Diskrete Strukturen

Prof. Dr. Gabriele Nebe

7. November 2006

Inhaltsverzeichnis

Teil I

Abzählende Kombinatorik

1 Zählen von Elementen aus einer Menge

Wieviele Möglichkeiten gibt es k Objekte aus einer Menge von n Objekten zu zählen? Präzision!

Beispiel $M = \{1, 2, 3\}$, 2 Elemente aus M ziehen:

	geordnet	ungeordnet
mit zurücklegen	S $(1,1),(1,2),(1,3),$ $(2,1),(2,2),(2,3),$ $(3,1),(3,2),(3,3)$	M $\{1,1\}'\{1,2\}',\{1,3\}',$ $\{2,2\}',\{2,3\}',$ $\{3,3\}'$
ohne zurücklegen	S_0 $(1,2),(1,3),$ $(2,1),(2,3),$ $(3,1),(3,2)$	M_0 $\{1,2\},\{1,3\},$ $\{2,3\}$

(1.1) Definition Sei $k, n \in \mathbb{N} = \{0, 1, 2, \dots\}$

(i) $S(n,k) = \{(a_1, a_2, \dots, a_k) | a_i \in \{1, \dots, n\}$ für $i = 1, \dots, k\}$

(ii) $S_0(n,k) = \{(a_1, a_2, \dots, a_k) | a_i \in \{1, \dots, n\}$ für $i = 1, \dots, k$ und $a_i \neq a_j$ für alle $i \neq j\}$

(iii) $M_0(n,k) = \{M \subseteq \{1, \dots, n\} \mid |M| = k\}$

(iv) $M(n,k) = \{f : \{0, 1, \dots, n\} \to \mathbb{N} \mid \sum_{i=1}^{k} f(i) = k\}$

Beispiel $f : \{1, 2, 3\} \to \mathbb{N}$

1	2	3	
2	0	0	$\{1,1\}'$
1	1	0	$\{1,2\}'$
⋮	⋮	⋮	⋮
0	0	2	$\{3,3\}'$

Bemerkung (a) $S(n,k)$ = Menge der Folgen der Länge k mit Einträgen aus $\{1, \dots, n\}$ (mit Wiederholungen, Anordnung relevant)

(b) $S_0(n,k)$ = Menge der Folgen der Länge k mit Einträgen aus $\{1, \dots, n\}$ ohne Wiederholung.
Sei $\mathfrak{F}(n,k) := \{f : \{1, \dots, k\} \to \{1, \dots, n\}\}$
$\mathfrak{F}_0(n,k) := \{f : \{1, \dots, k\} \to \{1, \dots, n\} | f$ ist injektiv $\}$
$\mathfrak{F}(n,k) \to S(n,k) : f \mapsto (f(1), \dots, f(k))$ ist Bijektion mit $\mathfrak{F}_0(n,k) \to S_0(n,k)$.

(c) $\bigcup_{k=0}^{n} M_0(n,k) = \mathrm{Pot}(\{1,\dots,n\}) =$ Menge aller Teilmengen von $\{1,\dots,n\}$.

(d) $f \in M(n,k)$ repräsentiert eine sogenannte Multimenge, also eine „Menge“, die Elemente mehrfach enthalten kann.

Beispiel $\mathrm{Pot}(\{1,2,3\}) = \{\underbrace{\emptyset = \{\}}_{M_0(3,0)}, \underbrace{\{1\},\{2\},\{3\}}_{M_0(3,1)}, \underbrace{\{1,2\},\{1,3\},\{2,3\}}_{M_0(3,2)}, \underbrace{\{1,2,3\}}_{M_0(3,3)}\}$

$|\mathrm{Pot}(\{1,2,3\})| = 8 = 2^3$

Es gilt: $\mathrm{Pot}(\{1,2,3\}) \leftrightarrow \mathfrak{F}(2,n)$

$$M \subseteq \{1,\dots,n\} \mapsto \chi_M : \{1,\dots,n\} \to \{0,1\}$$
$$a \mapsto \begin{cases} 0 & a \notin M \\ 1 & a \in M \end{cases}$$

Beispiel $M(3,2)$

1	2	3	
2	0	0	$\{1,1\}'$
1	1	0	$\{1,2\}'$
1	0	1	$\{1,3\}'$
0	1	1	$\{2,3\}'$
0	2	0	$\{2,2\}'$
0	0	2	$\{3,3\}'$

Zählen:

	geordnet	ungeordnet
mit Zurücklegen	$S(n,k)$	$M(n,k)$
ohne Zurücklegen	$S_0(n,k)$	$M_0(n,k)$

(1.2) Satz (a) $|S(n,k)| = n^k$

(b) $|S_0(n,k)| = n(n-1)(n-2)\cdots(n-k+1)$

Beweis. 1. $(a_1,\dots,a_k) \in S(n,k)$

n Möglichkeiten für a_1, n Möglichkeiten für a_2, $\dots n$ Möglichkeiten für a_k.

insgesamt: $\underbrace{n \cdot n \cdots n}_{k \text{ Faktoren}} = n^k$ Möglichkeiten.

2. $(a_1,\dots,a_k) \in S_0(n,k)$

n Möglichkeiten für a_1, $n-1$ Möglichkeiten für a_2, $\dots$, $n-k+1$ Möglichkeiten für a_k.

insgesamt: $\underbrace{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}_{k\text{Faktoren}}$ Möglichkeiten.

□

(1.3) Definition $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$
$0! := 1$
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ falls $n \geq k \in \mathbb{N}$

(1.4) Satz

$$|M_0(n,k)| = \binom{n}{k}$$

Beweis. Definiere $\varphi : S_0(n,k) \to M_0(n,k), \varphi((a_1,\ldots,a_k)) = \{a_1,\ldots,a_k\}$.
φ ist surjektiv aber im allgemeinen nicht injektiv.
Wieviele $(a_1,\ldots,a_k) \in S_0(n,k)$ gibt es mit $\varphi((a_1,\ldots,a_k)) = \{a_1,\ldots,a_k\}$?
Bestimme

$$\begin{aligned}
&\varphi^{-1}(\{\{a_1,\ldots,a_k\}\}) \\
&= \{(b_1,\ldots,b_k) | \varphi((b_1,\ldots,b_k)) = \{b_1,\ldots,b_k\} = \{a_1,\ldots,a_k\}\} \\
&= \{(a_\pi(1), a_\pi(2), \ldots, a_\pi(k)) | \pi : \{1,\ldots,k\} \to \{1,\ldots,k\} \text{ bijektiv}\}
\end{aligned}$$

$|\varphi^{-1}(\{\{a_1,\ldots,a_k\}\})| = |\mathfrak{F}_0(k,k)| = k!$
Es ist $S_0(n,k) = \biguplus_{X \in M_0(n,k)} \varphi^{-1}(\{X\})$

$$\Rightarrow |S_0(n,k)| = \sum_{X \in M_0(n,k)} \underbrace{|\varphi^{-1}(\{X\})|}_{k!} = \sum_{X \in M_0(n,k)} k! = |M_0(n,k)| \cdot k!$$

$$\Rightarrow |M_0(n,k)| = \frac{|S_0(n,k)|}{k!} = \binom{n}{k}$$

□

Beispiel

$$\begin{aligned}
|M_0(4,2)| &= \frac{4!}{2!(4-2)!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 2 \cdot 1} = 6 \\
M_0(4,2) &= \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}
\end{aligned}$$

(1.5) Bemerkung (a) $\binom{n}{k} = \binom{n}{n-k}$
Genauer $M_0(n,k) \leftrightarrow M_0(n,n-k)$
$X \mapsto \{1,\ldots,n\} \setminus X = \{a \in \{1,\ldots,n\} | a \notin X\}$

(b) $k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$

(c) $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

(d) $\sum_{k=0}^{n} \binom{n}{k} = 2^n = |\operatorname{Pot}(\{1,\ldots,n\})|$

Beweis. 1. ✓

2. direkt durch Nachrechnen oder:
   $k \cdot \binom{n}{k} = |\underbrace{\{(a,X)|a \in X \in M_0(n,k)\}}_{A}|$
   $n \cdot \binom{n-1}{k-1} = |\underbrace{\{(a,Y)|Y \subseteq \{1,\dots,n\} \setminus \{a\}, |Y| = k-1, a \in \{1,\dots,n\}\}}_{B}|$
   Bijektion $A \to B : (a,X) \mapsto (a, X \setminus \{a\})$
   $\Rightarrow |A| = |B|$
   $\Rightarrow k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$

3. Nachrechnen oder:

$$M_0(n+1,k) \to M_0(n,k) \cup M_0(n,k-1)$$
$$X \subseteq \{1,\dots,n+1\} \mapsto \begin{cases} X & n+1 \in X \\ X \setminus \{n+1\} & n+1 \in X \end{cases}$$

   ist Bijektion.

4.
$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} |M_0(n,k)| = \bigcup_{k=0}^{n} M_0(n,k)$$
$$= |\operatorname{Pot}(\{1,\dots,n\})| = |\mathfrak{F}(2,n)| = |S(2,n)| \overset{(1.2)}{=} 2^n$$

□

(1.6) Satz (Binomischer Lehrsatz) $x, y \in$ Ring

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Beweis. $(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n\text{Faktoren: } f_1,\dots,f_n}$
Beitrag zu $x^k \cdot y^{n-k}$:
dazu aus k Faktoren das x auswählen: $f_{a_1}, \dots, f_{a_k} \leftrightarrow \{a_1, \dots, a_k\}$
aus $n-k$ Faktoren das y auswählen
Koeffizienten von $x^k \cdot y^{n-k} = \sum_{\{a_1,\dots,a_n\} \subseteq \{1,\dots,n\}} 1 = |M_0(n,k)|.$ □

Folgerung $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
Setze $x = y = 1$ in (1.6):

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

(1.7) Folgerung Jede n elementige Menge hat genausoviele Teilmengen gerader Ordnung wie ungerader Ordnung.
(M Menge: $|M|$ = Ordnung von M)
Plausibelmachung: n ungerade
$|X|$ gerade $\Leftrightarrow$ $|\{1,\ldots,n\} \setminus X|$ ungerade

Beweis.

$$0 = (1-1)^n \overset{(1.6)}{=} \sum_{k=0}^{n} \binom{n}{k} 1^k (-1)^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k}$$
$$0 = ((-1)+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k$$

Die Summe am Ende ist die Summe über alle Teilmengen wobei Mengen mit gerader/ungerader Anzahl von Elementen je ± 1 zu der Summe beitragen. □

(1.8) Satz (Vandermonde Identität)

$$\binom{w+m}{k} = \sum_{l=0}^{k} \binom{w}{l} \binom{m}{k-l}$$

Beweis. Hörsaal mit w weiblichen und m männlichen Studenten. Die Anzahl der Möglichkeiten, k Studenten aus diesen $w+m$ auszuwählen, ist die Summe der Anzahl der Möglichkeiten, l weibliche und $k-l$ männliche auszuwählen.

□

(1.9) Satz $|M(n,k)| = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$

Beweis. $f \in M(n,k)$ ist $f : \{1,\cdots,n\} \to \mathbb{N} = \{0,1,\cdots\}$ mit $\sum_{i=1}^{n} f(i) = k$

Kodiere f durch: $\underbrace{*\cdots*}_{f(1)} | \underbrace{*\cdots*}_{f(2)} | * \cdots | \underbrace{*\cdots*}_{f(n)}$

Anzahl $*$: $\sum_{i=1}^{n} f(i) = k$

Anzahl $|$: $n-1$

Länge der Folge aus $*$, $|$: $n-1+k$

f ist eindeutig bestimmt durch die Positionen der $*$ bzw. $|$:

dafür $\binom{n-1+k}{k}$ Möglichkeiten

bzw. $\binom{n-1+k}{n-1}$ Möglichkeiten

$\Rightarrow$ Behauptung. □

Beispiel $|M(4,3)| = \binom{4+3-1}{3} = \binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} = 20$

Beispiel $f \in M(4,3)$

	1	2	3	4	
$\{1,1,3\}'$	2	0	1	0	$**\|\|*\|$
$\{2,3,4\}'$	0	1	1	1	$\|*\|*\|*$
$\{3,3,3\}'$	0	0	0	3	$\|\|\|***$

2 Permutationen, die symmetrische Gruppe

(2.1) Definition Sei Ω eine Menge.
$S_\Omega := \{f : \Omega \to \Omega | f \text{ ist bijektiv}\}$ heißt die *symmetrische Gruppe* von Ω.
$S_n := S_{\{1,\cdots,n\}}$
$S_n = \mathfrak{F}_0(n,n) \leftrightarrow S_0(n,n)$
$|S_0(n,n)| = n(n-1)(n-2)\cdots 2 \cdot 1 = n!$

Bemerkung $S_n = \mathfrak{F}_0(n,n)$
Sei $f : \{1,\cdots,n\} \to \{1,\cdots,n\}$ injektiv
$\Rightarrow$ Bild$(f) = \{f(1),\cdots,f(n)\}$ besteht aus n verschiedenen Werten
$\{f(1),\cdots,f(n)\} \subseteq \{1,\cdots,n\} \leftarrow$ auch n Elemente
$\Rightarrow$ Bild$(f) = \{1,\cdots,n\}$ d.h. f ist surjektiv.

Merke Ist M eine endliche Menge und $f : M \to M$ Funktion, so gilt:
f injektiv $\Leftrightarrow$ f surjektiv $\Leftrightarrow$ f bijektiv.

Dies ist falsch, sobald M unendlich ist:

Beispiel $M = \mathbb{N} = \{0,1,\cdots\}$
$f : M \to M, f(n) := n+1$ ist injektiv, aber $0 \notin$ Bild(f), also f nicht surjektiv.
$g : M \to M, g(n) := \begin{cases} n & n \text{ ungerade} \\ \frac{n}{2} & n \text{ gerade} \end{cases}$
$\Rightarrow$ g surjektiv
aber $g(1) = g(2) \Rightarrow g$ nicht injektiv.

Wir wissen bereits: $|S_n| = n!$.

Beispiel

$$|S_5| = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$
$$|S_6| = 720$$

Übung: $|S_{20}| = ?$

(2.2) Bemerkung (a) $f, g \in S_\Omega \Rightarrow$ Die Hintereinanderausführung $f \circ g \in S_\Omega$
$(f \circ g)(\omega) = f(g(\omega)), \forall \omega \in \Omega$
Umkehrabbildung: $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

Dann:

$$\begin{aligned}&(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ g \circ g^{-1} \circ f^{-1}\\ =&f \circ \mathrm{id}_\Omega \circ f^{-1} = f \circ \mathrm{id}_\Omega \circ f^{-1}\\ =&f \circ f^{-1} = \mathrm{id}_\Omega\end{aligned}$$

und umgekehrt ebenso.

(b) (i) Für $f, g, h \in S_\Omega$ gilt:
$(f \circ g) \circ h = f \circ (g \circ h)$ (Assoziativität)

(ii) Für $f \in S_\Omega$ gilt $id_\Omega \circ f = f \circ id_\Omega = f$

(iii) Für $f \in S_\Omega$ gibt es $f^{-1} \in S_\Omega$ mit
$f \circ f^{-1} = f^{-1} \circ f = id_\Omega$

(c) Eine Menge G mit einer Verknüpfung $\circ : G \times G \to G$ die (b)(i)-(iii) erfüllt, nennt man *Gruppe*

(2.3) Bemerkung (Schreibweise für die Elemente aus S_n)

$\sigma \in S_n$:

1	2	3	...	n
$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	...	$\sigma(n)$

Beispiel $n = 6$

σ :

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

Zykelschreibweise: $\sigma = (1)(23)(465)$

(2.4) Definition Ein k-Zykel ist eine Permutation $\sigma \in S_m$ die k Elemente zyklisch vertauscht.

$$\{\omega_1, \ldots, \omega_k\} \subseteq \{1, \ldots, n\}$$

$$\sigma(\omega_i) = \begin{cases} \omega_{i+1} & i = 1, \ldots, k-1 \\ \omega_1 & i = k \end{cases}$$

$$\sigma(l) = l \quad \forall l \in \{1, \ldots, n\} \setminus \{\omega_1, \ldots, \omega_k\}$$

$$\sigma = (\omega_1, \omega_2, \ldots, \omega_k) = (\omega_2, \ldots, \omega_k, \omega_{k-1}) = (\omega_{k-1}, \omega_k, \omega_1, \ldots, \omega_{k-2}) = \ldots$$

Beispiel $n = 5$

(1 3 5) 3-Zykel

(1 2 4 5) 4-Zykel

$(1\,3\,5) \circ (1\,2\,4\,5) = \underbrace{(1\,2\,4)(5\,3) = (5\,3)(1\,2\,4)}_{\text{disjunkte Zykel}}$

$(1\,2\,4\,5) \circ (1\,3\,5) = (1\,3)(2\,4\,5)$

(2.5) Bemerkung (a) Zwei Zykel $\omega = (\omega_1, \ldots, \omega_k), \sigma = (\sigma_1, \ldots, \sigma_l) \in S_n$ heißen disjunkt $:\Leftrightarrow \{\omega_1, \ldots, \omega_k\} \cap \{\sigma_1, \ldots, \sigma_l\} = \emptyset$.

(b) Sind $\sigma, \omega \in S_n$ disjunkte Zykel, so gilt $\sigma \circ \omega = \omega \circ \sigma$.

Beweis. $\{1, \ldots, n\} = A \uplus B \uplus C$ mit $A = \{\omega_1, \ldots, \omega_k\}, B = \{\sigma_1, \ldots, \sigma_l\}, C = \{1, \ldots, n\} \setminus (A \cup B)$.
Sei $j \in \{1, \ldots, n\}$. Zu zeigen: $\sigma(\omega(j)) = \omega(\sigma(j))$.
3 Fälle:

(1) $j \in C$: $\left.\begin{matrix}\sigma(j) = j \\ \omega(j) = j\end{matrix}\right\} \Rightarrow (\sigma \circ \omega)(j) = \sigma(\omega(j)) = \sigma(j) = j$
umgekehrt: $(\omega \circ \sigma)(j) = \omega(\sigma(j)) = \omega(j) = j$

(2) $j \in A$: $\sigma(j) = j, \omega(j) \in A \Rightarrow \sigma(\omega(j)) = \omega(j)$
$(\omega \circ \sigma)(j) = \omega(\sigma(j)) = \omega(j)$
$(\sigma \circ \omega)(j) = \sigma(\omega(j)) = \omega(j)$

(3) $j \in B$ genauso wie (2)

□

(2.6) Satz (a) Jedes $\pi \in S_n$ ist Produkt disjunkter Zykel.

(b) Die Schreibweise in (a) ist eindeutig bis auf: Vertauschen der Zykel.
(Achtung: $(\omega_1, \ldots, \omega_k) = (\omega_k, \omega_1, \ldots, \omega_{k-1}) = \cdots \in S_n$
$(\omega_1) = \mathrm{id}_{S_n}$ kann immer weggelassen werden.)

Beweis. (a) Input: $\pi \in S_n$
Init: $\Omega = \{1, \ldots, n\}; Z = \emptyset$
Algorithmus:

```
while Ω ≠ ∅ do
    wähle ω ∈ Ω;
    H := [ω]; l := 1; Ω = Ω \ {ω};
    while π(ω) ∉ H do
        H[l + 1] := [π(ω)];
        l := l + 1, ω := π(ω); Ω := Ω \ {ω};
    end while;
    Z := Z ∪ H;
end while;
```

Output: $Z = \{Z_1, \ldots, Z_a\} \Rightarrow \pi = Z_1 \circ \cdots \circ Z_a = Z_1 \ldots Z_a$ Produkt disjunkter Zykel

(b) Eindeutigkeit: Zyklen aus Graph ableitbar:
Ecken: $\{i, \ldots, n\}$, Kanten: $i \to \pi(i)$.

□

Beispiel $n = 9$

σ	1	2	3	4	5	6	7	8	9
	2	5	3	6	1	7	9	8	4

$\sigma = (1\,2\,5)(3)(4\,6\,7\,9)(8) = (6\,7\,9\,4)(2\,5\,1)$

Algorithmus:

$\Omega = \{1, \ldots, 9\}, Z = \emptyset$

$\omega := 1; H = [1]; l := 1;$

$\sigma(1) = \pi(1) = 2 \notin H : H = [1, 2]; l := l + 1;$

$\pi(2) = 5 \notin H : H = [1, 2, 5]; l := 3; \omega := 5;\ \ \pi(5) = 1 \in H; \to Z = Z \cup \{[1, 2, 5]\}$

$\Omega = \{1, \ldots, 9\} \setminus \{1, 2, 5\} = \{3, 4, 6, 7, 8, 9\}$

$\vdots$

(2.7) Definition Sei $\sigma \in S_n$.
Dann gibt es ein $m \in \mathbb{N}, m > 0$ mit $\sigma^m = \underbrace{\sigma\sigma \ldots \sigma}_{m\text{-Faktoren}} = \mathrm{id}$. Das kleinste solche m heißt die *Ordnung* von σ: $\mathrm{ord}(\sigma)$.

Beispiel $\sigma = (1\,2\,5)(3)(4\,6\,7\,9)(8)$
$\Rightarrow \mathrm{ord}(\sigma) = 12$
$\sigma^2 = (1\,2\,5)^2(4\,6\,7\,9)^2 = (1\,5\,2)(4\,7)(6\,9)$
$\sigma^3 = (1\,2\,5)^3(4\,6\,7\,9)^3 = (1)(2)(5)(4\,9\,7\,6)$
$\sigma^{12} = (\sigma^3)^4 = (4\,9\,7\,6)^4 = \mathrm{id}$

Bemerkung (a) $\mathrm{ord}(k\text{-Zykel}) = k$

(b) $\mathrm{ord}(\mathrm{id}) = 1$

(c) $\sigma_1 \ldots \sigma_s$ disjunkte Zykeln der Ordnung $k_i = \mathrm{ord}(\sigma_i)$ $(i = 1, \ldots, s)$
$\Rightarrow \mathrm{ord}(\sigma_1 \ldots \sigma_s) = \mathrm{kgV}(k_1, \ldots, k_s) =: a$
Denn: Für $m \in \mathbb{N}$ ist $(\sigma_1 \ldots \sigma_s)^m = \sigma_1^m \ldots \sigma_s^m$ also $(\sigma_1 \ldots \sigma_s)^m = \mathrm{id} \Leftrightarrow \sigma_1^m = \cdots = \sigma_s^m = \mathrm{id} \Leftrightarrow k_1 | m, \ldots, k_s | m$

Bemerkung Ist $a \in \mathbb{N}, a > 0, \sigma^a = \mathrm{id} \Rightarrow \mathrm{ord}(\sigma) | a$.
Denn: $m := \mathrm{ord}(\sigma) \Rightarrow \sigma^m = \mathrm{id}$
$\sigma^{-m} = \mathrm{id}^{-1} = \mathrm{id}$
$\sigma^{-m} := \underbrace{\sigma^{-1} \circ \cdots \circ \sigma^{-1}}_{m\text{-Faktoren}}$
Sei $a \in \mathbb{N}, a > 0, \sigma^a = \mathrm{id} \Rightarrow a \geq m$.
$\sigma^{a-m} = \sigma^a \circ \sigma^{-m} = \sigma^a = \mathrm{id}$.
Sei $s \in \mathbb{N}$ mit $a - sm \geq 0, a - sm < m$.
$\sigma^{a-sm} = \sigma^a \circ (\sigma^{-m})^s = \mathrm{id}$
$a - sm < m \overset{\text{m-minimal}}{\Rightarrow} a - sm = 0 \Rightarrow a = sm$. Also a durch m teilbar.

(2.8) Bemerkung (Konjunktion) (a) Seien $\sigma, \pi \in S_n$. σ, π heißen *konjugiert* $:\Leftrightarrow$ $\exists g \in S_n$ mit $\sigma = g \circ \pi \circ g^{-1} = {}^g\pi$ $(\Leftrightarrow \pi = g^{-1} \circ \sigma \circ g = {}^{g^{-1}}\sigma)$.

