On l-extension with given ramification points over a real quadratic field,

By Kazuo AMANO

(*Dep. of Math., Fac. of Gen. Educ., Gifu univ.*)

Received Oct., 31. 1969

Introduction

Let l ($\neq 2$) be a fixed rational prime number and $\mathfrak{G}$ the Galois group of a field extension K/k. We shall be interested in these groups in the case where k is a local or global field and K its maximal l-extension, i.e., the maximal normal extension whose Galois group is a pro-l-group. In the algebraic number theory, it is an important problem to determine concretely the structure of these groups. This problem is completely solved if k is a local number field [6]. But, for an algebraic number field k, it is not complete. In this case, I.R.Šafarevič [7] has pointed out the interest and importance of the group $\mathfrak{G}_S$, the Galois group of the maximal l-extension of k unramified outside of a set of prime divisors of k. In the present note, we shall give the structure of the group $\mathfrak{G}_S$ for a real quadratic field k and for a special set S.

Basic consideration

We shall introduce the following notation,

k : a finite algebraic number field

$k^{(\infty)}$: the maximal l-extension over k

$\mathfrak{G}$: the Galois group of the l-extension $k^{(\infty)}/k$

S : a finite set of finite prime divisors of k

$k_S^{(\infty)}$: the maximal l-extension unramified outside of S over k

$\mathfrak{G}_S$: she Galois group of the l-extension $k_S^{(\infty)}/k$.

It is obvious that the group $\mathfrak{G}_S$ is the factor group of $\mathfrak{G}$ modulo the normal subgroup generated by the inertia groups of $\mathfrak{P}$'s, where $\mathfrak{P}$ is a prime divisor in $k^{(\infty)}$ and $\mathfrak{P}$ divides $\mathfrak{P} \notin$ S.

Therefore $\mathfrak{G}_S$ is obtained from the knowledzes of $\mathfrak{G}$ and the inertia groups. More precisely, as is well known, the following is a exact sequence,

$$1 \longrightarrow \mathfrak{U}/k^{\times}\mathbf{I}^{l}\mathfrak{U} \longrightarrow \mathbf{I}/k^{\times}\mathbf{I}^{l} \longrightarrow C(k)/C(k)^{l} \longrightarrow 1,$$

where $\mathbf{I}$ is the ideles group, $\mathfrak{U}$ the unit ideles group, $C(k)$ the ideal classes group, $\mathbf{I}^{l}$ the l-th. power of $\mathbf{I}$,and $k^{\times}$ the multiplicative group of k.

Then generators of $\mathfrak{G}$ are obtained from the norm residue symbols for generators of $\mathbf{I}/k^{\times}\mathbf{I}^{l}$. Hence we may choose for generators of $\mathbf{I}/k^{\times}\mathbf{I}^{l}$ the preimages of a basis of

the finite cokernel and for each divisor $\mathfrak{p}$ the basis of $\mathfrak{U}_\mathfrak{p}/\mathfrak{U}_\mathfrak{p}^l$.

Especially, if k has class number one, we may only consider the generators of $\mathfrak{U}_\mathfrak{p}/\mathfrak{U}_\mathfrak{p}^l$. from now on, we shall only consider the field k with class number one. For any idele $\mathfrak{A}\in\mathbf{I}$, the norm residue symbol $(\mathfrak{A}, k^{(1)}/k)$ induces the map of $\mathfrak{U}/k^\times \mathbf{I}^l\mathfrak{U}\cong \mathbf{I}/k^\times\mathbf{I}^l$ onto $\mathfrak{G}/\mathfrak{G}^l[\mathfrak{G},\mathfrak{G}]$, where $[\mathfrak{G},\mathfrak{G}]$ is the commutators group of $\mathfrak{G}$ and $k^{(1)}$ the maximal abelian l-extension over k with Galois group $\mathfrak{G}/[\mathfrak{G},\mathfrak{G}]$.

