Skriptum Diskrete Mathematik

Sommersemester 2009

Prof. Dr. Thorsten Theobald

Inhaltsverzeichnis

1. Einleitung und Überblick

Gegenstand der diskreten Mathematik sind

- endliche Mengen;
- Strukturen, die „diskret“ (im Sinne von separat voneinander) im Raum liegen (z.B. $\mathbb{Z} \subset \mathbb{R}$).

Aufgrund der engen Beziehung zu algorithmischen Fragen und zu Computeranwendungen hat sich die diskrete Mathematik als ein sehr wichtiges mathematisches Teilgebiet etabliert. In der Vorlesung, die sich an Studierende der Mathematik und Informatik (Bachelor-Studiengang bzw. vor dem Vordiplom) sowie verwandter Studienziele richtet wird eine Einführung in dieses Gebiet gegeben.

Überblick:

I: Grundlagen

- Natürliche und ganze Zahlen
- Teilbarkeit, größte gemeinsame Teiler und der Euklidische Algorithmus

II: Modulare Arithmetik und endliche Gruppen

- Modulare Arithmetik; der Restklassenring $\mathbb{Z}_m$
- Endliche Gruppen
- Kryptographie: RSA- Codier- und Unterschriftenschema (Rivest, Shamir, Adleman; Turing Award 2002)

III: Graphentheorie

- Graphen
- Planarität
- Färbbarkeit
- der Heiratssatz

IV. Endliche Körper und Codierungstheorie

- Endliche Körper
- Fehlerkorrigierende Codes (BCH; Bose, Ray-Chaudhuri, Hocquenghem; Verwendung z.B. bei CDs)

(*) V: Polytope und Polyeder

- Systeme linearer Ungleichungen; Fourier-Motzkin-Elimination
- Polytope
- Lineare Optimierung und der Simplex-Algorithmus

Literatur:

- Lehrbücher zum Thema Diskrete Mathematik (jeweils neueste Auflagen)
  - M. Aigner: Diskrete Mathematik (Vieweg)
  - T. Ihringer: Diskrete Mathematik (Teubner)
  - L. Lovász, J. Pelikán, K. Vesztergombi: Discrete Mathematics – Elementary and Beyond (Springer, 2003)
  - D. Lau: Algebra und Diskrete Mathematik 2 (Springer, 2004)
  - A. Steger: Diskrete Strukturen (Springer)
  - N.L. Biggs: Discrete Mathematics (Oxford University Press)
  - B. Korte, J. Vygen: Combinatorial Optimization (Springer, 2000)
  - A. Schrijver: Combinatorial Optimization (Springer, 2003)
  - ...
- Vorlesungsskripten von Prof. Kersting und Prof. Schnorr

Teil 1

Grundlagen

2. Grundlegendes zu den natürlichen und den ganzen Zahlen

Wir setzen eine Kenntnis grundlegender Beweistechniken sowie eine Vertrautheit mit den natürlichen und ganzen Zahlen voraus, etwa zu Zählprinzipien (Binomialkoeffizienten). Im Folgenden stellen wir einige grundlegende Definitionen und Konzepte zusammen.

Die Addition und Multiplikation in der Menge $\mathbb{Z}$ der ganzen Zahlen genügen den folgenden fünf Gesetzen:

(R1) Addition und Multiplikation sind *assoziativ*:

$$(a+b)+c \;=\; a+(b+c) \text{ und } (a\cdot b)\cdot c \;= a\cdot(b\cdot c)\,.$$

(R2) Addition und Multiplikation sind *kommutativ*:

$$a+b \;=\; b+a \text{ und } a\cdot b \;= b\cdot a\,.$$

(R3) Es existiert ein *neutrales Element* bezüglich der Addition (Nullelement, 0) und ein *neutrales Element* bezüglich der Multiplikation (Einselement, 1):

$$0+a \;= a \text{ und } 1\cdot a = a\,.$$

Es ist $0 \neq 1$.

(R4) Jedes Element a besitzt ein additives Inverses $(-a)$.

(R5) Es gilt das Distributivgesetz

$$a\cdot(b+c) \;=\; a\cdot b + a\cdot c\,.$$

Bemerkung. Allgemein sagt man, dass eine Menge R zusammen mit zwei Operationen $\oplus$ und $\odot$ einen *kommutativen Ring mit Einselement* definiert, wenn die Regeln R1 bis R5 erfüllt sind. (Lässt man die Forderung der Kommutativität an die multiplikative Operation weg, dann spricht man von einem *Ring mit Einselement*.) Aus R1 bis R5 ergeben sich weitere Regeln, die in $\mathbb{Z}$ selbstverständlich sind. Wir kommen später auf allgemeinere kommutative Ringe und ihre Rechenregeln zurück.

Seien $a, b \in \mathbb{Z}$. Wir sagen a *teilt* b, wenn eine ganze Zahl m mit $b = am$ existiert.[1] Schreibweise $a|b$. Falls $a \neq 0$ ist, dann folgt aus $a|b$, dass der Bruch $\frac{b}{a}$ eine ganze Zahl ist. Falls $a > 0$ und a kein Teiler von b ist, dann können wir b immer noch durch a teilen, allerdings mit Rest. Der Rest r bei der Division $b \div a$ ist eine ganze Zahl r, die $0 \leq r < a$ erfüllt. Bezeichnet q den Quotienten einer Division mit Rest, dann ist also

$$b \;=\; aq + r\,.$$

[1] Insbesondere teilt also jede Zahl $a \in \mathbb{Z}$ die Null.

Der *größte gemeinsame Teiler* zweier von Null verschiedener ganzer Zahlen ist die größte natürliche Zahl, die sowohl a als auch b teilt,

$$\mathrm{ggT}(a,b) \;:=\; \max\{k \in \mathbb{N} : k \text{ teilt } a \text{ und } k \text{ teilt } b\}\,.$$

Ferner setzt man $\mathrm{ggT}(a,0) = |a|$, $\mathrm{ggT}(0,b) = |b|$, so dass insbesondere $\mathrm{ggT}(0,0) = 0$. Analog ist das kleinste gemeinsame Vielfache von $a, b \neq 0$ die kleinste natürliche Zahl, die sowohl von a als auch von b geteilt wird:

$$\mathrm{kgV}(a,b) \;:=\; \min\{k \in \mathbb{N} : a \text{ teilt } k \text{ und } b \text{ teilt } k\}\,.$$

Ferner ist $\mathrm{kgV}(a,0) := 0$, $\mathrm{kgV}(0,b) := 0$, $\mathrm{kgV}(0,0) := 0$.

Bemerkung. Die Begriffe des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen verallgemeinern sich in natürlicher Weise auf mehr als 2 Zahlen; $\mathrm{ggT}(a_1, \ldots, a_n)$ bzw. $\mathrm{kgV}(a_1, \ldots, a_n)$. Gilt $\mathrm{ggT}(a_1, \ldots, a_n) = 1$, so werden $a_1, \ldots, a_n$ *relativ prim* oder *teilerfremd* genannt.

Eine natürliche Zahl $p \geq 2$ heißt *prim*, wenn 1 und p die einzigen positiven Teiler sind. Jede natürliche Zahl lässt sich bekanntlich als Produkt von Primzahlen darstellen.

Satz 2.1. *Jede natürliche Zahl $n \geq 2$ besitzt eine eindeutige Darstellung als Produkt von Primzahlen:*

$$n \;=\; p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

mit Primzahlen $p_1 < p_2 < \cdots < p_k$ und $e_1, \ldots, e_k \in \mathbb{N}$.

Tatsächlich erfordert ein vollständiger Beweis der Eindeutigkeitsaussage eine gewisse Sorgfalt. Wir gehen die Eindeutigkeit deshalb erst in späteren Abschnitten an. Die Existenz lässt sich wie folgt beweisen:

Beweis. Zum Nachweis der Existenz verwenden wir eine Induktion nach n.

n=2: klar.

Induktionsschritt: Sei $n \in \mathbb{N}$ mit $n \geq 2$. Falls n eine Primzahl ist, dann ist die Aussage klar. Anderenfalls gibt es eine natürliche Zahl $m \in \{2, \ldots, n-1\}$, die n teilt; es gilt also $n = km$ mit einem $k \geq 2$. Durch Anwendung der Induktionsvoraussetzung auf die Zahlen k, m und Zusammensetzen der Primfaktorzerlegungen folgt die Behauptung. □

Aufgaben.

(1) Zeigen Sie, dass folgende Definition des ggT (für beliebig viele Zahlen) im Fall $r = 2$ mit der oben angegebenen übereinstimmt:

Eine nichtnegative Zahl $d \in \mathbb{Z}$ heißt ggT von $a_1, \ldots, a_r \in \mathbb{Z}$, wenn $d|a_i$ $(1 \leq i \leq r)$ sowie

$$t|a_i \ (1 \leq i \leq r) \implies t|d\,.$$

(2) Zeigen Sie folgende Rechenregeln für den größten gemeinsamen Teiler:
   (a) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - bq)$ für $a, b, q \in \mathbb{Z}$.
   (b) $\mathrm{ggT}(a_1, \ldots, a_r) = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{r-1}), a_r)$ für $r \geq 3$.
   (c) Für $a, b, c \in \mathbb{Z}$ mit $\mathrm{ggT}(a, c) = 1$ gilt $\mathrm{ggT}(ab, c) = \mathrm{ggT}(b, c)$.

(3) Zeigen Sie, dass für jede Primzahl p die Zahl $\sqrt{p}$ irrational ist.

3. Die Eulersche φ-Funktion

In diesem und dem nachfolgenden Abschnitt untersuchen wir zwei interessante Funktionen auf den natürlichen Zahlen (Eulersche φ-Funktion, Möbius-Funktion μ). Diese zeigen zentrale Prinzipien und Beweistechniken auf und werden zudem bei der späteren Behandlung von Anwendungen (RSA-Schema, Konstruktion endlicher Körper) eine Rolle spielen.

Definition 3.1. Für $n \in \mathbb{N}$ ist $\varphi(n)$ definiert als

$$\varphi(n) = |\{m \in \{1, 2, \ldots, n\} : \mathrm{ggT}(n, m) = 1\}|\,.$$

φ heißt die *Eulersche φ-Funktion.*

Zwei natürliche Zahlen, deren größter gemeinsamer Teiler 1 ist, werden auch *relativ prim* genannt.

Beispiel 3.2. i) Es gilt $\varphi(n) = n - 1$ genau dann, wenn n prim ist.
ii) $\varphi(6) = 2$, da in $\{1, \ldots, 6\}$ genau die Zahlen 1, 5 relativ prim zu 6 sind.
iii) $\varphi(8) = 4$, da in $\{1, \ldots, 8\}$ genau die Zahlen 1, 3, 5, 7 relativ prim zu 8 sind.
iv) $\varphi(12) = 4$, da in $\{1, \ldots, 12\}$ genau die Zahlen 1,5,7,11 relativ prim zu 12 sind.

Für $n \leq 12$ lauten die Werte der φ-Funktion

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Im Folgenden sehen wir, dass bei bekannter Primfaktorzerlegung einer Zahl n bekannt die Funktion $\varphi(n)$ leicht berechnet werden kann.

Satz 3.3. *Es gilt*

(1) $\varphi(p) = p - 1$, *falls p prim;*

(2) $\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$, *falls* p *prim und* $r \in \mathbb{N}$.
(3) *Sind* $p_1, \ldots, p_k$ *die* unterschiedlichen *Primteiler von* n, *dann ist*

$$\varphi(n) \;=\; n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Beweis. Aus Beispiel 3.2 wissen wir bereits $\varphi(p) = p - 1$ für p prim.

Ist $n = p^r$ mit primem p, dann sind die Zahlen, die nicht relativ prim zu p^r sind, Vielfache von p, d.h., $p, 2p, \ldots, p^{r-1}p$; innerhalb der Menge $\{1, \ldots, n\}$ gibt es p^{r-1} solche Vielfache. Es verbleiben

$$\varphi(p^r) \;=\; p^r - p^{r-1} \;=\; p^r\left(1 - \frac{1}{p}\right).$$

Zahlen, die relativ prim zu p^r sind. Um die dritte Aussage zu zeigen, genügt es, die im zweiten Teil des nachfolgenden Lemmas aufgeführte Multiplikativitätseigenschaft zu zeigen: □

Lemma 3.4.

(1) *Für* $n \in \mathbb{N}$ *gilt* $\sum_{d|n}\varphi(d) = n$.
(2) *Für teilerfremde* m *und* n *gilt*

$$\varphi(mn) \;=\; \varphi(m)\varphi(n).$$

Beispiel. $\varphi(4 \cdot 5) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$. Tatsächlich sind die zu 20 teilerfremden Zahlen in $\{1, \ldots, 20\}$ genau die Zahlen

$$\{1, 3, 7, 9, 11, 13, 17, 19\}.$$

Beweis. Für $d|n$ sei

$$S_d \;=\; \left\{k\frac{n}{d} \;:\; \mathrm{ggT}(k, d) = 1,\, 1 \le k \le d\right\},$$

also $|S_d| = \varphi(d)$. Wir zeigen, dass die Mengen S_d alle disjunkt sind, und dass jedes $m \in \{1, \ldots, n\}$ in einer Menge S_d enthalten ist. Disjunktheit: Gilt $k\frac{n}{d} = k'\frac{n}{d'}$, dann folgt $kd' = k'd$ und wegen der Teilerfremdheit von k und d weiter $k = k'$, $d = d'$. Enthaltensein: Ist $m \in \{1, \ldots, n\}$, dann existiert ein Teiler d von n mit $\mathrm{ggT}(m, n) = \frac{n}{d}$; es folgt $m \in S_d$.

Für die zweite Aussage seien m und n teilerfremd. Die Teiler von mn sind genau die Zahlen der Form $D = dt$ mit $d|m$, $t|n$; hierbei gilt natürlich $\mathrm{ggT}(d, t) = 1$. Wir beweisen die Multiplikationsformel nun durch vollständige Induktion nach der Teileranzahl von mn.

Induktionsanfang (genau ein Teiler): Es ist also $m = n = 1$, so dass wegen $\varphi(1) = 1$ insbesondere die zu zeigende Multiplikativitätsformel $\varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$ gilt.

Induktionsschluss: Es gilt nach Teilaussage a)

$$\begin{aligned} mn &= \sum_{D|mn} \varphi(D) = \sum_{d|m,t|n} \varphi(dt) \\ &= \varphi(mn) - \varphi(m)\varphi(n) + \sum_{d|m,t|n} \varphi(d)\varphi(t) \qquad \text{(nach Induktionsvoraussetzung)} \\ &= \varphi(mn) - \varphi(m)\varphi(n) + \left(\sum_{d|m} \varphi(d)\right)\left(\sum_{t|n} \varphi(t)\right) \\ &= \varphi(mn) - \varphi(m)\varphi(n) + mn \qquad \text{(nach Teilaussage a)}\,. \end{aligned}$$

Es folgt damit $\varphi(mn) = \varphi(m)\varphi(n)$. □

Bemerkung. Im nächsten Abschnitt (siehe Bemerkung 4.5) werden wir einen alternativen Beweis für die Multiplikativitätsaussage kennenlernen. Noch später werden wir – im Rahmen der Behandlung des Chinesischen Restsatzes – diese Multiplikativitätsaussage von einem etwas höheren Standpunkt aus betrachten.

Aufgaben.

(1) Berechnen Sie $\varphi(999)$.
(2) Für welche $n \in \mathbb{N}$ ist $\varphi(n) = 48$? (Tipp: Es gibt 11 Lösungen.)

Anmerkungen. R.D. Carmichael stellte im Jahr 1922 die Vermutung auf, dass die Gleichung $\varphi(x) = n$ für kein n nur eine einzige Lösung besitzt. Mit anderen Worten: Für jedes $x \in \mathbb{N}$ existiert mindestens ein $y \neq x$ mit $\varphi(x) = \varphi(y)$; vergleiche die obigen Übungsaufgabe. (Tatsächlich hatte Carmichael im Jahr 1907 zunächst einen – falschen – Beweis für diese Aussage veröffentlicht).

Unter massivem Computereinsatz zeigten A. Schlafly und S. Wagon (1994), dass die Aussage zumindestens bis zu der (extrem großen) Zahl von 10^{10^7} richtig ist. Durch Erweiterung dieses Resultats verbesserte K. Ford diese untere Schranke auf $10^{10^{10}}$ (Ann. Math. 150:283–311, 1999).

Tabelle der ersten Werte von $\varphi(n)$ (beispielsweise hat der φ-Wert die Vielfachheit, da $\varphi(5) = \varphi(8) = \varphi(10) = \varphi(12) = 4$ und keine weitere Zahl den φ-Wert 4 hat); ungerade Zahlen größer als 1 haben Vielfachheit 0, da $\varphi(x)$ für $x > 1$ gerade ist.

φ-Wert	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
Vielfachheit	2	3	4	4	5	2	6	0	6	4	5	2	10	0	2	2	7	0	8	0	9	4	3	2	11

4. Die Möbius-Inversion

Im vergangenen Abschnitt haben wir insbesondere eine Produktdarstellung für die Eulersche φ-Funktion kennengelernt. Als Motivation für den aktuellen Abschnitt kann die Frage dienen, ob es andere Darstellungen für die φ-Funktion gibt, beispielsweise eine Darstellung als Summe.

Die Möbius-Funktion[2] $\mu : \mathbb{N} \to \mathbb{Z}$ ist durch $\mu(1) = 1$ sowie für $n > 1$ durch

$$\sum_{d|n} \mu(d) \;=\; 0$$

definiert (Die Summation $d|n$ betrifft von hier an die *positiven* Teiler von n.) Diese Gleichung ist tatsächlich eine Rekursionsbeziehung, da die linke Seite eine Summe ist, die aus dem Term $\mu(n)$ sowie einigen Termen $\mu(d)$ mit $d < n$ besteht.

Beispiel. Für $n \leq 12$ lauten die Werte der Möbius-Funktion

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

Die Möbius-Funktion hat die folgenden Eigenschaften:

Satz 4.1. *Für jede Primzahl p gilt $\mu(p) = -1$ sowie $\mu(p^r) = 0$, falls $r > 1$ ist. Für teilerfremde $m, n \in \mathbb{N}$ gilt*

$$\mu(mn) \;=\; \mu(m)\mu(n)\,.$$

Beweis. Eine Primzahl p besitzt im Bereich $\{1, \ldots, p\}$ genau zwei Teiler, nämlich 1 und p; aus der Definition der Möbius-Funktion folgt daher $\mu(p) = -1$.

Allgemein besitzt eine Primzahlpotenz p^r mit $r \geq 1$ im Bereich $\{1, \ldots, p^r\}$ die Teiler $p^0, p^1, \ldots, p^r$. Für $r > 1$ gilt $p^{r-1} > 1$ und folglich

$$0 \;=\; \sum_{d|p^r} \mu(d) \;=\; \mu(p^r) + \underbrace{\sum_{d|p^{r-1}} \mu(d)}_{=0} \;=\; \mu(p^r)\,.$$

[2] nach August Ferdinand Möbius, 1790–1868

Zum Nachweis der Multiplikativität betrachten wir teilerfremde m und n. Die Teiler von mn sind genau die Zahlen der Form $D = dt$ mit $d|m$, $t|n$; hierbei gilt natürlich $\mathrm{ggT}(d,t) = 1$. Wir beweisen die Multiplikationsformel nun (wie bei der Eulerschen φ-Funktion) durch vollständige Induktion nach der Teileranzahl von mn.

Induktionsanfang (genau ein Teiler): Es ist also $m = n = 1$, so dass wegen $\mu(1) = 1$ insbesondere die zu zeigende Multiplikativitätsformel $\mu(1 \cdot 1) = \mu(1) \cdot \mu(1)$ gilt.

Induktionsschluss: Es gilt

$$\begin{aligned} 0 &= \sum_{D|mn} \mu(D) = \sum_{d|m,t|n} \mu(dt) \\ &= \mu(mn) - \mu(m)\mu(n) + \sum_{d|m,t|n} \mu(d)\mu(t) \qquad \text{(nach Induktionsvoraussetzung)} \\ &= \mu(mn) - \mu(m)\mu(n) + \left(\sum_{d|m} \mu(d)\right)\left(\sum_{t|n} \mu(t)\right) \\ &= \mu(mn) - \mu(m)\mu(n)\,. \end{aligned}$$

Es folgt damit $\mu(mn) = \mu(m)\mu(n)$. □

Korollar 4.2. *Für eine Zahl n mit der Primzahldarstellung $n = \prod_{i=1}^{k} p_i^{e_i}$ und $e_i \geq 1$ gilt*

$$\mu(n) = \begin{cases} (-1)^k & \text{falls } e_1 = \cdots = e_k = 1\,, \\ 0 & \text{falls mindestens ein Primfaktor mit Exponent} \geq 2 \text{ auftritt.} \end{cases}$$

Beweis. Falls mindestens ein Primfaktor p mit Exponent $e \geq 2$ auftritt, gilt $\mu(p^e) = 0$ und wegen der Multiplikativität weiter $\mu(n) = 0$. Falls jeder effektiv auftretende Primfaktor p mit Exponent 1 auftritt, folgt die Aussage aus $\mu(p) = -1$ sowie der Multiplikativität. □

Ein nützliches Werkzeug zum Auflösen zur Untersuchung von Summen über Teilern bietet die *Möbius-Inversion*. Sei $f : \mathbb{N} \to \mathbb{C}$ eine Funktion und $F(n) = \sum_{d|n} f(d)$. Ziel ist es, die Summe zu "invertieren", das heißt, nach $f(n)$ in Abhängigkeit von F aufzulösen. Beispielsweise liefert die Möbius-Inversion eine Darstellung eine *Summendarstellung* für $\varphi(n)$ (als Summe über eine Funktion der Teiler).

Satz 4.3. (Möbiussche Inversionsformel.) *Für jede Funktion $f : \mathbb{N} \to \mathbb{C}$ und*

$$F(n) = \sum_{d|n} f(d) \qquad (n \in \mathbb{N})$$

gilt die Beziehung

$$f(N) \;=\; \sum_{d|N} \mu(d) F\left(\frac{N}{d}\right) \qquad (N \in \mathbb{N})\,.$$

Beweis. Aus der Definition von F folgt

$$\begin{aligned}\sum_{d|N} \mu(d) F\left(\frac{N}{d}\right) &= \sum_{d|N} \mu(d) \sum_{n|\frac{N}{d}} f(n) \\ &= \sum_{n|N} \left(\sum_{d|\frac{N}{n}} \mu(d)\right) f(n) \\ &= f(N)\,.\end{aligned}$$

□

Korollar 4.4. *Für $N \in \mathbb{N}$ gilt*

$$\varphi(N) \;=\; \sum_{d|N} \mu(d) \frac{N}{d}\,.$$

Beweis. Aus der Darstellung $\sum_{d|n} \varphi(d) = n$ folgt mittels der Möbius-Inversion

$$\varphi(N) \;=\; \sum_{d|N} \mu(d) \frac{N}{d}\,.$$

□

Beispiel.

$$\begin{aligned}\varphi(6) &= \mu(1)\cdot\frac{6}{1} + \mu(2)\cdot\frac{6}{2} + \mu(3)\cdot\frac{6}{3} + \mu(6)\cdot\frac{6}{6} \\ &= 1\cdot 6 + (-1)\cdot 3 + (-1)\cdot 2 + 1\cdot 6 \\ &= 2\,, \\ \varphi(12) &= \mu(1)\cdot\frac{12}{1} + \mu(2)\cdot\frac{12}{2} + \mu(3)\cdot\frac{12}{3} + \mu(4)\cdot\frac{12}{4} + \mu(6)\cdot\frac{12}{6} + \mu(12)\cdot\frac{12}{12} \\ &= 1\cdot 12 + (-1)\cdot 6 + (-1)\cdot 4 + 0\cdot 3 + 1\cdot 2 + 0\cdot 1 \\ &= 4\,.\end{aligned}$$

BEMERKUNG 4.5. Aus Korollar 4.4 ergibt sich ein alternativer Beweis für die Multiplikativität der φ-Funktion (Lemma 3.4 b). Für teilerfremnde m, n gilt

$$\begin{aligned}\varphi(mn) &= \sum_{d|m,t|n} \mu(d)\mu(t)\frac{m}{d}\frac{n}{t} \\ &= \left(\sum_{d|m} \mu(d)\frac{m}{d}\right)\left(\sum_{t|n} \mu(t)\frac{n}{t}\right) \\ &= \varphi(m)\varphi(n)\,.\end{aligned}$$

Aufgaben.