(b) Ist $\sigma = (\sigma_1, \ldots, \sigma_k)$ ein k-Zykel und $g \in S_n$ so ist $g \circ \sigma \circ g^{-1} = (g(\sigma_1), g(\sigma_2), \ldots, g(\sigma_k))$ wieder ein k-Zykel:

$$(g \circ \sigma \circ g^{-1})(g(\sigma_i)) = g(\sigma(g^{-}1(g(\sigma_i)))) = g(\sigma(\sigma_i)) = \begin{cases} g(\sigma_{i+1}) & i < k \\ g(\sigma_i) & i = k \end{cases}$$

Rest klar:
$j \notin \{g(\sigma_1), \ldots, g(\sigma_k)\} \Rightarrow g^{-1} \notin \{\sigma_1, \ldots, \sigma_k\}$ d.h. $\sigma(g^{-1}(j)) = g^{-1}(j) \Rightarrow (g \circ \sigma \circ g^{-1})(j) = g(\sigma(g^{-1}(j))) = g(g^{-}1(j)) = j$.

Beispiel (a) $(4\,5\,8) \circ (1\,3\,5\,7) \circ (4\,5\,8)^{-1} = (1\,3\,8\,7)$

(b) $\mathrm{ord}(g \circ \sigma \circ g^{-1}) = \mathrm{ord}(\sigma)$ (Übung)

(c) $g \circ (\sigma \circ \pi) \circ g^{-1} = (g \circ \sigma \circ g^{-1}) \circ (g \circ \pi \circ g^{-1})$
Denn: $g \circ \sigma \circ \underbrace{g^{-1} \circ g}_{\mathrm{id}} \circ \pi \circ g^{-1} = g \circ \sigma \circ \pi \circ g^{-1}$

(d) Sind σ und π disjunkte Zyklen, so gilt für $g \in S_n$, $g \circ \sigma \circ g^{-1}$ und $g \circ \pi \circ g^{-1}$ sind disjunkte Zyklen.
Denn

$$\sigma = (\sigma_1, \ldots, \sigma_k) \qquad g \circ \sigma \circ g^{-1} = (g(\sigma_1), \ldots, g(\sigma_k))$$
$$\pi = (\pi_1, \ldots, \pi_k) \qquad g \circ \pi \circ g^{-1} = (g(\pi_1), \ldots, g(\pi_k))$$

σ, π disjunkt $\Leftrightarrow \{\sigma_1, \ldots, \sigma_k\} \cap \{\pi_1, \ldots, \pi_k\} = \emptyset$
$(g(\pi_j) = g(\sigma(j)) \underset{g \text{ injektiv}}{\Leftrightarrow} \pi_j = \sigma_j)$

Beispiel $\sigma = (1\,2\,5)(4)(3\,6\,8\,7), \pi = (5\,7\,4)(3)(1\,2\,6\,8)$ sind konjugiert in S_8.
Weiß: $g \in S_8, g \circ \sigma \circ g^{-1} = (g(1), g(2), g(5))(g(4))(g(3), g(6), g(8), g(7)) \overset{!}{=} (5\,7\,4)(3)(1\,2\,6\,8)$

g:

1	2	3	4	5	6	7	8
5	7	1	3	4	2	8	6

$\Rightarrow g = (1\,5\,4\,3)(2\,7\,8\,6) \in S_8$, d.h. $g \circ \sigma \circ g^{-1} = \pi$. g ist *ein* konjugiertes Element.
Ebenso: $h = (1\,7\,2\,4\,3\,6\,8)(5)$ erfüllt genauso $h \circ \sigma \circ h^{-1} = \pi$.

(2.9) Definition 1. Eine *Partition* von n ist ein $k-Tupel$ $\lambda = (\lambda_1, \ldots, \lambda_k)$ mit $\sum_{i=1}^{k} \lambda_i = n$ und $\lambda_i \in \mathbb{N}, \lambda_i > 0 \forall i, \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k > 0$.
Das Diagramm von λ besteht aus λ_i Kästchen in Zeile i.

2. Sei $\pi \in S_n, \pi = \sigma_1 \cdot \cdots \cdot \sigma_k$ Produkt disjunkter Zykeln der Ordnung $\lambda_i = \mathrm{ord}(\sigma_i) \geq 1$ so geordnet, dass $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$. Dann heißt die Partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ von n der *Zykeltyp* von π.

Beispiel (a) $\lambda = (4, 3, 3, 1)$ Partition von 11.

(b) σ, g, h wie oben.
Zykeltyp(σ) = Zykeltyp(π) = $(4, 3, 1)$
Zykeltyp(g) = $(4, 4)$
Zykeltyp(h) = $(7, 1)$

(2.10) Satz Seien $\pi, \sigma \in S_n$. Es gibt genau dann ein $g \in S_n$ mit ${}^g\sigma = g \circ \sigma \circ g^{-1} = \pi$, wenn Zykeltyp($\pi$) = Zykeltyp($\sigma$).

Beweis. „⇒“ $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ = Zykeltyp(π)
$\pi = (\pi_1, \ldots, \pi_{\lambda_1})(\pi_{\lambda_1+1}, \ldots, \pi_{\lambda_1+\lambda_2}) \ldots (\pi_{n-\lambda_k+1}, \ldots, \pi_n)$ sei die Zykelschreibweise von π als Produkt disjunkter Zykel.

Ist $g \in S_n$ so gilt $g \circ \pi \circ g^{-1} = (g(\pi_1), \ldots, g(\pi_{\lambda_1})) \ldots (g(\pi_{n-\lambda_k+1}, \ldots, g(\pi_n)))$ ist Produkt disjunkter Zykel, d.h. falls $\sigma = g \circ \pi \circ g^{-1}$ für ein $g \in S_n$, dann ist Zykeltyp(σ) = Zykeltyp(π).

„⇐“ Sei $\sigma = (\sigma_1, \ldots, \sigma_{\lambda_1})(\sigma_{\lambda_1+1}, \ldots, \sigma_{\lambda_1+\lambda_2}) \ldots (\sigma_{n-\lambda_k+1}, \ldots, \sigma_n) \in S_n$ ein beliebiges Element mit gleichem Zykeltyp $(\lambda_1, \ldots, \lambda_k)$.

Definiere $g : \{1, \ldots, n\} \to \{1, \ldots, n\}$ durch $g(\pi_i) := \omega_i$.
(Definition von g ist eindeutig, da jedes Element von $\{1, \ldots, n\}$ als π_i vorkommt. g surjektiv, da $\{\omega_1, \ldots, \omega_n\} = \{1, \ldots, n\} \Rightarrow g \in S_n$.)

Rechenregel $\Rightarrow g \circ \pi \circ g^{-1} = \omega$

□

Bemerkung (Verfahren zum Finden von g mit $g \circ \pi \circ g^{-1} = \sigma$)
Schreibe $\pi = (\pi_1, \ldots, \pi_{\lambda_1}) \ldots (\pi_{n-\lambda_{k-1}+1}, \ldots, \pi_n)$, $\sigma = (\sigma_1, \ldots, \sigma_{\lambda_1}) \ldots (\sigma_{n-\lambda_{k-1}+1}, \ldots, \sigma_n)$
Zerlegung in disjunkte Zykeln (Zykeln der Länge 1 nicht vergessen).
Definiere $g \in S_n$ durch $g(\pi_i) = \sigma_i \Rightarrow \sigma = g \circ \pi \circ g^{-1}$.

Beispiel $\pi = (1\,3\,7)(2\,5)(4)(8)(6)$, $\sigma = (2\,4\,6)(1\,3)(7)(8)(3)$
$g = (1\,2)(3\,4\,7\,6\,5)(8)$ erfüllt $g \circ \pi \circ g^{-1} = \sigma$.
Achtung: g ist *nicht* eindeutig bestimmt.

3 Operationen von Gruppen auf Mengen

(3.1) Definition (a) Eine *Gruppe* $(G, \cdot)$ ist eine Menge G mit einer Verknüpfung $\cdot : G \times G \to G, (a, b) \to a \cdot b$ mit

(i) $(g \cdot h) \cdot f = g \cdot (h \cdot f) \quad \forall g, h, f \in G$

(ii) $\exists 1 \in G$ mit

(a) $1 \cdot g = g \cdot 1 = g \;\; \forall \;\; g \in G$

(b) $\forall g \in G \; \exists g^{-1}$ mit $g \cdot g^{-1} = g^{-1} = 1$

(b) Ist $(G, \cdot)$ eine Gruppe, so heißt eine Teilmenge $U \subseteq G$ eine *Untergruppe* $:\Leftrightarrow$ $(U, \cdot_{|U\times U})$ wieder eine Gruppe ist.
In Zeichen: $U \leq G$

(c) Sind $(G, \cdot)$ und $(H, \cdot')$ Gruppen, so heißt eine Abbildung $f : G \to H$ mit $f(g_1 \cdot g_2) = f(g_1) \cdot' f(g_2) \ \forall\ g_1, g_2 \in G$ ein *Homomorphismus* von Gruppen.
G und H heißen isomorph $:\Leftrightarrow \exists f : G \to H$ bijektiver Homomorphismus
In Zeichen: $G \cong H$

Bemerkung: Ist $f : G \to H$ ein bijektiver Homomorphismus so ist die Umkehrabbildung $f^{-1} : H \to G$ wieder Homomorphismus.

(d) Ist $(G, \cdot)$ eine Gruppe, $M \subseteq G$ so heißt $< M >= \bigcap_{U\leq G, M\subseteq U} U =$ die kleinste Untergruppe von G, die M enthält das *Erzeugnis* von M.

Beispiel $(S_n, \circ)$ ist eine Gruppe
$1 = id_{\{1,\cdots,n\}}$

Beispiel $M = \{a = (12)(345)\} \subseteq S_5$

$$\begin{aligned} < M > &= < (12)(345) > \\ &= \left\{a^0 = id, a = (12)(345), a^2 = (354), a^3 = (12), a^4 = (345), a^5 = (12)(354)\right\} \\ &\quad (a^6 = (a^3)^2 = id) \end{aligned}$$

Die Menge auf der rechten Seite ist eine Untergruppe von S_5. Umgekehrt enthält jede Untergruppe von S_5, die a enthält auch die Menge auf der rechten Seite.

(3.2) Bemerkung Sei $(G, \cdot)$ Gruppe.

(a) Für $g \in G$ ist g^{-1} eindeutig bestimmt
Ebenso ist $1 \in G$ eindeutig bestimmt

(b) $U \subseteq G$ ist Untergruppe $\Leftrightarrow U \neq \emptyset$ und $a, b \in U$ so ist auch $a \cdot b^{-1} \in U$

(c) $U \leq G, V \leq G \Rightarrow U \cap V \leq G$

(d) $< M >= \left\{m_1 \cdot m_2 \cdots m_k | k \in \mathbb{N}, m_i \in M \text{ oder } m_i^{-1} \in M\ \forall\ i\right\}$

(e) $f : G \to H$ Homomorphismus von Gruppen
$\text{Bild}(f) = \{f(g) | g \in G\} \leq H$
$\text{Kern}(f) = \{g \in G | f(g) = 1\} \leq G$

Beweis. (a) Eindeutigkeit von 1:
Seien $1, 1' \in G$ mit (3.1)(ii)(a)

$$1 \underbrace{=}_{\text{da 1' neutrales Element}} 1 \cdot 1' \underbrace{=}_{\text{da 1 neutrales Element}} 1'$$

Eindeutigkeit von g^{-1}: Seien g^{-1}, g' inverse Elemente von $g \in G$

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

(b) „$\Leftarrow$“ Wir müssen (3.1)(i)+(ii) nachrechnen:
$\cdot : U \times U \to U$ d.h. $\forall\, a, b \in U, a \cdot b \in U$
Zunächst: $1 \in U$ denn: $U \neq \emptyset$ d.h. $\exists\, u \in U$ und damit $1 = u \cdot u^{-1} \in U$
$b \in U \Rightarrow 1 \cdot b^{-1} = b^{-1} \in U \Rightarrow a \cdot (b^{-1})^{-1} = a \cdot b \in U$

(i) Assoziativgesetz gilt automatisch, da es für G gilt.

(ii) $1_U = 1_G \in U$ und mit $b \in U$ ist auch $b^{-1} = 1 \cdot b^{-1} \in U$ (ii)(b) erfüllt.

(c) $U \cap V \leq G : 1 \in U \cap V \neq \emptyset$ und für $a, b \in U \cap V$ liegt auch $a \cdot b^{-1} \in U \cap V$

(d) zu Hause

(e) Bild$(f) \leq H$:
denn: Bild$(f) \neq 0$, da $\forall\, g \in G, f(g) \in Bild(f)$
$f(g), f(h) \in Bild(f)$ z.Zg. $f(g) \cdot f(h)^{-1}$
$f(g) \cdot f(h)^{-1} = f(g \cdot h^{-1}) \in Bild(f)$
Kern$(f) = \{g \in G | f(g) = 1\} \ni 1$
$g, h \in Kern(f) \Rightarrow f(g \cdot h^{-1}) = f(g) \cdot f(h)^{-1}$
$= 1 \cdot 1^{-1} = 1 \Rightarrow g \cdot h^{-1} \in Kern(f) \underbrace{\leq}_{\text{nach (3.2)(b)}} G$

□

Beispiel $G =< a := (12)(345) > \leq S_5, H =< b := (12) > \leq S_2$
$f : G \to H : f(a^i) := b^i\ \forall\, i = 0, 1, \ldots, 5$ ist ein Homomorphismus
Kern(f)=$\{a^i | f(a^i) = 1\} = \{a^{2i}\}$
$= \{id, a^2 = (354), a^4 = (345)\}$
Bild(f)=$H = \{id, (12)\}$
$|Kern(f)| \cdot |Bild(f)| = |G| = 3 \cdot 2 = 6$

Bemerkung Sind G, H endliche Gruppen und ist $f : G \to H$ Homomorphismus so ist $|Kern(f)| \cdot |Bild(f)| = |G|$

Beweis. $Bild(f) = \{b_1, \cdots, b_n\}$
$G_i = \{g \in G | f(g) = b_i\}\ (i = 1, \cdots, n)$
$G = \biguplus_{i=1}^{n} G_i$
$\Rightarrow |G| = \sum_{i=1}^{n} |G_i|$

Behauptung: $\forall\, i = 1, \ldots, n\ |G_i| = |Kern(f)|$. Sei $g_i \in G_i$.

$g \in Kern(f) \Rightarrow g_i \cdot g \in G_i$ (jede Verknüpfung mit einem Element aus dem Kern ist wieder in G_i), denn: $f(g_i \cdot g) = f(g_i) \cdot f(g) = b_i \cdot 1 = b_i$ d.h. $g_i \cdot g \in G_i$

Umgekehrt sei $h_i \in G_i \Rightarrow g_i^{-1} \cdot h_i \in Kern(f)$ (d.h. jedes Element lässt sich darstellen als Produkt eines Elements aus dem Kern und g_i), denn: $f(g_i^{-1} \cdot h_i) = f(g_i)^{-1} \cdot f(h_i) = b_i^{-1} \cdot b_i = 1$

Gesehen: $G_i = \{g_i \cdot g | g \in Kern(f)\}$

$$\left.\begin{array}{c} G_i \leftrightarrow Kern(f) \\ g_i \cdot g \mapsto g = g_i^{-1} \cdot h_i \end{array}\right\} \Rightarrow |G_i| = |Kern(f)| \qquad \square$$

Erinnerung LA: V ein K-VR $\Rightarrow (V, +)$ ist Gruppe, neutrales Element 0. „v^{-1}“ $= -v$. Die lineare Abbildung $V \to W$ ist ein Gruppenhomomorphismus.
$\text{Kern}(f) \leq V$, $\text{Bild}(f) \leq W$
$\dim(\text{Kern}(f)) + \dim(\text{Bild}(f)) = \dim(V)$

(3.3) Definition Sei M eine Menge und G eine Gruppe

(a) G *operiert* auf $M :\Leftrightarrow \exists$ Abbildung $\cdot : G \times M \to M, (g, m) \to g \cdot m \in M (g \in G, m \in M)$ mit

(i) $(g \cdot h) \cdot m = g \cdot (h \cdot m) \quad \forall\, m \in M \; g, h \in G$

(ii) $1 \cdot m = m \quad \forall\, m \in M$

(b) G operiere auf M. Dann ist für $m \in M$
$G \cdot m = \{g \cdot m | g \in G\}$ die *Bahn* von m unter G.
$\text{Stab}_G(m) := \{g \in G | g \cdot m = m\}$ heißt der *Stabilisator* von m in G.

Beispiel S_n operiert auf $\{1, \cdots, n\}$ durch Anwenden.

Beispiel $\{1, \ldots, n\} = M$, $G = S_n$
$\text{Stab}_G(n) = \{g \in S_n | g(n) = n\} \cong S_{n-1}$
$g \mapsto g_{|\{1,\ldots,n-1\}}$ permutiert nur die ersten $n-1$ Punkte.
$G \cdot n = \{1, \ldots, n\}$ (G operiert *transitiv* auf M.)
$|S_n| = n \cdot |S_{n-1}| = |G \cdot n| \cdot |\,\text{Stab}_G(n)|$

Bemerkung $\text{Stab}_G(m) \leq G$ (der Stabilisator ist eine Untergruppe).

Bemerkung G operiere auf M. Dann ist die Abbildung $\mu : G \to S_\mu, \mu(g) : M \to M, m \mapsto g \cdot m \; \forall m \in M$ ein Homomorphismus von Gruppen.

(3.4) Satz (Bahnenlemma) Sei G eine endliche Gruppe, M eine Menge und G operiere auf M. Für $m \in M$ gilt $|G \cdot m| \cdot |\,\text{Stab}_G(m)| = |G|$.

Beweis. Sei $S := \text{Stab}_G(m)$, $|G \cdot m| = n$, $G \cdot m = \{g_1 \cdot m, \ldots, g_n \cdot m\}$ mit $g_1, \ldots, g_n \in G$. $m_i := g_i \cdot m$.
$G_i := \{g \in G | g \cdot m = m_i, 1 \leq i \leq n\}$
$\Rightarrow G = \biguplus_{i=1}^{n} G_i$ Behauptung: $G_i = \{g_i \cdot s | s \in S\}$
$s \in \text{Stab}_G(m) \Rightarrow (g_i \cdot s) \cdot m = g_i \cdot (s \cdot m) = g_i \cdot m = m$; d.h. $g_i \cdot s \in G_i$.

Umgekehrt sei $h_i \in G_i \Rightarrow h_i \cdot m = m_i = g_i \cdot m \Rightarrow (g_i^{-1} \cdot h_i) \cdot m = g_i^{-1} \cdot (h_i \cdot m) = g_i^{-1} \cdot m_i = g_i^{-1} \cdot (g_i \cdot m) = (g_i^{-1} \cdot g_i) \cdot m = 1 \cdot m = m$
Also $s := g_i^{-1} \cdot h_i \in \mathrm{Stab}_G(m)$
$h_i = g_i \cdot s \Rightarrow G_i = \{g_i \cdot s | s \in S\}$ d.h. $|G_i| = |\mathrm{Stab}_G(m)|$. □

(3.5) Satz Bahnenalgorithmus Sei $G =< \{g_1, \cdots, g_n\} >$ eine endliche Gruppe. G operiere auf M, $m \in M$.
Gesucht: $G \cdot m$ (sowie Erzeugendensystem $E \subseteq G$ mit $< E >= \mathrm{Stab}_G(m)$)
Initialisieren: Bahn:=[m]; anz := 1; Weg:=[1]; akt:=1; $E = \emptyset$
Algorithmus:

```
while akt ≤ anz do
    for i in [1,...,n] do
        x := g_i· Bahn[akt];
        if x in Bahn then x = Bahn[j]
            s:=Weg[j]^{-1} · g_i· Weg[akt];
            E := E ∪ {s};
        else
            anz := anz+1;
            Bahn[anz] := x; weg[anz] := g_i· weg[akt];
        end if;
    end for;
    akt := akt+1;
end while
```

Ergebnis: Bahn $= G \cdot m$

Beispiel $G =< g_1 := (124), g_2 := (24) > \leq S_4$
$M = \{1, 2, 3, 4\}$
Gesucht: $G \cdot 1$

	akt = 1	akt = 2
Bahn = [1]	Bahn = [1, 2]	Bahn = [1, 2, 4]
Weg = [id]	Weg = $[id, g_1]$	Weg = $[id, g_1, g1^2]$
	$E := \{g_2\}$	$E = \{g_2, g_1^{-2} g_2 g_1\}$

$E = \{g_2 = (24), g_1^{-2} g_2 g_1 = (24), id^{-1} g_1 g_1^2 = id, g_1^{-1} g_2 g_1^{-1} = (24)\} = \{id, (24)\}$
$\Rightarrow \mathrm{Stab}_G(1) =< (24) >= \{id, (24)\}$
$|Gm| = |\{1, 2, 4\}| = 3$
$|G| = 3 \cdot 2 = 6$

Dies ist eine Effiziente Methode zur Berechnung von $|G|$.

Beispiel Sei K ein endlicher Körper.
$GL_n(K) = \{A \in K^{n \times n} | A$ invertierbar $\}$
$GL_n(K)$ operiert auf $V = K^{n \times 1}$ durch Linksmultiplikation $(A, v) \mapsto Av$

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow GL_n(K) \cdot v_1 = K^{n\times 1} \setminus \{0\}$$

Länge der Bahnen $= |GL_n(K) \cdot v_1| = |K^{n\times 1}| - 1 = |K|^n - 1$

$S = \mathrm{Stab}_{GL_n(K)}(v_1)$

$$= \left\{ \begin{pmatrix} 1 & a_2 \cdots a_n \\ 0 & \\ \vdots & A' \\ 0 & \end{pmatrix} \in GL_n(K) \right\}$$

$$= \left\{ \begin{pmatrix} 1 & a_2 \cdots a_n \\ 0 & \\ \vdots & A' \\ 0 & \end{pmatrix} | a_2, \cdots, a_n \in K, A' \in GL_{n-1}(K) \right\}$$

$|S| = |K|^{n-1}|GL_{n-1}(K)|$

$\Rightarrow |GL_n(K)| = |GL_n(K) \cdot v_1| \cdot |S|$

$= (|K|^n - 1) \cdot |K|^{n-1} \cdot |GL_{n-1}(K)|$

$= \prod_{a=1}^{n} (|K|^a - 1)|K|^{a-1}$

Berechenbar, indem man nur $\sum_{a=1}^{n} (|K|^a - 1)|K|^{a-1}$ Elemente aufzählt, das ist logarithmischer Gewinn.

Beispiel (Operationen) (a) G Gruppe operiert auf $M = G$ durch Linksmultiplikation: $G \times M \to M : (g, m) \mapsto g \cdot m$.

(b) G Gruppe operiert auf $M = G$ durch Konjugation: $G \times M \to M : (g, m) \mapsto g \cdot m \cdot g^{-1}$. Bahnen: Konjugiertenklassen.

Beispiel $G = S_n$ $(n \geq 3)$. $m = (1\,2\,3) \in G$. Bestimme $|\{gmg^{-1} | g \in G\}| =$ Länge der Bahn von m.

$$|G \cdot m| = \frac{|G|}{|\mathrm{Stab}_G(m)|} = \frac{n!}{3 \cdot (n-3)!} = \frac{n(n-1)(n-2)}{3}$$

$|\mathrm{Stab}_G(m)| = 3 \cdot |S_{n-3}| = 3 \cdot (n-3)!$

(3.6) Satz G operiere auf M, $m_1, m_2 \in M$. Dann gilt entweder $G \cdot m_1 = G \cdot m_2$ oder $G \cdot m_1 \cap G \cdot m_2 = \emptyset$: „Bahnen sind gleich oder disjunkt“.

Beweis. Angenommen $G \cdot m_1 \cap G \cdot m_2 \neq \emptyset$. Sei dann $m \in G \cdot m_1 \cap G \cdot m_2$. Wir wollen zeigen $G \cdot m_1 = G \cdot m_2$:

$m = g_1 \cdot m_1 = g_2 \cdot m_2$ mit geeigneten $g_1, g_2 \in G$.

