Ersetzungsregeln

Mykola Gazki

16. November 2006

Seminar "Computeralgebra"
WS 2006/2007

Definition 2.2.1
Sei $P = K[x_1, \ldots, x_n]$-Polynomring, σ-Termordnung auf $\mathbb{T}^n < e_1, \ldots, e_r >$. Sei $g_1, \ldots, g_s \in P^r \setminus \{0\}$ und $G = \{g_1, \ldots, g_s\}$.

a) Sei $m_1, m_2 \in P^r$, $\tilde{t} \in \text{Supp}(m_1)$ mit $\tilde{t} = t \cdot LT_\sigma(g_i)$, $t \in \mathbb{T}^n$ existieren, so dass

$$m_2 = m_1 - \frac{LC_\sigma(m_1)}{LC_\sigma(g_i)} t g_i \quad (\text{allgemein} : m_2 = m_1 - ctg_i)$$

und $\tilde{t} = t \cdot LT_\sigma(g_i) \notin \text{Supp}(m_2)$.
Dann sagt man, dass m_1 reduzierbar zu m_2 in einem Schritt mit benutzung der Ersetzungsregeln, die durch g_i definiert ist (oder anders: m_1 reduzierbar zu m_2 in einem Schritt durch g_i). Wir schreiben $m_1 \xrightarrow{g_i} m_2$. Der Durchgang von m_1 zu m_2 heißt Reduktionschritt.

Bsp.: $m_1 = x^2y \quad g_1 = xy - x - y + 3$
$m_2 = m_1 - ctg_i = x^2y - yg_1 = x^2y - x(xy - x - y + 3) = x^2y - x^2y + x^2 + xy + 3x = x^2 + xy + 3x$. Also: $m_1 \xrightarrow{g_1} m_2$

b) Das transitive Abschluss von Relationen $\xrightarrow{g_1}, \ldots, \xrightarrow{g_s}$ heißt Ersetzungsrelation, die durch G definiert ist und bezeichnet als $\xrightarrow{G}$. Anders gesagt für $m_1, m_2 \in P^r$ schreiben wir $m_1 \xrightarrow{G} m_2$ genau dann, wenn die Indizes $i_1, \ldots, i_t \in \{1, \ldots, s\}$ und Elemente $m'_0, \ldots, m'_t \in P^r$ existieren, so dass $m_1 = m'_0 \xrightarrow{g_{i1}} \cdots \xrightarrow{g_{it}} m'_t = m_2$

c) Element $m_1 \in P^3$ mit der Eigenschaft, dass es kein $i \in \{1, \ldots, s\}$ und kein $m_2 \in P^r \setminus \{m_1\}$ existiert, so dass $m_1 \xrightarrow{g_i} m_2$, heißt irreduzibel bzgl $\xrightarrow{G}$.

d) Äquivalente Relation, difinierte durch $\xrightarrow{G}$ bezeichnet man als $\xleftrightarrow{G}$.

Satz 2.2.2. Eigenschaften von Ersetzungsrelationen.
Sei $g_1, \ldots, g_s \in P^r \setminus \{0\}$ und $G = \{g_1, \ldots, g_s\}$
a) Wenn $m_1, m_2 \in P^r$ erfüllt $m_1 \xrightarrow{G} m_2$ und $m_2 \xrightarrow{G} m_1$, dann $m_1 = m_2$.
b) Wenn $m_1, m_2 \in P^r$ erfüllt $m_1 \xrightarrow{G} m_2$ und $t \in \mathbb{T}^n$, dann haben wir $tm_1 \xrightarrow{G} tm_2$
c) Jede Kette $m_1 \xrightarrow{G} m_2 \xrightarrow{G} \ldots$ mit $m_1, m_2, \cdots \in P^r$ wird schlißlich stationär.
d) Wenn $m_1, m_2 \in P^r$ erfüllt $m_1 \xrightarrow{g_i} m_2$ für $i \in \{1, \ldots, s\}$ und $m_3 \in P^r$, dann existiert Element $m_4 \in P^r$, so dass $m_1 + m_3 \xrightarrow{G} m_4$ und $m_2 + m_3 \xrightarrow{G} m_4$.
e) Wenn $m_1, m_2, m_3, m_4 \in P^r$ erfüllt $m_1 \xleftrightarrow{G} m_2$ und $m_3 \xleftrightarrow{G} m_4$, dann hat man $m_1 + m_3 \xleftrightarrow{G} m_2 + m_4$.
f) Wenn $m_1, m_2 \in P^r$ erfüllt $m_1 \xleftrightarrow{G} m_2$ und wenn $f \in P$, dann hat man $fm_1 \xleftrightarrow{G} fm_2$.
g) Für $m \in P^r$ hat man $m \xleftrightarrow{G} 0$ genau dann wenn $m \in < g_1, \ldots, g_s >$.
h) Für $m_1, m_2 \in P^r$ haben wir $m_1 \xleftrightarrow{G} m_2$ genau dann wenn
$m_1 - m_2 \in < g_1, \ldots, g_s >$.

