

# Der Hauptsatz der Algebra in effektiver Gestalt: ein reell-algebraischer Beweis mittels sturmscher Ketten

Michael Eisermann

Institut Fourier, Université Grenoble I  
[www-fourier.ujf-grenoble.fr/~eiserm](http://www-fourier.ujf-grenoble.fr/~eiserm)

15. Januar 2009



Carl Friedrich Gauß (1777–1855)



Augustin Louis Cauchy (1799–1857)



Charles-François Sturm (1803–1855)

Mathematisches Kolloquium, Johannes-Gutenberg-Universität Mainz

1/30

## Überblick

- 1 Der Hauptsatz der Algebra
  - Der Satz und seine Geschichte
  - Reelle Nullstellen reeller Polynome
  - Komplexe Nullstellen komplexer Polynome
- 2 Sturm 1829/1835: reelle Nullstellen reeller Polynome
  - Cauchy-Index für reelle Polynome
  - Cauchys Inversionsformel
  - Sturmsche Ketten
- 3 Sturm 1836: komplexe Nullstellen komplexer Polynome
  - Cauchy-Index für komplexe Polynome
  - Die Produktformel
  - Homotopie-Invarianz
- 4 Zusammenfassung und Ausblick

Bibliographie:

*The Fundamental Theorem of Algebra made effective:  
an elementary real-algebraic proof via Sturm chains.*

[www-fourier.ujf-grenoble.fr/~eiserm/publications.html#roots](http://www-fourier.ujf-grenoble.fr/~eiserm/publications.html#roots)

3/30 1/1

## Vorwort

Der Hauptsatz der Algebra ist ein klassisches Ergebnis der Mathematik des 19. Jahrhunderts. Er wird oft benutzt, zitiert, gelehrt, ... und verdient daher eine angemessene Aufmerksamkeit. Er ist auch heute noch aktuell, zum Beispiel im Hinblick auf seine algorithmischen und numerischen Aspekte.

Die Aussage des Satzes kann heutzutage kaum überraschen, ein schöner Beweis hingegen schon. Ich möchte hier einen reell-algebraischen Beweis vorstellen, der bemerkenswerte Vorzüge aufweist: er ist elegant, elementar, und effektiv. Das Ziel meines Vortrags ist seine Popularisierung.

Der reell-algebraische Beweis geht zurück auf Ideen von Gauß (1799), Cauchy (1831/37), und vor allem Sturm (1836), scheint aber heute völlig unbekannt. Ich hatte das Glück, ihn bei der Ausarbeitung eines Computer-Algebra-Kurses zu entdecken, und war anschließend sehr erstaunt, ihn nicht in der modernen Literatur zu finden.

Mein Beitrag besteht darin, diesen wunderschönen Beweis wieder an das Licht der (mathematischen) Öffentlichkeit zu bringen, und Sturms Skizze in moderner Strengung auszuführen.

2/30

## Der Hauptsatz der Algebra

### Satz (Kurzfassung)

*Jedes komplexe Polynom vom Grad  $n$  hat genau  $n$  komplexe Nullstellen.*

### Satz (Langfassung)

*Sei  $\mathbb{R}$  der Körper der reellen Zahlen und sei  $\mathbb{C} = \mathbb{R}[i]$  mit  $i^2 = -1$ .*

*Dann gilt: Für jedes Polynom*

$$F = Z^n + c_1 Z^{n-1} + \dots + c_{n-1} Z + c_n$$

*mit  $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$  existieren  $z_1, z_2, \dots, z_n \in \mathbb{C}$  so dass*

$$F = (Z - z_1)(Z - z_2) \dots (Z - z_n).$$

Nahe liegende Fragen:

Gibt es einen elementaren, geometrisch ansprechenden Beweis?

Kann man die Voraussetzung abschwächen? Welche geordneten Körper?

Kann man die Schlussfolgerung verstärken? Zu einer effektiven Version?

4/30

## Einige Daten zum Hauptsatz der Algebra

Scipione del Ferro (1456-1526)  
Niccolò Fontana Tartaglia (1500-1557)  
Gerolamo Cardano (1501-1576)  
Lodovico Ferrari (1522-1565)  
...  
Niels Henrik Abel (1802-1829)  
Évariste Galois (1811-1832)

Albert Girard (1595-1632)  
René Descartes (1596-1650)  
Gottfried Leibniz (1646-1716)

...  
Leonhard Euler (1707-1783)  
Jean le Rond d'Alembert (1717-1783)  
Joseph-Louis Lagrange (1736-1813)  
Pierre-Simon Laplace (1749-1827)  
...  
Carl Friedrich Gauß (1777-1855)

Augustin Louis Cauchy (1789-1857)  
Charles-François Sturm (1803-1855)

Mathematischer Tourismus



§1.1

§1.1

## Beweisstrategien

Es gibt drei Beweisstrategien zum Hauptsatz der Algebra:

- 1 Analysis, mittels Kompaktheit, Integration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820);
- 2 Algebra, mittels symmetrischer Funktionen oder Galois-Theorie (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816);
- 3 Algebraische Topologie, mittels einer Form der Umlaufzahl (Gauß 1799/1816, Cauchy 1831, Sturm-Liouville 1836)

Der hier vorgestellte Beweis ist *reell-algebraisch*, zwischen 2 und 3.

Was ist an diesem reell-algebraischen Beweis interessant?

