On local cyclotomic fields.

Dedicated to Professor Z. Suetuna.

By Kenkichi IWASAWA

(Received May 4, 1959)

Introduction.

Let \( p \) be an odd prime, \( Q_p \) the \( p \)-adic number field, and \( \Omega \) an algebraic closure of \( Q_p \). For each \( n \geq 0 \), we denote by \( F_n \) the extension field of \( Q_p \) generated by the set \( W_n \) of all \( p^{n+1} \)-th roots of unity in \( \Omega \). The local cyclotomic field \( F_n \) is then a cyclic extension of degree \( p^n(p-1) \) over \( Q_p \). Let \( W \) be the union of the increasing sequence of groups \( W_n \) for \( n \geq 0 \) and let \( F \) be the union of the increasing sequence of fields \( F_n \) for \( n \geq 0 \). Then \( F = Q_p(W) \), and it is an infinite abelian extension of \( Q_p \). Let \( j \psi \) be the maximal abelian extension of \( F \) in \( \Omega \); \( j \psi \) is clearly a Galois extension of \( Q_p \).

We now consider the following problems on the local fields \( F_n \) and \( j \psi \): To determine the structure of the multiplicative group of the field \( F_n \) acted on by the Galois group \( G(F_n/Q_p) \), and to describe explicitly the structure of the Galois group of the extension \( M/Q_p \). In the present paper, we shall give a solution to these problems by using the result of a previous paper, in which we studied some arithmetic properties of local cyclotomic fields in applying the theory of \( \Gamma \)-finite modules. We hope that the result of the present paper, combined with our previous results on Galois groups of local fields, will give us further insight into the structure of the Galois group of the extension \( \Omega/Q_p \).

1. The structure of the multiplicative group of \( F_n \).

Let \( U \) be the group of all \( p \)-adic units in \( Q_p \) and \( U^0 \) the subgroup of all \( a \) in \( U \) such that \( a \equiv 1 \mod p \). Then \( U \) is the direct product of \( U^0 \) and a cyclic subgroup \( V \) of order \( p-1 \) consisting of all roots of unity in \( Q_p \):

\[
U = U^0 \times V.
\]


By local class field theory, there exists a topological isomorphism \( \kappa \) of \( G = G(F/Q_p) \) onto \( U \) such that

\[
\zeta^\sigma = \zeta^{\kappa(\sigma)}, \quad \sigma \in G,
\]

for every \( \zeta \) in \( W \). Then, for any \( \sigma \) in \( G \), there exists a unique element \( \eta_\sigma \) in \( V \) such that

\[
\kappa(\sigma) \equiv \eta_\sigma \pmod{p},
\]

and the mapping \( \sigma \rightarrow \eta_\sigma \) defines a homomorphism of \( G \) onto \( V \) with kernel \( G(F/F_0) \).

Let \( n (\geqq 0) \) be fixed. Let \( p_n \) be the unique prime ideal of \( F_n \) dividing the rational prime \( p \), and let \( B_n \) and \( B_n^0 \) denote, respectively, the group of all \( p_n \)-adic units in \( F_n \) and the subgroup of all \( \beta \) in \( B_n \) such that \( \beta \equiv 1 \pmod{p_n} \). Then \( B_n \) is the direct product of \( B_n^0 \) and \( V \):

\[
B_n = B_n^0 \times V.
\]

The groups \( B_n, B_n^0, \) and \( V \) are invariant under the Galois group \( G_n = G(F_n/Q_p) \). The action of \( G_n \) on \( V \) is obviously trivial. But the action of \( G_n \) on \( B_n^0 \) is given as follows\(^3\): Let \( R_n \) be the group ring of \( G_n \) over the ring \( O_p \) of \( p \)-adic integers, and let \( I_n \) be the ideal of \( R_n \) consisting of all elements of the form \( \sum a_\sigma \sigma \) (\( a_\sigma \in O_p \)) with \( \sum a_\sigma = 0 \). Since \( B_n^0 \) is a \( p \)-primary compact abelian group, we may consider \( O_p \) as an operator domain of \( B_n^0 \). Hence we may also consider \( R_n \) as acting on \( B_n^0 \). As an \( R_n \)-group, \( B_n^0 \) is then the direct product of \( U^0, W_n, \) and a subgroup \( C_n \) isomorphic with the \( R_n \)-module \( I_n \):

\[
B_n^0 = U^0 \times W_n \times C_n.
\]

