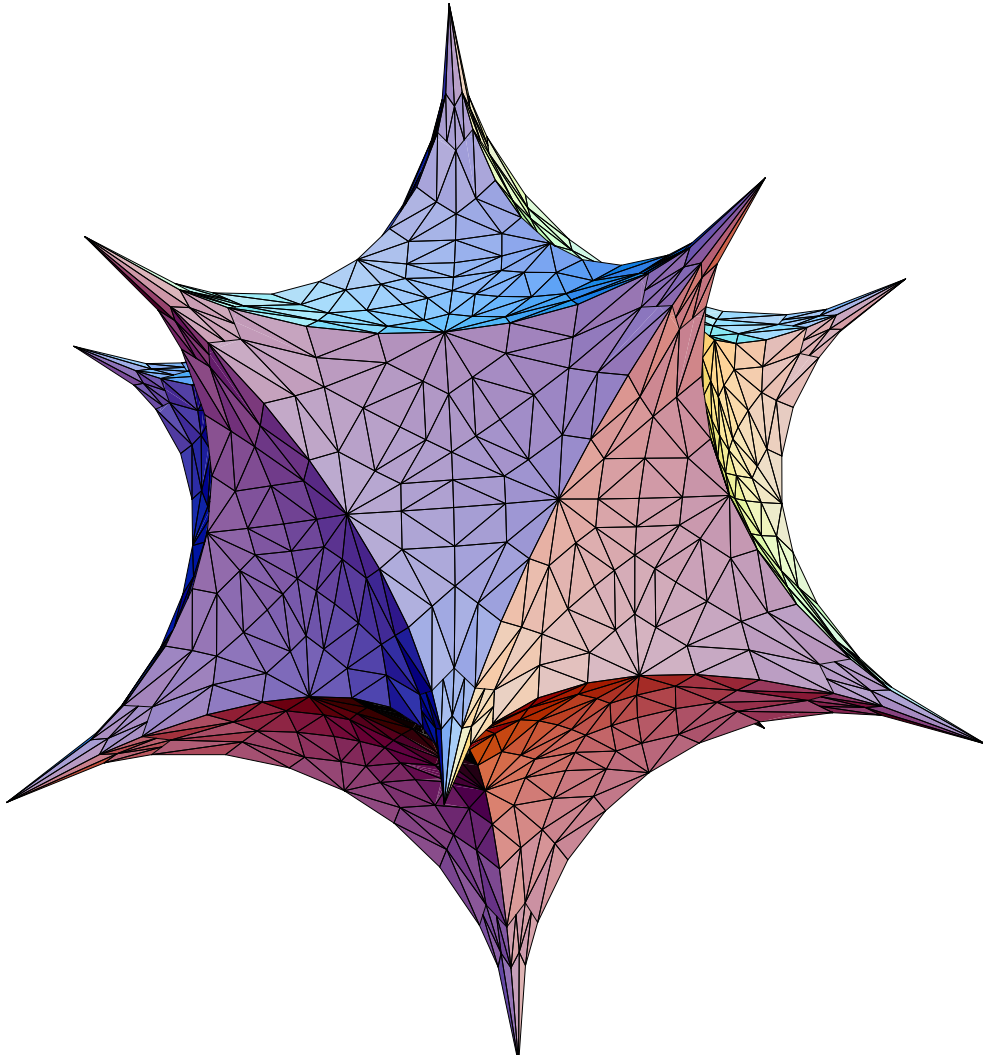


Diskrete Mathematik 2



Berner Fachhochschule - Technik und Informatik
Fachbereich Informatik

Dr. W. Businger

Dr. V. Bigler

HS 2020/21

Diese Seite ist leer.

Inhaltsverzeichnis

1	Kombinatorik	1
1.1	Grundlegende Prinzipien	1
1.2	Permutationen	3
1.3	Variationen ohne Wiederholung	5
1.4	Kombinationen	6
1.5	Permutationen mit Wiederholung	7
1.6	Variationen mit Wiederholung	8
1.7	Kombinationen mit Wiederholungen	9
1.8	Die Ein- und Ausschlussformel	10
2	Graphentheorie	12
2.1	Das Königsberger Brückenproblem	12
2.2	Definition eines Graphen	13
2.3	Grad eines Knoten	16
2.4	Wege, Pfade und Zyklen	17
2.5	Eulersche Graphen	19
2.6	Hamiltonsche Graphen	22
2.7	Bäume	23
2.8	Erzeugender Baum	29
2.9	Das Problem des kürzesten Wegs	32
2.10	Die Eulersche Polyederformel	39
2.11	Polyeder und platonische Körper	42
2.12	Das Färben von ebenen Landkarten	45
2.13	Ergänzungen zum Färbungsproblem	50
2.14	Digraphen	51
2.15	Bipartite Graphen	53
3	Rekursion	58
3.1	Folgen	58
3.2	Auflösung von Rekursionen	60
3.3	Rekursive Programmierung	62
3.3.1	Komplexität	66
4	Gruppentheorie	70
4.1	Die Diedergruppe D_3	70
4.2	Der allgemeine Gruppenbegriff	72
4.3	Untergruppen	77
4.4	Nebenklassen und der Satz von Lagrange	78
4.5	Ordnung eines Elements	81
4.6	Restklassen	84
4.7	Die Gruppen (\mathbb{Z}_p^*, \cdot)	87
4.8	Klassifizierung einiger Gruppen	88
4.9	Endliche Körper	91
4.9.1	Einführung	91
4.9.2	Polynomringe	91
4.9.3	Der euklidische Algorithmus für Polynome	93
4.9.4	Faktorisierung von Polynomen	96
4.9.5	Konstruktion der endlichen Körper	97
4.9.6	Anwendungen	99

1 Kombinatorik

Die Kombinatorik ist ein Zweig der Mathematik, der sich mit dem Anordnen endlicher Mengen und dem *Abzählen* der verschiedenen Anordnungsmöglichkeiten beschäftigt.

Beispiel: Beim Lotto zieht man zufällig 6 Zahlen aus 45 Zahlen. Wie viele Möglichkeiten gibt es, einen Vierer zu erzielen?

Falls man genügend Zeit (und Lust) hätte, so könnte man alle möglichen Tipps von 6 Zahlen anschreiben und abzählen, wie viele davon bei einem bestimmten Ausgang einen Vierer ergeben. Wie wir weiter unten sehen werden, gibt es 8'145'060 mögliche Tipps, wovon 11'115 Vierer sind.

Die Kombinatorik erlaubt die Antwort auf solche Fragen durch Überlegungen und Rechnen statt durch stures Abzählen zu finden.

1.1 Grundlegende Prinzipien

Wir betrachten zuerst zwei grundlegende Abzählprinzipien:

Summenprinzip: Falls man eine Aufgabe auf n_1 Arten und eine zweite Aufgabe auf n_2 Arten ausführen kann, und falls die beiden Aufgaben **nicht** gleichzeitig ausgeführt werden können, dann gibt es $n_1 + n_2$ Möglichkeiten, die eine oder andere Aufgabe auszuführen.

Das Summenprinzip kann auch in der folgenden Form formuliert werden:

Wenn n_1 Objekte mit der Eigenschaft 1 und n_2 Objekte mit der Eigenschaft 2 gegeben sind, und wenn die beiden Eigenschaften sich ausschliessen, dann gibt es $n_1 + n_2$ Möglichkeiten, ein Objekt auszuwählen, das entweder Eigenschaft 1 oder 2 hat.

Beispiel 1 Angenommen eine Mathematikprofessorin **oder** eine Mathematik-Studentin soll als Vertreterin eines Universitätsausschusses gewählt werden. Auf wie viele Arten kann diese Vertreterin gewählt werden, wenn es 37 Professorinnen und 83 Studentinnen gibt.

Die Aufgabe wird im Unterricht gelöst. ◇

Das Summenprinzip lässt sich natürlich auf den Fall verallgemeinern, in dem Objekte mit mehr als zwei Eigenschaften gegeben sind.

Produktprinzip: Angenommen eine Aufgabe lässt sich in zwei Teilschritte zerlegen, die hintereinander ausgeführt werden. Wenn der erste Teilschritt auf n_1 Arten und der zweite Teilschritt für jede Möglichkeit des ersten Teilschritts auf n_2 Arten ausgeführt werden kann, dann kann die Aufgabe auf $n_1 \cdot n_2$ Arten ausgeführt werden.

Beispiel 2 Angenommen eine Mathematikprofessorin **und** eine Mathematik-Studentin sollen als zwei Vertreterinnen eines Universitätsausschusses gewählt werden. Auf wie viele Arten können diese beiden Vertreterinnen ausgewählt werden, wenn es 37 Professorinnen und 83 Studentinnen gibt.

Die Aufgabe wird im Unterricht gelöst. ◇

Das obige Prinzip lässt sich auf Aufgaben mit 3 oder mehr Teilschritten verallgemeinern.

Beispiel 3 Ein Code besteht aus zwei verschiedenen Buchstaben gefolgt von einer von Null verschiedenen Ziffer. Wie viele verschiedene Codes lassen sich bilden?

Die Aufgabe wird im Unterricht gelöst. \diamond

Beispiel 4 Bei einem Getränkeautomat kann Kaffee, Tee oder Kakao gewählt werden. Weiter kann das gewählte Getränk kalt oder warm sein und Zucker oder kein Zucker enthalten. Wie viele verschiedene Getränke können gewählt werden? Verwenden Sie ein Baumdiagramm.

Die Aufgabe wird im Unterricht gelöst. \diamond

In vielen Abzählproblemen benötigen wir sowohl das Summen- wie auch das Produktprinzip:

Beispiel 5 Ein Passwort kann aus 6 bis acht Zeichen bestehen (Klein- oder Grossbuchstaben oder Ziffern). Wie viele mögliche Passwörter gibt es?

Die Aufgabe wird im Unterricht gelöst. \diamond

Ein anderes elementares Prinzip ist das **Schubfachprinzip**: falls man N Objekte in m Fächer versorgt, und falls $N > m$ ist, dann gibt es mindestens ein Fach mit mindestens zwei Objekten.

Beispiel 6 Ein Mensch hat normalerweise 150'000 Haare auf dem Kopf. Zeigen Sie, dass es in der Schweiz mindestens zwei Menschen gibt mit der exakt gleichen Anzahl von Haaren.

Die Aufgabe wird im Unterricht gelöst. \diamond

Nachfolgend noch eine **Verallgemeinerung des Schubfachprinzips**: falls N Objekte in m Fächer versorgt werden, dann gibt es mindestens ein Fach, welches mindestens $\lceil N/m \rceil$ Objekte enthält. Hier bezeichnet $\lceil x \rceil$ die kleinste ganze Zahl, welche grösser oder gleich x ist.

Beweis: Angenommen keines der Fächer enthält mehr als

$$\left\lceil \frac{N}{m} \right\rceil - 1$$

Objekte. Dann ist die Gesamtzahl der Objekte höchstens gleich

$$m \left\{ \left\lceil \frac{N}{m} \right\rceil - 1 \right\} < m \left\{ \left(\frac{N}{m} + 1 \right) - 1 \right\} = N .$$

Man erhält also einen Widerspruch. \square

Beispiel 7 Beweisen Sie, dass in einer Gruppe von 100 Personen mindestens 9 im gleichen Monat Geburtstag haben.

Die Aufgabe wird im Unterricht gelöst. \diamond

1.2 Permutationen

Beispiel 8 5 Läufer A, B, C, D und E machen einen Wettlauf. Wie viele verschiedenen Ranglisten gibt es?

Lösung: Wir zählen alle Möglichkeiten auf:

$ABCDE$	$ABCED$	$ABDCE$	$ABDEC$	$ABECD$	$ABEDC$
$ACBDE$	$ACBED$	$ACDBE$	$ACDEB$	$ACEBD$	$ACEDB$
$ADBCE$	$ADBEC$	$ADCBE$	$ADCEB$	$ADEBC$	$ADECB$
$AEB CD$	$AEBDC$	$AECBD$	$AECDB$	$AEDBC$	$AEDCB$
$BACDE$	$BACED$	$BADCE$	$BADEC$	$BAECD$	$BAEDC$
$BCADE$	$BCAED$	$BCDAE$	$BCDEA$	$BCEAD$	$BCEDA$
$BDACE$	$BDAEC$	$BDCAE$	$BDCEA$	$BDEAC$	$BDECA$
$BEACD$	$BEADC$	$BECAD$	$BECDA$	$BEDAC$	$BEDCA$
$CABDE$	$CABED$	$CADBE$	$CADEB$	$CAEBD$	$CAEDB$
$CBADE$	$CBAED$	$CBDAE$	$CBDEA$	$CBEAD$	$CBEDA$
$CDABE$	$CDAEB$	$CDBAE$	$CDBEA$	$CDEAB$	$CDEBA$
$CEABD$	$CEADB$	$CEBAD$	$CEBDA$	$CEDAB$	$CEDBA$
$DABCE$	$DABEC$	$DACBE$	$DACEB$	$DAEBC$	$DAECB$
$DBACE$	$DBAEC$	$DBC AE$	$DBCEA$	$DBEAC$	$DBECA$
$DCABE$	$DCAEB$	$DCBAE$	$DCBEA$	$DCEAB$	$DCEBA$
$DEABC$	$DEACB$	$DEBAC$	$DEBCA$	$DECAB$	$DECBA$
$EABCD$	$EABDC$	$EACBD$	$EACDB$	$EADBC$	$EADCB$
$EBACD$	$EBADC$	$EBCAD$	$EBCDA$	$EBDAC$	$EBDCA$
$ECABD$	$ECADB$	$ECBAD$	$ECBDA$	$ECDAB$	$ECDBA$
$EDABC$	$EDACB$	$EDBAC$	$EDBCA$	$EDCAB$	$EDCBA$

Es gibt also 120 verschiedene Ranglisten. \diamond

Beispiel 9 Lösen Sie das obige Problem durch eine Überlegung.

Die Aufgabe wird im Unterricht gelöst. \diamond

Wir betrachten den allgemeinen Fall mit n ($n \in \mathbb{N}$) Läufern. Wir bezeichnen die n Läufer mit

$$A_1, A_2, A_3, \dots, A_n.$$

Gesucht wird die Anzahl der Anordnungen dieser n Elemente. Man bezeichnet jede solche Anordnung als **Permutation** der n Elemente. Wir betrachten zwei Verfahren wie wir diese Formel finden können:

Erstes Verfahren: Rekursion

Wir bezeichnen die Anzahl Permutationen von n Elementen mit P_n . Wir betrachten eine Permutation der $n - 1$ Elemente A_i ($i = 1, 2, \dots, n - 1$):

$$A_1 A_2 A_3 \dots A_{n-1}$$

Wir überlegen uns jetzt, wo wir das n -te Element A_n platzieren können:

$$\begin{array}{ccccccc}
 A_n & & A_n & & A_n & & A_n & \dots & A_n & & A_n \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow & \dots & \downarrow & & \downarrow \\
 & & A_1 & & A_2 & & A_3 & \dots & & & A_{n-1}
 \end{array}$$

Es gibt also n verschiedene Plätze. Da dies für jede der P_{n-1} Permutationen der $n - 1$ Elemente A_i ($i = 1, 2, \dots, n - 1$) der Fall ist, ergibt sich so:

$$P_n = n \cdot P_{n-1}$$

Da $P_1 = 1$ ist, ergibt sich so

$$P_n = n \cdot (n - 1) \cdot (n - 2) \cdots 2 \cdot 1 .$$

Wir kürzen den Ausdruck auf der rechten Seite als $n!$ ab, gelesen ***n Fakultät***.

Zweites Verfahren: direkte Herleitung

Wir betrachten die n Plätze (=Ränge):

$$\textcircled{1} \quad \textcircled{2} \quad \textcircled{3} \quad \textcircled{4} \quad \dots \quad \textcircled{n}$$

Für den ersten Platz haben wir n Läufer zur Auswahl. Unabhängig davon, wer den ersten Platz belegt, haben wir für den zweiten Platz noch $n - 1$ Läufer zur Auswahl. Unabhängig von der Belegung der ersten beiden Plätze haben wir für den 3. Platz $n - 2$ Läufer Auswahl, usw. Für den letzten Platz haben wir schliesslich einen Läufer zur Auswahl. Gemäss der Multiplikationsregel erhalten wir so:

$$P_n = n!$$

Nachfolgend noch einige Bemerkungen zu den Fakultäten. Aus praktischen Gründen vereinbart man:

$$0! = 1$$

Es gibt verschiedene Begründungen hierfür. Will man beispielsweise die rekursive Definition der Fakultät

$$n! = n \cdot (n - 1)!$$

bei 0 verankern, dann muss man $0!$ als 1 definieren. Man kann auch sagen, dass es genau 1 Möglichkeit gibt, um null Objekte anzuordnen, nämlich die leere Anordnung.

Die folgende Tabelle enthält die Fakultäten der Zahlen 0, 1, \dots , 19. Man stellt fest, dass $n!$ *sehr schnell* wächst.

0 ! = 1	10 ! = 3'628'800
1 ! = 1	11 ! = 39'916'800
2 ! = 2	12 ! = 479'001'600
3 ! = 6	13 ! = 6'227'020'800
4 ! = 24	14 ! = 87'178'291'200
5 ! = 120	15 ! = 1'307'674'368'000
6 ! = 720	16 ! = 20'922'789'888'000
7 ! = 5'040	17 ! = 355'687'428'096'000
8 ! = 40'320	18 ! = 6'402'373'705'728'000
9 ! = 362'880	19 ! = 121'645'100'408'832'000

Von $n = 10$ an, bewegt sich $n!$ in den Millionen. Zur Berechnung von Näherungswerten für grosse n ist die folgende Formel von grossem Nutzen („Formel von Stirling¹“)

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

Sie zeigt, dass die Fakultät exponentiell wächst. Wir werden diese Formel nicht beweisen.

Beispiel 10 Bestimmen Sie die Summe aus allen vierstelligen Zahlen, mit den Ziffern 1, 3, 5 und 7, wenn in einer Zahl alle Ziffern verschieden sein sollen.

Die Aufgabe wird im Unterricht gelöst. ◇

Beispiel 11 Wie viele Möglichkeiten gibt es 8 Türme auf einem Schachbrett zu platzieren, so dass sie sich nicht bedrohen?

Die Aufgabe wird im Unterricht gelöst. ◇

1.3 Variationen ohne Wiederholung

Beispiel 12 Wir betrachten wiederum das Problem der 5 Läufer. Diesmal interessieren wir uns aber bloss für die Klassierung der ersten 3 Läufer. Wie viele verschiedene Ranglisten gibt es?

Lösung: Wir schreiben alle Möglichkeiten auf:

<i>ABC</i>	<i>BAC</i>	<i>CAB</i>	<i>DAB</i>	<i>EAB</i>
<i>ABD</i>	<i>BAD</i>	<i>CAD</i>	<i>DAC</i>	<i>EAC</i>
<i>ABE</i>	<i>BAE</i>	<i>CAE</i>	<i>DAE</i>	<i>EAD</i>
<i>ACB</i>	<i>BCA</i>	<i>CBA</i>	<i>DBA</i>	<i>EBA</i>
<i>ACD</i>	<i>BCD</i>	<i>CBD</i>	<i>DBC</i>	<i>EBC</i>
<i>ACE</i>	<i>BCE</i>	<i>CBE</i>	<i>DBE</i>	<i>EBD</i>
<i>ADB</i>	<i>BDA</i>	<i>CDA</i>	<i>DCA</i>	<i>ECA</i>
<i>ADC</i>	<i>BDC</i>	<i>CDB</i>	<i>DCB</i>	<i>ECB</i>
<i>ADE</i>	<i>BDE</i>	<i>CDE</i>	<i>DCE</i>	<i>ECD</i>
<i>AEB</i>	<i>BEA</i>	<i>CEA</i>	<i>DEA</i>	<i>EDA</i>
<i>AEC</i>	<i>BEC</i>	<i>CEB</i>	<i>DEB</i>	<i>EDB</i>
<i>AED</i>	<i>BED</i>	<i>CED</i>	<i>DEC</i>	<i>EDC</i>

Es gibt also 60 verschiedene Ranglisten. ◇

Beispiel 13 Lösen Sie das obige Problem durch Überlegung.

Die Aufgabe wird im Unterricht gelöst. ◇

Falls n Läufer ein Rennen bestreiten und wir uns für die Klassierung der ersten k ($1 \leq k \leq n$) Läufer interessieren, so ist die Zahl der verschiedenen Ranglisten gleich

$$V_n^k := n \cdot (n-1) \cdot (n-2) \cdots (n-k+2) \cdot (n-k+1)$$

¹James Stirling (1692-1770): schottischer Mathematiker

V_n^k ist die Anzahl der möglichen *geordneten* Folgen bestehend aus k verschiedene Objekten, die aus einem Vorrat von n Objekten gebildet werden können. Jede solche geordnete Folge heisst eine **Variation ohne Wiederholung**.

Mit Hilfe der Fakultäten erhalten wir die folgende Formel:

$$V_n^k := \frac{n!}{(n-k)!} .$$

Beispiel 14 Wie viele Zahlen n ($1000 \leq n \leq 9999$) besitzen 4 verschiedene Ziffern in ihrer Dezimaldarstellung?

Die Aufgabe wird im Unterricht gelöst. ◇

Beispiel 15 Die Post will eine neue Briefmarkenserie mit 4 verschiedenen Werten herausbringen. Die Druckerei bietet 8 verschiedene Farben an. Wie viele mögliche Serien gibt es, falls jeder Wert eine andere Farbe besitzen soll?

Die Aufgabe wird im Unterricht gelöst. ◇

1.4 Kombinationen

Beispiel 16 Wir betrachten wiederum das Beispiel der 5 Läufer. Diesmal interessieren wir uns nur für die 3 Medaillengewinner. Wie viele mögliche Gruppen von Medaillengewinnern gibt es (die Reihenfolge innerhalb der ersten 3 interessiert uns nicht mehr)?

Lösung: Im Beispiel 12 hatten wir $5 \cdot 4 \cdot 3 = 60$ Möglichkeiten für die ersten 3 Ränge aus den 5 Athleten berechnet. Darunter waren z.B. die Anordnungen:

$$ABC \ ACB \ BAC \ BCA \ CAB \ CBA \ . \quad (1)$$

Im jetzigen Problem, wo es nicht mehr auf die Reihenfolge ankommt, zählen diese 6 Anordnungen nur noch als eine einzige Möglichkeit, nämlich

$$A, B, C \text{ sind die Medaillengewinner.}$$

Die Zeile (1) enthält die $3! = 6$ Permutationen der 3 Elemente A, B und C .

Wir können diese Überlegung für jede Dreiergruppe von Athleten (z.B. A, B, D oder C, D, E usw.) wiederholen und stellen jedesmal fest, dass aus $3! = 6$ Anordnungen eine einzige Möglichkeit wird.

Wir finden also die Antwort auf unsere Frage, indem wir die 60 Möglichkeiten des Beispiels 12 durch 6 dividieren:

Es gibt also $60:6=10$ Möglichkeiten, aus den 5 Läufern eine Dreiergruppe auszuwählen. ◇

Das Problem kann auch auf eine andere Art interpretiert werden. Gegeben ist eine Menge bestehend aus 5 Elementen (den Läufern) $\{A, B, C, D, E\}$. Wir wollen Teilmengen mit 3 Elementen (Medaillengewinner) auswählen. Unsere Überlegung hat gezeigt, dass es 10 solcher Teilmengen gibt:

$$\begin{array}{cccccc} \{A, B, C\} & \{A, B, D\} & \{A, B, E\} & \{A, C, D\} & \{A, C, E\} \\ \{A, D, E\} & \{B, C, D\} & \{B, C, E\} & \{B, D, E\} & \{C, D, E\} \end{array}$$

In dieser Formulierung ist es automatisch klar, dass die Reihenfolge keine Rolle spielt, denn 2 Mengen sind gleich, wenn sie die gleichen Elemente enthalten.

Falls eine Menge bestehend aus n ($n \in \mathbb{N}$) Elementen gegeben ist, ist die Anzahl der Teilmengen bestehend aus k ($0 \leq k \leq n$) Elementen gegeben durch

$$\binom{n}{k} := \frac{n(n-1)(n-2) \cdots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Der Ausdruck $\binom{n}{k}$ heisst **Binomialkoeffizient** und wird „ n tief k “ gelesen.

$\binom{n}{k}$ gibt die Anzahl der Möglichkeiten an, mit der aus n Objekten ohne Berücksichtigung der Reihenfolge k Objekte herausgegriffen werden können. Jede solche Gruppe von k Objekten heisst eine **Kombination**.

Beispiel 17 Sei $n \in \mathbb{N}$ und seien $a, b \in \mathbb{R}$. Der binomische Lehrsatz lautet:

$$\begin{aligned} (a+b)^n &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}a^1b^{n-1} + \binom{n}{n}b^n \\ &= \sum_{k=0}^n \binom{n}{k}a^{n-k}b^k \end{aligned}$$

Geben Sie einen kombinatorischen Beweis dieses Satzes.

Die Aufgabe wird im Unterricht gelöst. ◇

Die Überlegungen, die wir beim Beweis des vorhergehenden Satzes angestellt haben, lassen sich auf Trinome oder noch kompliziertere Ausdrücke anwenden:

Beispiel 18 Gegeben ist der Ausdruck:

$$(a - 2b + c)^{10}$$

Bestimmen Sie den Koeffizienten von:

(a) $a^2b^4c^4$

(b) a^5b^5

Die Aufgabe wird im Unterricht gelöst. ◇

1.5 Permutationen mit Wiederholung

Wir wollen die Anzahl aller Wörter mit 5 Buchstaben bestimmen, die man mit den Buchstaben des Wortes DADDY bilden kann. Es gibt $5! = 120$ Permutationen der Objekte $D_1AD_2D_3Y$, wobei die drei D's unterschieden werden. Zu beachten ist, dass die folgenden sechs Permutationen

$$D_1D_2D_3AY, D_2D_1D_3AY, D_3D_1D_2AY, D_1D_3D_2AY, D_2D_3D_1AY, D_3D_2D_1AY$$

dasselbe Wort ergeben, wenn wir die Indizes weglassen. Die 6 ergibt sich aus der Tatsache, dass es $3! = 3 \cdot 2 \cdot 1$ verschiedene Möglichkeiten gibt, die drei D's an die ersten drei Stellen zu schreiben. Das ist für jede der anderen möglichen Stellen, an die die D's geschrieben werden können, der Fall. Also können

$$\frac{5!}{3!} = \frac{120}{6} = 20$$

verschiedene Wörter mit 5 Buchstaben aus den Buchstaben des Wortes DADDY gebildet werden.

Beispiel 19 Wie viele verschiedene Wörter mit 7 Buchstaben lassen sich aus den Buchstaben des Wortes ANTENNE bilden.

Die Aufgabe wird im Unterricht gelöst. \diamond

Beispiel 20 Wir betrachten die Gleichung

$$x_1 + x_2 + x_3 + x_4 = 15$$

wobei $x_i \in \mathbb{N} \cup \{0\}$. Wie viele Lösungen gibt es?

Die Aufgabe wird im Unterricht gelöst. \diamond

Der folgende Satz drückt die allgemeine Situation aus

Satz 1 Die Anzahl Permutationen von n Objekten, von denen je n_1 , je n_2 , ... und je n_r gleich sind, ist

$$\frac{n!}{n_1! n_2! \cdots n_r!}$$

1.6 Variationen mit Wiederholung

Beim TOTOGOal müssen die Ausgänge von 13 Spielen vorausgesagt werden. Es gibt die 3 möglichen Ausgänge 1, 2 oder x, je nachdem, ob die Heimmannschaft oder die Gastmannschaft gewonnen hat, oder ob unentschieden gespielt wurde:

FC Thun	:	FC Lugano	1
FC Vaduz	:	Young Boys	2
FC Sion	:	FC St. Gallen	1
FC Luzern	:	FC Zürich	1
Grasshoppers	:	FC Basel	x
VfB Stuttgart	:	Hertha BSC	1
VfL Wolfsburg	:	FC Ingolstadt	x
Hamburger SV	:	Mönchengladbach	1
Juventus	:	SSC Napoli	2
AC Milan	:	Genoa CFC	x
AC Fiorentina	:	Inter Milano	2
Bournemouth AFC	:	Stoke City	x
Chelsea FC	:	Newcastle United	x

Wir wollen die Zahl der möglichen Tipps bestimmen. Für die erste Paarung gibt es 3 Möglichkeiten und ebenso für jede weitere Paarung. Es gibt also

$$\underbrace{3 \cdot 3 \cdots 3}_{13 \text{ fois}} = 3^{13} = 1'594'323$$

mögliche Tipps.

Beispiel 21 Bestimmen Sie die Summe aller vierstelligen Zahlen, die sich aus den Ziffern 3, 5, 8 bilden lassen.

Die Aufgabe wird im Unterricht gelöst. \diamond

Beispiel 22 Wie viele Telefonnummern gibt es in denen die Ziffer 1 mindestens zweimal vorkommt?

Die Aufgabe wird im Unterricht gelöst. \diamond

1.7 Kombinationen mit Wiederholungen

Der Binomialkoeffizient $\binom{n}{k}$ ist gleich der Anzahl der Kombinationen, die gebildet werden können, wenn k Objekte aus n *verschiedenen* Objekten ausgewählt werden. Angenommen es gäbe von jedem Objekt verschiedene identische Kopien. Beispielsweise können wir an eine Buchhandlung denken, wo es zu einem Buch mehrere gleiche Exemplare gibt. Wir können dann das folgende Problem studieren: Gegeben seien n Kategorien von Objekten, wobei jede Kategorie einen beliebigen Vorrat an identischen Objekten enthält. Auf wie viele Arten können wir k Objekte auswählen, wenn die Reihenfolge keine Rolle spielt und mehrere Objekte aus der gleichen Kategorie ausgewählt werden können? Man nennt eine solche Auswahl eine **Kombination mit Wiederholung**.

Die Anzahl Kombinationen mit Wiederholung von k Elementen aus n Kategorien ist gleich der Anzahl von nicht-negativen, ganzzahligen Lösungen der Gleichung

$$x_1 + x_2 + x_3 + \cdots + x_n = k. \quad (2)$$

Hier ist der Wert von x_1 gleich der Anzahl Elemente, die wir aus der ersten Kategorie auswählen, der Wert von x_2 gleich der Anzahl Elemente, die wir aus der zweiten Kategorie auswählen, usw.

Um eine Formel für die Anzahl dieser Lösungen zu finden, betrachten wir ein konkretes Beispiel mit $n = 4$ und $k = 10$. Die Gleichung (2) lautet in diesem Fall

$$x_1 + x_2 + x_3 + x_4 = 10. \quad (3)$$

Die Lösung $x_1 = 4, x_2 = 0, x_3 = 5, x_4 = 1$ können wir folgendermassen codieren

$$1111|11111|1.$$

Hier spielt $|$ die Rolle eines Separators. Die Anzahl Zeichen 1 vor dem ersten Strich entspricht dem Wert von x_1 , die Anzahl Zeichen 1 zwischen dem ersten und dem zweiten Strich entspricht dem Wert von x_2 , usw. Wie man sich leicht überlegt, ist die Anzahl der Lösungen von (3) gleich der Anzahl Permutationen mit Wiederholung, die mit den 10 Zeichen 1 und 3 Zeichen $|$ gebildet werden können. Diese Zahl ist gegeben durch

$$\frac{(10+3)!}{3!10!} = \frac{13!}{3!10!} = \binom{13}{3}.$$

Im allgemeinen Fall der Gleichung (2) müssen wir $n-1$ Separatoren $|$ setzen. Die Anzahl Lösungen ist gleich der Zahl der Permutationen mit Wiederholungen von k Zeichen 1 und $n-1$ Zeichen $|$:

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

Beispiel 23 Wir werfen 5 nicht unterscheidbare Würfel. Wie viele verschiedene Wurfbilder gibt es?

Die Aufgabe wird im Unterricht gelöst. \diamond

1.8 Die Ein- und Ausschlussformel

In der Mengenlehre haben wir für 3 endliche Mengen A , B und C die folgende Formel bewiesen

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \quad (4)$$

Hier bezeichnet $|M|$ die **Anzahl Elemente** der Menge M .

Die analoge Formel für 4 Mengen A , B , C und D lautet:

$$\begin{aligned} |A \cup B \cup C \cup D| &= |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| \\ &\quad - |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| \\ &\quad + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D| \end{aligned}$$

Es ist klar, wie die Formel auf 5 oder mehr Mengen verallgemeinert werden kann. Man bezeichnet diese Formeln als **Ein- und Ausschlussformeln**.

Wir betrachten eine Anwendung der Formel (4) in der Kombinatorik:

Beispiel 24 Wie viele Zahlen zwischen 1 und 6300 (inklusive) sind weder durch 3, 5 noch 7 teilbar?

Lösung: Wir definieren die folgenden Mengen

- U : Menge der Zahlen zwischen 1 und 6300
- A : Menge der Zahlen zwischen 1 und 6300, die durch 3 teilbar sind
- B : Menge der Zahlen zwischen 1 und 6300, die durch 5 teilbar sind
- C : Menge der Zahlen zwischen 1 und 6300, die durch 7 teilbar sind

Gesucht ist also $|U| - |A \cup B \cup C| = 6300 - |A \cup B \cup C|$. Nach der Formel (4) gilt:

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cap C| \\ &= 2100 + 1260 + 900 - 420 - 300 - 180 + 60 = 3420. \end{aligned}$$

Also ist die gesuchte Anzahl gleich $6300 - 3420 = 2880$. ◇

Allgemein kann dieses Resultat folgendermassen formuliert werden: Gegeben sei eine endliche Menge U . Die Teilmenge A enthalte alle Elemente, die eine gewisse Eigenschaft x besitzen, die Teilmenge B enthalte alle Elemente, die eine gewisse Eigenschaft y besitzen und die Teilmenge C enthalte alle Elemente, die eine gewisse Eigenschaft z besitzen. Die Anzahl Elemente N in U , die *keine* der drei Eigenschaften besitzen, ist dann gegeben durch

$$N = |U| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|$$

Das nachfolgende Problem gibt es in diversen Einkleidungen.

Beispiel 25 Gegeben seien 4 Briefe und 4 Umschläge. Auf wie viele Arten können die 4 Briefe in die Umschläge gesteckt werden, so dass sich jeder Brief in einem falschen Umschlag befindet?

Die Aufgabe wird im Unterricht gelöst. ◇

Zum ersten Mal wurde ein analoges Problem vom französischen Mathematiker Pierre Rémond de Montmort² analysiert. Er interessierte sich für die Gewinnchancen beim Spiel *Treize*: ein Spieler mischt 13 Karten einer Farbe und legt den Stapel vor sich hin. Er ruft dann die Karten gemäss der Reihenfolge As, Zwei, Drei, . . . , König auf und nimmt jeweils eine Karte vom Stapel. Er gewinnt das Spiel, wenn die aufgedeckte Karte mit der aufgerufenen übereinstimmt.

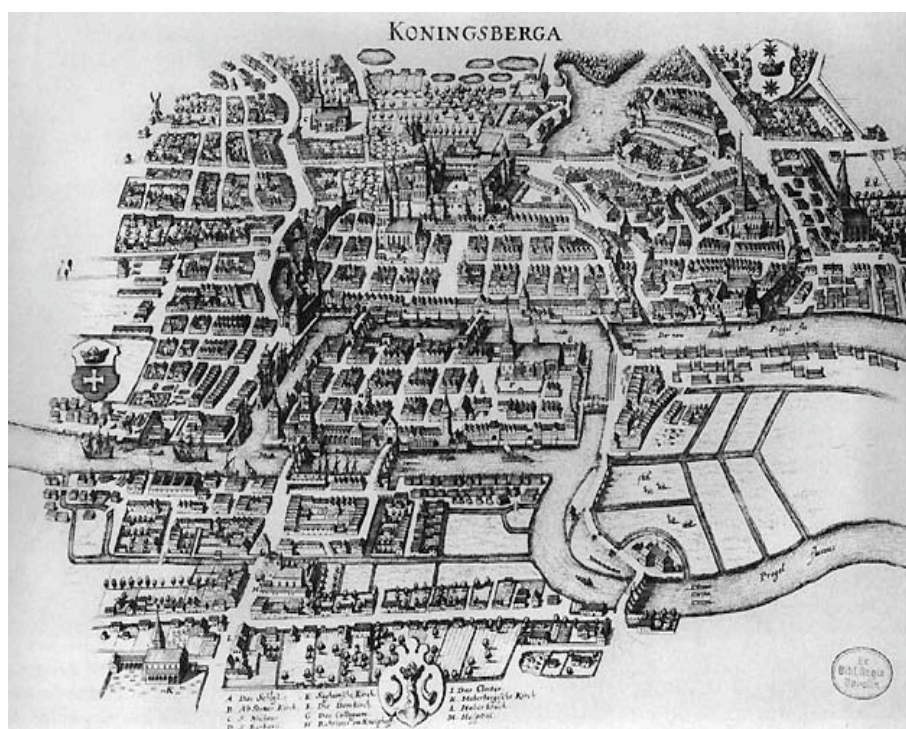
Wir können das obige Problem noch unter einem andern Gesichtspunkt beleuchten. Eine Permutation von n Elementen ist eine Bijektion f der Menge $A = \{1, 2, 3, \dots, n\}$ auf sich. Das Element $i \in A$ heisst **Fixpunkt** von f , wenn $f(i) = i$ ist. Die Anzahl der Permutationen mit Fixpunkt ist gleich der Anzahl der Permutationen minus der Anzahl der **fixpunktfreien** Permutationen. Im Beispiel 25 haben wir die Anzahl der fixpunktfreien Permutationen auf der Menge $\{1, 2, 3, 4\}$ bestimmt.

²Pierre Rémond de Montmort: (1678 Paris - 1719 ebenda): französischer Mathematiker

2 Graphentheorie

2.1 Das Königsberger Brückenproblem

Die Geburtsstunde der Graphentheorie schlug mit der Lösung des folgenden Problems. Die Stadt Königsberg³ wird vom Fluss Pregel durchflossen. Dieser umfließt zwei Inseln. Die nachfolgende Figur zeigt Königsberg im 18. Jahrhundert. In jener Zeit stellten sich die Einwohner die Frage, ob es möglich sei, einen Spaziergang zu machen, so dass jede der 7 Brücken *genau einmal* überschritten wird und man wieder zum Ausgangspunkt zurückkehrt.

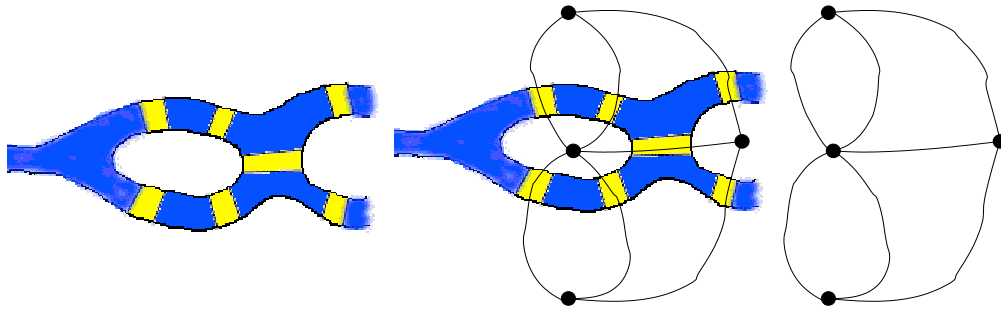


Ansicht von Königsberg. Die Insel in der Mitte heisst Kneiphof. Der Pregel fliesst von rechts nach links.

Leonard Euler⁴, der zu jener Zeit in St. Petersburg arbeitete, hörte von diesem Problem. Im Jahre 1736 publizierte er einen Artikel mit dem Titel *Solutio problematis ad geometriam situs pertinentis* (Die Lösung eines Problems der Positionsgeometrie). Euler ersetzte die Quartiere durch Punkte und die Spazierwege über die Brücken als gerade oder gebogene Kanten. Er erhielt so eine Figur, die wir heute als **Graphen** bezeichnen.

³ Königsberg war bis 1945 Hauptstadt der Provinz Ostpreussen, die zu Deutschland gehörte. Nach dem Ende des Zweiten Weltkriegs vereinbarten die Siegermächte an der Konferenz von Potsdam, dass Königsberg - oder was davon noch übrigblieb - zusammen mit dem nördlichen Teil Ostpreussens Teil der Sowjetunion wird. Die Stadt wurde 1946 in Kaliningrad umbenannt und ist heute Hauptstadt des Kaliningrader Gebiets, einer russischen Exklave.

