Skript zur Vorlesung

Einführung in die Algebraische Geometrie

Wintersemester 2007/2008
Frankfurt am Main

Prof. Dr. Annette Werner

Inhaltsverzeichnis

1 Einführung

In der Algebraischen Geometrie studiert man Lösungsmengen von Polynomgleichungen mit geometrischen Methoden. Beispiele für Polynomgleichungen sind etwa die linearen Gleichungssysteme

$$\begin{aligned} a_{11}x_1+ \quad &\cdots \quad +a_{1n}x_n = b_1 \\ &\vdots \\ a_{m1}x_1+ \quad &\cdots \quad a_{mn}x_n = bm, \end{aligned}$$

wobei $(a_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$ und $b_1, \ldots, b_m$ Elemente eines Körpers k sind.
In der Linearen Algebra lernt man, wann ein solches Gleichungssystem eine Lösung in k^n besitzt und wie man die Lösungsmenge beschreiben kann.

Ein weiteres Beispiel sind die Polynomgleichungen in einer Unbestimmten

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

für $a_1, \ldots, a_n \in k$, die man in der Algebra studiert. Ist eine solche Gleichung über k nicht lösbar, so gibt es eine algebraische Körpererweiterung L/K, in der sie lösbar ist.

In der Algebraischen Geometrie wollen wir Lösungsmengen von beliebigen Polynomen in beliebig vielen Unbestimmten studieren. Das erfordert natürlich etwas mehr Aufwand.

Wir bezeichnen den Polynomring in n Unbestimmten über dem Körper k mit $k[x_1, \ldots, x_n]$. Für $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ setzen wir dann

$$\begin{aligned} V_k(f_1, \ldots, f_m) = \{P = (P_1, \ldots, P_n) \in k^n : \\ f_1(P_1, \ldots, P_n) = \ldots = f_m(P_1, \ldots, P_n) = 0. \end{aligned}$$

$V_k(f_1, \ldots, f_m)$ ist also die Menge aller gemeinsamen Nullstellen von $f_1, \ldots, f_m$ in k.

Beispiel:

i) Ist $f(x, y) = x^2 + y^2 - 1 \in \mathbb{Q}[x, y]$, so ist $V_{\mathbb{R}}(f) = \{(P_1, P_2) \in \mathbb{R}^2 : P_1^2 + P_2^2 = 1\}$ der Einheitskreis in $\mathbb{R}^2$.

Wir können auch

$$V_{\mathbb{Q}}(f) = \{(P_1, P_2) \in \mathbb{Q}^2 : P_1^2 + P_2^2 = 1\}$$

betrachten, dies ist die Menge der rationalen Zahlen auf dem Einheitskreis. Auch $V_{\mathbb{C}}(f) = \{(P_1, P_2) \in \mathbb{C}^2; P_1^2 + P_2^2 = 1\}$ ist definiert; dies ist allerdings nicht der Einheitskreis in $\mathbb{C}^2$!

Da f nur die Koeffizienten 0 und 1 hat, können wir f auch im Polynomring $\mathbb{F}_2[x, y]$ auffassen. Dann ist

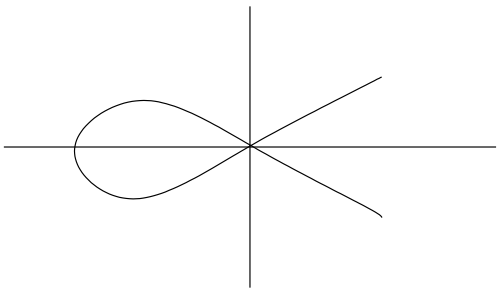
$$\begin{aligned} V_{\mathbb{F}_2}(f) &= \{P_1, P_2) \in \mathbb{F}_2^2 : P_1^2 + P_2^2 = 1\} \\ &= \{(0, 1), (1, 0)\}. \end{aligned}$$

Wir sehen schon an diesem einfachen Beispiel, dass die Nullstellenmenge von f entscheidend vom gewählten Grundkörper abhängt.

ii) Wir betrachten $f(x, y) = y^2 - x^3 - x^2$. Hier ist

$$V_{\mathbb{R}}(f) = \{(P_1, P_2) \in \mathbb{R}^2 : P_2^2 = P_1^3 + P_1^2\}.$$

Dies ist eine Kurve mit einem Doppelpunkt:



