GRENZFRAGEN
DER GRUPPENTHEORIE UND LOGIK

(Oleg Bogopolski, WiSe 2020/21)

1. Primitiv rekursive, partiell rekursive und allgemein rekursive Funktionen

Sei $\mathbb{N} = \{0, 1, 2, \dots\}$ die Menge von natürlichen Zahlen. Für eine Funktion $f : X \to Y$ wird ihr Definitionsbereich X mit δ_f bezeichnet. Mit ρ_f wird das Bild von f bezeichnet. Im Folgenden arbeiten wir mit *n-ary partiellen Funktionen* der Sorte

$$f(x_1, \dots, x_n) : \delta_f \to \mathbb{N},$$

wobei $n \in \{1, 2, \dots\}$ und $\delta_f \subset \mathbb{N}^n$ ist. Manchmal schreiben wir $f^{(n)}$, um zu unterstreichen, dass f eine n-ary Funktion ist. Eine n-ary partielle Funktion f heißt *total*, falls $\delta_f = \mathbb{N}^n$ ist.

Definition 1.1. Folgende totale Funktionen heißen *Elementarfunktionen*:

1) $s^{(1)}(x) = x + 1$ (Successor=Nachfolger)
2) $o^{(n)}(x_1, \dots, x_n) = 0$ (Null)
3) $P^n_m(x_1, \dots, x_n) = x_m$, (Projektion)
   wobei $n, m \in \{1, 2, \dots\}$ und $1 \leqslant m \leqslant n$ ist.

Definition 1.2. Wir betrachten drei Arten, eine Funktion aus den gegebenen Funktionen zu konstruieren:

(a) (**Komposition**)
Seien $g^{(m)}$ und $h^{(n)}_1, \dots, h^{(n)}_m$ partielle Funktionen. Die partielle Funktion

$$f^{(n)}(x_1, \dots, x_n) = g^{(m)}\big(h^{(n)}_1(x_1, \dots, x_n), \dots, h^{(n)}_m(x_1, \dots, x_n)\big)$$

heißt *Komposition* von Funktionen $g^{(m)}$ und $h^{(n)}_1, \dots, h^{(n)}_m$.

(b) (**Primitive Rekursion**)
• Eine partielle Funktion $f^{(n+1)}(x_1, \dots, x_n, y)$ entsteht aus den partiellen Funktionen $g^{(n)}(x_1, \dots, x_n)$ und $h^{(n+2)}(x_1, \dots, x_n, y, z)$ durch *primitive Rekursion*, wenn Folgendes gilt:

$$\begin{aligned} f^{(n+1)}(x_1, \dots, x_n, 0) &= g^{(n)}(x_1, \dots, x_n), \\ f^{(n+1)}(x_1, \dots, x_n, y+1) &= h^{(n+2)}\big(x_1, \dots, x_n, y, f^{(n+1)}(x_1, \dots, x_n, y)\big). \end{aligned}$$

• Zudem definieren wir die primitive Rekursion für $n = 0$ deutlich:
Eine partielle Funktion $f^{(1)}$ entsteht aus der Zahl $a \in \mathbb{N}$ und der partiellen Funktion $h^{(2)}(y, z)$ durch *primitive Rekursion*, wenn Folgendes gilt:

$$\begin{aligned} f^{(1)}(0) &= a, \\ f^{(1)}(y+1) &= h^{(2)}\big(y, f^{(1)}(y)\big). \end{aligned}$$

(c) (**μ-Operator**)
Sei $g^{(n+1)}(x_1, \ldots, x_n, y)$ eine partielle Funktion. Wir definieren eine neue partielle Funktion

$$f^{(n)}(x_1, \ldots, x_n) = \mu y[g^{(n+1)}(x_1, \ldots, x_n, y) = 0]$$

wie folgt:
$f^{(n)}(x_1, \ldots, x_n)$ ist definiert und gleich y genau dann, wenn

- $g^{(n+1)}(x_1, \ldots, x_n, y) = 0$ ist und
- $g^{(n+1)}(x_1, \ldots, x_n, 0), \ldots, g^{(n+1)}(x_1, \ldots, x_n, y-1)$ definiert und ungleich 0 sind.

Definition 1.3. (1) Eine Funktion $f^{(n)}(x_1, \ldots, x_n)$ heißt *primitiv rekursiv*, falls sie aus der Elementarfunktionen mit Hilfe endlich vieler Anwendungen von Komposition und primitiver Rekursion konstruiert werden kann. Die Klasse aller primitiv rekursiven Funktionen wird mit **PrR** bezeichnet.

(2) Eine partielle Funktion $f^{(n)}(x_1, \ldots, x_n)$ heißt *partiell rekursiv*, falls sie aus den Elementarfunktionen mit Hilfe endlich vieler Anwendungen von Komposition, primitiver Rekursion und den μ-Operator konstruiert werden kann. Die Klasse aller partiell rekursiven Funktionen wird mit **PaR** bezeichnet.

(3) Eine Funktion $f^{(n)}(x_1, \ldots, x_n)$ heißt *allgemein rekursiv*, falls sie partiell rekursiv und total ist, also falls sie auf ganzem $\mathbb{N}^n$ definiert ist. Die Klasse aller allgemein rekursiven Funktionen wird mit **AR** bezeichnet.

Folgendes ist klar: $\mathbf{PrR} \subseteq \mathbf{AR} \subseteq \mathbf{PaR}$.

Behauptung 1.4. $\mathbf{AR} \subsetneqq \mathbf{PaR}$.

Beweis. Die Funktion $g(x, y) = x + y + 1$ liegt in **PrR** (leichte Aufgabe). Somit liegt die Funktion

$$f(x) = \mu y[g(x, y) = 0]$$

in **PaR**. Sie liegt aber nicht in **AR**, weil sie nirgendwo definiert ist. □

Satz 1.5. $\mathbf{PrR} \subsetneqq \mathbf{AR}$.

Vorbereitung zum Beweis. Für jede partielle Funktion f aus einer Teilmenge von $\mathbb{N}$ nach $\mathbb{N}$ und jede Zahl $n \in \{1, 2, \ldots\}$ sei $f[n]$ die n-Fache Komposition von f mit sich:

$$f[n](x) = \underbrace{f \circ f \circ \cdots \circ f}_{n}(x).$$

Nun definieren wir eine Folge von Funktionen $a_0, a_1, \dots$ aus $\mathbb{N}$ nach $\mathbb{N}$:

$$\begin{aligned} a_0(x) &= x+1, \\ a_{i+1}(x) &= a_i[x+2](x). \end{aligned}$$

Lemma 1.6. (1) Für alle i und x gilt $a_i(x) > x$. Außerdem gilt

$$a_{i+1}(x) > a_i(x) > \cdots > a_0(x) > x.$$

(2) Für alle $x, y \in \mathbb{N}$ gilt

$$a_k[y+1](x) < a_{k+1}(\max(x,y)). \tag{1.1}$$

Beweis. (1) ist leicht. Wir beweisen (2). Wenn $y \leqslant x$ ist, dann gilt

$$a_k[y+1](x) < a_k[x+2](x) = a_{k+1}(x) = a_{k+1}(\max(x,y)).$$

Wenn $y > x$ ist, dann gilt

$$a_k[y+1](x) < a_k[y+2](y) = a_{k+1}(y) = a_{k+1}(\max(x,y)).$$

□

Lemma 1.7. Für jede primitiv rekursive Funktion $f(x_1, \dots, x_n)$ existiert ein $k \in \{1, 2, \dots\}$, so dass für alle $(x_1, \dots, x_n) \in \mathbb{N}^n$ gilt:

$$f(x_1, \dots, x_n) < a_k\big(\max(x_1, \dots, x_n)\big).$$

Kurz gesagt, ist jede primitiv rekursive Funktion von einer der Funktionen a_k majoriert.

Beweis. Wir beweisen, dass diese Eigenschaft für alle Elementarfunktionen gilt und nach einer Anwendung einer Komposition oder einer primitiven Rekursion weiterhin gilt.

- Elementarfunktionen:

$$s(x) = x+1 = a_0(x) < a_1(x),$$

$$o^{(n)}(x_1, \dots, x_n) = 0 < \max(x_1, \dots, x_n) + 1 = a_0(\max(x_1, \dots, x_k)),$$

$$P^n_k(x_1, \dots, x_n) = x_k \leqslant \max(x_1, \dots, x_k) < a_0(\max(x_1, \dots, x_k)).$$

• Komposition: Seien $g^{(m)}$ und $h_1^{(n)}, \dots, h_m^{(n)}$ primitiv rekursive Funktionen, die von einer Funktion a_K majoriert sind. Wir beweisen, dass ihre Komposition $f^{(n)}$ von a_{K+1} majoriert ist:

$$\begin{aligned} f(x_1, \dots, x_n) &= g\big(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n)\big) \\ &< a_K\big(\max(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))\big) \\ &< a_K\big(\max\big(a_K(\max(x_1, \dots, x_n)), \dots, a_K(\max(x_1, \dots, x_n))\big)\big) \\ &= a_K\big(a_K\big(\max(x_1, \dots, x_n)\big)\big) \\ &\leqslant a_{K+1}\big(\max(x_1, \dots, x_n)\big). \end{aligned}$$

• Primitive Rekursion:

Seien $g(x_1, \dots, x_n)$ und $h(x_1, \dots, x_n, y, z)$ primitiv rekursive Funktionen, die von einer Funktion a_K majoriert sind. Sei $f(x_1, \dots, x_n, y)$ die Funktion, die durch primitive Rekursion aus g und h entsteht. Wir beweisen, dass f von a_{K+1} majoriert ist. Es gilt

$$f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n) < a_K(\max(x_1, \dots, x_n)),$$

$$\begin{aligned} f(x_1, \dots, x_n, 1) &= h\big(x_1, \dots, x_n, 0, f(x_1, \dots, x_n, 0)\big) \\ &< a_K\big(\max(x_1, \dots, x_n, 0, f(x_1, \dots, x_n, 0))\big) \\ &< a_K\big(\max(x_1, \dots, x_n, 0, a_K(\max(x_1, \dots, x_n, 0)))\big) \\ &= a_K\big(a_K\big(\max(x_1, \dots, x_n)\big)\big) \\ &\leqslant a_K[2]\big(\max(x_1, \dots, x_n)\big). \end{aligned}$$

Per Induktion erhalten wir

$$f(x_1, \dots, x_n, y) < a_K[y+1]\big(\max(x_1, \dots, x_n)\big),$$

Daraus und aus (1.1) folgt

$$f(x_1, \dots, x_n, y) < a_{K+1}\big(\max(x_1, \dots, x_n, y)\big).$$

Also ist f von a_{K+1} majoriert. □

Beweis des Satzes 1.5. Wir definieren $A(x) = a_x(x)$. Diese Funktion ist nicht primitiv rekursiv:

Nehmen wir an, dass $A(x)$ primitiv rekursiv ist. Nach Lemma 1.7 existiert ein $k \in \mathbb{N}$ mit $A(x) < a_k(x)$ für alle $x \in \mathbb{N}$. Insbesondere gilt

$$A(k+1) < a_k(k+1) < a_{k+1}(k+1) \overset{Def.}{=} A(k+1).$$

Ein Widerspruch.

