Diskrete Algebraische Strukturen

Markus Junker
Universität Freiburg

Sommersemester 1999

Inhaltsverzeichnis

Teil I: Endliche Kombinatorik

Problem: wieviel Objekte einer gewissen Art gibt es in Abhängigkeit von einer oder mehreren Größen? Etwa: wieviel Kohlenwasserstoffe, wieviele Alkohole mit n Kohlenstoffatomen? wieviel Kaninchen (oder Computerviren) in der n-ten Generation? wieviele Primzahlen $\leqslant n$? Wieviele Möglichkeiten, $a_1 + \cdots + a_n$ zu klammern?

Zu berechnen ist also eine Funktion $f : \mathbb{N} \to \mathbb{N}$. Mehrere Lösungsarten sind möglich. Etwa in absteigender Güte sind dies:

(1) eine explizite Formel für $f(n)$ mit wenig/viel Rechenaufwand;

(2) eine Rekursionsformel für $f(n+1)$ in Abhängigkeit von $f(0), \dots, f(n)$;

(3) eine Formel für die erzeugende Funktion $F(x) = \sum f(n)x^n$;

(4) Schranken für das asymptotisches Verhalten: "wie schnell wächst f für $n \to \infty$" (dies ist vor allem wichtig bei Komplexitätsbetrachtungen).

I.1 Mengen, Abbildungen, Partitionen

Voraussetzungen: "naive Mengenlehre". Kurze Zeichenerklärung:

$\mathbb{N}$	die Menge $\{0, 1, 2, 3, \dots\}$
$A \subseteq M$	A ist Teilmenge von M.
$A \subset M$	A ist echte Teilmenge von M.
$M = \dot{\bigcup}_{i \in I} M_i$	M ist die disjunkte Vereinigung der M_i; ähnlich $A \dot{\cup} B$.
$\lvert M \rvert$	die Anzahl der Elemente von M, auch <u>Mächtigkeit</u> von M genannt. $\lvert M \rvert$ ist entweder ein Element von $\mathbb{N}$ oder ∞.
$M \simeq N$	M ist in Bijektion mit N (keine Standardnotation).
$\boxed{\text{Text}}$	enthält Hinweise zu Beweisen.

Seien in der Folge M, N endliche Mengen mit $\lvert M \rvert = m$ und $\lvert N \rvert = n$. Sprechweise um der Einfachheit willen: M ist m-Menge, N ist n-Menge. (Ähnlich: K ist k-Teilmenge von M.)

Satz 1.1 (Additive Mächtigkeitsregeln)

(a) *Angenommen* $M \subseteq N$. *Dann gilt* $m \leqslant n$*;* $M \subset N \iff m < n$ *und* $|N \setminus M| = n - m$.

(b)

$$\max\{m, n\} \leqslant |M \cup N| \leqslant n + m$$
$$0 \leqslant |M \cap N| \leqslant \min\{m, n\}$$
$$\max\{m, n\} = |M \cup N| \iff |M \cap N| = \min\{m, n\} \iff (M \subseteq N \textit{ oder } N \subseteq M)$$
$$|M \cup N| = n + m \iff 0 = |M \cap N| \iff M, N \textit{ disjunkt}$$

(c) *Allgemeiner:* $\left|\dot{\bigcup}_{i=0}^{k} M_i\right| = \sum_{i=0}^{k} |M_i|$.

(d) $|M| + |N| = |M \cup N| + |M \cap N|$

Übung: Welche der Rechenregeln machen Sinn für unendliche Mengen?

Punkt (d) kann man verallgemeinern zu

Satz 1.2 (Prinzip der Inklusion–Exklusion oder Sylvestersche Siebformel)
Seien $M_1, \ldots, M_k$ *endliche Mengen. Dann gilt:*

$$\left|M_1 \cup \cdots \cup M_k\right| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,k\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} M_i\right|$$

Setzt man $\bigcap_{i\in\emptyset} M_i = M_1 \cup \cdots \cup M_k$ (was Sinn macht, falls man etwa in der Booleschen Algebra $\mathfrak{P}(M_1 \cup \cdots \cup M_k)$ arbeitet), so ergibt sich die einprägsamere Formel:

$$\sum_{I \subseteq \{1,\ldots,k\}} (-1)^{|I|} \cdot \left|\bigcap_{i \in I} M_i\right| = 0$$

Satz 1.3 (Multiplikative Mächtigkeitsregeln)

(a) $|M \times N| = mn$.

(b) *Allgemeiner:* $|M_1 \times \cdots \times M_k| = |M_1| \cdots |M_k|$.

(c) *Insbesondere:* $|M^k| = m^k$, *wobei* $M^n := \underbrace{M \times \cdots \times M}_{n \textit{ mal}}$, *also* $M^1 := M$ *und* $M^0 = \{\emptyset\}$.

Abbildungen

Definition 1.1

$$\left.\begin{array}{r} \mathrm{Abb}(M,N) = {}^{M}N \\ \mathrm{Inj}(M,N) \\ \mathrm{Surj}(M,N) \\ \mathrm{Bij}(M,N) \end{array}\right\} \textit{sei die Menge aller} \left\{\begin{array}{l} \textit{Abbildungen (Funktionen)} \\ \textit{Injektionen} \\ \textit{Surjektionen} \\ \textit{Bijektionen} \end{array}\right\} f : M \to N$$

Dabei heißt $f : M \to N$ *<u>injektiv</u> falls* $f(m) \neq f(m')$ *für alle* $m, m' \in M$ *mit* $m \neq m'$*;*
f *heißt <u>surjektiv</u>, falls es zu jedem* $n \in N$ *ein* $m \in M$ *mit* $f(m) = n$ *gibt;*
f *heißt <u>bijektiv</u>, falls* f *injetiv und surjektiv ist.*

Satz 1.4 *Sei* $f : M \to N$ *gegeben.*

(a) *Ist* f *bijektiv, so* $|M| = |N|$.

(b) *Ist* f *surjektiv, so* $|M| \geqslant |N|$*; für endliches* M *gilt dann* $|M| = |N| \iff f$ *bijektiv.*

(c) *Ist* f *injektiv, so* $|M| \leqslant |N|$*; für endliches* N *gilt dann* $|M| = |N| \iff f$ *bijektiv.*

Teil (c) ergibt umformuliert das sogenannte <u>Schubfachprinzip</u>:

Satz 1.5 (Schubfachprinzip) *Ist* $f : M \to N$ *gegeben und* $|M| > |N|$*, so gibt es* $m, m' \in M$ *mit* $m \neq m'$ *und* $f(m) = f(m')$.

Allgemeiner: für $k := \lceil \frac{|M|}{|N|} \rceil$ *gibt es eine* k*-Teilmenge von* M*, auf der* f *konstant ist.*

Hierbei ist $\lceil r \rceil :=$ die kleinste ganze Zahl, die nicht kleiner als r ist ("<u>obere Gaußklammer</u>") und $\lfloor r \rfloor :=$ die größte ganze Zahl, die nicht größer als r ist ("<u>untere Gaußklammer</u>").

Satz 1.6 (Exponentielle Mächtigkeitsregeln)

(a) $|\mathrm{Abb}(M, N)| = |{}^M N| = n^m$

(b) *Spezialfall:* $|\mathfrak{P}(M)| = 2^m$*, da* $\mathfrak{P}(M) \simeq {}^M\{0, 1\}$.

(c) *Spezialfall:* $|M^k| = m^k$*, da* $M^k \simeq {}^{k\text{-}Menge}M$.

Frage: Wieviele Injektionen, Surjektionen, Bijektionen von M nach N? Man kann sich leicht überlegen, daß dies nur von $|M|$ und $|N|$ abhängt, nicht von der speziellen Wahl der Mengen.

Satz 1.7

$$\begin{aligned} \left|\mathrm{Abb}(M,N)\right| &= n^m \\ \left|\mathrm{Bij}(M,N)\right| &= n! \ \textit{falls}\ m = n; \quad = 0 \ \textit{sonst} \\ \left|\mathrm{Inj}(M,N)\right| &= n(n-1)\cdots(n-m+1) = m! \cdot \binom{n}{m} \\ \left|\mathrm{Surj}(M,N)\right| &= \sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^m = n! \cdot S_{m,n} \end{aligned}$$

Satz 1.8

$$n^m = \sum_{j=0}^{m} \binom{n}{j} \cdot j! \cdot S_{m,j} \qquad \boxed{\textit{jede Abbildung ist surjektiv auf ihr Bild}}$$

$$n! = \sum_{j=0}^{n} (-1)^j \binom{n}{j} \cdot (n-j)^n \qquad \boxed{\textit{nach Formel für surjektive Abb. } N \to N}$$

Teilmengen und Binomialkoeffizienten

Jede Injektion $K \to M$ entspricht einer k-Teilmenge von M mit einer Aufzählung. Folglich gilt $\left|\mathrm{Inj}(K, M)\right| = \left|\mathrm{Bij}(K, K)\right| \cdot \left|k\text{-Teilmengen von } M\right| = k! \cdot \binom{m}{k}$.

Definition 1.2 *Sei* M m*-Menge. Die Anzahl der* k*-Teilmengen von* M *heiße* $\binom{m}{k}$*, der sogenannte* <u>*Binomialkoeffizienten "*m *über* k*"*</u>*. (Hängt nur von* $|M|$ *und* k *ab!)*

Satz 1.9 (Eigenschaften der Binomialkoeffizienten)

Explizite Formel:

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} = \frac{m(m-1)\cdots(m-k+1)}{k!} = \frac{m}{k}\cdot\frac{m-1}{k-1}\cdots\frac{(m-k+1)}{1}$$

einige konkrete Werte:

$$\binom{m}{k} = 0 \quad \textit{für } k > m \qquad \binom{m}{0} = \binom{m}{m} = 1 \qquad \binom{m}{1} = \binom{m}{m-1} = m$$

$$\binom{m}{k} = \binom{m}{m-k}$$ Komplement

Rekursionsformel:

$$\binom{m+1}{k} = \binom{m}{k-1} + \binom{m}{k} \quad \textit{für } k > 0$$ einen Punkt in Gesamtmenge aussondern

$$k\binom{m}{k} = m\binom{m-1}{k-1} = (m-k+1)\binom{m}{k-1}$$ einen Punkt in k-Teilmenge auszeichnen

Summenformel:

$$\sum_{k=0}^{m}\binom{m}{k} = 2^m$$ ganz $\mathfrak{P}(M)$

Aus der Rekursionsformel ergibt sich das sogenannte Pascalsche Dreieck:

m							$k=$	0						2^m
0							1		1					1
1						1		1		2				2
2					1		2		1		3			4
3				1		3		3		1		4		8
4			1		4	+	6		4		1			16
5		1		5		10		10		5		1		32
6	1		6		15		20		15		6		1	64

Satz 1.10 (Binomischer Satz)

$$(x+y)^m = \sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} \qquad \textit{für } x, y \in \mathbb{C}, m \in \mathbb{N}$$

Es gibt auch sogenannte Polynomialkoeffizienten (auch Multinomialkoeffizienten genannt):

$$\binom{m}{k_1, \ldots, k_r} := \frac{m!}{k_1! \cdots k_r!},$$

wobei stets $k_1 + \cdots + k_r = m$ gelten soll. Speziell ist also $\binom{m}{k} = \binom{m}{k, m-k}$. Die Polynomialkoeffizienten kann man auch kombinatorisch definieren als die Menge der Abbildungen einer m-Menge M nach $\{1, \ldots, r\}$, wobei genau k_j Elemente auf j abgebildet werden. Es gilt dann der

Satz 1.11 (Polynomischer Satz)

$$(x_1 + \cdots + x_r)^m = \sum_{k_1+\cdots+k_r=m} \binom{m}{k_1, \ldots, k_r} \cdot x_1^{k_1} \cdot x_2^{k_3} \cdots x_r^{k_r} \qquad \textit{für } x_i \in \mathbb{C}, m \in \mathbb{N}$$

Man kann diesen Satz per Induktion nach n und r beweisen. Hübscher ist der kombinatorische Beweis: für natürliche Zahlen x_i steht links die Anzahl der Abbildungen einer m-Menge in die disjunkte Vereinigung von x_i-Mengen; rechts dagegen die Anzahl der Möglichkeiten, m in r Stücke der Größe k_i aufzuteilen und Abbildungen einer k_i-Menge in eine x_i-Menge zu betrachten. Beide Zahlen sind offenbar gleich. Für beliebige komplexe Zahlen x_i folgert man mit Hilfe des Identitätssatzes für Polynome.

Mengenpartitionen und Stirling–Zahlen zweiter Art

Definition 1.3 *Eine* k-*Partition einer Menge* M *ist eine Darstellung* $M = M_1 \dot\cup \ldots \dot\cup M_k$ *mit* $M_i \neq \emptyset$. *Eine Partition von* M *ist eine* k-*Partition für ein* $k \in \mathbb{N}$.

Die Anzahl der k-*Partitionen von* M *heiße* $S_{m,k}$, *die sogenannten Stirling–Zahlen zweiter Art. Die Anzahl der Partitionen von* M *heiße* B_m, *die sogenannten Bell–Zahlen.*

In einer Partition heißen die M_i "Blöcke" oder auch "Klassen", da jede k-Partition von M einer Äquivalenzrelation auf M mit den k Äquivalenzklassen $M_1, \ldots, M_k$ entspricht. Die m-te Bellzahl B_m ist also auch die Anzahl der Äquivalenzrelationen auf einer m-Menge.

"Partition" ist der zu "Teilmenge" duale Begriff, wie "Surjektion" zu "Injektion". Eine Surjektion $M \to K$ entspricht nämlich einer k-Partition von M mit einer Aufzählung der Blöcke. Folglich gilt $\left|\mathrm{Surj}(M,K)\right| = \left|\mathrm{Bij}(K,K)\right| \cdot \left|k\text{-Partitionen von } M\right| = k! \cdot S_{n,k}$.

Satz 1.12 (Eigenschaften der Stirling–Zahlen zweiter Art)

Explizite Formel:

$$S_{m,k} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^m = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^m = \sum_{j=0}^{k} (-1)^{k-j} \frac{j^m}{j!(k-j)!}$$

einige konkrete Werte:

$S_{m,m} = 0$ *für alle* $m \geqslant 0$ $\qquad S_{m,k} = 0$ *für* $k > m$

$S_{m,0} = 0 \qquad S_{m,1} = 1 \qquad S_{m,2} = 2^{m-1} - 1 \qquad S_{m,m-1} = \binom{m}{2}$ *je für* $m > 0$

Rekursionsformel:

$S_{m+1,k} = S_{m,k-1} + k \cdot S_{m,k}$ *für* $k > 0$ $\boxed{\text{ein Element aussondern}}$

$S_{0,0} = 1$ kann man als Konvention auffassen, um die Gültigkeit von Rekursionsformeln zu erhalten. Man kann dem aber auch Sinn verleihen, indem man die Vereinigung von 0 Mengen als Partition von $\emptyset$ ansieht, also $\emptyset = \dot\bigcup_{i \in \emptyset} M_i$.

Aus der Rekursionsformel ergibt sich das Stirling–Dreieck zweiter Art:

m									B_m
				$k=$ 0					
0				1	1				1
1			0		1	2			1
2		0		1		1	3		2
3	0		1		3		1		5
4	0	1		7 $+k\cdot$	6		1		15
5	0	1	15		25	10		1	52

Satz 1.13 (Eigenschaften der Bell–Zahlen)

$$B_0 = 1 \qquad B_m = \sum_{k=0}^{m} S_{m,k} \qquad B_{m+1} \overset{(1)}{=} \sum_{k=0}^{m} \binom{m}{k} B_k \overset{(2)}{=} \sum_{k=0}^{m} (k+1) S_{m,k}$$

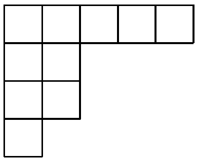
ein Element aussondern; Größe des Restblocks in (1), Anzahl der Blöcke in (2) betrachten

Zahlpartitionen

Eine Zahlpartition der natürlichen Zahl m ist eine Darstellung $m = m_1 + \cdots + m_k$ mit $m_i \geqslant 1$ für alle i, wobei die Reihenfolge der Summanden keine Rolle spiele. Ohne Einschränkung kann man also $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_k$ annehmen. Eine solche Zahlpartition von m in k Stücke entspricht einer k-Partition einer m-Menge, deren Elemente nicht zu unterscheiden sind. Die m_i sind dann die Mächtigkeiten der Blöcke.

Definition 1.4 *Die Anzahl der Zahlpartition von m in k Stücke sei $P_{m,k}$. Die Anzahl der Zahlpartitionen von m sei P_m.*

Die Darstellung einer Zahlpartition erfolgt oft durch ein Ferrers– oder Young–Diagramm (in der Literatur oft auch gedreht oder gespiegelt):



Ferrers–Diagramm für die Partition $10 = 5 + 2 + 2 + 1$.

Satz 1.14 (Eigenschaften der Zahlpartitionszahlen)

einige konkrete Werte:

$$P_{0,0} = 1 \qquad P_{m,2} = \left\lfloor \frac{m}{2} \right\rfloor \qquad P_{m,k} = 0 \ \textit{für}\ k > m$$

$$P_{m,0} = 0 \qquad P_{m,1} = P_{m,m-1} = P_{m,m} = 1 \qquad \textit{für}\ m > 0$$

Rekursionsformeln:

Wegstreichen der ersten Spalte im Young– Diagramm

$$P_{m,k} = \sum_{j=0}^{k} P_{m-k,j} \qquad P_{m,k} = P_{m-k} \ \textit{falls}\ 2k \geqslant m \qquad P_{m,k} \leqslant P_{m-k}$$

insbesondere: $P_{m,m-3} = 3$ *für* $m \geqslant 6$ $\qquad$ $P_{m,m-2} = 2$ *für* $m \geqslant 4$

Bemerkung: Für die Partitionszahlen P_m gibt es folgende Rekusionsgleichung (ohne Beweis):

$$P_m = \sum_{k=0}^{m} P_{m,k} = \sum_{k\geqslant 0} (-1)^k \Big(P_{m-\frac{1}{2}k(3k-1)} + P_{m-\frac{1}{2}k(3k+1)} \Big)$$

mit der Konvention, daß $P_m = 0$ für negative m. (In Wirklichkeit ist die Summe also endlich). Explizite Formeln für die Partitionszahlen $P_{m,k}$ und P_m sind nicht bekannt.

Aus der Rekursionsgleichung ergibt sich der Aufbau des Zahlpartitionsdreiecks. Die Summe der oberen Zeile eines in der linken Diagonale beginnenden Dreiecks ergibt die Spitze:

m	$k = 0$	P_m
0	1 $\quad_1$	1
1	0 1 $\quad_2$	1
2	0 1 1 $\quad_3$	2
3	0 1 1 1 $\quad_4$	3
4	0 1 2 1 1 $\quad_5$	5
5	0 1 2 2 1 1 $\quad_6$	7
6	0 1 3 3 2 1 1 $\quad_7$	11
7	0 1 3 4 3 2 1 1	15
8	0 1 4 5 5 3 2 1 1	22

Geordnete Zahlpartitionen

Eine geordnete Zahlpartition der natürlichen Zahl m ist eine Darstellung $m = m_1 + \cdots + m_k$ mit $m_i \geqslant 1$ für alle i, unter Beachtung der Reihenfolge der Summanden. Etwa sind $3 = 1+2$ und $3 = 2+1$ verschiedene geordnete Zahlpartitionen von 3.

Satz 1.15 *Die Anzahl der geordneten Zahlpartition von m in k Stücke ist*

$$\begin{aligned} &\binom{m-1}{k-1} && \textit{für } m \geqslant 1, k \geqslant 1 \\ &0 && \textit{für } m = 1, k = 0 \textit{ oder für } k > m \\ &1 && \textit{für } m = k = 0 \end{aligned}$$

Man fasse die m_i als Differenzen der Elemente einer $(k-1)$-Teilmenge von $\{1, \ldots, m-1\}$ auf.

Kleine Zusammenfassung

Wir haben also bislang vier Arten von Partitionen von einer m-Menge in k Blöcke untersucht:

Blöcke / Elemente	ungeordnet	Anzahl	angeordnet	Anzahl
ununterscheidbar	Zahlpartition	$P_{m,k}$	geordnete Zahlpartitionen	$\binom{m-1}{k-1}$
unterschieden	Mengenpartition	$S_{m,k}$	Surjektion	$k! \cdot S_{m,k}$

Ähnlich kann man vier verschiedene Arten von Auswahlen von k Elementen aus einer m-Menge betrachten:

Auswahl / Wiederholungen	ungeordnet	Anzahl	angeordnet	Anzahl
nicht erlaubt	Teilmenge	$\binom{m}{k}$	Injektion	$k! \cdot \binom{m}{k}$
erlaubt	"Multiteilmenge"	$\binom{m+k-1}{k}$	beliebige Abbildung	k^m

Multiteilmenge: i komme a_i oft vor; die $a_i + 1$ bilden eine geordnete Zahlpartition von $m + k$.

Permutationen und Stirling–Zahlen erster Art

Eine Permutation einer Menge M ist eine Bijektion von M auf M. Die Menge der Permutationen von M heißt die symmetrische Gruppe auf M und wird mit $\mathrm{Sym}(M)$, S_M oder $\mathfrak{S}_M$ bezeichnet. Für $M = \{1, \dots, m\}$ schreibt man auch $\mathrm{Sym}(m)$ usf. Eine Permutation $\sigma \in \mathrm{Sym}(n)$ hat einerseits den "aktiven" Aspekt einer Abbildung $i \mapsto \sigma(i)$; andererseits den "passiven" Aspekt der Anordnung der Zahlen $1, \dots, m$ als $\sigma(1), \sigma(2) \cdots \sigma(m)$. Darstellungsmöglichkeiten:

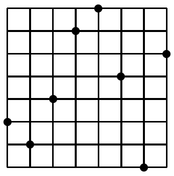
Wertetabelle:

i	1	2	3	4	5	6	7	8
$\sigma(i)$	3	2	4	7	8	5	1	6

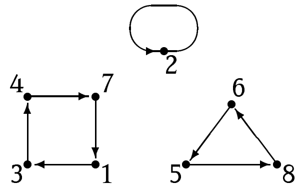
Wort: 3 2 4 7 8 5 1 6

Zyklenzerlegung: (4713)(587)(2)

Funktionsgraph:



Graph:



Die Zusammenhangskomponenten des Graphen rechts heißen Zyklen der Permutation. Genauer ist ein Zyklus (der Länge l) eine Folge $a_1 \dots a_l$ von Zahlen aus $1, \dots, m$ mit $\sigma(a_i) = a_{i+1}$ für $i = 1, \dots, l-1$ und $\sigma(a_l) = a_1$. Ein Zyklus der Länge 1 heißt Fixpunkt der Permutation. Jede Permutation läßt sich als "Produkt" ihrer Zyklen schreiben wie im obigen Beispiel; die Schreibweise ist eindeutig bis auf Reihenfolge der Zyklen und zyklische Vertauschung der Elemente in jedem Zyklus. Beginnt man jeden Zyklus mit dem kleinsten Element und den nächsten Zyklus mit dem minimalen noch verbleibenden Element, erhält man eine kanonische Schreibweise. Im Beispiel wäre dies (1347)(2)(587).

Definition 1.5 *Die Anzahl der Permutationen von m Elementen mit k Zyklen heißt die Stirling–Zahl erster Art* $s_{m,k}$.

Die Zyklenzerlegung liefert offenbar eine Partition einer m-Menge mit einer zyklischen Ordnung auf jedem Block. Insbesondere gilt also $s_{m,k} \leqslant S_{m,k}$ für alle m, k. Jede Permutation ist bestimmt durch: den Typ der Partition, d.h. die Anzahl der Zyklen von gegebener Länge; die Zuordnung der Zahlen zu den Blöcken; eine zyklische Ordnung auf jedem Block. Nehmen wir an, daß es b_i Zyklen der Länge i gibt, so gilt also

$$s_{m,k} = \sum \left\{ \frac{m!}{b_1! \cdots b_m! 1^{b_1} \cdots m^{b_m}} \;\middle|\; \sum_{i=1}^{m} b_i = k, \sum_{i=1}^{m} i b_i = m \right\}$$

Diese Formel ist allerdigns für praktische Belange wenig nützlich.

