J. Math. Soc. Japan
Vol. 30, No. 2, 1978

On Grunwald-Hasse-Wang's theorem

By Hiroo MIKI*)

(Received Oct. 8, 1976)
(Revised Aug. 3, 1977)

Let k be a field with discrete valuations, $k_{\mathfrak{p}}$ the completion of k with respect to a prime divisor $\mathfrak{p}$ of k, k_{sep} the separable algebraic closure of k, and $k_{\mathfrak{p},\mathrm{sep}}$ the separable algebraic closure of $k_{\mathfrak{p}}$ containing k_{sep}. Here a *prime divisor* is a normalized discrete valuation. Let S be a finite set of prime divisors of k, G a finite abelian group, and $(K^{\mathfrak{p}}, j_{\mathfrak{p}})$ a pair of a finite abelian extension $K^{\mathfrak{p}}$ of $k_{\mathfrak{p}}$ in $k_{\mathfrak{p},\mathrm{sep}}$ and an injective homomorphism $j_{\mathfrak{p}}$ from the Galois group $G(K^{\mathfrak{p}}/k_{\mathfrak{p}})$ into G for each $\mathfrak{p}\in S$. An *imbedding problem*

$$P=P\{k, G, S, (K^{\mathfrak{p}}, j_{\mathfrak{p}})\ (\mathfrak{p}\in S)\}$$

is to find a pair (K, j) of an abelian extension K of k in k_{sep} and a surjective isomorphism $j: G(K/k)\simeq G$ satisfying $K_{\mathfrak{p}}=K^{\mathfrak{p}}$ and $j_{\mathfrak{p}}=j\circ\mathrm{Res}_{\mathfrak{p}}$ for any $\mathfrak{p}\in S$, where $K_{\mathfrak{p}}=Kk_{\mathfrak{p}}$ and $\mathrm{Res}_{\mathfrak{p}}$: $G(K_{\mathfrak{p}}/k_{\mathfrak{p}})\to G(K/k)$ is the restriction from $K_{\mathfrak{p}}$ to K. We call the pair (K, j) a *solution* of the imbedding problem P.

When k is a finite algebraic number field or an algebraic function field in one variable over a finite constant field, Grunwald, Hasse and Wang ([**2**], [**3**], [**6**]) gave a condition for an imbedding problem P to have a solution, and in particular proved that an imbedding problem P has a solution if (k, G, S) is not the "special case" (see also Chap. 10 of [**1**] and Theorem of [**5**]). Their proofs were based on class field theory, and Hasse ([**3**], § 4, 1) raised the problem of giving a proof based on Kummer theory.

In the present paper, we shall give a certain sufficient condition for an imbedding problem P to have a solution for *any field k with discrete valuations.* More precisely, we shall prove the following

THEOREM. *Let k be a field, S a finite set of prime divisors of k, and G a finite abelian group of type $(p_1^{m_1}, p_2^{m_2}, \cdots, p_t^{m_t})$. Then an imbedding problem $P\{k, G, S, (K^{\mathfrak{p}}, j_{\mathfrak{p}})\ (\mathfrak{p}\in S)\}$ has a solution if the following two conditions are satisfied*:

(i) *There exist t distinct prime divisors $\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_t$ of k outside S such that $\zeta(p_i^{m_i})\in k_{\mathfrak{q}_i}$ if $p_i\neq\mathrm{ch}(k)$.*

(ii) *If* $\exp(G)$ *is divisible by* 4 *and if* $\mathrm{ch}(k)\neq 2$, *then* $\zeta(4)\in k$ (see Notation below and Theorem 5).

*) Partially supported by Fūjukai Foundation.

COROLLARY. *Let k be a finite algebraic number field or an algebraic function field in n variables* ($n \geqq 1$) *over any field. Then an imbedding problem* $P\{k, G, S, (K^{\mathfrak{p}}, j_{\mathfrak{p}})\ (\mathfrak{p} \in S)\}$ *has a solution if the condition* (ii) *is satisfied* (see Proposition 6).

Note that our method of proof gives an answer to Hasse's problem under the condition (ii) which is stronger than the condition that (k, G, S) is not the "special case", and that the prime divisors of an algebraic function field in the above corollary are not necessarily trivial on the constant field.

Our proof depends only upon Kummer theory, Galois theory, the approximation theorem on valuations, Čebotarev's density theorem and Hensel's lemma, and the key to our proof is Lemma 1 which is a generalization of Proposition 3 of [4].

NOTATION. $\mathrm{ch}(k)$: the characteristic of a field k. $\zeta(m)$: a primitive m-th root of unity. $\exp(G)$: the exponent of a finite abelian group G. A finite abelian group G is called of *type* $(p_1^{m_1}, p_2^{m_2}, \cdots, p_t^{m_t})$, if G is isomorphic to the direct product of t cyclic groups of order $p_i^{m_i}$ $(1 \leqq i \leqq t)$ with $p_1 \leqq p_2 \leqq \cdots \leqq p_t$ and $m_i \geqq 1$ $(1 \leqq i \leqq t)$, where p_i is a prime number for any i $(1 \leqq i \leqq t)$, $\gamma | K$: the restriction of $\gamma \in G(L/k)$ to K, where L and K are finite Galois extensions of k such that $L \supset K$.

§ 1. An explicit construction of cyclic extensions.

Let $\boldsymbol{Z}$ denote the ring of rational integers and $\boldsymbol{N}$ the set of natural numbers. Let p be a fixed prime number and let ζ_i be a primitive p^i-th root of unity such that $\zeta_{i+1}^p = \zeta_i$ with $i \in \boldsymbol{N} \cup \{0\}$. Let k be a field of characteristic different from p. Assume that k *contains a primitive* 4-*th root of unity if* $p=2$. If $\zeta_m \in \tilde{k}$ for all $m \in \boldsymbol{N}$, then let $n_0 = \infty$, otherwise let $n_0 \in \boldsymbol{N}$ be such that $\zeta_{n_0} \in \tilde{k}$ and $\zeta_{n_0+1} \notin \tilde{k}$, where $\tilde{k} = k(\zeta_1)$. Fix $n \in \boldsymbol{N}$, and put $k(\zeta_n) = \tilde{k}'$. Put $N = [\tilde{k}' : k]$, $N' = [\tilde{k}' : \tilde{k}]$ and $N'' = [\tilde{k} : k]$, then $N = N'N''$. Let k' be a unique cyclic extension of k of p-power degree such that $k'(\zeta_1) = \tilde{k}'$. Let σ be a fixed generator of the Galois group $G(\tilde{k}'/k)$ and let $l \in \boldsymbol{Z}$ be such that $\zeta_n^\sigma = \zeta_n^l$ and $l \neq 1$. Let $n_1 \in \boldsymbol{N}$ be such that p^{n_1} is the exact power of p dividing $(1-l^N)$, and put $s = (1-l^N)/p^{n_1}$. We have $n_1 = n$ if $\tilde{k}' \neq \tilde{k}$, by the above assumption. For any sub-extension S/M of $\tilde{k}'/k$, put

$$\Sigma(S/M) = \sum_{i=0}^{g-1} \tilde{\sigma}^{g-1-i} \tilde{l}^i \in \boldsymbol{Z}[G(\tilde{k}'/k)],$$

where $\tilde{\sigma} = \sigma^{[M:k]}$, $\tilde{l} = l^{[M:k]}$ and $g = [S : M]$. Here $\boldsymbol{Z}[G(\tilde{k}'/k)]$ is a group ring of $G(\tilde{k}'/k)$ over $\boldsymbol{Z}$. It is easily verified that $\Sigma(T/M) = \Sigma(T/S)\Sigma(S/M)$ for $\tilde{k}' \supset T \supset S \supset M \supset k$.

