ACTA ARITHMETICA
XXI (1972)

# Algebraische Abhängigkeit von Wurzeln

von

Carl Ludwig Siegel (Göttingen)

*Waclaw Sierpiński zum Gedächtnis*

**1.** Es sei ein reeller Körper $\Re$ gegeben. Zwei von 0 verschiedene reelle Zahlen mögen äquivalent heissen, wenn ihr Verhältnis zu $\Re$ gehört. Hierdurch wird für jede reelle Zahl $\alpha \neq 0$ eine Klasse $[\alpha]$ erklärt, und diese Klassen bilden eine multiplikative Abelsche Gruppe mit dem Einheitselement [1]. Weiterhin sind von dieser Gruppe nur solche Untergruppen $\Gamma$ zu betrachten, deren Ordnung $N$ endlich ist. Bedeutet $[\varrho]$ ein beliebiges Element von $\Gamma$, so ist dann

$$[\varrho^N] = [\varrho]^N = [1],$$

also $\varrho$ eine reelle $N$-te Wurzel aus einer Zahl von $\Re$. Geht man umgekehrt von endlich vielen reellen Wurzeln

$$\varrho_k = \sqrt[n_k]{m_k} \neq 0 \qquad (k = 1, \ldots, h) \tag{1}$$

mit Radikanden in $\Re$ und natürlichen $n_k$ aus, so erzeugen die $h$ Klassen $[\varrho_k]$ bei Multiplikation eine Gruppe $\Gamma$ der betrachteten Art, die genauer mit $\Gamma(\varrho_1, \ldots, \varrho_h) = \Gamma_h$ bezeichnet werde. Unter $\Gamma_0$ sei die aus [1] allein bestehende Gruppe verstanden.

Ausserdem wird die durch Adjunktion von $\varrho_1, \ldots, \varrho_h$ zu $\Re$ entstehende algebraische Erweiterung $\Re(\varrho_1, \ldots, \varrho_h) = \Re_h$ von $\Re = \Re_0$ eingeführt. Es bietet sich die Aufgabe, für den Körper $\Re_h$ den Grad in bezug auf $\Re$ zu bestimmen und eine Basis aufzustellen. Dieses Problem ist von Besicovitch [1] unter speziellen Voraussetzungen gelöst worden. Dabei ist nämlich $\Re$ der rationale Zahlkörper und $m_k = a_k p_k$ $(k = 1, \ldots, h)$, worin $p_1, \ldots, p_h$ voneinander verschiedene Primzahlen und $a_1, \ldots, a_h$ durch keine dieser Primzahlen teilbare natürliche Zahlen bedeuten. Für diesen Fall zeigte Besicovitch, daß der algebraische Zahlkörper $\Re_h$ den Grad $n_1 \ldots n_h$ besitzt und folglich die Potenzprodukte $\varrho_1^{l_1} \ldots \varrho_h^{l_h}$ $(l_k = 0, 1, \ldots, n_k - 1;\ k = 1, \ldots, h)$ eine Basis von $\Re_h$ bilden.

Es hat sich nun herausgestellt, daß der von Besicovitch verwendete Gedankengang auch zur Lösung des allgemeinen Problems führt, wobei sogar einige Schlüsse noch einfacher und durchsichtiger erscheinen. Offenbar genügt es, für die aufeinander folgenden Erweiterungen $\Re(\varrho_1, \ldots, \varrho_k) = \Re_k = \Re_{k-1}(\varrho_k)$ $(k = 1, \ldots, h)$ von $\Re$ die Relativgrade $(\Re_k, \Re_{k-1})$ zu untersuchen. Die Lösung des gestellten Problems ergibt sich sodann aus folgender Aussage, durch welche die obige Einführung der Gruppe $\Gamma(\varrho_1, \ldots, \varrho_h)$ erst einen Nutzen bekommt.

