Der kombinatorische Nullstellensatz

Bachelorarbeit (LA)
Unterrichtsfach Mathematik

Matthias Schwab

Betreuer:

Univ.-Prof. Dr. Tim Netzer

Innsbruck, November 2020

Einleitung

Ein allgemein bekanntes Resultat in der Algebra ist, dass ein Polynom $n-$ten Grades, das nicht das konstante Nullpolynom ist, keine $n + 1$ Nullstellen besitzen kann (vgl. Satz 1). Der kombinatorische Nullstellensatz (vgl. Satz 2) kann durchaus als Erweiterung dieses Resultats auf Polynome in mehreren Variablen verstanden werden. Dieser Satz wurde zuerst von Noga Alon formuliert und bewiesen [1]. In dieser und mehreren anschließenden Arbeiten von Alon wird der kombinatorische Nullstellensatz benutzt, um unterschiedlichste mathematische Resultate zu beweisen.

Das Ziel dieser Arbeit ist es dem Leser die Aussage des kombinatorischen Nullstellensatzes näherzubringen sowie mögliche Anwendungen für den Schulunterricht zu erläutern. Dabei ist die Arbeit in 3 Abschnitte unterteilt. Im ersten Abschnitt wird versucht alle für das Verständnis des Satzes notwendigen Konzepte und Definitionen zu erarbeiten. Hierbei werden vor allem die Begriffe Menge, Körper und Polynomring behandelt. Der zweite Abschnitt dreht sich dann um den Beweis des Satzes. Ausgehend vom eindimensionalen Fall wird die Aussage mit Hilfe von Induktion auf beliebige Dimensionen erweitert. Anschließend wird durch wiederholte Gradreduktion das Ergebnis noch verschärft was dann zur Formulierung des kombinatorischen Nullstellensatzes führt. Schlussendlich werden im dritten Abschnitt mögliche Anwendungen des Satzes in der Schule diskutiert. Des Weiteren wird aufgezeigt in welchen Bereichen ein Bezug zum Lehrplan hergestellt werden kann.

Inhaltsverzeichnis

1 Vorbereitungen

Im folgenden Abschnitt werden wir das Vorwissen erarbeiten, welches für das Formulieren und Beweisen des kombinatorischen Nullstellensatzes nötig sein wird. Dabei werden hauptsächlich die mathematischen Begriffe Menge, Körper und Polynomring erklärt. Der Inhalt dieses Kapitels ist teilweise an [6] angelehnt.

1.1 Der Mengenbegriff

Um die Nullstellenmengen von Polynomen untersuchen zu können ist es notwendig zu klären, was mathematisch mit einer "Menge" gemeint ist. Der Mengenbegriff geht ursprünglich auf Bernhard Bolzano und Georg Cantor zurück. Cantor formulierte auch eine erste "naive" Definition der Menge.

Definition 1 (Cantor)**.** *Eine **Menge** ist eine Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.*

Die Objekte x, die in einer Menge M zusammengefasst werden, bezeichnet man als Elemente der Menge M. Man schreibt $x \in M$ falls x in der Menge M enthalten ist, bzw. $x \notin M$ falls x nicht in M enthalten ist. Eine Menge, in der nur endlich viele unterscheidbare Elemente enthalten sind bezeichnet man als endliche Menge. Die Anzahl der Elemente einer endlichen Menge M bezeichnet die Mächtigkeit der Menge und wird durch $|M|$ notiert. Der Begriff der Mächtigkeit kann auch auf unendliche Mengen ausgedehnt werden, worauf aber in dieser Arbeit verzichtet wird, da im Weiteren nur die Mächtigkeiten von endlichen Mengen eine Rolle spielen.

Es ist zu erwähnen, dass die hier angegebene Definition einer Menge streng genommen zu Widersprüchen führen kann. So können zum Beispiel Mengen konstruiert werden, welche bei der Beschreibung ihrer Elemente auf sich selbst referenzieren was dazu führen kann, dass nicht mehr klar entschieden werden kann ob ein gewisses Element in der Menge liegt oder nicht. Diese Widersprüche konnten in der Mathematik durch einen strengen axiomatischen Aufbau der Mengenlehre gelöst werden. So gilt heute die Zermelo-Fraenkel-Mengenlehre mit dem Auswahlaxiom (siehe z.B. [3]) als Grundlage der mathematischen Mengenlehre. Wir verzichten darauf dies genauer auszuführen, da die Definition von Cantor für die hier behandelten Mengen ausreichend und widerspruchsfrei ist. Da allerdings in der Formulierung des kombinatorischen Nullstellensatzes die Begriffe der Teilmenge und des kartesischen Produkts vorkommen, werden wir diese kurz erklären.

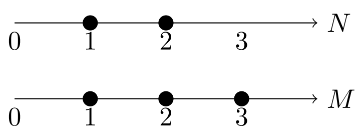
Definition 2. *Eine Menge N heißt **Teilmenge** von $M (N \subset M)$, wenn jedes Element von N auch in M enthalten ist.*

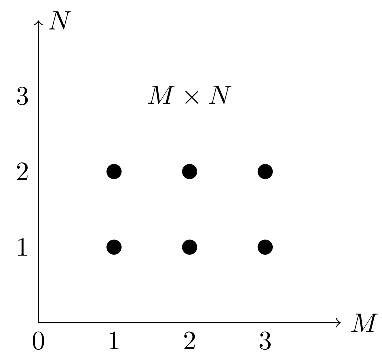
Definition 3. *Für zwei Mengen M, N ist das **kartesische Produkt** von M und N die Menge aller geordneten Paare von Elementen aus M und N:*

$$M \times N := \{(a, b) : a \in M, b \in N\}$$

Betrachten wir zum Beispiel die Mengen $M = \{1, 2, 3\}, N = \{1, 2\}$. Die Menge N hat zwei, die Menge M drei Elemente. Also: $|N| = 2, |M| = 3$. Beide Elemente in N sind auch in M enthalten und daher gilt $N \subset M$. Das kartesische Produkt von M und N ist die Menge

$$M \times N = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}.$$



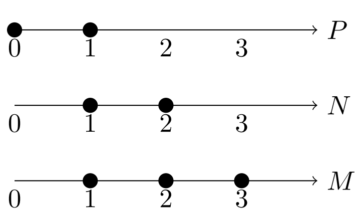


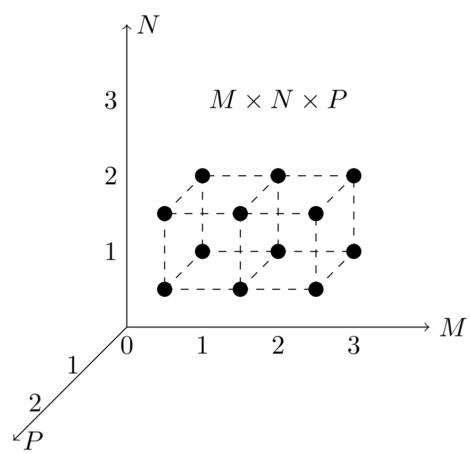
Das kartesische Produkt kann in gleicher Art und Weise auch für mehr als zwei Mengen gebildet werden. Für Mengen $M_1, \ldots, M_n$ definiert man

$$M_1 \times \cdots \times M_n \coloneqq \{(a_1, \ldots, a_n) : a_1 \in M_1, \ldots, a_n \in M_n\}.$$

So ist zum Beispiel das kartesische Produkt der drei Mengen $M = \{1, 2, 3\}, N = \{1, 2\}, P = \{0, 1\}$ die Menge

$$\begin{aligned} M \times N \times P = \{&(1, 1, 0), (1, 1, 1), (1, 2, 0), (1, 2, 1), (2, 1, 0), (2, 1, 1), (2, 2, 0), (2, 2, 1), \\ &(3, 1, 0), (3, 1, 1), (3, 2, 0), (3, 2, 1)\}. \end{aligned}$$





1.2 Körper und Polynomringe

Der kombinatorische Nullstellensatz trifft eine Aussage über die Nullstellen eines Polynoms über einem beliebigen Körper. In der Schule behandelt man hauptsächlich Polynome über dem Körper der reellen Zahlen. Allerdings umfasst der Begriff des Körpers viel mehr als nur die reellen Zahlen. Im Folgenden versuchen wir zu erklären was man aus mathematischer Sicht unter einem Körper versteht. Um dies zu erreichen, definieren wir zuerst den Begriff der kommutativen Gruppe

Definition 4. *Eine **kommutative Gruppe** ist eine Menge G zusammen mit einer Abbildung*

$$* : G \times G \to G,$$

die folgende Bedingungen erfüllt:

- $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ *(Assoziativgesetz)*
- $\forall a, b \in G : a * b = b * a$ *(Kommutativgesetz)*
- $\exists e \in G : \forall a \in G : a * e = a$ *(neutrales Element)*
- $\forall a \in G : \exists b \in G : a * b = e$ *(inverse Elemente)*

