Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Számítástudományi és Információelméleti Tanszék

Német nyelvű számítástudományi példatár

Mann Zoltán, Orbán András és Recski András

Budapest, 2001

Bevezetés

Ez a példatár azoknak a hallgatóknak készült, akik a Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Karán a **német nyelvű képzés keretében** hallgatják

- a műszaki informatika szakon az *Einführung in die theoretische Informatik* tárgyat (a magyar nyelvű "Bevezetés a számításelméletbe" tárgy helyett), vagy
- a villamosmérnöki szakon a *Grundlagen der theoretischen Informatik* tárgyat (a magyar nyelvű "A számítástudomány elemei" tárgy helyett).

A példatár 18 része több, mint 200 feladatot tartalmaz, megoldásokkal együtt. A példák egy részéhez megoldási ötletet is adunk, ezeket a sor szélén lévő  ábra jelzi.

Az anyag összeállításakor felhasználtuk számos kollégánk, így elsősorban Friedl Katalin, ifj. Katona Gyula, Rónyai Lajos és Simonyi Gábor, valamint számos volt diákunk, elsősorban Faragó Gergely, Harcos Gergely, Koblinger Egmont, Németh Zoltán és Urbán Péter feladatgyűjteményeit. Rajtuk kívül köszönettel tartozunk támogatásáért a "Pro Renovanda Cultura Hungariæ" alapítvány "Tudomány az oktatásban" szakalapítványának is.

Recski András

Inhaltsverzeichnis

Aufgaben

1 Kombinatorik

1.1 Elementare Kombinatorik

1.1.1. Was ist die Anzahl der Reihenfolgen von 2 weissen und 6 schwarzen Kugeln, wenn die zwei weissen nicht nebeneinander stehen dürfen?

1.1.2. Was ist die Anzahl der Möglichkeiten, wie König Arthur und seine $n-1$ Ritter (insgesamt n Personen) an dem runden Tisch sitzen können? (2 Reihenfolgen werden nicht unterschieden, falls jeder die gleichen Nachbarn hat.)

1.1.3. Es gibt zwei Schachteln. In Schachtel A sind alle Dominosteine genau einmal darin, die an beiden Hälften eine Zahl zwischen 1 und 8 haben. In Schachtel B sind alle Dominosteine genau einmal darin, die an beiden Hälften eine Zahl zwischen 1 und 9 haben, aber die Doppelsteine (z. B. (7,7)) sind nicht enthalten. In welcher Schachtel gibt es mehr Dominos? (Die Dominos (2,1) und (1,2) sind gleich.)

1.1.4. Man würfelt 10-mal mit einem gewöhnlichen Spielwürfel. Was ist die Anzahl der möglichen Ergebnisfolgen, falls mindestens einmal die 6 gewürfelt werden muss?

1.1.5. Auf einem $n \times n$-Schachbrett soll der König aus der linken unteren Ecke die rechte obere Ecke erreichen, wobei er in jedem Schritt entweder ein Feld nach rechts oder ein Feld nach oben gezogen werden kann. Was ist die Anzahl der verschiedenen möglichen Wegen?

1.1.6. Es gibt $2n$ Kinder, die alle unterschiedlichen Grössen haben. Wir müssen sie in 2 Reihen stellen, so dass sie fotografiert werden können. (Jedes Kind in der zweiten Reihe muss grösser sein als das vor ihm stehende.) Was ist die Anzahl der verschiedenen Fotos?

1.1.7. Was ist die Anzahl solcher Kopf-Wappen Reihen der Länge n, die in beiden Richtungen gelesen gleich sind? (Z. B.: WKKWWKKW)

1.1.8. Ein Club hat 25 Mitglieder. Wieviele Möglichkeiten hat man, einen Präsidenten und 2 Vizepräsidenten zu wählen?

1.1.9. Beim Skat bekommt man 8 Karten aus 32. Was ist die Anzahl der Möglichkeiten, dass man genau
a) 2 Asse
b) 2 rote Karten und einen König
bekommt?

1.1.10. Man finde eine geschlossene Form für die folgenden Ausdrücke:
a) $\sum_{k=0}^{n} \binom{n}{k}$

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

c) $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}$

d) $\sum_{k=0}^{n} k \binom{n}{k}$

1.1.11. Man zieht 4-mal nacheinander (ohne Zurücklegen) aus einem Hut, in dem sich die Zahlen $1, 2, \ldots, 7$ befinden. Was ist die Anzahl solcher Möglichkeiten, wo die gezogenen Zahlen eine monotone Folge bilden? (Z. B. $1, 4, 5, 6$ oder $5, 4, 2, 1$)

1.1.12. Im Totospiel muss man 14 Tippe angeben. Was ist die Anzahl solcher Tippfolgen, die in einer konkreten Woche genau 13 Treffer haben?

1.1.13. Beim Lottospiel in Wunderland zählt als ein Treffer auch wenn die Zahl neben der vom Spieler markierten Zahl gezogen wird. Joachim spielt mit folgenden Zahlen:

$$1, 10, 13, 20, 75$$

Wie viele Möglichkeiten hat man, aus 90 Zahlen 5 so auszuziehen, dass Joachim 5 Treffer hat?

1.1.14. Auf einem 8×8 Schachbrett möchten wir einen Turm von der linken unteren Ecke in die rechte obere Ecke in 3 Schritten ziehen. Was ist die Anzahl der möglichen Wege?

1.2 Rekursionen

Bei diesen Aufgaben soll die Antwort immer als eine Funktion von n in expliziter Form angegeben werden.

1.2.1. Wieviele Möglichkeiten hat man, auf eine Treppe von n Stufen hochzulaufen, wenn man in jedem Schritt entweder eine Stufe oder zwei Stufen hinterlegen kann?

1.2.2. Wieviele verschiedene Matchings hat eine "Leiter" von n Stufen? (Für eine Leiter, siehe Abbildung 1. Ein Matching ist eine n-elementige Menge der Strecken der Länge 1, die alle Kopplungspunkte abdeckt.)

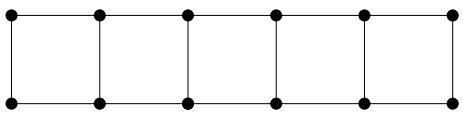


Abbildung 1: Eine Leiter mit 6 Stufen

1.2.3. Man löse die folgenden Rekursionen:
a) $a_n = 2a_{n-1} - 2a_{n-2}$, $a_0 = 1$, $a_1 = 2$
b) $a_n = 2a_{n-1} - a_{n-2}$, $a_0 = 1$, $a_1 = -1$

1.2.4. Wieviele Möglichkeiten hat man, ein $2 \times n$-Schachbrett mit 1×2-Dominosteinen abzudecken?

2 Graphentheorie

Bei diesen Aufgaben geht es immer – falls nicht anders angedeutet – um endliche, einfache Graphen. Wenn jedoch auch Schlingen erlaubt sind, dann erhöhen sie die Gradzahl des jeweiligen Punktes um 2 (und nicht um 1). Unter der Länge eines Weges versteht man die Anzahl der enthaltenen Kanten (und nicht die Anzahl der enthaltenen Knotenpunkte). Isomorphe Graphen werden nur dann als verschieden betrachtet, wenn die Aufgabe explizit aussagt, dass die Knotenpunkte verschieden, z. B. numeriert sind. Die Anzahl der Knotenpunkte wird immer – falls nicht anders angedeutet – mit n, die Anzahl der Kanten mit e bezeichnet.

2.1 Grundbegriffe der Graphentheorie

2.1.1. Wieviele nicht-isomorphe Bäume gibt es mit 7 Knotenpunkten?

2.1.2. Wieviele nicht-isomorphe Graphen gibt es, die 5 Knotenpunkte und 3 Kanten haben?

2.1.3. Wie können jene Graphen, wo jeder Punkt
a) genau 2
b) höchstens 2
Nachbarn hat, charakterisiert werden?

2.1.4. Wie sehen solche Graphen aus, wo jede Kante höchstens in einem Kreis vorkommt?

2.1.5. Sei $G_{n,k}$ ein Graph, dessen Knotenpunkte den k-elementigen Teilmengen einer n-elementigen Menge entsprechen. Zwei Punkte sind mit einer Kante verbunden, falls die entsprechenden Teilmengen disjunkt (fremd) sind.
Ist $G_{5,2}$ isomorph mit dem Petersen-Graphen (siehe Abbildung 2)?

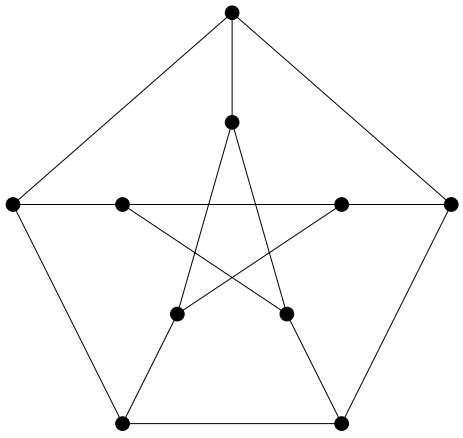


Abbildung 2: Der Petersen-Graph

2.1.6. Gebe alle nicht-isomorphen *gerichteten* Graphen an, die im *ungerichteten* Sinne Bäume sind und 4 Punkte haben!

2.1.7. Im Graphen G sei $e = n + k - 1$. Beweise, dass es mindestens k Kreise in G gibt!

2.1.8. Wie können jene Graphen charakterisiert werden, wo beliebige 2 Kanten inzident sind?

2.1.9. Sei G ein d-regulärer Graph mit $2n$ Punkten. Was ist das kleinste d, damit G sicherlich zusammenhängend ist?

2.1.10. Beweise, dass es nicht möglich ist, dass weder G, noch sein Komplement $\overline{G}$ zusammenhängend ist.

2.1.11. Sei G ein einfacher Graph. In G habe jeder Punkt mindestens k Nachbarn. Beweise:
a) es gibt einen Weg in G, der aus mindestens k Kanten besteht
b) für $k \geq 2$ es gibt einen Kreis in G, der aus mindestens $k + 1$ Kanten besteht

2.1.12. Wie können solche Kanten in einem nicht unbedingt schlichten Graphen G charakterisiert werden, die
a) in keinem aufspannenden Baum von G
b) in jedem aufspannenden Baum von G
beinhaltet sind?

2.1.13. Sei d der maximale Grad in einem Baum B. Beweise, dass es in B mindestens d Punkte mit Grad 1 gibt!

2.1.14. Im Graphen G hat jeder Knotenpunkt mindestens k Nachbarn. Beweise, dass jeder Baum mit $k + 1$ Punkten ein Teilgraph von G ist! (Genauer formuliert: zu einem beliebigen Baum mit $k + 1$ Punkten gibt es einen Teilgraphen in G, der mit diesem Baum isomorph ist.)

2.1.15. Gibt es Graphen, wo die Knotenpunkte die folgenden Gradzahlen haben?
a) $1, 1, 1, 2, 3, 3, 4, 4, 5, 7$
b) $0, 1, 1, 2, 3, 3, 4, 6, 8$
c) $1, 1, 1, 2, 2, 2, 3, 3, 3$
d) $5, 5, 5, 6, 6, 6, 7, 7, 7$
e) $1, 3, 4, 4, 5, 5$

2.1.16. Der Graph G sei ein gerichteter vollständiger Graph. Beweise, dass es einen Knotenpunkt in G gibt, so dass alle anderen Punkte aus diesem Punkt über einen gerichteten Weg, der aus höchstens 2 Kanten besteht, erreichbar sind!

2.1.17. Ein Graph ist isomorph mit seinem Komplement. Beweise, dass er zusammenhängend ist!

2.1.18. Zeige einen Graphen, der isomorph mit seinem Komplement ist, falls
a) $n = 5$
b) $n = 6$

2.1.19. Sind die Graphen in Abbildung 3 isomorph?

2.1.20. Sind die Graphen in Abbildung 4 isomorph?

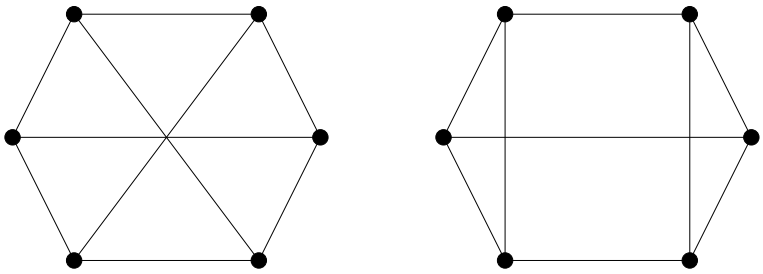


Abbildung 3:

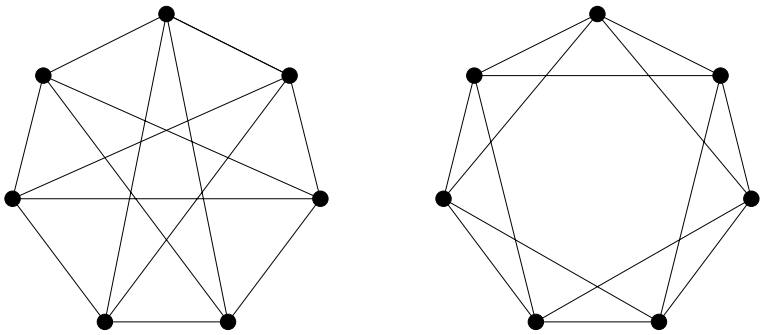


Abbildung 4:

2.1.21. Seien $d_1, \ldots, d_n$ gegebene positive ganze Zahlen, ihre Summe sei $2n-2$. Beweise, dass es einen Baum mit diesen Gradzahlen gibt!

2.1.22. Was ist die maximale Anzahl von Kanten in einem solchen einfachen Graphen, wo es unter beliebigen 3 Punkten höchstens eine Kante gibt?

2.1.23. Sei G ein einfacher Graph mit 6 Punkten. Beweise, dass entweder G oder $\overline{G}$ ein Dreieck beinhaltet!

2.2 Bipartite Graphen und Matchings

2.2.1. Man beweise, dass die Kantenmenge eines r-regulären bipartiten Graphen die Vereinigung von r disjunkten vollständigen Matchings ist!

2.2.2. Die Behauptung von Aufgabe **2.2.1.** ist für nicht bipartite Graphen nicht gültig: zeige, dass die Kantenmenge des Petersen Graphen (siehe Abbildung 2 auf Seite 8) nicht die Vereinigung von drei disjunkten vollständigen Matchings ist.

2.2.3. Sei r der maximale Grad in einem bipartiten Graphen G. Beweise, dass G mit neuen Punkten und Kanten so ergänzt werden kann, dass er r-regulär wird, und noch immer bipartit bleibt.

2.2.4. Sei r der maximale Grad in einem bipartiten Graphen G. Beweise, dass die Kantenmenge von G die Vereinigung von höchstens r disjunkten Matchings ist!

2.2.5. Der Graph G hat zwei verschiedene vollständige Paarungen. Beweise, dass es in G einen Kreis gibt! (2 Paarungen werden als verschieden betrachtet, falls sie sich in mindestens einer Kante unterscheiden.)

2.2.6. Ist es möglich, dass ein Baum zwei verschiedene vollständige Paarungen hat?

2.2.7. Beweise, dass alle Kreise in einem bipartiten Graphen eine gerade Länge haben!

2.2.8. Es ist bekannt, dass solche Graphen, in dem alle Kreise eine gerade Länge haben, sind eben die bipartite Graphen. Wie sehen solche Graphen aus, die nur Kreise ungerader Länge beinhalten?

2.2.9. Der Graph G besitzt folgende Eigenschaft: wenn man einen beliebigen Knotenpunkt (und damit auch die Kanten, die aus ihm laufen) aus G entfernt, dann hat der zurückbleibende Graph ein vollständiges Matching. Beweise, dass es in G keine Brücke gibt.

2.2.10. Sei der Graph G zusammenhängend und bipartit. In beiden Klassen von G befinden sich n Punkte. In einer der Klassen haben alle Punkte verschiedene Gradzahlen. Beweise, dass es in G ein vollständiges Matching gibt!

2.2.11. Das Kantennetz des 3-dimensionalen Würfels ist ein Graph mit 8 Knotenpunkten und 12 Kanten. Wieviele verschiedene Paarungen hat dieser Graph, wenn die Kanten numeriert sind? (2 Paarungen werden als verschieden betrachtet, falls sie sich in mindestens einer Kante unterscheiden.)

2.2.12. Sei G ein schlichter, bipartiter Graph mit einem maximalen Grad von k. Beweise, dass es ein (nicht unbedingt vollständiges) Matching in G gibt, das alle Punkte mit Gradzahl k abdeckt!

2.2.13. An einem Tischtennisturnier nehmen $2n+1$ Spieler teil. Während des Turniers muss jeder Spieler mit allen anderen genau einmal spielen. Die Spiele finden in Runden statt; die Spiele einer Runde werden gleichzeitig gespielt.
a) Beweise, dass mindestens $2n+1$ Runden stattfinden müssen!
b) Beweise, dass das Turnier in $2n+1$ Runden durchgeführt werden kann!

2.2.14. Sei G ein bipartiter Graph mit k Knotenpunkten in Klasse A und $2k$ Knotenpunkten in Klasse B. Wie kann man mit einem Algorithmus einen solchen Teilgraphen in G finden, der die Knotenpunkte in A zweimal und die Knotenpunkte in B einmal abdeckt?

2.2.15. Bestehe G aus k punktdisjunkten Kreisen. Wir möchten m Kanten einziehen so, dass G eine vollständige Paarung hat. Wann ist es möglich? Falls es möglich ist, was ist das Minimum von m?

2.2.16. Suche eine maximale Paarung in dem Graphen in Abbildung 5!

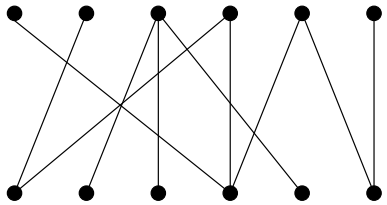


Abbildung 5:

2.3 Die vier griechischen Buchstaben: $\alpha, \tau, \nu, \varrho$

2.3.1. Bestimme den Wert der 4 griechischen Buchstaben für den Petersen-Graphen (siehe Abbildung 2 auf Seite 8)!

2.3.2. Der Graph G hat 8 Knotenpunkte, die mit $1, 2, \ldots, 8$ numeriert sind. Zwei Knotenpunkte sind mit einer Kante verbunden, falls die Differenz ihrer Zahlen 1, 2, 6 oder 7 ist. Bestimme für G den Wert der vier griechischen Buchstaben!

2.3.3. Sei H die Menge aller Graphen, wo $e = n$ gilt. Bestimme
a) $\min\{\tau(G) \ : \ G \in H\}$
b) $\min\{\varrho(G) \ : \ G \in H\}$

2.3.4. Bestimme die vier griechischen Buchstaben für den Graphen in Abbildung 6!

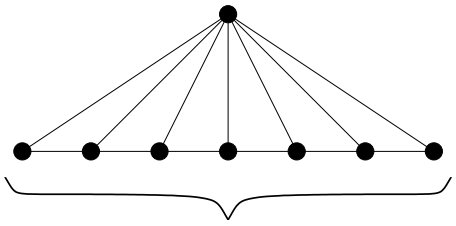


Abbildung 6:

2.3.5. Der maximale Grad im Graphen G sei d. Beweise, dass $d \cdot \tau \geq e$ gilt!

2.3.6. Man zerlegt die Ebene mit 4 Geraden auf 11 Länder. Bestimme den Wert der vier griechischen Buchstaben in dem dualen Graphen!
(Der duale Graph sieht folgenderweise aus: seine Knotenpunkte sind die Länder, und zwei Knotenpunkte sind genau dann mit einer Kante verbunden, falls die zugehörigen Länder entlang einer *Strecke* benachbart sind.)

2.3.7. Was ist das Maximum von $\frac{\tau}{\nu}$ in einem einfachen Graphen? Zeige ein Beispiel, wo dieses Maximum erreicht wird!

2.4 BFS, DFS, Dijkstra, Ford, Floyd, PERT

2.4.1. Man überprüfe mit Hilfe des DFS-Algorithmus, ob der Graph in Abbildung 7 einen gerichteten Kreis beinhaltet. Falls ja, gebe einen gerichteten Kreis, falls nein, eine topologische Ordnung an!

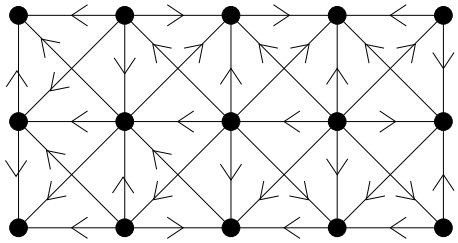


Abbildung 7:

2.4.2. Erweitere die Breitsuche zu einem Algorithmus, mit dem man überprüfen kann, ob ein Graph bipartit ist!

2.4.3. Erweitere die Breitsuche zu einem Algorithmus, mit dem man ein Matching in einem bipartiten Graphen suchen kann.

2.4.4. Gegeben ist der Graph in Abbildung 8. Berechne die Entfernungen der einzelnen Punkte vom Punkt S mit dem Algorithmus von Dijkstra!

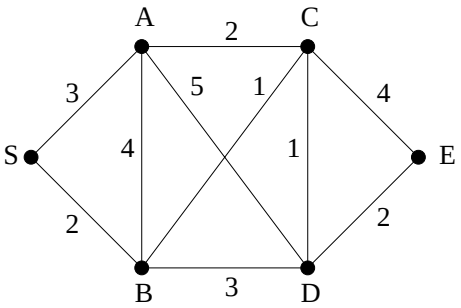


Abbildung 8:

2.4.5. Gegeben ist der Graph in Abbildung 9. Berechne die Entfernungen der Knotenpunkte vom Punkt A mit dem Algorithmus von Dijkstra!

2.4.6. Wie lange dauert der Prozess, der auf dem PERT-Diagramm von Abbildung 10 geschildert ist? Gebe die Dauer als eine Funktion von x an! ($x \in \mathbb{R}^{\geq 0}$) Bestimme ausserdem die kritischen Tätigkeiten!

2.4.7. Gegeben ist der Graph in Abbildung 11.
a) Berechne die Entfernungen der einzelnen Punkte vom Punkt **1** mit dem Algorithmus von Ford!
b) Berechne die Entfernungen aller Punktpaare mit dem Algorithmus von Floyd!

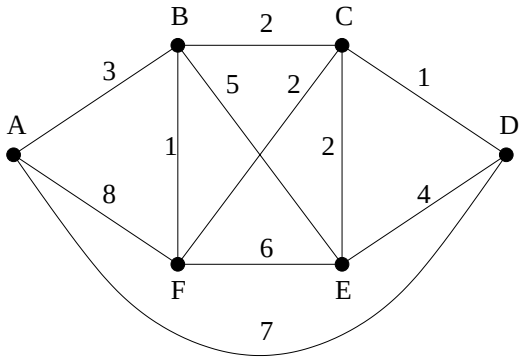


Abbildung 9:

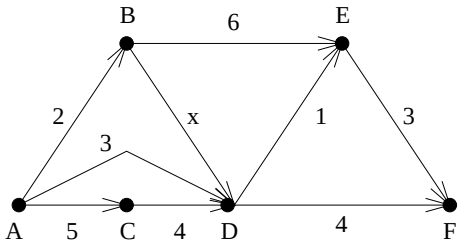


Abbildung 10:

2.4.8. Bestimme die Dauer der Aufgabe in Abbildung 12, und gebe die kritischen Tätigkeiten abhängig von x an!

2.5 Netzwerke und Flüsse

2.5.1. Man gebe den maximalen Fluss und eine minimale Schnittmenge im Netzwerk von Abbildung 13 als eine Funktion von x an. (x ist eine nicht-negative reelle Zahl.)

2.5.2. Man gebe die minimale Schnittmenge im Netzwerk von Abbildung 14 als eine Funktion

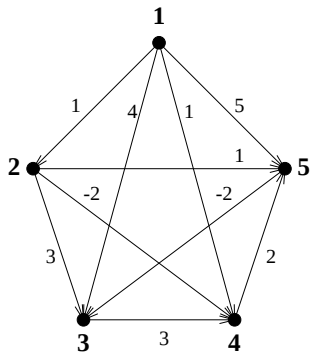


Abbildung 11:

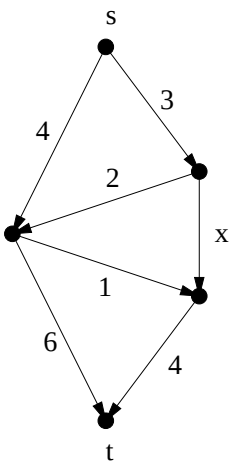


Abbildung 12:

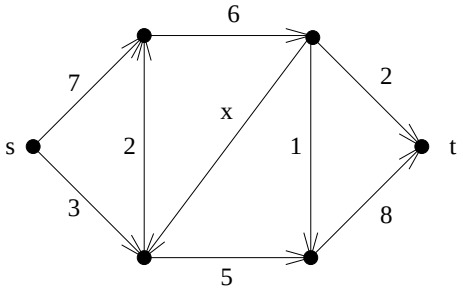


Abbildung 13:

von x und y an. (x und y sind nicht-negative reelle Zahlen.)

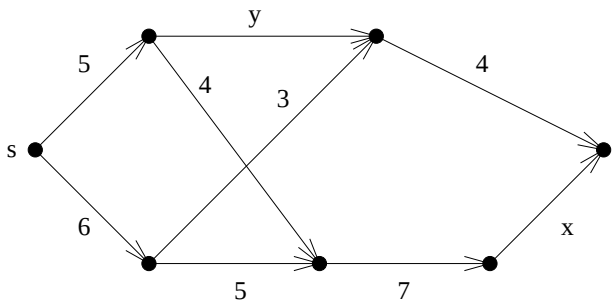


Abbildung 14:

2.5.3. Die Punkte von G seien die $0-1$ Folgen der Länge n. Seien $a, b \in V(G)$. Von a nach b führt eine Kante mit Kapazität i, falls man b aus a so bekommt, dass man die 0 an der i-ten Stelle in a auf 1 stellt. Sei $s = (0 \dots 0)$, $t = (1 \dots 1)$ und f_n der maximale Fluss.
a) Wieviel ist f_3?
b) Beweise, dass $f_n \leq 2^{n-1}$

2.5.4. Beweise den Satz von König-Hall-Frobenius mit Hilfe des Satzes von Ford-Fulkerson (mit dem Hilfssatz für ganzzahlige Kapazitäten).

2.5.5. Sind die folgenden Behauptungen wahr?
a) Wenn alle Kantenkapazitäten in einem Netzwerk *gerade* sind, dann *gibt es einen* maximalen Fluss, bei dem über jede Kante eine *gerade* Zahl transportiert wird.
b) Wenn alle Kantenkapazitäten in einem Netzwerk *gerade* sind, dann wird in *jedem* maximalen Fluss über jede Kante eine *gerade* Zahl transportiert.
c) Wenn alle Kantenkapazitäten in einem Netzwerk *ungerade* sind, dann *gibt es einen* maximalen Fluss, bei dem über jede Kante eine *ungerade* Zahl transportiert wird.
d) Wenn alle Kantenkapazitäten in einem Netzwerk *ungerade* sind, dann wird in *jedem* maximalen Fluss über jede Kante eine *ungerade* Zahl transportiert.

2.5.6. Bestimme den Wert des maximalen Flusses und die minimale Schnittmenge im Netzwerk in Abbildung 15 abhängig von x und y (x und y sind nicht-negative reelle Zahlen)!

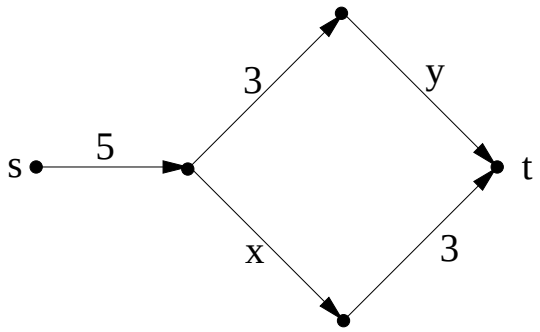


Abbildung 15:

2.6 k-facher Zusammenhang

2.6.1. Beweise, dass ein 3-regulärer Graph genau dann k-fach zusammenhängend ist, wenn er k-fach kantenzusammenhängend ist!

2.6.2. G sei ein k-fach kantenzusammenhängender Graph mit n Knotenpunkten. Beweise, dass G mindestens $\frac{kn}{2}$ Kanten hat!

2.6.3. G sei ein Graph mit n Knotenpunkten, $k < n$. Für jeden Knotenpunkt x gilt, dass $d(x) \geq (n + k - 2)/2$. Beweise, dass G k-fach zusammenhängend ist!

2.6.4. Ist die folgende Behauptung wahr:
Falls es für beliebige 3 Punkte einen Kreis gibt, welcher die 3 Punkte enthält, dann ist der Graph 3-fach zusammmenhängend.
(Falls ja, zeige ein Beweis, falls nein, gebe ein Gegenbeispiel an!)

