
Ein funktionentheoretischer Beweis für Masons Nullstellensatz

Joachim Klose

Joachim Klose studierte Mathematik an der Universität Göttingen, wo er 1983 mit einer Arbeit aus der algebraischen Zahlentheorie promovierte. Seitdem ist er als Softwareentwickler für Anwendungen aus der Technik und Wissenschaft tätig. Sein Interesse an der Mathematik besteht aber unvermindert fort.

1 Einleitung

Masons Nullstellensatz (d.i. die Ungleichung **(M)** im dritten Abschnitt dieser Arbeit) wurde bereits in zwei Beiträgen ([1], [2]) dieser Zeitschrift behandelt, und zwar in beiden Fällen auf elementare Weise. Für Polynome über \mathbb{C} , dem Körper der komplexen Zahlen, läßt sich Masons Ergebnis unmittelbar aus der Riemann-Hurwitzschen Formel für die Riemannsche Zahlenkugel $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ herleiten. Zugleich erhält man auf diesem Wege eine Verfeinerung von Masons Abschätzung.

Besonders hervorzuheben ist die enge Analogie, die zwischen Masons Nullstellensatz und der wichtigen zahlentheoretischen *abc*-Vermutung besteht (vgl. [1]).

2 Grundlagen

Die allgemeine Riemann-Hurwitzsche Formel ([3], S. 128) verknüpft das Geschlecht zweier kompakter Riemannscher Flächen mit der Blätterzahl und der Gesamtverzweigungsordnung einer holomorphen Überlagerungsabbildung zwischen diesen Riemannschen Flächen. Der Beweis des Satzes von Mason benötigt nur den Spezialfall des

Die *abc*-Vermutung zählt zu den interessantesten Problemen der Zahlentheorie. Diese Vermutung verknüpft die absoluten Größen dreier teilerfremder ganzer Zahlen $a, b, c = a + b$ mit den in ihnen enthaltenen Primteilern. Masons Nullstellensatz beantwortet die analoge, auf Polynome übertragene Fragestellung. Verschiedene elementare Beweise dieses Satzes sind in dieser Zeitschrift bereits vorgestellt worden (siehe Elem. Math. 48 (1993), 89–99 und Elem. Math. 55 (2000), 93–94). Der vorliegende Beitrag gewinnt mit einer funktionentheoretischen Sichtweise einen weiteren Zugang zu Masons Ergebnis. Diese funktionentheoretische Sicht ermöglicht darüber hinaus eine genaue Klärung der in Masons Satz vorgenommenen Abschätzungen.

Geschlechts 0, da er sich auf die Untersuchung rationaler Funktionen $\frac{a}{b} : \tilde{\mathbb{C}} \rightarrow \tilde{\mathbb{C}}$ stützt. Hierbei sind $a, b \in \mathbb{C}[z]$ nichtkonstante teilerfremde Polynome, $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ ist die zur zweidimensionalen Sphäre homöomorphe Riemannsche Zahlenkugel. Eine solche rationale Funktion ist eine d -blättrige Überlagerungsabbildung, wobei

$$d := \max(\deg(a), \deg(b))$$

der Grad der rationalen Funktion $\frac{a}{b}$ ist ($\deg(f)$ bezeichne den Grad des Polynoms $f \in \mathbb{C}[z]$).

Ist $w \in \tilde{\mathbb{C}}$ ein beliebiger Punkt, so ist die zugehörige Faser $F_w\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)^{-1}(\{w\})$ nicht leer und enthält mit Vielfachheit gezählt genau d Punkte aus $\tilde{\mathbb{C}}$.

Bezeichnet $f_w\left(\frac{a}{b}\right) = \left|F_w\left(\frac{a}{b}\right)\right|$ die Anzahl der verschiedenen Elemente von $F_w\left(\frac{a}{b}\right)$, so ist also $d \geq f_w\left(\frac{a}{b}\right)$. Der Punkt w heißt *kritischer Wert* von $\frac{a}{b}$, wenn die strikte Ungleichung $d > f_w\left(\frac{a}{b}\right)$ besteht; in diesem Falle enthält die Faser $F_w\left(\frac{a}{b}\right)$ Verzweigungspunkte der rationalen Funktion $\frac{a}{b}$. Ein *Verzweigungspunkt* von $\frac{a}{b}$ ist ein Punkt $z \in \tilde{\mathbb{C}}$, in dem die Funktion $\frac{a}{b}$ den Wert $\frac{a}{b}(z) \in \tilde{\mathbb{C}}$ mit einer Vielfachheit größer als 1 annimmt; dabei ist der Begriff der Vielfachheit in der üblichen, aus der Funktionentheorie bekannten Weise erklärt. Ist $v\left(\frac{a}{b}, z\right)$ die dem Punkt $z \in \tilde{\mathbb{C}}$ bezüglich der Funktion $\frac{a}{b}$ zugeordnete Vielfachheit, so ist $v\left(\frac{a}{b}, z\right) - 1$ die *Verzweigungsordnung* von $\frac{a}{b}$ im Punkt z . Da $\frac{a}{b}$ nur endlich viele Verzweigungspunkte hat, kann man die Summe

