Seminar über Kommutative Algebra: Gröbnerbasen und Regularität

Generic Freeness

Universität Regensburg
Fakultät Mathematik

Florian Seidl
Regensburg, November 2016

10 Fibers and Images of Morphisms Revisited

In dieser Ausarbeitung wird das Kapitel 10 aus dem Buch “A Course in Commutative Algebra“ von Gregor Kemper behandelt. Als Erstes wird die in den vorangegangenen Kapiteln und Vorträgen eingeführte Theorie der Gröbnerbasen genutzt, um das generic freeness lemma zu beweisen. Dies führt dann zu einem Algorithmus zur Bestimmung des Bildes eines Morphismus von affinen Varietäten. Im Anschluss wird dies theoretischer im Hinblick auf die Bilder von Morphismen und die Dimension von Fasern betrachtet. Zum Schluss werden die erarbeiteten Ergebnisse auf die Invariantentheorie angewandt. Diese Ausarbeitung beschränkt sich auf den ersten Teil des Kapitels und es wird hauptsächlich der zuvor genannte Algorithmus betrachtet. Es werden hin und wieder Teile aus Kapitel 7 aufgegriffen, die an entsprechender Stelle nochmals erläutert werden, da Kapitel 7 nicht Teil des Seminars ist.
Im Hinblick auf unser Seminar steht das Kapitel 10 relativ alleine. Was hier erarbeitet wird, findet keine Verwendung mehr, ist aber allgemein für die Algebraische Geometrie von Bedeutung.

10.1 The Generic Freeness Lemma

Grob gesagt sagt das generic freeness lemma aus, dass unter geeigneten Hypothesen eine Ringerweiterung, nachdem fast überall lokalisiert wurde, zu einem freien Modul wird. Das folgende Lemma ist eine Vorbereitung auf die eigentliche Version des generic freeness lemma. Dabei sollte Proposition 9.18 aus dem Buch von Kemper, die auch im vorangegangenen Vortrag behandelt wurde, im Kopf behalten werden. Darin wird für den Fall von affinen Algebren erklärt, wie die Gröbnerbasis im Lemma konstruiert werden kann.

Lemma 10.1 (generic freeness, Aufbauversion)**.** *Sei $R \subseteq S$ eine endlich erzeugte Ringerweiterung mit Epimorphismus $\psi : R[x_1, \dots, x_n] \to S$. Sei $G \subseteq R[x_1, \dots, x_n]$ eine Gröbnerbasis von ker(ψ) bzgl. einer monomialen Ordnung. Ist $U \subseteq R$ eine multiplikative Teilmenge, die das Produkt $\prod_{g \in G} LC(g)$ enthält, so ist $U^{-1}S$ frei als $U^{-1}R$-Modul und es existiert eine Basis, die $1 \in U^{-1}S$ enthält.*

Bemerkung: Ist R kein Integritätsbereich, so ist es möglich, dass das Produkt $\prod_{g \in G} LC(g)$ null wird. Dies hängt damit zusammen, dass dann Nullteiler auftreten könnten. Das Lemma wäre dann bedeutungslos.

Bemerkung: Neu ist hier die Betrachtung der Thematik über Ringen. In Kapitel 9 des Buches bzw. im ersten Vortrag wurden immer Körper betrachtet. Die meisten dieser anfänglichen Definitionen, Propositionen, etc. können aber auch analog über beliebigen Ringen definiert werden. Bei Algorithmus 9.8 muss lediglich ein Schritt angepasst werden. Schritt (6) wird dabei zu

$$(6') \quad f^* := LC(g_i) \cdot f^* - \frac{ct}{LM(g_i)} \cdot g_i \quad \text{und} \quad h_i := LC(g_i) \cdot h_i + \frac{ct}{LM(g_i)}$$

Durch diese Modifikation wird verhindert, dass Nullteiler Probleme bereiten.
Theorem 9.9 und Korollar 9.10 gelten nicht über beliebigen Ringen, weswegen der Begriff Gröbnerbasis in diesen Fällen manchmal etwas irreführend ist. Gröbnerbasen über Ringen kommen nur in Proposition 9.18 und Lemma 10.1 vor. Später werden wieder Körper betrachtet.

Nun kommen wir zum Beweis des Lemmas.

