# ON GALOIS GROUPS OF LOCAL FIELDS

BY

KENKICHI IWASAWA

Let $p$ be a prime number, $Q_p$ the field of $p$-adic numbers, and $\Omega$ an algebraic closure of $Q_p$. In the present paper, we take a finite extension $k$ of $Q_p$ in $\Omega$ as the ground field and study the structure of the Galois group $G(\Omega/k)$ of the extension $\Omega/k$. Let $V$ be the ramification field of $\Omega/k$, i.e. the composite of all finite tamely ramified extensions of $k$ in $\Omega$, and let $G(\Omega/V)$ and $G(V/k)$ denote the Galois groups of the extensions $\Omega/V$ and $V/k$ respectively. We shall first determine the structure of the groups $G(V/k)=G(\Omega/k)/G(\Omega/V)$, and $G(\Omega/V)$ and show that the group extension $G(\Omega/k)/G(\Omega/V)$ splits. Our main result is, then, to describe explicitly the effect of inner automorphisms of $G(\Omega/k)$ on the factor group of $G(\Omega/V)$ modulo its commutator subgroup, i.e., on the Galois group $G(V'/V)$ of the maximal abelian extension $V'$ of $V$ in $\Omega$. This is, of course, not sufficient to determine the structure of the group $G(\Omega/k)$ completely; to do that, we still have to find the effect of inner automorphisms of $G(\Omega/k)$ on the normal subgroup $G(\Omega/V)$ itself. However, it gives us some insight into the structure of $G(\Omega/k)$; and we hope it will help somehow, in the future, in the study of the group $G(\Omega/k)$ as well as in that of the Galois groups of algebraic number fields.

An outline of the paper is as follows: in §1 we prove some group-theoretical lemmas which will be used later. In §2 we study the behavior of the Galois group of a certain type of finite tamely ramified Galois extension $E$ of $k$ acting on the multiplicative group of $E$. Using those results, we then prove in §3 the properties of $G(\Omega/k)$ as mentioned above(1).

## 1. Group-theoretical preparations

1.1. Let $q$ be a power of a prime number $p$: $q=p^{f_0}$, $f_0\geqq 1$. In sections 1.1 and 1.2, we shall denote by $G$ a finite group of order $n=ef$ generated by two elements $\sigma$ and $\tau$ satisfying the relations

$$\sigma^f = 1, \qquad \tau^e = 1, \qquad \sigma\tau\sigma^{-1} = \tau^q. \tag{1.1}$$

If such a group $G$ exists, $e$ and $f$ satisfy the congruence relation

$$q^f \equiv 1 \bmod e. \tag{1.2}$$

Hence, in particular, $e$ must be an integer prime to $p$. Conversely, if $e$ and $f$ are integers $\geqq 1$ satisfying (1.2), there exists, up to isomorphisms, a unique finite group $G$ of order $n=ef$ as described above.

Received by the editors March 13, 1955.

(1) For the structure of Galois groups of $p$-extensions of $k$, cf. [5; 8].

Let $G$ be such a finite group of order $n=ef$. We denote by $GF(q^f)$ the finite field with $q^f$ elements and by $\eta$ a primitive $e$th root of unity in $GF(q^f)$. According to (1.2), the field $GF(q^f)$ certainly contains such an $\eta$. For any integer $i$, we then make the additive group of $GF(q^f)$ a $G$-module $A_i$ by putting

$$\sigma a = a^q, \qquad \tau a = \eta^i a$$

for any $a$ in $GF(q^f)$. Obviously $A_i$ is a $G$-module with dimension $ff_0$ over the prime field $GF(p)$ of $GF(q^f)$, and we denote by $A_i'$ the $G$-module over the algebraic closure $\Omega_p$ of $GF(p)$ obtained from $A_i$ by extending the scalar field $GF(p)$ to $\Omega_p$. $A_i'$ then contains an $\Omega_p$-basis $a_j'$ indexed by residue classes $j$ mod $ff_0$, such that

$$\sigma a_j' = a_{j-f_0}', \qquad \tau a_j' = \eta^{ip^j} a_j' \text{(2)}.$$

In the following, we shall denote by $R_p$ and $R_p'$ the group rings of $G$ over the fields $GF(p)$ and $\Omega_p$ respectively. We make $R_p$ and $R_p'$ into (left) $G$-modules in an obvious way. We then prove the following

LEMMA 1. *Let $e_0$ and $s$ be integers $\geqq 1$ such that $ee_0=(p-1)s$ and let $i_1<i_2<\cdots<i_r$ $(r=ee_0)$ be all the integers $i$ such that $1\leqq i\leqq sp$, $(i, p)=1$. Let, furthermore, $M$ be a $G$-module over $GF(p)$ containing a sequence of $G$-invariant submodules*

$$M = M_0 \supset M_1 \supset \cdots \supset M_r = \{0\},$$

*such that $M_{l-1}/M_l$ is isomorphic with $A_{i_l}$ as defined above $(l=1, \cdots, r)$. Then, $M$ is isomorphic with the direct sum of $e_0f_0$ copies of the $G$-module $R_p$.*

**Proof.** Let $M'$, $M_l'$ denote the $G$-modules over $\Omega_p$ which are obtained from $M$, $M_l$ by extending the scalar field $GF(p)$ to $\Omega_p$. We have again a sequence of $G$-modules

$$M' = M_0' \supset M_1' \supset \cdots \supset M_l' = \{0\},$$

and $M_{l-1}'/M_l'$ is isomorphic with $A_{i_l}'$. For $j=0, 1, \cdots, f_0-1$, let $a_{j,l}$ denote elements of $M_{l-1}'$ such that the residue class of $a_{j,l}$ mod $M_l'$ is mapped to $a_j'$ in $A_{i_l}'$ by the above isomorphism. Since the order $e$ of the normal subgroup $N$ of $G$ generated by $\tau$ is prime to $p$, $M'$ is completely reducible as an $N$-module; and we may choose $a_{j,l}$ so that

$$\tau a_{j,l} = \eta^{ip^j} a_{j,l}$$

with $i=i_l$. For any integer $j$ with $j=j_0+tf_0$, $0\leqq j_0<f_0$, we then put

$$a_{j,l} = \sigma^{-t} a_{j_0,l}.$$

$a_{j,l}$ then depends only upon the residue class of $j$ mod $ff_0$ and those $a_{j,l}$,

(2) Cf. Deuring [2, p. 38].

$0 \leqq j < ff_0$, represent a basis of $M'_{l-1}/M'_l$ over $\Omega_p$. From the definition, it also follows easily that

$$\sigma a_{j,l} = a_{j-f_0,l}, \qquad \tau a_{j,l} = \eta^{ip^j} a_{j,l}$$

with $i = i_l$.

Now, the $rff_0$ elements $a_{j,l}$, thus obtained for $0 \leqq j < ff_0$, $1 \leqq l \leqq r$, obviously form an $\Omega_p$-basis of $M'$. They are all characteristic elements for the operator $\tau$; and the corresponding characteristic values are given by $\eta^t$, where $t$ runs over the residue classes $ip^j$ mod $e$ with $1 \leqq i \leqq sp$, $(i, p) = 1$, and $0 \leqq j < ff_0$. However, since $sp = s + ee_0$ and $p^{ff_0} \equiv 1 \bmod e$, we have

$$\begin{aligned}
&\{ip^j \bmod e;\ 1 \leqq i \leqq sp,\ 0 \leqq j < ff_0\}\ (3)\\
&\qquad = \{ip^j \bmod e;\ 1 \leqq i \leqq s,\ j\} \cup \{ip^j \bmod e;\ 1 \leqq i \leqq ee_0,\ j\},\\
&\{ip^j \bmod e;\ 1 \leqq i \leqq sp,\ i \mid p,\ 0 \leqq j < ff_0\}\\
&\qquad = \{ip^{j+1} \bmod e;\ 1 \leqq i \leqq s,\ 0 \leqq j < ff_0\}\\
&\qquad = \{ip^j \bmod e;\ 1 \leqq i \leqq s,\ 0 \leqq j < ff_0\}.
\end{aligned}$$

It follows that

$$\begin{aligned}
&\{ip^j \bmod e;\ 1 \leqq i \leqq sp,\ (i, p) = 1,\ 0 \leqq j < ff_0\}\\
&\qquad = \{ip^j \bmod e;\ 1 \leqq i \leqq ee_0,\ 0 \leqq j < ff_0\}\\
&\qquad = e_0f_0f \text{ times the complete residue classes mod } e.
\end{aligned}$$

Therefore, every $\eta^t$ $(0 \leqq t < e)$ appears exactly $e_0f_0f$ times as a characteristic value of $\tau$ belonging to some $a_{j,l}$. On the other hand, the operator $\sigma$ permutes the $a_{j,l}$ among themselves in $ee_0f_0$ cycles of length $f$; and if the characteristic value of $\tau$ belonging to $a_{j,l}$ is $\eta^t$, that of $\tau$ for $\sigma^{-1}a_{j,l}$ is given by $\eta^{tq}$. It then follows immediately that, as a $G$-module over $\Omega_p$, $M'$ is isomorphic with the direct sum of $e_0f_0$ copies of $R'_p$.