2.6.5.
Behauptung 1.: G ist zweifach kantenzusammenhängend
Behauptung 2.: In G kommen in jeder Schnittmenge gerade Anzahl von Kanten vor

a) Folgt aus Behauptung 1 Behauptung 2?
b) Folgt aus Behauptung 2 Behauptung 1?

2.7 Eulersche und Hamiltonsche Kreise und Wege

2.7.1. Kann man alle Felder eines 4×4-Schachbrettes mit nacheinanderfolgenden Pferdesprüngen besuchen?

2.7.2. G sei ein ungerichteter, zusammenhängender Graph. Beweise, dass es in G eine geschlossene Kantenfolge gibt, die jede Kante genau einmal in die eine und einmal in die andere Richtung benutzt.

2.7.3. Im Graphen von Abbildung 16 sei a die Anzahl der Knotenpunkte in einer Zeile, b die Anzahl der Knotenpunkte in einer Spalte, $a > 1$, $b > 1$. Wie müssen a und b gewählt werden, so dass der Graph
a) einen Eulerschen Kreis
b) einen Eulerschen Weg
c) einen Hamiltonschen Kreis
d) einen Hamiltonschen Weg
beinhaltet?

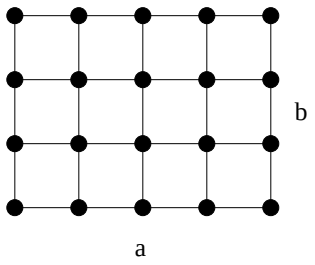


Abbildung 16:

2.7.4. Man betrachte
a) $G_{6,3}$ (Siehe die Definition von $G_{n,k}$ in Aufgabe **2.1.5.**)
b) $G_{16,3}$
Enthalten diese Graphen einen Hamiltonschen Kreis?

2.7.5. K sei ein Kreis im zusammenhängenden Graphen G mit der folgenden Eigenschaft: wenn man eine Kante aus K entfernt, so bekommt man einen längsten Weg von G. Beweise, dass K ein Hamiltonscher Kreis ist.

2.7.6. L_n sei der Graph, den man bekommt, wenn man eine Kante aus K_n entfernt. Wieviele Hamiltonsche Kreise gibt es in L_n falls die Punkte numeriert sind?

2.7.7. Gibt es einen solchen Graphen, der einen Eulerschen Kreis enthält und die Anzahl der Knotenpunkte ist gerade, die Anzahl der Kanten ist ungerade?

2.7.8. Sind die folgenden Behauptungen für jedes $n > 4$ wahr?
a) Es gibt einen Graphen G mit n Knotenpunkten, so dass sowohl G als auch $\overline{G}$ einen Hamiltonschen Kreis enthält.
b) Es gibt einen Graphen G mit n Knotenpunkten, so dass weder G noch $\overline{G}$ einen Hamiltonschen Kreis enthält.

2.7.9. Enthält der Graph in Abbildung 17 einen Hamiltonschen Kreis?

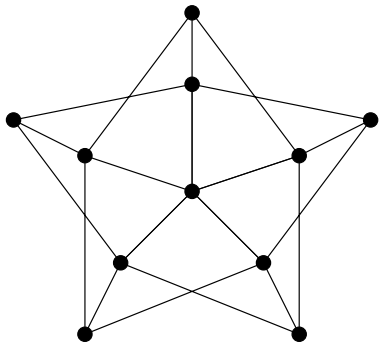


Abbildung 17:

2.8 Färbungen

2.8.1. Bestimme die chromatische Zahl für den folgenden Graphen:
$V(G) = \{v_1, \ldots, v_{106}\}$; v_i und v_j sind mit einer Kante verbunden, falls $|i - j| \leq 7$.

2.8.2. M_n sei ein Graph, den man erhält, wenn man einen Hamiltonschen Kreis aus K_n weglässt. Bestimme die chromatische Zahl für
a) M_{2k}
b) M_{2k+1}

2.8.3. In G kommt jede Kante höchstens in einem Kreis vor. Beweise, dass $\chi(G) \leq 3$ gilt!

2.8.4.
a) Beweise, dass die Kanten eines r-regulären paarschen Graphen mit r Farben färbbar sind!
b) Beweise, dass die Kanten eines paarschen Graphen mit d Farben färbbar sind, wo d die maximale Gradzahl ist!

2.8.5. Beweise, dass das Komplement eines Kreises mit ungerader Länge kein perfekter Graph sein kann, falls $n \geq 5$ ist!

2.8.6. P sei der Petersen-Graph. Wieviel ist $\chi(P)$ und $\chi_e(P)$?

2.8.7. Sei $\chi(G) = 3$. Weiterhin hat G die folgende Eigenschaft: $\chi(G - e) < 3$ für beliebige Kante $e \in E(G)$. Gebe alle solche Graphen an!

2.8.8. Sei $\chi(G) = k$. Beweise, dass die Kanten von G so gerichtet werden können, dass der längste gerichtete Weg höchstens $k - 1$ lang wird!

2.8.9. Bestimme χ in den Graphen die in Abbildung 18 dargestellt sind!

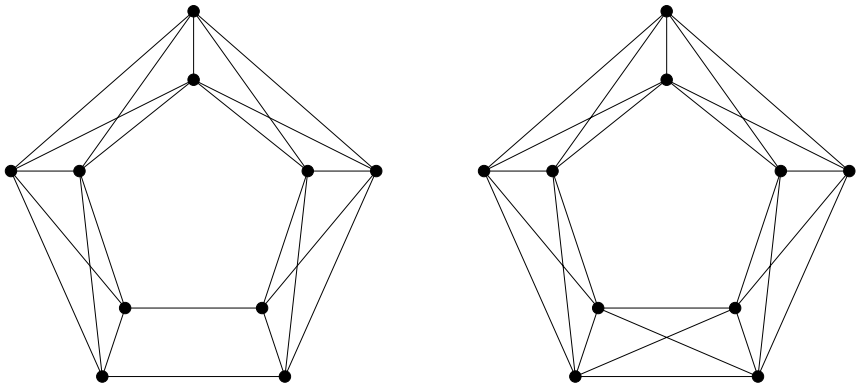


Abbildung 18:

2.8.10. Wir wissen, dass Bäume mit 2 Farben färbbar sind. Beweise, dass unter den Bäumen nur die Sterne die Eigenschaft haben, dass sie nicht mehr 2-färbbar bleiben, wenn man 2 *beliebige* Punkte, die bisher nicht adjazent waren, mit einer Kante verbindet!

2.9 Planarität

2.9.1. Sind die Graphen in Abbildung 19 planar? Falls ja, zeichne sie kreuzungsfrei mit geraden Linien und gebe ihren Dualen an! Ist der Graph nicht planar, so beweise es!

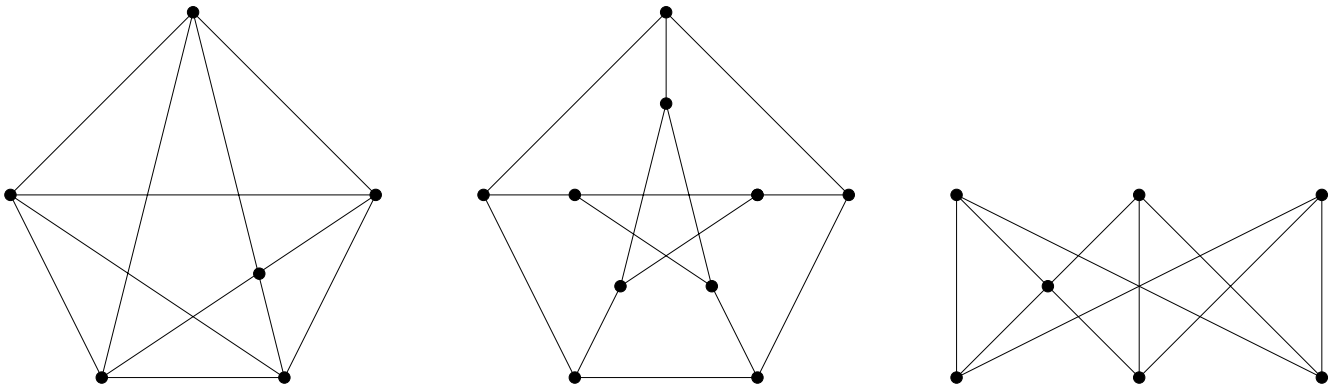


Abbildung 19:

2.9.2. Sind die zwei Graphen in Abbildung 20 isomorph bzw. schwach isomorph?

2.9.3. G sei ein planarer Graph mit einer minimalen Gradzahl von 5.
a) Wieviele Punkte muss G mindestens haben?
b) Zeige ein Beispiel mit dieser Punktzahl.

2.9.4.

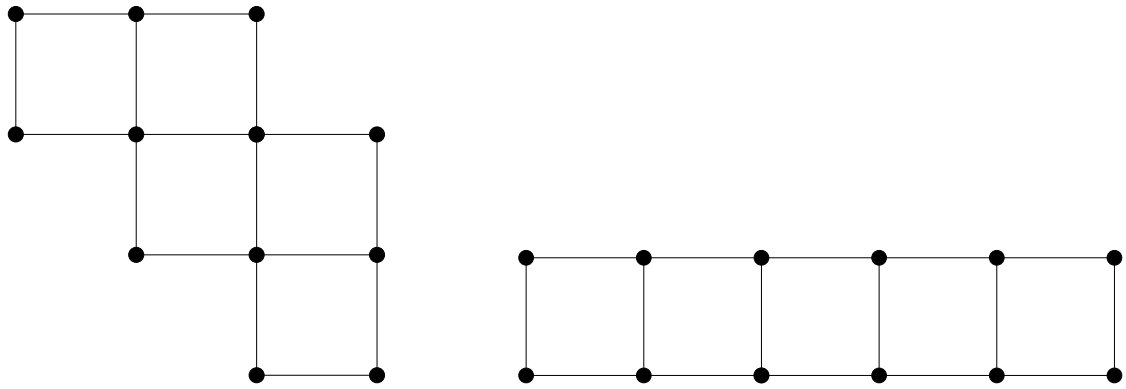


Abbildung 20:

a) Ist $G_{6,2}$ planar? (Siehe die Definition von $G_{n,k}$ in Aufgabe **2.1.5.**)
b) Für welches k ist $G_{2k,k-1}$ planar?

2.9.5. Man zerlegt die Ebene mit Geraden auf Länder.
a) Beweise, dass diese Landeskarte mit 2 Farben färbbar ist!
b) Bleibt die Behauptung wahr, wenn man ausser Geraden auch Kreise benutzt?

2.9.6. Zeige eine Landeskarte, die nicht mit 5 Farben färbbar ist, falls man auch solche Länder als Nachbarn betrachtet, die nur einen gemeinsamen Punkt haben!

2.9.7. Ist der Graph in Abbildung 21 planar?

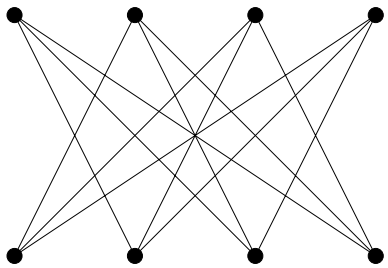


Abbildung 21:

2.9.8. Gibt es einen einfachen Graphen, der sechsfach zusammenhängend und planar ist?

2.9.9. Lassen wir eine beliebige Kante von dem Petersen Graphen weg. Ist der übriggebliebene Graph planar?

2.9.10. Beweise, dass in einem planaren Graphen $\alpha \geq \frac{n}{4}$. Gebe ein Beispiel, wo $\alpha = \frac{n}{4}$.

3 Zahlentheorie

3.1 Teilbarkeit

In diesem Kapitel geht es immer – falls nicht anders angedeutet – um positive ganze Zahlen.

3.1.1. Beweise für beliebige natürliche Zahlen a, b und k:
a) $a - b \mid a^k - b^k$
b) $a + b \mid a^{2k+1} + b^{2k+1}$
c) Zeige ein Beispiel, wo $a + b \mid a^{2k} + b^{2k}$ nicht erfüllt wird.

3.1.2. Welche ist die kleinste Zahl, die mit 3 nicht teilbar ist und 15 Teiler hat?

3.1.3. Beweise, dass

$$\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$$

sich für keine ganze Zahl n vereinfachen lässt!

3.1.4. Beweise: $2^{37} - 1 \mid 2^{1998} - 1$.

3.1.5. Bestimme alle möglichen Paare von Zahlen, die als grössten gemeinsamen Teiler 9 und als kleinstes gemeinsames Vielfaches 1998 haben!

3.1.6. Mit welcher Ziffer endet $23^{15^{23}}$?

3.1.7. Klaus wurde im Jahre 1998 37 Jahre alt. In wievielen Jahren wird seine Alter wieder ein Teiler des Jahres sein?

3.1.8. Für welche Werte von n ist $3^n + 1$ mit 8 teilbar?

3.1.9. Beweise für jedes n: $7 \mid 3^{2n+1} + 2^{n+2}$

3.2 Kongruenzen

3.2.1. Was sind die letzten zwei Ziffern von
a) $1997^{7^{2000}}$
b) $57^{67^{79}}$?

3.2.2. Löse die folgende Kongruenz:

$$2x \equiv 9 \pmod{21}$$

3.2.3. Löse die folgenden Kongruenzsysteme!
a)

$$5x \equiv 3 \pmod{7}$$

$$4x \equiv 1 \pmod 3$$

b)

$$\begin{aligned} 6x &\equiv 4 \pmod{11} \\ 5x &\equiv 2 \pmod 6 \end{aligned}$$

3.2.4. Löse die folgende Kongruenz:

$$x^{1999} + x^{1998} + x^{1997} + 1 \equiv 0 \pmod 5$$

3.2.5. Sei p eine Primzahl, n eine positive ganze Zahl. Man nehme an, dass $p \mid 10n - 1$. Beweise, dass

$$10^{p-2} \equiv n \pmod p$$

3.2.6. m sei eine zusammengesetzte Zahl ($m > 4$). Beweise:

$$(m-1)! \equiv 0 \pmod m$$

3.2.7. Leite den "kleinen" Satz von Fermat ohne den Euler-Fermatschen Satz her.

3.3 Zahlentheoretische Algorithmen

3.3.1. Bestimme mit dem euklidischen Algorithmus
a) $(1275, 442)$
b) $(2x^3 - x^2 + x + 1, 2x^2 - 5x - 3)$

3.3.2. Beweise, dass der euklidische Algorithmus nicht mehr in Polinomzeit arbeiten würde, falls man statt Divisionen Subtraktionen verwenden würde.

3.3.3. p und q seien verschiedene Primzahlen. Man beweise, dass es zwei ganze Zahlen k und n mit folgender Eigenschaft gibt: gibt man einem Drachen mit p Köpfen k Äpfel pro Kopf und einem Drachen mit q Köpfen n Äpfel pro Kopf, dann bekommt der eine Drache genau einen Apfel mehr als der andere.

3.3.4. In einem Spiel-RSA sei $p = 7, q = 11$. Sei e der kleinstmögliche öffentliche Schlüssel. Kodiere die Nachricht $x = 2$ und dekodiere das Ergebnis!

3.3.5.

a) Sei $n = p_1 \cdot \ldots \cdot p_k$, wobei die p_i-s verschiedene Primzahlen sind. Beweise:

$$\forall x: \quad x^{r\varphi(n)+1} \equiv x \pmod n$$

(Bemerkung: für den Spezialfall $k = 2$ sagt dieser Satz eben aus, dass der RSA Algorithmus korrekt ist.)
b) Zeige, dass diese Kongruenz nicht unbedingt erfüllt wird, falls einige p_i-s gleich sein dürfen.

3.3.6. Man zeige mit Hilfe des Fermat-Tests mit einer Gewissheit von mindestens 90%, dass 17 eine Primzahl ist! (Wir wissen, dass es keine Carmichaelsche Zahl ist.)

3.3.7. Die Carmichaelschen Zahlen haben die Form $n = p_1 \cdot \ldots \cdot p_k$, wobei die p_i-s verschiedene Primzahlen sind und $p_i - 1 \mid n - 1$ für jedes i. (Z. B. $561 = 3 \cdot 11 \cdot 17$ ist eine solche Zahl.) Beweise, dass der Fermat-Test solche Zahlen fast immer (d. h. bei jeder solchen Testzahl, die zu n teilerfremd ist) als Primzahlen identifizert.

3.3.8. Zeige mit Hilfe des Miller-Rabin-Tests, dass 561 keine Primzahl ist!

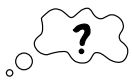
3.4 Weitere Aufgaben

3.4.1. Welchen Rest kann das Quadrat einer natürlichen Zahl
a) modulo 3
a) modulo 4
a) modulo 5
haben?

3.4.2. Schreibe $\frac{1}{3}$ im Zweiersystem auf!

3.4.3. Für welche Zahlen n gilt: $d(2n) = \frac{3}{2}d(n)$?

3.4.4. Beweise, dass $2^n + 1$ nur dann eine Primzahl sein kann, falls n eine Potenz von 2 ist.



3.4.5. Zeige, dass nicht jede Zahl, die die Form $2^{2^k} + 1$ hat, eine Primzahl ist.

3.4.6. $ab = n^2$, $(a, b) = 1$. Beweise, dass a und b selber Quadraten von natürlichen Zahlen sind.

3.4.7. Beweise: die positiven ganze Zahlen x, y, z sind genau dann Lösungen der Gleichung $x^2 + y^2 = z^2$, wenn $z = d(n^2 + m^2)$ und $x = 2dnm$, $y = d(n^2 - m^2)$ oder $x = d(n^2 - m^2)$, $y = 2dnm$, wobei $(n, m) = 1$, $n > m$, $2 \nmid n - m$.

3.4.8. Die positiven ganze Zahlen x, y, z seien Lösungen der Gleichung $x^2 + y^2 = z^2$. Beweise: $60 \mid xyz$.

4 Algebra

4.1 Elementare Gruppentheorie

4.1.1. a und b sind zwei Elemente der Gruppe G. Gegeben ihre Inverse a^{-1} und b^{-1}, wie kann das Invers von ab berechnet werden?

4.1.2. Trifft es für beliebige Elemente a, b, x, y einer Gruppe zu, dass aus $abx = aby$ auch $x = y$ folgt?

4.1.3. Trifft es für beliebige Elemente c, x, y einer Gruppe zu, dass aus $xc = cy$ auch $x = y$ folgt?

4.1.4. Formen die folgenden Operationen über die gegebenen Mengen eine Halbgruppe oder Gruppe? Was sind die neutralen Elemente der (Halb)Gruppen? Sind die (Halb)Gruppen kommutativ?
a) $x * y$ ist das Skalarprodukt, $x, y \in \mathbb{R}^n$, $n > 1$
b) $x * y := x + y + 1, \quad x, y \in \mathbb{Z}$
c) $x * y := |x + y|, \quad x, y \in \mathbb{Z}$
d) $x * y := xy/(x + y + 1), \quad x, y \in \mathbb{R}^+$

4.1.5. Beweise für beliebige Elemente a, b einer kommutativen Gruppe, dass $o(ab)$ ein Teiler vom kleinsten gemeinsamen Mehrfachen von $o(a)$ und $o(b)$ ist!

4.1.6. Man beweise, dass es in jeder endlichen Gruppe mit mindestens zwei Elementen ein Element a gibt, die die Eigenschaft besitzt, dass $o(a)$ eine Primzahl ist.

4.1.7. x und y seien Elemente einer Gruppe mit folgenden Eigenschaften: $x^2 = e, y = x^{-1}y^3x$. Beweise: $y^8 = e$.

4.1.8. Beweise folgende Behauptung: wenn für jedes Element g in einer Gruppe G gilt, dass $o(g) = 2$, dann ist G kommutativ.

4.1.9. Gibt es eine solche Gruppe, die für jede natürliche Zahl k ein Element mit Ordnung k beinhaltet?

4.1.10. G ist eine Gruppe. Beweise:

$$\forall x \in G \quad o(x) = o(x^{-1})$$

4.2 Untergruppen, Nebenklassen, Normalteiler

4.2.1. H sei eine Untergruppe von G, g ein beliebiges Element in G. Beweise, dass $H^* = \{g^{-1}hg \mid h \in H\}$ auch eine Untergruppe ist. Ist es wahr, dass H^* genau dann Normalteiler ist, wenn H Normalteiler ist?

4.2.2. Man beweise, dass jede Untergruppe mit Index 2 ein Normalteiler ist.

4.2.3. Man beweise, dass alle Untergruppen einer kommutativen Gruppe Normalteiler sind.

4.2.4. G sei eine Gruppe mit 32 Elementen, x ein beliebiges Element in G mit der Eigenschaft, dass $x^8 \neq e$. Beweise, dass die von x generierte Untergruppe ein Normalteiler von G ist.

4.2.5. G sei eine Gruppe, $Z = \{g \in G \mid gh = hg \ \forall h \in G\}$. Man beweise, dass Z eine Untergruppe von G ist. Ist Z auch Normalteiler von G?

4.2.6. G sei die multiplikative Gruppe der reellen Zahlen ausser 0. $H = \{-1; 1\}$. Man beweise, dass H Untergruppe, sogar Normalteiler von G ist. Was sind die Nebenklassen von H?

4.2.7. G sei die multiplikative Gruppe der komplexen Zahlen ausser 0. H sei die multiplikative Gruppe der positiven reellen Zahlen. Beweisse, dass H eine Untergruppe von G ist! Ist H auch Normalteiler in G? Was sind die Nebenklassen von H?

4.2.8. Man beweise folgende Behauptung: wenn eine endliche Gruppe G mit mindestens 2 Elementen keine echte Untergruppe hat, dann ist $G = C_p$ für eine geeignete Primzahl p.

4.2.9. G sei eine Gruppe, H eine endliche, nicht leere, bezüglich die Operation von G geschlossene Teilmenge von G.
a) Beweise, dass H eine Untergruppe von G ist.
b) Zeige, dass die Endlichkeit von H wirklich nötig ist, d. h. gebe ein Beispiel, wo H nicht endlich und auch keine Untergruppe ist.

4.2.10. Beweise, dass jede Untergruppe einer zyklischen Gruppe zyklisch ist!

4.2.11. Wieviele verschiedene (d. h. nicht isomorphe) Untergruppen hat C_{12}?

4.3 Homomorphismen, Ringe, Körper

4.3.1. $G = C_{12}$, $f(x) = x^3$. Beweise, dass f homomorph ist! Was ist $\mathrm{Ker} f$ bzw. $G/\mathrm{Ker} f$?

4.3.2. Die Abbildung f bildet jedes Element einer Gruppe in sein Invers ab. Beweise, dass diese Abbildung genau dann homomorph ist, wenn die Gruppe kommutativ ist.

4.3.3. Sind die folgenden Abbildungen homomorph bzw. isomorph?
a) $\varphi : R[x] \to R, \quad \varphi(p(x)) = p(a) \quad (a$ ist eine gegebene reelle Zahl.)
b) $\varphi : R[x] \to R[x], \quad \varphi(p(x)) = p(3x + 2)$

4.3.4. Man betrachte jene Brüche, deren Nenner – nachdem man alle möglichen Vereinfachungen vorgenommen hat – mit weder 2 noch 5 teilbar ist. Bilden sie einen Ring bzw. einen Körper mit der üblichen Addition und Multiplikation?

4.3.5. Bilden die reellen Funktionen mit einem Veränderlichen einen Ring bzw. einen Körper, falls die Addition die Übliche und die Multiplikation das Zusammensetzen von Funktionen

ist?

4.3.6. Welche Elemente im Ring der Restklassen modulo 12 haben ein multiplikatives Invers?

4.3.7. x und y seien linksseitige Nullteiler in einem Ring. Beweise, dass xy (falls ungleich 0) auch ein linksseitiger Nullteiler ist, $x + y$ aber nicht unbedingt.

4.3.8. Was für algebraische Strukturen sind die Folgenden?
a) R^2 mit den Operationen $\oplus$ und $\otimes$, die wie folgt definiert sind:

$$\begin{aligned}(a, b) \oplus (c, d) &= (a + c, b + d)\\ (a, b) \otimes (c, d) &= (ac - bd, bc + ad)\end{aligned}$$

b) Die reellen Zahlenfolgen; Addition und Multiplikation erfolgen gliedweise.
c) Die 0-1-Folgen der Länge n (n ist gegeben); mit XOR als Addition und AND als Multiplikation.

Hinweise

Aufgabe **1.1.10.** c): Man addiere die Formeln vom Punkt a) und b).

Aufgabe **2.1.11.**: Betrachte den längsten Weg des Graphen.

Aufgabe **2.1.14.**: Versuche die Aufgabe mit vollständiger Induktion zu lösen!

Aufgabe **2.1.21.**: Man soll den Prüfer-Code des Bäumes mit Hilfe von $d_1, d_2, \ldots, d_n$ erstellen. (Bemerkung: es ist klar, dass die Bedingung $\sum_{i=1}^{n} d_i = 2n - 2$ notwendig ist, da ein Baum mit n Knotenpunkten $n - 1$ Kanten hat, und die Summe aller Gradzahlen das Zweifache davon sein muss. Diese Aufgabe sagt aus, dass diese Bedingung auch hinreichend ist.)

Aufgabe **2.2.1.**: Finde zuerst nur eine vollständige Paarung in dem Graphen.

Aufgabe **2.2.3.**: Suche einen r-regulären Graphen, der zu den originalen Graphen so addiert werden kann, dass in dem originalen Graphen die Anzahl der fehlenden Kanten verringert wird.

Aufgabe **2.2.14.**: Modifiziere den Graphen, so dass man im modifizierten Graphen mit dem gelernten Algorithmus vorgehen kann!

Aufgabe **3.3.5.**: Da x und n nicht unbedingt teilerfremd sind, kann man den Euler-Fermatschen Satz nicht benutzen. Stattdessen soll man für alle p_i-s den kleinen Satz von Fermat verwenden.

Aufgabe **3.4.5.**: Man soll beweisen, dass $641 \mid 2^{32} + 1$.

Aufgabe **3.4.6.**: Man betrachte indirekt das kleinste Gegenbeispiel und konstruiere daraus ein kleineres Gegenbeispiel.

Aufgabe **3.4.7.**: Man betrachte eine primitive Lösung der Gleichung. (Eine Lösung ist primitiv, wenn x, y und z teilerfremd sind.) x und y können weder beide gerade noch beide ungerade sein. Wenn z. B. y gerade ist, dann gilt:

$$\left(\frac{y}{2}\right)^2 = \frac{z+x}{2} \cdot \frac{z-x}{2}$$

und Aufgabe **3.4.6.** kann verwendet werden.

Aufgabe **3.4.8.**: Man benutze Aufgabe **3.4.7.** und **3.4.1.**.

Lösungen

1 Kombinatorik

1.1 Elementare Kombinatorik

1.1.1. Die Anzahl der guten Reihenfolgen ist die Anzahl aller Reihenfolgen minus die Anzahl der schlechten Reihenfolgen. Unter einer guten Reihenfolge verstehe man einen solche Anordnung der Kugeln, wo die zwei weissen nicht nebeneinander stehen; der Rest zählt zu den schlechten Reihenfolgen.
Die Anzahl aller Reihenfolgen kann man als eine Permutation mit Wiederholung berechnen, also ist es $\frac{8!}{2!\cdot 6!} = 28$. Die Anzahl der schlechten Reihenfolgen ist 7, weil die erste Kugel von den zwei nebeneinander stehenden weissen an 7 verschiedenen Stellen stehen kann: von der Stelle 1 bis 7. Also ist die Anzahl der guten Reihenfolgen $28 - 7 = 21$.

1.1.2. Die Anzahl aller Permutationen von n Personen ist $n!$. Da der Tisch rund ist, ist es egal, mit wem man beginnt, also wird in $n!$ jede Lösung n-mal gezählt, deswegen muss mit n dividiert werden. Ebenso ist es egal, ob man die Ritter im Uhrzeigersinn oder gegen den Uhrzeigersinn zusammenzählt, so muss man noch mit 2 dividieren. Schliesslich erhält man $\frac{n!}{2n} = \frac{(n-1)!}{2}$.

1.1.3. Hinter den folgenden zwei Lösungen stecken zwei verschiedene Ideen: in der ersten Lösung wird die Anzahl der Dominos in beiden Schachteln bestimmt, und gemerkt, dass sie gleich sind, die zweite Lösung dagegen berechnet die konkreten Zahlen nicht, sie zeigt einfach ihre Gleichheit.

Lösung 1: Die Anzahl von Dominos in Schachtel A ist die Kombination von 2 aus 8 Zahlen mit Wiederholung; das ist $\binom{8+2-1}{2} = 36$. Die Anzahl von Dominos in Schachtel B ist die Kombination von 2 aus 9 Zahlen ohne Wiederholung, also $\binom{9}{2} = 36$. So ist die Anzahl der Dominos in Schachtel A und B gleich.