LEMMA 1. *Let notations and assumptions be as above. Moreover let d and*

m be rational integers such that $1 \leqq p^d \leqq [k' : k]$ and $d \leqq m \leqq n$, and let k_1/k be the unique sub-extension of k'/k of degree p^d. Put $\sigma_1 = \sigma^{p^d}$, $l_1 = l^{p^d}$, $\tilde{k}_2 = \tilde{k}(\zeta_{m-d})$ and $m_0 = \mathrm{Max}\,(0, n'' - (m-d))$, where $n'' = \mathrm{Min}\,(n, n_0)$. Then the following two statements (i) *and* (ii) *hold:*

(i) *For any $b \in \tilde{k}_2$, put $a = b^{p^{m_0}}, w = \zeta_m a$, $z = \sqrt[p^n]{w^{\Sigma(\tilde{k}'/k)}}$ and $\tilde{K}' = \tilde{k}'(z)$. Assume that $w^{\Sigma(\tilde{k}'/k)} \notin (\tilde{k}')^{p^{n-(m-d)+1}}$ if $m-d \neq 0$. Then $\tilde{K}'/k$ is an abelian extension of degree Np^{m-d}, and there exists a unique $\gamma \in G(\tilde{K}'/k)$ satisfying*

$$(*) \qquad \begin{cases} z^{\gamma} = z^{l_1} (w^{sp^{n_1-n}})^{\Sigma(k_1/k)} \\ \gamma \,|\, \tilde{k}' = \sigma_1 . \end{cases}$$

Let K be the sub-field of $\tilde{K}'$ fixed by γ. Then K/k is a cyclic extension of degree p^m satisfying $K \cap k' = k_1$ and $K\tilde{k}' = \tilde{K}'$. If $n = n_1$, then there exists a unique $\tilde{\gamma} \in G(\tilde{K}'/k)$ satisfying

$$(**) \qquad \begin{cases} z^{\tilde{\gamma}} = z^{l} a^{s} \\ \tilde{\gamma} \,|\, \tilde{k}' = \sigma . \end{cases}$$

Then $\tilde{\gamma} \,|\, K$ is a generator of $G(K/k)$.

(ii) *Conversely every cyclic extension K of k of degree p^m satisfying $K \cap k' = k_1$ can be obtained in the way of* (i).

PROOF. We will prove the lemma in the following two cases (A) and (B).

(A) The case where $n_1 = n$. Put $p^d = p'$, $[\tilde{k}_2 : \tilde{k}] = p^{d'} = q$, $[\tilde{k}' : \tilde{k}_2] = p^{d''} = q'$ and $[\tilde{k}' : \tilde{k}_1] = p^{d_1} = p''$, where $\tilde{k}_1 = k_1(\zeta_1)$. Then $N' = qq' = p'p'' = p^{n-n''}$. It is easily verified that $d'' = n - (m-d) - m_0$ and $n'' + d = m - d' + m_0$. Put $1 - l^{N''q} = s_1 p^{n-d''}$ and $(1 - l^N)/(1 - l^{N''q}) = s_2 q'$, then $s_1, s_2 \in \boldsymbol{Z}$, $s_1, s_2 \not\equiv 0 \pmod{p}$ and $s = s_1 s_2$. Put $\Sigma = \Sigma(\tilde{k}'/k)$, $\Sigma_1 = \Sigma(k_1/k)$ and $\Sigma_2 = \Sigma(\tilde{k}_2/k)$.

(i) Using the equality $\Sigma = \Sigma(\tilde{k}'/\tilde{k}_2)\Sigma_2$ and that $a \in \tilde{k}_2$, we easily obtain $w^{\Sigma} = \zeta_m^{Nl^{N-1}} (a^{\Sigma_2})^{s_2 q'} = (\zeta_{n''+d}^{N''l^{N-1}} b^{s_2 \Sigma_2})^{p^{n-(m-d)}}$. Hence, if we put

$$(1) \qquad y = \zeta_{n''+d}^{N''l^{N-1}} (b^{s_2})^{\Sigma_2},$$

then

$$(2) \qquad z = \sqrt[p^{m-d}]{y} .$$

By assumption, y$\notin (\tilde{k}')^p$ if m$-$d$\neq$0, hence $[\tilde{K}' : \tilde{k}] = p^{m-d}$. By using (1) and that $b \in \tilde{k}_2$, we have $y^{\sigma-l} = b^{s_2(1-l^{N''q})} = b^{s_1 s_2 p^{n--d''}}$, hence

$$(3) \qquad y^{\sigma-l} = (a^s)^{p^{m-d}}.$$

By [4], Proposition 2, (3) implies that $\tilde{K}'/k$ is an abelian extension of degree Np^{m-d}. Let $\tilde{\sigma} \in G(\tilde{K}'/k)$ be such that $\tilde{\sigma} \,|\, \tilde{k}' = \sigma$. Then by (3),

$$(4) \qquad z^{\tilde{\sigma}-l} = \zeta_{m-d}^{r} a^{s}$$

for some $r\in \boldsymbol{Z}$. Let $\tau\in G(\tilde{K}'/\tilde{k}')$ be such that $z^{\tau}=z\zeta_{m-d}$, and let $r'\in \boldsymbol{Z}$ be such that $r+lr'\equiv 0 \pmod{p^{m-d}}$. Put $\tilde{\gamma}=\tilde{\sigma}\tau^{r'}$. Then by (4), we have

$$\begin{cases} z^{\tilde{\gamma}-l}=a^{s} \\ \tilde{\gamma}\,|\,\tilde{k}'=\sigma. \end{cases} \tag{5}$$

Put $\tilde{\Sigma}_1=\tilde{\gamma}^{p'-1}+\tilde{\gamma}^{p'-2}l+\cdots+\tilde{\gamma}l^{p'-2}+l^{p'-1}\in \boldsymbol{Z}[G(\tilde{K}'/k)]$. Making $\tilde{\Sigma}_1$ operate on both members of (5), we obtain

$$z^{\gamma_1}=z^{l_1}(a^{s})^{\Sigma_1}, \tag{6}$$

where $\tilde{\gamma}_1=\tilde{\gamma}^{p'}$. Since $(w^{\Sigma_1})^{s}=\zeta_{m-d}^{l^{p'-1}s}(a^{s})^{\Sigma_1}$, (6) gives $z^{\tilde{\gamma}_1}=z^{l_1}(w^{s})^{\Sigma_1}\zeta_{m-d}^{-sl^{p'-1}}$. Hence if we put $\gamma=\tilde{\gamma}_1\tau^{r''}$, where $r''\in \boldsymbol{Z}$ is such that $-sl^{p'-1}+r''l_1\equiv 0 \pmod{p^{m-d}}$, then $z^{r}=z^{l_1}(w^{s})^{\Sigma_1}$ and $\gamma\,|\,\tilde{k}'=\sigma_1$, i.e., γ satisfies the condition (*) in Lemma 1. Since $\tilde{K}'=\tilde{k}'(z)$, such γ is unique. Since $K\cap\tilde{k}'$ is the sub-field of $\tilde{k}'$ fixed by σ_1, $K\cap\tilde{k}'=k_1$, so $K\cap k'=k_1$. Now we will show that the order of γ is $p''N''$. Put $\tilde{\Sigma}_1'=\gamma^{N''p''-1}+\gamma^{N''p''-2}l_1+\cdots+\gamma l_1^{N''p''-2}+l_1^{N''p''-1}$. By making $\tilde{\Sigma}_1'$ operate on $z^{\gamma-l_1}=(\mathrm{w}^{s})^{\Sigma_1}$, we have $z^{\gamma^{N''p''}-l_1{}^{N''p''}}=(w^{s})^{\Sigma}$, hence $z^{\gamma^{N''p''}}=z$, since $z^{1-l^{N}}=(w^{s})^{\Sigma}$. Since $r^{N''p''}\,|\,\tilde{k}'=\sigma^{N}=1$, this implies $\gamma^{N''p''}=1$. From this and $\gamma\,|\,\tilde{k}'=\sigma_1$, we see that the order of γ is $N''p''$, hence $[K:k]=p^{m}$. Now we will show that the order of $\tau \bmod \langle\gamma\rangle\in G(\tilde{K}'/k)/\langle\gamma\rangle$ is p^{m-d}. Here $\langle\gamma\rangle$ denotes the subgroup of $G(\tilde{K}'/k)$, generated by γ. Suppose that $\tau^{i}=\gamma^{j}$ with $i, j\in \boldsymbol{Z}$. Restrict them to $\tilde{k}'$, then $1=\sigma^{jp'}$, so $N''p''\,|\,j$, i.e., $N''p''$ divides j. Since the order of γ is $N''p''$, $\tau^{i}=\gamma^{j}=1$, so $p^{m-d}\,|\,i$, hence the order of τ mod $\langle\gamma\rangle$ is p^{m-d}. Since $\gamma=\tilde{\gamma}_1\tau^{r''}$ and since $r''\not\equiv 0 \pmod{p}$, the order of $\tilde{\gamma}_1 \bmod \langle\gamma\rangle$ is equal to that of τ mod $\langle\gamma\rangle$, i.e., to p^{m-d}. This implies that the order of $\tilde{\gamma}\,|\,K$ is p^{m}. From this fact and $[K:k]=p^{m}$, we see that K/k is a cyclic extension of degree p^{m} and that $\tilde{\gamma}\,|\,K$ is a generator of $G(K/k)$.

