K. KOMATSU
KŌDAI MATH. SEM. REP.
26 (1974), 44-52

THE GALOIS GROUP OF THE ALGEBRAIC CLOSURE OF AN ALGEBRAIC NUMBER FIELD

BY KEIICHI KOMATSU

Introduction

Let Q be the rational number field and let Q_p be the field of p-adic numbers for any prime number p. For any field F, we will denote by $\bar{F}$ the algebraic closure of F and by G_F the automorphism group of $\bar{F}$ over F. Let k and k' be algebraic extensions of Q such that they are contained in the same algebraically closed field $\bar{Q}$.

In [2], Neukirch has shown the following results.

THEOREM A. *For an algebraic extension k of Q, the following assertions are equivalent to each other:*

1) *G_k is isomorphic to an open subgroup of G_{Q_p}.*

2) *There exists a discrete place v of k such that v satisfies the following conditions:*

a) *v lies above p.*

b) *The residue field of v is finite.*

c) *The extension of v to $\bar{Q}$ is unique.*

THEOREM B. *For finite algebraic extensions k and k' of Q, let W and W' be the sets of finite places of k and k', respectively. If G_k and $G_{k'}$ are isomorphic, then there exists a bijection f of W onto W' such that G_{k_v} is isomorphic to $G_{k'_{f(v)}}$ for any place $v \in W$, where k_v (or $k'_{f(v)}$) is the completion of k at v (or k' at $f(v)$).*

THEOREM C. *If k is a finite Galois extension of Q and if k' is a finite algebraic extension of Q such that G_k and $G_{k'}$ are isomorphic, then we have $k=k'$.*

Without the assumption that k is Galois over Q, Theorem C does not hold: In fact, there exist distinct two finite algebraic extensions k and k' such that G_k and $G_{k'}$ are isomorphic and that k is isomorphic to k'. Hence, as for a generalization of Theorem C, it is natural and interesting to consider whether, for any finite algebraic extensions k and k', $G_k \cong G_{k'}$ implies $k \cong k'$ or not. In this paper we shall give some affirmative data of this problem. For this purpose in § 3, we shall obtain a refinement of the above Theorem B as follows:

Recieved March 15, 1973.

PROPOSITION. *For finite algebraic extensions k and k' of Q, let V and V' be the sets of places of k and of k', respectively. If G_k and $G_{k'}$ are isomorphic, then there exists a bijection f of V onto V' such that G_{k_v} is isomorphic to $G_{k'_{f(v)}}$ for any place $v \in V$.*

By the above Proposition and local class field theory, we shall show that if G_k and $G_{k'}$ are isomorphic, then the idele groups of k and k' are isomorphic, the unit groups of k and k' are isomorphic, the ideal class groups of k and k' are isomorphic, $D=D'$ and $R=R'$, where D and D' are the discriminants of k and k', respectively and where R and R' are the regulators of k and k', respectively.

§ **1. Neukirch's results.** In this paper, fields shall be local fields of characteristic 0 or algebraic number fields and isomorphisms mean topological ones. Let F be a field, let N be a Galois extension of F, let G be a profinite group and let A be a topological G-module. We shall use the following notations:

$\bar{F}$; the algebraic closure of F
$G(N/F)$; the topological Galois group of N over F
G_F; the topological Galois group of $\bar{F}$ over F
μ_F; all the roots of 1 in F
$F^\times$; the multiplicative group of F
Q; the rational number field
Z_p; the ring of p-adic integers
Q_p; the field of p-adic numbers
$G(l)$; the maximal l factor group of G for any prime l
(G, G); the topological commutator group of G
G^{ab}; the factor group of G by (G, G)
$H^n(G, A)$; the n-th cohomology group of G with coefficients in A.

We adopt similar notations for k, K and so forth.

Let p be a prime number. Then a profinite group G is said to be a pro-p-group if G is a projective limit of finite p-groups. For a pro-p-group G, the rank of G means the minimal number of topological generators of G.

