Schwerpunkte der Vorlesung Mathematik für Informatik III

Prof. Dr. Konrad Engel [1]
Universität Rostock
Institut für Mathematik
D–18051 Rostock

14. Juli 2019

[1] konrad.engel@uni-rostock.de

Kapitel 1

Kombinatorik

1.1 Grundformeln

Seien A, B endliche Mengen.
Summenregel: $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$
Produktregel: $|A \times B| = |A||B|$
Gleichheitsregel: $\exists$ bijektive Abbildung $f : A \to B \Rightarrow |A| = |B|$

Sei $n := |A|$ und $k := |B|$.

Variationen mit Wiederholung:
Anzahl aller Abbildungen von A in $B = k^n$

Variationen ohne Wiederholung:
Anzahl aller injektiven Abbildungen von A in $B = (k)_n := k(k-1)\dots(k-n+1)$ (fallende Faktorielle)

Permutationen ohne Wiederholung:
Anzahl aller bijektiven Abbildungen von A auf $A = n!$

Permutationen mit Wiederholung:
Sei $i_1 + \dots + i_k = n$. Anzahl aller Abbildungen $f : A \to \{b_1, \dots, b_k\}$, bei denen i_j Elemente von A auf b_j abgebildet werden $= \binom{n}{i_1,\dots,i_k} := \frac{n!}{i_1!\dots i_k!}$

Kombinationen ohne Wiederholung:
Anzahl aller k–elementigen Teilmengen von $A = \binom{n}{k}$

Kombinationen mit Wiederholung:
Anzahl aller Abbildungen $f : \{a_1, \dots, a_n\} \to \mathbb{N}$ mit $f(a_1) + \dots + f(a_n) = k$ $= \binom{n+k-1}{k}$

Satz 1.1.1 (Multinomialsatz)**.** *Es gilt*

$$(a_1 + \cdots + a_k)^n = \sum_{i_1+\cdots+i_k=n} \binom{n}{i_1, \ldots, i_k} a_1^{i_1} \ldots a_k^{i_k}.$$

1.2 Lineare Rekursionsgleichungen

i heißt Fixpunkt der Permutation π von $A :\Leftrightarrow \pi(i) = i$
Derangement-Zahl D_n :=Anzahl der fixpunktfreien Permutationen einer n-elementigen Menge ($D_0 := 1$)

Satz 1.2.1. *Es gilt:*

a) $D_n = (n-1)(D_{n-1} + D_{n-2})$ *für alle* $n \geq 2$

b) $D_n = nD_{n-1} + (-1)^n$ *für alle* $n \geq 1$

Lineare Rekursionsgleichung (LRGL) 1. Ordnung:=Gleichung der Form

$$p_n y_n = q_n y_{n-1} + r_n, n \geq 1, \tag{1.1}$$

wobei $(p_n), (q_n), (r_n)$ gegebene Folgen mit $p_n, q_n \neq 0$ für alle n sind und die Folge (y_n) gesucht ist.
Anfangsbedingung:= Gleichung der Form

$$y_0 = \alpha \tag{1.2}$$

Satz 1.2.2. *Mit*

$$s_n := \begin{cases} \frac{p_1 \ldots p_{n-1}}{q_1 \ldots q_n}, & \text{falls } n > 1 \\ \frac{1}{q_1}, & \text{falls } n = 1 \end{cases}$$

ist die Lösung der LRGL (1.1) und der Anfangsbedingung (1.2) gegeben durch

$$y_n = \frac{1}{s_n p_n} \left(\alpha + \sum_{i=1}^{n} s_i r_i \right).$$

Lineare Rekursionsgleichung (LRGL) k-ter Ordnung mit konstanten Koeffizienten:=Gleichung der Form

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \cdots + a_1 y_{n+1} + a_0 y_n = b_n, n \geq 0, \tag{1.3}$$

wobei die Zahlen $a_k \neq 0, a_{k-1}, \ldots, a_1, a_0 \neq 0$ gegeben sind und die Folge (y_n) gesucht ist. Gilt $b_n = 0$ für alle n, d.h.

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \cdots + a_1 y_{n+1} + a_0 y_n = 0, n \geq 0, \tag{1.4}$$

so heißt die LRGL homogen, ansonsten inhomogen.

Anfangsbedingungen:= Gleichungen der Form

$$y_0 = \alpha_0, \ldots, y_{k-1} = \alpha_{k-1} \tag{1.5}$$

Satz 1.2.3. *Die Menge der Lösungen der homogenen LRGL k–ter Ordnung (1.4) bildet mit der üblichen Addition zweier Folgen + und der üblichen Multiplikation einer Folge mit einer reellen Zahl einen k–dimensionalen Vektorraum L.*

$\{(y_n^{(1)}), \ldots, (y_n^{(k)})\}$ Fundamentalsystem (FLS) von (1.4):$\Leftrightarrow \{(y_n^{(1)}), \ldots, (y_n^{(k)})\}$ Basis von L.

Bestimmung eines FLS für homogene LRGL mit konstanten Koeffizienten:

Ansatz: $y_n = \lambda^n$
Charakteristisches Polynom: $p(\lambda) = a_k\lambda^k + a_{k-1}\lambda^{k-1} + \cdots + a_1\lambda + a_0$
Charakteristische Gleichung: $p(\lambda) = 0$
Jede l–fache reelle Nullstelle λ von $p(\lambda)$ liefert l Folgen für das FLS:

$$(\lambda^n), (n\lambda^n), \ldots (n^{l-1}\lambda^n).$$

Jedes Paar konjugierter l–facher komplexer Nullstellen $\lambda = r(\cos(\varphi) + i\sin(\varphi)), \overline{\lambda} = r(\cos(\varphi) - i\sin(\varphi))$ von $p(\lambda)$ liefert $2l$ Folgen für das FLS:

$$(r^n\cos(n\varphi)), (r^n\sin(n\varphi)), (nr^n\cos(n\varphi)), (nr^n\sin(n\varphi)), \ldots, \\ (n^{l-1}r^n\cos(n\varphi)), (n^{l-1}r^n\sin(n\varphi)).$$

Hat man das FLS $\{(y_n^{(1)}), \ldots, (y_n^{(k)})\}$ für (1.4), so findet man die Lösung (y_n), die auch noch die Anfangsbedingungen (1.5) erfüllt, durch den Ansatz

$$y_n = c_1 y_n^{(1)} + \cdots + c_k y_n^{(k)}$$

und Lösung des LGS

$$\begin{array}{ccccccccc} y_0^{(1)}c_1 & + & y_0^{(2)}c_2 & + & \ldots & + & y_0^{(k)}c_k & = & \alpha_0 \\ y_1^{(1)}c_1 & + & y_1^{(2)}c_2 & + & \ldots & + & y_1^{(k)}c_k & = & \alpha_1 \\ & & & & \ldots & & & & \\ y_{k-1}^{(1)}c_1 & + & y_{k-1}^{(2)}c_2 & + & \ldots & + & y_{k-1}^{(k)}c_k & = & \alpha_{k-1} \end{array}$$

Satz 1.2.4. *Sei $(y_n^{(s)})$ eine spezielle Lösung der inhomogenen LRGL (1.3). $(y_n^{(a)})$ ist Lösung von (1.3) $\Leftrightarrow$ $\exists$ Lösung $(y_n^{(H)})$ von (1.4), sodass $y_n^{(a)} = y_n^{(s)} + y_n^{(H)}$ für alle n ist, d.h., die allgemeine Lösung der inhomogenen LRGL ist Summe aus einer speziellen Lösung der inhomogenen LRGL und einer beliebigen Lösung der zugehörigen homogenen LRGL.*

Ähnlich wie bei DGL kann man spezielle Lösungen mittels Variation der Konstanten bestimmen, was wir hier nicht im Einzelnen behandeln.

Außerdem kann man wie bei DGL bei speziellen rechten Seiten spezielle Lösungen durch analoge Ansätze erhalten, hier nur zwei Beispiele:

1. b_n ist Polynom in n. Dann Ansatz $(y_n^{(s)})$ als Polynom in n mit unbekannten Koeffizienten, die man aus Koeffizientenvergleich durch Einsetzen in (1.3) erhält.

2. b_n ist Potenz in n, deren Basis nicht Nullstelle des charakteristischen Polynoms ist. Dann Ansatz $(y_n^{(s)})$ als gleiche Potenz in n mit unbekanntem Faktor, den man aus Einsetzen in (1.3) erhält.