(ii) Put $s_2'=1$ or $(1-l^{N''p'})/(1-l^{N''q})q''$ according as $d'\geqq d$ or $d'\leqq d$, where $q''=p^{d-d'}$. Then $s_2'\in \boldsymbol{Z}$, $s_2'\not\equiv 0 \pmod{p}$. Let $r, t, t'\in \boldsymbol{N}$ be such that $-rs_2\equiv N''l^{N-1} \pmod{p^{n''+d}}$, $-s_2+s_2'N''l^{N}t\equiv 0 \pmod{p^{m-d}}$, and $N''tt'\equiv 1 \pmod{p^{m-d}}$. Since $s_2\equiv s_2' \pmod{p^{m-d-d_1}}$ by the next Lemma 2 and since $l^{N}\equiv 1 \pmod{p^{n}}$, we have $t'\equiv 1$ (mod p^{m-d-d_1}). Put $K'=Kk'$, $\tilde{K}'=K\tilde{k}'$ and $G=G(\tilde{K}'/k)$. Let $\tilde{\sigma}\in G$ be such that $\tilde{\sigma}\,|\,\tilde{k}'=\sigma$ and such that $\tilde{\sigma}\,|\,\tilde{K}$ is a generator of $G(\tilde{K}/k)$, where $\tilde{K}=K(\zeta_1)$. Since $\tilde{\sigma}_1\,|\,K$ is a generator of $G(K/k_1)$, where $\tilde{\sigma}_1=\tilde{\sigma}^{p'}$, there exists a generator τ of $G(\tilde{K}'/\tilde{k}')$ such that $\tau\,|\,K=\tilde{\sigma}_1^{-1}\,|\,K$. Put $\gamma=\tilde{\sigma}_1\tau$. Since $\gamma^{N''p''}=1$ on K and $\tilde{k}'$, $\gamma^{N''p''}=1$. If $\gamma^{i}=1$, then $\gamma^{i}\,|\,\tilde{k}'=\sigma_1^{i}=1$, hence $N''p''\,|\,i$. Therefore the order of γ is $N''p''$. Since $\gamma\,|\,K=1$ and $[\tilde{K}':K]=N''p''$, this implies that K is the sub-field of $\tilde{K}'$ fixed by γ. Let L be the sub-field of $\tilde{K}'$ fixed by γ', where $\gamma'=\tilde{\sigma}_1\tau^{t'}$, and put $\tilde{L}=L(\zeta_1)$. Then $\gamma'\,|\,\tilde{k}'=\sigma_1$ implies that $L\cap\tilde{k}'=k_1$. If $\gamma'^{i}=1$ with an $i\in \boldsymbol{Z}$, then $\gamma'^{i}\,|\,\tilde{k}'=\sigma_1^{i}=1$, so $N''p''\,|\,i$. Conversely $\gamma'^{N''p''}=(\tau^{t'-1})^{N''p''}=1$ on K, since $t'\equiv 1 \pmod{p^{m-d-d_1}}$. From this fact and that $\gamma'^{N''p''}=\sigma^{N}=1$ on $\tilde{k}'$, it follows that $\gamma'^{N''p'}=1$. Hence the order of γ' is $N''p''$, so, $[L:k]=p^m$. Since $L\cap k'=k_1$, this implies $[Lk':k']=p^{m-d}$. Therefore $K'=Lk'$ and $\tilde{K}'=L\tilde{k}'$. Since $L\tilde{k}'=\tilde{K}'$ and $L\cap\tilde{k}'=k_1$, the order of $\tau^{-t'}|L=\tilde{\sigma}_1|L$ is p^{m-d}. Hence the order of $\tilde{\sigma}|L$ is p^m. Since $[L:k]=p^m$, this implies that L/k is a cyclic extension of degree p^m. Put $\tilde{\sigma}_2=\tilde{\sigma}^{N''q}$, $\sigma_2=\sigma^{N''q}$, $l_2=l^{N''q}$ and $\tau'=\tau^{N''t'}$. Now we will prove the statement (ii) in the following two cases (I) and (II).

(I) The case where $\tilde{k}_1\supset\tilde{k}_2$. Let $r'\in\boldsymbol{Z}$ be such that $r'N''l^{N''-1}\equiv1 \pmod{p^{m-d'+m_0}}$. Applying (ii) of the following Lemma 3 to $\tilde{L}\supset\tilde{k}_1\supset\tilde{k}_2$, $\tilde{\sigma}_2|\tilde{L}$ and $A=\zeta_{m-d'}^{rr'}$, we see that there exists a $y_1\in\tilde{k}_1$ such that $\tilde{L}=\tilde{k}_1(z_1)$ and such that

$$z_1^{\tilde{\sigma}_2}=z_1\zeta_{m-d'}^{rr'}, \tag{1}$$

where $z_1=\sqrt[p^{m-d}]{y_1}$. Since $\tilde{L}\tilde{k}'=\tilde{K}'$, $y_1\notin(\tilde{k}')^p$ if m$-$d$>$0. On the other hand, since $\tilde{L}/k$ is an abelian extension, by [4], Proposition 2, there exists $a_0\in\tilde{k}_1$ such that

$$z_1^{\tilde{\sigma}-l}=a_0. \tag{2}$$

By making $(\tilde{\sigma}_2-1)$ operate on (2) and by using (1), we have $a_0^{\sigma_2-1}=1$, hence $a_0\in\tilde{k}_2$. Put $\tilde{\Sigma}_2=\tilde{\sigma}^{N''q-1}+\tilde{\sigma}^{N''q-2}l+\cdots+\tilde{\sigma}l^{N''q-2}+l^{N''q-1}\in\boldsymbol{Z}[G]$. Making $\tilde{\Sigma}_2$ operate on (2),

$$z_1^{\tilde{\sigma}_2-l_2}=a_0^{\Sigma_2}. \tag{3}$$

From this equality and (1), it follows that

$$(\zeta_{m-d'+m_0}^{rr'}y_1^{s_1})^{p^{m_0}}=a_0^{\Sigma_2}. \tag{4}$$

Put $\tilde{\Sigma}'=\tilde{\sigma}^{N''-1}+\tilde{\sigma}^{N''-2}l+\cdots+\tilde{\sigma}l^{N''-2}+l^{N''-1}\in\boldsymbol{Z}[G]$, $\tilde{\Sigma}=\Sigma(\tilde{k}/k)$, $z_2=z_1^{\tilde{\Sigma}'}$, $y_2=y_1^{\tilde{\Sigma}}$ and $a_1=a_0^{\tilde{\Sigma}}$. It follows from (2) that $z_2=z_1^{N''l^{N''-1}}B$ with some $B\in\tilde{k}_2^{\times}$. Put $b=a_1$ or $\zeta_{m-d'+m_0}^{rr'}y_1^{s_1}$ according as $m_0=0$ or not. Then by (1) and the fact that $a_0\in\tilde{k}_2$, we see that $b^{\tilde{\sigma}_2-1}=1$, hence $b\in\tilde{k}_2$. Note that $\tilde{k}_2=\tilde{k}$ if $m_0>0$. Put $y=y_2^s$ and $z=z_2^s$. Then by the definition of b, (2) and (4),

$$y=\zeta_{m-d'+m_0}^{N''l^{N-1}}(b^{s_2})^{\Sigma_2} \tag{5}$$

and

$$z^{\tilde{\sigma}-l}=a_1^s. \tag{6}$$

Since $[\tilde{K}':\tilde{k}']=p^{m-d}$, $y\notin(\tilde{k}')^p$ if $m-d>0$. Put $\Omega=\alpha^{q''-1}+\alpha^{q''-2}+\cdots+\alpha+1\in\boldsymbol{Z}[G]$, where $\alpha=\tilde{\sigma}^{N''q}$. By making Ω operate on (1), we have