Ein Beispiel für eine kommutative Gruppe wäre die Menge der ganzen Zahlen $\mathbb{Z}$ zusammen mit der Addition (also der Verknüpfung $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}; (a, b) \mapsto a + b$). Denn offensichtlich gilt

$$\begin{aligned}
(3+1)+(-2) = 3+(1+(-2)) &= 2 \quad \text{(Assoziativgesetz)} \\
5+0 &= 5 \quad \text{(das neutrale Element ist also die 0)} \\
3+(-3) &= 0 \quad \text{(inverse Elemente)} \\
3+(-2) = (-2)+3 &= 1 \quad \text{(Kommutativgesetz),}
\end{aligned}$$

wobei die Zahlen in den obigen Rechnungen natürlich beliebig aus $\mathbb{Z}$ gewählt werden können. Die Menge der natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition bildet keine kommutative Gruppe, da keine inversen Elemente existieren (die Verknüpfung der Addition liefert nicht gleichzeitig auch eine Subtraktion). Die Menge der reellen Zahlen bildet zusammen mit der Addition in der selben Weise wie die Menge der ganzen Zahlen eine kommutative Gruppe. Man kann sich allerdings auch recht leicht davon überzeugen, dass $\mathbb{R} \setminus \{0\}$ zusammen mit der Multiplikation ebenfalls eine kommutative Gruppe bildet. Das neutrale Element ist hierbei die 1, das inverse Element eines Elements a ist $1/a$. Das heißt in den reellen Zahlen kann sowohl addiert, subtrahiert, multipliziert und dividiert werden. Dies motiviert die Definition des Körperbegriffs.

Definition 5. *Ein **Körper** ist eine Menge K zusammen mit zwei Verknüpfungen*

$$\begin{aligned}
+ &: K \times K \to K, \\
\cdot &: K \times K \to, K
\end{aligned}$$

genannt Addition und Multiplikation, sodass gilt:

- *K ist bezüglich der Addition eine kommutative Gruppe (das neutrale Element wird mit 0 bezeichnet).*
- *K ist bezüglich der Multiplikation eine kommutative Gruppe mit der kleinen Ausnahme, dass das neutrale Element bezüglich der Addition kein multiplikatives Inverses besitzt. (das neutrale Element bezüglich der Multiplikation wird mit $1 (\neq 0)$ bezeichnet).*
- *Addition und Multiplikation erfüllen das Distributivgesetz*

$$\forall a, b, c \in K : a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Bemerkung 1. *Wenn das Distributivgesetz gelten soll dann kann das neutrale Element der Addition gar kein multiplikatives Inverses besitzen. Denn angenommen es gibt ein Element $a \in K$ mit $a \cdot 0 = 1$ und das Distributivgestz gilt, dann haben wir*

$$a = a \cdot 1 = a \cdot (0 + 1) = a \cdot 0 + a \cdot 1 = 1 + a,$$

ein Widerspruch. Insbesondere muss daher für jedes Element $a \in G$ gelten , dass $a \cdot 0 = 0$ ist.

Bemerkung 2. *Erfüllt das Tripel $(R, +, \cdot)$ die gleichen Eigenschaften wie in Definition 5 , mit der Ausnahme, dass nicht jedes Element in $R \setminus \{0\}$ ein Inverses bezüglich der Multiplikation besitzt, dann nennt man R einen kommutativen Ring.*

Wie schon zuvor erwähnt ist $\mathbb{R}$ bzw. $\mathbb{R} \setminus \{0\}$ bezüglich der Addition bzw. bezüglich der Multiplikation eine kommutative Gruppe. Des Weiteren sind die Rechenregeln auf den reellen Zahlen genau so definiert, dass das Distributivgesetz gilt. Somit wird $\mathbb{R}$ zu einem Körper. Auch die rationalen Zahlen $\mathbb{Q}$ und die komplexen Zahlen $\mathbb{C}$ sind Körper. Es gibt in der Mathematik allerdings noch unzählige andere Körper. So bildet zum Beispiel die Menge $\{0, 1\}$ mit der Addition

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0,$$

und der Multiplikation

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1,$$

einen Körper. Dieser Körper besitzt nur zwei Elemente und gehört daher zur Klasse der endlichen Körper. Wir erwähnen die Existenz endlicher Körper hier insofern, dass in vielen Beweisen, in denen der kombinatorische Nullstellensatz Anwendung findet, Polynome über endlichen Körpern betrachtet werden.
Da wir nun den Begriff des Körpers kennen, können wir nun auch Polynome über Körpern betrachten.

Definition 6. *Für einen Körper K ist der* ***Polynomring über*** *K (in einer Variablen) definiert als die Menge aller Polynome mit Koeffizienten in K*

$$K[x] := \left\{ \sum_{i=0}^{m} a_i x^i : a_i \in K, m \in \mathbb{N} \right\}.$$

Analog ist der Polynomring über K in mehreren Variablen definiert als

$$K[x_1, \ldots, x_n] \coloneqq \left\{ \sum_{\alpha \in \mathbb{N}^n} c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} : c_\alpha \in K, \text{ nur endlich viele } c_\alpha \neq 0 \right\}.$$

Bemerkung 3. *Für ein Polynom $p = \sum_{i=0}^n a_n x^i \in K[x]$ nennt man den Koeffizient vor der höchsten auftretenden Potenz (a_n) auch Leitkoeffizient von p, kurz $LC(p)$.*

So ist das Polynom

$$p(x) = \frac{1}{2}x^2 + \frac{2}{3}x + \frac{3}{4}$$

ein Element des Polynomrings über dem Körper $\mathbb{Q}$ mit Leitkoeffizient $\mathrm{LC}(p) = 1/2$. Ein Element des Polynomrings $\mathbb{Q}[x, y]$ wäre beispielsweise das Polynom

$$p(x, y) = \frac{2}{3}x^2 + \frac{7}{6}y^3.$$

Am Beispiel $p = x$ ist leicht zu sehen, dass das Polynom $p \in K[x]$ kein inverses bezüglich der Multiplikation besitzt da $x^{-1} \notin K[x]$. Somit ist $K[x]$ kein Körper. Allerdings erfüllen die Polynomringe sowohl in einer als auch in mehreren Variablen zusammen mit der gewöhnlichen Addition und Multiplikation von Polynomen alle Voraussetzungen eines kommutativen Ringes.

Da im folgenden Kapitel Polynome in mehreren Variablen betrachtet werden, führen wir nun noch einige wichtige Schreibweisen und Begriffe ein:
Für den Polynomring $K[x_1, \ldots x_n]$ und $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ definieren wir die Kurzschreibweisen:

$$\begin{aligned} K[\underline{x}] &\coloneqq K[x_1, \ldots x_n] \\ \underline{x}^\alpha &\coloneqq x_1^{\alpha_1} \cdots x_n^{\alpha_n} \\ |\alpha| &\coloneqq \alpha_1 + \cdots + \alpha_n. \end{aligned}$$

Für jedes Polynom $p = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \underline{x}^\alpha \in K[\underline{x}]$ ist die Menge

$$\mathrm{supp}(p) = \{\alpha \in \mathbb{N}^n : c_\alpha \neq 0\}$$

eine endliche Menge. Die natürliche Zahl

$$\deg(p) = \max\{|\alpha| : \alpha \in \mathrm{supp}(p)\}$$

heißt der Grad von p. Weiters notieren wir mit

$$\deg_i(p) = \max\{\alpha_i : \alpha \in \mathrm{supp}(p)\}$$

den Grad von p in der i-ten Variablen.

Betrachten wir zum Beispiel das Polynom

$$p(x_1, x_2) = 3x_1^4 x_2 - 2x_1^2 x_2^3 + x_1 x_2 - x_2^2 - x_1 + 3.$$

Hier wäre $\mathrm{supp}(p) = \{(4,1), (2,3), (1,1), (0,2), (1,0), (0,0)\}$ und der Grad von p ist gegeben durch $\max\{5,5,2,2,1,0\} = 5$. Der Grad von p in der ersten Variablen ist $\max\{4,2,1,0,1,0\} = 4$, der Grad in der zweiten Variablen beträgt $3 = \max\{1,3,1,2,0,0\}$.
Das Polynom geschrieben in der oben definierten Schreibweise wäre

$$p(\underline{x}) = 3\underline{x}^{(4,1)} - 2\underline{x}^{(2,3)} + \underline{x}^{(1,1)} - \underline{x}^{(0,2)} - \underline{x}^{(1,0)} + 3\underline{x}^{(0,0)}.$$

Wir haben nun alle Vorbereitungen getroffen, um den kombinatorischen Nullstellensatz formulieren und beweisen zu können.

