Weil, A.

L'arithmétique sur les courbes algébriques. (French) JFM 55.0713.01

Acta Math. 52, 281-315 (1929).

Die Gleichung $y^2 = 4x^3 - g_2x - g_3$ einer Kurve dritter Ordnung vom Geschlecht $p = 1$ habe rationale Koeffizienten; sie werde uniformisiert durch $x = \wp(u)$, $y = \wp'(u)$. Wie *Mordell* (Proceedings Cambridge 21 (1922), 179-192; F. d. M. 48, 140 (JFM 48.0140.*)-141) zeigte, gibt es endlich viele Zahlen u_1, ..., u_r, so daß jeder Kurvenpunkt mit rationalen Koordinaten zu einem Argument $u = n_1u_1 + \cdots + n_ru_r$ gehört, wo n_1, ..., n_r alle ganzen rationalen Zahlen durchlaufen. Dieser Satz wird von *Weil* auf algebraische Kurven beliebigen Geschlechts p mit Koeffizienten aus einem beliebigen Zahlkörper verallgemeinert. Alsdann muß man Systeme von p Punkten betrachten und *Abel*sche Funktionen heranziehen. – Die Arbeit führt ganz neuartige Methoden in die Theorie der diophantischen Gleichungen ein und wird für die weitere Entwicklung grundlegend sein; dies ist bereits ersichtlich aus den Anwendungen, die *C. Siegel* von ihr macht (Abhandlungen Akad. Berlin 1929, Nr. 1; F. d. M. 56_{I}, 180-184).

I. Zerlegungssätze.

1. Definitionen.

k sei ein endlicher algebraischer Zahlkörper. Unter C wird eine ebene algebraische Kurve verstanden, deren Gleichung $F(x, y) = 0$ Koeffizienten aus k hat. Ein Punkt M auf C heißt algebraisch, wenn seine Koordinaten algebraische Zahlen sind; sind M_1, M_2, ..., M_q endlich viele algebraische Punkte, so bedeutet $k(M_1, M_2, \dots, M_q)$ den aus k durch Adjunktion ihrer Koordinaten entstehenden Zahlkörper.

Unter einer Verteilung (distribution) $\boldsymbol{d}$ in bezug auf k wird eine Funktion verstanden, die jedem algebraischen Punkt M auf C ein ganzes Ideal $\mathfrak{d} = \boldsymbol{d}(M)$ aus $k(M)$ zuordnet; dabei sollen aber Punkten, deren Koordinaten in bezug auf k konjugiert sind, auch in bezug auf k konjugierte Ideale entsprechen. (Entsprechend sind Verteilungen in bezug auf einen Oberkörper K von k zu definieren). Man kann Produkt $\boldsymbol{dd}'$ und größten gemeinschaftlichen Teiler $(\boldsymbol{d}, \boldsymbol{d}')$ zweier Verteilungen und ebenso beliebig vieler bilden.

Eine Verteilung $\boldsymbol{d}$ heißt durch eine zweite $\boldsymbol{d}'$ teilbar: $\boldsymbol{d}'/\boldsymbol{d}$, wenn eine von M unabhängige natürliche Zahl a existiert, derart daß in jedem algebraischen Punkt M auf C das Ideal $a \cdot \boldsymbol{d}(M)$ durch das Ideal $\boldsymbol{d}'(M)$ teilbar ist. Gilt gleichzeitig $\boldsymbol{d}'/\boldsymbol{d}$ und $\boldsymbol{d}/\boldsymbol{d}'$, so heißen $\boldsymbol{d}$ und $\boldsymbol{d}'$ äquivalent: $\boldsymbol{d} \sim \boldsymbol{d}'$. Ist $\boldsymbol{d} \sim \boldsymbol{d}'$ und $\boldsymbol{e} \sim \boldsymbol{e}'$, so gilt $\boldsymbol{de} \sim \boldsymbol{d}'\boldsymbol{e}'$ und $(\boldsymbol{d}, \boldsymbol{e}) \sim (\boldsymbol{d}', \boldsymbol{e}')$. Unter $\mathbf{1}$ wird die Verteilung verstanden, die überall gleich dem Einheitsideal ist; zwei Verteilungen heißen teilerfremd, wenn ihr größter gemeinschaftlicher Teiler gleich $\mathbf{1}$ ist.