$$z^{\tau'}=z\zeta_{m-d}^{N''l^{N-1}s_1s_2'}, \tag{7}$$

since $\tilde{\sigma}_1^{N''}=\tau'^{-1}$ on $\tilde{L}$. Put $a=b^{p^{m_0}}$ and $w=\zeta_m a$. Since $m-d'+m_0=n''+d$, by using (5), we have

$$z=\sqrt[pn]{w^{\Sigma}}. \tag{8}$$

By (4) and the definition of a, we see easily that $a=a_1$. Put $\tilde{\Sigma}_1=\tilde{\sigma}^{p'-1}+\tilde{\sigma}^{p'-2}l+\cdots+\tilde{\sigma}l^{p'-2}+l^{p'-1}\in \boldsymbol{Z}[G]$. By making it operate on (6) and using that $a_1=a$, we have $z^{\tilde{\sigma}_1-l_1}=(a^s)^{\Sigma_1}$. Since $(w^s)^{\Sigma_1}=\zeta_{m-d}^{slp'-1}(a^s)^{\Sigma_1}$, we have $z^{\tilde{\sigma}_1-l_1}=(w^s)^{\Sigma_1}\zeta_{m-d}^{-slp'-1}$. By this equality and (7), $z^{\tilde{\sigma}_1\tau't}=z^{l_1}(w^s)^{\Sigma_1}\zeta_{m-d}^{i}$ with $i=-sl^{p'-1}+N''l^{N-1}s_1s_2'l_1t$. Hence by the definitions of t and t',

$$z^{\gamma}=z^{l_1}(w^s)^{\Sigma_1}. \tag{9}$$

(II) The case where $\tilde{k}_1\subset\tilde{k}_2$. If $\tilde{k}=\tilde{k}_2$, then $\tilde{k}=\tilde{k}_1=\tilde{k}_2$, hence the case is contained in (I), so we may suppose that $\tilde{k}\neq\tilde{k}_2$, hence $m_0=0$. Put $\tilde{L}_2=\tilde{L}\tilde{k}_2$ and $\tilde{K}_2=\tilde{K}\tilde{k}_2$. There exists $y_2\in\tilde{k}_2$ such that $\tilde{L}_2=\tilde{k}_2(z_2)$, where $z_2=\sqrt[p^{m-d}]{y_2}$. Since $\tilde{K}'=\tilde{L}_2\tilde{k}'$, $y_2\notin(\tilde{k}')^p$ if $m-d>0$. We have

$$z_2^{\tau'}=z_2\zeta_{m-d}^{r_1} \tag{10}$$

with some $r_1\in\boldsymbol{N}$, $r_1\not\equiv 0 \pmod p$. Let $r_1'\in\boldsymbol{N}$ be such that $r_1r_1'\equiv -r \pmod p$, and put $z_1=z_2^{r'_1}$ and $y_1=y_2^{r'_1}$. Then $z_1=\sqrt[p^{m-d}]{y_1}$. By taking the r_1'-th power of (10),

$$z_1^{\tau'}=z_1\zeta_{m-d}^{-r}. \tag{11}$$

Since $\tilde{L}_2/k$ is abelian, by [4], Proposition 2, there exists $a\in\tilde{k}_2$ such that

$$z_1^{\tilde{\sigma}-l}=a. \tag{12}$$

By making $\tilde{\Sigma}_2$ operate on (12),

$$z_1^{\tilde{\sigma}_2-l_2}=a^{\Sigma_2}. \tag{13}$$

Since $\tilde{\sigma}_1^{N''}=\tau'^{-1}$ on $\tilde{L}$ and since $\tilde{\sigma}_2|\tilde{k}_2=1$, we have $\tilde{\sigma}_2=(\tau'^{-1})^{p^{d'-d}}$ on $\tilde{L}_2$. Hence by (11) and (13), we have $z_1^{1-l_2}=\zeta_{m-d'}^{-r}a^{\Sigma_2}$, so $y_1^{s_1}=\zeta_{m-d'}^{-r}a^{\Sigma_2}$, since $m_0=0$. Put $y=y_1^s$ and $z=z_1^s$. Then by the definition of r,

$$y=\zeta_{m-d}^{N''l^{N-1}}(a^{s_2})^{\Sigma_2} \tag{14}$$

and

$$z=\sqrt[p^{m-d}]{y}. \tag{15}$$

Since $[\tilde{K}':\tilde{k}']=p^{m-d}$, $y\notin(\tilde{k}')^p$ if $m-d>0$. By taking the s-th power of (11) and (12),

$$z^{\tau'}=z\zeta_{m-d}^{s_1l^{N-1}N''} \tag{16}$$

and

$$z^{\tilde{\sigma}-l}=a^s. \tag{17}$$

By making $\tilde{\Sigma}_1$ operate on (17),

$$z^{\tilde{\sigma}_1-l_1}=(a^s)^{\Sigma_1}. \tag{18}$$

Put $w=\zeta_m a$. Then, in the same way as in the proof of (i), using (18), (14) and (15), we have

$$z^{\tilde{\sigma}_1}=z^{l_1}(w^s)^{\Sigma_1}\zeta_{m-d}^{-l^{p'-1}s} \tag{19}$$

and

$$z=\sqrt[p^n]{w^{\Sigma}}\,. \tag{20}$$

By (16) and (19), $z^{\tilde{\sigma}_1\tau'^t}=z^{l_1}(w^s)^{\Sigma_1}\zeta_{m-d}^i$ with $i=s_1 l^{N-1}N'' t l_1-l^{p'-1}s$. Hence by the definitions of t and t', $z^{\gamma}=z^{l_1}(w^s)^{\Sigma_1}$, so γ satisfies the condition (*) in Lemma 1.

(B) The case where $n_1\neq n$. Then $\tilde{k}'=\tilde{k}$, $d=0$ and $m_0=n-m$.

(i) Put $y=\zeta_n b$. Then $w=y^{p^{n-m}}$. By assumption, $y^{\Sigma(\tilde{k}/k)}\notin(\tilde{k})^p$ if $m-d>0$, and $z=\sqrt[p^m]{y^{\Sigma(\tilde{k}/k)}}$. Since $(y^{\Sigma(\tilde{k}/k)})^{\sigma-l}=y^{1-l^N}$, by [4], Proposition 2, $\tilde{K}'/k$ is an abelian extension. Let $\tilde{\sigma}\in G(\tilde{K}'/k)$ be such that $\tilde{\sigma}|\tilde{k}=\sigma$. Then $z^{\tilde{\sigma}-l}=\zeta_m^r y^{(1-l^N)/p^m}$ $=\zeta_m^r w^{sp^{n_1-n}}$ with some $r\in\boldsymbol{Z}$. Let $\tau\in G(\tilde{K}'/\tilde{k})$ be such that $z^{\tau}=\zeta_m z$. Let $r'\in\boldsymbol{N}$ be such that $r'l+r\equiv 0 \pmod{p^m}$. Put $\gamma=\tilde{\sigma}\tau^{r'}$. Then $z^{\gamma}=z^l(w^s)^{p^{n_1-n}}$, hence γ satisfies the condition (*) in Lemma 1. Put $\tilde{\Sigma}=\gamma^{N-1}+\gamma^{N-2}l+\cdots+\gamma l^{N-2}+l^{N-1}\in \boldsymbol{Z}[G(\tilde{K}'/k)]$. By making it operate on the above equality, $z^{\gamma^N-l^N}=(w^{sp^{n_1-n}})^{\Sigma(\tilde{k}/k)}$, hence $z^{\gamma^N}=z$. Since $\gamma|\tilde{k}=\sigma$, this implies that the order of γ is N. Since $N\not\equiv 0 \pmod{p}$, K/k is a cyclic extension of degree p^m.

(ii) Put $\tilde{K}=K(\zeta_1)$. Then there exists $y\in\tilde{k}^{\times}$ such that $\tilde{K}=\tilde{k}(\sqrt[p^m]{y})$. Since $\tilde{K}/k$ is an abelian extension, by [4], Proposition 2, $y^{\sigma-l}=A^{p^m}$ with an $A\in\tilde{k}$. From this, it follows that $y^{\Sigma(\tilde{k}/k)}=y^{Nl^{N-1}}B^{p^m}$ with a $B\in\tilde{k}$. Since $Nl^{N-1}\not\equiv 0 \pmod{p}$, this implies that $\tilde{K}=\tilde{k}(\sqrt[p^m]{y^{\Sigma(\tilde{k}/k)}})$. Put $b=\zeta_n^{-1}y$, $a=b^{p^{n-m}}$ and $w=\zeta_m a$. Then $w=y^{p^{n-m}}$ and $\tilde{K}=\tilde{k}(z)$, where $z=\sqrt[p^n]{w^{\Sigma(\tilde{k}/k)}}$. Since K/k is a unique subextension of $\tilde{K}/k$ of p-power degree such that $K(\zeta_1)=\tilde{K}$, K is the sub-field of $\tilde{K}$ fixed by γ. This completes the proof of Lemma 1.

