DISKRETE STRUKTUREN

DR. YUBAO GUO

RWTH AACHEN

Mitschrift von Oswald Jaskolla
E-Mail: oswald@jaskolla.net

4. August 2002

Dieses Skript spiegelt meine Aufzeichnungen aus der Vorlesung „Diskrete Strukturen“, gehalten von Dr. Yubao Guo an der RWTH Aachen im Sommersemester 2002, wider. Es handelt sich nicht um ein offizielles Skript von Dr. Guo oder einer Einrichtung der RWTH Aachen. Für die Richtigkeit der hier präsentierten Ergebnisse (und für evtl. nicht bestandene Prüfungen) übernehme ich selbstverständlich keine Haftung. Falls du Fehler, Ungenauigkeiten oder Unklarheiten entdeckst würde ich mich über eine Mitteilung freuen.

Die Numerierung entspricht der in der Vorlesung benutzten, ich habe lediglich *„Punkt n.k“* durch *„n.k Punkt“* ersetzt, da mir dies für eine Präsentation in gedruckter Form sinnvoller erschien. Außerdem habe ich den meisten Punkten eine mir sinnvoll erscheinende Beschreibung hinzugefügt, soweit nicht schon in der Vorlesung eine solche angegeben wurde. Hauptsächlich möchte ich dadurch die Lesbarkeit des Inhaltsverzeichnisses erhöhen.

Diese Mitschrift wurde mit *dem* Textsatzsystem LaTeX erstellt, unter Verwendung *der* Benutzeroberfläche LyX.

Viel Spaß beim büffeln.

Inhaltsverzeichnis

Abzählung, Rekursion, Erzeugende Funktionen **11**

1.1 Elementare Zählprinzipien 11

1.1 Lemma *(Rechenregeln für Mächtigkeiten)* 11

1.2 Folgerung *(Anzahl der Abbildungen)* 11

1.3 Definition *(Permutation)* 12

1.4 Lemma *(Mächtigkeit der symmetrischen Gruppe)* 12

1.5 Satz *(Mächtigkeit der Potenzmenge)* 12

1.6 Definition *(Menge der k-Teilmengen)* 12

1.7 Bemerkung *(Partitionierung der Potenzmenge)* 13

1.8 Lemma *(Anzahl der k-Teilmengen)* 13

1.9 Lemma *(Pascal-Dreieck)* 13

1.10 Satz *(Vandermonde'sche Identität)* 14

Anwendung *(Bezierkurven)* 14

1.11 Lemma *(doppeltes Abzählen)* 14

1.12 Satz *(Schubfachprinzip)* 15

1.13 Beispiel 15

1.14 Satz *(verallgemeinertes Schubfachprinzip)* 16

Rückblick *(Verallgemeinerungen von Lemma 1.11)* 16

1.15 Satz *(Prinzip der Inklusion und Exklusion / Siebformel)* 17

1.16 Beispiel 17

1.2 Mengenpartitionen 18

1.17 Definition *(Partition, Stirlingzahlen zweiter Art)* 18

1.18 Beispiel 18

1.19 Satz *(Stirling-Dreieck zweiter Art)* 18

1.20 Satz *(Anzahl der injektiven und surjektiven Abbildungen)* 19

1.21 Satz *(Potenzen und Stirlingzahlen)* 21

1.3 Permutationen 21

Wiederholung 21

1.22 Definition *(k-Zyklus)* 22

1.23 Bemerkung *(Zykeldarstellung von Permutationen)* 22
1.24 Definition *(Stirlingzahlen erster Art)* 22
1.25 Satz *(Stirling-Dreieck erster Art)* 22
1.4 Erzeugende Funktionen / Formale Potenzreihen 23
1.27 Definition *(formale Potenzreihe, erzeugende Funktion)* 23
1.28 Bemerkung 23
1.29 Definition *(Rechnen mit Potenzreihen)* 24
1.30 Lemma *(Verschieben von Folgengliedern)* 24
1.31 Beispiel 25
1.32 Satz *(Eigenschaften von $K[[x]]$)* 25
1.33 Bemerkung *(Invertierbarkeit in Ringen)* 25
1.34 Lemma *(Invertierbarkeit der geometrischen Reihe)* 25
1.35 Beispiel *(Code mit variabler Wortlänge zur Datenkompression)* 26
1.36 Satz *(Invertieren von Potenzreihen)* 26
1.37 Beispiel 27
1.38 Definition *(formale Ableitung)* 27
1.39 Lemma *(Linearität und Produktregel der formalen Ableitungen)* 27
1.40 Folgerung *(Ableitung des Inversen)* 28
1.41 Folgerung 28
1.42 Bemerkung 29
1.5 Rekursionsgleichungen 29
1.43 Definition *(lineare Rekursionsgleichung)* 30
1.44 Beispiel 30
1.45 Beispiel 31
1.46 Beispiel *(Fibonacci-Zahlen)* 31
1.47 Bemerkung *(goldener Schnitt)* 32
1.48 Satz *(homogene lineare Rekursionsgleichungen zweiter Ordnung)* 32
Schema *(zum Lösen linearer Rekursionsgleichungen)* 33
1.49 Beispiel 34
1.50 Beispiel *(Catalan-Zahlen)* 34
1.51 Lemma *(Rekursionsformel für Catalan-Zahlen)* 35
1.52 Satz *(explizite Darstellung der Catalan-Zahlen)* 35
Schema *(zum Lösen allgemeiner Rekursionsgleichungen)* 37

Graphentheorie **39**

2.1 Grundbegriffe der Graphentheorie 39

2.1 Definition *(Graph)* 39

2.2 Beispiel *(einige Beispielgraphen)* 39

2.3 Bemerkung *(Graph, Multigraph, schlichter Graph)* 42

2.4 Definition *(Nachbarschaft, Eckengrad, regulärer Graph)* 43

2.5 Beispiel 43

2.6 Satz *(Handschlaglemma, Euler 1736)* 43

2.7 Folgerung 44

2.8 Lemma 44

2.9 Definition *(Isomorphie zwischen Graphen)* 44

2.10 Beispiel 44

2.2 Darstellung von Graphen 45

2.11 Definition *(Adjazenzmatrix, Inzidenzmatrix)* 45

2.12 Beispiel 45

2.13 Satz *(Zusammenhang zwischen Adjazenz- und Inzidenzmatrix)* 46

2.14 Definition *(Teilgraph, induzierter Teilgraph)* 46

2.15 Definition *(Zusammenhang, Komponenten)* 46

2.16 Satz *(Abschätzung der Komponenten nach unten)* 47

2.17 Folgerung 47

2.18 Satz *(Anzahl der Kanten in zusammenhängenden Graphen)* 48

2.19 Satz *(Abschätzung der Kanten nach oben)* 48

2.3 Bäume 49

2.20 Definition *(Baum, Wald)* 49

2.21 Lemma *(Endecken in Bäumen)* 49

2.22 Satz *(Charakterisierung von Bäumen)* 50

2.23 Definition *(Wurzelbaum)* 50

2.24 Definition *(Tiefe)* 51

2.25 Definition *(binärer Baum)* 51

2.26 Satz *(Anzahl der Ecken in binären Bäumen)* 51

2.27 Folgerung *(Tiefe von binären Bäumen)* 51

2.28 Definition *(Gerüst eines Graphen)* 51

2.29 Satz *(Existenz von Gerüsten)* 52

2.30 Satz *(Cayley's Tree Formula)* 53

2.4 Matching in Graphen 54

2.31 Definition *(Matching)* 54

2.32 Beispiel 54

2.33 Bemerkung . . . 54
2.34 Bemerkung *(bipartite Graphen)* . . . 54
2.35 Beispiel . . . 54
2.36 Satz *(Bipartität und Kreise)* . . . 54
2.37 Satz *(Matchings in bipartiten Graphen)* . . . 55
2.38 Folgerung . . . 56
2.39 Folgerung . . . 56
2.40 Definition (Multipartite Graphen) . . . 56
2.5 Hamilton Graphen . . . 56
2.41 Definition *(Hamiltonkreis, Hamilton-Weg)* . . . 56
2.42 Beispiel . . . 56
2.43 Satz *(notwendige Bedingung für hamiltonsche Graphen)* . . . 56
2.44 Satz *(Lemma von Ore, 1960)* . . . 57
2.45 Folgerung *(hinreichende Bedingung für hamiltonsche Graphen)* . . . 57
2.46 Folgerung *(Dirac, 1052)* . . . 57
2.47 Bemerkung . . . 57
2.6 Eulersche Graphen . . . 58
2.48 Definition *(Kantenfolge, Kantenzug, Eulertour)* . . . 58
2.49 Definition *(semi-eulerscher Graph, eulerscher Graph)* . . . 58
2.50 Beispiel . . . 58
2.51 Satz *(hinreichende und notwendige Bedingung für Eulertouren)* . . . 59
2.52 Folgerung . . . 59
2.53 Bemerkung . . . 59
2.7 Planare Graphen . . . 59
2.54 Definition *(planarer Graph, Landkarte, Gebiet)* . . . 60
2.55 Satz *(Eulersche Polyederformel, 1752)* . . . 60
2.56 Satz *(notwendige Bedingung für planare Graphen)* . . . 61
2.57 Beispiel . . . 61
2.58 Definition *(Unterteilungsgraph)* . . . 61
2.59 Satz *(Satz von Kuratowski, 1930)* . . . 61
2.60 Definition *(Färbung)* . . . 61
2.61 Beispiel . . . 62
2.62 Satz *(Vierfarbenvermutung, Guthrie 1852)* . . . 62
2.63 Bemerkung . . . 62
2.8 Digraphen . . . 62
2.64 Definition *(Digraph)* . . . 62
2.65 Definition *(Weg, Kreis, Kantenfolge, Kantenzug, Nachbarschaft, Eckengrad)* . . . 62

2.66 Definition *(starker Zusammenhang)* 63
2.67 Definition *(Turnier)* 63
2.68 Satz *(hamiltonsche Wege in Turnieren)* 63
2.69 Satz *(Kreise in stark zusammenhängenden Turnieren)* 63
2.70 Bemerkung 64

Algebraische Strukturen **65**
3.1 Universelle Algebren 65
3.1 Definition *(Operation, Stelligkeit)* 65
3.2 Definition (Algebra, Signatur) 65
3.3 Beispiel 65
3.4 Definition *(neutrale Elemente)* 66
3.5 Beispiel 66
3.6 Lemma *(Existenz und Eindeutigkeit neutraler Elemente)* 66
3.7 Beispiel *(Fortsetzung von Beispiel 3.3)* 67
3.8 Definition *(inverse Elemente)* 67
3.9 Definition *(Halbgruppe)* 67
3.10 Definition *(Monoid)* 67
3.11 Definition *(Gruppe)* 67
3.12 Definition *(abelsche Algebren)* 68
3.13 Definition *(Ring)* 68
3.14 Definition *(Körper)* 68
3.15 Definition *(boolsche Algebra)* 68
3.16 Beispiel 68
3.2 Unteralgebren, Homomorphismen, Kongruenzen 69
3.17 Definition *(Unteralgebra)* 69
3.18 Definition (Untergruppe, Teilring) 69
3.19 Beispiel 70
3.20 Lemma *(Abgeschlossenheit von Unteralgebren bezüglich Durchschnitt)* 70
3.21 Definition *(erzeugte Unteralgebra)* 70
3.22 Beispiel 70
3.23 Definition *(Homomorphismus)* 70
3.24 Beispiel 71
3.25 Definition *(Isomorphismus, Automorphismus)* 71
3.26 Beispiel 71
3.27 Lemma *(Strukturerhaltung durch Isomorphismen)* 71
3.28 Lemma *(Umkehrabbildung von Isomorphismen)* 72
3.29 Beispiel 72

3.30 Definition *(Kongruenzrelation)* . . . 72
3.31 Beispiel . . . 72
3.32 Satz *(Homomorphiesatz)* . . . 72
3.33 Beispiel . . . 73
3.3 Ringe und Ideale . . . 73
3.34 Lemma . . . 73
3.35 Definition *(Ideal)* . . . 73
3.36 Satz *(Kongruenzrelationen und Ideale)* . . . 73
3.37 Satz *(Hauptideale)* . . . 74
3.38 Beispiel *(vgl. Beispiel 3.29)* . . . 74
3.39 Beispiel . . . 74
3.4 Gößter gemeinsamer Teiler . . . 74
3.40 Definition *(Nullteiler, Integritätsbereich)* . . . 75
3.41 Beispiel . . . 75
3.42 Definition (*größter gemeinsamer Teiler*) . . . 75
3.43 Bemerkung (*Einheit*) . . . 75
3.5 Eindeutige Primfaktorenzerlegung . . . 75
3.44 Definition (*irreduzibel*) . . . 75
3.45 Beispiel . . . 76
3.46 Beispiel . . . 76
3.47 Definition (*eindeutige Primfaktorzerlegung*) . . . 76
3.48 Bemerkung . . . 76
3.49 Definition (*Hauptidealring*) . . . 76
3.50 Satz (hinreichende Bedingung für eindeutige Primfaktorenzerlegung) . . . 76
3.51 Satz (*Euklidischer Ring*) . . . 76
3.52 Folgerung . . . 77
3.53 Satz . . . 77
3.54 Folgerung . . . 77
3.55 Bemerkung (*Fundamentalsatz der Arithmetik*) . . . 77
3.56 Satz (*Existenz unendlich vieler Primzahlen*) . . . 77
3.57 Satz (*Primzahlsatz*) . . . 78
3.58 Bemerkung (*Algorithmus zum Bestimmen von Primzahlen*) . . . 78
3.59 Lemma (*kleiner Fermat'sche Satz*) . . . 78
3.60 Satz (*eulersche* φ*-Funktion*) . . . 78
3.61 Lemma . . . 78
3.62 Satz (*Euler*) . . . 79
3.63 Lemma . . . 79

3.64 Satz (*Euklidischer Algorithmus*) 79
3.65 Definition (*normiertes Polynom*) 79
3.66 Folgerung 79
3.67 Satz 79
3.68 Beispiel 79
3.69 Bemerkung (*diskreter Logarithmus*) 80
3.6 Endliche Körper 80
3.70 Folgerung (*Existenz endlicher Körper*) 80
3.71 Satz (*Eindeutigkeit endlicher Körper*) 80
3.72 Satz (*zyklische multiplikative Gruppen*) 80

Abzählung, Rekursion, Erzeugende Funktionen

1.1 Elementare Zählprinzipien

Sei M eine endliche Menge. Dann wird mit $|M|$ die *Mächtigkeit* (Anzahl der Elemente) von M bezeichnet.

$$|M| = n \in \mathbb{N} \Leftrightarrow \exists f : M \to \{1 \dots n\}, f \text{ ist Bijektion}$$

Eine Menge M mit n Elementen heißt *n-Menge*.

$$|M| = 0 \Leftrightarrow M = \emptyset$$

1.1 Lemma *(Rechenregeln für Mächtigkeiten)*

Seien A,B Mengen. Es gilt:

a) $|A| = |B| \Leftrightarrow \exists f : A \to B$ bijektiv

b) $|A \uplus B| = |A| + |B|$

$A \uplus B$ heißt *disjunkte Vereinigung von A und B*. Die disjunkte Vereinigung von A und B ist nur definiert wenn A und B disjunkt sind, d.h. $A \cap B = \emptyset$. Es gilt dann $A \uplus B := A \cup B$.

c) $|A \times B| = |A| \cdot |B|$.

$A \times B$ heißt *kartesisches Produkt von A und B*.

$$A \times B := \{(a,b) | a \in A \wedge b \in B\}$$

1.2 Folgerung *(Anzahl der Abbildungen)*

Seien A, B endliche Mengen und $Abb(A,B) := B^A := \{ f : A \to B\}$. Dann gilt:

$$\left|B^A\right| = |B|^{|A|}$$

Beweis: Sei $|A| = n \in \mathbb{N}$, $A = \{a_1, \ldots, a_n\}$. Es existiert eine Bijektion von B^A nach B^n, z.B.

$$f : B^A \to B^n, g \mapsto (g(a_1), \ldots, g(a_n))$$

Nach Lemma 1.1 folgt

$$\left|B^A\right| = |B^n| = |B|^n = |B|^{|A|}$$

♢

1.3 Definition *(Permutation)*

Sei A eine Menge. Eine bijektive Abbildung $f : A \to A$ heißt *Permutation von A*.

1.4 Lemma *(Mächtigkeit der symmetrischen Gruppe)*

Sei $S_n := \{a : \{1, \ldots, n\} \to \{1, \ldots, n\} | a \text{ bijektiv}\}$ (S_n heißt *symmetrische Gruppe vom Grad n*). Dann gilt:

$$|S_n| = n!$$

Beweis siehe LA1

Bemerkung $n!$ =Anzahl der Möglichkeiten, eine n-Menge anzuordnen.

1.5 Satz *(Mächtigkeit der Potenzmenge)*

Die Menge $\wp(A) := \{B \subseteq A\}$ heißt *Potenzmenge von A*. Für $A = \{1,2\}$ gilt z.B. $\wp(A) = \{\emptyset, \{1\}, \{2\}, A\}$.
Ist $|A| = n \in \mathbb{N}$, dann gilt:

$$|\wp(A)| = 2^n$$

Beweis Definiere für jedes $B \subseteq A$

$$\Upsilon_B : \quad A \to \{0,1\}$$
$$\Upsilon_B(x) = \begin{cases} 1 & \text{falls } x \in B \\ 0 & \text{falls } x \notin B \end{cases}$$

Es gilt $f : \wp(A) \to \{0,1\}^A$ mit $f(B) = \Upsilon_B$ ist eine Bijektion von $\wp(A)$ nach $\{0,1\}^A$, und somit

$$|\wp(A)| = \left|\{0,1\}^A\right| = 2^{|A|} = 2^n$$

♢

1.6 Definition *(Menge der k-Teilmengen)*

Sei A eine Menge, $k \in \mathbb{N}$, $k \leq |A|$

$$\wp_k(A) := \left(\begin{array}{c} A \\ k \end{array} \right) := \{B \subseteq A \,|\, |B| = k\}$$

$\wp_k(A)$ heißt *Menge der k-Teilmengen von A*.

1.7 Bemerkung *(Partitionierung der Potenzmenge)*

$$\wp(A) = \biguplus_{k=0}^{|A|} \wp_k(A)$$

$$|\wp(A)| = \sum_{k=0}^{|A|} |\wp_k(A)|$$

1.8 Lemma *(Anzahl der k-Teilmengen)*

Sei A eine n-Menge. Dann gilt:

$$\left(\begin{array}{c} n \\ k \end{array} \right) := \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = |\wp_k(A)|$$

$\left(\begin{array}{c} n \\ k \end{array} \right)$ heißt *Binomialkoeffizient*.

Beweis Es gilt für die Permutationen von k Elementen einer n-Menge:

$$\left| \{(a_1 \ldots a_k) \in A^k | a_i \neq a_j \forall i \neq j\} \right| = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

.

Es gibt jedoch $k!$ Anordnungen von $\{a_1 \ldots a_k\}$, also gilt

$$|\wp_k(A)| = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!}$$

$\Diamond$

Dieses Lemma ermöglicht es, einen alternativen Beweis für Satz 1.5 anzugeben:

$|\wp(A)| = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \cdot 1^k \cdot 1^{n-k} = (1+1)^n = 2^n.$

1.9 Lemma *(Pascal-Dreieck)*

Behauptung $\forall n,k \in \mathbb{N}$ mit $n > k$ gilt $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right)$

Beweis (kombinatorisch) $\left(\begin{array}{c} n \\ k \end{array} \right)$ =Anzahl der k-Teilmengen einer n-Menge

Sei $A = \{a_1 \ldots a_n\}$, $|A| = n$. Dann gilt:

$$\begin{array}{rrcl} & \wp_k(A) & = & \{M \subseteq A \,|\, |M| = k\} \\ & & = & \{M' \uplus \{a_n\} | M' \subseteq A \setminus \{a_n\} \wedge |M'| = k-1\} \uplus \{M'' \subseteq A \setminus \{a_n\} \,|\, |M''| = k\} \\ \Rightarrow & |\wp_k(A)| & = & \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right) \end{array}$$

$\Diamond$

						1										n=0
					1		1									n=1
				1		2		1								n=2
			1		3		3		1							n=3
		1		4		6		4		1						n=4
	1		5		10		10		5		1					n=5
1		6		15		20		15		6		1				n=6
	7		21		35		35		21		7		1			n=7
8		28		56		70		56		28		8		1		n=8
						⋮										

Tabelle 1: Pascal-Dreieck

1.10 Satz *(Vandermonde'sche Identität)*

$$\binom{n+m}{k} = \sum_{l=0}^{k} \binom{n}{l} \cdot \binom{m}{k-l}$$

Beweis Sei A eine Menge, $A = B \uplus C$, $|B| = n$, $|C| = m$. Ferner sei $\binom{A}{k}_l := \{X \subseteq A \,|\, |X| = k \wedge |X \cap B| = l\}$. Dann gilt:

$$\binom{A}{k} = \biguplus_{l=0}^{k} \binom{A}{k}_l$$

also:

$$\binom{m+n}{k} = \sum_{l=0}^{k} \left| \binom{A}{k}_l \right| = \sum_{l=0}^{k} \binom{n}{l} \binom{m}{k-l}$$

♢

Anwendung *(Bezierkurven)*

Seien $P_1 \ldots P_n$ Stützstellen. Dann ist $p(t) = \sum_{i=1}^{n} B_{n,i}(t) \cdot P_i$ $t \in [0,1]$ mit $B_{n,i}(t) = \binom{n}{i} \cdot t^i \cdot (1-t)^{n-i}$ eine Bezierkurve. Nach Satz 1.9 gilt $B_{n,i}(t) = t \cdot B_{(n-1),(i-1)}(t) + (1-t)B_{(n-1),i}(t)$. Man erreicht eine effiziente Berechnung der Kurve, da man zur Berechnung eines Summanden von $p(t)$ auf bereits berechnete Koeffizienten $B_{p,q}(t)$ zurückgreifen kann.

1.11 Lemma *(doppeltes Abzählen)*

Seien S und T Mengen und $R \subseteq S \times T$ eine Relation. Es gilt:

$$|R| = \underbrace{\sum_{s \in S} |\{t \in T \,|\, (s,t) \in R\}|}_{\text{Zeilensumme}} = \underbrace{\sum_{t \in T} |\{s \in S \,|\, (s,t) \in R\}|}_{\text{Spaltensumme}}$$

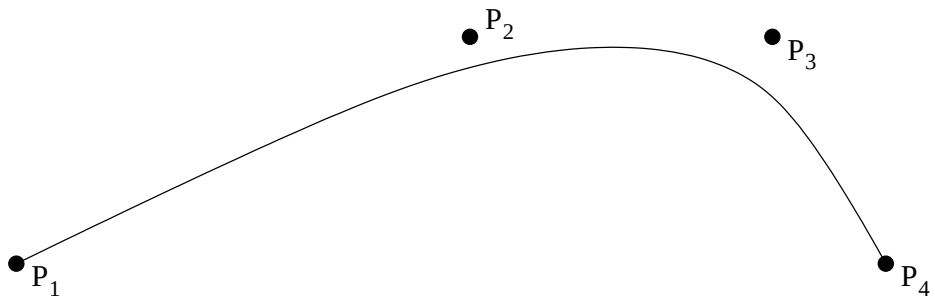


Abbildung 1: Bezierkurve

1.12 Satz *(Schubfachprinzip)*

Seien X und Y Mengen mit $|X| > |Y|$und $f : X \to Y$ eine Abbildung. Dann gilt:

$$\exists y \in Y : \left| f^{-1}(y) \right| \geq 2$$

Verteilt man n Elemente auf m Fächer (wobei $n > m$), so gibt es ein Fach, das mindestens zwei Elemente erhält.

1.13 Beispiel

1) In jeder Gruppe von 13 Personen befinden sich mindestens zwei, die im gleichen Monat Geburtstag haben.

2) In jeder Gruppe P von Personen gibt es zwei Personen, die die gleiche Anzahl von Personen kennen. „Kennen“ ist dabei als symmetrische Relation gemeint, d.h A kennt $B \Rightarrow B$ kennt A. Dieser Sachverhalt kann anhand eines ungerichteten Graphen veranschaulicht werden (siehe Abbildung 2). Die Knoten stellen die Personen dar, Wenn zwei Personen einander kennen wird dies durch eine Kante zwischen den entsprechenden Knoten gekennzeichnet.

