S. HAMADA
KODAI MATH. J
6 (1983), 47—50

NORM THEOREM ON SPLITTING FIELDS OF SOME BINOMIAL POLYNOMIALS

By Suguru Hamada

Let K be a finite algebraic number field and let M/K be a finite Galois extension. Let Knot (M/K) be the factor group $\{a \in K^{\times}$, a is a local norm everywhere$\} / \{a \in K^{\times}$, a is a global norm$\}$. Hasse's norm theorem asserts that if M/K is a cyclic extension then $\mathrm{Knot}(M/K)=1$. H. HASSE ([4]) showed that the norm theorem not always holds for arbitrary abelian extension by giving a counter example: $M=\boldsymbol{Q}(\sqrt{-39}, \sqrt{-3})$ and $K=\boldsymbol{Q}$, where $\boldsymbol{Q}$ is the field of rational numbers.

And related theories are in [1], [2], [3], [6], and [7]. In this paper we prove the following:

THEOREM. *Let p be an odd prime number, ζ a primitive p^r-th root of unity $(r \geqq 1)$, K a finite algebraic number field, $L=K(\zeta)$ and $M=L(a^{1/p^r})$ $(a \in K)$.*

If $f(X)=X^{p^r}-a$ is irreducible in $L[X]$ then $\mathrm{Knot}(M/K)=1$. When $\sqrt{-1} \in K$ the same assertion holds also for $p=2$.

In Remark, by examples, we shall show that in Theorem if we replace p^r by a number which is not a power of an odd prime number or by 2^r ($r \geqq 2$ and $\sqrt{-1} \notin K$) then the conclusion is not always valid.

In § 1, we shall prove Theorem and Remark by determing $\mathrm{Knot}(M/K)$ explicitely by the following Lemma:

LEMMA. *Let l, n be positive integers and let G be a group of order ln generated by two elements σ, τ whose fundamental relations are $\sigma^l=\tau^n=1$, $\tau\sigma\tau^{-1}=\sigma^m$ $(1 \leqq m < l$ and m^n-1 is a multipler of $l)$. Then $H^3(G, Z) \approx Z/dZ$ where $d=(1+m+\cdots+m^{n-1}, l, (m^n-1)/l, m-1)$ and Z is the ring of rational integers on which G operates trivially.*

In § 2, we shall give a proof of the Lemma as a corollary of a proposition in [4].

§ 1. Proofs of Theorem and Remark.

In the following the notations are same as those in our Theorem. Let $G=$

Received January 13, 1982

Gal(M/K) be the Galois group of M/K, $M^\times$ the multiplicative group of M, J_M the idèle group of M, and C_M the idèle class group of M.

Then the exact sequence

$$1 \longrightarrow M^\times \longrightarrow J_M \longrightarrow C_M \longrightarrow 1$$

gives an exact sequence

$$\cdots \longrightarrow H^{-1}(G, C_M) \longrightarrow H^\circ(G, M^\times) \longrightarrow H^\circ(G, J_M) \longrightarrow H^\circ(G, C_M) \longrightarrow \cdots .$$

By Tate's Theorem, we have $H^{-1}(G, C_M) \approx H^{-3}(G, Z)$. In the following, by Lemma we show that $H^{-3}(G, Z)=0$ then we have an exact sequence $1 \to H^\circ(G, M^\times) \to H^\circ(G, J_M)$.

Therefore, the canonical map $K^\times/N_{M/K}M^\times \to J_K/N_{M/K}J_M$ is injective and we have Theorem. Now we show that $H^3(G, Z)=0$ by Lemma then $H^{-3}(G, Z)=0$ follows because in general $H^{-3}(G, Z) \approx H^3(G, Z)$.

