Nullstellen von Polynomen und Erweiterungskörper
Vortrag im Modul "Kommunikation über Mathematik"

Alexander Steen,
a.steen@fu-berlin.de

1 Polynome und ihre Nullstellen

Als erstes betrachten wir Nullstellen von Polynomen genauer und identifizieren einen engen Zusammenhang zwischen Nullstellen und der Irreduzibilität von Polynomen. Einige Ergebnisse dieses Abschnitts haben tiefgreifende Bedeutung und kommen in allen möglichen Teilgebieten der Mathematik wieder vor.

Satz 1.1 (Zerlegung) Sei $A \in \mathbb{F}[X]$ ein Polynom, $\lambda \in \mathbb{F}$ mit $A(\lambda) = 0$. Dann existiert ein $F \in \mathbb{F}[X]$, s.d. $A = (X - \lambda) \cdot F$. ⌟

Beweis 1.1 Es wird nur der Fall grad $A \geq 1$ betrachtet, im Falle von grad $A = 0$ folgt die Behauptung direkt. Betrachten wir also zunächst die Division mit Rest von A und $(X - \lambda)$. Danach gilt: Für $F, R \in \mathbb{F}[X]$ ist

$$A = F \cdot (X - \lambda) + R, \quad \text{grad } R < 1$$

Gleichzeitig gilt aber

$$\begin{aligned} 0 = A(\lambda) &= F(\lambda) \cdot (\lambda - \lambda) + R(\lambda) \\ &= F(\lambda) \cdot 0 + R(\lambda) \\ &= R(\lambda) \end{aligned}$$

und da grad $R < 1$ damit $R \equiv 0$. □

Für Polynome A mit mehreren Nullstellen $\lambda_1, \ldots, \lambda_n$, liefert das iterierte Argument von Satz 1.1 eine entsprechende Zerlegung: So existiert dann ein $F \in \mathbb{F}$ mit

$$A = (X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n) \cdot F$$

Sind wir nun an der Anzahl der Nullstellen von A interessiert, können wir dies für Polynome vom Grad 1 direkt ermittelt:

Sei also $A = aX + b \in \mathbb{F}[X]$ ein Polynom und $a \neq 0$ (sonst wäre A nicht von Grad 1). Dann hat A genau eine Nullstelle, nämlich $\lambda = -\frac{b}{a}$. Dies ist z.B. aus $a \cdot X + b = X + \frac{b}{a}$ ersichtlich. Für Polynome höherer gerade können wir à priori keine Schätzung der Nullstellen vornehmen. Die obige Überlegung sichert uns allerdings eine obere Schranke für die Anzahl der Nullstellen eines Polynomes zu:

Satz 1.2 (Anzahl der Nullstellen) Sei $A \in \mathbb{F}[X]$ ein Polynom mit grad$A = n$. Dann hat A höchstens n Nullstellen. ⌟

Beweis 1.2 Da jeder Linearfaktor $(X - \lambda_i)$ vom Grad 1 ist und das Produkt

$$(X - \lambda_1) \cdot \ldots \cdot (X - \lambda_m)$$

vom Grad m ist, folgt die Aussage direkt aus der vorigen Überlegung. □

Nun verbinden wir die nicht irreduziblen Polynome mit denen, die Nullstellen in $\mathbb{F}$ haben:

Satz 1.3 (Irreduzibilität)

(1) Sei $A \in \mathbb{F}[X]$ ein Polynom mit grad $A \geq 2$. Besitzt A in $\mathbb{F}$ eine Nullstelle, dann ist A nicht irreduzibel in $\mathbb{F}[X]$.

(2) Sei $A \in \mathbb{F}[X]$ ein Polynom mit grad $A \in \{2, 3\}$. Besitzt A keine Nullstelle in $\mathbb{F}$, so ist A irreduzibel.

⌟

Beweis 1.3

(1) Nach Satz 1.1 ist $A = (X - \lambda) \cdot F$ für ein $F \in \mathbb{F}[X]$.

(2) Durch Widerspruch:
Nehmen wir an, A sei nicht irreduzibel. Dann ex. aber $F, G \in \mathbb{F}[X]$ mit $A = F \cdot G$; insbesondere ist F echter Teiler von A. Dann muss aber F oder G eine Nullstelle haben, da grad $F = 1$ oder grad $G = 1$.

□

Am Ende der Einführung betrachten wir noch folgendes Beispiel:

Beispiel 1.1 (Irreduzibilität) Sei $A = X^2 + 1 \in \mathbb{F}[X]$ ein Polynom. Dann ist A genau dann irreduzibel, wenn wir A nicht als Produkt der Linearpolynome $A = (X - \lambda) \cdot (X + \lambda)$ mit $\lambda^2 = -1$ schreiben können. Beachte, dass dafür insbesondere ein $\lambda \in \mathbb{F}$ existieren muss, mit $\lambda^2 = -1$.

