Freie Auflösungen und das Syszygien Theorem

Jens Heinrich

10.01.2017

1 Einleitung

In diesem Vortrag geht es vor allem um Syzygien und Freie Auflösungen, was der Titel nahe legt. Aus dem Titel geht allerdings kein Grund hervor, nach diesen Dingen zu suchen. Fangen wir doch damit an, wie eine Syzygie definiert ist um zu sehen, was sie ist. Auf dem Weg sammeln wir noch ein paar Grundlagen mit ein:

Definition 1 (Komplex). Ein **Komplex von R-Modulen** ist eine Sequenz von Modulen F_i und Abbildungen $F_i \to F_{i-1}$, sodass für alle i die Komposition $F_{i+1} \to F_i \to F_{i-1}$ Null wird.
Die **Homologie** dieses Komplexes in F_i ist der Modul

$$\ker\left(F_i \to F_{i-1}\right) \big/ \operatorname{im}\left(F_{i+1} \to F_i\right).$$

Eine **freie Auflösung** eines R-Moduls M ist ein Komplex

$$\mathcal{F} : \cdots \to F_n \overset{\phi_n}{\to} \cdots \to F_1 \overset{\phi_1}{\to} F_0$$

von freien R-Modulen, sodass $\operatorname{coker} \phi_1 = M$ und $\mathcal{F}$ exakt ist. (Man schreibt auch gelegentlich ein $\to 0$ an das Ende des Komplexes und fordert Exaktheit ausser in F_0. Diese Schreibweise wird häufig missbraucht, um zu sagen, dass die exakte Sequenz

$$\mathcal{F} : \cdots \to F_n \overset{\phi_n}{\to} \cdots \to F_1 i \overset{\phi_1}{\to} F_0 \to M \to 0$$

eine Aufloesung von M ist. Das Bild von ϕ_i nennen wir die *i-te Syzygie* von M.
Ein Auflösung heisst freie, graduierte Auflösung, wenn R ein graduierter Ring, die F_i graduierte freie Module und die Abbildungen homogen vom Grad 0 sind. Wenn es ein $n < \infty$ gibt, sodass $F_{n+1} = 0$, aber $F_i \neq 0 \ \forall\ 0 \leq i \leq n$, nennen wir $\mathcal{F}$ eine endliche Auflösung von Länge n.

Hier eine kurze Auffrischung der Begrifflichkeiten:

Definition 2 (Freier Modul [1]0.3). Ein freier R-Modul ist ein Moduln der isomorph zu einen direkten Summe von R Kopien ist.

Beispiel 1. Ein sehr einfaches Beispiel ist

$$M := \mathbb{R} \cdot x \oplus \mathbb{R} \cdot y \oplus \mathbb{R} \cdot z = \mathbb{R}^3$$

Definition 3 (Graduierter Ring [1]1.5)**.** Ein **graduierter Ring ist ein Ring R zusammen mit einer direkten Summenzerlegung**

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \dots \textbf{ als abelsche Gruppen,}$$

sodass

$$R_i R_j \subset R_{i+1} \textbf{ für } \quad i, j \geq 0.$$

Beispiel 2. Der einfachste graduierte Ring ist der Ring Polynome $S = k[x_1, \dots, x_r]$ mit der Graduierung

$$S = S_0 \oplus S_1 \oplus \dots,$$

wobei S_d der Vektorraum der homogenen Polynome vom Grad d ist.

Also das hat jetzt nicht so viel zum Verständnis beigetragen, wie ich dachte; wobei, unsere Syzygie besteht also aus Punkten aus einer direkten Summe, sozusagen einem n-Tupel $a_1, \dots, a_n$. Desweiteren folgt aufgrund der Exaktheit und der Tatsache, das unsere Abbildungen von Grad 0 sind, d.h. sie sind jeweils der Form

$$f(x) = x_1 f_1 + \dots + x_k f_k,$$

dass alle Punkte der Syzygie die folgende Gleichung erfüllen:

$$a_1 f_1 + \dots + a_n f_n = 0$$

Also sind unsere Syzygien Lösungen von linearen Gleichungen.

