# Über den algebraischen Funktionenkörper der Fermatschen Gleichung.

LÁSZLÓ RÉDEI zum 50. Geburtstag.

Von HELMUT HASSE in Berlin.

## Einleitung.

Im Hinblick auf die große Fermatsche Vermutung erscheint es mir von Interesse, den durch die homogene Gleichung

$$x^n + y^n + z^n = 0$$

definierten algebraischen Funktionenkörper vom Standpunkt der allgemeinen Theorie der algebraischen Funktionenkörper einer Unbestimmten aus zu betrachten. In den zahlreichen bisher zugrunde gelegten Ansätzen zur Behandlung der Fermatschen Gleichung, angefangen von der descente infinie über elementare Kongruenzbetrachtungen bis zum Einsatz der Idealtheorie und des allgemeinen Reziprozitätsgesetzes, steckt nämlich jedesmal ein rein-algebraischer Kern, auf den sich dann die spezifisch-arithmetischen Schlüße aufbauen. Ebenso nun, wie etwa für den Aufbau der Arithmetik der Algebren die rein-algebraische Strukturtheorie der Algebren grundlegend und methodisch richtunggebend ist, scheint es mir auch beim Fermatschen Problem naturgemäß zu sein, sich für den rein-algebraischen Kern an den invarianten Begriffsbildungen und Struktursätzen hier der Theorie der algebraischen Funktionenkörper einer Unbestimmten zu orientieren. Soweit ich sehe, ist das bisher nirgends geschehen.

Die nachstehenden Betrachtungen sollen ein erster Beitrag in dieser Richtung sein. Ich lege dabei die Theorie der algebraischen Funktionenkörper einer Unbestimmten in ihrer arithmetischen Gestalt zugrunde[1]. Zunächst zeige ich, wie sich die trivialen Lösungen der Fermatschen Gleichung d. h. die, in denen eine Koordinate Null ist, in jene Theorie

[1] Insbesondere verwende ich ohne nachmalige Erklärung einige Begriffe und Ergebnisse aus meiner Arbeit: Zur arithmetischen Theorie der algebraischen Funktionskörper, *Jahresbericht der Deutschen Math.-Vereinigung*, **52** (1942), S. 1–48.

einordnen. Ferner bestimmte ich explizit den Modul der ganzen Differentiale, berechne mit seiner Hilfe einige für die algebraische Behandlung wichtige Dimensionszahlen und zeige, daß die durch die homogene Grundgleichung gegebenen Koordinaten die algebraischen Punkte des zugeordneten Funktionenkörpers eindeutig beschreiben. Weiter gehe ich auf die Frage nach den Weierstraßpunkten dieses Funktionenkörpers ein. Hier stellt sich die überraschende Tatsache heraus, daß neben den Punkten, die den trivialen Grundgleichunglösungen entsprechen, für $n > 4$ noch weitere Weierstraßpunkte existieren. Eine explizite Angabe dieser Punkte ist mir leider nicht gelungen; sie würde deswegen von Interesse sein, weil es sich ja dabei um algebraisch-ausgezeichnete algebraische Lösungen der Fermatschen Gleichung handelt. Schließlich mache ich noch einige Angaben zu einer weiteren wichtigen Fragestellung, nämlich der expliziten Bestimmung des additiven Rechenschemas der rationalen $g$-gliedrigen Punktgruppen, wo $g = 1 + 2 + \cdots + (n-2)$ das Geschlecht des Funktionenkörpers ist, und damit des Rechnens in der Divisorenklassengruppe nullten Grades. Daß dieses mit der Fermatschen Gleichung invariant verbundene Rechenschema sich in den bisherigen rein-algebraischen Ansätzen zur Behandlung des Fermatschen Problems noch niemals eingestellt hat, ist im Hinblick auf die Fülle solcher mehr oder weniger weittragenden Ansätze einigermaßen erstaunlich. Allerdings ist es ja erst durch die in neuerer Zeit von A. Weil[2]) bewiesene Endlichkeit des Ranges der Additionsgruppe der rationalen $g$-gliedrigen Punktgruppen nahegelegt worden, die rationalen Lösungen der Fermatschen Gleichung unter den rationalen $g$-gliedrigen Punktgruppen vermöge einer Basisdarstellung als diejenigen mit $g$ gleichen Punkten aufzusuchen.

## 1. Erzeugung.

Gegeben seien eine natürliche Zahl $n > 1$ (später sogar $n > 2$ und ein Körper $\Omega$, von dem einfachheitshalber vorausgesetzt sei, daß seine Charakteristik $\chi(\Omega) \nmid n$ (später sogar $\chi(\Omega) = 0$) ist[3]). Außerdem soll $\Omega$ die $2n$-ten Einheitswurzeln enthalten[4]) Betrachtet werde der durch die

[2]) A. Weil, L'arithmétique sur les courbes algébriques, *Acta Math.*, **52** (1928), S. 281—315.

[3]) Der hier ausgeschlossene Fall einer Primzahlcharakteristik $\chi(\Omega) | n$ würde weitere algebraische Invarianten liefern, wie sie etwa im Falle eines Primzahlgrades $n$ der vielfach herangezogenen Betrachtung der Fermatschen Gleichung als Kongruenz mod. $n$ entsprechen. Der Kürze des zur Verfügung stehenden Raumes halber muß ich hier von der Betrachtung dieses Falles absehen.