COROLLARY. *Let notations and assumptions be as in* (i) *of Lemma* 1, *and moreover let* $w'\in\tilde{k}'^{\times}$ *be such that* $w'=wA^{p^n}$ *with some* $A\in(\tilde{k}')^{\times}$. Put $z'=\sqrt[p^n]{w'^{\Sigma(\tilde{k}/k)}}$. *Then* $\tilde{K}'=\tilde{k}'(z')$ *and* $z'^{\gamma-l_1}=(w'^{sp^{n_1-n}})^{\Sigma(k_1/k)}$.

PROOF. Put $\Sigma=\Sigma(\tilde{k}'/k)$ and $\Sigma_1=\Sigma(k_1/k)$. Since $w'^{\Sigma}=w^{\Sigma}(A^{\Sigma})^{p^n}$, it is obvious that $\tilde{K}'=\tilde{k}'(z')$ and that $z'=zA^{\Sigma}\zeta_n^i$ with some $i\in\boldsymbol{Z}$. Hence, by using $\Sigma=\Sigma_1\cdot\Sigma(\tilde{k}'/k_1)$, $z'^{\gamma-l_1}=z^{\gamma-l_1}A^{\Sigma(\sigma_1-l_1)}=(w^{sp^{n_1-n}})^{\Sigma_1}(A^{\Sigma_1})^{1-l^N}=(w'^{sp^{n_1-n}})^{\Sigma_1}$, so $z'^{\gamma-l_1}=(w'^{sp^{n_1-n}})^{\Sigma_1}$. (q. e. d.)

REMARK 1. (1) If $k'\neq k$, $k'\neq k_1$ and $m-d>0$, then the condition in Lemma 1 that $w^{\Sigma(\tilde{k}'/k)}\notin(\tilde{k}')^{p^{n-(m-d)+1}}$ is equivalent to that $N_{\tilde{k}_2/\tilde{k}}(b)^{\Sigma(\tilde{k}/k)}\notin(\tilde{k}^{\times})^p\langle\zeta_{n_0}\rangle$. If $k'\neq k$, $k_1=k'$ and $m-d>0$, then the condition always holds.

(2) Let w and w' be as in (i) of Lemma 1. Assume that $n=n_1$. Then w

and w' define the same field K if and only if there exist $t\in \boldsymbol{Z}$, $t\not\equiv 0 \pmod{p}$, and $c\in\tilde{k}'$ such that $c^{\sigma_1-l_1}=(w'^t/w)^{s\Sigma(k_1/k)}$.

LEMMA 2. *Let notations and assumptions be as in the case* (A) *in the proof of Lemma* 1. *Then* $s_2\equiv s_2' \pmod{p^{m-d-d_1}}$.

PROOF. When $\tilde{k}'=\tilde{k}$, we have $s_2=s_2'=1$. Hence we may assume that $\tilde{k}'\neq\tilde{k}$. We will prove the assertion in the following two cases (I) and (II).

(I) The case where $\tilde{k}_1\supset\tilde{k}_2$. Put $s_1'=(1-l^N)/(1-l^{N''p'})p''$. Then $s_1'\in\boldsymbol{Z}$ and $s_1'\not\equiv 0 \pmod{p}$. We have easily $N_{\tilde{k}'/\tilde{k}_1}(\zeta_n)=\zeta_n^{1+\tilde{l}_1+\cdots+\tilde{l}_1^{p''-1}}=\zeta_{n-d_1}^{s_1'}$, where $\tilde{l}_1=l^{p'N''}$. On the other hand, since ζ_n is a root of an irreducible polynomial $X^{p''}-\zeta_{n-d_1}$ over $\tilde{k}_1$, we have $N_{\tilde{k}'/\tilde{k}_1}(\zeta_n)=\zeta_{n-d_1}$ or $-\zeta_{n-d_1}=\zeta_{n-d_1}^{1+p^{n-d_1-1}}$ according as $p\neq 2$ or $p=2$. Hence $s_1'\equiv 1 \pmod{p^{n-d_1-1}}$. If $n-d_1=m-d-d_1$, then $n=m$ and $d=0$, so $\tilde{k}_2=\tilde{k}'$, hence $\tilde{k}_1=\tilde{k}_2=\tilde{k}'=\tilde{k}$, since $\tilde{k}_1\supset\tilde{k}_2$; this is a contradiction. Hence $n-d_1-1\geqq m-d-d_1$. Therefore $s_1'\equiv 1 \pmod{p^{m-d-d_1}}$. Since $s_1'=s_2/s_2'$, this implies the assertion.

(II) The case where $\tilde{k}_1\subset\tilde{k}_2$. We have $N_{\tilde{k}'/\tilde{k}_2}(\zeta_n)=\zeta_n^{1+\tilde{l}_2+\cdots+\tilde{l}_2^{q'-1}}=\zeta_{n-d''}^{s_2}$, where $\tilde{l}_2=l^{N''q}$. On the other hand, since ζ_n is a root of an irreducible polynomial $X^{q'}-\zeta_{n-d''}$ over $\tilde{k}_2$, we have $N_{\tilde{k}'/\tilde{k}_2}(\zeta_n)=\zeta_{n-d''}$ or $\zeta_{n-d''}^{1+p^{n-d''-1}}$ according as $p\neq 2$ or $p=2$. Hence $s_2\equiv 1 \pmod{p^{n-d''-1}}$. If $n-d''=m-d-d_1$, then $n=m$ and $d'=0$, so $\tilde{k}_1=\tilde{k}_2=\tilde{k}'=\tilde{k}$, since $\tilde{k}_1\subset\tilde{k}_2$; this is a contradiction, hence $n-d''-1\geqq m-d-d_1$. Therefore $s_2\equiv 1 \pmod{p^{m-d-d_1}}$. This implies the assertion.

The following Lemma 3 is well known.

LEMMA 3 (Albert). *Let p be a prime number and let k be a field of characteristic different from p. Let m, $n\in\boldsymbol{N}\cup\{0\}$, and assume that $\zeta_m\in k$. Let K/k be a cyclic extension of degree p^n. Then the following two statements* (i) *and* (ii) *hold:*

(i) *There exists a cyclic extension L of k of degree p^{n+m} containing K, if and only if there exists an $A\in K$ such that $N_{K/k}(A)=\zeta_m$.*

(ii) *Let L/k be a cyclic extension of degree p^{n+m} containing K and let $\tilde{\sigma}$ be a generator of $G(L/k)$. Then for any $A\in K$ satisfying $N_{K/k}(A)=\zeta_m$, there exists a $y\in K$ such that $L=K(z)$ and $z^{\tilde{\sigma}-1}=A$, where $z=\sqrt[p^m]{y}$.*

§ 2. Theorems.

For the proof of Theorem 5, the cyclic case is essential (see Theorem 4 below).