First let $p \neq 2$, $[L:K]=n$, $\theta=a^{1/p^r}$ and ρ a rational integer such that $\rho \bmod p^r$ generates the units group of Z/p^rZ. By assumption, M/L is a cyclic Kummer extension of degree p^r and L/K is also a cyclic extension of degree n. Let σ, τ be the elements of G such that $\sigma(\theta)=\theta\zeta$, $\sigma(\zeta)=\zeta$; $\tau(\theta)=\theta$, $\tau(\zeta)=\zeta^m$, where $m \equiv \rho^{\varphi(p^r)/n} \bmod p^r$ (φ is Euler's function and $1 \leqq m < p^r$).

Then $G=\langle\sigma, \tau\rangle$, $\sigma^{p^r}=\tau^n=1$, $\tau\sigma\tau^{-1}=\sigma^m$ and G is a group of the type in Lemma. Therefore, we have $H^3(G, Z)=Z/dZ$ where $d=(1+m+\cdots+m^{n-1}, p^r, (m^n-1)/p^r, m-1)$. We show that $d=1$.

Now, $d \neq 1$ if and only if $m \equiv 1 \bmod p$, $n \equiv 0 \bmod p$ and $(m^n-1)/p^r \equiv 0 \bmod p$. While if $n \equiv 0 \bmod p$, we have $m^n \equiv \rho^{\varphi(p^r)} \bmod p^{r+1}$ and $\rho^{\varphi(p^r)} \not\equiv 1 \bmod p^{r+1}$, because in fact n is a divisor of $\varphi(p^r)$ and $n \equiv 0 \bmod p$ implies $r \geqq 2$. Therefore we have $(m^n-1)/p^r \not\equiv 0 \bmod p$ and $d=1$.

Next let $p=2$, $\sqrt{-1} \in K$ and $[L:K]=n$. If $r \leqq 2$ we have the result immediately, so let $r \geqq 3$. Since $\sqrt{-1} \in K$, Gal(L/K) is also a cyclic group generated by τ_0 such that $\tau_0(\zeta)=\zeta^m$ where $m \equiv 5^{2^{r-1}/n} \bmod 2^r$ and $1 \leqq m < 2^r$.

And $G=\langle\sigma, \tau\rangle$ ($\sigma(\theta)=\theta\zeta$, $\sigma(\zeta)=\zeta$; $\tau(\theta)=\theta$, $\tau(\zeta)=\zeta^m$), $\sigma^{2^r}=\tau^n=1$ and $\tau\sigma\tau^{-1}=\sigma^m$. Now if $n \equiv 0 \bmod 2$ we have $m^n \equiv 5^{2^{r-2}} \bmod 2^{r+1}$, and $5^{2^{r-2}} \not\equiv 1 \bmod 2^{r+1}$. Therefore $H^3(G, Z)=0$ follows just as the case $p \neq 2$.

Thus the proof of Theorem is completed.

Remark. In Theorem, if we replace p^r by a number which is not a power of an odd prime number, or by 2^r ($r \geqq 2$, $\sqrt{-1} \notin K$) then our Theorem not always holds.

To show this, we use the following well known theorem ([1] p. 198). Let K be a finite algebraic number field and let M/K be a finite Galois extension with Galois group $G=G(M/K)$. For each prime divisor $\mathfrak{p}$ of K, we fix a prime divisor $\mathfrak{P}$ of M lying above $\mathfrak{p}$ and let $G_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$. Let F be the subgroup of $H^{-3}(G, Z)$ generated by all cor$(H^{-3}(G_{\mathfrak{P}}, Z))$ where $\mathfrak{p}$ runs over all prime divisors of K and cor is the correstriction homomorphism from $H^{-3}(G_{\mathfrak{P}}, Z)$ into $H^{-3}(G, Z)$. Then the theorem asserts that Knot$(M/K) \approx H^{-3}(G, Z)/F$.

In the following Examples, ζ_t is a primitive t-th root of unity.

EXAMPLE 1. Let $L=\boldsymbol{Q}(\zeta)$, $\zeta=\zeta_{21}$ and let K be the subfield of L which corresponds to the subgroup $\langle\tau_0\rangle$ of $\mathrm{Gal}(L/\boldsymbol{Q})$, where $\tau_0(\zeta)=\zeta^4$. Then we have $\mathrm{Knot}(M/K)\approx Z/3Z$ where $M=L(883^{1/21})$.

