DISKRETE UND STRUKTURELLE MATHEMATIK —FÜR INFORMATIKER—

MICHAEL JOSWIG

Skript zur Vorlesung an der TU Berlin im Sommersemester 2004. Nach Vorlage eines Skriptes von Christian Pommerenke.

Via `http://www.math.tu-berlin.de/~joswig` ist die jeweils aktuelle Version dieses Skripts zu finden.

1. Graphen

1.1. Grundlagen.

1.1.a. *Notation für Mengen.* Die Menge der natürlichen Zahlen sei mit $\mathbb{N} = \{0, 1, 2, \dots\}$ bezeichnet. Oft kürzen wir ab $[k] = \{0, 1, \dots, k-1\}$ für $k \in \mathbb{N}$. Das Symbol $|M|$ steht für die *Kardinalität* einer Menge M. Für den Zweck der Vorlesung ist es nicht notwendig, zwischen verschiedenen unendlichen Kardinalitäten zu unterscheiden, d.h. stets $|M| \in \mathbb{N} \cup \{\infty\}$.

Für eine beliebige Menge M und $k \in \mathbb{N}$ sei

$$\binom{M}{k} = \{M' \ : \ M' \subseteq M \text{ und } |M'| = k\}.$$

Mit

$$2^M = \{M' \ : \ M' \subseteq M\}$$

bezeichnen wir die *Potenzmenge* von M. Falls $|M| = n < \infty$, so gilt offenbar

$$2^M = \binom{M}{0} \cup \binom{M}{1} \cup \cdots \cup \binom{M}{n}.$$

Lemma 1.1.1. *Es sei M endlich. Dann gilt*

$$\left|\binom{M}{k}\right| = \binom{|M|}{k}.$$

Beweis. Übungsaufgabe. □

1.1.b. *Definition.*

Definition 1.1.2. Ein *(ungerichteter) Graph* mit *Knotenmenge V* ist ein Paar $\Gamma = (V, E)$ mit $E \subseteq \binom{V}{2}$. Die Elemente aus E heißen *Kanten* von Γ.

Für einen gegebenen Graphen Γ schreiben wir auch $V(\Gamma)$ für seine Knotenmenge sowie $E(\Gamma)$ für seine Kantenmenge.

Version vom: 5. Juli 2004.

Beispiel 1.1.3. Sei $\Gamma_1 = (V_1, E_1)$ mit $V_1 = [5]$ und

$$E_1 = \{\{0,1\},\{1,2\},\{2,3\},\{0,3\},\{0,4\}\}.$$

Oft werden Graphen durch (ebene) Diagramme visualisiert, in denen die Knoten als (verdickte) Punkte und Kanten als Verbindungsbögen gezeichnet werden. Diese Darstellung ist aber nicht eindeutig; vgl. Abbildung 1.

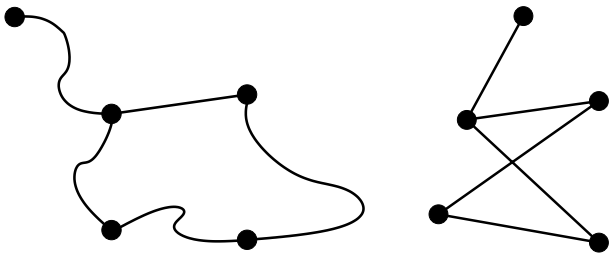

ABBILDUNG 1. Zwei Darstellungen des Graphen Γ_1 aus Beispiel 1.1.3.

Nicht alle Graphen lassen sich überschneidungsfrei in der Ebene zeichnen. Wir kommen auf diesen Aspekt in Abschnitt 1.4 zu sprechen.

1.1.c. *Beschränkung der Kantenzahl.*

Lemma 1.1.4. *Sei $\Gamma = (V, E)$ ein Graph. Dann gilt $|E| \leq 1/2|V|\cdot(|V|-1)$.*

Beweis. Sei $n = |V|$. Dann gilt $E \subseteq \binom{V}{2}$ und wegen Lemma 1.1.1 $|E| \leq \binom{n}{2} = 1/2n(n-1)$. □

1.1.d. *Knotengrad.* Sei $\Gamma = (V, E)$ ein Graph.

Definition 1.1.5. Für $x \in V$ heißt

$$\deg_\Gamma(x) = |\{e \in E \ : \ x \in e\}|$$

der *Grad* von x in Γ.

Proposition 1.1.6.

$$\sum_{x \in V} \deg_\Gamma(x) = 2|E|.$$

Beweis. Jede Kante enthält genau zwei Knoten. □

1.1.e. *Wege.* Sei im folgenden $\Gamma = (V, E)$ ein Graph.

Definition 1.1.7. Eine Folge $(v_0, v_1, \ldots, v_l)$ von Knoten heißt *Weg* der *Länge* l in Γ, falls für alle $i \in [l]$ gilt, dass $\{v_i, v_{i+1}\} \in E$ ist.

Ein Weg darf Länge 0 haben. Solche Wege nennen wir *trivial*.

Definition 1.1.8. Ein Weg $(v_0, v_1, \ldots, v_l)$ heißt

(i) *geschlossen*, falls $v_0 = v_l$ ist,

(ii) *einfach*, falls für alle $\{i,j\} \in \binom{[l+1]}{2} \setminus \{\{0,l\}\}$ gilt, dass $v_i \neq v_j$, und zusätzlich $v_0 \neq v_2$ (dies spielt nur eine Rolle im Falle $l = 2$),
(iii) *Kreis*, falls er einfach und geschlossen aber nicht trivial ist.

Der triviale Weg ist einfach und geschlossen, aber kein Kreis. Jeder Kreis hat Länge mindestens drei.

Definition 1.1.9. Sei $\Gamma = (V,E)$ ein Graph und

$$V' \subseteq V, \quad E' \subseteq E \cap \binom{V'}{2}$$

Teilmengen der Knoten- bzw. Kantenmenge. Dann heißt das Paar (V',E') *Teilgraph* (oder *Untergraph*) von Γ (Notation $(V',E') \leq \Gamma$).

1.2. **Zusammenhang.** Sei $\Gamma = (V,E)$ ein endlicher Graph.

1.2.a. *Verbindbarkeit.* Zwei Knoten $x,y \in V$ heißen *verbindbar* (Notation $x \sim y$), falls ein Weg von x nach y existiert.

Proposition 1.2.1. *Die Relation $\sim$ ist eine Äquivalenzrelation auf der Menge V.*

Beweis. Wir verifizieren *Reflexivität*, *Symmetrie* und *Transitivität*.

(i) Für $x \in V$ existiert der triviale Weg (der Länge 0) von x nach x. Damit ist $\sim$ reflexiv.
(ii) Wenn $(v_0 = x, v_1, \ldots, v_l = y)$ ein Weg von x nach y ist, dann ist auch $(v_l = y, v_{l-1}, \ldots, v_0 = x)$ ein Weg von y nach x. Damit ist $\sim$ symmetrisch.
(iii) Wenn $(v_0 = x, v_1, \ldots, v_l = y)$ ein Weg von x nach y und $(v_l = y, v_{l+1}, \ldots, v_{l+l'} = z)$ ein Weg von y nach z ist, dann ist $(v_0 = x, v_1, \ldots, v_{l+l'} = z)$ ein Weg von x nach z. Damit ist $\sim$ transitiv.

□

1.2.b. *Äquivalenzrelationen und Partitionen.* Sei $M \neq \emptyset$ eine Menge und $\sim$ eine (beliebige) Äquivalenzrelation. Die Menge

$$[x]_\sim = \{y \in M \ : \ y \sim x\}$$

heißt *Äquivalenzklasse* von x bezüglich $\sim$.

Proposition 1.2.2. *Die Menge* $\{[x]_\sim \ : \ x \in M\}$ *ist eine* Partition *der Menge M, d.h.*

(i) *Für alle $x,y \in M$ gilt* $[x]_\sim = [y]_\sim$ *oder* $[x]_\sim \cap [y]_\sim = \emptyset$.
(ii) $\bigcup_{x \in M} [x]_\sim = M$.
(iii) *Für alle $x \in M$ gilt* $[x]_\sim \neq \emptyset$.

Beweis. Da $\sim$ reflexiv ist, gilt $x \in [x]_\sim \neq \emptyset$. Hieraus folgt zusätzlich, dass $\bigcup_{x \in M} [x]_\sim = M$.

Seien $x,y \in M$ mit $[x]_\sim \cap [y]_\sim \neq \emptyset$. Also existiert $z \in [x]_\sim \cap [y]_\sim$. Sei nun $x' \in [x]_\sim$. Es gilt also $x' \sim x$ und $z \sim x$. Weil $\sim$ symmetrisch und transitiv

ist, folgt, dass $x' \sim z$ und weiter, dass $x' \in [y]_\sim$ ist. Daher gilt $[x]_\sim \subseteq [y]_\sim$ und aus Symmetriegründen auch die Umkehrung $[y]_\sim \subseteq [x]_\sim$. □

Bemerkung 1.2.3. Umgekehrt kann man auch zeigen, dass jede Partition eine Äquivalenzrelation stiftet.

Definition 1.2.4. Die Äquivalenzklassen der Verbindbarkeitsrelation auf dem Graphen Γ heißen *(Zusammenhangs-)Komponenten* von Γ. Der Graph Γ heißt *zusammenhängend*, wenn er genau eine Zusammenhangskomponente besitzt.

Proposition 1.2.5. *Wenn x verbindbar ist mit y, dann existiert auch ein einfacher Weg von x nach y.*

Beweis. Übungsaufgabe. □

1.2.c. *Eulersche Wege.*

Satz 1.2.6. *Falls der Graph Γ zusammenhängend ist, sind die beiden folgenden Aussagen äquivalent:*

(i) *Es gibt einen geschlossenen Weg in Γ, in dem jede Kante genau einmal vorkommt* [Eulerscher Weg].
(ii) *Jeder Knoten hat geraden Grad.*

Beweis. Zunächst "(i)⇒(ii)": Nehmen wir also an, dass es einen geschlossenen Weg $\eta = (v_0, v_1, \ldots, v_l = v_0)$ gibt, so dass für alle $e \in E$ genau ein $i \in [l]$ existiert mit $e = \{v_i, v_{i+1}\}$. Sei v ein beliebiger Knoten. Dann gibt es zu jeder Kante, durch die η in den Knoten v hineinläuft, genau eine Kante, durch die η aus v herausläuft. Also $\deg_\Gamma(x) \in 2\mathbb{N}$.