⁴Leonard Euler (geb. 1707 in Basel - gest. 1783 in St. Petersburg): Leonard Euler ist einer der grössten Mathematiker aller Zeiten.



Die Punkte eines Graphen werden als **Knoten** und die Verbindungslinien als **Kanten** bezeichnet. Unter dem **Grad** eines Knoten verstehen wir die Anzahl Kanten, welche von diesem Punkt weggehen. Euler zeigte, dass ein solcher Rundgang nur möglich ist, wenn jeder Knoten einen geraden Grad hat. Jedesmal, wenn man nämlich über eine Kante zu einem Knoten gelangt, muss man auf einer andern Kante wieder von diesem Knoten wegkommen. Im obigen Graphen haben aber alle Knoten ungeraden Grad.

Es gibt auch keinen Spaziergang mit verschiedenem Anfangs- und Endpunkt, wo jede Brücke einmal überschritten wird. Anfangs- und Endknoten müssten dann ungeraden Grad und alle übrigen Knoten einen geraden Grad besitzen.

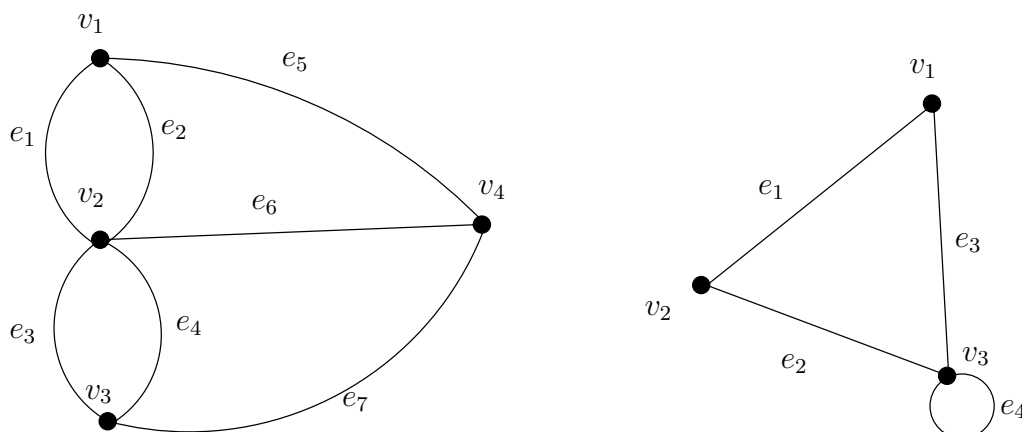
Der Titel von Eulers Arbeit zeigt, dass sich Euler durchaus bewusst war, dass er ein Problem löste, das nicht zur üblichen Geometrie gehört. Bei diesem Problem spielen nämlich die genauen Abstände keine Rolle.

2.2 Definition eines Graphen

Wir definieren jetzt, was wir unter einem Graphen verstehen.

Definition 1 Ein Graph ist ein geordnetes Quadrupel (V, E, g_1, g_2) , wobei gilt:

- V ist eine nichtleere endliche Menge von Knoten (vertices).
- E ist eine endliche Menge von Kanten (edges).
- $g_1, g_2 : E \rightarrow V$ sind Abbildungen, die jeder Kante die Endpunkte zuordnen.



Beispiel 26 Bestimmen Sie für die beiden oben abgebildeten Graphen V , E , g_1 und g_2 .

Die Aufgabe wird im Unterricht gelöst. ◇

Im Graphen auf der linken Seite verbinden e_1 und e_2 sowie e_3 und e_4 die gleichen Knoten. Man spricht von **Mehrfachkanten**. Im Graphen auf der rechten Seite verbindet die Kante e_4 den Knoten v_3 mit sich selbst. Man spricht von einem **Loop** oder einer **Schleife**.

Graphen ohne Mehrfachkanten und ohne Loops heissen **einfach**. Wir werden nachher meistens einfache Graphen betrachten. Die direkte Definition eines einfachen Graphen lautet:

Definition 2 Ein **einfacher Graph** besteht aus einer endlichen, nichtleeren Menge V , deren Elemente **Knoten** heissen, und einer Menge E von 2-elementigen Teilmengen von V , den **Kanten**. Wir schreiben $G = (V, E)$, wobei V die Knotenmenge und E die Kantenmenge ist.

Beispiel 27 Erstellen Sie eine Figur des folgenden Graphen:

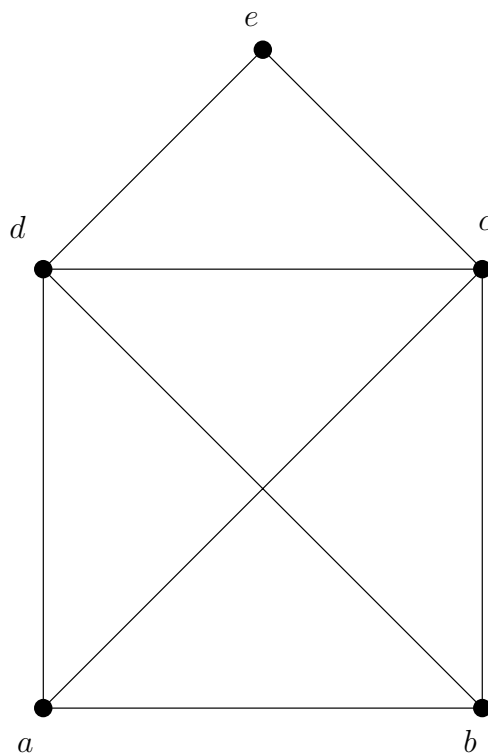
$$V = \{a, b, c, d, e\} \quad \text{und} \quad E = \{\{a, b\}, \{a, d\}, \{b, e\}, \{c, d\}, \{d, e\}\}$$

Die Aufgabe wird im Unterricht gelöst. \diamond

Beispiel 28 Professor McBrain und seine Frau April geben eine Party, zu welcher vier andere verheiratete Paare eingeladen werden. Einige Paare schütteln Hände, wenn sie sich treffen, aber natürlich schütteln die Paare untereinander keine Hände. Am Ende der Party fragt der Professor jede Person wie oft sie Hände geschüttelt hätte und erhält 9 verschiedene Antworten. Wie viele Personen haben mit April Hände geschüttelt?

Die Aufgabe wird im Unterricht gelöst. \diamond

Beispiel 29 Bestimmen Sie die Mengen V und E beim nachfolgenden Graphen.



Die Aufgabe wird im Unterricht gelöst. \diamond

Wir wollen uns jetzt überlegen, wie wir einen Graph im Computer darstellen können. Zu diesem Zweck müssen wir die Knoten nummerieren. Beachten Sie bitte, dass in der Definition eines einfachen Graphen nicht verlangt wird, dass die Menge der Knoten geordnet sein muss. Zum Beispiel kann es sich bei der Menge der Knoten um eine Menge von Buchstaben handeln. Für die Zwecke der Abspeicherung müssen wir aber die Knoten mit natürlichen Zahlen nummerieren. Wenn der Graph beispielsweise 5 Knoten umfasst, dann nummerieren wir die Knoten irgendwie von 1 bis 5. Wir definieren dann die 5×5 -Matrix:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix},$$

wobei gilt:

$$a_{ij} = \begin{cases} 1 & \text{falls eine Kante zwischen den Knoten } i \text{ und } j \text{ existiert} \\ 0 & \text{sonst} \end{cases}$$

Diese binäre Matrix wird als **Adjazenzmatrix** des Graphen bezeichnet.

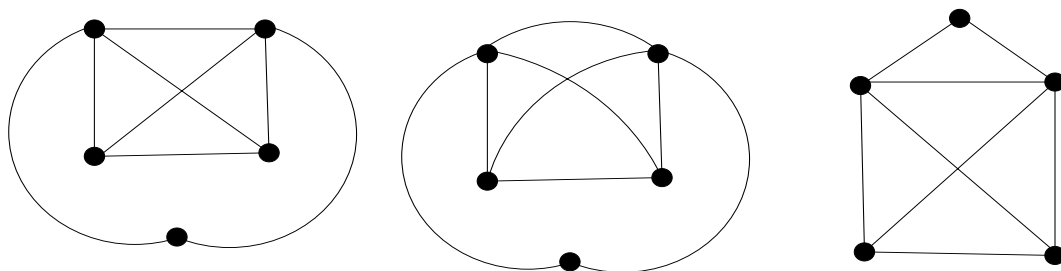
Beispiel 30 Wir nummerieren im vorhergehenden Beispiel die Knoten in alphabetischer Reihenfolge von 1 bis 5. Bestimmen Sie die Adjazenzmatrix.

Die Aufgabe wird im Unterricht gelöst. \diamond

Wir wollen uns jetzt überlegen, wann zwei Graphen als gleich angesehen werden können. Sicher sollte es keine Rolle spielen, wie wir die Ecken bezeichnen. Auch die graphische Darstellung des Graphen kann kein Kriterium sein. Die entscheidende Eigenschaft des Graphen ist die Art wie die Knoten durch Kanten verbunden sind. Die genaue Definition lautet:

Definition 3 Zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ heißen **isomorph**, wenn es eine Bijektion α von V_1 nach V_2 gibt, so dass $\{\alpha(x), \alpha(y)\}$ genau dann eine Kante von G_2 ist, wenn $\{x, y\}$ eine Kante von G_1 ist. Man bezeichnet α als einen **Isomorphismus**.

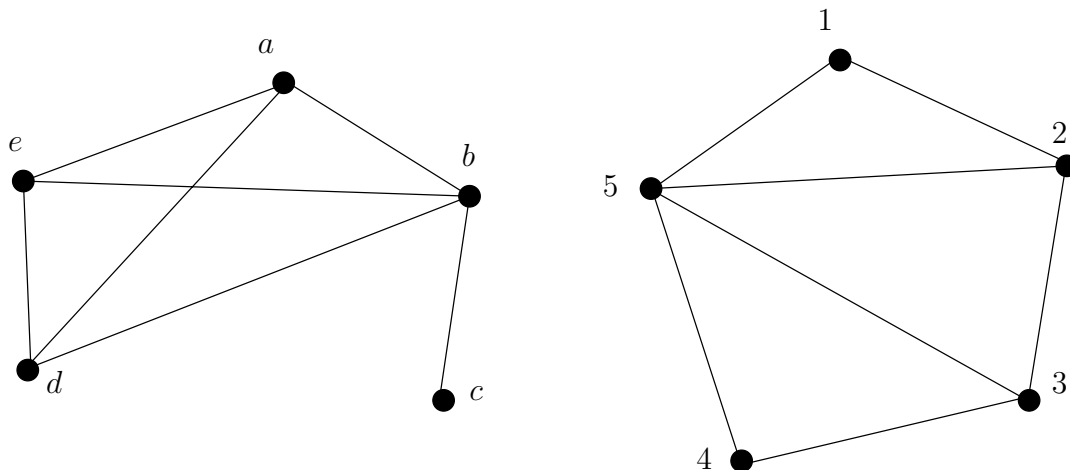
Beispiel 31 Überlegen Sie sich, dass die drei untenstehenden Graphen alle isomorph zueinander sind.



Die Aufgabe wird im Unterricht gelöst. \diamond

Es ist klar, dass zwei Graphen nur isomorph sein können, wenn sie die gleiche Anzahl von Knoten und Kanten besitzen. Diese Bedingung ist aber nur notwendig und nicht hinreichend.

Beispiel 32 Zeigen Sie, dass die beiden folgenden Graphen nicht isomorph sind.



Die Aufgabe wird im Unterricht gelöst.

◇

2.3 Grad eines Knoten

Unter dem **Grad** eines Knoten v in einem Graphen $G = (V, E)$ verstehen wir die Anzahl der Kanten, welche von diesem Knoten ausgehen. Wir verwenden die Notation $\delta(v)$.

Eine Schleife in einem nicht-einfachen Graphen trägt zwei Mal zum Grad eines Knotens bei. Ein isolierter Knoten hat den Grad 0.

Es gilt das folgende Resultat:

Lemma 1 (Handshaking Lemma) In einem Graphen $G = (V, E)$ ist die Summe aller Grade gleich der doppelten Anzahl der Kanten:

$$\sum_{v \in V} \delta(v) = 2|E| \quad (5)$$

Dieses Resultat gilt auch für Graphen mit Schleifen und Mehrfachkanten.

Beweis: Jede Kante hat einen Anfangs- und Endpunkt und wird also in der obigen Summe zweimal gezählt.

Wir betrachten eine Folgerung aus (5). Wir bezeichnen mit V_o („o“ für „odd“) die Knoten mit ungeradem Grad und mit V_e („e“ für „even“) die Knoten mit geradem Grad. Natürlich gilt dann:

$$\sum_{v \in V_o} \delta(v) + \sum_{v \in V_e} \delta(v) = 2|E|$$

Jeder Summand der zweiten Summe ist gerade und damit auch die zweite Summe. Da die rechte Seite gerade ist, muss auch die erste Summe gerade sein. Eine Summe von

ungeraden Zahlen kann aber nur gerade sein, wenn wir es mit einer geraden Anzahl zu tun haben. Es gilt also:

In einem einfachen Graphen ist die Anzahl der Knoten mit ungeradem Grad gerade.

Es gibt eine interessante Interpretation von dieser Aussage: Wir betrachten eine Menge von Personen, die sich teilweise die Hand schütteln. Dann ist die Teilmenge der Personen, welche mit einer ungeraden Anzahl Personen die Hand schüttelt, gerade.

Eine wichtige Anwendung des Begriffs des Grads besteht darin zu entscheiden, ob zwei Graphen isomorph sind oder nicht. Falls $\alpha : V_1 \rightarrow V_2$ ein Isomorphismus zwischen zwei Graphen G_1 und G_2 ist, und falls $\alpha(v) = w$ ist, dann führt α jede Kante, die v enthält, in eine Kante über, die w enthält. Umgekehrt führt α^{-1} jede Kante, die w enthält, in eine Kante, welche v enthält, über. Es gilt also:

$$\delta(v) = \delta(w)$$

Falls andererseits G_1 einen Knoten mit Grad δ_0 enthält, G_2 aber keinen Knoten mit Grad δ_0 besitzt, dann können G_1 und G_2 nicht isomorph sein.

2.4 Wege, Pfade und Zyklen

Ein Knoten w heisst **Nachbar** eines Knoten v , wenn es eine Kante gibt, welche v und w verbindet.

Man versteht unter einem **Weg** in einem Graphen G eine Folge von Knoten,

$$v_1, v_2, \dots, v_n,$$

so dass v_i und v_{i+1} ($1 \leq i \leq n-1$) Nachbarn sind. Falls alle Knoten in einem Weg paarweise verschieden sind, spricht man von einem **Pfad**. In einem Weg kann der gleiche Knoten also mehrmals besucht werden, nicht aber in einem Pfad.

Wir betrachten einen (endlichen) Graphen, der nicht unbedingt einfach sein muss. Mehrfachkanten oder Schlingen sind also zugelassen. Unter einem **Zyklus** versteht man eine Folge von Knoten

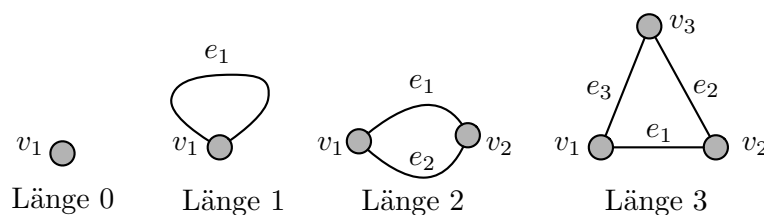
$$v_1, v_2, v_3, \dots, v_n, v_1$$

und Kanten

$$e_1 = v_1v_2, e_2 = v_2v_3, e_3 = v_3v_4, \dots, e_n = v_nv_1,$$

wobei mit Ausnahme des Anfangs- und Endknoten alle Knoten sowie alle Kanten **von-einander verschieden sind**. Die **Länge** des Zyklus ist gleich der Anzahl seiner Kanten. Wir betrachten noch die folgenden Spezialfälle:

- Ein einzelner Knoten ist ein Zyklus der Länge 0.
- Ein Knoten mit einer Schleife bildet einen Zyklus der Länge 1.

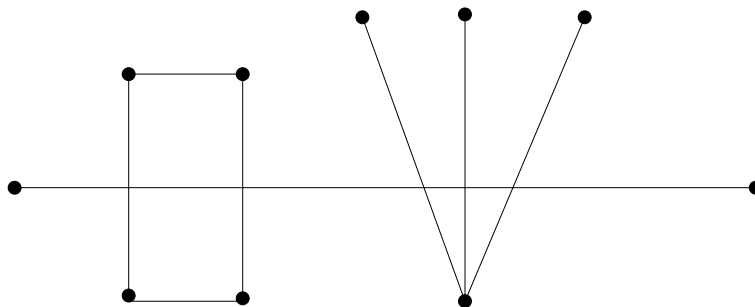


Sei $G = (V, E)$ ein Graph und x, y zwei Knoten. Wir schreiben $x \sim y$, wenn es einen Weg von x nach y gibt. Offensichtlich ist \sim eine Äquivalenzrelation auf der Menge der Knoten V von G (überprüfen Sie dies!). Die Äquivalenzklassen V_1, V_2, \dots, V_r bilden eine Partition von V :

$$V = V_1 \cup V_2 \cup \dots \cup V_r$$

Sei E_i ($1 \leq i \leq r$) die Teilmenge von E , welche die Kanten der Knoten in V_i umfasst. Wir nennen dann die Graphen $G_i = (V_i, E_i)$ die **Komponenten** von G . Falls G nur eine Komponente besitzt, dann nennt man G **zusammenhängend**.

Beispiel 33 Bestimmen Sie die Anzahl der Zusammenhangskomponenten des folgenden Graphen:



Die Aufgabe wird im Unterricht gelöst. ◇

Der folgende Satz liefert eine interessante Interpretation für die Potenzen der Adjazenzmatrix A eines Graphen:

Satz 2 Sei G ein Graph mit den Knoten v_1, v_2, \dots, v_n und sei A die zugehörige Adjazenzmatrix. Dann ist für jede natürliche Zahl m das Matrixelement (i, j) von A^m gleich der Anzahl der Wege der Länge m vom Knoten v_i zum Knoten v_j .

Beweis durch Induktion nach m :

Verankerung: $m = 1$

Die Behauptung ist nach Definition der Adjazenzmatrix offensichtlich richtig.

Induktionsvoraussetzung: Die Behauptung sei richtig für ein $m \in \mathbb{N}$.

Vererbung: Wir müssen beweisen, dass die Aussage auch für den Nachfolger $m + 1$ richtig ist. Es gilt:

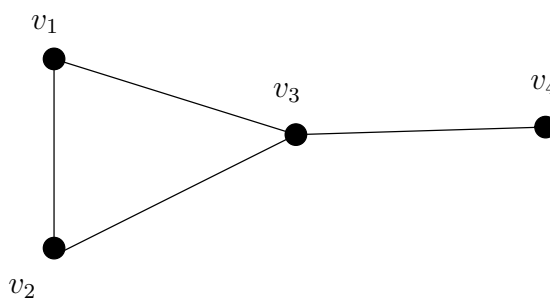
$$A^{m+1} = A \cdot A^m$$

Für das Element (i, j) der Matrix A^{m+1} gilt:

$$a_{ij}^{(m+1)} = \sum_{k=1}^n a_{ik} \cdot a_{kj}^{(m)} = a_{i1} \cdot a_{1j}^{(m)} + a_{i2} \cdot a_{2j}^{(m)} + \dots + a_{in} \cdot a_{nj}^{(m)}$$

Betrachten wir den ersten Term dieser Summe. Der Faktor a_{i1} gibt an, ob eine Kante von v_i zu v_1 besteht. Der zweite Faktor $a_{1j}^{(m)}$ ist nach Induktionsvoraussetzung gleich der Anzahl der Wege der Länge m von v_1 nach v_j . Das Produkt ist also gleich der Anzahl der Wege der Länge $m + 1$ von v_i nach v_j , deren zweiter Knoten gleich v_1 ist. Analog ist der zweite Term gleich der Anzahl dieser Wege mit zweiten Knoten v_2 etc. Es ist klar, dass die Summe gleich der Anzahl Wege von v_i nach v_j mit Länge $m + 1$ ist. □

Beispiel 34 Wir betrachten den folgenden einfachen Graphen:



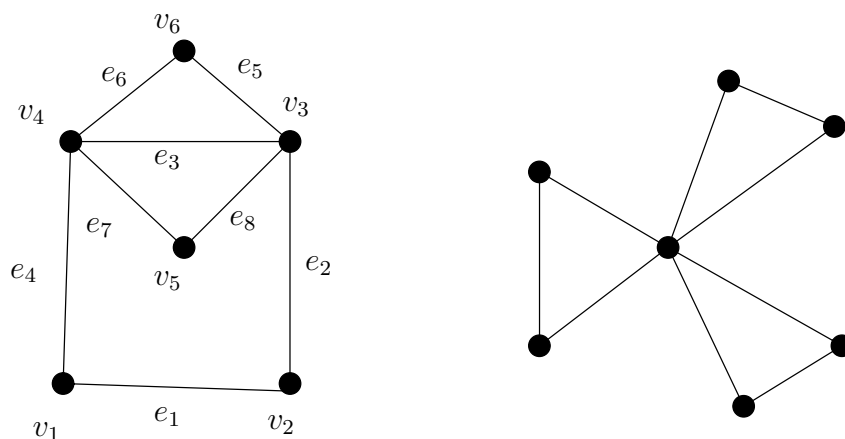
Bestimmen Sie die Anzahl der Wege der Länge 3 vom Knoten i zum Knoten j ($i, j \in \{1, 2, 3, 4\}$).

Die Aufgabe wird im Unterricht gelöst. \diamond

2.5 Eulersche Graphen

In diesem Abschnitt betrachten wir allgemeine Graphen mit Mehrfachkanten und Loops.

Ein zusammenhängender Graph heisst **Eulersch**, wenn es einen geschlossenen Weg gibt, der jede Kante genau einmal enthält. Man bezeichnet einen solchen Weg als **Eulertour**.



Betrachten wir jetzt einen Eulerschen Graphen mit einer Eulertour. Im Graphen auf der linken Seite ist eine Eulertour beispielsweise durch die folgende Folge von Knoten gegeben:

$$v_1, v_4, v_3, v_6, v_4, v_5, v_3, v_2, v_1$$

Jedesmal wenn wir auf einer Kante in einen inneren Knoten gelangen (z.B. v_4), wird er auf einer bisher unbenutzten Kante wieder verlassen. Der Grad erhöht sich also jedesmal um 2. Nur beim Endknoten (=Startknoten) erhöht sich ganz am Schluss der Grad nur um 1. Zusammen mit dem erstmaligen Verlassen des Startknotens ergibt sich aber auch hier eine Erhöhung um 2. Da wir *alle* Kanten benutzen, ergibt sich das folgende Ergebnis:

Satz 3 In einem Eulerschen Graphen ist der Grad jedes Knoten gerade.

Es stellt sich die Frage, ob auch die Umkehrung gilt, das heisst, ob ein Graph Eulersch ist, wenn jeder Knoten einen geraden Grad besitzt. Es ist klar, dass der Graph zusammenhängend sein muss. Aber das reicht aus, damit die Umkehrung gilt.

Satz 4 Falls in einem zusammenhängenden Graphen jeder Knoten einen geraden Grad besitzt, dann ist er Eulersch.

Wir benötigen das folgende Lemma um diesen Satz beweisen zu können:

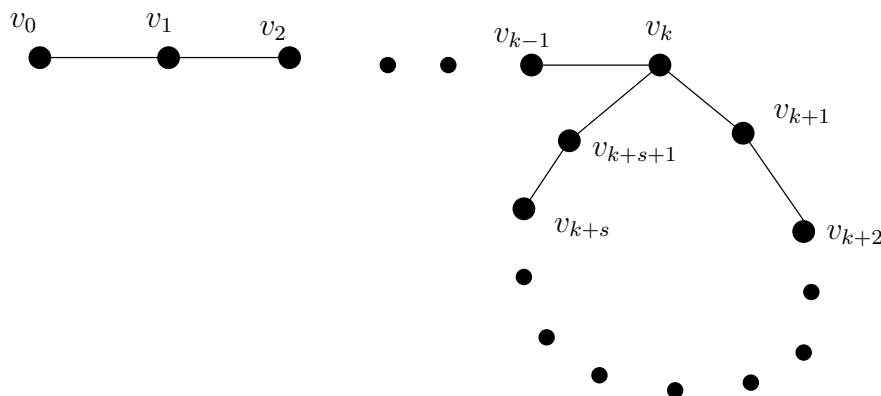
Lemma 2 Es sei G ein Graph, in dem der Grad jedes Knotens mindestens zwei beträgt. Dann enthält G einen Zyklus mit positiver Länge.

Bew.: Wenn G kein einfacher Graph ist, dann enthält er eine Schlaufe oder eine Doppelkante. In beiden Fällen gibt es einen Zyklus.

Sei nun G ein einfacher Graph. Sei v_0 ein beliebiger Knoten von G . Da $\delta(v_0) \geq 2$ ist, gibt es eine Kante e_1 deren einen Endpunkt v_0 ist und deren zweiten Endpunkt wir mit v_1 bezeichnen. Da $\delta(v_1) \geq 2$ ist, gibt es eine Kante $e_2 \neq e_1$ mit den Endpunkten v_1 und v_2 , wobei $v_2 \neq v_0$ ist. Wir wiederholen dieses Verfahren. Im $(i+1)$ -ten Schritt haben wir eine Kante e_i mit den Endpunkten v_i und v_{i+1} , wobei $v_{i+1} \neq v_{i-1}$ ist.



Da G nur endlich viele Knoten enthält, müssen wir einmal einen Knoten wählen, der bereits zuvor einmal durchlaufen wurde. Sei v_k der erste derartige Knoten. Dann ist die Folge der Knoten, die durch den ersten Knoten v_k und den zweiten Knoten v_k begrenzt wird, ein Zyklus. Denn die inneren Knoten dieser Folge sind paarweise verschieden und auch verschieden von v_k , da v_k der erste Knoten ist, der wiederholt wird.



□

Beweis von Satz 4: Wir machen einen Induktionsbeweis über die Anzahl Kanten.

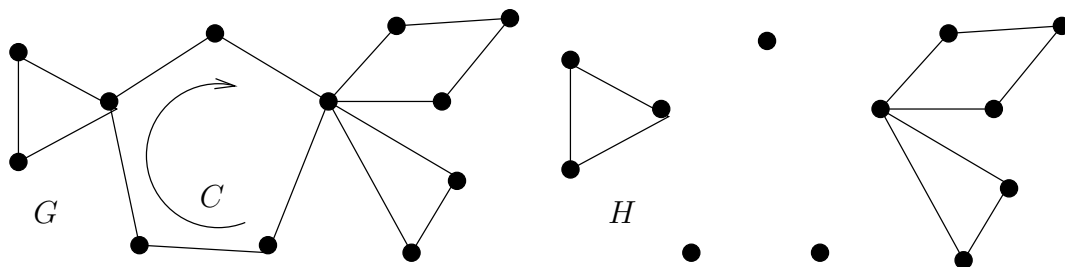
Verankerung: Die Zahl der Kanten sei gleich Null.

Dann besteht der Graph G aus einem einzigen Knoten v_0 , da G zusammenhängend ist. Der triviale Zyklus v_0 enthält dann alle Kanten von G , denn G besitzt überhaupt keine Kanten. Also ist die Behauptung in diesem Fall richtig.

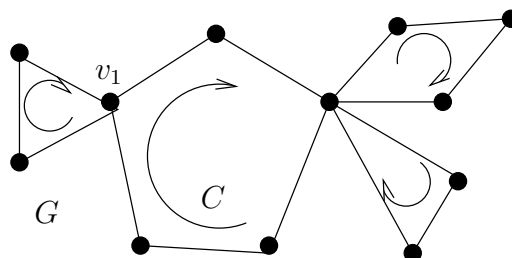
Induktionsvoraussetzung: Sei $n \in \mathbb{N}$ die Anzahl der Kanten. Die Behauptung sei richtig für alle zusammenhängenden Graphen, deren Knoten alle einen geraden Grad haben, und deren Kantenzahl $\leq n$ sei. (starke Induktion)

Vererbung: Wir müssen beweisen, dass die Behauptung richtig ist für alle zusammenhängenden Graphen, deren Knoten einen geraden Grad haben, und deren Kantenzahl gleich $n + 1$ ist.

Sei G ein derartiger Graph. Da der Graph *zusammenhängend* ist, kann kein Knoten den Grad 0 besitzen. Da der Grad jedes Knotens gerade ist, muss jeder Knoten einen Grad ≥ 2 besitzen. Nach dem obigen Lemma existiert dann ein Zyklus C . Wenn C alle Kanten von G enthält, dann sind wir fertig, denn C ist dann eine Eulertour. Wenn C nicht alle Kanten von G enthält, entfernen wir in G jene Kanten, die in C enthalten sind. Wir erhalten so einen Graphen H , der möglicherweise nicht mehr zusammenhängend ist.



Jede dieser Zusammenhangskomponenten hat eine Kantenzahl $\leq n$ und weiter besitzt jeder Knoten einen geraden Grad. Nach Induktionsvoraussetzung besitzt also jede Komponente eine Eulertour. Weiter hat jede dieser Komponenten mindestens einen Knoten mit C gemeinsam. Wir erhalten jetzt folgendermassen eine Eulertour für G . Wir beginnen mit einem beliebigen Knoten von C und gehen die Kanten von C entlang bis wir zu einem Knoten v_1 gelangen, der zu einer Komponente von H gehört. Wir durchlaufen dann eine Eulertour dieser Komponente und gelangen wieder zu v_1 zurück. Wir setzen dann den Weg in C fort bis wir wieder zu einem Knoten gelangen, der zu einer neuen Komponente von H gehört. Wir durchlaufen dann eine Eulertour dieser Komponente. Dieses Verfahren setzen wir fort, bis wir wieder an unserem Startpunkt des Zyklus C angelangt sind. Wir haben auf diese Weise eine Eulertour von G erhalten.



□

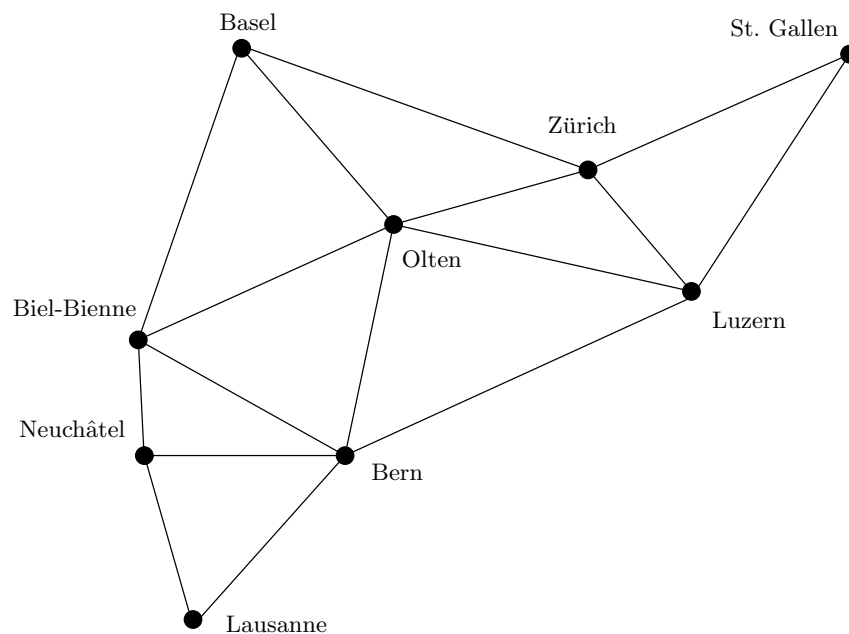
Falls wir einen zusammenhängenden Graphen haben, in welchem zwei Knoten u^* und v^* einen ungeraden Grad und alle übrigen einen geraden Grad besitzen, dann existiert ebenfalls ein Weg, der jede Kante genau einmal enthält. Allerdings ist dieser Weg nicht mehr geschlossen. Sein Anfang und Ende befindet sich in den Knoten mit ungeradem Grad. Die Existenz eines solchen Weges können wir folgendermassen einsehen: wir

verbinden die Knoten mit ungeradem Grad u^* und v^* mit einer Kante e^* und erhalten so einen Eulerschen Graph. Es gibt also eine Tour $C = v_0 e_1 v_1 e_2 \dots e_n v_n$ wo jede Kante genau einmal durchlaufen wird. Wir können annehmen, dass $e_1 = e^*$, $v_0 = u^*$, $v_1 = v^*$ und so $v_n = u^*$ ist. Wenn wir e^* wegnehmen, erhalten wir eine Eulertour von v^* nach u^* .

2.6 Hamiltonsche Graphen

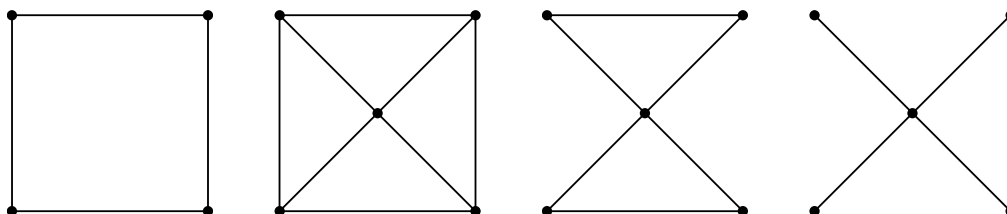
Im vorhergehenden Kapitel wurde untersucht, unter welchen Bedingungen ein geschlossener Weg in einem Graphen existiert, der alle Kanten genau einmal enthält. Jetzt interessieren wir uns dafür einen geschlossenen Weg zu finden, der jeden Knoten genau einmal enthält. Man nennt einen solchen Weg einen **Hamiltonkreis**. Falls in einem Graphen ein Hamiltonkreis existiert, nennt man ihn **Hamiltonisch**⁵.

Beispiel 35 Der untenstehende Graph zeigt einen Ausschnitt des Eisenbahnnetzes der Schweiz. Existiert ein hamiltonscher Kreis?



Die Aufgabe wird im Unterricht gelöst. ◇

Beispiel 36 Bestimmen Sie für jeden der unten abgebildeten Graphen ob er Eulersch und/oder Hamiltonisch ist.



Die Aufgabe wird im Unterricht gelöst. ◇

⁵William Rowan Hamilton (1805-1865): irischer Mathematiker

Im vorhergehenden Kapitel haben wir eine einfache notwendige und hinreichende Bedingung dafür gefunden, dass ein zusammenhängender Graph Eulersch ist. Bis heute konnte keine analoge Charakterisierung für Hamiltonsche Graphen gefunden werden. Man weiss nur, dass wenn ein Graph „genügend“ Kanten hat, dass er dann Hamiltonisch ist. Wir zitieren ohne Beweis den folgenden Satz:

Satz 5 (Dirac, 1952) *Falls G ein einfacher Graph ist mit $n \geq 3$ Knoten und $\delta(v) \geq \frac{1}{2}n$ für jede Ecke v , dann ist G hamiltonisch.*

Es gibt bisher auch keinen effizienten Algorithmus, mit welchem Hamiltonsche Kreise bestimmt werden können. Es gibt natürlich einige einfache Regeln, welche man beachten muss:

- Wenn man einen Knoten passiert hat, können alle nicht benutzten Kanten gestrichen werden.
- Es dürfen keine Knoten mit Grad 1 entstehen.
- Es dürfen keine Untergraphen entstehen, die mit dem übrigen Graphen nicht zusammenhängen.

Beim Problem des Handlungsreisenden (Travelling Salesperson problem TSP) sucht man einen Hamiltonschen Kreis, der eine zusätzliche Bedingung erfüllt. Beispielsweise soll die Anzahl der zurückgelegten Kilometer minimal sein. Oder man gibt eine Kostenfunktion vor, welche für jede Kante, die Kosten für das Passieren angibt, und sucht dann einen hamiltonschen Kreis mit minimalen Kosten.

Ein möglicher Lösungsweg für dieses Problem könnte darin bestehen, dass man alle Hamiltonsche Kreise bestimmt und dann jenen auswählt, für welche die Kosten minimal sind. Wenn wir aber einen Graph mit n Knoten betrachten, in welchem jeder Knoten mit jedem andern verbunden ist, dann ergeben sich $(n - 1)!$ Hamiltonkreise, die von einem bestimmten Knoten starten. Dies ergibt für $n = 30$ die astronomische Zahl:

$$29! = 8'841'761'993'739'701'954'543'616'000'000 \approx 8.84 \cdot 10^{30}$$

Dieser Weg ist also für Graphen mit vielen Knoten und Kanten nicht praktikabel.

Trotz intensivster Forschung fand man bisher keinen effizienten Algorithmus für die Lösung des TSP. Es gibt aber verschiedene Algorithmen, welche zwar nicht die optimale, aber relativ gute Lösungen liefern.

2.7 Bäume

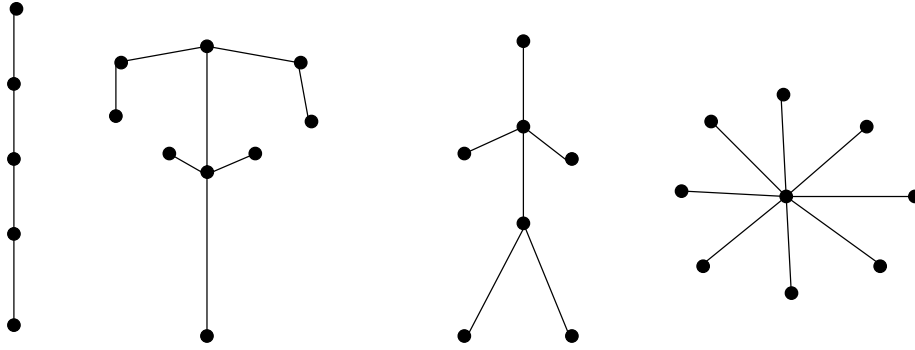
Wir erinnern daran, dass ein Zyklus ein geschlossener Weg mit paarweise verschiedenen Knoten ist.

Definition 4 *Ein Graph T heisst **Baum** (Tree), wenn er die beiden folgenden Eigenschaften besitzt:*

(T1) T ist **zusammenhängend**;

(T2) T ist **azyklisch**, das heisst, es existiert kein Zyklus in T .

Nachfolgend einige Beispiele für Bäume:



Bevor wir einige Resultate zu den Bäumen betrachten können, benötigen wir ein Hilfsresultat. Wir erinnern daran, dass in einem *Weg* der gleiche Knoten mehrmals vorkommen darf, aber *nicht in einem Pfad*. Der nachfolgende Satz zeigt, dass wir aus einem Weg durch Weglassen von Knoten einen Pfad gewinnen können.

Satz 6 Sei G ein Graph und u und v zwei Knoten von G . Sei

$$W = uv_1v_2 \dots v_{n-1}v$$

ein Weg von u nach v . Dann existiert eine Teilfolge von W , die ein Pfad von u nach v definiert.

Bew.: Wenn $u = v$ ist, das heisst, wenn der Weg geschlossen ist, dann erfüllt der triviale Pfad $P = u$ den Satz.

Angenommen $u \neq v$. Wenn keiner der Knoten

$$u = v_0, v_1, v_2, \dots, v_{n-1}, v = v_n$$

mehr als einmal vorkommt, dann ist W bereits ein Pfad und wir setzen $P = W$.

Angenommen W besitze Knoten, die zwei oder mehrmals vorkommen. Dann existieren Indizes i, j mit $i < j$ und $v_i = v_j$. Wenn wir im Weg W die Knoten

$$v_i, v_{i+1}, \dots, v_{j-1}$$

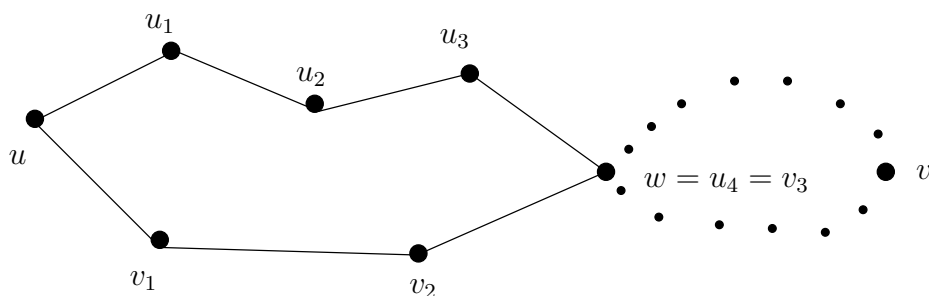
weglassen, dann erhalten wir einen verkürzten Weg W_1 von u nach v . Wenn W_1 keinen Knoten mehrmals enthält, dann sind wir fertig, sonst wiederholen wir das obige Verfahren, bis wir einen Pfad von u nach v erhalten.