2 Der kombinatorische Nullstellensatz

2.1 Der eindimensionale Fall

Die in diesem Kapitel formulierten Sätze und Beweise sind angelehnt an [1]. Im folgenden Kapitel wird versucht dem Leser den kombinatorischen Nullstellensatz näherzubringen. Dieser sagt etwas über die Struktur der Nullstellen von Polynomen in mehreren Variablen aus und findet Anwendungen in Gebieten wie Graphentheorie, Zahlentheorie, oder Kombinatorik. Im Schulunterricht betrachtet man hauptsächlich Polynome in einer Variablen mit Koeffizienten in den reellen Zahlen. Dabei werden vor allem die Nullstellen von Polynomen ersten Grades (lösen von linearen Gleichungen) bzw. zweiten Grades (große und kleine Lösungsformel) untersucht. Man kann mit der Lösungsformel für quadratische Polynome aber auch alle Nullstellen von Polynomen dritten Grades bestimmen, wenn schon eine Nullstelle des Polynoms bekannt ist. Auch dies wird teilweise in der Schule unterrichtet.
Betrachten wir zum Beispiel das Polynom

$$p(x) = x^3 + 2x^2 - x - 2.$$

Offensichtlich ist $p(1) = 0$, also 1 eine Nullstelle von p. Das Durchführen der Polynomdivision

$$\begin{array}{l}
(x^3 + 2x^2 - x - 2) : (x - 1) = x^2 + 3x + 2 \\
-(x^3 + x^2) \\
\qquad 3x^2 - x \\
\quad -(3x^2 + 3x) \\
\qquad\qquad 2x - 2 \\
\qquad\quad -\ (2x - 2) \\
\qquad\qquad\qquad 0 \text{ Rest}
\end{array}$$

ergibt, dass $p(x) = (x^2+3x+2)(x-1)$ und wir können durch das Berechnen der Nullstellen von x^2+3x+2 die restlichen zwei Nullstellen des Polynoms bestimmen. Das folgende Lemma besagt, dass dieses "wegdividieren der Nullstelle" immer ohne Rest möglich ist.

Lemma 1. *Gegeben seien ein Körper K, ein Polynom $p = \sum_{i=0}^{n} a_i x^i \in K[x]$ und ein Element $s \in K$. Falls $p(s) = 0$, dann gibt es ein Polynom $h \in K[x]$ mit $deg(h) = deg(p) - 1$, sodass*

$$p(x) = h(x)(x-s).$$

Beweis: Es sei $p = \sum_{i=0}^{n} a_i x^i \in K[x], s \in K$ und $p(s) = 0$. Der Leitterm von p ist $a_n x^n$. Setzen wir nun $x = s$ für ein x in x^n, erhalten wir ein Polynom p_{n-1} von höchstens Grad $n-1$, welches immer noch s als Nullstelle hat. Durch n-maliges iterieren erhalten wir folgende Folge von Polynomen

$$\begin{aligned}
p &= \sum_{i=0}^{n} a_i x^i, \\
p_{n-1} &= a_n s x^{n-1} + \sum_{i=0}^{n-1} a_i x^i \\
&= (\mathrm{LC}(p_n)s + a_{n-1})x^{n-1} + \sum_{i=0}^{n-2} a_i x^i, \\
p_{n-2} &= (\mathrm{LC}(p_{n-1})s + a_{n-2})x^{n-2} + \sum_{i=0}^{n-3} a_i x^i, \\
&\vdots \\
p_0 &= p(s) = 0.
\end{aligned}$$

Allgemein erhalten wir also die Rekursion

$$\mathrm{LC}(p_i) = \mathrm{LC}(p_{i+1})s + a_i \quad \text{für } i \in \{0, \dots n-1\} \tag{1}$$

für die Leitkoeffizienten der Polynome, wobei wir $p_n := p$ definieren. Hier ist streng genommen zu erwähnen, dass wir die Polynome p_i immer als Polynome vom Grad i auffassen, wobei diese (im Falle der Existenz von doppelten Nullstellen) auch von niedrigerem Grad sein können. Somit lassen wir zu, dass der Leitkoeffizient eines Polynoms Null sein kann, wobei dies eigentlich nicht mit der Definition des Leitkoeffizienten übereinstimmt. Anderenfalls könnten wir Gleichung (1) allerdings nicht in einer allgemeinen geschlossenen Form angeben.

Weiter beobachten wir, dass

$$
\begin{aligned}
p_{n-1}(x) &= \sum_{i=0}^{n} a_i x^i - (a_n x^n - a_n s x^{n-1}) \\
&= p_n(x) - a_n x^{n-1}(x-s) \\
&= p_n(x) - \mathrm{LC}(p_n) x^{n-1}(x-s), \\
p_{n-2}(x) &= p_{n-1}(x) - \mathrm{LC}(p_{n-1}) x^{n-2}(x-s), \\
&\vdots \\
0 = p_0(x) &= p_1(x) - \mathrm{LC}(p_1)(x-s).
\end{aligned}
$$

Daher gilt, dass

$$
\begin{aligned}
0 = p_0(x) &= p_1(x) - \mathrm{LC}(p_1)(x-s) \\
&= p_2(x) - \mathrm{LC}(p_2)x(x-s) - \mathrm{LC}(p_1)(x-s) \\
\cdots &= p(x) - \sum_{i=0}^{n-1} \mathrm{LC}(p_{i+1}) x^i (x-s).
\end{aligned}
$$

Also $p(x) = h(x)(x-s)$ mit

$$
h(x) = \sum_{i=0}^{n-1} \mathrm{LC}(p_{i+1}) x^i.
$$

Offensichtlich ist h ein Polynom vom Grad $n-1$ da $\mathrm{LC}(p_n) = a_n \neq 0$ ist. $\square$

Der Beweis von Lemma 1 liefert mit den Formeln (1) auch gleich ein effizientes Verfahren zur Berechnung des Polynoms h. Wir können nun von einem Polynom sukzessiv Nullstellen “wegdividieren” und somit den Grad des Polynoms reduzieren. Für ein Polynom von Grad n ist daher relativ klar, dass dies höchstens n mal möglich ist. Somit folgt ziemlich unmittelbar aus Lemma 1 folgender Satz.

Satz 1. *Es sei K ein Körper, $p \in K[x]$ ein Polynom vom Grad $n \in \mathbb{N}$. Dann gibt es für alle Teilmengen $S \subset K$ mit $|S| > n$ zumindest ein Element $s \in S$, sodass*

$$
p(s) \neq 0.
$$

In anderen Worten: Jedes Polynom $0 \neq p \in K[x]$ hat höchstens deg(p) viele unterschiedliche Nullstellen, bzw. hat ein Polynom mehr unterschiedliche Nullstellen als dessen Grad, dann ist es das konstante Nullpolynom.

Beweis: Es sei $0 \neq p \in K[x]$ ein Polynom vom Grad n und $S = \{s_1, \ldots s_n, s_{n+1}\} \subset K$. Angenommen alle Punkte aus S sind Nullstellen von p

$$
p(s_i) = 0 \quad \text{für alle } i \in \{1, \ldots, n+1\}.
$$

Insbesondere ist also $p(s_1) = 0$ und daher gibt es laut Lemma 1 ein Polynom $h \in K[x]$ mit $\deg(h) = n - 1$ und

$$p(x) = (x - s_1)h(x).$$

Da $p(s_2) = 0$ und $s_2 \neq s_1$ folgt, dass $h(s_2) = 0$ ist und daher gibt es laut Lemma 1 ein Polynom $\tilde{h}$ sodass,

$$p(x) = (x - s_1)(x - s_2)\tilde{h}(x) \quad \text{wobei } \deg(\tilde{h}) = n - 2.$$

Iteratives Wiederholen bis s_n liefert

$$p(x) = (x - s_1) \cdots (x - s_n)q(x),$$

für ein $q \in K[x]$ mit $\deg(q) = n - n = 0$. Also ist $q(x) = c$ für eine Konstante $c \in K$. Da aber auch $p(s_{n+1}) = 0$ und $s_{n+1} \neq s_i$ für $i \in \{1, \ldots, n\}$ folgt, dass $q(s_{n+1}) = c$ Null sein muss. Somit ist q das konstante Nullpolynom. Das heißt aber auch, dass p das konstante Nullpolynom ist, ein Widerspruch. □