Diese Kurve lässt sich „parametrisieren“ durch die Abbildung

$$\begin{aligned} \varphi = \mathbb{R} &\to \mathbb{R}^2 \\ t &\mapsto (t^2 - 1, t^3 - t). \end{aligned}$$

Es gilt $\varphi(\mathbb{R}) \subset V_{\mathbb{R}}(f)$, wie man sofort nachrechnet.
Ferner ist φ injektiv für $t \notin \{\pm 1\}$, denn aus $t^2 - 1 = s^2 - 1$ und $t^3 - t = s^3 - s$ folgt $t(s^2 - 1) = s(s^2 - 1)$, also für $s \neq \pm 1$ auch $t = s$.

Die Tatsache, dass $\varphi(-1) = \varphi(1) = 0$ gilt, erklärt den Doppelpunkt der Kurve.

iii) Die aus der Linearen Algebra bekannte Menge

$$GL_n(k) = \{A \in k^{n \times n} : \det A \neq 0\}$$

der invertierbaren $(n \times n)-$ Matrizen mit Einträgen in k lässt sich ebenfalls als Nullstellenmenge von Polynomen schreiben.
Dazu brauchen wir n^2 Unbestimmte $(x_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,n}}$ und eine zusätzliche Unbestimmte T. Die Determinante einer Matrix ist ein Polynom in den Einträgen, wie man etwa an der Leibniz-Formel sieht. Daher ist $\det\big((x_{ij})_{i,j}\big)$ ein Polynom in $k[x_{11}, \dots, x_{nn}]$. Wir betrachten das Polynom

$$f\big((x_{ij})_{i,j}, T\big) = \det(x_{ij})T - 1 \in k[x_{11}, \dots, x_{nn}, T].$$

Es ist

$$V_k(f) = \{(a_{ij})_{i,j} \in k^{n \times n}, t \in k : \det(a_{ij})_{i,j}\ t = 1\}.$$

Diese Nullstellenmenge lässt sich mit Hilfe der Abbildung

$$GL_n(k) \to V_k(f)$$

$$A \mapsto (A, \tfrac{1}{\det A})$$

mit der Menge $GL_n(k)$ identifizieren.

iv) Wir betrachten nun für $n \geq 2$ noch das berühmte Beispiel

$$f(x, y, z) = x^n + y^n - z^n.$$

Es ist

$$V_{\mathbb{Q}}(f) = \{(a, b, c) \in \mathbb{Q}^3 : a^n + b^n = c^n\}$$

gerade die Menge der rationalen Lösungen der Fermat-Gleichung $x^n + y^n = z^n$. (Pierre de Fermat (1601 oder 1607/08 bis 1665) war ein französischer Jurist und genialer Hobbymathematiker, der u.a. das Traktat „Arithmetika“ von Diophantos von Alexandria mit Randnotizen versah.) Diese hat immer die trivialen Lösungen $(0, 1, 1)$, $(1, 0, 1)$ (und Vielfache davon) sowie $(-1, 1, 0)$, falls n ungerade ist bzw. $(0, 1, -1)$ und $(1, 0, -1)$, falls n gerade ist. Man nennt eine Lösung (a, b, c) nicht trivial, falls $abc \neq 0$ ist.
Für $n = 2$ gibt es unendlich viele nicht-triviale Lösungen, die sogenannten Pythagoräischen Tripel

$$a = 2AB \ , \ b = A^2 - B^2 \ , \ c = A^2 + B^2$$

für ganze Zahlen $A > B > 0$. Es gilt nämlich

$$\begin{aligned} a^2 + b^2 &= (2AB)^2 + (A^2 - B^2)^2 \\ &= 4A^2B^2 + A^4 - 2A^2B^2 + B^4 \\ &= (A^2 + B^2)^2 = c^2. \end{aligned}$$

Für $A = 2$ und $B = 1$ ergibt sich das bekannte Pythagoräische Tripel $(2, 3, 5)$.
Ist $n \geqq 3$, so sagt die berühmte Fermatsche Vermutung, dass die Gleichung

$$x^n + y^n = z^n$$

keine nicht-triviale Lösung in $\mathbb{Q}^3$ besitzt. Mit anderen Worten, die Nullstellenmenge $V_{\mathbb{Q}}(f)$ besteht nur aus den oben angegebenen trivialen Lösungen.

