

T. Hakobyan

**ON THE REDUCED GROUP OF PRINCIPAL UNITS IN
CYCLIC EXTENSIONS OF LOCAL FIELDS**

ABSTRACT. In this paper, the structure of reduced group of main units of cyclic extensions of local fields as a Galois module is studied by examining the Jordan canonical form of the generating automorphism of Galois group.

§1. INTRODUCTION

Suppose p is an odd prime number, k is a finite extension of \mathbb{Q}_p of degree n , K/k is a cyclic extension of degree p with Galois group $G = \langle \sigma \rangle$. If $R = \mathbb{F}_p[G]$ denotes the group ring over G , then the multiplicatively written \mathbb{F}_p -vector space $V = K^*/K^{*p}$ can be considered as a multiplicatively written R -module, the multiplication by scalars from R being given in a natural way

$$[x]_{g \in G}^{\sum \alpha_g g} = \left[\prod_{g \in G} (x^g)^{\alpha_g} \right],$$

where x^g stands for $g(x)$ for all $x \in K^*$ and $g \in G$. Therefore, $(\sigma - \text{Id})^p \equiv \sigma^p - \text{Id} = 0 \pmod{p}$, showing that $\sigma - \text{Id}$ is nilpotent. Henceforth we will write $\sigma - 1$ instead of $\sigma - \text{Id}$. We notice that determine the structure of V as an R -module means to analyse the Jordan canonical form of σ , or equivalently the Jordan canonical form of $\sigma - 1$. Suppose $\Gamma = N(K^*)$ where $N = N_{K/k}$ is the norm map of the extension K/k and ζ_p denotes a primitive p -th root of unity. In [1] Faddeev proved that

$$(g_p, g_{p-1}, \dots, g_1) = \begin{cases} (n, 0, \dots, 0, 1), & \text{if } \zeta_p \notin K, \\ (n, 0, \dots, 1, 0), & \text{if } \zeta_p \in K, \zeta_p \notin \Gamma, \\ (n, 0, \dots, 0, 2), & \text{if } \zeta_p \in \Gamma, \end{cases}$$

where for each i , g_i denotes the number of i -dimensional Jordan blocks in Jordan canonical form of $\sigma - 1$. Moreover, he managed to prove that in the

Key words and phrases: local field, Galois group, group of principal units, totally ramified extension, unramified extension, norm group of an extension, Jordan canonical form.

irregular case, where K contains a primitive p -th root of unity ζ_p , the vector space V possesses an almost normal basis of the form $\{\sigma^i(A_j), a, \sigma(a) | 1 \leq i \leq p, 1 \leq j \leq n\}$ or $\{\sigma^i(A_j), a, b | 1 \leq i \leq p, 1 \leq j \leq n\}$, depending on whether $\zeta_p \notin \Gamma$ or $\zeta_p \in \Gamma$. In this paper, we similarly consider the R -module $V' = U'_1/U_1{}^p$ and analyse the Jordan canonical form of $\sigma - 1$ on V' , where U'_1 denotes the group of principal units of K . In the same way as we defined the numbers g_i for V , we define the numbers l_i for V' , i.e. for each i we denote by l_i the number of i -dimensional Jordan blocks in Jordan canonical form of $\sigma - 1$ on V' .

We start with the following proposition.

Proposition 1. $(g_p, g_{p-1}, \dots, g_1) \succcurlyeq (l_p, l_{p-1}, \dots, l_1)$ i.e. $\sum_{j \geq t} g_j \geq \sum_{j \geq t} l_j$ for all $t \geq 1$.

