Seminararbeit zum Vortrag "Satz von Roth I" im Seminar "Analysis" bei Prof. Dr. Hein

Marius Müller

Juli 2022

Abstract

Diese Arbeit behandelt den *Satz von Thue-Siegel-Roth*, der mittels des Irrationalitätsmaßes eine Aussage über die Irrationalität algebraisch irrationaler Zahlen liefert.
In dieser Arbeit wird zur Thematik hingeführt, die nötigen Grundlagen behandelt und das erste Theorem im Beweis des Satzes erklärt und bewiesen.

Contents

1 Einleitung

Der *Satz von Thue-Siegel-Roth* (im Folgenden kurz *Satz von Roth* genannt) wurde erstmals von *Klaus Friedrich Roth* bewiesen, der im Jahre 1958 für diesen Meilenstein die *Fields-Medallie* verliehen bekam.
Diese Arbeit ist eng an das Kapitel VI des Buches "An Introduction To Diophantine Approximation" von John W. S. Cassels aus 1957 angelehnt.
Der Beweis des *Satzes von Roth* gliedert sich hier in drei Theorems. Von diesen wird in dieser Arbeit der erste Satz, das *Theorem II*, beschrieben, erklärt und bewiesen (der *Satz von Roth* selbst ist hier das *Theorem I*; der Übersichtlichkeit halber wird sich an die Nummerierung der Quelle gehalten; die Notation wurde jedoch stellenweise abgeändert.)

2 Motivation des Themas

Das sogenannte *Irrationalitätsmaß* quantifiziert die Irrationalität einer reellen Zahl. Dazu wird die folgende Definition verwendet:

2.1 Das Irrationalitätsmaß

Sei $x \in \mathbb{R}$ beliebig. Sei M die Menge aller $\mu \in \mathbb{R}$, sodass die Ungleichung

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^\mu}$$

nur endlich viele Lösungen in $p \in \mathbb{Z}, q \in \mathbb{N}$ besitzt. Dann heißt

$$\mu(x) \coloneqq \inf(M)$$

das *Irrationalitätsmaß* von x.
Die folgenden Beispiele illustrieren diese Definition.

2.2 Beispiele zum Irrationalitätsmaß

- Für $x \in \mathbb{Q}$ gilt: $\mu(x) = 1$
- Für irrationale x wurde gezeigt, dass gilt: $\mu(x) \geq 2$
- Für die *eulersche Zahl* e gilt: $\mu(e) = 2$
- Das Irrationalitätsmaß der Kreiszahl π ist bisher unbekannt. Der neuste Fortschritt setzt die obere Schranke bei $\mu(\pi) \leq 7,1032\ldots$ fest.

2.3 Grundlegende Aussage des *Satzes von Roth*

Es stellt sich nach den oben genannten Beispielen die Frage, ob alle irrationalen Zahlen dasselbe Irrationalitätsmaß besitzen.
Dies ist zwar im Allgemeinen nicht der Fall, der *Satz von Roth* liefert jedoch eine teilweise Antwort:
Das Irrationalitätsmaß aller *algebraisch* irrationalen Zahlen ist genau zwei.

3 Grundlagen und Voraussetzungen

In diesem Kapitel werden die Grundlagen behandelt, die für den Beweis des *Satzes von Roth* benötigt werden. Außerdem wird die formale Aussage des Satzes dargelegt; der Beweis wird jedoch nicht in dieser Arbeit vollzogen.

3.1 Notation

In dieser Arbeit wird $\mathbb{N}$ verwendet als natürliche Zahlen *ohne* Null, wogegen $\mathbb{N}_0$ die natürlichen Zahlen *inklusive* der Null meint.

