9. Musterlösung zu Mathematik für Informatiker II, SS 2004

MARTIN LOTZ & MICHAEL NÜSKEN

Aufgabe 9.1 (Endliche Körper). (6 Punkte)

Sei q eine Primpotenz. (Man darf auch getrost annehmen, q sei prim. Dadurch ändert sich eigentlich nichts.) Wir nehmen an, dass $\mathbb{F}_q$ ein Körper mit q Elementen ist. (Tatsächlich gibt es einen und bis auf Isomorphie auch nur einen.) In dieser Aufgabe soll gezeigt werden, dass dann in $\mathbb{F}_q[x]$ die Gleichung

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

gilt.

(i) Berechne die rechte Seite für $q = 3$ und $q = 5$.

Lösung. In der üblichen symmetrischen Darstellung besteht der Körper $\mathbb{F}_3$ aus den Elementen $\{0, 1, -1\}$ mit denen wir modulo 3 zu rechnen haben:

$$\begin{aligned} x(x-1)(x+1) &= x(x^2-1) \\ &= x^3 - x. \end{aligned}$$

In der üblichen symmetrischen Darstellung haben wir $\mathbb{F}_5 = \{0, 1, -1, 2, -2\}$ und müssen modulo 5 rechnen.

$$\begin{aligned} x(x-1)(x+1)(x-2)(x+2) &= x(x^2-1)(x^2+1) \\ &= x(x^4-1) \\ &= x^5 - x. \end{aligned}$$

◯

(ii) Zeige, dass zwei Polynome f und g genau dann gleich sind, wenn $g \mid f$, $\deg f = \deg g$ und $\mathrm{lc}(f) = \mathrm{lc}(g)$ gilt.

Lösung. Wenn f und g gleich sind, dann sind natürlich auch die Leitkoeffizienten und Grade gleich, und es gilt $g|f$. Nimm umgekehrt an, dass $g|f$ sowie $\mathrm{lc}(f) = \mathrm{lc}(g)$ und $\deg f = \deg g$ gilt. Es gibt also ein $h \in \mathbb{F}_q[x]$ so, dass $f = gh$. Wegen der Bedingung $\deg f = \deg g$ folgt $\deg h = 0$, also gilt $h \in \mathbb{F}_q$. Für die Leitkoeffizienten folgt daraus $\mathrm{lc}(f) = h\,\mathrm{lc}(g)$. Also ist $h = 1$ und folglich $f = g$. ◯

(iii) Zeige, dass für $a \in \mathbb{F}_q \setminus \{0\}$ die Gleichung $a^{q-1} = 1$ gilt.

Lösung. Die Menge $\mathbb{F}_q \setminus \{0\}$ bildet mit der Multiplikation eine Gruppe ($\mathbb{F}_q^\times$), weil $\mathbb{F}_q$ ein Körper ist. Nach dem Satz von Lagrange erhalten wir daraus sofort $a^{q-1} = 1$ für alle ihre Elemente. ◯

(iv) Zeige, dass für $a \in \mathbb{F}_q$ die Gleichung $a^q = a$ gilt.

Lösung. Aus $a^{q-1} = 1$ folgt $a^q = a$ für $a \neq 0$. Für $a = 0$ gilt diese Gleichung natürlich auch. ◯

(v) Schließe, dass für alle $a \in \mathbb{F}_q$ das Polynom $x - a$ das Polynom $x^q - x$ in $\mathbb{F}_q[x]$ teilt.

Lösung. Aus $a^q = a$ folgt, dass a eine Nullstelle des Polynoms $x^q - x$ ist. Wir wissen bereits: ist a eine Nullstelle eines Polynoms f über einem Körper, so teilt $x - a$ dieses Polynom. ◯

(vi) Folgere nun, dass $\prod_{a \in \mathbb{F}_q} (x - a)$ das Polynom $x^q - x$ teilt und sogar gleich diesem ist.

