

Extremstellen ohne Nebenbedingungen

Skalare Extremstellenfindung:

→ Max-Stelle: $f'(x) = 0$ und $f''(x) \leq 0$

→ Min-Stelle: $f'(x) = 0$ und $f''(x) \geq 0$

Global: Zeige, dass kein größerer Punkt

Definition Definitheit:

→ symmetrisch positiv definit: $\langle A\vec{v}, \vec{v} \rangle > 0$

→ symmetrisch negativ definit: $\langle A\vec{v}, \vec{v} \rangle < 0$

→ symmetrisch positiv semidefinit: $\langle A\vec{v}, \vec{v} \rangle \geq 0$

→ symmetrisch negativ semidefinit: $\langle A\vec{v}, \vec{v} \rangle \leq 0$

→ ansonsten Indefinit

Beispiel:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow v^T A v \rightarrow (v_1, v_2) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

→ $(v_1)^2 + (v_2)^2 \rightarrow$ positiv definit

Erinnerung Hessematrix:

$$H_f(x, y) = \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{pmatrix}$$

Erinnerung Gradient:

→ Vektor der partiellen Ableitung nach jeder Variable

Extremstellen mit Hessematrix:

→ Max-Stelle: $\nabla f(\vec{x}) = \vec{0}$ und $Hf(\vec{x})$ ist neg. semidefinit

→ Min-Stelle: $\nabla f(\vec{x}) = \vec{0}$ und $Hf(\vec{x})$ ist pos. semidefinit

Eigenwerte berechnen:

→ Diagonaleinträge minus λ

→ 2-Dimensional: $a_{11}a_{22} - a_{12}a_{21}$

→ 3-Dimensional: $a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$

→ Charakteristisches Polynom lösen

Eigenwertkriterium für Definitheit:

→ positiv definit: $\lambda_1, \dots, \lambda_n > 0$

→ negativ definit: $\lambda_1, \dots, \lambda_n < 0$

→ positiv semidefinit: $\lambda_1, \dots, \lambda_n \geq 0$

→ negativ semidefinit: $\lambda_1, \dots, \lambda_n \leq 0$

→ indefinit, wenn zwei λ unterschiedliche Vorzeichen

Extremstellen mit Nebenbedingungen

Lagrange Formalismus (1. Nebenbedingung):

→ Nebenbedingung umstellen, sodass gleich 0

→ Lagrange Bedingung aufstellen: $f(x) - \lambda g(x) = C$

→ Lagrange Bedingung pro Variable partiell ableiten

→ Gleichungssystem aus Ableitungen lösen

→ Tipp: Matrizenform und Gauß anwenden

Beispiel:

→ $f(x, y) = 5xy - y^2$ und NB: $x + y = 12 \rightarrow x + y - 12 = 0$

→ $L(x, y, \lambda) = 5xy - y^2 - \lambda(x + y - 12)$

→ $L'(x, y, \lambda) = 5y + \lambda = 0$

→ $L'(x, y, \lambda) = 5x - 2y + \lambda = 0$

→ $L'(x, y, \lambda) = x + y - 12 = 0$

Lagrange Formalismus (mehrere Nebenbedingungen):

→ Alle NB umstellen, sodass gleich 0

→ Lagrange Bedingung: $L = f(x) - \lambda_1 g(x) - \dots - \lambda_n g(x)$

→ Lagrange Bedingung pro Variable partiell ableiten

→ Gleichungssystem aus Ableitungen lösen

Implizite Funktionen

→ explizite Funktionen: $f(x) = y$

→ implizite Funktionen: $x^2 + y^2 = 1$

→ Umrechnung von explizit zu implizit nicht trivial

Satz über implizite Funktionen:

Sei $f : D \rightarrow \mathbb{R}, D \subseteq \mathbb{R}^2$ offen, $(x', y') \in D$ und $f(x', y') = 0$

Zudem gilt: $\partial_2 f(x', y') \neq 0$

⇒ Existenz der Auflösungsfunktion: $f(x, y(x) = 0) \wedge y' = y'(x')$

Die Auflösungsfunktion ist stetig differenzierbar und es gilt:

$$y'(x) = -\frac{\partial_1 f(x, y(x))}{\partial_2 f(x, y(x))}$$

Satz über implizite Fkt (mehrdimensional):

