Zum Hilbertschen Irreduzibilitätssatz.

Von

Karl Dörge in Berlin.

In Crelles Journal, Band 110, beweist D. Hilbert den folgenden Satz: $F(x, y, \ldots, w; t_1, \ldots, t_s)$ sei ein im natürlichen Rationalitätsbereich P irreduzibles Polynom von $x, y, \ldots, t_s$ mit ganzen rationalen Koeffizienten. Dann gibt es ganze rationale Zahlen $t_1^0, t_2^0, \ldots, t_s^0$, so daß $F(x, y, \ldots, w; t_1^0, \ldots, t_s^0)$ als Funktion von $x, y, \ldots, w$ in P irreduzibel ist.

Th. Skolem[1]) hat diesen Satz für den Fall, daß es sich um Polynome der Form $F(x, t)$ handelt, dahin verschärft, daß für die ganzen rationalen positiven t-Werte,

$$t_1 < t_2 < t_3 < \ldots,$$

für die F als Funktion von x in P zerfällt, und deren Anzahl unterhalb ν mit $N(\nu)$ bezeichnet werde, die Relation besteht

$$N(\nu) = o(\nu),$$

wo o das Landausche Symbol bezeichnet.

Ich werde in dieser Arbeit einen Satz beweisen, der besagt, daß die Systeme ganzer rationaler Werte $t_1, t_2, \ldots, t_s$, für die F in P zerfällt, sehr selten sind, so daß im Falle der Funktionen der Form $F(x, t)$ die Skolemsche Bedingung dahin verschärft wird, daß es eine positive Zahl α gibt, für die gilt

$$N(\nu) = o(\nu^{1-\alpha}).$$

Im allgemeinen Falle erhalte ich einen Satz, aus dem z. B. folgt: Man kann für $t_1, t_2, \ldots, t_s$ Primzahlen wählen, so daß dafür F in P irreduzibel wird.

---

[1]) Th. Skolem, „Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen“, erschienen in Kristiania.

In § 5 forme ich den Satz etwas um und erhalte z. B. das Resultat: In jedem beliebig kleinen Würfel des Raumes mit den Koordinaten $t_1, t_2, \ldots, t_s$ gibt es einen Punkt mit rationalen Koordinaten, für den F in P irreduzibel ist[2]).

In § 6 wende ich die vorher benutzte Puiseuxsche Entwicklung der algebraischen Funktionen auf das E. Noethersche[3]) Kriterium für absolute Irreduzibilität an und gewinne damit auf analytischem Wege einen Teil desselben, genauer eine unmittelbare Folgerung des Satzes, aus der aber dieser nicht zurückfolgt. Überlegungen derselben Art führen aber auch — wie ich am Schluß kurz andeute — zu Sätzen über das Zerfallen im Körper der reellen Zahlen, die in dem Noetherschen Kriterium nicht enthalten sein dürften. Der Fall, daß $F(x, y, \ldots, w; t)$ in bezug auf t absolut irreduzibel ist, erscheint in dieser Arbeit als der einfacher zu behandelnde Teil des Hilbertschen Irreduzibilitätssatzes.

Herrn Dr. Walter Dubislav, Berlin, spreche ich für Anregungen zu § 6 meinen besten Dank aus.

Über meinen Sprachgebrauch möchte ich folgendes bemerken:

Unter einer ganzen Zahl verstehe ich immer eine ganze rationale Zahl. Unter $x^{\frac{\varkappa}{q}}$ mit ganzem positivem q und $\varkappa$ verstehe ich $\left(x^{\frac{1}{q}}\right)^{\varkappa}$, wobei wir von vornherein für $x^{\frac{1}{q}}$ immer den Ausdruck mit der kleinsten möglichen Amplitude wählen.

§ 1.

Der Hilfssatz und Vorbemerkungen über dichte und dünne Mengen.

In meiner Arbeit „Zur Theorie der diophantischen Gleichungen mit zwei Unbekannten", welche in der Mathematischen Zeitschrift erscheint, habe ich das Folgende bewiesen:

Hilfssatz. *Die Reihe*

$$\varphi(t) = a_{-k} t^{\frac{k}{q}} + a_{-(k-1)} t^{\frac{k-1}{q}} + \ldots + a_0 + a_1 \frac{1}{t^{\frac{1}{q}}} + \ldots,$$

in welcher k ganz, q positiv und ganz sein mögen, möge für absolut hinreichend große t konvergieren. $\varphi(t)$ sei nicht ein Polynom in t mit

---

[2]) Für den Spezialfall, daß die Gleichung von Primzahlgrad ist und die Koeffizienten selbst als Parameter aufgefaßt werden, findet sich dieser Satz schon im Weberschen Lehrbuch der Algebra I.

[3]) E. Noether, „Ein algebraisches Kriterium für absolute Irreduzibilität", Math. Ann. 85. Für den hier in Betracht kommenden Sonderfall gewöhnlicher Zahlkörper hat auch Herr Ostrowski den Satz aufgestellt und bewiesen.

rationalen Koeffizienten. Wir betrachten dann die Reihe der positiven ganzen Zahlen

$$t_1 < t_2 < t_3 < \ldots,$$

für die $\varphi(t)$ eine ganze Zahl werden möge. Dann gibt es eine positive, ganze Zahl m und eine positive Zahl α, so daß von einem Index ν an gilt

$$t_{\nu+m} - t_\nu > t_\nu^\alpha.$$

Ebenso gilt für die Reihe der negativen ganzen Zahlen

$$t_1' > t_2' > t_3' > \ldots,$$

für die $\varphi(t)$ ganz wird: Es gibt eine ganze positive Zahl m' und eine positive Zahl α', so daß von einem Index ν an gilt

$$|t'_{\nu+m'} - t'_\nu| > t'^{\alpha}_\nu.$$

Wir verzichten hier auf die Wiederholung des Beweises.

