Der Fundamentalsatz der Algebra

Vortrag im Rahmen des Proseminars zur Analysis, 24. April 2006

Micha Bittner

§ 1 Motivation

Den ersten Beweis des Fundamentalsatzes der Algebra erbrachte C.F. Gauss im Jahr 1799 im Rahmen seiner Dissertation. Heute sind mehrere Beweise des Fundamentalsatzes der Algebra aus unterschiedlichen Bereichen der Mathematik (Analysis, Algebra und Topologie) bekannt. Trotz seines Namens kann der Fundamentalsatz der Algebra jedoch nicht mit rein algebraischen Methoden bewiesen werden.

Hier werden zwei Beweise des Fundamentalsatzes der Algebra präsentiert. Dabei wird zunächst ein eleganter Beweis mit Methoden der Funktionentheorie vorgestellt und im Anschluss gezeigt, dass sogar mit den Methoden der Analysis I ein Beweis des Fundamentalsatzes vollzogen werden kann.

§ 2 Beweis des Fundamentalsatzes der Algebra

(2.1) Satz.
Zu jedem *nicht-konstanten* Polynom

$$p(Z) = a_0 + a_1 Z + \cdots + a_n Z^n \in \mathbb{C}[Z]$$

existiert ein $c \in \mathbb{C}$ mit $p(c) = 0$.

— *Beweis mit Mitteln der Funktionentheorie* —

1. Beweis von (2.1)
Sei $a_n \neq 0$. Nach der 2. Dreiecksungleichung gilt für $z \in \mathbb{C}^*$,

$$\begin{aligned} |p(z)| &= |a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0| \\ &\geq |a_n z^n| - |a_{n-1} z^{n-1}| - \cdots - |a_0| \\ &= |a_n||z|^n \cdot \left[1 - \frac{|a_{n-1}|}{|a_n|} \cdot \frac{1}{|z|} - \cdots - \frac{|a_0|}{|a_n|} \cdot \frac{1}{|z|^n}\right]. \end{aligned}$$

Wegen

$$\lim_{|z|\to\infty}\left[1-\frac{|a_{n-1}|}{|a_n|}\cdot\frac{1}{|z|}-\cdots-\frac{|a_0|}{|a_n|}\cdot\frac{1}{|z|^n}\right]=1$$

existiert ein $R>0$ mit

$$\underbrace{|p(z)|\geq\frac{1}{2}|a_n||z|^n}_{\text{Wachstumsaussage für Polynome}}\quad\text{für alle}\quad|z|\geq R.$$

Daraus folgt

$$\frac{1}{|p(z)|}\leq\frac{2}{|a_n|\cdot|z|^n}\leq\frac{2}{|a_n|\cdot R^n}\quad\text{für alle }|z|\geq R.\quad(*)$$

Annahme: Sei $p(z)\neq 0$ für alle $z\in\mathbb{C}$.

Dann ist $f:\mathbb{C}\to\mathbb{C},\ z\longmapsto\frac{1}{p(z)}$, als rationale Funktion auf ihrem Definitionsbereich $\mathbb{C}$ stetig. Auf dem Kompaktum $K:=\{z\in\mathbb{C};|z|\leq R\}$ ist $f(K)$ kompakt und folglich auch beschränkt. Zusammen mit $(*)$ können wir also die Beschränktheit von f auf $\mathbb{C}$ folgern. Als ganze Funktion[1] ist f und damit auch $p(z)$ nach dem Satz von LIOUVILLE[2] konstant. Das ist ein Widerspruch zur Voraussetzung. Also existiert eine Nullstelle.

— *Beweis mit Methoden der reellen Analysis* —

(2.2) Lemma.
Zu jedem $n\in\mathbb{N}$ und $a\in\mathbb{C}$ existiert ein $c\in\mathbb{C}$ mit $c^n=a$.

Beweis
Wir verwenden vollständige Induktion nach n.
(IA) n = 1: $c=a$ ist trivial.
n = 2: Dazu wähle $a=u+iv$, $c:=\sqrt{\frac{1}{2}(|a|+u)}+i\varepsilon\sqrt{\frac{1}{2}(|a|-u)}$,
wobei $\varepsilon\in\{\pm1\}$ so gewählt ist, dass $v=\varepsilon|v|$.
Dann gilt:

[1] vgl. Krieg, A.: Analysis IV
[2] vgl. Krieg, A.: Analysis IV, S. 470, Kap. XVIII., (4.8);
Aussage: Jede beschränkte, ganze Funktion ist konstant

$$
\begin{aligned}
c^2 &= \frac{1}{2}(|a| + u) - \underbrace{\varepsilon^2}_{=1}\frac{1}{2}(|a| - u) + 2i\varepsilon\sqrt{\frac{1}{4}(|a|^2 - u^2)} \\
&= \frac{1}{2}(|a| + u) - \frac{1}{2}(|a| - u) + 2i\varepsilon\sqrt{\frac{1}{4}(u^2 + v^2 - u^2)} \\
&= u + i\varepsilon\sqrt{v^2} = u + i\varepsilon|v| = u + iv = a.
\end{aligned}
$$

(IV) Sei also $n \geq 2$. Es gelte $b^m = a$ für ein $b \in \mathbb{C}$, $m \in \mathbb{N}$.