3.2 algebraische Zahlen

Eine komplexe Zahl $z \in \mathbb{C}$ heißt *algebraisch* genau dann, wenn gilt:

$$\exists f \in \mathbb{Q}[x] : f(z) = 0 \tag{1}$$

d.h. falls z eine Lösung eines Polynoms mit rationalen Koeffizienten $a_k = \frac{p_k}{q_k}$ mit $p_k \in \mathbb{Z},\ q_k \in \mathbb{N}\ (\forall\ 1 \leq k \leq n)$ ist.
Die Zahl $n = \deg f$ heißt *Grad* der algebraischen Zahl z.
OBdA kann angenommen werden, dass $f \in \mathbb{Z}[x]$, da sich die Gleichung $f(x) = 0$ mit dem Produkt der Nenner der Koeffizienten multiplizieren lässt, wodurch alle Koeffizienten ganzzahlig werden, die Gleichung und damit auch das resultierende Polynom jedoch dieselben Lösungen bzw. Nullstellen besitzen. Weiterhin lässt sich oBdA annehmen, dass für den Koeffizienten der höchsten Potenz von x gilt: $a_n \neq 0$.

3.3 Der Satz von Roth (*Theorem I*)

Sei $\xi \in \mathbb{R}$ algebraisch irrational und $\delta > 0$ beliebig. Dann besitzt die Ungleichung

$$0 < \left| \xi - \frac{p}{q} \right| < q^{-(2+\delta)} \tag{2}$$

nur endlich viele Lösungen in $p \in \mathbb{Z}$, $q \in \mathbb{N}$.

Hiermit liefert der Satz die obere Schranke 2 für das Irrationalitätsmaß algebraisch irrationaler Zahlen; zusammen mit der unteren Schranke von ebenfalls 2 gilt somit $\mu(x) = 2$ für alle algebraisch irrationalen Zahlen x.

Zunächst wird gezeigt, dass der Satz nur für $a_n = 1$ aus 3.2 zu zeigen ist.

3.4 Normieren des Polynoms einer algebraischen Zahl

Angenommen, der *Satz von Roth* gelte. Dann folgt aus $f(\xi) = 0$ aus 3.2 durch Multiplikation mit a_n^{n-1} für $a_n\xi \coloneqq \Xi$:

$$0 = \Xi^n + a_{n-1}\Xi^{n-1} + a_{n-2}a_n\Xi^{n-2} + \cdots + a_n^{n-1}a_0$$

und nach Multiplikation mit $|a_n|$ und geeigneter Abschätzung von (2) gilt:

$$\left|\Xi - a_n\frac{p}{q}\right| < |a_n|\, q^{-(2+\delta)} < q^{-(2+\frac{1}{2}\delta)}$$

für hinreichend große q. Da δ beliebig gewählt wurde, gilt der Satz somit nun für Ξ genau dann, wenn er für ξ gilt. Somit gilt insgesamt oBdA:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \text{ mit } f(\xi) = 0 \text{ und } a_{n-1}, \ldots, a_0 \in \mathbb{Z}. \quad (3)$$

Sei im Übrigen

$$a = \max\{1, |a_{n-1}|, \ldots, |a_0|\}. \quad (4)$$

Dies wird im weiteren Verlauf der Arbeit und des Beweises verwendet.

3.5 Polynome

In diesem Abschnitt werden Polynome und weitere Begriffe definiert, die in diesem Kapitel verwendet werden. Darauf folgen zwei Lemmata, die diese jeweils kurz näher beleuchten.

3.5.1 Definition der Polynome

Es werden Polynome der folgenden Form behandelt:

$$R : \mathbb{R}^m \to \mathbb{R},\ R(x_1, \ldots, x_m) = \sum_{\substack{0 \le j_\mu \le r_\mu \\ 1 \le \mu \le m}} c_{j_1,\ldots,j_m} \cdot x_1^{j_1} \ldots x_m^{j_m} \quad (5)$$

wobei $m \in \mathbb{N}$, r_μ der Grad des Polynoms in x_μ und $c_{j_1,\ldots,j_m} \in \mathbb{R}$ seien.

