Séminaire Delange-Pisot-Poitou.
Théorie des nombres

JÜRGEN NEUKIRCH

Über die absolute Galoisgruppe algebraischer Zahlkörper

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, n° 2 (1971-1972), exp. n° 18, p. 1-19

<http://www.numdam.org/item?id=SDPP_1971-1972__13_2_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
13e année, 1971/72, n° 18, 19 p.

20 mars 1972

ÜBER DIE ABSOLUTE GALOISGRUPPE ALGEBRAISCHER ZAHLKÖRPER

von Jürgen NEUKIRCH [Regensburg]

Man kann in der Theorie der algebraischen Zahlkörper von zwei fundamentalen Fragestellungen sprechen, über die in diesem Aufsatz ein kurzer Bericht gegeben werden soll. Das erste dieser probleme besteht darin, eine Übersicht über die Erweiterungen eines fest zu Grunde gelegten Zahlkörpers k zu gewinnen (wichtigster Fall $k = \mathbb{Q}$) ; zu erforschen, wie sich diese Erweiterungen übereinander aufbauen, in welchen Beziehungen sie zueinander stehen und wie sie sich klassifizieren lassen. Mit diesem Problemkreis eng verknüpft ist die zweite der gemeinten fundamentalen Fragestellungen, nämlich die nach den arithmetischen Gesetzmässigkeiten der Erweiterungen K über k, und hierbei ist insbesondere die Frage nach dem Zerlegungsgesetz der Primideale $\mathfrak{p}$ von k im Oberkörper K von grundlegender Bedeutung. Beide Fragestellungen lassen sich wie folgt in einer einfachen gruppentheoretischen Weise formulieren.

Sei $\mathfrak{G} = G_k$ die absolute Galoisgruppe über dem Körper k, d. h. die topologische Galoisgruppe ([1]) der algebraisch abgeschlossenen Hülle $\overline{k}$ über k, und seien entsprechend $\mathfrak{G}_\mathfrak{p} = G_{k_\mathfrak{p}}$ die absoluten Galoisgruppen über den $\mathfrak{p}$-adischen Komplettierungen $k_\mathfrak{p}$ von k, wobei $\mathfrak{p}$ die einzelnen Primstellen des Körpers k durchläuft. Bettet man den algebraischen Abschluss $\overline{k}$ von k in den algebraischen Abschluss $\overline{k}_\mathfrak{p}$ von $k_\mathfrak{p}$ ein, so erhält man durch die Einschränkung der $k_\mathfrak{p}$-Automorphismen von $\overline{k}_\mathfrak{p}$ auf $\overline{k}$ eine Einbettung von $\mathfrak{G}_\mathfrak{p}$ in $\mathfrak{G}$, die bis auf Konjugiertheit kanonisch ist. $\mathfrak{G}_\mathfrak{p}$ tritt dann als die Zerlegungsgruppe (= Standgruppe) einer Fortsetzung $\overline{\mathfrak{p}}$ von $\mathfrak{p}$ auf $\overline{k}$ auf. Die algebraischen Erweiterungen K von k entsprechen nun umkehrbar eindeutig den abgeschlossenen Untergruppen $\mathfrak{H}$ von $\mathfrak{G}$. Ist $\mathfrak{H}$ normal in $\mathfrak{G}$, so ist $\mathfrak{G}/\mathfrak{H}$ die Galoisgruppe der galoisschen Erweiterung $K|k$, und das Bild der Gruppe $\mathfrak{G}_\mathfrak{p}$ in $\mathfrak{G}/\mathfrak{H}$ wird eine zur Primstelle $\mathfrak{p}$ gehörige Zerlegungsgruppe von $K|k$. Da das Zerlegungsgesetz der Primstellen $\mathfrak{p}$ in K durch diese Zerlegungsgruppen bestimmt wird, ergeben sich somit die

Erste fundamentale Frage : Wie sieht die Struktur der pro-endlichen Gruppe $\mathfrak{G}$ aus ?

([1]) $\mathfrak{G}$ ist als projektiver Limes der Galoisgruppen aller endlichen galoisschen Erweiterungen $K|k$ eine pro-endliche, d. h. kompakte, total diskontinuierliche topologische Gruppe. Homomorphismen solcher Gruppen sind durchweg als stetig, Untergruppen stets als abgeschlossen vorausgesetzt, und es sind Begriffe wie "frei", "Erzeugende", "Relationen" immer im topologischen Sinne zu verstehen.

Zweite fundamentale Frage : Wie lässt sich die Lage der Untergruppen $\mathfrak{G}_p$ in der Gruppe $\mathfrak{G}$ beschreiben ?

Von einer erschöpfenden Antwort auf diese beiden Fragen ist man, wie es heute scheint, noch durch Welten von kaum zu erahnender Weite getrennt. Es ist jedoch klar, dass das ganze Geheimnis in den inneren Gesetzmässigkeiten des Grundkörpers k verborgen liegt, so dass es auch das letzte Ziel sein muss, die Struktur von $\mathfrak{G}$ und die Lage der $\mathfrak{G}_p$ in $\mathfrak{G}$ in einer kanonischen Weise durch Invarianten des Körpers k aufzuklären. Die Struktur der lokalen Galoisgruppen $\mathfrak{G}_p$ wurde erst in jüngster Zeit von Jakovlev durch Erzeugende und (recht komplizierte) Relationen aufgedeckt (vgl. JAKOVLEV [23]).

Eine vollständige Antwort auf beide Fragen liegt uns vor, wenn wir uns auf die Betrachtung der abelschen Erweiterungen beschränken. Dies ist der Inhalt der Klassenkörpertheorie. Das Resultat ist einfach zu beschreiben. Sei

$$\mathfrak{G}^{ab} = G(k^{ab}|k) \text{ , bzw. } \mathfrak{G}_p^{ab} = G(k_p^{ab}|k_p)$$

die Galoisgruppe der maximalen abelschen Erweiterung von k , bzw. k_p . $\mathfrak{G}^{ab}$, bzw. $\mathfrak{G}_p^{ab}$, ist offenbar die Faktorkommutatorgruppe von $\mathfrak{G}$, bzw. $\mathfrak{G}_p$. Bezeichnet nun $\overline{C}_k$ die Idealklassengruppe von k mod ihrer Zusammenhangskomponente und k_p^* die multiplikative Gruppe des Körpers k_p , so lässt sich der Hauptsatz der Klassenkörpertheorie durch ein kommutatives Diagramm

$$\begin{array}{ccc} \overline{C}_k & \xrightarrow{(\ ,k)} & \mathfrak{G}^{ab} \\ \uparrow & & \uparrow \\ k_p^* & \xrightarrow{(\ ,k_p)} & \mathfrak{G}_p^{ab} \end{array}$$

ausdrücken, wobei $(\ ,k)$, bzw. $(\ ,k_p)$, das sogenannte Normrestsymbol bedeutet. Die Struktur der Galoisgruppe $\mathfrak{G}^{ab}$ wird also in einer kanonischen Weise durch die dem Grundkörper k direkt zugeordnete Idealklassengruppe $\overline{C}_k$ beschrieben, während die Einbettung der Zerlegungsgruppen $\mathfrak{G}_p^{ab}$ in $\mathfrak{G}^{ab}$ der Einbettung von k_p^* in $\overline{C}_k$ entspricht. Es darf nicht darüber hinweggesehen werden, dass dies so einfach zu formulierende Ergebnis eine tiefliegende Gesetzmässigkeit der abelschen Zahlkörper widerspiegelt, die sich schon in den Gaussschen und Kummerschen Entdeckungen andeutete und erst im Artinschen Reziprozitätsgesetz ihre vollendete, glanzvolle Darstellung fand. In ihm haben sich viele klassische Sätze kristallisiert, von denen wir hier nur den berühmten Kronecker-Weberschen Satz erwähnen wollen :

SATZ. - Die Erweiterung $\underset{\sim}{Q}^{ab}|\underset{\sim}{Q}$ wird durch alle Einheitswurzeln erzeugt, und es ist

$$\mathfrak{G}^{ab} = G(\underset{\sim}{Q}^{ab}|\underset{\sim}{Q}) \cong \hat{\underset{\sim}{Z}}^*$$

wobei $\hat{\mathbb{Z}}^*$ die Einheitengruppe des Ringes $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n$ ist.

Im allgemeinen kann man die Galoisgruppe $\mathfrak{G}^{ab}$ keineswegs in solch expliziter Weise niederschreiben. Jedoch ist dieses Problem auf eine Untersuchung der dem Grundkörper k zugeordneten Gruppe $\overline{C}_k$ zurückgeführt. Und selbst, wenn sich die Struktur von $\mathfrak{G}^{ab}$ wegen ungenügender Kenntnis der Idealklassengruppe nicht vollends ergibt, so kann man dennoch zu interessanten, allgemeingültigen Resultaten gelangen. Um dies zu erläutern, sei einmal kurz auf die von K. IWASAWA entwickelte Theorie der Γ-Erweiterungen eingegangen (vgl. IWASAWA [19], [20], [21]).