Lösung 2: Man zeige, dass sich in beiden Schachteln die gleiche Anzahl von Dominos befinden. Dafür konstruiere man eine Bijektion zwischen den Dominos in Schachtel A und B. Jene Dominos (i, j), für die $1 \leq i < j \leq 8$ gilt, befinden sich in beiden Schachteln, also braucht man sich nur mit dem Rest zu beschäftigen; die übriggebliebenen Dominos in Schachtel A sind gerade die Doppelsteine, (i, i), wo $1 \leq i \leq 8$. Die übriggebliebenen Dominos in Schachtel B haben die Form $(i, 9)$, wo $1 \leq i \leq 8$. Mit $(i, i) \leftrightarrow (i, 9)$ haben wir eine Bijektion konstruiert.

1.1.4. Die Anzahl der günstigen Fälle, bei denen also mindestens einmal 6 gewürfelt wurde, ist die Anzahl aller Fälle minus die Anzahl der schlechten Fälle; eine Reihe von Würfen wird schlecht genannt, falls gar keine 6 gewürfelt wurde, also sind bei jedem Wurf 5 Ergebnisse möglich.
Die Anzahl aller möglichen Würfen ist 6^{10} (Variation mit Wiederholung), da man bei jedem Wurf 6 verschiedene Möglichkeiten hat, und diese Würfe sind unabhängig voneinander.

Ähnlicherweise ist die Anzahl der schlechten Fälle gleich 5^{10}. So ist die Lösung $6^{10} - 5^{10}$.

1.1.5. Lösung 1: Insgesamt muss er $n-1$-mal nach oben und $n-1$-mal nach rechts gezogen werden. Also ist sein Weg dadurch bestimmt, welche $n-1$ aus seinen $2n-2$ Zügen nach oben passieren. So gibt es $\binom{2n-2}{n-1}$ verschiedene Lösungsfolgen.

Lösung 2: Man bezeichne mit (i, j) das Feld j in Zeile i (die Zeilen werden von unten nach oben numeriert), wo $i, j \in \{1, \ldots, n\}$. Sei $f(i, j)$ die Anzahl der möglichen Wege von dem Startfeld $(1, 1)$ zu dem Feld (i, j). Die Aufgabe ist also $f(n, n)$ zu bestimmen. Offensichtlich gilt, dass

$$f(1, i) = 1 \text{ und } f(i, 1) = 1 \quad i \in \{1, \ldots, n\}$$

denn zum Beispiel um das Feld $(1, i)$ zu erreichen hat man nur eine Möglichkeit, nämlich i-mal nach rechts zu treten. Die folgende Regel definiert die übrigen Werte der Funktion:

$$f(i, j) = f(i, j-1) + f(i-1, j) \quad i, j \in \{2, \ldots, n\}$$

denn der König kann das Feld (i, j) entweder von dem Feld $(i, j-1)$ oder von dem Feld $(i-1, j)$ erreichen. Diese Regeln entsprechen eben den Bildungsregeln des Pascalschen Dreiecks, also bilden die Diagonalen eben die Reihen des Pascalschen Dreiecks (nur beide Indizen sind mit 1 verschoben). Daraus folgt, dass

$$f(i, j) = \binom{i+j-2}{i-1}$$

Deswegen ist

$$f(n, n) = \binom{2n-2}{n-1}$$

Ein Beispiel für $n = 5$ in Abbildung 22 soll die Lösung veranschaulichen. Die Zahlen in der Tabelle bedeuten die Anzahl der Möglichkeiten, die Zahlen ausser der Tabelle sagen, welcher Reihe des Pascalschen Dreiecks die gezeigte Diagonale entspricht.

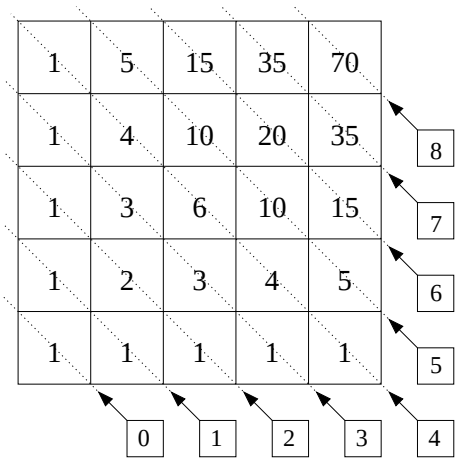


Abbildung 22: In jedem Feld des Schachbrettes ist die Anzahl der verschiedenen Wege aus der linken unteren Ecke zu diesem Feld geschrieben. Die Diagonalen entsprechen genau den Reihen des Pascalschen Dreiecks

1.1.6. Man muss aus den $2n$ Kindern n Paare bilden; bei einem Paar ist es eindeutig, dass das grössere Kind hinten und das kleinere Kind vorne stehen muss. Für das erste Paar hat man $\binom{2n}{2}$ Möglichkeiten, für das zweite $\binom{2n-2}{2}$, für das k-te $\binom{2n-2k+2}{2}$, für das letzte $\binom{2}{2}$. Die Anzahl der Möglichkeiten ist das Produkt dieser Zahlen: $\prod_{k=1}^{n} \binom{2n-2k+2}{2}$; nach Vereinfachung des Ausdrucks ergibt sich $\frac{(2n)!}{2^n}$.

1.1.7. Intuitiv spürt man, dass eine symmetrische Kopf-Wappen Folge (KW-Folge) in der Mitte geteilt werden kann, so dass die Teile Spiegelbilder voneinander sind. Auch umgekehrt kann man es formulieren: aus einer beliebigen KW-Folge kann man eine symmetrische Folge bilden, welche doppelt so lang ist. Diese Gedanken zeigen, dass eine symmetrische KW-Folge der Länge n zu einer KW-Folge der Länge $\frac{n}{2}$ zugeordnet werden kann. Das ist natürlich nur dann wahr, falls n gerade ist; man muss den Fall, falls n ungerade ist, speziell behandeln. Hier folgen die obigen Ideen in präziser Form:
Sei u eine KW-Folge, dann bezeichne man mit $\widetilde{u}$ die umgekehrte KW-Folge. Z. B.:

$$u = KWW \Rightarrow \widetilde{u} = WWK$$

Man muss also zwei Fälle unterscheiden:
a) n ist gerade. Zu einer beliebigen KW-Folge u der Länge $\frac{n}{2}$ kann man eine symmetrische KW-Folge w der Länge n zuordnen, nämlich

$$w = u\widetilde{u}$$

Z. B.:

$$KWWKW \leftrightarrow KWWKWWKWWK$$

Diese Zuordnung ist bijektiv. Daraus folgt, dass die Anzahl der symmetrischen KW-Folgen der Länge n gleich der Anzahl der KW-Folgen der Länge $\frac{n}{2}$ ist. Die Anzahl der KW-Folgen der Länge $\frac{n}{2}$ ist $2^{\frac{n}{2}}$.

b) n ist ungerade. Ähnlicherweise bilde man eine Bijektion zwischen den KW-Folgen der Länge $\frac{n+1}{2}$ und den symmetrischen KW-Folgen der Länge n. Sei $v = uX$ eine KW-Folge der Länge $\frac{n+1}{2}$, wo u eine KW-Folge der Länge $\frac{n-1}{2}$ und X entweder K oder W ist. Mit

$$w = uX\widetilde{u}$$

wurde eine Bijektion konstruiert. z. B.:

$$KWKKW \leftrightarrow KWKKWKKWK$$

Daraus folgt, dass die Anzahl der symmetrischen KW-Folgen der Länge n gleich der Anzahl der KW-Folgen der Länge $\frac{n+1}{2}$ ist. Die Anzahl der KW-Folgen der Länge $\frac{n+1}{2}$ ist $2^{\frac{n+1}{2}}$.
Die Lösung ist also $2^{\frac{n}{2}}$ falls n gerade ist, und $2^{\frac{n+1}{2}}$ falls n ungerade ist.

1.1.8. Die Anzahl der Möglichkeiten bleibt unverändert, wenn man zuerst 3 Leute auswählt, die den Vorstand bilden, und erst dann aus diesen Leuten den Präsidenten auswählt.
Um aus 25 Leuten 3 auszuwählen, gibt es $\binom{25}{3}$ Möglichkeiten. Um aus dieser 3 nun noch einen Präsidenten auszuwählen, hat man 3 Möglichkeiten. Insgesamt also $\binom{25}{3} \cdot 3$ Möglichkeiten.

1.1.9.
a) Von den 4 Assen muss man 2 bekommen und von den restlichen 28 Karten 6. Also ist die Anzahl der Möglichkeiten $\binom{4}{2} \cdot \binom{28}{6}$

b) Der rote König ist eine spezielle Karte in dieser Aufgabe; mit dieser Karte werden nämlich 2 Bedingungen gleichzeitig erfüllt. Zwei Fälle muss man also unterscheiden:

- man hat den roten König: von den restlichen 7 roten muss man 1 bekommen und von den 21 Karten, die weder rot noch König sind, 6. Also gibt es $\binom{7}{1} \cdot \binom{21}{6}$ Möglichkeiten.
- man hat den roten König nicht: von den restlichen 7 roten muss man 2 bekommen, von den restlichen 3 Königen 1 und von den 21 Karten, die weder rot noch König sind, 5. Das bedeutet $\binom{3}{1} \cdot \binom{7}{2} \cdot \binom{21}{5}$ Möglichkeiten

Diese 2 Fälle schliessen einander aus, aber einer der Fälle wird sicherlich erfolgen, also ist die Anzahl der Möglichkeiten die Summe der zwei obigen Zahlen: $\binom{7}{1} \cdot \binom{21}{6} + \binom{3}{1} \cdot \binom{7}{2} \cdot \binom{21}{5}$.

1.1.10. a)

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = (1+1)^n = 2^n$$

wegen des Binomialsatzes.

b)

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

wegen des Binomialsatzes.

c) Man addiere die Formeln vom Punkt a) und b):

$$\begin{array}{ccccccccccccccc}
\binom{n}{0} & + & \binom{n}{1} & + & \binom{n}{2} & + & \dots & + & \binom{n}{2k} & + & \binom{n}{2k+1} & + & \dots & + & \binom{n}{n} \\
\binom{n}{0} & - & \binom{n}{1} & + & \binom{n}{2} & - & \dots & + & \binom{n}{2k} & - & \binom{n}{2k+1} & + & \dots & \pm & \binom{n}{n} \\
\hline
2 \cdot \binom{n}{0} & + & 0 & + & 2 \cdot \binom{n}{2} & + & \dots & + & 2 \cdot \binom{n}{2k} & + & 0 & + & \dots & + & \binom{n}{n} \pm \binom{n}{n}
\end{array}$$

Daraus ergibt sich, dass jene Glieder, die zu einem geraden Wert von k gehören, zweimal gezählt werden und die anderen Glieder ausfallen. Der zu berechnende Ausdruck ist eben die Hälfte dieser Summe.

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = \frac{1}{2} \cdot \left(\sum_{k=0}^{n} \binom{n}{k} + \sum_{k=0}^{n} (-1)^k \binom{n}{k} \right) = \frac{1}{2} \cdot (2^n + 0) = 2^{n-1}$$

(Die obere Grenze in der Summe kann vielleicht störend sein: $\lfloor n/2 \rfloor$ fasst einfach folgendes zusammen: $\frac{n}{2}$ falls n gerade ist, $\frac{n-1}{2}$ falls n ungerade ist.)

d) Zuerst wird der summierte Ausdruck umgeformt:

$$\begin{aligned} k\binom{n}{k} &= k \cdot \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1)!}{\frac{k!}{k}(n-k)!} = n \cdot \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \\ &= n\binom{n-1}{k-1} \end{aligned} \tag{1}$$

Daraus folgt

$$\sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=1}^{n} k\binom{n}{k} \overset{(1)}{=} \sum_{k=1}^{n} n\binom{n-1}{k-1} \overset{j:=k-1}{=} n \cdot \sum_{j=0}^{n-1} \binom{n-1}{j} \overset{a)}{=} n \cdot 2^{n-1}$$

1.1.11. Aus 4 verschiedenen Zahlen kann man 2 monotone Folgen bilden: eine monoton fallende und eine monoton steigende. (Zum Beispiel aus den Zahlen 2, 5, 8, 7 können die Folgen 2, 5, 7, 8 und 8, 7, 5, 2 zusammengestellt werden.) Daraus folgt, dass es zweimal so viele monotone Folgen gibt, wie man 4 Zahlen auswählen kann, also $2 \cdot \binom{7}{4}$.

1.1.12. Man hat 14 Möglichkeiten die Stelle des falschen Tips auszuwählen und hat zwei Möglichkeiten an dieser Stelle falsch zu tippen, also ist die Antwort $2 \cdot 14 = 28$.

1.1.13. Aus den folgenden Mengen muss je eine Zahl ausgezogen werden:

$$\{1, 2\}, \{9, 10, 11\}, \{12, 13, 14\}, \{19, 20, 21\}, \{74, 75, 76\}$$

Dazu hat man $2 \cdot 3^4$ Möglichkeiten.

1.1.14. Entweder geht der Turm einmal horizontal und zweimal vertikal oder einmal vertikal und zweimal horizontal. Das bedeutet einen Faktor zwei. Betrachten wir nur den ersten Fall. Der horizontale Schritt kann entweder vor oder nach oder zwischen den zwei vertikalen Schritten kommen, also es bedeutet weitere 3 Möglichkeiten. Der horizontale Schritt muss natürlich 7 Feld lang sein, aber man hat 6 Möglichkeiten die zwei vertikale Schritte zu bestimmen. (1-6, 2-5, 3-4, 4-3, 5-2, 1-6). Also hat man insgesamt $2 \cdot 3 \cdot 6 = 36$ Wege.

1.2 Rekursionen

1.2.1. Sei $f(n)$ die Anzahl der Möglichkeiten für n Stufen. Als letzter Schritt kann man entweder von der Stufe $n-1$ oder von der Stufe $n-2$ auf Stufe n landen, also:

$$f(n) = f(n-1) + f(n-2)$$

Offensichtlich ist $f(1) = 1$ und $f(2) = 2$, also ist die Lösung die Fibonacci-Zahlenfolge.

1.2.2. Man hat 2 Möglichkeiten anzufangen, wie es Abbildung 23 darstellt. In dem ersten Fall bleibt eine Leiter der Länge $n-2$, in dem zweiten eine Leiter der Länge $n-1$ übrig. Wenn man also die Anzahl der Paarungen einer Leiter der Länge n mit $f(n)$ bezeichnet, erhält man folgende Rekursion:

$$f(n) = f(n-1) + f(n-2)$$

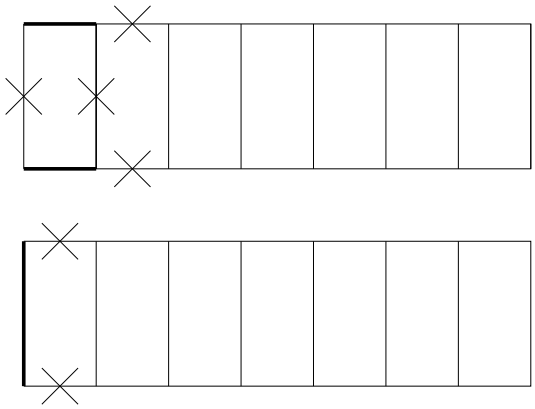


Abbildung 23: Mögliche Anfangsschritte der vollständigen Paarung in der Leiter

Es ist trivial, dass $f(1) = 1$ und $f(2) = 2$, also ist $f(n)$ die Fibonacci-Zahlenfolge.

1.2.3. a) Die charakteristische Gleichung der Rekursion ist:

$$x^2 = 2x - 2$$

die 2 (komplexen) Wurzeln sind

$$x_1 = 1 - i,\ x_2 = 1 + i$$

also ist die Lösung in der Form

$$a_n = c_1 \cdot (1 - i)^n + c_2 \cdot (1 + i)^n,\ c_i \in \mathbb{C}$$

zu suchen. Die Konstanten c_1 und c_2 können aus den Anfangsbedingungen bestimmt werden. Dafür muss man folgendes Gleichungssystem lösen:

$$c_1 + c_2 = 1$$

$$c_1 \cdot (1 - i) + c_2 \cdot (1 + i) = 2$$

Daraus ergibt sich

$$c_1 = \frac{1 + i}{2}, c_2 = \frac{1 - i}{2}$$

Also

$$a_n = \frac{1 + i}{2} \cdot (1 - i)^n + \frac{1 - i}{2} \cdot (1 + i)^n$$

b) Die charakteristische Gleichung der zweiten Rekursion ist:

$$x^2 = 2x - 1$$

die 2 Wurzeln sind

$$x_1 = x_2 = 1$$

also ist die Lösung in der Form

$$a_n = c_1 + c_2 \cdot n$$

zu suchen, wo die Konstanten c_1 und c_2 die folgenden Gleichungen erfüllen:

$$c_1 = 1$$

$$c_1 + c_2 = -1$$

Daraus ergibt sich

$$c_1 = 1, c_2 = -2$$

Also

$$a_n = 1 - 2 \cdot n$$

1.2.4. Man betrachte die Felder des Schachbrettes als die Knotenpunkte eines Graphen. Zwei Knotenpunkte dieses Graphen werden genau dann verbunden, wenn die zugehörigen Felder benachbart sind. Dieser Graph ist genau die "Leiter" aus Aufgabe **1.2.2.**; die gesuchte Abdeckung mit den Dominosteinen entspricht genau einem Matching. Also kann diese Aufgabe auf Aufgabe **1.2.2.** zurückgeführt werden. Somit ist die Anzahl der Möglichkeiten genau die n-te Fibonacci-Zahl[1] :

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

[1]Manchmal definiert man die Fibonacci-Zahlenfolge anders: $F(0) = 0$ und $F(1) = 1$. Hier wird immer $F(0) = 1$ und $F(1) = 1$ benutzt. Deswegen sind die Potenzen mit 1 verschoben.

2 Graphentheorie

2.1 Grundbegriffe der Graphentheorie

2.1.1. Die möglichen Bäume werden systematisch, nach der Länge des längsten Weges zusammengezählt (siehe Tabelle 1).

Länge des längsten Weges	*Anzahl der nicht-isomorphen Bäume*
6	1
5	2
4	5
3	2
2	1
insgesamt	11

Tabelle 1: Anzahl der nicht-isomorphen Bäume mit $n = 7$

Diese Fälle produzieren natürlich nicht-isomorphe Lösungen, da zwei Graphen nicht isomorph sein können, falls sie sich in der Länge des längsten Weges unterscheiden. Wir haben alle Möglichkeiten betrachtet, da die Länge des längsten Weges mindestens 2 und höchstens 6 sein kann. (Ein Weg der Länge 7 bräuchte schon 8 Punkte; hat der Graph 2 inzidente Kanten, so ist der längste Weg schon mindestens 2 lang.) Also gibt es insgesamt 11 nicht-isomorphe Bäume mit $n = 7$ (siehe Abbildung 24).

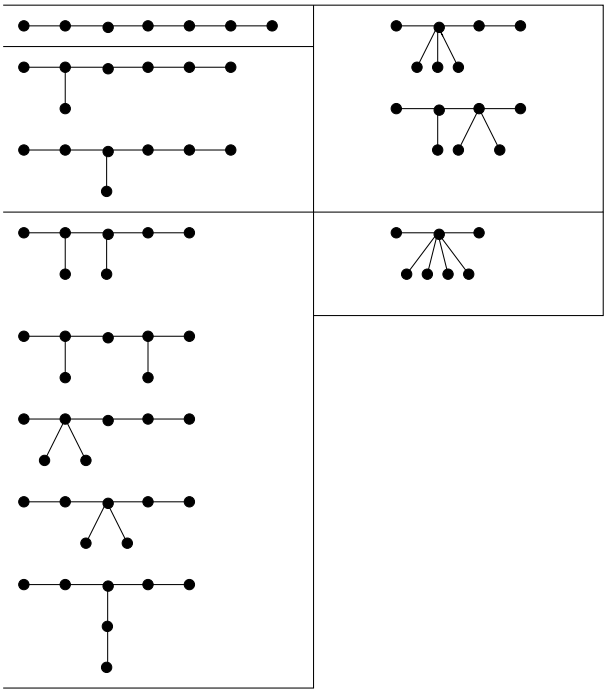


Abbildung 24: Alle Bäume mit 7 Knotenpunkten

2.1.2. Die möglichen Graphen werden systematisch, nach der Länge des längsten Weges zusammengezählt. Der längste Weg hat entweder die Länge 3 oder 2. (Mehr als 3 ist unmöglich, da der Graph nur 3 Kanten hat; Länge 1 würde bedeuten, dass der Graph aus disjunkten Kanten besteht, aber zu 3 solchen Kanten bräuchte man 6 Knotenpunkte.) Besteht der längste Weg aus 3 Kanten, dann ist der Graph eben dieser Weg; besteht er aus zwei Kanten, dann haben die Endpunkte der dritten Kante entweder beide Grad 1 oder Grad 1 und 3 oder beide Grad 2. Die Lösungen sind in Abbildung 25 zusammengefasst.

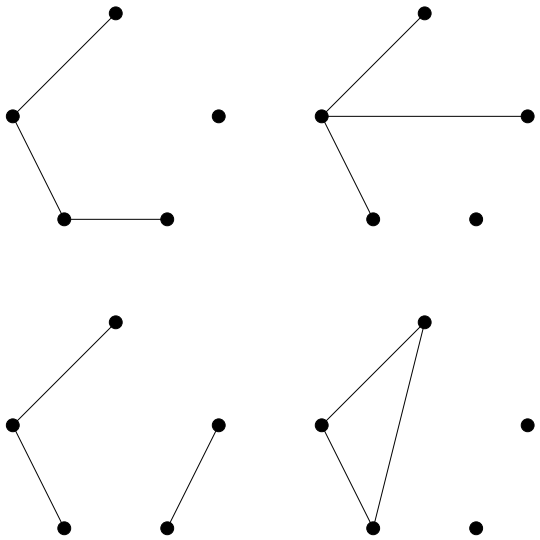


Abbildung 25: Alle Graphen mit 5 Kontenpunkten und 3 Kanten

2.1.3.
a) Es wird nur die Struktur einer Komponente bestimmt, die anderen sehen ähnlich aus. Sei W der längste Weg in einer Komponente. Ausser den Endpunkten von W haben schon alle Punkte in W Grad 2, also können keine weitere Kanten zu ihnen gefügt werden. Die Endpunkte haben erst Grad 1, also muss noch eine Kante aus ihnen auslaufen. Aber die Endpunkte können mit keinem inneren Punkt des Weges verbunden sein, weil dann jener innere Punkt schon Grad 3 hätte. Die Endpunkte können auch mit keinem solchen Punkt verbunden sein, der in W nicht enthalten ist, weil dann W doch nicht der längste Weg wäre. Also können die beiden Endpunkte nur miteinander verbunden sein. Daraus ergibt sich, dass diese Komponente ein Kreis ist (da die Komponente zusammenhängend ist, kann sie keine weiteren Punkte ausser W enthalten); der Graph ist also die Vereinigung von fremden Kreisen.

b) Ähnlicherweise kann bewiesen werden, dass der Graph die Vereinigung von fremden Kreisen, Wegen und isolierten Punkten ist.

2.1.4. Eine Komponente des Graphen sieht etwa so aus, wie es in Abbildung 26 geschildert ist. In einem Kreis darf keine Sehne vorkommen, das heisst, die Kreisen dürfen sich nur höchstens in einem Punkt berühren. Fremde Kreisen sind durch Bäume verbunden.

2.1.5. Ja. Siehe eine mögliche Bijektion in Abbildung 27.

2.1.6. Ein gerichteter Baum entsteht aus einem ungerichteten Baum durch Richten der Kanten. Deswegen wird zuerst untersucht, wieviele ungerichtete Bäume mit 4 Punkten existieren.

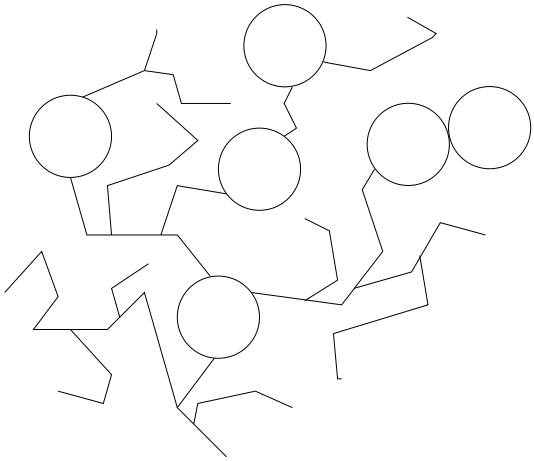


Abbildung 26: Jede Kante kommt höchstens in einem Kreis vor

Dazu wird der grösste Grad im Baum betrachtet; 1 ist unmöglich, da in diesem Fall der Baum nicht zusammenhängend wäre. Ist der grösste Grad 2, dann ist der Baum ein Weg (siehe Aufgabe **2.1.3.**); ist er 3, dann ist der Baum ein "Stern". (Stern bedeutet einen Graphen, in dem ein Punkt Grad $n-1$ hat und alle anderen Punkte Grad 1 haben.) Da der Baum nur 3 Kanten hat, kann der Grösste Grad höchstens 3 sein. Im ungerichteten Sinn wurden also 2 entsprechende Bäume gefunden: ein Weg der Länge 3 und ein Stern mit 4 Punkten. Beide Graphen kann man auf 4 verschiedene Arten richten, wie es Abbildung 28 zeigt. Offensichtlich erhält man nicht-isomorphe gerichtete Graphen, falls man nicht-isomorphe ungerichtete Graphen richtet, und man bekommt alle Lösungen auf diese Weise. Insgesamt gibt es also 8 Lösungen.

2.1.7. Ein Graph mit n Punkten und ohne Kanten besteht aus n Komponenten. Wenn man die Kanten nacheinander einzieht, gibt es bei jeder Kante zwei Möglichkeiten. Entweder verbindet die Kante zwei Punkte, die in verschiedenen Komponenten waren; in diesem Fall wird die Anzahl der Komponenten um 1 verringert. Oder zwei Punkte aus derselben Komponente werden verbunden; in diesem Fall ensteht mindestens ein Kreis. Man kann höchstens $n-1$ solche Kanten einziehen, die die Anzahl der Komponenten verringern, denn am Ende wird es mindestens eine Komponente geben. Jede der restlichen k Kanten muss einen Kreis abschliessen. Also gibt es mindestens k Kreise in dem Graphen.

2.1.8. Zu jeder Lösung kann man eine beliebige Anzahl von isolierten Punkten zufügen, also nehmen wir jetzt an, dass der Graph keine isolierten Punkte beinhaltet. Der längste Weg im Graphen darf höchstens die Länge 2 haben, sonst wären 2 nicht inzidente Kanten in diesem Weg. Falls er die Länge 1 hat, dann besteht der Graph aus einer Kante. Das ist eine Lösung. Falls der längste Weg die Länge 2 hat, dann sind die 2 Endpunkte entweder adjazent, so bekommen wir ein Dreieck, und weitere Kanten sind nicht möglich, oder sie sind nicht adjazent, dann können wir eine beliebige Anzahl von Kanten zu dem mittleren Punkt im Weg zufügen, so bekommen wir einen Stern. Der Graph mit einer Kante ist eigentlich auch ein spezieller Stern, also gibt es 2 wesentlich verschiedene Arten von Lösungen, das Dreieck und den Stern. (Und natürlich noch die beliebige Anzahl von isolierten Punkten.)

