

Algebra / NT

Note: Theiler = Teiler

85

Product = Produkt etc

Elementarer Beweis des Satzes, dass in jeder unbegrenzten arithmetischen Progression $my+1$ unendlich viele Primzahlen vorkommen.

(Von Herrn *E. Wendt* in Berlin.)

Der Beweis des Satzes, dass jede unbegrenzte arithmetische Progression $ax+b$, in der das Anfangsglied a und die Differenz b theilerfremd sind, unendlich viele Primzahlen enthält, ist von *Dirichlet* in einer der Berliner Akademie im Jahre 1837 vorgelegten Arbeit gegeben worden und hat seitdem keine wesentlichen Vereinfachungen erfahren. Derselbe beruht auf sehr schwierigen Grundlagen. Daher wird es, wie ich glaube, erwünscht sein, einen einfachen Beweis eines Theiles des Satzes, nämlich für $b=1$, zu kennen.

Es sei m eine beliebige positive ganze Zahl, nur grösser als Eins. Man betrachte die Reihe der unendlich vielen Zahlen

$$z = x^m - 1,$$

wo x alle ganzen Zahlen durchläuft. Es sei α eine primitive Wurzel der Gleichung $\alpha^m = 1$; ξ sei eine unbestimmte Variable. Dann zerfällt $\xi^m - 1$ in das Product der beiden Factoren:

$$f(\xi) = \prod_{(r)} (\xi - \alpha^r) = \xi^{\varphi(m)} + A_1 \xi^{\varphi(m)-1} + \dots + A_{\varphi(m)-1} \xi + A_{\varphi(m)},$$

$$g(\xi) = \prod_{(t)} (\xi - \alpha^t) = \xi^{m-\varphi(m)} + a_1 \xi^{m-\varphi(m)-1} + \dots + a_{m-\varphi(m)-1} \xi + a_{m-\varphi(m)},$$

wo r alle $\varphi(m)$ zu m relativ primen, unter m gelegenen Zahlen und t alle die unter m gelegenen Zahlen durchläuft, welche mit m einen echten Theiler gemeinsam haben (m eingeschlossen, 1 ausgeschlossen), und wo $A_1, \dots, A_{\varphi(m)}$, $a_1, \dots, a_{m-\varphi(m)}$ ganze Zahlen bezeichnen, die bestimmt sind, wenn m gegeben ist.

Die Functionen $f(\xi)$ und $g(\xi)$ der Variablen ξ sind bekanntlich theilerfremd. Es fragt sich nun, ob sie es auch sind, wenn man für ξ eine ganze Zahl x setzt.

Angenommen, $f(x)$ und $g(x)$ haben den Primtheiler n gemeinsam; es mögen also gleichzeitig die Congruenzen bestehen:

$$\begin{aligned} f(x) &\equiv x^{\varphi(m)} + A_1 x^{\varphi(m)-1} + \dots + A_{\varphi(m)-1} x + A_{\varphi(m)} \equiv 0, \\ g(x) &\equiv x^{m-\varphi(m)} + a_1 x^{m-\varphi(m)-1} + \dots + a_{m-\varphi(m)-1} x + a_{m-\varphi(m)} \equiv 0 \pmod{n}. \end{aligned}$$

Wenn dies möglich sein soll, muss² bekanntlich die Resultante R der rationalen Functionen $f(\xi)$ und $g(\xi)$ durch n theilbar sein. Dieselbe ist eine ganze Zahl, die nur von den Coefficienten $a_1, \dots, a_{m-\varphi(m)}, A_1, \dots, A_{\varphi(m)}$ abhängt, d. h. durch den Exponenten m bestimmt ist, von der Zahl x aber nicht abhängt und deswegen von Null verschieden ist, weil die Gleichungen $f(\xi) = 0$ und $g(\xi) = 0$ keine gemeinsame Wurzel haben.

