# Das Dehnsche Wortproblem

Philipp Hauchwitz

11. Juni 2025

> Irgend ein Element der Gruppe ist durch seine Zusammensetzung aus den Erzeugenden gegeben. Man soll eine Methode angeben, um mit einer endlichen Anzahl von Schritten zu entscheiden, ob dies Objekt der Identität gleich ist oder nicht.
>
> (Max Dehn)

## 1 Normalformen

### 1.1 Definition

Sei $G$ eine Gruppe, $S' \subseteq G$ ein Erzeugendensystem, $S$ eine Kopie von $S'$ und sei $S^{-1}$ eine gleichmächtige Menge, sodass die Elemente von $S^{-1}$ formal die Inversen zu den Elementen von S seien. Sei weiter eine Funktion $\pi : \{S \cup S^{-1}\}^* \to G$ gegeben, die jedes $s \in S$ auf den zugehörigen Erzeuger von G, sowie $s^{-1} \in S^{-1}$ auf das jeweilige Inverse abbildet. Somit wird jedes Wort $w \in \{S \cup S^{-1}\}^*$ auf das korrespondierende Produkt aus den Erzeugenden und ihrer Inversen abgebildet. Da $S'$ $G$ erzeugt, ist $\pi$ offenbar surjektiv. Für eine bessere Unterscheidung sei, sofern nicht explizit anders definiert, w eine Zeichenkette in $\{S \cup S^{-1}\}^*$ und $\pi(w)$ ein Element der Gruppe.

Bsp: Sei $G = \mathbb{Z} \oplus \mathbb{Z}$ und $S' = \{a, b\}$, $a = (1, 0) \in \mathbb{Z} \oplus \mathbb{Z}$ und $b = (0, 1) \in \mathbb{Z} \oplus \mathbb{Z}$. Dann sind $w_1 = aba^{-1}bbba$ und $w_2 = bbabb$ verschiedene Elemente von $\{a, b, a^{-1}, b^{-1}\}$, während $\pi(w_1) = \pi(w_2) = (1, 4) \in \mathbb{Z} \oplus \mathbb{Z}$.

Damit wir nicht mehrere Schreibweisen für ein Element erhalten, wollen wir die Normalform definieren. Sei eine Funktion $\eta : G \to \{S \cup S^{-1}\}^*$ gegeben, sodass $\pi \circ \eta : G \to G$ die Identität darstellt und $\pi|_{Bild(\eta)}$ bijektiv ist. Dann nennt man $Bild(\eta) \subseteq \{S \cup S^{-1}\}^*$ eine Normalform.

### 1.2 Bsp

(1) Für eine freie Gruppe sind genau die reduzierten Wörter (in W) eine Normalform.
(2) Sei $G = \mathbb{Z} \oplus \mathbb{Z}$ die freie abelsche Gruppe mit erzeugenden $\{a, b\}$ wie zuvor. Dann lassen sich mehrere Normalformen bilden:

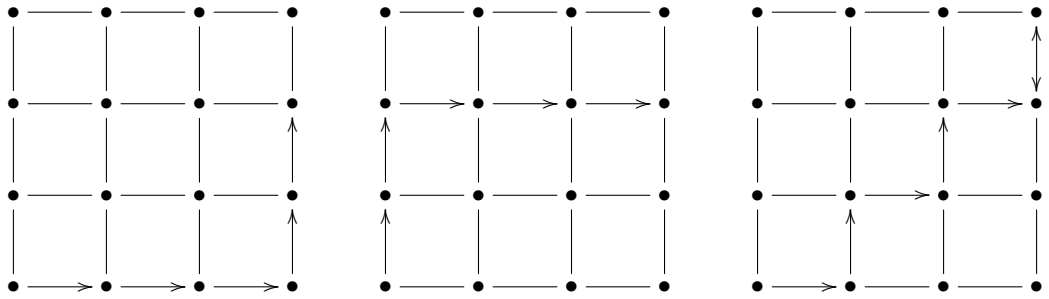
$$NF_1 = \{a^i b^j | i, j \in \mathbb{Z}\} \tag{1}$$

$$NF_2 = \{b^i a^j | i, j \in \mathbb{Z}\} \tag{2}$$

$$NF_3 = \{(ab)^i b^j | i, j \in \mathbb{Z}\} \tag{3}$$

Das Element $a^3b^2$ in den drei Normalformen sieht also wie folgt aus: $NF_1 : a^3b^2, NF_2 : b^2a^3, NF_3 : (ab)^3b^{-1}$. siehe unten für eine Visualisierung der Betrachtungsweise als Pfade des Cayley-Graphen.

