Astérisque

JÜRGEN NEUKIRCH

# Über die Absoluten Galoisgruppen Algebraischer Zahlkörper

*Astérisque*, tome 41-42 (1977), p. 67-79

<http://www.numdam.org/item?id=AST_1977__41-42__67_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.67-79

# ÜBER DIE ABSOLUTEN GALOISGRUPPEN ALGEBRAISCHER ZAHLKÖRPER

Jürgen NEUKIRCH (Regensburg)

Einleitung. Die vorliegenden Ausführungen betreffen die Ergebnisse einer früheren Arbeit (vgl. [6], [7]) die durch jüngste Resultate von Ikeda, Iwasawa und Uchida in ein neues Licht gerückt wurden. In jener Arbeit wurde gezeigt, daß zwei normale endlich-algebraische Zahlkörper $K_1$ und $K_2$ isomorph sind, wenn ihre absoluten Galoisgruppen $G_{K_1}$ und $G_{K_2}$ als abstrakte pro-endliche Gruppen isomorph sind. An diesen Satz knüpfte sich die Vermutung, daß die absolute Galoisgruppe $G_{\mathbb{Q}}$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen nur innere Automorphismen besitzt. Diese Vermutung gründete sich auf die Tatsache, daß sie sich über das sogenannte Einbettungsproblem auf eine rein gruppentheoretische Aufgabe zurückführen ließ (vgl. [7]). Diese Aufgabe wurde nach Vorarbeiten von Kanno [4] und Komatsu [5] von Uchida [13] in einer sogar weitergreifenden Weise gelöst, die zu dem folgenden Resultat führte:

Satz: Seien $K_1$ und $K_2$ zwei endliche algebraische Zahlkörper und $\sigma: G_{K_1} \to G_{K_2}$ ein topologischer Isomorphismus. Dann wird $\sigma$ durch einen inneren Automorphismus von $G_{\mathbb{Q}}$ induziert.

Gleichzeitig und unabhängig davon gelang auch Ikeda ein Beweis der oben erwähnten Vermutung, der allerdings auf sehr viel komplizierteren zahlentheoretischen Überlegungen beruhte (vgl. [2]). Dieser Beweis wurde von Iwasawa [3] stark vereinfacht, der i.w. die gleichen Resultate erhielt wie Uchida. Alle Beweise jedoch gründen sich auf den Anfangs erwähnten Satz über normale Zahlkörper mit isomorphen absoluten Galoisgruppen. In der vorliegenden Note sollen die auf mehrere Arbeiten verteilten Argumentationen zu einem vollständigen und in seinem zahlentheoretischem Teil vereinfachten Beweis des Satzes von Uchida und Iwasawa zusammengefaßt werden.

Wir betrachten im folgenden die (nicht notwendig endlichen) algebraischen Erweiterungen K des Körpers $\mathbb{Q}$ der rationalen Zahlen und unter diesen die henselschen Körper, d.h. die Körper, die eine im

algebraischen Abschluß unzerlegte nicht-archimedische Bewertung besitzen. Jeder solche Henselkörper K enthält einen kleinsten Henselkörper $K_o$. Dieser ist isomorph zum Körper $\mathbb{Q}_p^a$ aller algebraischen p-adischen Zahlen, wenn p die Restkörpercharakteristik von K ist. Wir nennen $n(K) = [K:K_o]$ den lokalen Grad von K.

Für jede Primzahl l definieren wir die l-Charakteristik der absoluten Galoisgruppe $G_K$ durch

$$\chi_l(G_K) = \sum_{q=0}^{2} (-1)^q \dim_{\mathbb{F}_l} H^q(G_K,\mathbb{F}_l) \text{ oder } \chi_l(G_K) = -\infty,$$

je nachdem $\dim H^1(G_K,\mathbb{F}_l)$ endlich oder unendlich ist. Mit $\mu_l$ bezeichnen wir die Gruppe der l-ten Einheitswurzeln und setzen $\mu_l(K) = \mu_l \cap K$.

Lemma 1: Sei K ein Henselkörper mit der Restkörpercharakteristik p. Geht die Primzahl l im lokalen Grad n(K) nur endlich oft auf, so ist

$$\chi_l(G_K) = 0 \text{ für } l \neq p, \quad \chi_l(G_K) = -n(K) \text{ für } l = p,$$

und $H^2(G_K,\mathbb{F}_l) \cong \mathbb{F}_l$ oder $= 0$, je nachdem $\mu_l(K) = \mu_l$ oder $= 1$. Geht l unendlich oft im Grad n(K) auf, so ist $H^2(G_K,\mathbb{F}_l) = 0$.