Also ist $A(x)$ nicht primitiv rekursiv. Es bleibt zu beweisen, dass $A(x)$ allgemein rekursiv ist. Das ist nicht leicht und folgt aus dem Fakt, dass die Klasse aller allgemein rekursiven Funktionen und die Klasse aller totalen Funktionen, die mit der Turing Maschine berechenbar sind, gleich sind. □

2. Zwei Sätze über primitiv rekursive Funktionen

Lemma 2.1. Ist $g(x_1, \ldots, x_n, x_{n+1})$ eine primitiv rekursive Funktion. Dann ist die Funktion

$$G(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, 0)$$

priminiv rekursiv.

Lemma 2.2. Sei $g(x_1, \ldots, x_n, x_{n+1})$ primitiv rekursiv. Dann sind auch die Funktionen

$$f_1(x_1, \ldots, x_n, y) = \sum_{i=0}^{y} g(x_1, \ldots, x_n, i)$$

und

$$f_2(x_1, \ldots, x_n, y) = \prod_{i=0}^{y} g(x_1, \ldots, x_n, i)$$

primitiv rekursiv.

Lemma 2.3. Seien $h(x_1, \ldots, x_n)$ und $g(x_1, \ldots, x_n, x_{n+1})$ primitiv rekursiv. Dann sind auch die Funktionen

$$F_1(x_1, \ldots, x_n) = \sum_{i=0}^{h(x_1,\ldots,x_n)} g(x_1, \ldots, x_n, i)$$

und

$$F_2(x_1, \ldots, x_n) = \prod_{i=0}^{h(x_1,\ldots,x_n)} g(x_1, \ldots, x_n, i)$$

primitiv rekursiv.

Definition 2.4. Seien $g(x_1, \ldots, x_n, y)$ und $h(x_1, \ldots, x_n)$ zwei totale Funktionen. Nehmen wir an, dass die Funktion

$$f(x_1, \ldots, x_n) = \mu y[g(x_1, \ldots, x_n, y) = 0]$$

für alle $x_1, \ldots, x_n$ definiert ist und für alle $x_1, \ldots, x_n$ gilt:

$$f(x_1, \ldots, x_n) \leqslant h(x_1, \ldots, x_n).$$

Dann sagen wir, dass f mit Hilfe des *begrenzten μ-Operators* aus g und h entsteht und schreiben

$$f(x_1, \ldots, x_n) = \big(\mu y \leqslant h(x_1, \ldots, x_n)\big)[g(x_1, \ldots, x_n, y) = 0].$$

Bevor wir weiter fortfahren, definieren wir vier nützliche Funktionen:
1)

$$\mathrm{sg}(x) = \begin{cases} 0, & x = 0 \\ 1, & x \geqslant 1. \end{cases}$$

2)

$$\overline{\mathrm{sg}}(x) = \begin{cases} 1, & x = 0 \\ 0, & x \geqslant 1. \end{cases}$$

3) $p(x)$ ist die x-te Primzahl. Also gilt $p(0) = 2$, $p(1) = 3$, $p(2) = 5$ u.s.w.

4) $\mathrm{ex}(x, y)$ ist die Exponente von $p(x)$ in der Primzahlzerlegung von y, falls $y \geqslant 2$ ist; dabei ist $\mathrm{ex}(x, 1) = \mathrm{ex}(x, 0) = 0$.

Zum Beispiel gilt $\mathrm{ex}(0, 60) = 2$, $\mathrm{ex}(1, 60) = 1$, $\mathrm{ex}(2, 60) = 1$ und $\mathrm{ex}(7, 60) = 0$.

In der ersten Übung haben wir bewiesen, dass diese Funktionen primitiv rekursiv sind.

Satz 2.5. Seien $g(x_1, \ldots, x_n, y)$ und $h(x_1, \ldots, x_n)$ zwei primitiv rekursive Funktionen. Nehmen wir an, dass die Funktion $f(x_1, \ldots, x_n)$ mit Hilfe des begrenzten μ-Operators aus g und h entsteht. Dann ist $f(x_1, \ldots, x_n)$ ebenfalls primitiv rekursiv.

Beweis. Wir haben

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{h(x_1,\ldots,x_n)} \mathrm{sg}\Big(\prod_{j=0}^{i} g(x_1, \ldots, x_n, j)\Big).$$

Dann ist f primitiv rekursiv nach Lemma 2.3. □

Definition 2.6. Wir sagen, dass die partielle Funktion $f^{(n+1)}$ aus den partiellen Funktionen $g^{(n)}$, $h^{(n+s+1)}$, $t_1^{(1)}, \ldots, t_s^{(1)}$ mit Hilfe der *zurückgreifenden Rekursion* entsteht, wenn $t_1^{(1)}(y) \leqslant y, \ldots, t_s^{(1)}(y) \leqslant y$ für alle y ist und es gilt:

$$\begin{aligned} f(x_1, \ldots, x_n, 0) &= g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, y+1) &= h\big(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, t_1(y)), \ldots, f(x_1, \ldots, x_n, t_s(y))\big). \end{aligned}$$

Satz 2.7. Nehmen wir an, dass die Funktion $f^{(n+1)}$ aus den rekursiv primitiven Funktionen $g^{(n)}$, $h^{(n+s+1)}$, $t_1^{(1)}, \ldots, t_s^{(1)}$ mit Hilfe der zurückgreifenden Rekursion entsteht. Dann ist $f^{(n+1)}$ ebenfalls primitiv rekursiv.

Beweis. Wir definieren eine Funktion $F(x_1, \ldots, x_n, y)$ durch

$$F(x_1, \ldots, x_n, y) := \prod_{i=0}^{y} p(i)^{f(x_1,\ldots,x_n,i)}.$$

Merken wir an: $f(x_1, \ldots, x_n, y) = \mathrm{ex}(y, F(x_1, \ldots, x_n, y))$. Deswegen reicht es zu zeigen, dass die Funktion F primitiv rekursiv ist. Das folgt aber aus den primitiv rekursiven Schemata:

$$\begin{aligned} F(x_1, \ldots, x_n, 0) &= 2^{f(x_1,\ldots,x_n,0)}, \\ F(x_1, \ldots, x_n, y+1) &= F(x_1, \ldots, x_n, y) \cdot p(s(y))^{H(x_1,\ldots,x_n,y)}, \end{aligned}$$

wobei

$$\begin{aligned} H(x_1, \ldots, x_n, y) = h\Big(x_1, \ldots, x_n, y, \;& \mathrm{ex}\big(t_1(y), F(x_1, \ldots, x_n, y)\big), \\ & \ldots, \\ & \mathrm{ex}\big(t_s(y), F(x_1, \ldots, x_n, y)\big)\Big) \end{aligned}$$

ist. □

3. Turing Maschinen

• Eine *Turing Maschine* T ist definiert durch die folgenden drei Punkte:

(1) *Externes Alphabet* $\mathcal{A} = \{a_0, a_1, \ldots, a_n\}$, wobei $a_0 = 0$, $a_1 = 1$ ist;
(2) Alphabet der internen *Zustände* $Q = \{q_0, q_1, \ldots, q_m\}$;
(3) *Programm*, also eine Menge der *Kommandos* $T(i,j)$, $(i = 1, \ldots, m;$ $j = 0, \ldots, n)$, jedes von ihnen hat eine der folgenden Formen:

$$q_i a_j \to q_k a_l, \quad q_i a_j \to q_k a_l R, \quad q_i a_j \to q_k a_l L, \quad (0 \leqslant k \leqslant m, 0 \leqslant l \leqslant n).$$

• Ein *Maschinenwort* (oder eine *Konfiguration*) ist ein Wort der Form $Aq_k a_l B$, wobei $q_k \in Q$, $a_l \in \mathcal{A}$ ist und A und B Worte im Alphabet $\mathcal{A}$ sind (können leere Worte sein).

Wir werden auch folgende Schreibweisen verwenden:
Für die Kommandos:

$$\overset{q_i}{a_j} \to \overset{q_k}{a_l}, \quad \overset{q_i}{a_j} \to a_l \overset{q_k}{*}, \quad \overset{q_i}{a_j} \to \overset{q_k}{*} a_l$$

Für die Konfiguration:

$$A\overset{q_k}{a_l}B$$

• Sei T eine Turing Maschine und sei $M = A\overset{q_i}{a_j}B$ ein Maschinenwort. Mit M'_T bezeichen wir ein Maschinenwort, das aus M mit Hilfe folgender Regeln entsteht:

(1) Wenn $i = 0$ ist, dann ist $M'_T = M$.
(2) Wenn $i > 0$ ist, dann gelten folgende Regeln:
   (a) Wenn $T(i,j)$ die Form $\overset{q_i}{a_j} \to \overset{q_k}{a_l}$ hat, dann ist $M'_T = A\overset{q_k}{a_l}B$;
   (b) Wenn $T(i,j)$ die Form $\overset{q_i}{a_j} \to a_l \overset{q_k}{*}$ hat, dann ist

$$M'_T = \begin{cases} Aa_l\overset{q_k}{a_s}B_1, & \text{falls } B = a_s B_1, \qquad \text{[Fall (b1)]} \\ Aa_l\overset{q_k}{a_0}, & \text{falls } B = \varnothing. \qquad \text{[Fall (b2)]} \end{cases}$$

   (c) Wenn $T(i,j)$ die Form $\overset{q_i}{a_j} \to \overset{q_k}{*} a_l$ hat, dann ist

$$M'_T = \begin{cases} A_1\overset{q_k}{a_s}a_l B, & \text{falls } A = A_1 a_s, \qquad \text{[Fall (c1)]} \\ \overset{q_k}{a_0}a_l B, & \text{falls } A = \varnothing. \qquad \text{[Fall (c2)]} \end{cases}$$

• Sei T eine Turing Maschine und M eine Konfiguration. Wir definieren $M_T^{(0)} = M$, $M_T^{(n+1)} = (M_T^{(n)})'$, $n = 0, 1, \ldots$. Für zwei Konfigurationen M und M_1 sagen wir, dass die Maschine T die Konfiguration M in die Konfiguration M_1 *transformiert*, wenn $M_1 = (M_T^{(n)})'$ für ein n ist.

