Der Hilbertsche Nullstellensatz

Robert Wilms

Inhaltsverzeichnis

1 Moduln

Es sei R stets ein kommutativer Ring mit Einselement. Zu einer abelschen Gruppe M erhalten wir den Ring $(\mathrm{End}(M), +, \circ)$ der Gruppenhomomorphismen $G \to G$.

Definition 1.1. *Ein R-Modul ist eine abelsche Gruppe M zusammen mit einem Ringhomomorphismus $R \to \mathrm{End}(M)$. Wir schreiben kurz $r \cdot m$ für die Anwendung des zu $r \in R$ gehörigen Endomorphismus auf $m \in M$.*

Beispiel 1.2. *(a) Für einen Körper K sind die K-Moduln gerade die K-Vektorräume.*

(b) Die Gruppe $\mathrm{Mat}(p \times q, R)$ der $p \times q$ Matrizen mit Einträgen in R mit der gewöhnlichen Multiplikation durch Skalare rA für $r \in R$ und $A \in \mathrm{Mat}(p \times q, R)$ ist ein R-Modul.

(c) Ein Ideal $I \subseteq R$ ist ein R-Modul mit der gewöhnlichen Multiplikation ra im Ring R für $r \in R$ und $a \in I$.

Definition 1.3. *Es seien M, M' zwei R-Moduln.*

(a) Ein Gruppenhomomorphismus $f \colon M \to M'$ heißt R-Homomorphismus, falls $f(rm) = rf(m)$ für alle $m \in M$ und $r \in R$ gilt.

(b) Eine Untergruppe $N \subseteq M$ heißt R-Untermodul, falls $rn \in N$ für alle $r \in R$ und $n \in N$ gilt.

Beispiel 1.4. *(a) Die R-Untermodule von R sind gerade die Ideale von R.*

(b) Für einen R-Untermodul $N \subseteq M$ ist auch M/N durch $r(m+N) = rm + N$ ein Modul und $M \to M/N$ ist ein R-Homomorphismus.

(c) Es sei $S \subseteq M$ eine Teilmenge. Dann ist $RS = \{\sum_{j=1}^{n} r_j s_j \mid n \in \mathbb{N}, s_j \in S, r_j \in R\}$. ein R-Untermodul von M und wird der von S erzeugte R-Untermodul genannt.

Definition 1.5. *Ein R-Modul M heißt endlich erzeugt, falls $M = SR$ für eine endliche Teilmenge $S \subseteq M$ gilt.*

2 Endlichkeitseigenschaften

Lemma 2.1. *Für eine partiel geordnete Menge $(A, \leq)$ sind folgende Aussagen äquivalent:*

(i) Die Menge $(A, \leq)$ erfüllt die aufsteigende Kettenbedingung: Jede aufsteigende Kette $a_1 \leq a_2 \leq a_3 \leq \ldots$ von Elementen $a_j \in A$ wird stationär, das heißt es gilt $a_n = a_{n+1} = \ldots$ für hinreichend großes n.

(ii) Jede nicht-leere Teilmenge $B \subseteq A$ besitzt ein maximales Element, das heißt ein Element $b_0 \in B$, so dass für jedes $b \in B$ mit $b_0 \leq b$ bereits $b_0 = b$ gilt.

Beweis. $(i) \Rightarrow (ii)$: Sei $\emptyset \neq B \subseteq A$. Wähle $b_1 \in B$. Falls b_1 maximal ist, sind wir fertig. Andernfalls gibt es ein b_2 mit $b_2 > b_1$. Wiederholt man dieses Argument, erhält man eine Kette $b_n > b_{n-1} > \cdots > b_2 > b_1$. Nach (i) können wir nicht endlos so fortfahren. Folglich muss irgendwann ein b_j maximal sein.
$(ii) \Rightarrow (i)$: Sei $a_1 \leq a_2 \leq a_3 \leq \ldots$ eine aufsteigende Kette. Die Menge $\{a_1, a_2, \ldots\}$ hat nach (ii) ein maximales Element a_n. Folglich gilt $a_n = a_{n+1} = \ldots$. □

Ersetzt man $\leq$ durch $\geq$, erhält man die *absteigende Kettenbedingung*, welche äquivalent dazu ist, dass jede nicht-leere Teilmenge ein minimales Element besitzt.

