S. HAMADA
KODAI MATH. J.
2 (1979), 406—410

SOME REMARKS ON THE LUBIN-TATE EXTENSIONS

BY SUGURU HAMADA

In this paper, we consider the possibility of characterization of the Lubin-Tate extensions, among the totally ramified abelian extensions over a local number field K, by means of their Galois groups.

The tamely ramified case is well known (Remark 1). In other cases, if K is a finite unramified local number field, the Lubin-Tate extension is characterized by the order and the exponent of its Galois group (Theorem). However, in general such characterization of Lubin-Tate extension is impossible; namely, we can find fields K over which their exist always other totally ramified abelian extensions whose Galois groups are isomorphic to those of Lubin-Tate extensions (Proposition 1).

Finally, we give a remark on the composite of two Lubin-Tate extensions (Proposition 2).

NOTATIONS. $\mathbf{Z}$: the ring of rational integers. p: a prime number. $\mathbf{Z}_p$: the ring of p-adic integers. $\mathbf{Q}_p$: the field of p-adic numbers. K: a finite extension of $\mathbf{Q}_p$. π: a prime element of K. $\mathfrak{p}$: the maximal ideal of K. U: the group of units of K. H_m: the multiplicative group $1+\mathfrak{p}^m$ ($m=1, 2, \cdots$). q: the number of elements of the residue class field of K. ρ: a primitive $(q-1)$-th root of unity in K. $M^\times$: the multiplicative group of a field M. $\langle\alpha\rangle$: the cyclic group generated by α. $N_{M/N}$: the norm map of a field extension M/N. $\mathrm{Gal}(M/N)$: the Galois group of a Galois extension M/N.

Now, the Lubin-Tate extension $L(\pi, m)$ is defined as follows; For $f(X)=X^q+\pi X$ let $\lambda_n (n=1, 2, \cdots)$ be elements of an algebraic closure of $\mathbf{Q}_p$ such that $f(\lambda_1)=0$ $(\lambda_1\neq 0)$, $f(\lambda_n)=\lambda_{n-1} (n\geqq 2)$ and we set $L(\pi, m)=K(\lambda_m)$.

Then $L(\pi, m)$ is a totally ramified abelian extension of K such that $N_{L(\pi, m)/K}(L(\pi, m)^\times)=\langle\pi\rangle H_m$ and $\mathrm{Gal}(L(\pi, m))\cong U/H_m$ (J. Lubin and J. Tate [3]).

THEOREM. *Let $K/\mathbf{Q}_p$ $(p\neq 2)$ be a finite unramified extension and M/K be a finite totally ramified abelian extension. Then $M\subseteqq L(\pi, m)$ for some π if and only if the exponent of* $\mathrm{Gal}(M/K)$ *is a divisor of $(q-1)p^{m-1}$. Moreover, if the order of* $\mathrm{Gal}(M/K)$ *is $(q-1)q^{m-1}$ then $M=L(\pi, m)$ for some π.*

Proof. "If" part: Let $N_{M/K}(U_M)=U'$ where U_M is the group of units of M. By class field theory $\mathrm{Gal}(M/K)\cong U/U'$. Since the exponent of $\mathrm{Gal}(M/K)$ is a

Received July 17, 1978

divisor of $(q-1)p^{m-1}$ we have $U^{(q-1)p^{m-1}} \subseteqq U'$.

On the other hand $U=\langle\rho\rangle \times H_1$ (direct), $H_1^{q-1}=H_1$ because $q-1$ is a unit of Z_p, and $H_n^p=H_{n+1}$ $(n=1, 2, \cdots)$ because $p\neq 2$ and K/Q_p is unramified (J. P. Serre [4]).

Hence $U^{(q-1)p^{m-1}}=H_m$ and we have $H_m \subseteqq U'$. Now let $N_{M/K}(\pi_M)=\pi$ where π_M is a prime element of M then $\langle\pi\rangle H_m \subseteqq \langle\pi\rangle U'$ and $L(\pi, m) \supseteqq M$ by class field theory.

Moreover, if the order of $\mathrm{Gal}(M/K)$ is $(q-1)q^{m-1}$ we have $L(\pi, m)=M$ since $[L(\pi, m):K]=(q-1)q^{m-1}$.

