Notiz über einen Satz der Galoisschen Theorie.

Von

Alexander Ostrowski in Hamburg.

Durch den Hilbertschen Irreduzibilitätssatz wird nicht nur eine wesentliche und tiefliegende Eigenschaft irreduzibler Polynome in mehreren Variablen aufgedeckt, sondern es werden durch ihn mehrere wichtige Probleme aufgeworfen, deren Erforschung als eine der vornehmsten Aufgaben der modernen Algebra und Zahlentheorie gelten darf. Insbesondere gehört hierher das Problem, die Beziehung des Begriffes der absoluten Irreduzibilität zum gewöhnlichen Irreduzibilitätsbegriff aufzuklären, eine Beziehung, die bereits in den Hilbertschen Irreduzibilitätssatz hineinspielt, ohne jedoch, bei dem von Hilbert gewählten Beweisgang — und auch bei allen späteren Beweisen — klar zutage zu treten. Als einen Beitrag zur Untersuchung dieser Frage möchte ich nun im Folgenden einen Satz der Galoisschen Theorie beweisen, der bisher unbemerkt geblieben zu sein scheint, und in dem der wesentliche Unterschied zwischen der gewöhnlichen und der absoluten Irreduzibilität in helles Licht gerückt wird. Der Formulierung und dem Beweis dieses Satzes in § 2 schicke ich in § 1 einige allgemeinere Betrachtungen voraus über die Normierung von Koeffizienten bei Teilern von Polynomen mit Koeffizienten aus einem bestimmten Körper, die trotz ihres durchaus elementaren Charakters wohl jedesmal von Bedeutung sein können, wenn es sich um die Frage handelt, wie die Adjunktion von algebraischen Größen den Irreduzibilitätscharakter eines Polynoms beeinflußt.

§ 1.

Es sei $F(x_1, \ldots, x_n)$ ein Polynom in den Variablen $x_1, \ldots, x_n$, und es sei der kleinste seine Koeffizienten $\gamma_1, \gamma_2, \ldots$ enthaltende Körper durch R bezeichnet. Es zerfalle F in ein Produkt von zwei Polynomen $A(x_1, \ldots, x_n)$ und $B(x_1, \ldots, x_n)$ mit Koeffizienten $\alpha_1, \alpha_2, \ldots$ bzw. $\beta_1, \beta_2, \ldots$.

Diese Koeffizienten sind natürlich nur bis auf eine multiplikative Größe bestimmt, so daß wir allgemeiner auch

$$(1) \qquad t\alpha_1, t\alpha_2, \ldots \quad \text{bzw.} \quad \frac{1}{t}\beta_1, \frac{1}{t}\beta_2, \ldots$$

als Koeffizienten von A und B annehmen könnten. — Alle Zerlegungen, die man so für verschiedene t erhält, werden wir *ähnliche* Zerlegungen nennen. — Dagegen sind die Produkte $\alpha_i\beta_k$ von t unabhängig. Es sei der kleinste alle α_i enthaltende Körper durch A, der kleinste alle β_k enthaltende Körper durch B, der kleinste alle Produkte $\alpha_i\beta_k$ enthaltende Körper durch T bezeichnet. Den kleinsten, beide Körper R und A enthaltenden Körper, der ja nicht mit A übereinzustimmen braucht, bezeichnen wir durch A′, den entsprechenden kleinsten Körper, der R und B enthält, durch B′. Dann ist B ein Teiler von A′, da B aus F und A durch rationale Operationen hervorgeht. Daher ist B′ ein Teiler von A′, A′ ein Teiler von B′, also $\mathsf{A}' = \mathsf{B}'$. Da in $\mathsf{A}' = \mathsf{B}'$ alle Produkte $\alpha_i\beta_k$ liegen, ist T ein Teiler von A′. Andererseits sind alle Koeffizienten von F in T enthalten, also ist R ein Teiler von T, so daß A′ = B′ auch definiert werden kann als der kleinste Körper, in dem A und B liegen, also als der kleinste Körper, in dem die Zerlegung $F = AB$ gilt. Andererseits gibt es bereits in T eine ähnliche Zerlegung. Denn wählen wir in (1) für t etwa einen nicht verschwindenden Koeffizienten β_1 von B. so werden die Größen (1) zu