Unter einer Γ-Erweiterung versteht man eine unendliche galoissche Erweiterung von k, die eine zur Gruppe $\mathbb{Z}_p$ der ganzen p-adischen Zahlen isomorphe Galoisgruppe besitzt, d. h. die sich aus einer Kette zyklischer Erweiterungen vom Grade p^n, $n = 1, 2, 3, \ldots$, aufbaut. Durch die Untersuchungen von Iwasawa erhielten die Γ-Erweiterungen eine bemerkenswerte, die Klassenzahl der Kreiskörper betreffende Bedeutung. Ist nämlich p eine ungerade Primzahl und ζ_{p^n} eine primitive p^n-te Einheitswurzel, so bilden die Körper $k_n = \mathbb{Q}(\zeta_{p^n})$ eine Kette

$$\mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq k_3 \subseteq \ldots \subseteq K = \bigcup_{n=1}^{\infty} k_n ,$$

und es wird $K|k_1$ eine Γ-Erweiterung. Ordnet man nun jedem Körper k_n den p-primären Teil A_n seiner Idealklassengruppe zu und bildet hinsichtlich der Norm den projektiven Limes $A = \varprojlim A_n$, so erhält man auf diese Weise einen kompakten Modul A über der zu $\mathbb{Z}_p$ isomorphen Galoisgruppe Γ von $K|k_1$. Da Γ topologisch durch ein Element x erzeugt wird, kann man A auch als einen Modul über dem zweidimensionalen regulären lokalen Potenzreihenring $\mathbb{Z}_p[[x]]$ auffassen. Indem nun IWASAWA die kompakten p-primären Moduln "vom endlichen Typ" über diesem Ring klassifiziert, ergibt sich insbesondere eine Strukturaussage über den Modul A. Weil aber A aus den Idealklassengruppen der Körper $k_n = \mathbb{Q}(\zeta_{p^n})$ aufgebaut ist, erhält man auf diese Weise eine Aussage über die Klassenzahlen der Kreiskörper k_n: Bedeutet nämlich p^{e_n} die maximale in der Klassenzahl von k_n aufgehende p-Potenz, so schreiten die Exponenten e_n bei hinreichend hohem n nach dem Gesetz

$$e_n = \lambda n + \mu p^n + \nu$$

fort, mit allein von der Primzahl p abhängigen Konstanten λ, μ, ν. Dieses Resultat ist interessant für jeden, der um die Rolle weiss, die der p-Teil der Klassenzahl des Körpers $k_1 = \mathbb{Q}(\zeta_p)$ in der Zahlentheorie gespielt hat, und überraschend für jeden, der weiss, wie selten es gelingt, eine Beziehung zwischen den Klassenzahlen verschiedener Körper aufzudecken.

Da die Methoden, die zu diesem Ergebnis führen, nicht auf den Grundkörper $k_1 = \mathbb{Q}(\zeta_p)$ beschränkt sind, stellt sich die Frage nach den möglichen Γ-Erweite-

rungen eines beliebigen Zahlkörpers k , oder, was offenbar das gleiche bedeutet, nach den zu $\underset{\sim}{Z}_p$ isomorphen Faktorgruppen der Galoisgruppe $\mathfrak{G}^{ab}$. Dies ist eine Strukturfrage über $\mathfrak{G}^{ab}$, deren Beantwortung sich unschwer aus der erwähnten klassenkörpertheoretischen Beschreibung von $\mathfrak{G}^{ab}$ ergibt :

SATZ (IWASAWA). - Die Anzahl s_k unabhängiger Γ-Erweiterungen eines Zahlkörpers k ist

$$s_k = [k:\underset{\sim}{Q}] - r_{k,p} ,$$

wobei $r_{k,p}$ den "p-adischen Einheitenrang" bedeutet, d. h.

$$r_{k,p} = \mathrm{Rang}(\log_p(\tau_j \varepsilon_i)) ,$$

mit einem Fundamentalsystem von Einheiten $\varepsilon_1 , \dots , \varepsilon_r$ und den verschiedenen Einbettungen $\tau_j : k \to \overline{\underset{\sim}{Q}}_p$ in den algebraischen Abschluss des Körpers $\underset{\sim}{Q}_p$ der p-adischen Zahlen.

Es wird vermutet, dass $r_{k,p}$ mit dem üblichen Einheitenrang r_k von k übereinstimmt (die "Leopoldt-Vermutung"). Dies wurde für den Fall der abelschen Erweiterungen k von $\underset{\sim}{Q}$ und der abelschen Erweiterungen eines beliebigen imaginär-quadratischen Körpers von A. BRUMER bewiesen.

Verlässt man den Bereich der abelschen Erweiterungen, so sieht man sich einer rauheren Landschaft ausgesetzt. In der Tat fehlt bis heute jeglicher Hinweis, wie eine natürliche Fortsetzung der Klassenkörpertheorie auf den Fall nicht notwendig abelscher Zahlkörper aussehen sollte. Dessenungeachtet liegen eine ganze Anzahl von Resultaten vor, die für sich genommen interessant genug sind, und die gleichzeitig die komplexe Natur unserer beiden fundamentalen Fragestellungen aufzeigen.

Ein wichtiges Problem ist in diesem Zusammenhang das sogenannte Umkehrproblem der Galoistheorie. Es handelt sich um die Frage, ob es über dem festen Grundkörper k eine galoissche Erweiterung $K|k$ gibt, die eine vorgegebene endliche Gruppe G als Galoisgruppe besitzt. Dies ist wiederum eine die Struktur der absoluten Galoisgruppe $\mathfrak{G} = G_k$ betreffende Frage. Sie lautet : Gibt es zu gegebener endlicher Gruppe G einen surjektiven Homomorphismus $\varphi : \mathfrak{G} \longrightarrow G$?

Durch den Kern eines solchen φ wird nämlich ein Körper $K|k$ mit der Galoisgruppe $\mathfrak{G}/\mathrm{Ker}(\varphi) \cong G$ festgelassen. Eine generelle Antwort auf diese Frage liegt bis heute nicht vor, obwohl man fast der Annahme zuneigen möchte, dass sie bejahend ausfallen sollte. Man kennt jedenfalls eine Reihe positiver Resultate, von denen wir die wichtigsten aufzählen wollen.

1° $G = \mathfrak{S}_n$ = symmetrische Permutationsgruppe von n Ziffern. Die klassische Methode, um diese Gruppe als Galoisgruppe einer Erweiterung $K|k$ auszuweisen, ist die folgende. Es seien $x_1, \ldots, x_n$ Unbestimmte, auf denen die Gruppe $\mathfrak{S}_n$ in der natürlichen Weise als Permutationsgruppe wirken möge. $\mathfrak{S}_n$ wird dann zu einer Automorphismengruppe des rationalen Funktionenkörpers $k(x_1, \ldots, x_n)$. Der Fixkörper von $\mathfrak{S}_n$ ist der Körper $k(\sigma_1, \ldots, \sigma_n)$ der symmetrischen Funktionen, der durch die elementar-symmetrischen Funktionen $\sigma_1, \ldots, \sigma_n$ erzeugt wird. Man erhält $k(x_1, \ldots, x_n)$ auf diese Weise als eine galoissche Erweiterung des rein transzendenten Körpers $k(\sigma_1, \ldots, \sigma_n)$ mit der Galoisgruppe $\mathfrak{S}_n$. Die "allgemeine Gleichung"

$$x^n + \sigma_1 x^{n-1} + \ldots + \sigma_n = 0$$

mit den Nullstellen $x_1, \ldots, x_n$ ist eine definierende Gleichung für

$$k(x_1, \ldots, x_n) .$$

Ersetzt man nunmehr die Koeffizienten σ_1 durch Zahlen $\bar{\sigma}_1 \in k$, so erhält man eine Gleichung

$$x^n + \bar{\sigma}_1 x^{n-1} + \ldots + \bar{\sigma}_n = 0 ,$$

deren Nullstellen $\bar{x}_1, \ldots, \bar{x}_n$ eine galoissche Erweiterung $K|k$ erzeugen. Indem man jetzt die Tatsache ausnützt, dass die $\sigma_1, \ldots, \sigma_n$ über k algebraisch unabhängig sind und den Hilbertschen Irreduzibilitätssatz anwendet, kann man zeigen, dass die Wahl der "Spezialisierungen" $\bar{\sigma}_1, \ldots, \bar{\sigma}_n$ in einer solchen Weise getroffen werden kann, dass die Galoisgruppe von $K|k$ die symmetrische Gruppe $\mathfrak{S}_n$ bleibt.

Mit dieser Methode hatte sich die Hoffnung verbunden, jede Gruppe G als Galoisgruppe über k darstellen zu können, indem man G auf dem Körper $k(x_1, \ldots, x_n)$ als transitive Permutationsgruppe der x_1 operieren lässt. In der Tat wäre ein solches Vorgehen ohne weiteres möglich, wenn sich nur zeigen liesse, dass der Fixkörper von $k(x_1, \ldots, x_n)$ unter dieser Operation wieder rein transzendent über k ist. Dieses alte unter dem Namen "Noethersche Vermutung" bekannte Problem wurde nun kürzlich für den Körper $k = \underset{\sim}{Q}$ von SWAN in negativem Sinne beantwortet. Mit Hilfe von Methoden der algebraischen K-Theorie erhielt SWAN das folgende Resultat (vgl. SWAN [50]) :

SATZ. - Sei G zyklisch von der Ordnung n, und operiere G auf den Unbestimmten $x_1, \ldots, x_n$ durch zyklische Vertauschung.