2.2 Erweiterung auf beliebige Dimensionen

Wir wissen nun also, dass ein Polynom in einer Variable höchsten so viele Nullstellen haben kann wie dessen Grad. Wir wollen nun diese Aussage verwenden, um auch Aussagen über die Nullstellen von Polynomen in mehreren Variablen treffen zu können. Allerdings haben Polynome in mehreren Variablen nicht mehr unbedingt endlich viele Nullstellen. Betrachten wir zum Beispiel den Polynomring $\mathbb{R}[x, y]$. Hier verschwindet beispielsweise das Polynom $p(x, y) = xy$ genau dann, wenn $x = 0$ und/oder $y = 0$ ist. Das Polynom p verschwindet also auf dem gesamten Koordinatenkreuz $\{(a, b) \in \mathbb{R}^2 : a = 0 \vee b = 0\} \subset \mathbb{R}^2$ und hat somit unendlich viele Nullstellen. Wir können daher keine Aussage mehr über die Anzahl der Nullstellen von Polynomen in zwei Variablen machen. Allerdings ist es möglich eine Aussage zu treffen wie die Nullstellen sicher nicht in $\mathbb{R}^2$ verteilt sein können. Dazu betrachten wir ein Beispiel:
Gegeben seien das Polynom

$$p(x, y) = x^2y + 2x^2 - 2xy - 4x - 3y - 6$$

im Polynomring $\mathbb{R}[x, y]$ sowie Mengen

$$\begin{aligned} S_1 &= \{a_1, a_2, a_3\} \subset \mathbb{R}, \quad a_1 \neq a_2 \neq a_3 \neq a_1 \\ S_2 &= \{b_1, b_2\} \subset \mathbb{R}, \quad b_1 \neq b_2 \end{aligned}$$

Wir behaupten, dass das Polynom p nicht auf dem kartesischen Produkt $S_1 \times S_2$ verschwinden kann.
Um dies zu zeigen fassen wir die x-Terme in p zusammen

$$p(x, y) = (y + 2)x^2 + (-2y - 4)x + (-3y - 6).$$

Einsetzten von b_1 bzw. b_2 für y liefert zwei Polynome in einer Variablen:

$$p_1(x) = (b_1+2)x^2 + (-2b_1-4)x + (-3b_1-6)$$
$$p_2(x) = (b_2+2)x^2 + (-2b_2-4)x + (-3b_2-6)$$

Angenommen p verschwindet auf $S_1 \times S_2$, dann hat jedes der Polynome p_1, p_2 die drei unterschiedlichen Nullstellen a_1, a_2, a_3. Da aber beide Polynome vom Grad 2 sind folgt aus Satz 1, dass sowohl p_1 als auch p_2 das konstante Nullpolynom sind. Das wiederum bedeutet, dass zum Beispiel

$$0 = b_1 + 2 = b_2 + 2,$$

also das Polynom $y+2$ zwei unterschiedliche Nullstellen besitzt was wiederum im Widerspruch zur Aussage von Satz 1 steht. Daher muss es also ein Element $(a_i, b_j) \in S_1 \times S_2$ $(i \in \{1,2,3\}, j \in \{1,2\})$ geben, mit

$$p(a_i, b_j) \neq 0.$$

Allgemein lässt sich folgendes Lemma formulieren

Lemma 2. *Es sei K ein Körper und $p \in K[\underline{x}]$ ein Polynom in n Variablen über K. Des Weiteren seien für alle $i \in \{1,\dots,n\}$ Mengen $S_i \subset K$ gegeben mit $|S_i| > deg_i(p)$. Falls $p(s_1,\dots,s_n) = 0$ für alle n-Tupel $(s_1,\dots,s_n) \in S_1 \times \dots \times S_n$, dann ist $p \equiv 0$, also das konstante Nullpolynom.*

Beweis: Der Beweis funktioniert wie im vorherigen Beispiel mittels vollständiger Induktion über n.
Induktionsanfang: $n = 1$
Für $n = 1$ ist die Aussage des Lemmas, dass ein Polynom $0 \neq p \in K[x]$ höchstens $\deg(p)$ viele unterschiedliche Nullstellen haben kann, was wir bereits in Satz 1 gezeigt haben.

Induktionsschritt: $n-1 \to n$
Es sei $n \in \mathbb{N} (n \geq 2)$ und die Aussage des Lemmas gelte für $n-1$. Sei $p \in K[\underline{x}]$, sowie $S_1,\dots,S_n$ Teilmengen von K mit $|S_i| > \deg_i(p)$ für alle $i \in \{1,\dots,n\}$. Umschreiben von p als ein Polynom in x_n liefert

$$\begin{aligned}
p &= \sum_{\alpha \in \mathbb{N}^n} c_\alpha \underline{x}^\alpha \\
&= \sum_{\alpha \in \mathbb{N}^n : \alpha_n = 0} c_\alpha \underline{x}^\alpha + \sum_{\alpha \in \mathbb{N}^n : \alpha_n = 1} c_\alpha \underline{x}^\alpha + \dots + \sum_{\alpha \in \mathbb{N}^n : \alpha_n = \deg_n(p)} c_\alpha \underline{x}^\alpha \\
&= \sum_{k=0}^{\deg_n(p)} p_k(x_1,\dots,x_{n-1}) x_n^k.
\end{aligned}$$

Dabei sind die Polynome p_k Polynome in den Variablen $x_1, \ldots, x_{n-1}$ mit

$$\deg_i(p_k) \leq \deg_i(p) \quad \text{für alle } i \in \{1, \ldots, n-1\}.$$

Daher gilt für alle $k \in \{0, \ldots \deg_n(p)\}$, dass für die Polynome p_k zusammen mit den Mengen $S_1, \ldots S_{n-1}$ die Aussage von Lemmas 2 angewendet werden kann. Fixiere nun ein beliebiges Element $(s_1, \ldots s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$ und betrachte das Polynom

$$p(s_1, \ldots, s_{n-1}, x_n) = \sum_{k=0}^{\deg_n(p)} p_k(s_1, \ldots, s_{n-1}) x_n^k \in K[x_n].$$

Dieses Polynom verschwindet auf allen Punkten $s_n \in S_n$ und hat somit mindestens $|S_n| > \deg_n(p)$ viele unterschiedliche Nullstellen woraus aus Satz 1 folgt, dass $p(s_1, \ldots, s_{n-1}, x_n) \equiv 0$
Da $(s_1, \ldots s_{n-1})$ beliebig gewählt war, gilt für alle $k \in \{0, \ldots \deg_n(p)\}$ und für alle $(s_1, \ldots s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, dass

$$p_k(s_1, \ldots, s_{n-1}) = 0.$$

Dies impliziert aber aufgrund der Induktionsvoraussetzung, dass

$$p_k \equiv 0 \quad \text{für alle } k \in \{0, \ldots \deg_n(p)\}$$

woraus wiederum folgt, dass $p \equiv 0$. □

2.3 Gradreduktion und Formulierung des Satzes

Das Ergebnis von Lemma 2 können wir nun verwenden, um zu zeigen, dass etwas ähnliches wie das "wegdividieren von Nullstellen" auch für Polynome in mehreren Variablen immer ohne Rest möglich ist. Betrachten wir zum Beispiel ein Polynom $p = \sum_{i=1}^n h_i g_i$ wobei die Polynome $h_i \in K[\underline{x}]$ und die Polynome $g_i \in K[x_i]$, also jeweils nur von der Variable x_i abhängen und von der Form $g_i = \prod_{s \in S_i}(x_i - s)$ sind, für Mengen $S_1, \ldots S_n \subset K$. Offensichtlich verschwindet dieses Polynom auf dem gesamten kartesischen Produkt $S_1 \times \cdots \times S_n$, da alle Summanden stehts Null werden. Das folgende Lemma besagt, dass falls umgekehrt ein Polynom p auf dem kartesischen Produkt $S_1, \ldots S_n$ verschwindet man immer eine Darstellung der Form $p = \sum_{i=1}^n h_i g_i$ finden kann. Im Grunde funktioniert der Beweis des Lemmas sehr ähnlich wie der Beweis in Lemma 1, nämlich durch kontinuierliche Reduktion des Grades des Polynoms bis man beim konstanten Nullpolynom angekommen ist.

Lemma 3. *Gegeben seien ein Körper K, ein Polynom $p \in K[\underline{x}]$, nichtleere Mengen $S_1, \dots S_n \subset K$, sowie Polynome $g_i = \prod_{s \in S_i}(x_i - s) \in K[\underline{x}]$ für $1 \leq i \leq n$. Falls p auf allen gemeinsamen Nullstellen von $g_1, \dots g_n$ verschwindet (das heißt $p(s) = 0$ für alle $s \in S_1 \times \dots \times S_n$), dann gibt es Polynome $h_1, \dots h_n \in K[\underline{x}]$ mit $deg(h_i) \leq deg(p) - deg(g_i)$, sodass*

$$p = \sum_{i=1}^{n} h_i g_i.$$

Beweis: Seien $p \in K[\underline{x}], S_1, \dots, S_n \subset K$ mit

$$p(s_1, \dots, s_n) \equiv 0, \tag{2}$$

wobei wir $s_1, \dots, s_n$ als Variablen in $S_1, \dots, S_n$ betrachten. Für alle $i \in \{1, \dots, n\}$ definieren wir die Polynome

$$g_i(x_i) = \prod_{s \in S_i}(x_i - s) = x_i^{|S_i|} - \sum_{j=0}^{|S_i|-1} g_{ij} x_i^j, \quad g_{ij} \in K. \tag{3}$$

Da $g_i(s_i) \equiv 0$, gelten die Gleichungen

$$s_i^{|S_i|} = \sum_{j=0}^{|S_i|-1} g_{ij} s_i^j \quad \text{für alle } i \in \{1, \dots, n\}. \tag{4}$$