Die Fermatsche Vermutung wurde 1995 von Andrew Wiles mit den hochentwickelten Methoden der Algebraischen Geometrie bewiesen.

2 Der Hilbert’sche Basissatz

Wir erinnern zunächst an einige Begriffe aus der Ringtheorie.

Ein **Ring** ist eine Menge A mit zwei Verknüpfungen $+$ und $\cdot$, für die folgende Bedingungen gelten:

i) $(A, +)$ ist eine abelsche Gruppe, insbesondere existiert also ein Nullelement 0 in A.

ii) Die Multiplikation $\cdot$ ist assoziativ und distributiv, d. h. es gilt in A

$$a(b+c) = ab + ac$$

und

$$(a+b)c = ac + bc.$$

Alle Ringe, die wir betrachten werden, sind **kommutativ mit 1**, d.h. es gilt zusätzlich

iii) $ab = ba$ für alle $a, b \in A$.

iv) Es gibt ein Einselement $1 \in A$ mit $1a = a1 = a$ für alle $a \in A$.

Ab sofort treffen wir folgende Vereinbarung: Mit Ring meinen wir immer einen kommutativen Ring mit Eins.

Ein **Ringhomomorphismus** ist eine Abbildung $f : A \to B$ zwischen Ringen, für die

i) $f(a+b) = f(a) + f(b)$

ii) $f(ab) = f(a)f(b)$

iii) $f(1) = 1$

gilt.
f heißt **Isomorphismus** von Ringen, falls es einen Ringhomomorphismus $g : B \to A$ gibt, so dass $f \circ g = id_B$ und $g \circ f = id_A$ gilt. Dies ist genau dann der Fall, wenn der Ringhomomorphismus f injektiv und surjektiv ist.
Eine Teilmenge $\mathfrak{a} \subset A$ heißt **Ideal**, falls

i) $(\mathfrak{a}, +)$ eine Untergruppe von $(A, +)$ ist, d.h. es ist $0 \in \mathfrak{a}$ und $\mathfrak{a}$ ist abgeschlossen unter $+$ und $-$

ii) $\mathfrak{a}A = \mathfrak{a}$ gilt, d.h. für alle $a \in \mathfrak{a}$ und $x \in A$ ist $xa \in \mathfrak{a}$.

Ist $\mathfrak{a} \subset A$ ein Ideal, so erbt die Quotientengruppe $A/\mathfrak{a}$ eine Multiplikationsabbildung von A und wird damit selbst ein Ring. Die Abbildung

$$A \to A/\mathfrak{a}$$

$$x \mapsto x + \mathfrak{a},$$

die x auf die Nebenklasse von x modulo $\mathfrak{a}$ abbildet, ist ein surjektiver Ringhomomorphismus.

Ein **Nullteiler** in A ist ein Element $a \in A$, so dass ein $b \in A$ existiert mit $b \neq 0$ und $ab = 0$.

Beispiel: Ist $k > 1$ und $l > 1$, so existieren für $n = kl$ Nullteiler im Ring $\mathbb{Z}/n\mathbb{Z}$, denn es gilt

$$(k + n\mathbb{Z})(l + n\mathbb{Z}) = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}$$

und beide Faktoren sind $\neq 0$.

Definition 2.1 Ein kommutativer Ring mit 1, der keine Nullteiler enthält, heißt **Integritätsring**.

Beispiel: $\mathbb{Z}$, jeder Körper k und jeder Polynomring $k[x_1, \ldots, x_n]$ über einem Körper k sind Beispiele für Integritätsringe.

Wir benötigen nun noch einige Tatsachen über Ideale. Jedes $a \in A$ definiert ein sogenanntes **Hauptideal** $(a) = aA = \{ab : b \in A\}$.
Ist jedes Ideal $\mathfrak{a} \subset A$ ein Hauptideal, so heißt A **Hauptidealring**. Ein Ideal $\mathfrak{p} \neq A$ in A heißt **Primideal**, falls gilt: Ist $ab \in \mathfrak{p}$ für a und b in A, so gilt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Also ist $\mathfrak{p} \subset A$ genau dann ein Primideal, wenn $A/\mathfrak{p}$ nullteilerfrei ist.