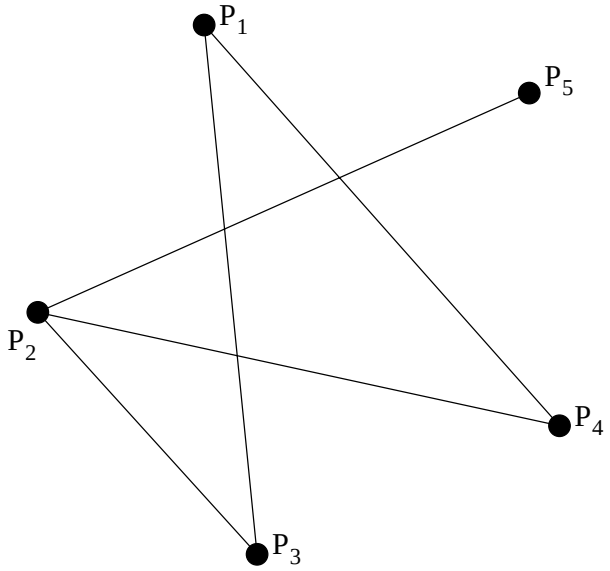


Abbildung 2: Ungerichteter Graph

Beweis: Setze $P = \{p_1, \ldots, p_n\}$ und $f : P \to \{0, \ldots, n-1\}$ so daß

$$f(x) = y \Leftrightarrow \text{Person x kennt genau y Personen aus P}$$

Fall 1: $f(p_i) = 0$ für ein $p_i \in P$

$\Rightarrow \forall j \neq i : f(p_j) \neq n-1$

$\Rightarrow f(P) \subseteq \{0, \ldots, n-2\}$

Fall 2: $\forall p \in P : f(p) \neq 0$

$\Rightarrow f(P) \subseteq \{1, \ldots, n-1\}$

In jedem Fall gilt also $|P| > |f(P)|$. Nach dem Schubfachprinzip gilt also $\exists p_k, p_l \in P : f(p_k) = f(p_l)$.

$\Diamond$

1.14 Satz *(verallgemeinertes Schubfachprinzip)*

Ist $f : X \to Y$ eine Abbildung, so gibt es ein $y \in Y$ mit $\left|f^{-1}(y)\right| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$.

Beweis (indirekt): Angenommen $\forall y \in Y : \left|f^{-1}(y)\right| \leq \left\lceil \frac{|X|}{|Y|} \right\rceil - 1$. Dann gilt:

$$\begin{array}{rcl} |X| & = & \left|\biguplus_{y \in Y} f^{-1}(y)\right| \\ & = & \sum_{y \in Y} \left|f^{-1}(y)\right| \\ & \leq & |Y| \cdot \left(\left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \right) \\ & \leq & |Y| \cdot \left(\left(\frac{|X|-1}{|Y|} + 1 \right) - 1 \right) \\ & = & |X| - 1 \end{array}$$

$\Diamond$

Rückblick *(Verallgemeinerungen von Lemma 1.11)*

c) Sei $M = A_1 \times \ldots \times A_n$.

Dann gilt: $|M| = \prod_{i=1}^{n} A_i$ (Produktregel).

b) Seien $A_1, \ldots, A_n$ paarweise disjunkt (d.h. gilt $\forall i \neq j : A_i \cap A_j = \emptyset$) und $S = \biguplus_{i=1}^{n} A_i$.

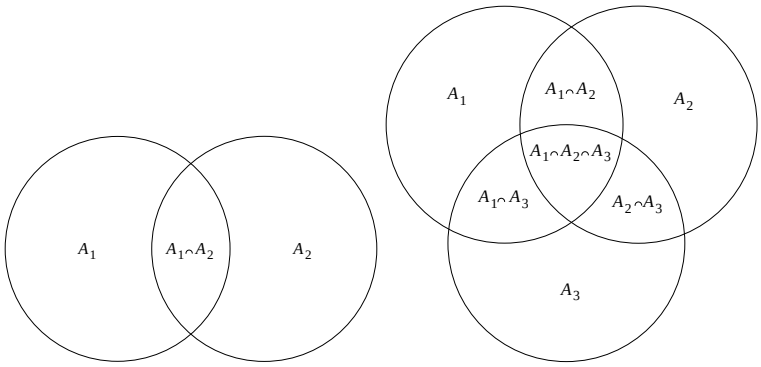
Dann gilt: $|S| = \sum_{i=1}^{n} |A_i|$(Summenregel).

Problem: Wie bestimmt man die Mächtigkeit von S wenn $A_1, \ldots, A_n$ nicht paarweise disjunkt sind?

Für zwei Mengen A_1 und A_2 gilt $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

Für drei Mengen A_1,A_2 und A_3 gilt

$$\begin{array}{rcl} |A_1 \cup A_2 \cup A_3| = & & |A_1| + |A_2| + |A_3| \\ & - & |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ & + & |A_1 \cap A_2 \cap A_3| \end{array}$$



(a) 2 Mengen (b) 3 Mengen

Abbildung 3: Schnittmengen

1.15 Satz *(Prinzip der Inklusion und Exklusion / Siebformel)*

Für endliche Mengen $A_1, \ldots, A_n$ gilt

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{r=1}^{n} (-1)^{r-1} \cdot \sum_{1 \le i_1 < \ldots < i_r \le n} \left| \bigcap_{j=1}^{r} A_{i_j} \right|$$

Beweis: Sei $a \in \bigcup_{i=1}^{n} A_i$.

Auf der linken Seite der Behauptung wird a genau ein mal gezählt. Es genügt, zu zeigen, daß auf der rechten Seite a auch genau ein mal gezählt wird.

o.B.d.A gilt $a \in A_{t_j}$ für $j = 1 \ldots l$ (d.h. $a \in \bigcap_{j=1}^{l} A_{t_j}$ und $a \notin (\bigcup_{i=1}^{n} A_i) \setminus \left(\bigcap_{j=1}^{l} A_{t_j} \right)$). Dann wird a in der Summe $\sum_{1 \le i_1 < \ldots < i_r \le n} \left| \bigcap_{j=1}^{r} A_{i_j} \right|$ genau $\binom{l}{r}$ mal gezählt, denn $\{t_1, \ldots, t_l\}$ enthält genau $\binom{l}{r}$ r-Teilmengen.

Es folgt, a wird auf der rechten Seite genau $\sum_{r=1}^{l} (-1)^{r-1} \cdot \binom{l}{r}$

$= 1 + (-1 + \sum_{r=1}^{l} (-1)^{r-1} \cdot \binom{l}{r}$

$= 1 - \sum_{r=0}^{l} (-1)^r \cdot \binom{l}{r}$

$= 1 - \sum_{r=0}^{l} \binom{l}{r} \cdot (-1)^r \cdot 1^{r-l}$

$= 1 - (-1+1)^l$

$= 1$ mal gezählt.

$\Diamond$

1.16 Beispiel

Sei $k \in N$ und $M_k = \{n \in \mathbb{N} | 1 \le n \le 100 \wedge n | k\}$. Bestimme $|M_2 \cup M_3 \cup M_5|$.

Lösung: $|M_k| = \left\lfloor \frac{100}{k} \right\rfloor$ da genau jede k-te natürliche Zahl durch k teilbar ist.

$$\begin{aligned}|M_2 \cup M_3 \cup M_5| &= |M_2| + |M_3| + |M_5| - |M_2 \cap M_3| - |M_2 \cap M_5| - |M_3 \cap M_5| + |M_2 \cap M_3 \cap M_5| \\ &= |M_2| + |M_3| + |M_5| - |M_6| - |M_{10}| - |M_{15}| + |M_{30}| \\ &= 50 + 33 + 20 - 16 - 10 - 6 + 3 \\ &= 74\end{aligned}$$

1.2 Mengenpartitionen

1.17 Definition *(Partition, Stirlingzahlen zweiter Art)*

Sei M eine n-Menge.

- Eine „Partition von M“ ist eine Zerlegung von M in disjunkte, nicht leere Teilmengen.
  $P = \{A_1, \ldots, A_k\}$ ist Partition von M $\Leftrightarrow \bigcup_{i=1}^{k} A_i = M \wedge \forall i \neq j \in \{1, \ldots, k\} : A_i \neq \emptyset \wedge A_i \cap A_j = \emptyset$.
- Eine Partition P von M heißt k-Partition von M genau dann wenn $|P| = k$.
- $Part_k(M) := \{P \subseteq \wp(M) | P \text{ ist k} - \text{Partition von } M\}$.
- $\left\{ \begin{array}{c} n \\ k \end{array} \right\} := S_{n,k} := |Part_k(M)|$ wenn M eine n-Menge ist und $n, k > 0$. $S_{0,0} := 1$
  Die Zahlen $S_{n,k}$ heißen „Stirlingzahlen zweiter Art“.

1.18 Beispiel

i) Sei $M = \{1,2,3,4\}$.

$$\begin{aligned}Part_1(M) &= \{\{M\}\} \\ Part_2(M) &= \{\{\{1\},\{2,3,4\}\},\{\{2\},\{1,3,4\}\},\{\{3\},\{1,2,4\}\}, \\ &\quad \{4\},\{1,2,3\}\}\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\}, \\ &\quad \{\{1,4\},\{2,3\}\}\} \\ &= \{\{A, M \setminus A\} | A \neq \emptyset \wedge A \neq M\}\end{aligned}$$

Im allgemeinen gilt $|Part_2(M)| = \frac{1}{2} \cdot (2^n - 2)$ für jede n-Menge M.

ii) Für $n \geq 1$ gilt:

$$\begin{aligned}S_{n,,0} &= 0 \\ S_{n,1} &= 1 \\ S_{n,n-1} &= \left(\begin{array}{c} n \\ 2 \end{array} \right) \\ S_{n,n} &= 1 \\ S_{n,k} &= 0 \forall k > n\end{aligned}$$

1.19 Satz *(Stirling-Dreieck zweiter Art)*

$\forall n, k \in \mathbb{N}$ mit $1 \leq k \leq n$ gilt:

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$$

Beweis (kombinatorisch): Sei $A = \{a_1, \ldots, a_n\}$. Die Idee des Beweises ist, die Menge aller k-Partitionen von A in zwei disjunkte Teilmengen T_1 und T_2 zu zerlegen, daß $|T_1| = S_{n-1,k-1}$ und $|T_2| = k \cdot S_{n-1,k}$. Nach Summenregel (Lemma 1.1) gilt dann $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$.

$$
\begin{aligned}
Part_k(A) &= \{P \in Part_k(A) | \{a_n\} \in P\} \uplus \\
&\quad \{P \in Part_k(A) | \{a_n\} \notin P\} \\
&= \{P' \cup \{a_n\} | P' \in Part_{k-1}(A \setminus \{a_n\})\} \uplus \\
&\quad \biguplus_{i=1}^{k} \{\{B_1, \ldots, B_i \cup \{a_n\}, \ldots, B_k\} | \{B_1, \ldots, B_k\} \text{ ist k – Partition von } A \setminus \{a_n\}\} \\
\Rightarrow |Part_k(A)| &= \left|\{P' \cup \{a_n\} | P' \in Part_{k-1}(A \setminus \{a_n\})\}\right| + \\
&\quad \sum_{i=1}^{k} |\{\{B_1, \ldots, B_i \cup \{a_n\}, \ldots, B_k\} | \{B_1, \ldots, B_k\} \text{ ist k – Partition von } A \setminus \{a_n\}\}| \\
&= S_{n-1,k-1} + \\
&\quad k \cdot |\{\{B_1, \ldots, B_k\} \in Part_k(A \setminus \{a_n\})\}| \\
&= S_{n-1,k-1} + k \cdot S_{n-1,k}
\end{aligned}
$$

♢

				1					n=0
			0		1				n=1
		0		1		1			n=2
	0		1		3		1		n=3
0		1		7		6		1	n=4
				⋮				⋱	

Tabelle 2: Stirling-Dreieck zweiter Art

1.20 Satz *(Anzahl der injektiven und surjektiven Abbildungen)*

Seien M und N Mengen mit $|M| = m \in \mathbb{N}$ und $|N| = n \in \mathbb{N}$, so gilt:

a) $|Abb(M,N)| = n^m$.

b) $|Inj(M,N)| = n^{\underline{m}} = n \cdot (n-1) \cdot \ldots \cdot (n-(m+1))$.

$n^{\underline{m}}$ wird ausgesprochen „n hoch m fallend“. $Inj(M,N)$ ist die Menge der injektiven Abbildungen von M nach N.

c) $|Surj(M,N)| = n! \cdot S_{m,n}$.

Beweis: Sei $M = \{a_1, \ldots, a_m\}$ eine m-Menge.

a) siehe Folgerung 1.2

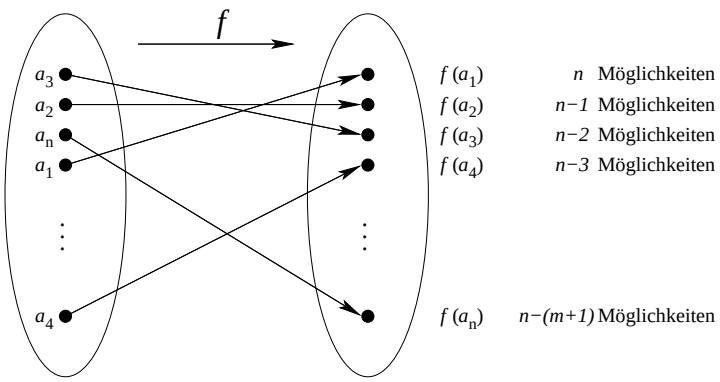


Abbildung 4: Injektive Abbildung

b) $f : M \to N$ ist injektiv $\Leftrightarrow \forall i \neq j : f(a_i) \neq f(a_j)$

Mit der Produktregel (Lemma 1.1) folgt die Behauptung aus

$$|Inj(M,N)| = |N \times N \setminus \{f(a_1)\} \times N \setminus \{f(a_1), f(a_2)\} \times \ldots \times N \setminus \{f(a_1), \ldots, f(a_{m-1})\}|$$

$\Diamond$

c) Sei $N = \{b_1, \ldots, b_n\}$ eine n-Menge und $f : M \to N$ surjektiv.

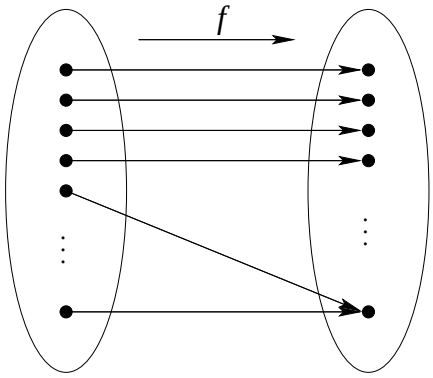


Abbildung 5: Surjektive Abbildung

Die Menge $\{f^{-1}(b_i) | b_j \in N\}$ bildet eine n-Partition von M. Jede n-Partition von M induziert allerdings durch jede Permutation von N eine unterschiedliche surjektive Funktion. Es folgt:

$$\begin{aligned} |Surj(M,N)| &= \text{Anzahl der Permutationen von } N \cdot \text{ Anzahl der n – Partitionen von } M \\ &= n! \cdot S_{m,n} \end{aligned}$$

$\Diamond$

1.21 Satz *(Potenzen und Stirlingzahlen)*

$$n^m = \sum_{k=0}^{n} n^{\underline{k}} \cdot S_{m,k}$$

Beweis: Sei M eine m-Menge und N eine n-Menge. Jede Abbildung $f : M \to N$ kann dann als surjektive Abbildung $f' : M \to Bild(f)$ interpretiert werden. Es gilt dann:

$$\begin{aligned}
Abb(M,N) &= \biguplus_{A \subseteq N} Surj(M,A) \\
\Rightarrow |Abb(M,N)| &= \sum_{A \subseteq N} |Surj(M,A)| \\
&= \sum_{k=0}^{n} \sum_{A \in \binom{N}{k}} |Surj(M,A)| \\
&= \sum_{k=0}^{n} \sum_{A \subseteq \binom{N}{k}} k! \cdot S_{m,k} \\
&= \sum_{k=0}^{n} \binom{n}{k} k! \cdot S_{m,k} \\
&= \sum_{k=0}^{n} \frac{n^{\underline{k}}}{k!} k! \cdot S_{m,k} \\
\Rightarrow n^m &= \sum_{k=0}^{n} n^{\underline{k}} \cdot S_{m,k}
\end{aligned}$$

♢

1.3 Permutationen

Wiederholung

$S_n := Sym(\{1,\ldots,n\}) := \{\sigma : \{1,\ldots,n\} \to \{1,\ldots,n\} | \sigma \text{ ist bijektiv}\}$, $|S_n| = n!$.

Bemerkung Jede Permutation $\sigma \in S_n$ kann wie folgt dargestellt werden:

- durch eine Wertetabelle

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 3 & 7 & 2 & 1 & 9 & 5 & 8 & 11 & 6 & 10 \end{pmatrix}$$

- als Produkt von Zyklen

$$\sigma = (1\,4\,2\,3\,7\,5) \circ (8) \circ (6\,9\,11\,10)$$

1.22 Definition *(k-Zyklus)*

Ein k-Zyklus $(i_1 \dots i_k)$ ist eine Permutation $\sigma \in S_n$ mit

$$\begin{aligned} \sigma(i_j) &= \sigma(i_{j+1}) \forall j = 1,\dots,k-1 \\ \sigma(i_k) &= i_1 \\ \sigma(i) &= i \forall i \notin \{i_1,\dots,i_k\} \end{aligned}$$

1.23 Bemerkung *(Zykeldarstellung von Permutationen)*

1) Ein Zyklus ist durch die (zyklische) Reihenfolge der Elemente des Zykels eindeutig bestimmt. $(1234) = (2341)$

2) Jede Permutation $\sigma \in S_n$ läßt sich als Produkt von Zyklen schreiben.

Beispiel: $S_3 = \{(1)(2)(3),(1)(23),(2)(13),(3)(12),(123),(132)\}$, $|S_3| = 3! = 6$.

1.24 Definition *(Stirlingzahlen erster Art)*

Die Anzahl der Permutationen von $\{1,\dots,n\}$ mit genau $k \in \mathbb{N}$ Zyklen wird mit $s_{n,k}$ oder $\left[\begin{array}{c} n \\ k \end{array} \right]$ bezeichnet. Die Zahlen $s_{n,k}$ heißen „Stirlingzahlen erster Art“. Es gilt:

$$\begin{aligned} s_{0,0} &:= 1 \\ s_{n,0} &= 0 \; \forall n \in \mathbb{N} \\ s_{n,k} &= 0 \; \forall k > n \end{aligned}$$

1.25 Satz *(Stirling-Dreieck erster Art)*

$\forall n,k \in \mathbb{N}$ mit $n \geq k \geq 1$ gilt:

$$s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$$

Beweis (kombinatorisch): Der Beweis funktioniert ähnlich wie der Beweis von Satz 1.19. Die Menge aller Permutationen mit genau k Zyklen wird in zwei disjunkte Teilmengen T_1 und T_2 zu zerlegen, daß $|T_1| = s_{n-1,k-1}$ und $T_2 = (n-1) \cdot S_{n-1,k}$.

$$\begin{aligned} & \{\sigma_1 \circ \dots \circ \sigma_k | \sigma_1 \circ \dots \circ \sigma_k \text{ ist Permutation von } \{1,\dots,n\} \text{ mit genau } k \text{ Zyklen}\} \\ = \; & \{\sigma'_1 \circ \dots \circ \sigma'_{k-1} \circ (n) | \sigma'_1 \circ \dots \circ \sigma'_{k-1} \text{ ist Permutation von } \{1,\dots,n-1\} \text{ mit genau } k-1 \text{ Zyklen}\} \quad \uplus \\ & \uplus_{i=1}^{n-1} \{\sigma''_1 \circ \dots \circ \sigma''_k | \sigma''_1 \circ \dots \circ \sigma''_k \text{ ist Permutation von } (\{1,,n-1\} \setminus \{i\}) \cup \{(in)\}\} \\ \Rightarrow \; & s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k} \end{aligned}$$

$\Diamond$

Beispiel (zum Beweis) Betrachte die Permutationen von $\{1,2,3,4,5\}$ mit genau 3 Zyklen [... Beispiel fehlt ...]

					1							n=0
				0		1						n=1
			0		1		1					n=2
		0		2		3		1				n=3
	0		6		11		6		1			n=4
0		24		15		35		10		1		n=5
					⋮							⋱

Tabelle 3: Stirling-Dreieck erster Art

1.4 Erzeugende Funktionen / Formale Potenzreihen

Bei der Komplexitätsanalyse von Algorithmen entstehen oft Rekursionsgleichungen, z.B. $a_0 = 0$, $a_1 = 1$, $a_i = a_{i-1} + a_{i-2} \forall i \geq 2$. Um die Lösung einer Rekursionsgleichung zu finden benutzen wir erzeugende Funktionen. Rekursionsgleichungen beschreiben eine unendliche Folge $(a_n)_{n\in\mathbb{N}} := a_1, a_2, \ldots$. Wir führen für Folgen eine andere Schreibweise ein:

$$\sum_{n=0}^{\infty} a_n x^n := (a_n)_{n\in\mathbb{N}}$$

1.27 Definition *(formale Potenzreihe, erzeugende Funktion)*

Sei K ein Körper (z.B. $K = \mathbb{R}$ oder $K = \mathbb{C}$) und $(a_n)_{n\in\mathbb{N}}$ eine Folge. Die formale Potenzreihe

$$A(x) := \sum_{n=0}^{\infty} a_n x^n$$

heißt „erzeugende Funktion der Folge $(a_n)_{n\in\mathbb{N}}$“. Die Menge aller formalen Potenzreihen über K wird mit $K[[x]]$ bezeichnet.

$$K[[x]] := \left\{ \sum_{n=0}^{\infty} a_n x^n | a_n \in K \forall n \in \mathbb{N}_0 \right\}$$

1.28 Bemerkung

1) Für $k \in \mathbb{N}_0$ gilt $x^k = (a_n)_{\mathbb{N}_0}$ mit $a_n = \begin{cases} 1 & \text{falls } n = k \\ 0 & \text{sonst} \end{cases}$.

$$\begin{aligned} \delta_{n,k} &:= \begin{cases} 1 & \text{falls } n = k \\ 0 & \text{sonst} \end{cases} \quad \text{heißt } 'Kronecker - Symbol' \\ x^k &= (\delta_{n,k})_{n\in\mathbb{N}_0} \end{aligned}$$

2) Für $m \in \mathbb{N}_0$ gilt $\sum_{n=m}^{\infty} a_n x^n = (b_j)_{j\in\mathbb{N}_0}$ mit $b_j = \begin{cases} 0 & \text{falls } j < m \\ a_j & \text{falls } j \geq m \end{cases}$.

3) $\sum_{n=0}^{\infty} a_n x^{kn} = (b_j)_{j\in\mathbb{N}_0}$ mit $b_j = \begin{cases} a_n & \text{falls } j = kn \text{ für ein } n \in \mathbb{N}_0 \\ 0 & \text{sonst} \end{cases}$.

4) Unterschiede zwischen Potenzreihen der Analysis und formalen Potenzreihen:

Potenzreihen in der Analysis	formale Potenzreihe
• $f(x) = \sum_{n=0}^{\infty} a_n x^n$	• $A(x) = \sum_{n=0}^{\infty} a_n x^n = (a_n)_{n\in\mathbb{N}_0}$
• beschreibt eine unendliche Summe	• beschreibt eine unendliche Folge
• Funktion in der Variable x	• für x wird im allgemeine nichts eingesetzt
• Konvergenz als zentrale Frage	• Konvergenz interessiert nicht

5) Seien $(a_n)_{n\in\mathbb{N}_0}$, $(b_n)_{n\in\mathbb{N}_0}$ Folgen und $A(x) = \sum_{n=0}^{\infty} a_n x^n$, $B(x) = \sum_{n=0}^{\infty} b_n x^n$ formale Potenzreihen.

$$A(x) = B(x) :\Leftrightarrow \forall n \in \mathbb{N}_o : a_n = b_n$$

1.29 Definition *(Rechnen mit Potenzreihen)*

Sei K ein Körper und $(a_n)_{n\in\mathbb{N}_0}, (b_n)_{n\in\mathbb{N}_0} \in K^{\infty}$, $a \in K$.

- Die Addition von Potenzreihen ist definiert durch:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

- Die Multiplikation von Potenzreihen ist definiert durch:

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n\right) := \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

  Die Multiplikation heißt auch „Faltung“ oder „Konvolution“ von $(a_n)_{n\in\mathbb{N}_0}$ und $(b_n)_{n\in\mathbb{N}_0}$, und ist analog zum Cauchy-Produkt der Analysis definiert.