Since \( U = U^0 \times V, \) we also have

\[
B_n = U \times W_n \times C_n, \quad C_n \cong I_n.
\]

Now, let \( A_n \) denote the multiplicative group of the field \( F_n \) and let \( \pi_n \) be any prime element of \( F_n \). Then \( A_n/B_n \) is an infinite cyclic group generated by the coset of \( \pi_n \mod B_n \) and the Galois group \( G_n \) acts trivially on \( A_n/B_n \). Therefore \( \pi_n^{\sigma^{-1}} \) is contained in \( B_n \) for any \( \sigma \) in \( G_n \). For such a \( \sigma \), we also put

\[
\eta_\sigma = \eta_{\sigma'},
\]

where \( \sigma' \) is any element of \( G = G(F/Q_p) \) inducing \( \sigma \) on \( F_n \). We then have the following

**Lemma.** For any prime element \( \pi_n \) of \( F_n \) and for any \( \sigma \) in \( G_n \),

\[
\pi_n^{\sigma^{-1}} \equiv \eta_\sigma \pmod{p_n}.
\]

3) Cf. I. c. 1), Theorem 19.
PROOF. Let $\pi'_n$ be any other prime element of $F_n$. Then $\pi'_n = \beta \pi_n$, with $\beta$ in $B_n$; and since $G_n$ acts trivially on $V$, $\beta^{\sigma-1} \equiv 1 \mod p_n$. Hence $\pi_n^{\sigma-1} \equiv \pi_n^{\sigma-1} \mod p_n$ and we see that it is sufficient to prove the lemma for one particular $\pi_n$. Let $\zeta_{n+1}$ be a primitive $p^{n+1}$-th root of unity in $F_n$. Then $\pi_n = 1 - \zeta_{n+1}$ is a prime element of $F_n$, and

$$\pi_n^{\sigma} \equiv \pi_n^{\sigma'} \equiv 1 - \zeta_{n+1}^{\pi_n^{\sigma} \equiv 1 - (1 - \pi_n)^{\pi_n^{\sigma} \equiv 1 \mod p_n^2}}.$$

Therefore $\pi_n^{\sigma-1} \equiv \eta_{\sigma} \mod p_n$, q.e.d.

Let $\pi_n$ be again any prime element of $F_n$. By the above lemma, we put

$$\pi_n^{\sigma-1} = \beta_{\sigma} \eta_{\sigma}, \quad \sigma \in G_n,$$

with $\beta_{\sigma}$ in $B_n^0$. We then denote by $D(\pi_n)$ the closure of the subgroup of the compact group $B_n^0$ generated by these $\beta_{\sigma}$ ($\sigma \in G_n$); $D(\pi_n)$ consists of all elements of the form

$$\prod_{\sigma} \beta_{\sigma}^{a_{\sigma}}$$

with arbitrary $p$-adic integers $a_{\sigma}$. Since the elements $\beta_{\sigma}$ ($\sigma \in G_n$) define a 1-cocycle of $G_n$ in $B_n^0$ and satisfy the relations $\beta_{\tau \sigma} = \beta_{\sigma} \beta_{\tau}^{a_{\sigma}}$ ($\sigma, \tau \in G_n$), $D(\pi_n)$ is an $R_n$-subgroup of $B_n^0$.

**Theorem 1.** There exists a prime element $\pi_n$ of $F_n$ such that $B_n = U \times W_n \times D(\pi_n)$.

The $R_n$-group $D(\pi_n)$ is then isomorphic with the $R_n$-module $L_n$ under an isomorphism $\varphi$ such that $\varphi(\beta_{\sigma}) = \sigma - 1$ ($\sigma \in G_n$).