$$\beta_1\alpha_1, \beta_1\alpha_2, \ldots \quad \text{und} \quad \frac{\beta_1}{\beta_1} = 1, \ \frac{\beta_2}{\beta_1} = \frac{\beta_2\alpha_1}{\beta_1\alpha_1}, \ \frac{\beta_3}{\beta_1} = \frac{\beta_3\alpha_1}{\beta_1\alpha_1}, \ \ldots,$$

wenn $\alpha_1 \neq 0$ ist, d. h. Größen von T. T ist also der kleinste Körper, in dem eine ähnliche Zerlegung stattfindet. *Wir sehen außerdem, daß alle Koeffizienten von A und B gewiß in T liegen, d. h. die Zerlegung im kleinstmöglichen Körper stattfindet, wenn einer von diesen Koeffizienten gleich* 1 *ist.* (Es genügt aber allgemeiner, daß wenigstens einer der Koeffizienten von A oder B in R oder noch allgemeiner in T liegt.)

Dieser Körper T kann sich indessen noch ändern, wenn wir F mit irgendeiner Größe t multiplizieren, also die Koeffizienten von F durch

$$t\gamma_1, t\gamma_2, \ldots$$

ersetzen, da sich dann auch alle Produkte $\alpha_i\beta_k$ mit t multiplizieren. Die Quotienten $\frac{\alpha_i\beta_k}{\alpha_{i'}\beta_{k'}}$ sind jedoch von t unabhängig, und der kleinste sie enthaltende Körper T' ist daher in allen, verschiedenen t entsprechenden Körpern T enthalten. Es läßt sich aber t so wählen, daß der entsprechende Körper T mit T' zusammenfällt. Denn wenigstens ein Koeffizient von F, etwa γ_1, ist gleich dem Produkt eines Koeffizienten von A und eines

von B, etwa $\alpha_1 \beta_1$. Wählen wir also für t einfach $\frac{1}{\gamma_1}$, so multiplizieren sich alle $\alpha_i \beta_k$ mit $\frac{1}{\alpha_1 \beta_1}$, und T geht in T' über. Die Koeffizienten $\gamma_1, \gamma_2, \ldots$ von F werden aber zu

$$1, \frac{\gamma_2}{\gamma_1}, \frac{\gamma_3}{\gamma_1}, \ldots,$$

der Körper R zu dem kleinsten Körper $\overline{R}$, der alle Verhältnisse $\frac{\gamma_i}{\gamma_k}$ enthält. Machen wir einen anderen Koeffizienten von F zu 1, so multiplizieren sich alle $\alpha_i \beta_k$ mit einem Quotienten $\frac{\gamma_l}{\gamma_1}$, der zu R, also auch zu T' gehört, und der Körper T bleibt unverändert.

Wir erreichen also gewiß, daß der Körper T der kleinstmögliche wird, wenn wir einen der Koeffizienten von F gleich 1 *machen.*

Wir wollen daher von nun an annehmen, daß bei allen Polynomen, die wir betrachten, die Koeffizienten gewisser Glieder gleich 1 sind, nämlich die Koeffizienten des höchsten Gliedes bei irgendeiner willkürlichen aber festen Anordnung der Variablen. Offenbar ist das Produkt von zwei so normierten Polynomen ebenfalls normiert.

§ 2.

Es sei nun R irgend ein algebraischer Zahlkörper. Ist F ein von den Unbestimmten $u, u_1, \ldots, u_m$ abhängiges Polynom mit algebraischen Koeffizienten, und zerfällt F in ein Produkt von zwei Polynomen in $u, u_1, \ldots, u_m$ mit *beliebigen* Zahlenkoeffizienten, so müssen bekanntlich diese Koeffizienten *algebraische* Zahlen sein. Denn führen wir die Kroneckersche Substitution $u = x$, $u_1 = x^g$, $u_2 = x^{g^2}$, $\ldots$, $u_m = x^{g^m}$ mit hinreichend großem g aus, so geht jeder Faktor von F in ein Polynom in x mit denselben Koeffizienten über, die Koeffizienten eines Faktors eines Polynoms in x mit algebraischen Koeffizienten sind aber, wenn einer unter ihnen gleich 1 ist, ebenfalls algebraische Zahlen. Ist also F nicht in zwei Faktoren mit algebraischen Zahlenkoeffizienten zerlegbar, so ist F überhaupt unzerlegbar, auch wenn man alle Zahlen als Koeffizienten zuläßt.