→ $f : D \subseteq \mathbb{R}^{m+n} \rightarrow \mathbb{R}^m$ mit $n, m \in \mathbb{N}$ und $(x', y') \in D$ und $x' \in \mathbb{R}^n \wedge y' \in \mathbb{R}^m$

→ $\vec{f}(x', y') = \vec{0}$

→ Die $m \times m$ -Matrix $\partial \vec{f} / \partial \vec{y}(x', y')$ muss invertierbar sein

→ $\vec{f}(x', y'(x')) = \vec{0}$ und $\vec{y}(x') = \vec{y}'$

⇒ Es existiert eine Auflösungsfunktion

Jacobi Matrix:

→ Alle Partiellen Ableitungen einer Funktion nebeneinander

Satz der inversen Abbildung:

Vorraussetzung: $\vec{f} : D \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^n$ sei offen, $\vec{x}' \in D$,

$f \in C^1(D)$, Jacobimatrix $J\vec{f}(\vec{x}') = df/d\vec{x}(\vec{x}')$ ist invertierbar

⇒ Umkehrfunktion existiert

Bemerkung:

→ Die Existenz einer Umkehrfunktion in jedem Punkt impliziert nicht die Existenz einer globalen Umkehrfunktion

Kurvenberechnung

Parameterdarstellung:

→ Darstellung durch einen Vektor mit Parametern

→ Zum ableiten jede Zeile einzeln ableiten

Beispiel:

$$\vec{r}(t) = \begin{pmatrix} \cos(t) \\ \sin(t) \end{pmatrix} \rightarrow \vec{r}'(t) = \begin{pmatrix} -\sin(t) \\ \cos(t) \end{pmatrix}$$

Erinnerung:

→ " $\|y(t)\|$ ": Betrag der euklidischen Norm

→ " $\langle \vec{x}, \vec{y} \rangle$ ": Skalarprodukt: $x_1 y_1 + \dots + x_n y_n$

→ " $\vec{x} \times \vec{y}$ ": Kreuzprodukt: $(23 - 32, 31 - 13, 12 - 21)^T$

→ Kreuzprodukt 2 dimensional: skalarer Wert (Determinante)

Bogenlänge Kurve: $\int_a^b \|\vec{y}'(t)\| dt$

1. Kurvenintegral: $\int_a^b f(\vec{y}(t)) \|\vec{y}'(t)\| dt$

2. Kurvenintegral: $\int_a^b \langle \vec{F}(\vec{y}(t)), \vec{y}'(t) \rangle dt$

1. Oberflächenint.: $\int_a^b f(\vec{y}(s, t)) \|\partial_1 \vec{y}(s, t) \times \partial_2 \vec{y}(s, t)\| ds dt$

2. Oberflächenint.: $\int_a^b \langle \vec{f}(\vec{y}(s, t)), \partial_1 \vec{y}(s, t) \times \partial_2 \vec{y}(s, t) \rangle ds dt$

Tangente Berechnen: $T(s) = y'(t) \cdot s + y(t)$ mit $s \in \mathbb{R}$

Bemerkung:

→ 1. Art wird bei skalaren Funktionen verwendet

→ 2. Art wird bei vektorialen Funktionen verwendet

Definitionen:

→ Para-Darstellung glatt/regulär: keine erste Ableitung ist 0

→ Bogenlängenparametrisiert: Kurvenintegral ist 1

Optimierung

konvexe Mengen:

- Verbindungsstrecke zweier Punkte immer in der Menge
- $\forall \vec{x}, \vec{y} \in M \forall a \in (0, 1) : a\vec{x} + (1-a)\vec{y} \in M$

konvexe Funktion:

- Funktionswerte unterhalb der Verbindungsstrecke
- Bei konkav oberhalb der Verbindungsstrecke
- $\forall \vec{x}, \vec{y} \in D \forall a \in (0, 1) : f(a\vec{x} + (1-a)\vec{y}) \leq af(\vec{x}) + (1-a)f(\vec{y})$
- strikt konvex wenn $<$

Ableitungskriterium für Konvexität:

- f konvex $\leftrightarrow Hf(\vec{x})$ positiv semidefinit
- f strikt konvex $\leftarrow Hf(\vec{x})$ positiv definit

Eigenschaften:

- Jede lokale Minstelle ist auch globale Minstelle
- alle lokalen Minstellen bilden eine zusammenhängende, konvexe Minstelle
- alle lokalen Minima haben den gleichen Wert
- Die Menge aller lokalen Minima kann leer sein
- Wenn f strikt konvex ist, gibt es max. eine Minstelle
- Eine nichtleere kompakte Levelmenge hat mind. eine globale Minstelle

Quadratische Optimierung:

- ! Nur mit quadratischen Matrizen! Problemstellung:
- $\min 1/2 \cdot \langle A\vec{x}, \vec{x} \rangle + \langle \vec{b}, \vec{x} \rangle (+c)$ → mit $A \in \mathbb{R}^{n \times n}, \vec{b} \in \mathbb{R}^n$
- $\partial f(\vec{x}) = A\vec{x} + \vec{b}$ und $Hf(\vec{x}) = A$
- ⇒ $\vec{x}' = -A^{-1} \cdot \vec{b} \Rightarrow A\vec{x}' = -\vec{b} \Rightarrow$ Gaußverfahren

Linear-Quadratisches Minimierungsproblem:

- Funktion: $f(\vec{x}) = 1/2 \langle A\vec{x}, \vec{x} \rangle + \langle \vec{b}, \vec{x} \rangle$
- Nebenbedingung: $B\vec{x} = \vec{c}$ mit $B \in \mathbb{R}^{m \times n}, \vec{c} \in \mathbb{R}^m$

Fall 1: Vektor Nebenbedingung:

- $B_i \cdot c = c_i$ mit $i = 1, \dots, m \Rightarrow$ m Nebenbedingungen.
- ⇒ Lagrange Multiplikator und Lagrangestyle lösen

Fall 2: Skalare Nebenbedingung:

- Ausgangsformel in skalare Form bringen durch ausmultiplizieren,
- Nebenbedingung unverändert lassen \Rightarrow Lagrange Lösen

Simplex Algorithmus

- Simplex ist ein von Geraden aufgestellter Körper
- Idee: Laufe Geraden entlang bis Ergebnis
- 1. Mathematische Formulierung mit Variablen (HaVa)
 - Nebenbedingung z(Variablen) = ... \rightarrow max
 - Variablen ≥ 0
- 2. Pro Gleichung eine Variable (HiVa) einführen
 - NB Vorzeichenwechsel und \rightarrow Min (wenn positiv)
 - Alle Variable ≥ 0
- 3. Tabelle aufstelle:

	HaVa	HiVa	Wert	Quotient
HiVa 1	HaVa 1ter Wert	HiVa = HiVa:1	Wert	Quotient
Hiva n	HaVa nter Wert	Hiva \neq HiVa:0	Wert	Quotient
NB	NB HaVa Wert	0	0	0

- 4. IF links bei NB keine negativen Werte: Fertig
- 5. IF links bei NB nur negative Werte: LP unbeschränkt
- 6. ELSE Basiswechsel:
 - Wähle Spalte mit kleinstem Quotienten/Nebenbedingung
 - Gaußmäßig Zeile auf andere Zeilen addieren, sodass:
 - 1 in der ausgewählten Zeile, sonst 0

Bemerkung: → Basis sind 0er und 1er Zeilen

→ Nicht Basis alle anderen Zeilen

→ Quotient = Wert / (Spalte kleinster NB)

Fixpunktiterationen

Fixpunkt:

- Abbildung f: A \rightarrow B mit $A \subseteq B$
- Fixpunkt: $f(x) = x$ Bsp: Nullpunkt einer Ursprungsgeraden
- Fixpunktiteration mit rekursiven Funktionen $g(x)$ möglich
- Falls $g(x)$ konvergiert und stetig: Grenzwert: Fixpunkt

Banach Raum und Vollständigkeit:

- Vollständig: Normierter Vektorraum, indem jede Cauchy-Folge konvergiert
- vollständiger normierter Vektorraum \Leftrightarrow Banach-Raum
- Hilbert-Raum: Banach-Raum + $\forall x \in V : \|x\| = \sqrt{\langle x, x \rangle}$
- \mathbb{R}^n mit jeder beliebigen Norm ist ein Banach-Raum