Wenn nun der absolute Betrag von R von Eins verschieden ist, so werden also $f(x)$ und $g(x)$ für $x = R^k$, wo k irgend eine positive ganze Zahl bedeutet, relativ prim sein. Denn angenommen, diese beiden Zahlen hätten einen gemeinsamen Primtheiler, so müsste dieser, wie eben bewiesen, in R , andererseits aber auch in dem Producte

$$f(R^k) \cdot g(R^k) = (R^k)^m - 1$$

enthalten sein. Das aber ist nicht möglich, weil die Zahlen $(R^k)^m - 1$ und R keinen gemeinsamen Divisor besitzen können. Sollte aber $R = \pm 1$ sein*), so sind $f(x)$ und $g(x)$ für jeden die Eins übersteigenden Werth von x theilerfremd. In jedem Falle giebt es mithin eine unendlich grosse Anzahl von Zahlen x von der Beschaffenheit, dass $f(x)$ und $g(x)$ keinen gemeinsamen Divisor haben.

Es seien nun z. B. $f(x')$ und $g(x')$ theilerfremd. Ferner sei $f(x')$ von Null und ± 1 verschieden. Dies kann man voraussetzen, da jede der algebraischen Gleichungen

$$f(\xi) = 1, \quad f(\xi) = -1$$

überhaupt nur $\varphi(m)$ Wurzeln ξ hat, da ferner $f(x)$ ein Theiler von $x^m - 1$

*) In Wirklichkeit kann dieser Fall nie eintreten.

ist und diese letztere Zahl nur für $x = 1$ verschwindet. Dann hat also $f(x')$ einen Primtheiler q_1 , welcher in $g(x')$ nicht enthalten ist, mithin in keiner Zahl $x'^{\mu} - 1$ aufgeht, wo μ ein Divisor von m ist, da $g(x')$ durch alle Zahlen von dieser Form theilbar ist. Dann kann aber auch q_1 in keiner Zahl $x'^{\mu'} - 1$ aufgehen, wo $\mu' < m$ ist, d. h. m ist die kleinste Zahl für welche

$$x'^m \equiv 1 \pmod{q_1}$$

ist. Nach dem *Fermatschen* Satze hat aber die Congruenz statt

$$x'^{q_1-1} \equiv 1 \pmod{q_1},$$

folglich muss $q_1 - 1$ durch m theilbar sein, d. h. q_1 hat die Form

$$q_1 = mk + 1.$$

Es ist somit bis jetzt folgender Satz bewiesen:

Wenn m eine willkürlich gegebene positive ganze Zahl ist, so gibt es stets eine Primzahl von der Form $q_1 = mk + 1$. (Die bisher gemachte Annahme, dass m nicht gleich 1 sei, kann man nun offenbar fallen lassen.)

Zufolge dieses Satzes gehört auch zu mm_1k , wo m_1 eine die Einheit übersteigende positive ganze Zahl bedeuten soll, eine Primzahl

$$q_2 = mm_1kk_1 + 1,$$

ferner zur Zahl $mm_1m_2kk_1$ eine Primzahl

$$q_3 = mm_1m_2kk_1k_2 + 1$$

u. s. w. Diese Primzahlen q_1, q_2, q_3, \dots sind alle unter einander verschieden, weil die folgende stets grösser als die vorhergehende ist, und haben alle die Form $my + 1$. Mithin gilt der Satz:

In jeder unbegrenzten arithmetischen Progression $my + 1$, wo die Differenz m eine gegebene positive ganze Zahl bedeutet, sind unendlich viele Primzahlen enthalten.

Man kann den Beweis auch ohne Zuhilfenahme der Resultante R und der Grösse α führen, indem man von dem Satze Gebrauch macht, nach welchem die Zahlen $\frac{u^p - 1}{u - 1}$ und $u - 1$, wobei p eine Primzahl bedeutet, ent-

Logic

Beweis, daß jede Menge wohlgeordnet werden kann.

(Aus einem an Herrn Hilbert gerichteten Briefe.)

Von

E. ZERMELO in Göttingen.

... Der betreffende Beweis ist aus Unterhaltungen entstanden, die ich in der vorigen Woche mit Herrn Erhard Schmidt geführt habe, und ist folgender.