(1) Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt *multiplikativ*, falls $f(1) = 1$ und für alle teilerfremden m, n die Eigenschaft $f(mn) = f(m)f(n)$ gilt. Ist diese Gleichung sogar für alle $m, n \in \mathbb{N}$ richtig, dann nennt man f auch *strikt multiplikativ*. Zeigen Sie:
   (a) Das Produkt zweier (strikt) multiplikativer Funktionen ist wieder (strikt) multiplikativ.
   (b) Die summatorische Funktion $F(n) = \sum_{d|n} f(d)$ einer multiplikativen Funktion ist wieder multiplikativ.
   (c) Für jede multiplikative Funktion f gilt

$$f(n) = \prod_{i=1}^{k} f(p_i^{r_i})\,,$$

   falls n die Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{r_i}$ hat.

(2) Für eine natürliche Zahl n bezeichne $\sigma(n)$ die Summe der positiven Teiler von n im Bereich $\{1, \ldots, n\}$. (Beispiel: $\sigma(6) = 1 + 2 + 3 + 6 = 12$.) Zeigen Sie:
   (a) Hat n die Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{r_i}$, dann gilt

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{r_i+1} - 1}{p_i - 1}\,.$$

   (b) Die Funktion σ ist multiplikativ.

Anmerkungen. Eine Zahl n heißt *perfekt*, wenn die Summen aller ihrer Teiler, welche kleiner als n sind, die Zahl n ergibt. Beispiel: $6 = 1 + 2 + 3$ ist perfekt. Es ist keine einzige ungerade perfekte Zahl bekannt, aber niemand kann beweisen, dass es tatsächlich keine gibt.

Der Möbius-Inversion werden wir später im Rahmen größerer Kontexte (beim Zählen irreduzibler Polynome) erneut begegnen.

Aufgaben.

(1) In der Theorie der formalen Sprachen betrachtet man für eine endliche Menge A (Alphabet) die Menge A^+ aller (nichtleeren) endlichen Zeichenketten über A („Wörter“). Ein Wort $w \in T^+$ heißt *primitiv*, falls w nicht als Konkatenation $\underbrace{uu\cdots u}_{k-\text{mal}}$ mit einem kürzeren Wort u und $k \geq 2$ geschrieben werden kann.

Beispiel: Für $A = \{a, b, c\}$ ist das Wort ca primitiv und $bcbcbc$ nicht primitiv.

(a) Bestimmen Sie mittels der Möbius-Inversion die Anzahl $p(n)$ der primitiven Wörter der Länge n.

(b) Zeigen Sie, dass der Anteil der primitiven Wörter unter allen Wörtern der Länge n gegen 1 konvergiert:

$$\lim_{n\to\infty} \frac{p(n)}{|A|^n} = 1\,.$$

5. Der Euklidische Algorithmus

Der Euklidische Algorithmus zur Berechnung größter gemeinsamer Teiler gehört zu den ältesten Rechenverfahren. Er war schon Eudoxus (375 v. Chr.) bekannt und ist im Band 7 der „Elemente“ von Euklid (300 v. Chr.) beschrieben. Er ist von fundamentaler Bedeutung und kommt in vielen Rechenprozeduren zur Anwendung.

Fragen:

(1) Wie lässt sich der ggT effizient berechnen?
(2) Lässt sich der ggT durch die gegebenen Zahlen ausdrücken?

Eine Möglichkeit zur Berechnung des größten gemeinsamen Teilers besteht darin, a und b in Primfaktoren zu zerlegen. Seien etwa a und b natürlich, und bezeichne mit $p_1, \ldots, p_r$ die Primzahlen, die in a oder b als Teiler enthalten sind. Dann gibt es Zahlen $e_1, \ldots, e_r$, $f_1, \ldots, f_r \geq 0$, so dass $a = p_1^{e_1} \cdots p_r^{e_r}$. Die gemeinsamen Teiler von a und b sind dann von der Gestalt $z = \pm p_1^{g_1} \cdots p_r^{g_r}$ mit $g_i \in \{0, \ldots, m_i\}$, $m_i = \min\{e_i, f_i\}$, und der größte gemeinsame Teiler von a und b ist $d = p_1^{m_1} \cdots p_r^{m_r}$. Diese Überlegung macht davon Gebrauch, dass man ganze Zahlen in eindeutiger Weise in Primfaktoren zerlegen kann. Vom algorithmischen Standpunkt ist dieses Vorgehen nicht befriedigend, da die Zerlegung einer Zahl in ihre Primfaktoren sehr rechenaufwendig ist.

Beim Euklidischen Algorithmus wird anders vorgegangen; der Algorithmus beruht auf der Division mit Rest. Wie bereits aus Abschnitt 2 bekannt, gibt es zu ganzen Zahlen $a, b \neq 0$

Zahlen $m, r \in \mathbb{Z}$ mit

$$a \;=\; mb + r \;\text{ und } 0 \le r < |b|\,.$$

Euklidischer Algorithmus:

Eingabe: $a, b \in \mathbb{Z} \setminus \{0\}$.
Ausgabe: $r_{j-1} = \mathrm{ggT}(a, b)$.
Verfahren: Setze $r_{-1} = a$, $r_0 = b$. Bestimme durch Division mit Rest sukzessive $r_1, \ldots, r_{j-1}$ mit $|b| > r_1 > \cdots > r_{j-1} > r_j = 0$, bis kein Rest mehr bleibt. r_{i+1} sei also der Rest, der bei Division von r_{i-1} durch r_i entsteht:

$$\begin{aligned}
r_{-1} &= m_1 r_0 + r_1\,,\\
r_0 &= m_2 r_1 + r_2\,,\\
&\vdots\\
r_{i-1} &= m_{i+1} r_i + r_{i+1}\,,\\
&\vdots\\
r_{j-3} &= m_{j-1} r_{j-2} + r_{j-1}\,,\\
r_{j-2} &= m_j r_{j-1}\,,
\end{aligned}$$

mit $m_1, \ldots, m_j \in \mathbb{Z}$.

Termination: Da die Divisionsreste r_i strikt fallen, bricht das Verfahren nach endlich vielen Schritten ab.

Korrektheit: r_{j-1} teilt der Reihe nach $r_{j-2}, r_{j-3}, \ldots, r_0 = b$ und $r_{-1} = a$, wie sich sukzessive aus den Gleichungen $r_{i-1} = m_{i+1} r_i + r_{i+1}$ ergibt; also ist r_{j-1} ein Teiler von a und b.

Teilt umgekehrt z sowohl a als auch b, so teilt z der Reihe nach $r_1, \ldots, r_{j-1}$ wie aus den Gleichungen $r_{i+1} = r_{i-1} - m_{i+1} r_i$ folgt; also ist r_{j-1} der größte unter den Teiler von a und b.

Beispiel. Für $a = 9876$, $b = 3456$ ergibt sich

$$\begin{aligned}
9876 &= 2 \cdot 3456 + 2964\,,\\
3456 &= 1 \cdot 2964 + 492\,,\\
2964 &= 6 \cdot 492 + 12\,,\\
492 &= 41 \cdot 12\,(+\,0)\,.
\end{aligned}$$

D.h. $\mathrm{ggT}(9876, 3456) = 12$.

Dabei haben wir den *Satz von Bézout* für den Fall $n = 2$ gezeigt.

SATZ 5.1. (Bézout.) *Zu* $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ *gibt es* $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a_1, \ldots, a_n) = \lambda_1 a_1 + \cdots + \lambda_n a_n$.

BEWEIS. Der Fall $n = 2$ ist bereits geklärt. Den Fall $n \geq 2$ kann man induktiv abhandeln: Sei $d' = \lambda'_1 a_1 + \ldots + \lambda'_{n-1} a_{n-1}$ der ggT von $a_1, \ldots, a_{n-1}$ und $d = \mu_1 d' + \mu_2 a_n$ der ggT von d' und a_n. Dann ist d der ggT von $a_1, \ldots, a_n$ und als ganzzahlige Linearkombination von $a_1, \ldots, a_n$ darstellbar. □

Durch Erweiterung des Euklidischen Algorithmus kann man gleichzeitig mit dem ggT zweier Zahlen a und b auch eine Darstellung nach dem Satz von Bézout gewinnen. Man bestimmt dazu ganze Zahlen

$$\begin{array}{rclcrcl} s_{-1} & = & 1\,,\ s_0 = 0\,, & \qquad & t_{-1} & = & 0\,,\ t_0 = 1\,, \\ s_{i-1} & = & m_{i+1} s_i + s_{i+1}\,, & & t_{i-1} & = & m_{i+1} t_i + t_{i+1}\,, \end{array}$$

unter Benutzung der vom Euklidischen Algorithmus gewonnenen ganzen Zahlen $m_1, \ldots, m_j$. Dann gilt

$$\mathrm{ggT}(a, b) \;=\; r_{j-1} \;=\; a s_{j-1} + b t_{j-1}\,.$$

BEWEIS. Es gilt sogar $r_i = a s_i + b t_i$ für alle $-1 \leq i < j$. Für $i = -1, 0$ folgt dies aus der Wahl von s_{-1}, s_0, t_{-1}, t_0, und der Induktionsschritt folgt aus

$$\begin{array}{rcl} r_{i+1} & = & r_{i-1} - m_{i+1} r_i \\ & = & a s_{i-1} + b t_{i-1} - m_{i+1}(a s_i + b t_i) \\ & = & a s_{i+1} + b t_{i+1}\,. \end{array}$$

□

BEISPIEL. $a = 9876$, $b = 3456$.

i	r_{i-1}	r_i	m_{i+1}	s_{i-1}	s_i	t_{i-1}	t_i
0	9876	3456	2	1	0	0	1
					/		/
1	3456	2964	1	0	1	1	−2
2	2964	492	6	1	−1	−2	3
3	492	12	41	−1	7	2	−20

Also $\mathrm{ggT}(9876, 3456) = 12 = 7 \cdot 9876 - 20 \cdot 3456$.

Laufzeit des Euklidischen Algorithmus. Der Euklidische Algorithmus ist effizient in dem Sinne, dass die Anzahl der benötigten Divisionen logarithmisch in den Eingabedaten a und b beschränkt ist. Die worst-case Laufzeit des Algorithmus kann abgeschätzt werden, indem Eingaben a und b betrachtet werden, für die besonders viele Divisionen anfallen.

Ohne Einschränkung sei $a > b > 0$. (Im Fall $b > a > 0$ werden a und b im ersten Schritt vertauscht.) Das kleinste Paar (a, b) (formal im Sinne $(a_1, b_1) < (a_2, b_2) \iff (b_1 < b_2$ oder $(b_1 = b_2$ und $a_1 < a_2)))$, für das j Divisionen benötigt werden, ergibt sich, wenn man r_{j-1} und die m_i möglichst klein wählt: $m_1 = \ldots = m_{j-1} = 1$, $m_j = 2$ und $r_{j-1} = 1$ ($m_j = 1$ ist ausgeschlossen, da mit $r_j = 0$ dann $r_{j-1} = r_{j-2}$ folgen würde). Die Gleichungen

$$r_{j-1} = 1\,, \quad r_{j-2} = 2\,, \quad r_{i-1} = r_i + r_{i+1} \text{ für } i = j-2, \ldots, 0$$

bestimmen dann $r_{-1} = a$ und $r_0 = b$ eindeutig. Es ergibt sich ein Zusammenhang zur Fibonacci-Folge $0, 1, 1, 2, 3, 5, 8, 13 \ldots$.

Satz 5.2. *Der Euklidische Algorithmus benötigt bei der Eingabe $a > b > 0$ höchstens $c \ln(b\sqrt{5})$ Divisionen, mit $c = (\ln \frac{1+\sqrt{5}}{2})^{-1} \approx 2.08$.*

Beweis. Siehe Übungen. □

Wir können nun auch die in Satz 2.1 aufgeschobene Eindeutigkeit der Primfaktorzerlegung nachweisen.

Lemma 5.3. (Euklid.) *Wenn eine Primzahl p das Produkt ab zweier ganzer Zahlen a, b teilt, dann teilt sie mindestens einen der beiden Faktoren.*

Beweis. Wir nehmen an, dass p kein Teiler von a ist.

Zu zeigen: $p|b$.

Da p prim ist, gilt $\mathrm{ggT}(p, a) = 1$. Nach dem Satz von Bézout existieren daher $s, t \in \mathbb{Z}$ mit $sp + ta = 1$. Es folgt

$$spb + t(ab) \;=\; b\,.$$

Da p die beiden Summanden auf der linken Seite teilt, folgt $p|b$. □

Induktiv ergibt sich daraus unmittelbar: Ist ein Produkt $\prod_{i=1}^{r} a_i$ von $r > 2$ ganzen Zahlen durch die Primzahl p teilbar, so ist mindestens ein Faktor durch p teilbar.

Beweis der Eindeutigkeit der Primfaktorzerlegung in Satz 2.1. Wir nehmen an, dass es eine kleinste natürliche Zahl n mit zwei verschiedenen Primfaktorzerlegungen

$$n \;=\; p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \;=\; q_1^{f_1} q_2^{f_2} \cdots q_l^{f_l}$$

und $p_1 < \cdots < p_k$, $q_1 < \cdots < q_l$ gibt. Nach dem voranstehenden Lemma teilt jede Primzahl p_i als Teiler des rechten Produkts auch eine der Primzahlen q_j, ist also gleich

dieser Primzahl. Ebenso ist jede der Primzahlen q_j identisch mit einer der Primzahlen p_i. Es folgt die Gleichheit der Mengen

$$\{p_i : 1 \leq i \leq k\} = \{q_j : 1 \leq j \leq l\}.$$

Da die Zahlen p_i und die Zahlen q_j der Größe nach sortiert sind, erhalten wir $r = s$ und $p_i = q_i$ $(1 \leq i \leq k)$.

Annahme: Es existiert ein i mit $e_i \neq f_i$.

Sei t ein minimales solches i und ohne Einschränkung $e_t < f_t$. Division durch $n' := \prod_{i=1}^{t} p_i^{e_i}$ liefert eine Zahl

$$n'' := \frac{n}{n'} = \prod_{i=t+1}^{k} p_i^{e_i} = p_t^{f_t - e_t} \cdot \prod_{j=t+1}^{k} p_j^{f_j},$$

mit zwei verschiedenen Primfaktorzerlegungen. Wegen $n'' < n$ ist dies ein Widerspruch zur Minimalität von n.

Die Primfaktorzerlegung jeder Zahl n ist daher (bis auf die Reihenfolge der Faktoren) eindeutig. □

Aufgaben

(1) Der Euklidische Algorithmus benötigt bei der Eingabe $a > b > 0$ höchstens $c \ln(b\sqrt{5})$ Divisionen, mit $c = (\ln \frac{1+\sqrt{5}}{2})^{-1} \approx 2.08$.

Anmerkungen

Eine Division mit Rest hat man nicht nur für die ganzen Zahlen, sondern auch für wichtige andere Strukturen (z.B. Polynomringe, siehe Übungen und Abschnitt 17). Allgemein nennt man einen nullteilerfreien[3] kommutativen Ring mit Einselement einen *Euklidischen Ring*, falls eine Funktion $g : R \setminus \{0\} \to \mathbb{N}_0$ mit der folgenden Eigenschaft existiert: Zu beliebigen $a, b \in R \setminus \{0\}$ existieren $m, r \in R$, so dass $a = mb + r$ mit entweder $r = 0$ oder $g(r) < g(b)$.

Die Überlegungen zu größten gemeinsamen Teilern übertragen sich auf Euklidische Ringe. Man hat den Euklidischen Algorithmus zur Verfügung, und daher existieren größte gemeinsame Teiler im folgenden Sinne:

Definition 5.4. Sei R ein Euklidischer Ring. $d \in R$ heißt *ein größter gemeinsamer Teiler von* $a_1, \ldots, a_n \in R \setminus \{0\}$, falls

[3]Gilt für $a, b \neq 0$ die Eigenschaft $a \cdot b = 0$, dann heißen a und b Nullteiler.

i) $d|a_1, \ldots, d|a_n$,
ii) $z|a_1, \ldots, z|a_n \implies z|d$ für alle $z \in R$.

Man beachte, dass wir bei dem ggT in $\mathbb{Z}$ in Abschnitt 2 die Konvention getroffen haben, dass der ggT positiv ist.

Teil 2

Modulare Arithmetik und endliche Gruppen

6. Die Restklassenringe von $\mathbb{Z}$

Beim Rechnen mit ganzen Zahlen ist es häufig von Vorteil, nicht mit den Zahlen selbst zu operieren, sondern mit den Resten, die beim Teilen der Zahl durch einen fest vorgegebenen *Modul* $m \geq 2$ übrigbleiben.

DEFINITION 6.1. Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$.

i) a und b heißen *kongruent modulo* m, falls $m|(b-a)$, falls also a und b denselben Rest bei Division durch m haben. Schreibweise: $a \equiv b \pmod{m}$.
ii) Die Menge $\overline{a} := a + m\mathbb{Z} = \{a + mz \,:\, z \in \mathbb{Z}\}$ heißt *Restklasse* von a modulo m. Die Menge aller Restklassen wird mit $\mathbb{Z}_m$ oder $\mathbb{Z}/m\mathbb{Z}$ bezeichnet.

BEISPIEL. Beispielsweise gilt also

$$\overline{3} \;=\; 3 \;\equiv\; 15 \pmod{6}\,.$$

Die Restklasse von 3 modulo 6 ist

$$3 + 6\mathbb{Z} \;= \{\ldots, -9, -3, 3, 9, 15, 21, \ldots\}\,.$$

Wir beobachten zunächst, dass für jedes gegebene $m \geq 2$ die oben definierte Kongruenzrelation eine Äquivalenzrelation ist. Jede Äquivalenzklasse besitzt einen Vertreter in der Menge $\{0, \ldots, m-1\}$.

Wir betrachten nun Operationen auf den Restklassen. Für Restklassen $\overline{a}$, $\overline{b}$ sei

$$\begin{aligned} \overline{a} + \overline{b} \;&:=\; \overline{a+b}\,, \\ \overline{a} \cdot \overline{b} \;&:=\; \overline{a \cdot b}\,. \end{aligned}$$

In dieser Definition ist zunächst die Wohldefiniertheit zu klären. Zu einer gegebenen Restklasse modulo m gibt es unendlich viele Vertreter, so dass die angegebenen Definition nur dann sinnvoll ist, wenn die angegebene Definition unabhängig von der Wahl des Vertreters ist.

BEISPIEL. Sei $m = 3$. Die Restklasse

$$3 + 6\mathbb{Z} \;=\; \{\ldots, -9, -3, 3, 9, 15, 21, \ldots\}$$

kann beispielsweise Restklasse zu $a = 3$ oder etwa auch als Restklasse zu $a' = 21$ interpretiert werden. Die Restklasse

$$4 + 6\mathbb{Z} \;=\; \{\ldots, -8, -2, 4, 10, 16, 22, \ldots\}$$

kann beispielsweise als Restklasse zu $b = 4$ oder zu $b' = -8$ interpretiert werden.

Es gilt

$$\begin{aligned} \overline{a+b} &= (3+4)+6\mathbb{Z}\,, \\ \overline{a'+b'} &= (21+(-8))+6\mathbb{Z} \;=\; 13+6\mathbb{Z}\,. \end{aligned}$$

Diese beiden Mengen stimmen überein.

Das nachfolgende Lemma besagt, dass sowohl die Addition als auch die Multiplikation von Restklassen stets unabhängig von den gewählten Vertretern und damit wohldefiniert ist.

LEMMA 6.2. *Sei $m \geq 2$. Für Restklassenvertreter a, a', b, b' modulo m gilt*

$$a \equiv a',\, b \equiv b' \pmod{m} \implies a+b \equiv a'+b', ab \equiv a'b' \pmod{m}\,,$$

Folglich sind die angegebenen Vernüpfungen in $\mathbb{Z}_m$ wohldefiniert.

BEISPIEL. Um beispielsweise die zwei Restklassen $\overline{3}$ und $\overline{5}$ in $\mathbb{Z}_6$ zu multiplizieren, genügt es, beliebige Vertreter zu wählen, diese zu multiplieren und die zugehörige Restklasse zu betrachten. Bei Wahl der Vertreter 3 und 5 ergibt sich

$$3 \cdot 5 + 6\mathbb{Z} \;=\; 3+6\mathbb{Z}\,.$$

Bei Wahl anderer Vertreter, etwa 9 und 11 ergibt sich die gleiche Restklasse, da

$$9 \cdot 11 + 6\mathbb{Z} \;=\; 3+6\mathbb{Z}\,.$$

BEWEIS. Nach Voraussetzung gilt $m|(a-a')$ und $m|(b-b')$. Es folgt $m|(a+b-(a'+b'))$, so dass

$$a+b \equiv a'+b' \pmod{m}\,.$$

Wegen $ab - a'b' = a(b-b') + (a-a')b'$ gilt auch $m|(ab-a'b')$; folglich ist

$$a+b \equiv a'+b' \pmod{m}\,.$$

□

SATZ 6.3. *Sei $m \geq 2$. Die Menge $\mathbb{Z}_m$ bildet mit den Operationen $+$ und $\cdot$ einen kommutativen Ring mit Einselement, der als* Restklassenring modulo m *bezeichnet wird. Hierbei ist die Restklasse $\overline{0}$ von 0 das neutrale Element bezüglich der Addition und die Restklasse $\overline{1}$ von 1 das neutrale Element bezüglich der Multiplikation.*

BEWEIS. Die Rechenregeln eines Rings übertragen sich von $\mathbb{Z}$ unmittelbar auf $\mathbb{Z}_m$, z.B.

$$\overline{a} + (\overline{b} + \overline{c}) \;=\; \overline{a} + \overline{b+c} \;=\; \overline{a + (b+c)} \;=\; \overline{(a+b)+c} = (\overline{a} + \overline{b}) + \overline{c}\,.$$

Das Nullelement ist $\overline{0}$, das Einselement ist $\overline{1}$. □

BEISPIEL 6.4. *(Neunerprobe.)* Seien $a = \sum a_i 10^i$ und $b = \sum b_i 10^i$ ganze Zahlen in Dezimaldarstellung und $c = \sum c_i 10^i$ ihr Produkt. Dann gilt wegen $10 \equiv 1 \pmod 9$

$$\sum a_i \sum b_i \equiv ab \equiv c \equiv \sum c_i \pmod 9\,.$$

Die Neunerprobe zur Kontrolle von Multiplikationen (bei der jede Zahl durch die Summe ihrer Ziffern aus ihrer Dezimaldarstellung ersetzt wird) beruht auf dieser Feststellung.

Die Restklassenringe $\mathbb{Z}_m$ haben Besonderheiten, wie man sie von $\mathbb{Z}$ nicht kennt.

Nullteiler: Im Gegensatz zu $\mathbb{Z}$ kann $\mathbb{Z}_m$ Nullteiler enthalten, z.B. $\overline{2} \cdot \overline{3} = \overline{0}$ in $\mathbb{Z}_6$. Genauer gilt für $m \geq 2$: $\mathbb{Z}_m$ enthält Nullteiler $\iff$ m ist keine Primzahl.

Einheiten: Sind a und m teilerfremd, dann gibt es ein $\overline{b} \in \mathbb{Z}_m$ mit $a \cdot b \equiv 1 \pmod m$. Diese Eigenschaft folgt unmittelbar aus dem Satz von Bézout, der eine Darstellung der Form $sa + tm = 1$ mit $s, t \in \mathbb{Z}$ garantiert, d.h. für $b := s$ gilt $ab \equiv 1 \pmod m$. Elemente in $\mathbb{Z}_m$, die bezüglich der multiplikativen Operation invertiert werden können, heißen *Einheiten.*

Ein kommutativer Ring $(R, \oplus, \odot)$ mit Einselement definiert einen *Körper*, wenn $R \setminus \{0\}$ bezüglich der multiplikativen Operation eine abelsche Gruppe bildet. Endliche Körper werden in späteren Abschnitten im Detail besprochen. Wir halten jedoch bereits fest:

SATZ 6.5. *Sei $p \geq 2$. $\mathbb{Z}_p$ ist genau dann ein Körper, wenn p prim ist.*

BEWEIS. Siehe Übungen □

Aufgaben.

(1) Sei $p \geq 2$. Zeigen sie, dass $\mathbb{Z}_p$ ist genau dann ein Körper ist, wenn p prim ist.