$$V\left(\frac{a}{b}\right) = \sum_{z \in \tilde{\mathbb{C}}} \left(v\left(\frac{a}{b}, z\right) - 1\right)$$

bilden, in der fast alle Summanden 0 sind. $V\left(\frac{a}{b}\right)$ ist die *Gesamtverzweigungsordnung* der rationalen Funktion $\frac{a}{b}$. $V\left(\frac{a}{b}\right)$ läßt sich auch durch Summation über die (endliche) Menge $\text{Krit}\left(\frac{a}{b}\right)$ der kritischen Werte von $\frac{a}{b}$ darstellen:

$$\begin{aligned} V\left(\frac{a}{b}\right) &= \sum_{w \in \text{Krit}\left(\frac{a}{b}\right)} \sum_{z \in F_w\left(\frac{a}{b}\right)} \left(v\left(\frac{a}{b}, z\right) - 1\right) \\ &= \sum_{w \in \text{Krit}\left(\frac{a}{b}\right)} \left(\sum_{z \in F_w\left(\frac{a}{b}\right)} v\left(\frac{a}{b}, z\right) - \sum_{z \in F_w\left(\frac{a}{b}\right)} 1 \right) \\ &= \sum_{w \in \text{Krit}\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right). \end{aligned} \tag{1}$$

Die Riemann-Hurwitzsche Formel ([3], S. 128) besagt nun für $\frac{a}{b} : \tilde{\mathbb{C}} \rightarrow \tilde{\mathbb{C}}$, da $\tilde{\mathbb{C}}$ das Geschlecht 0 hat:

$$\frac{1}{2} V\left(\frac{a}{b}\right) = d - 1. \quad (2)$$

Anmerkung: Die diesem Abschnitt zugrundeliegenden funktionentheoretischen Resultate finden sich in [3].

3 Anwendung auf Masons Nullstellensatz

Die Menge der verschiedenen Nullstellen in \mathbb{C} eines nichtkonstanten Polynoms $f \in \mathbb{C}[z]$ sei $N_0(f)$, ihre Anzahl $n_0(f) = |N_0(f)|$.

Masons Satz legt drei nichtkonstante, teilerfremde Polynome $a, b, c := a + b$ aus $\mathbb{C}[z]$ zugrunde; gesucht ist eine Abschätzung für $n_0(abc) = n_0(a) + n_0(b) + n_0(c)$. Die Abschätzung soll dabei naturgemäß nur durch solche Größen geleistet werden, die man bestimmen kann, *ohne* die Nullstellen der beteiligten Polynome zu kennen.

Betrachtet man die aus a, b durch Quotientenbildung entstehende rationale Funktion $\frac{a}{b} : \tilde{\mathbb{C}} \rightarrow \tilde{\mathbb{C}}$ und zieht den vorangehenden Abschnitt heran, so ist zunächst $N_0(a) = F_0\left(\frac{a}{b}\right) \cap \mathbb{C}$, $N_0(b) = F_\infty\left(\frac{a}{b}\right) \cap \mathbb{C}$, $N_0(c) = N_0(a + b) = F_{-1}\left(\frac{a}{b}\right) \cap \mathbb{C}$. Berücksichtigt man, daß der Punkt $\infty \in \tilde{\mathbb{C}}$ in höchstens einer der drei Fasern $F_0\left(\frac{a}{b}\right), F_\infty\left(\frac{a}{b}\right), F_{-1}\left(\frac{a}{b}\right)$ enthalten sein kann und setzt demgemäß

$$\delta(a, b) := \begin{cases} 0 & \infty \notin F_0\left(\frac{a}{b}\right) \cup F_\infty\left(\frac{a}{b}\right) \cup F_{-1}\left(\frac{a}{b}\right), \\ 1 & \text{sonst,} \end{cases}$$

so ergibt sich mit

$$d := \max(\deg(a), \deg(b), \deg(c)) = \max(\deg(a), \deg(b))$$

sowie

$$\text{Krit}'\left(\frac{a}{b}\right) := \text{Krit}\left(\frac{a}{b}\right) \setminus \{0, -1, \infty\}$$