Wir schreiben $M \Rightarrow_T M_1$, wenn die Maschine T die Konfiguration T in die Konfiguration T_1 transformiert und der Fall (c2) nicht benutzt wird; wir schreiben $M \models\!\Rightarrow_T M_1$, falls bei der Transformation die Fälle (b2) und (c2) nicht benutzt werden.

• Im Folgenden benutzen wir die Abkürzung a_i^x für das Wort $\underbrace{a_i a_i \ldots a_i}_{x}$.

Wir sagen, dass die Turing Maschine T eine n-ary partielle Funktion $f : \delta_f \to \mathbb{N}$ *berechnet*, wobei $\delta_f \subseteq \mathbb{N}^n$ und $\rho_f \subseteq \mathbb{N}$ ist, falls folgende zwei Bedingungen erfüllt sind:

(i) Wenn $(x_1, \ldots, x_n) \in \delta_f$ ist, dann transformiert die Turing Maschine T die Input-Konfiguration $\overset{q_1}{0}1^{x_1}0 \ldots 1^{x_n}0$ in eine Konfiguration $A\overset{q_0}{a_i}B$, die genau $f(x_1, \ldots, x_n)$ 1-Symbole enthält[1].

(ii) Wenn $(x_1, \ldots, x_n) \notin \delta_f$ ist, dann arbeitet T bei der Input-Konfiguration $M = \overset{q_1}{0}1^{x_1}0 \ldots 1^{x_n}0$ so, dass das Symbol q_0 bei keiner der Nachfolgekonfigurationen $M_T^{(m)}$ auftreten wird.[2].

• Wir sagen, dass die Turing Maschine T die Funktion $f^{(n)}$ *regulär berechnet*, wenn folgendes gilt:

(i) Wenn $(x_1, \ldots, x_n) \in \delta_f$ ist, dann gilt

$$\overset{q_1}{0}1^{x_1}0 \ldots 1^{x_n}0 \Rightarrow_T \overset{q_0}{0}1^{f(x_1,\ldots,x_n)}00 \ldots 0;$$

(ii) Wie (ii) oben.

• Eine partielle Funktion f heißt *(regulär) Turing berechenbar*, wenn eine Turing Maschine T existiert, die diese Funktion (regulär) berechnet.

---

[1]Nach Definition (1) ist klar, dass die letzte Konfiguration nicht mehr in eine andere Konfiguration transformiert wird. Somit kann man sagen, dass die Maschine bei diesem Input nach endlich vielen Schritten stoppt.

[2]In diesem Fall sagen wir, dass die Maschine bei diesem Input unendlich lange arbeitet.

• Seien T_1 und T_2 zwei Turing Maschinen mit demselben externen Alphabet $\mathcal{A} = \{a_0, a_1, \ldots, a_n\}$ und mit den Alphabeten von internen Zuständen

$$Q_1 = \{q_0, q_1, \ldots, q_r\} \text{ und } Q_2 = \{q_0, q_1, \ldots, q_s\}.$$

und den Programmen $\prod_1$ und $\prod_2$.

Die Komposition der Maschinen $T_1 \cdot T_2$ wird als Turing Maschine mit

a) dem externen Alphabet $\mathcal{A}$,

b) dem Alphabet der internen Zustände $Q_3 = \{q_0, q_1, \ldots, q_{r+s}\}$,

c) dem Programm $\prod_3 = S^{q_0}_{q_{r+1}} \prod_1 \cup S^{q_1 \cdots q_s}_{q_{r+1} \cdots q_{r+s}} \prod_2$ definiert,

wobei $S^{q_j}_{q_i} \prod$ die Menge von Kommandos ist, die aus $\prod$ durch Ersetzen von q_j durch q_i entsteht.

Beispiel. Die Funktion $s(x) = x + 1$ ist berechenbar mit Hilfe von Turing Maschine mit $\mathcal{A} = \{0, 1\}$, $Q = \{q_0, q_1, q_2\}$ und $\prod$:

$$\overset{q_1}{0} \to 0\overset{q_2}{*}, \quad \overset{q_1}{1} \to \overset{q_0}{1}, \quad \overset{q_2}{0} \to \overset{q_0}{1}, \quad \overset{q_2}{1} \to 1\overset{q_2}{*}.$$

In der Tat, für $x = 0$ erhalten wir

$$\overset{q_1}{0}0 \to 0\overset{q_2}{0} \to 0\overset{q_0}{1}$$

und für $x \geqslant 1$ erhalten wir

$$\overset{q_1}{0}1^x0 \to 0\overset{q_2}{1}1^{x-1}0 \to \cdots \to 01^{x-1}\overset{q_2}{1}0 \to 01^x\overset{q_2}{0} \to 01^x\overset{q_0}{1}.$$

Satz 3.1. Für jede n-ary partielle Funktion $f : \delta_f \to \mathbb{N}$ sind folgende Bedingungen äquivalent:

(1) f ist partiell rekursiv.
(2) f ist Turing berechenbar.
(3) f ist regulär Turing berechenbar.

Lemma 3.2.

(a) Die Funktion $c : \mathbb{N}^2 \to \mathbb{N}$ gegeben durch

$$c(x, y) = \frac{(x + y)^2 + 3x + y}{2}$$

bildet $\mathbb{N}^2$ bijektiv auf $\mathbb{N}$ ab[3].

[3]Diese Funktion heißt *Cantor Funktion* von 2 Unbekannten.

(b) Nach (a) existieren Funktionen $\ell : \mathbb{N} \to \mathbb{N}$ und $r : \mathbb{N} \to \mathbb{N}$ mit

$$c(\ell(x), r(x)) = x.$$

Diese Funktionen sind primitiv rekursiv.

Satz 3.3. Jede partiell rekursive Funktion $f(x_1, \ldots, x_n)$ kann in einer *Kleene Normalform* präsentiert werden:

$$f(x_1, \ldots, x_n) = \ell\Big(\mu t\,[g(x_1, \ldots, x_n, t)] = 0\Big),$$

wobei $g(x_1, \ldots, x_n, t)$ eine passende primitiv rekursive Funktion und ℓ die primitiv rekursive Funktion aus Lemma 3.2 ist.

4. Rekursive und rekursiv abzählbare Mengen

Wir reservieren zwei Symbole $\mathbf{t}, \mathbf{f}$ (true und false).

Definition 4.1. Sei $n \geqslant 1$ eine natürliche Zahl.

1) Eine Funktion $P : \mathbb{N}^n \to \{\mathbf{t}, \mathbf{f}\}$ heißt *n-ary Prädikat* auf $\mathbb{N}$. Mit dem Prädikat P assoziieren wir seine *charakteristische Funktion* $\chi_P : \mathbb{N}^n \to \{0, 1\}$, so dass gilt:

$$\chi_P(x_1, \ldots, x_n) = \begin{cases} 0, & \text{falls } P(x_1, \ldots, x_n) = \mathbf{t}, \\ 1, & \text{falls } P(x_1, \ldots, x_n) = \mathbf{f}. \end{cases}$$

Das Prädikat P heißt *rekursiv (primitiv rekursiv)*, falls χ_P rekursiv (primitiv rekursiv) ist.

2) Eine Menge $M \subseteq \mathbb{N}^n$ heißt *rekursiv (primitiv rekursiv)*, falls das mit M assoziierte Prädikat $P_M(x_1, \ldots, x_n) = \mathbf{t} \Leftrightarrow (x_1, \ldots, x_n) \in M$ *rekursiv (primitiv rekursiv)* ist. Die charakteristische Funktion χ_{P_M} bezeichnen wir einfach χ_M. Es ist klar:

$$\chi_M(x_1, \ldots, x_n) = \begin{cases} 0, & \text{falls } (x_1, \ldots, x_n) \in M, \\ 1, & \text{falls } (x_1, \ldots, x_n) \notin M. \end{cases}$$

Mit anderen Worten heißt die Menge $M \subseteq \mathbb{N}^n$ *rekursiv (primitiv rekursiv)*, falls ihre *charakteristische Funktion* χ_M rekursiv (primitiv rekursiv) ist.

3) Eine Menge $M \subseteq \mathbb{N}^n$ heißt *rekursiv aufzählbar*, wenn ein $(n+1)$-ary Prädikat $\widetilde{M}(x_1, \ldots, x_n, y)$ existiert, so dass gilt

(a) $\widetilde{M}$ ist primitiv rekursiv,

(b) $(x_1, \ldots, x_n) \in M \Leftrightarrow \exists y\, \widetilde{M}(x_1, \ldots, x_n, y) = \mathbf{t}$.

Mit anderen Worten:
Eine Menge $M \subseteq \mathbb{N}^n$ heißt *rekursiv aufzählbar*, wenn eine Menge $M' \subseteq \mathbb{N}^{n+1}$ existiert, so dass gilt:

(a) M' ist primitiv rekursiv,
(b) $(x_1, \ldots, x_n) \in M \Leftrightarrow \exists y : (x_1, \ldots, x_n, y) \in M'$.

Satz 4.2. (Post) Eine Teilmenge $M \subseteq \mathbb{N}$ ist rekursiv genau dann, wenn M und $\mathbb{N} \setminus M$ rekursiv aufzählbar sind.

5. Rekursive und rekursiv abzählbare Mengen: Fortsetzung

Satz 5.1. Eine nicht leere Teilmenge $A \subseteq \mathbb{N}$ ist rekursiv genau dann, wenn eine monotone rekursive Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $A = \mathrm{im} f$ existiert.