2. Die Verteilung $\boldsymbol{d}_A$.

Sei $f(M)$ eine rationale Funktion auf C mit Koeffizienten aus k. In jedem algebraischen Punkt M auf C kann $f(M)$ als Quotient $\frac{\mathfrak{m}}{\mathfrak{n}}$ zweier teilerfremder Ideale $\mathfrak{m}$ und $\mathfrak{n}$ aus $k(M)$ dargestellt werden; dabei soll $\mathfrak{m} = 0$, $\mathfrak{n} = 1$ für $f(M) = 0$ und $\mathfrak{m} = 1$, $\mathfrak{n} = 0$ für $f(M) = \infty$ gesetzt werden. Die Werte des Ideals $\mathfrak{n}$ bilden "die durch f erzeugte Verteilung $[f]$", entsprechend die Ideale $\mathfrak{m}$ die Verteilung $\left[\frac{1}{f}\right]$. Über solche Verteilungen gilt:

(1) *Sind alle Pole von g unter denen von f enthalten, so ist $[g]/[f]$. Stimmen die Pole beider Funktionen überein, so ist $[f] \sim [g]$. Haben leide Funktionen keine gemeinsamen Pole, so ist endlich $([f], [g]) \sim \mathbf{1}$.*

Jetzt werde jedem algebraischen Punkt A auf C ein Paar rationaler Funktionen $x_{\boldsymbol{A}}$ und $y_{\boldsymbol{A}}$ mit Koeffizienten aus $k(A)$ zugeordnet, die A als einzigen Pol, und zwar erster Ordnung, gemein haben. Die Verteilung in bezug auf $k(A)$

$$\boldsymbol{d}_{\boldsymbol{A}} = ([x_A], [y_A])$$

ist dann nach (1) bis auf Äquivalenz eindeutig bestimmt; sind A und B verschiedene Punkte auf C, so sind ferner $\boldsymbol{d}_{\boldsymbol{A}}$ und $\boldsymbol{d}_{\boldsymbol{B}}$ in $k(A, B)$ teilerfremd. Der Wert $\omega(A, M)$ von $\boldsymbol{d}_{\boldsymbol{A}}$ im Punkt M ist ein ganzes Ideal aus $k(A, M)$; aus (1) folgt, daß dasselbe folgende Eigenschaft hat:

(2) *Hat die rationale Funktion $f(M)$ auf C Koeffizienten aus k, und sind A_1, A_2, ..., A_n ihre Pole, A'_1, A'_2,..., A'_n ihre Nullstellen, alle in der richtigen Vielfachheit gezählt, so ist in jedem algebraischen Punkt M*

$$f(M) = \frac{\mathfrak{k}\,\omega(A'_1M)\,\omega\,(A'_2M)\ldots\omega\,(A'_nM)}{\mathfrak{l}\,\omega(A_1M)\,\omega\,(A_2M)\ldots\omega\,(A_nM)},$$

wobei $\mathfrak{k}$, $\mathfrak{l}$ una der größte gemeinschaftliche Teiler von Zahler und Nenner ganze Ideale sind, die in einer von M unabhängigen natürlichen Zahl aufgehen.

Identisch mit dieser Aussage sind die beiden Zerlegungen von $[f]$ und $\left[\frac{1}{f}\right]$:

$$[f] \sim \boldsymbol{d}_{\boldsymbol{A}_1}\,\boldsymbol{d}_{\boldsymbol{A}_2}\ldots\boldsymbol{d}_{\boldsymbol{A}_N},\,\left[\frac{1}{f}\right] \sim \boldsymbol{d}'_{\boldsymbol{A}_1}\,\boldsymbol{d}'_{\boldsymbol{A}_2}\ldots\boldsymbol{d}'_{\boldsymbol{A}_n}.$$

