Natural Science Report, Ochanomizu University, Vol. 27, No. 2, 1976 99
お茶の水女子大学 自然科学報告 第27巻 第2号

On the Galois groups of the Maximal p-extensions of Algebraic Number Fields

Yumiko Hironaka-Kobayashi

Department of Mathematics, Faculty of Science
Ochanomizu University

(Received September 9, 1976)

§ 0. Introduction.

Let $K(p)$ be the maximal p-extension of an algebraic number field K, where p is a rational prime. We call an algebraic number field p-*Henselian* if it has a valuation which does not split in its maximal p-extension. It is known that the center of the absolute Galois group of a finite algebraic number field is trivial. In § 1 we shall prove that the center of the Galois group $Gal(K(p)/K)$ is trivial if K is a finite algebraic extension over the rational number field $\boldsymbol{Q}$ containing a primitive p-th root of unity. In the proof the decomposition groups play an important role. In § 2 we assume that K is an algebraic extension over $\boldsymbol{Q}$ containing a primitive p-th root of unity and that K is totally imaginary if $p=2$. We shall give a necessary and sufficient condition, in terms of $Gal(K(p)/K)$, for K to be p-Henselian with respect to a discrete valuation over p which has a finite residue class field. Using this we shall derive a number theoretical result, which is the purpose of § 2: when K is a finite algebraic extension of $\boldsymbol{Q}$, $Gal(K(p)/K)$ determines the degree of K over $\boldsymbol{Q}$, the number of prime ideals of K over the ideal (p), $e(\mathfrak{p})f(\mathfrak{p})$, where $e(\mathfrak{p})$ denotes the ramification index and $f(\mathfrak{p})$ denotes the degree of inertia of a prime ideal $\mathfrak{p}$ of K over (p), and the maximal integer m for which K contains a primitive p^m-th root of unity.

§ 1. The center of $Gal(K(p)/K)$.

In this paper we denote by p a rational prime. Let k be a field. We say that an extension K of k is *a finite p-extension* if it is a Galois extension and its Galois group is a finite p-group. We donote by $k(p)$ the composite field of all the finite p-extensions of k in a fixed algebraic closure of k, and call it *the maximal p-extension of k*.

Let K be an algebraic extension of $\boldsymbol{Q}$ and v be a valuation of K. K_v denotes the composite field of K_{iv_i} in a fixed algebraic closure of $\boldsymbol{Q}_{v_0}$, where K_i runs all the subfields of K which are of finite degree over $\boldsymbol{Q}$, v_0 (resp. v_i) is the restriction of v to $\boldsymbol{Q}$ (resp. K_i), and $\boldsymbol{Q}_{v_0}$ (resp. K_{iv_i}) is the completion of $\boldsymbol{Q}$ (resp. K_i) with respect to v_0 (resp. v_i). We note

that if K is a finite extension of $\boldsymbol{Q}$, K_v is the ordinary completion of K with respect to v.

LEMMA 1. *Let K be a finite p-extension of k and L be a finite p-extension of K. Then the normal closure of L over k is a finite p-extension of k.*

PROOF. Clear.

PROPOSITION 2. *Let K be an intermediate field of k and $k(p)$. Then $K(p)=k(p)$.*

PROOF. Since clearly $K(p)\supseteq k(p)$, we have only to show the converse. For any finite p-extension K' of K, there exists an element x in K' such that $K'=K(x)$. We can assume that $K=\bigcup_{i=1}^{\infty}K_i$, K_i/k is a finite p-extension and $K_i\subseteq K_{i+1}$. For sufficiently large m, the irreducible polynomial $\mathrm{Irr}(x, K, X)\in K_m[X]$ and every K-conjugate of x is contained in $K_m(x)$. Since $K_m(x)/K_m$ is a finite p-extension, the assertion follows from Lemma 1.