Let $L(I)$ be the discrete free group generated by a set I and let F_p be the field with p elements. G is said to be a free pro-p-group if G is the projective limit of $L(I)/U$, where U is a normal subgroup of $L(I)$ such that U contains almost all elements of I and that $L(I)/U$ is a finite p group. Then the rank of G is equal to the cardinality of I and $\dim_{F_p} H^1(G, Z/pZ)$, where the action of G on Z/pZ is trivial and where $\dim_{F_p} H^1(G, Z/pZ)$ is the dimension of the vector space $H^1(G, Z/pZ)$ over F_p. From the definitions follows the following:

LEMMA 1. *For two finitely generated free pro-p-groups G_1 and G_2, G_1 is isomorphic to G_2 if and only if $G_1{}^{ab}$ is isomorphic to $G_2{}^{ab}$.*

A pro-p-group G is said to be a Demushkin group if

(1) $\dim_{F_p} H^2(G, Z/pZ)=1$

(2) the cup product $H^1(G, Z/pZ)\times H^1(G, Z/pZ)\to H^2(G, Z/pZ)$ is a non-degenerate bilinear form.

The characterization of Demushkin groups (cf. [1]) gives the following:

LEMMA 2. *For two finitely generated Demushkin groups G_1 and G_2, G_1 is isomorphic to G_2 if and only if $G_1{}^{ab}$ is isomorphic to $G_2{}^{ab}$.*

The following lemma (cf. [3]) is well known.

LEMMA 3. *For a prime number l, let ζ_l be a primitive l-th root of 1 and let K be a finite algebraic extension of Q_p. Then the following assertions hold:*

1) *If $\zeta_l \notin K$, then $G_K(l)$ is a finitely generated free pro-l-group.*

2) *If $\zeta_l \in K$, then $G_K(l)$ is a finitely generated Demushkin group.*

We shall use the following lemmas (cf. [2]) in § 3.

LEMMA 4. *For finite algebraic extensions k and k' of Q, let W and W' be the sets of finite places of k and of k', respectively. If G_k and $G_{k'}$ are isomorphic, then there exists a bijection f of W onto W' such that G_{k_v} and $G_{k'_{f(v)}}$ are isomorphic for any place $v\in W$, where k_v (or $k'_{f(v)}$) is the completion of k at v (or k' at $f(v)$).*

LEMMA 5. *Let k and k' be finite algebraic extensions of Q. If G_k and $G_{k'}$ are isomorphic, then the maximal Galois extension of Q contained in k and the maximal Galois extension of Q contained in k' coincide.*

LEMMA 6. *Let k and k' be finite algebraic extensions of Q. If G_k and $G_{k'}$ are isomorphic, then the minimal Galois extension N of Q containing k coincides with the minimal Galois extension N' of Q containing k' and the cardinality of $C(\sigma)\cap G(N/k)$ is equal to the cardinality of $C(\sigma)\cap G(N/k')$ for any $\sigma\in G(N/Q)$, where $C(\sigma)=\{\tau^{-1}\sigma\tau \mid \tau\in G(N/Q)\}$.*

COROLLARY. *If G_k and $G_{k'}$ are isomorphic, we have $|k;Q|=|k';Q|$, where $|k;Q|$ (or $|k';Q|$) is the degree of k (or k', respectively) over Q.*

It should be noted that Theorem A is a generalization of the following Artin's result.

LEMMA 7. *Let k be an algebraic extension of Q, then the following assertions are equivalent to each other:*

1) *The order of G_k is 2.*

2) *There exists a real place v of k such that v is uniquely extended to $\bar{k}$.*

(The above v is uniquely determined by k.)

§ 2. The Galois group of the algebraic closure of a local field.

In this

section, K, K_1 and K_2 shall be finite algebraic extensions of Q_p such that they are contained in the same algebraic closure $\bar{Q}_p$ of Q_p. We will denote by q the cardinality of the residue field of K, by e the order of ramification of K over Q_p and by f the modular degree of K over Q_p. Then we have $q=p^f$. Let $n=|K; Q_p|$. Then we have $n=ef$. Let m be the largest integer such that K contains a primitive p^m-th root of 1. We adopt similar notations, viz, q_i, e_i, f_i, n_i, for K_i, for $i=1, 2$. See [4] as for results of number theory used in the followings.

It is well known

$$K^\times \cong Z \times Z_p^n \times Z/(q-1)Z \times Z/p^m Z. \tag{1}$$

By local class field theory, we have

$$G_K^{ab} \cong \prod_l Z_l \times Z_p^n \times Z/(q-1)Z \times Z/p^m Z, \tag{2}$$

where $\prod_l$ is taken over all prime numbers. For completeness we shall give a proof of the following lemma.