Beweis:
a) Um a) zu zeigen, betrachten wir die Kette von Reduktionschritten: $m_0' = m_1 \xrightarrow{g_{i1}} m_1' \xrightarrow{g_{i2}} \cdots \xrightarrow{g_{it}} m_t' = m_1$, so dass $i_1, \ldots, i_t \in \{1, \ldots, s\}$ und $m_j' = m_2$ für ein $j \in \{1, \ldots, t-1\}$. ($m_1' = m_1 - c_1 t_1 g_{i1}$, d.h. es fällt der Term in m_1: $\tilde{t}_1 = t_1 LT_\sigma(g_{i1})$ weg). Sei te_k der größte reduzierter Term, d.h. $te_k = \max_\sigma\{\tilde{t}_1, \tilde{t}_2, \ldots\}$. Es gilt entweder $te_k \in \mathrm{Supp}(m_1)$ oder $te_k \in \mathrm{Supp}(t_i g_i) \setminus \{LT_\sigma(t_i g_i)\}$.

1. Fall:
$te_k \in \mathrm{Supp}(t_i g_i) \setminus \{LT_\sigma(t_i g_i)\} \Rightarrow te_k <_\sigma LT_\sigma(t_i g_i) = tLT_\sigma(g_i)$ - aber das ist Wiederspruch zur Maximalität von te_k.

2.Fall:
$te_k \in \mathrm{Supp}(m_1)$. Dieser Term wird reduziert, d.h. er kommt nicht mehr vor. Das kann nicht sein, außer wenn jeder Schritt eine triviale Reduktion ist.

b) Behauptung b) gilt, da die in jedem Reduktionschritt gilt. $m_1 \xrightarrow{g} m_2$, d.h. $m_2 = m_1 - c\tilde{t}g$ (reduziert der Term $\tilde{t}LT_\sigma(g)$) $\Rightarrow tm_2 = tm_1 - c\tilde{t}tg$ (reduziert der Term $\tilde{t}tLT_\sigma(g)$ und $\tilde{t}tLT_\sigma(g) \notin \mathrm{Supp}(tm_2)$)

c) Nehmen wir an, es existiert $i_1, i_2, \cdots \in \{1, \ldots, s\}$ und $m_1, m_2, \cdots \in P^r$, so dass wir die Reduktionskette haben: $m_1 \xrightarrow{g_{i1}} m_2 \xrightarrow{g_{i2}} m_3 \cdots \xrightarrow{g_{ij-1}} m_j \xrightarrow{g_{ij}} m_{j+1} \longrightarrow \ldots$ die nicht stationär ist. Sei t_j der maximale Term in $\mathrm{Supp}(m_j)$, der später reduziert wird. Dann gilt: $t_1 \geq_\sigma t_2 \geq_\sigma t_3 \ldots$. Da wir hier Wohlordnung haben, wird diese Kette nach Satz 1.4.19(18) schließlich stationär.

d) Sei $c \in K, t \in \mathbb{T}^n$ und $i \in \{1, \ldots, s\}$ so, dass $m_2 = m_1 - ctg_i$ und $tLT_\sigma(g_i) \notin \mathrm{Supp}(m_2)$. Offenbar kann man annehmen, dass $c \neq 0$. Sei c'-Koeffizient von $tLT_\sigma(g_i)$ in m_3 und wir unterscheiden 2 Fälle: wenn $c' = -c$ dann haben wir $m_1 + m_3 = m_2 + m_3 + ctg_i = m_2 + m_3 - c'tg_i$. Da Koeffizient von $tLT_\sigma(g_i)$ in $m_2 + m_3 - ctg_i$ verschwindet, bekommt man $m_2 + m_3 \xrightarrow{g_i} m_1 + m_3$ und wir können wählen $m_4 = m_1 + m_3$.