Anmerkungen. Als Konsequenz aus den Operationen + und · auf $\mathbb{Z}_m$ sind beispielsweise auch *modulare Quadratwurzeln*, also Lösungen von Gleichungen der Form

$$x^2 \;\equiv\; a \pmod m\,,$$

oder *modulare Logarithmen*, also Lösungen von Gleichungen der Form

$$a^x \;\equiv b \pmod m$$

sinnvolle – und tatsächlich sehr wichtige – Konzepte.

7. Endliche Gruppen

Die folgenden Paare aus Mengen und Operationen sind Beispiele algebraischer Strukturen, die eine *Gruppe* definieren:

- $(\mathbb{Z}, +)$,
- $(\mathbb{Z}_n, +)$ für $n \geq 2$,
- $(\mathbb{R}, +)$,
- $(\mathbb{R} \setminus \{0\}, \cdot)$.

Wir stellen hier die wichtigsten Konzepte (endlicher) Gruppen zusammen.

DEFINITION 7.1. Eine nichtleere Menge G mit einer binären Verknüpfung $\circ : G \times G \to G$ heißt *Gruppe*, wenn folgende Bedingungen erfüllt sind.

i) $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativität) ,
ii) $\exists e \in G \quad \forall a \in G : e \circ a = a \circ e = a$ (neutrales Element) ,
iii) $\forall a \in G \quad \exists b \in G \quad a \circ b = b \circ a = e$ (inverses Element; Schreibweise a^{-1}) .

Gilt darüber hinaus Kommutativität (d.h. $a \circ b = b \circ a \; \forall a, b \in G$), dann heißt G *abelsch*.

Gelten i) und ii), dann heißt $(G, \circ)$ eine Halbgruppe.

Eine Gruppe heißt *endlich*, wenn die zu Grunde liegende Menge G endlich ist.

BEMERKUNG. Beachte, dass beispielsweise $(\mathbb{N}, +)$ und $(\mathbb{Z}, \cdot)$ keine Gruppe bilden, denn diese Mengen sind nicht bezüglich der Inversenbildung abgeschlossen.

Beachte ferner, dass nicht jede Gruppe abelsch ist; Permutationsgruppen liefern Beispiele für nicht-abelsche Gruppen.

Wir betrachten nun die Multiplikation im Restklassenring $\mathbb{Z}_n (n \geq 2)$. Aufgrund der Eigenschaft $0 \cdot x = 0 \pmod{n}$ für alle $x \in \mathbb{Z}_n$ bildet $\mathbb{Z}_n$ bezüglich der Multiplikation offensichtlich keine Gruppe; denn wegen $0 \cdot 0$ müsste 0 das neutrale Element sein, was aber im Widerspruch zu $0 \cdot x = 0 \pmod{n}$ für $x \neq 0$ steht.

Wir fragen nun, ob eventuell $\mathbb{Z}_n \setminus \{0\}$ bezüglich der Multiplikation eine Gruppe bildet? Wegen $1 \cdot x \equiv x \pmod{n}$ für alle $x \in \mathbb{Z}_n \setminus \{0\}$ kommt 1 als neutrales Element in Frage. Um die Frage nach der Existenz inverser Elemente zu klären, betrachten wir zunächst zwei Beispiele.

BEISPIEL. a) Die Multiplikation auf $\mathbb{Z}_5 \setminus \{0\}$ ist durch folgende Verknüpfungstafel gegeben:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Aus der Verknüpfungstafel ist ersichtlich, dass jedes Element ein inverses Element besitzt. $\mathbb{Z}_5 \setminus \{0\}$ definiert daher eine Gruppe bezüglich der Multiplikation.

b) Die Multiplikation auf $\mathbb{Z}_6 \setminus \{0\}$ ist durch folgende Verknüpfungstafel gegeben:

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Offensichtlich ist die Operation nicht abgeschlossen, da beispielsweise

$$2 \cdot 3 = 0 \pmod 6 .$$

Folglich kann $\mathbb{Z}_6 \setminus \{0\}$ bezüglich der Multiplikation keine Gruppe definieren.

Aus dem Beispiel mit $\mathbb{Z}_6$ ersichtlich, dass im Allgemeinen die Multiplikation in $\mathbb{Z}_n$ nicht abgeschlossen nicht. Wie im nächsten Satz präzisiert passiert dies immer dann, wenn n eine zusammengesetzte Zahl der Form $n = n_1 \cdot n_2$ mit $n_1, n_2 \geq 2$ ist. In diesem Fall gilt $n_1 \cdot n_2 = 0 \pmod n$. Tatsächlich liegt jedoch eine Gruppenstruktur vor, wenn wir uns auf die Elemente in $\mathbb{Z}_n$ beschränken, die relativ prim zu n sind.

Für $n \geq 2$ sei

$$\mathbb{Z}_n^* \;=\; \{x \in \mathbb{Z}_n \setminus \{0\} \,:\, \mathrm{ggT}(x, n) = 1\} .$$

$\mathbb{Z}_n^*$ heißt die *prime Restklassengruppe modulo n*. Aus Abschnitt 3 wissen wir, dass $|\mathbb{Z}_n^*| = \varphi(n)$, wobei $\varphi(n)$ die Eulersche φ-Funktion bezeichnet.

SATZ 7.2. *Für $n \geq 2$ definiert $\mathbb{Z}_n^*$ bezüglich der Multiplikation modulo n eine Gruppe.*

BEWEIS. Die Abgeschlossenheit der multiplikativen Operation ergibt sich dadurch, dass für $x, y \in \mathbb{Z}_n \setminus \{0\}$ mit $\mathrm{ggT}(x, n) = 1$ und $\mathrm{ggT}(y, n) = 1$ auch $\mathrm{ggT}(xy, n) = 1$ folgt. Wir wissen bereits, dass die Multiplikation modulo n assoziativ ist, und offensichtlich ist 1 das neutrale Element.

Es verbleibt, die Existenz der inversen Elemente zu zeigen. Betrachte hierzu ein $x \in \mathbb{Z}_n \setminus \{0\}$ mit $\mathrm{ggT}(a,n) = 1$. Nach dem Satz von Bézout existieren $s,t \in \mathbb{Z}$, so dass die ganzzahlige Gleichung

$$sx + tn \;=\; 1$$

erfüllt ist. Modulo n betrachtet bedeutet diese Gleichung

$$sx \equiv 1 \pmod{n}\,,$$

so dass s ein inverses Element zu x modulo n ist.[4]

Insgesamt folgt, dass $\mathbb{Z}_n^*$ bezüglich der Multiplikation modulo n eine Gruppe definiert. □

Wir betrachten nun allgemeine Eigenschaften (endlicher) Gruppen.

Satz 7.3. *Sei $(G,\circ)$ eine Gruppe und $a \in G$ ein fest gewähltes Element. Dann sind die beiden Abbildungen*

$$\begin{aligned} L_a &: G \to G\,, \quad x \mapsto a \circ x \qquad \text{(Linkstranslation)} \\ \textit{und } R_a &: G \to G\,, \quad x \mapsto x \circ a \qquad \text{(Rechtstranslation)} \end{aligned}$$

bijektiv.

Beweis. Sei $a \in G$ fest gewählt. Aus Symmetriegründen genügt es, die Linkstranslation L_a zu betrachten.

Zeige: L_a ist surjektiv.

Sei $y \in G$. Dann ist $a^{-1} \circ y$ ein Urbild von y unter L_a, denn

$$L_a(a^{-1} \circ y) \;=\; a \circ a^{-1} \circ y \;=\; y\,.$$

Zeige: L_a ist injektiv. Seien $x, y \in G$ mit $a \circ x = a \circ y$. Dann folgt durch Multiplikation mit a^{-1} von links $x = y$. □

Satz 7.4. *Sei $(G,\circ)$ eine Gruppe. Für $a,b,c \in G$ gelten die folgenden Rechenregeln:*

Involution: $a = (a^{-1})^{-1}$

Kürzungsregeln:

$$\begin{aligned} a \circ b = c \circ b \;&\Rightarrow\; a = c\,, \\ b \circ a = b \circ c \;&\Rightarrow\; a = c\,. \end{aligned}$$

[4] Für jede beliebige Gruppe gilt, dass aus der Existenz des Inversen zu einem Element a bereits folgt, dass dieses auch eindeutig ist — im Falle zweier inverser Elemente b, b' würde nämlich gelten $b \cdot 1 = b \cdot a \cdot b' = 1 \cdot b'$.

Eindeutige Lösbarkeit linearer Gleichungen:

$$\begin{aligned} a \circ x = b &\iff x &= a^{-1} \circ b\,, \\ x \circ a = b &\iff x &= b \circ a^{-1}\,. \end{aligned}$$

BEWEIS. Wir zeigen exemplarisch die Involutionseigenschaft. Für $z := (a^{-1})^{-1}$ folgt

$$z \;=\; z \circ e \;=\; z \circ (a^{-1} \circ a) \;=\; (z \circ a^{-1}) \circ a \;=\; e \circ a \;=\; a\,.$$

□

Von fundamentaler Bedeutung ist der Satz von Euler. Für eine Gruppe G bezeichnet $|G|$ die Anzahl der Elemente in G. Wir schreiben wie üblich $a^n := \underbrace{a \circ \ldots \circ a}_{n-\text{mal}}$.

SATZ 7.5. *Sei G eine endliche abelsche Gruppe. Für alle $a \in G$ gilt $a^{|G|} = e$.*

Für den Fall der primen Restklassengruppen $(\mathbb{Z}_m^*, \cdot)$ bedeutet das:

KOROLLAR 7.6. *(Satz von Euler.) Für alle $\overline{a} \in \mathbb{Z}_m^*$ gilt $\overline{a}^{\varphi(m)} = \overline{1}$.*

BEWEIS VON SATZ 7.5. Sei $n := |G|$ und $G = \{a_1, \ldots, a_n\}$. Ferner sei $a \in G$ beliebig. Aus der Bijektivität der Linkstranslation $L : G \to G, x \mapsto a \circ x$ folgt, dass dann auch $\{a \circ a_1, \ldots, a \circ a_n\} = G$. Multiplikation jeweils aller Elemente dieser beiden Vertretersysteme liefert

$$a_1 \circ \cdots \circ a_n = a \circ a_1 \circ \cdots \circ a \circ a_n$$

und nach Kürzen $a^n = e$. □

KOROLLAR 7.7. *(Kleiner Satz von Fermat.) Sei p eine Primzahl. Dann gilt für jedes $a \in \mathbb{Z}$*

$$a^p \equiv a \pmod{p}\,.$$

BEWEIS. Für $a \equiv 0 \pmod{p}$ ist die Aussage offensichtlich, und für $a \neq 0$ gilt wegen $|\mathbb{Z}_p^*| = \varphi(p) = p - 1$ die Kongruenz $a^{p-1} \equiv 1 \pmod{p}$. □

8. Die Ordnung von Gruppenelementen

Ein zentrales Konzept in einer endlichen Gruppe ist das der Ordnung eines Elements. Es gibt insbsondere eine Antwort auf die Frage, ob durch hinreichend häufiges Verknüpfen eines Elements mit sich selbst stets zum neutralen Element gelangt werden kann.

DEFINITION 8.1. Sei G eine endliche Gruppe und $a \in G$. Das kleinste $k \in \mathbb{N}$ mit $a^k = e$ heißt *Ordnung* von a.

Wir beobachten zunächst, dass jedes Element einer endlichen Gruppe G überhaupt eine endliche Ordnung besitzt. (Im Falle unendlicher Gruppen ist dies i.A. nicht gegeben; für den Fall endlicher abelscher Gruppen ist dies bereits aus dem Satz 7.5 von Euler klar.) Sei hierzu $a \in G$. Dann existiert wegen der Endlichkeit von G ein minimales $m \in \mathbb{N}$, so dass in der Folge

$$e, a, a^2, a^3, \ldots, a^m$$

nicht alle Elemente verschieden sind. Sei etwa $a^j = a^m$ mit $0 \leq j < m$. Durch Multiplikation mit a^{-j} folgt

$$e \;=\; a^{m-j}\,. \tag{8.1}$$

Wegen $m - j \in \mathbb{N}$ ist die Gruppenordnung also insbesondere endlich und durch $m - j$ nach oben beschränkt. Aufgrund der Eigenschaft (8.1) sowie der Minimalität von m folgt tatsächlich sogar $j = 0$, so dass also gilt $\mathrm{ord}(a) = m$.

Beispiel. Wir betrachten die Gruppe $\mathbb{Z}_8$ bezüglich der Addition.

a	0	1	2	3	4	5	6	7
$\mathrm{ord}(a)$	1	8	4	8	2	8	4	8

Wir stellen einige Eigenschaften der Gruppenordnung zusammen. Diese werden sich später bei der Untersuchung endlicher Körper als sehr nützlich erweisen.

Lemma 8.2. *Sei G eine endliche abelsche Gruppe und $a \in G$. Dann gilt für $k \in \mathbb{N}$:*

$$a^k = e \iff \mathrm{ord}(a) | k\,.$$

Beweis. „$\Longleftarrow$“: klar.

„$\Longrightarrow$“: Nach Definition ist $\mathrm{ord}(a)$ die kleinste natürliche Zahl l mit $a^l = e$. Folglich gilt $k \geq \mathrm{ord}(a)$. Aufgrund der Division mit Rest existieren daher $m \in \mathbb{N}$ und $0 \leq t < \mathrm{ord}(a)$ mit

$$k \;=\; m\,\mathrm{ord}(a) + t\,.$$

Wegen

$$e \;=\; a^k \;=\; a^{m\,\mathrm{ord}(a)} \circ a^t \;=\; e \circ a^t \;=\; a^t$$

folgt aus der Minimalität von $\mathrm{ord}(a)$, dass $t = 0$. □

Lemma 8.3. *Sei G eine endliche abelsche Gruppe. Für $a, b \in G$ mit teilerfremden Ordnungen gilt*

$$\mathrm{ord}(a \circ b) \;=\; \mathrm{ord}(a) \cdot \mathrm{ord}(b)\,.$$

BEWEIS. Sei $l := \mathrm{ord}(a \circ b)$, $m := \mathrm{ord}(a)$ und $n := \mathrm{ord}(b)$.

Zeige: $l|mn$.

Aus der Beziehung

$$(a \circ b)^{mn} \;=\; (a^m)^n \circ (b^n)^m \;=\; e \circ e \;=\; e\,.$$

ergibt sich mit Lemma 8.2 die Behauptung.

Zeige: $mn|l$.

Gilt für ein $k \in \mathbb{N}$ die Eigenschaft $(a \circ b)^k = e$, dann folgt $(a \circ b)^{km} = e$ und $(a \circ b)^{kn} = e$, so dass

$$\begin{aligned} e \;&=\; (a^m)^k \circ b^{mk} \;=\; b^{mk}\,, \\ \text{und } e \;&=\; a^{nk} \circ (b^n)^k \;=\; a^{nk}\,. \end{aligned}$$

Nach Lemma 8.2 ergibt sich also $n|mk$ sowie $m|nk$. Wegen $\mathrm{ggT}(m,n) = 1$ impliziert dies $m|k$ und $n|k$, also $mn|k$. Insbesondere ist mn also ein Teiler von l.

Aus den beiden Teilbarkeitsrelationen ergibt sich die Behauptung. □

LEMMA 8.4. *Sei G eine endliche abelsche Gruppe, und sei*

$$m \;=\; \max\{\mathrm{ord}(a) \,:\, a \in G\}\,.$$

Dann gilt $a^m = e$ für alle $a \in G$.

BEWEIS. Sei $a \in G$, und sei $r := \mathrm{ord}(a)$ seine Ordnung, also die kleinste natürliche Zahl, so dass $a^r = e$. Sei $b \in G$ so, dass $\mathrm{ord}(b) = m$.

Es genügt zu zeigen: $r \mid m$.

Annahme: Es existiert eine Primzahlpotenz p^i mit $p^i \mid m$, $p^{i+1} \nmid m$, aber $p^{i+1}|r$. Sei $a' := a^{r/(p^{i+1})}$, $b' := b^{(p^i)}$. Dann gilt $\mathrm{ord}(a') = p^{i+1}$ und $\mathrm{ord}(b') = m/p^i$. Insbesondere sind $\mathrm{ord}(a')$ und $\mathrm{ord}(b')$ teilerfremd, so dass nach dem voranstehenden Lemma folgt $\mathrm{ord}(a'b') = \mathrm{ord}(a')\mathrm{ord}(b')$. Also gilt $\mathrm{ord}(a'b') = pm$, im Widerspruch zur Maximalität von m. □

9. Der Chinesische Restsatz

Mit Hilfe des nachfolgend diskutierten Chinesischen Restsatzes ist es möglich, Berechnungsprobleme in kleinere Probleme aufzuteilen. Hierzu wird eine ganze Zahl a durch

ein Zahlentupel $(a_1, \ldots, a_k)$ ersetzt, das man dadurch erhält, dass man a modulo k vorgegebener, paarweise teilerfremder Moduln $m_1, \ldots, m_k$ betrachtet. Da sich das Rechnen mit a auf kanonischer Weise auf die a_i überträgt, kann daher mit den Resten modulo m_i gearbeitet werden.

Diese Strategie setzt voraus, dass man am Ende einer Rechnung eine Zahl wieder aus den Resten zurückgewinnen kann. Eine Antwort auf diese Frage der Rekonstruierbarkeit wird durch den Chinesischen Restsatz gegeben, der in einem speziellen Fall bereits Sun Tsu etwa 300 n. Chr. bekannt war.

SATZ 9.1. *Seien $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd und $a_1, \ldots, a_k \in \mathbb{Z}$. Dann existiert eine Lösung a des Systems von Kongruenzen*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_k \pmod{m_k},$$

und sie ist modulo $m := m_1 \cdot \ldots \cdot m_k$ eindeutig.

BEWEIS. *Eindeutigkeit:* Sind x und x' Lösungen, d.h. $x \equiv x' \equiv a_i \pmod{m_i}$, so gilt $m_i | (x - x')$ für alle i. Aus der Eindeutigkeit der Primfaktorzerlegung und der paarweisen Teilerfremdheit der m_i folgt $m | (x - x')$, d.h. $x \equiv x' \pmod{m}$.

Existenz: Der nachfolgende Existenzbeweis liefert gleichzeitig ein algorithmisches Verfahren zur Bestimmung von x. Seien e_i, $1 \leq i \leq k$, Lösungen des Gleichungssystems für den speziellen Fall $a_i = 1$, $a_j = 0$ für $j \neq i$ („Basislösungen“). Setze

$$m_i' := \prod_{j \neq i} m_j = \frac{m}{m_i}.$$

Da die Moduln $m_1, \ldots, m_k$ paarweise teilerfremd sind, gilt $(m_i, m_i') = 1$. Nach dem Satz von Bézout existieren daher ganze Zahlen s_i, t_i, so dass $1 = m_i s_i + m_i' t_i$, und diese Zahlen können mit dem erweiterten Euklidischen Algorithmus berechnet werden. Wir setzen nun

$$e_i := m_i' t_i = 1 - m_i s_i .$$

Dann gilt nach Definition von m_i' wie gewünscht

$$e_i \equiv \begin{cases} 1 \pmod{m_i}, \\ 0 \pmod{m_j} \quad \text{für } j \neq i . \end{cases}$$

Aus den Basislösungen können wir nun eine Lösung

$$x = \sum_{i=1}^{k} a_i e_i$$

für das Ausgangssystem zusammensetzen. □

In Restklassen ausgedrückt bedeutet das:

KOROLLAR 9.2. *Seien $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd und $m := m_1 \cdot \ldots \cdot m_k$. Dann ist die Abbildung*

$$\mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}, \quad a \bmod m \mapsto (a \bmod m_1, \ldots, a \bmod m_k)$$

bijektiv.

BEWEIS. Die Injektivität folgt aus der Eindeutigkeitssaussage. Die Surjektivität folgt alternativ aus der im Beweis angegebenen Berechnungsmethode oder aus der Tatsache, dass $\mathbb{Z}_m$ und $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ gleichmächtig sind (und damit die Injektivität unmittelbar die Surjektivität impliziert). □

BEISPIEL. Gesucht ist eine Lösung des Systems

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 4 \pmod 7 .$$

Es gilt $m_1' = 5 \cdot 7 = 35$, $m_2' = 3 \cdot 7 = 21$, $m_3' = 3 \cdot 5 = 15$. Aus

$$\begin{array}{rcccl} 1 & = & (3, 35) & = & 12 \cdot 3 - 1 \cdot 35 , \\ 1 & = & (5, 21) & = & -4 \cdot 5 + 1 \cdot 21 , \\ 1 & = & (7, 15) & = & -2 \cdot 7 + 1 \cdot 15 \end{array}$$

erhalten wir die Basislösungen $e_1 = -35$, $e_2 = 21$, $e_3 = 15$. Folglich ist

$$2 \cdot (-35) + 3 \cdot 21 + 4 \cdot 15 = 53$$

Lösung der Kongruenz.

Anwendung: *Ein probabilistischer Gleichheitstest.*

Zwei Personen an den Enden eines Nachrichtenkanals wollen zwei binäre Nachrichten der Länge < 10000 auf Gleichheit hin überprüfen. Dabei sollen möglichst wenige Bits übertragen werden. Das folgende Verfahren erlaubt einen Vergleich der beiden als Zahlen $a, b < 2^{10000}$ interpretierbaren Nachrichten, wobei anstatt der bis zu 10000 Bits für die gesamte Nachricht nur $k \cdot 101$ (bzw. $k \cdot 202$ bei erforderlicher Übertragung der Moduln) Bits gesendet werden. Wir werden sehen, dass das Verfahren schon für $k = 1$ höchste Sicherheit garantiert.

PROBABILISTISCHER GLEICHHEITSTEST:

Ausgabe: „$a \neq b$“ oder „mit großer Wahrscheinlichkeit $a = b$“

Verfahren: Wähle zufällig Primzahlen $p_1, \ldots, p_k \in [2^{100}, 2^{101})$. Übertrage a modulo p_i für alle $i = 1, \ldots, k$. Falls $a \not\equiv b \pmod{p_i}$ für ein i, gilt „$a \neq b$“. Ansonsten treffe die Entscheidung „mit großer Wahrscheinlichkeit $a = b$“

Das Verfahren setzt voraus, dass man sich die benötigten Primzahlen leicht verschaffen kann. Darauf kommen wir später zurück.

Wir schätzen nun die Wahrscheinlichkeit ab, dass das Verfahren zu einer Fehlentscheidung führt. Nehmen wir dazu zunächst an, dass es 100 verschiedene Primzahlen $q_1, \ldots, q_{100} \in [2^{100}, 2^{101})$ gibt, für die $a \equiv b \pmod{q_i}$ gilt. Nach dem Chinesischen Restsatz folgt $a \equiv b \pmod{m}$, mit $m := q_1 \cdot \ldots \cdot q_{100}$. Es gilt $m > (2^{100})^{100} = 2^{10000}$, nach Annahme folgt daher $a = b$. In diesem Fall ist eine Fehlentscheidung also ausgeschlossen.

Eine Fehlentscheidung ist also nur möglich, falls es weniger als 100 Primzahlen $q > 2^{100}$ mit der Eigenschaft $a \equiv b \pmod{q}$ gibt, und eine Fehlentscheidung tritt nur dann ein, wenn das Verfahren zufälligerweise nur derartige Primzahlen auswählt. Nach dem berühmten Primzahlsatz gilt für die Anzahl $\pi(x)$ der Primzahlen $\leq x$ die asymptotische Formel $\pi(x) \sim x/\ln x$. Zwischen 2^{100} und 2^{101} gibt es daher approximativ

$$\pi(2^{101}) - \pi(2^{100}) \approx \frac{2^{101}}{\ln 2^{101}} - \frac{2^{100}}{\ln 2^{100}} \geq \frac{1}{\ln 2^{100}}(2^{101} - 2^{100}) = \frac{2^{100}}{100 \ln 2} \geq 2^{93}\,.$$

Primzahlen. Bei k-facher unabhängiger Wahl einer Primzahl ist die Fehlerwahrscheinlichkeit also höchstens

$$\left(\frac{99}{2^{93}}\right)^k \leq 2^{-86k}\,.$$

Schon für $k = 1$ ist dies ein verschwindend kleiner Wert. Diese Schranke für die Fehlerwahrscheinlichkeit ist unabhängig von den Nachrichten a und b. Wenn wir dagegen an zufälligen Bitpositionen prüfen, erkennen wir die Ungleichheit oft nicht, wenn a und b an fast allen Bitpositionen übereinstimmen.

Eine andere Anwendung des chinesischen Restsatzes ist beispielsweise die exakte Lösung großer ganzzahliger linearer Gleichungssysteme mittels modularer Arithmetik.