LEMMA 8. *For a profinite group G and prime number p, $G^{ab}(p)$ and $G(p)^{ab}$ are isomorphic.*

Proof. Let N be a normal subgroup of G such that the factor group G/N is $G(p)$. Then we have $G(p)^{ab} \cong G/(G, G)N$. Suppose that the group $(G, G)N$ contains a subgroup H such that the index $|(G, G)N; H|$ is p and that H contains the subgroup (G, G). It follows $|N; N \cap H| = p$ from $|HN; H| = |N; N \cap H|$ and $HN = (G, G)N$. This contradicts the definition of N. Hence $G^{ab}(p)$ is isomorphic to $G/(G, G)N$. This completes our proof.

PROPOSITION 1. *Let K_1 and K_2 be two finite algebraic extensions of Q_p. Then the following assertions are equivalent to each other.*

1) *$K_1^\times$ is isomorphic to $K_2^\times$.*
2) *$\mu_{K_1} = \mu_{K_2}$ and $n_1 = n_2$.*
3) *$q_1 = q_2$, $e_1 = e_2$ and $m_1 = m_2$.*
4) *$G_{K_1}^{ab}$ is isomorphic to $G_{K_2}^{ab}$.*
5) *$G_{K_1}(l)$ is isomorphic to $G_{K_2}(l)$ for any prime l.*

Proof. 2) from 1): Since $K_1^\times$ is isomorphic to $K_2^\times$, we have that the torsion subgroups of $K_1^\times$ and of $K_2^\times$ are isomorphic. Hence we have $\mu_{K_1} = \mu_{K_2}$. By (1), $K_i^\times$ is isomorphic to $Z \times Z_p^{n_i} \times Z/(q_i-1)Z \times Z/p^{m_i}Z$ for $i=1, 2$. Therefore the maximal compact subgroup U_i of $K_i^\times$ is isomorphic to $Z_p^{n_i} \times Z/(q_i-1)Z \times Z/p^{m_i}Z$ and then $U_i(p)$ is isomorphic to $Z_p^{n_i} \times Z/p^{m_i}Z$ for $i=1, 2$. For the torsion subgroup T_i of $U_i(p)$, the factor group $U_i(p)/T_i$ is isomorphic to $Z_p^{n_i}$ for $i=1, 2$. Since n_i is the rank of $U_i(p)/T_i$ as Z_p-module and since $U_1(p)/T_1$ is isomorphic to $U_2(p)/T_2$, we have $n_1 = n_2$. In a similar way, we can prove 1) from 4) part, so its proof is omitted.

3) from 2): The cardinality of μ_{K_i} is $p^{m_i}(q_i-1)$, $q_i=p^{f_i}$ and $n_i=e_i f_i$ for $i=1, 2$. Therefore it is clear.

4) from 3): It follows from (2).

4) from 5): Let $q_i-1=\prod_l l^{\alpha_{l,i}}$ be the decomposition of q_i-1 into the product of powers of distinct prime numbers for $i=1, 2$. From (2) and Lemma 8, we have

$$G_{K_i}(l)^{ab} \cong \begin{cases} Z_l \times Z/l^{\alpha_{l,i}}Z & \text{for } l \neq p, \\ Z_p^{n_i+1} \times Z/p^{m_i}Z & \text{for } l=p, \end{cases} \tag{3}$$

for $i=1, 2$. Since $G_{K_1}(l)^{ab}$ and $G_{K_2}(l)^{ab}$ are isomorphic for any prime l, we shall obtain $\alpha_{l,1}=\alpha_{l,2}$, $n_1=n_2$ and $m_1=m_2$ in a similar way as the above 2) from 1) part. From (2), it follows that $G_{K_1}^{ab}$ and $G_{K_2}^{ab}$ are isomorphic.

5) from 4): Since $G_{K_i}^{ab}(l)$ and $G_{K_i}(l)^{ab}$ are isomorphic for $i=1, 2$, $G_{K_1}(l)^{ab}$ $G_{K_2}(l)^{ab}$ are isomorphic. From Lemma 3, $G_{K_1}(l)$ and $G_{K_2}(l)$ are finitely generated free pro-l-groups or finitely generated Demushkin groups. Hence from Lemma 1 and Lemma 2, we have that $G_{K_1}(l)$ and $G_{K_2}(l)$ are isomorphic. This completes our proof.

