Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes.

Von

Karl Dörge in Köln.

Der Hilbertsche Irreduzibilitätssatz besagt das Folgende:

$$F(x_1, x_2, \ldots, x_m, t_1, \ldots, t_s)$$

sei ein im Bereich P der rationalen Zahlen irreduzibles Polynom von $x_1, \ldots, x_m, t_1, \ldots, t_s$ mit ganzen rationalen Koeffizienten. Dann kann man für $t_1, \ldots, t_s$ auf unendlich viele Arten solche ganze rationale Zahlen $t_1^0, \ldots, t_s^0$ wählen, daß $F(x_1, \ldots, x_m, t_1^0, \ldots, t_s^0)$ als Polynom der x in P irreduzibel ist. D. Hilbert hat den Satz im Jahre 1892 in Crelles Journal **110** bewiesen. Einen etwas einfacheren Beweis gab Mertens 1911 in den Wiener Akademieberichten. Erst Th. Skolem hat den Satz im Jahre 1921 in seiner Arbeit „Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen" für den Fall, daß F nur von einer Variablen x und einem Parameter t abhängt, verschärft, indem er folgendes zeigte: Die Folge aller ganzen rationalen positiven [1]) Zahlen t, für welche $F(x, t)$ in P zerfällt, sei $t_1 < t_2 < t_3 < \ldots$. Ist dann $A(S)$ die Anzahl derjenigen unter ihnen, welche unterhalb der reellen Zahl S liegen, so gilt

$$\lim_{S \to \infty} \frac{A(S)}{S} = 0.$$

Ich habe in meiner in den Math. Annalen **95**, S. 84—97 erschienenen Note „Zum Hilbertschen Irreduzibilitätssatz" [2]) die Skolemsche Methode verschärft und folgendes erhalten: Es gibt eine positive Zahl α zwischen 0 und 1, so daß statt der Skolemschen Relation die schärfere besteht

$$\text{(I)} \qquad \lim_{S \to \infty} \frac{A(S)}{S^{1-\alpha}} = 0.$$

[1]) Alles, was hier und im folgenden von den positiven Zahlen ausgesprochen wird, gilt analog für die negativen Zahlen.

[2]) Im folgenden benutze ich die Abkürzungen H. I. für Hilbertscher Irreduzibilitätssatz, Z. H. I. für „Zum Hilbertschen Irreduzibilitätssatz".

Entsprechendes ließ sich dort zeigen für den allgemeinen Fall, in dem es sich um Polynome der Form $F(x_1, \ldots, x_m, t_1, \ldots, t_s)$ handelt, welche also von beliebig vielen Variablen und beliebig vielen Parametern abhängen. In meiner Note „Über die Seltenheit der reduziblen Polynome und der Normalgleichungen“ [3]), die in den Math. Annalen **95**, S. 247—256, erschienen ist, zeigte ich, daß man in wichtigen Spezialfällen des H. I. die Relation (I) sehr einfach aus dem Mittelwertsatz der Differentialrechnung folgern kann. Erst als ich dies vortrug, wurde ich von Herrn Professor E. Schmidt darauf aufmerksam gemacht, daß man nicht nur die Spezialfälle auf diese Weise behandeln kann, sondern daß wohl ebenso einfach der allgemeine Irreduzibilitätssatz mit der Verschärfung (I) folgt, wenn man nicht den Mittelwertsatz, sondern eine von H. A. Schwarz herrührende Verallgemeinerung desselben benutzt. Damit ist ein sehr einfacher Beweis der Verschärfung (I) des Irreduzibilitätssatzes erhalten, welcher in folgendem dargestellt werden soll [4]). Der Beweis benutzt außer dem verallgemeinerten Mittelwertsatz nur die auch allen bisherigen Beweisen zugrunde liegende Reihenentwicklung der algebraischen Funktionen.

Erster Teil:

Polynome von einer Variablen und einem Parameter.

