Allgemeine Termersetzungssysteme

Seminar: "Gruppentheorie und Kryptographie"
Veranstaltet von: M. Kreuzer und G. Rosenberger
1.Vortrag: Christian Christensen am 15.10.2003

1.1 Notation

Sei M eine beliebige Menge, x, y, z ∈ M.

- $\longrightarrow$ ist eine Relation auf der Menge M
- id ist die Identität, $id = \{\langle x|x\rangle \mid x \in M\}$
- • ist die Verknüpfung zweier Relationen:
  $\longrightarrow_a \bullet \longrightarrow_b = \{\langle x|x\rangle \mid \exists z : x \longrightarrow_a z \wedge y \longrightarrow_b z\}$
- $\longrightarrow^{-1}$ ist die Inverse Relation von $\longrightarrow$: $\longrightarrow^{-1} = \{\langle x|y\rangle \mid y \longrightarrow x\}$

1.2 Definition

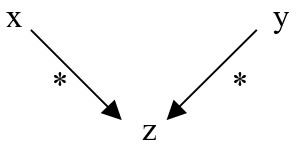
- $\xrightarrow{0} = id$	identische Relation, $\{\langle x|x\rangle \mid x \in M\}$
- $\xrightarrow{M} = \longrightarrow \bigcup id$	Reflexiver Abschluss von $\longrightarrow$
- $\xrightarrow{i} = \longrightarrow \bullet \xrightarrow{i-1}$	∀i > 0, i-fache Ausführung von $\longrightarrow$
- $\xrightarrow{+} = \bigcup_{i>0} \xrightarrow{i}$	Transitiver Abschluss von $\longrightarrow$
- $\xrightarrow{*} = \xrightarrow{+} \bigcup id$	Transitiver - reflexiver Abschluss von $\longrightarrow$
- $\longleftrightarrow = \longrightarrow \bigcup \longrightarrow^{-1}$	Symmetrischer Abschluss von $\longrightarrow$
- $\xleftrightarrow{\wedge *} = \xrightarrow{*} \bigcup \xrightarrow{*}^{-1}$	Symmetrischer, transitiver und reflexiver Abschluss von $\longrightarrow$, dass heißt $\xleftrightarrow{*}$ ist eine Äquivalenzrelation

1.3 Definition

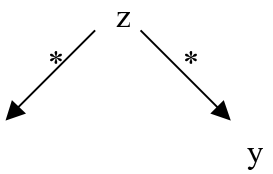
Wenn x minimal in Beziehung auf die Relation $\longrightarrow$ ist, das heißt, es existiert kein y ∈ M mit x$\longrightarrow$y, dann wird x irrreduzibles Element genannt. Die Menge aller irrreduziblen Elemente wird mit N bezeichnet.
Wenn für x ein Element y ∈ N existiert, so dass x$\xrightarrow{*}$y gilt, dann wird y irrreduzibler Teil von x genannt.

1.4 Definition

- $x \downarrow y \Leftrightarrow \exists z : x \xrightarrow{*} z \wedge y \xrightarrow{*} z$



- $x \uparrow y \Leftrightarrow \exists z : z \xrightarrow{*} x \wedge z \xrightarrow{*} y$



- $\Delta(x) = \{y \mid x \longrightarrow y\}$ (Alle direkten Nachfolger von x)
- $\Delta^+(x) = \{y \mid x \xrightarrow{+} y\}$ (Alle möglichen Nachfolger von x)

1.5 Definition

(i) Die Relation $\longrightarrow$ wird induktiv genannt, wenn für jede Folge $x_1 \longrightarrow x_2 \longrightarrow \cdots \longrightarrow x_n \longrightarrow \cdots$ ein y ∈ M existiert, so dass gilt: $\forall i \geq 1 : x_i \xrightarrow{*} y$

(ii) Die Relation $\longrightarrow$ wird azyklisch genannt, wenn $\xrightarrow{+}$ irreflexsiv ist, das heißt $\langle x | x \rangle \notin \xrightarrow{+}$ für $\forall x \in M$.

(iii) Die Relation $\longrightarrow$ wird noether'sch genannt, wenn es keine unendliche Folge $x_1 \longrightarrow x_2 \longrightarrow \cdots \longrightarrow x_n \longrightarrow \cdots$ gibt.

1.6 Bemerkung

Wenn die Relation $\longrightarrow$ noether'sch ist, dann hat jedes Element in M einen irrreduziblen Teil in M, der nicht eindeutig bestimmt sein muss.

Beweis:
Folgt direkt aus der Definition 1.5 (iii).

q.e.d.

1.7 Proposition

Wenn die Relation $\longrightarrow$ noether'sch ist, dann ist sie auch induktiv und azyklisch.

Beweis:
Folgt direkt aus der Definition 1.5.

q.e.d.