- Die Multiplikation einer Potenzreihe mit einem Skalar ist definiert als:

$$a \cdot \left(\sum_{n=0}^{\infty} a_n x^n\right) := \sum_{n=0}^{\infty} a \cdot a_n x^n$$

1.30 Lemma *(Verschieben von Folgengliedern)*

$$x^m \cdot \sum_{n=0}^{\infty} a_n x^n = \sum_{n=m}^{\infty} a_n x^n$$

das heißt:

$$x^m \cdot (a_0\, a_1 \ldots) = (\underbrace{0 \ldots 0}_{m \text{ mal}}\, a_0\, a_1 \ldots)$$

Beweis: $x^m = (\delta_{m,n})_{n\in\mathbb{N}_0}$

$$\begin{aligned} x^m \cdot \sum_{n=0}^{\infty} a_n x^n &= \left(\sum_{n=0}^{\infty} \delta_{m,n} x^n\right) \cdot \left(\sum_{n=0}^{\infty} a_n x^n\right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \delta_{n,k} a_k\right) x^n \\ &= \sum_{n=m}^{\infty} a_{n-m} x^n \end{aligned}$$

♢

1.31 Beispiel

Es gilt $x^m \cdot x^n = x^{m+n} \forall m,n \in \mathbb{N}_0$.

1.32 Satz *(Eigenschaften von $K[[x]]$)*

a) $K[[x]]$ ist ein K-Vektorraum.

b) $(K[[x]],+,\cdot)$ ist ein kommutativer Ring mit Nullelement $0 = 0 \cdot x^0$ und Einselement $1 = 1 \cdot x^0$.

Beweis Nachrechnen.

◊

1.33 Bemerkung *(Invertierbarkeit in Ringen)*

Gilt in einem kommutativen Ring mit Eins $A \cdot B = 1$, so ist B durch A eindeutig bestimmt. Ebenso ist dann auch A durch B eindeutig bestimmt. $B = A^{-1} = \frac{1}{A}$ und $A = B^{-1} = \frac{1}{B}$. A und B heißen „invertierbar“.

1.34 Lemma *(Invertierbarkeit der geometrischen Reihe)*

In $K[[x]]$ ist $\sum_{i=0}^{\infty} c^i x^i$ für jedes $c \in K$ invertierbar und es gilt:

$$\sum_{i=0}^{\infty} c^i x^i = \frac{1}{1-cx}$$

Beweis

$$\begin{aligned}
(1-cx) \cdot \sum_{i=0}^{\infty} c^i x^i &= \sum_{i=0}^{\infty} c^i x^i - cx \sum_{i=0}^{\infty} c^i x^i \\
&= \sum_{i=0}^{\infty} c^i x^i - \sum_{i=0}^{\infty} cxc^i x^i \\
&= \sum_{i=0}^{\infty} c^i x^i - \sum_{i=0}^{\infty} c^{i+1} x^{i+1} \\
&= \sum_{i=0}^{\infty} c^i x^i - \sum_{i=1}^{\infty} c^i x^i \\
&= c^0 x^0 \\
&= 1
\end{aligned}$$

◊

Bemerkung Wegen der Gleichheit $\sum_{i=0}^{\infty} c^i x^i = \frac{1}{1-cx}$ ist $\frac{1}{1-cx}$ auch eine formale Potenzreihe.

$\sum_{i=0}^{\infty} c^i x^i$ heißt „geometrische Reihe“.

1.35 Beispiel *(Code mit variabler Wortlänge zur Datenkompression)*

Sei $Bn = \{a,b,c\}$, $Zi = \{0,1\}$. Für $k \in \mathbb{N}$ sei $W_k = \{\text{Folge aus } i \text{ Buchtaben gefolgt von } k-i \text{ Ziffern} \mid 1 < i < k\}$. Es gilt

$$\begin{aligned} w_k := |W_k| &= \sum_{i=1}^{k-1} 3^i 2^{k-i} \\ &= \underbrace{\sum_{i=0}^{k} 3^i 2^{k-i}}_{=:c_k} - 2^k - 3^k \end{aligned}$$

Behauptung: $c_k = 3^{k+1} - 2^{k+1}$

Beweis:

$$\begin{aligned} \sum_{k=0}^{\infty} c_k x^k &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} 3^i 2^{k-i} \right) x^k \\ &= \left(\sum_{i=0}^{\infty} 3^i x^i \right) \cdot \left(\sum_{i=0}^{\infty} 2^i x^i \right) \\ &= \frac{1}{1-3x} \cdot \frac{1}{1-2x} \\ &= \frac{3}{1-3x} - \frac{2}{1-2x} \\ &= \left(3 \cdot \sum_{k=0}^{\infty} 3^k x^k \right) - \left(2 \cdot \sum_{k=0}^{\infty} 2^k x^k \right) \\ &= \sum_{k=0}^{\infty} \left(3^{k+1} - 2^{k+1} \right) x^k \\ \Rightarrow c_k &= 3^{k+1} - 2^{k+1} \end{aligned}$$

♢

$\Rightarrow w_k = 3^{k+1} - 2^{k+1} - 2^k - 3^k = 2 \cdot 3^k - 2^k$

1.36 Satz *(Invertieren von Potenzreihen)*

$A = \sum_{i=0}^{\infty} a_n x^n \in K[[x]]$ ist genau dann invertierbar wenn $a_0 \neq 0$.

Beweis: A ist invertierbar $\Leftrightarrow \exists B = \sum_{i=0}^{\infty} b_n x^n \in K[[x]] : A \cdot B = 1$.

$$\begin{aligned} & A \cdot B = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n = 1 \\ \Leftrightarrow \quad & \sum_{k=0}^{n} a_k b_{n-k} = \begin{cases} 1 & \text{, für } n = 0 \\ 0 & \text{, sonst} \end{cases} \\ \Leftrightarrow \quad & \begin{aligned} a_0 b_0 &= 1 \\ a_0 b_1 + a_1 b_0 &= 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \\ &\vdots \end{aligned} \end{aligned}$$

Ist A invertierbar, so muß also $a_0 \neq 0$ gelten. Ist umgekehrt $a_0 \neq 0$, so definiere:

$$\begin{aligned} b_0 &= \frac{1}{a_0} \\ &\vdots \\ b_n &= -\frac{1}{a_0}(a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0) \; \forall n \in \mathbb{N} \end{aligned}$$

$\Diamond$

1.37 Beispiel

a) $A = 1 - cx = \sum_{n=0}^{\infty} a_n x^n$ mit $a_0 = 1$, $a_1 = -c$, $a_i = 0 \, \forall i > 1$. Bestimme A^{-1}.

Lösung: Sei $A^{-1} = \sum_{n=0}^{\infty} b_n x^n$. Dann gilt:

$$\begin{aligned} a_0 b_0 = 1 &\Rightarrow b_0 = 1 \\ a_0 b_1 + a_1 b_0 = 0 &\Rightarrow b_1 = c \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 &\Rightarrow b_2 = c^2 \\ &\vdots \\ \ldots &\Rightarrow b_n = c^n \end{aligned}$$

Also gilt $\frac{1}{1-cx} = \sum_{n=0}^{\infty} c^n x^n$.

b)

$$\begin{aligned} \frac{1}{(1-cx)^2} &= \frac{1}{1-cx} \cdot \frac{1}{1-cx} \\ &= \left(\sum_{n=0}^{\infty} c^n x^n \right) \cdot \left(\sum_{n=0}^{\infty} c^n x^n \right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} c^k c^{n-k} \right) x^n \\ &= \sum_{n=0}^{\infty} (n+1) c^n x^n \end{aligned}$$

Insbesonders gilt $\frac{c}{(1-cx)^2} = \sum_{n=0}^{n} (n+1) c^{n+1} x^n$.

1.38 Definition *(formale Ableitung)*

Die Abbildung $D : K[[x]] \to K[[x]]$, $\sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n$ heißt „formale Ableitung“.

Bemerkung D ist eine Operation auf Folgen mit

$$D : (a_0 \, a_1 \, a_2 \ldots a_n \ldots) \mapsto (a_1 \, 2a_2 \, 3a_3 \ldots n a_n \ldots)$$

1.39 Lemma *(Linearität und Produktregel der formalen Ableitungen)*

Die Abbildung formale Ableitung ist K-linear und es gilt

a) $D(x^n) = nx^{n-1}$

b) $D(A \cdot B) = D(A) \cdot B + A \cdot D(B)$

Beweis: Nachrechnen!

♢

1.40 Folgerung *(Ableitung des Inversen)*

Ist $A \in K[[x]]$ eine invertierbare erzeugende Funktion, so gilt:

$$D(A^{-1}) = -\frac{D(A)}{A^2}$$

Beweis:

$$\begin{aligned} & A \cdot A^{-1} = 1 \text{ und } D(1) = 0 \\ \Rightarrow \quad & 0 = D(1) = D(A \cdot A^{-1}) = D(A) \cdot A^{-1} + A \cdot D(A^{-1}) \\ \Rightarrow \quad & A \cdot D(A^{-1}) = -D(A) \cdot A^{-1} \\ \Rightarrow \quad & D(A^{-1}) = -D(A) \cdot A^{-2} = -\frac{D(A)}{A^2} \end{aligned}$$

♢

Beispiel *(ein alternativer Beweis für Beispiel 1.37 2))*: Ist $A = 1 - cx$, dann gilt $A^{-1} = \sum_{n=0}^{\infty} c^n x^n$, $D(A) = -c$ und $\frac{1}{1-cx} = \sum_{n=0}^{\infty} c^n x^n$. Nach Definition 1.38 gilt $D(A^{-1}) = \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n$.

$$\begin{aligned} \Rightarrow \quad & D(A^{-1}) = \frac{D(A)}{A^2} = -\frac{c}{(1-cx)^2} = \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n \\ \Rightarrow \quad & \frac{1}{(1-cx)^2} = \sum_{n=0}^{\infty} (n+1)c^n x^n \end{aligned}$$

♢

1.41 Folgerung

$$\forall m \in \mathbb{N} : \frac{1}{(1-cx)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{n-1} c^n x^n$$

Beweis: Übung.

♢

1.42 Bemerkung

- Erzeugende Funktionen können im Prinzip wie normale Funktionen behandelt werden.
- Falls zu einer Funktion F eine Potenzreihe existiert, dann kann man diese durch Taylor-Entwicklung um 0 beschreiben.
$$F(x) = \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!} = \left(\frac{F^{(n)}(0)}{n!} \right)_{n \in \mathbb{N}_0}$$
- Einige wichtige Potenzreihen und ihre erzeugenden Funktionen sind in Tabelle 4 aufgelistet. Dabei gilt
$$\binom{r}{0} := 1, \binom{r}{k} := \frac{r \cdot (r-1) \cdot \ldots \cdot (r-k+1)}{k!} \forall r \in \mathbb{R}$$
$\binom{r}{k}$ heißt „verallgemeinerter Binomialkoeffizient“ und es gilt $(1+x)^y = \sum_{k=0}^{\infty} \binom{y}{k} x^k \forall y \in \mathbb{R}$.

a_n	Folge	Potenzreihe	erzeugende Funktion
1	$1,1,1,1,\ldots$	$\sum_{n=0}^{\infty} x^n$	$\frac{1}{1-x}$
n	$1,2,3,4,\ldots$	$\sum_{n=0}^{\infty} nx^n$	$\frac{x}{(1-x)^2}$
c^n	$1,c,c^2,c^3\ldots$	$\sum_{n=0}^{\infty} c^n x^n$	$\frac{1}{c-x}$
n^2	$0,1,4,9,\ldots$	$\sum_{n=0}^{\infty} n^2 x^n$	$\frac{x(1+x)}{(1-x)^3}$
$\binom{r}{n}$	$1, r, \binom{r}{2}, \binom{r}{3}, \ldots$	$\sum_{n=0}^{\infty} \binom{r}{n} x^n$	$\frac{1}{(1+x)^r}$
$\binom{r+n}{n}$	$1, r+1, \binom{r+2}{2}, \binom{r+3}{3}, \ldots$	$\sum_{n=0}^{\infty} \binom{r+n}{n} x^n$	$\frac{1}{(1-x)^{r+1}}$
$\frac{1}{n}$	$0,1,\frac{1}{2},\frac{1}{3},\ldots$	$\sum_{n=0}^{\infty} \frac{1}{n} x^n$	$\ln \frac{1}{1-x}$
$\frac{1}{n!}$	$1,1,\frac{1}{2},\frac{1}{6},\ldots$	$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$	e^x

Tabelle 4: Formale Potenzreihen und ihre erzeugenden Funktionen

1.5 Rekursionsgleichungen

In einigen grundlegenden algorithmischen Verfahren kommen Rekursionsgleichungen vor:

- „Divide and Conquer“-Algorithmen

  Idee:

  - teile das Problem in kleinere Teilprobleme auf (Divde)
  - löse die Teilprobleme
  - berechne aus den Lösungen der Teilprobleme die Gesamtlösung (Conquer)

  Diese Strategie wird zum Beispiel bei binärer Suche, Mergesort oder dem euklidischen Algorithmus verwendet.
- dynamische Programmierung (Optimierungsprobleme)
- Greedy-Algorithmen

1.43 Definition *(lineare Rekursionsgleichung)*

Eine Rekursionsgleichung der Form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + b_k \forall n \geq k$$

mit Anfangsbedingungen $a_i = b_i \forall i = 0, \ldots, k-1$ heißt "lineare Rekursionsgleichung k-ter Ordnung".

- gilt $b_k = 0$, so heißt die Gleichung „homogene lineare Rekursionsgleichung"
- gilt $b_k \neq 0$, so heißt die Gleichung „inhomogene lineare Rekursionsgleichung"

1.44 Beispiel

1) eine homogene lineare Rekursionsgleichung:

$$\begin{aligned} a_n &= ca_{n-1} \forall n \geq 1, a_0 = 0 \\ a_1 &= ca_0 = cb_0 \\ a_2 &= ca_1 = c^2 b_0 \\ &\vdots \\ \Rightarrow a_n &= c^n b_0 \end{aligned}$$

2) eine inhomogene lineare Rekursionsgleichung:

$$a_0 = b_0,\ a_n = ca_{n-1} + b_1 \text{wobei } c, b_0, b_1 \text{ konstant sind}$$

Behauptung:

$$a_n = \begin{cases} b_0 c^n + b_1 \frac{c^n - 1}{c-1} & \text{falls } c \neq 1 \\ b_0 + n b_1 & \text{falls } c = 1 \end{cases}$$

Beweis: Induktion über n

Induktionsverankerung: Sei $n = 1$

$$a_1 = ca_0 + b1 = \begin{cases} b_0 c^1 + b_1 \frac{c^1 - 1}{c-1} & \text{falls } c \neq 1 \\ b_0 + 1 b_1 & \text{falls } c = 1 \end{cases}$$

Induktionsschluß: Sei $n > 1$ und für alle $m < n$ gelte $a_m = \begin{cases} b_0 c^m + b_1 \frac{c^m - 1}{c-1} & \text{falls } c \neq 1 \\ b_0 + m b_1 & \text{falls } c = 1 \end{cases}$

1. Fall: $c \neq 1$. Es gilt

$$\begin{aligned} a_n &= ca_{n-1} + b_1 \\ &= c\left(b_0 c^{n-1} + b_1 \frac{c^{n-1} - 1}{c-1}\right) + b_1 \\ &= b_0 c^n + b_1 \left(\frac{c^n - c}{c-1} + 1\right) \\ &= b_0 c^n + b_1 \frac{c^n - 1}{c-1} \end{aligned}$$

2.Fall: $c = 1$.

$$a_n = a_{n-1} + b_1 = b_0 + (n-1)b_1 + b_1 = b_0 + n b_1$$

1.45 Beispiel

Sei a_n :=Anzahl der Wörter der Länge n über dem Alphabet $\{a,b\}$ die keine zwei aufeinanderfolgende a's enthalten.

$$a_n = a_{n-1} + a_{n-1} \forall n \geq 3$$

1.46 Beispiel *(Fibonacci-Zahlen)*

Ein Kaninchen bringt ab seinem zweiten Lebensmonat jeden Monat ein weiteres Kaninchen zur Welt. Falls die Kaninchen unsterblich wären, wie viele Kaninchen gibt es nach n-Monaten wenn es im ersten Monat ein Kaninchen gibt.

Bezeichnet man die Anzahl der Kaninchen nach n Monaten mit F_n, so gilt:

$$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 1+1 = 2, F_4 = 2+1 = F_3 + F_2$$

und allgemein

$$F_n = F_{n-1} + F_{n-2}$$

Die Zahlen F_n definiert durch

$$F_0 := 0, F_1 := 1, \forall n > 1 : F_n := F_{n-1} + F_{n-2}$$

heißen „Fibonacci-Zahlen“. Wir werden nun eine explizite Darstellung der Fibonacci Zahlen herleiten.

Sei $F = F(x) = \sum_{n=0}^{\infty} F_n x^n$. Dann gilt:

$$\begin{aligned}
F &= \sum_{n=0}^{\infty} F_n x^n \\
&= F_0 x^0 + F_1 x^1 + \sum_{n=2}^{\infty} F_n x^n \\
&= F_0 x^0 + F_1 x^1 + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) x^n \\
&= F_0 + F_1 x + x \sum_{n=1}^{\infty} F_n x^n + x^2 \sum_{n=0}^{\infty} F_n x^n \\
&= F_0 + F_1 x + x \sum_{n=0}^{\infty} F_n x^n - x F_0 + F x^2 \\
&= F_0 + F_1 x + xF - xF_0 + Fx^2 \\
&= x + xF + x^2 F \\
\Rightarrow F &= \frac{x}{1 - x - x^2}
\end{aligned}$$

Hat man nun $\alpha, \beta, a, b \in \mathbb{C}$ gefunden mit $\frac{x}{1-x-x^2} = \frac{a}{1-\alpha x} + \frac{b}{1-\beta x}$, dann gilt

$$\begin{aligned}
\sum_{n=0}^{\infty} F_n x^n &= \frac{a}{1-\alpha x} + \frac{b}{1-\beta x} \\
&= a \sum_{n=0}^{\infty} \alpha^n x^n + b \sum_{n=0}^{\infty} \beta^n x^n \\
&= \sum_{n=0}^{\infty} (a\alpha^n + b\beta^n) x^n \\
\text{und somit } F_n &= a\alpha^n + b\beta^n
\end{aligned}$$

Wegen $\frac{x}{1-x-x^2} = \frac{x}{\frac{5}{4}-(x+\frac{1}{2}x)^2} = \frac{x}{(\frac{\sqrt{5}}{2}-(x+\frac{1}{2}))\cdot(\frac{\sqrt{5}}{2}+(x+\frac{1}{2}))}$ folgt mittels Partialbruchzerlegung und AfI Übung 9 Aufgabe 8:

$$\frac{x}{1-x-x^2} = \frac{\frac{1}{\sqrt{5}}}{1-\frac{1+\sqrt{5}}{2}x} + \frac{-\frac{1}{\sqrt{5}}}{1-\frac{1-\sqrt{5}}{2}x}$$

also $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$, $a = \frac{1}{\sqrt{5}}$, $b = -\frac{1}{\sqrt{5}}$. Es folgt

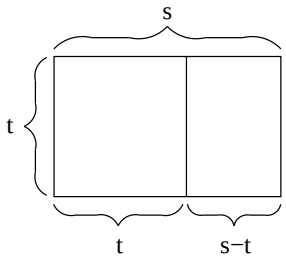
$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

1.47 Bemerkung *(goldener Schnitt)*

Die Zahl $\Phi := \frac{1+\sqrt{5}}{2} \approx 1.61803$ heißt „goldener Schnitt“ und taucht in verschiedenen Untersuchungen auf.

Beispiel

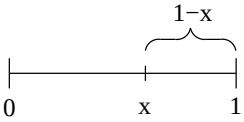
1) Einige Papierformate sind nach folgendem Schema aufgebaut:



Dabei gilt $\frac{s}{t} = \frac{t}{s-t} = \frac{1}{\frac{s}{t}-1}$, $0 < t < s$. Setze $x := \frac{s}{t}$, dann gilt:

$$\begin{aligned} & x = \frac{1}{x-1} \\ \Leftrightarrow \quad & x = \frac{1+\sqrt{5}}{2} \vee x = \frac{1-\sqrt{5}}{2} \end{aligned}$$

2)



$\frac{1}{x} = \frac{x}{1-x} \Leftrightarrow x^2 + x - 1 = 0 \Leftrightarrow x = \frac{-1+\sqrt{5}}{2} \vee x = \frac{-1-\sqrt{5}}{2} \Rightarrow x = \frac{\sqrt{5}-1}{2} = \frac{2}{1+\sqrt{5}} = \frac{1}{\Phi}$.

1.48 Satz *(homogene lineare Rekursionsgleichungen zweiter Ordnung)*

Sei $a_0 = b_0$, $a_1 = b_1$ und $\forall n > 1 : a_n = c_1 a_{n-1} + c_2 a_{n-2}$. Ferner seien α, β zwei Lösungen von $x^2 - c_1 x - c_2 = 0$ und

$$A := \begin{cases} \frac{b_0 - b_0\beta}{\alpha-\beta} & , \text{ falls } \alpha \neq \beta \\ \frac{b_1 - b_0\alpha}{\alpha} & , \text{ falls } \alpha = \beta \end{cases}$$

$$B := \begin{cases} \frac{b_1 - b_0\alpha}{\alpha-\beta} & , \text{ falls } \alpha \neq \beta \\ b_0 & , \text{ falls } \alpha = \beta \end{cases}$$

Dann gilt

$$a_n = \begin{cases} A\alpha^n - B\beta^n & , \text{ falls } \alpha \neq \beta \\ (An+B)\alpha^n & , \text{ falls } \alpha = \beta \end{cases}$$

Beweis: Induktion über n, analog zu Beweis von Beispiel 1.44 2).

♢

Schema *(zum Lösen linearer Rekursionsgleichungen)*

Eine lineare Rekursionsgleichung $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} \, \forall n \geq k$ mit $a_i = b_i$ für $i = 0, 1, \ldots, k-1$ kann nach folgendem Schema gelöst werden:

1) Aufstellen einer erzeugenden Funktion

$$A(x) = \sum_{n=0}^{\infty} a_n x^n$$

2) Anwendung der Rekursionsformel

$$\begin{aligned} A(x) &= a_0 + a_1 x_1 + a_2 x^2 + \ldots + a_{k-1} x^{k-1} + \sum_{n=k}^{\infty} a_n x^n \\ &= b_0 + b_1 x_1 + b_2 x^2 + \ldots + b_{k-1} x^{k-1} + \sum_{n=k}^{\infty} (c_1 a_{n-1} + c_2 a_{n-1} + \ldots + c_k a_{n-k}) x^n \\ &= b_0 + \ldots + b_{k-1} x^{k-1} + \underbrace{\sum_{n=k}^{\infty} c_1 a_{n-1} x^n}_{= c_1 x \underbrace{\sum_{n=k}^{\infty} a_{n-1} x^{n-1}}_{= A(x) - \sum_{i=0}^{k-2} a_i x^i}} + \underbrace{\sum_{n=k}^{\infty} c_2 a_{n-2} x^n}_{= c_2 x^2 \underbrace{\sum_{n=k}^{\infty} a_{n-2} x^{n-2}}_{= A(x) - \sum_{i=0}^{k-3} a_i x^i}} + \ldots + \underbrace{\sum_{n=k}^{\infty} c_k a_{n-k} x^n}_{= c_k x^k \underbrace{\sum_{n=k}^{\infty} a_{n-k} x^{n-k}}_{= A(x)}} \\ &= b_0 + \ldots + b_{k-1} x^{k-1} + c_1 x \left(A(x) - \sum_{i=0}^{k-2} a_i x^i \right) + c_2 x^2 \left(A(x) - \sum_{i=0}^{k-3} a_i x^i \right) + \ldots + c_k x^k A(x) \end{aligned}$$

3) Auflösen nach $A(x)$

$$A(x) = \frac{d_0 + d_1 x + d_2 x^2 + \ldots + d_{k-1} x^{k-1}}{1 - c_1 x - c_2 x^2 - \ldots - c_k x^k}$$

für geeignete $d_0, \ldots, d_{k-1}$.

4) Partialbruchzerlegung (in $\mathbb{C}$, vgl AfI Übung 9, Aufgabe 8)

Sei $1 - c_1 x - c_2 x^2 - \ldots - c_k x^k = (1 - \alpha_1 x)^{m_1} \cdot \ldots \cdot (1 - \alpha_t x)^{m_t}$ mit $\sum_{i=1}^{t} m_i = k$. Dann gilt

$$\begin{aligned} A(x) &= \frac{d_0 + d_1 x + d_2 x^2 + \ldots + d_{k-1} x^{k-1}}{1 - c_1 x - c_2 x^2 - \ldots - c_k x^k} \\ &= \frac{g_1(x)}{(1 - \alpha_1 x)^{m_1}} + \ldots + \frac{g_t(x)}{(1 - \alpha_t x)^{m_t}} \\ &= \sum_{i=1}^{t} \frac{g_i(x)}{(1 - \alpha_i x)^{m_i}} \end{aligned}$$

für geeignete Polynome g_i mit $\text{Grad}(g_i) \leq m_i - 1 \forall i = 1, \ldots, t$.