1.3 Das Prinzip von Inklusion und Exklusion

Satz 1.3.1 (Prinzip von Inklusion und Exklusion)**.** *Seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt:*

$$|A_1 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \cdots +$$
$$(-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}| \pm \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|$$

Folgerung 1.3.1. *Seien die Mengen $A_1, \ldots, A_n$ alle in einer endlichen Menge Ω enthalten. Sind die Mächtigkeiten der Durchschnitte von beliebigen k Mengen immer gleich einer festen Zahl $w(k)$, $k = 1, \ldots, n$, und setzt man $w(0) := |\Omega|$, so gilt*

$$|\Omega \setminus (A_1 \cup \cdots \cup A_n)| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} w(k).$$

Folgerung 1.3.2. *Für die Anzahl D_n aller fixpunktfreien Permutationen von $\{1, \ldots, n\}$ gilt*

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Folgerung 1.3.3. *Die Anzahl aller surjektiven Abbildungen einer n–elementigen Menge A auf eine k–elementige Menge B ist gleich* $\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$

Kapitel 2

Strukturen der Algebra

2.1 Faktormengen

Erinnerung:

(Binäre) Relation R auf A: $R \subseteq A \times A$
Schreibweise: $aRb :\Leftrightarrow (a,b) \in R$
R reflexiv $:\Leftrightarrow \forall a \in A : aRa$
R symmetrisch $:\Leftrightarrow \forall a,b \in A : aRb \Rightarrow bRa$
R transitiv $:\Leftrightarrow \forall a,b,c \in A : aRb \wedge bRc \Rightarrow aRc$
R Äquivalenzrelation $:\Leftrightarrow$ R reflexiv, symmetrisch, transitiv

Äquivalenzklasse von a (bez. R): $[a]_R := \{b \in A : aRb\}$ (kurz $[a]$)

Zerlegung (Partition) einer Menge A: Menge $\{A_i : i \in I\}$ von nichtleeren Teilmengen von A, sodass

$$\bigcup_{i \in I} A_i = A \text{ und } \forall i,j \in I : A_i = A_j \vee A_i \cap A_j = \emptyset.$$

Die Mengen A_i nennt man auch Klassen bzw. Blöcke.

Satz 2.1.1 (Hauptsatz über Äquivalenzrelationen)**.** *Sei A Menge.*

1) *Sei R Äquivalenzrelation auf A. Dann ist $\mathcal{Z} = \{[a] : a \in A\}$ Zerlegung von A.*

2) *Sei $\mathcal{Z} = \{A_i : i \in I\}$ Zerlegung von A. Dann ist die folgendermaßen definierte Relation $R_{\mathcal{Z}}$ eine Äquivalenzrelation: $aR_{\mathcal{Z}}b :\Leftrightarrow \exists i \in I : a,b \in A_i$.*

Wichtiges Beispiele von Äquivalenzrelationen:

1. Zahlenkongruenz modulo n.

Seien $a, b \in \mathbb{Z}$. Sagen a teilt b, d.h. $a|b :\Leftrightarrow \exists q \in \mathbb{Z} : qa = b$.

Sei $A = \mathbb{Z}$ und sei $n > 0$ eine feste natürliche Zahl. Setzen $aRb :\Leftrightarrow n|(b-a)$.
Schreibweise: $a \equiv b \mod n$.

2. Polynomkongruenz modulo p.

Sei z.B. $K \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ und sei $K[x]$ die Menge aller Polynome über K, d.h. die Menge aller Terme der Form $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ mit $a_0, \ldots, a_n \in K$ und $n \in \mathbb{N}$. Seien $f, g \in K[x]$. Sagen f teilt g, d.h. $f|g :\Leftrightarrow \exists q \in K[x] : qf = g$.

Sei $A = K[x]$ und sei $p \in K[x]$ fest. Setzen $fRg :\Leftrightarrow p|(g-f)$.
Schreibweise: $f \equiv g \mod p$.

Sei R Äquivalenzrelation auf A. Die zugehörige Zerlegung $\mathcal{Z} = \{[a] : a \in A\}$ heißt Faktormenge von A bez. R.
Bezeichung: allgemein A/R, bei Zahlenkongruenzen $\mathbb{Z}/_n$ und bei Polynomkongruenzen $K[x]/_p$.

In der Faktormenge wird üblicherweise jedes Element nur einmal aufgelistet.

Sei $S_{n,k}$ die Anzahl der (ungeordneten) Zerlegungen einer n-elementigen Menge in k Klassen, wobei $S_{0,0} := 1$ und $S_{n,0} := S_{0,k} := 0$ für $n, k > 0$ definiert wird.

Die Zahlen $S_{n,k}$ heißen Stirling-Zahlen 2. Art.

Satz 2.1.2. *Es gilt:*

a) $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$ *für* $n, k \geq 1$,

b) $S_{n,k} = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$.

Sei $\circ$ eine innere Verknüpfung auf A (d.h. Abbildung $A \times A \to A$).

Die Äquivalenzrelation R ist kompatibel mit $\circ :\Leftrightarrow \forall a, a', b, b' \in A : aRa' \wedge bRb' \Rightarrow (a \circ b)R(a' \circ b')$

Beispiele:
Zahlenkongruenz kompatibel mit Addition und Multiplikation,
Polynomkongruenz kompatibel mit Addition und Multiplikation.

Satz 2.1.3. *Seien $A \neq \emptyset$ und sei R Äquivalenzrelation auf A, die mit der inneren Verknüpfung $\circ$ kompatibel ist. Dann lässt sich auf A/R eine innere Verknüpfung wie folgt definieren:* $[a] \circ_R [b] := [a \circ b]$.

Die so definierte Verknüpfung ist also wirklich eine Abbildung, d.h. unabhängig von der Wahl der Elemente a, b in den Klassen $[a], [b]$ (man sagt: unabhängig von der Wahl der Repräsentanten a und b der entsprechenden Klassen).

Beispiel: Addition und Multiplikation der Zahlen- bzw. Polynomkongruenzklassen.

2.2 Elemente der Zahlentheorie

$p \in \mathbb{N}$ heißt Primzahl $:\Leftrightarrow p > 1$ und p besitzt in $\mathbb{N}$ nur die Teiler 1 und p.

Satz 2.2.1 (Fundamentalsatz der Zahlentheorie)**.** *Jede natürliche Zahl $n > 1$ ist durch ein Produkt von endlich vielen Primzahlen darstellbar, die nicht notwendig verschieden sind. Bis auf die Reihenfolge der Faktoren ist diese Darstellung, die Primfaktorzerlegung, eindeutig.*

Bemerkung 2.2.1. *Seien $a, b \in \mathbb{N}$ und sei $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ die Primfaktorzerlegung von a. Dann gilt $b|a :\Leftrightarrow b = p_1^{\beta_1} \dots p_n^{\beta_n}$ mit $\beta_1 \leq \alpha_1 \dots, \beta_n \leq \alpha_n$.*

Seien $a, b, t, v \in \mathbb{N}$.
t gemeinsamer Teiler von $a, b :\Leftrightarrow t|a \wedge t|b$
Sei $(a, b) \neq (0, 0)$. d größter gemeinsamer Teiler von $a, b :\Leftrightarrow d$ gemeinsamer Teiler von a, b und für jeden anderen gemeinsamen Teiler t von a, b gilt: $t < d$
Bezeichnung: $d = ggT(a, b)$

v gemeinsames Vielfaches von $a, b :\Leftrightarrow v \neq 0 \wedge a|v \wedge b|v$
Seien $a, b \neq 0$. k kleinstes gemeinsames Vielfaches von $a, b :\Leftrightarrow k$ gemeinsames Vielfaches von a, b und für jedes andere gemeinsame Vielfache v von a, b gilt: $k < v$
Bezeichnung: $k = kgV(a, b)$

Bemerkung 2.2.2. *Bei gegebenen Primfaktorzerlegungen $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ und $b = p_1^{\beta_1} \dots p_n^{\beta_n}$ gilt:*
$ggT(a, b) := p_1^{\min\{\alpha_1, \beta_1\}} \dots p_n^{\min\{\alpha_n, \beta_n\}}$
$kgV(a, b) := p_1^{\max\{\alpha_1, \beta_1\}} \dots p_n^{\max\{\alpha_n, \beta_n\}}$

Satz 2.2.2. *Seien $a, b \neq 0$. Dann gilt $ggT(a, b) \cdot kgV(a, b) = a \cdot b$.*

Lemma 2.2.1. *Seien $a, b \neq 0$, und sei v gemeinsames Vielfaches von a und b. Dann gilt $kgV(a, b)|v$.*

Lemma 2.2.2. *Sei $(a, b) \neq (0, 0)$, und sei t gemeinsamer Teiler von a und b. Dann gilt $t|ggT(a, b)$.*

Lemma 2.2.3. *Sei $(a, b) \neq (0, 0)$ und sei $q \in \mathbb{N}$. Dann gilt $ggT(a, b) = ggT(b, a - qb)$.*

Bezeichnung: $\lfloor x \rfloor$ ist die größte ganze Zahl $\leq x$.