Wir führen die folgende Bezeichnungsweise ein:

Definition. *Gegeben sei eine Menge ganzer positiver und negativer Zahlen t. Die Anzahl derjenigen, deren Betrag unterhalb ν liegt, sei $N(\nu)$. Die Menge soll dann und nur dann „dünn“ heißen, wenn es eine positive Zahl α gibt, so daß gilt*

$$N(\nu) = o(\nu^{1-\alpha}).$$

Eine Menge ganzer Zahlen, die nicht dünn ist, soll „dicht“ heißen.

Haben wir es nun mit endlich vielen Mengen ganzer Zahlen zu tun, so verstehen wir unter der Vereinigungsmenge der Mengen diejenige Menge, welche aus allen verschiedenen Zahlen besteht, die in einer der endlich vielen Mengen vorkommen. Dann gilt offenbar: Die Vereinigungsmenge von endlich vielen Mengen ist dann und nur dann dünn, wenn jede Menge dünn ist. Jede Menge, die nur aus endlich vielen Zahlen besteht, ist dünn.

Wir kommen nun noch einmal auf unsern Hilfssatz zurück und betrachten die *ganzen Zahlen t, für die $\varphi(t)$ ganz ist.* Wir wollen zeigen, daß *diese Menge dünn* ist. Dazu brauchen wir nur zu zeigen, daß die Menge der positiven Zahlen t für sich und die Menge der negativen Zahlen t für sich dünn ist. Da der Beweis für die negativen Zahlen ebenso verläuft, führen wir ihn nur für die positiven Zahlen

$$t_1 < t_2 < t_3 < \ldots.$$

β sei eine positive Zahl unterhalb 1. Die Menge der Zahlen t, die unterhalb ν liegen, zerfällt dann in zwei Klassen, einerseits die Zahlen, die unterhalb ν^β liegen, andrerseits die andern. Die Anzahl der Zahlen der ersten Klasse sei A_1, die der anderen sei A_2. Dann gilt $A_1 \leqq \nu^\beta$ und wegen des Hilfssatzes $\frac{A_2}{\nu} \leqq \frac{m+1}{\nu^{\alpha\cdot\beta}}$. Hieraus folgt für jede Zahl β'

$$\frac{\nu^{\beta'} N(\nu)}{\nu} \leqq \nu^{\beta+\beta'-1} + (m+1)\,\nu^{\beta'-\alpha\beta}.$$

Dies aber konvergiert, sobald $\beta + \beta' < 1$ und $\beta' < \alpha\beta$ ist, mit wachsendem ν gegen 0. Wählt man also β und β' so, daß diese beiden Ungleichungen erfüllt sind, so ist sicher

$$\lim_{\nu\to\infty} \frac{\nu^{\beta'} N(\nu)}{\nu} = 0.$$

Also ist die Menge der t dünn.

Definition. *Eine Menge ganzer Zahlen t soll „sehr dicht" heißen, wenn für jede positive Zahl α gilt*

$$\varliminf_{\nu\to\infty} \frac{\nu^{\alpha} N(\nu)}{\nu} > 0.$$

Jede sehr dichte Menge ist dann dicht.

Man denke sich nun zwei unendliche sehr dichte Mengen positiver ganzer Zahlen steigend angeordnet

$$t_1 < t_2 < t_3 < \dots$$

und

$$i_1 < i_2 < i_3 < \dots .$$

Dann gilt der Satz:

$$t_{i_1},\ t_{i_2},\ t_{i_3},\ \dots$$

ist sehr dicht. Da nämlich die Menge der $t_1 < t_2 < \dots$ sehr dicht ist, gilt für jedes positive α

$$\varliminf_{\nu\to\infty} \frac{t_{i_\nu}^{\alpha}\, i_\nu}{t_{i_\nu}} > 0,$$

und weil die i sehr dicht sind, gilt für jede positive Zahl β

$$\varliminf_{\nu\to\infty} \frac{i_\nu^{\beta}\cdot \nu}{i_\nu} > 0.$$

Durch Multiplikation entsprechender Glieder dieser beiden Folgen bekommen wir

$$\varliminf_{\nu\to\infty} \frac{t_{i_\nu}^{\alpha}\, i_\nu^{\beta}\cdot \nu}{t_{i_\nu}} > 0.$$

Hieraus folgt wegen $i_\nu \leqq t_{i_\nu}$

$$\varliminf_{\nu\to\infty} \frac{t_{i_\nu}^{\alpha+\beta}\cdot \nu}{t_{i_\nu}} > 0$$

bei beliebigen positiven Zahlen α und β. Daraus aber folgt: $t_{i_1}, t_{i_2}, \ldots$ ist wieder sehr dicht.

