Dicksons Lemma

Lemma Dicksons Lemma

Jedes Monomideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ besitzt eine endliche Basis $I = \langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}} \rangle$.

Beweis per Induktion über die Anzahl der Variablen n:

- $n = 1$: $I = \langle x_1^\alpha \mid \alpha \in A \rangle$. Sei β das kleinste Element in $A \subseteq \mathbb{N}_0$.
- Daher gilt $x_1^\beta \mid x_1^\alpha$ für alle $\alpha \in A$. D.h. $I = \langle x_1^\beta \rangle$.
- $n - 1 \to n$: Wir verwenden die Variablen $x_1, \ldots, x_{n-1}, y$.
- D.h. Monome besitzen die Form $x^\alpha y^t$ mit $\alpha \in \mathbb{N}_0^{n-1}$ und $t \in \mathbb{N}_0$.
- Sei J die Projektion von I auf $\mathbb{F}[x_1, \ldots, x_{n-1}]$. D.h. J wird generiert von denjenigen Monomen x^α, für welche $x^\alpha y^t \in I$ für ein $t \geq 0$.
- IV: Wir schreiben $J = \langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}} \rangle$. Für $i = 1, \ldots, m$ gilt
$$x^{\alpha^{(i)}} y^{t_i} \in I \text{ für ein festes } t_i \geq 0. \text{ Sei } t = \max_i \{t_i\}.$$
- Für jedes feste $k = 0, \ldots, t - 1$ definiere $J_k \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}]$ als die Projektion derjenigen Monome in I, die genau y^k enthalten.

Dicksons Lemma

Beweis: (Fortsetzung)

- Nach IV: $J_k = \langle x^{\alpha_k^{(1)}}, \ldots, x^{\alpha_k^{(m_k)}} \rangle$ für $k = 0, \ldots, t-1$.
- Wir behaupten, dass I von folgender Monomliste L generiert wird.

$$\begin{array}{rlcl}
\text{aus } J: & x^{\alpha^{(1)}}y^t, & \ldots & , x^{\alpha^{(m)}}y^t \\
\text{aus } J_0: & x^{\alpha_0^{(1)}}y^0, & \ldots & , x^{\alpha_0^{(m_0)}}y^0 \\
\vdots & & \vdots & \\
\text{aus } J_{t-1}: & x^{\alpha_{t-1}^{(1)}}y^{t-1}, & \ldots & , x^{\alpha_{m-1}^{(m_{t-1})}}y^{t-1}
\end{array}$$

- $\langle L \rangle \subseteq I$: Die Monome in unserer Liste L sind alle in I. Dies folgt für die Elemente $x^{\alpha_k^{(i)}}y^k$ nach Konstruktion der Elemente in J_k.
- Für die Elemente $x^{\alpha^{(i)}}y^t$ gilt dies aufgrund der Maximalität von t.
- $I \subseteq \langle L \rangle$: Jedes $x^\alpha y^p \in I$ wird von einem Listenmonom geteilt.
- Sei $p \geq t$. Dann teilt ein $x^{\alpha^{(i)}}y^t$ nach Konstruktion von J.
- Sei $p < t$. Dann teilt ein $x^{\alpha_p^{(i)}}y^p$ nach Konstruktion von J_p.
- D.h. $\langle L \rangle$ und I enthalten dieselben Monome und sind daher gleich.

Idealzugehörigkeit in Monomidealen

Lemma Dicksons Lemma (Teil II)

Jedes Monomideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ besitzt eine endliche Basis $I = \langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}} \rangle$ mit $a^{(i)} \in A$.

Beweis: Übungsaufgabe.

Satz Idealzugehörigkeit in Monomidealen

Sei $I = \langle x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}} \rangle$ ein Monomideal. Dann gilt $f \in I$ gdw f bei Division durch $x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}$ Rest 0 lässt.

Beweis:

- $\Leftarrow$: Aus $f = h_1 \cdot x^{\alpha^{(1)}} + \ldots + h_m \cdot x^{\alpha^{(m)}} + 0$ folgt $f \in I$.
- $\Rightarrow$: Nach *Satz zur Darstellung aus Monomen* folgt, dass $f \in I$ gwd
$$f = \sum_i c_i x^{\gamma^{(i)}} \text{ mit } x^{\gamma^{(i)}} \in I.$$
- Andererseits ist $x^{\gamma^{(i)}} \in I$ gwd $x^{\alpha^{(j)}}$ teilt $x^{\gamma^{(i)}}$ für ein $j \in [m]$.
- Damit wird jeder Term in f von einem der $x^{\alpha^{(j)}}$ geteilt.
- Sukzessives Teilen von f durch $x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(m)}}$ liefert also Rest 0.