1) Es sei M eine beliebige Menge von der Mächtigkeit m , deren Elemente mit m bezeichnet werden mögen, M' von der Mächtigkeit m' eine ihrer Teilmengen, welche mindestens ein Element m enthalten muß, aber auch alle Elemente von M umfassen darf, und $M - M'$ die zu M' „komplementäre“ Teilmenge. Zwei Teilmengen gelten als verschieden, wenn eine von beiden irgend ein Element enthält, das in der anderen nicht vorkommt. Die Menge aller Teilmengen M' werde mit \mathfrak{M} bezeichnet.

2) Jeder Teilmenge M' denke man sich ein beliebiges Element m_1' zugeordnet, das in M' selbst vorkommt und das „ausgezeichnete“ Element von M' genannt werden möge. So entsteht eine „Belegung“ γ der Menge \mathfrak{M} mit Elementen der Menge M von besonderer Art. Die Anzahl dieser Belegungen γ ist gleich dem Produkte $\Pi m'$ erstreckt über alle Teilmengen M' und ist daher jedenfalls von 0 verschieden. Im folgenden wird nun eine beliebige Belegung γ zu grunde gelegt und aus ihr eine bestimmte Wohlordnung der Elemente von M abgeleitet.

3) *Definition.* Als „ γ -Menge“ werde bezeichnet jede wohlgeordnete Menge M_γ aus lauter verschiedenen Elementen von M , welche folgende Beschaffenheit besitzt: ist a ein beliebiges Element von M_γ und A der „zugehörige“ Abschnitt, der aus den vorangehenden Elementen $x < a$ von M_γ besteht, so ist a immer das „ausgezeichnete“ Element von $M - A$.

4) *Es gibt γ -Mengen innerhalb M .* So ist z. B. m_1 , das ausgezeichnete Element von $M' = M$, selbst eine γ -Menge, ebenso die (geordnete) Menge $M_2 = (m_1, m_2)$, wo m_2 das ausgezeichnete Element von $M - m_1$ ist.

5) *Sind M_γ' und M_γ'' irgend zwei verschiedene γ -Mengen (die aber zu derselben ein für allemal gewählten Belegung γ gehören!), so ist immer eine von beiden identisch mit einem Abschnitte der anderen.*

Es sei nämlich M'_γ die eine der beiden wohlgeordneten Mengen, welche auf die andere, M''_γ , oder einen ihrer Abschnitte ähnlich abbildbar ist. Dann müssen je zwei bei dieser Abbildung einander entsprechende Elemente miteinander identisch sein. Denn das erste Element jeder γ -Menge ist m_1 , da der zugehörige Abschnitt A kein Element enthält, also $M - A = M$ ist. Wäre nun m' das erste Element von M'_γ , welches von dem entsprechenden Elemente m'' verschieden wäre, so müssten die zugehörigen Abschnitte A' und A'' noch miteinander identisch sein, mithin auch die Komplementärmengen $M - A'$ und $M - A''$ und als deren ausgezeichnete Elemente m' und m'' selbst, gegen die Annahme.

6) *Folgerungen.* Haben zwei γ -Mengen ein Element a gemeinsam, so haben sie auch den Abschnitt A der vorangehenden Elemente gemein. Haben sie zwei Elemente a, b gemein, so ist in beiden Mengen entweder $a < b$ oder $b < a$.

7) Bezeichnet man als „ γ -Element“ jedes Element von M , das in irgend einer γ -Menge vorkommt, so gilt der Satz: Die Gesamtheit L_γ aller γ -Elemente läßt sich so ordnen, daß sie selbst eine γ -Menge darstellt, und umfaßt alle Elemente der ursprünglichen Menge M . Die letztere ist damit selbst wohlgeordnet.

I) Sind a, b zwei beliebige γ -Elemente und M'_γ und M''_γ irgend zwei γ -Mengen, denen sie angehören, so enthält nach 5) die größere der beiden γ -Mengen beide Elemente und bestimmt die Ordnungsbeziehung $a < b$ oder $b < a$. Diese Ordnungsbeziehung ist nach 6) unabhängig von der Wahl der verwendeten γ -Menge.

