Der Fundamentalsatz der Algebra

Vortrag zum Proseminar zur Analysis, 06.10.2010

Stefan Bleß

Inhaltsverzeichnis

1 Vorwort **2**

2 Der Beweis **3**
2.1 n-te Wurzel auf $\mathbb{C}$ 3
2.2 Minimum des Betrages eines Polynoms 6
2.3 Spezielle Eigenschaften 8
2.4 Der Beweis 9

3 Eigenschaften **11**
3.1 Linearfaktoren 11
3.2 Der Fundamentalsatz der Algebra auf $\mathbb{R}$ 14
3.3 Irreduzible Polynome 16

4 Literaturverzeichnis **19**

§ 1 Vorwort

Der Fundamentalsatz der Algebra besagt, dass der Körper $\mathbb{C}$ algebraisch abgeschlossen ist:

(1.1) Satz (Fundamentalsatz der Algebra).
Zu jedem nicht-konstanten Polynom

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

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

In diesem Vortrag werde ich mich mit dem Fundamentalsatz der Algebra beschäftigen. Dazu führe ich neben dem Beweis auch noch nützliche Eigenschaften dieses Satzes auf. Neben dem Zerfall eines Polynoms in Linearfaktoren veranschaulicht der Fundamentalsatz der Algebra ebenso die irreduziblen Polynome über $\mathbb{R}$ und $\mathbb{C}$. Er wird aber auch in Beweisen immer für die Existenz von mindestens einer Nullstelle eines komplexen Polynoms angeführt.

Als Grundlage für den Beweis von (1.1) dient der 1815 von Carl Friedrich Gauß veröffentlichte Beweis, der auf Ideen von Leonhard Euler basiert. Gauß verwendete dazu, dass jedes reelle Polynom ungeraden Grades nach dem Zwischenwertsatz mindestens eine Nullstelle hat.
Genauso finden sich auch Ideen eines ersten analytischen Beweises von d'Alembert um 1746. Dieser Beweis basiert darauf, dass zu jedem Punkt $c \in \mathbb{C}$, der keine Nullstelle ist, ein Punkt $c + w \in \mathbb{C}$ existiert, der einen kleineren Betrag bezüglich des Funktionswertes des Polynoms aufweist. Dies führt dazu, dass die Minimalstelle dieser Funktionswerte eine Nullstelle sein muss.

Ich beginne meinen Vortrag mit den Beweisen einiger Hilfsaussagen, die ich für den Beweis von (1.1) benötige. Es folgt dann der eigentliche Beweis und anschließend werde ich die verschiedenen Eigenschaften des Fundamentalsatzes der Algebra betrachten.

§ 2 Der Beweis

— *n-te Wurzel auf* $\mathbb{C}$ —

Zu Beginn möchte ich mich kurz mit der n-ten Wurzel auf $\mathbb{C}$ beschäftigen, da diese einen interessanten Spezialfall eines Polynoms liefert. Dazu betrachte ich zunächst das

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

Beweis:
Für den Beweis verwende ich eine vollständige Induktion nach n:

Induktionsanfang:

$n = 1$: Mit $c := a$ trifft die Aussage für ein beliebiges $a \in \mathbb{C}$ zu.
Da ich ihn später benötige, betrachte ich ebenso den Fall

$n = 2$: Da $a \in \mathbb{C}$ ist, lässt sich a auch als

$$a := u + iv$$

darstellen, wobei u und $v \in \mathbb{R}$ sind. Ich definiere mir nun

$$\varepsilon := \begin{cases} 1 & , v \geq 0 \\ -1 & , v < 0 \end{cases}$$

Aus Analysis I (vgl. II(4.4)) ist bekannt, dass $|a| = \sqrt{u^2 + v^2}$ ist.
Somit ist $|a| \geq |u|$, da $\sqrt{u^2 + v^2} \geq \sqrt{u^2}$ für alle u und $v \in \mathbb{R}$ ist.

Daraus folgt, dass $c \in \mathbb{C}$ mit $c := \sqrt{\frac{1}{2}(|a| + u)} + i\varepsilon\sqrt{\frac{1}{2}(|a| - u)}$ stets wohldefiniert ist und es gilt mit Hilfe der binomischen Formel:

$$\begin{aligned} c^2 &= (\sqrt{\tfrac{1}{2}(|a| + u)})^2 + 2i\varepsilon\sqrt{\tfrac{1}{2}(|a| + u)}\sqrt{\tfrac{1}{2}(|a| - u)} + (i\varepsilon\sqrt{\tfrac{1}{2}(|a| - u)})^2 \\ &= \tfrac{1}{2}(|a| + u) + 2i\varepsilon\sqrt{\tfrac{1}{4}(|a|^2 - u^2)} + i^2\varepsilon^2\tfrac{1}{2}(|a| - u) \\ &\underset{\varepsilon^2=1}{=} \tfrac{1}{2}|a| + \tfrac{1}{2}u + i\varepsilon\sqrt{|a|^2 - u^2} - \tfrac{1}{2}|a| + \tfrac{1}{2}u \\ &= u + i\varepsilon\sqrt{|a|^2 - u^2}. \end{aligned}$$

Da $|a| = \sqrt{u^2 + v^2}$ äquivalent zu $|a|^2 = u^2 + v^2$ ist, ergibt sich

$$c^2 = u + i\varepsilon\sqrt{u^2 + v^2 - u^2} = u + i\varepsilon|v| \underset{\varepsilon|v|=v}{=} u + iv = a. \qquad \square$$

Induktionsvoraussetzung:
Es gelte die Behauptung für ein $n \in \mathbb{N}$.