10. Das RSA-Codier- und Unterschriftenschema

Die *Kryptographie* ist die Lehre von Chiffriersystemen. Wir betrachten die Situation, dass eine Person A eine geheime Nachricht an einer Person B übermitteln möchte. A codiert sie deshalb mit einer injektiven Codierabbildung

$$E : \mathcal{N} \to \mathcal{K}\,.$$

Anstelle der Nachricht $a \in \mathcal{N}$ sendet A die chiffrierte Nachricht $E(a)$. Der Empfänger decodiert mittels der inversen Abbildung

$$D = E^{-1} : \mathcal{K}' \to \mathcal{N}\,,$$

wobei $\mathcal{K}' := E(\mathcal{N}) \subset \mathcal{K}$. Ein bekanntes Verfahren beruht auf der Addition modulo 2. Wir nehmen an, dass die Nachrichten als binäre Folgen der Länge n vorliegen, d.h. $\mathcal{N} = \mathcal{K} = \{0,1\}^n$. Wir fassen die Folgen als Vektoren der Länge n über dem Körper $\mathbb{Z}_2$ auf. Zum Codieren wird ein binärer String $k = k_1 k_2 \dots k_n$ verwendet. Wir setzen

$$E(a) := a + k\,,$$

die beiden binären Folgen a und k werden also komponentenweise modulo 2 addiert. Es gilt $D = E$, denn $E + E$ bildet auf die nur aus Nullen bestehenden Folge ab. Nachrichten werden daher nach demselben Verfahren decodiert. Dieses klassische Verfahren hat den Namen 'One-time-pad'.

Es gilt $a + E(a) = k$. Gelingt es daher, eine codierte Nachricht $E(a)$ zu entschlüsseln, so kennt man k und damit bereits die vollständige Codier- und Decodiervorschrift. Ist k zufällig aus $\{0,1\}$ gewählt, so gilt dies auch für $E(a)$. Dies bedeutet, dass das Verfahren im folgenden Sinne sicher ist: Ein Unbefugter hat keine Chance, eine Nachricht zu dechiffrieren, wenn er auf k keinen Zugriff hat. Denn die gesendeten Nachrichten sind gleichverteilt auf $\{0,1\}^n$.

Das RSA-Schema. Für die klassischen Chiffrierverfahren besteht ein Sicherheitsproblem darin, dass man die Codiervorschrift- und Decodiervorschrift geheimhalten muss (beim One-time-pad also k) und zuvor vereinbaren muss. Diffie und Hellman haben 1976 den (damals völlig neuartigen) Vorschlag der sogenannten *Public-key-Kryptographie* gemacht. Jeder Teilnehmer des Systems besitzt einen öffentlichen Schüssel k und einen geheimen Schlüssel k'. D und E müssen die Eigenschaft haben, dass E leicht berechnet werden kann, D ohne Kenntnis von k' sehr "schwer" berechenbar ist, mit Kenntnis von k' jedoch leicht (*Trapdoor-Funktion*).

Das bekannteste öffentliche Chiffriersystem ist das 1978 von Rivest, Shamir und Adleman vorgeschlagene *RSA-Schema*. Es beruht darauf, dass es schwer ist, eine Zahl m in ihre Primfaktoren zu zerlegen.

Erzeugen eines Schlüsselspaares: Seien p, q sehr große Primzahlen (z.B. 1024 Bits), $N := pq$. Sei $e \in \mathbb{Z}^*_{\varphi(N)}$, d.h. $\mathrm{ggT}(e, \varphi(N)) = 1$, $d = e^{-1} \pmod{\varphi(N)}$.
Öffentlicher Schlüssel: (N, e).
Geheimer Schlüssel: d.
Codieren: Aufteilen von Nachrichten in Blöcke der Bitlänge $\leq \log_2 N$ und Betrachtung jedes Blockes als Zahl in $\mathbb{Z}_N$. $E : \mathbb{Z}_N \to \mathbb{Z}_N$, $E(x) = x^e \pmod{N}$.
Decodieren: $D : \mathbb{Z}_N \to \mathbb{Z}_N$, $D(y) = y^d \pmod{N}$.

BEISPIEL. Sei $p = 41$, $q = 19$. Dann ist $N = 41 \cdot 19 = 779$ und $\varphi(N) = 40 \cdot 18 = 720$. Wird als Codierexponent e etwa $e = 103$ gewählt, dann ist $d = 7$ (da $d \cdot e = 721 \equiv 1 \pmod{\varphi(N)}$).

Wir verschlüsseln nun einen durch die Zahl 5 gegebenen Nachrichtenblock lautet. Das Exponentieren erfolgt zweckmäßigerweise durch das Herausziehen von Zweierpotenzen und sukzessives Quadrieren,

$$5^{103} = 5^{64} \cdot 5^{32} \cdot 5^4 \cdot 5^2 \cdot 5^1 .$$

Wegen $5^4 = 625$, $5^8 = 625^2 \equiv 346 \pmod{779}$, $5^{16} = (5^8)^2 \equiv 346^2 \equiv 529 \pmod{779}$, $5^{32} = (5^{16})^2 \equiv 529^2 \equiv 180 \pmod{779}$, $5^{64} = (5^{32})^2 \equiv 180^2 \equiv 461 \pmod{779}$ ergibt sich

$$\begin{aligned} 5^{103} &\equiv 461 \cdot 180 \cdot 625 \cdot 25 \cdot 5 \\ &\equiv 207 \pmod{779} . \end{aligned}$$

Entschlüsselt man die Zahl 207 wieder, ergibt sich

$$\begin{aligned} 207^7 &\equiv (207^4) \cdot (207^2) \cdot 207 \\ &\equiv 16 \cdot 4 \cdot 207 \\ &\equiv 5 \pmod{779} . \end{aligned}$$

Das nachstehende Lemma formalisiert, dass die Decodierfunktion die Inverse der Codierfunktion ist:

LEMMA 10.1. $(x^e)^d \equiv (x^d)^e \equiv x \pmod{N}$.

BEWEIS. Nach Konstruktion von e und d gilt

$$e \cdot d = 1 + \nu\varphi(N) \quad \text{mit } \nu \in \mathbb{Z} .$$

Falls $x \in \mathbb{Z}_N^*$, dann gilt nach dem Satz von Euler

$$x^{ed} = x^{1+\nu\varphi(N)} \equiv x \pmod{N} .$$

Es verbleibt, die Ausage für $x \notin \mathbb{Z}_N^*$ zu zeigen. Nach dem Chinesischen Restsatz ist die Abbildung

$$\begin{aligned} \mathbb{Z}_N &\to \mathbb{Z}_p \times \mathbb{Z}_q \\ x &\mapsto (x \bmod p, x \bmod q) \end{aligned}$$

bijektiv. Für $x = 0$ gilt die Behauptung des Lemmas offensichtlich. Gilt o.B.d.A. $x \equiv 0 \pmod{p}$ und $x \not\equiv 0 \pmod{q}$, dann folgt $x^{ed} \equiv 0 \pmod{p}$ sowie aus dem kleinen Satz von Fermat $x^{ed} \equiv x \pmod{q}$, d.h., $x^{ed} \equiv x \pmod{N}$. □

Analyse: Die Kenntnis von $\varphi(N) = (p-1)(q-1)$ ist praktisch äquivalent zur Kenntnis der Faktorisierung von N, denn wegen (o.B.d.A. $p > q$)

$$\begin{aligned} \varphi(N) &= (p-1)(q-1) \quad \Longrightarrow p+q = N - \varphi(N) + 1 \\ p-q &= \sqrt{(p+q)^2 - 4pq} \;=\; \sqrt{(N-\varphi(N)+1)^2 - 4N} \end{aligned}$$

ist die Bestimmung von $\varphi(N)$ etwa genau so schwierig wie die Primfaktorzerlegung von N – und Faktorisierungsalgorithmen brauchen sehr viel Zeit. Ist also nur N, nicht aber die Faktorisierung bekannt, so kann man d $(= e^{-1} \pmod{\varphi(N)})$ praktisch nicht bestimmen. Ein offenes Problem ist, ob die Decodierung auch ohne Kenntnis von d möglich ist.

Um ein Gefühl für die Schwierigkeit des Faktorisierens großer Zahlen zu vermitteln, dienen die folgenden Anhaltspunkte. Im Jahr 1977 wurde in der Zeitschrift Scientific American eine 129-stellige Dezimalzahl (Bitlänge 429) als Herausforderung für das RSA-System veröffentlicht (und ein Preisgeld von \$100 ausgeschrieben). Diese Zahl wurde erst 1994 faktorisiert (unter Beteiligung von 600 Freiwilligen und einem Rechenaufwand von ca. 5000 MIPS-Jahren). Es folgten größere Herausforderungen und höhere Preisgelder. Im Jahr 2003 wurde mit 5-monatiger Rechenleistung auf 120 Maschinen die Zahl RSA-576 der Bitlänge 576 faktorisiert (Preisgeld \$10.000), und im Jahr 2005 wurde die Zahl RSA-640 der Bitlänge 640 faktorisiert (Preisgeld \$20.000). Aktuell sind \$100.000 auf eine Zahl RSA-1024 (309 Dezimalstellen) ausgeschrieben und \$200.000 auf eine Zahl RSA-2048 (617 Dezimalstellen).

Signaturschema: Das RSA-System kann auch zur Beglaubigung von Nachrichten verwendet werden (*Digitale Unterschrift*). Jeder Teilnehmer A und B besitzt einen öffentlichen Schüssel (N_A, e_A) bzw. (N_B, e_B) sowie einen geheimen d_A bzw. d_B.

Nachricht von A an B: $x \mapsto E_B(x) \;=\; x^{e_B}$
Entschlüsselung durch B: $D_B(E_B(x)) \;=\; (x^{e_B})^{d_B} \;=\; x \pmod{N_B}$
Unterschrift von A: durch Mitteilung von $c := D_A^{-1}(x) = x^{d_A} \pmod{N_A}$
Verifikation der Unterschrift durch B: durch Überprüfung, dass
$x = c^{e_A} \pmod{N_A}$.

Beispiel. In obigem Beispiel mit $N = 779$, $e = 103$, $d = 7$ soll die Nachricht 3 signiert werden. Der Teilnehmer berechnet

$$3^7 \;\equiv\; 629 \pmod{779}\,.$$

Zur Verifikation der berechneten Unterschrift 629 überprüft man, dass 629^{103} modulo 779 wieder mit der Nachricht übereinstimmt:

$$629^{103} \;\equiv\; 3 \pmod{779}\,.$$

11. Primalitätstests

Für das RSA-Schema benötigt man große zufällige Primzahlen. Da die Primzahlen $\leq N$ etwa die Dichte $\frac{1}{\ln N}$ haben, genügt ein effektiver Primalitätstest. Naive Verfahren (etwa „Dividiere einen Kandidaten N durch alle Primzahlen $p \leq \sqrt{N}$“) sind für die relevanten Größenordnungen nicht praktikabel.

Viele Primalitätstest beruhen auf Ideen des kleinen Satzes von Fermat. Nach diesem gilt: Sei $N \in \mathbb{N}$. Falls ein $a \in \mathbb{N}$, $0 < a < N$ mit $a^{N-1} \not\equiv 1 \pmod{N}$ existiert, dann ist N keine Primzahl.

Definition 11.1. Sei N eine zusammengesetzte Zahl. N heißt *pseudoprim* zur Basis a, falls N die Eigenschaft $a^{N-1} \equiv 1 \pmod{N}$ erfüllt. N heißt *Carmichael-Zahl*, falls N pseudoprim für alle $a \in \mathbb{Z}_N^*$ ist.

Ob eine Zahl N Carmichael-Zahl ist, kann man probabilistisch einfach testen. Die $a \in \mathbb{Z}_N^*$, welche die Fermat-Identität erfüllen, bilden eine Untergruppe von $\mathbb{Z}_N^*$. Die Ordnung dieser Untergruppe ist entweder $\varphi(N)$ oder (nach dem Satz von Lagrange) höchstens $\varphi(N)/2$. Explizit kann man dies auch wie folgt sehen: Seien $a_1, \ldots, a_k \in \mathbb{N}$ alle Elemente aus $\mathbb{Z}_N^*$ mit $a_i^{N-1} \equiv 1 \pmod{m}$. Gibt es ein $a \in \mathbb{Z}_N^*$ mit $a^{N-1} \not\equiv 1 (\mathrm{mod}\ N)$, dann gilt für $b_i := a \cdot a_i$ („Linkstranslation“):

$$b_i^{N-1} = a^{N-1} a_i^{N-1} \not\equiv 1 \pmod{N},$$

es gibt daher mindestens ebenso viele Elemente in $\mathbb{Z}_N^*$, die die Fermatsche Identität nicht erfüllen. D.h. $k \leq \varphi(N)/2$.

Korollar 11.2. (r-facher Fermat-Test.) *Gibt es zu $N \in \mathbb{N}$ ein $a \in \mathbb{Z}_N^*$ mit $a^{N-1} \not\equiv 1 \pmod{N}$, dann gilt für zufällige, unabhängige $a_1, \ldots, a_r \in \mathbb{Z}_N^*$*

$$\mathrm{Ws}\left(a_i^{N-1} \equiv 1 \pmod{N} \text{ für } 1 \leq i \leq r\right) \leq 2^{-r}.$$

Der r-fache Fermat-Test kann die Zusammengesetztheit einer Nicht-Carmichael-Zahl mit Wahrscheinlichkeit $\geq 1 - 2^r$ erkennen und nachweisen. Die Zusammengesetztheit von Carmichael-Zahlen kann er nicht erkennen. Für viele praktische Anwendungen ist der Fermat-Test jedoch bereits ausreichend, da Carmichael-Zahlen nur selten vorkommen. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Bis Anfang der 90er Jahre war unbekannt, ob es überhaupt unendlich viele Carmichael-Zahlen gibt.

Satz 11.3. (Alford, Granville, Pomerance; Annals of Mathematics, 1994). *Es existieren unendlich viele Carmichael-Zahlen.*

Die Anzahl $C(x)$ der Carmichael-Zahlen kleiner oder gleich x ist für hinreichend große x beschränkt durch $x^{2/7} < C(x) < x^{1-(\ln\ln\ln x)/(\ln\ln x)}$.

Der sogenannte *Primzahltest von Miller-Rabin* erweitert den Fermat-Test auf Carmichael-Zahlen. Mit dem Miller-Rabin-Test kann man die Zusammengesetztheit einer nicht primen, ungeraden Zahl mit Wahrscheinlichkeit mindestens $\frac{3}{4}$ in Polynomialzeit beweisen.

SATZ 11.4. *Sei $N \in \mathbb{N}$ zusammengesetzt und ungerade, $N-1 = 2^k t$ mit ungeradem t. Dann gilt für zufälliges $a \in \mathbb{Z}_N^*$:*

$$\mathrm{Ws}\left(a^t \equiv 1 \pmod N \text{ oder } \exists i \in \{0,\dots,k-1\} \quad a^{2^i t} \equiv -1 \pmod N\right) \le \frac{1}{4}.$$

BEWEIS. Siehe D.E. Knuth, The Art of Computer Programming, Vol. 2 (1981), Aufgabe 4.5.4 (22) oder R. Crandall, C. Pomerance, Prime Numbers: A computational perspective (2001), Theorem 3.4.4. □

DEFINITION 11.5. Sei $\mathcal{R}$ die Klasse der Sprachen $L \subset \{0,1\}^*$, für die es einen Polynomialzeit-Algorithmus gibt, der zu $x \in L$ mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ einen Beweis für $x \in L$ findet.

Aus dem Miller-Rabin-Test folgt, dass die Menge der zusammengesetzten Zahlen in $\mathcal{R}$ liegt. Umgekehrt zeigen Adleman, Huang (1992), dass es einen probabilistischen Algorithmus polynomialer Laufzeit gibt, der nach k Durchläufen entweder eine definitive Antwort auf die Frage der Primalität einer gegebenen Zahl liefert (Irrtum ausgeschlossen) oder gar keine Antwort gibt (letzteres mit Wahrscheinlichkeit kleiner 2^k). In der Sprache der Komplexitätstheorie heißt das, dass die Menge der Primzahlen in der Klasse $\mathcal{ZPP}$ enthalten ist. Zum Erwürfeln eines Primalitätsbeweises konstruiert man geeignete elliptische Kurven; die Beweisskizze von Adleman, Huang ist 140 Seiten lang. In jüngster Zeit wurde schließlich ein deterministischer Polynomialzeit-Primalitätstest gefunden:

SATZ 11.6. (Agrawal, Kayal, Saxena, 2002.) *Die Menge der Primzahlen ist in Polynomialzeit entscheidbar.*

Die derzeitigen praktikabelsten Primzahltests für „allgemeine“ Zahlen beruhen auf elliptischen Kurven. Darüber hinaus gibt es spezialisierte Tests für Zahlen besonderer Bauart, insbesondere für Fermat-Zahlen und Mersenne'sche Zahlen. Eine *Fermat-Zahl* ist eine Zahl der Form $2^{2^n}+1$ mit $n \in \mathbb{N}_0$. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sind prim. Bis heute ist jedoch keine weitere Fermat-Primzahl bekannt (bisher sind die Faktorisierungen von $F_5 = 641 \cdot 6700417$ bis F_{12} bekannt). Eine *Mersenne'sche Zahl* ist eine Zahl der Form $2^p - 1$ mit p prim). Diese Zahlen sind nicht immer prim (z.B. $23 | 2^{11}-1$), Prime Mersennesche Zahlen waren aber oft „Rekord“-Primzahlen, etwa im Jahr 2007: $2^{32582657}-1$ (hat 9808368 Dezimalstellen).

Teil 3

Graphentheorie

12. Graphen

In diesem Abschnitt werden Graphen als ein grundlegendes Konzepte der diskreten Mathematik eingeführt. Sehr schnell wird in den darauffolgenden Abschnitten ersichtlich, dass sich einige einfach zu formulierende Probleme als sehr weitreichend und schwierig erweisen.

Wir beginnen mit folgendem Beispielproblem:

> Beweisen Sie, dass auf einer Party mit 73 Personen immer eine Person existiert, die eine gerade Anzahl von anderen Personen kennt.

Wir setzen hierbei voraus, dass Bekanntschaft immer auf Gegenseitigkeit beruht (d.h. eine symmetrische Relation ist). Eine abstrakte Darstellung des Problems führt unmittelbar auf das Konzept eines Graphen, in dem Bekanntschaft durch Kanten modelliert wird.

DEFINITION 12.1. Ein *Graph* ist ein Paar $G = (V, E)$, wobei V eine nichtleere endliche Menge ist und E eine Menge zweielementiger Teilmengen von V. Die Elemente von V heißen *Knoten* von G und die Elemente von E *Kanten*.

Die Namen Knoten und Kanten deuten auf die bildliche Darstellung hin, mit der wir uns einen Graph vorstellen.

BEISPIEL 12.2. (i) Für $n \in \mathbb{N}$ bezeichnet K_n den vollständigen Graphen auf n Knoten, d.h. $E = \{(u, v) : u, v \in V \text{ mit } u \neq v\}$.

(ii) Für $n \in \mathbb{N}$ ist ein *Kreis* $C_n = (E_n, V_n)$ gegeben durch eine Menge $V_n = \{v_1, \ldots, v_n\}$ von verschiedenen Knoten $v_1, \ldots, v_n$ mit $\{v_i, v_{i+1}\} \in E_n$ sowie $\{v_n, v_1\} \in E_n$.

Wie für jede Struktur existiert ein natürlicher Isomorphiebegriff, den wir implizit in der Wahl der Bezeichnungen in dem voranstehenden Beispiel bereits verwendet haben.

DEFINITION 12.3. Zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ heißen *isomorph*, wenn es eine bijektive Abbildung $\varphi : V_1 \to V_2$ gibt, so dass für alle $u, v \in V_1$ gilt:

$$\{u, v\} \in E_1 \iff \{\varphi(u), \varphi(v)\} \in E_2 \,.$$

Beispielsweise sind also je zwei vollständige Graphen auf n Knoten isomorph, so dass hierdurch die Bezeichnung *„den“ vollständigen Graphen* des voranstehenden Beispiels gerechtfertigt wird.

Wir stellen einige Grundbegriffe zusammen. Ist $\{u, v\} \in E$, so nennen wir u und v *benachbart* oder *adjazent*. Falls $v \in V$ und $e \in E$ mit $v \in e$ gilt, sagen wir, dass v und e

inzident sind. Die Anzahl der Nachbarn eines Knotens v heißt *Grad von* v und wird mit $\deg(v)$ abgekürzt.

Die einführende Aufgabe wird nun durch die folgende Grapheneigenschaft beantwortet.

SATZ 12.4. *Jeder Graph hat eine gerade Anzahl von Knoten ungeraden Grades.*

BEWEIS. Seien V_g und V_u die Knoten geraden bzw. ungeraden Gerades. Dann gilt

$$2|E| \;=\; \sum_{v\in V} \deg(v) \;=\; \sum_{v\in V_g} \deg(v) + \sum_{v\in V_u} \deg(v)\,.$$

Da die linke Seite und der erste Summand rechts gerade Zahlen sind, muss auch der zweite Summand gerade ein. Also muss die Anzahl $|V_u|$ der Summanden gerade sein. □

Im folgenden soll die Struktur zweier grundlegender Graphenklassen untersucht werden: bipartiter Graphen und Bäume. Hierzu benötigen wir zunächst einige weitere Begriffe. Ein *Weg (Pfad)* in einem Graphen besteht aus einer Folge $v_1, \ldots, v_k$ von verschiedenen Knoten mit $\{v_i, v_{i+1}\} \in E$ für alle $i \in \{1, \ldots, k-1\}$. Die *Länge* eines Weges ist die Anzahl $k-1$ der Kanten $\{v_i, v_{i+1}\}$. Ein Graph G heißt *zusammenhängend*, falls jeder Knoten in G von jedem anderen durch einen Weg erreicht werden kann.

Ein *Kreis* ist eine Folge von verschiedenen Knoten $v_1, \ldots, v_k$ mit $\{v_i, v_{i+1}\} \in E$, $1 \le i \le k$ (modulo k). Die Länge des Kreises ist die Anzahl k der Kanten. (Mit anderen Worten: Der durch $V' = \{v_1, \ldots, v_k\}$ und $E' = \bigcup_i \{v_i, v_{i+1}\}$ definierte *Untergraph* ist ein Kreis im Sinne von Beispiel 12.2).

DEFINITION 12.5. Ein Graph $G = (V, E)$ heißt *bipartit*, wenn die Knotenmenge V in zwei disjunkte Teilmengen S und T zerlegt werden kann, so dass alle Kanten von G von der Form $\{s, t\}$ mit $s \in S$, $t \in T$ sind.

SATZ 12.6. *Ein Graph G mit $n \ge 2$ Knoten ist genau dann bipartit, wenn alle Kreise gerade Länge haben. Insbesondere ist G also bipartit, wenn überhaupt keine Kreise existieren.*

BEWEIS. Durch Betrachtung der einzelnen Komponenten können wir o.B.d.A. annehmen, dass G zusammenhängend ist.

„$\Longrightarrow$“: Sei G bipartit mit den Knotenmengen S und T. Die Knoten eines Kreises sind abwechselnd in S und T enthalten, so dass der Kreis gerade Länge hat.

„$\Longleftarrow$“: Wähle einen beliebigen Knoten $u \in V$ und setze $u \in S$. Die Mengen S und T definieren wir nun weiter mittels

$$v \in \begin{cases} S & \text{falls } d(u,v) \text{ gerade,} \\ T & \text{falls } d(u,v) \text{ ungerade,} \end{cases}$$

wobei $d(u,v)$ die Länge eines kürzesten Weges von u nach v bezeichne.

Es verbleibt zu zeigen, dass keine zwei Knoten aus S benachbart sind. (Und analog für T.)

Annahme: Es existieren $v, w \in S$ mit $\{v,w\} \in E$.

Dann folgt, dass $|d(u,v) - d(u,w)| \leq 1$ und daher $d(u,v) = d(u,w)$, da beide Zahlen gerade sind. Sei P ein u-v-Weg der Länge $d(u,v)$ und P' ein u-w-Weg der Länge $d(u,w)$. Bezeichnet x den letzten gemeinsamen Knoten von P und P', dann definiert der Weg $P(x,v), vw, P'(w,x)$ einen Kreis ungerader Länge. Widerspruch. (Beachte, dass in der Definition von x erlaubt ist, dass die Wege $P(u,x)$ und $P'(u,x)$ verschieden sind; in diesem Fall haben sie jedoch zwingend die gleiche Länge.) □

Bemerkung 12.7. Der Beweis liefert einen effizienten Algorithmus zur Entscheidung, ob ein Graph bipartit ist.

