Vorlesung

Algebraische Methoden in der Informatik

Prof. Dr. Peter Hauck

Skript getext von Monika Gehweiler

SS 2005

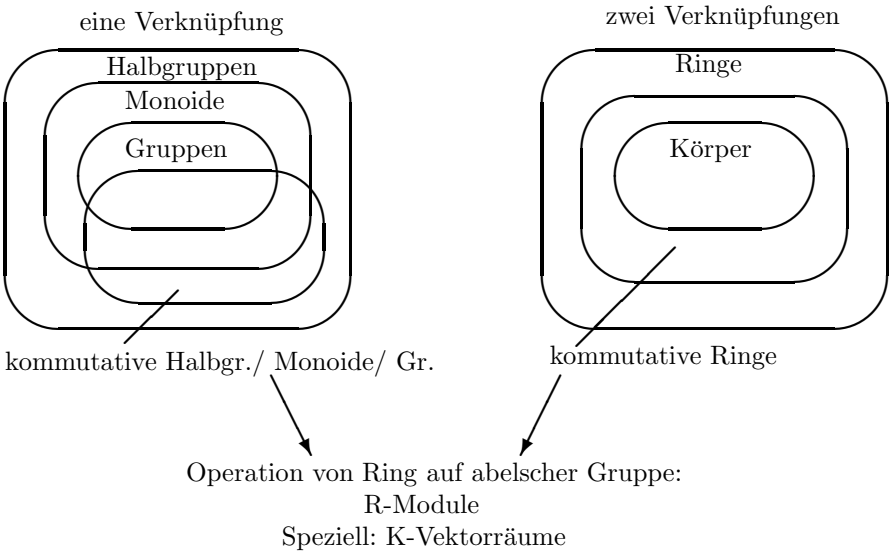
Arbeitsbereich Diskrete Mathematik
Wilhelm-Schickard-Institut
Fakultät für Informations- und Kognitionswissenschaften
Universität Tübingen

Inhaltsverzeichnis

Einleitung

In der Vorlesung werden algebraische Strukturen und Methoden behandelt, die in der Informatik relevant sind; es werden jeweils typische Anwendungen gegeben.

Welche Strukturen werden wir uns ansehen?



Anwendungen in der Informatik:

Monoide, Gruppen: Automatentheorie, formale Sprachen, Graphische Datenverarbeitung, Kryptologie, Abzählmethoden usw.

Ringe: Modulares Rechnen, Codierungstheorie, Rekursionen, Boolsche Algebren usw.

Körper: Kryptologie, Codierungstheorie usw.

Vektorräume (lin. Algebra): Graphische Datenverarbeitung, Robotik, Datenbanken, Kryptologie, Codierungstheorie usw.

Außerdem betrachtet man in der Informatik auch allgemeine algebraische Strukturen (universelle Algebra - Algebren und Signaturen) zur Beschreibung von Datenstrukturen. Hierauf werden wir hier nicht eingehen (vgl. Literatur).
An einigen Stellen der Vorlesung werden wir kurz auf Fragen der Computer-Algebra eingehen, d.h. auf Algorithmen zum Rechnen in gewissen algebraischen Strukturen.

Literatur

1. Ehrig, Mahr, Cornelius, Grosse-Rhode, Zeitz: Mathematisch - strukturelle Grundlagen der Informatik. Springer 2001

2. Garding, Tambour: Algebra for Computer Science. Springer 1998.

3. Gramlich: Anwendungen der linearen Algebra. Fachbuchverlag Leipzig 2004.

4. Grimaldi: Discrete and Combinatorial Mathematics. Addison-Wesley 1994.

5. Kaiser, Mlitz, Zeilinger: Algebra für Informatiker. Springer 1981.

6. Lipson: Elements of Algebra and Algebraic Computing. Benjamin/Cummings Publ.Comp. 1981.

7. Pareigis: Lineare Algebra für Informatiker. Springer 2000.

8. Witt: Algebraische Grundlagen der Informatik. Vieweg 2001.

9. Wolff, Hauck, Küchlin: Mathematik für Informatik und Bioinformatik. Springer 2004.

1 Lineare Algebra und Anwendungen

Wir wiederholen zunächst knapp einige bekannte Begriffe und Sätze aus der linearen Algebra.

1.1 Vektorraum

K heißt *Körper*, wenn $(K,+)$ kommutative Gruppe, $(K \setminus \{0\}, *)$ kommutative Gruppe und die Distributivgesetze gelten.

V ist ein K-*Vektorraum*, wenn

- $(V,+)$ ist kommutative Gruppe
- K operiert auf V, d.h.:
  - $a \in K, v \in V : av \in V$
  - $(a_1 a_2)v = a_1(a_2 v)$
  - $(a_1 + a_2)v = a_1 v + a_2 v$
  - $a(v+w) = av + aw$
  - $1v = v$

Jeder Vektorraum besitzt eine Basis, Dimension.

1.2 Lineare Abbildung

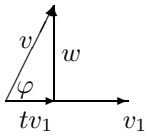
Eine *lineare Abbildung* $\alpha : V \to W$ (V, W $K-$Vektorräume) ist festgelegt durch die Bilder einer Basis. Dies führt zur Darstellungsmatrix $A_\alpha^{\mathcal{B},\mathcal{C}}$ von α bezüglich der Basis $\mathcal{B}$ von V und der Basis $\mathcal{C}$ von W.
Speziell: $\alpha : V \to V : A_\alpha^{\mathcal{B}} \quad (\mathcal{B} = \mathcal{C})$
i-te Spalte von A_α^B = Koordinatenvektor von $\alpha(v_i)$ bzgl $B = (v_1, \ldots, v_n)$.
$v \longrightarrow$ Koordinatenvektor $K_{\mathcal{B}}(v)$ bzgl. $\mathcal{B}$ (Spaltenvektor)
$A_\alpha^B K_B(v) = K_B(\alpha(v))$ (Daher oft Rechnung in K^n)

1.3 Euklidischer Vektorraum

V endlich dimensionaler IR-Vektorraum mit *Euklidischem Skalarprodukt* $(.,.)$.
Dann existiert eine ONB $(v_1, \ldots, v_n) = \mathcal{B}$
$v = \sum \alpha_i v_i,\ w = \sum \beta_i w_i \Rightarrow (v,w) = \sum \alpha_i \beta_i$
$\|v\| := \sqrt{(v,v)} = \sqrt{\sum \alpha_i^2}$ Länge von v
$(v,w) = 0 \Leftrightarrow v, w$ orthogonal
$-1 \leq \frac{(v,w)}{\|v\|\|w\|} \leq 1 \quad (v, w \neq 0) \quad (= \pm 1 \Leftrightarrow v, w$ linear abhängig)
Cauchy-Schwarzsche Ungleichung
$\cos\varphi = \frac{(v,w)}{\|v\|\|w\|} \quad (\varphi \in [0, \pi])$

1.4 Gram-Schmidtsches Orthonormalisierungsverfahren

Sei $v_1, \ldots, v_m$ ein Orthonormalsystem von V.
Sei $v \in V$. Dann ist $v - \sum_{i=1}^{m}(v, v_i)v_i$ zu allen v_i orthogonal.



$(v, v_1) = \cos\varphi \cdot \|v\| \cdot \|v_1\| = \cos\varphi \cdot \|v\| = t$
$w \perp v_1$
$w = v - tv_1$

Dies ist die Grundlage für das *Gram-Schmidtsche Orthonormalisierungsverfahren*:
Ist $v_1, \ldots, v_n$ eine linear unabhängige Teilmenge des Euklidischen Vektorraums V, so existiert ein Orthonormalsystem $w_1, ..., w_n$ mit $\langle v_1, ..., v_i\rangle = \langle w_1, ..., w_i\rangle$, $i = 1, ..., n$.
Wie konstruiert man $w_1, ..., w_n$?
$w_1 = \frac{v_1}{\|v_1\|}$
Seien schon $w_1, ..., w_i$ konstruiert.
Setze $w_{i+1}^{'} = v_{i+1} - \sum_{j=1}^{i}(v_{i+1}, w_j)w_j$. Nach obiger Bemerkung ist $w_{i+1}^{'}$ orthogonal zu $w_1, ..., w_i$.
Setze $w_{i+1} = \frac{w_{i+1}^{'}}{\|w_{i+1}^{'}\|}$. Dann ist klar: $\langle v_1, ..., v_{i+1}\rangle = \langle w_1, ..., w_{i+1}\rangle$.

1.5 Orthogonale Abbildungen

Eine lineare Abbildung $\alpha : V \to V$ (V Euklidischer Vektorraum) heißt *orthogonale Abbildung*, falls $(\alpha(v), \alpha(w)) = (v, w)$, insbesondere $\|\alpha(v)\| = \|v\|$.
Ist $\mathcal{B}$ eine ONB, so ist $A = A_\alpha^B$ eine *orthogonale Matrix*, d.h. $AA^t = A^tA = E_n$.
(Im $\mathbb{R}^n$ mit der kanonischen Orthonormalbasis (e_i) sind orthogonale Abbildungen gerade Multiplikationen mit orthogonalen Matrizen.)

1.6 Satz (QR-Zerlegung)

Sei A eine $k \times n$-Matrix über $\mathbb{R}$ vom Rang s. Die ersten s Spalten von A seien linear unabhängig. Dann gibt es eine orthogonale $k \times k$-Matrix Q und eine obere $k \times n$-Dreiecksmatrix R mit $A = Q \cdot R$, d.h. $Q \cdot Q^t = E_k, R = (r_{ij})$ mit $r_{ij} = 0$ für $i > j$. Dabei gilt sogar: $r_{ij} = 0$ für $s < i \leq k$, alle j (d.h. die letzten $k - s$ Zeilen von R sind Null).

Beweis: Seien $a_1, ..., a_n$ die Spaltenvektoren (der Länge k) von A. Wir wenden das Gram-Schmidtsche Orthonormalisierungsverfahren auf $a_1, ..., a_s$ an und erhalten s Spaltenvektoren (der Länge k) $b_1, ..., b_s$ mit $\langle a_1, ..., a_j\rangle = \langle b_1, ..., b_j\rangle$ für $j = 1, ..., s, (b_i, b_j) = \delta_{ij}$. Also: $a_j = \sum_{l=1}^{i} r_{lj}b_l, \quad j = 1, ..., s$ und $a_m = \sum_{l=1}^{s} r_{lm}b_l$, für $m = s + 1, ..., n$ (da $a_m \in \langle a_1, ..., a_s\rangle = \langle b_1, ..., b_s\rangle$).
Setze $r_{j+1,j} = ... = r_{k,j} = 0$ für $j = 1, ..., s$. Setze schließlich $r_{t,j} = 0$ für $s < t \leq k$ und alle j.
Ergänze $b_1, ..., b_s$ zu einer ONB $b_1, ..., b_k$ von $\mathbb{R}^k$ (falls $k > s$) und setze
$Q = (b_1, ..., b_k), R = (r_{ij})_{\substack{i=1,...,k \\ j=1,...,n}}$.
Dann ist $A = QR$.
R ist von der angegebenen Form, $QQ^t = E_n$, da $(b_i, b_j) = \delta_{ij}$.

$$Q = \left(\overbrace{b_1, ..., b_s}^{s} \middle| \overbrace{b_{s+1}, ..., b_k}^{k-s} \right) \qquad \langle b_1, ..., b_s \rangle = \langle a_1, ..., a_n \rangle$$

$$R = \begin{array}{c} \\ s \\ \\ \\ k-s \\ \\ \end{array} \left(\begin{array}{c|c} \overbrace{\begin{array}{ccc} \star & & \\ & \ddots & \\ 0 & & \star \\ 0 & \dots & 0 \\ \vdots & & \\ 0 & \dots & \end{array}}^{s} & \overbrace{\begin{array}{ccc} & & \\ & \star & \\ & & \\ 0 & \dots & 0 \\ & & \vdots \\ \dots & & 0 \end{array}}^{n-s} \end{array} \right)$$

$\langle b_{s+1}, \dots b_k \rangle = \langle a_1, \dots, a_n \rangle^{\perp}$ in $\mathbb{R}^k$

Bem: Algorithmisch ist es besser, nicht das Gram-Schmidt-Verfahren zu verwenden. Man verwendet besser sogenannte Householder-Matrizen oder Givens-Transformationen.

1.7 Vektorraumbasiertes Information Retrieval

Grundmodell:
Dokumente eines Informationssystems, einer Datenbank, werden als Vektoren $d_m \in \mathbb{R}^k$ dargestellt. Der gesamte Dokumentbestand (n Dokumente) wird dann als $k \times n$-Matrix D dargestellt, deren Spalten die d_m sind.
Was ist k und wie wird d_m für ein Dolument gebildet?
k = Anzahl aller Schlüsselwörter (key words), mit denen die Dokumente beschrieben wurden. Die Schlüssselwörter werden geordnet und die i-te Koordinate von d_m ist eine reelle Zahl $d_{i,m} \geq 0$, die ein Maß dafür ist, wie relevant das i-te Schlüsselwort für das Dokument d_m ist.
(Für die Wahl des Maßes gibt es viele Möglichkeiten; wir gehen hierauf nicht näher ein.)
In der Praxis sind also k und n große Zahlen.
Enzyklopädien: $k \gg n$ (viel mehr Schlüsselwörter als Dokumente)
www: $k \ll n$ (k max $5 \cdot 10^5$ = Anzahl der engl. Wörter, $2 \cdot 10^9 < n$ = Anzahl der Web-Seiten)

Wir machen ein kleines Beispiel:
Dokumentbestand: Bücher

- d_1 Mathematisch-strukturelle Grundlagen der Informatik
- d_2 Anwendungen der linearen Algebra
- d_3 Algebra für Informatiker
- d_4 Lineare Algebra für Informatiker
- d_5 Diskrete Strukturen
- d_6 Algebraische Grundlagen der Informatik
- d_7 Mathematik für Informatik und Bioinformatik

$n = 7$
Schlüsselwörter: (Wortstämme)

- Algebra
- diskret
- Informatik
- linear
- Mathematik
- Struktur

$k = 6$

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

Die Einträge wurden hier so gewählt, dass $d_{i,m} = 1$, falls Schlüsselwort i im Titel d_m vorkommt, sonst 0. (Andere Möglichkeit: relative Häufigkeiten, oder Normierung der Spaltenvektoren auf Länge 1).

Nachfragevektor $q = \begin{pmatrix} q_1 \\ \vdots \\ q_k \end{pmatrix}$ mit $q_i = 1$, falls i-tes Schlüsselwort für die Suche angegeben wird, sonst 0.
Auch hier sind Gewichtungen möglich (Relevanz des Suchbegriffs).

Z.B. $q = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ (Algebra, diskrete Mathematik, Informatik)

Wie geschieht die Suche?
Suche denjenigen Dokumentenvektor d_m, dessen Winkel zu q möglichst klein, d.h. wo $\cos(d_m, q) \in [1, -1]$ möglichst groß ist.
$\cos(d_m, q) = \frac{(d_m, q)}{\|d_m\| \|q\|}$
(Daran sieht man, dass Normierung von d_m und q auf $\|d_m\| = \|q\| = 1$ die Rechnung erleichtert. Das ändert den Winkel nicht. Es ist überdies $\|d_m - q\|^2 = \|d_m\|^2 + \|q\|^2 - 2(d_m, q)$. Bei Normierung: $\|d_m - q\|^2 = 2 - 2\cos(d_m, q)$. Also: $\cos(d_m, q)$ max $\Leftrightarrow$ Abstand zwischen (auf Länge 1 normierten) d_m und q minimal.)

$\cos(d_1, q) = \frac{1+1}{\sqrt{3} \cdot 2} = \frac{1}{\sqrt{3}} \approx 0,577$
$\cos(d_2, q) = \frac{1}{\sqrt{2} \cdot 2} \approx 0,354$
$\cos(d_3, q) = \frac{1+1}{\sqrt{2} \cdot 2} = \frac{1}{\sqrt{2}} \approx 0,707$
$\cos(d_4, q) = \frac{1+1}{\sqrt{3} \cdot 2} \approx 0,577$

$\cos(d_5, q) = \frac{1}{\sqrt{2}\cdot 2} \approx 0,354$
$\cos(d_6, q) \approx 0,707$
$\cos(d_7, q) = \frac{1+1}{\sqrt{2}\cdot 2} \approx 0,707$

Als passendste Dokumente zur Anfrage q werden d_3, d_6, d_7 genannt. Als zweite Gruppe d_1 und d_4. (Ggf. $\cos(d_m, q) \geq 0,5$ als Schwellenwert, d.h. Winkel $\leq 60°$)
Anzahl der Übereinstimmungen:

d_1	2	d_4	2	$\rightarrow d_7$	2
d_2	1	d_5	1		
$\rightarrow d_3$	2	$\rightarrow d_6$	2		

Wir zeigen jetzt, dass man mit Hilfe der QR-Zerlegung von D zum einen eine leichte Beschleunigung des Verfahrens erreichen kann, zum anderen aber auch Hinweise darauf erhält, wie man durch Änderung von D (Rang-Reduktion) redundante Information aus D entfernen kann. Damit werden die Kosten der Suche verringert.
Sei Rang $D = s$.
Wir nehmen an, dass die letzten s Spalten linear unabhängig sind (Umnummerierung von Dokumenten).
$D = QR$ $\quad Q$ ist $k \times k$-Matrix, R ist obere $k \times n$-Dreiecksmatrix.
Beachte: q_i, q_j Spalten von Q, so $(q_i, q_j) = \delta_{ij}$

$$Q = k\{\left(\overbrace{Q_D}^{s} \middle| \overbrace{Q_D^{\perp}}^{k-s}\right) \qquad R = \begin{pmatrix} \overbrace{R_D}^{n} \\ 0 \end{pmatrix} \begin{matrix} \} s \\ \} k-s \end{matrix}$$

$D = Q \cdot R = Q_D \cdot R_D + Q_D^{\perp} \cdot 0 = Q_D \cdot R_D$
(Beachte: Rang D = Rang R = Rang R_D)
$\cos(d_m, q) = \frac{(d_m,q)}{\|d_m\|\|q\|} = \frac{d_m^t q}{\|d_m\|\|q\|} = \frac{(Q_D r_m)^t q}{\underbrace{\|Q_D r_m\|}_{\|Q\left(\frac{r_m}{0}\right)\| = \|\left(\frac{r_m}{0}\right)\| = \|r_m\|} \|q\|}$, dabei sind $r_1, \ldots, r_n$ die Spalten von R_D

$\Rightarrow^{(*)} \cos(d_m, q) = \frac{r_m^t (Q_D^t q)}{\|r_m\|\|q\|} = \frac{(r_m, Q_D^t q)}{\|r_m\|\|q\|}$
- schneller, da R Dreiecksmatrix und $s \leq k$ (häufig $s \ll k$)
- einmal pro Suche berechnen

Wir sehen uns dies auch an einem Beispiel an, wobei wir die Matrix D nur noch aus 5 Dokumenten bestehen lassen (um die Rechnungen etwas zu vereinfachen).

d_1 Mathematisch-strukturelle Grundlagen der Informatik

d_2 Lineare Algebra für Informatiker

d_3 Algebra für Informatiker

d_4 Diskrete Strukturen

d_5 Algebraische Grundlagen der Informatik

Schlüsselwörter:

- Algebra
- dirskret
- Informatik
- linear
- Mathematik
- Struktur

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

Für $q = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$:

$$\begin{aligned} \cos(d_1, q) &= 0,577 \\ \cos(d_2, q) &= 0,577 \\ \cos(d_3, q) &= 0,707 \\ \cos(d_4, q) &= 0,354 \\ \cos(d_5, q) &= 0,707 \end{aligned}$$

QR-Zerlegung von D (z.B. mit Gram-Schmidt):

$$\underbrace{\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}}_{D} = \underbrace{\begin{pmatrix} \underbrace{\begin{matrix} 0 & \frac{3}{\sqrt{24}} & \frac{3}{\sqrt{40}} & \frac{1}{\sqrt{40}} \\ 0 & 0 & 0 & \frac{5}{\sqrt{40}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{24}} & \frac{2}{\sqrt{40}} & -\frac{1}{\sqrt{40}} \\ 0 & \frac{3}{\sqrt{24}} & -\frac{5}{\sqrt{40}} & 0 \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{24}} & -\frac{1}{\sqrt{40}} & -\frac{2}{\sqrt{40}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{24}} & -\frac{1}{\sqrt{40}} & -\frac{3}{\sqrt{40}} \end{matrix}}_{Q_D} & \underbrace{\begin{matrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{24}} \\ 0 & \frac{3}{\sqrt{24}} \\ -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{24}} \\ 0 & 0 \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{24}} \\ 0 & -\frac{3}{\sqrt{24}} \end{matrix}}_{Q_D^\perp} \end{pmatrix}}_{Q} \cdot \underbrace{\left.\begin{pmatrix} \sqrt{3} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{8}{\sqrt{24}} & \frac{5}{\sqrt{24}} & -\frac{1}{\sqrt{24}} & \frac{5}{\sqrt{24}} \\ 0 & 0 & \frac{5}{\sqrt{40}} & -\frac{1}{\sqrt{40}} & \frac{5}{\sqrt{40}} \\ 0 & 0 & 0 & \frac{8}{\sqrt{40}} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}\right\} R_D}_{R}$$

$$= \begin{pmatrix} 0 & 0,612 & 0,474 & 0,158 & 0,577 & -0,204 \\ 0 & 0 & 0 & 0,791 & 0 & 0,612 \\ 0,577 & 0,408 & 0,316 & -0,158 & -0,577 & 0,204 \\ 0 & 0,612 & -0,791 & 0 & 0 & 0 \\ 0,577 & -0,204 & -0,158 & -0,316 & 0,577 & 0,408 \\ 0,577 & -0,204 & -0,158 & 0,474 & 0 & -0,612 \end{pmatrix} \cdot$$

$$\underbrace{\begin{array}{c} R_{11} \\ \left\{ \begin{array}{c} \left(\begin{array}{ccc|cc} 1,732 & 0,577 & 0,577 & 0,577 & 0,577 \\ 0 & 1,633 & 1,021 & -0,204 & 1,021 \\ 0 & 0 & 0,791 & -0,158 & 0,791 \end{array} \right) \\ \hdashline \left(\begin{array}{ccc|cc} 0 & 0 & 0 & 1,265 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \end{array} \right. \begin{array}{l} \} R_{12} \\ \} R_{22} \end{array} \end{array}}_{\begin{pmatrix} R_{11} & R_{12} \\ 0 & R_{22} \end{pmatrix}}$$

Berechnung der $\cos(d_m, q)$ nach $(*)$ S.7:

$\cos(d_m, q) = \frac{(r_m, Q_D^t q)}{\|r_m\| \|q\|} \quad \|q\| = 2$

$$Q_D^t q = \begin{pmatrix} 0 & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{3}{\sqrt{24}} & 0 & \frac{2}{\sqrt{24}} & \frac{3}{\sqrt{24}} & -\frac{1}{\sqrt{24}} & -\frac{1}{\sqrt{24}} \\ \frac{3}{\sqrt{40}} & 0 & \frac{2}{\sqrt{40}} & -\frac{5}{\sqrt{40}} & -\frac{1}{\sqrt{40}} & -\frac{1}{\sqrt{40}} \\ \frac{1}{\sqrt{40}} & \frac{5}{\sqrt{40}} & -\frac{1}{\sqrt{40}} & 0 & -\frac{2}{\sqrt{40}} & \frac{3}{\sqrt{40}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{2}{\sqrt{3}} \\ \frac{4}{\sqrt{24}} \\ \frac{4}{\sqrt{40}} \\ \frac{3}{\sqrt{40}} \end{pmatrix}$$

$\|r_1\| = \sqrt{3}, \|r_2\| = \sqrt{3}, \|r_3\| = \sqrt{2}, \|r_4\| = \sqrt{2}, \|r_5\| = \sqrt{2}$

$\cos(d_1, q) = \frac{(r_1, Q_D^t q)}{\sqrt{3} \cdot 2} = \frac{2}{\sqrt{3} \cdot 2} = \frac{1}{\sqrt{3}} = 0,577$

$\cos(d_2, q) = \frac{(r_2, Q_D^t q)}{\sqrt{3} \cdot 2} = \frac{\frac{2}{3} + \frac{32}{24}}{\sqrt{3} \cdot 2} = \frac{1}{\sqrt{3}} = 0,577$

$\cos(d_3, q) = \frac{(r_3, Q_D^t q)}{\sqrt{2} \cdot 2} = \frac{2}{\sqrt{2} \cdot 2} = \frac{1}{\sqrt{2}} = 0,707$

$\cos(d_4, q) = \frac{(r_4, Q_D^t q)}{\sqrt{2} \cdot 2} = \frac{1}{\sqrt{2} \cdot 2} = 0,354$

$\cos(d_5, q) = \frac{(r_5, Q_D^t q)}{\sqrt{2} \cdot 2} = \frac{2}{\sqrt{2} \cdot 2} = \frac{1}{\sqrt{2}} = 0,707$

Die QR-Zerlegung wird auch benutzt zur sogenannten *Low-Rank-Approximation*.

Ziel: Verändere Dokumentmatrix (d.h. die Dokumentvektoren), um den Rang von D (und damit den Rang von R) zu verkleinern und damit Berechnungen zu vereinfachen, ohne die Ergebnisse zu verfälschen. Beachte: In D steckt ohnehin Unsicherheit durch subjektive Indexierung, Gewichtung usw.

Beobachtung: In R stehen die (betragsmäßig) großen Einträge meist links oben, die kleinen rechts unten.

Betrachte die obige Einteilung $R = \begin{pmatrix} R_{11} & R_{12} \\ 0 & R_{22} \end{pmatrix}$, wobei R_{22} durch die letzten drei Zeilen und die letzten zwei Spalten von R bestimmt wird.

Der "Inhalt" von R_{22} ist klein im Verhältnis zu dem von R. Wir messen dies

durch die Euklidische Norm der Matrix.

$$X \text{ reelle } m \times n\text{-Matrix:} \quad \|X\| = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{m} x_{ij}^2}$$

Es ist $\|R\| = \sqrt{12} = 3,464$, $\|R_{22}\| = 1,265$ und damit $\frac{\|R_{22}\|}{\|R\|} = 0,365$ (klein, aber nicht sehr klein).

Betrachte neue Matrix $\widetilde{R}$, bei der in R der Teil R_{22} zur Nullmatrix geändert wird (Rang $\widetilde{R} = 3 \rightarrow$ Rangreduktion)
$Q\widetilde{R} = D + F$, F "Fehlermatrix" (Rang$(D+F)$=3)
$F = (D+F) - D = Q\widetilde{R} - QR = Q \begin{pmatrix} 0 & 0 \\ 0 & -R_{22} \end{pmatrix}$
$\|F\| = \|R_{22}\|$, da Q orthogonal. Also $\frac{\|F\|}{\|D\|} = \frac{\|R_{22}\|}{\|R\|} \approx 0,365$.
36,5% relative Änderung in D. Man verwendet $\widetilde{D} = D + F$ anstelle von D. Dabei muss man $D + F$ gar nicht berechnen.

(In unserem Fall: $F = Q \begin{pmatrix} 0 & 0 \\ 0 & -R_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -\frac{8}{\sqrt{40}} & 0 \\ 0 & 0 & 0 & -\frac{40}{\sqrt{40}} & 0 \\ 0 & 0 & 0 & \frac{8}{\sqrt{40}} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{16}{\sqrt{40}} & 0 \\ 0 & 0 & 0 & -\frac{24}{\sqrt{40}} & 0 \end{pmatrix}$
$D + F$ ändert sich in der vierten Spalte:
$d_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \longrightarrow \widetilde{d}_4 = \begin{pmatrix} -1,265 \\ -5,325 \\ 1,265 \\ 0 \\ 2,530 \\ -2,795 \end{pmatrix}$.)
Man berechnet nach $(*)$ S.7: $cos(\widetilde{d}_m, q) = \frac{(\widetilde{r}_m, \widetilde{Q}_D^t q)}{\|\widetilde{r}_m\| \|q\|}$
Dabei ist $\widetilde{Q}_D$ die um die letzte Spalte verkleinerte Matrix Q_D und $\widetilde{Q}_D^t q$ der um die letzte Position verkleinerte Vektor $Q_D^t q$.

Beispiel:

- An dem $\cos(\widetilde{d}_m, q) = \cos(d_m, q), m = 1, 2, 3, 5$ ändert sich nichts, da die vierte Position von r_m für diese m ohnehin 0 ist.
  $\|\widetilde{r}_4\| = \frac{\sqrt{2}}{\sqrt{5}}$
  $\cos(\widetilde{d}_4, q) = \frac{\sqrt{5} \cdot 2}{\sqrt{2} \cdot 2 \cdot 5} = \frac{1}{\sqrt{2} \cdot \sqrt{5}} \approx 0,316$ (früher: $\cos(d_4, q) \approx 0,354$)
  An der Rangfolge hat sich *nichts* geändert.