Umgekehrt "(ii)⇒(i)": Wir nehmen an, dass jeder Knoten geraden Grad hat. Ausgehend von einem beliebigen Knoten $v_0 \in V$ ziehen wir (auf beliebige Art und Weise) einen Weg $\eta_0 = (v_0, v_1, \ldots, v_l)$, in dem jede Kante höchstens einmal vorkommt, und der nicht mehr verlängert werden kann (ohne eine Kante doppelt zu benutzen). Da alle Knotengrade gerade sind, folgt, dass η_0 geschlossen ist, d.h. $v_l = v_0$. Da η_0 nicht mehr verlängert werden kann, kommen alle Kanten durch v_0 in η_0 vor. Nun ist $(v_1, v_2, \ldots, v_l = v_0, v_1)$ ein geschlossener Weg von v_1 nach v_1. Falls dieser Weg nicht alle Kanten durch v_1 verbraucht, lässt er sich verlängern, bis es nicht mehr geht. Ebenso wie im Fall η_0 ist der so entstehende Weg η_1 geschlossen, da alle Knotengrade gerade sind. Wenn wir so induktiv fortfahren, erhalten wir geschlossene Wege $\eta_0, \eta_1, \eta_2, \ldots$. Da es insgesamt nur endlich viele Kanten gibt, erhalten wir irgendwann einen geschlossenen Weg η_k, der alle Kanten durch alle seine Knoten genau einmal durchläuft. Es folgt, dass η_k ein eulerscher Weg der Zusammenhangskomponente von v_0 ist. Da aber Γ zusammenhängend ist, folgt die Behauptung. □

Beispiel 1.2.7. Das Königsberger Brückenproblem hat keine Lösung: Man kann nicht über die sieben Königsberger Brücken von einem Punkt

zum Ausgangspunkt zurück gehen, so dass man jede Brücke genau einmal benutzt; vgl. Abbildung 2.

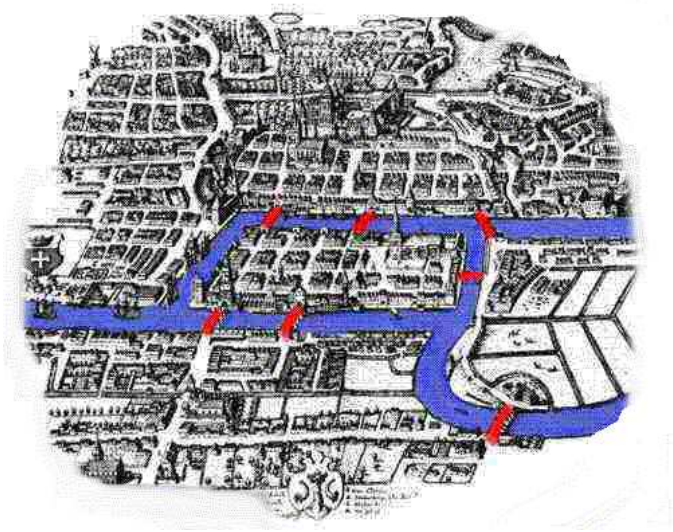

ABBILDUNG 2. Sieben Brücken in Königsberg über die Pregel.

1.3. **Bäume.**

1.3.a. *Definitionen.*

Definition 1.3.1. Ein *Baum* ist ein zusammenhängender Graph ohne Kreis. Ein Knoten vom Grad 1 in einem Baum heißt *Blatt* (oder *Endknoten*).

Lemma 1.3.2. *Jeder Baum mit mindestens zwei Knoten hat mindestens zwei Blätter.*

Beweis. Beginnend mit einem beliebigen Knoten, produziere einen einfachen Weg im Baum $\boldsymbol{B}$, der nicht verlängert werden kann. Da $\boldsymbol{B}$ keinen Kreis enthält, muss der letzte Knoten des Wegs Grad 1 haben.

Verlängern desselben Weges in die umgekehrte Richtung, bis es nicht mehr geht, liefert ein zweites Blatt. Die beiden Blätter sind verschieden, da der Baum mindestens zwei Knoten hat. □

Proposition 1.3.3. *Sei* Γ *ein zusammenhängender Graph mit* $\boldsymbol{n}$ *Knoten.*

(i) *Der Graph* Γ *hat mindestens* $\boldsymbol{n-1}$ *Kanten.*
(ii) *Der Graph* Γ *ist ein Baum genau dann, wenn er exakt* $\boldsymbol{n-1}$ *Kanten besitzt.*

Beweis. Übungsaufgabe. □

1.3.b. *Aufspannende Bäume.* Sei $\Gamma = (V, E)$ ein zusammenhängender endlicher Graph.

Definition 1.3.4. Ein Teilgraph $B = (V', E') \leq \Gamma$ heißt *aufspannender Baum*, falls B ein Baum ist und zusätztlich gilt $V' = V$.

Satz 1.3.5. *Der Graph Γ besitzt einen aufspannenden Baum.*

Beweis. Falls Γ keinen Kreis besitzt, so ist Γ selbst ein (aufspannender) Baum. Wir nehmen also an, dass ein Kreis $(v_0, v_1, \ldots, v_l = v_0)$ in Γ existiert. Der Graph $\Gamma' = (V, E \setminus \{v_0, v_1\})$ ist ein zusammenhängender Teilgraph von Γ mit weniger Kanten aber derselben Knotenmenge. Induktiv erhalten wir eine Folge von zusammenhängenden Teilgraphen $\Gamma = \Gamma_0 \geq \Gamma' = \Gamma_1 \geq \Gamma_2 \geq \ldots$, wobei alle Graphen Γ_i dieselbe Knotenmenge V haben, aber Γ_{i+1} hat genau eine Kante weniger als Γ_i. Da jeder endliche Graph nur endlich viele Kreise hat, existiert ein $k \in \mathbb{N}$, so dass Γ_k ein aufspannender Baum für $\Gamma_{k-1}, \Gamma_{k-2}, \ldots, \Gamma_0 = \Gamma$ ist. □

1.4. **Planare Graphen.**

1.4.a. *Definitionen.*

Definition 1.4.1. (vage) Ein Graph heißt *planar* (oder *eben*), wenn er überschneidungsfrei in der Ebene gezeichnet werden kann.

Definition 1.4.2. (exakt) Ein Graph $\Gamma = (V, E)$ ein Graph heißt *planar*, falls es ein Paar von Abbildungen (ν, ι) gibt, so dass $\nu : V \to \mathbb{R}^2$ injektiv ist, und so dass ι jede Kante $\{v, w\} \in E$ auf einen *Jordankurvenbogen* $\iota(v, w) \subset \mathbb{R}^2$ mit Endpunkten $\nu(v)$ und $\nu(w)$ abbildet mit $\nu(x) \notin \iota(v, w)$ für alle $x \in V \setminus \{v, w\}$ und zusätzlich $(\iota(v, w) \setminus \{\nu(v), \nu(w)\}) \cap (\iota(v', w') \setminus \{\nu(v'), \nu(w')\}) = \emptyset$ für $\{v, w\} \neq \{v', w'\}$ [Notation: $\iota(v, w) = \iota(\{v, w\}) = \iota(w, v)$.]

Bemerkung 1.4.3. Für die Definition von Jordankurven siehe geeignete Topologiebücher, z.B. Ossa: Topologie, Vieweg, 1992. Eine zentrale Eigenschaft ist der *Jordansche Kurvensatz*: Jede geschlossene Jordankurve trennt die Ebene $\mathbb{R}^2$ in zwei *Zusammenhangskomponenten* (im Sinne der Topologie). Für die Graphentheorie genügt eine stückweise lineare (oder polygonale) Version hiervon. Eine Konsequenz aus dem Jordanschen Kurvensatz ist, dass ein endlicher planarer Graph die Ebene in *Länder* (oder *Gebiete*) unterteilt; hiervon ist genau ein Land unbeschränkt, das *äußere Land*.

1.4.b. *Eulerscher Polyedersatz.* Sei $\Gamma = (V, E)$ ein planarer Graph mit Ländermenge L. Dann existiert der zu Γ *duale Graph* Γ^* mit Knotenmenge L, wobei je zwei Länder auf einer Kante in Γ^* liegen, falls sie (durch eine gemeinsame Kante) in Γ *benachbart* sind. Die Menge der *dualen Kanten* wird mit E^* bezeichnet.

Bemerkung 1.4.4. Das äußere Land liegt in der Menge L, ist also ein Knoten von Γ^*. Wenn zwei Länder $\alpha, \beta \in L$ mehrere gemeinsame Kanten haben, dann existieren in Γ^* auch mehrere Kanten zwischen α und β. Das heißt, der zu Γ duale Graph ist im allgemeinen kein Graph im Sinn der Definition 1.1.2, sondern ein *Graph mit Mehrfachkanten und Schleifen* (oder *Multigraph*). Dafür gilt aber, dass die Kanten von Γ den dualen Kanten bijektiv entsprechen: Wir bezeichnen die zu $e \in E$ duale Kante mit $e^* \in E^*$.

Auch Multigraphen besitzen Wege, Kreise, Teilgraphen (die Graphen oder Multigraphen sein können), aufspannende Bäume, etc. Der duale Graph eines planaren Graphen ist wieder planar. Außerdem ist Γ^* zusammenhängend, selbst wenn Γ nicht zusammenhängend ist.

Satz 1.4.5. *Sei Γ ein zusammenhängender planarer Graph. Dann hat Γ genau $|E| - |V| + 1$ beschränkte Länder (und ein unbeschränktes).*

Beweis. Nach Satz 1.3.5 hat Γ einen aufspannenden Baum B mit Kantenmenge E_B. Betrachte die Menge

$$E_{B^*} = \{e^* \ : \ e \in E \setminus E_B\}$$

von dualen Kanten. Weil B keinen Kreis enthält, ist der Graph $B^* = (L, E_{B^*})$ zusammenhängend. Da aber B umgekehrt zusammenhängend ist, und keine Kante von B^* eine Kante von B kreuzt, enthält wiederum B^* keinen Kreis. Es ist also B^* ein Baum, und zwar ein aufspannender Baum von Γ^*.

