Folgerungen aus dem Theorem von Golod - Schafarevich

Seminarausarbeitung

Vorgelegt von

Alina Eichhorst

aus Düsseldorf

Angefertigt am
Mathematischen Institut
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

9. Januar 2018

Betreuer: Prof. Dr. Oleg Bogopolski

1 Beispiel 1

Satz 1.1. *Haben wir alle Notationen, wie in Theorem* 2.4 (G-S) *(siehe Appendix* (5.5)*) gegeben und es gilt*

$$r_n \leq \epsilon^2(d-2\epsilon)^{n-2}$$

mit $\epsilon > 0$ *und* d *als Anzahl der nicht kommutativen Variablen, so ist die Algebra* F/I *unendlich-dimensional.*

Beweis. Um dies zu verifizieren, genügt es, zu zeigen, dass die Koeffizienten der Potenzreihe σ^{-1} alle positiv sind. Dabei hat σ folgende Gestalt:

$$\sigma = 1 - dt + \sum_{n=0}^{\infty} \epsilon^2(d-2\epsilon)^{n-2}t^n.$$

Um die Koeffizienten zu überprüfen, betrachten wir die bekannten Darstellungen der geometrischen Reihe mit Koeffizienten eins:

$$\frac{1}{1-a} = \sum_{n=0}^{\infty} a^n$$

Diese wollen wir nun quadrieren, um eine für uns hilfreiche Darstellung zu finden.

$$\frac{1}{(1-a)^2} = (\sum_{n=0}^{\infty} b_n a^n)^2, \quad \text{mit } b_n = 1 \quad \forall n.$$

$$= \sum_{n=0}^{\infty} c_n a^n,$$

wobei

$$c_n = \sum_{i=0}^{n} b_{n-i}b_i = n+1$$

$$\Rightarrow \frac{1}{(1-a)^2} = \sum_{n=0}^{\infty}(n+1)a^n.$$

Wenden wir diese auf σ an, so erhalten wir

$$\sigma = 1 - dt + \epsilon^2t^2 \sum_{n=0}^{\infty}(d-2\epsilon)^n t^n$$

$$= 1 - dt + \frac{\epsilon^2t^2}{1-(d-2\epsilon)t}$$

$$= \frac{(1-d)(1-(d-2\epsilon)t)}{(1-(d-2\epsilon)t)} + \frac{\epsilon^2t^2}{1-(d-2\epsilon)t}$$

$$= \frac{1-(d-2\epsilon)t - dt + dt(d-2\epsilon)t + \epsilon^2t^2}{1-(d-2\epsilon)t}$$

$$= \frac{1-dt+2t\epsilon - dt + d^2t^2 - 2d\epsilon t^2 + \epsilon^2t^2}{1-(d-2\epsilon)t}$$

$$= \frac{1-2(d-\epsilon)t + (d-\epsilon)^2t^2}{1-(d-2\epsilon)t}$$

$$= \frac{(1-(d-\epsilon)t)^2}{1-(d-2\epsilon)t}$$

und damit für σ^{-1}

$$\sigma^{-1} = \frac{1-(d-2\epsilon)t}{(1-(d-\epsilon)t)^2} = (1-(d-2\epsilon)t)\sum_{n=0}^{\infty}(n+1)(d-\epsilon)^n t^n$$

$$= (1-(d-\epsilon)t+\epsilon t)\sum_{n=0}^{\infty}(n+1)(d-\epsilon)^n t^n$$

$$= \left(\sum_{n=0}^{\infty}(n+1)(d-\epsilon)^n t^n\right) - \underbrace{\left(\sum_{n=0}^{\infty}(n+1)(d-\epsilon)^{n+1}t^{n+1}\right)}_{=\sum_{n=1}^{\infty} n(d-\epsilon)^n t^n} + \left(\sum_{n=0}^{\infty}\epsilon(n+1)(d-\epsilon)^n t^{n+1}\right)$$

$$= 1 + \sum_{n=1}^{\infty} \underbrace{(d-\epsilon)^n}_{=(d-\epsilon)(d-\epsilon)^{n-1}} t^n + \sum_{n=1}^{\infty}\epsilon n(d-\epsilon)^{n-1}t^n$$

$$= 1 + \sum_{n=1}^{\infty}(d-\epsilon+\epsilon n)(d-\epsilon)^{n-1}t^n$$

$$= 1 + \sum_{n=1}^{\infty}\underbrace{(d-\epsilon)^{n-1}(d+(n-1)\epsilon)}_{\text{Koeffizienten}}t^n.$$