Durch diese Gleichungen können wir nun in jedem Monom von $p(\underline{s})$ jedes Auftreten eines $s_i^{f_i} (1 \leq i \leq n)$ mit $f_i > |S_i|$ durch eine Linearkombination kleinerer Potenzen von s_i ersetzen.
Betrachten wir hierzu zum Beispiel ein Monom $\underline{s}^\alpha \in \operatorname{supp}(p)$ mit $\alpha_i > |S_i|$. Also $\underline{s}^\alpha = s_i^{|S_i|} \tilde{h}_i$ mit $\tilde{h}_i \in K[\underline{s}]$ und $\deg(\tilde{h}_i) \leq \deg(p) - \deg(g_i)$. Durch Anwenden der richtigen Gleichung in (4) erhalten wir also

$$\begin{aligned}
\underline{s}^\alpha &= s_i^{|S_i|} \tilde{h}_i(\underline{s}) \\
&\overset{(4)}{=} \left(\sum_{j=0}^{|S_i|-1} g_{ij} s_i^j \right) \tilde{h}_i(\underline{s}) \\
&\overset{(3)}{=} (s_i^{|S_i|} - g_i(s_i)) \tilde{h}_i(\underline{s}) \\
&= \underline{s}^\alpha - g_i(s_i) \tilde{h}_i(\underline{s}).
\end{aligned}$$

In der zweiten Zeile dieser Rechnung kann man gut erkennen, dass die Potenz in s_i um einen Grad gesenkt wurde und aus der letzten Zeile wird ersichtlich, dass diese Gradreduktion dem Subtrahieren des Polynoms $\tilde{h}_i g_i$ entspricht. Wiederholtes Reduzieren der Potenzen in allen Variablen liefert nun ein Polynom

$$\bar{p}(\underline{s}) = p(\underline{s}) - \sum_{i=1}^{n} h_i(\underline{s}) g_i(s_i),$$

mit $h_i \in K[\underline{s}]$ und $\deg(h_i) \leq \deg(p) - \deg(g_i)$ für alle $i \in \{1, \ldots, n\}$. Offensichtlich gilt, dass $\deg_i(\bar{p}) < |S_i|$ für alle $i \in \{1, \ldots n\}$. Da $g_i(s_i) \equiv 0$ für alle $i \in \{1, \ldots, n\}$ gilt, dass

$$\bar{p}(\underline{s}) = p(\underline{s}) \equiv 0$$

Das heißt aber nach Lemma 2, dass $\bar{p}$ auch als Polynom über dem gesamten Körper K das konstante Nullpolynom sein muss und daher gilt

$$p(\underline{x}) = \sum_{i=1}^{n} h_i(\underline{x}) g_i(\underline{x}).$$

□

Mithilfe dieses Ergebnisses können wir nun den kombinatorischen Nullstellensatz beweisen. Die gravierende Verbesserung zur Aussage von Lemma 2 ist dabei, dass die Kardinalitäten der Mengen S_i nicht mehr größer sein müssen als die jeweils höchsten im Polynom auftretenden Potenzen von x_i. Es genügt ein im Polynom vorkommendes Monom zu betrachten, dessen Grad gleich groß ist wie der Grad des Polynoms. Die Mengen S_i müssen dann lediglich mehr Elemente beinhalten als die jeweils höchste Auftretende Potenz von x_i in genau diesem Monom.

Satz 2 (Kombinatorischer Nullstellensatz)**.** *Es seien K ein Körper, $p \neq 0$ ein Polynom im Polynomring $K[\underline{x}]$, sowie $\alpha \in supp(p)$ mit $|\alpha| = deg(p)$. Dann gibt es für alle Teilmengen $S_1, \ldots, S_n$ mit $|S_i| > \alpha_i$, zumindest ein Element $s = (s_1, \ldots s_n) \in S_1 \times \cdots \times S_n$, sodass*

$$p(s) = p(s_1, \ldots, s_n) \neq 0$$

ist.

Beweis: Je größer die Kardinalitäten der Mengen $S_1 \ldots S_n$, desto mehr Punkte stehen zur Auswahl auf dem das Polynom ungleich Null sein könnte. Somit genügt es ohne Einschränkung der Allgemeinheit die Aussage für Mengen kleinstmöglicher Kardinalität zu zeigen, also für Mengen mit $|S_i| = \alpha_i + 1$.
Seien also $0 \neq p \in K[\underline{x}], \alpha \in \operatorname{supp}(p)$ mit $|\alpha| = \deg(p)$ und $S_1 \ldots S_n \subset K$ mit $|S_i| = \alpha_i + 1$. Weiters setzen wir $g_i = \prod_{s \in S_i}(x_i - s)$ für alle $i \in \{1, \ldots n\}$.
Angenommen $p(s_1, \ldots, s_n) = 0$ für alle $(s_1, \ldots s_n) \in S_1 \times \cdots \times S_n$. Dann gibt es laut Lemma 3 Polynome $h_1, \ldots h_n \in K[\underline{x}]$ mit $\deg(h_i) \leq \deg(p) - \deg(g_i) = |\alpha| - |S_i|$, sodass

$$p = \sum_{i=1}^{n} h_i g_i. \tag{5}$$

Laut Voraussetzung gilt nun, dass der Koeffizient von $\underline{x}^\alpha$ auf der linken Seite von Gleichung (5) ungleich Null ist. Falls aber andererseits in einem der Polynome $h_i g_i$ das Monom $\underline{x}^\alpha$ auftauchen soll, muss man aus Grad-Gründen

$(\deg(h_i) + \deg(g_i) \leq |\alpha|)$ dafür $x_i^{\alpha_i+1}$ aus g_i benutzen. Damit ist aber die i-te Potenz $(\alpha_i + 1)$ zu groß. Daher kann das Monom $\underline{x}^\alpha$ in keinem der Polynome $h_i g_i$ vorkommen. Dies steht allerdings im Widerspruch zur Gleichheit in (5).

□

Bemerkung 4. *In der Literatur findet man mehrere unterschiedliche Beweise diese Resultats, einschließlich deutlich kürzerer Beweise [10, 5]. Der Name "kombinatorischer Nullstellensatz" kommt daher, dass Alon in seiner ursprünglichen Arbeit auch die Aussage von Lemma 3 als kombinatorischen Nullstellensatz bezeichnet. Offensichtlich hat dieses Lemma eine sehr große Ähnlichkeit zum klassischen Nullstellensatz von Hilbert (siehe z. B. [1], S.1).*

3 Anwendungen in der Schule

3.1 Bezug zum Lehrplan

Der kombinatorische Nullstellensatz wird im österreichischen Lehrplan nicht erwähnt (wahrscheinlich in keinem einzigen Lehrplan der Welt). Nichtsdestotrotz werden in der Schule Themen behandelt, die durchaus mit der Thematik des Satzes in Verbindung gebracht werden können. So sind zum Beispiel zwei Hauptthemen der AHS-Unterstufe das **"Arbeiten mit Figuren und Körpern"** und das **"Arbeiten mit Variablen"**. Deshalb kann gegen Ende der Unterstufe durchaus anhand von Beispielen aufgezeigt werden, dass die Nullstellenmengen von Polynomen interessante geometrische Objekte sein können. Weiters sind dann im Lehrplan der 5. Klasse Oberstufe folgende Lernziele formuliert:

- Lineare Gleichungssysteme in zwei Variablen lösen und deren Lösungsfälle untersuchen und geometrisch interpretieren können.
- Quadratische Funktionen der Form $f(x) = ax^2 + bx + c$ beschreiben und untersuchen können.
- Lineare und quadratische Gleichungen in einer Variablen lösen können; Lösungsfälle untersuchen können [2].

Das Lösen von linearen Gleichungssystemen entspricht also dem Betrachten der Nullstellenmengen von Polynomen vom Grad 1 in zwei Variablen und das Lösen von quadratischen Gleichungen ist das Finden der Nullstellenmengen von Polynomen vom Grad 2 in einer Variablen. Schlussendlich werden in der 7. Klasse der AHS-Oberstufe Polynome höheren Grades in einer Variablen sowie einige Polynome in zwei Variablen behandelt.

- Einfache Polynomgleichungen vom Grad ≤ 4 im Bereich der reellen Zahlen lösen können.
- Untersuchungen von Polynomfunktionen in inner- und außermathematischen Bereichen durchführen können; einfache Extremwertaufgaben lösen können.

- Kreise, Kugeln und Kegelschnittslinien durch Gleichungen beschreiben können.
- Die gegenseitige Lage von Kreis und Gerade bestimmen und allenfalls vorhandene Schnittpunkte berechnen können; eine Gleichung der Tangente in einem Punkt eines Kreises ermitteln können.
- Die gegenseitige Lage von Kegelschnitt und Gerade bestimmen und allenfalls vorhandene Schnittpunkte berechnen können; eine Gleichung der Tangente in einem Punkt eines Kegelschnitts ermitteln können.
- Den Fundamentalsatz der Algebra kennen [2].

