

# UEBER EINE KLASSEN-EINTEILUNG DER P-ADISCHEN ZAHLEN.

VON

KURT MAHLER.

(In Groningen).

---

In meiner Arbeit: „Zur Approximation der Exponentialfunktion und des Logarithmus I“ (1931), Journal f. d. r. u. angew. Mathematik, 166, S. 118—136, machte ich Gebrauch von einer einfachen Klassen-Einteilung der komplexen Zahlen nach ihrer Fähigkeit, sich durch algebraische Zahlen mehr oder weniger gut annähern zu lassen (S. 120—122). Ueber diese Klassen-Einteilung teilte ich dort ohne Beweis einige Sätze mit, die die Invarianz dieser Einteilung bei dem Uebergang von einer Zahl zu irgend einer algebraisch abhängigen zeigten.

Es hat vielleicht doch Interesse, die an sich fast trivialen Beweise dieser Sätze zu veröffentlichen. Da jedoch fast dieselben Methoden sowohl im Körper der komplexen Zahlen, als auch im Körper der  $p$ -adischen Zahlen durchführbar sind und zu ganz analogen Ergebnissen führen, so möchte ich in der vorliegenden Note (die ich im Sommer 1932 schrieb) die Klassen-Einteilung allein für den Körper der  $p$ -adischen Zahlen darstellen; nur mache ich bei jedem Satz auf sein Analogon im Körper der komplexen Zahlen aufmerksam. Eine entsprechende Klasseneinteilung ist weiter noch möglich in dem Körper aller Potenzreihen einer Veränderlichen, und überhaupt in jedem Körper, in dem sich eine Theorie der Diophantischen Approximationen entwickeln lässt.

## I.

1. Sei  $\mathfrak{K}$  der Körper aller rationalen,  $\mathfrak{Z}$  der Ring aller ganzen rationalen Zahlen, ferner  $p$  eine feste Primzahl und  $\mathfrak{P}$  der Körper aller  $p$ -adischen Zahlen über  $\mathfrak{K}$ . Mit kleinen griechischen Buchstaben sollen Zahlen aus  $\mathfrak{P}$ , mit kleinen lateinischen solche aus  $\mathfrak{K}$  oder  $\mathfrak{Z}$  bezeichnet werden.

Im Folgenden wird von zwei verschiedenen Bewertungen

der Zahlen in  $\mathfrak{R}$  und in  $\mathfrak{S}$  Gebrauch gemacht. Allen Zahlen in  $\mathfrak{R}$  kann als Wert ihr absoluter Betrag zugeordnet werden; dieser werde mit

$$|a|$$

bezeichnet. Wenn allgemeiner  $P(x_1, x_2, \dots, x_n)$  ein Polynom in endlichvielen Unbestimmten mit Koeffizienten aus  $\mathfrak{R}$  ist, so bedeute

$$\overline{P(x_1, x_2, \dots, x_n)}$$

das genaue Maximum der Absolutbeträge der Koeffizienten von  $P(x_1, x_2, \dots, x_n)$ .

Sei dagegen  $a \neq 0$  eine  $p$ -adische Zahl; dann gibt es eine ganze rationale Zahl  $h$ , so dass  $ap^{-h}$  eine Einheit in  $\mathfrak{B}$  ist; jetzt werde  $\alpha$  der Wert

$$|\alpha|_p = p^{-h} \quad (|0|_p = 0)$$

zugesprochen. Für Zahlen  $\neq 0$  aus  $\mathfrak{S}$  gilt die Ungleichung:

$$|a|_p \geq |a|^{-1}.$$

Während die Bewertung  $|a|$  Archimedisch ist, ist die Bewertung  $|a|_p$  nicht-Archimedisch. Dadurch treten bei den folgenden Untersuchungen merkwürdige Abweichungen gegenüber dem Falle der gewöhnlichen komplexen Zahlen auf.