Da $d-2\epsilon \geq 0$ ist, folgt $d-\epsilon \geq \epsilon > 0$. Damit sind in der Tat alle Koeffizienten von σ^{-1} positiv. □

2 Beispiel 2

Nun haben wir alle Voraussetzungen gegeben (und auch bewiesen), um Golod's Konstruktion auszuführen. Der folgende Spezialfall soll die Idee dieser Konstruktion verdeutlichen.

Beispiel 2.1. Es sei K ein Körper mit abzählbar unendlich vielen Elementen, $F = K[x,y]$ die Algebra der Polynome über K in den nicht kommutativen Variablen x und y. F' sei die Subalgebra, die gebildet wird durch die Polynome deren konstante Terme alle gleich null sind.

Wir werden zeigen, dass in F ein (rechts-) Ideal (siehe (5.4)) $I \subseteq F'$ enthalten ist, für das gilt: $A' = F'/I$, $\forall z \in A'$: sie sind nilpotent, aber A' selber ist nicht nilpotent (siehe (5.3)).

Es sei $u_1, u_2, \ldots$ eine Aufzählung der Elemente von F'. Weiter definieren wir eine Folge positiver ganzer Zahlen durch $N_1, N_2, \ldots$, wobei $N_1 = 9$.

Nun potenzieren wir u_1 mit N_1 und zerlegen das entstehende Resultat $u_1^{N_1}$ in die (eindeutige) Summe seiner homogenen Komponenten $f_1, f_2, \ldots, f_{m_1}$. Dabei werden die Summanden in aufsteigender Reihenfolge des Grades aufgeschrieben.

An diesem Punkt definieren wir nun N_2, wie in der Voraussetzung, als beliebige ganze Zahl,

die den höchsten der Grade der $f's$ übersteigt. Mit u_2 und dem gerade gewählten N_2 verfahren wir, wie zuvor mit u_1 und N_1. Dadurch erhalten wir auch wieder eine untere Schranke für N_3.
Setzt man dies immer weiter fort, so erhält man schließlich eine unendliche Folge $f_1, f_2, \ldots$ von Polynomen mit steigendem Grad ≥ 9.

Sei nun I das Ideal, welches von diesen Polynomen in F' erzeugt wird. Da F' von x und y erzeugt wird, erhalten wir: $A' = F'/I$ wird von $\hat{x} = x + I$ und $\hat{y} = y + I$ erzeugt.
Damit wir A' von zwei Elementen erzeugt.
Durch die Art der Konstruktion von I ist ebenfalls sofort klar, dass A' eine Nilalgebra ist (siehe (5.3)).

Es bleibt also nur noch zu zeigen, dass A' selber nicht nilpotent ist und, dass dafür die unendliche Dimension von $A = F/I$ genügt.
Letzteres ist gültig, da $A' = A_1 \oplus A_2 \oplus \ldots$ dann ebenfalls unendlich Dimension haben wird und daher nicht nilpotent ist.

In der Notation von Theorem (5.5) haben wir also $d = 2$, $r_n \leq 1$ (und insbesondere $r_2 = r_3 = ... = r_8 = 0$).

$$\begin{aligned} r_n &\leq \epsilon^2(d - 2\epsilon)^{n-2} \\ &\leq \frac{1}{16}(2 - \frac{1}{2})^{n-2} \\ &\leq \frac{1}{16}(\frac{1}{2})^{n-2} \end{aligned}$$

Für $n = 9$ erhält man dann bereits $\frac{1}{2048} < 1$ und für wachsendes n wird der Nenner immer größer, damit der Bruch immer kleiner und bleibt also immer unter eins.
Diese direkte Berechnung zeigt, dass für $\epsilon = \frac{1}{4}$ die Voraussetzungen von Beispiel 1 erfüllt sind.
Damit folgt, dass A unendlich dimensional ist. Und insbesondere auch, dass A' nicht nilpotent ist.