Beispiel: Seien $m = 2,\ r_1 = 2$ und $r_2 = 1$.
Das zugehörige Polynom nach obiger Definition sieht folgendermaßen aus:

$$R_{Bsp}(x_1, x_2) = c_{0,0}x_1^0x_2^0 + c_{0,1}x_1^0x_2^1 + c_{1,0}x_1^1x_2^0 + c_{1,1}x_1^1x_2^1 + c_{2,0}x_1^2x_2^0 + c_{2,1}x_1^2x_2^1$$

Nach konkreter Definition der Koeffizienten ergibt sich beispielsweise:

$$R_{Bsp}(x_1, x_2) = 7 - \sqrt{\pi}x_2^1 + \frac{e}{\sqrt[3]{\gamma}}x_1^2x_2^1$$

3.5.2 Der Inhalt eines Polynoms

Sei R ein Polynom nach obiger Definition.
Dann sei der *Inhalt* eines Polynoms wie folgt definiert:

$$\left| \mathrm{R} \right| \coloneqq \max\{|c_{j_1,\ldots,j_m}|\} \ \forall\ 0 \leq j_\mu \leq r_\mu,\ 1 \leq \mu \leq m \tag{6}$$

3.5.3 Das Restpolynom

Sei R ein Polynom nach obiger Definition und seien $i_1, \ldots, i_m \in \mathbb{N}_0$. Es wird

$$R_{i_1,\ldots,i_m} = \frac{1}{i_1!, \ldots, i_m!} \frac{\partial^{i_1+\cdots+i_m}}{\partial x_1^{i_1} \ldots \partial x_m^{i_m}}(R) \tag{7}$$

das *Restpolynom* von R genannt.

3.5.4 Der Index eines Polynoms

Sei R ein Polynom nach obiger Definition, $\alpha \in \mathbb{R}^m$ und $s \in \mathbb{N}^m$. $I \in \mathbb{R}$ heißt *Index* von R an der Stelle α bezüglich s genau dann, wenn gilt:

$$I \coloneqq \mathrm{ind}(R) \coloneqq \min_{(i_1,\ldots,i_m)\in\mathbb{N}_0^m} \sum_{1\leq\mu\leq m} \frac{i_\mu}{s_\mu},\ \text{sodass}\ R_{i_1,\ldots,i_m}(\alpha) \neq 0. \tag{8}$$

Falls R verschwindet, wird konventionell $\mathrm{ind}(R) \coloneqq \infty$ gesetzt.

Dies erinnert an die *Nullstellenordnung* einer Funktion (beispielsweise Nullstellen *zweiter Ordnung* beziehungsweise *zweifache* Nullstellen), lässt sich jedoch mit Hilfe des m-Tupels s noch zusätzlich gewichten.

Zu diesem Begriff folgt wie erwähnt ein Lemma, das weitere Eigenschaften darlegt. In dieser Arbeit wird diese Definition über einen Nebensatz hinaus jedoch nicht weiter verwendet; er findet lediglich in den Beweisen der weiteren Theoreme im Beweis des *Satzes von Roth* weitere Anwendung.

3.6 Lemma 1

Sei R ein Polynom nach obiger Definition. Dann gilt:

1. R hat ausschließlich Koeffizienten in $\mathbb{Z} \Rightarrow R_{i_1,\ldots,i_m}$ hat auch ausschließlich Koeffizienten in $\mathbb{Z}$.
2. R hat Grad r_μ in $x_\mu \Rightarrow R_{i_1,\ldots,i_m}$ hat höchstens Grad $r_\mu - i_\mu$ in x_μ und verschwindet für $r_\mu < i_\mu$ ($\forall\ 1 \leq \mu \leq m$).
3. Es gilt $\left\lceil \mathrm{R}_{i_1,\ldots,i_m} \right\rceil \leq 2^{r_1+\cdots+r_m} \left\lceil \mathrm{R} \right\rceil$.

Diese Aussagen sind recht trivial; der Beweis wird nur kurz vollzogen, da die Aussagen der Schritte im späteren Verlauf benötigt werden.

Beweis.
Die Aussagen folgen aus

$$R_{i_1,\ldots,i_m}(x_1,\ldots,x_m) = \sum_{\substack{0\leq j_\mu \leq r_\mu \\ 1\leq \mu \leq m}} \binom{j_1}{i_1} \ldots \binom{j_m}{i_m} c_{j_1,\ldots,j_m} \cdot x_1^{j_1} \ldots x_m^{j_m}, \qquad (9)$$

wobei die Binominalkoeffizienten $\binom{j}{i}$ nach oben beschränkt sind durch:

$$\binom{j}{i} \leq \sum_{0\leq i\leq j} \binom{j}{i} = (1+1)^j \leq 2^r. \qquad (10)$$

Q.e.d.