"Only if" part: Suppose $M \subseteqq L(\pi, m)$. Let $\pi'=N_{M/K}(\pi_M)$ and $U'=N_{M/K}(U_M)$, then we have $\langle\pi'\rangle U' \supseteqq \langle\pi\rangle H_m$. From this it follows $U' \supseteqq H_m$. We have shown the exponent of U/H_m is a divisor of $(q-1)p^{m-1}$ so the exponent of $\mathrm{Gal}(M/K) \cong U/U'$ is also a divisor of $(q-1)p^{m-1}$.

COROLLARY. *M/Q_p $(p\neq 2)$ is a totally ramified abelian extension of degree $(p-1)p^{m-1}$ if and only if $M=L(pu, m)$ for some unit u of Z_p.*

The following is well known (S. Lang [2]).

REMARK 1. For arbitrary p, let K/Q_p a finite extension. Then M/K is a totally ramified abelian extension of degree $q-1$ if and only if $M=L(\pi, 1)$ for some π.

Proof. Since $H_1^{q-1}=H_1$ for arbitrary p and K, the proof is similar to that of Theorem.

Next we show

PROPOSITION 1. *Let $K=Q_p(\zeta_n)$ where $p\neq 2$ and $\zeta_n (n\geqq 2)$ is a primitive p^n-th root of unity.*

Then for any $m\geqq 2$, there exists a totally ramified abelian extension M over K such that $\mathrm{Gal}(M/K)\cong U/H_m$ *and $M\neq L(\pi, m)$ for any prime element π of K.*

For the proof, we sketch the proof of the structure theorem of H_1 of $K=Q_p(\zeta_n)$ where p is an arbitrary prime and $n\geqq 1$, following to H. Hasse (H. Hasse [1]).

Let $e=[K:Q_p]=(p-1)p^{n-1}$, $e_1=p^{n-1}$, $\pi=1-\zeta_n$ and R_t be a complete system of representatives of H_t/H_{t+1} (we take 1 as the representative of the class of 1).

Then every element η of H_1 is written uniquely as follows;

$$\eta=\prod_{t=1}^{\infty} \eta_t \qquad (\eta_t \in R_t).$$

And for $\xi \in H_1$ such that $\xi \equiv 1+\alpha\pi^{\iota} \bmod \mathfrak{p}^{\iota+1}$ for some integer α in K we have

$$(*) \qquad \begin{cases} \xi^p \equiv 1+\alpha^p\pi^{\iota p} \bmod \mathfrak{p}^{\iota p+1} & \text{if} \quad \iota<e_1 \\ \xi^p \equiv 1-\varepsilon\alpha\pi^{\iota+e} \bmod \mathfrak{p}^{\iota+e+1} & \text{if} \quad \iota>e_1 \end{cases}$$

where $-p=\varepsilon\pi^e$.

We set $F=\{i\,|\,1\leqq i<e_1p,\ (i,\ p)=1\}$ then e integers k $(e_1<k\leqq e_1p)$ are written uniquely $k=ip^{\kappa_i}$, $(i\in F$ and $n\geqq\kappa_i\geqq 0)$. Then every positive integer t is written uniquely and by (*) the corresponding R_t is given as follows; Case I. If $1\leqq t\leqq e_1$ then $t=ip^{\nu_i}$, $i\in F$, $\nu_i=0,\ 1,\ \cdots,\ \kappa_i-1$ and $R_t=\{(1-\pi^i)^{ap^{\nu_i}}\,|\,0\leqq a\leqq p-1\}$.

Case II(i). If $e_1<t=e_1+se+r$, $0\leqq s$ and $1\leqq r<e$ then $t=ip^{\kappa_i}+se$, $i\in F\,(i\neq 1)$ and $R_t=\{(1-\pi^i)^{ap^{\kappa_i+s}}\,|\,0\leqq a\leqq p-1\}$.

Case II(ii). If $e_1<t=e_1+se+e=e_1p+se$, $0\leqq s$ $R_t=\{(1-\pi^{e_1p})^{ap^s}\,|\,0\leqq a\leqq p-1\}$. We remark $(1-\pi)^{e_1p}=1$.

Thus every element η of H_1 is written uniquely as follows;

$$\eta=\prod_{t=1}^{\infty}\eta_t=(1-\pi)^{a_1}\cdot\prod_{i\in F,\,i\neq 1}(1-\pi^i)^{a_i}\cdot(1-\pi^{e_1p})^{a_{e_1p}}$$

where $a_1\in Z \bmod p^n$ reduced, $a_i\in Z_p$ and $a_{e_1p}\in Z_p$.

