1 Einleitung

In diesem Vortrag geht es vorallem um Syzygien und Freie Auflösungen, was der Title nahe legt. Was der Title aber nicht erfüllen kann, ist es uns einen Grund zu geben 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 ( ). 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

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

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

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

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 $n < \inf$ 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.

Nur für Expose Hier eine kurze Auffrischung der Begrifflichkeiten:

Definition 2 (Freier Modul [1]0.3). Ein freier R-Modul ist ein Modulm 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**

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \ldots \text{ als abelsche Gruppen,}$$

sodass

$$R_i R_j \subset R_{i+1} \mathbf{for} i, j \geq 0.$$

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

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

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 loesen

2 Das Hilbertsche Syzygientheorem

Theorem 3 (Das Hilberstsche Syzygien Theorem [1]1.13)**.** *Wenn $R = l[x_1, \dots, x_r]$ 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 □

Theorem 5 (Struktursatz für endlich erzeugte Moduln über Hauptidealringen [2])**.**

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 Gröbner Basen

Definition 4 (Initialer Term [1]325)**.** Wenn $>$ eine Ordnung auf Mononomen 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 7. Sei $>_{lex}$ Die Ordung in der gilt $x > y$, dann ist $\mathrm{in}_{>_{lex}}\left(x^2 + xy + y^2\right) = x^2$

Definition 5 (Gröbnerbasis [1]328)**.** Eine **Gröbnerbasis** bezüglich einer Ordnung $>$ auf einem freien Modul mit Basis F ist eine Menge von Elementen $g_1, dots, g_t$ in F ,sodass wenn M ein Untermodul von F erzeugt von $g_1, \dots, g_t$ ist, gilt, dass die $\mathrm{in}_>(g_1), \dots, \mathrm{in}_>(g_t)$ $\mathrm{in}_>(M)$ erzeugen.
Wir sagen dann, dass $g_1, \dots, g_t$ eine **Gröbnerbasis von** M sind.

Proposition-Definition 8 ([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 $(\in (g_1), \ldots, \mathrm{in}(g_t))$ 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 $g_1, \ldots, d_t$ 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, falls

$$f'_p := f - \sum_{u=1}^{p} m_u g_{s_u} \neq 0$$

und m der maximale Term von f'_p, der durch eines der der $in\,(g_i)$ teilbar ist,

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

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

Notation 1 ([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

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

entsprechen.
Für jedes Indexpaar i, j, sodass $\mathrm{in}\,(g_i)$ und $\mathrm{in}\,(g_j)$ dasselbe Basiselement von F enthalten, definieren wir

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

und setzen

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

. Diese σ_{ij} Erzeugen die Syzygie auf den $\mathrm{in}\,(g_i)$ nach 11. 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 $\mathrm{in}\left(f_u^{ij} g_u\right) < \mathrm{in}\,(m_{ji} g_i)$ Zur Vereinfachung setzen wir $h_{ij} = 0$, falls $\mathrm{in}\,(g_i)$ und $\mathrm{in}\,(g_j)$ verschiedene Basiselemente von F enthalten.

Theorem 9 (Buchberger Kriterium [1]15.8)**.** *Mit der Notation aus 1 folgt, dass die $g_1, \ldots, g_t$ eine Gröbnerbasis bilden, genau dann wenn h_{ij} für alle i und j.*

Beweis. REPLACE ME □

Algorithmus 2 (Buchberger Algorithmus [1]333)**.** Unter den Vorraussetzungen aus 9 sei M, das ein Untermodul von F und $g_1, \ldots, g_t$ seien Erzeuger von M. 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 wiederholen 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, und damit 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

$$\begin{aligned} r =& \text{number of variables} \\ d =& \text{maximum degree of the polynomials } g_i \text{ , and} \\ s =& \text{the degree of the Hilbert polynomial} \\ & \text{(this is one less than the dimension; it is between 0 and } r-1 \text{).} \end{aligned}$$

Definition 6 ([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 $in\left(g_i\right)$ und $in\left(g_j\right)$ dasselbe Basiselement von F enthalten.