3.7 Lemma 2

Seien $\alpha \in \mathbb{R}^m,\ s \in \mathbb{N}^m$ und R und T Polynome nach obiger Definition. Dann gilt:

1. $\mathrm{ind}(R_{i_1,\ldots,i_m}) \geq \mathrm{ind}(R) - \sum \frac{i_\mu}{s_\mu}$
2. $\mathrm{ind}(R_1 + R_2) \geq \min\{\mathrm{ind}(R_1), \mathrm{ind}(R_2)\}$
3. $\mathrm{ind}(R \cdot T) = \mathrm{ind}(R) + \mathrm{ind}(T)$

Da der Begriff des *Index* in dieser Arbeit keine größere weitere Anwendung findet und die Aussagen außerdem nach kurzem Durchdenken ebenfalls recht trivial sind, wird auch hier auf einen ausführlichen Beweis verzichtet.

4 Konstruktion des Polynoms R (*Theorem II*)

In diesem Kapitel wird das Polynom R konstruiert, das später im Beweis des *Satzes von Roth* verwendet werden wird. Zum Beweis des *Theorem II* werden drei Lemmata benötigt, von denen das Lemma 3 das zentrale Lemma ist, das am Ende die Bestimmung der Koeffizienten des Polynoms ermöglicht.

4.1 Aussage des *Theorem II*

Sei $\varepsilon > 0$ beliebig, ξ algebraisch irrational, n der Grad von ξ, sei

$$m \in \mathbb{Z}, \text{ sodass } m > 8n^2\varepsilon^{-2} \tag{11}$$

und seien $r_1, \ldots, r_m \in \mathbb{N}$.
Dann existiert ein Polynom R nach Definition in 3.5.1 mit ganzzahligen Koeffizienten und höchstens Grad r_μ in x_μ ($\forall\ 1 \leq \mu \leq m$), für das gilt:

1. R verschwindet nicht
2. $\text{ind}(R) \geq \frac{1}{2}m(1-\varepsilon)$ an der Stelle $(\xi, \ldots, \xi)$ bezüglich $(r_1, \ldots, r_m)$
3. $\left| \mathrm{R} \right| \leq \gamma^{r_1+\cdots+r_m}$ mit $\gamma = 4(a+1)$

mit a aus (4). Hier ist vor allem wichtig, dass diese Aussagen für ein $m >$ eine Konstante abhängig von ξ und ε gelten. Der genaue Wert von γ ist ebenfalls recht irrelevant, er kann von ε, ξ oder m abhängen.

Die folgenden drei Lemmata werden für den Beweis benötigt:

4.2 Lemma 3

Seien $N, M \in \mathbb{N}$ mit $N > M$ und seien

$$L_j(z_1, \ldots, z_N) = \sum_{1 \leq k \leq N} a_{jk} z_k \text{ mit } 1 \leq j \leq M$$

M viele N-Linearformen mit Koeffizienten $a_k \in \mathbb{Z}$ in N vielen Variablen z_k. Sei außerdem $A \in \mathbb{N}$, sodass

$$|a_{jk}| \leq A \quad \forall\ 1 \leq j \leq M, 1 \leq k \leq N$$

Dann besitzt das System $L = (L_1, \ldots, L_M)$ in den Variablen $z_1, \ldots, z_N$ Lösungen in $\mathbb{Z}$, die nicht alle verschwinden und sodass gilt:

$$L_j = 0 \text{ mit } 1 \leq j \leq M \text{ und } |z_i| \leq Z = \left[(NA)^{\frac{M}{N-M}} \right] \text{ mit } 1 \leq k \leq n.$$