Syzygien werden in Computeralgebra System verwendet, um multivariate Gleichungen zu lösen

2 Das Hilbertsche Syzygientheorem

Theorem 3 (Das Hilbert'sche Syzygien Theorem [1]1.13)**.** *Wenn $R = k[x_1, \dots, x_r]$ gilt, dann hat jeder endlich erzeugte graduierte R-Modul eine endlich erzeugte freie Auflösung von Länge $\leq r$ aus endlich erzeugten freien Moduln.*

Um das jetzt aber zu beweisen müssen wir etwas ausholen, doch wollen wir mit einem Beispiel beginnen.

Beispiel 4 (Exercise 1.22)**.** Sei $R = k[x]$ Dann haben alle endlich erzeugten R-Module eine endliche freie Auflösung.

Beweis. REPLACE ME
Sei M ein beliebiger endlich erzeugter Modul über R, dann gilt:
$M \simeq \oplus_{i=1}^{n} R$ für ein $n < \infty$.
Desweiteren gilt □

Theorem 5 (Struktursatz für endlich erzeugte Moduln über Hauptidealringen [3])**.** *Wenn ein Modul M über einem Körper F endlich erzeugt ist, dann können wir eine Basis aus n Elementen finden, sodass $M \simeq F^n$ und $n < \infty$.*

Beispiel 6. Sei $R = k[x] / (x^n)$, dann sehen die freien Auflösungen von $R/(x^m)$ für alle $m \leq n$ als MISSING geschrieben werden können.

Beweis. REPLACE ME

□

3 Syzygientricks

Definition 4 (GCD,LCM)**.** Im folgenden werden wir für den kleinsten gemeinsamen Teiler kgV und für den grössten gemeinsamen Teiler GCD schreiben

Notation 1 ([1]322)**.** Sei F ein freies Modul mit Basis und M Untermodul von F der von $m_1, \ldots, m_t$ erzeugt wird. Sei

$$\begin{aligned} \phi : \oplus_{j=1}^{t} S\epsilon_j & \rightarrow F \\ \phi(\epsilon_j) & := m_j \end{aligned}$$

die Abbildung eines freien Moduls, dessen Bild M ist. Für alle Indexpaare i, j, sodass m_i und m_j dasselbe Basiselement von F, definieren wir

$$m_{ij} := m_i / \operatorname{ggT}(m_i, m_j),$$

und sonst die σ_{ij} wie folgt als Elemente von $\ker \phi$ definieren:

$$\sigma_{ij} := m_{ji}\epsilon_i - m_{ij}\epsilon_j.$$

Lemma 7 ([1]15.1)**.** Mit der Notation 1 gilt, dass $\ker \phi$ von den σ_{ij} erzeugt wird.

Beweis.

$$\phi(\sigma_{ij}) = \phi(m_{ji}\epsilon_i) - \phi(m_{ij}\epsilon_j) = \frac{m_j}{\operatorname{ggT}(m_i, m_j)}\dot{m}_i - \frac{m_i}{\operatorname{ggT}(m_i, m_j)}\dot{m}_j = 0,$$

somit sind die $\sigma_{ij} \in \ker \phi$. $\ker \phi$ ist ein k-Vektorraum , also können wir annehmen, dass $\ker \phi = \bigoplus_{n \in F} (\ker \phi)_n$, wobei

$$(\ker \phi)_n = \left\{ \sum a_v n_v \epsilon_v \in \ker \phi \middle| m_v \text{ teilt } n,\ n_v = n/m_v \text{ and } a_v \in k \right\}$$

