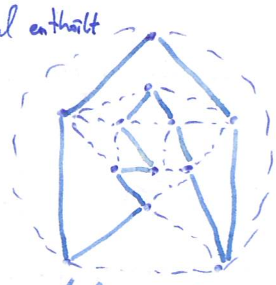
V. Hamilton'sche Graphen

· Def.: $G=(V,E)$ hamilton'sch $\Leftrightarrow$ $\exists$ Hamilton'scher Kreis $K=(V,E'\subseteq E) :=$ Kantenzug, der alle Knoten genau einmal enthält

· Bsp.:


Tetraeder


Oktaeder


Ikosaeder

· Def. Gray-Code := zyklische Folge bestehend aus allen 2^k verschiedenen binären Wörter der Länge $k \geq 1$, bei der sich aufeinanderfolgende Wörter in genau einer Stelle unterscheiden

i) Prop.: $\forall k \geq 1 : \exists$ Gray-Code (Wörtern mit Länge k)

· Bew. (Ind.): IA: $k=1$: $0 \to 1 \to 0$ ist GC

IV: $k=n$ ist GC: $(a_1, \dots, a_{2^k})$

IS: $k=n+1$: $(0a_1, 0a_2, \dots, 0a_{2^k}, 1a_{2^k}, 1a_{2^k-1}, \dots, 1a_1)$ ist GC

ii) Kor.: Der Kantengraph des k-dimensionalen Würfels ($k \geq 2$) ist hamiltonsch (2^k Ecken)

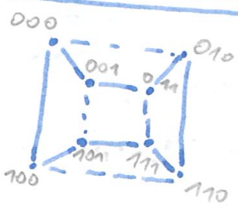
· Bew.: Binäre Wörter des Gray-Code werden als Würfelecken aufgefasst.

· Bsp.:

Gray-Code

000
001
011
010
110
→ 111
101
100
000

Hamilton-Kreis



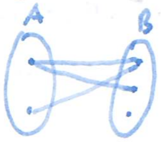
[k=3]

VI. Der Heiratssatz

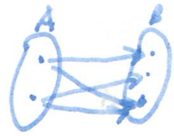
· Def. Digraph := Graph mit gerichteten Kanten

· Def. bipartiter Graph $(A,B,E) :=$ $V = A \cup B$ $\;E \subseteq E_g = \{(x,y) \mid x \in A \wedge y \in B\}$

ungerichteter Fall



gerichteter Fall



· Def. x befreundet y $\Leftrightarrow$ $x \in A \wedge y \in B \wedge xEy$

· Def. (Verheiratung): $\pi : A \to B$ mit $\pi \subseteq E$ inj.

i) Heiratssatz: Für bipartiten Digraphen (A,B,E) sind folgende Aussagen äquivalent:

a) $\exists \pi \in {}^{A}B : \pi \subseteq E \wedge \pi$ inj. ($\cong$ Eindeutige Verheiratung aller Elemente von A mit Elementen von B)

b) $\forall X \subseteq A : |X| \leq |EX := \{y \in B : \exists x \in X : x E y\}|$ [Hall'sche Bedingung]

Ind. in Skript 7/1

· Bew.: a) → b): π inj $\to$ $|X| = |\pi(X)| \leq |EX|$ $[E' = \min\{A' \mid E \setminus A' \leq A\}$

b) → a) (Kontraposition): $\nexists \pi : \pi$ inj $\to$ $\forall \pi \exists_{x,y} \in A : \pi(x) = \pi(y) \to |X = A \setminus E'| > |EX|$

II) Kor. $\forall (A, B, E)$: bipartiter Digraph $\wedge$ $|A| \leq |B|$ $\exists s, r \in \mathbb{Z}^+ : \forall a \in A : |E\{a\}| = r \wedge \forall b \in B : |E^{-1}\{b\}| = s$ $\to \exists \pi : A \to B$ (Verheiratung aller Elemente von A mit Elementen von B)

· Bew: $r \cdot |X| = |E| = s \cdot |EX| \to (s = r \frac{|X|}{|EX|} \wedge |X| \leq |EX| \to s \leq r)$

Ang. ¬Hall: $\exists X \subseteq A : |X| > |EX| : r \cdot |X| = |E \cap (X \times EX)| \leq s \cdot |EX|$

$\to (s \geq r \cdot \frac{|X|}{|EX|} \wedge |X| > |EX| \to s > r) \to$ ↯

VII. Paarungen und Trennungen

· Def.: U trennende Knotenmenge von $A, B \subseteq V$: $A \cap B = \emptyset \Leftrightarrow \forall a \forall b \forall H(a,b) :=$ Kantenzug von a nach b $: \exists v \in U : v \in H$

· Def.: $\pi \subseteq E$ ist Paarung $\Leftrightarrow$ $\forall \langle x,y \rangle, \langle x', y' \rangle \in \pi : \langle x,y\rangle \neq \langle x',y'\rangle \to \{x,y\} \cap \{x',y'\} = \emptyset$

· **Def.: D Defekt von X** $\Leftrightarrow D = |X| - |EX|$

1) Zusammenhang Paarung, Defekt, Trennung: $\forall (A,B,E)$ ungerichteter bipartiter Graph:

$$\underbrace{\max |\pi|}_{\pi \text{ Paarung}} = |A| - \underbrace{\max_{X \subseteq A}(|X| - |EX|)}_{\text{Defekt von } X} = \underbrace{\min |U|}_{U \text{ trennende Knotenmenge}}$$

· Bew.: · $\max |\pi| \geq |A| - \max(|X| - |EX|)$

Def.: $l := \max_{X \subseteq A}(|X| - |EX|)$; $X_0 \subseteq A : |X_0| - |EX_0| = l$; $Y_0 := A \setminus X_0$; $E' := \{\langle x,y \rangle \in E : x \in X_0\}$;