Wir charakterisieren nun die Klasse der Bäume.

Definition 12.8. Ein Graph heißt ein *Baum*, falls er zusammenhängend ist und keine Kreise enthält.

Satz 12.9. *Die folgenden Bedingungen sind äquivalent:*

(1) $G = (V,E)$ *ist ein Baum.*
(2) *Je zwei Knoten in* G *sind durch genau einen Weg verbunden.*
(3) G *ist zusammenhängend, und es gilt* $|E| = |V| - 1$.

Beweis. „(1) $\Longrightarrow$ (2)“: Falls zwei Knoten u und v existierten, die durch zwei Wege verbunden sind, so wäre in der Vereinigung dieser Wege ein Kreis enthalten.

„(2) $\Longrightarrow$ (1)“: Ist C ein Kreis, so sind je zwei Knoten aus C durch zwei verschiedene Wege verbunden.

„(1) $\Longrightarrow$ (3)“: O.B.d.A. sei $n \geq 2$. Wir zeigen zunächst, dass ein Baum mindestens einen Knoten vom Grad 1 besitzt. Sei nämlich $P = v_0 v_1 \dots v_k$ ein längster Pfad in G, so sind alle Nachbarn von v_0 in P enthalten. Da G keine Kreise hat, folgt $\deg(v_0) = 1$. Wir entfernen v_0

und die inzidente Kante $\{v_0, v_1\}$ und erhalten einen Baum $G_1 = (V_1, E_1)$ auf $n-1$ Knoten mit $|V_1|$ - $|E_1| = |V| - |E|$ Kanten. Induktiv erhalten wir nach $n-2$ Schritten einen Baum G_{n-2} auf 2 Knoten, d.h., $G_{n-2} = K_2$, und es gilt $|V| - |E| = |V_{n-2}| - |E_{n-2}| = 1$.

„(3) $\Longrightarrow$ (1)“: Sei T ein aufspannender Baum von G, d.h., ein Baum auf der Knotenmenge V, dessen Kantenmenge eine Teilmenge von E ist. Nach dem zuvor bewiesenen Beweisschritt gilt $|V(T)| - |E(T)| = 1$, so dass

$$1 = |V(G)| - |E(G)| \leq |V(T)| - |E(T)| = 1\,.$$

Es folgt $E(G) = E(T)$, d.h. $G = T$. □

Bemerkung 12.10. Eigenschaft (3) ist sehr einfach zu testen; Zeit $O(|V| + |E|)$.

13. Planare Graphen

Eine besonders wichtige und interessante Klasse bilden die Graphen, die sich in der Ebene ohne Überschneidungen zeichnen lassen. Dabei wird man jede Kante formal als eine Jordankurve darstellen: Eine Jordankurve des $\mathbb{R}^n$ ist eine Menge der Form

$$\{f(t) : t \in [0,1]\}\,,$$

wobei $f : [0,1] \to \mathbb{R}^n$ eine injektive stetige Abbildung ist. Anschaulich gesprochen sind Jordankurven also schnittpunktfreie Kurven mit Anfangs- und Endpunkt.

Definition 13.1. Ein Graph $G = (V, E)$ heißt *planar*, wenn er in den $\mathbb{R}^2$ so eingebettet werden kann, dass sich die Jordankurven je zweier Kanten nicht im Inneren schneiden.

Jede planare Einbettung eines Graphen unterteilt die Ebene in zusammenhängende Gebiete, die man *Flächen* bzw. *Seiten* nennt. Zur formalen Begründung dieses anschaulich einsichtigen Sachverhalts benötigt man den sogenannten Jordanschen Kurvensatz, auf den wir hier nicht näher eingehen.

Ein planarer Graph kann sehr verschiedene planare Einbettungen haben.

Beispiel 13.2. Zwei planare Einbettungen des gleichen Graphen:

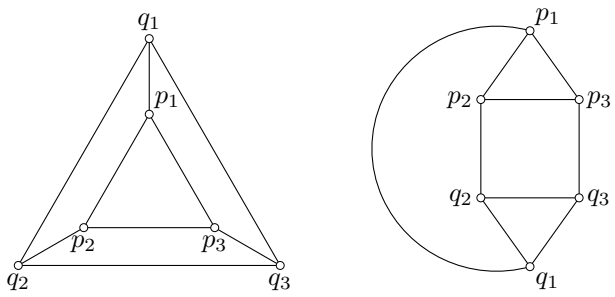

ABBILDUNG 1. $G = (V, E)$

Die folgende berühmte Formel zeigt, dass die Anzahl f der Flächen (einschließlich der äußeren Fläche) dabei immer gleich ist, also eine *Invariante* des Graphen.

SATZ 13.3. *(Euler-Formel.) Sei f die Anzahl der Flächen eines zusammenhängenden, eingebetteten planaren Graphen mit n Knoten und m Kanten. Dann gilt*

$$n - m + f \;=\; 2\,.$$

BEWEIS. Wir beweisen die Aussage durch Induktion nach der Anzahl m der Kanten.

Für $m = 0$ gilt $n = f = 1$, so dass die zu zeigende Aussage offensichtlich ist.

Wir nehmen nun an, dass die Euler-Formel für Graphen mit $m-1$ Kanten bereits bewiesen ist. Sei G ein zusammenhängender, eingebetteter planarer Graph mit m Kanten.

Fall 1: G ist ein Baum.

Dann gilt $m = n - 1$ und $f = 1$, woraus die Behauptung folgt.

Fall 2: G ist kein Baum.

Durch Weglassen einer Kante e von G, die in einem Kreis von G enthalten ist, erhält man einen Teilgraphen G'. Nach Induktionsannahme erfüllt G' die Euler-Formel. Jede planare Einbettung von G entsteht durch das Hinzufügen der Kante e zu einer planaren Einbettung von G'. Hierdurch wir eine Fläche der Einbettung in zwei Teile geteilt (zur formalen Begründung dieses anschaulich einsichtigen Sachverhalts benötigt man wieder den Jordanschen Kurvensatz). Folglich erhöhen sich bei diesem Übergang m und f um 1, und n bleibt konstant, woraus die zu zeigende Aussage folgt. □

Wir zeigen als nächstes folgende Hilfsaussage:

LEMMA 13.4. *Sei $G = (V, E)$ ein planarer Graph. Dann besitzt G einen Knoten vom Grad höchstens 5.*

BEWEIS. O.B.d.A. können wir annehmen, dass G zusammenhängend ist und dass $m \geq 3$. Dann besitzt jede Seite mindestens drei begrenzende Kanten. Bezeichnet f_i die Anzahl der Seiten mit i begrenzenden Kanten, dann lässt sich die Gesamtzahl f der Seiten als

$$f \;=\; f_3 + f_4 + f_5 + \cdots$$

ausdrücken. Für die Anzahl m der Kanten gilt

$$2m \;\geq\; 3f_3 + 4f_4 + \cdots,$$

da das Innere jeder Kante an höchstens zwei Flächen anstößt. Aus diesen beiden Gleichungen folgt $2m - 3f \geq 0$.

Annahme: Jeder Knoten hat Grad mindestens 6.

Bezeichnet n_i die Anzahl der Knoten vom Grad i, dann folgen die Darstellungen

$$\begin{aligned} n &= n_6 + n_7 + n_8 + \cdots, \\ 2m &= 6n_6 + 7n_7 + 8n_8 + \cdots, \end{aligned}$$

woraus $2m - 6n \geq 0$ folgt.

Aus den beiden hergeleiteten Ungleichungen ergibt sich

$$6(m - n - f) \;=\; (2m - 6n) + 2(2m - 3f) \;\geq\; 0$$

und folglich $m \geq n + f$. Dies ist jedoch ein Widerspruch zur Euler-Formel. □

Sei K_n der vollständige Graph auf n Knoten und $K_{m,n}$ der „vollständige bipartite“ Graph mit m und n Knoten.

KOROLLAR 13.5. *Die Graphen K_5 und $K_{3,3}$ sind nicht planar.*

BEWEIS. Im vorherigen Beweis haben wir gesehen, dass für jeden planaren Graphen mit $m \geq 3$ Kanten gilt, dass $2m \geq 3f$. Durch Einsetzen in die Euler-Formel ergibt sich $3n - m \geq 6$. Der K_5 besitzt 5 Knoten und 10 Kanten, so dass er nicht planar ist.

Gilt $m \geq 2$, und besitzt der planare Graph keine Kreise der Länge 3, dann verschärft sich die Bedingung $2m \geq 3f$ zu $2m \geq 4f$, und es folgt $2n - m \geq 4$. Der $K_{3,3}$ besitzt 6 Knoten und 9 Kanten, so dass er folglich nicht planar ist. □

Die Bedeutung dieser beiden Graphen liegt darin, dass *jeder* nichtplanare Graph eine „Unterteilung“ eines dieser beiden Graphen als Teilgraphen enthält.

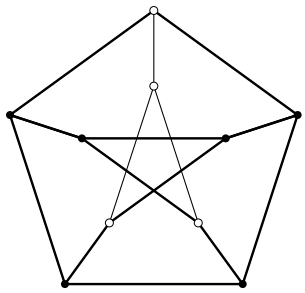

ABBILDUNG 2. Petersen-Graph

DEFINITION 13.6. Sei $G = (V, E)$ ein Graph, $\{a, b\}$ eine Kante von G und x ein *nicht* in V enthaltenes Element. Der Graph $G' = (V', E')$ entsteht *durch Einfügen des Knotens x in die Kante $\{a, b\}$*, falls $V' = V \cup \{x\}$ und $E' = (E \setminus \{\{a, b\}\}) \cup \{\{a, x\}, \{x, b\}\}$. Ein Graph H heißt eine *Unterteilung* eines Graphen G, wenn er aus G durch sukzessives Einfügen endlich vieler neuer Knoten gewonnen werden kann.

SATZ 13.7. *(Kuratowski, 1930.) Ein endlicher Graph ist genau dann planar, wenn er keine Unterteilung des K_5 oder des $K_{3,3}$ als Teilgraph enthält.*

Die eine Richtung des Beweises ist aus Korollar 13.5 bereits bekannt. Der Beweis der Umkehrung ist sehr aufwendig, und wir führen ihn hier nicht. Auf der Grundlage des Satzes von Kuratowski existieren effiziente Algorithmen zum Testen der Planarität eines Graphen.

BEISPIEL 13.8. Der in Abbildung 2 dargestellte Petersen-Graph ist nicht planar, da er eine Unterteilung des $K_{3,3}$ als Teilgraphen enthält.

Wir betrachten nun die „platonischen Körper“.

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

Bezeichnet n die Anzahl der Knoten, m die Anzahl der Kanten und f die Anzahl der Flächen, dann gilt ebenso wie in der graphentheoretischen Euler-Formel in Satz 13.3 für jeden platonischen Körper die Beziehung $n - m + f = 2$. Dies ist kein Zufall, sondern

liegt daran, dass wir den „Kantengraphen“ der platonischen Körper durch eine der Seitenflächen hindurch betrachten können (wobei die gewählte Seitenflächen dann zur äußeren Seitenfläche wird).

Anmerkung. Planare Graphen sind also solche, die man auf der zweidimensionalen Sphäre im $\mathbb{R}^3$ einbetten kann, und für sie gilt die Euler-Formel. Die Euler-Formel und ihre Verallgemeinerungen spielen in der Topologie eine fundamentale Rolle, und die Untersuchung dieser Konzepte im Rahmen der Graphentheorie bezeichnet man als topologische Graphentheorie.

14. Färbbarkeit

Bereits im vorigen Jahrhundert wurde die Frage untersucht, wie viele Farben man zur Färbung einer Landkarte benötigt, wenn Länder mit gemeinsamer Grenze verschiedene Farben bekommen sollen (wir gehen hierbei davon aus, dass jedes Land zusammenhängend ist). A priori ist nicht klar, ob es eine Konstante K gibt, so dass auch beliebig große Landkarten mit höchstens K Farben gefärbt werden können. Bereits seit vielen Jahren ist bekannt, dass es eine solche Konstante K gibt. Es war jedoch lange Zeit ein offenes Problem, ob man sogar immer mit vier Farben auskommt. Im Jahr 1977 zeigten Appel und Haken mittels eines computergestützten Beweises (spätere Vereinfachung von Robertson, Sanders, Seymour, Thomas, 1996):

Satz 14.1. *Jede Landkarte kann so mit vier Farben gefärbt werden, dass benachbarte Länder immer verschiedene Farben haben.*

Da jede Landkarte als Einbettung eines planaren Graphen aufgefasst werden kann, hat das Vier-Farben-Problem als ein fundamentales Problem sehr stark zur Entwicklung der Graphentheorie beigetragen. Wir wollen hier die Graphenmodellierung untersuchen und eine abgeschwächte Version des Satzes zeigen.

Um das Landkartenproblem in ein Graphenproblem zu überführen, werden die Länder als Knoten eines Graphen betrachtet (man wähle also etwa die Hauptstadt des Landes als Vertreter). Haben zwei Länder eine gemeinsame Grenze, dann werden die zugeordneten Knoten durch eine Kante verbunden. (Dieser Graph ist planar, was man sich z.B. dadurch überlegen kann, dass man als Kanten zwischen zwei Hauptstädten eine Bahnlinie zwischen ihnen wählt, die nur einmal die Grenze überschreitet.) Man spricht auch von dem „dualen“ Graphen der ursprünglichen Karte. (Zur Präzisierung: Die gemeinsame Grenze zwischen zwei Ländern muss nicht unbedingt zusammenhängend sein. In diesem Fall reicht es zur Untersuchung von Färbungen aus, die Hauptstädte der Länder durch eine einzige Kante zu verbinden.)

DEFINITION 14.2. Ein Graph G heißt *k-färbbar*, wenn jedem Knoten des Graphen eine von k Farben zugeordnet werden kann, so dass benachbarte Knoten verschieden gefärbt sind. Die *chromatische Zahl* $\chi(G)$ von G ist definiert als die kleinste natürliche Zahl k, für die G eine k-Färbung besitzt.

BEISPIEL 14.3. Für den vollständigen Graphen K_n auf n Knoten gilt $\chi(K_n) = n$. Für einen Kreis C_{2n} gerader Länge gilt $\chi(C_{2n}) = 2$. Für einen Kreis C_{2n+1} ungerader Länge gilt $\chi(C_{2n+1}) = 3$.

Mit dieser Notation lässt sich der Vier-Farben-Satz wie folgt formulieren:

SATZ 14.4. *Jeder planare Graph G ist 4-färbbar, d.h., $\chi(G) \leq 4$.*

Wir zeigen hier eine schwächere Version:

SATZ 14.5. *Jeder planare Graph ist 6-färbbar.*

BEWEIS. Nach Lemma 13.4 besitzt jeder planare Graph G einen Knoten v vom Grad höchstens 5. Wir entfernen v und alle zu v inzidenten Kanten. Der resultierende Graph $G' = G \setminus \{v\}$ ist ein planarer Graph auf $n-1$ Knoten. Nach Induktionsannahme besitzt er daher eine 6-Färbung. Da v höchstens fünf Nachbarn in G besitzt, werden in dieser Färbung für die Nachbarn höchstens 5 Farben benutzt. Wir können daher jede 6-Färbung von G' zu einer 6-Färbung von G erweitern, indem wir v eine Farbe zuweisen, die keinem Nachbarn in der Färbung von G' zugewiesen wurde. Folglich besitzt G eine 6-Färbung. □

15. Der Heiratssatz

Wir untersuchen nun die folgende grundlegende Frage, die dem Abschnitt seinen Namen gibt. Gegeben sei eine Menge $S = \{1, \ldots, n\}$ von Jungen und eine Menge $T = \{1, \ldots, n\}$ von Mädchen. Jeder Junge i hat eine Teilmenge L_i der Mädchen im Kopf, die er bereit wäre zu heiraten (und wir gehen hier zur Vereinfachung davon aus, dass auch das Mädchen hierzu bereit wäre). Unter welchen Bedingungen ist es möglich, dass jeder Junge ein Mädchen seiner Wahl heiraten kann. (Hierbei seien nur monogame Ehen erlaubt.)

Wir modellieren die Situation durch einen bipartiten Graphen mit Knotenmenge $S \cup T$. Eine Kante von $i \in S$ nach $j \in T$ existiert also genau dann, wenn $j \in L_i$. Für eine Teilmenge A von S bezeichnet $N(A)$ die Menge der Nachbarn von A.

Eine offensichtlich notwendige Bedingung für die Existenz einer vollständigen Heirat („eines perfekten Matchings“) ist, dass für alle $A \subseteq S$ die Eigenschaft $|A| \leq |N(A)|$ erfüllt ist. Der folgende Heiratssatz von Hall besagt, dass diese Bedingung auch hinreichend ist.

SATZ 15.1. *(Heiratssatz von Hall, 1935.) Sei der bipartite Graph $G = (S \cup T, E)$ gegeben. Dann existiert genau dann ein vollständige Heirat, wenn $|A| \leq |N(A)|$ für alle $A \subseteq S$.*

Wir geben hier einen elementaren Beweis per Induktion an und werden später – bei Betrachtung des Matching-Problems vom Standpunkt der kombinatorischen Optimierung – von einem höheren Standpunkt auf die Thematik zurückkommen.

BEWEIS. „$\Longrightarrow$“: klar.

„$\Longleftarrow$“: Für $n = 1$ ist nichts zu zeigen. Sei nun $n > 1$, und wir nehmen an, dass für alle Teilmengen A von S die Voraussetzung erfüllt ist. Wir nennen eine Teilmenge A von S mit $1 \leq |A| < n$ *kritisch*, wenn $|N(A)| = |A|$.

Fall 1: Es existiert keine kritische Teilmenge.

Wähle einen Knoten k aus der Nachbarschaftsmenge des Knoten $n \in S$. Wir entfernen k aus T und betrachten für $i \in \{1, \ldots, n-1\}$ die Listen $L_i' = L_i \setminus \{k\}$. Da nach Voraussetzung keine kritische Teilmenge existiert, besitzt jede Teilmenge A von S in dem durch die Listen L_i' neu definierten Graphen mindestens $|A|$ Nachbarn. Nach Induktionsvoraussetzung existiert eine vollständige Heirat auf dem induzierten bipartiten Graphen, die wir zusammen mit der Paarung von $n \in S$ und $k \in T$ zu einer vollständigen Heirat komplettieren können.

Fall 2: Es existiert eine kritische Teilmenge.

Nach Umnummerierung der Mengen können wir davon ausgehen, dass $A_0 = \{1, \ldots, l\}$ mit $l < n$ kritisch ist. Idee ist es nun, zunächst diese Menge zu verheiraten und dann zu zeigen, dass auch die verbleibenden Elemente die Induktionsvoraussetung erfüllen.

Nach Induktionsvoraussetzung existiert eine vollständige Heirat zwischen den Elementen von A_0 und $N(A_0)$. Wir betrachten nun $S' := S \setminus A_0$. Für jede Teilmenge A von S' hat $N(A_0 \cup A) = N(A_0) \cup N(A)$ nach Voraussetzung mindestens $|A_0 \cup A| = |A_0| + |A|$ Nachbarn. Folglich hat A mindestens $|A|$ Nachbarn, die nicht in $N(A_0)$ enthalten sind. Die Induktionsvoraussetzung lässt sich daher auch auf den induzierten bipartiten Graphen mit den Knotenmengen S' und $T \setminus A_0$ anwenden und liefert eine vollständige Heirat auf diesem induzierten Graphen. Durch Kombination der beiden Teilheiraten ergibt sich die Behauptung. □

Teil 4

Endliche Körper

In den Abschnitten 7–8 hatten wir einige Grundaspekte der Struktur endlicher Gruppen diskutiert. In den nachfolgenden Abschnitten behandeln wir nun die Kernaussage der Struktur endlicher Körper. Endliche Körper bilden die Grundlage für die im daran anschließenden Teil untersuchten fehlerkorrigierenden Codes.

16. Endliche Körper

Wir erinnern zunächst an die bereits früher verwendete Definition eines Körpers: Ein kommutativer Ring $(R, \oplus, \odot)$ mit Einselement definiert einen *Körper*, wenn $R \setminus \{0\}$ bezüglich der multiplikativen Operation eine abelsche Gruppe bildet. Etwas anders formuliert heißt das:

LEMMA 16.1. *Eine Menge K zusammen mit zwei Operationen $\oplus : K \times K \to K$, $\odot : K \times K \to K$ bildet einen Körper, wenn es zwei verschiedene, mit „0“, „1“ bezeichnete Elemente in K gibt, so dass*

(1) *$(K, \oplus)$ bildet eine abelsche Gruppe mit neutralem Element 0;*
(2) *$(K \setminus \{0\}, \odot)$ bildet eine abelsche Gruppe mit neutralem Element 1;*
(3) *$a \odot (b \oplus c) = a \odot b \oplus a \odot c$ für alle $a, b, c \in K$ (Distributivität).*

Im Folgenden bezeichnet $K^* := K \setminus \{0\}$ die Menge der multiplikativ invertierbaren Elemente eines Körpers.

Beispiele von Körpern mit unendlich vielen Elementen sind etwa $\mathbb{R}$, $\mathbb{Q}$ oder $\mathbb{C}$ bezüglich der gewöhnlichen Addition und Multiplikation.

Aus der Definition eines Körpers ergeben sich unmittelbar die folgenden Rechenregeln:

LEMMA 16.2. *Sei $(K, +, \cdot)$ ein Körper. Dann gilt für alle $a, b \in K$:*

(1) $a \cdot 0 = 0 \cdot a = 0$.
(2) *$ab = 0 \Longrightarrow a = 0$ oder $b = 0$, d.h., Körper sind nullteilerfrei.*

BEWEIS. Für die erste Aussage beobachten wir

$$0 + (a \cdot 0) \;=\; a \cdot 0 \;=\; a \cdot (0 + 0) \;=\; (a \cdot 0) + (a \cdot 0)\,,$$

wobei die letzte Gleichung aus der Distributivität folgt. Durch Kürzen in der additiven Gruppe $(K, +)$ folgt dann die Behauptung.

Für die zweite Aussage betrachten wir $a, b \in K$ mit $ab = 0$. Falls $a \neq 0$, dann existiert ein multiplikatives inverses Element a^{-1}, so dass

$$b \;=\; 1 \cdot b \;=\; a^{-1} \cdot a \cdot b \;=\; a^{-1} \cdot 0 \;=\; 0\,,$$

wobei die letzte Gleichheit auf der ersten Teilaussage des Lemmas beruht. □

In Satz 6.5 haben wir gesehen, dass es für jede Primzahl p einen endlichen Körper $\mathbb{Z}_p$ mit p Elementen gibt. Es stellt sich daher die natürliche Frage nach weiteren endlichen Körpern. Diese werden für die anschließend betrachteten Fragen der Codierungstheorie sehr nützlich sein.

Beispiel. Ein Beispiel für einen endlichen Körper, dessen Elementeanzahl keine Primzahl ist, ist durch die folgenden Additions- und Multiplikationstabellen gegeben.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Analog zu dem Isomorphiebegriff auf früher behandelten Strukturen (z.B. Graphen) bezeichnen zwei Körper als isomorph, wenn sie nur durch Umbezeichnung der Elemente auseinander hervorgehen:

Definition 16.3. Zwei Körper $(K, +, \cdot)$ und $(K', \oplus, \odot)$ heißen *isomorph*, wenn es eine bijektive Abbildung $\phi : K \to K'$ gibt, so dass für alle $x, y \in K$ gilt

$$\phi(x + y) \;=\; \phi(x) \oplus \phi(y)\,, \quad \phi(x \cdot y) \;=\; \phi(x) \odot \phi(y)\,.$$

Bemerkung. Es gilt dann $\phi(0_K) = 0_{K'}$, $\phi(1_K) = 1_{K'}$ sowie für alle $x \in K^*$ die Eigenschaft $\phi(x)^{-1} = \phi(x^{-1})$ (da $\phi(x) \odot \phi(x^{-1}) = \phi(x \cdot x^{-1}) = \phi(1_K) = 1_{K'}$).

In den nachfolgenden Abschnitten werden wir folgende Strukturergebnisse zeigen:

- Für jeden endlichen Körper ist die Elementeanzahl eine Primzahlpotenz p^m (p prim, $m \in \mathbb{N}$).
- Zu jeder solchen Primzahlpotenz p^m existiert tatsächlich ein endlicher Körper. (Wir werden sehen, wie wir diese Körper konstruieren können.)
- Je zwei endliche Körper mit der gleichen Elementanzahl sind isomorph.

