ON GROUPS OF PRINCIPAL UNITS OF \(p\)-EXTENSIONS OF A LOCAL FIELD

MATHEMATICS

1967

SovietRxiv

Abstract

Full Text

UDC 519.49

MATHEMATICS

Z. I. BOREVICH

ON GROUPS OF PRINCIPAL UNITS OF p-EXTENSIONS OF A LOCAL FIELD

(Presented by Academician Yu. V. Linnik on 14 V 1966)

Let k be a finite extension of the field of p-adic numbers of degree n (a local field), and let K/k be a normal p-extension with Galois p-group G of order m. The group of principal units E of the field K is a multiplicatively written module over the group ring $O = Z[G]$ of the group G with coefficients in the ring of p-adic integers Z. It is of known interest to determine the structure of the O-module E.

We shall call two finitely generated O-modules similar if they differ from each other by a direct O-summand that is a free O-module. Since the Krull-Schmidt theorem is valid for finitely generated O-modules (see [1], § 8), in studying the O-module E we may consider any O-module similar to it.

A prime element Π of the field K can be chosen so that $\sigma(\Pi)/\Pi = \theta_\sigma \in E$ for all $\sigma \in G$. We pass in the group $\{\Pi\} \times E$, invariant with respect to the operators from G, to additive notation and embed it in an O-module A, allowing as coefficients at Π arbitrary integral p-adic numbers (and not only rational integers). The structure of the O-module A may, in a certain sense, be considered known; see [2,3].

By I we denote the submodule of the ring O generated by the elements $\sigma - 1$ ($\sigma \in G$).

Theorem 1. *The O-module E is similar to a certain Z-splitting extension of the O-module A by means of I.*

Indeed, for the direct sum $X = E \oplus Ox$ define O-homomorphisms $i : I \to X$ and $j : X \to A$, putting

$$i(\sigma - 1) = -\theta_\sigma + (\sigma - 1)x; \qquad j(\varepsilon) = \varepsilon \ (\varepsilon \in E), \qquad j(x) = \Pi.$$

Then we shall have an exact sequence

$$0 \to I \xrightarrow{i} X \xrightarrow{j} A \to 0. \tag{1}$$

Let A and C be arbitrary O-modules and let $0 \to C \xrightarrow{i} X \xrightarrow{j} A \to 0$ be some Z-splitting extension. Define a Z-homomorphism $l : A \to X$ so that $jl = 1$. For $\sigma \in G$ and $a \in A$ put $f(\sigma)(a) = i^{-1}(\sigma l(\sigma^{-1}a) - l(a))$. This defines a 1-cocycle f on G with values in the group $\mathrm{Hom}_Z(A, C)$. It is easily verified that the correspondence $X \to f$ defines a natural isomorphism of the group $\mathrm{Ext}^*(A, C)$ of classes of equivalent Z-splitting extensions of the O-module A by means of C onto the group $H^1(G, \mathrm{Hom}_Z(A, C))$.

In view of Theorem 1, to determine the O-module E one must find, in the group $\mathrm{Ext}^*(A, I)$, which we identify with $H^1(G, \mathrm{Hom}_Z(A, I))$, the element corresponding to the extension (1).

Let Q be the periodic part of the O-module A; $A_0 = A^G$ the subgroup of G-invariant elements in A; Δ the group of norms $N(A)$ of elements of A, and D the set of those elements of A some multiple of which falls into A_0. For a finite p-group $\mathfrak{A}$ we denote the group $\mathrm{Hom}(\mathfrak{A}, R^+/Z)$, where R^+ is the additive group of all p-adic numbers, by $\mathrm{Char}\,\mathfrak{A}$, and its

elements characters of the group $\mathfrak{A}$. Let v be the valuation of the field K, considered as an element of the group $\mathrm{Hom}(A, Z)$.

Theorem 2. There is a natural isomorphism

$$\mathrm{Ext}^*(A, I) \approx \mathrm{Char}(D/(\Delta + Q)).$$

Under this isomorphism the extension (1) corresponds to the character χ for which

$$\chi(u \bmod (\Delta + Q)) = \frac{v(u)}{m} \bmod Z \qquad (u \in D).$$

Denote by f the degree of inertia of the extension K/k.

Theorem 3. There is an exact sequence

$$0 \to \mathrm{Char}\, H^1(G, Q) \xrightarrow{\lambda} \mathrm{Ext}^*(A, I) \xrightarrow{\mu} \mathrm{Char}\, G \tag{2}$$

with natural homomorphisms λ and μ. If an element $c \in \mathrm{Ext}^*(A, I)$ corresponds to the extension (1), then the kernel of the character $\mu(c) \in \mathrm{Char}\, G$ coincides with the inertia subgroup G_0 of the extension K/k, and

$$\mu(c)(\sigma) = \frac{1}{f} \bmod Z$$

for an automorphism $\sigma \in G$ inducing on the inertia subfield the Frobenius automorphism. Furthermore, $\mu(c)$ coincides with the composite homomorphism of the canonical sequence

$$G \to H^0(G, A) \xrightarrow{\delta} H^1(G, I) \to R^+/Z.$$

Suppose that K/k is a totally ramified extension. Since in this case $\mu(c) = 0$, there exists a uniquely determined element

$$\varphi \in \operatorname{Char} H^1(G, Q)$$

such that $\lambda(\varphi) = c$. The character φ is determined in terms of the extension K/k as follows. Let

$$[g] \in H^1(G, Q)$$

be a cohomology class determined by a cocycle $g \in Z^1(G, Q)$. For some element $u_g \in D$ we have

$$g(\sigma) = (\sigma - 1)u_g.$$

Put

$$\varphi([g]) = \frac{v(u_g)}{m} \bmod Z.$$

Theorem 4. If K/k is a totally ramified p-extension, then for the just-defined character φ from the group $\operatorname{Char} H^1(G, Q)$ we have $\lambda(\varphi) = c$.