Now, let $e_0f_0 \times R_p$ and $e_0f_0 \times R'_p$ denote the direct sums of $e_0f_0$ copies of $R_p$ and $R'_p$ respectively. $M$ and $e_0f_0 \times R_p$ are both $G$-modules over $GF(p)$ and their scalar extensions $M'$ and $e_0f_0 \times R'_p$ are proved to be isomorphic. Therefore $M$ and $e_0f_0 \times R_p$ are also isomorphic as $G$-modules over $GF(p)$, q.e.d.

1.2. Let $G$ be a finite group as considered in 1.1. $G$ is, namely, a group of order $n = ef$ generated by two elements $\sigma$ and $\tau$ satisfying the relations (1.1) with a prime power $q = p^{f_0}$, $f_0 \geqq 1$. In the following, we shall further assume that $f$ is divisible by $p$, and even by 4 if $p = 2$.

Let $O_p$ denote the ring of $p$-adic integers and $R$ the group ring of $G$ with coefficients in $O_p$. We consider an $R$-module $L$ with the following properties:

(i) as an $O_p$-module, $L$ is the direct sum of a finite cyclic $O_p$-module $W$

(3) In these formulae, the residue classes mod $e$ in the brackets are to be counted with multiplicities as $i$ and $j$ run over the domains as indicated.

generated by an element $w$ of order $p^\kappa$, $\kappa \geqq 1$, and $mn$ copies of the module $O_p$ for some integer $m \geqq 1$:

$$L = W + O_p + \cdots + O_p,$$
$$W = O_p w, \qquad p^\kappa w = 0, \qquad p^{\kappa-1} w \neq 0, \qquad \kappa \geqq 1.$$

$W$ is obviously invariant under $G$ so that we have

$$\sigma w = g_1 w, \qquad \tau w = g_2 w \tag{1.3}$$

with suitable integers $g_1$, $g_2$, which are uniquely determined mod $p^\kappa$.

(ii) let $f = f'p$ and $\sigma_1 = \sigma^{f'}$. Then, $\sigma_1 w = w$, and $L$ contains an element $z$ such that $\sigma_1 z = z + w_1$, where $w_1$ is an element of order $p$ in $W$, e.g., $p^{\kappa-1}w$.

(iii) the residue class module $\bar{L}$ of $L$ mod $pL$ is obviously an $(mn+1)$-dimensional $G$-module over the finite field $GF(p)$; and as such, it is the direct sum of $m$ copies of the group ring $R_p$ of $G$ over $GF(p)$ and a one-dimensional module $\bar{L}_0$ over $GF(p)$ such that

$$\sigma \bar{a} = g_1 \bar{a}, \qquad \tau \bar{a} = g_2 \bar{a} \tag{1.4}$$

for any $\bar{a}$ in $\bar{L}_0$.

We shall now study the structure of such an $R$-module $L$. For any element $c$ in $L$, let $\bar{c}$ denote the residue class of $c$ mod $pL$. By (iii), we can choose elements $c_0, c_1, \cdots, c_m$ in $L$ so that $\bar{c}_0$ is a basis of $\bar{L}_0$ and that $\bar{c}_0$ and $\rho \bar{c}_i$ $(\rho \in G, i = 1, \cdots, m)$ together form a basis of $\bar{L}$ over $GF(p)$. We put

$$L' = Rc_1 + \cdots + Rc_m.$$

$L/L'$ is then a cyclic $O_p$-module generated by the residue class of $c_0$ mod $L'$; and hence, it is either finite cyclic or isomorphic with $O_p$.

We first assume that $L/L'$ is isomorphic with $O_p$ and put

$$\sigma c_0 \equiv \zeta_1 c_0, \qquad \tau c_0 \equiv \zeta_2 c_0 \bmod L',$$

with suitable $\zeta_1$, $\zeta_2$ in $O_p$. By the assumption, $\zeta_1$ and $\zeta_2$ are uniquely determined by the above congruences; and, as $\sigma^f = 1$, $\tau^e = 1$, we must have $\zeta_1^f = 1$ and $\zeta_2^e = 1$. Since $\zeta_1$ and $\zeta_2$ are thus roots of unity in $O_p$, we have $\zeta_1^{p-1} = \zeta_2^{p-1} = 1$; and it also follows from (1.4) that

$$\zeta_1 \equiv g_1, \qquad \zeta_2 \equiv g_2 \bmod pO_p. \tag{1.5}$$

Let, then, $m \times R$ denote the direct sum of $m$ copies of the group ring $R$ considered as a $G$-module over $O_p$; and let $\phi$ be the $R$-homomorphism of $m \times R$ onto $L'$ defined by

$$\phi(\alpha_1, \cdots, \alpha_m) = \alpha_1 c_1 + \cdots + \alpha_m c_m, \qquad \alpha_i \in R.$$

We denote by $K$ the kernel of $\phi$. As $L/L' \cong O_p$ by the assumption, the finite module $W$ is contained in $L'$ and it follows from (i) that $L'$ is, as an $O_p$-

module, the direct sum of $W$ and $mn-1$ copies of the module $O_p$. Therefore, there is an element $x$ in $m\times R$ such that both $\phi(x)=w$ and $K=O_p p^\kappa x$ hold. Since $K$ is clearly $G$-invariant, we see, as we have done for $L/L'$, that

$$\sigma p^\kappa x = \zeta_1' p^\kappa x, \qquad \tau p^\kappa x = \zeta_2' p^\kappa x$$

with suitable roots of unity $\zeta_1'$, $\zeta_2'$ in $O_p$. It then follows that $\sigma x=\zeta_1' x$, $\tau x=\zeta_2' x$ and, consequently, that

$$\sigma w = \zeta_1' w, \qquad \tau w = \zeta_2' w.$$

We then have, by (1.3) and (1.5), that $\zeta_1' \equiv \zeta_1$, $\zeta_2' \equiv \zeta_2 \bmod pO_p$; and, as the $\zeta$'s are roots of unity in $O_p$, we get $\zeta_1' = \zeta_1$, $\zeta_2' = \zeta_2$. Let $\mu$ be an element in the center of $R$ defined by

$$\mu = \sum_{i=0}^{f-1} \sum_{j=0}^{e-1} \zeta_1^{-i} \zeta_2^{-j} \sigma^i \tau^j \text{ (4)}.$$

Since $\sigma x=\zeta_1 x$ and $\tau x=\zeta_2 x$, it is easy to see that there is an element $y$ of the form $y=(u_1, \cdots, u_m)$, $u_i \in O_p$, in $m\times R$, satisfying $x=\mu y$. On the other hand, as $\phi(x)=w$, there is no element $y'$ in $m\times R$ such that $y=py'$, and, hence, some $u_i$ is not divisible by $p$. Therefore, replacing $c_1, \cdots, c_m$ by their suitable linear combinations with coefficients in $O_p$ and changing the mapping $\phi$ accordingly, we can make

$$y = (1, 0, \cdots, 0), \qquad x = (\mu, 0, \cdots, 0).$$

In other words, we may assume that the generators $c_1, \cdots, c_m$ of $L'$ have a unique fundamental relation

$$p^\kappa \mu c_1 = 0.$$

We now put

$$c_1' = c_1 + \mu c_0, \qquad c_i' = c_i, \qquad \text{for } i = 0, 2, \cdots, m,$$
$$L'' = Rc_1' + \cdots + Rc_m'.$$

Using the above and

$$\sigma \mu c_0 = \zeta_1 \mu c_0, \qquad \tau \mu c_0 = \zeta_2 \mu c_0, \qquad \mu c_0 \equiv n c_0 \bmod L',$$

we can see easily that $c_1', \cdots, c_m'$ are linearly independent over $R$. Hence $w$ is not contained in $L''$ and $L/L''$ is a finite cyclic $O_p$-module. We have thus proved that we may always assume $L/L'$ is a finite cyclic $O_p$-module, for otherwise, we can take $c_0'$, $c_1'$, $\cdots$, $c_m'$ and $L''$ instead of the original $c_0, c_1, \cdots, c_m$ and $L'$.

We, now, therefore assume that $L/L'$ is a finite cyclic $O_p$-module of order,

(4) To see that $\mu$ is contained in the center of $R$, notice $\zeta_1^q=\zeta_1$, $\zeta_2^q=\zeta_2$. $\mu$ is, up to a scalar, the unique element in $R$ which takes the factors $\zeta_1$, $\zeta_2$ when multiplied by $\sigma$ and $\tau$ respectively.