Induktionsschritt:
Es sei nun $n > 2$.

n gerade: Ich definiere mir $m \in \mathbb{N}$ mit $m := \frac{n}{2}$. Dann existiert nach Induktionsvoraussetzung ein $b \in \mathbb{C}$ mit $b^m = a$. Wenn ich nun $c^2 := b$ wähle, so folgt $c^n = (c^2)^m = b^m = a$, da dieser Fall bereits im Induktionsanfang für $n = 2$ gezeigt wurde.

n ungerade: $a \in \mathbb{R}$: Für $a \geq 0$ und $c := \sqrt[n]{a} \in \mathbb{R}$ gilt:
$c^n = (\sqrt[n]{a})^n = a$.
Für $a < 0$, $b := -a$ und $c := -\sqrt[n]{b} \in \mathbb{R}$ gilt, da $b > 0$ ist:
$c^n = (-\sqrt[n]{b})^n = (-1)^n(\sqrt[n]{b})^n \underset{(-1)^n=-1}{=} -b = a$.

$a \notin \mathbb{R}$: Es sei nun $d^2 := a \in \mathbb{C}$. Da $a \notin \mathbb{R}$ ist, ist auch $d \notin \mathbb{R}$. Dazu muss ich folgendes mit $d := u + iv$ betrachten:

$$d^2 = (u + iv)^2 = u^2 + 2iuv + v^2 = a.$$

Da $a \notin \mathbb{R}$ ist, muss $2uv \neq 0$ sein. Somit müssen u und v ungleich 0 sein und und es folgt, dass $d \notin \mathbb{R}$ ist.

Des Weiteren ist $|d| = \sqrt{d\overline{d}}$ (vgl. II(4.4) in Analysis I) und somit $d\overline{d} = |d|^2 = |d^2| = |a|$. $(*)$

Ich betrachte nun das folgende Polynom mit Hilfe der binomischen Formel aus Analysis I (vgl. I(1.12))

$$\begin{aligned} p(X) &:= i[\overline{d}(X+i)^n - d(X-i)^n] \\ &= i[\overline{d}\sum_{k=0}^{n}(\binom{n}{k}X^k i^{n-k}) - d\sum_{k=0}^{n}(\binom{n}{k}X^k(-i)^{n-k})] \\ &= i\cdot\sum_{k=0}^{n}[\binom{n}{k}(\overline{d}i^{n-k} - d(-i)^{n-k})X^k] \\ &= i\cdot\sum_{k=0}^{n-1}[\binom{n}{k}(\overline{d}i^{n-k} - d(-i)^{n-k})X^k] + i(\overline{d}-d)X^n \end{aligned}$$

Da $d \notin \mathbb{R}$ ist, ist $d \neq \overline{d}$ und somit der Koeffizient von X^n stets ungleich 0. Da n ungerade ist, ist p ein Polynom ungeraden Grades.

p ist ein reelles Polynom, da nach Analysis I (vgl. II(4.3))

$$\begin{aligned}
\overline{p(x)} &= \overline{i \cdot \sum_{k=0}^{n} [\binom{n}{k} \cdot (\overline{d} \cdot i^{n-k} - d \cdot (-i)^{n-k}) \cdot x^k]} \\
&\underset{II(4.3)}{=} \overline{i} \cdot \sum_{k=0}^{n} [\overline{\binom{n}{k}} \cdot (\overline{\overline{d}} \cdot \overline{i^{n-k}} - \overline{d} \cdot \overline{(-i)^{n-k}}) \cdot \overline{x^k}] \\
&= (-i) \cdot \sum_{k=0}^{n} [\binom{n}{k} \cdot (d(-i)^{n-k} - \overline{d} i^{n-k}) \cdot x^k] \\
&= i \cdot \sum_{k=0}^{n} [\binom{n}{k} \cdot (\overline{d} i^{n-k} - d(-i)^{n-k}) \cdot x^k] \\
&= p(x) \text{ für alle } x \in \mathbb{R} \text{ ist.}
\end{aligned}$$

Aus Analysis I ist bekannt, dass ein reelles Polynom ungeraden Grades eine Nullstelle in $\mathbb{R}$ hat (vgl. IV(3.9)). Für p sei diese Nullstelle $\lambda \in \mathbb{R}$. Damit $p(\lambda) = 0$ sein kann, muss $\overline{d}(\lambda + i)^n - d(\lambda - i)^n = 0$ sein. Dies ist äquivalent zu $\overline{d}(\lambda + i)^n = d(\lambda - i)^n$, also nach $(*)$
$(\frac{\lambda+i}{\lambda-i})^n = \frac{d}{\overline{d}} = \frac{d^2}{d\overline{d}} = \frac{a}{|d|^2} = \frac{a}{|a|}$.
Es sei nun $z \in \mathbb{C}$ mit $z := \frac{\lambda+i}{\lambda-i}$. Da $\lambda \in \mathbb{R}$ ist, ist auch $\lambda - i \neq 0$ und z somit stets wohldefiniert. Daraus folgt $z^n = \frac{a}{|a|}$, was ebenfalls wohldefiniert ist, da $a \notin \mathbb{R}$ ist. $|a| = 0$ ist äquivalent zu $a = 0$, aber dies ist nicht möglich, da $0 \in \mathbb{R}$ ist. Es sei nun $c := \sqrt[n]{|a|}z \in \mathbb{C}$. Dann ist $z^n = \frac{a}{|a|}$ äquivalent zu $a = |a|z^n = (\sqrt[n]{|a|}z)^n = c^n$.

Es folgt die Behauptung durch eine vollständige Induktion nach n. □

Dieses Lemma ermöglicht die Betrachtung eines Spezialfalls des Fundamentalsatzes der Algebra. Es besagt, dass jedes Polynom der Form $X^n - a$ eine Nullstelle besitzt. Im Folgenden möchte ich mich wieder mit allgemeineren Fällen beschäftigen.