Kontraktion:

- Sei V ein Vektorraum: $M \subseteq V$ und $\phi : M \rightarrow V$
- ϕ heißt Kontraktion, falls es ein $k < 1$ gibt, sodass:

$$\|\phi(x) - \phi(y)\| \leq k\|x - y\| \forall x, y \in M$$
- grob: Bilder liegen näher beieinander als Urbilder
- Das k heißt dann Kontraktionskonstante von ϕ

Fixpunktsatz von Banach:

- Banach-Raum $V \wedge 0 \neq M \subseteq V =$ abgeschlossene Teilmenge
- Sei $\phi : M \rightarrow V$ mit $\phi(M) \subseteq M$ eine Kontraktion
- ⇒ ϕ genau ein Fixpunkt und Grenzwert: $x_{n+1} := \phi(x_n)$
- Fehlerabschätzung: k = Kontraktionskonstante von ϕ
 - Aproximationsfehler fällt pro Iterationsschritt um min. k
 - $\|x_{n+1} - x'\| \leq k\|x_n - x'\|$ somit $\|x_n - x'\| \leq k^n \|x_0 - x'\|$

Newton-Verfahren:

- $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$
- Stellt Fixpunktiteration zu folgender Funktion dar:

$$\phi(x) := x - \frac{f(x)}{f'(x)}$$
- Die Asymptotische Kontraktionskonstante von $\phi(x)$ ist 0

Definitionen:

- linear konvergent: $k < 1 : \|x_n - x'\| \leq k\|x_{n-1} - x'\|$
- quadratisch konvergent: $c > 0 : \|x_n - x'\| \leq c\|x_{n-1} - x'\|^2$

Newton-Verfahren im mehrdimensionalen:

- Sei $\vec{f} : \mathbb{R}^m \rightarrow \mathbb{R}^m$ zweimal stetig differenzierbar
- Sei die Jacobi-Matrix $Jf(\vec{x})$ invertierbar für alle \vec{x}
- $\vec{x}_{n+1} := \vec{x}_n - [(Jf)(\vec{x}_n)]^{-1} \vec{f}(\vec{x}_n)$

Differentialgleichungen

Eigenschaften von Differentialgleichungen:

- linear: Ausgangsfunktion ohne Potenzen / e-Funktion
- nte Ordnung: höchste Ableitung
- skalar: ohne Vektoren
- gewöhnlich: nur Ableitungen nach einer Variable
- autonom: Variable tritt nicht allein auf
- explizit: Umgestellt nach höchster Ableitung
- homogen: ohne Störfunktion
- System von DGL: Matrixschreibweise

Anfangswertproblem (AWP):

- Für DGL ohne Anfangswert nur allgemeine Lösung
- Mit Anfangswert lässt sich die Konstante berechnen
- Für explizite gewöhnliche DGL 1. Ordnung
- Gegeben: $y'(x) = f(x) \cdot g(y)$ mit $y(a) = b$

$$y_0 = c \cdot e^{kt_0} \Rightarrow c = y_0 e^{-kt_0} \Rightarrow y(t) = y_0 e^{-kt_0} e^{kt} = y_0 e^{k(t-t_0)}$$

- AWP n-ter Ordnung umwandelbar in AWP erster Ordnung:
- Es werden n Anfangswerte benötigt
- Gegeben: $y^n(t) = f(t, y(t), \dots, y^{n-1}(t))$
- 1. n Hilfsvariablen einführen: z_1, \dots, z_n
- 2. Hilfsvariablen zuweisen: $z_1(t) = y(t), \dots, z_n(t) = y^{n-1}(t)$
- 3. System von DGL erster Ordnung aufstellen:
- $z'_1(t) = z_2(t), z'_2(t) = z_3(t), \dots, z'_n(t) = f(t, z_1(t), \dots, z_{n-1}(t))$
- 4. System in Matrixschreibweise umwandeln
- Beispiel: $y'' = 3y' - 2y \Rightarrow z_1 = y, z_2 = y'$
- $z'_1 = z_2, z'_2 = -2z_1 + 3z_2$
- $y_{neu} = (0 \ 1, -2 \ 3)^T \cdot (z_1, z_2)^T$