Effizientes Verfahren zur Bestimmung des größten gemeinsamen Teilers (ohne Primfaktorzerlegung zu bestimmen):

Euklidischer Algorithmus
Vor.: $a, b \in \mathbb{N}$, $(a, b) \neq (0, 0)$.
Iteration: Solange $b > 0$ setze $q := \lfloor a/b \rfloor$ und simultan $a := b$, $b := a - q \cdot b$
Ausgabe: $d := a$

Satz 2.2.3. *Der Euklidische Algorithmus bricht nach endlich vielen Schritten ab und liefert den größten gemeinsamen Teiler.*

Satz 2.2.4. *Es existieren $\alpha, \beta \in \mathbb{Z}$, sodass $ggT(a, b) = \alpha a + \beta b$.*

Bestimmung von α und β:

Erweiterter Euklidischer Algorithmus
Vor.: $a, b \in \mathbb{N}$, $(a, b) \neq (0, 0)$.
Initialisierung: $\alpha_0 := 1, \alpha_1 := 0, \beta_0 := 0, \beta_1 := 1$,
Iteration: Solange $b > 0$ setze $q := \lfloor a/b \rfloor$ und simultan $a := b$, $b := a - q \cdot b$ und weiterhin simultan $\alpha_0 := \alpha_1$, $\alpha_1 := \alpha_0 - q \cdot \alpha_1$, $\beta_0 := \beta_1$, $\beta_1 := \beta_0 - q \cdot \beta_1$
Ausgabe: $d := a$, $\alpha := \alpha_0$, $\beta := \beta_0$.

2.3 Halbgruppen und Gruppen

Algebraische Struktur mit n Verknüpfungen:= $(n + 1)$–Tupel $(M, \circ_1, \circ_2, \ldots, \circ_n)$, wobei M eine nichtleere Menge und $\circ_1, \circ_2, \ldots, \circ_n$ innere Verknüpfungen auf M sind.

Halbgruppe:=Algebraische Struktur mit einer Verknüpfung $(H, \circ)$, in der das Assoziativgesetz gilt:

$$\forall a, b, c \in H : a \circ (b \circ c) = (a \circ b) \circ c$$

Satz 2.3.1. *In jeder Halbgruppe $(H, \circ)$ hängt das Produkt der beliebigen Elemente $a_1, \ldots, a_n$ in der durch die Nummerierung gegebenen Anordnung nicht von der Verteilung der Klammern ab.*

$(H, \circ)$ ist kommutativ (abelsch):$\Leftrightarrow \forall a, b \in H : a \circ b = b \circ a$

$e \in H$ neutrales Element :$\Leftrightarrow \forall a \in H : a \circ e = e \circ a = a$
$(H, \circ)$ Monoid :$\Leftrightarrow (H, \circ)$ Halbgruppe mit neutralem Element

Satz 2.3.2. *Jede Halbgruppe besitzt höchstens ein neutrales Element.*

Sei $(H, \circ)$ Monoid mit neutralem Element e.
$a \in H$ invertierbar:$\Leftrightarrow \exists a' \in H : a \circ a' = a' \circ a = e$.
Ein solches Element a' heißt Inverses von a (invers zu a).

Satz 2.3.3. *Jedes Element eines Monoids besitzt höchstens ein Inverses.*

Allgemeine Bezeichnung des zu a inversen Elementes: a^{-1}

Gruppe:=Algebraische Struktur $(G, \circ)$ mit einer Verknüpfung, für die gilt:
(A) $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$ (d.h. $(G, \circ)$ ist Halbgruppe)
(E) $\exists e \in G \; \forall a \in G : a \circ e = a$
(I) $\forall a \in G \; \exists a' \in G : a \circ a' = e$

Satz 2.3.4. $(G, \circ)$ *ist Gruppe* $\Leftrightarrow$ $(G, \circ)$ *Monoid, in dem alle Elemente invertierbar sind.*

$(G, \circ)$ ist kommutativ (abelsch):$\Leftrightarrow$
(K) $\forall a, b \in G : a \circ b = b \circ a$

Additiv geschriebene Gruppe: $(G, +)$ mit $0 := e$ und $-a := a^{-1}$
Multiplikativ geschriebene Gruppe: $(G, \cdot)$ mit $1 := e$

Einfache Beispiele: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}/_n, +)$

Es folgen zwei weitere Beispiele:

Erinnerung: $S_n :=$ Menge aller Permutationen von $\{1, \ldots, n\}$, $\circ :=$Hintereinanderausführung von Abbildungen.

Satz 2.3.5. $(S_n, \circ)$ *ist eine Gruppe, die sogenannte symmetrische Gruppe .*

Seien im Folgenden $a, b \in \mathbb{N}$

$[a]$ prime Restklasse modulo n (a und n sind prim):$\Leftrightarrow ggT(a, n) = 1$

Betrachten algebraische Struktur $(P_n, \cdot)$ mit
$P_n := \{[a] : [a]$ prime Restklasse modulo $n\}$
$[a] \cdot [b] := [a \cdot b]$

Satz 2.3.6. $(P_n, \cdot)$ *ist eine abelsche Gruppe, die Gruppe der primen Restklassen modulo n.*

Satz 2.3.7. *Sei $(G, \circ)$ Gruppe. Dann gilt:*

a) $\forall a, b \in G : (a \circ b)^{-1} = b^{-1} \circ a^{-1}$

b) $\forall a \in G : (a^{-1})^{-1} = a$

c) $\forall a, b \in G$ *besitzen die Gleichungen* $a \circ x = b$ *und* $y \circ a = b$ *jeweils genau eine Lösung* x *bzw.* y

d) $\forall a, b, x \in G : \ a \circ x = b \circ x \Rightarrow a = b$ *und* $x \circ a = x \circ b \Rightarrow a = b$

Potenzen von Gruppenelementen: Sei $a \in G$, $n \in \mathbb{N} \setminus \{0\}$.

$a^0 := e$
$a^n := a \circ a \circ \cdots \circ a$ (n Faktoren)
$a^{-n} := a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}$ (n Faktoren)

Bei additiver Schreibweise: $0a = 0$ statt $a^0 = e$, na statt a^n, $-na$ statt a^{-n}

Satz 2.3.8. *Sei $(G, \circ)$ Gruppe, $a \in G$, $m, n \in \mathbb{Z}$. Dann gilt:*

a) $a^n \circ a^m = a^{n+m}$

b) $(a^n)^{-1} = (a^{-1})^n = a^{-n}$

Ordnung des Elementes a: $ord(a) := \min\{n \in \mathbb{N} \setminus \{0\} : a^n = e\}$
Falls kein solches n existiert, setzt man $ord(a) := \infty$.

Bemerkung 2.3.1. *Ist G endlich, so hat jedes Element von G endliche Ordnung.*

Gruppe $(G', \circ')$ Untergruppe der Gruppe $(G, \circ) :\Leftrightarrow G' \subseteq G$ und $\forall g_1, g_2 \in G'$: $g_1 \circ' g_2 = g_1 \circ g_2$

Schreibweise einfach $(G', \circ)$ statt $(G', \circ')$, obwohl $\circ'$ und $\circ$ i.Allg. unterschiedlichen Definitionsbereich haben. Auch im Folgenden wird die Einschränkung von $\circ$ auf einen kleineren Definitionsbereich meist mit $\circ$ bezeichnet.