3 Beispiel 3

Nach diesem konkreten Beispiel geben wir nun Golod's Konstruktion allgemein an.

Satz 3.1. *Für jede ganze Zahl $d \geq 2$ und jeden Körper K existiert eine nicht-nilpotente, assoziative K-Algebra, die von d Elementen erzeugt wird, deren Subalgebren, welche von $(d-1)$ Elementen erzeugt werden, nilpotent sind.*

Beweis. Sei $F = K[x_1, \ldots, x_d]$ wie zuvor in Theorem 2.4, F' die Subalgebra, die durch alle Polynome mit konstantem Term null erzeugt wird (vgl. *Beispiel* 2).
Wir konstruieren ein Ideal I von F, enthalten in F', sodass F'/I unsere gewünschten Eigenschaften erfüllt.
Es sei ϵ eine feste Zahl zwischen 0 und $\frac{1}{2}$.
Mit Rückblick auf *Beispiel* 1 können wir für I das Ideal wählen, welches von den homogenen Polynomen $f_1, \ldots, f_{s_1}, f_{s_1+1}, \ldots, f_{s_2}, \ldots$ vom Grad ≥ 2 erzeugt wird. Dieses erfüllt die Bedingung aus unserem *Beispiel 1* (damit ist die nicht-Nilpotenz sichergestellt), sowie auch die folgende Bedingung (mit dieser gilt nach der Definition: Jede $(d-1)$-erzeugte Unteralgebra

ist nilpotent):

Für jedes Paar $(d-1)$-Elemente von F' mit einem Grad $\leq n$ existiert eine positive ganze Zahl N, sodass jedes Produkt (Wiederholungen erlaubt) von N Faktoren aus den $(d-1)$-Elementen in dem Ideal I_n liegt, welches von $f_1, \ldots, f_{s_n}$ erzeugt wird.

Wir nehmen an, dass $f_1, \ldots, f_s$, $s = s_{n-1}$ bereits so definiert sind, dass sie den Bedingungen genügen. Nun zeigen wir, wie man dies auf $f_1, \ldots, f_t$, $t = s_n$ erweitert.

Betrachten wir hierzu $d-1$ Polynome $g_1, \ldots, g_{d-1}$ vom Grad $\leq n$ aus der Unteralgebra F'. Weiter betrachten wir für ein beliebiges $N \in \mathbb{N}$ ein Produkt aus den gerade gewählten Polynomen $\{g_1, \ldots, g_{d-1}\}$ der Form

$$g = g_{i_1} * \ldots * g_{i_N}.$$

Nun überlegen wir uns zuerst, dass jedes der g_j, $j \in \{1, \ldots, d-1\}$, eine Summe von höchstens n homogenen Polynomen ist.
Dies ist offensichtlich, da die g_j aus F' kommen und somit Polynome mit Konstanter gleich Null sind.

Wir möchten nun das Produkt g ausmultiplizieren und als Summe seiner homogenen Polynome betrachten. Diese homogenen Polynome sollen unsere weiteren fs werden.
Um zu überprüfen, ob diese unseren Bedingungen genügen, schätzen wir ihre Anzahl ab.