3. Der allgemeine Zerlegungssatz:

Sei V eine algebraische n-dimensionale Mannigfaltigkeit ohne singuläre Punkte, eingebettet in einen l-dimensionalen projektiven Raum, definiert durch algebraische Gleichungen mit Koeffizienten aus k. "Fläche" wird jede irreduzible algebraische Mannigfaltigkeit U auf V von $n-1$ Dimensionen genannt, die durch Gleichungen mit algebraischen Koeffizienten definiert wird. Sind U_1, U_2, ..., U_q solche Flächen, M_1, M_2, ..., M_r Punkte auf V, so bezeichnet $k(U_1,\ldots,U_q,M_1,\ldots,M_r)$ den Oberkörper von k, der die Koeffizienten ihrer Gleichungen, bzw. ihre Koordinaten enthält. – Man kann auf V wie auf Kurven Verteilungen einführen; insbesondere geben rationale Funktionen $f(M)$ von Punkten M auf V wieder Veranlassung zu Verteilungen $[f]$, die ähnliche Eigenschaften wie in 2. haben. An Stelle von $\boldsymbol{d}_{\boldsymbol{A}}$ tritt jetzt für jede Fläche U eine Verteilung $\boldsymbol{d}_U$, die der größte gemeinschaftliche Teiler der Verteilungen $[f]$ ist, wo f alle rationalen Funktionen auf V durchläuft, die U als Pol erster Ordnung gemein haben. Wird der Wert von $\boldsymbol{d}_U$ im Punkt M auf V mit $\omega(U,M)$ bezeichnet, so gilt der Zerlegungssatz:

(3) *Hat die rationale Funktion $f(M)$ von M auf V Koeffizienten aus k, und sind U_1, U_2, ..., U_q ihre Pol-Flächen, U'_1, U'_2, ..., V'_r ihre Null-Flächen, alle in der richtigen Vielfachheit gezählt, so ist in jedem algebraischen Punkt M auf V*

$$f(M) = \frac{\mathfrak{k}\,\omega(U'_1M)\,\omega\,(U'_2M)\ldots\omega\,(U'_rM)}{\mathfrak{l}\,\omega(U_1M)\,\omega\,(U_2M)\ldots\omega\,(U_qM)},$$

wobei $\mathfrak{k}$ und $\mathfrak{l}$ ganze Ideale sind, die in einer natürlichen Zahl aufgehen, die nicht von M abhängt.

Identisch mit dieser Aussage sind die beiden Zerlegungen

$$[f] \sim \boldsymbol{d}_{U_1}\boldsymbol{d}_{U_2}\ldots\boldsymbol{d}_{U_q},\,\left[\frac{1}{f}\right] \sim \boldsymbol{d}_{U'_1}\boldsymbol{d}_{U'_2}\ldots\boldsymbol{d}_{U'_r}.$$

Die Verteilungen $\boldsymbol{d}_U$ besitzen folgende Invarianz-Eigenschaft: Ist S ein System von Flächen U_1, U_2,..., U_q, so werde zur Abkürzung $\boldsymbol{d}_S = \boldsymbol{d}_{U_1}\boldsymbol{d}_{U_2}\ldots\boldsymbol{d}_{U_q}$ gesetzt. Ist dann t eine Transformation, die jedem Punkt M auf V genau einen Punkt tM mit Koordinaten in $k(M)$ zuordnet, und deren Umkehrung t^{-1} genau r-deutig ist, ist S ein Flächensystem und $t^{-1}S$ das hieraus durch die r-deutige Transformation t^{-1} entstehende, so ist $\boldsymbol{d}_S\,(tM) \sim \boldsymbol{d}_{t^{-1}S}(M)$.

II. Der *Weyl*sche Basissatz.

4. Rationale Systeme und Basissatz.

Das Geschlecht p der Kurve C in 1. werde $\geqq 1$ angenommen. Unter Punktsystem auf C werde ein System von p Punkten auf C verstanden. Ein System heißt rational, wenn die in seinen Punkten symmetrischen rationalen Funktionen der Koordinaten mit Koeffizienten aus k wieder in k liegen.