- Wir testen noch einen anderen "Nachfrage"-Vektor $q_0 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

  (Schlüsselwort: Informatik)

Ursprüngliche Matrix D	Neue Matrix $\widetilde{D}$
$\cos(d_1, q_0) = \frac{1}{\sqrt{3}} \approx 0,577$	$\cos(d_m, q_0), m = 1,2,3,5$ ändert sich nicht
$\cos(d_2, q_0) = \frac{1}{\sqrt{3}} \approx 0,577$	$\cos(\widetilde{d}_4, q_0) \approx 0,193$
$\cos(d_3, q_0) = \frac{1}{\sqrt{2}} \approx 0,707$	
$\cos(d_4, q_0) = 0$	
$\cos(d_5, q_0) = \frac{1}{\sqrt{2}} \approx 0,707$	

Mit Schlüsselwort „Mathematik“ gilt sogar $\cos(\widetilde{d}_4, q_1) \approx 0,386$. Einziges anderes $\neq 0$: $\cos(d_1, q_1) = 0,577$

Also:
Rang-Reduktion vereinfacht Rechnungen. Häufig verfälscht sie die Ergebnisse nicht wesentlich. Es kann aber passieren, dass relevante Dokumente nicht mehr ausgegeben werden, oder irrelevante Dokumente ausgegeben werden.

Beispiel:
Der erste Fall tritt z.B. auf, wenn man bei unserem D nur eine Vertauschung der Spalten vornimmt:

$$D_0 = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Somit 2. Spalte von D = 4. Spalte von D_0, 3. Spalte von D = 2. Spalte von D_0 und 4. Spalte von D = 3. Spalte von D_0.

$$D_0 = \begin{pmatrix} 0 & 0,775 & 0,158 & 0 & 0,577 & -0,204 \\ 0 & 0 & 0,791 & 0 & 0 & 0,612 \\ 0,577 & 0,516 & -0,158 & 0 & -0,577 & 0,204 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0,577 & -0,258 & -0,316 & 0 & 0,577 & 0,408 \\ 0,577 & -0,258 & 0,474 & 0 & 0 & -0,612 \end{pmatrix} \cdot$$

$$\begin{pmatrix} 1,732 & 0,577 & 0,577 & 0,577 & 0,577 \\ 0 & 1,291 & -0,258 & 1,291 & 1,291 \\ 0 & 0 & 1,265 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(Hier sogar nur: $\frac{\|R_{22}\|}{\|R\|} \approx 0,289$)

Ersetzt man die 1 in der 4. Zeile von R durch 0, so liefert $q_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ (Stichwort „linear“) $\cos(\widetilde{d}_m, q_2) = 0$ für alle $m = 1, \ldots, 5$. D.h. das einzige relevante

Dokument d_4 wurde so geändert, dass Eintrag 0 an Stelle 4! $d_4 = \begin{pmatrix}1\\0\\1\\1\\0\\0\end{pmatrix} \rightarrow \begin{pmatrix}1\\0\\1\\0\\0\\0\end{pmatrix}$

Nähere Informationen zu Vektorraumbasiertem Information Retrieval: Berry, Drmač, Jessup: Matrices, Vector Spaces and Information Retrieval. SIAM Review 41, 335-362. 1999.

Wir geben eine zweite Anwendung der linearen Algebra an, nämlich im Bereich der *Codierungstheorie*.

1.8 Lineare Codes

Ziel der Codierungstheorie:
Finde ein Verfahren zur Codierung von Nachrichten, die über einen Kanal mit Störungen übertragen werden, so dass Änderungen bei der Übertragung entdeckt und gegebenfalls korrigiert weren können. ("Übertragung" kann auch "Speicherung", "Dateneingabe" usw. bedeuten.)

Wie geschieht das: Hinzufügen von *Redundanz*
Einfachstes Beispiel: *Parity Check*

Block der Länge $n-1$ über $\{0,1\}$ = Nachricht. (Ggf. Nachricht in mehrere Blöcke der Länge $n-1$ zerlegen.)
Verlängere Block zur Länge n durch zusätzliches Bit, so dass der verlängerte Block eine gerade Anzahl von Einsen hat.

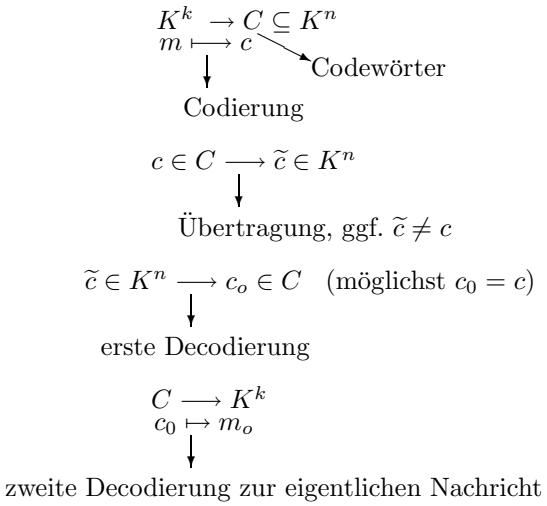
$\mathbb{Z}_2 = \{0,1\}$ ist Körper (Rechnen mod 2)

Obiges Parity-Check-Verfahren: Summe der Blockeinträge = 0 (in $\mathbb{Z}_2$).
Die gültigen Codewörter bilden also einen Unterraum
$\{x \in \mathbb{Z}_2^n \ : \ x = (x_1, \ldots, x_n), \sum x_i = 0\}$ in $\mathbb{Z}_2^n$.

Die ist ein Beispiel für einen *linearen Code*.

Allgemein:
Sei K ein endlicher Körper, z.B. $K = \mathbb{Z}_2$ oder $K = \mathbb{Z}_p, p$ Primzahl (ganze Zahlen mod p).
Ein *linearer Code* C der Länge n und Dimension k, $k \leq n$, ist ein Unterraum der Dimension k von K^n.

Ursprüngliche Nachrichten: Elemente in K^k



Ziele: Bestimme C so, dass

- möglichst viele Fehler bei der Übertragung erkannt werden und ggf. korrigiert werden können.
- k im Vergleich zu n nicht zu klein ist (Effizienz).
- Codierung und v.a. die (erste) Decodierung schnell möglich sind.

Wie funktioniert die (erste) Decodierung?
Wenn man davon ausgehen kann, dass bei der Übertragung relativ wenige Fehler auftreten, so wird man ein empfangenes Wort, wenn es nicht schon ein Codewort ist, zu einem möglichst ähnlichen Codewort decodieren.

Wie misst man Ähnlichkeit?
Definition
Sei K ein endlicher Körper, $n \in \mathbb{N}$

1. Ist $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$, so ist $w(x) = |\{i : x_i \neq 0\}|$ das *(Hamming-)Gewicht* von x.
   (R.W.Hamming, 1915-1998, Bell Labs, 1950 grundleg. Arbeit zur Codierungstheorie)
2. $x, y \in K^n, \quad d(x,y) := w(x-y)$ *Hamming-Abstand*

Es gilt:

1. w ist etwas Ähnliches wie die Norm auf $\mathbb{R}$-Vektorräumen:
   (a) $w(x) = 0 \Leftrightarrow x = 0$
   (b) $w(ax) = w(x) \ \ \forall\, 0 \neq a \in K$

   (c) $w(x+y) \leq w(x) + w(y)$

2. d ist translations-invariante Metrik:

   (a) $d(x,y) = 0 \Leftrightarrow x = y$
   (b) $d(x,y) = d(y,x)$
   (c) $d(x,y) \leq d(x,z) + d(z,y)$
   (d) $d(x,y) = d(x+z, y+z)$

Hamming-Decodierung: Decodiere ampfangenes Wort $\in K^n$ zu einem Codewort mit minimalem Hamming-Abstand (i.d.R. nicht eindeutig).

Minimalgewicht $w(C)$ eines Codes: $\min\{w(x) : x \neq 0, x \in C\}$.
Ist C ein linearer Code, so ist $w(C) = \min\{d(c,c') : c, c' \in C, c \neq c'\}$

Definition:
Ein linearer Code C der Länge n über K heißt *t-fehlererkennend*, falls $w(C) \geq t+1$ und *t-fehlerkorrigierend*, falls $w(C) \geq 2t+1$.

Satz:

1. Sei C ein t-fehlererkennender Code. Ist $c \in C$, so gibt es kein $c' \in C, c' \neq c$ mit $d(c,c') \leq t$.
   (Sind also max. t Fehler und mindestens ein Fehler aufgetreten, so wird das erkannt.)

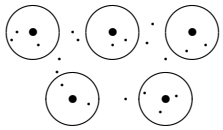
2. Sei C ein t-fehlerkorrigierender Code. Dann gibt es zu jedem $x \in K^n$ höchstens ein $c \in C$ mit $d(x,c) \leq t$.
   (Wenn also bei Übertragung eines Codewortes maximal t Fehler aufgetreten sind, so wird bei Hamming-Decodierung korrekt decodiert.)

Beweis. 1. Umformung der Definition

2. Angenommen, es existieren $c, c' \in C, c \neq c'$ mit $d(x,c) \leq t$ und $d(x,c') \leq t$. Dann $d(c,c') \leq d(c,x) + d(x,c') \leq 2t$ was ein Widerspruch ist.

□

t-fehlerkorrigierender Code:



In jeder "Kugel" vom Radius t um Codewörter liegt kein weiteres Codewort

$K_t(c) = \{x \in K^n : d(x,c) \leq t\}$ "Kugel" vom Radius t um c

Beispiel:

$C \subseteq \mathbb{Z}_2^5$ Basis von C: $\underbrace{\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix}}_{g_1}, \underbrace{\begin{pmatrix}0\\1\\1\\1\\0\end{pmatrix}}_{g_2}, \underbrace{\begin{pmatrix}1\\0\\1\\0\\1\end{pmatrix}}_{g_3}$ (klar: lin. unabh.)

$|C| = 2^3 = 8$

Neben Nullvektor und den Basisvektoren enhält C noch:

$$\underbrace{\begin{pmatrix}1\\0\\1\\1\\0\end{pmatrix}}_{g_1+g_2}, \underbrace{\begin{pmatrix}0\\1\\1\\0\\1\end{pmatrix}}_{g_1+g_3}, \underbrace{\begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix}}_{g_2+g_3}, \underbrace{\begin{pmatrix}0\\0\\0\\1\\1\end{pmatrix}}_{g_1+g_2+g_3}$$

$w(C) = 2$

z.B. $x = \begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}$ empfangen, $x \notin C$

Es ist unklar, ob man x zu $\begin{pmatrix}1\\0\\1\\1\\0\end{pmatrix} \in C$ oder zu $\begin{pmatrix}0\\1\\1\\1\\0\end{pmatrix} \in C$ decodieren soll.

Das sind alle Vektoren in C, die Absand 1 zu x haben.

Aufgabe:

Gibt es einen 3-dim. Code C der Länge 5 über $\mathbb{Z}_2$ mit $w(C) = 3$?

Wie sieht es bei Länge 6 aus? - Ja: $\left\langle \begin{pmatrix}1\\1\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\\0\\1\end{pmatrix} \right\rangle$

Beste Situation: C t-fehlerkorrigierend und $K^n = \dot{\bigcup}_{c\in C} K_t(c)$. Solche Codes heißen *perfekt*.

Wir geben die Konstruktion einer Familie perfekter linearer Codes an. (Viel mehr gibt es auch nicht!)

Wir benötigen dazu die Beschreibung von Codes durch Erzeugermatrizen und Kontrollmatrizen:

Sei C ein k-dim. Code der Länge n über K, $g_1 = \begin{pmatrix}g_{11}\\ \vdots \\ g_{n1}\end{pmatrix}, \ldots, g_k = \begin{pmatrix}g_{1k}\\ \vdots \\ g_{nk}\end{pmatrix}$ eine Basis von C.

Dann heißt $G = \begin{pmatrix}g_{11} & \cdots & g_{1k}\\ \vdots & & \vdots \\ g_{n1} & \cdots & g_{nk}\end{pmatrix}_{n\times k}$ eine *Erzeugermatrix* von C.

Erzeugermatrizen dienen der Codierung ursprünglicher Nachrichten (Elemente in K^k) in Elemente in $C \subseteq K^n$: $C = \{Gu : u \in K^k\}$

Beweis. Ist $u = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_k \end{pmatrix} \in K^k$, so ist $Gu = \mu_1 g_1 + \cdots + \mu_k g_k \in C$. Also $Gu \subseteq C$.
Umkehrung analog, da sich jedes Element von C als Linearkombination der $g_1, \ldots, g_k$ schreiben lässt. □

Also: Codierung $u \mapsto Gu$.

Am schönsten ist das, wenn $G = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ \star & \ldots & \star \\ \star & \ldots & \star \end{pmatrix}$ (Nicht jeder Code muss eine entsprechende Basis besitzen.)

In diesem Fall: $Gu = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_k \\ \star \\ \star \end{pmatrix}$, d.h. die Codewörter enthalten an den ersten k Stellen die ursprüngliche Nachricht, der Rest sind Redundanzelemente.

Die Beschreibung durch eine Kontrollmatrix entspricht der Beschreibung von Unterräumen als Lösungsräume homogener linearer Gleichungssysteme.

Satz:
Sei C ein k-dimensionaler Code der Länge n über K. Dann existiert eine $n \times (n-k)$-Matrix H über K, so dass für $x \in K^n$ gilt:

$$x \in C \Leftrightarrow x^t H = 0$$

H heißt *Kontrollmatrix* von C.
(Insb. $G^t H = 0$ für jede Erzeugermatrix G von C)

Also: Kontrollmatrix liefert schnelle Art der Fehlererkennung.

Beweis. Sei $g_1, \ldots, g_k$ eine Basis von C, $G = (g_1, \ldots, g_k)$, $g_i = \begin{pmatrix} g_{1i} \\ \vdots \\ g_{ni} \end{pmatrix}$.
Betrachte das lineare Gleichungssystem mit Koeffizientenmatrix G^t:

$$\begin{aligned} g_{11}t_1 + \cdots + g_{n1}t_n &= 0 \\ &\vdots \\ g_{1k}t_1 + \cdots + g_{nk}t_n &= 0 \end{aligned}$$

G^t hat Rang k, also Dimension des Lösungsraums $n-k$.
Sei $h_1, \ldots, h_{n-k} \in \mathbb{F}_q^n$ Basis des Lösungsraums, $H = (h_1, \ldots, h_{n-k})_{n \times (n-k)}$.
Dann gilt: $G^t h_i = 0, i = 1, \ldots, n-k$, d.h. $G^t H = 0$, d.h. $g_i^t H = 0$ für alle g_i.
Also: $C \subseteq \ker H$.

$\dim \ker H = n - \text{Rang } H = n - (n-k) = k$.
Also: $C = \ker H$. $\quad x^t H = 0 \Leftrightarrow x \in C$. □

Beispiel:

$K = \mathbb{F}_2 \quad C = \left\langle \begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\\1\end{pmatrix} \right\rangle$, Erzeugermatrix $G = \begin{pmatrix}1&0&1\\1&1&0\\0&1&1\\0&1&0\\0&0&1\end{pmatrix}$,

Kontrollmatrix:
$$\begin{array}{ccccccccc} t_1 & + & t_2 & & & & & = 0 \\ & & t_2 & + & t_3 & + & t_4 & = 0 \\ t_1 & & & + & t_3 & & & + & t_5 & = 0 \end{array},$$

Basis des Lösungsraums: $\begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}$, $\quad H = \begin{pmatrix}1&1\\1&1\\0&1\\1&0\\1&0\end{pmatrix}$

An der Kontrollmatrix kann man das Minimalgewicht eines Codes ablesen:
Satz:
Sei C ein k-dimensionaler Code der Länge n über K, $C \neq \{0\}$. Sei H die Kontrallmatrix von C. Dann gilt:

$$\begin{aligned} w(C) &= \min\{r \in \mathbb{N} : \text{es gibt } r \text{ linear abhängige Zeilen in } H\} \\ &= \max\{r \in \mathbb{N} : \text{je } r-1 \text{ Zeilen von } H \text{ sind linear unabhängig}\} \end{aligned}$$

(Insbesondere: $w(C) \leq rg(H) + 1$)

Beweis. Seien $z_1, \ldots, z_n$ die Zeilenvektoren von H (Länge $n-k$). Da $C \neq \{0\}$, existiert $0 \neq x = \begin{pmatrix}\mu_1\\ \vdots \\ \mu_n\end{pmatrix} \in C$.
$x^t H = 0$, d.h. $H^t x = 0$, d.h. $\mu_1 z_1 + \cdots + \mu_n z_n = 0$; also sind $z_1, \ldots, z_n$ linear abhängig.
Sei $w \in \mathbb{N}$ minimal, so dass es w linear abhängige Zeilen gibt, etwa $z_{i_1}, \ldots z_{i_w}$. Dann ex. $\lambda_j \in K$ mit $\sum_{j=1}^n \lambda_j z_j = 0$ und $\lambda_j \neq 0$ genau für $j = i_1, \ldots, i_w$.
Für $c = \begin{pmatrix}\lambda_1\\ \vdots \\ \lambda_n\end{pmatrix}$ gilt $H^t c = 0$, d.h. $c^t H = 0$, d.h. $c \in C$ und $w(c) = w$. Also: $w(C) \leq w$.
Angenommen es gibt $0 \neq \overline{c} \in C$ mit $\overline{w} = w(\overline{c}) < w$. Dann folgt aus $H^t \overline{c} = 0$, dass es $\overline{w}$ linear abhängige Zeilen in H gibt. Dies ist ein Widerspruch zur Wahl von w. Also: $w(C) = w$. □

Beispiel:
Bsp von vorne (S.17). Wir wissen schon: $w(C) = 2$.

Jetzt mit obigem Satz. $H = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}$

In H gibt es zwei linear abhängige Zeilen (z.B. 1. und 2. Zeile), keine Zeile ist Nullzeile. Also: $\min\{r \in \mathbb{N} : \text{es gibt } r \text{ lin. abh. Zeilen in H}\} = 2 = w(C)$

Wir können jetzt, wie angekündigt, eine wichtige Familie von perfekten Codes konstruieren, die sogenannten *Hamming-Codes*.

Sei q eine Primzahlpotenz. Dann gibt es einen Körper K mit $|K| = q$ (siehe später).

Sei $l \in \mathbb{N}, l \geq 2,\ n = \frac{q^l-1}{q-1}$. Dann gibt es einen perfekten Code über K der Länge n, Dimension $n - l$ und Minimalgewicht 3: *Hamming-Code*.

Konstruktion:
K^l enhält genau $q^l - 1$ viele von 0 verschiedene Vektoren, je $q - 1$ von ihnen erzeugen den gleichen 1-dim. Unterraum. Also hat K^l genau $n = \frac{q^l-1}{q-1}$ viele 1-dim. Unterräume.

Wähle aus jedem einen Vektor $\neq 0$. Schreibe diese als Zeilenvektoren und bilde daraus eine $n \times l$-Matrix H.

Sei C der Code mit Kontrollmatrix H, d.h. $C = \{x \in K^n : x^t H = 0\}$.

Klar: Rang $H = l$ (denn H enhält l linear unabhängige Zeilen - nämlich (bis auf skalare Vielfache) jede Basis von K^l - und größer kann der Rang nicht werden).

Also: $\dim C = n - l, |C| = q^{n-l}$.

Je zwei Zeilen sind linear unabhängig, aber es gibt drei linear abhängige Zeilen. Nach vorigem Satz (beachte $l \geq 2$): $w(C) = 3$

C ist perfekt:
Kugeln vom Radius 1 um Codewörter sind disjunkt. Jede solche Kugel enthält $1 + n(q - 1)$ viele Elemente des K^n.

$q^{n-l}(1 + n(q - 1)) = q^{n-l}(1 + \frac{q^l-1}{q-1}(q - 1)) = q^{n-l} \cdot q^l = q^n$.

Beh. folgt.

Beispiel:

$q = 2, l = 2 : n = 3$ und $k = 1$ uninteressant $C = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$

$q = 2, l = 3 : n = 7, k = 4 \quad H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

Basis des binären [7,4]-Hamming-Codes

$$\begin{aligned}(a_1,\ldots,a_7)^t \in C \quad \Leftrightarrow \quad & a_1+a_4+a_5+a_7=0\\ & a_2+a_4+a_6+a_7=0\\ & a_3+a_5+a_6+a_7=0\end{aligned}$$

Basis: $g_1=\begin{pmatrix}1\\0\\0\\0\\0\\1\\1\end{pmatrix}, g_2=\begin{pmatrix}0\\1\\0\\0\\1\\0\\1\end{pmatrix}, g_3=\begin{pmatrix}0\\0\\1\\0\\1\\1\\1\end{pmatrix}, g_4=\begin{pmatrix}0\\0\\0\\1\\1\\1\\0\end{pmatrix}$

z.B. $x=\begin{pmatrix}1\\0\\0\\0\\1\\0\\1\end{pmatrix}$ wird empfangen. $x^tH=(1,1,0)\neq(0,0,0)$, d.h. $x\notin C$.

Eindeutige Decodierung: $c=g_1+g_4=\begin{pmatrix}1\\0\\0\\1\\1\\0\\1\end{pmatrix}\in C, d(c,x)=1$. Decodierung zu c.

Ursprüngliche Nachricht $\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$ (falls codiert wurde $u\mapsto Gu, u\in\mathbb{F}_2^4$ $G=(g_1,g_2,g_3,g_4)$)

2 Halbgruppen, Monoide und formale Sprachen

2.1 Definition

1. Eine Menge H mit einer Verknüpfung $\cdot : H \times H \to H : (g,h) \mapsto g \cdot h$ heißt *Halbgruppe* $(H, \cdot)$, wenn die Verknüpfung *assoziativ* ist:
   $(g \cdot h) \cdot k = g \cdot (h \cdot k)\ \forall g,h,k \in H$.
   (Das Symbol für die Verknüpfung kann in konkreten Beispielen auch anders sein.)

2. Besitzt die Halbgruppe $(H, \cdot)$ ein *neutrales Element* e, d.h. $e \cdot h = h \cdot e = h\ \forall h \in H$, so heißt $(H, \cdot)$ *Monoid*
   (Neutrales Element ist eindeutig: $e_1 = e_1 \cdot e_2 = e_2$.)

2.2 Beispiele

1. $(\mathbb{N}, +)$ Halbgruppe, kein Monoid
   $(\mathbb{N}_0, +)$ Monoid
   $(\mathbb{N}, \cdot)$ Monoid

2. $(\mathbb{Z}, +)$ Monoid
   $(\mathbb{Z}, -)$ keine Halbgruppe $((3-4)-5 = -6, 3-(4-5) = 4)$

3. $\mathcal{P}(M)$ Potenzmenge der Menge M
   $(\mathcal{P}(M), \cup)$ und $(\mathcal{P}(M), \cap)$ sind Monoide

4. Sei X eine endliche Menge (Alphabet), $H = X^+$ die Menge aller endlichen (nicht-leeren) Wörter (Strings) über dem Alphabet X.
   Dann ist H mit Hintereinanderschreiben (Konkatenation) als Verknüpfung eine Halbgruppe.
   $H = X^* = X^+ \cup \{\varepsilon\}$, ε leeres Wort, ist Monoid (*nicht* kommutativ)

5. Sei M eine Menge, $H = Abb(M, M)$ die Menge aller Abbildungen von M nach M. Dann ist H bzgl. Hintereinanderausführung $\circ$ (Komposition) von Abbildungen eine Halbgruppe:

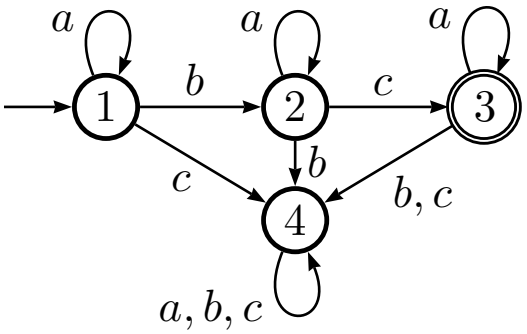
   $$(g \circ f)(m) := g(f(m)).$$

   H ist Monoid mit id_M als neutrales Element.
   (H nicht kommutativ, wenn $|M| > 1$).

6. Sei $\mathcal{A} = (Z, \delta, z_0, E)$ ein endlicher deterministischer Automat über dem endlichen Eingabealphabet X, d.h.

   - Z ist eine endliche Menge (die Menge der Zustände)
   - $z_0 \in Z$ der Anfangszustand
   - $E \subseteq Z$ eine Menge von Endzuständen
   - $\delta : Z \times X \to Z$ Übergangsfunktion

   Bildliche Darstellung (Beispiel):
   $X = \{a,b,c\}, \quad Z = \{1,2,3,4\}, \quad z_0 = 1, \quad E = \{3\}$



$\delta(1,a) = 1,$
$\delta(1,b) = 2,$
$\delta(1,c) = 4, ...$

(Der Anfangszustand wir mit eingehendem Pfeil gekennzeichnet, Endzustände durch Doppelkreise.)
Man schreibt $z \cdot x$ für $\delta(z,x)$.

Wichtige Frage bei Automaten: Welche Sprache L akzeptiert $\mathcal{A}$?

$L \subseteq X^*$: L = $\{w = x_1 \dots x_n$: nach Eingabe von $x_1, \dots, x_n$ befindet sich $\mathcal{A}$ in einem Endzustand, wenn er sich zu Beginn im Anfangszustand befunden hat$\}$
= Zeichenketten, die einen Pfad von z_0 zu einem Endzustand beschreiben.

In obigem Beispiel: $L = a^*ba^*ca^* = \{a^nba^mca^l \mid n,m,l \in \mathbb{N}_0\}$

Ist $w \in X^*$ ein Wort, so induziert w eine Abbildung $f_w : Z \to Z$ folgendermaßen:

$w = \varepsilon$	, so $f_\varepsilon(z) = z$			$\forall z \in Z$
$w = x \in X$	, so $f_x(z) = \delta(z,x)$	$=:$	zx	$\forall z \in Z$
$w = x_1 \dots x_n$	, so $f_w(z) = \delta(f_{x_1 \dots x_{n-1}}(z), x_n)$	$=$	$((zx_1)x_2) \dots x_n$	$=: zw$

$\{f_w | w \in X^*\}$ bildet ein Monoid bzgl $\cdot$: $f_{w_1} \cdot f_{w_2} := f_{w_2} \circ f_{w_1}$, d.h. $f_{w_1} \cdot f_{w_2} = f_{w_1 w_2}$
$(f_{w_1} \cdot f_{w_2})(z) = f_{w_2}(f_{w_1}(z)) = z w_1 w_2$.
Neutrales Element: f_ε.
Wir bezeichnen dieses Monoid mit $M(\mathcal{A})$, *Übergangsmonoid* von $\mathcal{A}$ (transition monoid).

Obiges Beispiel:

$w \in a^*$	$f_w = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$	$= id_z$	$=: 1$
$w \in a^*ba^*$	$f_w = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 4 & 4 \end{pmatrix}$		$=: \alpha$
$w \in a^*ca^*$	$f_w = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 4 & 4 \end{pmatrix}$		$=: \beta$
$w \in a^*ba^*ca^*$	$f_w = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 4 & 4 \end{pmatrix}$		$=: \gamma$
übrige w	$f_w = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$		$=: 0$

(Die übrigen w liegen in $a^*ba^*bX^* \cup a^*ba^*ca^*bX^* \cup a^*ba^*ca^*cX^* \cup a^*ca^*bX^* \cup a^*ca^*cX^*$.)

Verknüpfungstafel:

	1	α	β	γ	0
1	1	α	β	γ	0
α	α	0	γ	0	0
β	β	0	0	0	0
γ	γ	0	0	0	0
0	0	0	0	0	0

Konstruktion von Halbgruppen/ Monoiden ("aus alt mach neu")

2.3 Definition

Seien $H_1, \ldots, H_n$ Halbgruppen (bzw. Monoide).
Das kartesische Produkt $H_1 \times \cdots \times H_n = \{(a_1, \ldots, a_n) | a_i \in H_i\}$ ist Halbgruppe (bzw. Monoid) bzgl. $(h_1, \ldots, h_n) \cdot (g_1, \ldots, g_n) = (h_1 g_1, \ldots, h_n g_n)$.
Direktes Produkt

Beispiel: $H_i = (\mathbb{R}, +), H_1 \times \cdots \times H_n = (\mathbb{R}^n, +)$ (komponentenweise Addition).

2.4 Definition

Sei $(H, \cdot)$ Halbgruppe.

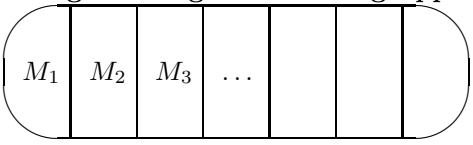
1. $\emptyset \neq U \subseteq H$ heißt *Unterhalbgruppe* von H, falls U mit der Verknüpfung $\cdot$ eine Halbgruppe ist.
   (D.h. $\forall u_1, u_2 \in U : u_1 \cdot u_2 \in U$)

2. Ist H Monoid, so heißt die Unterhalbgruppe U *Untermonoid* von H, falls $e_H \in U$. (Dann ist e_H das neutrale Element von U.)