Die Menge der positiven Primzahlen

$$p_1 < p_2 < p_3 < \ldots$$

ist sehr dicht, denn hier gilt

$$\lim_{\nu \to \infty} \frac{\log \nu \cdot N(\nu)}{\nu} = 1 .$$

Unter den Primzahlen zweiter Klasse verstehen wir diejenigen Primzahlen, deren Index eine Primzahl ist. Wir denken uns diese wieder aufsteigend angeordnet und mit den Indizes $1, 2, \ldots$ neu versehen. Diejenigen Primzahlen zweiter Klasse, deren Index dann eine Primzahl wird, nennen wir die Primzahlen dritter Klasse usw. Nach unserm Satze bildet dann jede Klasse von Primzahlen eine sehr dichte Menge.

§ 2.

Das Zerfallen von Polynomen mit einem Parameter in Faktoren, die eine Variable gemeinsam enthalten.

$F(x, y, z, \ldots, v, w; t)$ sei ein Polynom in $x, \ldots, t$ mit ganzen Koeffizienten. Der Grad in x sei n. F sei in x normiert, beginne also mit dem Gliede x^n. Deshalb werden wir in Zukunft beachten, daß jede Zerlegung von F in zwei Faktoren mit rationalen Koeffizienten, die beide x enthalten und beide in x normiert sind, von selbst eine Zerlegung in Faktoren mit ganzzahligen Koeffizienten darstellt. Wir betrachten die Gleichung

$$F(x, y, z, \ldots, v, w; t) = 0 .$$

Durch sie wird x als algebraische Funktion von $y, \ldots, t$ definiert. Dadurch bekommen wir n Wurzelfunktionen $x_1, x_2, \ldots, x_n$. Es gelten dann Darstellungen der Art

$$x_\nu = a_{-k}^{(\nu)} y^{\frac{k}{q}} + a_{-(k-1)}^{(\nu)} y^{\frac{k-1}{q}} + \ldots + a_0^{(\nu)} + a_1^{(\nu)} \frac{1}{y^{\frac{1}{q}}} + \ldots .$$

Die Koeffizienten a sind Funktionen von $z, \ldots, w, t$, und zwar läßt sich jedes a in der Form darstellen[4]):

$$a_\varkappa^{(\nu)} = b_{-l}^{(\nu,\varkappa)} z^{\frac{l}{q_1}} + b_{-(l-1)}^{(\nu,\varkappa)} z^{\frac{l-1}{q_1}} + \ldots + b_0^{(\nu,\varkappa)} + b_1^{(\nu,\varkappa)} \frac{1}{z^{\frac{1}{q_1}}} + \ldots .$$

---

[4]) Vgl. Th. Skolem, l. c. [1]), S. 32.

Hierin bedeuten die b Funktionen von den übrigen Variablen, welche sich als Funktionen von diesen durch ähnliche Reihen darstellen lassen, bis wir endlich zu Koeffizienten gelangen, welche Reihen in $t^{\frac{1}{q_s}}$ sind mit konstanten Koeffizienten.

Das Gebiet, in welchem die Reihenfunktionen, die wir so erhalten haben, konvergieren, sieht so aus: Zu jeder Zahl t, deren Betrag oberhalb einer gewissen Zahl T liegt, kann man eine Zahl $W(t)$ bestimmen, zu jedem Paar w, t, in dem $|t| > T$ und $|w| > W(t)$ ist, kann man eine Zahl $V(w, t)$ bestimmen, ..., endlich kann man zu jedem System von Zahlen $z, \ldots, t$, die gewissen Größenbedingungen unterliegen, eine Zahl $Y(z, \ldots, t)$ bestimmen, so daß gilt: Ist $|t| > T$, $|w| > W(t), \ldots, |y| > Y(z, \ldots, t)$, so konvergiert jede der Reihenfunktionen x_ν.

Unter den Wurzelfunktionen $x_1, \ldots, x_n$ denken wir uns nun auf alle möglichen Arten ν herausgegriffen, $0 < \nu < n$. Es seien $x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_\nu}$. Die übrigen seien $x_{\alpha_{\nu+1}}, \ldots, x_{\alpha_n}$. Wir bilden dann jedesmal das Paar von Funktionen

$$(x - x_{\alpha_1})(x - x_{\alpha_2}) \ldots (x - x_{\alpha_\nu}), \quad (x - x_{\alpha_{\nu+1}}) \ldots (x - x_{\alpha_n}).$$

Im ganzen erhalten wir so N Paare von Funktionen, die wir f_ν, f_ν^* nennen. Nun setzen wir voraus, daß F nicht in P in zwei Faktoren zerfallen möge, die beide die Variable x enthalten. Dann kann kein Funktionenpaar f_ν, f_ν^* zwei Polynome in $x, y, \ldots, t$ mit rationalen Koeffizienten darstellen.

Dagegen möge für die ganze Zahl t_0, deren Betrag größer als T ist, unser F als Funktion von $x, y, \ldots, w$ zerfallen in Faktoren mit rationalen Koeffizienten, die beide x enthalten. Dann muß also ein gewisses Paar f_ν, f_ν^* für $t = t_0$ in ein Paar von Polynomen in $x, y, \ldots, w$ übergehen mit ganzen Koeffizienten. Dann muß gewiß einer der folgenden Fälle eintreten:

1. f_ν enthält eine gebrochene oder negative Potenz von y oder $z \ldots$ oder w.[5])

2. f_ν ist zwar ein Polynom in $x, y, \ldots, w$, jedoch ist ein Koeffizient nicht ein Polynom in t mit rationalen Koeffizienten.

