ON A CERTAIN GROUP CONCERNING THE p-ADIC NUMBER FIELD.

By
Hideo Kuniyoshi.

In the local class field theory, we consider the norm group of a finite extension field of a p-adic number field $k$. An abelian extension $K$ of $k$ is uniquely determined by this subgroup of $k^*$, where $k^*$ is the multiplicative group of all non-zero elements of $k$. We denote this norm group of $K$ by $N_{K/k}$. Then the galois group of $K/k$ is isomorphic to the factor group $k^*/N_{K/k}$.

We may consider, in some sense dually to the above fact, a subgroup $G(k/K)$ of $K^*$ which consists of all the elements of $K^*$ whose norms to $k$ are unity. It is likely that $G(k/K)$ has close connections with the subfield $K$. When $K/k$ is cyclic, the structure of $G(k/K)$ was determined by Hilbert. When $K/k$ is abelian, a certain property of $G(k/K)$ was given by Prof. T. Tannaka, who gave also another theorem which is analogous to the ordering theorem of local class field theory. The former property was extended to non-abelian cases, by Mr. T. Nakayama and Mr. Y. Matsushima.

In this paper, restricting to the abelian case, I shall give a detailed structure of $G(k/K)$, and add a certain remark to a particular non-abelian case.

1. The structure of $G(k/K)$.

Let $k$ be a $p$-adic number field, and $K$ be a finite extension of $k$. We denote the multiplicative groups of their non-zero elements by $k^*$, $K^*$, respectively, and norm group of $K/k$, by $N_{K/k}$. The elements of $K$ whose norm to $k$ are unity, form a subgroup of $K^*$ and we denote this by $G(k/K)$. When $K$ is a normal extension of $k$ with its galois group $G$, we mean by a factor set of $K/k$ a system of elements $a_{\sigma, \tau} (\sigma, \tau \in G)$ of $K$ satisfying

\[ a_{\sigma, \tau}^p a_{\sigma, \tau^p, \rho} = a_{\sigma, \tau^p} a_{\sigma, \tau, \rho}. \]

* Received Aug. 1st, 1949.
1) T. Tannaka [8].
2) T. Nakayama and Y. Matsushima [4], T. Nakayama [7].
Further, we shall denote by $K_{a}^{\lambda-\lambda}$ the group generated by $\theta^{1-\sigma}, \theta \in K$, $\sigma \in G$.

One of Tannaka's results runs as follows:

**Theorem 1.** Let $\Omega$ be a finite abelian extension field of $k$ with its galois group $G$, and $(a_{\sigma}, \tau)$ be a factor set of $\Omega/k$ whose exponent is equal to the degree of extension $\Omega/k$. Then $G(k/\Omega)$ is generated by $\Omega_{a}^{\lambda-\lambda}$ and $a_{\sigma_{\tau}}, a_{\tau}$, where $\sigma_{\tau}$ run over $G$:

$$G(k/\Omega) = \left( a_{\sigma_{\tau}}, \Omega_{a}^{\lambda-\lambda} \right).$$

Let

$$(n_1, \ldots, n_r) \quad n_{i+1}|n_i$$

be an invariant system of $G$, then $G$ decomposes directly in cyclic groups $Z_{i}$ of order $n_{i}$:

$$A = Z_{1} \times Z_{2} \times \cdots \times Z_{r}.$$ This decomposition is up to isomorphism unique. Let $\sigma_{i}$ be a generator of $Z_{i}$, and we shall fix it throughout this section.

In the Theorem 1, it is not necessary to take all the elements of $G$, but sufficient to do with $\sigma_{i}$ of (4). We show this fact in next

**Lemma 1.**

$$G(k/\Omega) = \left( a_{\sigma_{\tau}}, \Omega_{a}^{\lambda-\lambda} \right).$$

We prove this by induction. Let $N = Z_{1} \times \cdots \times Z_{r-1}$ and $M$ be the corresponding intermediate field. We assume the lemma for the extension $\Omega/M$. Then we take an element $\theta$ of $G(k/\Omega)$,

$$N_{\Omega/M} \theta = 1.$$ 

As $N/k$ is cyclic, it follows from Hilbert's lemma that

$$N_{\Omega/M} \theta = n^{1-\sigma_{r}}, n \in M.$$ 

Furthermore, as $\Omega/M$ is abelian extension with its galois group $N$, there exists an element $\sigma$ of $N$ such that

$$n \equiv a_{\sigma_{r}}, n \mod N_{\Omega/M}.$$ 

where

$$\sigma = \Pi_{i} \sigma_{i}^{n_{i}}.$$ 

Then

$$n \equiv \Pi_{i} a_{\sigma_{r}}^{n_{i}}, n \mod N_{\Omega/M}.$$ 

---

3) We refer this theorem to [8].