Beweis. Sei $B \subset R[x_1, \dots, x_n]$ die Menge aller Monome, die nicht durch ein $LM(g)$, $g \in G$, teilbar sind. Aus der Injektivität von ψ auf R folgt $1 \in B$. Außerdem ist $\psi(B) \subseteq S$ linear unabhängig über R, da falls $\sum_{i=1}^m a_i \psi(t_i) = 0$ für $t_1, \dots, t_m \in B$ paarweise disjunkt und $a_i \in R$, so folgt $h := \sum_{i=1}^m a_i t_i \in ker(\psi)$, also $h = 0$, da kein Monom von h durch ein $LM(g)$, $g \in G$, teilbar ist.
Dabei ist eingegangen, dass G eine Gröbnerbasis auf dem Kern ist und unsere Argumentation folgt direkt aus der Definition von Gröbnerbasis.
Sei nun $M := (\psi(B))_R \subseteq S$ der von $\psi(B)$ erzeugte freie R-Modul.
Zwischenbehauptung: für jedes $s \in S$ existiert ein $u \in U$, so dass $us \in M$
Zwischenbeweis: Nehme $f \in R[x_1, \dots, x_n]$ mit $s = \psi(f)$. Aus 9.8 in Verbindung mit 9.11 (Anpassung des Algorithmus) folgt die Existenz eines $f^* \in R[x_1, \dots, x_n]$, das eine Normalform eines $u \cdot f$ bzgl. G ist, wobei u das Produkt aus Leitkoeffizienten von Elementen aus G ist. Durch Multiplikation von u mit weiteren Leitkoeffizienten von Elementen aus G können wir erreichen, dass u eine Potenz von $\prod_{g \in G} LC(g)$ ist, also $u \in U$.
Diese Beweisschritte folgen direkt aus 9.8 und 9.11.
Aus der Definition der Normalform folgt, dass f^* in $(B)_R$ liegt und $u \cdot f - f^* \in (G)_{R[x_1,\dots,x_n]} \subseteq ker(\psi)$. Also

$$u \cdot s = u \cdot \psi(f) = \psi(u \cdot f) = \psi(f^*) \in M.$$

Somit ist die Zwischenbehauptung bewiesen.
Man sieht nun noch leicht, dass $\tilde{B} := \{\frac{\psi(t)}{1} | t \in B\} \subseteq U^{-1}S$ eine Basis von $U^{-1}S$ als $U^{-1}R$-Modul ist. □

Kombiniert man nun Lemma 10.1 mit Proposition 9.18 und Lemma 7.16, so erhalten wir einen Algorithmus zur Bestimmung des Bildes eines Morphismus zwischen den Spektren von affinen Algebren (wobei dies im Falle eines algebraisch abgeschlossenen Grundkörpers, auf den Fall Bestimmen des Bildes eines Morphismus von affinen Varietäten zurückgeführt werden kann). Die Aussage von 7.16 wird an entsprechender Stelle noch erwähnt. Zunächst benötigen wir noch die Existenzversion des generic freeness lemma.

Korollar 10.2 (Generic freeness lemma)**.** *Sei R ein Integritätsbereich und S eine Ringerweiterung von R, die endlich erzeugt als R-Algebra ist. Dann existiert ein Element $0 \neq a \in R$, so dass für jede multiplikative Teilmenge $U \subseteq R$ mit $a \in U$, die Lokalisierung $U^{-1}S$ frei als $U^{-1}R$-Modul ist und eine Basis existiert, die $1 \in U^{-1}S$ enthält.*

Beweis. Wir haben einen Epimorphismus $\psi : R[x_1, \ldots, x_n] \to S$. Sei $I := ker(\psi), K := Quot(R), J := (I)_{K[x_1,\ldots,x_n]} = K \cdot I$. Wähle eine monomiale Ordnung auf $K[x_1, \ldots, x_n]$ und sei $G \subseteq J \setminus \{0\}$ eine Gröbnerbasis von J. Durch Multiplikation der Polynome in G mit geeigneten Elementen ungleich null aus R, ist es möglich, dass G in I liegt, also ist G eine Gröbnerbasis von I. Wählt man $a := \prod_{g \in G} LC(g) \in R \setminus \{0\}$, so folgt die Behauptung mit Lemma 10.1. □