Beweis.
($\Rightarrow$): Sei A rekursiv. Dann ist χ_A rekursiv.
Fall 1. Sei A unendlich. Wir definieren eine Funktion $f : \mathbb{N} \to \mathbb{N}$ durch

$$\begin{aligned} f(0) &= \mu x\,[\chi_A(x) = 0], \\ f(t+1) &= \mu x\,[\chi_A(x) = 0 \wedge x > f(t)] \\ &= \mu x\,[\chi_A(x) + \overline{\mathrm{sg}}(x \dot{-} f(t)) = 0]. \end{aligned}$$

Zu bemerken: Die Funktion $g(x,t) = \chi_A(x) + \overline{\mathrm{sg}}(x \dot{-} f(t))$ ist rekursiv. Deswegen ist f rekursiv. Offensichtlich ist f strikt monoton und $\mathrm{im}(f) = A$.
Fall 2. Sei $A = \{a_0, \ldots, a_n\}$ endlich mit $a_0 < a_1 < \cdots < a_n$. Dann definieren wir f wie folgt:

$$f(x) = \overline{\mathrm{sg}}(x \dot{-} n) \cdot \Big(\sum_{i=0}^{n} a_i \cdot \overline{\mathrm{sg}}|x - i|\Big) + \mathrm{sg}(x \dot{-} n) \cdot a_n.$$

($\Leftarrow$): Ist A unendlich, dann ist

$$\chi_A(x) = \mathrm{sg}\Big(\prod_{i=0}^{\mu z\,[x < f(z)]} |x - f(i)|\Big).$$

rekursiv, somit ist A rekursiv. Ist $A = \{a_0, \ldots, a_n\}$ endlich, dann ist A ebenfalls rekursiv:

$$\chi_A(x) = \mathrm{sg}\Big(\prod_{i=0}^{n} |x - a_i|\Big).$$

□

Definition 5.2. Sei $f : \delta_f \to \mathbb{N}$ eine partielle Funktion mit $\delta_f \subseteq \mathbb{N}^n$. Folgende Menge heißt *Graphen* von f:

$$\{(x_1, \ldots, x_n, f(x_1, \ldots, x_n)) \,|\, (x_1, \ldots, x_n) \in \delta_f\}.$$

Satz 5.3. (Graphen-Satz) Eine partielle Funktion $f : \delta_f \to \mathbb{N}$ mit $\delta_f \subseteq \mathbb{N}^n$. ist rekursiv genau dann, wenn ihre Graphen Γ_f rekursiv aufzählbar sind.

Satz 5.4. Eine nicht leere Teilmenge $M \subseteq \mathbb{N}^n$ ist rekursiv aufzählbar genau dann, wenn unare primitiv rekursive Funktionen $\alpha_1(x), \ldots, \alpha_n(x)$ existieren, so dass gilt:

$$M = \{\big(\alpha_1(x), \ldots, \alpha_n(x)\big) \,|\, x \in \mathbb{N}\}.$$

Beweis. Wir beweisen den Satz nur für $n = 1$. Sei also $\emptyset \neq M \subseteq \mathbb{N}$.

($\Rightarrow$): Sei M rekursiv aufzählbar. Dann existiert eine rekursiv primitive Menge $M' \subseteq \mathbb{N}^2$, so dass gilt:

$$x \in M \Leftrightarrow \exists y\, (x, y) \in M'.$$

Sei $a \in M$ ein beliebiges Element. Wir definieren eine Funktion $\alpha : \mathbb{N} \to \mathbb{N}$ durch

$$\alpha(x) := \ell(x) \cdot \overline{\text{sg}}\, \chi_{M'}\big(\ell(x), r(x)\big) + a \cdot \chi_{M'}\big(\ell(x), r(x)\big).$$

Dann ist α primitiv rekursiv und es gilt

$$\{\alpha(x) | x \in \mathbb{N}\} = M.$$

Die Inklusion $\subseteq$ folgt aus einer Analyse der zwei Fälle: $\big(\ell(x), r(x)\big) \in M'$ und $\big(\ell(x), r(x)\big) \notin M'$. Wir beweisen die Inklusion $\supseteq$. Sei $m \in M$. Dann existiert ein $y \in \mathbb{N}$ mit $(m, y) \in M'$. Definiere $x = c(m, y)$. Dann gilt $\alpha(x) = m$.

($\Leftarrow$): Sei $M = \{\alpha(x) \,|\, x \in \mathbb{N}\}$, wobei α primitiv rekursiv ist. Dann ist die Menge $M' = (\alpha(x), x)$ primitiv rekursiv: $\chi_{M'}(y, x) = \text{sg}|y - \alpha(x)|$. Da M die Projektion dieser Menge ist, ist M rekursiv aufzählbar. □

Satz 5.5. (Post) Eine Teilmenge $M \subseteq \mathbb{N}$ ist rekursiv genau dann, wenn M und $\mathbb{N} \setminus M$ rekursiv aufzählbar sind.

Beweis.

($\Rightarrow$): Sei $M \subseteq \mathbb{N}$ rekursiv. Nach Satz 5.1 existiert eine rekursive Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $M = \text{im}(f)$. Nach den Graphen-Satz ist $\Gamma_f \subseteq N^2$ rekursiv aufzählbar. Nach Satz 5.4 existieren unäre primitiv rekursive Funktionen α_1 und α_2, so dass gilt:

$$\Gamma_f = \{(\alpha_1(x), \alpha_2(x)) \,|\, x \in \mathbb{N}\}.$$

Dann ist

$$M = \text{im}(f) = \text{im}(\alpha_2).$$

Dann ist M rekursiv aufzählbar als eine Projektion der primitiv rekursiven Menge $M' = \{(\alpha_2(x), x) \mid x \in \mathbb{N}\}$.

Da M rekursiv ist, ist $\mathbb{N}\backslash M$ ebenfalls rekursiv (das folgt aus $\chi_{\mathbb{N}\backslash M} = 1 - \chi_M$). Wie oben ist dann $\mathbb{N} \setminus M$ rekursiv aufzählbar.

($\Leftarrow$): Diese Richtung folgt aus der Formel

$$\chi_M(x) = \chi_{M'}\Big(x, \mu y\,[\chi_{M'}(x,y) \cdot \chi_{(\mathbb{N}\setminus M)'}(x,y) = 0]\Big).$$

□

Definition 5.6.

a) Eine Diophantische Gleichung ist eine Gleichung der Form

$$P(x_1, \ldots, x_m) = 0,$$

wobei P ein Polynom mit ganzen Koeffizienten ist. Man schreibt $\overline{x}$ statt $(x_1, \ldots, x_m)$.

b) Eine Teilmenge $S \subseteq \mathbb{N}^n$ heißt Diophantisch, wenn ein Polynom $P(\overline{x}, \overline{y})$ mit ganzen Koeffizienten existiert, so dass gilt:

$$\overline{x} \in S \;\Leftrightarrow\; \exists \overline{y}\; P(\overline{x}, \overline{y}) = 0$$

Satz 5.7. (Yu. Matiyasevich) Eine Teilmenge $S \subseteq \mathbb{N}^n$ ist rekursiv aufzählbar genau dann, wenn S Diophantisch ist.

6. Freie Gruppen

Bezeichnungen:

1) Sei H eine Untergruppe einer Gruppe G. Der *Index* von H in G ist die Kardinalität der Menge von rechten Nebenklassen von H in G. Dieser Index wird mit $|G : H|$ bezeichnet.

2) Sei S eine Teilmenge einer Gruppe G. Wir bezeichnen

$$S^{-1} = \{s^{-1} \mid s \in S\}.$$

Mit $\langle S \rangle$ wird folgende Untergruppe von G bezeichnet:

$$\langle S \rangle = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N},\ x_i \in S \cup S^{-1},\ i = 1, \dots, n\}.$$

Man sagt, dass diese Untergruppe von S *erzeugt* ist. Eine Teilmenge X von G heißt *Erzeugersystem* von G, wenn G von X erzeugt ist.

Definition 6.1. Eine Gruppe G heißt *frei*, wenn sie eine Teilmenge X hat, so dass $X \cap X^{-1} = \emptyset$ ist und jedes Element $f \in F$ auf genau einer Weise in der Form $f = x_1 x_2 \dots x_n$ geschrieben werden kann, wobei $x_i \in X \cup X^{-1}$ und $x_i x_{i+1} \neq 1$ für $i = 1, \dots, n-1$ ist. Die Menge X heißt *Basis* von F.

Beispiel. Die Gruppe $(\mathbb{Z}, +)$ ist frei mit der Basis $\{1\}$. Eine andere Basis ist $\{-1\}$. Es gibt keine weitere Basis von $(\mathbb{Z}, +)$.

Sei X eine beliebige Menge. Des Weiteren folgt eine "abstrakte" Konstruktion einer freien Gruppe $F(X)$ mit der Basis X. In der Praxis ist es bequemer, mit einer etwas einfacheren Version von $F(X)$ zu arbeiten, s. die nächste Seite.

Eine abstrakte Konstruktion von $F(X)$. Zuerst setzen wir

$$X^{-1} = \{x^{-1} \mid x \in X\},$$

wobei x^{-1} als ein formales Symbol angesehen werden soll. Ein *Wort* in dem Alhabet $X \cup X^{-1}$ ist eine endliche Folge $x_1 x_2 \dots x_n$ mit $n \in \mathbb{N}$. Für $n = 0$ wird dieses Wort mit $\emptyset$ bezeichnet. Ein Wort heißt *gekürzt*, falls es keine Teilworte der Form xx^{-1} oder $x^{-1}x$ mit $x \in X$ enthält. Zum Beispiel für $X = \{a, b\}$ ist das Wort $aabab^{-1}$ gekürzt und das Wort $baa^{-1}b$ nicht.