5) We denote a product $\Pi_{\tau \in \tau} a_{\sigma_{\tau}}, a_{N_{\tau}}$, and in a similar way $a_{\sigma_{\tau}}^{N_{\tau}}$ by $a_{\sigma_{\tau}}^{N_{\tau}}$. I
Next, we calculate \( a_{\sigma_1, k} \), using the relation (1),

\[
a_{\sigma_1, k} = \frac{a_{\sigma_1, N}}{a_{\sigma_1, \sigma}} = \frac{a_{\sigma_1, N}}{a_{\sigma_1, \sigma} a_{\rho_1, N}} = \frac{a_{\sigma_1, N}}{a_{\sigma_1, \sigma} a_{\rho_1, N}} = N_{\Omega/M} \frac{a_{\sigma_1, \sigma}}{a_{\sigma_1, \sigma} a_{\rho_1, N}}.
\]

It follows from (6), (7) and (8) that

\[
N_{\Omega/M} \theta = (\prod \sigma_{\rho_1, k})^{a_{\sigma_1, \sigma}} N_{\Omega/M} (\omega^{1-\sigma}) = N_{\Omega/M} \left( \prod \left( a_{\sigma_1, \sigma} \right)^{a_{\sigma_1, \sigma}} \omega^{1-\sigma} \right),
\]

therefore

\[
N_{\Omega/M} \left[ \theta/\prod \left( a_{\sigma_1, \sigma} \right)^{a_{\sigma_1, \sigma}} \omega^{1-\sigma} \right] = 1.
\]

From the assumption of the induction, we obtain

\[
G(k/\Omega) = \left( \frac{a_{\sigma_1, \sigma}}{a_{\sigma_1, \sigma}} \right)^{\Omega_{k}^{-1}}
\]

q.e.d.

Let \( K \) be an abelian extension field of \( k \), whose galois group \( H \) has invariant system

\[
(n_1, n_2), \quad n_2 | n_1.
\]

Then

\[
H = H_1 \times H_2,
\]

where \( H_i \) are the cyclic groups of order \( n_i \), and \( \tau_i \) their fixed generators.

Let \( (b) \) be a factor set of \( K/k \) whose exponent is equal to the degree of \( K/k \). From the lemma 1

\[
G(k/K) = b_{T_1, T_2} b_{T_2, T_1} K_{\sigma_i} T_2 T_1
\]

Concerning the order of \( b_{T_1, T_2} \mod K_{\sigma_i}^{-1} \), we obtain next

**Lemma 2.** If \( (b_{T_2, T_2}, T_1) \mod K_{\sigma_i}^{-1} \), then

\[
n_2 | x.
\]

**proof.** Let \( K_i \) be the intermediate field which corresponds to \( H_i \). From the assumption of the lemma and (9), we have

\[
\left( b_{T_1, T_2} \right)^{a_{T_2, T_1}} = \theta^{1-\tau_1} \theta_2^{1-\tau_2}, \quad \theta_i \in K_i.
\]

Taking the norm with respect to \( K_i \), the left-hand side of the equation (10) becomes

\[
N_{K_i} \left( b_{T_1, T_2} \right)^{a_{T_2, T_1}} = \left( b_{T_1, T_2} \right)^{a_{T_2, T_1}} = \left( b_{T_2, T_2} N_{K_i} \theta_i^{1-\tau} \right),
\]

and the right-hand side

\[
N_{K_i} \theta_i^{1-\tau}.
\]
therefore,
\[ b_{x_1 x_2} = (N_{K/K_2} \theta)_{-\tau_1} \quad \theta \in K. \]
In this relation, \( b_{x_1 x_2} \), \( N_{K/K_2} \theta \) belong to the field \( K_2 \) and as the Galois group \( H_1 \) of \( K_2/k \) is generated by \( \tau_1 \), it follows that
\[ b_{x_1 x_2} = \alpha N_{K/K_2} \theta \]
where \( \alpha \) belongs to the field \( k \).

On the other hand we have
\[ \alpha \in N_{K/K_2} \]
where if we regard \( \alpha \) as an element of \( K_2 \), for
\[ N_{K_2/k} \alpha = \alpha^a = (\alpha^{n_1/n_2})^{n_2} \in N_{K_2/k} \]
implies (12), owing to the "verschiebungssatz" of the local class field theory.
From (11) and (12) follows
\[ b_{x_1 x_2} \in N_{K/K_2} \]
and from this using the Nakayama's theorem\(^7\) we get
\[ \tau_2 = 1, \]
hence
\[ n_2 | x. \]
q.e.d.