For a field k and a prime divisor $\mathfrak{p}$ of k, let k_{sep} and $k_{\mathfrak{p},\mathrm{sep}}$ denote the maximal separable algebraic extensions of k and $k_{\mathfrak{p}}$ such that $k_{\mathrm{sep}}\subset k_{\mathfrak{p},\mathrm{sep}}$, respectively. Here a prime divisor of k means an equivalence class of discrete valuations of k, and $k_{\mathfrak{p}}$ denotes the completion of k with respect to $\mathfrak{p}$. In the following, all separable algebraic extensions of k and $k_{\mathfrak{p}}$ are assumed to be contained in k_{sep} and $k_{\mathfrak{p},\mathrm{sep}}$ respectively. For a finite extension K of k in k_{sep}, let $\mathfrak{p}_K$ denote the restriction of the valuation of $k_{\mathfrak{p},\mathrm{sep}}$ to K, and $K_\mathfrak{p}$ the completion of K with respect to $\mathfrak{p}_K$, i.e., $K_\mathfrak{p}=Kk_\mathfrak{p}$ in $k_{\mathfrak{p},\mathrm{sep}}$. Then we have the following

THEOREM 4. *Let p, k, ζ_i, n and k' be as in the beginning of* § 1, *and let S be a finite set of prime divisors of k. Assume that there exists a prime divisor $\mathfrak{q}$ of k such that $\mathfrak{q}\notin S$ and $\zeta_n\in k_\mathfrak{q}$. Let G be a cyclic group of order p^n. For each $\mathfrak{p}\in S$, let a pair $(K^\mathfrak{p}, j_\mathfrak{p})$ of a cyclic extension $K^\mathfrak{p}$ of $k_\mathfrak{p}$ of degree $p^{m_\mathfrak{p}}$ with $0\leqq m_\mathfrak{p}\leqq n$ and an injective homomorphism $j_\mathfrak{p}$: $G(K^\mathfrak{p}/k_\mathfrak{p})\to G$ be given. Then there exists a cyclic extension K of k of degree p^n satisfying the following three conditions:*

(i) *$K_\mathfrak{p}=K^\mathfrak{p}$ for all $\mathfrak{p}\in S$.*

(ii) *There exists an isomorphism j from $G(K/k)$ onto G such that $j_\mathfrak{p}=j\circ\mathrm{Res}_\mathfrak{p}$, where $\mathrm{Res}_\mathfrak{p}$: $G(K_\mathfrak{p}/k_\mathfrak{p})\to G(K/k)$ is the restriction from $K_\mathfrak{p}$ to K.*

(iii) *$K\cap k'=k$.*

PROOF. We use the notations in the beginning of § 1. If $n_0\geqq n$, then Theorem 4 is easily verified, so we may assume that $n_0<n$. Put $\tilde{k}_\mathfrak{p}=k_\mathfrak{p}(\zeta_1)$, $k^\mathfrak{p}=k_\mathfrak{p}\cap\tilde{k}'$, $N_\mathfrak{p}=[\tilde{k}'_\mathfrak{p}:k_\mathfrak{p}]$ and $N'_\mathfrak{p}=[k^\mathfrak{p}: k]$. Then $N=N'_\mathfrak{p}N_\mathfrak{p}$. Identify $G(\tilde{k}'_\mathfrak{p}/k_\mathfrak{p})$ and $G(\tilde{k}'/k^\mathfrak{p})$ in the natural way. Put $\sigma_\mathfrak{p}=\sigma^{N'_\mathfrak{p}}\in G(\tilde{k}'_\mathfrak{p}/k_\mathfrak{p})$ and $l_\mathfrak{p}=l^{N'_\mathfrak{p}}$. For any subextension S/M of $\tilde{k}'_\mathfrak{p}/k_\mathfrak{p}$, define $\Sigma(S/M)=\sum_{i=0}^{g-1}\sigma_1^{g-1-i}l_1^i\in \boldsymbol{Z}[G(\tilde{k}'_\mathfrak{p}/k_\mathfrak{p})]$, where $\sigma_1=\sigma_\mathfrak{p}^{[M:k_\mathfrak{p}]}$, $l_1=l_\mathfrak{p}^{[M:k_\mathfrak{p}]}$ and $g=[S:M]$. Identify $\Sigma(S/M)$ and $\Sigma(S\cap\tilde{k}'/M\cap\tilde{k}')$ in the natural way. Put $k_1^\mathfrak{p}=K^\mathfrak{p}\cap k'_\mathfrak{p}$, $p'_\mathfrak{p}=p^{d_\mathfrak{p}}=[k_1^\mathfrak{p}:k_\mathfrak{p}]$ and $\tilde{k}_2^\mathfrak{p}=\tilde{k}_\mathfrak{p}(\zeta_{m_\mathfrak{p}-d_\mathfrak{p}})$. Let $\nu_\mathfrak{p}\in\boldsymbol{N}$ be such that $\zeta_{\nu_\mathfrak{p}}\in\tilde{k}_\mathfrak{p}$ and $\zeta_{\nu_\mathfrak{p}+1}\notin\tilde{k}_\mathfrak{p}$. For each $\mathfrak{p}\in S$, put $m_{0\mathfrak{p}}=\mathrm{Max}(0, \nu''_\mathfrak{p}-(m_\mathfrak{p}-d_\mathfrak{p}))$, where $\nu''_\mathfrak{p}=\mathrm{Min}(\nu_\mathfrak{p}, n)$. Then by Lemma 1, for each $\mathfrak{p}\in S$, there exists $b_\mathfrak{p}\in\tilde{k}_2^\mathfrak{p}$ satisfying the following: $w_\mathfrak{p}^{\Sigma(\tilde{k}'_\mathfrak{p}/k_\mathfrak{p})}\notin(\tilde{k}'_\mathfrak{p})^{p^{n-(m_\mathfrak{p}-d_\mathfrak{p})+1}}$ if $m_\mathfrak{p}-d_\mathfrak{p}>0$, where $a_\mathfrak{p}=b_\mathfrak{p}^{p^{m_{0\mathfrak{p}}}}$ and $w_\mathfrak{p}=\zeta_{m_\mathfrak{p}}a_\mathfrak{p}$; put $z_\mathfrak{p}=\sqrt[p^n]{w_\mathfrak{p}^{\Sigma_\mathfrak{p}}}$ and $\tilde{K}'^\mathfrak{p}=\tilde{k}'_\mathfrak{p}(z_\mathfrak{p})$, where $\Sigma_\mathfrak{p}=\Sigma(\tilde{k}'_\mathfrak{p}/k_\mathfrak{p})$, then $\tilde{K}'^\mathfrak{p}/k_\mathfrak{p}$ is an abelian extension; let $\gamma_\mathfrak{p}\in G(\tilde{K}'^\mathfrak{p}/k_\mathfrak{p})$ be such that

$$(1)\qquad \begin{cases} z_\mathfrak{p}^{\gamma_\mathfrak{p}}=z_\mathfrak{p}^{l_{\mathfrak{p}1}}(w_\mathfrak{p}^s)^{\Sigma_{\mathfrak{p}1}} \\ \gamma_\mathfrak{p}|\tilde{k}'_\mathfrak{p}=\sigma_{\mathfrak{p}1}, \end{cases}$$

where $l_{\mathfrak{p}1}=l_\mathfrak{p}^{p'_\mathfrak{p}}$, $\sigma_{\mathfrak{p}1}=\sigma_\mathfrak{p}^{p'_\mathfrak{p}}=\sigma^{N'_\mathfrak{p}p'_\mathfrak{p}}$ and $\Sigma_{\mathfrak{p}1}=\Sigma(k_1^\mathfrak{p}/k_\mathfrak{p})$, then $K^\mathfrak{p}$ is the subfield of $\tilde{K}'^\mathfrak{p}$ fixed by $\gamma_\mathfrak{p}$; there exists a unique $\alpha_\mathfrak{p}\in G(\tilde{K}'^\mathfrak{p}/k_\mathfrak{p})$ satisfying

$$(2)\qquad \begin{cases} z_\mathfrak{p}^{\alpha_\mathfrak{p}}=z_\mathfrak{p}^{l_\mathfrak{p}}(a_\mathfrak{p}^s) \\ \alpha_\mathfrak{p}|\tilde{k}'_\mathfrak{p}=\sigma_\mathfrak{p}, \end{cases}$$

then $\alpha_\mathfrak{p}|K^\mathfrak{p}$ is a generator of $G(K^\mathfrak{p}/k_\mathfrak{p})$. Let $\beta_0\in G$ be a generator of G, and for each $\mathfrak{p}\in S$, let $\beta_\mathfrak{p}\in G(K^\mathfrak{p}/k_\mathfrak{p})$ be a generator of $G(K^\mathfrak{p}/k_\mathfrak{p})$ such that $j_\mathfrak{p}(\beta_\mathfrak{p})=\beta_0^{p^{n-m_\mathfrak{p}}}$. Then there exists $t_\mathfrak{p}\in\boldsymbol{N}$, $t_\mathfrak{p}\not\equiv 0$ (mod p), such that $\beta_\mathfrak{p}=\alpha_\mathfrak{p}^{-l_\mathfrak{p}t_\mathfrak{p}s'}|K^\mathfrak{p}$, where $s'\in\boldsymbol{Z}$ is such that $ss'\equiv 1$ (mod p^n). Let $t_\mathfrak{q}=1$, and let $w_\mathfrak{q}$ be a prime element of $k_\mathfrak{q}$.