Seien w_1, w_2, ..., w_p p unabhängige normierte Integrale erster Gattung auf C. Unter $\mathit{\Gamma} = (A_1, A_2, \ldots, A_p)$ werde ein festes, unter $S = (M_1, M_2, \ldots, M_p)$ ein veränderliches System auf C verstanden. Dem letzten läßt sich durch die Gleichungen

$$u_\nu = \sum_{i=1}^{p} \int_{A_i}^{M_i} dw_\nu \qquad (\nu = 1, 2, \ldots, p)$$

ein Punkt $u = (u_1, u_2, \ldots, u_p)$ des p-dimensionalen Raumes zuordnen; er ist bis auf ein additives Periodensystem der Integrale w_ν bestimmt und bestimmt umgekehrt im allgemeinen das System S eindeutig (*Jacobi*sches Umkehrproblem). Indem zwischen äquivalenten Systemen und zwischen kongruenten Punkten nicht unterschieden wird, kommt man also zu einer $(1,1)$-deutigen Beziehung zwischen u und S. Entsprechen S, S', T die Punkte u, u', v, so bedeutet $S+S'-T$ das System, das dem Punkt $u+u'-v$ mit Koordinaten $u_\nu+u'_\nu-v_\nu$ entspricht.

Seien speziell Γ und S rationale Systeme; dann nennen wir die Punkte 0 und u, die ihnen entsprechen, auch rational. Mit u und v ist $u\mp v$ gleichzeitig rational; die rationalen Systeme auf C bilden also einen Modul. Nach *André Weil* gilt:

(4) **Der Modul der rationalen Systeme auf C besitzt eine endliche Basis.**

Es genügt diesen Satz für irgend einen Überkörper von k zu beweisen; indem man für diesen wieder k schreibt, darf also angenommen werden, daß in k gewisse endlich viele algebraische Zahlen liegen.

5. Erster Schritt: Anwendung der Wurzelfunktionen:

Ist Γ das gegebene rationale System, so gibt es $2^{2p}-1$ Systeme γ, die $\neq\Gamma$ sind, sich aber hiervon nur um ein Halbperiodensystem unterscheiden; sie seien rational in k. Seien ferner g, g' und g_0, g'_0 je zwei rationale Systeme und $G=g+g'-\Gamma$ und $G_0=g_0+g'_0-\Gamma$; dabei mögen Γ und die γ punktfremd zu g, g', g_0, g'_0, G, G_0 sein. Nach dem *Abel*schen Theorem existiert zu jedem γ eine rationale Funktion $f_\gamma(M)$ auf C, die in jedem Punkt von Γ einen doppelten Pol, in jedem von γ eine doppelte Nullstelle hat; ebenso existiert eine rationale Funktion $\psi(M)$ auf C, die g_0, $g'_)$, G als einfache Pole, g, g', G_0 als einfache Nullstellen hat. Sei S ein System $(M_1,\,M_2,\,...,\,M_p)$ und dann

$$F_\gamma(S)=h\prod_{i=1}^{p}f_\gamma(M_i),\;\;\Phi(S)=\prod_{i=1}^{p}\psi_\gamma(M_i),$$

ferner die Konstante h so bestimmt, daß $F_\gamma(g_0)\,F_\gamma(g'_0)=F_\gamma(G_0)$ ist. Mittels des Residuensatzes kann man dann folgende Identitäten beweisen:

$$\frac{F_\gamma(G)}{F_\gamma(g)\,F_\gamma(g')}=\left\{\frac{\Phi(\Gamma)}{\Phi(\gamma)}\right\}^2\text{ für }G=g+g'-\Gamma,\tag{5}$$

$$F_\gamma(G)=\left\{F_\gamma(g)\frac{\Phi(\Gamma)}{\Phi(\gamma)}\right\}^2\text{ für }G=2g-\Gamma.\tag{6}$$

Nach (2) ist $f_\gamma(M)=\frac{\lambda\eta^2(M)}{\mu H^2(M)}$, wo λ, μ, η, H ganze Ideale aus $k(M)$ sind, wobei für λ, μ nur endlich viele Möglichkeiten bestehen. Daraus folgt für rationale Systeme S durch Normenbildung bei Berücksichtigung der Einheiten, daß

$$F_\gamma(S)=m_\gamma a_\gamma\tag{7}$$

ist, wo die a_γ Zahlen aus k und die m_γ ganze Zahlen hieraus sind und letztere nur endlich viele Möglichkeiten haben. - Entspricht der Punkt u dem System S, so werde $F_\gamma(u)=F_\gamma(S)$ gesetzt; dies ist eine *Abel*sche Funktion.