□

Satz 7 Sei G ein Graph und u und v zwei unterschiedliche Knoten von G . Dann gilt: Der Graph G ist genau dann ein Baum, wenn es genau einen Pfad von u nach v gibt.

Beweis:

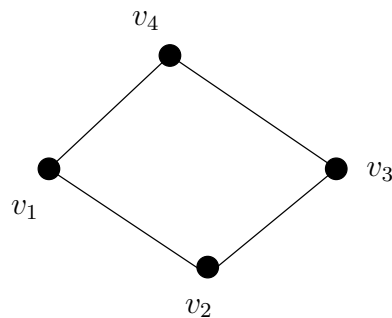
- (i) \Rightarrow : Sei also G ein Baum. Da G zusammenhängend ist, gibt es einen Weg und damit auch einen Pfad von u nach v . Angenommen es gäbe zwei verschiedene Pfade von u nach v . Dann könnte das beispielsweise so aussehen:



Wir stellen fest, dass die Folge $uu_1u_2u_3wv_2v_1u$ ein Zyklus ist. Dies im Widerspruch zur Voraussetzung.

- (ii) \Leftarrow : Es gibt jetzt also zwischen zwei beliebigen Knoten von G *genau einen* Pfad. Wir müssen beweisen, dass G zusammenhängend ist und keinen Zyklus enthält.

Da es zwischen zwei beliebigen Knoten einen Pfad gibt, ist G zusammenhängend. Angenommen es gäbe einen Zyklus. Die nachfolgende Figur zeigt einen Zyklus der Länge 4:



Es gäbe dann zum Beispiel zwischen v_1 und v_3 zwei verschiedene Pfade. Dies im Widerspruch zur Voraussetzung.

□

Satz 8 *Es sei T ein Baum mit mindestens zwei Knoten und es sei*

$$P = u_0u_1 \dots u_n$$

ein Pfad mit maximaler Länge in T , das heisst es gibt keinen Pfad in T der länger als n ist. Dann haben die Knoten u_0 und u_n den Grad 1.

Bew.: Angenommen $\delta(u_0) > 1$. Dann müsste u_0 neben u_1 noch mit einem andern Knoten w verbunden sein. Dieser Knoten wäre dann verschieden von allen Knoten des Pfades P , denn sonst hätten wir einen Zyklus. Dann wäre aber

$$P_1 = wu_0u_1 \dots u_n$$

ein Pfad der Länge $n+1$, dies im Widerspruch zur Voraussetzung. Also muss der Grad von u_0 gleich 1 sein. Analog für u_n .

□

Korollar 1 *Jeder Baum T mit mindestens zwei Knoten besitzt mehr als einen Knoten mit Grad 1.*

Satz 9 *Wenn T ein Baum mit n Knoten ist, dann hat er genau $n-1$ Kanten.*

Beweis durch Induktion über die Anzahl Knoten n .

Verankerung: Sei $n = 1$. Ein Baum mit nur einem Knoten kann keine Kante besitzen, da Schleifen nicht auftreten können. Die Zahl der Kanten ist also $0 = n - 1$.

Voraussetzung: Die Behauptung sei richtig für alle Bäume mit n Knoten.

Vererbung: Wir müssen zeigen, dass die Behauptung richtig ist für Bäume mit $n + 1$ Knoten.

Sei T ein Baum mit $n + 1$ Knoten. Dann existiert ein Knoten u mit Grad 1. Es bezeichne $e = uv$ die einzige Kante von T , die u als Endknoten hat. Wenn x, y zwei von u verschiedene Knoten in T sind, dann führt der Pfad von x nach y nicht über u , denn sonst würde e und damit der Knoten v 2 mal durchlaufen. Dies bedeutet, dass $T - u$ ein zusammenhängender Graph ist. $T - u$ kann auch keine Zyklen enthalten, denn sonst würde auch T ein Zyklus enthalten. Also ist $T - u$ ein *Baum* mit n Knoten. Nach Induktionsvoraussetzung enthält er $n - 1$ Kanten. Wir erhalten T indem wir u mit der Kante e hinzufügen. Also hat T n Kanten.

□

Es sei G ein azyklischer Graph. Dann ist jeder Untergraph von G ebenfalls azyklisch. Insbesondere sind auch die zusammenhängenden Komponenten von G azyklisch und damit Bäume. Aus diesem Grund wird ein azyklischer Graph als **Wald** bezeichnet.

Satz 10 *Es sei G ein azyklischer Graph mit n Knoten und k zusammenhängenden Komponenten. Dann hat G $n - k$ Kanten.*

Bew.: Wir bezeichnen die k Komponenten von G mit

$$T_1, T_2, \dots, T_k.$$

Wir nehmen an, dass T_i n_i Knoten hat. Dann gilt:

$$n = n_1 + n_2 + \dots + n_k$$

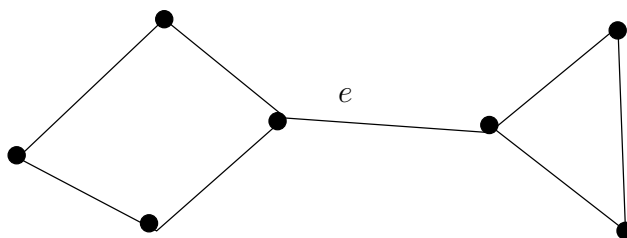
Da T_i ein Baum ist, besitzt T_i $n_i - 1$ Kanten. Damit ist die Anzahl der Kanten von G gegeben durch:

$$(n_1 - 1) + (n_2 - 1) + \dots + (n_k - 1) = (n_1 + n_2 + \dots + n_k) - k = n - k$$

□

Wir benötigen den folgenden Begriff:

Eine Kante e eines Graphen heisst eine **Brücke** oder **Isthmus**, wenn der Untergraph $G - e$ mehr zusammenhängende Komponenten besitzt als G .



Satz 11 *Eine Kante e eines Graphen G ist dann und nur dann eine Brücke, wenn e nicht Teil eines Zyklus in G ist.*

Bew.:

- (i) \Rightarrow : Es sei e eine Brücke. Wir müssen zeigen, dass e nicht Teil eines Zyklus ist. Wir betrachten die Kontraposition:

$$e \text{ ist Teil eines Zyklus} \Rightarrow e \text{ ist keine Brücke}$$

Sei also e Teil eines Zyklus

$$C = u_0 u_1 \dots u_m \quad \text{mit} \quad u_m = u_0.$$

Da wir keine Schlingen und Mehrfachkanten zulassen, ist $m > 2$. Wir nehmen an, dass $e = u_i u_{i+1}$ ist. Dann ist aber

$$P = u_i u_{i-1} \dots u_0 u_{m-1} \dots u_{i+1}$$

ein Pfad von u_i nach u_{i+1} , der nicht mit e identisch ist. Also kann e keine Brücke sein.

- (ii) \Leftarrow : Wir müssen zeigen, dass wenn e nicht Teil eines Zyklus in G ist, dass dann e eine Brücke ist. Wir beweisen wiederum die Kontraposition:

$$e \text{ ist keine Brücke} \Rightarrow e \text{ gehört einem Zyklus an}$$

Wir bezeichnen die Endknoten von e mit u und v . Wenn e keine Brücke ist, dann existiert ein Pfad

$$P = u u_1 \dots u_n v$$

von u nach v , der die Kante e nicht enthält. Dann ist aber

$$C = u u_1 \dots u_n v u$$

ein Zyklus.

□

Wir benötigen noch das folgende Resultat:

Satz 12 *Sei G ein zusammenhängender Graph und e eine Kante von G . Dann ist $G - e$ entweder zusammenhängend oder besitzt 2 Zusammenhangskomponenten.*

Bew.: Falls e keine Brücke ist, ist $G - e$ zusammenhängend. Sei nun e eine Brücke. Wir bezeichnen die beiden Endpunkte von e mit u und v . Sei x ein beliebiger Knoten von G , verschieden von u und v . Wir zeigen, dass x entweder der Zusammenhangskomponente von u oder von v angehört. Wenn es einen Pfad von x nach u gibt, in welchem die Kante e nicht vorkommt, dann gehört x der Zusammenhangskomponente von u an. Angenommen es gäbe nur einen Pfad von x nach u , in welchem die Kante e vorkommt. Der Pfad muss dann die folgende Form haben:

$$P = x v_1 v_2 \dots v_{n-1} v u$$

Die Kante e wird also am Schluss durchlaufen. Folglich liegt x in der Zusammenhangskomponente von v . Diese ist verschieden von der Zusammenhangskomponente von u , denn uv ist der einzige Pfad von u nach v . □

Satz 13 *Ein zusammenhängender Graph G mit n Knoten hat mindestens $n-1$ Kanten. (Mit andern Worten kann ein Graph mit n Knoten und weniger als $n-1$ Kanten nicht zusammenhängend sein.)*

Beweis durch Induktion über die Anzahl Kanten q .

Verankerung: Es sei $q = 1$. Da G zusammenhängend ist, besitzt der Graph nur die beiden Endknoten dieser Kante als Knoten. Es ist also $n = 2$ und es gilt folglich $q \geq n - 1 = 1$.

Induktionsannahme: Sei $k \in \mathbb{N}$. Die Behauptung gelte für alle zusammenhängenden Graphen, deren Kantenzahl $\leq k$ ist.

Vererbung: Sei G ein zusammenhängender Graph mit n Knoten und $q = k + 1$ Kanten.

Wir wählen eine Kante e von G aus. Wenn e keine Brücke ist, dann ist $G - e$ zusammenhängend und besitzt k Kanten. Nach Induktionsvoraussetzung gilt dann $k \geq n - 1$. Daraus folgt

$$q = k + 1 \geq n > n - 1 .$$

Sei nun e eine Brücke. Dann zerfällt $G - e$ in zwei Zusammenhangskomponenten G_1 und G_2 . Wir bezeichnen die Anzahl Knoten von G_i mit n_i und die Anzahl Kanten mit k_i ($1 \leq i \leq 2$). Es gilt $n = n_1 + n_2$ und $k = k_1 + k_2$. Weiter gilt nach Induktionsvoraussetzung:

$$k_1 \geq n_1 - 1 \quad \text{und} \quad k_2 \geq n_2 - 1$$

Also ist

$$k_1 + k_2 \geq n_1 + n_2 - 2 .$$

Daraus folgt

$$q = k + 1 \geq n - 1 .$$

Das ist die gesuchte Ungleichung. □

Wir können jetzt den folgenden Satz beweisen, der drei äquivalente Charakterisierungen für Bäume liefert:

Satz 14 *Es sei G ein Graph mit n Knoten. Dann sind die folgenden Aussagen äquivalent:*

- (a) G ist ein Baum.
- (b) G ist ein azyklischer Graph mit $n - 1$ Kanten.
- (c) G ist ein zusammenhängender Graph mit $n - 1$ Kanten.

Bew.: Wir beweisen $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

- $(a) \Rightarrow (b)$: Angenommen G ist ein Baum. Dann folgt aus der Definition, dass G azyklisch ist. Gemäss Satz 9 hat G $n - 1$ Kanten.
- $(b) \Rightarrow (c)$: Sei G ein azyklischer Graph mit $n - 1$ Kanten und k Zusammenhangskomponenten. Dann hat G gemäss Satz 10 $n - k$ Kanten. Also muss $k = 1$ sein. G ist also zusammenhängend.
- $(c) \Rightarrow (a)$: Angenommen G sei ein zusammenhängender Graph mit $n - 1$ Kanten. Wir müssen zeigen, dass G azyklisch ist. Wir machen einen indirekten Beweis. Angenommen G sei *nicht* azyklisch. Dann hat G einen Zyklus, der gemäss Satz 11 keine Brücke enthält. Wir wählen eine Kante e dieses Zyklus. Da e keine Brücke ist, ist $G - e$ immer noch zusammenhängend. Jedoch hat $G - e$ $n - 2$ Kanten und n Knoten, was nach dem Satz 13 nicht möglich ist.

□

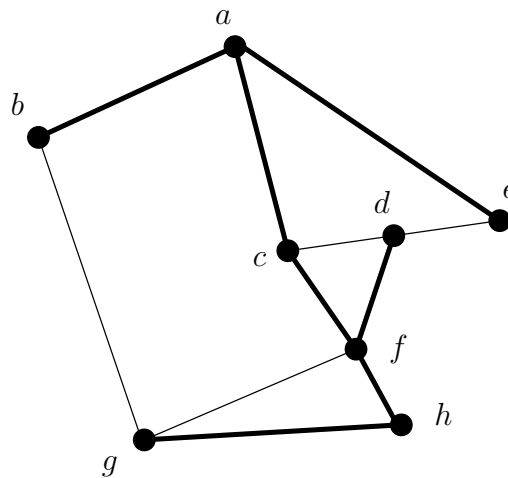
2.8 Erzeugender Baum

Sei $G = (V, E)$ ein Graph. Unter einem **Untergraphen** von G versteht man einen Graphen, dessen Knotenmenge eine Teilmenge von V und dessen Kantenmenge eine Teilmenge von E ist.

Wir betrachten einen zusammenhängenden Graphen $G = (V, E)$. Ein Untergraph T von G mit den beiden Eigenschaften:

- (i) T ist ein Baum;
- (ii) T umfasst alle Knoten von G

wird als **erzeugenden Baum** für G bezeichnet.



Ein erzeugender Baum kann leicht auf die folgende Weise konstruiert werden. Man wählt einen beliebigen Knoten aus und fügt nacheinander Kanten hinzu, wobei jede Kante einen neuen Knoten mit dem Baum verbindet. Im obigen Beispiel könnte man beispielsweise folgendermassen vorgehen: wir wählen den Knoten a aus und verbinden dann die Knoten b, c, e, f, d, h, g mit dem wachsenden Baum, indem wir die Kanten ab, ac, ae, cf, fd, fh und hg auswählen.

Wenn der Graph n Knoten besitzt, müssen wir $n-1$ Kanten auswählen und erhalten dann $1 + (n-1) = n$ Knoten. Dies ist in Übereinstimmung mit Satz 14.

Man kann leicht beweisen, dass diese Methode stets funktioniert. Sei S die Menge der Knoten im wachsenden Baum in einem beliebigen Stadium. Falls es keine Kante geben würde mit einem Knoten in S und dem andern in $V \setminus S$, dann würde es von einem beliebigen Knoten in S keinen Weg zu einem beliebigen andern Knoten in $V \setminus S$ geben. Dies widerspricht der Voraussetzung, dass der Graph zusammenhängend ist.

Beispiel 37 Bestimmen Sie für den abgebildeten Graphen einen erzeugenden Baum. Die Aufgabe wird im Unterricht gelöst. \diamond

Wir betrachten jetzt eine Anwendung für erzeugende Bäume. Angenommen es soll eine bestimmte Zahl von Städten durch eine Pipeline verbunden werden. Gewisse Städte können aus geografischen Gründen nicht direkt untereinander verbunden werden. Für jede mögliche Verbindung werden die entsprechenden Kosten angegeben. Formal haben

wir es mit einem Graphen $G = (V, E)$ zu tun, dessen Knoten die Städte darstellen, und dessen Kanten die möglichen Verbindungen sind. Weiter gibt es eine Kostenfunktion

$$w : E \rightarrow \mathbb{N} ,$$

wo $w(e)$ die Kosten für den Bau der Verbindung e sind. Man spricht von einem **gewichteten Graphen** mit der **Gewichtsfunktion** w .

Beim Pipelineproblem besteht das Ziel darin, ein Netzwerk zu konstruieren, so dass die Kosten minimal sind. Ein solches Netzwerk entspricht einem erzeugenden Baum für G , dessen Gewichtssumme minimal ist:

$$w(T) = \sum_{e \in T} w(e) = \min!$$

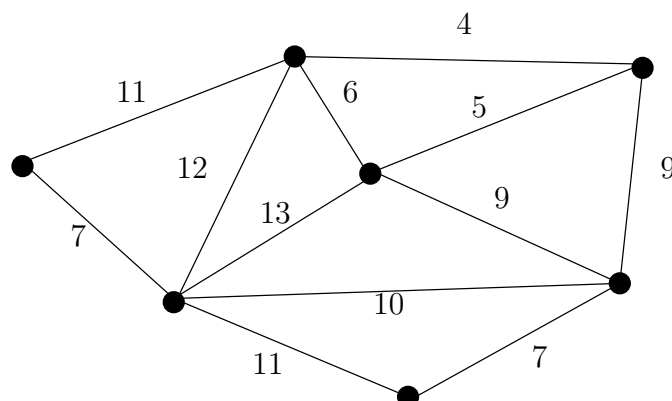
Dieses Problem wird als Problem des **minimalen erzeugenden Baums** für den gewichteten Graphen G bezeichnet (minimum spanning tree problem MST).

Da es nur endlich viele erzeugende Bäume gibt, ist klar, dass eine Lösung existiert. Natürlich ist es auch möglich, dass es mehrere Lösungen gibt.

Eine solche Lösung kann konstruktiv mit dem **Algorithmus von Kruskal** bestimmt werden. Dieser Algorithmus gehört zur Klasse der „greedy“-Algorithmen:

Am Anfang besteht T nur aus den Knoten des gewichteten, zusammenhängenden Graphen G . Das heisst T enthält keine Kanten. Wir ordnen dann die Kanten von G nach den Gewichten in aufsteigender Reihenfolge. Bei Kanten mit gleichem Gewicht sind wir frei, wie wir die Reihenfolge wählen. Wir nehmen im ersten Schritt die Kante mit dem kleinsten Gewicht und fügen sie in T ein. In jedem Schritt wird die nächste Kante in der Liste ausgewählt. Diese wird aber nur eingefügt, wenn sie zwei verschiedene Komponenten von T verbindet (sonst würde ein Zyklus entstehen). In jedem Schritt, wo eine Kante eingefügt wird, nimmt die Anzahl Komponenten von T um Eins ab. Der Algorithmus endet, wenn T nur noch eine Zusammenhangskomponente besitzt.

Beispiel 38 Bestimmen Sie mit dem Algorithmus von Kruskal einen minimalen erzeugenden Baum für den nachfolgenden gewichteten Graphen.



Die Aufgabe wird im Unterricht gelöst. ◇

Satz 15 Sei $G = (V, E)$ ein zusammenhängender Graph mit Gewichtsfunktion

$$w : E \rightarrow \mathbb{N} .$$

Angenommen T sei der erzeugende Baum, den wir mit dem Algorithmus von Kruskal gefunden haben. Dann gilt:

$$w(T) \leq w(U)$$

für jeden erzeugenden Baum von G .

Wir verzichten auf einen Beweis, da wir jetzt noch einen andern Algorithmus zur Konstruktion eines minimalen erzeugenden Baums vorstellen werden.

Es sei G ein gewichteter, zusammenhängender Graph mit n Knoten. Der **Algorithmus von Prim** zur Konstruktion eines minimalen erzeugenden Baums lautet wie folgt:

- 1: Man wähle einen beliebigen Knoten v_1 von G .
- 2: Eine Kante $e_1 = v_1 v_2$ von G ist nun so zu wählen, dass $v_2 \neq v_1$ und e_1 das kleinste Gewicht unter den mit v_1 verbundenen Kanten von G hat.
- 3: Wenn e_1, e_2, \dots, e_i unter Einbeziehung der Endpunkte v_1, v_2, \dots, v_{i+1} gewählt worden sind, wird eine Kante $e_{i+1} = v_j v_k$ mit

$$v_j \in \{v_1, \dots, v_{i+1}\}$$

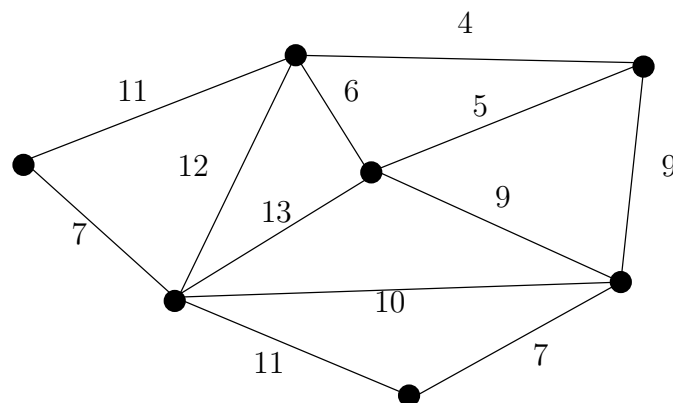
und

$$v_k \notin \{v_1, \dots, v_{i+1}\}$$

so ausgesucht, so dass e_{i+1} das kleinste Gewicht unter den Kanten von G hat, die genau einen Endknoten in $\{v_1, \dots, v_{i+1}\}$ haben.

- 4: Man beende das Verfahren, nachdem $n - 1$ Kanten ausgewählt worden sind. Andernfalls wird Schritt 3 wiederholt.

Beispiel 39 Bestimmen Sie mit dem Algorithmus von Prim einen minimalen erzeugenden Baum für den nachfolgenden gewichteten Graphen.



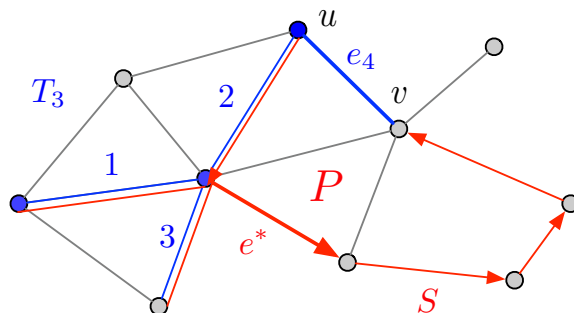
Die Aufgabe wird im Unterricht gelöst. ◇

Satz 16 Es sei G ein gewichteter, zusammenhängender Graph (mit positiven Gewichten) mit n Knoten. Es sei T ein Untergraph von G , der mit dem Algorithmus von Prim erzeugt wurde. Dann ist T ein minimaler erzeugender Baum von G .

Bew.: Aufgrund der Beschreibung des Algorithmus wird klar, dass T ein erzeugender Baum von G ist. Es bleibt also zu zeigen, dass T ein *minimaler* erzeugender Baum von G ist. Angenommen S sei ein *minimaler erzeugender Baum*, der so gewählt wurde, dass er möglichst viele Kanten mit T gemeinsam hat. Wir werden zeigen, dass $T = S$ ist, womit bewiesen ist, dass T ein minimaler erzeugender Baum ist.

Wir machen einen indirekten Beweis. Angenommen $S \neq T$. Dann besitzt T mindestens eine Kante, die nicht in S liegt. Es sei e_k die erste gemäss dem Algorithmus von Prim gewählte Kante ausserhalb von S . Wir bezeichnen die Endpunkte von e_k mit u und v . Da u und v auch im Baum S enthalten sind, gibt es einen einzigen Pfad P in S , der von u nach v führt.

Wir bezeichnen mit T_i den Unterbaum von T , der nach Hinzufügen der i -ten Kante e_i ($1 \leq i \leq n-1$) in G gebildet wird. Nach Beschreibung des Algorithmus von Prim muss ein Endknoten von e_k in T_{k-1} und der andere ausserhalb von T_{k-1} liegen. Wir nehmen an, dass u in T_{k-1} liegt. Da der Pfad P von u nach v führt, muss er eine Kante e^* enthalten mit einem Endknoten in T_{k-1} und dem andern ausserhalb von T_{k-1} . Da wir im k -ten Schritt des Algorithmus von Prim die Kante e_k und nicht e^* gewählt haben, muss $w(e^*) \geq w(e_k)$ sein, denn sonst wäre e^* ausgewählt worden. Da der Pfad P zusammen mit e_k ein Zyklus ist, erhalten wir, wenn wir in S die Kante e_k mit e^* austauschen einen zusammenhängenden Untergraphen von G . Da dieser Untergraph n Knoten und $n-1$ Kanten besitzt, handelt es sich um einen Baum (Satz 14) und zwar um einen erzeugenden Baum, den wir mit R bezeichnen. Wegen $w(e_k) \leq w(e^*)$ ist die Summe der Gewichte von R nicht grösser als jene von S . Damit ist R ein minimaler erzeugender Baum. Dieser minimale erzeugende Baum R hat aber wegen e_k eine Kante mehr gemeinsam mit T als S . Dies steht im Widerspruch zu unserer Voraussetzung, wonach S der minimale erzeugende Baum ist, der am meisten Kanten mit T gemeinsam hat. Folglich muss $S = T$ gelten.

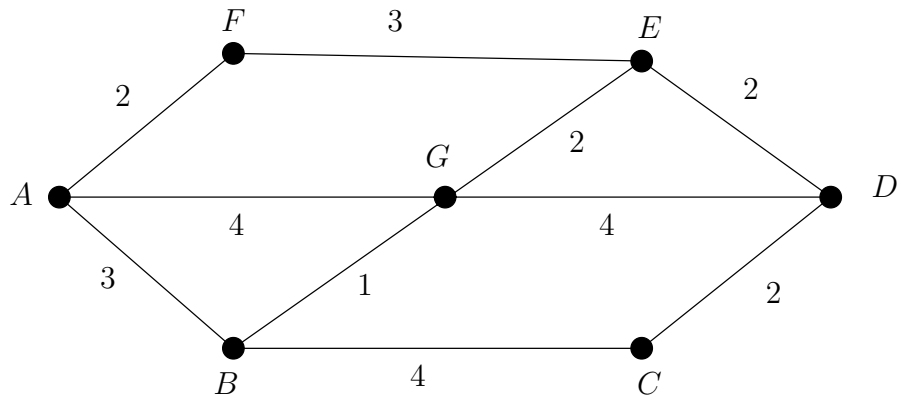


□

2.9 Das Problem des kürzesten Wegs

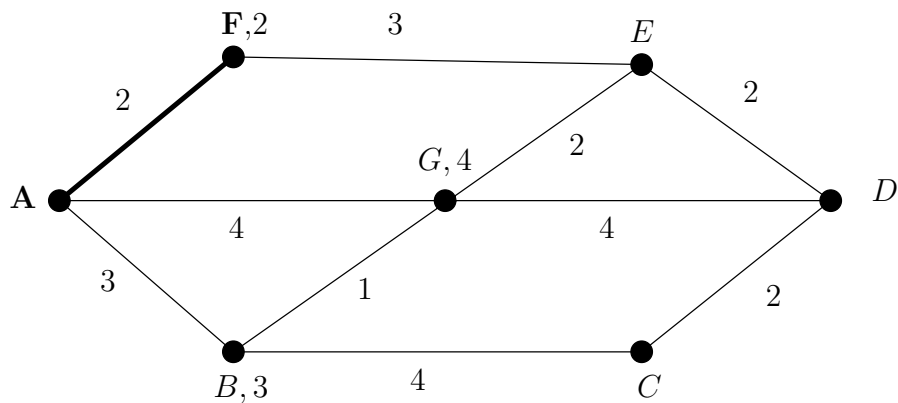
Wir betrachten wiederum einen bewerteten Graphen. Gesucht wird der Weg mit der kleinsten Gewichtssumme zwischen zwei gegebenen Knoten.

Wir erklären den *Algorithmus von Dijkstra* anhand des untenstehenden Graphen:

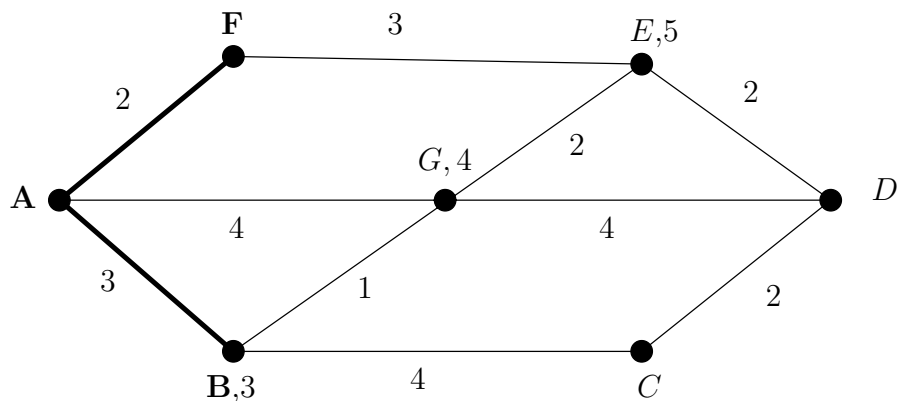


Wir interpretieren die Gewichte als Distanzen. Aber natürlich können diese Zahlen auch etwas ganz anderes bedeuten. Gesucht wird der Weg von A nach D , wofür die Distanz minimal ist.

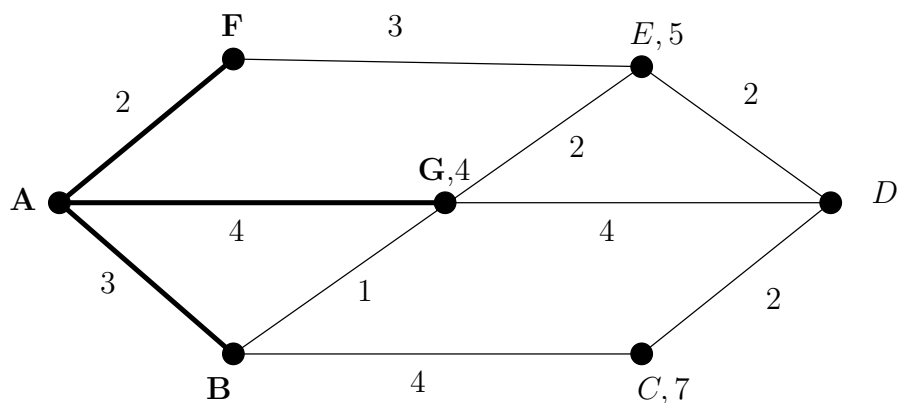
Wir erklären den Algorithmus zuerst für die Handrechnung. Wir bestimmen alle Nachbarknoten von A . Im obigen Fall sind das B , F und G . Wir notieren direkt neben den Knoten ihren Abstand von A und wählen dann jenen mit kleinstem Abstand. Dies ist F . Die Kante AF wird dick ausgezeichnet, denn es gibt keinen kürzeren Weg, um von A nach F zu gelangen.



Wir bestimmen dann alle Nachbarknoten von A und F . Das sind B , E und G und bestimmen wiederum den kürzesten Weg (entweder direkter Weg von A aus oder über F). Wir notieren die Weglängen wiederum neben den Punkten. Wir wählen dann jenen Punkt, wofür die Weglänge minimal ist. Das ist der Punkt B . Die Kante AB wird dick ausgezogen, denn es gibt keinen kürzeren Weg, um von A nach B zu gelangen (Überlegen Sie sich bitte, dass dies allgemein gilt!).

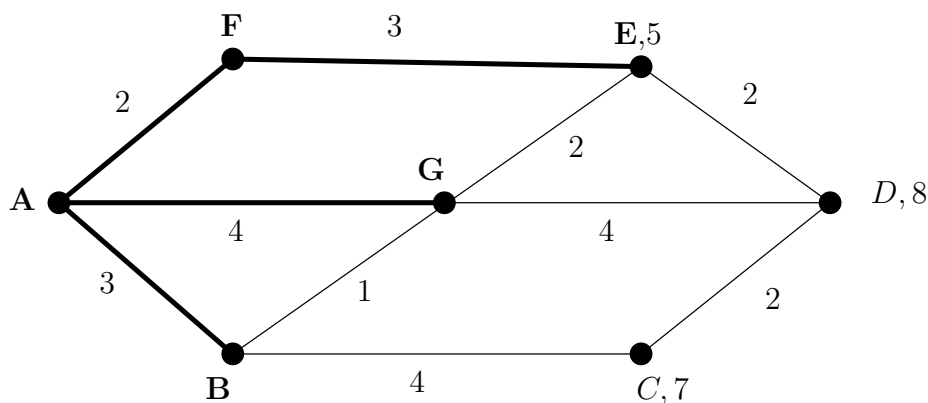


Wir bestimmen dann alle Nachbarknoten von A , B und F , die noch nicht fett markiert sind. Das sind C , E und G und notieren wiederum die kleinste Weglänge der Wege von A aus, die über markierte Knoten führen. Der Knoten mit dem kleinsten Abstand von A ist G . Diese kleinste Weglänge wird durch zwei Wege erreicht. Es spielt keine Rolle, welchen wir bevorzugen. Wenn wir den direkten Weg bevorzugen, dann wird die entsprechende Kante dick ausgezogen.



Nachbarn von A, B, F, G	C	D	E
Zugehörige minimale Weglänge	7	8	5

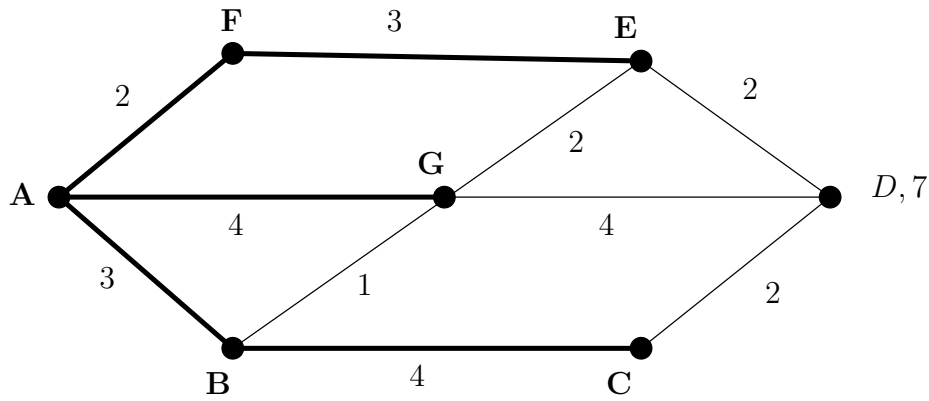
Der Punkt E wird ausgewählt.



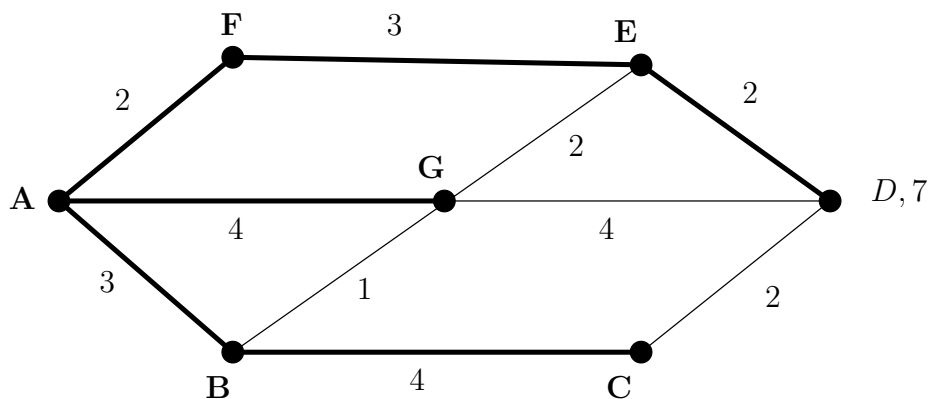
Beachten Sie, dass sich die Länge des kürzesten Wegs, der über markierte Punkte nach D führt, um 1 vermindert hat!

Nachbarn von A, B, E, F, G	C	D
Zugehörige minimale Weglänge	7	7

Wir wählen den Punkt C .



Nachbarn von A, B, C, E, F, G	D
Zugehörige minimale Weglänge	7



Wir erhalten mit diesem Algorithmus einen Baum, denn jeder Knoten wird auf genau einem Weg erreicht. Jeder Knoten wird auf einem Weg mit minimaler Länge erreicht.

Wir interessieren uns jetzt für die Implementierung des Algorithmus auf einem Computer. Seien x und y zwei beliebige Knoten des Graphen. Wir definieren

$$w(x, y) = \begin{cases} 0 & \text{falls } x = y \\ \infty & \text{falls } xy \text{ keine Kante des Graphen ist} \\ d & \text{falls } xy \text{ eine Kante mit Gewicht } d \text{ ist} \end{cases}$$

Wir speichern diese Gewichte in einer Matrix ab. Die erste Zeile und erste Kolonne gehören nicht zur Matrix, sondern dienen nur der besseren Lesbarkeit:

$$G = \begin{array}{c} \begin{array}{ccccccc} & A & B & C & D & E & F & G \\ A & 0 & 3 & \infty & \infty & \infty & 2 & 4 \\ B & 3 & 0 & 4 & \infty & \infty & \infty & 1 \\ C & \infty & 4 & 0 & 2 & \infty & \infty & \infty \\ D & \infty & \infty & 2 & 0 & 2 & \infty & 4 \\ E & \infty & \infty & \infty & 2 & 0 & 3 & 2 \\ F & 2 & \infty & \infty & \infty & 3 & 0 & \infty \\ G & 4 & 1 & \infty & 4 & 2 & \infty & 0 \end{array} \end{array}$$

Algorithmus von Dijkstra

Wir betrachten einen einfachen, zusammenhängenden Graphen $G = (V, E)$ mit positiven Gewichten. Wir bezeichnen die Knoten mit v_0, v_1, \dots, v_n . Das Gewicht der Kante zwischen den Knoten u und v wird mit $w(u, v)$ bezeichnet. Gesucht wird der kürzeste Weg zwischen $a = v_0$ und $z = v_n$.

Der Algorithmus von Dijkstra arbeitet iterativ. Er startet, mit der Initialisierung einer Abstandsfunktion: $L_0(a) = 0$ und $L_0(v) = \infty$ für die übrigen Knoten. Der Index 0 besagt, dass es sich um die 0-te Iteration handelt.

Es wird dann eine Menge bestehend aus Knoten aufgebaut, für die der kürzeste Entfernung von a bekannt ist. Sei S_k diese Menge nach k Iterationen. Wir beginnen mit $S_0 = \emptyset$. Die Menge S_k entsteht dann aus der Menge S_{k-1} , indem der Knoten $u \in V \setminus S_{k-1}$ mit dem kleinsten Abstand hinzugefügt wird. Nachdem u hinzugefügt wurde, werden die Abstände aller Knoten aus $V \setminus S_k$ wieder aktualisiert. Für $v \in V \setminus S_k$ erfolgt die Anpassung des Abstands nach der folgenden Formel:

$$L_k(v) = \min\{L_{k-1}(v), L_{k-1}(u) + w(u, v)\}$$

Die Iteration wird so lange fortgesetzt bis der Knoten z zur Menge hinzugefügt wird.

Wir erweitern den Algorithmus noch so, dass wir auch die kürzesten Wege kennen. Dazu speichern wir den Vorgängerknoten von v des aktuellen kürzesten Wegs in $P(v)$ ab. Wir initialisieren $P(v)$ mit ”.

Im nachfolgenden Algorithmus verwenden wir die Konvention:

$$\infty + \infty = \infty \quad \text{und} \quad a + \infty = \infty \quad (a \in \mathbf{R}^+)$$

Der Algorithmus wird beendet, wenn $z = v_n \in S$ ist. Natürlich kann man die Schleife auch so oft durchlaufen bis alle Knoten in S sind. Wir kennen dann die kürzesten Distanzen und Wege von a zu allen Punkten.


```

procedure Dijkstra(G: weighted connected simple graph,
    with all weights positive)
(* G has vertices  $a = v_0, v_1, v_2, \dots, v_n = z$  and weights  $w(v_i, v_j)$ 
    where  $w(v_i, v_j) = \infty$  if  $\{v_i, v_j\}$  is not an edge in G *)
for  $i := 1$  to  $n$ 
     $L(v_i) := \infty$ 
     $P(v_i) := "$ 
 $L(a) := 0$ 
 $S := \emptyset$ 
(* the labels are now initialized so that the label  $a$  is zero and all
    other labels are  $\infty$ , and  $S$  is the empty set *)
while  $z \notin S$ 
begin
     $u :=$  a vertex not in  $S$  with  $L(u)$  minimal
     $S := S \cup \{u\}$ 
    for all vertices not in  $S$ 
        if  $L(u) + w(u, v) < L(v)$  then
             $L(v) := L(u) + w(u, v)$ 
             $P(v) := u$ 
    (*this adds a vertex to  $S$  with minimal label and updates the
    labels of vertices not in  $S$  *)
end
(*  $L(z)$  = length of shortest path from  $a$  to  $z$  *)
(*  $P(v)$  = predecessor of  $v$  *)

```

Behauptung: Dijkstras Algorithmus findet die kürzeste Distanz zwischen a und z .