Again we return to the extension \( \Omega/k \), and use the same notations as in the Theorem 1 and the Lemma 1.

Lemma 3.
\[ \left( \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} \right)^{n_j} \in \Omega^{-\lambda}. \]
Proof. Let \( L_j \) be an intermediate field which corresponds to the subgroup \( Z_j \) of \( A \), then \( \Omega/L_j \) is a cyclic extension with its Galois group \( Z_j \). From this and (8) we get
\[ N_{\Omega/L_j} \left( \frac{a_{\sigma_j \sigma_i}}{a_{\sigma_i \sigma_j}} \right)^{n_j} = (a_{\sigma_j \sigma_i})^{n_j} = (a_{\sigma_j \sigma_i} N_{\Omega/L_j} \omega')^{-n_i} = N_{\Omega/L_j} \omega^{i-n_i}. \]
Hence,
\[ \left( \frac{a_{\sigma_j \sigma_i}}{a_{\sigma_i \sigma_j}} \right)^{n_j} = \omega^{i-n_i} \omega^{i-n_i} \in \Omega^{-\lambda}. \]
q.e.d.

Now, we point out a relation between the Galois group \( A \) of \( \Omega/k \) and the group \( G(k/\Omega) \).

Theorem 2.
\[ G(k/\Omega)/\Omega^{-\lambda} = A_2 \times A_3 \times \cdots \times A_r \]

7) This proof is given by prof. T. Tannaka. Our original proof was much longer and considerably complicated.
where \( A_t \cong Z_t \times Z_{t+1} \times \cdots \times Z_r \)
and \( Z_t \) are the cyclic groups of (4).

Proof. We assume a relation between \( \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} \) and \( \Omega_t^{-\lambda} \), i.e.

\[
\Pi \left( \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} \right)^{a_{t-j}} \in \Omega_t^{-\gamma}.
\]

We choose \( Z_i, Z_j, i < j \) arbitrary, and let \( \mathcal{N} \) be a direct factor excluding \( Z_i \times Z_j \), and \( Z \) be the corresponding intermediate field, then \( Z/k \) is a normal extension with its galois group \( Z_i \times Z_j \). We take norm of (14) with respect to \( Z \), then a simple calculation will show that

\[
N_{Z/k} \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} = 1 \quad \left( t \neq i, j \right),
\]

\[
N_{Z/k} \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} = a_{\sigma_i \sigma_j}^{t-j} \quad \left( t \neq i, j \right),
\]

hence (14) changes to the form

\[
\left( \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} \right)^{t-j} \in Z_t^{-\lambda}. \tag{15}
\]

From Chevalley's lemma, \( \left( a_{\sigma_i \sigma_j} \right) \) is also a factor set of \( Z/k \) whose exponent is equal to \( (Z:k) \). Thus we can regard \( \left( a_{\sigma_i \sigma_j} \right) \) and \( Z \) as \( (b, \gamma) \), and \( K \) respectively in the lemma 2, hence

\[
n_j \equiv x^{t-j} \tag{16}.
\]

This shows that in the relation (14) no \( \frac{a_{\sigma_i \sigma_j}}{a_{\sigma_j \sigma_i}} \) can really appear, and there exists essentially only relations of the form (15) with (16). It follows that \( a_{\sigma_i \sigma_j}/a_{\sigma_j \sigma_i} \) mod \( \Omega_t^{-\lambda} \) forms a cyclic subgroup \( Z_t \), of degree \( n_j \), and

\[
G(k/\Omega)/\Omega_t^{-\lambda} = Z_{n_1} \times Z_{n_2} \times Z_{n_2} \times \cdots \times Z_{n_1} \times \cdots \times Z_{n_{r-1}}.
\]

Then putting

\[
A_t = Z_{t+1} \times Z_{t+2} \times \cdots \times Z_{r_t}
\]

we obtain the desired theorem.

q.e.d.

From this, as an immediate consequence, we obtain the Matsushima's result, namely:

**Theorem 3.** Let \( k \) be a \( p \)-adic number field and \( \Omega \) be a finite abelian extension field. If

\[
G(k/\Omega) = \Omega_t^{-\lambda},
\]

then \( \Omega/k \) is a cyclic extension.