Es sei nun m_j die Anzahl von g_j im Produkt g. Nach unserer Vorüberlegung wissen wir, dass die Anzahl der homogenen Komponenten in g kleiner gleich der Anzahl der homogenen Komponenten in $g_1^{m_1} * \ldots * g_{d-1}^{m_{d-1}}$ ist (wegen möglicher Kürzungen). Die kann man sich nun als Ziehung ohne Reihenfolge mit Zurücklegen vorstellen. Für einen solchen Fall kennen wir aus der Stochastik folgendes Lemma:

Lemma 3.2. *Bei einer Kombination mit Wiederholung werden aus n Objekten m ohne Beachtung der Reihenfolge ausgewählt, wobei Wiederholungen erlaubt sind. Die Anzahl solcher Kombinationen ist*

$$\binom{n+m-1}{m} = \binom{m+n-1}{n-1}.$$

Beweis. Der Beweis wird Anhand eines Beispiels verdeutlicht.
Nehmen wir an, wir wollen aus fünf Objekten drei mit Wiederholung und ohne Beachten der Reihenfolge ziehen. Diese Problematik können wir auf eine Tabelle übertragen:

1	2	3	4	5
I		I		I
II			I	
	I	I	I	

Wir verteilen also durch die I in der Tabelle mit fünf Objekten beliebig jeweils drei Plätze. Fasst man die I nun als Nullen und die Trennstriche der Spalten als Einsen auf, so erhält

man für jede Zeile eine entsprechende Kombination:

$$0110110$$
$$0011101$$
$$\underbrace{1010101}_{7 \text{ Stellen}}$$

Die Fragestellung lautet nun also: Wie viele Möglichkeiten gibt es, auf sieben Stellen drei Nullen zu verteilen, die restlichen Stellen werden zu Einsen.
Die Anzahl der insgesamt verfügbaren Stellen setzt sich hierbei aus den drei zu verteilenden Nullen zusammen, sowie den Einsen, deren Anzahl $5-1$ entspricht, da es immer einen Trennstrich weniger, als die Anzahl der Objekte gibt (Nach offensichtlichem Aufbau einer Tabelle).
Für diese Fragestellung kennen wir nun die passende Formel und wissen auch, wie wir die Zahl der Stellen bestimmen. Somit erhalten wir als Anzahl aller Möglichkeiten in unserem Beispiel:

$$\binom{5+3-1}{3}.$$

Da sich das vorgeführte Beispiel für jede beliebige Kombination aus m und n analog durchführen lässt, erhalten wir als allgemeine Formel für die Anzahl möglicher Kombinationen von m aus n Objekten mit Wiederholung und ohne Beachtung der Reihenfolge:

$$\binom{n+m-1}{m}.$$

Für die Gleichheit des Lemmas genügt es die Symmetrie des Binomialkoeffizienten zu zeigen:

$$\binom{n}{m} = \frac{n!}{m! * (n-m)!}$$

$$\frac{n!}{(n-m)! * m!} = \frac{n!}{(n-m)! * (n-(n-m))!}$$
$$= \binom{n}{n-m}$$

□

Für jedes beliebige positive N gibt es $(d-1)^N$ Möglichkeiten Produkte der Länge N der g_i zu bilden.
Damit ist die gesamte Anzahl der homogenen Komponenten in allen so zu erhaltenden g maximal

$$(d-N)^N * \prod_{j=1}^{d-1} \binom{m_j+n-1}{n-1}.$$

Diese lässt sich weiter abschätzen mit

$$(d-1)^N * \prod_{j=1}^{d-1} (m_j+n-1)^{n-1} \leq (d-1)^N * (N+n-1)^{(n-1)(d-1)}.$$

Um nun die Bedingung aus *Beispiel 1* zu erfüllen muss gelten:

$$(d-1)^N * (N+n-1)^{(n-1)(d-1)} \leq \epsilon^2 (d-2\epsilon)^{N-2}.$$

Für großes N lässt sich $N+n-1$ gegen $2N$ abschätzen. Weiter sei $k := (n-1)(d-1)$. Somit erhalten wir

$$(d-1)^N * 2^k * N^k \leq \epsilon^2 (d-2\epsilon)^{N-2}.$$

Es gilt

$$(d-1)^N * 2^k * N^k = (d-2\epsilon)^{N-2} * \underbrace{\left(\frac{d-1}{d-2\epsilon}\right)^{N-2} * (d-1)^2 * 2^k * N^k}_{:=r^{N-2}*C*N^k \quad \text{für} \quad 0<r<1, \quad \text{wegen} \quad 0<\epsilon<\frac{1}{2}}.$$

Es lässt sich (z.B. mit der Regel von l'Hospital) zeigen, dass

$$\lim \frac{r^{N-2}}{N^k} = 0 \quad \text{für} \quad N \to 0$$

ist. Somit ist auch diese Bedingung erfüllt.