[4]) Es wäre keine wesentliche Einschränkung, wenn man $\Omega$ von vornherein mit dem Körper dieser Einheitswurzeln über dem Primkörper einer Charakteristik $\chi \nmid n$ identifiziert.

homogene Grundgleichung
$$x^n+y^n+z^n=0$$
definierte algebraische Funktionenkörper einer Unbestimmten
$$K=\Omega(x:y:z).$$
Wegen $\chi(\Omega) \not| n$ ist die Grundgleichung über $\Omega$ absolut irreduzibel, so daß $\Omega$ der genaue Konstantenkörper von $K$ ist.

Die homogenen Erzeugenden $x, y, z$ seien in $K$ selbst gewählt; sie liegen dann bis auf Homogonitätssubstitutionen
$$x, y, z \to \frac{x}{t}, \frac{y}{t}, \frac{z}{t}$$
mit willkürlichem $t \neq 0$ aus $K$ fest. Nach der allgemeinen Theorie der homogenen Erzeugung hat man
$$x \cong \frac{\mathfrak{A}}{\mathfrak{U}}, \quad y \cong \frac{\mathfrak{B}}{\mathfrak{U}}, \quad z \cong \frac{\mathfrak{C}}{\mathfrak{U}},$$
wo der Divisor $\mathfrak{U}$ von $K/\Omega$ durch die größte gemeinsame Teilerbeziehung
$$(x, y, z) = \frac{1}{\mathfrak{U}}$$
bestimmt ist und $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ganze teilerfremde Divisoren von $K/\Omega$ sind, die im Hinblick auf die Grundgleichung sogar paarweise teilerfremd sind.

Die Klasse $U$ von $\mathfrak{U}$ liegt durch die gegebene Erzeugung eindeutig fest. Bei Anwendung der Homogenitätssubstitutionen auf $x, y, z$ durchläuft $\mathfrak{U}$ alle Divisoren aus $U$, während die ebenfalls zu $U$ gehörigen Divisoren $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ungeändert bleiben. Wegen $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C}) = 1$ ist die Klasse $U$ primitiv, und wegen $n > 1$ sind die ganzen Divisoren $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ aus $\mathfrak{U}$ über $\Omega$ linear unabhängig, so daß jedenfalls
$$\dim U \geqq 3$$
ist.

Durch eine Homogenitätssubstitution auf $x, y, z$ kann $\mathfrak{U}$ als ganzer Divisor aus $U$ normiert werden, also so, daß $\mathfrak{U}$ der Hauptnenner von $x, y, z$ ist. Dies sei im folgenden durchweg vorausgesetzt; es sind dann nur noch Homogenitätssubstitutionen mit Faktoren der Form
$$t = ax + by + cz \qquad (a, b, c \neq 0, 0, 0 \text{ aus } \Omega)$$
zulässig. Durch eine solche kann man auch noch $\mathfrak{U}$ so normieren, daß etwa $\mathfrak{A}$ prim zu $\mathfrak{U}$ ist (etwa indem man $\mathfrak{U} = \mathfrak{C}$, also $z \cong 1$ wählt), oder auch daß ein vorgegebener algebraischer Punkte $\mathfrak{p}$ von $K/\Omega$ prim zu $\mathfrak{U}$ ist (so daß $x, y, z$ primitiv für $\mathfrak{p}$ sind). Hiervon wird im folgenden, wo nötig, Gebrauch gemacht. Die Zählerdivisoren $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ und die Verhältnisse $x:y:z$ werden, wie gesagt, von diesen Normierungen nicht betroffen, so daß die über sie herzuleitenden Aussagen unabhängig von solchen Normierungen sind.

Die Permutationen von $x, y, z$ und die Multiplikationen der $x, y, z$ mit (voraussetzungsgemäß in $\Omega$ enthaltenen) $n$-ten Einheitswurzeln liefern Automorphismen von $K/\Omega$, die zusammen eine endliche Automorphismengruppe $\mathfrak{G}$ von $K/\Omega$ erzeugen. Der Divisor $\mathfrak{U}$ und damit auch seine Klasse $U$ ist bei $\mathfrak{G}$ invariant.

## 2 Primzerlegung der Zählerdivisoren.

Wegen $[K:\Omega(y:z)] = n$ und $y:z \cong \mathfrak{B}:\mathfrak{C}$ mit $(\mathfrak{B}, \mathfrak{C}) = 1$ ist

$$\text{Grad}\, U = n.$$

Demnach besitzt der Zählerdivisor $\mathfrak{A}$ von $x$ eine Zerlegung

$$\mathfrak{A} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$$

in $n$ algebraische Punkte $\mathfrak{a}_\nu$ von $K/\Omega$. Es ist dann

$$y^n + z^n \cong x^n \cong \frac{\mathfrak{A}^n}{\mathfrak{U}^n} = \frac{\mathfrak{a}_1^n}{\mathfrak{U}} \cdots \frac{\mathfrak{a}_n^n}{\mathfrak{U}}.$$

Nun besteht die Linearfaktorzerlegung

$$y^n + z^n = (y - \varepsilon_1 z) \cdots (y - \varepsilon_n z),$$

wo $\varepsilon_1, \ldots, \varepsilon_n$ für $2 \nmid n$ die entgegengesetzten zu den $n$ ten Einheitswurzeln und für $2 | n$ diejenigen $2n$-ten Einheitswurzeln sind, die nicht schon $n$-te Einheitswurzeln sind; sie liegen voraussetzungsgemäß in $\Omega$ und sind wegen $\chi(\Omega) \nmid n$ untereinander verschieden. Für die ihnen entsprechenden Linearfaktoren hat man daher

$$y - \varepsilon_\nu z \cong \frac{\mathfrak{A}_\nu}{\mathfrak{U}} \qquad (\nu = 1, \ldots, n)$$

mit untereinander verschiedenen, also paarweise teilerfremden Primdivisoren ersten Grades $\mathfrak{A}_\nu$ des rationalen Körpers $\Omega(y:z)/\Omega$. Nach dem zuvor Gesagten hat deren Produkt in $K/\Omega$ die Primzerlegung

$$\mathfrak{A}_1 \cdots \mathfrak{A}_n = \mathfrak{a}_1^n \cdots \mathfrak{a}_n^n.$$

