

Ein Analogon zu einem SCHNEIDERschen
Satz

(Erste Mitteilung)

VON

KURT MAHLER

Mathematics. — *Ein Analogon zu einem SCHNEIDERSchen Satz.* Von KURT MAHLER. (Erste Mitteilung.) (Communicated by Prof. J. G. VAN DER CORPUT).

(Communicated at the meeting of April 25, 1936).

In einer demnächst erscheinenden Arbeit (die mir der Verfasser liebenswürdigerweise bereits vor der Veröffentlichung zur Verfügung stellte) beweist TH. SCHNEIDER folgenden bemerkenswerten Satz:

Satz 1: *Ist ζ eine algebraische Zahl, μ eine Zahl > 2 und hat die Ungleichung*

$$\left| \frac{p}{q} - \zeta \right| \leq q^{-\mu} \cdot \dots \cdot \dots \cdot \dots \quad (1)$$

unendlichviele verschiedene Lösungen

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \dots \quad (2 \leq q_1 \leq q_2 \leq q_3 \leq \dots) \quad (2)$$

in gekürzten Brüchen mit positivem Nenner, so ist

$$\limsup_{r \rightarrow \infty} \frac{\log q_{r+1}}{\log q_r} = \infty. \quad \dots \cdot \dots \cdot \dots \quad (3)$$

Durch diesen Satz wird ein älteres und weniger weit gehendes Ergebnis von C. SIEGEL ¹⁾ überholt.

Die vorliegende Arbeit gibt einen Beweis für den analogen Satz:

Satz 2: *Ist ζ eine algebraische Zahl, μ eine Zahl > 1 und hat die Ungleichung (1) unendlichviele Lösungen (2) in gekürzten Brüchen mit positiven Nennern, die allein durch endlichviele gegebenen Primzahlen teilbar sind, so gilt (3). (Ein entsprechender Satz, bei dem gefordert wird, dass nicht die Nenner, sondern die Zähler allein durch die endlichvielen gegebenen Primzahlen teilbar sind, folgt hieraus für $\zeta \neq 0$ auf triviale Weise.)*

Spezielle Fälle dieses Satzes stammen bereits von SCHNEIDER. Verlangt man, dass Zähler und Nenner der Lösungen von (1) beschränkte Primteiler haben, so besteht ein weiteres Analogon, diesmal sogar für $\mu > 0$. Dasselbe hat jedoch kein besonderes Interesse, denn es ist möglich, mit

¹⁾ C. SIEGEL, Ueber Näherungswerte algebraischer Zahlen, Math. Ann. **84**, 80—99 (1921).

Hilfe des THUE-SIEGELSchen Satzes ²⁾) folgendes weitergehende Ergebnis zu beweisen:

Satz 3: *Ist ζ eine nichtverschwindende algebraische Zahl, μ eine positive Zahl, so gibt es höchstens endlichviele gekürzte Lösungen p/q von (1), für die pq allein durch endlichviele gegebenen Primzahlen teilbar ist. (Für $\zeta = 0$ stimmt dies nicht.)*

Es möge noch bemerkt werden, dass alle drei Sätze richtig bleiben, wenn man neben der Absolutbetragbewertung noch endlichviele p -adische Bewertungen berücksichtigt, also statt der Ungleichung (1) eine der beiden Ungleichungen

$$\prod_{\tau=1}^t \min \left(1, \left| \frac{p}{q} - \zeta_{\tau} \right|_{P_{\tau}} \right) \leq \max(|p|, |q|)^{-\mu}$$

oder

$$\min \left(1, \left| \frac{p}{q} - \zeta \right| \right) \prod_{\tau=1}^t \min \left(1, \left| \frac{p}{q} - \zeta_{\tau} \right|_{P_{\tau}} \right) \leq \max(|p|, |q|)^{-\mu}$$

betrachtet; dabei bezeichnen P_1, P_2, \dots, P_t endlichviele verschiedene Primzahlen, $\zeta, \zeta_1, \dots, \zeta_t$ je eine reelle, P_1 -adische, \dots, P_t -adische Nullstelle desselben irreduziblen Polynoms mit rationalen Koeffizienten, und $|a|_{P_{\tau}}$ den P_{τ} -adischen Wert der P_{τ} -adischen Zahl a .