Lösung für skalare DGLs erster Ordnung:

- Gegeben: $f(t, y) = g(y)h(t) \Rightarrow$ Trennung der Variablen
- Funktioniert nicht für Systeme n-ter Ordnung
- 1. Separation: $y'(t)/g(y) = h(t)$

$$\int_b^x \frac{1}{g(y)} dy = \int_a^x f(x) dx + c \Rightarrow G(y) = H(t) + c$$

- Gleichung nach $y(t)$ umstellen

Lösen mittels Substitution:

- Wenn keine bekannten Lösungsverfahren funktionieren
- Substitution, damit andere Lösungsverfahren möglich sind
- 1. Geeignete Substitution finden, z.B.:
- $y'(t) = f(y(t)/t) \Rightarrow$ Substitution: $z(t) = y(t)/t$
- $y'(t) = f(at + by(t) + c) \Rightarrow$ Substitution: $z(t) = at + by(t) + c$
- Substitution nach $y(t)$ umformen und nach t ableiten
- Substitution und Ableitung ins ursprüngliche DGL einsetzen
- Weitere Lösungsverfahren anwenden
- Beispiel: $y'(t) = (y(t)/t) \cdot (\log(y(t)/t) + 1)$
- $z(t) = y(t)/t \Rightarrow y(t) = tz(t), y'(t) = tz'(t) + z(t)$
- $tz'(t) + z(t) = z(t) \log(z(t)) + z(t) \Leftrightarrow tz'(t) = z(t) \log(z(t))$
- Jetzt noch Trennung der Variablen anwenden

Variation der Konstanten:

- 1. DGL in Ausgangslage bringen: $x'(t) = a(t)x(t) + b(t)$
- 2. homogene Lösung: $x_n(t) = c \cdot e^{-A(x)}$ mit $c \in \mathbb{R}$
- Lösen des inhomogenen Anteils:
- 3. C als Funktion: $x_n(t) = c(t) \cdot e^{-A(x)}$
- 4. Einsetzen $x_n(t)$ in $x(t)$ und nach $c(t)$ bzw. $c'(t)$ auflösen
- 5. Integrieren von $c(t)$ bzw. $c'(t)$
- 6. Einsetzen von $c(t)$ in $x_n(t)$
- 7. Anfangswert für Hilfsvariable aus 5. einsetzen
- 8. Formel aus 7. in DLG einsetzen

Existenztheorie:

- DGLs n-ter Ordnung umwandelbar in DGLs erster Ordnung
- Rechte Seite stetig \Rightarrow es existiert eine Lösung des AWP

Lineare DGL-Systeme erster Ordnung:

- Diesmal mit quadratischer Matrix $A(t)$
- Gegeben: $y'(t) = A(t)y(t) + b(t)$
- homogen, wenn $b(t) = 0$, ansonsten inhomogen
- Lösungsmenge: $L_{inhom} = \{y_p\} + L_{hom}$ mit: $y_p =$ feste Größe
- Dimension der Lösung ist Dimension der Matrix
- Fundamentalsystem: Basis von L_{hom}
- Fundamentallösung: Mitglieder des Fundamentalsystems
- Fundamentalmatrix: $w(t) := [\vec{y}_1(t), \dots, \vec{y}_n(t)] \in \mathbb{R}^{n \times n}$
- Wronski Determinante: $\det(w(t))$

Berechnung Fundamentalsystems (A unabhängig von t):

- Gegeben: $\vec{y}'(t) = A\vec{y}(t)$
- Fall 1: A ist eine Diagonalmatrix:

$$y'(t) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_n \end{pmatrix} y(t) \Rightarrow y_1(t) = c_1 e^{\lambda_1 t}, \dots, y_n(t) = c_n e^{\lambda_n t}$$