Proof. For $t \geq 1$ we define $G_t = \{x \in K^* : x^{(\sigma-1)^t} \in K^{*p}\}$ and $W_t = \{x \in U'_1 : x^{(\sigma-1)^t} \in U_1{}^p\}$. Observe that $W_t = G_t \cap U'_1$ for all $t \geq 1$. Indeed, if $x \in U'_1$ and $x^{(\sigma-1)^t} = \alpha^p$, then $\alpha^p \in U_1{}^p$, implying that $\alpha \in U'_1$. Therefore, the inclusions $W_t \hookrightarrow G_t$ induce monomorphisms $W_t/W_{t-1} \rightarrow G_t/G_{t-1}$, showing that

$$\dim_{\mathbb{F}_p}(W_t/W_{t-1}) \leq \dim_{\mathbb{F}_p}(G_t/G_{t-1}) \text{ for all } t \geq 1.$$

It remains only to recall that

$$\dim_{\mathbb{F}_p}(W_t/W_{t-1}) = \sum_{j \geq t} l_j \text{ and } \dim_{\mathbb{F}_p}(G_t/G_{t-1}) = \sum_{j \geq t} g_j. \quad \square$$

In the sequel we are going to investigate the numbers l_t , depending on the extension K/k . Recall that the total number of Jordan blocks is equal to $e_1 = \dim(\ker(\sigma - 1))$, while the number of p -dimensional blocks is equal to $l_p = \dim(\text{Im}(\sigma - 1)^{p-1})$. On the other hand, Teichmüller's group decompositions

$$k^* = \langle \pi \rangle \times R_k \times U_1 \text{ and } K^* = \langle \Pi \rangle \times R_K \times U'_1,$$

where π and Π are uniformizers, R_k and R_K are the corresponding Teichmüller groups, U_1 and U'_1 are groups of principal units, they all are well-known and will be used throughout the paper. For the proof we refer the reader to [2], chapter 3, paragraph 5 and to [3], chapter 2, paragraph 2. Henceforth, according to this decomposition, for any $\alpha \in K^*$ we will write $\alpha = \Pi^{v_{\Pi}(\alpha)} \eta_{\alpha} u_{\alpha}$, for uniquely determined elements $\eta_{\alpha} \in R_K, u_{\alpha} \in U'_1$. For convenience we denote $W = W_1$.

§2. CALCULATION OF W .

Notice that if $\zeta_p \in K$, then $\zeta_p = \alpha_0^{\sigma-1}$ for some $\alpha_0 \in K^*$. Furthermore, if $\zeta_p = N(\alpha_1) \in \Gamma$ then $N(\alpha_1^p) = 1$, showing that $\alpha_1^p = \beta_0^{\sigma-1}$, for some $\beta_0 \in K^*$. We first calculate G_1 , as

$$W = W_1 = G_1 \cap U_1'.$$

The following lemma is due to Faddeev.

Lemma 1.

$$G_1 = \begin{cases} k^* K^{*p}, & \zeta_p \notin \Gamma \\ \langle \beta_0 \rangle k^* K^{*p}, & \zeta_p \in \Gamma. \end{cases}$$

Proof. First suppose $\zeta_p \notin \Gamma$ and $x \in G_1$, which means that $x^{\sigma-1} = \alpha^p$ for some $\alpha \in K^*$. Taking norms, we get $N^p(\alpha) = 1$, which gives $N(\alpha) = 1$ and therefore $\alpha = y^{\sigma-1}$ for some $y \in K^*$, showing that $x^{\sigma-1} = (y^p)^{\sigma-1}$ and consequently $x \in k^* K^{*p}$. The opposite inclusion is clear. On the other hand, if $\zeta_p \in \Gamma$, then from $N^p(\alpha) = 1$ we infer that $N(\alpha) = \zeta_p^t$ for some t . Therefore $N(\alpha \alpha_1^{-t}) = 1$, which implies that $\alpha = \alpha_1^t y^{\sigma-1}$ for some $y \in K^*$. Hence

$$\begin{aligned} x^{\sigma-1} &= \alpha^p = (\alpha_1^t y^{\sigma-1})^p = (\alpha_1^p)^t (y^p)^{\sigma-1} \\ &= (\beta_0^{\sigma-1})^t (y^p)^{\sigma-1} = (\beta_0^t y^p)^{\sigma-1}, \end{aligned}$$

which yields $x \in \langle \beta_0 \rangle k^* K^{*p}$. As $\beta_0^{\sigma-1} = \alpha_1^p \in K^{*p}$, we deduce that $\beta_0 \in G_1$, and thereby the opposite inclusion $\langle \beta_0 \rangle k^* K^{*p} \subset G_1$ is also proved. \square

