Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1936
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0175
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0175

LOG Id: LOG_0007
LOG Titel: Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung.
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Zur Theorie der abstrakten elliptischen Funktionenkörper I.
Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung.

Von *Helmut Hasse* in Göttingen.

In meiner der Riemannschen Vermutung für einen elliptischen Funktionenkörper mit endlichem Konstantenkörper gewidmeten Arbeit [1]) habe ich eine ausführliche Darstellung dieses Gegenstandes in diesem Journal in Aussicht gestellt. Es ist mir inzwischen gelungen, den Aufbau der ganzen Theorie und insbesondere den Beweis der Riemannschen Vermutung ganz erheblich zu vereinfachen. Eine vorläufige Mitteilung darüber habe ich in den Göttinger Nachrichten 1935 erscheinen lassen. Ich gebe hier die in Aussicht gestellte ausführliche Darstellung.

Mit Hinblick auf die Aufgabe der Verallgemeinerung der ganzen Theorie auf beliebiges Geschlecht g vermeide ich es absichtlich, soweit nur irgend möglich, spezielle explizite Formeln oder Kenntnisse über elliptische Körper auszunutzen, selbst wenn dadurch die Beweise für den nur am elliptischen Fall Interessierten reichlich abstrakt erscheinen. Als vorläufig ausreichender Prüfstein für die anzustrebende Verallgemeinerungsfähigkeit hat mir die durchgängige zwanglose Einbeziehung des Falles der Charakteristik $p = 2$ gedient, den ich früher wegen der Abweichungen in der Erzeugung durch eine Normalform ausschließen mußte. Insbesondere brauche ich nirgends auf die expliziten Formeln des Additionstheorems zurückzugreifen, sondern komme mit dessen impliziter Darstellung durch eine Determinantenrelation sowie mit seiner Verankerung in der Multiplikation der Divisorenklassen aus. Der ganze Aufbau der Theorie hat jetzt rein strukturellen Charakter. Es werden keinerlei sogenannte Abschätzungen mehr vorgenommen. Auch fällt die Anwendung des Dirichletschen Einheitensatzes fort. In meiner vorläufigen Mitteilung trat an seine Stelle der Struktursatz von Ostrowski über archimedisch bewertete Körper. In einer daran anschließenden Note ist es Herrn Behrbohm gelungen, ohne diesen Struktursatz auszukommen. Durch seinen Beweis, den ich mit formalen Vereinfachungen durch Herrn Teichmüller hier aufnehmen werde, wird auch der letzte Rest des transzendenten Grenzwertbegriffs beseitigt; der gesamte Aufbau der Theorie hat nunmehr formal-algebraischen Charakter.

Ich beginne in diesem Teil I mit einem neuen Beweis des Satzes über die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. An Stelle des früher für diesen Beweis benutzten induktiven Verfahrens, verwende ich hier eine Schlußweise, die aus der Theroie der Weierstraßpunkte geläufig ist, nämlich die Betrachtung von Differential-

[1]) H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Hamburg **10** (1934), 325—348.

determinanten. Dabei stütze ich mich auf die in der vorstehenden Arbeit frei von Charakteristikeinschränkungen entwickelte Theorie der höheren Differentiale.

Das früher in diesem Beweis benutzte induktive Verfahren werde ich später in verallgemeinerter Form zur Herleitung der grundlegenden Normenidentität im Meromorphismenring entwickeln. Ich übersehe im Augenblick noch nicht, ob sich der in diesem ersten Teil gegebene mehr rechnerische Beweis nicht vielleicht doch ganz erübrigen läßt, vorläufig jedenfalls kann ich seine Vorwegnahme für gewisse Schlüsse in den folgenden Teilen nicht entbehren.

In einem weiteren Teil II werde ich die Theorie der Automorphismen und Meromorphismen, sowie das Additionstheorem entwickeln, und in einem letzten Teil III dann die Struktur des Meromorphismenrings untersuchen und die Riemannsche Vermutung beweisen.

1. Es handelt sich hier um den Beweis des folgenden Satzes:

Sei K ein algebraischer Funktionenkörper einer Unbestimmten vom Geschlecht 1 über einem algebraisch-abgeschlossenen Konstantenkörper k der Charakteristik p ($= 0$ oder Primzahl).