$\mathbb{F}$	$\lambda \in \mathbb{F}$	A irreduzibel
$\mathbb{Z}_2$	Ja, $1^2 = 1 = -1$	Nein
$\mathbb{Z}_3$	Nein	Ja
$\mathbb{Z}_5$	Ja, $2^2 = 4 = -1$	Nein
$\mathbb{R}$	Nein	Ja
$\mathbb{C}$	Ja, $i \in \mathbb{C}$	Nein

⌟

1.1 Vielfachheit und Ableitung

Man sagt, dass $A \in \mathbb{F}[X]$, grad $A = n$ in Linearfaktoren zerfällt, falls wir A schreiben können als

$$A = (X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n) \tag{1}$$

mit $\lambda_i \in \mathbb{F}$. Wenn man genau hinschaut, ist dies genau die Primfaktorzerlegung von A in $\mathbb{F}[X]$. Diese Darstellung existiert allerdings im Allgemeinem nicht für jedes Polynom. Eine Ausnahme bildet z.B. der Körper $\mathbb{C}$; hier sind die irreduziblen Polynome genau die Polynome mit Grad 1, also zerfällt jedes Polynom in $\mathbb{C}$ in Linearfaktoren (s. *Fundamentalsatz der Algebra*).

Im allgemeinen Fall ist es aber viel aufwändiger zu entscheiden, ob ein gegebenes Polynom irreduzibel ist – oft muss man "brutal" mögliche Zerlegungen durchprobieren. Ein Beispiel ist hier die Entscheidungsprozedur, ob eine natürliche Zahl n Primzahl ist. Für endliche Körper gibt es allerdings effizientere Algorithmen [LN94].
Nun untersuchen wir die Vielfachheit von Nullstellen: Sei $A = (X - \lambda) \cdot F$. Ist $F(\lambda) \neq 0$, so ist λ einfache Nullstelle von A. Ist andernfalls $F(\lambda) = 0$, so heißt λ mehrfache Nullstelle.

Beachte, dass $F(\lambda) \neq 0$ auch heißt, dass $(X-\lambda)^2 \nmid A$ da ansonsten $A = (X-\lambda)\cdot(X-\lambda)\cdot F' = (X - \lambda)^2 \cdot F'$ wäre.
Die Vielfacheit einer Nullstelle kann anhand der Ableitung des Polynoms untersucht werden:
Im Folgenden sei für einen Körper $\mathbb{F}$ die Zahl $\widetilde{i}$ definiert durch $\widetilde{i} := \underbrace{1 + \ldots + 1}_{i \text{ mal}}$ (wobei $1 \in \mathbb{F}$).

Definition 1.1 (Derivation) Sei $A = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}[X]$ ein Polynom. Dann heißt die lineare Funktion

$$\delta \ : \ \mathbb{F}[X] \to \mathbb{F}[X]$$

gegeben durch

$$\delta(X^i) = \begin{cases} 0 & \text{, für } i = 0 \\ \widetilde{i} \ X^{i-1} & \text{, sonst} \end{cases}$$

Derivation. Anstatt $\delta(A)$ schreibt man häufiger A' und nennt dies die *Ableiting* von A. ⌟

Beachte, dass die Funktion δ wegen ihrer Linearität durch die obige Definition auf allen Polynomen (und nicht nur auf der Monombasis) erklärt ist. Damit gilt nämlich für $A = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}[X]$:

$$A' = \delta(A) = \sum_{i=0}^{n} a_i \delta(X^i) = \sum_{i=0}^{n} a_i \ \widetilde{i} \ X^{i-1} \tag{2}$$

Satz 1.4 (Produktregel) Für $A, B \in \mathbb{F}[X]$ gilt $(A \cdot B)' = A' \cdot B + A \cdot B'$. ⌟

Beweis 1.4 Siehe [Kur08], Seite 72. □

Nun können wir unser Vielfachheitskriterium beweisen:

Satz 1.5 (Vielfachheitskriterium) Sei $A \in \mathbb{F}[X]$ ein Polynom, $A \neq 0$, und $A(\lambda) = 0$. Dann ist λ genau dann eine einfache Nullstelle, wenn $A'(\lambda) \neq 0$. ⌟

Beweis 1.5 Wegen 1.1 gilt $A = F \cdot (X - \lambda)$ für ein $F \in \mathbb{F}[X]$.
Dann gilt

$$(X - \lambda)^2 | A \Leftrightarrow (X - \lambda) | F \Leftrightarrow F(\lambda) = 0$$

Nach der Produktregel ist $A' = F' \cdot (X - \lambda) + F \cdot (X - \lambda)'$ und damit

$$A'(\lambda) = F(\lambda)$$

□

1.2 Hornerschema

Möchte man nun alle Nullstellen eines Polynoms vom Grad n finden, so bleibt im Allgemeinen keine andere Möglichkeit, als alle $\lambda \in \mathbb{F}$ durchzuprobieren. Ausnahmen bilden die bekannten Fälle $\mathbb{F} = \mathbb{R}$ und $n \in \{2, 3\}$. Um im allgemeinen Fall etwas Rechenaufwand zu sparen, kann man sich das sog. *Hornerschema* zu Nutze machen.

