P^{-1}AP = \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix} \text{ wobei } P = \begin{bmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{bmatrix}.$$

Daraus folgt:

$$P^{-1}A^nP = \begin{bmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & 0 \\ 0 & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{bmatrix}$$

oder

$$A^n = P \begin{bmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & 0 \\ 0 & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{bmatrix} P^{-1}$$

$$= \frac{1}{\sqrt{5}} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & 0 \\ 0 & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{bmatrix} \begin{bmatrix} 1 & \frac{-1+\sqrt{5}}{2} \\ -1 & \frac{1+\sqrt{5}}{2} \end{bmatrix}.$$

Das liefert das Ergebnis:

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right). \tag{2.1}$$

BEMERKUNG. Wählt man als Anfang $f_0 = 1, f_1 = 1$, so erhält man die Lösung

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right).$$

2. Löse das System der Differentialgleichungen

$$\begin{aligned} \frac{dx_1}{dt} &= 3x_1 + 2x_2 \\ \frac{dx_2}{dt} &= x_1 + 2x_2. \end{aligned}$$

Wir schreiben die Gleichung in der Form $\frac{dX}{dt} = AX$, wobei

$$X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \quad A = \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix}.$$

Versuchen wir den Ansatz $X(t) = e^{\lambda t}X$ (X konstant), so bekommen wir die Gleichung $\lambda e^{\lambda t}X = Ae^{\lambda t}X$ d.h. das Eigenwertproblem $AX = \lambda X$. Die Lösung davon ist: $\lambda = 1, 4$ mit Eigenvektoren $(-1, 1), (2, 1)$. Das liefert die zwei Lösungen

$$e^t \begin{bmatrix} -1 \\ 1 \end{bmatrix}, \quad e^{4t} \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

In der Tat ist die allgemeine Lösung

$$\begin{aligned} X(t) &= c_1 e^t \begin{bmatrix} -1 \\ 1 \end{bmatrix} + c_2 e^{4t} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \\ \text{d.h. } x_1(t) &= -c_1 e^t + 2c_2 e^{4t} \qquad x_2(t) = c_1 e^t + c_2 e^{4t}. \end{aligned}$$

BEISPIEL. Löse die Differentialgleichung:

$$\frac{d^2x}{dt^2} - 2\frac{dx}{dt} - 3x = 0.$$

Wir führen neue Unbekannte x_1, x_2 ein, wobei $x_1 = x$, $x_2 = \frac{dx}{dt}$. x_1, x_2 genügen dem System

$$\begin{aligned} \frac{dx_1}{dt} &= x_2 \\ \frac{dx_2}{dt} &= 3x_1 + 2x_2 \end{aligned}$$

mit Matrix

$$\begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix}.$$

Die Eigenwerte davon sind 3 (mit Eigenvektor $(1,3)$) und -1 (mit Eigenvektor $(1,-1)$). Damit ist die allgemeine Lösung

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = c_1 e^{3t} \begin{bmatrix} 1 \\ 3 \end{bmatrix} + c_2 e^{-t} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

d.h. $x(t) = c_1 e^{3t} + c_2 e^{-t}$.

BEISPIEL. Löse die Differenzengleichung $a_0 = 2$, $a_1 = 3$, $a_{n+2} = 3a_n - 2a_{n+1}$

$$\begin{bmatrix} a_{n+2} \\ a_{n+1} \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{n+1} \\ a_n \end{bmatrix} \text{ – also } \begin{bmatrix} a_{n+1} \\ a_n \end{bmatrix} = A^n \begin{bmatrix} 3 \\ 2 \end{bmatrix},$$

wobei

$$A = \begin{bmatrix} -2 & 3 \\ 1 & 0 \end{bmatrix}.$$

Die Eigenwerte von A sind

$$\begin{aligned} \lambda &= -3 \text{ (Eigenvektor } \begin{bmatrix} -3 \\ 1 \end{bmatrix}) \\ \lambda &= 1 \text{ (Eigenvektor } \begin{bmatrix} 1 \\ 1 \end{bmatrix}). \end{aligned}$$

Damit gilt

$$P^{-1}AP = \begin{bmatrix} -3 & 0 \\ 0 & 1 \end{bmatrix}, \text{ wobei } \begin{aligned} P &= \begin{bmatrix} -3 & 1 \\ 1 & 1 \end{bmatrix} \\ P^{-1} &= \frac{1}{4}\begin{bmatrix} -1 & 1 \\ 1 & 3 \end{bmatrix}. \end{aligned}$$

Daher:

$$A^n = P \begin{bmatrix} (-3)^n & 0 \\ 0 & 1 \end{bmatrix} P^{-1}.$$

Daraus folgt: $a_n = -\frac{1}{4}((-3)^n - 9)$.

Kapitel 3

Zahlentheorie

3.1 Teilbarkeit, Primzahlen

Wir arbeiten wieder mit den Zahlensystemen

$$\begin{aligned} \mathbf{N} &= \{1, 2, 3, \dots\} \\ \mathbf{N}_0 &= \{0, 1, 2, 3, \dots\} \\ \mathbf{Z} &= \mathbf{N}_0 \cup \{-1, -2, -3, \dots\} \end{aligned}$$

auf denen die Operation + und . definiert sind.

$(\mathbf{N}, +)$ ist eine kommutative Halbgruppe ohne neutralem Element;

$(\mathbf{N}, .)$ ist eine kommutative Halbgruppe mit Einselement 1;

$(\mathbf{N}_0, +)$ ist eine kommutative Halbgruppe mit neutralem Element 0;

$(\mathbf{Z}, +, .)$ ist ein Ring.

Satz 3.1.1 Teilbarkeit: *Falls $a, b \in \mathbf{Z}$, dann sagen wir, daß a ein* **Teiler** *von b ist (geschrieben: $a|b$), falls ein $r \in \mathbf{Z}$ existiert mit $b = ra$. Falls zusätzlich $a \neq b$, dann ist a ein* **echter Teiler** *von b. Es gilt:*

a) $a|b_i$ $(i = 1, \dots, n)$, $c_1, \dots, c_n \in \mathbf{Z}$, *dann* $a| \sum_{i=1}^{n} c_i b_i$;

b) $b|a$ *und* $c \in \mathbf{Z} \Rightarrow bc|ac$;

c) $ac|bc$ $(a, b, c \in \mathbf{Z},\ c \neq 0) \Rightarrow a|b$;

d) $b|a \Rightarrow |b| \leq |a|$ $(a, b \in \mathbf{Z},\ a \neq 0)$;

e) $a|b$ *und* $b|a \Rightarrow |a| = |b|$ $(a, b \in \mathbf{Z} \setminus \{0\})$;

f) $a|b$, $b|c \Rightarrow a|c$ $(a, b, c \in \mathbf{Z})$.

Wir kehren zum Thema Divisionsalgorithmus zurück, diesmal mit Beweis.

Satz 3.1.2 Der Divisionsalgorithmus: *Sei $a \in \mathbf{Z}$, $b \in \mathbf{N}$. Dann existieren eindeutig bestimmte Zahlen $q, r \in \mathbf{Z}$ mit $0 \leq r < b$ und $a = qb + r$.*

BEWEIS. **Existenz:** Sei q ist die größte ganze Zahl aus der Menge $\{t \in \mathbf{Z} : t \leq \frac{a}{b}\}$. Dann gilt: $q \leq \frac{a}{b} < q+1$ und daher $bq \leq a < b(q+1)$. Sei dann $r = a - bq$, sodaß $0 \leq r < b$ und $a = qb + r$.
Eindeutigkeit: Sei $a = qb + r = q_1 b + r_1$ etwa mit $r_1 \geq r$. Daher gilt: $(q - q_1)b = r_1 - r$. Aber $0 \leq r_1 - r < b$. Daher gilt $q = q_1$ usw.

■

3.1.1 1. Anwendung. Der größte gemeinsame Teiler.

Falls $a, b \in \mathbf{Z}$, dann gilt: eine positive ganze Zahl d heißt der *größte gemeinsame Teiler* von a, b (geschrieben: $d = \mathrm{ggT}\,(a, b)$), falls

1. $d|a$ und $d|b$,
2. $\bigwedge_{d_1 \in \mathbf{N}} d_1|a$ und $d_1|b \Rightarrow d_1|d$.

Falls $b = 0$, so definiert man naheliegend $ggT(a, 0) = a$
Wir untersuchen genauer den Algorithmus aus Kapitel 1, um $\mathrm{ggT}\,(a, b)$ zu berechnen.
Wir schreiben

$$a = qb + r.$$

Man sieht leicht, daß $\mathrm{ggT}\,(b, r) = \mathrm{ggT}\,(a, b)$. Ohne Verlust der Allgemeinheit können wir daher annehmen, daß $a, b > 0$ und $b < a$. Um die rekursive Vorgangsweise besser zu verdeutlichen, setzen wir $x_0 = a, q_1 = q, x_1 = b, x_2 = r$ und erhalten natürliche Zahlen q_i, x_i mit $q_i \geq 1$ und $x_1 > x_2 > \cdots > x_n > 0$

$$\begin{aligned} x_0 &= q_1 x_1 + x_2 \\ x_1 &= q_2 x_2 + x_3 \\ &\vdots \\ x_{n-2} &= q_{n-1} x_{n-1} + x_n \\ x_{n-1} &= q_n x_n + 0 \end{aligned}$$

x_n ist also der letzte nicht–verschwindende Rest.

Wir sehen unmittelbar

$$t|x_0, x_1 \Leftrightarrow t|x_2 \Leftrightarrow t|x_3 \cdots \Leftrightarrow t|x_{n-1} \Leftrightarrow t|x_n.$$

Daher gilt:
1. $x_n = \mathrm{ggT}\,(x_0, x_1)$.
2. Durch Rücksubstiuieren von der letzten bis zur ersten Zeile sehen wir: Der ggT d läßt sich schreiben als

$$d = ra + sb$$

mit geeigneten $r, s \in \mathbf{Z}$. Es gilt sogar: d ist die **kleinste positive Zahl**, die sich so schreiben läßt.
Wir schätzen nun die **Länge n des Algorithmus** ab. Zunächst bemerken wir:
n hängt nicht von d ab: wir können alle Gleichungen durch d dividieren, ohne damit n zu ändern. Zur Bestimmung von n können wir also o.B.d.A. annehmen $d = x_n = \mathrm{ggT}\,(x_0, x_1) = 1$.

Beginnen wir mit der Nummerierung am Ende, so erhalten wir nach einer entsprechenden Umbenennung

$$\begin{aligned} y_{n+1} &= p_n y_n + y_{n-1} \\ y_n &= p_{n-1} y_{n-1} + y_{n-2} \\ &\vdots \\ y_3 &= p_2 y_2 + y_1 \\ y_2 &= p_1 y_1 + 0 \end{aligned}$$

Daraus sehen wir einen Zusammenhang zu den Fibonacci–Zahlen: $f_1 = 1 = y_1 = f_2 \leq y_2$ und damit weiter

$$\begin{aligned} y_3 &\geq y_2 + y_1 \geq f_2 + f_1 = f_3 \\ &\vdots \\ y_k &\geq y_{k-1} + y_{k-2} \geq f_{k-1} + f_{k-2} = f_k \\ &\vdots \\ a &= y_{n+1} \geq f_{n+1} \end{aligned}$$

Durch Induktion zeigt man leicht die folgende Abschätzung der Fibonacci–Zahlen: sei $\theta = \frac{1}{2}(1 + \sqrt{5})$, dann gilt für alle n

$$f_{n+1} \geq \theta^n.$$

Daraus und aus der Rekursions–Formel für die Fibonacci–Zahlen folgt sofort

Satz 3.1.1 *Die maximale Länge im euklidischen Algorithmus ist nach oben begrenzt durch die binäre Länge von a. Genauer*

$$n \leq \frac{1}{\log \theta} \log a.$$

Diese maximale Länge wird erreicht bei Paaren aufeinander folgender Fibonacci–Zahlen.

Beispiel. Wir berechnen (191,35). Es gilt:

$$\begin{aligned} 191 &= 5 \cdot 35 + 16 \quad (\to (35, 16)) \\ 35 &= 2 \cdot 16 + 3 \quad (\to (16, 3)) \\ 16 &= 3 \cdot 5 + 1 \quad (\to (3, 1)) \end{aligned}$$

Daher gilt: $(191, 35) = 1$. Außerdem:

$$\begin{aligned} 1 &= 16 - 5 \cdot 3 \\ &= 16 - 5 \cdot (35 - 2 \cdot 16) \\ &= 11 \cdot 16 - 5 \cdot 35 \\ &= 11(191 - 5 \cdot 35) - 5 \cdot 35 \\ &= 11 \cdot 191 - 60 \cdot 35 \end{aligned}$$

Aus diesen Überlegungen folgt leicht:

1. $a, b, c \in \mathbf{Z}$, $m \in \mathbf{Z} \setminus \{0\} \Rightarrow \operatorname{ggT}(am, bm) = |m| \operatorname{ggT}(a, b)$

2. Falls $a, b, c \in \mathbf{Z}$ mit $a \neq 0$ und $\operatorname{ggT}(a, b) = 1$, dann gilt: $a|bc \Rightarrow a|c$.

   (Denn es existieren r, s mit $ra + sb = 1$. Daher $rac + sbc = c$. Da a ein Teiler der linken Seite ist, gilt $a|c$.)

3. Die Gleichung $ax + by = c$ hat eine ganzzahlige Lösung (d.h. gegeben $a, b \in \mathbf{N}$, dann existieren $x, y \in \mathbf{Z}$ mit dieser Eigenschaft) $\Leftrightarrow \operatorname{ggT}(a, b)|c$.

Definition 3.1.3 *Zwei Zahlen $a, b \in \mathbf{Z}$ sind* **relativ prim**, *falls* $\operatorname{ggT}(a, b) = 1$.

Es existieren dann $r, s \in \mathbf{Z}$ mit $ra + sb = 1$. Daraus folgt, daß jedes $n \in \mathbf{Z}$ eine Darstellung $r'a + s'b$ hat. (Denn $n = rna + snb$.)
Diese Überlegungen über gemeinsame Teiler lassen sich leicht auf mehrere Zahlen übertragen. Z.B. definieren wir:

$$\begin{aligned} \operatorname{ggT}(a_1, \ldots, a_n) &= \text{größter gemeinsamer Teiler von } a_1, \ldots, a_n \\ &= \text{kleinstes } d \in \mathbf{N}, \text{ das eine Darstellung } \sum a_i r_i \text{ besitzt} \end{aligned}$$

$\operatorname{ggT}(a_1, \ldots, a_n)$ kann man rekursiv wie folgt berechnen:

$$\operatorname{ggT}(a_1, \ldots, a_n) = \operatorname{ggT}(a_1, \operatorname{ggT}(a_2, \ldots, a_n)).$$

$\{a_1, \ldots, a_n\}$ sind **relativ prim**, falls $\operatorname{ggT}(a_1, \ldots, a_n) = 1$. $\{a_1, \ldots, a_n\}$ sind **paarweise relativ prim**, falls $\bigwedge_{i \neq j} \operatorname{ggT}(a_i, a_j) = 1$. (Die zweite Bedingung ist stärker.)

3.1.2 2. Anwendung. Primfaktorzerlegung ganzer Zahlen.

Definition 3.1.4 *Eine Zahl $n > 1$ heißt* **prim**, *falls die einzigen Teiler von n die Zahlen ± 1 und $\pm n$ sind. Sonst ist n eine* **zusammengesetzte Zahl**.

Falls n zusammengesetzt ist, dann besitzt n einen Primfaktor.
(Induktionsbeweis: 4 ist nicht prim und hat 2 als Primfaktor. Sei $n > 4$. Induktionsannahme: Jede zusammengesetzte Zahl $n_1 < n$ hat einen Primfaktor. Falls n nicht prim, dann hat n einen positiven Faktor n_1 mit $1 < n_1 < n$. Falls n_1 eine Primzahl ist, dann sind wir fertig. Falls nicht, dann besitzt n_1 einen Primfaktor.)
Im Kapitel 1 haben wir gesehen, daß es unendlich viele Primzahlen gibt.

Hilfssatz 3.1.5 *Falls p eine Primzahl ist und $p|ab$, wobei $a, b \in \mathbf{Z}$, dann gilt: $p|a$ oder $p|b$.*

Beweis. Falls $p \nmid a$, dann gilt $\operatorname{ggT}(p, a) = 1$, d.h. es existieren r, s mit $pr + as = 1$ und daher $pbr + abs = b$. Es gilt dann $p|b$ (da $p|pbr + abs$).

■

Korollar 3.1.6 *Sei p eine Primzahl, $a_1, \ldots, a_n \in \mathbf{Z}$. Dann gilt:*

$$p|a_1 \cdots a_n \Rightarrow \bigvee_i p|a_i.$$

Mit diesen Hilfsmitteln können wir jetzt beweisen:

Satz 3.1.7 (Fundamentalsatz der Zahlentheorie) *Sei $n \in \mathbf{N}$ und sei $p_1, p_2, \ldots$ die Folge der Primzahlen. Dann existiert für jedes i ein eindeutig bestimmtes $\alpha_i \in \mathbf{N}_0$, sodaß $n = \prod p_i^{\alpha_i}$. (Es ist klar, daß $\alpha_i = 0$ für fast alle i, d.h. das Produkt ist endlich.)*

BEWEIS. Zunächst beweisen wir die Existenz solcher Darstellungen. Wir verwenden einen Induktionsbeweis. Der Fall $n = 1$ ist klar. Es gelte der Satz für jedes $n_1 < n$. Wir betrachten den Fall n. Falls n eine Primzahl ist, dann ist $n = n$ eine geeignete Faktorisierung. Falls nicht, dann besitzt n eine Primzahl p als Faktor. Sei $n_1 = \frac{n}{p}$. n_1 hat eine Primzahlzerlegung und damit auch $n = n_1 p$.
Eindeutigkeit: $n \in \mathbf{N}$ habe zwei Zerlegungen:

$$n = \prod_j p_j^{\alpha_j} = \prod_j p_j^{\beta_j}.$$

Wir zeigen: $\alpha_j = \beta_j$ für jedes j. Falls nicht, dann existiert ein i mit $\alpha_i \neq \beta_i$, etwa $\alpha_i < \beta_i$. Wir kürzen den Faktor $p_i^{\alpha_i}$ und bekommen die Gleichung

$$\prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i - \alpha_i} \prod_{j \neq i} p_j^{\beta_j}.$$

p_i ist aber ein Faktor der rechten Seite — daher gilt: $p_i | \prod_{j \neq i} p_j^{\alpha_j}$ und damit $p_i | p_j^{\alpha_j}$ für irgendein j — Widerspruch!

■

$\prod p_i^{\alpha_i}$ heißt die **Primzahlzerlegung** von n.

Falls

$$a = \prod_i p_i^{\alpha_i} \text{ und } b = \prod_i p_i^{\beta_i}$$

dann gilt

$$\mathrm{ggT}\,(a, b) = \prod_i p_i^{\gamma_i}$$

wobei $\gamma_i = \min(\alpha_i, \beta_i)$. Das gleiche Argument zeigt, daß die Zahl

$$\prod_i p_i^{\delta_i},$$

wobei $\delta_i = \max(\alpha_i, \beta_i)$, die kleinste positive Zahl ist, die sowohl a als auch b als Faktor besitzt. Daher heißt diese Zahl das **kleinste gemeinsame Vielfache** von a und b, geschrieben: $\mathrm{kgV}\,(a, b)$. Daraus folgt unmittelbar

$$ab = \mathrm{ggT}\,(a, b).\mathrm{kgV}\,(a, b).$$

BEMERKUNG Für große Zahlen ist die Primfaktorzerlegung (derzeit und möglicherweise grundsätzlich) nicht in "realistischer" Rechenzeit möglich. Daher berechnet man $\mathrm{kgV}\,(a, b)$, indem man mit dem euklidischen Algorithmus zuerst den $ggT(a, b)$ berechnet und dann die vorige Formel verwendet.

Wir verwenden die Primzahlzerlegung, um folgendes Ergebnis zu beweisen:
Falls $a, b, c \in \mathbf{N}$ so sind, daß $c^n = ab$ $(n \in \mathbf{N})$, wobei $\mathrm{ggT}\,(a, b) = 1$, dann sind a und b auch n-te Potenzen, d.h. $\bigvee_{c_1, c_2 \in \mathbf{N}} a = c_1^n \wedge b = c_2^n$.

Denn, sei

$$a = \prod_{p \in P_1} p^{\alpha_p} \qquad b = \prod_{p \in P_2} p^{\alpha_p},$$

wobei P_1 (bzw. P_2) die Mengen der Primzahlen sind, die in der Zerlegung von a (bzw. b) vorkommen. Dann gilt: $P_1 \cap P_2 = \emptyset$ (da $\mathrm{ggT}\,(a,b) = 1$). Aus der Bedingung $ab = c^n$ folgt leicht: $p \in P_1 \cup P_2 \Rightarrow n | \alpha_p$. Damit sieht man, daß a und b n-te Potenzen sind.