Zwei Worte u und v heißen *äquivalent* (Bezeichnung $u \sim v$), falls v aus u durch endlich viele Kürzungen und Einsetzungen von Teilworten der Form xx^{-1} oder $x^{-1}x$ mit $x \in X$ entstent. Zum Beispiel ist $abaa^{-1}bb^{-1}b^{-1} \sim b^{-1}ba$. Die Äquivalenzklasse des Wortes u wird mit $[u]$ bezeichnet. Es gilt also

$$[u] = \{v \mid u \sim v\}.$$

Jede Äquivalenzklasse $[u]$ enthält *genau ein* gekürztes Wort. Zum Beispiel ist a das gekürzte Wort in der Klasse $[abaa^{-1}bb^{-1}b^{-1}]$. Auf der Menge

$$F = \{[u] \mid u \text{ ist ein Wort in dem Alphabet } X \cup X^{-1}\}$$

definieren wir eine Multiplikation durch

$$[u] \cdot [v] = [uv].$$

Man kann überprüfen, dass die Menge F mit dieser Multiplikation eine freie Gruppe mit der Basis $\{[x] \mid x \in X\}$ ist. Nun nennen wir $[x]$ durch x um. Dann erhalten wir die freie Gruppe $F(X)$ mit der Basis X.

Eine einfache Version von $F(X)$. In dieser Version ist $F(X)$ die Menge aller gekürzten Worte in dem Alphabet $X \cup X^{-1}$, wobei das Produkt von zwei gekürzten Worten u und v als die gekürzte Form des Wortes uv definiert wird. Zum Beispiel in $F(a, b)$ gilt

$$aabab^{-1} \cdot ba^{-2}b = aaba^{-1}b.$$

Das leere Wort wird mit 1 bezeichnet. Hier ist ein Beispiel eines inversen Elements:

$$(ab^2a^{-1}b)^{-1} = b^{-1}ab^{-2}a^{-1}.$$

Man kann unendlich viele Basen von $F(a, b)$ konstruieren. Zum Beispiel für jedes $n \in \mathbb{Z}$ ist $\{a, a^n b\}$ eine Basis von $F(a, b)$.

Satz 6.2. Alle Basen einer freien Gruppe F haben die gleiche Kardinalität.

Diese Kardinalität heißt *Rang* von F und wird mit $\mathbf{rk}(F)$ bezeichnet. Zwei freie Gruppen sind isomorph genau dann, wenn ihre Ränge gleich sind.

Satz 6.3. (Nielsen)

1) Jede Untergruppe einer freien Gruppe ist frei.
2) Sei H eine Untergruppe einer freien Gruppe F mit endlichem Index i. Wenn Rang $\mathbf{rk}(F)$ endlich ist, dann ist $\mathbf{rk}H$ endlich und es gilt

$$\frac{\mathbf{rk}(H) - 1}{\mathbf{rk}(F) - 1} = i.$$

Beispiel. Wir betrachten die Untergruppe $H = \langle ab, a^2, b^2 \rangle$ der freien Gruppe $F(a, b)$. Man kann überprüfen, dass diese Untergruppe die Basis $\{ab, a^2, b^2\}$ hat. Folglich ist ihr Rang gleich 3. Offensichtlich gilt

$$\frac{3 - 1}{2 - 1} = 2.$$

Satz 6.4. Sei $F = F(x_1, \ldots, x_n)$ eine freie Gruppe mit der endlichen Basis $\{x_1, \ldots, x_n\}$. Für jede natürliche Zahl $k \geqslant 1$ existieren nur endlich viele Untergruppen H von F mit Index k. Diese Untergruppen können mit Hilfe von markierten Graphen aufgelistet werden:

1. Zuerst werden markierte gerichtete zusammenhängende Graphen Γ mit folgenden Eigenschaften gelistet:
   a) Die Anzahl der Knoten von Γ ist k.
   b) Jede gerichtete Kante ist mit einem der Buchstaben $\{x_1, \ldots, x_n\}$ markiert.
   c) Für jeden Knoten v von Γ gibt es genau n Kanten, die in v eingehen und genau n Kanten, die aus v ausgehen. Die eingehenden Kanten sind mit $x_1, \ldots, x_n$ markiert, die ausgehenden Kanten sind ebenfalls mit $x_1, \ldots, x_n$ markiert.

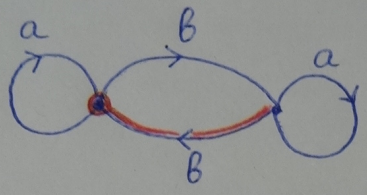
2. Sei Γ einer dieser Graphen. In Γ werden ein Knoten v_0 (Basisknoten) und ein maximaler Baum T gewählt.

3. Jeder gerichteten Kante e, die in Γ, aber nicht in T liegt, wird die Schleife $p_e e q_e$ zugeordnet, wobei p_e ein Weg in T von v_0 zum Anfang der Kante e ist und q_e ein Weg in T vom Ende der Kante e zu v_0 ist.

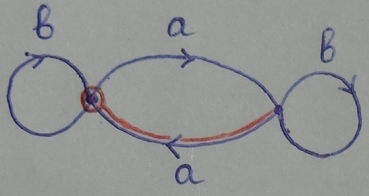
4. Die entsprechende Unteruppe H wird frei erzeugt von allen Worten, die wir über die Wege $p_e e q_e$ lesen.

Einige Beispiele finden Sie auf der nächsten Seite.

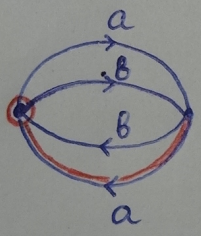
1) Es gibt 3 Untergruppen von Index 2 in $F(a,b)$



$H_1 = \langle a, b^2, b^{-1}ab \rangle$



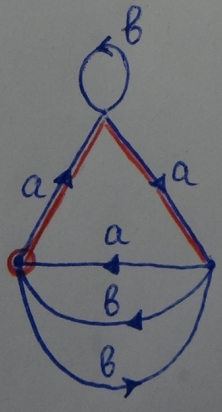
$H_2 = \langle b, a^2, a^{-1}ba \rangle$



$H_3 = \langle a^2, ba, a^{-1}b \rangle$

2) Es gibt 13 Untergruppen von Index 3 in $F(a,b)$

Z.B.



$H = \langle aba^{-1}, a^3, a^2b, ba^{-2} \rangle$

02 12 2020

7. Schnitt von zwei Untergruppen einer freien Gruppe. Normaler Abschluss. Präsentationen einer Gruppe

Bezeichnungen. Für einen Graph Γ bezeichnen wir mit Γ^0 die Menge seiner Eckpunkte und mit Γ^1 die Menge seiner Kanten. Für eine Kante $e \in \Gamma^1$ wird ihr Anfang mit e_- und die Ende mit e_+ bezeichnet. Die inverse zur e Kante wird mit $\overline{e}$ bezeichnet.

Definition 7.1. Sei $\mathcal{A}$ ein Alphabet. Ein Graph Γ heißt *$\mathcal{A}$-Graph*, wenn seine Kanten mit Buchstaben aus $\mathcal{A} \cup \mathcal{A}^{-1}$ markiert sind. Die Markierung einer Kante e wird mit $\mathrm{Mark}(e)$ bezeichnet. Dabei setzen wir voraus, dass $\mathrm{Mark}(\overline{e}) = (\mathrm{Mark}(e))^{-1}$ ist.

Wird in Γ ein Eckpunkt u ausgezeichnet, dann wird das Paar (Γ, u) *basierter Graph* genannt. In dem Fall wird u *Basispunkt* von Γ heißen.

Im Folgenden definieren wir formal und danach weniger formal den pull-back von zwei markierten Graphen.

Definition 7.2. Das *pull-back* von zwei $\mathcal{A}$-Graphen Γ_1 und Γ_2 ist ein $\mathcal{A}$-Graph Γ, der wie folgt definiert ist:

$$\begin{aligned}
\Gamma^0 &= \Gamma_1^0 \times \Gamma_2^0, \\
\Gamma^1 &= \{(e_1, e_2) \,|\, e_1 \in \Gamma_1^1,\ e_2 \in \Gamma_2^1,\ \mathrm{Mark}(e_1) = \mathrm{Mark}(e_2)\}, \\
(e_1, e_2)_- &= ((e_1)_-, (e_2)_-), \\
(e_1, e_2)_+ &= ((e_1)_+, (e_2)_+), \\
\mathrm{Mark}((e_1, e_2)) &= \mathrm{Mark}(e_1) = \mathrm{Mark}(e_2).
\end{aligned}$$

Definition 7.2′ (Pull-back informell) Das *pull-back* von zwei $\mathcal{A}$-Graphen Γ_1 und Γ_2 ist ein $\mathcal{A}$-Graph Γ, der wie folgt definiert ist:

Die Eckpunkte von Γ sind die Paare von Eckpunkten aus Γ_1^0 und Γ_2^0. Eine Kante in Γ läuft von (x, u) nach (y, v) genau dann, wenn eine Kante e_1 in Γ_1 und eine Kante e_2 in Γ_2 existieren, so dass e_1 von x nach y läuft, e_2 von u nach v läuft und die Markierungen von e_1 und e_2 gleich sind. Dabei wird diese Kante in Γ mit $\mathrm{Mark}(e_1)$ markiert.

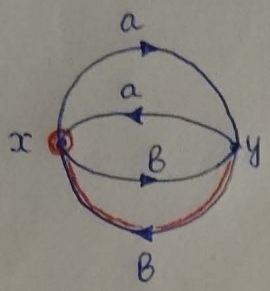
Bemerkung. Es ist möglich, dass das pull-back von zwei zusammenhängenden $\mathcal{A}$-Graphen nicht zusammenhängend ist.

Satz 7.3. Seien H_1 und H_2 zwei Untergruppen einer freien Gruppe $F(\mathcal{A})$. Seien (Γ_1, u_1) und (Γ_2, u_2) die basierten $\mathcal{A}$-Graphen, die mit H_1 und H_2 assoziiert sind.

Sei Γ die Komponente des pull-back von Γ_1 und Γ_2, die den Eckpunkt (u_1, u_2) enthält. Dann ist der basierte $\mathcal{A}$-Graph $(\Gamma, (u_1, u_2))$ mit dem Schnitt $H_1 \cap H_2$ assoziiert.