5) Nach Tabelle 4 in Bemerkung 1.42 gilt

$$A(x) = \sum_{i=0}^{t} \frac{g_i(x)}{(1-\alpha_i x)^{m_i}} = \sum_{i=0}^{t} g_i(x) \sum_{n=0}^{\infty} \binom{n+m_{i-1}}{m_{i-1}} (\alpha_i x)^n = \sum_{n=0}^{\infty} q_n x^n$$

q_n ist eine nicht rekursive Darstellung von a_n $\forall n \geq k$.

$\Diamond$

1.49 Beispiel

Gegeben sei folgende Rekursionsgleichung:

$$\begin{aligned} a_0 &= 1 \\ a_1 &= 5 \\ a_2 &= 19 \\ a_n &= 5a_{n-1} - 7a_{n-1} + 3a_{n-3} \forall n \geq 3 \end{aligned}$$

Lösung: Sei $A(x) = \sum_{n=0}^{\infty} a_n x^n$. Dann gilt

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \sum_{n=3}^{\infty} (5a_{n-1} - 7a_{n-2} + 3a_{n-3}) x^n \\ &= a_0 + a_1 x + a_2 x^2 + 5x \sum_{n=3}^{\infty} a_{n-1} x^{n-1} - 7x^2 \sum_{n=3}^{\infty} a_{n-2} x^{n-2} + 3x^3 \sum_{n=3}^{\infty} a_{n-3} x^{n-3} \\ &= 1 + 5x + 19x^2 + 5x(A(x) - (1+5x)) - 7x^2(A(x) - 1) + 3x^3 A(x) \\ \Rightarrow A(x) &= \frac{1+x^2}{1-5x+7x^2-3x^3} \\ &= \frac{1+x^2}{(1-x)^2 \cdot (1-3x)} \\ &= \frac{\frac{1}{2}x - \frac{3}{2}}{(1-x)^2} + \frac{\frac{5}{2}}{(1-3x)} \\ &= \frac{1}{2}(x-3) - \frac{1}{(1-x)^2} + \frac{5}{2}\frac{1}{(1-3x)} \\ &= \frac{1}{2}(x-3) - \sum_{n=0}^{\infty} \binom{n+1}{1} x^2 + \frac{5}{2} \sum_{n=0}^{\infty} (3x)^n \\ &= 1 + 5x + \sum_{n=0}^{\infty} \left(\frac{5}{2} 3^n - n + \frac{3}{2} \right) x^n \\ \Rightarrow a_n &= \frac{5}{2} 3^n - n + \frac{3}{2} \forall n \geq 2 \end{aligned}$$

Dieses Verfahren funktioniert auch für nicht homogene Rekursionsgleichungen.

1.50 Beispiel *(Catalan-Zahlen)*

Klammerketten sind Worte über dem Alphabet $\{(,)\}$, zum Beispiel (())(), () und)((.

Zulässige Klammerketten sind Klammerketten die die gleiche Anzahl von öffnenden und schließenden Klammern enthalten, und bei denen in jedem Präfix mindestens so viele öffnende wie schließende Klammern vorkommen.

$C_n := |\{c | c \text{ ist zulässige Klammerkette mit } 2n \text{ Klammern}\}|$

Berechne $C_n \forall n \in \mathbb{N}$ wenn $C_0 := 1$

$C_1 = 1 \qquad \{()\}$

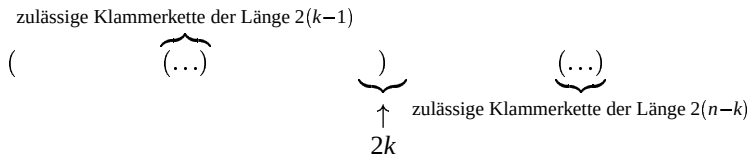
$C_2 = 2 \qquad \{()(), (())\}$

$C_3 = 5 \qquad \{()()(), ()(()), (())(), ((())), (()())\}$

1.51 Lemma *(Rekursionsformel für Catalan-Zahlen)*

$$C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k} \; \forall n \geq 1$$

Beweis Die zulässigen Klammerketten der Länge $2n$ können danach kategorisiert werden, wo die zur ersten öffnenden Klammer korospondierende schließende Klammer steht.



Sei für ein beliebiges $n \in \mathbb{N}$

$$A_k := \{\text{zulässige Klammerketten der Länge n, deren erste Klammer an Stelle } 2k \text{ geschlossen wird}\}.$$

Dann gilt $|A_k| = C_{k-1} C_{n-k}$. Es folgt

$$\begin{aligned} C_n &= \left| \biguplus_{k=1}^{n} A_k \right| \\ &= \sum_{k=1}^{n} |A_k| \\ &= \sum_{k=1}^{n} C_{k-1} C_{n-k} \end{aligned}$$

◊

1.52 Satz *(explizite Darstellung der Catalan-Zahlen)*

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

Beweis:

$$
\begin{aligned}
c(x) &:= \sum_{n=0}^{\infty} C_n x^n \\
\Rightarrow c(x) &= C_0 x^0 + \sum_{n=1}^{\infty} C_n x^n \\
\text{(Lemma 1.51)} &= C_0 + \sum_{n=1}^{\infty} \left(\sum_{k=1}^{n} C_{k-1} C_{n-k} \right) x^n \\
&= C_0 + x \sum_{n=1}^{\infty} \left(\sum_{k=1}^{n} C_{k-1} C_{n-k} \right) x^{n-1} \\
(t := n-1) &= C_0 + x \sum_{t=0}^{\infty} \left(\sum_{k=1}^{t+1} C_{k-1} C_{t+1-k} \right) x^t \\
(s := k-1) &= C_0 + x \sum_{t=0}^{\infty} \left(\sum_{s=0}^{t} C_s C_{t-s} \right) x^t \\
\text{(Definition 1.29)} &= C_0 + x(c(x) \cdot c(x))
\end{aligned}
$$

Somit gilt

$$
\begin{aligned}
x c^2(x) - x(x) &= -1 \\
x^2 c^2(x) - x c(x) &= -x \\
\Rightarrow (x c(x) - \frac{1}{2})^2 &= \frac{1}{4} - x \\
\Rightarrow x c(x) - \frac{1}{2} &= \pm (1-4x)^{\frac{1}{2}}
\end{aligned}
$$

$$
\begin{aligned}
\underbrace{\sum_{n=0}^{\infty} C_n x^{n-1}}_{=0+C_0 x + C_1 x^2 + \ldots} &= x \underbrace{c(x)}_{=\sum_{n=0}^{\infty} C_n x^n} \\
&= \frac{1}{2}(1 \pm (1-4x)^{\frac{1}{2}}) \\
\text{(nach Tabelle 4)} &= \frac{1}{2}(1 \pm \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4x)^n) \\
&= \frac{1}{2}(1 \pm (1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n))
\end{aligned}
$$

Der Koeffizient von x^0 ist 0, also gilt $C_0 + C_1x^2 + \ldots = -\frac{1}{2}\sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n$

$$\begin{aligned}
C_n &= -\frac{1}{2}\binom{\frac{1}{2}}{n+1}(-4)^{n+1} \\
&= -\frac{1}{2}\frac{(\frac{1}{2}-1)\cdot(\frac{1}{2}-2)\cdot\ldots\cdot(\frac{1}{2}-n)}{(n+1)!}(-1)^{n+1}4^{n+1} \\
&= (-1)^{n+2}\frac{(\frac{1}{2}-1)\cdot(\frac{1}{2}-2)\cdot\ldots\cdot(\frac{1}{2}-n)}{(n+1)!}4^n \\
&= \frac{(2-1)\cdot(4-1)\cdot\ldots\cdot(2n-1)}{(n+1)!\cdot n!}2^n n! \\
&= \frac{\overbrace{1\cdot 3\cdot\ldots\cdot(2n-1)\cdot 2\cdot 4\cdot\ldots\cdot 2n}^{=(2n)!}}{(n+1)!\cdot n!\cdot n!} \\
&= \frac{1}{(n+1)}\frac{(2n)!}{n!\cdot n!} \\
&= \frac{1}{(n+1)}\binom{2n}{n}
\end{aligned}$$

♢

Schema *(zum Lösen allgemeiner Rekursionsgleichungen)*

1) Aufstellen der erzeugenden Funktion $A(x) = \sum_{n=0}^{\infty} a_n x^n$

2) Umformen, so daß Anfangswerte und Rekursionsgleichung eingesetzt werden können

3) Weiter umformen bis auf der rechten Seite die noch vorhandenen unendlichen Summen (und mit ihnen alle Vorkommen von Folgegliedern a_n) durch $A(x)$ ersetzt werden können

4) Auflösen der erhaltenen Gleichung nach $A(x)$. Dadurch erhält man eine Gleichung der Form $A(x) = g(x)$, wobei g eine (hoffentlich einfache) Funktion ist.

5) Umschreiben der Funktion g als Potenzreihe (z.B. durch Partialbruchzerlegung und/oder Tabelle 4)

6) Ablesen der expliziten Darstellung für die a_n (durch Koeffizientenvergleich)

Graphentheorie

2.1 Grundbegriffe der Graphentheorie

2.1 Definition *(Graph)*

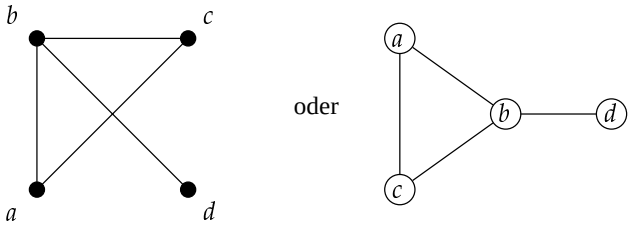
Ein Graph ist ein Paar $G = (V,E)$ aus einer endlichen Menge V und einer Menge $E \subseteq \binom{V}{2} (\binom{V}{2} = \{\{x,y\} \subseteq V | x! = y\}$, vgl. Definition 1.6). Die Elemente von V heißen Ecken, Punkte oder Knoten. Der Bezeichnung V kommt aus dem englischen Begriff „Vertices“. Die Elemente von E heißen Kanten (englisch: Edges).

Konvention: Für $\{x,y\} \in E$ schreiben wir auch $xy \in E$

Ein Graph wird im allgemeinen als Diagramm dargestellt. Jede Ecke wird durch einen Punkt repräsentiert und zwei Punkte x, y werden genau dann durch eine Linie verbunden, wenn $xy \in E$.

2.2 Beispiel *(einige Beispielgraphen)*

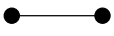
1) $G := (\{a,b,c,d\}, \{\{a,b\},\{b,c\},\{c,a\},\{b,d\}\})$

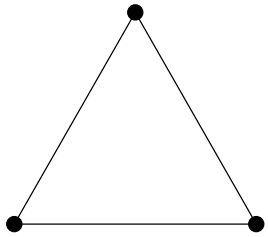


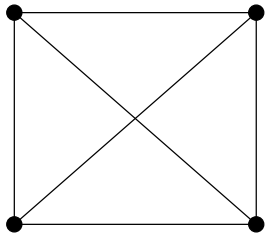
2) „Vollständige Graphen“ sind Graphen in denen jede Ecke mit jeder anderen durch eine Kante verbunden ist. Ein vollständiger Graph mit $n \in \mathbb{N}$ Ecken wird mit K_n bezeichnet. Ist V eine n-Menge, so gilt:

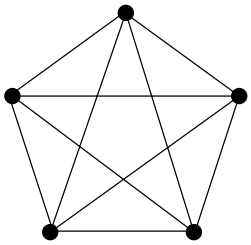
$$K_n := (V, \binom{V}{2})$$

$K_1 =$ 

$K_2 =$ 

$K_3 =$ 

$K_4 =$ 

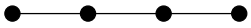
$K_5 =$ 

3) „Wege“ sind Graphen $G = (V,E)$ mit $V = \{v_0, \ldots, v_m\}$, $|V| = m+1$, $E = \{p_1, \ldots, p_m\}$, $|E| = m$ und $p_i = v_{i-1}v_i$ für alle $i \in \{1, \ldots, m\}$. Ein Weg der Länge m (d.h. bestehend aus m Kanten) wird mit P_m bezeichnet.

$P_0 =$ 

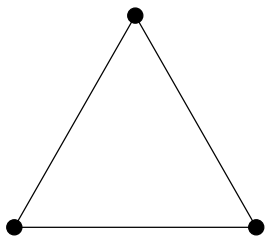
$P_1 =$

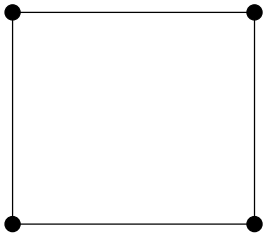
$P_2 =$ 

$P_3 =$ 

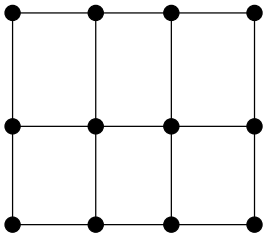
Für einen Weg P_m schreiben wir $P_m = p_1 \ldots p_m$.

4) „Kreise“ sind Graphen $G = (V,E)$ mit $V = \{v_1, \ldots, v_n\}$, $|V| = n$, $E = \{p_1, \ldots, p_n\}$, $|E| = n$ und $p_i = v_i v_{i+1}$ für alle $i \in \{1, \ldots, n-1\}$ sowie $p_n = v_n v_1$. Ein Kreis aus n Kanten wird mit C_n bezeichnet.

$C_3 =$ 

$C_4 =$ 

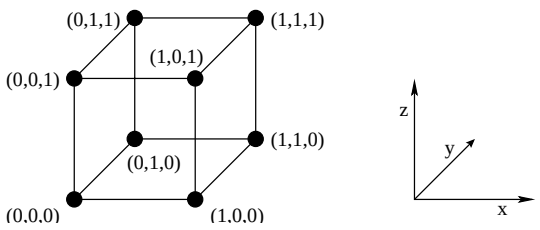
5) In „Gittergraphen“ aus $m \cdot n$ Ecken werden die Ecken in m Zeilen und n Spalten angeordnet und untereinander, bzw. nebeneinander liegende Ecken durch Kanten verbunden.

$M_{3,4} =$ 

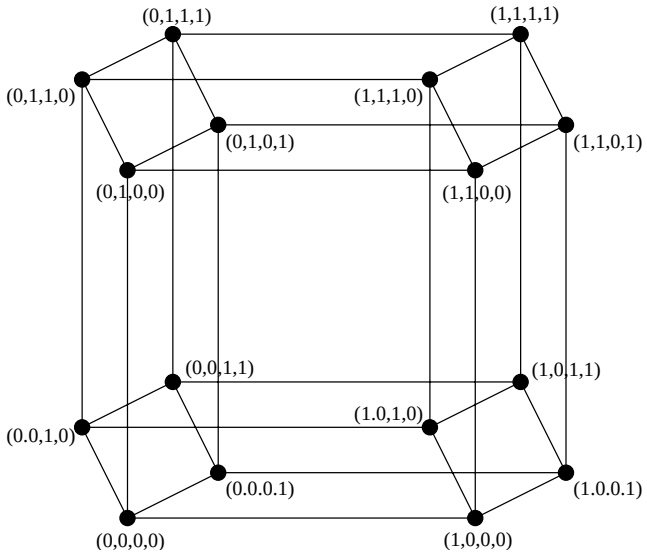
Gittergraphen treten unter anderem bei der Realisierung von programmierbaren logische Feldern auf (PLA, programmable logical array).

6) Ein „d-dimensionaler Hyperwürfel“ Q_d ist ein Graph $G = (V,E)$ mit

$$\begin{aligned} V &= \{0,1\}^d \\ E &= \{\{x,y\} \subseteq V \mid x = (x_1,\ldots,x_d) \text{ unterscheidet sich an genau einer Stelle von } y = (y_1,\ldots,y_d)\} \end{aligned}$$

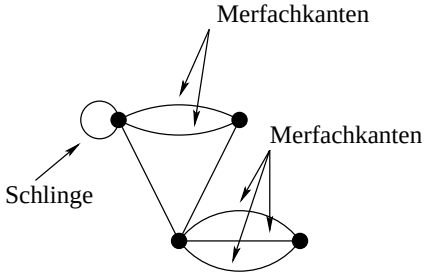
$Q_3 =$ 

Q_4 =



2.3 Bemerkung *(Graph, Multigraph, schlichter Graph)*

1) Allgemeinere Graphen können auch Mehrfachkanten und Schlingen enthalten. Um solche Graphen zu betrachten müßte die Definition 2.1 angepaßt werden, zum Beispiel durch $E = \{X \subseteq V \mid |X| = 1 \vee |X| = 2\}$ um Schlingen zu erlauben.



Ein Graph mit Schlingen und Mehrfachkanten

Ein Graph ohne Schlingen heißt „Multigraph“. Ein Multigraph ohne Mehrfachkanten heißt „schlichter Graph“. In der Vorlesung werden nur schlichte Graphen betrachtet.

2) Im Falle $G = (\emptyset, \emptyset)$ nennt man G „leerer Graph“ und im Falle $G = (E, \emptyset)$ „Nullgraph“.

3) Sei $G = (V, E)$ ein Graph mit Kante $e \in V$.

- x und y heißen „Endecken von e“
- e „inzidiert“ mit den Ecken x und y
- x und y sind durch e verbunden
- x und y heißen „benachbart“ oder „adjazent“

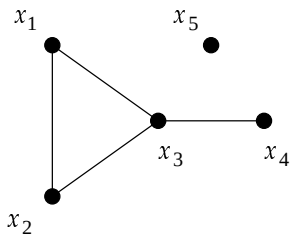
2.4 Definition *(Nachbarschaft, Eckengrad, regulärer Graph)*

Sei $G = (V,E)$ ein Graph mit Ecke $x \in V$.

- $N_G(x) := \{y \in V | xy \in E\}$ heißt „Nachbarschaft von x in G“
- $d_G(x) := |N_G(x)|$ heißt „Eckengrad von x in G“
  - $d_G(x) = 1 \Leftrightarrow$:$x$ ist „Endecke in G“
  - $d_G(x) = 0 \Leftrightarrow$:$x$ ist „isolierte Ecke in G“
- $\delta(G) := min_{x \in V} d(x)$ heißt „minimaler Eckengrad von G“
- $\Delta(G) := max_{x \in V} d(x)$ heißt „maximaler Eckengrad von G“
  - gilt für einen Graphen $\delta(G) = \Delta(G) = k$, so heißt G „k-regulärer Graph“ . So ist z.B jeder vollständige Graph K_n $(n-1)$-regulär.

2.5 Beispiel

1) Betrachte folgenden Graphen G:



Es gilt:

$$N(x_3) = \{x_1, x_2 x_4\}$$
$$N(x_1) = \{x_2, x_3\}$$
$$d(x_1) = 2\ d(x_2) = 2\ d(x_3) = 3$$
$$d(x_4) = 1\ (x_4 \text{ ist Endecke})$$
$$d(x_5) = 0\ (x_5 \text{ ist isolierte Ecke})$$
$$\delta(G) = 0\ \Delta(G) = 3$$

2) Jeder Kreis C_n ist 2-regulär.

2.6 Satz *(Handschlaglemma, Euler 1736)*

Sei $G = (V,E)$ ein Graph. Dann gilt:

$$\sum_{x \in V} d(x) = 2|E|$$

Beweis (doppeltes Abzählen): In $\sum_{x \in V} d(x)$ wird jede Kante $yz \in V$ genau zwei mal gezählt (ein mal in $d(y)$, zum zweiten mal in $d(z)$). Auf der rechten Seite wird jede Kante ebenfalls zwei mal gezählt.

$\Diamond$

2.7 Folgerung

In jedem Graphen ist die Anzahl der Ecken mit ungeraden Grad gerade.

Beweis: Sei $G = (V,E)$ und $V_1 = \{x \in V | d(x) \text{ ungerade}\}$, $V_2 = \{x \in V | d(x) \text{ gerade}\}$ ($\Rightarrow V = V_1 \uplus V_2$). Nach Satz 2.6 gilt:

$$\underbrace{2|E|}_{\text{gerade}} = \underbrace{\sum_{x \in V} d(x)}_{\text{gerade}} = \underbrace{\sum_{x \in V_2} d(x)}_{\text{gerade}} + \sum_{x \in V_1} d(x)$$

Die Summanden in $\sum_{x \in V_1} d(x)$ sind per Definition von V_1 ungerade. $\sum_{x \in V_1} d(x)$ selbst ist jedoch gerade. $\sum_{x \in V_1} d(x)$ muß demnach eine gerade Anzahl an Summanden enthalten, also ist $|V_1|$gerade.

♢

2.8 Lemma

Sei $G = (V,E)$ ein Graph mit $|V| \geq 2$. Dann gibt es zwei Ecken $x, y \in V$ mit $d(x) = d(y)$

Beweis: siehe Beispiel 1.13 2)

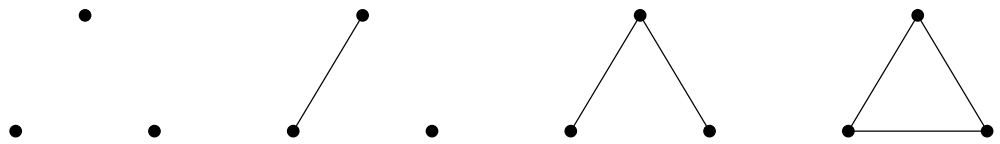
♢

2.9 Definition *(Isomorphie zwischen Graphen)*

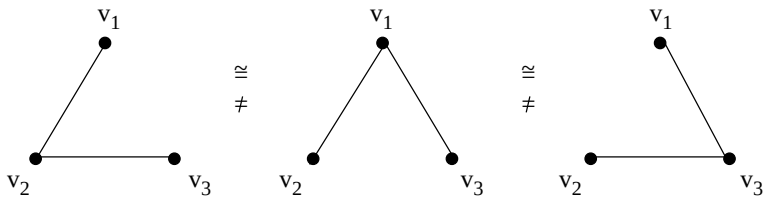
Seien $G = (V,E)$ und $G' = (V',E')$ Graphen. G und G' heißen „isomorph“ (in Zeichen $G \cong G'$) genau dann wenn eine bijektive Abbildung $\phi : V \to V$ existiert mit $xy \in E \Leftrightarrow \phi(x)\phi(y) \in E'$.

2.10 Beispiel

1) Nicht isomorphe Graphen mit 3 Ecken:



2) Werden die Namen von Ecken (und Kanten) eines Graphen berücksichtigt, so Sprich man von einem „markierten“ oder „benannten“ Graphen.



2.2 Darstellung von Graphen

2.11 Definition *(Adjazenzmatrix, Inzidenzmatrix)*

Ist $G = (V,E)$ ein Graph mit $V = \{v_1,\ldots,v_n\}$ und $E = \{e_1,\ldots,e_m\}$, so heißt die $n \times n$-Matrix

$$\begin{aligned} A &= (a_{ij}) \in \{0,1\}^{n\times n} \text{ mit} \\ a_{ij} = 1 &\Leftrightarrow v_i v_j \in E \end{aligned}$$

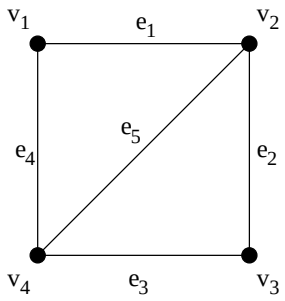
„Adjazenzmatrix von G“. Die $n \times m$-Matrix

$$\begin{aligned} I &= (b_{ij}) \in \{0,1\}^{n\times m} \text{ mit} \\ b_{ij} = 1 &\Leftrightarrow e_j \text{ inzidiert mit } v_i \end{aligned}$$

heißt „Inzidenzmatrix von G“.

2.12 Beispiel

Betrachte folgenden Graphen:



$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{array} = A \qquad \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array} = I$$

Für jede Adjazenzmatrix A eines Graphen $G = (V,E)$ gilt:

- $a_{ii} = 0$ (wir betrachten nur Graphen ohne Schlingen)
- $a_{ij} = a_{ji}$ ($v_i v_j \in E \Rightarrow v_j v_i \in E$).