Grob gesagt ist die Aussage von Korollar 10.2, dass freeness „fast überall“ erhalten bleibt. Im Buch von Gregor Kemper ist von „freeness holds almost everywhere“ die Rede. Genauer gesagt ist damit gemeint, dass freeness, nach Lokalisierung an allen Primidealen P aus dem Spektrum von R, erhalten bleibt, wobei das im Korollar auftauchende a nicht in P liegt. Das generic freeness lemma geht auf Grothendieck zurück und wurde ursprünglich auch generic flatness lemma genannt. Flatness ist etwas schwächer als freeness und wird im Buch von Kemper und auch in unserem Seminar nicht behandelt. Wir kommen nun zum Algorithmus zur Bestimmung des Bildes eines Morphismus $\varphi^* : Spec(A) \to Spec(B)$ von Spektren von affinen Algebren. B als Quotientenring eines Polynomringes zu definieren, ist dasselbe wie eine Einbettung $Spec(B) \hookrightarrow Spec(K[x_1, \ldots, x_n])$ anzugeben. Wir können also annehmen, dass B ein Polynomring ist. Im Folgenden sind $K[x_1, \ldots, x_n]$ und $K[y_1, \ldots, y_m]$ Polynomringe über einem Körper.

Algorithmus 10.3 (Bild eines Morphismus von Spektren)**.**
Input: Ein Ideal $I \subseteq K[y_1, \ldots, y_m]$, das eine affine Algebra $A := K[y_1, \ldots, y_m]/I$ definiert und Polynome $g_1, ..., g_n \in K[y_1, \ldots, y_m]$, die einen K-Algebren-Homomorphismus $\varphi : K[x_1, \ldots, x_n] \to A,\ x_i \mapsto g_i + I$ definieren.
Output: Ideale $J_1, \ldots, J_l \subseteq K[x_1, \ldots, x_n]$ und Polynome $f_1, \ldots, f_l \in K[x_1, \ldots, x_n]$, so dass das Bild des induzierten Morphismus $\varphi^* : Spec(A) \to Spec(K[x_1, \ldots, x_n]) =: Y$ durch

(10.1)
$$im(\varphi^*) = \bigcup_{i=1}^{l} \Big(\mathcal{V}_Y(J_i) \setminus \mathcal{V}_Y(f_i)\Big)$$

und der Abschluss durch

(10.2)
$$\overline{im(\varphi^*)} = \mathcal{V}_Y(J_1)$$

gegeben ist.
(1) Wähle monomiale Ordnungen “$\leq_x$“ auf $K[x_1, \ldots, x_n]$ und “$\leq_y$“ auf $K[y_1, ..., y_m]$

und sei “$\leq$“ die Blockordnung auf $K[x_1, \dots, x_n, y_1, \dots, y_m]$*, wobei “$\leq_y$“ dominiert.*
(2) Bilde das Ideal

$$J := (I \cup \{g_1 - x_1, \dots, g_n - x_n\})_{K[x_1,\dots,x_n,y_1,\dots,y_m]}$$

und bestimme die Gröbnerbasis G *von* J *bzgl. “$\leq$“.*
(3) Setze

$$G_x := K[x_1, \dots, x_n] \cap G, \quad G_y := \{NF_{G_x}(g) \mid g \in G\} \setminus \{0\}$$

und

$$M := \{LC_y(g) \mid g \in G_y\} \setminus K \subseteq K[x_1, \dots, x_n].$$

$LC_y(g)$ *bezeichnet den Leitkoeffizienten von* g *bzgl. “$\leq_y$“, aufgefasst als Polynom in* y_i*-Variablen.*
(4) Initialisiere die Listen $J_1, \dots, J_l$ *und* $f_1, \dots, f_l$ *durch setzen von* $l = 1$*,*

$$J_1 := (G_x)_{K[x_1,\dots,x_n]} \text{ und } f_1 := \prod_{f \in M \cup \{1\}} f$$

(5) Führe Schritt (6) *für alle* $f \in M$ *durch.*
(6) Führe den Algorithmus rekursiv mit $(I \cup \{f(g_1, \dots, g_n)\})_{K[y_1,\dots,y_m]}$ *als erstes Argument und* $g_1, \dots, g_n$ *als zweites Argument aus. Füge die resultierenden Listen von Idealen und Polynomen den aktuellen Listen* $J_1, \dots, J_l$ *und* $f_1, \dots, f_l$ *hinzu.*

