Zur Theorie der algebraischen Zahlkörper.

Von

Michael Bauer in Budapest.

1. Es seien K_1, K_2 zwei algebraische Zahlkörper, welche durch je eine Wurzel der rationalen ganzzahligen irreduziblen Gleichungen

$$f_1(x) = 0, \quad \text{bzw.} \quad f_2(x) = 0$$

gegeben sind; die zugehörigen Galoisschen Körper sollen durch G_1, G_2 bezeichnet werden. Die Menge der rationalen Primzahlen p, für welche die linke Seite der Kongruenz

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

in lineare Faktoren zerfällt, soll die Menge A, die Menge der rationalen Primzahlen p, für welche die Kongruenz (1) mindestens eine rationale ganze Wurzel besitzt, soll die Menge B genannt werden. Es ist bekannt, daß die Menge A — mit einer endlichen Anzahl von Ausnahmen — mit der Menge derjenigen rationalen Primzahlen p zusammenfällt, welche im Körper K, der durch eine Wurzel der irreduktiblen Gleichung

$$f(x) = 0$$

bestimmt wird, als ein Produkt verschiedener Primideale ersten Grades darstellbar sind; während die Menge B — mit einer endlichen Anzahl von Ausnahmen — mit der Menge der rationalen Primzahlen p identisch ist, welche in K mindestens einen Primidealfaktor ersten Grades besitzen.

In früheren Noten*) habe ich den folgenden Satz bewiesen.

I. Der Körper G_1 enthält dann und nur dann den Körper G_2, wenn die Menge A_1 — mit einer endlichen Anzahl von Ausnahmen — eine Teilmenge von A_2 ist. Der Beweis stützt sich einerseits auf Untersuchungen von Kronecker und Frobenius, welche von der Klassenanzahlformel aus-

*) Archiv der Math. und Physik Bd. 6, S. 212—222, Über einen Satz von Kronecker usw.

gehen*), andererseits auf die Dedekindsche**) Regel, nach welcher eine rationale Primzahl p in einem Körper zerfällt, der Unterkörper eines Galoissche Bereiches ist. In den folgenden Untersuchungen werden wir mit denselben Hilfsmitteln den Satz beweisen.

I*. *Der Körper K_1 enthält dann und nur dann den Körper G_2, wenn die Menge B_1 — mit einer endlichen Anzahl von Ausnahmen — eine Teilmenge von A_2 bildet.*

Der Beweis wird zeigen, daß man I. als eine Anwendung von I*. bekommt.

2. Es soll die rationale Primzahl p die Diskriminante des Galoisschen Körpers G nicht teilen, infolgedessen ist

$$p = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_e,$$

wo $\mathfrak{P}_i$ verschiedene Primideale f^{ten} Grades sind. Zu jedem Faktor $\mathfrak{P}_i$ gehört eine Untergruppe $\mathfrak{H}_i$ der Gruppe $\mathfrak{G}$ des Körpers, deren Elemente $\mathfrak{P}_i$ invariant lassen (Zerlegungsgruppe nach Hilbert). Die Gruppen $\mathfrak{H}_i$ sind zyklische Gruppen, welche zueinander in bezug auf $\mathfrak{G}$ konjugiert sind. Umgekehrt gehören zu jeder zyklischen Untergruppe f^{ter} Ordnung $\mathfrak{H}$ von $\mathfrak{G}$ unendlich viele rationale Primzahlen p (deren „Dichtigkeit“ nach Frobenius $\neq 0$ ist), welche einen Primfaktor $\mathfrak{P}$ f^{ten} Grades besitzen, dessen Zerlegungsgruppe die Gruppe $\mathfrak{H}$ bildet. Wenn der Körper K als Unterkörper von G zur Untergruppe $\mathfrak{K}$ gehört, wenn ferner die Zerlegungsgruppe eines bestimmten (jedoch beliebigen) Faktors $\mathfrak{P}$ durch $\mathfrak{H}$ bezeichnet wird, so bekommt man nach der Dedekindschen Regel die Zerfällung von p im Körper K auf folgende Weise.

Man bilde die symbolische Gruppenzerlegung:

$$\mathfrak{G} = \mathfrak{H} R_1 \mathfrak{K} + \mathfrak{H} R_2 \mathfrak{K} + \cdots$$

wo $R_1, R_2, \cdots$ die inkongruenten Repräsentanten (mod. $\mathfrak{H}$, $\mathfrak{K}$) sind. Ist nun die Ordnung des größten Teilers von

$$\mathfrak{H},\ R_i \mathfrak{K} R_i^{-1}$$

gleich d_i, dann ist im Körper K

$$p = \Pi y_i \tag{2}$$

*) Über die Irreduktibilität von Gleichungen. Berliner Monatsberichte 1880, S. 148. Über Beziehungen zwischen den Primidealen usw. Berliner Sitzungsberichte 1896, S 689

**) Zur Theorie der Ideale. Gött. Nachr. 1894, S. 272. Wir werden nur einen Teil der Regel anwenden, der sich auf solche Primzahlen bezieht, die in der Diskriminante nicht auftreten. Infolgedessen kommen hier die wichtigen Untersuchungen von Hilbert über Verzweigungskörper usw. nicht in Betracht.