COROLLARY. *Let K_1 and K_2 be two finite algebraic extensions of K such that K_1 is an unramified extension of K. If G_{K_1} and G_{K_2} are isomorphic, then we have $K_1=K_2$.*

Proof. Since K_1 is unramified over K, K_1 is the extension of K generated by μ_{K_1}. $G_{K_1} \cong G_{K_2}$ implies $G_{K_1}^{ab} \cong G_{K_2}^{ab}$. By Proposition 1, we have $\mu_{K_1}=\mu_{K_2}$ and $n_1=n_2$. Hence $K_1 \subset K_2$ and $|K_1 ; K|=|K_2 ; K|$. It follows $K_1=K_2$.

§ 3. The Galois group of the algebraic closure of an algebraic number field.

In this section, we denote by k and k' finite algebraic extensions of Q such that they are contained in the same algebraic closure $\bar{Q}$ of Q. We shall use the following notations:

a; the cardinality of μ_k
r_1; the number of the real places of k
r_2; the number of the imaginary places of k
$\zeta_k(s)$; the zeta-function of k
V; the set of places of k
W; the set of finite places of k
P_∞; the set of infinite places of k
S_∞; the set of real places of k
k_v; the completion of k at $v \in V$
q_v; the cardinality of the residue field of k_v.

We adopt similar notations, viz. a', r'_1, $\cdots$ for k'.

LEMMA 9. *Let k and k' be finite algebraic extensions of Q. If G_k and $G_{k'}$ are isomorphic, then we have $\mu_k=\mu_{k'}$.*

Proof. Let M be the maximal Galois extension of Q contained in k. Then by Lemma 5, M is the maximal Galois extension of Q contained in k'. Hence from $\mu_k=\mu_M$ and $\mu_{k'}=\mu_M$, we have $\mu_k=\mu_{k'}$.

LEMMA 10. *Let k and k' be finite algebraic extensions of Q. If G_k and $G_{k'}$ are isomorphic, then we have $r_1=r_1'$ and $r_2=r_2'$.*

Proof. Let α be an isomorphism of G_k onto $G_{k'}$. For $v\in S_\infty$, let $\bar{v}$ be an extension of v to $\bar{Q}$ and let $H_{\bar{v}}$ be the decomposition subgroup of G_k for $\bar{v}$. Since v is a real place of k and since G_{k_v} is isomorphic to $H_{\bar{v}}$, the order of $H_{\bar{v}}$ is 2. Therefore the order of $\alpha(H_{\bar{v}})$ is 2. Let K' be the subfield of $\bar{Q}$ attached to $\alpha(H_{\bar{v}})$ in the sense of Galois theory. By Lemma 7, there exists a real place $\bar{v}'$ of K' which is uniquely extended to $\bar{Q}$. Let $f_\alpha(v)$ be the restriction of $\bar{v}'$ to k' which is uniquely determined by $\bar{v}$. Let $\bar{v}^*$ be another extension of v to $\bar{Q}$, then $H_{\bar{v}}$ and $H_{\bar{v}^*}$ are conjugate in G_k to each other. Hence f_α is well defined as a mapping of S_∞ to S'_∞. By a similar way, using the inverse α^{-1} of α, we construct a mapping $f_{\alpha^{-1}}$ of S'_∞ to S_∞ such that $f_\alpha\circ f_{\alpha^{-1}}$ and $f_{\alpha^{-1}}\circ f_\alpha$ are identity mappings. Hence we have $r_1=r_1'$. It is well known that the degree $|k\,;Q|$ (or $|k'\,;Q|$) is equal to r_1+2r_2 (or $r_1'+2r_2'$). By the Corollary of Lemma 6, we have $r_1+2r_2=r_1'+2r_2'$. Hence we have $r_2=r_2'$. This completes our proof.

Now, using Lemma 10 we can extend the Neukirch's bijection between the finite place sets W and W' in Lemma 4 to a bijection between the place sets V and V'.

PROPOSITION 2. *Let k and k' be finite algebraic extensions of Q. If G_k and $G_{k'}$ are isomorphic, then there exists a bijection f of V onto V' such that G_{k_v} and $G_{k'_{f(v)}}$ are isomorphic for any place $v\in V$.*

COROLLARY. *If G_k and $G_{k'}$ are isomorphic, then there exists a bijection f of V onto V' such that $k_v^\times$ and $k'^\times_{f(v)}$ are isomorphic for any place $v\in V$. Hence $f(W)=W'$ and $f(P_\infty)=P'_\infty$.*

Proof. It follows from Proposition 1 and Proposition 2.