Wenn wir nun die Proposition 1.3.3 auf B und B^* anwenden, erhalten wir $|E_B| = |V|-1$ und $|E_{B^*}| = |L|-1$. Zusätzlich gilt aber $|E| = |E_B|+|E_{B^*}| = |V| - 1 + |L| - 1$. Dies entspricht der Behauptung. □

Bemerkung 1.4.6. Die Ecken-Kanten-Graphen von 3-dimensionalen *konvexen Polytopen* sind stets planar; vgl. Ziegler: Lectures on Polytopes, Springer, zweite Auflage 1998.

Satz 1.4.7. *Sei Γ ein zusammenhängender planarer Graph mit $|V| \geq 3$. Dann gilt $|E| \leq 3|V| - 6$.*

Beweis. Jedes beschränkte Land von Γ hat mindestens drei Kanten. Für das äußere Land trifft dies nicht zu, falls nämlich Γ ein Pfad der Länge 2 ist. Diesen Fall können wir aber außer acht lassen, da der Pfad der Länge 3 mit nur zwei Kanten die Behauptung erfüllt. In allen anderen Fällen liegen auch im äußeren Land mindestens drei Kanten.

Umgekehrt liegt jede Kante in höchstens zwei Ländern. Somit gilt

$$3|E| - 3|V| + 6 = 3(|E| - |V| + 2) \overset{1.4.5}{=} 3|L| \leq 2|E|,$$

also $|E| - 3|V| + 6 \leq 0$. □

Bemerkung 1.4.8. Der Satz 1.4.7 benutzt wesentlich, dass Γ ein Graph im Sinn der Definition 1.1.2 ist. Für Multigraphen ist die Aussage im

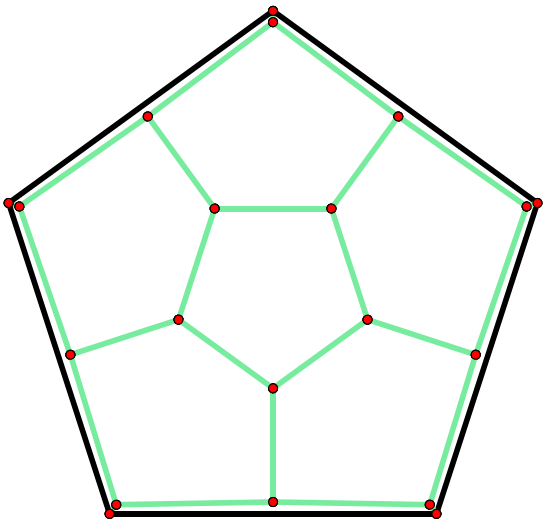

ABBILDUNG 3. Planare Darstellung (*Schlegeldiagramm*) des Ecken-Kanten-Graphen des regulären Dodekaeders.

allgemeinen natürlich falsch. Dagegen gilt der Satz 1.4.5 auch für Multigraphen.

Für $n \in \mathbb{N}$ heißt

$$K_n = \left([n], \binom{[n]}{2}\right)$$

der *vollständige Graph* auf n Knoten.

Korollar 1.4.9. *Die vollständigen Graphen K_n sind planar genau dann, wenn $n \leq 4$ ist.*

Beweis. Die Graphen K_n für $n \leq 4$ sind planar. Der Graph K_5 hat $\binom{5}{2} = 10$ Kanten, aber wegen $3 \cdot 5 - 6 = 9$ folgt aus Satz 1.4.7, dass K_5 nicht planar ist. Da K_5 Teilgraph von allen vollständigen Graphen K_n mit $n \geq 5$ ist, und weil Teilgraphen planarer Graphen planar sind, folgt die Behauptung. □

1.5. **Färbungen von Graphen.** Sei $\Gamma = (V, E)$ stets ein endlicher Graph.

1.5.a. *Definitionen.*

Definition 1.5.1. Sei $k \in \mathbb{N}$.

(i) Eine Partition $\{V_0, V_1, \ldots, V_{k-1}\}$ der Knotenmenge V heißt *Färbung mit k Farben* (oder *k-Färbung*) von Γ, falls für alle $i \in [k]$ und für alle $x, y \in V_i$ gilt, dass $\{x, y\} \notin E$.
(ii) Der Graph Γ heißt k-färbbar, falls er eine k-Färbung besitzt.
(iii) Die *chromatische Zahl* $\chi(\Gamma)$ ist die kleinste natürliche Zahl c mit der Eigenschaft, dass Γ eine c-Färbung besitzt.

(iv) Der Graph Γ heißt *bipartit*, falls $\chi(\Gamma) \leq 2$.

1.5.b. *Der* 4*-Farbensatz.*

Satz 1.5.2. *Jeder planare Graph ist mit höchstens vier Farben färbbar.*

Der Beweis dieses Satzes geht auf Appel, Haken und Koch (1977) zurück und beruht — nach einer Reduktion auf endlich viele Spezialfälle — auf Computerergebnissen. Ein neuerer Beweis von Robertson, Sanders, Seymour und Thomas (1996) reduziert den Computereinsatz, aber kommt auch nicht ohne aus.

1.5.c. *Das Museumswächterproblem.* Das Problem besteht darin, ein beliebiges Museum mit möglichst wenig Wächtern vollständig zu überwachen. Hierbei ist ein *Museum* ein *einfaches* (d.h. sich nicht selbst schneidendes) ebenes Polygon, das aber nicht konvex zu sein braucht (und das ist der eigentlich interessante Fall). Ein Wächter *sieht* einen Punkt im Museum, wenn die Verbindungsstrecke vom Wächter zum Punkt keine Wand trifft; vgl. Abbildung 4.

Satz 1.5.3. *Jedes einfache Polygon P in der Ebene kann* trianguliert *werden ohne zusätzliche Ecken, d.h., es lässt sich eine vollständige Zerlegung von P in Dreiecke finden, so dass die Ecken der Dreiecke alle Ecken von P sind, und so dass sich je zwei Dreiecke entweder gar nicht, in einer gemeinsamen Ecke oder in einer gemeinsamen Kante schneiden.*

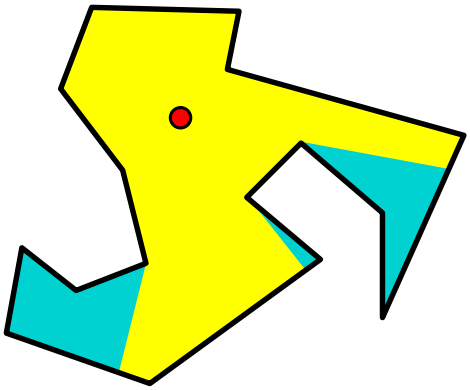

Abbildung 4. Museum mit einem Wächter und seinem Sichtbarkeitsbereich.

Dieser Satz ist nicht so schwer zu beweisen, sprengt aber — aus Zeitgründen — den Rahmen der Vorlesung. Nachzulesen beispielsweise in de Berg et al.: Computational Geometry, Springer, zweite Auflage, 2000.

Jede Triangulierung $\mathcal{T}$ eines einfachen Polygons P definiert einen planaren Graphen $\Gamma(\mathcal{T})$, wobei die Knoten und Kanten des Graphen die Ecken bzw. Kanten der Triangulierung sind.

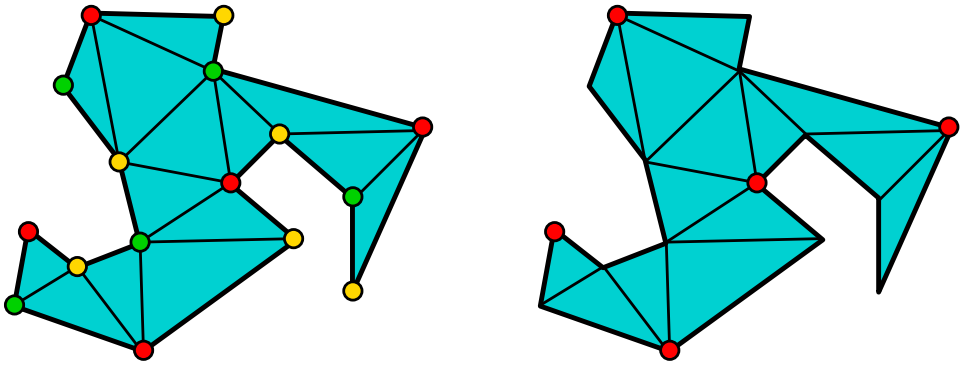

ABBILDUNG 5. 3-gefärbte Triangulierung und Lösung.

Satz 1.5.4. *Sei $\mathcal{T}$ eine Triangulierung eines einfachen ebenen Polygons P ohne zusätzliche Ecken. Dann gilt $\chi(\Gamma(\mathcal{T})) = 3$.*

Beweis. Wir definieren den dualen Graphen $\Delta(\mathcal{T})$ der Triangulierung $\mathcal{T}$ als den Teilgraphen des zu $\Gamma(\mathcal{T})$ dualen planaren Graphen, der dadurch entsteht, dass man das äußere Land und all seine dualen Kanten weglässt. Der Graph $\Delta(\mathcal{T})$ ist ein Graph im Sinn der Definition 1.1.2, hat also keine Mehrfachkanten oder Schleifen.

Sei n die Anzahl der Dreiecke in $\mathcal{T}$, das heißt, die Anzahl der Knoten von $\Delta(\mathcal{T})$. Per Induktion nach n zeigen wir zunächst, dass $\Delta(\mathcal{T})$ ein Baum ist: Falls $n = 1$, so hat $\Delta(\mathcal{T})$ gar keine Kanten und ist also ein Baum. Sei nun $n > 1$. Wir nehmen nun an, dass für jede Triangulierung eines einfachen Polygons mit weniger als n Dreiecken bereits gezeigt ist, dass der zugehörige duale Graph ein Baum ist. Weil aber $n > 1$ ist, existiert eine Kante e von $\mathcal{T}$, die keine Randkante von P ist. Sie trennt P in zwei kleinere einfache Polygon P_1 und P_2. An dieser Stelle ist ist wichtig, dass $\mathcal{T}$ keine zusätzlichen Ecken hat. Die Triangulierung $\mathcal{T}$ induziert dann Triangulierungen $\mathcal{T}_1$ und $\mathcal{T}_2$ von P_1 bzw. P_2. Unserer Induktionsannahme entsprechend wissen wir, dass $\Delta(\mathcal{T}_1)$ und $\Delta(\mathcal{T}_2)$ Bäume sind. Aber für die Kantenmenge von $\Delta(\mathcal{T})$ gilt nun

$$E(\Delta(\mathcal{T})) = E(\Delta(\mathcal{T}_1)) \cup E(\Delta(\mathcal{T}_2)) \cup \{e^*\}.$$

Es folgt, dass $\Delta(\mathcal{T})$ selbst auch ein Baum ist.