Für jede Inzidenzmatrix I eines Graphen $G = (V,E)$ gilt

- Die Summe einer Spalte ist immer zwei (jede Kante inzidiert mit genau zwei Ecken)
- Die Summe einer Zeile ist gleich dem Eckengrad der jeweiligen Ecke.

$$I \cdot I^t = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 3 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 3 \end{pmatrix} = A + diag(\underbrace{(d(v_i))_{1\le i\le n}}_{\text{Gradfolge von } G})$$

2.13 Satz *(Zusammenhang zwischen Adjazenz- und Inzidenzmatrix)*

Ist $G=(V,E)$ ein Graph mit Adjazenzmatrix $A=(a_{ij})$, Inzidenzmatrix $I=(b_{ij})$ und Eckenmenge $V=\{v_1,\ldots,v_n\}$, dann gilt

$$I\cdot I^t = A + diag(d(v_1),\ldots,d(v_n))$$

Beweis:

Fall 1 $i\neq j$

$$(I\cdot I^t)_{ij} = \sum_{k=1}^{m} b_{ik}b_{jk} = \begin{cases} 1 & v_iv_j\in E \\ 0 & \text{sonst} \end{cases} = a_{ij}$$

$$\text{da } b_{ik}=b_{jk}=1 \Leftrightarrow e_k = v_iv_j$$

Fall 2 $i=j$

$$(I\cdot I^t)_{ii} = \sum_{k=1}^{m} \underbrace{b_{ik}b_{ik}}_{=\begin{cases} 1\Leftrightarrow b_{ik}=1 \\ 0\Leftrightarrow b_{ik}=0 \end{cases}} = \underbrace{\sum_{k=1}^{m} b_{ik}}_{\text{Summe } i\text{-te Zeile von I}} = d(v_i)$$

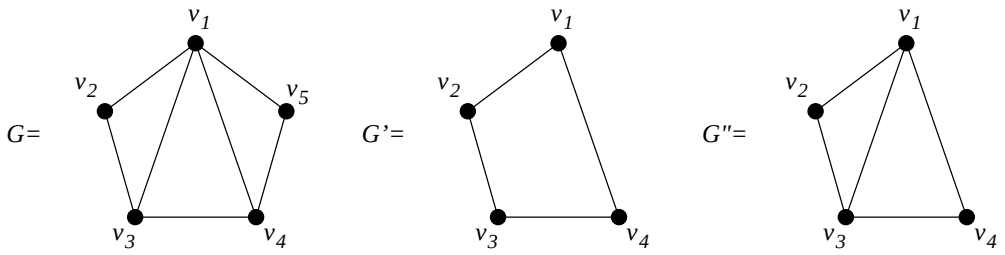
♢

2.14 Definition *(Teilgraph, induzierter Teilgraph)*

Sei $G=(V,E)$ ein Graph und $V'\subseteq V$.

- Der Graph $G'=(V',E')$ heißt „Teilgraph von G“ wenn $E'\subseteq E\cap\binom{V'}{2}$. Man schreibt dann auch $G'\subseteq G$.
- $G[V']:=(V',E\cap\binom{V'}{2})$ heißt „der von V' induzierte Teilgraph“.

Beispiel



$$G'\subseteq G,\ G''=G[\{v_1,v_2,v_3,v_4\}]$$

2.15 Definition *(Zusammenhang, Komponenten)*

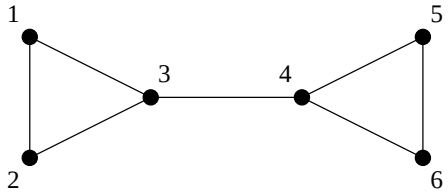
1) Sei $G=(V,E)$ ein Graph. G heißt „zusammenhängend“ genau dann wenn zwischen je zwei Ecken ein Weg existiert.

2) In einem (eventuell nicht zusammenhängenden) Graphen heißt jeder bezüglich der Anzahl von Ecken und Kanten maximaler zusammenhängender Teilgraph „Komponente von G“ oder „Zusammenhangskomponente von G“. Sind $G_1,\dots,G_k$ die Komponenten von G, so schriebt man auch $G=\bigcup_{i=1}^{k} G_i$. Die Anzahl der Komponenten von G wird mit $\kappa(G)$ bezeichnet.

3) Sei $G=(V,E)$ ein zusammenhängender Graph. Eine Ecke $x\in V$ heißt „Schnittecke von G“ falls $G[V\setminus\{x\}]$ nicht zusammenhängend ist.

Eine Kante $k\in E$ heißt „Brücke“ falls $(V,E\setminus\{k\})$ nicht zusammenhängend ist.

Beispiel



Die Ecken 3 und 4 sind Schnittecken, die Kante $\{3,4\}$ ist eine Brücke

2.16 Satz *(Abschätzung der Komponenten nach unten)*

Sei $G=(V,E)$ ein Graph. Dann gilt:

$$\kappa(G)\geq |V|-|E|$$

Beweis (per Induktion über $|E|$) Für $|E|=0$ gilt

$$\kappa(G)=|V|=|V|-0=|V|-|E|\geq |V|-|E|$$

Sei nun $|E|>0$, $e=ab\in E$ und $\kappa(F')\geq |V'|-|E'|$ für alle Graphen $F'=(V',E')$ mit $|E'|<|E|$. Der Graph $G':=(V,E\setminus\{e\}):=(V,E')$ hat weniger Kanten als G, somit gilt nach Induktionsvoraussetzung

$$\kappa(G')\geq |V|-|E\setminus\{e\}|=|V|-(|E|-1)=|V|-|E'|$$

Die Anzahl der Komponenten verringert sich durch Hinzufügen der Kante e zu G' genau dann, wenn a und b in unterschiedlichen Komponenten von G' liegen. Dann verringert sich die Anzahl der Komponenten jedoch genau um 1, da e zwei Komponenten von G' zu einer Komponente von G zusammenfaßt.

$$\begin{aligned} G=G'+e\Rightarrow \kappa(G) &= \begin{cases} \kappa(G') & \text{falls } e \text{ keine Brücke ist}\\ \kappa(G)-1 & \text{falls } e \text{ Brücke ist}\end{cases}\\ &\geq \underbrace{|V|-|E'|}_{=\kappa(G')}-1\\ &= |V|-(|E'|+1)\\ &= |V|-|E| \end{aligned}$$

♢

2.17 Folgerung

Sei $G=(V,E)$ ein zusammenhängender Graph mit $|V|=n$ und $|E|=m$. Dann gilt

$$n-1\leq m\leq \binom{n}{2}$$

Beweis selber machen.

2.18 Satz *(Anzahl der Kanten in zusammenhängenden Graphen)*

Sei $G = (V,E)$ ein Graph mit $n = |V|$ und $m = |E|$. Gilt $m > \underbrace{\frac{1}{2}(n-1)(n-2)}_{=\text{Anzahl der Kanten von } K_{n-1}}$ so ist G zusammenhängend.

Beweis Angenommen G ist nicht zusammenhängend. Seien $G_1 \dots G_k$ die Komponenten von G mit $|V(G_i)| = n_i \forall i = 1 \dots k$. Dann gilt $k \geq 2$ und $\sum_{i=1}^{k} n_i = n$.

$$\begin{aligned}
m &= \sum_{i=1}^{k} |E(G_i)| \\
&\leq \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2} \text{ (nach Folgerung 2.17)} \\
&= \frac{1}{2}\left(\sum_{i=1}^{k} n_i^2 - \sum_{i=1}^{k} n_i\right) \\
&= \frac{1}{2}\left(\underbrace{\sum_{i=1}^{k} n_i^2 + 2\sum_{1\leq i<j\leq k} n_i n_j}_{=\left(\sum_{i=1}^{k} n_i\right)^2 = n^2} - 2\sum_{1\leq i<j\leq k} n_i n_j - \underbrace{\sum_{i=1}^{k} n_i}_{=n}\right) \\
&= \frac{1}{2}\left(n^2 - 2\sum_{1\leq i<j\leq k} n_i n_j - n\right) \\
&\leq \frac{1}{2}\left(n^2 - 2n_1(n_2+n_2+\ldots+n_k) - n\right) \\
&\leq \frac{1}{2}\left(n^2 - 2(n-1) - n\right) \\
&= \frac{1}{2}\left(n^2 - 3n + 2\right) \\
&= \frac{1}{2}(n-1)(n-2)
\end{aligned}$$

Zusammenfassend:

$$\begin{aligned}
G \text{ nicht zusammenhängend} &\Rightarrow m(G) \leq \frac{1}{2}(n-1)(n-2) \text{ also auch} \\
G \text{ zusammenhängend} &\Rightarrow m(G) > \frac{1}{2}(n-1)(n-2)
\end{aligned}$$

♢

2.19 Satz *(Abschätzung der Kanten nach oben)*

Ist $G = (V,E)$ ein Graph mit $|V| = n$ und $|E| = m$, so gilt

$$m \leq \binom{n-\kappa(G)+1}{2}$$

Beweis (siehe auch Lutz Volkmann: „Diskrete Strukturen“ Satz 3.6)

Die Idee des Beweises ist, herauszufinden wann m maximal ist. Ohne Beschränkung der Allgemeinheit können alle Komponenten von G als vollständig angenommen werden, da dies keine Auswirkung auf $\binom{n-\kappa(G)+1}{2}$ hat, die Anzahl der Kanten jedoch nicht weniger wird. Die Anzahl der Kanten von G kann nun weiter erhöht werden indem man zwei Komponenten $G[V_1]$ und $G[V_2]$ mit $|V_1| \leq |V_2|$ und $v \in V_1$ ersetzt durch zwei Komponenten $G_1 = (V_1 \setminus \{v\}, \binom{V_1 \setminus \{v\}}{2})$ und $G_2 = (V_2 \cup \{v\}, \binom{V_2 \cup \{v\}}{2})$. Dadurch werden zwar $|V_1| - 1$ Kanten aus G entfernt, allerdings werden auch $|V_2|$ Kanten hinzugefügt, insgesamt erhöht sich dadurch die Anzahl der Kanten. Die Anzahl der Komponenten sowie die der Ecken bleibt jedoch konstant. Die Anzahl der Kanten wächst durch wiederholtes Ersetzen solange bis G aus einem vollständigen Graphen mit $n - \kappa(G) + 1$ Ecken und $\kappa(G) - 1$ isolierten Ecken besteht, und ist dann maximal. In diesem Fall gilt jedoch $m = \binom{n-\kappa(G)+1}{2}$

♢

Bemerkung Aus Satz 2.19 folgt unmittelbar Satz 2.18.

2.3 Bäume

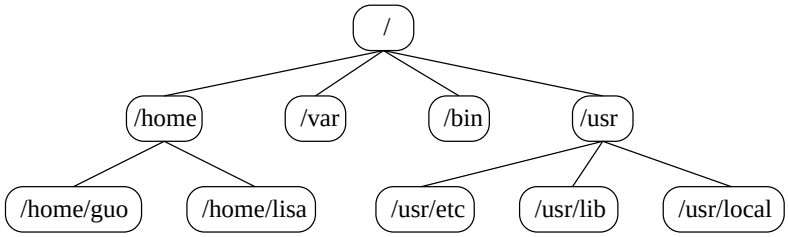


Abbildung 6: Dateisystem eines UNIX Systems

2.20 Definition *(Baum, Wald)*

Ein „Baum“ ist ein zusammenhängender Graph ohne Kreise. Ein „Wald“ ist ein Graph dessen Komponenten Bäume sind.

2.21 Lemma *(Endecken in Bäumen)*

Eine Endecke eines Graphen $G = (V,E)$ ist eine Ecke $x \in V$ mit $d(x) = 1$. Jeder Baum $T = (V,E)$ mit $|V| \geq 2$ enthält mindestens 2 Endecken.

Beweis Sei $P = v_1 \dots v_k$ ein längster Weg in T. Angenommen es existiert ein $v \in V$ so daß $v_k v \in E$. Dann ist $v \notin \{v_1, \dots, v_{k-2}\}$ da aus $v = v_i$ für ein $i \in \{1, \dots, k-2\}$ folgt $v_i \dots v_k v_i$ ist ein Kreis. Außerdem gilt auch nicht $v \in V \setminus \{v_1, \dots, v_k\}$ da in diesem Fall $v_1 \dots v_k v$ ein Weg wäre der länger als P ist. Es folgt also $v = v_{k-1}$ und somit $d(v_k) = 1$, womit v_k eine Endecke ist. Analog zeigt man daß v_1 ebenfalls Endecke ist.

♢

2.22 Satz *(Charakterisierung von Bäumen)*

Sei $G = (V,E)$ ein Graph mit $|V| = n$ und $|E| = m$. Folgende Aussagen sind äquivalent:

(1) G ist ein Baum

(2) G ist zusammenhängend und kreisfrei

(3) G ist zusammenhängend und $m = n-1$

(4) G ist kreisfrei und $m = n-1$

(5) zwischen zwei Ecken von G existiert genau ein Weg

(6) G ist maximal kreisfrei (d.h durch Hinzufügen einer weiteren Kante entsteht ein Kreis)

(7) G ist minimal zusammenhängend (d.h durch Herausnehmen einer Kante zerfällt G in zwei Komponenten)

Beweis Üblicherweise werden Beweise dieser Art geführt daß man zeigt $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (7) \Rightarrow (1)$. Hier bietet es sich jedoch an, zu zeigen daß $(2) \Leftrightarrow (1) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (7) \Rightarrow (2)$

$(2) \Leftrightarrow (1)$ folgt unmittelbar aus der Definition von Bäumen. Wir zeigen deshalb nur exemplarisch $(1) \Rightarrow (3)$ (per Induktion über n).

Induktionsanfang: Für $n = 2$ gilt $m = 1 = 2-1 = n-1$.

Induktionsschluß: Sei $n \geq 2$ und für alle Bäume $T' = (V',E')$ mit $|V'| = n$ gelte $|E'| = |V'| - 1$. Sei $T = (V,E)$ ein Baum mit $|V| = n+1$ und x eine Endecke von G (eine Endecke existiert nach Lemma 2.21). $G - x := G[V \setminus \{x\}]$ ist ein Baum mit genau n Ecken und somit gilt nach Induktionsvoraussetzung $|E(G-x)| = n-1$. Durch Hinzufügen von x zu $G-x$ wird auch genau eine Kante zu $G-x$ hinzugefügt ($d(x) = 1$) und somit gilt $|E(G)| = |E(G-x)| + 1 = (n-1)+1 = (n+1)-1$

♢

2.23 Definition *(Wurzelbaum)*

Ein „Wurzelbaum“ $T = (V,E)$ ist ein Baum in dem eine Ecke $w \in V$ als Wurzel ausgezeichnet ist.

Sei $T = (V,E)$ ein Wurzelbaum mit Wurzel w und x eine Ecke von T.

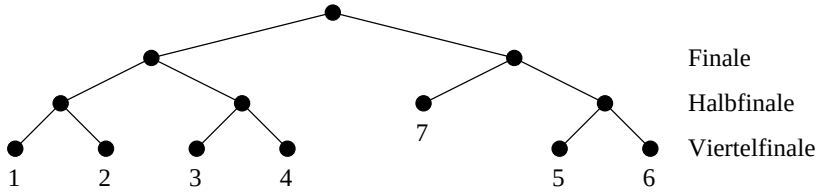
- Jede Ecke y auf dem Weg von w nach x heißt „Vorgänger von x“ (es existiert genau ein Weg von w nach x, da T ein Baum ist).
- Ist y Vorgänger von x und ist $x \neq y$, so heißt y „Nachfolger von x“.
- Ist y Nachfolger von x und gilt $yx \in E$, so heißt y „unmittelbarer Nachfolger von x“ und x heißt „unmittelbarer Vorgänger von y“.
- Ein „geordneter Baum“ ist ein Wurzelbaum in dem für die unmittelbaren Nachfolger jeder Ecke eine Ordnung festegelegt ist.

2.24 Definition *(Tiefe)*

Die Tiefe $depth(T)$ eines Wurzelbaumes T ist die maximale Länge eines Weges von der Wurzel zu einer Endecke.

Ein Wurzelbaum T mit der Tiefe t heißt „balanciert“ wenn jeder Weg von einer Endecke zu der Wurzel die Länge t oder $t-1$ hat.

Beispiel Ein Fußballturnier mit 7 Mannschaften



Ein balancierter Baum der Tiefe 3

2.25 Definition *(binärer Baum)*

Ein Wurzelbaum heißt „binärer Baum“ wenn jede Ecke höchstens zwei unmittelbare Nachfolger hat. Ein balancierter binärer Baum in dem jede Ecke entweder keine oder 2 Nachfolger hat, heißt „vollständiger binärer Baum“.

2.26 Satz *(Anzahl der Ecken in binären Bäumen)*

Sei $T=(V,E)$ ein binärer Baum mit Tiefe t und $|V|=n$. Dann gilt

$$t+1 \leq n \leq 2^{t+1}-1.$$

Beweis Sei $p_k :=$ Anzahl der Ecken die von der Wurzel die Entfernung k haben. Es gilt $\sum_{k=0}^{t} p_k = n$. Da für binäre Bäume weiterhin gilt $1 \leq p_k \leq 2p_{k-1} \forall 1 \leq k \leq t$ und $p_0 = 1$, folgt $\sum_{k=0}^{t} 1 \leq \sum_{k=0}^{t} p_k \leq \sum_{k=0}^{t} 2p_k$, und somit $t+1 \leq n \leq 2^{t+1}-1$.

♢

2.27 Folgerung *(Tiefe von binären Bäumen)*

Sei $T=(V,E)$ ein binärer Wurzelbaum mit Tiefe t und $|V|=n$. Dann gilt

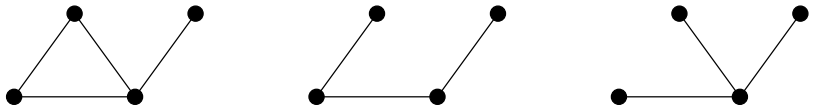
$$t \geq \left\lceil \lg_2 \frac{n+1}{2} \right\rceil$$

Beweis Übung

2.28 Definition *(Gerüst eines Graphen)*

Ein Teilgraph T eines zusammenhängenden Graphen G heißt „Gerüst von T“ (oder spannender Baum oder Baumfaktor) wenn T ein Baum ist und $V(T)=V(G)$.

Beispiel



Ein Graph und 2 seiner Gerüste

2.29 Satz *(Existenz von Gerüsten)*

Jeder zusammenhängende Graph enthält ein Gerüst.

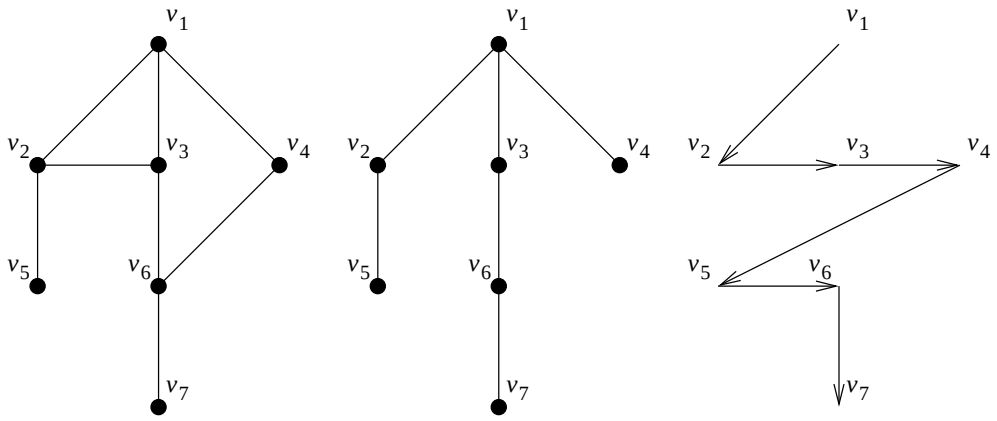
Beweis Sei $G = (V,E)$ ein zusammenhängender Graph.

Enthält G keinen Kreis, dann ist T ein Baum. Setzte $T = G$. T ist ein Baum mit $V(T) = V(G)$, also ist T ein Gerüst von G.

Enthält G eine Kreis dann entferne aus einem Kreis $C = v_0v_1 \dots v_kv_0$ eine beliebige Kante, z.B $G' = (V, E \setminus \{v_i\})$. G' ist dann immer noch zusammenhängend, da alle Wege die v_i als Kannte enthalten über $v_{i+1} \dots v_kv_0 \dots v_{i-1}$ umgelenkt werden können. Wiederholt man dieses Entfernen so lange bis kein Kreis mehr enthalten ist, so ist der resultierende Graph ein Baum der aus allen Ecken von G besteht, also ein Gerüst von G.

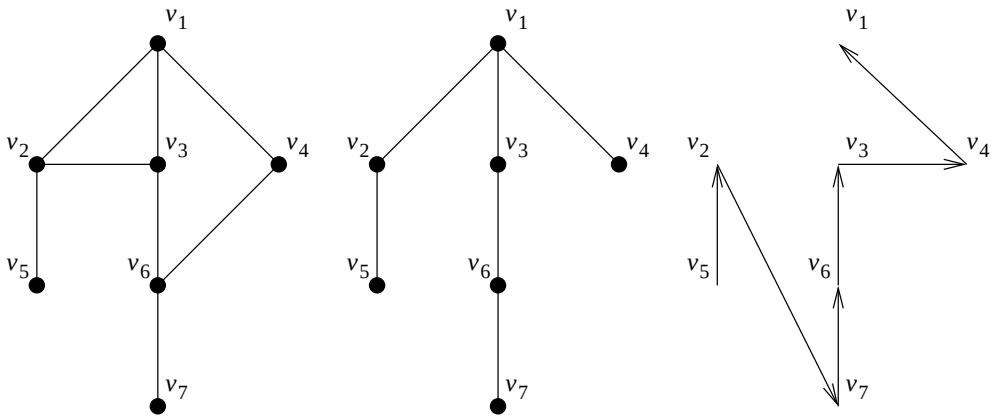
♢

Algorithmus 1 Breitensuche (BFS: Breadth-First-Search)



Graph Gerüst Breitensuche

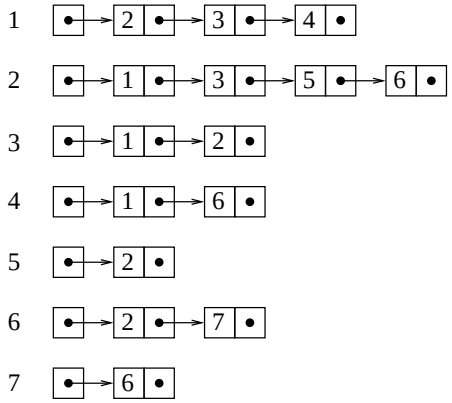
Algorithmus 2 Tiefensuche (DFS: Depth-First-Search)



Graph Gerüst Tiefensuche

Beide Algorithmen haben Laufzeit $O(|V|+|E|)$

Im Computer benutzt man auch gerne ein andere Darstellung von Graphen, die Darstellung als Adjazenzliste.



	Adjazenzmatrix	Adjazenzliste
Speicherverbrauch	$O(\|V\|^2)$	$O(\|V\|+\|E\|)$
Test ob $xy \in E$	$O(1)$	$O(min\{d(x),d(y)\})$
Bestimmen von $N(x)$	$O(\|V\|)$	$O(d(x))$

Tabelle 5: Komplexität von Graphenoperationen

2.30 Satz *(Cayley's Tree Formula)*

Sei G ein vollständiger markierter Graph mit $n \geq 2$ Ecken. Dann besitzt G n^{n-2} verschieden Gerüste.

Beweis folgt

2.4 Matching in Graphen

2.31 Definition *(Matching)*

Sei $G = (V, E)$ ein Graph. Ein „Matching von G“ ist eine Kantenmenge $M \subseteq E$ mit $\forall k_1 \neq k_2 \in M : V(k_1) \cap V(k_2) = \emptyset$, d.h. M ist eine Kantenmenge in der keine zwei Kanten inzident sind.

- Ein Matching M von G heißt „maximales Matching“, wenn es in G kein Matching M' gibt mit $M \subset M'$.
- Ein Matching M von G heißt „Maximum-Matching“, wenn es in G kein Matching M' gibt mit $|M| < |M'|$.
- Ein Matching M von G heißt „perfektes Matching“ wenn $V(M) = V(G)$.

2.32 Beispiel

2.33 Bemerkung

1) Jedes perfekte Matching ist ein Maximum-Matching.

2) Für jedes Matching M gilt $|V(M)| = 2|M|$.

3) Für jedes perfektes Matching M von G gilt $2|M| = V(G)$.

4) G hat ein perfektes Matching $\Rightarrow V(G)$ ist gerade.

2.34 Bemerkung *(bipartite Graphen)*

Ein Graph $G = (V, E)$ heißt „bipartit“ wenn man V so in zwei disjunkte Teilmengen A und B zerlegen kann, daß $G[A]$ und $G[B]$ Nullgraphen sind.

- A und B heißen Partitionsmengen.
- Ein vollständiger bipartiter Graph K_{pq} ist ein bipartiter Graph $G = (A \uplus B, E)$ mit $|A| = p$, $|B| = q$ und $\forall x \in A : \forall y \in B : xy \in E$.

2.35 Beispiel

Grafiken fehlen.

2.36 Satz *(Bipartität und Kreise)*

Ein Graph G ist genau dann bipartit wenn G keine Kreise ungerader Länge hat.