Wenn $c' \neq -c$, dann definieren wir m_4 als $m_4 = m_1 + m_3 - (c + c')tg_i = m_2 + m_3 - c'tg_i$ und bekommen Behauptung, weil der Koeffizient von $tLT_\sigma(g_i)$ in m_4 verschwindet.

Weiter, e) folgt aus d) und f) folgt aus b) und e) wenn man f als Summe von Monomen darstellt. Da h) folgt sofort aus e) und g), bleibt es noch zu zeigen g).
"$\Longrightarrow$"
$m \xleftarrow{G} 0$, d.h. $m \xrightarrow{g_{i1}} m_1 \xleftarrow{g_{i2}} m_2 \longleftarrow \cdots \xrightarrow{g_{ik}} m_k = 0$

$$\left.\begin{array}{rcl} m_1 &=& m - c_1 t_1 g_{i1} \\ m_1 &=& m_2 - c_2 t_2 g_{i2} \end{array}\right\} \Rightarrow \begin{array}{rcl} m &=& m_1 + c_1 t_1 g_{i1} \\ &=& m_2 - c_2 t_2 g_{i2} + c_1 t_1 g_{i1} \\ &\vdots& \\ &=& \underbrace{m_k}_{=0} + \underbrace{c_1 t_1 g_{i1} - c_2 t_2 g_{i2} \cdots \pm c_k t_k g_{ik}}_{\in <g_{i1}, \ldots, g_{ik}>} \end{array}$$

$\Rightarrow m \in < g_{i1}, \ldots, g_{ik} >$.
"$\Longleftarrow$"
$m = f_1 g_1 + \cdots + f_s g_s$ mit $f_1, \ldots, f_s \in P$. Z.z. ist: $m \overset{G}{\longleftrightarrow} 0$.
Wenn $f_i g_i \overset{G}{\longleftrightarrow} 0 \quad \forall i$ gilt, dann folgt mit e) $m \overset{G}{\longleftrightarrow} 0$.
Z.z.: $f_i g_i \overset{G}{\longleftrightarrow} 0$
Aus $g_i \overset{G}{\longleftrightarrow} 0$ folgt mit f) $f_i g_i \overset{G}{\longleftrightarrow} f_i \cdot 0 = 0$
Z.z.: $g_i \overset{G}{\longleftrightarrow} 0$ Trivial: $g_i \overset{g_i}{\longrightarrow} 0$ $(0 = g_i - g_i)$

□

Leider es ist noch nicht klar, wie können wir Teil g) benutzen um zu prüfen, ob unsere Element $m \in P^r$ zu Untermodul gehört. Wir wissen die Reihenfolge von Reduktionschritten in $m \overset{G}{\longleftrightarrow} 0$ nicht. Anders gesagt, wenn wir nur die Reduktionschritte $m = m_0 \overset{g_{i1}}{\longrightarrow} m_1 \overset{g_{i2}}{\longrightarrow} \cdots \longrightarrow$ benutzen, dann können wir auf irreduzible Element bzgl. $\overset{G}{\longrightarrow}$ aufstoßen. Nächste Beispiel zeigt das.

Beispiel 2.2.3
Sei $n = 3, \quad r = 1, \quad G = \{g_1, g_2\}, \quad g_1 = x_1^2 - x_2, \quad g_2 = x_1 x_2 - x_3$.
Sei σ - Termordnung `DegRevLex`.
Dann ist Polynom $f = x_1^2 x_2 - x_1 x_3$ in Ideal (g_1, g_2), da $f = x_1 g_2$. Aber wenn wir Reduktionschritt $f \overset{g_1}{\longrightarrow} x_2^2 - x_1 x_3$ benutzen, bekommen wir irreduzibles Element bzgl. $\overset{G}{\longrightarrow}$

Es ist auch wichtig zu sagen, dass wenn σ nicht Termordnung ist, dann kann die Voraussetzung c) von Satz 2.2.2 verletzt sein.