wo y_i verschiedene Primideale sind, deren Ordnungen gleich

$$f_i = \frac{f}{d_i}$$

ausfallen. Aus dieser Regel ersieht man, daß im Körper K — mit einer endlichen Anzahl von Ausnahmen — 1) die Menge A aus denjenigen rationalen Primzahlen p besteht, welche in G einen Primzahlfaktor besitzen, dessen Zerlegungsgruppe $\mathfrak{H}$ ein Teiler der sämtlichen Gruppen

(3) $$G\mathfrak{R}G^{-1}$$

ist, wo G ein beliebiges Element von $\mathfrak{G}$ bedeutet, 2) die Menge B wird aber aus denjenigen rationalen Primzahlen p bestehen, für welche die eben definierte Gruppe $\mathfrak{H}$ als Teiler von mindestens einer der Gruppen (3) auftritt. Es ist noch ferner ersichtlich, daß — ohne jede Ausnahme — eine Primzahl p dann und nur dann im Körper K als ein Produkt verschiedener Primideale darstellbar ist, wenn sie dieselbe Eigenschaft im zugehörigen Galoisschen Körper besitzt. Dies folgt daraus, daß einerseits der Galoissche Körper zur Untergruppe gehört, welche den größten Teiler sämtlicher Gruppen

$$G\mathfrak{R}G^{-1}$$

bildet und infolgedessen eine invariante Untergruppe ist, andererseits ist die Diskriminante von G nur durch die Primfaktoren der Diskriminante von K teilbar. Aus dieser Bemerkung geht aber hervor, daß der Satz I. wirklich eine Anwendung von Satz I*. bildet.

3. Nun sei G ein Galoisscher Körper, welcher K_1, K_2, G_1, G_2 enthält. Die Körper K_1, K_2 sollen zu den Untergruppen $\mathfrak{R}_1$, $\mathfrak{R}_2$ gehören, G_2 gehört zur invarianten Untergruppe J_2, welche der größte gemeinsame Teiler von den Gruppen

$$G\mathfrak{R}_2G^{-1}$$

ist. Nach der Galoisschen Theorie suchen wir die notwendigen und hinreichenden Bedingungen dafür, daß die Gruppe $\mathfrak{R}_1$ eine Untergruppe von J_2 sein soll. Da J_2 eine invariante Untergruppe ist, so muß sie nicht nur $\mathfrak{R}_1$, sondern sämtliche Untergruppen

(4) $$G\mathfrak{R}_1G^{-1}$$

enthalten. Wenn daher $\mathfrak{H}$ eine zyklische Untergruppe ist, welche in irgendwelcher der Gruppen (4) auftritt, so muß sie ein Teiler von J_2 sein, was wir nach dem Punkte 2) in folgender Weise aussprechen können, die Menge B_1 muß — mit einer endlichen Anzahl von Ausnahmen — eine Teilmenge von A_2 bilden.

Sei umgekehrt diese Bedingung erfüllt und es sei p eine Primzahl, welche einen Primidealfaktor $\mathfrak{P}$ besitzt, dessen Zerlegungsgruppe $\mathfrak{H}$ eine beliebig gegebene zyklische Untergruppe von $\mathfrak{R}_1$ ist. Die Primzahl p gehört

zur Menge B_1, folglich zur Menge A_2, und so muß die Gruppe $\mathfrak{H}$ in der Tat ein Teiler von J sein, die Gruppe $\mathfrak{K}_1$ ist ein Teiler von J, q. e. d.

4. Eine Anwendung des Vorigen bildet z. B. der folgende Satz:

Es sei

$$f(x) = c_0 x^m + \cdots + c_m = 0$$
$$(c_i \text{ rat. ganz})$$

eine Gleichung, die nicht notwendig irreduzibel ist. Es sei K der durch eine beliebige Wurzel der Gleichung bestimmte Körper. Der Körper K enthält dann und nur dann die n^{ten} primitiven Einheitswurzeln, wenn die Menge der rationalen Primzahlen p, für welche die Kongruenz

$$f(x) \equiv 0 \pmod{p}$$

mindestens eine rationale ganze Wurzel besitzt — mit einer endlichen Anzahl von Ausnahmen — die Gestalt $nt + 1$ aufweist.

Für andere Anwendungen und Bemerkungen vergleiche die zitierten Noten; ich hebe nur hervor, daß der dort für zusammengesetzte Körper bewiesene Satz ohne jede Ausnahme gültig ist, weil eine Primzahl dann und nur dann Teiler von der Diskriminante des aus K_1, K_2 gebildeten Körpers ist, wenn sie entweder in der Diskriminante von K_1 oder von K_2 als Teiler auftritt.*) Der Satz ist der folgende.

Im zusammengesetzten Körper von K_1 und K_2 ist eine Primzahl dann und nur dann als ein Produkt von verschiedenen Primidealen ersten Grades darstellbar, wenn sie dieselbe Eigenschaft sowohl in bezug auf K_1, wie in bezug auf K_2 besitzt.

*) Diese bekannte Tatsache ergibt sich aus der allgemeinen Dedekindschen Reihe.