Wähle nun ein beliebiges Dreieck in $\mathcal{T}$ und färbe seine Ecken. Für jedes seiner Nachbardreiecke (das sind solche mit dem es eine Kante teilt) gibt es dann eine lokal eindeutige Fortsetzung der Färbung. Diese kann aber ohne Schwierigkeiten in alle Richtungen durch die gesamte Triangulierung $\mathcal{T}$ fortgesetzt werden, weil $\Delta(\mathcal{T})$ ein Baum ist: Es gibt nämlich zwischen je zwei Dreiecken in $\mathcal{T}$ eine *eindeutigen* Weg im dualen Graphen $\Delta(\mathcal{T})$. □

Korollar 1.5.5. *Jedes Museum mit n Ecken lässt sich mit $\lfloor n/3 \rfloor$ Wächtern überwachen.*

Beweis. Weil eine Triangulierung des Museums ohne zusätzliche Ecken 3-färbbar ist, kann man je einen Wächter auf die Knoten der kleinsten Farbklasse stellen (oder leicht in den Raum hinein versetzt, wenn die Wächter nicht in den Wänden stehen sollen). Das sind höchstens $\lfloor n/3 \rfloor$. Dann steht in jedem Dreieck genau ein Wächter. Der Wächter kann jedes Dreieck, in dem er steht einsehen, weil Dreiecke konvex sind. Alle Dreiecke gemeinsam überdecken das Museum. □

Dieses Ergebnis ist optimal (im ungünstigsten Fall, nicht unbedingt für jedes einzelne Museum!), wie das Beispiel in Abbildung 6 zeigt.

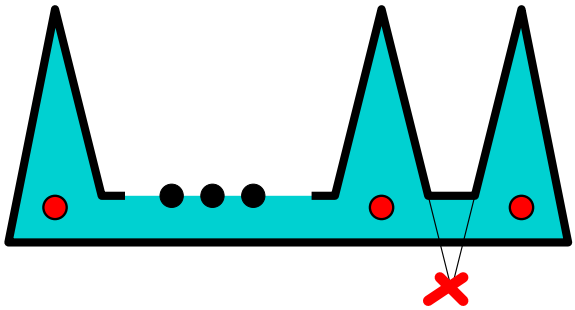

ABBILDUNG 6. Museum mit $3k$ Ecken, für dessen Bewachung k Wächter benötigt werden.

Die skizzierte Lösung des Museumswächterproblems geht auf Steve Fisk (1977) zurück.

2. ZAHLEN

Es sei $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ die Menge der ganzen Zahlen. Für $z \in \mathbb{Z}$ bezeichne $|z|$ den Absolutbetrag von z.

2.1. **Der euklidische Algorithmus.**

2.1.a. *Teilbarkeit und Division mit Rest.* Für $a, b \in \mathbb{Z}$ mit $b \neq 0$ existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$, so dass $a = qb + r$ und $0 \leq r < |b|$ gilt. Notation: $\lfloor a/b \rfloor = q$ und $\mathrm{rem}(a, b) = r$.

Falls $r = 0$, so gilt $a = qb$ und b *teilt* a. Notation: $b \mid a$ (und $b \nmid a$, falls b die Zahl a nicht teilt).

2.1.b. *Der euklidische Algorithmus.* Seien $x, y \in \mathbb{N}$ mit $1 \leq x \leq y$.

$x_0 \leftarrow y$, $x_1 \leftarrow x$, $k \leftarrow 0$
while $x_{k+1} \neq 0$ **do**
  $k \leftarrow k + 1$
  $q_k \leftarrow \lfloor x_{k-1}/x_k \rfloor$, $x_{k+1} \leftarrow \mathrm{rem}(x_{k-1}, x_k)$
return x_k

ALGORITHM 1. Euklidischer Algorithmus

Das Verfahren terminiert offenbar wegen $x_1 > x_2 > \cdots > x_k > x_{k+1} = 0$. Die Zahl x_k heißt *Resultat* des euklidischen Algorithmus zur Eingabe (x, y).

Beispiel 2.1.1. Seien $x_0 = y = 441$ und $x_1 = x = 42$.

Dann ist $q_1 = \lfloor 441/42 \rfloor = 10$ und $x_2 = \mathrm{rem}(441, 42) = 441 - 10 \cdot 42 = 21$. Weiter ist $q_2 = \lfloor 42/21 \rfloor = 2$ und $x_3 = 0$. Damit ist 21 das Resultat des euklidischen Algorithmus zur Eingabe $(42, 441)$.

Satz 2.1.2. *Das Resultat* $\gcd(x, y) := x_k$ *des euklidischen Algorithmus zur Eingabe* (x, y) *ist der* größte gemeinsame Teiler *von* x *und* y*, d.h.,*

(i) $\gcd(x, y) \mid x$ *und* $\gcd(x, y) \mid y$*,*
(ii) *falls* $d \mid x$ *und* $d \mid y$*, dann gilt auch* $d \mid \gcd(x, y)$*.*

Außerdem existieren $s, t \in \mathbb{Z}$ *mit* $sx + ty = \gcd(x, y)$*.*

Beweis. Es gilt $x_2 = x_0 - q_1 x_1 = s_2 x + t_2 y$, wobei $s_2 = -q_1$ und $t_2 = 1$. Damit gilt dann $x_3 = x_1 - q_2 x_2 = x - q_2(s_2 x + t_2 y) = s_3 x + t_3 y$, wobei $s_3 = 1 - q_2 s_2$ und $t_3 = -q_2 t_2$. Per Induktion ergibt sich schließlich $s_k x + t_k y = x_k$.

Außerdem gilt $x_{k-1} = q_k x_k + 0$, also $x_k \mid x_{k-1}$. Daraus folgt aber $x_k \mid q_{k-1} x_{k-1} + x_k = x_{k-2}$. Wiederum per Induktion gilt schließlich $x_k \mid x_1 = x$ und $x_k \mid x_0 = y$.

Sei nun d ein Teiler von x und y. Dann ist d auch ein Teiler von $s_k x + t_k y = x_k$. □

Durch die Konventionen $\gcd(y, x) = \gcd(x, y)$, sowie $\gcd(-x, y) = \gcd(x, -y) = \gcd(x, y)$ und $\gcd(0, x) = x$ ist die Funktion gcd für alle Paare von ganzen Zahlen außer $(0, 0)$ definiert.

Definition 2.1.3. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *relativ prim*, falls gilt $\gcd(a, b) = 1$. Wegen Satz 2.1.2 ist dies äquivalent dazu, dass zwei Zahlen $s, t \in \mathbb{Z}$ existieren mit $sa + tb = 1$.

Proposition 2.1.4. *Seien* $a, b, c \in \mathbb{Z}$ *und* $a \neq 0$*. Falls* $a \mid bc$ *und* $\gcd(a, b) = 1$*, dann gilt* $a \mid c$*.*

Beweis. Nach Satz 2.1.2 existieren $s, t \in \mathbb{Z}$ mit $sa + tb = 1$. Also ist

$$c = (sa + tb)c = (sc + t\frac{bc}{a})a.$$

□

Bemerkung 2.1.5. Jede rationale Zahl $q \in \mathbb{Q} \setminus \{0\}$ hat eine eindeutige *gekürzte* Darstellung $q = a/b$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und $\gcd(a, b) = 1$.

2.2. **Primzahlen.**

2.2.a. *Primfaktorzerlegung.*

Definition 2.2.1. Eine Zahl $p \in \mathbb{N}$ heißt *Primzahl*, falls $p > 1$ und p keine *echten Teiler* hat, d.h., keinen Teiler außer ± 1 und $\pm p$.

Satz 2.2.2. *Jede natürliche Zahl $n > 1$ hat eine eindeutige Zerlegung in Primfaktoren*

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

mit Primzahlen $p_1 < p_2 < \dots < p_r$ und $r, k_1, \dots, k_r \geq 1$.

Beweis. Zunächst beweisen wir per Induktion die Existenz einer Primfaktorzerlegung. Offenbar hat 2 als Primzahl eine solche Zerlegung. Sei nun $n > 2$ und die Existenz einer Primfaktorzerlegung für alle Zahlen kleiner als n bereits bewiesen. Dann ist entweder n eine Primzahl (und hat damit eine triviale Zerlegung in Primfaktoren) oder $n = ab$ mit $1 < a \leq b < n$. Durch Multiplikation und anschließende Umordnung gewinnen wir aus den nach Induktion existierenden Zerlegungen für a und b eine Primfaktorzerlegung von n.

Zum Beweis der Eindeutigkeit nehmen wir an, dass eine zweite Primfaktorzerlegung $n = q_1^{l_1} q_2^{l_2} \dots q_s^{l_s}$ existiert mit $q_1 < q_2 < \dots < q_s$ prim. Es ist p_r ein Teiler von n. Da nun je zwei verschiedene Primzahlen zueinander relativ prim sind, folgt aus Proposition 2.1.4, dass $p_r = q_j$ für $1 \leq j \leq s$. Falls $j < s$ dann stünde $q_s > p_r$ teilt n im Widerspruch zu Proposition 2.1.4. Also folgt, dass $j = s$ ist. Wir dividieren durch den beiden Darstellungen gemeinsamen Primfaktor $p_r = q_s$ und fahren (induktiv) fort. □

Beispiel 2.2.3. $476850 = 2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 17^2$, d.h. in diesem Fall: $r = 5$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 11$, $p_5 = 17$, $k_1 = k_2 = k_4 = 1$, $k_3 = k_5 = 2$.

2.2.b. *Weiteres zum Thema Primzahlen.*

Proposition 2.2.4. *Es gibt unendlich viele Primzahlen.*

Beweis. Übungsaufgabe. □

Es sei $\pi(x)$ die Anzahl der Primzahlen kleiner oder gleich $x \in \mathbb{R}$.

Satz 2.2.5. (Primzahlsatz von de la Vallée Poussin)

$$\lim_{x \to \infty} \pi(x) \Big/ \frac{x}{\ln x} = 1.$$

Das heißt, für sehr große x gilt $\pi(x) \approx x / \ln x$.

Bemerkung 2.2.6. Tatsächlich unterschätzt die Formel in Satz 2.2.5 die Anzahl der Primzahlen um ein wenig, z.B.: $\pi(611953) = 50000 \approx 611953/13,324\ldots = 45927,209\ldots$. Es gibt aber auch genauere Approximationen[1].