- ✓ Er ist elementar: Arithmetik und Zwischenwertsatz reeller Polynome.
- ✓ Alle Argumente gelten über jedem reell abgeschlossenem Körper.
- ✓ Der Beweis ist konstruktiv und erlaubt das Auffinden der Nullstellen.
- ✓ Der Algorithmus ist einfach zu implementieren und ausreichend effizient.
- ✓ Formaler, computer-verifizierbarer Beweis: Hauptsatz + Algorithmus.

Kurzum: minimale Voraussetzungen, maximale Information.

§1.1

## Von den reellen Zahlen zu reell abgeschlossenen Körpern

### Satz (Charakterisierung der reellen Zahlen)

Für jeden geordneten Körper  $(\mathbf{R}, +, \cdot, \leq)$  sind äquivalent:

- 1  $(\mathbf{R}, \leq)$  erfüllt die Supremums-Bedingung.
- 2 Jedes Intervall  $[a, b] \subset \mathbf{R}$  ist kompakt.
- 3 Jedes Intervall  $[a, b] \subset \mathbf{R}$  ist zusammenhängend.
- 4 Jede stetige Funktion  $f: \mathbf{R} \rightarrow \mathbf{R}$  erfüllt den Zwischenwertsatz:  
 $f(a)f(b) < 0 \implies \exists x \in \mathbf{R}: (x-a)(x-b) < 0 \wedge f(x) = 0.$

Zwischen je zwei solchen Körper besteht genau ein Isomorphismus.  
Ein solcher Körper existiert: wir nennen ihn den Körper der reellen Zahlen.

Dies benötigt die Logik zweiter Stufe. Es reicht aber viel weniger:

### Definition (reell abgeschlossener Körper)

Ein geordneter Körper  $(\mathbf{R}, +, \cdot, \leq)$  heißt *reell abgeschlossen* wenn jedes Polynom  $P \in \mathbf{R}[X]$  den Zwischenwertsatz über  $\mathbf{R}$  erfüllt.

Beispiele: die reellen Zahlen  $\mathbb{R}$ , die reell-algebraischen Zahlen  $\mathbb{Q}^c \subset \mathbb{R}$ , ...  
Jeder geordnete Körper erlaubt einen reellen Abschluss. Beispiel:  $\mathbb{R}(X)^c$ .

§1.2

§1.2

## Ergänzung: reell abgeschlossene Körper

### Proposition

Es sei  $(\mathbf{R}, +, \cdot, \leq)$  ein reell abgeschlossener Körper.  
Die Anordnung ist eindeutig bestimmt durch  $a \geq 0 \iff \exists r \in \mathbf{R}: r^2 = a$ .

**Beweis.** Für jedes  $a \in \mathbf{R}_{>0}$  hat  $X^2 - a$  eine Nullstelle in  $[0, 1 + a]$ .  
Somit hat jedes  $a \in \mathbf{R}_{>0}$  eine Quadratwurzel  $r \in \mathbf{R}_{>0}$ ,  $r^2 = a$ .  $\square$

### Satz (reeller Abschluss)

Jeder angeordnete Körper  $(\mathbf{K}, +, \cdot, \leq)$  erlaubt einen reellen Abschluss, d.h. eine algebraische Erweiterung  $\mathbf{R} \supset \mathbf{K}$  die reell abgeschlossen ist.  
Zwischen zwei reellen Abschlüssen existiert genau ein Isomorphismus.

Dies steht im Gegensatz zum algebraischen Abschluss!

### Satz (Artin-Schreier 1927)

Sei  $\mathbf{R}$  ein Körper und sei  $\mathbf{C} \supset \mathbf{R}$  ein algebraisch abgeschlossener Körper.  
Wenn  $1 < \dim_{\mathbf{R}}(\mathbf{C}) < \infty$ , dann ist  $\mathbf{R}$  reell abgeschlossen und  $\mathbf{C} = \mathbf{R}[i]$ .

Für uns bilden reell abgeschlossene Körper die minimale Voraussetzung.

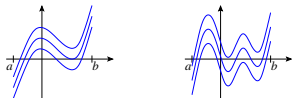
### Satz (Tarski 1951, Seidenberg 1954)

Je zwei reell abgeschlossene Körper haben dieselbe elementare Theorie.

§1.2

## Reelle Nullstellen reeller Polynome

Wie bestimmt man die Anzahl der Nullstellen von  $P \in \mathbb{R}[X]$  in  $[a, b]$ ?



Teilantworten von Descartes (1596-1650), Fourier (1768-1830), ...

### Sturmscher Satz (1829/35)

Wenn  $\mathbb{R}$  reell abgeschlossen ist, dann gilt

$$\#\{x \in [a, b] \mid P(x) = 0\} = V_a^b(S_0, S_1, \dots, S_n).$$

Hierbei entsteht die Kette  $S_0, S_1, \dots, S_n$  aus  $S_0 = P$  und  $S_1 = P'$  durch iterierte euklidische Division:  $S_{k-1} = Q_k S_k - S_{k+1}$  bis schließlich  $S_{n+1} = 0$ .

Sturms Satz erlaubt das Zählen und Auffinden aller reellen Nullstellen:



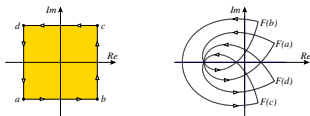
§1.2

§1.3

## Umlaufzahl: geometrische Motivation

Sei  $F \in \mathbb{C}[Z]$  ein Polynom und sei  $\Gamma \subset \mathbb{C}$  ein Rechteck.