aufgrund von (1) und (2)

$$\begin{aligned} n_0(abc) &= n_0(a) + n_0(b) + n_0(c) \\ &= f_0\left(\frac{a}{b}\right) + f_\infty\left(\frac{a}{b}\right) + f_{-1}\left(\frac{a}{b}\right) - \delta(a, b) \\ &= \sum_{w \in \{0, -1, \infty\}} \left(f_w\left(\frac{a}{b}\right) - d\right) + 3d - \delta(a, b) \\ &= \sum_{w \in \{0, -1, \infty\}} \left(f_w\left(\frac{a}{b}\right) - d\right) + \sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(f_w\left(\frac{a}{b}\right) - d\right) \\ &\quad + \sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right) + 3d - \delta(a, b) \end{aligned}$$

$$\begin{aligned}
&= -V\left(\frac{a}{b}\right) + \sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right) + 3d - \delta(a, b) \\
&= -2(d-1) + \sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right) + 3d - \delta(a, b) \\
&= d + 2 - \delta(a, b) + \sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right) \geq d + 1. \tag{3}
\end{aligned}$$

Die hiermit hergeleitete Ungleichung

$$\max(\deg(a), \deg(b), \deg(c)) \leq n_0(abc) - 1 \tag{M}$$

ist Masons Nullstellensatz für Polynome über \mathbb{C} (vgl. [1], S. 90).

Die jetzt noch zu bewältigende Aufgabe besteht darin, die in (3) auftretenden Summanden $\delta(a, b)$ und $\sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right)$ enger mit den Eigenschaften der Polynome a, b zu verknüpfen. Dabei seien $a, b \in \mathbb{C}[z]$ stets als teilerfremd und nichtkonstant vorausgesetzt (dann sind $a, b, c = a + b$ von selbst teilerfremd und auch paarweise teilerfremd).

Zunächst gilt

Hilfssatz 1

$$\delta(a, b) = \begin{cases} 0 & \deg(a) = \deg(b) = \deg(c), \\ 1 & \text{sonst.} \end{cases}$$

Beweis. Wegen

$$\frac{a}{b}(\infty) = \begin{cases} 0 & \deg(a) < \deg(b), \\ \infty & \deg(a) > \deg(b), \\ \frac{l(a)}{l(b)} & \deg(a) = \deg(b) \end{cases}$$

(wobei $l(f)$ der Leitkoeffizient des Polynoms f ist) ergeben sich die Äquivalenzen

$$\begin{aligned}
\infty &\notin F_0\left(\frac{a}{b}\right) \cup F_\infty\left(\frac{a}{b}\right) \cup F_{-1}\left(\frac{a}{b}\right) \\
&\Leftrightarrow \deg(a) = \deg(b) \quad \text{und} \quad l(a) \neq -l(b) \\
&\Leftrightarrow \deg(a) = \deg(b) = \deg(c);
\end{aligned}$$

somit ist $\delta(a, b) = 0$ genau dann, wenn die Grade von a, b und c übereinstimmen. \square

Um $\sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right)$ mit Eigenschaften der Polynome a, b beschreiben zu können, müssen die Verzweigungspunkte von $\frac{a}{b}$ und ihre Bilder unter $\frac{a}{b}$, die kritischen Werte von $\frac{a}{b}$, bestimmt werden. Die Verzweigungspunkte $z \in \mathbb{C}$ von $\frac{a}{b}$ sind dadurch gekennzeichnet, daß $\frac{a}{b}$ in ihnen die jeweils zugehörigen Funktionswerte mit einer Vielfachheit ≥ 2 annimmt.

Als erstes werde der Punkt ∞ betrachtet. Die Bestimmung von $\frac{a}{b}(\infty)$ im Beweis von Hilfssatz 1 zeigt, daß $\frac{a}{b}(\infty)$ höchstens dann zu $\text{Krit}'\left(\frac{a}{b}\right)$ gehört, wenn $a = \sum_{i=0}^d \alpha_i z^i$ ($\alpha_i \in \mathbb{C}$, $\alpha_d \neq 0$) und $b = \sum_{j=0}^d \beta_j z^j$ ($\beta_j \in \mathbb{C}$, $\beta_d \neq 0$) den gleichen Grad d haben und $\alpha_d \neq -\beta_d$. Seien diese Bedingungen erfüllt. Das Verhalten von $\frac{a}{b}$ in ∞ ist festgelegt als das Verhalten von $z \mapsto \frac{a}{b}\left(\frac{1}{z}\right)$ in 0. Wegen