Für die Anzahl h_n der Divisorenklassen C von K mit $C^n = 1$ gilt dann:

$$(1) \qquad h_n = n^2, \quad \text{wenn} \quad n \not\equiv 0 \bmod p;$$

$$(2) \qquad \left.\begin{matrix} h_n = n\,, & \text{wenn} & n = p^\nu & \text{und} & A \neq 0 \\ h_n = 1\,, & \text{wenn} & n = p^\nu & \text{und} & A = 0 \end{matrix}\right\} \qquad (p \neq 0).$$

Dabei ist A folgendermaßen erklärt: Ist $\mathfrak{p}$ irgendein Primdivisor von K und π ein (lokales) Primelement zu $\mathfrak{p}$, so gilt für das bis auf eine additive Konstante eindeutig bestimmte ganze Multiplum v von $\frac{1}{\mathfrak{p}^p}$ mit

$$v \equiv \frac{1}{\pi^p} \bmod \frac{1}{\mathfrak{p}}$$

genauer

$$v \equiv \frac{1}{\pi^p} - \frac{A}{\pi} \bmod \mathfrak{p}^0$$

mit A in k. Wie an anderer Stelle [2]) gezeigt wurde, ist die Klasse von A im Sinne der

---

[2]) Siehe dazu: 1. H. Hasse, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p, Journ. f. Math. **172** (1934), 77—85. 2. H. Hasse—E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p; erscheint demnächst in den Monatsh. f. Math. u. Phys. (Wirtinger-Festschr.).

Der in der letzteren Arbeit für beliebiges Geschlecht g gegebene Invarianzbeweis für die entsprechende g-reihige Matrix A bei Transformationen $\bar{A} = SAS^{-p}$ (S regulär, in k) stellt sich im hier vorliegenden Spezialfall $g = 1$ einfach so dar: Ist w das wesentlich einzige ganze Multiplum von $\frac{1}{\mathfrak{p}\bar{\mathfrak{p}}}$ ($\bar{\mathfrak{p}} \neq \mathfrak{p}$) mit

$$w \equiv \frac{1}{\pi} \bmod \mathfrak{p}^0,$$

so ist

$$w \equiv -\frac{S}{\bar{\pi}} \bmod \bar{\mathfrak{p}}^0$$

mit $S \neq 0$ aus k. Dann ist

$$\bar{v} = (v - w^p + Aw)\, S^{-p}$$

Transformationen $\bar{A} = A\,S^{1-p}$ ($S \neq 0$, in k), also die Alternative $A \neq 0$ oder $A = 0$ von der Wahl von $\mathfrak{p}$, π unabhängig, also eine Invariante von K.

Durch den obigen Satz wird ersichtlich die Struktur der Gruppe aller Divisorenklassen endlicher Ordnung von K vollständig beschrieben; für den Fall, daß k der absolut-algebraische algebraisch-abgeschlossene Körper der Primzahlcharakteristik p ist, ist damit die Struktur der Gruppe aller Divisorenklassen nullten Grades, und dann natürlich auch der Gruppe aller Divisorenklassen von K überhaupt bestimmt.

2. Zum Beweis des Satzes sei $\mathfrak{o}$ ein beliebiger Primdivisor von K. Nach dem Riemann-Rochschen Satz ist für jede Divisorenklasse C nullten Grades von K $\dim C(\mathfrak{o}) = 1$, also C durch einen Quotienten $\frac{\mathfrak{p}}{\mathfrak{o}}$ eindeutig repräsentierbar; umgekehrt repräsentiert natürlich jeder solche Quotient $\frac{\mathfrak{p}}{\mathfrak{o}}$ eine Divisorenklasse C nullten Grades. Die C mit $C^n = 1$ entsprechen dabei umkehrbar eindeutig den $\mathfrak{p}$ mit $\frac{\mathfrak{p}^n}{\mathfrak{o}^n} \sim 1$, für die also $\frac{\mathfrak{p}^n}{\mathfrak{o}^n} \cong y$ ein Element aus K ist.