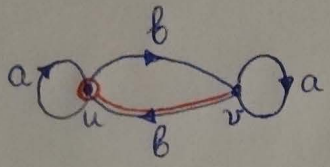
$H_1, H_2 \leq F(a,b)$

Γ_1:



$H_1 = \langle ab, b^{-1}a, b^2 \rangle$

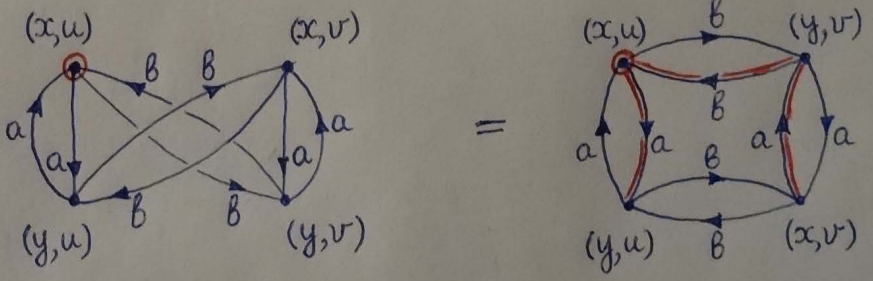
Γ_2:



$H_2 = \langle a, b^2, b^{-1}ab \rangle$

Pull-back von Γ_1 und Γ_2:

Γ:



$H_1 \cap H_2 = \langle a^2, b^2, b^{-1}a^2b, b^{-1}a^{-1}ba^{-1}, abab \rangle$

Eine andere Wahl des maximalen Baumes in Γ produziert eine andere Basis der Gruppe $H_1 \cap H_2$.

13 12 2020

Definition 7.4. Sei R eine nicht leere Teilmenge einer Gruppe G. Der normale Abschluss von R in G ist die Menge

$$\langle\langle R\rangle\rangle_G = \Big\{\prod_{i=1}^{k} g_i^{-1} r_i^{\varepsilon_i} g_i \,|\, k \in \mathbb{N}, g_i \in G, r_i \in R, \varepsilon_i \in \{-1,1\}\Big\}.$$

Für $R = \emptyset$ setzen wir $\langle\langle\emptyset\rangle\rangle_G = 1$.

Bemerkungen. Sei R eine Teilmenge einer Gruppe G. Dann gilt:

1) $\langle\langle R\rangle\rangle_G$ ist die kleinste normale Untergruppe von G, die R enthält.
2) Sei $r \in R \cup R^{-1}$ und seien $u, v \in G$. Dann gilt
$$urv \in \langle\langle R\rangle\rangle_G \Leftrightarrow uv \in \langle\langle R\rangle\rangle_G$$

Definition 7.5. Sei X eine Menge und sei R eine Teilmenge der freien Gruppe $F(X)$. Der Ausdruck $\langle X \,|\, R\rangle$ heißt *Präsentation* einer Gruppe G, wenn ein Homomorphismus $\varphi : F(X) \to G$ existiert, so dass folgendes gilt:

1) $\varphi(X)$ erzeugt die Gruppe G.
2) $\varphi(r) = 1$ in G für jedes $r \in R$.
3) Für jedes $w \in F(X)$ mit $\varphi(w) = 1$ gilt $w \in \langle\langle R\rangle\rangle_F$.

Beispiel. $\langle x, y \,|\, x^2,\, y^2,\, (xy)^3\rangle$ ist eine Präsentation der Gruppe S_3. In der Tat, die Abbildung

$$\begin{aligned} \varphi : \quad & F(x,y) \to S_3, \\ & x \mapsto (12), \\ & y \mapsto (13) \end{aligned}$$

erfüllt die Definition 7.5.

8. Präsentationen von Gruppen (Fortseztung)

Satz 8.1. Sei $n \geqslant 1$ eine natürliche Zahl und seien

$$A = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Die Gruppe $G = \langle A, B\rangle$ hat die Präsentation

$$\langle a, b \,|\, a^{-1}ba = b^n\rangle.$$

Satz 8.2. Die Permutationsgruppe S_n hat folgende Präsentation:

$\langle t_1, \ldots, t_{n-1} \,|\, t_i^2 = 1, \;\; t_i t_j = t_j t_i \;(|i-j| \geqslant 2), \;\; t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1} \;(i = 1, \ldots, n-2)\rangle$.

9. Freie Produkte, amalgamierte Produkte und HNN Erweiterungen

9.1. **Freie Produkte.**

Definition 9.1. Seien G_1 und G_2 zwei Gruppen. Ein formales Produkt $x_1x_2\dots x_n$ mit $x_1,\dots,x_n \in G_1 \cup G_2$, $n \geqslant 1$ heißt *alternierend*, wenn gilt:

1) Alle x_i sind ungleich 1,
2) Die benachbarten Faktoren x_i, x_{i+1} liegen nicht in derselben Gruppe G_j.

Das *freie Produkt* $G_1 * G_2$ ist die Menge aller formalen alternierenden Produkte $x_1x_2\dots x_n$, $n \geqslant 1$, zusammen mit 1, bezüglich der natürlichen Multiplikation.

Etwas ausführlicher: Seien $x = g_1\dots g_n$, $y = h_1\dots h_m$, $n, m \geqslant 1$ zwei alternierende Produkte. Dann wird ihr Produkt induktiv definiert:

$$x{\cdot}y = \begin{cases} g_1\dots g_nh_1\dots h_m, & \text{falls } g_n \in G_1, h_1 \in G_2 \text{ oder } g_n \in G_2, h_1 \in G_1, \\ g_1\dots g_{n-1}zh_2\dots h_m, & \text{falls } g_n, h_1 \in G_1 \text{ oder } g_n, h_1 \in G_2 \text{ und } z := g_nh_1 \neq 1, \\ g_1\dots g_{n-1}\cdot h_2\dots h_m, & \text{falls } g_n, h_1 \in G_1 \text{ oder } g_n, h_1 \in G_2 \text{ und } g_nh_1 = 1. \end{cases}$$

Behauptung. Seien G_1, G_2 zwei Untergruppen einer Gruppe G. Wenn jedes Element $g \in G \setminus \{1\}$ eindeutig als alternierendes Produkt $g = g_1g_2\dots g_n$ geschrieben werden kann, dann ist $G \cong G_1 * G_2$.

Beispiel. Sei Γ ein Graph mit Eckpunkten $\Gamma^0 = \mathbb{Z}$ und mit Kanten zwischen z und $z+1$ für $z \in \mathbb{Z}$. Sei a die Spiegelung von Γ um 0 und sei b die Spiegelung von Γ um 1. Wir betrachten die Gruppe $\langle a, b\rangle$, die von a, b in $\mathrm{Aut}(\Gamma)$ erzeugt ist. Dann ist $\langle a, b\rangle \cong \mathbb{Z}_2 * \mathbb{Z}_2$.

Satz 9.2.

1) Die Gruppen G_1 und G_2 sind in das freie Produkt $G_1 * G_2$ eingebettet.
2) Wenn G_1 und G_2 die Präsentationen $\langle X_1 \,|\, R_1\rangle$ und $\langle X_2 \,|\, R_2\rangle$ haben, dann hat ihr freies Produkt $G_1 * G_2$ die Präsentation $\langle X_1 \cup X_2 \,|\, R_1 \cup R_2\rangle$.

9.2. **Amalgamierte Produkte.**

Definition 9.3. Seien G_1 und G_2 zwei Gruppen und seien $A \leqslant G_1$ und $B \leqslant G_2$ zwei isomorphe Untergruppen. Sei $\varphi : A \to B$ ein Isomorphismus. Das *amalgamierte Produkt* von G_1 und G_2 bezüglich $\varphi : A \to B$ ist die Faktorgruppe von

$$G_1 * G_2$$

durch den normalen Abschluss der Menge $\{\varphi(a)a^{-1} \,|\, a \in A\}$ und wird mit

$$G_1 \underset{\substack{A=B \\ \varphi}}{*} G_2$$

bezeichnet.

Bemerkung. Mit der Bezeichnung $N = \langle\langle \{\varphi(a)a^{-1} \mid a \in A\} \rangle\rangle$ gilt also

$$G_1 \underset{\substack{A=B \\ \varphi}}{*} G_2 = \{Ng \mid g \in G_1 * G_2\}.$$

Um die weiteren Bezeichnungen zu vereinfachen, werden wir die Nebenklasse Ng einfach als g schreiben. Mit dieser Schreibweise ist $g = g'$ im amalgamierten Produkt genau dann, wenn $g^{-1}g' \in N$ gilt. Manchmal werden auch nicht vollständige Bezeichnungen $G_1 \underset{A=B}{*} G_2$ und $G_1 \underset{A}{*} G_2$ benutzt.

Satz 9.4. Wenn G_1 und G_2 die Präsentationen $\langle X_1 \mid R_1 \rangle$ und $\langle X_2 \mid R_2 \rangle$ haben, dann hat $G_1 \underset{A=B}{*} G_2$ die Präsentation $\langle X_1 \cup X_2 \mid R_1 \cup R_2, a = \varphi(a)\,(a \in A) \rangle$.

Beispiel. Es gilt $\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{Z}_4 \underset{\mathbb{Z}_2}{*} \mathbb{Z}_6$. Als Erzeuger von $\mathbb{Z}_4$, $\mathbb{Z}_6$ und $\mathbb{Z}_2$ gelten die Matrizen

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = a^2 = b^3.$$

Definition 9.5. Seien G_1, G_2, A, B und φ wie in Definition 9.3.
Sei T_A eine Menge von Repräsentanten der rechten Nebenklassen von A in G_1, so dass der Repräsentant von A gleich 1 ist.
Sei T_B eine Menge von Repräsentanten der rechten Nebenklassen von B in G_2, so dass der Repräsentant von B gleich 1 ist.

Eine *A-Normalform* (bezüglich T_A und T_B) ist eine Folge $(x_0, x_1, \ldots, x_n)$, wobei gilt:

1) $x_0 \in A$,
2) $x_i \in T_A \setminus \{1\}$ oder $x_i \in T_B \setminus \{1\}$ und die benachbarten x_i, x_{i+1} liegen in verschiedenen T_A, T_B.

Analog kann man eine B-Normalform definieren.