Definition 2.2. *(a) Ein topologischer Raum heißt* noethersch, *falls die Menge seiner abgeschlossenen Unterräume die absteigende Kettenbedingung erfüllen.*

(b) Ein Ring heißt noethersch, *falls die Menge seiner Ideale die aufsteigende Kettenbedingung erfüllt.*

(c) Ein R-Modul heißt noethersch, *falls die Menge seiner R-Untermoduln die aufsteigende Kettenbedingung erfüllen.*

Beispiel 2.3. *(a) Jeder Hauptidealring R ist noethersch: Ist $I_1 \subseteq I_2 \subseteq \ldots$ eine aufsteigende Kette von Idealen in R, so ist auch $\bigcup_{s \geq 1} I_s$ ein Ideal von R, somit ein Hauptideal erzeugt von einem $a \in \bigcup_{s \geq 1} I_s$. Ist nun s_0 so, dass $a \in I_{s_0}$, so folgt $I_{s_0} = I_{s_0+1} = \ldots$.*

(b) Jeder Unterraum Y eines noetherschen Raumes X ist noethersch, denn jede Kette von Unterräumen $Y_1 \supseteq Y_2 \supseteq \dots$ von abgeschlossenen Unterräumen Y_j von Y kommt von einer Kette $X_1 \supseteq X_2 \supseteq \dots$ von abgeschlossenen Unterräumen X_j in X mit $X_j \cap Y = Y_j$.

(c) Der Quotient R/I eines noetherschen Rings R und eines Ideals $I \subseteq R$ ist noethersch, denn jede Idealkette $I_1 \subseteq I_2 \subseteq \dots$ von Idealen in R/J kommt von einer Idealkette $J_1 \subseteq J_2 \subseteq \dots$ von Idealen in R mit $J_j/I = I_j$.

Proposition 2.4. *Ein R-Modul M ist genau dann noethersch, wenn jeder R-Untermodul von M ein eindlich erzeugter R-Modul ist.*

Beweis. "$\Rightarrow$": Es sei M noethersch und $N \subseteq M$ ein R-Untermodul. Die Menge der endlich erzeugten R-Untermoduln von M, die zugleich in N liegen, ist nicht leer. Nach Lemma 2.1 besitzt sie daher ein maximales Element N_0. Falls $N_0 \neq N$ gilt, können wir ein $x \in N \setminus N_0$ wählen. Dann ist auch $N_0 + Rx$ endlich erzeugt und in N. Dies widerspricht der Maximalität von N_0. Folglich ist $N = N_0$ und N somit endlich erzeugt. "$\Leftarrow$": Es sei jeder R-Untermodul von M endlich erzeugt. Für eine aufsteigende Kette $N_1 \subseteq N_2 \subseteq \dots$ von R-Untermoduln von M ist $N = \bigcup_{s \geq 1} N_s$ ein R-Untermodul von M. Es sei $S = \{s_1, \dots, s_k\}$ eine erzeugende Menge für N und $j_k \in \mathbb{N}$ so dass $s_k \in N_{j_k}$ und $j = \max\{j_1, \dots, j_k\}$. Dann gilt $S \subseteq N_j$ und somit $N = N_j = N_{j+1} = \dots$. □

Proposition 2.5. *Es sei R noethersch. Dann ist jeder endlich erzeugter R-Modul M noethersch.*

Beweis. Es sei M endlich erzeugt, das heißt $M = RS$ für eine endliche Menge $S \subseteq M$. Wir nutzen Induktion über $\#S$. Falls $S = \emptyset$, so ist $M = \{0\}$ noethersch. Sei also $\#S \geq 1$. Wir wählen $s \in S$. Nach Induktion ist $M' = R(S \setminus \{s\})$ noethersch. Sei $N_1 \subseteq N_2 \subseteq \dots$ eine aufsteigende Kette von R-Untermoduln von M.