Beweis: Mit Hilfe eines Induktionsbeweises über k (=Iterationsindex) wollen wir die folgenden beiden Aussagen beweisen:

- (i) Der Abstand $L_k(v)$ eines Knoten $v \in S_k$ ist die Länge des kürzesten Wegs von a nach v .
- (ii) Der Abstand $L_k(v)$ eines Knotens $v \in V \setminus S_k$ ist die Länge des kürzesten Wegs von a nach v , der ausser v nur Knoten in S_k besitzt.

Verankerung: $k = 0$. Da $S = \emptyset$ sind beide Aussagen richtig.

Voraussetzung: Die beiden Aussagen seien wahr für ein festes, aber beliebiges k .

Vererbung: Wir müssen zeigen, dass die Behauptung auch für $k + 1$ richtig ist.

Es sei $S_{k+1} = S_k \cup \{u\}$. Wir wollen zuerst (i) beweisen. Für $v \in S_{k+1}$, $v \neq u$ ist nach Induktionsvoraussetzung nichts zu beweisen. Für u gilt wegen (ii) und der Tatsache, dass u ausgewählt wurde, dass sein Abstand zu a , wenn nur Knoten aus S_k verwendet werden kleiner oder gleich ist als für jeden andern Knoten in $V \setminus S_k$. Gäbe es einen kürzeren Weg zu u , in welchem ein Knoten w vorkäme, der nicht in S_k enthalten ist, dann würde das bedeuten, dass

$$L_k(w) < L_k(u) .$$

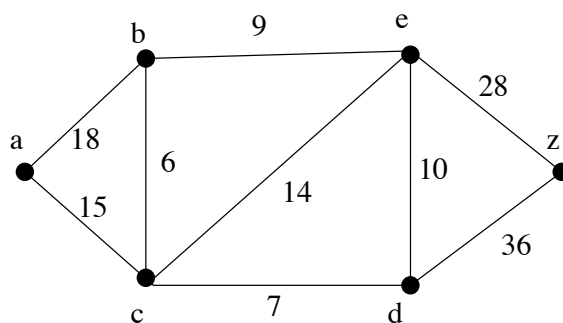
Dies steht aber im Widerspruch zur Auswahl von u .

Sei $v \in V \setminus S_{k+1}$. Nach Induktionsvoraussetzung (ii) ist $L_k(v)$ der Abstand des kürzesten Wegs von a nach v , der ausser v nur Knoten aus S_k enthält. Wegen

$$L_{k+1}(v) = \min\{L_k(v), L_k(u) + w(u, v)\}$$

muss das auch weiterhin gelten. □

Um den Algorithmus zu verstehen, betrachten wir das nachfolgende Beispiel:



Initialisierung:

Knoten v	a	b	c	d	e	z
S	{ }					
$L(v)$	0	∞	∞	∞	∞	∞

Schleife wird zum 1. Mal durchlaufen: Es ist $u = a$. Die neuen Distanzen werden nach der Formel

$$L(v) := \min(L(v), L(u) + w(u, v))$$

berechnet. Hier ist $v \in V \setminus S$ und u der Knoten der zuletzt in S hinzugefügt wurde. Es ist zu beachten, dass $w(u, v) = \infty$ ist, wenn zwischen u und v keine Kante vorhanden ist.

Wir erhalten:

$$\begin{aligned} L(b) &= \min(\infty, 0 + 18) = 18 \\ L(c) &= \min(\infty, 0 + 15) = 15 \\ L(d) &= \min(\infty, 0 + \infty) = \infty \\ L(e) &= \min(\infty, 0 + \infty) = \infty \\ L(z) &= \min(\infty, 0 + \infty) = \infty \end{aligned}$$

Die nachfolgenden Tabelle enthält die Werte aller Variablen am Ende der Schleife:

Knoten v	a	b	c	d	e	z
S	{ a }					
$L(v)$	0	18	15	∞	∞	∞
$P(v)$	—	a	a	—	—	—

Schleife wird zum 2. Mal durchlaufen: Es ist $u = c$ und wir erhalten:

$$\begin{aligned} L(b) &= \min(18, 15 + 6) = 18 \\ L(d) &= \min(\infty, 15 + 7) = 22 \\ L(e) &= \min(\infty, 15 + 14) = 29 \\ L(z) &= \min(\infty, 15 + \infty) = \infty \end{aligned}$$

Also:

Knoten v	a	b	c	d	e	z
S	$\{a, c\}$					
$L(v)$	0	18	15	22	29	∞
$P(v)$	—	a	a	c	c	—

Schleife wird zum 3. Mal durchlaufen: Es ist $u = b$ und wir erhalten:

$$\begin{aligned} L(d) &= \min(22, 18 + \infty) = 22 \\ L(e) &= \min(29, 18 + 9) = 27 \\ L(z) &= \min(\infty, 18 + \infty) = \infty \end{aligned}$$

Also:

Knoten v	a	b	c	d	e	z
S	$\{a, c, b\}$					
$L(v)$	0	18	15	22	27	∞
$P(v)$	—	a	a	c	b	—

Schleife wird zum 4. Mal durchlaufen: Es ist $u = d$ und wir erhalten:

$$\begin{aligned} L(e) &= \min(27, 22 + 10) = 27 \\ L(z) &= \min(\infty, 22 + 36) = 58 \end{aligned}$$

Also:

Knoten v	a	b	c	d	e	z
S	$\{a, c, b, d\}$					
$L(v)$	0	18	15	22	27	58
$P(v)$	—	a	a	c	b	d

Schleife wird zum 5. Mal durchlaufen: Es ist $u = e$ und wir erhalten:

$$L(z) = \min(58, 27 + 28) = 55$$

Also:

Knoten v	a	b	c	d	e	z
S	$\{a, c, b, d, e\}$					
$L(v)$	0	18	15	22	27	55
$P(v)$	—	a	a	c	b	e

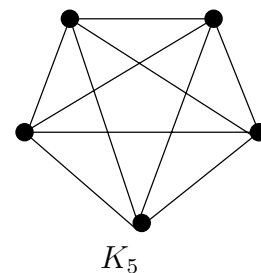
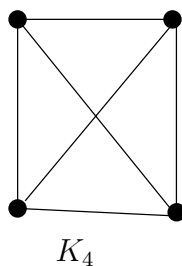
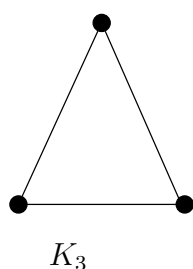
Schleife wird zum 6. Mal durchlaufen: Es ist $u = z$. Die Distanzen ändern natürlich nicht mehr. Also:

Knoten v	a	b	c	d	e	z
S	$\{a, c, b, d, e, z\}$					
$L(v)$	0	18	15	22	27	55
$P(v)$	—	a	a	c	b	e

2.10 Die Eulersche Polyederformel

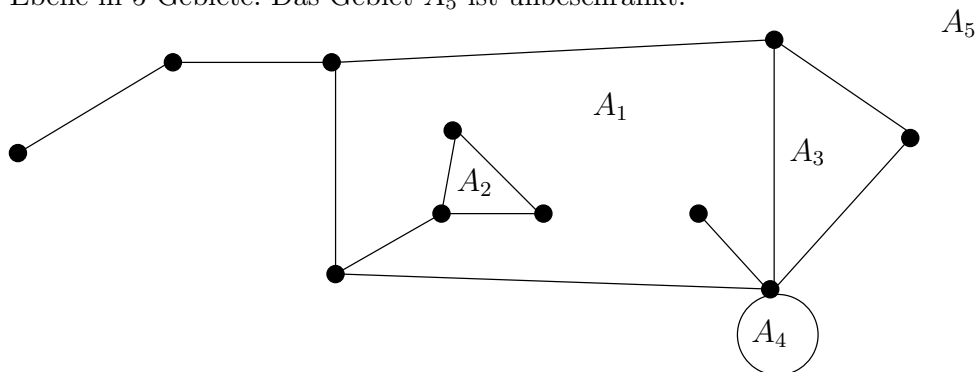
Ein Graph heisst **eben**, wenn seine Knoten in der gleichen Ebene liegen und sich seine Kanten nur in den Knoten schneiden. Ein Graph heisst **plättbar** oder **planar**, wenn er isomorph zu einem ebenen Graphen ist. Es gibt also eine Darstellung des Graphen in der Ebene, so dass sich die Kanten nur in den Knoten schneiden.

Beispiel 40 Welche der folgenden Graphen sind eben, welche sind plättbar?



Die Aufgabe wird im Unterricht gelöst. ◇

In diesem Abschnitt betrachten wir ebene zusammenhängende Graphen, wobei Schleifen und Doppelkanten zugelassen sind. Ein solcher Graph zerlegt die Ebene in verschiedene Gebiete. Wir verzichten darauf eine exakte Definition eines solchen Gebiets zu geben und begnügen uns mit einem Beispiel. Der nachfolgende Graph zerlegt die Ebene in 5 Gebiete. Das Gebiet A_5 ist unbeschränkt.



Der folgende Satz ist in der Literatur unter dem Namen **Eulerscher Polyedersatz** bekannt. Wir werden den Zusammenhang mit den Polyedern später erläutern.

Satz 17 (Euler 1752) Sei G ein zusammenhängender, ebener Graph mit n Knoten (nodes), a Kanten (arcs) und r Gebieten (regions). Dann gilt:

$$n + r = a + 2 \quad (6)$$

Beweis durch vollständige Induktion über die Anzahl der Kanten von G .

Verankerung: Für $a = 1$ ist entweder $n = 1$ (Schleife) und damit $r = 2$ oder $n = 2$ und $r = 1$. In beiden Fällen ist die Formel richtig.

Induktionsvoraussetzung: Wir nehmen an, dass die Formel für Graphen mit $a - 1$ Kanten richtig sei.

Vererbung: Wir fügen eine neue Kante e hinzu. Es gibt drei Fälle zu beachten:

- (i) e ist eine Schleife: die Eckenzahl bleibt unverändert, aber die Anzahl der Gebiete nimmt um 1 zu.
- (ii) e verbindet zwei verschiedene Ecken: die Eckenzahl bleibt unverändert, aber die Anzahl der Gebiete nimmt um 1 zu, da ein bestehendes Gebiet in zwei Gebiete zerlegt wird.

- (iii) Die Kante e wird an eine bestehende Ecke angehängt: in diesem Fall nimmt die Eckenzahl um 1 zu und die Anzahl der Gebiete bleibt unverändert.

In allen drei Fällen bleibt die Formel richtig.

□

Indem wir zusätzliche Forderungen an den Graphen stellen erhalten wir die folgenden Ungleichungen:

Satz 18 Für einen einfachen, zusammenhängenden, ebenen Graphen mit n Knoten und a Kanten gilt:

- (i) Falls $n \geq 3$, dann gilt:

$$a \leq 3n - 6$$

- (ii) Falls $n \geq 3$ ist und falls es keine Zyklen mit der Länge 3 gibt, dann gilt:

$$a \leq 2n - 4$$

Beweis:

- (i) Es gibt keine Gebiete, welche nur durch eine Kante begrenzt werden, denn es gibt keine Loops. Es gibt auch keine Gebiete, welche nur durch zwei Kanten begrenzt werden, denn es gibt keine parallelen Kanten. Folglich werden alle Gebiete durch *mindestens* 3 Kanten begrenzt. Da jede Kante doppelt gezählt wird, erhalten wir die folgende Ungleichung:

$$2a \geq 3r$$

Wir lösen die Eulersche Formel nach r auf und setzen den Ausdruck in die obige Ungleichung ein.

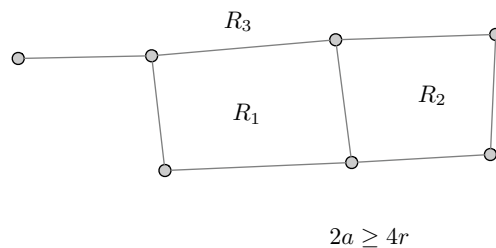
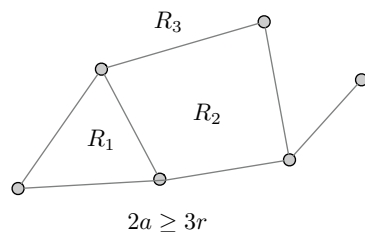
$$2a \geq 3(2 - n + a) \implies a \leq 3n - 6$$

- (ii) Falls es keine Zyklen der Länge 3 gibt, wird jedes Gebiet von mindestens 4 Kanten begrenzt. Als:

$$2a \geq 4r .$$

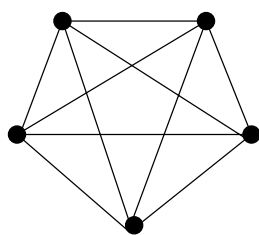
Wir ersetzen r wiederum durch $2 - n + a$ und erhalten die Ungleichung

$$a \leq 2n - 4 .$$

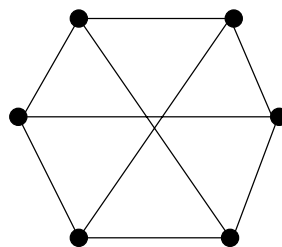


□

Beispiel 41 Zeigen Sie mit Hilfe der obigen Ungleichungen, dass die Graphen K_5 und $K_{3,3}$ nicht plättbar sind.



K_5



$K_{3,3}$

Die Aufgabe wird im Unterricht gelöst.

◇

2.11 Polyeder und platonische Körper

Unter einem **Polyeder** versteht man einen 3-dimensionalen Körper, der durch Polygone (Vielecke) beschränkt ist. Ein Polyeder heisst **konvex**, wenn für zwei beliebige Punkte des Polyeders die ganze Verbindungsstrecke im Polyeder enthalten ist.

Beispiel 42 Überlegen Sie sich, dass zu einem konvexen Polyeder ein ebener, zusammenhängender Graph gehört. Gehört zu jedem ebenen, zusammenhängenden Graphen ein Polyeder?

Die Aufgabe wird im Unterricht gelöst.

◇

Der Graph eines Polyeders erfüllt also den eulerschen Polyedersatz (6):

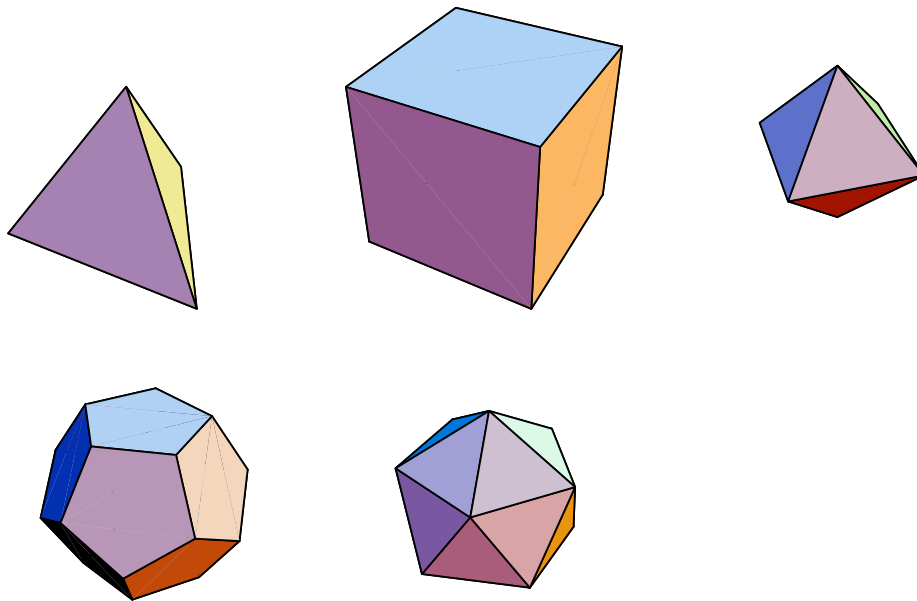
$$n + r = a + 2$$

Euler ist übrigens auf diesen Satz gestossen, indem er Polyeder betrachtet hat.

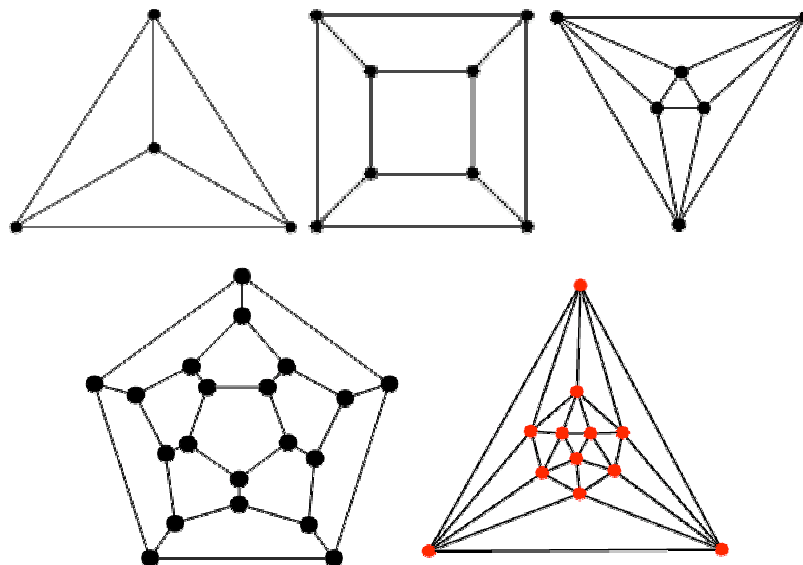
Unter einem **Platonischen⁶ Körper** versteht man einen konvexen Polyeder, der von kongruenten Polygonen begrenzt wird. In jeder Ecke trifft darüberhinaus die gleiche Anzahl von Polygonen zusammen. Seit Jahrtausenden kennt man die 5 platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder:

	Ecken	Flächen	Kanten
Tetraeder	4	4	6
Würfel	8	6	12
Oktaeder	6	8	12
Dodekaeder	20	12	30
Ikosaeder	12	20	30

⁶Platon (427 v. Chr. bis 347 v. Chr.): griechischer Philosoph



Nachfolgend die ebenen Graphen der platonischen Körper.



Diese Graphen haben die folgenden Eigenschaften:

- Alle Ecken haben den gleichen Grad und zwar mindestens 3. Graphen, in denen jeder Knoten den gleichen Grad besitzt heissen **regulär**.
- Alle Flächen haben die gleiche Anzahl Ecken und zwar mindestens 3.

Graphen mit diesen Eigenschaften nennt man **platonische Graphen**. Wir werden beweisen, dass es nur diese 5 platonischen Graphen gibt. Damit haben wir dann gezeigt, dass es nur 5 platonische Körper gibt.

Wir verwenden die Bezeichnungen:

- n : die Anzahl der Knoten (totale Anzahl Ecken, nombre total de noeuds)
- r : die Anzahl der Flächen (régions)
- a : die Anzahl der Kanten (arcs)
- d : der Grad der Ecken (degré)
- s : die Flächen sind s -Ecke

Es gilt dann:

$$n \cdot d = 2a$$

Wir dividieren durch d , um die Knotenzahl mit der Kantenzahl auszudrücken:

$$n = \frac{2 \cdot a}{d}.$$

Auch die Anzahl der Ecken der Polygone lässt sich durch die Anzahl der Kanten ausdrücken:

$$r \cdot s = 2 \cdot a \implies r = \frac{2 \cdot a}{s}.$$

Wir verwenden dann die eulersche Formel:

$$n + r - a = 2$$

Hier setzen wir die obigen Ausdrücke für n und r ein:

$$\frac{2 \cdot a}{d} + \frac{2 \cdot a}{s} - a = 2$$

Wir dividieren durch $2a$ und erhalten:

$$\frac{1}{d} + \frac{1}{s} - \frac{1}{2} = \frac{1}{a}$$

Da der Ausdruck $\frac{1}{a}$ positiv ist, muss auch der Ausdruck auf der linken Seite positiv sein, das heisst, es muss gelten:

$$\frac{1}{d} + \frac{1}{s} > \frac{1}{2}$$

Für d und s kommen nur die Zahlen 3, 4, 5, ... in Frage. Wir setzen jetzt die kleinsten Zahlen ein und überprüfen, ob $\frac{1}{d} + \frac{1}{s}$ wirklich grösser als $\frac{1}{2}$ ist.

d	s	$\frac{1}{d} + \frac{1}{s}$
3	3	$\frac{1}{3} + \frac{1}{3} = \frac{2}{3} > \frac{1}{2}$
3	4	$\frac{1}{3} + \frac{1}{4} = \frac{7}{12} > \frac{1}{2}$
3	5	$\frac{1}{3} + \frac{1}{5} = \frac{8}{15} > \frac{1}{2}$
3	6	$\frac{1}{3} + \frac{1}{6} = \frac{1}{2}$
4	3	$\frac{1}{4} + \frac{1}{3} = \frac{7}{12} > \frac{1}{2}$
4	4	$\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$
5	3	$\frac{1}{5} + \frac{1}{3} = \frac{8}{15} > \frac{1}{2}$
6	3	$\frac{1}{6} + \frac{1}{3} = \frac{1}{2}$

Es gibt also genau 5 platonische Körper.

2.12 Das Färben von ebenen Landkarten

Wir betrachten eine ebene Landkarte, die aus **zusammenhängenden Ländern** besteht, das heisst man kann von jedem Punkt eines Landes zu jedem andern Punkt gelangen, ohne es zu verlassen. Sie soll so gefärbt werden, dass zwei Länder, die eine Grenze gemeinsam haben (die nicht nur aus einem Punkt besteht) verschiedene Farben besitzen. Länder, welche nur in einem Punkt aneinanderstossen, dürfen die gleiche Farbe besitzen.

Beispiel 43 Zeichnen Sie eine Landkarte, für welche vier Farben benötigt werden.

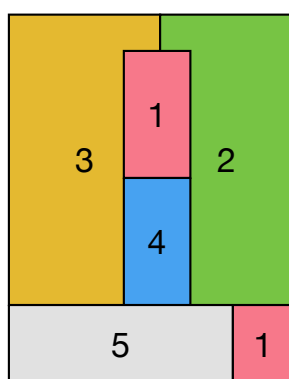
Die Aufgabe wird im Unterricht gelöst. \diamond

Die Vermutung, dass maximal vier Farben benötigt werden, wurde im Jahre 1852 in einem Brief von De Morgan⁷ an Hamilton⁸ formuliert. Im Jahre 1878 stellte Arthur Cayley⁹ das Problem der mathematischen Gesellschaft Londons vor. Innerhalb eines Jahres fand Alfred Kempe¹⁰ einen Beweis für den Satz. Erst 11 Jahre später erkannte man, dass der Beweis fehlerhaft war.

Die „Vierfarbenvermutung“ blieb dann über ein Jahrhundert lang unbewiesen. Schliesslich lieferten im Jahre 1976 zwei Mathematiker der Universität Illinois, Ken Appel und Wolfgang Haken, einen Beweis, der teilweise mit dem Computer durchgeführt werden muss, da die Durchführung des Beweises von Hand nicht machbar ist. Der Beweis reduziert die Anzahl der problematischen Fälle auf 1'939, die durch einen Computer einzeln geprüft wurden. Der Beweis wurde von der Wissenschaftsgemeinde als richtig anerkannt. Dies ist das erste Mal, dass eine berühmte Vermutung mit dem massiven Einsatz eines Computers bewiesen wird. Bis heute ist kein Beweis des **Vierfarbensatzes** bekannt, der ohne Computer auskommt.

Satz 19 Für jede ebene Landkarte mit zusammenhängenden Ländern genügen 4 Farben.

Hinweis: Wenn die Länder nicht zusammenhängend sind, können mehr als vier Farben notwendig sein, wie das folgende Beispiel zeigt.



Das Land 1 besteht aus zwei Zusammenhangskomponenten.
Es sind 5 Farben notwendig.

⁷Augustus De Morgan (1806-1871): englischer Mathematiker

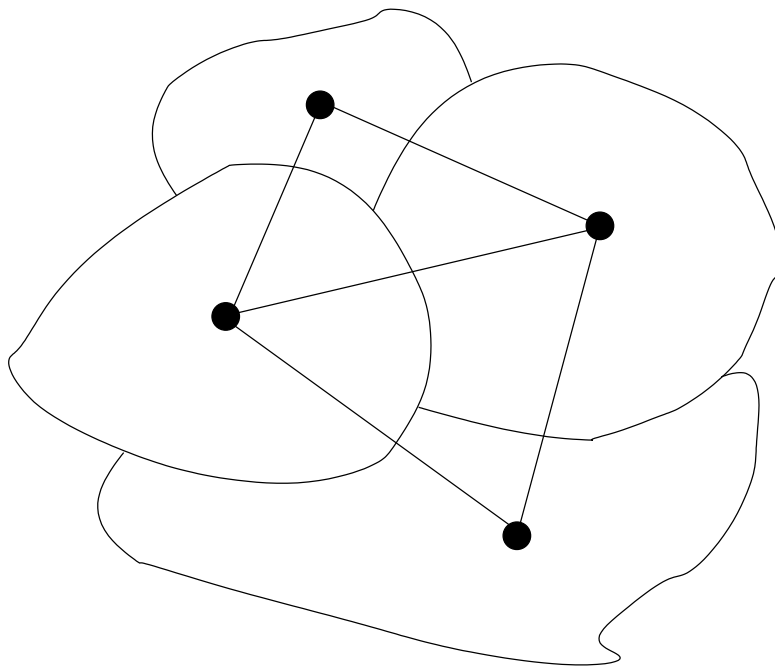
⁸William Rowan Hamilton (1805-1865) irischer Mathematiker

⁹Arthur Cayley (1821-1895) englischer Mathematiker

¹⁰Alfred Bray Kempe (1849-1922): englischer Jurist. Kempe studierte auch Mathematik und übte dies als Hobby aus.

Natürlich können wir den Satz 19 nicht beweisen. Wir werden aber beweisen, dass 5 Farben genügen. Um diese Aussage zu beweisen, werden wir die Landkarte in einen Graph umwandeln. Wir erhalten den **dualen Graphen** der Landkarte, indem wir die Länder durch Knoten ersetzen und die Knoten durch eine Kante verbinden, wenn die Länder aneinandergrenzen.

Die nachfolgende Abbildung zeigt eine Landkarte mit dem zugehörigen dualen Graphen.



Definition 5 Unter einer **Färbung** eines Graphen versteht man eine Zuordnung einer Farbe zu jedem Knoten des Graphen, so dass benachbarte Knoten verschiedene Farben besitzen. Die **chromatische Zahl** eines Graphen ist die kleinste Zahl von Farben, welche für eine Färbung benötigt wird.

Lemma 3 In einem einfachen, zusammenhängenden, ebenen Graphen mit drei oder mehr Knoten, existiert mindestens ein Knoten dessen Grad kleiner oder gleich 5 ist.

Beweis: Wir machen einen indirekten Beweis. Angenommen die Aussage ist nicht richtig. Dann hat jeder Knoten den Grad 6 oder grösser. Die Anzahl der Kantenenden ist dann mindestens $6n$, wo n die Anzahl der Knoten ist. Da die Anzahl der Kantenenden das Doppelte der Anzahl Kanten a ist, gilt:

$$6n \leq 2a$$

Andererseits gilt wegen Satz 18 $a \leq 3n - 6$ oder $2a \leq 6n - 12$. Wir kombinieren die beiden Ungleichungen und erhalten:

$$6n \leq 6n - 12$$

Dies ist ein Widerspruch!

□

Satz 20 Die chromatische Zahl für jeden einfachen, zusammenhängenden, ebenen Graphen ist höchstens 5.

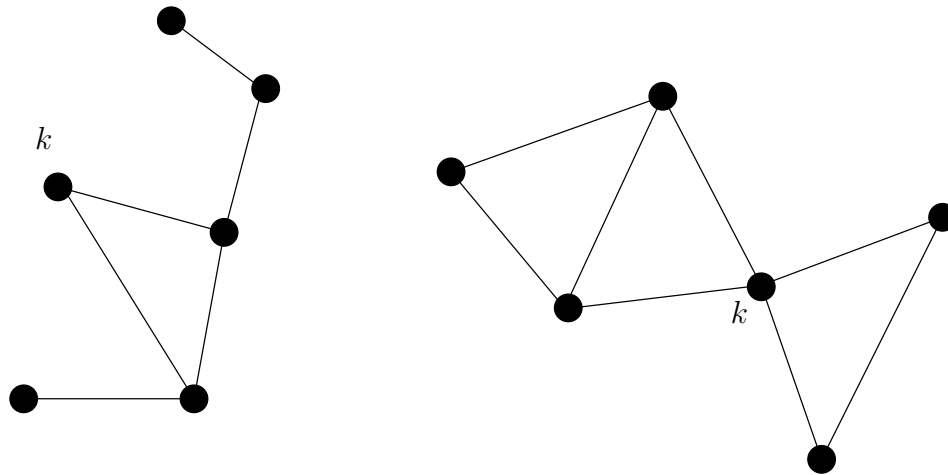
Beweis durch vollständige Induktion über die Anzahl Knoten n .

Verankerung: Die Behauptung ist offensichtlich für $n = 1$ richtig.

Induktionsannahme: Die Behauptung ist richtig für die Werte $1, \dots, n - 1$.

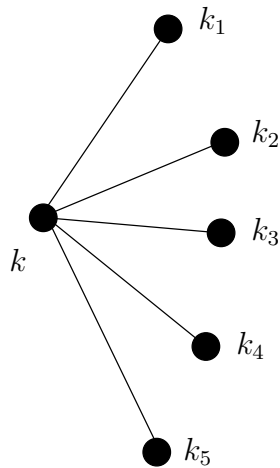
Verebung: Sei G ein einfacher, zusammenhängender, ebener Graph mit n Knoten.

Nach dem vorhergehenden Lemma besitzt der Graph mindestens einen Knoten, dessen Grad höchstens 5 ist. Sei k ein solcher Knoten. Wir lassen diesen Knoten und die zu ihm führenden Kanten kurzfristig weg. Wir erhalten so einen Graphen G' , der aus einer oder mehreren Zusammenhangskomponenten besteht. Jede dieser Komponenten hat weniger als n Knoten und kann deshalb nach der Induktionshypothese mit höchstens 5 Farben gefärbt werden.



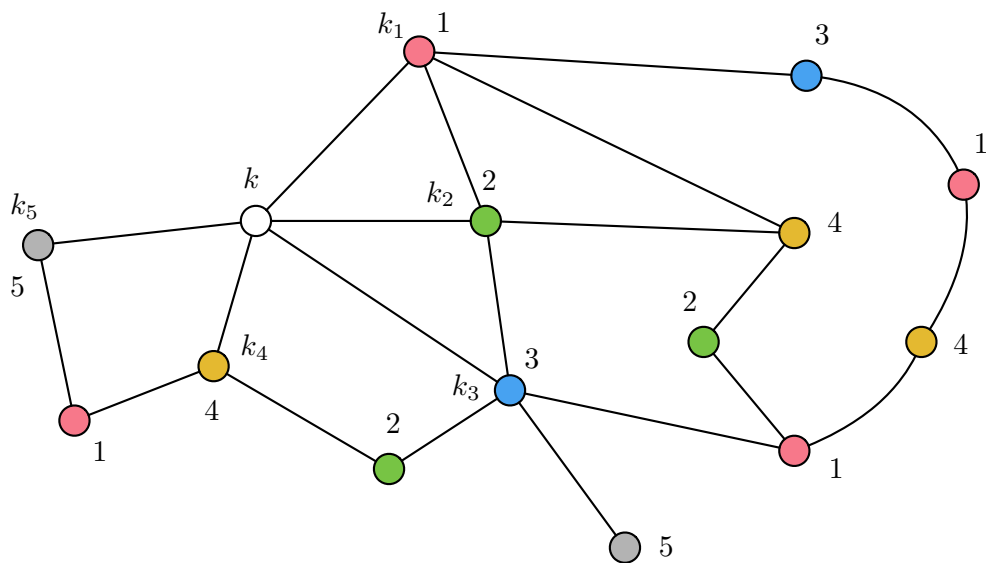
Wir möchten jetzt den Knoten k und seine Kanten wieder in den Graphen einführen.

- Falls der Grad von k kleiner als 5 ist, oder falls die Nachbarknoten nicht alle verschiedene Farben besitzen, bleibt eine Farbe übrig, mit welcher wir den Knoten k färben können und wir erhalten so eine zulässige Färbung des Graphen mit 5 Farben.
- Falls der Knoten k den Grad 5 besitzt und seine 5 Nachbarn alle verschieden gefärbt sind, dann bezeichnen wir die 5 Knoten mit k_1, k_2, k_3, k_4, k_5 . Diese 5 Knoten sind in einer ebenen Darstellung von G in dieser Reihenfolge um den Knoten k herum angeordnet. Wir bezeichnen die zugehörigen Farben mit $1, 2, \dots, 5$.

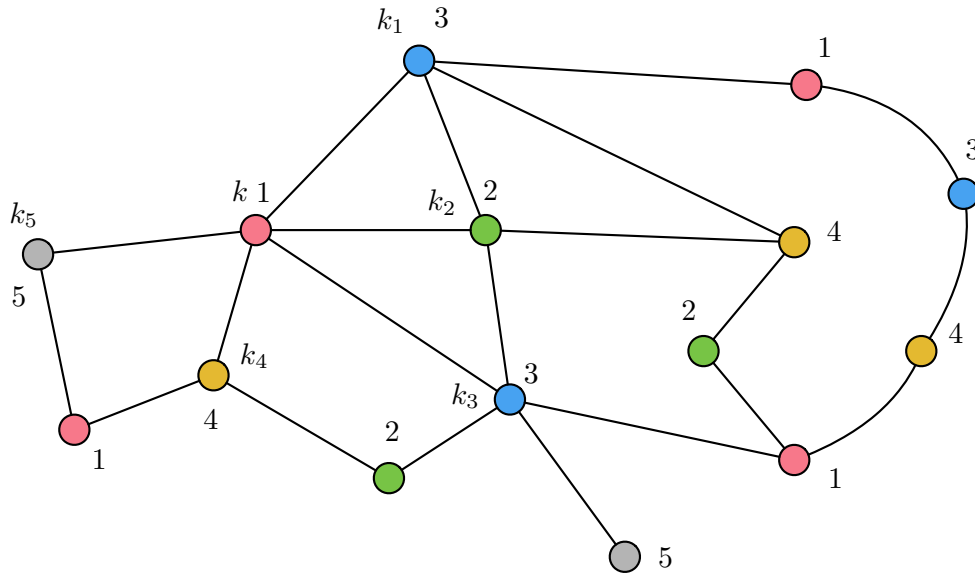


Wir betrachten den Untergraphen G_{13} von G , der durch die Knoten mit den Farben 1 oder 3 induziert wird. Da zwei Knoten mit der gleichen Farbe nicht Nachbarn sein können, handelt es sich um einen bipartiten Graphen. Andererseits besitzen die Nachbarknoten von G_{13} , die in G liegen, eine Farbe die verschieden von 1 und 3 ist.

Falls k_3 nicht zur Zusammenhangskomponente von k_1 gehört, dann können wir die Farben 1 und 3 der Knoten dieser Komponente (=Komponente von k_1) von G_{13} vertauschen und wir erhalten so eine zulässige Färbung. Wir können dann dem Knoten k die Farbe 1 geben.

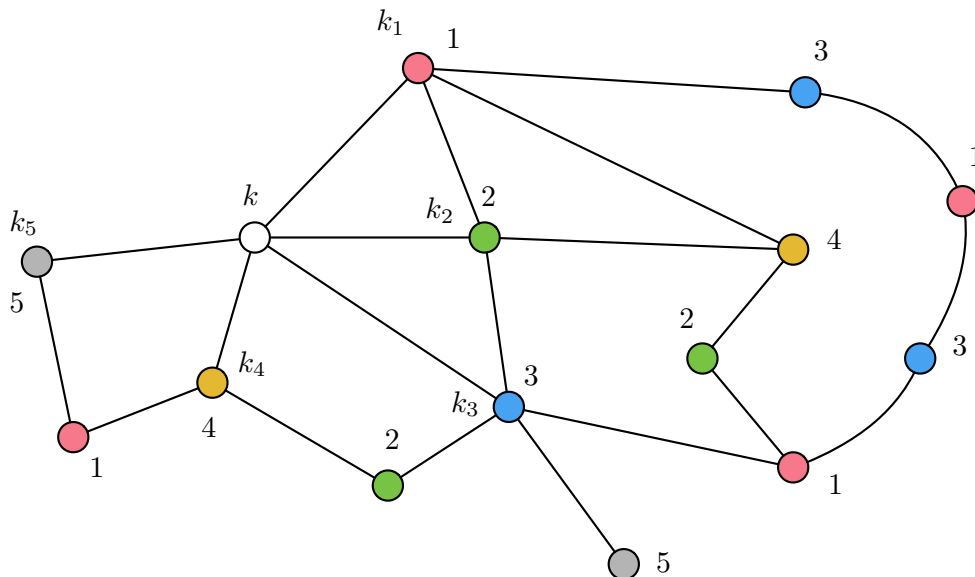


k_1 und k_3 gehören verschiedenen Zusammenhangskomponenten von G_{13} an.



In der Zusammenhangskomponenten von G_{13} , welcher k_3 angehört, vertauschen wir die Farben 1 und 3.

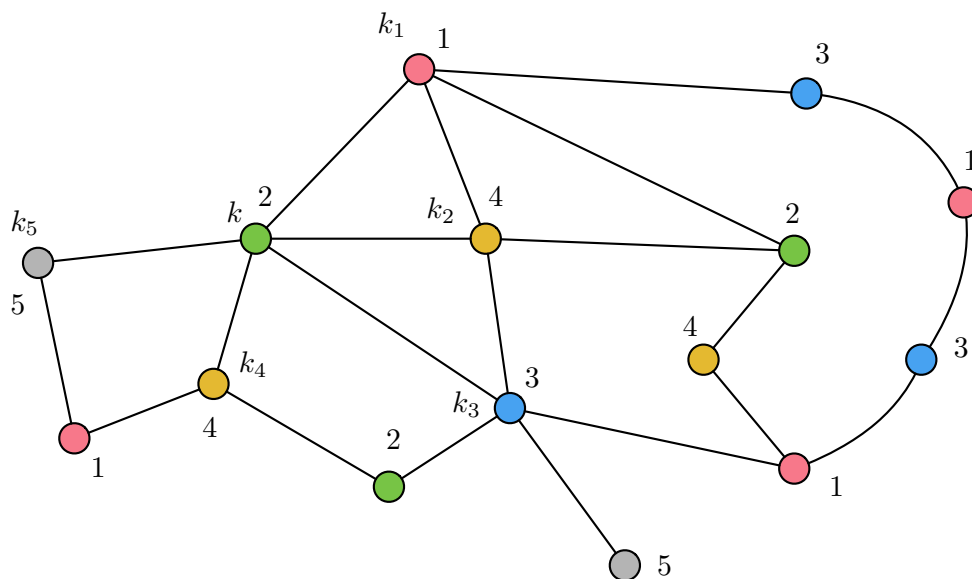
Falls k_1 und k_3 zur gleichen Zusammenhangskomponente des Graphen G_{13} gehören, dann betrachten wir den Untergraphen G_{24} , der von den Knoten mit den Farben 2 und 4 induziert wird. Da die Knoten k_1 und k_3 in G_{13} durch einen Pfad P verbunden sind und deshalb $C = k k_1 + P + k_3 k$ ein Zyklus in G ist, liegt von den Knoten k_2 und k_4 in der aktuellen ebenen Darstellung von G einer innerhalb und der andere ausserhalb des Zyklus. Kein Weg in G_{24} kann sie deshalb verbinden, ohne über einen Knoten von C zu führen, was nicht möglich ist, da die Farben verschieden sind.



k_2 und k_4 liegen nicht in der gleichen Zusammenhangskomponenten von G_{24} .

Wenn wir also die Farben in der Zusammenhangskomponente von k_2 in G_{24} ändern, erhalten wir eine zulässige Färbung der Knoten von $G \setminus \{k\}$. In dieser Färbung besitzt

k_2 die Farbe 4. Wir erhalten eine zulässige Färbung von G , indem wir k die Farbe 2 zuweisen.