Beweis Sei G $= (A \uplus B, E)$ ein bipartiter Graph mit einem Kreis ungerader Länge $C = (v_0 \dots v_{2k} v_0)$. Weiterhin gelte (o.B.d.A.) $v_0 \in A$.

v_i und $v_{i+1(\mathrm{mod}\ 2k+1)}$ können nicht in der selben Partitionsmenge sein, da v_i und $v_{i+1(\mathrm{mod}\ 2k+1)}$ adjazent sind, der durch diese Partitionsmenge induzierte Teilgraph wäre also kein Nullgraph. Somit gilt:

$$\begin{aligned} v_0 \in A &\Rightarrow v_1 \in B \\ &\Rightarrow v_2 \in A \\ &\Rightarrow \dots \\ &\vdots \\ &\Rightarrow v_{2k-1} \in B \\ &\Rightarrow v_{2k} \in A \\ &\Rightarrow v_0 \in B \end{aligned}$$

was offensichtlich ein Widerspruch ist. Ein bipartiter Graph kann also keinen Kreis ungerader Länge enthalten.

Sei nun $G = (V, E)$ ein Graph ohne Kreise ungerader Länge mit $a \in V$. Definiere

$$\begin{aligned} A &:= \{v \in V | \text{der kürzeste Weg von } v \text{ nach } a \text{ hat gerade Länge}\} \\ B &:= \{v \in V | \text{der kürzeste Weg von } v \text{ nach } a \text{ hat ungerade Länge}\} \end{aligned}$$

Offensichtlich gilt $A \cap B = \emptyset$ und $A \cup B = V$, somit genügt es zu zeigen:

$$\begin{aligned} v_1 \in A \wedge v_2 \in A &\Rightarrow v_1 v_2 \notin E \\ v_1 \in B \wedge v_2 \in B &\Rightarrow v_1 v_2 \notin E \end{aligned}$$

Angenommen es gibt eine Kante $uv \in E$ mit $u \in A$ und $v \in A$. Sei dann P_{au} ein kürzester Weg von a nach u und W_{av} ein kürzester Weg von a nach v. Ferner sei y die letzte gemeinsame Ecke von P_{au} und W_{av} ($P_{au} = P_{ay} + P_{yu}$, $W_{av} = P_{ay} + W_{yv}$ wie in Abbildung 7) Bezeichnet man die Länge eines Weges W mit $L(W)$,

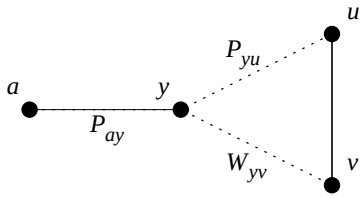


Abbildung 7: Kürzeste Wege

so gilt:

$$L(P_{au}) + L(W_{av}) = 2L(P_{ay}) + L(P_{yu}) + L(W_{yv})$$

$L(P_{au}) + L(W_{av})$ ist nach Konstruktion gerade, ebenso ist $2L(P_{ay})$ gerade. Demnach muß auch $L(P_{yu}) + L(W_{yv})$ gerade sein. $P_{yu} + W_{yv} + uv$ bildet dann aber einen Kreis ungerader Länge. Da solche aber in G nach Voraussetzung nicht existieren ist $uv \notin E$. G ist also ein bipartiter Graph mit Partitionsmengen A und B.

♢

2.37 Satz *(Matchings in bipartiten Graphen)*

Sei $G = (A \uplus B, E)$ ein bipartiter Graph. G besitzt ein Matching M mit $|M| = |A|$ genau dann wenn $\forall S \subseteq A$: $|N(S)| \leq |S|$.

Beweis fehlt

2.38 Folgerung

Sei $G = (A \uplus B, E)$ ein r-regulärer bipartiter Graph mit $r \geq 1$, so enthält G ein perfektes Matching.

Beweis Es gilt $|A| = |B|$, sowie $\forall S \subseteq A : |N(S)| \geq |S|$. Aus Satz 2.37 folgt dann die Behauptung.

2.39 Folgerung

Ein r-regulärer bipartiter Graph läßt sich in r kantendisjunkte perfekte Matchings zerlegen.

Beweis sukzessives Anwenden von Folgerung 2.38

2.40 Definition (Multipartite Graphen)

Ein Graph $G = (V, E)$ heißt „k-partit“ (allgemein auch „multipartit“), wenn man V so in k disjunkte Teilmengen $V_1, \ldots, V_k$ zerlegen kann, daß $G[V_i]$ für $i \in \{1, \ldots, k\}$ Nullgraphen sind.

2.5 Hamilton Graphen

2.41 Definition *(Hamiltonkreis, Hamilton-Weg)*

Sei $G = (V, E)$ ein Graph.

- Ein „Hamiltonkreis“ ist ein Kreis C mit $V(C) = V(G)$. Ein Graph der einen Hamiltonkreis enthält heißt „hamiltonscher Graph“.
- Ein „Hamilton-Weg“ ist ein Weg W mit $V(W) = V(G)$. Ein Graph der einen Hamilton-Weg enthält heißt „semi-hamiltonscher Graph“

2.42 Beispiel

1) K_n ist hamiltonsch für $n > 2$.

2) D_{20} ist hamiltonsch.

3) Der Peterson-Graph ist nicht hamiltonsch, aber semi-hamiltonsch.

2.43 Satz *(notwendige Bedingung für hamiltonsche Graphen)*

Sei $G = (V, E)$ ein hamiltonscher Graph. Dann gilt für jede nicht leere Menge $S \subseteq V$

$$\kappa(G - S) \leq |S|$$

Beweis Ist G selbst ein Kreis, so erhält man einen Weg durch Herausnehmen einer Ecke. Sukzessives Herausnehmen weiterer Ecken erhöht die Anzahl der Komponenten jeweils höchstens um 1 (pro Ecke). Entfernt man also p Ecken, so erhält man höchstens p Komponenten.

Ist G kein Kreis, so ist die Anzahl der erhaltenen Komponenten sogar noch geringer, da es mehr Kanten gibt, die den Graphen zusammenhalten.

$\Diamond$

2.44 Satz *(Lemma von Ore, 1960)*

Sei $G = (V,E)$ ein Graph mit $|V| = n$. Ferner seien u und v zwei nicht adjazente Ecken von G mit $d(u) + d(v) \geq n$. Dann gilt

$$G \text{ ist hamiltonsch } \Leftrightarrow \; G + uv \text{ ist hamiltonsch}$$

Beweis[1] „$\Rightarrow$“: trivial (durch Hinzufügen von Kanten zu einem hamiltonschen Graphen geht der Hamiltonkreis nicht verloren)

„$\Leftarrow$“: Existiert ein Hamiltonkreis von G der nicht die Kante uv enthält, so ist offensichtlich auch G hamiltonsch.

Da jedoch $G + uv$ hamiltonsch ist existiert in G ein Hamilton-Weg $(u, x_1, \ldots, x_{n-2}, v)$. Sei nun $S := \{i \in \{1,\ldots,n-3\} | ux_{i+1} \in E\}$ und $T := \{i \in \{1,\ldots,n-3\} | x_i v \in E\}$. Wegen $1 \leq |S| \leq n-3$ und $1 \leq |T| \leq n-3$ und $d(u) + d(v) \geq n$ gilt $S \cap T \neq \emptyset$. Also existiert ein $p \in \{1,\ldots,n-3\}$ mit $ux_{p+1} \in E$ und $x_p v \in E$. Dann ist aber auch $(u, x_1, \ldots x_p, v, x_{n-2}, \ldots x_{p+1}, u)$ ein Hamiltonkreis.

$\Diamond$

2.45 Folgerung *(hinreichende Bedingung für hamiltonsche Graphen)*

Sei $G = (V,E)$ ein Graph mit $|V| = n \geq 3$ in dem für alle Ecken u und v gilt $d(u) + d(v) \geq n$, so ist G hamiltonsch.

Beweis Nach Satz 2.44 kann man zu dem Graphen G Kanten hinzufügen ohne dabei zu verändern ob der resultierende Graph hamiltonsch ist oder nicht. Man fügt Kanten solange hinzu bis der vollständige Graph K_n entstanden ist, welcher offensichtlich hamiltonsch ist.

2.46 Folgerung *(Dirac, 1052)*

Sei $G = (V,E)$ ein Graph mit $|V| = n$ und $d(v) \geq \frac{n}{2} \forall v \in V$. Dann ist G hamiltonsch.

Beweis Wegen $d(v) \geq \frac{n}{2} \forall v \in V$ gilt auch für $\forall u \neq v$: $d(u) + d(v) \geq \frac{n}{2} + \frac{n}{2} = n$ womit die Voraussetzungen von Folgerung 2.45 erfüllt sind.

2.47 Bemerkung

1) Eine bekannte Anwendung ist das Travelling Salesman Problem (TSP). Darin geht es darum in einem gewichteten Graphen (ein Graph in dem die Kanten mit Kosten belegt sind) einen günstigsten Hamiltonkreis zu finden. TSP benötigt exponentielle Laufzeit, es existieren jedoch effiziente Heuristiken die zwar nicht unbedingt den besten, dennoch aber einen recht preiswerten Hamiltonkreis finden.

[1] Der Beweis der Vorlesung ging etwas anders, den hab ich aber nicht verstanden

2) Das Entscheidungsproblem ob ein Graph einen Hamiltonkreis enthält ist NP-vollständig, das heißt es kann in polynomieller Zeit entschieden werden ob ein Lösungskandidat (in diesem Fall eine Folge von Ecken) ein korrekte Lösung ist (also ein Hamiltonkreis), eine korrekte Lösung kann allerdings nach dem gegenwärtigen Stand der Forschung in polynomieller Zeit nicht gefunden werden.

2.6 Eulersche Graphen

Eulersche Graphen (und Graphen überhaupt) wurden durch das von Leonard Euler aufgeworfene Königsberger Brückenproblem inspiriert.

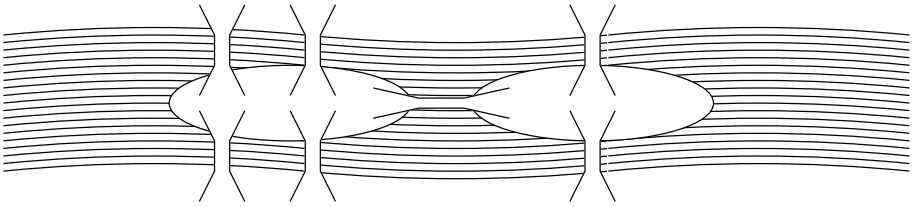


Abbildung 8: Königsberger Brückenproblem

Es geht darum, einen Weg durch Königsberg zu finden bei dem jede Brücke genau ein mal überquert wird, so daß man am Ende dort herauskommt wo man seine Reise begonnen hat.

2.48 Definition *(Kantenfolge, Kantenzug, Eulertour)*

Sei $G = (V, E)$ ein zusammenhängender Graph.

- Eine Folge $x_0 \dots x_k$ mit $\forall 0 \leq i \leq k : x_i \in V$ und $\forall 0 \leq i < k : x_i x_{i+1} \in E$ heißt „Kantenfolge der Länge k“.
- Eine Kantenfolge aus paarweise verschiedenen Kanten heißt „Kantenzug“
- Eine Kantenzug Z mit $E(Z) = E(G)$ heißt „eulerscher Kantenzug“
- Ein geschlossener eulerscher Kantenzug (d.h. ein eulerscher Kantenzug $x_0 x_1 \dots x_k$ mit $x_0 = x_k$) heißt „Eulertour“

2.49 Definition *(semi-eulerscher Graph, eulerscher Graph)*

Sei $G = (V, E)$ ein zusammenhängender Graph mit $|V| \geq 2$.

- G heißt „semi-eulerscher Graph“ falls G einen eulerschen Kantenzug enthält.
- G heißt „eulerscher Graph“ falls G eine Eulertour enthält.

2.50 Beispiel

2.51 Satz *(hinreichende und notwendige Bedingung für Eulertouren)*

Sei $G = (V,E)$ ein zusammenhängender Graph mit $|V| \geq 2$. Dann gilt

$$G \text{ ist eulersch } \Leftrightarrow \text{ Jede Ecke von } G \text{ hat geraden Grad}$$

Beweis:

„⇒“: Existiert in G eine Ecke $x \in V$ mit ungeradem Grad, so muß diese Ecke auf der Eulertour ungerade oft besucht werden. Sei z.B. $d(x) = 3$. Eine Eulertour enthält eine Kantenfolge $y_0xy_1 \ldots y_2x$. Die Kanten y_0x, y_1x und y_2x wurden allerdings schon benutzt und es gibt keine Möglichkeit mehr die Startecke zu erreichen.

„⇐“: Sei $z = x_0 \ldots x_k$ ein längster Kantenzug in G.

Jedes Auftauchen von x_0 in z (außer am Anfang und am Ende der Kantenfolge) liefert zum Grad von x_0 den Beitrag 2: Ist $x_ix_0x_{i+1}$ Teil von z, so sind $x_ix_0 \in E$ sowie $x_0x_{i+1} \in E$ inzident mit x_0. Bezieht man das Auftauchen von x_0 am Anfang der Kantenfolge mit ein, so erhält man eine ungerade Anzahl von Kanten, die von x_0 ausgehen. Da der Grad von x_0 jedoch gerade ist, müßte eine Ecke x_{-1} existieren so daß $z' = x_{-1}x_0 \ldots x_k$ eine Kantenfolge in G ist. Diese wäre länger als z, also gilt $x_0 = x_k$.

Da obiges für jeden Startpunkt einer längsten Kantenfolge gilt, müssen mit z alle Kanten durchlaufen worden sein. Die Kantenfolge z ist also eine Eulertour.

♢

Euler zeigte 1736 nur die Implikation „⇒“, der vollständige Beweis wurde von Hierhölzer 1873 niedergeschrieben.

2.52 Folgerung

Ein zusammenhängender Graph $G = (V,E)$ mit $|V| \geq 2$ ist semi-eulersch genau dann wenn G keine oder genau zwei Ecken mit ungeradem Grad besitzt.

2.53 Bemerkung

- Es existiert ein effizienter Algorithmus um in einem eulerschen Graphen $G = (V,E)$ eine Eulertour zu finden (Fleury Algorithmus, Komplexität: $O(E)$).
- Eine Anwendung ist das Chinesische Briefträgerproblem. Dabei wird versucht , in einem bewerteten (d.h. die Kanten sind mit Kosten belegt) zusammenhängenden Graphen eine geschlossene Kantenfolge mit minimalen Kosten zu finden. Als erster befaßte sich der chinesische Mathematiker Kuan 1962 mit diesem Problem.

2.7 Planare Graphen

Planare Graphen können so auf eine 2-dimensionale Ebene projiziert werden, daß sich keine Kanten überschneiden.

2.54 Definition *(planarer Graph, Landkarte, Gebiet)*

Sei $G = (V,E)$ ein Graph.

- G heißt *einbettbar in* $\mathbb{R}^2$ genau dann wenn es eine injektive Abbildung $\varphi : V \to \mathbb{R}^2$ und eine Abbildung $\varphi' : E \to J := \{\text{bild}(e) | e : [0,1] \to \mathbb{R}^2 \text{ stetig, injektiv}\}$ gibt, so daß
  - $\forall uv \in E : \varphi'(uv) = \text{bild}(e) \Rightarrow \varphi(u) = e(0) \wedge \varphi(v) = e(1)$, d.h. jede Kante wird durch φ' auf einen Jordanbogen im $\mathbb{R}^2$ abgebildet. J ist die Menge aller Jordanbögen.
  - $\forall uv \in E : \forall wx \neq uv : \varphi'(uv) \cap \varphi'(wx) = \varphi(\{u,v\} \cap \{w,x\})$, d.h. die Jordanbögen von je zwei verschiedenen Kanten sind bis auf eventuell gemeinsamer Ecken disjunkt.
- G heißt *planar* wenn G in $\mathbb{R}^2$ einbettbar ist.
- Eine Einbettung eines planaren Graphen G in $\mathbb{R}^2$ heißt *ebener Graph* oder *Landkarte* (in Zeichen (G, φ, φ')).
- Die Zusammenhangskomponenten von $\mathbb{R}^2 | \bigcup_{e \in E} \varphi'(e)$ heißen Gebiete oder *Länder* von (G, φ, φ').
- Die Anzahl der Länder eines ebenen Graphen G wird mit $l(G)$ bezeichnet.

2.55 Satz *(Eulersche Polyederformel, 1752)*

Sei $G = (V,E)$ ein zusammenhängender, ebener Graph. Dann gilt:

$$l(G) = |E| - |V| + 2$$

Beweis: Induktion über $m = |E|$. Nach Folgerung 2.17 gilt $m \geq |V| - 1$. Es genügt also, $|V| - 1$ als Induktionsanfang zu wählen.

Sei $m = |V| - 1$:

G ist ein Baum und es gilt

$$\begin{aligned} l(G) &= 1 \\ &= -1 + 2 \\ &= |V| - |V| - 1 + 2 \\ &= (|V| - 1) - |V| + 2 \\ &= |E| - |V| + 2 \end{aligned}$$

Sei $m \geq V$ und $l(G) = |E| - |V| + 2$ für alle zusammenhängenden ebenen Graphen mit $m(G) \leq m$:

Aus G zshg. und $|E| \geq |V|$ folgt mit Satz 2.22: G enthält mindestens einen Kreis C. Sei $e \in E(C)$ eine Kante dieses Kreises. Dann gilt $|E(G-e)| = m$ und nach Induktionsvoraussetzung $l(G-e) = m - |V| + 2$. Durch Entfernen der Kante e aus G verschmelzen zwei Länder von G zu einem Land von $G-e$. Es folgt

$$\begin{aligned} l(G) &= l(G-e) + 1 \\ &= m - |V| + 2 + 1 \\ &= m + 1 - |V| + 2 \\ &= |E| - |V| + 2 \end{aligned}$$

$\Diamond$

2.56 Satz *(notwendige Bedingung für planare Graphen)*

In jedem planaren Graphen $G = (V,E)$ mit $|V| \geq 3$ gilt

$$|E| \leq 3 \cdot |V| - 6$$

Beweis: Sei G o.B.d.A in $\mathbb{R}^2$ eingebettet. Die Menge der Länder von G sei mit L bezeichnet.

Jedes Land wird von mindestens 3 Kanten begrenzt. Jede Kante teilt höchstens zwei Länder. Es folgt

$$\begin{aligned} 3|L| &\leq 2|E| \\ \Rightarrow \frac{2}{3}|E| &\geq l(G) = |E| - |V| + 2 \\ \Rightarrow |E| &\leq 3|V| - 6 \end{aligned}$$

♢

2.57 Beispiel

1) Der vollständige Graph K_5 ist nicht planar, denn es gilt $|E(K_5)| = \begin{pmatrix} 5 \\ 2 \end{pmatrix} = 10 > 9 = 3 \cdot 5 - 6 = 3 \cdot |V(K_5)| - 6$.

2) Der vollständig bipariter Graph $K_{3,3}$ ist nicht planar, denn $K_{3,3}$ besitzt keine Kreise der Länge 3 und für solche Graphen gilt $|E| \leq 2 \cdot |V| - 4$.

2.58 Definition *(Unterteilungsgraph)*

Sei $G = (V,E)$ ein Graph und $e = ab \in E$ eine Kante von G. Man sagt „e wird *unterteilt*“, wenn man zu G eine neu Ecke x hinzufügt und die Kante e durch zwei neue Kanten ax und bx ersetzt.

Ein Graph H heißt *Unterteilungsgraph* von G, wenn man H aus G durch Unterteilen von Kanten gewinnen kann.

2.59 Satz *(Satz von Kuratowski, 1930)*

Ein Graph G ist genau dann planar wenn er keinen Unterteilungsgraphen von K_5 und keinen Unterteilungsgraphen von $K_{3,3}$ als Teilgraphen enthält.

2.60 Definition *(Färbung)*

Sei G eine Landkarte mit Ländern L.

- Zwei verschiedene Länder F_1 und F_2 heißen *benachbart*, wenn es eine Kante gibt die sowohl zum Rand von F_1 als auch zum Rand von F_2 gehört.
- Eine Abbildung $h : L \to \{1,2,\ldots,p\}$ so daß

  $$F_1 \text{benachbart zu } F_2 \Rightarrow h(F_1) \neq h(F_2)$$

  heißt *Färbung* von G oder *p-Färbung* von G. Existiert eine solche Abbildung, so läßt sich die Landkarte G mit p Farben färben.

2.61 Beispiel

2.62 Satz *(Vierfarbenvermutung, Guthrie 1852)*

Jede Landkarte läßt sich mit vier Farben färben.

Beweis: N.Robertson et.al. 1997

2.63 Bemerkung

1) Bei Anwendung planarer Graphen in der Informatik steht der algorithmische Aspekt im Vordergrund. Es gibt Verfahren, die in $O(|V|+|E|)$ testen ob ein Graph $G=(V,E)$ planar ist, und diesen auch in $\mathbb{R}^2$ einbetten.

2) Neben Färbung von Ländern gibt es auch die Probleme der Eckenfärbung und der Kantenfärbung.

3) Jeder Graph läßt sich in $\mathbb{R}^3$ einbetten.

2.8 Digraphen

2.64 Definition *(Digraph)*

Ein Digraph $D=(V,A)$ besteht aus einer nicht-leeren Menge von Ecken V (aus dem englischen: „vertex“) und einer Menge von Bogen $A \subseteq V \times V$ (aus dem englischen: „arc“).

Auch Digraphen können im allgemeinen Mehrfachkanten und Schlingen enthalten. In dieser Vorlesung werden jedoch nur schlichte Digraphen betrachtet, d.h. Digraphen ohne Mehrfachkanten und Schlingen.

2.65 Definition *(Weg, Kreis, Kantenfolge, Kantenzug, Nachbarschaft, Eckengrad)*

Sei $D=(V,A)$ ein Digraph.

- $D'=(V',A')$ heißt *Teildigraph* von D, wenn $V' \subseteq V$ und $A' \subseteq A \cap (V' \times V')$. In Zeichen: $D' \subseteq D$.
- Ein Teildigraph $D'=(V',A')$ heißt *von V' induzierter Teildigraph, wenn* $A'=A \cap (V' \times V')$. In Zeichen: $D'=D[V']$
- Eine Folge $F=x_0 \ldots x_p$ von Ecken mit $\forall 0 \leq i < p : x_i x_{i+1} \in A$ heißt *orientierte Kantenfolge*.
- Eine orientierte Kantenfolge aus paarweise verschiedenen Kanten heißt *orientierter Kantenzug*.
- Ein orientierter Kantenzug aus paarweise verschiedenen Ecken heißt *orientierter Weg*.
- Eine orientierte Kantenfolge $F=x_0 \ldots x_p$ mit $x_0=x_p$ heißt *geschloßene orientierte Kantenfolge.*
- Ein orientierter Kantenzug $F=x_0 \ldots x_p$ mit $x_0=x_p$ heißt *geschloßener orientierter Kantenzug.*
- Ein orientierter Weg $F=x_0 \ldots x_p$ mit $x_0=x_p$ heißt *orientierter Kreis.*

- Ein geschloßener orientierterKantenzug $F = x_0 \dots x_p$ mit $A(F) = A(D)$ heißt *Eulertour in D.*
- Ein orientierter Weg $F = x_0 \dots x_p$ mit $V(F) = V(D)$ heißt *hamiltonscher Weg in D.*
- Ein orientierter Kreis $F = x_0 \dots x_p$ mit $V(F) = V(D)$ heißt *hamiltonscher Kreis in D.*
- Für $x \in V$ definiert man
  - $N^+(x) := \{y \in V | xy \in A\}$ heißt *positive Nachbarschaft* von x. Die Elemente von $N^+(x)$ heißen *positive Nachbarn* von x.
  - $N^-(x) := \{y \in V | yx \in A\}$ heißt *negative Nachbarschaft* von x. Die Elemente von $N^-(x)$ heißen *negative Nachbarn* von x.
  - $d^+(x) := |N^+(x)|$ heißt *Aussengrad* von x. $\delta^+(D) := \min\{d^+(x) | x \in V\}$ heißt minimaler Aussengrad von D. $\Delta^+(D) := \max\{d^+(x) | x \in V\}$ heißt maximaler Aussengrad von D.
  - $d^-(x) := |N^-(x)|$ heißt *Innengrad* von x.$\delta^-(D) := \min\{d^-(x) | x \in V\}$ heißt minimaler Innengrad von D. $\Delta^-(D) := \max\{d^-(x) | x \in V\}$ heißt maximaler Innengrad von D.
- Der Graph $G = (V,E)$ mit $V = V(D)$ und $E = \{\{x,y\} \in \wp_2(V) | xy \in A\}$ heißt *untergeordneter Graph* von D. In Zeichen $G = G(D)$.

2.66 Definition *(starker Zusammenhang)*

Sei $G = (V,A)$ ein Digraph.

Eine *starke Zusammenhangskomponente* von D ist ein maximaler Teildigraph H von D, so daß in H für zwei beliebige verschiedene Ecken $(x,y) \in V(H) \times V(H)$ ein orientierter Weg von x nach y existiert. Ein Digraph der aus einer einzigen stark zusammenhängenden Komponente besteht heißt *stark zusammenhängend*.