$E'' := \{\langle x,y \rangle \in E : x \in Y_0 \wedge y \notin EX_0\}$

1. Beh.: $(Y_0, E''Y_0, E'')$ erfüllt Hall'sche Bed.:

Ang. $\exists Y \subseteq Y_0 : |Y| > |E''Y| \to |X_0 \sqcup Y| - |E(X_0 \sqcup Y)| = |X_0| + |Y| - |EX_0 \sqcup E''Y| =$
$= |Y| - |E''Y| + l > l$ ↯ Def. l $\to \exists \pi'' : Y_0 \hookrightarrow E''Y_0$ mit $\pi'' \subseteq E''$ (Paarung)

2. Beh.: $(EX_0, X_0, (E')^{-1})$ erfüllt Hall'sche Bedingung:

Ang. $Z \subseteq EX_0 : |Z| > |Z_0 := (E')^{-1}Z| \to |X_0 \setminus Z_0| - |E(X_0 \setminus Z_0)| = |X_0| - |Z_0| - |EX_0| + |Z|$
$= |X_0| - |EX_0| + |Z| - |Z_0| > l \to$ ↯ Def. l. $\to \exists \pi' : EX_0 \hookrightarrow X_0 : \pi' \subseteq E'$ Paarung

$\Rightarrow \pi := \pi_1 \sqcup \pi_2 : |\pi| = |A| - l \to \max |\pi| \geq |A| - l$

· $|A| - \max(|X| - |EX|) \geq \min |U|$: X_0, l wie oben; $U_0 := (A \setminus X_0) \sqcup EX_0$

$\to U_0$ trennt A und B $\wedge$ $|U_0| = (|A| - |X_0|) + (|X_0| - l) = |A| - l$

· $\min |U| \geq \max |\pi|$: π Paarung, U trennende Knotenmenge:

$\forall \langle x,y \rangle \in \pi : \{x,y\} \cap U \neq \emptyset \to |\pi| \leq |U|$

$\Rightarrow \max |\pi| \geq |A| - \max(|X| - |EX|) \geq \min |U| \geq \max |\pi|$ (→ Gleichheit)

Serie 7 - Bäume

- Def.: $G(V,E)$ kreisfrei $\Leftrightarrow \nexists H \subseteq E$: H geschlossener Kantenzug
- Def. (Baum): $G(V,E)$ ist Baum $\Leftrightarrow$ G zusammenhängend $\wedge$ G kreisfrei

i) Lemma: $G(V,E)$ ungerichtet, zsh., nicht-leer, **endlich**: $|E| \geq |V| - 1$

- Bew. (Ind.):

  FI: $|V| = 1 \rightarrow 0 \geq 0$

  FII: $|V| > 1$: i) $\forall v \in V: \deg(v) \geq 2 \rightarrow |E| \geq |V|$

  ii) $\exists v_0 \in V: \deg(v) = 1$

  IS: Betr. $|V' := V \setminus \{v_0\}|$; $|E' := E \setminus \{\langle v_0, v_{01}\} : v_{01}$ adjazent $v_0|$

  Base case: FI $\vee$ FII. i)

ii) Lemma: $G(V,E)$ ungerichtet, kreisfrei, nicht-leer, endlich: $|E| \leq |V| - 1$

- Bew.: FI: G zsh.: Kreisfrei $\rightarrow \exists v_0 \in V: \deg(v_0) = 1$

  Bew.: Ang $\forall v \in V: \deg(v) \geq 2 \rightarrow \forall \langle v_1, v \rangle : \exists \langle v, v_2 \rangle : v_1 \neq v_2$

  Sei H Kantenzug: $H = \{v_1, v_2, \dots, v_i\} \wedge \exists v_j : \langle v_i, v_j \rangle \in E \wedge v_j \neq v_{i-1}$

  FI.I: $v_j \in \{v_1, \dots, v_{i-2}\} \rightarrow \lightning$ kreisfrei

  FI.II: $\exists H' = \{v_1, \dots, v_i, v_{j=i+1}\}$ Kantenzug

  $|V| < \infty \rightarrow \exists H_{max} = \{v_1, \dots, v_n\} : \forall v \in V : v \in H_{max} \wedge \exists \langle v_n, v_j \rangle : v_j \neq v_{n-1}$

  $\rightarrow \{v_j, \dots, v_n\}$ ist Kreis $\rightarrow \lightning$ kreisförmig

  Also existiert für jeden kreisfreien Graphen $G(V,E)$ ein $v_0 : \deg(v_0) = 1$

  $G' := (V' = V \setminus \{v_0\}, E' = E \setminus \{\langle v_j, v_0 \rangle\}) \rightarrow |V'| = |V| - 1$; $|E'| = |E| - 1$

  Wegen $E' \subseteq E$ ist aber folglich auch G' kreisfrei $\rightarrow \exists v_0 \in V' : \deg(v_0) = 1$

  $\Rightarrow |V| = |E| + 1$

  FII: G nicht zsh.: $\exists G_1, \dots, G_n : G_1 \cup \dots \cup G_n = G$ mit G_i zsh.

