

On a characterization of algebraic number fields by their
Galois groups of p -closed Galois extensions

Yutaka SUEYOSHI (末吉 豊)

Department of Mathematics, Kyushu University

In this note, we give a characterization of finite algebraic number fields by the Galois groups of their p -closed Galois extensions. This characterization is a refinement of a theorem of K. Uchida [11]. For details, see [9].

We use the following notations throughout this note.

Notations. Let K be a field of characteristic 0 and let p be a prime number. For a normal extension L/K , $G(L/K)$ denotes its Galois group. In this note, a " p -extension" always means a normal p -extension. A "solvable" extension is a normal extension whose Galois group is a projective limit of finite solvable groups.

\bar{K} : the algebraic closure of K ,

\hat{K} : the solvable closure of K (i.e. the maximal solvable extension over K),

$K(p)$: the maximal p -extension over K ,

$G_K = G(\bar{K}/K)$: the absolute Galois group of K ,

$\hat{G}_K = G(\hat{K}/K)$, $G_K(p) = G(K(p)/K)$,

ζ_p : a primitive p -th root of unity in \bar{K} ,

P_0 : the set of all prime numbers.

§1. Introduction.

Let k_1 and k_2 be finite algebraic number fields. In 1969, J. Neukirch characterized finite normal algebraic number fields by their absolute Galois groups.

THEOREM A (Neukirch [5]). If k_1/\mathbb{Q} is normal and $G_{k_1} \cong G_{k_2}$, then $k_1 = k_2$.

And he conjectured [5]:

If $G_{k_1} \cong G_{k_2}$, then $k_1 \cong k_2$.

Furthermore, he proved a refinement of Theorem A.

THEOREM A' (Neukirch [6]). If k_1/\mathbb{Q} is normal and $\tilde{G}_{k_1} \cong \tilde{G}_{k_2}$, then $k_1 = k_2$.

Neukirch's conjecture was proved by Uchida [10], [11], in a generalized form.

THEOREM B (Uchida [11]). Let Ω_1/k_1 and Ω_2/k_2 be

solvably closed (i.e. Ω_1 and Ω_2 have no proper abelian extension) Galois extensions. If there exists a topological isomorphism $\sigma: G(\Omega_1/k_1) \xrightarrow{\sim} G(\Omega_2/k_2)$, then there exists a unique isomorphism of fields $g: \Omega_1 \xrightarrow{\sim} \Omega_2$ such that $\sigma(h) = ghg^{-1}$ for all $h \in G(\Omega_1/k_1)$. In particular, $g|_{k_1}$ gives an isomorphism of fields k_1 and k_2 .

In this note, we consider the following problem.

PROBLEM. In Theorem B, can we replace Ω_1/k_1 and Ω_2/k_2 with some smaller extensions?

We give an answer to this problem by using p -closed extensions.

To prove Theorems A and A', Neukirch used a characterization of algebraic number fields with henselian valuations [5], [6]. So, first, we generalize his characterization in §2, and next, we apply it to finite algebraic number fields in §3.

§2. \tilde{p} -closed extensions and Ω -henselian fields.

Let Ω be a field of characteristic 0, p be a prime number and P be a subset of P_0 .

DEFINITION. We call Ω \tilde{p} -closed if and only if Ω is

p -closed (i.e. Ω has no proper p -extension) and Ω contains ζ_p . We call Ω \tilde{P} -closed if and only if Ω is \tilde{p} -closed for all $p \in P$.

REMARK 1. Ω is solvably closed if and only if Ω is \tilde{P}_0 -closed.