geschrieben wird. Angenommen

$$\sigma = \sum p_i \epsilon_i \in S^t, \qquad p_i \in S$$

ist eine Syzygie, sodass $\sum P_i m_i = 0$. Für jedes Monom n aus F, das in einem der $p_j m_j$ vorkommt, und für alle i sei $p_{i,n}$ der Term von p_i, sodass $p_{i,n} m_i$ ein Vielfaches von n ist. Es muss gelten $\sum p_{i,n} m_i = 0$, damit $\sum p_{i,n}\epsilon_i$ aus $(\ker \phi)_n$. Nehmen wir an, dass $\sigma = \sum a_v n_v \in (\ker \phi)_n$. Wenn $\sigma \neq 0$. dann sind mindestens zwei der $a_v n_v \neq 0$, da σ eine Syzygie ist. OBdA die i-te und die j-te , wobei $i < j$. Es folgt n wird von m_i und m_j geteilt. und somit ist n_i teilbar durch

$$\operatorname{kgV}(m_i, m_j) / m_i = m_j / \operatorname{ggT}(m_i, m_j) = m_{ji}$$

Somit können wir ein Vielfaches von $(n_i/m_{ji})\,\sigma_{ij}$ von σ abziehen um unsere Relation zu reduzieren. □

Lemma 8 ([1]323)**.** Mit der Notation aus 7 erhalten wir, dass jedes Element von $\ker \phi$ eindeutig als ein Summe von Elementen $\tau = \sum n_{ij}\sigma_{ij} \in \ker \phi$ schreiben können, sodass n_v, m_v zum gleichen Monom $n \in F$ äquivalent sind. Solche Elemente können wir als

$$\tau = \sum n_{ij}\sigma_{ij},$$

wobei über alle $i < j$, sodass $\operatorname{kgV}(m_i, m_j) | n$ und n_{ij} ein Vielfaches von $n / \operatorname{kgV}(m_i, m_j) = n_i/m_{ji}$ ist, summieren.

Beweis. Die Eindeutigkeit folgt aus 7. Da wir im letzten Schritt des obigen Beweises nur Terme entfernen, können wir die σ_{ij} von dort nehmen. □

Diese σ_{ij} nennt man oft **geteilte Koszul Relationen**.

4 Gröbner Basen

Definition 5 (Initialer Term [1]325)**.** Wenn $>$ eine Ordnung auf Monomen ist, dann definieren wir für alle $f \in F$ den **initialen Term von** f , geschrieben als $\mathrm{in}_>(f)$, als den grössten Term von f bezüglich der Ordnung $>$. Wenn M ein Untermodul von F ist, dann bezeichnet $\mathrm{in}_>(M)$ den Untermodul, der von $\left\{\mathrm{in}_>(f) \,\middle|\, f \in F\right\}$ erzeugt wird. Wir werden oft $\mathrm{in}_>$ mit in abkürzen, wenn die Ordnung klar ist.

Beispiel 9. Sei $>_{lex}$ Die Ordung in der gilt $x > y$, dann ist $\mathrm{in}_{>_{lex}}\left(x^2 + xy + y^2\right) = x^2$

Definition 6 (Gröbnerbasis [1]328)**.** Eine **Gröbnerbasis** bezüglich einer Ordnung $>$ auf einem freien Modul mit Basis F ist eine Menge von Elementen $g_1, \ldots, g_t \in F$, sodass wenn M ein Untermodul von F erzeugt von $g_1, \ldots, g_t$ ist, gilt, dass die $\mathrm{in}_>(g_1), \ldots, \mathrm{in}_>(g_t)$ $\mathrm{in}_>(M)$ erzeugen.
Wir sagen dann, dass $g_1, \ldots, g_t$ eine **Gröbnerbasis von** M sind.

Proposition-Definition 10 ([1]15.6)**.** *Sei F ein freier S-Modul mit einer Basis und Monomordnung $>$. Wenn $f, g_1, \ldots, g_t \in F$ dann gibt es einen Ausdruck*

$$f = \sum f_i g_i + f' mit f' \in F, f_i \in S_i,$$

bei dem kein f' in $(\mathrm{in}(g_1), \ldots, \mathrm{in}(g_t))$ vorkommt und

$$\mathrm{in}(f) \geq \mathrm{in}(f_i g_i)$$

*für alle i. Jedes solches f' heisst **Rest** von f in Bezug auf $g_1, \ldots, g_t$ und ein Ausdruck $f = \sum f_i g_i + f'$, der die Bedingungen von oben erfüllt, heisst **Standard Ausdruck** für f ausgedrückt in g_i.*

