S. Shirai
Nagoya Math. J.
Vol. 71 (1978), 87-90

A REMARK CONCERNING THE 2-ADIC NUMBER FIELD

SUSUMU SHIRAI

1. Introduction

Let Q_2 be the 2-adic number field, T/Q_2 be a finite unramified extension, ζ_ν be a primitive 2^ν-th root of unity, and let $K_\nu = T(\zeta_\nu)$. In a previous paper [1, Theorem 11], we stated the following theorem without its proof.

THEOREM A. *Let $R = T(\zeta_\nu + \zeta_\nu^{-1})$, and let σ be a generator of the cyclic Galois group $G(R/T)$. Assume $\nu \geqq 3$. If $N_{R/T}\varepsilon = 1$ for $\varepsilon \in U_R^{(4)}$, then*

$$\varepsilon \in (N_{K_\nu/R}K_\nu^\times)^{\sigma-1},$$

where $U_R^{(i)}$ denotes the i-th unit group of R.

The aim of the present paper is to prove this theorem, which is a detailed version of Hilbert's theorem 90 in the 2-adic number field.

2. Preliminaries

Let $\theta = \zeta_\nu + \zeta_\nu^{-1}$. Since $1 - \zeta_\nu$ is a prime element of K_ν,

$$N_{K_\nu/R}(1 - \zeta_\nu) = (1 - \zeta_\nu)(1 - \zeta_\nu^{-1}) = 2 - \theta$$

is a prime element of R. Set $\pi = 2 - \theta$ and denote by ν_π the normalized exponential valuation of R. The Galois group $G(K_\nu/T)$ is isomorphic to the group of prime residue classes mod 2^ν, and hence we can choose the generator σ of $G(R/T)$ such that

$$\theta^\sigma = (\zeta_\nu + \zeta_\nu^{-1})^\sigma = \zeta_\nu^5 + \zeta_\nu^{-5} = \theta^5 - 5\theta^3 + 5\theta,$$

without loss of generality. Then

$$\pi^\sigma = \pi^5 - 10\pi^4 + 35\pi^3 - 50\pi^2 + 25\pi. \tag{1}$$

LEMMA 1. *Notation being as above, if $\nu \geqq 3$, then*

Received June 10, 1977.

https://doi.org/10.1017/S0027763000021644 Published online by Cambridge University Press

$$\nu_\pi(\pi^\sigma - \pi) = 3 .$$

Proof. Immediate from (1).

LEMMA 2. *If* $\nu \geqq 3$, *then*

$$\nu_\pi((\pi^n)^{\sigma-1} - 1)\begin{cases} = 2 & \text{when } n \text{ is odd} , \\ \geqq 4 & \text{when } n \text{ is even} . \end{cases}$$

Proof. By Lemma 1, we have

$$\nu_\pi(\pi^{\sigma-1} - 1) = 2 ,$$

and hence we can write

$$\pi^{\sigma-1} = 1 + a\pi^2 , \qquad (a, \pi) = 1 .$$

Therefore, for $n \geqq 1$,

$$(\pi^n)^{\sigma-1} - 1 = \pi^2(na + n(n-1)/2\cdot a^2\pi^2 + \cdots) .$$

We have $\nu_\pi((\pi^n)^{\sigma-1} - 1) = 2$ if n is odd. Since $\nu_\pi(2) = 2^{\nu-2} \geqq 2$, we have $\nu_\pi((\pi^n)^{\sigma-1} - 1) \geqq 4$ if n is even. For $n \leqq -1$, according as n is odd or even, we obtain

$$(\pi^{-n})^{\sigma-1} \in U_R^{(2)} - U_R^{(3)} \quad \text{or} \quad \in U_R^{(4)} .$$

This completes the proof.

LEMMA 3. *If* $\nu \geqq 3$, *then*

$$\nu_\pi(\beta^{\sigma-1} - 1) \geqq 4 \qquad \text{for } \beta \in U_R^{(2)} .$$

Proof. We may write

$$\beta = 1 + a\pi^2 , \qquad a \in O_R, \text{ the ring of integers of } R.$$

Then

$$\beta^{\sigma-1} - 1 = (a^\sigma(\pi^\sigma)^2 - a\pi^2)/\beta .$$

Since R/T is totally ramified, $\{1, \pi, \cdots, \pi^{2^{\nu-2}-1}\}$ is an integral basis for R/T. Set

$$a \equiv a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 \qquad \text{mod } \pi^4,\ a_i \in O_T .$$

Then

$$a^\sigma \equiv a_0 + a_1\pi^\sigma + a_2(\pi^\sigma)^2 + a_3(\pi^\sigma)^3 \qquad \text{mod } \pi^4 .$$

By (1) and $\nu_\pi(50) = 2^{\nu-2} \geqq 2$, we have

https://doi.org/10.1017/S0027763000021644 Published online by Cambridge University Press

$$\pi^\sigma \equiv 35\pi^3 + 25\pi \qquad \bmod \pi^4 .$$

Hence

$$\begin{aligned} a^\sigma(\pi^\sigma)^2 - a\pi^2 &\equiv 624a_0\pi^2 + 15624a_1\pi^3 \\ &= 2^4\cdot 3\cdot 13a_0\pi^2 + 2^3\cdot 3^2\cdot 7\cdot 31a_1\pi^3 \\ &\equiv 0 \qquad \bmod \pi^4 . \end{aligned}$$