Beweis: Identifizieren wir den kleinsten in K enthaltenen Henselkörper $K_o$ mit $\mathbb{Q}_p^a$, und setzen wir $K' = K\cdot\mathbb{Q}_p$, so ist $G_K \cong G_{K'}$ und $n(K) = [K:\mathbb{Q}_p^a] = [K':\mathbb{Q}_p]$. Es genügt daher das Lemma für den Fall der algebraischen Erweiterungen K des Körpers $\mathbb{Q}_p$ der p-adischen Zahlen zu beweisen.

Wir stellen dazu K als Vereinigung $K = \bigcup_i K_i$ seiner endlichen Teilerweiterungen $K_i|\mathbb{Q}_p$ dar und erhalten

$$H^q(G_K,\mathbb{F}_l) = \varinjlim_i H^q(G_{K_i},\mathbb{F}_l).$$

Sei $l^\infty \nmid [K:\mathbb{Q}_p]$ und $i_o$ so gewählt, daß $l \nmid [K:K_{i_o}]$ und $\mu_l(K) = \mu_l(K_{i_o})$. Dann werden die Homomorphismen

$$(*) \qquad H^q(G_{K_i},\mathbb{F}_l) \xrightarrow{\text{Res}} H^q(G_{K_j},\mathbb{F}_l)$$

für $j \geq i \geq i_o$ injektiv. Mit Hilfe des Dualitätssatzes von Tate und Poitou erhalten wir

$$H^o(G_{K_i},\mathbb{F}_l) \cong \mathbb{F}_l,$$

$$H^1(G_{K_i},\mathbb{F}_l) \cong H^1(G_{K_i},\mu_l)\hat{} = (K_i^*/K_i^{*l})\hat{},$$

$$H^2(G_{K_i},\mathbb{F}_l) \cong H^o(G_{K_i},\mu_l)\hat{} = \mu_l(K_i)\hat{} = \mu_l(K)\hat{}$$

wobei $\hat{}$ das Pontrjagindual andeutet. Nun ist aber bekanntlich
$(K_i^*:K_i^{*l}) = l\cdot\#\mu_l(K)$ falls $l \nmid p$ und
$(K_i^*:K_i^{*l}) = l^{[K_i:\mathbb{Q}_p]+1}\cdot\#\mu_l(K)$ falls $l = p$.
Wegen der Injektivität der Homomorphismen (*) ergibt sich hieraus

$$\dim H^o(G_K,\mathbb{F}_l) = 1$$

$$\dim H^1(G_K,\mathbb{F}_l) = 1 + \dim \mu_l(K) \text{ für } l \nmid p$$

$$\dim H^1(G_K,\mathbb{F}_l) = [K:\mathbb{Q}_p]+1 + \dim \mu_l(K) \text{ für } l = p$$

$$\dim H^2(G_K,\mathbb{F}_l) = \dim \mu_l(K).$$

Hieraus ergibt sich das Lemma bis auf die letzte Aussage. Diese aber folgt aus der Tatsache, daß die Homomorphismen

$$(*) \qquad \text{Res}: H^2(G_{K_i},\mathbb{F}_l) \to H^2(G_{K_j},\mathbb{F}_l),\ j \geq i \geq i_o,$$

bei der Isomorphie $H^2(G_{K_i},\mathbb{F}_l) \cong \mu_l(K)\hat{}$ denjenigen Abbildungen $\text{Cor}\hat{}: \mu_l(K_i)\hat{} \to \mu_l(K_j)\hat{}$ entsprechen, die durch die Normenbildung $N_{K_j|K_i}: \mu_l(K_j) \to \mu_l(K_i)$, also wegen $\mu(K_j) \subseteq K_i$ durch die Zuordnung $\zeta \mapsto \zeta^{[K_j:K_i]}$ induziert werden. Daher ist (*) die Nullabbildung wann immer $l \mid [K_j:K_i]$, also im Fall $l^\infty \mid [K:\mathbb{Q}_p]$ zu oft, um etwas von $H^2(G_K,\mathbb{F}_l) = \varinjlim H^2(G_{K_i},\mathbb{F}_l)$ übrigzulassen.

Lemma 2: Sei $K|\mathbb{Q}$ ein (endlicher oder unendlicher) algebraischer Zahlkörper und $K_\wp$ seine Henselisierungen. [1] Dann ist der Homomorphismus

---

1) Hier sind ausnahmsweise die archimedischen "Henselisierungen" mit aufgenommen.

$$H^2(G_K,\mathbb{F}_1) \to \prod_{\mathfrak{p}} H^2(G_{K_\mathfrak{p}},\mathbb{F}_1)$$

injektiv, und der Homomorphismus

$$H^2(G_K,\mathbb{F}_1) \to \prod_{\mathfrak{p}\in S} H^2(G_{K_\mathfrak{p}},\mathbb{F}_1)$$

für jede endliche Primstellenmenge S von K surjektiv.