Bei passender Reihenfolge der $\mathfrak{a}_\nu$ ist somit notwendig

$$\mathfrak{A}_\nu = \mathfrak{a}_\nu^n \quad \text{und} \quad \mathfrak{a}_\nu = (\mathfrak{A}, \mathfrak{A}_\nu) \qquad (\nu = 1, \ldots, n).$$

Wegen der letzteren Beziehungen sind die $\mathfrak{a}_\nu$ untereinander verschieden und rationale Punkte (Primdivisoren ersten Grades) von $K/\Omega$; sie entsprechen den trivialen Grundgleichungslösungen

$$x(\mathfrak{a}_\nu) : y(\mathfrak{a}_\nu) : z(\mathfrak{a}_\nu) = 0 : \varepsilon_\nu : 1 \qquad (\nu = 1, \ldots, n)$$

mit erster Koordinate 0. Wegen der ersteren Beziehungen sind die $\mathfrak{A}_\nu$ für $K/\Omega(y:z)$ von der Ordnung $n$ verzweigt.

Entsprechendes gilt für die Primzerlegung der beiden anderen Zählerdivisoren

$$\mathfrak{B} = \mathfrak{b}_1 \cdots \mathfrak{b}_n, \quad \mathfrak{C} = \mathfrak{c}_1 \cdots \mathfrak{c}_n.$$

Insbesondere ist damit festgestellt:

*Den $3n$ durch die Automorphismengruppe $\mathfrak{G}$ von $K/\Omega$ transitiv verbundenen trivialen Grundgleichungslösungen entsprechen $3n$ ebenso verbundene rationale Punkte von $K/\Omega$, nämlich die je $n$ Primfaktoren $\mathfrak{a}_\nu$, $\mathfrak{b}_\nu$, $\mathfrak{c}_\nu$ der Zählerdivisoren $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ von $x$, $y$, $z$.*

## 3. Geschlecht, Differentialklasse, ganze Differentiale.

Wie aus der Grundgleichung ersichtlich, sind die Zählerdivisoren $\mathfrak{A}_\nu$ der $y-\varepsilon_\nu z$ auch die einzigen für $K/\Omega(y:z)$ verzweigten Primdivisoren von $\Omega(y:z)/\Omega$. Wegen $\chi(\Omega)\nmid n$ hat daher $K/\Omega(y:z)$ den Differentendivisor

$$\mathfrak{D}_{y:z} = \mathfrak{A}^{n-1}.$$

Da $z:y \cong \mathfrak{C}:\mathfrak{B}$ den Nennerdivisor $\mathfrak{B}$ hat, ist somit das Differential

$$d\left(\frac{z}{y}\right) = \frac{\begin{vmatrix} y & z \\ dy & dz \end{vmatrix}}{y^2} \cong \frac{\mathfrak{A}^{n-1}}{\mathfrak{B}^2}.$$

Hieraus bestimmen sich das Geschlecht $g$ und die Differentialklasse $W$ von $K/\Omega$ zu

$$2g-2 = n(n-1)-2n = n(n-3),$$

also

$$g = \frac{(n-1)(n-2)}{2} = 1+2+\cdots+(n-2)$$

und

$$W = U^{n-3}.$$

Um den trivialen Fall $n=2$ mit $g=0$ auszuschließen, sei fortan $n>2$ und damit $g>0$ vorausgesetzt.

Aus dem Gleichungssystem

$$\begin{aligned} x^{n-1}x + y^{n-1}y + z^{n-1}z &= 0, \\ x^{n-1}dx + y^{n-1}dy + z^{n-1}dz &= 0, \end{aligned}$$

letzteres unter Beachtung von $\chi(\Omega)\nmid n$, folgt

$$\begin{vmatrix} y & z \\ dy & dz \end{vmatrix} : \begin{vmatrix} z & x \\ dz & dx \end{vmatrix} : \begin{vmatrix} x & y \\ dx & dy \end{vmatrix} = x^{n-1} : y^{n-1} : z^{n-1}.$$

Hiernach und nach obiger Differentialformel ist das Differential

$$du = \frac{\begin{vmatrix} y & z \\ dy & dz \end{vmatrix}}{x^{n-1}} = \frac{\begin{vmatrix} z & x \\ dz & dx \end{vmatrix}}{y^{n-1}} = \frac{\begin{vmatrix} x & y \\ dx & dy \end{vmatrix}}{z^{n-1}} \cong \mathfrak{U}^{n-1}$$

von $K/\Omega$ bei der Automorphismengruppe $\mathfrak{G}$ invariant und ganz. Man erhält dann in der Gestalt

$$x^\lambda y^\mu z^\nu du \cong \mathfrak{A}^\lambda \mathfrak{B}^\mu \mathfrak{C}^\nu \qquad \begin{pmatrix} \lambda, \mu, \nu \geqq 0 \\ \lambda+\mu+\nu = n-3 \end{pmatrix}$$