Der Fixkörper von $\underset{\sim}{Q}(x_1, \ldots, x_n)$ unter dieser Aktion ist dann für $n = 47, 113, 233$, und einige weitere Primzahlen nicht rein transzendent.

Es mag darauf hingewiesen werden, dass die Noethersche Vermutung gleichwohl offen bleibt für andere Körper k als dem der rationalen Zahlen und eine positive Antwort

insbesondere bei algebraisch abgeschlossenem Körper k nicht gar so unwahrscheinlich ist. Wie dem aber auch sei, die Hoffnung, das Umkehrproblem über dem Körper $\underset{\sim}{Q}$ auf die beschriebene klassische Weise generell zu lösen, ist dem Swanschen Ergebnis anheimgefallen.

2° $G = \mathfrak{A}_n$ = alternierende Gruppe vom Grade n. Es ist nur für kleine n bekannt, dass der Fixkörper von $k(x_1, \ldots, x_n)$ unter $\mathfrak{A}_n$ wieder rein transzendent ist, so dass man auf dem für die Gruppe $\mathfrak{S}_n$ beschrittenen Weg nicht zum Ziele kommt. Jedoch hat HILBERT eine Methode angegeben, die auch die Gruppe $\mathfrak{A}_n$ allgemein als Galoisgruppe über k ergibt, und die sich folgendermassen darstellt (vgl. HILBERT [14]). Man betrachte für gerades n die Gleichung

$$f(x) + t^2 = 0 , \tag{1}$$

wobei t eine Unbestimmte ist und $f(x)$ ein Polynom vom Grade n mit rationalen Koeffizienten. Dieses besitze den Faktor x^2 und die Ableitung

$$f'(x) = n\, x\, (x - a_1)^2 \times \ldots \times (x - a_r)^2$$

mit untereinander verschiedenen positiven rationalen Zahlen $a_1, \ldots, a_r$. Man betrachtet (1) als Gleichung über dem Körper $k(t)$ und berechnet die Diskriminante sofort zu

$$D = n^n\, t^2\, (f(a_1) + t^2)^2 \times \ldots \times (f(a_r) + t^2)^2 ,$$

wobei die Werte $f(a_1)$ wegen der positiven Ableitung $f'(x)$, $a_{i-1} \leqslant x \leqslant a_i$, von 0 und untereinander verschieden sind. Da n gerade ist, ist das Differenzenprodukt

$$D^{\frac{1}{2}} = \prod_{i<k} (x_i - x_k) = \pm\, n^{n/2}\, t(f(a_1) + t^2) \times \ldots \times (f(a_r) + t^2)$$

der Wurzeln $x_1, \ldots, x_n$ von (1) ein Element des Körpers $k(t)$ und bleibt somit unter allen Permutationen der Galoisgruppe invariant. Daher sind diese Permutationen sämtlich gerade. Zum Nachweis, dass alle geraden Permutationen als Elemente der Galoisgruppe auftreten, genügt es die Gleichung (1) über dem komplexen Funktionenkörper $\underset{\sim}{C}(t)$ zu untersuchen. Betrachtet man aber die durch (1) definierte Riemannsche Fläche, so erhält man eine in den Punkten $t = \pm \sqrt{- f(a_i)}$ verzweigte Überlagerung der Riemannschen Zahlenkugel. Die Verzweigungsstellen sind so beschaffen, dass jeweils drei der n Blätter der Fläche zusammenfallen. Man schliesst hieraus, dass die Galoisgruppe der Gleichung (1) über dem Körper $\underset{\sim}{C}(t)$ von Dreierzykeln erzeugt wird und wegen der Transitivität die volle alternierende Gruppe sein muss.

Im Falle, dass n ungerade ist, verschafft man sich ein Polynom $f(x)$, das der Gleichung

$$x.f'(x) - f(x) = (n - 1)(x - a_1)(x - a_2)^2(x - a_3)^2 \times \ldots \times (x - a_r)^2$$

genügt, und ersetzt die Gleichung (1) durch

$$f(x) + (t^2 - f'(a_1)).x = 0 \ .$$

3° $G = GL(2 , \mathbb{Z}/p)$ = Gruppe aller invertierbaren 2-2-Matrizen über dem Körper von p Elementen. In einer erst vor kurzem erschienenen Arbeit hat SERRE ein aus einer Anregung von SHIMURA (vgl. SHIMURA [49]) hervorgehendes Theorem bewiesen, das über den blossen Existenznachweis eines Körpers mit dieser Galoisgruppe weit hinausgeht, indem es solche Körper in einer kanonischen und gewissermassen expliziten Weise angibt. Man gehe aus von einer über dem Grundkörper k definierten elliptischen Kurve E, die (im Gegensatz zur sonst üblichen Voraussetzung) keine komplexe Multiplikation besitzt. Das soll heissen, dass das Gitter $\Gamma \subseteq \mathbb{C}$ in einer Darstellung $E = \mathbb{C}/\Gamma$ nur die Multiplikation mit ganzen rationalen Zahlen, nicht aber mit weiteren komplexen Zahlen als Endomorphismen zulässt. Betrachtet man E als kommutative algebraische Gruppe über k, so bilden die rationalen Punkte über dem algebraischen Abschluss $\bar{k}$ von k einen $\mathfrak{G} = G(\bar{k}|k)$-Modul $E(\bar{k})$. Der Untermodul

$$E_p = \{x \in E(\bar{k}) \mid p.x = 0\}$$

der p-Teilungspunkte ist als abelsche Gruppe vom Typ $\mathbb{Z}/p \times \mathbb{Z}/p$, so dass man durch die $\mathfrak{G}$-Aktion einen Homomorphismus

$$\varphi : \mathfrak{G} \to \mathrm{Aut}(E_p) \cong GL(2 , \mathbb{Z}/p)$$

erhält. Dieser Homomorphismus legt eine galoissche Erweiterung $K_p|k$ mit der Galoisgruppe $G_p = \varphi(\mathfrak{G})$ fest, den Körper, der durch die Koordinaten der p-Teilungspunkte erzeugt wird. Das Serresche Resultat besagt nun u. a., dass G_p für fast alle Primzahlen p die volle Gruppe $\mathrm{Aut}(E_p) = GL(2 , \mathbb{Z}/p)$ ist (vgl. SERRE [48]), und durch die Betrachtung verschiedener elliptischer Kurven ergibt sich $GL(2 , \mathbb{Z}/p)$ sogar für jede Primzahl p als Galoisgruppe über k.

4° G auflösbar. Ein überaus tiefliegendes Theorem von ŠAFAREVIČ besagt, dass jede auflösbare Gruppe G als Galoisgruppe über dem Zahlkörper k auftritt (vgl. ŠAFAREVIČ [41]). Der grundlegende Beweisgedanke ist der, dass man den gesuchten Körper durch eine Kette übereinander abelscher Körper aufbaut. Bei diesem Versuch stösst man jedoch sehr rasch auf die heftigsten Schwierigkeiten. Hat man nämlich schon eine Erweiterung $K_i|k$ mit gegebener Galoisgruppe G_i konstruiert, so ist es i. a. unmöglich, auf K_i eine abelsche Erweiterung K_{i+1} aufzubauen, die über k eine gewünschte Galoisgruppe G_{i+1} besitzt. Man wird daher gezwungen, nach Bedingungen für die Erweiterung $K_i|k$ zu suchen, die die Existenz eines Körpers K_{i+1} garantieren. Es zeigt sich, dass man zu solchen Bedingungen zunächst nur dann gelangen kann, wenn G_{i+1} eine zentrale Gruppenerweiterung von G_i ist. Bei dieser Beschränkung können natürlich nur Körper mit nilpotenter Galoisgruppe entstehen. Nimmt man diesen Mangel vorübergehend in Kauf, so lässt sich ein System von Bedingungen über das Zerlegungsverhalten der Primstellen von k in K_i bereitstellen, unter denen ein Körper K_{i+1} mit der vorgeschriebenen Galoisgruppe G_{i+1}

gefunden werden kann. Es taucht aber jetzt eine neue Schwierigkeit auf, denn da man nach der Konstruktion von K_{i+1} einen nächsten Schritt auszuführen hat, muss der Körper K_{i+1} so konstruiert werden, dass auch er diesen Bedingungen genügt. Wie sich herausstellt, ist dies i. a. unmöglich. Man kann aber eine Reihe von "Hindernissen" aufstellen (bei ŠAFAREVIČ geschieht dies mit Hilfe der Theorie der höheren Potenzreste), deren Verschwinden mit der Existenz eines solchen Körpers K_{i+1} gleichbedeutend ist. ŠAFAREVIČ entwickelt nun einen feinsinnigen gruppentheoretischen Prozess, durch den sich das Verschwinden der Hindernisse erzwingen lässt. Bei diesem Prozess muss man jedoch die schon konstruierte Erweiterung $K_i|k$ wesentlich abändern und zu einer Teilerweiterung $K_i'|k$ übergehen. Durch diese Vorgehensweise wird die Möglichkeit, den Induktionsbeweis über den Körpergrad zu führen zerstört. Die entscheidende Idee besteht vielmehr darin, dass sich die Induktion anstatt dessen über die Nilpotenzklasse, d. h. die Länge der absteigenden Zentralreihe der betreffenden Galoisgruppen vollzieht.