Definition 1.2 (Hornerschema) Sei $A = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}[X]$ ein Polynom und $\lambda \in \mathbb{F}$. Dann ist das zugehörige **Hornerschema** die Berechnungsfolge

$$h_0 := a_n, \qquad h_i := \lambda h_{i-1} + a_{n-i}, \quad \text{für } 1 \leq i \leq n$$

⌟

Die Idee ist es, für gegebenes λ den Wert von h_n auszurechnen und dann zu prüfen ob $h_n = 0$ gilt, also ob eine Nullstellen bei λ vorliegt. Dass uns das Hornerschema dabei tatsächlich etwas nützt, sichert der folgende Satz.

Satz 1.6 (Auswertung) Sei $A \in \mathbb{F}[X]$ ein Polynom mit grad $A = n$, $\lambda \in \mathbb{F}$ und $(h_i)_{0 \leq i \leq n}$ das Hornerschema zu A. Dann gilt $A(\lambda) = h_n$ ⌟

Beweis 1.6 durch Induktion □

Erstaunlich hierbei ist, dass mit dieser Methode nur n Additionen und n Multiplikationen ausgeführt werden müssen (zum Vergleich: Die naive Methode benötigt $O(n^2)$ Multiplikationen). Sie ist für Polynomauswertung sogar optimal, jede andere Auswerungsmethode benötigt mindestens so viele Additions- und Multiplikationsoperationen wie das Hormerschema (Pan, Ostrowski). Für weitere Informationen siehe z.B. [BE95].

2 Erweiterungskörper

Hier betrachten wir allgemeine Erweiterungskörper $\mathbb{E} \supset \mathbb{F}$ um Vorarbeit für die Untersuchung der allgemeinen Struktur von endlichen Körpern zu leisten. Dabei soll $\mathbb{E}_\mathbb{F}$ nun sets endlichdimensional sein und $n := \dim \mathbb{E}_\mathbb{F} \in \mathbb{N}$.

Für $v \in \mathbb{E}$, setze $\mathbb{F}(v) := \{A(v) \mid A \in \mathbb{F}[X]\} \subset \mathbb{E} \subset \mathbb{E}_\mathbb{F}$. Es ist $\mathbb{F}(v)$ Ring und $\mathbb{F} \subset \mathbb{F}(v)$.
Wir wollen schließlich zeigen, dass $\mathbb{F}(v)$ Körper ist (also Teilkörper von $\mathbb{E}$).

Setze $\mathcal{N}_v := \{A \in \mathbb{F}[X] \mid A(v) = 0\} \subset \mathbb{F}[X]$ die Menge aller Polynome mit Nullstelle $v \in \mathbb{E}$. Um zu sehen, dass dies eine sinnvolle Definition ist, muss man sich klar machen, dass $\mathcal{N}_v \setminus \{0\} \neq \emptyset$; also dass es von 0 verschiedene Polynome in $\mathcal{N}_v$ gibt. Dies ergibt sich durch Betrachtung von $\mathbb{E}_\mathbb{F}$ zur Basis $1, v, \ldots, v^n$. Hier können wir 0 darstellen, als $0 = a_0 + a_1 v + \ldots + a_n v^n$ wobei nicht alle a_i gleich Null sind. Dann gilt für $A = a_0 + a_1 X + \ldots + a_n X^n$ allerdings $A(v) = 0$, aber $A \not\equiv 0$.

Satz 2.1 (Minimalpolynom) Sei $M \in \mathcal{N}_v, M \neq 0$, von minimalem Grad, normiert. Dann ist

(1) $\mathcal{N}_v = \{F \cdot M \mid F \in \mathbb{F}[X]\}$

(2) M eindeutig bestimmt

⌟

Beweis 2.1

(1) Da $(FM)(v) = F(v)M(v)$ und $M \in \mathcal{N}_v$, gilt $(FM)(v) = 0$. Also sind alle Vielfachen von M in $\mathcal{N}_v$. Nun zeigen wir noch, dass $M|A$, für $A \in \mathcal{N}_v, A \neq 0$. Für $A = F \cdot M + R$ gilt $A(v) = F(v) \cdot M(v) + R(v) = 0$, also $R(v) = 0$. Damit ist $R \in \mathcal{N}_v$. Da aber M minimal, folgt $R \equiv 0$.