(IS) 1. Fall: Sei n ungerade. Für $a = 0$, wähle $c = 0$. Sei also weiterhin $a \neq 0$. Wähle Œ $|a| = 1$, da sonst $c^n = \frac{a}{|a|}$ auch $(\sqrt[n]{|a|}c)^n = a$ impliziert. Die Behauptung ist für $a \in \mathbb{R}_+$ klar und wegen $(-c)^n = -c^n$ für $a < 0$ ebenso[3]. Sei weiterhin also $a \notin \mathbb{R}$. Wir wählen nach (IA) ein $d \in \mathbb{C}$ mit $d^2 = a$, also $d\overline{d} = |d|^2 = |a| = 1$ und betrachen das Polynom

$$p(X) = i\left[\overline{d}(X + i)^n - d(X - i)^n\right] = i(\overline{d} - d)X^n + \ldots \quad .$$

Es gilt $\overline{p(x)} = p(x)$ für alle $x \in \mathbb{R}$, da

$$\overline{p(x)} = -i\left[d(X - i)^n - \overline{d}(X + i)^n\right] = p(X).$$

$p(X)$ ist also ein reelles Polynom, das wegen $d \notin \mathbb{R}$, d.h. $\overline{d} - d \neq 0$, den ungeraden Grad n hat. Da n ungerade ist folgt mit dem Zwischenwertsatz[4], dass p als reelles Polynom ungeraden Gerades eine Nullstelle $\lambda \in \mathbb{R}$ hat.

$$\overline{d}(\lambda + i)^n = d(\lambda - i)^n, \text{ also } \quad \left(\frac{\lambda + i}{\lambda - i}\right)^n \underbrace{|d|^2}_{=1} = \frac{d^2\overline{d}}{\overline{d}} = d^2 = a.$$

2. Fall: Sei $n = 2m$, n gerade. Wähle $b \in \mathbb{C}$ mit $b^m = a$ nach (IV) und nach Induktionsanfang $c \in \mathbb{C}$ mit $b = c^2$. Daraus folgt $c^n = c^{2m} = b^m = a$.

[3] vgl. Krieg, A: Analysis I, S. 27, Kap.I., (3.26)
[4] vgl. Krieg, A.: Analysis I, S. 104, Kap. V., (3.10)

Alternativer Beweis: Sei $a \in \mathbb{C}$, $a \neq 0$. Nach dem Satz von der Polarkoordinatendarstellung[5] besitzt a eine Darstellung der Form:

$$a = |a| \cdot e^{i\varphi}.$$

Definiere

$$c := \sqrt[n]{|a|} \cdot e^{i\frac{\varphi}{n}} \in \mathbb{C}.$$

Dann gilt:

$$c^n = \left(\sqrt[n]{|a|} \cdot e^{i\frac{\varphi}{n}} \right)^n = |a| \cdot e^{i\varphi} = a.$$

□

Mit diesem Lemma folgt unmittelbar das

(2.3) Korollar.
Jedes *nicht-konstante* Polynom der Form $q(Z) = Z^n - a \in \mathbb{C}[Z]$ hat stets eine Nullstelle in $\mathbb{C}$.

Der nächste Beweisschritt ist enthalten in dem

(2.4) Lemma.
Zu jedem *nicht-konstanten* Polynom

$$p(Z) = a_0 + a_1 Z + \cdots + a_n Z^n \in \mathbb{C}[Z]$$

existiert ein $c \in \mathbb{C}$ mit

$$|p(c)| \leq |p(z)| \text{ für alle } z \in \mathbb{C}.$$

Beweis
Sei $a_n \neq 0$. Wie im ersten Beweis von (2.1) schließt man $|p(z)| \geq \frac{1}{2}|a_n|R^n$ für $|z| \geq R$. Die Funktion $z \longmapsto |p(z)|$ ist stetig und nimmt deshalb nach dem Satz vom Minimum und Maximum ihr Minimum auf dem Kompaktum $K := \{z \in \mathbb{C};\ |z| \leq R\}$ in c an. Es gilt also $|p(c)| \leq |p(z)|$ für alle $z \in K$. Da $0 \in K$ ist, gilt $|p(c)| \leq |p(0)|$. Wir erhalten unser c also, wenn wir $R \geq \sqrt[n]{2\frac{|p(0)|}{|a_n|}}$ wählen. Dann gilt nämlich

$$|p(z)| \geq \frac{1}{2}|a_n|R^n \geq |p(0)| \geq |p(c)| \text{ für alle } |z| \geq R.$$

