Journal of the Mathematical Society of Japan Vol. 12, No. 1, January, 1960

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 Ω an algebraic closure of Q_p. For each $n \geqq 0$, 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 Ω. 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 $(n \geqq 0)$ and let F be the union of the increasing sequence of fields F_n $(n \geqq 0)$. Then $F = Q_p(W)$, and it is an infinite abelian extension of Q_p. Let M be the maximal abelian extension of F in Ω; M is clearly a Galois extension of Q_p.

We now consider the following problems on the local fields F_n and M: 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 Γ-finite modules.[1] We hope that the result of the present paper, combined with our previous results on Galois groups of local fields,[2] will give us further insight into the structure of the Galois group of the extension Ω/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 $a \equiv 1 \bmod p$. 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:

$$U = U^0 \times V.$$

1) Cf. K. Iwasawa, On the theory of cyclotomic fields, Ann. of Math., 70 (1959), 530-561.

2) Cf. K. Iwasawa, On Galois groups of local fields, Trans. Amer. Math. Soc., 80 (1955), 448-469.

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

$$\zeta^{\sigma} = \zeta^{\kappa(\sigma)}, \qquad \sigma \in G,$$

for every ζ in W. Then, for any σ in G, there exists a unique element η_σ in V such that

$$\kappa(\sigma) \equiv \eta_\sigma \mod p,$$

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

Let n ($\geqq 0$) be fixed. Let $\mathfrak{p}_n$ 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 $\mathfrak{p}_n$-adic units in F_n and the subgroup of all β in B_n such that $\beta \equiv 1 \mod \mathfrak{p}_n$. 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 $\sum_\sigma a_\sigma \sigma$ ($a_\sigma \in O_p$) with $\sum_\sigma a_\sigma = 0$. 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

$$B_n = U \times W_n \times C_n, \qquad C_n \cong I_n.$$

Now, let A_n denote the multiplicative group of the field F_n and let π_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 σ in G_n. For such a σ, we also put

$$\eta_\sigma = \eta_{\sigma'},$$

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

LEMMA. *For any prime element π_n of F_n and for any σ in G_n,*

$$\pi_n^{\sigma-1} \equiv \eta_\sigma \mod \mathfrak{p}_n.$$

---

3) Cf. l. c. 1), Theorem 19.

PROOF. Let π_n' be any other prime element of F_n. Then $\pi_n' = \beta\pi_n$, with β in B_n; and since G_n acts trivially on V, $\beta^{\sigma-1} \equiv 1 \bmod \mathfrak{p}_n$. Hence $\pi_n'^{\sigma-1} \equiv \pi_n^{\sigma-1} \bmod \mathfrak{p}_n$, and we see that it is sufficient to prove the lemma for one particular π_n. Let ζ_{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

$$\begin{aligned}\pi_n^{\sigma} &\equiv \pi_n^{\sigma'} \equiv 1-\zeta_{n+1}^{\kappa(\sigma')} \equiv 1-(1-\pi_n)^{\kappa(\sigma')} \\ &\equiv \kappa(\sigma')\pi_n \equiv \eta_{\sigma'}\pi_n \equiv \eta_\sigma\pi_n \qquad \bmod \mathfrak{p}_n^2 .\end{aligned}$$

Therefore $\pi_n^{\sigma-1} \equiv \eta_\sigma \bmod \mathfrak{p}_n$, q. e. d.

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

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

with β_σ 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 β_σ ($\sigma \in G_n$); $D(\pi_n)$ consists of all elements of the form

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

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

THEOREM 1. *There exists a prime element π_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 I_n under an isomorphism φ 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 ξ in A_n, $\xi^{\sigma-1}$ ($\sigma \in G_n$) is always contained in B_n. Hence we put

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

Then $\{\xi_\sigma\}$ defines a 1-cocycle of G_n in C_n; and since $H^1(G_n; A_n) = 1$, the mapping $\xi \to \{\xi_\sigma\}$ 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 ω_σ ($\sigma \in G_n$) 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 π_n of F_n. Since A_n/B_n is an infinite cyclic group generated by the coset of $\pi_n \bmod B_n$, 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