say, $p^l$, $l \geqq 0$. It then follows immediately from (i) that $L'$ contains $mn$ linearly independent elements over $O_p$, and hence that $L'$ is isomorphic with $m \times R$ by the mapping $\phi$ as defined above. In particular, $L'$ contains no element of finite order except 0 and $W \cap L' = \{0\}$. $W$ is therefore mapped isomorphically into $L/L'$ by the canonical homomorphism of $L$ onto $L/L'$; and we see that the order of $L/L'$ is not less than the order of $W$, i.e., that $l \geqq \kappa$. Suppose that $l = \kappa$. $L$ is then the direct sum of $W$ and $L'$; and, for the element $z$ in (ii) above, we may put $z = rw + b_1$ with some integer $r$ and some $b_1$ in $L'$. It then follows from (ii) that $w_1 = (\sigma_1 - 1)z = r(\sigma_1 - 1)w + (\sigma_1 - 1)b_1 = (\sigma_1 - 1)b_1$. But, as $(\sigma_1 - 1)b_1$ is an element in $L'$, this contradicts the fact that $W \cap L' = \{0\}$. We must have therefore

$$l \geqq \kappa + 1. \tag{1.6}$$

Now, as $L/L'$ is a cyclic module of order $p^l$, there exists an integer $g$ such that $\sigma a \equiv ga \bmod L'$ for any element $a$ in $L$. Since $\sigma^f = 1$, we obviously have $g^f \equiv 1 \bmod p^l$. It follows, in particular, that $g^f \equiv 1 \bmod p$; and as $f = f'p$, $g^{f'} \equiv 1 \bmod p$ also holds. If $p = 2$, $f'$ is an even integer by the assumption; and we have also $g^{f'} \equiv 1 \bmod 4$. Therefore, if $g^{f'} - 1$ were divisible by $p^{l+1}$, we would have $g^{f'} \equiv 1 \bmod p^l$ and

$$\sigma_1 a \equiv \sigma^{f'} a \equiv g^{f'} a \equiv a \bmod L'$$

for any $a$ in $L$. Applying this to $a = z$, we see that $w_1 = (\sigma_1 - 1)z$ is in $L'$, which is again a contradiction. We obtain therefore

$$g^f \equiv 1 \bmod p^l, \qquad g^f \not\equiv 1 \bmod p^{l+1}. \tag{1.7}$$

We next take an element $a_0'$ in $L$ which generates $L \bmod L'$ and satisfies $p^{l-\kappa} a_0' \equiv w \bmod L'$. As $p^\kappa w = 0$, $p^l a_0'$ is contained in $p^\kappa L'$, and so is $(g^f - 1)a_0'$. Put $(\sigma - g)a_0' = b$. $b$ is then an element in $L'$ such that

$$\left( \sum_{i=0}^{f-1} g^i \sigma^{f-i-1} \right) b = (\sigma^f - g^f) a_0' = (1 - g^f) a_0' \in p^\kappa L'. \tag{1.8}$$

Since, however, $L'/p^\kappa L'$ is (as a $G$-module) isomorphic with the direct sum of $m$ copies of the group ring of $G$ over $O_p/p^\kappa O_p$, it follows from (1.8) that there is an element $b'$ in $L'$ satisfying

$$b \equiv (\sigma - g)b' \bmod p^\kappa L'.$$

Replacing $a_0'$ by $a_0' - b'$, if necessary, we may therefore assume that

$$(\sigma - g)a_0' \equiv 0 \bmod p^\kappa L'. \tag{1.9}$$

We now consider the action of $\tau$ on $L/L'$. Just as for $\sigma$, there is an integer $g'$ such that $\tau a \equiv g' a \bmod L'$ for any $a$ in $L$. Since $\tau^e = 1$, $g'^e \equiv 1 \bmod p^l$; and as $(e, p) = 1$, it follows immediately that $g' \equiv \zeta \bmod p^l O_p$ with some root of unity $\zeta$ in $O_p$. For any $a$ in $L$, we have then $\tau a \equiv \zeta a \bmod L'$; and using $W \cap L'$

$=\{0\}$, we see in particular that

$$\tau w = \zeta w. \tag{1.10}$$

Clearly, the root of unity $\zeta$ is uniquely determined by the above equality. Using such $\zeta$, we define an element $\lambda$ in the center of $R$ by

$$\lambda = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{-i}\tau^{i}(^{5}). \tag{1.11}$$

It then follows that $\lambda a_0' \equiv a_0' \bmod L'$, and hence we may replace $a_0'$ by $\lambda a_0'$ and denote it again by $a_0'$. For the new $a_0'$, (1.9) still holds; and furthermore we have also

$$\lambda a_0' = a_0', \qquad (\tau - \zeta)a_0' = 0. \tag{1.12}$$

Using (1.9), we put $(\sigma - g)a_0' = p^{\kappa}c''$ with $c''$ in $L'$. It then follows that

$$(\sigma - g)a_0' = p^{\kappa}c' \tag{1.13}$$

with $c' = \lambda c''$, which is also an element in $L'$ satisfying

$$\lambda c' = c'.$$

We may hence put

$$c' = \sum_{i=1}^{m} \alpha_i \lambda c_i,$$

where the $\alpha_i$ $(i = 1, \cdots, m)$ are linear combinations of $\sigma^i$ with coefficients in $O_p$, i.e., elements of the group ring $R_\sigma$, over $O_p$, of the cyclic group generated by $\sigma$. We put

$$\alpha_i = u_i + (\sigma - g)\beta_i, \qquad u_i \in O_p,\ \beta_i \in R_\sigma,$$

for $i = 1, \cdots, m$, and also

$$a_0 = a_0' - p^{\kappa}\sum_{i=1}^{m} \beta_i \lambda c_i, \qquad c = \sum_{i=1}^{m} u_i \lambda c_i.$$

We have then

$$\lambda a_0 = a_0, \qquad (\sigma - g)a_0 = p^{\kappa}c, \qquad (\tau - \zeta)a_0 = 0. \tag{1.14}$$

We shall next show that some $u_i$ is not contained in $pO_p$. Suppose, on the contrary, that all $u_i$ are in $pO_p$. We have then

$$(\sigma - g)a_0 = p^{\kappa+1}d_1$$

with some $d_1$ in $L'$. Multiplying both sides of the above by $\sum_{i=0}^{f-1} g^i\sigma^{f-i-1}$, we get

(5) Cf. footnote (4).

$$(1 - g^f)a_0 = p^{\kappa+1}d_2, \qquad d_2 \in L'.$$

Using (1.6), (1.7), put

$$d_3 = (1 - g^f)p^{-\kappa-1}a_0 - d_2.$$

We have then $p^{\kappa+1}d_3 = 0$. But, as $1 - g^f$ is not divisible by $p^{l+1}$, the order of $d_3$ mod $L'$ is exactly $p^{\kappa+1}$. Hence the order of $d_3$ itself must be also $p^{\kappa+1}$, and this contradicts the assumption (i). Therefore, some $u_i$, say $u_1$, is not contained in $pO_p$.

Finally, we then put

$$a_1 = \sum_{i=1}^{m} u_i c_i, \qquad a_j = c_j,\ j = 2, \cdots, m.$$

Since $u_1$ is a unit in $O_p$, we have

$$L' = Ra_1 + Ra_2 + \cdots + Ra_m;$$

and as $a_0$ generates $L$ mod $L'$, $a_0, a_1, \cdots, a_m$ obviously generate $L$ over $R$. Furthermore, we also get from (1.12), (1.13), and (1.14) that

$$(1.15) \qquad (\sigma - g)a_0 = p^{\kappa}\lambda a_1, \qquad (\tau - \zeta)a_0 = 0.$$

From the definition of $g$, it follows that $\sigma w = g_1 w \equiv gw$ mod $L'$. But, as $W \cap L' = \{0\}$, we have $g_1 w = gw$, $\sigma w = gw$. Now, take any rational integer $g^* = g + sp^{\kappa}$ which is congruent to $g$ mod $p^{\kappa}$. $a_0, a_1 - sa_0, a_2, \cdots, a_m$ is then clearly another system of generators of $L$ over $R$ and (1.15) holds for $a_0$, $a_1 - sa_0$, and $g^*$ instead of $a_0$, $a_1$, and $g$. Hence, by such a substitution, we can let $g$ take any given integer value satisfying $\sigma w = gw$. We have therefore proved the following lemma:

LEMMA 2. *Let $L$ be an $R$-module having the properties* (i), (ii), (iii) *as given at the beginning of this section. Then, $L$ has a system of $m+1$ generators $a_0, a_1, \cdots, a_m$ over $R$ such that*

$$(\sigma - g)a_0 = p^{\kappa}\lambda a_1, \qquad (\tau - \zeta)a_0 = 0,$$

*where $\zeta$ and $\lambda$ are given by* (1.10) *and* (1.11), *and $g$ is a rational integer satisfying $\sigma w = gw$ which can otherwise be arbitrarily given beforehand.*

We shall next prove the following

LEMMA 3. *Let $a_0, a_1, \cdots, a_m$ be a system of generators of $L$ over $R$ as given in the previous lemma. Then $a_0$ and $\rho a_i$ ($\rho \in G$, $i = 1, \cdots, m$) form a system of generators of $L$ over the ring $O_p$, and every $O_p$-linear relation among $a_0$ and the $\rho a_i$ is a consequence of the following fundamental relation:*

$$(1.16) \qquad (g^f - 1)a_0 + p^{\kappa} \frac{1}{} \sum_{i=0}^{f-1} \sum_{j=0}^{e-1} g^i \zeta^j \sigma^{f-i-1} \tau^{e-j} a_1 = 0.$$

**Proof.** The first half of the lemma is trivial. Let $L^*$ denote the free $O_p$-module which is the direct sum of $O_p$ and $m$ copies of the group ring $R$, and let $\psi$ be the $O_p$-homomorphism of $L^*$ onto $L$ defined by

$$\psi(u, \alpha_1, \cdots, \alpha_m) = ua_0 + \sum_{i=1}^{m} \alpha_i a_i, \qquad u \in O_p, \ \alpha_i \in R.$$

Using the property (i) of $L$, we can then choose a basis $b_0, b_1, \cdots, b_{mn}$ of $L^*$ over $O_p$ such that the kernel of $\psi$ is given by $O_p p^\kappa b_0$. Now, multiplying both sides of $(\sigma - g)a_0 = p^\kappa \lambda a_1$ by $\sum_{i=0}^{f-1} g^i \sigma^{f-i-1}$, we get immediately the relation (1.16). Therefore, if we put

$$b = \left((g^f - 1)p^{-\kappa}, \sum_{i=0}^{f-1} g^i \sigma^{f-i-1}\lambda, 0, \cdots, 0\right),$$

$p^\kappa b$ is contained in the kernel $O_p p^\kappa b_0$; and we get

$$b = u_0 b_0$$

with some $u_0$ in $O_p$. However, $b$ is obviously not contained in $pL^*$. $u_0$ is hence a unit in $O_p$ and the kernel of $\psi$ is also equal to $O_p p^\kappa b$. The lemma is therefore proved.