Since $\mathfrak{p}_{\tilde{k}'}^{\sigma^i}$ with $\mathfrak{p}\in S$ and $i=0, 1, \cdots, N'_\mathfrak{p}-1$ are distinct prime divisors of $\tilde{k}'$, by the approximation theorem, we see easily that there exists a $w\in\tilde{k}'$ such that

$$(w^{t_\mathfrak{p}})^{\Sigma_{\mathfrak{p}0}}\equiv w_\mathfrak{p} \pmod{\mathfrak{p}^{r}_{\tilde{k}'_\mathfrak{p}}} \tag{3}$$

for all $\mathfrak{p}\in S\cup\{\mathfrak{q}\}$, where r is a sufficiently large number and $\Sigma_{\mathfrak{p}0}=\Sigma(k^\mathfrak{p}/k)$. Since $w_\mathfrak{q}\notin k_\mathfrak{q}^p$ and since $k_\mathfrak{q}=\tilde{k}'_\mathfrak{q}$, $w^\Sigma\notin(\tilde{k}')^p$, where $\Sigma=\Sigma(\tilde{k}'/k)$. Put $z=\sqrt[p^n]{w^\Sigma}$ and $\tilde{K}'=\tilde{k}'(z)$. Then by Lemma 1, $\tilde{K}'/k$ is an abelian extension of degree Np^n; let $\gamma\in G(\tilde{K}'/k)$ be such that

$$\begin{cases} z^\gamma=z^l w^s \\ \gamma\,|\,\tilde{k}'=\sigma\,, \end{cases} \tag{4}$$

and let K be the sub-field of $\tilde{K}'$ fixed by γ, then K/k is a cyclic extension of degree p^n such that $K\cap k'=k$. By (3), we have $(w^{t_\mathfrak{p}})^\Sigma\equiv w_\mathfrak{p}^{\Sigma_\mathfrak{p}} \pmod{\mathfrak{p}^{r}_{\tilde{k}'_\mathfrak{p}}}$, hence $\tilde{K}'_\mathfrak{p}=\tilde{K}'^\mathfrak{p}$ for any $\mathfrak{p}\in S$. Let $\tau\in G(\tilde{K}'/k)$ be such that

$$\begin{cases} z^\tau=\zeta_n z \\ \tau\,|\,\tilde{k}'=1\,, \end{cases} \tag{5}$$

and put $\beta=\tau\,|\,K$. Then β is a generator of $G(K/k)$. In the following, we will prove that $K_\mathfrak{p}=K^\mathfrak{p}$ and that $\beta_\mathfrak{p}\,|\,K=\beta^{p^{n-m_\mathfrak{p}}}$ for all $\mathfrak{p}\in S$. For simplicity, put $m=m_\mathfrak{p}$, $k_0=k^\mathfrak{p}$, $k_1=k_1^\mathfrak{p}$, $d=d_\mathfrak{p}$, $w_0=w^{t_\mathfrak{p}}$, $z_0=z^{t_\mathfrak{p}}$, $p'=p'_\mathfrak{p}$, $\Sigma_0=\Sigma_{\mathfrak{p}0}$ and $\Sigma_1=\Sigma_{\mathfrak{p}1}$. Let L/k and U/k be the sub-extensions of K/k of degree p^{n-m} and p^{n-m+d}, respectively. Put $K_0=Kk_0$, $L_0=Lk_0$, $\tilde{L}'=L\tilde{k}'$, $U_0=Uk_0$ and $\tilde{U}'=U\tilde{k}'$. Let M be the decomposition field of $\mathfrak{p}_{\tilde{K}'}$, with respect to k. Then $M\cap\tilde{k}'=k_0$ and $M\tilde{k}'=\tilde{U}'$, since $\tilde{K}'_\mathfrak{p}=\tilde{K}'^\mathfrak{p}$. Hence $[\tilde{U}' : M]=[\tilde{k}' : k_0]$. By (3),

$$w_0^{\Sigma_0}=w_\mathfrak{p}A^{p^n} \tag{6}$$

with some $A\in\tilde{k}'_\mathfrak{p}$, hence $w_0^\Sigma=w_\mathfrak{p}^{\Sigma_\mathfrak{p}}(A^{\Sigma_\mathfrak{p}})^{p^n}$. This implies that

$$z_0=z_\mathfrak{p}A^{\Sigma_\mathfrak{p}}\zeta_n^j \tag{7}$$

with some $j\in\boldsymbol{Z}$. By making $(\alpha_\mathfrak{p}-l_\mathfrak{p})$ operate on (7) and by using (2), we have $z_0^{\alpha_\mathfrak{p}-l_\mathfrak{p}}=(a_\mathfrak{p}A^{p^n})^s=\zeta_m^{-s}(w_\mathfrak{p}A^{p^n})^s$, hence by (6),

$$z_0^{\alpha_\mathfrak{p}-l_\mathfrak{p}}=\zeta_m^{-s}(w_0^s)^{\Sigma_0}\,. \tag{8}$$

On the other hand, by (4), $z_0^{\gamma-l}=w_0^s$. By making Σ_0 operate on this equality,

$$z_0^{\gamma_1-l_\mathfrak{p}}=(w_0^s)^{\Sigma_0}, \tag{9}$$

where $\gamma_1=\gamma^{N'_\mathfrak{p}}$. Let $\tau_0\in G(\tilde{K}'/\tilde{k}')$ be such that $z_0^{\tau_0}=\zeta_n z_0$, and put $\delta=\gamma_1\tau_0^{ip^{n-m}}$, where $i\in\boldsymbol{Z}$ is such that $il_\mathfrak{p}\equiv-s \pmod{p^n}$. Then by (9), $z_0^{\delta-l_\mathfrak{p}}=\zeta_m^{-s}(w_0^s)^{\Sigma_0}$ and $\delta\,|\,\tilde{k}'=\sigma^{N'_\mathfrak{p}}$. From this and (8), it follows that

$$\alpha_\mathfrak{p}\,|\,\tilde{K}'=\delta\,. \tag{10}$$

We see that M is the sub-field of $\tilde{U}'$ fixed by δ. In fact, by (10), $M \subset M'$, where M' is the sub-field of $\tilde{U}'$ fixed by δ. Since $[\tilde{U}' : M] = [\tilde{k}' : k_0]$, it is enough to show that the order of $\delta | \tilde{U}'$ is $[\tilde{k}' : k_0]$, and this fact follows from $\delta | \tilde{k}' = \sigma^{N'_{\mathfrak{p}}}$ and $\delta | U_0 = \tau_0^{ip^{n-m}} | U_0$. Hence $M = M'$. By this fact we see easily that $M \cap U_0 = L_0$, hence $K_0 \cap M = L_0$. Since $[M : L_0] = p'$, we have $K_1 = K_0 M$, where K_1 is the sub-field of $\tilde{K}'$ fixed by $\gamma_1^{p'}$, hence $K_1 = KM$, so

$$(K_1)_{\mathfrak{p}} = K_{\mathfrak{p}}\,. \tag{11}$$

By using (6), (1) and Corollary to Lemma 1,

$$\begin{cases} z_0^{\gamma_{\mathfrak{p}} - l_{\mathfrak{p}}^{p'}} = (w_0^{s\Sigma_0})^{\Sigma_1} \\ \gamma_{\mathfrak{p}} | \tilde{k}' = \sigma^{N'_{\mathfrak{p}} p'}. \end{cases} \tag{12}$$

On the other hand, by making $t_{\mathfrak{p}} \tilde{\Sigma}_1 \Sigma_0$ operate on (4), $z_0^{\gamma_1^{p'} - l_{\mathfrak{p}}^{p'}} = (w_0^{s\Sigma_0})^{\Sigma_1}$, where $\tilde{\Sigma}_1 = \sum_{i=0}^{p'-1} \gamma_1^{p'-1-i} l_{\mathfrak{p}}^i$. From this and (12), it follows that $\gamma_{\mathfrak{p}} | \tilde{K}' = \gamma_1^{p'}$. Therefore $(K_1)_{\mathfrak{p}} = K^{\mathfrak{p}}$. Hence by (11), $K_{\mathfrak{p}} = K^{\mathfrak{p}}$. By (10), $\alpha_{\mathfrak{p}} | K = \tau_0^{ip^{n-m}} | K$, so $\beta_{\mathfrak{p}} | K = \tau_0^{t_{\mathfrak{p}} p^{n-m}} | K = \tau^{p^{n-m}} | K$, since $\tau = \tau_0^{t_{\mathfrak{p}}}$. Therefore

$$\beta_{\mathfrak{p}} | K = \beta^{p^{n-m}_{\mathfrak{p}}}. \tag{13}$$

Let $j : G(K/k) \to G$ be the isomorphism such that $j(\beta) = \beta_0$. Then by (13), we see that $j_{\mathfrak{p}} = j \circ \mathrm{Res}_{\mathfrak{p}}$. This completes the proof of Theorem 4.