2.67 Definition *(Turnier)*

Ein Digraph in dem zwischen je zwei Ecken genau ein Bogen existiert heißt *Turnier*. Ein Turnier aus genau n Ecken heißt n-Turnier (in Zeichen T_n).

2.68 Satz *(hamiltonsche Wege in Turnieren)*

Jedes Turnier besitzt einen orientierten hamiltonschen Weg.

Beweis: Sei T_n ein Turnier mit längstem orientierten Weg $W = x_1 \dots x_k$.

Ist $k < n$, so existiert $x \in V(T_n) \setminus V(W)$. Da T_n ein Trunier ist, existiert ein $i \in \{1, \dots k-1\}$ so daß $(x_i,x) \in A(T_n)$ und $(x,x_i) \in A(T_n)$. Dann ist aber $x_1 \dots x_i x x_{i+1} \dots x_k$ ein längerer Weg als W. Es gilt also $V(T_n) \setminus V(W) = \emptyset$ und somit $V(T_n) = V(W)$. W ist also ein hamiltonscher Weg.

$\Diamond$

2.69 Satz *(Kreise in stark zusammenhängenden Turnieren)*

Ist T_n ein stark zusammenhängendes Turnier, so liegt jede Ecke von T_n auf einem p-Kreis $\forall p \in \{3 \dots n\}$.

Beweis: Vollständige Induktion über p

$\Diamond$

2.70 Bemerkung

Jede Relation auf einer endlichen Menge induziert einen Digraphen.

Algebraische Strukturen

In diesem Kapitel werden, wie in der Linearen Algebra, Körper, Ringe, Gruppen, etc. vorgestellt, allerdings in einer umgekehrter Reihenfolge.

3.1 Universelle Algebren

Allgemein ist einer Algebra ein Menge auf der Operationen definiert sind.

3.1 Definition *(Operation, Stelligkeit)*

Sei M eine Menge.

- Eine Abbildung $f : M^n \to M$ heißt „n-stellige Operation auf M“ oder auch „n-stelliger Operator auf M“.
- $s(f) := n$ heißt „Stelligkeit von f“.
- Eine zweistellige Operation $f : M \times M \to M$ heißt auch „Verknüpfung auf M“ (englisch: „binary operation“).

3.2 Definition (Algebra, Signatur)

Sei M eine Menge und für $i \in I$ sei f_i eine n_i-stellige Operation auf M.

- $(M, (f_i)_{i\in I})$ heißt „universelle Algebra vom Typ $(n_i)_{i\in I}$“.
- $(n_i)_{i\in I}$ heißt „Signatur der Algebra $(M, (f_i)_{i\in I})$“.

3.3 Beispiel

1) Die boolsche Algebra $(\{\mathrm{T},\mathrm{F}\}, (\wedge, \vee, \neg))$ ist einer universelle Algebra mit Signatur $(2, 2, 1)$.

x_1	x_2	$x_1 \wedge x_2$	$x_1 \vee x_2$	$\neg x_1$	$\neg x_2$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	T
T	T	T	T	F	F

Tabelle 6: Wahrheitstabelle

2) Mit den üblichen arithmetischen Operationen wie „+“ und „·“ können folgende Algebren definiert werden:

- $(\mathbb{N},+)$, $(\mathbb{N},+,\cdot)$
- $(\mathbb{Z},\cdot)$
- $(\{x\in\mathbb{N}|\exists n\in\mathbb{N}: n^2\in\mathbb{N}\},\cdot)=(\{n^2|n\in\mathbb{N}\},\cdot)$
  $x=a^2, y=b^2\Rightarrow x\cdot y=a^2\cdot b^2=ab\cdot ab=(ab)^2$, also $\cdot: M\times M\to M$

$(\{n^2|n\in\mathbb{N}\},+)$ ist keine Algebra, da z.B $2^2+3^2=13\neq x^2\forall x\in\mathbb{N}$

3) Sei Σ eine endliche Menge (ein Alphabet) und $\Sigma^*:=\{(a_1\ldots a_n)|n\in\mathbb{N}_0, a_i\in\Sigma\forall i=1\ldots n\}$ eine formale Sprache. Ferner sei $\circ:\Sigma^*\times\Sigma^*\to\Sigma^*$mit $(a_1\ldots a_n)\circ(b_1\ldots b_m)=(a_1\ldots a_nb_1\ldots b_m)$.

Dann ist $(\Sigma^*,\circ)$ eine universelle Algebra.

4) Sei U eine Menge und $F(U)=\{f:U\to U\}$ die Menge aller Funktionen von U nach U. Ferner sei $\circ$ die übliche Komposition von Funktionen: $(f\circ g)(x)=f(g(x))\forall x\in U$.

Dann ist $(F(U),\circ)$ eine universelle Algebra auf $F(U)$.

3.4 Definition *(neutrale Elemente)*

Sei $(M,\circ)$ eine 2-stellige Algebra.

- Ein Element $e\in M$ heißt „linksneutrales Element für den Operator $\circ$“ falls gilt $\forall a\in M: e\circ a=a$.
- Ein Element $e\in M$ heißt „rechtsneutrales Element für den Operator $\circ$“ falls gilt $\forall a\in M: a\circ e=a$.
- Ein Element $e\in M$ heißt „neutrales Element für den Operator $\circ$“ falls e sowohl links- als auch rechtsneutral ist.
  $$e\circ a=a\circ e=a\,\forall a\in M$$

3.5 Beispiel

Sei $(\{b,c\},\circ)$ eine universelle Algebra mit $\circ$ definiert durch Tabelle 7.

$\circ$	b	c
b	b	b
c	c	c

Tabelle 7: Wertetabelle von $\circ$

Es gilt:

$$b\circ b=b\wedge c\circ b=c\Rightarrow b \text{ ist rechtsneutral}$$

$$b\circ c=b\wedge c\circ c=c\Rightarrow b \text{ ist rechtsneutral}$$

Wegen $c\circ b=c$ ist c nicht linksneutral, wegen $b\circ c=b$ ist b nicht linksneutral.

3.6 Lemma *(Existenz und Eindeutigkeit neutraler Elemente)*

Sei $(M,\circ)$ eine universelle Algebra vom Typ (2). Ist $c\in M$ linksneutral und $d\in M$ rechtsneutral, so gilt $c=d$. Insbesonders gilt: $(M,\circ)$ enthält höchstens ein neutrales Element.

Beweis:

$$\left.\begin{array}{rcccl} c \text{ linksneutral} & \Rightarrow & c \circ d & = & d \\ d \text{ rechtsneutral} & \Rightarrow & c \circ d & = & c \end{array}\right\} \Rightarrow c = d$$

Seien nun e_1 und e_2 neutrale Elemente von $(M, \circ)$ bezüglich $\circ$.

Dann ist insbesonders auch e_1 linksneutral. Ebenso ist e_2 rechtsneutral, und somit $e_1 = e_2$.

$\Diamond$

3.7 Beispiel *(Fortsetzung von Beispiel 3.3)*

- $(\mathbb{N}, +)$ hat neutrales Element 0.
- $(\mathbb{Z}, \cdot)$ hat neutrales Element 1.
- $(\mathbb{N}, +, \cdot)$ hat neutrale Elemente 0 (bezüglich $+$) und 1 (bezüglich $\cdot$)

3.8 Definition *(inverse Elemente)*

Sei $(M, \circ)$ eine universelle Algebra vom Typ (2) mit neutralem Element e.

- $x \in M$ heißt „Linksinverses“ von $a \in M$ falls $x \circ a = e$.
- $x \in M$ heißt „Rechtsinverses“ von $a \in M$ falls $a \circ x = e$.
- $x \in M$ heißt „Inverses“ von $a \in M$ falls x Links- und Rechtsinverses von a ist.

Aufgabe: Eindeutigkeit von Inversen.

3.9 Definition *(Halbgruppe)*

Eine universelle Algebra $A = (M, \circ)$ vom Typ (2) heißt „Halbgruppe“ falls $\circ$ assoziativ ist, d.h $\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$.

Beispiel: $(\Sigma^*, \circ)$ aus Beispiel 3.3 ist eine Halbgruppe.

3.10 Definition *(Monoid)*

Ein „Monoid“ $A = (M, \circ)$ ist eine universelle Algebra vom Typ (2) mit

M1: $(M, \circ)$ ist eine Halbgruppe (d.h. $\circ$ ist assoziativ)

M2: $(M, \circ)$ hat ein neutrales Element

3.11 Definition *(Gruppe)*

Eine „Gruppe“ ist eine universelle Algebra vom Typ (2) mit

G1: $(M, \circ)$ ist eine Halbgruppe (d.h. $\circ$ ist assoziativ)

G2: $(M, \circ)$ hat ein neutrales Element

G3: Zu jedem $a \in M$ existiert ein inverses Element in M

3.12 Definition *(abelsche Algebren)*

Eine Halbgruppe (Monoid, Gruppe, ...) $(M,\circ)$ heißt „abelsch“ falls $\circ$ kommutativ ist, d.h. wenn $\forall a,b \in M$: $a \circ b = b \circ a$.

3.13 Definition *(Ring)*

Ein „Ring“ ist eine universelle Algebra $A = (M,\oplus,\odot)$ vom Typ $(2,2)$ mit

R1: $(M,\oplus)$ ist eine abelsche Gruppe (das neutrale Element dieser Gruppe wird mit „0“ bezeichnet).

R2: $(M,\odot)$ ist ein Monoid (das neutrale Element dieses Monoids wird mit „1“ bezeichnet).

R3: Es gelten folgende Distributivgesetze:

$$\begin{aligned}(b\oplus c)\odot a &= (b\odot a)\oplus(c\odot a)\\ a\odot(b\oplus c) &= (a\odot b)\oplus(a\odot c)\end{aligned}$$

3.14 Definition *(Körper)*

Ein „Körper“ ist eine universelle Algebra $A = (M,\oplus,\odot)$ vom Typ $(2,2)$ mit

K1: $(M,\oplus)$ ist eine abelsche Gruppe (das neutrale Element dieser Gruppe wird mit „0“ bezeichnet)

K2: $(M\setminus\{0\},\odot)$ ist eine abelsche Gruppe (das neutrale Element dieser Gruppe wird mit „1“ bezeichnet)

K3: Es gilt das Distributivgesetz $a\odot(b\oplus c) = (a\odot b) + (a\odot c)$

Beispiel: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ sind Körper.

3.15 Definition *(boolsche Algebra)*

Eine „boolsche Algebra“ ist eine universelle Algebra $A = (M,\oplus,\odot,\neg)$ vom Typ $(2,2,1)$ mit

B1: $(M,\oplus)$ ist ein abelsches Monoid (mit neutralem Element 0)

B2: $(M,\odot)$ ist eine abelsches Monoid (mit neutralem Element 1)

B3: $\forall a \in M : a\oplus(\neg a) = 1$
$\forall a \in M : a\odot(\neg a) = 0$

B4: $a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c)$
$a\oplus(b\odot c) = (a\oplus b)\odot(a\oplus c)$

3.16 Beispiel

1) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer Ring, d.h. $(\mathbb{Z},+,\cdot)$ ist ein Ring und es gilt $\forall a,b \in \mathbb{Z} : a\cdot b = b\cdot a$

2) Sei K ein Körper.

- $K[x] := \{\sum_{k=0}^{n} a_k x^k | n \in \mathbb{N}_0, \forall i = 1 \ldots n : a_i \in K\}$ ist ein kommutativer Ring (Polynomring)
- $K[[x]] := \{\sum_{k=0}^{\infty} a_k x^k | \forall i = 1 \ldots n : a_i \in K\}$ ist ein kommutativer Ring (siehe auch Satz 1.32)
- $K^{n\times n} := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \middle| \forall 1 \leq i,j \leq n : a_{ij} \in K \right\}$ ist ein Ring. Für $n > 1$ ist dieser Ring nicht kommutativ.

3) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.

4) Der kleinste Ring besteht lediglich aus der Null. $(\{0\}, \oplus, \odot)$ ist ein Ring mit $\oplus = \odot$ und $1 = 0$.
Der kleinste Körper ist $(\{0,1\}, \oplus, \odot)$ definiert durch Tabelle 8. Diese Körper wird mit $\mathbb{F}_2$ bezeichnet.

x	y	$x \oplus y$	$x \odot y$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Tabelle 8: Multiplikations- und Additionstabelle für $(\{0,1\}, \oplus, \odot)$

Konvention: Sei $(K, \oplus, \odot)$ ein Körper.

- Das neutrale Element bezüglich $\oplus$ wird mit 0 bezeichnet.
- Das neutrale Element bezüglich $\odot$ wird mit 1 bezeichnet.
- Das inverse Element von $a \in K$ bezüglich $\oplus$ wird mit $-a$ bezeichnet.
- Das inverse Element von $a \in K$ bezüglich $\odot$ wird mit a^{-1} bezeichnet.

3.2 Unteralgebren, Homomorphismen, Kongruenzen

Es sei $A = (A, (f_i)_{i\in I})$ eine Algebra vom Typ $T = (n_i)_{i\in I}$ für eine Indexmenge I.

3.17 Definition *(Unteralgebra)*

$U \subseteq A$ heißt „Unteralgebra von A“ (geschrieben $U \leq A$), falls die Operationen $(f_i)_{i\in I}$ in U abgeschlossen sind, d.h. $\forall i \in I : f(U^{n_i}) \subseteq U$ (anders gesagt $\forall i \in I : \forall u_1 \ldots u_{n_i} \in U : f_i(u_1, \ldots, u_{n_i}) \in U$).

3.18 Definition (Untergruppe, Teilring)

- Sei $G = (G, \odot)$ eine Gruppe.
  Eine „Untergruppe von G“ ist eine Unteralgebra von G die eine Gruppe ist.
- Sei $R = (R, \oplus, \odot)$ ein Ring.
  Ein „Teilring von R“ ist eine Unteralgebra von R, die ein Ring ist.

3.19 Beispiel

1)

- $(\mathbb{Z},+,\cdot) \leq (\mathbb{Q},+,\cdot) \leq (\mathbb{R},+,\cdot) \leq (\mathbb{C},+,\cdot)$ sind Teilringe von $(\mathbb{C},+,\cdot)$
- $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$ sind Untergruppen von $(\mathbb{C},+)$

2) Sei $Z_n := \{0,\ldots,n-1\}$ und $+_n : \mathbb{N}\times\mathbb{N} \to Z_n$ eine Operation auf Z_n mit $a +_n b = a + b \,(\mathrm{mod}\, n)$.

$(Z_n, +_n)$ ist eine Gruppe, jedoch keine Untergruppe von $\mathbb{Z}$. Gegenüber $(\mathbb{Z},+)$ hat sich die Operation geändert.

Beispiel: $3 +_5 6 = 9\,(mod\ 5) = 4$ aber $3+6=9$.

3.20 Lemma *(Abgeschlossenheit von Unteralgebren bezüglich Durchschnitt)*

Sei J eine Indexmenge und $\forall j \in J : U_j \leq A$. Dann gilt

$$\bigcap_{j\in J} U_j \leq A$$

3.21 Definition *(erzeugte Unteralgebra)*

Sei M eine Teilmenge einer Algebra A. Dann heißt

$$\langle M\rangle := \bigcap_{U\leq A \text{ mit } M\subseteq U} U$$

die „von M erzeugte Unteralgebra“.

3.22 Beispiel

1) Sei $G = (G,\odot)$ eine Gruppe und $g \in G$.

$$\langle g\rangle := \langle\{g\}\rangle = \{g^i | i \in \mathbb{Z}\}$$

ist die von g erzeugte Untergruppe. Dabei ist

$$g^i := \begin{cases} \overbrace{g\odot\ldots\odot g}^{i \text{ mal}} & \text{falls } i>0 \\ 1 & \text{falls } i=0 \\ \underbrace{g^{-1}\odot\ldots\odot g^{-1}}_{-i \text{ mal}} & \text{falls } i<0 \end{cases}$$

2) $\langle\{g_1,\ldots,g_n\}\rangle = \{g_1\odot\ldots\odot g_m | m\in\mathbb{N}_0 \wedge g_i \in \{g_1,\ldots,g_n,g_1^{-1},\ldots,g_n^{-1}\}\,\forall i = 1\ldots m\}$

3.23 Definition *(Homomorphismus)*

Seien $A = (A,(f_i)_{i\in I})$ und $\widetilde{A} = (\widetilde{A},(\widetilde{f}_i)_{i\in I})$ Algebren vom Typ $T = (n_i)_{i\in I}$. Ein „(Algebra-)Homomorphismus“ ist eine Abbildung $\varphi : A \to \widetilde{A}$ mit $\forall i \in I : \forall a_1\ldots a_{n_i} \in A : \widetilde{f}_i(\varphi(a_1),\ldots,\varphi(a_{n_i})) = \varphi(f_i(a_1),\ldots,f_i(a_{n_i}))$. Die Reihenfolge der Anwendung von f_i bzw. $\widetilde{f}_i$ und φ ist also beliebig. Folgende zwei Rechnungen müssen für jede Operation bei beliebigen Operanden das gleiche Ergebnis ergeben:

- Operation auf die Operanden anwenden, anschließend φ auf das Ergebnis anwenden
- φ auf die Operanden anwenden, anschließend die Operation auf den Ergebnissen anwenden

3.24 Beispiel

1) Sei $A = (A, (f_i)_{i\in I})$ eine Algebra mit Unteralgebra $A' \leq A$. Ferner sei $id : A' \to A$ eine Abbildung mit $\forall a \in A' : id(a) = a$.

id ist ein Algebrahomomorphismus. Durch *id* wird A' in A eingebettet. Zum Beispiel wird so auch $(\mathbb{N}, +)$ in $(\mathbb{Z}, +)$ eingebettet.

2) Seien $A = (\Sigma^*, \circ)$ (siehe Beispiel 3.3) und $\widetilde{A} = (\mathbb{N}_0, +)$. Dann ist $\varphi : \Sigma^* \to \mathbb{N}_0$ mit $\forall w \in \Sigma^* : \varphi(w) = \underbrace{|w|}_{\text{Länge von } w}$ ein Homomorphismus.

3) Sei K ein Körper, V und W K-Vektorräume (LA Definition 2.25)

$$\begin{aligned} \varphi : V \to W \text{ ist Homomorphismus} \quad \Leftrightarrow \quad & \varphi \text{ ist } K-\text{linear, d.h. } \forall v, w \in V : \forall \alpha \in K : \\ & \varphi(v+w) = \varphi(v) + \varphi(w) \\ & \varphi(-v) = -\varphi(v) \\ & \varphi(0) = 0 \\ & \varphi(\alpha \cdot v) = \alpha \cdot \varphi(v) \end{aligned}$$

3.25 Definition *(Isomorphismus, Automorphismus)*

Seien $A = (A, (f_i)_{i\in I})$ und $\widetilde{A} = (\widetilde{A}, (\widetilde{f}_i)_{i\in I})$ Algebren

- Ein „Isomorphismus“ $\varphi : A \to \widetilde{A}$ ist ein bijektiver Homomorphismus.
- A und $\widetilde{A}$ heißen „isomorph“ (in Zeichen $A \cong \widetilde{A}$) genau dann wenn ein Isomorphismus $\varphi : A \to \widetilde{A}$ existiert.
- Ein „Automorphismus“ ist ein Isomorphismus $\varphi : A \to A$.

3.26 Beispiel

1) $A := (\mathbb{N}, +)$, $\widetilde{A} := (\{2n | n \in \mathbb{N}\}, +)$, dann ist $\varphi : \mathbb{N} \to \{2n | n \in \mathbb{N}\}$, $n \mapsto 2n$ ein Isomorphismus.

2) $A := (\underbrace{\{x \in \mathbb{R} | x > 0\}}_{=:\mathbb{R}^+}, \cdot)$, $\widetilde{A} = (\mathbb{R}, \cdot)$, dann ist $\varphi : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto \log x$ ein Isomorphismus: $\forall x, y \in \mathbb{R}^+ :$ $\log(x \cdot y) = \log x + \log y$.

3) Sei $A = (\{1,2,3\}, \circ)$ eine Algebra mit $\forall x, y \in \{1,2,3\} : x \circ y = 3$ und $\varphi : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$ ist ein Automorphismus.

3.27 Lemma *(Strukturerhaltung durch Isomorphismen)*

Ein Isomorphismus bildet neutrale Elemente auf neutrale Elemente ab und inverse Elemente auf inverse Elemente

3.28 Lemma *(Umkehrabbildung von Isomorphismen)*

Ist $\varphi : A \to \widetilde{A}$ ein Isomorphismus, so existiert die Umkehrabbildung $\varphi^{-1} : \widetilde{A} \to A$. Die Umkehrabbildung ist ebenfalls ein Isomorphismus.

3.29 Beispiel

Betrachte $\mathbb{Z}$ und ein $m \in \mathbb{N}$. Definiere $\sim_m$ so daß $a \sim_m b \Leftrightarrow m | a \cdot b$ (d.h. $a \equiv b \pmod m$). Dann gilt

$$\mathbb{Z} = \underbrace{\{k_m | k \in \mathbb{Z}\}}_{=[0]_{\sim_m}} \cup \underbrace{\{k_{m+1} | k \in \mathbb{Z}\}}_{=[1]_{\sim_m}} \cup \ldots \cup \underbrace{\{k_{n+(m+1)} | k \in \mathbb{Z}\}}_{=[m-1]_{\sim_m}}$$

.

$$\begin{aligned} \mathbb{Z}_m &:= \{[0]_{\sim_m}, [1]_{\sim_m}, \ldots, [m-1]_{\sim_m}\} \\ &= \mathbb{Z}/_m\mathbb{Z} \\ &= \{[a]_{\sim_m} | a \in \mathbb{Z}\} \\ &= \{\{a + mz | z \in \mathbb{Z}\} | a \in \mathbb{Z}\} \\ &= \{a + m\mathbb{Z} | a \in \mathbb{Z}\} \end{aligned}$$

3.30 Definition *(Kongruenzrelation)*

Sei $A = (A, (f_i)_{i \in I})$ ein Algebra vom Typ $(n_i)_{i \in I}$. Eine „Kongruenzrelation“ auf A ist eine Äquivalenzrelation für die mit allen Operatoren der Algebra verträglich ist, d.h. $\forall i \in I : a_1 \sim a'_1, \ldots, a_{n_i} \sim a'_{n_i} \Rightarrow f(a_1, \ldots, a_{n_i}) \sim f(a'_1, \ldots, a'_{n_i})$.

3.31 Beispiel

Sei $G = (G, \odot)$ eine Gruppe und $\sim$ eine Äquivalenzrelation auf G. Dann ist $\sim$ eine Kongruenz genau dann wenn $a \sim a', b \sim b' \Rightarrow a \odot b \sim a' \odot b'$ und $a^{-1} \sim (a')^{-1}$.

3.32 Satz *(Homomorphiesatz)*

Sei $A = (A, (f_i)_{i \in I})$ ein Algebra vom Typ $T = (n_i)_{i \in I}$ und $\sim$ eine Kongruenzrelation auf A.

1) Für jedes $a \in A$ heißt $[a]_\sim := \{a' \in A | a' \sim a\}$ „Äquivalenzklasse von a“. Die Menge aller Äquivalenzklassen $A/_\sim := \{[a]_\sim | a \in A\}$ ist eine Algebra vom Typ T mit den Operationen $\overline{f_i}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) := f_i(a_1, \ldots, a_{n_i})$.

$\pi_\sim : A \to A/_{sim}$ mit $a \mapsto [a]_\sim$ ist ein surjektiver Homomorphismus (Epimorphismus).

2) Sei $\varphi : A \to B$ ein Homomorphismus von A in eine Algebra B. durch $a \sim a' \Leftrightarrow \varphi(a) \sim \varphi(a')$ wird eine Kongruenzrelation auf B definiert und $\varphi(A)$ ist eine Unteralgebra von B.

$\overline{\varphi} : A/_\sim \to \varphi(A); [a] \mapsto \varphi(a)$ ist ein Isomorphismus.

Beweis nachrechnen!

3.33 Beispiel

Sei K ein Körper und V, W zwei K-Vektorräume. Ferner sei $\varphi : V \to W$ eine K-lineare Abbildung (also ein Homomorphismus). Definiere $\sim$ durch $v \sim v' :\Leftrightarrow \varphi(v) = \varphi(v')$. Es gilt dann:

$$\begin{aligned} v \sim v' &\Leftrightarrow \varphi(v) = \varphi(v') \\ &\Leftrightarrow \varphi(v) - \varphi(v') = 0 \\ &\Leftrightarrow \varphi(v - v') = 0 \\ &\Leftrightarrow v - v' \in \mathrm{Kern}(\varphi) \leq V \end{aligned}$$

also $\forall v \in V : [v]_\sim = v + \mathrm{Kern}(\varphi)$ und $[0]_\sim = \mathrm{Kern}(\varphi)$.