**2.** Es liegt nahe, eine Zahl  $\alpha$  algebraisch zu nennen, wenn es ein Polynom  $P(x)$  mit Koeffizienten aus  $\mathfrak{S}$  gibt, so dass

$$P(x) \equiv 0, \quad P(\alpha) = 0$$

ist; wenn dagegen kein solches Polynom existiert, heisse die Zahl transzendent. Es ist empfehlenswert, diese Bezeichnungsweise mit Hilfe der Bewertung schärfer zu fassen:

Zu einer gegebenen Zahl  $\alpha$  werde die Gesamtheit aller Polynome  $P(x)$  von höchstens  $m$ -tem Grade mit Koeffizienten aus  $\mathfrak{S}$  und

$$\overline{P(x)} \leq a$$

betrachtet, wo  $m$  und  $a$  zwei natürliche Zahlen sind. Wenn jedem der Polynome  $P(x)$  die Zahl  $P(\alpha)$  aus  $\mathfrak{B}$  zugeordnet wird, so können diese endlichvielen Zahlen  $P(\alpha)$  nicht alle gleich Null sein. Es gibt also eine unter ihnen, vielleicht auch mehrere, so dass der Wert  $|P(\alpha)|_p \neq 0$  möglichst klein ist. Dann werde dieses Minimum mit

$$\omega_m(a | \alpha) = \min_{\substack{|\overline{P(x)}| \leq a \\ P(\alpha) \neq 0}} (|P(\alpha)|_p)$$

bezeichnet. Es ist klar, dass

$$0 < \omega_m(a | \alpha) \leq 1$$

ist, denn für das Polynom  $P(x) \equiv 1$  ist ja  $|P(\alpha)|_p = 1$ . Weiter ist offenbar  $\omega_m(a | \alpha)$  bei festem  $m$  eine monoton abnehmende Funktion von  $a$  und bei festem  $a$  eine monoton abnehmende Funktion von  $m$ . Der obere Grenzwert

$$\omega_m(a) = \overline{\lim}_{a \rightarrow \infty} \frac{\log \frac{1}{\omega_m(a | \alpha)}}{\log a}$$

ist jedenfalls als nichtnegative, endliche oder unendliche Zahl vorhanden und selbst eine monoton zunehmende Funktion von  $m$ . Entweder gibt es eine kleinste natürliche Zahl  $\mu(\alpha)$ , so dass alle Ausdrücke

$$\omega_m(a) \text{ mit } m < \mu(\alpha)$$

endlich und alle Ausdrücke

$$\omega_m(a) \text{ mit } m \geq \mu(\alpha)$$

unendlich gross sind, oder alle Ausdrücke

$$\omega_m(a) \quad (m = 1, 2, \dots)$$

müssen gleichzeitig endlich sein; alsdann werde  $\mu(\alpha) = \infty$  gesetzt. Der Ausdruck

$$\omega(a) = \overline{\lim}_{m \rightarrow \infty} \frac{\omega_m(a)}{m},$$

der eine nichtnegative, endliche oder unendliche Zahl darstellt, ist daher nicht gleichzeitig mit  $\mu(\alpha)$  endlich.

Jetzt werde definiert:

Eine Zahl  $a$  mit  $\omega(a) = 0$ ,  $\mu(a) = \infty$  heisse A-Zahl.

Eine Zahl  $a$  mit  $0 < \omega(a) < \infty$ ,  $\mu(a) = \infty$  heisse S-Zahl.

Eine Zahl  $a$  mit  $\omega(a) = \infty$ ,  $\mu(a) = \infty$  heisse T-Zahl.

Eine Zahl  $a$  mit  $\omega(a) = \infty$ ,  $\mu(a) < \infty$  heisse U-Zahl.

**3.** Sei  $\alpha$  algebraisch; es gibt also ein in  $\mathfrak{F}$  irreduzibles Polynom

$Q(x) = A_0 + A_1 x + \dots + A_M x^M$ ;  $A_M \neq 0$ ,  $|\overline{Q(x)}| = A \geq 1$  mit Koeffizienten aus  $\mathfrak{F}$  etwa genau vom Grad  $M$ , so dass

$$Q(\alpha) = 0$$

ist; jedes andere Polynom  $Q^*(x)$  mit der Nullstelle  $\alpha$  und Koeffizienten aus  $\mathfrak{F}$  ist durch  $Q(x)$  teilbar.