Next, let $[T:Q_2] = f$, and let ξ be a primitive $(2^f - 1)$st root of unity. It is well-known that $T = Q_2(\xi)$ and $\{1, \xi, \cdots, \xi^{f-1}\}$ is an integral basis for T/Q_2, and moreover $U_R^{(1)}/U_R^{(2)} \approx \bar{R} = \bar{T}$ is a module of type $\underbrace{(2, \cdots, 2)}_{f}$, where $\bar{R}, \bar{T}$ stand for the residue class fields of R and T, respectively. As a complete system of representatives for $U_R^{(1)}/U_R^{(2)}$, we can choose

$$\{\gamma = (1+\pi)^{n_0}(1+\xi\pi)^{n_1}\cdots(1+\xi^{f-1}\pi)^{n_{f-1}};\ n_i = 0 \text{ or } 1, i = 0, 1, \cdots, f-1\} .$$

LEMMA 4. *Notation being as above, if* $\nu \geqq 3$ *and* $\gamma \neq 1$, *then*

$$\nu_\pi(\gamma^{\sigma-1} - 1) = 3 .$$

Proof. Since

$$\gamma = (1 + n_0\pi)(1 + n_1\xi\pi)\cdots(1 + n_{f-1}\xi^{f-1}\pi) ,$$

we have

$$\begin{aligned} \gamma^\sigma - \gamma = (\pi^\sigma - \pi)&(n_0 + n_1\xi + \cdots + n_{f-1}\xi^{f-1}) \\ &+ ((\pi^\sigma)^2 - \pi^2)(\cdots\cdots) \\ &+ \cdots . \end{aligned}$$

From Lemma 1, we obtain

$$\nu_\pi(\pi^\sigma - \pi) = 3 , \qquad \nu_\pi((\pi^\sigma)^2 - \pi^2) \geqq 4 , \cdots .$$

Thus it suffices to show that

$$n_0 + n_1\xi + \cdots + n_{f-1}\xi^{f-1} \not\equiv 0 \qquad \bmod \pi .$$

Suppose $\equiv 0 \bmod \pi$. Then we have

$$n_0 + n_1\xi + \cdots + n_{f-1}\xi^{f-1} \equiv 0 \qquad \bmod \pi_T ,$$

π_T being a prime element of T. Since $\{\xi^i \bmod \pi_T ; i = 0, 1, \cdots, f-1\}$ is a basis of the residue class field extension $\bar{T}/\bar{Q}_2$, we conclude all

$n_i = 0$, a contradiction.

3. Proof of Theorem A

We first note that

$$\pi = 2 - \theta = N_{K_\nu/R}(1 - \zeta_\nu) \in N_{K_\nu/R}K_\nu^\times , \quad \xi \in N_{K_\nu/R}K_\nu^\times , \quad U_R^{(2)} \subset N_{K_\nu/R}K_\nu^\times ,$$

in which the second follows from that the order $2^f - 1$ of ξ is prime to $[R^\times : N_{K_\nu/R}K_\nu^\times] = 2$ and the third from that the π-exponent of the conductor of K_ν/R is two. Now, let ε be an element in $U_R^{(4)}$ such that $N_{R/T}\varepsilon = 1$. Then we can write, by Hilbert's theorem 90,

$$\varepsilon = \alpha^{\sigma-1} , \qquad \alpha \in R^\times .$$

Since $R^\times = \langle\pi\rangle \times \langle\xi\rangle \times U_R^{(1)}$ (a direct product) and $U_R^{(1)} \supset U_R^{(2)}$, we may set

$$\alpha = \pi^n \cdot \xi^m \cdot \gamma \cdot \beta , \qquad \beta \in U_R^{(2)} ,$$

here γ is as in Lemma 4. By virtue of the above remark, it completes the proof that we obtain $\gamma = 1$. Assume $\gamma \neq 1$. Then we have

$$\varepsilon = (\pi^n)^{\sigma-1} \cdot \gamma^{\sigma-1} \cdot \beta^{\sigma-1} ,$$

in which Lemmas 3, 4 give $\beta^{\sigma-1} \in U_R^{(4)}$ and $\gamma^{\sigma-1} \in U_R^{(3)} - U_R^{(4)}$, respectively. If n is even, then we have, by Lemma 2, $(\pi^n)^{\sigma-1} \in U_R^{(4)}$, a contradiction. If n is odd, then we have, by Lemma 2, $(\pi^n)^{\sigma-1} \in U_R^{(2)} - U_R^{(3)}$ from which follows $(\pi^n)^{\sigma-1} \cdot \gamma^{\sigma-1} \in U_R^{(2)} - U_R^{(3)}$, a contradiction, and the proof is complete.

REFERENCE

[1] S. Shirai, On the central class field mod $\mathfrak{m}$ of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.

Toyama Medical and Pharmaceutical University