Satz 9.6. Sei $G = G_1 \underset{A=B}{*} G_2$ und seien T_A und T_B wie in Def. 9.5. Dann gilt:

1) Jedes Element $g \in G$ kann eindeutig in der Form $g = x_0x_1 \ldots x_n$ geschrieben werden, wobei $(x_0, x_1, \ldots, x_n)$ eine A-Normalform ist.
2) Die Gruppen G_1 und G_2 sind kanonisch in G eingebettet und es gilt $G = \langle G_1, G_2 \rangle$.
3) Ist $g = y_1y_2 \ldots y_n \in G$ ein alternierendes Produkt mit $y_i \in (G_1 \setminus A) \cup (G_2 \setminus B)$ für $i = 1, \ldots, n$, dann ist $g \neq 1$ in G.
4) Es gilt $G_1 \cap G_2 = A = B$ in G.

Beispiel. Seien $G_1 = \langle a \,|\, a^{12} = 1\rangle$ und $G_2 = \langle b \,|\, b^{15} = 1\rangle$. Seien $A = \langle a^4\rangle \leqslant G_1$ und $B = \langle b^5\rangle \leqslant G_2$. Es gilt $A \cong B \cong \mathbb{Z}_3$. Wir betrachten den Isomorphismus $\varphi : A \to B,\ a^4 \mapsto b^5$. Dann hat die Gruppe

$$G = G_1 \underset{A=B}{*} G_2$$

die Präsentation $\langle a, b \,|\, a^{12} = 1, b^{15} = 1, a^4 = b^5\rangle$.

Wir setzen $T_A := \{1, a, a^2, a^3\}$ und $T_B := \{1, b, b^2, b^3, b^4\}$. Jetzt schreiben wir das Element $a^3ba^5 \in G$ in der Form, die im Satz 9.6.1) definiert wurde:

$$a^3ba^5 = a^3ba^4 \cdot a = a^3b^6a = a^3b^5 \cdot ba = a^7ba = a^4 \cdot a^3ba.$$

9.3. **HNN-Erweiterungen.**

Definition 9.7. Sei $G = \langle X \,|\, R\rangle$ eine Gruppe und seien A, B zwei isomorphe Untergruppen von G. Sei $\varphi : A \to B$ ein Isomorphismus. Die *HNN Erweiterung* von G bezüglich A, B, φ ist die Gruppe

$$G^* := \langle X, t \,|\, R,\ t^{-1}at = \varphi(a)\,(a \in A)\rangle.$$

Definition 9.8. Seien G, A, B und φ wie in Definition 9.7.
Sei T_A eine Menge von Repräsentanten der rechten Nebenklassen von A in G, so dass der Repräsentant von A gleich 1 ist,
Sei T_B eine Menge von Repräsentanten der rechten Nebenklassen von B in G, so dass der Repräsentant von B gleich 1 ist.

Eine *Normalform* (bezüglich T_A und T_B) ist eine Folge $(g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n)$, wobei gilt:

1) $g_0, g_1, \ldots, g_n \in G$, $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$,
2) $\varepsilon_i = -1 \Rightarrow g_i \in T_A$,
3) $\varepsilon_i = 1 \Rightarrow g_i \in T_B$,
4) es gibt keine Teilfolge $(t^{\varepsilon}, 1, t^{-\varepsilon})$.

Satz 9.9. Sei G^* die HNN-Erweiterung aus der Definition 9.7 und seien T_A, T_B die Mengen von Repräsentanten aus der Definition 9.8. Dann gilt:

1) Jedes Element $x \in G^*$ kann eindeutig in der Form $x = g_0t^{\varepsilon_1}g_1 \ldots t^{\varepsilon_n}g_n$ geschrieben werden, wobei die Folge $(g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n)$ eine Normalform (bezüglich T_A, T_B) ist.
2) Die Gruppe G ist in die Gruppe G^* eingebettet und es gilt $G^* = \langle G, t\rangle$.
3) Sei $x = z_0t^{\varepsilon_1}z_1 \ldots t^{\varepsilon_n}z_n \in G^*$, wobei gilt:
   a) $n \geqslant 1,\ z_0, z_1, \ldots, z_n \in G$ und $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$,
   b) x hat keine Unterwörter $t^{-1}z_it$ mit $z_i \in A$,
   c) x hat keine Unterwörter tz_it^{-1} mit $z_i \in B$.

Dann ist $x \neq 1$.

Beispiel. Seien $G = F(a,b)$, $A = \langle a^2 \rangle$ und $B = \langle b^3 \rangle$. Es gilt $A \cong B \cong \mathbb{Z}$. Wir betrachten den Isomorphismus $\varphi : A \to B$, $a^2 \mapsto b^3$. Dann ist

$$G^* = \langle a, b, t \,|\, t^{-1}a^2t = b^3 \rangle.$$

Wir setzen

$$T_A := \{w, aw \,|\, w \text{ ist ein Wort in } G, \text{ das nicht mit } a^{\pm 1} \text{ anfängt}\},$$
$$T_B = \{w, bw, b^2w \,|\, w \text{ ist ein Wort in } G, \text{ das nicht mit } b^{\pm 1} \text{ anfängt}\}.$$

Jetzt schreiben wir das Element $x = b^2t^{-1}a^{-4}tb^5abt^{-1}a^4b^3a \in G^*$ in der Form, die im Satz 9.9.1) definiert wurde:

$$x = b^2t^{-1}a^{-4}tb^5ab \cdot b^6t^{-1}b^3a = b^2t^{-1}a^{-4} \cdot a^2tb^2ab^7t^{-1}b^3a = bab^7t^{-1}b^3a.$$

Bemerkung. Die isomorphen Untergruppen A und B von G sind in G möglicherweise nicht konjugiert. In der Obergruppe G^* sind sie schon konjugiert.

Satz 9.10.

1) Sei G ein amalgamiertes Produkt $G = G_1 \underset{A=B}{*} G_2$. Dann ist jede enliche Gruppe von G zu einer der endlichen Untergruppen von G_1 oder G_2 konjugiert.
2) Sei G eine HNN Erweiterung von H. Dann ist jede endliche Gruppe von G zu einer der endlichen Untergruppen von H konjugiert.

10. Einige Beispiele von amalgamierten Produkten und HNN Erweiterungen

Definition 10.1. Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$, d.h. $a, b, c, d \in \mathbb{C}$, $ad - bc = 1$. Die Abbildung

$$\begin{aligned} \mathcal{T}_A : \mathbb{C} \cup \{\infty\} &\to \mathbb{C} \cup \{\infty\} \\ z &\mapsto \frac{az+b}{cz+d} \end{aligned}$$

heißt mit A assoziierte *Möbius-Transformation* von $\mathbb{C} \cup \{\infty\}$. Dabei ist

$$\frac{az+b}{cz+d} := \infty, \text{ falls } cz + d = 0 \text{ ist}$$

und

$$\frac{a\infty + b}{c\infty + d} := \begin{cases} a/c, & \text{falls } c \neq 0 \text{ ist,} \\ \infty, & \text{falls } c = 0 \text{ ist.} \end{cases}$$

Merken wir an:

$$\mathcal{T}_A \circ \mathcal{T}_B = \mathcal{T}_{AB}, \qquad \mathcal{T}_E = id,$$

wobei E die Einheitsmatrix bezeichnet.

Satz 10.2. Es gilt $\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{Z}_4 \underset{\mathbb{Z}_2}{*} \mathbb{Z}_6$. Als Erzeuger von $\mathbb{Z}_4$, $\mathbb{Z}_6$ und $\mathbb{Z}_2$ gelten die Matrizen

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

Beweisskizze. Sei $A^{k_1}B^{\ell_1} \dots A^{k_s}B^{\ell_s} = E$ eine Relation in $\mathrm{SL}_2(\mathbb{Z})$. Wir müssen zeigen, dass diese Relation aus den Relationen $A^4 = E$, $B^6 = E$ und $A^2 = B^3$ folgt.

`Schritt 1.` (Einfache Reduktion) Mit Hilfe der Relationen $A^4 = E$, $B^6 = E$, können wir die Exponenten k_i und ℓ_i reduzieren:

$$k_i \in \{1, 2, 3\}, \quad \ell_i \in \{1, 2, 3, 4, 5\} \quad (i = 1, \dots, s)$$

`Schritt 2.` ("Durchkämmen" von rechts nach links) Mit Hilfe der Relation $A^2 = B^3$ (und, wenn es notwendig ist, den Relationen $A^4 = E$, $B^6 = E$) erhalten wir die Relation

$$A^r \cdot A^{p_1}B^{q_1} \dots A^{p_t}B^{q_t} = E$$

mit

$$r \in \{0, 2\}, \quad p_i \in \{1\}, \quad q_i \in \{1, 2\} \quad (i = 1, \dots, t).$$

Ist $t = 0$, dann muss auch $r = 0$ sein. In diesem Fall sind wir fertig. Sei $t \neq 0$. Wir schreiben die letzte Relation in der Form

$$A^{p_1}B^{q_1} \dots A^{p_t}B^{q_t} = \pm E.$$

In dem Fall erhalten wir einen Widerspruch mit Hilfe des *Ping-Pong*-Arguments:

$$\mathcal{T}_A(\mathbb{R}_+) \subseteq \mathbb{R}_-, \quad \mathcal{T}_B(\mathbb{R}_-) \subseteq \mathbb{R}_+, \quad \mathcal{T}_{B^2}(\mathbb{R}_-) \subseteq \mathbb{R}_+.$$

□

Seien G und G' zwei Gruppen und sei X ein Erzeugendensystem von G. Im Folgenden benötigen wir ein Kriterium, wann eine Abbildung aus X nach G' bis zu einem Homomorphismus aus G nach G' erweitert werden kann. Folgender Satz ist eine Variante dieses Kriteriums für Präsentationen von zwei Gruppen.

Satz 10.3. Seien G und G' zwei Gruppen mit den Präsentationen $\langle X \mid R \rangle$ und $\langle X' \mid R' \rangle$. Jeder Homomorphismus $\varphi : F(X) \to F(X')$ mit der Eigenschaft

$$\varphi(r) \in \langle\langle R' \rangle\rangle_{F(X')}.$$

induziert einen Homomorphismus $\varphi_* : G \to G'$.

Bemerkung. Der Satz 10.3 kann so interpretiert werden: Wenn jede Relation von G unter φ gleich 1 in G' ist, dann bestimmt φ einen Homomorphismus $\varphi_* : G \to G'$.