Zwei rationale Punkte u und v heißen zur selben Klasse gehörig, in Zeichen $u\infty v$, wenn alle $2^{2p}-1$ Zahlen $\dfrac{F_\gamma(u)}{F_\gamma(v)}$ Quadrate in k sind. Nach (7) ist die Anzahl h der Klassen endlich; nach (5) folgt aus $u\infty v$, $u'\infty v'$, daß $u+u'\infty v+v'$ ist, nach (6) ist ferner für jeden rationalen Punkt u auch $2u\infty 0$; dabei wird die Nullklasse durch Γ erzeugt. Die Gruppe der Klassen enthält demnach nur Elemente der Ordnung 2. Man zeigt den wichtigen Satz:

(8) *Ist u rational und $u\infty 0$, so sind die 2^{2p} Punkte $\dfrac{u}{2}$, die aus einem unter ihnen durch Addition sämtlicher Halbperiodensysteme hervorgehen, alle auch rational.*

6. Zweiter Schritt: Die *Jacobi*sche Mannigfaltigkeit.

Sei $\vartheta(v)$ die Thetafunktion von $v=(v_1,v_2,\ldots,v_p)$, gebildet aus den Perioden der u_ν. Es gibt genau $P=3^p$ linear unabhängige Thetafunktionen dritter Ordnung $\theta_i(v)$ $(i=1,\,2,\,...,\,P)$, d. h. solche ganzen Funktionen der v, daß die Quotienten $\dfrac{\theta_i(v)}{\vartheta(v)^3}=f_i(v)$ die Periodensysteme der v_ν als Perioden haben. Gehört zu dem System $(M_1,\,M_2,\,...,\,M_p)$ auf C der Punkt u im u-Raum, so sind die $f_i(u)$ symmetrische rationale Funktionen der Punkte dieses Systems; indem man k nötigenfalls erweitert, kann man erreichen, daß sie Koeffizienten aus k bekommen.

Im $(P-1)$-dimensionalen projektiven Raum wird durch die Gleichungen

$$X_1 : X_2 : \cdots : X_P = \theta_1(u) : \theta_2(u) : \cdots : \theta_P(u) = f_1(u) : f_2(u) : \cdots : f_P(u)$$

eine p-dimensionale, nämlich die *Jacobi*sche Mannigfaltigkeit V von C definiert. Die Koeffizienten ihrer definierenden Gleichungen liegen in k. Jeder Punkt von V wird genau einmal durchlaufen, wenn u im u-Raum alle Punkte eines Fundamentalbereichs $\varPi$ in bezug auf das Periodensystem der u_ν durchläuft; außerdem steht V in birationaler Beziehung zu den Systemen von p Punkten auf C. V ist eine Mannigfaltigkeit ohne singuläre Punkte.

Sei $\theta(u) = \sum_{i=1}^{P} e_i\,\theta_i(u)$ eine Funktion dritter Ordnung mit Koeffizienten e_i aus k. Durch $\theta(u) = 0$ wird ein System von rationalen Flächen auf V als Schnitt von V mit der Ebene $\sum_{i=1}^{P} e_i\,X_i = 0$ definiert. Man kann auf V die Sätze aus 3. anwenden. Danach gehört zu diesem Flächensystem eine Verteilung $\omega(u)$; ihr Wert ist für rationale Punkte ein ganzes Ideal aus k, ferner gehört entsprechenderweise zu den Flächen $\theta(2u-a)$ die Verteilung $\omega(2u-a)$, wenn a irgendein rationaler Punkt ist; denn $u \longleftrightarrow 2u-a$ ist eine $(1, 2^{2p})$-deutige Transformation von V in sich. Sei nun ε ein Halbperiodensystem der Integrale u_ν und $c \neq 0$ eine solche Konstante, daß die auf V rationale Funktion $F(u) = c\dfrac{\theta^2(u)\,\vartheta^3(u-a-\varepsilon)\,\vartheta^3(u-a+\varepsilon)}{\theta(2u-a)}$ Koeffizienten aus k erhalt. Für rationale Punkte u ist nach (3) alsdann $F(u) = \dfrac{\lambda\omega^2(u)\,\eta^6(u)}{\mu\omega(2u-a)}$, wo $\eta(u)$ die zu den Flächen $\vartheta(u-a\mp\varepsilon) = 0$ gehörige Verteilung und λ, μ ganze Ideale aus k sind, die in einer von u unabhängigen natürlichen Zahl aufgehen. Sei $\vartheta(u-a\mp\varepsilon) \neq 0$, so daß auch das ganze Ideal $\eta(u)$ ungleich Null, also seine Norm $N\eta(u) \geqq 1$ ist; somit gilt alsdann mit einer von a und ε abhängigen Zahl $m > 0$