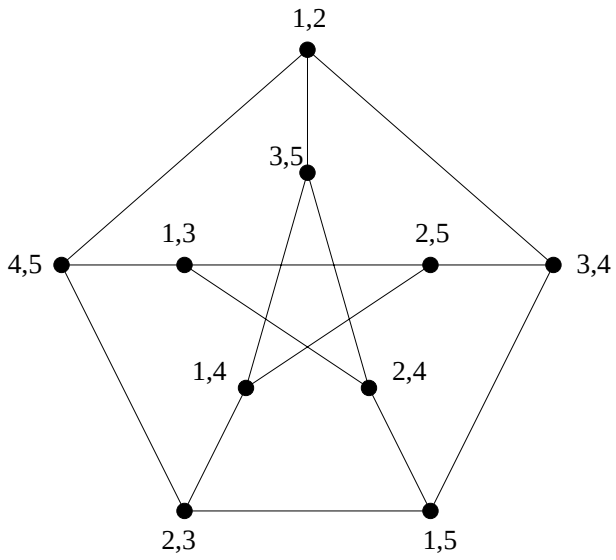


Abbildung 27: Bijektion zwischen dem Petersen-Graphen und $G_{5,2}$

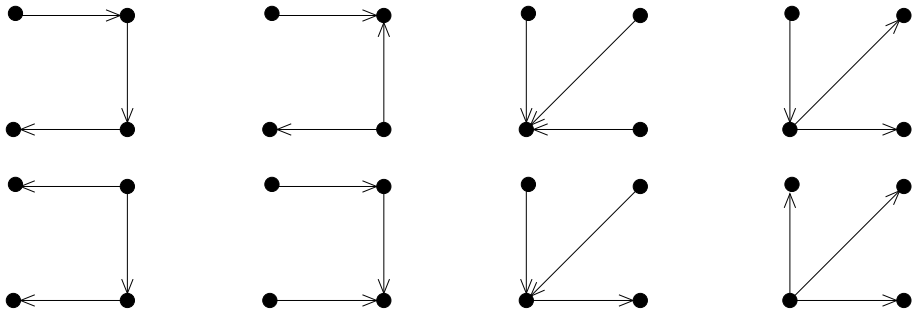


Abbildung 28: Mögliche gerichtete Bäume mit 4 Knotenpunkten

2.1.9. Falls $d \geq n$ ist, dann muss G zusammenhängend sein. Wäre er nämlich nicht zusammenhängend, dann gäbe es mindestens 2 Komponenten; die kleinste könnte höchstens n Punkte beinhalten. Also könnten die Knotenpunkte in dieser Komponente höchstens Grad $n-1$ haben, was ein Widerspruch wäre.
Es muss noch bewiesen werden, dass der Graph für $d = n-1$ nicht unbedingt zusammenhängend ist. Dazu muss lediglich ein Gegenbeispiel gezeigt werden: sei G die Vereinigung von zwei fremden K_n. Dieser Graph ist zwar $d = n-1$-regulär, aber nicht zusammenhängend.

2.1.10. Falls G nicht zusammenhängend ist, dann hat er 2 Komponenten: G_1 und G_2, zwischen denen keine Kanten laufen. Dann sind aber in $\overline{G}$ alle Punktpaare $(x, y),\ x \in G_1, y \in G_2$ mit einer Kante verbunden. Es soll gezeigt werden, dass $\overline{G}$ zusammenhängend ist. Dafür muss man zwischen beliebigen Punkten x, y einen Weg in $\overline{G}$ finden.
Falls $x \in G_1$ und $y \in G_2$, dann sind die Punkte miteinander verbunden, also ein Weg der Länge 1 führt zwischen ihnen.
Falls x und y in der gleichen Komponente sind, also z. B. $x, y \in G_1$, dann gibt es einen Weg der Länge 2 zwischen x und y: nämlich über einen beliebigen Punkt in G_2.

2.1.11.
a) Der längste Weg des Graphen sei $a_1, a_2, \ldots, a_m$. Die Nachbarn von a_1 gehören alle zu der Menge $\{a_2, ..., a_m\}$, sonst gäbe es einen längeren Weg. Da aber a_1 mindestens k Nachbarn hat, muss diese Menge aus mindestens k Knotenpunkten bestehen. Also besteht der längste Weg aus mindestens $k+1$ Knotenpunkten.

b) (Die Bezeichnungen von Aufgabe a) werden weiterhin benutzt.) a_h sei jener Nachbar von a_1, der im betrachteten Weg am weitesten von a_1 entfernt ist (der also den höchsten Index hat). Das bedeutet, dass die Nachbarn von a_1 zu der Menge $\{a_2, \ldots, a_h\}$ gehören, und diese Menge muss ja aus mindestens k Elementen bestehen. Daraus folgt: $h > k$. Da aber a_1 und a_h verbunden sind, hat der Kreis $a_1, \ldots, a_h$ mindestens die Länge $k+1$.

2.1.12.
a) Eine Schlinge ist ein Kreis der Länge 1, so kann sie in keinem aufspannenden Baum enthalten sein. Andere Kanten können wohl in einem aufspannenden Baum enthalten sein, da der aufspannende Baum – aus einer beliebigen Kante angefangen – gierig aufgebaut werden kann.
b) Die Brücken sind dagegen in jedem aufspannenden Baum enthalten, da ohne sie der Graph nicht mehr zusammenhängend wäre, und nur die Brücken haben diese Eigenschaft.

2.1.13. Lösung 1: Sei P der Punkt, der Gradzahl d hat. Aus P kann man in d Richtungen gehen, so dass man nie zu einem solchen Punkt zurückkehrt, wo man schon war. (B ist ein Baum, also beinhaltet er keinen Kreis.) Alle dieser Wege enden in einem Punkt mit Grad 1, und diese Punkte sind verschieden.

Lösung 2: In einem Baum gilt: $\sum_{i=1}^{n} d_i = 2e = 2n-2$. Nehmen wir indirekt an, dass in G höchstens $d-1$ Punkte mit Grad 1 existieren. P hat Grad d, also haben mindestens $n-1-(d-1) = n-d$ Punkte mindestens Grad 2. Dann wäre aber

$$\sum_{i=1}^{n} d_i \geq 1 \cdot d + (d-1) \cdot 1 + (n-d) \cdot 2 = 2n-1$$

und das ist ein Widerspruch.

2.1.14. Beweisen wir die Behauptung mit vollständiger Induktion. Der Fall $k = 1$ ist trivial. Sei die Behauptung für $k-1$ schon bewiesen. Sei B ein beliebiger Baum mit $k+1$ Punkten, und lassen wir einen Punkt mit Grad 1 von B weg; der übriggebliebene Baum wird mit B' bezeichnet. Die weggelassene Kante sei $e = (u, v)$, $u \in B', v \in B \setminus B'$ (siehe Abbildung 29). In G hat jeder Punkt mindestens Grad k, also auch mindestens $k-1$, so existiert laut unserer Induktionsbedingung ein Teilgraph $H' \subset G$, so dass $B' \simeq H'$. Sei das Bild von u bei dieser Isomorphie $w \in H'$. Um einen Teilgraphen $H \subset G$ zu finden, wofür $B \simeq H$ gilt, müssen wir eine Kante aus w zwischen H' und $G \setminus H'$ finden. Aber eine solche Kante kann man immer finden, da w mindestens Grad k hat, und H' ausser ihm nur aus $k-1$ Punkten besteht, also muss mindestens eine Kante aus w nach $G \setminus H'$ führen.

2.1.15.
a) Unmöglich. Die Summe der Zahlen ist ungerade, aber die Summe der Gradzahlen muss wegen $\sum d_i = 2e$ gerade sein.

b) Unmöglich. Falls es einen Punkt mit Grad 0 gibt, dann ist es unmöglich, dass ein Punkt

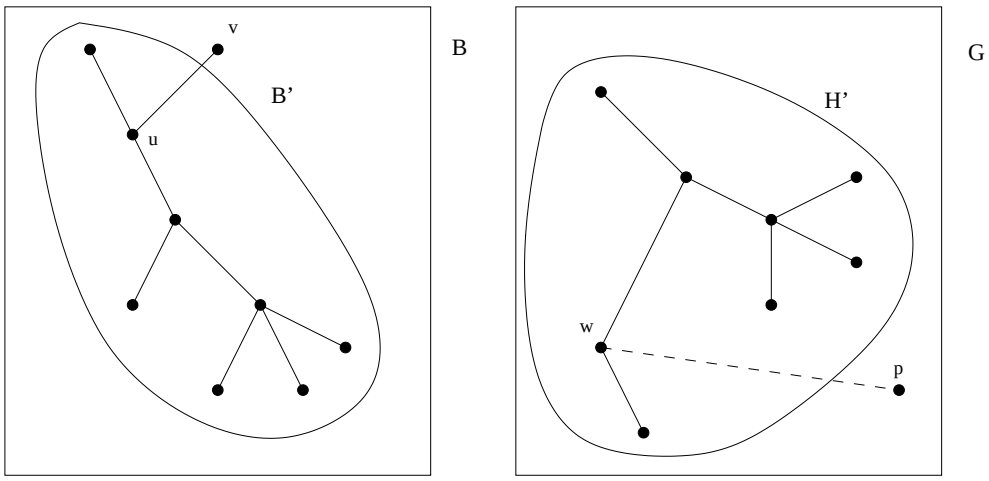


Abbildung 29: Der Baum B' ist isomorph mit $H' \subset G$. Das Bild von u ist w. Die Aufgabe ist, einen Punkt $p \in G \setminus H'$ zu finden, der mit w verbunden ist.

mit jedem Punkt verbunden ist, also Grad 8 hat.

c) Siehe ein Beispiel in Abbildung 30.

d) Beispiel: das Komplement von c).

e) Unmöglich. Der Graph hat 6 Knotenpunkte. Zwei Knotenpunkte haben Grad 5, also sind sie mit allen Punkten verbunden. Daraus folgt, dass jeder Punkt mindestens Grad 2 haben muss, also kann kein Punkt mit Grad 1 existieren.

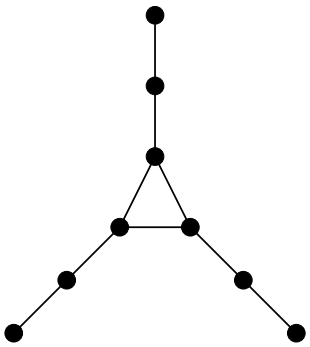


Abbildung 30: Ein Graph mit den Gradzahlen: 1,1,1,2,2,2,3,3,3

2.1.16. u sei der Punkt mit dem grössten positiven Halbgrad. B sei die Menge der Punkte, die aus u über eine Kante erreichbar sind, C der Rest (siehe Abbildung 31). Falls es zu jedem Punkt $c \in C$ einen Punkt $b \in B$ mit einer $b \to c$ Kante gibt, dann sind wir fertig, denn aus u können wir die Punkte in B über eine Kante, die Punkte in C über 2 Kanten erreichen. Sonst gibt es einen Punkt $x \in C$, der nicht aus u über 2 Kanten erreichbar ist, also sind alle Kanten, die x mit Punkten aus B verbinden, von x nach B gerichtet. Auch die Kante (x, u) ist von x nach u gerichtet, denn $x \notin B$. Dann gilt aber $d_+(x) > d_+(u)$, was ein Widerspruch ist.

2.1.17. Da $G \simeq \overline{G}$, so folgt, dass entweder G und $\overline{G}$ beide zusammenhängend oder beide

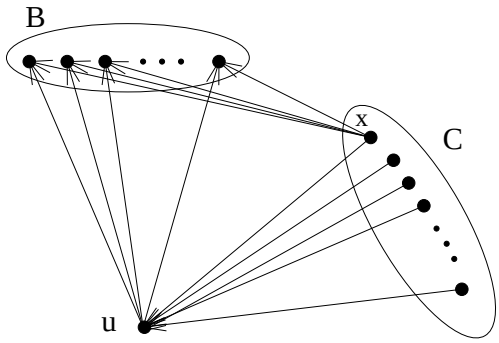


Abbildung 31: Die Punkte in B sind von u direkt erreichbar, die Punkte in C kann man über B erreichen, weil kein solcher Punkt x in C existieren darf.

nicht zusammenhängend sind. Aber der zweite Fall ist wegen **2.1.10.** ausgeschlossen, also ist G zusammenhängend.

2.1.18.
a) Ein Kreis der Länge 5 ist ein gutes Beispiel.

b) Da alle Kanten, die nicht in G sind, in $\overline{G}$ enthalten sind, ist die Summe ihrer Kantenzahlen eben die Anzahl aller möglichen Kanten, also $\binom{n}{2}$. Für $n = 6$ ist diese Zahl ungerade, also G und $\overline{G}$ haben sicherlich verschiedene Anzahl von Kanten, so können sie auch nicht isomorph sein.

2.1.19. Die 2 Graphen sind nicht isomorph, weil es in dem einen Graphen Dreiecke gibt, aber in dem anderen nicht.

2.1.20. Die 2 Graphen sind isomorph, eine mögliche Bijektion zwischen den Punkten ist in Abbildung 32 dargestellt.

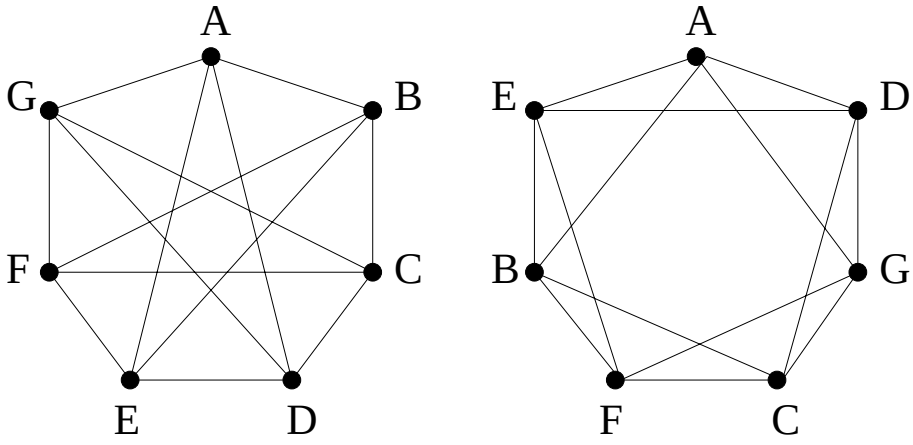


Abbildung 32: Die Bijektion beweist die Isomorphie der Graphen

2.1.21. Man versuche, den Prüfer-Code eines Baumes mit der gegebenen Eigenschaft herzustellen. Es ist bekannt, dass jede Zahlenfolge der Länge $n - 2$, wo alle Zahlen kleiner oder gleich n sind, ein gültiger Prüfer-Code ist, also einen Baum repräsentiert. Weiterhin wissen

wir, dass jeder Punkt x im Prüfer-Code $d(x) - 1$-mal vorkommt. (Jedesmal, wenn wir einen seiner Nachbarn löschen, schreiben wir x auf, bis zum Löschen seiner vorletzten Nachbar. Was bei dem letzten Nachbar passiert, hängt davon ab, ob x der letzte Punkt im Prüfer-Code sein wird. Falls x nicht der letzte Punkt sein wird, dann müssen wir x vor seinem letztem Nachbar löschen, deswegen kommt x im Prüfer-Code nur $d(x) - 1$-mal vor. Falls x der letzte Punkt ist, dann schreiben wir es zwar $d(x)$-mal auf, jedoch löschen wir dann die letzte Zahl im Code, so kommt x wirklich nur $d(x) - 1$-mal vor.)
Betrachten wir die folgende Zahlenfolge:

$$\underbrace{1,\ldots,1}_{d_1-1},\underbrace{2,\ldots,2}_{d_2-1},\ldots,\underbrace{n,\ldots,n}_{d_n-1}$$

Diese Folge hat $n-2$ Elemente, da $\sum_{i=1}^{n} d_i = 2n-2$ und davon haben wir n-mal 1 subtrahiert. Der Baum, der zu diesem Prüfer-Code gehört, ist eine entsprechende Lösung.
(Bemerkung: die obige Zahlenfolge kann natürlich auch in anderen Reihenfolgen aufgeschrieben werden; so kann man eventuell verschiedene Lösungen erhalten. Es kann aber auch sein, dass diese Lösungen isomorph sind.)

2.1.22. Falls es unter beliebigen 3 Punkten höchstens eine Kante gibt, dann können keine zwei Kanten inzident sein. Das heisst, dass jeder Punkt höchstens Grad 1 hat. Daraus folgt, dass die maximale Anzahl der Kanten $\lfloor \frac{n}{2} \rfloor$ sein kann.

2.1.23. Für $\forall x \in V(G)$ gilt, dass $d_G(x) + d_{\overline{G}}(x) = 5$. Daraus folgt, dass entweder $d_G(x)$ oder $d_{\overline{G}}(x)$ mindestens 3 ist. Nehmen wir an, dass für einen konkreten Punkt p gilt, dass $d_G(p) \geq 3$. Seien $u, v, w \in V(G)$ Nachbarpunkte von p in G. Falls es eine Kante zwischen u, v, w in G gibt, z. B. zwischen u und v, dann existiert ein Dreick in G (nämlich $\{u, v, p\}$), sonst bilden u, v und w ein Dreieck in $\overline{G}$.

2.2 Bipartite Graphen und Matchings

2.2.1. Es wird zuerst gezeigt, dass es in einem r-regulären bipartiten Graphen ein vollständiges Matching gibt. Dafür muss man die zwei Bedingungen der Existenz eines vollständigen Matchings prüfen.
(i) In Klasse A gebe es a, in Klasse B gebe es b Knotenpunkte. Dann laufen aus Klasse A genau ra Kanten aus, aus Klasse B laufen rb Kanten aus, und da diese beiden Grössen gleich sein müssen, gilt $a = b$.
(ii) C sei eine Teilmenge von A mit c Punkten, die Menge der Nachbarn dieser Punkte sei $D = N(C)$ mit d Punkten. Dann laufen aus D mindestens so viele Kanten aus, wie aus C (weil ja alle Kanten, die aus C auslaufen, auch bei D zählen, aber es können noch weitere Kanten aus D auslaufen), so gilt $d \cdot r \geq c \cdot r$, also $d \geq c$.
Dieser Graph befriedigt also die Hall-Bedingungen, so beinhaltet er ein vollständiges Matching. Wenn man die Kanten dieses Matchings entfernt, so bleibt ein $r-1$- regulärer bipartiter Graph zurück. Darin kann man wieder ein vollständiges Matching finden, es weglassen usw. Am Ende bleibt ein 1-regulärer Graph, der ein Matching ist. Insgesamt besteht also der Originalgraph aus r fremden vollständigen Matchings.

2.2.2. Betrachten wir zuerst jene Kanten, die das innere Fünfeck mit dem äusseren zusammenbinden. Es ist einfach zu sehen, dass ein vollständiges Matching entweder 1 oder 5 von diesen Kanten benutzt (siehe Abbildung 33). Daraus folgt, dass es mit drei vollständigen Matchings unmöglich ist, die 5 solchen Kanten genau einmal abzudecken, also ist es auch unmöglich, die Kantenmenge des Graphen mit drei disjunkten vollständigen Matchings abzudecken.

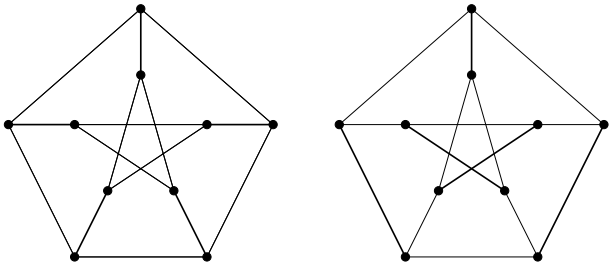


Abbildung 33: Die verschiedenen Paarungen in dem Petersen Graphen

2.2.3. Bezeichne man mit δ die Anzahl der fehlenden Kanten, damit der Graph r-regulär wird. Seien $x \in A$ und $y \in B$ zwei Punkte mit $d(x) < r$ und $d(y) < r$. Falls x und y nicht adjazent sind, dann kann man sie einfach verbinden, und mit diesem Schritt hat man δ mit 1 verringert. Falls x und y adjazent sind, so ergänzt man G mit dem Graphen in Abbildung 34. $2r$ neue Punkte werden also aufgenommen, die alle Grad r haben und je eine weitere Kante wird zu x und y geschlossen. Damit hat man δ wieder vermindert. Daraus folgt, dass der Algorithmus nach endlich vielen Schritten terminiert, und mit $\delta = 0$ wird ein r-regulärer Graph gemacht.
(Bemerkung: wenn auch Parallelkanten erlaubt sind, dann ist die Aufgabe natürlich einfacher, weil man dann x und y ruhig verbinden kann, auch wenn sie schon adjazent waren.)

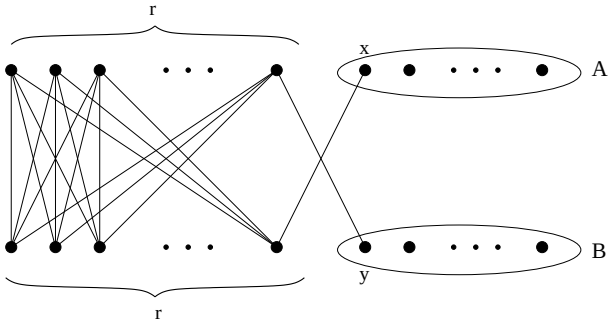


Abbildung 34: Dieser Graph soll zu den Punkten x und y zugefügt werden

2.2.4. Im Sinne von Aufgabe **2.2.3.** kann man den Graphen mit zusätzlichen Kanten und Punkten so ergänzen, dass der neue Graph G' r-regulär ist. Aufgabe **2.2.1.** sagt aus, dass G' die Vereinigung von r disjunkten Matchings ist. Da $E(G) \subset E(G')$, ein Matching M' in G' definiert auch ein Matching in G, nämlich $M = M' \cap E(G)$. So erhält man höchstens r disjunkte Matchings in G.

2.2.5. Man betrachte den folgenden Graphen G^* :

$$V(G^*) = V(G) \quad \text{und} \quad E(G^*) = E(M_1) \triangle E(M_2)$$

wo M_1 und M_2 die 2 verschiedene vollständige Paarungen sind, und $\triangle$ bedeutet die symmetrische Differenz. (Also sind in G^* solche Kanten, die in genau einer der beiden Paarungen beinhaltet sind.) Es ist einfach zu sehen, dass jeder Punkt in G^* entweder Grad 0 oder Grad 2 hat, und es gibt mindestens einen Punkt mit Grad 2, sonst wären M_1 und M_2 nicht verschieden. In Aufgabe **2.1.3.** wurde gezeigt, dass ein solcher Graph die Vereinigung von disjunkten Kreisen (und isolierten Punkten) ist, also gibt es in G^* mindestens einen Kreis. Da G^* ein Teilgraph von G ist, daraus folgt, dass auch G einen Kreis beinhaltet.

2.2.6. Es ist nicht möglich. (Folgt sofort aus Aufgabe **2.2.5.**)

2.2.7. Wenn man entlang eines Kreises läuft, muss man k-mal von A nach B und k-mal von B nach A laufen, damit man am Ende wieder den Startpunkt erreicht. Insgesamt sind das $2k$ Kanten.

2.2.8. Wenn alle Kreise eine ungerade Länge haben, dann kann ein Kreis keine Sehnen haben, da eine Sehne einen solchen Kreis in zwei Kreise schneidet, einer von beiden eine gerade Länge hat. Das ist eben die Eigenschaft von Aufgabe **2.1.4.**, also sehen die Graphen so aus, wie es in Abbildung 26 dargestellt ist (wobei natürlich alle Kreise eine ungerade Länge haben).

2.2.9. Nehmen wir indirekt an, dass die Kante xy eine Brücke ist. Wenn man x aus G entfernt, hat der zurückbleibende Graph ein vollständiges Matching, daraus folgt, dass die Komponente von x (aber ohne x) eine gerade Anzahl von Punkten beinhaltet, sonst könnte kein Matching existieren. Wenn man y aus G entfernt, hat auch dieser Graph ein vollständiges Matching, daraus folgt, dass die Komponente von x auch mit x eine gerade Anzahl von Knotenpunkten beinhaltet. Das ist ein Widerspruch.

2.2.10. Der Graph ist zusammenhängend, also kann kein isolierter Punkt existieren. Das heisst, dass die Gradzahlen zwischen 1 und n sind. Wenn sie also in Klasse A alle verschieden sind, bedeutet das, dass jede Zahl zwischen 1 und n genau einmal unter den Gradzahlen der Punkte in Klasse A vorkommt. Es wird bewiesen, dass die zwei Bedingungen für die Existenz eines vollständigen Matchings erfüllt sind.
Die Anzahl der Punkte in den beiden Klassen ist gleich.
Sei $X \subset A$ und $|X| = k$. In X kommen k verschiedene Gradzahlen aus der Menge $\{1, \ldots, n\}$ vor, so ist die grösste Gradzahl in X mindestens k, also hat der Punkt mit der grössten Gradzahl allein schon mindestens k Nachbarn, also $|N(X)| \geq |X|$.

2.2.11. Wir zählen die Möglichkeiten nach der Anzahl der Strahlen in der Paarung zusammen (siehe Abbildung 35). Die Lösungen sind in Tabelle 2 aufgezählt.

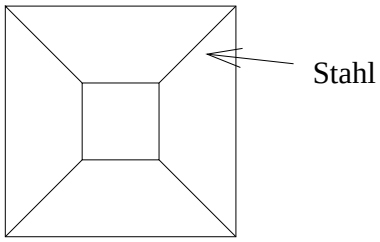


Abbildung 35: Das Kantennetz des Würfels

Anzahl der Strahlen	*Anzahl der Matchings*
0	4
1	0
2	4
3	0
4	1
$\sum$	9

Tabelle 2: Matchings in dem 3-dimensionalen Würfel

2.2.12. Aufgabe **2.2.3.** zeigt, dass G mit neuen Punkten und Kanten zu einem k-regulären Graphen G' ergänzt werden kann. Dabei bleiben die Punkte mit Grad k ungeändert. In Aufgabe **2.2.1.** wurde gezeigt, dass es in einem regulären bipartiten Graphen ein vollständiges Matching M' gibt. $M = M' \cap E(G)$ ist ein (nicht unbedingt vollständiges) Matching in G, das die Knotenpunkte mit Grad k abdeckt.

2.2.13.
a) In jeder Runde können höchstens n Spiele stattfinden, insgesamt gibt es $\binom{2n+1}{2} = (2n+1)n$ Spiele. Deswegen braucht man mindestens $2n+1$ Runden.

b) Ein Turnier kann mit einem Graphen modelliert werden. Die Knotenpunkte entsprechen den Spielern, die Kanten den Spielen. Der Graph ist ein K_{2n+1}. Wir organisieren das Turnier wie es in Abbildung 36 zu sehen ist. Die fett gedruckten Spiele werden in der ersten Runde gespielt.
k. Runde: wie in Abbildung 36, nur mit $\frac{k \cdot 2\pi}{n}$ gedreht. Es ist leicht zu sehen, dass diese Konstruktion die Aufgabe löst.

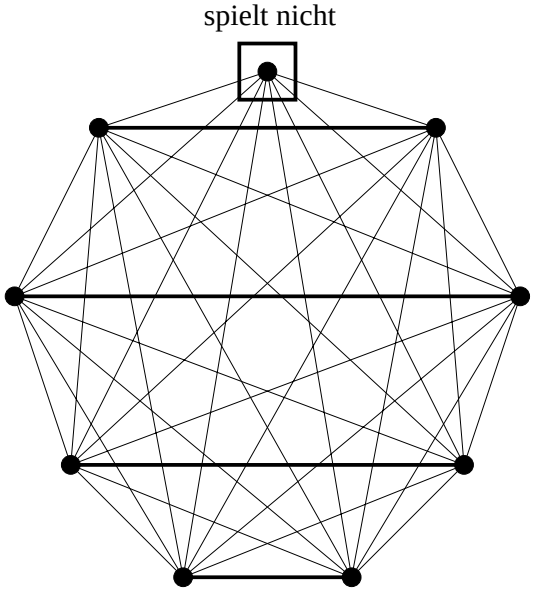


Abbildung 36: Eine Runde des Turniers für $2n+1 = 9$

2.2.14. Die Aufgabe kann auf die Suche einer "herkömmlichen" vollständigen Paarung in einem entsprechend modifizierten Graphen zurückgeführt werden. In A verdoppelt man nämlich alle Punkte (mit ihren Kanten), so bekommt man einen bipartiten Graphen, der in beiden Gruppen eine gleiche Anzahl von Knotenpunkten hat, und wo nun mit der gelernten Methode ein vollständiges Matching gesucht werden kann. Wenn hier ein vollständiges Matching gefunden wird, das entspricht eben einem Teilgraphen in dem originalen Graphen mit der gewünschten Eigenschaft.

2.2.15. Falls die Anzahl der Punkte ungerade ist, dann ist es sicherlich nicht möglich, eine vollständige Paarung zu machen. Wir zeigen, dass es sonst möglich ist.
In den geraden Kreisen können wir eine vollständige Paarung machen, ohne irgendeine Kante einzuziehen. In den ungeraden Kreisen bleibt je ein Punkt übrig. Wir müssen eine Kante zwischen zwei solchen Punkten einziehen. Sei die Anzahl der ungeraden Kreise c_p. c_p muss gerade sein, um eine vollständige Paarung zu ermöglichen; in diesem Fall braucht man eben $m = \frac{c_p}{2}$ Kanten, um die ausgebliebenen Punkte paarweise zu verbinden.

2.2.16. Der Graph besteht aus zwei Komponenten (siehe Abbildung 37). In der ersten Komponente besteht die maximale Paarung aus einer Kante. In der zweiten Komponente kann die maximale Paarung aus höchstens drei Kanten bestehen, da sich in einer Klasse der Komponente nur drei Punkte befinden. Es ist trivial, dass eine Paarung mit drei Kanten in dieser Komponente existiert, also besteht die maximale Paarung in dem Graphen aus insgesamt vier Kanten.