Beispiel 2.2.4.
Sei $n = 2, \quad r = 1, \quad G = \{g\}, \quad g = x - xy$ und $\sigma =$`RevLex`. Dann wird die Kette $x \overset{g}{\longrightarrow} xy \overset{g}{\longrightarrow} xy^2 \overset{g}{\longrightarrow} \ldots$ nicht stationär.

Satz 2.2.5
Sei $g_1, \ldots g_s \in P^r \setminus \{0\}, \quad G = \{g_1, \ldots, g_s\}$ und $M =< g_1, \ldots, g_s > \subseteq P^r$. Dann sind äqivalent:

C1) Für Element $m \in P^r$ haben wir $m \overset{G}{\longrightarrow} 0$ denau dann wenn $m \in M$.

C2) Wenn $m \in M$ irreduzibel bzgl. $\overset{G}{\longrightarrow}$, dann haben wir $m = 0$.

C3) Für jedes Element $m_1 \in P^r$ gibt es genau ein $m_2 \in P^r$, so dass $m_1 \overset{G}{\longrightarrow} m_2$ und m_2 irreduzibel bzgl. $\overset{G}{\longrightarrow}$.

C4) Wenn $m_1, m_2, m_3 \in P^r$ erfüllt $m_1 \overset{G}{\longrightarrow} m_2$ und $m_1 \overset{G}{\longrightarrow} m_3$, dann existiert Element $m_4 \in P^r$, so dass $m_2 \overset{G}{\longrightarrow} m_4$ und $m_3 \overset{G}{\longrightarrow} m_4$. (Relation mit dieser

Eigenschaft heißt **Konfluent**)

Beweis:
Für Beweis von C1)⇒C2) beachten wir, dass wenn $m \in M$, dann C1) impliziert $m \xrightarrow{G} 0$. Dann, wenn m-irreduzibel und $m \xrightarrow{G} 0$, dann ist es nur möglich, wenn das die triviale Reduktion ist $\Rightarrow m = 0$.

Weiter zeigen wir, dass C2) impliziert C3). Nach Satz 2.2.2.c existiert Element $m_2 \in P^r$-irreduzibel bzgl. $\xrightarrow{G}$ und erfüllt $m_1 \xrightarrow{G} m_2$. Jetzt zur Eindeutigkeit. Angennomen $m_2' \in P^r$ ein anderes Element mit dieser Eigenschaft, d.h. $m_1 \xrightarrow{G} m_2$ und $m_1 \xrightarrow{G} m_2'$. D.h. $m_2 = m_1 - \sum_{j=1}^{k} c_j t_j g_{ij}$ und $m_2' = m_1 - \sum_{j=1}^{l} \tilde{c}_j \tilde{t}_j g_{ij}$.

$\Longrightarrow m_2 - m_2' = (m_1 - \sum_{j=1}^{k} \dots) - (m_1 - \sum_{j=1}^{l} \dots) = -\sum_{j=1}^{k} c_j t_j g_{ij} + \sum_{j=1}^{l} \tilde{c}_j \tilde{t}_j g_{ij} \in M$ Weiter, Element $m_2 - m_2'$ ist irreduzibel bzgl. $\xrightarrow{G}$, da keine Terme in $\mathrm{Supp}(m_2) \cup \mathrm{Supp}(m_2')$ vielfaches von $LT_\sigma(g_1), \dots, LT_\sigma(g_s)$. Nach C2) bekommen wir $m_2 = m_2'$.

C3)$\Longrightarrow$C4)
Nach Satz 2.2.2.c existieren Elemente $m_2', m_3' \in P^r$ die irreduzibel bzgl. $\xrightarrow{G}$ sind und die erfüllen $m_2 \xrightarrow{G} m_2'$ bzw. $m_3 \xrightarrow{G} m_3'$. Aus $m_1 \xrightarrow{G} m_2', m_2 \xrightarrow{G} m_3'$ und C3)bekommen wir $m_2' = m_3'$. Die Behauptung folgt dann für $m_4 = m_2' = m_3'$