Der Beweis des Primzahlsatzes benutzt Methoden der komplexen Analysis, insbesondere die *Riemannsche Zetafunktion*

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}, \qquad \text{für } z = x + iy \in \mathbb{C},\ x > 0.$$

[1] `http://mathworld.wolfram.com/PrimeNumberTheorem.html`

Es gilt

$$\zeta(z) = \prod_{p \text{ prim}} \frac{1}{1-\frac{1}{p^z}} = \frac{1}{1-\frac{1}{2^z}} \cdot \frac{1}{1-\frac{1}{3^z}} \cdot \frac{1}{1-\frac{1}{5^z}} \cdots .$$

Die Klärung der folgenden offenen Vermutung würde 1 Million US-$ als Preisgeld einbringen[2]:

Vermutung 2.2.7. (Riemannsche Vermutung)

$$\zeta(x+iy) \neq 0, \qquad \text{für } x > 1/2.$$

Weitere fast ebenso berühmte unbewiesene Vermutungen über Primzahlen sind die beiden folgenden.

Vermutung 2.2.8. (Goldbachsche Vermutung)
Jede gerade Zahl $n > 2$ kann als Summe $n = p + q$ zweier Primzahlen p, q geschrieben werden.

Vermutung 2.2.9. (Primzahlzwillingsvermutung)
Es gibt unendlich viele Primzahlen p mit der Eigenschaft, dass auch $p + 2$ eine Primzahl ist.

Kürzlich hat Richard Arenstorf einen Beweis der Primzahlzwillingsvermutung vorgelegt, der auf Methoden der analytischen Zahlentheorie beruht[3].

2.3. **Kongruenzen.**

2.3.a. *Definition und Rechenregeln.* Sei $m > 1$ eine natürliche Zahl.

Definition 2.3.1. Es heißen $x, y \in \mathbb{Z}$ *kongruent modulo* m, falls $m \mid x-y$. [Notation $x \equiv y \mod m$.]

Beispiel 2.3.2. $23 \equiv 3 \equiv -7 \equiv -17 \mod 10$ und $2 \not\equiv 11 \mod 10$.
$255 \equiv -1 \equiv -257 \mod 256$ und $128 \not\equiv 0 \mod 256$.

Satz 2.3.3. *Modulo m gilt:*

(i) $x \equiv y,\ x' \equiv y' \Longrightarrow x + x' \equiv y + y',\ xx' \equiv yy'$.
(ii) $xz \equiv yz,\ \gcd(z, m) = 1 \Longrightarrow x \equiv y$.
(iii) *Es existiert* $\xi \in \mathbb{Z}$ *mit* $x\xi \equiv 1 \Longleftrightarrow \gcd(x, m) = 1$.

Beweis. Wir beweisen nur die erste Aussage, die zweite und die dritte wird als Übungsaufgabe gestellt.

Sei also $x = \xi m + y$ und $x' = \xi' m + y'$. Dann ist $x + x' = (\xi + \xi')m + y + y'$, also $x + x' \equiv y + y'$, und $xx' = (y + \xi m)(y' + \xi' m) = yy' + (y\xi' + y'\xi + \xi\xi' m)m$, also $xx' \equiv yy'$. □

[2] http://www.claymath.org/millennium/Riemann_Hypothesis/
[3] http://arxiv.org/math.NT/0405509

2.3.b. *Der chinesische Restsatz.*

Satz 2.3.4. *Seien $m_1, \dots, m_k$ relativ prim, und seien $r_1, \dots, r_k$ natürliche Zahlen mit $0 \le r_j < m_j$ für $j = 1, \dots, k$. Dann existiert genau ein $x \in \mathbb{N}$ mit $0 \le x < m_1 \cdots m_k$, so dass gilt*

$$x \equiv r_j \mod m_j, \qquad \text{für } j = 1, \dots, k.$$

Beispiel 2.3.5. Sei $k = 2$ und $m_1 = 10, m_2 = 13$ mit $r_1 = 5$ und $r_2 = 11$. Dann ist die einzige Lösung von

$$\begin{aligned} x &\equiv 5 \mod 10 \\ x &\equiv 11 \mod 13 \end{aligned}$$

mit $0 \le x < 130$ die Zahl $x = 115 = 11 \cdot 10 + 5 = 8 \cdot 13 + 11$.

Beispiel 2.3.6. Die Voraussetzung, dass die Moduln relativ prim sind, ist wesentlich: Es gibt keine Zahl, die gleichzeitig kongruent 2 modulo 5 und kongruent 3 modulo 10 ist.

$m \leftarrow m_1 \cdots m_k$
for $j \leftarrow 1, \dots, k$ **do**
  berechne (s_j, t_j) mit $s_j m/m_j + t_j m_j = 1 = \gcd(m/m_j, m_j)$
  $x_j \leftarrow \mathrm{rem}(r_j s_j, m_j)$
return $x := \sum_{j=1}^{k} x_j m/m_j$

ALGORITHM 2. Konstruktive Lösung zum Chinesischen Restsatz

Chinesischer Restsatz, konstruktiver Beweis. Mit der Notation von Algorithmus 2 gilt offenbar

$$s_j m/m_j = 1 - t_j m_j \equiv 1 \mod m_j.$$

Wegen Satz 2.3.3, (ii) und $\gcd(m_j, m/m_j) = 1$ folgt dann, dass $s_j \equiv 1 \mod m_j$. Also $x_j \equiv r_j s_j \equiv r_j \mod m_j$ und damit auch $x_j m/m_j \equiv r_j \mod m_j$. Nun gilt aber auch $x_j m/m_j \equiv 0 \mod m_l$ für alle $l \ne j$. Schließlich folgt, dass $x \equiv r_j \mod m_j$ für alle $j = 1, \dots, k$ ist. Nach Konstruktion gilt $0 \le x < m$.

Angenommen es gäbe eine zweite Lösung $y \ne x$ mit $0 \le y < m$. Da $x \equiv y \mod m_j$ für alle $j = 1, \dots, k$, gilt $m_j \mid x - y$. Da aber die Zahlen m_j relativ prim sind, folgt, dass auch $m \mid x - y$. Dies ist ein Widerspruch dazu, dass $|x - y| < m$ ist. □

2.3.c. *Die Eulersche Funktion ϕ.*

Definition 2.3.7. Für $n \in \mathbb{N} \setminus \{0, 1\}$ sei

$$\phi(n) = \left| \{k \ : \ 0 < k < n \text{ und } \gcd(k, n) = 1\} \right|.$$

Es gilt für jede Primzahl p, dass $\phi(p) = p - 1$. Allgemeiner folgt $\phi(p^k) = p^{k-1}(p-1)$.

Beispiel 2.3.8. $\phi(2) = 1$, $\phi(8) = |\{1,3,5,7\}| = 4 = 2^2 \cdot 1$.

Proposition 2.3.9. *Wenn $m_1, \ldots, m_k$ relativ prim sind, dann gilt*

$$\phi(m_1 \cdots m_k) = \phi(m_1) \cdots \phi(m_k).$$

Beweis. Unter der Voraussetzung, dass die Zahlen m_j relativ prim sind gilt: Eine Zahl x ist zu $m = m_1 \ldots m_k$ relativ prim genau dann, wenn sie zu allen Zahlen m_j relativ prim ist. □

Mit dem Satz 2.2.2 über die Primfaktorzerlegung ergibt sich eine allgemeine Formel für die Funktion ϕ.

Beispiel 2.3.10. $\phi(720) = \phi(6!) = \phi(2^4 \cdot 3^2 \cdot 5) = \phi(2^4) \cdot \phi(3^2) \cdot \phi(5) = 8 \cdot \phi(2) \cdot 3 \cdot \phi(3) \cdot \phi(5) = 8 \cdot 3 \cdot 2 \cdot 4 = 720(1 - 1/2)(1 - 1/3)(1 - 1/5) = 192$.

2.3.d. *Potenzreste.* Im folgenden sei stets ϕ die Eulersche ϕ-Funktion.

Satz 2.3.11. (Kleiner Satz von Fermat) *Seien x und m natürliche Zahlen mit $m \geq 2$. Falls $\gcd(x, m) = 1$, dann gilt*

$$x^{\phi(m)} \equiv 1 \mod m.$$

Beweis. Sei $n = \phi(m)$ und seien $y_1, \ldots, y_n$ die Zahlen zwischen 0 und m, die zu m relativ prim sind. Es ist

$$xy_k = q_k m + r_k \quad \text{mit } q_k \in \mathbb{N},\ 0 \leq r_k < m$$

für $k = 1, \ldots, n$. Die Reste r_k sind zu m teilerfremd (und insbesondere $r_k \neq 0$), da sowohl x als auch y_k zu m teilerfremd sind.

Weiter gilt $r_j \neq r_k$ für $j \neq k$. Denn, falls doch $r_j = r_k$ wäre, dann hätte man $xy_j - q_j m = r_j = r_k = xy_k - q_k m$ und damit $xy_j \equiv xy_k \mod m$. Wegen $\gcd(x, m) = 1$ wäre dann $y_j \equiv y_k \mod m$ und damit $y_j = y_k$.

Hieraus folgt nun, dass $\{y_1, \ldots, y_n\} = \{r_1, \ldots, r_n\}$. Insbesondere gilt dann $y_1 \cdots y_n = r_1 \cdots r_n$ und somit

$$x^n(y_1 \cdots y_n) = (xy_1) \cdots (xy_n) \equiv r_1 \cdots r_n \equiv y_1 \cdots y_n \mod m.$$

Da das Produkt $y_1 \cdots y_n$ zu m relativ prim ist, folgt $x^n \equiv 1 \mod m$. □

Satz 2.3.12. *Sei p eine Primzahl und $0 < x < p$. Dann ist $x^{p-1} \equiv 1 \mod p$. Weiter existiert eine Zahl a mit $0 < a < p$, so dass*

$$a^k \not\equiv 1 \mod p \quad \textit{für } 0 < k < p - 1.$$

Beweis. Die erste Aussage folgt unmittelbar aus dem kleinen Fermatschen Satz. Die zweite Aussage wird hier *ohne* Beweis angegeben. □

Beispiel 2.3.13. Sei $p = 7$. Dann gilt modulo 7: $3^1 = 3$, $3^2 = 9 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 3 \cdot 6 \equiv 4$, $3^5 \equiv 3 \cdot 4 \equiv 5$, $3^6 \equiv 1$, aber $2^1 \equiv 2$, $2^2 = 4$, $2^3 \equiv 1$, $2^4 \equiv 2$, $2^5 \equiv 4$, $2^6 \equiv 1$.