By virtue of local field theory, for any $\mathfrak{p}$-adic unit $u_\mathfrak{p}$, $(u_\mathfrak{p}, k^{(1)}/k)$ is an element of the inertia grop in $k^{(1)}/k$. Hence it is unit in $\mathfrak{G}_S$ for $\mathfrak{p}\in$S.

As above mention, the studies of $\mathfrak{G}_S$ are reduced to study the structure of $\mathfrak{U}_\mathfrak{p}/\mathfrak{U}_\mathfrak{p}$ for $\mathfrak{p}\in$ S.

Structure of G_S

Let k be a real quadratic field with class number one over rational field Q, i,e., $k=Q(\sqrt{d})$ for $d>$o, η the unique fundamental unit in k, and $\mathfrak{U}_\mathfrak{p}$ the units group in $\mathfrak{p}$-adic field $k_\mathfrak{p}$ for each $\mathfrak{p}$. In addition, we suppose that the set S consists of two prime divisors p and l which are also prime divisors in k. By virtue of local field theory [2, 5], the following lemma is well known.

LMEMA 1. The base of $\mathfrak{U}_p/\mathfrak{U}_p^l$ is $\{\zeta_{p^2-1}\}$, where ζ_{p^2-1} is the primitive $(p^2-1)-$th. root of unit. The base of $\mathfrak{U}_l/\mathfrak{U}_l^l$ is $\{1+l,\ 1+l\sqrt{d}\}$.

LEMMA 2. *Put* $\eta\equiv(1+l)^{a_1}\ (1+1\sqrt{d})^{a_2}$ *in* $\mathfrak{U}_l/\mathfrak{U}_l^l$, *where* a_1 *and* a_2 *are* l*-adic integers. Then we have* $a_2\not\equiv$ o *(mod* l*).*

Proof. Let Δ be the discriminant of k. We put $\eta=\frac{a+b\sqrt{\Delta}}{2}$ and $\eta^{l^2-1}=\frac{A+B\sqrt{\Delta}}{2}$, where a, b, A, and B are rational integers. By Fermat theorem, we have $\frac{A}{2}\equiv1$(mod l,) $\not\equiv1$(mod l^2), and $\frac{B}{2}\equiv$o (mod l). On the other hand, since l^2-1 is even, we have $A^2-\Delta B^2=4$. Hence $B\not\equiv$o (mod l^2). In other words, $a_2 l\not\equiv$o (mod l^2) and therfore $a_2\not\equiv$o (mod l^2),

We shall denote by $(\alpha)_p$ the idele of k such that its p-component is α and the other 1. We put

$$\bar{\tau}_p = ((\zeta_{p^2-1})_p,\ \overset{(1)}{k_S}/k)$$
$$\bar{\tau}_{l,1} = ((1+l)_l,\ \overset{(1)}{k_S}/k)$$
$$\bar{\tau}_{l,2} = ((1+l\sqrt{d})_l,\ \overset{(1)}{k_S}/k)$$

where $\overset{(1)}{k_S}/k$ is the maximal abelian l-extension unramified outside of S over k. We denote by τ the preimage of τ for the map of $\mathfrak{G}_S$ onto $\mathfrak{G}_S/[\mathfrak{G}_S,\mathfrak{G}_S]\mathfrak{G}_S^l$.

PROPOSITION 3. *Let* k, S *and* $\mathfrak{G}_S$ *be as above. Then the group* $\mathfrak{G}_S$ *is generated by miniimal system* $\{\tau_p, \tau_{l,1}\}$.

