L. V. Kuz'min, Arithmetic of certain ℓ-extensions ramified at three places. III, *Izvestiya: Mathematics*, 2022, Volume 86, Issue 6, 1143–1161

DOI: 10.4213/im9241e

Izvestiya: *Mathematics* **86**:6 1143–1161 *Izvestiya RAN*: *Ser. Mat.* **86**:6 123–142

DOI: https://doi.org/10.4213/im9241e

Arithmetic of certain ℓ-extensions ramified at three places. III

L. V. Kuz'min

Abstract. Let ℓ be a regular odd prime, K the ℓth cyclotomic field and $K = k(\sqrt[\ell]{a}\,)$, where a is a positive integer. Under the assumption that there are exactly three places ramified in the extension K_∞/k_∞, we study the ℓ-component of the class group of the field K. We prove that in the case $\ell > 3$ there always is an unramified extension $\mathcal{N}/K$ such that $G(\mathcal{N}/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ and all places over ℓ split completely in the extension $\mathcal{N}/K$. In the case $\ell = 3$ we give a complete description of the situation. Some other results are obtained.

Keywords: Iwasawa theory, Tate module, extensions with restricted ramification.

§ 1. Introduction

Let ℓ be a regular odd prime number, $k = \mathbb{Q}(\zeta_0)$, where ζ_0 is a primitive root of unity of degree ℓ and $K = k(\sqrt[\ell]{a}\,)$, where a is a natural number of the form (3.1) such that its prime divisors p_1, p_2, p_3 remain prime in the cyclotomic $\mathbb{Z}_\ell$-extension k_∞ of K. The arithmetic of K, which has many interesting features, was a subject of our investigation in [1] and [2]. So, it appeared that the ℓ-component of the class group $\mathrm{Cl}(K)_\ell$ of K is non-zero. It has an order at most $\ell^{\ell-1}$, and its period is ℓ. In the simplest case $\ell = 3$ there were found in empirical way the fields K, such that their places over ℓ, generate a subgroup of order ℓ in the class group $\mathrm{Cl}(K)_\ell$ (the fields of the type A1 in terminology of [2]) and the fields such that all their places over ℓ are principal divisors (the fields of the type A2). Essentially nothing was known in the case $\ell > 3$,though it was proved in [1] that in the case of infinite Tate module $T_\ell(K_\infty)$ of K_∞ the generator γ_0 of the Galois group $\Gamma = G(K_\infty/K)$, which acts on the roots of unity of the ℓ-primary degree by the rule $\gamma_0(\zeta_n) = \zeta_n^{\varkappa(\gamma_0)}$, where $\varkappa(\gamma_0) \in \mathbb{Z}_\ell$, acts on $T_\ell(K_\infty)$ by multiplication by $\sqrt{\varkappa(\gamma_0)}$ [1], Theorem 5.1.

It was proved in [2] that in the case of finite Tate module $T_\ell(K_\infty)$ there is some greater group $E'(K_\infty)$, which contains $T_\ell(K_\infty)$, such that γ_0 acts on it also by multiplication by $\sqrt{\varkappa(\gamma_0)}$.

In the present paper we use a new method to study the arithmetic of K. Namely, simultaneously with K we consider another field L of the form (3.2) such that there are only two places p_1 and p_2 ramified in L/k. The arithmetic of L is simpler than

This paper was written with the support of the NRC "Kurchatov Institute" (order 24.05.2020 no. 1917).

AMS 2020 *Mathematics Subject Classification*. 11R23, 11R18.

that of K. Moreover, we can fix the field L and change a prime number p_3. Thus, we consider a family of the fields $K = K(p_3)$, and this consideration leads to a series of interesting consequences.

In § 3 we consider the Galois cohomologies groups $H^i(G(L/k), U(L))$ and $H^i(G(K/k), U(K))$. We define some critically important subgroup $\overline{U}_2(L)$ or $\overline{U}_2(K)$ of the group of units $U(L)$ or $U(K)$ and prove that $\overline{U}_2(L)$ is a cohomologically trivial module. Concerning the field K, in the present moment we cannot say whether the module $\overline{U}_2(K)$ may be not cohomologically trivial. In the present paper we use only results that take place for L, but since the proofs for L and for K are just the same, we give both proofs, thou the results for K will be used only in the next our paper.

In § 4 we consider some general properties of G-modules, where $G = G(K/\mathbb{Q})$ and $G = \widetilde{G} = G(L/\mathbb{Q})$. We apply these results for characterization of the Galois module $\mathcal{A}(L)/\mathcal{A}(L)^\ell$ (Theorem 4.1), where $\mathcal{A}(L) = \prod_{v|\ell} U^{(1)}(L_v)$ and $U^{(1)}(L_v)$ is the group of principal units of the local field L_v.

In § 5 we apply the obtained results for characterization of some Abelian extensions of the field L. Namely, let $N = N(p_3)$ be the maximal Abelian ℓ-extension of L such that $N \supset K$, N/K is unramified, and the Galois group $G(N/L)$ is of period ℓ. Using the obtained information about the group $\mathcal{A}(L)/\mathcal{A}(L)^\ell$, we can calculate the Kummer group of the extension N/L, and thus, determine its degree. It appears that always we have $[N : L] = \ell^r$ with an even r and $2 \leqslant r \leqslant \ell - 1$. At last, using the Chebotarev density theorem, we prove that any possible value of r realize for infinitely many values of p_3.