Möge nun zunächst Fall 1 eintreten. Dann muß t_0 den Koeffizienten des Gliedes zum Verschwinden bringen, das die gebrochene Potenz von y oder $z \ldots$ oder w enthält. Dieser Koeffizient aber hat die Gestalt

$$c_{-p} t^{\frac{p}{q}} + c_{-(p-1)} t^{\frac{p-1}{q}} + \ldots,$$

[5]) In diesem Falle ist F in bezug auf t absolut irreduzibel. Hierauf gehe ich in § 6 noch näher ein.

kann also nur für endlich viele ganze Zahlen t_0 verschwinden. Die Menge der ganzen Zahlen t_0, für die f_ν ein Polynom mit ganzen Koeffizienten wird, ist also in diesem Falle dünn.

Im zweiten Falle muß der Koeffizient, der nicht ein Polynom mit rationalen Koeffizienten ist, aber die im Hilfssatze betrachtete Form hat, einen ganzen Wert annehmen. Also muß nach dem Hilfssatze auch hier die Menge der ganzen Werte t_0, für die f_ν ein Polynom in $x, \ldots, w$ wird, dünn sein. Wir erhalten also: Die Menge der ganzen Werte t_0, für die ein Paar f_ν, f_ν^* in ein Paar von Polynomen in $x, \ldots, w$ mit ganzen Koeffizienten übergeht, ist dünn. Diejenigen ganzzahligen Werte, für die die in P irreduzible Funktion $F(x, y, \ldots, w; t)$ in P in zwei beide x enthaltende Faktoren zerfällt, bilden die Vereinigungsmenge der Mengen der ganzen Zahlen, für die die Paare f_ν, f_ν^* in Paare von Polynomen mit ganzen Koeffizienten übergehen, $\nu = 1, 2, \ldots, N$. Also bilden auch sie eine dünne Menge.

Nun habe F in x nicht den höchsten Koeffizienten 1. Vielmehr sei dieser $h(y, \ldots, t)$. Es sei also

$$F(x, y, \ldots, w; t) = h(y, \ldots, t)x^n + \ldots.$$

Wir betrachten die ganzen Zahlen t_0, für die h verschwindet. Sie bilden eine dünne Menge. Wir setzen

$$x' = x \cdot h(y, \ldots, t)$$

und

$$F^*(x', y, \ldots; t) = (h(y, \ldots, t))^{n-1} F(x, y, \ldots; t).$$

Dann hat F^* in x' den höchsten Koeffizienten 1. Ferner gilt: F zerfällt dann und nur dann für eine solche ganze Zahl t_0, für die $h \neq 0$ ist, in zwei Faktoren mit rationalen Koeffizienten, die beide x enthalten, wenn für t_0 die Funktion F^* in zwei Faktoren mit rationalen Koeffizienten, die beide x' enthalten, zerfällt. Daraus aber folgt: Die Menge der ganzen Zahlen t_0, für die F in zwei x enthaltende Faktoren mit rationalen Koeffizienten zerfällt, ist dünn. Das gleiche gilt auch für $y, z, \ldots, w$. Daraus folgt: *$F(x, y, \ldots, w; t)$ habe ganze Koeffizienten und sei in P irreduzibel. Wir betrachten dann die ganzen Zahlen t_0, für die F in zwei solche Faktoren mit rationalen Koeffizienten zerfällt, die eine der Variablen $x, y, \ldots, w$ gemeinsam enthalten. Ihre Menge ist dünn.*

§ 3.

Das Zerfallen von Funktionen mit einem Parameter in Faktoren, die keine Variable gemeinsam enthalten[6]).

Für wie viele ganze Werte t_0 kann die in P irreduzible Funktion F mit ganzen Koeffizienten in zwei solche Faktoren mit rationalen Koeffizienten zerfallen, die keine Variable gemeinsam haben? Es möge also für t_0 unser F in die Faktoren F_1 und F_2 mit rationalen Koeffizienten zerfallen, so daß (wie man nach einer etwaigen Umnennung der Variablen annehmen kann) F_1 nur die Variablen $x, y, \ldots, r$, F_2 nur die Variablen $s, \ldots, w$ enthält. Wir schreiben F in der Form

$$F = g_0(s, \ldots, w, t) P_0(x, y, \ldots, r) + g_1(s, \ldots, w, t) P_1(x, y, \ldots, r) + \ldots + g_N(s, \ldots, w, t) P_N(x, y, \ldots, r).$$

Hier sollen die P Potenzprodukte nur von $x, y, \ldots, r$, die g also Funktionen von $s, \ldots, w, t$ sein. Es soll natürlich $g_0(s, \ldots, w, t)$ nicht verschwinden. Wegen der Irreduzibilität von F gibt es dann in der Reihe $g_1, g_2, \ldots, g_N$ ein g_ν, so daß gilt: Faßt man die g als Linearformen der Potenzprodukte Q auf, welche aus den Variablen $s, \ldots, w$ gebildet werden können, so ist der Rang der Linearformen g_0, g_ν gleich 2. Daher gilt dasselbe für alle festgewählten Werte t höchstens mit Ausnahme von endlich vielen. Soll nun F für den festen Wert t_0 in der besprochenen Weise zerfallen, so müssen g_0, g_ν für t_0 in den Q den Rang 1 haben. Das kann also nur für endlich viele Werte t_0 eintreten.