Proof. It is obvious that $\bar{\tau}_p$, $\bar{\tau}_{l.1}$ and $\bar{\tau}_{l.2}$ are generators system. On the other hand, we have

$$1=((\eta),\ \overset{(1)}{k_S}/k)=((\zeta_{2-1})_p,\ \overset{(1)}{k_S}/k)^\alpha((1+l)_l,\ \overset{(1)}{k_S}/k)^{a_1}((1+l\sqrt{d})_l,\ \overset{(1)}{k_S}/k)^{a_2}$$
$$=\bar{\tau}_p{}^\alpha\ \bar{\tau}_{l.1}{}^{a_1}\ \bar{\tau}_{l.2}{}^{a_2}$$

Since $a_2\not\equiv$o (mod l), $\bar{\tau}_p$ and $\bar{\tau}_{l.1}$ are minimal generators system. Therefore, we have

our proposition.

The following is well known[4].

PROPOSITION 4. *Let k be a finite $\mathfrak{p}$-adic extension of Qp and $N(\mathfrak{p})\equiv 1 (mod\ l)$. Then the Galois group $\mathfrak{G}$ of the maximal l-extension over $k_{\mathfrak{p}}$ is a pro-l-group with two generators σ, τ, and a single relation $\sigma^{-1}\tau\sigma=\tau^{N\mathfrak{p}}$ where σ is a Frobenivs-automorphism of the maximal unramified l-extension and τ a generator of the cyclic inertia group of $\mathfrak{G}$.*

We put $\bar{\sigma}_p=((p)_p, \overset{(1)}{k_S}/k)$. Then it is obvious that σ_p is a Frobenius-automrphism of the maximal l-extension over k_{l^ν} and $\bar{\tau}_p$ a generator of the cyclic inertia group of $\mathfrak{G}$.

LEMMA 5. *Put $p\equiv(1+l)^b$ in $\mathfrak{U}_l/\mathfrak{U}_l{}^l$, where b is p-adic integer. Then we have $b\not\equiv o$ $(mod\ l)$ if and only if $p\equiv 1$ $(mod\ l)$ and $p\not\equiv 1$ $(mod\ l^2)$.*

Proof. Put $p=\sum_{i=o}^{\infty} a_i\, p^i$ in Q_{l^ν}. Then we have that $a_0\equiv 1$ (mod l) and $a_1\not\equiv o$ (mod l^2) are equivalent to $p\equiv 1$ (mod l) and $p\not\equiv 1$ (mod l^2). Therefore we have our lemma.

THEOREM 6. *Let k, S and $\mathfrak{G}_S$ be as above and let $p\not\equiv 1$ $(mod\ l^2)$. Then $\mathfrak{G}_S$ is a pro-1-group with two generators σ_p, τ_p and a single relation $\sigma_p^{-1}\tau_p\sigma_p=\tau_p{}^{p^{2-1}}$ Proof.* Since

$$1=((p)\ \overset{(1)}{k_S}/k)=((p)_p, \overset{(1)}{k_S}/k)\ ((p)_l, \overset{(1)}{k_S}/k)\ ((p)_p, \overset{(1)}{k_S}/k)\ ((1+l)_l, \overset{(1)}{k_S}/k)^b$$
$$=\bar{\sigma}_p\, \bar{\tau}_{p\cdot 1}{}^b$$

and lemma 5, $\tau_{l\cdot 1}$ is generated by σ_p . By virtue of proposition 3 and 4, we have our theorem.

References

1) E.Artin and J.Tate, Class field theory, Hahvard (1961)
2) H.Hasse, Zahlentheorie, Berlin Akademie-Verlage (1949)
3) Y.Kawada, On the structure of the Galois group of some infinite extensions, J. Fac. Sci., Univ. of Tokyo, Sect. I,7 (1954) 1-18
4) H.Koch, l-Erweiterungen mit vorgegebenen Verzeigungsstellen, J. f. reine u. angew. Math. 219 (1965) 30-61
5) J.-P. Serre, Corps locaux, Hermann Paris (1962)
6) J.-P.Serre, Cohomologie Galoisienne, Berlin (1964)
7) I.R. Šafarevič, Algebraic number fields (Russian,) Proc. Int. Congr. Math. Stockholm (1962) 163-173