$G \cdot m_2 \subseteq G \cdot m_2$: Sei $g \cdot m_2 \in G \cdot m_2$. $g \cdot m_2 = g \cdot (g^{-1} \cdot g_1 \cdot m_1) = (g \cdot g_2^{-1} \cdot g_1) \cdot m_1 \in G \cdot m_1$.

Ebenso $G \cdot m_1 \subseteq G \cdot m_2$ also $G \cdot m_1 = G \cdot m_2$.

Die Bahnen partitionieren M (unterschiedliche Bahnenlänge möglich). □

(3.7) Satz (Satz von Lagrange) G endliche Gruppe, $U \leq G$ Untergruppe.
Dann ist $|U|$ ein Teiler von $|G|$.

Beweis. U operiert auf G via $U \times G \to G : (u, g) \mapsto u \cdot g$. G disjunkt zerlegt in Bahnen: $G = \biguplus_{i=1}^{k} U \cdot g_i$, wobei in jeder Bahn genau ein g_i liege.
Behauptung: $|U| = |U \cdot g_i|$. Denn wir haben eine Bijektion:

$$U \to U_{g_i} : u \mapsto u \cdot g_i$$
$$v \cdot g_i^{-1} \mapsfrom v$$

Es folgt: $|G| = \sum_{i=1}^{k} |U_{g_i}| = \sum_{i=1}^{k} |U| = k \cdot |U|$. □

Beispiel Die Ordnung eines Elementes $g \in G$ teilt $|G|$.
Denn: Ordnung von $g = | < g > |$ (vergleiche Aufgabe 9(i)) und $| < g > |$ teilt $|G|$.

(3.8) Satz G Gruppe, M G-Menge (M Menge mit G Operation).
Es ist $\mathrm{Stab}_G(g \cdot m) = g \cdot \mathrm{Stab}_G(m) \cdot g^{-1}$ für alle $g \in G$ und alle $m \in M$.

Beweis.

$$\begin{aligned} x \in \mathrm{Stab}_G(g \cdot m) &\Leftrightarrow x \cdot g \cdot m = g \cdot m \\ &\Leftrightarrow (g^{-1} \cdot x \cdot g) \cdot m = m \\ &\Leftrightarrow g^{-1} \cdot x \cdot g \in \mathrm{Stab}_G(m) \\ &\Leftrightarrow x \in g \cdot \mathrm{Stab}_G(m) \cdot g^{-1} \\ &\quad = \{g \cdot s \cdot g^{-1} | s \in \mathrm{Stab}_G(m)\} \end{aligned}$$

□

Anzahl von Bahnen

(3.9) Satz (Burnsidesches Fixpunktlemma) Sei G eine endliche Gruppe und M eine endliche G-Menge.
$\mathrm{Fix}_M(g) := \{m \in M | g \cdot m = m\} \subseteq M$ ist die *Fixpunktmenge* von g in M für $g \in G$.
Sei $M = \biguplus_{i=1}^{n} G \cdot m_i$ disjunkt in Bahnen zerlegt. Dann ist die Anzahl der Bahnen $n = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_M(g)|$.

Beweis. (a) Fall $n = 1$, d.h. M transitiv. Sei $X := \{(g, m) \in G \times M | g \cdot m = m\}$

$$\begin{aligned} |X| &= \sum_{g \in G} |\operatorname{Fix}_M(g)| = \sum_{m \in M} |Stab_G(m)| \\ &\overset{\text{Bahnenlemma}}{=} \sum_{m \in M} \frac{|G|}{|G \cdot m|} \overset{M \text{ transitiv}}{=} \sum_{m \in M} \frac{|G|}{|M|} = |G| \\ &\Rightarrow \frac{1}{|G|} \cdot \sum_{g \in G} |\operatorname{Fix}_M(g)| = 1 \end{aligned}$$

(b) Allgemeiner Fall:

$$\begin{aligned} M &= \biguplus_{i=1}^{n} \underbrace{G \cdot m_i}_{=:M_i \text{ transitiv}} \\ \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_M(g)| &= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} |\operatorname{Fix}_{M_i}(g)| \\ = \sum_{i=1}^{n} \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_{M_i}(g)| &\overset{(a)}{=} \sum_{i=1}^{n} 1 = n \end{aligned}$$

□

(3.9 a) Folgerung Bezeichnungen wie in (3.9)
Sei ${}^G g = \{\underbrace{xgx^{-1}}_{{}^x g} | x \in G\}$ die Konjugationsklasse von $g \in G$.
Schreibe $G = \biguplus_{j=1} {}^G g_i$ disjunkt in Konjugationsklassen zerlegt.
Sei $\operatorname{Stab}_G(g_j) = \{x \in G | x \cdot g_j \cdot x^{-1} = g_j\}$
Dann ist die Anzahl der Bahnen von G auf M:

$$\begin{aligned} n &\overset{1.}{=} \frac{1}{|G|} \sum_{j=1}^{k} |\operatorname{Fix}_M(g_j)| \cdot |{}^G g_j| \\ &\overset{2.}{=} \sum_{j=1}^{k} \frac{|\operatorname{Fix}_M(g_j)|}{|\operatorname{Stab}_G(g_j)|} \end{aligned}$$

Beweis. $\overset{1.}{=}$: Zu zeigen: $|\operatorname{Fix}_M(g_j)| = |\operatorname{Fix}_M(xg_jx^{-1})|$
Genauer: $\operatorname{Fix}_M(xg_jx^{-1}) = x \operatorname{Fix}_M(g_j)$
Denn:

$$\begin{aligned} m \in \operatorname{Fix}_M(xg_jx^{-1}) \quad &\Leftrightarrow xg_jx^{-1}m = m \quad &&\Leftrightarrow g_j(x^{-1}m) = x^{-1}m \\ &\Leftrightarrow x^{-1}m \in \operatorname{Fix}_M(g_j) \quad &&\Leftrightarrow m \in x \operatorname{Fix}_M(g_j) \end{aligned}$$

$\overset{2.}{=}$: Einsetzen von Bahnenlemma: $|{}^G g_j| = \dfrac{|G|}{|\operatorname{Stab}_G(g_j)|}$ □

Beispiel Wieviele Perlenketten aus 5 Perlen, entweder grün oder rot, gibt es? Dabei sind zwei Ketten als gleich anzusehen, wenn sie durch Drehen auseindander hervorgehen.
Menge der Färbungen $F := \{f : \{1,\dots,5\} \to \{\text{grün}, \text{rot}\}\}$
Darauf operiert $G :=< (1,2,3,4,5), (1,2)(3,5) >$ via $g \cdot f : i \mapsto f(g^{-1} \cdot i)$ für $g \in G$.

$$G \overset{\text{Bahnenalgo.}}{=} \{\,\mathrm{id}, (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2),$$
$$(1,2)(3,5), (2,5)(3,4), (1,5)(2,4), (1,4)(2,3), (1,3)(4,5)\}$$

$\mathrm{Fix}_F((2,5)(3,4)(1))$: Färbungen, die auf $\{2,5\}, \{3,4\}, \{1\}$ konstant sind.
$\Rightarrow |\mathrm{Fix}_F((2,5)(3,4)(1))| = |\{\text{rot}, \text{grün}\}|^{\text{Anzahl der Zykel}} = 2^3$
$\Rightarrow$ Anzahl den Bahnen ist nach (3.9) $\frac{1}{10}(\underbrace{1 \cdot 2^5}_{\text{id}} + \underbrace{4 \cdot 2^1}_{(1,2,3,4,5)\text{ etc.}} + \underbrace{5 \cdot 2^3}_{(1,3)(3,5)(4)\text{ etc.}}) = \frac{80}{10} = 8$

(3.10) Bemerkung $G \leq S_n$
$F := \{f : \{1,\dots,n\} \to A\}$ mit A endliche Menge, G operiert auf F via $(g \cdot f)(i) = f(g^{-1}i)$ für $g \in G$ und $f \in F$. Dann ist $|\mathrm{Fix}_F(g)| = |A|^k$, wenn g vom Zykeltyp $(\lambda_1,\dots,\lambda_k)$ ist. (Vorsicht: Einzykel zählen mit!) $k =$ Anzahl der Zykel.

Beispiel Färbungen eines Würfels. $M = \{1,2,3,4,5,6\}$.
Symmetriegruppe des Würfels: $W =< (1\,3\,4\,6), (4\,5\,6)(1\,2\,3) >\leq S_M = S_6$.
Färbungen: $\mathfrak{F} = \{f : M \to \{1,\dots,a\}\}$.

Gesucht: Anzahl der verschiedenen Färbungen der Seiten des Würfels mit a verschiedenen Farben. Dies entspricht der Anzahl der W-Bahnen auf $\mathfrak{F}$.

W besteht aus 24 Elementen:

# Elemente	Typ	Zykeltyp	# Bahnen auf M	# Fixpunkte auf $\mathfrak{F}$
1	id	$(1,1,1,1,1,1)$	6	a^6
6	90° (grün)	$(4,1,1)$	3	a^3
3	180° (grün)	$(2,2,1,1)$	4	a^4
6	180° (blau)	$(2,2,2)$	3	a^3
8	120° (rot)	$(3,3)$	2	a^2

(Achsen zwischen zwei gegenüberliegenden Quadraten (grün), Kanten (blau) und Ecken (rot).)

Anzahl der Bahnen: $p(a) = \dfrac{1}{24} \cdot (1a^6 + 6a^3 + 3a^4 + 6a^3 + 8a^2) = \frac{1}{24}(a^6 + 3a^4 + 12a^3 + 8a^2)$

a	1	2	3	4	5	6	7	...
$p(a)$	1	10	57	240	800	2226	5390	...

4 Siebformeln

Beispiel $A_1, A_2, A_3 \subseteq M$
$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cup A_2| - |A_1 \cup A_3| - |A_2 \cup A_3| + |A_1 \cup A_2 \cup A_3|$

(4.1) Satz (Siebformel) (engl. PIE = principal of inclusion and exclusion)
Sei M eine endliche Menge, $A_1, \dots, A_n \subseteq M$, $N := \{1, \dots, n\}$. Für $I \subseteq N$ sei $A_I := \bigcap_{i \in I} A_i$, $A_\emptyset := M$. Dann ist

$$|M \setminus \bigcup_{i \in N} A_i| = \sum_{I \subseteq \{1,\dots,n\}} (-1)^{|I|} |A_I|$$

äquivalente Formulierung:

$$|\bigcup_{i \in \{1,\dots,n\}} A_i| = - \sum_{\emptyset \neq I \subset \{1,\dots,n\}} (-1)^{|I|} |A_I|$$

Beweis. Sei $x \in M$. Bestimme „Beitrag“ von x auf linker bzw. rechter Seite.

$x \in M \setminus \bigcup_{i \in N} A_i$: linke Seite Beitrag 1, rechte Seite $x \in A_I \Leftrightarrow I = \emptyset$, Beitrag $(-1)^{|\emptyset|} = 1$

$x \in \bigcup_{i \in N} |A_i|$: Beitrag auf linker Seite ist 0. Beitrag auf rechter Seite:
Sei $J(x) = J = \{i \in N | x \in A_i\}$. Dann ist $x \in A_I \Leftrightarrow I \subseteq J$.

$$\sum_{I \subseteq J} (-1)^{|J|} = \sum_{i=0}^{j} \binom{j}{i} (-1)^i = \oplus$$

$$\text{mit } j = |J|, \binom{j}{i} = |\{I \subseteq J | |I| = i\}|$$

$$\oplus = (1-1)^j = 0 \quad (\text{da } j > 0 \text{ da } \exists i \text{ mit } x \in A_i)$$

□

Anwendungen:

(4.2) Satz $a := |\{f : \{1, \dots, n\} \to \{1, \dots, k\} | f \text{ ist surjektiv}\}|$
$= \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$
Insbesondere für $l = n$: $|S_n| = n! = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n$.

Beweis. Sei $M := \mathfrak{F}(k, n) = \{f : \{1, \dots, n\} \to \{1, \dots, k\}\}$ ($\Rightarrow |M| = k^n$). Für $i \in \{1, \dots, k\}$ sei $A_i = \{f \in M | i \notin f(\{1, \dots, n\})\} \leftrightarrow \{f : \{1, \dots, n\} \to \{1, \dots, k\} \setminus \{i\}\}$. $|A_i| = (k-1)^n$. Allgemeiner: $I \subseteq \{1, \dots, k\}$, $A_I = \bigcap_{i \in I} A_i \Rightarrow |A_I| = (k - |I|)^n$.
Also nach (4.1)

$$a = |M \setminus \bigcup_{i=1}^{k} A_i| = \sum_{I \subseteq \{1,\dots,k\}} (-1)^{|I|} (k - |I|)^n = \sum_{j=0}^{k} \binom{k}{j} (-1)^j (k-j)^n$$

□

(4.3) Satz Eine Permutation $\pi \in S_n$ heißt *fixpunktfrei* $:\Leftrightarrow \forall i \in \{1, \dots, n\}$ ist $\pi(i) \neq i$ (derangement).

Dann ist die Anzahl der fixpunktfreien Permutationen in $S_n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$ ($\leq n!$).

Beweis. $M = S_n, A_i := \{\pi \in S_n | \pi(i) = i\}$
Zählen: $|M \setminus \bigcup_{i\in\{1,\ldots,n\}} A_i|$
$|A_I| = |\bigcap_{i\in I} A_i| = |\{\pi \in S_n | \pi(i) = i \forall i \in I\}| = |S_{\{1,\ldots,n\}\setminus I}| = (n - |I|)!$
d.h. mit (4.1) ist

$$|M \setminus \bigcup_{i\in\{1,\ldots,n\}} A_i| = \sum_{I\subseteq\{1,\ldots,n\}} (-1)^{|I|}(n-|I|)! = \sum_{i=0}^{n} \binom{n}{i}(-1)^i(n-i)!$$
$$= \sum_{i=0}^{n}(-1)^i \frac{n!}{(n-i)!\cdot i!}(n-i)! = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$$

□

Verallgemeinerung:

(4.4) Satz Sei $N = \{1, \ldots, n\}, f, g : \mathrm{Pot}(N) \to \mathbb{R}$ Funktionen. Äquivalent sind:

(a) $g(I) = \sum_{J\supseteq I} f(J) \quad \forall I \subseteq N$

(b) $f(I) = \sum_{J\supseteq I} (-1)^{|J\setminus I|} g(J) \quad \forall I \subseteq N$

Beweis. Seien $A, B \in \mathbb{R}^{2^n\times 2^n}$ indiziert durch die Teilmengen von $\{1, \ldots, n\}$ ($|\mathrm{Pot}(\{1, \ldots, n\})| = 2^n$).

$$A_{I,J} := \begin{cases} 1 & \text{falls } I \subseteq J \\ 0 & \text{sonst} \end{cases} \quad \text{und } B_{I,J} := \begin{cases} (-1)^{|J\setminus I|} & \text{falls } I \subseteq J \\ 0 & \text{sonst} \end{cases}.$$

(a) übersetzt sich als $A \cdot \begin{pmatrix} f(\emptyset) \\ \vdots \\ f(N) \end{pmatrix} = \begin{pmatrix} g(\emptyset) \\ \vdots \\ g(N) \end{pmatrix}$ und

(b) heißt $B \cdot \begin{pmatrix} g(\emptyset) \\ \vdots \\ g(N) \end{pmatrix} = \begin{pmatrix} f(\emptyset) \\ \vdots \\ f(N) \end{pmatrix}$.

Zu zeigen ist $B = A^{-1}$, d.h. $A \cdot B = B \cdot A = E_{2^n}$.

$$(A\cdot B)_{I,J} = \underbrace{\sum_{K\subseteq N} A_{I,K}\cdot B_{K,J}}_{=0 \text{ falls } I\not\subseteq K \text{ oder } K\not\subseteq J} = \sum_{I\subseteq K\subseteq J} (-1)^{|J\setminus K|} = \oplus$$

Klar: $\oplus = 1$ falls $I = J$, zu zeigen: $\oplus = 0$ falls $I \subsetneq J$.
Mit Siebformel (4.1):

Sei $M = \{1\}, A_i = \{1\} \forall i \in J \setminus I =: L$

$$\underbrace{|M \setminus \bigcup_{i \in L} A_i|}_{=0} = \sum_{X \subseteq L} (-1)^{|X|} \underbrace{|A_X|}_{=1}$$

$$= \sum_{\substack{X \subseteq J \setminus I \\ (X = J \setminus K \subseteq J \setminus I)}} (-1)^{|X|} = \sum_{I \subseteq K \subseteq J} (-1)^{|J \setminus K|} = 0$$

□

(4.5) Folgerung

$$\sum_{I \subseteq K \subseteq J} (-1)^{|J \setminus K|} = \begin{cases} 0 & I \subsetneq J \\ 1 & I = J \end{cases}$$

Äquivalente Formulierung

(4.4') Satz $N = \{1, \ldots, n\}, f, g : \mathrm{Pot}(N) \to \mathbb{R}$. Äquivalent sind

(a) $g(I) = \sum_{J \subseteq I} f(J) \quad \forall I \subseteq N$

(b) $f(I) = \sum_{J \subseteq I} (-1)^{|I \setminus J|} g(J) \quad \forall I \subseteq N$

Beweis. Analog zu (4.4) oder setze $f'(X) := f(N \setminus X), g'(X) := g(N \setminus X)$ und benutze (4.4) für f' und g' und benutze $Y \subseteq X \Leftrightarrow N \setminus Y \supseteq N \setminus X$. □

Anwendungen:

(4.6) Folgerung Seien $f, g : \{0, \ldots, n\} \to \mathbb{R}$. Äquivalent sind

(a) $g(i) = \sum_{j=0}^{i} \binom{i}{j} f(j) \quad \forall i \in \{0, \ldots, n\}$

(b) $f(i) = \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} g(j) \quad \forall i \in \{0, \ldots, n\}$

Beweis. Definiere $G, F : \mathrm{Pot}(\{1, \ldots, n\}) \to \mathbb{R}$ durch $G(I) = g(|J|)$ bzw. $F(I) = f(|I|)$ und wende (4.4') an:
$\binom{i}{j} = |\{J \subseteq I || J| = j\}|$ falls $|I| = i$. Sei $|I| = i \Rightarrow G(I) = g(i) \overset{(4.4')(a)}{=} \sum_{J \subseteq I} F(J) = \sum_{j=0}^{i} \binom{i}{j} f(j)$ d.h. (4.4') für F und G ist äquivalent zu (4.6)(a) für f, g. Ebenso (4.4')(b) für F und G ist äquivalent zu (4.6)(b) für f, g. □

(4.7) Folgerung (Inverse des Pascalschen Dreiecks) Seien $A, B \in \mathbb{R}^{(n+1) \times (n+1)}$ mit Zeilen- und Spaltenindizes in $\{0, \ldots, n\}$ definiert durch

$A_{i,j} = \begin{cases} \binom{i}{j} & j \leq i \\ 0 & j > i \end{cases}$, $B_{i,j} = \begin{cases} (-1)^{i+j} \binom{i}{j} & j \leq i \\ 0 & j > i \end{cases}$. Dann gilt $B = A^{-1}$.

Beispiel $n = 3$

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 & \\ -1 & 1 & 0 & 0 \\ 1 & -2 & 1 & 0 \\ -1 & 3 & -3 & 1 \end{pmatrix} = A^{-1}$$

Beweis. (4.7): (4.6) sagt aus:

für $f = \begin{pmatrix} f(0) \\ \vdots \\ f(n) \end{pmatrix} \in \mathbb{R}^{n+1}$ und $g = \begin{pmatrix} g(0) \\ \vdots \\ g(n) \end{pmatrix} \in \mathbb{R}^{n+1}$ gilt $g = A \cdot f \Leftrightarrow f = B \cdot g$ d.h. $A = B^{-1}$ bzw. $B = A^{-1}$. □

5 Partiell geordnete Mengen und Möbiusinversion

(5.1) Definition Eine *partiell geordnete Menge* (engl. poset = partially ordered set) p.g.M. $(M, \leq)$ ist eine Menge M mit einer Relation $\leq (\subseteq M \times M = \{(x, y) | x, y \in M\})$ $(x, y) \in \leq \Leftrightarrow x \leq y$ wenn gilt:

(i) $x \leq x \quad \forall x \in M$ (reflexiv)

(ii) $x \leq y$ und $y \leq x \Rightarrow x = y$ (antisymmetrisch)

(iii) $x \leq y$ und $y \leq z \Rightarrow x \leq z$ (transitiv)

Beispiel

- $(\mathbb{R}, \leq)$ ist p.g.M. (sogar totalgeordnete Menge, d.h. $\forall x, y \in \mathbb{R}$ gilt $x \leq y$ oder $y \leq x$)
- N Menge $\Rightarrow (\mathrm{Pot}(N), \subseteq)$ ist p.g.M. (keine Totalordnung: $\{1\} \not\subseteq \{2\}$ und $\{2\} \not\subseteq \{1\}$)

(5.2) Satz Sei $(M, \trianglelefteq)$ partiell geordnete Menge.
Dann existiert eine Totalordnung $\trianglelefteq'$ mit $x \trianglelefteq y \Rightarrow x \trianglelefteq' y \; \forall x, y \in M$.
Analoge Formulierung: Man kann M so nummerieren $M = \{m_1, \ldots, m_n\}$, dass $m_i \trianglelefteq m_j \Rightarrow i \leq j$.
Totalordnung $\trianglelefteq'$: $m_1 \trianglelefteq' m_2 \trianglelefteq' m_3 \trianglelefteq' \ldots$

Beweisskizze zu (5.2):
Angenommen $\trianglelefteq$ ist noch keine Totalordnung. Dann gibt es $a, b \in M$ mit $a \not\trianglelefteq b$ und $b \not\trianglelefteq a$
Setze $\trianglelefteq' : a \trianglelefteq b$ (Auswahlmöglichkeit, nicht eindeutig!) und schliesse transitiv ab:
$x \trianglelefteq' y :\Leftrightarrow$ entweder $x \trianglelefteq y$ oder $x \trianglelefteq a$ und $b \trianglelefteq y$ (Zeige: $\trianglelefteq'$ ist transitiv, reflexiv und antisymmetrisch), mache weiter mit $\trianglelefteq'$ anstelle von $\trianglelefteq$ (hört auf, falls M endlich).
Achtung: $\trianglelefteq'$ ist nicht eindeutig bestimmt.

(5.3) Definition Sei $M = (\{m_1, \ldots, m_n\}, \trianglelefteq)$ p.g.M. mit $m_i \trianglelefteq m_j \Rightarrow i \leq j$
$I(M) := \{A \in \mathbb{R}^{n\times n} | A_{ij} \neq 0 \Rightarrow m_i \trianglelefteq m_j\}$ heißt die *Inzidenzalgebra* von $(M, \trianglelefteq)$.

Beispiel $M = \{1, \ldots, n\}$, $\trianglelefteq = \leq$
$\Rightarrow I(M) = \mathbb{R}^{n\times n}_{\trianglelefteq} = \{A \in \mathbb{R}^{n\times n} | A_{ij} = 0 \text{ falls } i > j\}$
$$= \begin{pmatrix} \mathbb{R} & \cdots & \mathbb{R} \\ & \ddots & \vdots \\ 0 & & \mathbb{R} \end{pmatrix} = \text{obere Dreiecksmatrix}$$
Für $A \in I(M)$ schreiben wir auch $A(m_i, m_j) := A_{ij}$
$A \in I(M) \Leftrightarrow (A(m,n) \neq 0 \Rightarrow m \trianglelefteq n \forall m, n \in M)$
Matrixmultiplikation: In $I(M)$ übersetzt sich als:
$$(A \cdot B)(m,n) = \sum_{z\in M,\ m\trianglelefteq z \text{ und } z\trianglelefteq n} A(m,z)B(z,n) \neq 0, \text{ falls } m \trianglelefteq n$$
Also ist $I(M)$ abgeschlossen unter Matrixmultiplikation, Matrixaddition und Multiplikation mit Skalaren ($\in \mathbb{R}$) (sogenannte Algebra).