Lösung. Wir benutzen hier die Aussage: Gilt $g|f$, $h|f$ und $\mathrm{ggT}(g,h) = 1$, so folgt $gh|f$. Induktiv lässt sich dies auf Produkte mehrerer Polynome verallgemeinern, indem man verwendet, dass dann auch jedes dieser Polynome teilerfremd zum Produkt beliebig vieler der anderen ist. Nun sind die Polynome $(x-a)$ paarweise teilerfremd, und jedes einzelne teilt $x^q - x$. Also teilt auch das Produkt der $x - a$ das Polynom $x^q - x$. Beide Polynome haben Leitkoeffizient 1 und gleichen Grad, also folgt, dass diese Polynome gleich sind. ◯

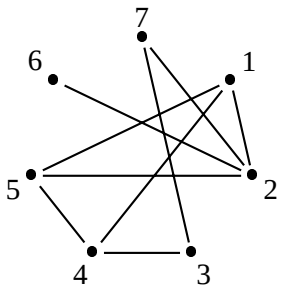
Bemerkung: Diese Beobachtung ist die Grundlage für den Beweis der Existenz und Eindeutigkeit eines endlichen Körpers $\mathbb{F}_q$ mit q Elementen, wenn nur q eine Primpotenz ist.

Aufgabe 9.2 (Graphen und Matrizen). (2 Punkte)

(i) Zeichne den Graphen mit der Inzidenzmatrix

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Lösung. Der folgende Graph hat die angegebene Matrix als Inzidenzmatrix.

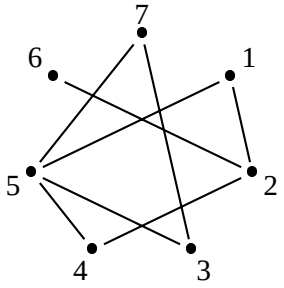


○

(ii) Zeichne den Graphen mit der Adjazenzmatrix

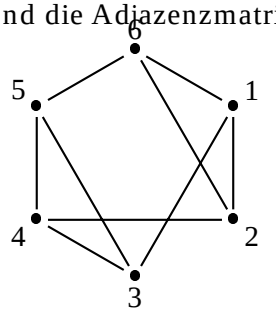
$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Lösung. Der folgende Graph hat die angegebene Matrix als Adjazenzmatrix.



○

(iii) Bestimme die Inzidenz- und die Adjazenzmatrix für den Graphen



Lösung. Wir erhalten die Inzidenzmatrix B, wobei die Reihenfolge der Spalten natürlich gleichgültig ist, und die Adjanzenzmatrix A:

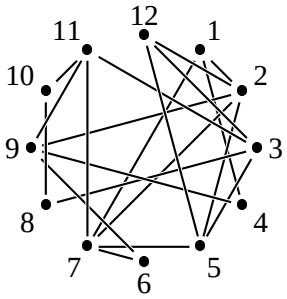
$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \end{bmatrix}, \qquad A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

○

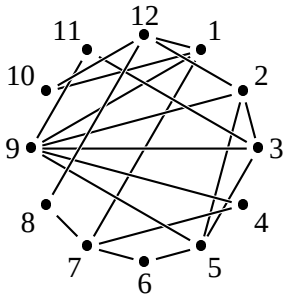
Aufgabe 9.3 (Kreise). (8 Punkte)

Prüfe bei den folgenden Graphen, jeweils ob sie einen Eulerkreis enthalten und ob sie einen Hamiltonkreis enthalten. (Begründung erforderlich!)