Choose any uniformizers $\pi \in k$ and $\Pi \in K$, and define

$$\lambda_{\pi, \Pi} = \begin{cases} 1, & K/k \text{ is unramified} \\ u_{\pi \Pi^{-p}}, & K/k \text{ is totally ramified.} \end{cases}$$

Observe that the class

$$\lambda_{\pi, \Pi} \pmod{U_1 U_1'^p}$$

is independent of the choice of uniformizers π and Π . In other words, if we take uniformizers $\pi_1 \in k$ and $\Pi_1 \in K$, then

$$\lambda_{\pi_1, \Pi_1} \in \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p.$$

Indeed, if K/k is unramified then

$$\lambda_{\pi_1, \Pi_1} = \lambda_{\pi, \Pi} = 1$$

by definition. On the other hand, if K/k is totally ramified, then $\pi\Pi^{-p}$ and $\pi_1\Pi_1^{-p}$ differ by a factor of the form $\mu\mu_1^p$ for some units $\mu \in k$ and $\mu_1 \in K$. Therefore

$$\lambda_{\pi_1, \Pi_1} \lambda_{\pi, \Pi}^{-1} = u_\mu \mu_1^p = u_\mu u_{\mu_1}^p \in U_1 U_1'^p,$$

as claimed. If $\zeta_p \in \Gamma$, then as we have shown, $\beta_0^{\sigma-1} = \alpha_1^p$. Suppose $\beta_0 = \Pi^l u_{\beta_0} \eta_{\beta_0}$, where l is an integer, $u_{\beta_0} \in U_1'$ and $\eta_{\beta_0} \in R_K$. Dividing by a convenient power of π , we may assume that $0 \leq l < p$. If $l = 0$, then

$$u_{\alpha_1}^p \eta_{\alpha_1}^p = \alpha_1^p = \beta_0^{\sigma-1} = u_{\beta_0}^{\sigma-1} \eta_{\beta_0}^{\sigma-1},$$

implying that $u_{\beta_0}^{\sigma-1} = u_{\alpha_1}^p$, by the uniqueness of Teichmüller's decomposition. Furthermore, assume that

$$s = \begin{cases} 1, & l = 0 \\ 0, & l \neq 0. \end{cases}$$

We next calculate W in the following lemma.

Lemma 2.

$$W = \begin{cases} \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p, & \zeta_p \notin \Gamma \\ \langle \lambda_{\pi, \Pi} \rangle \langle u_{\beta_0}^s \rangle U_1 U_1'^p, & \zeta_p \in \Gamma. \end{cases}$$

Moreover, $u_{\beta_0} \notin \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p$.

Proof. We first assume that $\zeta_p \notin \Gamma$. In this case

$$W = G_1 \cap U_1' = k^* K^{*p} \cap U_1',$$

by Lemma 1. Suppose $x = ay^p \in U_1'$, for some $a \in k^*$ and $y \in K^*$. If K/k is unramified, we may assume $\Pi = \pi$ and write $a = \pi^m b$, $y = \pi^r z$ for some integers m, r and units $b \in k, z \in K$. Therefore $m = -rp$, as $x \in U_1'$, implying that $x = bz^p$. Hence

$$x = u_{bz^p} \in U_1 U_1'^p.$$

Suppose K/k is totally ramified and write $a = \pi^m b, y = \Pi^r z$ for some integers m, r and units $b \in k, z \in K$. The condition $v_\Pi(x) = 0$ implies that $m = -r$, but this time we get $x = (\pi\Pi^{-p})^m bz^p$, which yields

$$x = \lambda_{\pi, \Pi}^m u_b u_z^p \in \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p.$$