  $\rightarrow |E| = \sum_{i=1}^{n} E_i = \sum_{i=1}^{n} V_i - 1 = |V| - n \leq |V| - 1$

Kapitel 8 – Der Verallgemeinerte Euklid'sche Algorithmus (I)

$a_0, a_1 \in \mathbb{N}^+$

FI: $a_0 = a_1 = ggT(a_0, a_1)$

FII: $a_0 \neq a_1$: $\exists \max\{B := \{b \mid a_0 \geq b_0 a_1 \wedge b \in \mathbb{N}\}\}$

$\rightarrow b_0$ kl. nat. Zahl: $a_0 < (b_0+1)\cdot a_1$

FII.I: $a_0 = b_0 a_1 \rightarrow ggT(a_0, a_1) = a_1$

FII.II: $a_0 > b_0 a_1 \rightarrow 0 < a_0 - b_0 a_1 =: a_2 < a_1$

mit a_1, a_2 [Euklid'scher Algorithmus]

Bsp.:
$$986 = 357\cdot 2 + 272$$
$$357 = 272 \cdot 1 + 85$$
$$272 = 85 \cdot 3 + 17$$
$$85 = 17 \cdot 5 + 0 \quad \rightarrow ggT(986, 357) = 17$$

Def. (endlicher Kettenbruch):

$b_0 \in \mathbb{Z}; b_{1\leq i \leq n} \in \mathbb{N}^+$

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots\, b_{n-1} + \cfrac{1}{b_n}}}}}$$

I) Jeder Bruch lässt sich als endlicher Kettenbruch schreiben.

Bew. Sei $\frac{a_0}{a_1}$ ein Bruch. Mittels Euklid'schen Algorithmus folgt:
$$\frac{a_0}{a_1} = \frac{b_0 \cdot a_1 + a_2}{a_1} = b_0 + \frac{a_2}{a_1} = b_0 + \cfrac{1}{\frac{a_1}{a_2}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\frac{a_2}{a_3}}} = \ldots =$$

$$a_n = b_n \cdot a_{n+1} + 0 \quad \underset{=}{} \quad b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots\, b_{n-1} + \cfrac{1}{b_n}}}$$

Bsp.: $$\frac{986}{357} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{5}}}$$

Bsp.: $\sqrt{3} = \overset{b_0}{1} + (\sqrt{3} - 1)$
$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = 1 + \left(\frac{\sqrt{3}-1}{2}\right)$$
$$\frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} = 2 + (\sqrt{3}-1)$$
$$\rightarrow \sqrt{3} = [1, \overline{1, 2}]$$

Def. (unendlicher Kettenbruch):
$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots}}}$$
nicht abbrechend

II) Kettenbruch irrationaler Zahlen: $\forall \xi \in \mathbb{I}^+ := \mathbb{R}^+ \setminus \mathbb{Q}^+ \;\exists\; [b_0, b_1, \ldots]$ unendl. KB: $[b_0, b_1, \ldots] = \xi$

Def. (Gaußklammer): $\lfloor \xi \rfloor := \max\{n \in \mathbb{N} \mid n \leq \xi\}$

$\xi = b_0 + r_1$ $\quad [b_0 := \lfloor \xi \rfloor;\ r_1 = \xi - b_0 : 0 < r_1 < 1]$

$\frac{1}{r_1} = b_1 + r_2$ $\quad [b_1 := \lfloor \frac{1}{r_1} \rfloor;\ r_2 = \frac{1}{r_1} - b_1 : 0 < r_2 < 1]$

$\frac{1}{r_2} = b_2 + r_3$ $\quad [b_2 := \lfloor \frac{1}{r_2} \rfloor;\ r_3 = \frac{1}{r_2} - b_2 : 0 < r_3 < 1]$

$\Big\}$ $[b_0, b_1, b_2, \ldots]$ unendl. KB. von ξ

III) Verallgemeinerter Euklid'scher Algorithmus

· Berechnung von Näherungsbrüchen: $P_{-2} := 0,\ P_{-1} := 1,\ Q_{-2} := 1,\ Q_{-1} := 0,\ P_n := b_n P_{n-1} + P_{n-2}$

$Q_n := b_n Q_{n-1} + Q_{n-2}$

Bsp.:

n	-2	-1	0	1	2	3	4	…
b_n			1	2	2	2	2	…
P_n	0	1	1	3	7	17	41	…
Q_n	1	0	1	2	5	12	29	…

Tabelle für KB: $[1,\overline{2}] = \sqrt{2}$

Näherungsbrüche von $\sqrt{2}$: $\frac{P_0}{Q_0} = \frac{1}{1},\ \frac{P_1}{Q_1} = \frac{3}{2},\ \frac{P_2}{Q_2} = \frac{7}{5},\ \frac{P_3}{Q_3} = \frac{17}{12},\ \frac{P_4}{Q_4} = \frac{41}{29},\ \frac{P_5}{Q_5} = \frac{99}{70}$

· Korrektheit vEA: Beh.: $[b_0,\dots,b_n] = \frac{P_n}{Q_n}$

Bew. (Ind.): IA $(n=0)$: $b_0 = \frac{b_0\cdot 1+0}{b_0\cdot 0+1} = \frac{b_0}{1}$ ✓ IV: $[b_0,\dots,b_n] = \frac{P_n}{Q_n}$

IS: $[b_0,\dots,b_{n+1}] = [b_0,\dots,b_n + \frac{1}{b_{n+1}}] = \frac{(b_n + \frac{1}{b_{n+1}})P_{n-1} + P_{n-2}}{(b_n + \frac{1}{b_{n+1}})Q_{n-1} + Q_{n-2}} = \frac{b_n b_{n+1} P_{n-1} + P_{n-1} + P_{n-2}\cdot b_{n+1}}{b_n b_{n+1} Q_{n-1} + Q_{n-1} + Q_{n-2}\cdot b_{n+1}} =$

$= \frac{b_{n+1}(P_{n-1}\cdot b_n + P_{n-2}) + P_{n-1}}{b_{n+1}(b_n Q_{n-1} + Q_{n-2}) + Q_{n-1}} = \frac{P_{n+1}}{Q_{n+1}}$ □

· Zsh. $P_{n-1}, P_n, Q_{n-1}, Q_n$: $\forall n \geq -1$: $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$