— *Minimum des Betrages eines Polynoms* —

Jedes Polynom nimmt betragsmäßig ein Minimum an. Für die konstanten Polynome ist dies klar, da dann alle Funktionswerte des Polynoms dieses Mininum annehmen. Deswegen muss ich diese Aussage nur noch für alle nicht-konstanten Polynome zeigen und betrachte dafür das

(2.2) Lemma.
Zu jedem nicht-konstanten Polynom

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

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

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

Beweis:
Der Beweis zu diesem Lemma besteht aus mehreren Schritten. Ich betrachte dazu eine kompakte Menge auf der der Betrag eines Polynoms, da dieser stetig ist, auf diesem Kompaktum sein Minimum annimmt. Weiterhin zeige ich, dass ein Element dieses Kompaktums existiert, sodass der Betrag vom dem entsprechenden Funktionswert dieses Elementes kleiner oder gleich dem Betrag der anderen Funktionswerte auf ganz $\mathbb{C}$ ohne dem Kompaktum ist. Da der Betrag des Polynoms auf dem Kompaktum sein Mininum annimmt, folgt dann, dass dieses Minimum nicht nur auf dem Kompaktum, sondern auf ganz $\mathbb{C}$ angenommen wird.

Damit p den Grad n hat, sei ohne Einschränkung $a_n \neq 0$. Im Folgenden zeige ich, dass ein $R > 0$ existiert, so dass $|p(z)| \geq \frac{1}{2}|a_n|R^n$ für $|z| \geq R$ ist. Das bedeutet, dass sich $|p(z)|$ für alle $|z| \geq R$ nach unten durch einen divergenten Ausdruck abschätzen lässt und somit auch selber divergent ist.

Ich definiere mir dazu $\varepsilon := \frac{1}{2}$ und
$R := 1 + \frac{1}{|a_n|\varepsilon} \sum_{k=0}^{n-1} |a_k|$, was äquivalent ist zu $\varepsilon = \frac{\varepsilon}{R} + \frac{1}{|a_n|R} \sum_{k=0}^{n-1} |a_k|$.
Da der Betrag stets größer oder gleich 0 ist, folgt somit, dass auch stets $R \geq 1$ ist.

Mit der 2. Dreiecksungleichung aus Analysis I (vgl. I(2.9)) erhalte ich nun

$$|p(z)| = |\sum_{k=0}^{n} a_k z^k| \geq |a_n z^n| - \sum_{k=0}^{n-1} |a_k z^k|$$

und mit $|z|^n \geq |z|^k$ für alle $z \in \mathbb{C}$ mit $|z| \geq 1$ und $n, k \in \mathbb{N}$ mit $n \geq k$

$$|p(z)| \geq |a_n z^n| - \sum_{k=0}^{n-1} |a_k z^{n-1}|.$$

Es folgt für $z \neq 0$

$$|p(z)| \geq |a_n z^n|(1 - \tfrac{|z|^{n-1}}{|a_n z^n|} \sum_{k=0}^{n-1} |a_k|) = |a_n||z|^n(1 - \tfrac{1}{|a_n||z|} \sum_{k=0}^{n-1} |a_k|)$$

und somit für alle $|z| \geq R \geq 1$, da dann auch $|z|^n \geq R^n$ ist

$$|p(z)| \geq |a_n| R^n (1 - \tfrac{1}{|a_n| R} \sum_{k=0}^{n-1} |a_k|).$$

Es ist $\frac{\varepsilon}{R} > 0$ und es folgt daraus

$$|p(z)| \geq |a_n| R^n \cdot [1 - (\tfrac{\varepsilon}{R} + \tfrac{1}{|a_n| R} \sum_{k=0}^{n-1} |a_k|)] = |a_n| R^n (1 - \varepsilon) \underset{\varepsilon = \frac{1}{2}}{=} \tfrac{1}{2} |a_n| R^n$$

für alle $|z| \geq R \geq 1$.

Ich betrachte nun die Menge $M := \{z \in \mathbb{C}; |z| \leq R\}$ und aus Analysis II ist bekannt, dass es sich hierbei um ein Kompaktum handelt.

Des Weiteren betrachte ich die Funktion $f : \mathbb{C} \to \mathbb{R}$, $z \mapsto |p(z)|$. Der Körper $\mathbb{C}$ ist isomorph zum $\mathbb{R}^2$, da sich $z \in \mathbb{C}$ auch als $z = u + iv$ mit $\binom{u}{v} \in \mathbb{R}^2$ darstellen lässt. Aus Analysis II ist bekannt, dass jedes Polynom über $\mathbb{R}^n$, $n \in \mathbb{N}$, stetig ist und es folgt somit, dass auch alle komplexen Polynome stetig sind.

Der Betrag von $z = u + iv \in \mathbb{C}$ mit $|z| = \sqrt{u^2 + v^2}$ ist eine Komposition der Addition von Monomen und der Wurzelfunktion. Alle diese reellen Funktionen sind stetig, und nach Analysis I (vgl. IV(1.10)) ist somit auch der Betrag auf $\mathbb{C}$ stetig. Da f ebenfalls eine Komposition der Betragsfunktion und p ist, folgt somit, dass f stetig ist.

Da f stetig und M kompakt ist, folgt nach dem Satz vom Minimum und Maximum aus Analysis I (vgl. IV(3.7)), dass f auf M Minimum und Maximum annimmt. Dieses Minimum sei nun $c \in \mathbb{C}$, das heißt es sei $f(c) \leq f(z)$ für alle $z \in M$.

Für das oben gewählte R folgt, da der Betrag immer größer oder gleich 0 ist und wegen der Monotonie der Wurzel

$$R = 1 + \tfrac{2}{|a_n|} \sum_{k=0}^{n-1} |a_k| \geq 1 + \tfrac{2}{|a_n|} |a_0| \geq \sqrt[n]{1 + 2\tfrac{|p(0)|}{|a_n|}} \geq \sqrt[n]{2\tfrac{|p(0)|}{|a_n|}}.$$

Somit folgt für die oben gezeigte Ungleichung $|p(z)| \geq \frac{1}{2}|a_n|R^n$ für alle $|z| \geq R$:

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

Es ist stets $0 \in M$ für alle $R > 0$, das heißt es existiert ein $m \in M$, so dass $|p(m)| \leq |p(z)|$ für alle $|z| \geq R$ ist. Ich betrachte nun wieder die kompakte Menge M, auf der f sein Minimum c annimmt, das heißt es gilt $|p(c)| \leq |p(m)|$. Daraus folgt, dass $|p(c)| \leq |p(z)|$ für alle $z \in \mathbb{C}$ ist. □