Bem: In einer anderen Betrachtungsweise lassen sich Normalformen als eine Sammlung an Pfaden in einem Cayley-Graphen verstehen, wobei jeweils, ausgehend vom Knoten, der zur Identität gehört, zum Knoten eines Elements aus der Gruppe, die Kante des nächsten erzeugenden in der Zeichenkette unter $\eta$ durchlaufen wird.

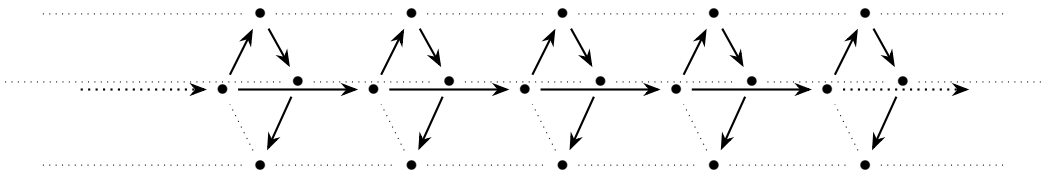


$NF_1$ $NF_2$ $NF_3$

Bem: Manchmal wird eine solche Betrachtung einer Normalform auch als combing, also Kämmung, eines Graphen bezeichnet. Dies ergibt zumindest für einige Normalformen Sinn, sofern diese gewisse geometrische und oder sprachtheoretische Eigenschaften erfüllen.

## 1.3 Bsp

(1) Betrachte die Gruppe $G = \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ mit Normalform $N = \{x^i y^j | i \in \mathbb{Z}, 0 \leq j \leq 3\}$, wobei $x = (1, 0)$ und $y = (0, 1)$.



Gekämmter Cayley-Graph von $\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$

Wdh: Allgemein gilt $BS(m, n) =< a, b|ab^m a^{-1} = b^n >$ und in einem vorherigen Kapitel des Buchs wurde gezeigt, dass jedes Element in $BS(1, 2)$ sich in der Form $W = \{a^{-k}b^m a^{k+n}|k, m, n \in \mathbb{Z}\}$ schreiben lässt. Wir wollen uns nun die Frage stellen ob dies eine Normalform ist und falls nicht ob wir hieraus eine Normalform bilden können.
Man findet relativ schnell die Elemente $w_1 = aba^{-1}$ und $w_2 = b^2$, welche in W unterschiedlich, allerdings in BS(1,2) gleich sind. Folglich ist W keine Normalform.

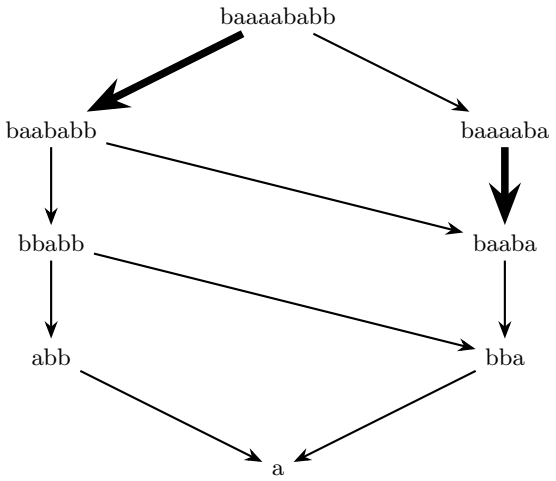
## 1.4 Lemma

Die Menge $NF = \{a^{-k}b^{2m+1}a^{k+n}|k, m, n \in \mathbb{Z}\} \cup \{a^n|n \in \mathbb{Z}\}$ ist eine Normalform von $BS(1, 2)$.