Proof. 883 is a prime number and $883\equiv 1 \bmod (21)^2$. We have $\mathrm{Gal}(M/K)=\langle\sigma, \tau\rangle$ ($\sigma(\theta)=\theta\zeta$, $\sigma(\zeta)=\zeta$; $\tau(\theta)=\theta$ and $\tau(\zeta)=\zeta^4$ where $\theta=883^{1/21}$), $\sigma^{21}=\tau^3=1$ and $\tau\sigma\tau^{-1}=\sigma^4$. By Lemma, we have $H^{-3}(G, Z)\approx Z/3Z$. On the other hand, for any prime divisor $\mathfrak{P}$ of M the decomposition group $G_{\mathfrak{P}}$ is cyclic. For the proof, we may consider only $\mathfrak{P}$ which is above 883, 3 or 7. When $\mathfrak{P}$ is above 883, $G_{\mathfrak{P}}\subseteqq \mathrm{Gal}(M/L)=\langle\sigma\rangle$ because the prime of K under $\mathfrak{P}$ splits completely in L. When $\mathfrak{P}$ is above 3 or 7 the prime of L under $\mathfrak{P}$ splits completely in M, because $X^{21}\equiv 883 \bmod 3^2$ or $\bmod 7^2$ has a solution $X=1$. Hence the order of $G_{\mathfrak{P}}$ is $\leqq 3$ and $G_{\mathfrak{P}}$ is cyclic. Therefore for any $\mathfrak{P}$, $H^{-3}(G_{\mathfrak{P}}, Z)=0$ and by the above theorem we have $\mathrm{Knot}(M/K)\approx Z/3Z$.

EXAMPLE 2. Let $K=\boldsymbol{Q}$, $L=\boldsymbol{Q}(\zeta_4)=\boldsymbol{Q}(\sqrt{-1})$, and $M=L(17^{1/4})$, then $\mathrm{Knot}(M/K)\approx Z/2Z$.

Proof. $\mathrm{Gal}(M/K)=\langle\sigma, \tau\rangle$, $\sigma^4=\tau^2=1$ and $\tau\sigma\tau^{-1}=\sigma^3$. By Lemma, we have $H^3(G, Z)\approx Z/2Z$. On the other hand, just as Example 1, we see that for any prime divisor $\mathfrak{P}$ of M, $G_{\mathfrak{P}}$ is cyclic and $\mathrm{Knot}(M/K)\approx Z/2Z$.

Remark. As we have seen in the proof of Theorem, we have a slightly generalized theorem as follows; let p be an odd prime number and let M/K be a finite Galois extension. If $\mathrm{Gal}(M/K)=\langle\sigma, \tau\rangle$, $\sigma^{p^r}=\tau^n=1$ $(n\,|\,\varphi(p^r))$, $\langle\sigma\rangle\cap\langle\tau\rangle=1$, $\tau\sigma\tau^{-1}=\sigma^m$ and $m \bmod p^r$ has order n in the unit group of Z/p^rZ, then $\mathrm{Knot}(M/K)=1$. We have also a similar generalization for $p=2$.

2. A Proof of Lemma.

Let G be a group of the type in Lemma: G is a group of order ln, generated by two elements σ, τ with fundamental relations $\sigma^l=\tau^n=1$, $\tau\sigma\tau^{-1}=\sigma^m$ where $1\leqq m<l$ and m^n-1 is a multipler of l. In the following, let $N=1+\sigma+\cdots+\sigma^{l-1}$, $\Delta=1-\sigma$, $S=1+\sigma+\cdots+\sigma^{m-1}$, $T_i=\tau^{-1}S^i$, $N_i=1+T_i+\cdots+T_i^{n-1}$, $\Delta_i=1-T_i$ and $L_i=\dfrac{(l_0N+1)^i-1}{N}$, where $i\geqq 0$ and $l_0=(m^n-1)/l$.

