p-adische Kettenbrüche und Irrationalität p-adischer Zahlen

Autor(en): **Bundschuh, P.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **32 (1977)**

Heft 2

PDF erstellt am: **24.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-32150

Nutzungsbedingungen

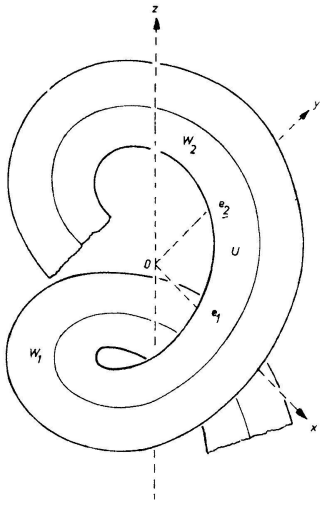
Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch



Figur 3. Übergangsfläche $\dot{U}$ zwischen einer Wendelfläche W_1 und einer Wendelfläche W_2 (Übergang zwischen W_1 und $\dot{U}$ längs der Erzeugenden e_1, zwischen $\dot{U}$ und W_2 längs e_2; $p_1 = 3/\pi = 2p_2$, $n = 1$, $v = \pi/3$).

Der Anschluss an die erste Wendelfläche kann stattfinden in der Erzeugenden $v = 0$; als Übergangsbedingung für die zweite Wendelfläche erhält man die folgende Beziehung: $p_2 = p_1 \cdot \cos nv$.

Durch geeignete Wahl von n kann noch die Höhe beeinflusst werden, in der der zweite Übergang stattfinden soll; danach erst kann die genaue Lage der zweiten Wendelfläche festgelegt werden. Die Abwicklung des koaxialen Einheitszylinders gemäss Figur 1 würde hier zwei geneigte Geraden mit den Anstiegen p_1 bzw. p_2 zeigen, die durch eine Sinuslinie knicklos miteinander verbunden sind.

E. Hartmann, Zuoz

LITERATURVERZEICHNIS

[1] K. Fladt und A. Baur, *Analytische Geometrie spezieller Flächen und Raumkurven* (Braunschweig 1975).
[2] J. Hoschek, *Liniengeometrie* (Zürich 1971).
[3] K. Strubecker, *Differentialgeometrie I, II, III* (Berlin, ab 1958).

p-adische Kettenbrüche und Irrationalität p-adischer Zahlen

In der vorliegenden Note wird zunächst der Körper der p-adischen Zahlen und ein von Th. Schneider angegebener Kettenbruchalgorithmus für solche Zahlen beschrieben. Als Hauptergebnis wird sodann ein notwendiges und hinreichendes Kriterium für Irrationalität p-adischer Zahlen bewiesen.

1. p-adische Zahlen. Sei p eine feste Primzahl. Für $m \in \mathbf{Z}$, $m \neq 0$ werde $\operatorname{ord}(m; p) := \operatorname{Max}\{j \in \mathbf{Z} \mid p^j \text{ teilt } m\}$ gesetzt. Ist $a \in \mathbf{Q}$, $a \neq 0$ und $a = s/t$ mit $s, t \in \mathbf{Z}$ und beide $\neq 0$,

so setzt man weiter $|a|_p := p^{\mathrm{ord}(t;p)-\mathrm{ord}(s;p)}$; diese Definition ist offensichtlich von der für a gewählten Darstellung s/t unabhängig. Mit $|0|_p := 0$ ist klar, dass die Abbildung $|\cdot|_p$: $\mathbf{Q}\to\mathbf{R}$ alle Eigenschaften besitzt, die man von einer *Bewertung* eines Körpers, hier des speziellen Körpers $\mathbf{Q}$ der rationalen Zahlen, verlangt (vgl. etwa [1], S. 49). Diese Bewertung ist *nichtarchimedisch*, da $|a+b|_p \leq \mathrm{Max}(|a|_p, |b|_p)$ für alle $a, b \in \mathbf{Q}$ gilt.