PROPOSITION 3. *Let K be an algebraic extension of $\boldsymbol{Q}$ containing a primitive p-th root ζ of unity. Assume that K has no proper p-extension of itself. Then for any non-archimedian valuation v of K, K_v has no proper p-extension of itself.*

PROOF. Assume that $Gal(K_v(p)/K_v)\neq\{1\}$. Then there exists a cyclic extension L of K_v of degree p. Since K_v contains ζ, $L=K_v(\sqrt[p]{a})$ for some a in K_v. As K is dense in K_v, $a=v-\lim a_i$, $a_i\in K$, and the polynomial X^p-a can be arbitrary approximated by X^p-a_i. Therefore for sufficiently large i, $L=K_v(\sqrt[p]{a_i})$. But by the assumption $K(\sqrt[p]{a_i})=K$, hence $\sqrt[p]{a_i}\in K\subseteq K_v$. We have a contradiction.

PROPOSITION 4. *Let K be an algebraic extension of $\boldsymbol{Q}$ containing a primitive p-th root ζ of unity. Assume that K has a proper p-extension of itself. Then K has at most one valuation up to equivalence which does not split in $K(p)$.*

PROOF. Assume that there exist two such valuations v_1 and v_2. We show first that $(K^*)^p=(K_{v_i}{}^*)^p\cap K^*$, $i=1, 2$; where K^* denotes the multiplicative group of K. If there is an element a in $(K_{v_i}{}^*)^p\cap K^*$ and not in $(K^*)^p$, the polynominal X^p-a is irreducible over K. Since K contains ζ, $K(\sqrt[p]{a})$ is contained in $K(p)$. As v_i does not split in $K(\sqrt[p]{a})$, $[K(\sqrt[p]{a})_{V_i}: K_{v_i}]=p$, where V_i is the valuation of $K(\sqrt[p]{a})$ over v_i, $i=1, 2$. This is a contradiction, for $a\in(K_{v_i}{}^*)^p\cap K^*$.

Next we show that $K^*=(K^*)^p$. For any element a of K^*, take an arbitary neighbourhood U of a in $K_{v_1}{}^*$. For any element b of $(K^*)^p$ take a neighbourhood W of b in $K_{v_2}{}^*$ which is contained in $(K_{v_2}{}^*)^p$. By the approximation theorem, there exists an element c of K^* contained both in U and in W. Then $c\in W\cap K^*\subseteqq(K_{v_2}{}^*)^p\cap K^*=(K^*)^p\subseteqq(K_{v_1}{}^*)^p$. Therefore a is in the closure of $(K_{v_1}{}^*)^p$ which is a closed subgroup of $K_{v_1}{}^*$, hence $a\in(K_{v_1}{}^*)^p\cap K^*=(K^*)^p$. On the other hand K has a Galois extension L of K of degree p. Then $L=K(\sqrt[p]{a})$ with some a in K. Thus we have a contradiction.

DEFINITION. An algebraic number field K is called *p-Henselian* if K has a valuation which does not split in $K(p)$.

We denote $G_k(p)=Gal(k(p)/k)$. We remark here that $G_k(p)$ is the maximal quotient of $G_k=Gal(\bar{k}/k)$ which is a pro-p-group, where $\bar{k}$ denotes an algebraic closure of k.

THEOREM 5. *Let K be a finite algebraic extension of $\boldsymbol{Q}$ containing a primitive p-th root of unity. Then the center of $G_K(p)$ is trivial.*

From here to the end of the proof of this theorem we assume that K satisfies the assumption of Theorem 5.

LEMMA 6. *Let V be a non-archimedian valuation of $K(p)$. Then $N(D(V))=D(V)$, where $D(V)$ is the decomposition group of V in $G_K(p)$ and $N(D(V))$ is the normalizer of $D(V)$ in $G_K(p)$.*

PROOF. It is sufficient to show that $D(V)$ contains $N(D(V))$. Now, $N(D(V))=\{\sigma\in G_K(p):\sigma D(V)\sigma^{-1}=D(V)\}=\{\sigma\in G_K(p):D(V^\sigma)=D(V)\}$, where V^σ is the valuation of $K(p)$ such that $V^\sigma(x)=V(x^\sigma)$ for any element x in $K(p)$. Let L be the intermediate field of $K(p)/K$ such that $G_L(p)=D(V)$, and v be the restriction of V to K. Then by Proposition 3,

$$G_L(p)\cong Gal(K(p)_V/K_v)\cong Gal(K_v(p)/K_v)\,.$$

It is clear that $L\neq L(p)$, for K is a finite extension of $\boldsymbol{Q}$. For any σ in $N(D(V))$, L is p-Henselian with respect to the restrictions of both V and V^σ to L. Hence $V=V^\sigma$ by Proposition 4.