It follows immediately from Lemma 3 that all the $R$-linear relations among the generators $a_0, a_1, \cdots, a_m$ are consequences of the fundamental relations (1.15) and, hence, that the $R$-module $L$ is, up to isomorphisms, uniquely determined by the properties (i), (ii), (iii) given above.

1.3. We shall next prove a lemma on a certain type of totally disconnected compact groups.

Let $J$ be an arbitrary group. Let $\{N_\delta\}$ be the family of all normal subgroups of $J$ such that the indices $[J:N_\delta]$ are finite, and let $J_0$ be the intersection of all such $N_\delta$'s. We can make the factor group $J' = J/J_0$ a totally bounded topological group by taking the family of subgroups $\{N_\delta/J_0\}$ as a system of neighborhoods of 1 in $J'$. The completion of $J'$ then gives us a totally disconnected compact group $\overline{J}$ which we shall call the total completion of $J$.

Instead of the family $\{N_\delta\}$ of all normal subgroups of $J$ with finite indices, we can also start with suitable subfamilies of $\{N_\delta\}$ and get various totally disconnected compact groups in a similar way. In particular, taking the family of all normal subgroups $N_\delta'$ of $J$ such that the indices $[J:N_\delta']$ are finite and not divisible by a given prime number $p$, we get a compact group ${}^p\overline{J}$ which we shall call the $p$-complementary completion of $J$. The $p$-completion $\overline{J}^p$ of $J$ can be obtained similarly considering those normal subgroups $N_\delta''$ of $J$ whose indices in $J$ are powers of $p$.

Now, let $G$ be a totally disconnected compact group and let there be a homomorphism $\phi$ of $J$ into $G$ such that the image $\phi(J)$ of $J$ is everywhere dense in $G$. The group $J_0$ above is then contained in the kernel of $\phi$ so that $\phi$

induces a homomorphism $\phi'$ of $J'$ into $G$ and $\phi'$ can be uniquely extended to a continuous homomorphism $\psi$ of $\overline{J}$ onto $G$. In that sense, $\overline{J}$ may be called the universal group in the family of totally disconnected compact groups $G$ having everywhere dense homomorphic images of the group $J$; and it is, up to isomorphisms, uniquely characterized by that property. We can also give similar characterizations for ${}^{p}\overline{J}$ and $\overline{J}^{p}$.

We now consider the special case where the group $J$ is generated by two elements $\alpha$ and $\beta$ satisfying the unique relation

$$\alpha\beta\alpha^{-1} = \beta^{q},$$

where $q$ is, as before, a power $p^{f_0}$ of a prime number $p$. We shall denote by $\Gamma$ the total completion of such $J$, and by $\sigma$ and $\tau$ the elements of $\Gamma$ which are the images of $\alpha$ and $\beta$ by the canonical homomorphism of $J$ onto $J'$. We have then obviously

$$\sigma\tau\sigma^{-1} = \tau^{q}.$$

Let $\Gamma_0$ be the closure of the cyclic subgroup of $\Gamma$ generated by $\tau$. $\Gamma_0$ is then a closed normal subgroup of $\Gamma$; and $\Gamma/\Gamma_0$ and $\Gamma_0$ are isomorphic with the total and $p$-complementary completions of an infinite cyclic group, respectively. It is also easy to see that $\Gamma$ is an inverse limit of the type of finite groups as considered in 1.1 and 1.2.

LEMMA 4. *Let $G$ be a totally disconnected compact group and $N$ a closed normal subgroup of $G$ such that $G/N=\Gamma$. If, furthermore, $N$ is an inverse limit of finite $p$-groups, then the group extension $G/N$ splits, i.e. there exists a closed subgroup $H$ in $G$ such that $G=HN$, $H\cap N=1$.*

For the proof, we first notice the following: let $G_1$ and $G_2$ be both totally disconnected compact groups. We say that $G_1$ and $G_2$ are relatively prime if the index $[G_1:N_1]$ of any open normal subgroup $N_1$ in $G_1$ is always prime to the index $[G_2:N_2]$ of any open normal subgroup $N_2$ in $G_2$. We can then prove the following

LEMMA 5. *Let $G$ be a totally disconnected compact group and $N$ a closed normal subgroup of $G$ such that $G/N$ and $N$ are relatively prime. Then the group extension $G/N$ splits, i.e., there is a closed subgroup $H$ in $G$ such that $G=HN$, $H\cap N=1$. If, furthermore, either $G/N$ or $N$ is solvable, then any two such closed subgroups $H_1$, $H_2$ satisfying $G=H_iN$, $H_i\cap N=1$ $(i=1, 2)$ are conjugate in $G$.*

It is known that Lemma 5 holds if $G$ is a finite group and the proof for the general case can be easily reduced to that special case. We, therefore, omit the details here(6).

(6) For the proof of the lemma for a finite group $G$, cf. [9, p. 126]. To prove the existence of $H$ in the compact case, take a minimal closed subgroup $H$ such that $G=HN$.

Now, Lemma 4 can be proved as follows; let $G'$ be the closed normal subgroup of $G$ containing $N$ such that $G'/N=\Gamma_0$. Since $\Gamma_0$ is isomorphic with the $p$-complementary completion of an infinite cyclic group and $N$ is an inverse limit of $p$-groups, $G'/N$ and $N$ are relatively prime. Hence, by Lemma 5, there is a closed subgroup $H_1$ of $G'$ such that $G'=H_1N$, $H_1\cap N=1$. Let $a$ be an element of $G$ such that the coset $a'=aG'$ generates an everywhere dense cyclic subgroup of $G/G'$. $H_2=aH_1a^{-1}$ then also satisfies $G'=H_2N$, $H_2\cap N=1$; and by Lemma 5, there is an element $b$ in $G'$ such that $H_1=bH_2b^{-1}$. Let $C$ denote the closure of the cyclic group generated by $a_1=ba$. As $G/G'$ is the total completion of the infinite cyclic group generated by $a'=a_1G'$, it is easy to see that $G=CG'$, $C\cap G'=1$. Since $a_1H_1a_1^{-1}=H_1$, $H=CH_1$ is then a closed subgroup of $G$ such that $G=HN$, $H\cap N=1$.

## 2. Finite tamely ramified extensions

2.1. Let $p$ be a prime number, $Q_p$ the field of $p$-adic numbers, and $\Omega$ an algebraic closure of $Q_p$. All the fields we shall consider in the following are extensions of $Q_p$ contained in $\Omega$.

We take such a finite extension $k$ of $Q_p$ in $\Omega$ as our ground field and denote by $m$, $e_0$, and $f_0$ the degree, the ramification, and the residue class degree of the extension $k/Q_p$ respectively. We have then $m=e_0f_0$. Let $E$ be a finite extension of $k$ in $\Omega$ and let $F$ be the inertia field of $E/k$. We denote the degree, the ramification, and the residue class degree of $E/k$ by $n$, $e$, and $f$, respectively. We have then clearly $e=[E:F]$, $f=[F:k]$, and $n=ef=[E:k]$. We assume that the extension $E/k$ is tamely ramified, i.e., that $e$ is prime to $p$. Furthermore, we also assume that $E/k$ is a Galois extension and denote by $G$ and $N$ the Galois groups of $E/k$ and $E/F$ respectively. $N$ is then a normal subgroup of $G$, and $G/N$ and $N$ are both cyclic. We say that the tamely ramified Galois extension $E/k$ splits if the group extension $G/N$ splits. It is easy to see that $E/k$ splits if and only if $E$ contains a prime element $\pi$ such that $\pi^e$ is a prime element of $k$. In fact, suppose that $E$ contains such an element $\pi$. Since the residue class degree of the extension $E/Q_p$ is $ff_0$, $E$ contains a root of unity $\xi$ of order $p^{ff_0}-1$; and we have

$$F = k(\xi), \qquad E = k(\xi, \pi).$$

Put $F'=k(\pi)$ and denote by $\sigma$ the Frobenius automorphism of the unramified extension $E/F'$. If we then take any generator $\tau$ of $N$, the group $G$ is generated by $\sigma$ and $\tau$; and we have

$$\begin{aligned} \xi^\sigma &= \xi^q, \qquad \pi^\sigma = \pi, \\ \xi^\tau &= \xi, \qquad \pi^\tau = \eta\pi, \end{aligned} \tag{2.1}$$

where $q=p^{f_0}$ is the number of elements in the residue class field of $k$ and $\eta$ is a suitable $e$th root of unity in $E$. It follows immediately that

$$\sigma^f = 1, \qquad \tau^e = 1, \qquad \sigma\tau\sigma^{-1} = \tau^q.$$

Therefore, the group extension $G/N$ splits and $G$ is the type of group we considered in 1.1. We can also see easily that if, conversely, $E/k$ splits, then $E$ contains a prime element $\pi$ such that $\pi^e$ is in $k$.