Satz 1.16 (Eigenschaften der Stirling–Zahlen erster Art)

einige konkrete Werte:

$s_{m,m} = 1$ *für alle* $m \geqslant 0$ $\qquad s_{m,k} = 0$ *für* $k > m$ $\qquad$ *für* $m > 0$:

$s_{m,0} = 0 \qquad s_{m,1} = (m-1)! \qquad s_{m,2} = (m-1)!\Big(1 + \frac{1}{2} + \cdots + \frac{1}{m-1}\Big) \qquad s_{m,m-1} = \binom{m}{2}$

Rekursionsformel:

$s_{m+1,k} = s_{m,k-1} + m \cdot s_{m,k}$ *für* $k > 0$

Summenformel:

$$\sum_{k=0}^{m} s_{m,k} = m!$$

Aus der Rekursionsformel ergibt sich das Stirling–Dreieck erster Art:

m	$k=0$	1	2	3	4	5	$m!$
0	1						1
1	0	1					1
2	0	1	1				2
3	0	2	3	1			6
4	0	6	11	6	1		24
5	0	24	50	35	10	1	120

Bemerkung: $\{1, x, x^2, \ldots, x^n\}$ und $\{1, x, x(x-1), \cdots, x(x-1)\cdots(x-n+1)\}$ sind Basen des Vektorraums $\mathbb{C}_n[x]$ der Polynome vom Grad $\leqslant n$. Name und Zusammenhang der Stirling–Zahlen erklärt sich daraus, daß sie die Einträge der Basiswechselmatrizen sind; genauer gilt:

Satz 1.17

$$x^n = \sum_{k=0}^{n} S_{n,k} \cdot x(x-1)\cdots(x-k+1) \qquad \boxed{\textit{folgt aus 1.8}}$$

$$x(x-1)\cdots(x-n+1) = \sum_{k=0}^{n} (-1)^{n-k} s_{n,k} \cdot x^k \qquad \boxed{\textit{Induktion nach } n}$$

In der Literatur werden daher auch oft die $(-1)^{n-k}s_{n,k}$ als Stirling–Zahlen erster Art bezeichnet.

Satz 1.18 *Die Anzahl der fixpunktfreien Permutationen von* m *Elementen ist*

$$m! \sum_{j=0}^{m} \frac{(-1)^j}{j!} \qquad \boxed{\text{Inklusion–Exklusion}}$$

Wichtig in Abschnitt 1.1:
Die vier Arten von Partitionen, die vier Arten von Auswahlen und ihre jeweiligen Anzahlen. Binomialkoeffizienten, Partitionszahlen, Stirling–Zahlen: ihre Bedeutung, Anfangswerte und Rekursionsgleichungen.

I.2 Diskrete Wahrscheinlichkeitstheorie

Ein (diskreter) Wahrscheinlichkeitsraum (Ω, p) besteht aus einer endlichen oder abzählbaren Menge Ω, dem Ereignisraum, deren Elemente Elementarereignisse oder Ergebnisse heißen, und einer Abbildung $p : \Omega \to [0, 1] \subseteq \mathbb{R}$, der sogenannten (Wahrscheinlichkeits–) Verteilung, für die

$$\sum_{\omega \in \Omega} p(\omega) = 1$$

gilt. Ein Ereignis ist eine Teilmenge von Ω; die Wahrscheinlichkeit eines Ereignisses A wird definiert als $p(A) := \sum\limits_{\omega \in A} p(\omega)$.

Beispiele:

(1) "Modell eines Würfels": $\Omega = \{1, 2, 3, 4, 5, 6\}$, $p(1) = p(2) = \cdots = p(6) = \frac{1}{6}$ beim "fairen" Würfel. Für das Ereignis "gerade Augenzahl" ist z.B. die Wahrscheinlichkeit $\frac{1}{2}$.

(2) "Mächtigkeit einer Teilmenge einer n-Menge": $\Omega = \{0, \ldots, n\}$ und $p(k) = 2^{-n}\binom{n}{k}$ bei gleichmäßigem Vorkommen aller Teilmengen.

(3) Man wirft solange eine Münze, bis Zahl erscheint, und fragt nach der Anzahl der Würfe. $\Omega = \mathbb{N} \setminus \{0\}$ und $p(n) = 2^{-n}$.

Satz 2.1 (Eigenschaften der Wahrscheinlichkeit von Ereignissen)

(a) $p(\emptyset) = 0$, $p(\Omega) = 1$, $p(\Omega \setminus A) = 1 - p(A)$.

(b) $A \subseteq B \Rightarrow p(A) \leqslant p(B)$; *insbesondere gilt* $0 \leqslant p(A) \leqslant 1$ *für alle Ereignisse* A.

(c) $p(A \cup B) = p(A) + p(B) - p(A \cap B)$; *woraus folgt:*

$$\begin{aligned}
p(A_1 \dot\cup \ldots \dot\cup A_k) &= p(A_1) + \cdots + p(A_k) \\
p(A_1 \cup \cdots \cup A_k) &\leqslant p(A_1) + \cdots + p(A_k) && \text{(Subadditivität)} \\
p(A_1 \cup \cdots \cup A_k) &= \sum_{\emptyset \neq I \subseteq \{1,\ldots,k\}} (-1)^{|I|+1} \cdot p\Big(\bigcap_{i \in I} A_i\Big) && \text{(Sylvestersche Siebformel)}
\end{aligned}$$

Ist Ω endlich, so wird durch $p(\omega) = \frac{1}{|\Omega|}$ für alle $\omega \in \Omega$ die sogenannte Laplace– oder Gleichverteilung definiert; (Ω, p) heißt dann auch Laplace–Raum. Für Ereignisse A gilt darin: $p(A) = \frac{1}{|\Omega|} \cdot |A| =$ "Anzahl der günstigen Fälle durch Anzahl der möglichen Fälle", was die Analogie der obigen Regeln zu den Mächtigkeitsregeln erklärt.

Bedingte Wahrscheinlichkeit

Sei von nun an (Ω, p) fest gegeben.

Definition 2.1 *Falls* $p(B) > 0$, *definiert man die bedingte Wahrscheinlichkeit von* A *gegeben* B *als*

$$p(A|B) := \frac{p(A \cap B)}{p(B)}$$

Zwei Ereignisse A, B *heißen* <u>*unabhängig*</u>*, falls* $p(A \cap B) = p(A) \cdot p(B)$. *Allgemeiner heißen Ereignisse* A_i, $i \in I$, *unabhängig, falls* $p(\bigcap_{j=1}^{k} A_{i_j}) = p(A_{i_1}) \cdots p(A_{i_k})$ *für alle* k *und paarweise verschiedenen* $i_1, \ldots, i_k \in I$.

Insbesondere gilt also $p(A \cap B) = p(A|B) \cdot p(B) = p(B|A) \cdot p(A)$, vorausgesetzt die vorkommenden bedingten Wahrscheinlichkeiten sind definiert. Falls $p(B) > 0$, so sind A und B also genau dann unabhängig sind, wenn $p(A|B) = p(A)$. Falls zudem $p(\Omega \setminus B) > 0$, so sind A und B genau dann unabhängig, wenn $p(A|B) = p(A|\Omega \setminus B)$. Insbesondere folgt aus der Unabhängigkeit von A und B auch die von A und $\Omega \setminus B$.

Beispiel:

(a) Laplace–Raum (Ω, p) für den Würfelwurf: Ereignis $A =$ "gerade Zahl" mit $p(A) = \frac{1}{2}$; Ereignis $B =$ "Zahl $\geqslant 5$" mit $p(B) = \frac{1}{3}$; Ereignis $C =$ "Primzahl" mit $p(C) = \frac{1}{3}$. Dann gilt $p(A \cap B) = \frac{1}{6}$ und $p(A \cap C) = \frac{1}{6}$. Also sind A und B unabhängig, A und C dagegen nicht.

(b) Zwei Würfelwürfe nacheinander: wir arbeiten im Produktraum (Ω^2, p') (s.u.), also $|\Omega^2| = 36$. Ereignis $A =$ "erster Wurf ergibt 2" mit $p_2'(A) = \frac{1}{6}$; Ereignis $B =$ "zweiter Wurf ergibt 3" mit $p_2'(B) = \frac{1}{6}$; Ereignis $C =$ "Augensumme 7" mit $p_2'(C) = \frac{1}{6}$. Diese Ereignisse sind paarweise unabhängig, aber nicht unabhängig.

Satz 2.2 (Eigenschaften der bedingten Wahrscheinlichkeit) *Sei* $p(B) > 0$.

(a) (Ω, p_B) *mit* $p_B(A) := p(A|B)$ *ist ein Wahrscheinlichkeitsraum.*

(b) *Falls* $A \cap B = \emptyset$, *so* $p(A|B) = 0$.

(c) *Falls* $p(A \cap B) \neq 0$, *so* $p(A \cap C|B) = p(A|B) \cdot p(C|A \cap B)$.

(d) *Sofern* $p(\bigcap_{i=1}^{k-1} A_i) > 0$, *gilt allgemeiner:*

$$p\Big(\bigcap_{i=1}^{k} A_i\Big) = p(A_1) \cdot p(A_2|A_1) \cdot p(A_3|A_1 \cap A_2) \cdots p\Big(A_k \Big| \bigcap_{i=1}^{k-1} A_i\Big)$$

Sei im folgenden $\Omega = B_1 \dot\cup \ldots \dot\cup B_k$ eine Partition mit $p(B_i) > 0$ für alle i.

Satz 2.3 (von der totalen Wahrscheinlichkeit) $p(A) = \sum_{i=1}^{k} p(A|B_i) \cdot p(B_i)$.

Satz 2.4 (Bayessche Regel) *Falls* $p(A) \neq 0$, *so* $p(B_j|A) = \dfrac{p(A|B_j) \cdot p(B_j)}{\sum_{i=1}^{k} p(A|B_i) \cdot p(B_i)}$.

Produkträume

Seien $(\Omega_1, p_1), \ldots, (\Omega_k, p_k)$ Wahrscheinlichkeitsräume. Der <u>Produktraum</u> (Ω, p) ist ein Modell für das unabhängige Hintereinanderausführen von Zufallsexperimenten in den Wahrscheinlichkeitsräumen (Ω_i, p_i). Er ist definiert durch:

$$\begin{aligned} \Omega &:= \Omega_1 \times \cdots \times \Omega_k \\ p\big((\omega_1, \ldots, \omega_k)\big) &:= p(\omega_1) \cdots p(\omega_k) \end{aligned}$$

Satz 2.5 **(a)** *Falls alle* (Ω_i, p_i) *Laplace–Räume sind, so auch der Produktraum.*

(b) $p(A_1 \times \cdots \times A_k) = p(A_1) \cdots p(A_k)$ *für Ereignisse* $A_i \subseteq \Omega_i$.

(c) *Falls* $(\Omega_1, p_1) = (\Omega_2, p_2)$, *so sind zwei Ereignisse* $A, B \subseteq \Omega_1$ *unabhängig genau dann, wenn* $p(A \times B) = p_1(A \cap B)$.

Zufallsvariablen

Eine Zufallsvariable ist eine Abbildung $X : \Omega \to W$, wobei W eine Menge (von "Werten") ist. Im Falle $W = \mathbb{R}$ spricht man auch gerne von Zufallsgröße. Intuitiv beschreibt X die Auswertung eines Zufallsexperiments; X kann die gegenüber dem genauen Ausgang eigentlich interessante Information enthalten. Beispiele bei zweimaligem Würfen: die Augensumme oder "Pasch" bzw. "nicht Pasch". Beispiel bei einer Lottoziehung: die Anzahl der Richtigen.

Satz 2.6 (Induzierte Verteilung) *Ist* $X : \Omega \to W$ *Zufallsvariable, so wird durch* $p_X(w) := p(X^{-1}[w]) = p\big(\{\omega \in \Omega \mid X(\omega) = w\}\big)$ *eine Verteilung auf* W *gegeben, die von* X *induzierte Verteilung. Mit anderen Worten:* (W, p_X) *ist ein Wahrscheinlichkeitsraum.*

$p_X(w)$ mißt die Wahrscheinlichkeit, daß ein Experiment den Wert w annimmt. Für $p_X(w)$ schreibt man auch $p(X = w)$. Entsprechend erklären sich Ausdrücke der Form $p(X > w)$, falls W geordnet ist, usw.

Sind mehrere Zufallsvariablen $X_1 : \Omega \to W_1, \dots, X_k : \Omega \to W_k$ gegeben, so definieren sie eine Zufallsvariable $X_1 \times \cdots \times X_k : \Omega^k \to W_1 \times \cdots \times W_k$ auf dem Produktraum vermöge $X_1 \times \cdots \times X_k\big((\omega_1, \dots, \omega_k)\big) := \big(X_1(\omega_1), \dots, X_k(\omega_k)\big)$ und induzieren somit eine Verteilung $p_{X_1 \times \cdots \times X_k}$ auf $W_1 \times \cdots \times W_k$. Es gilt $p_{X_1 \times \cdots \times X_k}\big((w_1, \dots, w_k)\big) = p_{X_1}(w_1) \cdots p_{X_k}(w_k)$. Zum anderen gibt es auf $W_1 \times \cdots \times W_k$ die sogenannte gemeinsame Verteilung der X_i definiert durch $p\big((w_1, \dots, w_k)\big) := p(X_1 = w_1, \dots, X_k = w_k) = p\big(\{\omega \mid X_1(\omega) = w_1, \dots, X_k(\omega) = w_k\}\big)$.

Definition 2.2 *Zufallsvariablen* $X_1, \dots, X_k$ *heißen unabhängig, falls die induzierte Verteilung* $p_{X_1 \times \cdots \times X_k}$ *mit der gemeinsamen Verteilung übereinstimmt, d.h. falls*

$$p(X_1 = w_1 \wedge \cdots \wedge X_k = w_k) = p(X_1 = w_1) \cdots p(X_k = w_k)$$

für alle $w_1, \dots, w_k$.

Zu einem Ereignis $A \subseteq \Omega$ kann man die Indikatorvariable $\chi_A : \Omega \to \{0,1\}$ definieren mit $\chi_A(\omega) = 1 \iff \omega \in A$. Dann sind Ereignisse $A_1, \dots, A_k$ unabhängig genau dann, wenn die Zufallsvariablen $\chi_{A_1}, \dots, \chi_{A_k}$ unabhängig sind.

Erwartungswert und Varianz

Seien im folgenden alle betrachteten Zufallsvariablen reellwertig.

Definition 2.3 *Sei X eine reellwertige Zufallsvariable. Der* <u>*Erwartungswert*</u> *von X ist*

$$E(X) := \sum_{\omega \in \Omega} p(\omega) \cdot X(\omega)$$

Falls X nur endlich viele Werte annimmt, so ist die Summe endlich und existiert immer. Andernfalls braucht die Reihe nicht zu konvergieren, oder kann die Werte $+\infty$ oder $-\infty$ annehmen. Man sagt, daß der Erwartungswert existiert, wenn der Wert endlich ist. Im folgenden sollen die betrachteten Erwartungswerte stets existieren.

Durch Zusammenfassen der Ereignisse mit gleichem Wert sieht man

$$E(X) = \sum_{r \in \mathbb{R}} p_X(r) \cdot r = \sum_{r \in \mathbb{R}} r \cdot p(X = r)$$

Bei Gleichverteilung ist der Erwartungswert genau der Mittelwert der Wahrscheinlichkeiten.

Für reellwertige Zufallsvariablen X, Y sind auch $X + Y$, $X \cdot Y$ und $r \cdot X$ für $r \in \mathbb{R}$ Zufallsvariablen. Es gilt:

Satz 2.7 **(a)** *Der Erwartungswert ist linear, d.h.* $E(rX + sY) = rE(X) + sE(Y)$.

(b) *Für unabhängige Zufallsvariablen ist der Erwartungswert multiplikativ, d.h. für unabhängige X, Y gilt* $E(X \cdot Y) = E(X) \cdot E(Y)$.

Definition 2.4 (Weitere Maßzahlen für Zufallsgrösen)

(1) *Die* <u>*Varianz*</u> $V(X) := E\big((X - E(X))^2\big)$ *mißt, wie weit die Werte sich um den Erwartungswert gruppieren.*

(2) *Die* <u>*Standardabweichung*</u> *oder* <u>*Streuung*</u> $\sigma_X = \sqrt{V(X)}$ *ist ein skalenunabhängiges solches Maß.*

(3) *Die* <u>*Kovarianz*</u> $Cov(X, Y) := E\big((X - E(X))(Y - E(Y))\big)$ *mißt das gegenseitige Variieren von X und Y.*

(4) *Die* <u>*Korrelation*</u> $Kor(X, Y) := \dfrac{Cov(X, Y)}{\sqrt{V(X)V(Y)}}$ *ist das zugehörige skalenunabhängige Maß.*

Unter anderem gelten folgende Rechenregeln:

$V(X) = E(X^2) - E(X)^2$;
falls X, Y unabhängig sind, so gilt $V(X + Y) = V(X) + V(Y)$;
$Cov(X, Y) = E(XY) - E(X)E(Y)$ und $Cov(X, X) = V(X)$;
Cov ist symmetrisch und bilinear;
falls X, Y unabhängig, so $Cov(X, Y) = 0$.

Wichtig in Abschnitt 1.2:
Definition und grundliegende Eigenschaften von: Wahrscheinlichkeitsräumen, Verteilungen, Ereignissen. Gleichverteilung. Unabhängigkeit zweier Ereignisse. Zufallsvariablen, Erwartungswert, Varianz.

I.3 Erzeugende Funktionen

Formale Potenzreihen

Sei K ein Körper, etwa $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definition 3.1 *Eine (formale) Potenzreihe über* K *ist ein Ausdruck der Form* $\sum_{n\in\mathbb{N}} a_n X^n$ *mit* $a_n \in K$. *Die Menge der Potenzreihen über* K *bezeichnet man mit* $K[[X]]$.

In den Potenzreihen ist X eine Variable; die a_n heißen die Koeffizienten der Potenreihe. "Formal" werden sie deshalb manchmal genannt, da das Konvergenzverhalten in der Regel keine Rolle spielt: man kann mit diesen Reihen rechnen, ohne daß ihnen für Einsetzungen $X \in K$ Werte zugeteilt werden. Per Definition sind zwei Potenzreihen $\sum_{n\in\mathbb{N}} a_n X^n$ und $\sum_{n\in\mathbb{N}} b_n X^n$ genau dann gleich, wenn $a_n = b_n$ für alle $n \in \mathbb{N}$.

Die algebraische Struktur von K überträgt sich teilweise auf $K[[X]]$; man kann Potenzreihen addieren, subtrahieren und multiplizieren, sowie formale Ableitungen bilden:

$$\sum_{n\in\mathbb{N}} a_n X^n + \sum_{n\in\mathbb{N}} b_n X^n = \sum_{n\in\mathbb{N}} (a_n + b_n) X^n \qquad -\sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in\mathbb{N}} (-a_n) X^n$$

$$\sum_{n\in\mathbb{N}} a_n X^n \cdot \sum_{n\in\mathbb{N}} b_n X^n = \sum_{n\in\mathbb{N}} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n \qquad \frac{d}{dX}\Big(\sum_{n\in\mathbb{N}} a_n X^n \Big) = \sum_{n\in\mathbb{N}} (n+1) a_{n+1} X^n$$

Das Inverse zu $\sum_{n\in\mathbb{N}} a_n X^n$ existiert genau dann, wenn $a_0 \neq 0$; dann gilt:

$$\frac{1}{\sum_{n\in\mathbb{N}} a_n X^n} = \sum_{n\in\mathbb{N}} b_n X^n \quad \text{mit } b_0 = \frac{1}{a_0}, b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}$$

In $K[[X]]$ gelten dann viele der bekannten Rechenregeln, etwa Kommutativität und Assoziativität von $+$ und $\cdot$ und insbesondere Distributivität von Addition und Multiplikation, was erklärt, warum die Multiplikation nicht koeffizientenweise erklärt wird. Genauer ausgedrückt ist $K[[X]]$ eine differentielle K-Algebra.

Beispiele

$$\sum_{n\in\mathbb{N}} (cX)^{kn} = \frac{1}{1-(cX)^k} \quad \text{für } k \in \mathbb{N}, c \in \mathbb{C}$$

$$\sum_{n\in\mathbb{N}} \binom{m+n-1}{n} X^n = \frac{1}{(1-X)^m} \quad \text{für } m \in \mathbb{Z}$$

$$\frac{1}{1-X} \cdot \sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in\mathbb{N}} \Big(\sum_{k=0}^{n} a_k \Big) X^n$$

$$\sum_{n\in\mathbb{N}} \binom{c}{n} X^n = (1+X)^c \quad \text{für } c \in \mathbb{C} \text{ wobei } \binom{c}{n} := \frac{c(c-1)\cdots(c-n+1)}{n!}$$

Im letzten Beispiel stehen nicht unbedingt Identitäten zwischen formalen Potenzreihen, sondern Gleichheiten von Funktionen (auf dem Konvergenzgebiet der Reihe). Es ist oft nützlich, zwischen beiden Aspekten hin– und herzuspringen, ohne in einem einheitlichen mathematischen Rahmen zu arbeiten. Das Rechnen mit Potenzreihen hinterläßt daher oft ein ungutes Gefühl: man sollte dann die erhaltenen Ergebnisse auf ihre Richtigkeit hin überprüfen. Zwei andere wichtige Beziehungen für (konvergierende) Reihen sind:

$$\sum_{n\in\mathbb{N}} \frac{X^n}{n!} = e^X \qquad\qquad \sum_{n\geqslant 1} \frac{(-1)^n X^n}{n} = \ln(1+X)$$

Zwei einfache Rekursionsgleichungen

Definition 3.2 *Für eine Folge von Zahlen $a_0, a_1, a_2, \ldots$ sei die erzeugende Funktion die Potenzreihe*

$$\sum_{n\in\mathbb{N}} a_n X^n$$

Typischerweise sind die a_n durch ein kombinatorisches Problem gegeben, also etwa die Anzahl von Permutationen von n Elementen oder die n-te Bellzahl. Durch Rechnen mit den erzeugenden Funktionen lassen sich nun viele kombinatorisch gegebene Zahlen bestimmen, insbesondere Rekursionsgleichungen auflösen.

Beispiel der Ordnung 1:

Sei t_n die Anzahl der Teilmengen einer n-Menge. Dann gilt die Rekursion $t_{n+1} = 2t_n$ (warum?); zusätzlich hat man den Anfangswert $t_0 = 1$. Also gilt

$$\sum_{n\in\mathbb{N}} t_n X^n = t_0 + \sum_{n\in\mathbb{N}} t_{n+1} X^{n+1} = 1 + \sum_{n\in\mathbb{N}} 2t_n X^{n+1} = 1 + 2X \cdot \sum_{n\in\mathbb{N}} t_n X^n$$

$$\text{also} \quad \sum_{n\in\mathbb{N}} t_n X^n = \frac{1}{1-2X} = \sum_{n\in\mathbb{N}} 2^n X^n \quad \text{und folglich} \quad t_n = 2^n \quad \text{für alle} \quad n$$

Beispiel der Ordnung 2:

Die Fibonacci–Zahlen sind definiert durch die Anfangswerte $F_0 = 0, F_1 = 1$ und die Rekursion $F_{n+2} = F_n + F_{n+1}$. Also gilt hier:

$$\begin{aligned}
\sum_{n\in\mathbb{N}} F_n X^n &= 0 + 1 \cdot X + \sum_{n\in\mathbb{N}} F_{n+2} X^{n+2} \\
&= X + \sum_{n\in\mathbb{N}} (F_n + F_{n+1}) X^{n+2} \\
&= X + X^2 \cdot \sum_{n\in\mathbb{N}} F_n X^n + X \cdot \sum_{n\in\mathbb{N}} F_{n+1} X^{n+1} \\
&= X + X^2 \cdot \sum_{n\in\mathbb{N}} F_n X^n - X \cdot F_0 + X \cdot \sum_{n\in\mathbb{N}} F_n X^n
\end{aligned}$$

Es folgt also $\sum_{n\in\mathbb{N}} F_n X^n = \frac{X}{1-X-X^2}$ und man muß nur noch den Bruch in eine Reihe auflösen. Dazu bestimmt man die Nullstellen des Polynoms $1-X-X^2$; es gilt $1-X-X^2 = -(X+\frac{1+\sqrt{5}}{2})(X+\frac{1-\sqrt{5}}{2})$. Durch Partialbruchzerlegung erhält man dann

$$\frac{X}{1-X-X^2} = -X\Big(\frac{A}{X+\frac{1-\sqrt{5}}{2}} + \frac{B}{X+\frac{1+\sqrt{5}}{2}}\Big)$$

mit noch zu bestimmenden A und B. Durch Ausrechnen der rechten Seite und Koeffizientenvergleich ergibt sich $A+B=0$ und $A\frac{1+\sqrt{5}}{2}+B\frac{1-\sqrt{5}}{2}=1$, also $A=-\frac{1}{\sqrt{5}}$ und $B=\frac{1}{\sqrt{5}}$. Aus der Formel für die geometrische Reihe erhält man ferner

$$\frac{a}{X+c}=\frac{a}{c}\cdot\frac{1}{1-\frac{X}{-c}}=\frac{a}{c}\cdot\sum_{n\in\mathbb{N}}\left(\frac{1}{-c}\right)^n X^n=\sum_{n\in\mathbb{N}}\frac{(-1)^n a}{c^{n+1}}X^n$$

und schließlich

$$\sum_{n\in\mathbb{N}}F_nX^n=\sum_{n\in\mathbb{N}}\left(\frac{(-1)^nA}{(\frac{1-\sqrt{5}}{2})^{n+1}}+\frac{(-1)^nB}{(\frac{1+\sqrt{5}}{2})^{n+1}}\right)X^{n+1}=\sum_{n\in\mathbb{N}}\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)X^n$$

Satz 3.1 (Fibonacci–Zahlen) *Für die Fibonacci–Zahlen gilt*

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

Sie sind bestimmt durch die Anfangswerte $F_0=0, F_1=1$ *und die Rekursion* $F_{n+2}=F_n+F_{n+1}$ *bzw. die erzeugende Funktion* $F(X)$ *mit* $F(X)=\dfrac{X}{1-X-X^2}$.