Bemerkung. Die letzte Eigenschaft ist insofern sehr bemerkenswert, da etwa für endliche Gruppe eine solche Isomorphieaussage nicht gilt; beispielsweise sind die beiden durch die

folgenden Gruppentafeln gegebenen Gruppen nicht isomorph:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	4	1	2

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

($(\mathbb{Z}_4, +)$ und die *Kleinsche Vierergruppe*).

Ein wichtiges Konzept bei der Untersuchung von Körpern ist die *Charakteristik*.

Definition 16.4. Sei K ein Körper mit multiplikativem neutralem Element 1. Das kleinste $p \in \mathbb{N}$ mit

$$\underbrace{1+1+\ldots+1}_{p-\text{mal}} \;=\; 0$$

heißt *Charakteristik* von K. Schreibweise: $\text{char}(K) = p$. Existiert kein solches $p \in \mathbb{N}$, wird $\text{char}(K) = 0$ gesetzt.

Im Endlichkeitsfall ist $\text{char}(K)$ also die Ordnung des multiplikativen neutralen Elements in der additiven Gruppe $(K, +)$.

Definition 16.5. Ist $(K, +, \cdot)$ ein Körper und L eine Teilmenge von K, die mit $+$ und $\cdot$ selbst ein Körper ist, dann heißt L ein *Unterkörper* von K (und K ein *Oberkörper* oder *Erweiterungskörper* von L).

Lemma 16.6. *Sei K ein Körper mit endlicher Charakteristik p. Dann gilt:*

i) *p ist eine Primzahl.*
ii) *Für jedes $a \in K$ gilt $\underbrace{a+a+\ldots+a}_{p-mal} = 0$.*
iii) *Die Elemente 0, 1, $2 := 1+1$, $3 := 1+1+1$, …, $p-1 := 1+1+\ldots+1$ bilden einen Unterkörper P von K. Man nennt P den* Primkörper *von K.*

Beweis. i) *Annahme:* p habe eine Darstellung $p = st$ mit $s, t \geq 2$.

Dann gilt nach dem Distributivgesetz

$$\begin{aligned} 0 &= \underbrace{1+1+\ldots+1}_{p-\text{mal}} \\ &= (\underbrace{1+1+\ldots+1}_{s-\text{mal}}) \cdot (\underbrace{1+1+\ldots+1}_{t-\text{mal}}). \end{aligned}$$

Da $(K^*, \cdot)$ eine Gruppe bildet, muss einer der beiden Faktoren Null sein. Hierdurch ergibt sich ein Widerspruch zur Minimalität in der Definition der Charakteristik.

ii) $a + a + \ldots + a = a \cdot (1 + 1 + \ldots + 1) = a \cdot 0 = 0$.

iii) Der Primkörper P von K ist isomorph zu $\mathbb{Z}_p$. □

Wir können jeden endlichen Körper $(K, +, \cdot)$ (und jeden seiner Unterkörper) als einen Vektorraum über seinem Primkörper P auffassen (also auch als Vektorraum über einem Körper $\mathbb{Z}_p$). Als additive Verknüpfung zwischen zwei „Vektoren“ wählen wir hierbei die Körperaddition und als Skalarmultiplikation (die also eine Abbildung $P \times K \to K$ ist) die Körpermultiplikation.

Wir überzeugen uns davon, dass die Axiome eines Vektorraums erfüllt sind. Die additive Operation auf den „Vektoren“ definiert eine abelsche Gruppe, da $(K, +)$ eine abelsche Gruppe ist. Für alle „Skalare“ $\lambda, \mu \in P$ und alle „Vektoren“ $x, y \in K$ gilt außerdem

$$(\lambda + \mu)x = \lambda x + \mu x\,, \quad \lambda(x + y) = \lambda x + \mu y\,, \quad (\lambda\mu)x = \lambda(\mu x)\,, \quad 1x = x\,,$$

denn dasselbe gilt nach Definition sogar für alle $\lambda, \mu \in K$. Damit sind alle Vektorraumaxiome erfüllt. Jeder endliche Vektorraum hat eine endliche Dimension. Ist also K endlich und von der Dimension m über P, mit $|P| = \mathrm{char}(K) = p$, dann gilt $|K| = p^m$. Wir halten fest:

Satz 16.7. *Für jeden endlichen Körper ist die Anzahl der Elemente eine Primzahlpotenz.*

Ein endlicher Körper (engl. Galois field) mit q Elementen wird oft mit $\mathrm{GF}(q)$ oder kürzer mit $\mathbb{F}_q$ bezeichnet. Wir werden bald sehen, dass es für jede Primzahlpotenz $q = p^n$ bis auf Isomorphie genau einen Körper mit q Elementen gibt. Die Primkörper können also mit $\mathbb{F}_p$, p prim, bezeichnet werden; sie sind isomorph zu $\mathbb{Z}_p$.

Für die Untersuchung der weiteren genannten Eigenschaften endlicher Körper ist es zweckmäßig, Körper als „Restklassenringe über Polynomringen“ zu interpretieren. Hierzu stellen wir im nachfolgenden Abschnitt die Grundlagen bereit.

17. Polynome und ihre Restklassenringe

Über jedem (endlichen oder unendlichen) Körper können Polynome betrachtet werden.[5]

[5] Allgemeiner können auch Polynomringe über Ringen betrachtet werden.

Sei K ein Körper. Wir betrachten die Menge $K[x]$ aller (formalen) Polynome $a_n x^n + \ldots + a_1 x + a_0$ mit $a_i \in K$. Zwei Polynome gelten als gleich, wenn sie sich nur um Summanden unterscheiden, deren Koeffizienten 0 sind (die Polynome 0 und $x^2 + x$ in $\mathbb{Z}_2[x]$, die beide überall Null sind, sind beispielsweise sind diesem Sinne verschieden.) Addition und Multiplikation zweier Polynome $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{j=0}^{n} b_j x^j$ sind definiert durch

$$\begin{aligned} f + g &:= \sum_{i=0}^{n} (a_i + b_i) x^i \quad \text{(o.B.d.A. } m = n\text{)}, \\ f \cdot g &:= \sum_{i=0}^{m+n} c_i x^i \quad \text{mit } c_i := \sum_{j+k=i} a_j b_k \,. \end{aligned}$$

Durch diese beiden Operationen wird ein kommutativer Ring mit Einselement definiert, der *Polynomring in der Unbestimmten x über dem Körper K*. Kurz: $(K[x], +, \cdot)$ oder einfach $K[x]$.

Der Körper K ist in $K[x]$ durch die Polynome vom Grad 0 eingebettet. Ein Einselement in K ist auch ein Einselement in $K[x]$. Man sagt, $K[x]$ entsteht aus K durch Adjunktion einer Unbestimmten x.

Beispiel. (i) Sei $K = \mathbb{R}$. Dann ist $f := 2x^3 + 5x^2 + 3x + 4$ ein Polynom vom Grad 3 über K.

(ii) Sei $K = \mathbb{Z}_3$. Dann ist $f := 2x^2 + x + 2$ ein Polynom vom Grad 2 über K.

Beachte, dass stets das Polynom p selbst und die durch das Polynom p definierte *Polynomfunktion* $p : K \to K$ zu unterscheiden sind.

Sei K ein Körper. In analoger Weise zur Restklassenbildung von $\mathbb{Z}$ kann eine Restklassenbildung auf dem Polynomring $K[x]$ ausgeführt werden.

Sei $m = m(x)$ ein Polynom (vom Grad ≥ 1) mit Koeffizienten in K. Zwei Polynome $a(x)$ und $b(x)$ heißen *kongruent* modulo m, falls

$$a(x) \;=\; b(x) + q(x) m(x)$$

mit einem Polynom $q(x) \in K[x]$. Schreibweise: $a \equiv b \pmod{m(x)}$. Hierdurch wird eine Äquivalenzrelation auf $K[x]$ definiert. Die Äquivalenzklasse

$$\overline{a} \;:=\; \{b \in K[x] \,:\, a \equiv b \pmod{m(x)}\}$$

heißt *Restklasse von a.*

Die Addition und die Multiplikation überträgt sich auf die Restklassen, denn aus $a \equiv a' \pmod{m(x)}$, $b \equiv b' \pmod{m(x)}$ folgt die Existenz zweier Polynome $h_1, h_2 \in K[x]$ mit

$a - a' = h_1 m$ und $b - b' = h_2 m$, so dass $a + b - (a' + b') = (h_1 + h_2)m$ und $ab - a'b' = (a - a')b + a'(b - b') = (h_1 b + h_2 a)m$, d.h. $a + b = a' + b' \pmod m$ und $ab = a'b' \pmod m$. Die Operationen $\overline{a} + \overline{b} := \overline{a + b}$ und $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ auf den Restklassen sind also wohldefiniert. Die Menge der Restklassen zusammen mit den darauf definierten Operationen bildet einen Ring, den *Restklassenring modulo f* (bzw. *Restklassenring modulo dem von f erzeugten Ideal*). Notation: $K[x]/(f)$.

Definition 17.1. Ein nichtkonstantes Polynom $f \in K[x]$ heißt *irreduzibel* über K, falls für alle $g, h \in K[x]$ gilt

$$f = gh \quad \Longrightarrow \quad \operatorname{grad} f = 0 \text{ oder } \operatorname{grad} g = 0.$$

Wir haben früher bereits gesehen, dass für Polynome aus $K[x]$ das Konzept der Teilbarkeit, eine Division mit Rest und damit ein größter gemeinsamer Teiler erklärt ist. In analoger Weise zum Lemma von Euklid (Lemma 5.3) und der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ lassen sich daher zeigen:

Lemma 17.2. *Sei K ein Körper und f ein nichtkonstantes, irreduzibles Polynom aus $K[x]$. Teilt p das Produkt ab zweier Polynome $a, b \in K[x]$, dann teilt p mindestens einen der beiden Faktoren.*

Satz 17.3. *Sei K ein Körper. In $K[x]$ kann jedes nichtkonstante Polynom als Produkt endlich vieler irreduzibler Elemente dargestellt werden. Diese Zerlegung ist eindeutig bis auf konstante Faktoren und die Reihenfolge. Genauer: Hat ein Polynom f vom Grad mindestens 1 die Primfaktorzerlegungen $f = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$, so folgt $r = s$, und nach einer geeigneten Permutation der q_i gilt $p_i = e_i q_i$ mit Konstanten $e_i \in K^*$ für $i \in \{1, \ldots, r\}$.*

(Tatsächlich gilt eine solche Eigenschaft für jeden „faktoriellen“ Ring. $K[x]$ ist ein faktorieller Ring.)

Anmerkung. Allgemeiner kann in der Ringtheorie „modulo“ einem Ideal gerechnet werden. Auf diese Weise lassen sich neue Ringe erzeugen. Wir betrachten hierzu einen kommutativen Ring R mit Einselement.

Definition 17.4. Eine Teilmenge I von R heißt *Ideal*, wenn folgende beiden Bedingungen erfüllt sind:

i) $(I, +)$ ist eine Untergruppe von $(R, +)$.
ii) Für alle $r \in R$ gilt $rI \subset I$ und $Ir \subset I$.

Ist I ein Ideal, dann wird, wie man leicht nachprüft, in R durch $a \equiv b \ :\Longleftrightarrow a - b \in I$ eine Äquivalenzrelation erklärt. Wir schreiben dann

$$a \equiv b \bmod I$$

und nennen a und b *kongruent modulo* I. Die Relation ist mit der Addition und der Multiplikation verträglich, denn aus $a - a', b - b' \in I$ folgt $a + b - (a' + b') \in I$ und $ab - a'b' = (a - a')b + a'(b - b') \in I$. Wir können daher (in Analogie zum Restklassenring $\mathbb{Z}_m$) die Restklassen $\overline{a} = a + I$, $a \in R$ betrachten, und die Operationen $\overline{a} + \overline{b} := \overline{a + b}$, $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ auf den Restklassen sind wohldefiniert. Dieser Ring wird als *Restklassenring* oder *Faktorring* R/I bezeichnet. Speziell erhalten wir bei der Wahl $R = \mathbb{Z}$ und $I = m\mathbb{Z}$ den Restklassenring $\mathbb{Z}_m$.

18. Endliche Körper und irreduzible Polynome

Wir wollen zeigen, wie zu jeder Primzahlpotenz p^m ein endlicher Körper mit p^m Elementen konstruiert werden kann. Da ein endlicher Körper als Vektorraum über seinem Primkörper aufgefasst werden kann, können die Körperelemente als Tupel $(k_0, k_1, \ldots, k_{m-1})$ geschrieben werden, mit den Elementen k_i des Primkörpers. Es wird sich als vorteilhaft herausstellen, solche Tupel formal als Polynome $k_{m-1}x^{m-1} + \ldots + k_1 x + k_0$ zu interpretieren.

In diesem Abschnitt untersuchen wir daher die Konstruktion von Körpern durch Restklassenringe von Polynomen. Auf dieser Grundlage können wir dann die gewünschte Konstruktionsaussage für gegebenes p^m herleiten.

Unter der Voraussetzung, dass ein irreduzibles Polynom f vom Grad m in $\mathbb{Z}_p[x]$ bekannt ist, lässt sich ein endlicher Körper mit p^m Elementen wie folgt konstruieren.

Satz 18.1. *Sei K ein Körper und $f \in K[x] \setminus \{0\}$. Dann ist $K[x]/(f)$ genau dann ein Körper, wenn f irreduzibel ist. Ist $K = \mathbb{Z}_p$ und f irreduzibel vom Grad m, dann besitzt der Körper $\mathbb{Z}_p[x]/(f)$ genau p^m Elemente.*

Beweis. „$\Leftarrow$“ Zu zeigen: a) $(K[x]/(f)) \setminus \{0\}$ ist multiplikativ abgeschlossen, d.h. aus $\overline{g}, \overline{h} \neq 0$ in $K[x]/(f)$ folgt $\overline{g}\overline{h} \neq 0$ in $K[x]/(f)$.
b) Zu jedem $\overline{g} \in (K[x]/(f)) \setminus \{0\}$ existiert ein multiplikatives Inverses, d.h. ein $\overline{h} \neq 0$ mit $\overline{g}\overline{h} = 1$.

Alle anderen Körperaxiome sind offensichtlich erfüllt.

Zu a) Seien $g, h \in K[x]$ mit $\overline{g}, \overline{h} = 0$ in $K[x]/(f)$. Dann existiert ein $a \in K[x]$ mit $gh = af$. Also teilt f das Produkt gh. Hieraus und aus Lemma 17.2) folgt, dass f ein Teiler von

g oder von h ist. Im ersten der beiden Fälle gilt $g = bf$ für ein $b \in K[x]$, also $\overline{g} = 0$ in $K[x]/(f)$, und analog im zweiten Fall $\overline{h} = 0$ in $K[x]/(f)$.

Zu b) Sei $\overline{g} \in K[x]/(f)$. Aufgrund der Division mit Rest können wir annehmen, dass der Grad des Repräsentanten g die Eigenschaft grad $g <$ grad f erfüllt. Da f irreduzibel ist, folgt $\mathrm{ggT}(f, g) = 1$. Nach dem Satz von Bézout existieren daher $r, s \in K[x]$ mit $rf + sg = 1$, d.h. die Restklasse $\overline{s}$ ist Inverses zu $\overline{g}$ in $K[x]/(f)$.

„$\Rightarrow$“ Sei $f = gh$ mit $g, h \notin K$. Dann sind die Restklassen $\overline{g}$, $\overline{h}$ zwei von Null verschiedene Elemente in $K[x]/(f)$. Es gilt jedoch

$$\overline{g}\overline{h} \;=\; \overline{f} \;=\; \overline{0}$$

d.h. $\overline{g}$ und $\overline{h}$ sind Nullteiler in $K[x]/(f)$. $K[x]/(f)$ ist also kein Körper .

Die Anzahl der Elemente ergibt sich unmittelbar aus der Tatsache, dass $\mathbb{Z}_p$ der Primkörper von $\mathbb{Z}_p[x]$ ist. □

Beispiel 18.2. Das Polynom $f := x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel. Folglich bilden die Polynome 0, 1, x, $x + 1$ einen 4-elementigen Körper, wenn jeweils modulo f gerechnet wird. Die zugehörigen Additions- und Multiplikationstabellen lauten also.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Die im voranstehenden Satz beschriebene Möglichkeit zur Konstruktion endlicher Körper ist diejenige, welche bei der späteren Betrachtung fehlerkorrigierender Codes verwendet wird. Sie beruht jedoch auf der Existenz irreduzibler Polynome vom Grad m in $\mathbb{Z}_p[x]$. Eine Möglichkeit zur Klärung dieser Frage ist, mittels Erzeugendenfunktionen und Möbius-Inversion die genaue Anzahl der irreduziblen Polynome N_m vom Grad m zu berechnen; wir zeigen in Abschnitt 20, dass $N_m \geq 1$.

19. Isomorphie endlicher Körper gleicher Mächtigkeit

Das Ziel dieses Abschnitts ist es zu zeigen, dass je zwei endliche Körper gleicher Kardinalität isomorph sind.

Satz 19.1. *Zwei endliche Körper K und K' gleicher Mächtigkeit sind isomorph.*

Wir benötigen hierzu ein weiteres Konzept: das Minimalpolynom eines Körperelements.

Ist K ein Erweiterungskörper eines Körpers K_0, dann können wir in gleicher Weise wie oben für Primkörper K_0 erläutert den Körper K als Erweiterungskörper von K_0 auffassen.

Definition 19.2. Sei K ein endlicher Erweiterungskörper eines Körpers K_0. Ist $\alpha \in K$ und $g \in K_0[x] \setminus \{0\}$ ein normiertes Polynom mit $g(\alpha) = 0$ von kleinstmöglichem Grad, dann heißt g *Minimalpolynom* von α über K_0.

Beispiel. In umserem einführenden Beispiel aus Abschnitt 16 gilt (modulo 2) $1 \cdot a^2 + 1 \cdot a + 1 = 0$, das Minimalpolynom des Elements a über dem zweielementigen Primkörper lautet daher $x^2 + x + 1 = 0$.

Für jedes α existiert ein Minimalpolynom endlichen Grades, da die Folge $1, \alpha, \alpha^2, \ldots, \alpha^m$ in dem Vektorraum K über K_0 für ein endliches m linear abhängig wird.

Lemma 19.3. *Sei K ein endlicher Erweiterungskörper eines Körpers K_0. Ist $g \in K_0[x] \setminus \{0\}$ ein Minimalpolynom von $\alpha \in K$ über K_0 und $f \in K_0[x]$ ein beliebiges Polynom mit $f(\alpha) = 0$, dann gilt $g|f$. Insbesondere ist das Minimalpolynom eindeutig bestimmt.*

Beweis. Division von f durch g liefert $f = sg + r$ mit grad $r <$ grad g. Setzt man $x = \alpha$, dann ergibt sich $r(\alpha) = 0$. Aufgrund der Gradminimalität eines Minimalpolynoms folgt $r = 0 \in K_0[x]$. □

Lemma 19.4. *In jedem q-elementigen endlichen Körper K gilt*

$$\prod_{a \in K} (x - a) \;=\; x^q - x\,.$$

Beispiel. In dem Beispiel aus Abschnitt 16 gilt etwa die folgende Gleichung in $(\mathbb{Z}_2[x]/(x^2 + x + 1))[X]$ (zur Unterscheidung bezeichnen wir die Unbestimmte aus Lemma 19.4 mit einem großen X):

$$\begin{aligned}(X - 0)(X - 1)(X - x)(X - (x + 1)) &= (X^2 - X)(X^2 - X - 1)\\ &= X^4 - X\,.\end{aligned}$$

Beweis. Die multiplikative Gruppe $(K \setminus \{0\}, \cdot)$ hat genau $q - 1$ Elemente. Nach Satz 7.5 erfüllen alle $a \in K \setminus \{0\}$ daher die Gleichung $a^{q-1} = 1$. Also ist jedes $a \in K$ (insbesondere

auch $a = 0$) eine Nullstelle des Polynoms $x^q - x$. Aufgrund der eindeutigen Zerlegung in irreduzible Elemente in $K[x]$ wird $x^q - x$ daher auch von dem Produkt der $x - a$ geteilt,

$$\prod_{a \in K} (x - a) \mid x^q - x \,.$$

Beide Polynome haben den Grad q, und der Koeffizient von x^q ist in beiden Fällen gleich 1. Deshalb sind die Polynome gleich. □

SATZ 19.5. *Ist K ein endlicher Körper, so ist K^* bezüglich der Multiplikation eine zyklische Gruppe, d.h. K^* besteht aus den Elementen $1, \alpha, \alpha^2, \ldots, \alpha^{|K|-2}$ für ein geeignetes $\alpha \in K^*$. Man nennt ein solches α ein* primitives Element *von K.*

BEWEIS. Sei $q := |K|$ und m die maximale Ordnung m der Elemente aus K^*. Da $m \leq q-1$, genügt es zu zeigen, dass $m \geq q - 1$.

Nach dem gruppentheoretischen Lemma 8.4 gilt $a^m = 1$ für alle $a \in K^*$. Das Polynom $x^m - 1 \in K[x]$ hat daher $q - 1$ verschiedene Nullstellen. Folglich ist $m \geq q - 1$. □

LEMMA 19.6. *Sei K ein p^m-elementiger Körper, α ein primitives Element von K und g das Minimalpolynom von α über dem Primkörper $\mathbb{Z}_p$. Dann ist g ein über $\mathbb{Z}_p$ irreduzibles Polynom vom Grad m, und es gilt*

$$g \mid x^{p^m} - x \,.$$

BEWEIS. i) Als Minimalpolynom ist g irreduzibel.
ii) Sei $q := p^m$. Da α eine Nullstelle von $x^q - x$ ist, folgt nach Lemma 19.3, dass $g \mid x^q - x$.
iii) Sei $d := \operatorname{grad}(g)$.

Zu zeigen: $d = m$.

Da K ein Vektorraum über $\mathbb{Z}_p$ der Dimension m ist, gibt es $(c_0, \ldots, c_m) \in \mathbb{Z}_p^{m+1} \setminus \{0\}$ mit $c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_m\alpha^m = 0$. Deshalb ist α eine Nullstelle des Polynoms $c_m x^m + \ldots + c_1 x + c_0$. Mit Lemma 19.3 folgt, dass $d := \operatorname{grad}(g) \leq m$.

Zeige: Die Menge

$$K' \;:=\; \{\lambda_{d-1}\alpha^{d-1} + \ldots + \lambda_1\alpha + \lambda_0 \,:\, \lambda_0, \lambda_1, \ldots, \lambda_{d-1} \in \mathbb{Z}_p\}$$

bildet einen p^d-elementigen Unterkörper von K, der das Element α enthält. Da α als primitives Element ganz K erzeugt, folgt dann $d = m$.

Offenbar ist K' unter Addition abgeschlossen und enthält 0 und 1. Bei der Multiplikation zweier Elemente aus K' können wir mittels des Minimalpolynoms von α Potenzen α^r

mit $r \geq d$ durch kleinere Potenzen ersetzen. Dies zeigt, dass K' unter Multiplikation abgeschlossen ist. Um zu zeigen, dass jedes Element in K' ein inverses Element besitzt, benutzen wir (ähnlich wie früher für $\mathbb{Z}_p$) den Satz von Bézout. Wir interpretieren die Koeffizienten $a_0, \ldots, a_{d-1}$ einer Linearkombination in der Definition von K' als Polynom $f(x) := a_0 + a_1 x + \ldots + a_{d-1}x^{d-1}$ (d.h., das Element in K' ist $f(\alpha)$).

Da g irreduzibel ist und $\text{grad}(f) < \text{grad}(g)$, sind f und g teilerfremd. Daher existieren $s, t \in \mathbb{Z}_p[x]$ mit $sf + tg = 1$. Wegen $g(\alpha) = 0$ folgt $1 = s(\alpha)f(\alpha)$, so dass $s(\alpha)$ das inverse Element zu $f(\alpha)$ ist. Andererseits gehört $s(\alpha)$ zu K', denn Potenzen α^r mit $r \geq d$ können wir erneut durch kleinere Potenzen ersetzen. □

Eine wichtige Konsequenz der behandelten Strukturaussagen ist, dass sich zwei endliche Körper gleicher Mächtigkeit strukturell nicht unterscheiden (im Sinne des Isomorphiebegriffs aus Definition 16.3). Wir beweisen nun den zu Beginn des Abschnitts angegebenen Isomorphiesatz.