Beispiele

- $(\mathbb{N}, \cdot)$ Untermonnoid von $(\mathbb{Z}, \cdot)$
- $(\mathbb{N}, +)$ Unterhalbgruppe von $(\mathbb{Z}, +)$, aber *kein* Untermonoid
- $(\mathbb{N}_0, +)$ Untermonoid von $(\mathbb{Z}, +)$
- $k \in \mathbb{Z}$. $(k\mathbb{Z}, +)$ Untermonoid von $(\mathbb{Z}, +)$
- $A \subseteq M$. $\{A\}$ ist Unterhalbgruppe von $(\mathcal{P}(M), \cup)$
  Ist $A \neq \emptyset$, so kein Untermonoid, obwohl $(\{A\}, \cup)$ Monoid

"Vergröberung" einer Halbgruppe.



Gegeben Partition $H = \bigcup_{i \in I} M_i$;
$M_i \neq \emptyset,\ M_i \cap M_j = \emptyset\ \ \forall i, j \in I,\ i \neq j.$

$\{M_i \mid i \in I\}$ soll zu Halbgruppe gemacht werden, wobei die Verknüpfung von der aus H abstammt.

Forderung: Definiere $M_k \odot M_j \in \{M_i \mid i \in I\}$ so, dass

$$\forall k, j \; \forall a \in M_k, b \in M_j : a \cdot b \in M_k \odot M_j$$

Für welche Partitionen geht das?

Dazu: Zusammenhang: Äquivalenzrelationen $\leftrightarrow$ Partitionen

Äquivalenzrelation $\sim$ auf H:
(1) $h \sim h \;\; \forall h \in H$ (Reflexivität)
(2) $g \sim h \Rightarrow h \sim g$ (Symmetrie)
(3) $g \sim h, \; h \sim k \Rightarrow g \sim k$ (Transitivität)
(Die einfachste Äquivalenzrelation ist $=$.)

Für $g \in H$ ist $[g] = \{h \in H | g \sim h\}$ Äquivalenzklasse von g.
$[g] = [h] \Leftrightarrow g \sim h$
H ist die disjunkte Vereinigung der verschiedenen Äquivalenzklassen: Partition.

Umgekehrt:
Partition $H = \bigcup_{i \in I} M_i$
Definiere Relation $\sim$ auf H: $g \sim h \Leftrightarrow \exists i \in I : g, h \in M_i$

Äquivalenzrelation, Äquivalenzklassen sind gerade die M_i.

Obige Forderung lautet in der Sprache der Äquivalenzrelationen:

$$(*) \quad g' \sim g \text{ und } h' \sim h, \text{ so } g' \cdot h' \sim g \cdot h$$

2.5 Definition

Eine Äquivalenzrelation auf einer Halbgruppe, die die Bedingung $(*)$ erfüllt, heißt *Kongruenzrelation*.

2.6 Satz

1. Ist $(H, \cdot)$ eine Halbgruppe, $\sim$ eine Kongruenzrelation auf H, so wird die Menge der Äquivalenzklassen $\{[h] | h \in H\}$ zu einer Halbgruppe bezüglich der Verknüpfung $[g] \odot [h] := [g \cdot h]$
   Sie heißt *Quotienten-* oder *Faktorhalbgruppe* von H nach $\sim$: $H/\sim$

2. Ist $(H, \cdot)$ ein Monoid, so auch $(H/\sim, \odot)$: neutrales Element: $[e]$

2.7 Beispiele

1. $H = (\mathbb{Z}, +)$
   $n \in \mathbb{N} : \; a, b \in \mathbb{Z}. \; a \equiv b \mod n \;\Leftrightarrow\; n | a - b$
   Kongruenzrelation auf $\mathbb{Z}$
   Äquivalenzklassen: $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}, \; r = 0, 1, \ldots, n-1$
   In $\mathbb{Z}/\equiv \mod n$: $(r + n\mathbb{Z}) + (s + n\mathbb{Z}) = (r + s + n\mathbb{Z})$.
   Schreibweise: $\mathbb{Z}/n\mathbb{Z}$ statt $\mathbb{Z}/\equiv \mod n$

2. Sei $X \neq \emptyset$ endliches Alphabet, $H = X^*$ Monoid aller endlichen Wörter über X.
   Definiere $\sim$ auf H: $w_1 \sim w_2 \Leftrightarrow l(w_1) \equiv l(w_2) \mod 2$
   Wegen $l(w_1w_2) = l(w_1)+l(w_2)$ folgt sofort, dass $\sim$ Kongruenzrelation ist.
   $H/\sim = \{[\varepsilon], [x]\}$ für ein $x \in X$. $H/\sim$ hat dieselbe Verknüpfung wie $\mathbb{Z}/2\mathbb{Z}$.

2.8 Definition

Sei $X \neq \emptyset$ Alphabet, $H = X^*$. Sei $L \subseteq H$ (L=Language)
Definiere Relation auf H durch:

$$w_1, w_2 \in H: \; w_1 \equiv_L w_2 \quad \Leftrightarrow \quad \{(u,v) \in H \times H \mid uw_1v \in L\} = \{(u,v) \in H \times H \mid uw_2v \in L\}$$

$\equiv_L$ ist Kongruenzrelation auf H:
Äquivalenzrelation $\surd$
Kongruenzrelation: $w_1 \equiv_L w_2,\; w_1' \equiv_L w_2'$
Zeige: $w_1w_1' \equiv_L w_2w_2'$
Seien $u, v \in H$ mit $uw_1w_1'v \in L \overset{w_1 \equiv_L w_2}{\Longrightarrow} uw_2w_1'v \in L \overset{w_1' \equiv_L w_2'}{\Longrightarrow} uw_2w_2'v \in L$.
$\equiv_L$ heißt *syntaktische Kongruenz* bezüglich L auf $H = X^*$.
Faktormonoid: $H/\equiv_L$ *syntaktisches Monoid* bezüglich L: $M(L)$.
Beachte: L ist Vereinigung von Äquivalenzklassen unter $\equiv_L$
($w \in L, w \equiv_L w'$, so $\varepsilon w' \varepsilon \in L$)

2.9 Beispiele

1. $\emptyset \neq X$ endlich, $L = \{w \in X^* \mid l(w) \equiv 0 \mod 2\} \subseteq H = X^*$. Sind $u, v, w \in H$, so gilt: $uwv \in L \Leftrightarrow l(u) + l(v) \equiv l(w) \mod 2$,
   d.h. $w_1 \equiv_L w_2 \Leftrightarrow l(w_1) \equiv l(w_2) \mod 2$
   Also besitzt $\equiv_L$ genau 2 Äquivalenzklassen, nämlich $L = [\varepsilon]$ und $[x]$ für ein $x \in X$.
   $M(L) = H/\equiv_L$ ist also das gleiche Monoid wie das aus Beispiel 2.7 2.

2. Alphabet $X = \{a, b, c\}$; Sprache $L = a^*ba^*ca^* \subseteq X^*$ (Sprache die vom Automaten $\mathcal{A}$ aus 2.2 5. erkannt wird.)

   Wie sieht $M(L)$ aus?
   Wir untersuchen zunächst $[a]$. $\varepsilon \equiv_L a^n$ für jedes $n \in \mathbb{N}$, denn:

$$\begin{aligned} u\varepsilon v \in L \quad &\Leftrightarrow \quad u \in a^*,\; v \in a^*ba^*ca^* \text{ oder} \\ &\qquad\; u \in a^*ba^*,\; v \in a^*ca^* \text{ oder} \\ &\qquad\; u \in a^*ba^*ca^*,\; v \in a^* \\ &\Leftrightarrow \quad ua^nv \in L \end{aligned}$$

   Ist $\varepsilon \equiv_L w$ für ein $w \notin a^*$?

   Nein: Angenommen w enthält b oder c.
   Dann $\varepsilon wbc \notin L$, aber $\varepsilon\varepsilon bc \in L$.
   Also: $[\varepsilon] = a^* = [a^n]$ für jedes $n \in \mathbb{N}_0$

Jetzt Äquivalenzklasse von b

$$\begin{aligned} ubv \in L &\Leftrightarrow u \in a^*,\ v \in a^*ca^* \\ &\Leftrightarrow ua^nba^mv \in L \end{aligned}$$

Also: $b \equiv_L a^nba^m \ \ \forall n, m \in \mathbb{N}_0$
Ist $b \equiv_L w$ für ein $w \notin a^*ba^*$? - $a^nwa^mca^l \in L \Leftrightarrow w \in a^*ba^*$
Also: $[b] = a^*ba^*$
Äquivalenzklasse von c: $[c] = a^*ca^*$ analog
Äquivalenzklasse von bc: $[bc] = a^*ba^*ca^* = L$ analog

Sei jetzt $w \notin a^* \cup a^*ba^* \cup a^*ca^* \cup a^*ba^*ca^*$.
Dann $uwv \notin L$ für alle $u, v \in H = X^*$.
Also: alle übrigen w sind äquivalent,
$[cb] = X^* \setminus (a^* \cup a^*ba^* \cup a^*ca^* \cup a^*ba^*ca^*)$

$[\varepsilon] =: \overline{1}, [b] =: \overline{\alpha}, [c] =: \overline{\beta}, [bc] =: \overline{\gamma}, [cb] =: \overline{0}$

Verknüpfungstafel:

	$\overline{1}$	$\overline{\alpha}$	$\overline{\beta}$	$\overline{\gamma}$	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{\alpha}$	$\overline{\beta}$	$\overline{\gamma}$	$\overline{0}$
$\overline{\alpha}$	$\overline{\alpha}$	$\overline{0}$	$\overline{\gamma}$	$\overline{0}$	$\overline{0}$
$\overline{\beta}$	$\overline{\beta}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{\gamma}$	$\overline{\gamma}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$

Verknüpfungstafel wie $M(\mathcal{A})$, $\mathcal{A}$ erkannte Sprache L (2.2 5.) Das ist kein Zufall, wie wir gleich sehen werden.
Zunächst benötigen wir jedoch einen weiteren wesentlichen Begriff:

2.10 Definition

Seien H, K Halbgruppen.

1. Eine Abbildung $\varphi : H \to K$ heißt *(Halbgruppen-)Homomorphismus*, falls gilt
$$\varphi(h_1 \cdot h_2) = \varphi(h_1) \cdot \varphi(h_2) \quad \forall h_1, h_2 \in H.$$

2. Sind H, K Monoide, so heißt ein Halbgruppen-Homomorphismus $\varphi : H \to K$ *Monoid-Homomorphismus*, falls
$$\varphi(e_H) = e_K.$$

Ein bijektiver Homomorphismus heißt *Isomorphismus* ($H \cong K$)

2.11 Beispiele

1. $\mathbb{R}_+ = \{r \in \mathbb{R} \mid r > 0\}$ mit Multiplikation
   $\log : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ Monoid-Isomorphismus
   $\log(xy) = \log(x) + \log(y)$
2. Bsp 2.2 5: $f : X^* \to M(\mathcal{A}) : w \mapsto f_w$ surjektiver Monoid-Homomorphismus
   $f_{w_1} \cdot f_{w_2} = f_{w_1 w_2}$
3. $M(\mathcal{A})$ aus 2.2 5, $M(L)$ aus 2.9 2: $M(\mathcal{A}) \cong M(L)$

Zusammenhang: Kongruenzrelation - Homomorphismen

2.12 Satz

1. Seien H und K Halbgruppen, $\varphi : H \to K$ Homomorphismus.
   Definiere Relation $\sim_\varphi$ auf H durch:
   $h_1 \sim_\varphi h_2 \Leftrightarrow \varphi(h_1) = \varphi(h_2)$
   Dann ist $\sim_\varphi$ eine Kongruenzrelation auf H.
2. Ist H eine Halbgruppe, $\sim$ eine Kongruenzrelation auf H, so ist
   $\varphi : \begin{cases} H & \to & H/\sim \\ h & \mapsto & [h] \leftarrow \text{Äquivalenzklasse bzgl. } \sim \end{cases}$
   ein surjektiver Homomorphismus und $\sim_\varphi = \sim$.
   (φ heißt der *kanonische Homomorphismus* von H auf $H/\sim$.)

Beweis. 1. Klar: $\sim_\varphi$ ist Äquivalenzrelation.
Kongruenzrelation: $h_1 \sim_\varphi h_1', h_2 \sim_\varphi h_2'$
$\varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2) = \varphi(h_1')\varphi(h_2') = \varphi(h_1' h_2')$, d.h. $h_1 h_2 \sim_\varphi h_1' h_2'$.

2. $\varphi(h_1 h_2) = [h_1 h_2] = [h_1] \cdot [h_2] = \varphi(h_1)\varphi(h_2)$
   $h_1 \sim_\varphi h_1' \Leftrightarrow \varphi(h_1) = \varphi(h_1') \Leftrightarrow [h_1] = [h_1'] \Leftrightarrow h_1 \sim h_1'$

□

2.13 Homomorphiesatz

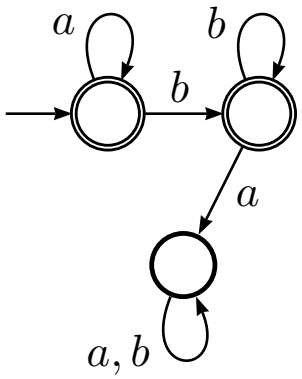
Seien H, K Halbgruppen, $\varphi : H \to K$ ein surjektiver Homomorphismus.
Dann ist $\widetilde{\varphi} : \begin{cases} H/\sim_\varphi & \to & K \\ [h] & \mapsto & \varphi(h) \end{cases}$
ein Isomorphismus, d.h. $K \cong H/\sim_\varphi$.
(Sind H, K Monoide, so ist $\widetilde{\varphi}$ ein Monoid-Isomorphismus)

Beweis. $\widetilde{\varphi}$ ist wohldefiniert und injektiv:
$[h_1] = [h_2] \Leftrightarrow h_1 \sim_\varphi h_2 \Leftrightarrow \varphi(h_1) = \varphi(h_2)$
$\widetilde{\varphi}$ ist surjektiv, da φ surjektiv.
$\widetilde{\varphi}([h_1] \cdot [h_2]) = \widetilde{\varphi}([h_1 h_2]) = \varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2) = \widetilde{\varphi}([h_1]) \cdot \widetilde{\varphi}([h_2])$ □

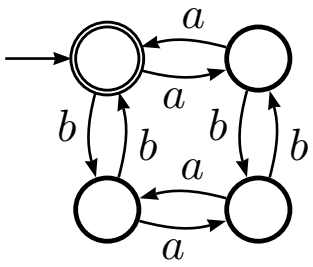
Anwendung von 2.13
$L \subseteq X^*$ heißt *reguläre Sprache*, falls es einen endlichen deterministischen Automaten $\mathcal{A}$ gibt, der L erkennt.

Beispiel:
Sei $X = \{a, b\}$.

1. $L = a^*b^*$ ist regulär



2. $L = \{w \in X^* : \#a\text{'s in } w \text{ gerade } \#b\text{'s in } w \text{ gerade}\}$ ist regulär



3. $L = \{a^n b^n : n \in \mathbb{N}_0\}$ ist nicht regulär
   (Pumping-Lemma:
   L regulär $\Rightarrow \exists n \in \mathbb{N} \, \forall z \in L, l(z) \geq n : z = uvw, |uv| \leq n, |v| \geq 1$ und $uv^i w \in L \; \forall i \in \mathbb{N}$. (Dabei $n \leq$ Anzahl der Zustände im kleinsten Automat, der L akzeptiert.))
   Nur mit Automaten nicht ganz so einfach zu sehen.
   Wir werden gleich sehen, dass wir es mit dem syntaktischen Monoid von L leicht einsehen können.

2.14 Satz

Sei $L \subseteq X^*$ eine reguläre Sprache über X. Sei $\mathcal{A} = (Z, \delta, z_0, E)$ ein endlicher deterministischer Automat, der L erkennt. Dann ist $M(L)$ isomorph zu einem Faktormonoid von $M(\mathcal{A})$.

Beweis. Für $w \in X^*$ sei $[w]$ die $\equiv_L$-Äquivalenz-Klasse von w, also $M(L) = \{[w] | w \in X^*\}$.

Definiere: $\varphi : \left\{ \begin{array}{lcl} M(\mathcal{A}) & \to & M(L) \\ f_w & \mapsto & [w] \end{array} \right.$
Zu zeigen: φ ist wohldefiniert
$f_{w_1} = f_{w_2} \Rightarrow f_{w_1}(z) = f_{w_2}(z) \; \forall z \in Z$, d.h. $(*)$ $zw_1 = zw_2 \; \forall z \in Z$

Zu zeigen: $w_1 \equiv_L w_2$.
Seien $u, v \in X^*$ mit $uw_1v \in L$, d.h. $z_0uw_1v \in E$
Dann: $z_0uw_2v = (\underbrace{(z_0u)}_{\text{Zustand}} w_2)v \overset{(*)}{=} ((z_0u)w_1)v = z_0uw_1v \in E$, also $uw_2v \in L$.

Umgekehrt analog. Also: $w_1 \equiv_L w_2$.
Wegen $\varphi(f_{w_1} \cdot f_{w_2}) = \varphi(f_{w_1w_2}) = [w_1w_2] = [w_1][w_2] = \varphi(f_{w_1})\varphi(f_{w_2})$,
$\varphi(f_\varepsilon) = [\varepsilon]$ ist φ ein Monoid-Homomorphismus und surjektiv.
Behauptung folgt mit 2.13 □

2.15 Satz von Myhill-Nerode

Sei $X \neq \emptyset$ endliches Alphabet, $L \subseteq X^*$. Dann gilt:

$$L \text{ ist regulär } \Leftrightarrow \ M(L) \text{ ist endlich.}$$

Beweis. $\Rightarrow$: Sei $\mathcal{A} = (Z, \delta, z_0, E)$ endlicher deterministischer Automat, der L erkennt.

Nach 2.14: $M(L)$ ist isomorph zu Faktormonoid von $M(\mathcal{A})$.
$M(\mathcal{A}) \subseteq Abb(Z, Z)$, $|Abb(Z, Z)| = |Z|^{|Z|} \Rightarrow M(\mathcal{A})$ endlich, also ist auch $M(L)$ endlich.

$\Leftarrow$: $M(L)$ endlich.
Konstruiere einen endlichen deterministischen Automat $\mathcal{A} = (Z, \delta, z_0, E)$, der L erkennt.

$Z := M(L),\ z_0 := [\varepsilon],\ E =$ Menge der $\underbrace{[w]}_{\equiv_L\text{-Äquivalenzklasse}}$, $w \in L$

Übergangsfunktion: $\delta([w], x) := [wx]$
Klar: $w \in X^*$ wird von $\mathcal{A}$ erkannt
$\Leftrightarrow z_0w \in E \Leftrightarrow [\varepsilon \cdot w] \in E \Leftrightarrow [w] = [w_0]$ für ein $w_0 \in L$
$\Leftrightarrow w \in L$

Also ist $\mathcal{A}$ endlicher deterministischer Automat, der L erkennt; L regulär. □

Beispiel:
$L = \{a^nb^n : n \in \mathbb{N}_0\}$ ist nicht regulär:
$w_i = ab^i, i \in \mathbb{N}$
$i \neq j$, so $a^{i-1}w_i\varepsilon \in L,\ a^{i-1}w_j\varepsilon \notin L \Rightarrow w_i \not\equiv_L w_j \Rightarrow M(L)$ unendlich $\overset{2.15}{\Rightarrow} L$ nicht regulär.

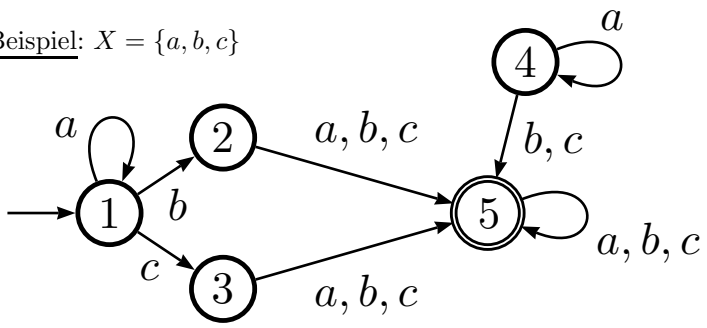
Wir haben gesehen:
L regulär, $\mathcal{A}$ erkennt $L \Rightarrow M(L) \cong M(\mathcal{A})/\sim$
Tatsächlich existiert ein Automat $\mathcal{A}$ mit $M(L) \cong M(\mathcal{A})$, nämlich der *minimale Automat*, der L erkennt:

Sei $\mathcal{B} = (Z, \delta, z_0, E)$ ein Automat, der L erkennt.

1.) Lasse alle Zustände weg, die nicht von der Form z_0w für ein $w \in X^*$ sind.

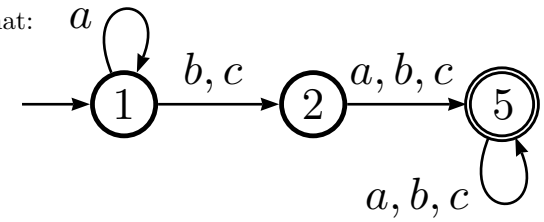
2.) Identifiziere Zustände z_1, z_2 genau dann, wenn $\forall w \in X^* : z_1 w \in E \Leftrightarrow z_2 w \in E$.

Beispiel: $X = \{a, b, c\}$



Dieser Automat erkennt $a^*bX^+ \cup a^*cX^+ \quad (X^+ = aX^* \cup bX^* \cup cX^*)$

Zugehöriger minimaler Automat:



2.16 Satz

Sei L eine reguläre Sprache, $\mathcal{A}$ ein minimaler Automat der L erkennt.
Dann ist $M(\mathcal{A}) \cong M(L)$.
($M(\mathcal{A})$ häufig leicher zu bestimmen als $M(L)$)

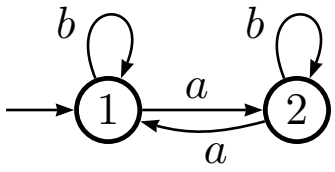
Beweis. Wir zeigen, dass die Abbildung $\varphi : M(\mathcal{A}) \to M(L) : f_w \mapsto [w]$ aus dem Beweis von 2.14 injektiv ist.
$[w_1] = [w_2] \quad \equiv_L$-Äquivalenzklasse
Sei $z \in Z$. Dann gilt (da $\mathcal{A}$ minimal): $\exists u \in X^*$ mit $z = z_0 u$

Sei $z_1 = f_{w_1}(z) = z_0 u w_1$
$\quad z_2 = f_{w_2}(z) = z_0 u w_2$.

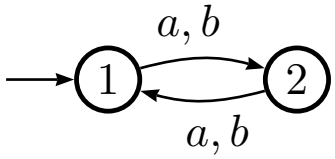
Es ist $uw_1 v \in L \Leftrightarrow uw_2 v \in L$.
Also: $z_1 v \in E \Leftrightarrow z_2 v \in E$
Wegen der Minimalität von $\mathcal{A}$ folgt: $z_1 = z_2$, d.h. $f_{w_1}(z) = f_{w_2}(z)$.
$z \in Z$ war beliebig, daher gilt $f_{w_1} = f_{w_2}$. □

Aufgabe:
$X = \{a, b\}$ Für welche L ist $M(L) \cong (\mathbb{Z}_2, \oplus)$?

Antwort:



Endzustandswahl liefert:
$L_1 = \{w \mid \#a\text{'s gerade}\}$
$L_2 = \{w \mid \#a\text{'s ungerade}\}$
(oder mit b, wenn man Rollen von a und b vertauscht)



Endzustandswahl liefert:
$L_3 = \{w \mid l(w) \text{ gerade}\}$
$L_4 = \{w \mid l(w) \text{ ungerade}\}$

2.17 Bemerkung

Zusammenhang: Familie von regulären Sprachen $\leftrightarrow$ Familie von endlichen Monoiden
Wichtig dabei: Zusammenhang zur Prädikatenlogik erster Stufe

Wir geben (ohne Beweis) ein Beispiel:
Wir betrachten Formeln der Prädikatenlogik erster Stufe:

1. $\exists i \exists j\ (i < j)$
   i, j bezeichnen Positionen in einem Wort über dem Alphabet X. Damit beschreibt die Formel gerade die Sprache $L = \{w \in X^* \mid l(w) \geq 2\}$

2. $\exists i \exists j\ (\forall k\ (k \geq i) \wedge Q_x i \wedge \forall k\ (k \leq j) \wedge Q_y j)$
   i, j, k bezeichen wieder Positionen in einem Wort.
   Das Prädikat $Q_x i$ soll bedeuten: "an der Stelle i steht der Buchstabe x".
   Dann ist die durch diese Formel beschriebene Sprache genau xX^*y.

Bei einer Formel der Prädikenlogik erster Stufe beziehen sich Quantoren nur auf einzelne Variablen (d.h. einzelne Positionen) und nicht auf Teilmengen von Variablen.
Mit $FO[<]$ bezeichnen wir die Menge aller Sprachen über einem Alphabet X, die durch eine Formel der Prädikatenlogik erster Stufe (wie oben) beschrieben werden, wobei nur die Symbole Q_x und als Relation auf den Positionen der Worte nur $<$ verwendet werden.
(Alle auftretenden Variablen (= Positionen) sind quantifiziert.)
Welche Sprachen liegen in $FO[<]$?
Eine Antwort gibt der Satz von McNaughton und Papert (1971), der diese Sprachen L durch eine Eigenschaft von $M(L)$ charakterisiert.

Dazu: Ein Monoid M heißt *aperiodisch*, falls ein $k > 0$ existiert, so dass

$$m^k = m^{k+1} \text{ für alle } m \in M.$$

(Man kann zeigen: M aperiodisch $\Leftrightarrow$ es existiert keine Teilmenge $N, |N| > 1$, so dass N eine Gruppe ist (bzgl. $\cdot$)).

Satz (McNaughton, Papert)

$$L \in FO[<] \;\Leftrightarrow\; M(L) \text{ ist endlich und aperiodisch}$$

Die beiden Sprachen oben liegen in $FO[<]$.
Aber: $L = \{w \mid w \in X^*, l(w) \equiv 0 \mod 2\} \notin FO[<]$, denn $M(L) \cong \mathbb{Z}/2\mathbb{Z}$ (2.9 1) ist nicht aperiodisch: $k \cdot 1 = \begin{cases} 0 & \text{falls } k \text{ gerade} \\ 1 & \text{falls } k \text{ ungerade} \end{cases}$

Literatur:

Straubing: Finite Automata, Formal Logic and Circuit Complexity. Birkhäuser 1994.
Howie: Automata and Languages. Clarendon Press. 1999.

3 Gruppen

3.1 Definition

1. Ein Monoid $(G, \cdot)$ heißt *Gruppe*, falls zu jedem Element $g \in G$ ein (von g abhängendes) Element $h \in G$ existiert mit $h \cdot g = g \cdot h = 1$. (1 neutrales Element)

2. Eine Gruppe G heißt *abelsch* oder *kommutativ*, falls $g \cdot h = h \cdot g$ für alle $g, h \in G$.

3. Ist G endlich, so heißt die Anzahl der Elemente von G die *Ordnung* von G.
   Bezeichnung: $|G|$

3.2 Bemerkung

1. Zu $g \in G$ gibt es *genau ein* Element $h \in G$ mit $gh = hg = 1$.
   (Gäbe es zwei, $h, h' :\ h = 1 \cdot h = (h'g)h = h'(gh) = h' \cdot 1 = h'$.)
   Dieses eindeutig bestimmte Element heißt *Inverses* zu g.
   Bezeichnung: g^{-1}
   Klar: $1^{-1} = 1$.

2. In Gruppen kann man Gleichungen der Form $a = bx$ bzw. $a = xb$ eindeutig lösen: $x = b^{-1}a$ bzw. $x = ab^{-1}$

3. Wird die Gruppe additiv geschreiben, so $-h$ statt h^{-1}.
   (Neutrales Element 0)

3.3 Beispiele

1. $(\mathbb{Z}, +)$ ist Gruppe, $(\mathbb{Z}, \cdot)$ ist keine Gruppe

2. $(\mathbb{Q}, +)$ ist Gruppe, $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist Gruppe

3. $n \in \mathbb{N}, \mathbb{Z}_n = \{0, 1, \ldots, n-1\}, a \oplus b := (a + b) \bmod n$ abelsche Gruppe

4. X^* keine Gruppe; $M(L), M(\mathcal{A})$ sind im Allgemeinen keine Gruppen

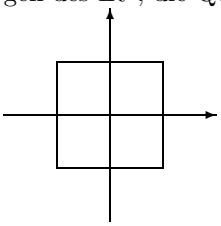
5. X Menge, $\mathrm{Bij}(X)$ = Menge aller bijektiven Abbildungen $X \to X$ ist eine Gruppe bzgl. der Hintereinanderausführung als Verknüpfung.
   X endlich: $\mathrm{Sym}(X)$ *Symmetrische Gruppe* auf X.
   $X = \{1, \ldots, n\}$. $S_n = \mathrm{Sym}(X)$ Permutationen auf $\{1, \ldots, n\}$. $|S_n| = n!$
   S_n abelsch $\Leftrightarrow n \leq 2$.
   Schreibweise für Elemente aus S_n: $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$

   Bsp: S_3 $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

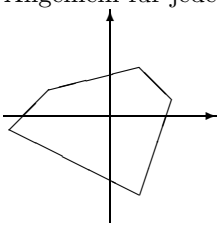
6. V Vektorraum, $GL(V)$ = Menge der invertierbaren linearen Abbildungen $V \to V$ ist Gruppe bzgl. der Hintereinanderausführung.