Bew. (Ind.): IA $(n=-1)$: $1\cdot 1 - 0\cdot 0 = 1$ ✓

IS: $P_{n+1} Q_n - P_n Q_{n+1} = (b_{n+1} P_n + P_{n-1}) Q_n - P_n (b_{n+1} Q_n + Q_{n-1}) = P_{n-1} Q_n - P_n Q_{n-1} = -(-1)^{n-1} =$

$= (-1)^n$ □

II. Eindeutigkeit der Primfaktorzerlegung

1) Lemma: $\forall a,b,c \in \mathbb{N}^+ : a|bc \wedge ggT(a,b) = 1 \rightarrow a|c$ $\quad [[b_0,\dots,b_n] =: KB(\frac{a}{b})]$

· Bew.: FI $(n=0)$: $a = b\cdot b_0 \rightarrow b = 1 \rightarrow a|c$

FII $(n>0)$: $ggT(a,b) = 1 \rightarrow \frac{P_n}{Q_n} = \frac{a}{b} \xrightarrow{\text{Zsh. } Q,P} a\cdot Q_{n-1} - P_{n-1} b = (-1)^{n-1}$

$\rightarrow \exists k, l \in \mathbb{Z} : |k| = Q_{n-1} \wedge |l| = P_{n-1} : k\cdot a + l\cdot b = 1$

$\rightarrow c = c\cdot(ka + lb) = cka + lbc \overset{\exists s: as = bc}{=} cka + las = a\cdot(ck + ls)$ □

· Def.: $p \in \mathbb{N}$ ist prim $\leftrightarrow p > 1 \wedge n|p \rightarrow n = 1 \vee n = p$

II) Lemma: $\forall m \in \mathbb{N}_{>1} : \exists p_i : i \in \mathbb{N} : \prod p_i = m$

Bew.: IA $(m=2)$: $m = p_0 = 2$ IV: $\forall n \leq m-1\ \exists p_i : \prod p_i = n$

IS: FI: $\exists p : p|m \rightarrow m = p\cdot n \overset{IV}{=} p\cdot \prod p_i = \prod p_i$

FII: $\nexists p : p|m \rightarrow m$ prim $\rightarrow m = p_0$ □

III) Lemma: $\forall m \in \mathbb{N}_{>1} : \exists! \prod_{i\in I} p_i = m$

Bew.: $a := \prod_{i\leq n} p_i$; $b := \prod_{j\leq m} q_j$ z.z.: $a = b \rightarrow \prod_{i\leq n} p_i = \prod_{j\leq m} q_j$

IA $(n=0)$: $p_0 = a = b \rightarrow p_0 = b = \prod_{j\leq m} q_j = q_0$

IS: $p_0 | a \wedge \underset{(\equiv p_0 = q_0)}{a = b} \rightarrow p_0 | b$; $p_0 \cdot \prod_{1\leq i\leq n} p_i = a = b = q_0 \prod_{0<j\leq m} q_j$

FI: $p_0 | q_0 \rightarrow \prod p_i = \prod q_j$ mit Anzahl $p_i^{\leq n}, q_j \leq m \xrightarrow{IV}$ Aussage

FII: $p_0 \nmid q_0 \rightarrow p_0 | \prod_{0\leq j\leq m} q_j \rightarrow \exists j_0 : q_{j_0} = p_0 \rightarrow \prod_{0<i\leq n} p_i = \prod_{\substack{0\leq j\leq m \\ \setminus\{j_0\}}} q_j \xrightarrow{IV}$ Aussage

IV) Korollar: Jede natürliche Zahl $n \geq 2$ lässt sich, bis auf Vertauschung der Faktoren, eindeutig als Produkt von Primzahlen schreiben.

III. Bemerkungen zu unendlichen Kettenbrüchen

$\left[\frac{P_n}{Q_n}\right.$ n-ter Näherungsbruch$\left.\right]$

1) Kettenbruch von ξ konvergiert gegen ξ: $\forall \xi \in I: [b_0, b_1, \dots]$ KB von ξ: $\lim_{n\to\infty} \frac{P_n}{Q_n} = \xi$

Bew.: Sei $\xi_n := \frac{1}{r_n}$. $\xi = [b_0, \xi_1] = [b_0, b_1, \xi_2] = \dots = [b_0, b_1, \dots, b_n, \xi_{n+1}]$

$$\xi \overset{I.III)}{=} \frac{P_n \xi_{n+1} + P_{n-1}}{Q_n \xi_{n+1} + Q_{n-1}} \to \left|\xi - \frac{P_n}{Q_n}\right| = \left|\frac{P_{n-1}Q_n - P_n Q_{n-1}}{Q_n(Q_n \xi_{n+1} + Q_{n-1})}\right| \underset{\substack{Q_n \geq n \\ \xi > 1}}{\overset{I.III)}{\leq}} \left|\frac{(-1)^n}{n^2}\right| = \frac{1}{n^2}$$

II) Konvergenz von Kettenbrüchen: $\forall [b_0, b_1, \dots]$ KB unendl., $\forall \frac{P_n}{Q_n}$ Näherungsbrüche von $[b_0, b_1, \dots]$:

$$\exists! \, \xi \in \mathbb{R}: \xi = \lim_{n\to\infty} \frac{P_n}{Q_n}$$

Bew. (Intervallschachtelung): $I_n := \left[\frac{P_{2n}}{Q_{2n}}, \frac{P_{2n+1}}{Q_{2n+1}}\right]$. Zeige I_n ist Intervallschachtelung.