Um diese $\mathfrak{p}$, soweit $\neq \mathfrak{o}$, zu charakterisieren, wählen wir eine Basis $y_0 = 1, y_1, \ldots, y_{n-1}$ der ganzen Multipla von $\frac{1}{\mathfrak{o}^n}$ in K; es ist ja $\dim(\mathfrak{o}^n) = n$. Ein nicht-konstantes ganzes Multiplum

$$y = c_0 y_0 + c_1 y_1 + \cdots + c_{n-1} y_{n-1} \quad \begin{pmatrix} c_0, c_1, \ldots, c_{n-1} \text{ in } k \\ c_1, \ldots, c_{n-1} \text{ nicht alle } 0 \end{pmatrix}$$

von $\frac{1}{\mathfrak{o}^n}$ ist dann und nur dann von der Form $y \cong \frac{\mathfrak{p}^n}{\mathfrak{o}^n}$, wenn ein Primdivisor $\mathfrak{p}$ von K derart existiert, daß für die lokalen Differentialquotienten

$$D_\pi^{(\varkappa)} y \equiv 0 \bmod \mathfrak{p} \qquad (\varkappa = 0, \ldots, n-1)$$

gilt; dabei bezeichnet π irgendein lokales Primelement zu $\mathfrak{p}$. Die fraglichen $\mathfrak{p}$ sind daher dadurch charakterisiert, daß für sie das Kongruenzensystem

$$D_\pi^{(\varkappa)} y = \sum_{i=0}^{n-1} c_i D_\pi^{(\varkappa)} y_i \equiv 0 \bmod \mathfrak{p} \qquad (\varkappa = 0, \ldots, n-1)$$

eine Lösung $c_0, c_1, \ldots, c_{n-1}$ in k mit nicht sämtlich verschwindenden $c_1, \ldots, c_{n-1}$ hat. Wegen $y_0 = 1$, also $D_\pi^{(0)} y_0 = 1, D_\pi^{(1)} y_0, \ldots, D_\pi^{(n-1)} y_0 = 0$ ist dafür notwendig und hinreichend, daß die Determinante

$$|D_\pi^{(\varkappa)} y_i| \equiv 0 \bmod \mathfrak{p} \qquad (i, \varkappa = 1, \ldots, n-1).$$

Nach dem in der vorstehenden Arbeit bewiesenen Satz ist nun

$$\mathfrak{d}_n \cong |D^{(\varkappa)} y_i| \qquad (i, \varkappa = 1, \ldots, n-1)$$

---

das wesentlich einzige ganze Multiplum von $\frac{1}{\bar{\mathfrak{p}}^p}$ mit

$$\bar{v} \equiv \frac{1}{\bar{\pi}^p} \bmod \frac{1}{\bar{\mathfrak{p}}},$$

und es ist

$$\bar{v} \equiv \frac{1}{\bar{\pi}^p} - \frac{A S^{1-p}}{\bar{\pi}} \bmod \bar{\mathfrak{p}}^0.$$

ein von der Wahl der Basis unabhängiger Divisor aus der $(1 + \cdots + (n-1))$-ten Potenz der Differentialklasse von K. Damit haben wir:

I. *Die Primdivisoren* $\mathfrak{p} \neq \mathfrak{o}$ *von* K *mit* $\frac{\mathfrak{p}^n}{\mathfrak{o}^n} \sim 1$ *sind genau die Zählerprimteiler des Differentialdivisors*

$$\mathfrak{d}_n \cong |D^{(\varkappa)} y_i| \qquad (i, \varkappa = 1, \ldots, n-1)$$

von K, *wo die* y_i *eine Basis der nicht-konstanten ganzen Multipla von* $\frac{1}{\mathfrak{o}^n}$ *in* K *sind.*

Die Anzahl der verschiedenen $\mathfrak{p}$ ergibt sich hiernach, wenn man zum Ausdruck bringt, daß $\mathfrak{d}_n$ den Grad 0 hat, weil die Differentialklasse von K den Grad 0 hat, und wenn man beachtet, daß der Nenner von $\mathfrak{d}_n$ nur eine Potenz von $\mathfrak{o}$ ist, weil die y_i, also auch die $D^{(\varkappa)} y_i$ diese Eigenschaft haben.