Theorem 10.4. *Algorithmus* 10.3 *endet nach endlich vielen Schritten und berechnet das Bild und den Abschluss von* φ^* *korrekt.*

Beweis. Nutze die Notation aus dem Algorithmus. Wir beweisen durch Widerspruch.
Annahme: Es existiert ein Ideal $I \subseteq K[y_1, \dots, y_m]$, so dass der darauf angewandte Algorithmus nicht nach endlich vielen Schritten endet. Nach Hilberts Basis Theorem 2.13 können wir annehmen, dass I maximal mit dieser Eigenschaft ist. Da alle Schritte außer (6) offensichtlich nach endlich vielen Schritten enden, existiert ein $f = LC_y(g) \in M$ (mit $g \in G_y$), so dass Schritt (6) für f nicht endet . Die Maximalität von I impliziert $f(g_1, \dots, g_n) \in I$, also $f \in J$ nach der Definition von J. Da $f \in K[x_1, \dots, x_n] \setminus \{0\}$, liefert uns Theorem 9.16 ein $g' \in G_x$, dessen Leitmonom $LM(f)$ teilt. Dieser Beweisschritt ist so direkt im Beweis von 9.16 nachzulesen. Da “$\leq$“ eine Blockordnung ist, gilt $LM(g) = LM_y(g) \cdot LM(f)$, also teilt $LM(g')$ auch $LM(g)$. Dies ist ein Widerspruch dazu, dass alle $g \in G_y$ in Normalform bzgl. G_x sind. Diese Argumentation folgt direkt aus der Definition von Normalform.
Somit ist die Endlichkeit des Algorithmus bewiesen.
Wir zeigen nun die Richtigkeit.
Die Richtigkeit von (10.2) folgt aus (9.10)

(9.10)
$$\overline{im(\varphi^*)} = \mathcal{V}_{Spec(R)}(ker(\varphi)),$$

Proposition 9.17 und Theorem 9.16. Mit den Aussagen über die Gröbnerbasis aus 9.16 und der Beschreibung des Kerns aus 9.17 sieht man schnell, dass 10.2 folgt.
Um 10.1 zu beweisen betrachten wir die Zerlegung

(10.3)
$$im(\varphi^*) = \Big((im\varphi^*) \setminus \mathcal{V}_Y(f_1)\Big) \cup \bigcup_{f \in M} \Big(im(\varphi^*) \cap \mathcal{V}_Y(f)\Big).$$

Diese Zerlegung folgt aus der Definition von f_i aus Schritt (4). Wir stellen nun eine Zwischenbehauptung auf.
Zwischenbehauptung:

(10.4)
$$im(\varphi^*) \setminus \mathcal{V}_Y(f_1) = \mathcal{V}_Y(J_1) \setminus \mathcal{V}_Y(f_1).$$

Zwischenbeweis:

" $\subseteq$ "

Man sieht leicht $im(\varphi^*) \setminus \mathcal{V}_Y(f_1) \subseteq \overline{im(\varphi^*)} \setminus \mathcal{V}_Y(f_1) \overset{(10.2)}{=} \mathcal{V}_Y(J_1) \setminus \mathcal{V}_Y(f_1)$.

" $\supseteq$ "

Nehme umgekehrt ein $P \in \mathcal{V}_Y(J_1) \setminus \mathcal{V}_Y(f_1)$. Wir benutzen die Notation aus Proposition 9.18. Mit