*Beweis.* Es ist bekannt (auch aus dem vorherigen Kapitel), dass sich $g \in BS(1, 2)$ als lineare Funktion verstehen lässt: $g(x) = 2^n x + \frac{\hat{m}}{2^k}$. Nach Kürzung dürfen wir annehmen, dass $\hat{m}$ entweder ungerade oder 0 ist. Somit kann man g in der Form $g(x) = 2^n x + \frac{2m+1}{2^k}$ oder $g(x) = 2^n x$ darstellen. Die Wörter der Form $\{a^{-k}b^{2m+1}a^{k+n}|k, n, m \in \mathbb{Z}\}$ beschreiben die Funktionen der Form $g(x) = 2^n x + \frac{2m+1}{2^k}$ und die Wörter der Form $\{a^n|n \in \mathbb{Z}\}$ liefern die Form $g(x) = 2^n x$. Somit bildet die NF unter $\pi$ surjektiv auf BS(1,2) ab. Um Injektivität zu zeigen, wollen wir eine Widerspruchsannahme machen:
Es existieren k,n,m,K,N,M $\in \mathbb{Z}$, sodass $a^{-k}b^{2m+1}a^{k+n} = a^{-K}b^{2M+1}a^{K+N}$ und mindestens eine Ungleichheit von $k \neq K$, $n \neq N$ und $m \neq M$ gilt.
Der linke Teil der Gleichung bildet, betrachtet als Funktion, wie folgt ab: $[0, 1] \mapsto [\frac{m}{2^k}, \frac{2m+1}{2^k} + 2^n]$, während der rechte Teil als Funktion so abbildet: $[0, 1] \mapsto [\frac{M}{2^K}, \frac{2m+1}{2^K} + 2^N]$. Daraus folgt $\frac{2m+1}{2^k} = \frac{2M+1}{2^K}$ und $2^n = 2^N$. Somit gilt $m = M$, $k = K$ und $n = N$, was einen Widerspruch zur Annahme darstellt. Die selbe Argumentation liefert, dass kein Ausdruck der Form $a^{-k}b^{2m+1}a^{k+n}$ eine Funktion der Form $g(x) = 2^n x$ induzieren kann. Somit ist NF eine Normalform für BS(1,2). □

# 2 Das Wortproblem

Wie eingangs formuliert, geht es beim Wortproblem darum, bei einer endlich erzeugten Gruppe entscheiden zu können, ob ein beliebiges Element der Wortmenge in der Gruppe gleich der Identität ist oder nicht. Zum Einstieg wollen wir zunächst zwei Beispiele betrachten:
(1) Für $\mathbb{Z} \oplus \mathbb{Z}$ ist das Wortproblem sehr leicht lösbar, indem man Erzeugende wählt, sich klar macht, wann diese in $\mathbb{Z} \oplus \mathbb{Z}$ gleich Null werden und dann die Erzeugenden eines Wortes abzählt. In dem vorher betrachteten Beispiel ergibt dies, dass das Wort genau dann die Identität ist, wenn die Summen beider Exponenten Null sind.
(2) Ein leicht schwieriger Fall ist die unendliche Diedergruppe $D_\infty$. Aus vorherigen Vorträgen ist bekannt, dass $D_\infty =< a, b|a^2 = b^2 = 1 >$. Wir betrachten also Wörter in $\{a, b\}^*$. Mit der folgenden Regel lässt sich das Problem dann lösen: Falls ein Wort $w \in \{a, b\}^*$ ein Teilwort der Form aa oder bb enthält, entferne dieses Teilwort, um ein neues Wort $w'$ zu erhalten.
Da betrachtete Worte endliche Länge haben und $\pi(w) = \pi(w')$, bleiben alle resultierenden Worte in $D_\infty$ dasselbe Wort und es genügt zu entscheiden, ob das letzte Wort das leere Wort ist, oder ob es eine beliebig lange abwechselnde Folge von a und b ist. Hierbei gibt es offenbar verschiedene Wahlmöglichkeiten zur Entfernung von Teilwörtern, da alle resultierenden Wörter unter $\pi$ jedoch äquivalent zu $w$ bleiben, ist die Wahl des Teilwortes irrelevant.




Entscheidungsmöglichkeiten bei dieser Regel zum Wort baaaababb
Die dickeren Pfeile bedeuten, dass es für den Weg mehrere Möglichkeiten gibt

Neben dem ursprünglichen Wortproblem gibt es noch eine weitere Version des Wortproblems, wobei nicht gefragt ist, ob ein Wort gleich der Identität ist,sondern ob zwei Worte
$w_1, w_2 \in \{S \cup S^{-1}\}^*$ gleich unter $\pi$ sind, also $\pi(w_1) = \pi(w_2)$ gilt. Diese Version wird auch als Identitätsproblem bezeichnet.