REMARK 2. *Theorem* 4 *holds also when* $\mathrm{ch}(k) = p$, if we remove the assumptions in Theorem 4 that k contains a primitive 4-th root of unity if $p = 2$ and that $\zeta_n \in k_{\mathfrak{q}}$. We can prove easily the statement, by using Sätze 12 and 13 of Witt [8], and the approximation theorem.

By Theorem 4 and Remark 2, we have the following

THEOREM 5, *Let k be a field, S a finite set of prime divisors of k, and G a finite abelian group of type $(p_1^{m_1}, p_2^{m_2}, \cdots, p_t^{m_t})$. Then an imbedding problem $P\{k, G, S, (K^{\mathfrak{p}}, j_{\mathfrak{p}})\ (\mathfrak{p} \in S)\}$ has a solution if the following two conditions are satisfied:*

(i) *There exist t distinct prime divisors $\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_t$ of k outside S such that $\zeta(p_i^{m_i}) \in k_{\mathfrak{q}_i}$ if $p_i \neq \mathrm{ch}(k)$.*

(ii) *If* $\exp(G)$ *is divisible by* 4 *and if* $\mathrm{ch}(k) \neq 2$, *then* $\zeta(4) \in k$.

PROOF. Let $G = \prod_{i=1}^{t} G_i$ (direct product), where G_i are cyclic subgroups of G of order $p_i^{m_i}$ for $1 \leqq i \leqq t$. Put $K^{\mathfrak{q}_i} = k_{\mathfrak{q}_i}(\sqrt[p_i^{m_i}]{\pi_i})$ or $k_{\mathfrak{q}_i}(\theta_i)$ according as $\mathrm{ch}(k) \neq p_i$ or not, for $1 \leqq i \leqq t$, where π_i is a prime element of $k_{\mathfrak{q}_i}$ and θ_i is the Witt vector of length m_i such that $\mathcal{P}_i(\theta_i) = (\pi_i^{-1}, 0, \cdots, 0)$. Here $\mathcal{P}_i(\alpha) = (\alpha_0^{p_i}, \alpha_1^{p_i}, \cdots, \alpha_{m_i-1}^{p_i}) - (\alpha_0, \alpha_1, \cdots, \alpha_{m_i-1})$ for any Witt vector $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{m_i-1})$ of length m_i. Then by the condition (i) and Satz 13 of Witt [8], we see that $K^{\mathfrak{q}_i}/k_{\mathfrak{q}_i}$ is a cyclic extension of degree $p_i^{m_i}$. Let $j_{\mathfrak{q}_i} : G(K^{\mathfrak{q}_i}/k_{\mathfrak{q}_i}) \to G_i$ be any isomorphism.

By Galois theory, we see easily that Theorem 4 and Remark 2 imply that there exists a pair (K, j) of an abelian extension K of k and an isomorphism j of $G(K/k)$ *into* G satisfying $K_{\mathfrak{p}}=K^{\mathfrak{p}}$ and $j_{\mathfrak{p}}=j\circ \mathrm{Res}_{\mathfrak{p}}$ for any $\mathfrak{p}\in S\cup\{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\}$. Since $j_{\mathfrak{q}_i}$: $G(K^{\mathfrak{q}_i}/k_{\mathfrak{q}_i})\cong G_i$ for $1\leqq i\leqq t$, we see that j is the isomorphism of $G(K/k)$ *onto* G. This completes the proof of Theorem 5.

On the condition (i) of Theorem 5, we have the following

Proposition 6. *Let k be a finite algebraic number field or a field finitely generated over a field k_0 with transcendental degree$\geqq 1$, and let S be a finite set of prime divisors of k. Let p be a prime number different from the characteristic of k. Then for any $n\in \boldsymbol{N}$, there exists a prime divisor $\mathfrak{q}$ of k such that $\mathfrak{q}\notin S$ and such that $k_{\mathfrak{q}}$ contains a primitive p^n-th root of unity ζ_n.*

Proof. If k is a finite algebraic number field, then the assertion is a direct consequece of Čebotarev's density theorem or Dirichlet's theorem of the arithmetic progression. Now let k be finitely generated over k_0 with transcendental degree$\geqq 1$. Then there exist a subfield k_1 of k and an element x of k, transcendental over k_1, such that k is a finite algebraic extension of $k_1(x)$. Hence we may suppose that $k=k_1(x)$. If $\zeta_n\in k_1$, then for any prime divisor $\mathfrak{q}$ of k, $\zeta_n\in k_{\mathfrak{q}}$. Now suppose that $\zeta_n\notin k_1$, and let $f_m(X)\in k_1[X]$ be a monic minimal polynomial of ζ_m over k_1 for any $m\geqq n$. Then there exist infinitely many $f_m(X)$. Let $\mathfrak{p}_m\notin S$ be a prime divisor of k, trivial over k_1, corresponding to $f_m(X)$. Then residue field of $k_{\mathfrak{p}_m}$ is $k_1(\zeta_m)$. Therefore by Hensel's lemma, $\zeta_m\in k_{\mathfrak{p}_m}$, so $\zeta_n\in k_{\mathfrak{p}_m}$. This completes the proof of Proposition 6.

Remark 3. (1) In view of the proof of Theorem 4, we see that the assumption of the existence of $\mathfrak{q}$ in Theorem 4 can be replaced by a weaker condition: *There exists a cyclic extension $K^{\mathfrak{q}}/k_{\mathfrak{q}}$ of degree p^n such that $K^{\mathfrak{q}}\cap\tilde{k}'_{\mathfrak{q}}=k_{\mathfrak{q}}$ with a prime divisor $\mathfrak{q}\notin S$.* By [4], Corollary to Proposition 3, this condition is equivalent to that $N_{\tilde{k}'_{\mathfrak{q}}/\tilde{k}_{\mathfrak{q}}}(\tilde{k}'_{\mathfrak{q}})^{\Sigma(\tilde{k}_{\mathfrak{q}}/k_{\mathfrak{q}})}\not\subset\langle\zeta_{\nu_{\mathfrak{q}}}\rangle\tilde{k}_{\mathfrak{q}}^p$ with a prime divisor $\mathfrak{q}\notin S$. The condition (i) of Theorem 5 can be also weakened in the same way.

(2) When k is a finite algebraic number field, the proof of Theorem 4 is also valid for a finite set S of prime divisors containing *infinjte* prime divisors of k if it is slightly modified, and so is Theorem 5.

References

[1] E. Artin and J. Tate, Class Field Theory, Benjamin, New York-Amsterdam, 1967.

[2] W. Grunwald, Ein allgemeines Existenztheorem für algebraische Zahlkörper, J. Reine Angew. Math., **169** (1933), 103-107.

[3] H. Hasse, Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. Reine Angew. Math., **188** (1950), 40-64.

[4] H. Miki, On $\mathbf{Z}_p$-extensions of complete p-adic power series fields and function fields, J. Fac. Sci. Univ. Tokyo Sec. IA, **21** (1974), 377-393.

[5] J. Neukirch, Eine Bemerkung zum Existenzsatz von Grunwald-Hasse-Wang, J. Reine

Angew. Math., **268/269** (1976), 315-317.

[6] S. Wang, On Grunwald's theorem, Ann. of Math., **51** (1950), 471-484.

[7] G. Whaples, Non-analytic class field theory and Grunwald's theorem, Duke Math. J., **9** (1942), 455-473.

[8] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grade p^n, J. Reine Angew. Math., **176** (1936), 126-140.

Hiroo MIKI
Department of Mathematics
Faculty of Engineering
Yokohama National University
Tokiwadai, Hodogaya-ku
Yokohama, Japan