2.2. Let $E/k$ be a splitting tamely ramified finite Galois extension of $k$ as considered in 2.1 and let $F$, $\xi$, $\pi$, $\sigma$, $\tau$ etc. be the same as given there. We also denote by $p^\kappa$ ($\kappa \geqq 0$) the highest power of $p$ dividing the order of any root of unity in $E$ and by $w$ a primitive $p^\kappa$th root of unity in $E$. In the following, we shall assume that $\kappa \geqq 1$, i.e., that $E$ contains at least a primitive $p$th root of unity, and also that the degree of the extension $E/k(w)$ is divisible by $p$, and even by 4 if $p=2$.

We shall now study the action of the Galois group $G$ of $E/k$ operating on the multiplicative group $E^*$ of $E$. For any positive integer $i$, let $U_i$ denote the $G$-invariant subgroup of $E^*$ consisting of all units $a$ in $E$ such that $a \equiv 1 \bmod \pi^i$. We have then obviously the following direct product decomposition:

$$E^* = \{\pi\} \times \{\xi\} \times U_1, \tag{2.2}$$

where $\{\pi\}$ denotes the infinite cyclic group generated by $\pi$ and $\{\xi\}$ the finite cyclic group of order $q^f-1$ generated by $\xi$. Since the action of $G$ on the first two direct factors is given by (2.1), we simply have to study the behavior of $G$ acting on the group $U_1$.

Let $O_p$ and $R$ denote, as in 1.2, the ring of $p$-adic integers and the group ring of $G$ with coefficients in $O_p$ respectively, and let $u$ be any element in $O_p$. For any $a$ in $U_1$, the element $a^u$ in $U_1$ is defined as usual; and as $(a^u)^\rho = (a^\rho)^u$ for any $\rho$ in $G$, we can consider the group ring $R$ as an operator domain of the abelian group $U_1$ in an obvious way. We shall next show that the group $U_1$ with the operator domain $R$ has the properties (i), (ii), (iii) of 1.2, though $U_1$ here is a multiplicative group and those conditions have to be modified accordingly.

It is well-known that (i) holds for $U_1$ with $m=[k:Q_p]$ and with the primitive $p^\kappa$th root of unity $w$. We put here

$$w^\sigma = w^{\sigma_1}, \qquad w^\tau = w^{\sigma_2}.$$

By the assumption, $[E:k(w)]$ is divisible by $p$. On the other hand, as $k(w)/k$ is a Galois extension, $[k(\pi, w):k(w)]$ divides $e=[k(\pi):k]$ and, hence, is prime to $p$. $[E:k(\pi, w)]$ is therefore also divisible by $p$ and $k(\pi, w)$ is contained in the fixed field of $\sigma_1=\sigma^{f'}$ where $f=f'p$. We have then $w^{\sigma_1}=w$, and the existence of an element $z$ in $U_1$ satisfying $z^{\sigma_1}=zw_1$ with a primitive $p$th root of unity $w_1$ also follows immediately from the fact that $E$ is a cyclic unramified extension of degree $p$ over the fixed field of $\sigma_1$ containing primitive $p$th roots of unity. The second property (ii) is hence verified for $U_1$.

To show, finally, that (iii) also holds for $U_1$, we first consider the action of $\sigma$ and $\tau$ on the factor group $U_i/U_{i+1}$. By the definition of $U_i$, every element $a$ in $U_i$ satisfies a congruence relation of the form

$$a \equiv 1 + b\pi^i \bmod \pi^{i+1}$$

with some integer $b$ in $E$; and the residue class $b'$ of $b$ mod $\pi$ is uniquely determined by $a$. The mapping $b'=\phi(a)$ of $U_i$ into the residue class field $GF(q^f)$ of $E$ then induces an isomorphism of $U_i/U_{i+1}$ onto the additive group of $GF(q^f)$, and it follows from (2.1) that the same isomorphism gives an isomorphism of the $G$-group $U_i/U_{i+1}$ onto the $G$-module $A_i$ as defined in 1.1.

Put $V_i=U_iU_1^p$ for $i\geqq 1$. We then get a sequence of $G$-invariant subgroups

$$U_1 = V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots,$$

concerning which we know the following results(7):

(1) let $ee_0=(p-1)s$. $s$ is then an integer; and if $i>sp$, $V_i=U_1^p$.

(2) let $w_1$ be a primitive $p$th root of unity in $E$. Since $sp=ee_0+s=ee_0+ee_0/(p-1)$, $p(1-w_1)$ is exactly divisible by $\pi^{sp}$. Hence, for any $a$ in $U_{sp}$, we have

$$a \equiv 1 - bp(1 - w_1) \bmod \pi^{sp+1}$$

with some integer $b$ in $E$; and a mapping $b'=\phi(a)$ is defined much as before. It can be then proved that $a$ is in $U_{sp}\cap U_1^p$ if and only if $\phi(a)$ is in the subgroup $D$ of the additive group of the residue class field $GF(q^f)$ formed by the elements $a'^p-a'$, $a'\in GF(q^f)$, and that $\phi$ induces an isomorphism of

$$V_{sp}/V_{sp+1} = V_{sp}/U_1^p$$

onto the factor group of $GF(q^f)$ mod $D$. Take an integer $b_0$ of $E$ such that the residue class of $b_0$ mod $\pi$ is not in $D$ and put

$$a_0 = 1 - b_0p(1 - w_1).$$

It then follows from the above that $V_{sp}/U_1^p$ is a cyclic group of order $p$ generated by the coset $a_0U_1^p$. Now, since $w_1^\sigma=w_1^{g_1}$, we have

$$1 - w_1^\sigma = 1 - w_1^{g_1} \equiv g_1(1 - w_1) \equiv g_1^q(1 - w_1) \bmod \pi^{s+1}.$$

It then follows that

$$a_0^\sigma = 1 - b_0^\sigma p(1 - w_1^\sigma) \equiv 1 - g_1^q b_0^q p(1 - w_1) \bmod \pi^{sp+1};$$

and as the residue classes of $(g_1b_0)^q$ and $g_1b_0$ are congruent mod $D$, we obtain

$$a_0^\sigma \equiv a_0^{g_1} \bmod U_1^p.$$

Similarly, we also have

$$a_0^\tau \equiv a_0^{g_2} \bmod U_1^p.$$

(3) let $i$ be an integer such that $1\leqq i\leqq sp$. If $p$ divides $i$, then $V_i=V_{i+1}$.

(7) Cf. [3, §15].

On the other hand, if $i$ is prime to $p$, $V_i/V_{i+1}$ is isomorphic with $U_i/U_{i+1}$, both being considered as $G$-groups. Therefore, by the remark mentioned above, the $G$-group $V_i/V_{i+1}$ is isomorphic with $A_i$ of 1.1.

Now, let $i_1 < i_2 < \cdots < i_r$ be all the integers $i$ such that $1 \leqq i \leqq sp$, $(i, p) = 1$ and put

$$V'_{i-1} = V_{i_j}/V_{sp}, \qquad i = 1, \cdots, r,$$
$$V'_r = 1.$$

It follows from (3) that the sequence of the $G$-invariant subgroups

$$V'_0 \supset V'_1 \supset \cdots \supset V'_r = 1$$

satisfies the assumption of Lemma 1; and by that lemma, we see immediately that as a $G$-group, $V'_0 = U_1/V_{sp}$ is isomorphic with the direct sum of $m = e_0 f_0$ copies of the group ring $R_p$ of $G$ over the finite field $GF(p)$. On the other hand, we also know by (2) that $V_{sp}/U_1^p$ is a cyclic group of order $p$ satisfying (1.4). It then follows easily that the $G$-group $U_1/U_1^p$ has the structure as given in (iii).

We have thus verified that the group $U_1$ with the operator domain $R$ has all the properties (i), (ii), (iii) in 1.2. Therefore, applying Lemmas 2, 3, we can immediately obtain the following theorem:

THEOREM 1. *Let $k$ be a finite extension of degree $m$ over the field of $p$-adic numbers $Q_p$ and $E = k(\xi, \pi)$ a splitting tamely ramified Galois extension of degree $n = ef$ over $k$ whose Galois group $G$ is generated by $\sigma$ and $\tau$ satisfying* (2.1). *Let $p^\kappa$ denote the highest power of $p$ dividing the order of any root of unity in $E$ and $w$ a primitive $p^\kappa$th root of unity in $E$. Assume that $\kappa \geqq 1$ and that $[E:k(w)]$ is divisible by $p$, and even by 4 if $p = 2$. Then, the multiplicative group $U_1$ consisting of all units $a$ in $E$ with $a \equiv 1 \bmod \pi$ contains a set of elements $a_0, a_1, \cdots, a_m$ such that*

(1) *every element $a$ in $U_1$ can be written in the form*

$$a = a_0^u a_1^{\alpha_1} \cdots a_m^{\alpha_m},$$

*where $u$ is an element in the ring of $p$-adic integers $O_p$ and $\alpha_i$ are elements of the group ring $R$ of $G$ with coefficients in $O_p$,*

$$(2) \qquad a_0^{\sigma - g} = a_1^{p^\kappa \lambda}, \qquad a_0^{\tau - \zeta} = 1,$$

*where $g$ is a given rational integer satisfying $w^\sigma = w^g$, $\zeta$ is a root of unity in $O_p$ uniquely determined by $w^\tau = w^\zeta$, and $\lambda$ is an element in the center of $R$, defined by*

$$\lambda = \frac{1}{e} \sum_{j=0}^{e-1} \zeta^{-j} \tau^j,$$

(3) $a=a_0^{u}a_1^{\alpha_1}\cdots a_m^{\alpha_m}$ *is* 1 *if and only if* $\alpha_i=0$ *for* $i>1$ *and*

$$u = v(g^f - 1), \qquad \alpha_1 = vp^\kappa \frac{1}{e}\sum_{i=0}^{f-1}\sum_{j=0}^{e-1} g^i\zeta^{-i}\sigma^{f-i-1}\tau^{e-j}$$

*with some* $v$ *in* $O_p$.