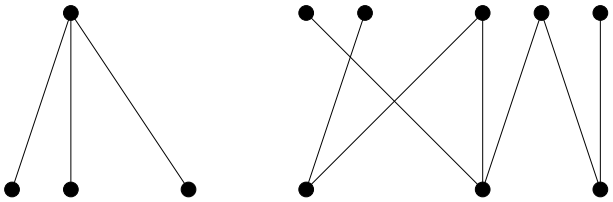


Abbildung 37: Anschauliche Darstellung von den zwei Komponenten des Graphen

2.3 Die vier griechischen Buchstaben: $\alpha, \tau, \nu, \varrho$

2.3.1. Zuerst wird τ, also die minimale Anzahl der abdeckenden Punkte, bestimmt. Der Petersen-Graph hat 2 disjunkte Kreise der Länge 5 als Teilgraphen (K_1, K_2), wie es Abbildung 38 darstellt. Um K_1 abzudecken braucht man mindestens 3 Punkte, und damit wird keine Kante in K_2 abgedeckt, also um beide Kreise abzudecken braucht man mindestens 6 Punkte. Es ist leicht zu sehen, dass es mit 6 Punkten möglich ist, alle Kanten abzudecken, also $\tau = 6$. Daraus folgt sofort, dass $\alpha = 4$. Der Graph hat 10 Punkte, also die maximale Anzahl der unabhängigen Kanten kann höchstens 5 sein, und das ist erreichbar. (Z. B. die 5 Kanten, die K_1 und K_2 zusammenbinden.) Das bedeutet, dass $\nu = 5$ und $\varrho = 5$.

2.3.2. Der Graph ist in Abbildung 39 dargestellt. Zuerst wird α bestimmt. Jeder Punkt hat Grad 4, also mit der Auswahl eines Punktes sind weitere 4 Punkte ausgeschlossen. Die restlichen 3 Punkte bilden ein Dreieck, also kann aus ihnen nur noch ein Punkt ausgewählt werden.

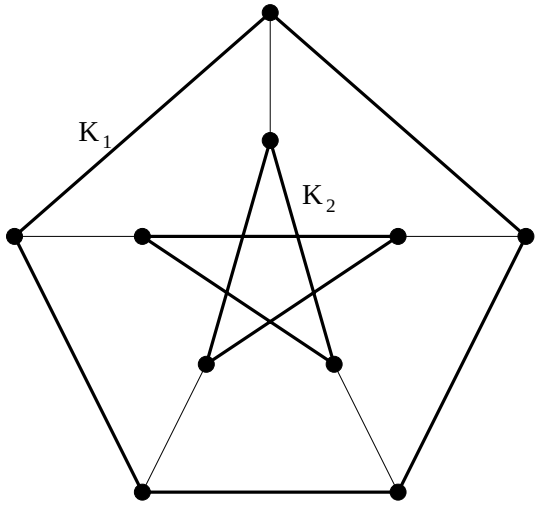


Abbildung 38: Zwei Kreise der Länge 5 in dem Petersen-Graphen

So ist $\alpha = 2 \Rightarrow \tau = 6$. Der Graph hat ein vollständiges Matching (z. B.: (1,2),(3,4),(5,6),(7,8)), also $\nu = 4 \Rightarrow \varrho = 4$.

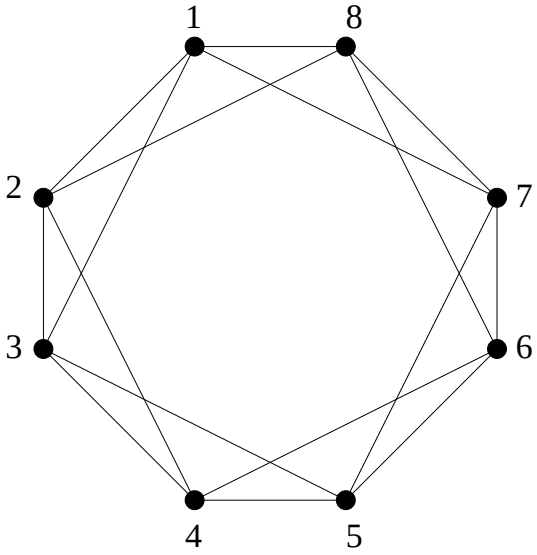


Abbildung 39:

2.3.3. a) $\tau = 1$ ist unmöglich, da ein Punkt höchstens Grad $n-1$ haben kann, so kann er nicht alle n Kanten abdecken. $\tau = 2$ ist aber schon erreichbar, siehe Abbildung 40.

b) Jede Kante kann höchstens 2 Punkte abdecken, also $\varrho \geq \lceil \frac{n}{2} \rceil$. Wenn n gerade ist, so kann man diese Grenze erreichen, falls der Graph ein vollständiges Matching beinhaltet. Ist n ungerade, so soll der Graph ein "fast" vollständiges Matching beinhalten, also ein Matching, das $n-1$ Punkte abdeckt. Dazu braucht man $\frac{n-1}{2}$ Kanten, und noch eine Kante, um den letzten Punkt abzudecken. Insgesamt $\frac{n-1}{2} + 1 = \frac{n+1}{2} = \lceil \frac{n}{2} \rceil$, also wird auch in diesem Fall die untere Grenze erreicht.

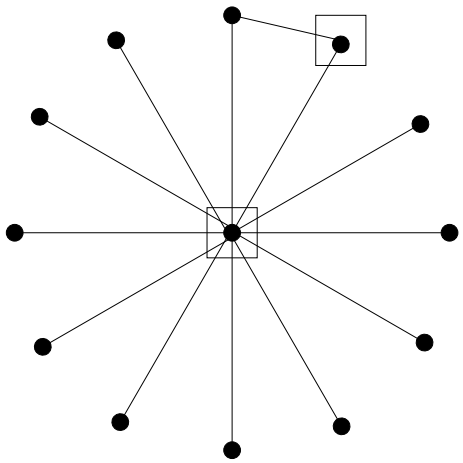


Abbildung 40: Ein Beispiel für $\tau = 2$

2.3.4. Der Graph hat $2n$ Punkte. Sei der "untere" $2n-1$-lange Weg W und der "obere" Punkt P. Man kann ein vollständiges Matching finden (jede zweite Kante in W und der letzte Punkt mit P verbunden), also $\nu = n \Rightarrow \varrho = n$. Es ist trivial, dass P nicht in der maximalen Menge der unabhängigen Punkte sein kann, weil er zu jedem anderen Punkt adjazent ist. Also muss man die maximale unabhängige Punktmenge in W finden. Es ist einfach zu sehen, dass W genau n unabhängige Punkte hat (jeder zweite Punkt), daraus folgt, dass $\alpha = n \Rightarrow \tau = n$.

2.3.5. Sei T die minimale abdeckende Punktmenge. Dann gilt:

$$e \leq \sum_{x \in T} d(x) \leq \sum_{i=1}^{\tau} d = d \cdot \tau$$

2.3.6. Der Graph ist in Abbildung 41 dargestellt. Der Graph hat 11 Knotenpunkte, deswegen kann ν höchstens 5 sein. Z.B. die Kanten (1,2) (3,7), (4,5), (8,9), (10,11) sind unabhängig, also $\nu = 5$. Dieser Graph ist bipartit (siehe auch Aufgabe **2.9.5.**). Aus den Sätzen von König und Gallai erhält man sofort, dass $\tau = 5$ und $\alpha = \varrho = 6$.

2.3.7. $\tau \leq 2\nu$ gilt auf jeden Fall, denn die 2ν Endpunkte der ν Kanten in dem maximalen Matching bilden eine abdeckende Punktmenge. Wäre nämlich eine Kante durch diese Punkte nicht abgedeckt, so könnte man das Matching noch mit dieser Kante ergänzen. Daraus folgt, dass das Maximum von $\frac{\tau}{\nu}$ höchstens 2 sein kann. Das kann erreicht werden, zum Beispiel wenn der Graph ein Dreieck ist; dann ist $\tau = 2$ und $\nu = 1$. Also ist die Antwort 2.

2.4 BFS, DFS, Dijkstra, Ford, Floyd, PERT

2.4.1. Bei der Durchführung des DFS-Algorithmus treten keine Rückwärtskanten auf, also kann der Graph keinen gerichteten Kreis enthalten. Ein möglicher DFS-Wald ist in Abbildung 42 dargestellt. Die Knotenpunkte wurden so nummeriert, dass der Punkt beim ersten Rücktritt die Nummer 15, beim zweiten die Nummer 14 usw. bekommen hat. Die Zahlen entsprechen einer topologischen Ordnung.

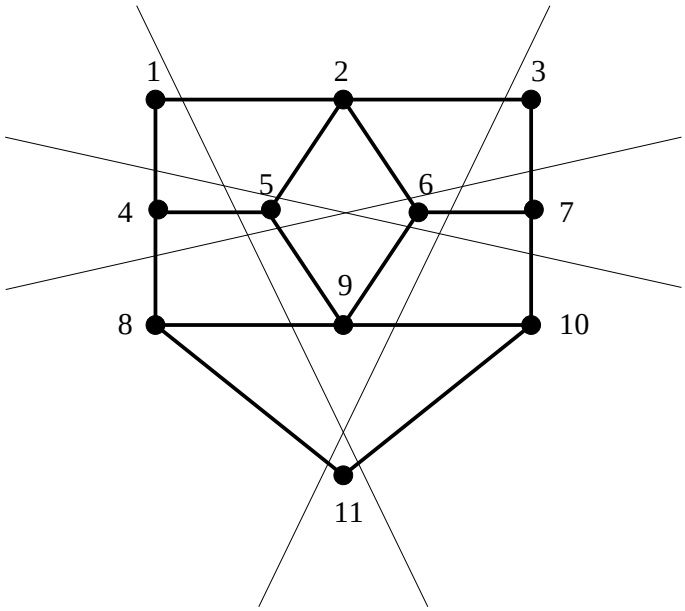


Abbildung 41: Der duale Graph des durch die 4 Geraden gebildeten Graphen

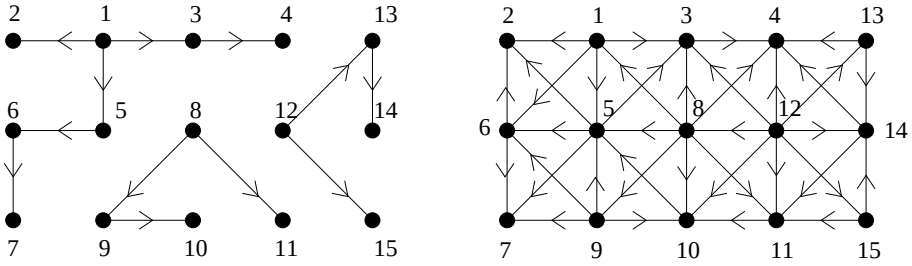


Abbildung 42: Ein möglicher DFS-Wald und die dazu gehörende topologische Ordnung

2.4.2. Man beginne mit der Breitsuche aus dem Punkt x. Dieser Punkt soll zur Klasse A gehören. Seine Nachbarn im BFS-Baum gehören dann zur Klasse B, die Nachbarn dieser Punkte zur Klasse A usw. Am Ende bekommt man entweder eine Bipartition, oder zwei Punkte in derselben Klasse, die verbunden sind. Dann bilden aber diese Kante und die Wegstücke, die aus diesen 2 Punkten nach x bis zu ihrem Schnittpunkt y führen (siehe Abbildung 43), einen ungeraden Kreis, also kann der Graph nicht bipartit sein.

2.4.3. Man wählt einen Punkt aus, der noch nicht im Matching ist. Der BFS-Algorithmus wird aus diesem Punkt gestartet, so dass man im ersten, dritten, ... Schritt nur solche Kanten benutzt, die nicht im Matching sind, im zweiten, vierten, ... Schritt nur die Kanten des Matchings. Wenn ein Zweig des BFS-Baumes mit einer Kante terminiert, die nicht im Matching enthalten ist, hat man einen verbessernden Weg gefunden. Sonst hat man eine Menge gefunden, die der Hall-Bedingung widerspricht (siehe Abbildung 44).

2.4.4. Die Lösung der Aufgabe kann man in Tabelle 3. sehen.

2.4.5. Die Lösung der Aufgabe kann man in Tabelle 4. sehen.

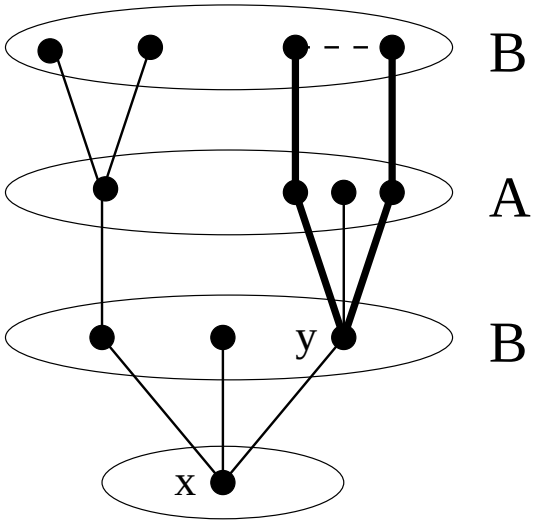


Abbildung 43: Falls es eine Kante zwischen zwei Punkten in derselben Klasse gibt (gestrichelt), dann existiert ein Kreis mit ungerader Länge (fett)

Schritt	D(S)	D(A)	D(B)	D(C)	D(D)	D(E)	Fertig
0	0	∞	∞	∞	∞	∞	S
1	0	3	2	∞	∞	∞	S,B
2	0	3	2	3	5	∞	S,B,(A oder C)
3	0	3	2	3	5	∞	S,B,A,C
4	0	3	2	3	4	7	S,B,A,C,D
5	0	3	2	3	4	6	S,B,A,C,D,E

Tabelle 3: Schritte des Dijkstra Algorithmus

Schritt	D(A)	D(B)	D(C)	D(D)	D(E)	D(F)	Fertig
0	0	∞	∞	∞	∞	∞	A
1	0	3	∞	7	∞	8	A,B
2	0	3	5	7	8	4	A,B,F
3	0	3	5	7	8	4	A,B,F,C
4	0	3	5	6	7	4	A,B,F,C,D
5	0	3	5	6	7	4	A,B,F,C,D,E

Tabelle 4: Schritte des Dijkstra Algorithmus

2.4.6. Der topologisch geordnete Graph ist in Abbildung 45 dargestellt. Die frühesten Anfangszeiten sind in Tabelle 5 zusammengefasst. Die Dauer des Prozesses ist:

$$f(x) = \begin{cases} 13 & \text{falls} \quad 0 \leq x \leq 7 \\ 6 + x & \text{falls} \quad x > 7 \end{cases}$$

Die kritischen Tätigkeiten sind:

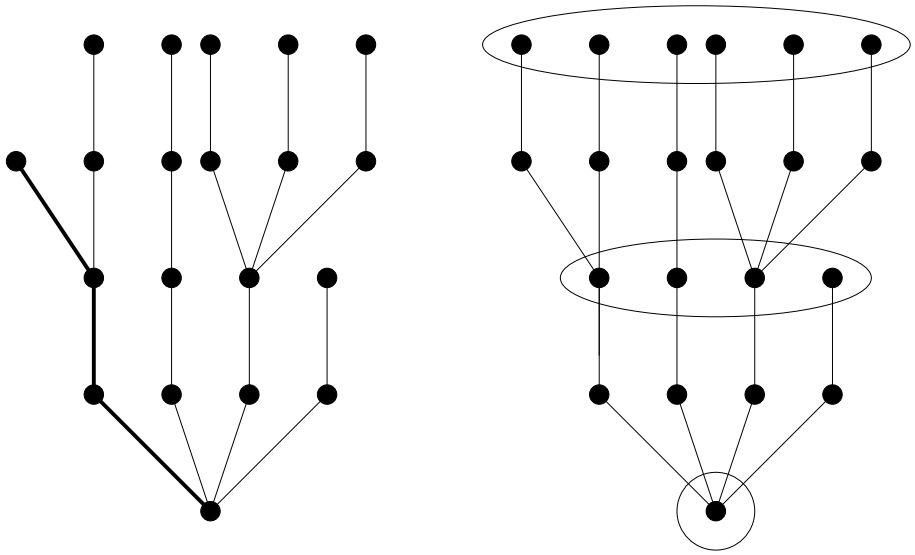


Abbildung 44: Ergebnis der Breitsuche; im ersten Fall ist ein verbessernder Weg fett gezeichnet, im zweiten Fall die markierte Menge widerspricht der Hall-Bedingung

$$\begin{array}{lll} \{A, C, D, E\} & \text{falls} & 0 \leq x < 7 \\ \{A, B, D, E\} & \text{falls} & x > 7 \\ \{A, B, C, D, E\} & \text{falls} & x = 7 \end{array}$$

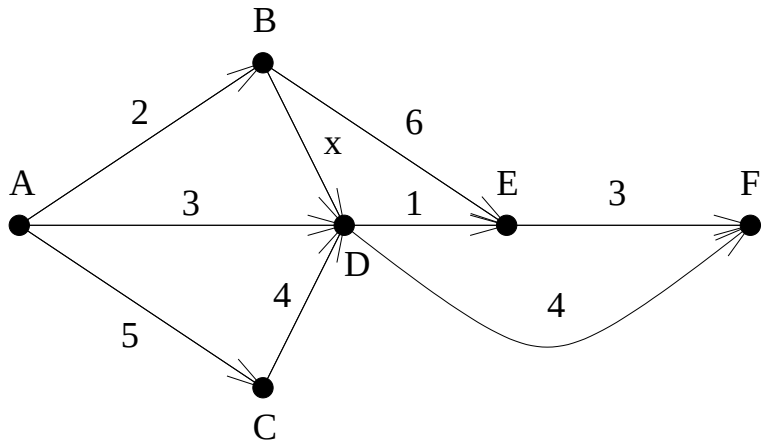


Abbildung 45: Der Graph nach der topologischen Ordnung; nun kann der PERT-Algorithmus durchgeführt werden

A	B	C	D	E	F
0	2	5	$\max(9, 2+x)$	$\max(10, 3+x)$	$\max(13, 6+x)$

Tabelle 5: Anfangszeiten

2.4.7. a) Das Ergebnis des Algorithmus von Ford ist in Tabelle 6 zu sehen. Wir haben gezeigt,

dass die Reihenfolge der Kanten die Länge des Algorithmus beeinflussen kann. Die Entfernung vom Punkt 1 haben wir mit $d(\cdot)$ bezeichnet. Zusammenfassend:

$$d(2) = 1, \quad d(3) = 4, \quad d(4) = -1, \quad d(5) = 1$$

b) Das Ergebnis des Algorithmus von Floyd ist in Tabelle 7 zu sehen. Die letzte Tabelle enthält die Entfernungen. (Bemerkung: die Kanten waren in diesem Beispiel so gerichtet, dass aus einem Punkt mit höherer Zahl ein Punkt mit niedrigerer Zahl nicht erreichbar war. Deswegen stand in jeder Tabelle unter der Hauptdiagonale immer ∞. Im allgemeinen Fall gilt diese Eigenschaft nicht.)

	(1,2)	(1,3)	(1,4)	(1,5)	(2,3)	(2,4)	(2,5)	(3,4)	(3,5)	(4,5)
1	d(2)=1	d(3)=4	d(4)=1	d(5)=5	-	d(4)=-1	d(5)=2	-	-	d(5)=1
2	-	-	-	-	-	-	-	-	-	-

	(4,5)	(3,5)	(3,4)	(2,5)	(2,4)	(2,3)	(1,5)	(1,4)	(1,3)	(1,2)
1	-	-	-	-	-	-	d(5)=5	d(4)=1	d(3)=4	d(2)=1
2	d(5)=3	-	-	d(5)=2	d(4)=-1	-	-	-	-	-
3	d(5)=1	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-

Tabelle 6: Schritte des Ford-Algorithmus bei zwei verschiedenen Reihenfolgen der verbessernden Kanten

2.4.8. Die Dauer der Aufgabe ist $\max(11, 7+x)$. Die kritischen Tätigkeiten sind in Abbildung 46 zu sehen, in Abhängigkeit davon, ob $x < 4$, $x > 4$ oder $x = 4$.

2.5 Netzwerke und Flüsse

2.5.1. In kleineren Graphen ist es oft einfacher, statt des maximalen Flusses die minimale $\{s, t\}$-Schnittmenge zu finden und den Satz von Ford-Fulkerson anzuwenden. Betrachte man alle mögliche $\{s, t\}$-Schnittmengen des Graphen, wie es in Abbildung 47 dargestellt ist. (Dieser Schritt geht in grösseren Graphen nicht, weil es exponentiell viele $\{s, t\}$-Schnittmengen geben können.) Die unterschiedlichen Kapazitäten sind:

$$10, 9, 14, 11, 6 + x, 8, 17$$

0	1	2	3	4	5
1	0	1	4	1	5
2	∞	0	3	-2	1
3	∞	∞	0	3	-2
4	∞	∞	∞	0	2
5	∞	∞	∞	∞	0

1	1	2	3	4	5
1	0	1	4	1	5
2	∞	0	3	-2	1
3	∞	∞	0	3	-2
4	∞	∞	∞	0	2
5	∞	∞	∞	∞	0

2	1	2	3	4	5
1	0	1	4	-1	2
2	∞	0	3	-2	1
3	∞	∞	0	3	-2
4	∞	∞	∞	0	2
5	∞	∞	∞	∞	0

3	1	2	3	4	5
1	0	1	4	-1	2
2	∞	0	3	-2	1
3	∞	∞	0	3	-2
4	∞	∞	∞	0	2
5	∞	∞	∞	∞	0

4	1	2	3	4	5
1	0	1	4	-1	1
2	∞	0	3	-2	0
3	∞	∞	0	3	-2
4	∞	∞	∞	0	2
5	∞	∞	∞	∞	0

5	1	2	3	4	5
1	0	1	4	-1	1
2	∞	0	3	-2	0
3	∞	∞	0	3	-2
4	∞	∞	∞	0	2
5	∞	∞	∞	∞	0

Tabelle 7: Schritte des Floyd-Algorithmus

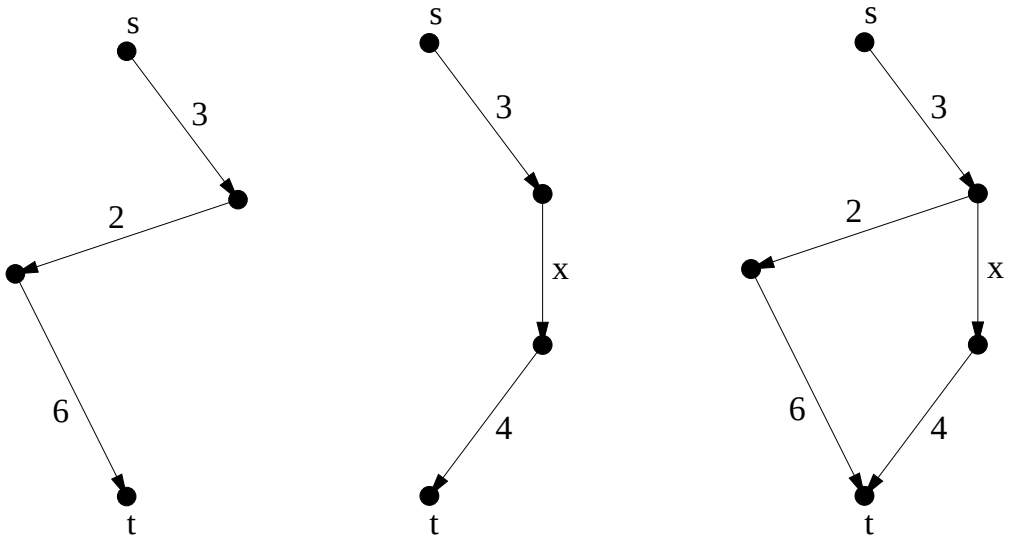


Abbildung 46: Die kritischen Tätigkeiten falls $x < 4$, $x > 4$ oder $x = 4$.

Die minimale Schnittmenge (und laut des Satzes von Ford-Fulkerson auch der maximale Fluss) ist also

$$\begin{cases} 6 + x & \text{falls } x < 2 \\ 8 & \text{falls } x \geq 2 \end{cases}$$

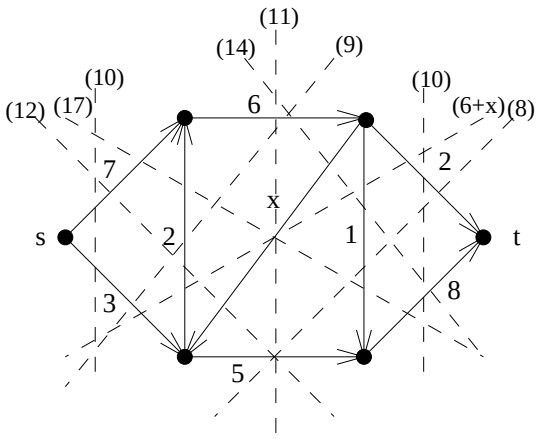


Abbildung 47: Alle $\{s,t\}$-Schnittmengen in dem Graphen

Der maximale Fluss kann man in Abbildung 48 sehen.

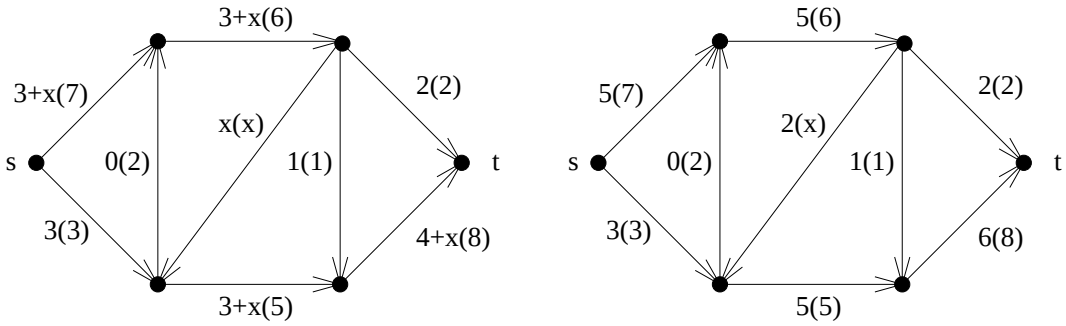


Abbildung 48: Der maximale Fluss, falls a) $x < 2$ b) $x \geq 2$.

2.5.2. Die minimale Schnittmenge ist

$$\begin{cases} x+4 & \text{falls } x \leq 7, y \geq 1 \\ y+10 & \text{falls } x \geq 7, y \leq 1 \\ 11 & \text{falls } x \geq 7, y \geq 1 \\ x+y+3 & \text{sonst} \end{cases}$$

2.5.3.
a) Die Kanten mit Kapazität 1 bilden eine Schnittmenge mit Kapazität 4, also kann f_3 höchstens 4 sein. Es gibt auch einen Fluss der Stärke 4, also $f_3 = 4$.

b) Man braucht nur eine Schnittmenge der Kapazität 2^{n-1} zu zeigen. Dazu betrachte man die folgenden Mengen: A bestehe aus den Punkten, die mit 0, B aus jenen, die mit 1 enden. Das ist eine Partition der Knotenpunkte mit $s \in A$ und $t \in B$, also bilden die Kanten zwischen A und B einen (s,t)-Schnitt. Andererseits haben alle dieser Kanten die Kapazität 1. Es gibt 2^{n-1} solche Kanten und sie zeigen alle von A nach B. Also ist die Kapazität dieser Schnittmenge tatsächlich 2^{n-1}.
(Allgemein ist der Fluss wesentlich kleiner, weil z. B. die Schnittmenge, die s von dem Rest des Netzwerks teilt, die Kapazität $1+2+\ldots+n = n(n+1)/2 \ll 2^{n-1}$ hat.)

2.5.4. Man erweitert einen bipartiten Graphen $G = (A, B)$ zu einem Netzwerk, wie es in Abbildung 49 geschildert ist.(Die Kanten werden dabei von oben nach unten gerichtet; $|A| = |B| = n$.)
In diesem Netzwerk ist jede Kantenkapazität eine ganze Zahl, also gibt es einen maximalen

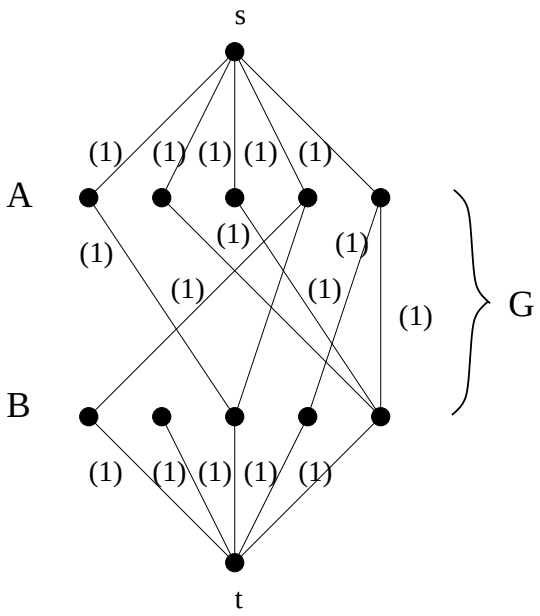


Abbildung 49:

Fluss, der über jede Kante eine ganze Zahl transportiert. Diese ganze Zahl kann entweder 0 oder 1 sein. Es ist einfach zu sehen, dass jene Kanten von G, über die 1 transportiert wird, ein Matching bilden. Daraus folgt, dass der maximale Fluss im Netzwerk und die Grösse des maximalen Matchings in G gleich sind, andererseits ist *maxFlow=minCut*. Folgendes muss also bewiesen werden:

Die minimale Schnittmengenkapazität im Netzwerk ist genau dann gleich n, wenn G die Hall-Bedingung erfüllt.