Beispiel:  $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$  und  $\Gamma = [-1, +1] \times [-1, +1]$ .



### Geometrische Beweisidee (Gauß 1799):

Wir definieren  $\text{ind}_{\partial\Gamma}(F)$  als die Umlaufzahl von  $F|_{\partial\Gamma}$  um 0.

- Wenn  $\Gamma$  groß ist, dann gilt  $\text{ind}_{\partial\Gamma}(F) = \text{ind}_{\partial\Gamma}(Z^n) = n$ .
- Wenn  $\Gamma$  klein ist, dann gilt  $\text{ind}_{\partial\Gamma}(F) = \text{ind}_{\partial\Gamma}(\text{const}) = 0$ .
- Die Umlaufzahl ändert sich nur, wenn 0 durchlaufen wird.

Für Grad  $n \geq 1$  muss also  $F$  eine Nullstelle haben.

**Technisches Problem:** Wie kann man die Umlaufzahl streng definieren?

§1.3

## Umlaufzahl: algebraische Eigenschaften

Sei  $\mathbb{R}$  ein reell abgeschlossener Körper und sei  $\mathbb{C} = \mathbb{R}[i]$ ,  $i^2 = -1$ .

Sei  $\Omega$  die Menge stückw. polynomialer Schleifen  $\gamma: [0, 1] \rightarrow \mathbb{C}^*$ ,  $\gamma(0) = \gamma(1)$ .

### Satz

Es gibt eine Abbildung  $\text{ind}: \Omega \rightarrow \mathbb{Z}$  mit folgenden Eigenschaften:

0 **Berechnung:**  $\text{ind}(\gamma)$  berechnet sich mittels Sturms Algorithmus über  $\mathbb{R}$ .

1 **Normalisierung:** Für jedes Rechteck  $\Gamma \subset \mathbb{C}$  gilt

$$\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{falls } 0 \in \text{Int } \Gamma, \\ 0 & \text{falls } 0 \in \mathbb{C} \setminus \Gamma. \end{cases}$$

2 **Multiplikatивität:**  $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$ .

3 **Homotopie-Invarianz:**  $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$  falls  $\gamma_0 \sim \gamma_1$  in  $\mathbb{C}^*$ .

Die Schwierigkeit liegt in der **Konstruktion** einer solchen Abbildung!

- Überlagerungstheorie, angewendet auf  $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$  mit Gruppe  $\mathbb{Z}$ .
- Fundamentalgruppe,  $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$  via Seifert–van Kampen.
- Homologietheorie,  $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$  via Eilenberg–Steenrod.
- Differentialtopologie, Satz von Sard und Abbildungsgrad.
- Komplexe Analysis, analytischer Index  $\text{ind}(\gamma) = \frac{1}{2\pi i} \int_{\gamma} \frac{dz}{z}$ .
- Reelle Algebra, algebraischer Index  $\text{ind}: \Omega \rightarrow \mathbb{Z}$  via sturmsche Ketten.

§1.3

§1.3

## Ergänzung: Homotopie-Beweis des Hauptsatzes der Algebra

Wir wählen  $\Gamma = [-1, +1] \times [-1, +1] \subset \mathbb{C}$ . Zu jedem Polynom

$$F = Z^n + c_{n-1}Z^{n-1} + \dots + c_1Z + c_0$$

konstruieren wir eine Homotopie  $H: [0, 1] \times \partial\Gamma \rightarrow \mathbb{C}$  wie folgt.

Für  $t > 0$  setzen wir

$$H_t(z) = t^n F(z(1-t)/t).$$

Dies setzt sich stetig nach  $t = 0$  fort:

$$H_t(z) = (1-t)^n z^n + c_{n-1}(1-t)^{n-1} t z^{n-1} + \dots + c_1(1-t)t^{n-1} z + c_0 t^n.$$

Wir erhalten so eine Homotopie zwischen  $H_0(z) = z^n$  und  $H_1(z) = c_0$  in  $\mathbb{C}$ .

Wenn  $F$  keine Nullstellen in  $\mathbb{C}$  hat, dann ist  $H$  eine Homotopie in  $\mathbb{C}^*$ .

Der Index ergibt dann  $n = \text{ind}_{\partial\Gamma}(H_0) = \text{ind}_{\partial\Gamma}(H_1) = 0$ .

Umgekehrt, für  $n \geq 1$  muss  $F$  mindestens eine Nullstelle  $z_1 \in \mathbb{C}$  haben.

Wir faktorisieren  $F = (Z - z_1)F_1$  und schließen per Induktion über  $n$ .

§1.3

## Komplexe Nullstellen komplexer Polynome

Sei  $\mathbf{R}$  ein reell abgeschlossener Körper und sei  $C = \mathbf{R}[i]$ ,  $i^2 = -1$ .