a) $\frac{P_{2n}}{Q_{2n}} < \frac{P_{2n+1}}{Q_{2n+1}}$ (nichtleere Intervalle):

$$0 < 1$$
$$0 < P_{2n+1}Q_{2n} - P_{2n}Q_{2n+1} \quad \} \, I.III)$$
$$\frac{P_{2n}}{Q_{2n}} < \frac{P_{2n+1}}{Q_{2n+1}} \quad \forall n \, P_n, Q_n \neq 0$$

b) $\frac{P_{2n}}{Q_{2n}} < \frac{P_{2n+2}}{Q_{2n+2}}$: $P_{2n}(b_{2n+2}Q_{2n+1} + Q_{2n}) < (b_{2n+2}P_{2n+1} + P_{2n})Q_{2n}$

$$0 < P_{2n+1}Q_{2n} - Q_{2n+1}P_{2n} = 1 \checkmark$$

c) $\frac{P_{2n+1}}{Q_{2n+1}} < \frac{P_{2n+3}}{Q_{2n+3}}$: $P_{2n+1}(b_{2n+3}Q_{2n+2} + Q_{2n+1}) < Q_{2n+1}(b_{2n+3}P_{2n+2} + P_{2n+1})$

$$Q_{2n+2}P_{2n+1} - Q_{2n+1}P_{2n+2} < 0$$
$$-1 < 0 \checkmark$$

d) $\lim_{n\to\infty} \frac{P_{2n+1}}{Q_{2n+1}} - \frac{P_{2n}}{Q_{2n}} = 0$: $\left|\frac{P_{n+k}}{Q_{n+k}} - \frac{P_n}{Q_n}\right| = \left|\sum_{l=1}^{k}\left(\frac{P_{n+l}}{Q_{n+l}} - \frac{P_{n+l-1}}{Q_{n+l-1}}\right)\right| \leq$

$$\leq \sum_{l=1}^{k}\left|\frac{P_{n+l}}{Q_{n+l}} - \frac{P_{n+l-1}}{Q_{n+l-1}}\right| = \sum_{l=1}^{k}\left|\frac{1}{Q_{n+l}Q_{n+l-1}}\right| \leq \sum_{l=1}^{k}\left|\frac{Q_{n+l} - Q_{n+l-1}}{Q_{n+l}Q_{n+l-1}}\right| = \sum_{l=1}^{k}\left|\frac{1}{Q_{n+l-1}} - \frac{1}{Q_{n+l}}\right|$$

$$\leq \frac{1}{Q_n} \leq \frac{1}{n} \to \text{Intervallschachtelung mit } \lim I_n = [\xi, \xi]$$

III) Anmerkung: Kettenbruch von Wurzeln natürlicher Zahlen: $\forall n \in \mathbb{N}: \sqrt{n} \notin \mathbb{Q} \to$

$\to \sqrt{n} = [b_0, \overline{b_1, \dots, b_k, 2b_0}]$ mit $k \in \mathbb{N}$, $b_0 = \lfloor\sqrt{n}\rfloor \wedge \forall i: 1 \leq i \leq k: b_i = b_{k-i}$

IV) Anmerkung: Lösung Pell'scher Gleichung $(x^2 - D \cdot y^2 = 1)$: $\sqrt{n} \notin \mathbb{Q} \to$ Näherungsbrüche von $\sqrt{n}$ lösen für $(k+1)m - 1$ ($k+1$ ... Periodenlänge, $n \in \mathbb{N}$) die Gleichung $x^2 - ny^2 = 1$

Bsp: $\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}] \to k = 5$, $\frac{P_5}{Q_5} = \frac{170}{39}$: $170^2 - 19 \cdot 39^2 = 1$

Kapitel 9 – Grundbegriffe der Gruppentheorie

· Def. (Gruppe): $(G, e, \circ)$ ist Gruppe $\Leftrightarrow$ $(G, e, \circ)$ ist Modell von GT $\Leftrightarrow$
$\Leftrightarrow$ $(G, e, \circ)$ hat $\mathcal{L}_{GT}$-Struktur $= \{e, \circ\}$ mit Bereich G

I. GT-Axiome:

I) $\forall x,y,z: (x \circ y) \circ z = x \circ (y \circ z)$ [Assoziativität]

II) $\forall x: e \circ x = x$ [neutrales Element]

III) $\forall x \exists y: x \circ y = e$ [inverses Element]

II. Folgerungen aus GT

a) **Linksinverses ist Rechtsinverses**: $\forall x,y: (x \circ y = e) \to (y \circ x = e)$

· Bew.: Sei $\bar{\bar{y}}$ inv. $\bar{y}$; $\bar{y}$ l.I. von x. $x \circ \bar{y} = e \circ x \circ \bar{y} = \bar{\bar{y}} \circ \bar{y} \circ x \circ \bar{y} = \bar{\bar{y}} \circ e \circ \bar{y} = \bar{\bar{y}} \circ \bar{y} = e$

b) e ist auch Rechtsneutrales.

Bew.: $ae \overset{II}{=} a(\bar{a}a) \overset{I}{=} (a\bar{a})a \overset{II}{=} ea \overset{II}{=} a$

c) G hat genau ein Neutrales.