On the other hand

$$\lambda_{\pi, \Pi}^{\sigma-1} = (\Pi^{1-\sigma})^p \in U_1'^p,$$

as $\Pi^{1-\sigma} \in U'_1$ for totally ramified extensions. Therefore $\lambda_{\pi, \Pi} \in W$, which together with the fact that $U_1 U_1'^p \in W$ proves the opposite inclusion $\langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p \subset G_1$. If $\zeta_p \in \Gamma$, then by Lemma 1, $G_1 = \langle \beta_0 \rangle k^* K^{*p}$ and therefore

$$W = \langle \beta_0 \rangle k^* K^{*p} \cap U'_1,$$

and by the same method we applied in case $\zeta_p \notin \Gamma$, one can show that both in unramified and totally ramified cases the inclusions

$$\langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p \subset W \subset \langle u_{\beta_0} \rangle \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p$$

hold. Suppose $x = a\beta_0^t y^p \in W$ for some $a \in k^*$ and $y \in K^*$, then

$$tl = v_{\Pi}(\beta_0^t) = v_{\Pi}(xa^{-1}y^{-p})p.$$

If $l \neq 0$, then $p \mid t$, hence $G_1 \cap U'_1 \subset k^* K^{*p}$ and

$$W = G_1 \cap U'_1 \subset k^* K^{*p} \cap U'_1 = \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p,$$

as we have already proved. On the other hand, if $l = 0$, then according to the paragraph before Lemma 2, $u_{\beta_0}^{\sigma-1} = u_{\alpha_1}^p$, implying that $u_{\beta_0} \in W$ and

$$W = \langle u_{\beta_0} \rangle \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p.$$

Let us prove that $u_{\beta_0} \notin \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p$.

Suppose to the contrary that $u_{\beta_0} = \lambda_{\pi, \Pi}^m a y^p$, for some $a \in k^*$ and $y \in K^*$, then

$$u_{\alpha_1}^p = u_{\beta_0}^{\sigma-1} = \begin{cases} (y^{\sigma-1})^p, & K/k \text{ is unramified} \\ ((\Pi^{-m}y)^{\sigma-1})^p, & K/k \text{ is totally ramified,} \end{cases}$$

which means that $u_{\alpha_1} = \zeta_p^{\nu} z^{\sigma-1}$, and therefore $N(u_{\alpha_1}) = 1$. So

$$\zeta_p = N(\alpha_1) = N(u_{\alpha_1})N(\eta_{\alpha_1}) = N(\eta_{\alpha_1}) \in R_K,$$

which is not true. \square

§3. CALCULATION OF e_1 AND l_p .

We define $\Gamma_0 = N_{K/k}(U'_1) \subset U_1$. Recall that if $\zeta_p \in K$, then $\zeta_p = \alpha_0^{\sigma-1}$ for some $\alpha_0 \in K^*$ and dividing by a power of π , we may assume that $0 \leq v_{\Pi}(\alpha_0) < p$. For simplicity we define

$$\delta = \begin{cases} 0, & v_{\Pi}(\alpha_0) \neq 0 \\ 1, & v_{\Pi}(\alpha_0) = 0. \end{cases}$$

Lemma 3.

$$U_1 \cap U_1'^p = \Gamma_0 \cap U_1'^p = \begin{cases} U_1^p, & \zeta_p \notin K \\ U_1^p \langle u_{\alpha_0}^{p\delta} \rangle, & \zeta_p \in K. \end{cases}$$