2.4. **Kryptographie.** In der Kryptographie werden Nachrichten verschlüsselt, um das unbefugte Abhören zu verunmöglichen (oder mindestens zu erschweren). Unser Standardszenario (und das der meisten anderen Texte zum Thema) sieht so aus, dass Alice an Bob eine Nachricht schicken möchte.

Zu einem Kryptoverfahren gehören zueinander passend je ein Verfahren zur *Verschlüsselung* und ein Verfahren zur *Entschlüsselung*.

2.4.a. *Codierung von Texten als Folgen von Zahlen.* Es gibt viele Möglichkeiten, Textinformation in Zahlen zu codieren. Eine weit verbreitete Variante ist der 8-Bit-ASCII-Code. Dabei wird je ein Buchstabe (oder Dezimalziffer oder Sonderzeichen) als eine Zahl zwischen 0 und 255 codiert, die also ihrerseits als eine Folge von acht Binärziffern (= ein Byte) dargestellt werden kann. Der besseren Lesbarkeit wegen gruppieren wir die acht Binärziffern eines Bytes in zwei Gruppen zu je vier Ziffern (= ein Nibble).

Beispiel 2.4.1. Beispieltext "Cafe de Guatemala" wird codiert als:

$$\underbrace{0100\,0011}_{\text{C}} \quad \underbrace{0110\,0001}_{\text{a}} \quad \underbrace{0110\,0110}_{\text{f}} \quad \underbrace{0110\,0101}_{\text{e}} \quad \underbrace{0010\,0000}_{\text{Leerzeichen}} \quad \dots$$

Im folgenden gehen wir stets davon aus, dass unsere Nachrichten bereits als Folgen von Zahlen vorliegen (vorgegebener Länge). Ein Kryptoverfahren muss sich daher nur mit der Kodierung und Dekodierung einzelner Zahlen befassen. Der Einfachheit halber gehen wir hier davon aus, dass unsere Codierungslänge 32 Bit beträgt, dass wir also je vier ASCII-codierte Buchstaben der Nachricht als einen gemeinsamen Block betrachten. Für praktische Anwendungen ist das aber zu wenig. Falls die Länge der Nachricht nicht durch vier teilbar ist, füllen wir sie mit Nullen auf (die im ASCII-Code kein gewöhnliches Zeichen kodiert).

Ein *Kryptoverfahren* ist dann ein Paar von Abbildungen

$$E, D : [2^{32}] \to [2^{32}],$$

so dass für alle Nachrichten $m \in [2^{32}]$ gilt, dass $D(E(m)) = m$ ist. Das heißt die Verschlüsselungsabbildung E und die Entschlüsselungsabbildung D sind zueinander invers und insbesondere beide bijektiv.

2.4.b. *Ein sehr einfaches Kryptoverfahren.* Die Bitoperation "xor" (exklusives oder) ist folgendermaßen definiert:

$$0 \oplus 0 := 0, \quad 0 \oplus 1 := 1, \quad 1 \oplus 0 := 1, \quad 1 \oplus 1 := 0.$$

Durch Wahl eines (geheimen) Schlüssels $k \in [2^{32}]$ lässt sich ein Kodierungsverfahren definieren durch

$$D(m) = m \oplus k \quad \text{und} \quad E(c) = c \oplus k.$$

Dabei versteht sich $\oplus : [2^{32}] \times [2^{32}] \to [2^{32}]$ als die bitweise Anwendung der oben erklärten Bitoperation "xor."

Beispiel 2.4.2.

$$\begin{array}{rcccccccc} m & = & 0100 & 0011 & 0110 & 0001 & 0110 & 0110 & 0110 & 0101 \\ k & = & 1001 & 0101 & 1111 & 1000 & 0110 & 0000 & 1011 & 0100 \\ m \oplus k & = & 1101 & 0101 & 1001 & 1001 & 0000 & 0110 & 1101 & 0001 \\ (m \oplus k) \oplus k & = & 0100 & 0011 & 0110 & 0001 & 0110 & 0110 & 0110 & 0101 \end{array}$$

Ein wesentlicher Nachteil dieser Methode liegt darin, dass der Schlüssel geheim bleiben muss, um die Nachricht sicher übermitteln zu können. Dies stellt Alice und Bob vor das Problem, dass sie sich auf den Schlüssel einigen müssen (und dafür einen sicheren Informationskanal benötigen).

2.4.c. *Das RSA-Kryptoverfahren.* Ein ganz anderes Kryptoverfahren geht auf Rivest, Shamir und Adleman zurück[4]. Es benutzt Methoden aus der elementaren Zahlentheorie.

Seien p und q Primzahlen. Dann setzen wir

$$n = pq \tag{1}$$

Wir wählen $e \in \mathbb{N}$ mit der Eigenschaft

$$\gcd(e, \phi(n)) = 1, \tag{2}$$

wobei $\phi(n) = (p-1)(q-1)$ die Eulersche Funktion ist. Nach dem kleinen Satz von Fermat 2.3.11 existiert dann ein $d \in \mathbb{N}$ mit

$$ed \equiv 1 \mod \phi(n). \tag{3}$$

Hiermit lässt sich das Kryptoverfahren RSA definieren: Die Nachricht $m \in [n]$, für $\gcd(m, n) = 1$ wird kodiert durch

$$E(m) = \operatorname{rem}(m^e, n). \tag{4}$$

Die entsprechende Vorschrift zur Entschlüsselung lautet

$$D(c) = \operatorname{rem}(c^d, n). \tag{5}$$

Satz 2.4.3. *Das Paar (E, D) definiert ein Kryptoverfahren, das heißt, für alle (zulässigen) m gilt, dass $D(E(m)) = m$ ist.*

Beweis. Setze $m' = D(E(m)) = \operatorname{rem}(\operatorname{rem}(m^e, n)^d, n)$. Zu zeigen ist also $m' = m$. Nach (3) gilt

$$ed = 1 + k(p-1)(q-1) \quad \text{für ein } k \in \mathbb{Z}. \tag{6}$$

Wenn nun m zulässig ist (das heißt $\gcd(m, n) = 1$), so folgt, dass m und $n = pq$ teilerfremd sind. Damit folgt aus Satz 2.3.11, dass

$$m^{(p-1)(q-1)} = m^{\phi(n)} \equiv 1 \mod n.$$

Hieraus folgt aber wegen (6), dass

$$m' \equiv m^{ed} = m(m^{(p-1)(q-1)})^k \equiv m \mod n. \tag{7}$$

[4]R. L. Rivest, A. Shamir and L. Adleman, Comm. ACM **21** (1978), no. 2, 120–126; MR 83m:94003

Die Behauptung ergibt sich dann aus $|m' - m| < n$. □

Und so funktioniert RSA in der Praxis: Die beiden Primzahlen p und q sind geheim, aber deren Produkt $n = pq$ ist öffentlich bekannt. Bob wählt e teilerfremd zu $\phi(n)$ (z.B. zufällig) und berechnet danach d mittels des Euklidischen Algorithmus. Dabei ist e Bobs *öffentlicher Schlüssel* und d Bobs *geheimer Schlüssel*.

Wenn nun Alice eine Nachricht an Bob schicken möchte, dann kodiert Alice die Nachricht mit Bobs öffentlichem Schlüssel e wie unter (4). Anschließend kann Bob mit seinem geheimen Schlüssel d die kodierte Nachricht wie unter (5) wieder entschlüsseln.

Die Sicherheit des Verfahrens beruht maßgeblich auf der Annahme, dass es (in angemessener Zeit) nicht möglich ist, die Zahl n zu faktorisieren (dazu muss n natürlich sehr groß sein und möglichst wenige Primfaktoren haben). Würde man die Faktoren p und q kennen (und damit auch $\phi(n) = (p-1)(q-1)$), dann ließe sich nach (3) leicht aus dem öffentlichen Schlüssel e auch der geheime Schlüssel d berechnen.

Leider ist die genaue Komplexität der Faktorisierung ganzer Zahlen noch immer unbekannt. Das heißt, es liegt kein Beweis vor, dass RSA ein sicheres Verfahren ist.

Bemerkung 2.4.4. In Satz 2.4.3 wurde vorausgesetzt, dass die Nachricht m teilerfremd ist zu $n = pq$. Tatsächlich gilt $D(E(m)) = m$ auch für alle anderen $m \in [n]$ (Übungsaufgabe!). Man kann aber zeigen, dass man aus einer kodierten unzulässigen Nachricht, relativ leicht n faktorisiert, das heißt also das Kryptosystem brechen kann.

Bemerkung 2.4.5. Zusätzlich zur Verschlüsselung lässt sich RSA auch zur digitalen Signatur verwenden: Wenn Bob eine Nachricht m an Alice schickt und beweisen möchte, dass er und niemand sonst die Nachricht geschickt hat, dann schickt er an Alice m zusammen mit $D(m)$. Alice kann dann mit Bobs öffentlichem Schlüssel $E(D(m))$ ausrechnen und das Ergebnis mit m vergleichen. Um m so zu signieren, dass am Ende $E(D(m)) = m$ gilt, muss man zum Signieren Bobs geheimen Schlüssel d kennen.

3. Ringe und Körper

Algebra, insbesondere die Ringtheorie, lässt sich verstehen als eine Abstraktion der Zahlentheorie.

3.1. **Grundlagen.**

3.1.a. *Definition eines Rings und erste Beispiele.* Sei R eine Menge mit zwei *binären Verknüpfungen* $+ : R \times R \to R$ und $\cdot : R \times R \to R$ und einem Element $0 \in R$. Oft wird das Multiplikationszeichen in Formeln unterdrückt, wir schreiben also xy statt $x \cdot y$.

Definition 3.1.1. Das Quadrupel $(R, +, \cdot, 0)$ heißt *Ring*, falls gilt

$$x + (y + z) = (x + y) + z, \tag{8}$$
$$x + y = y + x, \tag{9}$$
$$x + 0 = x, \tag{10}$$
$$\text{es existiert } -x \in R \text{ mit } x + (-x) = 0, \tag{11}$$
$$x(yz) = (xy)z, \tag{12}$$
$$(x + y)z = xz + yz \quad \text{und} \quad x(y + z) = xy + xz, \tag{13}$$

für alle $x, y, z \in R$.