$$\frac{a}{b}\left(\frac{1}{z}\right) - \frac{a}{b}(\infty) = \frac{\sum_{i=0}^d \alpha_i z^{d-i}}{\sum_{j=0}^d \beta_j z^{d-j}} - \frac{\alpha_d}{\beta_d} = \frac{\sum_{k=1}^d (\beta_d \alpha_{d-k} - \alpha_d \beta_{d-k}) z^k}{\beta_d^2 + \sum_{k=1}^d \beta_{d-k} z^k}$$

nimmt $\frac{a}{b}$ in ∞ den Wert $\frac{\alpha_d}{\beta_d}$ mit der Vielfachheit

$$v\left(\frac{a}{b}, \infty\right) = \min\{k \mid 1 \leq k \leq d, \beta_d \alpha_{d-k} - \alpha_d \beta_{d-k} \neq 0\}$$

an.

Damit ist gezeigt:

Hilfssatz 2 Für nichtkonstante teilerfremde Polynome $a = \sum_{i=0}^m \alpha_i z^i$, $b = \sum_{j=0}^n \beta_j z^j$ aus $\mathbb{C}[z]$ mit $\alpha_m \neq 0$, $\beta_n \neq 0$ ist ∞ genau dann ein Verzweigungspunkt von $\frac{a}{b}$ derart, daß dessen zugehöriger kritischer Wert $\frac{a}{b}(\infty)$ nicht in $\{0, -1, \infty\}$ enthalten ist, wenn

$$\deg(a) = m = n = \deg(b) =: d \quad \text{und} \quad \alpha_d \neq -\beta_d \quad \text{und} \quad \beta_d \alpha_{d-1} - \alpha_d \beta_{d-1} = 0. \quad (4)$$

Sind die Bedingungen (4) erfüllt, so ist

$$v\left(\frac{a}{b}, \infty\right) = \min\{k \mid 1 \leq k \leq d, \beta_d \alpha_{d-k} - \alpha_d \beta_{d-k} \neq 0\}.$$

Die in \mathbb{C} gelegenen Verzweigungspunkte von $\frac{a}{b}$ sind gerade die Nullstellen von $a'b - ab'$ (diese Nullstellenmenge besteht nämlich aus den Lösungen von $\left(\frac{a}{b}\right)'(z) = 0$ mit der Zusatzbedingung $b(z) \neq 0$, und den mehrfachen Nullstellen von b).

Hilfssatz 3 Seien $a, b, c = a + b \in \mathbb{C}[z]$ nichtkonstante teilerfremde Polynome; sei

$$\epsilon(a, b) := \begin{cases} v\left(\frac{a}{b}, \infty\right) - 1 & \text{falls die Bedingungen (4) von Hilfssatz 2 erfüllt sind,} \\ 0 & \text{sonst.} \end{cases}$$

Dann ist

$$\sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right)\right) = \epsilon(a, b) + \deg(a'b - ab') - \deg(\text{ggT}(a'b - ab', abc)).$$

Hierbei bezeichnet $\text{ggT}(a'b - ab', abc) \in \mathbb{C}[z]$ den größten gemeinsamen Teiler der Polynome $a'b - ab'$ und abc ; dieser kann ermittelt werden, ohne die Nullstellen von $a'b - ab'$ bzw. abc zu kennen (nämlich mit dem Euklidischen Algorithmus und der Polynomdivision im Polynomring $\mathbb{C}[z]$, vgl. [4], §17).

Beweis. Mit $R := \left\{ z \in \tilde{\mathbb{C}} \mid v\left(\frac{a}{b}, z\right) \geq 2 \text{ und } \frac{a}{b}(z) \notin \{0, -1, \infty\} \right\}$ ergibt sich, wie im zweiten Abschnitt vorgeführt wurde,

$$\sum_{w \in \text{Krit}'\left(\frac{a}{b}\right)} \left(d - f_w\left(\frac{a}{b}\right) \right) = \sum_{z \in R} \left(v\left(\frac{a}{b}, z\right) - 1 \right) = \sum_{z \in R \setminus \{\infty\}} \left(v\left(\frac{a}{b}, z\right) - 1 \right) + \epsilon(a, b). \quad (5)$$