3. Unsere Behauptungen (1) und (2) werden auf Grund von I und der anschließenden Bemerkungen bewiesen sein, wenn folgendes gezeigt ist:

II 1. *Ist* $n \not\equiv 0$ *mod.* p, *so ist*

$$\mathfrak{d}_n = \frac{\mathfrak{z}_n}{\mathfrak{o}^{n^2-1}}$$

mit einem ganzen durch $\mathfrak{o}$ *nicht teilbaren Divisor* $\mathfrak{z}_n$, *der jeden seiner Primdivisoren* $\mathfrak{p}$ *genau zur Potenz* $\mathfrak{p}^1$ *enthält.*

Die $n^2 - 1$ verschiedenen Primdivisoren $\mathfrak{p}$ von $\mathfrak{z}_n$ bilden dann mit $\mathfrak{o}$ zusammen das volle System der Lösungen von $\frac{\mathfrak{p}^n}{\mathfrak{o}^n} \sim 1$.

II 2. *Ist* $n = p^\nu$ $(p \neq 0)$, *so ist für* $A \neq 0$

$$\mathfrak{d}_{p^\nu} = \frac{\mathfrak{z}_{p^\nu}}{\mathfrak{o}^{(p^\nu-1)p^\nu}}$$

mit einem ganzen durch $\mathfrak{o}$ *nicht teilbaren Divisor* $\mathfrak{z}_{p^\nu}$, *der jeden seiner Primdivisoren* $\mathfrak{p}$ *genau zur Potenz* $\mathfrak{p}^{p^\nu}$ *enthält.*

Für $A = 0$ *ist der Nenner von* $\mathfrak{d}_{p^\nu}$ *niedriger als* $\mathfrak{o}^{(p^\nu-1)p^\nu}$, *und etwaige Zählerbeiträge von* $\mathfrak{d}_{p^\nu}$ *wären höher als* $\mathfrak{p}^{p^\nu}$.

Für $A \neq 0$ bilden dann die $p^\nu - 1$ verschiedenen Primdivisoren $\mathfrak{p}$ von $\mathfrak{z}_{p^\nu}$ mit $\mathfrak{o}$ zusammen das volle System der Lösungen von $\frac{\mathfrak{p}^{p^\nu}}{\mathfrak{o}^{p^\nu}} \sim 1$.

Für $A = 0$ folgt, daß in Wahrheit $\mathfrak{d}_{p^\nu} = 1$ ist. Denn die Gradbilanz ergibt jedenfalls $h_{p^\nu} - 1 < p^\nu - 1$; wegen der gruppentheoretischen Bedeutung der h_{p^ν} folgt daraus speziell $h_p = 1$, also erst recht $h_{p^\nu} = 1$. Man beachte für die Gradbilanz, daß auch hier jedenfalls $\mathfrak{d}_{p^\nu} \neq 0$ ist, was in den anderen Fällen aus der Endlichkeit der Zählerbeiträge folgte. Wäre nämlich $\mathfrak{d}_{p^\nu} = 0$, so gälte nach I $\frac{\mathfrak{p}^{p^\nu}}{\mathfrak{o}^{p^\nu}} \sim 1$ für alle Primdivisoren $\mathfrak{p}$ von K, im Widerspruch zu der nach II 1 bereits feststehenden Existenz von Primdivisoren $\mathfrak{p} \neq \mathfrak{o}$ mit $\frac{\mathfrak{p}^n}{\mathfrak{o}^n} \sim 1$ für irgendein zu p primes n.

4. Zum Beweise von II 1 und II 2 gehen wir nach dem Muster der Theorie der Weierstraßpunkte vor [3]).

[3]) Siehe etwa Hensel-Landsberg, Theorie der algebraischen Funktionen einer Variabeln, Leipzig 1902, 489 ff.