Beweis: Beide Aussagen ergeben sich durch einen unmittelbaren Aufstiegsprozeß aus dem Fall, daß K ein endlicher algebraischer Zahlkörper ist. Nehmen wir dies an, so ergibt sich die Injektivität der ersten Abbildung nach dem Dualitätssatz von Tate und Poitou aus der Injektivität der Abbildung $H^1(G_K,\mu_1) \to \prod_{\mathfrak{p}} H^1(G_{K_\mathfrak{p}},\mu_1)$, die ja nichts anderes als die Abbildung $K^*/K^{*1} \to \prod_{\mathfrak{p}} K_\mathfrak{p}^*/K_\mathfrak{p}^{*1}$ ist. Weiter liefert der Dualitätssatz die exakte Sequenz

$$H^2(G_K,\mathbb{F}_1) \xrightarrow{\rho} \coprod_{\mathfrak{p}} H^2(G_{K_\mathfrak{p}},\mathbb{F}_1) \to H^0(G_K,\mu_1)\hat{} \to 0.$$

Im Fall $H^0(G_K,\mu_1) = \mu_1(K) = 1$ ist sogar die ganze Abbildung $\rho$ surjektiv. Im Fall $\mu_1(K) = \mu_1$ ist für irgendeine nicht-archimedische Primstelle $\mathfrak{p}_0 \notin S$ der Homomorphismus $H^2(G_{K_{\mathfrak{p}_0}},\mathbb{F}_1) \cong H^0(G_{K_{\mathfrak{p}_0}},\mu_1)\hat{}$ $= \mu_1\hat{} \to H^0(G_K,\mu_1)\hat{} = \mu_1\hat{}$ bijektiv, so daß sich die Abbildung $H^2(G_K,\mathbb{F}_1) \to \coprod_{\mathfrak{p}\neq\mathfrak{p}_0} H^2(G_{K_\mathfrak{p}},\mathbb{F}_1)$ als surjektiv erweist.

Lemma 3: Ist K eine beliebige algebraische Erweiterung von $\mathbb{Q}$, so gilt

$$G_K \cong G_{\mathbb{Q}_p^a} \Rightarrow K \cong \mathbb{Q}_p^a.$$

Beweis: Wir zeigen zunächst, daß K ein Henselkörper ist. Sei dazu 1 eine von 2 und p verschiedene Primzahl und $K_2 = \mathbb{Q}_p^a(\mu_1)$. Durch die Isomorphie $G_K \cong G_{\mathbb{Q}_p^a}$ erhalten wir eine Isomorphie $G_{K_1} \cong G_{K_2}$, wobei $K_1|K$ eine endliche normale Erweiterung ist. Es genügt nun zu zeigen, daß $K_1$ henselsch ist. Ist nämlich $v_1$ eine henselsche Bewertung von $K_1$ und v die Einschränkung von $v_1$ auf K, so ergeben

sich die Fortsetzungen von v auf $K_1$ aus $v_1$ durch Automorphismen von $K_1$ und sind daher ebenso wie $v_1$ sämtlich henselsch. Da aber nach einem bekannten Satz von F.K. Schmidt (vgl. [9]) ein nicht-separabel abgeschlossener Körper höchstens eine henselsche Bewertung haben kann, ist $v_1$ die einzige Fortsetzung von v auf K. Daher ist mit $K_1$ auch K henselsch.

Für eine beliebige endliche Erweiterung $L_1$ von $K_1$ ergibt sich aus der Isomorphie $G_{K_1} \cong G_{K_2}$ eine Isomorphie $G_{L_1} \cong G_{L_2}$, wobei $L_2$ eine endliche Erweiterung von $K_1$ ist. Wegen Lemma 1 und wegen $\mu_1(L_2) = \mu_1$ haben wir daher für jedes solche $L_1$ (insbesondere für $L_1 = K_1$):

$$H^2(G_{L_1}, \mathbb{F}_1) \cong H^2(G_{L_2}, \mathbb{F}_1) \cong \mathbb{F}_1.$$

Wegen der Injektivität von

$$H^2(G_{K_1}, \mathbb{F}_1) \to \prod_{\mathfrak{p}} H^2(G_{K_{1\mathfrak{p}}}, \mathbb{F}_1)$$

ist weiter $H^2(G_{K_{1\mathfrak{p}}}, \mathbb{F}_1) \cong \mathbb{F}_1$ für mindestens eine Primstelle $\mathfrak{p}$ von $K_1$, die wegen $l \neq 2$ nicht-archimedisch sein muß. Wir zeigen jetzt, daß $K_1 = K_{1\mathfrak{p}}$, d.h. daß $K_1$ und damit K henselsch ist. Wäre dies nicht der Fall, so gäbe es eine endliche Erweiterung $L|K_1$, auf die die Primstelle $\mathfrak{p}$ zwei verschiedene Fortsetzungen $\mathfrak{p}_1$ und $\mathfrak{p}_2$ besitzt. Die Henselisierungen $L_{\mathfrak{p}_1}$ und $L_{\mathfrak{p}_2}$ von L sind endliche Erweiterungen der Henselisierung $K_{1\mathfrak{p}}$ von $K_1$. Wegen $H^2(G_{K_{1\mathfrak{p}}}, \mathbb{F}_1) \neq 0$ gilt nach Lemma 1 $l^\infty \nmid n(K_{1\mathfrak{p}})$, so daß auch $l^\infty \nmid n(L_{\mathfrak{p}_i})$ und somit - wiederum nach Lemma 1 - $H^2(G_{L_{\mathfrak{p}_i}}, \mathbb{F}_1) \cong \mathbb{F}_1$ ist, $i = 1,2$. Nun ist aber nach Lemma 2 der Homomorphismus