Nachdem man gelernt hat, Körper mit vorgegebener nilpotenter Galoisgruppe zu konstruieren, kann man sich dem allgemeinen auflösbaren Fall zuwenden. Man geht dabei wieder von einer schon konstruierten Erweiterung $K_i|k$ mit der Galoisgruppe G_i aus und betrachtet den zu einer p-Sylowgruppe H von G_i gehörigen Zwischenkörper L, $k \subseteq L \subseteq K_i$. Um auf K_i einen abelschen Körper K_{i+1} aufzubauen, der die gewünschte Galoisgruppe G_{i+1} besitzt, konstruiert man eine geeignete, über L galoissche Erweiterung $N \supseteq K_i \supseteq L$ in solcher Weise, dass sich der gesuchte Körper K_{i+1} im Kompositum der zu N über k konjugierten Körper N, N', N'', ... findet. Beschränkt man sich erlaubterweise auf den Fall, dass $K_{i+1}|K_i$ und damit $N|K_i$ eine abelsche p-Erweiterung werden soll, so gelingt dieses Vorgehen in der Tat, vorausgesetzt, dass die Erweiterung $K_i|k$ wieder ein System das Zerlegungsverhalten der Primstellen betreffender Bedingungen genügt. Weil man aber auf K_{i+1} einen weiteren Körper aufzubauen hat, muss auch der Körper N solche Bedingungen erfüllen, und nicht nur dies : N muss so konstruiert werden, dass die über k zu N konjugierten Körper N, N', N'', ... über K_i unabhängig sind und ebenfalls scharfen arithmetischen Forderungen genügen, wodurch sich die schon im nilpotenten Fall auftretenden Schwierigkeiten multiplizieren. Eine sorgfältige Durchführung dieses Gedankens führt indessen wieder auf ein System von Hindernissen, das erneut einem gruppentheoretischen Vernichtungsprozess unterworfen werden kann, der nun in ähnlicher Weise wie im nilpotenten Fall zum allgemeinen Ergebnis führt.

In der Aufgabenstellung des Umkehrproblems der Galoistheorie bleibt die zweite unserer fundamentalen Fragen, nämlich die nach dem Zerlegungsgesetz der Primideale, unberücksichtigt. Man kann sich aber fragen, inwieweit man neben der Galoisgruppe auch das Zerlegungsverhalten der Primstellen vorschreiben darf. In dieser Richtung hat man den klassischen Existenzsatz von Grunwald, der besagt, dass man bei Vorgabe zyklischer Erweiterungen $K_p|k_p$ der p-adischen Komplettierungen an endlich vielen Primstellen p von k stets eine globale zyklische Erweiterung $K|k$ vom Grade $[K:k] = k.g.V.\{[K_p:k_p]\}$ existiert, die an den besagten Primstellen p die Erweite-

rungen $K_p|k_p$ als Komplettierungen besitzt, es sei denn, man befindet sich in einem speziellen Fall, der z. B. dann nicht auftritt, wenn die Grade $[K_p:k_p]$ ungerade sind (vgl. etwa HASSE [12]). Durch ein systematisches Studium der von ŠAFAREVIČ entwickelten Ideen lässt sich dieser Satz unter Verwendung des Dualitätssatzes von TATE und POITOU auf nilpotente Erweiterung verallgemeinern. Sei z. B. $k = \mathbb{Q}$ der Körper der rationalen Zahlen und sei eine beliebige endliche nilpotente Gruppe G ungerader Ordnung vorgegeben. Sind dann an endlich vielen Stellen p von k nilpotente Erweiterungen $K_p|k_p$ mit in G einbettbaren Galoisgruppen $G(K_p|k_p)$ vorgeschrieben, so gibt es stets eine globale Erweiterung $K|k$, die einerseits die Gruppe G als Galoisgruppe besitzt, andererseits an den endlich vielen Stellen p die Erweiterungen $K_p|k_p$ als Komplettierungen annimmt (vgl. NEUKIRCH [35]).

Das Umkehrproblem ist, wie wir gesehen haben, eine Frage, die die Struktur der absoluten Galoisgruppe $\mathfrak{G}$ über k betrifft, nämlich die Frage nach den Typen endlicher Faktorgruppen von $\mathfrak{G}$. Aber selbst wenn wir einen vollständigen Überblick über diese Typen gewinnen könnten, so wäre dadurch keinesfalls eine erschöpfende Auskunft über die Struktur von $\mathfrak{G}$ selbst gegeben. Um in diese einen echten Einblick zu erhalten, hat man ein schärferes Problem zu studieren, das sogenannte Einbettungsproblem. Dieses besteht in einem exakten Diagramm

$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G} & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & A & \to & E & \xrightarrow{j} & G & \to & 1 \end{array}$$

mit endlichen Gruppen A, E, G und surjektivem Homomorphismus φ, und in der Frage nach der Existenz eines surjektiven Homomorphismus $\psi : \mathfrak{G} \to E$ mit $j \circ \psi = \varphi$. Körpertheoretisch lässt sich diese Aufgabenstellung folgendermassen verstehen. Durch den surjektiven Homomorphismus φ, genauer durch den Kern $\mathfrak{G}_0$ von φ wird eine galoissche Erweiterung $K|k$ mit der Galoisgruppe

$$G(K|k) = \mathfrak{G}/\mathfrak{G}_0 \cong G$$

festgelegt. Die Existenz eines surjektiven Homomorphismus $\psi : \mathfrak{G} \to E$ mit $j \circ \psi = \varphi$ bedeutet dementsprechend die Existenz einer galoisschen Erweiterung $N \supseteq K \supseteq k$ mit zu E isomorpher Galoisgruppe $G(N|k)$, derart dass der kanonische Homomorphismus $G(N|k) \to G(K|k)$ nach Identifizierung der Gruppen mit E, bzw. G, die vorgegebene Gruppenerweiterung $E \to G$ realisiert.

Das Einbettungsproblem stellt eine erhebliche Verschärfung des erwähnten Umkehrproblems dar, das man offenbar durch die Spezialisierung $G = 1$ zurückerhält. Im Gegensatz zu dem letzteren zeigen schon die einfachsten Beispiele, dass das Einbettungsproblem über einem endlichen algebraischen Zahlkörper i. a. unlösbar ist. Durch eine vollständige Übersicht über alle lösbaren Einbettungsprobleme würde man jedoch einen genauen Einblick in die Struktur von $\mathfrak{G}$ gewinnen. Dies wird besonders klar an einem von K. IWASAWA bewiesenen Satz. IWASAWA zeigte, dass über einem unendlichen Zahlkörper vom Typ des "Kroneckerschen Körpers", der über $\mathbb{Q}$ durch alle Einheitswurzeln erzeugt wird, jedes Einbettungsproblem eine Lösung besitzt, voraus-

gesetzt, der Kern A ist eine auflösbare Gruppe. Aufgrund dieser Tatsache konnte IWASAWA auf rein gruppentheoretische Weise den folgenden Satz beweisen (vgl. IWASAWA [18]) :

SATZ. - Sei k der Kroneckersche Körper und $\tilde{\mathfrak{G}}$ die Galoisgruppe der maximalen auflösbaren Erweiterung $\tilde{k}|k$. Dann ist $\tilde{\mathfrak{G}}$ die freie pro-auflösbare Gruppe vom Rang $\aleph_0$.

Die freie pro-auflösbare Gruppe vom Rang $\aleph_0$ erhält man dabei, indem man in der gewöhnlichen, durch x_1 , x_2 , x_3 , ... erzeugten freien Gruppe F alle Normalteiler N betrachtet, die fast alle x_i enthalten und eine endliche auflösbare Faktorgruppe F/N liefern, und sodann den Limes $\varprojlim_N F/N$ bildet.

Durch die Auflösbarkeitsvoraussetzung über A kann sich natürlich nur die Struktur der maximalen pro-auflösbaren Faktorgruppe $\tilde{\mathfrak{G}}$ von $\mathfrak{G}$ aufklären. Das Iwasawasche Resultat hat aber noch einen anderen Mangel, der darin besteht, dass sich Struktur von $\tilde{\mathfrak{G}}$ nicht in kanonischer Weise, d. h. nicht durch kanonische freie Erzeugenden ergibt.

Über einem endlichen algebraischen Zahlkörper ist das Einbettungsproblem von einem ungleich grösseren Schwierigkeitsgrad. HASSE schlug vor, die Aufgabe zunächst dahingehend abzuschwächen, dass man anstelle eines Körpers N|k lediglich eine galoissche Algebra als Lösung sucht (vgl. HASSE [13]). In unserer Formulierung bedeutet dies, dass man die Surjektivitätsforderung für den Lösungshomomorphismus $\psi : \mathfrak{G} \to E$ zunächst fallen lässt. Dieser Gedanke hat sich in vieler Hinsicht als fundamental erwiesen. So konnte M. IKEDA zeigen, dass über Einbettungsprobleme mit abelschem Kern A der folgende Satz gilt (vgl. IKEDA [17]) :

SATZ. - Jedes Einbettungsproblem mit abelschem Kern A , das durch eine galoissche Algebra lösbar ist, besitzt auch einen Körper als Lösung.