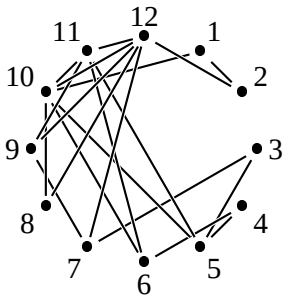
(i)



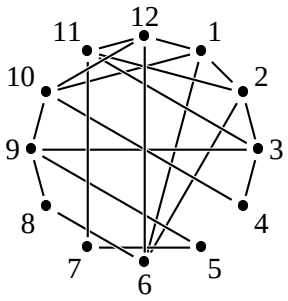
(iii)



(ii)

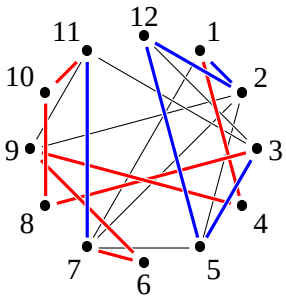


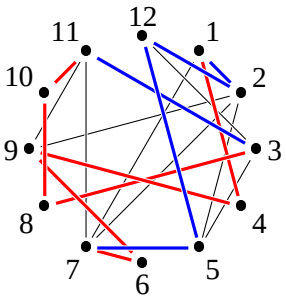
(iv)

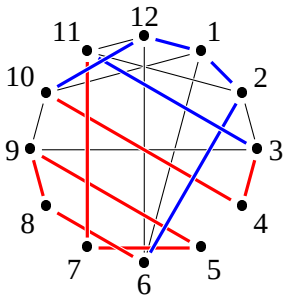


Lösung. In der Vorlesung wurde gezeigt, dass ein Graph genau dann einen Eulerkreis besitzt, wenn jeder Knoten geraden Grad hat. Demnach haben (i) und (ii) keinen Eulerkreis, (iii) und (iv) haben einen. (Es ist hier zwar möglich, aber nicht nötig den jeweiligen Eulerkreis anzugeben.)

Für Hamiltonkreis ist kein einfaches Kriterium bekannt. Wir müssen im positiven Fall den Hamiltonkreis angeben und im negativen ein schlaues Argument gegen die Existenz finden. (Notfalls müssen wir alle bei 1 beginnenden Punktreihenfolgen durchprobieren, aber das sind bei zwölf Punkten schon $11! = 39\,916\,800$ Möglichkeiten, die selbst bei einer schlauen Tiefensuche erhebliche Arbeit verursachen.) In unserem Fall hilft folgende kleine Beobachtung sehr viel weiter: *Jede* Kante, die an einem Knoten vom Grad 2 liegt, muss Teil eines Hamiltonkreises sein, falls dieser existiert. Die Graphen (i) und (iv) haben jeweils einen Hamiltonkreis. Für den linken geben wir gleich zwei an, ein Hamiltonkreis muss also nicht eindeutig bestimmt sein.

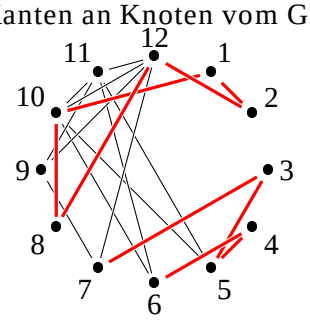




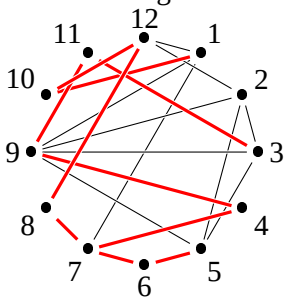


Die Graphen (ii) und (iii) besitzen keinen Hamiltonkreis. Um dies zu sehen,

merken wir wie eben die Kanten an Knoten vom Grad zwei vor:



Nun sehen wir aber, dass unter den markierten Kanten bereits ein Kreis ist, der nicht alle Knoten des Graphen durchläuft. Folglich kann (ii) keinen Hamiltonkreis haben. Im Fall (iii) erhalten wir folgendes Bild:



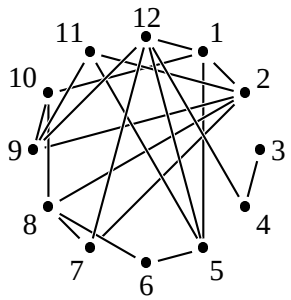
Wir sehen, dass drei der an den Knoten 7 angrenzenden Kanten zum Hamiltonkreis gehören müssten. Aber das kann natürlich nicht sein, da in einem Hamiltonkreis an jeden Knoten genau zwei Kanten grenzen.