— *Spezielle Eigenschaften* —

Ich komme nun zum letzten Hilfsmittel, um (1.1) beweisen zu können. Dazu betrachte ich spezielle Polynome, die später von großer Bedeutung sind. Dazu dient das

(2.3) 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:
Nach (2.1) existiert ein $d \in \mathbb{C}$ mit $d^k = -\frac{1}{b}$, was äquivalent zu $bd^k = -1$ ist. Es sei weiterhin $t \in \mathbb{R}$ mit $0 < t \leq 1$. Mit der Dreiecksungleichung gilt dann

$$\begin{aligned} |h(td)| &= |1 + b(td)^k + (td)^k g(td)| \leq |1 + b(td)^k| + |(td)^k g(td)| \\ &= |1 + bd^k t^k| + |t^k d^k g(td)| \underset{bd^k=-1}{=} |1 - t^k| + t^k |d^k g(td)|. \end{aligned}$$

Da $0 < t \leq 1$ ist, ist auch $0 < t^k \leq 1$, und es folgt

$$|h(td)| \leq 1 - t^k + t^k |d^k g(td)|.$$

Mit $b \neq 0$ ist auch $d^k = -\frac{1}{b} \neq 0$. Da g als Polynom stetig in 0 ist, existiert zu $\varepsilon = \frac{1}{2|d^k|}$ ein $\delta > 0$, sodass aus $|td - 0| < \delta$ folgt, dass $|g(td) - g(0)| < \varepsilon$ ist. Somit folgt aus $|td| < \delta$, dass $|g(td)| < \frac{1}{2|d^k|}$ ist. Dies ist äquivalent zu

$$|d^k||g(td)| < \tfrac{1}{2} \text{ für } 0 < |td| < \delta.$$

Da $d^k \neq 0$ ist, ist auch $d \neq 0$ und $|d| > 0$. Somit gilt

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

Weiterhin definiere ich mir $\gamma := \frac{\delta}{|d|}$. Da $\delta > 0$ und $|d| > 0$ sind, ist auch $\gamma > 0$. Des Weiteren kann ich $\gamma \leq 1$ einschränken, da $t \leq 1$ ist, und erhalte so für $0 < \gamma \leq 1$

$$|d^k g(td)| < \tfrac{1}{2} \text{ für } 0 < t < \gamma.$$

Daraus folgt

$$|h(td)| < 1 - t^k + \tfrac{1}{2}t^k = 1 - \tfrac{1}{2}t^k \text{ für } 0 < t < \gamma.$$

Wegen den Einschränkungen von t ist $0 < \frac{1}{2}t^k < 1$ und somit

$$|h(td)| < 1 \text{ für } 0 < t < \gamma.$$

Ich erhalte so für $u \in \mathbb{C}$ mit $u := td$ und den obigen Bedingungen $|h(u)| < 1$. □

— *Der Beweis* —

Nun habe ich alle notwendigen Hilfsmittel um den Fundamentsatz der Algebra beweisen zu können.

Beweis:
Nach (2.2) existiert ein $c \in \mathbb{C}$ mit $|p(c)| \leq |p(z)|$ für alle $z \in \mathbb{C}$. Des Weiteren nehme ich an, dass $p(c) \neq 0$ ist und definiere mir

$$h(Z) := \tfrac{p(c+Z)}{p(c)} \in \mathbb{C}[Z].$$

Dann ist nach der binomischen Formel aus Analysis I (vgl. I(1.12))

$$h(Z) = \frac{\sum_{k=0}^{n} a_k (c+Z)^k}{\sum_{k=0}^{n} a_k c^k} = \frac{\sum_{k=0}^{n} a_k \sum_{j=0}^{k} \binom{k}{j} c^{k-j} Z^j}{\sum_{k=0}^{n} a_k c^k} = \frac{\sum_{k=0}^{n} a_k (c^k + \sum_{j=1}^{k} \binom{k}{j} c^{k-j} Z^j)}{\sum_{k=0}^{n} a_k c^k}$$

$$= \frac{\sum_{k=0}^{n} a_k c^k + \sum_{k=0}^{n} \sum_{j=1}^{k} a_k \binom{k}{j} c^{k-j} Z^j}{\sum_{k=0}^{n} a_k c^k} = 1 + \frac{\sum_{k=1}^{n} \sum_{j=1}^{k} a_k \binom{k}{j} c^{k-j} Z^j}{\sum_{k=0}^{n} a_k c^k}.$$

Der Binomialkoeffizient $\binom{k}{n}$ ist laut Definition für $n > k$ immer 0 und es folgt

$$h(Z) = 1 + \sum_{k=1}^{n} \sum_{j=1}^{k} \frac{a_k}{p(c)} \binom{k}{j} c^{k-j} Z^j = 1 + \sum_{k=1}^{n} \sum_{j=1}^{n} \frac{a_k}{p(c)} \binom{k}{j} c^{k-j} Z^j.$$

Die Addition auf $\mathbb{C}$ ist assoziativ und kommutativ und es ergibt sich somit

$$h(Z) = 1 + \sum_{j=1}^{n} \sum_{k=1}^{n} \frac{a_k}{p(c)} \binom{k}{j} c^{k-j} Z^j = 1 + \sum_{j=1}^{n} (\sum_{k=1}^{n} \frac{a_k}{p(c)} \binom{k}{j} c^{k-j}) Z^j.$$