(9.12)
$$LC(\Phi(f)) = \varphi(LC_y(f))$$

erhalten wir

$$\prod_{g \in G_y} LC(\Phi(g)) \overset{(9.12)}{=} \prod_{g \in G_y} \varphi(LC_y(g)) = \varphi(cf_1) \in \varphi(K[x_1, \dots, x_n] \setminus P) =: U,$$

wobei $c \in K \setminus \{0\}$. Die Definition von G_y in (3) liefert $\Phi(G_y) = \Phi(G \setminus G_x) \setminus \{0\}$, also folgt mit Proposition 9.18 *c*), dass $\Phi(G_y)$ eine Gröbnerbasis von $ker(\psi)$ ist. Dies ist eine direkte Aussage aus 9.18 *c*). Aus 10.1 folgt nun, dass $U^{-1}A$ frei als $U^{-1}R$-Modul ist und eine Basis existiert, die 1 enthält.
Lemma 7.16 sagt aus, dass die Abbildung $Spec(U^{-1}A) \to Spec(U^{-1}R)$ surjektiv ist (direkte Aussage dieses Lemmas). Mit Theorem 6.5 (gibt Aussagen über das Spektrum von Ringen) liefert dies, dass für jedes $\mathfrak{p} \in Spec(R)$ mit $U \cap \mathfrak{p} = \emptyset$ ein $Q \in Spec(A)$ mit $R \cap Q = \mathfrak{p}$ existiert. Insbesondere erfüllt $\mathfrak{p} := \varphi(P) \in Spec(R)$ die Bedingung $U \cap \mathfrak{p} = \emptyset$, da sonst ein $h \in P$ und ein $u \in K[x_1, \dots, x_n] \setminus P$ mit $\varphi(h) = \varphi(u)$ existieren würde. Dies führt zu dem Widerspruch $u = (u - h) + h \in ker(\varphi) + P = P$, da $ker(\varphi) = J_1 \subseteq P$. Wir haben also $Q \in Spec(A)$ mit $R \cap Q = \mathfrak{p} = \varphi(P)$ und dies ist äquivalent zu $P = \varphi^{-1}(Q)$. Also ist $P \in im(\varphi^*) \setminus \mathcal{V}_Y(f_1)$ und unsere Zwischenbehauptung ist bewiesen.

Durch Induktion über die Rekursionstiefe können wir annehmen, dass für jedes $f \in M$ die Rekursion des Algorithmus das Bild von φ_f^* berechnet, wobei $\varphi_f : K[x_1, \dots, x_n] \to A/(\varphi(f))_A$ durch $x_i \mapsto \varphi(x_i) + (\varphi(f))_A$ gegeben ist. Mit (10.3) und (10.4) genügt es

(10.5)
$$im(\varphi^*) \cap \mathcal{V}_Y(f) = im(\varphi_f^*)$$

zu zeigen.
Tatsächlich besteht $im(\varphi_f^*)$ aus allen $P \in Spec(K[x_1, \dots, x_n])$, so dass $P = \varphi_f^{-1}(\mathfrak{q})$ mit $\mathfrak{q} \in A/(\varphi(f))_A$. Diese Bedingung ist äquivalent zu $P = \varphi^{-1}(Q)$ mit $Q \in Spec(A)$, $\varphi(f) \in Q$. Dies ist wiederum äquivalent zu $P = \varphi^{-1}(Q)$ und $f \in P$, d.h. $P \in im(\varphi^*) \cap \mathcal{V}_Y(f)$. Dies zeigt (10.5) und der Beweis ist vollständig.

$\square$

Algorithmus 10.3 *berechnet das Bild eines Morphismus $f : X \to Y$ von affinen Varietäten über einem algebraisch abgeschlossenen Körper K. Tatsächlich ist Y (genau wie X) eingebettet in ein K^n. Zur Berechnung des Bildes nehmen wir also $Y = K^n$ an. f induziert einen Homomorphismus $\varphi : K[x_1, \dots, x_n] \to K[X] =: A$. Anwenden von Algorithmus* 10.3 *auf φ liefert $J_1, \dots, J_l \subseteq K[x_1, \dots, x_n]$ und $f_1, \dots, f_l \in K[x_1, \dots, x_n]$, so dass*
$$im(\varphi^*) = \bigcup_{i=1}^{l} \left(\mathcal{V}_{Spec(K[x_1,\dots,x_n])}(J_i) \setminus \mathcal{V}_{Spec(K[x_1,\dots,x_n])}(f_i) \right)$$
Mit Algebraischer Geometrie folgt daraus
$$im(f) = \bigcup_{i=1}^{l} \left(\mathcal{V}_{K^n}(J_i) \setminus \mathcal{V}_{K^n}(f_i) \right).$$

Literaturverzeichnis

[1] Kemper, Gregor. , *A Course in Commutative Algebra* , Springer, 31.03.2009