Leider ist die hier verwendete Beobachtung im Allgemeinen bei weitem nicht ausreichend. Es ist bis heute kein Verfahren bekannt, um in polynomieller Zeit in der Eckenzahl zu entscheiden, ob ein Graph einen Hamiltonkreis hat oder nicht. Gäbe es so etwas, so wäre P $=$ NP. Die meisten Experten glauben, dass es sowas auch nicht gibt, und (äquivalent dazu) die Cooksche Vermutung P $\neq$ NP gilt. ○

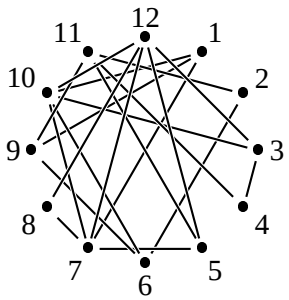
Aufgabe 9.4 (Isomorph oder nicht?). (6 Punkte)

Welche der folgenden Graphen sind isomorph und welche nicht?

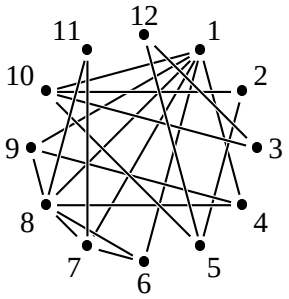
(i)



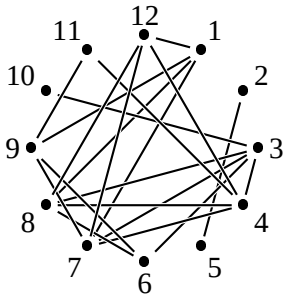
(ii)



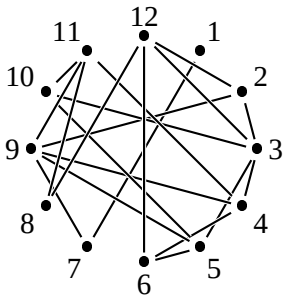
(iii)



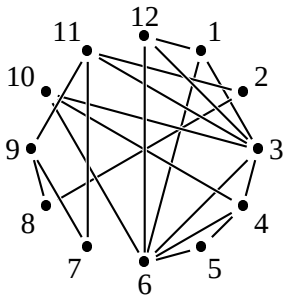
(v)



(iv)



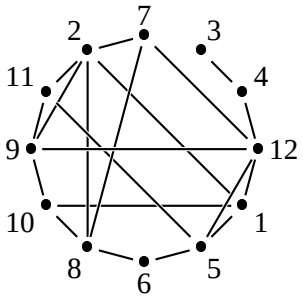
(vi)

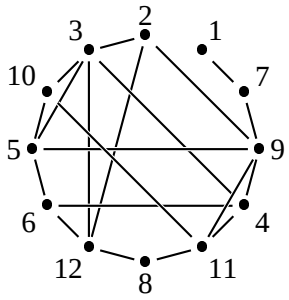


Lösung. Als erstes bestimmen wir die Grade der einzelnen Knoten in den Graphen.

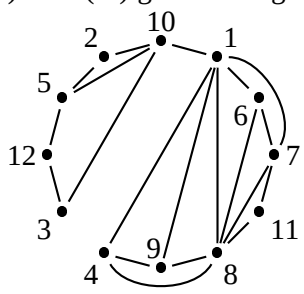
	1	2	3	4	5	6	7	8	9	10	11	12
(i)	4	5	1	2	4	2	3	4	4	3	3	5
(ii)	3	2	3	2	3	3	5	2	3	5	4	5
(iii)	6	2	2	3	3	3	4	6	3	4	2	2
(iv)	1	3	5	4	4	3	2	2	5	3	4	4
(v)	4	1	5	5	1	3	5	5	4	1	2	4
(vi)	3	2	6	4	2	6	2	2	3	3	4	3