Ist $\mathfrak{p}$ ein beliebiger Primdivisor von K und π ein zugehöriges lokales Primelement, so existiert eine für $\mathfrak{p}, \pi$ normierte Basis y_i der nicht-konstanten ganzen Multipla von $\frac{1}{\mathfrak{o}^n}$, nämlich derart, daß die π-adischen Entwicklungen der y_i folgendermaßen beginnen:

$$y_i = \pi^{\nu_i} + \cdots \qquad (i = 1, \ldots, n-1)$$

mit eindeutig bestimmten Exponenten

$$\nu_1 < \cdots < \nu_{n-1}.$$

Dann ist

$$D_\pi^{(\varkappa)} y_i = \binom{\nu_i}{\varkappa} \pi^{\nu_i - \varkappa} + \cdots,$$

und demnach

$$|D_\pi^{(\varkappa)} y_i| = \left|\binom{\nu_i}{\varkappa}\right| \pi^{\Sigma\nu_i - \Sigma\varkappa} + \cdots \qquad (i, \varkappa = 1, \ldots, n-1)$$

der Beginn der π-adischen Entwicklung der Determinante $|D_\pi^{(\varkappa)} y_i|$. Für die hier als Anfangskoeffizient auftretende Zahldeterminante ergibt sich ohne weiteres

$$\left|\binom{\nu_i}{\varkappa}\right| = \prod_i \frac{\nu_i}{i} \cdot \prod_{j>i} \frac{\nu_j - \nu_i}{j - i}.$$

a) Der Nenner von $\mathfrak{d}_n$ ($\mathfrak{p} = \mathfrak{o}$, $\pi = \omega$).

Die Dimensionsrelationen

$$\dim(\mathfrak{o}^i) = \begin{cases} 1 & (i = 0) \\ i & (i = 1, \ldots, n) \end{cases}$$

ergeben das Exponentensystem

$$(\nu_1, \ldots, \nu_{n-1}) = (-n, \ldots, -2), \text{ also } \nu_i = -n + i - 1.$$

Dafür ist

$$\Sigma\nu_i - \Sigma\varkappa = -(n^2 - 1), \quad \left|\binom{\nu_i}{\varkappa}\right| = (-1)^{n-1} n,$$

und somit

$$|D_\omega^{(\varkappa)} y_i| = (-1)^{n-1} n\, \omega^{-(n^2-1)} + \cdots.$$

Für $n \not\equiv 0 \bmod p$ ergibt das die Nennerbehauptung in II 1.

Für $n = p^\nu$ normieren wir $y_1 = \omega^{-p^\nu} + \cdots$ noch genauer. Sei w gemäß der Definition von A ein ganzes Multiplum von $\frac{1}{\mathfrak{o}^p}$ mit

$$w = \omega^{-p} - A\omega^{-1} + \cdots.$$

Dann hat das ganze Multiplum

$$w^{(\nu)} = w^{p^{\nu-1}} + A^{p^{\nu-1}} w^{p^{\nu-2}} + \cdots + A^{p^{\nu-1} + \cdots + p} w$$

von $\frac{1}{\mathfrak{o}^{p^\nu}}$ die Eigenschaft

$$w^{(\nu)} = \omega^{-p^\nu} - A^{(\nu)} \omega^{-1} + \cdots,$$

wo zur Abkürzung

$$A^{(\nu)} = A^{p^{\nu-1} + \cdots + p + 1}$$

gesetzt ist. $w^{(\nu)}$ ist also als erstes Basiselement y_1 geeignet.

Dann ist

$$D_\omega^{(\varkappa)} y_1 = \binom{-p^\nu}{\varkappa} \omega^{-p^\nu-\varkappa} - A^{(\nu)} \binom{-1}{\varkappa} \omega^{-1-\varkappa} + \cdots$$
$$= -A^{(\nu)} \binom{-1}{\varkappa} \omega^{-1-\varkappa} + \cdots,$$

weil nach dem Hilfssatz 1 am Schluß (Nr. 6)

$$\binom{-p^\nu}{\varkappa} = (-1)^\varkappa \binom{p^\nu - 1 + \varkappa}{\varkappa} \equiv 0 \bmod p \quad (\varkappa = 1, \ldots, p^\nu - 1)$$

gilt.