$$\big(N\omega(u)\big)^2 \leqq m|\,NF(u)\,|N\omega(2u-a). \tag{9}$$

k sei ohne Einschränkung ein *Galois*scher Körper und etwa reell, $A = E$, $\overline{A}$, $\overline{\overline{A}}$, ...seine Automorphismen. Dann transformiert z.B. $\overline{A}$ die Kurve C in $\overline{C}$; gleichzeitig entsprechen allen geometrischen Gebilden, Punktgruppen und Funktionen in bezug auf C solche in bezug auf $\overline{C}$ und sind mit ihnen zusammen rational. Wird durch einen, zwei, ...Querstriche die Anwendung von $\overline{A}$, $\overline{\overline{A}}$,...angedeutet, so ist insbesondere

$$|\,NF(u)\,| = |\,F(u)\overline{F}(\overline{u})\overline{\overline{F}}(\overline{\overline{u}})\ldots\,|,$$

und demnach folgt mit den Abkürzungen

$$\varOmega(u) = \frac{N\omega(u)}{\theta(u)\overline{\theta}(\overline{u})\overline{\overline{\theta}}(\overline{\overline{u}})\ldots},$$

$$\varLambda(u,\overline{u},\overline{\overline{u}},\ldots) = |\,\vartheta^3(u-a-\varepsilon)\vartheta^3(u-a+\varepsilon)\cdot\overline{\vartheta}^3(\overline{u}-\overline{a}-\overline{\varepsilon})\overline{\vartheta}^3(\overline{u}-\overline{a}+\overline{\varepsilon})\ldots\,|$$

aus (9) für $\theta(u) \neq 0$ die Ungleichung $\varOmega^2(u) \leqq m_1\varLambda(u,\overline{u},\ldots)\varOmega(2u-a)$, wo $m_1 > 0$ nur von a, $\overline{a}$, ..., ε, $\overline{\varepsilon}$, ...abhängt. Bei den Anwendungen können die a und ε nur endlich viele verschiedene Werte annehmen, während die u, $\overline{u}$, ...auf endliche Bereiche beschränkt bleiben. Dann vereinfacht sich die vorige Ungleichung, und mit einer absoluten Konstanten $M > 0$ folgt für $\varOmega(u) \neq 0$:

$$\varOmega^2(u) \leqq M\varOmega(2u-a). \tag{10}$$

7. Dritter Schritt: Die "descente infinie".

Nach 5. gibt es endlichviele Punktgruppen a_1, a_2,..., a_h auf C, so daß jedes rationale System u einer Beziehung $u\infty a_j$ genügt ($j = 1, 2, ..., h$). Werde nunmehr u auf einen Fundamentalbereich $\varPi$ im u-Raum in bezug auf die Periodensysteme der u_ν beschränkt, entsprechend $\overline{u}$, $\overline{\overline{u}}$, ...auf Bereiche $\overline{\varPi}$, $\overline{\overline{\varPi}}$, ... Für rationales u läßt sich dann nach (8) durch die Formeln

$$u\infty a_j,\ u' \equiv \frac{u+a_j}{2};\ u'\infty a_{j'},\ u'' \equiv \frac{u'+a_{j'}}{2};\ u''\infty a_{j''},\ u''' \equiv \frac{u''+a_{j''}}{2};\ldots$$