3.1.3 Weitere Anwendungen des euklidischen Algorithmus

1. Sei $g_0, g_1, \ldots$ eine Folge von positiven Zahlen, wobei $g_0 = 1$, $g_n \geq 2 \quad (n \geq 1)$. Dann hat jedes $x \in \mathbf{N}$ eine eindeutige Darstellung:

   $$x = a_n(g_n \cdots g_1) + a_{n-1}(g_{n-1} \cdots g_1) + \cdots + a_1 g_1 + a_0,$$

   wobei $a_n \neq 0$, $0 \leq a_i \leq g_i - 1$.

2. Eine **ägyptische Darstellung** einer Rationalzahl $r \in]0,1[$ ist eine der Gestalt:

   $$\frac{1}{n_1} + \cdots + \frac{1}{n_k},$$

   wobei die $n_i \in \mathbf{N}$, etwa

   $$\begin{aligned} \frac{2}{3} &= \frac{1}{2} + \frac{1}{6} \\ \frac{3}{10} &= \frac{1}{5} + \frac{1}{10} \\ \frac{3}{7} &= \frac{1}{3} + \frac{1}{11} + \frac{1}{231} \\ &= \frac{1}{4} + \frac{1}{7} + \frac{1}{28}. \end{aligned}$$

   (Das letzte Beispiel zeigt, daß die Darstellung nicht eindeutig ist). Es gilt allerdings:

Satz 3.1.8 *Jede Rationalzahl $r \in]0,1[$ hat eine eindeutige Darstellung*

$$r = \frac{1}{d_0} + \frac{1}{d_0 d_1} + \cdots + \frac{1}{d_0 \cdots d_n},$$

$(d_0, d_1, \ldots, d_n \in \mathbf{N})$.

Beweis. Sei $r = \frac{p}{q}$. Man bestimmt die d's rekursiv mit Hilfe des folgenden Schemas: Setze

$$\begin{aligned} q &= d_0 p - p_1, \text{ wobei } 0 \leq p_1 < p \quad (\text{sodaß } \frac{p}{q} = \frac{1}{d_0} + \frac{1}{d_0}(\frac{p_1}{q})) \\ q &= d_1 p_1 - p_2, \text{ wobei } 0 \leq p_2 < p_1 \\ &\vdots \\ q &= d_n p_n \end{aligned}$$

(d.h. der Algorithmus bricht dann ab, wenn p_i ein Teiler von q ist.) Es gilt:

$$\frac{p}{q} = \frac{1}{d_0} + \frac{1}{d_0 d_1} + \cdots + \frac{1}{d_0 \cdots d_{n-1}} + \frac{p_n}{q d_0 \cdots d_{n-1}}$$

wie man leicht mit Hilfe der Induktion beweist.

■

3.2 Restklassen

Wir untersuchen jetzt die algebraischen Operationen modulo einer gegebenen Zahl m. Diese Art von Addition und Multiplikation hat viele Anwendungen, z.B. kann man damit mit Hilfe eines Computers auch mit sehr großen Zahlen *genau* rechnen.
Wir schreiben $x = y \pmod m$, falls $m|x-y$.

Es gilt:

$a = b \pmod m$ und $t|m \Rightarrow a = b \pmod{|t|}$,

$a = b \pmod m$, $r \in \mathbf{Z} \Rightarrow ra = rb \pmod m$,

$a = b \pmod m$, $c = d \pmod m \Rightarrow a + c = b + d \pmod m$, $a - c = b - d \pmod m$, $ac = bd \pmod m$,

$ar = br \pmod m \Rightarrow a = b \pmod{(\frac{m}{d})}$ (wobei $d = \mathrm{ggT}(r, m)$),

$ar = br \pmod m \Rightarrow a = b \pmod m$, falls $\mathrm{ggT}(m, r) = 1$,

$a = b \pmod m \Rightarrow ac = bc \pmod{cm}$ $(c > 0)$,

$a = b \pmod m \Rightarrow \mathrm{ggT}(a, m) = \mathrm{ggT}(b, m)$,

$a = b \pmod m$, $0 \leq |b - a| < m \Rightarrow a = b$,

$a = b \pmod m$, $a = b \pmod n \Rightarrow a = b \pmod{mn}$, falls m und n relativ prim.

3.2.1 Anwendungen

I. Teilbarkeitsregeln im Dezimalsystem: Sei n eine natürliche Zahl mit Dezimalentwicklung $\sum_{i=0}^{p} a_i \ 10^i$. Man sieht leicht, daß $n = n_1 \pmod 3$ (sogar $\pmod 9$), wobei $n_1 = \sum_{i=0}^{p} a_i$, d.h. n ist genau dann durch 3 (bzw. 9) teilbar, wenn das Gleiche für n_1 gilt. Ähnlicherweise gilt:

$$
\begin{aligned}
n &= a_0 \pmod 2 \\
n &= 10a_1 + a_0 \pmod 4 \\
n &= a_0 \pmod 5 \\
n &= \sum_{i=0}^{p} (-1)^{[\frac{i}{3}]} 10^{i-3[\frac{i}{3}]} a_i \pmod 7 \\
n &= 100a_2 + 10a_1 + a_0 \pmod 8 \\
n &= \sum_{i=0}^{p} (-1)^i a_i \pmod{11} \\
n &= \sum_{i=0}^{p} (-1)^{[\frac{i}{3}]} 10^{i-3[\frac{i}{3}]} a_i \pmod{13}
\end{aligned}
$$

(Denn:

$$
\begin{aligned}
10^3 &= -1 \pmod 7 \\
10^3 &= -1 \pmod{13} \\
10 &= -1 \pmod{11} \\
10^2 &= 1 \pmod{11} \quad \text{usw.})
\end{aligned}
$$

II. Fermat'sche und Mersenne'sche Primzahlen:

Fermat'sche Primzahlen: Fermat hat geglaubt, daß alle Zahlen der Gestalt $2^{2^n}+1$ prim sind. In der Tat gilt: $641|2^{2^5}+1$ wie wir jetzt zeigen werden: $641 = 5\cdot 2^7+1$, d.h. $5\cdot 2^7 = -1 \pmod{641}$. Daher $5^4\cdot 2^{28} = 1 \pmod{641}$. Aber $641 = 625+16$ - also $5^4 = -2^4 \pmod{641}$. Daraus folgt: $-2^{32} = -2^4\cdot 2^{28} = 5^4\cdot 2^{28} = 1 \pmod{641}$, d.h. $641|2^{2^5}+1$.

Primzahlen der Gestalt $2^{2^n}+1$ heißen **Fermat'sche Primzahlen**. Falls eine Primzahl p die Gestalt 2^r+1 hat, dann ist r eine Potenz von 2 und damit p eine Fermat'sche Primzahl (sonst enthält die Primzerlegung von r eine ungerade Primzahl q und

$$(a^q+1) = (a+1)(a^{q-1}-a^{q-2}+a^{q-3}-\cdots+1).)$$

(Nebenbei bemerkt: Falls $m>n$, dann gilt:

$$2^{2^n}+1|2^{2^m}-1.$$

Daher sind die Zahlen $F_n = 2^{2^n}+1$ paarweise relativ prim).

Eine Primzahl der Gestalt 2^n-1 heißt eine **Mersenne'sche Primzahl.** In diesem Fall muß n auch prim sein. (Denn $m|n \Rightarrow 2^m-1|2^n-1$ — nach dem Schema

$$(a^r-b^r) = (a-b)(a^{r-1}+\cdots+b^{r-1}), \quad a=2^m, \quad b=1, \quad r=\frac{n}{m}.)$$

Die Mersenne'schen Zahlen (d.h. Zahlen der Gestalt 2^p-1), sind **die** Kandidaten für große Primzahlen (z.B. ist $2^{756839}-1$ eine Primzahl).

Wir zeigen, daß $47|2^{23}-1$, sodaß letztere keine Primzahl ist. Denn $2^{23} = (2^5)^4\cdot 2^3$ und $2^5 = 32 = -15 \pmod{47}$, also $2^{10} = 225 = -10 \pmod{47}$, also $2^{20} = 100 = 6 \pmod{47}$, also $2^{23} = 6\cdot 8 = 48 = 1 \pmod{47}$.

Gleichungen: Wir werden Polynomgleichungen der Gestalt $P(x) = 0 \pmod m$ behandeln. Folgende Beispiele zeigen, daß das Verhalten ganz anders als im Fall von Gleichungen in $\mathbf{R}$ oder $\mathbf{C}$ sein kann.

BEISPIELE. Die Gleichung $2x = 3 \pmod 4$ hat keine Lösungen. Die Gleichung $x^2 = 1 \pmod 8$ hat 4 Lösungen.
Der Fall von linearen Gleichungen mit einer Variablen kann man leicht erledigen.

Satz 3.2.1 *Die Gleichung $ax = b \pmod m$ hat genau dann eine Lösung, wenn gilt:* $\mathrm{ggT}(a,m)|b$. *Dann hat sie genau d Lösungen, wobei $d = \mathrm{ggT}(a,m)$.*

BEWEIS. Notwendigkeit: Sei x eine Lösung. Es gilt

$$d|ax, \quad d|m$$

und daher $d|b$ (da $b = ax - cm$).
Nehme jetzt an, daß $d|b$. Wir haben eine Darstellung $d = ar+ms$ für geeignete r,s und daher

$$b = \frac{b}{d}(d) = a(\frac{b}{d})r + ms\frac{b}{d}$$

d.h. $x = \frac{b}{d}r$ ist eine Lösung.
Anzahl der Lösungen: Falls x_0 eine Lösung ist, dann sieht man leicht, daß die Zahlen $\{t, t + \frac{m}{d}, \ldots, t + (d-1)\frac{m}{d}\}$ eine komplette Auflistung der Lösungen ist. Insbesondere gilt: Falls a und m relativ prim sind, dann hat die Gleichung genau **eine** Lösung.

Satz 3.2.2 (von Fermat) *Sei p eine Primzahl. Für jedes a mit $\mathrm{ggT}(a,p) = 1$ gilt $a^{p-1} = 1 \pmod p$. Allgemeiner: für jedes a gilt $a^p = a \pmod p$. Noch allgemeiner gilt: für jedes $m \in \mathbf{N}$ und jedes a mit $\mathrm{ggT}(a,m) = 1$ gilt*

$$a^{\phi(m)} = 1, \quad (\mathrm{mod}\, m)$$

wobei $\phi(m)$ die Anzahl aller Zahlen $\{r_1, \ldots, r_s\}$ aus $\{1, \ldots, m-1\}$ ist, die zu m relativ prim sind.

Satz 3.2.3 (von Wilson) *Sei p eine Primzahl. Es gilt $(p-1)! = -1 \pmod p$.*

Simultane Systeme: Wir betrachten jetzt Systeme der Gestalt

$$x = c_i \quad (\mathrm{mod}\, m_i) \quad (i = 1, \ldots, n),$$

wobei die m_i paarweise relativ prim sind. Sei $M = m_1 \cdots m_n$, $M_i = \frac{M}{M_i}$ (d.h. $M_i = \prod_{j \neq i} m_j$). Es gilt: $\mathrm{ggT}(M_i, m_i) = 1$. Daher ist die Gleichung $M_i y_i = 1 \pmod{m_i}$ lösbar. Sei $\overline{y}_i$ eine Lösung und setze $x = \sum_i c_i M_i \overline{y}_i$. Dies ist klarerweise eine Lösung des obigen Systems. Damit haben wir den Existenzteil des folgenden Satzes bewiesen.

Satz 3.2.4 Chinesischer Restsatz: *Das System $x = c_i \pmod{m_i}$ $(i = 1, \ldots, n)$ ist immer lösbar. Außerdem ist die Lösung eindeutig $\pmod M$ (d.h. für zwei Lösungen x, y des Systems gilt: $x = y \pmod M$).*

Beweis. **(der Eindeutigkeit)** Da $x = c_i = y \quad (\mathrm{mod}\, m_i)$, wissen wir, daß $m_i | x - y$ für jedes i — daher $M | x - y$.

■

Polynomgleichungen: Wir betrachten jetzt Gleichungen der Gestalt

$$P(x) = 0 \quad (\mathrm{mod}\, m),$$

wobei P ein Polynom ist.
Bemerkung. Falls $m = m_1 \cdots m_n$, wobei die m_i paarweise relativ prim sind, dann gilt:

$$P(x) = 0 \quad (\mathrm{mod}\, m)$$

hat genau dann eine Lösung, wenn gilt: für jedes i hat $P(x) = 0 \pmod{m_i}$ eine Lösung. Denn sei x_i eine Lösung dieser Gleichung und wähle x so, daß $x = x_i \pmod{m_i}$ für jedes i. Dann ist x eine Lösung der ursprünglichen Gleichung. Dieses Argument zeigt auch, daß

$$|\{x \in \mathbf{Z}_m : P(x) = 0\}| = \prod |\{x \in \mathbf{Z}_{m_i} : P(x) = 0\}|.$$

Wir können daher unsere Aufmerksamkeit dem Fall $m = p^\alpha$ widmen.
Zunächst der Fall $m = p$ eine Primzahl. Dann gilt:

Satz 3.2.5 (von Lagrange) *Sei P ein nicht-triviales Polynom vom Grad n. Dann hat die Gleichung*

$$P(x) = 0 \pmod p$$

höchstens n verschiedene Lösungen $(\mathrm{mod}\, p)$.

Wie wir oben gesehen haben, zeigt die Gleichung

$$x^2 = 1 \pmod 8,$$

daß dieser Satz für zusammengesetze Zahlen nicht mehr gelten muß.
Anwendungen des Satzes von Lagrange: Wir können den Satz wie folgt formulieren: Falls P ein Polynom vom Grad n ist, mit mehr als n Lösungen von $P(x) = 0 \pmod p$, dann gilt: p ist ein Teiler aller Koeffizienten von P.
Zum Beispiel betrachte das Polynom

$$P(x) = (x-1)\dots(x-p+1) - (x^{p-1} - 1) = G(x) - H(x).$$

Sowohl G als auch H haben $p-1$ Wurzeln — $1, 2, \dots, p-1$. P ist daher ein Polynom vom Grad $p-2$ mit $p-1$ Wurzeln. Daher gilt: p ist ein Teiler der Koeffizienten von p. Daraus folgt vgl. oben.

Satz 3.2.6 (von Wostenholme) *Für $p \geq 5$ gilt:*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} = 0 \pmod{p^2}.$$

Beweis. Übungsaufgabe.

■

Um die Gleichung $P(x) = 0 \pmod{p^\alpha}$ zu lösen, fangen wir an mit dem Fall $\alpha = 1$. Wir lösen diese Gleichung durch Probieren und verwenden dann die folgende Methode, um aus Lösungen für $P(x) = 0 \pmod{p^\alpha}$ ebensolche für $P(x) = 0 \pmod{p^{\alpha+1}}$ zu bekommen.

Satz 3.2.7 *Sei x eine Lösung der Gleichung $P(x) = 0 \pmod{(p^\alpha)}$, $(0 \leq x < p^\alpha)$. Es gilt:*

a) Falls $P'(x) \neq 0 \pmod p$, dann existiert genau ein $\overline{x}$ mit $0 \leq \overline{x} < p^{\alpha+1}$ und $\overline{x} = x \pmod{(p^{\alpha-1})}$, sodaß $p(\overline{x}) = 0 \pmod{(p^{\alpha+1})}$.

b) Falls $P'(x) = 0 \pmod p$, dann gibt es 2 Möglichkeiten. Entweder

b1) $P(x) = 0 \pmod{(p^{\alpha+1})}$. Dann existieren r Lösungen der Gleichung $P(\overline{x}) = 0 \pmod{p^{\alpha+1}}$ mit $\overline{x} = x \pmod{p^\alpha}$.

oder

b2) $P(x) \neq 0 \pmod{p^{\alpha+1}}$. Dann hat $P(\overline{x}) = 0 \pmod{p^{\alpha+1}}$ keine Lösungen $\overline{x}$ mit $\overline{x} = x \pmod{p^\alpha}$.

BEWEIS.

a) Wir setzen $\overline{x} = sp^\alpha + x$ in das Polynom ein. Es gilt:

$$P(x+h) = P(x) + hP'(x) + \cdots + \frac{P^{(n)}(x)}{n!}h^n,$$

wobei der Koeffizient $P^{(n)}\frac{(x)}{k!}$ von h^k ein Polynom mit ganzzahligen Koeffizienten ist. Für $\overline{x} = sp^\alpha + x$ gilt: $P(\overline{x}) = P(x) + P'(x)sp^\alpha +$ Glieder mit $p^{\alpha+1}$ als Faktor, d.h.

$$P(\overline{x}) = P(x) + P'(x)sp^\alpha \pmod{p^{\alpha+1}}.$$

Da $P(x) = 0 \pmod{p^\alpha}$ gilt: $P(x) = kp^\alpha$ $(k \in \mathbf{Z})$. Daher

$$\begin{aligned} P(\overline{x}) &= kp^\alpha + P'(x)sp^\alpha \pmod{p^{\alpha+1}} \\ &= p^\alpha(k + P'(x)s) \pmod{p^{\alpha+1}} \end{aligned}$$

Es reicht daher, wenn wir s als Lösung der Gleichung

$$P'(x)s + k = 0 \pmod{p}$$

wählen. (Die Eindeutigkeit von $\overline{x}$ folgt aus der Eindeutigkeit der Lösung dieser Gleichung).

Fall b) Hier ist das Argument ähnlich.

■

3.3 Arithmetische Funktionen

In diesem Kapitel studieren wir sogenannte **arithmetische Funktionen**. Das sind Funktionen von $\mathbf{N}$ (manchmal auch $\mathbf{N}_0$ bzw. $\mathbf{Z}$) in $\mathbf{C}$ (gewöhnlich gilt sogar, daß die Werte in $\mathbf{Z}$ sind).

BEISPIELE. Die folgenden Funktionen auf $\mathbf{N}$ sind $\mathbf{Z}$-wertige arithmetische Funktionen.

$$\begin{aligned} f(n) &= n \text{ (die Identitätsfunktion)} \\ f(n) &= n^\alpha \quad (\alpha \in \mathbf{N}) \\ f(n) &= \phi(n) \text{ (siehe oben)} \end{aligned}$$

$$\delta(n) = \begin{cases} 1 & (n = 1) \\ 0 & \text{sonst} \end{cases}$$

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1 \\ (-1)^\ell & \text{falls } n = p_1 \dots p_\ell \text{ ein Produkt von } \ell \text{ verschiedenen Primzahlen ist} \\ 0 & \text{falls es eine Primzahl } p \text{ gibt mit } p^2 | n. \end{cases}$$

BEISPIEL. Wir bringen eine Tabelle von den ersten Werten für μ:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

Eine solche Funktion f heißt **multiplikativ**, falls gilt: $f(m \cdot n) = f(m)f(n)$ $(m, n \in \mathbf{N}$ relativ prim), **stark multiplikativ**, falls $f(m \cdot n) = f(m)f(n)$ $(m, n \in \mathbf{N})$.

Z.B. sind $f(n) = n$ bzw. $f(n) = n^\alpha$ stark multiplikativ. μ und ϕ sind multiplikativ, aber nicht stark multiplikativ (für μ ist das klar — für ϕ siehe unten).
Falls f multiplikativ ist, dann gilt: $f(m) = \prod f(p_i^{\alpha_i})$, wobei $m = \prod p_i^{\alpha_i}$.
Falls f stark multiplikativ ist, dann gilt sogar: $f(m) = \prod (f(p_i))^{\alpha_i}$.
Für eine arithmetische Funktion f wird **die Summenfunktion** S_f wie folgt definiert:

$$S_f(n) = \sum_{d|n} f(\frac{n}{d}).$$

Beispiele. Es gilt:

$$\begin{aligned} S_\phi(12) &= \phi(12) + \phi(6) + \phi(4) + \phi(3) + \phi(2) + \phi(1) = 4 + 2 + 2 + 2 + 1 + 1 = 12 \\ S_\mu(12) &= 0 + 1 + 0 - 1 - 1 + 1 = 0 \end{aligned}$$

(in der Tat gilt:

$$\begin{aligned} S_\phi(n) &= n \quad (n \in \mathbf{N}) \\ S_\mu(n) &= \delta(n) \quad (n \in \mathbf{N}) \end{aligned}$$

wie wir später beweisen werden).

Beispiele. Weitere Beispiele von arithmetischen Funktionen sind:

$\tau(n) = \sum_{d|n} 1 = S_1(n)$ — die Anzahl der Teiler von n.
$\sigma(n) = \sum_{d|n} d = S_{\mathrm{Id}}(n)$ — die Summe der Teiler.
$\sigma_k(n) = \sum_{d|n} d^k = S_{\mathrm{Id}^k}(n)$ — die Summe der k-ten Potenzen der Teiler.