Eine unendliche Folge $\{a_n | a_n \in \mathbf{Q}\}_{n=0,1,\ldots}$ heisst nun eine *p-Cauchy-Folge*, wenn es zu jedem reellen $\varepsilon > 0$ ein $N = N(\varepsilon)$ gibt so, dass für alle $m, n > N$ gilt: $|a_m - a_n|_p < \varepsilon$. Zum Beispiel ist die durch $a_n := \Sigma_{\nu=0}^{n} p^\nu$ definierte Folge eine p-Cauchy-Folge; aus $a_n = (1-p^{n+1})/(1-p)$ sieht man weiter, dass $|a_n - 1/(1-p)|_p = |p^{n+1}/(p-1)|_p = p^{-n-1} \to 0$ mit $n \to \infty$ gilt. Daher sagt man, dass diese spezielle Folge $\{a_n\}$ bezüglich der Bewertung $|\cdot|_p$ gegen die rationale Zahl $1/(1-p)$ konvergiert. Hat man irgendeine p-Cauchy-Folge $\{a_n | a_n \in \mathbf{Q}\}$, so braucht es aber kein $a \in \mathbf{Q}$ zu geben so, dass $|a_n - a|_p \to 0$ bei $n \to \infty$ gilt; d.h. eine beliebige p-Cauchy-Folge rationaler Zahlen braucht bezüglich $|\cdot|_p$ in $\mathbf{Q}$ nicht zu konvergieren. Anders ausgedrückt: $\mathbf{Q}$ ist bezüglich der Bewertung $|\cdot|_p$ nicht vollständig.

Analog zur Cantorschen Methode der Konstruktion der reellen Zahlen aus den rationalen kann man aber einen neuen mit $\mathbf{Q}_p$ bezeichneten, $\mathbf{Q}$ umfassenden Körper konstruieren, in dem jede p-Cauchy-Folge rationaler Zahlen konvergiert (vgl. [1], S. 48ff). $\mathbf{Q}_p$ heisst Körper der *p-adischen Zahlen* und die Fortsetzung der (normierten) *p-adischen Bewertung* $|\cdot|_p$ von $\mathbf{Q}$ auf $\mathbf{Q}_p$ wird wieder mit $|\cdot|_p$ bezeichnet; jede p-Cauchy-Folge von Elementen aus $\mathbf{Q}_p$, also von p-adischen Zahlen, konvergiert bezüglich $|\cdot|_p$ in $\mathbf{Q}_p$, d.h. $\mathbf{Q}_p$ ist $|\cdot|_p$-vollständig.

Hat man nun irgendein $\xi \in \mathbf{Q}_p$, $\xi \neq 0$, so ist $|\xi|_p = p^{-a}$ mit einem gewissen wohlbestimmten $a \in \mathbf{Z}$. Weiter kann man dieses ξ in eindeutiger Weise in eine *kanonische p-adische Reihe* der folgenden Gestalt entwickeln

$$\xi = \Sigma_{\nu=a}^{\infty} b_\nu p^\nu \text{ mit allen } b_\nu \in \{0, 1, \ldots, p-1\} \text{ und } b_a \neq 0. \tag{1}$$

2. *p*-adische Kettenbrüche. Im Körper $\mathbf{R}$ der reellen Zahlen, also der Vervollständigung von $\mathbf{Q}$ bezüglich des gewöhnlichen Absolutbetrags $|\cdot|$, ist eine reichhaltige Kettenbruchtheorie entwickelt (vgl. etwa [4]). Die Frage liegt nahe, ob sich auch für p-adische Zahlen ein Algorithmus angeben lässt mit Eigenschaften, die analog sind zu solchen, wie sie von den regulären Kettenbrüchen reeller Zahlen her bekannt sind. Mit dieser Frage hat sich zuerst K. Mahler [2], [3] beschäftigt.

1968 hat dann Th. Schneider [5] einen vom Mahlerschen verschiedenen Kettenbruchalgorithmus für p-adische Zahlen vorgeschlagen. Dieser verläuft wie folgt: Für $\xi \in \mathbf{Q}_p$, $\xi \neq 0$ sei $a_0 \in \mathbf{Z}$ definiert durch $|\xi|_p = p^{-a_0}$; dann lässt sich schreiben $\xi = p^{a_0} \cdot \xi_0^{-1}$ mit $|\xi_0|_p = 1$. Entwickelt man nun ξ_0 in die kanonische p-adische Reihe (1), $\xi_0 = \Sigma_{\nu=0}^{\infty} b_{0,\nu} p^\nu$ mit $b_{0,\nu} \in \{0, \ldots, p-1\}$, $b_{0,0} \neq 0$, so ist $|\xi_0 - b_{0,0}|_p < 1$. Ist $\xi_0 - b_{0,0} \neq 0$, so gilt $\xi_0 = b_{0,0} + p^{a_1} \cdot \xi_1^{-1}$ mit $a_1 \geq 1$, $|\xi_1|_p = 1$ und die Entwicklung $\Sigma_{\nu=0}^{\infty} b_{1,\nu} p^\nu$ von ξ_1 liefert wieder ein $b_{1,0}$ mit $0 < b_{1,0} < p$ und $|\xi_1 - b_{1,0}|p < 1$. Auf diese Weise kann man fortfahren, solange die $\xi_\nu - b_{\nu,0} \neq 0$ sind. Man erhält eine Entwicklung von ξ der Gestalt