REMARK 2. Let K be a field of characteristic 0 and let P be a subset of P_0 . We put $K(\tilde{P}) = \bigcup_{i=0}^{\infty} K_i$, where

$$\begin{cases} K_0 = \prod_{p \in P} K(\zeta_p): \text{ the composite field of } K(\zeta_p), p \in P, \\ K_{i+1} = \prod_{p \in P} K_i(p): \text{ the composite field of } K_i(p), p \in P \\ \quad (i = 0, 1, 2, \dots). \end{cases}$$

Then, $K(\tilde{P})$ is the minimal \tilde{P} -closed Galois extension over K . If k is a finite algebraic number field and $P \subsetneq P_0$, then $k(\tilde{P}) \subsetneq \tilde{k}$.

Now, let K be an algebraic number field (not necessarily finite over \mathbb{Q}) and $v|\ell$ be a valuation of K induced from a fixed embedding $K \hookrightarrow \overline{\mathbb{Q}}_\ell$, where ℓ is either a prime number or ∞ and \mathbb{Q}_∞ denotes \mathbb{R} . We put $K_v = K \cdot \mathbb{Q}_\ell$. Let Ω/K be an algebraic extension.

DEFINITION. We call K Ω -henselian with respect to v if and only if there exists only one extension \tilde{v} of v to Ω

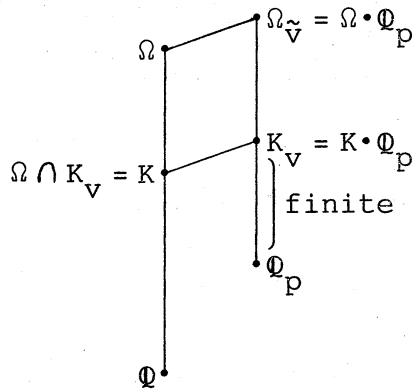
(i.e. for any extension $\Omega \hookrightarrow \overline{\mathbb{Q}}_\ell$ of the embedding $K \hookrightarrow \overline{\mathbb{Q}}_\ell$, we have $\Omega \cap K_v = K$). If K is $\overline{\mathbb{Q}}$ -henselian with respect to v , then K is simply called henselian with respect to v .

In the case of \tilde{p} -closed Galois extensions, we can characterize algebraic number fields which are Ω -henselian with respect to non-archimedean valuations, by their Galois groups.

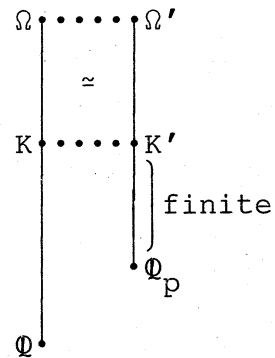
THEOREM 1. Let p be a prime number and let Ω/K be a \tilde{p} -closed (i.e. Ω is \tilde{p} -closed) Galois extension of algebraic number fields. Then the following two conditions are equivalent.

- (i) There exists a non-archimedean valuation $v|p$ of K such that K is Ω -henselian with respect to v and $[K_v:\mathbb{Q}_p] < \infty$.
- (ii) There exist a finite extension K'/\mathbb{Q}_p and a \tilde{p} -closed Galois extension Ω'/K' such that $G(\Omega/K) \simeq G(\Omega'/K')$.

Furthermore, v (in (i)) obtained from the condition (ii) is unique and $[K_v:\mathbb{Q}_p] = [K':\mathbb{Q}_p]$ holds.



(i)



(ii)

REMARK 3. In the following three cases, Theorem 1 has been proved.

Case 1. $\Omega = \bar{\mathbb{Q}}$ and $\Omega' = \bar{\mathbb{Q}}_p$: by Neukirch [5].

Case 2. $\Omega = \hat{K}$ and $\Omega' = \hat{K}' (= \bar{\mathbb{Q}}_p)$: by Neukirch [6].

Case 3. $\zeta_p \in K$ and $\Omega = K(p)$ (hence $\zeta_p \in K'$ and $\Omega' = K'(p)$): by Y. Hironaka-Kobayashi [3].