- $L_{hom} = \{\vec{y}(t) = c_1 e^{\lambda_1 t}, \dots, c_n e^{\lambda_n t}\}, c_i \in \mathbb{R}^n$
- Fundamentalsystem: $e^{\lambda_1 t} \vec{e}_1, \dots, e^{\lambda_n t} \vec{e}_n$
- Fall 2: A ist diagonalisierbare Matrix:
- 1. Berechne die EW λ_i von A
- 2. Berechne die EV V_i von A
- Fundamentalsystem: $e^{\lambda_1 t} v_1, \dots, e^{\lambda_n t} v_n$
- Sonderfall: komplexe Eigenwerte:
- Umwandeln in reelles Fundamentalsystem:
- komplexe Eigenwerte treten doppelt auf
- Zerlegen von λ_i und V_i in Real und Imaginärteil
- $\lambda = a + bi$ und $V = r + si$
- $y_1(t) = (r \cdot \cos(bt) - s \cdot \sin(bt))e^{at} + i(s \cdot \cos(bt) + r \cdot \sin(bt))e^{at}$
- $y_2(t) = (r \cdot \cos(bt) - s \cdot \sin(bt))e^{at} - i(s \cdot \cos(bt) + r \cdot \sin(bt))e^{at}$
- $y_{1, reell} = RE(y_1)$ und $y_{2, reell} = IM(y_1)$
- Einträge des reellen Fundamentalsystems
- Fall 3: A ist nicht diagonalisierbar:
- Es existiert mind. ein EW wo $alg \neq geo$
- Sei λ der EW \Rightarrow Berechnung Hauptvektoren (HV)
- 1. Einen EV V_n zu λ berechnen
- 2. Berechnung Hauptvektor: $(A - \lambda \cdot \text{Einheitsmatrix})V_2 = V_1$
- Man benötigt soviele Hauptvektoren wie alg von λ
- Fundamentalsystem für EW mit $alg \neq geo$ und V_m HV:

$$e^{\lambda t} (V_m + tV_{m-1} + (t^2/2!)V_{m-2} + \dots + (t^{m-1}/(m-1)!)V_1)$$

- Berechnung partikulärer Lösung für inhomogene DGL:
- Sei $\vec{y}_1, \dots, \vec{y}_n$ ein Fundamentalsystem:
- Partikuläre Lösung: $\vec{y}_p = W(t)\vec{c}(t)$
- \vec{y}_i Lösungen $\Rightarrow c'(t) = W(t)^{-1}b(t)$
- Integrations der einzelnen Komponenten ohne Konstante
- Einsetzen: $L_{inhom} = \vec{y}_p + L_{hom}$

Lineare skalare DGLn n-ter Ordnung:

- Gegeben: $y^{(n)} + a_{n-1}(t)y^{(n-1)}(t) + \dots + a_0(t)y(t) = b(t)$
- Umwandelbar in System von DGL erster Ordnung
- Nur für Konstante a_i lösbar
- Ist a_i abhängig von t \Rightarrow kein Fundamentalsystem
- Trick zum Bilden des charakteristischen Polynoms:
- $p(\lambda) = (-1)^n(\lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0)$
- Lösungsraum homogener DGL:
- a_i ist eine Konstante, $b = 0$
- Für jede Nullstelle $\lambda_i \in \mathbb{C}$ nehme die Funktion:
- $e^{\lambda_i t}, te^{\lambda_i t}, \dots, t^{r_j-1}e^{\lambda_i t}$
- r_j ist die Vielfachheit der NS λ_i
- Für die partikuläre Lösung: $\vec{y}_p = w(t)\vec{c}(t)$

Numerische Verfahren:

- Wenn man das Anfangswertproblem nicht exakt lösen kann
- genannt: Eulersches Polygonzugverfahren
- $y_{n+1} = y_n + hf(t_n, y_n)$ mit $h > 0 \in \mathbb{R}$
- $y_{n+1} = y_n + hf(t_n + h/2, y_n + h/2 \cdot f(t_n, y_n))$

Algebra

Definition Gruppe:

- Menge M mit einer Verknüpfung
- Halbgruppe: $a * (b * c) = (a * b) * c$ (Assoziativgesetz)
- Monoid: $a * e = e * a = a$ (neutrales Element)
- Gruppe: $a * b = b * a = e$ (inverses Element)
- Abel'sche Gruppe: $a * b = b * a$ (Kommutativgesetz)

Definition Ring:

- Menge M mit zwei Verknüpfungen: $+, *$
- $(M, +)$ ist eine Abelsche Gruppe
- $(M, *)$ ist assoziativ
- Distributivgesetz gilt: $(a + b) * c = a * c + b * c$
- Ring mit Einselement: enthält neutrales Element
- kommutativer Ring: $(M, *)$ ist kommutativ

Definition Körper:

- kommutativer Ring $(M, +, *)$ mit Einselement
- Jedes Element außer 0 hat Inverses bzgl. Multiplikation
- Oder: Ring $(M, +, *)$ mit $(M \setminus \{0\}, *)$ als Abelsche Gruppe

Definition Restklasse:

- Menge der Zahlen, die bei $a \bmod b$ denselben Rest haben
- Bsp: $[2]_3 = \{\dots - 4, -1, 2, 5, \dots\} = \{z \in \mathbb{Z} | z \equiv 2 \pmod{3}\}$
- Verknüpfungen: $[a]_n + [b]_n = [a + b]_n$ und $[a]_n \cdot [b]_n = [a \cdot b]_n$
- Mit Restklassen kann man Ringe und Körper bauen

Satz:

- Im Restklassenring $(\mathbb{Z}_n, +, *)$ gilt für jedes $[a]_n \in \mathbb{Z}_n$:
- $[a]_n$ invertierbar bzgl. Multiplikation ist äquivalent zu:
- ⇔ $\forall [b]_n \in \mathbb{Z}_n \setminus \{0\} : [a]_n * [b]_n \neq [0]_n$

Satz 1 (euklidischer Divisionsalgorithmus):

- $\forall a, b \in \mathbb{N} : \alpha, \beta \in \mathbb{Z} : ggT(a, b) = \alpha a + \beta b$

Satz 2 (teilerfremdheit):

- $a, b \in \mathbb{N}$ sind genau dann teilerfremd, wenn mit $\alpha, \beta \in \mathbb{Z}$ gilt:
- ⇒ $\alpha a + \beta b = 1$

Satz 3 (Folgerung aus Satz 2):

- $[a]_n \in \mathbb{Z}_n$ hat Inverses bzgl. $*$, wenn a und n teilerfremd

Satz:

- $\forall n \geq 2 : (\mathbb{Z}_n \setminus \{0\}, *)$ ist Gruppe ⇔ n ist prim

Satz (endliche Körper):

- $\forall p \geq 2 : (\mathbb{Z}_p, +, *)$ ist Körper ⇔ p ist prim

Beispielrechnung mit Restklassen:

- Mit welcher Ziffer endet $z = 9^{123}$
- $[9^{123}]_{10} = [9]_{10}^{123} = [-1]_{10}^{123} = [(-1)^{123}]_{10} = [-1]_{10} = [9]_{10}$

Fehlererkennung:

- Einzelfehler:
- ⇒ $\forall i = 1, \dots, m : [g_i]_n$ ist invertierbar
- ⇒ Also: $ggT(g_i, n) = 1 \forall i = 1, \dots, m$
- Vertauschfehler:
- ⇒ $\forall i, j = 1, \dots, m + 1$ mit $i \neq j : [g_i - g_j]$ ist invertierbar
- ⇒ Also: $ggT(|g_i - g_j|, n) = 1 \forall i \neq j$
- Nachbartauschungsfehler:
- ⇒ $\forall i = 1, \dots, m : [g_i - g_{i+1}]_n$ ist invertierbar
- ⇒ Also: $ggT(|g_i - g_{i+1}|, n) = 1 \forall i = 1, \dots, m$

Tipps:

- Berechnung der Inversen einer Gruppe (\mathbb{Z}_n^*) :
- ⇒ Große n : euklidischer Divisionsalgorithmus
- ⇒ Kleine n : Bilde Potenz von $[a]_n$ bis $[a]_n^k = [1]_n$
- Es ist dann $[a]_n^{k-1} \cdot [a]_n = [1]_n \Rightarrow [a]_n^{-1} = [a]_n^{k-1}$

Definition (Nullteilerfreiheit):

- Definiert für einen Ring $(R, +, *)$
- $\forall a, b \in R : (a * b = 0 \rightarrow a = 0 \vee b = 0)$
- Elemente $a, b \in R$ mit $a * b = 0$ nennt man Nullteiler
- Körper sind immer nullfrei

Satz (Primzahlen):