C4)$\Longrightarrow$C1)
Z.Z.: $m \in P^r$: $m \xrightarrow{G} 0 \Leftrightarrow m \in M$
$''\Longrightarrow'' m \xrightarrow{G} 0$, d.h. insbesondere $m \xleftarrow{G} 0 \Longrightarrow$(nach Satz 2.2.2.g) $m \in M$.
$''\Longleftarrow'' m \in M \Rightarrow$ (2.2.2.g)$m \xleftarrow{G} 0$. Z.Z.: $m \xrightarrow{G} 0$.
$m = m_1 \xrightarrow{G} m_l \xleftarrow{G} \underbrace{m_{l+1} \xrightarrow{G} \dots \xrightarrow{G} m_t = 0}_{m_{l+1} \xrightarrow{G} 0}$
Also hat man: $m_{l+1} \xrightarrow{G} 0$ und $m_{l+1} \xrightarrow{G} m_l$. Nach C4) gilt:
$m_l \xrightarrow{G} 0 \Longrightarrow m_1 \xrightarrow{G} \dots m_l \xrightarrow{G} 0$. Man sieht, dass die Behauptung folgt nach Induktion.

Lemma 2.2.6
Sei $g_1, \dots g_s \in P^r \setminus \{0\}, G = \{g_1, \dots, g_s\}$ und $M =< g_1, \dots, g_s >$. Nehmen wir an, dass Element $m \in M \setminus \{0\}$ elfüllt $m \xrightarrow{G} 0$.
a) Es existieren Index $\alpha \in \{1, \dots, s\}$ und Term $t \in \mathbb{T}^n$ so, dass $LT_\sigma(m) = tLT_\sigma(g_\alpha)$.
b) Durch Zusammenfassung allen Reduktionsschritten in $m \xrightarrow{G} 0$, bekommen wir $f_1', \dots, f_s' \in P$, so dass $m - \frac{LC_\sigma(m)}{LC_\sigma(g_\alpha)} t g_\alpha = \sum_{i=1}^{s} f_i' g_i'$ und so dass $LT_\sigma(m) >_\sigma LT_\sigma(f_i' g_i')$ für $i = 1, \dots, s$ mit $f_i' g_i' \neq 0$.
c) Wenn wir setzen $f_i = f_i'$ für $i \in \{1, \dots, s\} \setminus \{\alpha\}$ und $f_\alpha = f_\alpha' + \frac{LC_\sigma(m)}{LC_\sigma(g_\alpha)} t$, dann

bekommen wir Element $m = \sum_{i=1}^{s} f_i g_i$ mit $LT\sigma(m) = \max_\sigma\{LT_\sigma(f_i g_i), \quad i \in \{1,\ldots,s\}, f_i g_i \neq 0\}$

Beweis:

Die Behauptung a) folgt sofort aus der Tatsache, dass $LT_\sigma(m)$ in einem Reduktionsschritt eliminiert wird. Jetzt zu b). Sei $m_1,\ldots,m_t \in P^r$ so, dass $m_1 = m, m_t = 0$ und für alle $i = 1,\ldots,t-1$ haben wir $m_i \xrightarrow{G} m_{i+1}$ in einem Reduktionsschritt. Nach a), existiert Reduktionsschritt, der LT von m reduziert. Dieses Schritt ist eindeutig, weil $LT_\sigma(m)$ durch kleinere Terme ersetzt wird.

Sei $l \in \{1,\ldots,t-1\}$, so dass $m_{l+1} = m_l - \frac{LC_\sigma(m)}{LC_\sigma(g_\alpha)} t g_\alpha$. Dann $m - \frac{LC_\sigma(m)}{Lc_\sigma(g_\alpha)} t g_\alpha = m - (m_l - m_{l+1} = \sum_{i=1}^{l-1}(m_i - m_{i+1}) + \sum_{i=1+1}^{t-1}(m_i - m_{i+1})$ hat die Form $\sum_{i=1}^{s} g_i' g_i$. Hier die Polynome f_i' bekommen wir durch Zusammenfassung von Elementen ct, die in zwei Summen erscheinen, wobei jede $m_i - mi + 1$ von der Form $m_i - m_{i+1} = ctg_\beta$ für ein $c \in K, \quad t \in \mathbb{T}^n$ und $\beta \in \{1,\ldots,s\}$.