Sei

$$P(x) = a_0 + a_1x + \dots + a_mx^m, \quad a = \overline{P(x)} \geq 1$$

ein beliebiges Polynom  $m$ -ten Grades mit Koeffizienten aus  $\mathfrak{F}$ . Nach der vorigen Bemerkung ist nur dann  $P(\alpha) = 0$ , wenn  $P(x)$  durch  $Q(x)$  teilbar ist. Setzt man also  $P(\alpha) \neq 0$  voraus, so ist das Polynom  $P(x)$  zu dem Polynom  $Q(x)$  teilerfremd, die Resultante

$$d = \begin{vmatrix} a_0a_1 & \dots & a_m \\ & a_0a_1 & \dots & a_m \\ A_0A_1 & \dots & A_M \\ & A_0A_1 & \dots & A_M \end{vmatrix}$$

daher von Null verschieden, ferner Zahl aus  $\mathfrak{F}$ . Aus der Gestalt der Determinante erhält man die Ungleichung

$$|d| \leq (M + m)! A^m a^M$$

oder, wenn  $d$  als Zahl aus  $\mathfrak{F}$  betrachtet wird:

$$|d|_p \geq \{(M + m)! A^m a^M\}^{-1}.$$

Führt man die beiden Polynome

$$p(x) = \begin{vmatrix} 1 & a_1 & \dots & a_m \\ \vdots & \vdots & \ddots & \vdots \\ x^{M-1} & a_0 & a_1 & \dots & a_m \\ 0 & A_1 & \dots & A_M \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & A_0A_1 & \dots & A_m \end{vmatrix} \quad \text{und} \quad q(x) = \begin{vmatrix} 0 & a_1 & \dots & a_m \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & a_0a_1 & \dots & a_m \\ 1 & A_1 & \dots & A_M \\ \vdots & \vdots & \ddots & \vdots \\ x^{M-1} & A_0A_1 & \dots & A_M \end{vmatrix}$$

ein, so besteht die Identität:

$$P(x) p(x) + Q(x) q(x) = d$$

In dieser Beziehung sind  $p(x)$  und  $q(x)$  Polynome in  $x$ ;  $p(x)$  ist vom Grad  $M-1$  und beide Polynome haben Koeffizienten aus  $\mathfrak{F}$ . Wird in der Identität für  $x$  der Wert  $\alpha$  eingesetzt, so erhält man:

$$P(\alpha) = \frac{d}{p(\alpha)}.$$

Der Zähler wurde bereits nach unten abgeschätzt; wenn ferner

$$|\alpha|_p = p^{-h}, \quad t = \min(0, h)$$

ist, so muss offenbar

$$|\phi(a)|_p \leq \phi^{-(M-1)t}$$

sein, und man gelangt zu der Ungleichung:

$$|\mathbf{P}(a)|_p \geq \{(M+m)! A^m a^{M\lambda-1} \phi^{(M-1)t}.$$

Dieser Ungleichung entnimmt man sofort folgendes Ergebnis:

Satz 1: Für eine algebraische Zahl  $a$  aus  $\mathfrak{K}$ , die in Bezug auf  $\mathfrak{R}$  den Grad  $M$  besitzt, ist

$$\omega_m(a) \leq M, \quad \omega(a) = 0, \quad \mu(a) = \infty;$$

jede algebraische Zahl aus  $\mathfrak{K}$  ist daher  $A$ -Zahl.<sup>1)</sup>

4. Möge weiter  $a$  nicht algebraisch von  $m$ -tem oder niederem Grade sein. Das Polynom mit Koeffizienten aus  $\mathfrak{K}$ :

$$\mathbf{P}(x) = a_0 + a_1 x + \dots + a_m x^m$$

besitzt also nur dann  $a$  als Nullstelle, wenn es identisch verschwindet.

Man lasse die Koeffizienten  $a_0, a_1, \dots, a_m$  der Reihe nach alle Zahlen

$$0, 1, \dots, a$$

durchlaufen; ihnen entsprechen insgesamt

$$N = (a+1)^{m+1}$$

verschiedene Polynome  $\mathbf{P}_l(x)$  mit  $l = 1, 2, \dots, N$ . Sei ferner

$$|a|_p = \phi^{-h}, \quad t = \min(0, h)$$

gesetzt. Jeder der  $N$  Ausdrücke

$$\phi^{-mt} \mathbf{P}_l(a) = \beta_l \quad (l = 1, 2, \dots, N)$$

ist also eine ganze  $\phi$ -adische Zahl. Sei  $f$  diejenige natürliche Zahl, für welche