II) Sind a, b, c drei beliebige γ -Elemente und $a < b$ und $b < c$, so ist immer $a < c$. Denn jede c enthaltende γ -Menge enthält nach 6) auch b und mithin a , und da sie einfach geordnet ist, so folgt in ihr aus $a < b$ und $b < c$ in der Tat $a < c$. Die Menge L_γ ist also einfach geordnet.

III) Ist L'_γ eine beliebige Teilmenge von L_γ und a eines ihrer Elemente, das der γ -Menge M_γ angehören möge, so enthält M_γ nach 6) alle Elemente $< a$, also auch die Teilmenge L''_γ , welche aus L'_γ durch Weglassung aller auf a folgenden Elemente entsteht, und L''_γ besitzt als Teilmenge der wohlgeordneten Menge M_γ ein erstes Element, das zugleich erstes Element von L'_γ ist. L_γ ist also auch wohlgeordnet.

IV) Ist a ein beliebiges γ -Element und A die Gesamtheit aller vorangehenden Elemente $x < a$, so ist A nach 6) der zu a gehörige Abschnitt in jeder Menge M_γ , welche a enthält, und a ist mithin nach 3) das ausgezeichnete Element von $M - A$. Also ist L_γ selbst eine γ -Menge.

V) Gäbe es ein Element von M , das keiner γ -Menge angehörte, also Element von $M - L_\gamma$ wäre, so gäbe es auch ein ausgezeichnetes Element m'_1

von $M - L_\gamma$, und die geordnete Menge (L_γ, m_1') , in der jedes γ -Element dem Element m_1' vorangehe, wäre nach 3) selbst eine γ -Menge. Also wäre auch m_1' ein γ -Element gegen die Annahme, und es ist in Wirklichkeit $L_\gamma = M$, also M selbst eine wohlgeordnete Menge.

Somit entspricht jeder Belegung γ eine ganz bestimmte Wohlordnung der Menge M , wenn auch nicht zwei verschiedenen Belegungen immer verschiedene. Jedenfalls muß es *mindestens eine* solche Wohlordnung geben, und jede Menge, für welche die Gesamtheit der Teilmengen usw. einen Sinn hat, darf als eine wohlgeordnete, ihre Mächtigkeit als ein „Alef“ betrachtet werden. So folgt also für jede transfinite Mächtigkeit

$$m = 2m = \aleph_0 m = m^2 \text{ usw.},$$

und je zwei Mengen sind miteinander „vergleichbar“, d. h. es ist immer die eine ein-eindeutig abbildbar auf die andere oder einen ihrer Teile.

Der vorliegende Beweis beruht auf der Voraussetzung, daß Belegungen γ überhaupt existieren, also auf dem Prinzip, daß es auch für eine unendliche Gesamtheit von Mengen immer Zuordnungen gibt, bei denen jeder Menge eines ihrer Elemente entspricht, oder formal ausgedrückt, daß das Produkt einer unendlichen Gesamtheit von Mengen, deren jede mindestens ein Element enthält, selbst von Null verschieden ist. Dieses logische Prinzip läßt sich zwar nicht auf ein noch einfacheres zurückführen, wird aber in der mathematischen Deduktion überall unbedenklich angewendet. So kann z. B. die Allgemeingültigkeit des Satzes, daß die Anzahl der Teile, in die eine Menge zerfällt, kleiner oder gleich ist der Anzahl aller ihrer Elemente, nicht anders bewiesen werden, als indem man sich jedem der betrachteten Teile eines seiner Elemente zugeordnet denkt.

Die Idee, unter Berufung auf dieses Prinzip eine beliebige Belegung γ der Wohlordnung zu grunde zu legen, verdanke ich Herrn Erhard Schmidt; meine Durchführung des Beweises beruht dann auf der Verschmelzung der verschiedenen möglichen „ γ -Mengen“, d. h. der durch das Ordnungsprinzip sich ergebenden wohlgeordneten Abschnitte.

Münden i. Hann., den 24. September 1904.

Analysis

Untersuchungen über schlichte konforme Abbildungen des Einheitskreises. I.

Von

Karl Löwner in Berlin.