Lemma 3.1.2. *Das* Nullelement $0 \in R$ *ist eindeutig bestimmt. Das Element* $-x$ *heißt* additives Inverses *zu* $x \in R$. *Zu gegebenem* $x \in R$ *ist es ebenfalls eindeutig.*

Beweis. Übungsaufgabe. □

Lemma 3.1.3. *Für alle* $x \in R$ *gilt* $x \cdot 0 = 0 = 0 \cdot x$.

Beweis. Es gilt

$$x + x0 \overset{(10)}{=} xx - (xx) + x + x0 \overset{(13)}{=} -(xx) + x + x(x + 0) \overset{(10)}{=} -(xx) + x + xx \overset{(10)}{=} x.$$

Aus der Eindeutigkeit des Nullelements nach Lemma 3.1.2 folgt daher $x0 = 0$. Die zweite Gleichung $0 \cdot x = 0$ folgt nalog. □

Hieraus folgt weiter, z.B., für alle $x, y \in R$, dass $x(-y)+xy = x(-y+y) = x0 = 0$, also $x(-y) = -(xy)$.

Beispiel 3.1.4. Beispiele für Ringe sind:

(i) die ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0)$,
(ii) die rationalen Zahlen $(\mathbb{Q}, +, \cdot, 0)$,
(iii) die reellen Zahlen $(\mathbb{R}, +, \cdot, 0)$,
(iv) der Ring der (2×2)-Matrizen

$$\left(R^{2\times 2}, +, \cdot, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right)$$

für einen beliebigen Ring R.

Definition 3.1.5. Ein Ring R heißt ...

(i) *kommutativ*, falls für alle $x, y \in R$ gilt $xy = yx$,
(ii) *Ring mit Eins*, falls es ein *Einselement* $1 \in R$ gibt, so dass für alle $x \in R$ gilt $x \cdot 1 = x$.

Die ersten drei Beispiele unter 3.1.4 sind kommutative Ringe mit Eins. Der Ring $R^{2\times 2}$ ist nicht kommutativ (selbst wenn R kommutativ ist), und er hat ein Einselement, nämlich $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, falls 1 das Einselement von R ist.

3.1.b. *Teilringe.* Sei $(R, +, \cdot, 0)$ ein Ring.

Definition 3.1.6. Eine nicht leere Teilmenge $U \subseteq R$ heißt *Teilring* von R, falls für alle $u, v \in U$ gilt $u + v, u - v, uv \in U$. [Notation: $U \leq R$.]

Offenbar ist $0 \in U$, und $(U, +, \cdot, 0)$ ist ein Ring, wobei $+ : U \times U \to U$ und $\cdot : U \times U \to U$ die entsprechenden Einschränkungen der Addition und Multiplikation von R sind.

Sei $U \leq R$ ein Teilring von R. Dann heißt $x + U = \{x + u \ : \ u \in U\}$ die *Nebenklasse* von x in R bezüglich U. Seien im folgenden $x, y \in R$.

Lemma 3.1.7.

$$x + U \cap y + U \neq \emptyset \quad \Longleftrightarrow \quad x + U = y + U \quad \Longleftrightarrow \quad x - y \in U.$$

Beweis. Wir beweisen, dass aus der ersten Aussage die dritte folgt und hieraus die zweite. Die erste Aussage ist offensichtlich eine formale Abschwächung der zweiten.

Sei $z \in x + U \cap y + U$. Also existieren $u, v \in U$ mit $x + u = z = y + v$. Dann ist $x - y = v - u \in U$.

Sei nun $x - y \in U$, dann ist $x = y + (x - y) \in y + U$, also $x + U \subseteq y + U$. Symmetrisch folgt $x + U \supseteq y + U$ und damit $x + U = y + U$. □

Korollar 3.1.8. *Die Menge der Nebenklassen*

$$R/U = \{x + U \ : \ x \in R\}$$

partitioniert die Menge R.

Beispiel 3.1.9. Sei $R = \mathbb{Z}$. Dann bildet die Menge der geraden Zahlen $E = \{0, \pm 2, \pm 4, \dots\}$ einen Teilring, und es gilt $\mathbb{Z}/E = \{E, 1 + E\}$, wobei $1 + E = \{\pm 1, \pm 3, \dots\}$ die Menge der ungeraden Zahlen ist.

3.1.c. *Ideale und Quotientenringe.* Sei $(R, +, \cdot, 0)$ ein kommutativer Ring.

Definition 3.1.10. Eine Teilring $I \subseteq R$ heißt *Ideal* von R, falls zusätzlich gilt für alle $u \in I$ und alle $x \in R$, dass $ux \in I$ ist. [Notation: $I \trianglelefteq R$.]

Es sind stets $\{0\}$ und R Ideale. Jedes andere Ideal heißt *echt*.

Beispiel 3.1.11. Sei $m \in R$. Dann ist

$$mR = \{xm \ : \ x \in R\}$$

ein Ideal von R: Offenbar gilt für $x, y \in R$, dass $mx + my = m(x + y), mx - my = m(x - y), (mx)(my) = m(mxy) \in Rm$ ist, und $mR \leq R$. Nach Definition ist $(mx)y = m(xy) \in mR$, also $mR \trianglelefteq R$. Ideale dieser Form heißen *Hauptideale*.

Proposition 3.1.12. *Der Ring $(\mathbb{Z}, +, \cdot, 0)$ der ganzen Zahlen ist ein* Hauptidealring*, das heißt, dass jedes echte Ideal in $\mathbb{Z}$ ein Hauptideal ist.*

Beweis. Übungsaufgabe. □

Oben wurde gezeigt, dass die Menge der Nebenklassen zu einem Teilring von R die Menge R partitioniert. Falls der Teilring nun sogar ein Ideal ist, gilt Zusätzliches. Dazu definieren wir arithmetische Operationen auf der Menge R/I:

$$(x + I) + (y + I) := (x + y) + I \tag{14}$$

$$(x + I)(y + I) := (xy) + I \tag{15}$$

Proposition 3.1.13. *Mit der in (14) definierten Addition und der in (15) Multiplikation bildet R/I eine kommutative Ringstruktur. Das Nullelement ist die Nebenklasse $I = 0 + I$. Falls R ein Einselement 1 besitzt, so ist R/I ein Ring mit Einselement $1 + I$.*

Beweis. Übungsaufgabe. □

Definition 3.1.14. Der Ring $(R/I, +, \cdot, I)$ heißt *Quotientenring* von R modulo I.

Beispiel 3.1.15. Seien $R = \mathbb{Z}$ und E die Menge der geraden Zahlen wie in Beispiel 3.1.11. Wegen $\mathbb{Z}E \subseteq E$ ist $E = 2\mathbb{Z}$ ein Ideal (sogar ein Hauptideal). Addition und Multiplikation im Quotientenring $\mathbb{Z}/2\mathbb{Z}$ sehen folgendermaßen aus:

$+$	E	$1+E$
E	E	$1+E$
$1+E$	$1+E$	E

$\cdot$	E	$1+E$
E	E	E
$1+E$	E	$1+E$

Bemerkung 3.1.16. Man kann Ideale (und Quotientenringe) auch für nicht kommutative Ringe definieren, aber dann muss man zwischen Links- und Rechtsidealen (und beidseitigen Idealen) unterscheiden.

3.1.d. *Körper.*

Definition 3.1.17. Ein kommutativer Ring $(K, +, \cdot, 0)$ mit Einselement $1 \in K$ ist ein *Körper*, falls

$$\text{für alle } x \in K \setminus \{0\} \text{ existiert } x^{-1} \in K \setminus \{0\} \text{ mit } x \cdot x^{-1} = 1. \tag{16}$$

Beispiel 3.1.18. Die Ringe $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{Z}/2\mathbb{Z}$ sind Körper.

Für den Rest dieses Abschnitts betrachten wir den Ring $\mathbb{Z}$ und ein Element $m \in \mathbb{Z}$ mit $m \geq 2$.

Lemma 3.1.19. *Für $x, y \in \mathbb{Z}$ gilt $x + m\mathbb{Z} = y + m\mathbb{Z}$ genau dann, wenn $x \equiv y \mod m$.*

Beweis. $x+m\mathbb{Z} = y+m\mathbb{Z} \Leftrightarrow x-y \in m\mathbb{Z} \Leftrightarrow m \mid (x-y) \Leftrightarrow x \equiv y \mod m$. □

Satz 3.1.20. *Der Quotientenring $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper genau dann, wenn m prim ist.*

Beweis. Nach Proposition 3.1.13 ist $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring mit Einselement $1+m\mathbb{Z}$. Sei $x+m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ mit $0 < x < m$. Nach Satz 2.3.3 gilt $\gcd(x, m) = 1 \Leftrightarrow \exists x' \in \mathbb{Z} : xx' \equiv 1 \mod m \Leftrightarrow \exists x' \in \mathbb{Z} : (x + m\mathbb{Z})(x' +$

$m\mathbb{Z}) = 1 + m\mathbb{Z}$. Hieraus folgt, dass $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist genau dann, wenn jede Zahl $x \in \{1, \ldots, m-1\}$ relativ prim ist zu m, das heißt, wenn m eine Primzahl ist. □

Wenn Missverständnisse ausgeschlossen sind, identifizieren wir oftmals die Nebenklasse $x+m\mathbb{Z}$ mit der ganzen Zahl x, das heißt, *in diesem Sinne* gilt dann $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$. Im Falle, dass m prim ist, schreiben wir außerdem für den Körper $\mathbb{Z}/m\mathbb{Z}$ oft auch $\mathbb{F}_m$.

3.2. **Polynome.** Sei $(K, +, \cdot, 0, 1)$ ein Körper und t ein *Symbol*. Weder ist t ein Element von K noch eine Variable.

3.2.a. *Der Polynomring* $K[t]$. Ein *Polynom* über K ist ein formaler Ausdruck der Form

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n,$$

wobei $n \in \mathbb{N}$ und die *Koeffizienten* $a_0, a_1, \ldots, a_n$ Elemente aus K sind.

Zwei Polynome $f = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ und $g = b_0 + b_1 t + b_2 t^2 + \cdots + b_m t^m$ mit $m \leq n$ sind *gleich* falls gilt: $a_i = b_i$ für alle $i \in [m]$ und $a_i = 0$ für alle $i \in \{m+1, \ldots, n\}$.