Satz. *Der Grad von $\Re_h$ in bezug auf $\Re_{h-1}$ ist gleich dem Index $j$ von $\Gamma_{h-1}$ in $\Gamma_h$, und die Potenzen $\varrho_h^l$ $(l = 0, 1, \ldots, j-1)$ bilden eine Basis von $\Re_h$ in bezug auf $\Re_{h-1}$.*

Beweis. Da die Faktorgruppe $\Gamma_h/\Gamma_{h-1}$ durch $[\varrho_h]\Gamma_{h-1}$ erzeugt wird, so ist $[\varrho_h]^j$ die kleinste in $\Gamma_{h-1}$ gelegene Potenz von $[\varrho_h]$ und insbesondere $\varrho_h^j$ eine Zahl von $\Re_{h-1}$, also $\varrho_h$ Nullstelle des Polynoms

$$P_h = x^j - \varrho_h^j,$$

dessen Koeffizienten zu $\Re_{h-1}$ gehören. Bedeutet $n$ den Grad von $\Re_h$ in bezug auf $\Re_{h-1}$, so ist andererseits $\varrho_h$ Nullstelle eines in $\Re_{h-1}$ irreduziblen Polynoms

$$Q_h = x^n + \ldots + \lambda$$

mit Koeffizienten aus $\Re_{h-1}$, und es ist dann $Q_h$ ein Faktor von $P_h$, also

$$n \leqslant j. \tag{2}$$

Die sämtlichen Nullstellen von $P_h$ gehen aus $\varrho_h$ durch Multiplikation mit den $j$-ten Einheitswurzeln hervor. Demnach ist auch die Zahl $\lambda\varrho_h^{-n}$ eine Einheitswurzel, die aber 1 oder $-1$ sein muß, da $\lambda$ und $\varrho_h$ beide reell sind. Hieraus ersieht man, daß bereits die Potenz $\varrho_h^n$ in $\Re_{h-1}$ liegt. Im Falle $h = 1$ folgt nun aus (2) wegen der Minimaleigenschaft von $j$, daß $n = j$ ist, womit die Behauptung für $h = 1$ bewiesen ist. Es kann jetzt angenommen werden, daß $h > 1$ ist und der Satz für $h-1$ statt $h$ gilt.

Zur Abkürzung werde $(n, j) = d$ und $\varrho_{h-1} = \varrho$ gesetzt sowie der Index von $\Gamma_{h-2}$ in $\Gamma_{h-1}$ mit $m$ bezeichnet. Wegen der Induktionsannahme ist dann das Polynom $x^m - \varrho^m$ in $\Re_{h-2}$ irreduzibel, und für jede Zahl $\nu$ aus $\Re_{h-1}$ gilt eine Darstellung

$$\nu = \beta_1\varrho^{m-1} + \ldots + \beta_m \tag{3}$$

mit Koeffizienten $\beta_1, \ldots, \beta_m$ aus $\Re_{h-2}$. Bedeutet $S(\nu)$ die in bezug auf $\Re_{h-2}$ genommene Spur von $\nu$, so ist insbesondere

$$S(\varrho^q) = 0 \quad (q = 1, \ldots, m-1);$$



dies ergibt sich aus den Newtonschen Formeln für die Potenzsummen der Nullstellen eines Polynoms, oder auch unter Benutzung der Tatsache, daß aus $\varrho$ alle Konjugierten durch Multiplikation mit den $m$-ten Einheitswurzeln entstehen. Daher wird

$$S(\nu) = \beta_1 S(\varrho^{m-1}) + \ldots + \beta_m S(1) = m\beta_m. \tag{4}$$