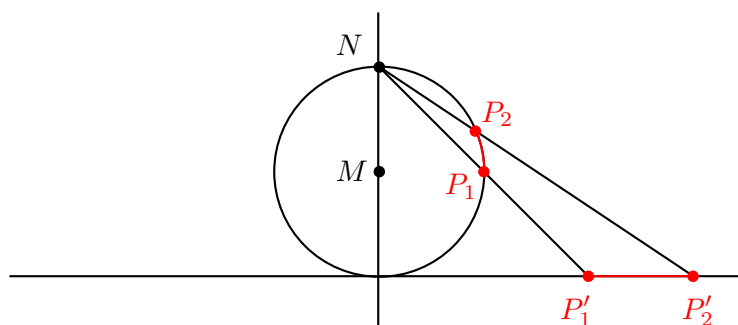


Wir vertauschen die Farben 2 und 4 in der Zusammenhangskomponente von G_{24} , welcher k_2 angehört.

□

2.13 Ergänzungen zum Färbungsproblem

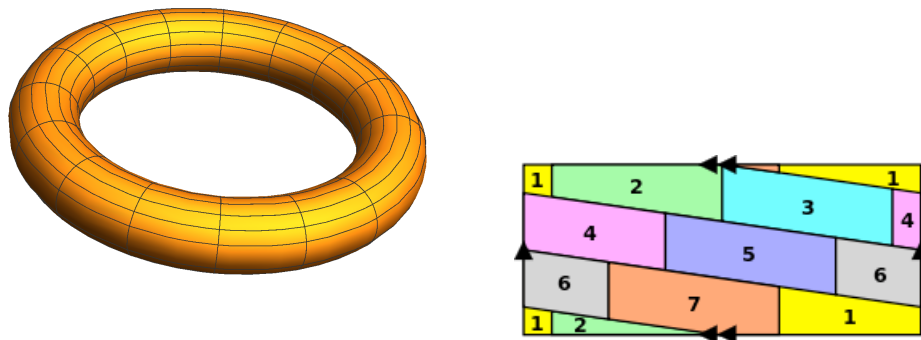
Das Färbungsproblem für Karten in der Ebene ist äquivalent zum Färbungsproblem für Karten auf der Sphäre (=Kugeloberfläche). Mithilfe einer stereographischen Projektion, lässt sich die Karte auf der Sphäre auf eine Karte in der Ebene abbilden. Natürlich werden die Länder so verzerrt, aber jedes Land in der Ebene hat die genau gleichen Nachbarn wie auf der Sphäre und nur dies ist für die Anzahl der benötigten Farben relevant.



Stereographische Projektion. Die Länder auf der Kugeloberfläche werden in die Ebene projiziert.

Interessanterweise ist das analoge Färbungsproblem für Landkarten auf einem Torus (Abbildung links unten) viel einfacher zu lösen als jenes auf der Sphäre. Man kann beweisen, dass höchstens 7 Farben benötigt werden (rechte Abbildung): man erhält

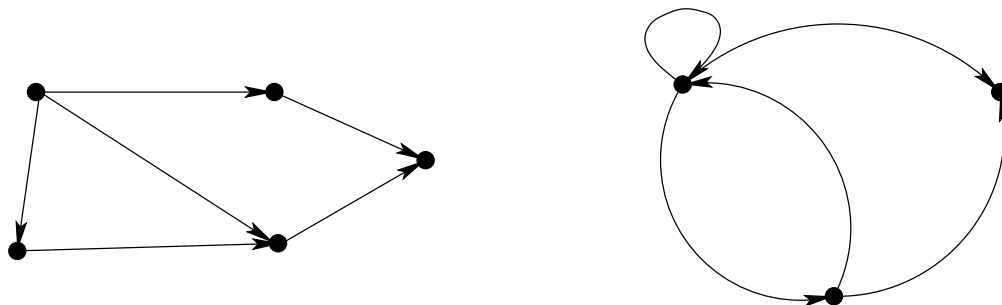
den Torus, indem man die Seiten mit den Doppelpfeilen zusammenfügt und so einen Zylinder erhält. Anschliessend werden die beiden Enden des Zylinders zusammengefügt (einfache Pfeile). (Quelle: Wikipedia)



2.14 Digraphen

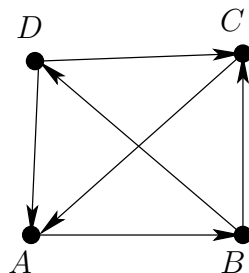
Ein **Digraph** oder **gerichteter Graph** besteht aus einer endlichen Menge V den Knoten, und einer Teilmenge A von $V \times V$, den gerichteten Kanten („arcs“ in Englisch). Wir schreiben $D = (V, A)$.

Digraphen können wie Graphen bildlich dargestellt werden. Der einzige Unterschied besteht darin, dass wir für die Kanten Pfeile verwenden. Falls (v, v) eine gerichtete Kante ist, stellen wir dies durch einen Loop dar.



Beachten Sie, dass formal ein Digraph einfach eine Relation auf der Menge V ist. Falls diese Relation symmetrisch ist, bedeutet dies, dass die gerichteten Kanten mit Ausnahme der Loops paarweise auftreten.

Bei Sportwettkämpfen gibt es manchmal Turniere, wo jeder gegen jeden spielt. Wir nehmen an, dass es bei jedem Spiel eine Siegerin bzw. einen Sieger gibt. Das heisst, es gibt kein Unentschieden. Den Ausgang des Turniers können wir dann durch einen Digraphen darstellen. Die Teilnehmerinnen und Teilnehmer bilden die Knoten. Wenn A gegen B gewinnt, dann zeichnen wir eine gerichtete Kante von A nach B . Wir erhalten so einen Digraphen. Dieser Digraph besitzt zwischen zwei Knoten genau eine Kante. Weiter besitzt er keine Loops.



Im obigen Graphen stellen wir fest, dass A gegen B gewonnen hat, B hat D besiegt und D hat C besiegt. Es gibt also einen gerichteten Pfad, der alle Knoten durchläuft. Dieses Resultat gilt allgemein:

Satz 21 *In jedem Turniergraphen gibt es (mindestens) einen gerichteten Weg, der durch alle Knoten führt.*

Beweis: Wir zeigen, dass wir jeden gerichteten Pfad

$$y_1, y_2, \dots, y_l,$$

der nicht alle Knoten enthält, durch Einfügung eines Knoten erweitern können.

Sei z ein Knoten, der nicht auf dem gerichteten Pfad liegt. Falls (z, y_1) eine gerichtete Kante des Graphs ist, fügen wir z am Anfang ein. Falls (z, y_1) keine gerichtete Kante ist, dann muss (y_1, z) eine gerichtete Kante sein. Wir bezeichnen mit r den grössten Index, wofür

$$(y_1, z), (y_2, z), \dots, (y_r, z)$$

gerichtete Kanten sind. Wir können dann z zwischen y_r und y_{r+1} einfügen.

□

Wir erhalten so eine Art Rangliste, die allerdings mit Vorsicht zu geniessen ist. Im oben abgebildeten Turniergraphen ist A am Anfang des gewichteten Pfads. Das bedeutet aber nicht, dass A gegen alle nachfolgenden Teilnehmerinnen und Teilnehmer gewinnt. In Tat und Wahrheit gewinnt A nur das Spiel gegen B und verliert die beiden andern Spiele!

Wir verstehen unter einem **Netzwerk** einen Digraphen $D = (V, A)$ mit einer Gewichtungsfunktion

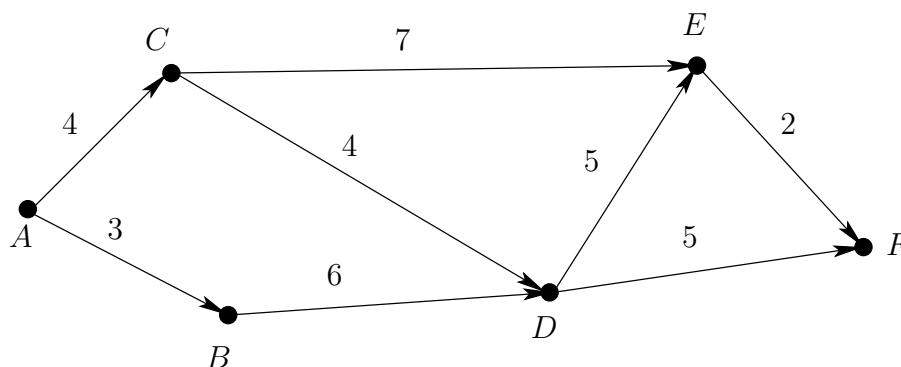
$$G : A \rightarrow \mathbb{N}.$$

Wir betrachten als Beispiel die Ausführung eines komplexen Projekts. Dieses wird in kleinere Teilprojekte zerlegt, welche untereinander in Beziehung stehen. Gewisse dieser Teilprojekte können nicht angefangen werden bevor andere abgeschlossen sind.

Aktivität	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8
Benötigte Zeit	4	3	7	4	6	5	2	5
Voraussetzung	-	-	α_1	α_1	α_2	α_4	α_3	α_4
						α_5	α_6	α_5

Wir müssen jetzt das zugehörige Netzwerk finden. Die Aktivitäten entsprechen gerichteten Kanten. Die Knoten entsprechen der Vollendung von gewissen Teilprojekten (Ereignisse). Die Knoten A und F entsprechen dem Start bzw. der Vollendung des Projekts.

Aktivität	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8
Gerichtete Kante	(A, C)	(A, B)	(C, E)	(C, D)	(B, D)	(D, E)	(E, F)	(D, F)



Wir berechnen jetzt für jeden Knoten v den frühesten Zeitpunkt $t(v)$, wo dieses Ereignis realisiert werden kann. Offensichtlich gilt $t(A) = 0$. Weiter sind $t(B) = 3$ und $t(C) = 4$. Es führen zwei Wege nach D . Der längere der beiden ist relevant:

$$t(D) = 9.$$

Weiter gilt

$$t(E) = \max(t(C) + 7, t(D) + 5) = \max(4 + 7, 9 + 5) = 14$$

und schliesslich

$$t(F) = \max(t(E) + 2, t(D) + 5) = \max(14 + 2, 9 + 5) = 16.$$

Die nachfolgende Tabelle enthält nochmals diese Resultate:

v	A	B	C	D	E	F
$t(V)$	0	3	4	9	14	16

Im vorhergehenden Problem musste also der *längste* Pfad durch das Netzwerk gefunden werden.

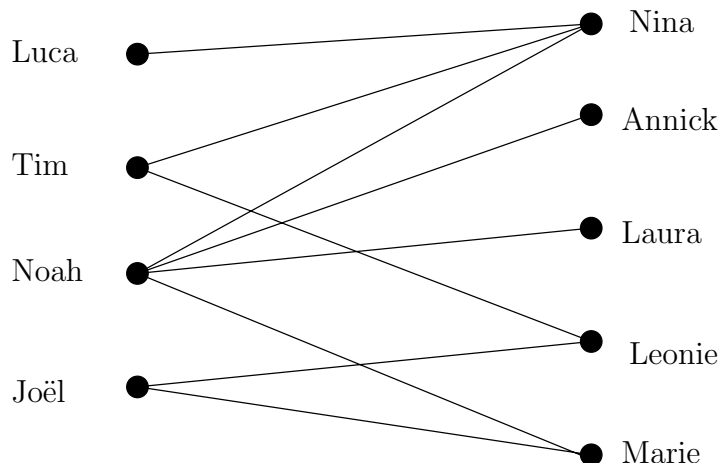
2.15 Bipartite Graphen

Wir betrachten zwei disjunkte Mengen X und Y sowie eine Relation R von X in Y (das heisst, R ist eine Teilmenge von $X \times Y$). Unter dem durch R definierten **bipartiten Graphen** verstehen wir den folgenden Graphen $G = (V, E)$:

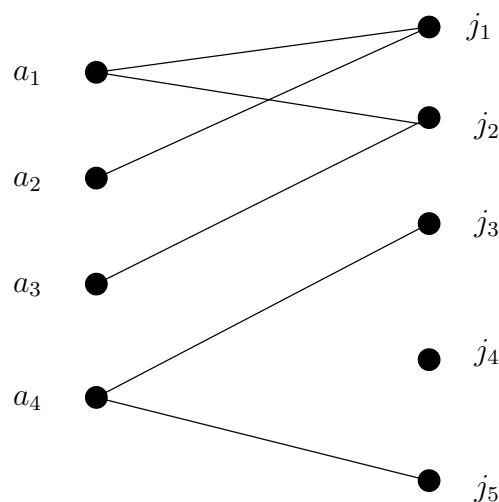
- Die Knotenmenge V ist die Vereinigung der Mengen X und Y ;
- xy ist genau dann eine Kante von G , wenn $(x, y) \in R$ ist.

Wir verwenden für bipartite Graphen die Bezeichnung $G = (X \cup Y, E)$.

Ein typisches Beispiel für einen bipartiten Graph finden wir in einem Heiratsinstitut. Die Menge X besteht aus den Männern, die Menge Y aus den Frauen. Falls ein Mann und eine Frau aufgrund ihrer Profile zusammenpassen, werden die Knoten durch eine Kante verbunden.



Eine Firma hat eine Reihe von offenen Stellen, für welche gewisse Qualifikationen notwendig sind. Man möchte die Stellenbewerberinnen und -bewerber nur für eine Stelle engagieren, für welche sie die Qualifikationen mitbringen. Ist es möglich jeder Bewerberin bzw. jedem Bewerber eine Stelle zuzuweisen?

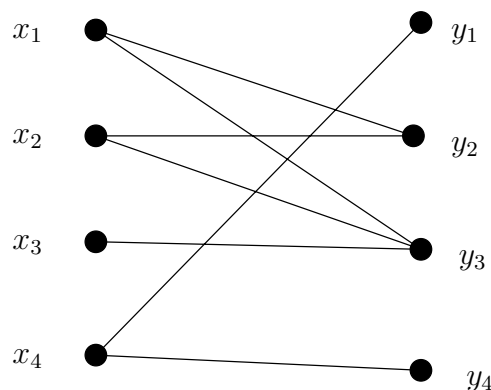


Definition 6 Sei $G = (X \cup Y, E)$ ein bipartiter Graph. Unter einer **Paarung** oder **Matching** versteht man eine Teilmenge M von E , so dass keine zwei Kanten einen gemeinsamen Knoten besitzen.

Die Paarung M heisst **maximal** für G , falls M durch Hinzunahme einer Kante keine Paarung mehr ist.

Die Paarung M heisst **perfekt**, wenn jeder Knoten aus X zu einer Kante von M gehört.

Beispiel 44 Zeichnen Sie im untenstehenden Graphen eine Paarung M_1 sowie eine maximale Paarung M_2 ein.



Die Aufgabe wird im Unterricht gelöst. ◇

Wir wollen uns jetzt der Frage zuwenden, wann es in einem bipartiten Graphen ein perfektes Matching gibt.

Halten wir uns zum Beispiel den Fall des Heiratsinstituts vor Augen mit der Menge X der Männer. Für jede Teilmenge A von X definieren wir die Menge:

$$J(A) = \{y \in Y \mid \text{die Kante } xy \text{ ist in } E \text{ für ein } x \text{ aus } A\}$$

Die Menge $J(A)$ ist also die Menge aller Frauen, die für die Männer in der Menge A in Frage kämen. Falls

$$|J(A)| < |A|$$

ist, dann geht mindestens ein Mann in A leer aus. Damit also ein perfektes Matching existiert, muss notwendigerweise

$$|J(A)| \geq |A|$$

für jede Teilmenge A von X gelten. Der sogenannte **Heiratssatz von Hall**¹¹ besagt, dass diese Bedingung notwendig und hinreichend ist:

Satz 22 *Der bipartite Graph $G = (X \cup Y, E)$ besitzt ein perfektes Matching, genau dann, wenn*

$$|J(A)| \geq |A| \quad \text{für jede Teilmenge } A \text{ von } X. \quad (7)$$

Bew.: Wir haben uns vorhin bereits überlegt, dass falls ein perfektes Matching existiert, dass dann die Bedingung (7) gelten muss.

Es gelte nun umgekehrt, die Bedingung (7). Wir wollen zeigen, dass ein perfektes Matching existiert. Sei M ein beliebiges Matching, mit weniger Kanten als es Knoten in X gibt. Wir wollen ein neues Matching M' konstruieren, das eine Kante mehr als M besitzt.

Sei x_0 irgendein Knoten aus X , der zu keiner Kante aus M gehört. Da

$$|J(x_0)| \geq |\{x_0\}| = 1$$

ist, gibt es eine Kante $x_0 y_1$, die von x_0 ausgeht. Falls die Kante $x_0 y_1$ nicht zu M gehört, fügen wir sie hinzu und erhalten so M' .

¹¹Philip Hall (1904-1982): englischer Mathematiker

Falls y_1 zu einer Kante aus M mit zweitem Knoten x_1 gehört, dann muss gelten:

$$|J(\{x_0, x_1\})| \geq |\{x_0, x_1\}| = 2$$

Damit existiert ein weiterer Knoten y_2 , der im Graph G durch eine Kante mit x_0 oder x_1 verbunden ist. Falls y_2 zu keiner Kante in M gehört, können wir abbrechen. Falls y_2 zu einer Kante in M mit zweitem Knoten x_2 gehört, dann gilt

$$|J(\{x_0, x_1, x_2\})| \geq |\{x_0, x_1, x_2\}| = 3$$

und wir können einen neuen Knoten y_3 finden, der im Graphen G mit mindestens einem der Knoten x_0, x_1 oder x_2 verbunden ist. Indem wir so weiterfahren, müssen wir den Algorithmus schliesslich bei einem Knoten y_r , der zu keiner Kante aus M gehört abbrechen, denn G ist endlich.

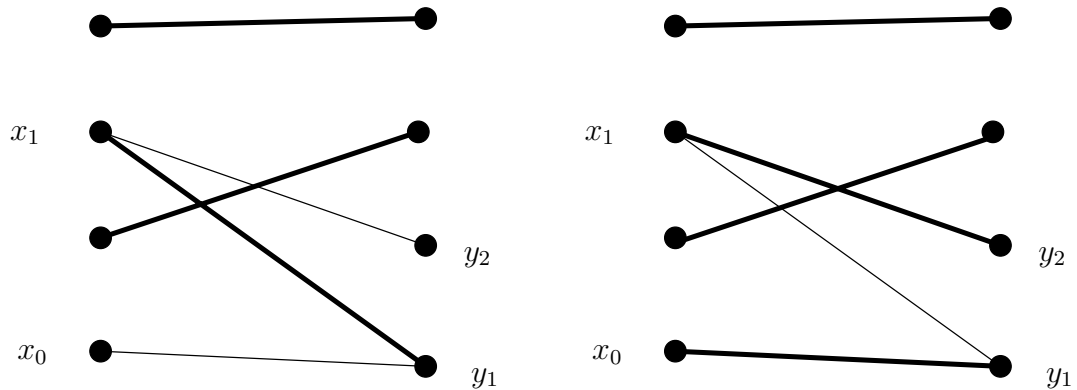
Jeder Knoten y_i ($1 \leq i \leq r$) ist zu mindestens einem der Knoten x_0, x_1, \dots, x_{i-1} verbunden. Indem wir unsere Schritte zurückverfolgen, erhalten wir einen Pfad

$$y_r, x_s, y_s, x_t, y_t, \dots, y_w, x_0,$$

in welchem die Kanten $x_i y_i$ zu M gehören, nicht aber die Kanten

$$y_r x_s, y_s x_t, \dots, y_w x_0. \quad (8)$$

Wir erhalten das neue Matching M' , indem wir in M die Kanten $x_i y_i$ ($1 \leq i \leq r$) durch die Kanten (8) ersetzen. Davon hat es eine Kante mehr.



□

Ein Graph heisst **regulär**, wenn jeder Knoten den gleichen Grad besitzt r besitzt. Wir können aus dem Heiratssatz eine einfache Schlussfolgerung für reguläre, bipartite Graphen ziehen.

Sei $G = (X \cup Y, E)$ ein regulärer, bipartiter Graph. Die Anzahl der Kanten ist dann einerseits $r|X|$ und andererseits $r|Y|$. Also gilt:

$$r|X| = r|Y| \implies |X| = |Y|$$

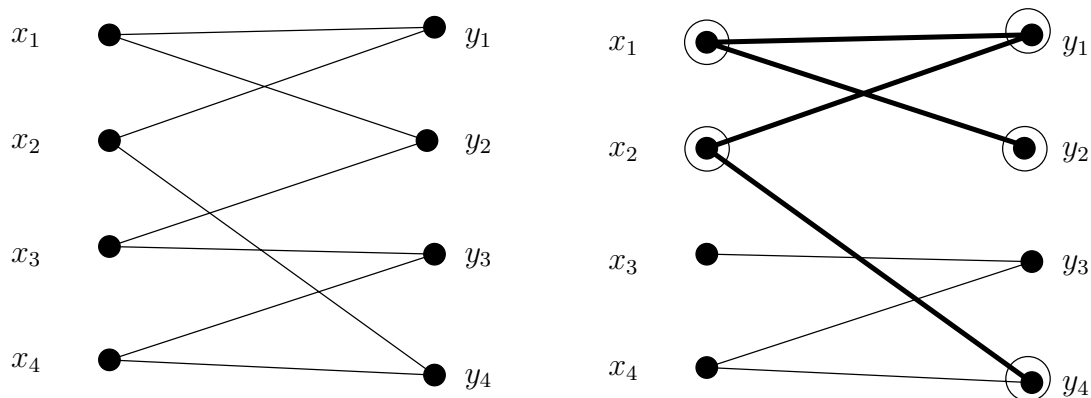
Die beiden Mengen müssen also die gleiche Anzahl Elemente enthalten. Wir betrachten jetzt eine beliebige Teilmenge A von X . Von dieser Menge gehen $r|A|$ Kanten aus. Diese Kanten treffen auf Knoten in der Menge Y , welche die Menge $J(A)$ bilden. Von den Knoten in der Menge $J(A)$ gehen sicher einmal die $r|A|$ Kanten aus, daneben aber eventuell noch weitere Kanten. Insgesamt sind es $r|J(A)|$ Kanten. Also gilt:

$$r|J(A)| \geq r|A| \implies |J(A)| \geq |A|$$

Dies ist aber die Bedingung des Heiratsatzes. Wir haben also den folgenden Satz:

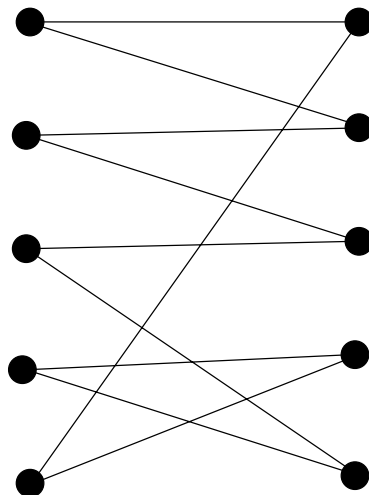
Satz 23 Ein regulärer, bipartiter Graph besitzt ein perfektes Matching. Dieses Matching berücksichtigt auch alle Knoten von Y .

In der nachfolgenden Abbildung ist links ein regulärer, bipartiter Graph mit $r = 2$ gezeichnet. Rechts ist $A = \{x_1, x_2\}$ und $J(A) = \{y_1, y_2, y_4\}$.



Wenn es also in der Datenbank des Heiratsinstituts gleich viele Männer wie Frauen hat und jeder Mann zu r Frauen passen würde und umgekehrt jede Frau zu r Männern, dann existiert ein Matching, das jedem Mann eine Frau zuordnet, die zu ihm passt und umgekehrt.

Beispiel 45 Finden Sie ein perfektes Matching im nachfolgenden Graphen:



Die Aufgabe wird im Unterricht gelöst.

◇

3 Rekursion

3.1 Folgen

Definition 7 Eine Funktion mit dem Definitionsbereich

$$A = \{x : x \in \mathbb{N} \wedge x \leq n\},$$

wo n eine gegebene natürliche Zahl ist, heisst **n -gliedrige Folge** oder auch **n -Tupel**. Eine Funktion mit dem Definitionsbereich $A = \mathbb{N}$ oder $A = \mathbb{N}_0$ heisst **unendliche Folge**.

Wir betrachten jetzt unendliche Folgen, welche kurz als Folgen bezeichnet werden. Bei einer Folge

$$\begin{aligned} a : \mathbb{N}_0 &\rightarrow \mathbb{R} \\ n &\rightarrow a(n) = a_n \end{aligned}$$

bezeichnet man den Funktionswert $a(n)$ als **n -tes Glied**. Man schreibt meistens a_n anstelle von $a(n)$. Die Folge a bezeichnen wir mit $(a_n)_{n \in \mathbb{N}_0}$ oder einfacher (a_n) .

Es gibt zwei Möglichkeiten, um eine Folge (a_n) zu definieren:

- (i) Das allgemeine Glied a_n ist als Funktion von n gegeben, zum Beispiel

$$a_n = \frac{n}{1+n^2}.$$

Man bezeichnet eine solche Formel als **explizite Formel**.

- (ii) Das n -te Glied ($n \geq 1$) ist als Funktion des $n-1$ -ten Glieds gegeben, z.B.

$$a_n = 2a_{n-1} + 1$$

Man bezeichnet eine solche Formel als **Rekursionsformel**. Damit die Folge eindeutig bestimmt ist, benötigen wir noch den Wert von a_0 , z.B.

$$a_0 = 1.$$

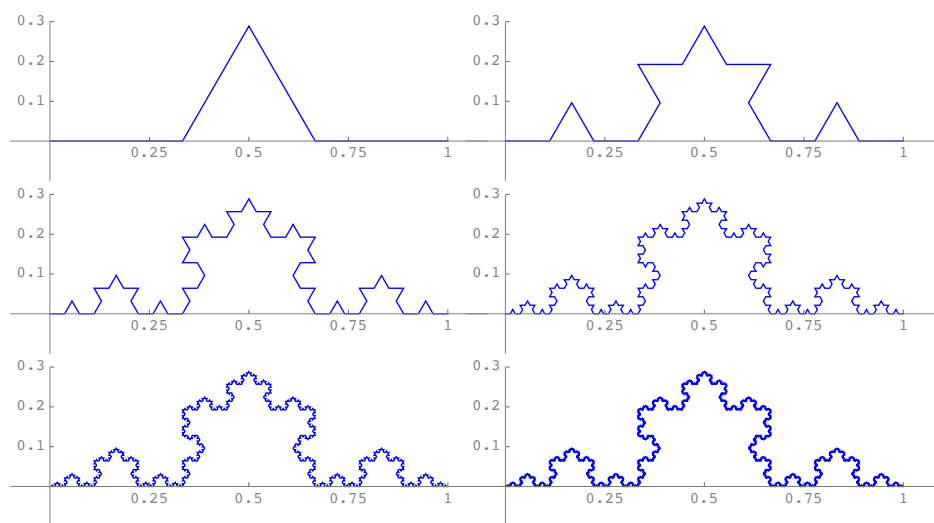
Wir können dann ein Glied nach dem andern berechnen:

$$\begin{aligned} a_1 &= 2a_0 + 1 = 2 \cdot 1 + 1 = 3 \\ a_2 &= 2a_1 + 1 = 2 \cdot 3 + 1 = 7 \\ a_3 &= 2a_2 + 1 = 2 \cdot 7 + 1 = 15 \\ a_4 &= 2a_3 + 1 = 2 \cdot 15 + 1 = 31 \\ &\vdots \quad \vdots \quad \vdots \end{aligned}$$

Natürlich ist es auch denkbar, dass a_n von a_{n-1} und a_{n-2} abhängt. Man sagt dann, dass die **Rekursionstiefe** 2 ist. In diesem Fall benötigen wir neben a_0 auch a_1 . Wir werden weiter unten ein Beispiel für eine solche Folge sehen.

In diesem Kapitel interessieren wir uns vor allem für Folgen, welche rekursiv definiert sind. Betrachten wir einige Beispiele:

- In der nachfolgenden Graphik gehen wir von der Einheitsstrecke aus. Die Rekursion besteht darin, dass wir in jeder Strecke den mittleren Abschnitt durch eine Ausbuchtung ersetzen, welche aus zwei Seiten eines gleichseitigen Dreiecks besteht:



- Definition der Fakultät für $n \in \mathbb{N}_0$:

$$\begin{aligned} 0! &= 1 \\ n! &= n \cdot (n-1)! \quad (n \in \mathbb{N}) \end{aligned}$$

- Definition der Binomialkoeffizienten für $n \in \mathbb{N}_0$ und $k \in \mathbb{N}_0$:

$$\begin{aligned} \binom{n}{0} &= 1 \\ \binom{n}{k} &= \binom{n}{k-1} \cdot \frac{n-k+1}{k} \quad (k \in \mathbb{N}) \end{aligned}$$

- Die **Fibonacci-Folge**. Leonardo Pisano, besser bekannt unter seinem Pseudonym Fibonacci (1170-1250), betrachtete im Jahre 1202 in seinem Buch „Liber Abaci“ das folgende idealisierte Modell des Wachstums einer Kaninchenpopulation:

- Zu Beginn gibt es ein Paar neugeborener Kaninchen.
- Jedes neugeborene Kaninchenpaar wirft nach 2 Monaten ein weiteres Paar.
- Anschließend wirft jedes Kaninchenpaar jeden Monat ein weiteres Paar.
- Die Kaninchen sterben nicht.

Wenn f_n die Anzahl der lebenden Paare nach n Monaten bezeichnet, so gilt:

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad (n \in \mathbb{N} \wedge n \geq 3) \end{aligned}$$

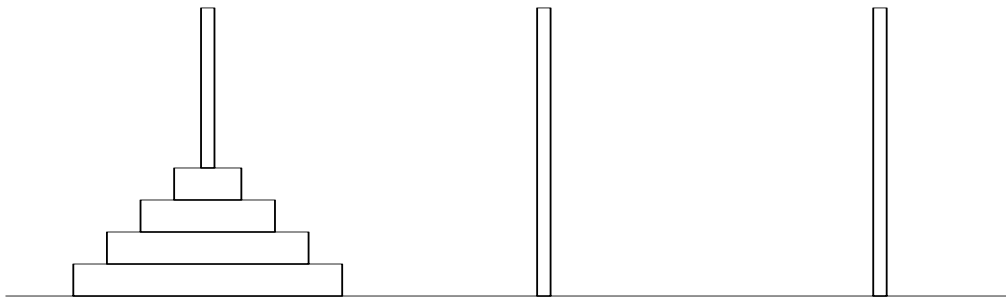
Wir geben einige Terme der Fibonacci-Folge an:

f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{20}	f_{50}
1	1	2	3	5	8	13	21	34	55	6'765	12'586'269'025

Wir geben noch den Term $f_{100} = 354'224'848'179'261'915'075$. Wir werden später sehen, dass die Fibonacci-Folge exponentiell wächst.

Beispiel 46 Beim Denkspiel *Die Türme von Hanoi* befinden sich auf einem Stab n verschieden grosse Scheiben, welche der Grösse nach angeordnet sind. Die Scheiben sollen in möglichst wenig Schritten auf einen der leeren Stäbe transferiert werden und zwar so, dass die Scheiben wieder der grösse nach angeordnet sind. In jedem Schritt darf nur eine Scheibe transferiert werden. Alle drei Stäbe dürfen zur Zwischlagerung benutzt werden, aber es darf nur eine kleinere Scheibe auf eine grössere gelegt werden.

Bestimmen Sie eine Rekursionsformel für die minimale Anzahl Schritte a_n , wobei n die Anzahl der Scheiben ist.



Die Aufgabe wird im Unterricht gelöst.

◇

3.2 Auflösung von Rekursionen

Manchmal ist es möglich für eine rekursiv definierte Folge eine explizite Darstellung des n -ten Gliedes zu finden. Betrachten wir das Beispiel mit den Fakultäten. Wie man leicht sieht, gilt:

$$n! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1 \quad (n \in \mathbb{N})$$

Dies zeigt, dass wir $n!$ in einem Programm mit einer **Schleife** berechnen können. Statt einer Rekursion haben wir dann eine **Iteration**, die weniger Speicherplatz benötigt.

Beispiel 47 Man beweise mittels vollständiger Induktion:

- (a) aus den Rekursionsformeln $a_1 = 1$, $a_n = 4a_{n-1} + 4^{n-1}$ folgt $a_n = n \cdot 4^{n-1}$ für alle natürliche Zahlen n .
- (b) aus den Rekursionsformeln $a_1 = 0$, $a_n = 4a_{n-1} + 4^{n-1}$ folgt $a_n = (n-1) \cdot 4^{n-1}$ für alle natürliche Zahlen n .

Die Aufgabe wird im Unterricht gelöst.

◇

Beispiel 48 Wir betrachten die folgende rekursiv definierte Folge:

$$\begin{aligned} a_0 &= c \\ a_n &= q \cdot a_{n-1} \quad (n \in \mathbb{N}) \end{aligned}$$

Jedes Glied entsteht also aus dem vorhergehenden Glied durch Multiplikation mit q . Man bezeichnet eine solche Folge als **geometrische Folge**.

Bestimmen Sie eine explizite Formel für a_n .

Die Aufgabe wird im Unterricht gelöst.

◇

Im Modul *Lineare Algebra* haben wir bereits eine explizite Formel für die Fibonacci-Folge hergeleitet. Im Folgenden werden wir eine andere Technik für diese Herleitung verwenden. Wir fragen uns, ob es geometrische Folgen gibt, welche die Rekursionsformel

$$f_n = f_{n-1} + f_{n-2} \quad (9)$$

erfüllen. Wir machen den Ansatz:

$$f_n = q^n ,$$

wobei q eine zu bestimmende reelle Zahl ist. Wenn wir diesen Ausdruck in die Rekursionsformel einsetzen, erhalten wir:

$$q^n = q^{n-1} + q^{n-2}$$

Wir lösen diese Gleichung nach q auf. Wir schaffen alle Terme auf die linke Seite und dividieren durch q^{n-2} :

$$q^n - q^{n-1} - q^{n-2} = 0 \implies q^2 - q - 1 = 0 \implies q_{1,2} = \frac{1 \pm \sqrt{(-1)^2 - 4(-1)}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

Also erfüllen die beiden geometrischen Folgen

$$a_n := q_1^n = \left(\frac{1 - \sqrt{5}}{2} \right)^n \quad \text{und} \quad b_n := q_2^n = \left(\frac{1 + \sqrt{5}}{2} \right)^n$$

die Rekursionsformel (9). Da diese **linear** ist, erfüllt auch die Linearkombination

$$c_n := k_1 \cdot a_n + k_2 \cdot b_n ,$$

mit $k_1, k_2 \in \mathbb{R}$ die Rekursionsformel. Wir bestimmen jetzt k_1 und k_2 so, dass die Anfangsbedingungen erfüllt sind, das heisst, dass gilt:

$$c_1 = 1 \quad \text{und} \quad c_2 = 1$$

Mit einem Trick können wir unsere Arbeit wesentlich vereinfachen und zu einem Gleichungssystem mit einfacheren Koeffizienten gelangen. Wir führen c_0 ein und verwenden die Anfangsbedingungen

$$c_0 = 0 \quad \text{und} \quad c_1 = 1$$

Aus der Rekursionsformel folgt dann $c_2 = c_0 + c_1 = 0 + 1 = 1$ und wir erhalten die gleiche Folge. Diese Folge ist **identisch** mit der Fibonacci-Folge. Mit den neuen Anfangsbedingungen ergibt sich das lineare Gleichungssystem:

$$\begin{cases} k_1 a_0 + k_2 b_0 &= 0 \\ k_1 a_1 + k_2 b_1 &= 1 \end{cases}$$

Wegen $a_0 = b_0 = 1$ folgt aus der ersten Gleichung $k_2 = -k_1$. Eingesetzt in die zweite Gleichung ergibt dies:

$$k_1 a_1 - k_1 b_1 = 1 \implies k_1 (a_1 - b_1) = 1 \implies k_1 = \frac{1}{a_1 - b_1}$$

Da

$$a_1 - b_1 = \left(\frac{1 - \sqrt{5}}{2} \right) - \left(\frac{1 + \sqrt{5}}{2} \right) = -\sqrt{5}$$

ist, folgt

$$k_1 = -\frac{1}{\sqrt{5}} \quad \text{und} \quad k_2 = \frac{1}{\sqrt{5}}.$$

Die explizite Formel für die Fibonacci-Folge lautet also:

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

Beachten Sie, dass f_n eine **natürliche Zahl** ist. Der Ausdruck auf der rechten Seite muss also auch eine natürliche Zahl sein, dies trotz den Koeffizienten und Basen, welche irrationale Zahlen sind.

Da

$$\left| \frac{1 - \sqrt{5}}{2} \right| < 1$$

strebt der zweite Term schnell gegen 0, wenn n gegen ∞ strebt. Man erkennt, dass die Fibonacci-Folge ein **exponentielles** Wachstum besitzt.

Wir erklären noch wie diese Formel mit einem Taschenrechner oder Computer mit Gleitzahlarithmetik verwendet werden kann. Der zweite Term ist bereits für $n = 2$ kleiner als 0.2. Es genügt also nur mit dem ersten Term zu arbeiten und diesen auf die nächste ganze Zahl zu runden. Also:

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

Wir führen einige Berechnungen mit einer 20-stelligen Mantissee durch:

$$\begin{array}{llll} f_{10} & = & \text{round}(55.003636123247413266) & = & 55 \\ f_{20} & = & \text{round}(6'765.0000295639318738) & = & 6'765 \\ f_{30} & = & \text{round}(832'040.00000024037306) & = & 832'040 \\ f_{40} & = & \text{round}(102'334'155.00000000195) & = & 102'334'155 \\ f_{50} & = & \text{round}(12'586'269'025.000000000) & = & 12'586'269'025 \end{array}$$

3.3 Rekursive Programmierung

Wir folgen in diesem Abschnitt der Darstellung in [4].

Als Beispiel für eine rekursive Programmierung betrachten wir die Berechnung der Glieder der Fibonacci-Folge:

```
function fib_rec(n: integer); integer;
begin
  if n <= 2 then
    return 1;
  else
    return fib_rec(n-1)+fib_rec(n-2);
  end;
end.
```

Sei T_n die Laufzeit für den Funktionsaufruf `fib_rec(n)`. Wir nehmen an, dass die Zeiteinheit so gewählt sei, dass $T(1) = T(2) = 1$ ist. Da `fib_rec(n)` die Funktionen `fib_rec(n-1)` und `fib_rec(n-2)` aufruft, gilt offenbar:

$$T_n \geq T_{n-1} + T_{n-2}$$

Das ist gleiche Beziehung wie für die Fibonacci-Zahlen mit dem Unterschied, dass wir anstelle des Gleichheitszeichens das „grösser-gleich“-Zeichen haben. Es folgt nun:

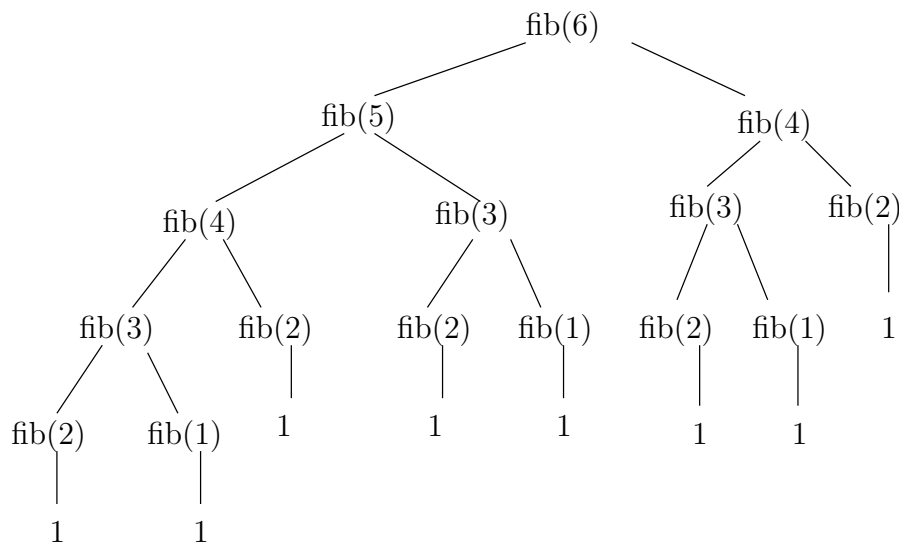
$$T_n \geq f_n$$

Der Zeitaufwand wächst also mindestens so schnell wie die Fibonacci-Zahlen. Wir wir gesehen haben, wächst (f_n) exponentiell. Angenommen die verwendete Zeiteinheit betrage eine Pico-Sekunde (10^{-12} sec.) Wir wollen T_{100} abschätzen. Es gilt:

$$T_{100} \geq 3.54 \cdot 10^{20} \text{ Pico-Sekunden}$$

Dies entspricht etwa 10.8 Jahren!