1.8 Definition

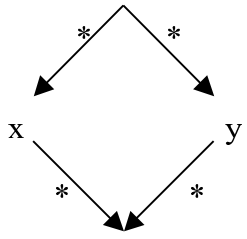
Sei P eine Teilmenge von M. Wir sagen P ist vollständig bezüglich der Relation $\longrightarrow$, wenn $\forall x \in M : [\forall y \in \Delta^+(x) : y \in P] \Rightarrow x \in P$. Dass heißt, wenn alle möglichen Nachfolger von x Elemente der Menge P sind, dann ist auch x Element der Menge P.

1.9 Prinzip der noether'schen Induktion

Wenn $\longrightarrow$ eine noether'sche Relation und P eine vollständige Teilmenge von M bezüglich $\longrightarrow$ ist, dann gilt: M = P.

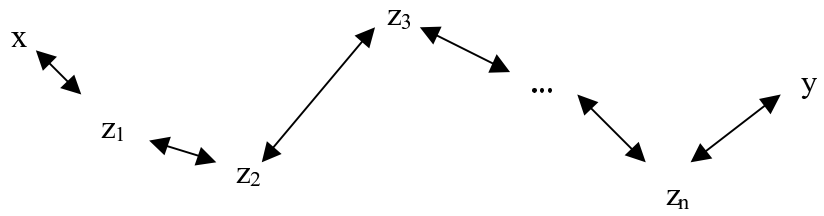
1.10 Definition

Die Relation $\longrightarrow$ wird konfluent genannt, wenn $\forall x, y \in M : x \uparrow y \Rightarrow x \downarrow y$.



1.11 Lemma
Genau dann, wenn die Relation $\longrightarrow$ konfluent ist, erfüllt sie „Church-Rosser“, das heißt: $\forall x, y \in M : x \overset{*}{\longleftrightarrow} y \Leftrightarrow x \downarrow y$.

Beweis:
Mit Induktion über n bei $x \overset{n}{\longleftrightarrow} y$ (immer paarweise einen Nachfolger bestimmen).



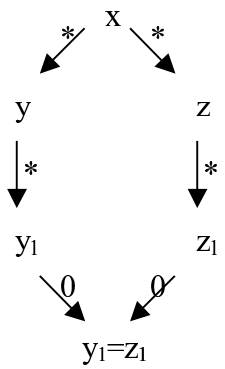
q.e.d.

1.12 Lemma
Wenn die Relation $\longrightarrow$ konfluent ist, dann ist der irrreduzible Teil y eines Elementes x, sofern er existiert, eindeutig bestimmt.

Beweis:
Annahme:
x besitzt zwei irrreduzible Teile $y \neq z$. Dann haben Aufgrund der Konfluenz der Relation $\longrightarrow$ y und z einen gemeinsamen Nachfolger. Dieses ist ein Widerspruch zur Irrreduzibilität von y und z und zu der Annahme, das $y \neq z$.

q.e.d.

1.13 Lemma
Wenn zu jedem Element x ∈ M eine eindeutige Normalform existiert, dann ist die Relation $\longrightarrow$ konfluent.
Beweis:
x habe zwei Nachfolger y und z mit ihren jeweiligen eindeutig bestimmten Normalformen y_1 bzw. z_1. Dann muss, da x eine eindeutige Normalform besitzt $y_1=z_1$ gelten. Somit haben x, y und z die gleiche Normalform und die Relation ist konfluent.

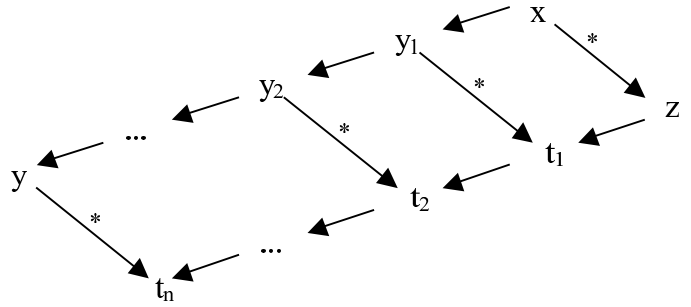


q.e.d.

Bemerkung
Lemma 1.13 ist die Umkehrung von Lemma 1.12 mit der Zusatzbedingung, dass eine eindeutige Normalform existieren muss.

1.14 Lemma
Die Relation $\longrightarrow$ ist konfluent, wenn $\forall x, y \in M : (x \longrightarrow y \wedge x \overset{*}{\longrightarrow} z) \Rightarrow y \downarrow z$.

Beweis:
Mit Induktion über n bei $x \overset{n}{\longrightarrow} z$ (Immer paarweise einen Nachfolger t_i bestimmen).



q.e.d.

1.15 Definition
Die Relation $\longrightarrow$ wird lokal konfluent genannt, wenn
$\forall x, y, z \in M : (x \longrightarrow y \wedge x \longrightarrow z) \Rightarrow y \downarrow z$.

1.16 Bemerkung
Jede Relation $\longrightarrow$ die konfluent ist, ist auch lokal konfluent.

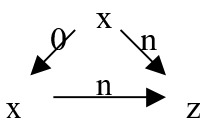
Beweis:
Folgt direkt aus den Definitionen 1.10 und 1.15.

q.e.d.