(2) Gäbe es zwei Minimalpolynome, wären sie jeweils gegenseitige Teiler. Damit sind die skalare Vielfache voneinander, was der Normiertheit widerspricht.

□

Wählen wir ein $M \in \mathbb{F}[X], M \neq 0$, normiert, mit $M(v) = 0$. Dann ist M das Minimalpolynom, also $M_v = M$, genau dann wenn M irreduzibel ist (ohne Beweis, siehe [Kur08]).

Für den Nachweis, dass $\mathbb{F}(v)$ Körper ist, konstruieren wir uns einen Isomorphismus und definieren dafür zunächst eine Restabbildung: Sei $v \in \mathbb{E}, M := M_v, m := \text{grad } M$. Die zu M gehörige Restabbildung sei dann $\varrho_M : \mathbb{F}[X] \to \mathbb{F}_m[X]$.

Lemma 2.1 Sei $A_0 := \varrho_M(A)$, für $A \in \mathbb{F}[X]$.

(1) $A(v) = A_0(v)$, also $\mathbb{F}(v) = \{A(v) \mid A \in \mathbb{F}_m[X]\}$

(2) $\{1, v, v^2, \ldots, v^{m-1}\}$ ist eine Basis von $\mathbb{F}(v)$

⌟

Beweis:
Siehe [Kur08], Seite 128. □.

Da $M = M_v$, ist M irreduzibel, also kann $\mathbb{F}_M$ als Körper mit der Multiplikation $A \cdot_M b = \varrho_M(A \cdot B)$ erklärt werden. Die restlichen Gesetze erbt es aus der Darstellung als Vektorraum $\mathbb{F}_M = \mathbb{F}_m[X]$.

Also können wir nun einen Isomorphismus entwickeln:

Die Funktion $\eta : \mathbb{F}_M \to \mathbb{F}(v)$, gegeben durch

$$a_0 + a_1 X + \ldots + a_{m-1} X^{m-1} \mapsto a_0 + a_1 v + \ldots + a_{m-1} v^{m-1}$$

und ist nach Lemma ein Vektorraumisomorphismus. Auch nach Lemma gilt weiterhin $A(v)B(v) = (AB)_0(v) = \varrho_M(AB)(v)$, also $\eta(A)\eta(B) = \eta(A \cdot_M B)$. Also ist η auch Körperisomorphismus und $\mathbb{F}_M$ kann mit $\mathbb{F}(v)$ identifiziert werden. Insbesondere ist dann $\mathbb{F}(v)$ auch Körper.
Diese Erkenntnis wird bei der Untersuchung der allgemeinen Struktur von endlichen Körpern wieder aufgegriffen. Dazu gehört auch die Konstruktion eines Erweiterungskörpers $\mathbb{E} \supset \mathbb{F}$, in dem ein Polynom $A \in \mathbb{F}[X]$ in Linearfaktoren zerfällt. Die Existenz wird gesichert durch folgenden Satz:

Satz 2.2 (Endliche Erweiterung) Sei $A \in \mathbb{F}[X]$, grad $A \geq 1$. Dann existiert eine endliche Erweiterung $\mathbb{E} \supset \mathbb{F}$, s.d. A in $\mathbb{E}[X]$ in Linearfaktoren zerfällt. ⌟

Beweis 2.2 Siehe [Kur08], Seite 131. □

Den kleisten dieser Erweiterungen nennt man *Zerfallungskörper*. Zerfallungskörper bilden ebenfalls einen zentralen Begriff in spätere Themen.

Körpererweiterungen können wir ebenfalls ausnutzen um Rechenoperationen besser zu organisieren. Um die bereits bekannte Technik der Strukturmatrix zu vereinfachen, führend wir einen Zwischenkörper $\mathbb{D}$ ein, der eine endliche Erweiterung von $\mathbb{F}$ ist. Es gilt also $\mathbb{F} \subset \mathbb{D} \subset \mathbb{E}$. Am Prinzip ändert sich nichts – einzig Nutzen wir dabei aus, dass wir statt einer großen Strukturmatrix, zwei kleinere Strukturmatrizen aufstellen müssen.

Literatur

[BE95] P. Borwein and T. Erdelyi. *Polynomials and Polynomial Inequalities*. Graduate Texts in Mathematics. Springer New York, 1995.

[Kur08] Hans Kurzweil. *Endliche Körper*. Springer-Lehrbuch. Springer London, Limited, 2008.

[LN94] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1994.