Inwiefern Kreise, Kugeln und Kegelschnitte mit dem kombinatorischen Nullstellensatz zusammenhängen, werden wir später noch ein wenig genauer erläutern. Der Fundamentalsatz der Algebra ist bezüglich dieses Themas insofern zu nennen, da dieser besagt, dass es einen Körper ($\mathbb{C}$) gibt, bezüglich dem die Schranke des kombinatorischen Nullstellensatzes (zumindest für $n = 1$) für jedes Polynom (mit dem Zählen von Vielfachheiten) scharf ist.

3.2 Einige Beispiele für die Schule

In diesem Abschnitt soll erläutert werden inwieweit die Aussage des kombinatorischen Nullstellensatzes im Schulunterricht veranschaulicht werden kann, ohne diesen explizit formulieren zu müssen. Ein mögliches Beispiel wäre der Einheitskreis, denn dieser ist ja die Nullstellenmenge des Polynoms

$$p(x, y) = x^2 + y^2 - 1.$$

Dies ist ein Polynom zweiten Grades in zwei Variablen und eine Aussage des kombinatorsischen Nullstellensatzes wäre, dass man keine Zahlen $a_1, a_2, a_3, b_1 \in \mathbb{R}$ finden kann, sodass

$$p(a_1, b_1) = p(a_2, b_1) = p(a_3, b_1) = 0$$

ist. Geometrisch würde das heißen, dass man keine Gerade zeichnen kann die 3 Schnittpunkte mit einem Kreis besitzt. In der Schule könnte man für dieses Beispiel folgendermaßen vorgehen.
Zuerst wird mit Hilfe einer Dynamischen-Geometrie-Software (z.B Geogebra) visualisiert, dass die Nullstellenmenge des Polynoms $x^2 + y^2 - 1$ ein Kreis mit Mittelpunkt im Koordinatenursprung und Radius 1 ist. Nun können die Schüler rechnerisch überprüfen, dass der Einheitskreis die $x-$Achse in nur zwei Punkten schneidet. Die $x-$Achse wird beschrieben durch die Gleichung $y = 0$. Das Einsetzen dieser Gleichung in die ursprüngliche Kreisgleichung liefert also

$$x^2 - 1 = 0$$

und durch Anwenden der binomischen Formel $(a + b)(a - b) = a^2 - b^2$ ergibt sich

$$(x + 1)(x - 1) = 0.$$

Damit sind die beiden Schnittpunkte mit der $x-$ Achse die beiden Punkte $(-1,0)$ und $(1,0)$. Das Beispiel könnte dann noch weitergeführt werden in dem die Gleichung $y = c$ für ein beliebiges $c \in \mathbb{R}$ betrachtet wird. Daraus ergibt sich dann, dass

$$x = \pm\sqrt{1-c^2}.$$

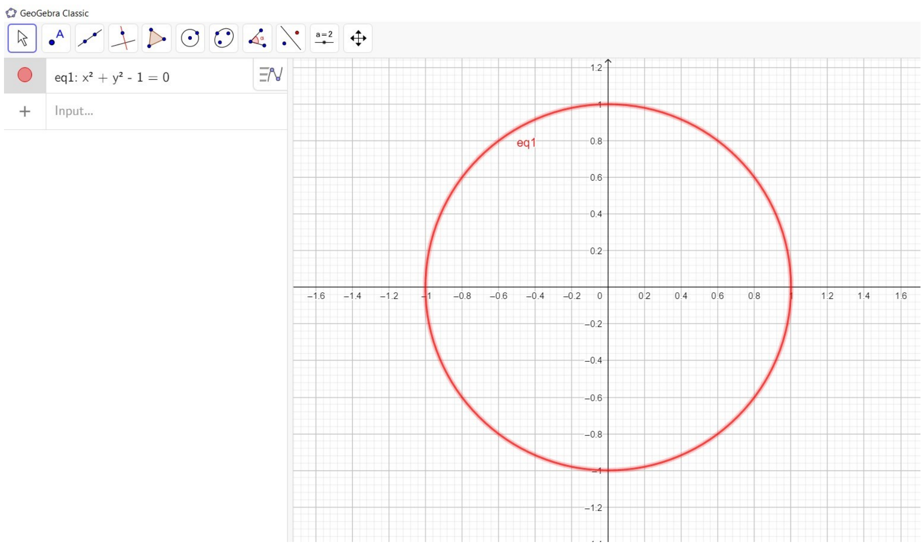


Abbildung 1: Visualisierung der Nullstellenmenge des Polynoms $x^2 + y^2 - 1$ mit Geogebra.

Somit ergeben sich die Schnittpunkte $(\sqrt{1-c^2}, c), (-\sqrt{1-c^2}, c)$ für $|c| < 1$. Für die Fälle $c = 1$ bzw. $c = -1$ gibt es jeweils nur einen Schnittpunkt und falls $|c| > 0$ ist, hat die obige Gleichung keine reelle Lösung und es existiert kein Schnittpunkt. Es gibt also für keinen $y-$ Wert drei $x-$Werte sodass die Gleichung $x^2 + y^2 - 1 = 0$ erfüllt ist und das ist genau die Aussage des kombinatorischen Nullstellensatzes für das Polynom $p(x,y) = x^2 + y^2 - 1$
Die gleichen Überlegungen könnte man auch für Hyperbeln, Parabeln oder Kugeln anstellen, da diese ja ebenfalls Nullstellenmengen von quadratischen Polynomen in zwei bzw. drei Variablen sind.

Ein weiteres für den Schulunterricht einsetzbares Beispiel wäre das Polynom

$$p(x,y) = xy$$

zu betrachten. Die geometrische Aussage des kombinatorischen Nullstellensatzes hierzu wäre, dass es kein Rechteck gibt, dessen Seitenkanten parallel zu den Koordinatenachsen sind und dessen Ecken alle auf dem Koordinatenkreuz liegen. Dies kann den Schülern und Schülerinnen wiederum mit Geogebra veranschaulicht werden. Hierbei könnte man im Sinne des entdeckenden Lernens die

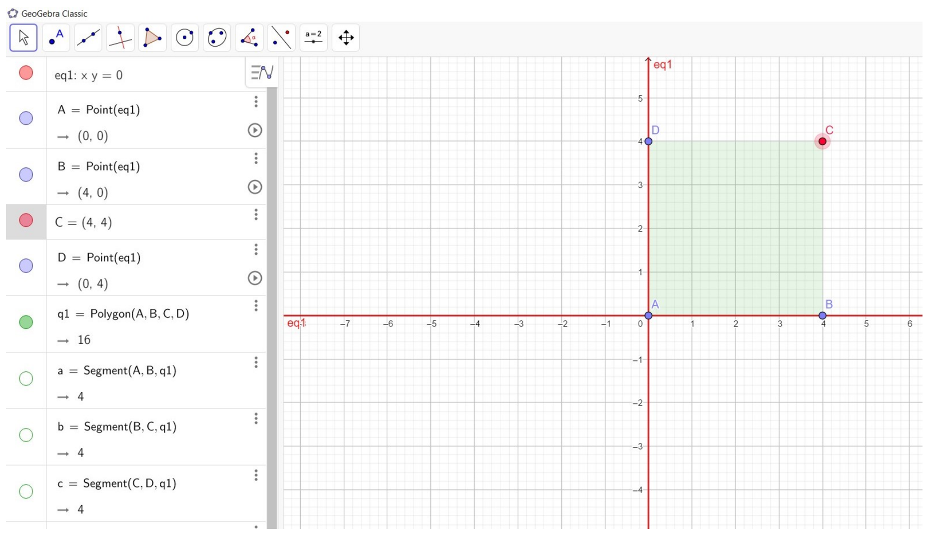


Abbildung 2: Kombinatorischer Nullstellensatz für das Polynom xy.

Schüler und Schülerinnen Nullstellenmengen von unterschiedlichsten Polynomen in zwei Variablen plotten lassen, um anschließend ein Gitter mit möglichst vielen Gitterpunkten (kartesisches Produkt von zwei möglichst großen Mengen) zu konstruieren, sodass noch jeder Gitterpunkt auf der Nullstellenmenge liegt. Dabei sollen sie versuchen Fragen zu beantworten wie:

- Ist die Anzahl der maximal möglichen Gitterpunkte immer gleich groß?
- Was denkst du, beeinflusst die maximale Anzahl der Gitterpunkte?
- Kannst du eine Gesetzmäßigkeit entdecken?
- Wenn ja, formuliere deine Vermutung.

Natürlich müssen hierbei die Polynome von der Lehrperson so geschickt vorgegeben werden, dass es talentierten Schülern und Schülerinnen zugetraut werden kann die Aussage des Nullstellensatzes für Polynome in zwei Variablen selbstständig erarbeiten zu können.