7. $\mathbb{R}^n$ mit Skalarprodukt $(a,b) = \sum a_i b_i$.
   $O(R^n)$ = Menge der invertierbaren linearen Abbildungen $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ mit $(\varphi(a), \varphi(b)) = (a,b) \quad \forall\ a,b \in \mathbb{R}^n$ ist Gruppe bzgl. Hintereinanderausführung (orthogonale Gruppe).

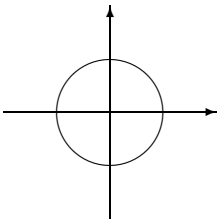
8. Symmetriegruppe eines Quadrates = Menge der orthogonalen Abbildungen des $\mathbb{R}^2$, die Quadrat in sich überführen.



4 Drehungen, 4 Spiegelungen
Allgemein für jede Figur:



Symmetriegruppe: {id}



$O(\mathbb{R}^2)$
(Gruppe dient als Maß für die Symmetrie.)

3.4 Bemerkung

Sei G Gruppe.

1. $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

2. $g \in G$. Definition: $g^0 := 1,\ g^n := g^{n-1} g\ (n \in \mathbb{N})$
   $g^n := (g^{-1})^{-n} = (g^{-n})^{-1},\ n \in \mathbb{Z} \setminus \mathbb{N}_0$

   Dann gilt: $g^a g^b = g^{a+b}, (g^a)^b = g^{a \cdot b}$
   Im Allgemeinen: $(gh)^a \neq g^a h^a$ (Gleichheit gilt, falls $gh = hg$)

3.5 Definition

Sei G eine Gruppe, H eine nichtleere Teilmenge von G.
H heißt *Untergruppe* von G, falls H bezüglich der Verknüpfung auf G selbst Gruppe ist.
Schreibweise: $H \leq G$
(Dann $1_H = 1_G$, denn in Gruppen gilt: $x^2 = x \Rightarrow x = x^{-1} \cdot x^2 = x^{-1} \cdot x = 1_G$)

3.6 Bemerkung

Sei $\emptyset \neq H \leq G$, G Gruppe.

1. $H \leq G \Leftrightarrow$ (1) H ist Unterhalbgruppe, d.h. $\forall\, h_1, h_2 \in H : h_1 \cdot h_2 \in H$.
   (2) $\forall\, h \in H : h^{-1} \in H$

2. Ist H endlich, so gilt:
   $H \leq G \Leftrightarrow H$ ist Unterhalbgruppe von G

Beweis. 1. $\surd$

2. $\Leftarrow$: Zeige: Ist $h \in H$, so auch $h^{-1} \in H$.
   $\{h^i | i \in \mathbb{N}\} \subseteq H$
   Da H endlich ist, existieren $i < j,\ i, j \in \mathbb{N}$ mit $h^i = h^j$.
   $1 = h^j (h^i)^{-1} \overset{3.4,2}{=} h^{j-i} = h^{j-i-1} \cdot h$
   Daraus folgt: $h^{j-i-1} = h^{-1}$ $(*)$. Da $j > i$, ist $h^{j-i-1} \in H$ und wegen $(*)$ auch $h^{-1} \in H$

□

3.7 Beispiel

Wie sehen die Untergruppen von $(\mathbb{Z}, +)$ aus?
$n \in \mathbb{N}_0 :\ n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ alle Vielfachen von n.
$n\mathbb{Z} \leq \mathbb{Z}$. $(n = 0 :\ n\mathbb{Z} = \{0\};\ \ n = 1 :\ n\mathbb{Z} = \mathbb{Z})$
Dies sind sämtliche Untegruppen:
$H \leq \mathbb{Z}$. $H = \{0\}$, so $H = 0 \cdot \mathbb{Z}\surd$
$H \neq 0, k \in H$, so $-k \in H$. Also $H \cap \mathbb{N} \neq \emptyset$.
Sei n die kleinste natürliche Zahl, die in H liegt. Dann $n\mathbb{Z} \subseteq H$.
Zeige: $n\mathbb{Z} = H$:
$h \in H$. $h = k \cdot n + r,\ 0 \leq r \leq n - 1$ (Division mit Rest)
$r = h + (-k)n \in H$. Mit der Minimalität von n folgt: $r = 0$. Also $h \in n\mathbb{Z}$.

3.8 Definition

Sei $H \leq G, g \in G$.
Dann heißt gH *Linksnebenklasse* und Hg *Rechtsnebenklasse* von H in G, wobei

$$gH = \{gh : h \in H\} \quad Hg = \{hg : h \in H\}.$$

(Beachte: Wird G additiv geschrieben, so

$$g + H = \{g + h : h \in H\} \quad H + g = \{h + g : h \in H\}$$

Links-/ Rechtsnebenklassen.
Also in $\mathbb{Z}$ sind die $n\mathbb{Z}$ keine Nebenklassen bzgl. +!)
Beachte: $H = 1 \cdot H = H \cdot 1$ ist selbst Links- bzw. Rechtsnebenklasse von sich selbst.
Ist G abelsch, so ist $Hg = gH$.

3.9 Satz

Sei $H \leq G$.

1. $G = \bigcup_{g \in G} Hg = \bigcup_{g \in G} gH$.
2. Sind $g_1, g_2 \in G$, so ist $Hg_1 = Hg_2$ oder $Hg_1 \cap Hg_2 = \emptyset$.
   (Analog für Linksnebenklassen)
3. $Hg_1 = Hg_2 \Leftrightarrow g_1 g_2^{-1} \in H$
   (Insbesondere: $H = Hg \Leftrightarrow g \in H$)
   $g_1 H = g_2 H \Leftrightarrow g_1^{-1} g_2 \in H$

Beweis. 1. $g \in G$, so $g = 1 \cdot g \in Hg,\ g = g \cdot 1 \in gH \quad \Rightarrow$ Beh.

2. Sei $Hg_1 \cap Hg_2 \neq \emptyset$. Dann existieren $h_1, h_2 \in H$ mit $h_1 g_1 = h_2 g_2$. Ist $h \in H$, so $hg_1 = hh_1^{-1} h_1 g_1 = hh_1^{-1} h_2 g_2 \in Hg_2$, d.h. $Hg_1 \subseteq Hg_2$.
   Analog $Hg_2 \subseteq Hg_1$.
   Also $Hg_1 = Hg_2$.

3. $\Rightarrow$: $\quad Hg_1 = Hg_2 \ \Rightarrow\ 1 \cdot g_1 = hg_2$ für ein $h \in H \ \Rightarrow\ g_1 g_2^{-1} = h \in H$.
   $\Leftarrow$: $\quad g_1 g_2^{-1} = h \in H \ \Rightarrow\ 1 \cdot g_1 = hg_2 \in Hg_1 \cap Hg_2 \neq \emptyset \overset{2.}{\Rightarrow}\ Hg_1 = Hg_2$.

□

3.10 Bemerkung

Die verschiedenen Rechts- (bzw. Linksnebenklassen) von H in G bilden also eine Partition von G.
Die Rechtsnebenklassen von H in G sind also die Äquivalenzklassen zur Äquivalenzrelation:

$g_1 \sim_r g_2 \Leftrightarrow g_1, g_2$ liegen in derselben Rechtsnebenklasse Hg
$\Leftrightarrow Hg_1 = Hg_2 (= Hg) \overset{3.9.3}{\Leftrightarrow} g_1 g_2^{-1} \in H$

Analog sind die Linksnebenklassen von H in G die Äquivalenzklassen zur Relation $g_1 \sim_l g_2 \Leftrightarrow g_1^{-1} g_2 \in H$.

3.11 Beispiel

$n\mathbb{Z} \leq \mathbb{Z}$ bzgl. $+$.
Linksebenklassen = Rechtsnebenklassen $= k + n\mathbb{Z},\ \ k \in \mathbb{Z}$.

$k_1 + n\mathbb{Z} = k_2 + n\mathbb{Z} \Leftrightarrow k_1 - k_2 \in n\mathbb{Z} \ \Leftrightarrow\ n | (k_1 - k_2)$
$\Leftrightarrow k_1 \equiv k_2 \bmod n$.

Die Nebenklassen von $n\mathbb{Z}$ in $\mathbb{Z}$ sind genau die Kongruenzklassen mod n.

3.12 Satz

Sei $H \leq G,\ g_1, g_2 \in G$.
Dann ist $\varphi : Hg_1 \to Hg_2 : hg_1 \mapsto hg_2$ eine Bijektion.
Insbesondere gilt: Ist H endlich, so ist $|H| = |Hg|$ für alle $g \in G$.
Analog für Linksnebenklassen.

Beweis. $hg_1 = h'g_1 \Rightarrow h = h' \Rightarrow hg_2 = h'g_2$. Also ist φ wohldefiniert.
Es ist klar, dass φ surjektiv.
φ injektiv: $hg_2 = h'g_2 \Rightarrow h = h' \Rightarrow hg_1 = h'g_1$. □

3.13 Korollar

Sei G eine endliche Gruppe, $H \leq G$

1. Anzahl der Linksnebenklassen von H in G = Anzahl der Rechtsnebenklassen von H in G, *Index* von H in $G = |G : H|$.

2. Satz von LAGRANGE
   $|G| = |H| \cdot |G : H|$. Insbesondere: $|H|$ teilt $|G|$.

Beweis.

$H = H1$	Hg_2	Hg_3	$\cdots$	Hg_m	G

$|Hg_i| = |H|$
$|G| = m \cdot |H|$

$H = 1H$	$g_2'H$	$g_3'H$	$\cdots$	$g_m'H$	G

Analog: $|H| = |g_i'H|, |G| = l \cdot |H|$

$m = l$.

□

3.14 Beispiel

$G = S_3,\ |G| = 3! = 6$
$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, (13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$
$(23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, (132) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Wir verwenden hier die Zyklenschreibweise von Permutationen. Näheres hierzu in 5.1.

Welches sind die Untergruppen von G?
$H = \{id\}, H = G$.
Jede andere Untergruppe hat nach 3.13 Ordnung 2 oder 3.

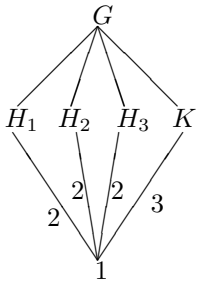
Ordnung 2: $\{id, (12)\}, \{id, (13)\}, \{id, (23)\}$ 3 Untergruppen der Ordnung 2.
Ordnung 3: $\{\text{id}, (123, (132)\} =: K$

Sei $H = \{id, (12)\}$.

Linksnebenklassen: $id \cdot H = (12) \cdot H = H$
$(13)H = (123)H = \{(13), (123)\}$
$(23)H = (132)H = \{(23), (132)\}$

Rechtsnebenklassen: $H \cdot id = H \cdot (12) = H$
$H \cdot (13) = H(132) = \{(13), (132)\}$
$H \cdot (23) = H(123) = \{(23), (123)\}$

Beachte: $H(13)$ ist keine Linksnebenklasse.



Bemerkung:
Wie sieht es mit den Faktorgruppen einer Gruppe aus?
Man kann zeigen:
Die einzigen Partitionen einer Gruppe G, die zu Kongruenzrelationen gehören, sind die Linksnebenklassen nach gewissen Untergruppen, den Normalteilern.

Wir zeigen nun, dass Linksnebenklassen zu Normalteilern die Äquivalenzklassen einer Kongruenzrelation sind.

3.15 Definition

$N \leq G$ heißt *Normalteiler*, falls $gN = Ng$ für alle $g \in G$.
Schreibweise: $N \trianglelefteq G$.
Äquivalent hierzu ist: $gNg^{-1} = \{gng^{-1} : n \in \mathbb{N}\} = N$ für alle $g \in G$.

3.16 Beispiele

1. In abelschen Gruppen sind alle Untergruppen Normalteiler.

2. $\{1\}$ und G sind stets Normalteiler (die trivialen Normalteiler).

3. In S_3 ist K mit $|K| = 3$ Normalteiler, die Untergruppen der Ordnung 2 sind keine Normalteiler.

3.17 Satz

Sei $N \trianglelefteq G$.

1. Die zu den (Rechts = Links-) Nebenklassen von N in G gehörende Äquivalenzrelation

$$g_1 \sim_N g_2 \quad \Leftrightarrow \quad g_1 N = g_2 N \quad \Leftrightarrow \quad g_1^{-1} g_2 \in N$$

ist eine Kongruenzrelation.

2. Die Menge der Nebenklassen $\{gN : g \in G\}$ wird durch
$$(g_1N) \cdot (g_2N) := g_1g_2N$$
eine Gruppe, die *Faktorgruppe* G/N von G nach N.

3. Ist G endlich, so $|G/N| = \frac{|G|}{|N|}$.

Beweis. 1. $g_1 \sim_N g_2,\ g_1' \sim_N g_2',\ g_1^{-1}g_2 \in N,\ g_1'^{-1}g_2' \in N$
Dann: $(g_1g_1')^{-1}(g_2g_2') = g_1'^{-1}g_1^{-1}g_2g_2' = \underbrace{g_1'^{-1}g_2'}_{\in N}\underbrace{g_2'^{-1}\underbrace{g_1^{-1}g_2}_{\in N}g_2'}_{\in N} \in N$

2. $G/N = G/\sim_N$ ist Monoid nach 1. und 2.6.1.
$(gN)^{-1} = g^{-1}N$.

3. Folgt aus dem Satz von Lagrange.

□

3.18 Beispiele

1. $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} \cong (\mathbb{Z}_n, \oplus)$ vgl. Bsp 2.7.1

2. $S_3/K,\ K = \{id, (123), (132)\}$
$S_3/K \cong \mathbb{Z}_2 (\cong \mathbb{Z}/2\mathbb{Z})$

3.19 Definition und Bemerkung

1. $\varphi : G \to H$ heißt Gruppenhomomorphismus, falls
$$\varphi(g_1g_2) = \varphi(g_1) \cdot \varphi(g_2)\ \ \forall g_1, g_2 \in G$$
Es gilt dann: $\varphi(1_G) = 1_H,\ \varphi(g^{-1}) = \varphi(g)^{-1}\ \forall g \in G$.

2. Bild $\varphi \leq H$

3. Kern $\varphi = \{g \in G : \varphi(g) = 1_H\} \trianglelefteq G$

4. φ injektiv $\Leftrightarrow$ Kern $\varphi = \{1_G\}$

3.20 Homomorphiesatz

Sei $\varphi : G \to H$ ein Homomorphismus.
Dann ist $\widetilde{\varphi} : G/\text{Kern}\varphi \ \to\ H : g\ \text{Kern}\varphi \mapsto \varphi(g)$ injektiv.
Also $G/\text{Kern}\varphi \cong \text{Bild}\varphi$

Beweis. Folgt aus 2.13 □

3.21 Beispiel

$\det : \begin{cases} GL(n, \mathbb{R}) \to \mathbb{R} \setminus \{0\} & \leftarrow \text{ Gruppe bzgl. Multiplikation} \\ A \mapsto \det(A) \end{cases}$ ist Homomorphismus.
Kern $\det = \{A \in GL(n, \mathbb{R}) : \det A = 1\} = SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$.
$GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R} \setminus \{0\}$.

3.22 Defnition

Sei G eine Gruppe.

1. Eine Teilmenge $\{x_1, \ldots, x_n\}$ von G heißt *Erzeugendensystem* von G, falls sich jedes $g \in G$ schreiben lässt in der Form

$$g = \underbrace{x_{i_1}}_{\varepsilon_1} \ldots \underbrace{x_{i_m}}_{\varepsilon_m},\ m \in \mathbb{N},\ i_j \in \{1, \ldots, n\},\ \varepsilon_j \in \{1, -1\}$$

   (Darstellung in der Regel nicht eindeutig)
   Schreibweise: $G = \langle x_1, \ldots, x_n \rangle$. (vgl. Basis von VR)

2. Eine Gruppe G heißt *zyklisch*, falls ein $x \in G$ existiert mit $G = \langle x \rangle$. Also: $G = \{x^i : i \in \mathbb{Z}\}$. Insbesondere: G ist abelsch.

3.23 Beispiele

1. $(\mathbb{Z}, +)$ und alle $(\mathbb{Z}/n\mathbb{Z}, +)$ sind zyklisch.

2. $\mathbb{Z}/6\mathbb{Z} = \langle 1 + 6\mathbb{Z} \rangle = \langle 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z} \rangle$.
   Beide Erzeugendensysteme sind nicht verkleinerbar! Unterschied zu Vektorräumen.

3. $S_3 = \langle (12), (123) \rangle$
   $\mathrm{id} = (12)(12),\ (23) = (12)(123),\ (13) = (123)(12),\ (132) = (123)(123)$
   Allgemein: $S_n = \langle (12), (1, 2, \ldots, n) \rangle$ für $n \geq 2$.
   ($(1, \ldots, n)$ steht für die Permutation $\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$.)

   Es gilt auch: $S_3 = \langle (12), (13) \rangle$;
   $(13)(12) = (123)$, also $\langle (12), (13) \rangle = \langle (12), (123), (1, 3) \rangle = S_3$.
   Allgemein: $S_n = \langle (12), (13), \ldots, (1n) \rangle$ für $n \geq 2$.

3.24 Satz

Sei $G = \langle x \rangle$ eine zyklische Gruppe.

1. Ist G unendlich, so ist $G \cong (\mathbb{Z}, +)$ $(x^i \to i)$ und alle x^i sind paarweise verschieden.

2. Ist G endlich, so existiert ein kleinstes $n \in \mathbb{N}$ mit $x^n = 1$. Dann ist $|G| = n$, $G = \{1, x, \ldots, x^{n-1}\}$ und $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

Beweis. $\varphi : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \to & (G, \cdot) \\ i & \mapsto & x^i \end{array} \right.$ ist ein surjektiver Homomorphismus.
Nach 3.20 gilt: $\mathbb{Z}/\mathrm{Kern}\varphi \cong G$
Nach 3.7 ist $\mathrm{Kern}\varphi = n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$.
$n = 0$: $\mathrm{Kern}\varphi = \{0\}$, $\mathbb{Z} \cong G$, alle x^i paarweise verschieden.
$n > 0$: $G \cong \mathbb{Z}/n\mathbb{Z}$ endlich, $G = \{1, \underbrace{x, \ldots, x^{n-1}}_{\text{paarw. versch.}}\}$, $x^n = 1$, da $n \in \mathrm{Kern}\varphi$

□

3.25 Korollar

Ist $|G| = p$, p eine Primzahl, so ist $G \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis. $1 \neq x \in G$. $\langle x \rangle \leq G$. Nach dem Satz von Lagrange gilt: $|\langle x \rangle|$ teilt $|G| = p$, also ist $|\langle x \rangle| = p$ und $G = \langle x \rangle$. Dann folgt die Behauptung mit 3.24.2. □

3.26 Satz

Untergruppen und Faktorgruppen zyklischer Gruppen sind zyklisch.

Beweis. Faktorgruppen klar.
Untergruppen beweist man wie bei $\mathbb{Z}$ ($n\mathbb{Z} = \langle n \rangle$) in 3.7. □

3.27 Definition

Sei G eine Gruppe, $x \in G$. Existiert kein $n \in \mathbb{N}$ mit $x^n = 1$, so hat x *unendliche Ordnung*. Im anderen Fall heißt das kleinste $n \in \mathbb{N}$ mit $x^n = 1$ die *Ordnung* von x, $o(x)$.

Nach 3.24: x von unendlicher Ordnung $\Rightarrow \langle x \rangle \cong \mathbb{Z}$
x von endlicher Ordnung $\Rightarrow o(x) = |\langle x \rangle|$.

Also: Ist G endlich, so $o(x) \mid |G|$.

3.28 Bemerkung

Sei $x \in G$.
Hat x endliche Ordnung und gilt $x^k = 1$, so gilt: $o(x) \mid k$.

Beweis. Sei $o(x) = n$, $k = qn + r$, $0 \leq r < n$.
$x^r = x^{k-qn} = x^k (x^n)^{-q} = 1 \Rightarrow r = 0$. □

3.29 Satz

Sei $G = \langle x \rangle$ eine zyklische Gruppe der Ordnung n.
Ist $k \in \mathbb{Z}$, so ist $|\langle x^k \rangle| = \frac{n}{d}$, wobei $d = \mathrm{ggT}(k, n)$ ($k = 0 : \ d = n$).
Insbesondere: $\langle x^k \rangle = \langle x \rangle \Leftrightarrow \mathrm{ggT}(k, n) = 1$ (d.h. $\langle x \rangle$ hat genau $\varphi(n)$ viele erzeugende Elemente)

Beweis. $(x^k)^{\frac{n}{d}} = (x^n)^{\frac{k}{d}} = 1 \overset{3.24.2}{\Longrightarrow} |\langle x^k \rangle| \leq \frac{n}{d}$.
Ist $(x^k)^m = 1$ für ein $m \in \mathbb{N}$, so $x^{km} = 1$. Nach 3.28: $n \mid km \ \Rightarrow \ \frac{n}{d} \mid \frac{k}{d} \cdot m \ \Rightarrow$ $\frac{n}{d} \mid m$, da $\mathrm{ggT}(\frac{n}{d}, \frac{k}{d}) = 1$. Also: $\frac{n}{d} \leq m$. Daher $|\langle x^k \rangle| = \frac{n}{d}$ □

3.30 Korollar

Ist $G = \langle x \rangle$ eine zyklische Gruppe der Ordnung n, so enthält G zu jedem Teiler m von n genau eine Untergruppe der Ordnung m, nämlich $\langle x^{\frac{n}{m}} \rangle$.

Beweis. $|\langle x^{\frac{n}{m}} \rangle| \overset{3.29}{=} \frac{n}{\mathrm{ggT}(\frac{n}{m}, n)} = \frac{n}{\frac{n}{m}} = m.$
Sei H eine Untergruppe der Ordnung m. $H = \langle x^k \rangle$ nach 3.26.
Nach 3.29 gilt: $m = \frac{n}{\mathrm{ggT}(k,n)}$, d.h. $\mathrm{ggT}(k, n) = \frac{n}{m}$.
Erweiterter Euklidischer Algorithmus: $\exists s, t \in \mathbb{Z} : ks + nt = \frac{n}{m}$.
$x^{\frac{n}{m}} = x^{ks+nt} = (x^k)^s (x^n)^t = (x^k)^s \in \langle x^k \rangle$. Also: $\langle x^{\frac{n}{m}} \rangle \leq \langle x^k \rangle$. Da beide die gleiche Ordnung haben, gilt also $\langle x^k \rangle = \langle x^{\frac{n}{m}} \rangle$ □

3.31 Exkurs

Im Beweis von 3.30 wurde verwendet: $a, b \in \mathbb{Z} \setminus \{0\}$, so ex. $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = sa + tb$. Solche s, t lassen sich mit Hilfe des Erweiterten Euklidischen Algorithmus' berechnen.
Bevor wir diesen angeben, beweisen wir kurz die Existenz von s, t:
$a\mathbb{Z} + b\mathbb{Z} \leq \mathbb{Z}$, d.h. $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ nach 3.7.
O.B.d.A. $d > 0$.
$d = sa + tb$.
$a\mathbb{Z} \subseteq d\mathbb{Z},\ b\mathbb{Z} \subseteq d\mathbb{Z} \Rightarrow\ d \mid a,\ d \mid b$. Also: $d \leq \mathrm{ggT}(a, b)$
Andererseits: $\mathrm{ggT}(a, b) \mid d$.
Also: $d = \mathrm{ggT}(a, b)$.

Der erweiterte Euklidische Algorithmus beruht auf folgenden Überlegungen:
Ist $\mathrm{ggT}(a, b) = sa + tb$, so ist $\mathrm{ggT}(-a, b) = (-s)(-a) + tb$ und $\mathrm{ggT}(a, -b) = sa + (-t)(-b)$. Daher genügt es, den Algorithmus für $a, b \geq 0$ anzugeben. Wegen $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$ und $\mathrm{ggT}(a, 0) = 1 \cdot a + 0 \cdot 0$ kann man außerdem $a \geq b > 0$ annehmen.
Wir setzen $a_0 = a$ und $a_1 = b$. Beim normalen Euklidischen Algorithmus wird nun durch wiederholte Division mit Rest auf folgende Weise der ggT von $a_0 = a$ und $a_1 = b$ bestimmt:

$$a_0 = q_1 a_1 + a_2, \ldots, a_{n-2} = q_{n-1} a_{n-1} + a_n, a_{n-1} = q_n a_n + 0.$$

Dann ist $a_n = \mathrm{ggT}(a_0, a_1)$.
Wir zeigen nun durch Induktion die Existenz von $u_j, v_j \in \mathbb{Z}$ mit $a_j = u_j a_0 + v_j a_1$ für $j = 0, \ldots, n$.
Sei $u_0 = 1, v_0 = 0$ und sei $u_1 = 0, v_1 = 1$. Dann gilt die Behauptung für $j = 0, 1$.
Sei nun $j \geq 2$ und es gelte $a_{j-2} = u_{j-2} a_0 + v_{j-2} a_1$ sowie $a_{j-1} = u_{j-1} a_0 + v_{j-1} a_1$.
Dann ist

$$a_j = a_{j-2} - q_{j-1} a_{j-1} = (u_{j-2} - q_{j-1} u_{j-1}) a_0 + (v_{j-2} - q_{j-1} v_{j-1}) a_1,$$

also der Induktionsschluss für j. Wegen $a_n = \mathrm{ggT}(a_0, a_1)$ folgt nun die Behauptung mit $s = u_n, t = v_n$.

Hieraus ergibt sich nun unmittelbar die Gültigkeit des folgenden *erweiterten Euklidischen Algorithmus*, den wir nur für den Fall $a, b > 0$ formulieren. Der

allgemeine Fall ist, wie oben erwähnt, leicht darauf zurückzuführen. Dabei verwenden wir folgende Bezeichnungen:
Sind x und y ganze Zahlen, $y \neq 0$, $x = qy + r, 0 \leq r < |y|$ (Division mit Rest), so ist $q = x \text{ div } y$ und $r = x \bmod y$.

Eingabe: Natürliche Zahlen a, b, $a > b$.

(1) Setze $x := a, y := b, s_1 := 1, s_2 := 0, s := 0, t_1 := 0, t_2 := 1, t := 1$.

(2) Solange $x \bmod y \neq 0$, wiederhole:
$g := x \text{ div } y, r := x \bmod y$;
$s := s_1 - gs_2, t := t_1 - gt_2$;
$s_1 := s_2, s_2 := s, t_1 := t_2, t_2 := t$;
$x := y, y := r$.

Ausgabe: $y \quad (= \text{ggT}(a, b)), \quad s, t \quad (y = sa + tb)$.

3.32 Korollar

Sei $n \in \mathbb{N}, n \geq 2$. Betrachte Monoid $(\mathbb{Z}_n, \odot)$.
$k \in \mathbb{Z}_n$ ist bezüglich der Multiplikation in $\mathbb{Z}_n$ invertierbar (d.h. $\exists\ l \in \mathbb{Z}_n$ mit $k \odot l = 1$, also $k \cdot l \equiv 1 \bmod n$) genau dann, wenn $\text{ggT}(k, n) = 1$.
(Bezeichung: $l =: k^{-1}$ in $\mathbb{Z}_n$)

Beweis. Angenommen $d = \text{ggT}(k, n) > 1$. Dann $k \odot \frac{n}{d} = \frac{k}{d} \odot n = 0$ in $\mathbb{Z}_n$. Angenommen es existiert ein $l \in \mathbb{Z}_n$ mit $k \odot l = 1$. Dann $0 = 0 \odot l = l \odot k \odot \frac{n}{d} = \frac{n}{d}$ in $\mathbb{Z}_n$. Widerspruch.

Sei $\text{ggT}(k, n) = 1$. Dann existieren nach dem Erweiterten Euklidischen Algorithmus $s, t \in \mathbb{Z}$ mit $sk + tn = 1$.
Setze $l = s \bmod n$.
Dann $1 = sk + \underbrace{tn}_{=0(\bmod n)} = ((s \bmod n) \cdot \underbrace{(k \bmod n)}_{=k}) \bmod n = l \odot k$ □

Bemerkung: k^{-1} mit Erweitertem Euklidischen Algorithmus berechenbar. Beispiel siehe nach 3.33 (S.43).

3.33 Korollar (Satz von Euler)

Ist $n \geq 2$, $x \in \mathbb{Z}$, $\text{ggT}(x, n) = 1$, so ist $x^{\varphi(n)} \equiv 1 \bmod n$. (Dabei ist φ die Eulersche Funktion.)