LEMMA 7. *Let V_1 and V_2 be non-equivalent non-archimedian valuations of $K(p)$. Then $D(V_1)\cap D(V_2)=\{1\}$.*

PROOF. For $i=1, 2$, let L_i be the intermediate field of $K(p)/K$ such that $G_{L_i}(p)=D(V_i)$ respectively. L denotes the composite field of L_1 and L_2. Then L is p-Henselian with respect to the restrictions of both V_1 and V_2 to L, hence $L=K(p)$ by Proposition 4.

PROOF OF THEOREM 5. Take any non-equivalent non-archimedian valuations V_1 and V_2 of $K(p)$. For any σ in the center of $G_K(p)$, $\sigma \in N(D(V_i))$, $i=1, 2$. Hence it follows from Lemma 6 and 7 that $\sigma=1$.

q. e. d.

§ 2. p-Henselian fields and the decomposition of (p).

In relation to Proposition 4, we naturally have a question: under what condition is K p-Henselian? The next proposition gives a partial answer.

THEOREM 8. *Let L be an algebraic extension of $\boldsymbol{Q}$ containing a primitive p-th root of unity. If $p=2$, assume further that L is totally imaginary. Then the following conditions are equivalent.*

1) *L is p-Henselian with respect to a discrete valuation v over p which has a finite residue class field.*

2) *$Gal(L(p)/L) \cong Gal(K(p)/K)$, where K is a finite algebraic extension of $\boldsymbol{Q}_p$ containing a primitive p-th root of unity.*

First we state several results to which we refer in the proof. (Lemma 9$\sim$12)

LEMMA 9 (cf. [4]-§ 2). *Let K be an algebraic extension of $\boldsymbol{Q}_l$ containing a primitive p-th root of unity and $p^\infty \nmid [K: \boldsymbol{Q}_l]$ i.e. $[K: \boldsymbol{Q}_l]$ being devided by p only finite times. Then $G_K(p)$ is a Demuškin group of rank 2 (resp. $[K: \boldsymbol{Q}_l]+2$) if $l \neq p$ (resp. $l=p$), and the cohomological dimension of $G_K(p)$ is 2. In case $[K: \boldsymbol{Q}_l]=\infty$, rank $[K: \boldsymbol{Q}_l]+2$ means rank $\aleph_0$.*

LEMMA 10 (cf. [5]-§ 1). *Let K be an algebraic extension of $\boldsymbol{Q}_l$. Then the p-cohomological dimension $\mathrm{cd}_p(G_K)$ is 0, 1 or 2. More precisely,*

$\mathrm{cd}_p(G_K)=0 \iff p \nmid [\overline{K}: K]$

$\mathrm{cd}_p(G_K)=1 \iff p \mid [\overline{K}: K]$ *and* $p^\infty \mid [K: \boldsymbol{Q}_l]$

$\mathrm{cd}_p(G_K)=2 \iff p^\infty \nmid [K: \boldsymbol{Q}_l] \iff B_K(p) \neq 0$,

where B_K is the Brauer group of K and $B_K(p)$ is its p-component.

LEMMA 11 (cf. [5]-§ 1). *Let K be an algebraic extension of $\boldsymbol{Q}$. Assume that $p \neq 2$ or K is totally imaginary. Then $\mathrm{cd}_p(G_K)=0, 1$ or 2. More precisely,*

$\mathrm{cd}_p(G_K)=0 \iff p \nmid [\overline{K}: K]$

$\mathrm{cd}_p(G_K)=1 \iff p \mid [\overline{K}: K]$ *and $p^\infty \mid n_v(K)$ for every non-archimedian valuation v of K, where $n_v(K)=[K_v: \boldsymbol{Q}_l]$*

$\mathrm{cd}_p(G_K)=2 \iff p^\infty \nmid n_v(K)$ *for some non-archimedian valuation v of K*

$\iff B_K(p) \neq 0$.