Wir haben im Schritt $m_{l+1} \xrightarrow{G} m_l$ $LT_\sigma(m)$ eliminiert. Dieses Schritt ist nicht mehr in unsere Summe, d.h. $LT_\sigma(m) >_\sigma LT_\sigma(f_i g_i)$. Schlißlich sehen wir, dass c) sofort aus b) folgt.

Beispiel 2.2.7

Sei $g_1 = x^2 - xy, \quad g_2 = xy - x - z, \quad g_3 = xy + xz$ - Polynome in $\mathbb{Q}[x,y,z]$ $G = \{g_1, g_2, g_3\}, \quad \sigma =$`DegLex`. Reduzieren x^3 bzgl. $\xrightarrow{G}$:

$x^3 \xrightarrow{g_1} x^2 y \xrightarrow{g_2} x^2 + xz \xrightarrow{g_1} xy + xz \xrightarrow{g_3} 0$

Weiter, wenn wir Reduktionsschritte zusammenfassen, dann bekommen wir $x^3 - xg_1 = xg_2 + g_1 + g_3$. Laut c) kann man schreiben $x^3 = (x+1)g_1 + xg_2 + g_3$.

Leider es kann so passieren: (Lemma braucht $m \xrightarrow{G} 0$):

$x^3 \xrightarrow{g_1} x^2 y \xrightarrow{g_1} xy^2 \xrightarrow{g_2} xy + yz \xrightarrow{g_2} yz + x + z$ - irreduzibel bzgl. $\xrightarrow{G}$.

Satz 2.11 (Spezielle erzeugung von Untermodule

Sei $M \subseteq P^r$, P-Untermodul, und $g_1,\ldots,g_s \in P^r \setminus \{0\}$. Dann sind folgende Aussagen äquivalent:

A1) Für jedes Element $m \in M \setminus \{0\}$ existieren $f_1,\ldots,f_s \in P$, so dass $m = \sum_{i=1}^{s} f_i g_i$ und $LT_\sigma(m) \geq_\sigma LT_\sigma(f_i g_i)$ für alle $i = 1 \ldots s$ mit $f_i g_i \neq 0$.

A2) Für jedes Element $m \in M \setminus \{0\}$ existieren $f_1,\ldots,f_s \in P$, so dass $m = \sum_{i=1}^{s} f_i g_i$ und $LT_\sigma(m) = \max_\sigma\{LT_\sigma(f_i g_i) | i \in \{1,\ldots,s\}, f_i g_i \neq 0\}$

Beweis: Aussage A2) impliziert A1).

$''\geq_\sigma''$ in A2) folgt sofort aus A1). $''\leq_\sigma''$ in A2) folgt aus dem Satz 1.5.3 a).

Satz 2.2.8

Sei $g_1,\ldots,g_s \in P^r \setminus \{0\}, \quad G = \{g_1,\ldots,g_s\}$ und $M =< g_1,\ldots,g_s >$. Dann sind die Aussagen A1), A2) aus dem Satz 2.11 äquivalent den Aussagen C1), C2), C3)

und C4) aus dem Satz 2.2.5.
Beweis: A2)$\Longrightarrow$C2) (durch Wiederschpruch)
Wir nehmen an, dass Element $m \in M \setminus \{0\}$ existiert, m-irreduziebel bzgl. $\xrightarrow{G}$. Nach Aussage A2) m kann man schreiben als $m = \sum_{i=1}^{s} f_i g_i$, so dass $f_1, \ldots, f_s \in P$ und $LT_\sigma(m) = \max\{LT_\sigma(f_i g_i) | i \in \{1, \ldots, s\}, f_i g_i \neq 0\}$. Sei $tLT_\sigma(g_i)$-der Term, der dieses Maximum erreicht. Dann Element $m' = m - \frac{LC_\sigma(m)}{LC_\sigma(g_i)} t g_i$ erfüllt $m \xrightarrow{G} m'$ und $m' \neq m$ (wir haben hier $LT_\sigma(m)$ eliminiert, aber wir haben angennomen, dass m-irreduzibel $\Rightarrow$ Wiederschpruch).
Schlißlich C1)$\Longrightarrow$A2) folgt direkt aus Lemma 2.2.6.