REMARK 4. Case 1 (in Remark 3) of Theorem 1 is a p -adic analogue of a theorem of E. Artin [1]:

If $K (\neq \bar{\mathbb{Q}})$ is an algebraic number field and $[\bar{\mathbb{Q}}:K]$ is finite, then K is henselian with respect to a unique archimedean valuation of K and $\bar{\mathbb{Q}} = K(\sqrt{-1})$, $[\bar{\mathbb{Q}}:K] = 2$.

We can generalize Artin's theorem as follows:

Let p be a prime number and Ω/K ($\Omega \neq K$) be a p -closed finite p -extension of algebraic number fields. Then $p = 2$ and K is Ω -henselian with respect to a unique archimedean valuation of K , and $\Omega = K(\sqrt{-1})$, $[\Omega:K] = 2$.

§3. A characterization of finite algebraic number fields.

For a finite algebraic number field k and a prime number p , we put $S_p(k) = \{\mathfrak{f} \mid \text{a prime ideal of } k \text{ above } (p)\}$. For $\mathfrak{f} \in S_p(k)$, we use the following notations.

$k_{\mathfrak{f}}$: the completion of k with respect to \mathfrak{f} ,

$e(\mathfrak{f}/p)$: the ramification index of $k_{\mathfrak{f}}/\mathbb{Q}_p$,

$f(\mathfrak{f}/p)$: the relative degree of $k_{\mathfrak{f}}/\mathbb{Q}_p$.

Then, from Theorem 1, we obtain the following

COROLLARY. Let p be a prime number, k_1 and k_2 be finite algebraic number fields, and Ω_1/k_1 and Ω_2/k_2 be \tilde{p} -closed Galois extensions. If $G(\Omega_1/k_1) \cong G(\Omega_2/k_2)$, then there exists a bijection $\phi_p: S_p(k_1) \rightarrow S_p(k_2)$ such that $[k_{\mathfrak{f}}:\mathbb{Q}_p] = [k_{\phi_p(\mathfrak{f})}:\mathbb{Q}_p]$ for all $\mathfrak{f} \in S_p(k_1)$.

PROOF. Using Theorem 1, we can define ϕ_p by the 1-1 correspondence of the decomposition subgroups of the prime ideals above (p) of k_1 and k_2 .

Let $A = (r; f_1, \dots, f_r)$ be a tuple of natural numbers such that $f_1 \leq \dots \leq f_r$. For such A and a finite algebraic number field k , we put

$$P_A(k) = \left\{ p \in P_0 \mid \begin{array}{l} (p) = \mathfrak{f}_1^{e(\mathfrak{f}_1/p)} \cdots \mathfrak{f}_r^{e(\mathfrak{f}_r/p)} \text{ in } k, \\ f(\mathfrak{f}_i/p) = f_i \quad (1 \leq i \leq r). \end{array} \right\}$$

For $P \subset P_0$, we put

$$\delta(P) = \lim_{s \rightarrow 1+0} \left(\sum_{p \in P} \frac{1}{p^s} \right) / \log \frac{1}{s-1} \quad (\text{if it exists}), \quad 0 \leq \delta(P) \leq 1$$

($\delta(P)$ is called the Dirichlet density of P).

For two subsets $P_1, P_2 \subset P_0$, we write

$$P_1 \doteq P_2 \quad \text{if and only if} \quad \#((P_1 \cup P_2) - (P_1 \cap P_2)) < \infty,$$

$$P_1 \underset{\delta}{=} P_2 \quad \text{if and only if} \quad \delta((P_1 \cup P_2) - (P_1 \cap P_2)) = 0.$$

DEFINITION. Let k_1 and k_2 be finite algebraic number

fields. Then k_1 and k_2 are called arithmetically equivalent over \mathbb{Q} if and only if $P_A(k_1) \doteq P_A(k_2)$ for all $A = (r; f_1, \dots, f_r)$ (This is equivalent to $P_A(k_1) \underset{\delta}{=} P_A(k_2)$ for all $A = (r; f_1, \dots, f_r)$). For arithmetically equivalent fields, see e.g. [2], [4], [7]).