Die Entdeckung des Verzerrungssatzes durch Koebe war der Ausgangspunkt einer Reihe von Untersuchungen, die sich zur Aufgabe stellen, den Einfluß zu ermitteln, den die Forderung der Schlichtheit einer konformen Abbildung auf den Verlauf der sie darstellenden Funktion ausübt¹⁾. Von besonderem Interesse ist die Frage, welche Beziehungen zwischen den Koeffizienten einer Potenzreihe

$$(1) \quad z + b_1 z^2 + b_2 z^3 + \dots$$

bestehen müssen, wenn sie den Einheitskreis schlicht abbildet. Das wichtigste in dieser Richtung bisher erzielte Resultat besteht in der Ungleichung $|b_1| \leq 2$ (erreichbar nur bei den Funktionen $\frac{z}{(1-\varepsilon z)^2}$, $|\varepsilon| = 1$ ²⁾).

In der vorliegenden Arbeit wird diese von neuem abgeleitet und werden darüber hinausgehende Resultate erzielt. Insbesondere wird gezeigt, daß $|b_2| \leq 3$ ist. (Wieder ist die Schranke nur bei den oben angegebenen Funktionen erreichbar.)

Das charakteristische Merkmal der angewandten Untersuchungsmethode besteht in der Ausnützung des Umstandes, daß bei Zusammensetzung von schlichten konformen Abbildungen wieder eine schlichte Abbildung entsteht, daß also die schlichten Abbildungen eine Gruppe bilden.

¹⁾ Siehe insbesondere Pick, G.: Leipz. Ber. 1916, S. 58–64 und Wien. Ber. 1917, Abtlg. IIa, 126, S. 247–263; Bieberbach, L.: Sitzber. kgl. Akad. Berlin 1916, S. 940–955; Faber, G.: Münch. Ber. 1916, S. 39–42 und 1920, S. 49–64.

²⁾ Siehe die in ¹⁾ zit. Arbeit von L. Bieberbach.

1. Zusammensetzung von beschränkten schlichten Abbildungen des Einheitskreises.

Es sei

$$(2) \quad w = f(z) = z + b_1 z^2 + b_2 z^3 + \dots$$

eine Potenzreihe, die das Innere des E. K.³⁾ schlicht abbildet. Wir machen außerdem die unwesentliche Voraussetzung, daß $|f(z)|$ beschränkt ist. Wenn man $f(z)$ mit einer positiven Konstanten β multipliziert, die nicht größer ist als der reziproke Wert der oberen Grenze M von $|f(z)|$ im E. K., so entsteht eine Funktion

$$(3) \quad b(z) = \beta(z + b_1 z^2 + b_2 z^3 + \dots),$$

die folgende Eigenschaften besitzt:

1. Sie bildet das Innere des E. K. schlicht ab auf einen Bereich \mathfrak{B} , der ganz im Innern des E. K. enthalten ist.

2. Es ist $b(0) = 0$; $b'(0) = \beta > 0$, geometrisch gesprochen: der Nullpunkt bleibt fest und auch die Richtungen daselbst.

Aus 2. folgt bekanntlich mit Hilfe des Schwarzschen Lemmas, daß sogar

$$(4) \quad \beta \leq 1$$

sein muß, und daß das Gleichheitszeichen nur für die Funktion $b(z) = z$ eintreten kann.

Abbildungen mit den Eigenschaften 1 und 2 — und nur solche sollen jetzt betrachtet werden — wollen wir kurz beschränkte Abbildungen nennen.

Es seien nun $b_\mu(z)$ ($\mu = 1, 2, \dots, n$) n Funktionen mit den Anfangskoeffizienten β_μ , die alle eine beschränkte Abbildung des E. K. liefern. Dann ist dasselbe auch bei der zusammengesetzten Funktion

$$(5) \quad b(z) = b_n(\dots b_2(b_1(z)))$$

der Fall. Ihr Anfangskoeffizient β hat den Wert

$$(6) \quad \beta = \beta_1 \beta_2 \dots \beta_n.$$

Aus der Ungleichung (4) schließen wir, daß

$$(7) \quad \beta \leq \beta_\mu \quad (\mu = 1, 2, \dots, n)$$

sein muß, und daß das Gleichheitszeichen nur dann eintreten kann, wenn sich alle $b_\nu(z)$ ($\nu \neq \mu$) auf z reduzieren.