Hieraus ergibt sich speziell das folgende schon früher von A. SCHOLZ bewiesene Ergebnis (vgl. SCHOLZ [44]) :

SATZ. - Jedes Einbettungsproblem mit abelschem Kern A und zerfallender Gruppenerweiterung

$$1 \to A \to E \xrightarrow{j} G \to 1$$

besitzt einen Körper als Lösung.

Ist nämlich $G \xrightarrow{s} E$ ein Zerfällungshomomorphismus, so erhält man in dem Kompositum $\mathfrak{G} \xrightarrow{\varphi} G \xrightarrow{s} E$ einen (i. a. nicht surjektiven) Homomorphismus $\psi_1 : \mathfrak{G} \to E$ mit $j \circ \psi_1 = \varphi$, so dass sich aufgrund des Ikedaschen Satzes sogar die Existenz eines surjektiven Lösungshomomorphismus ergibt.

Das bisher wohl allgemeinste Resultat über das Einbettungsproblem stammt von ŠAFAREVIČ. Es erweitert den Scholzschen Satz auf den Fall, dass der Kern A nicht

mehr notwendig abelsch sondern eine p-Gruppe, mit einer Nilpotenzklasse $< p$ ist (vgl. ŠAFAREVIČ [40]). Es lässt sich vermuten, dass das Einbettungsproblem im zerfallenden Fall sogar bei beliebiger auflösbarer Gruppe A als Kern Lösung (durch einen Körper) besitzt, jedoch scheitert zur Zeit der Beweis eines solchen Satzes vor allem an gruppentheoretischen Schwierigkeiten. Man hätte aber hierin das denkbar allgemeinste Ergebnis über das Einbettungsproblem zu sehen, weil man im nichtzerfallenden Fall zu allgemeingültigen Sätzen nur unter Bedingungen kommen kann, die die Grundkörpererweiterung $K|k$ mit der Galoisgruppe G einschränken.

Das Einbettungsproblem über einem algebraischen Zahlkörper trägt alle Kennzeichen eines algebraisch-arithmetischen Problems, und zwar insofern, als auch die zweite unserer beiden fundamentalen Fragen, d. h. die nach dem Zerlegungsverhalten der Primstellen in den gesuchten Körpererweiterungen eine unabweisliche Rolle spielt, obgleich dies in den Ergebnissen nicht unbedingt erkennbar werden muss. Jedem Einbettungsproblem über einem Zahlkörper k sind nämlich kanonischer Weise "lokale" Einbettungsprobleme über den Komplettierungen k_p zugeordnet, und es ergeben sich dadurch eine Reihe wichtiger Lokal-Global-Fragen, die etwa beim Aufbau von Körpern mit vorgegebener auflösbarer Galoisgruppe von entscheidender Bedeutung sind. Wann z. B. kann man von der Lösbarkeit der lokalen Einbettungsprobleme auf die Lösbarkeit des globalen Einbettungsproblems schliessen, oder wann existieren globale Lösungen, die im Lokalen vorgegebene Lösungen induzieren ? Ein systematisches Studium der Lösungsmannigfaltigkeiten solcher Probleme führt auf eine Hindernistheorie, die sich harmonisch in den Gedankenkreis um den Dualitätssatz von TATE und POITOU einlagert. Es zeigt sich dabei, dass die Theorie der auflösbaren Zahlkörper von diesem, die Ergebnisse der Klassenkörpertheorie voll ausschöpfenden Dualitätssatz beherrscht wird, der auch die von ŠAFAREVIČ entwickelten Ideen allgemeinen Prinzipien unterzuordnen vermag (vgl. NEUKIRCH [35]).

Der den abelschen Zahlkörpern nächst gelegene Bereich ist der der nilpotenten Erweiterungen, oder, was auf das gleiche hinausläuft, der p-Erweiterungen (Erweiterungen mit einer p-Gruppe als Galoisgruppe). Hier liegt in der Tat eine Fülle von Resultaten vor, von denen nur einige hervorgehoben seien. Sei k ein algebraischer Zahlkörper und sei jetzt $\mathfrak{G}$ die Galoisgruppe der <u>maximalen</u> p-<u>Erweiterung</u> $k(p)|k$ (Kompositum aller endlichen p-Erweiterungen). $\mathfrak{G}$ ist dann eine pro-p-Gruppe, d. h. der projektive Limes eines Systems endlicher p-Gruppen . In gleicher Weise seien $\mathfrak{G}_p$ die Galoisgruppen der maximalen p-Erweiterungen $k_p(p)|k_p$ über den Komplettierungen k_p von k . Die Struktur der lokalen Galoisgruppen $\mathfrak{G}_p$ wurde in expliziter Weise von DEMUSKIN durch Erzeugende und Relationen angegeben (vgl. DEMUSKIN [6]). Es handelt sich um endlich erzeugte pro-p-Gruppen mit entweder keiner oder nur einer definierenden Relation. Bettet man den Körper k(p) in $k_p(p)$ ein, so erhält man durch die Einschränkung der k_p-Automorphismen von $k_p(p)$ auf k(p) eine Einbettung von $\mathfrak{G}_p$ in $\mathfrak{G}$, derart dass $\mathfrak{G}_p$ als Zerlegungsgruppe einer Fortsetzung $\overline{p}$ von p auf k(p) erscheint. Auch hier besteht das fundamentale Problem wieder in der Frage nach der Struktur von $\mathfrak{G}$ und der Lage der Zerlegungs-

gruppen $\mathfrak{G}_p$ in $\mathfrak{G}$. Einen sehr interessanten Satz hierüber hat H. KOCH (neben vielen anderen) bewiesen. Man geht dabei von einer Darstellung der pro-p-Gruppe $\mathfrak{G}$ durch "Erzeugende und Relationen" aus. Dies soll genauer folgendes bedeuten. Man wähle ein beliebiges minimales Erzeugendensystem E der topologischen Gruppe $\mathfrak{G}$ und bilde neben $\mathfrak{G}$ die freie durch die Elemente aus E erzeugte pro-p-Gruppe $\mathfrak{J}$. Diese entsteht aus der gewöhnlichen von E erzeugten freien Gruppe F durch Bildung des projektiven Limes

$$\mathfrak{J} = \varprojlim F/N \ ,$$

wobei N alle Normalteiler von F durchläuft, die fast alle der Erzeugenden aus E enthalten, und für die F/N eine endliche p-Gruppe ist. Es ergibt sich dann eine kanonische exakte Sequenz

$$1 \to \mathfrak{R} \to \mathfrak{J} \to \mathfrak{G} \to 1 \ ,$$

wobei man die Elemente aus $\mathfrak{R}$ als "Relationen" zwischen den Erzeugenden aus E anzusehen hat. In gleicher Weise erhält man durch Auswahl eines minimalen, d. h. endlichen Erzeugendensystems E_p von $\mathfrak{G}_p$ eine kanonische exakte Sequenz

$$1 \to \mathfrak{R}_p \to \mathfrak{J}_p \to \mathfrak{G}_p \to 1 \ ,$$

wobei $\mathfrak{J}_p$ die freie durch E_p erzeugte pro-p-Gruppe ist. Es ist nun evident, dass man die Injektionen $\mathfrak{G}_p \to \mathfrak{G}$ zu Injektionen $\mathfrak{J}_p \to \mathfrak{J}$ hochheben kann, derart, das die kommutativen exakten Diagramme

$$\begin{array}{ccccccccc} 1 & \to & \mathfrak{R}_p & \to & \mathfrak{J}_p & \to & \mathfrak{G}_p & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathfrak{R} & \to & \mathfrak{J} & \to & \mathfrak{G} & \to & 1 \end{array}$$

entstehen. Der Satz von Koch lautet jetzt (vgl. KOCH [27], 11.2) :

SATZ. - Die globale Relationengruppe $\mathfrak{R}$ wird als Normalteiler von $\mathfrak{J}$ (topologisch) durch die Bilder aller lokalen Relationengruppen $\mathfrak{R}_p$ erzeugt.

Man muss sich davor hüten, hieraus schliessen zu wollen, dass $\mathfrak{G}$ in irgendeiner Weise das freie Produkt der lokalen Galoisgruppen $\mathfrak{G}_p$ ist. Dies wäre der Fall, wenn $\mathfrak{J}$ die freie durch die Vereinigung $\bigcup_p E_p$ erzeugte pro-p-Gruppe wäre. Diese Vereinigung aber ist alles andere als ein minimales Erzeugendensystem von $\mathfrak{G}$. Zu einer freien Zerlegung der globalen Galoisgruppe $\mathfrak{G}$ in die lokalen Untergruppen $\mathfrak{G}_p$ kommt man jedoch, wenn man anstelle des endlichen algebraischen Zahlkörpers k einen ganz bestimmten unendlichen Zahlkörper zugrunde legt, nämlich die zur Primzahl $p \neq 2$ gehörige Γ-Erweiterung des Körpers $\mathbb{Q}$. Diese entsteht folgendermassen : Sei k' der Körper, der über $\mathbb{Q}$ durch alle p^n-ten Einheitswurzeln, $n = 1 \ , \ 2 \ , \ 3 \ , \ \ldots \ ,$ erzeugt wird. Die Galoisgruppe von $k'|\mathbb{Q}$ ist dann vom Typ $\mathbb{Z}_p \times \mathbb{Z}/(p-1)$, wobei $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n$ die Gruppe der ganzen p-adischen Zahlen bedeutet. Die Γ-Erweiterung $k|\mathbb{Q}$ ist dann der in k' gelegene Teilkörper mit der Galoisgruppe $G(k|\mathbb{Q}) = \mathbb{Z}_p$. Über der Primzahl p liegt genau eine (total verzweigte) Primstelle von k , die mit p_0 bezeichnet werde. Es gilt dann (vgl.