## 2.1 Satz

Sei G eine Gruppe und S ein endliches Erzeugendensystem. Dann ist das Wortproblem ist lösbar genau dann, wenn das Identitätsproblem lösbar ist.

*Beweis.* " $\Rightarrow$ ": Es seien zwei Wörter $w_1, w_2 \in \{S \cup S^{-1}\}^*$ gegeben. Falls diese gleich sind, muss $\pi(w_1 w_2^{-1}) = e$ gelten. Also folgt aus der Lösbarkeit des Wortproblems die Lösbarkeit des Identitätsproblems.
" $\Leftarrow$ ": Da das leere Wort immer die Identität ist, lässt sich zu jedem Wort entscheiden, ob es gleich der Identität ist, was genau die Lösbarkeit des Wortproblems ist. □

## 2.2 Resultat ohne Beweis

Es gibt endlich präsentierbare Gruppen, sodass kein Algorithmus existiert, der entscheiden kann, ob ein Element der Wortmenge:
1. die Identität ist.
2. im Zentrum von G liegt.

3. ein Element von endlicher Ordnung ist.

# 3 Das Wortproblem und Cayley-Graphen

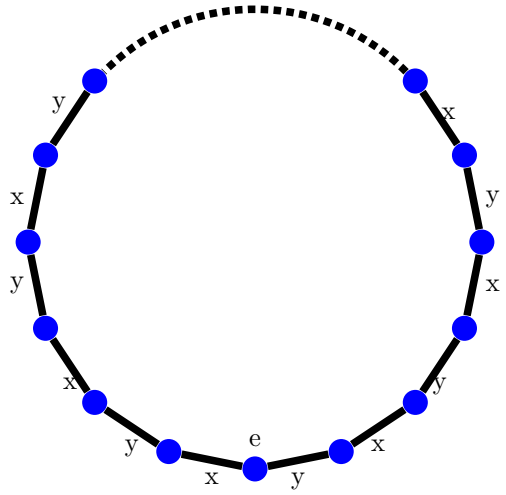
Mit dem, was wir bereits über Cayley-Graphen und das Wortproblem wissen, wollen wir jetzt einen Zusammenhang zwischen beidem herstellen.

## 3.1 Ziel

Sei G eine endlich erzeugte Gruppe mit Erzeugendensystem S. Dann lässt sich das Wortproblem lösen genau dann, wenn sich entscheiden lässt, welche Wörter $w$ einen geschlossenen Pfad $p_w$ im Cayley-Graphen $\Gamma_{G,S}$ implizieren.

## 3.2 Bsp

Für $D_{2n}$, mit $D_{2n} =< x, y | x^2 = y^2 = (xy)^n = 1 >$, lässt sich das Wortproblem lösen. Ein Wort $w$ entspricht der Identität genau dann, wenn der Pfad $p_w$ am Knoten der Identität endet.




Cayley-Graph zu $D_{2n}$ für die Erzeuger wie oben

Um dies zu verallgemeinern, müssen wir zunächst Cayley-Graphen genauer verstehen.

## 3.3 Definition

Sei $\Gamma$ ein zusammenhängender Graph. Bezeichne die Knotenmenge des Graphen mit $V(\Gamma)$. Der Abstand eines Knotens $v$ zu einem Knoten $w$ ist die minimale Anzahl an Kanten, die für einen verbindenden Pfad benötigt werden. Wir schreiben hierfür $d_\Gamma(v, w)$. Für einen bestimmten Knoten $v \in V(\Gamma)$ und ein $n \in \mathbb{N}$ ist die Sphäre mit Radius $n$ um $v$ die Menge der Knoten

$$S(v, n) = \{w \in V(\Gamma) | d_\Gamma(v, w) = n\} \subseteq V(\Gamma) \tag{4}$$