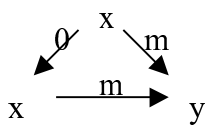
1.17 Lemma
Sei $\longrightarrow$ eine noether'sche Relation.
$\longrightarrow$ ist konfluent, genau dann, wenn $\longrightarrow$ lokal konfluent ist.

Beweis:
„$\Rightarrow$" Folgt direkt aus der Bemerkung 1.6.
„$\Leftarrow$" Sei $\longrightarrow$ eine noether'sche, lokal konfluente Relation.
Wir zeigen, dass die Menge
$P = \{x \in M \mid \forall y, z \in M : (x \overset{*}{\longrightarrow} y \wedge x \overset{*}{\longrightarrow} z) \Rightarrow y \downarrow z\}$ vollständig ist.
Induktionsannahme: $\forall y \in \Delta^+(x) : y \in P$
Sei $x \overset{m}{\longrightarrow} y$ und $x \overset{n}{\longrightarrow} z$. Wir wollen dann zeigen, dass gilt:
$\exists t \in M : y \overset{*}{\longrightarrow} t \wedge z \overset{*}{\longrightarrow} t$
1.Fall

$m = 0 \Rightarrow t = z$



$n = 0 \Rightarrow t = y$



2.Fall

$m \neq 0 \neq n.$

Dann gibt es y_1 und z_1, so dass gilt: $x \longrightarrow y_1 \overset{*}{\longrightarrow} y \wedge x \longrightarrow z_1 \overset{*}{\longrightarrow} z$.

Da die Relation lokal konfluent gilt: $\exists u : y_1 \overset{*}{\longrightarrow} u \wedge z_1 \overset{*}{\longrightarrow} u$.

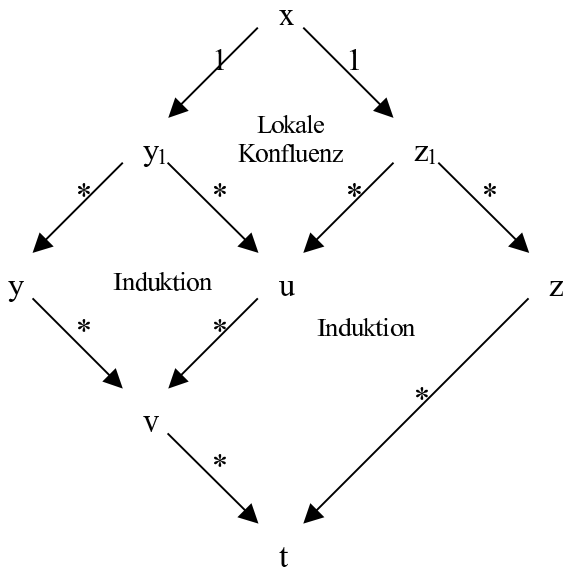
Nach der Induktionsannahme gilt:

$y_1 \in P \Rightarrow (\exists v : y \overset{*}{\longrightarrow} v \wedge u \overset{*}{\longrightarrow} v)$ und $z_1 \in P \Rightarrow (\exists t : v \overset{*}{\longrightarrow} t \wedge z \overset{*}{\longrightarrow} t)$.

Damit folgt: x∈P.

Jetzt sind die Bedingungen von 1.8 erfüllt und P ist somit vollständig.

Nach dem Prinzip der noether'schen Induktion (1.9) folgt: M = P.



q.e.d.

1.18 Satz

Sei $\longrightarrow$ eine noether'sche und konfluente Relation.

(i) Dann besitzt jedes Element x ∈ M einen eindeutigen irrreduziblen Teil z ∈ M, welcher Normalform von x genannt und mit z = N(x) bezeichnet wird.

(ii) Es gilt: $x \overset{*}{\longleftrightarrow} y \Leftrightarrow N(x) = N(y)$.

Beweis:

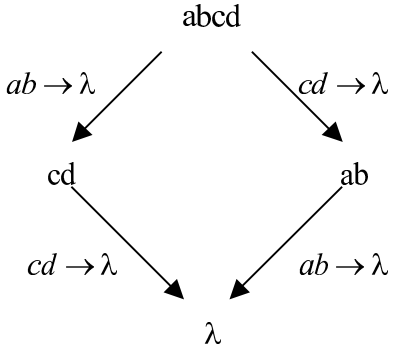
(i) Aus Lemma 1.12 folgt die Eindeutigkeit und aus Bemerkung 1.6 die Existenz der Normalform.

(ii) Mit Lemma 1.11 („Church-Rosser").

q.e.d.

1.19 Beispiel

$M = \{a,b,c,d\}$

$S = \{ab \longrightarrow \lambda, ba \longrightarrow \lambda, cd \longrightarrow \lambda, dc \longrightarrow \lambda\}$

S ist die Menge von Termersetzungsregeln, in der λ das „leere“ Element ist.
Dieses ist die von zwei Elementen erzeugte freie Gruppe.
Die Relation $\longrightarrow_S$ ist noether'sch, lokal konfluent und konfluent.
Dieses Beispiel entspricht dem Kürzen in freien Gruppen.