Zum noch ausstehenden Nachweis der Behauptung $n = j$ werden die Zahlen

$$\tau_0 = \varrho_h^d, \qquad \tau_f = \tau_0\varrho^f \qquad (f = 1, \ldots, m) \tag{5}$$

gebildet. Da beide Potenzen $\varrho_h^n$ und $\varrho_h^j$ zu $\Re_{h-1}$ gehören, so gilt das auch für $\tau_0$, und es wird demnach

$$\tau_0 = \gamma_1\varrho^{m-1} + \ldots + \gamma_m \tag{6}$$

mit gewissen $\gamma_1, \ldots, \gamma_m$ aus $\Re_{h-2}$. Benutzt man dann (3), (4) für $\nu = \tau_f$ und beachtet dabei, daß $\varrho^m$ zu $\Re_{h-2}$ gehört, so folgt

$$S(\tau_f) = m\gamma_f\varrho^m. \tag{7}$$

Bei gegebenem $f$ der Reihe 1 bis $m$ sei $w_f = w$ der Grad von $\tau_f = \tau$ in bezug auf $\Re_{h-2}$. Unter den $m$ Konjugierten der Zahl $\tau$ aus $\Re_{h-1}$ treten dann also genau $w$ voneinander verschiedene Grössen auf, jede davon gleich oft. Nach (5) ist $\tau$ Wurzel aus einer Zahl von $\Re$, so daß man die Induktionsannahme auf die $h-1$ Wurzeln $\varrho_1, \ldots, \varrho_{h-2}, \tau$ anwenden kann. Daher ist die Potenz $[\tau]^w$ ein Element von $\Gamma_{h-2}$ und das Polynom $x^w - \tau^w$ in $\Re_{h-2}$ irreduzibel. Wenn nun $w > 1$ ist, so wird die Summe aller $w$ verschiedenen Konjugierten von $\tau$ gleich 0, also auch $S(\tau_f) = 0$, und (7) ergibt $\gamma_f = 0$. Nach (1), (5), (6) sind aber die $m$ Koeffizienten $\gamma_1, \ldots, \gamma_m$ nicht alle 0. Bei geeigneter Wahl von $f$ ist daher $w_f = 1$. Dann ist $[\tau_f]$ selber ein Element von $\Gamma_{h-2}$; folglich erweist sich nach (5) die Potenz $[\varrho_h]^d$ als ein Element von $\Gamma_{h-1}$. Wegen der Minimaleigenschaft von $j$ gilt jedoch

$$j \leqslant d = (n, j) \leqslant n,$$

wodurch mit (2) der Beweis beendet ist.

Wird der Index von $\Gamma_{k-1}$ in $\Gamma_k$ mit $j_k$ $(k = 1, \ldots, h)$ bezeichnet, so ergibt sich aus dem Satze unmittelbar, daß der gesuchte Grad von $\Re(\varrho_1, \ldots, \varrho_h)$ in bezug auf $\Re$ gleich der Ordnung

$$N = j_1 \cdots j_h$$

der Gruppe $\Gamma(\varrho_1, \ldots, \varrho_h)$ ist und die Potenzprodukte $\varrho_1^{l_1} \ldots \varrho_h^{l_h}$ $(l_k = 0, 1, \ldots, j_k - 1;\ k = 1, \ldots, h)$ eine Basis bilden(1). Demnach sind irgend welche Potenzprodukte von $\varrho_1, \ldots, \varrho_h$ genau dann in bezug auf $\mathfrak{R}$ linear unabhängig, wenn sie es bereits paarweise sind.

**2.** Anschliessend an das Ergebnis des vorangehenden Abschnitts bieten sich eine zweite und dritte Aufgabe: Man bestimme alle in $\mathfrak{R}_h$ gelegenen von 0 verschiedenen Wurzeln aus Zahlen von $\mathfrak{R}$, also alle in $\mathfrak{R}_h$ gelegenen Zahlen $\sigma$ von der Art, daß eine der Potenzen $\sigma^l$ $(l = 1, 2, \ldots)$ mit 1 äquivalent ist; man bestimme sodann sämtliche Systeme $\sigma_1, \ldots, \sigma_t$ aus endlich vielen solcher Wurzeln, für welche die Potenzprodukte $\sigma_1^{l_1} \ldots \sigma_t^{l_t}$ $(l_r = 0, 1, \ldots, u_r - 1;\ r = 1, \ldots, t)$ bei geeigneter Wahl der natürlichen Zahlen $u_1, \ldots, u_t$ eine Basis von $\mathfrak{R}_h$ in bezug auf $\mathfrak{R}$ bilden.