Bezeichnung, falls die innere Verknüpfung klar ist: $G' \leq G$

Bemerkung 2.3.2. *Neutrales Element und inverse Elemente der Untergruppe stimmen mit dem neutralen Element und den entsprechenden inversen Elementen der Gruppe überein.*

Satz 2.3.9 (Untergruppenkriterien)**.** *Sei $(G, \circ)$ Gruppe und $\emptyset \neq U \subseteq G$. Dann ist $(U, \circ)$ Untergruppe, falls eine der folgenden Bedingungen erfüllt ist.*

a) $\forall a, b \in U : \ a \circ b \in U$ *und* $a^{-1} \in U$

b) $\forall a, b \in U : a \circ b^{-1} \in U$

c) $\forall a, b \in U : a^{-1} \circ b \in U$

d) U *endlich und* $\forall a, b \in U : a \circ b \in U$

Seien $(G_1, \circ_1)$ und $(G_2, \circ_2)$ Gruppen. $(G_1, \circ_1)$ isomorph zu $(G_2, \circ_2)$ $:\Leftrightarrow$ es existiert eine bijektive Abbildung $f : G_1 \to G_2$, sodass $\forall a, b \in G_1 : f(a \circ_1 b) = f(a) \circ_2 f(b)$. f heißt Isomorphismus.

Bemerkung 2.3.3. *"Isomorphsein" ist eine Äquivalenzrelation in der Menge aller Gruppen.*

Bezeichnung: $(G_1, \circ_1) \cong (G_2, \circ_2)$.

Seien $(G_1, \circ_1)$ und $(G_2, \circ_2)$ Gruppen. $f : G_1 \to G_2$ heißt Homomorphismus $:\Leftrightarrow \forall a, b \in G_1 : f(a \circ_1 b) = f(a) \circ_2 f(b)$. Ist zusätzlich f surjektiv, so heißt $(G_2, \circ_2)$ homomorphes Bild von $(G_1, \circ_1)$.

Satz 2.3.10 (Satz von Cayley)**.** *Sei* $(G, \circ)$ *eine endliche Gruppe,* $|G| = n$*. Dann existiert eine Untergruppe* $(U, \circ)$ *von* $(S_n, \circ)$ *mit* $(U, \circ) \cong (G, \circ)$*.*

Sei $(G, \circ)$ Gruppe, $(U, \circ)$ Untergruppe und $a \in G$. Sei
$a \circ U := \{a \circ u : u \in U\}$
$U \circ a := \{u \circ a : u \in U\}$
Definieren Relationen R_L und R_R auf G:
$\forall a, b \in G : aR_Lb :\Leftrightarrow a^{-1} \circ b \in U$
$\forall a, b \in G : aR_Rb :\Leftrightarrow b \circ a^{-1} \in U$

Satz 2.3.11.

a) Die Relationen R_L *und* R_R *sind Äquivalenzrelationen auf* G*. Für die Äquivalenzklassen gilt:* $[a]_{R_L} = a \circ U$*,* $[a]_{R_R} = U \circ a$*.*

b) Die Äquivalenzklassen haben alle gleiche Mächtigkeit.

Die Äquivalenzklassen $a \circ U$ bzw. $U \circ a$ heißen Links- bzw. Rechtsnebenklassen von $(G, \circ)$ nach $(U, \circ)$.

Sei G endlich.
Index von $(U, \circ)$ in $(G, \circ)$:=Anzahl der Links- bzw. Rechtsnebenklassen von $(G, \circ)$ nach $(U, \circ)$
Bezeichnung: $[G : U]$

Folgerung 2.3.1 (Satz von Lagrange)**.** *Sei* $(U, \circ)$ *Untergruppe von* $(G, \circ)$*, G endlich. Dann gilt:*

a) $|G| = [G : U] \cdot |U|$

b) $|U|$ *ist Teiler von* $|G|$

Folgerung 2.3.2. *Sei* $(G, \circ)$ *endliche Gruppe,* $a \in G$*. Dann gilt:* $a^{|G|} = e$*.*

Sei $\varphi(n) := |P_n|$ (= Anzahl der primen Restklassen modulo $n = |\{a \in \{1, \ldots, n-1\}: ggT(a, n) = 1\}|$).
$\varphi(n)$ heißt Eulersche Funktion.

Satz 2.3.12.

a) Sei p Primzahl. Dann gilt $\varphi(p) = p - 1$*.*

b) Sei $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$*. Dann gilt* $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$*.*

Satz 2.3.13 (Satz von Fermat–Euler)**.**

a) Sei p Primzahl und $a \in \mathbb{N}$*. Dann gilt* $a^p \equiv a \mod p$*.*

b) Seien $a, n \in \mathbb{N}$*,* $ggT(a, n) = 1$*. Dann gilt* $a^{\varphi(n)} \equiv 1 \mod n$*.*

2.4 Ringe und Körper

Ring:=Algebraische Struktur $(R, +, \cdot)$ mit zwei Verknüpfungen, sodass gilt:

1. $(R, +)$ ist abelsche Gruppe
2. $(R, \cdot)$ ist Halbgruppe
3. Es gelten die beiden Distributivgesetze:
   $\forall a, b, c : a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$

Kommutativer Ring:= Ring $(R, +, \cdot)$, wo $(R, \cdot)$ abelsche Halbgruppe ist.

Beispiele: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}/_n, +, \cdot)$

Bezeichnung:
Kurz R statt $(R, +, \cdot)$
Nullelement 0:= neutrales Element bez. $+$
Einselement 1:= neutrales Element bez. $\cdot$ (falls es existiert)
$-a$:=inverses Element von a bez. $+$

Satz 2.4.1. *Sei R ein Ring. Dann gilt:*

a) $\forall a \in R : 0 \cdot a = a \cdot 0 = 0$

b) $\forall a, b \in R : a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

c) $\forall a, b \in R : (-a) \cdot (-b) = a \cdot b$

Körper:=Algebraische Struktur $(K, +, \cdot)$ mit zwei Verknüpfungen, sodass gilt:

1. $(K, +, \cdot)$ ist kommutativer Ring
2. $(K \setminus \{0\}, \cdot)$ ist Gruppe

Beispiele: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ $(\mathbb{Z}/_p, +, \cdot)$, wobei p Primzahl ist.
Sei R kommutativer Ring. a Nullteiler $:\Leftrightarrow a \neq 0 \wedge \exists b \in R \setminus \{0\}$ sodass $a \cdot b = 0$.

Satz 2.4.2. *Sei R kommutativer Ring mit Einselement. Dann gilt:*

a) R Körper $\Rightarrow$ R hat keine Nullteiler

b) R hat keine Nullteiler und R ist endlich und $|R| \geq 2 \Rightarrow$ R ist Körper.

Sei K ein Körper. Das Polynom $p \in K[x]$ heißt irreduzibel $:\Leftrightarrow$ die einzigen Teiler von p sind die Polynome 0-ten Grades $a \in K \setminus \{0\}$ und die skalaren Vielfachen ap mit $a \in K \setminus \{0\}$.

Satz 2.4.3. *Sei K ein Körper und $p \in K[x]$ irreduzibel. Dann ist auch $K[x]/_p$ ein Körper.*

Seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ Körper. $(K_1, +_1, \cdot_1)$ isomorph zu $(K_2, +_2, \cdot_2)$ $:\Leftrightarrow$ es existiert eine bijektive Abbildung $f : K_1 \to K_2$, sodass $\forall a, b \in K_1 : f(a +_1 b) = f(a) +_2 f(b)$ und $f(a \cdot_1 b) = f(a) \cdot_2 f(b)$. f heißt Isomorphismus.

Satz 2.4.4. *Sei $(K, +, \cdot)$ Körper, für den K endlich ist. Dann existieren eine Primzahl p und eine natürliche Zahl n, sodass $|K| = p^n$ ist. Dieser Körper kann wie in Satz 2.4.3 mittels eines irreduziblen Polynoms vom Grad n über $\mathbb{Z}/_p$ konstruiert werden. Jeder andere Körper der Mächtigkeit p^n ist zu diesem Körper isomorph.*

Kapitel 3

Anwendungen der Algebra

3.1 Kryptographie und der RSA-Algorithmus

Nachricht:=Folge von Zahlen (z.B. über ASCII–Code und Blockbildung)
Ein Absender A möchte eine Nachricht an einen Empfänger E schicken. Hierbei soll jede einzelne Zahl von A verschlüsselt und von E entschlüsselt werden. Die Entschlüsselung soll nur E möglich sein, nicht einmal A darf es nach der Verschlüsselung können.

RSA–Verfahren:

1. E wählt zwei Primzahlen p und q (meist mit Hilfe des Miller-Rabin-Primzahltestes) sowie einen privaten Schlüssel in Form einer Zahl g, die zu $m := (p-1)(q-1)$ teilerfremd ist und in $\{1, \ldots, m\}$ liegt.

2. E ermittelt eine Zahl $k \in \{1, \ldots, m\}$, für die $kg \equiv 1 \mod m$ gilt und sendet diese Zahl k sowie die Zahl $n := pq$ (öffentlich) an A.