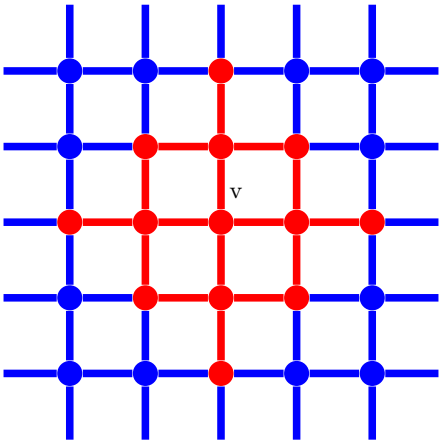
Weiter ist die Kugel mit Radius n, der Teilgraph, der aus der Vereinigung aller Knoten und Kanten von Pfaden in $\Gamma$ mit Länge $\leq n$ und Startpunkt v erzeugt wird. Wir schreiben für den Ball

$$B(v, n) = \bigcup_{|w| \leq n} \bigcup_{x \in p_w} x \subseteq \Gamma \tag{5}$$

Für den Graphen zu einer Gruppe G schreibe auch $S(g, n)$ und $B(g, n)$ für den Knoten zu einem Element $g \in G$. Ein Cayley-Graph heißt konstruierbar, falls für $n \in \mathbb{N}$, $B(e, n)$ in endlich vielen Schritten erzeugt werden kann.

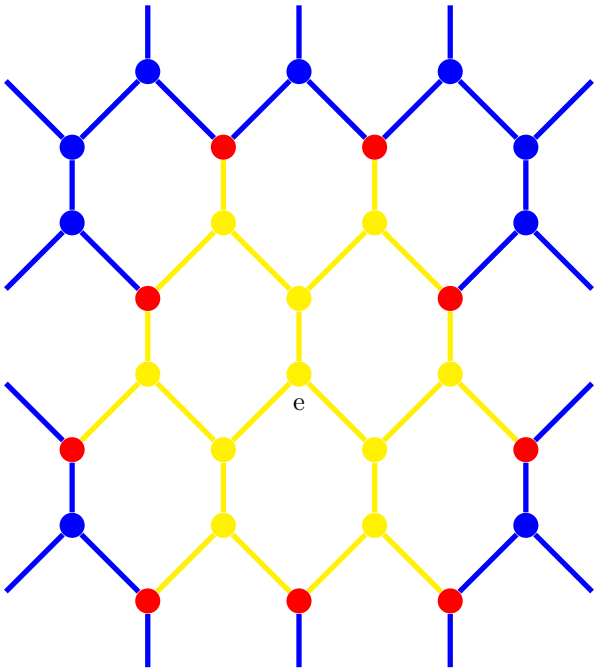
## 3.4 Beispiele

(1) Seien $\Gamma$ ein Graph und $v, w \in V(\Gamma)$ zwei Knoten, die durch eine Kante verbunden sind. Dann ist $d_\Gamma(v, w) = 1$.
(2) Sei $G = \mathbb{Z} \oplus \mathbb{Z}$, $\Gamma_G$ der Cayley-Graph zu G und $v \in V(\Gamma_G)$.




Ausschnitt aus $\Gamma_G$
$B(v, 2)$ in rot

(3) Sei $G = W_{333}$, $\Gamma_{W_{333}}$ der zugehörige Cayley-Graph und $e \in V(\Gamma_G)$ der Knoten, der die Identität in G repräsentiert.




Ausschnitt aus $\Gamma_{W_{333}}$ mit
$S(e, 3)$ in rot und $B(e, 3)$ in gelb und rot

## 3.5 Theorem

Sei G eine endlich erzeugte Gruppe mit endlichem Erzeugendensystem S. Das Wortproblem ist für G lösbar genau dann, wenn der Cayley-Graph $\Gamma_{G,S}$ konstruierbar ist.

*Beweis.* " $\Leftarrow$ ": Sei $w \in \{S \cup S^{-1}\}^*$ und sei $|w| = n$. Konstruiere den Teilgraph $B(e, n) \subseteq \Gamma_{G,S}$ und folge dem Pfad $p_w$ innerhalb dieser Kugel. Der Endknoten dieses Pfads ist $v_e$ genau dann, wenn $\pi(w) = e$. Somit lässt sich das Wortproblem lösen.
" $\Rightarrow$ ": Zeige per Induktion nach n, dass B(e,n) konstruierbar ist. Der Fall B(e,0) ist sofort klar,