Ich definiere mir nun $b_j := \sum_{k=1}^{n} \frac{a_k}{p(c)} \binom{k}{j} c^{k-j}$, $1 \leq j \leq n$, und erhalte

$$h(Z) = 1 + \sum_{j=1}^{n} b_j Z^j.$$

Betrachtet man

$$b_n = \sum_{k=1}^{n} \frac{a_k}{p(c)} \binom{k}{n} c^{k-n},$$

so folgt, da $\binom{k}{n}$ für $k < n$ gleich 0 ist, dass $b_n = \frac{a_n}{p(c)} \binom{n}{n} c^{n-n} = \frac{a_n}{p(c)}$ ist. Damit p den Grad n hat, sei ohne Einschränkung $a_n \neq 0$. Daraus folgt, da auch $p(c) \neq 0$ ist, dass $b_n \neq 0$ ist. Somit ist h ein nicht-konstantes Polynom. Es sei nun $1 \leq l \leq n$ minimal mit $b_l \neq 0$. Dann ist

$$h(Z) = 1 + \sum_{k=1}^{n} b_k Z^k = 1 + \sum_{k=l}^{n} b_k Z^k = 1 + b_l Z^l + Z^l \sum_{k=l+1}^{n} b_k Z^{k-l}.$$

Ich definiere mir nun $g \in \mathbb{C}[Z]$ mit

$$g(Z) := \sum_{k=l+1}^{n} b_k Z^{k-l}.$$

Dabei ist $g(0) = 0$, da stets $k \neq l$ und somit auch $0^{k-l} = 0$ ist.

Dann existiert nach (2.3) ein $u \in \mathbb{C}$ mit $|h(u)| < 1$. Dies ist äquivalent zu

$$|\frac{p(c+u)}{p(c)}| = \frac{|p(c+u)|}{|p(c)|} < 1.$$

Daraus folgt, dass $|p(c+u)| < |p(c)|$ sein muss. Dies ist ein Widerspruch zu $|p(c)| \leq |p(z)|$ für alle $z \in \mathbb{C}$. Es ist $|p(z)| \geq 0$ für alle $z \in \mathbb{C}$ und somit folgt, dass $p(c) = 0$ sein muss. □

§ 3 Eigenschaften

— Linearfaktoren —

Nun möchte ich mich mit Eigenschaften des Fundamentalsatzes der Algebra beschäftigen. Dazu betrachte ich zunächst das

(3.1) Lemma.
Sei $p(Z) \in \mathbb{C}[Z]$ vom Grad $n \in \mathbb{N}$ 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:
Es sei $p(Z) = \sum_{k=0}^{n} a_k Z^k$ und damit p den Grad n hat auch $a_n \neq 0$.
Das gewünschte c existiert nach (1.1) und somit gilt für alle $Z \neq c$

$$\begin{aligned} p(Z) = p(Z) - p(c) &= \sum_{k=0}^{n} a_k Z^k - \sum_{k=0}^{n} a_k c^k \\ &= \sum_{k=0}^{n} a_k (Z^k - c^k) = (Z - c) \sum_{k=0}^{n} a_k \frac{Z^k - c^k}{Z - c}. \end{aligned}$$

Mit Hilfe der Geometrischen Summenformel aus Analysis I (vgl. I(1.8)) erhalte ich

$$p(Z) = (Z - c) \sum_{k=1}^{n} a_k \sum_{j=0}^{k-1} Z^j c^{k-1-j}.$$

Mit $q(Z) := \sum_{k=1}^{n} a_k \sum_{j=0}^{k-1} Z^j c^{k-1-j} \in \mathbb{C}[Z]$ erhalte ich $p(Z) = (Z - c)q(Z)$.

Somit ist $p(z) = (z - c)q(z)$ für alle $z \in \mathbb{C}$, $z \neq c$. Für $z = c$ ist diese Gleichung allerdings auch erfüllt, da $p(c) = 0 = 0 \cdot q(z)$ ist.

Es ist auch $q(z) = \frac{p(z)}{z-c}$ für alle $z \in \mathbb{C}$, $z \neq c$. Somit ist $q(Z)$ durch $p(Z)$ und c eindeutig bestimmt, da auch für $z = c$ wegen der Stetigkeit von q die Eindeutigkeit folgt.

Im Folgenden betrachte ich den Grad von $q(Z)$. Dazu definiere ich mir

$$g_k(Z) := \sum_{j=0}^{k-1} Z^j c^{k-1-j}, \quad g_k(Z) \in \mathbb{C}[Z], \quad 1 \leq k \leq n.$$

Weiterhin ist

$$g_k(Z) = \sum_{j=0}^{k-2} Z^j c^{k-1-j} + Z^{k-1}$$

und somit der Grad von $g_k(Z)$ gleich $k-1$ für alle $1 \leq k \leq n$. Des Weiteren ist

$$q(Z) = \sum_{k=1}^{n} a_k g_k(Z)$$

und $a_n \neq 0$ sowie der Grad von $g_n(Z)$ gleich $n-1$. Daraus folgt, dass der Grad von $q(Z)$ gleich $n-1$ ist. □

Dies führt mich direkt zu dem

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

$$p(Z) = \alpha \prod_{k=1}^{n} (Z - a_k), \qquad 0 \neq \alpha \in \mathbb{C}, \qquad a_1, \ldots, a_n \in \mathbb{C}.$$

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

Beweis:
Nach (1.1) existiert ein $a_1 \in \mathbb{C}$ mit $p(a_1) = 0$. Somit existiert nach (3.1) genau ein $q_1(Z) \in \mathbb{C}[Z]$ vom Grad $n-1$, sodass $p(Z) = (Z - a_1) \cdot q_1(Z)$ ist.

Wenn $n > 1$ ist, existiert für alle $q_{k-1}(Z)$ nach (1.1) ein $a_k \in \mathbb{C}$ mit $q_{k-1}(a_k) = 0$ und nach (3.1) genau ein $q_k(Z) \in \mathbb{C}[Z]$ mit $q_{k-1}(Z) = (Z - a_k) \cdot q_k(Z)$ für alle $1 < k < n$. Dabei ist der Grad von $q_k(Z)$ gleich $n-k$.

Somit erhalte ich für $n > 1$

$$p(Z) = \prod_{k=1}^{n-1} (Z - a_k) \cdot q_{n-1}(Z)$$

wobei $q_{n-1}(Z)$ den Grad 1 hat.