Beweis. Nach 3.32 ist $\mathbb{Z}_n^* := \{k \in \mathbb{Z}_n \mid \text{ggT}(k, n) = 1\}$ eine Gruppe bzgl. der Multiplikation $\odot$. Es ist $|\mathbb{Z}_n^*| = \varphi(n)$.
Sei $x = qn + r$, $0 \leq r \leq n - 1$.
$x^{\varphi(n)} = (qn + r)^{\varphi(n)} \equiv r^{\varphi(n)} \bmod n$

$$r \in \mathbb{Z}_n^* \overset{o(r)\,||\,\mathbb{Z}_n^*|}{\Longrightarrow} r^{|\mathbb{Z}_n^*|} = 1 \overset{|\mathbb{Z}_n^*| = \varphi(n) \text{ nach } 3.32}{\Longrightarrow} r^{\varphi(n)} \equiv 1 \bmod n$$

Potenzierung in $\mathbb{Z}_n^*$ — Potzenzierung in $\mathbb{Z}$

$\Rightarrow x^{\varphi(n)} \equiv 1 \bmod n$. □

Beispiel: $n = 264 \quad k = 17$

x	y	s_1	s_2	s	t_1	t_2	t	$g := x \text{ div } y$	$r := x \bmod y$
264	17	1	0	0	0	1	1	15	9
17	9	0	1	1	1	-15	-15	1	8
9	8	1	-1	-1	-15	16	16	1	1
8	$\underline{1}$	-1	2	$\underline{2}$	16	-31	$\underline{\underline{-31}}$		0

$1 = 2 \cdot 264 + (-31) \cdot 17 (= 528 - 527)$
$-31 \bmod 264 = 233$
Also: $17^{-1} = 233$ in $\mathbb{Z}_{264}$ [$233 \odot 17 = 3961 \bmod 264 = 1$, denn $3961 = 15 \cdot 264 + 1$]

3.34 Satz

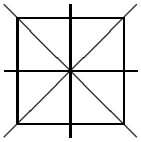
Sei G eine abelsche Gruppe der Ordnung pq, p, q Primzahlen $p \neq q$.
Dann ist G zyklisch.

Beweis. Existiert ein Element der Ordnung pq in G, so sind wir fertig.
Sei $1 \neq x \in G$. Dann $o(x) = p$ oder q.
Angenommen alle Elemente haben die Ordnung p. Dann gilt: $|G/\langle x\rangle| = q$. Sei $y \notin \langle x\rangle$. Dann $o(y\langle x\rangle) = p$ in $G/\langle x\rangle$. Dies ist ein Widerspruch zu Lagrange.
Genauso zeigt man, dass nicht alle Elemente die Ordnung q haben.
Also gibt es Elemente x, y mit $o(x) = p$ und $o(y) = q$. Setze $g = x \cdot y$.
Dann $g^p = y^p$, $\text{ggT}(p, q) = 1 \Rightarrow \langle y^p\rangle = \langle y\rangle$ nach 3.29
Also: $\langle y\rangle \leq \langle g\rangle$.
Analog: $\langle x\rangle \leq \langle g\rangle$.
$\Rightarrow p, q \mid |\langle g\rangle| \Rightarrow o(g) = p \cdot q$. □

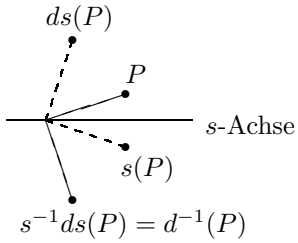
3.35 Beispiel

Sei G eine Gruppe der Ordnung $2n$ mit einem zyklischen Normalteiler N der Ordnung n, $N = \langle d\rangle$.
Angenommen in $G \setminus N$ existiert ein Element s mit $o(s) = 2$ und $s^{-1}ds = d^{-1}$. ($s^{-1} = s$)
[Beachte: In jeder Gruppe G gilt: Ist $N \leq G, g \in G$, so ist die Abbildung $\varphi_g : N \to N : n \mapsto g^{-1}ng$ ein bijektiver Homomorphismus (=Automorphismus) von N; *Konjugation* mit g.]
Dann auch $s^{-1}d^is = (d^i)^{-1}$; jedes Element von N wird durch Konjugation mit s auf sein Inverses abgebildet.
Dann gilt: Jedes Element $\overline{s} \in G \setminus N$ hat Ordnung 2 und $\overline{s}^{-1}d\overline{s} = d^{-1}$:
$G = N \cup sN$, also $\overline{s} = sd^i$
$\overline{s}^2 = sd^isd^i = (d^i)^{-1}d^i = 1$.
$\overline{s}^{-1}d\overline{s} = (d^i)^{-1}s^{-1}dsd^i = (d^i)^{-1}d^{-1}d^i = d^{-1}$.
Eine solche Gruppe heißt *Diedergruppe* der Ordnung $2n$. Sie ist bis auf Isomorphie eindeutig bestimmt. Bezeichnung: D_{2n}
z.B. S_3 ist Diedergruppe der Ordnung 6, $S_3 \cong D_6$.

D_{2n} tritt als Symmetriegruppe des regulären n-Ecks auf (n=4: Quadrat, siehe 3.3.8):
N besteht aus den Drehungen um Vielfache von $\frac{2\pi}{n}$, $G \setminus N$ aus lauter Spiegelungen.



d=Drehung um $\pi/2$
s=Spiegelung an einer der eingezeichneten Achsen



$D_{2n} = \langle d, s\rangle = \langle s, ds\rangle$
$D_{2n} = \{d^i, d^i s : i = 0, \ldots, n-1\}$
(Beachte: $sd^i s = d^{-i}$, d.h. $sd^i = d^{-i}s$ und $d^{-i} = d^{n-i}$ für $i \in \{1, \ldots, n-1\}$)
$d^i s d^j = d^{i-j} s$
$d^i s d^j s = d^{i-j}$

4 Gruppen und Prüfzeichencodierungen

Prüfzeichencodierungen (auch Prüfziffercodierungen)

Spezielle 1-fehlererkennende Codes.

Beispiel: Parity Check bei Alphabet $\{0, 1\}$ (vgl. Kapitel 1)

Typischerweise sind bei Prüfzeichncodierungen Alphabete größer, z.B.

- ISBN-Nr. (International Standard Book Number)
- EAN-Nr. (European Article Number)
- Banknotenkennzeichnungen

Hauptfehler bei der Eingabe oder Lesen einer "Ziffernfolge" $x_1, \ldots, x_n,\ n \geq 2$:

Einzelfehler (falsche Eingabe oder falsches Lesen einer Ziffer): 80%

Nachbartranspositionen ("Zahlendreher"; statt $x_i x_{i+1}$ wird $x_{i+1} x_i$ eingegeben): 10%

Fast alle praktisch vewendeten Prüfzeichencodierungen beruhen auf folgender Definition:

4.1 Definition

Sei $(G, \cdot)$ eine Gruppe.
Ein *Prüfzeichencode* $P_G = P_G(\pi_1, \ldots, \pi_n; c)$ über G wird bestimmt durch

1. n Permutationen $\pi_1, \ldots, \pi_n$ von G
2. ein Element $c \in G$.

Codewörter (über G) haben Länge n, sind also eine Teilmenge von $\underbrace{G \times \cdots \times G}_{n}$.

$(g_1, \ldots, g_n) \in P_G(\pi_1, \ldots, \pi_n; c) \Leftrightarrow \pi_1(g_1) \cdot \ldots \cdot \pi_n(g_n) = c$ (*Kontrollgleichung*)

(Dabei muss n nichts mit $|G|$ zu tun haben!)

4.2 Satz

Sei $P_G(\pi_1, \ldots, \pi_n; c)$ eon Prüfzeichencode.

1. Sind $g_1, \ldots, g_{n-1} \in G$, so gibt es genau ein $g_n \in G$ mit $(g_1, \ldots, g_n) \in P_G$ (g_n heißt *Prüfzeichen* oder *Prüfziffer*)
2. P_G ist 1-fehlererkennend (erkennt also Einzelfehler)
3. Sei $n \geq 3$. P_G erkennt Nachbartranspositionen
   $\Leftrightarrow g \cdot \pi_{i+1}(\pi_i^{-1}(h)) \neq h \cdot \pi_{i+1}(\pi_i^{-1}(g))\ \ \forall i = 1, \ldots, n-1\ \forall g, h \in G, g \neq h$

Beweis. 1.

$$\begin{aligned}(g_1,\ldots,g_n)\in P_G &\Leftrightarrow \pi_1(g_1)\cdot\ldots\cdot\pi_n(g_n)=c\\ &\Leftrightarrow \pi_n(g_n)=(\pi_1(g_1)\cdot\ldots\cdot\pi_{n-1}(g_{n-1}))^{-1}\cdot c\end{aligned}$$

Damit ist $\pi_n(g_n)$ eindeutig bestimmt, und da π_n eine Permutation ist, auch g_n.

2. Wie in 1. sieht man, dass für $(g_1,\ldots,g_n)\in P_G$ jedes g_i durch $g_1,\ldots,g_{i-1},g_{i+1},\ldots,g_n$ eindeutig bestimmt ist:

$$\pi_i(g_i)=(\pi_1(g_1)\cdot\ldots\cdot\pi_{i-1}(g_{i-1}))^{-1}\cdot c\cdot(\pi_{i+1}(g_{i+1})\cdot\ldots\cdot\pi_n(g_n))^{-1}$$

Daraus folgt die Behauptung.

3. $\Leftarrow$: Ang. $(g_1,\ldots,g_n)\in P_G,\ (g_1,\ldots,g_{i+1},g_i,\ldots,g_n)\in P_G\ \ g_{i+1}\neq g_i$
$\Rightarrow\ \pi_1(g_1)\cdot\ldots\cdot\pi_n(g_n)=c=\pi_1(g_1)\cdot\ldots\cdot\pi_i(g_{i+1})\pi_{i+1}(g_i)\cdot\ldots\cdot\pi_n(g_n)$
$\Rightarrow\ \underbrace{\pi_i(g_i)}_{=:g}\pi_{i+1}(g_{i+1})=\underbrace{\pi_i(g_{i+1})}_{=:h}\pi_{i+1}(g_i)$
$\Rightarrow\ g\pi_{i+1}(\pi_i^{-1}(h))=h\pi_{i+1}(\pi_i^{-1}(g))$, was ein Widerspruch ist.
$\Rightarrow$: Ang. es existieren $g,h\in G,\ g\neq h,\ i\in\{1,\ldots,n-1\}$ mit
$g\pi_{i+1}(\underbrace{\pi_i^{-1}(h)}_{g_{i+1}})=h\pi_{i+1}(\underbrace{\pi_i^{-1}(g)}_{g_i})$
$\Rightarrow\ \pi_i(g_i)\pi_{i+1}(g_{i+1})=\pi_i(g_{i+1})\pi_{i+1}(g_i)$.
Da $n\geq 3$, existieren dann $g_j,\ j\neq i,i+1$, so dass
$\pi_1(g_1)\cdot\ldots\cdot\pi_n(g_n)=c=\pi_1(g_1)\cdot\ldots\cdot\pi_i(g_{i+1})\pi_{i+1}(g_i)\cdot\ldots\cdot\pi_n(g_n)$ □

4.3 Beispiele

Allgemein: 1. $G=(\mathbb{Z}_m,\oplus)$

2. Wähle $w_1,\ldots,w_n$ mit $\mathrm{ggT}(w_i,m)=1\quad \pi_i:\begin{cases}\mathbb{Z}_m\to\mathbb{Z}_m\\ k\mapsto w_ik \bmod m\end{cases}$
$\langle w_i\rangle$ ist erzeugendes Element von $(\mathbb{Z}_m,\oplus)$ nach 3.29,
d.h. $\mathbb{Z}_m=\{w_ik : k=0,\ldots,m-1\}$
Also: π_i ist surjektiv und damit bijektiv.

3. $c=0$ und $w_n=1$ oder $w_n=-1(=m-1)$
Kontrollgleichung: $w_1k_1+\cdots+w_{n-1}k_{n-1}\pm k_n=0\ \ (\bmod m)\quad(*)$
(d.h. $k_n=\pm\sum_{i=1}^{n-1}w_ik_i$ in $\mathbb{Z}_m$)
$(k_1,\ldots,k_n)\in P_G\Leftrightarrow(*)$ gilt.
1-fehlererkennend mit Kontrollmatrix $H=\begin{pmatrix}w_1\\ \vdots\\ w_{n-1}\\ \pm1\end{pmatrix}$

Speziell: a) ISBN-Codierung
$n=10, m=11$ ($G=\mathbb{Z}_{11}$; statt 10 schreibt man X)
Bsp: 3-540-20521-7
Land Verlag Buch Prüfziffer

$w_i = i,\ i = 1, \ldots, 9$
$w_{10} = -1 = 10$

$$(k_1, \ldots, k_{10}) \text{ gültige ISBN-Nr. } \Leftrightarrow \sum_{i=1}^{10} i k_i \equiv 0 \mod 11$$

(Kontrollgleichung für ISBN-Code)

ISBN-Code erkennt Nachbartranspositionen:
Sei $k + \pi_{i+1}(\pi_i^{-1}(l)) = l + \pi_{i+1}(\pi_i^{-1}(k))$. Dann gilt:
$k + (i+1) \cdot i^{-1} \cdot l = l + (i+1) \cdot i^{-1} \cdot k \quad (i^{-1} \text{ in } \mathbb{Z}_{11})$
$ik + (i+1)l = il + (i+1)k$
$l = k$
Fertig mit 4.2.3

b) EAN-Codierung (genauer EAN-13)
$n = 13, m = 10$
$w_i = 1$ für i ungerade, $1 \leq i \leq 13$
$w_i = 3$ für i gerade, $2 \leq i \leq 12$
Kontrollgleichung:

$$(k_1, \ldots, k_{13}) \text{ gültige EAN-Nr. } \Leftrightarrow$$
$$k_1 + 3k_2 + k_3 + 3k_4 + \cdots + 3k_{12} + k_{13} \equiv 0 \mod 10$$

(k_1, k_2: Herstellungsland
$k_3 - k_7$: Hersteller
$k_8 - k_{12}$: Produkt)
Wird weiter codiert in Strichcode (siehe Vorlesung Codierungstheorie)
1-fehlererkennend
Aber: EAN-Code efüllt nicht die Bedingung aus 4.2.3

Sei i gerade: $0 + 3 \cdot 5 = 5 + 3 \cdot 0 \mod 10$
$\pi_i = \text{id},\ g = 0,\ h = 5$ in 4.2.3

Es ist leicht zu sehen:
Nachbartransposition $(k_i k_{i+1} \to k_{i+1} k_i)$ wird nicht erkannt, falls i gerade und $|k_i - k_{i+1}| = 5$.
(Näheres: http://www.barcodeisland.com/ean13.phtml)

Wir zeigen jetzt, dass es auf abelschen Gruppen der Ordnung 10 keinen 1-fehlererkennenden Prüfzeichencode gibt, der auch alle Nachbartranspositionen erkennt.
Allgemeiner:

4.4 Satz

Sei G eine abelsche Gruppe der Ordnung m. Sei $n \in \mathbb{N}, n \geq 3$.
Genau dann gibt es über G einen Prüfzeichencode der Länge n, der Nachbartranspositionen erkennt, falls m ungerade ist oder G mindestens zwei verschiedene Elemente der Ordnung 2 besitzt.

Der Beweis von 4.4 geht über den Rahmen der Vorlesung hinaus. Wir werden daher nur zwei Spezialfälle beweisen; einer davon wird die obige Behauptung für abelsche Gruppen der Ordnung 10 beinhalten.

Dazu benötigen wir einige Vorbereitungen:

Wir formulieren zunächst noch einmal die Behauptung aus 4.2.3 etwas anders:

4.5 Bemerkung

Sei $P_G(\pi_1, \ldots, \pi_n; c)$ ein Prüfzeichencode. Setze $\delta_i = \pi_{i+1} \circ \pi_i^{-1}$.
Dann gilt:

1. $$P_G \text{ erkennt Nachbartranspositionen an den Stellen } i, i+1 \\ \Leftrightarrow\ g \cdot \delta_i(h) \neq h \cdot \delta_i(g)\ \ \forall g, h \in G,\ g \neq h.$$

2. Ist G abelsch, so ist die Bedingung aus 1. gleichwertig mit
$$h^{-1}\delta_i(h) \neq g^{-1}\delta_i(g).$$

4.6 Definition

Sei G eine Gruppe, $\delta : G \to G$ eine Permutation.

1. δ heißt *antisymmetrisch*, falls
$$g \cdot \delta(h) \neq h \cdot \delta(g)\ \ \forall g, h \in G,\ g \neq h$$

2. δ heißt *Orthomorphismus*, falls die Abbildung $g \to g^{-1}\delta(g)$ wieder eine Permutation von G ist.

3. δ heißt *vollständige* Abbildung, falls die Abbildung $g \to g\delta(g)$ wieder eine Permutation von G ist.

4.7 Bemerkung

Ist G ablesch, so ist δ genau dann antisymmetrisch, wenn δ ein Orthomorphismus ist.

4.8 Satz

Sei G eine endliche Gruppe, $n \in \mathbb{N}, n \geq 3$.

1. Genau dann gibt es einen Prüfzeichencode der Länge n auf G, der jede Nachbartransposition erkennt, wenn es eine antisymmetrische Abbildung auf G gibt.
   Ist δ eine antisymmetrische Abbildung, so setze $\pi_i = \delta^i, i = 1, \ldots, n$. Dann ist $P_G(\pi_1, \ldots, \pi_n; c)$ für jedes $c \in G$ ein Prüfzeichencode, der jede Nachbartransposition erkennt.

2. Ist δ ein Orthomorphismus von G, so ist $\gamma : G \to G : g \mapsto g^{-1}\delta(g)$ eine vollständige Abbildung.

3. Ist δ eine vollständige Abbildung von G, so ist $\gamma : G \to G : g \mapsto g\delta(g)$ ein Orthomorphismus.

Beweis. 1. $\Rightarrow$: 4.5.1

$\Leftarrow$: Setze $\pi_i = \delta^i$; Permutation auf G.
$\pi_{i+1} \circ \pi_i^{-1} = \delta^{i+1} \circ \delta^{-i} = \delta$, d.h. die Behauptung folgt aus 4.5.1

2. γ Permutation auf G, da δ Orthomorphismus.
$g \mapsto g\gamma(g) = \delta(g)$ ist Permutation, da δ Permutation ist.
Also ist γ eine vollständige Abbildung.

3. Analog wie 2.

□

4.9 Korollar

Sei G eine endliche abelsche Gruppe, $n \in \mathbb{N}, n \geq 3$. Dann sind gleichwertig:

1. Es gibt einen Prüfzeichencode der Länge n auf G, der jede Nachbartransposition erkennt.

2. Es gibt eine antisymmetrische Permutation (d.h. nach 4.7 einen Orthomorphismus) auf G.

3. Es gibt eine vollständige Abbbildung auf G.

Spezialfall von Satz 4.4

Sei G eine endliche abelsche Gruppe, $n \in \mathbb{N}, n \geq 3$.

1. Ist $|G|$ ungerade, so gibt es auf G einen Prüfzeichencode der Länge n, der Nachbartranspositionen erkennt.

2. Ist $|G| = 2p$, p ungerade Primzahl, so gibt es auf G keinen Prüfzeichencode der Länge n, der Nachbartranspositionen erkennt.

Beweis. 1. Sei $|G| = 2k + 1$.
Dann ist $g^{2k+1} = 1$ für alle $g \in G$, also $(g^{k+1})^2 = g$ für alle $g \in G$.
Folglich ist die Abbildung $x \to x^2$ surjektiv, also eine Permutation auf G.
Daher ist $\delta = \mathrm{id}$ eine vollständige Abbildung auf G.
Nach 4.9 folgt die Behauptung.

2. Nach Satz 3.34 ist G zyklisch, enthält also nach Korollar 3.30 genau eine Untergruppe N der Ordnung p und genau eine Untergruppe $\langle s \rangle$ der Ordnung 2.
Angenommen die Behauptung ist falsch. Dann gibt es nach 4.9 einen Orthomorphismus δ von G. Es gilt:

$$\prod_{g \in G} g = \prod_{g \in G} g^{-1} \cdot \delta(g) = \prod_{g \in G} g^{-1} \cdot \prod_{g \in G} \delta(g) = (\prod_{g \in G} g)^{-1} \cdot (\prod_{g \in G} g) = 1$$

(Beachte: G ist abelsch)
Es ist $G = N \cup sN$.

Also: $N = (\prod_{g\in G})N = \prod_{g\in G}(gN) = \prod_{g\in N}(gN)\cdot\prod_{g\in G\setminus N}(gN)$
$= (sN)^{|N|} = s^{|N|}N = sN$, da $|N|$ ungerade und $s^2 = 1$.
Es folgt $s \in N$. Dies ist ein Widerspruch.

□

Mit Hilfe des Spezialfalls von Satz 4.4 wird klar, warum die EAN-Codierung (über $\mathbb{Z}_{10}$) gewisse Nachbartranspositionen nicht erkennt, und warum dies über $\mathbb{Z}_{11}$ möglich ist (vgl. ISBN-Code).
Tatsächlich gibt es nach diesem Satz über einer abelschen Gruppe der Ordnung 10 (also über $\mathbb{Z}_{10}$) überhaupt keinen Prüfzeichencode, der alle Nachbartranspositionen erkennt.
Andererseits ist $\{0, 1, \ldots, 9\}$ ein beliebtes Alphabet.
Frage: Kann man mit einer nicht-abelschen Gruppe der Ordnung 10 einen Prüfzeichencode konstruieren, der alle Nachbartranspositionen erkennt?
Antwort: Ja, mit D_{10} (dies ist übrigens bis auf Isomorphie die einzige nicht-abelsche Gruppe der Ordnung 10).
$D_{10} = \{d^j, d^j s : j = 0, \ldots, 4\}$, $sd^j s = d^{-j}$

Multiplikationstafel: $d^i d^j = d^{(i+j) \bmod 5}$
$d^i d^j s = d^{(i+j) \bmod 5} s$
$d^i s d^j = d^{(i-j) \bmod 5} s$
$d^i s d^j s = d^{(i-j) \bmod 5}$

4.10 Satz

Die Permutation $\delta = \begin{pmatrix} d^0 & d^1 & d^2 & d^3 & d^4 & d^0 s & d^1 s & d^2 s & d^3 s & d^4 s \\ d^1 & d^0 s & d^2 s & d^1 s & d^2 & d^3 s & d^3 & d^0 & d^4 s & d^4 \end{pmatrix}$ ist eine anti-symmetrische Abbildung auf D_{10}.

Beweis. Wir haben $g\cdot\delta(h) \neq h\cdot\delta(g)\ \forall g, h \in D_{10}, g \neq h$ zu zeigen.

		$h \to$	d^0	d^1	d^2	d^3	d^4	$d^0 s$	$d^1 s$	$d^2 s$	$d^3 s$	$d^4 s$
		$\delta(h) \to$	d^1	$d^0 s$	$d^2 s$	$d^1 s$	d^2	$d^3 s$	d^3	d^0	$d^4 s$	d^4
g	$\delta(g)$											
$\downarrow$	$\downarrow$											
d^0	d^1	$g\delta(h) \to$		-	-	-	d^2	$d^3 s$	-	-	$d^4 s$	-
		$h\delta(g) \to$					d^0	$d^4 s$			$d^2 s$	
d^1	$d^0 s$	$g\delta(h) \to$	-		$d^3 s$	$d^2 s$	-	-	d^4	d^1	-	d^0
		$h\delta(g) \to$			$d^2 s$	$d^3 s$			d^1	d^2		d^4
d^2	$d^2 s$	$g\delta(h) \to$	-	$d^2 s$		$d^3 s$	-	-	d^0	d^2	-	d^1
		$h\delta(g) \to$		$d^3 s$		$d^0 s$			d^4	d^0		d^2
d^3	$d^1 s$	$g\delta(h) \to$	-	$d^3 s$	$d^0 s$		-	-	d^1	d^3	-	d^2
		$h\delta(g) \to$		$d^2 s$	$d^3 s$				d^0	d^1		d^3
d^4	d^2	$g\delta(h) \to$	d^0	-	-	-		$d^2 s$	-	-	$d^3 s$	-
		$h\delta(g) \to$	d^2					$d^3 s$			$d^1 s$	
$d^0 s$	$d^3 s$	$g\delta(h) \to$	$d^4 s$	-	-	-	$d^3 s$		-	-	d^1	-
		$h\delta(g) \to$	$d^3 s$				$d^2 s$				d^0	
$d^1 s$	d^3	$g\delta(h) \to$	-	d^1	d^4	d^0	-	-		$d^1 s$	-	$d^2 s$
		$h\delta(g) \to$		d^4	d^0	d^1				$d^4 s$		$d^1 s$

d^2s	d^0	$g\delta(h) \to$ $h\delta(g) \to$	-	d^2 d^1	d^0 d^2	d^1 d^3	-	-	d^4s d^1s		-	d^3s d^4s
d^3s	d^4s	$g\delta(h) \to$ $h\delta(g) \to$	d^2s d^4s	-	-	-	d^1s d^3s	d^0 d^1	-	-		-
d^4s	d^4	$g\delta(h) \to$ $h\delta(g) \to$	-	d^4 d^0	d^2 d^1	d^3 d^2	-	-	d^1s d^2s	d^4s d^3s	-	

(-: Unter den $(g, h, \delta(g), \delta(h))$ treten entweder genau 3 Elemente der Form d^i oder der Form $d^i s$ auf; dann kann nach der Multiplikationstabelle für D_{10} nie $g\delta(h) = h\delta(g)$ gelten. Diese Felder brauchen also nicht überprüft zu werden.) □

Bemerkung: Es gibt einfachere anti-symmetrische Abbildungen auf D_{10}, aber die angegebene ist für das folgende Beispiel relevant.

4.11 Beispiel

Prüfzeichencodierung der Seriennummern der früheren DM-Banknoten:
Seriennummern sind 11-stellige Nummern über dem Alphabet
$\{A, D, G, K, L, N, S, U, Y, Z, 0, 1, \ldots, 9\}$.
Dabei: 2 Buchstaben - 7 Ziffern - 1 Buchstabe - 1 Prüfziffer (außer bei 5DM-Note; dort steht am Anfang nur ein Buchstabe)
Nennwert ist nicht in der Seriennummer codiert.
Buchstabenauswahl, um Lesefehler gering zu halten.

Zur Codierung:
Ersetze Buchstaben durch Ziffern $\{0, \ldots, 9\}$ wie folgt:

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

Jeder Geldscheinnummer entspricht dann eine 11-stellige Nummer über $\{0, \ldots, 9\}$.
Übertrage die Multiplikation von D_{10} auf $\{0, \ldots, 9\}$ wie folgt:

$$d^j \to j,\ 0 \le j \le 4$$

$$d^j s \to j + 5,\ 0 \le j \le 4$$

Die Multiplikation von D_{10} überträgt sich dann zu einer Multiplikation $*$ auf $\{0, \ldots, 9\}$ wie folgt:

$i * j$	$0 \le j \le 4$	$5 \le j \le 9$
$0 \le i \le 4$	$(i + j) \mod 5$	$5 + ((i + j) \mod 5)$
$5 \le i \le 9$	$5 + ((i - j) \mod 5)$	$(i - j) \mod 5$

Die anti-symmetrische Permutation δ auf D_{10} geht dann über zu einer Permutation von $\{0, \ldots, 9\}$, die wir auch mit δ bezeichnen:

$$\delta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix} = (01589427)(36)$$

Es ist $o(\delta) = 8$, d.h. $\delta^8 = \mathrm{id},\ \delta^9 = \delta,\ \delta^{10} = \delta^2,\ \delta^{11} = \delta^3$. Nach Satz 4.8.1 würde man jetzt eine Prüfzeichencodierung auf $\{0, \ldots, 9\}$ erhalten, die alle Nachbartranspositionen erhält, durch $P_G(\delta^1, \delta^2, \ldots, \delta^{11}; 0)$

Hier wäre auch jede andere Ziffer möglich.

Tatsächlich ist bei den DM-Scheinen eine Modifikation dieser Prüfzeichencodierung vorgenommen worden zu $P_G(\pi_1, \ldots, \pi_{11}; 0)$:
Man setzt $\pi_i = \delta^i,\ i = 1, \ldots, 10$, aber $\pi_{11} = \mathrm{id}$ (und $c = 0$).
Die Kontrollgleichung lautet daher:
$(x_1, \ldots, x_{11}), x_i \in \{0, \ldots, 9\}$ gültige Geldscheinnummer (nach Übersetzung)
$\Leftrightarrow\ \delta(x_1) * \delta^2(x_2) * \cdots * \delta^{10}(x_{10}) * x_{11} = 0$
(Dabei entspricht $*$ der Multiplikation in D_{10}.)

Beispiel: Geldscheinnummer $AA6186305Z2\ \ \rightarrow\ \ 00618630592$
Kontrollgleichung:
$\delta(0) * \delta^2(0) * \delta^3(6) * \delta^4(1) * \delta^5(8) * \delta^6(6) * \delta^7(3) * \delta^8(0) * \delta^9(5) * \delta^{10}(9) * 2$
$= \underbrace{1 * 5}_{6} * \underbrace{3 * 4}_{2} * \underbrace{0 * 6}_{6} * \underbrace{6 * 0}_{6} * \underbrace{8 * 2}_{6} * 2$
$= \underbrace{6 * 2}_{9} * \underbrace{6 * 6}_{0} * \underbrace{6 * 2}_{9}$
$= 9 * 9 = 0 \qquad \surd$

Tatsächlich erkennt $P_G(\pi_1, \ldots, \pi_{11}; 0)$ nach 4.5.1 die Nachbartranspositionen an den Stellen $1, \ldots, 10$ aber nicht notwendig zwischen den Stellen $10, 11$. Da in der Originalnummer an der Stelle 10 ein Buchstabe und an der Stelle 11 eine Ziffer steht, ist dies nicht problematisch.