Daraus folgt also insgesamt

$$|p(c)| \leq |p(z)| \text{ für alle } z \in \mathbb{C}.$$

□

[5] Krieg, A.: Analysis I, Kap. V., (5.11)

Von technischer Bedeutung ist das

(2.5) Lemma.
Sei $k \in \mathbb{N},\ b \in \mathbb{C},\ b \neq 0,\ g(Z) \in \mathbb{C}[Z]$ mit $g(0) = 0$ und

$$h(Z) = 1 + bZ^k + Z^k g(Z) \in \mathbb{C}[Z].$$

Dann existiert ein $u \in \mathbb{C}$ mit $|h(u)| < 1$.

Beweis
Wähle nach (2.2) ein $d \in \mathbb{C}$ mit $d^k = -\frac{1}{b}$. Dann folgt $bd^k = -1$. Damit gilt für alle $t \in \mathbb{R}$ mit $0 < t \leq 1$ und mit der Dreiecksungleichung

$$|h(td)| = |1 + b(td)^k + (td)^k g(td)| \leq |1 + b(td)^k| + |(td)^k g(td)| \underbrace{=}_{bd^k = -1} 1 - t^k + t^k |d^k g(td)|.$$

Da g als Polynom stetig in 0 mit $g(0) = 0$ ist, folgt mit der Definition der Stetigkeit[6] und $0 < t \leq 1$, also $0 < t^k \leq 1$, die Existenz eines $0 < \delta < 1$ mit

$$|d^k g(td) - 0| < \frac{1}{2},\ \text{für}\ 0 < t < \delta,$$

also

$$|h(td)| < 1 - \frac{1}{2}t^k < 1,\ \text{für}\ 0 < t < \delta.$$

□

2. Beweis von (2.1)
Wähle nach (2.4) $c \in \mathbb{C}$ mit $|p(c)| \leq |p(z)|$ für alle $z \in \mathbb{C}$ und nehme $p(c) \neq 0$ an. Mit $p(Z)$ ist auch

$$\begin{aligned} h(Z) := \frac{p(c+Z)}{p(c)} &= \frac{a_0 + a_1(c+Z) + \cdots + a_n(c+Z)^n}{a_0 + a_1 c + \cdots + a_n c^n} \\ &= 1 + b_k Z^k + \cdots + b_n Z^n,\ \ b_k \neq 0,\ \ 1 \leq k \leq n, \end{aligned}$$

nicht konstant. Mit (2.5) erhält man ein $u \in \mathbb{C}$ mit $|h(u)| < 1$, was $|p(c+u)| < |p(c)|$ impliziert. Dies ist ein Widerspruch zur Bedingung $|p(c)| < |p(z)|$ für alle $|z| \in \mathbb{C}$. Es folgt also $p(c) = 0$.

[6] vgl. Krieg, A.: Analysis I, S. 88, Kap. V, (1.1)

§ 3 Anwendungen

Nun wollen wir Polynome zerlegen.

(3.1) Lemma.
Sei $p(Z) \in \mathbb{C}[Z]$ vom Grad n und $c \in \mathbb{C}$ mit $p(c) = 0$. Dann existiert genau ein Polynom $q(Z) \in \mathbb{C}[Z]$ vom Grad $n-1$ mit

$$p(Z) = (Z - c) \cdot q(Z).$$

Beweis
Sei $p(Z) = a_0 + a_1 Z + \cdots + a_n Z^n,\ a_n \neq 0$. Nach der geometrischen Summenformel[7] gilt für $z \neq c$

$$\frac{Z^r - c^r}{Z - c} = \sum_{k=0}^{r-1} Z^k c^{(r-1)-k}$$

$$\Rightarrow Z^r - c^r = (Z - c) \cdot q_r(Z), \quad q_r(Z) = \sum_{k=0}^{r-1} Z^k c^{(r-1)-k} \quad \text{für alle } z \in \mathbb{C}. \tag{1}$$