□

4 Beispiel 4

Mit dieser Vorarbeit können wir nun auch folgendes eingeschränktes Beispiel betrachten.

Satz 4.1. *Für jedes $d \geq 2$ existiert eine nicht-nilpotente Gruppe (siehe (5.2)), die von d Elementen erzeugt wird und deren von $(d-1)$-Elementen erzeugten Untergruppen alle nilpotent sind.*

Eine solche Gruppe wird, wie im Beweis, aus einer Algebra mit den analogen Eigenschaften konstruiert. Das heißt, von einer (unendlich dimensionalen) nicht-nilpotenten Algebra A mit d Erzeugern, wobei alle ihre Subalgebren, die von $(d-1)$-Elementen erzeugt werden, nilpotent sind.

Beweis. Für unser jetziges Beispiel sei $K = \mathbb{F}_p$, $p \in Prim$.
Weiterhin sei $A = F'/I$, wobei die Komponenten wie in den Beispielen zuvor definiert sind.

Betrachten wir folgende Teilmenge von F/I:

$$1 + A = \{1 + a \quad | \quad a \in A\}.$$

Offensichtlich gilt:

$$(1+a)(1+b) = 1 + \underbrace{a + b + ab}_{\in A}.$$

Wenn $a^n = 0$, dann

$$(1+a)^{-1} = 1 - a + a^2 - \ldots + (-1)^{n-1} a^{n-1},$$

sodass $1 + A$ eine Gruppe ist. Dies ist ein Iverses, da

$$(1+a)(1+a)^{-1} = (1+a)(1-a+a^2-a^3+\ldots+(-1)^{n-1}a^{n-1}) + (a-a^2+\ldots+(-1)^{n-1}a^n) = 1.$$

Da weiter für jedes $a \in A$ ein m existiert mit $a^{p^m} = 0$ folgt aus dem binomischen Lehrsatz

$$(1+a)^{p^m} = \sum_{i=0}^{p^m} \binom{p^m}{i} a^i$$

$$= \ldots = \binom{p^m}{0} a^0 + \binom{p^m}{p^m} a^{p^m} = a^0 a^{p^m} = a^0 = 1,$$

da alle Binomialkoeffizienten mit der Form $\binom{p^m}{k} = \frac{p^m!}{(p^m-k)!k!}$, den ersten und letzten ausgenommen, durch p teilbar sind.
$\Rightarrow \quad 1 + A$ ist eine p-Gruppe.

Es sei nun G die Untergruppe, die von den Elementen der Form $1 + \hat{x}_1, \ldots, 1 + \hat{x}_d$ erzeugt wird, wobei $\hat{x}_i = x_i + I$ ist.

Es ist klar, dass die Untergruppe, welche von beliebigen $(d-1)$-Elementen aus $1 + A$ (z.B. $1 + a_1, \ldots, 1 + a_{d-1}$, $a_i \in A$) erzeugt wird, in $1 + A^*$ liegt. Dabei ist A^* die Subalgebra, die von $a_1, \ldots, a_{d-1}$ erzeugt wird.

Nach Konstruktion ist A^* nilpotent, dadurch ist auch $1+A^*$ nilpotent. Dies gilt nach folgender Aussage:

Lemma 4.2. *Es sei A ein assoziativer Ring mit 1, B ein Unterring. Wir schreiben B^n für den Unterring, welcher durch alle Produkte $b_1 * \ldots * b_n$, $b_i \in B$ erzeugt wird. Ist B nilpotent, also $B^n = 0$ für einige n, dann ist $G^{<i>} = \{1 + x | \quad x \in B^i\}$ eine Gruppe mit der Ringmultiplikation und es gilt $[G^{<i>}, G^{<j>}] \leq G^{<i+j>}$ (vgl. (5.1)). Es folgt, dass diese Gruppen alle nilpotent vom Grad $\leq n$ sind. (Vgl.[2] S.109)*

Und somit sind auch alle Untergruppen von G, welche $(d-1)$ Erzeuger besitzen, nilpotent. Aber G selber ist nicht nilpotent.