Wir betrachten $\phi\colon R \to M,\ r \mapsto rs$. Dann ist $\phi^{-1}(N_1) \subseteq \phi^{-1}(N_2) \subseteq \dots$ eine aufsteigende Kette von Idealen in R, welche stationär wird, da R noethersch ist, das heißt $\phi^{-1}(N_{j_1}) = \phi^{-1}(N_{j_1+1}) = \dots$. Ebenso wird $N_1 \cap M' \subseteq N_2 \cap M' \subseteq \dots$ stationär, da M' noethersch ist, das heißt $N_{j_2} \cap M' = N_{j_2+1} \cap M' = \dots$. Für $j \geq j_0 = \max\{j_1, j_2\}$ gilt dann das $N_j \cap M' = N_{j_0} \cap M'$ und $N_j/(N_j \cap M') = N_{j_0}/(N_{j_0} \cap M')$ und somit $N_j = N_{j_0}$, so dass auch $N_1 \subseteq N_2 \subseteq \dots$ stationär wird. □

3 Der Hilbertsche Basissatz

Satz 3.1 (Hilbertscher Basissatz)**.** *Falls R noethersch ist, so ist auch $R[X]$ noethersch.*

Beweis. Nach Proposition 2.4 genügt es zu zeigen, dass jedes Ideal $I \subseteq R[X]$ als $R[X]$-Modul endlich erzeugt ist. Für ein Polynom $f = \sum_{j=0}^{d} r_d X^d \in R[X]$ mit $r_d \neq 0$ bezeichnen wir den Leitkoeffizienten r_d mit $\mathrm{in}(f)$. Für $f, g \in I$ mit $d = \deg f - \deg g \geq 0$

gilt

$$\mathrm{in}(f) - \mathrm{in}(g) = \begin{cases} 0 & \text{falls } \mathrm{in}(f) = \mathrm{in}(g) \\ \mathrm{in}(f - t^d \cdot g) & \text{sonst,} \end{cases}$$

$$r \cdot \mathrm{in(f)} = \begin{cases} 0 & \text{falls } r \cdot \mathrm{in}(f) = 0 \\ \mathrm{in}(r \cdot f) & \text{sonst.} \end{cases}$$

Folglich ist $\mathrm{in}(I) = \{\mathrm{in}(f) \mid f \in I\}$ ein Ideal in R. Da R noethersch ist, ist $\mathrm{in}(I)$ endlich erzeugt: Es gibt $f_1, \ldots, f_k \in I$ mit $\mathrm{in}(I) = R\{\mathrm{in}(f_1), \ldots, \mathrm{in}(f_k)\}$. Sei $d_i = \deg f_i$ und $d_0 = \max\{d_1, \ldots d_k\}$ und $N \subseteq R[X]$ die Menge der Polynome von Grad $< d_0$, das heißt $N = R\{1, x, \ldots, x^{d_0 - 1}\} \subseteq R[X]$.

Beheauptung. *Es gilt* $I = R[X]\{f_1, \ldots, f_k\} + (I \cap N)$.

Es ist zu zeigen, dass jedes $f \in I$ modulo $R[X]\{f_1 \ldots f_k\}$ ein Polynom von Grad $< d_0$ ist. Wir zeigen dies mittels Induktion über $d = \deg f$. Für $d < d_0$ ist nichts zu zeigen. Sei $d \geq d_0$. Es gilt $\mathrm{in}(f) = \sum_{j=1}^{k} r_j \mathrm{in}(f_j)$ für gewisse $r_1, \ldots, r_k \in R$. Wir können annehmen, dass aus $r_j \mathrm{in}(f_j) = 0$ auch $r_j = 0$ folgt. Dann gilt

$$\mathrm{in}(f) = \sum_{j=1}^{k} r_j \mathrm{in}(f_j) = \sum_{j=1}^{k} \mathrm{in}(r_j f_j) = \mathrm{in}\left(\sum_{j=1}^{k} r_j f_j x^{d - d_j} \right).$$

Daher hat das Polynom $f' = f - \sum_{j=1}^{k} r_j f_j x^{d-d_j} \in I$ Grad $\deg f' < d$. Nach Induktion ist nun $f' \in R[X]\{f_1, \ldots, f_k\} + (I \cap N)$ und somit auch $f \in R[X]\{f_1, \ldots, f_k\} + (I \cap N)$.