Beim weiteren Vorgehen ist der Fall $n = 1$ analog, nur mit $q_0(Z) := p(Z)$.
Nach (1.1) existiert ein $a_n \in \mathbb{C}$ mit $q_{n-1}(a_n) = 0$. Es sei $q_{n-1}(Z) := b \cdot Z + c$. Damit $q_{n-1}(a_n) = 0$ sein kann, muss $ba_n + c = 0$ gelten, was äquivalent ist zu $a_n = -\frac{c}{b}$. Es ist $b \neq 0$, weil sonst $q_{n-1}(Z)$ nicht den Grad 1 hätte. Nach (3.1) existiert genau ein konstantes Polynom $\alpha \in \mathbb{C}[Z]$ mit $q_{n-1}(Z) = (Z - a_n) \cdot \alpha$. Da α ein konstantes Polynom ist, ist auch $\alpha \in \mathbb{C}$.

Für $\alpha = b \neq 0$ ist

$$(Z - a_n) \cdot \alpha = (Z + \tfrac{c}{b}) \cdot b = b \cdot Z + c = q_{n-1}(Z).$$

Somit ergibt sich

$$p(Z) = \alpha \cdot \prod_{k=1}^{n} (Z - a_k).$$

Weil alle $q_k(Z)$, $1 \leq k < n$, durch $q_{k-1}(Z)$ beziehungsweise $p(Z)$ und a_k eindeutig bestimmt werden, wird auch α eindeutig bestimmt. Ebenso werden $a_1, \ldots, a_n$ bis auf die Reihenfolge dadurch eindeutig bestimmt. □

Dieses Korollar besagt, dass jedes komplexe Polynom vom Grad $n \in \mathbb{N}$ in n Linearfaktoren zerfällt, und man erhält auch dadurch das

(3.3) Korollar.
Ein Polynom $p(Z) \in \mathbb{C}[Z]$ vom Grad $n \in \mathbb{N}$ hat höchstens n (komplexe) Nullstellen.

Beweis:
Nach (3.2) ist für $a_1, \ldots, a_n, \alpha \in \mathbb{C}$, $\alpha \neq 0$

$$p(Z) = \alpha \prod_{k=1}^{n} (Z - a_k)$$

und somit $p(a_k) = 0$ für alle $1 \leq k \leq n$, also n mögliche Kandidaten für Nullstellen. Dabei kann es vorkommen, dass ein Kandidat mehrfach vorkommt, das heißt, dass $a_i = a_j$ für $i \neq j$ ist. Es gebe $l \leq n$ verschiedene Kandidaten für Nullstellen. Dann definiere ich mir $b_k \in \{a_1, \ldots, a_n\}$, $1 \leq k \leq l$, $b_i \neq b_j$ für $i \neq j$ und erhalte

$$p(Z) = \alpha \prod_{k=1}^{l} (Z - a_k)^{c_k}$$

wobei c_k die Häufigkeit der einzelnen Kandidaten darstellt und $\sum_{k=0}^{l} c_k = n$ ist.

Da diese Darstellung eindeutig ist und ein Produkt nur dann gleich 0 sein kann, wenn ein Faktor gleich 0 ist, folgt, dass $p(Z)$ genau l paarweise verschiedene Nullstellen, also höchstens n Nullstellen, hat. □

Somit hat jedes komplexe Polynom vom Grad $n \in \mathbb{N}$ nach (1.1) mindestens eine und nach (3.3) höchtens n komplexe Nullstellen.

— *Der Fundamentalsatz der Algebra auf* $\mathbb{R}$ —

Im Folgenden möchte ich eine reelle Version des Fundamentsatzes der Algebra veranschaulichen. Dazu betrachte ich das

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

$$p(X) = \alpha \cdot \prod_{k=1}^{r} (X - a_k) \cdot \prod_{j=1}^{s} q_j(X), \qquad 0 \neq \alpha \in \mathbb{R}, \qquad a_1, \ldots, a_r \in \mathbb{R},$$
$$q_j(X) = X^2 + b_j X + c_j, \quad b_j, c_j \in \mathbb{R}, \quad b_j^2 - 4c_j < 0, \quad 1 \leq j \leq s, \quad r + 2s = n.$$

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

Beweis:
Da $p(X) \in \mathbb{R}[X]$ ist, ist auch $p(X) \in \mathbb{C}[X]$ mit reellen Koeffizienten und es gilt $\overline{p(z)} = p(\overline{z})$ für alle $z \in \mathbb{C}$. Daraus folgt nach (3.2), dass $0 \neq \alpha$, $a_1, \ldots, a_n \in \mathbb{C}$ existieren mit

$$p(X) = \alpha \prod_{k=1}^{n} (X - a_k).$$

Es sei $r \leq n$ die Mächtigkeit der Menge $\{a_k \mid a_k \in \mathbb{R}, 1 \leq k \leq n\}$. Da $a_1, \ldots, a_n$ bis auf die Reihenfolge eindeutig bestimmt sind, erhalte ich durch geschicktes Umsortieren

$$p(X) = \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=r+1}^{n} (X - a_j)$$

wobei für $0 < r < n$ dann $a_1, \ldots, a_r \in \mathbb{R}$ und $a_{r+1}, \ldots, a_n \notin \mathbb{R}$ sind. Für $r = 0$ sind $a_1, \ldots, a_n \notin \mathbb{R}$ und für $r = n$ sind $a_1, \ldots, a_n \in \mathbb{R}$.

Ab nun betrachte ich $a_j \notin \mathbb{R}$ mit $a_j := u_j + iv_j$, $u_j, v_j \in \mathbb{R}$, $v_j \neq 0$, $1 \leq j \leq n$.