Beweis.
Seien N, M, A, Z wie oben beschrieben. Sei $-B_j$ die Summe der negativen und P_j die Summe der positiven Koeffizienten in $L_j(z)$.
Es gilt:

$$NA < (Z+1)^{\frac{N-M}{M}}$$

woraus folgt:

$$NAZ + 1 \leq NA(Z+1) < (Z+1)^{\frac{N}{M}}$$

Für alle N-Tupel $\zeta = (z_1, \ldots, z_N)$ mit

$$0 \leq z_k \leq Z \text{ mit } 1 \leq k \leq N \tag{12}$$

gilt:

$$-B_j Z \leq L_j(z) \leq P_j Z \text{ und } B_j + P_j \leq NA$$

Somit ergeben sich für $L_j(z) \in \mathbb{Z}$ höchstens $NAZ + 1$ viele verschiedene Werte. Es existieren auch höchstens $(Z+1)^N$ viele verschiedene ζ, woraus sich jedoch höchstens $(Z+1)^N > (NAZ+1)^M$ viele verschiedene Systeme L ergeben.
Somit existieren zwei verschiedene M-Tupel ζ_1, ζ_2, sodass gilt:

$$L_j(\zeta_1) = L_j(\zeta_2) \text{ mit } 1 \leq j \leq M.$$

mit $\zeta = \zeta_1 - \zeta_2$ folgt die Behauptung. *Q.e.d.*

4.3 Lemma 4

Sei ξ algebraisch irrational und n dessen Grad. Für alle $l \in \mathbb{N}_0$ existieren Koeffizienten $a_{j,l} \in \mathbb{Z}$ mit $1 \leq j < n$, sodass gilt:

$$\xi^l = a_{n-1,l}\xi^{n-1} + \cdots + a_{0,l}$$

und sind mit a aus (4) folgendermaßen nach oben beschränkt:

$$|a_{a,l}| \leq (a+1)^l$$

Beweis.
Für $l < n$ ist die Aussage offensichtlich. Für $l \geq n$ wird eine kurze Induktion aufgezogen:

Induktionsanfang: $l = n$

Folgt durch Umformung aus $f(x) = 0$ aus 3.2.

Induktionsvoraussetzung:

Angenommen, die Behauptung gilt für ein $l > n$.

Induktionsschritt: $l \Rightarrow l + 1$

Folgt mit Hilfe von

$$\xi^{l+1} = \xi \cdot \xi^l = a_{n-1,l}\xi^n + \cdots + a_{0,l}\xi.$$

Per Induktionsaxiom folgt die Aussage für alle $l \in \mathbb{N}$. *Q.e.d.*

4.4 Lemma 5

Seien $r_1, \ldots, r_m \in \mathbb{N}$ und $0 < \lambda \in \mathbb{R}$. Dann gibt es höchstens

$$\sqrt{2m}\lambda^{-1}(r_1 + 1)\ldots(r_m + 1)$$

viele m-Tupel $(i_1, \ldots, i_m) \in \mathbb{Z}^m$, die die folgende Ungleichung erfüllen:

$$\sum_{\substack{0 \le i_\mu \le r_\mu \\ 1 \le \mu \le m}} \frac{i_\mu}{r_\mu} \le \frac{1}{2}(m - \lambda)$$

Beweis.
Falls $m = 1$, sieht man leicht, dass höchstens $r_1 + 1$ viele Lösungen möglich sind und die Ungleichung sogar unlösbar ist, falls $\lambda > 1$.
Für $\sqrt{2m} > \lambda$ ist das Lemma ebenfalls trivial.
Angenommen, die Aussage gelte für $m - 1$ und seien nun

$$m > 1 \text{ und } \lambda > \sqrt{2m} > 1. \tag{13}$$

Seien $r = r_m$ und $i = i_m$ beliebig, aber fest. Dann beschränkt sich die Anzahl der ganzen Zahlen $i_1, \ldots, i_{m-1}$ auf höchstens

$$\sqrt{2m-2}\left(\lambda - 1 + 2\frac{i}{r}\right)^{-1}(r_1 + 1), \ldots, (r_{m-1} + 1). \tag{14}$$