wo $\equiv$ die Kongruenz in bezug auf die Periodensysteme bedeutet, eine unendliche Folge u, u', u'', ...rationaler Punkte in $\varPi$ definieren; ihnen entsprechen Punkte in $\overline{\varPi}$, $\overline{\overline{\varPi}}$, ... Sei $a^{(\nu)} = 2u^{(\nu+1)} - u^{(\nu)}$, so daß $a^{(\nu)}$ von $a_{j^{(\nu)}}$ höchstens um ein Periodensystem abweicht und auch nur endlich viele Möglichkeiten hat; entsprechend $\overline{a}^{(\nu)}$, $\overline{\overline{a}}^{(\nu)}$,.... Unter ε werde ein Halbperiodensystem mit $\vartheta(u^{(\nu+1)} - a^{(\nu)} \mp \varepsilon) \neq 0$ verstanden, entsprechend $\overline{\varepsilon}$, $\overline{\overline{\varepsilon}}$,.... Sei der Einfachheit halber $\Omega(u^{(\nu)}) \neq 0$ für $\nu = 0, 1, 2,$.... Dann folgt aus (10): $\Omega(u^{(\nu+1)})^2 \leqq M\Omega(u^{(\nu)})$, also von einem ν ab: $\Omega(u^{(\nu)}) \leqq M + 1$ und wegen der Beschränktheit von $\theta\,(u^{(\nu)})$, $\overline{\theta}(\overline{u}^{(\nu)})$, $\overline{\overline{\theta}}(\overline{\overline{u}}^{(\nu)})$, ...die Ungleichung

$$N\omega(u^{(\nu)}) \leqq L, \tag{11}$$

wo L nur von dem betrachteten θ abhängt. Zum gleichen Ergebnis kommt man auch, wenn k imaginär ist oder ein $\Omega(u^{(\nu)}) = 0$.

In $\theta = \sum_{i=1}^{P} e_i\theta_i$ seien die ε_i insbesondere ganz rational; für die zugehörige Verteilung $\omega(u)$ ist dann, wie bewiesen, von einem ν ab $N\omega(u^{(\nu)})$ beschränkt. Dies trifft zu insbesondere für die Verteilungen $\omega_i(u)$ der Funktionen θ_i selbst. Seien $X_1^{(\nu)}$, $X_2^{(\nu)}$,..., $X_P^{(\nu)}$ die homogenen Koordinaten des Punktes auf V, der $u^{(\nu)}$ entspricht, so daß nach dem Zerlegungssatz (3)

$$\frac{\sum_{i=1}^{P} e_i X_i^{(\nu)}}{X_i^{(\nu)}} = \frac{\theta(u^{(\nu)})}{\theta_i(u^{(\nu)})} = \frac{\lambda_i\omega(u^{(\nu)})}{\mu_i\omega_i(u^{(\nu)})}$$

ist, mit Idealen λ_i, μ_i, die in einer festen natürlichen Zahl aufgehen. In jeder Idealklasse von k werde ein Repräsentant α_k gewählt; da die $u^{(\nu)}$ in k liegen, so können $X_1^{(\nu)}$, $X_2^{(\nu)}$, ..., $X_p^{(\nu)}$ ganz in k angenommen werden, und ihr größter gemeinsamer Teiler ist gleich einem der Ideale α_k, also nur endlichvieler Werte fähig. Dann ist die Norm $N\left(\sum_{i=1}^{P} e_i X_i^{(\nu)}\right)$ für großes ν beschränkt, welche ganzen rationalen Werte auch die e_i haben, so daß auch die $X_1^{(\nu)}$, $X_2^{(\nu)}$,..., $X_p^{(\nu)}$ nur endlichviele Werte annehmen können, folglich auch die $u^{(\nu)}$, sobald ν groß ist, w. z. b. w. (IV 6 C.)

Reviewer: Mahler, Dr. K. (Groningen)

Full Text: DOI EuDML

References:

[1] Afin de réserver le mot de groupe au sens qu'il a pris depuis Galois, je parlerai toujours de systèmes de points, bien qu'on ait l'habitude en géométrie algébrique de parler de groupes de points sur une courbe.