NEUKIRCH [34], § 11) :

SATZ. - Ist $\mathfrak{G}$, bzw. $\mathfrak{G}_p$, die Galoisgruppe der maximalen p-Erweiterung $k(p)|k$ bzw. $k_p(p)|k_p$, so gilt

$$\mathfrak{G} = \coprod_{p \neq p_0} \mathfrak{G}_p \quad \text{(freies pro-p-Produkt)}$$

Das freie pro-p-Produkt ist dabei ganz analog, wie die freie pro-p-Gruppe definiert : Man bilde zunächst übliche freie Produkt $\ast_{p \neq p_0} \mathfrak{G}_p$ und sodann den projektiven Limes $\coprod_{p \neq p_0} \mathfrak{G}_p = \varprojlim_N (\ast_{p \neq p_0} \mathfrak{G}_p)/N$, wobei N alle Normalteiler von $\ast_{p \neq p_0} \mathfrak{G}_p$ durchläuft, die eine endliche p-Gruppe als Faktorgruppe liefern, die fast alle der Untergruppen $\mathfrak{G}_p$ enthalten, und für die überdies $N \cap \mathfrak{G}_p$ offen in $\mathfrak{G}_p$ ist (vgl. NEUKIRCH [33]). Der obige Satz ist eine (fast) vollständige Antwort auf beide unserer fundamentalen Fragestellungen, was die p-Erweiterungen des Körpers k angeht : Sowohl die Struktur der globalen Galoisgruppe $\mathfrak{G}$, als auch die Lage der lokalen Gruppen $\mathfrak{G}_p$, $p \neq p_0$, in $\mathfrak{G}$ liegt in der denkbar einfachsten Weise zutage. Man kann das Resultat als ein Analogon zum Riemannschen Existenzsatz der Funktionentheorie auffasen. Als unmittelbares Korollar erhält man nämlich die Tatsache, dass es bei Vorgabe endlicher p-Erweiterungen $K_p|k_p$ an allen Stellen $p \neq p_0$ (Unverzweigtheit an fast allen Stellen vorausgesetzt) eine p-Erweiterung $K|k$ gibt, die einerseits eine vorgegebene p-Gruppe G als Galoisgruppe besitzt und andererseits an den Stellen $p \neq p_0$ die Erweiterungen $K_p|k_p$ als Komplettierungen annimmt ; dabei hat man nur zu fordern, dass die Galoisgruppen $G(K_p|k_p)$ in G einbettbar sind.

Im Falle eines endlichen algebraischen Zahlkörpers k ist die Gruppe $\mathfrak{G}$ der maximalen p-Erweiterung weit davon entfernt, freies Produkt der Untergruppen $\mathfrak{G}_p$ zu sein. Es lässt sich aber zeigen, dass je endlich viele $\mathfrak{G}_p$ frei in der Gruppe $\mathfrak{G}$ liegen, d. h. das (topologische) Erzeugnis endlich vieler Zerlegungsgruppen $\mathfrak{G}_p$ ist das freie pro-p-Produkt dieser Gruppen.

Durch den oben zitierten Satz über die Γ-Erweiterung k von $\mathbb{Q}$ bietet sich ein Weg an, die Struktur der maximalen p-Erweiterung von $\mathbb{Q}$ aufzudecken. Da nämlich die Galoisgruppe $\Gamma = G(k|\mathbb{Q}) \cong \mathbb{Z}_p$ selbst eine pro-p-Gruppe ist, ist $k(p)$ gleichzeitig die maximale p-Erweiterung von $\mathbb{Q}$. Bezeichnet man mit G die Galoisgruppe von $k(p)|\mathbb{Q}$, so erhält man eine zerfallende Gruppenerweiterung

$$1 \to \mathfrak{G} = \coprod_{p \neq p_0} \mathfrak{G}_p \to G \to \Gamma \to 1 \ .$$

Die Gruppe Γ wird dabei (topologisch) von einem Element φ erzeugt. Zur vollständigen Bestimmung der Struktur von G kommt es nun darauf an, die Aktion von φ auf dem Kern $\mathfrak{G} = \coprod_{p \neq p_0} \mathfrak{G}_p$ explizit anzugeben. Wegen der freien Zerlegung genügt es dabei sogar, nur die Bilder $\mathfrak{G}_p^{\varphi}$ der freien Faktoren $\mathfrak{G}_p$ explizit zu bestimmen. Man sieht sofort, dass $\mathfrak{G}_p^{\varphi}$ eine über der Primstelle φp gelegene Zerlegungsgruppe von $k(p)|k$ ist. Die Frage, ob sich die Auswahl der $\mathfrak{G}_p$ unter ihren Konjugierten so treffen lässt, dass für alle $p \neq p_0$ die Gleichheit $\mathfrak{G}_p^{\varphi} = \mathfrak{G}_{\varphi p}$

gilt, ist jedoch sofort zu verneinen. $\mathfrak{G}_p^{\varphi}$ ist in $\mathfrak{G}$ nur konjugiert zu $\mathfrak{G}_{\varphi p}$, und es ergibt sich daher die Aufgabe,. diese Konjugiertheit explizit anzugeben. Man darf sich aber nicht darüber hinwegtäuschen, dass dieses Problem von höchstem Schwierigkeitsgrad ist und nur einmal mehr zeigt, wie weit man von einer abschliessenden Theorie der p-Erweiterungen entfernt ist.

Im Zusammenhang mit den p-Erweiterungen wollen wir noch eine andere berühmte Fragestellung der Zahlentheorie erwähnen. Es sei $k_{nr}(p)|k$, bzw. $\tilde{k}_{nr}|k$, die maximale unverzweigte p-Erweiterung, bzw. die maximale unverzweigte auflösbare Erweiterung, von k. Man nennt $\tilde{k}_{nr}$ den Klassenkörperturm von k und $k_{nr}(p)$ den p-Klassenkörperturm. Unter dem Klassenkörperturmproblem versteht man die Frage :

Ist die Erweiterung $\tilde{k}_{nr}|k$ von endlichem Grad ?

Eine positive Antwort hierauf hätte eine wichtige Konsequenz : Aus dem Hauptidealsatz der Klassenkörpertheorie könnte man nämlich schliessen, dass $\tilde{k}_{nr}$ die Klassenzahl 1 besitzt, so dass also k in einem endlichen algebraischen Zahlkörper mit der Klassenzahl 1 eingebettet ist. Dieses Problem hat lange den durchaus intensiven Bemühungen der Zahlentheoretiker widerstanden, bis es schliesslich von ŠAFAREVIČ und GOLOD in negativem Sinne entschieden wurde (vgl. GOLOD-ŠAFAREVIČ [9]). Diese beiden Mathematiker zeigten, dass sogar die meisten quadratischen Zahlkörper schon einen unendlichen 2-Klassenkörperturm $k_{nr}(2)$ besitzen, so dass wegen $k_{nr}(2) \subseteq \tilde{k}_{nr}$ erst recht der Klassenkörperturm $\tilde{k}_{nr}$ von unendlichem Grade ist.

Den bisher geschilderten Erörterungen kann man eine ganz andere Betrachtungsweise der Körper entgegensetzen, indem man nämlich nicht mehr nach den Faktorgruppen etwa der absoluten Galoisgruppe $\mathfrak{G} = G_{\tilde{Q}}$ fragt, sondern nach ihren Untergruppen. Diese Untergruppen sind vielgestaltig, aber durchaus nicht von beliebigem Typus. Zwar zeigt ein Ergebnis von W. KUYK (vgl. KUYK [29]), dass jede pro-endliche Gruppe G, die eine abzählbare Umgebungsbasis des Einselementes besitzt, als Faktorgruppe einer passenden Untergruppe von $\mathfrak{G}$ auftritt (also als Galoisgruppe einer geeigneten Erweiterung i. a. unendlicher algebraischer Zahlkörper), doch gibt es viele andere Resultate, die die Struktur der Untergruppen selbst einschränken. Nach Untersuchungen von M. JARDEN (vgl. JARDEN [24]) tendieren z. B. die endlich erzeugten Untergruppen von $\mathfrak{G} = G_{\tilde{Q}}$ dahin, freie proendliche Gruppen zu sein, Genauer zeigte JARDEN, dass die Menge der n-Tupel $(\sigma_1, \ldots, \sigma_n) \in \mathfrak{G}^n$, für die die durch $\sigma_1, \ldots, \sigma_n$ erzeugte abgeschlossene Untergruppe von $\mathfrak{G}$ keine freie pro-endliche Gruppe ist, im n-fachen direkten Produkt $\mathfrak{G}^n$ das Haarsche Mass Null besitzt. Ein anderer, sehr interessanter Satz von W.-D. GEYER (vgl. GEYER [10]) besagt, dass $\mathfrak{G}$ ausser den pro-zyklischen, also den von einem Element erzeugten abgeschlossenen Untergruppen keine abelschen Untergruppen hat. F. K. SCHMIDT bewies ferner, dass $\mathfrak{G}$ keinen echten auflösbaren Normalteiler besitzt (vgl. SCHMIDT [43]). Insbesondere ist also das Zentrum und die Frattinigruppe von $\mathfrak{G}$ trivial. Da die Frattinigruppe der Durchschnitt aller maximalen Untergruppen ist, folgt hieraus, dass das Kompo-

situm aller minimalen Erweiterungen $K|\underset{\sim}{Q}$ der algebraische Abschluss $\overline{\underset{\sim}{Q}}$ von $\underset{\sim}{Q}$ ist.