Eine Lösung des zweiten Problems ergibt sich unmittelbar durch Anwendung des Satzes auf die $h+1$ Wurzeln $\varrho_1, \ldots, \varrho_h, \sigma$. Da nach Voraussetzung $\sigma$ in $\mathfrak{R}_h$ liegen soll, so ist die Klasse $[\sigma]$ nach dem Satze ein Element von $\Gamma_h$, also

$$\sigma = b\varrho^{g_1} \ldots \varrho_h^{g_h} \tag{8}$$

mit gewissen Exponenten $g_k$ der Reihe 0 bis $j_k - 1$ $(k = 1, \ldots, h)$ und einem von 0 verschiedenen Faktor $b$ aus $\mathfrak{R}$. Es ist trivial, daß umgekehrt durch (8), bei beliebigen ganzen rationalen Exponenten und irgend einer Zahl $b \neq 0$ aus $\mathfrak{R}$, stets eine in $\mathfrak{R}_h$ gelegene Wurzel aus einer Zahl des Grundkörpers $\mathfrak{R}$ gegeben wird. Das hiermit gewonnene Resultat lässt sich in der folgenden prägnanten Weise ausdrücken: Ist $\omega$ eine homogene lineare Verbindung der Potenzprodukte $\varrho_1^{g_1} \ldots \varrho_h^{g_h}$ $(g_k = 0, 1, \ldots, j_k - 1;\ k = 1, \ldots, h)$, mit Koeffizienten aus $\mathfrak{R}$, von denen mindestens zwei von 0 verschieden sind, so ist keine der Potenzen $\omega^l$ $(l = 1, 2, \ldots)$ in $\mathfrak{R}$ gelegen.

In $\mathfrak{R}_h$ seien nun endlich viele von 0 verschiedene Wurzeln $\sigma_1, \ldots, \sigma_t$ gegeben, für welche bei geeignet gewählten natürlichen Zahlen $u_1, \ldots, u_t$ die Potenzprodukte $\sigma_1^{l_1} \ldots \sigma_t^{l_t}$ $(l_r = 0, 1, \ldots, u_r - 1;\ r = 1, \ldots, t)$ eine Basis von $\mathfrak{R}_h$ in bezug auf $\mathfrak{R}$ bilden. Dann muss jedenfalls die Anzahl $u_1 \ldots u_t$ gleich dem Körpergrade sein, also $u_1 \ldots u_t = N$, und andererseits sind erst recht keine zwei dieser Potenzprodukte äquivalent. Daher sind auch die $N$ Klassen $[\sigma_1]^{l_1} \ldots [\sigma_t]^{l_t}$ sämtlich voneinander verschieden.

(1) Nach Einreichung des Manuskriptes bei der Redaktion erfuhr ich durch eine freundliche Mitteilung von A. Schinzel, daß dieses Resultat für den speziellen Fall $N = n_1 \ldots n_h$ bereits von L. J. Mordell bewiesen wurde (*On the linear independence of algebraic numbers*, Pacific J. Math. 3 (1953), S. 625–630). Mordell benutzte dabei ebenfalls die Schlußweise von Besicovitch und wies ausserdem darauf hin, daß der Beweis auch noch unter der Annahme eines komplexen Grundkörpers gültig bleibt, wenn dieser alle $n_k$-ten Einheitswurzeln $(k = 1, \ldots, h)$ enthält. Eine entsprechende Erweiterung liesse sich dann übrigens ohne Änderung des Gedankenganges in der vorliegenden allgemeineren Überlegung durchführen.