Zur konkreten Berechnung der Fibonacci–Zahlen ist allerdings die Rekursion geeigneter als die explizite Formel, der man nicht einmal ansieht, daß sie natürliche Zahlen liefert.

Lösungsverfahren für lineare Rekursionsgleichungen endlicher Ordnung

Allgemeiner funktioniert dieses Verfahren für Rekursionsgleichungen der Form:

$$A_{n+k+1}=c_0A_n+c_1A_{n+1}+\cdots+c_kA_{n+k} \qquad (*)$$

wobei eine eindeutige Lösung durch Anfangswerte $A_0,\dots,A_k$ festgelegt wird. Setzt man $A(X):=\sum_{n\in\mathbb{N}}A_nX^n$ als die erzeugende Funktion der A_n undf formt man um

$$\begin{aligned}
A(X) &= A_0+A_1X+\cdots+A_kX^k+\sum_{n\in\mathbb{N}}A_{n+k+1}X^{n+k+1}\\
&= A_0+A_1X+\cdots+A_kX^k+\sum_{n\in\mathbb{N}}\big(c_0A_n+c_1A_{n+1}+\cdots+c_kA_{n+k}\big)X^{n+k+1}\\
&= A_0+A_1X+\cdots+A_kX^k+c_0X^{k+1}\cdot A(X)\\
&\qquad +c_1X^k\cdot A(X)-c_1A_0X^k\\
&\qquad +c_2X^{k-1}\cdot A(X)-c_2A_0X^{k-1}-c_2A_1X^{k-1}\\
&\qquad \vdots\\
&\qquad +c_kX\cdot A(X)-c_kA_0X-c_kA_1X-\cdots-c_kA_{k-1}X
\end{aligned}$$

so ergibt sich analog zur Umformung im Fall der Fibonacci–Zahlen:

Satz 3.2

$$\sum_{n\in\mathbb{N}}A_nX^n=\frac{\textit{Polynom in } X \textit{ vom Grad } \leqslant k}{1-c_kX-c_{k-1}X^2-\cdots-c_1X^k-c_0X^{k+1}}=\frac{P(X)}{Q(X)}$$

Dabei könnte man das Polynom $P(X)$ problemlos explizit hinschreiben.

Wie oben im Fall der Fibonacci–Zahlen ergibt sich nun folgende Lösungsmöglichkeit:

(1) Man zerlege $Q(X)$ in Linearfaktoren.

(2) Man bestimme die Partialbruchzerlegung von $\frac{1}{Q(X)}$.

(3) Jeden Summanden entwickele man mit der Formel für die geometrische Reihe in eine Potenzreihe.

(4) Man summiere diese Potenzreihen und multipliziere das Ergebnis mit $P(X)$.

Schwierig und im allgemeinen nicht möglich ist dabei nur der erste Schritt. Sofern dies geht, kann man sich in einem vereinfachten Verfahren einige Rechenarbeit sparen. Um dieses Verfahren plausibel zu machen, einige Vorüberlegungen:

Jede Wurzel β von $Q(X)$ ergibt bei Entwicklung einen Summanden der Form $\sum_n K \cdot \beta^{-n} X^n$ in der schließlichen expliziten Darstellung der gesuchten erzeugenden Funktion. Ist β Nullstelle mit Vielfachheit d, so tauchen wegen $\frac{1}{(1-X)^m} = \sum\limits_{n\in\mathbb{N}} \binom{m+n-1}{n} X^n$ zusätzlich Summanden der Form $\sum_n K' \cdot (\text{Polynom in } n \text{ vom Grad} \leqslant d-1) \cdot \beta^{-n} X^n$ auf. Die Lösungsformel der A_n wird also eine Linearkombination von Ausdrücken der Form $n^j \cdot \beta^{-n}$ mit $0 \leqslant j < d$ sein.

Angenommen $Q(X) = -c_0 \cdot \prod\limits_{i=0}^{k} (X - \beta_i)$. Durch Einsetzen von $X = Y^{-1}$ und Durchmultiplizieren mit Y^{k+1} erhält man

$$-c_0 - c_1 Y - \cdots - c_k Y^k + Y^{k+1} = -c_0 \prod_{i=0}^{k} (1 - Y\beta_i) = \pm c_0 \beta_0 \cdots \beta_k \prod_{i=0}^{k} (Y - \frac{1}{\beta_i})$$

d.h. die Nullstellen von $Q(X)$ sind die Kehrwerte der Nullstellen des <u>reflektierten</u> Polynoms

$$x^{k+1} = c_0 + c_1 x + \cdots + c_k x^k \qquad (**)$$

Dieses Polynom heißt auch <u>charakteristisches Polynom</u> der Rekursiongleichung $(*)$. Umgekehrt sieht man sofort: wenn $(*)$, ohne Anfangsbedingungen, Lösungen der Form $A_n = \alpha^n$ für festes α hat, so muß α Wurzel des charakteristischen Polynoms sein. Wir erhalten somit:

Verfahren zur Lösung linearer Rekursionsgleichungen endlicher Ordnung:

Betrachten man A_n als Funktion $\mathbb{N} \to \mathbb{C}, n \mapsto A_n$, so bilden die Lösungen der Rekursionsgleichung $(*)$ einen $k+1$-dimensionaklen Unterraum von $\mathrm{Abb}(\mathbb{N}, \mathbb{C})$. Eine Basis dieses Lösungsraumes ist durch

$$\{\alpha_i^n, n \cdot \alpha_i^n, \ldots, n^{d_i - 1} \alpha_i^n \mid i = 1, \ldots, m\}$$

gegeben, wobei die $\alpha_1, \ldots, \alpha_m$ die verschiedenen Wurzeln des charakteristischen Polynoms $(**)$ mit jeweiliger Vielfachheit d_i sind. Jede andere Lösung ist dann eine Linearkombinationen

$$\sum_{i=1}^{m} \left(k_{i1} \alpha_i^n + k_{i2} n \alpha_i^n + \cdots + k_{i d_i} n^{d_i - 1} \alpha_i^n\right)$$

Durch Vergleich der Werte für $n = 0, \ldots, k$ mit den $k+1$ Anfangswerten $A_0, \ldots, A_k$ ermittelt man dann die Konstanten $k_{ij} \in \mathbb{C}$.

Ein Beispiel: Sei die Rekursionsgleichung

$$A_{n+3} = -12A_n + 8A_{n+1} + A_{n+2}$$

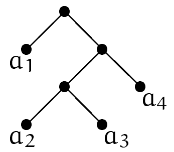
gegeben. Für das charakteristische Polynom gilt $X^3 - X^2 - 8X + 12 = (X-2)^2(X-3)$. Eine Basis der Lösungsmenge ist also durch $\{2^n, n \cdot 2^n, (-3)^n\}$ gegeben, die Lösungen sind genau die Folgen der Form $k_1 2^n + k_2 n 2^n + k_3(-3)^n$. Für gegebene Anfangswerte A_0, A_1, A_2 erhält man dann für $n = 0, 1, 2$ die eindeutg nach k_1, k_2, k_3 auflösbaren Gleichungen

$$\begin{aligned} k_1 + k_2 &= A_0 \\ 2k_1 + 2k_2 - 3k_3 &= A_1 \\ 4k_1 + 8k_2 + 9k_3 &= A_2 \end{aligned}$$

Eine nicht lineare Rekursionsgleichung

Die Catalan–Zahl C_n gibt die Anzahl der Möglichkeiten an, einen Ausdruck $a_1 + \cdots + a_n$ zu klammern. Per Konvention, $C_0 = 0$, $C_1 = 1$.

Man sieht sofort, daß C_n auch die Anzahl der binären Bäume mit n Blättern ist. Rechts der $a_1 + ((a_2 + a_3) + a_4)$ entsprechende Baum.



Aus der Baumdarstellung ergibt sich durch Weglassen der Wurzel die Rekursionsgleichung $C_{n+1} = \sum_{j=1}^{n} C_j \cdot C_{n+1-j}$ für $n \geqslant 0$. Wegen der Konvention $C_0 = 0$ folgt also $C_n = \sum_{j=0}^{n} C_j \cdot C_{n-j}$ für $n \geqslant 1$. Setzt man $C(X) := \sum_{n \in \mathbb{N}} C_n X^n$, so sieht man:

$$C(X)^2 = \sum_{n \in \mathbb{N}} \sum_{j=0}^{n} C_j \cdot C_{n-j} X^n = -X + \sum_{n \in \mathbb{N}} C_n X^n$$

Durch Auflösen der quadratischen Gleichung erhält man $C(X) = \frac{1}{2}\big(1 \pm \sqrt{1-4X}\big)$. Wegen $C(0) = C_0 = 0$ muß das Minuszeichen gewählt werden. Aus dem (in dieser Form hier nicht bewiesenen, aber gültigen) binomischen Satz folgt

$$C(X) = \frac{1}{2} - \frac{1}{2} \cdot \sum_{k \geqslant 0} \binom{\frac{1}{2}}{k} (-4X)^k$$

woraus man durch Ausrechnen die explizite Formel $C_n = \frac{1}{n}\binom{2n-2}{n-1}$ erhält. Wem diese Rechnungen suspekt sind, kann nun die Gültigkeit der Rekursionsgleichung nachprüfen.

Satz 3.3 (Catalan–Zahlen) *Für die Catalan–Zahlen gilt*

$$C_{n+1} = \sum_{j=1}^{n} C_j \cdot C_{n+1-j} \quad \textit{für } n \geqslant 0 \qquad\qquad C_n = \frac{1}{n}\binom{2n-2}{n-1}$$

Ihre erzeugende Funktion ist bestimmt durch $C(X) = X + C(X)^2$ *und Anfangswert* $C_0 = 0$.

Exponentielle erzeugende Funktionen

In vielen Fällen ist es nützlich, eine Variante der erzeugenden Funktionen zu betrachten:

Definition 3.3 *Für eine Folge von Zahlen* $a_0, a_1, a_2, \dots$ *sei*

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n$$

die exponentielle erzeugende Funktion.

Insbesondere wenn Permutationen im Spiel sind, etwa wenn die Elemente eines kombinatorischen Objektes durchnumeriert sind und jede Umsortierung ein neues Objekt ergibt, ist diese Normierung sinnvoll. Als Rechenregeln erhält man nun:

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n + \sum_{n\in\mathbb{N}} \frac{b_n}{n!} X^n = \sum_{n\in\mathbb{N}} \frac{(a_n + b_n)}{n!} X^n$$
$$\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n \cdot \sum_{n\in\mathbb{N}} \frac{b_n}{n!} X^n = \sum_{n\in\mathbb{N}} \frac{1}{n!} \Big(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \Big) X^n$$
$$\frac{d}{dX} \Big(\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n \Big) = \sum_{n\in\mathbb{N}} \frac{a_{n+1}}{n!} X^n \qquad \text{Shift!}$$

Die Exponentialfunktion ist also die der konstanten Folge $1, 1, \dots$ zugehörige exponentielle erzeugende Funktion. Ist $a_n = |\mathrm{Sym}(n)|$, so ergibt sich $\frac{1}{1-X}$ als exponentielle erzeugende Funktion, was den Nutzen der Normierung deutlich werden läßt.

Mit exponentiellen erzeugenden Funktionen werden die linearen Rekursionsgleichungen zu Differentialgleichungen, etwa im Falle der Fibonacci–Zahlen erhält man mit $F(X) = \sum \frac{F_n}{n!} X^n$ die Differentialgleichung:

$$\frac{d^2}{dX^2} F(X) = F(X) + \frac{d}{dX} F(X)$$

was die Analogie des Lösungsverfahrens linearer Rekursionsgleichungen mit dem linearer Differentialgleichungen erklärt. Der Rechenaufwand verringert sich freilich durch diese Betrachtungsweise nicht.

Anwendung auf die Bell–Zahlen

Sei $B(X)$ die exponentielle erzeugende Funktion der Bell–Zahlen. Dann

$$\frac{d}{dX} B(X) = \sum_{n\in\mathbb{N}} \frac{B_{n+1}}{n!} X^n = \sum_{n\in\mathbb{N}} \frac{1}{n!} \Big(\sum_{k=0}^{n} \binom{n}{k} B_k \Big) X^n = \sum_{n\in\mathbb{N}} \frac{X^n}{n!} \cdot \sum_{n\in\mathbb{N}} \frac{B_n}{n!} X^n = \exp(X) \cdot B(X)$$

woraus leicht folgt

Satz 3.4 (Exponentielle erzeugende Funktion der Bell–Zahlen)

$$B(X) = \exp\big(\exp(X) - 1\big)$$

Es folgt:

$$e^{e^X-1} = \frac{1}{e}\cdot e^{e^X} = \frac{1}{e}\sum_{k\in\mathbb{N}}\frac{e^{Xk}}{k!} = \frac{1}{e}\sum_{k\in\mathbb{N}}\Big(\frac{1}{k!}\cdot\sum_{n\in\mathbb{N}}\frac{X^nk^n}{n!}\Big) = \sum_{n\in\mathbb{N}}\Big(\frac{1}{e}\cdot\sum_{k\in\mathbb{N}}\frac{k^n}{k!}\Big)\frac{X^n}{n!} = B(X)$$

Also mit Koeffizientenvergleich:

Satz 3.5

$$B_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$$

Noch ein Beispiel ...

Für die (normale) erzeugende Funktion der Partitionszahlen findet man:

$$\sum_{n\in\mathbb{N}} P_nX^n = \prod_{n\geqslant 1}\frac{1}{1-X^n} = (1+t+t^2+\cdots)(1+t^2+t^4+\cdots)(1+t^3+t^9+\cdots)\cdots$$

Durch Ausmultiplizieren erhält man einen Term t^n genau aus $t^{a_1}(t^2)^{a_2}\cdots(t^k)^{a_k}$, wobei $a_1+2a_2+\cdots+ka_k=n$. Dies entspricht der Partition

$$n = \underbrace{1+\cdots+1}_{a_1 \text{ mal}} + \underbrace{2+\cdots+2}_{a_2 \text{ mal}} + \cdots + \underbrace{k+\cdots+k}_{a_k \text{ mal}}$$

Von dieser Darstellung der erzeugenden Funktion kommt man mit einiger (nicht offensichtlicher) Arbeit zur Rekursionsgleichung auf Seite 11.

Wichtig in Abschnitt 1.3:
Erzeugende Funktionen und exponentielle erzeugende Funktionen. Verfahren zum Lösen linearer Rekursionsgleichungen. Fibonacci–und Catalan–Zahlen.

I.4 Größenwachstum von Funktionen

Falls eine explizite Darstellung einer Zählfunktion nicht möglich ist, kann man eventuell eine Einschätzung des Größenwachstum erhalten. Aufgabe 4 Übungsblatt 2 etwa legt nahe, daß B_n stärker wächst als 2^n und schwächer als $n!$.

Obwohl wir eigentlich an Zählfunktionen $\mathbb{N}\to\mathbb{N}$ interessiert sind, ist es günstig, die Definitionen allgemein für Funktionen $\mathbb{N}\to\mathbb{C}$ einzuführen. Um dabei Größen vergleichen zu können, muß man mit Beträgen arbeiten. Stattdessen könnte man auch nur positive Funktionen $f:\mathbb{N}\to\mathbb{R}_0^+$ betrachten.

Grundannahme für dieses Abschnitt: alle Funktionen $f:\mathbb{N}\to\mathbb{C}$ mögen nur endlich viele Nullstellen haben.

Definition 4.1 *“g wächst stärker als f”:*

$$f \ll g :\iff \lim_{n\to\infty}\frac{|f(n)|}{|g(n)|} = 0 \iff \forall C>0\,\exists n_C\,\forall n\geqslant n_C : |f(n)|\leqslant C\cdot|g(n)|$$

"f und g sind asymptotisch gleich":

$$f \sim g :\iff \lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$$

Außerdem definiert man $o(g) := \{f \mid f \ll g\}$ (gesprochen: "klein o von g"). Man schreibt in der Regel leider $f = o(g)$ statt $f \in o(g)$. Meist taucht die Notation in Ausdrücken wie $f = h + o(g)$ auf, was für $f - h \in o(g)$ steht und intuitiv bedeutet, daß f und h für große Werte übereinstimmen bis auf einen Fehler, der weniger stark wächst als g. Per Definition gilt also: $f \ll g \iff f \in o(g)$.

Beispiel:

$f \in o(1) \iff \lim\limits_{n\to\infty} f(n) = 0$

$f \in o(n) \iff \lim\limits_{n\to\infty} \frac{f(n)}{n} = 0$, also etwa konstante Funktionen f.

Satz 4.1

(a) $\sim$ *ist eine Æquivalenzrelation.*

(b) $\ll$ *ist eine partielle (nicht totale) Ordnungsrelation (d.h. transitiv und irreflexiv).*

(c) *Verträglichkeit von* $\ll$ *mit* $\sim$*:* $f' \sim f \ll g \sim g' \Longrightarrow f' \sim g'$.

(d) *Verträglichkeit von* $\ll$ *mit der Vektorraumstruktur:* $f_1 \ll g, f_2 \ll g \Longrightarrow \alpha f_1 + \beta f_2 \ll g$ *für alle* $\alpha, \beta \in \mathbb{C}$*; also ist* $o(g)$ *ein Untervektorraum von* $\mathrm{Abb}(\mathbb{N}, \mathbb{C})$.

(e) *Multiplikative Verträglichkeit:* $f \ll g \Longrightarrow fh \ll gh$ *und* $f \sim g \Longrightarrow fh \sim gh$. *Insbesondere:* $f \ll g \iff \frac{1}{g} \ll \frac{1}{f}$.

Beispiele:

- Für Polynome f, g gilt:

$$\begin{aligned} f \ll g &\iff \mathrm{grad}(f) < \mathrm{grad}(g) \\ ?? &\iff \mathrm{grad}(f) = \mathrm{grad}(g) \\ f \sim g &\iff \mathrm{grad}(f) = \mathrm{grad}(g) \text{ und im Absolutbetrag gleicher Leitkoeffizienten} \end{aligned}$$

- Für $0 < a < b$ und $1 < c < d$ weiß man:

$$\mathrm{konst} \ll \log\log(n) \ll \log(n) \ll n^a \ll n^b \ll c^n \ll d^n \ll n! \ll n^n \qquad (*)$$

- Logarithmen verschiedener Basen wachsen "gleich schnell", ohne für $a \neq b$ asymptotisch gleich zu sein, da

$$\lim_{n\to\infty} \frac{\log_a(n)}{\log_b(n)} = \log_a(b)$$

Logarithmen verhalten sich also wie Polynome gleichen Grades; dafür fehlt noch ein "Zwischenbegriff":

Definition 4.2

$$\begin{aligned} O(g) &:= \{f \mid \exists C > 0\, \exists n_0\, \forall n \geqslant n_0 : |f(n)| \leqslant C \cdot |g(n)|\} \\ \Omega(g) &:= \{f \mid \exists C' > 0\, \exists n_0\, \forall n \geqslant n_0 : C' \cdot |g(n)| \leqslant |f(n)|\} &&= \{f \mid g \in O(f)\} \\ \Theta(g) &:= \{f \mid \exists C, C' > 0\, \exists n_0\, \forall n \geqslant n_0 : C' \cdot |g(n)| \leqslant |f(n)| \leqslant C \cdot |g(n)|\} &&= O(g) \cap \Omega(g) \end{aligned}$$

Die für o üblichen Schreibweisen werden auch für O, Ω und Θ verwendet, etwa $f = \Omega(g)$ statt $f \in \Omega(g)$. **Achtung:** In der Informatik wird $\Omega(g)$ manchmal anders definiert!

Satz 4.2

(a) $f \in \Theta(g)$ *ist eine Æquivalenzrelation, die gröber als* $\sim$ *ist, d.h.* $f \sim g \Longrightarrow f \in \Theta(g)$, *(Die Umkehrung gilt nicht, wie das Beispiel der Polynome zeigt.)*

(b) *Verträglichkeit mit* $\ll$*:* $f' \in O(f), g' \in \Omega(g), f \ll g \Longrightarrow f' \ll g'$.

(c) *Verträglichkeit mit der Vektorraumstruktur:* $f_1, f_2 \in O(g) \Longrightarrow \alpha f_1 + \beta f_2 \in O(g)$ *für alle* $\alpha, \beta \in \mathbb{C}$*; also ist* $O(g)$ *ein Untervektorraum von* $\mathrm{Abb}(\mathbb{N}, \mathbb{C})$ *(nicht aber* $\Omega(g), \Theta(g)$*!).*

(d) *Multiplikative Verträglichkeit:* $f \in \Theta(g) \Longrightarrow fh \in \Theta(gh)$.

Beispiel: Für Polynome f, g gilt:

$$\begin{aligned} f \in O(g) &\iff \mathrm{grad}(f) \leqslant \mathrm{grad}(g) \\ f \in \Omega(g) &\iff \mathrm{grad}(f) \geqslant \mathrm{grad}(g) \\ f \in \Theta(g) &\iff \mathrm{grad}(f) = \mathrm{grad}(g) \end{aligned}$$

Wie schnell wächst die Fakultätsfunktion? Aus $\log(n!) = \sum\limits_{k=1}^{n} \log(k)$ und einer Abschätzung der Summe durch das Integral $\int\limits_1^n \log(x)dx$ erhält man leicht

$$\log(n!) \sim n \cdot \log(n)$$

Daran sieht man, daß aus $f \sim g$ nicht $h \circ f \sim h \circ g$ folgt, da $\mathrm{Basis}^{\log(n!)} = n! \not\sim n^n = \mathrm{Basis}^{n \log n}$. Mit etwas Mehrarbeit folgt aus solchen Überlegungen auch:

Satz 4.3 (Stirlingsche Formel)

$$\begin{aligned} n! &\sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n = \sqrt{2\pi} \cdot e^{-n} \cdot n^{n+\frac{1}{2}} \\ n! &= \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdot \left(1 + O(\frac{1}{n})\right) \end{aligned}$$

In manchen Fällen ist es schwierig, explizite Lösungen für Rekursionsgleichungen zu finden; Wachstumsabschätzungen dagegen erhält man leicht:

Satz 4.4 *Seien* $a \geqslant 1, b > 1, c$ *gegeben und* $A(n)$ *durch* $A(0)$ *bzw.* $A(1)$ *und eine der beiden Rekursionsformeln*

$$A(n) = a \cdot A\left(\left\lceil \frac{n}{b} \right\rceil\right) + c \qquad A(n) = a \cdot A\left(\left\lfloor \frac{n}{b} \right\rfloor\right) + c$$

bestimmt. Dann gelten folgende Wachstumsabschätzungen für A*:*

$$\begin{array}{lll} \textit{falls} & a = 1 & , \textit{ so } A \in \Theta(\log(n)) \\ \textit{falls} & a = b > 1 & , \textit{ so } A \in \Theta(n) \\ \textit{falls} & a \neq b, a > 1, & \textit{so } A \in \Theta\left(n^{\log_b(a)}\right) \end{array}$$

Wichtig in Abschnitt 1.4:
Definition und Eigenschaften von $\ll, \sim, o, O, \Omega, \Theta$; die Größenvergleiche der Standardfunktionen in $(*)$; die Stirlingsche Formel.

Teil II: Graphen

Graphen sind grundlegende mathematische Strukturen, die in vielen Anwendungen, insbesondere auch in der Informatik, auftreten. Anschaulich ist ein Graph eine Menge von Punkten mit Verbindungen, wie sie etwa im Modell eines Wegenetzes vorkommen. In gewissem Sinne sind Graphen die einfachsten mathematischen Strukturen, in denen bereits Phänomene größtmöglicher Komplexität auftauchen.