(5.4) Beispiel Wichtige Funktionen in $I(M)$

(i) $e \in I(M)$ $\quad e \leftrightarrow \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$$e(x,y) = \begin{cases} 1 & \text{falls } x = y \\ 0 & \text{sonst} \end{cases} \quad \forall x, y \in M$$

(ii) $\iota_{\trianglelefteq}$ charakteristische Funktion von $\trianglelefteq$

$$\iota_{\trianglelefteq}(x,y) = \begin{cases} 1 & \text{falls } x \trianglelefteq y \\ 0 & \text{sonst} \end{cases} \quad \forall x, y \in M$$

(iii) $\mu_{\trianglelefteq} = (\iota_{\trianglelefteq})^{-1}$ (inverse Matrix) ist rekursiv definiert durch

$$\sum_{x\trianglelefteq z\trianglelefteq y} \mu_{\trianglelefteq}(x,z) = \begin{cases} 1 & \text{falls } x = y \\ 0 & \text{sonst} \end{cases}$$

(5.5) Bemerkung $A \in I(M)$ invertierbar in $I(M) \Leftrightarrow A \in \mathbb{R}^{n\times n}$ invertierbar
$\Leftrightarrow \det(A) \neq 0 \Leftrightarrow \forall m \in M$ ist $A(m,m) \neq 0$
Dann liegt auch die inverse Matrix A^{-1} wieder in $I(M)$.

$$A^{-1}_{ij} = \begin{cases} 0 & \text{falls } m_i \not\trianglelefteq m_j \\ A(m_i, m_j)^{-1} & \text{falls } i = j \\ * & \text{falls } m_i \trianglelefteq m_j \end{cases}$$

Wobei $*$ rekursiv definiert ist durch

$$* = A(m_i, m_j)^{-1} \cdot \sum_{m_i\trianglelefteq z\trianglelefteq m_j (m_i \neq z)} A(m_i, z) \cdot A(z, m_j)^{-1}$$

(5.6) Bemerkung $\mu_{\trianglelefteq}(x,y) \in \mathbb{Z} \forall x,y \in M$ denn $\mu_{\trianglelefteq} = (\iota_{\trianglelefteq})^{-1}$ und $\iota_{\trianglelefteq} \in \mathbb{Z}^{n\times n}$ und $\det(\iota_{\trianglelefteq}) = 1$ plus Cramersche Regel.

(5.7) Satz Seien $f, g \in I(M)$. Äquivalent sind

(a) $f(x,y) = \sum\limits_{x\trianglelefteq z\trianglelefteq y} (g(x,z)\iota_{\trianglelefteq}(z,y))$
$= \sum\limits_{x\trianglelefteq z\trianglelefteq y} g(x,z)$ (da $\iota_{\trianglelefteq}(z,y) = 1$ für $z \trianglelefteq y$) $\forall x,y \in M$

(b) $g(x,y) = \sum\limits_{x\trianglelefteq z\trianglelefteq y} (f(x,z)\cdot\mu(z,y)) \; \forall x,y \in M$

Beweis. (a) sagt aus $f = g \cdot \iota_{\trianglelefteq}$
(b) sagt aus $g = f \cdot \mu_{\trianglelefteq} = f(\iota_{\trianglelefteq})^{-1}$, also Aussage klar. □

Beispiel 1. $M = \{1,\dots,n\}, \trianglelefteq = \leq$

$$\Rightarrow \iota_{\leq} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ & \ddots & \ddots & \ddots & 1 \\ & & \ddots & \ddots & 1 \\ & & & \ddots & 1 \\ 0 & & & & 1 \end{pmatrix} \in \mathbb{R}^{n\times n}$$

$$\mu_{\trianglelefteq} = (\iota_{\trianglelefteq})^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ & \ddots & -1 \\ 0 & & 1 \end{pmatrix}$$

2. $M = \mathrm{Pot}(\{1,\dots,n\}), \trianglelefteq = \subseteq$

$$\iota_{\subseteq}(I,J) = \begin{cases} 1 & I \subseteq J \\ 0 & \text{sonst} \end{cases}$$

$$\mu_{\subseteq}(I,J) = \begin{cases} (-1)^{|I\setminus J|} & I \subseteq J \\ 0 & \text{sonst} \end{cases}$$

Beweis. $\iota_{\subseteq} \cdot \mu_{\subseteq} = e$ (zu zeigen)

d.h. $\sum\limits_{K,\, I\subseteq K\subseteq J} \iota_{\subseteq}(I,K)\cdot\mu_{\subseteq}(I,K) = \sum\limits_{I\subseteq K\subseteq J} (-1)^{|J\setminus K|} \underbrace{=}_{(4.5)} \begin{cases} 1 & I = J \\ 0 & \text{sonst} \end{cases}$ □

3. $M = \mathbb{N}_{\geq 1} = \{n \in \mathbb{N} | n \geq 1\}$
$a \trianglelefteq b \Leftrightarrow a|b$

$$\iota_{\text{teilt}}(a,b) = \begin{cases} 1 & a|b \\ 0 & \text{sonst} \end{cases}$$

$$\mu_{\text{teilt}}(a,b) = \begin{cases} 0 & \text{falls } a \nmid b \\ 0 & b/a \text{ durch } p^2 \text{ teilbar für Primzahl } p \\ (-1)^s & b/a = p_1\cdot p_2\cdots p_s \text{ mit paarw. versch. Primzahlen } p_1,p_2,\dots,p_s \\ 1 & \text{falls } b = a \end{cases}$$

Bemerkung Die Funktion $\mu : \mathbb{N}_{\geq 1} \to \{0, 1, -1\}$ mit

$$\mu(d) := \mu_{\text{teilt}}(1, d) = \begin{cases} 1 & d = 1 \\ (-1)^s & d = \prod_{i=1}^{s} p_i \text{ mit paarw. verschiedenen Primzahlen} \\ 0 & \text{sonst} \end{cases}$$

ist die klassische Möbiusfunktion der Zahlentheorie.

(5.8) Folgerung (Möbiusinversion, klassisch) Seien $f, g : \mathbb{N}_{\geq 1} \to \mathbb{R}$. Äquivalent sind

(a) $f(n) = \sum_{d|n} g(d) \qquad \forall n \in \mathbb{N}_{\geq 1}$

(b) $g(n) = \sum_{d|n} f(d) \cdot \mu\left(\frac{n}{d}\right) \qquad \forall n \in \mathbb{N}_{\geq 1}$

Beispiel $M = \{1, 2, 3, 4, 5, 6\}$, $\trianglelefteq$ teilt.
Charakteristische Matrix, $A^{-1} \widehat{=} \mu_{\text{teilt}}$

$$\left(\begin{array}{cccccc|cccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Bringe $(A|I_6)$ durch Zeilenumformungen auf die Form $(I_6|B)$. Dann ist $B = A^{-1}$ und beschreibt μ_{teilt}.

$$\left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Teil II

Graphentheorie

6 Graphen

(6.1) Definition (i) Ein *ungerichteter Graph* $G = (V, E, f)$ besteht aus nichtleeren disjunkten Mengen V (vertices bzw. Ecken oder Knoten) und E (edges bzw. Kanten) sowie einer Funktion $f : E \to \{\{x, y\} | x, y \in V\}$.

(ii) Zwei Graphen $G_1 = (V_1, E_1, f_1)$ und $G_2 = (V_2, E_2, f_2)$ heißen *isomorph* genau dann, wenn eine Bijektion $\beta : V_1 \to V_2$ existiert, so dass für alle $v, w \in V_1$ gilt $|f_1^{-1}(\{\{v, w\}\})| = |f_2^{-1}(\{\{\beta(v), \beta(w)\}\})|$

(iii) Eine endliche Folge $K = (v_0 e_1 v_1 e_2 v_2 \dots e_n v_n)$ mit $v_i \in V$, $e_j \in E$ heißt *Kantenzug*, falls $f(e_i) = \{v_{i-1}, v_i\}$ für alle $i \in \{1, \dots, n\}$.

- K heißt *offen* $:\Leftrightarrow v_0 \neq v_n$
- K heißt *geschlossen* $:\Leftrightarrow v_0 = v_n$
- K heißt *Weg* $:\Leftrightarrow v_i \neq v_j \; \forall i \neq j$
- K heißt *Kreis* $:\Leftrightarrow v_i \neq v_j \; \forall i \neq j, \; 1 \leq i, j \leq n$ und $v_0 = v_n$

Ein geschlossener Kantenzug $(v_0 e_1 v_1 \dots e_n v_n)$ heißt *Eulertour* $:\Leftrightarrow |E| = n$ und $E = \{e_1, \dots, e_n\}$ (jede Kante kommt genau einmal vor).

(iv) G heißt *endlich* $:\Leftrightarrow |V| < \infty$ und $|E| < \infty$. $A \in \mathbb{N}^{V \times V}$ mit $A_{v,w} = |f^{-1}(\{\{v, w\}\})|$ die *Adjazenzmatrix* von G.

(v) G heißt *zusammenhängend*, falls je zwei Ecken durch einen Kantenzug miteinander verbunden sind. Die Relation „$v \sim w \Leftrightarrow \exists$ Kantenzug in G der $v, w \in V$ verbindet“ ist eine Äquivalenzrelation. Die Äquivalenzklassen heißen *Zusammenhangskomponenten* von G.

(vi) Der *Grad* einer Ecke ist die Anzahl der von ihr ausgehenden Kanten: $v \in V$
$s(v) = |\{e \in E | f(e) = \{v\}\}|$ (Anzahl der Schlingen)
$t(v) = |\{e \in E | \exists w \neq v, w \in V \text{ mit } f(e) = \{v, w\}\}|$
$d(v) := t(v) + 2 \cdot s(v)$ ist der *Grad* von v.

(6.2) Satz Ein zusammenhängender endlicher Graph hat genau dann eine Eulertour, wenn $d(v)$ gerade ist für alle $v \in V$.

Beweis. „$\Rightarrow$“ Sei $(v_0 e_1 v_1 e_2 \dots e_n v_n = v_0)$ eine Eulertour d.h. $E = \{e_1, \dots, e_n\}$, $|E| = n$, jede Kante (die zu $d(v)$ beiträgt) kommt genau einmal vor.

e_1, e_n tragen beide 1 zu $d(v_0)$ bei, e_{i-1}, e_i tragen beide 1 zu $d(v_{i-1})$ bei)
$\Rightarrow d(v)$ gerade für alle $v \in V$.

„$\Leftarrow$“ Sei $d(v)$ gerade für alle $v \in V$.
Konstruiere Eulertour: Starte bei beliebigem $v \in V$. Arbeite zunächst alle Schlingen $e \in E$ ab mit $f(e) = \{v\}$, $K = (ve_1ve_2v \dots e_sv)$. Wähle beliebiges $w \in V$ mit $f^{-1}(\{\{v, w\}\} \neq \emptyset$ d.h. es existiert eine Kante zwischen v und w. Verlängere $K = (ve_1 \dots e_sve_{s+1}w)$.

Behauptung: Ist $w \neq v$ so gibt es $e \in E$ mit $w \in f(e)$ (es gibt eine Kante e (die bisher nicht benutzt wurde), die von w ausgeht).

e_{s+1} trägt 1 zu $d(w)$ bei, $d(w) - 1 \neq 0$ da $d(w)$ gerade d.h. es existiert e_{s+2} mit $w \in f(e_{s+2}) = \{w, x\}$. $K = (ve_1 \dots e_{s+1}we_{s+2}x)$.

Behauptung: Dies konstruiert eine Eulertour.

Achtung: nicht immer. Es kann passieren, dass $x = v$ ist und keine Kanten von x aus übrig bleiben.
Dann: neue Eulertour im Restgraph konstruieren.

Beachte: Für jede Ecke $\neq v = v_0$ die im Verlauf des Algorithmus besucht wird bleibt immer noch eine ungerade Anzahl von Kanten übrig, die von ihr ausgehen.
Wenn man also nicht mehr weiterkommt, so ist man wieder bei $v = v_0$ angekommen.
Hat man nicht alle Kanten verbraucht, so haben die Ecken im verbleibenden Graphen wieder alle geraden Grad und man kann geschlossene Kantenzüge so einfügen, dass am Ende eine Eulertour entsteht.

□

7 Bäume und Wälder

(7.1) Definition (i) Ein Graph ohne Kreise ist ein *Wald*. Ein zusammenhängender Wald ist ein *Baum*.

(ii) Für einen endlichen Graphen $G = (V, E, f)$ sei $\mu(G) = |E| - |V| +$ #Zusammenhangskomponenten von G der Index von G.

(7.2) Satz Ist G ein Baum, so ist $\mu(G) = 0$.

Beweis. Ein Baum hat genau eine Ecke mehr als Kanten.
Baum: neue Kante hinzufügen genau dann, wenn neue Ecke hinzugefügt. □

(7.3) Satz Jeder zusammenhängende Graph $G(V, E, f)$ hat einen *aufspannenden Baum* $T = (V, E', f_{|E'})$ d.h. einen zusammenhängenden Teilgraphen mit gleichen Ecken der keine Kreise besitzt.

Beweis. In jedem Kreis in G lasse eine Kante Weg. □

(7.4) Folgerung G endlicher Graph $\Rightarrow \mu(G) \geq 0$ und $\mu(G) = 0 \Leftrightarrow G$ ist Wald.

Bemerkung Vergleiche mit Konstruktion einer Basis eines Vektorraums durch Weglassen „abhängiger“ Vektoren aus einem Erzeugendensystem.

Umgekehrt: $\mathcal{E} = \{v_1, \ldots, v_n\}$ Erzeugendensystem, aus $\mathcal{E}$ Basis B auswählen.
$v_1 \in B$, falls $v_1 \neq 0$ ((v_1) nicht linear abhängig)
$v_2 \in B$, falls (v_1, v_2) linear unabhängig
$\vdots$
maximal linear unabhängige Teilmenge auch Basis.

Ebenso: Konstruktion eines aufspannenden Baumes in zusammenhängenden Graphen V, $E' = \emptyset$ füge neue $e \in E$ zu E' hinzu solange keine Kreise entstehen.

(7.5) Definition (bewerteter Graph) (i) Ein *bewerteter Graph* ist ein ungerichteter Graph $G = (V, E, f)$ mit einer *Kostenfunktion* $\alpha : E \to \mathbb{R}_{>0}$, $\alpha(e) =$ Kosten für die Kante $e \in E$.

(ii) Ein zusammenhängender Teilgraph $T = (V, E', f_{|E'})$ in einem bestimmten Graphen $G = (V, E, f, \alpha)$ heißt *minimaler aufspannender Teilgraph*, falls $\sum_{e \in E'} \alpha(e)$ minimal ist unter allen zusammenhängenden aufspannenden Teilgraphen.

(7.6) Satz Jeder minimale aufspannende Teilgraph $T = (V, E' f_{|E'})$ ist ein aufspannender Baum.

Beweis. Sonst kann man Kanten in E' weglassen, so dass T zusammenhängend bleibt und damit $\sum_{e \in E'} \alpha(e)$ verkleinert. □

(7.7) Algorithmus (Finden eines minimal aufspannenden Teilgraphen)
Gegeben: $G = (V, E', f)$, $\alpha : E \to \mathbb{R}_{>0}$, G zusammenhängend.
Gesucht: $T = (V, E', f_{|E'})$ zusammenhängend mit $\sum_{e \in E'} \alpha(e)$ minimal.
Init: $E' = \emptyset$, $T = (V, E', f_{|E'})$
Algorithmus:

- Setze $\widetilde{E} = \{e \in E | f(e) = \{x, y\}$ mit x, y liegen in verschiedenen zusammenhängenden Komponenten von $T\}$.
- Wähle $e \in \widetilde{E}$ mit $\alpha(e) = \min\{\alpha(\tilde{e}) | \tilde{e} \in \widetilde{E}\}$.
- Setze $E' := E' \cup \{e\}$ und wiederhole bis $\widetilde{E} = \emptyset$.

(7.8) Satz Algorithmus (7.7) endet nach $|V| - 1$ Schritten und produziert einen minimal zusammenhängenden Teilgraphen T.

Beweis. Der Algorithmus endet: Die Anzahl der Zusammenhangskomponenten von T verringert sich in jedem Schritt um eins. Das heißt, am Anfang haben wir $|V|$ Zusammenhangskomponenten, am Ende eine.

Minimalität: Sei $T = (V, E', f_{|E'})$ der vom Algorithmus produzierte Teilgraph und $E' = \{e_1, \ldots, e_{n-1}\}$ in der Reihenfolge, wie die Kanten im Algorithmus gewählt werden. Dann ist $\alpha(e_1) \leq \alpha(e_2) \leq \cdots \leq \alpha(e_{n-1})$.

Angenommen, es existiere ein aufspannender Baum $T' = (V, F, f_{|F})$ mit kleineren Kosten $\sum_{e \in F} \alpha(e) \leq \sum_{e \in E'} \alpha(e)$ und sei $F = \{f_1, \ldots, f_{n-1}\}$ so geordnet, dass $\alpha(f_1) \leq \alpha(f_2) \leq \cdots \leq \alpha(f_{n-1})$ mit $n = |V|$.

Wir wissen: $\sum_{i=1}^{m-1} \alpha(f_i) \lneqq \sum_{i=1}^{n-1} \alpha(e_i)$.

Sei k minimal mit $\sum_{i=1}^{k} \alpha(f_i) < \sum_{i=1}^{k} \alpha(e_i)$.

Dann ist $k \geq 2$, da $\alpha(e_1)$ minimal gewesen war und $\sum_{i=1}^{k-1} \alpha(f_i) \geq \sum_{i=1}^{k-1} \alpha(e_i)$ und daher $\alpha(f_1) \leq \cdots \leq \alpha(f_{k-1}) \leq \alpha(f_k) < \alpha(e_k)$.

Jetzt wählt der Algorithmus e_k im Schritt k und keines der $f_1, \ldots, f_k$ obwohl sie kleinere Kosten haben.

Setzt man $T_1 = (V, \{e_1, \ldots, e_{k-1}\}, f_{|\{e_1,\ldots,e_{k-1}\}})$ und $T_1' := (V, \{f_1, \ldots, f_k\}, f_{|\{f_1,\ldots,f_k\}})$ so sind beides Wälder.

Anzahl der Zusammenhangskomponenten $T_1 = |V| - (k-1) >$ Anzahl der Zusammenhangskomponenten $T_1' = |V| - k$.

$f_1, \ldots, f_k \notin \widetilde{E}$ im Schritt k, d.h. keines der f_i $(1 \leq i \leq k)$ verbindet zwei verschiedene Zusammenhangskomponenten von T_1

$\Rightarrow$ Widerspruch, da die Anzahl der Zusammenhangskomponenten $T_1' \lneqq$ Anzahl der Zusammenhangskomponenten T_1. $\square$

Teil III

Algebraische Strukturen

8 Ringe und Ideale

Beispiel $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ Ring der ganzen Zahlen (mit den Verknüpfungen $+$ und $\cdot$).

$K[X] = \{\sum_{i=0}^{n} a_i x^i | a_i \in K, n \in \mathbb{N}\}$ ist ein *Polynomring* mit den Verknüpfungen

$$\left(\sum a_i x^i\right) + \left(\sum b_j x^j\right) = \sum (a_i + b_i) x^i$$

$$\left(\sum a_i x^i\right) \cdot \left(\sum b_j x^j\right) = \sum c_k x^k \qquad \text{mit } c_k = \sum_{i=0}^{k} a_i \cdot b_{k-i}$$

Darstellung im Rechner

$$\sum_{i=0}^{n} a_i x^i \rightsquigarrow (a_0, a_1, \dots, a_n, 0, \dots)$$

Addition also Komponentenweise:

$$(a_0, a_1, \dots, a_n, 0, \dots, 0) + (b_0, b_1, \dots, b_m, 0, \dots, 0) = (a_0 + b_0, a_1 + b_1, \dots)$$

Multiplikation ist also Shift-Operation:

$$x \cdot (a_0, a_1, \dots, a_n, 0, \dots, 0) = (0, a_0, a_1, a_2, \dots, a_n, 0, \dots, 0)$$

$$\begin{aligned}\left(\sum b_j x^j\right) \cdot (a_0, a_1, \dots, a_n, 0, \dots, 0) = {} & (b_0 a_0, b_0 a_1, \dots, b_0 a_n, 0, \dots, 0) \\ & + (0, b_1 a_0, b_1 a_1, \dots, b_1 a_n, 0, \dots, 0) \\ & + (0, 0, b_2 a_0, \dots) \\ & + \dots \\ & + (0, 0, \dots, 0, b_m a_0, b_m a_1, \dots)\end{aligned}$$

Dadurch kann man erkennen, dass Polynome etwas anderes als Polynomfunktionen sind.

(8.1) Definition (a) Ein *Ring* $A = (A, +, \cdot)$ ist eine Menge A zusammen mit zwei Verknüpfungen $+ : A \times A \to A$, $\cdot : A \times A \to A$ mit

(i) $(A, +)$ ist *abelsche Gruppe*, d.h. $(A, +)$ ist Gruppe und es gilt $a + b = b + a \; \forall a, b \in A$

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \; \forall a, b, c \in A$ und $\exists 1 \in A$ mit $1 \cdot a = a \cdot 1 = a \; \forall a \in A$

(iii) Distributivgesetz: $(a + b) \cdot c = ac + bc$ und $a \cdot (b + c) = ab + ac \; \forall a, b, c \in A$

(b) $(A, +, \cdot)$ heißt *kommutativ* $\Leftrightarrow ab = ba \; \forall a, b \in A$
Bemerkung: $(A, \cdot)$ ist im Allgemeinen keine Gruppe, z.B. $(\mathbb{Z}, \cdot)$ ist zwar assoziativ, aber $2^{-1} \notin \mathbb{Z}$, d.h. $\forall a \in \mathbb{Z}$ ist $a \cdot 2 \neq 1$ (2 hat kein Inverses).

(c) Ist $(A, +, \cdot)$ ein Ring, so heißt $A^* = \{a \in A | \exists b \in A \text{ mit } a \cdot b = b \cdot a = 1\}$ die *Einheitengruppe* von A.

(d) $(A, +, \cdot)$ heißt *Körper*, falls A kommutativer Ring, $1 \neq 0$ und $A^* = A \setminus \{0\}$.

(e) $a \in A$ heißt *Nullteiler*, falls $a \neq 0$ und $\exists b \in A, b \neq 0$ mit $a \cdot b = 0$.
Ein kommutativer Ring ohne Nullteiler heißt *Integritätsbereich*.

(f) Sind A und B Ringe so heißt eine Abbildung $\varphi : A \to B$ ein *Ringhomomorphismus* $\Leftrightarrow \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \; \forall a_1, a_2 \in A$ und $\varphi(b_1 \cdot b_2) = \varphi(b_1) \cdot \varphi(b_2) \; \forall b_1, b_2 \in A$ sowie $\varphi(1) = 1$.
Ein Ringhomomorphismus heißt Isomorphismus, falls er bijektiv ist. Dann ist $A \cong B$ (A und B sind *isomorph*).

(g) Eine Teilmenge $I \subseteq A$ heißt *Ideal* $(I \trianglelefteq A) :\Leftrightarrow (I, +) \leq (A, +)$ (Untergruppe) und $\forall a \in A, i \in I$ ist $a \cdot i \in I$ und $i \cdot a \in I$.

Beispiel (Einheitengruppe)
- $\mathbb{Z}^* = \{1, -1\}$
- $(K[X])^* = K^* = \{(a_0, 0, \ldots, 0) \mid a_0 \in K^*\}$

Beispiel (Körper) $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q} = \{\frac{a}{b} | a, b \in Z, b \neq 0\}$. $\mathbb{F}_2 = \{0, 1\}$ mit $1 + 1 = 0$. $\mathbb{F}_2^* = \{1\} = \mathbb{F}_2 \setminus \{0\}$.

Beispiel (Integritätsbereich)
- $\mathbb{Z}$ ist Integritätsbereich
- K Körper $\Rightarrow K$ ist Integritätsbereich:
  $a, b \in K \setminus \{0\}, a \cdot b = 0 \Rightarrow b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$ Widerspruch zu $b \neq 0$.
- K Körper $\Rightarrow K[X]$ Integritätsbereich:
  $(a_0, a_1, \ldots, a_n, 0, \ldots, 0) \cdot (b_0, b_1, \ldots, b_m, 0, \ldots, 0) = (c_0, c_1, \ldots, c_{n+m}, 0, \ldots, 0)$ mit $c_{c+m} = a_n \cdot b_m \neq 0$ falls $a_n \neq 0 \neq b_m$. Definiert man für $a \in K[X], a \neq 0$ den Grad $\text{Grad}(a) = \deg(a) := \max\{n \in \mathbb{N} | a_n \neq 0\}$ dann gilt $\text{Grad}(a \cdot b) = \text{Grad}(a) + \text{Grad}(b)$.