And

$$(*1)\qquad \begin{cases} H_1\cong Z/(p^n)\times Z_p\times\cdots\times Z_p & \text{(direct)}\\ \eta\longmapsto(\bar{a}_1,\ a_2,\ \cdots,\ a_{e_1p-1},\ a_{e_1p}) \end{cases}$$

where $\bar{a}_1$ is the class of a_1 in $Z/(p^n)$.

Next, in order to write down the structure of H_1/H_m, in the Case I, for integer m such that $1\leqq m\leqq e_1$, let m_j $(j=0,\ 1,\ \cdots,\ n-1)$ be the number of the elements of the set $G_j\ (m)=\{i\,|\,i\in F,\ m/p^j\leqq i<m/p^{j-1}\}$ and in the Case II(i), for integer $m=e_1+se+r$ $(0\leqq s,\ 1\leqq r<e)$, we set $I(m)=\{i\,|\,i\in F,\ ip^{\kappa_i}<e_1+r\}$ and $J(m)=\{i\,|\,i\in F,\ e_1+r\leqq ip^{\kappa_i}<e_1p\}$.

LEMMA 1. *Let $K=Q_p(\zeta_n)$ where p is a prime and $n\geqq 1$ then we have;*
Case I. If $1\leqq m\leqq e_1$ then

$$H_1/H_m\cong\prod_{j=0}^{n-1}C_{p^j}^{m_j}\qquad (direct).$$

Case II(i). If $e_1<m=e_1+se+r$, $0\leqq s$, $1\leqq r<e$ then

$$H_1/H_m\cong C_{p^n}\times(\prod_{i\in I(m)}C_{p^{\kappa_i+s+1}}\times\prod_{i\in J(m)}C_{p^{\kappa_i+s}})\times C_{p^s}\qquad (direct).$$

Case II(ii). If $e_1<m=e_1p+se$, $0\leqq s$ then

$$H_1/H_m\cong C_{p^n}\times(\prod_{i\in F,\,i\neq 1}C_{p^{\kappa_i+s+1}})\times C_{p^s}\qquad (direct)$$

where C_{p^u} is a cyclic group of order p^u and $C_{p^u}^v$ is the direct product of v copies of C_{p^u}'s.

Proof. By the uniqueness of the representation $\eta=\prod_{t=1}^{\infty}\eta_t$ $(\eta_t\in R_t)$ we have $\eta\in H_m$ if and only if $\eta_t=1$ for all t, $1\leqq t<m$.

Thus, in the Case I, $\eta=(1-\pi)^{a_1}\cdot\prod_{i\in F,\,i\neq 1}(1-\pi^i)^{a_i}\cdot(1-\pi^{e_1p})^{a_{e_1p}}$ belongs to H_m if and only if

(*2) $a_i \equiv 0 \bmod p^j$ for such $i \in F$ as $ip^{j-1} < m \leqq ip^j$ (i. e $i \in G_j(m)$) $(j=0, 1, \cdots, n-1)$.

Analogousely, in the Case II(i) $\eta \in H_m$ if and only if

$$(*3)\quad \begin{cases} a_1 = 0 \bmod p^n, \quad a_i \equiv 0 \bmod p^{\kappa_i+s+1} & \text{if } i \in I(m) \\ a_i \equiv 0 \bmod p^{\kappa_i+s} \quad \text{if } i \in J(m) \text{ and } a_{e_1 p} \equiv 0 \bmod p^s. \end{cases}$$

And, in the Case II(ii) $\eta \in H_m$ if and only if

$$(*4)\quad \begin{cases} a_1 = 0 \bmod p^n, \quad a_i \equiv 0 \bmod p^{\kappa_i+s+1} & \text{if } i \in F (i \neq 1) \\ \text{and } \quad a_{e_1 p} \equiv 0 \bmod p^s. \end{cases}$$

Thus, the Lemma follows from the isomorphim (*1).