LEMMA 12 (cf. [6]-II § 2). *Let G be a pro-finite group and $G(p)=G/N$ be the maximal quotient of G such that G/N is a pro-p-group. Then $\mathrm{cd}_p(G(p))\leqq\mathrm{cd}_p(G)$ if $\mathrm{cd}_p(N)\leqq 1$.*

PROOF OF THEOREM 8. We show first that 1) implies 2). Since the canonical extension of v to L_v is discrete and has the same residue class field, $[L_v:\boldsymbol{Q}_p]<\infty$. Let V be the unique extension of v to $L(p)$. $L(p)_V=L_v(p)$ by Proposition 3, and $L(p)\cap L_v=L$, for v does not split in $L(p)$. Hence $Gal(L(p)/L)\cong Gal(L_v(p)/L_v)$.

Next we show the converse. $2=\mathrm{cd}_p(G_K(p))=\mathrm{cd}_p(G_L(p))$ by Lemma 10. Since $G_L(p)=G_L/G_{L(p)}$ and $\mathrm{cd}_p(G_L(p))\leqq 1$, $\mathrm{cd}_p(G_L)=2$ by Lemma 11 and 12. Hence $B_L(p)\neq 0$. On the other hand when v runs all the places of L, the canonical homomorphism $B_L\to\prod B_{L_v}$ is injective (cf. [3]), therefore there exists v such that

$$B_{L_v}(p)\neq 0\,. \qquad \cdots\cdots (1)$$

If v is archimedian, $L_v=\boldsymbol{C}$ so $B_{L_v}(p)=0$; this contradicts (1). Hence v is non-archimedian. Take any extension V of v to $L(p)$. Then $L(p)_V=L_v(p)$ from Proposition 3 and $D=L(p)\cap L_v$ is the decomposition field of V over L. Then

$$G_D(p)=Gal(L(p)/L)\cong G_{L_v}(p)\,.$$

Let v be over a rational prime q. Since $p^\infty\nmid[L_v:\boldsymbol{Q}_q]$ by (1) and Lemma 10, applying Lemma 9 we have

$$\mathrm{cd}_p(G_{L_v}(p))=2 \qquad \cdots\cdots (2)$$

and $G_{L_v}(p)$ is a Demuškin group. Now $G_{L_v}(p)\cong G_D(p)\subseteqq G_L(p)\cong G_K(p)$. K' denotes the intermediate field of $K(p)/K$ such that $G_D(p)\cong G_{K'}(p)\subseteqq G_K(p)$. Since $K'\supseteqq\boldsymbol{Q}_p$, $G_{L_v}(p)\cong G_{K'}(p)$ is of rank $[K':\boldsymbol{Q}_p]+2$. Hence $p=q$.

Let N be the normal closure of D over L. We show that $N\neq L(p)$. It is sufficient to show that $\bigcap_{\sigma\in G_{L(p)}}\sigma^{-1}G_D(p)\sigma\neq\{1\}$, i.e. that $\bigcap_{\sigma\in G_{K(p)}}\sigma^{-1}G_{K'}(p)\sigma\neq\{1\}$, namely that the normal closure of K' over K is not $K(p)$. From (2) $\mathrm{cd}_p(G_{K'}(p))=\mathrm{cd}_p(G_D(p))=\mathrm{cd}_p(G_{L_v}(p))=2$, $G_{K'}(p)=G_{K'}/G_{K'(p)}$, and $\mathrm{cd}_p(G_{K'(p)})\leqq 1$, for $p^\infty\mid[K'(p):\boldsymbol{Q}_p]$. Therefore $\mathrm{cd}_p(G_{K'})=2$ from Lemma 10 and 12. Hence $[K':\boldsymbol{Q}_p]$ is devided by p only finite times, so $[K':K]<\infty$. Thus the normal closure of K' over K is of finite degree over K, so this is not $K(p)$.