Der Grund für dieses exponentielle Wachstum der Laufzeit rührt daher, dass die beiden Funktionsaufrufe `fib_rec(n-1)` und `fib_rec(n-2)` unabhängig voneinander durchgeführt werden und der zweite nicht von den Zwischenergebnissen des ersten profitiert. Das wiederholt sich auf den nächsten Stufen, so dass viele Berechnungen mehrmals durchgeführt werden. Dies wird durch das nachfolgende Baumdiagramm sofort klar:



Die folgende *iterativ* definierte Funktion vermeidet diese Vergeudung:

```

function fib_it(n: integer): integer;
var
    f1, f2, temp, i: integer;
begin
    if n <= 2 then return 1 end;
    f1 := 1; f2 := 1;
    for i := 3 to n do
        temp := f2;
        f2 := f1 + f2;
        f1 := temp;
    end;
    return f2;
end.

```

In den Variablen **f1** und **f2** werden immer die beiden zuletzt berechneten, aufeinanderfolgenden Fibonacci-Zahlen gespeichert. Für die Berechnung von **fib(n)** wird die Schleife $n - 3$ -mal durchlaufen. Der Aufwand ist also proportional zu n .

Es gibt jedoch einen noch schnelleren Algorithmus. Wir schreiben die Rekursionsformel für f_{n+1} sowie die triviale Gleichung $f_n = f_n$ auf:

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ f_n &= f_n \end{aligned}$$

In Matrixschreibweise können wir dies folgendermassen schreiben:

$$\begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix}$$

Es folgt dann:

$$\begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = A \begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = A^2 \begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix} = A^3 \begin{pmatrix} f_{n-2} \\ f_{n-3} \end{pmatrix} \dots = A^n \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$$

Wir setzen wiederum $f_0 = 0$ und erhalten so die Beziehung:

$$\begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (10)$$

Wenn wir die vorhergehende Formel für $n - 1$ aufschreiben, erhalten wir:

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = A^{n-1} \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}.$$

Wir benützen jetzt, dass gilt

$$\begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = A \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

und erhalten so

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = A^n \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (11)$$

Wenn wir die beiden Beziehungen (10) und (11) kombinieren, erhalten wir:

$$\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = A^n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A^n$$

Wir ersetzen jetzt in dieser Beziehung n durch $2n$:

$$\begin{pmatrix} f_{2n+1} & f_{2n} \\ f_{2n} & f_{2n-1} \end{pmatrix} = A^{2n} = A^n A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

Aus

$$\begin{pmatrix} f_{2n+1} & f_{2n} \\ f_{2n} & f_{2n-1} \end{pmatrix} = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

folgt

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

und aus

$$\begin{pmatrix} f_{2n+1} & f_{2n} \\ f_{2n} & f_{2n-1} \end{pmatrix} = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

$$f_{2n} = f_n f_{n+1} + f_{n-1} f_n = f_n (f_n + f_{n-1}) + f_{n-1} f_n = f_n^2 + 2f_{n-1} f_n.$$

Wir haben damit den folgenden Satz bewiesen:

Satz 24 Für die Fibonacci-Zahlen f_n gelten die folgenden Formeln:

$$\begin{aligned} f_{2n-1} &= f_n^2 + f_{n-1}^2 \\ f_{2n} &= f_n^2 + 2f_{n-1} \cdot f_n \end{aligned} \quad (n \geq 2) \quad (12)$$

Wir zeigen wie die obigen Formeln zur schnellen Berechnung der Fibonacci-Zahlen verwendet werden können. Angenommen wir wollen f_{16} berechnen. Ausgehend von f_1 und f_2 berechnen wir mit Hilfe der obigen Formeln sukzessive

$$(f_1, f_2) \rightarrow (f_3, f_4) \rightarrow (f_7, f_8) \rightarrow (f_{15}, f_{16})$$

Die Schleife muss also nur $\log_2 16 = 4$ mal durchlaufen werden!

Wir betrachten jetzt den Fall, wo n keine 2-er Potenz ist. Sei Beispielsweise $n = 19$. Wir stellen $n = 19$ im Binärsystem dar:

$$n = (10011)_2$$

Wir betrachten jetzt die Folge von Binärzahlen:

$$10, 100, 1001, 10011$$

Jede dieser Zahlen entsteht aus der vorhergehenden entweder durch Multiplikation mit 2 oder durch Multiplikation mit 2 und Addition von 1, wenn das neu hinzukommende Bit gleich 1 ist. Die Fibonacci-Zahlen mit diesem Index können also gemäss den Formeln (12) berechnet werden, wobei die Zahlen f_{2n-1} und f_{2n} noch addiert werden müssen, wenn das neue Bit gleich 1 ist. Der nachfolgende Code implementiert diesen Algorithmus. Die Fibonacci-Folge beginnt hier mit $f_0 = 0$ und $f_1 = 1$.

```
function fib(n: integer): integer;
var
  k, x, y, xx, temp: integer;
begin
  if n <= 2 then return 1 end;
  x := 1; y := 0;
  for k := bit_length(n)-2 to 0 by -1 do
    xx := x*x;
    x := xx + 2*x*y;
    y := xx + y*y;
    if bit_test(n,k) then
      temp := x;
      x := x + y;
      y := temp;
    end;
  end;
  return x;
end.
```

In dieser Funktion enthalten die Variablen x und y jeweils nach dem Schleifendurchgang mit Index k die Werte $\text{fib}(n_k)$ und $\text{fib}(n_k-1)$. Die Funktion `fib` braucht zur Berechnung von $\text{fib}(n)$ nur $O(\log(n))$ Multiplikationen und Additionen. Allerdings werden natürlich die Zahlen mit wachsendem n immer grösser. Man muss eine Langzahlarithmetik verwenden, welche die Komplexität erhöht.

Rekursives Programm für die „Türme von Hanoi“

Nachfolgend eine rekursive Lösung für die „Türme von Hanoi“. Die n Scheiben müssen vom Stab **start** auf den Stab **finish** transferiert werden, wobei der Stab **temp** zur Zwischenspeicherung benützt werden darf. Das Programm basiert auf dem folgenden Algorithmus:

- (1) Wenn $n=1$ ist, dann wird die Scheibe von **start** nach **finish** transferiert.
- (2) Wenn $n > 1$ ist, geht man folgendermassen vor:
 - (i) Indem wir den gleichen Algorithmus verwenden, transferieren wir die obersten $n-1$ Scheiben von **start** nach **temp**. Der Stab **finish** wird in diesem Prozess als temporäres Zwischenlager benutzt.
 - (ii) Die unterste Scheibe wird von **start** nach **finish** transferiert.
 - (iii) Die obersten $n-1$ Scheiben werden von **temp** nach **finish** transferiert, wobei **start** als Zwischenlager verwendet wird.

```
procedure movetower(n : integer; start, finish, temp : char);  
  
begin  
  if n = 1 then  
    writeln(start, ' to ', finish)  
  else  
    begin  
      movetower(n-1, start, temp, finish);  
      writeln(start, ' to ', finish);  
      movetower(n-1, temp, finish, start);  
    end  
end;
```

Wenn wir diese Prozedur mit `movetower(3, 'a', 'b', 'c')` aufrufen, erhalten wir den vollständigen Ablauf:

```
a to b  
a to c  
b to c  
a to b  
c to a  
c to b  
a to b
```

3.3.1 Komplexität

Wir betrachten im Folgenden Funktionen f von \mathbb{N} in \mathbb{N} . Die folgende Definition gilt jedoch auch für Funktionen von \mathbb{R} in \mathbb{R} .

Will man zum Ausdruck bringen, dass eine Funktion $f(n)$ *höchstens so schnell wächst* wie eine Funktion $g(n)$ ($n \in \mathbb{N}$), so schreibt man:

$$f(n) = O(g(n))$$

Gelesen: „ $f(n)$ ist Gross-O von $g(n)$ “ Dies bedeutet, dass Konstanten $C \geq 0$ und $n_0 \in \mathbb{N}$ existieren, so dass für alle $n \geq n_0$ gilt:

$$|f(n)| \leq C \cdot |g(n)|$$

Die Ungleichung muss also nicht für alle $n \in \mathbb{N}$ gelten, sondern nur ab einem bestimmten Wert n_0 . Das Gleichheitszeichen muss mit Vorsicht interpretiert werden. Aus

$$f(n) = O(g(n)) \quad \text{und} \quad h(n) = O(g(n))$$

folgt natürlich **nicht**, dass $f(n) = h(n)$ ist.

Es gibt eine analoge Definition um auszudrücken, dass eine Funktion $f(n)$ mindestens so schnell wächst wie eine gegebene Funktion $g(n)$. Wir verfolgen dies jedoch nicht weiter.

Wir haben im Modul *Lineare Algebra* gesehen, dass der Gauss-Algorithmus

$$\frac{2n^3}{3} + \frac{3n^2}{2} - \frac{7n}{6} \text{ FLOPS}$$

benötigt, um ein lineares Gleichungssystem der Grösse $n \times n$ zu lösen.

Beispiel 49 Zeigen Sie, dass der Aufwand mit dem Gauss-Algorithmus zur Lösung eines $(n \times n)$ -Systems $O(n^3)$ ist.

Die Aufgabe wird im Unterricht gelöst. ◇

- Wird die Determinante einer $(n \times n)$ -Matrix rekursiv berechnet, indem man nach einer Zeile oder Spalte entwickelt, so ist der Rechenaufwand $O(n!)$. Der Supercomputer *Piz Daint* des *Swiss National Supercomputing Center* in Lugano gehört weltweit zu den 10 schnellsten Supercomputern. Pro Sekunde kann er 21.23 Petaflops (1 Petaflop = 10^{15} flops) ausführen. Dieser Computer würde für die rekursive Berechnung der Determinante einer Matrix der Ordnung 25 ungefähr 556 Jahre benötigen!
- Bei der Auswertung eines Polynoms n -ten Grades mit dem Horner-Algorithmus ist der Rechenaufwand $O(n)$. Man kann beweisen, dass der Horner-Algorithmus optimal ist, das heisst, es existiert kein anderer Algorithmus, mit welchem die Auswertung schneller durchgeführt werden kann.
- Die Multiplikation zweier $(n \times n)$ -Matrizen benötigt einen Aufwand $O(n^3)$.
- Im Modul *Diskrete Mathematik 1* haben wir gesehen, dass der euklidische Algorithmus zur Berechnung des ggT(a, b) höchstens $2 \log_2(2b)$ Divisionen mit Rest benötigt. Die Komplexität ist also $O(\log n)$. Der Algorithmus ist also sehr effizient! Wir zeigen jetzt noch, dass der Algorithmus nicht besser als $O(\log n)$ ist. Wir wählen für a und b zwei aufeinanderfolgende Fibonacci-Zahlen:

$$a = f_{n+1} \quad \text{und} \quad b = f_n$$

Aufgrund der Rekursionsformel der Fibonacci-Zahlen sind die Schritte des euklidischen Algorithmus gegeben durch:

$$\begin{aligned} f_{n+1} &= 1 \cdot f_n + f_{n-1} \\ f_n &= 1 \cdot f_{n-1} + f_{n-2} \\ f_{n-1} &= 1 \cdot f_{n-2} + f_{n-3} \\ &\vdots \\ f_4 &= 1 \cdot f_3 + f_2 \\ f_3 &= 2 \cdot f_2 \end{aligned}$$

Mit Ausnahme des letzten Schritts ist q_i stets 1. Wir benötigen $n - 1$ Divisionen mit Rest. Aufgrund der expliziten Formel wissen wir, dass

$$b \approx \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n = c \cdot D^n ,$$

wobei

$$c = \frac{1}{\sqrt{5}} \quad \text{und} \quad D = \frac{1 + \sqrt{5}}{2}$$

ist. Indem wir diese Beziehung logarithmieren, erhalten wir:

$$\ln b \approx \ln c + n \cdot \ln D$$

und damit:

$$n \approx \frac{\ln b - \ln c}{\ln D}$$

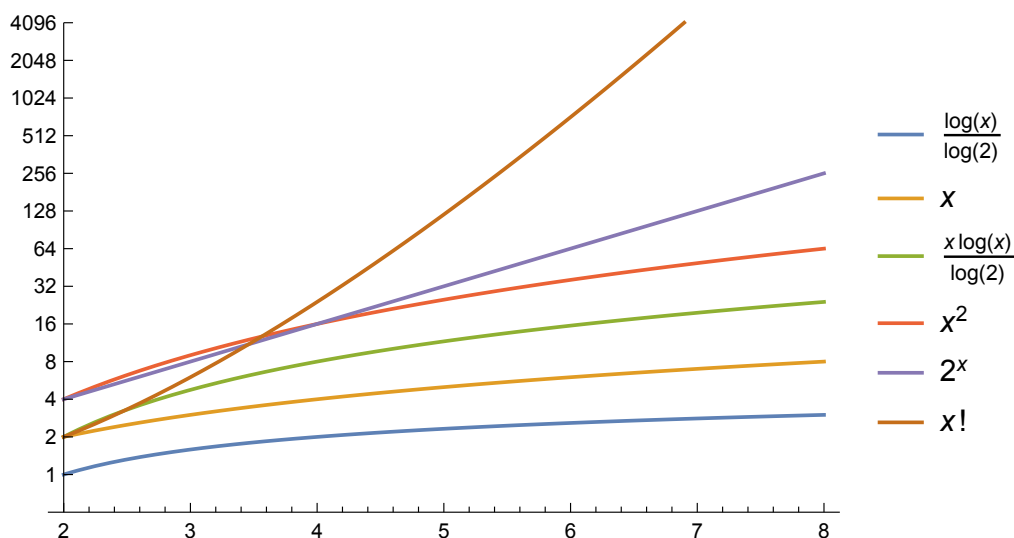
Daraus folgt, dass die Komplexität des euklidischen Algorithmus nicht besser als $O(\log b)$ sein kann.

- Die schnelle Fourier-Transformation (FFT, Fast Fourier Transformation) ist ein unentbehrliches Werkzeug in der Signal- und Bildverarbeitung. Der Aufwand der FFT ist $O(n \log n)$, falls die Länge der Folge, n , eine 2-er Potenz ist. Der naive Algorithmus besitzt eine Komplexität von $O(n^2)$.

Die folgende Tabelle enthält wichtige Komplexitätsklassen. Der Parameter $n \in \mathbb{N}$ definiert die Grösse des Problems, also z.B. die Ordnung einer Matrix, der Grad eines Polynoms, etc. :

$O(1)$	konstanter Aufwand
$O(\log n)$	logarithmischer Aufwand
$O(n)$	linearer Aufwand
$O(n \log n)$	Aufwand $n \log n$
$O(n^b)$ ($b \in \mathbb{N}$)	polynomialer Aufwand
$O(b^n)$ ($b \in \mathbb{R}$, $b > 1$)	exponentieller Aufwand
$O(n!)$	faktorieller Aufwand

Die nachfolgende Graphik zeigt das Wachstum dieser Funktionen, wobei auf der y -Achse ein **logarithmischer Massstab** verwendet wird. Wir weisen noch darauf hin, dass $\log x / \log 2 = \log_2 x$ ist:



In der nachfolgenden Tabelle ([9], [10]) steht n für die Grösse des Problems (Grösse der Matrix, Länge eines Tupels, Grad eines Polynoms, etc.). Wir nehmen an, dass der Aufwand an elementaren Operationen zur Lösung des Problems gleich einer der angegebenen Funktionen ist. Wenn jede dieser Operationen eine Nanosekunde ($= 10^{-9}$ s) in Anspruch nimmt, dann entsprechen die angegebenen Zahlen der Zeit, die für die Lösung des Problems benötigt wird. Man erkennt das unglaubliche Wachstum der Funktionen 2^n und $n!$:

Grösse n	Zeitaufwand					
	$\log_2 n$	n	$n \log_2 n$	n^2	2^n	$n!$
10	3.3×10^{-9} s	10^{-8} s	3.3×10^{-8} s	10^{-7} s	1.0×10^{-6} s	3.6×10^{-3} s
10^2	6.6×10^{-9} s	10^{-7} s	6.6×10^{-7} s	10^{-5} s	4×10^{13} Jahre	$> 10^{100}$ Jahre
10^3	1.0×10^{-8} s	10^{-6} s	1×10^{-5} s	10^{-3} s	$> 10^{100}$ Jahre	$> 10^{100}$ Jahre
10^4	1.3×10^{-8} s	10^{-5} s	1.3×10^{-4} s	10^{-1} s	$> 10^{100}$ Jahre	$> 10^{100}$ Jahre
10^5	1.7×10^{-8} s	10^{-4} s	1.7×10^{-3} s	10 s	$> 10^{100}$ Jahre	$> 10^{100}$ Jahre
10^6	2.0×10^{-8} s	10^{-3} s	2×10^{-2} s	17 Min.	$> 10^{100}$ Jahre	$> 10^{100}$ Jahre

4 Gruppentheorie

4.1 Die Diedergruppe D_3

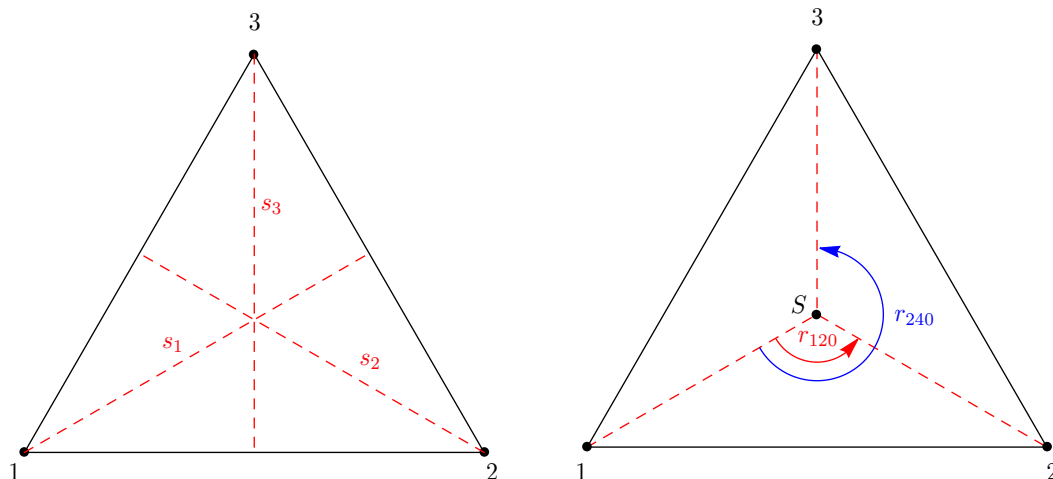
Unter einer **Isometrie** der Ebene \mathbb{R}^2 versteht man eine bijektive Abbildung $F(\vec{x})$ der Ebene auf sich, welche die Abstände nicht verändert. Konkret, wenn P und Q zwei beliebige Punkte der Ebene sind, dann muss gelten

$$\|F(P) - F(Q)\| = \|P - Q\|.$$

Man kann zeigen, dass es nur die folgenden drei Typen von Isometrien der Ebene gibt:

- (1) Translation: Parallelverschiebung um einen Vektor $\vec{a} : F(\vec{x}) = \vec{x} + \vec{a}$
- (2) Rotation um einen Punkt P mit einem Winkel α .
- (3) Spiegelung an einer Geraden g .
- (4) Gleitspiegelung: Hintereinanderschaltung (Komposition, Verkettung) einer Spiegelung an einer Geraden g mit einer Verschiebung um einen zu g parallelen Vektor $\vec{a} \neq \vec{0}$.

Wir betrachten jetzt ein **gleichseitiges** Dreieck und interessieren uns für die Isometrien, welche dieses Dreieck auf sich abbilden.



Die folgenden Isometrien leisten das Gewünschte:

- (1) Die identische Abbildung $\text{id}(\vec{x}) = \vec{x}$. Wir erhalten aus den obigen Isometrien diese Abbildung, wenn wir eine Rotation um den Schwerpunkt S um ein Vielfaches von 360° ausführen.
- (2) Die Spiegelungen s_i ($i = 1, 2, 3$) an einer der 3 Winkelhalbierenden.
- (3) Die Drehungen um den Schwerpunkt S mit den Winkeln 120° oder 240° .

Es handelt sich um insgesamt 6 Abbildungen. Es kann keine weiteren Abbildungen mehr geben, denn jede Isometrie, welches das Dreieck auf sich abbildet, permutiert die 3 Eckpunkte. Es gibt aber nur $3! = 6$ Permutationen von 3 Elementen. Beachten Sie, dass eine Permutation σ der Menge $M = \{1, 2, 3\}$ eine bijektive Abbildung von M auf sich ist. Wir verwenden die folgende Notation, um σ zu beschreiben:

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

In der zweiten Zeile geben wir jeweils das Bild der darüberstehenden Elemente an.

Wir beschreiben jetzt die 6 Isometrien durch die Permutationen der Eckpunkte. Es gilt:

$$\text{id} \hat{=} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Für die 3 Spiegelungen erhalten wir:

$$s_1 \hat{=} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad s_2 \hat{=} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad s_3 \hat{=} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Die beiden Rotationen mit den Drehwinkeln von 120° bzw. 240° entsprechen den beiden folgenden Permutationen:

$$r_{120} \hat{=} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad r_{240} \hat{=} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Wir bezeichnen die Menge dieser 6 Isometrien mit G :

$$G := \{\text{id}, s_1, s_2, s_3, r_{120}, r_{240}\}$$

Wir betrachten jetzt auf der Menge G der 6 Isometrien als Operation die Hintereinanderschaltung \circ (Komposition, Verkettung) von Abbildungen. Die nachfolgende Tabelle gibt für das Zeilenelement $x \in G$ und das Kolonnenelement $y \in G$ die Hintereinanderschaltung von x gefolgt von y , $y \circ x$, an:

\circ	id	s_1	s_2	s_3	r_{120}	r_{240}
id	id	s_1	s_2	s_3	r_{120}	r_{240}
s_1	s_1	id	r_{240}	r_{120}	s_3	s_2
s_2	s_2	r_{120}	id	r_{240}	s_1	s_3
s_3	s_3	r_{240}	r_{120}	id	s_2	s_1
r_{120}	r_{120}	s_2	s_3	s_1	r_{240}	id
r_{240}	r_{240}	s_3	s_1	s_2	id	r_{120}

Wir können die folgenden Feststellungen machen:

- (1) Die Hintereinanderschaltung zweier Elemente aus G ergibt wiederum ein Element aus G . Man sagt, dass die Operation \circ in G **abgeschlossen** sei.
- (2) Die Operation \circ ist **assoziativ**, das heisst, es gilt für $f, g, h \in G$:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

- (3) Wenn f ein beliebiges Element von G bezeichnet, so gilt:

$$f \circ \text{id} = \text{id} \circ f = f$$

Man sagt, dass id ein **Neutralelement** der Operation \circ sei.

- (4) Zu jedem $f \in G$ existiert ein $f^{-1} \in G$, so dass gilt

$$f \circ f^{-1} = f^{-1} \circ f = \text{id}$$

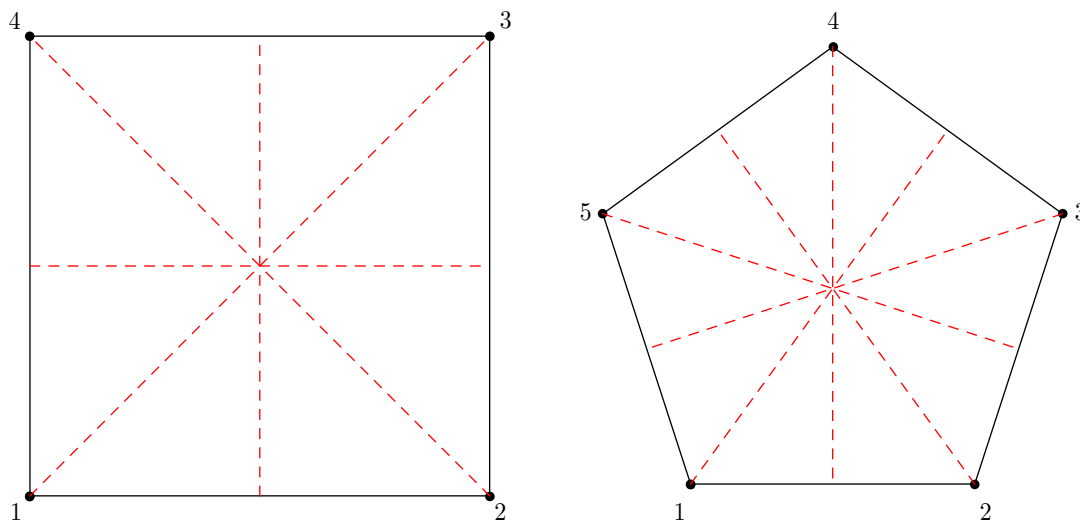
Man bezeichnet f^{-1} als das **inverse Element** von f .

Aufgrund dieser 4 Eigenschaften sagt man, dass G versehen mit der Operation \circ eine **Gruppe** bilde. Man bezeichnet diese Gruppe als **Diedergruppe** D_3 .

Beachten Sie, dass die Operation \circ nicht kommutativ ist. Es ist beispielsweise

$$s_1 \circ s_2 \neq s_2 \circ s_1 .$$

Beispiel 50 Bestimmen Sie alle Isometrien, die ein Quadrat bzw. ein regelmässiges 5-Eck auf sich abbilden. Wir erhalten so die Diedergruppen D_4 und D_5 .



Die Aufgabe wird im Unterricht gelöst.

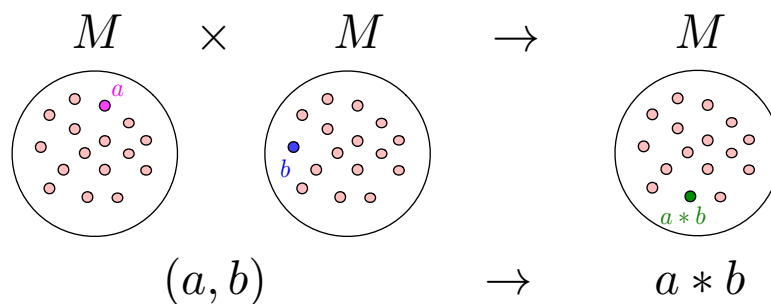
◇

4.2 Der allgemeine Gruppenbegriff

Sei M eine nichtleere Menge. Unter einer internen Operation $*$ in M versteht man eine Abbildung von $M \times M$ in M :

$$\begin{aligned} * : M \times M &\rightarrow M \\ (a, b) &\rightarrow a * b \end{aligned}$$

Da das Resultat von $a * b$ in M liegt, sagt man, die Operation $*$ sei **abgeschlossen** in M .



Definition 8 Sei G eine nichtleere Menge versehen mit einer internen Operation $*$. $(G, *)$ ist eine **Gruppe**, wenn die folgenden Bedingungen erfüllt sind:

(G1) Die Operation $*$ ist **assoziativ**, das heisst, es gilt für alle $a, b, c \in G$:

$$(a * b) * c = a * (b * c)$$

(G2) Es existiert ein Element $e \in G$, so dass für alle $a \in G$ gilt:

$$e * a = a * e = a$$

Man bezeichnet e als **Neutralelement** von G . Wir werden zeigen, dass dieses Element eindeutig bestimmt ist.

(G3) Zu jedem $a \in G$ existiert ein Element $a^{-1} \in G$, wofür gilt:

$$a^{-1} * a = a * a^{-1} = e$$

Man bezeichnet a^{-1} als das **Inverse** von a . Wir werden zeigen, dass das Inverse eines Elements a eindeutig bestimmt ist.

$(G, *)$ heisst **kommutativ** oder **abelsch**¹², wenn zusätzlich für alle $a, b \in G$ gilt:

$$a * b = b * a$$

Bemerkungen:

- Normalerweise schreibt man die Verknüpfung $*$ als Multiplikation „ \cdot “:

$$a \cdot b \quad \text{oder ohne Punkt} \quad ab$$

Das Neutralelement e wird manchmal mit 1 bezeichnet und heisst dann Einselement. Beachten Sie bitte, dass es sich dabei um ein Symbol handelt, das nichts mit der Zahl 1 zu tun haben muss.

Falls die Gruppe kommutativ ist, schreibt man die Gruppenoperation oft als Addition $a + b$. Das Neutralelement wird dann mit 0 (Null) bezeichnet und das inverse Element von a mit $-a$. Auch hier handelt es sich bei 0 um ein Symbol, das nichts mit der Zahl 0 zu tun haben muss.

- Mithilfe eines Induktionsbeweises kann man zeigen, dass das Assoziativgesetz für eine beliebige Anzahl von Faktoren und beliebige Klammerungen gültig ist.

Die **Ordnung** einer Gruppe (G, \cdot) , geschrieben $|G|$, ist die Anzahl Elemente der Gruppe. Diese kann natürlich auch unendlich sein.

Beispiele für Gruppen

- Die Menge der ganzen Zahlen versehen mit der Addition $(\mathbb{Z}, +)$ ist eine abelsche Gruppe. Das Neutralelement ist die Zahl 0 und das Inverse zu a ist die Gegenzahl $-a$.

¹²Niels Henrik Abel (1802-1829): norwegischer Mathematiker. Abel bewies, dass es keine Formel für die allgemeine Gleichung 5. Grades oder höher mehr gibt, in welcher nur die Grundoperationen und verschachtelte Wurzelausdrücke vorkommen.

- Die Menge der invertierbaren reellen 2×2 -Matrizen versehen mit der Matrixmultiplikation ist eine Gruppe. Das Neutralelement ist die Einheitsmatrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Das Inverse einer invertierbaren Matrix

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

ist die inverse Matrix

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

Beachten Sie, dass diese Gruppe **nicht** kommutativ ist.

Allgemein bilden die invertierbaren, reellen $n \times n$ -Matrizen bezüglich der Multiplikation eine Gruppe. Diese wird mit $GL(n, \mathbb{R})$ (General Linear Group, die allgemeine lineare Gruppe) bezeichnet.

- Sei n eine natürliche Zahl. Wir betrachten die Menge $M = \{1, 2, \dots, n\}$. Die Menge der bijektiven Abbildungen von M auf sich bildet bezüglich der Hintereinanderschaltung (Komposition) eine Gruppe. Das Neutralelement ist die identische Abbildung id_M :

$$\begin{aligned} \text{id}_M : M &\rightarrow M \\ x &\rightarrow \text{id}_M(x) = x \end{aligned}$$

Das inverse Element einer Abbildung $f : M \rightarrow M$ ist die inverse Abbildung f^{-1} . Die Hintereinanderschaltung von Abbildungen ist assoziativ:

$$(h \circ (g \circ f))(x) = h(g(f(x))) \quad \text{und} \quad ((h \circ g) \circ f)(x) = h(g(f(x)))$$

Man bezeichnet eine bijektive Abbildung von M auf sich selbst als **Permutation** von M . Die Gruppe der Permutationen von M wird als **symmetrische Gruppe** S_n bezeichnet. Die Ordnung der Gruppe S_n beträgt $n!$.

Wir betrachten jetzt einige allgemeine Resultate für Gruppen, welche aus den Axiomen (G1)-(G3) folgen:

Satz 25 Seien $a, b, x \in G$ beliebige Elemente einer Gruppe G . Dann gilt:

$$xa = xb \implies a = b \quad (\text{Linkskürzung})$$

und

$$ax = bx \implies a = b \quad (\text{Rechtskürzung})$$

Bew.: Wir multiplizieren die erste Gleichung mit x^{-1} :

$$\begin{aligned} x^{-1}(xa) &= x^{-1}(xb) \\ (x^{-1}x)a &= (x^{-1}x)b && (\text{gemäß G1}) \\ ea &= eb && (\text{gemäß G3}) \\ a &= b && (\text{gemäß G2}) \end{aligned}$$

Der Beweis der zweiten Aussage geht analog.

□

Satz 26 Seien a und b zwei beliebige Elemente einer Gruppe G . Dann besitzen die Gleichungen

$$ax = b \quad (13)$$

und

$$xa = b \quad (14)$$

eine eindeutige Lösung in G .

Bew.: Wir beweisen die Aussage nur für die Gleichung (13). Wir zeigen zuerst die Eindeutigkeit. Angenommen x und x' seien zwei Lösungen der Gleichung (13):

$$ax = b \quad \text{und} \quad ax' = b$$

Es folgt dann

$$ax = ax'$$

Mit der Linkskürzung folgt dann $x = x'$.

Wir zeigen als nächstes die Existenz einer Lösung. Wenn wir die Gleichung (13) mit a^{-1} multiplizieren, erhalten wir:

$$x = a^{-1}b$$

Dies ist eine Lösung der Gleichung.

□

Beispiel 51 Verwenden Sie den vorhergehenden Satz um zu beweisen, dass in einer Gruppe (G, \cdot) das Neutralelement e eindeutig ist und für jedes Element $a \in G$ das Inverse a^{-1} ebenfalls eindeutig ist.

Die Aufgabe wird im Unterricht gelöst.

◇

Die gleiche Gruppe kann in verschiedenen Ausprägungen vorkommen. Man sagt dann die Gruppen seien **isomorph**. Wir haben bereits gesehen, dass die Diedergruppe D_3 und die Gruppe der Permutationen von 3 Elementen, S_3 , sich entsprechen.

Formal sind zwei Gruppen $(G_1, *)$ und $(G_2, *')$ **isomorph**, wenn eine bijektive Abbildung $\phi : G_1 \rightarrow G_2$ existiert, so dass gilt:

$$\phi(a * b) = \phi(a) *' \phi(b) \quad (\forall a, b \in G_1) \quad (15)$$

Die Abbildung ϕ heisst **Isomorphismus**. Eine Abbildung von $\phi : G_1 \rightarrow G_2$, welche nicht bijektiv ist, aber die Bedingung (15) erfüllt, nennt man einen **Homomorphismus**. Homomorphismen erhalten die Gruppenstruktur.

Beispiel 52 Sei ϕ ein Isomorphismus zwischen den Gruppen G_1 und G_2 mit den Neutralelementen e und e' . Zeigen Sie, dass

$$\phi(e) = e' \quad \text{und} \quad \phi(a^{-1}) = (\phi(a))^{-1}$$

ist.

Die Aufgabe wird im Unterricht gelöst.

◇

Beispiel 53 Wir betrachten die Gruppen $G_1 := (\mathbb{R}, +)$ und $G_2 := (\mathbb{R}^+, \cdot)$. Zeigen Sie, dass die Abbildung

$$\begin{array}{ccc} \exp : \mathbb{R} & \rightarrow & \mathbb{R}^+ \\ x & \rightarrow & e^x \end{array}$$

ein Isomorphismus ist. Die inverse Abbildung ist dann natürlich auch ein Isomorphismus. Wie lautet diese?

Die Aufgabe wird im Unterricht gelöst. \diamond

Für kleine Werte der Ordnung n werden wir jetzt untersuchen, welche Gruppen es bis auf Isomorphie gibt.

Wir betrachten im Folgenden sogenannte Verknüpfungstabellen für **endliche** Gruppen. Wenn $G = \{e, a, b, c\}$ ist, dann lautet die Verknüpfungstabelle (F: table de Cayley):

\cdot	e	a	b	c
e	$e \cdot e$	$e \cdot a$	$e \cdot b$	$e \cdot c$
a	$a \cdot e$	$a \cdot a$	$a \cdot b$	$a \cdot c$
b	$b \cdot e$	$b \cdot a$	$b \cdot b$	$b \cdot c$
c	$c \cdot e$	$c \cdot a$	$c \cdot b$	$c \cdot c$

Wir geben also alle möglichen Verknüpfungen an.

Sei a ein beliebiges Element einer Gruppe G . Wir haben im Satz 26 gesehen, dass die Gleichungen

$$a \cdot x = b \quad \text{und} \quad x \cdot a = b$$

für jedes b eine eindeutige Lösung besitzen. Dies bedeutet, dass die beiden Abbildungen

$$\begin{array}{ccc} G & \rightarrow & G \\ x & \rightarrow & a \cdot x \end{array}$$

und

$$\begin{array}{ccc} G & \rightarrow & G \\ x & \rightarrow & x \cdot a \end{array}$$

bijektiv sind, d.h., die Elemente von G werden einfach permutiert. Dies hat zur Folge, dass in jeder Zeile und jeder Spalte der Verknüpfungstabelle alle Elemente von G genau einmal auftreten müssen. Verknüpfungstabellen für Gruppen sind sogenannte **lateinische Quadrate**.

- Für $n = 1$ gibt es nur eine Gruppe. Diese enthält das neutrale Element e .
- Für $n = 2$ gibt es ebenfalls nur eine Gruppe.

\cdot	e	a
e	e	a
a	a	e

Die Verknüpfung ist kommutativ. Für das Assoziativgesetz müssen wir die Gleichungen

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

überprüfen. Da wir für x, y und z zwei Elemente einsetzen können, müssen wir $2^3 = 8$ Gleichungen überprüfen. Wir verzichten darauf und begnügen uns mit der Feststellung, dass sie erfüllt sind.

- Für $n = 3$ gibt es ebenfalls nur eine Gruppe. Die Verknüpfungstafel sieht folgendermassen aus:

\cdot	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Da die Tabelle symmetrisch zur Diagonalen ist, ist die Verknüpfung wiederum kommutativ. Beachten Sie, dass die zweite Möglichkeit

$$a \cdot a = e \quad \text{und} \quad a \cdot b = b$$

zur Folge hätte, dass $a = e$ ist. Sie kommt also nicht infrage.

Für das Assoziativgesetz müssen jetzt $3^3 = 27$ Gleichungen überprüft werden. Diese sind wiederum erfüllt.

Wir stellen fest, dass $a^2 = b$ und $a^3 = a \cdot a^2 = a \cdot b = e$ ist. Die Gruppe G ist also gleich

$$G = \{a, a^2, a^3\}.$$

Man bezeichnet eine solche Gruppe als **zyklisch**.

- Man kann zeigen, dass es für $n = 4$ nur die folgenden zwei Möglichkeiten gibt:

\cdot	e	a	b	c		$*$	e	a	b	c
e	e	a	b	c		e	e	a	b	c
a	a	b	c	e	und	a	a	e	c	b
b	b	c	e	a		b	b	c	e	a
c	c	e	a	b		c	c	b	a	e

Die linke Gruppe ist wiederum zyklisch:

$$a^2 = b, \quad a^3 = a \cdot a^2 = a \cdot b = c, \quad a^4 = a^2 \cdot a^2 = b \cdot b = e$$

Also ist

$$G = \{a, a^2, a^3, a^4\}.$$

Die rechte Gruppe heisst **Kleinsche¹³ Vierergruppe** \mathcal{K}_4 . Jedes Element ist invers zu sich selbst.

Wenn weitere theoretische Resultate verfügbar sind, werden wir die Liste weiterführen.

4.3 Untergruppen

Wir führen jetzt das wichtige Konzept einer **Untergruppe** ein. Betrachten wir die Kleinsche Vierergruppe. Wir stellen fest, dass die Teilmenge $H = \{e, a\}$ unter der Gruppenoperation selbst eine Gruppe bildet. Das Axiom (G1) ist erfüllt, da das Assoziativgesetz in der Kleinschen Vierergruppe erfüllt ist. Weiter enthält die Teilmenge H das Neutralelement e und das zu a inverse Element $a^{-1} = a$. Man bezeichnet H als Untergruppe von G .

Definition 9 Sei H eine nichtleere Teilmenge von G . H heisst **Untergruppe** von G , geschrieben $H < G$, wenn die folgenden Bedingungen erfüllt sind:

¹³Felix Klein (1849-1925): deutscher Mathematiker

(U1) H ist abgeschlossen unter \cdot , das heisst, mit $a, b \in H$ ist $a \cdot b$ in H .

(U2) H ist mit der Operation \cdot selbst eine Gruppe.

Der folgende Satz ist nützlich um zu entscheiden, ob eine Teilmenge H einer Gruppe G eine Untergruppe ist.

Satz 27 Sei H eine nichtleere Teilmenge von G . H ist genau dann eine Untergruppe von G , wenn gilt:

$$a, b \in H \implies ab^{-1} \in H \quad (16)$$

Bew.: Wir müssen zwei Richtungen beweisen. Wir betrachten zuerst den Fall, wo H eine Untergruppe ist. Seien also $a, b \in H$. Da H eine Gruppe ist, muss b^{-1} in H sein. Da \cdot in H abgeschlossen ist, muss $a \cdot b^{-1}$ in H sein. Damit haben wir (16) gezeigt.