Sei also $F(x, t)$ ein in P irreduzibles Polynom von x und t. Der Grad in x sei n. Sieht man nun immer von denjenigen, endlich vielen ganzen rationalen Werten t ab, für die x^n aus F herausfällt, so genügt es für das Folgende, wie ich in Z. H. I. gezeigt habe, sich auf den Fall zu beschränken, daß in $F(x, t)$ — aufgefaßt als Polynom von x — der Koeffizient des höchsten Gliedes x^n gleich 1 ist. Sei dies also der Fall. Die Folge sämtlicher ganzer rationaler positiver Werte t, für die $F(x, t)$ als Funktion von x in P zerfällt, sei wieder $t_1 < t_2 < t_3 < \ldots$. Die Menge dieser Werte ist, wie in Z. H. I. gezeigt worden ist, enthalten in einer Menge, welche aufgefaßt werden kann als die Vereinigungsmenge endlich vieler Mengen, die man so erhält: Es existieren gewisse Funktionen $\varphi_1(t), \varphi_2(t), \ldots, \varphi_N(t)$. Diese Funktionen entstehen durch alle möglichen Zerlegungen von $F(x, t)$ im Gebiet der Potenzreihen, genauer Laurentreihen, nach gebrochenen Potenzen von t. Jede von ihnen hat die Gestalt

$$\varphi(t) = a t^{\frac{k}{q}} + b t^{\frac{k-1}{q}} + \ldots + c + d \frac{1}{t^{\frac{1}{q}}} + \ldots .$$

---

[3]) Im folgenden abgekürzt als R. P.

[4]) Gleichzeitig ergibt sich hier nunmehr, daß es möglich ist, eine geeignete Zahl α, mit der die Ungleichung (I) besteht, allein mittels der Grade von F zu bestimmen.

Darin ist q eine ganze rationale positive, k eine ganze rationale Zahl. $a, b, \ldots$ sind von t unabhängige reelle oder komplexe Konstanten. Die Anzahl N ist höchstens 2^{n-1}. Keine der Funktionen reduziert sich auf ein Polynom von t mit rationalen Koeffizienten. Jeder Funktion φ_ν ordne man die Folge aller ganzen rationalen positiven Werte $t_1^{(\nu)} < t_2^{(\nu)} < t_3^{(\nu)} < \ldots$ zu, für welche $\varphi_\nu(t_\mu^{(\nu)})$ eine ganze rationale Zahl wird. Die Folge der ganzen rationalen positiven Werte t, für welche $F(x, t)$ in P zerfällt, ist dann enthalten in der Folge, welche durch Vereinigung der N Folgen $t_1^{(\nu)} < t_2^{(\nu)} < t_3^{(\nu)} < \ldots$ entsteht.

Sei nunmehr

$$\varphi(t) = a t^{\frac{k}{q}} + b t^{\frac{k-1}{q}} + \ldots + c + d \frac{1}{t^{\frac{1}{q}}} + \ldots$$

eine der N Funktionen φ_ν und — unter Änderung der Bezeichnung gegenüber dem Früheren — sei

$$(II) \qquad t_1 < t_2 < t_3 < \ldots$$

die Folge der ganzen rationalen positiven Werte t, für die $\varphi(t_\nu)$ eine ganze rationale Zahl ist. Diese Folge enthalte nicht nur endlich viele Elemente. Dann kann $\varphi(t)$ nicht ein Polynom von t sein. Denn in diesem Falle müßte es rationale Koeffizienten enthalten. Dies ist aber nach Voraussetzung nicht der Fall. Ferner müssen — vgl. R. P., Beweis des ersten Hilfssatzes — sämtliche Koeffizienten $a, b, \ldots$ reell sein; im entgegengesetzten Fall wäre nämlich $\varphi(t)$ nur für endlich viele ganze rationale Werte t reell.