$$\phi^f < N \leq \phi^{f+1}$$

ist. Alsdann werde jeder der Zahlen  $\beta_l$  diejenige natürliche Zahl  $\mathbf{P}_l$  aus der Reihe der Zahlen

$$0, 1, 2, 3, \dots, \phi^f - 1$$

zugeordnet, für die

$$\mathbf{P}_l \equiv \beta_l \pmod{\phi^f}$$

1) Wenn die Definitionen in 1. und 2. in sinngemässer Weise auf den Körper  $\mathfrak{K}$  der komplexen Zahlen übertragen werden, so lautet Satz 1 in  $\mathfrak{K}$ :

$$\omega_m(a) \leq \frac{M - \sigma(a)}{\sigma(a)}, \quad \omega(a) = 0, \quad \mu(a) = \infty.$$

Dabei bedeutet  $\sigma(a)$  die Zahl Eins, wenn  $a$  reell, und die Zahl Zwei, wenn  $a$  nichtreell ist.

ist und

$$\beta_l = P_l + \gamma_l p^f \quad (l = 1, 2, \dots, N)$$

gesetzt; auch  $\gamma_l$  ist eine ganze Zahl aus  $\mathfrak{P}$ . Wegen der Wahl von  $f$  müssen nach dem Schubkasten-Prinzip mindestens zwei der Zahlen  $P_l$  einander gleich sein, etwas  $P_{l_1} = P_{l_2}$ . Dann werde

$$P_{l_1}(x) - P_{l_2}(x) = P(x), \quad \gamma_{l_1} - \gamma_{l_2} = \gamma$$

gesetzt, so dass

$$0 \leq \overline{|P(x)|} \leq a, \quad p^{-mt} P(a) = p^f \gamma$$

ist. Aus der Wahl von  $f$  folgt also, dass die Ungleichung

$$|P(a)|_p \leq p^{-mt+1}(a+1)^{-m-1}, \quad P(x) \equiv 0$$

sich lösen lässt, welchen Wert  $m$  und  $a$  auch haben. Dies kann folgendermassen ausgesprochen werden:

*Satz 2: Wenn die Zahl  $\alpha$  nicht algebraisch von  $m$ -tem oder niederem Grade ist, so bestehen die Relationen:*

$$\omega_m(a | \alpha) \leq C_0 a^{-m-1}, \quad \omega_m(\alpha) \geq m + 1,$$

wobei  $C_0$  eine positive Konstante ist, die von  $a$  nicht abhängt. <sup>1)</sup>

Hieraus und aus Satz 1 ergibt sich, dass für algebraische Zahlen von genau  $M$ -tem Grade die Beziehungen

$$m+1 \leq \omega_m(\alpha) \leq M \text{ für } m \leq M-2; \quad \omega_m(\alpha) = M \text{ für } m \geq M-1$$

gelten. Es bleibt also noch ungewiss, welchen Wert die Zahlen

$$\omega_m(\alpha) \quad (m = 1, 2, \dots, M-2)$$

besitzen.

Für transzendente Zahlen dagegen ist für jedes  $m$

$$\omega_m(\alpha) \geq m + 1; \quad \omega(\alpha) \geq 1.$$

Man sieht also, dass alle transzendenten Zahlen entweder S-Zahlen oder T-Zahlen oder U-Zahlen sind, dagegen niemals A-Zahlen; diese sind genau mit den algebraischen Zahlen

1) Für  $\alpha$  in  $\mathfrak{K}$  wird statt dessen

$$\omega_m(\alpha) \geq \frac{m-1}{\sigma(\alpha)} + 1$$

und also speziell für transzendente Zahlen  $\alpha$ :

$$\omega(\alpha) \geq \frac{1}{\sigma(\alpha)},$$

und demnach ist für transzendente Zahlen insbesondere:

$$\omega(\alpha) \geq 1 \text{ für reelles } \alpha, \quad \omega(\alpha) \geq \frac{1}{2} \text{ für nichtreelles } \alpha.$$

Diese unteren Schranken werden wirklich angenommen, denn man hat

$$\omega(e) = 1, \quad \omega(ie) = \frac{1}{2}.$$

Ob im  $p$ -adischen Körper die entsprechende untere Schranke  $\omega(\alpha) = 1$  auch erreicht wird, ist bisher nicht bekannt.