Next we show that $L=D$. Assume that $L\neq D$, then v has an extension V' to $L(p)$ distinct from V. The decomposition field D' of V' over L is conjugate to D. As N is normal over L, N contains both D and D'. Then N is p-Henselian with respect to V and V'. From Proposition 4, $N=L(p)$, this is a contradiction.

Thus we have shown that L is p-Henselian with respect to v. We have $G_L(p)\cong G_{L_v}(p)$, for v does not split in $L(p)$. Hence $G_{L_v}(p)\cong G_K(p)$. The right hand side (resp. the left hand side) is a Demuškin group of

rank $[L_v : \boldsymbol{Q}_p]+2$ (resp. $[K : \boldsymbol{Q}_p]+2$) by Lemma 9. Hence $[L_v : \boldsymbol{Q}_p]=[K : \boldsymbol{Q}_p]<\infty$. Consequently v is discrete and has a finite residue class field. q.e.d.

In virtue of the proof of Theorem 8 we have the next result.

COROLALLY 13. *Let L be as in Theorem 8. Then L is p-Henselian with respect to a non-archimedian valuation v if there exists a field K which satisfies the following conditions; K is an algebraic extension of $\boldsymbol{Q}_l$ containing a primitive p-th root of unity where l is a rational prime, $p^\infty \nmid [K : \boldsymbol{Q}_l]$, and $Gal(L(p)/L)\cong Gal(K(p)/K)$. In this case if $l=p$ (resp. $l\neq p$), then v is over p (resp. v is not over p).*

REMARK. From Theorem 8 we know that any finite totally imaginary algebraic number field L containing a primitive p-th root of unity can not be p-Henselian. Clearly it is not p-Henselian with respect to an archimedian valuation. It is known that the rank of $G_L(p)=\dim_{\boldsymbol{Z}/p\boldsymbol{Z}}H^1(G_L(p), \boldsymbol{Z}/p\boldsymbol{Z})=\dim_{\boldsymbol{Z}/p\boldsymbol{Z}}L^*/(L^*)^p$ (cf. [1]-§ 9). Hence the rank of $G_L(p)=\aleph_0$ if L is a finite extension of $\boldsymbol{Q}$. Therefore the condition 2) can not be satisfied, for the right hand side of it has a finite rank.

From Theorem 8 we can obtain some results on the prime decomposition law. The next theorem is a purpose of § 2.

THEOREM 14. *Let K be a finite totally imaginary algebraic number field containing a primitive p-th root of unity. Then $Gal(K(p)/K)$ determines the degree of K over $\boldsymbol{Q}$, the number of prime ideals of K over (p), $e(\mathfrak{p})f(\mathfrak{p})$ where $e(\mathfrak{p})$ denotes the ramification index and $f(\mathfrak{p})$ denotes the degree of inertia of a prime ideal $\mathfrak{p}$ of K over (p), and the maximal integer $m=m(K)$ for which K contains a primitive p^m-th root of unity.*

PROOF. Let K_1 and K_2 satisfy the assumption of Theorem 14 and $G_{K_1}(p)\cong G_{K_2}(p)$. Let the prime ideal decomposition of (p) in K_1 and K_2 be as follows;

$$(p)=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t} \text{ in } K_1, \quad \text{and} \quad (p)=\mathfrak{p}_1'^{e'_1}\cdots\mathfrak{p}_s'^{e'_s} \text{ in } K_2$$

$$N_{K_1/\boldsymbol{Q}}(\mathfrak{p}_i)=p^{f_i}, \quad N_{K_2/\boldsymbol{Q}}(\mathfrak{p}_j')=p^{f_j'} \qquad (1\leqq i\leqq t,\ 1\leqq j\leqq s).$$