$$\xi = a_0/b_0 + a_1/b_1 + \ldots + a_{n-1}/b_{n-1} + a_n/\xi_n, \tag{2}$$

wo $a_\nu = p^{\alpha_\nu}$ und $b_\nu = b_{\nu,0}$ gesetzt und die Pringsheimsche Schreibweise ([4], S. 3) benutzt ist; der Kürze wegen sei (2) im folgenden als

$$\xi = [a_0; b_0, a_1; \ldots; b_{n-1}, a_n; \xi_n]$$

geschrieben. Bricht das geschilderte Verfahren ab, d.h. wird irgendwann $\xi_n = b_n$, so hat man ξ in einen *endlichen p-adischen Kettenbruch* $[a_0; b_0, a_1; \ldots; b_{n-1}, a_n; b_n]$ entwickelt; andernfalls wird ξ durch die Anwendung des beschriebenen Algorithmus ein Symbol der Art

$$[a_0; b_0, a_1; \ldots; b_{n-1}, a_n; \ldots] \tag{3}$$

zugeordnet, das man einen *unendlichen p-adischen Kettenbruch* nennt.

Dies sei an einem numerischen Beispiel verdeutlicht: Sei $p=3$, $\xi = -1/2$; dann ist $a_0 = 0$, $\xi_0 = -2$ und für -2 erhält man die kanonische 3-adische Reihe $1 + \Sigma_{\nu=1}^{\infty} 2 \cdot 3^\nu$, da nach **1.** gilt: $\Sigma_{\nu=0}^{\infty} 3^\nu = 1/(1-3) = -1/2$. Somit ist $b_{0,0} = 1$, also $3^{\alpha_1} \cdot \xi_1^{-1} = -3$ und damit $\alpha_1 = 1$, $\xi_1 = -1$. Die Entwicklung $\xi_1 = -1 = \Sigma_{\nu=0}^{\infty} 2 \cdot 3^\nu$ zeigt dann $b_{1,0} = 2$ und $-3 = \xi_1 - b_{1,0} = 3^{\alpha_2} \cdot \xi_2^{-1}$ also $\alpha_2 = 1$, $\xi_2 = -1$. Es ist klar, dass hier das Verfahren nicht abbricht und dass man $\alpha_\nu = 1$, $\xi_\nu = -1$, $b_{\nu,0} = 2$ für alle $\nu \geq 1$ erhält; damit wird der Zahl $\xi = -1/2$ der folgende unendliche (periodische) 3-adische Kettenbruch zugeordnet: $[1; 1, 3; 2, 3; \ldots; 2, 3; \ldots]$.

Schneider hat nun a.a.O. analog zur Vorgehensweise bei den regulären Kettenbrüchen im Reellen gezeigt, dass die Folge $\{[a_0; b_0, a_1; \ldots; b_n]\}_{n=0,1,\ldots}$ der rationalen Näherungsbrüche von (3) p-adisch (d.h. bezüglich $|\cdot|_p$) gegen ξ konvergiert, dass man also ξ gleich dem Ausdruck in (3) setzen kann. Und ausserdem: Schreibt man irgendeinen unendlichen Kettenbruch der Form (3) hin mit $b_\nu \in \{1, 2, \ldots, p-1\}$ und a_ν von der Form p^{α_ν}, $\alpha_\nu \in \mathbf{Z}$ und $\alpha_\nu \geq 1$ für $\nu \geq 1$, so konvergiert dieser p-Kettenbruch immer in $\mathbf{Q}_p$; bezeichnet man noch $b_n + [a_{n+1}; b_{n+1}, a_{n+2}; \ldots]$ mit ξ_n, so ist in den Schneiderschen Formeln implizit die Aussage $|\xi_n|_p = 1$ für alle $n \geq 0$ enthalten.