über $\Omega$ linear unabhängige ganze Differentiale von $K/\Omega$ in der Anzahl

$$\sum_{\substack{\lambda,\mu,\nu\geqq 0\\ \lambda+\mu+\nu=n-3}}' 1=\sum_{\varkappa=0}^{n-3}\sum_{\substack{\lambda,\mu\geqq 0\\ \lambda+\mu=\varkappa}} 1=\sum_{\varkappa=0}^{n-3}(\varkappa+1)=g,$$

also eine Basis des $\Omega$-Moduls der ganzen Differentiale von $K/\Omega$. Daraus folgt:

*Die ganzen Differentiale von $K/\Omega$ sind die Gesamtheit der Ausdrücke*

$$f_{n-3}(x,y,z)\,du,$$

*wo $du$ die angegebene Bedeutung hat und $f_{n-3}$ alle homogenen ternären Polynome über $\Omega$ vom Grade $n-3$ durchläuft.*

### 4. Dimensionsformeln, homogene Koordinaten.

Die ganzen Differentiale von $K/\Omega$ lassen sich unter Hervorhebung der obigen Linearfaktoren

$$y_\nu=y-\varepsilon_\nu z \qquad (\nu=1,\ldots,n)$$

als

$$[g_{n-3}(y,z)+xg_{n-4}(y,z)+\cdots+x^{n-3}g_0(y,z)]\,du$$

schreiben, wo die homogenen Polynome $g_k(y,z)$ in der Form

$$g_\varkappa(y,z)=c_{\varkappa 0}z^\varkappa+c_{\varkappa 1}y_1z^{\varkappa-1}+c_{\varkappa 2}y_1y_2z^{\varkappa-2}+\cdots+c_{\varkappa\varkappa}y_1\cdots y_\varkappa \quad (\varkappa=0,\ldots,n-3)$$

mit Koeffizienten $c_{\varkappa 0},\ldots,c_{\varkappa\varkappa}$ aus $\Omega$ angesetzt sind. Unter Beachtung von

$$x\cong\frac{\mathfrak{A}}{\mathfrak{U}},\quad y_\nu\cong\frac{\mathfrak{a}_\nu^n}{\mathfrak{U}},\quad \mathfrak{A}=\mathfrak{a}_1\cdots\mathfrak{a}_n,$$

und indem man ohne Einschränkung $\mathfrak{U}$ prim zu $\mathfrak{A}$ normiert, folgert man hieraus durch Abzählung der über $\Omega$ linear-unabhängigen, durch den jeweiligen Nenner teilbaren ganzen Differentiale von $K/\Omega$ die Dimensionsformeln:

$$\dim\frac{W}{\mathfrak{a}_1}=g-1,\qquad \dim\frac{W}{\mathfrak{A}\mathfrak{a}_1}=g-(n-2)-1,\ \ldots$$

$$\dim\frac{W}{\mathfrak{A}\mathfrak{a}_1\cdots\mathfrak{a}_{n-3}}=g-(n-2)-(n-3),\ \ldots$$

$$\dim\frac{W}{\mathfrak{a}_1\cdots\mathfrak{a}_{n-2}}=g-(n-2),$$

$$\dim\frac{W}{\mathfrak{a}_1\cdots\mathfrak{a}_{n-1}}=g-(n-2);$$

$$\dim\frac{W}{\mathfrak{A}}=g-(n-2),\qquad \dim\frac{W}{\mathfrak{A}^2}=g-(n-2)-(n-3),\ldots,$$

$$\dim\frac{W}{\mathfrak{A}^{n-3}}=g-(n-2)-(n-3)-\cdots-2=1,$$

und dann natürlich

$$\dim \frac{W}{\mathfrak{A}^{n-3+\varkappa}} = 0 \qquad \text{für alle } \varkappa \geqq 1.$$

Nach dem Riemann-Rochschen Satz ergibt sich daraus:

$$\begin{array}{lll}
\dim \mathfrak{a}_1 = 1, & \dim \mathfrak{A}\mathfrak{a}_1 = 1+2, & \ldots\ldots \\
\vdots & \vdots & \\
 & \dim \mathfrak{A}\mathfrak{a}_1 \cdots \mathfrak{a}_{n-3} = 1+2, & \ldots\ldots \\
\dim \mathfrak{a}_1 \cdots \mathfrak{a}_{n-2} = 1, & \dim \mathfrak{A}\mathfrak{a}_1 \cdots \mathfrak{a}_{n-2} = 1+2+1, & \ldots\ldots \\
\dim \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} = 1+1, & \dim \mathfrak{A}\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} = 1+2+2, & \ldots\ldots \\
\dim \mathfrak{A} = 1+2, & \dim \mathfrak{A}^2 = 1+2+3, & \ldots\ldots, \\
 & & \dim \mathfrak{A}^{n-3} = 1+2+\cdots+(n-2) = g,
\end{array}$$

und dann natürlich

$$\dim \mathfrak{A}^{n-3+\varkappa} = g-1+\varkappa n \qquad \text{für alle } \varkappa \geqq 1,$$

während die vorhergehenden Schlußformeln sich zu

$$\dim \mathfrak{A}^{\nu} = \binom{\nu+2}{2} \qquad \text{für } \nu = 0, \ldots, n-3$$

zusammenfaßen lassen.

Da $\mathfrak{A}$ in $U$ liegt, darf in diesen Formeln $\mathfrak{A}$ durch $\mathfrak{U}$ ersetzt werden. Insbesondere steht damit jetzt fest, daß genau

$$\dim U = 3$$

ist. Demnach bilden die Erzeugenden $x, y, z$ eine Basis des $\Omega$-Moduls der Vielfachen von $\frac{1}{\mathfrak{U}}$ in $K$. Hieraus folgt, daß bei jeder festen Normierung von $\mathfrak{U}$ als ganzer Divisor aus $U$ eine bestimmte inhomogene lineare Relation

$$\alpha x + \beta y + \gamma z = 1 \qquad (\alpha, \beta, \gamma \text{ in } \Omega)$$

zwischen den zugehörigen Erzeugenden $x, y, z$ besteht, entsprechend der Basisdarstellung des Vielfachen 1 von $\frac{1}{\mathfrak{U}}$.