Das erste Kapitel bringt den Beweis von Satz 2 und zwar im wesentlichen nach dem Verfahren von SCHNEIDER. Jedoch gelingt es mir, einen Teil seiner Ueberlegungen überflüssig zu machen und so insbesondere Rechnungen zu ersparen. Eine entsprechende Vereinfachung ist auch beim Beweis des SCHNEIDERSchen Satzes 1 möglich; *alsdann kann man insbesondere ohne das Schubfachprinzip auskommen.* (Wie mir Herr SCHNEIDER mitteilte, war ihm ebenfalls bekannt, dass man seinen Satz 1 ohne Verwendung des Schubfachprinzips zeigen kann; aus seiner Mitteilung konnte ich jedoch nicht ersehen, ob er damit dieselbe Beweisänderung wie bei mir im Auge hatte.) — Im zweiten Kapitel wird Satz 3 mittels einer SIEGELSchen Methode abgeleitet. Es schliesst mit zwei Bemerkungen über die Kettenbruch-Näherungsbrüche einer algebraischen Irrationalzahl.

KAPITEL 1.

Beweis von Satz 2.

§ 1. Die Existenzannahme.

Um Satz 2 zu beweisen, wird indirekt geschlossen und angenommen, der Satz sei falsch.

Es gebe somit eine unendliche Folge

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \dots \quad (2 \leq q_1 < q_2 < q_3 < \dots) \quad \dots \quad (4)$$

²⁾ Siehe etwa: C. SIEGEL, Approximation algebraischer Zahlen, Math. Zeitschr. 10, 173–213 (1921).

§ 3. Konstruktion von Lösungssystemen.

Seien $k > 1$ und r_k zwei natürliche Zahlen, über die später verfügt wird; sei ferner $N = (k - 1) T + 1$.

Zu jeder natürlichen Zahl s , die grösser als eine von k und r_k abhängige Schranke ist, kann man nach § 1 ein System $S(s, r_k)$ von N Elementen

$$\frac{p(l; s, r_k)}{q(l; s, r_k)} = \frac{p_\nu}{q_\nu}, \quad \nu = \nu(l; s, r_k) \quad (l=0, 1, \dots, N-1)$$

der Folge (4) mit

$$s r_k^{-3^l} \leq \log q(l; s, r_k) < c s r_k^{-3^l} \quad (8)$$

und also erst recht mit

$$\frac{1}{c} r_k^{3^{l''} - 3^{l'}} \leq \frac{\log q(l'; s, r_k)}{\log q(l''; s, r_k)} \leq c r_k^{3^{l''} - 3^{l'}} \quad (l', l'' = 0, 1, \dots, N-1) \quad . (9)$$

finden. Die Glieder dieses Systems verteilen sich auf die T Klassen C_1, C_2, \dots, C_T ; wegen $N > (k - 1) T$ müssen folglich gewisse k von ihnen, etwa

$$\frac{p(l_\alpha; s, r_k)}{q(l_\alpha; s, r_k)} \quad (\alpha = 1, 2, \dots, k)$$

mit den Indizes

$$l_\alpha = l_\alpha(s, r_k) \quad (0 \leq l_k < l_{k-1} < \dots < l_2 < l_1 \leq N-1)$$

in ein und derselben Klasse $C = C(s, r_k)$ liegen. Jedem System $S(s, r_k)$ werden auf diese Weise $k + 1$ Symbole

$$C(s, r_k), l_1(s, r_k), l_2(s, r_k), \dots, l_k(s, r_k)$$

zugeordnet. Die Gesamtheit dieser Symbole hat aber nur höchstens $N^k T$ Möglichkeiten. Also existiert eine unendliche Folge \mathfrak{F}^* :

$$s = s^{(1)}, s^{(2)}, s^{(3)}, \dots \quad (s^{(1)} < s^{(2)} < s^{(3)} < \dots)$$

von Zahlwerten für s , für die

$$C(s, r_k) = C(a_1, a_2, \dots, a_t), \quad l_1(s, r_k) = l_1, \quad l_2(s, r_k) = l_2, \dots, \quad l_k(s, r_k) = l_k \quad . (10)$$

wird, wo jetzt a_1, a_2, \dots, a_t und l_1, l_2, \dots, l_k nicht mehr von s abhängen. Aus \mathfrak{F}^* denken wir eine unendliche Teilfolge \mathfrak{F} :

$$s = s_1, s_2, s_3, \dots \quad (s_1 < s_2 < s_3 < \dots)$$

von s -Werten ausgewählt, so dass die k Grenzwerte

$$\lim_{\substack{s \rightarrow \infty \\ s \text{ in } \mathfrak{F}}} r_k \frac{\log q(l_k; s, r_k)}{\log q(l_\alpha; s, r_k)} = r_\alpha \quad (\alpha = 1, 2, \dots, k) \quad . . (11)$$

existieren; dies ist möglich auf Grund der Ungleichungen (9).