Die gesamte Aussage des kombinatorischen Nullstellensatzes verständlich zu erklären erscheint im regulären Schulunterricht schwer umsetzbar. Allerdings könnte des Satz durchaus in Projekten mit hochbegabten Schülern und Schülerinnen behandelt werden. Hierbei gibt es dann durchaus Aufgaben, welche durch Verwendung des Satzes sehr elegant gelöst werden können. Hierzu erwähnen wir noch eine Aufgabe, welche im Jahr 2007 bei der russischen Mathematikolympiade gestellt wurde (9. Klasse, Aufgabe 5, `https://imomath.com/othercomp/Rus/RusMO07.pdf`).

Gegeben sei ein konvexes $100-$gon. Jede Ecke wurde (vom heimtückischen Algebra-Professor) mit zwei beliebigen, aber unterschiedlichen Zahlen beschriftet. Nun soll jeweils eine der beiden Zahlen von jeder Ecke entfernt werden, sodass sich die übrigen Zahlen aller angrenzenden Ecken unterscheiden. Zeige, dass dies immer möglich ist.

Lösung:
Wir bezeichnen die Beschriftungen der Ecken 1-100 mit den zweielementigen Mengen $S_1, S_2, \ldots S_{100} \subset \mathbb{R}$ und betrachten das Polynom

$$p(x_1, \ldots, x_{100}) = (x_1 - x_2)(x_2 - x_3) \cdots (x_{99} - x_{100})(x_{100} - x_1).$$

Dies ist ein Polynom in 100 Variablen und hat Grad 100. Des weiteren kommt das Monom

$$x_1 \cdot x_2 \cdots x_{99} \cdot x_{100}$$

im Polynom nach dem Ausmultiplizieren genau zweimal vor ($x_1 \cdot x_2 \cdots x_{99} \cdot x_{100}$ und $(-x_2) \cdots (-x_{100}) \cdot (-x_1)$). Da $(-1)^{100}$ positiv ist, ist der Koeffizient dieses Monoms 2, also ungleich Null. Der Grad des Monoms ist ebenfalls 100 und somit gibt es nach dem kombinatorischen Nullstellensatz zumindest ein Element $(s_1, \ldots, s_{100}) \in S_1 \times \cdots \times S_{100}$, sodass

$$p(s_1, \ldots, s_{100}) \neq 0$$

ist. Das heißt aber ja nichts anderes als, dass $s_1 \neq s_2, s_2 \neq s_3, \ldots s_{99} \neq s_{100}, s_{100} \neq s_1$, was genau der in der Aufgabe geforderten Beschriftung entspricht.

Offensichtlich funktioniert dieses Beispiel auch für beliebige $n-$gone, solange n eine gerade Zahl ist. Deshalb kann man den Schülern und Schülerinnen durch das Behandeln von Polygonen mit deutlich weniger Ecken die Fragestellung vermitteln. So könnte zum Beispiel ein Schüler die Ecken eines konvexen $5-$gons bzw. $6-$gons möglichst fies beschriften und eine Schülerin versucht durch das Entfernen der richtigen Zahlen eine Beschriftung zu erreichen, sodass sich die Zahlen aller angrenzenden Ecken unterscheiden. Die Mathefreaks bekommen dabei auf spielerische Art und Weise eine erste Intuition für die Aufgabe, bevor sie dann den "overkill" durch den kombinatorischen Nullstellensatz kennenlernen.

3.3 Das Horner-Schema

Im Beweis von Lemma 3 werden die Potenzen eines Polynoms durch iteratives Anwenden von Ganzheitsgleichungen immer weiter reduziert. Diese Technik der kontinuierlichen Reduktion des Grades findet in vielen Beweisen der Algebra seine Anwendung. Die wohl einfachste Variante so einer Gradreduktion ist das Horner-Schema. Dieses wird vor allem verwendet, um Funktionswerte von Polynomen numerisch effizient zu berechnen. Will man zum Beispiel eine Polynomfunktion $n-$ten Grades an der Stelle $x = a$ auswerten so benötigt man

- $n-1$ Multiplikationen zur Berechnung der Potenzen $a^2, a^3, \dots a^n$,
- weitere n Multiplikationen zur Multiplikation der Potenzen $a, a^2, \dots a^n$ mit ihren Koeffizienten,

also insgesamt $2n-1$ Multiplikationen [11]. Beim Horner-Schema allerdings reduziert man den Grad des Polynoms kontinuierlich, indem man nur für die jeweils höchste Potenz die Gleichung $x = a$ eisetzt. Da sich der Grad dabei immer um mindestens 1 reduziert muss man dies höchstens $n-$mal iterieren und kommt somit mit n Multiplikationen aus.
Obwohl das Horner-Schema nicht explizit im österreichischen Lehrplan erwähnt wird, kann man es durchaus in manchen Schulbüchern finden. So könnte in einer leistungsstarken Klasse das Horner-Schema mit Hilfe dieser iterativen Gradreduktion erarbeitet werden. Ein mögliches Beispiel dazu wäre:

Betrachte das Polynom $p(x) = x^3 - 5x^2 - 4x + 20$. Reduziere kontinuierlich den Grad des Polynoms, indem du jeweils im Term der höchsten Potenz ein x durch (-2) ersetzt.

$$\begin{aligned}\text{Lösung: } p_3(x) &= x^3 - 5x^2 - 4x + 20\\ p_2(x) &= -7x^2 - 4x + 20\\ p_1(x) &= 10x + 20\\ p_0(x) &= 0\end{aligned}$$

Sind die Schüler und Schülerinnen mit diesem “Reduzieren des Grades” vertraut können nun Fragen behandelt werden wie:

- An was kann man hier erkennen, dass -2 eine Nullstelle von p ist?
- Wie viele Multiplikationen musstest du durchführen um bei p_0 zu landen?
- Wie viele Multiplikationen müsstest du durchführen um p(-2) zu berechnen
- Ist -2 eine Nullstelle von p_2, p_1 oder p_0?
- Wie entstehen die Leitkoeffizienten in den jeweiligen Polynomen

Das Ziel wäre nun weiters Rekursionformel (1) für die Leitkoeffizienten der Polynome p_i zu erarbeiten, bzw. die Schüler und Schülerinnen die Rekursion selbst entdecken zu lassen.
Danach können durch das Durchführen der Polynomdivision $(x^3 - 5x^2 - 4x + 20) : (x+2) = x^2 - 7x + 10$ die Leitkoeffizienten der Polynome p_3, p_2, p_1, p_0 mit dem Ergebnis der Polynomdivision in Verbindung gebracht werden. Schlussendlich kann eine effektive Variante für die Polynomdivision mit linearem Divisor entwickelt werden.

Betrachten wir zum Beispiel wieder das Polynom $p(x) = x^3 - 5x^2 - 4x + 20$ mit Nullstelle -2. .

$$+ \qquad\qquad \cdot$$

$$(1,\ -5,\ -4,\ 20|-2)\ =\ (1,\ -7,\ 10,\ 0)$$

Abbildung 3: Effiziente Berechnung der Polynomdivision $x^3 - 5x^2 - 4x + 20 : x + 2$ mit Hilfe des Horner-Schemas.

Wir schreiben die Koeffizienten des Polynoms nach fallenden Potenzen in eine Zeile und nach einem Querstrich noch die Nullstelle die "wegdividiert" werden soll. Danach berechnen wir die Koeffizienten des Ergebnisses nach fallenden Potenzen. Der Koeffizient der höchsten Potenz ist der gleiche wie jener des ursprünglichen Polynoms. Zur Berechnung des Koeffizienten der zweithöchsten Potenz multiplizieren wir den bereits berechneten Koeffizienten mit der Nullstelle und addieren dazu den Koeffizienten der zweithöchsten Potenz im ursprünglichen Polynom. Dies wird so lange wiederholt, bis man in beim konstanten Koeffizienten des Polynoms angelangt ist. In der neu berechneten Zeile stehen nun die Koeffizienten des Ergebnisses der Polynomdivision, wobei der letzte Eintrag den Rest der Division angibt (vgl. z.B, [8]). Eine kompakte Schreibweise für die Division $(x^3 - 5x^2 - 4x + 20) : (x + 2)$ ist in Abbildung 3 dargestellt.