Nun verwenden wir folgenden Satz von H. A. Schwarz [5]):

$$t_\nu < t_{\nu+1} < \ldots < t_{\nu+n}$$

seien reelle Zahlen. Es sei $f(t)$ eine reelle, in dem Intervall $t_\nu < t < t_{\nu+n}$ mindestens n mal differenzierbare und bei t_ν und $t_{\nu+n}$ stetige Funktion. Dann gibt es zwischen t_ν und $t_{\nu+n}$ eine Stelle τ derart, daß die Gleichung besteht

$$n! \frac{\begin{vmatrix} 1 & t_\nu & t_\nu^2 & \ldots & t_\nu^{n-1} & f(t_\nu) \\ 1 & t_{\nu+1} & t_{\nu+1}^2 & \ldots & t_{\nu+1}^{n-1} & f(t_{\nu+1}) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & t_{\nu+n} & t_{\nu+n}^2 & \ldots & t_{\nu+n}^{n-1} & f(t_{\nu+n}) \end{vmatrix}}{\begin{vmatrix} 1 & t_\nu & \ldots & t_\nu^{n-1} & t_\nu^n \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & t_{\nu+n} & \ldots & t_{\nu+n}^{n-1} & t_{\nu+n}^n \end{vmatrix}} = f^{(n)}(\tau).$$

[5]) Ges. math. Werke 2, S. 236–237.

Diesen Satz wenden wir auf die Funktion φ an, indem wir für $t_\nu, t_{\nu+1}, \ldots, t_{\nu+n}$ aufeinanderfolgende Werte unserer Folge (II) setzen. n wählen wir so groß, daß $\varphi^{(n)}$ nur noch negative Potenzen von $t^{\frac{1}{q}}$ enthält[6]). Beachten wir dann, daß der Nenner links das Differenzenprodukt der $t_\nu, \ldots, t_{\nu+n}$ ist, so schließen wir daraus wie in R. P., Hilfssatz 1 und 2: Es gibt eine positive Zahl α zwischen 0 und 1, so daß die Ungleichung besteht

$$t_{\nu+n} - t_\nu > t_\nu^\alpha. \tag{III}$$

Daraus schließt man wiederum wie in R. P.: Bedeutet $A(S)$ die Anzahl der t Werte aus (II) unterhalb S, so ist von einer gewissen Zahl S ab

$$A(S) \leqq \text{konst. } S^{1-\alpha}. \tag{IV}$$

Für jede der N Folgen $t_1^{(\nu)} < t_2^{(\nu)} < \ldots$ gilt also eine Formel (IV). *Also gilt für die Folge, welche durch Vereinigung der N Folgen entsteht und welche alle t, für die $F(x, t)$ in P zerfällt, enthält, ebenfalls eine Ungleichung der Gestalt* (IV)[7]).

Dazu hat man nur für α die kleinste der N erhaltenen Zahlen α und für konst. die Summe der N erhaltenen, mit konst. bezeichneten Größen zu verstehen. Dabei ergibt sich hier nunmehr auch, daß es möglich ist, eine Zahl α, für die die Ungleichung (IV) besteht, bereits dann anzugeben, wenn man nur eine obere Schranke für die höchsten Exponenten der Reihen φ_ν kennt. Eine solche obere Schranke kann man bestimmen, wenn man nur die Grade von F kennt. *Es ist also eine geeignete Zahl α allein durch die Grade von F bestimmbar.*

Etwas schärfer kann man für die Folge der t, für die $F(x, t)$ in P zerfällt, aus (III) auch den folgenden Satz ableiten: *Es gibt eine positive ganze rationale Zahl M und eine positive Zahl α, so daß von einem gewissen Index ab die Ungleichung besteht*

$$t_{\nu+M} - t_\nu > t_\nu^\alpha. \tag{V}$$

Darin können geeignete Zahlen M und α allein durch die Grade von F bestimmt werden. Eine ganz grobe Abschätzung zeigt, daß man ein geeignetes Zahlenpaar α, M auf folgende Weise erhält. Unter Auszeichnung von x habe F die Gestalt $F(x, t) = a_0(t)x^n + a_1(t)x^{n-1} + \ldots + a_n(t)$. Die Grade der a_ν in bezug auf t seien g_ν für $\nu = 0, 1, \ldots, n$. Unter M

[6]) Tatsächlich empfiehlt es sich, um einen möglichst günstigen Wert α zu erhalten, $2\left[\frac{k}{q}\right]$ oder $2\left[\frac{k}{q}\right]+1$ oder $2\left[\frac{k}{q}\right]+2$ mal zu differenzieren.