For a left G-module A, in [4], by giving a free resolution of G, we determined cohomology groups $H^r(G, A)$ as follows:

PROPOSITION. *Let* $M_1=\begin{pmatrix}\Delta\\ \Delta_0\end{pmatrix}$, $M_2=\begin{pmatrix}N & 0\\ \Delta_1 & -\Delta\\ 0 & N_0\end{pmatrix}$ *and for* $q\geqq 1$

$$M_{2q+1}=\left(\begin{array}{cc:c} \Delta & 0 & \\ & & 0 \\ \Delta_q & -N & \\ \hdashline L_q & N_q & \\ & & M_{2q-1} \\ 0 & & \end{array}\right), \qquad M_{2(q+1)}=\left(\begin{array}{cc:c} N & 0 & \\ & & 0 \\ \Delta_{q+1} & -\Delta & \\ \hdashline 0 & N_q & \\ 0 & -L_q & M_{2q} \\ 0 & & \end{array}\right),$$

where 0 *means that all elements in the places are* 0. *Then*

$$H^i(G, A)=\{a\}/\{M_ib\} \qquad (i=1, 2, \cdots),$$

where $\{a\}=\{a=(a_1, \cdots, a_{i+1})^t$(column vector)$|\, a_j\in A$ *and* $M_{i+1}a=0\}$ *and* $\{M_ib\}=\{M_i(b_1, \cdots, b_i)^t|\, b_j\in A\}$.

Now we prove our Lemma by above Proposition. Since G operates trivially on Z, we have, for $r\in Z$, $Nr=lr$, $\Delta_2r=(1-m^2)r$, $\Delta r=\Delta_0r=0$, $N_1r=\mu r$ $(\mu=1+m+\cdots+m^{n-1})$, $L_1r=l_0r$, $\Delta_1r=(1-m)r$ and $N_0r=nr$.

By Proposition, $H^3(G, Z)\approx\{a\}/\{M_3b\}$ and direct computations give $\{a\}\approx\{x(r_0, -s_0)|\, x\in Z\}$ where $\mu=d_0s_0$, $l=d_0r_0$ $((s_0, r_0=1))$ and $\{M_3b\}\approx\{((1-m)y-lz, l_0y+\mu z)^t|\, y, z\in Z\}=\{(d_1y+d_0z)(r_0, -s_0)^t|\, y, z\in Z\}$, where $d_1=(m-1, l_0)$. (For convenience if $m-1=l_0=0$ we set $d_1=0$.)

Hence $\{M_3b\}\approx\{dx(r_0, -s_0)^t|\, x\in Z\}$, where $d=(d_0, d_1)$. Consequentely we have $H^3(G, Z)\approx Z/dZ$, where $d=(1+m+\cdots+m^{n-1}, l, (m^n-1)/l, m-1)$.

References

[1] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Proceedings of a Conference (Brighton 1965), LONDON-NEW YORK ACADEMIC PRESS 1967.

[2] D. A. Garbanti, The Hasse norm theorem for l-extensions of the rationals, In: Number and Algebra (ed. H. ZASSENHAUS), LONDON-NEW YORK ACADEMIC PRESS (1977), 77-90.

[3] D. A. Garbanti, The Hasse norm theorem for non-cyclic extensions of the rationals, Proc. London Math. Soc. (3) **37** (1978), 143-164.

[4] S. Hamada, On cohomology groups of dihedral groups (in Japanese), "Sūgaku" Vol. **16** (2) (1964), 106-107.

[5] H. Hasse, Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol, Nach. Ges. Wiss. **1** (1931), 64-69.

[6] F. Lolenz, Über eine Verallgemeierung des Hasseschen Normensatzes, Math. Z. **173** (1980), 203-210.

[7] H. Opolka, Zur Auflösung zahlentheoretischer Knoten, Math. Z. **173** (1980), 95-103.

Department of Mathematics
Miyagi University of Education
Sendai