· Bew.: $e = e \circ \tilde{e} = \tilde{e}$

d) $\forall a \in G: \exists! \, \bar{a}: a\bar{a} = \bar{a}a = e$

· Bew.: $\bar{a}' = \bar{a}'e = \bar{a}'a\bar{a} = e\bar{a} = \bar{a}$

III. Abelsche Gruppen

· Def. (Abelsch): G ist abelsch $\Leftrightarrow$ G kommutativ $\Leftrightarrow$ $\forall x,y \in G: x \circ y = y \circ x$

1) Faktum: $\forall a \in G: a \circ a = e \to G$ abelsch

· Bew.: Sei x^{-1} das Inverse von x.

$$\forall a,b \in G: (b \circ a) \circ (a \circ b) \overset{Vor.}{=} b \circ e \circ b \overset{V.}{=} e \Rightarrow b \circ a = (a \circ b)^{-1}$$
$$(a \circ b) \circ (a \circ b) \overset{V.}{=} e \Rightarrow a \circ b = (a \circ b)^{-1}$$
$$\Big\} \; b \circ a = (a \circ b)^{-1} = a \circ b$$

IV. Untergruppen

· Def. (Untergruppe): H ist Untergruppe von G $\Leftrightarrow$ G Gruppe $\wedge$ H nichtleer $\wedge$ $H \subseteq G$ $\wedge$
$\wedge \; \forall x,y \in H: x \circ y^{-1} \in H$

· Schreibweise: $H \leq G$; für $H \neq G$ auch $H < G$

i) <u>Prop.</u>: $H \leq G \rightarrow H$ ist Gruppe

· Bew.: GTO: $x,y \in H \overset{\text{Def.}}{\Rightarrow} e \circ y^{-1} = y^{-1} \in H \overset{\text{Def.}}{\Rightarrow} x(y^{-1})^{-1} = xy \in H \rightarrow H$ abgeschlossen unter assoziativer Operation $\circ$

ii) <u>Triviale Untergruppen</u>: $\{e\}$, G nennt man triviale Untergruppen

iii) <u>$\bigcap_{i \in \Lambda} U_i : U$ ist Untergruppe ist Untergruppe</u>

· Bew.: Sei Λ Indexmenge, $\forall \lambda \in \Lambda: H_\lambda \leq G$, $H := \bigcap_{\lambda \in \Lambda} H_\lambda$.

$x,y \in H \rightarrow \forall \lambda \in \Lambda: x,y \in H_\lambda \rightarrow GT_{0,1,2}$

$\hookrightarrow xy^{-1} \in H_\lambda \rightarrow xy^{-1} \in H$

V. Ordnung

· Def. (Ordnung einer Gruppe): $\operatorname{ord}(G) = |G|$

· Def. (Ordnung eines Gruppenelements): $\operatorname{ord}(x) = n \Leftrightarrow n \in \mathbb{N}_{\geq 1} \wedge n = \min\{\bar{n} \in \mathbb{N}_{\geq 1} \mid x^{\bar{n}} = e\}$

$\operatorname{ord}(x) = \infty \Leftrightarrow \nexists n$ wie oben

i) <u>Wohldefiniertheit der Ordnung einer endlichen Gruppe</u>

· <u>Beh.</u>: G endlich $\rightarrow \forall x: \operatorname{ord}(x) < \infty$

$x^n \cdot x^{m-n} = x^n \cdot e = x^m$

· Bew.: $\{x^1, x^2, \dots\} \subseteq G \rightarrow \exists n,m \in \mathbb{N}_{\geq 1}: n < m \wedge x^{m-n} = x^0 := e$

ii) <u>Kor.</u>: $\{x^k \mid k < \operatorname{ord}(x)\} \leq G$

VI. Erzeugte Untergruppe

· Def.: $\langle X \rangle$ erzeugte Untergruppe von $X \Leftrightarrow \langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$

i) <u>Folgerung</u>: a) $\langle X \rangle$ ist Untergruppe $\overset{\text{IV iii)}}{:}$ $\langle X \rangle \leq G$

b) $\langle X \rangle$ ist kleinste von X generierte Gruppe

$\langle x \rangle := \langle \{x\} \rangle$

VII. Zyklische Gruppen

· Def.: G ist <u>zyklisch</u> $\Leftrightarrow |G| = n \rightarrow \exists g \in G: G = \{g^k : k < n\}$

i) <u>Faktum</u>: G zyklisch $\Leftrightarrow \exists g \in G: \operatorname{ord}(g) = |G|$

ii) <u>Faktum</u>: Zyklische Gruppen sind immer abelsch: $x^n \circ x^m = x^{m+n} = x^m \circ x^n$

iii) <u>Faktum</u>: G Gruppe, $x \in G: \operatorname{ord}(x) = n \rightarrow \langle x \rangle$ ist zykl. Gr. $\wedge |\langle x \rangle| = n$

· Bew.: $\langle x \rangle = \{x^1, x^2, \dots, x^n = e\} \Rightarrow$ zykl. $\wedge |\langle x \rangle| = n$

· **Kor.**: Sei G Gruppe, $x \in G$. $\mathrm{ord}(x) < \infty \rightarrow \langle x \rangle \leq G \wedge |\langle x \rangle| = \mathrm{ord}(x)$

VIII. Produkte von Gruppen

i) **Prop.**: Seien $(G, \circ, e_G)$, $(H, \bullet, e_H)$ Gruppen. Dann: $(G \times H, *, \langle e_G, e_H \rangle)$ mit $\langle g_1, h_1 \rangle * \langle g_2, h_2 \rangle := \langle g_1 \circ g_2, h_1 \bullet h_2 \rangle$ Gruppe

· Bew.: GT_0: $*$ komponentenweise def. $\wedge$ GT_0 für $\circ, \bullet \rightarrow *$ assoziativ
GT_1: $\langle e_G, e_H \rangle$ neutr. El. GT_2: $\langle g^{-1}, h^{-1} \rangle$ inv. El.