The extension (1) will be O-split if and only if $c = 0$. This gives us the following result.

Theorem 5. If K/k is a totally ramified p-extension and if the maximal subfield of K radical over k is generated by adjoining roots of principal units of the field k, then the group E, as an O-module, is similar to the direct sum $I \oplus A$.

Let us now consider the case of a regular local field k (not containing a primitive root of degree p from 1). For regular k, the exact sequence (2) reduces to the isomorphism

$$\operatorname{Ext}^*(A, I) = \operatorname{Ext}(A, I) \approx \operatorname{Char} G.$$

Theorem 6. If k is a regular local field, then the O-module E is similar to the tensor product $I \otimes Y$ (over Z), where the O-module Y is determined as the extension

$$0 \to Z \to Y \to I \to 0,$$

corresponding to a character

$$\chi \in \operatorname{Char} G \approx \operatorname{Ext}(I, Z),$$

whose kernel coincides with the inertia subgroup G_0 of the extension K/k, and for which

$$\chi(\sigma) = \frac{1}{f} \bmod Z$$

for an automorphism $\sigma \in G$ inducing on the inertia subfield the Frobenius automorphism.

In the paper [4], Theorem 6 was established (by another method) for the case when the minimal number of generators of the group G does not exceed n.

Keeping the regularity condition on k, suppose that the minimal number of generators of the group G is equal to $d+1$, and that its generators $\sigma_0, \sigma_1, \dots, \sigma_d$ are chosen so that

$$G/[G,G] = \{\overline{\sigma}_0\} \times \{\overline{\sigma}_1\} \times \cdots \times \{\overline{\sigma}_d\}$$

(here $\overline{\sigma}_i$ denotes the coset modulo the commutator subgroup $[G,G]$ with representative σ_i). Let

a_i is the order of the element $\bar{\sigma}_i$ $(0 \le i \le d)$. Consider the free O-module W of rank $d+1$ with free O-generators $x_0, x_1, \dots, x_d$. The mapping $x_i \mapsto \sigma_i - 1$ defines an operator epimorphism $W \to I$. Denote its kernel by Ω. The module Ω is indecomposable[4] into a direct sum of O-modules. The elements

$$l_i = \sum_{\tau \in G} \tau(x_i) \quad (0 \le i \le d)$$

form a basis of the Z-lattice $\Omega^G = W_G$.

Denote by Θ the kernel of the mapping

$$N: \; x \mapsto N(x) = \sum_{\tau \in G} \tau(x), \quad x \in \Omega.$$

The O-module Θ is also indecomposable. Since the elements $a_i l_i$ $(0 \le i \le d)$ form a basis of the Z-lattice $N(\Omega)$, we have $a_i l_i = N(v_i)$ for some $v_i \in \Omega$. It is obvious that the module Ω is generated by the submodule Θ and the elements v_i, i.e.

$$\Omega = \{\Theta, v_0, v_1, \dots, v_d\}.$$

We may assume that σ_0 induces the Frobenius automorphism on the inertia subfield. Let the rational integers r_i $(1 \le i \le d)$ be chosen so that $\sigma_i \sigma_0^{-r_i} \in G_0$. Then

$$G_0 = \{\sigma_0^f, \sigma_1 \sigma_0^{-r_1}, \dots, \sigma_d \sigma_0^{-r_d}\}.$$

Put

$$c_0 = a_0/f, \quad c_i = a_i r_i / f \quad (1 \le i \le d).$$

In the direct sum $\Omega \oplus Ow$, consider the submodule

$$M = \{\Theta, Iw, v_0 + c_0 w, v_1 + c_1 w, \dots, v_d + c_{dw}\}.$$

Theorem 7. *For regular k, the group of principal units E of the field K, as an O-module, is similar to the O-module M constructed above. If $f > 1$ and $c_i \equiv 0 \pmod{p}$ for all $i = 0, 1, \dots, d$, then the O-module M is indecomposable. If, however, at least one of the numbers c_i is not divisible by p, then M decomposes into a direct sum of an indecomposable O-module and a free O-module with one generator.*

Thus, if $f > 1$, the group E decomposes into a direct sum of a free O-module and a certain indecomposable O-module E_0. The Z-rank of the module E_0 is determined by the following theorem.

Theorem 8. *If K/k is not a totally ramified extension of a regular local field k, then the group of principal units E of the field K, as an O-module, is similar to an indecomposable O-module E_0, which is a Z-lattice of rank $(d+1)m$, if the inertia subfield inside K is embeddable in a cyclic ramified extension over k, and of rank dm in the opposite case.*

Leningrad State University
named after A. A. Zhdanov

Received
28 IV 1966

CITED LITERATURE

[1] Z. I. Borevich, D. K. Faddeev, *Vestn. Leningradsk. Univ.*, No. 7, 72 (1959).
[2] Z. I. Borevich, *Izv. AN SSSR, Ser. Matem.*, 16, No. 5, 427 (1952).
[3] Z. I. Borevich, *Uch. Zap. Kabardino-Balkarsk. Gos. Univ., Ser. Fiz.-Matem.*, vol. 24, 53 (1965).
[4] Z. I. Borevich, *Tr. Matem. Inst. im. V. A. Steklova AN SSSR*, 80, 30 (1965).

Note: Figure translations are in progress. See original paper for figures.