**Proof.** Let $B_n = U \times W_n \times C_n$ as in the above, and let $g$ be the projection from $B_n$ on the factor $C_n$. For any $\xi$ in $A_n$, $\xi^{\sigma-1}$ ($\sigma \in G_n$) is always contained in $B_n$. Hence we put

$$\xi_{\sigma} = g(\xi^{\sigma-1}), \quad \sigma \in G_n.$$

Then $\{\xi_{\sigma}\}$ defines a 1-cocycle of $G_n$ in $C_n$; and since $H^1(G_n; A_n) = 1$, the mapping $\xi \rightarrow \{\xi_{\sigma}\}$ induces a homomorphism of $A_n/B_n$ onto the cohomology group $H^1(G_n; C_n)$. Let $f$ be an $R_n$-isomorphism of $C_n$ onto $I_n$, and let $\omega_{\sigma}$ ($\sigma \in G_n$) be the elements of $C_n$ such that $f(\omega_{\sigma}) = \sigma - 1$. It is then easy to see that $H^1(G_n; C_n)$ is a cyclic group of order $p^n$ generated by the cohomology class of $\{\omega_{\sigma}\}$. Take a prime element $\pi_n$ of $F_n$. Since $A_n/B_n$ is an infinite cyclic group generated by the coset of $\pi_n$ mod $B_n$, the 1-cocycle $\{g(\pi_n^{\sigma-1})\}$ also generates $H^1(G_n; C_n)$. Therefore there is an integer $m$, prime to $p$, such that

$$g(\pi_n^{\sigma-1}) = \omega_{\sigma}^{m \tau^{\sigma-1}}, \quad \sigma \in G_n,$$

with an element $\tau$ in $C_n$. Since $\pi_n^{\sigma-1}$ is also a prime element of $F_n$, we
replace $\pi_n$ by $\pi_n^{-1}$ and denote the latter again by $\pi_n$. Then we have
$$g(\pi_n^{\sigma-1}) = \omega_\sigma^m, \quad \sigma \in G_n.$$ 

As in the above, let $\pi_n^{\sigma-1} = \beta_{\sigma} \pi_{n\sigma}$. Then $g(\beta_{\sigma}) = \omega_\sigma^m$ (\sigma \in G_n) and $g$ induces an $O_p$-homomorphism of $D(\pi_n)$ into $C_n$. Therefore, if $h$ is the $O_p$-homomorphism of $I_n$ onto $D(\pi_n)$ such that $h(\sigma - 1) = \beta_{\sigma}$, then
$$f \circ g \circ h(\sigma - 1) = m(\sigma - 1), \quad \sigma \in G_n.$$

Since $m$ is prime to $p$, $f \circ g \circ h$ is an automorphism of $I_n$. It follows that $g$ induces an isomorphism of $D(\pi_n)$ onto $C_n$, and we have
$$B_n = U \times W \times D(\pi_n).$$

Suppose next that $\pi_n$ is any prime element of $F_n$ satisfying $B_n = U \times W \times D(\pi_n)$; $\pi_n$ need not be the particular prime element obtained in the above argument. Clearly, there is an $O_p$-homomorphism $\psi$ of $I_n$ onto $D(\pi_n)$ such that $\psi(\sigma - 1) = \beta_{\sigma}$. Since $\beta_{\sigma} = \beta_{\sigma} \pi_{n\sigma}^\sigma$, $\psi$ is then also an $R_n$-homomorphism. However, it follows from $B_n = U \times W_n \times C_n$ that $I_n \cong C_n \cong D(\pi_n)$. In particular, as compact abelian groups, both $I_n$ and $D(\pi_n)$ are isomorphic with the direct sum of $p^n(p - 1) - 1$ copies of $O_p$. Hence $\psi$ must be one-one, and $\varphi = \psi^{-1}$ is an $R_n$-isomorphism of $D(\pi_n)$ onto $I_n$ such that $\varphi(\beta_{\sigma}) = \sigma - 1$. Thus the theorem is completely proved.