Hilfssatz 3.3.1 *Falls f multiplikativ ist, dann auch S_f.*

Beweis. Wir bemerken zunächst, daß jeder Teiler d eines Produktes mn von zwei Zahlen, die zueinander relativ prim sind, eine eindeutige Darstellung als $d_1 d_2$ hat, wobei $d_1|m$, $d_2|n$.
Z.B. die Teiler

$$\begin{aligned} \text{von } 12 &: 1, 2, 3, 4, 6, 12, \\ \text{von } 25 &: 1, 5, 25, \\ \text{von } 12 \times 25 = 300 &: 1, 2, 3, 4, 6, 12, 5, 10, 15, 20, 30, 60, 25, 50, 75, 100, 150, 300. \end{aligned}$$

Es gilt daher:

$$\begin{aligned} S_f(mn) &= \sum_{d|mn} f(d) = \sum_{d_1,d_2,d_1|m,d_2|n} f(d_1)f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= S_f(m)S_f(n). \end{aligned}$$

■

BEISPIEL. Wir berechnen die Werte von ϕ, τ und σ_k. Da diese multiplikativ sind, genügt es, die Werte für Primpotenzen auszurechnen. Da die Teiler von p^α die Zahlen $\{1, p, p^2, \ldots, p^\alpha\}$ sind, gilt:

$$\begin{aligned}
\phi(p^\alpha) &= p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p}) \\
\tau(p^\alpha) &= \alpha + 1 \\
\sigma_k(p^\alpha) &= \sum_{i=0}^{\alpha} p^{ik} = \frac{p^{k(\alpha+1)} - 1}{p^k - 1} \quad (k \neq 0)
\end{aligned}$$

Daraus folgt, für $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$$\begin{aligned}
\sigma_k(n) &= \prod_i \frac{p_i^{k(\alpha_i+1)} - 1}{p_i^k - 1} \\
\tau(n) &= \prod_i (\alpha_i + 1) \\
\phi(n) &= \prod p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = n \prod_i \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

(Wir verwenden stillschweigend die Tatsache, daß ϕ multiplikativ ist - siehe unten.)
Wir berechnen die Summenfunktion S_μ der μ-Funktion wie folgt: Da μ multiplikativ ist, so auch S_μ. Für eine Primpotenz p^α gilt:

$$\begin{aligned}
S_\mu(p^\alpha) &= \mu(1) + \mu(p) + \mu(p^2) + \ldots \\
&= 1 - 1 + 0 \ldots \\
&= 0 \text{ falls } \alpha > 0.
\end{aligned}$$

Das heißt $S_\mu(n) = \delta(n)$ für n eine Primpotenz und daher für jedes n (weil beide Funktionen multiplikativ sind).
Die Formel $S_\mu = \delta$ folgt auch aus den folgenden allgemeinen Überlegungen:
Falls f multiplikativ ist, dann gilt:

$$\sum_{d|n} f(d) = (1 + f(p_1) + \cdots + f(p_1^{\alpha_1}))(1 + f(p_2) + \cdots + f(p_2^{\alpha_2})) \cdots (1 + \cdots + f(p_r^{\alpha_r})),$$

wobei $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Z.B. für $f(n) = n^s$ gilt:

$$\begin{aligned}
\sum_{d|n} d^s &= (1 + p_1^s + \cdots + p_1^{\alpha_1 s}) \cdots (1 + p_r + \cdots + p_r^{\alpha_r s}) \\
&(= \prod_i \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \text{ für } s = 1).
\end{aligned}$$

Korollar 3.3.2 $\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_r))$.

Dies liefert, für $f = 1$:

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & (n > 1) \\ 1 & (n = 1) \end{cases}$$

bzw.

$$\sum_{d|n} \frac{\mu(d)}{d} = \begin{cases} (1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}) & (n>1) \\ 1 & (n=1) \end{cases}$$

Satz 3.3.3 *Sei f eine zahlentheoretische Funktion und setze $g = S_f$. Dann gilt:*

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}).$$

BEWEIS. Die rechte Seite ist

$$\sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d').$$

Aber die Paare d, d', sodaß $d|n$ bzw. $d'|\frac{n}{d}$ sind genau die Paare d, d' mit $dd'|n$. Daraus folgt:

$$\sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d'd;dd'|n} \mu(d) f(d')$$

Aus Symmetriegründen ist dies auch die Summe

$$\sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} f(d') S_\mu(\frac{n}{d'}) = f(n)$$

(da $S_\mu(\frac{n}{d'}) = 0$, außer wenn $\frac{n}{d'} = 1$, d.h. $d' = n$.)
Ein ähnliches Argument zeigt, daß eine Funktion g mit der Eigenschaft

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$$

gleich S_f sein muß.

■

BEISPIEL. Da $S_\phi = \mathrm{Id}$, gilt:

$$\phi(n) = n \sum_{d|n} \frac{1}{d} \mu(d).$$

BEISPIEL. Eine Zahl n heißt **vollkommen**, falls n gleich der Summe ihrer **echten** Teiler ist, d.h. $\sigma(n) = 2n$. Z.B. sind die Zahlen

$$6 = 1+2+3, \quad 28 = 1+2+4+7+14$$

vollkommen. Es gilt: Falls $n = 2^p - 1$ eine Mersenne'sche Primzahl ist, dann ist

$$m = 2^{p-1}(2^p - 1)$$

vollkommen. Denn

$$\begin{aligned} \sigma(m) &= \sigma[(2^{p-1})(2^p-1)] \\ &= \sigma(2^{p-1})\sigma(2^p-1) \\ &= (2^p-1)(2^p-1+1) \\ &= 2.2^{p-1}(2^p-1) = 2m. \end{aligned}$$

In der Tat gilt: Jede gerade vollkommene Zahl hat diese Gestalt. (Z.B. $6 = 2\cdot 3$, $28 = 2^2 \cdot 7$). (Es ist unbekannt, ob ungerade vollkommene Zahlen existieren.)

BEWEIS. (daß jede gerade vollkommene Zahl n der Gestalt $2^{p-1}(2^p-1)$ ist, mit 2^p-1 eine Mersenne'sche Primzahl.) Sei $\sigma(n) = 2n$ wobei $n = 2^k m$, mit m ungerade. Es gilt:

$$\sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1}-1)\sigma(m).$$

Da $\sigma(n) = 2n$, gilt:

$$2^{k+1}m = (2^{k+1}-1)\sigma(m).$$

Daraus folgt, daß 2^{k+1} ein Teiler von $\sigma(m)$ ist. Sei etwa $\sigma(m) = 2^{k+1}\ell$ und daher $m = (2^{k+1}-1)\ell$. Falls $\ell > 1$, dann gilt:

$$\sigma(m) \geq \ell + m + 1$$

(da $1, \ell, m$ Teiler von m sind). Aber $\ell + m = 2^{k+1}\ell = \sigma(m)$ - Widerspruch. Daraus folgt, daß $\ell = 1$, d.h. $\sigma(m) = 2^{k+1}$ und $m = 2^{k+1}-1$. Es gilt dann $\sigma(m) = m+1$, daher ist $m = (2^{k+1}-1)$ eine Primzahl — also die Mersenne'sche Primzahl (2^k-1) ($p = k+1$ prim). Es gilt dann

$$n = 2^k m = 2^{p-1}(2^p-1)$$

■

Kapitel 4

Erzeugende Funktionen, Differenzengleichungen

4.1 Bruchzerlegungen

Sei r eine Rationalfunktion, d.h. eine der Gestalt $\frac{p}{q}$, wobei p und q Polynome sind. Wir nehmen an, dass der Grad von p streng kleiner als der von q ist. Wir suchen eine Darstellung von r als Summe von einfacheren Funktionen (einfacher in dem Sinn, dass Darstellungen als Potenzreihen leicht zu berechnen sind).

Fall 1) q hat n verschiedene (reelle oder komplexe) Nullstellen $\lambda_1, \ldots, \lambda_n$, wobei n der Grad von q ist.

Wir verwenden dann den Ansatz

$$\frac{p(x)}{(x-\lambda_1)\cdots(x-\lambda_n)} = \frac{a_1}{x-\lambda_1} + \cdots + \frac{a_n}{x-\lambda_n}.$$

Man berechnet $a_1, \ldots, a_n$, indem man ausmultipliziert und x sukzessiv gleich $\lambda_1, \ldots, \lambda_n$ setzt.

BEISPIEL.

$$r(x) = \frac{1}{(1-x)(1-2x)}$$

(also $\lambda_1 = 1$, $\lambda_2 = \frac{1}{2}$).
Ansatz:

$$\frac{1}{(1-x)(1-2x)} = \frac{A}{1-x} + \frac{B}{1-2x}.$$

Daher gilt:

$$1 = A(1-2x) + B(1-x).$$

Setzen wir $x = 1$ bzw. $x = \frac{1}{2}$, so bekommen wir $A = -1$, $B = 2$, also

$$r(x) = \frac{2}{1-2x} - \frac{1}{1-x}.$$

Fall 2) $q(x)$ hat eine Nullstelle λ mit Vielfachheit $k > 1$. Dann arbeiten wir wie oben mit zusätzlichen Termen

$$\frac{1}{(x-\lambda)^2}, \frac{1}{(x-\lambda)^3}, \ldots, \frac{1}{(x-\lambda)^k}.$$

BEISPIEL.

$$r(x) = \frac{1-2x+2x^2}{(1-x)^2(1-2x)}.$$

Ansatz:

$$\frac{A}{(1-x)^2} + \frac{B}{(1-x)} + \frac{C}{(1-2x)}.$$

Wir multiplizieren die entsprechende Gleichung mit $(1-x)^2$ und setzen $x = 1$. Das liefert $A = -1$. Man multipliziert jetzt mit $(1-2x)$ und setzt $x = \frac{1}{2}$. Das liefert $C = 2$. Jetzt setzen wir $x = 0$ und bekommen eine einfache Gleichung in A, B und C. Da A und C schon bekannt sind, können wir diese Gleichung leicht lösen und bekommen $B = 0$.
Daher gilt:

$$\frac{1-2x+2x^2}{(1-x)^2(1-2x)} = \frac{-1}{(1-x)^2} + \frac{2}{(1-2x)}.$$

4.2 Potenzreihen

Wir betrachten jetzt Potenzreihen, d.h. Summen der Gestalt

$$a_0 + a_1 x + a_2 x^2 + \cdots,$$

die wir auch als $\sum_{n=0}^{\infty} a_n x^n$ schreiben können. Diese kommen hauptsächlich als Taylorreihen von elementaren Funktionen vor (vgl. Vorlesung, Teil II).
Z. B. ist jedes Polynom

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

eine (endliche) Potenzreihe. Besonders wichtig sind die uns schon bekannten binomischen Reihen, d.h. die Potenzreihe

$$1 + rx + \binom{r}{2} x^2 + \cdots + x^r = \sum_{n=0}^{r} \binom{r}{n} x^n$$

von $(1+x)^r$ $(r \in \mathbf{N})$.
Der n-te Koeffizient in dieser Reihe ist

$$\binom{r}{n} = \frac{r(r-1)\ldots(r-n+1)}{n!}.$$

Man sieht sofort, dass dieser Ausdruck für jede reelle Zahl r (sogar für r komplex) sinnvoll ist. Damit können wir die Potenzreihe

$$(1+x)^\alpha \sim \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n$$

definieren. (Im Teil II wird man sehen, in welchem Sinn die Summe rechts tatsächlich die Funktion $(1+x)^\alpha$ darstellt).
Der Fall $\alpha = -1$, d.h.

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{n=0}^{\infty} x^n$$

wird für uns besonders wichtig sein (geometrische Reihe!).

Weitere Beispiele von Potenreihendarstellungen:

$$\begin{aligned}
e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!} \\
\ln \frac{1}{1-x} &= x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots = \sum_{n=1}^{\infty} \frac{x^n}{n} \\
\ln \frac{1}{1+x} &= -x + \frac{x^2}{2} - \frac{x^3}{3} + \cdots = \sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n} \\
\sin x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!} \\
\cos x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} \\
\frac{1}{(1-x)^{k+1}} &= \sum_{n=0}^{\infty} \binom{n+k}{n} x^n \\
\frac{1}{\sqrt{1-4x}} &= \sum_{n=0}^{\infty} \binom{2n}{n} x^n .
\end{aligned}$$

Beispiel. Zeige:

a) aus $f' = 0$ folgt f konstant, bzw.

b) aus $f' = f$ folgt $f(x) = ce^x$ (c eine Konstante).

Ansatz:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

Es gilt dann

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots$$

Wir machen einen Koeffizientenvergleich und bekommen:

a) $a_1 = 0$, $a_2 = 0$, $a_3 = 0$ ...—also $f(x) = a_0$;

b) $a_0 = a_1$, $a_1 = 2a_2$, $a_2 = 3a_3$ usw.

Daraus folgt leicht, dass $a_n = \frac{1}{n!} a_0$ — also

$$f(x) = a_0 (1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots) = a_0 e^x .$$

BEISPIEL. Berechne die Potenzreihendarstellungen von

a) $$\frac{x}{(1-x)(1-2x)}$$

b) $$\frac{1-2x+2x^2}{(1-x)^2(1-2x)}.$$

Wir haben die Bruchzerlegungen oben berechnet.
Daher gilt:
a)

$$\begin{aligned}\frac{x}{(1-x)(1-2x)} &= x\left\{\frac{2}{1-2x}-\frac{1}{1-x}\right\} = 2x(1+2x+4x^2+8x^3+\cdots)\\ &\quad -x(1+x+x^2+x^3+\cdots)\\ &= \sum_{n=1}^{\infty}(2^n-1)x^n\end{aligned}$$

b) $$\frac{1-2x+2x^2}{(1-x)^2(1-2x)} = \frac{2}{1-2x}-\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty}(2^{n+1}-n-1)x^n.$$

BEISPIEL. Bestimme ein Potenzreihendarstellung für

$$F(x) = \frac{x}{1-x-x^2}.$$

Es gilt:

$$1-x-x^2 = (1-\phi_+x)(1-\phi_-x),$$

wobei

$$\phi_+ = \frac{1+\sqrt{5}}{2}, \quad \phi_- = \frac{1-\sqrt{5}}{2}.$$

Daher

$$\begin{aligned}\frac{x}{1-x-x^2} &= \frac{x}{(1-\phi_+x)(1-\phi_-x)}\\ &= \frac{1}{\phi_+-\phi_-}\left(\frac{1}{1-\phi_+x}-\frac{1}{1-\phi_-x}\right)\\ &= \frac{1}{\sqrt{5}}\left(\sum_{n=0}^{\infty}\phi_+^nx^n-\sum_{n=0}^{\infty}\phi_-^nx^n\right).\end{aligned}$$

Wir listen in Tabellenform einige nützliche Regeln für die Berechnung von Potenzreihen auf.

f und g sind Funktionen mit Potenzreihen $\sum_{n=0}^{\infty} a_n x^n$ bzw. $\sum_{n=0}^{\infty} b_n x^n$.

$$\begin{aligned}
\alpha \cdot f &\quad \sum_{n=0}^{\infty} \alpha a_n x^n \\
f + g &\quad \sum_{n=0}^{\infty} (a_n + b_n) x^n \\
f' &\quad \sum_{n=1}^{\infty} n a_n x^{n-1} \\
\int_0^x f(u)\,du &\quad \sum_{n=0}^{\infty} \frac{a_n}{n+1} x^{n+1} \\
\frac{f - a_0}{x} &\quad \sum_{n=0}^{\infty} a_{n+1} x^n \\
\frac{f - a_0 - a_1 x}{x^2} &\quad \sum_{n=0}^{\infty} a_{n+2} x^n \\
\frac{f}{1-x} &\quad \sum_{n=0}^{\infty} s_n x^n, \\
\text{wobei} &\quad s_n = a_0 + \cdots + a_n \\
f \cdot g &\quad \sum_{n=0}^{\infty} c_n x^n, \text{ wobei } c_n = a_n b_0 + \cdots + a_0 b_n \\
f(cx) &\quad \sum_{n=0}^{\infty} c^n a_n x^n.
\end{aligned}$$

4.3 Differenzengleichungen und Potenzreihendarstellungen

Gewisse Gleichungen (sogenannte Differenzengleichungen) lassen sich mit Hilfe von Potenzreihendarstellungen lösen. Wir beginnen mit einem einfachen Beispiel:

BEISPIEL. Bestimme eine Folge (a_n), sodass

$$a_{n+1} = 2a_n + 1, \quad a_0 = 0.$$

Die ersten Terme sind also $0, 1, 3, 7, 15, \ldots$.
Eine Methode: Man stelle die naheliegende Vermutung auf, dass $a_n = 2^n - 1$. Diese Vermutung beweist man mit Hilfe der vollständigen Induktion (Übung).
Die zweite Methode funktioniert oft, auch wenn es keine solche vordergründige Vermutung gibt.
Wir betrachten die Potenzreihe mit der unbekannten Folge (a_n) als Koeffizientenfolge d.h.

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n.$$

(A heißt die **erzeugende Funktion** der Folge). Wir versuchen zunächst aus der Differenzengleichung eine (algebraische) Gleichung für A aufzustellen, indem wir die abgeleiteten Gleichungen

$$a_{n+1} x^n = 2a_n x^n + x^n$$

summieren. Damit gilt:

$$\frac{A(x)}{x} = 2A(x) + \frac{1}{1-x}.$$

Wir lösen diese Gleichung für A und bekommen

$$A(x) = \frac{x}{(1-x)(1-2x)}.$$

Jetzt brauchen wir die Potenzreihendarstellung von A. Die haben wir schon berechnet: Es gilt

$$A(x) = \sum_{n=0}^{\infty} (2^n - 1)x^n,$$

also $a_n = 2^n - 1$.

BEISPIEL. Löse die Differenzengleichung

$$a_{n+1} = 2a_n + n, \quad a_0 = 1.$$

Wiederum setzen wir $A(x) = \sum_{n=0}^{\infty} a_n x^n$ und bekommen wie vorher die Gleichung

$$\frac{A(x) - 1}{x} = 2A(x) + \sum_{n=0}^{\infty} nx^n = 2A(x) + \frac{x}{(1-x)^2}.$$

Wir lösen diese algebraische Gleichung und bekommen

$$A(x) = \frac{1 - 2x + 2x^2}{(1-x)^2(1-2x)}.$$

Die entsprechende Potenzreihendarstellung haben wir schon berechnet. Wir bekommen damit die Lösung $a_n = 2^{n+1} - n - 1$.

BEISPIEL. Wir berechnen eine explizite Formel für die Fibonacci-Reihe:

$$F_{n+2} = F_{n+1} + F_n \quad (F_0 = 0, F_1 = 1).$$

Dieses Beispiel haben wir schon berechnet (Kapitel 2 — Achtung!: die Reihe ist jetzt $0, 1, 1, 2, 3, \ldots$, nicht $1, 1, 2, 3, 5, \ldots$ wie vorher).
Wir setzen $F(x) = \sum_{n=0}^{\infty} F_n x^n$ und bekommen die Gleichung

$$\frac{F(x) - x}{x^2} = \frac{F(x)}{x} + F(x),$$

mit Lösung: $F(x) = \dfrac{x}{1 - x - x^2}$.
Aus der Potenzreihentwicklung (die wir oben berechnet haben) folgt:

$$F_n = \frac{1}{\sqrt{5}}(\phi_+^n - \phi_+^n).$$

BEMERKUNG. Um den allgemeinen Differenzenausdruck $b_n g_{k+n} + \cdots + b_0 f_k$ zu behandeln, verwenden wir das Polynom p, wobei

$$p(x) = b_0 + b_1 x + \cdots + b_n x^n.$$

Dazu betrachten wir das "gespiegelte" Polynom:

$$\bar{p}(x) = b_0 x^n + b_1 x + \cdots + b_n.$$

Z.B. für $p(x) = 1 - x - x^2$ ist $\bar{p}(x) = x^2 - x - 1$.
Es gilt $p(x) = (1 - \rho_1 x)(1 - \rho_2 x) \cdots (1 - \rho_n x)$ wobei $\rho_1, \ldots, \rho_n$ die Nullstellen von $\bar{p}$ sind.
Damit ist $\dfrac{1}{p(x)}$ eine Linearkombination der Funktionen

$$\frac{1}{1 - \rho_1 x}, \frac{1}{1 - \rho_2 x}, \cdots, \frac{1}{1 - \rho_n x}.$$

Daraus folgt, dass die allgemeine Lösung der Differenzengleichung

$$b_n g_{k+n} + b_{n-1} g_{k+n-1} + \cdots + b_0 g_k = 0$$

die Gestalt

$$g_k = c_1 \rho_1^k + \cdots + c_n \rho_n^k$$

hat.