Wäre dies der Fall, so wäre G endlich, nach folgender Aussage:

Lemma 4.3. *Eine periodische, endlich erzeugte, nilpotente Gruppe ist endlich. (Vgl.[2] S.109)*

Dann wären aber auch der Ring über der Gruppe, $K[G]$, und sein natürliches homomorphes Bild $F/I = k \oplus A$ endlich, im Widerspruch dazu, dass die Algebra A unendlich ist. □

5 Appendix

Definition 5.1. Der *Kommutator* einer Gruppe G ist definiert als

$$[g,h] = g^{-1}h^{-1}gh = (hg)^{-1}gh.$$

Dabei sind g und h Elemente der Gruppe G.
In Ringen und assoziativen Algebren hat der *Kommutator* zweier Elemente folgende Gestalt

$$[a,b] = ab - ba.$$

(Vgl.[2] S. 20)

Definition 5.2. (Eine von mehreren äquivalenten Definitionen)
Man definiere für eine Gruppe G die folgende Reihe induktiv

$$L_1(G) := G \quad , \quad L_n(G) := [L_{n-1}(G); G]$$

für $n > 1$. Mit dieser Zuweisung lässt sich die *absteigende Zentralreihe* definieren als

$$G = L_1(G) \geq L_2(G) \geq \ldots \geq L_n(G).$$

G ist *nilpotent*, wenn die absteigende Zentralreihe, für ein $n \in \mathbb{N}$ mit $L_n(G) = 1$ endet. (Vgl.[2] S.106)

Definition 5.3. Eine assoziative Algebra A heißt *nilpotente Algebra*, falls für deren Elemente $a \in A$ ein n existiert, sodass gilt

$$a_1 * \ldots * a_n = 0, \quad \forall a_i \in A, \quad i = 1, \ldots, n.$$

Definition 5.4. Die Menge $I \subset R$, R ein Ring, wird *Linksideal* genannt, falls folgende Bedingungen gelten

- $0_R \in I$
- $\forall a, b \in I: \quad a - b \in I$
- $\forall a \in I$ und $r \in R: \quad ra \in I$.

Gilt anstelle der dritten Bedingung $\forall a \in I, r \in R: \quad ar \in I$, so nennt man I ein *Rechtsideal*. Sind beide Bedingungen erfüllt, so ist I ein (*beidseitiges*) *Integral*. (Vgl.[1] S.35)

Theorem 5.5. *(Wiederholung von Theorem 2.4 Golod-Šafarevič)*
Es sei $F = K[x_1, \ldots, x_d]$ der Polynomring über K in den nicht kommutativen Variablen $x_1, \ldots, x_d$. Weiter seien $f_1, f_2, \ldots$ homogene Polynome aus F vom Grad ≥ 2, angeordnet in nicht absteigender Reihenfolge des Grades. Letztlich sei I das Ideal, welches von diesen fs erzeugt wird. Falls die Anzahl r_n der Polynome des Grades n unter den f_i die Zahl s_n nicht übersteigt, dann ist die Algebra F/I unendlich dimensional. Dabei müssen mit einer Zahl s_n die Koeffizienten der Potenzreihe σ^{-1} alle positiv sein.

$$\sigma = 1 - dt + \sum_{n=0}^{\infty} s_n t^n$$

(Vgl.[2])

6 Quellen

Literatur

[1] Siegfried Bosch. *Algebra*. 8. Auflage. Springer-Spektrum, 2013.

[2] Ju.I. Merzljakov M.I. Kargapolov. *Fundamentals of the Theory of Groups*. Springer-Verlag, 1979.