Let K (or K') be a finite algebraic extension of k (or k') and let W_K (or $W_{K'}$) be the set of finite places of K (or K'). For a place $v\in W$ such that v lies above prime p, let $e_k(v)$ be the order of ramification of k_v over Q_p. We adopt similar notations, viz. $e_{k'}(v')$, $e_K(w)$ and $e_{K'}(w')$ for k', K and K', respectively.

LEMMA 11. *If α is an isomorphism of G_k onto $G_{k'}$ such that $\alpha(G_K)=G_{K'}$, then there exist two bijections f of W onto W' and F of W_K onto $W_{K'}$ such that f and F satisfy the following conditions:*

a) *G_{k_v} is isomorphic to $G_{k'_{f(v)}}$ for any place $v\in W$.*
b) *G_{K_w} is isomorphic to $G_{K'_{F(w)}}$ for any place $w\in W_K$.*
c) *A place $w\in W_K$ lies above $v\in W$ if and only if $F(w)$ lies above $f(v)$.*

Proof. Using Theorem A, we can prove this Lemma in a similar way to the proof of Lemma 10. So its proof is omitted.

LEMMA 12. *Assumptions and notations being as above, if K is an unramified extension of k', then K' is an unramified extension of k'.*

Proof. Using Proposition 1 and Lemma 11, we have $e_k(v)=e_{k'}(f(v))$ and $e_K(w)=e_{K'}(F(w))$ for any place $v\in W$ and $w\in W_K$. Suppose that w lies above v. Since K is an unramified extension of k, we have $e_K(w)=e_k(v)$. A place w lies above v if and only if $F(w)$ lies above $f(v)$. So we have $e_{K'}(F(w))=e_{k'}(f(v))$ and K' is an unramified extension of k'.

LEMMA 13. *Assumptions and notations being as Lemma 12, if K is the absolute class field of k, then K' is the absolute class field of k'.*

Proof. Let L' be the absolute class field of k'. From Lemma 12, K' is an unramified extension of k' and $G(K'/k')$ is commutative. Hence we have $K'\subset L'$. Let L be the extension of k such that $\alpha(G_L)=G_{L'}$, then we have $L\subset K$. Since $L'\subset K'$ follows from $L\subset K$, we have $L=K$.

LEMMA 14. *Let $C(k)$ and let $C(k')$ be the ideal class groups of k and k', respectively. If G_k and $G_{k'}$ are isomorphic, then $C(k)$ and $C(k')$ are isomorphic.*

Proof. Let K be the absolute class field of k and let α be an isomorphism of G_k onto $G_{k'}$. It is well known that $C(k)$ is isomorphic to $G(K/k)$. Let K' be the extension of k' such that $\alpha(G_K)=G_{K'}$, then K' is the absolute class field of k'. Hence, $C(k')$ is isomorphic to $G(K'/k')$. From $G_k/G_K\cong\alpha(G_k)/\alpha(G_K)$, we have $G(K/k)\cong G(K'/k')$. So we have $C(k)\cong C(k')$.

THEOREM. *Let k and k' be finite algebraic extensions of Q. Let D be the discriminant of k over Q, let $C(k)$ be the ideal class group of k, let R be the regulator of k, let E be the unit group of k and let $k_A^\times$ be the idele group of k. We adopt similar notations for k'. If G_k and $G_{k'}$ are isomorphic, then we have $D=D'$, E and E' are isomorphic, $k_A^\times$ and $k_A'^\times$ are isomorphic, $C(k)$ and $C(k')$ are isomorphic and $R=R'$.*

Proof. In Lemma 14, it has shown that $C(k)$ and $C(k')$ are isomorphic. Let h and h' be the class numbers of k and k', respectively. We have $h=h'$. Using the bijection f of Proposition 2, we have $q_v=q'_{f(v)}$ for any $v\in W$. So it follows that

$$\begin{aligned}\zeta_k(s)&=\prod_{v\in W}(1-q_v^{-s})^{-1}\\&=\prod_{v\in W}(1-q_{f(v)}^{-s})^{-1}\\&=\zeta_{k'}(s)\end{aligned}$$

for Re$(s)>1$. From the theorem of identity, we have $\zeta_k(s)=\zeta_{k'}(s)$ for any complex number s. Let G_1 and G_2 be defined by the formulas