4.12 Bemerkung

Die Codierung der Euro-Scheine ist einfacher.
Die Seriennummern bestehen aus einem führenden Buchstaben A-Z, der das Ausgabeland bezeichnet (es sind nicht alle verteilt, nämlich A-I, O, Q; X steht für Deutschland) und einer 11-stelligen Zahl; dabei ist die letzte Ziffer eine Prüfziffer.
Verfahren:
Codiere die Buchstaben in 2-stellige Dezimalzahl, entsprechend ihrer Position im Alphabet.
Dies liefert eine 13-stellige Ziffernfolge $x_1, \ldots, x_{13}$.
Gültige Ziffernfolge $\Leftrightarrow\ \sum x_i \equiv 8 \bmod 9$
(Also könnte man 9 auch durch 0 ersetzen und in $\mathbb{Z}_9$ rechnen.) Die Ersetzung $9 \leftrightarrow 0$ zeigt, dass nicht alle Einzelfehler erkannt werden; überdies werden keine Nachbartranspositionen erkannt.
Vorteil: Modulo 9 - Rechnung = (iterierte) Quersummenbildung, bis 1-stelliges Ergebnis. Warum die Kontrollgleichung gerade 8 ergeben soll, ist unklar.

5 Permutationsgruppen und die Pólya'sche Abzählmethode

5.1 Zyklenschreibweise von Permutationen

Beispiel: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 1 & 6 & 4 & 3 \end{pmatrix} = (1\ 2\ 5)(3\ 7\ 4\ 8)(6) = (3\ 7\ 4\ 8)(1\ 2\ 5)$
Allgemein: Zyklus $(a_1, \ldots, a_k)$ beschreibt die Permutation
$a_1 \to a_2,\ a_2 \to a_3, \ldots, a_{k-1} \to a_k, a_k \to a_1$, alle übrigen Elemente bleiben fest.

Beachte: $(1\ 2\ 5) = (2\ 5\ 1) = (5\ 1\ 2)$; Zyklen sind nur eindeutig bis auf zyklische Vertauschung der Einträge!

Allgemein gilt: Jede Permutation (auf endlicher Menge) lässt sich als Produkt von elementefremden Zyklen schreiben. Diese Darstellung ist bis auf die Reihenfolge eindeutig. Elementefremde Zyklen sind vertauschbar (Zyklenzerlegung).

Bemerkung: Ordnung einer Permutation g = kgV der Zyklenlängen von g.

5.2 Definition

Sei $g \in S_n$. Der *Permutationstyp* $t(g)$ von g ist das folgende Polynom in n Variablen $x_1, \ldots, x_n$:

$$t(g) = \prod_{i=1}^{n} x_i^{k(i)}$$

wobei $k(i)$ die Anzahl der Zyklen der Länge i in der Zyklenzerlegung von g ist.
Also: $\sum_{i=1}^{n} k(i) = k =$ Anzahl aller Zyklen in der Zyklenzerlegung von g (inklusive Zyklen der Länge 1).
$\sum_{i=1}^{n} ik(i) = n.$

Beispiel:
$n = 8;\ g = (1\ 2\ 5)(3\ 7\ 4\ 8)(6)$
$t(g) = x_1 x_3 x_4$
$h = (12)(34)(56)(78);\ t(h) = x_2^4$

5.3 Definition

Sei Ω eine endliche Menge, $\mathrm{Sym}(\Omega)$ die symmetrische Gruppe auf Ω, d.h. die Gruppe aller Permutationen auf Ω. (Also $\mathrm{Sym}(\Omega) \cong S_n$, wenn $|\Omega| = n$.)

1. Ist $H \leq \mathrm{Sym}(\Omega)$, so heißt H *Permutationsgruppe* auf Ω.

2. Sei G eine Gruppe. G *operiert bzgl.* φ *auf* Ω, falls $\varphi : G \to \mathrm{Sym}(\Omega)$ ein Gruppenhomomorphismus ist. ($\varphi(G)$ ist dann eine Permutationsgruppe auf Ω.)
   Oft schreibt man für $(\varphi(g))(\alpha)$ einfach $g(\alpha)$ für $g \in G,\ \alpha \in \Omega$, wenn φ aus dem Kontext klar ist.
   In dieser Schreibweise:

$$\begin{aligned} 1(\alpha) &= \alpha && \forall \alpha \in \Omega \\ (g_1 g_2)(\alpha) &= g_1(g_2(\alpha)) && \forall \alpha \in \Omega \; \forall g_1, g_2 \in G \end{aligned}$$

(daher: $g(\alpha) = \beta$, so $g^{-1}(\beta) = \alpha$)

5.4 Beispiel

Sei G Gruppe, $\Omega = G$
G operiert auf Ω durch Linksmultiplikation:
$\varphi : G \to \mathrm{Sym}(\Omega)$, $\varphi(g)(h) = gh$
Kern $\varphi = \{g \in G \mid \varphi(g) = \mathrm{id}_\Omega\} = \{g \in G \mid gh = h \; \forall h \in \underbrace{G}_{\Omega}\} = \{1\}$

Homomorphiesatz:
$G \cong G/\{1\} = G/\mathrm{Kern}\varphi \cong \varphi(G) \leq \mathrm{Sym}(\Omega)$

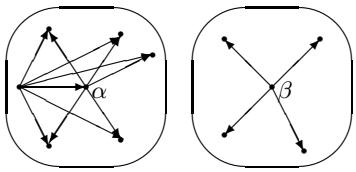
Also: Jede endliche Gruppe ist isomorph zu einer Untergruppe einer endlichen symmetrischen Gruppe. (Satz von Cayley)

5.5 Definition

G operiere auf Ω. Definiere die Relation $\sim_G$ auf Ω durch:

$$\alpha \sim_G \beta \;\Leftrightarrow\; \exists g \in G : g(\alpha) = \beta.$$

$\sim_G$ ist Äquivalenzrelation auf Ω. Ist $\alpha \in \Omega$, so ist die Äquivalenzklasse, die α enthält, gerade $G(\alpha) = \{g(\alpha) \mid g \in G\}$. $G(\alpha)$ wird die *Bahn* von α unter G genannt.



Wenn es nur eine Bahn gibt, so operiert G *transitiv* auf Ω

Beispiele

1. $\Omega = \{1, 2, 3, 4, 5\}$ $\quad G = \langle (12)(34)(5) \rangle$ $\quad |G| = 2$

   Bahnen von G: $G(1) = G(2) = \{1, 2\}$
   $G(3) = G(4) = \{3, 4\}$
   $G(5) = \{5\}$

2. Ω wie oben, $G = \langle (1\ 2\ 3\ 4\ 5) \rangle$. Es gibt nur eine Bahn; G operiert transitiv auf Ω.

3. G operiere auf $\Omega = G$ durch Linksmultiplikation: Eine Bahn, G operiert transitiv.

5.6 Definition

G operiere auf Ω.

1. Ist $\alpha \in \Omega$, so heißt $G_\alpha = \{g \in G \mid g(\alpha) = \alpha\}$ *Stabilisator* von α unter G.
2. Ist $g \in G$, so ist $\mathrm{Fix}(g) = \{\alpha \in \Omega \mid g(\alpha) = \alpha\}$ die *Fixpunktmenge* von g auf Ω.

5.7 Satz

G operiere auf Ω, $\alpha \in \Omega$

1. $G_\alpha \leq G$
2. $|G(\alpha)| = |G : G_\alpha| \left(= \frac{|G|}{|G_\alpha|}\right)$
3. $\sum\limits_{\beta \in G(\alpha)} |G_\alpha| = |G|$

Beweis. 1. $\surd$

2. $g_1, g_2 \in G:\ g_1(\alpha) = g_2(\alpha) \ \Leftrightarrow\ g_2^{-1} g_1(\alpha) = \alpha \Leftrightarrow g_2^{-1} g_1 \in G_\alpha$
   $\Leftrightarrow g_1 G_\alpha = g_2 G_\alpha$.
   $|G(\alpha)| = |G : G_\alpha|$
3. $\alpha \in \Omega$, so nach 2. $|G| = |G(\alpha)| \cdot |G_\alpha|$.
   Ist $\beta \in G(\alpha)$, so ist $G(\beta) = G(\alpha)$ (Äquivalenzrelation).
   $\sum\limits_{\beta \in G(\alpha)} |G_\beta| \overset{2.}{=} \sum\limits_{\beta \in G(\alpha)} \frac{|G|}{|G(\beta)|} = \sum\limits_{\beta \in G(\alpha)} = \frac{|G|}{|G(\alpha)|} = |G(\alpha)| \cdot \frac{|G|}{|G(\alpha)|} = |G|.$

□

5.8 Satz

G operiere auf Ω. Dann: $\sum\limits_{g \in G} |\mathrm{Fix}(g)| = \sum\limits_{\alpha \in \Omega} |G_\alpha|$

Beweis. Prinzip des doppelten Abzählens:
$\mathcal{M} = \{(g, \alpha) : g \in G, \alpha \in \Omega, g(\alpha) = \alpha\} \subseteq G \times \Omega$
$\sum\limits_{g \in G} |\mathrm{Fix}(g)| = |\mathcal{M}| = \sum\limits_{\alpha \in \Omega} |G_\alpha|$ □

5.9 Satz (Burnside-Lemma; Frobenius)

G operiere auf Ω. Dann gilt:
Anzahl der Bahnen von G auf $\Omega = \frac{1}{|G|} \sum\limits_{g \in G} |\mathrm{Fix}(g)|$.

Beweis. Sei t die Anzahl der Bahnen von G auf Ω: $G(\alpha_1), \ldots, G(\alpha_t)$, $\alpha_i \in \Omega$.
$\sum\limits_{g \in G} |\mathrm{Fix}(g)| \overset{5.8}{=} \sum\limits_{\alpha \in \Omega} |G_\alpha| = \sum\limits_{i=1}^{t} \sum\limits_{\beta \in G(\alpha_i)} |G_\beta| \overset{5.7.3}{=} t \cdot |G|$ □

5.10 Beispiele

1. Ω = Ecken eines Quadrats, $G = D_8$ operiert auf Ω als Symmetriegruppe.
   $t = 1$
   $g = \mathrm{id}$, $|\mathrm{Fix}(g)| = 4$
   g Drehung um 90°, 180°, 270° um Mittelpunkt des Quadrats, $|\mathrm{Fix}(g)| = 0$
   g Spiegelung an einer der Seitenhalbierenden: $|\mathrm{Fix}(g)| = 0$
   g Spiegelung an einer der Diagonalen: $|\mathrm{Fix}(g)| = 2$
   Anzahl der Bahnen $t = 1$
   Überprüfung mit Burnside: $1 = \frac{1}{8}(4 + 2 + 2)$ $\surd$

   s Spiegelung an einer Diagonalen, $H = \langle s \rangle$.
   Anzahl der Bahnen von H auf Ω: 3
   $3 = \frac{1}{2}(4 + 2)$. $\surd$

2. Färbe die Ecken des Quadrats mit jeweils einer der Farben $g = \text{grün}, r = \text{rot}$.
   Wieviele unterschiedliche Färbungen gibt es?
   Was heißt dabei unterschiedlich?
   - Zwei Färbungen heißen äquivalent (und werden dann als gleich angesehen), wenn sie durch eine Drehung des Quadrats auseinander hervorgehen.

   Sei $\widetilde{\Omega} = \{(y_1, y_2, y_3, y_4) \mid y_i \in \{g, r\}\}$ Menge der Färbungen (y_1, y_2, y_3, y_4), y_i = Farbe der Ecke i.
   Anzahl aller Möglichkeiten: $|\widetilde{\Omega}| = 2^4$

   $Z_4 = \langle d \rangle$ operiert auf $\widetilde{\Omega}$ durch
   $$\begin{array}{lcl} d(y_1, y_2, y_3, y_4) & = & (y_4, y_1, y_2, y_3) \\ d^2(y_1, y_2, y_3, y_4) & = & (y_3, y_4, y_1, y_2) \\ \ldots & & \end{array}$$

   Äquivalenzklassen der Färbungen = Anzahl der Bahnen von Z_4 auf $\widetilde{\Omega}$.
   Bestimmung der Anzahl t der Bahnen von Z_4 auf $\widetilde{\Omega}$ mit 5.9:

   $$\begin{array}{lcll} |\mathrm{Fix}(d^0)| & = & 2^4 = 16 & \\ |\mathrm{Fix}(d)| & = & 2 & (rrrr), (gggg) \\ |\mathrm{Fix}(d^2)| & = & 4 & (rrrr), (gggg), (rgrg), (grgr) \\ |\mathrm{Fix}(d^3)| & = & 2 & (rrrr), (gggg) \end{array}$$

   Anzahl der unterschiedlichen Färbungen (wie oben definiert) =
   $t = \frac{1}{4}(16 + 2 + 2 + 4) = 6$.
   Es gibt 6 verschiedene Färbungen.
   Vertreter der Äquivalenzklassen:
   $(rrrr), (gggg), (rggg), (rgrg), (rrgg), (rrrg)$.
   (vgl. Ketten mit 4 Perlen von 2 verschiedenen Farben)

   Was ist der Grund für die Fixpunktanzahlen von $d^0, \ldots, d^3$ auf $\widetilde{\Omega}$?
   $$\begin{array}{lll} d^0 & = (1)(2)(3)(4) & \text{Zyklenzerlegung auf } \Omega \\ d & = (1234) & \text{Zyklenzerlegung auf } \Omega \\ d^2 & = (13)(24) & \text{Zyklenzerlegung auf } \Omega \\ d^3 & = (1432) & \text{Zyklenzerlegung auf } \Omega \end{array}$$

Färbung (y_1, y_2, y_3, y_4) fest unter d^i
$\Leftrightarrow$ sind a, b im gleichen Zyklus von d^i, so $y_a = y_b$; d.h. alle Elemente innerhalb eines Zyklus von d^i sind gleich gefärbt.
Hat d^i k viele Zyklen, so sind es 2^k viele Möglichkeiten für Färbungen, die unter d^i fest sind.

Diese Überlegung lässt sich verallgemeinern:

5.11 Bemerkung

Sei $|\Omega| = n$, o.B.d.A. $\Omega = \{1, \ldots, n\}$. G sei eine endliche Gruppe, G operiere auf Ω.
Wir betrachten Färbungen der Elemente von Ω mit m verschiedenen Farben $f_1, \ldots, f_m$.
Die Menge aller Färbungen lässt sich beschreiben durch:

$$\widetilde{\Omega} = \{(y_1, \ldots, y_n) \mid y_i \in \{f_1, \ldots, f_m\}\}$$

y_i = Farbe des Elements $i \in \Omega$
G operiert auf $\widetilde{\Omega}$ durch

$$g(y_1, \ldots, y_n) := (y_{g^{-1}(1)}, \ldots, y_{g^{-1}(n)}),$$

(Nachrechnen: $g_1(g_2(y_1, \ldots, y_n)) = (g_1 g_2)(y_1, \ldots, y_n)$)

Zwei Färbungen $(y_1, \ldots, y_n)$, $(y'_1, \ldots, y'_n)$ heißen äquivalent bzgl. G, falls sie in derselben Bahn von G auf $\widetilde{\Omega}$ liegen, d.h. falls $g \in G$ existiert mit $(y'_1, \ldots, y'_n) = (y_{g(1)}, \ldots, y_{g(n)})$.

Anzahl der nicht-äquivalenten Färbungen bzgl. G = Anzahl der Bahnen von G auf $\widetilde{\Omega} \overset{5.9}{=} \frac{1}{|G|} \sum\limits_{g \in G} |\mathrm{Fix}_{\widetilde{\Omega}}(g)|$.
$(y_1, \ldots, y_n) \in \mathrm{Fix}_{\widetilde{\Omega}}(g) \Leftrightarrow$ Liegen i, j im selben Zyklus von g, so $y_i = y_j$.
Hat g k Zyklen (auf Ω), so $|\mathrm{Fix}_{\widetilde{\Omega}}(g)| = m^k$.
Ist $t(g) = \prod_{i=1}^{n} x_i^{k(i)}$ Permutationstyp ($k(i)$ = Anzahl der Zyklen der Länge i, also $k = k(1) + \ldots + k(n)$), so $|\mathrm{Fix}_{\widetilde{\Omega}}(g)| = m^k = \prod_{i=1}^{n} m^{k(i)}$.

5.12 Definition

G operiere auf Ω, $|\Omega| = n$. Dann ist der *Zyklenzeiger* von G definiert als $Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum\limits_{g \in G} t(g)$, Polynom in $x_1, \ldots, x_n$.

Aus 5.11 ergibt sich:

5.13 Satz

G operiere auf Ω, $|\Omega| = n$. Ω sei mit m Farben gefärbt. Dann ist die Anzahl der bzgl. G nicht-äquivalenten Färbungen gerade $Z_G(m, \ldots, m)$.

5.14 Beispiel

4×4-Schachbrett, Felder schwarz oder weiß färben.
Wieviele bzgl. D_8 unterschiedliche Färbungen gibt es?
$|\Omega| = 16,\ \Omega$ = Felder des Schachbretts.
d^i Drehungen um $i \cdot 90°,\ i = 0, 1, 2, 3$
$t(d^0) = x_0^{16},\ t(d^1) = x_4^4 = t(d^3),\ t(d^2) = x_2^8$
s Spiegelung an Seitenhalbierenden: $t(s) = x_2^8$ (2-mal)
$\widetilde{s}$ Spiegelung an Diagonalen: $t(\widetilde{s}) = x_1^4 x_2^6$ (2-mal)

$G = D_8$:

$$\begin{aligned} Z_G(x_1, \ldots, x_{16}) &= \tfrac{1}{8}(x_1^{16} + 2x_1^4x_2^6 + 3x_2^8 + 2x_4^4) \\ Z_G(2, \ldots, 2) &= \tfrac{1}{8}(2^{16} + 2^{11} + 3 \cdot 2^8 + 2^5) \\ &= 2^{13} + 2^8 + 3 \cdot 2^5 + 2^2 \\ &= 8548 \end{aligned}$$

Wieviele unterschiedliche Färbungen gibt es bezüglich $Z_4 = \{d^0, \ldots, d^3\}$?
$G = Z_4$:

$$\begin{aligned} Z_G(x_1, \ldots, x_{16}) &= \tfrac{1}{4}(x^{16} + x_2^8 + 2x_4^4) \\ Z_G(2, \ldots, 2) &= \tfrac{1}{4}(2^{16} + 2^8 + 2^5) \\ &= 2^{14} + 2^6 + 2^3 \\ &= 18456 \end{aligned}$$

Wir gehen jetzt einen Schritt weiter:
Ω mit $|\Omega| = n$ werde mit m Farben gefärbt, G operiere auf Ω.
Wieviele bzgl. G nicht-äquivalente Färbungen gibt es, wenn Farbe f_1 genau n_1-mal, $\ldots$, f_m genau n_m-mal verwendet werden darf, $n_1 + \ldots + n_m = n$?

Dazu überlegen wir zunächst, wieviele Fixpunkte ein $g \in G$ auf der Menge derjenigen Färbungen hat, in denen die Farbe f_i genau n_i-mal vorkommt.

Beispiel:

$n = 7$	$g = (1)(4)(2\ 6)(3\ 5\ 7)$		
$m = 2$	$n_1 = 3$	$n_2 = 4$	
(1)	(4)	(2 6)	(3 5 7)
f_1	f_2	f_1	f_2
f_2	f_1	f_1	f_2
f_2	f_2	f_2	f_1

In $t(g) = x_1^2x_2x_3$ ersetze x_1 durch $f_1 + f_2$, x_2 durch $f_1^2 + f_2^2$ und x_3 durch $f_1^3 + f_2^3$ (formale Ausdrücke).

Ausmultiplizieren: aus jeder Klammer einen möglichen Summanden nehmen und aufaddieren. Jedes Produkt ist von der Form $f_1^i f_2^j$, $i + j = 7$.

Beispiel:

$$\begin{array}{cccccc} (f_1 + f_2) & (f_1 + f_2) & (f_1^2 + f_2^2) & (f_1^3 + f_2^3) & & \\ \downarrow & \downarrow & \downarrow & \downarrow & & \\ f_1 & f_2 & f_1^2 & f_2^3 & \to & f_1^3 f_2^4 \end{array}$$

Auswahl von f_1^l aus einer Klammer bei Produktbildung entspricht Einfärben eines l-Zyklus mit f_1.

Obiges Beispiel: 1 1-er Zyklus mit f_1 und 1 2-er Zyklus mit f_2

Andere Möglichkeiten: $f_2\ f_1\ f_1^2\ f_2^3\ \to f_1^3 f_2^4$
$f_2\ f_2\ f_2^2\ f_1^3\ \to f_1^3 f_2^4$

Also: Koeffizient von $f_1^3 f_2^4$ in $(f_1+f_2)^2(f_1^2+f_2^2)(f_1^3+f_2^3)$ = Anzahl der Färbungen von $\{1,\dots,7\}$, alle Zyklen von g gleichfarbig, genau 3 Elemente mit f_1 gefärbt.

Dies gilt allgemein:

5.15 Satz

G operiere auf Ω, $|\Omega| = n$. Ω werde mit m vielen Farben $f_1,\dots,f_m$ gefärbt.
Ist $g \in G$, so ersetze in $t(g) = \prod_{i=1}^n x_i^{k(i)}$ jedes x_i durch $f_1^i + \dots + f_m^i$. Dies liefert ein "formales" Polynom in $f_1,\dots,f_m$, das eine Summe von Monomen der Form $f_1^{n_1}\dots f_m^{n_m}, n_1+\dots+n_m = n$ ist $(1\cdot k(1) + 2\cdot k(2) + \dots + nk(n) = n)$.
Fasst man gleiche Monome zusammen, so gibt der Koeffizient von $f_1^{n_1}\cdots f_m^{n_m}$ die Anzahl der Färbungen an, die fest sind unter g und die genau n_i-mal Farbe f_i, enthalten, $i = 1,\dots,m$.

5.16 Satz von Pólya (1937)

G operiere auf Ω, $|\Omega| = n$. Ω werde mit m Farben $f_1,\dots,f_m$ gefärbt.
Ersetze im Zyklenzeiger $Z_G(x_1,\dots,x_n) = \frac{1}{|G|}\sum\limits_{g\in G} t(g)$ jedes x_i durch
$f_1^i + \dots + f_m^i$: $\quad Z_G(f_1+\dots+f_m, f_1^2+\dots+f_m^2, \dots, f_1^n+\dots+f_m^n)$
In diesem Polynom ist der Koeffizient von $f_1^{n_1}\cdots f_m^{n_m}$ die Anzahl der bzgl. G verschiedenen Färbungen von Ω, in denen die Farbe f_i genau n_i-mal vorkommt, $i = 1,\dots,m$.

Beweis. Sei $v = (n_1,\dots,n_m),\ n_i \in \mathbb{N}_0,\ n_1+\dots+n_m = n$.
$\widetilde{\Omega}_v = \{(y_1,\dots,y_m) \mid y_j \in \{f_1,\dots,f_m\},\ f_i$ tritt n_i-mal auf, $i = 1,\dots,m\} \subseteq \widetilde{\Omega}$.
G operiert auf $\widetilde{\Omega}_v$.
Gesuchte Anzahl = Anzahl der Bahnen von G auf $\widetilde{\Omega}_v$.
Ist $g \in G$, so $|\mathrm{Fix}_{\widetilde{\Omega}_v}(g)| \overset{5.15}{=}$ Koeff. von $f_1^{n_1}\cdots f_m^{n_m}$ in
$t(g)(f_1+\dots+f_m, \dots, f_1^n+\dots+f_m^n)$.
Also: $\sum\limits_{\substack{v=(n_1,\dots,n_m)\\ n_1+\dots+n_m=n\\ n_i\in\mathbb{N}_0}} |\mathrm{Fix}_{\widetilde{\Omega}_v}(g)| f_1^{n_1}\dots f_m^{n_m} = t(g)(f_1+\dots+f_m, \dots, f_1^n+\dots+f_m^n)$
Aufsummieren über alle $g \in G$ und dividieren durch $|G|$:
Links:
$\frac{1}{|G|}\sum\limits_{g\in G} \sum\limits_{\substack{v=(n_1,\dots,n_m)\\ n_1+\dots+n_m=n\\ n_i\in\mathbb{N}_0}} |\mathrm{Fix}_{\widetilde{\Omega}_v}| f_1^{n_1}\dots f_m^{n_m}$

$= \sum\limits_{\substack{v=(n_1,\dots,n_m)\\ n_1+\dots+n_m=n\\ n_i\in\mathbb{N}_0}} \underbrace{\left(\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_{\widetilde{\Omega}_v}(g)|\right)}_{\overset{5.9}{=}\text{ Anzahl der Bahnen von } G \text{ auf } \widetilde{\Omega}_v \ =\ \text{gesuchte Anzahl}} f_1^{n_1}\dots f_m^{n_m}$

Rechts:

$$\frac{1}{|G|}\sum_{g\in G} t(g)(f_1+\ldots+f_m,\ldots,f_1^n+\ldots+f_m^n) = Z_G(f_1+\ldots+f_m,\ldots,f_1^n+\ldots+f_m^n)$$

□

5.17 Beispiele

1. Wieviele Halsketten mit 20 Perlen, davon 2 rot, 9 grün, 9 blau gibt es? Ketten sind gleich, wenn sie äquivalent bzgl. D_{40} sind.
   - Drehungen: $d^i, i = 0,\ldots,19$ Drehung um $\frac{2\pi\cdot i}{20}$.
   $t(d^0) = x_1^{20}$ Identität
   $t(d^i) = x_{20}^1$, für alle i mit $\mathrm{ggT}(i,20) = 1$ ($\varphi(20) = 8$)

   $$\begin{array}{lllllllll} t(d^2) & = & t(d^6) & = & t(d^{14}) & = & t(d^{18}) & = & x_{10}^2 \\ t(d^4) & = & t(d^8) & = & t(d^{12}) & = & t(d^{16}) & = & x_5^4 \\ t(d^5) & = & t(d^{15}) & & & & & = & x_4^5 \\ t(d^{10}) & & & & & & & = & x_2^{10} \end{array}$$

   - Spiegelungen s durch gegenüberliegende Seitenmitten, $t(s) = x_2^{10}$ (10-mal)
   - Spiegelungen $\tilde{s}$ durch gegenüberliegende Ecken (Perlen), $t(\tilde{s}) = x_1^2x_2^9$ (10-mal)

   $$Z_G(x_1,\ldots,x_{20}) = \tfrac{1}{40}(x_1^{20} + 10x_1^2x_2^9 + 11x_2^{10} + 2x_4^5 + 4x_5^4 + 4x_{10}^2 + 8x_{20}^1)$$

   Nach 5.16 ist die gesuchte Anzahl der Koeffizient von $f_1^2f_2^9f_3^9$ in

   $$\frac{1}{40}\big((f_1+f_2+f_3)^{20}+10(f_1+f_2+f_3)^2(f_1^2+f_2^2+f_3^2)^9+11(f_1^2+f_2^2+f_3^2)^{10} +2(f_1^4+f_2^4+f_3^4)^5+4(f_1^5+f_2^5+f_3^5)^4+4(f_1^{10}+f_2^{10}+f_3^{10})^2+8(f_1^{20}+f_2^{20}+f_3^{20})\big)$$

   $$(f_1+f_2+f_3)^{20} = \tbinom{20}{2}\tbinom{18}{9}f_1^2f_2^9f_3^9 + \cdots$$

   $$10(f_1+f_2+f_3)^2(f_1^2+f_2^2+f_3^2)^9 = 10\cdot \underbrace{2}_{\substack{f_2f_3\\ \text{1. Faktor}}} \cdot \underbrace{9\cdot\underbrace{\binom{8}{4}}_{f_2^8f_3^8}}_{\substack{f_1^2\\ \text{2.Faktor}}} f_1^2f_2^9f_3^9 + \cdots$$

   Rest liefert kein Monom $f_1^2f_2^9f_3^9$.

   $$\frac{1}{40}\left(\binom{20}{2}\cdot\binom{18}{9} + 180\cdot\binom{8}{4}\right) = 231260$$

   Der gesamte Ausdruck $Z_G(f_1+f_2+f_3,\ldots,f_1^{20}+f_2^{20}+f_3^{20})$ ist zu finden in: Harris, Hirst, Mossinghoff: Combinatorics and Graph Theory; Springer, 2000, Seite 136.