This theorem is not true for a nonabelian extension \( K/k \). For example, let \( K/k \) be a nonabelian extension with galois group \( G \). And we assume

8) C. Chevalley [3] or E. Witt [9].
that $G/G'$ and $G'$ are both cyclic groups, $G'$ being the commutator subgroup of $G$. Then after a slight calculation we get
\[ G(k/K) = K_{1-\alpha}^G. \]

2. Connections with the class field theory.

Let $\Omega$ and $k$ denote the local fields as in the section 1. There exists the maximum abelian extension field $\Omega$ of $k$, and obviously $\Omega > \Omega$. Let $\bar{A}$ be an infinite abelian extension field of $k$ and we put
\[ H(\bar{A}/k) = \langle N_{\bar{A}/k}^1 \rangle, \]
where $A$ is any intermediate field of $\bar{A}/k$ of finite degree over $k$. For the infinite abelian extension $\bar{A}$ of $k$, we are able to constitute similar theory with finite abelian extension fields by using $H(A/k)$ instead of $N^*$.

Now, we shall show that $G(k/\Omega)$ is closely connected with the maximum abelian extension field $\Omega$ of $k$.

Lemma 4.

(17) \[ H(\Omega/k) = 1. \]

Proof. Let $\alpha \in H(\bar{\Omega}/k)$, and we put $\alpha$ in the from
\[ \alpha = P^e \cdot e \]
where $P$ is a fixed prime element of $k$, and $e$ an unit element. If $\varepsilon \neq 0$, we denote the group of all the units by $E$, and construct a subgroup $H$ of $k^*$ generated by $E$ and $P^e$, $|\beta| = 0$ (2 $|\varepsilon|$). Then $H$ has finite index in $k^*$
\[ (k^*; H) < \infty, \]
hence from the existence theorem of the local class field theory, there exists a finite abelian extension $A_i$ of $k$ such that
\[ H_i = N_{A_i/k}^1. \]
Furthermore from (16)
\[ \alpha \in H(\bar{\Omega}/k) < N_{A_i/k}^1 = H_i. \]
On the other hand, from the construction of $H_i$, it is obvious that
\[ \alpha \in H_i, \]
and this contradicts with (18). Therefore $\varepsilon = 0$, $\alpha$ is a unit.

If $\alpha \neq 1$, there exists a natural number $n$ such that
\[ \alpha \equiv 1 \mod p^n, \]
and we denote by $E_n$ the group of all the element $e_n$ of $k^*$ congruent with unity modulus $p^n$:
\[ e_n \equiv 1 \mod p^n. \]
From $E_n$ and $P$, we construct a subgroup of $k^*$ which has a finite group index in $k^*$.
(20) \[ H_n = (P, E_n). \]
Analogously to the above discussion, we get an abelian extension \( A_n \) of \( k \) such that
\[ H_n = N_{A_n/k}. \]
And similarly
\[ \alpha \in H(\overline{\Omega}/k) \subset N_{A_n/k} = H. \]
From (19) and (20) obviously
\[ \alpha \in H. \]
Thus we lead to a contradiction, and the lemma is proved.

**Theorem 4.**

Let \( K/k \) be any finite extension, then
\[ (22) \quad G(k/K) = H(K\overline{\Omega}/K). \]

**Proof.** Obviously
\[ G(k/K) < H(K\overline{\Omega}/K). \]

Conversely, we take an element \( \Theta \) from \( H(K\overline{\Omega}/K) \) and put
\[ \theta = N_{K/k}\Theta. \]
We assume \( \Theta \neq 1 \) and lead to a contradiction. If \( \Theta \neq 1 \) there exists an abelian extension \( A \) of \( k \) such that
\[ (23) \quad \theta \in N_{A/k}. \]
From (16) follows
\[ \Theta \in N_{A/k}. \]
Therefore, using the Verschiebungssatz we get
\[ N_{K/k}\Theta = \theta \in N_{A/k}. \]
This contradicts with (23), hence we have
\[ N_{K/k}\Theta = \theta = 1, \quad \Theta \in G(k/K). \]

As an immediate consequence of this theorem, using the ordering theorem of the local class field theory, we get one of Chevalley’s results (2):

**Corollary.** Let \( k \) be a \( p \)-adic number field and \( K \) be its finite extension field. When we take a finite abelian extension \( A \) of \( K \), then \( A/k \) is abelian, if and only if
\[ G(k/K) < N_{A/k}. \]

**References**

2. C. CHEVALLEY; Sur la théorie du corps de classes dans les corps finis et

Mathematical Institute, Tōhoku University, Sendai.