By (2.1), (2.2), and Theorem 1, the action of $G$ on the multiplicative group $E^*$ of $E$ is completely determined. Here we have made certain assumptions on $E/k$. However, as every finite tamely ramified Galois extension $E'$ of $k$ can be imbedded in an extension $E/k$ satisfying those conditions, we can also see, using the above results, the behavior of the Galois group of $E'/k$ acting on the multiplicative group of such $E'$. But we omit here the details(8).

## 3. The Galois group of $\Omega/k$

3.1. Let $k$ be, as in §2, a finite extension of degree $m$ over the field of $p$-adic numbers $Q_p$ and $\Omega$ an algebraic closure of $Q_p$ containing $k$. We denote by $V$ the composite of all finite tamely ramified extensions of $k$ contained in $\Omega$ and call it the ramification field of $\Omega/k$. Obviously, $V$ contains the composite of all finite unramified extensions of $k$ in $\Omega$, i.e., the inertia field $T$ of the extension $\Omega/k$. Let $q=p^{f_0}$ be, as before, the number of elements in the residue class field of $k$ and $\pi_1$ a prime element of $k$ which we shall fix in the following. For any positive integer $e$ prime to $p$, we choose a primtive $e$th root of unity $\xi_e$ and an $e$th root $\pi_e$ of $\pi_1$ in $\Omega$ so that if $e=e_1e_2$, then

$$\xi_{e_2} = \xi_e^{e_1}, \qquad \pi_{e_2} = \pi_e^{e_1}. \tag{3.1}$$

We put, for any integer $f\geqq 1$,

$$E_f = k(\xi_e, \pi_e), \qquad F_f = k(\xi_e),$$

where $e=e_f=q^f-1$. $E_f/k$ is then a splitting tamely ramified Galois extension of degree $ef$ as considered in §2 and $F_f$ is the inertia field of $E_f/k$. As $V$ and $T$ are also the composites of all $E_f$ and $F_f$ ($f\geqq 1$) respectively, $V$ is obtained by adjoining all $\xi_e$ and $\pi_e$ to $k$ and $T$ is obtained by adjoining all $\xi_e$ to $k$.

$V$ is obviously an infinite Galois extension of $k$ and we denote by $G(V/k)$ the Galois group of $V/k$. $G(V/k)$ is then a totally disconnected compact group in Krull's topology; and as $T/k$ is also a Galois extension, the Galois group $G(V/T)$ of $V/T$ is a closed normal subgroup of $G(V/k)$. It is now clear from (3.1) that $G(V/k)$ contains automorphisms $\sigma'$ and $\tau'$ such that

$$\begin{aligned} \xi_e^{\sigma'} &= \xi_e^{q}, & \pi_e^{\sigma'} &= \pi_e, \\ \xi_e^{\tau'} &= \xi_e, & \pi_e^{\tau'} &= \xi_e\pi_e. \end{aligned} \tag{3.2}$$

(8) More general, but less explicit results on the action of the Galois group on the multiplicative group of a local field are given in [6; 7].

$\sigma'$ and $\tau'$, then, generate an everywhere dense subgroup of $G(V/k)$ and $\tau'$ generates an everywhere dense subgroup of $G(V/T)$. It also follows from (3.2) that

$$\sigma'\tau'\sigma'^{-1} = \tau'^{q}.$$

Therefore, if we denote by $J$, as in 1.3, the group generated by $\alpha, \beta$ satisfying the relation $\alpha\beta\alpha^{-1}=\beta^{q}$, and by $\Gamma$ the total completion of $J$, there is a continuous homomorphism $\psi$ of $\Gamma$ onto $G(V/k)$ such that $\psi(\sigma)=\sigma'$, $\psi(\tau)=\tau'$, $\sigma$ and $\tau$ being the elements of $\Gamma$ corresponding to $\alpha$ and $\beta$ in $J$ respectively. Since $G(V/k)$ contains, for each $f\geqq 1$, an open normal subgroup $G(V/E_f)$ of index $ef$, we can see immediately that $\psi$ is an isomorphism of $\Gamma$ onto $G(V/k)$.

3.2. We shall next consider the structure of the ramification group of $\Omega/k$, i.e., the structure of the Galois group $G(\Omega/V)$ of the extension $\Omega/V$. Let $K$ be an arbitrary finite Galois extension of $k$ and $E$ the ramification field of the extension $K/k$, i.e. $E=K\cap V$. It is well-known that the Galois group $G(K/E)$ of $K/E$ is a $p$-group, and it follows immediately that $G(\Omega/V)$ is an inverse limit of finite $p$-groups. Let $V^*$ denote the multiplicative group of $V$ and $V^{*p}$ the subgroup of $V^*$ consisting of $p$th powers of elements in $V^*$. Using the fact that $V^*$ is the union of the multiplicative groups of $E_f$ $(f\geqq 1)$, it is easy to see that $V^*/V^{*p}$ is an infinite group. On the other hand, given any integer $f\geqq 1$, $V$ contains the field $F_f$ which is an extension of degree $f$ over $k$. Hence, by local class field theory, every Galois 2-cocycle over the field $V$ splits(9). As $G(\Omega/V)$ is obviously a separable topological group, it follows from a result in [4] that the ramification group $G(\Omega/V)$ is the $p$-completion of a free group with a countable number of free generators. Using, then, the fact that $G(\Omega/k)/G(\Omega/V)$ is isomorphic with $G(V/k)\cong\Gamma$, we can see also by Lemma 4 that the group extension $G(\Omega/k)/G(\Omega/V)$ splits. We thus have the following

THEOREM 2. *Let $k$ be a finite extension of the field of $p$-adic numbers $Q_p$ and $\Omega$ an algebraic closure of $Q_p$ containing $k$. Furthermore, let $T$ and $V$ be the inertia field and the ramification field of the extension $\Omega/k$, respectively. Then:*

(i) *the Galois group $G(V/k)$ of the extension $V/k$ is isomorphic with the total completion $\Gamma$ of a group $J$ generated by two elements $\alpha, \beta$ satisfying a unique relation $\alpha\beta\alpha^{-1}=\beta^{q}$, where $q$ is the number of elements in the residue class field of $k$; if $\sigma$ and $\tau$ denote the elements of $\Gamma$ corresponding to $\alpha$ and $\beta$ in $J$ respectively, there exists an isomorphism $\psi$ of $\Gamma$ onto $G(V/k)$ such that $\psi(\sigma)$ induces the Frobenius automorphism of $T/k$ and such that $\psi(\tau)$ generates an everywhere dense subgroup of $G(V/T)$, the Galois group of $V/T$,*

(ii) *the ramification group $G(\Omega/V)$, i.e., the Galois group of the extension $\Omega/V$, is isomorphic with the $p$-completion of a free group with a countable number of free generators,*

(9) For the results in local class field theory used here and in the following, cf. [1].

(iii) *$G(\Omega/V)$ is a closed normal subgroup of the Galois group $G(\Omega/k)$ of $\Omega/k$ and the group extension $G(\Omega/k)/G(\Omega/V)$ splits, i.e., there is a closed subgroup $H$ of $G(\Omega/k)$ such that $G(\Omega/k)=HG(\Omega/V)$, $H\cap G(\Omega/V)=1$.*

Now, Theorem 2 being proved, the structure of the Galois group $G(\Omega/k)$ can be determined completely, if we know the automorphisms $\phi_b(a)=bab^{-1}$ of the normal subgroup $G(\Omega/V)$ defined by elements $b$ in $H$. However, the determination of those automorphisms $\phi_b$ seems to be a different problem and, in the following, we shall only describe explicitly the effect of the automorphisms $\phi_b$ on the factor commutator group of $G(\Omega/V)$, i.e., on the Galois group $G(V'/V)$ of the maximal abelian extension $V'$ of $V$ in $\Omega$.

3.3. We shall now denote by $G$ and $N$ the Galois groups of $V'/k$ and $V'/V$ respectively. $G$ is again a totally disconnected compact group and $N$ a closed abelian normal subgroup of $G$. The factor group $G/N$ is then canonically isomorphic with the Galois group $G(V/k)$ and hence also with the group $\Gamma$ as given in Theorem 2. For simplicity, we put $G/N=G(V/k)=\Gamma$ and denote by $\sigma$ and $\tau$ the elements of $\Gamma$ which, when considered as Galois automorphisms of $V/k$, are the same as $\sigma'$ and $\tau'$ in (3.2) respectively. We put, namely,

$$\begin{aligned} \xi_e^{\sigma} &= \xi_{e'}, & \pi_e^{\sigma} &= \pi_e, \\ \xi_e^{\tau} &= \xi_e, & \pi_e^{\tau} &= \xi_e\pi_e, \end{aligned} \tag{3.3}$$

where $\xi_e$ and $\pi_e$ are elements of $V$ as given in 3.1. The group $\Gamma=G/N$ then operates on the abelian group $N$ in a natural way and our problem now is to determine the structure of the $\Gamma$-group $N$.