Sei jetzt die Hall-Bedingung nicht erfüllt, das heisst, dass es eine k-elementige Menge $X \subset A$ gibt, so dass $|N(X)| < k$. Dann kann man eine Schnittmenge Q definieren, die eine Kapazität $< n$ hat (siehe Abbildung 50 linkes Bild). In diesem Fall ist $c(Q) = n - k + |N(X)| < n$.

Umgekehrt, es soll gezeigt werden, dass falls die Hall-Bedingung erfüllt ist, dann haben alle Schnittmengen eine Kapazität von mindestens n. Betrachten wir eine allgemeine Schnittmenge (siehe Abbildung 50 rechtes Bild). Sei l die Anzahl der Punkte in B, die sich an der linken Seite von Q befinden. Dann gilt, dass $c(Q) = n-k+l+t$, wo t die Anzahl solcher Kanten bezeichnet, die von X nach $B \setminus N(X)$ führen. Daraus folgt, dass in B an der rechten Seite von Q höchstens t Punkte sein können, also sind mindestens $k - t$ Punkte an der linken Seite, weil $|N(X)| \geq k$ wegen der Hall-Bedingung. So folgt, dass $l \geq k - t$, das heisst, dass $c(Q) = n - k + l + t \geq n$. Das sollte bewiesen werden.

2.5.5.
a) Richtig. Wenn man alle Kantenkapazitäten halbiert, bekommt man ein Netzwerk mit ganzzahligen Kapazitäten. In diesem Netzwerk gibt es also einen maximalen Fluss, der über jede

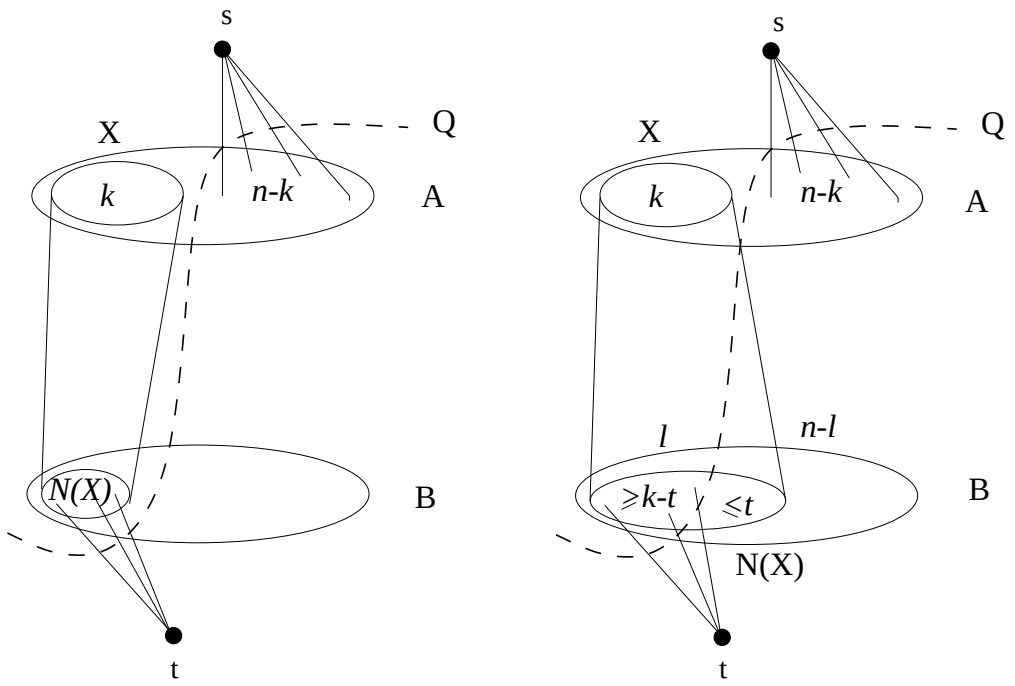


Abbildung 50:

Kante eine ganze Zahl transportiert. Das Zweifache dieses Flusses ist ein maximaler Fluss im Originalnetzwerk, der über jede Kante eine gerade Zahl transportiert.

b) Falsch. Ein Gegenbeispiel siehe in Abbildung 51.

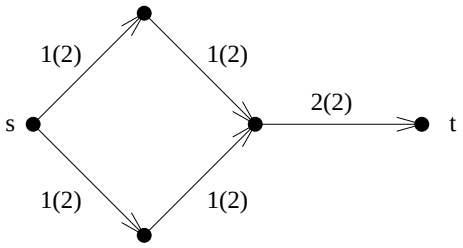


Abbildung 51:

c) Falsch. Ein Gegenbeispiel siehe in Abbildung 52. In diesem Netzwerk hat der maximale Fluss den Wert 1. Um überhaupt ganze Zahlen über die einzelnen Kanten zu transportieren, darf man nur einen der beiden "Zweigen" benutzen. Dann wird aber über die Kanten des anderen Zweiges 0 transportiert.

d) Falsch. Daraus würde nämlich c) folgen.

2.5.6. Statt des maximalen Flusses bestimmen wir die minimale Schnittmenge abhängig von x und y. (Ford-Fulkerson Satz). Die möglichen minimalen Schnittmengen sind:

$$5,\ 3+x,\ 3+y,\ x+y$$

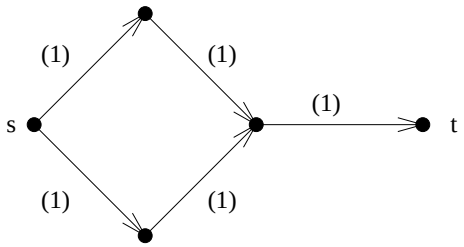


Abbildung 52:

5 ist die minimale Schnittmenge, falls:

$$\begin{aligned} 5 &\leq 3+x \\ 5 &\leq 3+y \\ 5 &\leq x+y \end{aligned}$$

gleichzeitig gültig sind.

Ähnlicherweise kann man die andere Fälle erledigen, und das Ergebnis kann man in Abbildung 53 sehen.

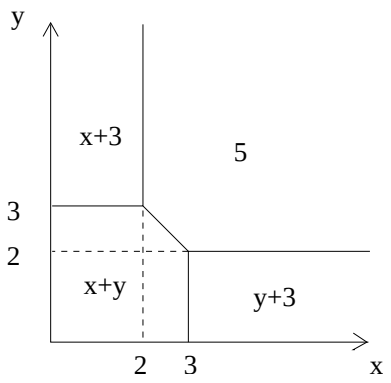


Abbildung 53:

2.6 k-facher Zusammenhang

2.6.1. Ein Graph ist genau dann k-fach zusammenhängend, wenn es zwischen beliebigen zwei Punkten mindestens k disjunkte Wege gibt. Ein Graph ist genau dann k-fach kantenzusammenhängend, wenn es zwischen beliebigen zwei Punkten mindestens k kantendisjunkte Wege gibt. Die zwei Begriffe sind dann verschieden, wenn es Wege gibt, die sich in einem Knotenpunkt schneiden (dann sind sie nämlich kantendisjunkt, aber nicht disjunkt). Das kann aber in einem 3-regulären Graphen nicht vorkommen (der Punkt, wo sich die Wege schneiden, müsste mindestens Grad 4 haben).

2.6.2. Jeder Knotenpunkt hat mindestens k Nachbarn. (Wenn nämlich ein Punkt weniger Nachbarn hätte, würde der Graph nicht mehr zusammenhängend bleiben, wenn man die aus

diesem Punkt hinausgehenden Kanten entfernt.) Daraus folgt

$$e = \frac{1}{2}\sum_{x\in V} d(x) \geq \frac{1}{2}\sum_{x\in V} k = \frac{1}{2}nk$$

(Bemerkung: die Behauptung gilt natürlich auch für k-fach knotenpunktzusammenhängende Graphen, da diese ja auch k-fach kantenzusammenhängend sind.)

2.6.3. Man nehme indirekt an, dass es eine Punktmenge X mit $k-1$ Knotenpunkten gibt, so dass $G - X$ in zwei Komponenten (G_1 und G_2) zerfällt. Ein Punkt in G_1 hat seine Nachbarn in X und G_1, insgesamt mindestens $\frac{n+k-2}{2}$. Da er aber in X höchstens $k-1$ Nachbarn haben kann, muss er in G_1 mindestens $\frac{n+k-2}{2} - (k-1)$ Nachbarn haben. Es gilt also

$$|V(G_1)| \geq 1 + \frac{n+k-2}{2} - (k-1) = \frac{n-k+2}{2}$$

Ähnlicherweise gilt

$$|V(G_2)| \geq \frac{n-k+2}{2}$$

und somit

$$|V(G)| \geq \frac{n-k+2}{2} + \frac{n-k+2}{2} + k - 1 = n + 1$$

was ein Widerspruch ist.

2.6.4. Nein. Ein Gegenbeispiel ist ein Kreis. Die Bedingung ist natürlich erfüllt, da durch beliebige 3 Punkte ein Kreis läuft, nämlich der ganze Graph. Aber er ist nur zweifach zusammenhängend, denn wir können zwei nicht adjazente Punkte weglassen, so dass der Graph in zwei Komponenten zerfällt.

2.6.5.
a) Nein, Abbildung 54 zeigt ein Gegenbeispiel.

b) Ja. Wenn der Graph nicht zweifach kantenzusammenhängend wäre, dann würde eine Brücke im Graphen existieren, die eine einelementige Schnittmenge ist – was der Bedingung widerspricht.

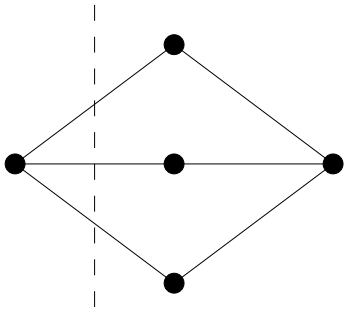


Abbildung 54:

2.7 Eulersche und Hamiltonsche Kreise und Wege

2.7.1. Man kann die Felder des Schachbrettes als die Knotenpunkte eines Graphen auffassen, wobei zwei Punkte genau dann verbunden sind, falls die zugehörigen Felder mit einem Pferdesprung voneinander erreichbar sind. Die Aufgabe ist, in diesem Graphen einen Hamiltonschen Weg zu finden. Das geht aber nicht, weil der Graph in 6 Komponenten zerfällt (mit 1, 2, 3, 4, 5, 6 bezeichnet; siehe Abbildung 55), falls die inneren 4 Felder (mit x bezeichnet) gestrichen werden.

1	5	6	2
6	x	x	5
5	x	x	6
3	6	5	4

Abbildung 55: Wenn man die inneren 4 Punkte entfernt, zerfällt der Graph in 6 Komponenten

2.7.2. G' sei ein gerichteter Graph, den man aus G bekommt, wenn man alle Kanten von G verdoppelt und einmal in die eine, einmal in die andere Richtung richtet. Für alle Punkte von G' gilt $d_+ = d_-$ und G' ist stark zusammenhängend, also hat G' einen gerichteten Eulerschen Kreis. Dieser "Kreis" benutzt alle Kanten von G genau einmal in die eine und einmal in die andere Richtung.

2.7.3.
a) $a = b = 2$. Sonst gibt es nämlich Punkte mit Grad 3.

b) Es muss genau 2 Punkte mit Grad 3 geben, also ist entweder $a = 2$ und $b = 3$, oder $a = 3$ und $b = 2$.

c) a oder b muss gerade sein (vielleicht auch beide). Sonst wäre nämlich die Anzahl der Punkte (ab) und damit auch die Länge des Hamiltonschen Kreises ungerade. Da aber dieser Graph bipartit ist, kann er überhaupt keine Kreise mit ungerader Länge enthalten. Falls die Anzahl der Punkte gerade ist, dann kann man einfach einen Hamiltonschen Kreis im Graphen finden.

d) Einen Hamiltonschen Weg gibt es für alle Werte von a und b.

2.7.4. $G_{m,k}$ hat $\binom{m}{k}$ Knotenpunkte, jeder Knotenpunkt hat Grad $\binom{m-k}{k}$.

a) Nein. Jeder Punkt hat Grad 1, also ist der Graph nicht zusammenhängend. Deswegen kann er auch keinen Hamiltonschen Kreis enthalten.

b) Ja. Der Graph hat 560 Knotenpunkte, jeder hat Grad 286. Nach dem Satz von Dirac hat der Graph einen Hamiltonschen Kreis.

2.7.5. K bestehe aus den Punkten $x_1, \ldots, x_k$. So besteht der längste Weg aus k Knotenpunkten und $k-1$ Kanten. Man nehme indirekt an, dass K kein Hamiltonscher Kreis ist.

Daraus folgt (da der Graph zusammenhängend ist), dass mindestens einer der Punkte von K (z. B. x_i) einen Nachbarn y hat, der nicht in K enthalten ist. In diesem Fall wäre aber $y, x_i, x_{i+1}, \ldots, x_k, x_1, \ldots, x_{i-1}$ ein Weg mit $k+1$ Knotenpunkten, was ein Widerspruch ist (siehe Abbildung 56).

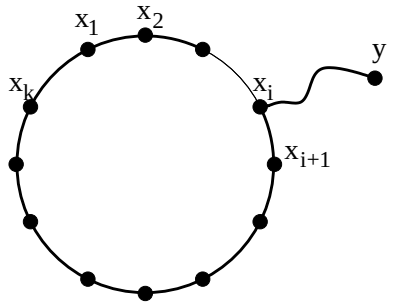


Abbildung 56: $y, x_i, x_{i+1}, \ldots, x_k, x_1, \ldots, x_{i-1}$ wäre ein längerer Weg als $x_1, \ldots, x_k$

2.7.6. K_n hat $\dfrac{(n-1)!}{2}$ Hamiltonsche Kreise. (Es gibt $n!$ Reihenfolgen, doch bei einem Kreis ist es egal, wo man anfängt und in welche Richtung man vorgeht; siehe auch Aufgabe **1.1.2.** – deswegen muss mit $2n$ dividiert werden.) Davon müssen jetzt diejenigen abgezogen werden, die eine gegebene Kante benutzen: $(n-2)!$ (Für die Reihenfolge der restlichen $n-2$ Punkte hat man soviele Möglichkeiten, und diesmal ist der Anfangspunkt und die Richtung schon eindeutig.) Also ist das Ergebnis $\dfrac{(n-1)!}{2} - (n-2)!$

2.7.7. Ja. Ein Beispiel sieht man in Abbildung 57.

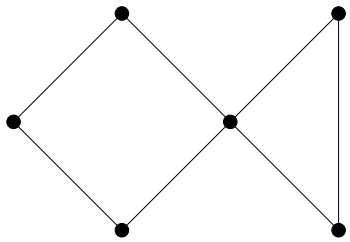
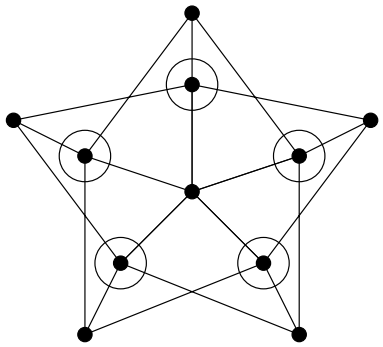


Abbildung 57: Die Anzahl der Knptenpunkte is gerade, die Anzahl der Kanten ist ungerade, und es gibt einen Eulerschen Kreis im Graphen.

2.7.8.
a) Ja. Sei G ein Kreis mit n Punkten. Klar, dass es einen Hamiltonschen Kreis in G gibt. In $\overline{G}$ hat jeder Punkt Grad $n-3$. Falls $n > 5$ ist, dann ist $n - 3 \geq \frac{n}{2}$, also existiert laut des Satzes von Dirac ein Hamiltonscher Kreis in $\overline{G}$. Es ist einfach zu sehen, dass der Kreis auch für $n = 5$ gut ist.

b) Ja. Sei G ein Stern mit n Punkten. G hat keinen Hamiltonschen Kreis, da er Punkte mit Grad 1 beinhaltet. $\overline{G}$ hat einen isolierten Punkt, also kann er auch keinen Hamiltonschen Kreis enthalten.

2.7.9. Nein, der Graph beinhaltet keinen Hamiltonschen Kreis. Beweis: man entferne die markierten 5 Knotenpunkte, und der Graph zerfällt in 6 Komponenten.



2.8 Färbungen

2.8.1. Die chromatische Zahl ist mindestens 8, da z. B. $v_1, \ldots, v_8$ einen K_8 bilden. 8 Farben reichen aber auch aus, wie die folgende Färbung zeigt: die Farben werden mit $0, \ldots, 7$ bezeichnet, v_i bekommt die Farbe: $i \ mod \ 8$. Das ist eine korrekte Färbung, weil die Entfernung von Knotenpunkten mit derselben Farbe ein Vielfaches von 8 ist und so können sie nicht verbunden sein.

2.8.2.
a) Die maximale Anzahl der unabhängigen Knotenpunkte ist 2 (man kann höchstens 2 Knotenpunkte auswählen, so dass keine Kante zwischen ihnen läuft, nämlich zwei Punkte, die im Hamiltonschen Kreis benachbart sind), so braucht man mindestens $2k/2 = k$ Farben. k Farben reichen auch aus, wie die folgende Färbung zeigt: man bezeichne die Knotenpunkte entlang des weggelassenen Hamiltonschen Kreises mit $v_1, \ldots, v_{2k}$; v_{2i} und v_{2i-1} bekommen die Farbe i $(i = 1, \ldots, k)$.

b) Die maximale Anzahl der unabhängigen Knotenpunkte ist 2, so braucht man mindestens $\lceil (2k+1)/2 \rceil = k + 1$ Farben. $k + 1$ Farben reichen auch aus, eine mögliche Färbung ist die von Aufgabe a), mit dem Unterschied, dass der letzte Punkt allein die Farbe $k + 1$ bekommt.

2.8.3. Zuerst eine triviale Bemerkung: wenn ein Graph mit 3 Farben färbbar ist, dann ist er auch so mit 3 Farben färbbar, dass die Farbe eines Knotenpunktes schon im voraus festgelegt ist.
Nun betrachte man einen Graphen mit n Knotenpunkten (der Graph hat genau die Eigenschaft von Aufgabe **2.1.4.** und sieht wie in Abbildung 26 aus). Die Behauptung wird mit vollständiger Induktion für n bewiesen. Für $n = 1$ ist die Behauptung trivial. Man nehme an, die Behauptung ist schon für $\forall k < n$ bewiesen. Falls der Graph kreisfrei ist, ist die Behauptung selbstverständlich (ein kreisfreier Graph hat auch keine ungeraden Kreise und so ist er bipartit, also kann er sogar mit 2 Farben gefärbt werden). Sonst nimmt man einen Kreis (C) und färbt ihn (unabhängig vom Rest des Graphen) mit 3 Farben (wenn der Kreis eine gerade Länge hat, reichen 2 Farben aus, sonst braucht man alle 3). Wenn man die Kanten dieses Kreises entfernt, zerfällt der Graph in Komponenten.
Zwei Knotenpunkte des Kreises können nicht in derselben Komponente sein. Wenn nämlich die Punkte x und y des Kreises beide in der Komponente K liegen, dann gibt es einen $x - y$ Weg sowohl in K als auch in C. Diese Wege bilden zusammen wiederum einen Kreis, also sind die Kanten, die in C zwischen x und y laufen, in mindestens zwei Kreisen enthalten (siehe

Abbildung 58).
Die Färbung von C schreibt also nur die Farbe eines einzigen Punktes in jeder Komponente vor, und so können die Komponenten laut der Induktionsbedingung (sie haben weniger als n Knotenpunkte) und der ersten Bemerkung entsprechend gefärbt werden.

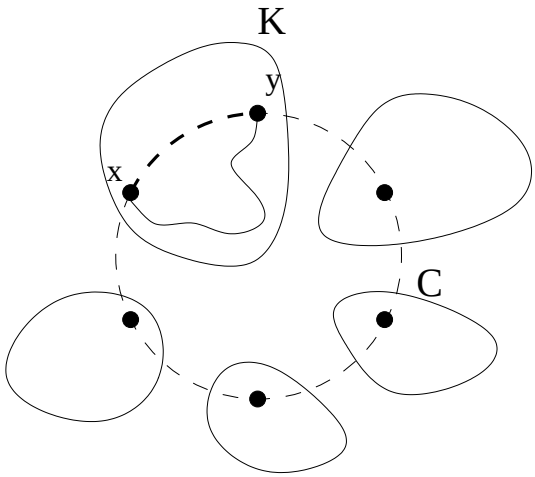


Abbildung 58: Wenn sich x und y in derselber Komponente befinden, wären die Kanten des Kreises K zwischen x und y in zwei Kreisen enthalten.

2.8.4.
a) Ein r-regulärer bipartiter Graph ist die Vereinigung von r disjunkten Matchings (siehe Aufgabe **2.2.1.**), die den r Farben entsprechen.

b) Siehe Aufgabe **2.2.4.**.

2.8.5. In Aufgabe **2.8.2.** b) wurde bewiesen, dass die chromatische Zahl dieses Graphen $k+1$ ist, falls der Graph $2k+1$ Punkte hat. Aber es gibt keinen K_{k+1} in diesem Graphen, weil es unter beliebigen $k+1$ Punkten mindestens zwei gibt, die im weggelassenen Kreis benachbart sind, also sind sie im Graphen nicht verbunden. Es gilt also:

$$\chi = k+1, \quad \omega < k+1$$

Der Graph ist also nicht perfekt.

2.8.6. $\chi(P) = 3$. Weniger kann es nicht sein, da P kein bipartiter Graph ist. (Er beinhaltet nämlich Kreise mit ungerader Länge.) Eine Färbung mit 3 Farben kann man einfach konstruieren.
$\chi_e(P) = 4$. Wären die Kanten von P mit 3 Farben färbbar, dann würden 3 disjunkte vollständige Matchings in P existieren, was Aufgabe **2.2.2.** widerspricht.

2.8.7. Falls $\chi(G) = 3$, dann gibt es einen ungeraden Kreis K in G. Wenn wir eine beliebige Kante weglassen, dann ist G schon mit 2 Farben färbbar, also darf kein ungerader Kreis in $G - e$ existieren. Das bedeutet, dass $e \in K$. Da e beliebig war, folgt, dass $G = K$. Also die Antwort ist: ein Kreis mit ungerader Länge (und eventuell noch isolierte Punkte).

2.8.8. Numerieren wir die k Farben von 1 bis k. Numerieren wir auch die Punkte, so dass jeder Punkt die Zahl seiner Farbe bekommt. Richten wir alle Kanten, so dass sie von dem Punkt mit der kleineren Zahl zu dem Punkt mit der grösseren Zahl zeigen. (Zwischen Punkten mit der gleichen Zahl führen ja keine Kanten.) In diesem Fall geht ein gerichteter Weg immer von Punkten mit kleineren Zahlen zu Punkten mit grösseren Zahlen. Klar, dass der längste Weg höchstens durch k Punkte gehen kann.

2.8.9. In beiden Graphen befindet sich ein K_4, also $\chi \geq 4$ in beiden Fällen. Den linken Graphen kann man mit 4 Farben färben (siehe Abbildung 59 linkes Bild), also $\chi = 4$. Bei dem anderen Graphen ist es einfach zu sehen, dass $\alpha = 2$, also muss χ wegen des Satzes $\chi \geq \frac{n}{\alpha}$ mindestens 5 sein. Mit fünf Farben ist es schon färbbar, siehe das rechte Bild in Abbildung 59.

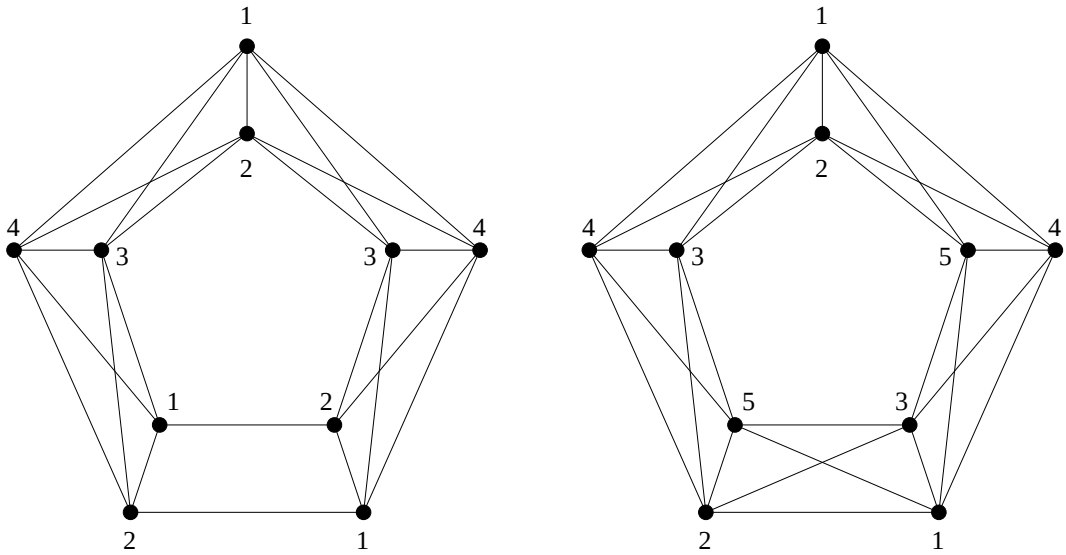


Abbildung 59:

2.8.10. Sei der Baum mit zwei Farben gefärbt. Falls der längste Weg im Baum aus mindestens vier Punkten besteht, dann existieren zwei Punkte in diesem Weg, die verschiedene Farben haben und nicht adjazent sind. Diese Punkte kann man verbinden und der Graph bleibt noch mit zwei Farben färbbar. Also, um die gewünschte Eigenschaft zu erfüllen, darf der längste Weg aus höchstens drei Punkten, das heisst, aus höchstens zwei Kanten bestehen. Das charakterisiert eben die Sterne. Es ist trivial, dass die Sterne die gewünschte Eigenschaft tatsächlich erfüllen.

2.9 Planarität

2.9.1.
a) Der Graph ist planar; eine mögliche kreuzungsfreie Umzeichnung mit geraden Linien siehe in Abbildung 60.

b) Nicht planar; der Petersen-Graph enthält $K_{3,3}$ als topologischen Teilgraphen (siehe Abbildung 61).

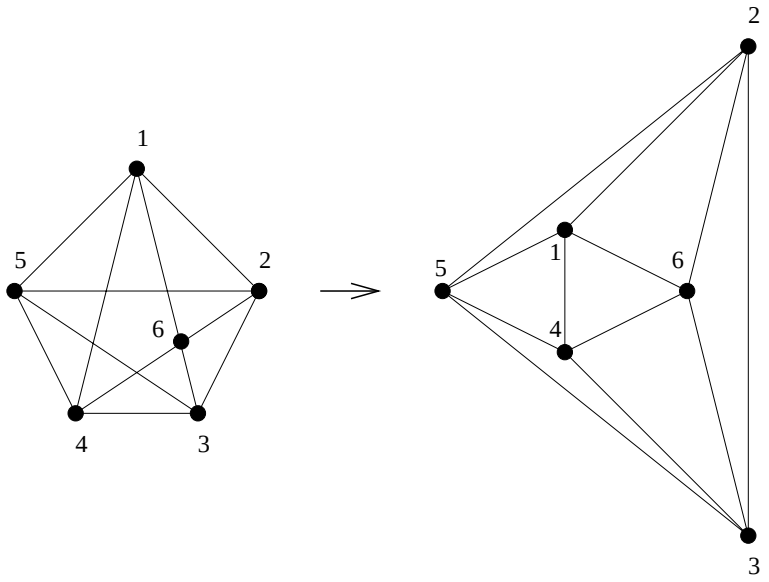


Abbildung 60:

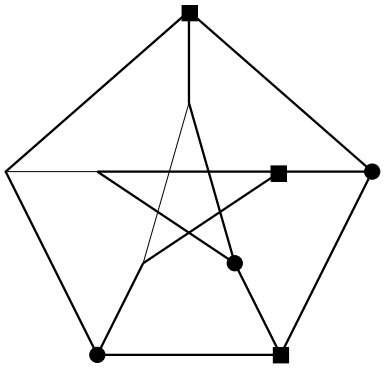


Abbildung 61: $K_{3,3}$ in dem Petersen Graphen

c) Der Graph ist planar; eine mögliche kreuzungsfreie Umzeichnung mit geraden Linien siehe in Abbildung 62.