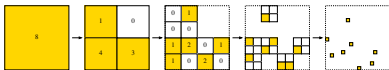
Wir können einen Index mit den nötigen Eigenschaften konstruieren:

$$\text{ind}: \left\{ \begin{array}{l} \text{stückweise polynomiale} \\ \text{Schleifen } \gamma: [0, 1] \rightarrow C^* \end{array} \right\} \rightarrow \mathbb{Z}$$

Dieser liefert einen effektiven Beweis des Hauptsatzes der Algebra:

- $\text{ind}_{\partial\Gamma}(F)$  zählt die Nullstellen von  $F$  in  $\Gamma$ . (Sturmscher Satz /  $C$ )
- $\text{ind}_{\partial\Gamma}(F) = \deg(F)$  für  $\Gamma$  ausreichend groß. (Cauchy-Schranke)

Der Index erlaubt somit alle Wurzeln von  $F$  in  $C$  zu lokalisieren:



(Nach ausreichender Näherung geht man zum Newton-Verfahren über.)

61.3

13.90

## Einige Daten zu konstruktiven und algorithmischen Aspekten

### Reell-algebraischer Index

- Sturm 1829/35: Mémoire sur la résolution des équations numériques
- Cauchy 1831/37: Calcul des résidus et calcul des indices
- Sturm–Liouville 1836: Démonstration d'un théorème de M. Cauchy

### Rezeption in Lehrbüchern

- Serret 1877: Cours d'algèbre supérieure (Sturm reell und komplex)
- Weber 1898: Lehrbuch der Algebra (Sturm reell, kaum komplex)
- Runge 1898: Enzyklopädie (Sturm reell und komplex)

### Index und Abbildungsgrad

- Kronecker 1869: Systeme von Functionen mehrer Variabeln
- Brouwer 1912: Abbildungen von Mannigfaltigkeiten
- Weyl 1924: Fundamentalsatz der Algebra

### Algorithmen und Implementationen

- Lehmer 1969: Search procedures for polynomial equation solving
- Wilf 1978: Bisection algorithm for computing zeros of polynomials
- Schönhage 1982: The fundamental theorem of algebra in terms of computational complexity

14.30

## Vorzeichenwechsel

Im Folgenden sei  $(\mathbf{R}, +, \cdot, \leq)$  ein geordneter Körper.

Wir zählen Vorzeichenwechsel  $V(s_0, s_1)$  zwischen  $s_0, s_1 \in \mathbf{R}$ :

$$V(+, -) = V(-, +) = 1,$$

$$V(+, +) = V(-, -) = V(0, 0) = 0,$$

$$V(+, 0) = V(0, +) = V(-, 0) = V(0, -) = \frac{1}{2}.$$

### Definition

Die Anzahl der Vorzeichenwechsel einer Folge  $(s_0, \dots, s_n)$  in  $\mathbf{R}$  ist

$$V(s_0, \dots, s_n) := \sum_{k=1}^n V(s_{k-1}, s_k) = \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

Für eine Folge von Polynomen  $(S_0, \dots, S_n)$  in  $\mathbf{R}[X]$  setzen wir

$$V_a(S_0, \dots, S_n) := V(S_0(a), \dots, S_n(a)).$$

Für die Differenz in  $a, b \in \mathbf{R}$  schreiben wir  $V_a^b := V_a - V_b$ .

⚠ Traditionelle Definition (Descartes, Fourier): man bildet die reduzierte Folge  $\tilde{s}$  aus  $s$  durch Weglassen aller Nullen und definiert  $V(\tilde{s}) := V(s)$ .

62.0

15.30

## Die Regeln von Descartes und Fourier

Wie bestimmt man die Anzahl der Nullstellen von  $P \in \mathbf{R}[X]$  in  $[a, b]$ ?

Viele Mathematiker haben diese Frage untersucht. Zwei berühmte Beispiele:

- Die Regel von Descartes beschränkt die Anzahl der positiven Nullstellen:

### Satz (Regel von Descartes)

Für jedes Polynom  $P = c_0 + c_1X + \dots + c_nX^n$  in  $\mathbf{R}[X]$  gilt

$$\#_{\text{mult}} \{x \in \mathbf{R}_{>0} \mid P(x) = 0\} \leq \hat{V}(c_0, c_1, \dots, c_n).$$

- Fourier hat diese Abschätzung auf beliebige Intervalle verallgemeinert:

### Satz (Regel von Fourier)

Für jedes Polynom  $P = c_0 + c_1X + \dots + c_nX^n$  in  $\mathbf{R}[X]$  gilt

$$\#_{\text{mult}} \{x \in ]a, b[ \mid P(x) = 0\} \leq \hat{V}_a^b(P, P', \dots, P^{(n)}).$$

Wenn  $P$  genau  $n$  Nullstellen in  $\mathbf{R}$  hat, dann gilt Gleichheit für alle  $]a, b[ \subset \mathbf{R}$ .

**Vorteil:** Die Abschätzung ist leicht zu berechnen.

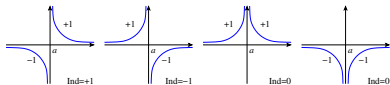
**Nachteil:** Die so erhaltenen Schranken sind oft ungenau.

Dies war der Kenntnisstand vor Sturms bahnbrechender Arbeit 1829.

16.30

## Cauchy-Index: Zählen reeller Polstellen

Es erweist sich als vorteilhaft, rationale Funktionen  $f \in \mathbf{R}(X)^*$  zu betrachten.