[7]) Daraus folgt das Bestehen der Relation (I). Unser Satz ist also bewiesen.

verstehe man $\frac{n}{2}$ Max $\left(\frac{g_\nu}{\nu}+\frac{\nu-1}{\nu}g_0\right)$ [8]) für $\nu=1, 2, \ldots, n$. Setzt man dann

$$\alpha=\frac{[\mathsf{M}]}{([\mathsf{M}]+1)(2[\mathsf{M}]+1)}, \qquad M=2[\mathsf{M}]+1,$$

so besteht mit diesem Paar α, M die Ungleichung (V). Diese ist jedoch im Falle $\mathsf{M}<1$ nichtssagend, weil dann $\alpha=0$ wird. Man kann auch in diesem Falle leicht ein geeignetes Paar α, M bestimmen.

Zweiter Teil:

Der allgemeine Fall.

Der allgemeine Fall, in dem es sich um Polynome von beliebig vielen Variablen und beliebig vielen Parametern handelt, läßt sich im wesentlichen auf den im ersten Teil behandelten Fall zurückführen. Wir stützen uns dabei auf einen von Kronecker herrührenden Satz, mittels dessen man die Frage, ob ein Polynom von mehreren Veränderlichen zerfällt, auf die Frage zurückführt, ob ein dem ursprünglichen zuzuordnendes Polynom einer Veränderlichen in der Weise zerfällt, daß in den Faktoren nur Exponenten auftreten, welche einer gewissen Bedingung unterliegen [9]). Die Zuordnung geschieht dabei auf folgende Weise: Das zu untersuchende Polynom sei $F(x_1, x_2, \ldots, x_m)$. Sein Grad [10]) sei h. Man setze $d=h+1$. Dann mache man die Substitution $x_\mu=\xi^{d^\mu}$, $\mu=1, 2, \ldots, m$. Dadurch geht $F(x_1, \ldots, x_m)$ in ein Polynom $F(\xi)$ der einen Variablen ξ über. Dann gilt der Satz: $F(x_1, \ldots, x_m)$ zerfällt in P als Polynom der x dann und nur dann in zwei Faktoren, wenn $F(\xi)$ in P derart in zwei Faktoren zerfällt, daß diese nur Glieder mit — von E. Noether so genannten — induzierten Exponenten enthalten.

Wir betrachten nun zunächst Polynome, welche von beliebig vielen Variablen, aber nur von einem Parameter abhängen, welche also die Gestalt $F(x_1, \ldots, x_m, t)$ haben. Dabei sei F wiederum als Polynom von $x_1, \ldots, t$ in P irreduzibel. Wir fragen nach den ganzen rationalen positiven Werten t^0, für die es als Polynom von $x_1, \ldots, x_m$ in P zerfällt. Wir machen dazu

---

[8]) Das gilt auch, wenn man bei der Bestimmung von M von dem in bezug auf x reziproken Polynom ausgeht, also g_ν mit $g_{n-\nu}$ vertauscht, für $\nu=0, 1, \ldots, n$. Das folgt daraus, daß ein Polynom dann und nur dann in P zerfällt, wenn das reziproke Polynom in P zerfällt.

[9]) Auf diese Bedingung für die Exponenten wurde hingewiesen von E. Noether: Ein algebraisches Kriterium für absolute Irreduzibilität, Math. Annalen 85.

[10]) Unter dem Grade von F verstehen wir die höchste der Exponentensummen der Potenzprodukte von F.