Es gelte jetzt umgekehrt die Bedingung (16). Da H nicht die leere Menge ist, gibt es ein $a \in H$. Wir wenden (16) auf a und $b = a$ an. Es folgt, dass

$$a \cdot a^{-1} = e \in H$$

ist. Wir wählen jetzt in (16) $a = e$ und $b = a$, wobei a ein beliebiges Element von H ist. Es folgt dann:

$$e \cdot a^{-1} = a^{-1} \in H$$

Also ist für jedes Element $a \in H$ das Inverse ebenfalls in H . Wir wählen jetzt zwei beliebige Elemente $a, b \in H$. Wir haben eben gezeigt, dass b^{-1} dann auch in H ist. Also ist $a, b^{-1} \in H$. Aus der Bedingung (16) folgt dann

$$a \cdot (b^{-1})^{-1} = a \cdot b \in H$$

Also ist \cdot abgeschlossen in H . Da das Assoziativgesetz in G gilt, gilt es auch in der Teilmenge H . Damit haben wir bewiesen, dass H eine Untergruppe von G ist. \square

Bemerkungen und Beispiele:

- Jede Gruppe (G, \cdot) besitzt die beiden trivialen Untergruppen $\{e\}$ und G .
- Wir betrachten die Gruppe $(\mathbb{Z}, +)$. Sei $m \in \mathbb{N}_0$. Dann ist die Menge der ganzzahligen Vielfachen von m

$$m\mathbb{Z} = \{m \cdot n : n \in \mathbb{Z}\}$$

eine Untergruppe von \mathbb{Z} . Man kann zeigen, dass dies die einzigen Untergruppen von $(\mathbb{Z}, +)$ sind.

4.4 Nebenklassen und der Satz von Lagrange

Sei jetzt $H < G$. Für jedes $a \in G$ nennt man die Menge

$$aH = \{ah : h \in H\}$$

eine **Linksnebenklasse** von H . Analog ist

$$Ha = \{ha : h \in H\}$$

eine **Rechtsnebenklasse** von H .

Bemerkungen und Beispiele:

- Wenn a und b zwei verschiedene Elemente von G sind, bedeutet dies nicht, dass $aH \neq bH$ ist. Die beiden Elemente können die gleiche Nebenklasse erzeugen. Wir werden dies weiter unten sehen.
- Falls G eine abelsche Gruppe ist, gilt $ah = ha$. Damit ist natürlich $aH = Ha$. Jede Linksnebenklasse ist gleich der entsprechenden Rechtsnebenklasse. Wir müssen also nicht zwischen Links- und Rechtsnebenklassen unterscheiden und sprechen einfach von Nebenklassen. Falls G keine abelsche Gruppe ist, müssen die Linksnebenklassen nicht gleich den entsprechenden Rechtsnebenklassen sein.
- Falls $H < G$ ist und $aH = Ha$ für jedes $a \in G$ gilt, so nennt man H einen **Normalteiler** von G . Falls G eine abelsche Gruppe ist, so ist jede Untergruppe H von G ein Normalteiler. Weiter sind in jeder Gruppe G die trivialen Untergruppen $\{e\}$ und G Normalteiler. In der Diedergruppe D_3 ist die Untergruppe $N = \{\text{id}, r_{120}, r_{240}\}$ ein Normalteiler. Normalteiler sind wichtig, da sie die Konstruktion neuer Gruppen ermöglichen. Wir werden dies allerdings nicht weiterverfolgen.
- Wir wählen für a das Neutralelement e . Da $eH = He = H$ ist, ist die Untergruppe H sowohl eine Links- wie eine Rechtsnebenklasse.

Falls $a \notin H$, ist aH (bzw. Ha) **keine** Untergruppe von G , denn diese Nebenklasse enthält das Neutralelement e nicht. Wäre nämlich $e \in aH$, dann gäbe es ein $h \in H$, wofür gilt

$$ah = e.$$

Es würde dann folgen

$$a = h^{-1} \cdot e = h^{-1} \in H$$

Widerspruch!

- Wir betrachten $G = (\mathbb{Z}, +)$ und als Untergruppe

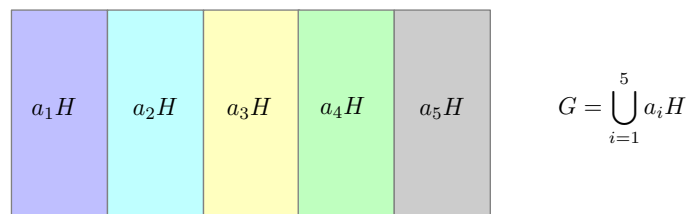
$$H := 2 \cdot \mathbb{Z} = \{2h : h \in \mathbb{Z}\}$$

die Menge der **geraden** ganzen Zahlen. Die Nebenklassen lauten in der additiven Schreibweise $a + H$. Offenbar gibt es nur zwei verschiedene Nebenklassen. Wenn a gerade ist, dann ist $a + H = H$. Wenn a ungerade ist, dann ist $a + H$ gleich der Menge der **ungeraden** ganzen Zahlen.

Wir kommen jetzt zu einem wichtigen Resultat:

Satz 28 Sei (G, \cdot) eine Gruppe und $H < G$. Dann bilden die Linksnebenklassen aH (bzw. Rechtsnebenklassen Ha) eine Partition von G , das heisst, es gelten die folgenden Bedingungen:

- (i) Keine Nebenklasse ist leer.
- (ii) Zwei Nebenklasse aH und bH sind entweder gleich oder disjunkt ($aH \cap bH = \emptyset$).
- (iii) Die Vereinigung aller Nebenklassen ist G .



$$G = \bigcup_{i=1}^5 a_i H$$

Bew.: Da $H < G$ ist, ist $e \in H$. Jede Untergruppe enthält mindestens das Neutralelement. Daraus folgt dann, dass $a \in aH$ ist. Damit haben wir (i) aber auch (iii) bewiesen, denn

$$\bigcup_{a \in G} aH = G.$$

Es bleibt der Beweis von (ii). Wenn $aH \cap bH = \emptyset$, gibt es nichts zu beweisen. Wir müssen also nur den Fall

$$aH \cap bH \neq \emptyset$$

betrachten. Wir müssen beweisen, dass die beiden Nebenklassen gleich sind. Sei

$$x \in aH \cap bH.$$

Es existieren dann Elemente $h_1, h_2 \in H$, so dass gilt:

$$x = ah_1 = bh_2$$

Aus diesen Gleichungen folgt:

$$a = b(h_2h_1^{-1}) \in bH \quad \text{und} \quad b = a(h_1h_2^{-1}) \in aH$$

Wenn man beweisen muss, dass zwei Mengen gleich sind, zeigt man, dass die eine in der andern enthalten ist und umgekehrt. Sei $y \in aH$. Dann existiert ein $h \in H$, so dass gilt:

$$y = ah$$

Wir ersetzen jetzt a durch den Ausdruck $b(h_2h_1^{-1})$. Es folgt dann:

$$y = b(h_2h_1^{-1}) \cdot h = b \underbrace{(h_2h_1^{-1}h)}_{\in H} \in bH$$

Sei umgekehrt $z \in bH$. Es existiert dann ein Element $h \in H$, so dass gilt:

$$z = bh = a(h_1h_2^{-1}) \cdot h = a \underbrace{(h_1h_2^{-1}h)}_{\in H} \in aH$$

Wir haben bewiesen, dass die beiden Nebenklasse gleich sind. □

Alle Nebenklassen aH (bzw. Ha) haben gleich viele Elemente wie H , denn für jedes $a \in G$ ist die Abbildung

$$\begin{aligned} f_a : H &\rightarrow aH \\ h &\rightarrow ah \end{aligned}$$

bijektiv. Es sei jetzt G eine **endliche** Gruppe und $H < G$. Unter dem **Index von H in G** , geschrieben $\text{ind}(G : H)$, versteht man die Anzahl der Nebenklassen aH (bzw. Ha). Beachten Sie bitte, dass die Anzahl der Links- gleich der Anzahl der Rechtsnebenklassen ist. Wir können jetzt ein ganz zentrales Resultat der Gruppentheorie formulieren:

Satz 29 (Satz von Lagrange¹⁴) Sei G eine **endliche** Gruppe und $H < G$. Dann gilt:

$$|G| = \text{ind}(G : H) \cdot |H|$$

Insbesondere ist $|H|$ ein Teiler von $|G|$.

¹⁴Joseph-Louis Lagrange (1736 Turin - 1813 Paris): Lagrange machte bedeutende Beiträge in der Mathematik (Variationsrechnung, Zahlentheorie), Physik und Himmelsmechanik

Bew.: Dies folgt sofort aus der Tatsache, dass alle Nebenklassen $|H|$ Elemente besitzen und die Menge aller Nebenklassen eine Partition von G bilden.

□

Beachten Sie bitte, dass die Umkehrung des Satzes von Lagrange nicht richtig ist. Wenn d ein Teiler der Gruppenordnung ist, dann muss keine Untergruppe existieren, deren Ordnung gleich d ist.

Wir können aus dem Satz von Lagrange sofort eine wichtige Schlussfolgerung ziehen:

Satz 30 Sei G eine endliche Gruppe mit Primzahlordnung, das heisst, $|G|$ ist eine Primzahl. Dann besitzt G nur die trivialen Untergruppe $\{e\}$ und G .

Beispiel 54 Bestimmen Sie alle Untergruppen von D_3 .

Die Aufgabe wird im Unterricht gelöst.

◇

4.5 Ordnung eines Elements

Sei G eine Gruppe und $a \in G$. Für $n \in \mathbb{N}$ definieren wir wie üblich:

$$a^n := \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ Faktoren } a}$$

Weiter definieren wir:

$$a^0 := e$$

Für negative Exponenten gilt:

$$a^{-n} := (a^n)^{-1}$$

Man kann zeigen, dass die üblichen Potenzgesetze gelten: für $m, n \in \mathbb{Z}$ gilt dann:

$$\begin{aligned} a^m \cdot a^n &= a^{m+n} \\ a^n \cdot b^n &= (ab)^n \\ (a^m)^n &= a^{m \cdot n} \end{aligned}$$

Wir betrachten die Folge von Elementen:

$$a, a^2, a^3, \dots$$

Es können zwei Fälle auftreten:

- (1) Alle diese Potenzen sind paarweise verschieden. Dies ist natürlich nur möglich, wenn G unendlich viele Elemente enthält. Man sagt dann, a habe die Ordnung unendlich, und man schreibt:

$$\text{ord}(a) = \infty$$

- (2) Es gibt natürliche Zahlen k und ℓ , $k < \ell$, so dass gilt:

$$a^\ell = a^k$$

Aus dieser Gleichung folgt durch Multiplikation mit a^{-k} :

$$a^{\ell-k} = e$$

Es gibt dann eine kleinste natürliche Zahl, die man die Ordnung von a nennt, geschrieben $\text{ord}(a)$, so dass gilt:

$$a^{\text{ord}(a)} = e$$

Wir nehmen an, dass $\text{ord}(a) < \infty$ ist. Wir betrachten die Menge

$$H := \{a, a^2, a^3, \dots, a^{\text{ord}(a)}\} \subseteq G.$$

Diese Menge enthält e . Weiter ist die Menge abgeschlossen bezüglich der Gruppenoperation. Wenn $k, \ell \in \{1, 2, 3, \dots, \text{ord}(a)\}$ Exponenten sind, dann sind 2 Fälle möglich:

(1) $k + \ell \leq \text{ord}(a)$. Dann ist:

$$a^k \cdot a^\ell = a^{k+\ell} \in H$$

(2) $\text{ord}(a) < k + \ell \leq 2 \cdot \text{ord}(a)$. Dann ist:

$$a^k \cdot a^\ell = a^{\text{ord}(a)} \cdot a^{k+\ell-\text{ord}(a)} = e \cdot a^{k+\ell-\text{ord}(a)} = a^{k+\ell-\text{ord}(a)} \in H$$

Weiter ist das Inverse von a^k gegeben durch $a^{\text{ord}(a)-k}$. Also ist H eine Untergruppe von G .

Wir haben den folgenden Satz bewiesen:

Satz 31 Sei (G, \cdot) eine Gruppe und $a \in G$ mit $\text{ord}(a) < \infty$. Dann ist

$$H := \{a, a^2, a^3, \dots, a^{\text{ord}(a)}\} \subseteq G$$

eine **Untergruppe** von G .

Wir betrachten jetzt den Fall, wo G eine **endliche** Gruppe ist. Nach dem Satz von Lagrange muss die Ordnung von H ein Teiler der Gruppenordnung $|G|$ sein. Da

$$|H| = \text{ord}(a)$$

muss auch die Ordnung eines Elements ein Teiler der Gruppenordnung sein.

Satz 32 Sei (G, \cdot) eine endliche Gruppe. Dann gilt für jedes $a \in G$:

$$\text{ord}(a) \mid |G|$$

Sei G wiederum eine endliche Gruppe und a ein Element von G . Da die Ordnung von a ein Teiler der Gruppenordnung $|G|$ ist, existiert eine natürliche Zahl k , wofür gilt:

$$k \cdot \text{ord}(a) = |G|$$

Es folgt dann:

$$a^{|G|} = a^{k \cdot \text{ord}(a)} = \left(a^{\text{ord}(a)}\right)^k = e^k = e$$

Wenn wir also ein Element mit der Gruppenordnung potenzieren, erhalten wir e .

Satz 33 Sei G eine endliche Gruppe und $a \in G$. Dann gilt:

$$a^{|G|} = e$$

Falls eine endliche Gruppe G ein Element a besitzt mit

$$G = \{a, a^2, a^3, \dots, a^{\text{ord}(a)}\}$$

nennt man die Gruppe **zyklisch**. Man bezeichnet a als **erzeugendes Element**. Zyklische Gruppen werden also durch ein einziges Element erzeugt.

Falls $\text{ord}(G) = \infty$ ist, dann ist G zyklisch, wenn ein Element $a \in G$ existiert, so dass gilt

$$G = \{a^k : k \in \mathbb{Z}\} .$$

Beispiel 55 Zeigen Sie, dass eine zyklische Gruppe abelsch (=kommutativ) ist.

Die Aufgabe wird im Unterricht gelöst. \diamond

Beispiel 56 Zeigen Sie, dass eine Gruppe mit Primzahlordnung zyklisch ist.

Die Aufgabe wird im Unterricht gelöst. \diamond

Sei a ein Element mit endlicher Ordnung. Der folgende Satz liefert eine Formel für die Ordnung einer Potenz von a :

Satz 34 Sei (G, \cdot) eine Gruppe und $a \in G$ ein Element mit endlicher Ordnung n . Für $k \in \mathbb{N}$ gilt:

(a)

$$a^k = e \iff n|k$$

(b)

$$\text{ord}(a^k) = \frac{\text{kgV}(n, k)}{k} = \frac{n}{\text{ggT}(n, k)} \quad (17)$$

Bew.:

(a) Sei $a^k = e$. Wir dividieren k durch n :

$$k = q \cdot n + r \quad \text{mit} \quad 0 \leq r < n$$

Wir wollen zeigen, dass $r = 0$ ist. Angenommen $r > 0$. Dann wäre:

$$e = a^k = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

Da $0 < r < n$ haben wir einen Widerspruch zur Tatsache, dass n die kleinste natürliche Zahl mit $a^n = e$ ist.

Die andere Richtung ist trivial.

(b) Sei $\ell = \text{ord}(a^k)$. Gemäss Definition ist ℓ die **kleinste** natürliche Zahl mit

$$(a^k)^\ell = a^{k\ell} = e .$$

Aus Teil (a) folgt

$$n|(k \cdot \ell) .$$

Also ist $k\ell$ ein Vielfaches von n und von k . Wegen der Minimalität von ℓ folgt:

$$k \cdot \ell = \text{kgV}(n, k) \implies \ell = \frac{\text{kgV}(n, k)}{k}$$

Wie man leicht über die Primfaktorisation sieht, gilt für beliebige natürliche Zahlen c und d :

$$\text{kgV}(c, d) \cdot \text{ggT}(c, d) = c \cdot d$$

Also ist

$$\frac{\text{kgV}(n, k)}{k} = \frac{nk}{k \text{ggT}(n, k)} = \frac{n}{\text{ggT}(n, k)}$$

□

Mithilfe des obigen Satzes folgt jetzt leicht, dass in endlichen zyklischen Gruppen die Umkehrung des Satzes von Lagrange gilt:

Satz 35 *Sei (G, \cdot) eine zyklische Gruppe mit Ordnung n . Dann gilt: zu jedem Teiler d von n existiert eine Untergruppe, deren Ordnung d ist.*

Bew.: Sei d ein Teiler von n und a ein erzeugendes Element. Dann existiert eine natürliche Zahl k mit

$$n = kd$$

Gemäss Formel (17) gilt:

$$\text{ord}(a^k) = \frac{n}{\text{ggT}(n, k)} = \frac{kd}{k} = d$$

□

Dank dem Satz 34 können wir auch die Anzahl der erzeugenden Elemente in einer zyklischen Gruppe mit Ordnung n bestimmen. Das Element a^k besitzt genau dann die Ordnung n , wenn $\text{ggT}(k, n) = 1$ ist. Dies ist Anzahl, der zu n teilerfremden Zahlen $\leq n$. Diese Anzahl ist gleich $\phi(n)$ (Eulersche Phi-Funktion, siehe Modul *Diskrete Mathematik 1*).

Satz 36 *Sei (G, \cdot) eine zyklische Gruppe der Ordnung n . Dann besitzt G $\phi(n)$ erzeugende Elemente.*

4.6 Restklassen

In diesem Kapitel werden wir weitere Gruppen einführen, die für viele Anwendungen (z.B. in der Kryptographie) sehr wichtig sind.

Sei $m \in \mathbb{N}$. Im Modul *Diskrete Mathematik 1* haben wir die Kongruenzrelation eingeführt. Seien $x, y \in \mathbb{Z}$. Wir definieren:

$$x \equiv y \pmod{m} \iff m \mid (x - y)$$

Dies wird so gelesen: x und y sind kongruent modulo m . Wir haben gesehen, dass x und y genau dann kongruent modulo m sind, wenn bei der Division durch m der gleiche nichtnegative Rest bleibt. Es handelt sich um eine **Äquivalenzrelation**. Die Äquivalenz- oder Restklassen sind gegeben durch:

$$\bar{a} = a + k\mathbb{Z} = \{a + k \cdot m : k \in \mathbb{Z}\}$$

Für $m = 5$ haben wir beispielsweise die 5 Restklassen:

$$\begin{aligned}\bar{0} &= \{k \cdot m : k \in \mathbb{Z}\} &= \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} \\ \bar{1} &= \{1 + k \cdot m : k \in \mathbb{Z}\} &= \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} \\ \bar{2} &= \{2 + k \cdot m : k \in \mathbb{Z}\} &= \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} \\ \bar{3} &= \{3 + k \cdot m : k \in \mathbb{Z}\} &= \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} \\ \bar{4} &= \{4 + k \cdot m : k \in \mathbb{Z}\} &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}\end{aligned}$$

Die Restklassen bilden eine **Partition** von \mathbb{Z} .

Die Menge der Restklassen modulo m bezeichnen wir mit \mathbb{Z}_m , also

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}.$$

Wir werde jetzt auf dieser Menge eine Addition und Multiplikation definieren. Dazu benötigen wir das folgende Resultat aus dem Modul *Diskrete Mathematik 1*: sei $m \in \mathbb{N}$ und seien $x, y, u, v \in \mathbb{Z}$. Dann gilt:

$$x \equiv y \pmod{m} \quad \wedge \quad u \equiv v \pmod{m} \implies x + u \equiv y + v \pmod{m} \quad (18)$$

und

$$x \equiv y \pmod{m} \quad \wedge \quad u \equiv v \pmod{m} \implies x \cdot u \equiv y \cdot v \pmod{m} \quad (19)$$

Wir definieren jetzt auf \mathbb{Z}_m eine Addition und eine Multiplikation:

$$\begin{aligned}\bar{a} + \bar{b} &:= \overline{a + b} \\ \bar{a} \cdot \bar{b} &:= \overline{a \cdot b}\end{aligned}$$

Wegen (18) und (19) sind diese Operationen wohldefiniert, das heisst, unabhängig von den gewählten Repräsentanten a und b der Restklassen.

Beispiel 57 Führen Sie die folgenden Operationen in \mathbb{Z}_{12} aus:

$$\bar{5} + \bar{9} \quad \text{und} \quad \bar{5} \cdot \bar{9}$$

Die Aufgabe wird im Unterricht gelöst. ◇

Beispiel 58 Zeigen Sie, dass $(\mathbb{Z}_m, +)$ eine zyklische Gruppe ist.

Die Aufgabe wird im Unterricht gelöst. ◇

Wir haben eben bewiesen, dass die folgenden Gesetze für die Addition gelten: für alle $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ gilt:

(R1) Assoziativgesetz :

$$(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$$

(R2) Kommutativgesetz :

$$\bar{a} + \bar{b} = \bar{b} + \bar{a}$$

(R3) Existenz eines Neutralelements:

$$\bar{a} + \bar{0} = \bar{a}$$

(R4) Existenz eines inversen Elements:

$$\bar{a} + \overline{-a} = \bar{0}$$

Wenn wir die Multiplikation betrachten, gelten zusätzlich die folgenden Gesetze:

(R5) Assoziativgesetz der Multiplikation:

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$

(R6) Kommutativgesetz der Multiplikation:

$$\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$$

(R7) Distributivgesetz:

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

(R8) Existenz eines Einselements $\bar{1} \neq \bar{0}$ (=Neutralelement der Multiplikation):

$$\bar{1} \cdot \bar{a} = \bar{a}$$

Eine Menge, in welcher zwei interne Operationen definiert sind, welche die Gesetze (R1)-(R8) erfüllen, heisst **kommutativer Ring mit Einselement**.

Satz 37 Sei $m \in \mathbb{N}$. $(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring mit Einselement.

Wir betrachten jetzt den Fall, wo $m \in \mathbb{N}$ **keine Primzahl** ist. Sei $a \in \mathbb{N}$, $1 < a < m$, mit $\text{ggT}(a, m) = d > 1$. Die Restklasse \bar{a} besitzt dann kein multiplikatives Inverses, das heisst, es gibt kein $\bar{b} \in \mathbb{Z}_m$, wofür gilt:

$$\bar{a} \cdot \bar{b} = \bar{1}.$$

Wir führen einen Beweis durch Widerspruch: angenommen es gäbe ein solches $\bar{b} \in \mathbb{Z}$ mit dieser Eigenschaft. Nach Definition der Multiplikation gilt dann

$$\overline{a \cdot b} = \bar{1}.$$

Nach Definition der Kongruenzrelation existiert dann eine Zahl $k \in \mathbb{Z}$, wofür gilt:

$$a \cdot b = 1 + k \cdot m \implies a \cdot b - k \cdot m = 1$$

Da $d|a$ und $d|m$ gilt, teilt d die linke Seite. d kann aber kein Teiler von 1 sein. Wir haben einen Widerspruch.

Weiter besitzt in diesem Fall \mathbb{Z}_m sogenannte **Nullteiler**, das heisst, es gibt $\bar{a}, \bar{b} \in \mathbb{Z}_m$, $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$, so dass gilt

$$\bar{a} \cdot \bar{b} = \bar{0}$$

Wenn ein Produkt gleich $\bar{0}$ ist, können wir also nicht schliessen, dass einer der Faktoren gleich $\bar{0}$ ist. Wenn $m = 6$ ist, so gilt beispielsweise

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0},$$

aber $\bar{2} \neq \bar{0}$ und $\bar{3} \neq \bar{0}$.

Insbesondere gilt dann auch die Kürzungsregel nicht. Aus

$$\bar{a} \cdot \bar{c} = \bar{b} \cdot \bar{c}$$

können wir nicht folgern, dass $\bar{a} = \bar{b}$ ist.

Falls hingegen $m = p$ eine Primzahl ist, dann ist für jedes $a \in \mathbb{N}$ mit $1 \leq a \leq p - 1$

$$\text{ggT}(a, p) = 1 .$$

Es existiert dann ein $\bar{b} \in \mathbb{Z}_p$ mit

$$\bar{a} \cdot \bar{b} = \bar{1} .$$

Wir können b mithilfe des **erweiterten euklidischen Algorithmus** berechnen.

Beispiel 59 Sei $p = 89$. Berechnen Sie das multiplikative Inverse von $\overline{35}$.

Die Aufgabe wird im Unterricht gelöst. ◇

Falls $m = p$ eine Primzahl ist, gilt also zusätzlich:

(R9) Zu jedem $\bar{a} \in \mathbb{Z}_p \setminus \{\bar{0}\}$ existiert ein multiplikatives Inverses $\bar{a}^{-1} \in \mathbb{Z}_p$ mit

$$\bar{a} \cdot \bar{a}^{-1} = \bar{1} .$$

Beachten Sie, dass $\bar{0}$ kein multiplikatives Inverses besitzt. Wir führen für $\mathbb{Z}_p \setminus \{\bar{0}\}$ die Abkürzung \mathbb{Z}_p^* ein. Wir können den folgenden Satz formulieren:

Satz 38 Sei p eine Primzahl. Dann besitzt jedes Element in \mathbb{Z}_p^* ein multiplikatives Inverses, das heisst, (\mathbb{Z}_p^*, \cdot) ist eine kommutative Gruppe.

4.7 Die Gruppen (\mathbb{Z}_p^*, \cdot)

Sei p eine Primzahl. Die Gruppen (\mathbb{Z}_p^*, \cdot) spielen in der Kryptographie eine grosse Rolle. Nachfolgend geben wir die wichtigsten Eigenschaften:

- Die Gruppen sind zyklisch. Der Beweis hierzu findet sich in Bücher über Zahlentheorie, z.B. [11].
- Sie besitzen $p - 1$ Elemente. Beachten Sie, dass $p - 1$ für $p > 2$ gerade ist. Es ist also keine Primzahl mehr.
- Aus Satz 36 folgt, dass sie $\phi(p - 1)$ erzeugende Elemente besitzen.
- Aus Satz 35 folgt, dass für jeden Teiler d von $p - 1$ eine zyklische Untergruppen der Ordnung d existiert.

Beispiel 60 Bestimmen Sie die Ordnungen der Elemente von $(\mathbb{Z}_{11}^*, \cdot)$. Verifizieren Sie, dass die Anzahl der erzeugenden Elemente gleich $\phi(10)$ ist.

Die Aufgabe wird im Unterricht gelöst. ◇

Ein erzeugendes Element der Gruppe (\mathbb{Z}_p^*, \cdot) nennen man auch eine **Primitivwurzel modulo p** .

Wenn wir den Satz 33 für die Gruppe (\mathbb{Z}_p^*, \cdot) formulieren, erhalten wir den kleinen Fermatschen Satz:

Satz 39 (Kleiner Fermatscher Satz) Sei $\bar{a} \in (\mathbb{Z}_p^*, \cdot)$. Dann gilt:

$$\bar{a}^{p-1} = \bar{1}$$

oder als Kongruenz:

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

Beachten Sie, dass die Bedingung $\bar{a} \neq \bar{0}$ bedeutet, dass a kein Vielfaches von p ist.

Die Sicherheit verschiedener kryptographischer Verfahren basiert auf der Schwierigkeit den diskreten Logarithmus zu berechnen. Wir betrachten (\mathbb{Z}_p^*, \cdot) , wobei p eine grosse Primzahl ($p > 2^{1'024}$) ist. Sei $\bar{b} \in \mathbb{Z}_p^*$ ein erzeugendes Element und \bar{a} ein beliebiges Element in \mathbb{Z}_p^* . Beide Elemente sind öffentlich bekannt. Gesucht wird $x \in \mathbb{N}$, wofür gilt:

$$\bar{b}^x = \bar{a}$$

oder als Kongruenz

$$b^x \equiv a \pmod{p}.$$

Man bezeichnet dieses Problem als **diskretes Logarithmus-Problem**.

Wenn $p-1$ nicht in lauter kleine Primfaktoren zerfällt, existiert zur Zeit kein schneller Algorithmus, um dieses Problem zu lösen.

Beachten Sie, dass das umgekehrte Problem, in welchem \bar{b} und $x \in \mathbb{N}$ bekannt sind, aber \bar{a} gesucht wird, mit dem „Square and multiply“-Algorithmus schnell gelöst werden kann. Das ist wichtig für die Chiffrierung und Dechiffrierung.

Das diskrete Logarithmus-Problem kann für eine beliebige Gruppe formuliert werden. Die Gruppe muss nicht einmal zyklisch sein, sollte aber ein Element mit sehr hoher Ordnung enthalten. Es eignen sich aber nicht alle Gruppen. In $(\mathbb{Z}_p, +)$ ist das Problem trivial. Gesucht wird eine natürliche Zahl x , wofür gilt:

$$x \cdot \bar{b} = \bar{a}$$

oder als Kongruenz:

$$x \cdot b \equiv a \pmod{p}$$

Wir können x leicht berechnen, indem wir das multiplikative Inverse von b modulo p berechnen, was mit dem erweiterten euklidischen Algorithmus schnell geht, und die Kongruenz mit dieser Zahl multiplizieren.

Normalerweise verwendet man für das diskrete Logarithmus-Problem Gruppen, welche auf elliptischen Kurven basieren, da in diesen Gruppen das Problem noch schwieriger zu lösen ist als in (\mathbb{Z}_p^*, \cdot) . Man kann dann p wesentlich kleiner wählen und so Rechenzeit für die Chiffrierung und Dechiffrierung sparen.

4.8 Klassifizierung einiger Gruppen

Mithilfe des folgenden Satzes können wir alle zyklischen Gruppen klassifizieren:

Satz 40 Sei G eine zyklische Gruppe.

(i) Falls G endliche Ordnung m besitzt, so ist G isomorph zu $(\mathbb{Z}_m, +)$.

(ii) Falls G unendliche Ordnung besitzt, so ist G isomorph so $(\mathbb{Z}, +)$.

Bew.: (i) Sei g ein erzeugendes Element von G . Wir definieren die Abbildung

$$\begin{aligned}\phi: \mathbb{Z}_m &\rightarrow G \\ \bar{a} &\rightarrow g^a\end{aligned}$$

Wir müssen zeigen, dass ϕ wohldefiniert ist, das heisst, nicht vom Repräsentanten der Restklasse abhängt. Sei $\bar{a} = \bar{b}$. Es existiert dann eine ganze Zahl k , so dass

$$b = a + km.$$

Es folgt dann:

$$g^b = g^{a+km} = g^a \cdot g^{km} = g^a (g^m)^k = g^a e^k = g^a$$

Weiter ist klar, dass ϕ surjektiv ist, denn

$$\phi(\bar{0}) = g^0 = e, \quad \phi(\bar{1}) = g^1, \quad \phi(\bar{2}) = g^2, \dots, \quad \phi(\overline{m-1}) = g^{m-1}.$$

Wir haben so alle Elemente von G erhalten. Wegen $|\mathbb{Z}_m| = |G| = m$ ist dann ϕ auch injektiv. Da

$$\phi(\bar{a} + \bar{b}) = g^{a+b} = g^a \cdot g^b = \phi(\bar{a}) \cdot \phi(\bar{b}),$$

ist ϕ ein Isomorphismus.

Der Beweis von (ii) ist analog. □

Wir erwähnen noch den folgenden Satz:

Satz 41 *Die Untergruppen einer zyklischen Gruppe sind auch zyklisch.*

Der Beweis ist nicht schwierig, aber wir verzichten darauf.

In den folgenden Klassifizierungen kommt das direkte Produkt von Gruppen vor. Es handelt sich dabei um ein einfaches Verfahren, mit welchem aus zwei Gruppen eine neue Gruppe konstruiert werden kann.

Seien $(G_1, *)$ und $(G_2, *')$ zwei Gruppen. Wir betrachten das kartesische Produkt $G_1 \times G_2$ und statten dieses mit einer Operation aus: Wenn $(a, b), (c, d) \in G_1 \times G_2$ sind, dann definieren wir:

$$(a, b) \cdot (c, d) = (a * c, b *' d)$$

Auf die ersten Komponenten wird also die Gruppenoperation in G_1 und auf die zweiten Komponenten jene in G_2 ausgeübt. Man kann leicht beweisen, dass wir so eine Gruppe mit $|G_1| \cdot |G_2|$ Elementen erhalten.

Natürlich bedeutet dies nicht, dass man immer eine neue Gruppe erhält. Die erhaltene Gruppe kann isomorph zu einer bekannten Gruppe sein.

Das obige Verfahren lässt sich auf kartesische Produkte von mehr als 2 Gruppen verallgemeinern.

Beispiel 61 Wir betrachten $G_1 = (\mathbb{Z}_2, +)$ und $G_2 = (\mathbb{Z}_3, +)$. Zeigen Sie, dass $G_1 \times G_2$ isomorph zu $(\mathbb{Z}_6, +)$ ist.

Die Aufgabe wird im Unterricht gelöst. ◇

Wir haben bereits die Gruppen mit den Ordnungen 1 bis 4 klassifiziert. Wir führen diese Liste noch ein wenig weiter:

- $|G| = 5$: Da die Ordnung eine Primzahl ist, ist die Gruppe zyklisch und damit isomorph zu $(\mathbb{Z}_5, +)$.
- $|G| = 6$: Wir kennen bereits zwei Gruppen mit 6 Elementen: die zyklische Gruppe $(\mathbb{Z}_6, +)$ und die Diedergruppe D_3 . Bis auf Isomorphie sind dies die einzigen Gruppen. Beweis: Fall 1: wenn G ein erzeugendes Element enthält, dann ist G zyklisch und damit isomorph zu $(\mathbb{Z}_6, +)$. Fall 2: G besitzt kein erzeugendes Element. Dann besitzt G neben e nur Elemente mit den Ordnungen 2 oder 3. Wir zeigen, dass G ein Element der Ordnung 3 besitzen muss. Angenommen G enthält kein Element der Ordnung 3. Dann können wir zwei Elemente a und b der Ordnung 2 auswählen und die Menge

$$H := \{e, a, b, ab\}$$

bilden. Wie man sofort sieht, gilt

$$ab \neq e \wedge ab \neq a \wedge ab \neq b.$$

Weiter muss ab ebenfalls die Ordnung 2 besitzen und ist damit invers zu sich selbst. Damit ist H eine Untergruppe von G der Ordnung 4. Da 4 kein Teiler von 6 ist, ist das nicht möglich. Wir haben einen Widerspruch.

Sei jetzt also a ein Element mit Ordnung 3 und b ein Element, wofür gilt

$$b \notin \{e, a, a^2\}.$$

Wir bilden dann die Menge

$$\{e, a, a^2, b, ab, a^2b\}.$$

Diese 6 Elemente sind paarweise verschieden, das heisst, diese Menge ist gerade G . Man überprüft leicht, dass b zu keinem der 4 anderen Elementen invers ist. Also muss b zu sich selber invers sein und damit die Ordnung 2 haben. Damit haben auch ab und a^2b die Ordnung 2. Es liegt also die gleiche Situation vor wie bei der Gruppe D_3 . Wir erhalten einen Isomorphismus $\phi : D_3 \rightarrow G$, indem wir definieren

$$\phi(s_1) = b \quad \text{und} \quad \phi(r_{120}) = a.$$

- $|G| = 7$: Wir haben wieder eine Primzahlordnung. Damit ist G isomorph zu $(\mathbb{Z}_7, +)$.
- $|G| = 8$: Hier wird die Angelegenheit bereits komplizierter. Wir haben die Gruppen $(\mathbb{Z}_8, +)$ und D_4 . Weiter haben wir die Gruppen $\mathbb{Z}_4 \times \mathbb{Z}_2$ und $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Weiter haben wir noch die Quaternionengruppe.

4.9 Endliche Körper

4.9.1 Einführung

Eine Menge versehen mit zwei Operationen $+$ und \cdot , welche die Gesetze (R1)-(R9) erfüllen, nennt man einen **Körper**.

$(\mathbb{Z}_p, +, \cdot)$ ist also ein Körper mit p Elementen. Man bezeichnet diesen Körper häufig mit \mathbb{F}_p (auf Englisch heissen Körper *fields*). Sie kennen bereits Körper mit unendlich vielen Elementen: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. Endliche Körper spielen in der Kryptographie und Codierungstheorie eine grosse Rolle.

Wir werden jetzt weitere endliche Körper mit p^n Elementen, wo p eine Primzahl und n eine natürliche Zahl ist, konstruieren. Wir benötigen dazu Polynome.

4.9.2 Polynomringe

Polynome sind Ausdrücke der Form:

$$4x^3 - 2x^2 + x + 1 \quad , \quad x^2 + x + 10 \quad , \quad x^5 + 2x^x + 10x - 5 \quad .$$

Polynome sind also spezielle Funktionen. Allerdings interessiert man sich in der Algebra im Zusammenhang mit Polynomen nicht für diesen Aspekt. Im Vordergrund steht die Addition und die Multiplikation von Polynomen.

Sei $n \in \mathbb{N}$. Allgemein versteht man unter einem Polynom einen Ausdruck der Form:

$$\sum_{k=0}^n a_k x^k = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad . \quad (20)$$

Hier sind die a_k gegebene Elemente aus einem Körper \mathbb{K} . Sie heissen Koeffizienten. Die Grösse x ist die Unbekannte. Natürlich kommt es auch in der Algebra vor, dass man für x ein Element aus \mathbb{K} einsetzt. Wie gesagt, ist dieser Aspekt aber nicht zentral. Eigentlich könnte man die Unbekannte x auch weglassen. Ein Polynom ist dann einfach eine Folge von Koeffizienten

$$(a_0, a_1, a_2, a_3, \dots, a_n, \dots) \quad , \quad (21)$$

wobei nur endlich viele Koeffizienten verschieden von Null sind. Auf der Menge dieser Folgen definiert man dann eine Addition und eine Multiplikation:

$$\begin{aligned} (a_0, a_1, a_2, \dots, a_n, \dots) + (b_0, b_1, b_2, \dots, b_n, \dots) \\ := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, \dots) \end{aligned}$$

und

$$\begin{aligned} (a_0, a_1, a_2, \dots, a_n, \dots) \cdot (b_0, b_1, b_2, \dots, a_n, \dots) = \\ := \left(a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots, \sum_{k=0}^n a_k b_{n-k}, \dots \right) \end{aligned}$$

Dieser exakte Zugang besitzt den Vorteil, dass man erklären kann, was die Unbekannte x ist. Sie entspricht der Folge

$$(0, 1, 0, \dots)$$

Man verifiziert leicht, dass gilt:

$$x^2 = x \cdot x = (0, 0, 1, 0, \dots), \quad x^3 = x \cdot x^2 = (0, 0, 0, 1, 0, \dots), \quad \text{etc.}$$

Indem man die Folge

$$(a, 0, 0, \dots)$$

mit $a \in \mathbb{K}$ identifiziert, erhält man schliesslich die Darstellung (20). Für die Handrechnung, insbesondere im Zusammenhang mit der Multiplikation, ist die Darstellung (20) wesentlich angenehmer. Die Potenzen von x definieren die Position des Koeffizienten. Wir werden im Folgenden nur diese Darstellung benützen. Wir weisen noch darauf hin, dass wir den Koeffizienten 1 nicht explizit hinschreiben. Statt $1x^2 + 1x + 1$ schreiben wir $x^2 + x + 1$.

Unter dem Grad eines Polynoms (20) versteht man den grössten Index k , wofür $a_k \neq 0$ ist. Sind alle Koeffizienten gleich Null, erhalten wir das **Nullpolynom**. Es ist praktisch den Grad des Nullpolynoms als $-\infty$ zu definieren. Ein konstantes Polynom $a_0 \neq 0$ besitzt den Grad 0. Wir bezeichnen den Grad eines Polynoms $f(x)$ mit $\deg(f(x))$. Die Menge aller Polynome mit Koeffizienten im Körper \mathbb{K} wird mit $\mathbb{K}[x]$ bezeichnet.

Die Elemente im Körper \mathbb{K} identifizieren wir mit den konstanten Polynomen. In diesem Sinne wird \mathbb{K} zu einer Teilmenge von $\mathbb{K}[x]$.