identisch. Schärfer lässt sich folgendes Transzendenz-Kriterium aussprechen :

Satz 3: Eine Zahl  $\alpha$  ist dann und nur dann transzendent, wenn zu jeder noch so grossen natürlichen Zahl  $\Omega$  eine natürliche Zahl  $m$  und dazu unendlichviele Polynome von höchstens  $m$ -tem Grade  $P(x) \equiv 0$  mit Koeffizienten aus  $\mathfrak{F}$  existieren, so dass

$$0 < |P(\alpha)| \leq \overline{P(x)}^{-\Omega}$$

ist.

Es sei noch auf die merkwürdige Tatsache hingewiesen, dass die arithmetische Funktion  $\omega(a)$  alle Werte des beiderseits offenen Intervalles  $(0, 1)$  auslässt. Die untere Grenze wird von allen algebraischen Zahlen und nur von ihnen angenommen.

5. Der Sinn der Einteilung der transzendenten Zahlen in S-Zahlen, T-Zahlen und U-Zahlen wird durch den folgenden einfachen Invariansatz nachgewiesen.

Seien  $\alpha$  und  $\beta$  zwei transzendent Zahlen, die von einander algebraisch abhängig sind. Es gibt demnach eine in  $\mathfrak{R}$  irreduzible Gleichung mit Koeffizienten aus  $\mathfrak{F}$ :

$$Q(\alpha, \beta) = 0; \quad Q(x, y) = \sum_{h=0}^M \sum_{k=0}^N A_{hk} x^h y^k; \quad \overline{Q(x, y)} \geq 1,$$

zwischen  $\alpha$  und  $\beta$ ; sie muss beide Grössen wirklich enthalten. Wenn  $P(x)$  ein Polynom  $m$ -ten Grades mit Koeffizienten aus  $\mathfrak{F}$ :

$$P(x) = a_0 + a_1 x + \dots + a_m x^m, \quad \overline{P(x)} = a \geq 1$$

ist, so müssen also  $P(x)$  und  $Q(x, y)$  teilerfremd sein; denn sonst wäre  $P(x)$  durch das irreduzible Polynom  $Q(x, y)$  in zwei Unbestimmten teilbar und das ist unmöglich. Also ist die Resultante

$$d(y) = \begin{vmatrix} a_0 & a_1 & \dots & a_m \\ & a_0 & a_1 & \dots & a_m \\ A_0(y) & A_1(y) & \dots & A_M(y) \\ & A_0(y) & A_1(y) & \dots & A_M(y) \end{vmatrix}; \quad \begin{aligned} A_h(y) &= \sum_{k=0}^N A_{hk} y^k, \\ A_M(y) &\equiv 0 \end{aligned}$$

nicht identisch in  $y$  gleich Null. Offenbar hat  $d(y)$  die Form

$$d(y) = \sum_{k=0}^{mN} d_k y^k$$

mit Koeffizienten aus  $\mathfrak{F}$ ; man sieht leicht, dass

$$\overline{d(y)} \leq C_0 a^M$$

ist, wobei  $C_0$  eine natürliche Zahl bedeutet, die nicht von  $a$  abhängt.

Die Resultante  $d(y)$  lässt sich darstellen in der Form

$$P(x)p(xy) + Q(xy)q(xy) = d(y),$$

wobei  $p(x,y)$  und  $q(x,y)$  die folgenden zwei Polynome sind:

$$p(x, y) = \begin{vmatrix} 1 & a_1 & \dots & a_m \\ x^{M-1} a_0 a_1 & \dots & a_m \\ 0 & A_1(y) & \dots & A_M(y) \\ 0 & A_0(y) & A_1(y) & \dots & A_M(y) \end{vmatrix};$$

$$q(x, y) = \begin{vmatrix} 0 & a_1 & \dots & a_m \\ 0 & a_0 a_1 & \dots & a_m \\ 1 & A_1(y) & \dots & A_M(y) \\ x^{m-1} A_0(y) & A_1(y) & \dots & A_M(y) \end{vmatrix}.$$