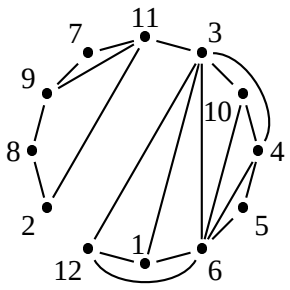
An dieser Tabelle sehen wir, dass nur die Graphen (i) und (iv), sowie (iii) und (vi) für Isomorphismen in Frage kommen. Tatsächlich haben wir Isomorphismen zwischen diesen Graphen. In diesen Fällen kann man den Isomorphismus finden, indem man zunächst mal die Punkte nach den Graden sortiert und daraus notwendige Zuordnungen ableitet. Dann kann man sich an den Kanten „entlanghangeln“. Am Einfachsten sieht man das Ergebnis, indem man die Knoten im Bild permutiert und die Kanten dabei mitnimmt, sodass die Bilder gleich sind. Wir haben das für (i) und (iv) in beiden Graphen gemacht, sodass die entstandenen Bilder leicht zu überblicken und gleich sind.





Der Fall (iii) und (vi) geht analog:





Man sieht, dass ein Isomorphismus nicht eindeutig bestimmt sein muss, hier können etwa die Punkte 4 und 9 im linken Bild einfach vertauscht werden. Man erkennt aber auch neben den Ordnungen der Punkte andere Merkmale, die zur Konstruktion des Isomorphismus hilfreich sein können, wie etwa die Brücke, die links von 10 nach 1 verläuft. (Ein Brücke ist eine Kante, deren Löschung den Graphen zerfallen lässt.) ○

☺**Aufgabe 9.5** (Eiszeit). (0+2 Punkte)

Als es noch richtige Winter gab, war einmal der Möhnesee zugefroren. Eine Zeitung berichtete am Ende der Saison über ein erstaunliches Phänomen:

Außerirdische am Werk?

Seit der See zugefroren ist, hat es eine Menge Zusammenstöße zwischen Eisläufern gegeben. Beim Zählen der Zusammenstöße machte unser Korrespondent jedoch eine verblüffende Entdeckung: An jedem Tag war die Anzahl der Eisläufer, die mit einer ungeraden Zahl von Eisläufern zusammenstieß, gerade! Umfragen unter den Menschen auf dem Eis haben keinerlei Anhaltspunkte ergeben. Die Behörden schweigen sich aus. Trotz beharrlicher Nachfragen bei den örtlichen Ämtern weigerten diese sich standhaft Stellung zu dem Phänomen zu nehmen: Die Wasserpolizei dementierte jegliche Verdacht auf kriminelle Hintergründe. Die ansässigen Feuerwehren bestritten ihre Zuständigkeit. Lokale Politiker ließen sich verleugnen oder verwiesen auf Sonderkommissionen und strenge Geheimhaltungsvorschriften. Wissenschaftler der Universität Paderborn sind ratlos.

Ihr auch?

Lösung. Nein, wir können helfen. Die Situation lässt sich durch einen Graphen G beschreiben: die Eisläufer sind die Ecken, je zwei Knoten sind durch eine Kante verbunden, wenn die Eisläufer zusammenstoßen. Die Aussage ist dann die, dass die Anzahl Knoten mit ungeradem Grad gerade ist. Benutze hier die aus der Vorlesung bekannte Formel:

$$\sum_{v \in E} d(v) = 2\#K,$$

wobei $d(v)$ den Grad von v bezeichnet. Da die geraden $d(v)$ einen geradzahligen Beitrag zur linken Seite der Gleichung liefern, muss dies auch bei den ungeraden $d(v)$ der Fall sein. Eine Summe ungerader Zahlen ist aber genau dann gerade, wenn die Anzahl der Summanden gerade ist. Damit ist der Fall gelöst. ○