THEOREM 2. Let P be a subset of P_0 such that $\delta(P) = 1$. Let k_1 and k_2 be finite algebraic number fields and let Ω_1/k_1 and Ω_2/k_2 be $\overset{\circ}{P}$ -closed Galois extensions. If there exists a topological isomorphism $\sigma: G(\Omega_1/k_1) \xrightarrow{\sim} G(\Omega_2/k_2)$, then there exists a unique isomorphism of fields $g: \Omega_1 \xrightarrow{\sim} \Omega_2$ such that $\sigma(h) = ghg^{-1}$ for all $h \in G(\Omega_1/k_1)$. In particular, $g|_{k_1}$ gives an isomorphism of fields k_1 and k_2 .

PROOF. From Corollary, it follows easily that k_1 and k_2 are arithmetically equivalent over \mathbb{Q} . Let k'_1 be an intermediate field of Ω_1/k_1 such that k'_1/k_1 is finite, and let k'_2 be the corresponding subfield of Ω_2 by σ , then k'_1 and k'_2 are also arithmetically equivalent over \mathbb{Q} . Using this, we can prove Theorem 2 by slightly modifying the proof of Theorem B.

REMARK 5. In Theorem 2, the conclusion $k_1 \simeq k_2$ (over \mathbb{Q}) cannot be strengthened to $k_1 \simeq k_2$ over $k_1 \cap k_2$.

Example. Put $k_1 = \mathbb{Q}(\sqrt[3]{2})$ and $k_2 = \mathbb{Q}(\sqrt[3]{2} \cdot \sqrt{-1})$. Then, $k_1 \cap k_2 = \mathbb{Q}(\sqrt{2})$. Since $k_1 \simeq k_2$ (over \mathbb{Q}), $G_{k_1} \simeq G_{k_2}$. But, for any isomorphism $g: k_1 \xrightarrow{\sim} k_2$, we have

$g(\sqrt{2}) = -\sqrt{2}$. Hence, g cannot be an isomorphism over $k_1 \cap k_2$.

§4. An outline of the proof of Theorem 1.

Using Krasner's lemma, we can prove the following two lemmas.

LEMMA 1. Let p be a prime number, Ω be a \tilde{p} -closed algebraic number field and v be a non-archimedean valuation of Ω . Then Ω_v is also \tilde{p} -closed.

LEMMA 2. Let p be a prime number and Ω/K be a \tilde{p} -closed Galois extension of algebraic number fields. If $p \mid [\Omega:K]$, then K is Ω -henselian with respect to at most one non-archimedean valuation.

We use the following propositions from Galois cohomology (See [5], [6], [8]).

PROPOSITION 1. Let ℓ, p be prime numbers and K/\mathbb{Q}_ℓ be an algebraic extension.

(1) If $p^\infty \nmid [K:\mathbb{Q}_\ell]$ and $\zeta_p \notin K$, then

$G_K(p)$ is a free pro- p -group of rank $\begin{cases} 1 & (\ell \neq p), \\ [K:\mathbb{Q}_p] + 1 & (\ell = p) \end{cases}$

(Here, if $[K:\mathbb{Q}_p] = \infty$, then $[K:\mathbb{Q}_p] + 1$ means \aleph_0 .),

and $cd_p(G_K(p)) = 1$.

(2) If $p^\infty \nmid [K:\mathbb{Q}_\ell]$ and $\zeta_p \in K$, then

$$\left\{ \begin{array}{l} \text{generator-rank } (G_K(p)) = \begin{cases} 2 & (\ell \neq p), \\ [K:\mathbb{Q}_p] + 2 & (\ell = p) \end{cases} \\ \text{(Here, if } [K:\mathbb{Q}_p] = \infty, \text{ then } [K:\mathbb{Q}_p] + 2 \text{ means } \aleph_0 \text{.)} \\ \text{relation-rank } (G_K(p)) = 1, \end{array} \right.$$

and $cd_p(G_K(p)) = 2$.