Die so bestimmten Grenzwerte genügen wegen (9) den Ungleichungen

$$\frac{1}{c} \leq \frac{1}{c} r_k^{3^{l'_z} - 3^{l_k + 1}} \leq r_z \leq c r_k^{3^{l'_z} - 3^{l_k + 1}} \quad (z = 1, 2, \dots, k).$$

Da $3^{l'_k} \geq 1$, ferner nach Voraussetzung $l_z > l_{z+1}$, also $l_{z+1} + 1 \leq l_z$ und somit

$$3^{l'_z} - 3^{l_k} + 1 \geq 3(3^{l'_z + 1} - 3^{l_k} + 1) \quad (z = 1, 2, \dots, k - 1)$$

ist, so folgt

$$r_z \geq \frac{1}{c} r_k^{3^{l'_z} - 3^{l_k + 1}} \geq \frac{1}{c} r_k^{3(3^{l'_z + 1} - 3^{l_k + 1})} \geq \frac{1}{c} \left(\frac{r_{z+1}}{c} \right)^3 \geq \frac{(r_{z+1} + 1)^3}{c^4 (c + 1)^3}.$$

Also gelten die Ungleichungen

$$r_1 \geq (r_2 + 1)^2, \quad r_2 \geq (r_3 + 1)^2, \dots, \quad r_{k-2} \geq (r_{k-1} + 1)^2, \quad r_{k-1} \geq \frac{k-1}{\varepsilon} (r_k + 1) \quad (12)$$

und erst recht deren Folgerungen

$$r_z \geq \frac{k-1}{\varepsilon} \prod_{\lambda=z+1}^k (r_\lambda + 1) \quad (z = 1, 2, \dots, k-1), \quad . \quad (13)$$

sobald r_k grösser als eine gewisse von c , k und ε abhängige natürliche Zahl c_1 ist. Dies werde von jetzt ab vorausgesetzt. Wir wollen ferner annehmen, dass $\varepsilon \leq 1/2$ ist; dann gilt nach (11) für alle genügend grossen Elemente s der Folge \mathfrak{F} :

$$\frac{r_z}{1 + \varepsilon} \leq r_k \frac{\log q(l_k; s, r_k)}{\log q(l_z; s, r_k)} \leq \frac{r_z}{1 - \varepsilon} \quad (z = 1, 2, \dots, k). \quad (14)$$

§ 4. Bestimmung oberer Schranken für zwei Ausdrücke A und M .

Bedeute A das Maximum aller Ausdrücke der Gestalt

$$\prod_{z=1}^{k-1} \left| \frac{p(l_z; s, r_k)}{q(l_z; s, r_k)} - \zeta \right|^{h_z - \tau_z} \cdot \left| \frac{p(l_k; s, r_k)}{q(l_k; s, r_k)} - \zeta \right|^{h_k},$$

wo $h_1, h_2, \dots, h_k, \tau_1, \tau_2, \dots, \tau_{k-1}$ alle ganzen rationalen Zahlen mit

$$h_1 \geq 0, \quad h_2 \geq 0, \dots, \quad h_k \geq 0, \quad \sum_{z=1}^k \frac{h_z}{r_z} \geq 1 - \varepsilon,$$

$$0 \leq \tau_z \leq h_z, \quad 0 \leq \tau_z \leq \prod_{\lambda=z+1}^k (r_\lambda + 1) \quad (z = 1, 2, \dots, k-1)$$

durchlaufen. Wegen

$$\left| \frac{p(l_z; s, r_k)}{q(l_z; s, r_k)} - \zeta \right| \leq q(l_z; s, r_k)^{-\mu} \quad (z = 1, 2, \dots, k)$$

ist A offenbar nicht grösser als das Maximum der Potenzprodukte

$$\prod_{z=1}^{k-1} q(l_z; s, r_k)^{-(h_z - \tau_z)\mu} \cdot q(l_k; s, r_k)^{-h_k\mu}.$$

Aus (14) folgt somit

$$A \leq \left\{ q(l_k; s, r_k)^{(1-\varepsilon) \sum_{z=1}^{k-1} \frac{h_z - \tau_z}{r_z} + \frac{h_k}{r_k}} \right\}^{-r_k\mu} \leq q(l_k; s, r_k)^{-(1-\varepsilon)r_k\mu} \left\{ \sum_{z=1}^{k-1} \frac{h_z - \tau_z}{r_z} + \frac{h_k}{r_k} \right\},$$

und da nach (13)

$$\tau_z \leq \frac{\varepsilon}{k-1} r_z, \quad \sum_{z=1}^{k-1} \frac{\tau_z}{r_z} \leq \varepsilon, \quad \sum_{z=1}^{k-1} \frac{h_z - \tau_z}{r_z} + \frac{h_k}{r_k} \geq (1-\varepsilon) - \varepsilon = 1 - 2\varepsilon$$

ist, so ergibt sich die Schranke

$$A \leq q(l_k; s, r_k)^{-(1-\varepsilon)(1-2\varepsilon)r_k\mu} \dots \dots \dots (15)$$