Since $A_n/B_n$ is an infinite cyclic group generated by the coset of $\pi_n$ mod $B_n$ and since the action of $G_n$ on $U \times W_n$ is well-known, the structure of the $G_n$-group $A_n$, the multiplicative group of $F_n$, is completely determined by Theorem 1.

2. The structure of the Galois group $G(M/Q_p)$.

Let $E$ be the maximal unramified extension of $Q_p$ in $Q$. It is known that $E$ is an abelian extension of $Q_p$ generated by all roots of unity in $Q$ whose orders are prime to $p$, and also that the Galois group $G(E/Q_p)$ is isomorphic with the so-called total completion $\overline{Z}$ of the additive group $Z$ of rational integers.\(^4\) It follows that the Galois group $G(E'/Q_p)$ of the maximal $p$-complementary unramified extension $E'$ of $Q_p$ is isomorphic with the $p$-complementary completion $p\overline{Z}$ of $Z$. Furthermore, for each $n \geq 0$, $EF_n$ is the maximal unramified extension of $F_n$ in $Q$, and $EF_{n+1}$ is the maximal $p$-complementary unramified extension of $F_n$ in $Q$. Let $L_n$ be the maximal $p$-complementary abelian extension of $F_n$ in $Q$. Then $EF_n$ is contained in $L_n$ and,

\(^4\) For compact completions of (discrete) groups, cf. l.c. 2), 1.3. We also notice that a compact topological group is called $p$-primary ($p$-complementary) if and only if it is the inverse limit of a family of finite groups whose orders are powers of $p$ (prime to $p$).
by local class field theory, \( G(L_n/E'F_n) \) is naturally isomorphic with \( B_n/B_n^0 \equiv V \). Since \( F_n \cap L_0 = F_n, G(F_nL_0/F_n) \equiv G(L_0/F_0), F_nL_0 \) is clearly contained in \( L_n \). But, since \( F_nL_0 \) contains both \( E'F_n \) and a ramified extension of degree \( p-1 \) over \( F_n \), it follows that
\[
F_nL_0 = L_n, \quad n \geq 0.
\]
If \( F_n' \) denotes the unique subfield of \( F_n \) with degree \( p^n \) over \( Q_p \), then we also have
\[
F_n'L_0 = L_n, \quad F_n' \cap L_0 = Q_p, \quad n \geq 0.
\]
Let \( F' \) be the union of the increasing sequence of subfields \( F_n' \) in \( \Omega \). Then \( F' \) is a subfield of \( F \) such that \( \kappa(G(F/F')) = V \), and we have
\[
G(F'/Q_p) \cong U^0.
\]
On the other hand, the union \( L \) of the increasing sequence of subfields \( L_n \) in \( \Omega \) is, as one sees easily, the maximal \( p \)-complementary abelian extension of \( F \) in \( \Omega \). We then prove the following

**Theorem 2.** Let \( F' \) be the subfield of \( F \) such that \( \kappa(G(F/F')) = V \) and let \( L_0 \) and \( L \) be the maximal \( p \)-complementary abelian extensions of \( F_0 \) and \( F \) in \( \Omega \), respectively. Then
\[
F'L_0 = L, \quad F' \cap L_0 = Q_p, \quad G(L/Q_p) = G(L/F') \times G(L/L_0),
\]
\[
G(L/F') \cong G(L_0/Q_p), \quad G(L/L_0) \cong G(F'/Q_p) \cong U^0.
\]
Furthermore, \( G(L_0/Q_p) \) is the \( p \)-complementary completion of a group generated by two elements \( \sigma \) and \( \tau \) satisfying the only relations
\[
\sigma \tau \sigma^{-1} = \tau^p, \quad \tau^{(p-1)^2} = 1;
\]
\( \sigma \) is a Frobenius automorphism for \( L_0/Q_p \) and \( \tau \) is a generator of the inertia group for \( L_n/Q_p \).

**Proof.** The first half of the theorem is an immediate consequence of what is stated in the above; one has only to notice that \( L_0 \) is a Galois extension of \( Q_p \).