Beispiel: Ist p eine Primzahl, so ist das von p erzeugte Hauptideal (p) in $\mathbb{Z}$ ein Primideal. Ferner ist $(0) \subset \mathbb{Z}$ ein Primideal.

Ein Ideal $\mathfrak{m} \subset A$ heißt **maximales Ideal**, falls $\mathfrak{m} \neq A$ ist und falls für jedes Ideal $\mathfrak{m} \subset \mathfrak{a} \subset A$ schon $\mathfrak{m} = \mathfrak{a}$ folgt. Ein Ideal $\mathfrak{m} \subset A$ ist genau dann ein maximales Ideal, wenn $A/\mathfrak{m}$ ein Körper ist.

Beispiel: Ist p eine Primzahl, so ist $(p) \subset \mathbb{Z}$ ein maximales Ideal. Das Nullideal ist nicht maximal in $\mathbb{Z}$.

Ist $f : A \to B$ ein Ringhomomorphismus, und $\mathfrak{b} \in B$ ein Ideal, so ist $f^{-1}(\mathfrak{b}) \subset A$ ein Ideal. Ist $\mathfrak{b}$ ein Primideal, so ist auch $f^{-1}(\mathfrak{b})$ ein Primideal.

Definition 2.2 i) Es sei I eine beliebige Indexmenge und $(a_i)_{i\in I}$ eine Familie von Elementen aus A. Ein Ideal $\mathfrak{a}$ heißt erzeugt von $(a_1')_{i\in I}$, wir schreiben $\mathfrak{a} = (a_i)_{i\in I}$, falls alle $a_i \in \mathfrak{a}$ sind und falls sich jedes $x \in \mathfrak{a}$ als $x = x_{i_1}a_{i_1} + \ldots + x_{i_m}a_{i_m}$ schreiben lässt mit geeigneten Indizes $i_1, \ldots, i_m \in I$ und Elementen $x_{i_1}, \ldots, x_{i_m} \in A$.

ii) Ein Ideal $\mathfrak{a} \subset A$ heißt **endlich erzeugt**, falls es endlich viele Elemente $a_1, \ldots, a_m \in \mathfrak{a}$ gibt mit $\mathfrak{a} = (a_1, \ldots, a_m)$.

Definition 2.3 Ein Ring A heißt **noethersch**, falls jedes Ideal endlich erzeugt ist.

Lemma 2.4 Die folgenden Aussagen sind äquivalent:

i) A ist noethersch.

ii) Jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_k \subset \ldots$ in A wird stationär, d.h. es gibt ein n_0 mit $\mathfrak{a}_{n_0} = \mathfrak{a}_n$ für alle $n \geqq n_0$.

iii) Jede nicht-leere Menge von Idealen besitzt ein maximales Element bezüglich der Inklusion.

Beispiel: Jeder Hauptidealring ist noethersch, insbesondere ist $\mathbb{Z}$ noethersch.

Lemma 2.5 Ist A ein noetherscher Ring und $\mathfrak{a} \subset A$ ein Ideal, so ist $A/\mathfrak{a}$ ein noetherscher Ring.

Beweis : Es sei $\pi : A \to A/\mathfrak{a}$ die kanonische Abbildung. Ist $\mathfrak{b} \subset A/\mathfrak{a}$ ein Ideal, so ist $\pi^{-1}(\mathfrak{b}) \subset A$ ein Ideal. Nach Voraussetzung ist $\pi^{-1}(\mathfrak{b})$ endlich erzeugt, also $\pi^{-1}(\mathfrak{b}) = (a_1, \ldots, a_m)$ für geeignete $a_1, \ldots, a_m \in A$. Man rechnet leicht nach, dass dann $\mathfrak{b} = \big(\pi(a_1), \ldots, \pi(a_m)\big)$ gilt. Also ist $\mathfrak{b}$ endlich erzeugt. □

Definition 2.6 Sei A ein Ring. Ein **A−Modul** M ist eine Menge mit einer Verknüpfung $+$ und einer Abbildung (skalare Multiplikation)

$$A \times M \to M,$$

$$(a, m) \mapsto am$$

so dass folgende Bedingungen gelten:

i) $(M, +)$ ist eine abelsche Gruppe.

ii) $a(x + y) = ax + ay$ für $a \in A, x, y \in M$

iii) $(a+b)x = ax + bx$ für $a, b \in A, x \in M$

iv) $(ab)x = a(bx)$ für $a, b \in A, x \in M$

v) $1x = x$ für $x \in M$.