Sei weiter M das kleinste gemeinschaftliche Vielfache der Zahlen

$$\prod_{z=1}^k q(l_z; s, r_k)^{h_z},$$

wo die Indizes h_1, h_2, \dots, h_k alle ganzen rationalen Werte mit

$$h_1 \geq 0, h_2 \geq 0, \dots, h_k \geq 0, \quad \sum_{z=1}^k \frac{h_z}{r_z} \leq 1$$

durchlaufen. Nach Voraussetzung ist jede der Zahlen

$$q(l_z; s, r_k) \quad (z = 1, 2, \dots, k)$$

allein durch die Primzahlen P_1, P_2, \dots, P_t teilbar; da die Brüche

$$\frac{p(l_z; s, r_k)}{q(l_z; s, r_k)} \quad (z = 1, 2, \dots, k)$$

aber nach der Konstruktion in § 3 sämtlich zur Klasse $C(a_1, a_2, \dots, a_t)$ gehören, so kann nach (6) die höchste in $q(l_z; s, r_k)$ aufgehende Potenz von P_τ nicht grösser als

$$q(l_z; s, r_k)^{\frac{a_\tau}{f}}$$

sein. Wegen (14) ist demnach die höchste Potenz von P_τ , durch die M teilbar ist, höchstens gleich

$$\prod_{z=1}^k q(l_z; s, r_k)^{\frac{a_\tau}{f} h_z} \leq q(l_k; s, r_k)^{\frac{a_\tau}{f} (1+\varepsilon)r_k} \sum_{z=1}^k \frac{h_z}{r_z} \leq q(l_k; s, r_k)^{\frac{a_\tau}{f} (1+\varepsilon)r_k},$$

und da auch M keine anderen Primteiler als P_1, P_2, \dots, P_t haben kann, so ergibt sich wegen (7) die obere Schranke

$$M \leq \prod_{\tau=1}^t q(l_k; s, r_k)^{\frac{a_\tau}{f} (1+\varepsilon)r_k} \leq q(l_k; s, r_k)^{(1+\varepsilon)^2 r_k} \dots \dots \dots (16)$$

§ 5. Ein Hilfssatz über Gitterpunkte.

Seien r_1, r_2, \dots, r_k die in § 3 konstruierten positiven Zahlen. Wir verstehen unter n den Grad der untersuchten algebraischen Zahl ζ und setzen von jetzt ab ausser der Ungleichung $r_k \geq c_1$ noch voraus, dass

$$k \geq \frac{\log \frac{1}{2n}}{\log \left(1 - \frac{\varepsilon}{2}\right)}, \quad r_k \geq \frac{k}{2\varepsilon}, \quad \dots \quad (17)$$

wegen (12) also

$$r_\nu \geq \frac{k}{2\varepsilon} \text{ für } \nu = 1, 2, \dots, k \text{ und folglich } \sum_{\nu=1}^k \frac{1}{r_\nu} \leq \frac{\varepsilon}{2} \quad (18)$$

ist.

Sei $M(v)$ für beliebiges positives v die Menge aller Punkte (x_1, x_2, \dots, x_k) im k -dimensionalen Raum, die den Ungleichungen

$$x_1 \geq 0, x_2 \geq 0, \dots, x_k \geq 0, \quad \sum_{\nu=1}^k \frac{x_\nu}{r_\nu} \leq v$$

genügen, $J(v)$ der Rauminhalt von $M(v)$ und $G(v)$ die Anzahl der Gitterpunkte im Innern oder auf dem Rande von $M(v)$. Ordnet man jedem solchen Gitterpunkte (h_1, h_2, \dots, h_k) den Einheitswürfel

$$h_1 \leq x_1 \leq h_1 + 1, \quad h_2 \leq x_2 \leq h_2 + 1, \quad \dots, \quad h_k \leq x_k \leq h_k + 1$$

zu, so erfüllen diese Würfel zusammen ein Raumstück, dessen Inhalt gerade gleich $G(v)$ ist. Dieses Raumstück enthält offenbar alle Punkte von $M(v)$ und ist seinerseits ganz in $M\left(v + \sum_{\nu=1}^k \frac{1}{r_\nu}\right)$ enthalten; folglich ist