$$\mathbb{F}_1 \cong H^2(G_L, \mathbb{F}_1) \to H^2(G_{L_{\mathfrak{p}_1}}, \mathbb{F}_1) \times H^2(G_{L_{\mathfrak{p}_2}}, \mathbb{F}_1) \cong \mathbb{F}_1 \times \mathbb{F}_1$$

surjektiv. Wir erhalten also einen Widerspruch, d.h. $K_1$ ist henselsch, und damit auch K.

Wegen $H^2(G_{K_1}, \mathbb{F}_1) \cong H^2(G_{K_2}, \mathbb{F}_1) \neq 0$ muß nach Lemma 1 weiter $l^\infty \nmid n(K_1)$, also $l^\infty \nmid n(K)$ gelten. Ferner folgt aus

$$\chi_p(G_K) = \chi_p(G_{\mathbb{Q}_p^a}) = -n(\mathbb{Q}_p^a) = -1 ,$$

daß p die Restkörpercharakteristik von K ist, weil ja sonst nach Lemma 1 $\chi_p(G_K) = 0$ wäre. Dies liefert gleichzeitig

$$n(K) = -\chi_p(G_K) = -\chi_p(G_{\mathbb{Q}_p^a}) = 1 ,$$

also $K \cong \mathbb{Q}_p^a$ .

Lemma 4 : Sind $K_1$ und $K_2$ zwei endliche algebraische Zahlkörper und ist $K_1 | \mathbb{Q}$ normal, so gilt

$$G_{K_1} \cong G_{K_2} \Longrightarrow K_1 = K_2 .$$

Beweis : Mit $K_1$ ist auch $K_2$ normal. Zum Beweis sei p eine in $K_1.K_2$ unverzweigte Primzahl und $p = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ ihre Primzerlegung in $K_2$ . Wir nehmen an, daß $\mathfrak{p}_1$ vom Grad 1 ist, d.h. $K_{2\mathfrak{p}_i} \cong \mathbb{Q}_p^a$ . Sei $K_{1\mathfrak{p}_i} \supseteq K_1$ derjenige Körper, für den $G_{K_{1\mathfrak{p}_i}} \cong G_{K_{2\mathfrak{p}_i}}$ vermöge $G_{K_1} \cong G_{K_2}$ ist. Da $K_{2\mathfrak{p}_i}$ henselsch ist, ist aufgrund des Beweises zu Lemma 3 auch $K_{1\mathfrak{p}_i}$ henselsch. Wegen $G_{K_{1\mathfrak{p}_1}} \cong G_{\mathbb{Q}_p^a}$ ist sogar $\mathbb{Q}_p^a \cong K_{1\mathfrak{p}_1} \supseteq K_1$ . Dies bedeutet, dass p voll zerlegt ist im normalen Körper $K_1$ . Daher gilt $K_{1\mathfrak{p}_i} \supseteq k_{1i} \supseteq K_1$ mit $k_{1i} \cong \mathbb{Q}_p^a$ . Die Isomorphie $G_{K_1} \cong G_{K_2}$ liefert nun $K_{2\mathfrak{p}_i} \supseteq k_{2i} \supseteq K_2$ mit $G_{k_{2i}} \cong G_{k_{1i}} \cong G_{\mathbb{Q}_p^a}$, und aus Lemma 3 folgt $k_{2i} \cong \mathbb{Q}_p^a$ , so daß $K_{2\mathfrak{p}_i} = k_{2i} \cong \mathbb{Q}_p^a$ ist für alle $i = 1,\ldots,r$ . Dies zeigt daß die Primzahl p voll zerlegt ist in $K_2$ , wenn sie nur einen Linearfaktor abspaltet, was bekanntlich die Normalität von $K_2$ bedeutet (vgl. [1], Teil II, § 25). Für jede Primzahl p wählen wir jetzt eine zu p gehörige Zerlegungsgruppe $G_p \subseteq G_{\mathbb{Q}}$ der algebraisch abgeschlossenen Hülle $\bar{\mathbb{Q}}$ über $\mathbb{Q}$ aus. Die Menge $P(K_1) = \{p | G_p \subseteq G_{K_1}\}$ besteht dann aus allen in $K_1$ voll zerlegten Primzahlen. Sie besitzt die Dirichlet-Dichte $d(P(K_1)) = \frac{1}{[K_1:\mathbb{Q}]}$ (vgl. [1], Teil II, § 25, S. 139). Sei $L \supseteq K_1 \supseteq \mathbb{Q}$ eine weitere endliche normale Erweiterung von $\mathbb{Q}$ mit $G_p \subseteq G_L$ für alle $p \in P(K_1)$.