3. A verschlüsselt die Zahl $a \in \{0, \ldots, n-1\}$ mittels $a \to e := a^k \mod n$ (Repräsentant e in $\{0, \ldots, n-1\}$).

4. E entschlüsselt die Zahl e mittels $e \to b := e^g \mod n$ (Repräsentant b in $\{0, \ldots, n-1\}$).

Satz 3.1.1. *Im RSA–Verfahren gilt $a = b$.*

Bemerkung 3.1.1. *a) Aus n und m kann man sehr leicht p und q ermitteln.*

b) Würde ein Unbefugter in vernünftiger Zeit aus der öffentlichen Zahl n die Zahl m und damit aus dem öffentlichen Schlüssel k den geheimen Schlüssel g ermitteln können, so könnte er die Zahl n in vernünftiger Zeit faktorisieren: $n = pq$.

c) Es gibt aber trotz massiver Bemühungen bisher noch keinen effizienten Algorithmus zur Faktorisierung.

3.2 Elemente der Codierungstheorie

Die Erkennung von Fehlern (ohne Korrektur) kann einfach mittels einer Prüfziffer realisiert werden. Betrachten als Beispiel den ISBN-Code:

9 Ziffern $a_1, a_2, \ldots, a_9$ und eine Prüfziffer $a_{10} \in \{0, 1, \ldots 9, X\}$ (mit $X := 10$), sodass

$$a_{10} \equiv \sum_{i=1}^{9} i a_i \mod 11$$

Beispiel: ISBN 0-521-45206-6

Satz 3.2.1. *Der ISBN-Code erkennt Einzelfehler und Vertauschungen an beliebigen Stellen.*

Betrachten nun in einer allgemeinen Formulierung die Frage nach der Korrektur von Fehlern.

Gegeben sei ein Alphabet A. Wollen die Elemente von A als n–dimensionale Vektoren mit Elementen aus $\{0, 1\}$, d.h. als Elemente von $K^{n\times 1}$ mit $K := \mathbb{Z}/_2$ darstellen. Verschiedenen Zeichen sollen natürlich verschiedene Vektoren entsprechen. Tritt bei der Übertragung der Vektoren an höchstens einer Stelle ein Fehler auf, so soll das ursprüngliche Zeichen trotzdem eindeutig bestimmbar sein. Benötigen daher eine Funktion $f : A \to K^{n\times 1}$, sodass für $C := \{f(z) : z \in A\}$ gilt: Die Vektoren aus C unterscheiden sich an wenigstens 3 Stellen. Eine solche Menge heißt 1–Fehler–korrigierender Code.

Sinnvolles Ziel: Finde für gegebenes A einen 1–Fehler–korrigierenden Code C, für den n minimal ist!

Äquivalentes Problem: Finde für gegebenes n einen 1–Fehler–korrigierenden Code $C \subseteq K^{n\times 1}$, für den $|C|$ maximal ist.

Satz 3.2.2. *Sei $C \subseteq K^{n\times 1}$ ein 1–Fehler–korrigierender Code. Dann gilt*

$$|C| \leq \frac{2^n}{n+1}.$$

$|C|$ ist sicher dann maximal, wenn $|C| = \frac{2^n}{n+1}$, d.h. wenn C "perfekt" ist. Konstruieren nun einen solchen perfekten Code im Spezialfall $n = 2^l - 1$, wobei $l \in \mathbb{N} \setminus \{0\}$ ist.

Für $a \in \{1, \ldots, 2^l - 1\}$ sei $\boldsymbol{h}_a$ derjenige Vektor $(h_{1a}, h_{2a} \ldots, h_{la})^{\mathbf{T}}$, für den $a = h_{la}2^{l-1} + h_{l-1,a}2^{l-2} + \cdots + h_{1a}$ gilt. $\boldsymbol{h}_a$ kann also als Binärdarstellung von a angesehen werden.

Sei $H = (\boldsymbol{h}_1 | \ldots | \boldsymbol{h}_{2^l-1})$. Offenbar ist $[H] = l \times n$. Über $K = \mathbb{Z}/_2$ sei

$$C := \{\boldsymbol{c} : H\boldsymbol{c} = \boldsymbol{0}\}.$$

Satz 3.2.3. *a) C ist 1–Fehler–korrigierend.*

b) $|C| = \frac{2^n}{n+1}$.

c) Unterscheidet sich $\boldsymbol{x}$ von einem Element $\boldsymbol{c} \in C$ an der Stelle j, so gilt $H\boldsymbol{x} = \boldsymbol{h_j}$, d.h. j kann aus dem 1–fehlerbehafteten $\boldsymbol{x}$ leicht berechnet und somit $\boldsymbol{x}$ zu $\boldsymbol{c}$ korrigiert werden.

Der so konstruierte Code heißt Hamming–Code.

Die Matrix H heißt Kontrollmatrix.

Eine Matrix G, deren Spalten aus einer Basis von C gebildet werden, heißt Generatormatrix.

Sei nun q eine Primzahlpotenz und $K = GF(q)$ der Körper aus q Elementen. Betrachten Teilmengen C von $K^{n\times 1}$ als Codes. Seien $\boldsymbol{a}, \boldsymbol{b} \in K^{n\times 1}$.
Hamming-Abstand von $\boldsymbol{a}$ und $\boldsymbol{b}$: $\rho(\boldsymbol{a}, \boldsymbol{b}) := |\{i : a_i \neq b_i\}|$,
Hamming-Gewicht von $\boldsymbol{a}$: $w(\boldsymbol{a}) := |\{i : a_i \neq 0\}|$.
Der Code C heißt
t-fehlererkennend $:\Leftrightarrow \forall \boldsymbol{a}, \boldsymbol{b} \in C : \boldsymbol{a} \neq \boldsymbol{b} \Rightarrow \rho(\boldsymbol{a}, \boldsymbol{b}) \geq t + 1$,
t-fehlerkorrigierend $:\Leftrightarrow \forall \boldsymbol{a}, \boldsymbol{b} \in C : \boldsymbol{a} \neq \boldsymbol{b} \Rightarrow \rho(\boldsymbol{a}, \boldsymbol{b}) \geq 2t + 1$.
Von Interesse sind also Codes C, für die

$$d(C) := \min\{\rho(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a}, \boldsymbol{b} \in C, \boldsymbol{a} \neq \boldsymbol{b}\}$$

möglichst groß ist.

C heißt linearer (n, k)-Code $:\Leftrightarrow C$ ist k-dimensionaler Teilraum des Vektorraums $K^{n\times 1}$.

Lemma 3.2.1. *Sei $C \subseteq K^{n\times 1}$ ein linearer (n, k)-Code. Dann gilt:*

a) $\rho(\boldsymbol{a}, \boldsymbol{b}) = w(\boldsymbol{b} - \boldsymbol{a})$ für alle $\boldsymbol{a}, \boldsymbol{b} \in K^{n\times 1}$,

b) $d(C) = \min\{w(\boldsymbol{a}) : \boldsymbol{a} \in C, \boldsymbol{a} \neq \boldsymbol{0}\}$,

c) $|C| = q^k$.

Satz 3.2.4. *Sei* $C \subseteq K^{n\times 1}$ *ein linearer* (n,k)*-Code und sei* $C = \{\boldsymbol{c} \in K^{n\times 1} : H\boldsymbol{c} = \boldsymbol{0}\}$ *mit einer* $((n-k)\times n)$*-Matrix* $H = (\boldsymbol{h}_1|\ldots|\boldsymbol{h}_n)$ *vom Rang* $n-k$*. Dann gilt:* $d(C) \geq \tau \Leftrightarrow$ *je* $\tau - 1$ *von den Vektoren* $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_n$ *in* $K^{(n-k)\times 1}$*sind linear unabhängig.*

Beispiel: Reed-Solomon-Code.
Sei $K = GF(q) = \{0, 1, a_1, \ldots, a_{q-2}\}$, $\tau < q+2$. Wähle

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 1 & a_1 & \ldots & a_{q-2} \\ 0 & 0 & 1 & a_1^2 & \ldots & a_{q-2}^2 \\ & & & & \vdots & \\ 1 & 0 & 1 & a_1^{\tau-2} & \ldots & a_{q-2}^{\tau-2}. \end{pmatrix}$$

Man erhält einen $(q+1, q+2-\tau)$-Code mit $d(C) \geq \tau$.