Weiterhin ist

$$R \setminus \{\infty\} = N_0(a'b - ab') \setminus N_0(abc), \quad (6)$$

denn $\left(\frac{a}{b}\right)^{-1}(\{0, -1, \infty\}) \cap \mathbb{C} = N_0(abc)$. Aus der Gleichung $\left(\frac{a}{b}\right)' \cdot b^2 = a'b - ab'$ ersieht man anhand der Leibnizschen Regel für die höheren Ableitungen von Produkten, daß $z \in \mathbb{C}$ genau dann k -fache Nullstelle von $\left(\frac{a}{b}\right)'$ und keine Nullstelle von b ist, wenn z k -fache Nullstelle von $a'b - ab'$ und keine Nullstelle von b ist. Daraus folgt in Verbindung mit (6) für $a'b - ab'$ die Produktdarstellung

$$a'b - ab' = p(z) \cdot \prod_{u \in R \setminus \{\infty\}} (z - u)^{v\left(\frac{a}{b}, u\right) - 1}$$

mit einem Polynom $p(z)$, dessen Nullstellen sämtlich zu $N_0(abc)$ gehören. Mehr noch: $p(z)$ ist ein Teiler von abc . Ist nämlich θ eine k -fache Nullstelle von a , so gehört θ einerseits nicht zu $R \setminus \{\infty\}$ und ist andererseits, wie sich aus der Teilerfremdheit von a und b sofort ergibt, eine Nullstelle der Ordnung $k - 1$ von $a'b - ab'$; also ist θ eine Nullstelle der Ordnung $k - 1$ von $p(z)$. Entsprechendes gilt für die Nullstellen von b und auch für die Nullstellen von c , wenn man $a'b - ab' = c'b - cb'$ beachtet. Da nach (6) die Polynome

$\prod_{u \in R \setminus \{\infty\}} (z - u)^{v\left(\frac{a}{b}, u\right) - 1}$ und abc teilerfremd sind, folgt $\text{ggT}(a'b - ab', abc) = p$. Damit erhält man

$$\begin{aligned} \sum_{z \in R \setminus \{\infty\}} \left(v\left(\frac{a}{b}, z\right) - 1 \right) &= \deg \left(\prod_{u \in R \setminus \{\infty\}} (z - u)^{v\left(\frac{a}{b}, u\right) - 1} \right) = \deg \left(\frac{a'b - ab'}{p} \right) \\ &= \deg(a'b - ab') - \deg(\text{ggT}(a'b - ab', abc)). \end{aligned}$$

Bringt man dies in Gleichung (5) ein, ist der Beweis des Hilfssatzes abgeschlossen. \square

Fassen wir abschließend die Aussagen der Hilfssätze 1, 2, 3 mit der Gleichung (3) zusammen.

Satz Seien $a = \alpha_m z^m + \alpha_{m-1} z^{m-1} + \dots + \alpha_0$, $b = \beta_n z^n + \beta_{n-1} z^{n-1} + \dots + \beta_0$, $c := a + b$ nichtkonstante teilerfremde Polynome über \mathbb{C} mit $\alpha_m \neq 0, \beta_n \neq 0$; $d := \max(\deg(a), \deg(b), \deg(c))$ bedeute das Maximum der Grade dieser Polynome.

Setzt man

$$\eta(a, b) := \begin{cases} \min\{k \mid 1 \leq k \leq d, \beta_d \alpha_{d-k} - \alpha_d \beta_{d-k} \neq 0\} & \deg(a) = \deg(b) = \deg(c), \\ 0 & \text{sonst,} \end{cases}$$

so ist die Anzahl $n_0(abc)$ der verschiedenen Nullstellen von abc gegeben durch

$$n_0(abc) = d + 1 + \eta(a, b) + (\deg(a'b - ab') - \deg(\text{ggT}(a'b - ab', abc))). \quad (7)$$

Sämtliche auf der rechten Seite von (7) auftretenden Größen sind ohne Kenntnis der Nullstellen von abc und $a'b - ab'$ bestimmbar.

Genau dann besteht die Gleichung $n_0(abc) = d + 1$, wenn die Grade $\deg(a)$, $\deg(b)$, $\deg(c)$ nicht alle übereinstimmen und $a'b - ab'$ ein Teiler von abc ist.

Literatur

- [1] Lang, S.: Die abc -Vermutung. *Elem. Math.* 48 (1993), 89–99.
- [2] Snyder, N.: An Alternate Proof of Mason's Theorem. *Elem. Math.* 55 (2000), 93–94.
- [3] Forster, O.: *Riemannsche Flächen*. Heidelberger Taschenbücher Band 184. Springer-Verlag, 1977.
- [4] van der Waerden, B.L.: *Algebra I*. Achte Auflage. Heidelberger Taschenbücher Band 12. Springer-Verlag, 1971.

Joachim Klose
Weiherstr. 16
D–53111 Bonn, Deutschland



To access this journal online:
<http://www.birkhauser.ch>