Dann ist $P(K_1) \subseteq P(L)$ , also

$$\frac{1}{[K_1:\mathbb{Q}]} = d(P(K_1)) \leq d(P(L)) = \frac{1}{[L:\mathbb{Q}]} ,$$

d.h. $[K_1:\mathbb{Q}] \geq [L:\mathbb{Q}]$ und daher $K_1 = L$ . Dies zeigt, daß $G_{K_1}$ durch die Gruppen $G_p$ , $p \in P(K_1)$ , und alle ihre Konjugierten in $G_{\mathbb{Q}}$ topologisch erzeugt wird.

Sei jetzt $\sigma : G_{K_1} \to G_{K_2}$ ein Isomorphismus und $G_p = G_{k_1}$ , $\sigma(G_p) = G_{k_2}$, wobei $k_1$ und $k_2$ algebraische Erweiterungen von $\mathbb{Q}$ sind. Da $k_1 \cong \mathbb{Q}_p^a$ und $G_{k_1} \cong G_{k_2}$ , gilt nach Lemma 3 $k_2 \cong \mathbb{Q}_p^a$ ; $k_1$ und $k_2$ sind also über $\mathbb{Q}$ konjugiert, so daß $G_p$ und $\sigma(G_p)$ in $G_{\mathbb{Q}}$ konjugiert sind. Es folgt, daß der Normalteiler $G_{K_2}$ von $G_{\mathbb{Q}}$ mit den $\sigma(G_p)$ auch die $G_p$ und alle ihre Konjugierten für alle $p \in P(K_1)$ enthält. Da $G_{K_1}$ durch diese Gruppen erzeugt wird, erhalten wir $G_{K_1} \subseteq G_{K_2}$ , und aus Symmetriegründen $G_{K_1} = G_{K_2}$ , also $K_1 = K_2$ .

Lemma 5 : Seien $N \supseteq \mathbb{Q}$ endliche algebraische Zahlkörper, $N|\mathbb{Q}$ normal und $N|K_1$ zyklisch. Dann gilt :

$$G_{K_1} \cong G_{K_2} \Longrightarrow K_1 \cong K_2 .$$

Beweis : Nach dem Tschebotareffschen Dichtigkeitssatz gibt es eine in $N$ unverzweigte Primzahl $p$ , so daß $K_1$ ein zu $p$ gehöriger Zerlegungskörper von $N|\mathbb{Q}$ ist. Mit anderen Worten : Es gibt eine zu $p$ gehörige Zerlegungsgruppe $G_p \subseteq G_{\mathbb{Q}}$ von $\bar{\mathbb{Q}}|\mathbb{Q}$ , die unter dem Homomorphismus $G_{\mathbb{Q}} \to G(N|\mathbb{Q})$ surjektiv auf $G(N|K_1)$ abgebildet wird. Ist nun $\sigma : G_{K_1} \to G_{K_2}$ ein Isomorphismus, so $\sigma(G_N) = G_{N'} \cong G_N$ d.h. $N = N'$ und somit $\sigma(G_N) = G_N$ nach Lemma 4. Daher induziert $\sigma$ einen Isomorphismus $\bar{\sigma} : G(N|K_1) \to G(N|K_2)$ . Unter der Projektion $G_{\mathbb{Q}} \to G(N|\mathbb{Q})$ wird $G_p$ surjektiv auf $G(N|K_1)$ und somit $\sigma(G_p)$ surjektiv auf $G(N|K_2)$ abgebildet. Wie schon im Beweis zu Lemma 4 dargelegt, folgt aber aus Lemma 3, daß $G_p$ und $\sigma(G_p)$ in $G_{\mathbb{Q}}$ konjugiert sind. Daher sind $G(N|K_1)$ und $G(N|K_2)$ in $G(N|\mathbb{Q})$ konjugiert, $K_1$

und $K_2$ also konjugiert über $\mathbb{Q}$ .

Lemma 6: Sei G eine endliche Gruppe der Ordnung n und $\varkappa$ ein Körper von n teilerfremder Charakteristik, der die n-ten Einheitswurzeln enthält. Dann wird der Gruppenring $\varkappa[G]$ als $\varkappa$-Vektorraum durch seine Idempotenten erzeugt.