die Substitution $x_\mu = \xi^{d^\mu}$. Dabei geht $F(x_1, \ldots, x_m, t)$ in ein Polynom $F(\xi, t)$ über. Von diesem wissen wir dann das Folgende: Aufgefaßt als Polynom von ξ zerfällt es — bei variablem t — nicht derart in dem Körper, der durch Adjunktion der Variablen t zu P entsteht, in zwei Faktoren, daß diese nur induzierte Exponenten enthalten. Soll nun aber für die ganze rationale Zahl t das Polynom $F(x_1, \ldots, x_m, t)$ in P zerfallen, also $F(\xi, t^0)$ in P in zwei Faktoren zerfallen, die nur induzierte Exponenten enthalten, so muß für diesen Wert t^0 — wie man sich wiederum analog den Ausführungen von Z. H. I. leicht überlegt — entweder mindestens eine von gewissen Funktionen $\varphi(t)$, welche die im ersten Teil angegebene Gestalt haben, einen rationalen — und wenn man, wie wir wieder annehmen, $F(\xi, t)$ durch die in Z. H. I. angegebene Transformation als Polynom von ξ normiert hat — einen ganzen rationalen Wert annehmen oder mindestens eine von gewissen Funktionen $\varphi(t)$ derselben Gestalt, welche aber nunmehr sich auch auf Polynome von t mit rationalen Koeffizienten reduzieren können, verschwinden. Das Letztere tritt nur für endlich viele ganze rationale Zahlen t ein. Daher ist wiederum nur die erste Bedingung wesentlich. *Daher gilt, wie im ersten Teil, für die Folge der positiven ganzen rationalen Zahlen t^0, für die $F(x_1, \ldots, x_m, t^0)$ in P zerfällt, wiederum die Ungleichung* (I).

Haben wir es nun mit Polynomen $F(x_1, \ldots, x_m, t_1, \ldots, t_s)$ zu tun, welche also auch von beliebig vielen Parametern abhängen, so gehen wir schrittweise vor. Wir fassen zunächst allein t_s als Parameter auf, also $x_1, \ldots, t_{s-1}$ sämtlich als Variable. Dann denken wir uns hierin die ganzen rationalen Zahlen t_s^0 bestimmt, für die $F(x_1, \ldots, x_m, t_1, \ldots, t_{s-1}, t_s^0)$ in P irreduzibel ist. Für jede feste der so bestimmten Zahlen t_s^0 fassen wir dann t_{s-1} allein als Parameter auf und schreiten so fort, bis wir die Systeme $t_1^0, \ldots, t_s^0$ erhalten, für welche $F(x_1, \ldots, x_m, t_1^0, \ldots, t_s^0)$ in P irreduzibel ist. Dabei erhalten wir den folgenden Satz: Eine Menge von ganzen rationalen positiven Zahlen $t_1 < t_2 < t_3 < \ldots$ heiße „*dicht in bezug auf die positive Zahl α*“, wenn für sie die Ungleichung (I) *nicht* besteht, wenn also erfüllt ist:

$$\text{(VI)} \qquad \overline{\lim_{S \to \infty}} \frac{A(S)}{S^{1-\alpha}} > 0.$$

Man habe nun eine in bezug auf die positive Zahl α dichte Menge von Zahlen t_1. Jede dieser Zahlen verbinde man mit Zahlen t_2 zu Systemen von je zwei Zahlen, und zwar soll jedes t_1 mit einer — für die verschiedenen t_1 nicht notwendig übereinstimmenden — in bezug auf α_2 dichten Menge von Zahlen t_2 verbunden werden. Jedes dieser Paare verbinde man mit einer — für die verschiedenen Paare nicht notwendig

übereinstimmenden — in bezug auf α_3 dichten Menge von Zahlen t_3. Indem man so fortfährt, erhält man eine Menge von Systemen ganzer rationaler positiver Zahlen $t_1, t_2, \ldots, t_s$. Die Menge dieser Systeme werde „*in bezug auf* $\alpha_1, \alpha_2, \ldots, \alpha_s$ *dicht*“ genannt. Dann gilt der H. I. in der folgenden Form: *$F(x_1, \ldots, x_m, t_1, \ldots, t_s)$ sei in P irreduzibel. Dann lassen sich allein mittels der Grade von F positive Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_s$ derart bestimmen, daß in jeder in bezug auf $\alpha_1, \alpha_2, \ldots, \alpha_s$ dichten Menge von Systemen ganzer rationaler positiver Zahlen $t_1, \ldots, t_s$ sich solche Systeme befinden, für die F als Polynom der x in P irreduzibel wird.*

(Eingegangen am 10. 8. 1925.)

Berichtigung

zu dem Aufsatz von K. Dörge, „Über die Seltenheit der reduziblen Polynome und der Normalgleichungen“ in Math. Ann. **95**, S. 247—256:

S. 255 Z. 4 v. u. statt $n' < n$ lies $n' \leqq n$.