Das Ideal der führenden Terme

Definition Ideal der führenden Terme

Sei $I \subseteq \mathbb{F}[x_1, \ldots, x_n] \setminus \{0\}$ ein Ideal, $LT(I)$ die Menge führender Terme

$$LT(I) = \{cx^\alpha \mid \text{es existiert } f \in I \text{ mit } LT(f) = cx^\alpha\}.$$

Dann heißt $\langle LT(I) \rangle$ das *Ideal der führenden Monome von* I.

Anmerkung:

- Sei $I = \langle f_1, \ldots, f_m \rangle$. Es gilt $LT(f_i) \in LT(I)$ für alle $i \in [m]$.
- Daher folgt $\langle LT(f_1), \ldots, LT(f_m) \rangle \subseteq \langle LT(I) \rangle$.
- Andererseits kann $LT(I)$ weitere Element enthalten.
- Sei $I = \langle f_1, f_2 \rangle$ mit $f_1 = x^3 - 2xy$ und $f_2 = x^2y + x - 2y^2$.
- Es gilt $x^2 \in I$ wegen $x^2 = -y \cdot f_1 + x \cdot f_2$. D.h. $x^2 \in \langle LT(I) \rangle$.
- Aber x^2 wird weder von $LT(f_1) = x^3$ noch von $LT(f_2) = x^2y$ geteilt.
- Daraus folgt, dass x^2 nicht im Monomideal $\langle LT(f_1), LT(f_2) \rangle$ ist.

Existenz einer Gröbnerbasis

Definition Gröbnerbasis

Eine Menge $G = \{g_1, \ldots, g_m\} \subseteq I$ heißt *Gröbnerbasis* falls

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_m)\rangle.$$

Satz Existenz einer Gröbnerbasis

Sei I ein Ideal. Dann ist $\langle LT(I)\rangle$ ein Monomideal und es existiert eine Gröbnerbasis $\{g_1, \ldots, g_m\} \subseteq I$ mit $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_m)\rangle$.

Beweis:

- Es gilt $\langle\{LT(g) \mid g \in I \setminus \{0\}\}\rangle = \langle\{LM(g) \mid g \in \setminus\{0\}\}\rangle$.
- Die führenden Monome von I generieren aber ein Monomideal.
- Anwendung von Dicksons Lemma liefert

$$\begin{aligned} & \langle LT(I)\rangle = \langle LM(I)\rangle = \langle\{LM(g_i) | g_i \in I\}\rangle \\ = \; & \langle LM(g_1), \ldots, LM(g_m)\rangle = \langle LT(g_1), \ldots, LT(g_m)\rangle. \end{aligned}$$

Hilbert Basissatz

Satz Hilbert Basissatz

Jedes Ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ wird endlich generiert, d.h.

$$I = \langle g_1, \ldots, g_m \rangle \text{ für } g_1, \ldots, g_m \in I.$$

Beweis:

- Falls $I = \{0\}$, verwende 0 als Generator. Sei also $I \neq \{0\}$.
- Sei $\{g_1, \ldots, g_m\} \subseteq I$ eine Gröbnerbasis für I.
- Wir wissen, dass $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle$ für $g_i \in I$.
- Behauptung: $I = \langle g_1, \ldots, g_m \rangle$. Es gilt $\langle g_1, \ldots, g_m \rangle \subseteq I$, da $g_i \in I$.
- $I \subseteq \langle g_1, \ldots, g_m \rangle$: Sei $f \in I$ beliebig.
- Teilen von f durch $g_1, \ldots, g_m$ liefert $f = a_1 g_1 + \ldots + a_m g_m + r$, wobei kein Term von r von einem der $LT(g_i)$ geteilt wird.
- Angenommen $r \neq 0$. Es gilt $r = f - a_1 g_1 - \ldots - a_m g_m \in I$.
- Aus $r \in I$ folgt $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle$.
- Dann muss aber nach Teilbarkeitssatz $LT(r)$ von einem der Terme $LT(g_i)$ geteilt werden. (Widerspruch)
- D.h. es folgt $r = 0$ und damit $f \in \langle g_1, \ldots, g_m \rangle$.