Beweis. Gilt $|K| = |K'| = q := p^m$, dann gilt $\text{char}(K) = \text{char}(K') = p$. Sei α ein primitives Element von K. Für das Minimalpolynom $g \in \mathbb{Z}_p[x]$ von α über $\mathbb{Z}_p$ gilt nach dem voranstehenden Lemma 19.6 die Eigenschaft $\text{grad}\, g = m$ und $g \mid x^q - x$. Da $x^q - x$ wegen Lemma 19.4 über K' vollständig in Linearfaktoren zerfällt, hat g auch in K' eine Nullstelle α' und ist wegen seiner Irreduzibilität über $\mathbb{Z}_p$ das Minimalpolynom von α'. Wir erhalten die Bijektion

$$\begin{array}{rcl} K & \to & K' \\ \lambda_0 + \lambda_1\alpha + \ldots + \lambda_{m-1}\alpha^{m-1} & \mapsto & \lambda_0 + \lambda_1\alpha' + \ldots + \lambda_{m-1}(\alpha')^{m-1}\,, \quad \lambda_1, \ldots, \lambda_m \in \mathbb{Z}_p\,, \end{array}$$

und diese Abbildung ist ein Körperisomorphismus. □

20. Existenz irreduzibler Polynome

Wir zeigen nun, dass zu jeder Primzahlpotenz p^m ein endlicher Körper mit p^m Elementen konstruiert werden kann. Nach den vorangegangenen Abschnitten genügt es hierzu hierzu, die Existenz eines irreduziblen Polynoms f vom Grad m in $\mathbb{Z}_p[x]$ nachzuweisen.

Wir untersuchen zunächst, wie endliche Körper als Nullstellenmenge eines Polynoms hervorgehen. Im Falle eines irreduziblen Polynoms erweitern wir den Körper geeignet (analog zu dem über $\mathbb{R}$ irreduziblen Polynom $x^2 + 1$, das durch die "Adjunktion" des Elements i in $(x + i)(x - i)$ zerfällt).

Lemma 20.1. *Ist K_0 ein Körper und $g \in K_0[x]$ irreduzibel, dann gibt es einen Erweiterungskörper K von K_0, in dem g eine Nullstelle besitzt.*

BEWEIS. Sei $g \in K_0[x]$ mit $g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$ ein (o.B.d.A.) normiertes, irreduzibles Polynom vom Grad n. Folglich besitzt g keine Nullstellen in K_0. Wir wählen nun K als Restklassenring von $K_0[x]$ modulo g, $K := K_0[x]/(g)$. Nach Satz 18.1 ist K ein Körper. Ferner ist die Restklasse $\overline{x}$ eine Nullstelle von g in K, da $g(\overline{x}) \equiv g(x) \equiv 0 \,(\mathrm{mod}\ (g))$. □

SATZ 20.2. *Sei p prim und $q = p^m$ für ein $m \in \mathbb{N}$. Dann ist das Polynom $x^q - x \in \mathbb{Z}_p[x]$ gleich dem Produkt aller normierten, irreduziblen Polynome in $\mathbb{Z}_p[x]$, deren Grad m teilt.*

BEWEIS. $x^q - x$ hat keine Quadrate von Polynomen als Faktor, da die formale Ableitung gleich -1 ist (siehe Übungen).

„$\supset$“: Sei g ein irreduzibles Polynom vom Grad n, so dass $n|m$. Nach Satz 20.1 besitzt g eine Nullstelle α in einem Körper mit p^n Elementen. Es folgt nach Satz 7.5 die Eigenschaft $\alpha^{p^n} = \alpha$, und, da m Vielfaches von n ist, $\alpha^{p^m} = (\ldots(\alpha^{p^n})^{p^n}\ldots)^{p^n} = \alpha$. α ist also auch eine Nullstelle von $x^q - x$. Ferner ist g das Minimalpolynom von α, denn die Existenz eines Minimalpolynoms h von α kleineren Grades würde (nach Lemma 19.3) $h \mid g$ und damit die Reduzibilität von g nach sich ziehen. Ebenfalls mit Lemma 19.3 folgt, dass $g \mid x^q - x$.

„$\subset$“: Sei g ein normierter, irreduzibler Teiler von $x^q - x$ vom Grad n.

Zu zeigen: $n \mid m$.

g hat eine Nullstelle $\alpha \in \mathbb{F}_q$. Dann ist g (analog zum ersten Beweisteil) das Minimalpolynom von α. Für den kleinsten, das Element α enthaltenden Unterkörper K_α gilt (wie im Beweis von Lemma 19.6)

$$K_\alpha \;=\; \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \,:\, a_0, \ldots, a_{n-1} \in \mathbb{Z}_p\}\,,$$

und er besitzt daher p^n Elemente. Wir fassen nun $\mathbb{F}_q$ als Vektorraum über K_α auf, mit der Basis $\beta_1, \ldots, \beta_d$. Dann hat jedes Element aus $\mathbb{F}_q$ eine eindeutige Darstellung

$$b_1\beta_1 + \ldots + b_d\beta_d \quad \text{mit } b_1, \ldots, b_d \in K_\alpha\,.$$

$\mathbb{F}_q$ hat also genau $(p^n)^d = p^{nd}$ Elemente, und es folgt $m = nd$. □

Mittels Satz 20.2 kann die Anzahl N_m der irreduziblen Polynome vom Grad m über $\mathbb{Z}_p$ bestimmt werden. Nach diesem Satz gilt nämlich

$$p^m \;=\; \sum_{d|m} dN_d\,,$$

da das Polynom $x^{p^m} - x$ als Polynom vom Grad p^m als Faktoren N_d irreduzible Polynome vom Grad d hat, für jeden Teiler d von m.

Durch Anwendung der Möbius-Inversion ergibt sich

$$mN_m \;=\; \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d\,,$$

also

$$N_m \;=\; \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d\,.$$

Um zu zeigen, dass $N_m \geq 1$ für alle m, verwenden wir $\mu(\frac{n}{n}) = \mu(1) = 1$, so dass

$$N_m \;\geq\; \frac{1}{m}(p^m - \sum_{0\leq d<m} p^d)\,.$$

Mit der Summenformel für die geometrischen Reihe $\sum_{0\leq 0\leq m-1} p^d = \frac{p^m-1}{p-1} < p^m$ ergibt sich $N_m > 0$ und aufgrund der Ganzzahligkeit $N_m \geq 1$.

Beispiel. Für $p = 7, m = 5$ ergibt sich

$$\begin{aligned} N_m &= \frac{1}{5}\left(\mu(1)7^5 + \mu(7)7^1\right) \\ &= \frac{1}{5}(16807 - 7) \\ &= 3360\,. \end{aligned}$$

Wir fassen unsere Resultate in dem folgenden Satz zusammen:

Satz 20.3. *Es gibt genau dann einen endlichen Körper K mit q Elementen, wenn q Potenz einer Primzahl ist. K ist dann bis auf Isomorphie eindeutig bestimmt.*

Anmerkung. Für ein gegebenes p wächst die Anzahl N_m der irreduziblen Polynome vom Grad m über $\mathbb{Z}_p$ sehr schnell. Beispiel für $p = 7$:

m	N_m
1	7
2	21
3	112
4	588
5	3360
6	19544
7	117648

Teil 5

Codes

21. Fehlerkorrigierende Codes

Die Kommunikation von Informationen erfolgt oft über „gestörte“ Kanäle, welche Fehler in der übertragenen Nachricht bewirken können. Dies ist beispielsweise bei Satellitenübertragungen oder bei der Speicherung von Daten (z.B. auf Magnetbändern oder Compact Discs) der Fall. Daher soll Information möglichst so codiert werden, dass Fehler erkannt und/oder korrigiert werden können.

Ein *Alphabet* A ist eine Menge der Kardinalität mindestens 2. $A^* := \cup_{n\geq 0} A^n$ bezeichnet die Menge der Wörter über dem Alphabet A.

Definition 21.1. Sei A ein Alphabet. Ein *Code* über A ist eine nichtleere Teilmenge von A^*. Falls alle Codewörter die gleiche Länge n haben, spricht man von einem *Blockcode* der Länge n. Ein *binärer Code* ist ein Code über dem Alphabet $A = \{0, 1\}$.

Wir betrachten nur Blockcodes über endlichen Körpern, z.B. $\mathbb{F} = \mathbb{Z}_p$ für p prim oder $\mathbb{F} = \mathbb{Z}_p[x]/(g)$ mit p prim und $g \in \mathbb{Z}_p[x]$ irreduzibel.

Definition 21.2. Der *Hamming-Abstand* (kurz *Abstand*) zweier Vektoren $x, y \in \mathbb{F}^n$ ist die Anzahl der Stellen, in denen sich x und y unterscheiden:

$$d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) := |\{i \,:\, x_i \neq y_i\}| \,.$$

Das *Gewicht* $w(x)$ ist definiert als die Anzahl der von 0 verschiedenen Stellen von x:

$$w((x_1, \ldots, x_n)) := |\{i \,:\, x_i \neq 0\}| \,.$$

Für $\mathbb{F} = \{0, 1\}$ ist $d(x, y) = w(x + y)$.

Definition 21.3. Der *Minimalabstand* eines Codes C ist definiert als

$$d(C) := \min\{d(x, y) \,:\, x, y \in C,\, x \neq y\} \,.$$

Bei der Maximum-Likelihood-Decodierung decodiert man das empfangene Tupel $v = (v_1, \ldots, v_n)$ als ein Codewort, dessen Abstand zu v minimal ist.

Definition 21.4. (*t-Fehler-erkennender und -korrigierender Code.*) Ein Code heißt *t-Fehler-korrigierend*, falls Fehler an bis zu t Stellen eines Codeworts immer korrekt decodiert werden können. Ein Code heißt *t-Fehler-erkennend*, falls bei Fehlern an bis zu t Stellen eines Codeworts die *Anzahl* der fehlerhaften Stellen immer korrekt erkannt wird.

Es folgt unmittelbar:

Satz 21.5. *Ein Code mit Minimalabstand d ist $\lfloor \frac{d-1}{2} \rfloor$-Fehler-korrigierend. Ist d gerade, dann ist der Code $\frac{d}{2}$-Fehler-erkennend.*

Wir betrachten hier fast ausschließlich lineare Codes. Diese Codes lassen sich besonders gut untersuchen und anwenden, da hierfür Methoden aus der linearen Algebra benutzt werden können.

DEFINITION 21.6. Ein Code $C \subset \mathbb{F}^n$ heißt *linearer Code*, wenn er ein Unterraum von $\mathbb{F}^n$ ist. Hat C die Dimension k, dann spricht man von einem $[n,k]$-*Code*. Ein $[n,k,d]$-*Code* ist ein $[n,k]$-Code mit Minimalabstand $d := d(C)$.

LEMMA 21.7. *Der Minimalabstand d eines linearen Codes C ist*

$$d \;=\; \min\{w(x) \,:\, x \in C,\, x \neq 0\}\,.$$

BEWEIS. „$\leq$“ klar.

„$\geq$“: Seien $y \neq z \in C$ mit $d = d(y,z)$. Für $y - z \in C$ folgt

$$w(x) = d(y-z,0) = d(y,z) = d\,.$$

□

DEFINITION 21.8. Sei C ein linearer $[n,k]$-Code und $g_1, \ldots, g_k$ eine Basis des Vektorraums C. Dann heißt die $k \times n$-Matrix $G := (g_{ij})_{1 \leq i \leq k, 1 \leq j \leq n}$ eine *Generatormatrix* von C.

Wir verwenden das formale innere Produkt auf $\mathbb{F}^n$, das durch die bilineare Abbildung

$$\begin{array}{rcl} \langle \cdot, \cdot \rangle \,:\, \mathbb{F}^n \times \mathbb{F}^n & \to & \mathbb{F}\,, \\ (v,w) & \mapsto & \sum_{i=1}^n v_i w_i\,. \end{array}$$

gegeben ist. (Im Gegensatz zu einem Skalarprodukt gibt es hier nicht den Begriff der positiven Semidefinitheit.)

DEFINITION 21.9. Sei $C \subset \mathbb{F}^n$ ein $[n,k]$-Code. Der *duale* Code $C^\perp$ zu C ist definiert als

$$C^\perp \;:=\; \{u \in \mathbb{F}^n \,:\, \langle u, c \rangle = 0 \quad \forall c \in C\}\,.$$

$C^\perp$ ist ein $[n, n-k]$-Code, und es gilt $(C^\perp)^\perp = C$.

DEFINITION 21.10. Ein Code $C \subset \mathbb{F}^n$ heißt *systematisch in den Stellen* $i_1, \ldots, i_k$, wenn zu jedem Vektor $u = (u_1, \ldots, u_k) \in \mathbb{F}^k$ *genau* ein Codewort $c = (c_1, \ldots, c_n)$ mit $c_{i_1} = u_1, \ldots, c_{i_k} = u_k$ existiert.

Ist ein Code systematisch in den Stellen $i_1, \ldots, i_k$, so kann in diesen Stellen eine Ausgangsnachricht der Länge k untergebracht werden. Die verbleibenden Stellen dienen zur Redundanz, mit deren Hilfe Fehler erkannt und korrigiert werden können.

SATZ 21.11. *Sei C ein linearer $[n,k]$-Code, der in den ersten k Stellen systematisch ist. Dann hat C eine* kanonische Generatormatrix*, d.h. eine (sogar eindeutig bestimmte) Generatormatrix der Form $G = (I_k|A)$, wobei I_k die $k \times k$-Einheitsmatrix ist und $A \in \mathbb{F}^{k\times(n-k)}$.*

BEWEIS. Für alle $i \in \{1,\ldots,k\}$ existiert nach Voraussetzung genau ein Codewort g_i mit $(g_{i1},\ldots,g_{ik}) = e^{(i)}$ (i-ter Einheitsvektor). Sei G die Generatormatrix mit den Zeilen $g_1,\ldots,g_k$. □

BEISPIEL. Sei C der lineare Code $\{(000),(011),(101),(110)\} \subset \{0,1\}^3$. Mögliche Generatormatrizen sind:

$$G_1 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \qquad G_3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

G_2 ist die kanonische Generatormatrix. Mit der kanonischen Generatormatrix eines linearen $[n,k]$-Codes $C \subset \mathbb{F}^n$ kann eine k-stellige Nachricht $u \in \mathbb{F}^k$ mittels

$$c \;:=\; u \cdot G \;= (u_1,\ldots,u_k,c_{k+1},\ldots,c_n)$$

codiert werden.

Bis jetzt haben wir uns mit dem Erzeugen von linearen Codes beschäftigt. Als nächstes untersuchen wir, wie man erkennt, ob ein gegebener Vektor zum Code gehört.

DEFINITION 21.12. Sei $C \subset \mathbb{F}^n$ ein linearer Code. Eine Matrix $H \in \mathbb{F}^{l\times n}$ (mit $l \in \mathbb{N}$) heißt *Kontrollmatrix*, falls

$$C = \{v \in \mathbb{F}^n \;:\; H \cdot v^T = 0\}.$$

SATZ 21.13. *Sei $C \subset \mathbb{F}^n$ ein $[n,k]$-Code mit Generatormatrix G. Eine Matrix $H \in \mathbb{F}^{l\times n}$ ist genau dann eine Kontrollmatrix von C, wenn gilt:*

$$H \cdot G^T = 0 \quad \textit{und} \quad \operatorname{rang}(H) = n-k.$$

BEWEIS. „⇒“: Da H eine Kontrollmatrix ist, ist C der Lösungsraum des linearen Gleichungssystems $H \cdot v^T = 0$. Es folgt $H \cdot G^T = 0$ und $\operatorname{rang}(H) = n-k$. (Insbesondere ist H also eine Generatormatrix des dualen Codes $C^\perp$.)

„⇐“: Sei $H \cdot G^T = 0$ und $\operatorname{rang}(H) = n-k$.
Zeige: $C = \{v \in \mathbb{F}^n \;:\; H \cdot v^T = 0\}$.

„⊂“: gilt, da jedes Codewort $c \in C$ eine Linearkombination der Zeilenvektoren von G ist. Da die beiden Unterräume von $\mathbb{F}^n$ die gleiche Dimension k haben, folgt die Gleichheit. □

Mit Hilfe der kanonischen Generatormatrix lässt sich eine Kontrollmatrix besonders leicht finden.

SATZ 21.14. *Der lineare $[n,k]$-Code habe die kanonische Generatormatrix $G = (I_k|A)$. Dann ist die Matrix $H = (-A^T|I_{n-k})$ eine Kontrollmatrix von C, die sogenannte* kanonische Kontrollmatrix.

BEWEIS. Die $n-k$ Zeilen von H sind linear unabhängig (wegen I_{n-k}), daher gilt $\operatorname{rang}(H) = n-k$. Die Eigenschaft $H \cdot G^T = 0$ folgt aus

$$\underbrace{(-A^T|I_{n-k})}_{\in \mathbb{F}^{(n-k)\times n}} \cdot \underbrace{(I_k|A)^T}_{\in \mathbb{F}^{n\times k}} \;=\; -A^T + A^T \;=\; 0\,.$$

□

BEISPIEL. Sei $n = 3$, $C = \{(000), (011), (110), (101)\} \subset \mathbb{F}_2^3$ und $k = 2$:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Die kanonische Kontrollmatrix ist $H = (-A^T|I_1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

22. Hamming-Codes

Ziel: Konstruktion fehlerkorrigierender linearer Codes.

SATZ 22.1. *Sei $C \subset \mathbb{F}^n$ ein linearer Code mit Kontrollmatrix H. Dann sind folgende Aussagen äquivalent:*

(1) $d(C) \geq d$;
(2) *Je $d-1$ der Spalten von H sind linear unabhängig.*

BEWEIS. Sei $H = (u_1, \ldots, u_n)$.

„⇒“: *Annahme:* Es existiert ein $d' < d$, $i_1, \ldots, i_{d'} \in \{1, \ldots, n\}$ und $c' = (c'_{i_1}, \ldots, c'_{i_{d'}}) \neq 0$, so dass $\sum_{j=1}^{d'} c'_{i_j} u_{i_j} = 0$. Der durch Nullen ergänzte Vektor c' liefert ein Codewort c mit Gewicht $\leq d' < d$, im Widerspruch zur Voraussetzung.

„⇐“: *Annahme:* Es existiert ein Codewort $c = (c_1, \ldots, c_n)$ mit $w(c) = d' < d$. Wegen $\sum_{i=1}^{n} u_i c_i = 0$ sind die Vektoren u_i mit $c_i \neq 0$ linear abhängig, im Widerspruch zur Voraussetzung. □

Für die nachfolgend betrachteten Hamming-Codes konzentrieren wir uns auf $\mathbb{F} = \mathbb{F}_2$.

DEFINITION 22.2. Ein linearer Code mit einer Kontrollmatrix H, die jeden der $2^r - 1$ Vektoren aus $\mathbb{F}_2^r \setminus \{0\}$ genau einmal als Spalte enthält (für ein $r \geq 2$) heißt *(binärer)* $[2^r - 1, 2^r - 1 - r]$-*Hamming-Code*.

BEISPIEL. Für $r = 3$ erhalten wir einen $[7, 4]$-Code. H lautet beispielsweise

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} .$$

Obige Definition wird durch folgenden Satz gerechtfertigt.

SATZ 22.3. *Ein* $[2^r - 1, 2^r - 1 - r]$-*Hamming-Code ist ein linearer* $[2^r - 1, 2^r - 1 - r]$-*Code, und er ist* 1-*Fehler-korrigierend.*

BEWEIS. Der Hamming-Code ist natürlich ein $[n, k]$-linearer Code für ein Paar (n, k). Auf der Definition ergibt sich unmittelbar $n = 2^r - 1$, und da die Kontrollmatrix H (nach eventueller Permutation der Spalten) eine Untermatrix $I_{r,r}$ enthält, hat sie Rang r, d.h. $k = n - r = 2^r - 1 - r$.

Je zwei Spalten von H sind verschieden und damit wegen $\mathbb{F} = \mathbb{F}_2$ linear unabhängig. Mit Satz 22.1 folgt für die Distanz $d(C) = 3$, der Code ist also 1-Fehler-korrigierend. □

Die nachfolgenden Überlegungen zeigen, dass Hamming-Codes optimal sind, wenn $|C|$ bei gegebenem $d(C)$ maximiert werden soll.

SATZ 22.4. (Hamming-Schranke.) *Sei* $M(n, d, q) := \max\{|C| \,:\, C \subset \mathbb{F}_q^n \,, d(C) \geq d\}$. *Für ungerades* $d = 2t + 1$ *gilt*

$$M(n, d, q) \;\leq\; \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i} \,.$$

BEWEIS. Sei $C \subset \mathbb{F}_q^n$ ein Code mit $d(C) \geq 2t + 1$, und sei

$$B_t(a) \;:=\; \{b \in \mathbb{F}_q^n \,:\, d(a, b) \leq t\}$$

die „Kugel“ um ein Codewort a mit Hamming-Radius t. Wegen $d(C) \geq 2t + 1$ sind die Kugeln zu verschiedenen Codewörtern disjunkt, und es folgt $q^n \geq |C| \cdot |B_t(a)|$. Da es $\binom{n}{i}(q-1)^i$ Wörter in $B_t(a)$ mit Hamming-Abstand i zu a gibt, gilt

$$|B_t(a)| \;=\; \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

und daher

$$M(n,d,q) \;\leq\; \frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i}\,.$$

□

DEFINITION 22.5. Ein Code $C \subset \mathbb{F}_q^n$ heißt t-perfekt, wenn $d(C) \geq 2t+1$ und

$$|C| = \frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i}\,.$$

SATZ 22.6. *Der binäre* $[2^r-1, 2^r-1-r]$*-Hamming-Code ist* 1*-perfekt.*

BEWEIS. Siehe Übungen. □

Benutzt man wie in obigem Beispiel für einen Hamming-Code eine Kontrollmatrix, in der in der i-ten Spalte die Binärdarstellung von i steht, dann lässt sich die Decodierung eines Vektors v besonders einfach ausführen. Zuerst wird das Syndrom $s := Hv^T \in \mathbb{F}_2^r$ berechnet. Ist s der Nullvektor, dann ist v ein Codewort. Anderenfalls suchen wir ein Codewort c, das sich von v nur in einem einzigen Bit unterscheidet. Ist s die Binärdarstellung einer Zahl i, dann wird v als $c := v + e^{(i)}$ decodiert, wobei $e^{(i)}$ der i-te Einheitsvektor von $\mathbb{F}^{2^r-1}$ ist. Denn dann ändern sich beim Übergang von v zu c genau diejenigen Bits im Syndrom, an denen eine 1 in der Binärdarstellung von i steht, d.h. $Hc^T = 0$. Im obigen Beispiel ergibt sich für $v = (1\,1\,0\,0\,0\;1\,0)$ das Syndrom $s^T = (101)$, also $i = 5$ und $c = (1\,1\,0\,0\,\underline{1}\,1\,0)$.

23. Zyklische Codes

Für die Behandlung zyklischer Codes behandeln wir zunächst kurz das Konzept eines Ideals in einem Ring. Sei R im Folgenden ein kommutativer Ring mit Einselement.

DEFINITION 23.1. Eine Teilmenge I von R heißt *Ideal*, wenn folgende beiden Bedingungen erfüllt sind:

i) $(I,+)$ ist eine Untergruppe von $(R,+)$.
ii) Für alle $r \in R$ gilt $rI \subset I$ und $Ir \subset I$.

Für ein gegebenes Element $g \in R$ definiert

$$(g) \;:=\; \{r \cdot g \,:\, r \in R\}$$

das von g *erzeugte Hauptideal*. Man überzeugt sich leicht davon, dass (g) tatsächlich ein Ideal ist. Einen Ring R bezeichnet man als Hauptidealring, wenn jedes Ideal I von R ein Hauptideal ist, d.h., für jedes Ideal I von R ein Polynom $g \in R$ mit

$$I \;=\; (g)$$

existiert.

SATZ 23.2. *Die folgenden Ringe sind Hauptidealringe: a) $\mathbb{Z}$;*
b) $\mathbb{Z}_m$ für eine natürliche Zahl $m \geq 2$;
c) $K[x]$ für einen Körper K;
d) $K[x]/(f)$ für einen Körper K und ein Polynom $f \in K[x]$.