Proof. Suppose $x = y^p$, for some $x \in U_1$, and $y \in U_1'$, which shows that $(\sigma(y))^p = y^p$. If $\zeta_p \notin K$, then $\sigma(y) = y$, hence $y \in k \cap U_1' = U_1$ and consequently $x = y^p \in U_1^p$, showing that $U_1 \cap U_1'^p = U_1^p$. On the other hand, if $\zeta_p \in K$, then $\sigma(y) = \zeta_p^t y$ for some t , which implies that $y = a\alpha_0^t$, for some $a \in k$. If $\delta = 0$ i.e. $v_\Pi(\alpha_0) \neq 0$, then K/k is totally ramified, hence

$$tv_\Pi(\alpha_0) = -v_\Pi(a)p,$$

showing that

$$p|t, \sigma(y) = y, \text{ and therefore } U_1 \cap U_1'^p = U_1^p,$$

as in case $\zeta_p \notin K$. If $\delta = 1$, i.e. $v_\Pi(\alpha_0) = 0$, then $\alpha_0 = \eta_{\alpha_0} u_{\alpha_0}$, where $\eta_{\alpha_0} \in R$ and $u_{\alpha_0} \in U_1'$. As we have shown before, $y = a\alpha_0^t$, for some $a \in k$, and therefore

$$y = u_{a\alpha_0^t} = u_a u_{\alpha_0}^t,$$

which yields

$$x = y^p = u_{\alpha_0}^{pt} u_a^p \in \langle u_{\alpha_0}^p \rangle U_1^p,$$

as claimed. On the other hand, the condition $\sigma(\alpha_0) = \zeta_p \alpha_0$ implies that $\sigma(u_{\alpha_0}) = \zeta_p u_{\alpha_0}$, showing that $u_{\alpha_0}^p \in U_1 \cap U_1'^p$. Observing that $U_1^p \subset \Gamma_0 \cap U_1'^p \subset U_1 \cap U_1'^p$ and that $u_{\alpha_0}^p = N(u_{\alpha_0})$ (when $v_\Pi(\alpha_0) = 0$), we infer that in both cases considered above, the equality $\Gamma_0 \cap U_1'^p = U_1 \cap U_1'^p$ holds. The lemma is proved. \square

Lemma 4. *Suppose K/k is a totally ramified extension. If $\zeta_p \notin K$, then $\lambda_{\pi, \Pi} \notin U_1 U_1'^p$. Otherwise, the following three conditions are equivalent.*

- (1) $\lambda_{\pi, \Pi} \in U_1 U_1'^p$.
- (2) There exist uniformizers $\pi_0 \in k$ and $\Pi_0 \in K$ such that $\pi_0 = \Pi_0^p$.
- (3) $v_\Pi(\alpha_0) \neq 0$.

Proof. We first assume that $\zeta_p \notin K$. Suppose to the contrary that $\lambda_{\pi, \Pi} = ay^p$ for some $a \in U_1$ and $y \in U_1'$. Then

$$(\Pi^{1-\sigma})^p = \lambda_{\pi, \Pi}^{\sigma-1} = (y^{\sigma-1})^p,$$

implying that $\Pi^{1-\sigma} = y^{\sigma-1}$, or equivalently, that $\Pi y \in k$, which is a contradiction, as $v_\Pi(\Pi y) = 1$. Suppose $\zeta_p \in K$. In order to prove the

lemma, it is enough to prove the following implications.

(2) \Rightarrow (1) If such uniformizers π_0 and Π_0 do exist, then $\lambda_{\pi_0, \Pi_0} = 1 \in U_1 U_1'^p$.

It remains to recall that the condition $\lambda_{\pi, \Pi} \in U_1 U_1'^p$ is independent of the choice of uniformizers π and Π .

(1) \Rightarrow (2) If $\lambda_{\pi, \Pi} = ay^p$ for some uniformizers π, Π and elements $a \in U_1$, $y \in U_1'$, then

$$\pi \Pi^{-p} = ay^p \eta_{\pi \Pi^{-p}} = ay^p \eta^p,$$

for some $\eta \in R_K$, as the order of the cyclic group R_K is $q-1$, which is coprime to p and therefore each element from R_K is a p -th power. If we denote $\pi_0 = \pi a^{-1}$ and $\Pi_0 = \Pi y \eta$, then we get $\pi_0 = \Pi_0^p$, as claimed.