2. Naphtalin $C_{10}H_8$

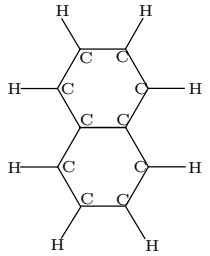


Abbildung 1: Naphtalin

Dihydroxynaphtalin entsteht aus Naphtalin durch Ersetzen von zwei H-Atomen durch jeweils eine OH-Gruppe. Wieviele Isomere (gleiche Atom-Anzahlen, unterschiedliche Anordnung) bzgl $G = \{id, d_{180}, s_1, s_2\}$ gibt es? (s_1, s_2 Spiegelungen an horizontaler bzw. vertikaler Achse)

$$\begin{array}{lllll} n=8 & t(id) & = & x_1^8 & \\ & t(d) & = & x_2^4 & \qquad Z_G = \frac{1}{4}(x_1^8 + 3x_2^4) \\ & t(s_1) & = & x_2^4 & = \quad t(s_2) \end{array}$$

$f_1 = H:$ 6 mal, $f_2 = OH:$ 2 mal

Anzahl: Koeffizient von $f_1^6 f_2^2$ in $\frac{1}{4}\left((f_1+f_2)^8 + 3(f_1^2+f_2^2)^4\right)$
Anzahl $\frac{1}{4}\left(\binom{8}{2} + 3 \cdot 4\right) = \frac{1}{4}(28+12) = 10$

Es gibt 10 Isomere mit 2 OH-Gruppen und 6 H-Atomen.

3. Anzahl der unmarkierten ungerichteten Graphen mit $n = 5$ Ecken

$E = \{1, \ldots, 5\}$,
$\Omega =$ Menge der 2-elementigen Teilmengen von E.
Färbungen von Ω mit zwei Farben f_1 und f_2:
Färbung von $\{a, b\} \in \Omega$ mit f_1 bedeutet: a und b sind durch eine Kante verbunden;
Färbung von $\{a, b\} \in \Omega$ mit f_2 bedeutet: a und b sind durch keine Kante verbunden.

Zu bestimmen ist die Anzahl der Bahnen von $G = S_5$ auf der Menge der Färbungen von Ω.

1.Schritt: Bestimmung aller Elemente von S_5

Wir beschreiben die Elemente von S_5 in ihrer Zyklendarstellung bezüglich der natürlichen Operation auf $E = \{1, \ldots, 5\}$:

(I)	24	=	$4 \cdot 3 \cdot 2$	5-er-Zyklen
(II)	30	=	$5 \cdot (3 \cdot 2)$	4-er-Zyklen
(III)	20	=	$\binom{5}{3} \cdot 2$	3-er-Zyklen
(IV)	10	=	$\binom{5}{2}$	2-er-Zyklen
(V)	15	=	$5 \cdot 3$	Produkte zweier disjunkter 2-er-Zyklen
(VI)	20	=	$\binom{5}{3} \cdot 2$	Produkte disjunkter 3-er- und 2-er-Zyklen
(VII)	1			Identität

Insgesamt $120 = 5!$ Elemente.

2.Schritt: Bestimmung der Zyklenzerlegung der Elemente von S_5 bezüglich ihrer Operation auf Ω

(I) $g = (abcde)$ hat zwei 5-er-Zyklen auf Ω
$(\{a,b\}\{b,c\}\{c,d\}\{d,e\}\{e,a\}) \quad (\{a,c\}\{b,d\}\{c,e\}\{d,a\}\{e,b\})$
Permutationstyp auf Ω:
$t(g) = x_5^2$

(II) $g = (abcd)$ hat einen 2-er-Zyklus auf Ω
$(\{a,c\}\{b,d\})$
und zwei 4-er-Zyklen
$(\{a,b\}\{b,c\}\{c,d\}\{d,a\}) \quad (\{a,e\}\{b,e\}\{c,e\}\{d,e\})$
Permutationstyp auf Ω:
$t(g) = x_2 x_4^2$

(III) $g = (abc)$ hat einen 1-er-Zyklus auf Ω
$(\{d,e\})$
und drei 3-er-Zyklen
$(\{a,b\}\{b,c\}\{c,a\}) \quad (\{a,d\}\{b,d\}\{c,d\}) \quad (\{a,e\}\{b,e\}\{c,e\})$
Permutationstyp auf Ω:
$t(g) = x_1 x_3^3$

(IV) $g = (ab)$ hat vier 1-er-Zyklen auf Ω
$(\{a,b\}) \quad (\{c,d\}) \quad (\{c,e\}) \quad (\{d,e\})$
und drei 2-er-Zyklen
$(\{a,c\}\{b,c\}) \quad (\{a,d\}\{b,d\}) \quad (\{a,e\}\{b,e\})$
Permutationstyp auf Ω:
$t(g) = x_1^4 x_2^3$

(V) $g = (ab)(cd)$ hat zwei 1-er-Zyklen auf Ω
$(\{a,b\}) \quad (\{c,d\})$
und vier 2-er-Zyklen
$(\{a,c\}\{b,d\}) \quad (\{a,d\}\{b,c\}) \quad (\{a,e\}\{b,e\}) \quad (\{c,e\}\{d,e\})$
Permutationstyp auf Ω:
$t(g) = x_1^2 x_2^4$

(VI) $g = (abc)(de)$ hat einen 1-er-Zyklus auf Ω
$(\{d,e\})$
einen 3-er-Zyklus
$(\{a,b\}\{b,c\}\{c,a\})$
und einen 6-er-Zyklus
$(\{a,d\}\{b,e\}\{c,d\}\{a,e\}\{b,d\}\{c,e\})$
Permutationstyp auf Ω:
$t(g) = x_1 x_3 x_6$

(VII) $g = id$
Permutationstyp auf Ω:
$t(g) = x_1^{10}$

3.Schritt: Bestimmung des Zyklenzeigers von S_5 auf Ω

$z_{S_5}(x_1, \ldots, x_{10}) =$
$\frac{1}{120}(x_1^{10} + 10x_1^4x_2^3 + 15x_1^2x_2^4 + 20x_1x_3^3 + 20x_1x_3x_6 + 30x_2x_4^2 + 24x_5^2)$

4.Schritt: Anzahlbestimmungen

a) Anzahl aller unmarkierten Graphen mit 5 Ecken

Diese Anzahl ist nach 5.13
$z_{S_5}(2, \ldots, 2) =$
$\frac{1}{120}(2^{10} + 10 \cdot 2^7 + 15 \cdot 2^6 + 20 \cdot 2^4 + 20 \cdot 2^3 + 30 \cdot 2^3 + 24 \cdot 2^2) = 34$

Zum Vergleich: Es gibt $2^{10} = 1024$ markierte Graphen mit 5 Ecken.

b) Anzahl aller unmarkierten Graphen mit 5 Ecken und 4 Kanten

Diese Anzahl ist nach dem Satz von Pólya (5.16) der Koeffizient von $f_1^4 \cdot f_2^6$ in $z_{S_5}(f_1 + f_2, \ldots, f_1^{10} + f_2^{10})$.

$$\begin{aligned}
(f_1 + f_2)^{10} &= \tbinom{10}{4} f_1^4 f_2^6 + \ldots \\
10(f_1 + f_2)^4(f_1^2 + f_2^2)^3 &= 10 \cdot (1 + \tbinom{4}{2} \cdot 3 + 3) f_1^4 f_2^6 + \ldots \\
15(f_1 + f_2)^2(f_1^2 + f_2^2)^4 &= 15 \cdot (\tbinom{4}{2} + 4) f_1^4 f_2^6 + \ldots \\
20(f_1 + f_2)(f_1^3 + f_2^3)^3 &= 20 \cdot 3 \cdot f_1^4 f_2^6 + \ldots \\
20(f_1 + f_2)(f_1^3 + f_2^3)(f_1^6 + f_2^6) &= 20 f_1^4 f_2^6 + \ldots \\
30(f_1^2 + f_2^2)(f_1^4 + f_2^4)^2 &= 30 \cdot 2 \cdot f_1^4 f_2^6 + \ldots
\end{aligned}$$

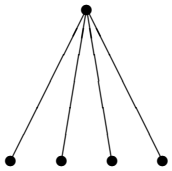
$24(f_1^5 + f_2^5)^2$ liefert kein Monom $f_1^4 f_2^6$.

Damit erhält man $\frac{1}{120}(210 + 220 + 150 + 60 + 20 + 60) = 6$ unmarkierte Graphen mit 5 Ecken und 4 Kanten.

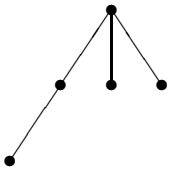
Zum Vergleich: Es gibt $\binom{10}{4} = 210$ markierte Graphen mit 5 Ecken und 4 Kanten.

Die sechs verschiedenen unmarkierten Graphen mit 5 Ecken und 4 Kanten:

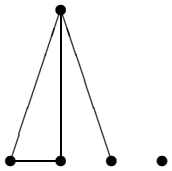
1)



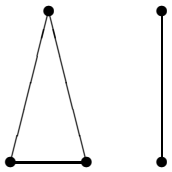
2)



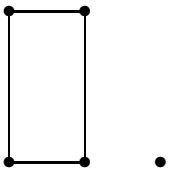
3)



4)



5)



6)

6 Ringe und Körper

6.1 Definition

- Eine Menge R mit 2 Verknüpfungen $+, \cdot$ heißt *Ring*, falls gilt:

  i) $(R, +, 0)$ ist kommutative Gruppe

  ii) $(R, \cdot)$ ist Halbgruppe

  iii) $a(b+c) = ab + ac$ und $(a+b)c = ac + bc$ für alle $a, b, c \in R$

- Ist R Ring mit Element $1 \neq 0$, so dass $(R, \cdot, 1)$ ein Monoid ist, so heißt R *Ring mit Eins*.

- Ist $(R, \cdot)$ kommutativ, so heißt R *kommutativer Ring*.

6.2 Bemerkung

Sei R ein Ring.
$0a = a0 = 0,\ (-a)b = -(ab) = a(-b)\ \forall\ a, b \in R$

6.3 Beispiele

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ kommutative Ringe mit Eins.

2. $\mathbb{Z}_n$ kommutativer Ring mit Eins bzgl. $\oplus$ und $\odot$.

3. Sei R kommutativer Ring mit 1.
   $R[x] = \{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}_0, a_i \in R\}$ Polynomring
   Addition komponentenweise
   Mutliplikation: $(\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j) = \sum_{k=0}^{n+m} c_k x^k$, dabei $c_k = \sum_{i+j=k} a_i b_j$ (distributiv ausmultiplizieren)

4. $R = \mathrm{Mat}(n, \mathbb{R})$ bzw. $\mathrm{Hom}_{\mathbb{R}}(V, V)$ (V n-dimensionaler $\mathbb{R}$-Vektorraum) ist ein nicht-kommutativer Ring für $n \geq 2$.

6.4 Definition

Sei R Ring mit 1.
$x \in R$ heißt *Einheit*, falls $y \in R$ existiert mit $xy = yx = 1$ ($y = x^{-1}$). Die Menge der Einheiten bildet bzgl. $\cdot$ eine Gruppe R^*. (0 ist nie Einheit.)

6.5 Beispiel

1. $\mathbb{Z}^* = \{1, -1\},\ \mathbb{Q}^* = \mathbb{Q} \setminus \{0\},\ \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

2. $\mathbb{Z}_n^* = \{i \mid 0 \leq i < n, \mathrm{ggT}(i, n) = 1\}$ (3.32)

3. $(\mathrm{Mat}(n, \mathbb{R}))^* = GL(n, \mathbb{R})$, $\mathrm{Hom}_{\mathbb{R}}(V, V)^* = GL(V)$

6.6 Definition

Sei R ein kommutativer Ringe mit Eins.
R heißt *Körper*, falls $R^* = R \setminus \{0\}$

6.7 Beispiele

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper
2. $\mathbb{Z}_n$ ist Körper $\Leftrightarrow$ n ist Primzahl.

6.8 Definition

Sei R ein Ring. $U \subseteq R$ heißt *Unterring*, falls U bezüglich der Verknüpfungen in R ein Ring ist.
(Beachte: Unterringe von Ringen mit Eins brauchen keine Eins zu besitzen. Bsp: $2\mathbb{Z}$ ist Unterring von $\mathbb{Z}$)

Frage nach Faktorringen:
Gebildet aus den Nebenklassen von Untergruppen I von $(R, +)$, bzgl. derer sich die Multiplikation vertreterweise definieren lässt.
Wir wollen definieren: $(a + I) \odot (b + I) := ab + I \ \ \forall a, b \in R$

Notwendig und hinreichend für die Wohldefiniertheit dieser Multiplikation ist:

$$(*) \quad \left.\begin{array}{rcl} a - a' & \in & I \\ b - b' & \in & I \end{array}\right\} \Rightarrow ab - a'b' \in I \ \ \forall a, b \in R.$$

6.9 Proposition und Definition

Sei R ein Ring, I Untergruppe von $(R, +)$.
Genau dann gilt $(*)$, wenn I folgende Eigenschaft besitzt:

Für alle $i \in I$ und alle $a \in R$ gilt: $ai \in I$ und $ia \in I$.

Ein solches I heißt *Ideal* von R.
(Beachte: Ideale sind Unterringe)

Beweis. Es gelte $(*)$. Sei $a \in R, \ i \in I$.
Dann: $a - a \in I, i - 0 \in I \overset{(*)}{\Rightarrow} ai \in I$ (analog $ia \in I$)
Also ist I Ideal.

Umgekehrt sei I Ideal. Wir zeigen $(*)$.
Sei dazu $a, a', b, b' \in R, \ a - a' \in I, \ b - b' \in I$.
$ab - a'b' = (a - a')b + a'(b - b') \in I$. □

6.10 Definition

Sei R ein Ring, I Ideal in R.
Dann wird $R/I = \{a + I \mid a \in R\}$ ein Ring bzgl. der Verknüpfungen

$$\begin{array}{rcccl} (a+I) & + & (b+I) & := & (a+b) \quad + \quad I \\ (a+I) & \cdot & (b+I) & := & \quad ab \quad\ + \quad I \end{array}$$

R/I heißt *Faktorring* von R nach I.
R kommutativ $\Rightarrow$ R/I kommutativ
R mit Eins $\Rightarrow$ R/I mit Eins: $1 + I$

6.11 Beispiele

1. $n\mathbb{Z}$ ist Ideal von $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Dies sind sämtliche Ideale, da dies schon sämtliche Untergruppen von $(\mathbb{Z}, +)$ sind (vgl. 3.7).

2. Körper K besitzen nur die trivialen Ideale $\{0\}$ und K:
   $I \neq \{0\}$ Ideal, $0 \neq i \in I \Rightarrow 1 = ii^{-1} \in I \Rightarrow a = a \cdot 1 \in I \; \forall a \in K$.
   Also $I = K$.

6.12 Definition

1. Seine R, R' Ringe.
   $\varphi : R \to R'$ heißt *Ringhomomorphismus*, falls $\varphi(a + b) = \varphi(a) + \varphi(b)$ und $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ $\forall a, b \in R$.
   (Bijektiver Ringhomomorphismus heißt (Ring-)Isomorphismus, $R \cong R'$.)

2. Sei R ein kommutativer Ring mit Eins, $a \in R$. Dann ist $aR = \{ar | r \in R\}$ ein Ideal in R, und zwar das eindeutig bestimmte kleinste Ideal von R, das a enthält.
   Jedes Ideal von der Form aR heißt *Hauptideal* von R.

6.13 Satz

Seien R, R' Ringe, $\varphi : R \to R'$ ein Ringhomomorphismus.

1. Ist φ ein Isomorphismus, so ist $\varphi^{-1} : R' \to R$ ein Isomorphismus

2. Kern$\varphi = \{a \in R \mid \varphi(a) = 0\}$ ist Ideal in R, $\varphi(R)$ Unterring von R'.

3. φ injektiv $\Leftrightarrow$ Kern$\varphi = \{0\}$

4. (Homomorphiesatz) $R/\text{Kern}\varphi \cong \varphi(R)$.

5. Ist I Ideal in R, so ist $\Psi : \left\{ \begin{array}{ccc} R & \to & R/I \\ a & \mapsto & a + I \end{array} \right.$ ein surjektiver Ringehomomorphismus, Kern $\Psi = I$

Also: Ideale von R sind genau die Kerne von Ringhomomorphismen $R \to R'$

Nach 6.11.1 sind alle Ideale von $\mathbb{Z}$ Hauptideale. Dies beruhte im Wesentlichen darauf (vgl. 3.7), dass es in $\mathbb{Z}$ eine Division mit Rest gibt. Auf dieselbe Weise kann man zeigen, dass für jeden Körper K im Polynomring $K[x]$ jedes Ideal ein Hauptideal ist. Dazu benötigen wir:

6.14 Definition

Sei K ein Körper. Ist $f \in K[x], f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$, so ist n der *Grad* von f.
Bezeichung: $\text{grad} f = n$
$\text{grad } 0 := -\infty$

6.15 Satz

Sei K ein Körper.

1. Sind $f, g \in K[x]$, so ist $\text{grad}(fg) = \text{grad } f + \text{grad } g$.
2. Sind $f, g \in K[x], g \neq 0$. Dann gibt es eindeutig bestimmte $s, r \in K[x]$ mit $f = sg + r$ und $\text{grad } r < \text{grad } g$ (Division mit Rest)

Statt Beweis ein Beispiel:

6.16 Beispiel

$f = x^4 + 2x^3 - x + 1,\ g = 3x^2 + 2\ \in \mathbb{Q}[x]$.

$$
\begin{array}{rrrrrrrrrrrrrrr}
x^4 & + & 2x^3 & & & - & x & + & 1 & : & 3x^2+2 & = & \frac{1}{3}x^2 + \frac{2}{3}x - \frac{2}{9} \\
\cline{1-1}\cline{11-11}
\frac{1}{3}x^4 & & & + & \frac{2}{3}x^2 & & & & & & & & \\
\cline{1-5}
 & & 2x^3 & - & \frac{2}{3}x^2 & - & x & + & 1 & & & & \\
 & & 2x^3 & & & + & \frac{4}{3}x & & & & & & \\
\cline{3-7}
 & & & - & \frac{2}{3}x^2 & - & \frac{7}{3}x & + & 1 & & & & \\
 & & & - & \frac{2}{3}x^2 & & & - & \frac{4}{9} & & & & \\
\cline{4-9}
 & & & & & - & \frac{7}{3}x & + & \frac{13}{9} & & & &
\end{array}
$$

Also: $f = \underbrace{\left(\frac{1}{3}x^2 + \frac{2}{3}x - \frac{2}{9}\right)}_{s} \cdot g + \underbrace{\left(-\frac{7}{3}x + \frac{13}{9}\right)}_{r}$

6.17 Folgerung

Sei K Körper.

1. $f \in K[x]$. f Einheit $\Leftrightarrow \text{grad } f = 0$
2. Sind $f, g \in K[x] \setminus \{0\}$, so ist $f \cdot g \neq 0$
3. Jedes Ideal in $K[x]$ ist ein Hauptideal.

Beweis. 1. folgt aus 6.15.1

2. folgt aus 6.15.1
3. Sei $I \neq \{0\}$ Ideal in $K[x]$. Sei $0 \neq g \in I$ von minimalem Grad.
   Klar: $g \cdot K[x] \subseteq I$.
   Sei $f \in I$. Nach 6.15.2: $f = sg + r,\ \text{grad } r < \text{grad } g$.
   $r = f - sg \in I$. Wahl von f: $r = 0, f = s \cdot g \in gK[x], I = gK[x]$.

□

(In $\mathbb{Z}[x]$ gilt 3. nicht!)

6.18 Definition

Sei K ein Körper, $f, g \in K[x]$.
f heißt *Teiler* von g ($f|g$), falls $s \in K[x]$ existiert mit $f \cdot s = g$. (Dies geht in jedem kommutativen Ring.)
($gK[x] \subseteq fK[x] \Leftrightarrow f \mid g$)

6.19 Bemerkung und Definition

1. $f \mid g,\ a \in K \setminus \{0\}$, so $af \mid g$.
   Man kann einen Teiler normieren:
   $f \in K[x]$ heißt *normiert*, falls $f \neq 0$ und der höchste Koeffizient von f gleich 1 ist.

2. $f \mid g,\ g \neq 0$, so grad $f \leq$ grad g (6.15.1)

6.20 Definition

Sei K ein Körper, $g, h \in K[x]$, nicht beide gleich 0.
$f \in K[x]$ heißt *größter gemeinsamer Teiler* von g und h, falls f normiertes Polynom von maximalem Grad, das g und h teilt.

Klar: Ein größter gemeinsamer Teiler existiert; unklar an dieser Stelle ist allerdings, ob er eindeutig ist. Dies folgt aus folgendem Satz:

6.21 Satz von Bezout

Sei K ein Körper, $g, h \in K[x]$, nicht beide gleich 0.
Ist f ein größter gemeinsamer Teiler von g und h, so existieren $s, t \in K[x]$ mit $f = sg + th$. f ist eindeutig bestimmt.

Beweis. $gK[x] \subseteq fK[x],\ hK[x] \subseteq fK[x]$; also $gK[x] + hK[x] \subseteq fK[x]$.
$gK[x] + hK[x]$ ist Ideal, also existiert ein $d \in K[x]$ mit $gK[x] + hK[x] = dK[x]$ (6.17.3)
OBdA d normiert. ($d \neq 0$, da g, h nicht beide 0)
Also: $dK[x] \subseteq fK[x],\ f \mid d$.
Umgekehrt: Es ist $d = sg + th, s, t \in K[x]$. $f \mid g, h$, d.h. $f \mid sg + th = d$.
$f \mid d$ und $d \mid f$, beide haben höchsten Koeffizient 1. Also $f = d$. Damit ist f eindeutig bestimmt. □

Bezeichnung: $f = \mathrm{ggT}(g, h)$ für den größten gemeinsamen Teiler f von g und h.

Wie bestimmt man $\mathrm{ggT}(g, h)$ und $s, t \in K[x]$ mit $\mathrm{ggT}(g, h) = sg + th$?
Euklidischer Algorithmus/ Erweiterter Euklidischer Algorithmus entsprechend der Vorgehensweise in $\mathbb{Z}$.

Dazu Bezeichnung

1. $f = sg + r$, grad $r <$ grad g Division mit Rest
   $s = f$ div g $r = f$ mod g

2. Ist $f = a_n x^n + \cdots + a_0,\ a_n \neq 0$, so ist $\widetilde{f} = x^n + a_n^{-1} a_{n-1} x^{n-1} + \cdots + a_n^{-1} a_0$ das zugehörige normierte Polynom.

6.22 Größter gemeinsamer Teiler in $K[x]$

a) Euklidischer Algorithmus

Da $\mathrm{ggT}(f,0) = \tilde{f}$ für $f \neq 0$, genügt es, den Fall $f \neq 0 \neq g$ zu betrachten.

Eingabe: $f, g \in K[x],\ f \neq 0 \neq g$

$y := f$
$z := g$
Wiederhole, solange $y \bmod z \neq 0$
$r := y \bmod z, \quad y := z, \quad z := r;$

Ausgabe: $\tilde{z} \quad (= \mathrm{ggT}(f,g))$

Gültigkeit des Euklidischen Algorithmus:

$y = sz + r$
$\mathrm{ggT}(y,z) = \mathrm{ggT}(sz+r,z) = \mathrm{ggT}(z,r)$
Ist $r = 0$, so $\mathrm{ggT}(y,z) = \mathrm{ggT}(z,0) = \tilde{z}$

Beispiel

$f = x^4 - 3x^3 + 3x^2 - 3x + 2,\ g = x^3 + 2x^2 - x - 2 \in \mathbb{Q}[x]$

$y = f,\ z = g;$
$y = (x-5)\cdot z + (14x^2 - 6x - 8)$
$r = 14x^2 - 6x - 8,\ y = x^3 + 2x^2 - x - 2,\ z = 14x^2 - 6x - 8$
$y = (\frac{1}{14}x + \frac{17}{98})\cdot z + (\frac{30}{49}x - \frac{30}{49})$
$r = \frac{30}{49}x + \frac{30}{49},\ y = 14x^2 - 6x - 8,\ z = \frac{30}{49}x - \frac{30}{49}$
$y = (\frac{343}{15}x + \frac{196}{15})\cdot z$
$r = 0$

Ausgabe: $\tilde{z} = x - 1 = \mathrm{ggT}(f,g)$

b) Erweiterter Euklidischer Algorithmus

Wie bestimmt man $u, v \in K[x]$ mit $\mathrm{ggT}(f,g) = uf + vg$?

Es genügt wieder, den Fall $f \neq 0 \neq g$ zu betrachten. Der erweiterte Euklidische Algorithmus läuft wie bei ganzen Zahlen ab, und seine Korrektheit beweist man wie in 3.31.

Eingabe: $f, g \in K[x],\ f \neq 0,\ g \neq 0$

$u_1 := 1,\ u_2 := 0,\ u := 0$
$v_1 := 0,\ v_2 := 1,\ v := 1$
$y := f,\ z := g$

Wiederhole, solange $y \bmod z \neq 0$

$s := y \operatorname{div} z$ $\qquad r := y \bmod z,$
$u := u_1 - su_2$ $\qquad v := v_1 - sv_2,$
$u_1 := u_2,\ u_2 := u,$ $\qquad v_1 := v_2,\ v_2 := v,$
$y := z,\ z := r$

Ausgabe: $\tilde{z} \quad (= \mathrm{ggT}(f, g))$
Ist $\tilde{z} = a \cdot z$, setze $\tilde{u} = a \cdot u,\ \tilde{v} = a \cdot v$
$\tilde{u}, \tilde{v} \quad (\tilde{z} = \tilde{u}f + \tilde{v}g).$

Beispiele

1) $\quad f = x^4 - 3x^3 + 3x^2 - 3x + 2, \quad g = x^3 + 2x^2 - x - 2 \in \mathbb{Q}[x]$

$u_1 = 1,\ u_2 = 0,\ u = 0$
$v_1 = 0,\ v_2 = 1,\ v = 1$
$y = f,\ z = g$

$y \bmod z = 14x^2 - 6x - 8, \quad y \operatorname{div} z = x - 5$
$s = x - 5,\ r = 14x^2 - 6x - 8$
$u = 1 - (x - 5) \cdot 0 = 1,\ v = 0 - (x - 5) \cdot 1 = -x + 5$
$u_1 = 0,\ u_2 = 1,\ v_1 = 1,\ v_2 = -x + 5$
$y = x^3 + 2x^2 - x - 2, \quad z = 14x^2 - 6x - 8$

$y \bmod z = \frac{30}{49}x - \frac{30}{49}, \quad y \operatorname{div} z = \frac{1}{14}x + \frac{17}{98}$
$s = \frac{1}{14}x + \frac{17}{98}, \quad r = \frac{30}{49}x - \frac{30}{49}$
$u = 0 - (\frac{1}{14}x + \frac{17}{98}) \cdot 1 = -\frac{1}{14}x - \frac{17}{98}$
$v = 1 - (\frac{1}{14}x + \frac{17}{98})(-x + 5) = \frac{1}{14}x^2 - \frac{9}{49}x + \frac{13}{98}$
$u_1 = 1, u_2 = -\frac{1}{14}x - \frac{17}{98},\ v_1 = -x + 5,\ v_2 = \frac{1}{14}x^2 - \frac{9}{49}x + \frac{13}{98}$
$y = 14x^2 - 6x - 8, \quad z = \frac{30}{49}x - \frac{30}{49}$
$y \bmod z = 0$

Ausgabe:
$\tilde{z} = x - 1 = \mathrm{ggT}(f, g) \qquad (\tilde{z} = \frac{49}{30}z)$

$\tilde{u} = \frac{49}{30}(-\frac{1}{14}x - \frac{17}{98}) = -\frac{7}{60}x - \frac{17}{60}$
$\tilde{v} = \frac{49}{30}(\frac{1}{14}x^2 - \frac{9}{49}x + \frac{13}{98}) = \frac{7}{60}x^2 - \frac{3}{10}x + \frac{13}{60}$

$(x - 1 = (-\frac{7}{60}x - \frac{17}{60})f + (\frac{7}{60}x^2 - \frac{3}{10}x + \frac{13}{60})g)$

2) $\quad f = x^4 + x^3 + x, \quad g = x^3 + x + 1 \in \mathbb{Z}_2[x]$

$u_1 = 1,\ u_2 = 0,\ u = 0$
$v_1 = 0,\ v_2 = 1,\ v = 1$
$y = f,\ z = g$

$y \bmod z = x^2 + x + 1, \quad y \operatorname{div} z = x + 1$
$s = x + 1,\ r = x^2 + x + 1$
$u = 1 - (x + 1) \cdot 0 = 1,\ v = 0 - (x + 1) \cdot 1 = x + 1$

$u_1 = 0,\ u_2 = 1,\ v_1 = 1,\ v_2 = x + 1$
$y = x^3 + x + 1, \quad z = x^2 + x + 1$

$y \bmod z = x, \quad y \operatorname{div} z = x + 1$
$s = x + 1,\ r = x$
$u = 0 - (x + 1) \cdot 1 = x + 1,\ v = 1 - (x + 1) \cdot (x + 1) = x^2$
$u_1 = 1,\ u_2 = x + 1,\ v_1 = x + 1,\ v_2 = x^2$
$y = x^2 + x + 1, \quad z = x$

$y \bmod z = 1, \quad y \operatorname{div} z = x + 1$
$s = x + 1,\ r = 1$
$u = 1 - (x + 1) \cdot (x + 1) = x^2,\ v = x + 1 - (x + 1) \cdot x^2 = x^3 + x^2 + x + 1$
$u_1 = x + 1,\ u_2 = x^2,\ v_1 = x^2,\ v_2 = x^3 + x^2 + x + 1$
$y = x, \quad z = 1$
$y \bmod z = 0$

Ausgabe:
$z = 1 = \mathrm{ggT}(f, g)$
$u = x^2, \quad v = x^3 + x^2 + x + 1$

$(1 = x^2 \cdot f + (x^3 + x^2 + x + 1) \cdot g)$

6.23 Satz

Sei $f \in K[x], \operatorname{grad} f = n$.