2.9.2. Graph *1* enthält Punkte mit Grad 4, Graph *2* aber nicht, also können sie nicht isomorph sein. Sie sind aber schwach isomorph, weil sie mit Hilfe der Whitney-Sätze ineinander transformiert werden können.

2.9.3.
a) Wenn G planar ist, dann gilt $3n - 6 \geq e$. Wenn die minimale Gradzahl gleich 5 ist, dann hat G mindestens $5n/2 = 2.5n$ Kanten, also $e \geq 2.5n$. Daraus folgt

$$3n - 6 \geq 2.5n$$

$$n \geq 12$$

b) Einen entsprechenden Graphen mit $n = 12$ siehe in Abbildung 63. Es ist das Kantennetz eines Ikosaeders.

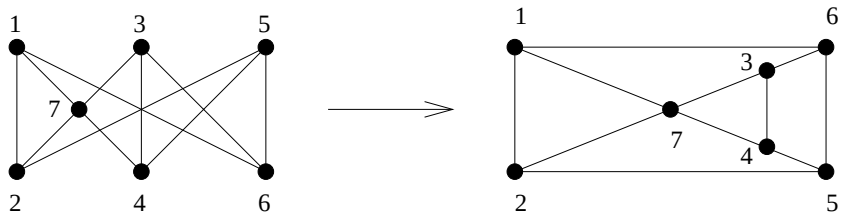


Abbildung 62:

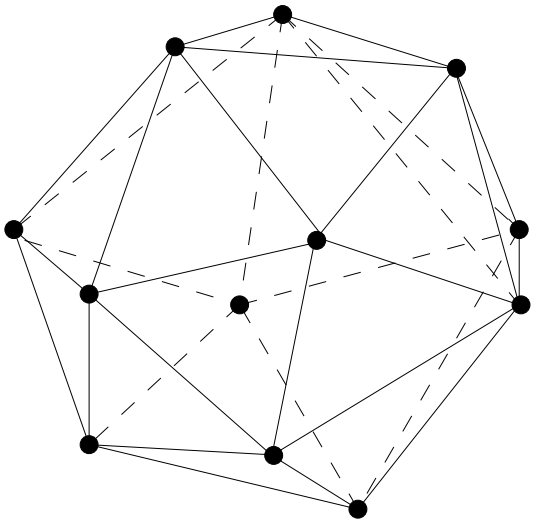


Abbildung 63:

2.9.4.
a) Nicht planar. Für den Beweis siehe b).

b) Jeder Punkt hat $\binom{k+1}{k-1}$ Nachbarn. In einem planaren Graphen ist die minimale Gradzahl höchstens 5, also es gilt $\binom{k+1}{k-1} = \binom{k+1}{2} \leq 5$. Daraus folgt, dass $k \leq 2$. Also ist nur $G_{4,1}$ planar.

2.9.5.
a) Der entstandene Graph sei G, sein Dual sei G'. Eine Kante in G' entspricht dem Durchquären einer Gerade in G. Man betrachte einen Kreis in G'. Das entspricht einer geschlossenen Folge von benachbarten Flächen in G. Wenn dabei eine Gerade durchquärt wird, wird sie noch einmal in die andere Richtung durchquärt. Daraus folgt, dass die Kreise in G' eine gerade Länge haben und so können die Knotenpunkte von G' mit 2 Farben gefärbt werden. Das bedeutet, dass die Flächen in G mit 2 Farben färbbar sind.

b) Der gleiche Beweis funktioniert auch für Kreise, weil auch Kreise die Eigenschaft besitzen, dass die geschlossene Folge von Flächen jedes Mal, wenn sie sie in die eine Richtung durchquährt, auch in die andere Richtung durchquären muss.

2.9.6. Eine Landeskarte, für die man mindestens 6 Farben braucht, ist in Abbildung 64 zu sehen. Ähnlicherweise kann man Landeskarten konstruieren, für die man eine beliebig hohe

Anzahl von Farben braucht.

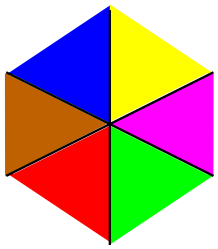


Abbildung 64:

2.9.7. Ja, das ist nämlich das Kantennetz eines Würfels (siehe Abbildung 65).

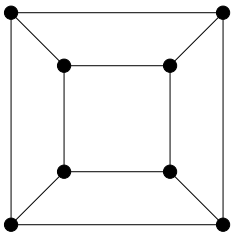


Abbildung 65: Ein Würfel in planarer Darstellung

2.9.8. In einem sechfach zusammenhängenden Graphen muss jeder Punkt mindestens Grad sechs haben, sonst könnte man einen Punkt so isolieren, dass man seine (höchstens fünf) Nachbarpunkte weglässt. Daraus folgt, dass $e \geq \frac{6n}{2} = 3n$. Es ist aber bekannt, dass in einem planaren Graphen $e \leq 3n - 6$ gilt. Das ist ein Widerspruch, also existiert kein solcher Graph.

2.9.9. In Abbildung 61 auf der Seite 64. ist zu sehen, dass der Petersen-Graph $K_{3,3}$ als topologischen Teilgraphen beinhaltet. Bei der Konstruktion wurden nicht alle Kanten benutzt: eine innere und eine mittlere Kante wurde nicht verwendet. Das bedeutet, dass man (wegen der Symmetrie) eine beliebige innere oder mittlere Kante weglassen kann und der Graph ist immer noch nicht planar. Da die Rolle der inneren und äusseren Kanten auch symmetrisch ist, geht das auch für eine äussere Kante. Also ist der übriggebliebene Graph auf keinen Fall planar.

2.9.10. Wegen dem 4-Farben Satz gilt in einem planaren Graphen $\chi \leq 4$. Ausserdem gilt in jedem Graphen $\chi \geq \frac{n}{\alpha}$. Aus diesen beiden folgt eben $\alpha \geq \frac{n}{4}$. Ein Beispiel, wo hier Gleichheit steht, ist K_4 (wegen $n = 4$ und $\alpha = 1$).

3 Zahlentheorie

3.1 Teilbarkeit

3.1.1.
a) $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1})$
b) $a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - + \ldots - ab^{2k-1} + b^{2k})$
c) $1 + 2$ ist kein Teiler von $1^2 + 2^2$.

3.1.2. Sei n die kleinste solche Zahl. In kanonischer Form:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

Dann gilt:

$$3 \cdot 5 = 15 = d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

Es kommen also nur Zahlen der Form p^{14} und p^2q^4 in Frage, wobei p und q verschiedene Primzahlen sind, $p \neq 3$, $q \neq 3$. Die kleinste solche Zahl ist $2^4 5^2$.

3.1.3. Es soll bewiesen werden, dass der grösste gemeinsame Teiler des Zählers und des Nenners für jeden Wert von n gleich 1 ist. Sei x der Zähler und y der Nenner, $d = (x, y)$. Daraus folgt:

$$d \mid y - nx = n^2 + 1 =: z$$

Daraus folgt wiederum

$$d \mid x - nz = n^3 + 2n - n(n^2 + 1) = n$$

Es ergibt sich

$$d \mid z - n^2 = 1$$

also kann d nur 1 sein.

3.1.4. Wegen $1998 = 37 \cdot 54$ gilt, dass $2^{1998} - 1 = (2^{37})^{54} - 1^{54}$. Aufgabe **3.1.1.** a) mit $a = 2^{37}$, $b = 1$ und $k = 54$ liefert eben die gewünschte Behauptung.

3.1.5. $1998 = 2 \cdot 3^3 \cdot 37$. Damit der grösste gemeinsame Teiler 9 ist und das kleinste gemeinsame Vielfache mit 27 teilbar ist, muss eine der Zahlen mit 9 (aber nicht mit 27), die andere mit 27 (aber nicht mit 81) teilbar sein. Bezeichne a jene Zahl, die nur mit 9 teilbar ist und b die andere, die auch mit 27 teilbar ist.
Damit das kleinste gemeinsame Vielfache 1998 wird, muss man noch ein Faktor 2 und ein Faktor 37 zwischen a und b verteilen. Dafür hat man 4 Möglichkeiten:

$$a = 9,\ b = 27 \cdot 2 \cdot 37$$

$$a = 9 \cdot 2,\ b = 27 \cdot 37$$

$$a = 9 \cdot 37,\ b = 27 \cdot 2$$

$$a = 9 \cdot 2 \cdot 37,\ b = 27$$

3.1.6. Die letzte Ziffer der Potenzen von 23 hat eine Periode der Länge 4:

$$3 \to 9 \to 7 \to 1 \to 3 \to \dots$$

Deswegen muss man untersuchen, welchen Rest 15^{23} gibt, falls es mit 4 dividiert wird.
Der Rest der Potenzen von 15 hat eine Periode der Länge 2:

$$3 \to 1 \to 3 \to \dots$$

Da 23 ungerade ist, bedeutet das, dass der Rest von 15^{23} gleich 3 ist, wenn es mit 4 dividiert wird, und somit ist die letzte Ziffer von $23^{15^{23}}$ gleich 7.
(Im Kapitel *Kongruenzen* wird eine allgemeinere Methode für die Lösung solcher Probleme dargestellt.)

3.1.7. Wenn das in x Jahren passiert, bedeutet es:

$$37 + x \mid 1998 + x$$

also kann man folgende Gleichung aufstellen:

$$1998 + x = y(37 + x)$$

wobei x und y positive ganze Zahlen sind. Diese Gleichung kann so umgeformt werden:

$$(x + 37)(y - 1) = 1961$$

Das ergibt die folgende, einzig vorstellbare Lösung:

$$x + 37 = 53,\ y - 1 = 37$$

Also wird das in $x = 16$ Jahren wieder vorkommen.

3.1.8. Nie. Wenn n gerade ist ($n = 2k$), dann folgt aus **3.1.1.** a), dass $3^{2k} - 1 = 9^k - 1$ mit $9 - 1 = 8$ teilbar ist, also kann $3^{2k} + 1$ mit 8 nicht teilbar sein.
Wenn $n = 2k + 1$, dann ist $3^n + 1 = 3 \cdot 3^{2k} + 1$. Eben wurde eingesehen, dass 3^{2k} den Rest 1 hat, wenn es mit 8 geteilt wird, also hat $3^n + 1$ den Rest 4.

3.1.9.

$$3^{2n+1} + 2^{n+2} = 3 \cdot 9^n + 4 \cdot 2^n = 3 \cdot 9^n - 3 \cdot 2^n + 3 \cdot 2^n + 4 \cdot 2^n = 3 \cdot (9^n - 2^n) + 7 \cdot 2^n$$

Sowohl $3 \cdot (9^n - 2^n)$ als auch $7 \cdot 2^n$ ist mit 7 teilbar. (Dass $9^n - 2^n$ mit 7 teilbar ist, folgt aus Aufgabe **3.1.1.** a.)

3.2 Kongruenzen

3.2.1. a) Man soll die letzten 2 Ziffern bestimmen, also ist die folgende Kongruenz zu lösen:

$$1997^{7^{2000}} \equiv x \pmod{100}$$

$(1997, 100) = 1$, also ist wegen des Euler-Fermatschen Satzes

$$1997^{\varphi(100)} = 1997^{40} \equiv 1 \pmod{100}$$

und ähnlicherweise

$$1997^{40u+v} = (1997^{40})^u \cdot 1997^v \equiv 1^u \cdot 1997^v = 1997^v \pmod{100}$$

gültig. (Also zählt nur der Rest der Potenz modulo 40.) Wenn man also die Kongruenz

$$7^{2000} \equiv y \pmod{40} \tag{2}$$

löst, dann gilt, dass

$$x \equiv 1997^y \pmod{100}$$

Mit der gleichen Idee kann man das Lösen von (2) vereinfachen, und zuerst die Kongruenz

$$2000 \equiv z \pmod{\varphi(40)}$$

lösen. Da $\varphi(40) = 16$ ist, folgt sofort, dass

$$z = 0 \implies y \equiv 7^z = 1 \pmod{40} \implies x \equiv 1997^y = 1997 \equiv 97 \pmod{100}$$

Die gesuchten Ziffern sind also 97.

b) Man soll mit der Methode von Punkt a) vorgehen. Die Aufgabe ist,

$$57^{67^{79}} \equiv x \pmod{100}$$

zu lösen. Dazu braucht man y und z aus

$$67^{79} \equiv y \pmod{40}$$

und

$$79 \equiv z \pmod{16}$$

zu bestimmen. (Benutzt wird, dass $(57, 100) = 1$ und $(67, 40) = 1$.) Es ist einfach zu sehen, dass $z = -1$. Dann ist

$$y = 67^{-1} \pmod{40}$$

das heisst, dass

$$67y \equiv 1 \pmod{40}$$

Wegen $67 \cdot 3 = 201 \equiv 1 \pmod{40}$ ist $y = 3$. (Da $(67, 40) = 1$, weitere Lösungen sind nicht möglich.) Daraus folgt

$$x \equiv 57^y = 57^3 = 185193 \equiv 93 \pmod{100}$$

Die Lösung ist also 93.

3.2.2. Bei einer "normalen" Gleichung würde man mit 2 dividieren. Ähnlicherweise sucht man auch hier das Invers von 2, um damit multiplizieren zu können.
$\varphi(21) = 12$. Da 2 und 21 teilerfremd sind, erhält man aus dem Euler-Fermatschen Satz:

$$2^{12} \equiv 1 \pmod{21}$$

Wenn man also die ursprüngliche Kongruenz mit 2^{11} multipliziert, erhält man

$$x \equiv 9 \cdot 2^{11} = 9 \cdot 2048 \equiv 9 \cdot 11 = 99 \equiv 15 \pmod{21}$$

(Dieses Verfahren gibt eine allgemeine Methode, solche Kongruenzen zu lösen. In den einzelnen Fällen kann man natürlich einfacher vorgehen. Z. B. in dieser Aufgabe kann man die Kongruenz mit 11 multiplizieren, und das Ergebnis folgt sofort.)

3.2.3. a) Aus der zweiten Kongruenz erhält man

$$1 \equiv 4x \equiv x \pmod{3}$$

Deswegen kann x in die Form

$$x = 3y + 1 \tag{3}$$

geschrieben werden. Das wird in die erste Kongruenz substituiert:

$$\begin{aligned} 5 \cdot (3y + 1) &\equiv 3 \pmod{7} \\ y \equiv 15y &\equiv -2 \pmod{7} \end{aligned}$$

$$\Longrightarrow y = 7z - 2$$

Mit Hilfe von (3) bekommt man

$$x = 3 \cdot (7z - 2) + 1 = 21z - 5 \Longrightarrow x \equiv -5 \pmod{21}$$

Eine Restklasse modulo 21 bildet also die Lösung.

b) Aus der ertsen Kongruenz wird x ausgedrückt

$$\begin{aligned} 6x &\equiv 4 \pmod{11} \\ x \equiv 12x &\equiv 8 \pmod{11} \end{aligned}$$

$$x = 11y + 8 \tag{4}$$

Die zweite Kongruenz sieht also folgenderweise aus

$$\begin{aligned} 5 \cdot (11y + 8) &\equiv 2 \pmod{6} \\ y \equiv 55y &\equiv -38 \equiv 4 \pmod{6} \end{aligned}$$

$$\Longrightarrow y = 6z + 4$$

Aus (4) erhält man

$$x = 11 \cdot (6z + 4) + 8 = 66z + 52 \Longrightarrow x \equiv 52 \pmod{66}$$

3.2.4. Selbstverständlich wird die Lösung eine Restklasse modulo 5 sein, also reicht es, nur $x \in \{0, 1, 2, 3, 4\}$ zu betrachten. Die 0 ist natürlich keine Lösung, also ist $(x, 5) = 1$. Aus dem Fermatschen Satz folgt nun, dass

$$x^4 \equiv 1 \pmod{5}$$

also

$$x^{4u+v} = (x^4)^u \cdot x^v \equiv 1^u \cdot x^v = x^v \pmod 5$$

Daraus folgt, dass

$$x^{1999} \equiv x^3 \pmod 5$$
$$x^{1998} \equiv x^2 \pmod 5$$
$$x^{1997} \equiv x^1 \pmod 5$$

Also bekommt die Gleichung die Form

$$x^3 + x^2 + x + 1 \equiv 0 \pmod 5$$

Man kann jetzt manuell die 4 Möglichkeiten ausprobieren, und so ergibt sich, dass

$$\begin{array}{rcll} x & \equiv & 2 \pmod 5 & \text{oder} \\ x & \equiv & 3 \pmod 5 & \text{oder} \\ x & \equiv & 4 \pmod 5 & \end{array}$$

3.2.5. Da $p \mid 10n - 1$, so gilt $(p, 10) = 1$. Aus dem Fermatschen Satz folgt also

$$10^{p-1} \equiv 1 \pmod p$$

Ausserdem

$$p \mid 10n - 1 \Longrightarrow 10n \equiv 1 \pmod p$$

Aus den letzten zwei Kongruenzen erhält man, dass

$$10^{p-1} \equiv 10n \pmod p$$

Nach der Division mit 10 (wegen $(p, 10) = 1$ bleibt der Modulus p):

$$10^{p-2} \equiv n \pmod p$$

was eben die Behauptung war.

3.2.6. Da m eine zusammengesetzte Zahl ist, kann es als ein Produkt aufgeschrieben werden:

$$m = ab, \quad 1 < a < m,\ 1 < b < m$$

Wenn $a \neq b$, dann ist sowohl a als auch b unter den Zahlen

$$1, 2, \ldots, m - 1$$

enthalten, also ist $(m-1)!$ mit m teilbar, was zu beweisen war.
Wenn $a = b$, dann ist $m = a^2$ und wegen $m > 4$ gilt $a > 2$, also $2a < m$. Deswegen ist sowohl a als auch $2a$ unter den Zahlen

$$1, 2, \ldots, m - 1$$

enthalten, also ist $(m-1)!$ mit $m = a^2$ teilbar.

3.2.7. p sei eine Primzahl. Dann ist

$$1, 2, \ldots, p-1$$

ein reduziertes System von Restklassen. Wenn $(a, p) = 1$ gilt, dann ist

$$1a, 2a, \ldots, (p-1)a$$

auch ein reduziertes System von Restklassen. Also enthalten die beiden Systeme die gleichen Restklassen. Daraus folgt speziell, dass

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1a \cdot 2a \cdot \ldots \cdot (p-1)a \pmod{p}$$

Also

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$$

Wegen

$$(p, (p-1)!) = 1$$

kann man mit $(p-1)!$ dividieren und so erhält man

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

3.3 Zahlentheoretische Algorithmen

3.3.1. a)

$$\begin{aligned} 1275 &= 2 \cdot 442 + 391 \\ 442 &= 1 \cdot 391 + 51 \\ 391 &= 7 \cdot 51 + 34 \\ 51 &= 1 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

Also $(1275, 442) = 17$.

b)

$$\begin{aligned} 2x^3 - x^2 + x + 1 &= (x+2) \cdot (2x^2 - 5x - 3) + 14x + 7 \\ 2x^2 - 5x - 3 &= \left(\frac{1}{7}x - \frac{3}{7}\right) \cdot (14x + 7) + 0 \end{aligned}$$

Also $(2x^3 - x^2 + x + 1, 2x^2 - 5x - 3) = 14x + 7$. (Oder $c \cdot (14x + 7)$, wo c eine beliebige reelle Konstante sein kann.)

3.3.2. Wenn man den grössten gemeinsamen Teiler von 1 und a $(a > 1)$ bestimmen möchte, läuft der Algorithmus wie folgt:

$$(a, 1) = (a-1, 1) = (a-2, 1) = \ldots = (1, 1) = 1$$

Das sind insgesamt a Schritte. Die Länge der Eingabe ist $\lceil \log a \rceil$, also ist die Anzahl der Schritte eine exponentielle Funktion der Länge der Eingabe. Daraus folgt, dass der Algorithmus nicht in Polinomzeit arbeitet. (Es ist natürlich möglich, dass der Algorithmus für manche Eingaben schnell ist, aber im schlimmsten Fall dauert er exponentiell lang.)

3.3.3. Da p und q verschiedene Primzahlen sind, gilt $(p, q) = 1$. Aus dem euklidischen Algorithmus folgt die Existenz von k und l mit $pk + ql = 1$. Hier muss aber entweder k oder l negativ sein. Z. B. sei $l < 0$. Dann erfüllen k und $n := -l$ die gewünschte Eigenschaft: $pk - qn = 1$ also $pk = qn + 1$.

3.3.4. $m = pq = 77$, $\varphi(m) = (p-1)(q-1) = 60$. Der öffentliche Schlüssel muss zu 60 teilerfremd sein; die kleinste solche Zahl ist $e = 7$. Der geheime Schlüssel ist sein Invers modulo 60; das ist $d = 43$, da $7 \cdot 43 = 301 \equiv 1 \pmod{60}$.
Kodierung der Nachricht:

$$y = x^e = 2^7 = 128 \equiv -26 \pmod{77}$$

Dekodierung:

$$y^d = (-26)^{43} \equiv ? \pmod{77}$$

Das kann man folgenderweise berechnen:

$$\begin{aligned}
(-26)^1 &= -26 \\
(-26)^2 &= 676 \equiv -17 \pmod{77} \\
(-26)^4 &= ((-26)^2)^2 \equiv (-17)^2 = 289 \equiv -19 \pmod{77} \\
(-26)^8 &= ((-26)^4)^2 \equiv (-19)^2 = 361 \equiv -24 \pmod{77} \\
(-26)^{16} &= ((-26)^8)^2 \equiv (-24)^2 = 576 \equiv 37 \pmod{77} \\
(-26)^{32} &= ((-26)^{16})^2 \equiv 37^2 = 1369 \equiv -17 \pmod{77}
\end{aligned}$$

Da $43 = 32 + 8 + 2 + 1$, so gilt

$$\begin{aligned}
(-26)^{43} &= (-26)^{32}(-26)^8(-26)^2(-26)^1 \equiv (-17)(-24)(-17)(-26) \equiv \\
&\equiv (-19)(-24)(-26) \equiv (-6)(-26) \equiv 2 \pmod{77}
\end{aligned}$$

und somit haben wir die originale Nachricht zurückbekommen.

3.3.5.
a) Man soll beweisen, dass

$$n \mid x^{r\varphi(n)+1} - x$$

Es reicht natürlich zu beweisen, dass für alle p_i-s

$$p_i \mid x^{r\varphi(n)+1} - x$$

oder:

$$x^{r\varphi(n)+1} \equiv x \pmod{p_i}$$

Falls $p_i \mid x$, dann wird das trivialerweise erfüllt. Sonst kann man den kleinen Satz von Fermat benutzen, und es ergibt sich

$$x^{p_i - 1} \equiv 1 \pmod{p_i}$$

Andererseits ist

$$\varphi(n) = (p_1 - 1) \cdot \ldots \cdot (p_k - 1)$$

also

$$p_i - 1 \mid \varphi(n)$$

und auch

$$p_i - 1 \mid r\varphi(n)$$

Es folgt:

$$x^{r\varphi(n)} \equiv 1 \pmod{p_i}$$

also

$$x^{r\varphi(n)+1} \equiv x \pmod{p_i}$$

was eben zu beweisen war.
b) Sei z. B. $n = 9$, $x = 3$, $r = 1$. $\varphi(9) = 6$.

$$x^{r\varphi(n)+1} = 3^7 = 9 \cdot 3^5 \equiv 0 \not\equiv 3 \pmod{9}$$

3.3.6. Da man mit k Tests eine Gewissheit von $1 - 2^{-k}$ erreichen kann, braucht man 4 Tests, um die Gewissheit von mindestens 90% garantieren zu können.
Man wähle also 4 zufällige Zahlen aus $1 \ldots 16$, z. B.: 9, 2, 5 und 12.

$$\begin{aligned}
9^{16} &= 81^8 \equiv (-4)^8 = 16^4 \equiv (-1)^4 = 1 \pmod{17} \\
2^{16} &= 4^8 = 16^4 \equiv (-1)^4 = 1 \pmod{17} \\
5^{16} &= 25^8 \equiv 8^8 = 64^4 \equiv (-4)^4 = 16^2 \equiv (-1)^2 = 1 \pmod{17} \\
12^{16} &\equiv (-4)^{16} = 16^8 \equiv (-1)^8 = 1 \pmod{17}
\end{aligned}$$

Also kann man mit einer Gewissheit von über 90% behaupten, dass 17 eine Primzahl ist.

3.3.7. Man soll beweisen, dass für jedes x, das zu n teilerfremd ist:

$$n \mid x^{n-1} - 1$$

Dazu reicht natürlich zu beweisen, dass

$$\forall p_i : \quad p_i \mid x^{n-1} - 1$$

also

$$x^{n-1} \equiv 1 \pmod{p_i} \tag{5}$$

Da x und n teilerfremd sind, ist x mit p_i nicht teilbar, also gilt wegen dem kleinen Satz von Fermat:

$$x^{p_i-1} \equiv 1 \pmod{p_i}$$

und daraus folgt wegen $p_i - 1 \mid n - 1$ eben (5).

3.3.8. Nehmen wir als Testzahl $x = 2$:

$$2^{560} - 1 = (2^{280} + 1)(2^{280} - 1) = (2^{280} + 1)(2^{140} + 1)(2^{140} - 1) =$$

$$= (2^{280}+1)(2^{140}+1)(2^{70}+1)(2^{70}-1) =$$
$$= (2^{280}+1)(2^{140}+1)(2^{70}+1)(2^{35}+1)(2^{35}-1)$$

Nun soll man die Potenzen von 2 modulo 561 bestimmen:

$$2^1 = 2$$
$$2^2 = 4$$
$$2^4 = 16$$
$$2^8 = 256$$
$$2^{16} = 65536 \equiv -101$$
$$2^{32} \equiv (-101)^2 = 10201 \equiv 103$$
$$2^{35} = 2^{32}2^3 \equiv 103 \cdot 8 = 824 \equiv 263$$
$$2^{70} \equiv 263^2 = 69169 \equiv 166$$
$$2^{140} \equiv 166^2 = 27556 \equiv 67$$
$$2^{280} \equiv 67^2 = 4489 \equiv 1$$

Weder $2^{35}-1$, noch $2^{35}+1$, $2^{70}+1$, $2^{140}+1$ oder $2^{280}+1$ ist kongruent zu 0, also ist 561 keine Primzahl.
(Bemerkung: man sieht auch, dass der Fermat-Test das nicht detektieren würde, weil $2^{560}-1 = (2^{280}+1)(2^{280}-1) \equiv 2 \cdot 0 = 0$. Der Grund ist, dass $2^{140}+1$ und $2^{140}-1$ Nullteiler sind: sie sind zwar nicht 0, ihr Produkt ist aber schon 0. Daraus folgt natürlich auch, dass 561 keine Primzahl ist.)

3.4 Weitere Aufgaben

3.4.1. a)
Wenn $n \equiv 0 \pmod 3$, dann ist $n^2 \equiv 0 \pmod 3$.
Wenn $n \equiv 1 \pmod 3$, dann ist $n^2 \equiv 1 \pmod 3$.
Wenn $n \equiv 2 \pmod 3$, dann ist auch $n^2 \equiv 1 \pmod 3$.
Also ist das Ergebnis entweder 0 oder 1.

b) Mit demselben Gedankengang: 0 oder 1.

c) Mit demselben Gedankengang: 0, 1 oder 4.

3.4.2. Wenn man versucht, $\frac{1}{3}$ als Summe von Potenzen von 2 aufzuschreiben, sieht man, dass dabei die Zahlen

$$\frac{1}{4},\ \frac{1}{16},\ \frac{1}{64},\ \dots$$

benutzt werden. In der Tat, wenn man die Summe

$$\sum_1^\infty \left(\frac{1}{4}\right)^k = \frac{1}{4} \cdot \frac{1}{1-\frac{1}{4}} = \frac{1}{4} \cdot \frac{4}{3} = \frac{1}{3}$$

bildet, erhält man $\frac{1}{3}$. Also ist die Lösung

$$\frac{1}{3} = 0,01010101...$$

3.4.3. Sei $n = 2^k \cdot m$, wo $2 \nmid m$. Dann gilt wegen der Multiplikativität von d, dass

$$d(n) = (k+1) \cdot d(m)$$

und

$$d(2n) = (k+2) \cdot d(m)$$

also

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

Es wurde angenommen, dass

$$d(2n) = \frac{3}{2} \cdot d(n)$$

daraus folgt, dass

$$\frac{k+2}{k+1} = \frac{3}{2} \Longrightarrow k = 1$$

Das bedeutet, dass genau jene Zahlen, die mit 2 teilbar sind, aber mit 4 nicht, eine Lösung der Aufgabe sind:

$$n \equiv 2 \pmod 4$$

3.4.4. Es soll bewiesen werden, dass $2^n + 1$ keine Primzahl sein kann, wenn n keine Potenz von 2 ist.
Wenn n keine Potenz von 2 ist, dann hat n (mindestens) einen ungeraden Teiler, der grösser als 1 ist:

$$n = m(2l+1) \quad (l > 0)$$

Dann gilt aber (siehe Aufgabe **3.1.1.**b))

$$2^m + 1 \mid (2^m)^{2l+1} + 1^{2l+1} = 2^n + 1$$

also ist $2^n + 1$ mit $2^m + 1$ teilbar. $2^m + 1$ ist auf jeden Fall grösser als 1, und wegen

$$n = m(2l+1) > m$$

ist $2^m + 1$ kleiner als $2^n + 1$. Daraus folgt, dass $2^m + 1$ ein echter Teiler von $2^n + 1$ ist, also kann $2^n + 1$ keine Primzahl sein.
(Es wurde natürlich nicht behauptet, dass jede Zahl, die die Form $2^{2^k} + 1$ hat, eine Primzahl wäre. Siehe dazu auch Aufgabe **3.4.5.**! Auf jeden Fall werden Primzahlen dieser Form Fermatsche Primzahlen genannt.)