Kapitel 4

Lineare Optimierung

4.1 Problemstellung

Seien $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^{n\times 1}$.
Bezeichnung: $\boldsymbol{x} \leq \boldsymbol{y} :\Leftrightarrow \forall i \in [n] := \{1, \ldots, n\} : x_i \leq y_i$
Allgemeines lineares Optimierungsproblem (LOP):
Gegeben: $A \in \mathbb{R}^{m\times n}, A' \in \mathbb{R}^{m'\times n}, A'' \in \mathbb{R}^{m''\times n}, \boldsymbol{b} \in \mathbb{R}^{m\times 1}, \boldsymbol{b'} \in \mathbb{R}^{m'\times 1}, \boldsymbol{b''} \in \mathbb{R}^{m''\times 1}, \boldsymbol{c} \in \mathbb{R}^{n\times 1}$
Gesucht: $\boldsymbol{x} \in \mathbb{R}^{n\times 1}$, sodass

$$\begin{array}{rl} A\boldsymbol{x} & = \boldsymbol{b} \\ A'\boldsymbol{x} & \leq \boldsymbol{b'} \\ A''\boldsymbol{x} & \geq \boldsymbol{b''} \\ \boldsymbol{c}^{\mathrm{T}}\boldsymbol{x} & \to \text{max bzw. min} \end{array} \tag{4.1}$$

Zulässiger Bereich: Z:=$\{\boldsymbol{x} \in \mathbb{R}^{n\times 1} : A\boldsymbol{x} = \boldsymbol{b}, A'\boldsymbol{x} \leq \boldsymbol{b'}, A''\boldsymbol{x} \geq \boldsymbol{b''}\}$
$\boldsymbol{x}$ ist zulässig :$\Leftrightarrow \boldsymbol{x} \in Z$
Zielfunktion (ZF): $f(\boldsymbol{x}) := \boldsymbol{c}^{\mathrm{T}}\boldsymbol{x}$
$\boldsymbol{x}$ ist optimale Lösung :$\Leftrightarrow \boldsymbol{x} \in Z$ und $\forall \boldsymbol{x'} \in Z$:
$f(\boldsymbol{x}) \geq f(\boldsymbol{x'})$ bei ZF $\to$ max bzw. $f(\boldsymbol{x}) \leq f(\boldsymbol{x'})$ bei ZF $\to$ min.

4.2 Graphische Lösung im Fall $n = 2$

Wissen von der Hesseschen Normalform: Durch eine Ungleichung der Form

$$ax + by \leq c \quad (\text{bzw. } ax + by \geq c)$$

mit $(a, b) \neq (0, 0)$ wird eine Halbebene beschrieben, deren Rand die durch $ax+by = c$ gegebene Gerade ist und in die, ausgehend von dieser Geraden, der negative Stellungsvektor $(-a, -b)$ (bzw. der Stellungsvektor (a, b)) zeigt. Bei mehreren linearen Ungleichungen ist also der zulässige Bereich Durchschnitt entsprechender Halbebenen, den man auch (konvexes) Polyeder nennt. Will man das Verhalten einer linearen Zielfunktion $f(x, y) = ax + by$ studieren, so betrachtet man zunächst eine Niveaulinie (Gerade) der Form $ax + by = c$. Auf dieser Geraden hat die Zielfunktion den konstanten Wert c. Verschiebt man nun die Gerade in Richtung des Stellungsvektors (a, b) parallel, so erhält man eine neue Gerade der Form $ax + by = d$. Hierbei ergibt sich d aus

$$d = a(x + \lambda a) + b(y + \lambda b) = ax + by + \lambda(a^2 + b^2) = c + \lambda(a^2 + b^2),$$

wenn um den Vektor $\lambda(a, b)$ mit $\lambda > 0$ verschoben wurde. Insbesondere ist $d > c$, sodass sich hierbei der Wert der Zielfunktion vergrößert.

Bei einem Maximierungsproblem versucht man nun, die Gerade soweit wie möglich parallel in Richtung des Stellungsvektors zu verschieben, sodass sie noch Punkte des zulässigen Bereichs enthält. In der Extremlage (falls sie existiert) sind die Schnittpunkte der Gerade mit dem zulässigen Bereich offenbar genau die optimalen Lösungen. Falls keine Extremlage existiert, gibt es klarerweise auch keine optimale Lösung.

Bei einem Minimierungsproblem wählt man die entgegengesetzte Richtung bei der Verschiebung.

4.3 Transformation auf Normalform

Beachte:
$\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x} \geq b \Leftrightarrow -\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x} \leq -b$
$\boldsymbol{c}^{\mathrm{T}}\boldsymbol{x} \to \min \Leftrightarrow -\boldsymbol{c}^{\mathrm{T}}\boldsymbol{x} \to \max$

Deswegen können wir statt von (4.1) gleich von dem vereinfachten LOP

$$\begin{aligned} A\boldsymbol{x} &= \boldsymbol{b} \\ A'\boldsymbol{x} &\leq \boldsymbol{b'} \\ \boldsymbol{c}^{\mathrm{T}}\boldsymbol{x} &\to \max \end{aligned} \tag{4.2}$$

ausgehen.

Ein LOP ist in Normalform gegeben, falls es die Form hat:

$$\begin{aligned} A\boldsymbol{x} &= \boldsymbol{b} \\ \boldsymbol{x} &\geq \boldsymbol{0} \\ \boldsymbol{c}^{\mathrm{T}}\boldsymbol{x} &\to \max \end{aligned} \tag{4.3}$$

Die Transformation von (4.2) in die Form (4.3) wird wie folgt durchgeführt:
1. Führe für jede Ungleichung $\boldsymbol{a}^{\mathbf{T}}\boldsymbol{x} \leq b$ eine Schlupfvariable z ein, sodass aus der Ungleichung eine Gleichung $\boldsymbol{a}^{\mathbf{T}}\boldsymbol{x} + z = b$ mit $z \geq 0$ wird.
2. Führe eine neue Variable y_{n+1} sowie neue Variablen y_j, $j = 1, \ldots, n$, ein und ersetze jede Variable x_j durch $y_j - y_{n+1}$ (später kann man dann auch jedes y wieder als x schreiben).
Es entsteht das LOP in Normalform (mit $\mathbf{1}^{\mathbf{T}} = (1, \ldots, 1)$):

$$\begin{aligned} \begin{pmatrix} A| & -A\mathbf{1} & |O \\ A'| & -A'\mathbf{1} & |E \end{pmatrix} \begin{pmatrix} \boldsymbol{y} \\ y_{n+1} \\ \boldsymbol{z} \end{pmatrix} &= \boldsymbol{b} \\ \begin{pmatrix} \boldsymbol{y} \\ y_{n+1} \\ \boldsymbol{z} \end{pmatrix} &\geq \mathbf{0} \\ (\boldsymbol{c}^{\mathbf{T}}| - \boldsymbol{c}^{\mathbf{T}}\mathbf{1}|\mathbf{0}^{\mathbf{T}}) \begin{pmatrix} \boldsymbol{y} \\ y_{n+1} \\ \boldsymbol{z} \end{pmatrix} &\to \max \end{aligned} \tag{4.4}$$

Satz 4.3.1.

a) Ist durch $\boldsymbol{y}, y_{n+1}, \boldsymbol{z}$ eine zulässige Lösung von (4.4) gegeben, so ist $\boldsymbol{x} := \boldsymbol{y} - y_{n+1}\mathbf{1}$ eine zulässige Lösung von (4.2) mit dem gleichen Wert der Zielfunktion.

b) Ist durch $\boldsymbol{x}$ eine zulässige Lösung von (4.2) gegeben, so ist $y_{n+1} := \max\{0, -x_1, \ldots, -x_n\}$, $\boldsymbol{y} := \boldsymbol{x} + y_{n+1}\mathbf{1}$ und $\boldsymbol{z} := \boldsymbol{b}' - A'\boldsymbol{x}$ eine zulässige Lösung von (4.4) mit dem gleichen Wert der Zielfunktion.

Folgerung 4.3.1.

a) Das LOP (4.2) hat genau dann eine optimale Lösung, wenn dies für das LOP (4.4) gilt. Man erhält mittels Satz 4.3.1 aus einer optimalen Lösung eines der beiden LOPs eine jeweilige optimale Lösung des anderen LOPs.

b) Der zulässige Bereich von (4.4) ist genau dann leer, wenn dies auch für (4.2) gilt.

c) Die Zielfunktion von (4.4) ist genau dann auf dem zulässigen Bereich unbeschränkt, wenn dies für (4.2) gilt.