Damit kann man nun zeigen, dass die Entwicklung von ξ in einen p-Kettenbruch eindeutig ist. Denn sei

$$\xi = [a_0; b_0, a_1; \ldots] = [a_0'; b_0', a_1'; \ldots] \tag{4}$$

mit a_ν', a_ν' und b_ν, b_ν' wie bisher und seien etwa beide p-Kettenbrüche unendlich, so ist $a_0 \xi_0^{-1} = a_0'(\xi_0')^{-1}$, also $|a_0|_p = |a_0'|_p$ und $a_0 = a_0'$, $\xi_0 = \xi_0'$ und somit $b_0 + a_1/\xi_1 = b_0' + a_1'/\xi_1'$. Dies ergibt

$$|b_0 - b_0'|_p = |a_1'/\xi_1' - a_1/\xi_1|_p \leq \mathrm{Max}(|a_1'|_p, |a_1|_p) < 1,$$

also $b_0 = b_0'$ und $a_1/\xi_1 = a_1'/\xi_1'$ und man kann induktiv fortfahren. Ist in (4) einer der p-Kettenbrüche endlich, so zeigt man ebenso leicht, dass beide endlich sein müssen von gleicher Länge und dass wieder $a_\nu = a_\nu'$, $b_\nu = b_\nu'$ gilt.

3. Irrationalitätskriterium. In [5] wurde weiter die Frage nach der Darstellung rationaler bzw. quadratisch irrationaler Zahlen aus $\mathbf{Q}_p$ durch p-Kettenbrüche aufgeworfen. Das erste Problem wird vollständig gelöst in folgendem Satz, der ein notwendiges und hinreichendes Irrationalitätskriterium für p-adische Zahlen enthält.

Satz. *Sei $\xi \in \mathbf{Q}_p$, $\xi \neq 0$. Es ist $\xi \in \mathbf{Q}$ genau dann, wenn der p-Kettenbruch von ξ entweder endlich ist oder periodisch mit der Periodenlänge 1 und $a_n = p$, $b_n = p-1$ für alle genügend grossen n.*

Beweis. Zunächst habe ξ einen unendlichen p-Kettenbruch, der periodisch ist von der angegebenen Form. Es gibt also ein $n_0 \geq 0$ so, dass für alle $n \geq n_0$ gilt:

$$\xi_n = p-1+[p;p-1,p;\ldots;p-1,p;\ldots] = p-1+p/\xi_n .$$

Hieraus folgt, dass ξ_n für $n \geq n_0$ der quadratischen Gleichung $\xi_n^2-(p-1)\xi_n-p = (\xi_n-p)(\xi_n+1)=0$ genügt. $|\xi_n|_p = 1$ impliziert $\xi_n = -1$ für $n \geq n_0$ und nach (2) ist $\xi \in \mathbf{Q}$.

Zum Beweis der Umkehrung sei $\xi \in \mathbf{Q}$, habe aber einen unendlichen p-Kettenbruch der Form (3). Schreibt man

$$\xi = p^{a_0'}(x_0/x_1)^{-1} \text{ mit } x_0, x_1 \in \mathbf{Z}, x_0 > 0, (x_0, x_1) = (x_0, p) = (x_1, p) = 1, \tag{5}$$

so werden in eindeutiger Weise rekursiv

$$b_{n-1}' \in \{1,\ldots,p-1\}, a_n' = p^{a_n'} (\text{mit } a_n' \geq 1) \text{ und } x_{n+1} \in \mathbf{Z}-p\mathbf{Z} \tag{6}$$

in dieser Reihenfolge so bestimmt, dass gilt

$$x_{n-1} = b_{n-1}' x_n + a_n' x_{n+1} \text{ für } n \geq 1 . \tag{7}$$

Schreibt man noch a_0' für $p^{a_0'}$, so folgt aus (5) und (7)

$$\xi = [a_0'; b_0', a_1'; \ldots] .$$

Hieraus und weil für ξ die p-Kettenbruchentwicklung (3) vorausgesetzt wurde, folgt wegen der Eindeutigkeit dieser Entwicklung sofort $a_n = a_n'$, $b_n = b_n'$ für alle $n \geq 0$; speziell bricht damit auch die Folge $\{x_n\}$ nicht ab. Weiter ist $x_n \in \mathbf{Z}$, $x_n \neq 0$ und $(x_n, x_{n+1}) = 1$ für alle $n \geq 0$ wie man aus (5), (6) und (7) induktiv leicht sieht. Aus (6) und (7) folgt

$$|x_{n+1}| = |x_{n-1} - b_{n-1} x_n| / a_n \leq (|x_{n-1}| + (p-1)|x_n|)/p \text{ für } n \geq 1 . \tag{8}$$