II.5 Definition und Begriffe

Mehrere Definitionen von Graphen sind möglich und in der Literatur vertreten. Meistens werden weder Schleifen, d.h. Verbindungen eines Punktes mit sich selbst, noch Mehrfachkanten, d.h. mehrere Verbindungen zwischen denselben Punkten, erlaubt. Mathematisch definiert man also:

Definition 5.1 *Ein Graph* $G = (E, K)$ *ist eine Menge* E *und eine Teilmenge* K *der zweielementigen Teilmengen* $\mathfrak{P}_2(E)$ *von* E*. Die Elemente aus* E *nennt man Ecken (auch Knoten, engl.: vertices), die Elemente aus* K *Kanten (engl.: edges).*

Häufiger noch wird ein Graph als ein Paar (E, R) definiert, wobei R eine zweistellige, irreflexive, symmetrische Relation auf der Eckenmenge E ist. Dabei gilt mit obiger Definition $e_1 R e_2 \iff \{e_1, e_2\} \in K$; beide Aspekte können also einfach ineinander überführt werden. Man schreibt oft $e_1 K e_2$ oder $e_1 e_2 \in K$ statt $\{e_1, e_2\} \in K$; die beiden Ecken e_1, e_2 heißen dann benachbart oder adjazent. Die Menge der Nachbarn von e sei $N(e)$ und $d(e) := |N(e)|$ der Grad (oder die Valenz) von e.

Für die Größe eines Graphen gibt es zwei Parameter: die Anzahl der Ecken, auch Ordnung des Graphen genannt, und die Anzahl der Kanten, auch Größe des Graphen genannt. Wir werden nur endliche Graphen betrachten, d.h. Graphen endlicher Ordnung. Diese haben dann auch automatisch nur endliche viele Kanten. Möchte man die Komplexität von Algorithmen auf Graphen berechnen, muß man festlegen, welches Maß für die Größe eines Graphen zugrundegelegt wird. Wegen

$$|K| \leqslant \binom{|E|}{2} = \frac{1}{2} \cdot n(n+1) \sim \frac{1}{2} n^2$$

unterscheidet sich i.a. die Komplexität nach Eckenanzahl oder Kantenanzahl berechnet.

Oft legt man daher $|E| + |K|$ als Maß zugrunde.

Satz 5.1

$$\sum_{e \in E} d(e) = 2 \cdot |K|$$

$\square$ Jede Kante wird links doppelt gezählt – bei Anfangs– und Endpunkt. $\square$

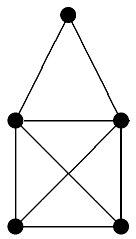
Folgerung: Ein Graph hat stets eine gerade Anzahl von Ecken ungeraden Grades.

Beispiele

- Der vollständige Graph K_n: dieser hat n Ecken und alle $\binom{n}{2}$ möglichen Kanten zwischen diesen Ecken.
- Der Kreis C_n ($n \geqslant 3$) hat n Ecken $e_1, \dots, e_n$ und Kanten $\{e_i, e_{i+1}\}$ für $i = 1, \dots, n-1$ sowie die Kante $\{e_1, e_n\}$, insgesamt also auch n Kanten.
- Der Graph $K_3 = C_3$ heißt auch das Dreieck.
- Bei bipartiten Graphen gibt es eine Partition $E = E' \dot\cup E''$ der Eckenmenge, so daß Kanten nur zwischen Ecken aus E' und E'' bestehen. Beim vollständigen bipartiten Graphen $K_{n,m}$ ist dabei $|E'| = n$, $|E''| = m$ und alle möglichen Kanten zwischen Ecken aus E' und E'' sind vorhanden. Es gilt also $|E| = n + m$ und $|K| = nm$.
- Entsprechend liegt bei r-partiten Graphen eine Partition $E = E_1 \dot\cup \dots \dot\cup E_r$ vor und Kanten bestehen nur zwischen Ecken aus verschiedenen Blöcken. Der vollständige r-partite Graph $K_{n_1,\dots,n_r}$ besitzt Blöcke der Größe $n_1, \dots, n_r$ und alle möglichen Kanten dazwischen, also $|E| = n_1 + \dots + n_r$ und $|K| = n_1 \cdots n_r$.
- Ein k-regulärer Graph ist ein Graph, dessen sämtliche Ecken Grad k haben. Beispielsweise ist C_n 2-regulär und K_n $(n-1)$-regulär.
- Ein planarer Graph ist ein in die reelle Ebene einbettbarer Graph, d.h. ein Graph, den man zeichnen kann, ohne daß sich die Kanten überschneiden. Man überzeuge sich, daß K_5 und $K_{3,3}$ nicht planar sind. Jeder nicht-planare Graph enthält in einem technischen Sinne einen dieser beiden Graphen.

Darstellungen von Graphen

graphisch:



als Adjazenzmatrix:

$$\begin{matrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{matrix}$$

als Inzidenzmatrix:

$$\begin{matrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{matrix}$$

Dabei hängt die Darstellung als Adjazenzmatrix von einer Numerierung der Ecken ab; die Darstellung als Inzidenzmatrix von Numerierungen der Ecken und der Kanten. Bei der graphischen Darstellung hat man die Wahl, wie man die Ecken zueinander plaziert, und wie man die Kanten (nicht unbedingt gerade) zieht. Den obigen Graphen kann man zum Beispiel auch überschneidungsfrei zeichnen.

Zwei Graphen $G = (E, K)$ und $G' = (E', K')$ heißen isomorph, wenn es einen Isomorphismus zwischen G uind G' gibt, d.i. eine Bijektion $\varphi : G \to G'$ mit $\{e, e'\} \in K \iff \{\varphi(e), \varphi(e')\} \in K'$. Ein Isomorphismus von G auf sich selbst heißt Automorphismus.

Es ist i.a. kein leichtes Problem zu entscheiden, ob zwei Darstellungen (auch der gleichen Art) isomorphe Graphen ergeben. Dieses Problem ist nicht NP-vollständig, man kennt aber nur in Spezialfällen polynomiale Algorithmen (etwa für planare Graphen oder für Graphen beschränkter Valenz).

Ein Graph $G' = (E', K')$ heißt Untergraph von $G = (E, K)$, falls $E' \subseteq E$ und $K' \subseteq K$ gilt. Man sagt dann auch, daß G den Graphen G' enthält. G' heißt induzierter Untergraph, falls zusätzlich $K' = K \cap \mathfrak{P}_2(E')$ gilt, d.h. G' enthält alle zwischen Ecken aus E' in G vorhandenen Kanten. Zu jeder Teilmenge E' gibt es genau einen induzierten Untergraphen mit Eckenmenge E', dieser wird mit $G[E']$ bezeichnet. G' heißt aufspannender Untergraph von G, falls G' ein Untergraph von G mit $E = E'$ ist. (Insbesondere ist G der einzige aufspannende induzierte Untergraph von sich selbst.)

Varianten von Graphen

In Multigraphen läßt man Schlingen und mehrere Kanten zwischen zwei Ecken zu. Multigraphen tauchen auf natürliche Weise in der Graphentheorie auf, etwa wenn man duale Graphen betrachtet, so daß manchmal Multigraphen einfach als Graphen bezeichnet werden.

Bei gerichteten Graphen haben die Kanten eine Orientierung, also festgelegte Anfangs– und Endpunkte. Man läßt dann auf jeden Fall zwischen zwei Ecken Kanten in beide Richtungen zu und meist auch Schlingen.

In numerierten Graphen sind die Ecken wohlunterschieden; man kann sie sich als fest von 1 bis n durchnumeriert denken. Numerierte Graphen haben als solche also keine nicht-trivialen Automorphismen.

In Anwendungen betrachtet man oft gewichtete Graphen: G trägt dann noch eine Kosten– oder Gewichtsfunktion, entweder auf den Ecken als $w : E \to \mathbb{R}_0^+$, oder auf den Kanten als $w : K \to \mathbb{R}_0^+$. Letzteres könnte etwa eine Straßenkarte mit Abständen zwischen Städten sein. Geht die Gewichtsfunktion in eine endliche Menge von "Farben", spricht man auch von gefärbten Graphen.

Anzahl der Graphen

Wieviele Graphen mit n Ecken gibt es? Numeriert man die Ecken, hat man für jedes Eckenpaar die zwei Möglichkeiten, eine Kante zu ziehen oder nicht. Also existieren $2^{\binom{n}{2}}$ viele numerierte Graphen auf n Ecken. Man kann die n Ecken auf $n!$ viele Arten mumerieren;

verschiedenen Numerierungen führen aber eventuell zu isomorphen numerierten Graphen, und zwar genau dann, wenn die eine durch einen Automorphismus des Graphen in die andere übergeht. Man kann aber zeigen, daß für große n fast kein Graph nicht-triviale Automorphismen besitzt. Asymptotisch hat man also oben jeden Graph $n!$ mal gezählt; es gilt

$$\text{Anzahl der Graphen auf } n \text{ Ecken} \sim \frac{1}{n!} \cdot 2^{\binom{n}{2}}$$

Wege, Abstand, Zusammenhang

Definition 5.2 *Ein Weg der Länge n ist eine Folge $e_0k_1e_1 \dots k_ne_n$ von Ecken e_i und Kanten $k_i = \{e_{i-1}, e_i\}$. Dabei heißt e_0 der Anfangs– und e_n der Endpunkt des Weges. Ist $e_0 = e_n$, so heißt der Weg geschlossen, sonst offen.*

Ein (Kanten–) xZug ist ein Weg, bei dem $k_i \neq k_j$ für $i \neq j$ gilt.
Ein Pfad ist ein Weg, bei dem $e_i \neq e_j$ für $i \neq j$ gilt.
Ein Kreis ist ein Weg, bei dem $e_0 = e_n$ gilt, sonst aber $e_i \neq e_j$.

Achtung: diese Terminologie ist nicht standardisiert!

Ein Kreis ist also im Grunde ein geschlossener Pfad; Pfade sind allerdings per Definition offen. Jeder Pfad und jeder Kreis ist auch ein Zug. Man sagt, daß ein Weg mit Anfangspunkt e und Endpunkt e' die Ecken e und e' verbindet. Jeder e und e' verbindende Weg läßt sich zu einem e und e' verbindenden Pfad verkürzen. In G gibt s genau dann einen Kreis der Länge n, wenn C_n Untergraph von G ist.

Wir definieren auf E eine Äquivalenzrelation K^* durch eK^*e', falls e und e' durch einen Weg verbunden sind. Die Äquivalenzklassen von K^* heißen die Zusammenhangskomponenten des Graphen. Ein Graph heißt zusammenhängend, falls er aus nur einer Zusammenhangskomponente besteht, d.h. wenn je zwei Ecken durch einen Weg verbunden sind.

Algorithmus zum Finden der Zusammenhangskomponenten:

Starte in einer Ecke e_0. Sei $E_0 := \{e_0\}$ und $E_{i+1} := E_i \cup \bigcup_{e \in E_i} N(e)$. Halte an, falls $E_i = E_{i+1}$. Dann ist $G[E_i]$ die Zusammenhangskomponente von e_0. Falls $E_i = E$, so ist G zusammenhängend; falls nicht, starte mit einer neuen Ecke $e_0 \notin E_i$. Dieser Algorithmus berechnet in $O(|E|^2)$ vielen Schritten die Zusammenhangskomponenten und/oder testet, ob G zusammenhängend ist.

Der Abstand $d(e,e')$ zweier Ecken ist definiert als die minimale Länge eines e und e' verbindenden Weges, falls ein solcher existiert, und als ∞ sonst. Es gilt dann

$$\begin{aligned}
d(e,e') = 0 &\iff e = e' \\
d(e,e') = 1 &\iff e \text{ und } e' \text{ sind benachbart} \\
d(e,e') = 2 &\iff e \text{ und } e' \text{ haben gemeinsamen Nachbarn, aber } e \neq e', e \notin N(e') \\
d(e,e') = \infty &\iff e \text{ und } e' \text{ liegen in verschiedenen Zusammenhangskomponenten}
\end{aligned}$$

Satz 5.2 *Ein nicht trivialer Graph ist genau dann bipartit, wenn alle Kreise darin gerade Länge haben.*

□ "$\Rightarrow$" Ein Kreis in einem bipartiten Graphen muß abwechselnd zwischen Ecken aus den beiden Blöcken der Bipartition verlaufen, hat also gerade Länge.

"$\Leftarrow$" Sei $e_0 \in E$ beliebig und definiere $E' := \{e \in E \,|\, d(e_0, e) \text{ gerade}\}$, $E'' := E \setminus E' = \{e \in E \,|\, d(e_0, e) \text{ ungerade}\}$. Zeige: dies liefert eine Bipartition des Graphen. Angenommen es gibt eine Kante k zwischen $e, e' \in E'$ (analog für E''). Betrachte Pfade minimaler Länge von e_0 nach e bzw. e'. Sei e'' deren letzter gemeinsamer Punkt: dann ist die Länge beider Teilpfade von e_0 nach e'' die gleiche, d.h. die Restpfade zusammen mit k ergeben einen Kreis ungerader Länge: Widerspruch. □

II.6 Besondere Wege

Euler–Züge

Meist schon als Kind beschäftigt man sich mit Graphentheorie, nämlich mit dem Problem, das „Haus des Nikolaus" ohne Absetzen zu zeichnen. Tatsächlich gilt dieses Problem in der Form des „Königsberger Brückenproblems" auch als der mathematische Anfang der Graphentheorie. Euler hat gezeigt, daß ein Spaziergang durch das damalige Königsberg, der alle Brücken genau einmal überquert, nicht möglich ist. Die mathematische Modellisierung des Stadtplans führt natürlich zu einem Multigraphen; durch zusätzliche Ecken, etwa auf den Brücken, erhält man aber ein gleichwertiges Problem für einfache Graphen.

Definition 6.1 *Ein Eulerscher Zug in einem Graphen ist ein alle Kanten durchlaufender Zug.* G *heißt Eulersch, falls es in* G *einen (geschlossenen) Euler–Zug gibt.*

Satz 6.1 *Ein Graph ohne isolierte Punkte hat genau dann einen geschlossenen (bzw. offenen) Eulerschen Zug, wenn er zusammenhängend ist und keine (bzw. genau zwei) Ecken ungeraden Grades besitzt.*

□ Die Bedingungen sind offenbar notwendig. Durch Hinzufügen einer neuen verbindung zwischen den beiden Ecken ungeraden Grades führt man das Problem des offenen Euler–Zuges auf das andere zurück. Betrachte dann einen Zug maximaler Länge $e_0 k_1 \ldots k_n e_n$. Es gilt dann $e_0 = e_n$, da sonst nur eine ungerade Anzahl zu e_n inzidenter Kanten in dem Zug vorkäme, dieser also noch verlängert werden könnte. Gäbe es nun eine in dem Zug nicht vorkommende Kante k, so gäbe es auch eine (da G zusammenhängend), die mit einer der vorkommenden Ecken e_i inzident ist. Beginne dann obigen Zug mit e_i und hänge am Ende k an: Widerspruch. □

Dieser Beweis ist im Prinzip konstruktiv, d.h. man kann daraus einen Euler–Zug gewinnen, aber umständlich. Hier folgt ein besserer Algorithmus:

Algorithmus zur Konstruktion von Euler–Zügen:

Starte in einer beliebigen Ecke e_0 bzw. in einer der beiden Ecken ungeraden Grades. Sei der Anfang $e_0 k_1 e_1 \ldots k_i e_i$ des Euler–Zuges bereits konstruiert. Sei $G_i := (E, K_i)$ mit

$K_i := K \setminus \{k_1, \dots, k_i\}$ der Restgraph. Falls $K_i = \emptyset$, so fertig. Falls $K_i \neq \emptyset$, aber keine zu e_i inzidente Kante enthält, so Abbruch. Falls K_i eine zu e_i inzidente Kante enthält, die keine Brücke in G_i ist, so wähle eine dieser als k_{i+1}. Andernfalls wähle beliebige zu e_i inzidente Kante aus K_i als k_{i+1}.

Wie groß ist die Komplexität des Algorithmus? Er läuft höchstens $|K|$ Schritte lang. In jedem Schritt müssen $|K_i|$ viele Kanten daraufhin getestet werden, ob sie zu e_i inzident sind und ob ein Graph mit $|E|$ Ecken zusammenhängend ist. Letzteres ist in $O(|E|^2)$ möglich. Insgesamt ist der Algorithmus also in $O(|K|^2 \cdot |E|^2) \subseteq O(|E|^6)$, insbesondere polynomial.

Hamiltonsche Kreise

Definition 6.2 *Ein Hamiltonscher Kreis in einem Graphen ist ein alle Ecken druchlaufender Kreis.* G *heißt Hamiltonsch, falls es in* G *einen Hamiltonschen Kreis gibt.*

G ist also genau dann Hamiltonsch, wenn G einen aufspannenden Kreis enthält. Das Hamilton–Problem ist das Analogon des Euler–Problems für Ecken statt für Kanten: erstaunlicherweise ist es viel schwerer zu lösen. Historisch tauchte es bei Hamilton für den Dodekaeder auf.

Beispiele: K_n, der Würfel, der Dodekaeder sind Hamiltonsch. $K_{2n,2m+1}$ ist nicht Hamiltonsch.

Es gibt einen naheliegenden Algorithmus zu entscheiden, ob ein Graph Hamiltonsch ist oder nicht: erzeuge alle Kreise des Graphen und überprüfe, ob eines davon alle Ecken durchläuft. Aber: im K_n etwa gibt es $(n-1)!$ viele Kreise mit gegebenem Anfangspunkt; in einem beliebigen Graphen muß man daher auch erwarten, daß es zu viele sind, um in vernünftiger Zeit obigen Algorithmus durchführen zu können. Man kennt bis heute keinen „vernünftigen" Algorithmus, einen Hamiltonschen Kreis zu finden, und kein vernünftiges notwendiges und hinreichendes Kriterium für seine Existenz. Man hat allerdings gute Gründe, einen solchen Algorithmus nicht zu erwarten: das Hamilton–Problem ist nämlich ein sogenanntes NP–vollständiges Problem. Es gibt aber eine Reihe von hinreichenden Kriterien, von denen das einfachste folgt:

Satz 6.2 *Sei* $G = (E, K)$ *so, daß* $n := |E| \geqslant 3$ *und* $d(e) \geqslant \frac{n}{2}$ *für alle* $e \in E$. *Dann ist* G *Hamiltonsch.*

□ Zunächst ist G zusammenhängend: sonst hätte eine Ecke in einer minimalen Zusammenhangskomponente mehr Nachbarn als möglich. Betrachte dann einen Pfad $P = e_0k_1e_1 \dots k_me_m$ maximaler Länge. Dann muß P alle Nachbarn von e_0 und e_m bereits enthalten, sonst könnte man ihn verlängern. Betrachte $I_1 := \{i \mid e_i \in N(e_m)\}$ und $I_2 := \{i \mid e_{i+1} \in N(e_0)\}$. Beides sind Teilmengen von $\{0, \dots, m-1\}$ der Mächtigkeit mindestens $\frac{n}{2}$, also schneiden sie sich. Es gibt also i, eine Kante $k = \{x_0, x_{i+1}\}$ und eine Kante $k' = \{x_i, x_m\}$. Aus P, k, k' erhält man einen Kreis der Länge $m + 1$, aus dem wiederum, wäre er nicht bereits Hamiltonsch, ein Pfad der Länge $m + 1$ im Widerspruch zur Maximalität von P zu gewinnen wäre. □

Diesen Beweis kann man leicht in einen polynomialen Algorithmus zur Konstruktion eines Hamiltonschen Kreises umformen.

Die Klasse der Probleme, die man in polynomialer Zeit lösen kann, heißt P. Die Klasse der Probleme, für die man in polynomialer Zeit feststellen kann, ob eine vorgeschlagene Lösung stimmt oder nicht, heißt NP. Das Problem der Euler–Züge ist also in P; man sieht sofort, daß das Hamilton–Problem in NP liegt. Ebenfalls ist es nicht schwierig, $P \subseteq NP$ zu zeigen. Ob $P = NP$ gilt, ist eine der großen offenen Fragen der Mathematik und theoretischen Informatik, allgemein wird Ungleichheit angenommen. NP–vollständige Probleme sind nun „maximal schwierige" Probleme in der Klasse NP: jedes andere NP–Problem läßt sich in polynomialer Zeit darauf zurückführen, oder anders ausgedrückt: findet man einen polynomialen Algorithmus für ein NP–vollständiges Problem, so gilt $P = NP$. Daher gelten NP–vollständige Probleme als schwer. Trotzdem kann es sehr gute Näherungsalgorithmen geben oder welche, die in den meisten Fällen ein Ergebnis liefern.

Problem des Handlungsreisenden

Gegeben ist hier ein zusammenhängender Graph $G = (E, K)$ mit einer Gewichtsfunktion $w : K \to \mathbb{R}_0^+$. Für einen Weg $W = e_0 k_1 e_1 \dots k_n e_n$ definiere das Gewicht des Weges durch $w(W) := \sum\limits_{i=1}^{n} w(k_i)$. Das Problem des Handlungsreisenden besteht nun darin, einen alle Ecken durchlaufenden (geschlossenen) Weg minimalen Gewichts zu finden. Als Variante des Problems kann man auch nach einem Hamiltonschen Kreis minimales Gewichts fragen.

Bemerkungen:

- Ohne Einschränkunng kann man G als vollständig annehmen, indem man neue Kanten mit einem Gewicht größer als die Summe der bisherigen Gewichte hinzunimmt.
- Falls w Abstände angibt oder allgemeiner die Dreiecksungleichung erfüllt, so ist ein geschlossener Weg minimalen Gewichts automatisch Hamiltonsch.
- Falls w konstant auf allen Kanten ist, so ergibt sich das Hamilton–Problem als Spezialfall des Problems des Handlungsreisende. In diesem Sinne ist letzteres also schwerer.
- An einfachen Beispielen bereits sieht man, daß der naheliegende Algorithmus der lokalen Wahl, d.h. in jeder bereits erreichten Ecke die Kante minimalen Gewichts zu wählen, i.a. nicht den Gesamtweg minimalen Gewichts liefert.

Das Problem des Handlungsreisenden ist ebenfalls NP–vollständig; im Gegensatz zu dem vorherigen Entscheidungsproblem „Gibt es einen Hamiltonschen Kreis oder nicht" aber ein Optimierungsproblem.

Kürzeste Wege

Zum Abschluß dieses Abschnittes eine verwandte Fragestellung, für die es einen guten Algorithmus gibt. Gegeben ist wieder ein zusammenhängender gewichteter Graph $G = (E, K)$, $w : K \to \mathbb{R}_0^+$. Nun möchte man für zwei gegebene Ecken e und e' den beide verbindenden Weg minimalen Gewichts finden. Klar ist, daß solch ein Weg in zusammenhängenden Graphen existiert, er braucht allerdings nicht eindeutig zu sein, und daß er ein Pfad ist.

Man kann leicht Beispiele konstruieren, bei denen es nicht ausreicht, sich von e schrittweise nach e' vorzutasten, indem man in jedem Schritt eine zu e' hinführende, noch nicht benutzte Kante minimalen Gewichts wählt. Eine geringe Variante dieser lokalen wahl genügt allerdings, indem man einerseits gleichzeitig Pfade minimalen Gewichts von e zu allen anderen Ecken konstruiert und andererseits das Gewicht des bereits konstruierten Pfades beachtet.

Algorithmus zur Konstruktion von Wegen minimalen Gewichts:

Definiere induktiv e_i, $l(e_0, e_i)$ und k_i für $i \geqslant 1$.

e_0 sei die Startecke, $l(e_0, e_0) := 0$. Im $i+1$-ten Schritt, berechne für alle Paare (e, e_j) mit $e \notin \{e_0, \ldots, e_1\}$ und $e \in N(e_j)$, $j \leqslant i$, die Größe $w(\{e, e_j\}) + l(e_0, e_j)$ und wähle (e, e_j) so, daß sie minimal wird. Setze dann $e_{i+1} := e$, $k_i = \{e_j, e\}$ und $l(e_0, e_{i+1}) = l(e_0, e_j) + w(k_i)$. Breche ab, sobald die Zielecke erreicht ist bzw. bis keine neuen adjazenten Ecken mehr zur Verfügung stehen. Die Kanten k_i bilden dann einen aufspannenden Baum der Zusammenhangskomponente von e_0, in denen der eindeutige Pfad von e_0 zu jeder anderen Ecke minimales Gewicht hat.

Bemerkung: Für eine konstante Gewichtsfunktion berechnet der Algorithmus kürzeste Wege. Im allgemeinen wird der berechete aufspannende Baum kein aufspannender Baum minimalen Gewichts sein.

II.7 Färbungen

Eckenfärbungen

Gegeben sei ein Graph $G = (E, K)$. Eine <u>Eckenfärbung</u> (mit k Farben) ist eine Abbildung $c : E \to \{1, \ldots, k\}$, die benachbarte Ecken unterschiedlich färbt, d.h. $\{e, e'\} \in K \Longrightarrow c(e) \neq c(e')$. Ein Graph, für den eine Eckenfärbung mit k Farben existiert, heißt auch <u>k-färbbar</u>. Offenbar ist ein Graph genau dann k-färbbar, wenn er k-partit ist: die Blöcke der k-Partition werden durch die gleichgefärbten Ecken gebildet.