4 Bemerkungen und Ausblick

Wir haben in dieser Arbeit versucht einen Überblick über den kombinatorischen Nullstellensatz und dessen möglichen Anwendungsmöglichkeiten im Schulunterricht zu verschaffen. Insgesamt ist zu sagen, dass die Aussage des Satzes, wenn man mit Polynomen in mehreren Variablen und dem kartesischen Produkt von Mengen vertraut ist, "relativ" leicht zu verstehen ist. So kann man mathematisch Begabten in der AHS-Oberstufe durchaus zutrauen den kombinatorischen Nullstellensatz zu verstehen und für einige leichtere Beispiele anzuwenden. Insgesamt findet man in der Literatur mehrere Resultate für deren Beweise der Satz angewendet werden kann. Dabei wird im Grunde meist folgendermaßen vorgegangen. Die Idee ist es ein Gegenbeispiel zur Aussage zu konstruieren und dieses dann zu nützen, um ein Polynom zu konstruieren, welches auf einer großen kartesischen Produktmenge verschwindet. Gleichzeitig ist das Polynom aber auch explizit genug, sodass für ein bestimmtes Monom maximalen Grades versichert werden kann, dass dieses im Polynom vorkommt. Schließlich besagt dann der Nullstellensatz, dass dieses Polynom nicht auf der gesamten Produktmenge verschwinden kann und liefert somit einen Widerspruch.
Insgesamt lässt sich die Aussage des Nullstellensatzes noch ein wenig verallgemeinern. So muss der Grad des betrachteten Monoms in $\mathrm{supp}(p)$, nicht unbedingt gleich dem Grad des Polynoms sein. Denn es genügt wenn das Monom maximal

bezüglich einer speziellen partiellen Monomordnung ist.(für die genaue Formulierung und den Beweis des Satzes siehe Anhang).
Abschließend wollen wir noch erwähnen, dass der kombinatorische Nullstellensatz zwar eine Aussage über die Existenz eines Punktes, auf dem ein Polynom nicht verschwindet, macht, allerdings kann durch den Satz nicht angegeben werden, wie dieser Punkt gefunden werden kann. Es kann gezeigt werden, dass es, unter gewissen Einschränkungen an die univariaten Polynome (diese dürfen jeweils aus höchstens zwei Monomen bestehen), durchaus Algorithmen gibt, die den gesuchten Punkt in polynomieller Zeit finden können [9, 7]. Im Allgemeinen ist die Frage nach dem genauen Punkt, auf dem das Polynom nicht verschwindet, NP-schwer und kann daher nicht in polynomieller Zeit gelöst werden.

Literatur

1. Alon, N. Combinatorial Nullstellensatz. *Combin. Probab. Comput* **8,** 7–29 (1999).
2. BMBWF. *Lehrpläne der AHS-Unter- und Oberstufe* [Online Zugriff am 31.Oktober 2020]. `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568`.
3. Brunner, N. Axiome der Mengenlehre und mathematische Praxis (2002).
4. Lasoń, M. A generalization of Combinatorial Nullstellensatz. *arXiv preprint arXiv:1302.4647* (2013).
5. Michałek, M. A short proof of Combinatorial Nullstellensatz. *The American Mathematical Monthly* **117,** 821–823 (2010).
6. Netzer, T. *Vorlesungsskriptum: Lineare Algebra* [Online Zugriff am 31.Oktober 2020]. `https://www.uibk.ac.at/mathematik/algebra/media/teaching/lineare-algebra.pdf`.
7. Olaf, P. *Der kombinatorische Nullstellensatz und seine Anwendungen* Bachelorarbeit. 2012.
8. Rapp, H. in *Mathematik für die Fachschule Technik* 417–420 (Springer, 2001).
9. Schauz, U. *Algebraically Solvable Problems* Doktorarbeit. 2007.
10. Tao, T. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *arXiv preprint arXiv:1310.6482* (2013).
11. Wikipedia Beitragende. *Horner-Schema — Wikipedia, Die freie Enzyklopädie* [Online Zugriff am 31.Oktober 2020]. `https://de.wikipedia.org/wiki/Horner-Schema`.

Anhang

Im Laufe des Schreibens dieser Arbeit stieß ich zufällig darauf, dass mit der eingeführten Kurzschreibweise für die Polynomdivision mit linearem Divisor (vgl, Abbildung 3), der Beweis der Verschärfung des kombinatorischen Nullstellensatzes relativ ausführlich und trotzdem verständlich aufgeschrieben werden kann. Deshalb will ich dieses Resultat noch im Anhang präsentieren.

Wir definieren die partielle Monomordnung $\leq$ auf $\mathbb{N}^n$ durch

$$(\alpha_1, \dots \alpha_n) \leq (\beta_1, \dots, \beta_n) :\Longleftrightarrow \alpha_i \leq \beta_i \quad \text{für alle } i \in \{1, \dots, n\}.$$

Falls im Folgenden von einem maximalen $n-$Tupel $\alpha \in \mathbb{N}^n$ die Rede ist, dann ist hiermit gemeint, dass α maximal bezüglich der oben definierten partiellen Ordnung $\leq$ auf $\mathbb{N}^n$ ist.

Satz 3 (Verallgemeinerung der kombinatorischen Nullstellensatzes)**.** *[4] Es seien K ein Körper, $p \neq 0$ ein Polynom im Polynomring $K[\underline{x}]$, sowie α maximal in supp(p). Dann gibt es für alle Teilmengen $S_1, \dots, S_n$ mit $|S_i| > \alpha_i$, zumindest ein Element $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$, sodass*

$$p(s_1, \dots, s_n) \neq 0$$

ist.

Beweis: Sei $n \in \mathbb{N}$ beliebig. Wir beweisen mittels Induktion über $k := |\alpha|$.
Induktionsanfang: $k = 0$:
Für $|\alpha| = 0$ ist $p \equiv c \neq 0$ und somit ist die Aussage wahr.

Induktionsschritt: $k - 1 \to k$:
Die Aussage gelte für alle Polynome $p \in K[\underline{x}]$ für die es ein maximales $n-$Tupel α gibt mit $|\alpha| = k - 1 (k \geq 1)$.

Sei nun $p \in K[\underline{x}]$ mit maximalem $\alpha \in \text{supp}(p)$ und $|\alpha| = k$. O.E.d.A. können wir annehmen, dass $\alpha_1 > 0$. Wir setzen $m := \deg_1(p)$ und schreiben p ähnlich wie im Beweis von Lemma 2 als Polynom von x_1 mit Koeffizienten in $K[x_2, \dots, x_n]$. Also

$$p = \sum_{j=0}^{m} p_j(x_2, \dots, x_n) x_1^j,$$

mit $\text{supp}(p_j) = \{(\beta_2, \dots, \beta_n) : (\beta_1, \dots, \beta_n) \in \text{supp}(p), \beta_1 = j\}$ für alle $j \in \{0, \dots m\}$. Wir fixieren ein $s \in S_1$ und wollen nun p durch $(x - s)$ dividieren und schreiben wie in Abbildung 3 in Kurzschreibweise

$$(p_m, p_{m-1}, \dots, p_0 | s) = (\underbrace{p_m, sp_m + p_{m-1}, \dots,}_{\text{Koeffizienten von } g} \underbrace{h)}_{\text{Rest}}, \tag{6}$$

also

$$p = g(x_1 - s) + h,$$

wobei die Koeffizienten von g (als Polynom von x_1) bzw. das Restpolynom h in (6) auf der rechten Seite stehen. Offensichtlich sind alle Koeffizienten von g sowie auch das Restpolynom h Linearkombinationen von den p_j. Deshalb hängt h nicht von x_1 ab und wenn es $s_2 \in S_2, \dots s_n \in S_n$ gib mit $h(s_2, \dots, s_n) \neq 0$, dann ist auch $p(s, s_2, \dots, s_n) \neq 0$ was die Aussage beweist. Andernfalls gilt dass h auf $S_2 \times \cdots \times S_n$ verschwindet.
Wir zeigen nun noch, dass das Tupel $(\alpha_1 - 1, \alpha_2, \dots \alpha_n)$ maximal in $\operatorname{supp}(g)$ ist. Falls $\alpha_1 = m$, ist dies klar. Falls $\alpha_1 < m$ wissen wir durch die Maximalität von α in $\operatorname{supp}(p)$, dass $(\alpha_2, \dots \alpha_n)$ maximal in $\cup_{j=\alpha_1}^{m} \operatorname{supp}(p_j)$ ist und dass p_{α_1} das einzige Polynom in dieser Vereinigung ist in dem das Monom $x^{\alpha_2 \cdots \alpha_n}$ vorkommt. Aber der Koeffizient von $x^{\alpha_1 - 1}$ des Polynoms g ist eine Linearkombination der Polynome $p_m, p_{m-1}, \dots, p_{\alpha_1}$, wobei der Koeffizient von p_{α_1} Eins ist.
Also ist $(\alpha_1 - 1, \alpha_2, \dots \alpha_n)$ maximal in $\operatorname{supp}(g)$ und nach der Induktionsvoraussetzung existiert ein Element $(s_1, s_2, \dots, s_n) \in S_1 \setminus \{s\} \times S_2 \times \cdots \times S_n$, sodass $g(s_1, \dots, s_n) \neq 0$ ist und daher ist auch

$$p(s_1, s_2, \dots, s_n) = \underbrace{g(s_1, s_2, \dots s_n)}_{\neq 0} \underbrace{(s - s_1)}_{\neq 0} + \underbrace{h(s_2, \dots s_n)}_{=0} \neq 0.$$

$\square$