Algorithmus 1 (Divisionsalgorithmus [1]15.7)**.** Sei F ein freier S-Modul mit Basis und fester Monomordnung. Wenn $f, g_1, \ldots, g_t \in F$, dann können wir einen Standard Ausdruck

$$f = \sum m_u g_{s_u} + f'$$

von f bezüglich $g_1, \ldots, g_t$ finden, indem wir die Indices s_u und die Terme m_u induktiv definieren. Wenn wir bereits $s_1, \ldots, s_p$ und $m_1, \ldots, m_p$, gewählt haben, dann wählen wir,

$$f'_p := f - \sum_{u=1}^{p} m_u g_{s_u},$$

falls $f'_p \neq 0$ und m der maximale Term von f'_p, der durch eines der der $\mathrm{in}(g_i)$ teilbar ist,

$$s_{p+1} = i, m_{p+1} = m / \mathrm{in}(g_i)$$

. Dieser Vorgang bricht entweder ab, wenn $f'_p = 0$ oder wenn keines der $\mathrm{in}(g_i)$ ein Monom aus f'_p teilt; der Rest f' ist dann f'_p.

F	{freier S-Modul mit Basis }
$>$	{ Monomordnung }
f	{ $\in F$ }
$G = g_1, \ldots, g_t$	
	$\{\in F\}$

$s = []$

$m = []$

$j = 1$

$f' := f$

$\bar{m} := ini\,(f')$

$\exists g_q \in G\ : \bar{m} | ini\,(g_q)$

- $i = \arg\max \{g_q \in G\ : m | ini\,(g_q)\}$
- $s_j := i$
- $m_j := \bar{m} / ini\,(g_{s_j})$
- $f' := f - \sum_{l=1}^{j} g_{s_l} * m_l$
- $m := ini\,(f')$
- $j := j + 1$

Notation 2 ([1]331)**.** Sei F ein freier Modul über S mit Basis und Monomordnung $>$. Seien $0 \neq g_1, \ldots, g_t \in F$ und $\oplus S\epsilon_i$ ein freier Modul mit Basis $\{\epsilon_i\}$ die den $\{g_i\}$ aus F über die folgenden Abbildungen

$$\begin{aligned} \phi : \oplus\, S\epsilon_i &\to F \\ \epsilon_i &\mapsto g_i \end{aligned}$$

entsprechen.
Für jedes Indexpaar i, j, sodass in (g_i) und in (g_j) dasselbe Basiselement von F enthalten, definieren wir ein neues

$$m_{ij} = \mathrm{in}\,(g_i) \,/\, \mathrm{ggT}\,(\mathrm{in}\,(g_i)\,, \mathrm{in}\,(g_j)) \in S$$

und setzen

$$\sigma_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j.$$

Diese σ_{ij} Erzeugen die Syzygie auf den in (g_i) nach 7 und sind auch an die dortige Notation angepasst. Desweiteren wählen wir für jedes der Indexpaare einen Standardausdruck

$$m_{ji}g_i - m_{ij}g_j = \sum f_u^{(ij)} g_u + h_{ij}$$

für $m_{ji}g_i - m_{ij}g_j$ bezüglich der $g_1, \ldots, g_t$. Man kann sehen, dass in $(f_u^{ij} g_u) <$ in $(m_{ji}g_i)$ Zur Vereinfachung setzen wir $h_{ij} = 0$, falls in (g_i) und in (g_j) verschiedene Basiselemente von F enthalten sind.