Da $p(c) = 0$ ist, gilt

$$p(Z) = p(Z) - p(c) = \sum_{r=0}^{n} a_r Z^r - \sum_{r=0}^{n} a_r c^r = \sum_{r=0}^{n} a_r (Z^r - c^r) = \sum_{r=1}^{n} a_r (Z^r - c^r)$$

$$\underbrace{=}_{\text{mit (1)}} (Z - c) \cdot q(Z) \ \text{ mit } \ q(Z) = \sum_{r=1}^{n} a_r q_r(Z).$$

Aufgrund von $a_n \neq 0$ hat $q(Z)$ den Grad $n-1$ (vgl. q_r). Wegen $q(Z) = \frac{p(z)}{z-c}$ für alle $z \in \mathbb{C}, z \neq c$ ist $q(z)$ durch $p(z)$ und c eindeutig bestimmt. □

Durch Induktion erhalten wir das folgende

(3.2) Korollar.
a) Jedes Polynom $p(Z) \in \mathbb{C}[Z]$ vom Grad $n \in \mathbb{N}$ besitzt eine Darstellung

$$p(Z) = \alpha(Z - a_1) \cdot \ldots \cdot (Z - a_n), \quad 0 \neq \alpha \in \mathbb{C}, \quad a_1, \ldots, a_n \in \mathbb{C}.$$

Dabei sind α und bis auf die Reihenfolge auch $a_1, \ldots, a_n$ eindeutig bestimmt.

b) Die irreduziblen Polynome über $\mathbb{C}$ sind genau diejenigen vom Grad 1, d.h $\mathbb{C}$ ist algebraisch abgeschlossen.

[7] vgl. Krieg, A.: Analysis I, S. 11, Kap I., (2.8)

Eine reelle Version des Fundamentalsatzes der Algebra beeinhaltet das

(3.3) Korollar.
a) Jedes Polynom $p(X) \in \mathbb{R}[X]$ vom Grad $n \in \mathbb{N}$ besitzt eine Darstellung

$$p(X) = \alpha(X - a_1) \cdot \ldots \cdot (X - a_r) \cdot q_1(X) \cdot \ldots \cdot q_s(X), \quad 0 \neq \alpha \in \mathbb{R}, \quad a_1, \ldots, a_r \in \mathbb{R}$$

$$\text{mit } q_j(X) = X^2 + b_j X + c_j, \ b_j, c_j \in \mathbb{R}, \ b_j^2 - 4c_j < 0, \ 1 \leq j \leq s, \ r + 2s = n.$$

Dabei sind α und bis auf die Reihenfolge auch $a_1, \ldots, a_r$ und $q_1(X), \ldots, q_s(X)$ eindeutig bestimmt.

b) Die irreduziblen Polynome über $\mathbb{R}$ sind genau diejenigen vom Grad 1, sowie diejenigen vom Grad 2 ohne reelle Nullstellen.

Beweis
Seien $a_1, \ldots, a_r$ alle reelle Nullstellen von p. Wir fassen p als komplexes Polynom auf, dann hat p nach (3.2) eine Darstellung der Form

$$p(Z) = \alpha(Z - a_1) \cdot \ldots \cdot (Z - a_r) \cdot q(Z),$$

wobei $\deg q = n - r$ ist und die Nullstellen von q komplex sind. Da die Koeffizienten von q reell sind, gilt $\overline{q(z)} = q(\overline{z})$ für alle $z \in \mathbb{C}$. Für $z \in \mathbb{C}$, $z \notin \mathbb{R}$ gilt dann: Ist $z = u + iv$, eine Nullstelle von q, dann gilt $0 = \overline{p(z)} = p(\overline{z})$, also ist $\overline{z}$ eine von z verschiedene Nullstelle. Da $v \neq 0$ hat man

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} = X^2 - 2uX + (u^2 + v^2) \in \mathbb{R}[X],$$
$$(2u)^2 - 4(u^2 + v^2) = -4v^2 < 0.$$

Umgekehrt hat ein Polynom $X^2 + bX + c \in \mathbb{R}[X]$ mit $b^2 - 4c < 0$ auch keine reelle Nullstelle, sondern zwei konjugiert komplexe Lösungen. Damit führt jede Darstellung in (3.3) auf eine in (3.2), so dass auch die Eindeutigkeit folgt[8]. □

(3.4) Beispiele.
a) Sei $p(X) = X^4 + 1 \in \mathbb{R}[X]$. Um p in irreduzible Polynome über $\mathbb{R}$ zu zerlegen bestimmen wir zunächst die Nullstellen über $\mathbb{C}$. Es gilt

$$X^4 + 1 = 0 \quad \Leftrightarrow \quad X^4 = -1 \quad \Rightarrow \quad X^8 = 1.$$