### Definition (Cauchy-Index)

Wir definieren den Cauchy-Index von  $f \in \mathbf{R}(X)^*$  in  $a \in \mathbf{R}$  durch

$$\text{Ind}_a(f) := \frac{1}{2} [\text{Ind}_a^+(f) - \text{Ind}_a^-(f)] \quad \text{wobei} \quad \text{Ind}_a^\pm(f) := \begin{cases} +1 & \text{falls } \lim_{x \rightarrow a^\pm} f = +\infty, \\ -1 & \text{falls } \lim_{x \rightarrow a^\pm} f = -\infty, \\ 0 & \text{sonst.} \end{cases}$$

Auf einem Intervall  $[a, b] \subset \mathbf{R}$  setzen wir

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in ]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Eigenschaften:  $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$  und  $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_{\tau(a)}^{\tau(b)}(f)$ .

§.2

17/30

## Cauchy-Index: Zählen reeller Nullstellen

### Proposition (logarithmische Ableitung)

$$\text{Für } f \in \mathbf{R}(X)^* \text{ gilt } \text{Ind}_a(f'/f) = \begin{cases} +1 & \text{falls } a \text{ eine Nullstelle von } f \text{ ist,} \\ -1 & \text{falls } a \text{ eine Polstelle von } f \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

**Beweis.** Wir faktorisieren  $f = (X - a)^m g$  so dass  $g(a) \in \mathbf{R}^*$ .

Die Leibniz-Regel ergibt  $\frac{f'}{f} = \frac{m}{X-a} + \frac{g'}{g}$ . Also  $\text{Ind}_a(\frac{f'}{f}) = \text{sign}(m)$ .  $\square$

### Korollar (reelle Nullstellen reeller Polynome)

Der Index  $\text{Ind}_a^b(P'/P)$  zählt die Nullstellen von  $P \in \mathbf{R}[X]^*$  in  $[a, b]$ :

$$\#\{x \in [a, b] \mid P(x) = 0\} = \text{Ind}_a^b\left(\frac{P'}{P}\right).$$

Nullstellen auf dem Rand  $\{a, b\}$  zählen nur zur Hälfte.

**Problem:** Kann man den Index berechnen ohne die Polstellen zu kennen?

Beispiel: Der Zwischenwertsatz lautet nun  $\text{Ind}_a^b(\frac{1}{P}) = V_a^b(1, P)$ .

Dies verlagert die Zählung vom Intervall  $[a, b]$  auf den Rand  $\{a, b\}$ .

**Allgemeine Lösung:** Sturmische Kette zur Berechnung von  $\text{Ind}_a^b(\frac{P'}{P})$ .

18/30

## Cauchys Inversionsformel über einem reell abgeschlossenem Körper

### Inversionsformel (Cauchy 1837)

Wenn  $P, Q \in \mathbf{R}[X]$  keine gemeinsame Nullstelle in  $a$  oder  $b$  haben, dann

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

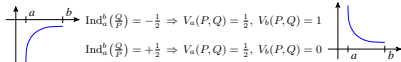
**Beweis.** Wir können  $P \neq 0$  und  $Q \neq 0$  und  $\text{ggT}(P, Q) = 1$  annehmen.

① Betrachten wir ein Intervall  $[a, b]$  das keine Wurzeln von  $P$  und  $Q$  enthält:

- Ohne Pole verschwinden die Indices  $\text{Ind}_a^b(\frac{P}{Q})$  und  $\text{Ind}_a^b(\frac{Q}{P})$ .
- Gemäß ZWS behalten  $P$  und  $Q$  ihr Vorzeichen also  $V_a^b(P, Q) = 0$ .

② Die Formel ist additiv bezüglich Unterteilung des Intervalls  $[a, b]$ .

Es reicht daher, einen einzigen Pol zu betrachten:  $P(a) = 0$  und  $Q(a) \neq 0$ .



⚠ Die Indexzählung  $\bullet$  gilt lokal um jeden Pol, auf  $[a, a + \delta]$  und  $[a - \delta, a]$  mit  $\delta > 0$ . Hierzu reicht die Stetigkeit der Polynome; dies gilt über jedem angeordneten Körper. Das globale Argument  $\bullet$  auf ganz  $[a, b]$  hingegen benötigt den Zwischenwertsatz!

§.2

19/30

## Sturmische Ketten

### Definition (sturmische Kette)

Eine Folge  $(S_0, \dots, S_n)$  in  $\mathbf{R}[X]$  heißt *sturmische Kette* auf  $[a, b] \subset \mathbf{R}$  falls gilt: Wenn  $S_k(x) = 0$  für  $0 < k < n$  und  $x \in [a, b]$ , dann  $S_{k-1}(x)S_{k+1}(x) < 0$ .

### Korollar (der Inversionsformel)

Für sturmische Ketten gilt  $\text{Ind}_a^b(\frac{S_1}{S_0}) + \text{Ind}_a^b(\frac{S_{n-1}}{S_n}) = V_a^b(S_0, S_1, \dots, S_{n-1}, S_n)$ .