Theorem 10 (Schreyer [1][15.10])**.** *With the notation as above, suppose that $g_1, \ldots, g_t$ is a Gröbner basis. Let $>$ be the monomial order on $\oplus_{j=1}^t S\epsilon_j$ defined by taking $m\epsilon_u > n\epsilon_v \iff$*

$$\in (mg_u) > \in (ng_v) \text{ with respect to the given order on} F$$

or

$$\in (mg_u) = \in (ng_v) \text{ (up to a scalar) but} u < v.$$

The τ_{ij} generate the syzygies on the g_i. In fact, the τ_{ij} are a Gröbner basis for the syzygies with respect to the order $>$, and $\in(\tau_{ij}) = m_{ji}\epsilon_i$.

Beweis. We show first that the initial term of τ_{ij} is $m_{ji}\epsilon_i$. We have

$$m_{ji} \in (g_i) = m_{ij} \in (g_j),$$

and these terms are by hypothesis greater than any that appear in the $f_u^{(ij)} g_u$. Thus, $\in(\tau_{ij})$ is either $m_{ji}\epsilon_i$ or $-m_{ij}\epsilon_j$ by the first part of the definition of $>$, and since $i < j$ we have $m_{ji}\epsilon_i > m_{ij}\epsilon_j$.
Now we show that the τ_{ij} form a Gröbner basis. Let $\tau = \sum f_v \epsilon_v$ be any syzygy. We must show that $\in(\tau)$ is divisable by one of the $\in(\tau_{ij})$; that is, $\in(\tau)$ is a multiple of some $m_{ji}\epsilon_i$ with $i < j$. For each index v, set $n_v\epsilon_v = \in(f_v\epsilon_v)$. Since these terms cannot cancel with each other, we have $\in\left(\sum f_v\epsilon_v\right) = n_i\epsilon_i$

for some i. Let $\sigma = \sum' n_v \epsilon_v$ be the sum over all indices v for which $n_v \in (g_v) = n_i \in (g_i)$ up to a scalar; all indices v in this sum must be $\geq i$ because we assume that $n_i \epsilon_i$ is the initial term of τ. Thus, σ is a syzygy on the $\in (g_v)$ with $v \geq i$. By 11 , all such syzygies are generate by the σ_{uv} for $u, v \geq i$, and the ones in which ϵ_i, appears are the σ_{ij} for $j > i$. It follows that the coefficient n_i is in the ideal generated by the m_{ji} for $j > i$, and we are done. □

4 Syzygientricks

Notation 2 ([1]322)**.** Sei F ein freies Modul mit Basis und M Untermodul von F der von $m_1, \ldots, m_t$ erzeugt wird. Sei

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

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

$$m_{ij} := m_i / \operatorname{GCD}\left(m_i, m_j\right)$$

, wobei wir die σ_{ij} wie folgt als Elemente von $\ker \phi$ definieren:

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

Lemma 11 ([1]15.1)**.** Mit der Notation 2 gilt, dass $\ker \phi$ von den σ_{ij} erzeugt wird.

Beweis. $\ker \phi$ ist ein k-Vektorraum , also können wir annehmen, dass $\ker \phi = \underset{n \in F}{\oplus}$, wobei

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

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 $\left(\ker \phi\right)_n$. Nehmen wir an, dass $\sigma = \sum a_v n_v^{\epsilon} \left(\ker \phi\right)_n$. 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

$$\operatorname{LCM}\left(m_i, m_j\right) / m_i = m_j / \operatorname{GCD}\left(m_i, m_j\right) = m_{ji}$$

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

Lemma 12 ([1]323)**.** Mit der Notation aus 11 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 $\operatorname{LCM}\left(m_i, m_j\right) | n$ und n_{ij} ein Vielfaches von $n / \operatorname{LCM}\left(m_i, m_j\right) = n_i / m_{ji}$ ist, summieren.

Beweis. Die Eindeutigkeit folgt aus 11. Da wir im letzten Schritt des obigen Beweises nur Terme entfernen, können wir die σ_{ij} von dort nehmen. $\square$

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

Literatur

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

[2] 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`.

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