Beweis: Da $\varkappa[G]$ durch die Unterräume $\varkappa[(g)]$ erzeugt wird, wenn (g) die zyklischen Untergruppen von G durchläuft, können wir annehmen, daß G zyklisch ist. Als halbeinfache Algebra hat $\varkappa[G]$ die Zerlegung

$$\varkappa[G] = \bigoplus_{i=1}^{r} \mathfrak{a}_i$$

wobei $\mathfrak{a}_i = \varkappa[G]\cdot\varepsilon_i$ minimale Linksideale und $\varepsilon_i$ Idempotente sind. Nun besitzt aber G als zyklische Gruppe nur 1-dimensionale irreduzible Darstellungen, so daß die G-Moduln $\mathfrak{a}_i$ 1-dimensional sind und somit

$$\varkappa[G] = \bigoplus_{i=1}^{r} \varkappa\cdot\varepsilon_i$$

ist.

Wir sind jetzt in der Lage, das folgende von Uchida und Iwasawa angegebene Theorem zu beweisen, wobei wir uns nach Uchida [13] richten.

Theorem: Seien $K_1$ und $K_2$ endliche algebraische Zahlkörper und $\sigma\colon G_{K_1} \to G_{K_2}$ ein topologischer Isomorphismus.

Dann wird $\sigma$ durch einen inneren Automorphismus von $G_{\mathbb{Q}}$ induziert.

Beweis: Sei $N|\mathbb{Q}$ eine beliebige endliche normale Erweiterung, die $K_1$ und $K_2$ enthält. Es ist dann $\sigma(G_N) = G_{N'}$ mit einem endlichen Normalkörper N'. Wegen $G_N \cong G_{N'}$ ergibt sich aus Lemma 4 $N = N'$, also $\sigma(G_N) = G_N$. $\sigma$ induziert somit einen Isomorphismus $\sigma_N\colon G(N|K_1) \to G(N|K_2)$. Es genügt nun zu zeigen, daß $\sigma_N$ für jedes N durch einen inneren Automorphismus von $G(N|\mathbb{Q})$ induziert wird. In der Tat, bedeutet $i_g$ für $g \in G(N|\mathbb{Q})$ den durch g gegebenen inneren Automorphismus, so stellen die endlichen Mengen

$$I_N = \{g \in G(N|\mathbb{Q}) \mid i_g|_{G(N|K_1)} = \sigma_N\}$$

bei laufendem N ein projektives System dar. Sind die $I_N$ nicht leer, so ist auch der Limes $I = \varprojlim_N I_N \subseteq G_{\mathbb{Q}}$ nicht leer, und der durch ein Element $g \in I$ gegebene innere Automorphismus $i_g$ von $G_{\mathbb{Q}}$ induziert den Isomorphismus $\sigma$.

Sei nun $G = G(N|\mathbb{Q})$, $G_1 = G(N|K_1)$ und $G_2 = G(N|K_2)$. Sei $n = \#G$ und p eine Primzahl $\equiv 1 \bmod n$, so daß der Körper $\mathbb{F}_p$ die n-ten Einheitswurzeln enthält. Wir betrachten dann den Gruppenring

$$A = \mathbb{F}_p[G] = \{\sum_{g \in G} a_g \, \bar{g} \mid a_g \in \mathbb{F}_p\},$$

wobei wir zur Unterscheidung die den Elementen $g \in G$ entsprechenden Elemente aus A mit $\bar{g}$ bezeichnen. Ferner betrachten wir die zerfallende Gruppenerweiterung

$$1 \to A \to E \to G \to 1,$$

wobei G auf A durch $\alpha^g = \bar{g} \cdot \alpha$ operiert. Dabei schreiben wir A im Gegensatz zu E und G additiv; insbesondere darf also das Element $\bar{1} \in A$ nicht mit dem Einselement 1 von E verwechselt werden. Nach einem Satz von Scholz (vgl. [11]) gibt es eine Körpererweiterung $M \supseteq N \supseteq \mathbb{Q}$, so daß $M|\mathbb{Q}$ die Gruppe E, und $M|N$ die Gruppe A als Galoisgruppe besitzt.

Wie wir oben gesehen haben, überführt der Isomorphismus $\sigma$ die Normalteiler $G_N$ und $G_M$ von $G_{\mathbb{Q}}$ in sich selbst und induziert daher einen Isomorphismus $\sigma_M: G(M|K_1) \to G(M|K_2)$ und einen Automorphismus

$$\sigma_M: A \to A$$

von $A = G(M|N)$. Diesen Automorphismus wollen wir explizit beschreiben. Seien $L_1$, $L_2$ die Fixkörper der Elemente $\bar{1}$, $\sigma_M(\bar{1}) \in A \subseteq E = G(M|\mathbb{Q})$. $\sigma$ induziert dann einen Isomorphismus $G_{L_1} \to G_{L_2}$. Nach Lemma 5 sind daher die Körper $L_1$ und $L_2$ konjugiert, so daß die zyklischen Gruppen $(\bar{1})$ und $(\sigma_M(\bar{1}))$ der Ordnung p in E konjugiert sind. Die zu $\bar{1}$ konjugierten Elemente sind aber gerade die Elemente $\bar{1}^g = \bar{g} \cdot \bar{1} = \bar{g}$, $g \in G$. Daher ist $\sigma_M(\bar{1}) = r \cdot \bar{g}_o$ mit einem $g_o \in G$ und einem $r \in \mathbb{F}_p$, $r \neq 0$. Wir behaupten nun, daß allgemein