**Beweis.** Die Inversionsformel bildet eine Teleskopsumme! Für  $n = 2$ :

$$\text{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \text{Ind}_a^b\left(\frac{S_0}{S_1}\right) + \text{Ind}_a^b\left(\frac{S_2}{S_1}\right) + \text{Ind}_a^b\left(\frac{S_1}{S_2}\right) = V_a^b(S_0, S_1, S_2).$$

### Proposition (euklidische Kettenbruchentwicklung)

Zu  $\frac{R}{S}$  mit  $\text{ggT}(R, S) = 1$  liefert der euklidische Algorithmus eine sturmische Kette  $S_0 = S, S_1 = R, \dots, S_n = 1, S_{n+1} = 0$  mit  $S_{k-1} = Q_k S_k - S_{k+1}$ .  $\square$

### Folgerung: der sturmische Satz

Für jedes Polynom  $P \in \mathbf{R}[X]$  über einem reell abgeschlossenem Körper gilt

$$\#\{x \in [a, b] \mid P(x) = 0\} = \text{Ind}_a^b\left(\frac{P'}{P}\right) = V_a^b(S_0, S_1, \dots, S_n).$$

20/30

## Umlaufzahl: algebraische Eigenschaften

Sei  $\mathbf{R}$  ein reell abgeschlossener Körper und sei  $\mathbf{C} = \mathbf{R}[i]$ ,  $i^2 = -1$ .

Wir wollen die algebraische Umlaufzahl konstruieren:

$$\text{ind}: \left\{ \begin{array}{l} \text{stückweise polynomiale} \\ \text{Schleifen } \gamma: [0, 1] \rightarrow \mathbf{C}^* \end{array} \right\} \rightarrow \mathbb{Z}$$

Diese soll folgende Eigenschaften haben:

1 Normalisierung: Für jedes Rechteck  $\Gamma \subset \mathbf{C}$  gilt

$$\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{falls } 0 \in \text{Int } \Gamma, \\ 0 & \text{falls } 0 \in \mathbf{C} \setminus \Gamma. \end{cases}$$

2 Multiplikativität:  $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$ .

3 Homotopie-Invarianz:  $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$  falls  $\gamma_0 \sim \gamma_1$  in  $\mathbf{C}^*$ .

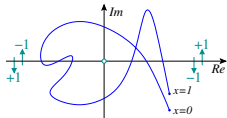
**Algorithmischer Bonus:** Berechnung mittels sturmscher Ketten.  
Computer-Algebra statt Numerik: Alle Rechnungen sind exakt.

§3.1

21/30

## Umlaufzahl: geometrische Motivation und algebraische Definition

Für  $F \in \mathbf{C}[X]$  beschreibt  $\gamma: [0, 1] \rightarrow \mathbf{C}$  mit  $\gamma(x) = F(x)$  einen Pfad in  $\mathbf{C}$ :



Beobachtung

Der Index  $\text{ind}_0^1(F) := \frac{1}{2} \text{Ind}_0^1\left(\frac{xF}{i\bar{x}F}\right)$  zählt die Umläufe um 0.

Allgemeiner: für  $a, b \in \mathbf{C}$  betrachte den Pfad  $\gamma(x) = F(a + (b-a)x)$ .

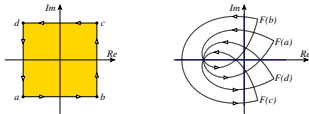
Definition

Für  $F \in \mathbf{C}[Z]$  und  $a, b \in \mathbf{C}$  setzen wir  $\text{ind}_a^b(F) = \text{ind}_0^1 F(a + (b-a)X)$ .

22/30

## Umlaufzahl bezüglich eines Rechtecks

Beispiel:  $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$  und  $\Gamma = [-1, +1] \times [-1, +1]$ .



Definition

Für jedes Polynom  $F \in \mathbf{C}[Z]$  und jedes Rechteck  $\Gamma \subset \mathbf{C}$  setzen wir

$$\text{ind}_{\partial\Gamma}(F) := \text{ind}_a^b(F) + \text{ind}_b^c(F) + \text{ind}_c^d(F) + \text{ind}_d^a(F).$$

Proposition (Normalisierung)

$$\text{Es gilt } \text{ind}_{\partial\Gamma}(Z - z_0) = \begin{cases} 1 & \text{falls } z_0 \text{ im Inneren von } \Gamma \text{ liegt,} \\ \frac{1}{2} & \text{falls } z_0 \text{ auf dem Rand von } \Gamma \text{ liegt,} \\ \frac{1}{4} & \text{falls } z_0 \text{ auf einer Ecke von } \Gamma \text{ liegt,} \\ 0 & \text{falls } z_0 \text{ im Äußeren von } \Gamma \text{ liegt.} \end{cases}$$

§3.1

23/30

## Die Produktformel

Für  $F = P + iQ$  und  $G = R + iS$  gilt  $FG = (PR - QS) + i(PS + QR)$ .

Lemma (Produktformel)

Für je zwei rationale Funktionen  $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$  gilt

$$\text{Ind}_a^b\left(\frac{PR - QS}{PS + QR}\right) = \text{Ind}_a^b\left(\frac{P}{Q}\right) + \text{Ind}_a^b\left(\frac{R}{S}\right) - \text{Val}_a^b\left(1, \frac{P}{Q} + \frac{R}{S}\right).$$

Spezialfall: Für  $P = S$  und  $Q = R$  ist dies Cauchys Inversionsformel.  
Den allgemeinen Fall beweist man genauso wie den Spezialfall.