[8] vgl. Hiß, G.: Vorl. Lineare Algebra I, Kap. V, (5.32)

Diese Gleichung hat nach Analysis I, Kapitel V, (5.12) genau die 8 Lösungen

$$z = \exp\left(\frac{2\pi i k}{8}\right), \quad k = 0, 1, \ldots, 7$$

$$z_0 = e^0,\ z_1 = e^{\frac{\pi i}{4}},\ z_2 = e^{\frac{2\pi i}{4}},\ z_3 = e^{\frac{3\pi i}{4}},\quad \ldots,\ z_7 = e^{\frac{7\pi i}{4}}.$$

Uns interessieren jedoch nur die Lösungen mit $(z_j)^4 = -1$, für $0 \leq j \leq 7$.
Damit finden wir z_1, z_3, z_5 und z_7 als Lösungen. Um herauszufinden, welche der Lösungen die komplex konjugierten zueinander sind, greifen wir auf die Polarkoordinatendarstellung von komplexen Zahlen zurück. Es gilt

$$e^{iz} = \cos(z) + i\sin(z) \quad \text{für alle } z \in \mathbb{C}.$$

Wir erhalten

$$z_1 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ z_3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ z_5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},\ z_7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}.$$

z_1 und z_7, sowie z_3 und z_5 sind also jeweils die komplex konjugierten zueinander.
Mit den Ergebnissen aus dem Beweis von (3.3) erhält man die irreduziblen Polynome

$$(X - z_1) \cdot (X - z_7) = X^2 - \sqrt{2}X + 1$$
$$(X - z_3) \cdot (X - z_5) = X^2 + \sqrt{2}X + 1$$

und es gilt

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

b) Damit haben wir dann auch die Zerlegung des Polynoms $p(X) = X^4 + 1 \in \mathbb{C}[X]$ durch

$$X^4 + 1 = \left(X - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\left(X + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\left(X + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\left(X - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right).$$

(3.5) Korollar.
Sei $p(X)$ ein reelles Polynom ungeraden Grades. Dann hat p eine Nullstelle in $\mathbb{R}$.

Beweis
Annahme: $p(X) \in \mathbb{R}[X]$ hat nur Nullstellen $z \in \mathbb{C} \setminus \mathbb{R}$

Wegen $0 = \overline{p(z)} = p(\overline{z})$ ist auch $\overline{z} \in \mathbb{C} \setminus \mathbb{R}$ eine Nullstelle. Dann gilt, dass $p(X)$ in quadratische Polynome zerfällt, also geraden Grad hat. Dies ist ein Widerspruch zur Voraussetung. Also hat p eine Nullstelle in $\mathbb{R}$[9]. □

[9] vgl. Krieg, A.: Analysis I, S. 104, Kap V., (3.10)

(3.6) Korollar.
Sei $p(X) \in \mathbb{R}[X]$ normiert vom Grad 4. Dann existiert ein $\alpha \in \mathbb{R}$ und ein Polynom $q(X) = X^4 + aX^2 + bX + c \in \mathbb{R}[X]$ mit $p(X) = q(X + \alpha)$.

Beweis
p ist ein Polynom der Form $p(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$. Wähle $\alpha = \frac{a_3}{4}$, $a = a_2 - \frac{3}{8} \cdot a_3^2$, $b = a_1 + \frac{a_3^3}{8} - \frac{a_2a_3}{2}$, $c = a_0 + \frac{5}{256} \cdot a_4^4 + \frac{a_2a_3^2}{16} - \frac{a_1a_3}{4} - \frac{a_3^2}{128}$,
dann gilt:

$$\begin{aligned} q(X+\alpha) &= X^4 + 4\alpha X^3 + (6\alpha^2 + a)X^2 + (4\alpha^3 + 2a\alpha + b)X + (\alpha^4 + a\alpha^2 + b\alpha + c) \\ &= X^4 + a_3X^3 + (\frac{3}{8} \cdot a_3^2 + a_2 - \frac{3}{8} \cdot a_3^2)X^2 + (\frac{a_2a_3^2}{2} - \frac{3}{8} \cdot a_3^3 + \frac{3}{8} \cdot a_3^2 - \frac{a_2a_3^2}{2} + a_1)X \\ &\quad \frac{a_1a_3}{4} + \frac{a_3^2}{128} - \frac{a_2a_3^2}{16} - \frac{5}{256} \cdot a_4^4 - \frac{a_1a_3}{4} - \frac{a_3^2}{128} + \frac{a_2a_3^2}{16} + \frac{5}{256} \cdot a_4^4 + a_0 \\ &= p(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = p(X). \end{aligned}$$

□