Beispiele:

i) Jedes Ideal $\mathfrak{a} \subset A$ ist ein $A-$Modul. Insbesondere ist A selbst ein $A-$Modul.

ii) Ist $A = k$ ein Körper, so sind die $A-$Moduln genau die $k-$Vektorräume.

iii) Die $\mathbb{Z}-$Moduln sind genau die abelschen Gruppen, wobei wir auf einer abelschen Gruppe die skalare Multiplikation mit $\mathbb{Z}$ so definieren:

$$ma = \begin{cases} \underbrace{a + \ldots + a}_{m-\text{mal}} & , \text{ falls } m > 0 \\ 0 & , \text{falls } m = 0 \\ \underbrace{-a - \ldots - a}_{(-m)-\text{mal}} & , \text{ falls } m < 0 \end{cases}$$

Eine Abbildung $f : M \to N$ zwischen zwei $A-$Moduln heißt **Homomorphismus** von $A-$Moduln, falls

$$f(x+y) = f(x) + f(y) \text{ und}$$
$$f(ax) = af(x)$$

für alle $a \in A,\ x, y \in M$ gilt.

Eine Teilmenge $N \subset M$ heißt **Untermodul**, falls N eine Untergruppe von M ist, die abgeschlossen unter der $A-$Multiplikation ist.

Beispiel: Ist $f : M \to N$ ein Homomorphismus, so ist Kern $f = \{x \in M : f(x) = 0\}$ ein Untermodul von M und Bild $f = \{y \in N : \text{es gibt ein } x \in M \text{ mit } f(x) = y\}$ ein Untermodul von N.

Ist $N \subset M$ ein Untermodul, so existiert die Faktorgruppe M/N. Auf dieser können wir durch

$$A \times M/N \to M/N$$
$$(a, x + N) \mapsto ax + N$$

eine skalare Multiplikation definieren, die M/N zu einem $A-$Modul macht. Die natürliche Abbildung

$$\pi : M \to M/N$$
$$x \to x + N$$

ist ein surjektiver Homomorphismus von $A-$Moduln mit kern $\pi = N$.

Ein $A-$Modul M heißt **endlich erzeugt**, falls es Elemente $x_1, \ldots, x_n$ in M gibt, so dass sich jedes $x \in M$ als Linearkombination

$$x = \sum_{i=1}^{n} a_i x_i$$

mit geeigneten $a_1, \ldots, a_n \in A$ darstellen lässt. Die Koeffizienten $a_1, \ldots, a_n$ sind natürlich im allgemeinen nicht eindeutig bestimmt.

Ist I eine beliebige Indexmenge und ist M_i für alle $i \in I$ ein $A-$Modul, so wird die **direkte Summe**

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i, \text{fast alle } m_i = 0\}$$

der abelschen Gruppen M_i zusammen mit der skalaren Multiplikation

$$a(m_i)_{i \in I} = (am_i)_{i \in I}$$

ein $A-$Modul. Wir nennen einen $A-$Modul M, der isomorph zu $\bigoplus_{i \in I} A$ für eine beliebige Indexmenge I ist, einen **freien A$-$Modul**. Ist I eine endliche Menge mit n Elementen, so ist $M \simeq A \oplus \ldots \oplus A = A^n$. In diesem Fall gibt es ein Erzeugendensystem $x_1, \ldots, x_n$ von M, so dass jedes $x \in M$ eine Darstellung der Form $x = a_1 x_1 + \cdots + a_n x_n$ mit eindeutig bestimmten $a_1, \ldots, a_n$ besitzt.

Proposition 2.7 Sei M ein $A-$Modul. M ist genau dann endlich erzeugt, wenn M isomorph zu einem Quotienten von A^n für ein $n > 0$ ist, d.h. wenn es einen surjektiven $A-$Modul-Homomorphismus $\varphi : A^n \to M$ gibt.