Satz (Multiplikativität)

Wenn  $F, G \in \mathbf{C}[Z]$  keine Nullstellen in den Ecken von  $\Gamma \subset \mathbf{R}^2$  haben, dann

$$\text{ind}_{\partial\Gamma}(F \cdot G) = \text{ind}_{\partial\Gamma}(F) + \text{ind}_{\partial\Gamma}(G).$$

Korollar (Zählen komplexer Nullstellen zerfallender Polynome)

Angenommen  $F \in \mathbf{C}[Z]$  zerfällt über  $\mathbf{C}$  gemäß  $F = c(Z - z_1) \cdots (Z - z_n)$ , ohne Wurzeln auf den Ecken von  $\Gamma$ . Dann zählt  $\text{ind}_{\partial\Gamma}(F)$  die Wurzeln in  $\Gamma$ .

⚠ Wir müssen noch zeigen, dass über  $\mathbf{C}$  jedes Polynom zerfällt.

24/30

## Zählen komplexer Nullstellen

Wir wollen zeigen: Wenn  $\text{ind}_{\partial\Gamma}(F) > 0$ , dann  $F(z) = 0$  für ein  $z \in \Gamma$ .

Äquivalent hierzu: Wenn  $F(z) \neq 0$  für alle  $z \in \Gamma$ , dann  $\text{ind}_{\partial\Gamma}(F) = 0$ .

Wir betrachten die Einbettung  $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$  gemäß  $Z = X + iY$ .

### Lemma (lokale Version)

Wenn  $F \in \mathbb{C}[X, Y]$  in  $(x, y) \in \mathbb{R}^2$  nicht verschwindet, dann gibt es  $\delta > 0$  so dass  $\text{ind}_{\partial\Gamma}(F) = 0$  für alle  $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$ .

**Beweis.** Stetigkeit (explizites  $\delta$ , über beliebigem angeordneten Körper).  $\square$

### Satz (globale Version)

Wenn  $F \in \mathbb{C}[X, Y]$  auf  $\Gamma \subset \mathbb{R}^2$  nicht verschwindet, dann gilt  $\text{ind}_{\partial\Gamma}(F) = 0$ .

**Beweis.** Speziell über den reellen Zahlen  $\mathbb{R}$ : Kompaktheits-Argument. Allgemein über reell abgeschlossenen Körpern: sturmscher Satz.  $\square$

### Korollar (Zählen komplexer Nullstellen beliebiger Polynome)

Für jedes  $F \in \mathbb{C}[Z]$  zählt der Index  $\text{ind}_{\partial\Gamma}(F)$  die Wurzeln von  $F$  in  $\Gamma$ .

**Beweis.** Sei  $F = (Z - z_1) \cdots (Z - z_m)G$  so dass  $G$  keine Nullstellen in  $\mathbb{C}$  hat. Wir benutzen die Multiplikativität des Index, und obigen Satz für  $G$ .  $\square$

§3.3

25/30

## Ergänzung: Beweis mittels sturmscher Ketten

Sei  $F \in \mathbb{C}[X, Y]$  ohne Nullstellen auf  $\Gamma = [x_0, x_1] \times [y_0, y_1]$ .

Wir betrachten  $S_0 = \text{im } F$  und  $S_1 = \text{re } F$  in  $\mathbb{C}[X, Y] = \mathbb{C}[Y][X]$ .

Wir konstruieren  $S_2, \dots, S_n \in \mathbb{C}[Y][X]$  durch (pseudo-)euklidische Division:

$$\begin{aligned} c_k^2 S_{k-1} &= Q_k S_k - S_{k+1}, & Q_k &\in \mathbb{C}[Y][X], & c_k &\in \mathbb{C}[Y], \\ \deg_X S_{k+1} &< \deg_X S_k, & \deg_X S_n &= 0, & \deg_X S_0 &\in \mathbb{C}[Y]. \end{aligned}$$

● Wenn  $S_n$  auf  $[y_0, y_1]$  keine Nullstellen hat, dann gilt Sturm:  
wenn  $S_k(x, y) = 0$  in  $(x, y) \in \Gamma$ , dann  $S_{k-1}(x, y)S_{k+1}(x, y) < 0$ .

$$\begin{aligned} 2 \text{ind}_{\partial\Gamma}^{\text{C}}(F) &= + \text{Ind}_{x_0}^{x_1} \left( \frac{\text{re } F}{\text{im } F} \mid Y = y_0 \right) + \text{Ind}_{y_0}^{y_1} \left( \frac{\text{re } F}{\text{im } F} \mid X = x_1 \right) \\ &\quad + \text{Ind}_{x_1}^{x_0} \left( \frac{\text{re } F}{\text{im } F} \mid Y = y_1 \right) + \text{Ind}_{y_1}^{y_0} \left( \frac{\text{re } F}{\text{im } F} \mid X = x_0 \right) \\ &= + V_{x_0}^{x_1} (S_0, \dots, S_n \mid Y = y_0) + V_{y_0}^{y_1} (S_0, \dots, S_n \mid X = x_1) \\ &\quad + V_{x_1}^{x_0} (S_0, \dots, S_n \mid Y = y_1) + V_{y_1}^{y_0} (S_0, \dots, S_n \mid X = x_0) = 0. \end{aligned}$$

● Schlimmstenfalls endliche Menge kritischer Werte  $y \in [y_0, y_1]$ .  
Analoges Argument in  $\mathbb{C}[X][Y]$ : endliche Menge kritischer Werte  $x \in [x_0, x_1]$ .  
Um einen kritischen Punkt  $(x, y)$  wenden wir das Lemma (lokale Version) an.  
Außerhalb kritischer Punkte wenden wir das globale Ergebnis ● an.