Auf Grund des obigen Resultats gehören sie aber alle der Gruppe $\Gamma_h$ der Ordnung $N$ an und sind folglich die Elemente dieser Gruppe, jedes genau einmal. Nach dem tiefliegenden Ergebnis von Hajós [2] existiert dann eine Permutation $q_1, \ldots, q_t$ der Zahlen $1, \ldots, t$ von folgender Art: Versteht man unter $\Delta_r$ $(r = 1, \ldots, t)$ die durch $[\sigma_{q_1}], \ldots, [\sigma_{q_r}]$ erzeugte Untergruppe von $\Gamma_h$, wobei $\Delta_t = \Gamma_h$ ist, und setzt noch $\Delta_0 = \Gamma_0$, so ist $u_{q_r}$ der Index von $\Delta_{r-1}$ in $\Delta_r$. Wenn nun durch Abänderung der Numerierung anstelle von $q_r$ wieder $r$ eingeführt wird, so ist also zufolge des Satzes der Index $u_r$ gleich dem Grade von $\mathfrak{R}(\sigma_1, \ldots, \sigma_r)$ in bezug auf $\mathfrak{R}(\sigma_1, \ldots, \sigma_{r-1})$.

Die Umkehrung des Gedankenganges liefert die volle Lösung des dritten Problems. Aus den $N$ Potenzprodukten $\varrho_1^{l_1} \ldots \varrho_h^{l_h}$ $(l_k = 0, 1, \ldots, j_k - 1;\ k = 1, \ldots, h)$ wähle man irgend welche Zahlen $\eta_1, \ldots, \eta_t$, deren Adjunktion zu $\mathfrak{R}$ den gesamten Körper $\mathfrak{R}_h$ liefert, und verstehe unter $u_r$ den Index der Gruppe $\Gamma(\eta_1, \ldots, \eta_{r-1})$ in $\Gamma(\eta_1, \ldots, \eta_r)$. Indem man die $\eta_r$ mit beliebigen Zahlen $b_r \neq 0$ aus $\mathfrak{R}$ multipliziert und noch irgend eine Permutation der $t$ Produkte $b_r\eta_r$ $(r = 1, \ldots, t)$ vornimmt, bekommt man alle Systeme von Wurzeln $\sigma_1, \ldots, \sigma_t$ der gewünschten Art.

**3.** Wenn $\mathfrak{R}$ der rationale Zahlkörper ist, so lassen sich mittels des Satzes die einzelnen Relativgrade $(\mathfrak{R}_k, \mathfrak{R}_{k-1})$ für $k = 1, \ldots, h$ leicht aus der Zerlegung der Radikanden $m_1, \ldots, m_h$ in Primfaktoren bestimmen. Diese Zerlegung sei

$$m_k = \pm p_1^{s_{k1}} \ldots p_g^{s_{kg}} \qquad (k = 1, \ldots, h),$$

worin $p_1, \ldots, p_g$ voneinander verschiedene natürliche Primzahlen und die Exponenten ganze rationale Zahlen bedeuten. Es wird genau dann

$$[\varrho_1]^{l_1} \ldots [\varrho_k]^{l_k} = [1],$$

wenn die ganzen rationalen Exponenten $l_1, \ldots, l_k$ den $g$ Kongruenzen

$$\sum_{v=1}^{k} \frac{s_{vw}}{n_v} l_v \equiv 0 \pmod 1 \qquad (w = 1, \ldots, g) \tag{9}$$

genügen. Zur Bestimmung von $j_k$ braucht man nur die endlich vielen Lösungen von (9) zu untersuchen, die sich durch Probieren der Wertsysteme

$$l_v = 0, 1, \ldots, n_v - 1 \ (v = 1, \ldots, k-1), \qquad l_k = 1, 2, \ldots, n_k \tag{10}$$

ergeben. Unter diesen befindet sich die triviale Lösung $l_v = 0$, $l_k = n_k$, und jede Lösung mit kleinstem positiven $l_k$ ergibt $l_k = j_k$. Insbesondere ist genau dann $j_k = n_k$, für alle $k = 1, \ldots, h$, und daher der Körpergrad $(\mathfrak{R}_h, \mathfrak{R}) = n_1 \ldots n_h$, wenn (9), (10) im Falle $k = h$ nur die triviale Lösung

$l_1 = 0, \ldots, l_{h-1} = 0$, $l_h = n_h$ besitzen. Ein Beispiel liefert hierfür der von Besicovitch behandelte Fall $m_k = a_k p_k$ $(k = 1, \ldots, h)$, wobei

$$h \leqslant g, \quad s_{vw} = 0 \quad (v, w = 1, \ldots, h;\ v \neq w), \quad s_{vv} = 1 \quad (v = 1, \ldots, h)$$

wird und (9) mit den $k$ Kongruenzen

$$l_v \equiv 0 \pmod{n_v} \quad (v = 1, \ldots, k)$$

gleichbedeutend ist.