(*) $$\sigma_M(\alpha) = r\cdot\overline{g}_o\cdot\alpha \text{ für alle } \alpha \in A$$

gilt. Dies braucht nur für die Idempotenten von A gezeigt zu werden, da A nach Lemma 6 von diesen erzeugt wird. Sei also $\varepsilon$ ein Idempotent. Da $A\cdot\varepsilon$ ein Normalteiler von $E = G(M|\mathfrak{Q})$ ist, wird $A\varepsilon$ aus dem gleichen Grund wie A durch $\sigma_M$ in sich überführt. Es ist also

$$\sigma_M(\varepsilon) = \beta\cdot\varepsilon$$

mit einem $\beta \in A$, und da mit $\varepsilon$ auch $\overline{1}-\varepsilon$ ein Idempotent ist, gilt auch

$$\sigma_M(\overline{1}-\varepsilon) = \gamma(\overline{1}-\varepsilon)$$

mit einem $\gamma \in A$. Wir erhalten also

$$\sigma_M(\overline{1}) = \sigma_M(\varepsilon) + \sigma_M(\overline{1}-\varepsilon) = \beta\varepsilon + \gamma(\overline{1}-\varepsilon)$$

und nach Multiplikation mit $\varepsilon$ von rechts

$$\sigma_M(\varepsilon) = \beta\varepsilon = \sigma_M(\overline{1})\cdot\varepsilon = r\cdot\overline{g}_o\cdot\varepsilon .$$

Wir bilden nun den Unterring $A_1 = \{\sum_{g\in G_1} a_g\,\overline{g} \mid a_g \in \mathbb{F}_p\}$ von A

und betrachten neben der Abbildung $\sigma_M\colon A_1 \to A$ die Abbildung

$$\sigma_N\colon A_1 \to A$$

mit $\sigma_N(\sum_{g\in G_1} a_g\,\overline{g}) = \sum_{g\in G_1} a_g\,\overline{\sigma_N(g)}$; insbesondere ist also

$\sigma_N(\overline{g}) = \overline{\sigma_N(g)}$ für $g \in G_1$. Zwischen $\sigma_M$ und $\sigma_N$ besteht die Beziehung

$$\sigma_M(\overline{g}) = \sigma_N(\overline{g})\cdot\sigma_M(\overline{1}), \text{ für } g \in G_1,$$

denn es ist ja

$$\sigma_M(\overline{g}) = \sigma_M(\overline{1}^g) = \sigma_M(\overline{1})^{\sigma_N(g)} = \overline{\sigma_N(g)}\cdot\sigma_M(\overline{1}) = \sigma_N(\overline{g})\cdot\sigma_M(\overline{1}).$$

Mit (*) erhalten wir also

$$r\cdot\overline{g}_o\cdot\overline{g} = r\cdot\sigma_N(\overline{g})\cdot\overline{g}_o,$$

d.h. $\sigma_N(\bar{g}) = \bar{g}_o\ \bar{g}\ \bar{g}_o^{-1}$ für alle $g \in G_1$ im Ring A und somit $\sigma_N(g) = g_o\ g\ g_o^{-1}$ in der Gruppe G. In der Tat wird also $\sigma_N$ durch einen inneren Automorphismus von G induziert.

Korollar 1: Sind $K_1$ und $K_2$ endliche algebraische Zahlkörper, so gilt

$$G_{K_1} \cong G_{K_2} \Longleftrightarrow K_1 \cong K_2.$$

In der Tat sind ja nach dem Theorem die Gruppen $G_{K_1}$ und $G_{K_2}$ unter der Voraussetzung $G_{K_1} \cong G_{K_2}$ in $G_{\mathbb{Q}}$ konjugiert, so daß auch die Körper $K_1$ und $K_2$ konjugiert sind.

Korollar 2: Für jeden endlichen algebraischen Zahlkörper K ist in kanonischer Weise

$$\mathrm{Aut}(G_K)/\mathrm{Inn}(G_K) \cong \mathrm{Aut}(K).$$

Dabei ist $\mathrm{Inn}(G_K)$ die Gruppe der inneren und $\mathrm{Aut}(G_K)$ die Gruppe aller topologischen Automorphismen von $G_K$.