[2] Ueber die diophantischen Gleichungen vom Geschlecht Null, Acta math. t. 14 (1890), p. 217.

[3] Sur les propriétés arthmétiques des courbes algébriques, J. de Liouville (V), t. 7 (1901), p. 161.

[4] On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. of the Cambridge Philos. Soc., t. 21 (1922), p. 179.–Sur l'ensemble de la question, on consultera T. Nagell,L'Analyse Indéterminée de degré supérieur (Paris, Gauthiers-Villars, Collection "Mémorial des Sciences Mathématiques") où se trouve aussi une bibliographie étendue.

[5] Je dois encore signaler tout particulièrement de remarquables résultats de B. L. van der Waerden, qui paraîtront dans les Math. Ann. sous le titreZur Produktzerlegung der Ideale in ganz-abgeschlossenen Ringen, et qui, entre autres applications importantes, semblent susceptibles d'être employés avec fruit à l'étude des questions abordées dans notre chapitre I.

[6] {\(\lambda\)}/{\(\mu\)} signifie que l'idéal {\(\mu\)} est divisible par {\(\lambda\)}.

[7] La définition des distributions rationnelles et la règle faisant correspondre à toutA des fonctionsx A ,y A ont été formulées justement de telle sorte qu'il en soit bien ainsi.

[8] Une telle théorie serait également indispensable pour asseoir sur des bases solides la théorie des fonctions algébriques de plusieurs variables et la géométrie algébrique (cf. pour les courbes algébriques le mémoire bien connu de Dedekind et Weber,Theorie der algebraischen Funktionen einer Veränderlichen, J. de Crelle, t. 92 (1882), p. 181). Elle rentre naturellement dans le cadre des travaux généraux de E. Noether (v. p. ex.Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörper, Math. Ann. t. 96 (1926), p. 26) et de W. Krull (Theorie der allgemeinen Zahlringe, Math. Ann. t. 99 (1928), p. 51); elle présente cependant encore des difficultés considérables. Dans cet ordre d'idées, on consultera avec grand profit les travaux de B. L. van der Waerden, particulièrementZur Nullstellentheorie der Polynomideale, Math. Ann. t. 96 (1926), p. 183, ainsi que le mémoire cité note.· doi:10.1515/crll.1882.92.181

[9] Ces dénominations de pged, de produit, etc., reçoivent leur sens plein par la considération des idéaux dans le corps des fonctions rationnelles surV. Nos "surfaces" et nos "systèmes de surfaces" ne sont autres, en effet, que les "Primdivisoren" et les "Divisoren" de B. L. van der Waerden (loc. cit. note5, {\S} 8), au travail duquel on pourra donc se reporter pour des démonstrations purement algébriques de nos affirmations.

[10] Il est essentiel, pour qu'il en soit ainsi, queV soit sans singularité ou du moins transformable en une variété sans singularité par une transformation birationnelle et biunivoque sans exception; et il n'en serait pas ainsi, par exemple, sur un cône du second degré. Je dois cette remarque et cet exemple à B. L. van der Waerden.

[11] Hilbert,Ueber die Theorie der algebraischen Formen, Math. Ann. t. 36 (1890), p. 473 (v. {\S} 1, Th. 1). Cf. sur ce théorème les mémoires de E. Noether et B. L. van der Waerden déjà cités. · Zbl 22.0133.01 · doi:10.1007/BF01208503

[12] Ici, contrairement au cas oùV était à une dimension, le pged du numérateur et du dénominateur n'est plus nécessairement un idéal borné.

[13] Sur les propriétés, utilisées ici, des fonctions thêta, v. p. ex. Krazer-Wirtinger,Enzykl. d. math. Wiss. II, B. 7.

[14] La démonstration repose d'une part sur l'application, convenablement effectuée, du théorème de la base finie démontré dans le présent travail, et d'autre part sur une extension nouvelle des méthodes d'approximation des nombres algébriques qui tirent leur origine des travaux de Axel Thue. Les théorèmes antérieurs de Thue et de Siegel sur les équations indéterminées ne sont que des cas particuliers du résultat général cité ici.