Bemerkung. Falls

$$\bar{p}(x) = (x - \rho_1)^{d_1} \cdots (x - \rho_r)^{d_r},$$

dann ist die allgemeine Lösung

$$g_k = f_i(k)\rho_1^k + \cdots + f_r(k)\rho_r^k,$$

wobei f_i ein Polynom von Grad d_{i-1} ist.
Beispiel. Wir lösen die Gleichung

$$\begin{aligned} g_0 &= g_1 = 1 \\ g_n &= g_{n-1} + 2g_{n-2} + (-1)^n \quad (n \geq 2). \end{aligned}$$

Wie oben bekommen wir die Gleichung

$$G(x) = \frac{1 + x + x^2}{(1 - 2x)(1 + x)^2}.$$

Damit hat die allgemeine Lösung die Gestalt

$$g_n = a2^n + (bn + c)(-1)^n$$

für geeignete Konstanten a ,b, c. Wir setzen $n = 0, 1, 2$ ein und lösen das System für a, b, c.
Ergebnis:

$$g_n = \frac{7}{9}2^n + \left(\frac{n}{3} + \frac{2}{9}\right)(-1)^n.$$

4.4 Abschliessende Beispiele (nur für Fortgeschrittene)

BEISPIEL. Zeige:

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

Es gilt:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Differenziere:

$$n(1+x)^{n-1} = \sum_{k=0}^{n} k\binom{n}{k} x^{k-1}$$

Setze $x = 1$

$$n2^{n-1} = \sum_{k=0}^{n} k\binom{n}{k}.$$

BEISPIEL. Zeige:

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Es gilt

$$(1+x)^n(1+x)^n = (1+x)^{2n}.$$

Ein Koeffizientenvergleich (für x^n) liefert

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} = \binom{2n}{n}.$$

Aber

$$\binom{n}{i} = \binom{n}{n-i}.$$

BEISPIEL. Löse das System

$$\begin{aligned} u_0 &= 1, \quad u_1 = 0, \quad v_0 = 0, \quad v_1 = 1 \\ u_n &= 2v_{n-1} + u_{n-2}, \quad v_n = u_{n-1} + v_{n-2}. \end{aligned}$$

(Motivierende Bemerkung: u_n ist die Anzahl der Möglichkeiten, ein $3 \times n$ Schachbrett mit Dominosteinen zu überdecken.)

n	0	1	2	3	4	5	6	7
u_n	1	0	3	0	11	0	41	0
v_n	0	1	0	4	0	15	0	56.

Für die erzeugenden Funktionen u, v bekommen wir die algebraischen Gleichungen

$$\begin{aligned} u(x) &= 2xv(x) + x^2u(x) + 1 \\ v(x) &= xu(x) + x^2v(x) \end{aligned}$$

mit Lösungen

$$u(x) = \frac{1-x^2}{1-4x^2+x^4}, \quad v(x) = \frac{x}{1-4x^2+x^4}$$

oder $u(x) = (1-x^2)w(x^2)$, $v(x) = xw(x^2)$ mit $w(y) = \dfrac{1}{1-4y+y^2}$.
Daher gilt:

$$v_{2n+1} = w_n, \quad u_{2n} = w_n - w_{n-1}.$$

Aus der Faktorisierung $1-4y+y^2 = (1-(2+\sqrt{3})y)(1-(2-\sqrt{3})y)$ folgt:

$$\begin{aligned} v_{2n-1} &= \frac{3+2\sqrt{3}}{6}(2+\sqrt{3})^n + \frac{3-2\sqrt{3}}{6}(2-\sqrt{3})^n \\ u_{2n} &= \frac{(2+\sqrt{3})^n}{3-\sqrt{3}} + \frac{(2-\sqrt{3})^n}{3\sqrt{3}}. \end{aligned}$$

BEISPIEL. Folgende Rekursionsbeziehung spielt eine wichtige Rolle in der theoretischen Informatik:

$$b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-1} b_0, \quad b_0 = 1, b_1 = 1.$$

(b_n ist die Anzahl der "binären Bäume".)
Setze $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots$.
Es gilt dann: $b(x) = 1 + xb(x)^2$.
Daher ist

$$b(x) = \frac{1+\sqrt{1-4x}}{2x} \quad (*) \quad \text{oder} \quad \frac{1-\sqrt{1-4x}}{2x} \quad (**).$$

Aber für (*) gilt $b(0) = \infty$. Also ist (**) die einzige Möglichkeit.
Aber

$$\sqrt{1-4x} = (1-4x)^{1/2} = \sum_{k=0}^{\infty} (-4)^k \binom{\frac{1}{2}}{k} x^k$$

und so

$$b_n = -\frac{1}{2}(-4)^{n+1}\binom{\frac{1}{2}}{n+1}$$

und dies ist $\dfrac{1}{n+1}\binom{2n}{n}$ (die Catalansche Zahl).

Kapitel 5

Übungen und Lösungsbeispiele

Übungsblatt 0

Thema—Induktion, dyadische Zahlen, das Pascalsche Dreieck

1,2. Konstruiere die Multiplikations- und Additionstabelle für Zahlen bezüglich der Basis 8 (zwei Beispiele).

3. Stelle die Zahlen 35 und 17 als dyadische Zahlen dar und berechne ihre Summe und Produkt.

4. (Induktionsbeweis)

$$a + (a + d) + \cdots + (a + nd) = \frac{(n + 1)2a + nd)}{2}.$$

(Summe der arithmetischen Reihe).

5. (Induktionsbeweis)

$$a + aq + \cdots + aq^n = a\frac{1 - q^{n+1}}{1 - q} \qquad (q \neq 1).$$

(Summe der geometrischen Reihe).

6. (Die Bernoullische Ungleichung)

$$(1 + p)^n \geq 1 + np \quad (p > -1, n \in \mathbf{N}).$$

(Induktionsbeweis).

7. (Induktionsbeweis)

$$\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n + 1)} = \frac{n}{n + 1}.$$

8. (Induktionsbeweis)

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{3^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n + 2}{2^n}.$$

9. Was ist die 10-te Zeile des Pascalschen Dreiecks?

10. Was ist $\sum_{r=0}^{n}(-1)^r\binom{n}{r}$?

Lösungsvorschläge

Bsp. 4. Induktionsbeweis:

$n = 1\surd$

$n \to n+1$:

$$\begin{aligned} a+(a+d) \quad +\cdots+ \quad & (a+nd)+(a+(n+1)d) = [a+\cdots+(a+nd)]+[a(n+1)] \\ = \quad & \frac{(n+1)(2a+nd)}{2}+[a+(n+1)d] \text{ (Induktionsannahme)} \\ = \quad & \frac{(n+2)(2a+(n+1)d)}{2} \quad \text{QED.} \end{aligned}$$

Bsp. 6. Induktionsbeweis:

$n = 1\surd$

$n \to n+1$:

Es gilt: $(1+p)^n \geq 1+np$ (Induktionsannahme).

Da $1+p > 0$

$$(1+p)(1+p)^n \geq (1+p)(1+np)$$

also

$$\begin{aligned} (1+p)^{n+1} \quad & \geq \quad 1+(n+1)p+np^2 \\ & \geq \quad 1+(n+1)p \quad \text{QED.} \end{aligned}$$

Bsp. 10. Versuch

$n = 1 \quad 1-1 = 0$

$n = 2 \quad 1-2+1 = 0$

$n = 3 \quad 1-3+3-1 = 0.$

Vermutung:

$$\sum_{r=0}^{n}(-1)^r\binom{n}{r} = 0.$$

In der Tat

$$0 = (-1+1)^n = \sum_{r=0}^{n}(-1)^r\binom{n}{r} \quad \text{(binomischer Lehrsatz).}$$

Übungsblatt 1

Thema—die natürlichen Zahlen

11. Drücke die Zahlen $179, 233$ bezüglich der Basis 2 bzw. 3 aus.

12. Was is 999 (zur Basis 12)?

13. Berechne $\mathrm{ggT}\,(189, 77)$.

14. Beschreibe einen Algorithmus zum Berechnen von $\mathrm{ggT}\,(a_1, \ldots, a_n)$.

15. Beweise: $m + n = n + m$, $m.n = n.m$.

16. Seien $n_1, \ldots, n_k$ natürliche Zahlen > 1. Zeige: Es existiert ein ganze Zahl N, sodass kein n_i ein Teiler von N ist.

17. Für $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ gilt
$$\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}.$$

Induktionsbeispiele

18.
$$\sum_{r=1}^{n} r^2 = \frac{1}{6} n(n+1)(2n+1).$$

19.
$$\sum_{r=1}^{n} r^3 = \frac{1}{4} n^2 (n+1)^2$$

.

20.
$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r.$$

Lösungsvorschläge

Bsp. 11.
$$\begin{aligned} 179 &= 3 \cdot 59 + 2 \\ 59 &= 3 \cdot 19 + 2 \\ 19 &= 3 \cdot 6 + 1 \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

Lösung 20122. (Kontrolle: $2 \cdot 81 + 9 + 3 \cdot 2 + 2 = 179$).

Bsp. 12. Wir benutzen das Symbol B für 11 (Basis 12).

$$\begin{aligned} 999 &= 12 \cdot 83 + \underline{3} \\ 83 &= 12 \cdot 6 + \underline{11}; \quad 6 = 12 \cdot 0 + \underline{6}. \end{aligned}$$

Lösung: 633. (Kontrolle: $6 \cdot 144 + 11 \cdot 12 + 3 = 999$).

Bsp 13.

$$\begin{aligned} 189 &= 2 \cdot 77 + 35 \\ 77 &= 2 \cdot 35 + 7 \end{aligned}$$

also $ggT(= 189, 77) = 7$.

Bsp. 15. Wir zeigen:

I. $(m + n) + p = m + (n + p)$ (Induktion bzgl. p)

II. $m + 1 = 1 + m$ (Induktion)

III. $m + n = n + m$ (Induktion bzgl. n)

IV. $m(n + p) = mn + mp$ (Induktion bzgl. p)

V. $(m + n)p = mp + np$ (analog zu IV.)

VI. $m \cdot 1 = 1 \cdot m = m$ (Induktion)

VII. $mn = nm$ (Induktion bzgl. n).

I. $p = 1 \surd$

$$\begin{aligned} LS = (m + n) + 1 = (m + n)' &= m + n' \text{ (Definition)} \\ &= m + (n + 1) = RS. \end{aligned}$$

$p \to p + 1$ Induktionsannahme $(m + n) + p = m + (n + p)$.
Es gilt dann:

$$\begin{aligned} (m + n) + p' &= ((m + n) + p)' \text{ (Definition)} \\ &= (m + (n + p))' \text{ (Induktionsannahme)} \\ &= m + (n + p)' \text{ (Definition)} \\ &= m + (n + p') \text{ (Definition)} \end{aligned}$$

QED.

II. $m = 1 \surd$
$m \to m + 1$ Induktionsannahme $m + 1 = 1 + m$.
Es gilt dann:

$$\begin{aligned} m' + 1 &= (m + 1) + 1 \text{ (Definition)} \\ &= (1 + m) + 1 \text{ (Induktionsannahme)} \\ &= (1 + m)' \text{ (Definition)} \\ &= 1 + m' \text{ (Definition)} \end{aligned}$$

QED.

III. $m + n = n + m$
Induktion bzgl. n
$n = 1$ ist II.

$n \to n+1$

$$\begin{aligned} m+n' &= m+(n+1) \\ &= (m+n)+1 \text{ (I)} \\ &= (n+m)+1 \text{ (Induktionsannahme)} \\ &= n+(m+1) \text{ (I)} \\ &= n+(1+m) \text{ (II)} \\ &= (n+1)+m \text{ (I)} \\ &= n'+m \text{ (Definition)} \end{aligned}$$

QED.

IV. $m(n+p) = mn+mp$
Induktion bzgl. p
$p = 1$ ist die Definition.
$p \to p+1$:

$$\begin{aligned} m(n+p') &= m(n+(p+1)) \text{ (Definition)} \\ &= m(n+(1+p)) \text{ (II)} \\ &= m((n+1)+p) \text{ (I)} \\ &= m(n'+p) = mn'+mp \text{ (Induktionsannahme)} \\ &= (mn+m)+mp \text{ (Definition)} \\ &= mn+(m+mp) \text{ (I)} \ = mn+(mp+m) \text{ (III)} \\ &= mn+mp' \text{ (Definition)} \end{aligned}$$

QED.

Bem. Die Induktionsannahme ist: $m(n+p) = mn+mp$ für **alle** natürliche Zahlen m und n.

V. Ähnlich.

VI. Induktionsbeweis: $m = 1\surd$.
$m \to m+1$

$$\begin{aligned} 1 \cdot m' &= 1 \cdot m + 1 = m+1 \text{ (Induktionsannahme)} \\ &= m' \text{ (Definition)} \end{aligned}$$

QED.

VII. Induktionsbeweis bzgl. n
$n = 1$ (VI.)
$n \to n+1$

$$\begin{aligned} mn' &= mn+m \text{ (Definition)} \\ &= nm+m \text{ (Induktionshypothese)} \\ &= (n+1)m \text{ (V)} \\ &= n'm \text{ (Definition)} \end{aligned}$$

QED.

Bsp. 16. Wähle $N = n_1, n_2 \ldots n_n + 1$.

Bsp. 18. Induktionsbeweis:

$n = 1\surd$

$n \to n + 1$:

$$\begin{aligned}
\sum_{r=1}^{n=1} r^2 &= \sum_{r=1}^{n} r^2 + (n+1)^2 \\
&= \frac{1}{6}n(n+1)(2n+1) + (n+1)^2 \text{ (Induktionsannahme)} \\
&= \frac{1}{6}(n+1)(2n^2+n+6n+6) \\
&= \frac{1}{6}(n+1)(2n+3)(n+2) \\
&= \frac{1}{6}(n+1)(n+2)(2(n+2)+1) \quad \text{QED.}
\end{aligned}$$

Bsp. 19. Induktionsbeweis:

$n = 1\surd$

$n \to n + 1$:

$$\begin{aligned}
\sum_{r=1}^{n=1} r^3 &= \frac{1}{4}n^2(n+1)^2 + (n+1)^3 \text{ (Induktionsannahme)} \\
&= \frac{1}{4}(n+1)^2((n+1)+1)^2 \quad \text{QED.}
\end{aligned}$$

Bsp. 20. $n = 1$

$n \to n = 1$

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)^n(x+y) = x(x+y)^n + y(x+y)^n \\
&= \sum_{r=0}^{n} \binom{n}{r} x^{n+1-r}y^r + \sum_{r=0}^{n} \binom{n}{r} x^{n-r}y^{r+1} \text{ (Induktionsbeweis)} \\
&= \sum_{r=0}^{n} \binom{n}{r} x^{n+1-r}y^r + \sum_{S=1}^{n=1} \binom{n}{S-1} x^n - (S-1)y^S \quad (S-1=r) \\
&= \sum_{r=0}^{n} \binom{n}{r} x^{n+1-r}y^r + \sum_{r=1}^{n+1} \binom{n}{r-1} x^{n-r+1}y^n \\
&= \sum_{r=1}^{n} \underbrace{\left[\binom{n}{r} + \binom{n}{r-1}\right]} x^{n+1-r}y^r + x^{n+1} + y^{n+1} \\
&\qquad = \binom{n+1}{r} \text{ wegen Bsp. 17.} \\
&= \sum_{r=0}^{n+1} \binom{n+1}{r} x^{n+1r}y^r \qquad \text{QED.}
\end{aligned}
$$

Übungsblatt 2

Thema—Die Zahlensysteme **Q**, **R**, **C**.

21. Betrachte die folgenden Gleichungen:

    $x+22=107$, $x+22=17$, $72x=144$, $72x=143$, $x^3=26$, $x^3=27$, $x^3=-27$, $x^2=-27$, $x^2+27x+2=0$.

    Im welchem System (**N**, **Z**, **Q**, **R**, **C**) sind sie jeweils lösbar?

22. Seien r, s Rationalzahlen. Zeige: $r+s=s+r$, $r.s=s.r$.

23. Seien p, q, r, s ganze Zahlen, mit q und s positiv und $\frac{p}{q}<\frac{r}{s}$. Zeige:

$$\frac{p}{q}<\frac{p+r}{q+s}<\frac{r}{s}.$$

24. Sei x eine reelle Zahl, mit $0<x$. Zeige: Es existeren $r\in\mathbf{Q}$ und $s\in\mathbf{R}\setminus\mathbf{Q}$ mit $0<r<x$, $0<s<x$.

25. Löse das Gleichungssystem

$$\begin{aligned}(1+i)x-2y &= i\\ ix+(1-i)y &= 3.\end{aligned}$$

26. Sei $z=\sqrt{3}+i$. Berechne z^{-1}, $|z|$, z^3, die Polardarstellung von z, $z^{1.000.000}$, $z^{1/2}$.

27. Zeige: $(\cos\theta+i\sin\theta)^n=\cos n\theta+i\sin n\theta$, falls $n<0$.

28. Sei $\omega=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$. Berechne die Polardarstellung von ω. Zeige $\omega^3=1$, $1+\omega+\omega^2=0$.

29. Sei $z_1=a+b$, $z_2=a\omega+b$, $z_3=a\omega^2+b$ (ω wie im Beispiel 28). Zeige: $z_1+\omega z_2+\omega^2 z_3=0$. (Hinweis: die Punkte $1,\omega,\omega^2$ bilden die Eckpunkte eines gleichseitigen Dreiecks. Die algebraische Bedingung $z_1+\omega z_2+\omega^2 z_3=0$ entspricht der geometrischen Bedingung, dass z_1, z_2, z_3 Eckpunkte eines gleichseitigen Dreiecks sind).

30. Seien z_1, z_2, z_3 drei komplexe Zahlen und setze: $w_1=z_1(2+\omega)+z_2(1-\omega)$, $w_2=z_2(2+\omega)+z_3(1-\omega)$, $w_3=z_3(2+\omega)+z_1(1-\omega)$ (ω wie im Beispiel 28). Zeige: $w_1+\omega w_2+\omega^2 w_3=0$.

    (Hinweis: Dies ist ein "Beweis" des Satzes von NAPOLEON).

Lösungsvorschläge

Bsp. 25.

$$\begin{aligned}(1+i)x-2y &= i \quad &|\cdot i\\ ix+(1-i)y &= 3 \quad &|\cdot(1+i)\end{aligned}$$

$$\begin{aligned}(1+i)ix - 2iy &= -1\\ (1+i)ix + 2y &= 3(1+i)\end{aligned}$$

$$\begin{aligned}-y(2+2i) &= -3-3i-1\\ \underline{y} &= \frac{4+3i}{2+2i} = \frac{(4+3i(1-i)}{2(1+i)(1-i)} = \underline{\frac{7-i}{4}}.\end{aligned}$$

$$\Rightarrow \underline{x} = \frac{i+2y}{1+i} = \frac{(i+\frac{7}{2}-\frac{1}{2}i)(1-i)}{2} = \frac{1}{4}(7+i)(1-i) = \underline{2-\frac{3}{2}i}.$$

Bsp. 26.

$$\begin{aligned}z &= \sqrt{3}+i\\ z^{-1} &= \frac{\sqrt{3}-i}{3+1} = \frac{1}{4}(\sqrt{3}-1), \quad |z| = \sqrt{\sqrt{3}^2+1} = 2\\ z^3 &= (\sqrt{3}+i)^3 = \sqrt{3}^3 + 3\sqrt{3}^2 i + 3\sqrt{3}i^2 + i^3 = 8i\\ z &= 2\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right) = 2(\cos 30^\circ + i\sin 30^\circ) \quad \left(2\left(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right)\right)\\ z^{1/2} &= \sqrt{2}(\cos 15^\circ + i\sin 15^\circ)\end{aligned}$$

$1.000.000 : 6 = 166.666,\underline{4}$ Rest

$\Rightarrow z^{1.000.000} = 2^{1.000.000}(\cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi)$.

Bsp. 28.

$$\begin{aligned}\omega &= \cos 120^\circ + i\sin 120^\circ - \text{also } \omega^2 = \cos 240^\circ - i\sin 240^\circ\\ \omega^3 &= 1.\end{aligned}$$

$$1+\omega+\omega^2 = \frac{1-\omega^3}{1-\omega} = 0.$$

Bsp. 29.

$$\begin{aligned}z_1+\omega z_2+\omega^2 z_3 &= a+b+\omega(a\omega+b)+\omega^2(a\omega^2+b)\\ &= a(1+\omega^2+\omega^4)+b(1+\omega+\omega^2)\\ &= a(1+\omega+\omega^2)+b(1+\omega+\omega^2) = 0.\end{aligned}$$

Bsp. 30.

$$\begin{aligned}w_1+\omega w_2+\omega w_3 &= z_1(2+\omega)+z_2(1-\omega)+\omega(z_2(2+\omega)+z_3(1-\omega))\\ &\quad +\omega^2(z_3(2+\omega)+z_1(1-\omega))\\ &= z_1(2+\omega+\omega^2-\omega^3)+z_2(\omega(2+\omega)+1-\omega)+z_3(\omega(1-\omega)+\omega^2(2+\omega),\\ &= z_1(1+\omega+\omega^2)+z_2(1+\omega+\omega^2)+z_3\omega(1+\omega+\omega^2) = 0.\end{aligned}$$

Übungsblatt 3

Thema: Permutationen

31. Betrachte die Permutationen

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 3 & 5 & 7 & 9 & 2 & 4 & 6 & 8 & 10 \end{pmatrix}$$

Berechne $\pi_1 \circ \pi_2$, $\pi_2 \circ \pi_1$.

32. Berechne π_1^{-1} und π_2^{-1} (π_1 und π_2 wie im Bsp. 31).

33. Stelle die Permutationen π_1 und π_2 als Produkt von disjunkten Zyklen dar. (π_1 und π_2 wie im Bsp. 31).

34. Stelle die Permutationen π_1 und π_2 als Produkt von Transpositionen dar (π_1 und π_2 wie im Bsp. 31).

35. Berechne ε_{π_1} und ε_{π_2} (π_1 und π_2 wie im Bsp. 31).

36. Sei $\pi = (i_1\, i_2 \ldots i_r)$ ein Zyklus. Was ist die kleinste natürliche Zahl n, sodass $\pi^n = \mathrm{Id}$? (Versuch $\pi = (2\,4\,6\,8)$.)