Der Satz folgt nun wie folgt: Der R-Modul N ist endlich erzeugt und somit nach Proposition 2.5 noethersch. Nach Propostion 2.4 ist daher auch $I \cap N$ ein endlich erzeugter R-Modul. Sei $\{f_{k+1}, f_{k+2}, \ldots, f_l\}$ eine erzeugende Menge für $N \cap I$, dann ist $I = R[X]\{f_1, \ldots, f_l\}$ endlich erzeugt. □

Unter einer R-Algebra verstehen wir einen kommutativen Ring A zusammen mit einem Ringhomomorphismus $R \to A$. Eine endlich erzeugte R-Algebra ist eine R-Algebra A, so dass $R \to A$ sich als Komoposition der kanonischen Abbildung $R \to R[X_1, \ldots, X_n]$ für ein $n \in \mathbb{N}$ und einem surjektiven Ringhomomorphismus $R[X_1, \ldots, X_n] \to A$ darstellen lassen kann.

Korollar 3.2. *Falls R noethersch ist, so ist auch jede endlich erzeugte R-Algebra neothersch. Insbesondere ist für einen Körper k jeder Quotient von $k[X_1, \ldots, X_n]$ noethersch. Ebenso ist jeder Unterraum von $\mathbb{A}_k^n$ noethersch.*

Beweis. Nach Satz 3.1 ist $R[X_1, \ldots, X_n]$ noethersch. Nach Beispiel 2.3 ist auch $R[X_1, \ldots, X_n]$ noethersch. Nach Definition sind dies gerade die endlich erzeugten R-Algebren. Weiter ist $\mathbb{A}_k^n$ noethersch, denn ist $\mathbb{A}_k^n \supseteq Y_1 \supseteq Y_2 \supseteq \ldots$ eine absteigende Kette abgeschlossener Unterräume, so ist $I(Y_1) \subseteq I(Y_2) \subseteq \ldots$ eine aufsteigende Kette von Idealen in

$k[X_1, \ldots, X_n]$, welche stationär wird, da $k[X_1, \ldots, X_n]$ noethersch ist. Da die Y_j's abgeschlossen sind, gilt $Z(I(Y_j)) = Y_j$. Somit wird auch die Kette $Y_1 \supseteq Y_2 \supseteq \ldots$ stationär. Nach Beispiel 2.3 ist nun wiederum auch jeder Unterraum von $\mathbb{A}_k^n$ noethersch. □

4 Lokalisierungen

Definition 4.1. *Eine Teilmenge $S \subseteq R$ im Ring R heißt multiplikativ, falls $1 \in S$, $0 \notin S$ und $a \cdot b \in S$ für alle $a, b \in S$.*

Es sei $S \subseteq R$ eine multiplikative Teilmenge. Wir betrachten die folgende Äquivalenzrelation auf $S \times R$:

$$(s, r) \equiv (s', r') \Leftrightarrow \exists s'' \in S \text{ mit } s''(s'r - sr') = 0.$$

Wir bezeichnen die Menge der Äquivalenzklassen mit $S^{-1}R$ und die Äquivalenzklasse von (s, r) mit $\frac{r}{s}$. Wir erhalten auf $S^{-1}R$ eine Ringstruktur mittels $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ und $\frac{r}{s} + \frac{r'}{s'} = \frac{s'r+sr'}{ss'}$ mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$.