3.4.5. Es wird gezeigt, dass $641 \mid 2^{32} + 1$.
$641 = 2^4 + 5^4 \implies 2^4 \equiv -5^4 \pmod{641}$
$641 = 5 \cdot 2^7 + 1 \implies 5 \cdot 2^7 \equiv -1 \pmod{641}$
$2^{32} + 1 \equiv 2^4 \cdot 2^{28} + 1 \equiv -5^4 \cdot 2^{28} + 1 \equiv -(5 \cdot 2^7)^4 + 1 \equiv -(-1)^4 + 1 \equiv -1 + 1 \equiv 0 \pmod{641}$
Also ist $2^{32} + 1$ wirklich teilbar mit 641.

3.4.6.
Lösung 1:
Wenn man indirekt annimmt, dass die Behauptung falsch ist, kann man das kleinste Gegenbeispiel betrachten. Darunter wird in diesem Fall ein solches Gegenbeispiel (also ein solches

(a, b, n)-Tupel) verstanden, wo n minimal ist. (Gibt es mehrere solche Tupeln, so nimmt man ein beliebiges.) Es sei also (a_1, b_1, n_1) ein minimales Gegenbeispiel. Wenn a_1 gleich 1 ist, ist die Behauptung trivialerweise erfüllt, also kann dieses Tupel kein Gegenbeispiel sein. Sonst hat a_1 (mindestens) einen Primteiler: p. Es folgt

$$p \mid a_1 \implies p \mid n_1^2 \implies p \mid n_1 \implies p^2 \mid n_1^2 \implies p^2 \mid a_1 \cdot b_1 \implies p^2 \mid a_1$$

(Bei der letzten Folgerung wurde benutzt, dass a_1 und b_1 teilerfremd sind, dass also p kein Teiler von b_1 sein kann.)
Also $a_1 = p^2 \cdot a_2$, $n_1 = p \cdot n_2$. Es sei $b_2 = b_1$. Es ist trivial, dass $(a_2, b_2) = 1$, $a_2 \cdot b_2 = n_2^2$, (a_2, b_2, n_2) ist auch ein Gegenbeispiel (wenn nämlich $a_2 = u^2$ und $b_2 = v^2$ wäre, dann wäre $a_1 = (pu)^2$, $b_1 = v^2$ und damit auch kein Gegenbeispiel) und $n_2 < n_1$, also ist (a_2, b_2, n_2) ein kleineres Gegenbeispiel, was ein Widerspruch ist.

Lösung 2:
Eine Zahl ist genau dann ein Quadrat, wenn alle seiner Primfaktore mit einem geraden Exponent in der kanonischen Form vorkommen. Wenn man indirekt annimmt, dass z. B. a diese Eigenschaft nicht erfüllt, das bedeutet, dass a z. B. mit p^{2k+1} teilbar ist, aber mit p^{2k+2} nicht. Das heisst aber auch, dass n^2 mit p^{2k+2} teilbar sein muss (in der kanonischen Form von n^2 kommen ja alle Primfaktore mit einem geraden Exponent vor), und daraus folgt, dass b auch mit p teilbar ist. Aber das ist ein Widerspruch, da a und b teilerfremd sind.

3.4.7. Zuerst wird gezeigt, dass x, y und z, wenn sie die Form

$$x = d(n^2 - m^2),\ y = 2dnm,\ z = d(n^2 + m^2)$$

haben, die Gleichung

$$x^2 + y^2 = z^2 \tag{6}$$

erfüllen. (Der andere Fall, in dem die Rollen von x und y verkehrt sind, ist genauso zu behandeln.) In der Tat:

$$x^2 + y^2 = d^2(n^2 - m^2)^2 + 4d^2n^2m^2 = d^2(n^4 - 2n^2m^2 + m^4 + 4n^2m^2) = d^2(n^2 + m^2)^2 = z^2$$

Nun wird die andere Richtung bewiesen. Man betrachte die sogenannten primitive Lösungen von (6), das heisst: solche (x, y, z)-Tupel, die als grössten gemeinsamen Teiler 1 haben. (Das bedeutet auch, dass sie paarweise teilerfremd sind, weil ein Teiler von zwei der Variablen automatisch auch ein Teiler des dritten wäre: wenn zum Beispiel sowohl x als auch z mit k teilbar wäre, würde das bedeuten, dass $y^2 = z^2 - x^2$ mit k^2 teilbar wäre, y wäre also auch mit k teilbar.) Die allgemeine Lösung kann man erhalten, in dem man alle Variablen einer primitiven Lösung mit einer Konstante d multipliziert. (Man kann nämlich aus einer beliebigen Lösung die zugehörige primitive Lösung erhalten, in dem man alle drei Zahlen mit ihrem grössten gemeinsamen Teiler dividiert.)
In einer primitiven Lösung können x und y nicht beide gerade Zahlen sein, weil sie teilerfremd sind. Es ist auch nicht möglich, dass sie beide ungerade wären, denn in diesem Fall wäre

$$x^2 \equiv 1 \pmod 4, \quad y^2 \equiv 1 \pmod 4 \implies z^2 \equiv 2 \pmod 4$$

was unmöglich ist, da das Quadrat einer natürlichen Zahl entweder die Form $4k$ oder $4k + 1$ hat. (Siehe Aufgabe **3.4.1.** b).) Also ist einer von x und y gerade, der andere ungerade. Da

ihre Rollen symmetrisch sind, kann man annehmen, dass x ungerade und y gerade ist. Dann ist z natürlich auch ungerade. Wenn man nun (6) etwas umformt und mit 4 dividiert, erhält man

$$\left(\frac{y}{2}\right)^2 = \frac{1}{4} \cdot (z^2 - x^2) = \frac{z+x}{2} \cdot \frac{z-x}{2}$$

Mit

$$t = \frac{y}{2},\ a = \frac{z+x}{2},\ b = \frac{z-x}{2}$$

erhält man

$$t^2 = ab$$

wo a, b und t ganze Zahlen sind. Dabei ist $(a, b) = 1$. Wenn nämlich d ein gemeinsamer Teiler von a und b wäre, dann wäre d auch ein Teiler von $a + b = z$ und $a - b = x$, aber $(x, z) = 1$. Das bedeutet also, dass a, b und t die Bedingungen der Aufgabe **3.4.6.** erfüllen. Also gilt:

$$a = n^2,\ b = m^2$$

Wenn man das in die Definition von a und b einschreibt, erhält man:

$$\frac{z+x}{2} = n^2,\ \frac{z-x}{2} = m^2$$

woraus sich eben

$$x = n^2 - m^2,\ z = n^2 + m^2$$

ergibt. Wegen

$$\frac{y}{2} = t = nm$$

erhält man ausserdem

$$y = 2nm$$

was eben zu beweisen war. Es ist auch klar, dass $(n, m) = 1$ und $n > m$. Da $z = n^2 + m^2$ ungerade ist, gilt ausserdem $2 \nmid n - m$.
(Das ist also die Form einer primitiven Lösung. Um die allgemeine Lösung zu erhalten, muss man x, y und z mit derselben — mit d bezeichneten — Zahl multiplizieren.)

3.4.8. Wenn (x, y, z) eine Lösung der Gleichung

$$x^2 + y^2 = z^2$$

ist, dann gilt laut Aufgabe **3.4.7.**:

$$x = d(n^2 - m^2),\ y = 2dnm,\ z = d(n^2 + m^2)$$

wobei $2 \nmid n - m$. (Oder die Rolle von x und y ist umgekehrt, aber das ist egal wegen ihrer Symmetrie.) Es soll bewiesen werden, dass xyz mit 3, 4 und 5 teilbar ist.
Wenn entweder n oder m mit 3 teilbar ist, dann ist auch $y = 2nm$ und damit auch xyz mit 3 teilbar. Sonst, d. h. wenn weder n noch m mit 3 teilbar ist, dann folgt

$$n^2 \equiv m^2 \equiv 1 \pmod 3$$

(siehe Aufgabe **3.4.1.** a).) Daraus folgt, dass $x = d(n^2 - m^2)$ und damit auch xyz mit 3 teilbar ist.

Da entweder n oder m gerade ist, ist $y = 2dnm$ und damit auch xyz mit 4 teilbar.
Wenn entweder n oder m mit 5 teilbar ist, dann ist auch $y = 2nm$ und damit auch xyz mit 5 teilbar. Sonst, d. h. wenn weder n noch m mit 5 teilbar ist, dann ist sowohl n^2 als auch m^2 kongruent zu entweder 1 oder 4 modulo 5 (siehe Aufgabe **3.4.1.** c)). Wenn sie zueinander kongruent sind, dann ist $x = d(n^2 - m^2)$ teilbar mit 5. Wenn sie nicht zueinander kongruent sind, dann ist aber ihre Summe und damit auch $z = d(n^2 + m^2)$ mit 5 teilbar.

4 Algebra

4.1 Elementare Gruppentheorie

4.1.1. Da $abb^{-1}a^{-1} = e$, ist das Invers von ab eben $b^{-1}a^{-1}$.

4.1.2. Ja. Man multipliziere beide Seiten der Gleichung von links zuerst mit a^{-1}, dann mit b^{-1}. So erhält man, dass $x = y$.
Bemerkung: man könnte erwidern, dass bei reellen Zahlen zum Beispiel aus $0 \cdot x = 0 \cdot y$ nicht $x = y$ folgt. Aber das ist kein Gegenbeispiel, denn die multiplikative Gruppe der reellen Zahlen enthält die 0 nicht.

4.1.3. Allgemein stimmt das nicht. (In einigen speziellen Fällen, wie z. B. in kommutativen Gruppen, natürlich ja.) Beispiel: man nehme die Diedergruppe D_3, c sei eine Spiegelung, x die Drehung um $\frac{2\pi}{3}$, y die Drehung um $\frac{4\pi}{3}$. Dann ist zwar $xc = cy$, aber x und y sind verschieden.

4.1.4.
a) Die Operation führt aus der Menge der reellen Vektoren der Länge n aus, da das Ergebnis des Skalarprodukts eine reele Zahl ist.
b) Die Operation führt nicht aus der Menge der ganzen Zahlen aus.
Assoziativität:

$$(x * y) * z = x * (y * z)$$

soll gelten. Das heisst:

$$(x + y + 1) + z + 1 = x + (y + z + 1) + 1 \quad \Rightarrow \quad \text{assoziativ}$$

Neutrales Element:

$$\forall x \quad e * x = x$$

soll gelten. Das heisst:

$$(e + x + 1) = x \quad \Rightarrow \quad e = -1$$

Invers:

$$\forall x \; \exists x^{-1} \quad x * x^{-1} = e$$

soll gelten. Das heisst:

$$x + x^{-1} + 1 = -1 \quad \Rightarrow \quad x^{-1} = x - 2$$

Kommutativität:

$$x * y = y * x$$

soll gelten. Das heisst:

$$x + y + 1 = y + x + 1 \quad \Rightarrow \quad \text{kommutativ}$$

Also es ist eine kommutative Gruppe mit $e = -1$.
c) Nicht assoziativ (z. B. $| \, |1+1|+(-2) \, | = | \, 1+|1+(-2)| \, |$ stimmt nicht), also weder Gruppe noch Halbgruppe.
d) Die Operation führt nicht aus der Menge der positiven reellen Zahlen aus.
Assoziativität:

$$\frac{\frac{xy}{x+y+1} \cdot z}{\frac{xy}{x+y+1} + z + 1} = \frac{x \cdot \frac{yz}{y+z+1}}{x + \frac{yz}{y+z+1} + 1}$$

Nach einigen Vereinfachungen erhält man:

$$\frac{xyz}{xy + xz + yz + z + x + y + 1} = \frac{xyz}{xy + xz + x + yz + y + z + 1}$$

Also ist die Operation assoziativ.
Neutrales Element:

$$\forall x \quad \frac{xe}{x + e + 1} = x$$

soll gelten. Diese Gleichung kann für e unabhängig von x nicht gelöst werden, also gibt es kein neutrales Element. So folgt, dass es eine Halbgruppe ist.
Kommutativität ist trivial, also es ist eine kommutative Halbgruppe ohne neutrales Element.

4.1.5. Sei $[o(a), o(b)] = k$. Die Aufgabe ist zu beweisen, dass $o(ab) \mid k$. Es ist genug zu zeigen, dass $(ab)^k = e$. In einer kommutativen Gruppe gilt $(ab)^k = a^k \cdot b^k$. Da $o(a) \mid k$ und $o(b) \mid k$, so folgt, dass $a^k = e$ und $b^k = e$. Zusammenfassend:

$$(ab)^k = a^k \cdot b^k = e \cdot e = e$$

Damit wurde die Behauptung bewiesen.

4.1.6. Da die Gruppe mindestens 2 Elemente hat, können wir ein Element x wählen, so dass $x \neq e$. Wenn $o(x)$ eine Primzahl ist, dann sind wir fertig. Sonst sei $o(x) = pq$, wobei p eine Primzahl ist. Dann gilt aber $o(x^q) = p$.

4.1.7. Aus $x^2 = e$ folgt, dass $x = x^{-1}$. Weiterhin gilt:

$$y = xy^3x^{-1} = x^{-1}y^3x = x^{-1} \cdot y \cdot y \cdot y \cdot x = x^{-1} \cdot xy^3x^{-1} \cdot xy^3x^{-1} \cdot xy^3x^{-1} \cdot x = y^9 \quad \Rightarrow \quad y^8 = e$$

Genau das war zu beweisen.

4.1.8. x und y seien beliebige Elemente aus G. Da $o(x) = 2$, gilt $x^{-1} = x$, ähnlicherweise $y^{-1} = y$ und $(xy)^{-1} = xy$. Andererseits ist $(xy)^{-1} = y^{-1}x^{-1} = yx$ (siehe Aufgabe **4.1.1.**). Daraus folgt $xy = yx$, also ist G kommutativ.

4.1.9. Ja, z. B. die Transformationsgruppe des Kreises beinhaltet für jede natürliche Zahl k die Drehung um $\frac{2\pi}{k}$, die Ordnung k hat.

4.1.10. Sei x ein beliebiges Element von G, $k = o(x)$. $(x^{-1})^k = (x^k)^{-1} = e^{-1} = e$, also gilt: $o(x^{-1}) \leq k = o(x)$.
Wenn man denselben Gedankengang für x^{-1} statt x benutzt, erhält man: $o(x) \leq o(x^{-1})$. Aus den beiden Ungleichungen folgt eben $o(x) = o(x^{-1})$.

4.2 Untergruppen, Nebenklassen, Normalteiler

4.2.1. Da $e \in H$, $g^{-1}eg = e$ ist auch ein Element von H^*.
Wenn x^* und y^* zwei Elemente von H^* sind, dann haben sie die Form $x^* = g^{-1}xg$, $y^* = g^{-1}yg$, wobei x und y Elemente aus H sind. Daraus folgt, dass xy auch ein Element von H ist, also gilt $g^{-1}xyg \in H^*$. Andererseits ist das eben

$$g^{-1}xyg = g^{-1}xgg^{-1}yg = x^*y^*$$

also ist H^* geschlossen bezüglich Multiplikation.
Aus $x \in H$ folgt auch $x^{-1} \in H$ und dadurch $g^{-1}x^{-1}g \in H^*$. Das ist aber wegen

$$x^*(g^{-1}x^{-1}g) = g^{-1}xgg^{-1}x^{-1}g = g^{-1}xx^{-1}g = g^{-1}g = e$$

genau $(x^*)^{-1}$, also ist H^* geschlossen bezüglich Inversbildung. Also ist H^* eine Untergruppe.
Wenn H ein Normalteiler ist, dann ist $H^* = H$, und damit ist H^* auch ein Normalteiler.
Wenn H^* ein Normalteiler ist, daraus folgt $gH^*g^{-1} = H^*$, aber gH^*g^{-1} ist eben H. Also ist H auch ein Normalteiler. Die Antwort ist also ja.

4.2.2. H sei eine Untergruppe von G mit Index 2. Die Nebenklassen von H bilden eine Partition von G. In diesem Fall kann es nur zwei Nebenklassen geben: H und den Rest, den wir kurz mit H^* bezeichnen werden. Man nehme ein beliebiges Element $g \in G$.
Wenn $g \in H$, dann ist sowohl gH als auch Hg eben H. Sonst muss sowohl gH als auch Hg eben H^* sein. In beiden Fällen ist $gH = Hg$, also ist H ein Normalteiler von G.

4.2.3. H sei eine Untergruppe von G, g ein beliebiges Element von G. Da G kommutativ ist, bestehen $gH = \{gh \mid h \in H\}$ und $Hg = \{hg \mid h \in H\}$ aus denselben Elementen, also ist H ein Normalteiler von G.

4.2.4. Da $|G| = 32$, gilt: $o(x) \mid 32$. Da aber $x^8 \neq e$, ist $o(x)$ kein Teiler von 8. Also kann $o(x)$ entweder 16 oder 32 sein. Wenn $o(x) = 16$, dann hat die von x generierte Untergruppe die Index 2, also ist sie laut Aufgabe **4.2.2.** auch Normalteiler. Wenn $o(x) = 32$, dann ist die von x generierte Untergruppe eben G, was natürlich auch ein Normalteiler ist.

4.2.5. $e \in Z$, weil $\forall g \in G\ eg = g = ge$.
Wenn $x, y \in Z$, dann gilt $\forall g \in G\ g(xy) = (gx)y = (xg)y = x(gy) = x(yg) = (xy)g$, also ist auch $xy \in Z$, d. h. Z ist geschlossen bezüglich Multiplikation.
Wenn $z \in Z$, dann gilt $\forall g \in G\ g^{-1}z = zg^{-1}$ (da g^{-1} auch ein Element von G ist). Wenn man das Invers dieser Gleichung betrachtet, bekommt man: $\forall g \in G\ z^{-1}g = gz^{-1}$ (siehe Aufgabe **4.1.1.**), was eben bedeutet, dass Z auch bezüglich die Inversbildung geschlossen ist.
Damit ist also bewiesen, dass Z eine Untergruppe von G ist. Z ist auch Normalteiler, weil für jedes $g \in G\ gZ = \{gz \mid z \in Z\} = \{zg \mid z \in Z\} = Zg$ aus der Definition von Z folgt.
(Bemerkung: Z wird das Zentrum von G genannt.)

4.2.6. H ist eine Untergruppe von G, weil $1 \in H$, die Multiplikation führt nicht aus H hinaus $(1 \cdot 1 = 1, (-1) \cdot 1 = -1, 1 \cdot (-1) = -1, (-1) \cdot (-1) = 1)$ und die Inversbildung auch nicht $(1^{-1} = 1, (-1)^{-1} = -1)$. Da G kommutativ ist, ist H auch Normalteiler (siehe Aufgabe **4.2.3.**). Die Nebenklassen sind: $gH = Hg = \{g, -g\}$.

4.2.7. H ist natürlich eine Untergruppe von G, da sie beide eine Gruppe mit der gleichen Operation sind und H eine Teilmenge von G ist. Da G kommutativ ist, ist H auch Normalteiler (siehe Aufgabe **4.2.3.**). Die Nebenklassen sind: $z\mathbb{R}^+ = \mathbb{R}^+ z = \{zr \mid r \in \mathbb{R}^+\}$, aus dem Ursprung ausgehende Halbgeraden auf der komplexen Ebene.

4.2.8. Aus Aufgabe **4.1.6.** folgt die Existenz eines Elementes $a \in G$ mit der Eigenschaft, dass $o(a) = p$ eine Primzahl ist. Da G keine echte Untergruppe hat und $\langle a \rangle$ eine Untergruppe von G ist, kann es keine echte Untergruppe sein, also ist $G = \langle a \rangle = C_p$ ($\langle a \rangle = \{e\}$ ist nicht möglich).

4.2.9.
a) Wir wissen, dass H bezüglich die Operation geschlossen ist. Was man noch beweisen muss, ist die Geschlossenheit bezüglich Inversbildung und dass $e \in H$.

Da H nicht leer ist, enthält es mindestens ein Element: x. Wegen der Geschlossenheit von H folgt: $\langle x \rangle \subset H$. Daraus folgt auch, dass $\langle x \rangle$ endlich ist. Also gibt es ein $x^k = e \in \langle x \rangle$. Daraus folgt natürlich $e \in H$. Ausserdem ist x^{k-1} eben das Invers von x, und das ist auch enthalten in $\langle x \rangle$ und damit auch in H. Da x ein beliebiges Element von H sein kann, haben wir auch bewiesen, dass H bezüglich Inversbildung geschlossen ist.
b) Sei z. B. G die additive Gruppe der ganzen Zahlen, H die Menge der positiven ganzen Zahlen. H ist zwar geschlossen bezüglich Addition, aber keine Untergruppe (es gibt kein Invers). H ist natürlich auch nicht endlich.

4.2.10. Sei $G = C_n = \langle g \rangle$ eine zyklische Gruppe, und H eine Untergruppe von G. Alle Elemente von H sind Potenzen von g. Das Element mit dem kleinsten Exponent in H sei g^k. Behauptung: $H = \langle g^k \rangle$.
Es ist trivial, dass $H \supseteq \langle g^k \rangle$. Nehmen wir indirekt an, dass $H \neq \langle g^k \rangle$. Das würde bedeuten, dass es ein Element g^m in H gibt, das in $\langle g^k \rangle$ nicht enthalten ist. Das heisst: $k \not| m$, also ist $d = (m, k) < k$. Andererseits weiss man aus dem Euklidischen Algorithmus, dass $d = ak + bm$ für geeignete ganze Zahlen a und b. Also $g^d = g^{ak+bm} = (g^k)^a (g^m)^b$, und da g^k und g^m in H enthalten sind, ist auch g^d in H enthalten. Aber das ist ein Widerspruch wegen $d < k$, weil wir angenommen haben, dass k das kleinste Exponent in H ist.

4.2.11. Laut Aufgabe **4.2.10.** kommen nur zyklische Gruppen in Frage. Ausserdem muss die Ordnung der Teilgruppe ein Teiler von 12 sein. Also kommen – neben den trivialen Untergruppen $\{e\}$ und C_{12} – nur die Gruppen C_2, C_3, C_4 und C_6 in Frage.
Man muss noch beweisen, dass diese tatsächlich Untergruppen sind. Sei g das Generatorelement von C_{12}. Dann sind $\{e, g^6\}$, $\{e, g^4, g^8\}$, $\{e, g^3, g^6, g^9\}$ und $\{e, g^2, g^4, g^6, g^8, g^{10}\}$ eben die 2-, 3-, 4- und 6-elementigen zyklischen Untergruppen.
Also hat C_{12} insgesamt 6 verschiedene nicht-isomorphe Untergruppen.

4.3 Homomorphismen, Ringe, Körper

4.3.1. Da G kommutativ ist, gilt $x^3y^3 = (xy)^3$, also ist f homomorph.
$\mathrm{Ker}f = \{x \mid x^3 = e\} = \{e, g^4, g^8\}$, wobei g das Generatorelement von C_{12} ist.
$G/\mathrm{Ker}f \simeq \mathrm{Im}f = \{e, g^3, g^6, g^9\} \simeq C_4$

4.3.2. Nehmen wir zuerst an, dass G kommutativ ist. In diesem Fall gilt für beliebige Elemente x und y (siehe auch Aufgabe **4.1.1.**):

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

also ist f homomorph.
Nehmen wir nun an, dass f homomorph ist. Nehmen wir beliebige Elemente x und y. Da f homomorph ist, gilt

$$f(x^{-1})f(y^{-1}) = f(x^{-1}y^{-1})$$

also

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

d. h. G ist kommutativ.

4.3.3.
a) φ ist homomorph, weil für beliebige Polynome p und q:

$$\varphi(p(x))\varphi(q(x)) = p(a)q(a) = (pq)(a) = \varphi(p(x)q(x))$$

und

$$\varphi(p(x)) + \varphi(q(x)) = p(a) + q(a) = (p+q)(a) = \varphi(p(x) + q(x))$$

φ ist aber nicht isomorph, weil es nicht injektiv ist (es gibt viele Polynome, deren Wert im Punkt a gleich ist).

b) φ ist homomorph, weil für beliebige Polynome p und q:

$$\varphi(p(x))\varphi(q(x)) = p(3x+2)q(3x+2) = (pq)(3x+2) = \varphi(p(x)q(x))$$

und

$$\varphi(p(x)) + \varphi(q(x)) = p(3x+2) + q(3x+2) = (p+q)(3x+2) = \varphi(p(x) + q(x))$$

φ ist auch isomorph, wie das sein Invers zeigt:

$$\varphi^{-1}(q(x)) = q\left(\frac{x-2}{3}\right)$$

(φ ist nur eine Umskalierung der x-Koordinatenaxe; die Operationen werden dadurch nicht beeinflusst.)

4.3.4. Da die Operationen die Üblichen sind, wissen wir, dass die Assoziativität, die Kommutivität und die Distributivität stimmt.
Die Addition führt aus der Menge nicht hinaus, weil

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

und wenn weder b noch d mit 2 oder 5 teilbar ist, dann ist bd auch nicht teilbar mit weder 2 noch 5, und das bleibt auch nach eventuellen Vereinfachungen wahr.
Mit ähnlichem Gedankengang sieht man, dass die Multiplikation auch nicht aus der Menge hinausführt:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Die 0 und die 1 sind auch enthalten ($\frac{0}{1}$ und $\frac{1}{1}$) und es gibt auch additives Invers:

$$\frac{a}{b} \rightarrow \frac{-a}{b}$$

Es gibt aber kein multiplikatives Invers, z. B. $\frac{2}{1}$ ist zwar enthalten, aber $\frac{1}{2}$ nicht.
Also ist diese Struktur ein kommutativer Ring mit Einheitselement, aber kein Körper.

4.3.5. Diese Struktur ist weder Ring noch Körper, weil sie nicht distributiv ist. Z. B. sei $f(x) = x^2$, $g(x) = x$, $h(x) = -x$. Dann ist

$$f(g(x) + h(x)) = 0$$

aber

$$f(g(x)) + f(h(x)) = 2x^2$$

4.3.6. Folgende Elemente haben ein Invers: 1, 5, 7, 11. (Diese Elemente sind selber ihre Inversen.) Die restlichen Elemente sind nicht teilerfremd zu 12, also können sie auch kein multiplikatives Invers haben.

4.3.7. x ist ein linksseitiger Nullteiler, d. h. $x \neq 0$ und es gibt ein $\bar{x} \neq 0$ mit $\bar{x}x = 0$. Daraus folgt auch, dass

$$\bar{x}(xy) = (\bar{x}x)y = 0y = 0$$

also ist xy auch ein linksseitiger Nullteiler.
Ein Beispiel, wo $x + y$ kein Nullteiler ist: sei $x = 2$ und $y = 3$ im Ring der Restklassen modulo 6.

4.3.8.
a) Diese Struktur ist isomorph mit dem Körper der komplexen Zahlen, wobei die komplexe Zahl $a + bi$ als (a, b) representiert ist; die beiden Operationen sind eben die komplexe Addition bzw. Multiplikation.
b) Diese Struktur erbt fast alle Eigenschaften vom Körper der reellen Zahlen. Das einzige Problem ist die Division mit 0: das Nullelement dieser Struktur ist die Folge $(0, 0, \ldots)$, aber es gibt auch andere Elemente, die kein multiplikatives Invers haben, nämlich alle solche Folgen, die mindestens eine 0 enthalten. Diese Struktur ist also ein kommutativer Ring, aber kein Körper.
c) Diese Struktur ist isomorph mit der folgenden: die Elemente sind die Teilmengen einer n-elementigen Menge (jede Teilmenge wird mit einer 0-1-Folge der Länge n kodiert), mit symmetrischer Differenz als Addition (dies entspricht der XOR-Operation) und Durchschnitt als Multiplikation (dies entspricht der AND-Operation). Es ist also ein Boolscher Ring.