Weil ferner $\binom{\nu+2}{2}$ gleich der Anzahl der Potenzprodukte aus $x, y, z$ vom Grade $\nu$ ist, bilden diese Potenzprodukte für $\nu = 0, \ldots, n-3$ jeweils eine Basis des $\Omega$-Moduls der Vielfachen von $\frac{1}{\mathfrak{U}^{\nu}}$ in $K$. Dies gilt auch noch für $\nu = n-2,\ n-1$; denn es ist

$$\dim U^{n-2} = g + (n-1) = \binom{n-1}{2} + (n-1) = \binom{n}{2},$$

$$\dim U^{n-1} = g + (n-1) + n = \binom{n}{2} + n = \binom{n+1}{2}.$$

Und es gilt auch noch für alle $\nu \geqq n$; denn einerseits ist nach dem Gezeigten

$$\dim U^{n+\varkappa+1} = \dim U^{n+\varkappa} + n \qquad \text{für alle } \varkappa \geqq 0;$$

andererseits ist mit Rücksicht auf die Grundgleichung $x^n + y^n + z^n = 0$ die Anzahl der über $\Omega$ linear-unabhängigen Potenzprodukte aus $x, y, z$ vom Grade $n + \varkappa$ nur noch $\binom{n+\varkappa+2}{2} - \binom{\varkappa+2}{2}$, und auch dieser Ausdruck nimmt bei $\varkappa \to \varkappa + 1$ um $n$ zu.

Zusammengenommen ist damit gezeigt:

*Die homogenen Polynome über $\Omega$ in $x, y, z$ erschöpfen den Integritätsbereich der höchstens für $\mathfrak{N} = \frac{1}{(x, y, z)}$ gebrochenen Elemente aus $K$.*

Hinsichtlich der Einbettung der Vielfachen von $\frac{1}{\mathfrak{N}^\nu}$ in die von $\frac{1}{\mathfrak{N}^{\nu+1}}$ beachte man hierbei die oben erwähnte inhomogene lineare Relation zwischen $x, y, z$.

Indem man bei gegebenem algebraischem Punkt $\mathfrak{p}$ von $K/\Omega$ den Nennerdivisor $\mathfrak{N}$ prim zu $\mathfrak{p}$ normiert, so daß die Erzeugenden $x, y, z$ primitiv für $\mathfrak{p}$ werden und somit durch konstante Restbildung mod. $\mathfrak{p}$ zur Definition der homogenen Koordinaten $x(\mathfrak{p}) : y(\mathfrak{p}) : z(\mathfrak{p})$ von $\mathfrak{p}$ verwendet werden können, ergibt sich aus dem vorstehendem Sachverhalt die für die Anwendung auf das Fermatsche Problem wichtige Tatsache:

*Die algebraischen Punkte $\mathfrak{p}$ von $K/\Omega$ entsprechen vermöge ihrer homogenen Koordinaten $x(\mathfrak{p}) : y(\mathfrak{p}) : z(\mathfrak{p})$ umkehrbar eindeutig den über $\Omega$ algebraischen Grundgleichungslösungen, und speziell die rationalen Punkte von $K/\Omega$ den Grundgleichungslösungen in $\Omega$.*

## 5. Weierstraßpunkte.

Es seien zunächst kurz die Grundtatsachen über Weierstraßpunkte für einen beliebigen algebraischen Funktionenkörper $K/\Omega$ mit Konstantenkörper $\Omega$ der Charakteristik $\chi(\Omega) = 0$ zusammengestellt[5]. Ohne Einschränkung sei das Geschlecht $g > 0$; mit $W$ sei die Differentialklasse von $K/\Omega$ bezeichnet.

Zu jedem algebraischen Punkt $\mathfrak{p}$ von $K/\Omega$ gibt es, entsprechend dem schrittweisen Abnehmen der $\dim \frac{W}{\mathfrak{p}^\varrho}$ für $\varrho = 0, 1, 2, \ldots$, eine eindeutig bestimmte Folge von $g$ Lückenzahlen

$$1 = \varrho_1 < \varrho_2 < \cdots < \varrho_g \leqq 2g - 1$$

[5]) Im Falle $\chi(\Omega) \neq 0$ wäre die von F. K. Schmidt (Zur arithmetischen Theorie der algebraischen Funktionen. II. Allgemeine Theorie der Weierstraßpunkte. *Math. Zeitschrift*, **45** (1939), S. 75—96) gegebene Modifikation der geläufigen Theorie der Weierstraßpunkte zu berücksichtigen, eine an sich lohnende Aufgabe, von deren Durchführung aber hier mit Rücksicht auf den beschränkten Raum abgesehen werden muß.