37. Sei $\pi = (i_1\, i_2 \ \ldots \ i_r)\ (j_1 \ \ldots \ j_s)$ das Produkt von zwei Zyklen. Was ist die kleinste natürliche Zahl n, sodass $\pi^n = \mathrm{Id}$? (Versuch $\pi = (2\,4\,6\,8)(1\,3\,5\,7\,9)$.)

38. Was ist die kleinste natürliche Zahl n, sodass $\pi_1^n = \mathrm{Id}$ bzw. $\pi_2^n = \mathrm{Id}$? (π_1 und π_2 wie im Bsp. 31).

39. (Ergänzung zu Blatt 2) Seien z_1, z_2 komplexe Zahlen. Bestimme eine Zahl z_3, sodass z_1, z_2, z_3 die Eckpunkte eines gleichseitigen Dreiecks bilden (2 mögliche Lösungen).

40. Drücke den Schwerpunkt (Mittelpunkt) der beiden möglichen Dreiecke aus Bsp. 39 mithilfe von z_1 und z_2 aus.

Lösungsvorschläge

Bsp. 31.

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 2 & 6 & 10 & 1 & 5 & 9 & 4 & 8 \end{pmatrix}.$$

Bsp. 32.

$$\pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 1 & 7 & 2 & 8 & 3 & 9 & 4 & 10 & 5 \end{pmatrix}.$$

Bsp. 33.

$$\begin{aligned} \pi_1 &= (1\ 2\ 4\ 8\ 5\ 10\ 9\ 7\ 3\ 6) \\ \pi_2 &= (2\ 3\ 5\ 9\ 8\ 6)(4\ 7). \end{aligned}$$

Bsp. 34.

$$\begin{aligned}\pi_2 &= (2\ 6)(2\ 8)(2\ 9)(2\ 5)(2\ 3)(4\ 7)\\ \pi_1 &= (1\ 0)(1\ 3)(1\ 7)(1\ 9)(1\ 10)(1\ 5)(1\ 8)(1\ 4)(1\ 2).\end{aligned}$$

Bsp. 35.

$$\begin{aligned}\epsilon_{\pi_1} &= -1\\ \epsilon\pi_2 &= +1.\end{aligned}$$

Bsp. 36.

$$\begin{aligned}(2\ 4\ 6\ 8)^2 &= (2\ 6)(4\ 8); (2\ 4\ 6\ 8)^3 = (2\ 8\ 6\ 4)\\ (2\ 4\ 6\ 8)^4 &= \mathrm{Id}\,.\end{aligned}$$

Allgemein gilt: Die gesuchte Zahl für $(i_1 \dots i_r)$ ist r.

Bsp. 37. Es gilt: $\pi^{20} = \mathrm{Id}\,,\ \pi^r \neq \mathrm{Id}\ \ (r < 20)$.

Allgemein gilt: die gesuchte Zahl ist k.g.V. (r, s).

i.a. gilt: die kleineste Zahl n für die gilt $\pi^a = \mathrm{Id}\,.$ (π eine allgemeine Permutation) ist das kleinste gemeinsame Vielfach der Längen der Zyklen bei einer Darstellung von π als Produkt von Zyklen.

Bsp. 38. Mit Bsp. 33 und 37 gilt: $\pi_1^{10} = \mathrm{Id}\,,\ \pi_2^6 = \mathrm{Id}\,.$

Bsp. 39. Es gilt: $z_1 + \omega z_2 + \omega^2 z_3 = 0$ (Bsp. 29.),

also $\omega^2 z_3 - z_1 - \omega z_2$ (Multiplikation mit ω und Verwendung von $\omega^3 = 1$ (Bsp. 28.)),

also $z_3 = -\omega z_1 - \omega^2 z_2 = -\omega z_1 + (1+\omega) z_2$ ($\omega^2 = -1 - \omega$ (Bsp. 28.)).

(2. Lösung: $z_1(1+\omega) - \omega z_2$) (erhält man durch Vertauschung von z_1 und z_2 in obiger Rechnung).)

Bsp. 40.

$$\frac{z_1 + z_2 + z_3}{3} = \frac{1}{3}((1-\omega)z_1 + (1-\omega^2)z_2) = \frac{1}{3}((1-\omega)z_1 + (2+\omega)z_2)$$

(wegen $1 + \omega + \omega^2 = 0$ (Bsp. 28.)), bzw.

$$\begin{aligned}\frac{z_1 + z_2 + z_3}{3} &= \frac{1}{3}(z_1(2+\omega) + (1-\omega)z_2)\\ &= \frac{1}{3}(z_1(1-\omega^2) + (1-\omega)z_2).\end{aligned}$$

Übungsblatt 4

Thema: Logik und Mengenlehre

41. Die symmetrische Differenz $A \triangle B$ von zwei Mengen ist $(A \setminus B) \cup (B \setminus A)$. Zeichne ein Venndiagramm von $A \triangle B$.

    Gilt die Aussage $(A \triangle B) \triangle C = A \triangle (B \triangle C)$?

42. Zeige: $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ (Venndiagramm).

43. Gilt: $A \triangle (B \cap C) = (A \triangle B) \cap (A \triangle C)$? (Venndiagramm)

44. Zeige: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Venndiagramm).

45. Zeige: $(\Omega \setminus A) \cap (\Omega \setminus B) = \Omega \setminus (A \cup B)$ (Venndiagramm), wobei A und B Teilmengen von Ω seien.

46. Berechne: $f + g$, $f \cdot g$, $f \circ g$, $g \circ f$ wobei

$$f : x \mapsto x^3, \quad g : x \mapsto \sin x$$

    (bzw. $f : x \mapsto |x|$, $g : x \mapsto x^4$).

47. Berechne die Wahrheitstafel von

$$(\neg P \wedge Q) \Rightarrow (P \wedge Q).$$

48. Berechne die Wahrheitstafel von

$$A \wedge (\neg B \Rightarrow \neg A) \Rightarrow B.$$

49. Berechne die Wahrheitstafel von

$$(A \Rightarrow \neg B) \wedge C.$$

50. Berechne die Wahrheitstafel von

$$[A \wedge \neg(B \vee C)] \Rightarrow B.$$

Lösungsvorschläge

Bsp. 46.

$$\begin{array}{rcccll} (f+g)(x) & = & x^3 + \sin x & \text{bzw.} & |x| + x^4 & \\ (f \cdot g)(x) & = & x^3 \sin x & \text{bzw.} & |x|x^4 & (= |x^5|) \\ f \circ g(x) & = & \sin^3 x & \text{bzw.} & |x^4| & (= x^4) \\ g \circ f(x) & = & \sin x^3 & \text{bzw.} & |x|^4 & (= x^4) \end{array}$$

Bsp. 47.

P	Q	$\neg P$	$\neg P \wedge Q$	$P \wedge Q$	$(\neg P \wedge Q) \Rightarrow (P \wedge Q)$
T	T	F	F	T	T
F	T	T	T	F	F
T	F	F	F	F	T
F	F	T	F	F	T

Bsp. 49.

A	B	C	$\neg B$	$A \Rightarrow \neg B$	$(A \Rightarrow \neg B) \wedge C$
T	T	T	F	F	F
F	T	T	F	T	T
T	F	T	T	T	T
F	F	T	T	T	T
T	T	F	F	F	F
F	T	F	F	T	F
T	F	F	T	T	F
F	F	F	T	T	F

Übungsblatt 5

Thema: Lineare Gleichungssysteme und Matrizen

51. Löse das System

$$\begin{array}{rcrcrcl} 3x & + & 7y & + & z & = & 1 \\ 2x & + & y & & & = & 1 \\ 2x & + & 3y & - & z & = & 5. \end{array}$$

52. Löse das System

$$\begin{array}{rcrcl} ax & + & by & = & e \\ cx & + & dy & = & f. \end{array}$$

53. Bestimme Koeffizienten a, b, c, d, sodaß für alle $n \in \mathbf{N}$

$$1^2 + 2^2 + \cdots + n^2 = an^3 + bn^2 + cn + d.$$

(Zeige: $d = 0$, $a + b + c + d = 1$, $8a + 4b + 2c + d = 5$, $27a + 9b + 3c + d = 14$ und löse dieses System.)

54. Bestimme eine hermitesche Form für

$$A = \begin{bmatrix} 2 & -2 & 1 & 4 \\ 3 & 5 & -1 & 0 \\ 2 & -2 & 1 & 1 \end{bmatrix}$$

und löse damit

$$\begin{array}{rcrcrcrcl} 2x & - & 2y & + & z & + & 4w & = & 7 \\ 3x & + & 5y & - & z & & & = & 2 \\ 2x & - & 2y & + & z & + & w & = & 0. \end{array}$$

55. Aus den Gleichungen

$$\begin{array}{rcrcrcrcl} x & + & 2y & + & 4z & - & w & = & 1 \\ x & - & 3y & + & 2z & - & 2w & = & 7 \\ -4x & + & y & + & 2z & + & 3w & = & 0 \end{array}$$

und

$$\begin{array}{rcrcl} u & - & v & = & x \\ 2u & + & v & = & y \\ 6u & + & 2v & = & z \\ -u & + & v & = & w \end{array}$$

leite eine Gleichung für u, v ab.

56. Berechne

$$\begin{bmatrix} 1 & 2 & 4 & -1 \\ 1 & -3 & 2 & -2 \\ -4 & 1 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & -1 \\ 2 & 1 \\ 6 & 2 \\ -1 & 1 \end{bmatrix}.$$

57. Berechne A^{-1} (falls existent), wobei

$$A = \begin{bmatrix} -1 & 2 & -2 \\ 3 & -2 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

58. Berechne **alle** Lösungen des Systems:

$$\begin{array}{rcrcrcl} 2x & + & 4y & + & z & = & 0 \\ 3x & + & 5y & & & = & 0 \\ 5x & + & 13y & + & 7z & = & 0 \end{array}$$

bzw.

$$\begin{array}{rcrcrcl} 2x & + & 4y & + & z & = & 1 \\ 3x & + & 5y & & & = & 1 \\ 5x & + & 13y & + & 7z & = & 5. \end{array}$$

59. Was ist der Rang von

$$A = \begin{bmatrix} 1 & 5 & 2 \\ 1 & 1 & 7 \\ 0 & -4 & 5 \end{bmatrix}$$

bzw.

$$A = \begin{bmatrix} 1 & 5 & 2 & 9 \\ 1 & 1 & 7 & 6 \\ 0 & -4 & 5 & -2 \end{bmatrix}?$$

60. Bestimme a, b, c, sodaß

$$1 + 3 + 5 + \cdots + (2n + 1) = an^2 + bn + c.$$

Lösungsvorschläge

Bsp. 51.

$$\begin{array}{rcrcrcl} 3x & + & 7y & + & z & = & 1 \\ 2x & + & y & & & = & 1 \\ 2x & + & 3y & - & z & = & 5 \end{array}$$

$$\downarrow$$

$$\begin{array}{rcrcrcl} 3x & + & 7y & + & z & = & 1 \\ 2x & + & y & & & = & 1 \\ 5x & + & 10y & & & = & 6 \end{array}$$

$$\downarrow$$

$$\begin{array}{rcrcrcl} 3x & + & 7y & + & z & = & 1 \\ 2x & + & y & & & = & 1 \\ -15x & & & & & = & -4 \end{array}.$$

Lösung: $x = \frac{4}{15}$, $y = \frac{7}{15}$, $z = -\frac{46}{15}$.
(Kontrolle: $3x + 7y + z = \frac{12+49-46}{15} = 1$, $2x + y = 1$, $2x + 3y - z = \frac{8+21+46}{15} = 5$.)

Bsp. 52.

$$\begin{array}{rcrcl} ax & + & by & = & e \\ cx & + & dy & = & f \end{array} \rightarrow \begin{array}{rcrcl} adx & + & bdy & = & ed \\ bcx & + & bdy & = & bf \end{array} \rightarrow (ad-bc)x = cd - bf.$$

Lösung

$$x = \frac{ed-bf}{ad-bc}, \quad y = \frac{af-ce}{ad-bc}.$$

(Kontrolle:

$$ax + by = \frac{aed - abf + baf - bce}{ad-bc} = e.)$$

(Stillschweigende Annahme: $ad - bc \neq 0$.)

Bsp. 53.

$$\begin{array}{rcrcrcl} a & + & b & + & c & = & 1 \\ 8a & + & 4b & + & 2c & = & 5 \\ 27a & + & 9b & + & 3c & = & 14 \end{array} \rightarrow \begin{array}{rcrcrcl} a & + & b & + & c & = & 1 \\ 6a & + & 2b & & & = & 3 \\ 24a & + & 6b & & & = & 11 \end{array} \rightarrow \begin{array}{rcrcrcl} a & + & b & + & c & = & 1 \\ 6a & + & 2b & & & = & 3 \\ 6a & & & & & = & 2 \end{array}.$$

Lösung:

$$a = \frac{1}{3}, \quad b = \frac{1}{2}, \quad c = \frac{1}{6}, \quad d = 0.$$

Also

$$1^2 + \cdots + n^2 = \frac{1}{6}(2n^3 + 3n^2 + n) = \frac{1}{6}n(n+1)(2n+1).$$

Bsp. 54.

$$\left[\begin{array}{cccc|c} 2 & -2 & 1 & 4 & 7 \\ 3 & 5 & -1 & 0 & 2 \\ 2 & -2 & 1 & 1 & 0 \end{array}\right] \rightarrow \left[\begin{array}{cccc|c} 1 & -1 & \frac{1}{2} & 2 & \frac{7}{2} \\ 0 & 8 & -\frac{5}{2} & -6 & -\frac{17}{2} \\ 0 & 0 & 0 & -3 & -7 \end{array}\right].$$

Lösung:

$$w = \frac{7}{3}, \quad z = \lambda \text{ (freier Parameter)}, \quad y = \frac{1}{16}(11 + 5\lambda), \quad x = -\frac{1}{48}(23 + 9\lambda).$$

Probe:

$$\begin{array}{rcrcrcl} -\frac{1}{24}(23+9\lambda) & - & \frac{1}{8}(11+5\lambda) & + & \lambda + \frac{28}{3} & = & 7 \\ -\frac{1}{16}(23+9\lambda) & + & \frac{5}{16}(11+5\lambda) & - & \lambda & = & 2 \\ -\frac{1}{24}(23+9\lambda) & - & \frac{1}{8}(11+5\lambda) & + & \lambda + \frac{7}{3} & = & 0 \end{array}.$$

Bsp. 58.

$$\left[\begin{array}{ccc|c} 2 & 4 & 1 & 1 \\ 3 & 5 & 0 & 1 \\ 5 & 13 & 7 & 5 \end{array}\right] \rightarrow \left[\begin{array}{ccc|c} 2 & 4 & 1 & 1 \\ 3 & 5 & 0 & 1 \\ -9 & -15 & 0 & -2 \end{array}\right] \rightarrow \left[\begin{array}{ccc|c} 2 & 4 & 1 & 1 \\ 3 & 5 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right].$$

Wir bekommen damit äquivalente Systeme

$$\begin{array}{rcrcl} 2x & +4y & +z & = & 0 \\ 3x & +5y & & = & 0. \end{array}$$

Allgemeine Lösung:

$$x = \lambda, \quad y = -\frac{3\lambda}{5}, \quad z = \frac{2\lambda}{5} \text{ (eine einparametrige Lösungsschar)}$$

bzw.

$$\begin{array}{rcrcrcl} 2x & + & 4y & + & z & = & 0 \\ 3x & + & 5y & & & = & 0 \\ & & & & 0 & = & 1 \end{array} \quad \text{keine Lösung.}$$

Bsp. 59.

$$\begin{bmatrix} 1 & 5 & 2 \\ 1 & 1 & 7 \\ 0 & -4 & 5 \end{bmatrix} \to \begin{bmatrix} 1 & 5 & 2 \\ 0 & -4 & 5 \\ 0 & -4 & 5 \end{bmatrix} \Rightarrow \text{Rang 2}$$

$$\begin{bmatrix} 1 & 5 & 2 & 9 \\ 1 & 1 & 7 & 6 \\ 0 & -4 & 5 & -2 \end{bmatrix} \to \begin{bmatrix} 1 & 5 & 2 & 9 \\ 1 & -4 & 5 & -3 \\ 0 & -4 & 5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 5 & 2 & 9 \\ 0 & -4 & 5 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow \text{Rang 3}$$

Bsp. 60.

$$\begin{array}{lrcrcrcl} n = 0 & & & & & c & = & 1 \\ n = 1 & a & + & b & + & c & = & 4 \\ n = 2 & 4a & + & 2b & + & c & = & 9 \end{array}$$

Lösung: $c = 1$, $b = 2$, $a = 1$ d.h. $1 + 3 + \cdots + (2n + 1) = (n + 1)^2$.

Übungsblatt 6

Matrizen

61. Berechne AB, BA, wobei

a)
$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \quad B = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}$$

b)
$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \quad B = \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix}$$

c)
$$A = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}, \quad B = \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix}.$$

62. Berechne A^n, wobei

a)
$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

b)
$$A = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}.$$

63. Prüfe direkt, daß
$$x = \frac{\det \begin{bmatrix} m & b & c \\ n & e & f \\ p & k & l \end{bmatrix}}{\det \begin{bmatrix} a & b & c \\ d & e & f \\ h & k & l \end{bmatrix}} \quad \text{usw.}$$
die Lösung der Gleichung
$$\begin{array}{rcrcrcl} ax & + & by & + & cz & = & m \\ dx & + & ey & + & fz & = & n \\ hx & + & ky & + & lz & = & p \end{array}$$
ist.

64. Löse mit Hilfe der Cramerschen Regel die Gleichung
$$\begin{array}{rcrcrcl} 4x & + & y & + & 2z & = & 3 \\ x & + & y & - & 2z & = & 2 \\ x & & & + & z & = & 7. \end{array}$$

65. Berechne A^{-1}, wobei
$$A = \begin{bmatrix} -1 & 2 & -2 \\ 3 & -2 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$
(benutze Determinanten).

66. Sei
$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}.$$
Zeige: $\det AB = \det A \det B$.

67. Berechne
$$\det \begin{bmatrix} 2 & 4 & 1 \\ 3 & 5 & 0 \\ 5 & 13 & 7 \end{bmatrix}, \quad \det \begin{bmatrix} 1 & -1 & 2 & -1 \\ 0 & -1 & 3 & 1 \\ 2 & 1 & 2 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

68. Berechne
$$\det \begin{bmatrix} x+1 & 1 & 1 \\ 1 & x+1 & 1 \\ 1 & 1 & x+1 \end{bmatrix}.$$

69. Berechne
$$\det \begin{bmatrix} x & -1 & 0 \\ 0 & x & -1 \\ c & b & x+a \end{bmatrix}.$$

70. Berechne
$$\det \begin{bmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{bmatrix}.$$

Lösungsvorschläge

Bsp. 61a)
$$AB = \begin{bmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{bmatrix} = BA$$
(Drehung +Drehung = Drehung!)

b)
$$\begin{aligned} AB &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \\ &= \begin{bmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi & \cos\theta\sin\phi + \sin\theta\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & \sin\theta\sin\phi - \cos\theta\cos\phi \end{bmatrix} = \begin{bmatrix} \cos(\theta+\phi) & \sin(\theta+\phi) \\ \sin(\theta+\phi) & -\cos(\theta+\phi) \end{bmatrix} \end{aligned}$$
(Drehung + Spiegelung = Spiegelung!)

c)
$$\begin{aligned} AB &= \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \\ &= \begin{bmatrix} \cos\theta\cos\phi + \sin\theta\sin\phi & \cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi - \cos\theta\sin\phi & \sin\theta\sin\phi + \cos\theta\cos\phi \end{bmatrix} = \begin{bmatrix} \cos(\theta-\phi) & -\sin(\theta-\phi) \\ \sin(\theta-\phi) & \cos(\theta-\phi) \end{bmatrix} \end{aligned}$$
(Spiegelung + Spiegelung = Drehung!)