Man nennt nun ein Polynom in $u, u_1, \ldots, u_m$ mit algebraischen Zahlenkoeffizienten bekanntlich absolut irreduzibel, wenn es sich nicht als Produkt von zwei Polynomen in $u, u_1, \ldots, u_m$ mit algebraischen Zahlenkoeffizienten darstellen läßt. — Der Begriff der absoluten Irreduzibilität dürfte von Kronecker herrühren. —

Es sei nun $F(u; u_1, \ldots, u_m)$ ein in R irreduzibles Polynom mit Zahlenkoeffizienten aus R vom Grade n in bezug auf u. Es sei dann eine Wurzel der Gleichung $F(u; u_1, \ldots, u_m) = 0$, wenn u als Unbekannte

betrachtet wird. Ist F selbst noch nicht absolut irreduzibel, so enthält es sicher ein absolut irreduzibles Polynom $\varphi(u; u_1, \ldots, u_m)$ als Faktor, dessen Wurzel — in bezug auf u — ζ ist. Wir bezeichnen den aus allen algebraischen *Zahlen*, die im Körper $R(\zeta; u_1, \ldots, u_m)$ vorkommen, gebildeten Körper durch K_1. Es gilt nun das

Theorem. *Im Körper $K_1(u_1, \ldots, u_m)$ sondert sich von $F(u; u_1, \ldots, u_m)$ jedenfalls derjenige absolut irreduzible Faktor $\varphi(u; u_1, \ldots, u_m)$ ab, dessen Wurzel ζ ist, und jeder Zahlkörper, in dem sich von $F(u; u_1, \ldots, u_m)$ der Faktor φ absondert, enthält K_1 als Unterkörper. Mit anderen Worten: Der durch die algebraischen Zahlenirrationalitäten, die in den Koeffizienten von $\varphi(u)$ vorkommen, bestimmte Zahlkörper K_2 ist mit dem Zahlkörper K_1 identisch, der durch alle im Körper $R(\zeta; u_1, \ldots, u_m)$ enthaltenen Zahlenirrationalitäten bestimmt wird*[1]).

Der Satz läßt sich auf mehrere Arten beweisen, wohl am einfachsten wie folgt:

Bildet man die Norm $N(\varphi)$ von φ in K_2, so besteht sie aus lauter voneinander verschiedenen Faktoren, die sich auch nicht bloß durch multiplikative Konstanten voneinander unterscheiden, da in ihnen die Koeffizienten bei einem gewissen Glied gleich 1 sind. F muß daher durch $N(\varphi)$ teilbar sein, da F durch φ teilbar ist. Da aber $N(\varphi)$ Koeffizienten aus R hat, und F irreduzibel in R ist, müssen die Polynome F und $N(\varphi)$ miteinander identisch sein, weil in ihnen die Koeffizienten bei einem gewissen Glied gleich sind, nämlich gleich 1. Wir erhalten die Gleichung:

$$F(u; u_1, \ldots, u_m) = N(\varphi(u; u_1, \ldots, u_m)). \tag{2}$$

Es seien nun die Grade von F und φ in bezug auf u durch n und n' bezeichnet. Dann genügt ein primitives Element ϱ von K_2 einer in R irreduziblen Gleichung $\omega(z) = 0$ vom Grade $\bar{n} = \frac{n}{n'}$, wie aus (2) durch Vergleichung der Grade in bezug auf u folgt. Die Gleichung $F(u) = 0$ ist also eine sogenannte *imprimitive* Gleichung im Körper $\Omega = R(u_1, \ldots, u_m)$. Daher ergibt sich unsere Behauptung aus dem folgenden Hilfssatz: *Ist eine Gleichung $F(u) = 0$ vom Grade n in bezug auf einen Körper Ω imprimitiv, und genügt etwa eine Wurzel ζ von F einer im Körper $\Omega(\varrho)$ irreduziblen Gleichung $\varphi(u, \varrho) = 0$ vom Grade n', wo ϱ eine Wurzel der in Ω irreduziblen Gleichung $\omega(z) = 0$ vom Grade $\bar{n}$ und $n'\bar{n} = n$ ist, so liegt ϱ im Körper $\Omega(\zeta)$.* In der Tat gilt unter den Voraussetzungen des Hilfssatzes die Gleichung:

$$F(u) = N(\varphi(u, \varrho)) = \varphi(u, \varrho)\varphi(u, \varrho') \ldots \varphi(u, \varrho^{(\bar{n}-1)})$$