Man sieht schnell:

$$\begin{aligned}\sum_{0 \le i \le r} \frac{2}{\lambda - 1 + 2\frac{i}{r}} &= \sum_{0 \le i \le r}\left(\frac{1}{\lambda - 1 + 2\frac{i}{r}} + \frac{1}{\lambda + 1 - 2\frac{i}{r}}\right) \\ &= \sum_{0 \le i \le r} \frac{2\lambda}{\lambda^2 - \left(1 - 2\frac{i}{r}\right)^2} < \frac{2(r+1)\lambda}{\lambda^2 - 1}\end{aligned}$$

und durch die Beschränkung aus 14 folgt:

$$\lambda^2 - 1 > \lambda^2(1 - (2m)^{-1}) > \lambda^2\sqrt{1 - m^{-1}}.$$

Für $i = i_m \in (0, \ldots, r = r_m)$ folgt nun die Behauptung. *Q.e.d.*

4.5 Beweis des *Theorem II*

Wie in der Einleitung des Kapitels erwähnt, läuft der Beweis darauf hinaus, das Lemma 3 anzuwenden. Die nötige Vorarbeit wird in erster Linie mit den Lemmata 4 und 5 geleistet.

Beweis(*Theorem II*):
Sei R ein Polynom nach Definition in 3.5.1 und seien $\varepsilon,\ \xi,\ n,\ m$ und $r_1, \ldots, r_m$ wie in 4.1 beschrieben.
Zu zeigen ist, dass die $(r_1 + 1) \ldots (r_m + 1) = N$ vielen Koeffizienten von R existieren.
Dazu soll gelten $\forall\ i_1, \ldots, i_m \in \mathbb{N}$:

$$R_{i_1,\ldots,i_m}(\xi, \ldots, \xi) = 0 \tag{15}$$

sodass (wegen 2) ebenfalls gilt:

$$\sum_{1 \le \mu \le m} \frac{i_\mu}{r_\mu} \le \frac{1}{2} m(1 - \varepsilon) \tag{16}$$

Da das Polynom verschwindet und (15) somit trivial ist, falls $i_\mu > r_\mu$, sei also $i_\mu \le r_\mu$ ($\forall\ 1 \le \mu \le m$).
Lemma 4 erlaubt es, alle Potenzen von ξ als Linearkombinationen von $1, \xi, \ldots, \xi^{n-1}$ zu schreiben. Diese lassen sich als lineares Gleichungssystem mit n Gleichungen in den Variablen $c_{j_1,\ldots,j_m}$ auffassen:

$$L_k = \sum_{\substack{0 \le j_\mu \le r_\mu \\ 1 \le \mu \le m}} a_{k,j_1,\ldots,j_m} c_{j_1,\ldots,j_m} \text{ mit } 1 \le k \le n.$$

Lemma 4 und (9) liefern, dass die Koeffizienten die folgende Form haben:

$$\binom{j_1}{i_1} \ldots \binom{j_m}{i_m} a_{j,l} \text{ mit } 0 \le j < n$$

wobei $l = (j_1 - i_1) + \cdots + (j_m - i_m) \le r_1 + \cdots + r_m$ sei. Wegen (10) und erneut Lemma 4 sind die Koeffizienten betragsmäßig nach oben beschränkt durch:

$$A = (2a + 2)^{r_1 + \cdots + r_m} \tag{17}$$

Das Lemma 5 (mit $\lambda = m\varepsilon$) und (11) liefern, dass die Anzahl M an Gleichungen im System L in N Variablen aus Lemma 3 folgendermaßen beschränkt sind:

$$M \leq n\frac{\sqrt{2m}}{m\varepsilon}N \leq \frac{1}{2}N \tag{18}$$

Dies zeigt 2.
Nun sagt Lemma 3 aus, dass die Koeffizienten $c_{j_1,\ldots,j_m}$ als ganze Zahlen existieren, nicht alle verschwinden (was 1 impliziert) und (15), (16) und die Beschränkung $i_\mu \leq r_\mu$ erfüllen und wegen (17) und (18) betragsmäßig beschränkt sind durch:

$$|c_{j_1,\ldots,j_m}| \leq (NA)^{\frac{M}{N-M}} \leq NA \leq \gamma^{r_1+\cdots+r_m}$$

und mit (10) folgt

$$N = (r_1+1)\ldots(r_m+1) \leq \gamma^{r_1+\cdots+r_m}.$$

Dies zeigt 3; somit gelten alle Aussagen aus *Theorem II*. *Q.e.d.*