· Def. (Isomorphe Gruppen): $(G_0, \circ) \underset{\text{isom.}}{\cong} (G_1, \bullet) \Leftrightarrow \exists \alpha : G_0 \rightarrow G_1$ mit α bij. $\wedge\ \forall x,y \in G_0 : \alpha(x \circ y) = \alpha(x) \bullet \alpha(y)$

· Bemerkung: Abbildung von n. El.$(G_0) \rightarrow$ n. El.(G_1); i. El$(G_0) \rightarrow$ i. El(G_1) bei isomorphen Gruppen

ii) **Faktum**: $G \times \{e_H\} \leq G \times H \wedge G \cong G \times \{e_H\}$

· Bew.: $\bar{x} := \langle x, e_H \rangle$, $\bar{y} := \langle y, e_H \rangle \in G \times \{e_H\} \overset{x,y \in G}{\rightarrow} \bar{x}\bar{y}^{-1} = \langle xy^{-1}, e_H \bullet e_H^{-1} \rangle = \langle xy^{-1}, e_H \rangle$
$\alpha : G \rightarrow G \times \{e_H\}, x \mapsto \langle x, e_H \rangle$

IX. Nebenklassen

· Def. (Linksnebenklasse): Sei $H \leq G \wedge x \in G$. $xH := \{xh : h \in G\}$

· Def. (Rechtsnebenklasse): Sei $H \leq G \wedge x \in G$. $Hx := \{hx : h \in G\}$

i) **Lemma** (Links-Version; analoges für Rechts-Version)
Sei G Gruppe, $H \leq G$, $x,y \in G$.

a) $|xH| = |H|$ $[\Leftrightarrow \exists \varphi : H \rightarrow xH : \varphi$ bij.$]$

·Bew.: $\varphi_x : H \rightarrow xH$; $\varphi_x(h) := xh$; Inj.: $\varphi_x(h_1) = \varphi_x(h_2) \rightarrow xh_1 = xh_2 \rightarrow xh_1h_2^{-1} = x \rightarrow h_1h_2^{-1} = e$
$\rightarrow h_1 = h_2$; Surj.: $z \in xH \rightarrow z = xh \rightarrow \exists h : \varphi_x(h) = z \rightarrow \varphi$ bij. $\rightarrow |xH| = |H|$

b) $x \in xH$ [Bew.: $e_H \in H \rightarrow x \circ e_H = x \in H$]

c) $xH = H \Leftrightarrow x \in H$ [Bew.: „$\rightarrow$": $x \circ e_H = x \in H$; „$\leftarrow$": $y \in xH$; $y = x \circ h \wedge x,h \in H \rightarrow y \in H$]

d) $xH = yH \Leftrightarrow x^{-1}y \in H$ [Bew.: „$\rightarrow$": $x^{-1}y \notin H \rightarrow \nexists h : x \circ h = y \rightarrow xH \neq yH$ (Kontrapos.); „$\leftarrow$": $x^{-1}y \in H \rightarrow$
$\rightarrow \exists h : x \circ h = x \circ x^{-1} \circ y \circ \bar{h} = y \circ \bar{h} \rightarrow xH = yH$]

e) $xH = \{g \in G : gH = xH\}$ [Bew.: $z \in xH \underset{\exists g \in G}{\rightarrow} z = g \circ h$; $\bar{g} \in \{g \in G \mid gH = xH\} \rightarrow \exists h_1, h_2 : \bar{g} h_1 =$
$\overset{1)}{=} \bar{g} \circ \bar{g}^{-1} \circ x \circ \tilde{h}_1 = x \circ \tilde{h}_1 \in xH$]

ii) **Kor.** (IX.1) b) $\wedge$ IX.1) b) rechts.-Version): $H \leq G \rightarrow \bigcup_{x \in G} xH = G = \bigcup_{x \in G} Hx$

iii) **Lemma** (Folgerung IX.1) d)): $H \leq G \rightarrow \forall x,y \in G : xH = yH$ XOR $xH \cap yH = \emptyset$

· Bew.: $xH \cap yH = \emptyset \rightarrow$ fertig; $z \in xH \cap yH \rightarrow \exists h_1, h_2 \in H : yh_2 = z = xh_1 \rightarrow z^{-1}y = h_2^{-1} \in H \wedge$
$\wedge\ x^{-1}z = h_1 \in H \rightarrow (x^{-1}z)(z^{-1}y) = x^{-1}y \in H \overset{1)d)}{\rightarrow} xH = yH$

· Def.:

Kapitel 10 – Modulrechnung

Betrachte hier stets kommutative, unitäre Ringe (Axiome $RT_0 - RT_8$; $\mathcal{L}_{RT} = \{0, 1, +, \cdot\}$)

I. Ideale

Def.: $I \subseteq R$ $(RT_0 - RT_8)$ Ideal $\leftrightarrow$
$$I_0 : I \neq \emptyset$$
$$I_1 : \forall a, b \in I : a + b \in I$$
$$I_2 : \forall x \in R \; \forall a \in I : x \cdot a \in I$$

i) $(I, 0, +)$ abelsche Untergruppe von $(R, 0, +)$

ii) $1 \in I \to I$ Ring

iii) $1 \notin I \to I$ kein Ring

iv) triviale Ideale: $R \subseteq R \wedge \{0\} \subseteq R =:$ Nullideal

v) Bsp.: a) $m\mathbb{Z} := \{x \cdot m \mid x \in \mathbb{Z}\}$ Ideal in $(\mathbb{Z}, 0, 1, +, \cdot)$

Bew.: $y \cdot (x \cdot m) = (y \cdot x) \cdot m \in m\mathbb{Z}$

$ym + xm = (y + x) m \in m\mathbb{Z}$

b) $(f) := \{g \cdot f \mid g \in \mathbb{Z}[X]\}$ ist Ideal für $\mathbb{Z}[X]$ Ring der Polynome mit Koeff. in $\mathbb{Z}$; $f = 1 - X^2 + 7X^3 \in \mathbb{Z}[X]$

$$g_1 \cdot f + g_2 \cdot f = (g_1 + g_2) \cdot f \in (f)$$
$$g_1 \cdot (g_2 \cdot f) = (g_1 \cdot g_2) \cdot f \in (f)$$

vi) Prop.: $I \subseteq \mathbb{Z}$ Ideal $\to \exists m \in \mathbb{Z} : I = m\mathbb{Z}$

Bew.: FI: $I =$ Nullideal $\to I = 0\mathbb{Z}$

FII: $I \neq$ Nullideal.