Bsp. 62a)

$$A^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

(Induktionsbeweis).

b)

$$A^2 = \mathrm{Id} \quad \text{– daher} \quad \begin{array}{rcl} A^{2n} & = & \mathrm{Id} \\ A^{2n+1} & = & A. \end{array}$$

Bsp. 63.

$$(ax+by+cz)\det\begin{bmatrix} a & b & c \\ d & e & f \\ h & k & l \end{bmatrix} = a\begin{pmatrix} mcl & + & nkc & + & pbf \\ -pec & - & nbl & - & mkf \end{pmatrix}$$
$$+b\begin{pmatrix} anl & + & dpc & + & hmf \\ -hnc & - & pfa & - & ldm \end{pmatrix} + c\begin{pmatrix} aep & + & dkm & + & hbn \\ -hem & - & dhp & - & akn \end{pmatrix}$$
$$= m(ael + dkc + hbf - hec - dbl - akf) = m\det\begin{bmatrix} a & b & c \\ d & e & f \\ h & k & l \end{bmatrix}.$$

Bsp. 66.

$$\begin{array}{rcl} \det A & = & ad - bc, \quad \det B = a_1d_1 - b_1c_1 \\ \det AB & = & (aa_1 + bc_1)(cb_1 + dd_1) - (aa_1 + dc_1)(ab_1 + bd_1) \\ & = & aa_1cb_1 + bc_1cb_1 + aa_1dd_1 + bc_1dd_1 - ca_1ab_1 - dc_1ab_1 - ca_1bd_1 - dc_1bd_1 \\ & = & aa_1dd_1 + bcb_1c_1 - bca_1d_1 - adb_1c_1 \\ & = & \det A \det B. \end{array}$$

Bsp. 68.

$$\det\begin{bmatrix} x+1 & 1 & 1 \\ 1 & x+1 & 1 \\ 1 & 1 & x+1 \end{bmatrix} = \det\begin{bmatrix} x & -x & x \\ 1 & x+1 & 1 \\ 0 & -x & x \end{bmatrix} = \det\begin{bmatrix} x & 0 & 0 \\ 1 & x+2 & 1 \\ 0 & -x & x \end{bmatrix}$$
$$= x(x^2 + 2x + x) = x^2(x+3).$$

Bsp. 69.

$$\det\begin{bmatrix} x & -1 & 0 \\ 0 & x & -1 \\ c & b & x+a \end{bmatrix} = x(x^2 + ax + b) + c = x^3 + ax^2 + bx + c.$$

Bsp. 70.

$$\det\begin{bmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{bmatrix} = \det\begin{bmatrix} 1 & 0 & 0 \\ x & y-x & z-x \\ x^2 & y^2-x^2 & z^2-x^2 \end{bmatrix} = (y-x)(z-x)\det\begin{bmatrix} 1 & 1 \\ y+x & z+x \end{bmatrix}$$
$$= (y-x)(z-x)(z-y).$$

Allgemein

Bsp. 68.

$$\det \begin{bmatrix} x+1 & 1 & \dots & 1 \\ 1 & x+1 & \dots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & & 1+x \end{bmatrix} = x^{n-1}(x+n).$$

Bsp. 69

$$\det \begin{bmatrix} 1 & 1 & \dots & 1 \\ \vdots & & & \\ x_1^{n-1} & & \dots & x_n^{n-1} \end{bmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i)$$

(VANDERMONDE-Determinante).

Bsp. 70

$$\det \begin{bmatrix} x & -1 & 0 & \dots & 0 \\ 0 & x & -1 & \dots & 0 \\ \vdots & & & & \\ a_0 & a_1 & a_2 & \dots & x + a_{n-1} \end{bmatrix} = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

(Begleitmatrix).

Übungsblatt 7

Thema: Eigenwertprobleme

71. Löse das Eigenwertproblem für
$$A = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}.$$

72. Löse das Eigenwertproblem für
$$A = \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix}.$$

73. Löse das Eigenwertproblem für
$$A = \begin{bmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{bmatrix}.$$

74. Berechne A^n (A wie in 73).

75. Löse die Differenzengleichung
$$G_{n+2} = \frac{1}{2}(G_{n+1} + G_n)$$
$$G_0 = 0, \qquad G_1 = \frac{1}{2}.$$

76. Löse das System
$$\begin{array}{rcrcr} \frac{df}{dt} & = & & & g \\ \frac{dg}{dt} & = & -6f & + & 5g. \end{array}$$

77. Löse das System
$$\begin{array}{rcrcr} \frac{dx}{dt} & = & & & 2y \\ \frac{dy}{dt} & = & 3x & + & y. \end{array}$$

78. Löse die Gleichung
$$y'' + 2y' - 3y = 0.$$

79. Berechne das kleinste r, sodaß $\pi^r = \mathrm{Id}$, wobei
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots\ldots\ldots & 26 \\ 1 & 14 & 2 & 15 & 3 & \ldots\ldots\ldots & 26 \end{pmatrix}.$$

80. Berechne das kleinste r, sodaß $\pi^r = \mathrm{Id}$, wobei
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots\ldots\ldots & 26 \\ 14 & 1 & 15 & 2 & 16 & \ldots\ldots\ldots & 13 \end{pmatrix}.$$

Lösungsvorschläge

Bsp. 71)

$$\det(A-\lambda I)=\det\begin{bmatrix}1-\lambda & 3\\ 3 & 1-\lambda\end{bmatrix}=1-2\lambda+\lambda^2-9=(\lambda+2)(\lambda-4).$$

$\lambda=-2$: Eigenvektor $(1,-1)$;

$\lambda=4$: Eigenvektor $(1,1)$.

Also

$$P^{-1}AP=\begin{bmatrix}-2 & 0\\ 0 & 4\end{bmatrix}\quad\text{mit}\quad P=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}.$$

Bsp. 72. $\det(A-\lambda I)=6-5\lambda+\lambda^2-2=(\lambda-4)(\lambda-1)$

$\lambda=4$: Eigenvektor $(2,1)$;

$\lambda=1$: Eigenvektor $(1,-1)$.

Also

$$P^{-1}AP=\begin{bmatrix}4 & 0\\ 0 & 1\end{bmatrix}\quad\text{mit}\quad P=\begin{bmatrix}2 & 1\\ 1 & -1\end{bmatrix}.$$

Bsp. 73.

$$P^{-1}AP=\begin{bmatrix}-2 & 0 & 0\\ 0 & -2 & 0\\ 0 & 0 & 4\end{bmatrix}\quad\text{mit}\quad P=\begin{bmatrix}1 & 1 & 1\\ 1 & 0 & 1\\ 0 & -1 & 2\end{bmatrix}.$$

Bsp. 74. Also

$$\begin{aligned}A^n &= P\begin{bmatrix}(-2)^n & 0 & 0\\ 0 & (-2)^n & 0\\ 0 & 0 & 4^n\end{bmatrix}P^{-1}\\ &= \frac{1}{2}\begin{bmatrix}1 & 1 & 1\\ 1 & 0 & 1\\ 0 & -1 & 2\end{bmatrix}\begin{bmatrix}(-2)^n & 0 & 0\\ 0 & (-2)^n & 0\\ 0 & 0 & 4^n\end{bmatrix}\begin{bmatrix}-1 & 3 & -1\\ 2 & -2 & 0\\ 1 & -1 & 1\end{bmatrix}\\ &= \frac{1}{2}\begin{bmatrix}1 & 1 & 1\\ 1 & 0 & 1\\ 0 & -1 & 2\end{bmatrix}\begin{bmatrix}-(-2)^n & 3(-2)^n & -(-2)^n\\ 2(-2)^n & -2(-2)^n & 0\\ 4^n & -4^n & 4^n\end{bmatrix}\\ &= \frac{1}{2}\begin{bmatrix}(-2)^n+4^n & (-2)^n-4^n & -(-2)^n+4^n\\ -(-2)^n+4^n & 3(-2)^n-4^n & -(-2)^n+4^n\\ -2(-2)^n+2\cdot 4^n & 2(-2)^n-2\cdot 4^n & 2\cdot 4^n\end{bmatrix}.\end{aligned}$$

Bsp. 75. Für

$$X_n=\begin{bmatrix}G_{n+1}\\ G_n\end{bmatrix}\quad\text{gilt}\quad X_{n+1}=AX_n\quad\text{— also}\quad X_n=A^nX_0,\quad\text{wobei}$$

$$X_0=\begin{bmatrix}\frac{1}{2}\\ 0\end{bmatrix},\quad A=\begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ 1 & 0\end{bmatrix}.$$

$$P^{-1}AP = \begin{bmatrix} -\frac{1}{2} & 0 \\ 0 & 1 \end{bmatrix} \quad \text{mit} \quad P = \begin{bmatrix} 1 & 1 \\ -2 & 1 \end{bmatrix}.$$

Also

$$A^n = P \begin{bmatrix} (-\frac{1}{2})^n & 0 \\ 0 & 1 \end{bmatrix} P^{-1}.$$

Also

$$\begin{bmatrix} G_{n+1} \\ G_n \end{bmatrix} = P \begin{bmatrix} (-\frac{1}{2})^n & 0 \\ 0 & 1 \end{bmatrix} P^{-1} \begin{bmatrix} \frac{1}{2} \\ 0 \end{bmatrix} \quad \text{— also} \quad G_n = \frac{1}{3} - \frac{1}{3}\left(-\frac{1}{2}\right)^n.$$

Bsp. 76.

$$\text{Diagonalisiere} \quad A = \begin{bmatrix} 0 & 1 \\ -6 & 5 \end{bmatrix} \quad \text{— Ergebnis} \quad P^{-1}AP = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}.$$

Daher: $f = c_1e^{3t} + c_2e^{2t}$, $g = 3c_1e^{3t} + 2c_2e^{2t}$.

Bsp. 77.

$$\text{Diagonalisiere} \quad A = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} \quad \text{— Ergebnis} \quad P^{-1}AP = \begin{bmatrix} 3 & 0 \\ 0 & -2 \end{bmatrix} \quad \text{mit} \quad P = \begin{bmatrix} 2 & 1 \\ 3 & -1 \end{bmatrix}.$$

Daher: $x = 2c_1l^{3t} + c_2e^{-2t}$, $y = 3c_1e^{3t} - c_2e^{-2t}$.

Bsp. 78. Setze $x_1 = y, x_2 = y'$. Wir bekommen das System

$$\begin{aligned} \frac{dx_1}{dt} &= x_2 \\ \frac{dx_2}{dt} &= 3x_1 - 2x_2. \end{aligned}$$

$$\text{Diagonalisiere} \quad \begin{bmatrix} 0 & 1 \\ 3 & -2 \end{bmatrix} \quad \text{— Ergebnis} \quad P^{-1}AP = \begin{bmatrix} -3 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{mit} \quad P = \begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix}.$$

Also $y = c_1e^{-3t} + c_2e^t$.

Bsp. 79.

$$\pi = (2\ 14\ 20\ 23\ 12\ 19\ 10\ 18\ 22\ 24\ 25\ 13\ 7\ 4\ 15\ 8\ 17\ 9\ 5\ 3)(6\ 16\ 21\ 11)$$

— also $r = 20 = \text{kgV}\,(4, 20)$.

Bsp. 80.

$$\pi = (1\ 14\ 7\ 17\ 22\ 11\ 19\ 23\ 25\ 26\ 13\ 20\ 10\ 5\ 16\ 8\ 4\ 2)(3\ 15\ 21\ 24\ 12\ 6)(18\ 9)$$

— also $r = 18 = \text{kgV}\,(18, 6, 2)$.

Übungsblatt 8

Thema: Gleichungssysteme (Wiederholung) — Zahlentheorie

81. Löse das Eigenwertproblem für

$$A = \begin{bmatrix} 13 & 0 & -12 \\ 12 & 1 & -12 \\ 16 & 0 & -15 \end{bmatrix}.$$

82. Löse die vier Systeme:

$$\begin{array}{rcrcl} 3x & - & 5y & = & 1 \\ 2x & - & y & = & 10, \end{array} \quad \begin{array}{rcrcl} 7x & + & 5y & = & 0 \\ 3x & - & 2y & = & 0, \end{array} \quad \begin{array}{rcrcl} -8x & + & 2y & = & 1 \\ 9x & - & 3y & = & -2, \end{array} \quad \begin{array}{rcrcl} 12x & + & 9y & = & 18 \\ 8x & + & 6y & = & 12. \end{array}$$

83. Berechne A^{-1}, wobei $A = \begin{bmatrix} 3 & 0 & 2 \\ 7 & -1 & 5 \\ 0 & 4 & 2 \end{bmatrix}$.

84. Berechne

$$\det \begin{bmatrix} 3 & 10 & 3 & 7 \\ 2 & -1 & 6 & 8 \\ 1 & 3 & -2 & 5 \\ 6 & -3 & 1 & 4 \end{bmatrix}.$$

85. Löse das System

$$\begin{array}{rcrcrcrcl} x & + & y & + & 5z & + & 2u & = & 1 \\ 3x & - & 2y & & & - & u & = & 5 \\ 2x & + & y & + & 7z & + & 5u & = & 0. \end{array}$$

86. Berechne $d = \mathrm{ggT}\,(1819, 3587)$ und Zahlen s, t mit

$$1819s + 3587t = d.$$

87. Bestimme $s, t, u \in \mathbf{Z}$ mit $35s + 55t + 77u = 1$.

    (Bemerkung: $35, 55, 77$ sind relativ prim, aber nicht paarweise relativ prim.)

88. Bestimme die kleinste Zahl k, sodaß k genau einen (bzw. $2, 3, 4, 5, 6$) Teiler hat.

89. Berechne das Stein-Brocot Verfahren mit den Anfangswerten

$$\left(\frac{0}{1}, \frac{1}{1}\right) \quad \text{bzw.} \quad \left(\frac{0}{1}, \frac{1}{0}, \frac{0}{-1}, \frac{-1}{0}\right).$$

90. Brüche $\frac{m}{n} < \frac{m'}{n'}$ heißen **adjazent**, falls $m'n - mn' = 1$.

    (Bem. Dies impliziert, daß m und n bzw. m' und n' relativ prim sind).

    Zeige: $\frac{m}{n}$ und $\frac{m'}{n'}$ adjazent $\Rightarrow$ $\frac{m}{n}$ und $\frac{m+m'}{n+n'}$ (bzw. $\frac{m+m'}{n+n'}$ und $\frac{m'}{n'}$) sind adjazent.

    (NB. Die Bruchpaare, die in *einer* Fareyreihe vorkommen, sind adjazent — also der Gestalt $\frac{m}{n}$ mit m, n Teilerfrei.)

Lösungsvorschläge

Bsp. 81)

$$\begin{aligned}\det(A-\lambda\cdot E) &= \det\begin{pmatrix}13-\lambda & 0 & -12\\ 12 & 1-\lambda & -12\\ 16 & 0 & -15-\lambda\end{pmatrix} = (1-\lambda)(13-\lambda)((15-\lambda)+12\cdot 16)\\ &= (1-\lambda)(2\lambda+\lambda^2-3) = (1-\lambda)(\lambda-1)(\lambda+3).\end{aligned}$$

EW: $1, 1, -3$.

Eigenvektoren:

$$\underline{\lambda=-3:}\quad \begin{pmatrix}16 & 0 & -12\\ 12 & 4 & -12\\ 16 & 0 & -12\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix} = \begin{pmatrix}0\\ 0\\ 0\end{pmatrix} \Rightarrow (x,y,z) = (3,3,4) = e_1.$$

$$\underline{\lambda=1:}\quad \begin{pmatrix}12 & 0 & -12\\ 12 & 0 & -12\\ 16 & 0 & -16\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix} = \begin{pmatrix}0\\ 0\\ 0\end{pmatrix} \Rightarrow \begin{array}{rcl} e_2 &=& \underline{(1,0,1)}\\ & & \\ e_3 &=& \underline{(0,1,0)}\end{array}.$$

Bsp. 82.

$$x=7, y=4;\quad x=0, y=0;\quad x=\frac{1}{6}, y=\frac{7}{6};\qquad \begin{array}{rcl} x &=& \text{frei wählbar!}\\ y &=& 2-\frac{4}{3}x\end{array}.$$

Bsp. 83.

$$\left(\begin{array}{cccccc}3 & 0 & 2 & 1 & 0 & 0\\ 7 & -1 & 5 & 0 & 1 & 0\\ 0 & 4 & 2 & 0 & 0 & 1\end{array}\right) \to \left(\begin{array}{cccccc}1 & 0 & \frac{2}{3} & \frac{1}{3} & 0 & 0\\ 0 & -1 & \frac{1}{3} & -\frac{7}{3} & 1 & 0\\ 0 & 4 & 2 & 0 & 0 & 1\end{array}\right) \to \left(\begin{array}{cccccc}1 & 0 & \frac{2}{3} & \frac{1}{3} & 0 & 0\\ 0 & 1 & -\frac{1}{3} & \frac{7}{3} & -1 & 0\\ 0 & 4 & 2 & 0 & 0 & 1\end{array}\right) \to$$

$$\left(\begin{array}{cccccc}1 & 0 & \frac{2}{3} & \frac{1}{3} & 0 & 0\\ 0 & 1 & -\frac{1}{3} & \frac{7}{3} & -1 & 0\\ 0 & 0 & \frac{10}{3} & -\frac{28}{3} & 4 & 1\end{array}\right) \to \left(\begin{array}{cccccc}1 & 0 & \frac{2}{3} & \frac{1}{3} & 0 & 0\\ 0 & 1 & 0 & \frac{7}{5} & -\frac{3}{5} & \frac{1}{10}\\ 0 & 0 & 1 & -\frac{14}{5} & \frac{6}{5} & \frac{3}{10}\end{array}\right) \to \left(\begin{array}{cccccc}1 & 0 & 0 & \frac{11}{5} & -\frac{4}{5} & -\frac{1}{5}\\ 0 & 1 & 0 & \frac{7}{5} & -\frac{3}{5} & \frac{1}{10}\\ 0 & 0 & 1 & -\frac{14}{5} & \frac{6}{5} & \frac{3}{10}\end{array}\right).$$

Bsp. 84.

$$\begin{aligned}\det\begin{pmatrix}3 & 10 & 3 & 7\\ 2 & -1 & 6 & 8\\ 1 & 3 & -2 & 5\\ 6 & -3 & 1 & 4\end{pmatrix} &= 3\cdot\det\begin{pmatrix}-1 & 6 & 8\\ 3 & -2 & 5\\ -3 & 1 & 4\end{pmatrix} - 10\cdot\det\begin{pmatrix}2 & 6 & 8\\ 1 & -2 & 5\\ 6 & 1 & 4\end{pmatrix}\\ &\quad + 3\cdot\det\begin{pmatrix}2 & -1 & 8\\ 1 & 3 & 5\\ 6 & -3 & 4\end{pmatrix} - 7\cdot\det\begin{pmatrix}2 & -1 & 6\\ 1 & 3 & -2\\ 6 & -3 & 1\end{pmatrix}\\ &= -3\cdot 173 - 10\cdot 234 - 3\cdot 140 + 7\cdot 119 = -2446.\end{aligned}$$

Bsp. 85.

$$\left(\begin{array}{ccccc}1 & 1 & 5 & 2 & 1\\ 3 & -2 & 0 & -1 & 5\\ 2 & 1 & 7 & 5 & 0\end{array}\right) \to \left(\begin{array}{ccccc}1 & 1 & 5 & 2 & 1\\ 0 & -5 & -15 & -7 & 2\\ 0 & -1 & -3 & 1 & -2\end{array}\right) \to \left(\begin{array}{ccccc}1 & 1 & 5 & 2 & 1\\ 0 & 5 & 15 & 7 & -2\\ 0 & 0 & 0 & \frac{12}{5} & -\frac{12}{5}\end{array}\right)$$

$$\Rightarrow u = \frac{-12/5}{12/5} = \underline{-1}$$

z ... frei wählbarer Parameter.

$5y = -2 - 7u - 15z = 5 - 15z \Rightarrow \underline{y = 1 - 3z}$

$x = 1 - 2u - 5z - y = 1 + 2 - 5z - 1 + 3z = \underline{2 - 2z}$.

Bsp. 86.

$$\begin{aligned}
3587 &= 1 \cdot 1819 + 1768 \\
1819 &= 1 \cdot 1768 + 51 \\
1768 &= 34 \cdot 51 + 34 \\
51 &= 1 \cdot 34 + 17 \\
34 &= 2 \cdot 17 + 0 \quad \Rightarrow \underline{\text{ggT}\,(3587, 1819) = 17}
\end{aligned}$$

$$\begin{aligned}
\underline{17} &= 51 - 34 \\
&= 51 - (1768 - 34 \cdot 51) \\
&= -1768 + 35 \cdot 51 \\
&= -1768 + 35 \cdot (1819 - 1768) \\
&= 35 \cdot 1819 - 36 \cdot 1768 \\
&= 35 \cdot 1819 - 36 \cdot (3587 - 1819) \\
&= \underline{-36 \cdot 3587 + 71 \cdot 1819.}
\end{aligned}$$

Bsp. 87. $35s + 55 + 77u = 1$. Betrachte die Gleichung $\bmod 5, 7, 11$:

$$\begin{aligned}
\bmod 5: \quad 2u &= 1 (\bmod 5) / \cdot 3 \\
\Rightarrow \quad u &= 3 (\bmod 5) \Rightarrow u = 5\tilde{u} + 3 \\
\bmod 7: \quad 6t &= 1 (\bmod 7) / \cdot 6 \\
\Rightarrow \quad t &= 6 (\bmod 7) \Rightarrow t = 7\tilde{s} + 6 \\
\bmod 11: \quad 2s &= 1 (\bmod 11) / \cdot 6 \\
\Rightarrow \quad s &= 6 (\bmod 11) \Rightarrow s = 11\tilde{s} + 6
\end{aligned}$$

$$\begin{aligned}
\Rightarrow 385(\tilde{s} + \tilde{t} + \tilde{u}) + 210 + 330 + 231 &= 1 \\
385(\tilde{s} + \tilde{t} + \tilde{u}) &= -770 \\
\tilde{s} + \tilde{t} + \tilde{u} &= -2 \quad \Rightarrow \text{ z.B. } \tilde{s} = \tilde{t} = -1, \tilde{u} = 0
\end{aligned}$$

$\Rightarrow \underline{s = -5, t = -1, u = 3}$.