(2) \Leftrightarrow (3) If $\pi_0 = \Pi_0^p$, then $\Pi_0^{\sigma^{-1}} = \zeta_p^t$, for some $0 < t < p$. Hence $\zeta_p = (\Pi_0^t)^{\sigma^{-1}}$, where $0 < l < p$ is the inverse of t modulo p . Therefore $v_{\Pi}(\alpha_0) = l$, as $0 \leq v_{\Pi}(\alpha_0) < p$, showing that $v_{\Pi}(\alpha_0) \neq 0$.

Recall that if $\zeta_p \in k$, then any cyclic extension of k of order p has the form $K = k(\sqrt[p]{a})$ for some $a \in k^*$. Moreover, a can be chosen either as a uniformizer, or a main unit.

Suppose there are no uniformizers π_0 and Π_0 , such that $\pi_0 = \Pi_0^p$. Then we can choose $a \in U_1$ and conclude that $\beta = \sqrt[p]{a} \in U_1'$. Therefore $\zeta_p = (\beta^l)^{\sigma^{-1}}$ for some $0 < l < p$, showing that $v_{\Pi}(\alpha_0) = 0$, as $v_{\Pi}(\beta^l) = 0$. \square

To prove the next lemma we recall that if k is any finite extension of \mathbb{Q}_p with group of main units U_1 , then

$$\dim_{\mathbb{F}_p} U_1/U_1^p = \begin{cases} [k : \mathbb{Q}_p], & \zeta_p \notin K \\ [k : \mathbb{Q}_p] + 1, & \zeta_p \in K. \end{cases}$$

For the proof we refer the reader to [4], chapter 15, paragraph 5.

Lemma 5.

$$e_1 = \begin{cases} n, & \zeta_p \notin K, K/k \text{ is unramified} \\ n+1, & \zeta_p \in K, K/k \text{ is unramified} \\ n+1, & \zeta_p \notin \Gamma, K/k \text{ is totally ramified} \\ n+1+s, & \zeta_p \in \Gamma, K/k \text{ is totally ramified.} \end{cases}$$

Proof. We first notice that

$$e_1 = \dim_{\mathbb{F}_p} (W/U_1^p) = \dim_{\mathbb{F}_p} (W/U_1 U_1'^p) + \dim_{\mathbb{F}_p} (U_1 U_1'^p/U_1^p).$$

It will be convenient to denote

$$e_1' = \dim_{\mathbb{F}_p} (W/U_1 U_1'^p) \quad \text{and} \quad e_1'' = \dim_{\mathbb{F}_p} (U_1 U_1'^p/U_1^p).$$

If $\zeta_p \notin \Gamma$ then by Lemma 2, $W = \langle \lambda_{\pi, \Pi} \rangle U_1 U_1'^p$ and together with Lemma 4,

$$e'_1 = \begin{cases} 0, & K/k \text{ is unramified} \\ 1, & \zeta_p \notin K, K/k \text{ is totally ramified} \\ \delta, & \zeta_p \in K, K/k \text{ is totally ramified.} \end{cases}$$

If $\zeta_p \in \Gamma$ then again by Lemma 2, $W = \langle \lambda_{\pi, \Pi} \rangle \langle u_{\beta_0}^s \rangle U_1 U_1'^p$ and again together with Lemma 4 we obtain

$$e'_1 = \begin{cases} 1, & K/k \text{ is unramified} \\ \delta + s, & K/k \text{ is totally ramified.} \end{cases}$$

Recall that for unramified extensions K/k , $\zeta_p \in \Gamma$ if and only if $\zeta_p \in K$. Therefore, combining cases $\zeta_p \notin \Gamma$ and $\zeta_p \in \Gamma$, we get

$$e'_1 = \begin{cases} 0, & \zeta_p \notin K, K/k \text{ is unramified} \\ 1, & \zeta_p \in K, K/k \text{ is unramified} \\ 1, & \zeta_p \notin K, K/k \text{ is totally ramified} \\ \delta, & \zeta_p \in K \setminus \Gamma, K/k \text{ is totally ramified} \\ \delta + s, & \zeta_p \in \Gamma, K/k \text{ is totally ramified.} \end{cases}$$

On the other hand, Lemma 3 together with the paragraph before Lemma 5 implies

$$e''_1 = \begin{cases} n, & \zeta_p \notin K \\ n + 1 - \delta, & \zeta_p \in K. \end{cases}$$

To finish the proof of Lemma it remains to recall that

$$e_1 = e'_1 + e''_1. \quad \square$$

Finally, we calculate l_p in the following lemma.