Bemerkung 4.3.1. *Hat man ein LOP, bei dem schon für einige Variablen eine Nichtnegativitätsbedingung vorhanden ist, so braucht man nur noch für die restlichen Variablen x_j die Ersetzung $x_j := y_j - y_{n+1}$ vorzunehmen.*

Bemerkung 4.3.2. *Eine vereinfachte Variante zur Einführung von Nichtnegativitätsbedingungen besteht darin, dass man jede entsprechende Variable x als Differenz $x = x' - x''$ zweier nichtnegativer Variablen $x', x'' \geq 0$ schreibt. Hierbei verdoppelt sich allerdings die Anzahl der Variablen.*

4.4 Basisdarstellungen

Sei ein LOP in Normalform (4.3) gegeben, wobei hier vorausgesetzt wird:
A ist eine $m \times (n+m)$ Matrix mit $rg(A) = m$.
Sei $\boldsymbol{A}_j$ der j-te Spaltenvektor von A, $j \in J := \{1, \ldots, n+m\}$.
Basis von $A :=$ Menge von m linear unabhängigen Spaltenvektoren von A.
Basismenge:=Menge $B \subseteq J$ von Indizes, sodass $\{\boldsymbol{A}_j, j \in B\}$ Basis von A ist.
Basisvariable (BV): Alle Variablen x_j mit $j \in B$.
Nichtbasismenge:=Menge $NB \subseteq J$, sodass $J \setminus NB$ Basismenge ist.
Nichtbasisvariable (NBV): Alle Variablen x_j mit $j \in NB$.

Für $S = \{j_1, \ldots, j_s\} \subseteq J$ sei

$$A_S := (\boldsymbol{A}_{j_1} | \ldots | \boldsymbol{A}_{j_s}), \boldsymbol{x}_S := \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_s} \end{pmatrix}, \boldsymbol{c}_S := \begin{pmatrix} c_{j_1} \\ \vdots \\ c_{j_s} \end{pmatrix}$$

Satz 4.4.1. *Sei B Basismenge für A. Das folgende LOP hat den gleichen zulässigen Bereich und auf dem zulässigen Bereich die gleiche Zielfunktion wie (4.3):*

$$\begin{array}{rl} \boldsymbol{x}_B & = A_B^{-1}\boldsymbol{b} - A_B^{-1}A_{NB}\boldsymbol{x}_{NB} \\ \boldsymbol{x} & \geq \boldsymbol{0} \\ \boldsymbol{c}_B^{\mathrm{T}}A_B^{-1}\boldsymbol{b} & -(\boldsymbol{c}_B^{\mathrm{T}}A_B^{-1}A_{NB} - \boldsymbol{c}_{NB}^{\mathrm{T}})\boldsymbol{x}_{NB} \to \max \end{array} \tag{4.5}$$

Sei

$$R := A_B^{-1}A_{NB}, \boldsymbol{s} := A_B^{-1}\boldsymbol{b}, \boldsymbol{g} := \boldsymbol{c}_B^{\mathrm{T}}A_B^{-1}A_{NB} - \boldsymbol{c}_{NB}^{\mathrm{T}}, w := \boldsymbol{c}_B^{\mathrm{T}}A_B^{-1}\boldsymbol{b}$$

Dann lautet (4.5)

$$\begin{array}{rl} \boldsymbol{x}_B & = \boldsymbol{s} - R\boldsymbol{x}_{NB} \\ \boldsymbol{x} & \geq \boldsymbol{0} \\ w - \boldsymbol{g}^{\mathrm{T}}\boldsymbol{x}_{NB} & \to \max \end{array} \tag{4.6}$$

Diese Darstellung wird Basisdarstellung des LOP's genannt. Sie wird wie folgt durch die Simplextabelle angegeben:

		NB
	w	$\boldsymbol{g}^{\mathbf{T}}$
B	$\boldsymbol{s}$	R

Zur Abkürzung setzt man

$$r_{0,0} := w, r_{0,j} := g_j, j = 1, \ldots, n, r_{i,0} := s_i, i = 1, \ldots, m$$

Bemerkung 4.4.1. *Die Simplextabelle ist durch B (und durch die Reihenfolge der Auflistung der Elemente von B und NB) eindeutig festgelegt.*

Satz 4.4.2. *Sei $B = \{\beta_1, \ldots, \beta_k, \ldots, \beta_m\}$ Basismenge und $NB = \{\gamma_1, \ldots, \gamma_l, \ldots, \gamma_n\}$ die zugehörige Nichtbasismenge. Dann ist die durch den Austausch β_k und γ_l erhaltene Menge $B' = \{\beta_1, \ldots, \gamma_l, \ldots, \beta_m\}$ genau dann Basismenge, wenn in der Simplextabelle für B $r_{kl} \neq 0$ gilt.*

Satz 4.4.3. *Sei $B = \{\beta_1, \ldots, \beta_k, \ldots, \beta_m\}$ Basismenge und $NB = \{\gamma_1, \ldots, \gamma_l, \ldots, \gamma_n\}$ die zugehörige Nichtbasismenge. Es sei $r_{kl} \neq 0$. Ferner seien $B' = \{\beta_1, \ldots, \gamma_l, \ldots, \beta_m\}$ und $NB' = \{\gamma_1, \ldots, \beta_k, \ldots, \gamma_n\}$ die durch den Austausch β_k und γ_l erhaltene Basismenge bzw. Nichtbasismenge. Die weiteren Elemente der Simplextabelle für B' seien mit r'_{ij} bezeichnet, $i = 0, \ldots, m, j = 0, \ldots, n$. Dann gilt:*

$$r'_{ij} = \begin{cases} \frac{1}{r_{ij}}, & \text{falls } i = k, j = l \\ \frac{r_{ij}}{r_{kl}}, & \text{falls } i = k, j \in \{0, \ldots, n\} \setminus \{l\} \\ -\frac{r_{ij}}{r_{kl}}, & \text{falls } i \in \{0, \ldots, m\} \setminus \{k\}, j = l \\ r_{ij} - \frac{r_{il} r_{kj}}{r_{kl}}, & \text{falls } i \in \{0, \ldots, m\} \setminus \{k\}, j \in \{0, \ldots, n\} \setminus \{l\} \end{cases}$$

Bei einem solchen Austausch heißt die Spalte mit der Nummer l Eingangsspalte und die Zeile mit der Nummer k Ausgangszeile. Das Element r_{kl} wird Kreuz- oder Pivotelement genannt.

4.5 Die Simplexmethode

Sei wieder das LOP in Normalform (4.3) mit einer $m \times (n + m)$ Matrix A, $rg(A) = m$, gegeben. Sei (4.6) eine Basisdarstellung. Offenbar ist der folgende Vektor $\boldsymbol{x}^B$ eine Lösung des LGS $A\boldsymbol{x} = \boldsymbol{b}$:

$$\boldsymbol{x}^B_{NB} = \mathbf{0}, \boldsymbol{x}^B_B = \boldsymbol{s}$$

Man nennt $\boldsymbol{x}^B$ Basislösung. Falls zusätzlich $\boldsymbol{s} \geq \mathbf{0}$ gilt, heißt $\boldsymbol{x}^B$ zulässige Basislösung. Für den Wert der Zielfunktion $f(\boldsymbol{x}) = \boldsymbol{c}^{\mathrm{T}}\boldsymbol{x}$ auf der Basislösung $\boldsymbol{x}^B$ gilt:

$$f(\boldsymbol{x}^B) = w.$$

Satz 4.5.1. *Sei $\boldsymbol{x}^B$ zulässige Basislösung und sei $x^{B'}$ eine durch den Austausch $\beta_k \leftrightarrow \gamma_l$ gemäß Satz 4.4.3 erhaltene neue Basislösung. Es ist $x^{B'}$ genau dann zulässig, wenn gilt:*

$$r_{kl} > 0 \text{ und } \frac{s_k}{r_{kl}} = \min\{\frac{s_i}{r_{il}} : i \in [m], r_{il} > 0\}$$

oder

$$r_{kl} \neq 0 \text{ und } s_k = 0.$$

Satz 4.5.2. *Sei $\boldsymbol{x}^B$ eine zulässige Basislösung. Gilt in der zugehörigen Simplextabelle*

$$g_j \geq 0 \ \forall j \in [n],$$

so ist $\boldsymbol{x}^B$ eine optimale Lösung des LOP's (4.3) und w ist der optimale Wert der Zielfunktion.