Setzt man in der vorigen Identität die Werte  $\alpha$  und  $\beta$  ein, so erhält man:

$$P(\alpha) = \frac{d(\beta)}{p(\alpha, \beta)}.$$

In dieser Gleichung ist offenbar der Nenner nach oben beschränkt durch

$$|p(\alpha, \beta)|_p \leq C_1^{-1},$$

wobei  $C_1^{-1}$  eine natürliche Zahl ist, die von  $a$  nicht abhängt. Der Zähler dagegen ist wegen der Transzendenz von  $\beta$  ungleich Null; erst recht wird

$$|d(\beta)|_p \geq \omega_{mN} (C_0 a^M | \beta)$$

und folglich

$$|P(\alpha)|_p \geq C_1 \omega_{mN} (C_0 a^M | \beta).$$

Diese Ungleichung muss gelten, wie auch das Polynom  $P(x)$  gewählt wird. Man darf folglich annehmen, dass gerade

$$|P(\alpha)|_p = \omega_m(a | \alpha)$$

ist und bekommt so die Ungleichung

$$\omega_m(a | \alpha) \geq C_1 \omega_{mN} (C_0 a^M | \beta),$$

die die Annäherungen von  $\alpha$  in Beziehung setzt zu denen von

$\beta$ . Man gewinnt aus dieser einen Ungleichung sofort die weiteren Ungleichungen:

$$\begin{aligned}\omega_m(a) &= \overline{\lim}_{a \rightarrow \infty} \frac{\log \frac{1}{\omega_m(a|\alpha)}}{\log a} \leq M \overline{\lim}_{a \rightarrow \infty} \frac{\log \frac{1}{\omega_{mN}(C_0 a^M \beta)}}{\log(C_0 a^M)} \leq \\ &\leq M \omega_{mN}(\beta), \\ \omega(a) &= \overline{\lim}_{m \rightarrow \infty} \frac{\omega_m(a)}{m} \leq MN \overline{\lim}_{m \rightarrow \infty} \frac{\omega_{mN}(\beta)}{mN} \leq MN \omega(\beta), \\ \mu(a) &\geq \frac{1}{N} \mu(\beta).\end{aligned}$$

Offenbar gelten ganz entsprechende Ueberlegungen, wenn  $\alpha$  und  $\beta$  vertauscht werden. Demnach lässt sich folgender Satz aussprechen:

Satz 4: Wenn die beiden Zahlen  $\alpha$  und  $\beta$  algebraisch voneinander abhängen, so dass zwischen ihnen etwa die irreduzible Gleichung

$$Q(\alpha\beta) = \sum_{h=0}^M \sum_{k=0}^N A_{hk} \alpha^h \beta^k = 0, \quad Q(xy) \equiv \equiv 0$$

mit Koeffizienten aus  $\mathfrak{S}$  besteht, so gelten die Ungleichungen:

$$\begin{aligned}\omega_m(a) &\leq M \omega_{mN}(\beta); & \omega_m(\beta) &\leq N \omega_{mM}(a), \\ \omega(a) &\leq MN \omega(\beta); & \omega(\beta) &\leq MN \omega(a), \\ \mu(a) &\leq M \mu(\beta); & \mu(\beta) &\leq N \mu(a).\end{aligned}$$

Zwei von einander algebraisch abhängige Zahlen  $\alpha$  und  $\beta$  sind also speziell immer gleichzeitig  $S$ -Zahl oder  $T$ -Zahl oder  $U$ -Zahl.<sup>1)</sup>

Besonders erwähnt sei der Fall, dass  $\alpha$  und  $\beta$  durch eine bilineare Gleichung

$$A_{00} + A_{10} \alpha + A_{01} \beta + A_{11} \alpha\beta = 0$$

mit Koeffizienten aus  $\mathfrak{S}$  verbunden sind; die Formeln

$$\omega_m(a) = \omega_m(\beta), \quad \omega(a) = \omega(\beta), \quad \mu(a) = \mu(\beta)$$

zeigen, dass in diesem Fall beide Zahlen sich völlig gleich bei Approximation durch algebraische Zahlen verhalten.

1) Die Funktional-Ungleichungen zwischen  $\omega(a)$ ,  $\mu(a)$  und  $\omega(\beta)$ ,  $\mu(\beta)$  gelten im Körper  $\mathfrak{K}$  ohne jede Aenderung; es lassen sich also dieselben Folgerungen ziehen.