Lemma 6.

$$l_p = \begin{cases} n, & K/k \text{ is unramified} \\ n - 1, & \zeta_p \notin K, K/k \text{ is totally ramified} \\ n - \delta, & \zeta_p \in K, K/k \text{ is totally ramified.} \end{cases}$$

Proof. Observe that

$$l_p = \dim_{\mathbb{F}_p}(\text{Im}(\sigma - 1)^{p-1}) = \dim_{\mathbb{F}_p}(\Gamma_0 U_1'^p / U_1'^p) = \dim_{\mathbb{F}_p}(\Gamma_0 / \Gamma_0 \cap U_1'^p).$$

If K/k is unramified, then $\Gamma_0 = U_1$ and by Lemma 3

$$l_p = \begin{cases} n, & \zeta_p \notin K, \\ n+1-\delta, & \zeta_p \in K, \end{cases}$$

which gives $l_p = n$, since $\delta = 1$ in this case. On the other hand, if K/k is totally ramified then $[U_1 : \Gamma_0] = p$, which together with Lemma 3 yields

$$l_p = \begin{cases} n-1, & \zeta_p \notin K, \\ n-\delta, & \zeta_p \in K, \end{cases}$$

and we are done. \square

§4. CALCULATION OF $(l_p, l_{p-1}, \dots, l_1)$.

1) If $\zeta_p \notin K$ then we know that $(g_p, g_{p-1}, \dots, g_1) = (n, \dots, 1)$. Lemmas 5 and 6 imply that if K/k is unramified, then $e_1 = l_p = n$, while if K/k is totally ramified then $e_1 = n+1$ and $l_p = n-1$. Recall that $\dim_{\mathbb{F}_p}(V') = np$, which shows that in unramified case $(l_p, l_{p-1}, \dots, l_1) = (n, 0, \dots, 0)$, while in totally ramified case $(l_p, l_{p-1}, \dots, l_1) = (n-1, ..1, ..1, ..)$, where 1's are at positions a and b with $a+b = p$. Proposition 1 shows that

$$(n, 0, \dots, 1) = (g_p, g_{p-1}, \dots, g_1) \succ (l_p, l_{p-1}, \dots, l_1) = (n-1, ..1, ..1, ..),$$

which means that if $a < b$ then $a = 1$ and therefore $b = p-1$, showing that $(l_p, l_{p-1}, \dots, l_1) = (n-1, 1, \dots, 1)$.

2) If $\zeta_p \in K \setminus \Gamma$, then K/k is a totally ramified extension and therefore $e_1 = n+1, l_p = n-\delta$, by Lemma 5 and Lemma 6. On the other hand, $(g_p, g_{p-1}, \dots, g_1) = (n, \dots, 1, 0)$ and $\dim_{\mathbb{F}_p}(V') = np+1$. Hence, if $\delta = 0$, then $(l_p, l_{p-1}, \dots, l_1) = (n, \dots, 1)$, while if $\delta = 1$, then $(l_p, l_{p-1}, \dots, l_1) = (n-1, ..1, .., 1, ..)$, where 1's are at positions a and b with $a \leq b, a+b = p+1$, which shows that $a > 1$ as $b < p$. Using Proposition 1 we obtain