Satz 4.5.3. *Sei $\boldsymbol{x}^B$ eine zulässige Basislösung. Falls es einen Index $\gamma_l \in NB$ gibt, sodass in der zugehörigen Simplextabelle*

$$g_l < 0 \text{ und } r_{il} \leq 0 \ \forall i \in [m]$$

gilt, so ist die Zielfunktion auf dem zulässigen Bereich unbeschränkt.

Simplexmethode:
Initialisierung:
Berechne eine zulässige Basislösung und die zugehörige Simplextabelle
Iteration:
1. Finde ein l mit $g_l < 0$. Gibt es ein solches l nicht, so ist die optimale Lösung aus der aktuellen Simplextabelle ablesbar, STOP.
2. Finde ein k mit $r_{kl} > 0$ und $\frac{s_k}{r_{kl}} = \min\{\frac{s_i}{r_{il}} : i \in [m], r_{il} > 0\}$. Gibt es ein solches k nicht, so ist die Zielfunktion unbeschränkt, STOP.
3. Führe den Austausch $\beta_k \leftrightarrow \gamma_l$ gemäß Satz 4.4.3 durch.

Eine zulässige Basislösung heißt entartet, falls für die zugehörige Simplextabelle gilt: Es gibt ein $i \in [m]$ mit $s_i = 0$.
Ein LOP in der Normalform (4.3) heißt entartet, wenn es eine entartete zulässige Basislösung hat.

Satz 4.5.4. *Ist das LOP (4.3) nicht entartet, so bricht die Simplexmethode nach endlich vielen Schritten ab.*

Dieser Satz bleibt auch im entarteten Fall richtig, wenn die Wahl von l und k nach der Regel von Bland eindeutig festgelegt wird:

Regel von Bland:
1. Wähle l so, dass $g_l < 0$ gilt und unter dieser Bedingung γ_l minimal ist.
2. Wähle k so, dass $r_{kl} > 0$ und $\frac{s_k}{r_{kl}} = \min\{\frac{s_i}{r_{il}} : i \in [m], r_{il} > 0\}$ gilt und unter dieser Bedingung β_k minimal ist.

Satz 4.5.5. *Wird im Simplexalgorithmus das Pivotelement nach der Regel von Bland ausgewählt, so kann sich keine Basismenge wiederholen und der Algorithmus bricht daher nach endlich vielen Schritten ab.*

4.6 Bestimmung einer ersten zulässigen Basislösung

Suchen erste zulässige Basislösung für das LOP

$$\begin{aligned} A\boldsymbol{x} &= \boldsymbol{b} \\ \boldsymbol{x} &\geq \boldsymbol{0} \\ \boldsymbol{c}^{\mathrm{T}}\boldsymbol{x} &\to \max \end{aligned} \tag{4.7}$$

mit einer $m \times n$-Matrix A, für die nicht notwendigerweise $rg(A) = m$ ist. O.B.d.A. sei $\boldsymbol{b} \geq \boldsymbol{0}$ (sonst entsprechende Gleichungen mit -1 multiplizieren). Führen künstliche Variable $y_i = x_{n+i}$, $i = 1, \ldots, m$, ein und betrachten das Hilfsproblem (mit $\mathbf{1} = (1, \ldots, 1)^{\mathrm{T}}$)

$$\begin{aligned} A\boldsymbol{x} + \boldsymbol{y} &= \boldsymbol{b} \\ \boldsymbol{x} &\geq \boldsymbol{0} \\ \boldsymbol{y} &\geq \boldsymbol{0} \\ -\mathbf{1}^{\mathrm{T}}\boldsymbol{y} &\to \max \end{aligned} \tag{4.8}$$

Eine erste zulässig Basislösung für (4.8) ist mit $B = \{n+1, \ldots, n+m\}$ gegeben:

$$\begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix}^B = \begin{pmatrix} \boldsymbol{0} \\ \boldsymbol{b} \end{pmatrix}$$

Die zugehörige Simplextabelle lautet wegen $-\mathbf{1}^{\mathrm{T}}\boldsymbol{y} = -\mathbf{1}^{\mathrm{T}}(\boldsymbol{b} - A\boldsymbol{x}) = -\mathbf{1}^{\mathrm{T}}\boldsymbol{b} - (-\mathbf{1}^{\mathrm{T}}A)\boldsymbol{x}$:

		1	$\ldots$	n
	$-\mathbf{1}^{\mathrm{T}}\boldsymbol{b}$	$-\mathbf{1}^{\mathrm{T}}\boldsymbol{A}_1$	$\ldots$	$-\mathbf{1}^{\mathrm{T}}\boldsymbol{A}_n$
$n+1$	b_1			
$\vdots$	$\vdots$		A	
$n+m$	b_m			

Da die Zielfunktion nach oben durch 0 beschränkt ist, führt die Zielfunktion zu einer optimalen Lösung des Hilfsproblems (4.8)

$$\begin{pmatrix} \boldsymbol{x}_h \\ \boldsymbol{y}_h \end{pmatrix}$$

mit der Simplextabelle

		γ_1	$\dots$	γ_n
	w	g_1	$\dots$	g_n
β_1	s_1			
$\vdots$	$\vdots$		R	
β_m	s_m			

(4.9)

Satz 4.6.1. *Das LOP (4.7) besitzt genau dann eine zulässige Lösung, wenn* $\boldsymbol{y}_h = \mathbf{0}$ *ist.*

Sei $\boldsymbol{y}_h = \mathbf{0}$. Um eine erste zulässige Basislösung für das LOP (4.7) zu bekommen, werden soviel wie möglich künstliche Variablen zu Nichtbasisvariablen gemacht:

Solange in der jeweils aktuellen Simplextabelle ein $\beta_k \in \{n+1, \dots, n+m\}$ und ein $\gamma_l \in [n]$ existiert, sodass $r_{kl} \neq 0$ ist, tausche β_k und γ_l gemäß Satz 4.4.3 aus. Die zum Schluss erhaltene Tabelle sei wieder in der Form (4.9) gegeben.

Die erste Simplextabelle (und damit die erste zulässige Basislösung) für das LOP (4.7) bekommt man nun wie folgt:
1. Streiche alle Spalten, die zu künstlichen Variablen gehören ($\gamma_j \in \{n+1, \dots, n+m\}$).
2. Streiche alle Zeilen, die zu künstlichen Variablen gehören ($\beta_i \in \{n+1, \dots, n+m\}$).
Die jetzt erhaltene Tabelle habe wieder die Form (4.9)
3. Aktualisiere die Zielfunktion: Sei $B = \{\beta_1, \dots, \beta_m\}$. Setze

$$\begin{aligned} w &:= \boldsymbol{c}_B^{\mathrm{T}} \boldsymbol{s} \\ g_j &:= \boldsymbol{c}_B^{\mathrm{T}} \boldsymbol{R}_j - c_{\gamma_j}, \ j = 1, \dots, n \end{aligned}$$

Bemerkung 4.6.1. *Am Anfang braucht man nur für solche Gleichungen künstliche Variable einzuführen, die nicht einen Kandidaten für eine Basisvariable besitzen. Man kann die Rechnung abkürzen, indem man nach jedem Schritt, bei dem eine künstlichen Basisvariable Nichtbasisvariable geworden ist, sofort die entsprechende Spalte streicht.*

Folgerung 4.6.1. *Für jedes lineare Optimierungsproblem tritt genau einer der folgenden Fälle ein:*

1. *Der zulässige Bereich ist leer.*
2. *Es gibt eine optimale Lösung.*
3. *Die Zielfunktion ist auf dem (nichtleeren) zulässigen Bereich unbeschränkt.*

Inhaltsverzeichnis

1 Kombinatorik **3**

1.1 Grundformeln 3

1.2 Lineare Rekursionsgleichungen 4

1.3 Das Prinzip von Inklusion und Exklusion 6

2 Strukturen der Algebra **9**

2.1 Faktormengen 9

2.2 Elemente der Zahlentheorie 11

2.3 Halbgruppen und Gruppen 12

2.4 Ringe und Körper 16

3 Anwendungen der Algebra **19**

3.1 Kryptographie und der RSA-Algorithmus 19

3.2 Elemente der Codierungstheorie 20

4 Lineare Optimierung **23**

4.1 Problemstellung 23

4.2 Graphische Lösung im Fall $n = 2$ 23

4.3 Transformation auf Normalform 24

4.4 Basisdarstellungen 26

4.5 Die Simplexmethode 27

4.6 Bestimmung einer ersten zulässigen Basislösung 29