Es liegt nun die Frage nahe: Gegeben sei eine beschränkte Abbildung $b(z)$ mit dem Anfangskoeffizienten $\beta < 1$, und n positive Konstanten β_μ , die ebenfalls alle < 1 sind, und die zum Produkt β ergeben.

³⁾ E. K. = Abkürzung für Einheitskreis.

Gibt es beschränkte Abbildungen $b_\mu(z)$ mit den Anfangskoeffizienten β_μ , die zusammengesetzt $b(z)$ ergeben?

Daß diese Frage zu bejahen ist und die Funktionen $b_\mu(z)$ im allgemeinen auf unendlich viele Arten gewählt werden können, soll jetzt bewiesen werden. Zu dem Zwecke diene folgende einfache Vorbetrachtung: Die aus n gegebenen beschränkten Abbildungen $b_\mu(z)$ durch Zusammensetzung entstehenden beschränkten Abbildungen

$$(8) \quad c_\mu(z) = b_\mu(\dots b_{\mu+1}(b_\mu(z)))$$

liefern Bildbereiche \mathfrak{G}_μ , die folgende Bedingung erfüllen: *Es ist \mathfrak{G}_β in \mathfrak{G}_α enthalten, wenn $\alpha > \beta$. Die Anfangskoeffizienten γ_μ der $c_\mu(z)$ berechnen sich aus den β nach der Gleichung*

$$(9) \quad \gamma_\mu = \beta_\mu \beta_{\mu+1} \dots \beta_n.$$

Umgekehrt: Sind die Bildbereiche \mathfrak{G}_μ von n gegebenen beschränkten Abbildungen $c_\mu(z)$ so ineinander eingeschachtelt, wie eben beschrieben worden ist, so liefern die durch Auflösung der Gleichung (8) eindeutig gewonnenen Funktionen

$$(8') \quad b_\mu(z) = c_{\mu+1}^{-1}(c_\mu(z)) \quad (\mu = 1, 2, \dots, n; c_{n+1}(z) = z)^4$$

offenbar wieder beschränkte Abbildungen, deren Anfangskoeffizienten β_μ aus den γ_μ sich auf Grund der Gleichung (9) ergeben.

An Stelle also bei der oben aufgeworfenen Frage die Funktionen $b_\mu(z)$ zu suchen, ist es offenbar zweckmäßiger, auf Konstruktion von Funktionen $c_\mu(z)$ bzw. der zugehörigen Bereiche \mathfrak{G}_μ auszugehen.

Im Falle, daß der zur Funktion $b(z)$ gehörige Bereich \mathfrak{B} von einer Jordankurve \mathfrak{J} begrenzt ist, die ganz im Innern des E. K. gelegen ist, kann man folgendermaßen verfahren: Man bilde den von \mathfrak{J} und der Peripherie des E. K. begrenzten Ringbereich auf einen gewöhnlichen Kreisring so ab, daß etwa \mathfrak{J} in den innern, die Peripherie des E. K. in den äußern Begrenzungskreis desselben übergeht. Den zu den Begrenzungskreisen konzentrischen im Kreisring verlaufenden Kreisen entspricht in unserem Ringbereich eine Schar von ineinander eingeschachtelten Jordankurven \mathfrak{J}_r , die vom Radius r des Bildkreises stetig abhängen. Es hängen deshalb auch die Abbildungsfunktionen $c_r(z)$ auf die von den \mathfrak{J}_r begrenzten Jordanbereiche mit allen ihren Ableitungen nach z stetig von r ab. Insbesondere durchläuft somit der Anfangskoeffizient γ_r von $c_r(z)$ mit wachsendem r *monoton alle Werte von β bis 1, und nimmt also auch die Werte (9) an. Die zugehörigen Jordanbereiche können als Bereiche \mathfrak{G}_μ verwendet werden.*

⁴⁾ Der Exponent -1 ist Zeichen für die Umkehrfunktion.