Soll nun F für t_0 überhaupt in P zerfallen, so muß das entweder auf die in § 2 oder auf die hier besprochene Weise geschehen. *Also ist die Menge der ganzen rationalen Werte t_0, die ein Zerfallen von $F(x, y, \ldots, t)$ in P verursachen, dünn.*

§ 4.

Das Zerfallen von Funktionen mit beliebig vielen Parametern.

Definition. *Gegeben sei eine Menge von Systemen von je s ganzen Zahlen $t_1, \ldots, t_s$. Diese Menge soll dann und nur dann „dicht" heißen, wenn sie eine Teilmenge von Systemen enthält mit folgender Eigenschaft: Die verschiedenen Zahlen t_1, die in der Teilmenge vorkommen, bilden eine dichte Menge. Jede in der Teilmenge vorkommende Zahl t_1 ist in der Teilmenge mit einer dichten Menge von Zahlen t_2 gepaart. Jedes vorkommende Paar ist mit einer dichten Menge von Zahlen t_3 verbunden. ...*

---

[6]) Die vorliegende einfache Formulierung dieses Beweises verdanke ich Fräulein E. Noether.

Endlich ist jedes vorkommende System $t_1, \ldots, t_{s-1}$ *mit einer dichten Menge von Zahlen* t_s *verbunden. Eine nicht dichte Menge von Systemen heißt „dünn".*

Die Gesamtheit aller Systeme von je s Primzahlen bilden offenbar eine dichte Menge.

Nun sei also $F(x, y, \ldots, w; t_1, \ldots, t_s)$ ein in P irreduzibles Polynom von $x, \ldots, t_s$ mit ganzen Koeffizienten. Wir fassen zunächst t_s allein als Parameter auf. Dann ist die Menge der ganzen Zahlen t_s, für die F als Funktion von $x, \ldots, t_{s-1}$ reduzibel wird, dünn. Haben wir also irgendeine dichte Menge ganzer Zahlen t_s, so sind darunter gewiß solche, für die F in $x_1, \ldots, t_{s-1}$ irreduzibel wird. Wir denken uns unter diesen Zahlen t_s^0 herausgegriffen. Dann wird $F(x, \ldots, w; t_1, \ldots, t_{s-1}, t_s^0)$ nur für eine dünne Menge ganzer Zahlen t_{s-1} in P reduzibel. Das lehrt: Die Paare ganzer Zahlen t_{s-1}, t_s, für die F als Funktion von $t_1, \ldots, t_{s-2}$ in P reduzibel wird, bilden eine dünne Menge. Geht man so weiter, so erhält man schließlich: *Die Systeme ganzer Zahlen* $t_1, \ldots, t_s$, *für die die in* P *irreduzible Funktion* F *mit ganzzahligen Koeffizienten als Funktion von* $x, \ldots, w$ *in* P *reduzibel wird, sind dünn.*

Durch eine Verfeinerung der vorliegenden Methode kann man einen wesentlich schärferen Satz gewinnen. Bezeichnet man nämlich eine Menge positiver ganzer Zahlen $t_1, t_2, \ldots$ als dicht in bezug auf die ganze positive Zahl m und die positive Zahl α, wenn für unendliche viele Indizes ν gilt

$$t_{\nu+m} - t_\nu < t_\nu^\alpha,$$

und definiert mittels dieses Begriffes der „Dichte in bezug auf m, α" die Dichte in bezug auf m, α von Systemen von je s ganzen Zahlen genau ebenso wie wir es vorhin getan haben, so gilt: Zu jedem in P irreduziblen Polynom $F(x, y, \ldots, w; t_1, \ldots, t_s)$ mit ganzen Koeffizienten gibt es eine ganze positive Zahl m und eine positive Zahl α, so daß die Menge der Systeme ganzer Zahlen $t_1, \ldots, t_s$, für die F in P reduzibel wird, in bezug auf m, α nicht dicht sind.

Hier gehen wir darauf nicht näher ein. Außerdem möchte ich darauf hinweisen, daß man durch Übertragung des Hilfssatzes auf mehr Dimensionen allgemeinere Sätze gewinnen kann. Man kann zeigen, daß die ganzen Werte $t_1, \ldots, t_s$, für die Funktionen $F(x, y, \ldots, w; t_1, \ldots, t_s)$, die in x normierte Polynome und in $y, \ldots, w$ analytische Funktionen gewisser sehr allgemeiner Art sind, durch andere Funktionen von $x, y, \ldots, w$ derselben Art, aber nun mit ganzen Koeffizienten teilbar sind, sehr selten sind. Wenn sich dies als interessant genug erweist, behalte ich mir eine Veröffentlichung hierüber vor.

§ 5.