Beispiel: Man möchte die Länder einer Landkarte so färben, daß benachbarte Länder unterschiedliche Farben haben. Die Landkarte kann man in einen Graphen übersetzen, indem man die Hauptstädte als Ecken nimmt und Kanten zwischen den Hauptstädten zieht, deren Länder eine gemeinsame Grenze haben. Das berühmte <u>4–Farben–Problem</u> aus der Mitte des letzten Jahrhunderts fragte, ob dies stets mit 4 Farben möglich ist. Ein erster Beweis von 1977 führte das Problem auf etwa 1500 durch Computereinsatz überprüfte Einzelfälle zurück. Die mathematische Gültigkeit wurde deshalb und wegen der mangelnden Nachvollziehbarkeit bezweifelt. Seit kurzem gibt es kürzere, überschaubarere und akzeptiertere Beweise.

Es macht für die Anzahl der Farben keinen Unterschied, ob man Graphen auf der Ebene oder auf der Kugeloberfläche färbt: eine Landkarte auf einer Kugel wird im Inneren eines Landes aufgeschnitten und auf eine Ebene gezogen. Umgekehrt legt man um eine ebene Landkarte ein alles umfassendes neues Land, in dem man die Ebene zur Kugel zusammenbinden kann.

Hier soll bewiesen werden, daß jeder planare Graph 5-färbbar ist. Ohne Beweis seien folgende beiden Sätze zitiert:

Satz 7.1 (Appel, Haken, ...) *Jeder planare Graph ist 4-färbbar.*

Satz 7.2 (Grötzsch) *Jeder planare, dreiecksfreie Graph ist 3-färbbar.*

Sei ein planarer Graph $G = (E, K)$ gegeben. G grenzt dann eine Menge F von Flächen ab; denkt man sich G eingebettet in $\mathbb{R}^2$, so sind dies die Zusammenhangskomponenten von $\mathbb{R}^2 \setminus G$. Insbesondere ist dabei die Außenfläche mitgezählt; für ein Dreieck gilt etwa $|F| = 2$.

Satz 7.3 (Euler–Formel) *Für zusammenhängende planare Graphen gilt* $|F| - |K| + |E| = 2$.

□ Induktion nach $|E|$: der Satz gilt offenbar für den einpunktigen Graphen mit $|E| = 1$, $|K| = 0$ und $|F| = 1$. Eine neue Ecke e wird in eine Fläche f eingesetzt und über m viele Kanten verbunden. Dabei wird die Fläche f in m viele Flächen zerlegt, es kommen also $m - 1$ neue Flächen hinzu. □

Folgerung: In einem triangulierten Graphen gilt $|K| = 3 \cdot |E| - 6$.

□ G heißt trianguliert, falls alle auftretenden Flächen Dreiecke sind. Jede Fläche hat also 3 Kanten, aber jede Kante zählt für zwei Flächen, also $3 \cdot |F| = 2 \cdot |K|$. □

Folgerung: In jedem planaren Graphen gibt es eine Ecke vom Grad $\leqslant 5$.

□ Durch Hinzufügen von Kanten kann man annehmen, daß der Graph trianguliert ist. Hätte jede Ecke mindestens 6 Nachbarn, würde $|K| \geqslant \frac{1}{2} 6 \cdot |E| = 3 \cdot |E|$ gelten, im Widerspruch zur vorherigen Folgerung. □

Folgerung: K_5 ist nicht planar.

Satz 7.4 *Jeder planare Graph ist 5-färbbar.*

□ O.B.d.A. ist der Graph zusammenhängend, sonst färbe einzeln die Zusammenhangskomponenten. Induktion nach $|E|$; klar für $|E| \leqslant 5$. Im Induktionsschritt wähle e_0 mit $d(e_0) \leqslant 5$. Sei $N(e_0) = \{e_1, \dots, e_5\}$. Da G planar ist und also keine Kopie des K_5 enthalten kann, gibt es unter den Nachbarn von e_0 zwei nicht benachbarte Ecken e_i, e_j. Man betrachtet nun den Graphen G', der aus $G[E \setminus \{e_0\}]$ durch Zusammenziehen der Ecken e_i und e_j entsteht. Per Induktion gibt es eine 5-Färbung von G', aus der man eine 5-Färbung von $G[E \setminus \{e_0\}]$ erhält, in der e_i und e_j dieselbe Farbe tragen. Also sind nur 4 Farben für die Nachbarn von e_0 verwendet: man kann e_0 mit der fünften Farbe färben. □

Die chromatische Zahl $\chi(G)$ ist die kleinste Zahl k, so daß G k-färbbar ist. Es gibt eine Vermutung, daß $\chi(G)$ eng damit zusammenhängt, welche vollständigen Graphen in einem gewissen technischen Sinn in G enthalten sind.

Kantenfärbungen

Unter einer Kantenfärbung (mit k Farben) versteht man in der Regel eine Abbildung $c : K \to \{1, \ldots, k\}$, die aneinanderstoßende Kanten unterschiedlich färbt, d.h. $k \cap k' \neq \emptyset \Longrightarrow c(k) \neq c(k')$. Man kann nun ähnliche Fragen wie für Eckenfärbungen stellen.

Als Anwendungsbeispiel kann man sich einen Turnierplan vorstellen: Ecken repräsentieren Mannschaften, die Farben der Kanten entsprechen Spieltagen.

Der Satz von Ramsey

Nun soll ein duales Problem behandelt werden: statt Graphen so zu färben, daß keine gleichfarbigen Kanten aufeinanderstoßen, sollen in einem gefärbten Graphen möglichst große einfarbige Stücke gefunden werden. Dazu betrachten wir $G = (E, K)$ und eine Abbildung $c : K \to \{1, \ldots, k\}$ ohne Zusatzbedingung. Dies ist also keine Kantenfärbung im obnigen Sinn, soll der Einfachheit halber aber auch Färbung genannt werden. Ein induzierter Untergraph $G' = (E', K')$ heißt einfarbig, falls $c\restriction_{K'}$ konstant ist.

Auf K_5 gibt es eine 2-Färbung ohne einfarbiges Dreieck: man färbe ein Fünfeck in einer Farbe, das verbleibende mit der anderen. Auf K_6 dagegen hat man notwendig ein einfarbiges Dreieck: eine fest gewählte Ecke ist mit drei Ecken gleichfarbig verbunden. Ein Dreieck des aus den vier Ecken bestehenden Tetraeders muß einfarbig sein. Dies ist ein allgemeines Phänomen:

Satz 7.5 (Ramsey) *Gegeben $r, k \in \mathbb{N}$, so gibt es ein $n \in \mathbb{N}$, so daß K_m mit $m \geqslant n$ für jede k-Färbung einen einfarbigen Untergraphen K_r enthält.*

□ Zunächst sei $k = 2$. Es reicht dann, $m = n$ zu betrachten, da die Eigenschaft mit Vergrößern der Eckenmenge erhalten bleibt. Wähle $n = 2^{2r-3}$ und konstruiere induktiv Teilmengen $E_i \subseteq E$, $e_i \in E_i$ und Farben $c_i \in \{1, 2\}$ für $i = 0, \ldots, 2r-3$ mit den Eigenschaften:

- $|E_i| = 2^{2r-3-i}$
- $E_{i+1} \subseteq E_i \setminus \{e_i\}$
- alle Kanten von e_i nach E_{i+1} haben die gleiche Farbe c_i.

Sei $E_0 = E$ und stets $e_i \in E_i$ beliebig. Sei E_i bereits gewählt. Da $|E_i \setminus \{e_i\}| = 2^{2r-3-i} - 1$, gibt es eine Teilmenge E_{i+1} der Größe $\lceil \frac{2^{2r-3-i}-1}{2} \rceil = 2^{2r-3-(i+1)}$ und eine Farbe c_i, die die obigen Bedingungen erfüllen.

In der $2r-1$ langen Folge $(c_0, c_1, \ldots, c_{2r-4})$ taucht eine Farbe c mindestens $\lceil \frac{2r-3}{2} \rceil = r - 1$ mal auf. Setze dann $c_{2r-3} := c$ und betrachte die Menge $R = \{e_i \mid c_i = c\}$. Es gilt $|R| = r$ und jede zwischen Ecken aus R verlaufende Kante trägt nach Definition die Farbe c.

Für $k > 2$ ändert man entweder den Beweis entsprechend ab, oder schließt induktiv, indem man zunächst die k Farben in zwei Gruppen einordnet. □

Der Satz von Ramsey hat viele Verallgemeinerungen und ist von großer Nützlichkeit in vielen Teilen der Mathematik. Sein Inhalt wird gerne durch die Aussage „totale Unordnung ist unmöglich" paraphrasiert. Im Beweis ergaben sich obere Schranken für die Wahl von n. Man kennt bessere obere Schranken und auch untere Schranken. Nennt man den genauen Wert $R(r,k)$, so wurde am Anfang $R(3,2) = 6$ gezeigt. Andere bekannte Werte sind $R(4,2) = 18$ und $R(3,3) = 17$, aber schon für relativ kleine r und k ist $R(r,k)$ unbekannt.

II.8 Bäume

Definition 8.1 *Ein* Baum *ist ein zusammenhängender kreisfreier Graph. Ein* Wald *ist ein kreisfreier Graph.*

Also ist ein Baum ein zusammenhängender Wald und die Zusammenhangskomponenten eines Waldes sind Bäume. Ecken vom Grad 1 heißen Blätter. Jeder nicht-triviale Baum hat mindestens zwei Blätter. Ist e ein Blatt des Baumes $G = (E,K)$, so ist auch $G[E \setminus \{e\}]$ ein Baum. Dies erlaubt es oft, Eigenschaften von Bäumen per Induktion zu zeigen. Allgemeiner ist jeder Untergraph eines Waldes wieder ein Wald. Wälder sind offenbar bipartit bzw. 2-färbbar nach Satz 5.2.

Satz 8.1 $G = (E,K)$ *ist ein Baum*

$\iff$ *je zwei Ecken sind durch einen eindeutigen Pfad verbunden*

$\iff$ G *ist maximal zusammenhängend, d.h. zusammenhängend und jede Kante ist eine Brücke*

$\iff$ G *ist minimal azyklisch, d.h. kreisfrei, aber durch jede neue Kante zwischen vorhandenen Ecken entsteht ein Kreis*

$\iff$ G *ist zusammenhängend und* $|E| = |K| + 1$.

Satz 8.2 *Jeder zusammenhängende Graph enthält einen aufspannenden Baum. Jeder Graph enthält einen aufspannenden Wald.*

□ Entferne solange Kanten aus Kreisen, bis keine Kreise mehr existieren. Da eine Kante in einem Kreis keine Brücke sein kann, wird Zusammenhang nicht zerstört. □

Dieser Beweis liefert zugleich einen Algorithmus, der allerdings nicht besonders effektiv ist. Der Algorithmus zur Konstruktion von Wegen minimalen Gewichts liefert für die konstante Gewichtsfunktion ebenfalls einen aufspannenden Baum. Zwei weitere Möglichkeiten sind:

Breitensuche: Starte in einer beliebigen Ecke mit Nummer 0 und gib im i-ten Schritt einem noch nicht numerierten Nachbarn einer Ecke mit minimaler Nummer die Nummer i.

Tiefensuche: Starte in einer beliebigen Ecke mit Nummer 0 und gib im i-ten Schritt einem noch nicht numerierten Nachbarn einer Ecke mit maximaler Nummer die Nummer i.

Der Breitensuchalgorithmus konstruiert flache, breitverzweigte Bäume, der Tiefensuchalgorithmus dagegen tiefe und schmale.

Wieviele Bäume mit n Ecken gibt es? Wie bei Graphen kann man nur numerierte Bäume explizit zählen. Anders betrachtet fragt man nach der Anzahl der aufspannenden Bäume eines K_n, bei dem man die Ecken unterscheiden kann. Dazu zunächst eine Definition:

Ein Wurzelbaum ist ein Baum mit einer ausgezeichneten Ecke, der sogenannten Wurzel. Jeder Wurzelbaum trägt eine natürliche Orientierung der Kanten, etwa von der Wurzel weg. Damit macht es Sinn, von Vorgängern und Nachfolgern einer Ecke zu sprechen. Blätter sind dann die Ecken ohne Nachfolger, die Wurzel die einzige Ecke ohne Vorgänger.

Satz 8.3 (Cayley) *Es gibt n^{n-2} numerierte Bäume auf n Ecken.*

□ Statt Bäume zählt ma Wirbeltiere, das sind Bäume mit zwei ausgezeichneten Ecken, dem Kopf K und dem Schwanz S. Es gibt also n^2 Möglichkeiten, K und S zu wähle ($K = S$ ist gestattet!), also behauptet der Satz von Cayley, daß es n^n Wirbeltiere mit n Ecken gibt. Dies ist aber genau die Anzahl der Funktionen der Menge $\{1, \dots, n\}$ in sich selbst. Zum Beweis wird also jedem Wirbeltier eineindeutig eine Funktion und umgekehrt zugeordnet.

Ein Wirbeltier ist bestimmt durch

- eine nicht-leere Teilmenge $R = \{e_1, \dots, e_r\} \subseteq E$, dem sogenannten Rückgrat, das aus den Ecken des eindeutigen K und S verbindenden Pfades besteht;
- einer Ordnung auf R, von K nach S;
- einer Aufteilung der Restecken $E \setminus R$ in r eventuell leere Teile $e_1, \dots, e_r$;
- einem Wurzelbaum auf $E_i \cup \{e_i\}$ mit Wurzel e_i.

Einer Funktion $f : \{1, \dots, n\} \to \{1, \dots, n\}$ ordnen wir zunächst den gerichteten Graphen mit Ecken $\{1, \dots, n\}$ und Kanten $(i, f(i))$ zu. Sei R die Menge der Ecken, die auf gerichteten Kreisen liegen. Auf R induziert f eine Permutation. Läßt man die Kanten der gerichteten Kreise fort, so bilden die Zusammenhangskomponenten des Restgraphen Wurzelbäume mit Wurzel in R und natürlicher Orientierung zur Wurzel hin.

Da es gleich viele Permutationen wie totale Ordnungen gibt, sind also Wirbeltiere und Funktionen durch gleichwertige Daten gegeben. Die Zuordnung von Permutation und totaler Ordnung ist allerdings nicht kanonisch, sondern bedarf einer Auswahl (dem Bild der Identitätspermutation etwa.) □

Häufig tauchen in Anwendungen sogenante Suchbäume auf. Dies sind Wurzelbäume (mit gedachter Orientierung von der Wurzel weg), bei der die Nachfolger einer Ecke geordnet sind. Solche Bäume tauchen als Modell für Entscheidungs– oder Suchvorgänge auf: jede Ecke steht für eine Entscheidung oder Anfrage, die auslaufenden Kanten für die Möglichkeiten oder Antworten. Suchbäume zählt man eher nach der Anzahl der Blätter. Ein (n, q)-Baum ist ein Suchbaum mit n Blättern, bei dem jede Ecke höchstens q direkte Nachfolger hat. Ein vollständiger (n, q)-Baum ist einer, bei dem jede Ecke, die kein Blatt ist, genau q Nachfolger hat. Zur Erinnerung: die Anzahl der vollständigen $(n, 2)$-Bäume ist C_n, die n-te Catalan–Zahl.

II.9 Optimierungsprobleme

Paarungen (Matchings)

Definition 9.1 *Eine Paarung in einem Graphen ist eine Menge von paarweise nicht-adjazenten Kanten (d.h. je zwei Kanten der Paarung haben keine End-Ecke gemeinsam). Die Paarungszahl $m(G)$ ist das Maximum der Mächtigkeiten von Paarungen in G. Eine Paarung P heißt maximal, falls $|P| = m(G)$.*

Es gilt offenbar stets $m(G) \leqslant \lfloor \frac{|E|}{2} \rfloor$; etwa $m(K_n) = m(C_n) = \lfloor \frac{n}{2} \rfloor$; dagegen $m(K_{1,n}) = 1$.

Es kann vorkommen, daß eine Paarung P nicht mehr durch Hinzufügen einer Kante zu einer größeren Paarung erweitert werden kann, ohne darum maximal zu sein.

Ein P-alternierender Pfad ist ein Pfad $e_0 k_1 e_1 \dots e_{2n+1}$ ungerader Länge mit nicht zu P inzidenten End-Ecken e_0, e_n und mit $k_i \in P \iff i$ gerade. Falls ein solcher P-alternierender Pfad existiert, so ist P nicht maximal, da man die in P vorkommenden Kanten des Pfades durch die anderen ersetzten kann. Tatsächlich gilt sogar die Umkehrung:

Satz 9.1 *P ist genau dann maximale Paarung, wenn es keine P-alternierenden Pfade gibt.*

□ Gibt es einen P-alternierenden Pfad wie oben, so ist eine größere Paarung gegeben durch $P' := P \setminus \{k_2, k_4, \dots, k_{2n}\} \cup \{k_1, k_3, \dots k_{2n+1}\}$.

Sei umgekehrt P eine nicht-maximale Paarung ohne P-alternierenden Pfad. Wähle eine Paarung P' mit $|P'| = |P| + 1$ und betrachte $N := (P \setminus P') \cup (P' \setminus P)$. Dann ist $|N|$ ungerade. Die Zusammenhangskomponenten des von N aufgespannten Untergraphen sind entweder zwischen P und P' alternierende Kreise (mit gerader Kantenzahl) oder zwischen P und P' alternierende Pfade. Da die Gesamtkantenzahl ungerade ist mit mehr Kanten aus P' als aus P, muß es einen solchen Pfad mit Anfangs- und Endkante aus P' geben. Dies ist dann aber ein P-alternierender Pfad: wären die End-Ecken P-inzident, so mit einer Kante aus $P \cap P'$, was unmöglich ist, da P' eine Paarung ist. □

Dieser Satz ist konstruktiv, d.h. er liefert einen (sogar polynomialen) Algorithmus zur Konstruktion maximaler Paarungen, indem man nach und nach P-alternierende Pfade bestimmt und jedesmal die Paarung entsprechend vergrößert.

Paarungen werden meist in bipartiten Graphen betrachtet – oft handelt es sich um Zuordnungsprobleme, wie im berühmten Beispiel des Heiratsproblems: ist es möglich, n Frauen mit n Männern, von denen manche untereinander befreundet sind, so zu verheiraten, daß nur befreundete Paare heiraten? Die Personen werden durch die Ecken, die Freundschaftsrelation durch die Kanten eines bipartiten Graphen wiedergegeben; die Auswahl von Ehepartnern ist eine Paarung.

Für $A \subseteq E$ sei $N(A) := \{e \in E \mid \exists a \in A \{e, a\} \in K\} = \bigcup\limits_{a \in A} N(a)$ die Menge der Nachbarn von A. Die Heiratsbedingung für E' sei die Eigenschaft $|A| \leqslant |N(A)|$ für alle $A \subseteq E'$.

Satz 9.2 (Heiratssatz von Hall) *Sei $G = (E, K)$ ein Graph mit Bipartition $E = E' \dot\cup E''$. Dann gilt $m(G) = |E'|$ genau dann, wenn G die Heiratsbedingung für E' erfüllt.*

□ "$\Rightarrow$" ist klar, da eine maximale Paarung für jedes $a \in A$ einen verschiedenen Nachbarn aus E'' auswählt.

"$\Leftarrow$" Sei P eine maximale Paarung. Angenommen, $e_0 \in E'$ ist dazu nicht inzident. Konstruiere aufgrund der Heiratsbedingung $e_i \in E'$ und $f_i \in E''$ mit $\{e_i, f_i\} \in P$ und $\{f_1, \dots, f_k\} \subseteq N\big(\{e_0, \dots, e_{k-1}\}\big)$, bis ein zu P nicht inzidentes f_m gefunden ist. Von f_m kann man nun einen P-alternierenden Pfad rückwärts verfolgen: Widerspruch zur Maximalität. □

Satz 9.3 *Sei* G *wie oben. Dann gilt* $m(G) = |E'| - \max\limits_{A \subseteq E'} \big\{|A| - |N(A)|\big\}$.

□ Offenbar sind für jede Paarung P und jedes $A \subseteq E'$ mindestens $|A| - |N(A)|$ viele Ecken nicht inzident zu P, woraus "$\leqslant$" folgt. Sei nun $A' \subseteq E'$ so, daß obiges Maximum für A' angenommen wird. Dann erfüllt einerseits $G[(E' \setminus A') \cup (E'' \setminus N(A'))]$ die Heiratsbedingung bezüglich $E' \setminus A'$: gäbe es ein widersprechendes $A'' \subseteq E' \setminus A'$, so wäre $|A' \cup A''| - |N(A' \cup A'')| > |A'| - |N(A')|$. Andererseits erfüllt aus analogen Gründen $G[A' \cup N(A')]$ die Heiratsbedingung bezüglich $N(A')$. Man wähle jeweils eine maximale Paarung: zusammen ergeben diese eine Paarung von G der gewünschten Größe. □

Eine Eckenüberdeckung in einem Graphen ist eine Menge von Ecken, zu der jede Kante inzident ist.

Satz 9.4 (König) *Die minimale Mächtigkeit einer Eckenüberdeckung eines bipartiten Graphen ist gleich* $m(G)$.

□ Offenbar gilt "$\leqslant$", da für jede Kante in einer Paarung eine (verschiedene) Ecke in der Überdeckung sein muß. Umgekehrt ist wie in obigem Beweis $(E' \setminus A') \cup N(A')$ eine Eckenüberdeckung der Mächtigkeit $m(G)$. □

Der Satz von König ist ein Beispiel für ein in der Graphentheorie häufig auftretendes "Dualitätsphänomen": die minimale Lösung eines Problems entspricht der maximalen Lösung eines dualen Problems.

Anwendungsbeispiel des Heiratssatzes:
Sei M eine Menge und $\{M_i \mid i \in I\}$ eine endliche Familie von Teilmengen von M. Dann heißt eine injektive Funktion $f : I \to M_i$ eine Auswahlfunktion, falls $f(i) \in M_i$ für alle $i \in I$. Solch einer Situation ordnet man einen bipartiten Graphen mit Eckenmenge $M \dot\cup I$ und Kanten $\{m, i\} \iff m \in M_i$ zu. Eine Auswahlfunktion entspricht dann genau einer maximalen Paarung. Sie existiert also genau dann, wenn $|\bigcup_{j \in J} M_j| \geqslant |J|$ für alle $J \subseteq I$ ist.

Gewichtete Paarungen

Sei nun zusätzlich auf dem bipartiten Graphen $G = (E' \dot\cup E'', K)$ eine Gewichtsfunktion $w' : K \to \mathbb{R}_0^+$ gegeben, und eine Paarung minimalen Gewichts gesucht. Wie üblich, ist das Gewicht einer Paarung P definiert als $w'(P) := \sum\limits_{k \in P} w'(k)$.

Zunächst kann man durch Hinzufügen neuer Ecken und neuer Kanten mit Gewicht 0 annehmen, daß $G = K_{n,n}$ mit $E' = \{e_1, \ldots, e_n\}$ und $E'' = \{f_1, \ldots, f_n\}$. Sei $w'_{max} := \max_{k \in K} w'(k)$. Betrachtet man die Gewichtsfunktion $w := w' - w'_{max}$, so ist das Ausgangsproblem äquivalent dazu, eine maximale Paarung minimalen Gewichts bzgl. w zu finden.

Den bipartiten gewichteten Graphen kann man nun geschickt durch eine (n, n)-Matrix W mit Einträgen $w_{ij} = w(\{e_i, f_j\})$ darstellen. Eine maximale Paarung entspricht nun einer sogenannten Diagonalen, d.h. einer Auswahl von n Einträgen der Matrix, von denen keine zwei in einer Spalte oder einer Zeile liegen. Ziel ist es nun, eine Diagonale minimaler Summe zu finden. Offenbar ändert man an der Lösungsmenge nichts, wenn man von einer Spalte bzw. einer Zeile einen festen Betrag abzieht.

Algorithmus zum Finden einer minimalen Diagonalen:
1. Schritt: Ziehe zunächst von jeder Zeile den minimalen Zeileneintrag ab, dann in der entstehenden Matrix von jeder Spalte den minimalen Spalteneintrag ab. Ersetze W durch die verbleibende Matrix.

2. Schritt: Gibt es in W eine Diagonale aus lauter Nullen? Eine solche Diagonale entspricht einer maximalen Paarung in dem bipartiten Graphen $G' = (E, K')$ mit $K' = \big\{\{e_i, f_j\} \,\big|\, w_{ij} = 0\big\}$, wofür es im vorigen Abschnitt einen Algorithmus gab.

Wenn ja liefert diese eine Paarung minimalen Gewichts.