da B(e,0) nur der zur Identität assoziierte Knoten ist.
Sei nun B(e,n) konstruierbar und $|S \cup S^{-1}| = k$. Jeder Knoten in $\Gamma_{G,S}$ ist mit exakt k Knoten verbunden. Falls $v \in B(e, n-1)$, so muss v in $B(e,n)$ bereits mit k Kanten verbunden sein. Falls $d_{\Gamma_{G,S}}(v_e, v) = n$, bezeichne mit $L_n(v)$ die Teilmenge von $S \cup S^{-1}$, zu denen korrespondierenden Kanten bereits in $B(e,n)$ mit $v$ verbunden sind. Bei der Konstruktion von $B(e, n+1)$ müssen wir also zu jedem $s \in (S \cup S^{-1}) \setminus L_n(v)$ jeweils eine Kante zu $v$ hinzufügen. Hierfür müssen wir wissen, welcher Knoten am anderen Ende dieser Kante ist. Offenbar kann keiner der fehlenden Kanten $v$ mit einem Knoten in $B(e, n-1)$ verbinden, da sonst die Kante bereits Teil von $B(e,n)$ wäre. Weiter benötigen wir für die Konstruktion eine beliebige Sortierung von $S(e,n)$. Nummeriere also $S(e,n) = \{v_1, \ldots, v_m\}, m \in \mathbb{N}$ beliebig und wähle zu jedem Element $v_i \in S(e,n), 1 \leq i \leq m$ ein Wort $w_i \in \{S \cup S^{-1}\}^*$, mit $|w_i| = n$, sodass der Pfad $p_{w_i}$ in $B(e,n)$ vom Knoten der Identität zu $v_i$ führt. Beginnend mit $v_1$ wollen wir nun $B(e, n+1)$ konstruieren. Wie bereits erwähnt benötigen wir hierfür $|(S \cup S^{-1}) \setminus L_n(v_1)| = l_1 \in \mathbb{N}$ neue Kanten, die wir mit $\hat{s_1}, \ldots, \hat{s_{l_1}}$ bezeichnen wollen, wobei sich $\hat{s_i}$ jeweils eindeutig zu einem Element $s_i \in S \cup S^{-1}$ zuordnen lässt. Da wir bereits wissen, dass $\hat{s_i}$ $v_1$ nicht mit Knoten aus $B(e, n-1)$ verbinden kann, bleiben noch Knoten aus $S(e,n) \setminus \{v_1\}$ oder Kanten aus $\Gamma_{G,S}$, die nicht Teil von $B(e,n)$ sind. Der Fall, dass $v_1$ mit $v_j \in S(e,n) \setminus \{v_1\}$ verbunden wird, tritt genau dann auf, wenn $\pi(w_1 s_i w_j^{-1}) = e$. Da das Wortproblem für G lösbar ist, lässt sich diese Bedingung prüfen. Sofern $\pi(w_1 s_i w_j^{-1}) \neq e$ für alle j, so verbindet $\hat{s_i}$ $v_1$ mit einem neuen Knoten, der nicht schon Teil von $B(e,n)$ war.
Sei nun $i > 1$ und $\hat{s_j}$ eine fehlende Kante zum Knoten $v_i \in S(e,n)$. Dann verbindet $\hat{s_j}$ $v_i$ in $\Gamma_{G,S}$ mit einem der folgenden Knoten:

1. $v_k \in S(e,n)$
2. Ein Knoten in $S(e, n+1)$, der bereits mit einem $v_j, j < i$ verbunden ist
3. Ein Knoten in $S(e, n+1)$, der nicht bereits mit einem Knoten aus $\{v_1, \ldots, v_{i-1}\} \subseteq S(e,n)$ verknüpft ist

Für den ersten Fall prüfe iterativ, ob wie bei $v_1$ gilt, dass $\pi(w_i s_j w_k^{-1}) = e$. Wenn dies nicht der Fall ist, prüfe nach dem 2. Fall, indem man für alle bereits bekannten Knoten aus $S(e, n+1)$ überprüft, ob $\pi(w_i s_j (w_m s_n)^{-1}) = e$ für einen Knoten $v_m$, der mit der Kante $\hat{s_n}$ mit diesem Knoten verbunden ist. Falls diese Gleichheit für keinen der bereits bekannten Knoten gilt, so liegt Fall 3 vor. Da wegen der endlichen Erzeugtheit von G dieser Prozess nach einer endlichen Anzahl von Schritten endet, ist $B(e, n+1)$ konstruierbar. □