derart, daß

$$\dim \frac{W}{\mathfrak{p}^{\varrho_1}}, \ldots, \dim \frac{W}{\mathfrak{p}^{\varrho_2-1}} = g-1,$$
$$\dim \frac{W}{\mathfrak{p}^{\varrho_2}}, \ldots, \dim \frac{W}{\mathfrak{p}^{\varrho_3-1}} = g-2,$$
$$\cdots\cdots\cdots\cdots$$
$$\dim \frac{W}{\mathfrak{p}^{\varrho_g}}, \ldots\ldots\ldots\ldots = 0,$$

also nach dem Riemann-Rochschen Satz

$$\dim \mathfrak{p}^{\varrho_1}, \ldots, \dim \mathfrak{p}^{\varrho_2-1} = \varrho_1, \ldots, \varrho_2 - 1,$$
$$\dim \mathfrak{p}^{\varrho_2}, \ldots, \dim \mathfrak{p}^{\varrho_3-1} = \varrho_2 - 1, \ldots, \varrho_3 - 2,$$
$$\cdots\cdots\cdots\cdots$$
$$\dim \mathfrak{p}^{\varrho_g}, \dim \mathfrak{p}^{\varrho_g+1}, \ldots = \varrho_g - (g-1), \varrho_g - (g-1) + 1, \ldots$$

so daß also genau zu den Nennern $\mathfrak{p}^{\varrho_1}, \ldots, \mathfrak{p}^{\varrho_g}$ keine Elemente in $K$ existieren. Man nennt

$$\gamma(\mathfrak{p}) = \sum_{i=1}^{g} (\varrho_i - i) = \sum_{i=1}^{g} \varrho_i - \frac{g(g+1)}{2}$$

das Gewicht von $\mathfrak{p}$. Es ist $\gamma(\mathfrak{p}) = 0$ dann und nur dann, wenn die minimale Lückenzahlverteilung $\varrho_1, \ldots, \varrho_g = 1, \ldots, g$ vorliegt. Ist $\gamma(\mathfrak{p}) > 0$, so heißt $\mathfrak{p}$ ein Weierstraßpunkt von $K/\Omega$. Da die maximale Lückenzahlverteilung $\varrho_1, \ldots, \varrho_g = g, \ldots, 2g-1$ wegen $\varrho_1 = 1$ nur für $g = 1$ vorliegt, hat man die obere Gewichtsabschätzung

$$\gamma(\mathfrak{p}) < \sum_{k=0}^{g-1} (g+k) - \frac{g(g+1)}{2} = (g-1)g \qquad \text{für } g > 1.$$

Durch Betrachtung der Differentialdeterminante

$$|d^i u_j| = \left|\frac{d^i u_j}{dt^i}\right| (dt)^{\frac{g(g+1)}{2}} \qquad (i, j = 1, \ldots, g),$$

wo $du_j$ eine Basis des $\Omega$-Moduls der ganzen Differentiale von $K/\Omega$ und $t$ ein nicht-konstantes Element aus $K$ ist, zeigt man, daß die über alle algebraischen Punkte $\mathfrak{p}$ von $K/\Omega$ erstreckte Gewichtsumme

$$\gamma = \sum_{\mathfrak{p}} \gamma(\mathfrak{p}) = (g-1)g(g+1)$$

ist. Für $g = 1$ gibt es daher keine Weierstraßpunkte von $K/\Omega$, während es für $g > 1$ stets solche gibt, und zwar in einer Anzahl $N$, die den Ungleichungen

$$(g-1)g(g+1) \geqq N > g+1$$

genügt.

Für den Funktionenkörper $K/\Omega$ der Fermatschen Gleichung, wobei jetzt $n > 3$, somit $g > 1$, und $\chi(\Omega) = 0$ vorausgesetzt sei, bestimmen sich die Lückenzahlen eines der Punkte $\mathfrak{a}_\nu, \mathfrak{b}_\nu, \mathfrak{c}_\nu$, etwa von $\mathfrak{a}_1$, wie folgt. Die ganzen Differentiale von $K/\Omega$ lassen sich unter Hervorhebung des $\mathfrak{a}_1$ entsprechenden Linearfaktors $y_1 = y - \varepsilon_1 z$, etwas anders als oben, durch die $\Omega$-Basis

$$x^\lambda y_1^\mu z^\nu \, du \qquad \left(\begin{matrix} \lambda, \mu, \nu \geqq 0 \\ \lambda + \mu + \nu = n-3 \end{matrix}\right)$$

darstellen. Normiert man wieder ohne Einschränkung $\mathfrak{U}$ prim zu $\mathfrak{A}$

und beachtet, daß dann diese Basiselemente die Ordnungszahlen $\lambda+\mu n$ in $\mathfrak{a}_1$ haben, so erkennt man durch Abzählung der über $\Omega$ linear-unabhängigen, durch die einzelnen Potenzen von $\mathfrak{a}_1$ teilbaren ganzen Differentiale von $K/\Omega$, daß die Lückenzahlen $\varrho_i$ von $\mathfrak{a}_1$ die Zahlen $\lambda+\mu n+1$ sind, die ja wegen $0\leqq\lambda,\ \mu\leqq n-3$ alle untereinander verschieden sind und wegen $\lambda+\mu\leqq n-3$ die richtige Anzahl $1+2+\cdots+(n-2)=g$ haben. Der Größe nach geordnet lauten diese Lückenzahlen

$$1, 2, \ldots, n-2;\ n+1, n+2, \ldots, n+(n-3);\ 2n+1, \ldots, 2n+(n-4);\ \ldots;(n-3)n+1,$$

und ihre Nummern $i$ sind den $n-2$ Abschnitten entsprechend um

$$0,\ 2,\ 2+3, \ldots, 2+3+\cdots+(n-2)$$

kleiner. Demnach ist das Gewicht

$$\gamma(\mathfrak{a}_1)=\sum_{i=1}^{g}(\varrho_i-i)=(n-2)\,0+(n-3)\,2+(n-4)\,(2+3)+\cdots+ \\ +1\,(2+3+\cdots+(n-2)),$$

oder also nach leichter Rechnung

$$\gamma(\mathfrak{a}_1)=\frac{g(n-3)\,(n+4)}{12}.$$

Für die $3n$ Punkte $\mathfrak{a}_\nu,\ \mathfrak{b}_\nu,\ \mathfrak{c}_\nu$ zusammen ergibt sich daraus durch Multiplikation mit $3n$ unter Beachtung von $n(n-3)=2(g-1)$ die Gewichtsumme

$$\gamma_0=\sum_{\nu=1}^{n}(\gamma(\mathfrak{a}_\nu)+\gamma(\mathfrak{b}_\nu)+\gamma(\mathfrak{c}_\nu))=\frac{(g-1)g\,(n+4)}{2}.$$