Wegen $(x_{n-1}, x_n) = 1$ ist $|x_{n-1}| \neq |x_n|$, solange nicht $|x_{n-1}| = |x_n| = 1$.
Daher folgt aus (8)

$$|x_{n+1}| < \mathrm{Max}(|x_{n-1}|, |x_n|), \text{ falls nicht } x_{n-1}, x_n \in \{+1, -1\} .$$

Da alle $|x_n| \geq 1$ sind, muss es also ein n_0 geben so, dass $x_n \in \{+1, -1\}$ für alle $n \geq n_0$. $x_{n-1} = x_n$ für ein $n > n_0$ impliziert nach (6) und (7) $b_{n-1} \equiv 1 \pmod{p}$, also $b_{n-1} = 1$, was $a_n x_{n+1} = 0$ liefern würde. So ist $x_n = -x_{n-1}$ für alle $n > n_0$, also $(1 + b_{n-1}) x_{n-1} = a_n x_{n+1}$ und somit $1 + b_{n-1} = a_n$ für alle $n > n_0$. Nach (6) hat man $a_n = p, b_{n-1} = p - 1$ für diese n, was den Satz vollständig beweist.

Das *Analogon zum Eulerschen Satz* ist natürlich hier auch richtig: Hat $\xi \in \mathbf{Q}_p$ einen unendlichen periodischen p-Kettenbruch mit einer Periode, die nicht von der Form des obigen Satzes ist, so ist ξ eine quadratische Irrationalität. Ob die Umkehrung hiervon, also das *Analogon zum Satz von Lagrange,* richtig ist, bleibt ein interessantes offenes Problem; man siehe dazu auch [5]. Jedenfalls scheinen sich die aus dem Reellen bekannten Beweismethoden für diese Umkehrung im p-adischen Fall nicht zu bewähren.

In dieser Situation kann man wenigstens folgendes tun: Man nehme spezielle quadratische Polynome der Form $X^2 - c$ mit $c \in \mathbf{Z}$ und nicht Quadratzahl; ist die Primzahl $p \neq 2$ kein Teiler von c und ist das Legendre-Symbol $\left(\frac{c}{p}\right)$ gleich $+1$, so zerfällt $X^2 - c$ über $\mathbf{Q}_p$, aber nicht über $\mathbf{Q}$, in Linearfaktoren $(X - \xi)(X - \eta)$. Nun lasse man einen Computer ein hinreichend langes Anfangsstück der p-Kettenbruchentwicklung für eines der $\xi, \eta \in \mathbf{Q}_p$ berechnen. In den Fällen $(p, c) = (5, -1)$, $(7, 2)$, $(11, 5)$, $(13, 3)$ wurden jeweils die ersten fünfhundert Elemente a_ν, b_ν des p-Kettenbruchs tatsächlich ermittelt; dabei zeichnete sich in keinem Fall eine Periodizität ab. Diese Rechnungen wurden auf der Anlage CYBER 76/72 von Control Data am Rechenzentrum der Universität zu Köln durch Herrn Dr. M. Pohst durchgeführt, der auch das Programm geschrieben hat und dem an dieser Stelle nochmals gedankt sei.

P. Bundschuh, Universität Köln

LITERATUR

[1] S.I. Borewicz und I.R. Šafarevič, *Zahlentheorie,* Birkhäuser-Verlag, Basel/Stuttgart, 1966.
[2] K. Mahler, *On a geometrical representation of p-adic numbers,* Ann. of Math. *41*, 8–56 (1940).
[3] K. Mahler, *Lectures on diophantine approximations* (Part 1), University of Notre Dame, 1961.
[4] O. Perron, *Die Lehre von den Kettenbrüchen,* 2.Aufl., 1929; Repr. by Chelsea Publ. Comp., New York, N.Y.
[5] Th. Schneider, *Über p-adische Kettenbrüche,* Symposia Math. Vol. IV, 181–189 (1970).

Aufgaben

Aufgabe 761. In einer Ebene seien ein Dreieck ABC sowie ein Punkt P gegeben. $A'B'C'$ bezeichne das aus ABC durch Punktspiegelung an P entstehende Dreieck. Eine durch P verlaufende Gerade schneide $B'C'$ in A_1, $C'A'$ in B_1, $A'B'$ in C_1. Man zeige, dass sich die Geraden AA_1, BB_1, CC_1 in einem Punkt schneiden.

G. Bercea, München, BRD