LEMMA 2. *Let $K = Q_p(\zeta_n)$, $p \neq 2$ and $n \geqq 2$. Then for any integer $m \geqq 2$ their exists a subgroup U' of H_1 such that $U' \neq H_m$ and $H_1/U' \cong H_1/H_m$.*

Proof. As for the Case I of Lemma 1, let U' be the group consisting of those η,

$$\eta = (1-\pi)^{a_1} \cdot \prod_{i \in F, i \neq 1} (1-\pi^i)^{a_i} \cdot (1-\pi^{e_1 p})^{a_{e_1 p}}$$

where a_1 is arbitrary, $a_{e_1 p} \equiv 0 \bmod p^j$ if $1 \in G_i(m)$, and other a_i's satisfy the same conditions in (*2) of Lemma 1. Then, since $m > 1$ $1-\pi \notin H_m$ and $1-\pi \in U'$. Thus we have $H_m \neq U'$. While $H_1/U' \cong H_1/H_m$ because H_1/U' has also the type described in Case I of Lemma 1.

As for the Case II(i), let U' be the group consisting of those η in which $a_1 = 0 \bmod p^n$, $a_2 \equiv 0 \bmod p^s$, and

$$a_{e_1 p} \equiv \begin{cases} 0 \bmod p^{\kappa_2+s+1} & \text{if } 2 \in I(m) \\ 0 \bmod p^{\kappa_2+s} & \text{if } 2 \in J(m) \end{cases}$$

and other a_i's satisfy the same conditions in (*3). The since $n \geqq 2$, $\kappa_2 = n-1 \geqq 1$, $\kappa_2 + s > s$ and $\kappa_2 + s + 1 > s$ we have $(1-\pi^2)^{p^s} \notin H_m$, $(1-\pi^2)^{p^s} \in U'$ and $H_m \neq U'$. While $H_1/U' \cong H_1/H_m$ because H_1/U' has also the type described in Case II(i) of Lemma 1. As for the Case II(ii) the proof is similar as above.

Proof of Proposition 1. Let M be the class field which corresponds to the class group $\langle \pi \rangle U'$ where U' is that of Lemma 2. Then $U' \neq H_m$ implies $\langle \pi \rangle U' \neq \langle \pi u \rangle H_m$ for any $u \in U$, so that M is never a Lubin-Tate extension but Gal $(M/K) \cong U/U' \cong U/H_m$.

Remark 2. Lemma 2 does not hold for $n=1$; namely $H_1/U' \cong H_1/H_{p+1}$ if and only if $U' = H_{p+1}$.

Finally, we give a remark on the composite field of two Lubin-Tate extensions.

PROPOSITION 2. *Let p be a prime number, K a finite extension of* Q_p, *$L(\pi_1, n)$, $L(\pi_2, m)$ $(n \leqq m)$ two Lubin-Tate extensions over K, and d the order $\pi_1\pi_2^{-1} \bmod H_n$ in the group U/H_n.*

Then the inertia field of the composite field $L(\pi_1, n)L(\pi_2, m)$ is of degree d over K. $[L(\pi_1, n)L(\pi_2, m) : K]=(q-1)q^{m-1}d$ and $[L(\pi_1, n) \cap L(\pi_2, m) : K]=(q-1)q^{n-1}d^{-1}$.

Proof. By assumption we have $\langle\pi_1\rangle H_n \cap \langle\pi_2\rangle H_m = \langle\pi_2^d\rangle H_m = \langle\pi_2^d\rangle U \cap \langle\pi_2\rangle H_m$, so we have by class field theory $L(\pi_1, n)L(\pi_2, m) = T_d L(\pi_2, m)$ where T_d is the unramified extension of degree d over K. From this we have the Proposition immediately.

EXAMPLE. $\mathrm{Q}_2(\sqrt{3})(\sqrt{-1})$ is unramified of degree 2 over $\mathrm{Q}_2(\sqrt{3})$ (H. Hasse [1] p 214).

For, $\mathrm{Q}_2(\sqrt{3}) = L(-2, 2)$, $\mathrm{Q}_2(\sqrt{-1}) = L(2, 2)$ and -1 has order 2 mod H_2.

REFERENCES

[1] H. HASSE, Zahlentheorie, AKADEMIC-VERLAG, BERLIN (1969).
[2] S. LANG, Algebraic Number theory, Addison-Wesley (1970).
[3] J. LUBIN AND J. TATE, Formal complex multiplication in local fields, Ann. Math. 81 (1965) 380-387.
[4] J.P. SERRE, Corps Locaux, Hermann, Paris (1962).

DEPARTMENT OF MATHEMATICS
MIYAGI UNIVERSITY OF EDUCATION
SENDAI
DEPARTMENT OF MATHEMATICS
TOKYO INSTITUTE OF TECHNOLOGY
TOKYO