Vergleich mit der vollen Gewichtsumme,

$$\gamma=(g-1)\,g\,(g+1)$$

ergibt:

*Unter den Voraussetzungen $n>3$ und $\chi(\Omega)=0$ sind die den $3n$ trivialen Grundgleichungslösungen entsprechenden Punkte von $K/\Omega$ sämtlich Weierstraßpunkte gleichen Gewichts mit der Gewichtsumme*

$$\gamma_0=\frac{(g-1)\,g\,(n+4)}{2}.$$

*Im Falle $n=4$, wo $g=3$ ist, sind damit alle Weierstraßpunkte von $K/\Omega$ erschöpft. Im Falle $n>4$ besitzt $K/\Omega$ noch weitere Weierstraßpunkte mit der Gewichtsumme*

$$\bar{\gamma}=\frac{(g-1)\,g\,(2g-n-2)}{2}.$$

## 6. Zum Additionsschema der rationalen $g$-gliedrigen Punktgruppen.

Um dieses Schema aufzustellen, muß man eine rationale $g$-gliedrige Punktgruppe, d. h. einen ganzen Divisor $g$-ten Grades $\mathfrak{O}$ von $K/\Omega$ als Bezugsdivisor auszeichnen. Dann stellt sich jenes Schema in multiplikativer Form durch die Äquivalenzbeziehung

$$\frac{\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}}{\mathfrak{O}^3}\sim 1$$

dar, wo $\mathfrak{P}_1$, $\mathfrak{P}_2$ gegebene ganze Divisoren $g$-ten Grades von $K/\Omega$ sind und $\mathfrak{P}$ als ebensolcher zu bestimmen ist; in additiver Form entspricht dem dann die Beziehung $\mathfrak{P}_1+\mathfrak{P}_2+\mathfrak{P}\sim 0$ (in bezug auf $\mathfrak{O}$).

Aus Gründen der Einfachheit und Eleganz sollte man versuchen, den auszuzeichnenden Bezugsdivisor $\mathfrak{O}$, entspechend wie den Nennerdivisor $\mathfrak{U}$ im vorhergehenden, invariant bei der Automorphismengruppe $\mathfrak{G}$ von $K/\Omega$ zu wählen. Wie leicht zu sehen, läßt sich aber jedenfalls aus den bisher allein explizit aufgewiesenen $3n$ Primdivisoren $\mathfrak{a}_\nu$, $\mathfrak{b}_\nu$, $\mathfrak{c}_\nu$ kein dieser Invarianzforderung genügender ganzer Divisor $g$-ten Grades zusammensetzen. Im Hinblick auf den additiven Aufbau $g=1+2+ + \cdots + (n-2)$ des Geschlechts erscheint bei dieser Sachlage die Wahl

$$\mathfrak{O}=\mathfrak{a}_1^1\mathfrak{a}_2^2\cdots\mathfrak{a}_{n-2}^{n-2}$$

noch am meisten naturgemäß.

Man muß dann eine Basis des $\Omega$-Moduls der Vielfachen von $\frac{1}{\mathfrak{O}^3}$ in $K$ angeben. Diese Aufgabe und auch die beabsichtigte Anwendung vereinfachen sich, wenn man statt $\mathfrak{O}$ den äquivalenten (gebrochenen) Divisor

$$\mathfrak{O}'=\frac{\mathfrak{O}}{y_1y_2\cdots y_{n-2}}=\frac{\mathfrak{U}^{n-2}}{\mathfrak{a}_1^{n-1}\mathfrak{a}_2^{n-2}\cdots\mathfrak{a}_{n-2}^2}$$

zugrundelegt. Die Vielfachen von $\frac{1}{\mathfrak{O}'^3}$ in $K$ sind diejenigen homogenen Polynome in $x, y, z$ über $\Omega$ vom Grade $3(n-2)$, welche (bei zu $\mathfrak{A}$ prim normiertem $\mathfrak{U}$) an den Punkten $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{n-2}$ Nullstellen von mindestens den Ordnungen $n-1, n-2, \ldots, 2$ haben. Indem man die zwischen den Potenzprodukten des Grades $3(n-2)$ auf Grund der Gleichung $x^n+y^n+z^n=0$ bestehenden linearen Abhängigkeiten durch entsprechende Reduktion mod. $n$ der Exponenten von $x$ eliminiert, ergibt sich daraus, analog wie oben bei den ganzen Differentialen, als Basis des $\Omega$-Moduls der Vielfachen von $\frac{1}{\mathfrak{O}'^3}$ in $K$ das System der Potenzprodukte