Beweis: Für $g \in G_{\mathbb{Q}}$ bedeute $i_g$ den durch g gegebenen inneren Automorphismus. Genau dann ist $i_g(G_K) = G_K$, wenn g im Normalisator $N_{G_{\mathbb{Q}}}(G_K)$ von $G_K$ in $G_{\mathbb{Q}}$ liegt. Durch die Zuordnung $g \to i_g|_{G_K}$ erhalten wir einen Homomorphismus

$$N_{G_{\mathbb{Q}}}(G_K) \to \mathrm{Aut}(G_K),$$

bei dem $G_K$ auf $\mathrm{Inn}(G_K)$ abgebildet wird. Dieser Homomorphismus ist surjektiv nach dem Theorem. Er ist aber auch injektiv. Ist nämlich $i_g|_{G_K} = \mathrm{id}_{G_K}$, so ist $g\ h\ g^{-1} = h$ für alle $h \in G_K$. g liegt daher im Zentrum der durch $G_K$ und g erzeugten offenen Untergruppe von $G_{\mathbb{Q}}$. Nach einem Satz von F.K. Schmidt (vgl. [10]) ist aber das Zentrum einer offenen Untergruppe von $G_{\mathbb{Q}}$ trivial, d.h. $g = 1$. Wir erhalten somit

$$\mathrm{Aut}(G_K)/\mathrm{Inn}(G_K) \cong N_{G_{\mathbb{Q}}}(G_K)/G_K \cong \mathrm{Aut}(K).$$

Für einen galoisschen endlichen Zahlkörper K erhält man hiernach die Galoisgruppe von $K|\mathbb{Q}$ aus der Galoisgruppe von $\overline{\mathbb{Q}}|K$ durch die einfache Formel

$$\mathrm{Aut}(G_K)/\mathrm{Inn}(G_K) \cong G(K|\mathbb{Q}).$$

Korollar 3: Die Gruppe $G_{\mathbb{Q}}$ besitzt nur innere Automorphismen. Es ist sogar

$$\mathrm{Aut}(G_{\mathbb{Q}}) \cong G_{\mathbb{Q}}.$$

In der Tat ist $\mathrm{Aut}(G_{\mathbb{Q}}) = \mathrm{Inn}(G_{\mathbb{Q}}) \cong G_{\mathbb{Q}}$, ersteres wegen $\mathrm{Aut}(\mathbb{Q}) = 1$, letzteres wegen der Tatsache, daß das Zentrum von $G_{\mathbb{Q}}$ nach dem erwähnten Satz von F.K. Schmidt [10] trivial ist.

Bemerkung: Betrachten wir anstelle der absoluten Galoisgruppe $G_K$ eines Körpers K die Galoisgruppe $\tilde{G}_K$ der maximal auflösbaren Erweiterung $\tilde{K}|K$, oder allgemeiner - wie dies bei Iwasawa geschieht - durch die Galoisgruppe einer beliebigen Erweiterung $N|K$, die ihrerseits keine echte abelsche Erweiterung besitzt, so lassen sich alle Beweise fast wörtlich auf diesen Fall übertragen. In dem Theorem und seinen Korollaren kann man also $G_K$ durch $\tilde{G}_K$ ersetzen.

-:-:-:-

## Literatur


[1] Hasse, H.: Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Jahresber. der D. Math. Ver. 35 (1926), 36 (1930).

[2] Ikeda, M.: Completeness of the absolute Galois group of the rational number field. Unveröffentlicht.

[3] Iwasawa, K.: On the automorphisms of Galois groups. Erscheint demnächst.

[4] Kanno, T.: Automorphisms of the Galois group of the algebraic closure of the rational number field. Kodai Math. Sem. Rep. 25 (1973) S. 446-448

[5] Komatsu, K.: A remark of a Neukirch's conjecture. Proc. Akad. Japan 50 (1974), 253-255

[6] Neukirch, J.: Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. Inv. Math. 6 (1969), 296-314.

[7] Neukirch, J.: Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximalen auflösbaren Erweiterungen. J. reine angew. Math. 238 (1970), 135-147.

[8] Poitou, G.: Cohomologie Galoisiennes des Modules finis. Paris: Dunod 1967

[9] Schmidt, F.K.: Mehrfach perfekte Körper. Math. Annalen 108, (1933)

[10] Schmidt, F.K.: Körper, über denen jede Gleichung durch Radikale auflösbar ist. Sitzber. Heidelb. Akad. Wiss. 1933, S. 37-47.

[11] Scholz, A.: Über die Bildung algebraischer Zahlkörper mit auflösbarer galoisscher Gruppe. Math. Z. 30 (1929), S 332-356.

[12] Serre: Cohomologie Galoisienne. Lecture Notes in Math. 5, Berlin-Göttingen-Heidelberg: Springer 1964 ($4^{th}$-edition, 1973).

[13] Uchida, K.: Isomorphisms of Galois groups. Erscheint demnächst.

Jürgen NEUKIRCH
Universität Regensburg
Fachbereich Mathematik
D - 8400 REGENSBURG
Universitätsstr. 31
(Bundesrepublik Deutschland)