$m := \min\{n \in \mathbb{N} \setminus \{0\} : n \in I\}$

Wid. Bew.: Ang. $\exists a \in I : a \notin m\mathbb{Z}$.

Dann $\exists n := \max\{n' \in \mathbb{N} \setminus \{0\} \mid n' \cdot m < a\}$

$\to a - n \cdot m < m \in I$ ↯

II. Faktorringe

- Def (Restklasse): $\overline{x} := x + I = \{x + a \mid a \in I\}$
- Def. (binäre Relation): $\sim := \; x \sim y \leftrightarrow \overline{x} = \overline{y} \leftrightarrow x + I = y + I \leftrightarrow (x-y) + I = I$

  $\sim$ Äquivalenzrelation wegen „=" Äquiv. r. $\qquad \leftrightarrow (x-y) \in I$
- Def. (Operationen auf $R\backslash I$): $\overline{x} \oplus \overline{y} := \overline{x+y}$; $\overline{x} \otimes \overline{y} := \overline{x \cdot y}$

1) Lemma: $x_0, x_1, y_0, y_1 \in R : \overline{x_0} = \overline{x_1} \wedge \overline{y_0} = \overline{y_1} \rightarrow$ i) $\overline{x_0} \oplus \overline{y_0} = \overline{x_1} \oplus \overline{y_1}$

   ii) $\overline{x_0} \otimes \overline{y_0} = \overline{x_1} \otimes \overline{y_1}$

   Bew.: siehe Skript

   $\rightarrow (R\backslash I, \overline{0}, \overline{1}, \oplus, \otimes)$ ist Faktorring

   Def.: $R\backslash I := \{\overline{x} \in \mid x \in R\}$

III. Die Ringe $\mathbb{Z}_m$

- Def.: $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/I$

i) Prop.: $\forall m \geq 2 \; \forall \overline{a} \in \mathbb{Z}_m : \exists \overline{b} \in \mathbb{Z}_m : \overline{a} \cdot \overline{b} = \overline{1} \leftrightarrow ggT(a, m) = 1$

   Bew.: „$\rightarrow$": $d := ggT(a, m)$. $\overline{a} \cdot \overline{b} = \overline{1} \leftrightarrow a \cdot b = m \cdot l + 1$

   $\xrightarrow{d \mid ab;\, d \mid ml} d \mid ab - ml = 1 \rightarrow d = 1$

   „$\leftarrow$": $ggT(a, m) = 1 \rightarrow ba + ml = 1 \rightarrow ab \equiv 1 \pmod m$

ii) Die Elemente von $\mathbb{Z}_m$, die ein Inverses besitzen bilden eine Gruppe bzgl. der Multiplikation (Einheitengruppe): $\mathbb{Z}_m^*$.

iii) $|\mathbb{Z}_m^*| =: \varphi(m)$ Euler'sche-Phifunktion

iv) Satz von Euler-Fermat: $a^{\varphi(m)} \equiv 1 \pmod m$

v) Kleiner Fermat: $a^p \equiv a \pmod p$ [Kor. Satz v. Euler-Fermat]

IV. Der Chinesische Restsatz

Seien $m_{0 \leq i \leq k} \in \mathbb{Z}^+$ paarweise teilerfremd, $a_{0 \leq i \leq k} \in \mathbb{Z}$. Dann $\exists n \in \mathbb{Z} \; \forall 0 \leq i \leq k$:

$n \equiv a_i \pmod{m_i}$

V. Die Körper $\mathbb{F}_p$

1) $\mathbb{Z}_m$ ist Körper $\leftrightarrow$ m prim

· Bew.: m prim $\rightarrow$ $(\mathbb{Z}_p, \bar{0}, \bar{1}, +, \cdot)$ ist Ring mit $(\overset{\mathbb{Z}_p \setminus \{0\}}{\overset{\shortparallel}{\mathbb{Z}_p^*}}, \bar{1}, \cdot)$ abelsche Gruppe

$\rightarrow$ $\mathbb{Z}_p$ Körper

$\neg$ m prim $\rightarrow \exists n \in \mathbb{Z}_m : \nexists n^{-1} \in \mathbb{Z}_m : n^{-1} n = 1 \rightarrow \mathbb{Z}_m$ kein Körper

· Def (maximales Ideal): I max. Ideal $\leftrightarrow \nexists J \subsetneq R : J$ echtes Ideal $(:= J \neq R) \wedge I \subsetneq J$
$\wedge\, I \neq R$

11) <u>Prop.</u>: R Ring; $I \neq R$ Ideal: R/I Körper $\Leftrightarrow$ I max. Ideal

· Bew.: $(\Leftarrow)$ Kontraposition: Ang. $I \subsetneq R$ Ideal $\wedge$ R/I kein Körper.

$\rightarrow \exists a_0 \in R/I \; \forall x \in R : \bar{a}_0 \cdot \bar{x} \neq \bar{1}$.

$J_0 := \{x \cdot a_0 + y \cdot b : x, y \in R \wedge b \in I\} \rightarrow J_0$ Ideal $\wedge$ $1 \notin J_0$

$[\bar{x} \cdot \bar{a}_0 + y \cdot b = 1 \wedge b \in I \rightarrow \bar{x} \cdot \bar{a}_0 = \bar{1} \rightarrow \lightning]$

$\Rightarrow I \subsetneq J_0 \subsetneq R \Rightarrow \lightning$

$(\Rightarrow)$ R/I Körper $\rightarrow 1 \in$