Definition 4.2. *Für eine multiplikative Teilmenge $S \subseteq R$ nennen wir den Ring $S^{-1}R$ zusammen mit dem kanonischen Homomorphismus $R \to S^{-1}R$, $r \to \frac{r}{1}$ die Lokalisierung von R abseits von S.*

Bemerkung 4.3. *(a) Falls S keine Nullteiler beinhaltet, gilt*

$$\frac{r}{s} = \frac{r'}{s'} \Leftrightarrow s'r = sr'.$$

Insbesondere ist $\frac{r}{1} = \frac{0}{1} \Leftrightarrow r = 0$, so dass $R \to S^{-1}R$ injektiv ist.

(b) Das Bild von $s \in S$ unter $R \to S^{-1}R$ hat in $S^{-1}R$ ein Inverses: $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$.

(c) Besteht S genau aus allen Nichtnullteilern, so heißt $S^{-1}R$ der Quotientenring $K(R)$ von R. Falls R ein Integritätsring ist, so ist $K(R)$ ein Körper und wird der Quotientenkörper von R genannt.

Beispiel 4.4. *(a) Es sei $a \in R$ nicht nilpotent, das heißt $a^n \neq 0$ für alle $n \in \mathbb{N}$. Dann ist $S = \{a^n \mid n \geq 0\}$ eine multiplikative Menge und wir bezeichnen $S^{-1}R$ auch mit $R\left[\frac{1}{a}\right]$.*

(b) Ist $\mathfrak{p} \subseteq R$ ein Primideal, so ist $S = R \setminus \mathfrak{p}$ eine multiplikative Menge und wir bezeichnen $S^{-1}R$ mit $R_\mathfrak{p}$. In diesem Ring ist $\mathfrak{p}R_\mathfrak{p} \subseteq R_\mathfrak{p}$ das einzige maximale Ideal. Ringe mit nur einem maximalen Ideal nennen wir lokale *Ringe.*

Lemma 4.5. *Es gilt $R[X]/(aX - 1) \cong R\left[\frac{1}{a}\right]$.*

Beweis. Übung. □

5 Der Hilbertsche Nullstellensatz

Proposition 5.1 (Artin–Tate)**.** *Es sei R noethersch, A eine R-Algebra und B eine A-Algebra, die als A-Modul endlich erzeugt ist. Dann ist A genau dann eine endlich erzeugte R-Algebra, wenn B eine endlich erzeugte R-Algebra ist.*

Beweis. Es seien $b_1, \ldots, b_m \in B$ mit $B = \sum_{j=1}^m Ab_j$.

"$\Rightarrow$": Falls es $a_1, \ldots a_n \in A$ gibt, die A als R-Algebra erzeugen, das heißt $A = R[a_1, \ldots, a_n]$, dann erzeugen $a_1, \ldots, a_n, b_1, \ldots, b_m$ die R-Algebra B.

"$\Leftarrow$": Wir nehmen nun an, dass B eine endlich erzeugte R-Algebra ist. Durch Vergrößern der Menge $\{b_1, \ldots, b_m\}$ können wir $B = R[b_1, \ldots, b_m]$ annehmen. Für die Produkte $b_j b_k$ gibt es dann Linearkombinationen

$$b_j b_k = \sum_{l=1}^m a_{jkl} b_k, \quad a_{jkl} \in A.$$

Es sei $A_0 \subseteq A$ die von den a_{jkl}'s erzeugte R-Unteralgebra. Diese ist nach Korollar 3.2 noethersch. Wegen $b_j b_k \in \sum_{l=1}^m A_0 b_l$ folgt mit Induktion $B = R[b_1, \ldots, b_m] \subseteq \sum_{l=1}^m A_0 b_l$. Daher ist B ein endlich erzeugter A_0-Modul. Da A ein A_0-Untermodul von B ist, ist auch A ein endlich erzeugter A_0-Modul nach Proposition 2.4. Somit ist A nach dem Argument in "$\Rightarrow$" eine endlich erzeugte R-Algebra. □

Korollar 5.2. *Eine Körpererweiterung L/K ist genau dann endlich, wenn L eine endlich erzeugte K-Algebra ist.*

Beweis. "$\Rightarrow$": Falls L ein endlich dimensionaler K-Vektorraum ist, so ist L auch eine endlich erzeugte K-Algebra.