Let $E_f/k$ be the tamely ramified extension of degree $ef(e=q^f-1)$ as defined in 3.1, and let $G_f$ denote the Galois group of $V'/E_f$. We also denote by $G_f'$ the topological commutator group of $G_f$ and put $N_f=N\cap G_f'$. $G_f/G_f'$ is then clearly the Galois group of the maximal abelian extension $K_f$ of $E_f$ in $\Omega$; and $NG_f'/G_f'$ is the ramification group of $K_f/E_f$, for it corresponds to the ramification field $V\cap K_f$ of the extension $K_f/E_f$. Therefore, if we denote by $U_1(E_f)$ the group of all units $a$ in $E_f$ such that $a\equiv 1 \bmod \pi_e$, the norm residue mapping of $E_f$ gives, by local class field theory, a topological isomorphism $\phi_f'$ of $U_1(E_f)$ onto $NG_f'/G_f'$, the group $U_1(E_f)$ being considered as a compact group with respect to the natural topology of the local field $E_f$. Combining $\phi_f'$ with the canonical isomorphism of $NG_f'/G_f'$ onto $N/N_f$, we also have a topological isomorphism $\phi_f$ of $U_1(E_f)$ onto $N/N_f$. Furthermore, $U_1(E_f)$ and $N/N_f$ both have the group $\Gamma$ as an operator domain in obvious ways, and it follows from a property of the norm residue mapping that $\phi_f$ defined above is a $\Gamma$-isomorphism of $U_1(E_f)$ onto $N/N_f$.

Now, let $f'$ be a divisor of $f$. $E_{f'}$ is then a subfield of $E_f$ and $N_f$ is a subgroup of $N_{f'}$. We denote by $v_{f',f}$ the norm mapping of the field $E_f$ to the subfield $E_{f'}$ and by $\psi_{f',f}$ the canonical homomorphism of $N/N_f$ onto $N/N_{f'}$. $v_{f',f}$ then

maps $U_1(E_f)$ onto $U_1(E_{f'})$ and it again follows from one of the properties of the norm residue mapping that

$$\phi_{f'} \circ \nu_{f',f} = \psi_{f',f} \circ \phi_f. \tag{3.4}$$

On the other hand, the intersection of all $N_f$, $f \geqq 1$, is clearly the identity and, hence, $N$ is the inverse limit of the groups $N_f$, $f \geqq 1$, with the homomorphisms $\psi_{f',f}$. Therefore, we also see from (3.4) that the $\Gamma$-group $N$ is isomorphic with the inverse limit $U$ of the $\Gamma$-groups $U_1(E_f)$ with the homomorphisms $\nu_{f',f}$.

Now, let $p^\kappa$ be the highest power of $p$ dividing the order of any root of unity contained in $V$. From the definition of the ramification field $V$, it follows easily that there is such a finite power $p^\kappa$ of $p$ and that $\kappa \geqq 1$. We denote by $w$ a primitive $p^\kappa$th root of unity in $V$ and put, as in Theorem 1,

$$w^\sigma = w^q, \qquad w^\tau = w^g, \tag{3.5}$$

with a rational integer $g$ prime to $p$ and a root of unity $\zeta$ in $O_p$. The existence of such $\zeta$ follows from the fact that the order of the automorphism induced by $\tau$ on $k(w)$ is prime to $p$. Though $\zeta$ is uniquely determined by the above equality, the integer $g$ is only determined mod $p^\kappa$ by (3.5). But, we shall fix such an integer $g$ once for all in the following considerations.

We now take a positive integer $f_1$ such that $E_{f_1}$ contains $w$ and that the degree $[E_{f_1}:k(w)]$ is divisible by $p$, and also by 4 if $p=2$. For any positive integer $f$ divisible by $f_1$, the extension $E_f/k$ then satisfies all the assumptions of Theorem 1, the Galois group of $E_f/k$ being generated by the restrictions on $E_f$ of the automorphisms $\sigma$ and $\tau$ in $\Gamma = G(V/k)$ defined by (3.3). Therefore, by that theorem, the group $U_1(E_f)$ contains a system of $m+1$ elements $a_0, a_1, \cdots, a_m$, having the properties (1), (2), (3) of Theorem 1 with respect to $\sigma$, $\tau$, $g$ and $\zeta$ given by (3.3) and (3.5) respectively. Hence, if we denote by $\Theta$ the set of all such systems of $m+1$ elements $\theta = (a_0, a_1, \cdots, a_m)$ having the properties mentioned above, $\Theta$ is nonempty; and it is also compact when considered as a subset of the direct product of $m+1$ copies of the compact group $U_1(E_f)$ with its natural topology. We now choose a sequence of positive integers $f_2, f_3, \cdots$, such that $f_i$ divides $f_{i+1}$, $i=1, 2, \cdots$, and such that every integer $f$ is a divisor of some $f_i$. Then $U$ is also the inverse limit of the sequence of $\Gamma$-groups $U_1(E_{f_i})$, $i=1, 2, \cdots$, with the homomorphisms $\nu'_{j,i} = \nu_{f_j, f_i}$ $(j \leqq i)$. For each $i \geqq 1$, let $\Theta_i$ denote the $\Theta$-set of $E_{f_i}$ as defined above. If, then, $j \leqq i$ and $\theta = (a_0, a_1, \cdots, a_{m_0})$ is in $\Theta_i$, $\nu'_{j,i}\theta = (a'_0, a'_1, \cdots, a'_m)$ with $a'_t = \nu'_{j,i} a_t$ $(t=0, 1, \cdots, m)$ belongs to $\Theta_j$; and those $\nu'_{j,i}\theta$ form a closed subset $\nu'_{j,i}\Theta_i$ of $\Theta_j$. Since $\nu'_{1,j} \circ \nu'_{j,i} = \nu'_{1,i}$ for any $1 \leqq j \leqq i$, $\nu'_{1,i}\Theta_i$ is contained in $\nu'_{1,j}\Theta_j$ for $j \leqq i$, and the intersection of all $\nu'_{1,i}\Theta_i$, for $i=1, 2, \cdots$, is nonempty by the compactness of $\Theta_1$. Take an element $\theta_1$ in the intersection and let $\Theta'_i$ denote, for $i=2, 3, \cdots$, the set of all $\theta$ in $\Theta_i$ such that $\nu'_{1,i}\theta = \theta_1$. Again $\Theta'_i$ is compact and $\nu'_{j,i}\Theta'_i$ is a subset of $\Theta'_j$ for $j \leqq i$. Therefore, the intersection of all $\nu'_{2,i}\Theta'_i$, $i \geqq 2$, is nonempty and we can take an element $\theta_2$ in the intersection. Proceed-

ing similarly, we get a sequence of elements $\theta_1, \theta_2, \cdots$, such that $\theta_i$ is in $\Theta_i$ and that $\nu'_{j,i}\theta_i = \theta_j$ for $j \leqq i$. Put

$$\theta_i = (a_{i0}, a_{i1}, \cdots, a_{im}), \qquad a_{i,t} \in U_1(E_{f_i}).$$

We have then

$$\nu'_{j,i}a_{it} = a_{jt}, \qquad t = 0, 1, \cdots m; j \leqq i. \tag{3.6}$$

Now, if we use those elements $a_{i0}, a_{i1}, \cdots, a_{im}$ of $U_1(E_{f_i})$, the action of $\sigma$ and $\tau$ on $U_1(E_{f_i})$ is given explicitly by Theorem 1. Furthermore, the systems of those elements $\theta_i$, $i = 1, 2, \cdots$, are coherent in the sense that they satisfy (3.6) for any $j \leqq i$. Therefore, taking the limits of $a_{it}$, we can see immediately how $\sigma$ and $\tau$ act on the inverse limit $U$ of $U_1(E_{f_i})$; and thus the structure of the $\Gamma$-group $N = G(V'/V)$ can also be determined explicitly.

3.4. The result obtained above can be stated more clearly if it is formulated, as we shall do it in the following, in terms of the character group $\tilde{N}$ of the compact abelian group $N$. In general, let $A$ be a locally compact abelian group, $\tilde{A}$ the character group of $A$ and let

$$(a, \chi), \qquad a \in A, \chi \in \tilde{A},$$

be a dual pairing of $A$ and $\tilde{A}$. For any $\chi$ in $\tilde{A}$ and for any element $\rho$ in a group $\Sigma$ acting on $A$, there exists a unique character $\chi^\rho$ such that

$$(a^\rho, \chi^\rho) = (a, \chi)$$

for all $a$ in $A$. $\Sigma$ thus becomes also an operator domain of $\tilde{A}$ and the structure of the $\Sigma$-group $A$ is, conversely, uniquely determined by that of the $\Gamma$-group $\tilde{A}$. In our case, we have therefore only to describe the structure of the $\Gamma$-group $\tilde{N}$ explicitly.