The field \( E' \) defined in the above is obviously the inertia field for the tamely ramified extension \( L_0/Q_p \). Since \([L_0: E'F_0] = [F_0 : Q_p] = p-1\) and \( E' \cap F_0 = Q_p \), we see that \([L_0: E'] = (p-1)^2\). The second half of the theorem is then an easy consequence of a result on the structure of the Galois group for the maximal tamely ramified extension of a local field.5)

If we are merely interested in the purely group-theoretical structure of the group \( G(L/Q_p) \), we have the following corollary, which is an immediate consequence of the above theorem:

5) Cf. l. c. 2), 3.1.
Corollary. The Galois group $G(L/Q_p)$ is the total completion of a group generated by two elements $\lambda$ and $\mu$ satisfying the only relations

$$\lambda\mu\lambda^{-1}=\mu^p, \; \mu^{(p-1)^2}=1.$$  

Theorem 3. Let $L$ and $M$ be as in the above and let $K$ be the maximal $p$-primary abelian extension of $F$ in $Q$ so that $KL=M, K\cap L=F$. Then:

i) $G(M/L)$ is a closed normal subgroup of $G(M/Q_p)$ such that $G(M/Q_p)/G(M/L)=G(L/Q_p)$, and the group extension $G(M/Q_p)/G(M/L)$ splits,

ii) $G(L/F)$ acts trivially on $G(M/L)$ so that $G(M/L)$ can be considered as a $G$-group $(G=G(F/Q_p)=G(L/Q_p)/G(L/F))$, and as such, $G(M/L)$ is naturally isomorphic with $G(K/F)$.

Proof. Let

$$X=G(M/Q_p), \; P=G(M/L_0), \; N=G(M/L).$$

Then $P$ is a closed $p$-primary normal subgroup of $X$, and $X/P=G(L_0/Q_p)$ is a $p$-complementary compact group. Hence the group extension $X/P$ splits and there exists a closed subgroup $H$ of $X$ such that

$$HP=X, \; H\cap P=1, \; H\cong X/P.$$  

Such a group $H$ also satisfies $HN=G(M/F^\prime)$. On the other hand, since $P/N=G(L/L_0)\cong U^\prime$, there is an element $\sigma$ in $P$ such that $N\sigma$ generates a cyclic group which is everywhere dense in $P/N$. Let $S$ be the closure of the cyclic subgroup of $P$ generated by $\sigma$. Using $P/N\cong U^\prime$, we then see easily that

$$NS=P, \; N\cap S=1.$$  

Since both $N$ and $HN=G(M/F^\prime)$ are normal in $X$, we have $(\sigma H\sigma^{-1})N=\sigma(HN)\sigma^{-1}=HN$, and $\sigma H\sigma^{-1}\cap N=\sigma(H\cap N)\sigma^{-1}=1$. Hence there is an element $\tau$ in $N$ such that $\tau\sigma H\sigma^{-1}\tau^{-1}=H$. Let $\sigma'²=\sigma\tau\tau^{-1}$. Then $N\sigma=No\sigma'$, and the closure $S'$ of the cyclic subgroup of $P$ generated by $\sigma'$ also satisfies $NS'=P$ and $N\cap S'=1$. Furthermore, since $\sigma'H\sigma'=H, S'$ is contained in the normalizer of $H$ in $X$. Therefore $T=HS'$ is a closed subgroup of $X$, and it is easy to see that $NT=X, N\cap T=1$. Thus the first part of the theorem is proved.

The second part is an immediate consequence of the fact that $KL=M, K\cap L=F$, and $G(M/F)=G(M/K)\times G(M/L)$.

Now, the action of $G=G(F/Q_p)$ on $G(K/F)$ is explicitly known. Therefore, combining that with the above Theorems 2, 3, we see that the structure of the Galois group $G(M/Q_p)$ is thus completely determined.

Massachusetts Institute of Technology.

---

6) Cf. l. c. 2), Lemma 5.
7) Cf. l. c. 6).
8) Cf. l. c. 1), Theorem 18.