Beweis : „$\Rightarrow$:“ Es sei $x_1, \ldots, x_n$ ein Erzeugendensystem von $\mathcal{M}$. Wir definieren einen $A-$Modul-Homomorphismus

$$\varphi : A^n \to M$$

durch $\varphi(a_1, \ldots, a_n) = a_1 x_1 + \ldots + a_n x_n$. Dann ist φ surjektiv, also folgt $M \simeq A^n/\text{Kern } \varphi$.

„ $\Leftarrow$ “: Sei $\varphi : A^n \to M$ ein surjektiver $A-$Modul-Homomorphismus. Wir bezeichnen mit $e_i = (0 \dots 0\ 1\ 0 \dots 0)$ den $i-$ten Einheitsvektor in A^n. Da φ surjektiv ist, wird M von $\varphi(e_1), \dots, \varphi(e_n)$ erzeugt. $\square$

Jetzt können wir eine wichtige Tatsache zeigen, die der Schlüssel zum Hilbertschen Basissatz ist.

Satz 2.8 Sei A ein noetherscher Ring und M ein endlich erzeugter $A-$Modul. Dann ist jeder Untermodul von M ebenfalls endlich erzeugt.

Beweis : Da M endlich erzeugt ist, gibt es nach Proposition 2.7 einen surjektiven Homomorphismus $\varphi : A^n \to M$ für ein $n > 0$. Sei $N \subset M$ ein Untermodul. Dann ist $\varphi^{-1}(N)$ ein Untermodul von A^n und $\varphi^{-1}(N) \to N$ ist ebenfalls surjektiv. Ist $\varphi^{-1}(N)$ endlich erzeugt, so ist also auch N endlich erzeugt. Daher genügt es zu zeigen, dass jeder Untermodul von A^n endlich erzeugt ist. Dies beweisen wir mit Induktion nach n.
Für $n = 1$ sind die Untermoduln von A gerade die Ideale in A. Diese sind endlich erzeugt, da A ein noetherscher Ring ist. Die Behauptung gelte also für ein $n > 1$. Wir betrachten den surjektiven Homomorphismus

$$\varphi : A^{n+1} \to A^n$$

$$(a_1, \dots, a_{n+1}) \mapsto (a_1, \dots, a_n)$$

und den injektiven Homomorphismus

$$\psi : A \to A^{n+1}$$

$$a \mapsto (0, \dots, 0, a).$$

Dann ist offenbar Kern $\varphi =$ Bild ψ. Also ist die kurze exakte Sequenz

$$0 \to A \xrightarrow{\psi} A^{n+1} \xrightarrow{\varphi} A^n \to 0$$

exakt.
Sei $N \subset A^{n+1}$ ein Untermodul. Nach Induktionsvoraussetzung ist $\psi^{-1}(N)$ als Untermodul von A und $\varphi(N)$ als Untermodul von A^n endlich erzeugt.

Wir wählen ein Erzeugendensystem $x_1, \dots, x_r$ von $\psi^{-1}(N)$ und Elemente $y_1, \dots, y_s \in N$, so dass $\varphi(y_1), \dots, \varphi(y_s)$ ein Erzeugendensystem von $\varphi(N)$ ist. Jetzt sei $x \in N$ ein

beliebiges Element. Dann ist $\varphi(x) \in \varphi(N)$, also von der Form $\varphi(x) = b_1\varphi(y_1) + \ldots + b_s\varphi(y_s)$ für $b_1, \ldots, b_s \in A$. Daher ist $x' = x - (b_1y_1 + \ldots + b_sy_s)$ in Kern φ = Bild ψ enthalten, also gilt $x' = \psi(x'')$ für ein $x'' \in A$. Da x' in N liegt, liegt $x'' \in \psi^{-1}(N)$. Somit ist x'' von der Form $x'' = a_1x_1 + \ldots + a_rx_r$ für $a_1, \ldots, a_r \in A$. Insgesamt folgt

$$x = a_1\psi(x_1) + \ldots + a_r\psi(x_r) + b_1y_1 + \ldots + b_sy_s.$$

Daher ist $\psi(x_1), \ldots, \psi(x_r), y_1, \ldots, y_s$ ein Erzeugendensystem von N, d.h. N ist endlich erzeugt.

□

Ein $A-$Modul, der die Eigenschaft hat, dass alle seine Untermoduln endlich erzeugte $A-$Moduln sind, heißt **noetherscher A−Modul**.