Beispiel (Ringhomomorphismus) V sei K-Vektorraum der Dimension n. $\mathrm{End}(V) = \{f : V \to V | f \text{ ist } K\text{-linear}\}$ ist ein Ring: $(f+g)(v) = f(v) + g(v)$, $(f \cdot g)(v) = f(v) \cdot g(v)$.
Ist $B = (v_1, \ldots, v_n)$ eine Basis von V so ist $M_B : \mathrm{End}(V) \to K^{n \times n} : f \mapsto M_B(f)$ ein Ringhomomorphismus (Ergmöglicht das Rechnen in $\mathrm{End}(V)$).

Definition Ist A ein kommutativer Ring, $n \in A$ so ist
$(n) := n \cdot A := \{n \cdot a | a \in A\} \trianglelefteq A$ das von n *erzeugte Hauptideal*.

Beweis. $(n) \leq (A, +)$ denn $0 \in (n)$ und für $n \cdot a$ und $n \cdot b$ aus (n) gilt:

$$\Rightarrow n \cdot a + n \cdot b = n(a+b) \in (n)$$
$$n \cdot a - n \cdot b = n \cdot (a-b) \in (n)$$

Ist jetzt $a \in A$, $n \cdot b \in (n) \Rightarrow a \cdot (n \cdot b) = n(a \cdot b) \in I$ und $(n \cdot b) \cdot a = n \cdot (b \cdot a) \in I$. □

Beispiel

- $A = \mathbb{Z}$, $n \in \mathbb{Z}$
  $(n) = n\mathbb{Z} = \{n \cdot a | a \in \mathbb{Z}\} \trianglelefteq \mathbb{Z}$ (Menge aller durch n teilbaren Zahlen).

- $\varphi : A \to B$ Ringhomomorphismus $\Rightarrow \mathrm{Kern}(\varphi) = \{a \in A | \varphi(a) = 0\} \trianglelefteq A$.

  Beweis. $\mathrm{Kern}(\varphi) \leq (A, +)$ als Kern eines Gruppenhomomorphismus $\varphi : (A, +) \to (B, +)$.
  Sind $i \in \mathrm{Kern}(\varphi)$ und $a \in A$ so sind auch $a \cdot i$ und $i \cdot a$ in $\mathrm{Kern}(\varphi)$:
  $\varphi(a \cdot i) = \varphi(a) \cdot \varphi(i) = \varphi(a) \cdot 0 = 0 \Rightarrow a \cdot i \in \mathrm{Kern}(\varphi)$
  $\varphi(i \cdot a) = \varphi(i) \cdot \varphi(a) = 0 \cdot \varphi(a) = 0 \Rightarrow i \cdot a \in \mathrm{Kern}(\varphi)$ □

(8.2) Bemerkung (a) $I \trianglelefteq A$, $J \trianglelefteq A \Rightarrow I \cap J \trianglelefteq A$

(b) $I \trianglelefteq A$ mit $I \cap A^* \neq \emptyset \Rightarrow I = A$

Beweis. Sei $a \in I \cap A^*$, $b \in A$ beliebig. Zu zeigen: $b \in I$.
$b = b \cdot 1 = \underbrace{(b \cdot a^{-1})}_{\in A} \cdot \underbrace{a}_{\in I} \in I$ □

Restklassenringe

(8.3) Bemerkung Sei R Ring, $(I, +) \leq (R, +)$.
Dann operiert die Gruppe I auf der Menge R durch $I \times R \to R, (i, r) \mapsto i + r$.
R ist disjunkte Vereinigung von Bahnen. Bahn von $r \in R = r + I = \{r + i | i \in I\} =: [r]_I$.
Für $a, b \in R$ gilt: a, b liegen in der selben Bahn $\Leftrightarrow [a]_I = [b]_I \Leftrightarrow a + I = b + I \Leftrightarrow a - b \in I$.
Bahnengleichheit definiert eine Äquivalenzrelation auf R: $a \equiv_I b \Leftrightarrow [a]_I = [b]_I \Leftrightarrow a - b \in I$ $R/I := \{[a]_I | a \in R\} = R/_{\equiv_I}$ Menge der Äquivalenzklassen.

Errinerung: M Menge, $\sim$ heißt *Äquivalenzrelation* auf M falls $\forall x, y, z \in M$:

(i) symmetrisch: $x \sim y \Leftrightarrow x \sim y$

(ii) reflexiv: $x \sim x$

(iii) transitiv: $x \sim y, y \sim z \Rightarrow x \sim z$

Beispiel
- „=“ Gleichheit ist Äquivalenzrelation.
- Bildgleichheit ist Äquivalenzrelation: Sei $f : M \to N$. $\sim_f$ Äquivalenzrelation, $a \sim_f b \Leftrightarrow f(a) = f(b)$. Äquivalenzklassen: Fasern von $f = \{f^{-1}(\{n\}) | n \in \text{Bild}(f)\}$.

(8.4) Satz Sei R (kommutativer) Ring, $I \trianglelefteq R$ Ideal.
$\Rightarrow$ R/I ist Ring mit $[a]_I + [b]_I = [a+b]_I$ und $[a]_I \cdot [b]_I = [a \cdot b]_I$. R/I heißt *Restklassenring.*

Beweis. Zu zeigen: R/I ist Ring.
Ringgesetze (Assoziativitätsgesetz, Kommutitativitätsgesetz, Distributivgesetz, ...) folgen direkt aus denen von R.
Wesentlich hier: Wohldefiniertheit von $+$ und $\cdot$: also Unabhängigkeit von der Wahl der Vertreter $a \in [a], b \in [b]$:
Sei $a, a' \in [a], b, b' \in [b]$. Zu zeigen: $[a+b] = [a'+b']$ und $[a \cdot b] = [a' \cdot b']$.
$a, a' \in [a] \Leftrightarrow a - a' \in I$ und $b, b' \in [b] \Leftrightarrow b - b' \in I$. Zu zeigen: $(a+b) - (a'+b') \in I$, $(a \cdot b) - (a' \cdot b') \in I$.
$(a+b) - (a'+b') = \underbrace{(a-a')}_{\in I} + \underbrace{(b-b')}_{\in I} \in I$ da $(I, +)$ Gruppe.
$(a \cdot b) - (a' \cdot b') = (a-a') \cdot b + a' \cdot b - a' \cdot b' = \underbrace{\underbrace{(a-a')}_{\in I} \cdot \underbrace{b}_{\in R}}_{\in I} + \underbrace{\underbrace{a'}_{\in R} \cdot \underbrace{(b-b')}_{\in I}}_{\in I}$ da $I \trianglelefteq R$.
Summe wieder in I da $(I, +)$ Gruppe. □

Beispiel $R = \mathbb{Z}$. $I = 2\mathbb{Z} = (2) = \{\text{Menge der geraden Zahlen}\}$.
$R/I = \{[0]_2, [1]_2\}$
$[0]_2 = \{\text{geraden Zahlen}\} = (2) =: g$, $[1]_2 = \{\text{ungeraden Zahlen}\} =: u$
$g \cdot u = g$, $g + u = u$, $u + u = g$.

Beispiel $n \in \mathbb{N}$. $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ ist ein Ring.
$n = 6$: $[2]_6 \cdot [4]_6 = [8]_6 = [2+6]_6 = [2]_6$
$[8]_6 \cdot [-2]_6 = [-16]_6 = [2 + (-3) \cdot 6]_6 = [2]_6$
$[1]_6 + [4]_6 = [5]_6 = [-1]_6 = -[1]_6$, denn $[1]_6 + [-1]_6 = [0]_6$.
$\mathbb{Z}/6\mathbb{Z}$ ist kein Integritätsbereich: $[2]_6 \cdot [3]_6 = [6]_6 = 0$. $[2]_6, [4]_6, [3]_6$ sind Nullteiler.
$(\mathbb{Z}/6\mathbb{Z})^* = \{[1]_6, [5]_6\}$ (Element $\neq 0$ die keine Nullteiler sind). $[5]_6^{-1} = [5]_6$ denn $[5]_6 \cdot [5]_6 = [25]_6 = [1]_6 = 1$.

Beispiel Sei $p(x) = X^2 + 1 \in \mathbb{R}[X]$. $I = (X^2 + 1) \trianglelefteq \mathbb{R}[X]$.
$A = \mathbb{R}[X]/I = \mathbb{R}[X]/(X^2 + 1)$ ist ein Restklassenring. Rechne: $[X]_p^2 = [X^2]_p = [X^2 - (X^2 + 1)]_p = [-1]_p = -[1]_p = -1$.
Die Abbildung: $A \to \mathbb{C}, [ax + b]_p \mapsto a \cdot i + b$ $(i^2 = -1)$ ist ein Ringhomomorphismus.

Weitere Möglichkeiten in A zu rechnen:
A ist 2-dimensionaler $\mathbb{R}$-Vektorraum mit Basis $[X]_p, [1]_p$. $a, b \in \mathbb{R}$, $a[X]_p + b[1]_p = [aX + b]_p$.
$\mathbb{R}$-Vektorraum-Homomorphismus: $A \to \mathbb{R}^{2\times 2}, [X] \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, [1] \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist Ringhomomorphismus (injektiv). $a[X] + b[1] = [aX + b]_p \mapsto \begin{pmatrix} b & -a \\ a & b \end{pmatrix}$.

(8.5) Bemerkung (a) Sei K ein Körper, $(A, +, \cdot)$ ein Ring. Ist K Teilring von A mit $s \cdot a = a \cdot s \; \forall s \in K, a \in A$ so heißt A eine *K-Algebra*.
A wird zu einem K-Vektorraum durch $+$ als Vektorraum-Addition und $K \times A \to A, (s, a) \mapsto s \cdot a$ als skalare Multiplikation.

(b) Ist A eine K-Algebra und ist $I \lhd A (I \neq A)$ so ist auch A/I eine K-Algebra.
($K \to A/I, s \mapsto s + I = [s]_I$ ist injektiver Ringhomomorphismus, denn $K \cap I = \{0\}$ da $K \setminus \{0\} \subseteq A^*$ und daher $K \setminus \{0\} \cap I = \emptyset$ (8.2)(b).)

Beispiel $K[X]$ ist eine K-Algebra $(1, X, X^2, X^3, \dots)$ ist K-Basis von $K[X]$.

Beispiel $\mathbb{R}[X]/(X^2 + 1)$ ist eine $\mathbb{R}$-Algebra.

Beispiel Sei K ein Körper, $p(x) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in K[X]$.
$K[X]/(p(x)) = \{[q(x)]_p | q \in K[X]\}$ ist K-Algebra, Basis: $B = ([1], [X], [X^2], \dots, [X^{n-1}])$.

Nachrechnen: B ist linear unabhängig:
Seien $c_0, c_1, \dots, c_{n-1} \in K$ mit $c_0[1] + c_1[X] + \dots + c_{n-1}[X^{n-1}] = 0 = [0]_p$ d.h. $[c_0 + c_1X + \dots + c_{n-1}X^{n-1}]_p = [0]_p$
$\Leftrightarrow c_0 + c_1X + \dots + c_{n-1}X^{n-1} \in (p)$
$\Leftrightarrow \exists q \in K[X]$ mit $p \cdot q = c_0 + c_1X + \dots + c_{n-1}X^{n-1} = r(X)$.
Ist $q \neq 0$ so gilt: $\mathrm{Grad}(p \cdot q) = \mathrm{Grad}(p) + \mathrm{Grad}(q) = n + \mathrm{Grad}(q) \geq n$. $\mathrm{Grad}(r) = \mathrm{Grad}(c_0 + c_1X + \dots c_{n-1}X^{n-1}) \leq n - 1 < n$ oder $r = 0$.
Also gilt $r = 0$ d.h. $c_0 + c_1X + \dots + c_{n-1}X^{n-1} = 0 \in K[X]$. $(1, X, X^2, \dots)$ ist K-Basis von $K[X]$ also folgt $c_0 = c_1 = \dots = c_{n-1} = 0$.

Erzeugendensystem:
Sei $q(x) = b_0 + b_1X + \dots + b_mX^m \in K[X]$. Zu zeigen: $\exists c_0, \dots, c_{n-1} \in K$ mit $[q(x)]_p = c_0[1]_p + c_1[X]_p + \dots + c_{n-1}[X^{n-1}]_p = [c_0 + c_1X + \dots + c_{n-1}X^{n-1}]_p$.
Angenommen dies gilt nicht, dann sei $q(X) \in K[X]$ so ein Polynom minimalen Grades $\Rightarrow \mathrm{Grad}(q) =: m \geq n = \mathrm{Grad}(p)$ (sonst wähle $c_i = b_i \forall i$).
Sei $\tilde{q}(x) := a(X) - b_mX^{m-n}p(X) \Rightarrow [\tilde{q}]_p = [q]_p$ und $\mathrm{Grad}(\tilde{q}) \leq m - 1 < \mathrm{Grad}(q)$.
Dann nach Minimalannahme: $[\tilde{q}]_p \in < [1]_p, \dots, [X^{n-1}]_p >_K \Rightarrow [q]_p = [\tilde{q}]_p$ Widerspruch!

(8.6) Beispiel Sei $p(x) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$, Körper.
$A = K[X]/(p(x))$: Dann ist A eine K-Algebra und $B = ([1], [X], \ldots, [X^{n-1}])$ ist K-Basis von A. $a \in A \Rightarrow m_a : A \to A : b \mapsto a \cdot b$ ist K-linear. $a \cdot (s_1b_1 + s_2b_2) = s_1ab_2 + s_2ab_2 \; \forall s_1, s_2 \in K, b_1, b_2 \in A$.

Matrix von m_a bezüglich Basis B?
$a = [X]_p : [X]_p \cdot [X^i]_p = [X^{i+1}]_p \; \forall i \in \{0, 1, \ldots, n-1\}$ $(X^0 := 1)$.

$$M_B(m_{[X]}) = \begin{pmatrix} 0 & 0 & \cdots & 0 & \square \\ 1 & 0 & \ddots & \ddots & \square \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \square \\ 0 & \cdots & \cdots & 1 & \square \end{pmatrix}$$

$$\begin{aligned} [X]_p \cdot [X^{n-1}]_p &= [X^n]_p = [X^n - p(x)]_p \\ &= [-a_0 - a_1X - \cdots - a_{n-1}X^{n-1}] \\ &= -a_0 - a_1[X]_p - a_2[X^2]_p - \cdots - a_{n-1}[X^{n-1}]_p \end{aligned}$$

$M_B(m_{[X]_p})$ = Begleitmatrix des Polynoms p. Matrix von m_a $a = \sum_{j=0}^{n-1} \alpha_j [X^j]_p$ ist $M_B(m_a) = \sum_{j=0}^{k-1} \alpha_j M_p^j$, $m_a \in \mathrm{End}(A) \cong K^{n \times n}$.
$f \mapsto M_B(f) \Rightarrow$ Die Abbildung $A \to K^{n \times n}, a \mapsto M_B(m_a)$ ist injektiver Ringhomomorphismus d.h. Rechnen in A übertragt sich zur Matrixrechnung in $\Phi(A) \in K^{n \times n}$.
Φ: Ringhomomorphismus: da $p(M_p) = 0$, injektiv: da $p =$ Minimalpolynom $\mu_p =$ kleinstes Polynom mit dieser Eigenschaft (Details: Übung).

9 Euklidische Ringe

(9.1) Definition Ein Integritätsbereich (kommutativer Ring ohne Nullteiler) heißt *Euklidischer Ring* genau dann, wenn es eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ gibt mit der folgenden Eigenschaft:
Für jedes $a \in R$ und $b \in R \setminus \{0\}$ gibt es $q, r \in R$ mit $r = 0$ oder $\delta(r) < \delta(b)$, sodass $a = b \cdot q + r$.

Beispiel (a) $\mathbb{Z}$ ist Euklidischer Ring. $\delta : \mathbb{Z} \to \mathbb{N}, \delta(a) = |a| = \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$.

(b) K Körper, dann ist $K[X]$ Euklidischer Ring, $\delta : K[X] \to \mathbb{N}, \delta(p) = \mathrm{Grad}(p)$.

(9.2) Definition Sei R ein Integritätsbereich.

(a) Für $a, b \in R$ sagen wir $a|b$ (a teilt b) genau dann, wenn ein $c \in R$ existiert mit $b = a \cdot c$.

(b) Sind $a, b \in R \setminus \{0\}$ so heißt $d := \mathrm{ggT}(a,b) \in R$ ein *größter gemeinsamer Teiler* von a und b genau dann, wenn $d|a$ und $d|b$ und $\forall c \in R$ mit $c|a$ und $c|b$ folgt $c|d$.

(c) Sind $a, b \in R \setminus \{0\}$ so heißt $k := \mathrm{kgV}(a,b) \in R$ ein *kleinstes gemeinsames Vielfaches* von a und b genau dann, wenn $a|k$ und $b|k$ und $\forall c \in R$ mit $a|c$ und $b|c$ gilt $k|c$.

(9.3) Bemerkung Gibt es ein $g = \mathrm{ggT}(a,b)$ so ist $\{d | d = \mathrm{ggT}(a,b)\} = g \cdot R^*$.

Beweis. Sei $g = \mathrm{ggT}(a,b)$ und $d = \mathrm{ggT}(a,b)$.
$\Rightarrow g|d$ und $d|g$, d.h. $\exists x, y \in R$ mit $d = g \cdot x$, $g = d \cdot y$.
Zu zeigen: $x \in R^*$.
$g = d \cdot y = g \cdot x \cdot y$ d.h. $g \cdot (1 - x \cdot y) = 0$. R Nullteilerfrei also $g = 0$ (Widerspruch, Teiler sind $\neq 0$) oder $x \in R^*$. □

(9.4) Satz In einem Euklidischen Ring R gibt es ggT und kgV.

Genauer konstruiert der folgende Algorithmus zu gegebenen $a, b \in R \setminus \{0\}$ ein $g, x, y \in R$ mit $g = ax + by = \mathrm{ggT}(a,b)$. (Übung: $\mathrm{kgV}(a,b) = \dfrac{a}{\mathrm{ggT}(a,b)}$)

Euklidischer Algorithmus

Idee: Schreibe $a = bq + r$ $(\delta(r) < \delta(b))$. Dann ist $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$.
Denn: $c|a$ und $c|b \Leftrightarrow c|b$ und $c|r = a - bq$.

Algorithmus

$$
\begin{aligned}
a &= bq_0 + r_1 && \text{mit } r_1 = 0 \text{ oder } \delta(r_1) < \delta(b)\\
b &= r_1 q_1 + r_2 && \text{mit } r_2 = 0 \text{ oder } \delta(r_2) < \delta(r_1)\\
r_1 &= r_2 q_2 + r_3 && \text{mit } r_3 = 0 \text{ oder } \delta(r_3) < \delta(r_2)\\
&\vdots && \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n\\
r_{n-1} &= r_n q_n
\end{aligned}
$$

Konstruierte Folge von Resten r_i mit $\delta(b) > \delta(r_1) > \delta(r_2) > \cdots > \delta(r_{n-1}) > \delta(r_n) > \ldots$ Echt absteigende Kette natürlicher Zahlen. Diese ist endlich. D.h. $\exists n$ mit $r_{n+1} = 0$ und $r_n \neq 0$.
Behauptung: $r_n = \mathrm{ggT}(a,b)$
Denn: $r_n = \mathrm{ggT}(r_{n-1}, r_n) \overset{\text{Idee}}{=} \mathrm{ggT}(r_{n-2}, r_{n-1}) = \cdots = \mathrm{ggT}(r_1, r_2) = \mathrm{ggT}(b, r_1) = \mathrm{ggT}(a,b)$.

Alternativ:

(1) $g = r_1$ teilt a und g teilt b denn:
$g|r_n$ und $g|r_{n-1} \Leftrightarrow g|r_{n-1}$ und $g_{n-2} \Leftrightarrow \ldots \Leftrightarrow g|a$ und $g|b$.

(2) $\exists x, y \in R$ mit $g = ax + by$. Es ist $r_j = r_{j-2} - r_{j-1}q_{j-1}$.

$$\begin{aligned} g = r_n &= r_{n-2} - r_{n-1}q_{n-1} \\ &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1} \\ &= r_{n-2}(1 + q_{n-2}q_{n-1}) - r_{n-3}q_{n-1} \\ &= (r_{n-4} - r_{n-3}q_{n-3})(1 + q_{n-2}q_{n-1}) - r_{n-3}q_{n-1} \\ &= \cdots = ax + by \end{aligned}$$

(1) + (2) $\Rightarrow g = \mathrm{ggT}(a, b)$. Sei dazu $d \in R$, $d|a$ und $d|b \Rightarrow d|ax + by$ $(\forall x, y \in R)$, also auch $d|g$.

Beispiel $\mathrm{ggT}(31, 399)$

$$\begin{aligned} 91 &= 0 \cdot 399 + 91 \\ 399 &= 4 \cdot 91 + 35 \\ 91 &= 2 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

$\Rightarrow 7 = \mathrm{ggT}(91, 399)$

$$\begin{aligned} 7 &= 21 - 14 = 21 - (35 - 21) \\ &= 2 \cdot 21 - 35 = 2 \cdot (91 - 2 \cdot 35) - 35 \\ &= (-5) \cdot 35 + 2 \cdot 91 = (-5) \cdot (399 - 4 \cdot 91) + 2 \cdot 91 \\ &= 22 \cdot 91 - 5 \cdot 399 \end{aligned}$$

(9.5) Satz Sei R ein Euklidischer Ring und $f \in R$. Dann ist die Einheitengruppe $(R/(f))^* = \{[a]_f | a \in R, \mathrm{ggT}(a, f) = 1\}$. Sind $x, y \in R$ mit $ax + fy = 1$ so ist $[a]_f^{-1} = [x]_f$.

Beweis. „$\supseteq$“ Sei $a \in R$ mit $\mathrm{ggT}(a, f) = 1$. Dann gibt es $x, y \in R$ mit $1 = ax + fy$.
$\Rightarrow [a]_f \cdot [x]_f = [a \cdot x]_f = [1 - fy]_f = [1]_f - [fy]_f = 1 \cdot 0 = 0$.

„$\subseteq$“ Sei umgekehrt $[a]_f \in (R/(f))^*$ dann gibt es $b \in R$ mit $[a]_f \cdot [b]_f = [1]_f$ d.h. $[a \cdot b]_f = [1]_f$.
$\Rightarrow ab - 1 \in (1) = f \cdot R = \{f \cdot y | y \in R\}$ d.h. $\exists y \in R$ mit $ab - 1 = fy \Rightarrow ab + (-y)f = 1$ d.h. 1 hat die Eigenschaft (2) aus Beweis (9.4). Außerdem $1|a$ und $1|f \Rightarrow 1 = \mathrm{ggT}(a, f)$.

□

Beispiel $(\mathbb{Z}/6\mathbb{Z})^* = (\mathbb{Z}/(6))^* = \{[1],[5]\}$. Es gilt $[5]_6 \cdot [5]_6 = [25]_6 = [1]_6$ d.h. $[5]_6^{-1} = [5]_6$.

(9.6) Folgerung $|\mathbb{Z}/N\mathbb{Z}|^* = \varphi(N)$ (Eulersche φ-Funktion: $\varphi(N) := |\{d \in \{0,\dots,N-1\} | \operatorname{ggT}(d,N) = 1\}|$). Denn $(\mathbb{Z}/N\mathbb{Z})^* = \{[d]_N | d \in \{0,\dots,N-1\}, \operatorname{ggT}(d,N) = 1\}$.