1. Es ist $K[x]/fK[x] = \{g + fK[x] : \operatorname{grad} g < n\}$ und die $g + fK[x]$, $\operatorname{grad} g < n$, sind paarweise verschieden.

2. Setze $K[x]_n = \{g \in K[x] : \operatorname{grad} g < n\}$.
   Definiere Addition $\oplus$ auf $K[x]_n$ wie Addition $+$ in $K[x]$ und Multiplikation $\odot_f$ auf $K[x]_n$ durch

   $$g_1 \odot_f g_2 := g_1 \cdot g_2 \mod f \quad \text{(Multiplikation hängt von } f \text{ ab!)}$$

   Dann ist $K[x]_n$ ein Ring, $K[x] \cong K[x]/fK[x]$.

3. Es ist $K[x]_n^* = \{g \in K[x] : \operatorname{grad} g < n,\ \mathrm{ggT}(g, f) = 1\}$. (Also auch $(K[x]/fK[x])^* = \{g + fK[x] : \mathrm{ggT}(g, f) = 1\}$)

Beweis. 1. klar

2. klar

3. beweist man auf Grund des Satzes von Bezout (erweiterter Euklidischer Algorithmus) wie in $\mathbb{Z}_n$ (3.32).

□

6.24 Bemerkung

Das Inverse von $g \in K[x]_n$ bezüglich $\odot_f$ bestimmt man mit dem Erweiterten Euklidischen Algorithmus. $\mathrm{ggT}(f, g) = 1 \Rightarrow \exists u, v \in K[x]$ mit $uf + vg = 1$.

Es ist $g^{-1} = v \bmod f \in K[x]_n$:
$(v + fK[x])(g + fK[x]) = (1 - fu) + fK[x]$, also $(v \bmod f) \odot_f g = 1$.

Beispiel: $f = x^4 + x^3 + 1 \in \mathbb{Z}_2[x],\ g = x^3 + x + 1$
$g^{-1} = x^3 + x^2 + x + 1$ in $\mathbb{Z}_2[x]_4$ bzgl. $\odot_f$. (6.22)

6.25 Definition

Ein Polynom $f \in K[x]$ heißt *irreduzibel*, falls gilt:

$$\text{Ist } g \mid f, \text{ so grad } g = 0 \text{ oder } g = af \text{ für ein } a \in K \setminus \{0\}.$$

6.26 Korollar

$K[x]/fK[x]$ ist Körper $\Leftrightarrow$ f ist irreduzibel.

6.26 liefert eine neue Möglichkeit, endliche Körper zu konstruieren.

Bisher kennen wir die $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$, p Primzahl.

6.27 Bemerkung

Sei $K \subseteq L$ Körper. Dann ist L ein K-Vektorraum.

6.28 Satz

Ist K ein endlicher Körper, so gibt es eine Primzahl p und ein $a \in \mathbb{N}$ mit $|K| = p^a$. Es gilt dann $p \cdot 1 = \underbrace{1 + \cdots + 1}_{p} = 0$.

Beweis. Setze $K_0 = \{n \cdot 1 : n \in \mathbb{N}_0\}$, wobei $n \cdot 1 = \begin{cases} 0, & \text{für } n = 0 \\ \underbrace{1 + \cdots + 1}_{n}, & n > 0 \end{cases}$
Klar: K_0 ist kommutativer Ring mit Eins, $K_0 \subseteq K$.
Da K_0 endlich ist, existiert ein minimales $m > 0$ mit $m \cdot 1 = 0$ (m = Ordnung von 1 in $(K, +)$.)
Ist $m = b \cdot c, 1 < b, c < m$, so $(b \cdot 1) \cdot (c \cdot 1) = 0$; da K Körper, ist $b \cdot 1 = 0$ oder $c \cdot 1 = 0$. Also ist $m = p$ eine Primzahl.
Nun sieht man sofort, dass $K_0 \cong \mathbb{Z}_p$ ein Körper ist. Nach 6.27 ist K ein K_0-Vektorraum endlicher Dimension a. Also: $|K| = p^a$. □

6.29 Korollar

Sei K ein endlicher Körper, $|K| = p^a$, p Primzahl.

1. $o(k) = p$ für alle $k \in (K, +), k \neq 0$, d.h. $p \cdot k = \underbrace{k + \cdots + k}_{p} = 0$.

2. $(k + l)^p = k^p + l^p \quad \forall k, l \in K$

Beweis. 1. $p \cdot k = (p \cdot 1) \cdot k = 0$ nach 6.28

2. $(k+l)^p = \sum_{i=0}^{p} \binom{p}{i} k^i l^{p-i} \quad (k^0 = l^0 = 1)$.
   Ist $1 \leq i \leq p-1$, so $p \mid \binom{p}{i} = \frac{p \cdot \ldots \cdot (p-i+1)}{i!}$. Daher $\binom{p}{i} k^i l^{p-i} = 0$ nach 1. □

6.30 Satz

Ist $f \in \mathbb{Z}_p[x]$ ein irreduzibles Polynom vom Grad a, so ist $K = \mathbb{Z}_p[x]/f\mathbb{Z}_p[x] \cong (\mathbb{Z}_p[x]_a, \oplus, \odot_f)$ ein Körper und $|K| = p^a$.

Beweis. Folgt direkt aus 6.23. □

Beachte: Es gibt genau p^a viele Polynome in $\mathbb{Z}_p[x]$ vom Grad $< a$.

6.31 Beispiel

$f = x^2 + x + 1$ irreduzibel vom Grad 2 über $\mathbb{F}_2$.
$K = \mathbb{F}_2[x]/f \cdot \mathbb{F}_2[x] \cong \mathbb{F}_2[x]_2$ Körper der Ordnung 4.
$K = \{0, 1, x, x+1\}$

$\odot$	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

$\oplus$	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

Beachte: $K^* = \{1 = x^0, x = x^1, x^2 = x+1\}$

6.32 Eigenschaften endlicher Körper

1. Ist p Primzahl, $a \in \mathbb{N}$, so existiert ein irreduzibles Polyom vom Grad a über $\mathbb{F}_p$.
   Also gibt es einen Körper der Ordnung p^a.

2. Sind K_1, K_2 endliche Körper gleicher Ordnung, so sind sie isomorph.

3. Ist K ein endlicher Körper, so ist K^* zyklisch. (Ein erzeugendes Element von K^* heißt *primitives* Element von K. Ist $K = \mathbb{Z}_p$, so *Primitivwurzel mod p.*)

(Beweise: Z.B. Lidl, Niederreiter: Introduction to Finite Fields and their Applications.)

7 Anwendungen: Codes und kryptographische Verschlüsselungen

7.A Codes Lineare Codes hatten wir schon in 1.8 betrachtet.

7.1 Polynomcodierung

Sei $k < n$, q Primzahlpotenz, K ein Körper mit $|K| = q$.
Nachrichten, Daten seien Elemente aus K^k.
Codiere $m = \begin{pmatrix} m_0 \\ \vdots \\ m_{k-1} \end{pmatrix} \in K^k$ auf folgende Weise:

1. Identifiziere m mit $m(x) = m_0 + m_1 x + \cdots + m_{k-1}x^{k-1} \in (K[x])_k$. Diese Zuordnung ist ein Vektorraumisomorphismus.

2. Wähle Polynom $g(x)$ vom Grad $n-k$. Multipliziere $m(x)$ mit x^{n-k}:
   $x^{n-k}m(x) = m_0x^{n-k} + m_1x^{n-k+1} + \cdots + m_{k-1}x^{n-1}$
   Codiere $m(x)$ in $c(x) := x^{n-k}m(x) - \underbrace{(x^{n-k}m(x) \bmod g(x))}_{\text{Grad} < n-k}$
   Ist $x^{n-k}m(x) \bmod g(x) = b_0 + b_1x + \cdots + b_{n-k-1}x^{n-k-1}$, so ergibt sich
   $c(x) = -b_0 - b_1x - \cdots - b_{n-k-1}x^{n-k-1} + m_0x^{n-k} + \cdots + m_{k-1}x^{n-1}$
   $$\longleftrightarrow \begin{pmatrix} -b_0 \\ \vdots \\ -b_{n-k-1} \\ m_0 \\ \vdots \\ m_{k-1} \end{pmatrix}$$
   $g(x)$ heißt *Erzeugerpolynom* der Codierung

Decodierung:
Für jedes Codewort $c(x)$ ist $c(x) \bmod g(x) = 0$.
Wird $d(x)$ empfangen und gilt $d(x) \bmod g(x) \neq 0$, so ist ein Fehler aufgetreten.
Ist $d(x) \bmod g(x) = 0$, so vermutet man eine korrekte Übertragung. Die Originalnachricht steht dann an den letzten k Stellen in $d(x)$.

1-Fehler-entdeckender Code.
Codierung von Datenpaketen in LANs.
Entdeckung eines Fehlers: Neuanforderung der Daten.
Dort sind die Erzeugerpolynome z.T. standardisiert, z.B. $g(x) = x^{16}+x^{15}+x^2+1$ (CRC-16-Polynom (Cyclic Redundancy Code))

Zusammenhang zu linearen Codes:

7.2 Satz

Bezeichnungen wie in 7.1.

1. Die Menge $\mathcal{C}$ aller Codewörter in $K[x]_n$ ist gerade

$$g(x) \cdot K[x]_k = \{gh : h \in K[x]_k\}$$

2. $\mathcal{C}$ ist linearer $[n,k]$-Code über K (d.h. Länge n, Dimension k).

Beweis. 1. Zu $m(x) \in K[x]_k$ ist das Codewort

$$c(x) = x^{n-k}m(x) - (x^{n-k}m(x) \mod g(x))$$

ein Vielfaches von $g(x)$; also $\mathcal{C} \subseteq g(x) \cdot K[x]_k$.
Umgekehrt: grad $t(x) < k$,
$g(x)t(x) = a_0 + a_1x + \cdots + a_{n-k-1}x^{n-k-1} + m_0x^{n-k} + \cdots + m_{k-1}x^{n-1}$,
$m(x) = m_0 + \cdots + m_{k-1}x^{k-1}$.
$m(x) \cdot x^{n-k} = g(x)t(x) \underbrace{-a_0 - a_1x - \cdots - a_{n-k-1}x^{n-k-1}}_{m(x)x^{n-k} \bmod g(x)}$

2. $g(x) \cdot 1, g(x) \cdot x, \ldots, g(x) \cdot x^{k-1}$ ist Basis von $\mathcal{C}$.

□

7.3 Beispiel

$K = \mathbb{Z}_2,\ n = 24,\ k = 8,\ g(x) = x^{16} + x^{15} + x^2 + 1$
$m = (10110101) \in \mathbb{Z}_2^8$.
$m(x) = 1 + x^2 + x^3 + x^5 + x^7$
Multiplikation mit $x^{n-k} = x^{16}$: $x^{16}m(x) = x^{16} + x^{18} + x^{19} + x^{21} + x^{23}$
Division durch $g(x)$ mit Rest:

$$x^{23} + x^{21} + x^{19} + x^{18} + x^{16}$$
$$= (x^7 + x^6 + x^3 + 1) \cdot g(x) + \underbrace{x^{15} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1}_{x^{16}m(x) \bmod g(x)}$$

$$c(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{15} + x^{16} + x^{18} + x^{19} + x^{21} + x^{23}$$

$$\longleftrightarrow \quad (\underbrace{1011011111000001}_{\text{Ethernet-Trailer}} | \underbrace{10110101}_{m})$$

Polynomcodierung wird vor allem für zyklische Codes verwendet.

7.4 Definition

Sei $\mathcal{C}$ ein $[n,k]$-Code über einem endlichen Körper K. $\mathcal{C}$ heißt *zyklisch*, falls gilt:
Ist $(c_0, \ldots, c_{n-1}) \in \mathcal{C}$, so ist auch $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

7.5 Satz

Sei $\mathcal{C}$ ein linearer Code der Länge n über einem endlichen Körper K. Identifiziere K^n mit $K[x]_n$ wie in 7.1. Dabei: $\mathcal{C} \subseteq K^n \quad \longleftrightarrow \quad \widetilde{\mathcal{C}} \subseteq K[x]_n$.
Sei $f = x^n - 1 \in K[x]$. Dann gilt:
$\mathcal{C}$ ist zyklisch genau dann, wenn $\widetilde{\mathcal{C}}$ ein Ideal in $(K[x]_n, \oplus, \odot_f)$ ist.

Beweis. $c = (c_0, \ldots, c_{n-1}) \in \mathcal{C} \Longleftrightarrow c(x) = c_0 + c_1 x + \cdots c_{n-1}x^{n-1} \in \widetilde{\mathcal{C}}$.

$(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$

$\Longleftrightarrow \quad c_{n-1} + c_0 x + \cdots c_{n-2}x^{n-1} \in \widetilde{\mathcal{C}}$

$\Longleftrightarrow \quad x \odot_f (c_0 + c_1 x + \cdots c_{n-1}x^{n-1}) \in \widetilde{\mathcal{C}}$ (denn $x^n \bmod (x^n - 1) = 1$)

$\Longleftrightarrow \quad h(x) \odot_f (c_0 + c_1 x + \cdots c_{n-1}x^{n-1}) \in \widetilde{\mathcal{C}}$ für alle $h(x) \in K[x]_n$.

Damit folgt die Behauptung. □

7.6 Satz

Sei $\mathcal{C}$ ein zyklischer $[n, k]$-Code über einem endlichen Körper K, identifiziert mit dem Ideal $\widetilde{\mathcal{C}} \subseteq K[x]_n \cong K[x]/(x^n - 1)K[x]$.

1. Es existiert ein eindeutig bestimmtes normiertes Polynom $g(x)$ vom Grad $n - k$ mit $\widetilde{\mathcal{C}} = \{m(x) \cdot g(x) : \operatorname{grad}(m(x)) < k\}$.
   (Die Multiplikation $m(x) \cdot g(x)$ entspricht $m(x) \odot_f g(x)$, da $\operatorname{grad}(m(x) \cdot g(x)) < n$).
   $g(x)$ ist also das Erzeugerpolynom von $\widetilde{\mathcal{C}}$ (bzw. $\mathcal{C}$) entsprechend 7.1.

2. Es ist $x^n - 1 = g(x) \cdot h(x)$ und $\widetilde{\mathcal{C}} = \{c(x) \in K[x]_n : c(x) \odot_f h(x) = 0\}$.
   (Dabei ist $f = x^n - 1$.)
   $h(x)$ heißt *Kontrollpolynom* von $\widetilde{\mathcal{C}}$ (bzw. $\mathcal{C}$).

Beweis. 1. Nach 6.17 sind die Ideale von $K[x]$ von der Form $g(x)K[x]$, $g(x)$ normiert. Daraus folgt sofort, dass die Ideale von $K[x]/(x^n - 1)K[x]$ von der Form $g(x)K[x]/(x^n - 1)K[x]$ mit $g(x)K[x] \supseteq (x^n - 1)K[x]$, also $g(x) \mid x^n - 1$, sind.
Sei $g(x) \mid x^n - 1$. Ist $g(x)t(x) \in g(x)K[x]$, so $g(x)t(x) = s(x) + k(x)(x^n - 1)$, $\operatorname{grad}(s(x)) < n$ (Division mit Rest durch $x^n - 1$). Folglich ist $g(x) \mid s(x)$ und $g(x)t(x) = g(x)m(x) + k(x)(x^n - 1)$, $\operatorname{grad}(m(x)) < k$.
Jedes Element $g(x)t(x) + (x^n - 1)K[x] \in g(x)K[x]/(x^n - 1)K[x]$ ist also von der Form $g(x)m(x) + (x^n - 1)K[x]$, $\operatorname{grad}(m(x)) < k$.
In $(K[x]_n, \oplus, \odot_f)$ sind die Ideale also gerade die $\{m(x) \cdot g(x) : \operatorname{grad}(m(x)) < k\}$ für jedes $g(x) \mid x^n - 1$.

2. Es ist $g(x) \cdot h(x) = x^n - 1$ nach Teil a). $h(x)$ ist also normiert vom Grad k. Dann ist $g(x) \odot_f h(x) = 0$, also auch $c(x) \odot_f h(x) = 0$ für alle $c(x) \in \widetilde{\mathcal{C}}$.
   Ist umgekehrt $c(x) \odot_f h(x) = 0$, so $g(x)h(x) = x^n - 1 \mid c(x)h(x)$, also $g(x) \mid c(x)$, $c(x) \in \widetilde{\mathcal{C}}$.

□

7.7 Korollar

1. Es gibt genauso viele zyklische Codes der Länge n über K, wie es normierte Teiler von $x^n - 1$ in $K[x]$ gibt.

2. Sei $\mathcal{C}$ ein zyklischer $[n,k]$-Code über K, $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$ Erzeugerpolynom ($g_{n-k} = 1$) und $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ Kontrollpolynom von $\mathcal{C}$.
   Dann ist die $n \times k$ - Matrix

$$G = \begin{pmatrix} g_0 & 0 & \cdots & \cdots & 0 \\ g_1 & g_0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ \vdots & \vdots & & & g_0 \\ g_{n-k} & \vdots & & & \vdots \\ 0 & g_{n-k} & & & \vdots \\ \vdots & 0 & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & g_{n-k} \end{pmatrix}$$

   Erzeugermatrix von $\mathcal{C}$ und die $n \times (n-k)$ - Matrix

$$H = \begin{pmatrix} h_k & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ h_{k-1} & h_k & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & & & \vdots \\ \vdots & \vdots & & \ddots & & & \vdots \\ h_0 & \vdots & & & \ddots & & \vdots \\ 0 & h_0 & & & & \ddots & \vdots \\ 0 & 0 & & & & & h_k \\ \vdots & \vdots & & & & & \vdots \\ \vdots & \vdots & & & & & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & h_0 \end{pmatrix}$$

   Kontrollmatrix von $\mathcal{C}$.

Beweis. 1. Folgt aus 7.6.1.

2. Nach 7.6.1 bilden $g(x), x \cdot g(x), \ldots, x^{k-1} \cdot g(x)$ eine Basis von $\widetilde{\mathcal{C}}$. Daraus folgt, dass G eine Erzeugermatrix von $\mathcal{C}$ ist.
   Es ist $x^n - 1 = g \cdot h = \sum_{i=0}^{n} (\sum_{j=0}^{n} g_j h_{i-j}) x^i$ (dabei sind alle nicht definierten h_i, g_j gleich 0 zu setzen).
   Koeffizientenvergleich ergibt $\sum_{j=0}^{n-k} g_j h_{i-j} = 0$ für $i = 1, \ldots, n-1$, d.h.

$G^t H = 0$.
$g_0 h_0 = -1$, also $\operatorname{rg}(H) = n - k$. Also ist H Kontrollmatrix von $\mathcal{C}$.

□

7.8 Beispiel

$n = 4$, $K = \mathbb{Z}_2$. Zyklische Codes der Länge 4 über $\mathbb{Z}_2$:

$$x^4 + 1 = (x+1)^4 \text{ in } \mathbb{Z}_2[x]$$

Teiler:		
1	$\mathcal{C} = \mathbb{Z}_2^4$	
$x+1$	Erzeugermatrix $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$,	$\dim \mathcal{C} = 3$
$(x+1)^2 = x^2 + 1$	Erzeugermatrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$,	$\dim \mathcal{C} = 2$
$(x+1)^3 = x^3 + x^2 + x + 1$	Erzeugermatrix $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$,	$\dim \mathcal{C} = 1$
$(x+1)^4$	$\mathcal{C} = \{0\}$	

Für zyklische Codes gibt es häufig besonders schnelle Decodierverfahren. Außerdem sind sie gut geeignet, Fehlerbündel (mehrere aufeinanderfolgende Bits gestört) zu erkennen, wie es bei Übertragungen von Nachrichten oder Speicherungen von Daten auf CD's oft passiert.
Dazu:

7.9 Definition

Ein Vektor $v = (0, \ldots, 0, \underbrace{a, *, \ldots, *, \tilde{a}}_{b \text{ Stellen}}, 0, \ldots, 0)^t$ in K^n mit $a, \tilde{a} \neq 0$ heißt *Bündel* der Länge b ("burst").

Wird $c \in \mathcal{C}$ gesendet, $d \in K^n$ empfangen und ist $f = d - c$ (der Fehlervektor) ein Bündel der Länge b, so heißt f *Fehlerbündel* der Länge b.

7.10 Satz

Sei $\mathcal{C}$ ein zyklischer $[n, k]$-Code. Dann enthält $\mathcal{C}$ keine Bündel der Länge $\leq n - k$. Daher entdeckt ein zyklischer $[n, k]$-Code Fehlerbündel der Länge $\leq n - k$.

Beweis. Angenommen $c = (0, \ldots, 0, a_i, \ldots, a_{i+b-1}, 0, \ldots, 0)^t \in \mathcal{C}$, $a_i, a_{i+b-1} \neq 0$, $b \leq n-k$. Dann auch $\tilde{c} = (a_i, \ldots, a_{i+b-1}, \underbrace{0, \ldots, 0}_{\geq k \text{ Stellen}})^t \in \mathcal{C}$, da $\mathcal{C}$ zyklisch.

Die b-te Spalte der Kontrollmatrix H aus 7.7.2 ist
$h = (0, \ldots, 0, h_k = 1, \ldots, h_0, 0, \ldots, 0)^t$.
$\tilde{c}^t h = a_{i+b-1} \cdot h_k \neq 0$, also $\tilde{c}^t H \neq 0$, d.h. $\tilde{c} \notin \mathcal{C}$. Also auch $c \notin \mathcal{C}$, Widerspruch.
Ist $d = c + f$, f Fehlerbündel der Länge $\leq n-k$, so gilt:
$d^t H = c^t H + f^t H = f^t H \neq 0$, da $c \in \mathcal{C}$ und $f \notin \mathcal{C}$ (siehe oben).

□

7.11 Korrektur von Fehlerbündeln

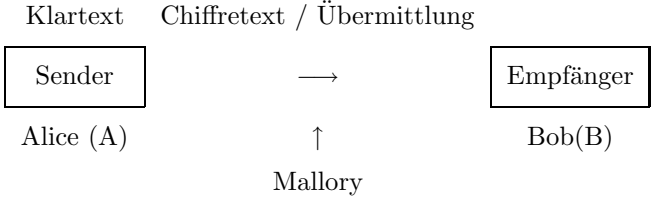
Sei K ein Körper der Ordnung p^m, p Primzahl. K ist ein m-dimensionaler Vektorraum über $K_0 \subseteq K$, $\mid K_0 \mid = p$; wir können K_0 mit $\mathbb{Z}_p$ identifizieren. Jedem $a \in K$ kann dann genau ein m-Tupel über $\mathbb{Z}_p$ zugeordnet werden.
Ist $\mathcal{C}$ ein t-fehlerkorrigierender zyklischer Code über K der Länge n, so wird diesem ein Code $\mathcal{C}_0$ der Länge nm über $\mathbb{Z}_p$ zugeordnet. Mit $\mathcal{C}_0$ können Fehlerbündel bis zur Länge $(t-1)m+1$ über $\mathbb{Z}_p$ korrigiert werden, denn $(t-1)m+1$ nebeneinanderliegende Stellen über $\mathbb{Z}_p$ beeinflussen höchstens t Stellen im zugehörigen Codewort in $\mathcal{C}$.

Mit Hilfe dieser und anderer Techniken werden Audio-Daten auf CD's codiert, um auch größere Fehlerbündel (Kratzer) korrigieren zu können. Ausgangspunkt ist dabei ein spezieller zyklischer Code (ein Reed-Solomon-Code) über einem Körper K mit 2^8 Elementen, der Länge 255, Dimension 251 und Minimalgewicht 5 hat.

Näheres z.B. in:
Friedrich, Kanalcodierung, Springer, 1996.
Willems, Codierungstheorie, de Gruyter, 1999.

7.B Kryptographische Verschlüsselungen

Ziel: Geheimhaltung von Nachrichten zwischen einem Sender (A = Alice) und einem Empfänger (B = Bob) gegen Abhören oder Veränderung durch einen Angreifer (Mallory).
Dies geschieht durch Verschlüsselungsverfahren. Dies sind Algorithmen, die die ursprünglichen Nachrichten (Klartexte) in Abhängigkeit von einem Parameter, dem Schlüssel, verschlüsseln (chiffrieren). Dadurch entstehen Chiffretexte.



Man unterscheidet zwei Typen von Verschlüsselungsverfahren:

Symmetrische Verfahren:
Sender und Empfänger haben einen gemeinsamen Schlüssel: wer verschlüsseln kann, kann auch entschlüsseln.
Problem: Schlüssel muss auf sicherem Weg ausgetauscht werden.

Wichtige Vertreter symmetrischer Verfahren sind der
DES (Data Encryption Standard); lange Zeit das am häufigsten eingesetzte Verfahren; jetzt abgelöst durch
AES (Advanced Encryption Standard); dieses Verfahren beruht u.a. auf Rechnungen in einem Körper der Ordnung 2^8.

Asymmetrische Verfahren oder *Public-Key-Verfahren*:
Jeder Teilnehmer T hat 2 Schlüssel:
öffentlicher Schlüssel P_T (jedem bekannt)
geheimer Schlüssel S_T (nur T bekannt)

A will B Nachricht m schicken:
Verschlüsselung durch Verschlüsselungsfunktion E: $E(m, P_B) = c$
Entschlüsselung durch Entschlüsselungsfunktion D, die Inverse zu E:
$D(c, G_B) = m$
Damit das funktioniert, muss E eine Einwegfunktion sein:
Sie ist leicht zu berechnen, aber die Inverse ist sehr schwer zu berechnen.
Mit Zusatzinformation (geheimer Schlüssel) ist die Inverse leicht zu berechnen.
(Diffie-Hellmann, 1976)

Einer der wichtigsten Vertreter von Public-Key-Verfahren ist das RSA-Verfahren:

7.12 RSA-Verfahren (Rivest, Shamir, Adleman; 1977)

Dieses Verfahren beruht auf Rechnungen im Ring $\mathbb{Z}_n$.

B erzeugt seinen öffentlichen und seinen geheimen Schlüssel:
B wählt zwei große Primzahlen p, q ($p \neq q$) (100- bis 200-stellig) [Zufallszahlen, Primzahltests]
$n = p \cdot q$

B wählt $e \in \mathbb{Z}$ mit $ggT(e, \varphi(n)) = 1$.
($\varphi(n) = (p-1) \cdot (q-1)$, Zufallszahlen und Euklidischer Algorithmus oder kleine Wahl von e)

B wählt $d \in \mathbb{Z}$ mit $ed \equiv 1 \bmod \varphi(n)$.
(D.h. $d + \varphi(n)\mathbb{Z} = (e + \varphi(n)\mathbb{Z})^{-1}$. Dies geht, da $ggT(e, \varphi(n)) = 1$; d berechnen mit Erweitertem Euklidischen Algorithmus - vgl. Bemerkung nach 3.32.)

Öffentlicher Schlüssel: (n, e)
Geheimer Schlüssel: d (p, q kann (und sollte) man löschen !)

A sendet Nachricht m an B: (m sei codiert als natürliche Zahl $< n$)
Chiffrierte Nachricht: $c = m^e \bmod n$
Entschlüsselung durch B : $m = c^d \bmod n$

Warum ist $m^{ed} \equiv m \bmod n$?

$ed \equiv 1 \bmod \varphi(n)$, $ed = 1 + k\varphi(n)$.

Ist $ggT(m,n) = 1$: $m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi(n)})^k \overset{3.33}{\equiv} m \cdot 1^k = m \bmod n$

Ist $ggT(m,n) \neq 1$, $n = p \cdot q$, $m < n$: $p|m$, $q \not| m$ (oder umgekehrt)

$$
\begin{array}{lll}
m \equiv 0 \bmod p & & \\
m^{ed} \equiv 0 \equiv m \bmod p & (ed = 1 + k(p-1)(q-1) & \\
m^{ed} \equiv m^{1+k(p-1)(q-1)} & = m(m^{q-1})^{k\cdot(p-1)} & \overset{3.33}{\equiv} m \cdot 1^{k(p-1)} = m \bmod p \\
m^{ed} \equiv m \bmod pq & (pq = n). &
\end{array}
$$

Sicherheit:
Wer d kennt, kann entschlüsseln.
Jeder kann d bestimmen, falls er $\varphi(n)$ kennt.
Jeder kann $\varphi(n) = (p-1)(q-1)$ bestimmen, falls er p, q kennt.

d oder $\varphi(n)$ zu bestimmen oder Faktorisierung von n zu bestimmen sind etwa gleich schwer.
Faktorisierung eines 200-stelligen Produkts zweier großer Primzahlen ist sehr schwierig. Schnellste Algorithmen benötigen Jahre.

Verwendung von RSA: Vor allem auch zum Austausch von Schlüsseln symmetrischer Verfahren.

Näheres z.B. in
Ertel, Angewandte Kryptographie, Fachbuchverlag Leipzig, 2003.