## Große Lokalisierung der Nullstellen

### Definition (Cauchy-Schranke)

Sei  $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_1Z + c_0$  in  $\mathbb{C}[Z]$ .

Wir setzen  $M := \max\{|c_0|, \dots, |c_{n-1}|\}$  und  $\rho_F := 1 + M$ .

### Satz (große Lokalisierung der Nullstellen)

Für jedes  $z \in \mathbb{C}$  mit  $|z| \geq \rho_F$  gilt  $|F(z)| \geq 1$ .

Also liegen alle komplexen Nullstellen von  $F$  in  $B(\rho_F) = \{z \in \mathbb{C} \mid |z| < \rho_F\}$ .

**Beweis.** Der Satz gilt für  $F = Z^n$ : hier ist  $M = 0$  und  $\rho_F = 1$ .  
Im Weiteren können wir also  $M > 0$  und  $\rho_F > 1$  annehmen.

Sei  $z \in \mathbb{C}$  so dass  $|z| \geq \rho_F$ , also  $|z| - 1 \geq M$ . Hier finden wir

$$\begin{aligned} |F(z) - z^n| &= |c_0 + c_1z + \dots + c_{n-1}z^{n-1}| \leq |c_0| + |c_1||z| + \dots + |c_{n-1}||z|^{n-1} \\ &\leq M + M|z| + \dots + M|z|^{n-1} = M \frac{|z|^n - 1}{|z| - 1} \leq |z|^n - 1. \end{aligned}$$

Schließlich erhalten wir

$$\begin{aligned} |z^n| &= |z^n - F(z) + F(z)| \leq |z^n - F(z)| + |F(z)|, \quad \text{und daraus} \\ |F(z)| &\geq |z^n| - |F(z) - z^n| \geq |z|^n - (|z|^n - 1) = 1. \end{aligned}$$

§3.3

27/30

## Homotopie-Invarianz

### Satz (Homotopie-Invarianz)

Sei  $F \in \mathbb{C}[T, Z]$ . Angenommen für jedes  $t \in [0, 1]$  hat das Polynom  $F_t \in \mathbb{C}[Z]$  keine Nullstellen auf  $\partial\Gamma$ . Dann gilt  $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$ .

**Beweis.** Die Abwesenheit von Nullstellen auf  $[0, 1] \times [a, b]$  impliziert

$$\text{ind}_a^b(F \mid T = 0) - \text{ind}_a^b(F \mid T = 1) = \text{ind}_0^1(F \mid Z = a) - \text{ind}_0^1(F \mid Z = b).$$

Die Summe über alle vier Kanten von  $\Gamma$  ergibt  $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$ .  $\square$

### Korollar

Für  $F \in \mathbb{C}[Z]^n$  und  $\Gamma \supset B(\rho_F)$  gilt  $\text{ind}_{\partial\Gamma}(F) = \deg F$ .

**Beweis.** Sei  $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_0$  ein Polynom vom Grad  $n$ .  
 $F_t = Z^n + t(c_{n-1}Z^{n-1} + \dots + c_0)$  deformiert  $F_1 = F$  zu  $F_0 = Z^n$ .  
Die Cauchy-Schranke  $\rho_t = 1 + tM$  schrumpft von  $\rho_1 = \rho_F$  zu  $\rho_0 = 1$ .  
Somit hat  $F_t$  keine Nullstelle auf  $\partial\Gamma$ , und  $\text{ind}_{\partial\Gamma}(F_1) = \text{ind}_{\partial\Gamma}(F_0) = n$ .  $\square$

Dies beweist den Hauptsatz: das Rechteck  $\Gamma$  enthält  $n$  Nullstellen von  $F$ .

28/30

## Zusammenfassung und Ausblick

Über reell abgeschlossenen Körpern können wir einen Index konstruieren:

$$\text{ind}: \left\{ \begin{array}{l} \text{stückweise polynomiale} \\ \text{Schleifen } \gamma: [0, 1] \rightarrow \mathbb{C}^* \end{array} \right\} \rightarrow \mathbb{Z}.$$

Dieser erlaubt einen elementaren und effektiven Beweis des Hauptsatzes.

### Algebraische Grad-Schranken

Gilt  $\mathbb{R}$  reell  $n$ -abgeschlossen  $\iff \mathbb{R}[i]$  algebraisch  $n$ -abgeschlossen?

Die Implikation " $\implies$ " gilt in kleinen Graden. Die Umkehrung " $\Leftarrow$ " ist klar.

### Algorithmische Optimierung: asymptotische Komplexität

Auffinden der Nullstellen eines Polynoms vom Grad  $n$ :  
algebraisch:  $\tilde{O}(n^4)$ ; numerisch:  $\tilde{O}(n^3)$ , Schönhage 1982.

Wie kann der algebraische Kalkül noch effizienter gemacht werden?

### Algebraischer Abbildungsgrad in höheren Dimensionen

Brouwerscher Fixpunktsatz über reell abgeschlossenen Körpern.

Algebraische Grad-Schranken?



Vielen Dank für Ihre Aufmerksamkeit!

Michael.Eisermann@ujf-grenoble.fr  
www-fourier.ujf-grenoble.fr/~eiserm

*The Fundamental Theorem of Algebra made effective:*

*an elementary real-algebraic proof via Sturm chains*

Für Kommentare und Anregungen bin ich dankbar!