$$x^{\lambda} y_1^{\mu_{\lambda,1}} \cdots y_{n-2}^{\mu_{\lambda,n-2}} y^{\mu} z^{\nu} \left\{ \begin{array}{l} \lambda=0,\ldots,n-1 \\ \mu_{\lambda,\varrho}=3-\left[\dfrac{\lambda+3\varrho}{n}\right] \quad (\varrho=1,\ldots,n-2) \\ \mu,\nu \geqq 0;\ \mu+\nu=3(n-2)-\lambda-\sum\limits_{\varrho=1}^{n-2}\mu_{\lambda,\varrho} \end{array} \right\},$$

wo also für $\lambda=0,\ldots,n-1$ und $\varrho=1,\ldots,n-2$ jeweils $\mu_{\lambda,\varrho}$ die kleinste ganze Zahl mit $\lambda+n\mu_{\lambda,\varrho}\geqq 3(n-\varrho)$ ist, und wo — den Bedingungen für $\mu, \nu$ entsprechend — nur diejenigen solchen Systeme $\lambda, \mu_{\lambda,\varrho}$ in Betracht zu ziehen sind, für welche die Summe $\lambda+\sum\limits_{\varrho=1}^{n-2}\mu_{\lambda,\varrho}\leqq 3(n-2)$ ist. Auf Grund des Riemann-Rochschen Satzes sind das $2g+1$ Basiselemente, wie man auch durch direkte Abzählung bestätigen kann; sie seien zur Abkürzung mit $w_1,\ldots,w_{2g+1}$ bezeichnet.

Es seien nun

$$\mathfrak{P}_1=\mathfrak{p}_1^{(1)}\cdots\mathfrak{p}_g^{(1)},\quad \mathfrak{P}_2=\mathfrak{p}_1^{(2)}\cdots\mathfrak{p}_g^{(2)},\quad \mathfrak{P}=\mathfrak{p}_1\cdots\mathfrak{p}_g$$

die Zerlegungen der in die allgemeine Additionsrelation eingehenden rationalen Punktgruppen in algebraische Punkte von $K/\Omega$, und es sei einfachheitshalber angenommen, daß der „allgemeine“ Fall vorliegt, in dem die $3g$ Punkte $\mathfrak{p}_i^{(1)}, \mathfrak{p}_i^{(2)}, \mathfrak{p}_i$ $(i=1,\ldots,g)$ untereinander verschieden sind und überdies $\mathfrak{P}$ regulär ($\dim\mathfrak{P}=1$) ist; letzteres bedeutet, daß $\mathfrak{P}$ selbst (nicht nur die Klasse von $\mathfrak{P}$) durch die Additionsrelation eindeutig bestimmt ist. Sind dann

$$w_1(\mathfrak{p}_i^{(1)}):\cdots:w_{2g+1}(\mathfrak{p}_i^{(1)}),\quad w_1(\mathfrak{p}_i^{(2)}):\cdots:w_{2g+1}(\mathfrak{p}_i^{(2)}),\quad w_1(\mathfrak{p}_i):\cdots:w_{2g+1}(\mathfrak{p}_i)$$

die mittels der Basis $w_1,\ldots,w_{2g+1}$ gebildeten homogenen Koordinaten der Punkte $\mathfrak{p}_i^{(1)}, \mathfrak{p}_i^{(2)}, \mathfrak{p}_i$, so drückt sich die zu betrachtende Additionsrelation durch die Determinantengleichungen

$$\begin{vmatrix} w_1(\mathfrak{p}_1^{(1)}) & \cdots & w_{2g+1}(\mathfrak{p}_1^{(1)}) \\ \cdots & \cdots & \cdots \\ w_1(\mathfrak{p}_g^{(1)}) & \cdots & w_{2g+1}(\mathfrak{p}_g^{(1)}) \\ w_1(\mathfrak{p}_1^{(2)}) & \cdots & w_{2g+1}(\mathfrak{p}_1^{(2)}) \\ \cdots & \cdots & \cdots \\ w_1(\mathfrak{p}_g^{(2)}) & \cdots & w_{2g+1}(\mathfrak{p}_g^{(2)}) \\ w_1(\mathfrak{p}_i) & \cdots & w_{2g+1}(\mathfrak{p}_i) \end{vmatrix} = 0 \qquad (i=1,\ldots,g)$$

aus, d. h. die mit der Basis $w_1,\ldots,w_{2g}$ gebildeten homogenen Koordinaten der $\mathfrak{P}$ zusammensetzenden $g$ Punkte $\mathfrak{p}_i$ bestimmen sich, geometrisch ausgedrückt, als die Schnittpunkte der dieser Basis zugeordneten $2g$-dimensionalen Raumkurve (die zur gegebenen ebenen Kurve $x^n+y^n+z^n=0$ birational äquivalent ist) mit einer durch die homogenen Koordinaten der $\mathfrak{P}^{(1)}, \mathfrak{P}^{(2)}$ zusammensetzenden Punkte $\mathfrak{p}_i^{(1)}, \mathfrak{p}_i^{(2)}$ gegebenen $(2g-1)$-dimensionalen Hyperebene.

Dieses letztere Rechenschema und auch die an ihm für „spezielle" Fälle anzubringenden Modifikationen sind aus der allgemeinen Theorie der algebraischen Funktionenkörper wohlbekannt. Hier kam es nur auf die bisher nirgends gemachte explizite Angabe einer zur Darstellung dieses Rechenschemas geeigneten Basis $w_1, \ldots, w_{2g+1}$ im Falle des Funktionenkörpers der Fermatschen Gleichung an. Daß diese Basis recht kompliziert gebaut ist, scheint in der Natur der Sache zu liegen und sollte nicht von einer weiteren Verfolgung der in dieser Note angeschnittenen Fragestellungen abschrecken.

*(Eingegangen am 10. August 1950.)*