Eine Umformung des Satzes auf gebrochene rationale Systeme $t_1, \ldots, t_s$.

z sei eine feste ganze Zahl, $r_1, r_2, \ldots, r_s$ seien feste rationale Zahlen. $\tau_1, \tau_2, \ldots, \tau_s$ bedeuten die kleinsten ganzen positiven Zahlen, C eine ganze Zahl, so daß

$$F^*(x, y, \ldots, w;\, t_1, \ldots, t_s)$$
$$= C \cdot t_1^{\tau_1} \cdot t_2^{\tau_2} \cdot \ldots \cdot t_s^{\tau_s} F\left(x, y, \ldots, w;\; r_1 + \frac{z}{t_1}, r_2 + \frac{z}{t_2}, \ldots, r_s + \frac{z}{t_s}\right)$$

ein Polynom in $x, y, \ldots, w;\, t_1, \ldots, t_s$ wird mit ganzen Koeffizienten. Dann ist $F\left(x, y, \ldots, w;\; r_1 + \frac{z}{t_1}, \ldots, r_s + \frac{z}{t_s}\right)$ dann und nur dann für ein System ganzer Zahlen $t_1^0, t_2^0, \ldots, t_s^0$ als Polynom von $x, y, \ldots, w$ in P reduzibel, wenn dies für F^* zutrifft. Auf F^* aber können wir, weil F^* wiederum irreduzibel ist als Funktion von $x, y, \ldots, t_s$, unsern Satz anwenden und erhalten dadurch: *$F(x, y, \ldots, w;\, t_1, \ldots, t_s)$ sei ein Polynom von $x, y, \ldots, w;\, t_1, t_2, \ldots, t_s$ mit rationalen Koeffizienten und sei in P irreduzibel. z sei eine ganze rationale Zahl, $r_1, r_2, \ldots, r_s$ seien rationale Zahlen. Wir betrachten dann die Systeme ganzer rationaler Zahlen $t_1^0, t_2^0, \ldots, t_s^0$, für die $F\left(x, y, \ldots, w;\; r_1 + \frac{z}{t_1^0}, \ldots, r_s + \frac{z}{t_s^0}\right)$ in P als Polynom von $x, y, \ldots, w$ zerfällt. Die Menge dieser Systeme ist dünn.*

Hat man nun im Raume der Zahlen $t_1, t_2, \ldots, t_s$ einen beliebig kleinen s-dimensionalen Würfel, so enthält dieser einen rationalen Punkt $r_1, r_2, \ldots, r_s$ im Innern. Daraus folgt nach unserm Satze, daß *im Innern des Würfels auch solche rationalen Punkte liegen, für die F in P irreduzibel ist.* Man wähle nämlich R so klein, daß die s-dimensionale Kugel mit dem Radius R um $(r_1, \ldots, r_s)$ ganz im Würfel liegt. Dann gibt es nach unserm Satz ganze rationale Werte $t_1, t_2, \ldots, t_s$ von der Eigenschaft, daß $F\left(x, y, \ldots, w;\; r_1 + \frac{1}{t_1}, \ldots, r_s + \frac{1}{t_s}\right)$ als Funktion von $x, y, \ldots, w$ in P irreduzibel ist, und daß $|t_1| > \frac{1}{R}, \ldots, |t_s| > \frac{1}{R}$ wird, der Punkt $r_1 + \frac{1}{t_1}, \ldots, r_s + \frac{1}{t_s}$ also im Innern des Würfels liegt. Hieraus folgt z. B. nach bekanntem Verfahren[7]): In jedem beliebig kleinen Würfel des $n+1$ dimensionalen Raumes mit den Koordinaten $a_0, a_1, \ldots, a_n$ gibt es Gleichungen $a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0$ mit rationalen Koeffizienten, die ohne Affekt sind.

Ferner folgt beispielsweise aus unserm Satze eine Verschärfung des Satzes, den D. Hilbert am Schlusse seiner Arbeit ausspricht. Bei uns folgt

---

[7]) Siehe z. B. die Schlußweise in der Hilbertschen Arbeit, Crelles Journal **110**.

nämlich: Wenn eine algebraische Funktion von t für eine ganze rationale Zahl z, eine rationale Zahl r und für eine dichte Menge ganzer Zahlen t an den Stellen $r+\frac{z}{t}$ selbst rationale Werte annimmt, so ist sie notwendig eine rationale Funktion.

Die bisher abgeleiteten Resultate lassen sich natürlich auf algebraische Zahlkörper übertragen. Dies geschieht durch den folgenden leicht zu beweisenden Satz:

$F(x, y, \ldots, w;\, t_1, t_2, \ldots, t_s)$ sei ein in dem algebraischen Zahlkörper $P(\alpha)$ irreduzibles Polynom von $x, \ldots, t_s$ mit Koeffizienten aus $P(\alpha)$. $\alpha_1, \alpha_2, \ldots, \alpha_n$ seien eine Basis in $P(\alpha)$. Dann kann man F ein in P irreduzibles Polynom

$$F^*(x, y, \ldots, w;\, u_1^{(1)}, u_2^{(1)}, \ldots, u_n^{(1)}, u_1^{(2)}, u_2^{(2)}, \ldots, u_1^{(s)}, \ldots, u_n^{(s)})$$

von $x, y, \ldots, u_n^{(s)}$ mit ganzen rationalen Koeffizienten zuordnen, so daß das Folgende gilt: F ist als Funktion von $x, y, \ldots, w$ dann und nur dann für $t_1 = u_1^{(1)}\alpha_1 + \ldots + u_n^{(1)}\alpha_n, \ldots, t_s = u_1^{(s)}\alpha_1 + \ldots + u_n^{(s)}\alpha_n$ in $P(\alpha)$ reduzibel, wenn F^* für $u_1^{(1)}, u_1^{(2)}, \ldots, u_n^{(s)}$ als Funktion von $x, y, \ldots, w$ in P reduzibel ist.