"$\Leftarrow$": Seien $b_1, \ldots, b_m \in L$ Erzeuger für L als K-Algebra. Wir müssen zeigen, dass alle b_j algebraisch über K sind. Angenommen dies wäre nicht der Fall. Wir können annehmen, dass $b_1, \ldots, b_r$ algebraisch unabhängig über K sind und $b_{r+1}, \ldots, b_m$ algebraisch über dem Quotientenkörper $K(b_1, \ldots, b_r)$ von $K[b_1, \ldots, b_r]$ sind. Dann ist L eine endliche Erweiterung von $K(b_1, \ldots, b_r)$. Nach Proposition 5.1 angewandt auf $R = K$, $A = K(b_1, \ldots, b_r)$ und $B = L$ gibt es $\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n} \in K(b_1, \ldots b_r)$ mit $f_i, g_i \in K[b_1, \ldots, b_r]$ und $g_i \neq 0$, die $K(b_1, \ldots, b_r)$ als K-Algebra erzeugen. Da $K[b_1, \ldots, b_r] \subsetneq K(b_1, \ldots, b_r)$ ist $g = g_1 g_2 \cdot \cdots \cdot g_n \notin K$, das heißt $\deg g > 0$. Der Quotient $\frac{1}{1+g} \in K(b_1, \ldots, b_r)$ lässt sich als ein Polynom in $\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n} \in K(b_1, \ldots b_r)$ schreiben. Folglich ist $\frac{1}{1+g} = \frac{f}{g^N}$ für ein $f \in K[b_1, \ldots, b_r]$ mit $g \not| f$ und $N \in \mathbb{N}_0$. Wegen $f(1+g) = g^N$ und $\deg g \geq 1$ muss $N \geq 1$ gelten. Aber dann ist $f = g(-f + g^{N-1})$ im Widerspruch zu $g \not| f$. □

Satz 5.3 (Hilbertscher Nullstellensatz)**.** *Es sei k ein algebraisch abgeschlossener Körper. Für jedes Ideal $J \subseteq k[X_1, \ldots, X_n]$ gilt $I(Z(J)) = \sqrt{J}$.*

Beweis. Sei $J \subseteq k[X_1, \ldots, X_n]$ ein Ideal. Es genügt $I(Z(J)) \subseteq \sqrt{J}$ zu zeigen. Es ist zu zeigen, dass für jedes $f \in k[X_1, \ldots, X_n] \setminus \sqrt{J}$ ein $p \in Z(J)$ mit $f(p) \neq 0$ existiert. Wir

bezeichnen mit $\bar{f}$ das Bild von f in $k[X_1, \ldots, X_n]/J$. Da $\bar{f}$ nicht nilpotent ist gilt nach Lemma 4.5

$$A := (k[X_1, \ldots, X_n]/J)\left[\frac{1}{\bar{f}}\right] = k[X_0, X_1, \ldots, X_n]/(J, X_0 f - 1).$$

Dies ist eine endlich erzeugte k-algebra. Wegen $(k[X_1, \ldots, X_n]/J)\left[\frac{1}{\bar{f}}\right] \neq 0$ können wir ein maximales Ideal $\mathfrak{m} \subseteq A$ wählen. Dann ist $A/\mathfrak{m}$ eine endlich erzeugte k-Algebra und somit nach Korollar 5.2 eine endliche Körpererweiterung von k, und somit $A/\mathfrak{m} = k$, da k algebraisch abgeschlossen ist. Sei nun a_i das Bild von X_i in $A/\mathfrak{m} = k$ und $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$. Dann ist $(a_0, a_1, \ldots, a_n) \in Z((J, X_0 f - 1))$. Somit gilt $p \in Z(J)$ und $a_0 f(p) = 1$, so dass $f(p) \neq 0$. □