Da $\overline{p(a_j)} = 0 = p(\overline{a_j})$ ist, ist $\overline{a_j}$ eine von a_j verschiedene Nullstelle. Dabei ist wegen $v_j \neq 0$ auch $\overline{a_j} \notin \mathbb{R}$ und es ergibt sich für $s \leq \frac{n}{2}$ durch eine geeignete Umsortierung mit $\overline{a_j} = a_{s+j}$ und $r + 2s = n$

$$p(X) = \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} [(X - a_{r+j}) \cdot (X - a_{r+s+j})]$$

$$= \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} [(X - a_{r+j}) \cdot (X - \overline{a_{r+j}})]$$

$$= \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} (X^2 - \overline{a_{r+j}} X - a_{r+j} X + a_{r+j} \overline{a_{r+j}})$$

$$= \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} (X^2 - (\overline{a_{r+j}} + a_{r+j}) X + a_{r+j} \overline{a_{r+j}}).$$

Da $a_j = u_j + iv_j$ und nach Analysis I (vgl. II(4.3)) $a_j \cdot \overline{a_j} = u_j^2 + v_j^2$ ist, folgt

$$p(X) = \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} (X^2 - (u_{r+j} - iv_{r+j} + u_{r+j} + iv_{r+j}) X + u_{r+j}^2 + v_{r+j}^2)$$

$$= \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} (X^2 - 2u_{r+j} X + u_{r+j}^2 + v_{r+j}^2).$$

Dann definiere ich mir $q_j(X) \in \mathbb{R}[X]$, $q_j(X) := X^2 + b_j X + c_j$, $b_j, c_j \in \mathbb{R}$ mit $b_j := -2u_{r+j}$ und $c_j := u_{r+j}^2 + v_{r+j}^2$, $1 \leq j \leq s$, und erhalte

$$p(X) = \alpha \prod_{k=1}^{r} (X - a_k) \prod_{j=1}^{s} q_j(X)$$

Wegen $v_{r+j} \neq 0$ ist $v_{r+j}^2 > 0$ und es folgt

$$b_j^2 - 4c_j = 4u_{r+j}^2 - 4u_{r+j}^2 - 4v_{r+j}^2 = -4v_{r+j}^2 < 0.$$

Ich erhalte somit die gewünschte Darstellung von p und es bleibt nur noch die Eindeutigkeit zu zeigen. α und $a_1, \ldots, a_r$ existieren nach (3.2) und sind demnach auch eindeutig bestimmt. $q_1(X), \ldots, q_s(X)$ sind von den $a_{r+1}, \ldots, a_n$, also den nicht reellen Nullstellen von p, abgeleitet, indem ich die komplex konjugierten Nullstellen zu einem Polynom zusammengefasst habe, welches diese Nullstellen enthält. Diese sind nach (3.2) ebenfalls eindeutig bestimmt. Es bleibt nun nur noch die umgekehrte Richtung zu zeigen, dass ein Polynom $X^2 + bX + c \in \mathbb{R}[X]$ mit $b^2 - 4c < 0$ keine reellen, sondern nur 2 konjugiert komplexe Nullstellen hat:

Jede reelle Nullstelle ist auch eine komplexe Nullstelle und nach (3.3) hat ein solches Polynom höchstens 2 komplexe Nullstellen, das heißt es bleibt zu zeigen, dass diese beiden Nullstellen komplex konjugiert sind.

Dazu betrachte ich

$$X^2 + bX + c = 0$$

was äquivalent ist zu

$$X^2 + bX + (\tfrac{b}{2})^2 = (\tfrac{b}{2})^2 - c.$$

Mit Hilfe der binomischen Formel folgt dann

$$(X + \tfrac{b}{2})^2 = (\tfrac{b}{2})^2 - c$$

was wiederum äquivalent ist zu

$$X + \tfrac{b}{2} = \pm\sqrt{(\tfrac{b}{2})^2 - c}$$

und ich gelange somit zu der Gleichung

$$X = -\tfrac{b}{2} \pm \sqrt{(\tfrac{b}{2})^2 - c}.$$

Es ist $b^2 - 4c < 0$ äquivalent zu $(\frac{b}{2})^2 < c$ und somit $(\frac{b}{2})^2 - c < 0$. Dadurch ist der Term unter der Wurzel negativ und beide Nullstellen nicht auf $\mathbb{R}$ definiert. Dafür sind die beiden aber komplex konjugiert und es folgt dadurch die Eindeutigkeit von $q_1(X), \ldots, q_s(X)$. □

— Irreduzible Polynome —

Zum Schluss möchte ich mich mit irreduziblen Polynomen auseinandersetzen. Dazu verwende ich die aus der Linearen Algebra bekannte

(3.5) Definition.
Es seien K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom.
Dann ist f ein irreduzibles Polynom, wenn aus

$$f = g \cdot h, \qquad g, h \in K[X],$$

folgt, dass g oder h ein konstantes Polynom sein muss.

Als erstes betrachte ich die irreduziblen Polynome über $\mathbb{C}$ mit dem

(3.6) Korollar.
Die irreduziblen Polynome über $\mathbb{C}$ sind genau diejenigen vom Grad 1.

Beweis:
Zunächst werde ich zeigen, dass die Polynome vom Grad 1 über $\mathbb{C}$ irreduzibel sind. Dazu sei $p(Z) \in \mathbb{C}[Z]$ mit

$$p(Z) := a + bZ, \qquad a, b \in \mathbb{C}, b \neq 0.$$

Dann existiert nach (1.1) und (3.3) genau ein $c \in \mathbb{C}$ mit $p(c) = 0$ und nach (3.1) genau ein konstantes Polynom $q(Z) \in \mathbb{C}[Z]$, sodass $p(Z) = (Z - c) \cdot q(Z)$ ist. Diese Darstellung ist eindeutig bestimmt und somit ist p ein irreduzibles Polynom. Da p ein beliebiges komplexes Polynom vom Grad 1 ist, folgt, dass alle Polynome vom Grad 1 über $\mathbb{C}$ irreduzibel sind.