Theorem 11 (Buchberger Kriterium [1]15.8)**.** *Mit der Notation aus 2 folgt, dass die $g_1, \ldots, g_t$ eine Gröbnerbasis bilden, genau dann wenn h_{ij} für alle i und j.*

Beweis. Der Autor von [1] meint man sehe dieses Aussage leicht, doch das stimmt nur, wenn man es einmal gesehen hat:

“$\Rightarrow$” Wenn die $g_1, \ldots, g_t$ eine Gröbnerbasis bilden, dann können wir, da es eine *Basis* ist, alle Elemente in den $g_1, \ldots, g_t$ ohne Rest geschrieben werden. “$\Leftarrow$” Wenn wir alle Elemente ohne Rest ($h_{ij} = 0$) schreiben koennen, dann bilden die $g_1, \ldots, g_t$ ein erzeugendes System. Es fehlt noch die Minimalität, die aus dem folgenden Algorithmus folgt. □

Algorithmus 2 (Buchberger Algorithmus [1]333)**.** Unter den Vorraussetzungen aus 11 sei M ein Untermodul von F und $g_1, \ldots, g_t$ seien Erzeuger von M, dann gilt $M = \ker \phi$. Berechne die Reste h_{ij}. Wenn alle $h_{ij} = 0$, dann bilden die g_i eine Gröbnerbasis von M. Wenn einige der $h_{ij} \neq 0$ dann ersetze $g_1, \ldots, g_t$ mit $g_1, \ldots, g_t, h_{ij}$ und wiederhole dann den Prozess. Da der von $g_1, \ldots, g_t, h_{ij}$ erzeugte Untermodul echt grösser als der von $g_1, \ldots, g_t$ erzeugte Untermodul ist, terminiert der Prozess nach endlich vielen Schritten.
Die obere Schranke

$$b = \left((r+1)(d+1)+1\right)^{2^{(s+1)}(r+1)}$$

hält für

$$\begin{aligned} r &= \text{Anzahl der Variablen} \\ d &= \text{maximal Grad von } g_i \text{ , und} \\ s &= \text{dem Grad des Hilbertpolynoms} \\ &\quad (\text{ dieser ist um eins kleiner als die Dimension; er liegt zwischen } 0 \text{ und } r-1 \text{ }). \end{aligned}$$

Notation aus 2

F { freier Module über S}

$>$ { Monomordnung }

Groebner=$g_1, \dots, g_t$

{ $0 \neq g_1, \dots, g_t \in F$ }

$M := \oplus S\epsilon_i$

{ ein freier Modul mit Basis $\{\epsilon_i\}$ }

ϕ {

$$\begin{aligned} \phi : \oplus S\epsilon_i \to & \quad F \\ \epsilon_i \mapsto & \quad g_i \end{aligned}$$

}

$i = 1$

$i \leq t$

$j = 1$

$j \leq t$

ini (g_i) und *ini* (g_j) dasselber Basiselement enthalten

true:

$m_{ij} = ini\,(g_i)\; GCD\,(ini\,(g_i)\,, ini\,(g_j))$

$\sigma_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j$

$tmp := m_{ji}g_i - m_{ij}g_j$

nutze Divisionsalgorithmus um *tmp* als $\sum f_u^{(ij)} g_u +$ h_{ij} mit $g_u \in Groebner$ darzustellen

$h_{ij} \neq 0$

true: $Groebner = Groebner \cup h_{ij}$

false: $\varnothing$

false:

h_{ij}

$\varnothing$

$j{+}{+}$

$i{+}{+}$

Definition 7 ([1]334)**.** Wir definieren

$$\tau_{ij} := m_{ji}\epsilon_i - m_{ij}\epsilon_j - \sum_u f_u{}^{(ij)}\epsilon_u,$$

für $i < j$, sodass $\text{in}(g_i)$ und $\text{in}(g_j)$ dasselbe Basiselement von F enthalten.