Dabei hat F^* die folgende, hier sehr wichtige Eigenschaft: Wählt man in jeder Zeile des Schemas

$$\begin{array}{c} u_1^{(1)}, u_2^{(1)}, \ldots, u_n^{(1)}, \\ u_1^{(2)}, u_2^{(2)}, \ldots, u_n^{(2)}, \\ \cdots\cdots\cdots \\ u_1^{(s)}, u_2^{(s)}, \ldots, u_n^{(s)} \end{array}$$

eine Variable aus und gibt allen anderen Variablen beliebige rationale Werte, so bleibt F^* als Funktion von $x, y, \ldots, w$ und den ausgezeichneten Variablen in P irreduzibel.

§ 6.

Zu dem E. Noetherschen Kriterium für absolute Irreduzibilität.

Von jetzt an will ich unter einer Wurzel immer eine Potenz mit einem Exponenten der Form $\frac{1}{q}$ mit ganzem positivem q verstehen.

Wir beweisen den folgenden Hauptsatz dieses Paragraphen:

Satz. *$F(x, y, \ldots, w;\, t)$ sei ein Polynom in $x, y, \ldots, w$. Die Koeffizienten seien eindeutige analytische Funktionen von t, für welche t_0 entweder eine reguläre Stelle oder ein Pol sei. Dann kann man in der komplexen t-Ebene um den Punkt t_0 einen Kreis K beschreiben, so daß im Inneren von K mit etwaiger Ausnahme von t_0 selbst gilt: F zerfällt ent-*

weder für jeden Wert t als Funktion von $x, y, \ldots, w$ im Bereich aller Zahlen oder für keinen Wert.

Zum Beweise zeichnen wir zunächst die Variable x aus. Der Grad von F in x sei n. Der Koeffizient von x^n sei $h(y, \ldots, w;\, t)$. Wir betrachten die Funktion

$$F^* = (h(y, \ldots, w;\, t))^{n-1} F$$

und setzen $x' = h(y, \ldots, w;\, t) \cdot x$. Dann hat F^* in x' den höchsten Koeffizienten 1. Wir wählen K so klein, daß darin $h(y, \ldots, w;\, t)$ höchstens an der Stelle t_0 identisch verschwindet. Alle inneren Punkte von K, mit Ausnahme von t_0, wollen wir als die Punktmenge K^* bezeichnen. Dann zerfällt F in K^* dann und nur dann in zwei x enthaltende Faktoren, wenn F^* in K^* in zwei x' enthaltende Faktoren zerfällt.

Durch die Gleichung

$$F^*(x', y, \ldots, w;\, t) = 0$$

wird x' als algebraische Funktion von $y, \ldots, w;\, t$ definiert. Ist dann K von vornherein hinreichend klein gewählt, so ist es möglich, zu jedem t aus K^* eine Zahl $W(t)$, zu jedem Paar t, w, in dem $|w| > W(t)$ ist, eine Zahl $V, \ldots$, zu jedem System $z, \ldots, w;\, t$, das vorhergehenden Größenbedingungen genügt, eine Zahl $Y(z, \ldots, w;\, t)$ zu bestimmen, so daß das Folgende gilt: Für jedes System $y, \ldots, t$, für das t in K ist und $|w| > W$, $|v| > V, \ldots, |y| > Y$ ist, läßt sich jede Wurzel x'_ν in der Form darstellen

$$x'_\nu = a^{(\nu)}_{-k}\, y^{\frac{k}{q}} + a^{(\nu)}_{-(k-1)}\, y^{\frac{k-1}{q}} + \ldots + a^{(\nu)}_0 + a^{(\nu)}_1 \frac{1}{y^{\frac{1}{q}}} + \ldots .$$

Die Koeffizienten a sind wiederum nach oben abbrechende Laurentreihen in gewissen Wurzeln von $z, \ldots$. So kommt man endlich zu Koeffizienten, die nach oben abbrechende Laurentreihen von Wurzeln von w sind. Hierin sind die Koeffizienten nach unten abbrechende Laurentreihen von Wurzeln von $t - t_0$.[8]) Man denke sich aus den Wurzeln $x'_1, x'_2, \ldots, x'_n$ auf alle mög-

[8]) Ein Beispiel einer algebraischen Funktion von x und y, welche in keiner vollen Umgebung des Punktes $x = \infty$, $y = \infty$ konvergiert, erhält man so:

$$z = \sqrt{x^2 + y^2} = x\left(1 + \frac{y}{x}\right)^{\frac{1}{2}} = x + \binom{\frac{1}{2}}{1} x \cdot \left(\frac{y}{x}\right)^{-\frac{1}{2}} + \ldots$$

konvergiert nur für $y \leqq x$, also kann z nicht in einer vollen Umgebung von $x = 0$, $y = 0$ konvergieren, also kann die Funktion z, die durch die Gleichung $\frac{1}{z} = \sqrt{\frac{1}{x^2} + \frac{1}{y^2}}$ oder durch $xy = zx + zy$ definiert wird, nicht in einer vollen Umgebung von $x = \infty$, $y = \infty$ konvergieren.