$$J(v) \leq G(v) \leq J\left(v + \sum_{\nu=1}^k \frac{1}{r_\nu}\right).$$

Nach einer bekannten Integralformel ist ferner

$$J(v) = \frac{r_1 r_2 \dots r_k}{k!} v^k,$$

und somit gelten die Ungleichungen

$$\frac{r_1 r_2 \dots r_k}{k!} v^k \leq G(v) \leq \frac{r_1 r_2 \dots r_k}{k!} \left(v + \sum_{\nu=1}^k \frac{1}{r_\nu}\right)^k.$$

Hieraus folgt speziell wegen (18)

$$G(1-\varepsilon) \leq \frac{r_1 r_2 \dots r_k}{k!} \left(1 - \varepsilon + \frac{\varepsilon}{2}\right)^k \leq \frac{r_1 r_2 \dots r_k}{k!} \frac{1}{2n} \text{ und } G(1) \geq \frac{r_1 r_2 \dots r_k}{k!}$$

und damit schliesslich: ³⁾

$$G(1 - \varepsilon) < \frac{G(1)}{n} \dots \dots \dots (19)$$

§ 6. Konstruktion des Näherungspolynoms.

Die algebraische Zahl ζ , die wir untersuchen, sei Nullstelle des Polynoms n -ten Grades mit rationalen Koeffizienten

$$f(z) = z^n + f_1 z^{n-1} + \dots + f_{n-1} z + f_n.$$

Damit ein Polynom $F(z)$ durch $f(z)$ teilbar ist, müssen seine Koeffizienten offenbar gewissen n homogenen linearen Gleichungen mit rationalen Zahlkoeffizienten genügen.

Sei nun $R(z_1, z_2, \dots, z_k)$ ein Polynom in k Unbestimmten z_1, z_2, \dots, z_k von der speziellen Gestalt

$$R(z_1, z_2, \dots, z_k) = \left. \begin{array}{l} \sum_{h_1 \geq 0} \dots \sum_{h_k \geq 0} R_{h_1 h_2 \dots h_k} z_1^{h_1} z_2^{h_2} \dots z_k^{h_k}, \\ \sum_{z=1}^k \frac{h_z}{r_z} \leq 1 \end{array} \right\} \dots \dots (20)$$

und sei zur Abkürzung

$$R_{\lambda_1 \lambda_2 \dots \lambda_k}(z_1, z_2, \dots, z_k) = \frac{\partial^{\lambda_1 + \lambda_2 + \dots + \lambda_k} R(z_1, z_2, \dots, z_k)}{\lambda_1! \lambda_2! \dots \lambda_k! \partial z_1^{\lambda_1} \partial z_2^{\lambda_2} \dots \partial z_k^{\lambda_k}}.$$

Damit die $G(1 - \varepsilon)$ Polynome

$$R_{\lambda_1 \lambda_2 \dots \lambda_k}(z, z, \dots, z) \text{ mit } \lambda_1 \geq 0, \lambda_2 \geq 0, \dots, \lambda_k \geq 0, \sum_{z=1}^k \frac{\lambda_z}{r_z} \leq 1 - \varepsilon \quad (21)$$

sämtlich durch $f(z)$ teilbar sind, müssen die $G(1)$ Koeffizienten $R_{h_1 h_2 \dots h_k}$ von $R(z_1, z_2, \dots, z_k)$ nach der vorigen Bemerkung $n \cdot G(1 - \varepsilon)$, wegen (19) also weniger als $G(1)$ homogenen linearen Gleichungen mit rationalen Zahlkoeffizienten genügen. Diese Gleichungen lassen sich daher durch ganze rationale Werte für die $R_{h_1 h_2 \dots h_k}$, die nicht alle Null sind, befriedigen und es folgt damit die Existenz eines Polynoms (20), das nicht identisch verschwindet, dessen Koeffizienten ganz rational sind und für das die zugeordneten Polynome (21) sämtlich durch $f(z)$ teilbar sind.

Schluss des Beweises in der 2. Mitteilung.

³⁾ SCHNEIDER benutzt beim Beweis von Satz 1 einen tieferen Hilfssatz über Gitterpunkte im Innern eines Würfelteils. Will man aber, wie hier, allein Satz 2 zeigen, so leistet der elementarere Satz des Textes alles Gewünschte; doch kann man natürlich auch alle Ueberlegungen auf den SCHNEIDERSchen Hilfssatz stützen.