(9.7) Folgerung $p \in \mathbb{N}$ Primzahl (d.h. $p > 1$ und falls $p = a \cdot b$ mit $a, b \in \mathbb{Z}$, $a > 0$ so gilt $a = 1$ oder $b = 1$). Dann ist $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ ein Körper. (Errinerung: Ein Körper ist ein kommutativer Ring R mit $R^* = R \setminus \{0\}$.)

Beweis. $\mathbb{Z}/p\mathbb{Z}$ ist kommutativer Ring. Zu zeigen: $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.
$[a]_p \in \mathbb{Z}/p\mathbb{Z}$ ist invertierbar $\Leftrightarrow$ $\operatorname{ggT}(a,p) = 1$ $\Leftrightarrow$ $p \not| a$ $\overset{p \text{ Primzahl}}{\Leftrightarrow}$ $[a]_p \neq [0]_p$ $\square$

(9.8) Folgerung K Körper, $p(X) \in K[X]$ irreduzibel (d.h. $\operatorname{Grad}(p) > 0$ und falls $p = a \cdot b$ mit $a, b \in K[X]$ so gilt $\operatorname{Grad}(a) = 0$ oder $\operatorname{Grad}(b) = 0$).
Dann ist $K[X]/p(X)K[X]$ ein Körper.

Beweis. Wie bei (9.7) oder:
$R := K[X]/(p(X))$ ist kommutativer Ring.
$[a]_{(p(X))}$ ist invertierbar $(a \in K[X])$ $\Leftrightarrow$ $\operatorname{ggT}(a, p(X)) = 1$
$\overset{\text{da } p(X) \text{ irreduzibel}}{\Leftrightarrow}$ $p(X) \not| a$ $\Leftrightarrow$ $[a]_{(p(X))} \neq 0$.
$\Rightarrow R^* = R \setminus \{0\}$ d.h. R ist Körper. $\square$

Beispiel $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\} = \{0,1\}$, $p(X) = X^2 + X + 1 \in K[X]$ ist irreduzibel (da $p(1) = 1 = p(0)$, also hat p keinen Teiler vom Grad 1).
$\Rightarrow \mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1)$ ist Körper.
$\mathbb{F}_2$-Basis von $\mathbb{F}_4$: $([1]_{(X^2+X+1)}, [X]_{(X^2+X+1)})$
Sei $\omega := [X]_{(X^2+X+1)} \in \mathbb{F}_4$. $\mathbb{F}_2$-Basis von $\mathbb{F}_4$: $(1, \omega)$.
$F_4 = \{0, 1, \omega, \omega + 1\}$, $F_4^* = \{1, \omega, \omega + 1 = \omega^2\}$
Es gilt $[X]^2_{(X^2+X+1)} + [X]_{(X^2+X+1)} + [1]_{(X^2+X+1)} = \omega^2 + \omega + 1 = [X^2 + X + 1]_{(X^2+X+1)} = [0]_{(X^2+X+1)} = 0$, also $\omega^2 = -\omega - 1 \overset{\text{da } -1 = 1 \text{ in } \mathbb{F}_2}{=} \omega + 1$.
$\mathbb{F}_4^* = <\omega> = \{\omega^i | i \in \mathbb{Z}\} = \{\omega, \omega^2, \omega^3 = 1\}$.
$\omega^3 = 1$: Da in $\mathbb{F}_2[t]$ gilt $t^3 - 1 = (t-1)(t^2 + t + 1)$ oder:
$[X]^3_{(X^2+X+1)} = [1]_{(X^2+X+1)}$ $\Leftrightarrow$ $X^3 - 1 \in (X^2 + X + 1) \cdot \mathbb{F}_2[X]$. Dies gilt, da $(X-1)(X^2 + X + 1) = X^3 - 1$.

(9.9) Definition Eine Gruppe G heißt *zyklisch* falls es ein $g \in G$ gibt mit $G = < g > = \{g^i | i \in \mathbb{Z}\} = \{g^0 = 1, g, g^{-1}, g^2, \dots\}$.

Beispiel
- $(\mathbb{Z}, +)$ ist zyklisch: $(\mathbb{Z}, +) = <1> = \{0, 1, -1, 2 = 1 + 1, -2, \dots\}$.
- Bezeichnung: $G = < g >$ zyklisch und $|G| = N < \infty$ so heißt $G = C_N$ (die bis auf Isomorphie eindeutige zyklische Gruppe der Ordnung N, engl.: cyclic group of order N).

- $F_4^* \cong C_3$

(9.10) Satz Sei K ein endlicher Körper. $N := |K| - 1 = |K^*|$. Dann ist $K^* \cong C_N$.

Beweis. Setze $G = K^*$, Dann ist G eine endliche Gruppe.
Wir wollen zeigen, dass ein $g \in G$ existiert mit $| < g > | = |G| = N$.
Wir wissen:

- $g \in G \Rightarrow | < g > |$ teilt N und $| < g > | = N \Leftrightarrow G =< g >$.
- $N \in \mathbb{N} \Rightarrow \sum_{d|N} \varphi(d) = N$ (Übungsaufgabe 20(3)).

Zu zeigen: Für jeden Teiler d von N hat G genau $\varphi(d)$ Elemente der Ordnung d. Insbesondere hat G genau $\varphi(N) \geq 1$ Elemente g der Ordnung N (denn $< g >= G$).

$\psi(d) := \{a \in K^* | \operatorname{ord}(a) = d\}$.
Es gilt $K^* = G = \biguplus_{d|N} \psi(d)$ also $N = |G| = \sum_{d|N} |\psi(d)|$.
Ist $a \in \psi(d)$ so ist a Nullstelle von $X^d - 1 \in K[X]$ ($a^d = 1$). Dieses Polynom hat höchstens d verschiedene Nullstellen in K, d.h. $\{z \in K | z^d = 1\} = \underbrace{< a >}_{\text{hat } d \text{ Elemente}}$.
$\{$Elemente der Ordnung d in $< a >\} = \{a^i | 1 \leq i \leq d-1, \operatorname{ggT}(i,d) = 1\}$ denn $\operatorname{ord}(a^i) = \dfrac{\operatorname{ord}(a)}{\operatorname{ggT}(\operatorname{ord}(a), i)}$. Das sind genau $\varphi(d)$ Elemente.
$\Rightarrow |\psi(d)| = \varphi(d) \Rightarrow |\psi(N)| = \varphi(N)$ d.h. es gibt genau $\varphi(N)$ Erzeuger von K^* (das sind $g \in K^*$ mit $< g >= K^*$).
$\varphi(N) \neq 0 \Rightarrow K^* =< g >$ zyklisch. □

Beispiel $p = 7$, $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. Nach Satz (9.10) ist $\mathbb{F}_7^* \cong C_6$.

$2 := [2]_7 \in \mathbb{F}_7$. Ist $< 2 >= \mathbb{F}_7^*$?
$2^2 = 4$, $2^3 = 2 \cdot 4 = 8 = 1$ (in $\mathbb{F}_7$), also $| < 2 >= |\{1 = 2^0, 2, 2^2 = 4\}| = 3$, d.h. $< 2 >\neq \mathbb{F}_7^*$.

$3 := [3]_7 \in \mathbb{F}_7$. Ist $< 3 >= \mathbb{F}_7^*$?
$3^2 = 9 = 2$, $3^3 = 3 \cdot 2 = 6$, $3^4 = 6 \cdot 3 = 4$, $3^5 = 4 \cdot 3 = 5$, $3^5 = 5 \cdot 3 = 15 = 1$. D.h. $< 3 >= \{1, 3, 2, 6, 4, 5\} = \mathbb{F}_7^*$.

Definition $a \in K^*$ mit $< a >= K^*$ heißt *primitives Element* von K.

Beispiel $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$

10 Der chinesische Restsatz

(10.1) Definition Sei R Ring, $I_1 \trianglelefteq R$ und $I_2 \trianglelefteq R$ heißen *teilerfremd* $:\Leftrightarrow R = I_1 + I_2 = \{a + b | a \in I_1, b \in I_2\}$.

Beispiel R Euklidischer Ring, $I_1 = (a_1)$ und $I_2 = (a_2)$ teilerfremd $\Leftrightarrow \operatorname{ggT}(a_1, a_2) = 1$.

(10.2) Definition (a) Sind R, S Ringe so ist $R \times S = \{(r,s) | r \in R, s \in S\}$ wieder ein Ring mit $(r_1, s_1) \circ (r_2, s_2) = (r_1 \circ r_2, s_1 \circ s_2)$ $(\circ \in \{+, \cdot\})$ das sogenannte *ringdirekte Produkt*.

(b) Sind G, H Gruppen, so heißt $G \times H = \{(g,h) | g \in G, h \in H\}$ das *direkte Produkt*.
$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$
$|G \times H| = |G| \cdot |H|$
$(g,h)^{-1} = (g^{-1}, h^{-1})$, $1_{G \times H} = (1_G, 1_H)$

Ist $| < g > | = a$, $| < h > | = b$ so ist $| < g, h > | = \mathrm{kgV}(a,b)$.

Beispiel (ringdirektes Produkt) $0_{R \times S} = (0_R, 0_S)$, $1_{R \times S} = (1_R, 1_S)$
$(R \times S)^* = R^* \times S^* = \{(r,s) | r \in R^*, s \in S^*\}$

(10.3) Satz (chinesischer Restsatz) (a) Seien I_1, I_2 teilerfremde Ideale in R. Dann ist die Abbildung

$$\begin{aligned} \varphi : & R/(I_1 \cap I_2) \to R/I_1 \times R/I_2 \\ & [r]_{I_1 \cap I_2} \mapsto ([r]_{I_1}, [r]_{I_2}) \end{aligned}$$

ein Ringisomorphismus.

(b) Seien $I_1, \ldots, I_k$ paarweise teilerfremde Ideale in R (d.h. $I_i + I_j = R \; \forall i \neq j$). Dann ist

$$\begin{aligned} \varphi : & R/(I_1 \cap \cdots \cap I_k) \to R/I_1 \times \cdots \times R/I_k \\ & [r]_{I_1 \cap \cdots \cap I_k} \mapsto ([r]_{I_1}, \ldots, [r]_{I_k}) \end{aligned}$$

ein Ringisomorphismus.

Beweis. (a) φ wohldefiniert:
$[r]_{I_1 \cap I_2} = [s]_{I_1 \cap I_2} \Leftrightarrow r - s \in I_1 \cap I_2$
$[r]_{I_1} = [s]_{I_1} \Leftrightarrow r - s \in I_1$
$[r]_{I_2} = [s]_{I_2} \Leftrightarrow r - s \in I_2$
$r - s \in I_1 \cap I_2 \Rightarrow r - s \in I_1$ und $r - s \in I_2$.

Ringhomomorphismus: ✓(vertreterweise rechnen)

injektiv: $\varphi([r]_{I_1 \cap I_2}) = \varphi([s]_{I_1 \cap I_2}) \Leftrightarrow ([r]_{I_1}, [r]_{I_2}) = ([s]_{I_1}, [s]_{I_2})$
$\Leftrightarrow [r]_{I_1} = [s]_{I_1}$ und $[r]_{I_2} = [s]_{I_2}$ d.h. $r - s \in I_1$ und $r - s \in I_2$.
$\Leftrightarrow r - s \in I_1 \cap I_2 \Leftrightarrow [r]_{I_1 \cap I_2} = [s]_{I_1 \cap I_2}$.

surjektiv: Hier wird $I_1 + I_2 = R$ benötigt. Schreibe $1 = a_1 + a_2$ mit $a_1 \in I_1$, $a_2 \in I_2$. Sei $([r]_{I_1}, [s]_{I_2}) \in R/I_1 \times R/I_2$.
Wir suchen ein Urbild:
$([r]_{I_1}, [s]_{I_2}) = ([r]_{I_1}, [r]_{I_2}) \cdot (1,0) + ([s]_{I_1}, [s]_{I_2}) \cdot (0,1) = \varphi([r]_{I_1 \cap I_2}) \cdot (1,0) + \varphi([s]_{I_1 \cap I_2}) \cdot (0,1)$

Es genügt also ein Urbild von $(1,0)$ bzw. $(0,1)$ zu finden.
$\varphi([a_1]_{I_1\cap I_2}) = ([a_1]_{I_1},[a_1]_{I_2}) = (0,1)$ da $a_1 \in I_1$ ist $[a_1]_{I_1} = 0$ und wegen $a_1 = 1 - a_2$ mit $a_2 \in I_2$ folgt $[a_1]_{I_2} = 1$.
Ebenso $\varphi([a_2]_{I_1\cap I_2}) = (1,0)$.
$\varphi([r\cdot a_2 + s\cdot a_1]_{I_1\cap I_2}) = ([r]_{I_1},[s]_{I_2})$

(b) Übung

□

Beispiel $R = \mathbb{Z}$, $I_1 = (2)$, $I_2 = (3)$.
$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

$$[0]_6 \mapsto ([0]_2,[0]_3) \qquad [1]_6 \mapsto ([1]_2,[1]_3) \qquad [2]_6 \mapsto ([0]_2,[2]_3)$$
$$[3]_6 \mapsto ([1]_2,[0]_3) \qquad [4]_6 \mapsto ([0]_2,[1]_3) \qquad [5]_6 \mapsto ([1]_2,[2]_3)$$

Anders gesagt: $m,l \in Z$, $\mathrm{ggT}(m,l) = 1$, so ist $a \in \mathbb{Z} \mod m\cdot l$ bekannt sobald $a \mod m$ und $a \mod l$ bekannt ist.

Beispiel $a = 5$, $b = 7$, gesucht: $n \in \{0,\dots,34\}$ mit $n \equiv_5 2$ und $n \equiv_7 3$.

Übersetzt: $\mathbb{Z}/(35) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(7)$, $\varphi : [r]_{35} \to ([r]_5,[r]_7)$, gesucht: Urbild von $([2]_5,[3]_7)$.

Beweis von (10.3) sagt: Schreibe $1 = a_1 + a_2$ mit $a_1 = 5x$, $a_2 = 7y \Rightarrow \varphi([2a_2 + 3a_1]_{35}) = ([2]_5,[3]_7)$.

Euklidischer Algorithmus: $7 = 5+2$, $5 = 2\cdot 2+1 \Rightarrow 1 = 5-2\cdot 2 = 5-2\cdot(7-5) = 3\cdot 5 - 2\cdot 7$ (ebenso gut: Raten) $\Rightarrow x = 3$, $y = -2$.
$2\cdot(\underbrace{-2}_{y}\cdot\underbrace{7}_{b}) + 3\cdot(\underbrace{3}_{x}\cdot\underbrace{5}_{a}) \equiv_{35} 7 + 10 = 17$
$17 \equiv_5 2$ und $17 \equiv_7 3$

Allgemeine Formel: $-14s + 15t \equiv_5 s \equiv_7 t$

(10.4) Folgerung $N = \prod_{i=2}^{s} p_i^{n_i}$ mit p_i Primzahlen $\Rightarrow \mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{n_s}\mathbb{Z}$ und $(\mathbb{Z}/N\mathbb{Z})^* = (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s^{n_s}\mathbb{Z})^*$. Insbesondere $\varphi(N) = \prod_{i=1}^{s}\varphi(p_i^{n_i}) = \prod_{i=1}^{s} p_i^{n_i-1}(p_i-1)$.

Beweis. Es genügt $|(\mathbb{Z}/p^n\mathbb{Z})^*| = p^{n-1}(p-1)$ für Primzahlen p zu zeigen.

$\mathbb{Z}/p^n\mathbb{Z} = \{[0]_{p^n},[1]_{p^n},\dots,[p^n-1]_{p^n}\}$
$\#\{[a]_{p^n} \text{ mit } \mathrm{ggT}(a,p^n) = 1\}$
$= |\mathbb{Z}/p^n\mathbb{Z}| - |\{[p\cdot a]_{p^n} | a \in \mathbb{Z}\}|$
$= p^n - p^{n-1} = (p-1)p^{n-1}$ □

(10.5) Folgerung p,q Primzahlen, $N = p\cdot q$, $p \neq q$.
$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$
$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* = C_{p-1} \times C_{q-1}$

(10.6) Folgerung Allgemein gilt für eine Primzahl p

$$\begin{aligned} p > 2 \Rightarrow & (\mathbb{Z}/p^n\mathbb{Z})^* \cong C_{p^{n-1}(p-1)} \\ p = 2 \Rightarrow & (\mathbb{Z}/2^n\mathbb{Z})^* \cong C_2 \times C_{2^{n-2}} \qquad \text{für } n \geq 3 \\ & (\mathbb{Z}/4\mathbb{Z})^* \cong C_2 \\ & (\mathbb{Z}/2\mathbb{Z})^* = \{1\} \cong C_1 \end{aligned}$$

11 Kryptographie: das RSA Verfahren

Ziel: Sender sendet Daten an Empfänger über eine unsichere Leitung (mit Lauschern oder auch Personen die falsche Daten einschleusen).

Zur verschlüsselten Datenübertragung gibt es zwei wesentliche verschiedene Ansätze:

(S) Secret Key Kryptographie

Sender und Empfänger einigen sich auf einen geheimen Schlüssel mit dem die Nachricht verschlüsselt und nachher auch entschlüsselt wird. (Beispiel: Enigma im zweiten Weltkrieg)

Probleme:

- Schlüsselaustausch
- Schlüsselgeheimhaltung
- Anzahl der Schlüssel
  Wollen 1000 Teilnehmer paarweise sicher kommunizieren, so braucht jeder 999 Schlüssel. Insgesamt $\binom{1000}{2} \approx 500.000$ Schlüssel.

(P) Public Key Kryptographie

Empfänger macht Schlüssel öffentlich mit dem man verschlüsseln aber nicht entschlüsseln kann.

Vorteil:

- keine geheime Absprache nötig
- jeder braucht sich nur einen Schlüssel (den eigenen Entschlüsselungsschlüssel) geheim zu merken
- kleinere Anzahl von Schlüsseln: pro Teilnehmer einer

Nachteil: Schlüssel länger als bei Secret Key Kryptographie

In der Praxis wird ein Hybridverfahren eingesetzt. Ein geheimer Schlüssel wird mit der public key Methode übertragen und dann die Nachricht mit diesem Schlüssel mit secret key Kryptographie verschlüsselt.

Das RSA-Verfahren: (Rivest, Shamir, Adleman, 1977)

(11.1) Errinerung Sind p, q Primzahlen mit $p \neq q$ und sei $m = p \cdot q$. Dann ist $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ und $(\mathbb{Z}/m\mathbb{Z})^* = C_{p-1} \times C_{q-1}$.
Also ist $a \in \mathbb{N}$ mit $a \equiv_{(p-1)(q-1)} 1$ so gilt $\forall x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, m) = 1$: $x^a \equiv_m x$.

(11.2) Definition (Public Key Kryptosystem) Ein PKK mit Authentifikation besteht aus einer Menge von Teilnehmern $\{E, S, \dots\}$, einer Nachrichtenmenge $\mathcal{N}$, einer öffentlich bekannten Hashfunktion $H : \mathcal{N} \to \mathcal{N}$, sowie einer bekannten öffentlichen Funktion $f_t : \mathcal{N} \to \mathcal{N}$ für alle Teilnehmer t. Jeder Teilnehmer t kennt sein f_t^{-1} (geheim).

Verfahren: Will S an E die Nachricht N senden, so berechnet S $X = f_E(N)$ und $Y = f_E(f_S^{-1}(H(N))$ und schickt dies an E.
E entschlüsselt $N = f_E^{-1}(X)$ und verifiziert, dass N unverfälscht von S stammt durch Test ob $H(N) = f_S(f_E^{-1}(Y))$ ist.

(11.3) (RSA Verfahren) Übereinkunft: $a(\mod m) \in \{0, \dots, m-1\}$ mit $[a(\mod m)]_m = [a]_m$.

Verfahren: Empfänger E wählt (kauft) 2 große Primzahlen p und q ($p, q \approx 10^{150}$) und eine Zahl $v \in \mathbb{N}$ mit $\mathrm{ggT}(v, (p-1)(q-1)) = 1$ und bestimmt $e \in \mathbb{N}$ mit $v \cdot e = 1(\mod (p-1)(q-1))$. $m := p \cdot q$.

Öffentlich: (m, v)

Geheim: e

Verschlüsseln: $\mathcal{N} = \mathbb{N}$. S will $N \in \mathbb{N}$ an E schicken. Berechne zuerst $N = \sum_{i=0}^{n} n_i \cdot m^i$ mit $n_i \in \{0, \dots, m-1\}$ und $f_E(N) = (f_E(n_0), \dots, f_E(n_n))$.
Für $n \in \{0, \dots, m-1\}$ ist $f_E(n) = n^v(\mod m)$.

Empfänger bekommt $a \in \{0, \dots, m-1\}$ mit $a \equiv_m n^v$ und berechnet $a^e(\mod m) \overset{(11.1)}{=} n$. Es genügt zu zeigen $a^e \equiv_m n \in \{0, \dots, m-1\}$. Es ist $a^e \equiv_m (n^v)^e \equiv_m n^{v \cdot e} \equiv_m n$ nach (11.1) da $v \cdot e \equiv_{(p-1)(q-1)} = 1$ (nur richtig, falls $\mathrm{ggT}(m, n) = 1$, sonst Fehler; $\mathrm{ggT}(m, n) \in \{p, q\}$ unwahrscheinlich).

Beispiel Empfänger E, Sender S

$\boxed{E}$ $p = 11$, $q = 17$, $m = p \cdot q = 187$
$(p-1)(q-1) + 1 = 7 \cdot 23$
öffentlich: $m = 187$, $v = 7$
geheim: $e = 23$

$\boxed{S}$ $n = 3$ soll an E gesendet werden.
$n^v = 3^7 = 2187 = 11 \cdot 187 + 130$
$\Rightarrow v(n) = 130$

$\boxed{E}$

$$
\begin{array}{rlll}
130^{23} & \equiv 130 \mod 187 & & \\
23 & = 2^4 + 2^2 + 2 + 1 & & \\
130^1 & \equiv 130 & & \mod 187 \\
130^2 & \equiv 130 \cdot 130 & \equiv 70 & \mod 187 \\
130^4 & \equiv 70 \cdot 70 & \equiv 38 & \mod 187 \\
130^8 & \equiv 38 \cdot 38 & \equiv 135 & \mod 187 \\
130^{16} & \equiv 135 \cdot 135 & \equiv 86 & \mod 187 \\
\Rightarrow 130^{23} & \equiv 130^1 \cdot 130^2 \cdot 130^4 \cdot 130^{16} & & \mod 187 \\
& \equiv 130 \cdot 70 \cdot 38 \cdot 86 & & \mod 187 \\
& \equiv 3 & & \mod 187
\end{array}
$$

Sicherheit von RSA

Berechnung von e ist äquivalent zur Faktorisierung $m = p \cdot q$ (es wird angenommen, dass dies schwer ist; es ist kein schnelles Verfahren bekannt).

Man weiß nicht, ob das Entschlüsseln einer Nachricht über v-tes Wurzelziehen in $(\mathbb{Z}/m\mathbb{Z})^*$ (n^v bekannt $\Rightarrow n = \sqrt[v]{n^v}$) genauso schwierig ist, wie die Faktorisierung von m.

Kosten für das Potenzieren in $\mathbb{Z}/m\mathbb{Z}$: $\log_2(v) + \log_2(e)$.

12 Endliche Körper

(12.1) Satz Sei K ein endlicher Körper.

(i) Es gibt ein $n \in \mathbb{N}_{\geq 1}$ mit $n \cdot 1_K = \underbrace{1_K + \cdots + 1_K}_{n} = 0$.

(ii) $\mathrm{Char}(K) := \min\{n \in \mathbb{N} \,|\, n \geq 1, n \cdot 1_K = 0\}$ ist eine Primzahl und heißt die *Charakteristik* von K.

(iii) Sei $p := \mathrm{Char}(K)$. Dann ist K eine $\mathbb{F}_p$-Algebra. Genauer ist der von 1_K erzeugte Teilring isomorph zu $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{[0]_p, [1]_p, \ldots, [p-1]_p\}$. K ist $\mathbb{F}_p$-Vektorraum. Ist $f := \mathrm{Dim}_{\mathbb{F}_p}(K)$ so ist $|K| = p^f$.