BEWEIS. a) Sei $I \neq \{0\}$ ein Ideal in I. Setze $g := \min\{x \in I \,:\, x \geq 0\}$. Jedes Element in I ist ein Vielfaches von g, da sich durch Division mit Rest ansonsten ein kleineres Element in I konstruieren lassen würde.

b) In Analogie zu a) können wir auch für die Vertreter $\{0, 1, \ldots, m-1\}$ von $\mathbb{Z}_m$ die Division mit Rest betrachten, so dass I auch hier durch das kleinste von Null verschiedene Element in I erzeugt werden muss.

c) analog via der Division mit Rest in $K[x]$ und d) entsprechend durch die Übertragung dieser Division mit Rest auf $K[x]/(f)$. □

Anmerkung: Da $\mathbb{Z}_m$ und $\mathbb{F}_q[x]/(f)$ Nullteiler besitzen können, erfüllen diese Ringe i.A. nicht die Definition eines Euklidischen Rings.

Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen.

DEFINITION 23.3. Ein Code $C \subset \mathbb{F}_q^n$ heißt *zyklisch*, falls er gegen zyklisches Rotieren abgeschlossen ist, d.h., falls aus $(c_0, \ldots, c_{n-2}, c_{n-1})$ immer $(c_{n-1}, c_0, \ldots, c_{n-2})$ folgt.

Zur Erinnerung: Vektoren der Länge n können mittels des Vektorraum-Isomorphismus

$$\begin{array}{rcl} \psi : \mathbb{F}_q^n & \to & \mathbb{F}_q[x]/(x^n-1) \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1}x^{n-1} \pmod{x^{n-1}} \end{array}$$

als Polynome vom Grad $< n$ aufgefasst werden. Das Multiplizieren mit x bewirkt das zyklische Vertauschen der Koeffizienten von c. Von nun an betrachten wir lineare Codes daher als Teilmenge des Restklassenrings $\mathbb{F}_q[x]/(x^n-1)$. (Wir bemerken, dass das Polynom x^{n-1} nicht irreduzibel und damit $\mathbb{F}_q[x]/(x^n-1)$ kein Körper ist.)

SATZ 23.4. *Ein linearer Code $C \subset \mathbb{F}_q[x]/(x^n-1)$ ist genau dann zyklisch, wenn C ein Ideal von $\mathbb{F}_q[x]/(x^n-1)$ ist.*

BEWEIS. „⇒“: Als Untervektorraum von $\mathbb{F}_q[x]/(x^n-1)$ ist C insbesondere eine Untergruppe (bzgl. $+$). Sei nun $c(x) \in C$, $r(x) = r_0 + r_1 x + \ldots + r_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n-1)$. Da C zyklisch ist, gilt $xc(x), x^2c(x), \ldots, x^{n-1}c(x) \in C$, und wegen der Linearität dann

$$r(x)c(x) = r_0 c(x) + r_1 xc(x) + \ldots + r_{n-1}x^{n-1}c(x) \in C\,.$$

Also ist C ein Ideal.

„$\Leftarrow$“: Als Ideal ist C ein Untervektorraum von $\mathbb{F}_q[x]/(x^n-1)$, d.h. ein linearer Code. Für $r(x) = x$ und $c(x) \in C$ gilt aufgrund der Idealeigenschaft und der Restklassenstruktur $xc(x) \in C$, d.h. C ist zyklisch. □

Da $\mathbb{F}_q[x]/(x^n-1)$ nach Satz 23.2 ein Hauptidealring ist, wird jedes Ideal C von einem Polynom $g(x) \in C \setminus \{0\}$ minimalen Grades erzeugt. Ein solches Polynom heißt *Generatorpolynom* von C. (Beachte, dass im Sinne dieser Definition nicht jedes erzeugende Polynom von C ein Generatorpolynom von C ist.) Die Elemente von C sind gerade die Vielfachen von $g(x)$. Dies kann noch präziser formuliert werden:

Satz 23.5. *Sei C ein zyklischer linearer Code und $g(x)$ ein Generatorpolynom von C. Sei $s := \operatorname{grad} g(x)$, $k := n - s$. Dann ist C ein $[n,k]$-Code, und es gilt*

$$C = \{a(x)g(x) \,:\, a(x) \in \mathbb{F}_q[x]/(x^n-1),\ \operatorname{grad} a(x) < k\}\,.$$

Beweis. „$\supset$“: klar.

„$\subset$“: Sei $c(x) \in C$. Dann gibt es Polynome $a(x), r(x) \in \mathbb{F}_q[x]/(x^n-1)$ mit

$$c(x) \;=\; a(x)g(x) + r(x)\,, \quad \operatorname{grad} r(x) < \operatorname{grad} g(x)\,.$$

Es folgt $r(x) \in C$, und da $g(x) \in C \setminus \{0\}$ minimalen Grad hat, folgt $r(x) = 0$. Ferner gilt $\operatorname{grad} a(x) = \operatorname{grad} c(x) - \operatorname{grad} g(x) < n - s = k$.

Noch zu zeigen: $|C| = |\mathbb{F}|_q^k$.

Da es genau $|\mathbb{F}|_q^k$ viele Polynome vom Grad $< k$ gibt, genügt es zu zeigen, dass die Abbildung $\mathbb{F}_q[x]/(x^n-1) \to \mathbb{F}_q[x]/(x^n-1)$, $a(x) \mapsto a(x)g(x)$ injektiv ist.

Dies folgt daraus, dass das Produkt $a(x)g(x)$ höchstens den Grad $n-1$ hat. Im Detail:

Annahme: Es existieren $a(x)$ und $a'(x)$ vom Grad $< k$ mit $a(x)g(x) = a'(x)g(x)$.

Für $b(x) := a(x) - a'(x)$ gilt dann $b(x)g(x) = 0$, und zu zeigen ist $b(x) = 0$. Sei $b(x) = \sum_{i=0}^{k-1} b_i x^i$, $g(x) = \sum_{i=0}^{s} g_i x^i$. Dann folgt

$$0 \;=\; b(x)g(x) \;=\; b_0g_0 + (b_0g_1 + b_1g_0)x + (b_0g_2 + b_1g_1 + b_2g_0)x^2 + \ldots + b_{k-1}g_s x^{n-1}\,.$$

Durch Koeffizientenvergleich ergibt sich das lineare Gleichungssystem

$$(b_0, b_1, \ldots, b_{k-1}) \begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_s & & 0 & \\ & g_0 & g_1 & \cdots & \cdots & g_s & & \\ & & \ddots & \ddots & & & \ddots & \\ & 0 & & g_0 & g_1 & \cdots & \cdots & g_s \end{pmatrix} = (0, \ldots, 0)\,.$$

Die Koeffizientenmatrix hat wegen $g_0 \neq 0$ (da sonst ein Generatorpolynom kleineren Grades existiert) und wegen $g_s \neq 0$ den Rang k. Es folgt $b(x) = 0$. □

Die angegebene Koeffizientenmatrix ist offensichtlich eine Generatormatrix von C.

Korollar 23.6. *Ein zyklischer linearer Code $C \subset \mathbb{F}_q^n/(x^n-1)$ mit Generatorpolynom $g(x) = g_0 + g_1 x + \cdots + g_s x^s$ hat die folgende $(n-s) \times n$-Matrix als (nichtkanonische) Generatormatrix:*

$$\begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_s & & 0 & \\ & g_0 & g_1 & \cdots & \cdots & g_s & & \\ & & \ddots & \ddots & & & \ddots & \\ & 0 & & g_0 & g_1 & \cdots & \cdots & g_s \end{pmatrix}.$$

In Satz 23.5 kann man $a(x)$ als Nachricht betrachten, die zum Codewort $c(x) = a(x)g(x)$ verschlüsselt wird. Das Multiplizieren der Polynome kann mittels sogenannter Schieberegister sehr effizient in Schaltungen implementiert werden.

Für zyklische lineare Codes gibt es nicht nur Generator-, sondern auch Kontrollpolynome. Durch Division mit Rest folgt unmittelbar, dass jedes Generatorpolynom $g(x)$ (welches minimalen Grad in $C \setminus \{0\}$ hat) das Polynom $x^n - 1$ teilt.

Satz 23.7. *Sei $C \subset \mathbb{F}_q[x]/(x^n-1)$ ein zyklischer linearer Code mit Generatorpolynom $g(x)$. Für das sog.* Kontrollpolynom $h(x) := (x^n-1)/g(x)$ *von C und für alle $v(x) \in \mathbb{F}_q^n/(x^n-1)$ gilt*

$$v(x) \in C \iff h(x)v(x) = 0 \quad \textit{(in } \mathbb{F}_q[x]/(x^n-1)\textit{)}$$

Beweis. „⇒“ Für jedes $c(x) = a(x)g(x) \in C$ gilt

$$h(x)c(x) = h(x)a(x)g(x) = a(x)(x^n-1) = 0\,.$$

„⇐“ Sei $h(x)v(x) = 0$ in $\mathbb{F}_q[x]/(x^n-1)$. Dies bedeutet in $\mathbb{F}_q[x]$, dass es ein $a(x)$ gibt mit $h(x)v(x) = a(x)(x^n-1)$. Wegen $x^n - 1 = g(x)h(x)$ folgt $h(x)v(x) = a(x)g(x)h(x)$. Kürzen liefert $v(x) = a(x)g(x)$ und damit $v(x) \in C$. □

SATZ 23.8. *Ein zyklischer linearer Code $C \subset \mathbb{F}[x]/(x^n-1)$ mit Kontrollpolynom $h(x) = h_0 + h_1 x + \ldots + h_k x^k$ hat die folgende $(n-k) \times n$-Matrix als Kontrollmatrix:*

$$H = \begin{pmatrix} h_k & \ldots & h_1 & h_0 & & 0 \\ & h_k & \ldots & h_1 & h_0 & \\ & & \ddots & & \ddots & \ddots \\ & 0 & & h_k & \ldots & h_1 & h_0 \end{pmatrix}.$$

BEWEIS. Siehe Übungen. □

Hamming-Codes sind bei geeigneter Anordnung der Koordinaten zyklisch. Die Spaltenvektoren einer Kontrollmatrix H eines Hamming-Codes können als die von 0 verschiedenen Elemente des Körpers $\mathbb{F}_{2^r}$ aufgefasst werden. Ist α ein primitives Element von $\mathbb{F}_{2^r}$, dann ist beispielsweise

$$H = (1\ \alpha\ \alpha^2\ \ldots\ \alpha^{2^r-2})$$

eine Kontrollmatrix eines $[2^r-1, 2^r-1-r]$-Hamming-Codes. In der i-ten Spalte von H steht α^i, als Spaltenvektor über $\mathbb{F} = \{0,1\}$ geschrieben.

BEISPIEL. Da das Polynom $f(x) := x^3 + x + 1$ in $\mathbb{F}_2[x]$ irreduzibel ist, lässt sich $\mathbb{F}_8$ als $\mathbb{F}_2[x]/(f)$ konstruieren. x ist ein primitives Element dieses Körpers. Als Kontrollmatrix ergibt sich

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

wobei die Spalten zu den Elementen 1, x, x^2, …, x^6 ($\equiv x^2+1 \pmod f$) korrespondieren.

Allgemein gilt:

SATZ 23.9. *Sei $r \in \mathbb{N}$, α ein primitives Element von $\mathbb{F}_{2^r}$ und H die oben beschriebene Kontrollmatrix eines $[2^r-1, 2^r-r-1]$-Hamming-Codes C. Dann gilt:*

(1) *Ein Polynom $v(x) \in \mathbb{F}_2[x]/(x^n-1)$ ist genau dann in C enthalten, wenn $v(\alpha) = 0$ in $\mathbb{F}_{2^r}$, d.h.*

$$v(x) \in C \iff v(\alpha) = 0 \text{ in } \mathbb{F}_{2^r}.$$

(2) *C ist zyklisch und hat das Minimalpolynom $g(x)$ von α als Generatorpolynom.*

BEWEIS. (1) Sei $n := 2^r - 1$ und $v(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1}$. Dann gilt:

$$\begin{aligned} & v(x) \in C \\ \iff \quad & Hv^T = 0 \\ \iff \quad & v_0 + v_1\alpha + \ldots + v_{n-1}\alpha^{n-1} = 0 \text{ in } \mathbb{F}_{2^r} \\ \iff \quad & v(\alpha) = 0\,. \end{aligned}$$

(2) Nach Lemma 19.3 gilt $v(\alpha) = 0$ genau dann, wenn für das Minimalpolynom $g(x)$ von α gilt, dass $g(x) \mid v(x)$. Mit Aussage (1) sind die Codewörter also gerade die Vielfachen von $g(x)$. Folglich ist C nach Satz 23.4 zyklisch, und $g(x)$ ist ein Generatorpolynom. □

24. BCH-Codes

Wir betrachten zunächst eine weitere Möglichkeit zur Konstruktion einer Kontrollmatrix für einen zyklischen Code C. Sie ist theoretisch wichtig, für das praktische Decodieren jedoch weniger geeignet. Sei $g(x) = g_1(x)g_2(x)\cdots g_k(x)$ das Generatorpolynom von C, zerlegt in seine irreduziblen Teiler $g_1(x), \ldots, g_k(x) \in \mathbb{F}_q[x]$. Wir können dann $g_1(x), \ldots, g_k(x)$ als Minimalpolynome von Elementen $\alpha_1, \ldots, \alpha_l$ in einem Erweiterungskörper $\mathbb{F}'_q$ von $\mathbb{F}_q$ auffassen. Wir setzen nun voraus, dass $g_1(x), \ldots, g_k(x)$ alle voneinander verschieden sind. Nach den Eigenschaften von Minimalpolynomen ist dann $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ genau dann ein Vielfaches von $g(x)$, falls

$$c(\alpha_1) = c(\alpha_2) = \ldots = c(\alpha_l) = 0$$

gilt. In Matrizenschreibweise lautet diese Bedingung

$$H \cdot c^T$$

mit $c = (c_0, c_1, \ldots, c_{n-1})$ und der Matrix

$$H := \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_l & \alpha_l^2 & \cdots & \alpha_l^{n-1} \end{pmatrix}.$$

H ist also eine Kontrollmatrix des Codes.

Bose, Chaudhuri und Hocquenghem haben vorgeschlagen, solche zyklischen Codes zu betrachten, für die $\alpha_1 = \alpha, \alpha_2 = \alpha^2, \ldots, \alpha_l = \alpha^l$ für ein geeignetes α gilt.

DEFINITION 24.1. Ein zyklischer linearer Code $C \subset \mathbb{F}_q[x]/(x^n - 1)$ mit Generatorpolynom $g(x)$ heißt *BCH-Code*, falls ein α in einem Erweiterungskörper von $\mathbb{F}_q$ und eine natürliche Zahl $l < n$ existiert, so dass gilt:

(1) Die *Ordnung* von α ist n, d.h. $\alpha^n = 1$ und $\alpha^j \neq 1$ für $j < n$.
(2) $g(x)$ ist das Produkt der Minimalpolynome von $\alpha, \alpha^2, \ldots, \alpha^l$, wobei jedes Minimalpolynom in $g(x)$ als Faktor nur einmal auftritt.

Für einen BCH-Code ist also

$$H := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^l & \alpha^{2l} & \cdots & \alpha^{l(n-1)} \end{pmatrix} \tag{24.1}$$

Kontrollmatrix.

Hamming-Codes sind spezielle BCH-Codes. Nach den Überlegungen des Abschnitts über zyklische Codes gilt für einen $[2^r - 1, 2^r - r - 1]$-Hamming-Code mit primitivem Element α: Die Blocklänge n ist $2^r - 1$, und, da für das Minimalpolynom g von α nicht nur $g(\alpha) = 0$, sondern (wegen der Charakteristik 2) auch $g(\alpha^2) = g(\alpha)^2 = 0$ gilt, ist g das Minimalpolynom von α und α^2, d.h. $l = 2$.

Satz 24.2. *Der Minimalabstand eines BCH-Codes ist mindestens* $l + 1$.

Im Falle der Hamming-Codes ergibt sich also der bereits bekannte Minimalabstand von 3.

Beweis. Sei $H \in \mathbb{F}^{l \times n}$ die Kontrollmatrix des BCH-Codes C. Da die Elemente der ersten Zeile von H alle voneinander verschieden sind, ist jede $l \times l$-Untermatrix von H eine Vandermonde-Matrix (spaltenweise gelesen und beginnend bei Potenz 1) und damit regulär. Gilt daher $H \cdot c^T = 0$ für ein $c \neq 0$, so muß c mindestens das Gewicht $l + 1$ haben. Da C ein linearer Code ist, folgt die Behauptung aus Lemma 21.7. □

Beispiel. Wir konstruieren einen binären BCH-Code mit $n = 15$ und $l = 4$.

Das Polynom

$$m(x) := x^4 + x + 1$$

ist in $\mathbb{F}_2[x]$ irreduzibel. (Es hat in $\mathbb{F}_2$ keine Nullstellen und könnte höchstens in zwei Polynome vom Grad 2 zerfallen. Da die formale Ableitung $m'(x) = 1$ ist, müssten die beiden Faktoren verschieden sein. Es gibt aber in $\mathbb{F}_2[x]$ nur ein irreduzibles Polynom vom Grad 2, nämlich $x^2 + x + 1$.) Nach Satz 20.2 teilt $m(x)$ das Polynom $x^{16} - x$, daher besitzt $m(x)$ in $\mathbb{F}_{16}$ eine Nullstelle α und ist (mit der Argumentation wie im Beweis von Satz 20.2) das Minimalpolynom von α.

Zeige: α ist ein primitives Element in $\mathbb{F}_{16}$.

Nach dem Satz von Euler gilt $\alpha^{15} = 1$. Es ist jedoch $\alpha^3 \neq 1$ (da sich ansonsten ein Widerspruch zur Minimalpolynomeigenschaft von $m(x)$ ergeben würde), und $\alpha^5 = \alpha^2 + \alpha \neq 1$. Daher ist α primitives Element in $\mathbb{F}_{16}$.

$m(x)$ ist auch das Minimalpolynom von α^2 und α^4, denn es gilt $m(\alpha^2) = m(\alpha)^2 = 0$ und $m(\alpha^4) = m(\alpha^2)^2 = 0$. Wir bestimmen nun das Minimalpolynom von α^3 durch den Ansatz

$$0 \;=\; a + b\alpha^3 + c\alpha^6 + d\alpha^9 + e\alpha^{12}$$

mit $a, \ldots, e \in \{0, 1\}$ (da $\alpha^{15} = 1$ ist es höchstens vom Grad 4). Aus $\alpha^4 = \alpha + 1$ ergibt sich

$$\begin{aligned} \alpha^6 &= \alpha^4\alpha^2 = \alpha^3 + \alpha^2\,, \\ \alpha^9 &= (\alpha^4)^2\alpha = (\alpha+1)^2\alpha = \alpha^3 + \alpha\,, \\ \alpha^{12} &= (\alpha^4)^3 = (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1\,. \end{aligned}$$

Aufgrund des Grades des Minimalpolynoms ist α nicht Nullstelle eines Polynoms vom Grad ≤ 3. Es folgt $a+e = 0$, $d+e = 0$, $c+e = 0$, $b+c+d+e = 0$, d.h. $a = b = c = d = e$. Es gibt also genau ein normiertes Polynom $n(x) \neq 0$ vom Grad höchstens 4, so dass $n(\alpha^3) = 0$, nämlich

$$n(x) \;:=\; x^4 + x^3 + x^2 + x + 1\,,$$

d.h. $n(x)$ ist das Minimalpolynom von α^3. Das Generatorpolynom des Codes lautet deshalb

$$g(x) \;:=\; m(x)n(x) = x^8 + x^7 + x^6 + x^4 + 1\,.$$

$g(x)$ ist das Produkt der Minimalpolynome von $\alpha, \ldots, \alpha^4$, und nach Satz 24.2 ist der Minimalabstand von C folglich mindestens 5. Der Code kann also 2 Fehler korrigieren. Die Ordnung von α ist 15, und aufgrund Satz 23.5 ergibt sich die Dimension von C als $k = n - \operatorname{grad} g = 7$. Es liegt ein (15,7)-Code vor, d.h. der Code sendet Wörter der Länge 15, die 7 Informationsstellen haben. $c \in \mathbb{F}_2^{15}$ ist genau dann ein Codewort, wenn für das zugehörige Polynom $c(x) \in \mathbb{F}_2[x]/(x^{15} - 1)$

$$c(\alpha) \;=\; c(\alpha^3) \;=\; 0$$

gilt. Genau dann wird $c(x)$ von den Minimalpolynomen $m(x)$ und $n(x)$ geteilt, und damit von $g(x)$.

Codieren. Für das Codieren von Wörtern der Länge 7 bestehen verschiedene Möglichkeiten. Dies kann mit der in Korollar 23.6 angegebenen Generatormatrix geschehen. Übersichtlich ist die folgende Methode. Dem Wort $w = (w_0, \ldots, w_6)$ ordnen wir das Polynom

$$c_1(x) \;=\; w_0x^8 + w_1x^9 + \cdots + w_6x^{14}$$

zu. Wir ergänzen es wie folgt mit einem Polynom $c_2(x)$ vom Grad höchstens 7 zu

$$c(x) \;=\; c_1(x) + c_2(x)\,,$$

so dass $c(x)$ ein Vielfaches von $g(x)$ wird. Für ein Polynom $q(x)$ gilt

$$c_1(x) \;=\; q(x)g(x) - c_2(x) \;=\; q(x)g(x) + c_2(x)\,.$$

$c_2(x)$ ist also eindeutig bestimmt als der Rest, der bei Division von $c_1(x)$ durch $g(x)$ übrig bleibt.

Decodieren. Sei $f = (f_0, \ldots, f_{14})$ der Vektor der Fehler, es wird anstelle von c also die Nachricht $\tilde{c} = c + f$ empfangen. Für die zugehörigen Polynome $f(x)$ und $\tilde{c}(x)$ gilt dann

$$f(\alpha) \;=\; \tilde{c}(\alpha)\,,\; f(\alpha^2) \;=\; \tilde{c}(\alpha^2)\,,\; f(\alpha^3) \;=\; \tilde{c}(\alpha^3)\,,$$

da $c(\alpha) = c(\alpha^2) = c(\alpha^3) = 0$. Der Empfänger kann nun mit Hilfe des quadratischen Polynoms

$$p(x) \;=\; \tilde{c}(\alpha)x^2 + \tilde{c}(\alpha^2)x + \tilde{c}(\alpha^3) + \tilde{c}(\alpha)\tilde{c}(\alpha^2)$$

Fehler korrigieren. Wir unterscheiden drei Fälle:

Fall 1: Gibt es keine Übertragungsfehler, dann gilt $f(x) = 0$ und $p(x) = 0$.

Fall 2: Bei einem Übertragungsfehler ist $f(x)$ von der Gestalt x^r und damit

$$\begin{aligned} p(x) &= \alpha^r x^2 + \alpha^{2r} x + \alpha^{3r} + \alpha^r \alpha^{2r} \\ &= \alpha^r x(x + \alpha^r)\,. \end{aligned}$$

Fall 3: Bei zwei Übertragungsfehlern gilt $f(x) = x^r + x^s$ mit $r \neq s$. In diesem Fall ergibt sich

$$\begin{aligned} p(x) &= (\alpha^r + \alpha^s)x^2 + (\alpha^{2r} + \alpha^{2s})x + \alpha^{3r} + \alpha^{3s} + (\alpha^r + \alpha^s)(\alpha^{2r} + \alpha^{2s}) \\ &= (\alpha^r + \alpha^s)(x + \alpha^r)(x + \alpha^s)\,. \end{aligned}$$

Der Empfänger kann diese Fälle unterscheiden, indem er die Nullstellen von $p(x)$ bestimmt. Genau dann liegt Fall 2 vor, wenn 0 eine (einfache) Nullstelle ist, und ansonsten Fall 3. Gleichzeitig kann er in diesen beiden Fällen r bzw. r, s aus den Nullstellen bestimmen, da α ein primitives Element ist. Er kann also die falsch übertragenen Bits lokalisieren und korrigieren.

BCH-Codes, für die $n = q' - 1$ gilt (wie in obigem Beispiel mit $n = 15$, $q' = 16$), heißen *Reed-Solomon-Codes*. Dann stehen in der ersten Zeile der Kontrollmatrix (24.1) alle von Null verschiedenen Elemente von $\mathbb{F}^{q'}$. Diese Codes werden z.B. in CD-Spielern verwendet. Reed-Solomon-Codes sind besonders gut geeignet, um sogenannte „burst“ Fehler zu korrigieren, d.h. lange Ketten aufeinanderfolgender fehlerhafter Symbole (z.B. durch einen Kratzer). Zudem existieren effiziente Decodieralgorithmen für Reed-Solomon-Codes.