Hiernach treten für die Berechnung der ω-adischen Entwicklung der Determinante $|D^{(\varkappa)} y_i|$ nur folgende einfachen Änderungen ein: $\nu_1 = -p^\nu$ ist durch -1 zu ersetzen (dementsprechend erste Zeile an den Schluß) und der Koeffizient $A^{(\nu)}$ ist herauszuziehen. Man erhält so

$$|D_\omega^{(\varkappa)} y_i| = A^{(\nu)} \left|\binom{i-p^\nu}{\varkappa}\right| \omega^{-(p^{2\nu}-p^\nu)} + \cdots \quad (i, \varkappa = 1, \cdots, p^\nu - 1)$$
$$= A^{(\nu)} \omega^{-(p^\nu-1)p^\nu} + \cdots.$$

Das ergibt die Nennerbehauptung in II 2.

b) Der Zähler von $\mathfrak{d}_n$ ($\mathfrak{p}^n \sim \mathfrak{o}^n$, $\mathfrak{p} \neq \mathfrak{o}$).

Die Dimensionsrelationen

$$\dim \left(\frac{\mathfrak{o}^n}{\mathfrak{p}^i}\right) = \begin{cases} n-i & (i = 0, \ldots, n-1) \\ 1 & (i = n) \end{cases}$$

ergeben das Exponentensystem

$$(\nu_1, \ldots, \nu_{n-1}) = (1, \ldots, n-2, n), \text{ also } \nu_i = \begin{cases} i & (i = 1, \ldots, n-2) \\ n & (i = n-1) \end{cases}.$$

Dafür ist

$$\Sigma \nu_i - \Sigma \varkappa = 1, \quad \left|\binom{\nu_i}{\varkappa}\right| = n,$$

und somit

$$|D_\pi^{(\varkappa)} y_i| = n\pi + \cdots.$$

Für $n \not\equiv 0 \bmod p$ ergibt das die Zählerbehauptung in II 1.

Für $n = p^\nu$ müssen wir die Berechnung der π-adischen Entwicklung der Determinante $|D^{(\varkappa)} y_i|$ genauer anlegen. Wir können die ersten $p^\nu - 2$ Basiselemente y_i genauer so normieren:

$$y_i = \pi^i + b_i \pi^{p^\nu - 1} + \cdots \qquad (i = 1, \ldots, p^\nu - 2)$$

mit gewissen b_i aus k. Ferner sei genauer

$$y_{p^\nu-1} = \pi^{p^\nu} + \sum_{\lambda=1}^{p^\nu-1} c_\lambda \pi^{p^\nu+\lambda} + \cdots$$

mit gewissen c_λ aus k.

Dann ist

$$D_\pi^{(\varkappa)} y_i = \binom{i}{\varkappa} \pi^{i-\varkappa} + b_i \binom{p^\nu - 1}{\varkappa} \pi^{p^\nu-1-\varkappa} + \cdots \qquad (i = 1, \ldots, p^\nu - 2),$$

$$D_\pi^{(\varkappa)} y_{p^\nu-1} = \binom{p^\nu}{\varkappa} \pi^{p^\nu-\varkappa} + \sum_{\lambda=1}^{p^\nu-1} c_\lambda \binom{p^\nu + \lambda}{\varkappa} \pi^{p^\nu+\lambda-\varkappa} + \cdots.$$

Weil nun natürlich

$$\binom{i}{\varkappa} = \begin{cases} 0 & (i < \varkappa) \\ 1 & (i = \varkappa) \end{cases}$$

und nach den Hilfssätzen 1, 2 am Schluß (Nr. 6)

$$\binom{p^\nu + \lambda}{\varkappa} \equiv \begin{cases} 0 \bmod p & (0 \leqq \lambda < \varkappa) \\ 1 \bmod p & (\lambda = \varkappa) \end{cases} \qquad (\varkappa = 1, \ldots, p^\nu - 1)$$

gilt, ist die Matrix

$$(D_\pi^{(\varkappa)} y_i) \equiv \begin{pmatrix} 1 & 0 & \cdots & 0 & b_1 \\ 0 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & b_{p^\nu-2} \\ c_1 \pi^{p^\nu} & \cdots & c_{p^\nu-2}\pi^{p^\nu} & & c_{p^\nu-1}\pi^{p^\nu} \end{pmatrix} \bmod. \begin{pmatrix} \mathfrak{p} \\ \vdots \\ \mathfrak{p} \\ \mathfrak{p}^{p^\nu} \end{pmatrix},$$

also ihre Determinante

$$|D_\pi^{(\varkappa)} y_i| = (c_{p^\nu-1} - \sum_{\lambda=1}^{p^\nu-2} b_\lambda c_\lambda)\, \pi^{p^\nu} + \cdots .$$

Das ergibt die Zählerbehauptung in II 2 auf Grund des jetzt noch zu erbringenden Nachweises, daß

$$c_{p^\nu-1} - \sum_{\lambda=1}^{p^\nu-2} b_\lambda c_\lambda = A^{(\nu)}$$

in der schon früher auftretenden Bedeutung ist.