Definition 10.4. Eine Gruppe G heißt *Hopfsch*, wenn jeder Epimorphismus[4] $\varphi : G \to G$ injektiv ist, also wenn $\ker(\varphi) = 1$ ist.

Satz 10.5. Die Gruppe $G = \langle b, t \mid t^{-1}b^2t = b^3 \rangle$ ist nicht Hopfsch.

Beweis. Wir definieren $\varphi : G \to G$ durch $\varphi(t) = t$ und $\varphi(b) = b^2$. Dann ist φ ein Epimorphismus. Außerdem gilt $[t^{-1}bt, b] \in \ker(\varphi)$ und

$$[t^{-1}bt, b] = t^{-1}b^{-1}tb^{-1}t^{-1}btb \neq 1$$

nach Satz 9.9.3) . □

Definition 10.6. Eine Gruppe G heißt *residuell endlich*, wenn für jedes nichttriviale Element $g \in G$ eine endliche Gruppe K und ein Homomorphismus $\varphi : G \to K$ mit $\varphi(g) \neq 1$ existieren.

Behauptung 10.7.

(1) Jede Untergruppe einer residuell endlichen Gruppe ist residuell endlich.
(2) Eine Gruppe G ist residuell endlich genau dann, wenn eine der zwei äquivalenten Bedingungen erfüllt ist:
   a) Der Schnitt von allen normalen Untergruppen von G von endlichem Index gleich 1 ist.
   b) Der Schnitt von allen Untergruppen von G von endlichem Index gleich 1 ist.

Satz 10.8. Das Wortproblem für eine endlich präsentierbare residuell endliche Gruppe G ist algorithmisch lösbar.

Satz 10.9. Die Gruppe $\mathrm{GL}_n(Z)$ ist residuell endlich.

Satz 10.10. (Mal'cev) Jede endlich erzeugte Untergruppe von $\mathrm{GL}_n(K)$, wobei K ein Körper ist, ist residuell endlich.

Satz 10.11. Jede freie Gruppe ist residuell endlich.

Satz 10.12. Jede endlich erzeugte residuell endliche Gruppe ist Hopfsch.

Folgerung 10.13. Jede endlich erzeugte Untergruppe von $\mathrm{GL}_n(K)$, wobei K ein Körper ist, ist Hopfsch.

Folgerung 10.14. Für jedes $n \in \mathbb{Z}$ ist die Gruppe $\langle b, t \mid t^{-1}bt = b^n \rangle$ Hopfsch.

[4] Epimorphismus = surjektiver Homomorphismus.

11. Einige Einbettungssätze

Sei $\mathrm{Spec}(G)$ die Menge der Ordnungen von Elementen der endlichen Ordnung der Gruppe G.

Satz 11.1. (G. Higman, B. Neumann, H. Neumann) Jede abzählbare Gruppe G kann in eine Gruppe G^* eingebettet werden, so dass folgende Eigenschaften erfüllt sind.

1) G^* ist erzeugt von zwei Elementen der unendlichen Ordnung.

2) $\mathrm{Spec}(G) = \mathrm{Spec}(G^*)$.

3) Wenn G endlich präsentierbar ist, dann ist G^* ebenso endlich präsentierbar.

Folgerung 11.2. (B. Neumann) Es existieren $2^{\aleph_0}$ paarweise nicht isomorphe 2-erzeugte Gruppen.

Satz 11.3. (G. Higman, B. Neumann, H. Neumann) Jede aufzählbare Gruppe G kann in eine aufzählbare Gruppe G^* eingebettet werden, so dass je zwei Elemente von G^* mit der gleichen Ordnung in G^* konjugiert sind.

Satz 11.4. Jede aufzählbare Gruppe G kann in eine aufzählbare einfache und teilbare Gruppe G^* eingebettet werden.

Beweis. Sei $K = (\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \dots) * \langle x \,|\, \rangle$. Wir betrachten die Einbettungen

$$G \hookrightarrow G * K \hookrightarrow U = \langle u_1, u_2 \rangle \hookrightarrow G^*,$$

wobei die Ordnungen von u_1, u_2 unendlich sind, G^* abzählbar ist und alle Elemente der gleichen Ordnung in G^* konjugiert sind.

Sei $1 \neq N$ eine normale Untergruppe von G^* und sei $1 \neq z \in N$ ein Element.

- Hat z die unendliche Ordnung, dann ist z zu jedem Element u_1 und u_2 konjugiert. In diesem Fall ist $U \leqslant N$.

- Hat z eine endliche Ordnung, dann ist z zu einem Element $y \in \langle \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \dots)$ konjugiert. Dann ist $y \in N$ und auch $[y, x] \in N$. Da $[y, x]$ die unendliche Ordnung hat, gilt $U \leqslant N$ wie oben. Aber U besitzt Elemente aller möglichen Ordnungen. Deswegen gilt $N = G^*$. □

12. Weitere Einbettungssäte von Higman

Definition 12.1. Sei $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$ ein endliches Alphabet. Wir kodieren alle Worte im Alphabet $\mathcal{A} \cup \mathcal{A}^{-1}$ mit natürlichen Zahlen wie folgt:

Sei $w = x_1 x_2 \dots x_m$ ein Wort mit $x_i \in \mathcal{A} \cup \mathcal{A}^{-1}$, $i = 1, \dots, m$. Dieses Wort wird kodiert mit der Zahl $p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, wobei $p_1, p_2, \dots$ die Folge aller Primzahlen ist und

$$k_i = \begin{cases} 2j, & \text{falls } x_i = a_j \\ 2j-1, & \text{falls } x_i = a_j^{-1} \end{cases}$$

gilt, $i = 1, \ldots, m$. Wir bezeichnen diese Zahl mit $\varphi(w)$. Eine Präsentation $\langle \mathcal{A} \,|\, \mathcal{R} \rangle$ heißt *rekursiv präsentierbar*, falls die Menge der Zahlen $\{\varphi(r) \,|\, r \in \mathcal{R}\}$ rekursiv aufzählbar ist.

Satz 12.2. (Einbettungssatz von Higman) Eine endlich erzeugte Gruppe G kann eingebettet werden in eine endlich präsentierbare Gruppe G^* genau dann, wenn G rekursiv präsentierbar ist.

Satz 12.3. (Higman) Es existiert eine endlich präsentierbare Gruppe G, so dass jede rekursiv präsentierbare Gruppe H in G eingebettet werden kann.

Satz 12.4. (Novikov und Boone) Es existiert eine endlich präsentierte Gruppe mit unlösbarem Wortproblem.

Beweis. Sei $S \subset \mathbb{N}$ eine rekursiv aufzählbare aber nicht rekursive Menge. Wir betrachten die Gruppe

$$G = \langle a, b, c, d \,|\, a^{-i}ba^i = c^{-i}dc^i \,(i \in S) \rangle.$$

Merken wir an, dass $a^{-i}ba^i = c^{-i}dc^i$ in G genau dann gilt, wenn $i \in S$ ist. Da S nicht rekursiv ist, ist es unentscheidbar, ob i in S liegt, oder nicht. Somit ist das Wortproblem in G unentscheidbar. Nach Satz 12.2 kann G in eine endlich präsentierte Gruppe G^* eingebettet werden. Offensichtlich ist das Wortproblem in G^* unlösbar. □

13. Der Satz von Adian und Rabin

Definition 13.1. Eine Eigenschaft P von endlich präsentierbaren Gruppen heißt *Markov-Eigenschaft*, falls sie unter Isomorphismen erhalten wird und folgende zwei Bedingungen erfüllt sind:
1) Es existiert eine endlich präsentierbare Gruppe G_1 mit der Eigenschaft P.
2) Es existiert eine endlich präsentierbare Gruppe G_2, die in keine endlich präsentierbare Gruppe mit der Eigenschaft P eingebettet werden kann.

Satz 13.2. (Adian und Rabin) Ist P eine Markov-Eigenschaft von endlich präsentierbaren Gruppen, dann existiert kein Algorithmus, der für endliche Präsentationen von Gruppen entscheidet, ob die entsprechenden Gruppen die Eigenschaft P haben.

Beweis. Sei H eine endlich präsentierte Gruppe mit unlösbarem Wortproblem. Seien G_1 und G_2 zwei endlich präsentierte Gruppe aus Definition 13.1.

Zuerst betten wir die Gruppe $G_2 * H * \langle x \,|\, \rangle$ in eine Gruppe U, die von 2 Erzeugern u_1, u_2 der unendlichen Ordnung erzeugt ist. Wir betrachten zwei

weitere Einbettungen:

$$\begin{aligned} & G_2 * H * \langle x \,|\, \rangle \\ \hookrightarrow\ & U = \langle u_1, u_2 \rangle \\ \hookrightarrow\ & J = \langle U, y_1, y_2 \,|\, y_1^{-1} u_1 y_1 = u_1^2, y_2^{-1} u_2 y_2 = u_2^2 \rangle \\ \hookrightarrow\ & K = \langle J, z \,|\, z^{-1} y_1 z = y_1^2, z^{-1} y_2 z = y_2^2 \rangle. \end{aligned}$$

Sei

$$Q = \langle r, s, t \,|\, s^{-1} r s = r^2,\ t^{-1} s t = s^2 \rangle.$$

Mit jedem Element $w \in H$ assoziieren wir die Gruppe

$$D_w = \langle K * Q \,|\, r = z, t = [w, x] \rangle.$$

Behauptung 1. Es gelten folgende Aussagen.

(a) $\langle r, t \rangle_Q \cong F_2$.
(b) Ist $w \neq 1$ in H, dann gilt $\langle z, [w, x] \rangle_K \cong F_2$.
(c) Ist $w \neq 1$ in H, dann gilt $K \hookrightarrow D_w$.

Nun bilden wir die Gruppe

$$E_w = D_w * G_1.$$

Behauptung 2. Es gelten folgende Aussagen.

(a) Ist $w \neq 1$ in H, dann gilt $G_2 \hookrightarrow D_w \hookrightarrow E_w$, und deswegen besitzt E_w die Eigenschaft P nicht.
(b) Ist $w = 1$ in H, dann gilt $D_w = 1$ und $E_w = G_1$, und deswegen besitzt E_w die Eigenschaft P.

Da das Wortproblem in H unlösbar ist, ist die Eigenschaft P in der Klasse von endlich präsentierten Gruppen unlösbar.

□