Theorem 12 (Schreyer [1][15.10)**.** *Mit der Notation von 7, können wir annehmen, dass $g_1, \ldots, g_t$ eine Gröbnerbasis sind. Sei jetzt $>$ eine Monomordnung auf $\oplus_{j=1}^{t} S\epsilon_j$, für die gilt $m\epsilon_u > n\epsilon_v$*
$\Longleftrightarrow$

$$\text{in}(mg_u) > \text{in}(ng_v) \textit{ bezüglich der Ordnung auf } F$$

oder

$$\text{in}(mg_u) = \text{in}(ng_v) \, (\textit{bis auf Vielfachheit}) \;\; \textit{und} \;\; u < v.$$

. Die τ_{ij} erzeugen die Syzygien auf den g_i. Insbesondere sind die τ_{ij} eine Gröbnerbasis der Syzygien bezüglich der Ordnung $>$ und es gilt $\text{in}(\tau_{ij}) = m_{ji}\epsilon_i$.

Beweis. Wir beginnen damit zu zeigen, dass $\text{in}(\tau_{ij}) = m_{ji}\epsilon_i$. Es gilt

$$m_{ji} \, \text{in}(g_i) = \frac{\text{in}(g_j)}{\text{ggT}(\text{in}(g_i), \text{in}(g_j))} \cdot \text{in}(g_i) = \frac{\text{in}(g_j) \cdot (g_i)}{\text{ggT}(\text{in}(g_i), \text{in}(g_j))} = \frac{\text{in}(g_i)}{\text{ggT}(\text{in}(g_i), \text{in}(g_j))} \, \text{in}(g_j) = m_{ij} \, \text{in}(g_j),$$

und diese Terme sind nach Annahme grösser als alle, die in den $f_u^{(ij)} g_u$ vorkommen. Deshalb ist $\text{in}(\tau_{ij})$ entweder (a) $m_{ji}\epsilon_i$ oder (b) $-m_{ij}\epsilon_j$ aufgrund des ersten Teils der Definition der Monomordnung $>$, und da $i < j$ gilt $m_{ji}\epsilon_i > m_{ij}\epsilon_j$ und somit sind wir im Fall (a).
Jetzt ist noch zu zeigen, dass die τ_{ij} eine Gröbnerbasis bilden.
Sei $\tau = \sum f_v \epsilon_v$ eine beliebige Syzygie. Wir müssen nun zeigen, dass $\text{in}(\tau)$ durch eine der $\text{in}(\tau_{ij})$ teilbar ist, also $\text{in}(\tau)$ ein Vielfaches von einem $m_{ji}\epsilon_i$ mit $i < j$.
Für jeden Index v, sei $n_v\epsilon_v = \text{in}(f_v\epsilon_v)$. Da diese Terme sich gegenseitig nicht kürzen, schliesslich befinden wir uns in einer direkten Summe, gilt $\text{in}\left(\sum f_v\epsilon_v\right) = n_i\epsilon_i$ für ein i. Sei $\sigma = \sum' n_v\epsilon_v$ die Summe über alle Indices v für die gilt $n_v \, \text{in}(g_v) = n_i \, \text{in}(g_i)$ bis auf Skalarmultiplikation. Alle Indices v in dieser Summer sind $\geq i$, da wir angenommen haben, dass $n_i\epsilon_i$ der initiale Term von τ ist.
Deshalb ist σ eine Syzygie auf den $\in (g_v)$ mit $v \geq i$. Aus 7 folgt, dass alle solche Syzygien von den σ_{uv} für $u, v \geq i$, und die σ_{uv} , in denen ϵ_i vorkommen, sind die σ_{ij} mit $j > i$. Daraus folgt, dass die Koeffizienten n_i in dem von den m_{ji} erzeugten Ideal liegt, für $j > i$ und damit folgt die Behauptung. $\square$

Dieser komplette Vortrag mit allen LaTeX Documenten findet sich unter [2].

Literatur

[1] David Eisenbud. *Commutative Algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[2] Jens Heinrich. Talk-algebraic-geometry. `https://github.com/927589452/Talk-Algebraic-Geometry`, 2017.

[3] Structure theorem for finitely generated modules over a principal ideal domain. `https://en.wikipedia.org/wiki/`. `Structure_theorem_for_finitely_generated_modules_over_a_principal_ideal_domain`.

[4] Syzygy. `http://mathworld.wolfram.com/Syzygy.html`. Accessed: 2017-01-04.