Wenn nein, so suche eine Überdeckung sämtlicher in W vorkommenden Nullen durch eine minimale Anzahl von Spalten und Zeilen. Eine solche Überdeckung entspricht einer Eckenüberdeckung in G' und besteht daher nach dem Satz von König aus weniger als n Spalten und Zeilen. Sei m das Minimum der nicht-überdeckten Werte. Ziehe m von allen nicht-überdeckten Zeile ab und addiere es zu den überdeckten Spalten. Ersetze W durch die entstandene Matrix und wiederhole Schritt 2.

Da in jedem Schritt die Anzahl der auftretenden Nullen erhöht wird, stoppt der Algorithmus nach endlich vielen Schritten. Man kann sich leicht überlegen, daß der Algorithmus polynomial ist.

Flüsse in Netzwerken

Ein gerichteter Graph ist ein Paar (E, K) bestehend aus einer (endlichen) Eckenmenge E und einer Menge gerichteter Kanten $K \subseteq E^2$. Für $k = (e, e') \in K$ sei $e = k^-$ die Anfangs– oder Startecke, $e' = k^+$ die End– oder Zielecke der Kante. Für eine Ecke e definiert man den Ein-Grad $d^+(e) := |\{k \mid e = k^+\}|$ als die Anzahl der hineinlaufenden Kanten und den Aus-Grad $d^-(e) := |\{k \mid e = k^-\}|$ als die Anzahl der hinauslaufenden Kanten.

Jedem gerichteten Graphen liegt ein ungerichteter Graph zugrunde: dieser hat dieselben Ecken und Kanten, wobei man die Orientierungen vergißt, Schleifen wegläßt und eventuelle Mehrfachkanten identifiziert. Formal ergibt sich $G' = (E, K')$ mit $\{e, e'\} \in K' \iff [e \neq e' \text{ und } (e, e') \in K \text{ oder } (e', e) \in K]$.

Ein gerichteter Weg, der Länge n, von e_0 nach e_n, ist eine Folge $e_0 k_1 e_1 \ldots k_n e_n$ von Ecken e_i und Kanten $k_{i+1} = (e_i, e_{i+1})$. Entsprechend sind gerichtete Züge, Pfade und Kreise definiert. Die Eigenschaft, daß es zwischen zwei Ecken e, e' einen gerichteten Weg von e nach e' und einen gerichteten Weg von e' nach e gibt, definiert eine Äquivalenzrelation, deren Klassen starke Zusammenhangskomponenten heißen. Die starken Zusammenhangskomponenten sind Vereinigungen gerichteter Kreise. Ein gerichteter Graph heißt stark zusammenhängend, falls er nur aus einer starken Zusammenhangkomponente besteht, und (schwach) zusammenhängend, falls der zugrundeliegende ungerichtete Graph zusammenhängend ist.

Definition 9.2 *Ein Netzwerk ist ein gerichteter Graph* $G = (E, K)$ *mit zwei ausgezeichneten Ecken* $e_{ein} \neq e_{aus}$*, so daß ein gerichteter Weg von* e_{ein} *nach* e_{aus} *existiert, und einer Kapazitätsfunktion* $c : K \to \mathbb{R}_0^+ \cup \{\infty\}$.

Man nennt e_{ein} den Eingang, e_{aus} den Ausgang des Netzwerkes und alle anderen Ecken innere Ecken. Allgemeiner könnte es mehrere Ein– und Ausgänge geben; dies reduziert man auf obigen Fall, indem man je einen neuen Ein– und Ausgang hinzunimmt mit Kanten unendlicher Kapazität zu bzw. von den alten Ein– bzw. Ausgängen. Manchmal erlaubt man eine Rückflußkante von e_{Aus} nach e_{ein} mit unendlicher Kapazität.

Ein Fluß in einem gerichteten Graphen $G = (E, K)$ ist eine Funktion $f : K \to \mathbb{R}_0^+$. Der Wert des Flusses f in einer Ecke e ist die Differenz von Einfluß und Ausfluß, d.h. $w_e(f) := \sum_{e=k^+} c(k) - \sum_{e=k^-} c(k)$; der Wert des Flusses $w(f)$ ist sein Wert im Augang e_{Aus}.

Definition 9.3 *Ein Fluß* f *in einem Netzwerk* $G = (E, K, c)$ *heißt verträglich, falls einerseits* $f(k) \leqslant c(k)$ *für alle Kanten* k *gilt und andererseits der Wert des Flusses an allen inneren Ecken gleich Null ist („Kirchhoffs Gesetz“).*

Da offenbar stets $\sum_{e \in E} w_e(f) = 0$ gilt, folgt für einen verträglichen Fluß $w(f) = -w_{e_{ein}}(f)$.

Problem: Man finde einen verträglichen Fluß maximalen Wertes.

Satz 9.5 *Ein verträglicher Fluß maximalen Wertes existiert stets.*

□ Sei $\{f_i \mid i \in I\}$ die Menge der verträglichen Flüsse. Falls der Wert w darauf kein Maximum annimmt, so gibt es eine Teilfamilie $\{f_{i_j} \mid j \in \mathbb{N}\}$ mit $\sup\{w(f_{i_j}) \mid j \in \mathbb{N}\} = \sup\{w(f_i) \mid i \in I\}$ und so, daß $(f_{i_j}(k))_{j \in \mathbb{N}}$ für jede Kante k eine monotone Folge bildet. Man rechnet leicht nach, daß dann durch $f(k) := \lim_{j \in \mathbb{N}} f_{i_j}(k)$ ein verträglicher Fluß definiert wird mit Wert $w(f) = \sup\{w(f_i) \mid i \in I\}$: Widerspruch. □

Ein Schnitt (X, Y) ist eine Partition $E = X \dot\cup Y$ der Eckenmenge mit $e_{ein} \in X$ und $e_{aus} \in Y$. Sei $K(X, Y) = \{k \in K \mid k^- \in X, k^+ \in Y\}$ die Menge der von X nach Y laufenden Kanten. Die Kapazität des Schnittes ist $c(X, Y) := \sum_{k \in K(X,Y)} c(k)$.

Bemerkung Für jeden verträglichen Fluß f und jeden Schnitt (X, Y) gilt $w(f) \leqslant c(X, Y)$.

Denn: $w(f) = w_{e_{aus}} = \sum_{e \in Y} w_e(f) = \sum_{e \in Y, e=k^+} f(k) - \sum_{e \in Y, e=k^-} = \sum_{k \in K(X,Y)} f(k) = c(X, Y)$.

Es gilt nun auch die Umkehrung! Sei f ein verträglicher Fluß. Wir betrachten (ungerichtete) Züge $Z = e_0 k_1 e_1 \dots k_n e_n$ aus Ecken e_i und gerichteten Kanten k_i, wobei entweder k_i Vorwärtskante $k_i = (e_{i-1}, e_i)$ oder Rückwärtskante $k_i = (e_i, e_{i-1})$ ist. Ein zunehmender Zug für f ist solch ein Zug Z mit $f(k_i) < c(k_i)$ für alle Vorwärtskanten und $f(k_i) > 0$ für alle Rückwärtskanten. Die Restkapazität des zunehmenden Zuges ist

$$r_f(Z) := \min\Big(\big\{c(k_i) - f(k_i) \;\big|\; k_i \text{Vorwärtskante}\big\} \cup \big\{f(k_i) \;\big|\; k_i \text{Rückwärtskante}\big\}\Big)$$

Der zu Z gehörige elementare Fluß f_Z sei definiert durch $f_Z(k) = 1$ für alle Vorwärtskanten, $f_Z(k) = -1$ für alle Rückwärtskanten und $f_Z(k) = 0$ für alle in Z nicht vorkommenden Kanten. Dies ist kein Fluß im Sinne der obigen Definition, da er negative Werte annimmt; falls aber Z von e_{ein} nach e_{aus} läuft, so erfüllt f_Z die Verträglichkeitsbedingungen. Insbesondere ist dann $f + r_f(Z) \cdot f_Z$ ein verträglicher Fluß.

Außerdem definiert man $X_f := \{e \mid$ es gibt einen zunehmenden Zug von e_{ein} nach $e\}$ und $Y_f = E \setminus X_f$. Insbesondere gilt also $e_{ein} \in X_f$.

Satz 9.6 (Ford, Fulkerson) *Es sind äquivalent:*

- f *ist Fluß maximalen Wertes.*
- *Es gibt keine zunehmenden Züge von* e_{ein} *nach* e_{aus}.
- (X_f, Y_f) *ist ein Schnitt.*

Es gilt dann: (X_f, Y_f) *ist ein Schnitt minimaler Kapazität mit* $c(X_f, Y_f) = w(f)$.

□ (a)⇒(b) Wäre Z solch ein Zug, so wäre $f + r_f(Z) \cdot f_Z$ ein Fluß vom Wert $w(f) + r_f(Z)$.
(b)⇒(c) Alle Bedingungen eines Schnittes sind stets erfüllt bis auf $e_{aus} \in Y_f$, was gerade die Aussage von (b) ist.
(c)⇒(a) Für alle Kanten $k \in K(X_f, Y_f)$ gilt $f(k) = c(k)$, denn sonst könnte man den zu k^- hinführenden zunehmenden Zug noch um k verlängern. Es folgt $w(f) = c(X_f, Y_f)$, insbesondere ist f maximal. □

Man sieht, daß $K(X_f, Y_f)$ beim maximalen Fluß f aus lauter saturierten Kanten besteht, d.h. Kanten, in denen der Wert des Flusses gleich der Kapazität ist. Umgekehrt ist ein Fluß, der einen Schnitt aus saturierten Kanten zuläßt, schon maximal.

Folgerung aus dem Beweis: In einem Netzwerk mit ganzzahligen Kapazitäten gibt es einen maximalen ganzzahligen Fluß.

Algorithmus zum Finden eines maximalen Flusses:
Ausgehend von einem gegebenen Fluß (eventuell dem Null–Fluß), sucht man nach zunehmenden Zügen und addiert den mit der Restkapazität multiplizierten elementaren Fluß hinzu. Diese Züge sucht man am besten mit einem Tiefensuchalgorithmus.

Bei ganzzahligen (und damit auch bei rationalen) Kapazitäten ist klar, daß der Algorithmus terminiert, da sich der Wert des Flusses in jedem Schritt um mindestens 1 erhöht. Bei reellen Werten ist die Argumentation etwas schwieriger, ähnlich wie in 9.5.

Meist ist es geschickt, im Algorithmus zunächst nach gerichteten zunehmenden Zügen zu suchen. Gibt es keine solchen mehr, so hat man einen vollständigen Fluß erreicht, d.h. ein Fluß, in dem jeder gerichtete Zug von e_{ein} nach e_{aus} eine saturierte Kante enthält.

Aus dem Satz von Ford–Fulkerson erhält man ziemlich einfach den wichtigen Satz von Menger. Dazu einige Definitionen: Zwei Ecken e, e' werden durch Ecken $e_1, \dots, e_m$ (bzw. Kanten $k_1, \dots, k_m$) getrennt, falls e und e' in $G[E \setminus \{e_1, \dots, e_m\}]$ (bzw. in $(E, K \setminus \{k_1, \dots, k_m\})$ in verschiedenen Zusammenhangskomponenten liegen. Pfade (bzw. Züge) zwischen e und e' heißen unabhängig, falls sie paarweise außer e und e' keine Ecke (bzw. paarweise keine Kante) gemeinsam haben.

Satz 9.7 (Menger, lokale Version)

(a) *Seien e, e' zwei nicht-benachbarte Ecken. Dann ist die minimale Anzahl von e und e' trennenden Ecken die maximale Anzahl unabhängiger Pfade zwischen e und e'.*

(b) *Seien e, e' zwei Ecken. Dann ist die minimale Anzahl von e und e' trennenden Kanten die maximale Anzahl unabhängiger Züge zwischen e und e'.*

Zwei gute Heuristiken für das Problem des Handlungsreisenden

Sei $K_n = (E, K)$ mit $w : K \to \mathbb{R}_0^+$ gegeben. Im folgenden seien zwei polynomiale Näherungs–Algorithmen für das Problem des Handlungsreisenden vorgestllt. Falls die Gewichtsfunktion die Dreiecksungleichung erfüllt, gibt es für beide eine Gütegarantie: im ersten Fall ergibt sich höchstens das Doppelte, im zweiten höchstens das Anderthalbfache des optimalen Ergebnisses.

Die Heuristik des minimalen aufspannenden Baumes

- Konstruiere einen aufspannenden Baum B minimalen Gewichts.
- Verdoppele alle Kanten und suche einen Euler–Zug in dem entstehenden (Eulerschen) Multigraphen.
- Durch Überspringen bereits besuchter Ecken zieht man diesen Euler–Zug zu einem Hamiltonschen Kreis zusammen.

Die Christofides–Heuristik

- Konstruiere einen aufspannenden Baum B minimalen Gewichts.
- Konstruiere eine maximale Paarung minimalen Gewichts P auf der Menge der Ecken ungeraden Grades in T.
- Nimm die Kanten aus P zu T hinzu und suche einen Euler–Zug in dem entstehenden (Eulerschen) Multigraphen.
- Durch Überspringen bereits besuchter Ecken zieht man diesen Euler–Zug zu einem Hamiltonschen Kreis zusammen.

Teil III: Algebraische Strukturen

III.10 Gruppen

Definition 10.1 *Eine Gruppe $(G, \circ)$ besteht aus einer nicht-leeren Menge G und einer zweistelligen Operation $\circ : G \times G \to G$ mit folgenden Eigenschaften:*

- *$\circ$ ist assoziativ, d.h. $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$ für alle $g_1, g_2, g_3 \in G$;*
- *es gibt ein neutrales Element $e \in G$, d.h. $g \circ e = e \circ g = g$ für alle $g \in G$;*
- *für jedes $g \in G$ gibt es ein inverses Element, d.h. ein $h \in G$ mit $g \circ h = h \circ g = e$.*

Gilt zusätzlich $g \circ h = h \circ g$ für alle $g, h \in G$, so heißt die Gruppe kommutativ oder abelsch.

Die Ordnung der Gruppe ist die Anzahl ihrer Elemente.

Das Inverse ist eindeutig bestimmt: angenommen h und h' sind Inverse von g, so gilt: $h = h \circ e = h \circ (g \circ h') = (h \circ g) \circ h' = e \circ h' = h'$. Man schreibt dann $h = g^{-1}$. Allgemeiner ist jede Gleichung $g \circ x = h$ bzw. $y \circ g = h$ eindeutig lösbar, nämlich durch $x = g^{-1} \circ h$ und $y = h \circ g^{-1}$.

Ebenso sieht man, daß e eindeutig bestimmt ist. Manchmal spezifiziert man das neutrale Element und schreibt die Gruppe als $(G, e, \circ)$. Gerne schreibt man Gruppen multiplikativ, d.h. man läßt das Zeichen $\circ$ weg und schreibt 1 statt e. Im folgenden werden beide Möglichkeiten gemischt auftreten. Kommutative Gruppen notiert man oft additiv, d.h. mit $+$ statt $\circ$, 0 statt e und $-g$ statt g^{-1}.

Beispiele:

- $(\mathbb{Z}, 0, +)$ und $(\mathbb{Z}_m, 0, +)$.
- $(K, 0, +)$ und $(K \setminus \{0\}, 1, \cdot)$ für einen Körper K, z.B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $(K^+, 1, \cdot)$ für einen angeordneten Körper K, z.B. $K = \mathbb{Q}, \mathbb{R}$.
- Dagegen ist $(\mathbb{Z}^\times, 1, \cdot)$ keine Gruppe.
- Bewegungsgruppen, Symmetriegruppen, Matrizengruppen, etwa $GL(n, K)$.
- $\mathrm{Sym}(M)$ für eine Menge M mit $\circ =$ Hintereinanderausführung und $e = \mathrm{id}$.
- $(\mathrm{Aut}(G), \mathrm{id}, \circ)$ für einen Graphen G, oder allgemeiner Automorphismen einer Struktur.
- $\mathrm{Abb}(G, M)$ für eine Gruppe G und eine Menge M mit komponentenweiser Operation.
- Sind $G_1, \ldots, G_k$ Gruppen, so auch $G_1 \times \cdots \times G_k$ mit komponentenweiser Operation.

Seien $(G, e_g, \circ_G)$ und $(H, e_h, \circ_H)$ zwei Gruppen. Eine Abbildung $\varphi : G \to H$ heißt ein (Gruppen–)<u>Homomorphismus</u>, falls $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$ für alle $g_1, g_2 \in G$ gilt. Ist φ zusätzlich bijektiv, so heißt die Abbildung ein (Gruppen–)<u>Isomorphismus</u>. Man definiert $\mathrm{Bild}(\varphi) := \{h \in H \mid$ es gibt ein $g \in G$ mit $\varphi(g) = h\}$ und $\mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = e_H\}$.

Untergruppen

Sei im folgenden $(G, e, \circ)$ eine feste Gruppe.

Definition 10.2 *Eine Teilmenge* $U \subseteq G$ *heißt* <u>*Untergruppe*</u> *von* G*, in Zeichen* $U \leqslant G$*, falls* $(U, e \circ \restriction_{U \times U})$ *eine Gruppe ist, d.h. falls* $e \in U$ *und mit* $u, u' \in U$ *auch* $u^{-1} \in U$ *und* $u \circ u' \in U$.

Ist U eine Untergruppe von G, so ist die Inklusionsabbildung $U \to G$ ein Gruppenhomomorphismus.

Beispiele:

- $\{e\}$ und G selbst sind die <u>trivialen</u> Untergruppen von G.
- Ist $U \leqslant V \leqslant G$, so $U \leqslant G$.
- Das <u>Zentrum</u> $Z(G) := \{g \in G \mid g \circ h = h \circ g$ für alle $h \in G\}$ einer Gruppe G.
- Ist φ ein Gruppenhomomorphismus, so sind $\mathrm{Bild}(\varphi)$ und $\mathrm{Kern}(\varphi)$ Untergruppen.
- Die Untergruppen von $(\mathbb{Z}, +)$ sind $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$.
- $\mathrm{Aut}_A(G) := \{\alpha \in \mathrm{Aut}(G) \mid \alpha(a) = a$ für alle $a \in A\} \leqslant \mathrm{Aut}(G) \leqslant \mathrm{Sym}(G)$.
- $SL(n, K) \leqslant GL(n, K)$.

Sei $A \subseteq G$. Dann ist der Schnitt über alle A enthaltenden Untergruppen von G wieder eine Untergruppe, die von A <u>erzeugte Untergruppe $< A >$</u>. Gruppen, die von einem Element g erzeugt werden, heißen <u>zyklische</u> Gruppen. Zum Beispiel wird $(\mathbb{Z}, +)$ von 1 erzeugt.

Für $g \in G$ und $n \in \mathbb{Z}$ definiert man g^n durch $g^0 := e$, $g^{n+1} := g \circ g^n$ für positives n und $g^n := (g^{-1})^{-n})$ für negatives n. Man rechnet dann leicht nach, daß $(g^n)^m = g^{nm}$ und $(*)\ g^n \circ g^m = g^{n+m}$. Es folgt, daß $< g >= \{g^n \mid n \in \mathbb{Z}\}$ und daß die Abbildung $n \mapsto g^n$ einen surjektiven Gruppenhomomorphismus $g^{(\cdot)}$ von $(\mathbb{Z}, +)$ auf $< g >$ definiert.

Die <u>Ordnung</u> von g ist $| < g > | \in \mathbb{N} \cup \{\infty\}$. Es gibt nun zwei Fälle: Entweder die Ordnung von g ist unendlich. Dann ist $g^{(\cdot)}$ ein Isomorphimus zwischen $< g >$ und $(\mathbb{Z}, +)$. Oder die Ordnung von g ist endlich. Dann gibt es eine kleinste natürliche Zahl m, so daß $g^m = e$. Es folgt dann $< g >= \{g^0, g^1, \ldots, g^{m-1}\}$ und $\mathrm{Kern}(g^{(\cdot)}) = m\mathbb{Z}$. Der Homomorphismus $g^{(\cdot)}$ induziert dann einen Isomorphismus zwischen $< g >$ und $(\mathbb{Z}_m, +)$. Wir haben also gezeigt:

Satz 10.1 *Eine zyklische Gruppe ist entweder isomorph zu* $(\mathbb{Z}, +)$*, falls sie unendliche Ordnung hat, oder zu* $(\mathbb{Z}_m, +)$*, falls sie Ordnung* m *hat. Insbesondere sind zyklische Gruppen stets kommutativ.*

Satz 10.2 *Für* $k \neq 0$ *ist die Ordnung von* g^k *unendlich, falls* $\mathrm{ord}(g)$ *unendlich ist, sonst* $\mathrm{ord}(g^k) = \frac{\mathrm{ord}(g)}{\mathrm{ggT}(\mathrm{ord}(g), k)}$.

□ Ist $\mathrm{ord}(g^k) = n < \infty$, so gilt $g^{kn} = e$, also $\mathrm{ord}(g) < kn$ endlich. Falls $\mathrm{ord}(g) = m$, so gilt $(g^k)^{\frac{m}{\mathrm{ggT}(m,k)}} = g^m = 0$. Andererseits folgt aus $0 = (g^k)^d = g^{kd}$, daß $m < kd$. Also gilt $\mathrm{ord}(g^k) = \frac{m}{\mathrm{ggT}(m,k)}$. □

Folgerung: k ist genau dann ein Erzeuger der Gruppe $\mathbb{Z}_m$, wenn k und m teilerfremd sind. Die Untergruppen von $\mathbb{Z}_m$ sind genau die $\mathbb{Z}_d$ für $d|m$.

Satz 10.3 *Untergruppen zyklischer Gruppen sind wieder zyklisch. Homomorphe Bilder zyklischer Gruppen sind wieder zyklisch.*

□ Für Untergruppen haben wir es in allen möglichen Fällen nachgerechnet. Ist $\varphi : G \to H$ Homomorphismus und g ein Erzeuger von G, so wird $\mathrm{Bild}(\varphi) = \{\varphi(g^n) \mid n \in \mathbb{Z}\} = \{\varphi(g)^n \mid n \in \mathbb{Z}\}$ von $\varphi(g)$ erzeugt. □

Nebenklassenzerlegung

Sei $U \leqslant G$. Auf G definiert man zwei Äquivalenzrelationen. Zum einen $g \sim_L h :\iff g^{-1}h \in U$. Dies ist genau dann eine Äquivalenzrelation, wenn U eine Untergruppe ist. Die Äquivalenzklassen $gU := \{gu \mid u \in U\}$ heißen Linksnebenklassen von U in G. Die Menge der Linksnebenklassen wird mit G/U bezeichnet.

Es gilt $gU = hU \iff h^{-1}g \in U$.

Entsprechend ist $g \sim_L h :\iff hg^{-1} \in U$ eine Äquivalenzrelation mit Klassen $Ug := \{ug \mid u \in U\}$, den Rechtsnebenklassen von U in G, deren Menge mit $U\backslash G$ bezeichnet wird.

Satz 10.4

(a) $x \mapsto hg^{-1}x$ *ist eine Bijektion zwischen* gU *und* hU.

(b) $x \mapsto xg^{-1}h$ *ist eine Bijektion zwischen* Ug *und* Uh.

(c) $gU \mapsto Ug^{-1}$ *ist eine Bijektion zwischen* G/U *und* $U\backslash G$.

Der Index $|G : U|$ von U in G ist $|G/U| = |U\backslash G|$. Falls G endlich ist, so gilt $|U| \cdot |G : U| = |G|$.

Satz 10.5 (Lagrange) *Sei* G *endlich. Falls* $U \leqslant G$, *so* $|U|\,\big|\,|G|$. *Also* $\mathrm{ord}(g)\,\big|\,|G|$ *für* $g \in G$.

Satz 10.6 *Falls* $|G| = p$ *ein Primzahl ist, so ist* G *zyklisch, also* $\cong \mathbb{Z}/p\mathbb{Z}$. *Diese Gruppen sind die einzigen Gruppen ohne andere Untergruppen als die triviale und sich selbst.*

Gruppen von Primzahlordnung sind also bis auf Isomorphie durch ihre Ordnung festgelegt. Für andere Ordnungen gilt dies nicht. Zum Beispiel gibt es zwei Gruppen der Ordnung vier: $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Faktorgruppen

Man möchte nun gerne G/U so zu einer Gruppe machen, daß die natürliche Surjektion $G \to G/U$, $g \mapsto gU$ ein Gruppenhomomorphismus wird. Dann muß $gU \cdot hU = ghU$ gelten.

Definition 10.3 *Eine Untergruppe* $U \leqslant G$ *heißt* Normalteiler *oder* normale Untergruppe*, in Zeichen* $U \trianglelefteq G$*, falls* $gU = Ug$ *für alle* $g \in G$ *ist.*

Äquivalent: $g^{-1}Ug = U$ für alle $g \in G$

Beispiele:

- Die trivialen Untergruppen und das Zentrum sind Normalteiler.
- Jede Untergruppe in einer kommutativen Gruppe ist Normalteiler.