We construct mappings α and β such that

$$A=\{\mathfrak{p}_1, \cdots, \mathfrak{p}_t\} \underset{\beta}{\overset{\alpha}{\rightleftarrows}} \{\mathfrak{p}_1', \cdots, \mathfrak{p}_s'\}=B.$$

For any $\mathfrak{p}$ in A, take a valuation v of $K_1(p)$ over $\mathfrak{p}$. ..... (1)

L denotes the decomposition field of v over K_1. Then

$$G_{K_1}(p)\supseteq G_L(p)\cong Gal(K_{1\mathfrak{p}}(p)/K_{1\mathfrak{p}}), \quad \text{and} \quad [K_{1\mathfrak{p}} : \boldsymbol{Q}_p]<\infty. \quad \cdots\cdots (2)$$

M denotes the intermediate field of $K_2(p)/K_2$ such that $G_L(p)\cong G_M(p)$ through the given isomorphosm. There exists a valuation w of M over p such that M is p-Henselian with respect to w, from Theorem 8. Denote by $\alpha(\mathfrak{p})$ the prime ideal in K_2 corresponding to the restriction of w to K_2. If we show that $\alpha(\mathfrak{p})$ is uniquely determined by $\mathfrak{p}$ independent of the choice of v in (1), the mapping α is well-defined. If v' is another valuation of $K_1(p)$ over $\mathfrak{p}$, the decomposition field of v and v' are $G_{K_1}(p)$-conjugate. Hence taking M' corresponding to v', M and M' are $G_{K_2}(p)$-conjugate. Then w and w' and so prime ideals corresponding to these are $G_{K_2}(p)$-conjugate. Restricting them to K_2, we have the same prime ideal.

Similarly we can construct a mapping β, and it is evident that $\alpha\circ\beta=\mathrm{id}_B$ and $\beta\circ\alpha=\mathrm{id}_A$. Consequently $t=s$. We have $G_{K_{1\mathfrak{p}}}(p)\cong G_{K_{2\alpha(\mathfrak{p})}}(p)$ by (2) and the manner of the choice of M. The Galois group of the maximal abelian extension of $K_{1\mathfrak{p}}$ (resp. $K_{2\alpha(\mathfrak{p})}$) over $K_{1\mathfrak{p}}$ (resp. $K_{2\alpha(\mathfrak{p})}$) is known by the local class field theory. Now their maximal p-factor groups are isomorphic, namely

$$\boldsymbol{Z}_p^{[K_{1\mathfrak{p}}:Q_p]+1}\times\boldsymbol{Z}/p^{m(K_1)}\boldsymbol{Z}\cong\boldsymbol{Z}_p^{[K_{2\alpha(\mathfrak{p})}:Q_p]+1}\times\boldsymbol{Z}/p^{m(K_2)}\boldsymbol{Z},$$

where $\boldsymbol{Z}_p$ denotes the p-adic integer ring. We remark here that $m(K_1)=m(K_{1\mathfrak{p}})$ and $m(K_2)=m(K_{2\alpha(\mathfrak{p})})$. From above isomorphism we know that $m(K_1)=m(K_2)$ and $[K_{1\mathfrak{p}}:\boldsymbol{Q}_p]=[K_{2\alpha(\mathfrak{p})}:\boldsymbol{Q}_p]$ i. e. $e(\mathfrak{p})f(\mathfrak{p})=e(\alpha(\mathfrak{p}))f(\alpha(\mathfrak{p}))$ for every $\mathfrak{p}$ in A. From these results clearly we have $[K_1:\boldsymbol{Q}]=[K_2:\boldsymbol{Q}]$.

q. e. d.

References

[1] H. Koch: Galoissche Theorie der p-Erweiterungen, Springer (1970).

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

[3] J. Neukirch: Über eine algebraische Kennzeichnung der Henselkörper, Crelle, 231 (1968), 75-81.

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

[5] J. Neukirch: Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterung, Crelle, 238 (1969), 135-147.

[6] J. P. Serre: Cohomologie Galoisienne, Lecture Notes in math. 5, Springer (1964).

[7] A. Weil: Basic Number Theory, Springer (1967).