Die auflösbaren Untergruppen von $\mathfrak{G}$ sind insofern interessant, als ihre Fixkörper dadurch charakterisiert sind, dass über ihnen jede algebraische Gleichung durch Radikale auflösbar ist. Lässt man die Normalitätsvoraussetzung fallen, so findet man eine ganze Reihe auflösbarer Untergruppen von $\mathfrak{G}$, wiewohl eine vollständige Klassifizierung noch aussteht. So sind z. B. die Zerlegungsgruppen $\mathfrak{G}_p$ und die p-Sylowgruppen von $\mathfrak{G}$ auflösbar, und man kann darüberninaus viele weitere Beispiele konstruieren (vgl. NEUKIRCH [30]). Bei solchen Konstruktionen stösst man auf die merkwürdigsten Situationen. Es gibt z. B. Zahlkörper $k \neq \overline{\underset{\sim}{Q}}$, über denen ausser den linearen überhaupt keine irreduzible Gleichung durch Radikale auflösbar ist, während jeder echte algebraische Oberkörper von k die Eigenschaft besitzt, dass alle algebraischen Gleichungen durch Radikale auflösbar sind.

Ein von E. ARTIN gelöstes Problem ist das der endlichen Untergruppen von $G_{\underset{\sim}{Q}}$, also die Frage nach den Zahlkörpern k mit $[\overline{\underset{\sim}{Q}}:k] < \infty$ (vgl. ARTIN [1]). Es gilt hierüber der

SATZ. - Ist $k \subseteq \overline{\underset{\sim}{Q}}$ ein Körper mit $1 < [\overline{\underset{\sim}{Q}}:k] < \infty$, so ist k zum Körper $\underset{\sim}{R}^a$ aller algebraischen reellen Zahlen isomorph. Insbesondere ist also $[\overline{\underset{\sim}{Q}}:k] = 2$.

Dieser Satz ist nicht zuletzt deswegen bemerkenswert, als der i. w. topologisch definierte Körper $\underset{\sim}{R}^a$ rein algebraisch dadurch charakterisiert ist, dass die absolute Galoisgruppe $G_{\underset{\sim}{R}^a}$ über $\underset{\sim}{R}^a$ endlich ist. Eine analoge Problemstellung kann man für die p-adischen Zahlkörper $\underset{\sim}{Q}_p$ anstelle des Körpers $\underset{\sim}{R}$ der reellen Zahlen betrachten. Ist $k = \underset{\sim}{Q}_p^a$ der Körper aller algebraischen p-adischen Zahlen, d. h. der grösste absolut algebraische Teilkörper von $\underset{\sim}{Q}_p$, so wird man fragen, ob sich dieser Körper, aufgefasst als Teilkörper von $\overline{\underset{\sim}{Q}}$, ebenfalls durch Bedingungen charakterisieren lässt, die allein die Galoisgruppe $G_k = G(\overline{\underset{\sim}{Q}}|k)$ als abstrakte profendliche Gruppe betreffen (Für den Zahlentheoretiker sind die Körper $\underset{\sim}{R}^a$, $\underset{\sim}{Q}_p^a$ ein vollwertiges Äquivalent der Körper $\underset{\sim}{R}$, $\underset{\sim}{Q}_p$). Diese Frage lässt sich in der Tat positiv beantworten. Für eine Primzahl $p \neq 2$ kann man das Resultat etwa folgendermassen formulieren (vgl. NEUKIRCH [32]) :

SATZ. - Ist k ein Teilkörper des Körpers $\overline{\underset{\sim}{Q}}$ aller algebraischen Zahlen und G_k seine absolute Galoisgruppe, so sind die folgenden Bedingungen äquivalent :

(i) k ist isomorph zum Körper $\underset{\sim}{Q}_p^a$ aller algebraischen p-adischen Zahlen.
(ii) G_k ist auflösbar, $cd_\ell(G_k) = 2$ für alle Primzahlen ℓ und $\chi_p(G_k) \neq 0$.

Darin ist $cd_\ell(G_k)$ die kohomologische ℓ-Dimension von G_k, und es bedeutet $\chi_p(G_k) \neq 0$, dass die Euler-Poincaré-Charakteristik

$$\chi_p(G_k) = \sum_{i=1}^{\infty} (-1)^i \dim H^i(G_k, \underset{\sim}{Z}/p)$$

von G_k existiert und von Null verschieden ist.

Aus diesem Resultat lassen sich einige bemerkenswerte Folgerungen für die end-

lichen algebraischen Zahlkörper ziehen. Unter Ausnutzung gewisser klassischer Sätze von M. BAUER und F. GASSMANN über die Primzerlegung in endlichen algebraischen Zahlkörpern erhält man u. a. die Tatsache, dass ein endlicher Normaloberkörper K von $\underset{\sim}{Q}$ eindeutig durch den Typus der Gruppe G_K als abstrakte pro-endliche Gruppe bestimmt ist. Mit anderen Worten (vgl. NEUKIRCH [32]) :

SATZ. - Sind K und K' irgend zwei Normaloberkörper von $\underset{\sim}{Q}$, so folgt aus der Isomorphie $G_K \cong G_{K'}$ die Gleichheit $K = K'$.

Es überrascht hierbei, dass sich der Aufbau der algebraischen Erweiterungen selbst über vom algebraischen Standpunkt so scheinbar gleichgearteten Körpern, wir etwa $K = \underset{\sim}{Q}(\sqrt{3})$ und $K' = \underset{\sim}{Q}(\sqrt{5})$ in wesentlich verschiedener Art und Weise vollzieht. Aus dem obigen Satz gewinnt man auch die folgende Tatsache über die Struktur der absoluten Galoisgruppe $\mathfrak{G} = G_{\underset{\sim}{Q}}$:

SATZ. - Die (abgeschlossenen) Normalteiler von $\mathfrak{G} = G_{\underset{\sim}{Q}}$ sind sämtlich charakteristische Untergruppen von $\mathfrak{G}$.

Dies ist sehr leicht einzusehen. Da jeder abgeschlossene Normalteiler Durchschnitt von offenen Normalteilern ist, kann man sich auf die letzteren beschränken. Ist aber $\mathfrak{H}$ ein offener Normalteiler von $\mathfrak{G}$ und α ein topologischer Automorphismus von $\mathfrak{G}$, so ist auch $\alpha(\mathfrak{H})$ ein offener Normalteiler. Die Fixkörper K und K' von $\mathfrak{H}$ und $\alpha(\mathfrak{H})$ sind daher endliche Normaloberkörper von $\underset{\sim}{Q}$, und es ist $G_K = \mathfrak{H}$, $G_{K'} = \alpha(\mathfrak{H})$. Wegen der Isomorphie $\mathfrak{H} \cong \alpha(\mathfrak{H})$ liefert der obige Satz die Gleichheit $K = K'$, so dass in der Tat $\mathfrak{H} = \alpha(\mathfrak{H})$ gilt.

Ein kurzer Bericht, der sich wie dieser eines so umfangreichen Gebietes annimmt, wird immer mit dem Mangel grosser Unvollständigkeit behaftet sein. Weit davon entfernt, alle relevanten Ergebnisse aufzählen zu können, muss er auch über die vielfältigen Aspekte schweigen, unter denen die angedeuteten Resultate und Problemstellungen gesehen werden können, und kann auf die mannigfachen wesentlichen Beziehungen zu anderen mathematischen Theorien kaum eingehen, deren Kenntnis für ein volles Verständnis der ganzen Thematik letzten Endes nötig wäre. Vielleicht aber vermag eine solche Übersicht von dem blühenden Leben der doch so alten Zahlentheorie zu zeugen und von der Fülle der unmittelbar fordernden Aufgaben, die sie immer noch stellt. Wie in kaum einem anderen Gebiet liegen die Geheimnisse der Zahlentheorie mit steinerner Festgelegtheit in ihrem Dunkel. Dass sie nicht alle umsonst der Entkleidung ihrer uralten Verborgenheit harren, zeigen die vielen, sich ständig vermehrenden schönen Ergebnisse, die jede Mühe reichlich belohnen.