Satz 10.7

(a) *Sei* $U \trianglelefteq G$*, dann definiert* $gU \cdot hU = ghU$ *eine Gruppe auf* G/U *mit neutralem Element* eU *und so, daß* $g \mapsto gU$ *ein surjektiver Gruppenhomomorphismus ist.*

(b) *Sei* $\varphi : G \to H$ *Gruppenhomomorphismus. Dann gilt* $\mathrm{Kern}(\varphi) \trianglelefteq G$ *und* $G/\mathrm{Kern}(\varphi) \cong \mathrm{Bild}(\varphi)$.

Beispiele:

- $\_ \bmod m : \mathbb{Z} \to \mathbb{Z}_m$ ist surjektiver Homomorphismus mit Kern $m\mathbb{Z}$, also $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.
- $\mathrm{sgn} : \mathrm{Sym}(n) \to \mathbb{Z}_2$, $\sigma \mapsto$ "Parität der Anzahl der Transpositionen" ist surjektiver Homomorphismus. Der Kern ist die sogenannte alternierende Gruppe A_n; also $\mathrm{Sym}(n)/A_n = \mathbb{Z}_2$.
- $\det : GL(n, K) \to K^\times = (K \setminus 0, \cdot)$ ist surjektiver Homomorphismus mit Kern $SL(n, K)$, also $GL(n, K)/SL(n, K) = K^\times$.
- Vektorräume: $\mathbb{R}^3/\mathbb{R} = \mathbb{R}^2$.

Satz 10.8 (ohne Beweis) *Sei* $H \leqslant G$ *und* $K \trianglelefteq G$.

(a) *Es gilt* $K \trianglelefteq HK \leqslant G$*,* $H \cap K \trianglelefteq H$ *und* $H/(H \cap K) \cong HK/K$.

(b) *Gilt zusätzlich* $K \leqslant H \trianglelefteq G$*, so gilt* $K \trianglelefteq H$ *und* $(G/K)\big/(H/K) \cong G/H$.

Eine Gruppe heißt einfach, falls sie keine nicht-trivialen Normalteiler hat. Jede endliche Gruppe ist aus endlich vielen einfachen Gruppen zusammengebaut, d.h. es gibt $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$ mit G_{i+1}/G_i einfach. Man kennt alle einfachen endlichen Gruppen: es gibt mehrere unendliche Familien, wie die $\mathbb{Z}_p$ für Primzahlen p oder die alternierenden Gruppen A_n, $n \geqslant 5$, und 26 sogenannte sporadische Gruppen. Allerdings kann es noch mehrere Möglichkeiten geben, wie diese einfachen Gruppen zusammengesetzt werden. Für $\mathbb{Z}_4$ wie für $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist $n = 2$ und beide einfachen Quotienten sind $\mathbb{Z}_2$.

III.11 Ringe und Körper

Ringe

Definition 11.1 *Ein* Ring $R = (R, 0, 1, +, \cdot)$ *besteht aus einer nicht-leeren Menge* R*, zwei (nicht notwendig verschiedenen) ausgezeichneten Elementen* $0, 1 \in R$ *und zwei zweistel-*

ligen Operationen $+, \cdot : R^2 \to R$ *mit folgenden Eigenschaften:*

- $(R, 0, +)$ *ist eine kommutative Gruppe;*
- *die Multiplikation* $\cdot$ *ist assoziativ mit neutralem Element* 1*;*
- *es gelten die Distributivgesetze* $(r_1 + r_2) \cdot r = r_1 \cdot r + r_2 \cdot r$ *und* $r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2$ *für alle* $r, r_1, r_2 \in R$.

Der Ring heißt *kommutativ, falls zusätzlich die Multiplikation kommutativ ist.*

Man sieht leicht, daß in einem Ring $0 \cdot r = r \cdot 0 = 0$ für alle $r \in R$ gilt.

Beispiele:

- Der triviale Ring $\{0\}$. Dies ist der einzige Ring mit $0 = 1$, denn daraus folgt $r = r \cdot 1 = r \cdot 0 = 0$, da, wie man leicht einsieht, in einem Ring $0 \cdot r = r \cdot 0 = 0$ für alle $r \in R$ gilt.
- $\mathbb{Z}$; $\mathbb{Z}_m$; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Matrizenring $\mathrm{Mat}_n(R)$, nicht kommutativ!, für einen kommutativen Ring R.
- Polynomring $R[X]$ für einen kommutativen Ring R.

Ein Unterring eines Ringes R ist eine Teilmenge von R, die mit den eingeschränkten Operationen selbst wieder ein Ring ist. Ein Ringhomomorphismen ist eine Abbildung $\varphi : R \to S$ zwischen Ringen, die Gruppenhomomorphismus ist und Multiplikation und 1 respektiert, d.h. $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$ und $\varphi(1) = 1$ erfüllt. Das Bild von φ ist ein Unterring; $\mathrm{Kern}(\varphi)$ erfüllt alle Eigenschaften eines Unterrings, außer daß er i.a. nicht die 1 enthält. Wie im Fall von Gruppen besitzen Kerne von Homomorphismen weitere Eigenschaften, und es gilt ein Homomorphiesatz:

Definition 11.2 *Ein Ideal in einem Ring* R *ist eine Untergruppe* I *der additiven Gruppe* $(R, 0, +)$ *mit* $r \cdot I \subseteq I$ *und* $I \cdot r \subseteq I$ *für alle* $r \in R$.

Satz 11.1

(a) *Ist* I *ein Ideal von* R*, so wird* R/I *durch* $(r + I) \cdot (r' + I) := rr' + I$ *zu einem Ring und die natürliche Projektion* $R \to R/I$ *zu einem Ringhomomorphismus.*

(b) *Kerne von Ringhomomorphismes* $\varphi : R \to S$ *sind Ideale und es gilt* $R/\mathrm{Kern}(\varphi) \cong \mathrm{Bild}(\varphi)$.

Beispiele:

- $\{0\}$ und R selbst sind Ideal von R; letzteres ist das einzige Ideal, das 1 enthält.
- $m\mathbb{Z}$ ist Ideal in $\mathbb{Z}$.
- Für $r \in R$ ist $(x - r) \cdot R[X] := \{f \in R[X] \mid f(r) = 0\}$ ein Ideal in $R[X]$ mit $R[X]/(x - r) \cdot R[X] \cong R$.
- Allgemeiner ist für $r \in R$ die Menge $r \cdot R$ ein Ideal in R, das von r erzeugte Hauptideal. Ein Ring, in dem jedes Ideal Hauptideal ist, heißt Hauptidealring. Beispiele für Hauptidealringe: $\mathbb{Z}$, $\mathbb{K}[X]$ für Körper K. Dagegen sind $\mathbb{Z}[X]$ und $K[X, Y]$ keine Hauptidealringe.

Einheiten und Körper

Sind $a, b \in R$, so heißt a ein Teiler von b, in Zeichen $a|b$, falls es ein $c \in R$ gibt mit $ac = b$. Dies ist äquivalent zu $b \in aR$ bzw. $bR \subseteq aR$. Ein Element $r \in R$ heißt eine Einheit, falls r ein Inverses r^{-1} besitzt, d.h. $r \cdot r^{-1} = r^{-1} \cdot r = 1$. Einheiten sind also genau die Teiler der 1. Die Menge der Einheiten von R wird mit R^* bezeichnet; $(R^*, 1, \cdot)$ ist dann eine Gruppe, die größte in R enthaltene Gruppe bzgl. der Multiplikation.

Definition 11.3 *Ein Körper ist ein kommutativer Ring* R, *für den* $R = R^* \dot\cup \{0\}$ *gilt.*

Jedes Element $\neq 0$ in einem Körper K hat also ein Inverses, d.h. $(K \setminus \{0\}, 1, \cdot)$ ist eine Gruppe, die sogenannte multiplikative Gruppe $K^\times$ des Körpers, im Gegensatz zur additiven Gruppe $K^+ = (K, 0, +)$. ein Körper hat stets zwei Elemente: 0 und 1.

Beispiele:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Die zyklische Gruppe $\mathbb{Z}_2$ wird durch $0 \cdot 0 = 1 \cdot 0 = 0$ und $1 \cdot 1 = 1$ zu einem Körper (dem kleinsten möglichen Körper).

Ein Körper K hat keine Ideale I außer $\{0\}$ und K, denn mit $1 \neq r \in I$ ist auch $(kr^{-1}) \cdot r = k \in I$ für jedes $k \in K$. Also ist ein Ringhomomorphismus zwischen zwei Körpern immer injektiv; ein Homomorphisatz für Körper daher wenig aussagekräftig.

Satz 11.2 $\mathbb{Z}_n$ *ist genau dann ein Körper, wenn* n *eine Primzahl ist.*

□ Falls n keine Primzahl ist und d ein nicht-trivialer Teiler, so würde mit einem Inversen von d gelten: $\frac{n}{d} = d^{-1} \cdot d \cdot \frac{n}{d} = d^{-1} \cdot 0 = 0$: Widerspruch.

Ist n Primzahl, so sei $0 \neq x \in \mathbb{Z}_n$. Wegen des Distributivgesetzes ist die Multiplikation μ_x mit x ein Homomorphismus $\mathbb{Z}_n \to \mathbb{Z}_n$. Da $\mathbb{Z}_n$ einfach ist und $1 \notin \mathrm{Kern}(\mu_x)$, hat μ_x trivialen Kern, ist also injektiv und somit, als Abbildung zwischen gleichmächtigen endlichen Mengen, auch surjektiv. Also gibt es ein y mit $\mu_x(y) = x \cdot y = 1$. □

Satz 11.3 *Ein endlicher Körper* K *hat die Mächtigkeit* p^n *für eine Primzahl* p *und ein* $n \geqslant 1$. *Es ist* $K^+ \cong \mathbb{Z}_p^n$ *und* $K^\times \cong \mathbb{Z}_{p^n-1}$. *Dabei ist* p *die Charakteristik des Körpers, d.h. die kleinste Zahl, für die* $\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$ *gilt.*

□ Betrachte die Menge $\{0, 1, 1+1, 1+1+1, \ldots\}$. Wegen der Endlichkeit von K sind zwei dieser Ausdrücke gleich; deren Differenz ergibt einen Ausdruck $m \cdot 1 := 1 + \cdots + 1 = 0$. Gilt $m = kl$, so folgt aus der Distributivität $0 = (k \cdot 1)(l \cdot 1)$, also ist das kleinste solche m eine Primzahl p. Da die Multiplikation wegen des Distributivgesetzes auf $\{0, 1, 1+1, \ldots, (p-1) \cdot 1\}$ festgelegt ist, haben wir $\mathbb{Z}_p$ als Unterkörper von K. Nun ist K offensichtlich ein Vektorraum über $\mathbb{Z}_p$ der Dimension n, also gilt $K^+ \cong \mathbb{Z}_p^n$ und $|K| = p^n$. In Satz 11.5 wird bewiesen, daß $K^\times$ zyklisch ist. □

Satz 11.4 (ohne Beweis) *Für jede Primzahl p und jedes $n \geqslant 1$ gibt es einen bis auf Isomorphie eindeutig bestimmten Körper der Mächtigkeit p^n, der mit $\mathbb{F}_{p^n}$ bezeichnet wird.*

(Hinweis zum Beweis: Über den reellen Zahlen gibt es irreduzible Polynome ohne Nullstellen, etwa $X^2 + 1$. Nun kann man $\mathbb{R}$ erweitern zu dem Körper der komplexen Zahlen $\mathbb{C} \cong \mathbb{R}[i] \cong \mathbb{R}[X]/(X^2+1)\cdot\mathbb{R}[X]$. Dies Verfahren konstruiert allgemein für ein irreduzibles Polynomen $P \in K[X]$ einen kleinsten, eindeutig bestimmten Erweiterungkörper $K[X]/P \cdot K[X]$ des Körpers K, in dem P eine Nullstelle hat. $\mathbb{F}_{p^n}$ entsteht auf diese Weise aus $\mathbb{Z}_p$ durch ein irreduzibles Polynom vom Grad n.)

Die Eulersche φ-Funktion gibt für jede positive natürliche Zahl n die Anzahl der zu ihr teilerfremden positiven natürlichen Zahlen $\leqslant n$ an. Dies ist also auch die Anzahl der erzeugenden Elemente der Gruppe $(\mathbb{Z}_n, +)$. Da jedes Element a in $\mathbb{Z}_n$ Erzeugendes der einzigen Untergruppe der Ordnung $\mathrm{ord}(a)$ ist, gilt $n = \sum_{d|n} \varphi(d)$.

Satz 11.5 *Sei K ein Körper. Dann ist jede endliche Untergruppe von $K^\times$ zyklisch. Insbesondere ist $K^\times$ zyklisch für endliches K.*

□ Hilfssatz: eine Gruppe G der Ordnung n ist genau dann zyklisch, wenn es zu jedem $d|n$ höchstens d Elemente gibt, deren Ordnung d teilt (d.h. für die $g^d = 1$ gilt).

Beweis des Hilfssatzes: Angenommen G ist nicht zyklisch. Sei $\psi(d)$ die Anzahl der Elemente der Ordnung d. Wegen $n = \sum_{d|n} \varphi(n) = \sum_{d|n} \psi(n)$ und $\psi(n) = 0$ gibt es ein $d_0|n$ mit $\psi(d_0) > \varphi(d_0)$. Insbesondere gibt es dann eine zyklische Untergruppe der Ordnung d_0 und damit $\psi(d) \geqslant \varphi(d)$ für alle $d|d_0$. Dann gibt es aber $\sum_{d|d_0} \psi(d) > \sum_{d|d_0} \varphi(d) = d_0$ Elemente, deren Ordnung d_0 teilt: Widerspruch.

Aus dem Hilfssatz folgt nun leicht der Satz, da Elemente von $K^\times$, deren (multiplikative) Ordnung n teilen, Nullstellen des Polynoms $X^n - 1$ sind, von denen es höchstens n Stück gibt. □

Falls n keine Primzahl ist, so ist $\mathbb{Z}_n$ schon deshalb kein Körper, weil es Elemente $a \neq 0, b \neq 0$ mit $ab = 0$ gibt. Solche Elemente heißen Nullteiler und können keine Inverse haben. $\mathbb{Z}$ ist ein nullteilerfreier Ring, der kein Körper ist, kann aber zu einem Körper $\mathbb{Q}$ erweitert werden. Auf die gleiche Weise kann jeder nullteilerfreie, kommutative, nichttriviale Ring R in einen Körper eingebettet werden. Der kleinste solche Körper heißt der Quotientenkörper von R. Dieser besteht aus Äquivalenzklassen von formalen Brüchen $\frac{r}{s}$ mit $r, s \in R, s \neq 0$ bezüglich der Äquivalenzrelation $\frac{r}{s} \sim \frac{r'}{s'} :\iff rs' = r's$. Es gelten nun die selben Rechenregeln, wie man sie vom Bruchrechnen in $\mathbb{Q}$ her kennt. Jedes Element $r \neq 0$ hat nun ein Inverses: (die Äquivalenzklase von) $\frac{1}{r}$.

Endliche Ringe, insbesondere die Ringe $\mathbb{Z}_m$

Wie wir gesehen haben, besitzen die Ringe $\mathbb{Z}_m$ Nullteiler oder sie sind schon Körper. Dies gilt allgemein für endliche Ringe:

Satz 11.6 *Ein nullteilerfreier, endlicher, nicht-trivialer Ring ist ein Körper.*

□ Nullteilerfreiheit bedeutet genau, daß die Multiplikation mit Elementen $\neq 0$ trivialen Kern hat. Dann folgt wieder aus der Endlichkeit, daß sie bijektiv ist. □

Sei $n \geqslant 2$. Dann sind die Matrizenringe $\mathrm{Mat}_n(\mathbb{F}_q)$ Beispiele für nicht-kommutative endliche Ringe.

Wir wollen nun versuchen, die multiplikative Struktur der Ringe $\mathbb{Z}_m$, d.h. die Einheitengruppe, besser zu verstehen. Zur Erinnerung: Rechnen in $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$ ist das Gleiche wie Rechnen in $\mathbb{Z}$ modulo m.

Satz 11.7 $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \mathrm{ggT}(a, m) = 1\}$. *Insbesondere ist* $\varphi(m)$ *die Ordnung von* $\mathbb{Z}_m^*$.

□ Gilt $1+m\mathbb{Z} = (a+m\mathbb{Z})(s+m\mathbb{Z}) = as+m\mathbb{Z}$, so $1-as \in m\mathbb{Z}$ und $m|1-as$. Also $km+as = 1$ und es folgt $\mathrm{ggT}(m, a)\big|1$.

Sei umgekehrt $\mathrm{ggT}(a, m) = 1$. Dann gibt es s, t mit $as + mt = 1$. Es folgt $1 - as \in m\mathbb{Z}$ und die Zerlegung wie oben zeigt, daß a Einheit in $\mathbb{Z}_m^*$ ist. □

Satz 11.8 (Satz von Euler bzw. kleiner Satz von Fermat)

(a) $a^{\varphi(n)} \equiv 1 \pmod n$ *für alle* a *mit* $\mathrm{ggT}(a, n) = 1$.

(b) $a^{p-1} \equiv 1 \pmod p$ *für Primzahlen* p *und alle* a *mit* $p \not| a$.

Erste Anwendung: Primzahltest I

Wie testet man, ob eine gegebene Zahl n eine Primzahl ist? Aus der Definition ergibt sich die Möglichkeit, für alle $1 < d \leqslant \lfloor\sqrt{n}\rfloor$ zu überprüfen, ob $d|n$. Dies dauert aber bei großen n zu lange für einen praktikablen Test.

Ein schneller Test ergibt sich aus dem kleinen Satz von Fermat: für ausgewählte Zahlen $a \leqslant n$ überprüft man, ob $a^{n-1} \equiv 1 \pmod n$. Dieser Test ist negativ effektiv, d.h. bei negativer Antwort weiß man, daß n keine Primzahl ist, aber liefert nur mit einer gewissen (guten) Wahrscheinlichkeit ein positives Ergebnis. Selbst beim Testen mit allen Zahlen $a \leqslant n$ (was wiederum zu viele für eine vernünftige Laufzeit wären) ist der Test nicht effektiv, da es die sogenannten Carmichael–Zahlen gibt, die keine Primzahlen sind, aber den kleinen Satz von Fermat für alle a erfüllen. Erst 1992 konnte gezeigt werden, daß es unendlich viele Carmichael–Zahlen gibt. Die kleinste davon ist 561.

Zweite Anwendung: RSA–Kryptographie

Man möchte ein Verfahren zur Verfügung stellen, das es jedem erlaubt, Nachrichten so verschlüsselt an einen Empfänger E zu schicken, daß nur dieser sie entschlüsseln kann. Dazu wählt E zwei große Primzahlen $p \neq q$ und bildet $n = pq$ und wählt ein "zufälliges" zu $\varphi(n) = (p-1)(q-1) = n-p-q+1$ teilerfremdes e (also z.B. nicht $e = \varphi(n)-1$). Die Zahlen n und e gibt E als öffentlicher Schlüssel bekannt; p, q und damit auch $\varphi(n)$ bleiben geheim. Nachrichten sind Wörter über dem Alphabet $\mathbb{Z}_n^*$. Eine Nachricht $A = (a_1, \dots, a_k) \in (Z_n^*)^k$ wird als $A^e := (a_1^e, \dots, a_k^e)$ verschlüsselt verschickt, wobei a^e in $\mathbb{Z}_n^*$ berechnet wird.

E sucht nun in $\mathbb{Z}_n^*$ ein Inverses d zu e. Dies existiert wegen der Teilerfremdheit von e mit $\varphi(n)$ und kann mit dem Euklidischen Algorithmus schnell berechnet werden, wenn man $\varphi(n)$ kennt. Wegen des Satzes 11.8 gilt $A_i^{ed} = A_i$ in $\mathbb{Z}_n^*$, zur Entschlüsselung braucht E also nur $(A^e)^d = A^{ed} = A$ auszurechnen.

Eine andere Person müßte erst $\varphi(n)$ berechnen, dazu also n in Primfaktoren zerlegen, was man nicht schnell genug kann. Jede verschickte Nachricht enthält allerdings Informationen über $\varphi(n)$, so daß man mach einiger Zeit e und n wechseln muß.

Die genaue Struktur der Einheitengruppen $\mathbb{Z}_m$ ist wie folgt. Zum Beweis braucht man tiefergehende Gruppentheorie, als sie hier entwickelt werden konnte.

Satz 11.9 (ohne Beweis)

(a) *Ist* $p > 2$ *Primzahl so ist* $\mathbb{Z}_{p^k}^*$ *zyklisch der Ordnung* $\varphi(p^k) = (p-1)\cdot p^{k-1}$.

(b) *Für* $k \geqslant 2$ *gilt* $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. *Diese Gruppe hat die Ordnung* 2^{k-1} *und ist für* $k \geqslant 3$ *nicht zyklisch.*

(c) *Ist* $m = \prod_{i=1}^{l} p_i^{k_i}$ *die Primfaktorzerlegung von* m, *so gilt* $\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_l^{k_l}}$. *Insbesondere ist* $\varphi(m) = \prod_{i=1}^{l} \varphi(p_i^{k_i}) = \prod_{i=1}^{l} \left((p_i - 1)\cdot p_i^{k_i-1}\right)$.

Quadrate

Die Abbildung $\_^2 : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $x \mapsto x^2$ ist ein Gruppenhomomorphismus. Für eine Primzahl $p > 2$ gilt $\text{Kern}(\_^2) = \{1, -1\} = \{1, p-1\}$, ist also nicht trivial. Damit folgt $\left|\text{Bild}(\_^2)\right| = \frac{p-1}{2}$, d.h. genau die Hälfte der Zahlen in $\mathbb{Z}_p^*$ sind Quadrate. Man definiert nun für $a \in \mathbb{Z}$ mit $p \not| a$ das <u>Legendre–Symbol</u>

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } (a \bmod p) \text{ Quadrat in } \mathbb{Z}_p^* \\ -1 & \text{falls } (a \bmod p) \text{ kein Quadrat in } \mathbb{Z}_p^* \end{cases}$$

Satz 11.10 (Euler) $p > 2$ *Primzahl. Dann* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Wegen $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \pmod p$ folgt $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$.

□ Sei g ein Erzeuger von $\mathbb{Z}_p^*$. Dann gilt $g^{\frac{p-1}{2}} = -1$, da $\text{ord}(g) = p-1$. Nun gibt es ein j mit $a = g^j$. Offensichtlich ist a Quadrat, falls j gerade ist. Da genau die Hälfte aller Zahlen in $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$ Quadrate sind, bleiben für die Nicht–Quadrate genau die g^j mit ungeradem j übrig. Andererseits ist $a^{\frac{p-1}{2}} = (b^j)^{\frac{p-1}{2}} = (b^{\frac{p-1}{2}})^j = (-1)^j$, also $= 1 \iff j$ gerade. □

Das Legendre–Symbol induziert einen Gruppenhomomorphismus $\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p^* \to \{\pm 1\} \cong \mathbb{Z}_2$, dessen Kern gerade die Quadrate sind. Man ergänzt die Definition durch $\left(\frac{kp}{p}\right) = 0$. Es hängt dann $\left(\frac{a}{p}\right)$ nur von der Restklasse $a \bmod p$ ab und ist multiplikativ in a. Ferner gelten folgende Eigenschaften:

Satz 11.11 (ohne Beweis) *Seien p, q zwei verschiedene ungerade Primzahlen.*

(a) Quadratisches Reziprozitätsgesetz von Gauß: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

(b) Ergänzungsgesetze: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{4}}$ *und* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Für eine ungerade Zahl n mit Primfaktorzerlegung $n = \prod_{i=1}^{l} p_i^{k_i}$ weitet man nun die Definition des Legendre–Symbols aus durch

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{l} \left(\frac{a}{p_i}\right)^{k_i}$$

Man rechnet dann leicht nach, daß das erweiterte Symbol multiplikativ in beiden Argumenten ist und die Eigenschaften von Satz 11.11 nasch wie vor gelten. Daraus ergibt sich die Möglichkeit, das erweiterte Legendre–Symbol $\left(\frac{a}{b}\right)$ schnell, insbesondere ohne Primfaktorzerlegung, zu berechnen. Zunächst reduziert man a mod b, zieht dann die höchste Zweier–Potenz heraus, die man mit dem Ergänzungsgesetz berechnet, wendet das quadratische Reziprozitätsgesetz an und beginnt von vorne. Daraus ergibt sich

Dritte Anwendung: Primzahltest II

Ist gegebenes $n \in \mathbb{N}$ Primzahl? Teste, ob für ungerade a mit $\operatorname{ggT}(a, n) = 1$ der Satz von Euler gilt, d.h. ob $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$. Dieser Test gibt eine sichere negative Antwort und ist effektiv, falls er für alle a $(\leqslant n)$ ausgeführt wird. Nach einem Ergebnis von Solovay und Strassen gibt es für zusammengesetztes n weniger als $\frac{1}{2}\varphi(n)$ Zahlen $\leqslant n$, für die der Test eine positive Antwort liefert. Beim Testen von k unabhängigen a erhält man also mit Wahrscheinlichkeit mindestens $1 - \frac{1}{2^k}$ die richtige Antwort.