Wir definieren den *Grad* eines Polynoms. Es gibt zwei Fälle: Entweder verschwinden alle Koeffizienten von $f = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$, das heißt $a_0 = a_1 = \cdots = a_n = 0$, also $f = 0$, dann ist $\deg f := -\infty$. Oder es existiert ein von 0 verschiedener Koeffizient, dann ist

$$\deg f := \max\{i \ : \ a_i \neq 0\}.$$

Polynome können addiert und multipliziert werden:

$$\begin{aligned} f + g &= (a_0 + b_0) + (a_1 + b_1)t + (a_2 + b_2)t^2 + \cdots \\ fg &= (a_0 b_0) + (a_0 b_1 + a_1 b_0)t + (a_0 b_2 + a_1 b_1 + a_2 b_0)t^2 + \cdots + (a_n b_m)t^{m+n} \end{aligned}$$

Hier bezeichnen "+" und (das unterdrückte) "$\cdot$" sowohl die Addition bzw. Multiplikation von Elementen aus K als auch von Polynomen über K.

Lemma 3.2.1.

$$\deg(f+g) \leq \max\{\deg f, \deg g\} \quad \textit{und} \quad \deg(fg) = \deg f + \deg g.$$

Beispiel 3.2.2. Sei $K = \mathbb{Q}$. Wir betrachten die Polynome $f = 1 + t - \frac{3}{4}t^3 + t^5$ (mit $\deg f = 5$) und $g = t + \frac{2}{3}t^2$ (mit $\deg g = 2$). Dann ist $f + g = 1 + 2t + \frac{2}{3}t^2 - \frac{3}{4}t^3 + t^5$ und $fg = t + \frac{5}{3}t^2 + \frac{2}{3}t^3 - \frac{3}{4}t^4 - \frac{1}{2}t^5 + t^6 + \frac{2}{3}t^7$.

Beispiel 3.2.3. Sei $K = \mathbb{F}_2$. Wir betrachten die Polynome $f = 1 + t + t^2$ und $g = 1 + t$. Dann ist $f + g = t^2$ und $fg = 1 + t^3$.

Die Menge aller Polynome über K (in der *Unbestimmten* t) wird mit $K[t]$ bezeichnet.

Proposition 3.2.4. $(K[t], +, \cdot, 0, 1)$ *ist ein kommutativer Ring mit Eins.*

Für $f, g \in K[t]$ sagen wir g *teilt* f, falls ein Polynom $h \in K[t]$ existiert mit $f = gh$ [Notation: $g \mid f$]. Für $\alpha \in K \setminus \{0\}$ gilt wegen $f = gh = (\alpha g)(\alpha^{-1}h)$, dass $g \mid f \Leftrightarrow \alpha g \mid f$.

3.2.b. *Polynomdivision.* Im folgenden sei K stets ein Körper. Für Polynome über K gibt es eine Division mit Rest, ganz ähnlich wie die "schriftliche Division" mit Rest in $\mathbb{Z}$:

Proposition 3.2.5. *Seien $f, g \in K[t]$. Dann existieren eindeutig bestimmte Polynome $q, r \in K[t]$ mit $f = qg + r$ und $\deg r < \deg g$.*

Beispiel 3.2.6. Sei $K = \mathbb{F}_2$. Gemäß unserer *Konvention* schreiben wir wieder $\mathbb{F}_2 = \{0, 1\}$ statt $\{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$. Seien $f = t^3 + t^2 + 1$ und $g = t^2 + t + 1$. Dann ist $q = t$ und $r = t + 1$.

Die Division mit Rest in $K[t]$ ermöglicht es, den Euklidischen Algorithmus auf Polynome anzuwenden. Damit lässt sich der größte gemeinsame Teiler zweier Polynome über K berechnen.

3.2.c. *Irreduzible Polynome.* Sei wieder K ein Körper.

Definition 3.2.7. Ein Polynom $f \in K[t]$ mit $\deg f > 0$ heißt *irreduzibel*, falls es kein Polynom $g \in K[t]$ mit $0 < \deg g < \deg f$ gibt, das f teilt.

Beispiel 3.2.8. Das Polynom $t^2 + t + 1$ ist irreduzibel in $\mathbb{F}_2[t]$: Angenommen, $t^2 + t + 1$ wäre nicht irreduzibel. Dann gibt es $\alpha, \beta, \gamma, \delta \in \mathbb{F}_2$, so dass $t^2 + t + 1 = (\alpha t + \beta)(\gamma t + \delta) = \alpha\delta t^2 + (\alpha\delta + \beta\gamma) + \beta\delta$. Durch Koeffizientenvergleich ergibt sich, wegen $\alpha\delta t^2 = t^2$ und wegen $\beta\delta = 1$, dass $\alpha = \beta = \gamma = \delta = 1$ ist. Aber $\alpha\delta + \beta\gamma = 1 + 1 = 0 \neq 1$. Dies ist ein Widerspruch zu der Annahme, $t^2 + t + 1$ sei reduzibel.

Beispiel 3.2.9. Jedes Polynom in $\mathbb{R}[t]$ vom Grad mindestens drei ist reduzibel.

Satz 3.2.10. *Sei $f \in K[t]$ irreduzibel. Dann ist $K[t]/(fK[t])$ ein Körper.*

Beweis. Übungsaufgabe. Wir beweisen unten als Satz 3.2.12 den Spezialfall für endliches K. □

Beispiel 3.2.11. Das Polynom $t^2 + 1$ ist irreduzibel in $\mathbb{R}[t]$. Der Quotientenkörper $\mathbb{R}[t]/((t^2 + 1)\mathbb{R}[t])$ ist *isomorph* zu $\mathbb{C}$

3.2.d. *Endliche Körper.* In diesem Abschnitt sei K stets ein *endlicher* Körper der *Ordnung* $q = |K|$. Beispiele für endliche Körper (von Primzahlordnung) kennen wir aus Satz 3.1.20.

Eine wichtige Besonderheit bei endlichen Körpern ist, dass es für jede natürliche Zahl $n \in \mathbb{N}$ nur endlich viele Polynome vom Grad $\leq n$ gibt. Die Polynomdivision mit Rest zeigt, dass für $f \in K[t]$ mit $\deg f > 0$ gilt

$$K[t]/(fK[t]) = \{g + fK[t] \ : \ \deg g < n\}.$$

Insbesondere hat der Quotientenring $K[t]/(fK[t])$ genau q^n Elemente.

Wir beweisen den angekündigten Spezialfall von Satz 3.2.10.

Satz 3.2.12. *Sei $f \in K[t]$ irreduzibel. Dann ist $K[t]/(fK[t])$ ein Körper.*

Beweis. Setze $I = fK[t]$. Nach Proposition 3.1.13 ist $K[t]/I$ ein kommutativer Ring mit Nullelement I und Einselement $1+I$. Zu $g \in K[t] \setminus I$ betrachte die Abbildung $\lambda_g : K[t]/I \to K[t]/I : h + I \mapsto gh + I$. Es gilt $\lambda_g(I) = g0 + I = I$. Seien nun $h, h' \in K[t]$ beliebige Polynome. Dann ist $\lambda_g(h) - \lambda_g(h') = (gh - gh') + I = (g(h - h')) + I = \lambda_g(h - h')$. Angenommen $g(h - h') \in I$. Weil f irreduzibel ist, folgt aus $f \mid g(h - h')$, dass $f \mid g$ oder $f \mid (h - h')$ ist. Das heißt also $g \in I$ oder $h - h' \in I$. Hieraus folgt, dass die Abbildung $\lambda_g : (K[t]/I) \setminus \{I\} \to (K[t]/I) \setminus \{I\}$ injektiv ist. Weil aber K endlich ist (und damit auch $K[t]/I$), ist λ_g auch surjektiv, und jedes vom Nullelement I verschiedene Element in $K[t]/I$ hat ein multiplikatives Inverses. □

Der folgende wichtige Satz kann aus Zeitgründen in dieser Vorlesung nicht bewiesen werden.

Satz 3.2.13. *Für jeden endlichen Körper K der Ordnung q und für jede natürliche Zahl $n \geq 2$ existiert ein irreduzibles Polynom in $K[t]$ vom Grad n.*

Korollar 3.2.14. *Für jede Primzahlpotenz p^n mit p prim und $n \geq 1$ existiert ein endlicher Körper der Ordnung p^n.*

Bemerkung 3.2.15. Man kann zeigen, dass je zwei endliche Körper derselben Ordnung zueinander isomorph sind.

Man kann außerdem zeigen, dass die Ordnung eines beliebigen endlichen Körpers immer eine Primzahlpotenz ist.

Zusammenfassend kann man sagen:

Satz 3.2.16. *Für jeden endlichen Körper K der Ordnung q existiert eine Primzahl p, eine natürliche Zahl $n \geq 1$ und ein irreduzibles Polynom $f \in \mathbb{F}_p[t]$ vom Grad n, so dass $q = p^n$ und K isomorph ist zu $\mathbb{F}_p[t]/(f\mathbb{F}_p[t])$.*

Die direkte Berechnung eines irreduziblen Polynoms vom Grad n über $\mathbb{F}_p$ ist im allgemeinen nicht so einfach. Im konkreten Fall helfen Computeralgebrasysteme.

Es folgt eine Tabelle irreduzibler Polynome der Grade 2, 3, 4, 5 über den Körpern $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$.

	2	3	4	5
$\mathbb{F}_2$	t^2+t+1	t^3+t^2+1	$t^4+t^3+t^2+t+1$	$t^5+t^4+t^3+t^2+1$
$\mathbb{F}_3$	t^2+t+2	t^3+t^2+2	t^4+t^2+t+1	$t^5+t^4+2t^3+t^2+t+1$
$\mathbb{F}_5$	t^2+2t+4	t^3+3t^2+4t+1	t^4+3t^2+4t+3	$t^5+4t^3+t^2+3$
$\mathbb{F}_7$	t^2+2t+3	t^3+5t^2+6t+6	$t^4+3t^3+2t^2+t+5$	$t^5+2t^3+t^2+6t+3$
$\mathbb{F}_{11}$	t^2+2t+4	t^3+10t^2+6	$t^4+2t^3+5t^2+t+9$	$t^5+9t^4+9t^3+2t^2+4t+7$

Code für Maple[5], Version 8, zur Ausgabe irreduzibler Polynome:

```
p:=0;
for k from 1 to 5 do
   p:=nextprime(p);
   print([seq(GF(p,e)[extension],e=2..5)]);
end do;
```

[5]http://www.maplesoft.com/