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

with an element γ in C_n. Since $\pi_n\gamma^{-1}$ is also a prime element of F_n, we

replace π_n by $\pi_n\gamma^{-1}$ and denote the latter again by π_n. Then we have

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

As in the above, let $\pi_n^{\sigma-1} = \beta_\sigma\eta_\sigma$. Then $g(\beta_\sigma) = g(\pi_n^{\sigma-1}) = \omega_\sigma^m$ $(\sigma \in G_n)$ 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

$$f \circ g \circ h(\sigma-1) = m(\sigma-1), \qquad \sigma \in G_n.$$

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 π_n is any prime element of F_n satisfying $B_n = U \times W \times D(\pi_n)$; π_n need not be the particular prime element obtained in the above argument. Clearly, there is an O_p-homomorphism ψ of I_n onto $D(\pi_n)$ such that $\psi(\sigma-1) = \beta_\sigma$. Since $\beta_{\tau\sigma} = \beta_\sigma\beta_\tau^\sigma$, ψ 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 ψ 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 π_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 Ω. It is known that E is an abelian extension of Q_p generated by all roots of unity in Ω whose orders are prime to p, and also that the Galois group $G(E/Q_p)$ is isomorphic with the so-called total completion $\bar{Z}$ 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 ${}^p\bar{Z}$ of Z. Furthermore, for each $n \geqq 0$, EF_n is the maximal unramified extension of F_n in Ω, and $E'F_n$ is the maximal p-complementary unramified extension of F_n in Ω. Let L_n be the maximal p-complementary abelian extension of F_n in Ω. Then $E'F_n$ 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 $B_n/B_n^0 \cong V$. Since $F_n \cap L_0 = F_0$, $G(F_nL_0/F_n) \cong G(L_0/F_0)$, 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

$$F_nL_0 = L_n, \qquad n \geqq 0.$$

If F_n' denotes the unique subfield of F_n with degree p^n over Q_p, then we also have

$$F_n'L_0 = L_n, \quad F_n' \cap L_0 = Q_p, \qquad n \geqq 0.$$

Let F' be the union of the increasing sequence of subfields F_n' in Ω. 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 Ω is, as one sees easily, the maximal p-complementary abelian extension of F in Ω. 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 Ω, respectively. Then*

$$F'L_0 = L, \quad F' \cap L_0 = Q_p,$$

$$G(L/Q_p) = G(L/F') \times G(L/L_0),$$

$$G(L/F') \cong G(L_0/Q_p), \quad G(L/L_0) \cong G(F'/Q_p) \cong U^0.$$

Furthermore, $G(L_0/Q_p)$ is the p-complementary completion of a group generated by two elements σ and τ satisfying the only relations

$$\sigma\tau\sigma^{-1} = \tau^p, \quad \tau^{(p-1)^2} = 1;$$

σ is a Frobenius automorphism for L_0/Q_p and τ is a generator of the inertia group for L_0/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 element λ and μ satisfying the only relations*

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

THEOREM 3. *Let L and M be as in the above and let K be the maximal p-primary abelian extension of F in Ω 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

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

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 subgroups H of X such that

$$HP=X, \quad H\cap P=1, \quad H\cong X/P.^{6)}$$

Such a group H also satisfies $HN=G(M/F')$. On the other hand, since $P/N=G(L/L_0)\cong U^0$, there is an element σ 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 σ. Using $P/N\cong U^0$, we then see easily that

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

Since both N and $HN=G(M/F')$ 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 τ in N such that $\tau\sigma H\sigma^{-1}\tau^{-1}=H$.[7)] Let $\sigma'=\tau\sigma$. Then $N\sigma=N\sigma'$, and the closure S' of the cyclic subgroup of P generated by σ' also satisfies $NS'=P$ and $N\cap S'=1$. Furthermore, since $\sigma' H\sigma'^{-1}=H$, 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.[8)] 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.