Die meisten der klassischen Primzahltest beruhen auf Varianten und Kombination von Test I und II.

Vierte Anwendung: Codierungstheorie

Problemstellung: bei der Übertragung von Nachrichten treten in der Regel Fehler auf. Kann man Nachrichten so codieren, daß man fehlerhafte Nachrichten erkennen kann, möglichst viele Fehler korrigieren kann und die Codierung effektiv bleibt?

Eine ineffektive Codierung wäre z.B. das k-malige Wiederholen von Nachrichten: tritt im schlimmsten Fall stets an der selben Stelle ein Übertragungsfehler auf, so kann man immer noch die Fehlerhaftigkeit einer empfangenen Nachricht bei bis zu $k - 1$ Fehlern erkennen und bis zu $\lfloor \frac{k-1}{2} \rfloor$ Fehler korrigieren.

Praktisch ist es, die Buchstaben der Nachricht als Elemente in einem endlichen Körper zu wählen. Der ISBN-Code besteht z.B. aus einer neunstelligen Zahl $(a_1, \ldots, a_9)$, in der Sprache, Verlag und Buchnummer codiert sind. Zusätzlich fügt man eine Prüfstelle a_{10} so an, daß die Gleichung $\sum_{i=1}^{10} j \cdot a_j = 0$ in $\mathbb{Z}_{11}$ erfüllt ist. Dieser Code erkennt, ob zwei Ziffern vertauscht wurden.

Sei $K = \mathbb{F}_q$ ein endlicher Körper (das Alphabet der Nachrichten). Ein <u>Code</u> (die gültigen Nachrichten) ist eine Teilmenge $C \subseteq K^n$ für ein festes $n \in \mathbb{N}$. Auf K^n definiert man die

Hamming–Metrik durch $d\big((v_1,\dots,v_n),(w_1,\dots,w_n)\big) :=$ die Anzahl der j mit $v_j \neq w_j$. Das Gewicht des Codes ist $d(C) := \min\limits_{\bar{v},\bar{w}\in C} d(\bar{v},\bar{w})$.

Günstig sind besonders die linearen Codes, bei denen C ein Untervektorraum von K^n ist. Mit $k := \dim C$ und $d^* := d(C)$ nennt man einen solchen Code auch einen $[n,k,d^*]$-Code. Es gilt dann stets $d^* \leqslant n-k+1$. Ein $[n,k,d^*]$-Code erkennt bis zu d^*-1 Fehler und korrigiert bis zu $r := \lfloor \frac{d^*-1}{2} \rfloor$ Fehler. Ein Code heißt perfekt, falls jedes $\bar{v} \in K^n$ höchstens Abstand r zu C hat.

III.12 Arithmetik in Hauptidealringen

Rechnen mit Idealen

Sei R ein Ring und I, J, K Ideale. Dann sind auch

$$I \cap J, \qquad I + J := \big\{ r + s \;\big|\; r \in I, s \in J \big\} \quad \text{und} \quad I \cdot J := \Big\{ \sum_{j=1}^{n} r_j s_j \;\Big|\; n \in \mathbb{N}, r_j \in I, s_j \in J \Big\}$$

Ideale von R. Dabei ist $I \cap J$ das größte in I und J enthaltene Ideal und $I+J$ das kleinste I und J enthaltende Ideal von R. Es gelten folgende Rechenregeln:

$$\begin{array}{lll}
I+(J+K) = (I+J)+K & \text{und} & I\cdot(J\cdot K) = (I\cdot J)\cdot K \\
I + \{0\} = \{0\} + I = I & \text{und} & I \cdot R = R \cdot I = R \\
(I+J)\cdot K = I\cdot K + J \cdot K & \text{und} & I\cdot(J+K) = I\cdot J + I \cdot K \\
I + J = J + I & \text{und, falls } R \text{ kommutativ,} & I \cdot J = J \cdot I \\
I + I = I & \text{und} & I^2 := I \cdot I \subseteq I \quad \text{und} \quad I \cdot J \subseteq I \cap J
\end{array}$$

Satz 12.1 (Chinesischer Restsatz)
Sei R kommutativer Ring und $I_1, \dots, I_n$ Ideale mit $I_i + I_j = R$ für alle $i \neq j$.

(a) $(I_1 \cdots I_{n-1}) + I_n = R$ *und* $I_1 \cdots I_n = I_1 \cap \dots \cap I_n$.

(b) *Seien $r_1, \dots, r_n \in R$ gegeben. Dann gibt es ein $r \in R$ mit $r - r_j \in I_j$ für alle j.*

□ (a) $R = \prod\limits_{j=1}^{n-1} (I_j + I_n) = I_1 \cdots I_{n-1} + (\dots) \cdot I_n \subseteq I_1 \cdots I_{n-1} + I_n \subseteq R$, also Gleichheit.

Der zweite Teil per Induktion nach n:
$I_1 \cap I_2 = (I_1 \cap I_2)R = (I_1 \cap I_2)(I_1 + I_2) = (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subseteq I_2 I_1 + I_1 I_2 = I_1 I_2 \subseteq I_1 \cap I_2$, also überall Gleichheit. Im Induktionsschritt setze $J := I_1 \cdots I_{n-1}$. Mit dem ersten Teil gilt $J + I_n = R$, also $I_1 \cdots I_n = J \cdot I_n \overset{\text{Fall } n=2}{=} J \cap I_n \overset{\text{Induktion}}{=} I_1 \cap \dots \cap I_{n-1}$.

(b) Für $n = 2$ gibt es nach Voraussetzung $a_i \in I_i$ mit $a_1 + a_2 = 1$. Dann geht $r = r_1 a_2 + r_2 a_1$, da etwa $r - r1 = r_1(a_2 - 1) + r_2 a_1 = -r_1 a_1 + r_2 a_1 \in a_1 R$.
Sei per Induktion r' gefunden mit $r' - r_j \in I_j$ für alle $1 \leqslant j \leqslant n-1$. Setze $J := I_1 \cdots I_{n-1}$. Mit (a) und $n = 2$ existiert dann ein $r \in R$ mit $r - r' \in J$ und $r - r_n \in I_n$. Es folgt $r - r_j = (r - r') + (r' - r_j) \in J + I_j = (I_1 \cdots I_{n-1}) + I_j \subseteq I_j$. □

Anwendung: seien paarweise teilerfremde Zahlen $m_1, \dots, m_n \in \mathbb{Z}$ gegeben sowie Zahlen $r_1, \dots, r_n \in \mathbb{Z}$. Dann existiert $r \in \mathbb{Z}$ mit $r \equiv r_j \bmod m_j$ für alle $1 \leqslant j \leqslant n$.

kgV und ggT

Seien $r_1, \dots, r_n$ aus einem kommutativen Ring R gegeben. Ein Ringelement d heißt ein größter gemeinsamer Teiler (ggT) von $r_1, \dots, r_n$, falls d alle r_i teilt und von allen gemeinsamen Teilern der r_i geteilt wird. Ein Ringelement k heißt ein kleinstes gemeinsames Vielfaches (kgV) von $r_1, \dots, r_n$, falls k von allen r_i geteilt wird und alle Elemente teilt, die von allen r_i geteilt werden.

Die Multiplikation mit einem Ringelement $r \neq 0$ ist ein additiver Gruppenhomomorphismus μ_r, dessen Kern sogar ein Ideal ist. Sei R nun ein kommutativer Ring ohne Nullteiler, auch Integritätsbereich genannt. Dann ist $\mathrm{Kern}(\mu_r) = \{0\}$, also ist μ_r injektiv, d.h. es gilt die Kürzungsregel $ra = rb \implies a = b$, obwohl es für r kein Inverses zu geben braucht. Damit sieht man, daß auf R eine Äquivalenzrelation durch

$$\underline{r \sim s} :\iff rR = sR \iff (r|s \text{ und } s|r) \iff \text{ es gibt } e' \in R^* \text{ mit } r = e's$$

definiert ist. Die Äquivalenzklassen sind so etwas wie die "Nebenklassen" von R^* in R. In $\mathbb{Z}$ sind dies gerade die Mengen $\{+a, -a\}$. Die Menge der ggT (bzw. der kgV) von Elementen $r_1, \dots, r_n$ bildet nun genau eine Äquivalenzklasse bezüglich $\sim$. Man sagt, daß der ggT (bzw. der kgV) "bis auf Einheit" bestimmt ist (in $\mathbb{Z}$ also bis auf das Vorzeichen).

Satz 12.2

(a) *Genau dann existiert ein* kgV k *von* $r_1, \dots, r_n$*, wenn* $\bigcap_{i=1}^{n} r_i R = kR$.

(b) *Ist* $\sum_{i=1}^{n} r_i R = gR$*, so ist* g *ein* ggT *von* $r_1, \dots, r_n$. *Es gibt* $t_i \in R$ *mit* $g = t_1 r_1 + \dots + t_k r_k$.

(c) *Ist* $kR = r_1 R \cap r_2 R$ *und* $gR = r_1 R + r_2 R$*, so gilt* $r_1 r_2 R = gkR$.

Insbesondere existieren in Hauptidealringen ggT und kgV stets!

□ (a) Es gilt zum einen "$c \in \bigcap_{i=1}^{n} r_i R \iff c$ ist gemeinsames Vielfaches der r_i", zum andern "$c \in kR \iff k|c$". Daraus folgt leicht die Behauptung.

(b) In diesem Fall ist insbesondere $r_i \in gR$, also $g|r_i$. Sei c ein gemeiner Teiler der r_i. Dann gibt es $s_i \in R$ mit $cs_i = r_i$ und $t_i \in R$ mit $g = \sum_{i=1}^{n} r_i t_i = \sum_{i=1}^{n} c s_i t_i$, also $c|g$.

(c) Zunächst überlege man, daß stets $a(bR) = abR = (aR)(bR)$ gilt. Seien $r_1, r_2 \neq 0$ (sonst gilt $k = 0$). Aus $r_1 R + r_2 R = gR$ folgt $r_1 s_1 + r_2 s_2 = g$ für geeignete $s_i \in R$. Sei $\frac{r_i}{g} \in R$ so, daß $g \frac{r_i}{g} = r_i$. Dann hat man $\frac{r_1}{g} s_1 + \frac{r_2}{g} s_2 = 1$, somit $\frac{r_1}{g} R + \frac{r_2}{g} R = R$. Mit dem chinesischen Restsatz erhält man nun: $r_1 r_2 R = g^2 (\frac{r_1}{g} R \cdot \frac{r_2}{g} R) = g^2 (\frac{r_1}{g} R \cap \frac{r_2}{g} R) = g(r_1 R \cap r_2 R) = gkR$. □

Beispiele:

In $\mathbb{Z}[X]$ sind ± 1 die beiden ggT von 2 und X. Es gilt aber $1 \notin 2 \cdot \mathbb{Z}[X] + X \cdot \mathbb{Z}[X]$. Insbesondere folgt, daß $2 \cdot \mathbb{Z}[X] + X \cdot \mathbb{Z}[X]$ kein Hauptideal ist und $\mathbb{Z}[X]$ keine Haupidealring.

In $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ haben 6 und $2 - 2\sqrt{-5}$ keinen ggT d. Rechnen in $\mathbb{C}$ zeigt, daß einerseits als gemeinsamer Teiler $|d|^2 \big| 12$ folgt; andererseits aber auch $12 \big| |d|^2$, da sowohl 2 als auch $1 - \sqrt{-5}$ gemeinsame Teiler von 6 und $2 - 2\sqrt{-5}$ sind. Nun ist aber 12 nicht von der Form $a^2 + 5b^2$ für $a, b \in \mathbb{Z}$.

Euklidische Ringe und Primfaktorzerlegung

Ist e_0 eine Einheit, so läßt sich $r \in R$ als $r = e_0 \cdot (e_0^{-1} r)$ schreiben. Ein Element r heißt irreduzibel, falls $r \notin R^*$, $r \neq 0$ und r keine weiteren Produktdarstellungen zuläßt, d.h. falls aus $r = ab$ stets $a \in R^*$ oder $b \in R^*$ folgt. Idealtheoretisch bedeutet dies, daß rR maximal unter den Hauptidealen $\neq R$ ist.

In $\mathbb{Z}$ sind dies gerade die Primzahlen und die negativen Primzahlen. In $\mathbb{Z}_8$ sind 2 und 6 die irreduziblen Elemente.

Definition 12.1 *Ein nullteilerfreier kommutativer Ring R heißt euklidisch, falls es eine Abbildung $\varphi : R \setminus \{0\} \to \mathbb{N}$ gibt mit*

- $\varphi(ab) \geqslant \varphi(a)$ *für alle* $a, b \neq 0$
- *für alle* a, b *mit* $a \neq 0$ *gibt es* $q, r \in R$ *mit* $b = qa + r$ *und* $r = 0$ *oder* $\varphi(r) < \varphi(a)$.

Beispiele: $\mathbb{Z}$ mit $\varphi(z) = |z|$ und $K[X]$ mit $\varphi(P) = \mathrm{grad}(P)$.

Satz 12.3 *Jeder euklidische Ring ist ein Hauptidealring.*

□ Sei $I \neq \{0\}$ ein Ideal. Wähle $a \in I$ mit minimalem $\varphi(a)$. Insbesondere gilt also $aR \subseteq I$. Für $b \in I$ seien q, r wie in der Definition. Dann ist $r = b - qa \in I$, wegen der Minimalität von $\varphi(a)$ folgt also $r = 0$, somit $b \in aR$, d.h. $I = aR$. □

Satz 12.4 *Sei R ein euklidischer Ring. Seien $a, b \neq 0$. Ist $b \in R^*$, so $\varphi(a) = \varphi(ab)$. Ist b keine Einheit, so $\varphi(a) < \varphi(ab)$.*

□ Der erste Teil ist klar wegen $\varphi(a) \leqslant \varphi(ab) \leqslant \varphi(abb^{-1}) = \varphi(a)$.

Angenommen nun $\varphi(a) = \varphi(ab)$. Es gilt $abR \subseteq aR$. Sei $ax \in aR$. Dann gilt es (Division durch ab!) $q, r \in R$ mit $ax = q(ab) + r$. Falls $r \neq 0$, so folgt einerseits $\varphi(r) < \varphi(ab) = \varphi(a)$, andererseits $r = ax - qab = a(x - qb)$, also $\varphi(r) = \varphi(a(x - qb)) \geqslant \varphi(a)$: Widerspruch. Also gilt $r = 0$ und damit $ax = abq \in abR$. Wegen $aR = abR$ gibt es ein $c \in R$ mit $a \cdot 1 = abc$; mit der Nullteilerfreiheit folgt $bc = 1$ bzw. $b \in R^*$. □

Satz 12.5 (eindeutige Primfaktorzerlegung) *Sei R ein euklidischer Ring, $a \in R, a \neq 0, a \notin R^*$. Dann gibt es irreduzible Elemente $p_1, \ldots, p_k$ mit $a = p_1 \cdots p_k$. Dabei sind die p_i bis auf Reihenfolge und Einheit eindeutig bestimmt.*

□ Die Existenz einer solchen Zerlegung zeigt man mit Induktion nach $\varphi(a)$: für minimales $\varphi(a)$ ist a nach Satz 12.4 irreduzibel und für irreduzibles a wähle man $k = 1$ und $p_1 = a$. Sei nun a reduzibel, etwa $a = a_1 a_2$ mit $a_i \notin R^*$. Nach Satz 12.4 gilt $\varphi(a_1) < \varphi(a)$ und $\varphi(a_2) < \varphi(a)$; beide Elemente sind also per Induktion als Produkte irreduzibler Elemente schreibbar, somit auch a. □

Um die Eindeutigkeit zu beweisen, braucht man einen weiteren Begriff, der auch erklärt, warum man von "Primfaktorzerlegung" und nicht von "Zerlegung in irreduzible Elemente" spricht.

Definition 12.2 *Ein Primideal ist ein Ideal* $P \neq R$*, für das der Faktorring* R/P *nullteilerfrei ist. Ein Element* $p \in R, p \neq 0$ *heißt Primelement, falls* pR *ein Primideal ist.*

Die Nullteilerfreiheit von R/P bedeutet für Elemente $a, b \in R$: falls $a \cdot b \in P$, so gilt bereits $a \in P$ oder $b \in P$; bzw. für ein Primelement p: falls $p|ab$, so bereits $p|a$ oder $p|b$. In $\mathbb{Z}$ findet man auch mit dieser Definition bis auf das Vorzeichen die Primzahlen. Dies ist kein Zufall: in Hauptidealringen fallen beide Begriffe zusammen. Zum einen sind Primelemente in nullteilerfreien Ringen sind stets irreduzibel: aus $p = ab$ folgt für primes p etwa $p|a$. Da aber nun a auch p teilt, gilt $a \sim p$ und $b \in R^*$. Die Umkehrung ist kaum schwerer:

Satz 12.6 *Sei* R *nullteilerfreier Hauptidealring,* p *irreduzibel.*

(a) *Für* $a \in R$ *gilt* $p|a$ *oder* $pR + aR = R$.

(b) p *ist Primelement.*

(c) *Primideale* $P \neq \{0\}$ *sind maximal, d.h. es gibt kein Ideal* I *mit* $P \subset I \subset R$.

□ (a) Da R Hauptidealring ist, existiert ein ggT g von a und p, d.h. es gilt $aR + pR = gR$. Insbesondere gibt es $h \in R$ mit $gh = p$. Da p irreduzibel, ist entweder g oder h Einheit. Im ersten Fall gilt $aR + pR = gR = R$. Im zweiten Fall gilt $p \sim g$ und $a \in aR \subseteq aR + pR = gR = pR$, also $p|a$.

(b) Sei $p|ab$ und angenommen $p \not| a$. Mit (a) folgt $pR + aR = R$, also $b \in bR = b(pR + aR) = bpR + baR \subseteq bpR + pR \subseteq pR$.

(c) Sei I ein Ideal mit $P \subset I \subseteq R$ und $a \in I \setminus P$. Mit (a) folgt $R = pR + aR \subseteq I + I = I$, also $I = R$. □

Nun folgt leicht die Eindeutigkeit der Primfaktorzerlegung in Satz 12.5: sei $a = p_1 \cdots p_k = q_1 \cdots q_l$ mit irreduziblen p_i, q_j. Insbesondere gilt also $p_1 | q_1 \cdots q_l$. Da p_1 prim ist, folgt $p_1 | q_j$ für ein $1 \leqslant j \leqslant l$. Anders geschrieben heißt dies $q_j R \subseteq p_1 R \subset R$. Mit der oben bewiesenen Maximalität des Primideals $q_j R$ folgt $p_1 R = q_j R$, also etwa $p_1 = e_1 q_j$ für eine Einheit e_1. Aufgrund der Nullteilerfreiheit kann man nun mit p_1 kürzen, es gilt also $p_2 \cdots p_k = (e_1^{-1} q_1) \cdot q_2 \cdots q_{j-1} \cdot q_{j+1} \cdots q_l$ und man kann mit Induktion nach $\min\{k, l\}$ schließen.

Bemerkungen:

- In einem Ring läßt sich genau dann jedes Element als Produkt von Primelementen schreiben, wenn es eine eindeutige(!) Zerlegung in irreduzible Elemente wie im Satz 12.5 gibt. Solche Ringe heißen faktoriell; in ihnen sind irreduzible Elemente prim. Neben euklidischen Ringen sind auch beliebige nullteilerfreie Hauptidealringe, der Ring $\mathbb{Z}[X]$ und die Polynomringe $K[X_1, \ldots, X_n]$ über Körpern K faktoriell.
- Sind $a = e' \cdot \prod_{i=1}^{l} p_i^{a_i}$ und $b = e'' \cdot \prod_{i=1}^{l} p_i^{b_i}$ die Primfaktorzerlegungen mit Einheiten e', e'' und Primelementen p_i mit $p_i \not\sim p_j$ für $i \neq j$, so ist $\prod_{i=1}^{l} p_i^{\max\{a_i, b_i\}}$ ein kgV von a und b

und $\prod_{i=1}^{l} p_i^{\min\{a_i, b_i\}}$ ein ggT von a und b, die also stets in faktoriellen Ringen existieren. Insbesondere folgt, daß $\mathbb{Z}[\sqrt{-5}]$ kein faktorieller Ring ist.

- In nicht-faktoriellen Ringen können alle denkbaren Phänomene auftreten. Eine Zerlegung in Primfaktoren ist zwar stets eindeutig, braucht aber nicht zu existieren. Ein Element kann sich auf verschiedene Arten in irreduzible Faktoren zerlegen lassen, die dann nicht alle prim sind. Schließlich gibt es Ringe ohne Zerlegungen in irreduzible Elemente oder sogar ohne irreduzible Elemente (z.B. Boolesche Ringe) ... Ringtheorie ist kompliziert!
- Es gibt aber eine größere Klasse von Ringen als die faktoriellen, sogenannte Dedekind–Ringe, in denen eine verallgemeinerte Art der Primfaktorzerlegung gilt: jedes Ideal $\neq \{0\}$ läßt sich in eindeutiger Weise als Produkt von Primidealen schreiben. In faktoriellen Ringen sind dies die von den Primfaktoren erzeugten Hauptideale; im allgemeinen brauchen es keine Hauptideale zu sein. Für diese verallgemeinerte Primfaktorzerlegung wurden die Ideale, als "ideale Zahlen", eingeführt.
- Im Beispiel $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/(X^2+5)\cdot\mathbb{Z}[X]$ sieht man ähnlich wie oben, daß 2 ein irreduzibles Element ist. Die Zerlegung $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ zeigt, daß 2 nicht prim ist, da 2 weder $1-\sqrt{-5}$ noch $1-\sqrt{-5}$ teilt. Dem entspricht, daß $2\cdot\mathbb{Z}[\sqrt{-5}]$ zwar maximal unter den eigentlichen Hauptidealen ist, aber echt in dem von 2 und $1-\sqrt{-5}$ erzeugten Ideal enthalten ist.

Zum Abschluß eine Übersicht über die betrachteten Ringklassen:

$$
\begin{tikzcd}
 & & & \text{Ringe} \arrow[dl] \arrow[dr] & \\
 & & \text{kommutative (z.B. } \mathbb{Z}_6[X]\text{)} \arrow[dll] \arrow[dr] & & \text{nicht-kommutative (z.B. } \mathrm{Mat}_2(\mathbb{F}_7)\text{)} \\
\text{Integritätsbereiche (z.B. } \mathbb{Z}[\sqrt{-5}]\text{)} \arrow[d] & & & \text{Hauptidealringe (z.B. } \mathbb{Z}_6\text{)} \arrow[ddll] & \\
\text{faktorielle Ringe (z.B. } \mathbb{Z}[X], \mathbb{Q}[X,Y]\text{)} \arrow[dr] & & & & \\
 & \text{nullteilerfreie Hauptidealringe} \arrow[dr] & & & \\
 & & \text{euklidische Ringe (z.B. } \mathbb{Z}, \mathbb{Q}[X], \mathbb{F}_7[X]\text{)} \arrow[d] & & \\
 & & \text{Körper (z.B. } \mathbb{F}_7, \mathbb{Q}\text{)} & &
\end{tikzcd}
$$

Anmerkung: Beispiele nicht-euklidischer, nullteilerfreier Hauptidealringe sind schwierig zu finden bzw. es ist schwierig zu zeigen, daß es Beispiele sind. In der Literatur findet sich u.a. der Ring $S^{-1}\cdot\mathbb{Z}[X]$ für $S = \{X, X^m - 1 \mid m \geqslant 1\}$. Dies ist der kleinste Unterring des Quotientenkörpers von $\mathbb{Z}[X]$, der $\mathbb{Z}[X]$ und alle Inverse von Elementen aus S enthält.

Literaturverzeichnis

[1] Martin Aigner *Diskrete Mathematik*, 2e, Vieweg, Braunschweig 1996.

[2] Peter J. Cameron *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge 1994.

[3] Reinhard Diestel *Graphentheorie*, Springer, Heidelberg 1996.
(bzw. engl Übersetzung: *Graph Theory*, Springer GTM 173, New York 1997.)

[4] Bertram Huppert *Lineare Algebra III*, Vorlesung an der Universität Mainz, WS 1989/90.

[5] Serge Lang *Algebra*, 3e, Addison–Wesley, Reading 1993.