Wenn allgemeiner $\mathfrak{R}$ ein beliebiger reeller algebraischer Zahlkörper endlichen Grades ist, so läßt sich die Bedingung (9) ohne weiteres übertragen, indem man die Hauptideale $(m_k)$ in Primideale zerlegt. Für die Bestimmung von $j_k$ treten jedoch weitere Bedingungen hinzu, die von der Gruppe der Idealklassen und der Einheitengruppe herrühren. Deshalb ergibt sich auf diesem Wege doch kein einfaches Verfahren zur Berechnung von $N$, wenn nicht gerade $\mathfrak{R}$ der rationale Zahlkörper ist.

Zum Abschluss sei noch darauf hingewiesen, daß die Voraussetzung der Realität der Wurzeln beim Beweise nur an einer Stelle benutzt wurde und dort durch die schwächere Annahme ersetzt werden könnte, daß der Körper $\mathfrak{R}_h$ keine von 1 und $-1$ verschiedene Einheitswurzel enthält. Diese Annahme ist zugleich notwendig, wie bereits das einfachste Beispiel

$$h = 1, \quad m_1 = -4, \quad n_1 = 4, \quad \varrho_1 = \sqrt[4]{-4} = \pm 1 \pm i, \quad N = 4 \neq 2$$

zeigt.

### Literaturverzeichnis

[1] A. S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15 (1940), S. 3–6.

[2] G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Zeitschr. 47 (1941), S. 427–467.

*Eingegangen 12. 1. 1971* (132)

ACTA ARITHMETICA
XXI (1972)

# On some exponential sums related to Kloosterman sums

by

L. J. MORDELL

*In memory of Professor Waclaw Sierpiński*

Write

$$S_1(a, b) = S_1 = \sum_{x=1}^{p-1} e(ax + b\bar{x}), \qquad T_1 = \sum_{x=1}^{p-1} e(ax + b\bar{x}) \left(\frac{x}{p}\right), \tag{1}$$
$$ab \not\equiv 0 \pmod{p},$$

where $p$ is an odd prime number, $e(x) = e(2\pi i x/p)$, and we define $\bar{x}$ by $x\bar{x} \equiv 1 \pmod{p}$ and often write $\bar{x} \equiv 1/x \pmod{p}$, and $\left(\frac{x}{p}\right)$ is the Legendre symbol. It is well known that the Kloosterman sum $S_1$ satisfies the inequality

$$|S_1| < 2\sqrt{p}, \tag{2}$$

and that no elementary proof is known[1]. However, $T_1$ can be evaluated by elementary methods and

$$T_1 = 0 \quad \text{if} \quad \left(\frac{ab}{p}\right) = -1,$$
$$T_1 = 2\varepsilon^{-1} \left(\frac{-a}{p}\right) \sqrt{p} \cos(2\pi h/p) \quad \text{if} \quad \left(\frac{ab}{p}\right) = 1, \tag{3}$$

where $\varepsilon = i^{\left(\frac{p-1}{2}\right)^2}$ and $h$ is one solution of

$$h^2 - 4ab \equiv 0 \pmod{p}. \tag{4}$$

This result was first found by Salié [1] in 1931, and another proof has just been given by K. S. Williams [2]. Though their proofs are simple,

[1] Note added in proof by A. Schinzel: An elementary proof has been in the meantime given by S. A. Stiepanov, Trudy Mat. Inst. Stieklov. 112, pp. 346–371.