Wir definieren jetzt auf $\mathbb{K}[x]$ eine Addition und eine Multiplikation. In der Darstellung (20) werden Polynome wie üblich addiert und multipliziert. Wir zeigen dies anhand von Beispielen:

$$f(x) = x^2 + x + 1 \in \mathbb{R}[x] \quad \text{und} \quad g(x) = 2x^3 - x^2 + 5x - 1 \in \mathbb{R}[x]$$

Es ist dann:

$$\begin{aligned} f(x) + g(x) &= (x^2 + x + 1) + (2x^3 - x^2 + 5x - 1) \\ &= 2x^3 + 6x \end{aligned}$$

und

$$\begin{aligned} f(x)g(x) &= (x^2 + x + 1)(2x^3 - x^2 + 5x - 1) \\ &= 2x^5 - x^4 - x^2 + 2x^4 - x^3 + 5x^2 - x + 2x^3 - x^2 + 5x - 1 \\ &= 2x^5 + x^4 + x^3 + 3x^2 + 4x - 1 \end{aligned}$$

In der Kryptographie und Codierungstheorie betrachtet man ausschliesslich Polynome aus $\mathbb{F}_p[x]$, wo p eine Primzahl ist. Wir betrachten ein Beispiel für den wichtigen Spezialfall $p = 2$. Beachten Sie, dass wir 2 durch 0 ersetzen können:

$$f(x) = x^2 + x + 1 \in \mathbb{F}_2[x] \quad \text{und} \quad g(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$$

Wir erhalten:

$$\begin{aligned} f(x) + g(x) &= (x^2 + x + 1) + (x^3 + x^2 + 1) \\ &= x^3 + 2x^2 + x + 2 \\ &= x^3 + x \end{aligned}$$

und

$$\begin{aligned} f(x)g(x) &= (x^2 + x + 1)(x^3 + x^2 + 1) \\ &= x^5 + x^4 + x^2 + x^4 + x^3 + x + x^3 + x^2 + 1 \\ &= x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1 \\ &= x^5 + x + 1 \end{aligned}$$

Hinweis zur Notation: Das Polynom

$$f(x) = 3x^4 + 2x^3 + x^2 + 3x + 4 \in \mathbb{F}_p[x]$$

müssten wir eigentlich so schreiben

$$f(x) = \overline{3}x^4 + \overline{2}x^3 + x^2 + \overline{3}x + \overline{4} \in \mathbb{F}_p[x] ,$$

denn die Koeffizienten sind Äquivalenzklassen. In der Regel macht man dies jedoch nicht. Es ist klar, dass wir jeden Koeffizienten durch eine Zahl ersetzen können, die kongruent dazu ist modulo p .

Es ist aufwendig, aber nicht schwierig, zu zeigen, dass $\mathbb{K}[x]$ versehen mit der Addition und Multiplikation ein kommutativer Ring mit Einselement ist. Es gelten also die Gesetze (R1)-(R8) auf den Seiten 85 und 86. Darüberhinaus ist $\mathbb{K}[x]$ nullteilerfrei, das heisst, es gilt:

$$f(x)g(x) = 0 \implies f(x) = 0 \vee g(x) = 0$$

Hier bezeichnet 0 das Nullpolynom. Eine Menge, versehen mit zwei Operationen, welche (R1)-(R8) erfüllen, und die keine Nullteiler besitzt, nennt man in der Algebra ein **Integritätsbereich**. Beachten Sie aber, dass $\mathbb{K}[x]$ kein Körper ist. Da sich bei der Multiplikation zweier Polynome die Grade addieren, kann es zu einem Polynom $f(x)$ mit $\deg(f(x)) \geq 1$ kein Polynom $g(x)$ geben, so dass

$$f(x)g(x) = 1$$

ist. Auf der linken Seite steht ein Polynom, dessen Grad ≥ 1 ist. Rechts steht das konstante Polynom 1, dessen Grad gleich 0 ist.

4.9.3 Der euklidische Algorithmus für Polynome

Der Prototyp eines Integritätsbereichs ist $(\mathbb{Z}, +, \cdot)$. Wie in \mathbb{Z} haben wir auch in $\mathbb{K}[x]$ die Division mit Rest:

Satz 42 Seien $f(x)$ und $g(x)$ zwei Polynome in $\mathbb{K}[x]$, wobei $g(x) \neq 0$. Dann existieren eindeutige Polynome $q(x)$ und $r(x)$ in $\mathbb{K}[x]$, so dass gilt:

$$f(x) = q(x)g(x) + r(x) ,$$

wobei $\deg(r(x)) < \deg(g(x))$. Insbesondere kann $r(x)$ das Nullpolynom sein.

Wir verzichten auf den Beweis und begnügen uns mit einem Beispiel. Sei

$$f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x] \quad \text{und} \quad g(x) = x^2 + 1 \in \mathbb{F}_2[x] .$$

Wir erklären zuerst das allgemeine Vorgehen.

- (1) Gesucht wird das Monom, das heisst ein Ausdruck der Form $a_{k_1}x^{k_1}$, so dass gilt

$$\deg(f(x) - a_{k_1}x^{k_1}g(x)) < \deg(f(x)) .$$

Falls

$$\deg(f(x) - a_{k_1}x^{k_1}g(x)) < \deg(g(x))$$

kann man aufhören. Andernfalls muss man mit Schritt (2) weiterfahren. In unserem Beispiel ist das Monom gleich x^2 . Da

$$\deg(f(x) - a_{k_1}x^{k_1}g(x)) = \deg(x^3 + x + 1) > \deg(g(x)) ,$$

fahren wir mit Schritt (2) weiter.

(2) Man bestimmt ein zweites Monom $a_{k_2}x^{k_2}$, so dass gilt

$$\deg(f(x) - a_{k_1}x^{k_1}g(x) - a_{k_2}x^{k_2}g(x)) < \deg(f(x) - a_{k_1}x^{k_1}) .$$

Falls

$$\deg(f(x) - a_{k_1}x^{k_1}g(x) - a_{k_2}x^{k_2}g(x)) < \deg(g(x)) ,$$

kann man aufhören, andernfalls muss man einen dritten Schritt ausführen. In unserem Beispiel ist das zweite Monom gleich x und

$$\deg(f(x) - a_{k_1}x^{k_1}g(x) - a_{k_2}x^{k_2}g(x)) = \deg(1) < \deg(g(x)) .$$

Wir können also aufhören.

Es ist nützlich die verschiedenen Schritte folgendermassen aufzuschreiben:

$$\begin{array}{r} (x^4 + x^3 + x^2 + x + 1) \div (x^2 + 1) = x^2 + x \\ - (x^4 + + + +) \\ \hline + x^3 + + + \\ - (x^3 + + +) \\ \hline + + + + 1 \\ + + + + 1 \\ \hline + + + + 0 \end{array}$$

Also ist

$$q(x) = x^2 + x \quad \text{und} \quad r(x) = 1$$

und es gilt

$$x^4 + x^3 + x + 1 = (x^2 + x)(x^2 + 1) + 1 .$$

Beispiel 62 Dividieren Sie das Polynom $f(x) = 3x^4 + 4x^2 + x + 2$ durch das Polynom $g(x) = x^2 + 2$ in $\mathbb{F}_5[x]$.

Die Aufgabe wird im Unterricht gelöst. ◇

Genau gleich wie in \mathbb{Z} definieren wir in $\mathbb{K}[x]$ den Begriff des Teilers:

Definition 10 Seien $f(x)$ und $g(x)$ Polynome in $\mathbb{K}[x]$. Das Polynom $g(x)$ ist ein **Teiler** oder **Faktor** des Polynoms $f(x)$, falls ein Polynom $h(x)$ in $\mathbb{K}[x]$ existiert, so dass gilt:

$$f(x) = g(x)h(x) .$$

Wir schreiben dann wie üblich $g(x)|f(x)$.

Wir können jetzt definieren, was wir unter einem grössten gemeinsamen Teiler (ggT) verstehen:

Definition 11 Seien $f(x)$ und $g(x)$ Polynome in $\mathbb{K}[x]$. Das Polynom $d(x)$ in $\mathbb{K}[x]$ ist ein **grösster gemeinsamer Teiler** von $f(x)$ und $g(x)$, wenn die folgenden beiden Bedingungen erfüllt sind:

- (i) $d(x)$ ist ein Teiler von $f(x)$ und $g(x)$.
- (ii) Jeder gemeinsame Teiler von $f(x)$ und $g(x)$ ist ein Teiler von $d(x)$.

Beachten Sie bitte, dass der grösste gemeinsame Teiler nur bis auf ein Vielfaches eines konstanten Polynoms $c \in \mathbb{K} \setminus \{0\}$ bestimmt ist. Dies folgt aus der Tatsache, dass c ein multiplikatives Inverses besitzt. In \mathbb{Z} gibt es zwei Elemente, die ein multiplikatives Inverses besitzen: -1 und 1 . Der ggT ist in \mathbb{Z} eindeutig, weil wir verlangen, dass er positiv sein soll.

Wir können den ggT zweier Polynome $f(x)$ und $g(x)$ in $\mathbb{K}[x]$ mit dem euklidischen Algorithmus bestimmen. Wir definieren $r_0(x) := f(x)$ und $r_1(x) := g(x)$ und führen sukzessive Divisionen mit Rest durch:

$$\begin{aligned} r_0(x) &= q_1(x)r_1(x) + r_2(x) \\ r_1(x) &= q_2(x)r_2(x) + r_3(x) \\ r_2(x) &= q_3(x)r_3(x) + r_4(x) \\ &\vdots \\ r_{n-2}(x) &= q_{n-1}(x)r_{n-1}(x) + r_n(x) \\ r_{n-1}(x) &= q_n(x)r_n(x) \end{aligned}$$

wobei gilt:

$$\deg(r_1(x)) > \deg(r_2(x)) > \deg(r_3(x)) > \dots > \deg(r_{n-1}(x)) > \deg(r_n(x))$$

Da der Grad des Restpolynoms stets kleiner wird, muss der Algorithmus einmal abbrechen, indem man als Restpolynom das Nullpolynom erhält. Weiter ist klar, dass das zweitletzte Restpolynom, $r_n(x)$, ein ggT von $f(x)$ und $g(x)$ ist. Aus der letzten Gleichung folgt nämlich, dass $r_n(x)$ ein Teiler von $r_{n-1}(x)$ ist. Dann folgt aus der zweitletzten Gleichung, dass $r_n(x)$ auch ein Teiler von $r_{n-2}(x)$ ist. Indem wir so von unten nach oben gehen, sehen wir, dass $r_n(x)$ ein gemeinsamer Teiler von $r_0(x)$ und $r_1(x)$ ist.

Umgekehrt folgt aus der ersten Gleichung, dass ein gemeinsamer Teiler $h(x)$ von $r_0(x)$ und $r_1(x)$ auch ein gemeinsamer Teiler von $r_2(x)$ ist. Aus der zweiten Gleichung folgt dann, dass $h(x)$ auch ein Teiler von $r_3(x)$ ist, usw. Schliesslich folgt aus der zweitletzten Gleichung, dass $h(x)$ ein Teiler von $r_n(x)$ ist.

Beispiel 63 Gegeben sind

$$f(x) = x^5 + x^4 + 2x^3 + 3x \in \mathbb{F}_5[x] \quad \text{und} \quad g(x) = x^4 + 4x^3 + 3x + 1 \in \mathbb{F}_5[x].$$

Bestimmen Sie einen ggT von $f(x)$ und $g(x)$.

Die Aufgabe wird im Unterricht gelöst. ◇

Wie in \mathbb{Z} gilt der folgende Satz:

Satz 43 Seien $f(x)$ und $g(x)$ Polynome in $\mathbb{K}[x]$ und sei $d(x)$ ein ggT. Dann existieren Polynome $\lambda(x)$ und $\mu(x)$ in $\mathbb{K}[x]$, so dass gilt:

$$\lambda(x)f(x) + \mu(x)g(x) = d(x)$$

Bew.: Dies folgt sofort aus dem euklidischen Algorithmus, indem wir sukzessive nach den Restpolynomen auflösen. Aus der ersten Gleichung folgt:

$$r_2(x) = f(x) - q_1(x)g(x)$$

Wir setzen dann in der zweiten Gleichung für $r_1(x)$ $g(x)$ und für $r_2(x)$ den Ausdruck $f(x) - q_1(x)g(x)$ ein und lösen nach $r_3(x)$ auf:

$$r_3(x) = g(x) - q_2(x)(f(x) - q_1(x)g(x)) = [1 + q_1(x)q_2(x)]g(x) - q_2(x)f(x)$$

usw. □

Beispiel 64 Bestimmen Sie für die Polynome aus dem vorhergehenden Beispiel die Polynome $\lambda(x)$ und $u(x)$.

Die Aufgabe wird im Unterricht gelöst. \diamond

4.9.4 Faktorisierung von Polynomen

Sei $f(x)$ ein Polynom von Grad n in $\mathbb{K}[x]$. Wenn $x - c$ ($c \in \mathbb{K}$) ein Linearfaktor von $f(x)$ ist, dann existiert ein Polynom $q(x)$ in $\mathbb{K}[x]$ mit Grad $n - 1$, so dass gilt:

$$f(x) = (x - c)q(x)$$

Aus dieser Beziehung folgt, dass $f(c) = 0$ ist. Das Element c ist also eine Nullstelle des Polynoms $f(x)$.

Wir betrachten jetzt den umgekehrten Fall, wo $f(c) = 0$ ist. Wir dividieren $f(x)$ durch $x - c$ und erhalten:

$$f(x) = (x - c)q(x) + r,$$

wobei r ein konstantes Polynom ist. Wenn wir für x das Element c einsetzen, so ergibt sich aufgrund der Voraussetzung:

$$0 = f(c) = (c - c)q(c) + r = r$$

Also muss $r = 0$ sein und $x - c$ ist ein Linearfaktor von $f(x)$.

Wir haben den folgenden Satz bewiesen:

Satz 44 Sei $f(x)$ ein Polynom in $\mathbb{K}[x]$ und $c \in \mathbb{K}$. Dann gilt:

$$x - c \text{ ist ein Linearfaktor von } f(x) \iff f(c) = 0$$

Da wir bei einem Polynom n -ten Grades höchstens n Linearfaktoren abspalten können, kann ein Polynom n -ten Grades **höchstens** n Nullstellen in \mathbb{K} haben.

Zur Konstruktion der endlichen Körper benötigen wir Polynome, für welche es nur triviale Zerlegungen gibt.

Definition 12 Ein Polynom $f(x)$ in $\mathbb{K}[x]$ heisst **irreduzibel**, wenn die beiden folgenden Bedingungen erfüllt sind:

(i) $\deg(f(x)) \geq 1$

(ii) Es gilt:

$$f(x) = g(x)h(x) \implies \deg(f(x)) = 0 \vee \deg(g(x)) = 0$$

Bemerkungen:

- Die irreduziblen Polynome spielen in $\mathbb{K}[x]$ die gleiche Rolle wie die Primzahlen in \mathbb{Z} .
- In $\mathbb{C}[x]$ sind die irreduziblen Polynome identisch mit den Polynomen von Grad 1 (=lineare Polynome). Gemäss dem Fundamentalsatz der Algebra kann ein Polynom n -ten Grades, $n \geq 2$, in n Linearfaktoren zerlegt werden. Ist also reduzibel.
- In $\mathbb{R}[x]$ und $\mathbb{Q}[x]$ gibt es hingegen irreduzible Polynome mit Grad ≥ 2 . Beispielsweise kann $x^2 + 1$ nicht als Produkt zweier Linearfaktoren dargestellt werden.

- Das Polynom $x^2 - 2$ ist irreduzibel in $\mathbb{Q}[x]$, denn $\sqrt{2} \notin \mathbb{Q}$, aber reduzibel in $\mathbb{R}[x]$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

- Im Folgenden interessieren wir uns nur für Polynome in $\mathbb{F}_p[x]$. Wir betrachten zuerst quadratische Polynome:

$$f(x) = a_2x^2 + a_1x + a_0 \quad , \quad a_2, a_1, a_0 \in \mathbb{F}_p \wedge a_2 \neq 0$$

$f(x)$ ist genau dann reduzibel, wenn $f(x)$ das Produkt zweier Linearfaktoren ist. Aufgrund von Satz 44 ist dies genau dann der Fall, wenn ein $c \in \mathbb{F}_p$ existiert mit $f(c) = 0$. Wir können also einfach die Werte

$$0, 1, 2, \dots, p-1 \tag{22}$$

(eigentlich müssten wir diese wieder als Äquivalenzklassen schreiben) in das Polynom einsetzen und prüfen, ob wir 0 erhalten. Wenn wir nie 0 erhalten ist das Polynom irreduzibel.

Auch für kubische Polynome ist die Situation einfach. Ein kubisches Polynom

$$f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \quad , \quad a_3, a_2, a_1, a_0 \in \mathbb{F}_p \wedge a_3 \neq 0$$

ist genau dann reduzibel, wenn es das Produkt eines Linearfaktors und eines quadratischen Polynoms ist. Es genügt also wiederum die Werte (22) einsetzen. Wenn wir nie 0 erhalten ist das Polynom irreduzibel.

Für Polynome $f(x)$ mit $\deg(f(x)) \geq 4$ können wir nicht mehr so vorgehen, denn es können jetzt Zerlegungen auftreten, die keinen Linearfaktor enthalten.

Es gibt effiziente Algorithmen, mit denen festgestellt werden kann, ob ein Polynom über einem endlichen Körper irreduzibel ist oder nicht. In Computeralgebrasytemen wie *Mathematica* oder *Maple* ist ein solcher Algorithmus implementiert.

Beispiel 65 Überprüfen Sie, ob die folgenden Polynome irreduzibel sind:

$$(a) \ x^2 + x + 1 \in \mathbb{F}_2[x] \quad (b) \ x^3 + x^2 + 1 \in \mathbb{F}_2[x] \quad (c) \ x^4 + x^2 + 1 \in \mathbb{F}_2[x]$$

Die Aufgabe wird im Unterricht gelöst. ◇

4.9.5 Konstruktion der endlichen Körper

Ausgehend von \mathbb{Z} sind wir zu endlichen Körpern gelangt, indem wir Äquivalenzklassen modulo p , wo p eine Primzahl ist, gebildet haben. Wir übertragen jetzt dieses Verfahren auf $\mathbb{F}_p[x]$. Wir benötigen dazu ein irreduzibles Polynom in $\mathbb{F}_p[x]$ vom Grad n . Der folgende Satz garantiert die Existenz eines solchen Polynoms:

Satz 45 Zu jeder Primzahl p und jeder natürlichen Zahl n existiert ein irreduzibles Polynom vom Grad n in $\mathbb{F}_p[x]$. Das Polynom ist darüberhinaus normiert, das heisst, der Koeffizient a_n ist gleich 1.

Wir werden diesen Satz nicht beweisen. In praktischen Anwendungen, ist das irreduzible Polynom sowieso gegeben. Es sei noch betont, dass es mehrere solche Polynome gibt. Um die Rechnungen zu vereinfachen, wird man eines wählen, wo möglichst viele Koeffizienten gleich Null sind.

Wir bezeichnen das irreduzible Polynom mit $f(x)$. Wie in \mathbb{Z} definiert man dann für $g(x), h(x) \in \mathbb{F}_p[x]$ die folgende Relation:

$$g(x) \equiv h(x) \pmod{f(x)} \iff f(x) | (g(x) - h(x)) \quad (23)$$

Wir erhalten so eine Äquivalenzrelation auf $\mathbb{F}_p[x]$. Die Äquivalenzklassen werden durch die möglichen Restpolynome, die bei der Division durch $f(x)$ entstehen können, gebildet. Im allgemeinen Fall hat ein solches Polynom n Koeffizienten, die alle die Werte

$$0, 1, 2, \dots, p-1$$

annehmen können. Daraus folgt, dass es p^n solche Polynome und damit Äquivalenzklassen gibt. Wir bezeichnen die Menge dieser Äquivalenzklassen mit $\text{GF}(p^n)$. Die Bezeichnung ist eine Abkürzung für *Galois Field*.

Beispiel 66 Das Polynom $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ ist irreduzibel. Bestimmen Sie die Äquivalenzklassen der Relation (23).

Die Aufgabe wird im Unterricht gelöst. \diamond

Auf der Menge der Äquivalenzklassen definieren wir dann wie üblich eine Addition und eine Multiplikation:

$$\overline{g(x)} + \overline{h(x)} = \overline{g(x) + h(x)}$$

und

$$\overline{g(x)} \cdot \overline{h(x)} = \overline{g(x)h(x)}$$

Diese Operationen sind wiederum wohldefiniert, das heisst, unabhängig von den gewählten Repräsentanten in den Äquivalenzklassen. Weiter gelten die Gesetze (R1)-(R8) auf den Seiten 85 und 86. Es gilt aber auch (R9), das heisst, zu jedem $\overline{g(x)} \in \text{GF}(p^n)$ und $\overline{g(x)} \neq \bar{0}$ existiert ein $\overline{h(x)} \in \text{GF}(p^n)$, so dass gilt:

$$\overline{g(x)} \cdot \overline{h(x)} = \bar{1}$$

Beweis: Da $f(x)$ ein irreduzibles Polynom ist, ist der ggT von $f(x)$ und $g(x)$ ein konstantes Polynom $d \in \mathbb{F}_p$. Genau genommen ist jedes konstante Polynom ein ggT, denn der ggT ist nur bis auf ein Vielfaches von $c \in \mathbb{F}_p$ eindeutig bestimmt. Gemäss Satz (43) existieren Polynome $\lambda(x)$ und $\mu(x)$ in $\mathbb{F}_p[x]$, so dass gilt:

$$\lambda(x)f(x) + \mu(x)g(x) = d \quad (24)$$

Wir erhalten diese Gleichung mit dem erweiterten euklidischen Algorithmus. Das konstante Polynom d ist nicht unbedingt gleich 1. Wir erhalten eine Gleichung mit 1 auf der rechten Seite, indem wir (24) mit d^{-1} multiplizieren:

$$d^{-1}\lambda(x)f(x) + d^{-1}\mu(x)g(x) = 1$$

Das multiplikative Inverse von $\overline{g(x)}$ ist dann gegeben durch

$$\overline{g(x)}^{-1} = \overline{d^{-1}\mu(x)}.$$

Diese Berechnungen sind zwar elementar, aber für grössere Werte von n werden sie von Hand sehr aufwendig. Die Verwendung eines Computeralgebrasystems wie *Mathematica* oder *Maple* ist empfehlenswert.

Hinweis zur Notation: Wir werden nachher darauf verzichten, das Polynom $g(x)$ zu überstreichen, denn es ist klar, dass $g(x)$ ein Repräsentant einer Äquivalenzklasse ist. Die Elemente von $\text{GF}(p^n)$ sind zwar Äquivalenzklassen, aber die konkreten Berechnungen werden mit Repräsentanten durchgeführt.

Betrachten wir ein Beispiel: $f(x) = x^4 + x^3 + x^2 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$. Wir bestimmen das multiplikative Inverse von $g(x) = x^2 + x + 1 \in \text{GF}(2^4)$. Wir wenden zuerst den euklidischen Algorithmus an:

$$\begin{aligned} x^4 + x^3 + x^2 + x + 1 &= x^2(x^2 + x + 1) + (x + 1) \\ x^2 + x + 1 &= x(x + 1) + 1 \end{aligned}$$

Also ist 1 ein ggT. Wir schreiben dann

$$f(x) = x^2 \cdot g(x) + (x + 1)$$

und lösen die Gleichungen nach dem Restpolynom auf:

$$\begin{aligned} x + 1 &= f(x) - x^2 g(x) \\ 1 &= g(x) - x(f(x) - x^2 g(x)) = (x^3 + 1)g(x) - xf(x) \end{aligned}$$

Also ist $g(x)^{-1} = x^3 + 1$.

Die Menge $\text{GF}(p^n)$ versehen mit der obigen Addition und Multiplikation bildet also einen Körper mit p^n Elementen. Man bezeichnet diese Körper als **Galois-Körper** zu Ehren von Évariste Galois¹⁵

Bemerkungen:

- Für $n = 1$ erhalten wir die bereits bekannten Körper \mathbb{F}_p .
- Man kann beweisen, dass es bis auf Isomorphie nur einen Körper mit p^n Elementen gibt.
- Man kann beweisen, dass es keine weiteren endlichen Körper mehr gibt.
- Für die Anwendungen in der Kryptographie und Codierungstheorie sind vor allem die Körper $\text{GF}(2^n)$ wichtig, weil dann im Binärsystem gerechnet werden kann.

4.9.6 Anwendungen

In endlichen Körpern stehen uns wie in $(\mathbb{R}, +, \cdot)$ alle vier Grundoperationen zur Verfügung. Der Körper $(\mathbb{R}, +, \cdot)$ eignet sich gut um kontinuierliche Phänomene zu modellieren. In der digitalen Informationsverarbeitung treten jedoch oft diskrete Fragestellungen auf, für welche die endlichen Körper besser geeignet sind. Wir können im Folgenden nur zwei Hauptanwendungsgebiete skizzieren. Eine vertiefte Behandlung ist leider aus Zeitgründen nicht möglich.

Ein Anwendungsgebiet endlicher Körper ist die Codierungstheorie. In der Codierungstheorie geht es darum Information so zu codieren, dass Fehler erkannt und wenn möglich korrigiert werden können. Eine wichtige Klasse von fehlerkorrigierenden Codes sind die Reed-Solomon-Codes. Diese Codes wurden 1982 bei der Fehlerkorrektur von Compact Disks eingesetzt.

¹⁵Évariste Galois (1811 Bourg-La-Reine - 1832 Paris): französischer Mathematiker entwickelte eine Methode, mit der man herausfinden kann, welche polynomialen Gleichungen durch verschachtelte Wurzelausdrücke gelöst werden können. Diese Methode entwickelte sich zu einer mathematischen Theorie, der **Galois-Theorie**. Galois gilt auch als Erfinder des Gruppenbegriffs.

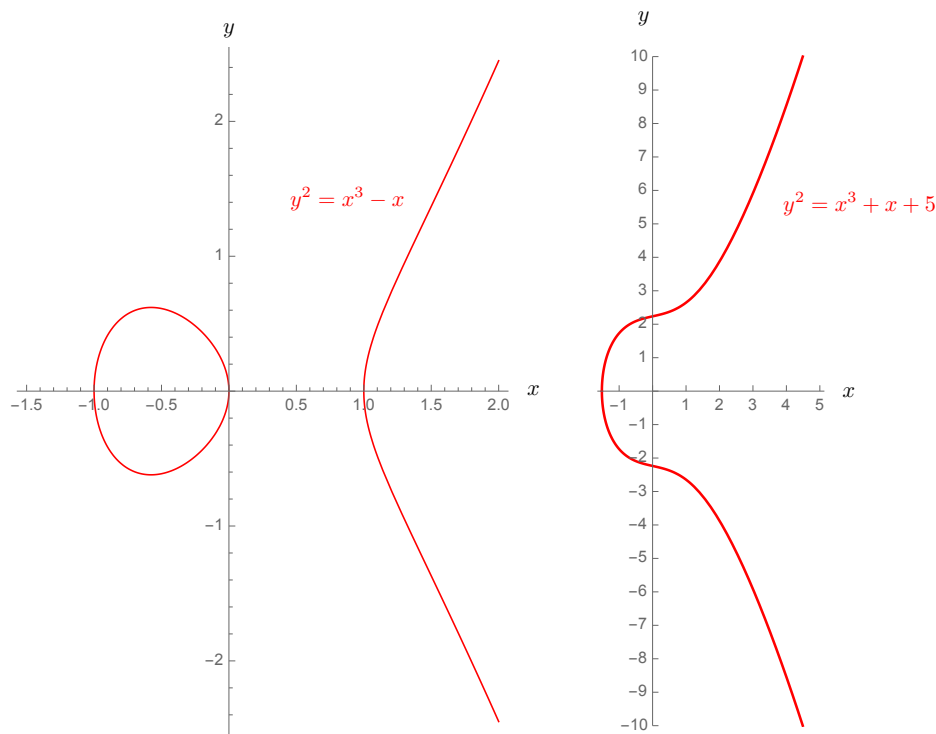
Gehen wir etwas genauer auf das zweite Anwendungsgebiet endlicher Körper ein. **Elliptische Kurven** über \mathbb{R} werden durch Gleichungen der Form

$$y^2 = x^3 + ax + b$$

definiert. Hier sind a, b gegebene reelle Zahlen, welche die Bedingung

$$4a^3 + 27b^2 \neq 0$$

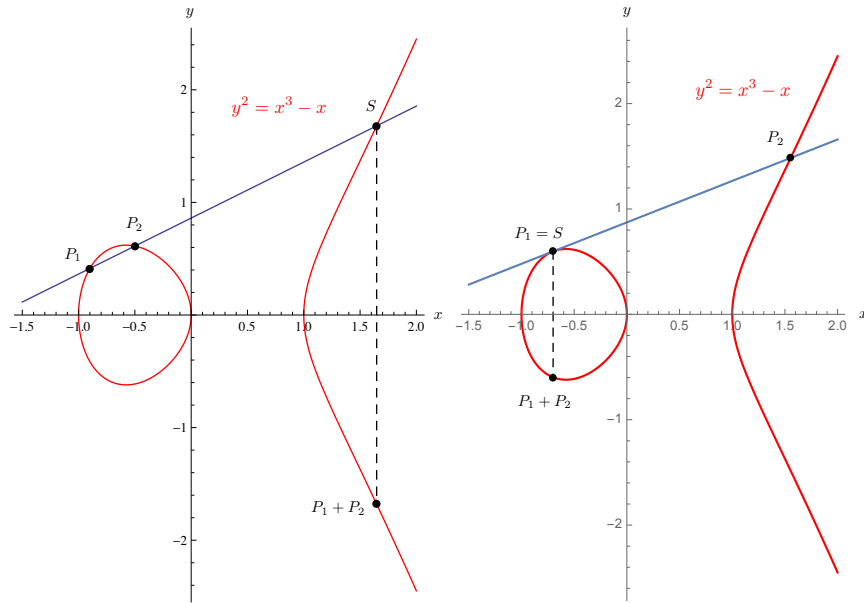
erfüllen. Diese Bedingung garantiert, dass das kubische Polynom $x^3 + ax + b$ entweder 3 verschiedene reelle oder eine reelle und zwei komplexe konjugierte Nullstellen besitzt. Die Kurve wird durch alle Punkte $(x, y) \in \mathbb{R}^2$ gebildet, welche die Gleichung erfüllen sowie einem zusätzlichen Punkt im Unendlichen, der mit \mathcal{O} bezeichnet wird. Nachfolgend sind zwei elliptische Kurven abgebildet:



Auf der Menge E dieser Punkte wird eine Addition definiert. Seien $P_1(x_1, y_1)$ und $P_2(x_2, y_2)$ zwei Punkte der Kurve E . Es müssen verschiedene Fälle unterschieden werden:

- (1) Sei $x_1 \neq x_2$.

Die Graphik auf der linken Seite zeigt die Situation, wo die Gerade durch P_1 und P_2 nicht Tangente an die Kurve ist. Die Gerade schneidet dann die Kurve in einem dritten Punkt S . Der Spiegelpunkt von S bezüglich der x -Achse wird als Summe $P_1 + P_2$ definiert. In der Graphik rechts ist die Gerade durch P_1 und P_2 Tangente an die Kurve. Der dritte Schnittpunkt S fällt mit P_1 zusammen. Der Spiegelpunkt ist wiederum als Summe $P_1 + P_2$ definiert.



Wir bezeichnen die Koordinaten von $P_1 + P_2$ mit (x_3, y_3) . Algebraisch ergeben beide Fälle die gleichen Formeln, nämlich:

$$\left. \begin{aligned} x_3 &= \alpha^2 - x_1 - x_2, \\ y_3 &= \alpha(x_1 - x_3) - y_1 \end{aligned} \right\} \quad \text{wobei} \quad \alpha = \frac{y_2 - y_1}{x_2 - x_1} \quad (25)$$

2. Falls $x_1 = x_2$, aber $y_1 \neq y_2$, dann ist die Gerade durch P_1 und P_2 parallel zur y -Achse. Die Gerade schneidet dann die Kurve im Unendlichen. Deshalb definiert man $P_1 + P_2 = \mathcal{O}$.
3. Falls $P_1 = P_2$ und $y_1 \neq 0$, dann betrachtet man die Tangente an die Kurve im Punkt $P_1 = P_2$. Neben diesem Berührungspunkt existiert ein Schnittpunkt S . $P_1 + P_1$ wird wiederum als Spiegelpunkt von S definiert. Es ergeben sich die Formeln:

$$\left. \begin{aligned} x_3 &= \alpha^2 - 2x_1, \\ y_3 &= \alpha(x_1 - x_3) - y_1 \end{aligned} \right\} \quad \text{wobei} \quad \alpha = \frac{3x_1^2 + a}{2y_1} \quad (26)$$

4. Falls $P_1 = P_2$ und $y_1 = 0$, dann definieren wir $P_1 + P_2 = \mathcal{O}$.

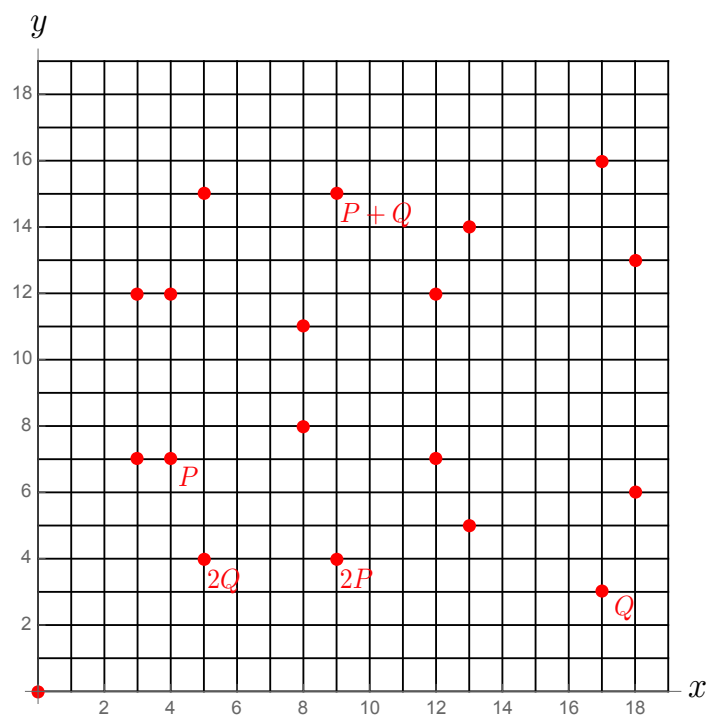
Wir erhalten so eine kommutative Gruppe $(E(a, b), +)$. Beachten Sie bitte, dass die Gruppenoperation additiv geschrieben wird:

- Der Punkt im Unendlichen \mathcal{O} ist das Neutralelement.
- Der Punkt $P(x, y)$ besitzt den inversen Punkt $-P(x, -y)$.
- Die Operation ist assoziativ $(P + Q) + R = P + (Q + R)$. Der Nachweis dieser Eigenschaft ist sehr aufwendig und benötigt Resultate aus der projektiven Geometrie.
- Die Operation ist kommutativ $P + Q = Q + P$.

Wenn Sie die obigen Formeln (25) und (26) betrachten, so stellen Sie fest, dass nur die Grundoperationen vorkommen, welche in jedem Körper definiert sind. Für Anwendungen in der Kryptographie ist der Körper \mathbb{R} nicht geeignet, denn man muss exakt ohne Rundungsfehler rechnen. Es bieten sich die endlichen Körper \mathbb{F}_p oder $\text{GF}(2^n)$ an. Natürlich besteht eine elliptische Kurve über diesen Körpern nur aus isolierten Punkten. Nachfolgend ist die elliptische Kurve

$$y^2 \equiv x^3 + x \pmod{19}$$

abgebildet:



Das diskrete Logarithmusproblem (DLP) lautet in der Gruppe $(E, +)$ folgendermassen. Gegeben ist ein Basispunkt B sowie ein beliebiger Punkt P . Der Basispunkt muss eine möglichst hohe Ordnung haben. P muss in der Untergruppe liegen, die von B erzeugt wird. Wenn B ein erzeugendes Element der Gruppe $(E, +)$ ist, dann ist diese Bedingung automatisch erfüllt. Gesucht wird eine natürliche Zahl k , so dass

$$kB = P$$

ist. Die Lösung dieses Problems ist in der Regel viel aufwendiger als das analoge Problem in der Gruppe (\mathbb{Z}_p^*, \cdot) . Aus diesem Grund kann der Parameter p wesentlich kleiner gewählt werden. Auch wenn die Operationen in $E(a, b, p, +)$ oder $E(a, b, 2^n, +)$ zur Codierung und Decodierung aufwendiger sind als in (\mathbb{Z}_p^*, \cdot) zahlt sich dies aus.

The End

Literatur

- [1] Beutelspacher, Albrecht; Schwarzpaul Thomas; Neumann Heike B.: *Kryptografie in Theorie und Praxis*, Vieweg, 2005
- [2] Beutelspacher, Albrecht; Zschiegner, Marc Alexander: *Diskrete Mathematik für Einsteiger*, Vieweg, 2002
- [3] Clark, John; Holton, Derek Allan: *Graphentheorie*, Übersetzung der englischen Ausgabe, Spektrum, 1994
- [4] Forster, Otto, *Algorithmische Zahlentheorie*, 2. Auflage, Springer Spektrum, 2015
- [5] Cogis, Olivier; Robert, Claudine: *Théorie des graphes*, Vuibert, 2003
- [6] Haggarty, Rod: *Mathématiques discrètes appliquées à l'informatique*, traduction de l'édition américaine, Pearson Education, 2005
- [7] Kumanduri, Ramanujachary; Romero, Cristina : *Number theory with computer applications*, Prentice Hall, 1998
- [8] Nitzsche, Manfred: *Graphen für Einsteiger*, Vieweg, 2004
- [9] Rosen, Kenneth H.: *Discrete mathematics and its applications*, 6th edition, Mc Graw-Hill International edition, 2007
- [10] Rosen, Kenneth H.: *Mathématiques discrètes*, traduction de l'édition américaine, Chenelière Mc Graw-Hill, 2002
- [11] Rosen, Kennet H.: *Elementary Number Theory*, 6th edition, Pearson, 2014
- [12] Teschl, Gerald; Teschl, Susanne: *Mathematik für Informatiker - Band 1: Diskrete Mathematik und Lineare Algebra*, Springer, 2006
- [13] Winter, Reiner: *Grundlagen der formalen Logik*, 2. Auflage, Verlag Harri Deutsch, 2001

Stichwortverzeichnis

- abgeschlossen, 72
- Adjazenzmatrix, 15
- Algorithmus
 - von Dijkstra, 32
 - von Kruskal, 30
 - von Prim, 31
- Baum, 23
 - erzeugender, 29
 - minimaler erzeugender, 30
- Binomialkoeffizient, 7
- Brücke, 26
- Diedergruppe, 72
- Digraph, 51
- diskretes Logarithmus-Problem, 88
- Elliptische Kurven, 100
- erzeugendes Element, 83
- Eulerscher Polyedersatz, 40
- Eulertour, 19
- Fakultät, 4
- Folge
 - n -gliedrige, 58
 - Fibonacci, 59
 - geometrische, 60
 - unendliche, 58
- Formel
 - Ein- und Ausschluss, 10
 - explizite, 58
- Glied einer Folge, 58
- Grad (eines Knoten), 16
- Graph, 12, 13
 - bipartiter, 53
 - dualer, 46
 - ebener, 39
 - einfacher, 14
 - Eulerscher, 19
 - gerichteter, 51
 - gewichteter, 30
 - hamiltonischer, 22
 - plättbarer, 39
 - planarer, 39
 - regulärer, 43, 56
 - zusammenhängender, 18
- Gruppe, 72
 - zyklisch, 77, 83
- Handshaking Lemma, 16
- Heiratssatz von Hall, 55
- Index, 80
- Integritätsbereich, 93
- Inverse, 73
- inverse Element, 71
- irreduzibel, 96
- Isometrie, 70
- isomorph, 75
- Isomorphismus, 15
- Isthmus, 26
- Königsberger Brückenproblem, 12
- Körper, 91
- Kanten, 13, 14
- Knoten, 13, 14
- Kombination, 7
 - mit Wiederholung, 9
- Loop, 14
- Matching, 54
- Mehrfachkanten, 14
- Nachbarknoten, 17
- Netzwerk, 52
- Neutralelement, 71, 73
- Normalteiler, 79
- Nullpolynom, 92
- Nullteiler, 86
- Ordnung, 73
- Paarung, 54
 - maximale, 54
 - perfekte, 54
- Permutation, 3
- Pfad, 17
- Platonischer Körper, 42
- Polyeder, 42
- Produktprinzip, 1
- Programmierung
 - rekursive, 62
- Rekursionsformel, 58
- Rekursionstiefe, 58
- Schleife, 14
- Schubfachprinzip, 2
- Summenprinzip, 1
- Türme von Hanoi, 60

Untergraph, 29

Variation

ohne Wiederholung, 6

Vierfarbensatz, 45

Wald, 26

Weg, 17

Zyklus, 17