Now, let $Q_p$ denote the additive group of the $p$-adic number field as well as the field itself and let $O_p$ also be the additive group of $p$-adic integers. With respect to the $p$-adic topology, $O_p$ is an open compact subgroup of $Q_p$ so that $\overline{Q}_p = Q_p/O_p$ is discrete. On the other hand, $Q_p$ is an $O_p$-module in an obvious way and, as $O_p$ is an invariant submodule of $Q_p$, $\overline{Q}_p$ is also an $O_p$-module. We now denote by $C(\Gamma)$ the set of all continuous functions defined on the compact group $\Gamma$ with values in $\overline{Q}_p$, and for any $\rho$ in $\Gamma$ and $h = h(\omega)$ in $C(\Gamma)$, we define a function $\rho h$ in $C(\Gamma)$ by

$$(\rho h)(\omega) = h(\rho^{-1}\omega), \qquad \omega \in \Gamma.$$

It is clear that $\Gamma$ thus becomes an operator domain of $C(\Gamma)$. For any integer $i \geqq 1$, the set of all functions $h$ in $C(\Gamma)$ such that $\rho h = h$ for any $\rho$ in the Galois group of $V/E_{f_i}$ forms a submodule of $C(\Gamma)$. We denote that submodule by $C(\Gamma_i)$, for it can be canonically identified with the set of all (continuous) functions with values in $\overline{Q}_p$ defined on the Galois group $\Gamma_i$ of $E_{f_i}/k$. It then follows immediately from the discreteness of $\overline{Q}_p$ that $C(\Gamma)$ is the union of all

such $C(\Gamma_i)$, $i=1, 2, \cdots$. Let $h=h(\omega)$ be again a function in $C(\Gamma)$ and let $h$ be in $C(\Gamma_i)$ for some $i$. We put

$$m_i(h) = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{-j} h(\tau^j),$$

where $e=q^{f_i}-1$ and $\zeta$ is the root of unity in $O_p$ given by (3.5). If $h$ is also contained in $C(\Gamma_j)$ and $m_j(h)$ is defined in a similar way, it is easy to see that $m_i(h)=m_j(h)$. We therefore denote those common values by $m(h)$. $m(h)$ is obviously an $O_p$-linear function on $C(\Gamma)$ with values in $\overline{Q}_p$.

We now denote by $X$ the direct sum of the group $\overline{Q}_p$ and $m$ copies of the module $C(\Gamma)$:

$$X = \overline{Q}_p + C(\Gamma) + \cdots + C(\Gamma).$$

For each $i \geqq 1$, we also denote by $X_i$ the submodule of $X$ consisting of all $x=(\bar{y}, h_1, \cdots, h_m)$ $(\bar{y}\in\overline{Q}_p,\ h_t\in C(\Gamma),\ t=1, \cdots, m)$ such that $h_t$ are in $C(\Gamma_i)$ for $t=1, \cdots, m$ and such that

$$(3.7) \qquad (g^f-1)\bar{y} + p^\kappa \frac{1}{e}\sum_{i=0}^{f-1}\sum_{j=0}^{e-1} g^i\zeta^j h_1(\sigma^{f-i-1}\tau^{e-j}) = 0,$$

where $f=f_i$, $e=q^f-1$. $X$ is then the union of those submodules $X_i$ $(i\geqq 1)$, and it is easy to see that there is a unique way of making $X$ a $\Gamma$-module so that $\rho x=x$ if $x$ is in $X_i$ and $\rho$ is an element of the Galois group of $V/E_{f_i}$ and that

$$(3.8) \qquad \begin{aligned} \sigma x &= (\bar{y}_1, \sigma h_1, \cdots, \sigma h_m), \qquad \bar{y}_1 = g^{-1}(\bar{y} - p^\kappa m(\sigma h_1)), \\ \tau x &= (\bar{y}_2, \tau h_1, \cdots, \tau h_m), \qquad \bar{y}_2 = \zeta^{-1}\bar{y}, \end{aligned}$$

for any $x=(\bar{y}, h_1, \cdots, h_m)$ in $X$. We shall next show that the $\Gamma$-module $X$ thus defined is $\Gamma$-isomorphic with the group $\tilde{N}$, the character group of $N$.

Let $\chi$ be an additive character of $Q_p$ with the kernel $O_p$, i.e. a homomorphism of $Q_p$ into the additive group of reals mod 1 such that the kernel of $\chi$ is $O_p$. The bilinear function $(u, y)$ on $Q_p\times Q_p$ defined by

$$(u, y) = \chi(uy), \qquad u, y \in Q_p,$$

then gives a dual pairing of the locally compact abelian group $Q_p$ with itself; and since the annihilator of $O_p$ in $Q_p$ with respect to this pairing is $O_p$ itself, it induces a pairing $(u, \bar{y})$ of $O_p$ and $\overline{Q}_p=Q_p/O_p$ $(u\in O_p,\ \bar{y}\in\overline{Q}_p)$. For any $v$ in $O_p$, we have then

$$(vu, \bar{y}) = (u, v\bar{y}).$$

We now fix an integer $i\geqq 1$ and consider the group $U_1=U_1(E_{f_i})$. For simplicity, we denote $f_i$, $a_{i0}$, $a_{i1}$, $\cdots$, $a_{im}$ by $f$, $a_0$, $a_1$, $\cdots$, $a_m$, respectively. Every element $a$ in $U_1$ can then be written in the form

$$a = a_0^{u} a_1^{\alpha_1} \cdots a_m^{\alpha_m}, \tag{3.9}$$

where $u$ is an element of $O_p$ and $\alpha_i$ are elements in the group ring of the Galois group $\Gamma_i$ of $E_{f_i}/k$ over $O_p$. We put

$$\alpha_i = \sum_{\rho'} u_{i,\rho'}\rho'. \qquad u_{i,\rho'} \in O_p,\ \rho' \in \Gamma_i.$$

For any $x=(\bar{y}, h_1, \cdots, h_m)$ in $X_i$, we then define a symbol $[a, x]_i$ by

$$[a, x]_i = (u, \bar{y}) + \sum_{i\rho',\rho'} (u_{i,\rho'}, h_i(\rho)),$$

where $\rho$ denotes any element of $\Gamma$ contained in the coset $\rho'$ of the factor group $\Gamma_i$ of $\Gamma$. Though the expression (3.9) is not unique for the given element $a$, the value of $[a, x]_i$ is uniquely defined according to Theorem 1, (2), and (3.7). As can be verified easily, $[a, x]_i$ then gives a dual pairing of the groups $U_1(E_{f_i})$ and $X_i$; and it also follows from Theorem 1, (3), and (3.8) that

$$[a^\rho, \rho x]_i = [a, x]_i \tag{3.10}$$

for any $\rho$ in $\Gamma$. Let $j$ be another integer such that $1 \leqq j \leqq i$ and let $[a, x]_j$ be the dual pairing of $U_1(E_{f_j})$ and $X_j$ defined in a similar way as above. $X_j$ is then contained in $X_i$, and it follows again easily from the definition that

$$[a, x]_i = [v'_{j,i}a, x]_j$$

for any $a$ in $U_1(E_{f_i})$ and for any $x$ in $X_j$. Since the group $U$ is the inverse limit of $U_1(E_{f_i})$ with homomorphisms $v'_{j,i}$ and since $X$ is the union of all $X_i$, it then follows immediately that $[a, x]_i$ $(i \geqq 1)$ together define a dual pairing $[a, x]$ of the compact abelian group $U$ and the discrete abelian group $X$ such that

$$[a^\rho, \rho x] = [a, x],$$

for any $\rho$ in $\Gamma$. We have thus proved that the group $X$ is $\Gamma$-isomorphic with the character group of $U$, and, hence, also with the character group $\tilde{N}$ of $N$. We have therefore the following theorem:

THEOREM 3. *Let $k$, $V$, $\Omega$ be as in Theorem 2. Let $\Gamma$ be the Galois group of $V/k$ and $N$ the Galois group of the maximal abelian extension $V'/V$ of $V$ in $\Omega$. Let, furthermore, $C(\Gamma)$ denote the module of all continuous functions defined on $\Gamma$ with values in $\overline{Q}_p = Q_p/O_p$ and $X$ the direct sum of $\overline{Q}_p$ and $m$ copies of the module $C(\Gamma)$, where $m=[k:Q_p]$. If we then make $X$ a $\Gamma$-group so that (3.8) holds, the character group $\tilde{N}$ of $N$ is $\Gamma$-isomorphic with the so defined $\Gamma$-module $X$.*

## BIBLIOGRAPHY

1. E. Artin, *Algebraic numbers and algebraic functions* I, Lecture notes at Princeton University, 1950–1951.

2. M. Deuring, *Algebren*, Berlin, 1935.

3. H. Hasse, *Zahlentheorie*, Berlin, 1949.

4. K. Iwasawa, *On solvable extensions of algebraic number fields*, Ann. of Math. vol. 58 (1953) pp. 548–572.

5. Y. Kawada, *On the structure of the Galois group of some infinite extensions* I, Journal of the Faculty of Science. Imperial University of Tokyo. Section I., vol. 7 (1954) pp. 1–18.

6. M. Krasner, *Sur la représentation multiplicative dans les corps de nombres P-adiques relativement galoisiens*, C. R. Acad. Sci. Paris vol. 203 (1936) pp. 907–908.

7. ———, *Sur la représentation exponentielle dans les corps relativement galoisiens de nombres P-adiques*, Acta Arithmetica vol. 3 (1939) pp. 133–173.

8. I. R. Safarevic, *On p-extensions*, Mat. Sbornik vol. 20 (1947) pp. 351–363.

9. H. Zassenhaus, *Lehrbuch der Gruppentheorie* I, Leipzig-Berlin, 1937.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
CAMBRIDGE, MASS.