[1]) Ich habe diesen Satz bereits in meiner Mitteilung: „Zur arithmetischen Theorie der algebraischen Größen", Gött. Nachr. 1919, ausgesprochen, jedoch für den Beweis auf eine spätere Abhandlung verwiesen.

wo $\varrho', \varrho'', \ldots$ die zu ϱ konjugierten Größen sind. Die mit $\varphi(u, \varrho)$ konjugierten Polynome $\varphi(u, \varrho')$, $\varphi(u, \varrho'')$, ... usw. können dann nur für von ζ verschiedene Wurzeln von F verschwinden, so daß der Gleichung $\varphi(\zeta, z) = 0$ nur eine einzige von den Wurzeln von $\omega(z) = 0$ genügt, nämlich ϱ. Daher läßt sich ϱ aus den Gleichungen $\varphi(\zeta, z) = 0$ und $\omega(z) = 0$ als deren einzige gemeinsame Wurzel mit Hilfe des Euklidischen Algorithmus rational durch ζ ausdrücken, wenn man, was ja stets möglich ist, $\varphi(u, \varrho)$ als ein Polynom in ϱ dargestellt hat.

Der hiermit bewiesene Satz läßt sich offenbar insofern etwas allgemeiner fassen, als der Körper R nicht als Zahlkörper angenommen zu werden braucht. Er kann auch algebraische Funktionen von Unbestimmten enthalten, von denen natürlich die Unbestimmten u_i unabhängig sein müssen. Man kann für R allgemeiner jeden abstrakten Körper mit der Charakteristik 0 (nach der Steinitzschen Terminologie) setzen.

Unser Satz hat eine gewisse Ähnlichkeit mit einem bekannten Satze von Kronecker, nach welchem jede Reduktion der Galoisschen Gruppe einer Gleichung, die durch Adjunktion einer algebraischen Irrationalität bewirkt wird, bereits durch Adjunktion einer natürlichen Irrationalität zu bewirken ist, die im zur Gleichung zugehörigen Galoisschen Bereich liegt. Der Unterschied besteht darin, daß in unserem Falle die zur Abspaltung eines absolut irreduziblen Faktors notwendige Irrationalität sich nicht nur durch *alle* Wurzeln der Gleichung rational ausdrücken läßt, sondern bereits durch *eine* Wurzel des abzuspaltenden Faktors.

In unserem Satze ist insbesondere ein bekannter und oft benutzter Satz enthalten: Es seien $\alpha_1, \alpha_2, \ldots, \alpha_k$ algebraische Irrationalitäten in bezug auf einen Körper R. Man fasse sie mit Hilfe verschiedener Potenzprodukte $U_1, \ldots, U_k$ neuer Unbestimmter $u_1, \ldots, u_m$ zu einem Ausdruck $U = \sum_1^k \alpha_i U_i$ zusammen. Dann läßt sich jede Irrationalität α_i rational mit Koeffizienten aus R durch $U, u_1, \ldots, u_m$ ausdrücken.

Denn genügt U in bezug auf $R(u_1, \ldots, u_m)$ einer Gleichung ν-ten Grades

$$F(U; u_1, \ldots, u_m) = 0,$$

so ist zur Abspaltung des absolut irreduziblen Bestandteiles $U - \sum_1^k \alpha_i U_i$, da der Koeffizient von U gleich 1 ist, die Adjunktion sämtlicher α_i notwendig.

Bei dem Beweis unseres Satzes hat sich ergeben, daß der Grad $\overline{n}$ des Körpers K_2 ein Teiler des Grades n von F in bezug auf u ist. Da aber K_2 durch die Koeffizienten von φ eindeutig bestimmt ist, kann für u jede im Polynom F vorkommende Variable genommen werden, und wir erhalten die Sätze:

1. *Der Grad n des kleinsten zur Abspaltung eines absolut irreduziblen Faktors eines in bezug auf R irreduziblen Polynoms F ausreichenden Zahlkörpers ist ein gemeinsamer Teiler der Grade von F in bezug auf die in F vorkommenden Variablen.*

2. *Ein in R irreduzibles Polynom ist zugleich auch absolut irreduzibel, wenn der größte gemeinsame Teiler der Grade von F in bezug auf die in F vorkommenden Variablen gleich* 1 *ist.*

Diese Sätze sind aber nur spezielle Folgerungen aus einem wesentlich allgemeineren Satze, den ich in einem anderen Zusammenhange veröffentlichen werde.

Hamburg, Mathematisches Seminar der Universität.

(Eingegangen am 8. Oktober 1921.)