(iv) $K^* = (K \setminus \{0\}, \cdot) \cong C_{p^f-1}$

(v) Ist $a \in K$ so ist $a^{p^f} = a$. $X^{p^f} - X = \prod_{a \in K} (X - a) \in K[X]$.

Beweis. (i) $1_K \in K$, $1_K + 1_K + \cdots + \underbrace{1_K + \ldots, 1_K}_{n} \in K$. $|K|$ endlich $\Rightarrow$ es existieren $n, m \in \mathbb{N}$, $n < m$ mit $m \cdot 1_K = n \cdot 1_K \Rightarrow (m-n) \cdot 1_K = 0$, $m - n \geq 1$.

(ii) Sei $n \in \mathbb{N}$, $n \geq 1$ minimal mit $n \cdot 1_K = 0$. Dann ist $n > 1$, denn $1_K \neq 0_K$.

Zu zeigen: n ist eine Primzahl.
Sei dazu $a, b \in \mathbb{N}$ mit $n = a \cdot b$. Dann $(a \cdot b) \cdot 1_K = 0 \Leftrightarrow (a \cdot 1_K) \cdot (b \cdot 1_K) = 0$ $\overset{K \text{ nullteilerfrei}}{\Rightarrow}$ $a \cdot 1_K = 0$ oder $b \cdot 1_K$, n war minimal $\Rightarrow a = n$ (und $b = 1$) oder $b = n$ (und $a = 1$), d.h. n ist Primzahl.

(iii) Sei $M = \{0, 1_K, 1_K + 1_K =: 2, \ldots, p-1\} \subseteq K$. M ist abgeschlossen unter $+$ und $\cdot$, also ein Teilring.
$\varphi : \mathbb{F}_p \to M, [a] \mapsto \cdot 1_K \in M$ ist Ringisomorphismus.

(iv) war Satz (9.10)

(v) Folgt aus (iv): $K = K^* \cup \{0\}$. $a \in K$: $a = 0$, dann ist $a^{p^f} = 0 = a$ oder $a \in K^*$, dann ist $a^{p^f - 1} = 1 \Leftrightarrow a^{p^f} = a$.

In K liegen damit p^f verschiedene Nullstellen von $X^{p^f} - X$. Polynom vom Grad p^f hat höchstens p^f verschiedene Nullstellen $\Rightarrow X^{p^f} - X = \prod_{a \in K}(X - a)$.

□

(12.2) Lemma Sei $g(X) \in \mathbb{F}_p[X]$ irreduzibel und normiert vom Grad f (d.h. $g(X) = X^f + a_1 X^{f-1} + \cdots + a_f$). Dann gilt $g(X)$ teilt $X^{p^f} - X$.

Beweis. Sei $K := \mathbb{F}_p[X]/(g(X))$. Dann ist K ein Körper (da g irreduzibel) und $|K| = p^f$ $(([1]_g, [X]_g, \ldots, [X^{f-1}]_g)$ ist $\mathbb{F}_p$-Basis von $K)$.
Nach (12.1) gilt daher $a^{p^f} = a$ für alle $a \in K$.
Insbesondere ist $[X]_g^{p^f} = [X]_g \Leftrightarrow [X]^{p^f} - [X] = [0]_g \Leftrightarrow [X^{p^f} - X]_g = [0]_g$
$\Leftrightarrow X^{p^f} - X \in (g)$, $(g) = \{g \cdot h | h \in \mathbb{F}_p[X]\}$ d.h. g teilt $X^{p^f} - X$. □

(12.3) Satz Sei K ein endlicher Körper, $|K| = p^f$ mit $p = \mathrm{Char}(K)$. Sei $g \in \mathbb{F}_p[X]$ irreduzibel und normiert. Dann ist $K \cong \mathbb{F}_p[X]/(g) =: F$.
Insbesondere sind je zwei Körper mit p^f Elementen isomorph. $\mathbb{F}_{p^f}$ bezeichne den bis auf Isomorphie eindeutig bestimmten Körper mit p^f Elementen; $\mathbb{F}_{p^f} \cong \mathbb{F}_p[X]/(g)$.

Beweis. „Konstruktion“ Isomorphismus $\varphi : F \to K$. In K gilt $a^{p^f} - a = 0 \; \forall a \in K$.
$X^{p^f} - X = \prod_{a \in K}(X - a) \in K[X]$. $X^{p^f} - X \overset{(12.2)}{=} g \cdot h \in \mathbb{F}_p[X] \subseteq K[X]$ (da $\mathbb{F}_p \subseteq K$)
d.h. es existieren $a_1, \ldots, a_k \in K$ mit $g = \prod_{i=1}^{f}(X - a_i)$. Sei $a := a_1 \in K$, $g(a) = 0$.

Die Abbildung $\varphi_a : \mathbb{F}_p[X]/(g(X)) \to K, \sum_{i=0}^{f-1} \alpha_i [X]_g^i \mapsto \sum_{i=0}^{f-1} \alpha_i a^i \; \forall \alpha_0, \ldots, \alpha_{f-1} \in \mathbb{F}_p$ ist ein Ringhomomorphismus (wohldefiniert da $g(a) = 0$).
φ_a ist injektiv da $\mathrm{Kern}(\varphi_a) = \{0\}$ ($\mathrm{Kern}(\varphi_a) \trianglelefteq F$, F Körper also sind alle Ideale in F entweder $\{0\}$ oder F).

Fact: $\psi : G \to H$ Gruppenhomomorphismus, $\text{Kern}(\psi) = \{1\}$ so ist ψ injektiv, denn sonst gibt es $g_1 \neq g\_2 \in G$ mit $\psi(g_1) = \psi(g_2) \Rightarrow \psi(g_1 g_2^{-1}) = \psi(G_1)\psi(g_2)^{-1} = 1$ also $g_1 \cdot g_2^{-1} \in \text{Kern}(\psi) = \{1\} \Rightarrow g_1 g_2^{-1} = 1 \Rightarrow g_1 = g_2$.

Fact anwenden auf die Gruppen $(F, +), (K, +)$ und φ_a also Gruppenhomomorphismus auffasen $\Rightarrow \varphi_a$ surjektiv da $|F| = |K|$. □

(12.4) Satz Für alle $f \in \mathbb{N}_{\geq 1}$ und alle Primzahlen p gibt es ein irreduzibles normiertes Polynom $g \in \mathbb{F}_p[X]$ mit $\text{Grad}(g) = f$. Insbesondere gibt es zu jeder Primzahlpotenz p^f genau einen Körper $(\mathbb{F}_p[X]/(g(x)))$ mit p^f Elementen.

Beweis. Übung 8 □

(12.5) Beispiel $\mathbb{F}_{16} \cong \mathbb{F}_2[X]/(X^4 + X + 1)$, $\gamma := [X]_{(X^4+X+1)} \in \mathbb{F}_{16}$ so gilt $\gamma^4 + \gamma + 1 = 0$ (alles andere folgt daraus). $\mathbb{F}_2$-Basis von $\mathbb{F}_{16}$: $(1, \gamma, \gamma^2, \gamma^3)$. $\gamma^6 = \gamma^2 \cdot \gamma^4 = \gamma^2(\gamma + 1) = \gamma^3 + \gamma^2$.
Darstellung als Koeffizientenspalten (oder Zeilen) bezüglich dieser Basis.

Addieren: leicht $(1001) + (0011) = (1010)$, $(1 + \gamma^3) + (\gamma^2 + \gamma^3) = (1 + \gamma^2)$.
Multiplikation: schwierig.
Daher Übergang zu sogenannten Zech-Logarithmen.

γ ist primitives Element (*Primitivwurzel*) von $\mathbb{F}_{16}$ d.h. $\mathbb{F}_{16}^* =< \gamma >$ d.h. Potenzen von γ erzeugen den $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{16}$ ($\Rightarrow (1, \gamma, \gamma^2, \gamma^3)$ ist eine $\mathbb{F}_2$-Basis von $\mathbb{F}_{16}$).

Potenzen von $\delta := \gamma^3$ erzeugen auch $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{16}$.
$1 = (1000), \delta = (0001), \delta^2 = (0011), \delta^3 = (0101)$ ($\gamma^2 = \delta^2 - \delta$, $\gamma^3 = \delta^3 - \delta$).
Jedoch ist δ kein primitives Element, denn $< \delta >=< \gamma^3 >= \{1, \delta, \delta^2, \delta^3, \delta^4\}$. $\delta^5 = \gamma^{15} = 1$ da $|\,\mathbb{F}_{16}^*\,| = 15$.

$\epsilon := \gamma^5$ Erzeugen Potenzen von ϵ $\mathbb{F}_{16}$?
$1 = (10000)$, $\epsilon = (0110)$, $\epsilon^2 = (1110)$, $\epsilon^3 = (1000) = \gamma^{15} = 1$.
Der von ϵ erzeugte Teilkörper von $\mathbb{F}_{16}$ hat 4 Elemente $\{0, 1, \epsilon, \epsilon^2 = \epsilon + 1\} = \mathbb{F}_2[\epsilon] \subseteq \mathbb{F}_{16}$. $\mathbb{F}_2[\epsilon] \cong \mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$. $\epsilon^2 + \epsilon + 1 = 0$.

(12.6) Rechnen in endlichen Körpern *Zech-Logarithmus*: K sei endlicher Körper.
$K = \{0\} \cup K^* = \{0\} \cup < \alpha >$ α primitives Element in K.
$< \alpha >= \{\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{p^f-2}\}$ falls $|K| = p^f$.
$\alpha^i \leftrightarrow i$ ($i \in \{0, \ldots, p^f - 2\}$), $0 \leftrightarrow *$

Multiplikation einfach: $\alpha^i \cdot \alpha^j = \alpha^{i+j}$ (Rechnen $\underline{i} \cdot \underline{j} = \underline{k}$ mit $k \in \{0, \ldots, p^f - 2\}$, $k \equiv i + j(\mod p^f - 1)$, $\underline{*} \cdot \underline{i} = \underline{*}$)

Addition: $\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i})$
$1 + \alpha^{j-i} = \alpha^{z(j-i)}$ (z = Zech-Logarithmus)
$\alpha^i + \alpha^j = \alpha^{i+z(j-i)}$

Beispiel $K = \mathbb{F}_{16}$, $K^* =< \gamma >$, $\gamma = [X]_{(X^4+X+1)}$

$\gamma^0 + 1 = 1 + 1 = 0$, $\gamma^1 + 1 = \gamma^4$, $\gamma^2 + 1 = \gamma^8$, $\ldots$:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$z(k)$	$*$	4	8	14	1	10	13	9	2	7	5	12	11	6	3

$\gamma^{10} + \gamma^7 = \gamma^7(1+\gamma^3) = \gamma^7 \cdot \gamma^{z(3)} = \gamma^7 \cdot \gamma^{14} = \gamma^{21} = \gamma^6$.

Platzbedarf: $\sim |K|$ (nur für „kleine“ Körper).

(12.7) Satz Sei $K = \mathbb{F}_{p^f}$ und $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$. Dann ist K ein $\mathbb{F}_p$-Vektorraum (Dimension f) und $\mathrm{Frob}_p : K \to K, a \mapsto a^p$ ist eine $\mathbb{F}_p$-lineare bijektive Abbildung mit $\mathrm{Frob}_p(a) \cdot \mathrm{Frob}_p(b) = \mathrm{Frob}_p(a \cdot b)$ (ein Körperautomorphismus). Frob_p heißt der *Frobenius-Automorphismus* von K (über $\mathbb{F}_p$).

Beweis. Klar: $\mathrm{Frob}_p(a) \cdot \mathrm{Frob}_p(b) = a^p \cdot b^p = (a \cdot b)^p = \mathrm{Frob}_p(a \cdot b)$.

$\mathbb{F}_p$-Linearität: seien $\alpha, \beta \in \mathbb{F}_p$ und $a, b \in K$.

Zu zeigen: $\mathrm{Frob}_p(\alpha \cdot a + \beta \cdot b) = \alpha \cdot \mathrm{Frob}_p(a) + \beta \cdot \mathrm{Frob}_p(b)$

Binomische Formel: $(\alpha \cdot a + \beta \cdot b)^p = \sum_{i=0}^{p} \binom{p}{i} (\alpha \cdot a)^i (\beta \cdot b)^{p-i}$

$\binom{p}{i} = \frac{p!}{i!(p-i)!}$ $(\in \mathbb{N})$

(Beachte: $n \in \mathbb{N}$, $a \in K$ so heißt $n \cdot a = \underbrace{a + a + \cdots + a}_{n} = (n \cdot 1_K) \cdot a$.)

$\binom{p}{i} \cdot 1_K = 0$ falls $1 \le i \le p-1$ denn dann teilt p den Zähler des Bruchs aber nicht den Nenner d.h. $p | \binom{p}{i} \in \mathbb{N}$, also $\binom{p}{i} = p \cdot m$ $(m \in \mathbb{N})$.

$\Rightarrow \binom{p}{i} \cdot 1_K = (p \cdot m) \cdot 1_K = \underbrace{(p \cdot 1_K)}_{0} \cdot (m \cdot 1_K) = 0 \in K$

$\Rightarrow (\alpha a + \beta b)^p = (\alpha a)^p + (\beta b)^p = \alpha^p \cdot a^p + \beta^p b^p$

$\alpha, \beta \in \mathbb{F}_p \Rightarrow \alpha^p = \alpha$, $\beta^p = \beta$ (12.1)(v)

$\Rightarrow \mathrm{Frob}_p$ ist $\mathbb{F}_p$-linear.

Lineare Algebra: Frob_p ist injektiv $\Leftrightarrow \mathrm{Kern}(\mathrm{Frob}_p) = \{0\}$

$\Leftrightarrow \{a \in K | a^p = 0\} = \{0\}$ (richtig, da K nullteilerfrei)

$\Rightarrow \mathrm{Frob}_p$ bijektiv, da $|K| < \infty$. □

(12.8) Folgerung Sei $a \in \mathbb{F}_{p^f}$, $h \in \mathbb{F}_p[X]$ mit $h(a) = 0$. Dann gilt $h(a^p) = h(\mathrm{Frob}_p(a)) = 0$.

Beweis. $h(a^p) = \underbrace{h(\mathrm{Frob}_p(a)) = \mathrm{Frob}_p(h(a))}_{\mathrm{Frob}_p \text{ ist } K_p\text{-Automorphismus und } \mathbb{F}_p\text{-linear}} = \mathrm{Frob}_p(0) = 0^p = 0$

Ausführlich: $h(X) = \sum_{i=0}^{n} \alpha_i X^i$ mit $\alpha_i \in \mathbb{F}_p$. $\mathrm{Frob}_p(h(a)) = (h(a))^p$.

$(\sum_{i=0}^{n} \alpha_i a^i)^p \overset{\mathbb{F}_p\text{-linear}}{=} \sum_{i=0}^{n} \alpha_i (a^i)^p = \sum_{i=0}^{n} \alpha_i (a^p)^i = h(a^p)$. □

Beispiel $X^{16} - X \in \mathbb{F}_2[X]$

$X^{16} - X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$

$\gamma \in \mathbb{F}_{16}$ sei Nullstelle von $X^4 + X + 1$
$\Rightarrow \mathrm{Frob}_2(\gamma) = \gamma^2, \mathrm{Frob}_2(\gamma^2) = \gamma^4, \mathrm{Frob}_2(\gamma^4) = \gamma^8, \mathrm{Frob}_2(\gamma^8) = \gamma^{16} = \gamma$ sind Nullstellen von $X^4 + X + 1$.

$\delta = \gamma^3$ ist Nullstelle von $X^4 + X^3 + X^2 + X + 1$ $(= \dfrac{X^5 - 1}{X - 1}$ und $\delta^5 = 1, \delta \neq 1)$
$\Rightarrow \delta^2, \delta^4, \delta^8 = \gamma^{24} = \gamma^9$ sind auch Nullstellen.
$X^4 + X^3 + X^2 + X + 1 = (X - \delta)(X - \delta^2)(X - \delta^4)(X - \delta^8)$

(12.9) Satz Sei $K \subseteq \mathbb{F}_{p^f}$ *Teilkörper* (= Teilring). Dann ist $|K| = p^d$ mit $d|f$. Umgekehrt hat F_{p^f} zu jedem d von f *genau* einen Teilkörper $K \subseteq \mathbb{F}_{p^f}$ mit $|K| = p^d$, nämlich $K = \{a \in \mathbb{F}_{p^f} \,|a^{p^d} = a\}$.

Beweis. (a) Sei $K \subseteq \mathbb{F}_{p^f} \Rightarrow K^* \leq \mathbb{F}_{p^f}^*$ Untergruppe.
$\Rightarrow |K^*| = p^d - 1$ teilt $|\,\mathbb{F}_{p^f}^*\,| = p^f - 1$.

Behauptung: $(p^d - 1)$ teilt $(p^f - 1) \Leftrightarrow d$ teilt f
Beweis: „$\Rightarrow$“ $\dfrac{p^f - 1}{p^d - 1}$ mit Division mit Rest:

$$\begin{aligned} p^f - 1 &= p^{f-d}(p^d - 1) + p^{f-d} - 1 \\ p^{f-d} - 1 &= p^{f-2d}(p^d - 1) + p^{f-2d} - 1 \\ &\vdots \\ p^{f-1} &= (p^{f-d} + p^{f-2d} + \cdots + p^{f-nd})(p^d - 1) + (p^{f-nd} - 1) \end{aligned}$$

Rest $= 0$ sobald $n \cdot d = f$ d.h. $d|f \Rightarrow p^d - 1 | p^f - 1$.

„$\Leftarrow$“: Zu zeigen: $p^d - 1 | p^f - 1 \Rightarrow d|f$
Sei $f \geq d$ minimal mit $p^d - 1 | p^f - 1$ aber $d \not| f$. Es ist $(p^f - 1) = p^{f-d}(p^d - 1) + (p^{f-d} - 1)$ mit $p^d - 1 | p^{f-d} - 1$ und $d \not| (f - d)$. Widerspruch zur Minimalität von f.

(b) $\mathbb{F}_{p^d} \leq \mathbb{F}_{p^f} \Rightarrow d|f$ denn dann ist $\mathbb{F}_{p^d}^* \leq \mathbb{F}_{p^f}^*$ und daher nach (3.7) $|\,\mathbb{F}_{p^d}^*\,| = p^{d-1}$ teilt $|\,\mathbb{F}_{p^f}^*\,| = p^f - 1$ also nach (a) $d|f$.

(c) Es gelte nun $d|f$ und $p^f - 1 = a(p^d - 1)$ mit $a \in \mathbb{N}$, $\mathbb{F}_{p^f}^* =< a >$, $\beta := \alpha^a$.
Behauptung: $\{0\} \cup \{\beta^i | 0 \leq i \leq p^d - 2\} =: K \overset{\text{zu zeigen}}{=} M := \{x \in \mathbb{F}_{p^f} \,|x^{(p^d)} = x\}$ ist ein Teilkörper von $\mathbb{F}_{p^f}$.
Beweis: Falls $K = M$ so ist $K \leq \mathbb{F}_{p^f}$. Dazu: $x, y \in K \Rightarrow x \cdot y \in K$ (da $\beta^i \cdot \beta^j = \beta^{i+j} \in K$). $x, y \in M \Rightarrow x + m \in M$ denn $(x + y)^{(p^d)} = \mathrm{Frob}_p^d(x + y) \overset{\text{Körperautomorphismus}}{=} \mathrm{Frob}_p^d(x) + \mathrm{Frob}_p^d(y) = x^{(p^d)} + y^{(p^d)} = x + y$ (da $x, y \in M$).
Zu zeigen: $M = K$.
$x \in M \Rightarrow x = 0$ oder $x \in \mathbb{F}_{p^f}^*$ und $x^{p^d - 1} = 1$
$x \in \mathbb{F}_{p^f}^* \Rightarrow \exists i \in \mathbb{N}$ mit $x = \alpha^i$. $x^{p^d - 1} = 1 \Rightarrow \alpha^{i \cdot (p^d - 1)} = (\alpha^i)^{p^d - 1} = 1$

$p^f - 1 =$ Ordnung von $a \Rightarrow i(p^d - 1)$ ist durch $p^f - 1 = a(p^d - 1)$ teilbar $\Rightarrow$ $a|i = j \cdot a \Rightarrow x = \alpha^i = (\alpha^a)^j = \beta^j \in < \beta >$, also $M \subseteq K$.

Umgekehrt: $x \in K \Rightarrow x = 0 \in M$ oder $x = \beta^j$ und dann ist $x^{p^d-1} = \beta^{j(p^d-1)} = \alpha^{a(p^d-1)j} = (a^{p^f-1})^j = 1$.

□

Beispiel $\mathbb{F}_4 \not\leq \mathbb{F}_8$ ($4 = 2^2$, $8 = 2^3$ und $2 \not| 3$). Es gilt wohl $\mathbb{F}_4 \leq \mathbb{F}_{16}$ (da $2|4$).

Teil IV

Codierungstheorie

13 Lineare Codes

13.1 Einführung

(13.1) Definition (i) Ein *Code* C der Länge N über einem endlichen Alphabet A ist eine Teilmenge $C \subseteq A^N = \{(a_1, \ldots, a_N) | a_i \in A\}$.

(ii) Die *Informationsrate* von C ist $r(C) := \frac{1}{N} \log_{|A|}(|C|) = \frac{\log(|C|)}{\log(|A^N|)}$.

(iii) Sind $x, y \in A^N$ so heißt $d(x,y) := |\{i \in \{1, \ldots, N\} | x_i \neq y_i\}|$ der *Hammingabstand* zwischen x und y. $d(C) := \min\{d(x,y) | x \neq y \in C\}$ heißt der *Minimalabstand* von C.

Ziel: Finde C mit $r(C)$ groß und $d(C)$ groß.

Beispiel Sei $A = \{a, b, \ldots, z\}$, $N = 3$, $C = \{(aaa), (bbb), \ldots, (zzz)\} \Rightarrow r(C) = \frac{1}{3} \log_{26}(26) = \frac{1}{3}$.
1 Fehler kann korrigiert werden: $(aba) \overset{\text{decode}}{\to} (aaa)$.
2 Fehler können erkannt werden: bei (abc) wissen wir, dass (mindestens) 2 Fehler aufgetreten sind, bei (aba) wissen wir, dass es fehlerhaft ist.

Bemerkung (i) Für den Hammingabstand gilt die Dreiecksungleichung $d(x,y) + d(y,z) \geq d(x,z)\ \forall x, y, z \in A^N$.

(ii) $r := r(C) = \log_{|A|^N}(|C|)$ erfüllt $|C|^r = |A|^N$.

(13.2) Definition Sei $C \subseteq A^N$ ein Code. Ein *minimal distance decoder (MDD)* ist eine Funktion $f : A^N \to C$ mit $d(f(a), a) = \min\{d(c, a) | c \in C\}\ \forall a \in A^N$.

(13.3) Satz Sei $C \subseteq A^n$, $d = d(C)$, f ein MDD für C.

(i) Ist $e < \frac{d}{2}$ so kann f e Übertragungsfehler korrigieren.

(ii) Ist die Anzahl der Übertragungsfehler $e < d$ so erkennt MDD, dass ein Fehler aufgetreten ist. Ist also $a \in A^N$ das empfangene Wort und sind bei der Übertragung von $c \in C$ e Fehler aufgetreten, so gilt: Ist $e < \frac{d}{2}$ so ist $f(a) = c$ und ist $e < d$ so ist $f(a) \neq a$ d.h. wir wissen es ist ein Fehler aufgetreten.

Beweis. Folgt aus der Dreiecksungleichung:
Ist $e = d(a,c) < \frac{d}{2}$ so ist $c \in C$ das einzige Codewort mit $d(a,c) \leq e$. Denn sei $\tilde{c} \in C$ ein weiteres Codewort mit $d(a,\tilde{c}) \leq e$, dann ist $d(\tilde{c},c) \leq d(a,c) + d(a,\tilde{c}) \leq 2 \cdot e < d = d(C) \Rightarrow c = \tilde{c}$.
$e < d \Rightarrow f(a) \neq a$ ebenso. □

Ziel: Finde C mit $d(C)$ groß (viele Fehler erkennen) und $r(C)$ groß, d.h. viel Information Übertragen. Codieren und Decodieren $\rightsquigarrow$ lineare Codes.