LITERATUR

[1] ARTIN (E.). - Kennzeichnung des Körpers der reellen algebraischen Zahlen, Abh. math. Semin. Univ. Hamb., t. 3, 1924, p. 319-323.

[2] ARTIN (E.) and TATE (J.). - Class field theory. - New York, Amsterdam, W. A. Benjamin, 1968.

[3] BAUER (M.). - Zur Theorie der algebraischen Zahlkörper, Math. Annalen, t. 77, 1916, p. 353-356.

[4] BRUMER (A.). - Galois groups of extensions of number fields with given ramification, Mich. math. J., t. 13, 1966, p. 33-40.

[5] CASSELS (J. W. S.) and FRÖHLICH (A.) [Editors]. - Algebraic number theory, Proceedings of an instructional conference organized by the London mathematical Society [1965, Brighton]. - London and New York, Academic Press, 1967.

[6] DEMUŠKIN (S. P.). - Über die maximale p-Erweiterung eines lokalen Körpers [Russ.], Izv. Akad. Nauk SSSR, Mat. Ser., t. 25, 1961, p. 329-346.

[7] DEMUŠKIN (S. P.). - Über 2-Erweiterungen eines lokalen Körpers [Russ.], Sibirsk. mat. Ž., t. 4, 1963, p. 951-955.

[8] DOUADY (A.). - Détermination d'un groupe de Galois, C. R. Acad. Sc. Paris, t. 258, 1954, p. 5305-5308.

[9] GOLOD (E. S.) und ŠAFAREVIČ (I. R.). - Über Klassenkörpertürme [Russ.], Izv. Akad. Nauk SSSR, t. 28, 1964, p. 261-272.

[10] GEYER (W. D.). - Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist, J. Number Theory, t. 1, 1969, p. 346-374.

[11] GRUNWALD (W.). - Ein allgemeines Existenztheorem für algebraische Zahlkörper, J. für reine und angew. Math., t. 169, 1933, p. 103-107.

[12] HASSE (H.). - Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. für reine und angew. Math., t. 188, 1950, p. 40-64.

[13] HASSE (H.). - Existenz und Mannigfaltigkeit abelscher Algebren I, II, III, Math. Nachr., t. 1, 1948, p. 40-61, 213-217, 277-283.

[14] HILBERT (D.). - Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten, J. für reine und angew. Math, t. 110, 1892, p. 104-129.

[15] HOECHSMANN (K.). - Über die Gruppe der maximalen ℓ-Erweiterung eines globalen Körpers, J. für reine und angew. Math., t. 222, 1966, p. 142-147.

[16] HOECHSMANN (K.). - Zum Einbettungsproblem, J. für reine und angew. Math., t. 229, 1968, p. 81-106.

[17] IKEDA (M.). - Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem, Abh. math. Semin. Univ. Hamb., t. 24, 1960, p. 126-131.

[18] IWASAWA (K.). - On solvable extensions of algebraic number fields, Annals of Math., t.58, 1953, p. 548-572.

[19] IWASAWA (K.). - On the theory of cyclotomic fields, Annals of Math., t. 70, 1959, p. 530-561.

[20] IWASAWA (K.). - On Γ-extensions of algebraic number fields, Bull. Amer. math. Soc., t. 65, 1959, p. 183-226.

[21] IWASAWA (K.). - On some properties of Γ-finite modules, Annals of Math., t. 70, 1959, p. 291-312.

[22] IWASAWA (K.). - On Galois groups of local fields, Trans. Amer. math. Soc., t. 80, 1955, p. 448-469.

[23] JAKOVLEV (A. V.). - Die Galoissche Gruppe der algebraischen Abschliessung eines lokalen Körpers [Russ], Izv. Akad. Nauk SSSR, Ser. Mat., t. 32, 1968, p. 1283-1322.

[24] JARDEN (M.). - Algebraic extensions of finite corank of hilbertian fields (Erscheint demnächst).

[25] KAWADA (Y.). - On the structure of the Galois group of some infinite extensions, J. Fac. Sc. Univ. Tokyo, Section I, t. 7, 1954, p. 1-18.

[26] KOCH (H.). - Über galoissche Gruppen von p-adischen Zahlkörpern, Math. Nachr., t. 29, 1965, p. 77-111.

[27] KOCH (H). - Galoissche Theorie der p-Erweiterungen. - Berlin, VEB Deutscher Verlag der Wissenschaften, 1970 (Mathematische Monographien, 10).

[28] KRULL (W.) und NEUKIRCH (J.). - Die Struktur der absoluten Galoisgruppe über dem Körper $\underset{\sim}{R}(t)$, Math. Annalen, t. 193, 1971, p. 197-209.

[29] KUYK (W.). - Generic approach to the Galois embedding and extension problem, J. of Algebra, t. 9, 1968, p. 393-407.

[30] NEUKIRCH (J.). - Eine Klasse von Körpern, über denen jede Gleichung durch Radikale auflösbar ist, Abh. math. Semin. Hamb., t. 30, 1967, p. 26-35.

[31] NEUKIRCH (J.). - Klassenkörpertheorie. - Mannheim, Wien, Zürich, Bibliographisches Institut, 1969.

[32] NEUKIRCH (J.). - Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper, Invent. Math., t. 6, 1969, p. 296-314.

[33] NEUKIRCH (J.). - Freie Produkte pro-endlicher Gruppen und ihre Kohomologie, Arch. der Math., t. 22, 1971, p. 337-357.

[34] NEUKIRCH (J.). - Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen, J. für reine und angew. Math. (Erscheint demnächst).

[35] NEUKIRCH (J.) - Über das Einbettungsproblem der algebraischen Zahlentheorie (Erscheint demnächst).

[36] POITOU (G.). - Cohomologie galoisienne des modules finis. - Paris, Dunod, 1967 (Travaux et Recherches mathématiques, 13).

[37] REICHARDT (H.). - Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, J. für und angew. Math., t. 177, 1937, p. 1-5.

[38] ŠAFAREVIČ (I. R.). - On p-extensions, Math. Sbornik, t. 20 (62), 1947, p. 351-363 ; AMS Translations, Ser. 2, vol. 4, 1956, p. 59-72.

[39] ŠAFAREVIČ (I. R.). - On the construction of fields with a given Galois group of order ℓ , Izv. Akad. Nauk SSSR, Ser. Mat., t. 18, 1954, p. 327-334 ; AMS Translations, Ser. 2, vol. 4, 1956, p. 107-142.

[40] ŠAFAREVIČ (I. R.). - On the problem of imbedding fields, Izv. Akad. Nauk SSSR, Ser. Mat., t. 18, 1954, p. 389-418 ; AMS Translations, Ser. 2, vol. 4, 1956, p. 151-183.

[41] ŠAFAREVIČ (I. R.). - Construction of fields of algebraic numbers with given solvable Galois group, Izv. Akad. Nauk SSSR, Ser. Mat., t. 18, 1954, p. 525-578 ; AMS Translations, Ser. 2, vol. 4, 1956, p. 185-237.

[42] ŠAFAREVIČ (I. R.). - Algebraische Zahlkörper [Russ.], Proceedings of the international Congress of mathematicians [1962. Stockholm], p. 163-176 ; AMS Translations, Series 2, vol. 31, 1963, p. 25-39.

[43] SCHMIDT (F. K.). - Körper, über denen jede Gleichung durch Radikale auflösbar ist, Sitzber. Heidelb. Akad. Wiss., 1933, p. 37-47.

[44] SCHOLZ (A.). - Über die Bildung algebraischer Zahlkörper mit auflösbarer galoisscher Gruppe, Math. Z., t. 30, 1929, p. 332-356.

[45] SCHOLZ (A.). - Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung, Math. Z., t. 42, 1937, p. 161-188.

[46] SERRE (J.-P.). - Cohomologie galoisienne. - Berlin, Heidelberg, New York, Springer-Verlag, 1964 (Lecture Notes in Mathematics, 5).

[47] SERRE (J.-P.). - Abelian ℓ-adic representations and elliptic curves. - New York, Amsterdam, W. A. Benjamin, 1968.

[48] SERRE (J.-P.). - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., t. 15, 1972, p. 259-331.

[49] SHIMURA (G.). - A reciprocity law in non-solvable extensions, J. für reine und angew. Math., t. 221, 1966, p. 209-220.

[50] SWAN (R. G.). - Invariant rational functions and a problem of Steenrod, Invent. Math., t. 7, 1969, p. 148-158.

[51] TATE (J.). - Duality theorems in Galois cohomology over number fields, Proceedings of the international Congress of mathematicians [1962. Stockholm], p. 288-295. - Djursholm, Institut Mittag-Leffler, 1963.

[52] UCHIDA (K.). - Unramified extensions of quadratic number fields, II., Tôhoku math. J., Series 2, t. 22, 1970, p. 220-224.

[53] WANG (S.). - On Grunwald's theorem, Annals of Math., t. 51, 1950, p. 471-484.

(Texte reçu le 6 mars 1973)

Jürgen NEUKIRCH
Universität Regensburg
Fachbereich Mathematik
Universitätsstrasse 31
D-8400 REGENSBURG (Allemagne fédérale)