3.3 Ringe und Ideale

3.34 Lemma

Sei R ein Ring. Es gilt

- $\forall a \in R : a \cdot 0 = 0 \cdot a = 0$
- $\forall a \in R : \forall b \in R : a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
- $\forall a \in R : -(-a) = a$
- $\forall a \in R : \forall b \in R : -(a + b) = (-a) + (-b)$
- Für $a + (-b)$ benutzt man üblicherweise die schreibweise „$a - b$“.

Sei $\sim$ eine Kongruenzrelation auf R. Betrachte den Teilring $[0]_\sim := \{a \in R | a \sim 0\}$

- $a \sim a' \Leftrightarrow a + (-a') \sim a' + (-a') \Leftrightarrow a - a' \in [0]_\sim$
  Die Kongruenzrelation $\sim$ ist also durch $[0]_\sim$ vollständig beschrieben.
- Seien $u \in [0]_\sim$, $v \in [0]_\sim$. Dann gilt
$$u \sim 0 \wedge v \sim 0 \Rightarrow u + v \sim 0 \Rightarrow u + v \in [0]_\sim$$

3.35 Definition *(Ideal)*

Sei $R = (R, +, \cdot)$ ein Ring. Ein *Ideal* von R ist eine Menge $I \subseteq R$ für die gilt:

- $0 \in I$
- $a \in I \wedge b \in I \Rightarrow a + b \in I \wedge (-a) \in I$
- $a \in I \wedge u \in I \Rightarrow a \cdot u \in I \wedge u \cdot a \in I$

3.36 Satz *(Kongruenzrelationen und Ideale)*

Ist $\sim$ eine Kongruenzrelation auf einem Ring R, so ist $I = [0]_\sim$ ein Ideal von R. Ist umgekehrt I ein Ideal von R, so wird durch $a \sim a' \Leftrightarrow a - a' \in I$ eine Kongruenzrelation definiert. Dabei gilt $[0]_\sim = I$ und $[a]_\sim = a + I$. Schreibweise: R/I oder auch $R/\sim$.

Beweis: Übung

3.37 Satz *(Hauptideale)*

Sei R ein kommutativer Ring mit $d \in R$. Dann gilt

- $R \cdot d := \{a \cdot d | a \in R\}$ ist Ideal von R (das von d erzeugte *Hauptideal*)
- $R \cdot d = R \Leftrightarrow d$ invertierbar in R

Beweis: Übung

3.38 Beispiel *(vgl. Beispiel 3.29)*

Sei $R = (\mathbb{Z}, +, \cdot)$ und $m \in \mathbb{N}$. Betrachte die Kongruenzrelation $\sim_m$.

$m\mathbb{Z}$ ist Ideal von $\mathbb{Z}$. $1\mathbb{Z} = \mathbb{Z}$.

Konvention: In einem kommutativen Ring schreibt man $k \cdot a := \underbrace{a + \ldots + a}_{k \text{ mal}}$

3.39 Beispiel

Behauptung: Keine ganze Zahl der Form $7 + n \cdot 8$ ist die Summe von 3 Quadratzahlen .

Beweis: Angenommen es gilt $z = 7 + n \cdot 8 = a^2 + b^2 + c^2$ für geeignete $a, b, c \in \mathbb{Z}$. Betrachte den Homomorphismus $\varphi : \mathbb{Z} \to 8 \cdot \mathbb{Z}$ mit $z \mapsto [z]_8$. Es gilt

$$\begin{aligned} \varphi(z) &= \varphi(a^2) + \varphi(b^2) + \varphi(c^2) \\ &= \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2 \\ &= [7]_8 \end{aligned}$$

In $\mathbb{Z}_8$ gilt jedoch:

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1

Quadratzahlen sin somit 0, 1 und 4. 7 kann also nicht die Summe von genau drei Quadratzahlen sein.

3.4 Gößter gemeinsamer Teiler

Unter Ringen gibt es folgende Spezialisierungen:

Ringe $\supseteq$ kommutative Ringe $\supseteq$ Integritätsbereiche $\supseteq$ Hauptidealringe $\supseteq$ Euklidische Ringe

Natürliche Zahlen $p > 1$ für die 1 und p die einzigen positiven Teiler sind nennt man *Primzahlen*.

Ist $m \in \mathbb{N}$ keine Primzahl, so gibt es $p \in \mathbb{N}$, $q \in \mathbb{N}$ so daß $1 < p \leq q < m$ und $m = p \cdot q$. Es gilt dann

$$[p]_m \cdot [q]_m = [p \cdot q]_m = [m]_m = [0]_m = 0 \in \mathbb{Z}_m$$

obwohl $[p]_m \neq 0$ und $[q]_m \neq 0$.

3.40 Definition *(Nullteiler, Integritätsbereich)*

Sei $R = (R, +, \cdot)$ ein kommutativer Ring. Gilt für $0 \neq a \in R$ und $0 \neq b \in R$: $a \cdot b = 0$, so heißen a und b *Nullteiler*.

Ein kommutativer Ring ohne Nullteiler heißt *Integritätsbereich*. In Integritätsbereichen gilt die Implikation $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$.

3.41 Beispiel

1. $\mathbb{Z}$ ist ein Integritätsbereich
2. $\mathbb{Z}[x]$ ist ein Integritätsbereich
3. Für jeden Körper K sind $K[x]$ und $K[[x]]$ Integritätsbereiche
4. $\mathbb{Z}_4$ ist kein Integritätsbereich, denn $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 = 0 \in \mathbb{Z}_4$
   $\mathbb{Z}_6$ ist kein Integritätsbereich, denn $[2]_6 \cdot [3]_6 = [6]_6 = [0]_6 = 0 \in \mathbb{Z}_6$
   $\mathbb{Z}_m$ ist kein Integritätsbereich für jedes m das keine Primzahl ist.

3.42 Definition (*größter gemeinsamer Teiler*)

Sei R ein Integritätsbereich.

1. $\underbrace{a|b}_{a \text{ teilt } b} :\Leftrightarrow \exists c \in R : c \cdot a = b$
2. $d \in R$ heißt *größter gemeinsamer Teiler* von a und b (in Zeichen: $d \in \mathrm{ggT}(a,b)$) wenn gilt:
   - $d|a \wedge d|b$
   - $c|a \wedge c|b \Rightarrow c|d$

3.43 Bemerkung (*Einheit*)

Sei $R = (R, +, \cdot)$ ein Integritätsbereich. $u \in R$ heißt *Einheit* falls $u^{-1} \in R$. $R^* := \{u \in R | u^{-1} \in R\}$.

1. In $\mathbb{Z}$ sind 1 und -1 Einheiten. Es gilt $\mathrm{ggT}(4,10) = \{2,-2\}$
2. Sei $u \in R$ Einheit in R. Dann gilt $\forall a \in R : u|a$ denn $a = u \cdot (u^{-1} \cdot a)$
3. $d \in \mathrm{ggT}(a,b)$ und $u \in R^* \Rightarrow u \cdot d \in \mathrm{ggT}(a,b)$. Umgekehrt gilt auch: $d, d' \in \mathrm{ggT}(a,b) \Rightarrow \exists u \in R^* : d = u \cdot d'$.
4. Nicht in jedem Integritätsbereich IB gilt $\forall a,b \in IB : \mathrm{ggT}(a,b) \setminus \{1,-1\} \neq \emptyset$.

3.5 Eindeutige Primfaktorenzerlegung

Welche Eigenschaften muß ein Ring haben, damit die Primfaktorzerlegung eindeutig ist?

3.44 Definition (*irreduzibel*)

Sei R ein Integritätsbereich und $p \in R$, so daß $p \neq 0 \wedge p \notin R^*$.

p heißt *irreduzibel* wenn gilt

$$p = a \cdot b \Rightarrow a \in R^* \vee b \in R^*$$

3.45 Beispiel

$$p \in \mathbb{Z} \text{ irreduzibel} \Leftrightarrow p \text{ Primzahl } \vee -p \text{ Primzahl}$$

3.46 Beispiel

Sei $I = \{a + b \cdot \sqrt{-3} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

1. $(I, +, \cdot)$ ist Integritätsbereich
2. $I^+ = \{1, -1\}$
3. $|\alpha|^2 = 4 \Rightarrow \alpha$ irreduzibel
4. $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ sind zwei verschiedene Primfaktorzerlegungen in I.

3.47 Definition (*eindeutige Primfaktorzerlegung*)

Sei R ein Integritätsbereich. $a \in R$ hat eine *eindeutige Primfaktorenzerlegung* genau dann wenn aus $a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ mit $p_i \in R$ irreduzibel und $q_i \in R$ irreduzibel folgt: $r = s$ un mit geeigneter Umsortierung gilt $q_i = u_i \cdot p_i$ für $u_i \in R^*$.

3.48 Bemerkung

Hat $a \in R$ eine eindeutige Zerlegungm so gilt $a \in R \setminus (\{0\} \cup R^*)$, da

$$\begin{aligned} 0 = a_1 \cdot \ldots \cdot a_\alpha &\Rightarrow \exists i : a_i = 0 \text{ aber 0 ist nicht irreduzibel} \\ R^* \ni u = a_1 \cdot \ldots \cdot a_\beta &\Rightarrow 1 = a_1 \cdot (u^{-1} \cdot a_2 \cdot \ldots \cdot a_\beta) \\ &\Rightarrow a_1 \in R^* \text{ aber Einheiten sind nicht irreduzibel} \end{aligned}$$

3.49 Definition (*Hauptidealring*)

Ein Integritätsbereich in dem jedes Ideal ein Hauptideal ist heißt *Hauptidealring*.

3.50 Satz (hinreichende Bedingung für eindeutige Primfaktorenzerlegung)

In einem Hauptidealring R hat jdes $a \in R \setminus (\{0\} \cup R^*)$ eine eindeutige Primfaktorzerlegung.

Beweis: ohne

3.51 Satz (*Euklidischer Ring*)

Ein *euklidischer Ring* ist ein Integritätsbereich in dem es eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}_0$ gibt, so daß

$$\forall a, b \in R, b \neq 0 : \exists q, r \in R : a = q \cdot b + r \wedge \delta(r) < \delta(b)$$

Ein euklidischer Ring (R, δ) mit

$$\begin{aligned} \delta(a) = 0 &\Leftrightarrow a = 0 \\ \delta(a \cdot b) &= \delta(a) \cdot \delta(b) \end{aligned}$$

heißt *Norm-euklidischer Ring*.

3.52 Folgerung

1. $(\mathbb{Z}, |\,|)$ ist ein euklidischer Ring mit $|a| = \begin{cases} a & , \text{ falls } a \geq 0 \\ -a & , \text{ falls } a < 0 \end{cases}$.
2. Sei K ein Körper und $R = (K[x], \text{grad})$. Dann ist R ein euklidischer Ring. Es gilt z.B. $x^5 + x^3 + 1 = (2x^2 + x) \cdot (\frac{1}{2}x^2 + \frac{1}{4}) + (-\frac{1}{4}x + 1)$ und $\text{grad}(-\frac{1}{4}x + 1) < \text{grad}(\frac{1}{2}x^2 + \frac{1}{4})$.
3. Sei K ein Körper. Dann ist $R = (K[x], \delta)$ mit $d(f) = \begin{cases} 2^{\text{grad}(f)} & , \text{ falls } f \neq 0 \\ 0 & , \text{ falls } f = 0 \end{cases}$ ein Norm-euklidischer Ring.

3.53 Satz

In einem euklidischen Ring hat jedes $a \in R \setminus (\{0\} \cup R^*)$ eine eindeutige Primfaktorzerlegung.

Beweis: Jeder euklidische Ring ist ein Hauptidealring.

3.54 Folgerung

In $\mathbb{Z}$ hat jedes $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ eine eindeutige Primfaktorzerlegung.

Beweis: $\mathbb{Z}$ ist euklidischer Ring.

3.55 Bemerkung (*Fundamentalsatz der Arithmetik*)

Aus Folgerung 3.54 folgt der *Fundamentalsatz der Arithmetik*: Jedes $n \in \mathbb{N}$ mit $n \geq 2$ läßt sich eindeutig als Prodikt von Primzahlen darstellen: $n = p_1^{t1} \cdot \ldots \cdot p_k^{t_k}$ mit Primzahlen $p_1 \ldots p_k$ und natürlichen Zahlen $t_1 \ldots t_k$.

3.56 Satz (*Existenz unendlich vieler Primzahlen*)

Es existieren unendlich viele Primzahlen.

Beweis: Setze $P_k = \{p \leq k \in \mathbb{N} | p \text{ ist Primzahl}\}$. Offensichtlich gilt $\forall i < j : P_i \subseteq P_j$.
Definiere $n := 1 + \prod_{p \in P_k} p$

Fall 1: n ist Primzahl.

$$\begin{aligned} n > k \quad &\Rightarrow \quad P_k \subset P_n \\ &\Rightarrow \quad \forall k \in \mathbb{N} \exists p \text{ Primzahl} : p > k \\ &\Rightarrow \quad \text{Es existieren unendlich viele Primzahlen} \end{aligned}$$

Fall 2: n ist keine Primzahl.

Es existiert eine eindeutige Primfaktorzerlegung $n = \prod_{i=1}^{s} p_{n_i}^{t_i}$ mit $p_{n_i} \in P_n \forall i = 1 \ldots s$. Es gilt jedoch $n \equiv 1 \,(\text{mod } p)$, also nicht $p | n$ $(\forall p \in P_k)$. Demnach existiert ein $q \in P_n$ mit $q \notin P_k$. Somit gilt $P_k \subset P_n$ und analog zu Fall 1 existieren unendlich viele Primzahlen.

3.57 Satz (*Primzahlsatz*)

Sei Prim : $\mathbb{N} \to \mathbb{N}$ mit $n \mapsto$ Anzahl der Primzahlen p für die gilt $p \leq n$.

Es gilt:

$\lim_{n\to\infty} \frac{\text{Prim}(n)}{\frac{n}{\ln n}} = 1$

3.58 Bemerkung (*Algorithmus zum Bestimmen von Primzahlen*)

Alle Primzahlen die kleiner oder gleich einer natürlichen Zahl n sind, können mit folgendem Algorithmus gefunden werden:

```
Schreibe alle Zahlen von 2 bis n auf
for i=2 to √n do
    if i nicht markiert
        markiere alle vielfachen von i
end
```

Die nicht markierten Zahlen sind genau die gesuchten Primzahlen.

Große Primzahlen können mit randomisierten Verfahren gefunden werden. Dabei wird ein Algorithmus mit folgendem Verhalten verwendet:

Eingabe: eine zu prüfende Zahl p
ein Hilfsparameter e

Ausgabe: 0 (p ist keine Primzahl)
1 (p ist mit einer Wahrscheinlichkeit von x% eine Primzahl)

Der Algorithmus wird mit verschiedenen Werten von e so lange angewendet bis eine 0 ausgegeben wird, oder die Gesammtwahrscheinlichkeit aller Tests hoch genug ist.

3.59 Lemma (*kleiner Fermat'sche Satz*)

Für alle $n \in \mathbb{N}$ mit $n \geq 2$ gilt:

$$n \text{ Primzahl} \Leftrightarrow \forall a \in \mathbb{Z}_n \setminus \{0\} : a^{n-1} \equiv 1 \,(\text{mod } n)$$

3.60 Satz (*eulersche* φ*-Funktion*)

Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ mit $n \mapsto |\mathbb{Z}_n^*|$ heißt *eulersche* φ*-Funktion*. Dabei ist $\mathbb{Z}_n^* := \{a \in \mathbb{Z} \setminus \{0\} | \text{ggT}(n,a) = 1\}$.

3.61 Lemma

Für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}$ gilt:

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{t_i - 1}$$

3.62 Satz (*Euler*)

$\forall 2 \leq n \in \mathbb{N} : \forall a \in \mathbb{Z}_n^+ : a^{\varphi(n)} \equiv 1 \pmod{n}$

Bemerkung: Für Primzahlen folgt Satz 3.59 aus Satz 3.62

3.63 Lemma

Für $m \leq n \in \mathbb{N}$ mit m teilt nicht n gilt

$$\text{ggT}(m,n) = \text{ggT}(n \bmod m, m)$$

Beweis: Übung

3.64 Satz (*Euklidischer Algorithmus*)

Der Größte gemeinsame Teiler von zwei Zahlen $a_0 \geq a_1$ kann mit dem *euklidischen Algorithmus* wie folgt bestimmt werden:

Bestimme sukzessiv a_i und q_i durch

$$\begin{aligned} a_0 &= q_1 a_1 + a_2 \text{ mit } 0 \leq a_2 \leq a_1 \\ a_1 &= q_2 a_2 + a_3 \text{ mit } 0 \leq a_3 \leq a_2 \\ &\vdots \\ a_{k-1} &= q_k a_k + 0 \end{aligned}$$

Es gilt dann $a_k = \text{ggT}(a_0, a_1)$

3.65 Definition (*normiertes Polynom*)

Ein Ploynom $f = \prod_{k=0}^{n} a_k x^k$ heißt *normiert*, falls $a_n = 1$.

3.66 Folgerung

Ist K ein Körper, so hat jedes Polynom $f \in K[x] \setminus \{0\}$ eine eindeutige Zerlegung $f = u f_1 \cdot \ldots \cdot f_r$ mit $u \in K^*$ und f_i irreduzibel.

Beweis: Folgt aus Beispiel 3.52 und Satz 3.53

3.67 Satz

Sei (R, δ) ein euklidischer Ring und $0 \neq f \in R$. Ferner sei $R/_{fR} = \{[g]_f | g \in R, \delta(g) < \delta(f)\}$ mit $[g]_f := g + fR := \{g + fz | z \in R\}$. Dann gilt:

$$R/_{fR} \text{ ist Körper} \Leftrightarrow f \text{ ist irreduzibel}$$

3.68 Beispiel

3.69 Bemerkung (*diskreter Logarithmus*)

Ist $\alpha^i = \beta$, so schreibt man $i = \log_\alpha \beta$.

3.6 Endliche Körper

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind unendliche Körper.
- $(\mathbb{Z}_2, +_2, \cdot_2)$ ist mit
  - $+_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2; (a +_2 b) = ((a + b) \bmod 2)$ und
  - $\cdot_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2; (a \cdot_2 b) = ((a \cdot b) \bmod 2)$

  ein endlicher Körper
- $(\mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]}, +_f, \cdot_f)$ ist mit
  - $f = x^3 + x + 1$
  - $+_f : \mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]} \times \mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]} \to \mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]}; (g +_f h) = ((g + h) \bmod f)$ und
  - $\cdot_f : \mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]} \times \mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]} \to \mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]}; (g \cdot_f h) = ((g \cdot h) \bmod f)$

  ein endlicher Körper

3.70 Folgerung (*Existenz endlicher Körper*)

1. $(\mathbb{Z}_n, +_n, \cdot_n)$ ist Körper $\Leftrightarrow$ n ist Primzahl.
2. Sei K ein Körper und $f \in K[x]$. Dann gilt $\mathbb{K}[x]/_{f\mathbb{K}[x]}$ ist Körper $\Leftrightarrow$ f ist irreduzibel in $K[x]$

Beweis: folgt aus Satz 3.67.

3.71 Satz (*Eindeutigkeit endlicher Körper*)

1. Für jede Primzahl p und jedes $k \in \mathbb{N}$ existiert ein Körper mit genau p^k Elementen.
2. Sind K_1 und K_2 endliche Körper mit $|K_1| = |K_2|$, so gilt $K_1 \cong K_2$.

Endliche Körper mit p^k Elementen werden als Galoiskörper (in Zeichen: $\mathrm{GF}(p^k)$, englisch: galois field) bezeichnet.

3.72 Satz (*zyklische multiplikative Gruppen*)

In jedem endlichen Körper K ist die multiplikative Gruppe K^* zyklisch, das heißt $\exists a \in K^* : K^* = \langle a \rangle := \{1, a, a^2, \ldots, a^{|K|-2}\}$ (ein solches a heißt *Generator*).

Literaturverzeichnis

[1] A. Steger: „Diskrete Mathematik I“, Springer 2001

[2] R. Graham, D.Knuth, O. Patashmik: „Concrete Mathematics“, Addison Wesley, Auflage 2000

[3] L. Volkmann: „Fundamente der Graphentheorie“, Springer 1996

Index

Äquivalenzklasse, 72

abelsch, 68
Ableitung
    formale, 27
adjazent, 42
Adjazenzliste, 53
Adjazenzmatrix, 45
Algebra
    abelsche, 68
    boolsche, 68
    universelle, 65
Ausengrad, 63
Automorphismus, 71

balanciert, 51
Baum, 49
    balancierter, 51
    binärer, 51
    geordneter, 50
    spannender, 51
Baumfaktor, 51
benachbart, 42, 61
Bezierkurve, 14
Binomialkoeffizient, 13
    verallgemeinerter, 29
bipartit, 54
Brücke, 47
Breadth-First-Search, 52
Briefträgerproblem, 59

Catalan-Zahlen, 34
Cauchy-Produkt, 24
Cayley
    Tree Formula, 53

Depth-First-Search, 52
Digraph, 62
disjunkte Vereinigung, 11
doppeltes Abzählen, 14

Ecke, 39
Eckengrad, 43
einbettbar, 60
Elemente
    inverse, 67
    neutrale, 66

Endecke, 42
erzeugende Funktion, 23
eulersch, 58
Exklusion, 17

Färbung, 61
Faltung, 24
Fibonacci-Zahlen, 31
formale Ableitung, 27
formale Potenzreihe, 23

Galoiskörper, 80
Gebiet, 60
geometrische Reihe, 25
Gerüst, 51
Gittergraph, 41
goldener Schnitt, 32
Graph, 39
    benannter, 44
    ebener, 60
    eulerscher, 58
    hamiltonscher, 56
    leerer, 42
    markierter, 44
    planarer, 60
    regulärer, 43
    schlichter, 42
    semi-eulerscher, 58
    untergeordneter, 63
    vollständiger, 39
Graphen
    bipartite, 54
Gruppe, 67

Halbgruppe, 67
Hamilton-Weg, 56
Hamiltonkreis, 56
hamiltonscher Graph, 56
    semi-, 56
Hauptideal, 74
Hauptidealring, 76
Hyperwürfel, 41

Ideal, 73
injektive Abbildung, 20
Inklusion, 17
Integritätsbereich, 75

Invertierbarkeit
  geometrische Reihe, 25
  in Ringen, 25
  Potenzreihen, 26
Invertieren, 26
Inzidenzmatrix, 45
inzidieren, 42
irreduzibel, 75
Isomorphie
  zwischen Graphen, 44
Isomorphismus, 71

Jordanbogen, 60

Körper, 68
Kante, 39
Kantenfolge, 58
  orientierte, 62
Kantenzug, 58
  eulerscher, 58
  orientierter, 62
kartesisches Produkt, 11
Knoten, 39
Komponente, 47
Kongruenzrelation, 72
Konvolution, 24
Kreis, 40
  Hamilton-, 56
Kronecker-Symbol, 23

Land, 60
Landkarte, 60
Logarithmus
  diskreter, 80

Mächtigkeit, 11
Matching, 54
  maximales, 54
  Maximum-, 54
  perfektes, 54
Maximum-Matching, 54
Mehrfachkanten, 42
Monoid, 67
Multigraph, 42

n-Menge, 11
Nachbarschaft, 43
  positive, 63
Nachfolger, 50
  unmittelbarer, 50
Nullgraph, 42
Nullteiler, 75

Operation, 65
Operator, 65

Partition, 18
Pascal-Dreieck, 13
Permutation, 12
planar, 60
Polynom
  normiertes, 79
Potenzmenge, 12
Potenzreihe, 23
Primzahlsatz, 78
Produktregel, 16
  formaler Ableitungen, 27

regulär, 43
Rekursionsgleichung
  lineare, 30
Ring, 68
  euklidischer, 76
  Norm-euklidischer, 76

Schlingen, 42
Schnittecke, 47
Schubfachprinzip, 15
  verallgemeinertes, 16
semi-eulersch, 58
Siebformel, 17
Signatur, 65
Stelligkeit, 65
Stirling-Dreieck
  erster Art, 22
  zweiter Art, 18
Stirlingzahlen
  erster Art, 22
  zweiter Art, 18
Summenregel, 16
surjektive Abbildung, 20
symmetrische Gruppe, 12

Teildigraph, 62
  induzierter, 62
Teilgraph, 46
  induzierter, 46
Teilring, 69
Tiefe, 51
Travelling Salesman Problem, 57
TSP, 57
Turnier, 63

Unteralgebra, 69
Untergruppe, 69
Unterteilungsgraph, 61

Vandermonde’sche Identität, 14
Verknüpfung, 65
Vorgänger, 50
  unmittelbarer, 50

Wald, 49

Weg, 40
    Hamilton-, 56
    orientierter, 62
Wurzelbaum, 50
    balanciert, 51

zusammenhängend, 46
    stark, 63
Zusammenhangskomponente, 47
    starke, 63
Zyklus, 22