Bsp. 88.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Anzahl der Teiler	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5

’

also $k = 1, 2, 4, 8, 16, 12$.

Bsp. 90.

$$\begin{aligned} \frac{m}{n} \text{ und } \frac{m+m'}{n+n'} \text{ adjazent} \quad &\Leftrightarrow \quad n(m+m') - m(n+n') = a+1 \\ &\Leftrightarrow \quad nm' - mn' = 1 \surd. \end{aligned}$$

Übungsblatt 9

Thema: Zahlentheorie

91. Lukaszahlen $L_0, L_1, L_2, \ldots$ sind die Zahlen der Reihe $1, 3, 4, 7, 11, 18, \ldots$.
    Bestimme eine geschlossene Formel für L_n. (Benutze die Formel aus dem Skriptum für A^n, wobei $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.)

92. Zeige: $L_n = F_{n-1} + F_{n+1}$, wobei $F_0, F_1, \ldots$ die Fibbonaci-Reihe $1, 1, 2, 3, 5, 8, \ldots$ ist.

93. Zeige: $F_n L_n = F_{2n+1}$.

94. Finde Zahlen x mit $2x = 1 \pmod 3$, $3x = 1 \pmod 5$, $x = 1 \pmod 7$.

95. Zeige: Jede Quadratzahl hat eine der folgenden Einerziffern $0, 1, 4, 5, 6, 9$.

96. Für jedes $n \in \mathbf{Z}$ ist $n^{13} - n$ durch $2, 3, 5, 7, 13$ teilbar.

97. Was ist die letzte Ziffer von 3^{400}, 2^{400}?

98. Zeige: $\frac{3^{77}-1}{2}$ ist ungerade und zusammengesetzt. (Hinweis: Berechne $3^{77} \pmod 4$ und zeige, dass $23 | \frac{3^{77}-1}{2}$.)

99. Falls $x = 1 \pmod 4$ bzw. $2 \pmod 3$, dann $x = ? \pmod{12}$.

100. Kürze den Ausdruck

     a) $\frac{3381821}{17759}$

     b) $\frac{48529591}{6186818}$.

Lösungsvorschläge

Bsp. 91.

$$\begin{pmatrix} L_{n+1} \\ L_n \end{pmatrix} = A^n \begin{pmatrix} L_1 \\ L_0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad L_0 = 1, L_1 = 3$$

$$A^n = P \cdot \begin{pmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & 0 \\ 0 & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{pmatrix} \cdot P^{-1}, \quad P = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} L_{n+1} \\ L_n \end{pmatrix} = P \cdot D \cdot P^{-1} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \qquad \Rightarrow \underline{L_n = \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} + \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}$$

Bsp. 93.

$$\begin{aligned} F_n \cdot L_n &= \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right) \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} + \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right) \\ &= \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{2n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{2n+2} \right) = F_{2n+1} \end{aligned}$$

Bsp. 94.

$$\begin{array}{rcll} 2x & = & 1 & (\mathrm{mod}\, 3) \\ x & = & 2 & (\mathrm{mod}\, 3) \end{array} \qquad \begin{array}{rcll} 3x & = & 1 & (\mathrm{mod}\, 5) \\ x & = & 2 & (\mathrm{mod}\, 5) \end{array} \qquad \begin{array}{rcll} x & = & 1 & (\mathrm{mod}\, 7) \\ x & = & 1 & (\mathrm{mod}\, 7) \end{array}$$

$$\begin{array}{rcl} c_1 = 2; \quad m_1 = 3 & \qquad c_2 = 2; \quad m_2 = 5 & \qquad c_3 = 1; \quad m_3 = 7 \\ M = m_1 \cdot m_2 \cdot m_3 = 105 & & \\ M_1 = 35 & \qquad M_2 = 21 & \qquad M_3 = 15 \end{array}$$

Löse

$$\begin{array}{rcll} 35\bar{y}_1 & = & 1 & (\mathrm{mod}\, 3) \\ \bar{y}_1 & = & 2 & \end{array} \qquad \begin{array}{rcll} 21\bar{y}_2 & = & 1 & (\mathrm{mod}\, 5) \\ \bar{y}_2 & = & 1 & \end{array} \qquad \begin{array}{rcll} 15\bar{y}_3 & = & 1 & (\mathrm{mod}\, 7) \\ \bar{y}_3 & = & 1 & \end{array}$$

$\Rightarrow x = \sum c_i M_i \bar{y}_i = 2 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 1 \cdot 15 \cdot 1 = \underline{197 = 92 \pmod{M}}$.

Bsp. 95. Für $j = 0, 1, \ldots, 9$ gilt: $a = j \pmod{10} \Rightarrow a^2 = j^2 \pmod{10}$
$\{j^2 \mod 10\} \mid = 0, 1, \ldots, 9\} = \{0, 1, 4, 9, 6, 5, 6, 9, 4, 1\} = \underline{\{0, 1, 4, 5, 6, 9\}}$.

Bsp. 97. $3^4 = 81 = 1 \pmod{10}$
$3^{400} = (3^4)^{100} = 1^{100} = \underline{1 \pmod{10}}$

$2^5 = 32 = 2 \pmod{10}$
$2^{400} = (2^5)^{80} = 2^{80} = (2^5)^{16} = 2^{16} = (2^5)^3 \cdot 2 = 2^3 \cdot 2 = 16 = \underline{6 \pmod{10}}$.

Bsp. 98. $3^4 = 81 = 1 \pmod{4}$
$3^{77} - 1 = (3^4)^{19} \cdot 3 - 1 = 3 - 1 = 2 \pmod{4}$

$\Rightarrow \dfrac{3^{77} - 1}{2} = \dfrac{4 \cdot k + 2}{2} = 2k + 1$, D.h. diese Zahl ist **ungerade**.

Bsp. 99. Falls $x = 1 \pmod{4}$, dann gilt $x \in \{1, 5, 9\}$ (betrachte nur x in $\{0, 1, \ldots, 11\}$).
Falls $x = 2 \pmod{3}$, dann gilt $x \in \{2, 5, 8, 11\}$.
Falls beide Bedingungen erfüllt sind, muß $\underline{x = 5}$ gelten.

Übungsblatt 10

Thema: Zahlentheorie

101. Zeige: $6|n^3+11n$ $(n \in \mathbf{N})$

$42|n^7-n$ $(n \in \mathbf{N})$

102. $4147|12^{512}-1$

$13|2^{70}+3^{70}$.

103. Stelle eine Inverstabelle modulo $2,3,4,5,6,7,13,17,19,20$ usw. auf.

104. Wir identifizieren die Zahlen $\{0,1,\ldots,25\}$ mit dem Alphabet $\{A,B,\ldots,Z\}$. Für jedes $a \in \mathbf{N}$, das zu 26 relativ prim ist und für jedes $m \in \mathbf{N}$ ist die Zuordnung $n \mapsto an+m \pmod{26}$ ein Kode. Chiffriere die Wörter KLAUSUR ($a=3$, $m=5$) bzw. INFORMATIK ($a=5$, $m=1$).

105. Berechne die Inverse der Abbildung $n \mapsto 3n+5 \pmod{26}$ und dechiffriere damit die kodierte Version von KLAUSUR aus Bsp. 104. Löse die Systeme

106. $x = 2 \pmod 7$, $x = 5 \pmod 9$

107. $x = -1 \pmod 3$, $x = 3 \pmod 4$

108. $x = 2 \pmod 6$, $x = 5 \pmod 9$

109. $x = 1 \pmod 8$, $x = 3 \pmod{12}$

110. a) $x = 20 \pmod{35}$, $x = 28 \pmod{36}$

b) $x = 10 \pmod{19}$, $x = -2 \pmod{28}$.

Lösungsvorschläge

Bsp. 101. $n = 0 \pmod 6 \Rightarrow n^3+11n = 0 \pmod 6$

$n = 1 \pmod 6 \Rightarrow n^3+11n = 12 = 0 \pmod 6$

$n = 2 \pmod 6 \Rightarrow n^3+11n = 8+22 = 30 = 0 \pmod 6$ usw.

$n = 0$ oder $1 \pmod 6 \Rightarrow n^7-n = 0 \pmod 6$

$n = 2 \pmod 6 \Rightarrow n^7-n = 2^7-2 = 0 \pmod 6$ usw.

Bsp. 102. $4147 = 13 \cdot 29 \cdot 11$

$12^{512}-1 = (1)^{512}-1 = 0 \pmod{11}$

$12^{512}-1 = (-1)^{512}-1 = 0 \pmod{13}$

$12^2 = 144 = -1 \pmod{29}$. Also $12^{512}-1 = (-1)^{256}-1 = 0 \pmod{29}$.

$2^7 = 128 = -2 \pmod{13}$.

Daher $2^{70} = (2^7)^{10} = (-2)^{10} = 2^{10} = 2^7 \cdot 8 = -16 = 10 \pmod{13}$

$3^4 = 3 \pmod{13}$. Daher $3^{70} = 3^{68} \cdot 9 = 3^{17} \cdot 9 = 3^{16} \cdot 27$

$= 3^4 = 3 \pmod{13}$.

Also $2^{70} + 3^{70} = 10 + 3 = 0 \pmod{13}$.

Bsp. 103.

x	1	2	3	4	5	6	7	8	9	10	11	12
x^{-1}	1	7	9	10	8	11	2	5	3	4	6	12

$\pmod{13}$

Bsp. 106. Lösungen von $x = 2 \pmod{7}$: $2, 9, 16, 23, \ldots$

Lösungen von $x = 5 \pmod{9}$: $5, 14, 23, \ldots \Rightarrow$ 23 löst beide Gleichungen (geht auch mit Chinesischem Restsatz).

Bsp. 107. Lösungen von $x = -1 \pmod{3}$: $2, 5, 8, 11, \ldots$

Lösungen von $x = 3 \pmod{4}$: $3, 7, 11, \ldots \Rightarrow$ 11 löst beide Gleichungen (geht auch mit Chinesischem Restsatz).

Bsp. 108. $x = 2 \pmod{6} \Rightarrow x = 2, 8, 14, \ldots$

$x = 5 \pmod{9} \Rightarrow x = 5, 14, \ldots \Rightarrow \underline{x = 14}$.

Bsp. 109. Keine Lösung.

Bsp. 110. a) $x = 20 \pmod{35} \Rightarrow m_1 = 35, M_1 = 36$

$x = 28 \pmod{36} \Rightarrow m_2 = 36, M_2 = 35$

$M = 35 \cdot 36 = 1260$

löse $36y_1 = 1 \pmod{35} \Rightarrow y_1 = 1$

löse $35y_2 = 1 \pmod{36} \Rightarrow y_2 = -1 = 35 \pmod{36}$

$x = 20 \cdot 36 \cdot 1 + 28 \cdot 35 \cdot 35 = 720 + 34300$

$= 35020 = 1000 \pmod{1260}$.

Übungsblatt 11

Thema: Erzeugende Funktionen
Falls g die erzeugende Funktion von (a_n) ist, was ist die von der Funktion

111. $\frac{1}{2}[g(x) + g(-x)]$

112. $\frac{1}{3}[g(x) + g(\omega x) + g(\omega^2 x)]$ (ω wie im Beispiel 28)

113. $\frac{1}{4}[g(x) + g(ix) + g(-x) + g(-ix)]$ erzeugte Folge?

Bestimme die erzeugende Funktion von

114. $1, 0, 0 \ldots; 0, 0, \ldots, 0, 1, 0, \ldots$ (1 im n-ten Platz).

115. $1, -1, 1, -1, 1, -1, \ldots$

116. $1, 0, 1, 0, 1, 0, \ldots$.

Löse die Differenzengleichungen

117. $a_0 = 1$, $a_{n+1} = 2a_n + 3$,

118. $a_0 = 2$, $a_1 = 3$, $a_{n+1} = 3a_n - 2a_{n-1}$,

119. $a_0 = 0$, $a_1 = 1$, $a_{n+2} = 4a_{n+1} - 4a_n$.

120. Was ist die erzeugende Funktion von $(1, 1, 2, 2, 4, 4, 8, 8, \ldots)$ bzw. $(1^2, 2^2, 3^2, 4^2, \ldots)$?

Lösungsvorschläge

Bsp. 111. $g(x) \sim a_0 + a_1 x + a_2 x^2 + \cdots$

$g(-x) \sim a_0 - a_1 x + a_2 x^2 + \cdots$

$\frac{1}{2}[g(x) + g(-x)] \sim a_0 + a_2 x^2 + a_4 x^4 + \ldots$ (d.h. die Folge $a_0, 0, a_2, 0, a_4, 0 \ldots$).

Bsp. 112. $(a_0, 0, 0, a_3, 0, 0, a_6)$. (Verwende dabei $1 + \omega + \omega^2 = 0$ und $\omega^3 = 1$.)

Bsp. 113. $(a_0, 0, 0, 0, a_4, 0, 0, 0, a_8, \ldots)$.

Bsp. 114. Die konstante Funktion 1;

die Funktion x^n.

Bsp. 115. $1 - x + x^2 - x^3 + \cdots \sim \dfrac{1}{1+x}$.

Bsp. 116. $(1, 1, 1, \ldots) \sim \dfrac{1}{1-x}$ — daher $\dfrac{1}{1-x^2}\left(= \dfrac{1}{2}\left(\dfrac{1}{1-x} + \dfrac{1}{1+x}\right)\right)$.

Bsp. 117. Sei $f(x) = a_0 + a_1 x + \cdots$

Es gilt

$$\sum_{n=0}^{\infty} a_{n+1} x^n = 2f(x) + 3\sum_{n=0}^{\infty} x^n = 2f(x) + \frac{3}{1-x}.$$

Also

$$\frac{f(x)-1}{x} = 2f(x) + \frac{3}{1-x}$$

— daher

$$\begin{aligned} f(x) &= \frac{1+2x}{(1-2x)(1-x)} = \frac{4}{1-2x} - \frac{3}{1-x} \\ &= 4(1 + 2x + (2x)^2 + \cdots + (2x)^n + \cdots) \\ &\quad -3(1 + x + \cdots + x^n + \cdots) \end{aligned}$$

Daher $a_n = 4 \cdot 2^n - 3$ (=Koeffizient von x^n in Entwicklung von $f(x)$).

Bsp. 118. $a_0 = 2$; $a_1 = 3$

$a_{n+2} = 3a_{n+1} - 2a_n$

$$\frac{f(x) - 2 - 3x}{x^2} = 3 \cdot \frac{f(x)-2}{x} - 2f(x) \Rightarrow f(x) = \frac{2-3x}{1-3x+2x^2} = \frac{1}{1-x} + \frac{1}{1-2x}$$

$$f(x) = \sum_{n=0}^{\infty} x^n + \sum_{n=0}^{\infty} 2^n x^n = \sum_{n=0}^{\infty} (1+2^n)n \Rightarrow \underline{a_n = 1 + 2^n}.$$

Bsp. 119. $a_0 = 0$, $a_1 = 1$

$a_{n+2} = 4a_{n+1} - 4a_n$

$$\sum_{n=0}^{\infty} a_{n+2} x^n = 4 \cdot \sum_{n=0}^{\infty} a_{n+1} x^n - 4 \cdot \sum_{n=0}^{\infty} a_n x^n, \text{ d.h. } \frac{f(x) - 0 - x}{x^2} = 4 \cdot \frac{f(x)-0}{x} - 4f(x)$$

$$f(x) = \frac{x}{(1-2x)^2} = -\frac{1}{2} \cdot \frac{1}{1-2x} + \frac{1}{2} \cdot \frac{1}{(1-2x)^2}$$

$$\frac{1}{1-2x} = \sum_{n=0}^{\infty} 2^n x^n; \frac{1}{(1-2x)^2} = \sum_{n=0}^{\infty} (n+1) \cdot 2^n \cdot x^n$$

$$f(x) = \sum_{n=0}^{\infty} ((n+1)2^{n-1} - 2^{n-1}) x^n = \sum_{n=0}^{\infty} n \cdot 2^{n-1} x^n \Rightarrow \underline{a_n = n \cdot 2^{n-1}}.$$

Bsp. 120. $(1, 1, 2, 2, 4, 4, 8, 8, \ldots)$

$$\begin{aligned} f(x) &= 1 + x + 2x^2 + 2x^3 + 4x^4 + 4x^5 + 8x^6 + 8x^7 + \ldots \\ f(x) &= \sum_{n=0}^{\infty} 2^n (x^{2n} + x^{2n+1}) = (1+x) \cdot \sum_{n=0}^{\infty} (2 \cdot x^2)^n = \underline{\frac{1+x}{1-2x^2}} \end{aligned}$$

$(1^2, 2^2, 3^2, 4^2, \dots)$

$$\begin{aligned} f(x) &= \sum_{n=0}^{\infty} n^2 x^n = \sum_{n=1}^{\infty} (n-1)^2 x^{n-1} = \sum_{n=1}^{\infty} n^2 x^{n-1} - 2\sum_{n=1}^{\infty} n x^{n-1} + \sum_{n=1}^{\infty} x^{n-1} \\ &= \frac{1}{x} \cdot \sum_{n=1}^{\infty} n^2 x^n - 2\sum_{n=0}^{\infty} (n+1) x^n + \sum_{n=0}^{\infty} x^n = \frac{1}{x} \sum_{n=0}^{\infty} n^2 x^n - \frac{2}{(1-x)^2} + \frac{1}{1-x} \\ &\Rightarrow \quad \underline{f(x) = \frac{x(1+x)}{(1-x)^3}}. \end{aligned}$$

Übungsblatt 12

Thema: Erzeugende Funktionen
Bestimme den Koeffizienten von x^n in

121. e^{2x}

122. $\frac{1}{(1-ax)(1-bx)} \quad (a \neq b)$

123. $(1+x^2)^m$.

Bestimme die erzeugenden Funktionen der Folgen:

124. (n), $(\alpha n + \beta)$

125. (n^2), $(\alpha n^2 + \beta n + \gamma)$

126. (3^n), $(5 \cdot 7^n - 3 \cdot 4^n)$.

127. Was ist $\sum_{k=1}^{n} k^2$?

128. Bestimme die erzeugende Funktion von $(F_1, 2F_2, 3F_3, 4F_4, \dots)$, wobei F_n die Fibonacci-Zahlen aus dem Skriptum (Seite 58) sind.