(3) If $p^\infty \mid [K:\mathbb{Q}_\ell]$, then $G_K(p)$ is a free pro- p -group and $cd_p(G_K(p)) \leq 1$.

PROPOSITION 2. Let K be an algebraic number field, then

the canonical homomorphism $B_K \xrightarrow{(\text{Res}_v)} \prod_v B_{K_v}$ is injective.

Here, B_K and B_{K_v} denote the Brauer groups of K and K_v ,

respectively, and v runs over all valuations of K .

An outline of the proof of Theorem 1. First, we assume (i).

Let \tilde{v} be the unique extension of v to Ω . We put $K' = K_{\tilde{v}}$ and $\Omega' = \Omega_{\tilde{v}}$. Then Ω' is \tilde{p} -closed by Lemma 1, and $[K':\mathbb{Q}_p]$ is finite by the assumption. Since $\Omega \cap K_v = K$ by the assumption, we have $G(\Omega/K) \cong G(\Omega'/K')$. Next, we assume (ii). Let $G(\Omega/L)$ be a p -Sylow subgroup of $G(\Omega/K)$ and $G(\Omega'/L')$ be the corresponding p -Sylow subgroup of $G(\Omega'/K')$ by the isomorphism. Then $\Omega = L(p)$, $\zeta_p \in \Omega$, $\Omega' = L'(p)$, $\zeta_p \in L'$ and $p^\infty \nmid [L':\mathbb{Q}_p]$. By Proposition 1, we have $cd_p(G_{L'}(p)) = 2$, therefore $cd_p(G_L(p)) = 2$

and $B_L(p) \neq 0$. Then, by Proposition 2, there exists a non-archimedean valuation w of L (say $w|\ell$) such that $B_{L_w}(p) \neq 0$

i.e. $p^\infty \nmid [L_w:\mathbb{Q}_\ell]$. Let \bar{w} be an extension of w to Ω and put $v = w|_K$, then we can prove the following:

$$\left\{ \begin{array}{l} p = \ell \text{ (by Proposition 1),} \\ \bar{w} \text{ is the unique extension of } v \text{ to } \Omega, \\ v \text{ is unique (by Lemma 2),} \\ [K_v:\mathbb{Q}_p] = [K':\mathbb{Q}_p] < \infty \text{ (by Proposition 1).} \end{array} \right.$$

This is an outline of the proof of Theorem 1.

References

- [1] E. Artin, Kennzeichnung des Körpers der reellen algebraischen Zahlen, Hamb. Abh., 3(1924), 319-323.
- [2] F. Gassmann, Bemerkungen zur vorstehenden Arbeit von Hurwitz, Math. Z., 25(1926), 665-675.
- [3] Y. Hironaka-Kobayashi, On the Galois groups of the maximal p -extensions of algebraic number fields, Natur. Sci. Rep. Ochanomizu Univ., 27(1976), 99-105.
- [4] N. Klingens, Zahlkörper mit gleicher Primzahlegung, J. Reine Angew. Math., 299/300(1978), 342-384.
- [5] J. Neukirch, Kennzeichnungen der p -adischen und der endlichen algebraischen Zahlkörper, Invent. Math., 6(1969), 296-314.
- [6] J. Neukirch, Kennzeichnung der endlich-algebraischen Zahl-

körper durch die Galoisgruppe der maximal auflösbaren
Erweiterungen, J. Reine Angew. Math., 238(1969), 135-147.

- [7] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory, 9(1977), 342-360.
- [8] J.-P. Serre, Cohomologie Galoisienne, Springer, Berlin-Heidelberg-New York, 1964.
- [9] Y. Sueyoshi, A characterization of number fields by p -closed extensions, in preparation.
- [10] K. Uchida, Isomorphisms of Galois groups, J. Math. Soc. Japan, 28(1976), 617-620.
- [11] K. Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions, Tôhoku Math. J., 31(1979), 359-362.