$$(n, \dots, 1, 0) \succ (n-1, ..1, ..1, ..)$$

and therefore $a = 2, b = p-1$, implying that

$$(l_p, l_{p-1}, \dots, l_1) = (n-1, 1, \dots, 1, 0).$$

3) Consider the last case $\zeta_p \in \Gamma$. Then one has $(g_p, g_{p-1}, \dots, g_1) = (n, \dots, 2)$ and $\dim_{\mathbb{F}_p}(V') = np+1$. Lemma 5 and Lemma 6 again imply that if K/k is unramified, then $e_1 = n+1, l_p = n$, while if K/k is totally ramified, then $e_1 = n+1+s$ and $l_p = n-\delta$. Hence, if K/k is unramified, then $(l_p, l_{p-1}, \dots, l_1) = (n, \dots, 1)$. Suppose K/k is totally ramified. If

Table 1

	The extension K/k	R -module V'
1.	$\zeta_p \notin k$, unramified	R^n
2.	$\zeta_p \notin k$, totally ramified	$R^{n-1} \oplus R/(\sigma-1)^{p-1} \oplus R/(\sigma-1)$
3.	$K = k(\sqrt[p]{u})$, $\zeta_p \in k \setminus \Gamma$	$R^n \oplus R/(\sigma-1)$
4.	$K = k(\sqrt[p]{\pi})$, $\zeta_p \in k \setminus \Gamma$	$R^{n-1} \oplus R/(\sigma-1)^{p-1} \oplus R/(\sigma-1)^2$
5.	$\zeta_p \in \Gamma$, unramified	$R^n \oplus R/(\sigma-1)$
6.	$K = k(\sqrt[p]{u})$, $\zeta_p \in \Gamma$, totally ramified	$R^n \oplus R/(\sigma-1)$
7.	$K = k(\sqrt[p]{\pi})$, $\zeta_p \in \Gamma$, totally ramified	$R^{n-1} \oplus R/(\sigma-1)^{p-1} \oplus R/(\sigma-1) \oplus R/(\sigma-1)$

$\delta = 0$, then again $(l_p, l_{p-1}, \dots, l_1) = (n, \dots, 1)$, as $l_p = n - \delta = n$, which simultaneously shows that $s = 0$. Assume now that $\delta = 1$. If $s = 0$, then by Proposition 1, we would have a relation

$$(n, \dots, 2) \succ (n-1, \dots, 1, \dots)$$

with two 1's at places a and b with $a \leq b$, $a + b = p + 1$, implying that $a = 1$ and $b = p$, which is a contradiction, as $b < p$. Therefore, $s = 1$ and we get a relation

$$(n, \dots, 2) \succ (n-1, \dots, 1, \dots, 1, \dots),$$

where 1's are at some positions a, b, c with $a \leq b \leq c$, $a + b + c = p + 1$, which yields $a = b = 1$ and $c = p - 1$, showing that $(l_p, l_{p-1}, \dots, l_1) = (n-1, 1, \dots, 2)$. \square

Thus, we can combine everything proven in Table 1. Here u denotes a principal unit in k^* . Observe that in all cases any \mathbb{F}_p -basis of V' modulo $\ker((\sigma-1)^{p-1})$ can serve as an R -basis of the corresponding free part. Moreover, it is not hard to show that in cases 3 and 6 the additional generator α of R -module V' can be chosen as any element from the set $U_1 \setminus \Gamma_0$, while in case 5, one may choose $\alpha = u_{\beta_0}$ (see section 2).

REFERENCES

1. D. K. Faddeev, *On the structure of the reduced multiplicative group of a cyclic extension of a local field*, — Izv. Akad. Nauk SSSR Ser. Mat., **24:2** (1960), 145–152.

2. J. Neukirch, *Algebraic number theory*, Springer (1999).
3. K. Iwasawa, *Local class field theory*, Oxford University Press (1986).
4. H. Hasse, *Number theory*, Springer (1980).

St. Petersburg
State University,
Universitetskaya nab. 7/9,
199034, St. Petersburg, Russia
E-mail: tigran19931026@gmail.com

Поступило 18 апреля 2017 г.