- Jede Zahl ist eine Multiplikation von Primzahlen
- Es gibt unendlich viele Primzahlen

Definition (Euler'sche Phi-Funktion):

- $\phi : \mathbb{N} \rightarrow \mathbb{N} \Rightarrow \phi(n) := |\mathbb{Z}_n^*| = \{k \in \{1, \dots, n\} | ggT(k, n) = 1\}$
- Für Primzahlen gilt $\phi(p) = p - 1$
- Für Primzahlpotenzen gilt $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$
- Für teilerfremde Zahlen $a, b \in \mathbb{N}$ gilt $\phi(a * b) = \phi(a) * \phi(b)$

Definition (Untergruppe):

- Sei $(G, *)$ eine Gruppe und $\emptyset \neq U \subseteq G$
- ⇒ $\forall a, b \in U : a * b \in U$
- ⇒ $\forall a \in U : a^{-1} \in U$

Definition (Homomorphismus / Isomorphismus):

- Seien $(G, *), (H, \circ)$ Gruppen
- Abbildung $f : G \rightarrow H$ heißt Homomorphismus, falls:
- ⇒ $f(a * b) = f(a) \circ f(b) \forall a, b \in G$
- ⇒ Isomorphismus, wenn f zusätzlich bijektiv

Satz (Homomorphismus Eigenschaften):

- Für $f : (G, *) \rightarrow (H, \circ)$ gilt:
- ⇒ $f(1_G) = 1_H$
- ⇒ $f(a^{-1}) = f(a)^{-1} \forall a \in G$
- ⇒ Ist f Isomorph, dann auch f^{-1}
- ⇒ Bild(f) ist eine Untergruppe von H
- ⇒ Kern(f) := $\{a \in G | f(a) = 1_H\}$ ist eine Untergruppe von G
- ⇒ f injektiv ⇔ Kern(f) = $\{1_G\}$

Satz:

- Sei G eine endliche Gruppe und U eine Untergruppe von G
- ⇒ Die Elementzahl von U ist Teiler der Elementzahl von G

Definition (Quotientengruppe):

- Sei $(G, *)$ eine Abelsche Gruppe und $U \subseteq G$
- Dann ist auf $G \setminus U$ die Verknüpfung wohldefiniert:
- ⇒ $[a]_U \circ [b]_U := [a * b]_U \forall a, b \in G$

Satz (Struktursatz endlicher abelscher Gruppen):

- Endliche abelsche Gruppen G sind isomorph zu Gruppen der Form: $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}, k \geq 1$
- wobei $n_1 \geq 2$ und n_i Teiler von n_{i+1} ist
- Es ist weiterhin $|G| = n_1 \cdot n_2 \cdot \dots \cdot n_k$

Satz (Homomorphiesatz):

- Gruppen G und H . $f : G \rightarrow H$ Gruppenhomomorphismus
- ⇒ Gruppen $G \setminus \text{Kern}(f)$ und $\text{Bild}(f)$ sind isomorph
- ⇒ $f : G \setminus \text{Kern}(f) \rightarrow \text{Bild}(f)$
- ⇒ $[a]_{\text{Kern}(f)} \mapsto f([a]_{\text{Kern}(f)}) := f(a)$

Satz:

- m, n teilerfremd. $(\mathbb{Z}_{nm}, +)$ und $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ isomorph
- ⇒ $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, [a]_{mn} \mapsto [a]_m \times [a]_n$ sind Isomorphismen
- m, n teilbar. $(\mathbb{Z}_{nm}, +)$ und $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ nicht isomorph
- Einschränkung von obigen f auf $\mathbb{Z}_{nm}^*, f : \mathbb{Z}_{nm}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$
- ⇒ falls m, n teilerfremd, f ist wohldefiniert und bijektiv

Satz (kleiner Fermat'scher Satz):

- Für Primzahl p und $x \in \mathbb{Z} : x^p \equiv x \pmod{p}$
- $x \in \mathbb{Z}$ nicht teilbar mit Primzahl $p : x^{p-1} \equiv 1 \pmod{p}$
- $n \in \mathbb{N}, x \in \mathbb{Z}$ mit $ggT(x, n) = 1 : x^{\phi(n)} \equiv 1 \pmod{n}$