Es bleibt zu zeigen, dass keine weiteren irreduziblen Polynome über $\mathbb{C}$ existieren. Dazu sei $f(Z) \in \mathbb{C}[Z]$ vom Grad $n \in \mathbb{N}$, $n \geq 2$. Nach (3.2) besitzt $f(Z)$ für $0 \neq \alpha \in \mathbb{C}$, $a_1, \ldots, a_n \in \mathbb{C}$ die Darstellung

$$f(Z) = \alpha \cdot \prod_{k=1}^{n} (Z - a_k) = \alpha \cdot (Z - a_1) \cdot (Z - a_2) \cdot \prod_{k=3}^{n} (Z - a_k)$$

Daraus folgt, dass nicht-konstante Polynome $g(Z)$, $h(Z) \in \mathbb{C}[Z]$ mit

$$f(Z) = g(Z) \cdot h(Z)$$

existieren und es ist somit $f(Z)$ kein irreduzibles Polynom. Daraus erhalte ich wiederum, dass nur die Polynome vom Grad 1 über $\mathbb{C}$ irreduzibel sind. □

Nun möchte ich mich mit den irreduziblen Polynomen über $\mathbb{R}$ beschäftigen und betrachte dazu das

(3.7) Korollar.
Die irreduziblen Polynome über $\mathbb{R}$ *sind genau diejenigen vom Grad* 1 *sowie diejenigen vom Grad* 2 *ohne reelle Nullstelle.*

Beweis:
Zunächst werde ich zeigen, dass die reellen Polynome vom Grad 1 über $\mathbb{R}$ irreduzibel sind. Dazu sei $p(X) \in \mathbb{R}[X]$ vom Grad 1 mit

$$p(X) = a + bX, \qquad a,b \in \mathbb{R}, b \neq 0.$$

Dann ist $-\frac{a}{b} \in \mathbb{R}$ mit $p(-\frac{a}{b}) = 0$ und ich erhalte mit (3.4) die Darstellung

$$p(X) = \alpha \cdot (X + \tfrac{a}{b}), \qquad 0 \neq \alpha \in \mathbb{R}.$$

Diese Darstellung ist eindeutig bestimmt und daraus folgt, dass $p(X)$ ein irreduzibles Polynom ist, da α auch als konstantes Polynom, also $\alpha \in \mathbb{R}[X]$, aufgefasst werden kann. Somit sind alle Polynome vom Grad 1 über $\mathbb{R}$ irreduzibel.

Ich betrachte nun die Polynome vom Grad 2 ohne reelle Nullstelle. Es sei $f(X) \in \mathbb{R}[X]$ ein solches Polynom mit

$$f(X) = aX^2 + bX + c, \qquad a, b, c \in \mathbb{R}, a \neq 0.$$

Dies ist äquivalent zu

$$f(X) = a \cdot (X^2 + \tfrac{b}{a}X + \tfrac{c}{a}).$$

Da $f(X)$ keine reelle Nullstelle hat, entspricht diese Darstellung der Darstellung von (3.4), welche eindeutig bestimmt ist. Man kann a auch als konstantes Polynom auffassen, also $a \in \mathbb{R}[X]$. Daraus folgt, dass $f(X)$ und somit jedes Polynom vom Grad 2 ohne reelle Nullstelle über $\mathbb{R}$ irreduzibel ist.

Nun bleibt zu zeigen, dass keine weiteren irreduziblen Polynome über $\mathbb{R}$ existieren. Dazu betrachte ich das Polynom $g(X) \in \mathbb{R}[X]$ vom Grad $n \in \mathbb{N}$. Nach (3.4) besitzt $g(X)$ die Darstellung

$$g(X) = a \cdot \prod_{k=1}^{r} (X - a_k) \cdot \prod_{j=1}^{s} q_j(X), \qquad 0 \neq a, a_1, \ldots, a_r \in \mathbb{R}, \qquad r + 2s = n,$$
$$q_j(X) = X^2 + b_j X + c_j, \qquad b_j, c_j \in \mathbb{R}, \qquad b_j^2 - 4c_j < 0, \qquad 1 \leq j \leq s.$$

Ich behandle zuerst den Fall $n = 2$ und $g(X)$ hat mindestens eine reelle Nullstelle. Da $g(X)$ mindestens eine reelle Nullstelle hat, ist $r \geq 1$. Weil $r + 2s = 2$ sein soll, folgt, dass $s = 0$ und $r = 2$ sein muss. Somit erhalte ich

$$g(X) = a \cdot (X - a_1) \cdot (X - a_2)$$

und es folgt, dass zwei nicht-konstante Polynome $f(X), h(X) \in \mathbb{R}[X]$ existieren mit

$$g(X) = f(X) \cdot h(X).$$

Daraus folgt, dass $g(X)$ für diesen Fall nicht irreduzibel ist. Es sei ab nun $n \geq 3$, also auch $r + 2s \geq 3$. Dadurch ergeben sich die folgenden Bedingungen: Für $r = 0$ muss $s \geq 2$ und für $r = 1$ muss $s \geq 1$ sein. Daraus folgt genauso wie für $r \geq 2$, dass zwei nicht-konstante Polynome $f(X), h(X) \in \mathbb{R}[X]$ existieren mit

$$g(X) = f(X) \cdot h(X).$$

Somit ist $g(X)$ auch für diesen Fall nicht irreduzibel und es folgt, dass nur die Polynome vom Grad 1 und die Polynome vom Grad 2 ohne eine reelle Nullstelle irreduzibel sind. □

§ 4 Literaturverzeichnis

[1] A.Krieg: Proseminar zur Analysis. Skript, RWTH Aachen 2010.

[2] A.Krieg: Analysis I. Skript, RWTH Aachen 2007.

[3] A.Krieg: Analysis II. Skript, RWTH Aachen 2008.

[4] B. Fine: The Fundamental Theorem of Algebra, New York 1997.

[5] M. Wiesemann: Lineare Algebra I. Vorlesungsmitschrift, Aachen 2002.

[6] H. Wussing: Vorlesung zur Geschichte der Mathematik.
Frankfurt am Main 2008.