Bestimme b_0, b_1, b_2, falls

129. $\frac{1}{\cos x} = b_0 + b_1 x + b_2 x^2 + \cdots$

130. $\frac{1}{(1+x)^m} = b_0 + b_1 x + b_2 x^2 + \cdots$

Lösungsvorschläge

Bsp. 121.

$$e^{2x} = \sum_{n=0}^{\infty} \frac{(2x)^n}{n!} = \sum_{n=0}^{\infty} \frac{2^n}{n!} x^n, \quad \text{d.h.} \quad \underline{a_n = \frac{2^n}{n!}}$$

Bsp. 122.

$$\frac{1}{(1-ax)(1-bx)} = \frac{a}{(a-b)} \cdot \frac{1}{1-ax} - \frac{b}{a-b}\frac{1}{(1-bx)}$$
$$= \frac{a}{a-b} \sum_{n=0}^{\infty} (ax)^n - \frac{b}{a-b} \sum_{n=0}^{\infty} (bx)^n = \sum_{n=0}^{\infty} \frac{a^{n+1} - b^{n+1}}{a-b} x^n$$

d.h.

$$\underline{a_n} = \frac{a^{n+1} - b^{n+1}}{a-b} = \underline{\sum_{k=0}^{\infty} a^{n-k} b^k}.$$

Bsp. 124.

$$\sum_{n=1}^{\infty} n \cdot x^n = x \cdot \sum_{n=1}^{\infty} n \cdot x^{n-1} = x \cdot \sum_{n=1}^{\infty} (n+1) x^n = \underline{\frac{x}{(1-x)^2}}$$

$$\sum_{n=0}^{\infty} (\alpha n + \beta) x^n = \sum_{n=0}^{\infty} \beta x^n + \alpha \cdot \sum_{n=1}^{\infty} n \cdot x^n = \underline{\frac{\beta}{1-x} + \frac{\alpha \cdot x}{(1-x)^2}}$$

Bsp. 125.

$$\sum_{n=0}^{\infty} n^2 x^n = \sum_{n=1}^{\infty} n^2 x^n = \frac{x(1+x)}{(1-x)^3} \quad \text{nach Bsp. 120}$$

$$\begin{aligned}\sum_{n=0}^{\infty}(\alpha n^2+\beta n+\gamma)x^n &= \alpha\cdot\frac{x(1+x)}{(1-x)^3}+\beta\cdot\frac{x}{(1-x)^2}+\gamma\cdot\frac{1}{1-x}\\ &= \underline{\frac{\alpha\cdot x(1+x)+\beta\cdot x(1-x)+\gamma(1-x)^2}{(1-x)^3}}\end{aligned}$$

Bsp. 126.

$$\begin{aligned}\sum_{n=0}^{\infty} 3^n x^n = \sum_{n=0}^{\infty}(3x)^n &= \underline{\frac{1}{1-3x}}\\ \sum_{n=0}^{\infty}(5\cdot 7^n - 3\cdot 4^n)x^n &= \underline{\frac{5}{1-7x}-\frac{3}{1-4x}}\end{aligned}$$

Bsp 127. Sei

$$c_n = \sum_{k=1}^{n} k^2 = \sum_{k=0}^{n} k^2$$

$\Rightarrow c_n = a_n b_0 + \cdots + a_0 b_0$ mit $a_i = 1$, $b_i = i^2$ für $i = 0, \ldots, n$

$\Rightarrow$ (vgl. Skriptum S. 57)

$$\sum_{n=0}^{\infty} c_n x^n = \left(\sum_{n=0}^{\infty} a_n x^n\right)\cdot\left(\sum_{n=0}^{\infty} b_n x^n\right) = \left(\sum_{n=0}^{\infty} x^n\right)\cdot\left(\sum_{n=0}^{\infty} n^2 x^n\right) = \frac{1}{1-x}\cdot\frac{x(1+x)}{(1-x)^3} = \frac{x(1+x)}{(1-x)^4}$$

Partialbruchzerlegung:

$$\frac{x(1+x)}{(1-x)^4} = \frac{1}{(1-x)^2}-\frac{3}{(1-x)^3}+\frac{2}{(1-x)^4} = \sum_{n=0}^{\infty}\left(\binom{n+1}{n}-3\binom{n+2}{n}+2\binom{n+3}{n}\right)x^n$$

$$\begin{aligned}\Rightarrow c_n &= \binom{n+1}{n}-3\binom{n+2}{n}+2\binom{n+3}{n} = n+1-\frac{3}{2}(n+2)(n+1)+\frac{1}{3}(n+3)(n+2)(n+1)\\ &= \frac{1}{6}(n+1)(1-9(n+2)+2(n+2)(n+3)) = \frac{1}{6}(n+1)(2n^2+n) = \underline{\frac{1}{6}n(n+1)(2n+1).}\end{aligned}$$

Bsp. 129.

$$\begin{aligned}1 &= \cos x(b_0+b_1x+b_2x^2+\ldots)\\ &= (1-\frac{x^2}{2}+\frac{x^4}{24}-\frac{x^6}{6!}+\cdots)(b_0+b_1x+b_2x^2+\cdots)\end{aligned}$$

Koeffizientenvergleich:

$$\left.\begin{aligned}1 &= b_0\\ 0 &= b_1\\ 0 &= b_2-\tfrac{1}{2}b_0 = b_2-\tfrac{1}{2}\end{aligned}\right\} \Rightarrow \underline{b_0=1, b_1=0, b_2=\frac{1}{2}}$$

Bsp. 130.

$$\begin{aligned} 1 &= (1+x)^m \cdot (b_0 + b_1 x + b_2 x^2 + \cdots) \\ &= \sum_{n=0}^{m} \binom{m}{n} x^n (b_0 + b_1 x + b_2 x^2 + \cdots) \\ &= (b_0 + b_1 x + b_2 x^2 + m b_0 x + m b_1 x^2 + m b_2 x^3 + \binom{m}{2} b_0 x^2 + \cdots \end{aligned}$$

Koeffizientenvergleich:

$$0 = b_1 + m b_0 = b_1 + m \Rightarrow \underline{b_1 = -m}$$

$$0 = b_2 + m b_1 + \binom{m}{2} b_0 \Rightarrow b_2 = -m b_1 - \binom{m}{2} b_0 = m^2 - \frac{1}{2}(m^2 - m) = \underline{\frac{1}{2}(m^2 + m)}.$$

Übungsblatt 13

Thema: Erzeugende Funktionen
Bestimme b_1, b_2, falls

131. $\sin y = x$

132. $\tan y = x$

133. $y + y^2\sqrt{1+y} = x$

134. $y + y^3 = x$

wobei $y = b_1x + b_2x^2 + b_3x^3 + \cdots$.

Bruchzerlegungen:

135. $\frac{x+1}{(x-1)(x+2)}$;

136. $\frac{1}{(x+1)(x^2+2)}$;

137. $\frac{x^2+4}{(x+1)^2(x-2)(x+3)}$.

Löse die Differenzengleichungen:

138. $y_{n+2} - 2y_{n+1} + 2y_n = 1$, $y_0 = 1$, $y_1 = 1$;

139. $4y_{n+2} + 12y_{n+1} - 7y_n = 35$, $y_0 = 6$, $y_1 = 3$.

140. Falls $f'' + f = 0$, zeige $f(x) = A\cos x + B\sin x$.

Lösungsvorschläge

Bsp. 131. $\sin y = y - \frac{y^3}{y!} + \cdots$, also

$$\sin y = (b_1x + b_2x^2 + b_3x^3 + \cdots) - \frac{1}{6}(b_1x + b_2x^2 + b_3x^3 + \cdots)^3 + \cdots = x$$

Koeffizientenvergleich: $\Rightarrow \underline{b_1 = 1, b_2 = 0}$.

Bsp. 132. $\tan y = y + \frac{y^3}{y} + \frac{2}{5}y^5 + \cdots$, also

$$\tan y = (b_1x + b_2x^2 + b_3x^3 + \cdots) + (b_1x + b_2x^2 + \cdots)^3/3 + \cdots = x$$

Koeffizientenvergleich: $\Rightarrow \underline{b_1 = 1, b_2 = 0}$.

Bsp. 133. $\sqrt{1+y} = 1 + \frac{1}{2}y - \frac{1}{8}y^2 + \cdots$, also

$$y + y^2 \cdot \sqrt{1+y}(b_1x + b_2x^2 + \cdots) + (b_1x + \cdots)^2(1 + \frac{1}{2}(b_1x + \cdots) - \frac{1}{8}(b_1x + \cdots)^2 + \cdots) = x$$

Koeffizientenvergleich: $\underline{b_1 = 1, b_2 = -1}$.

Bsp. 134. $y + y^3 = x$, also

$$(b_1x + b_2x^2 + \cdots) + (b_1x + \cdots)^3 = x$$

Koeffizientenvergleich: $\underline{b_1 = 1, b_2 = 0}$.

Bsp. 135.

$$\frac{x+1}{(x-1)(x+2)} = \frac{A}{x-1} + \frac{B}{x+2} = \frac{Ax + 2A + Bx - B}{(x-1)(x+2)} \Rightarrow$$

Koeffizientenvergleich: $1 = 2A - B \Rightarrow \underline{\frac{2}{3} = A}$

$1 = A + B \Rightarrow \underline{\frac{1}{3} = B}$.

Bsp. 137.

$$\frac{x^2+4}{(x+1)^2(x-2)(x+3)} = \frac{A}{x+1} + \frac{B}{(x+1)^2} + \frac{C}{x-2} + \frac{D}{x+3}$$

$$= \frac{A(x+1)(x-2)(x+3) + B(x-2)(x+3) + C(x+1)^2(x+3) + D(x-2)(x+1)^2}{(x+1)^2(x-2)(x+3)}$$

Koeffizientenvergleich: $\underline{A = \frac{17}{36}; B = -\frac{5}{6}; C = \frac{8}{45}; D = -\frac{13}{20}}$.

Bsp. 138. $f(x) = \sum_{n=0}^{\infty} y_n x^n$

$$\sum_{n=0}^{\infty} y_{n+2}x^n - 2\sum_{n=0}^{\infty} y_{n+1}x^n + 2\sum_{n=0}^{\infty} y_n x^n = \sum_{n=0}^{\infty} x^n; \quad y_0 = 1; y_1 = 1.$$

Wir benützen die Formeln im Skriptum (Seite 57) und erhalten:

$$\frac{f(x) - 1 - x}{x^2} - 2\frac{f(x) - 1}{x} + 2 \cdot f(x) = \frac{1}{1-x}$$

$$f(x)\left(\frac{1}{x^2} - \frac{2}{x} + 2\right) = \frac{1}{1-x} + \frac{1}{x^2} + \frac{1}{x} - \frac{2}{x} = \frac{x^2 + 1 - x - x + x^2}{x^2(1-x)}$$

$$f(x) = \frac{2x^2 - 2x + 1}{(1-x)(1-2x+2x^2)} = \frac{1}{1-x} \Rightarrow \underline{y_n = 1 \text{ für } n = 0, 1, 2, \ldots}$$

Weitere Beispiele

139. Beweisen Sie das Assoziativgesetz der Addition natürlicher Zahlen: Für alle natürlichen Zahlen m, n, r gilt
$$(m + n) + r = m + (n + r).$$

140. Beweisen Sie das Kommutativgesetz der Addition und Multiplikation natürlicher Zahlen (vgl. Bsp. 15, Skriptum, Seite 65): Für alle natürlichen Zahlen m, n gilt
$$m + n = m + n, \qquad m * n = n * m$$

141. Zeigen Sie: Für alle natürlichen Zahlen ist $n^3 + 2n$ durch 3 teibar.

142. a) Stellen Sie die Zahlen 105 und 52 dyadisch dar und berechnen Sie dyadisch ihre Summe und ihr Produkt.

b) Drücken Sie das Produkt hexadezimal aus.

143. a) Sei 15E01 die Hexadezimaldarstellung einer Zahl n. Finden Sie für n die dyadische und die dezimale Darstellung.

b) Stellen Sie 1.098.522 hexadezimal dar.

144. Zeigen Sie

$$1 + 2^2 + 3^2 + \cdots n^2 = \sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1).$$

145. Sei $a_1, a_2, a_3, \ldots$ eine Folge von (reellen) Zahlen. Wir definieren damit zwei neue Folgen:

$$s_1 := a_1, \qquad s_n := s_{n-1} + a_n$$
$$\pi_1 := a_1, \qquad \pi_n := \pi_{n-1} * a_n$$

Schreiben Sie explizit die ersten 5 Glieder der neuen Folgen an.

146. Was soll ein Computer tun, wenn er zu den Punkten in folgender "Summe" kommt? $1 + 4 + 9 + \cdots$

147. Die Folge p_n sei rekursiv definiert durch $p_0 = 1, \quad p_n = p_{n-1} + n$. Finden Sie eine Formel für p_n und beweisen Sie diese (z.B. durch Induktion).

148. Zu zwei reellen Zahlen a, b bezeichne $\max(a, b)$ die größere der beiden Zahlen (also etwa $\max(3, 5) = \max(5, 3) = 5, \quad \max(7, 7) = 7$). Was sagen Sie zu folgendem "Beweis" der Behauptung, daß alle natürlichen Zahlen gleich sind: Wir zeigen dazu induktiv die Gültigkeit der folgenden Aussage $A(n)$: Wenn für $a, b \in \mathbf{N}$ $\max(a, b) = n$, dann ist $a = b$.

$A(1)$ ist offenbar richtig (aus $\max(a, b) = 1$ und $a, b \in \mathbf{N}$ folgt $a = b = 1$). Gelte nun $A(n)$ für $a, b \in \mathbf{N}$ und sei $\max(a, b) = n+1$. Dann gilt für $\alpha := a-1, \beta := b-1$ $\max(\alpha, \beta) = n$, woraus wegen der angenommenen Gültigkeit von $A(n)$ folgt: $\alpha = \beta$ und daher $a = b$.

149. Geben Sie die Wahrheitstabelle für das *ausschließende Oder* an.

150. Für welche Belegungen von p, q, r ist die Aussageform

$$(\neg p \wedge q) \Rightarrow (r \wedge q)$$

falsch? Geben Sie Warheitstabelle an.

151. Eine Aussageform $p(x, y, z)$ in den Aussagevariablen x, y, z sei durch folgende Wahrheitstabelle festgelegt:

x	W	W	W	F	W	F	F	F
y	W	W	F	W	F	W	F	F
z	W	F	W	W	F	F	W	F
p	W	W	W	W	F	F	F	F

Stellen Sie p durch $\wedge, \vee, \neg$ dar.

152. Zeigen Sie, daß die Aussageform

$$p(x,y) := \big(x \wedge (x \Rightarrow y)\big) \Rightarrow y$$

eine Tautologie ist. (Es ist die dem *modus ponens* zu Grunde liegende Tautologie)

153. Zeigen Sie, daß die Aussageform

$$p(x,y) := \big((x \Rightarrow y)) \wedge (x \Rightarrow \neg y)\big) \Rightarrow \neg x$$

eine Tautologie ist. (Es ist die der *reductio ad absurdum* zu Grunde liegende Tautologie)

154. Zeigen Sie, daß die Aussageform

$$p(x,y) := \big((x \Rightarrow y)) \wedge (x \Rightarrow \neg y)\big) \Rightarrow \neg x$$

eine Tautologie ist. (Es ist die der *reductio ad absurdum* zu Grunde liegende Tautologie)

155. Aus: LOGELEIEN VON ZWEISTEIN

1. Willi sagt: *Herbert lügt*
2. Herbert sagt: *Otto lügt*
3. Otto sagt: *Willi und Herbert lügen*

Wer lügt nun wirklich? Versuchen Sie einen inirekten Beweis.

156. Die Aussagen A, B seien definiert durch
A := *Es gibt hier Haie.*
B := *Es ist mir hier zu gefährlich.*

Versuchen Sie Aussageformen in A,B zu formulieren, die folgenden Sätzen zu Grunde liegen:

a) Es ist nicht wahr, daß es hier Haie gibt.
b) Weil es hier Haie gibt, ist es mir hier zu gefährlich.
c) Obwohl es hier Haie gibt, ist es mir hier nicht zu gefährlich.

157. a) Zeigen Sie die 2. De MORGAN'sche Regel:

$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$

b) Zeigen Sie das 2. Distributivgesetz:

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

158. Bilden Sie die Negation der Aussage

$$\bigwedge_{n \in \mathbf{N}} \bigvee_{p \in \mathbf{P}} \quad n \leq p \leq n^2$$

Welche der beiden Aussagen ist wahr?

159. Zeigen Sie: Die Addition zweier natürlicher Zahlen m, n erfordert eine Rechenzeit $O(\max(\log m, \log n))$.

160. Welche der folgenden Ausdrücke ist eine Aussage? Welche ist wahr, falsch?

a) $2x - 1 = 3$

b) $(x+1)^2 = x^2 - 2x + 1$

c) $\bigwedge_{x \in \mathbf{R}} 2x - 1 = 4$

d) $\bigvee_{x \in \mathbf{R}} 2x - 1 = 4$, $\bigvee_{x \in \mathbf{N}} 2x - 1 = 4$

e) $\bigwedge_{x \in \mathbf{R}} (x+1)^2 = x^2 + 2x + 1$

f) $2x - 1$

g) $x^3 + y^3 = 725$

h) $a^2 + b^2 = c^2$

Wie können Sie a, b, c interpretieren, damit aus der letzten Zeile ein altbekannter Satz der Geometrie entsteht?

Welche der vorhergehenden Zeilen kann durch Angabe eines Grundbereiches zu einer Aussageform gemacht werden?

161. Drücken Sie die folgenden Aussagen mit Quantoren aus:

a) 12 ist nicht die größte ganze Zahl.
b) Es gibt keine größte ganze Zahl.
c) Zwischen je zwei rationalen Zahlen liegt eine dritte.

162. Bezeichne M die gesamte Menschheit und $L(x, y)$ das 2–stellige Prädikat "x liebt y".

Lesen Sie folgende Ausagen exakt und umgangsprachlich:

a) $\left(\bigvee_x\right)\left(\bigvee_y\right) \quad L(x, y)$
b) $\left(\bigwedge_x\right)\left(\bigvee_y\right) \quad L(x, y)$
c) $\left(\bigwedge_y\right)\left(\bigvee_x\right) \quad L(x, y)$
d) $\left(\bigvee_y\right)\left(\bigwedge_x\right) \quad L(x, y)$
e) $\left(\bigvee_x\right)\left(\bigwedge_y\right) \quad L(x, y)$
f) $\left(\bigwedge_x\right)\left(\bigwedge_y\right) \quad L(x, y)$

163. Bilden Sie die Negationen der Aussagen a) – f) der vorigen Aufgabe.

164. In der Menge $\mathbf{R}$ der reellen Zahlen finden Sie mindestens ein je 1–,2–,3–,4–,5– stelliges Prädikat.

165. Widerlegen Sie durch ein Gegenbeispiel die Behauptung $\bigwedge_a \bigvee_b A(a, b) \equiv \bigvee_b \bigwedge_a A(a, b)$.

166. Bestimmen Sie

a) die Potenzmenge der Menge $\mathcal{A} = \{A, B, C, D\}$.
b) das kartesische Produkt von $\mathcal{A}$ und $\mathcal{B} = \{0, 1, 2\}$.
c) Wieviele 2–elementige Teilmengen von $\mathcal{A}$ gibt es?

167. a) Wieviele Aussageformen in 2 Variablen gibt es? (16)
b) Schreiben Sie alle Aussageformen in 2 Variablen an.

168. a) Zeigen Sie: $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.
b) Zeigen Sie an einem Gegenbeispiel, daß $(p \Rightarrow q)$ im allgemeinen verschieden ist von $(\neg p \Rightarrow \neg q)$.

169. Seien A, B Teilmengen einer Menge M, bezüglich der A', B' das Komplement von resp. A, B bezeichne. Zeigen Sie die de MORGAN'schen Gesetze für Durchschnitt und Vereinigung:
$$(A \cup B)' = A' \cap B', \quad (A \cap B)' = A' \cup B'.$$

170. Für endliche Mengen X bezeichne $|X|$ die Anzahl der Elemente von X. Seien A, B endliche Mengen. Zeigen Sie (z.B. durch Induktion)
$$|A \times B| = |A||B|, \quad |\mathcal{P}(A) = 2^{|A|}.$$

171. A, B seien Mengen. Zeigen Sie: $\big(A = B\big) \Leftrightarrow \big(A \subset B \wedge B \subset A.\big)$

172. Bestimmen Sie von den folgenden komplexen Zahlen jeweils Real– und Imaginärteil sowie den Absolutbetrag:
$\frac{i-1}{i+1}$; $\frac{3+4i}{1-2i}$; $\left(\frac{1+i}{\sqrt{2}}\right)^n (n \in \mathbf{Z})$; $i^{4711} \quad -3+i$; $(1+i)^{17} - (1-i)^{17}$

173. Für $z_1 = 1 - i$, $z_2 = -2 + 4i$ berechnen Sie folgende Ausdrücke:
$z_1^2 + 2z_1 - 3$; $|2z_2 - 3z_1|^2$; Im $(z_1 + z_2 - 1)/(z_1 - z_2 + i)$.

174. Bestimmen Sie für die Abbildung $F : \mathbf{C} \to \mathbf{C}$, definiert durch $F(z) = z^2 - 2$ die Ausdrücke
$F^2(2)$, $F^3(2)$, $F^4(2)$, $\ldots$, $F^n(2)$.
Was ist $F^2(1)$, $F^3(-1)$?

175. Wieviele bijektive Abbildungen gibt es zwischen
a) $A = \{a, b\}$ und $B = \{1, 2\}$?
b) $A = \{a, b, c\}$ und $B = \{1, 2, 3\}$?
c) $A = \{a, b, c, d\}$ und $B = \{1, 2, 3, 4\}$?
d) $A = \{1, 2, 3, 4\} = B$?
Erkennen Sie eine allgemeine Formel?

176. a) Sei $f(x) = x/2 + 1/x$. Bestimmen Sie die größtmögliche Teilmenge $A \subset \mathbf{R}$, die als Definititonsbereich für f in Frage kommt.
b) Bestimmen Sie die Fixpunkte von f.

177. a) Zeichnen Sie eine Skizze des Graphen der Funktion f der vorigen Aufgabe.
b) Wo läßt sich die Funktion umkehren. Finden Sie geeignete Einschränkungen des Definitionsbereiches von f.

178. $f : \mathbf{R} \to \mathbf{R}$ sei definiert durch
$$f(x) = \begin{cases} x/3 & (x \leq 1) \\ 5(x-1) + 1/3 & (x > 1) \end{cases}$$
a) Zeichnen Sie das Schaubild von f.
b) Ist die Funktion umkehrbar (bijektiv)? Wenn ja, bestimmen Sie die Umkehrfunktion graphisch und rechnerisch.

179. Bestimmen Sie die Fixpunkte der Abbildungen $f(x) = \frac{1}{2}(x + \frac{1}{x})$ und $g(x) = x^2 - x + 1$.

180. Zeigen Sie mit Modularithmetik: für alle $n \in \mathbf{N}$ gilt $3|2n + n^3$.

181. Zeigen Sie folgende Aussagen:

$$a \equiv b \pmod{m} \quad \Rightarrow \quad ggT(a, m) = ggT(b, m)$$
$$a \equiv b \pmod{m}, \quad 0 \leq |b - a| < m \quad \Rightarrow \quad a = b$$
$$a \equiv b \pmod{m}, \quad a \equiv b \pmod{n}, \quad ggT(m, n) = 1 \quad \Rightarrow \quad a \equiv b \pmod{mn}$$