13.2 Lineare Codes

(13.4) Definition A endlicher Körper, $N \geq 1$, $A^N = A^{1\times N}$ ist A-Vektorraum der *Zeilenvektoren*. $C \subseteq A^N$ Unterraum heißt *linearer Code*.

Beispiel $A = \mathbb{F}_2 = \{0,1\}$, $N = 3$, $C = \{(0,0,0),(1,0,1),(0,1,1),(1,1,0)\}$ (dritter Eintrag Summe der ersten beiden).

Empfange: $(1,1,1) \notin C$, also Übertragungsfehler. Problem: original Wort ist kürzer.

(13.5) Bemerkung Informationsrate: $\frac{\dim_A(C)}{N}$

(13.6) Bemerkung C ist ein $[N, \dim(C), d(C)]$-Code (Kosten, Kapazität, Fehlertoleranz).

(13.7) Lemma Sei $C \subseteq A^N$ ein linearer Code. Dann ist $d(C) = \min\{d(c,0) | c \in C \setminus \{0\}\}$.

Beweis. Linke Seite $\leq$ rechte Seite, da das Minimum über eine größere Menge gebildet wird.

Linke Seite $\geq$ Rechte Seite: Seien $c, c' \in C$ mit $c \neq c'$ und $d(C) = d(c,c')$. Dann ist die linke Seite $= d(C) = d(c,c') = d(c+(-c'), c'+(-c')) = d(\underbrace{c-c'}_{\neq 0}, 0) \geq$ rechte Seite. □

(13.8) Definition (a) Das *Gewicht* $\omega(x)$ von $x \in A^N$ ist definiert als $\omega(x) := d(x,0)$.

(b) Sei $C \subseteq A^N$ ein linearer Code. $B \in A^{k\times N}$ heißt *Erzeugermatrix* von C, falls ihr Zeilentupel eine Basis von C ist. Dann: $dim(C) = k$.

Beispiel

(a) $B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \in \mathbb{F}_2^{3\times 6}$ von Zeilen erzeugter Code:
$C = \{(000000),(001110),(100011),(101101),(010101),(011011),(110110),(111000)\}$

$\Rightarrow d(C) = 3$
$\Rightarrow r(C) = \frac{3}{6} = \frac{1}{2}$
C ist ein $[6,3,3]$-Code.

(b) $B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 6}$ ist ein $[6,3,2]$-Code. (Verdoppelungscode – jedes Wort doppelt senden; nicht optimal, vergleiche (a).)

(13.9) Definition Seien $C, C' \subseteq A^n$ lineare Codes. C, C' heißen äquivalent, falls $\omega \in S_N$ und $\alpha_1, \ldots, \alpha_N \in A^*$ existieren mit

$$C' = \{(\alpha_1 x_{\omega(1)}, \alpha_2 x_{\omega(2)}, \ldots, \alpha_N x_{\omega(N)} | (x_1, x_2, \ldots, x_N) \in C\}.$$

Ist B Erzeugermatrix von C und entsteht B' aus B durch Umsortieren der Spalten und Multiplikation mit Skalaren $\neq 0$, so ist der zu B' gehörende Code C' zu C äquivalent.

Jeder Code ist dask Zeilenstufenform äquivalent zu einem Code mit Erzeugermatrix $(\underbrace{E_k}_{k\times k} \underbrace{P}_{k\times(N-k)}) \in A^{k\times N}$.

(13.10) Definition Schreibe $(x, y) := x \cdot y^t$ für $x, y \in A^N$. Ausgeschrieben: $(x, y) = x_1y_1 + x_2y_2 + \cdots + x_Ny_N$ (Standardskalarprodukt).

(13.11) Bemerkung Stets ist $(x, y) = (y, x)$ bilinear, d.h. $(\xi x + \xi' x', y) = \xi(x, y) + \xi'(x', y)$ und $(x, \eta y + \eta' y') = \eta(x, y) + \eta'(x, y')$ für $x, y, x', y' \in A^N$ und $\xi, \xi', \eta, \eta' \in A$.

(13.12) Definition Sei $C \subseteq A^N$ ein linearer Code. Setze $C^\perp := \{x \in A^N | (x, c) = 0 \forall c \in C\}$. $C^\perp$ ist der zu C *duale* Code.

(13.13) Bemerkung (i) $C^\perp$ ist linearer Code.

(ii) Sei $(c_1, \ldots, c_k)$ Basis von C. Dann: $C^\perp = \{x \in A^N | (x, c_i) = 0 \; \forall 1 \leq i \leq k\}$.

Beweis. (i) Unterraumkriterium anwenden:

(a) $0 \in C^\perp$

(b) $x, y \in C^\perp$, $\xi, \eta \in A$. Zu zeigen: $\xi x + \eta y \in C^\perp$. Sei $c \in C$. Es wird $(\xi x + \eta y, c) = \xi \underbrace{(x, c)}_{=0} + \underbrace{\eta(y, c)}_{=0} = 0$.

(ii) „$\subseteq$“: ✓

„$\supseteq$“: $x \in$ rechte Seite. Zu zeigen: $x \in C^\perp$. Sei $c \in C$. Zu zeigen: $(x, c) = 0$. Schreibe $c = \sum_{i=1}^{k} \alpha_i c_i$, $\alpha_i \in A$. Es wird $(x, c) = (x, \sum_i \alpha_i c_i) = \sum_i \alpha_i \underbrace{(x, c_i)}_{=0} = 0$.

□

(13.14) Satz (i) Es ist $\dim(C^\perp) = N - \dim(C)$.

(ii) Ist $(E_k P) \in A^{k\times N}$ Erzeugermatrix von C, dann ist $(-P^t E_{N-k}) \in A^{(N-k)\times N}$ eine Erzeugermatrix von $C^\perp$.

(iii) $C^{\perp\perp} = C$.

Beweis. (i) Sei $B \in A^{k\times N}$ Erzeugermatrix von C, $k = \dim(C)$. Dann: $C^\perp = \mathrm{Kern}(A^N \to A^k, x \mapsto \underbrace{X \cdot x^t}_{B\cdot x^t=0 \Leftrightarrow \text{ alle Zeilen von } B \text{ senkrecht auf } x})$.
Dimensionssatz (aus lineare Algebra): $\dim(C^\perp) + \underbrace{\mathrm{Rang}(B)}_{=k=\dim(C)} = N$.

(ii) Die Zeilen von $(-P^t E_{N-k})$ liegen in $C^\perp$, da $(E_k P) \cdot \begin{pmatrix} -P \\ E_{N-k} \end{pmatrix} = P - P = 0$, die Zeilentupel von $(-P^t E_{N-k})$ sind linear unabhängig und hat die Länge $N - k = \dim(C^\perp) \Rightarrow$ Basis.

(iii) $\dim(C^{\perp\perp}) \overset{\text{(iii)}}{=} N - \dim(C^\perp) \overset{\text{(ii)}}{=} \dim(C)$. Zu zeigen: $C \subseteq C^{\perp\perp}$. Sei $c \in C$, sei $x \in C^\perp$. Zu zeigen: $(x, c) = 0$. Das aber folgt schon aus $x \in C^\perp$.

□

Beispiel $A = \mathbb{F}_2$, $B = \left(\begin{array}{cc|cccc} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right)$ definiere C. $B' = \left(\begin{array}{cc|cccc} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \in \mathbb{F}_2^{4\times 6}$ Erzeugermatrix von $C^\perp$.

(13.15) Definition Sei $C \subseteq A^N$ ein linearer Code der Dimension k. Eine Matrix $H \in A^{N\times(N-k)}$ vom Rang $N - k$ mit der Eigenschaft, dass für $x \in A^N$ $x \in C \Leftrightarrow x \cdot H = 0$ gilt, heißt *Prüfmatrix* von C.

(13.16) Bemerkung Ist $(E_k P)$ Erzeugermatrix von $C \subseteq A^N$, so ist $\begin{pmatrix} -P \\ E_{N-k} \end{pmatrix}$ eine Prüfmatrix von C.

Denn: $x \in C \Leftrightarrow x = (\underbrace{u}_{k}, \underbrace{v}_{N-k})$ mit $v = uP \Leftrightarrow x = (uv)$ mit $(uv)\begin{pmatrix} -P \\ E \end{pmatrix} = 0 \Leftrightarrow x \begin{pmatrix} -P \\ E \end{pmatrix} = 0$.

(13.17) Definition Sei $C \subseteq A^N$ ein linearer Code mit Prüfmatrix H. Ist $x \in A^N$, so heißt $x \cdot H$ *Syndrom* von x (dieses ist Null gdw. $x \in C$).

(13.18) Bemerkung Sei für alle $s \in A^{N-k}$ ein $x_s \in A^N$ gewählt mit $x_s H = s$ und $\omega(x_s) = \min\{\omega(x) | x \in A^N, x \cdot H = s\}$, dann gilt $A^N \to C : x \mapsto x - x_{x\cdot H}$ ist ein MDD.

$x - x_{x\cdot H}$ ist Codewort (d.h. in C): $(x - x_{x\cdot H}) \cdot H = x \cdot H - x_{x\cdot H} H = x \cdot H - x \cdot H = 0$.

Beispiel $B = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right) \in \mathbb{F}_2^{3\times 5}$ Erzeugermatrix von C,

$H = \left(\begin{array}{cc} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right) \in \mathbb{F}_2^{5\times 2}$ $(2 = N - k)$.

s	x_s (nicht eindeutig, $x_s \cdot H = s$)
(00)	(00000)
(10)	(00010) (oder (00100))
(01)	(10000) (oder (00001))
(11)	(01000)

liefert einen MDD.

Sei das empfangene Wort $(10010) = x'$.
Syndrom $(11) = x'H$.
$x'' = x' - x_{x'\cdot H} = (10010) - (01000) = (11010)$.

13.3 Hamming Codes

(13.19) Definition Sei $A = \mathbb{F}_q$ und $N = \dfrac{q^r - 1}{q - 1}$ für ein $r \in \mathbb{N}$.
(Beachte: N ist die Anzahl der 1-dimensionalen Teilräume von $\mathbb{F}_q^r$, denn $q^r - 1$ ist die Anzahl der Vektoren ungleich 0 und $q - 1$ ist die Anzahl der Erzeuger eines 1-dimensionalen Teilraums.)

Sei $H \in \mathbb{F}_q^{N\times r}$ eine Matrix, deren Zeilen genau die N verschiedenen 1-dimensionalen Teilräume von $\mathbb{F}_q^N$ erzeugen:

$$H = \begin{pmatrix} x_1 \\ \dots \\ x_N \end{pmatrix}$$

mit $\mathbb{F}_q^r = \{0\} \cup \bigcup_{i=1}^{N} \{ax_i | a \in \mathbb{F}_q^*, 1 \le i \le r\}$. Der Code $C := H_N(\mathbb{F}_q) = H_N(q)$ mit Prüfmatrix H heißt der *Hammingcode* der Länge N.

Beispiel $A = \mathbb{F}_2$, $r = 2$, $N = \dfrac{2^2 - 1}{2 - 1} = 3$.

$H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$ (Zeilen = Vektoren $\neq 0$ in $\mathbb{F}_2^2$)

$C = \mathrm{Kern}(H) = \{x \in \mathbb{F}_2^{1\times 3} \,|xH = 0\}$, $\dim(C) = 3 - \mathrm{Rang}(H) = 1$
$\Rightarrow E = (1, 1, 1)$ ist eine Erezeugermatrix für $C = H_3(2)$.

Beispiel $A = \mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$, $\omega = [X]_{X^2+X+1} \in \mathbb{F}_2[X]/(X^2 + X + 1) = \mathbb{F}_4$, $r = 2$, $N = \dfrac{4^2 - 1}{4 - 1} = \dfrac{15}{3} = 5$.

Ist U ein 1-dimensionaler Teilraum von $\mathbb{F}_4^2$, dann ist $U =< (a,b)|a,b \in \mathbb{F}_4 >$. Falls $a \neq 0$, dann ist $U =< (1, \frac{b}{a}) >$; falls $a = 0$, dann ist $U =< (0,1) >$. Dann ist H beispielsweise:

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

Die Erzeugermatrix von $H_5(4)$ ist eine Basismatrix von Kern(H).
Aus Gewohnheit: Kern(H^{tr}).

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & \omega & \omega+1 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & \omega+1 & \omega & 1 \\ 0 & 1 & \omega & \omega+1 & 1 \end{pmatrix}$$

$$\Rightarrow \text{Kern}(H^t r) =< \begin{pmatrix} \omega+1 \\ \omega \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \omega \\ \omega+1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} >$$

(Beachte: Im allgemeinen wären die ersten zwei Einträge der Basisvektoren hier negativ, es gilt jedoch $x = -x$ in $\mathbb{F}_4$.)

Also haben wir nun eine Erzeugermatrix für $H_5(4)$:

$$E = \begin{pmatrix} \omega+1 & \omega & 1 & 0 & 0 \\ \omega & \omega+1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(13.20) Satz Sei $N = \dfrac{q^r - 1}{q-1}$. Dann gibt es (bis auf Äquivalenz) genau einen Hamming-Code $C = H_N(q) \leq \mathbb{F}_q^N$. Diseer hat die Dimension $\dim(C) = N - r$ und den Minimalabstand $d(C) = 3$.

Beweis. Eindeutigkeit: Umordnen der Zeilen bzw. Multiplikation mit Element $\neq 0 \in \mathbb{F}_q$ der Prüfmatrix H von C liefert zu C äquivalenten Code. (Multipliziert man eine Zeile von H mit einem $a \in \mathbb{F}_q, a \neq 0$, so muss man in C die enstsprechende Spalte mit a^{-1} multiplizieren.)

$\dim(C) = N - \text{Rang}(H) = N - r$. Zum Minimalabstand: Sei wie oben die i-te Zeile von H mit x_i bezeichnet. Ein Wort $c = (c_1, \ldots, c_N)$ liegt genau dann in C, falls $c_1 x_1 + \cdots + c_N x_N = 0$. Ist nun $c \neq 0$, so ist $w(c) \geq 3$, da je 2 verschiedene Vektoren x_i linear unabhängig sind. □

(13.21) Bemerkung Sei $C = H_N(q)$, $N = \dfrac{q^r - 1}{q-1}$. Dann ist die Syndrommenge $S = \mathbb{F}_q^r$ gerade die Menge der Vielfachen der Zeilen der Prüfmatrix von H zusammen

mit dem Nullvektor. Ist x_i die i-te Zeile von H und $a \in \mathbb{F}_q$, so ist der eindeutig bestimmte Vertreter zu $ax_i \in S$ gerade das a-fache des i-ten Einheitsvektors $ae_i = (0, \ldots, 0, a, \ldots, 0, \ldots, 0)$ (a an der i-ten Stelle).

(13.22) Definition Ein Code $C \subseteq A^N$ heißt *perfekt*, falls es eine Zahl $e \in \mathbb{N}$ gibt, so dass es zu jedem $a \in A^N$ genau ein $c \in C$ gibt mit $d(c, a) \leq e$.

Beispiel (i) $C = A^N$ ist ein perfekter Code mit $e = 0$.

(ii) Ist $A = \mathbb{F}_2$ und N ungerade, so ist der Wiederholungscode $C = \{(0, \ldots, 0), (1, \ldots, 1)\} \subseteq A^N$ ein perfekter Code mit $e = \dfrac{N-1}{2}$.

(iii) Der Hamming Code $H_7(2)$ ist ein perfekter Code mit $e = 1$.

(13.23) Satz Hamming Codes sind perfekte Codes mit $e = 1$.

Beweis. Sei $C = H_N(q)$ der Hamming Code der Länge $N = \dfrac{q^r - 1}{q - 1}$ mit Prüfmatrix H und $a \in \mathbb{F}_q^N$. Dann gilt entweder $aH = 0$ oder $aH = \alpha x_i = \alpha e_i H \neq 0$ und damit ist aH ein Vielfaches der i-ten Zeile von H. D.h. entweder ist $a \in C$ oder $a - \alpha e_i \in C$. Da $d(a - \alpha e_i, a) = w(\alpha e_i) = 1$ ist gibt es also zu jedem $a \in \mathbb{F}_q^N$ ein $c \in C$ mit $d(a, c) \leq 1$. Die Eindeutigkeit eines solchen c folgt aus $d(C) = 3$. □

Bemerkung Sei C ein perfekter Code binärer Code.
Ist $e = 1$ so ist C ein Hamming Code.
Ist $e > 1$, so ist C entweder ein Wiederholungscode ($C = \{(0, \ldots, 0), (1, \ldots, 1)\}$) oder C ist der binäre Golay Code G_{23} der Länge 23 und Dimension 12. Es gilt $d(G_{23}) = 7$ und G_{23} ist ein perfekter Code mit $e = 3$.

Bemerkung C ist genau dann ein perfekter Code für $e \in \mathbb{N}$, wenn die Kugeln um $c \in C$ mit Radius e paarweise disjunkt sind und ihre Vereinigung $\mathbb{F}_q^N$ ist.

Erweitern von Codes

(13.24) Definition Sei A ein Körper und $C \subseteq A^N$ ein Code. Dann ist der *erweiterte Code* $\tilde{C} = \{(c_1, \ldots, c_N, c_{N+1} \in A^{N+1} | (c_1, \ldots, c_N) \in C, \sum_{i=1}^{N+1} c_i = 0\}$. c_{N+1} ist das Kontrollsymbol.

Beispiel $C \leq \mathbb{F}_2^5$ mit Erzeugermatrix $E = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$, $b_1 := (10011)$, $b_2 := (01111)$. $C = \{0, b_1, b_2, b_1 + b_2\}$ (b_1, b_2) Basis von C. $\tilde{C} \leq \mathbb{F}_2^6$ hat die Erzeugermatrix $\tilde{E} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$

(13.25) Satz Sei $C \leq A^N$ ein linearer Code. Dann ist $\tilde{C} \leq A^{N+1}$ ein linearer Code. Es gilt $\dim(C) = \dim(\tilde{C} =: d$. Ist E eine Erzeugermatrix von C so ist $\tilde{E} = (E|e) \in A^{d\times(N+1}$ eine Erzeugermatrix von $\tilde{C}$ mit $e_i = -\sum j = 1^N E_{i,j}$. Ist H Prüfmatrix für C (d.h. $C = \{x \in A^N | xH = (0, \ldots, 0)\}$), so ist $\tilde{H} = \left(\begin{array}{ccc|c} & & & 1 \\ & H & & \vdots \\ & & & 1 \\ \hline 0 & \ldots & 0 & 0 \end{array}\right)$ eine Prüfmatrix für $\tilde{C}$.

(13.26) Bemerkung Seit $C \leq \mathbb{F}_2^N$ ein linearer binärer Code und $\tilde{C} \leq \mathbb{F}_2^{N+1}$ der erweiterte Code. Dann ist $w(\tilde{c}) = |\{i \in \{1, \ldots, N+1\} | \tilde{c_i} \neq 0\}|$ gerade für alle $\tilde{c} = (\tilde{c_1}, \ldots, \tilde{c_{N+1}}) \in \tilde{C}$. Also ist $d(\tilde{C}) = \min\{w(\tilde{c}) | 0 \neq \tilde{c} \in \tilde{C}\}$ gerade. Ist $d(C)$ also ungerade, so ist $d(\tilde{C}) = d(C) + 1$.

Beweis. $w(\tilde{c}) \equiv_2 \sum_{i=1}^{N+1} \tilde{c_i} = 0 \in \mathbb{F}_2$ also $w(\tilde{c})$ gerade.

$d(\tilde{C}) \geq d(C)$ da $c := (\underbrace{c_1, \ldots, c_N}_{\in C}, c_{N+1}) \in \tilde{C}$ und $w(c) \geq w((c_1, \ldots, c_N))$. Also $d(\tilde{C}) \geq d(C) + 1$.

„=“: $c \in C$ mit $w(c) = d(C)$ (ungerade), dann ist $(c, 1) = (c_1, \ldots, c_N, 1) \in \tilde{C}$ mit Gewicht $d(C) + 1$. □

Beispiel Der erweiterte Hammingcode der Länge 8. $e_8 = \widetilde{H_7(2)}$. $H_7(2) \leq \mathbb{F}_2^7$ ist der Hammingcode der Länge 7. Die Prüfmatrix von $H_7(2)$ hat als Zeilen die Vektoren aus $\mathbb{F}_2^7 \setminus \{0\}$.

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

Erzeugermatrix von $H_7(2)$: $E \in \mathbb{F}_2^{4\times 7}$, $E \cdot H = 0$, $\mathrm{Rang}(E) = 4$.

$$\tilde{E} = \left(\begin{array}{ccccccc|c} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

$\tilde{E} \in \mathbb{F}_2^{4\times 8}$ ist Erzeugermatrix von $e_8 = \widetilde{H_7(2)}$. e_8 ist ein sehr guter Code: $\dim(e_8) = 4$, $\text{Länge}(e_8) = 8$, Informationsrate $= \frac{\dim}{\text{Länge}} = \frac{1}{2} = r(e_8)$ genauso groß wie $r(C)$

mit $C =< (11000000), (00110000), (00001100), (00000011) >$ (Wiederholungscode). $d(C) = 2 < d(e_8) = \underbrace{d(H_7(2))}_{3} + 1 = 4$. $e_8^{\perp} = e_8$ (selbstdual).

Prüfmatrix von e_8 ist $(\tilde{E})^{tr} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$, $\tilde{E} \cdot (\tilde{E})^{tr} = 0$.

Man kann zeigen: $C \leq \mathbb{F}_2^8$, $\dim(C) = 4$, dann ist $d(C) \leq 4$ und falls $d(C) = 4$ dann ist $C \cong e_8$.

14 Zyklische Codes

Für diesen Abschnitt: Sei p Primzahl, $q = p^f$, $\mathbb{F}_q$ der Körper mit q Elementen.

(14.1) Definition Ein linearer Code $C \leq \mathbb{F}_q^N$ heißt *zyklisch* $:\Leftrightarrow (c_1, \ldots, c_N) \in C$, dann auch $(c_N, c_1, \ldots, c_{N-1}) \in C$.

(14.2) Satz (i) Die Abbildung

$$\varphi : \mathbb{F}_q^N \to \mathbb{F}_q[x]/(x^N - 1) : (a_1, \ldots, a_N) \mapsto \sum_{i=1}^{N} a_i [x]_{x^N-1}^{N-i}$$

ist ein $\mathbb{F}_q$-Vektorraum Isomorphismus.

(ii) $C \leq \mathbb{F}_q^N$ ist genau dann ein zyklischer Code, wenn $\varphi(C)$ ein Ideal in $\mathbb{F}_q[x]/(x^n - 1)$ ist.

Beweis. (i) $B = (1, [x]_{x^n-1}, \ldots, [x^{n-1}]_{x^n-1})$ ist $\mathbb{F}_q$-Basis von $\mathbb{F}_q[x]/(x^n - 1)$. $E := (e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_N = (0, \ldots, 0, 1))$ ist $\mathbb{F}_q$-Basis von $\mathbb{F}_q^N$. φ ist bijektive lineare Abbildung die E auf B abbildet. Also ist φ ein Vektorraum Isomorphismus.

(ii)

$$\begin{aligned} & [x]_{x^N-1} \cdot (a_1 + a_2[x] + \cdots + a_N[x^{n-1}]) \\ &= a_1[x]_{x^n-1} + a_2[x^2]_{x^n-1} + \cdots + a_N \underbrace{[x^N]_{x^n-1}}_{1} \\ &= a_N[1]_{x^N-1} + a_1[x]_{x^n-1} + \cdots + a_{N-1}[x^{N-1}]_{x^n-1} \end{aligned}$$

$\varphi(C)$ ist immer ein $\mathbb{F}_q$-Teilvektorraum von $\mathbb{F}_q[x]/(x^N - 1)$. Damit $\varphi(C)$ ein Ideal ist, muss zusätzlich noch $[x]_{x^N-1}\varphi(c) \in \varphi(C)$ sein für alle $c \in C$. Dies ist

nach obiger Rechnung aber genau die Bedingung dafür, dass C ein zyklischer Code ist.

□

Index