lichen Arten ν ausgewählt, $0 < \nu < n$, etwa $x'_{\alpha_1}, x'_{\alpha_2}, \ldots, x'_{\alpha_\nu}$. Wie früher bilde man wieder die N Paare

$$f_\nu = (x' - x'_{\alpha_1}) \ldots (x' - x'_{\alpha_\nu}), \qquad f_\nu^* = (x' - x'_{\alpha_{\nu+1}}) \ldots (x' - x'_{\alpha_n}).$$

Die Koeffizienten dieser Polynome von x' sind wieder Reihenfunktionen von der Art, wie es die Wurzeln x'_ν waren. Dann zerfällt F^* für t_1 in K^* dann und nur dann in zwei x' enthaltende Faktoren, wenn für t_1 ein Paar f_ν, f_ν^* in ein Paar von Polynomen in $x', y, \ldots, w$ übergeht. Ist nun ein Paar f_ν, f_ν^* bei variablem t ein Paar von Polynomen, so ist F für jedes t aus K^* reduzibel. Ist aber kein Paar f_ν, f_ν^* ein Paar von Polynomen, so kann F nur für solche Werte t_1 reduzibel werden, für die gewisse [unendlich viele!] nicht identisch verschwindende nach unten abbrechende Laurentreihen in Wurzeln von $t_1 - t_0$ verschwinden[9]). Dies tritt nur für endlich viele Werte t_1 aus K^* ein. Ist also K klein genug, so tritt es für keinen Wert t_1 ein.

Für welche Werte t kann F so in zwei Faktoren zerfallen, daß dieselben keine Variable gemeinsam enthalten? Hier schließt man genau wie früher: Dies tritt entweder immer in K^* oder nur endlich oft ein, oder wenn K^* klein genug ist, entweder immer oder nie. Hieraus folgt unser Satz. Derselbe wird für den Punkt $t_0 = \infty$ genau ebenso bewiesen. Wir verzichten hierauf.

Hat man ein abgeschlossenes Gebiet der t-Ebene, so daß jeder Punkt in bezug auf die Koeffizienten von F entweder regulär oder ein Pol ist, so kann man nach Borel-Heine das Gebiet durch endlich viele Kreise K überdecken. Daraus folgt, daß alle Punkte des Gebiets gleichwertig sind, d. h. wenn in der Umgebung eines Punktes die Funktion reduzibel ist, so ist sie es in der Umgebung jedes Punktes und umgekehrt. Also ist F für dieses ganze Gebiet mit endlich vielen Ausnahmestellen entweder immer reduzibel oder immer irreduzibel.

Etwas genauer überlegt man sich leicht: Nimmt man zu den Punkten, in denen F reduzibel wird, noch eventuell einige solche hinzu, in denen der Grad von F sich erniedrigt, so erhält man eine abgeschlossene Menge. Hieraus folgt: Ist F fast immer reduzibel, so kann es höchstens an solchen Punkten irreduzibel sein, in denen sich der Grad erniedrigt [und, wie man auch fortfahren kann, das Leitglied in jeder Reihenfolge der Variablen herausfällt].

Sind die Koeffizienten Polynome in t, so ist die ganze Ebene ein für uns mögliches Gebiet einschließlich des Punktes ∞. F ist also dann

---

[9]) An dieser Stelle erhält Fräulein Noether statt meiner unendlich vielen Potenzreihen endlich viele Potenzreihen, die Koeffizienten der Reduzibilitätsform.

in der ganzen Ebene bis auf endlich viele Punkte entweder reduzibel oder irreduzibel.

Man kann diesen Satz natürlich sukzessive auf beliebig viele Parameterwerte $t_1, t_2, \ldots, t_s$ übertragen.

Zum Schluß möchte ich darauf hinweisen, daß man auch im Falle des Zerfallens von Polynomen im Körper aller reellen Zahlen ziemlich weitgehende Aussagen machen kann. Für Polynome $f(x, y, \ldots, w; t)$, deren Koeffizienten Polynome von t mit reellen Koeffizienten sind, habe ich z. B. den folgenden Satz erhalten: Man kann auf der Geraden der reellen t Werte gewisse Punkte $A < t_1 < t_2 < \ldots < t_m < B$ auszeichnen, so daß folgendes gilt: Links von A liegen entweder nur solche Punkte, für die f reduzibel ist, oder nur solche, für die f irreduzibel ist. Dasselbe gilt für die Strecke rechts von B. Für jede der Strecken $A - t_1, t_1 - t_2, \ldots, t_{m-1} - t_m, t_m - B$ gilt: Entweder sie besteht nur aus Punkten, für die f reduzibel ist bis auf höchstens die Nullstellen eines gewissen Polynoms in t, oder sie enthält nur endlich viele Punkte, für die f reduzibel ist. Ich werde dies auf beliebig viele Parameterwerte $t_1, \ldots, t_s$ übertragen. Daß im Körper der reellen Zahlen der Hilbertsche Irreduzibilitätssatz nicht gilt, ist klar, denn jedes Polynom einer Variablen ungeraden Grades $a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + t$ ist für jeden reellen Wert t reduzibel.

(Eingegangen am 26. 10. 1924.)