Satz 2.8 lässt sich also auch so umformulieren: Ein endlich erzeugter Modul über einem noetherschen Ring A ist noethersch. Insbesondere ist ein noetherscher Ring A auch als Modul über sich selbst noethersch.

Jetzt können wir den Hilbertschen Basissatz beweisen.

Satz 2.9 (Hilbert'scher Basissatz)
Ist A ein noetherscher Ring, so ist auch der Polynomring $A[X]$ noethersch.

Beweis : Es sei $\mathfrak{a} \subset A[X]$ ein Ideal. Wir wollen zeigen, dass $\mathfrak{a}$ endlich erzeugt ist. Dafür können wir $\mathfrak{a} \neq 0$ annehmen. Nun betrachten wir die Menge aller Leitkoeffizienten von Elementen in $\mathfrak{a}$:

$$\mathfrak{b} = \{a \in A : a \neq 0 \text{ und } aX^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathfrak{a}\} \cup \{0\}.$$

$\mathfrak{b}$ ist ein Ideal in A, also nach Voraussetzung endlich erzeugt. Ist $\mathfrak{b} = (a_1, \ldots, a_m)$ mit $a_i \neq 0$ aus A, so gibt es für alle i ein Polynom: $f_i(X) \in \mathfrak{a}$, dessen Leitkoeffizient a_i ist. Wir bezeichnen den Grad von $f_i(X)$ mit r_i. Wir betrachten das Ideal $\mathfrak{a}' = (f_1, \ldots, f_m)$ in $A[X]$. Offenbar ist $\mathfrak{a}' \subset \mathfrak{a}$.
Es sei r das Minimum der Grade $r_1, \ldots, r_m$. Ferner bezeichnen wir mit M den $A-$Untermodul aller Polynome vom Grad $\leqq r - 1$ in $A[X]$. Er wird erzeugt von den Polynomen $1, x, x^2, \ldots, x^{r-1}$. Wir zeigen nun $\mathfrak{a} = \mathfrak{a}' + (\mathfrak{a} \cap M)$. Die Inklusion „$\supset$" ist klar. Um „$\subset$" zu zeigen, betrachten wir ein beliebiges Polynom $f(X) = \alpha X^n + \ldots + \alpha_0$ in $\mathfrak{a}$. Ist $n < r$, so ist $f \in M$ und wir sind fertig. Ist $n \geqq r$, so schreiben wir den Leitkoeffizienten $\alpha \in \mathfrak{b}$ als $\alpha = c_1a_1 + \ldots + c_ma_m$ für geeignete $c_1, \ldots, c_m \in A$. Das Polynom $h_1(X) = \sum_{i=1}^{n} c_iX^{n-r_i}fi$ liegt in $\mathfrak{a}'$. Wir betrachten $g_1(X) = f(X) - h_1(X) \in \mathfrak{a}$. Der

Koeffizient vor X^n von $g_1(X)$ ist $\alpha - \sum_{i=1}^{n} c_i a_i = 0$, also hat g_1 einen Grad $\leq n-1$. Ist grad $(g_1) < r$, so liegt g_1 in $\mathfrak{a} \cap M$ und wir erhalten $f \in \mathfrak{a}' + (\mathfrak{a} \cap \mathcal{M})$. Andernfalls wiederholen wir das obige Verfahren mit $g_1(X)$ und konstruieren ein Polynom $h_2(X) \in \mathfrak{a}'$, so dass der Grad von $g_1(X) - h_1(X)$ echt kleiner als der Grad von $g_1(X)$ ist. Nach endlich vielen Schritten erhalten wir so ein Polynom in $\mathfrak{a} \cap M$, und es folgt $f \in \mathfrak{a}' + (\mathfrak{a} \cap M)$.

Nun ist $(\mathfrak{a} \cap M)$ als Untermodul des endlich erzeugten $A-$Moduls M nach Satz 2.8 selbst ein endlich erzeugter $A-$Modul. Als Summe von zwei endlich erzeugten $A-$Moduln ist somit $\mathfrak{a}$ endlich erzeugt. □

Korollar 2.10 Ist A ein noetherscher Ring, so ist für jedes $n \geq 1$ der Polynomring $A[X_1, \ldots, X_n]$ noethersch.

Beweis : Das folgt mit Induktion aus Satz 2.9, da $A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$ gilt. □