5. Um diesen letzteren Nachweis zu erbringen, sei $v^{(\nu)}$ zu $\mathfrak{p}$ entsprechend erklärt, wie oben $w^{(\nu)}$ zu $\mathfrak{o}$. Wegen der Invarianz von A ist also $v^{(\nu)}$ ein ganzes Multiplum von $\frac{1}{\mathfrak{p}^{p^\nu}}$ mit

$$v^{(\nu)} = \frac{1}{\pi^{p^\nu}} - \frac{A^{(\nu)}}{\pi} + \cdots .$$

Wegen $y_{p^\nu-1} \cong \frac{\mathfrak{p}^{p^\nu}}{\mathfrak{o}^{p^\nu}}$ ist dann $y_{p^\nu-1} v^{(\nu)}$ ein ganzes Multiplum von $\frac{1}{\mathfrak{o}^{p^\nu}}$; seine π-adische Entwicklung beginnt so:

$$y_{p^\nu-1} v^{(\nu)} = 1 + \sum_{\lambda=1}^{p^\nu-2} c_\lambda \pi^\lambda + (c_{p^\nu-1} - A^{(\nu)})\pi^{p^\nu-1} + \cdots .$$

Daraus folgt

$$y_{p^\nu-1} v^{(\nu)} - \sum_{\lambda=1}^{p^\nu-2} c_\lambda y_\lambda = (c_{p^\nu-1} - A^{(\nu)} - \sum_{\lambda=1}^{p^\nu-2} c_\lambda b_\lambda)\, \pi^{p^\nu-1} + \cdots .$$

Das Element links ist hiernach ein ganzes Multiplum von $\frac{1}{\mathfrak{o}^{p^\nu}}$ mit durch $\mathfrak{p}^{p^\nu-1}$ teilbarem Zähler. Wegen $\dim\left(\frac{\mathfrak{o}^{p^\nu}}{\mathfrak{p}^{p^\nu-1}}\right) = \dim\left(\frac{\mathfrak{o}^{p^\nu}}{\mathfrak{p}^{p^\nu}}\right) = 1$ für einen Zählerprimteiler $\mathfrak{p}$ von $\mathfrak{d}_{p^\nu}$ ist dann der Zähler sogar durch $\mathfrak{p}^{p^\nu}$ teilbar, d. h. die Klammer rechts ist gleich 0. Das ist die noch zu beweisende Behauptung.

6. *Hilfssätze über Binomialkoeffizienten.*

Hilfssatz 1. $\binom{i+k}{k} = \frac{(i+k)!}{i!\,k!} \equiv 0 \bmod p$ für $i + k \geqq p^\nu$; $i, k = 1, \ldots, p^\nu - 1$.

Beweis. Bekanntlich ist der Exponent der genauen Potenz von p in $n!$ gleich $\sum_{\varrho \geqq 1} \left[\frac{n}{p^\varrho}\right]$. Daher ist der Exponent der genauen Potenz von p in $\binom{i+k}{k}$ gleich

$$\sum_{\varrho \geqq 1} \left(\left[\frac{i+k}{p^\varrho}\right] - \left[\frac{i}{p^\varrho}\right] - \left[\frac{k}{p^\varrho}\right] \right).$$

Für jedes ϱ ist der Beitrag zu dieser Summe $\geqq 0$. Unter den gemachten Voraussetzungen über i, k liefert $\varrho = \nu$ einen Beitrag > 0.

Hilfssatz 2. $\binom{p^\nu + k}{k} \equiv 1 \bmod. p$ für $k = 1, \ldots, p^\nu - 1$.

Beweis.

$$\binom{p^\nu + k}{k} = \left(1 + \frac{p^\nu}{1}\right) \cdots \left(1 + \frac{p^\nu}{k}\right).$$

Eingegangen 16. Oktober 1935.