$$G_1(s)=\pi^{-s/2}\Gamma(s/2)\,, \qquad G_2(s)=(2\pi)^{1-s}\Gamma(s)$$

where $\Gamma(s)$ is the gamma function. Let $Z_k(s)$ and $Z_{k'}(s)$ be defined by the formulas

$$Z_k(s)=G_1(s)^{r_1}G_2(s)^{r_2}\zeta_k(s)$$

$$Z_{k'}(s)=G_1(s)^{r'_1}G_2(s)^{r'_2}\zeta_{k'}(s)\,.$$

Since, from Lemma 10, we have $r_1=r'_1$ and $r_2=r'_2$, it follows that $Z_k(s)=Z_{k'}(s)$. It is well known that $Z_k(s)$ is a meromorphic function in the complex plane, holomorphic except for simple poles at $s=0$ and $s=1$. Further, it is well known

$$\lim_{s\to 0} sZ_k(s)=-2^{r_1}(2\pi)^{r_2}hR/a$$

$$\lim_{s\to 0} sZ_{k'}(s)=-2^{r'_1}(2\pi)^{r'_2}h'R'/a'\,.$$

By Lemma 9, we have $a=a'$. So we have $hR=h'R'$. Hence it follows $R=R'$. Since we have

$$\lim_{s\to 1}(s-1)Z_k(s)=|D|^{-\frac{1}{2}}2^{r_1}(2\pi)^{r_2}hR/a$$

$$\lim_{s\to 1}(s-1)Z_{k'}(s)=|D'|^{-\frac{1}{2}}2^{r'_1}(2\pi)^{r'_2}h'R'/a'\,,$$

it follows $|D|=|D'|$. So we have $D=D'$ because the signs of D and D' are $(-1)^{r_2}$. From the Dirichlet's theorem of the units, E is isomorphic to $\mu_k\times Z^{r_1+r_2-1}$ and E' is isomorphic to $\mu_{k'}\times Z^{r_1'+r_2'-1}$. By Lemma 9 we have $\mu_k=\mu_{k'}$. Hence E is isomorphic to E'. From Corollary of Proposition 2 and the definition of the idele group of k, $k_A^\times$ and $k'^\times_A$ are isomorphic. This completes our proof.

Now we shall give an example in which G_k determines the isomorphism class of k, using the theorem of P. Hall: Let G be a solvable finite group, and let H_1 and H_2 be subgroups of G such that the orders of H_1 and H_2 are equal and relatively prime to the index $|G\,;H_1|$, then H_1 and H_2 are conjugate in G.

PROPOSITION 3. *Let k and k' be finite algebraic extensions of Q, let $\tilde{Q}$ be the solvable closure of Q and let l be a prime number such that $|k\,;Q|=l$. If G_k and $G_{k'}$ are isomorphic and if k is contained in $\tilde{Q}$, then k is isomorphic to k'.*

Proof. Let us use the notations of Lemma 6. Since k is contained in $\tilde{Q}$, $G(N/Q)$ is solvable. By Lemma 6, $N=N'$ and the order of $G(N/k)$ is equal to that of $G(N/k')$. Since $|G(N/Q)\,;G(N/k)|$ is prime number l, it is easily seen that the common order of $G(N/k)$ and $G(N/k')$ is relatively prime to l. Hence by the theorem of P. Hall, $G(N/k)$ is conjugate to $G(N/k')$ in $G(N/Q)$. Therefore k is isomorphic to k'.

For the above Galois group $G(N/Q)$, it should be noted that the commutator group of $G(N/Q)$ is commutative. Now we shall give an example of the above field k: For an integer m such that $\sqrt[l]{m}$ is not contained in Q, the field $Q(\sqrt[l]{m})$ is contained in $\tilde{Q}$, $|Q(\sqrt[l]{m}); Q|=l$ and $N=Q(\sqrt[l]{m}, \zeta_l)$, where ζ_l is a primitive l-th root of 1.

BIBLIOGRAPHY

[1] J. LABUTE, Classification of Demushkin groups, Can. J. Math. **19** (1966), 106-132.
[2] J. NEUKIRCH, Kennzeichnung der p-adischen und der endlich algebraischen Zahlkörper, Inventiones math. **6** (1969), 296-314.
[3] J. P. SERRE, Cohomologie Galoissienne, Lecture notes in Math. **5** Springer-Verlag (1964).
[4] A. WEIL, Basic Number Theory, Springer-Verlag (1967).

DEPARTMENT OF MATHEMATICS,
TOKYO INSTITUTE OF TECHNOLOGY.