If $r < \ell - 1$ then all the places over ℓ split completely in the extension N/L. In the case $r = \ell - 1$, using the Chebotarev theorem, we prove that there are infinitely many p_3 such that $r = \ell - 1$ and all places over ℓ split completely in N/L and infinitely many p_3 such that $r = \ell - 1$ and all places over ℓ have inertia degree ℓ in N/L.

In § 6 we apply the results obtained for the extensions N/L to the extensions of K. We prove that for any prime p_3 the order of the ℓ-class group of $K = K(p_3)$ is at least ℓ^2 (Theorem 6.1). In the case $\ell = 3$ we prove that there are infinitely many p_3 such that $K(p_3)$ is of the type A1 and infinitely many p_3 such that $K(p_3)$ is of the type A2.

§ 2. Notations and definitions

We try to follow the notations of [1], [2]. For a regular odd prime ℓ, let ζ_n be a primitive root of unity of degree ℓ^{n+1}. Let $k = \mathbb{Q}(\zeta_0)$, $k_n = \mathbb{Q}(\zeta_n)$ and $k_\infty = \bigcup_{n=1}^{\infty} k_n$ be the cyclotomic $\mathbb{Z}_\ell$-extension of k. The prime number $p \neq \ell$ remains prime in the field k_∞ if and only if p is a primitive root modulo ℓ^2. We denote the set of all such primes p by $\mathbb{P}_0$. We consider two fields K and L defined by (3.1) and (3.2), respectively. We put $H = G(K/k)$ and $\widetilde{H} = G(L/k)$, where $G(K/k)$ means the Galois group of K/k. Thus, K and L are Galois extensions of degree $\ell(\ell - 1)$ with isomorphic Galois groups $G = G(K/\mathbb{Q})$ and $\widetilde{G} = G(L/\mathbb{Q})$. The Galois group $\Delta = G(k/\mathbb{Q})$ acts on H (or on $\widetilde{H}$) via the Teichmüller character $\omega\colon \Delta \to (\mathbb{Z}/\ell\mathbb{Z})^\times$.

By groups of cohomologies we mean everywhere the Tate groups if the opposite is not said explicitly. We denote by S the set of all places over ℓ of the field under consideration. By $\mathrm{Cl}(K)_\ell$ we denote the ℓ-component of the class group of K, and $\mathrm{Cl}_S(K)_\ell$ means a factorgroup of $\mathrm{Cl}(K)_\ell$ by the subgroup generated by all places in S.

Let $\overline{\mathbf{N}}$ be the maximal Abelian unramified ℓ-extension of K_∞ and $\mathbf{N}$ the maximal subfield of $\overline{\mathbf{N}}$ such that all places over ℓ split in $\mathbf{N}/K_\infty$. We denote the Galois groups of $\overline{\mathbf{N}}/K_\infty$ and $\mathbf{N}/K_\infty$ by $\overline{T}_\ell(K_\infty)$ and $T_\ell(K_\infty)$ respectively. These groups are modules with respect to the action of the Galois group $\Gamma = G(K_\infty/K)$. For a field K or its completion K_v, we denote by $U(K)$ and $U(K_v)$ the unit group of the corresponding field. By $\mu_\ell(K)$ we denote the group of all ℓ-primary roots of unity in K. For a local field K_v, we denote by $U^{(1)}(K_v)$ the group of principal units in K_v. By $D(K)$ we denote the group of divisors of K. For an Abelian group A, we denote by $A[\ell]$ the pro-ℓ-completion of A. By $\overline{U}(K)$ we denote the group $U(K)/\mu(K)$, where $\mu(K)$ is the group of all roots of unity in K. By $\mathcal{A}(K)$ we denote the group $\prod_{v\in S} U^{(1)}(K_v)$ and by $\overline{\mathcal{A}}(K)$ the group $\prod_{v\in S} \overline{U}^{(1)}(K_v)$, where $\overline{U}^{(1)}(K_v) = U^{(1)}(K_v)/\mu_\ell(K_v)$ and $\mu_\ell(K_v)$ is the ℓ-component of $\mu(K_v)$.

We shall often use additive notations for multiplication without special reminding, since we do not use addition in this paper.

§ 3. Cohomologies of certain groups of units

So, let $p_1, p_2, p_3 \in \mathbb{P}_0$ and $K = k(\sqrt[\ell]{a}\,)$, where

$$a = p_1^{r_1} p_2^{r_2} p_3^{r_3}, \qquad r_1 r_2 r_3 \not\equiv 0 \pmod{\ell}, \qquad a^{\ell-1} \equiv 1 \pmod{\ell^2}. \tag{3.1}$$

Then K/k is an extension described in [1], Proposition 2.1. This extension ramifies at $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$, where $\mathfrak{p}_i = (p_i)$ for $i = 1, 2, 3$, and any place v of K over ℓ splits in this extension. The analogous result holds also for any n for the extension K_n/k_n, where $K_n = K \cdot k_n$. The places $\mathfrak{p}_i$ remain prime in k_n and ramify in the extension K_n/k_n. In k_n there is the single place v_n over ℓ, and v_n splits completely in K_n/k_n.

In parallel with K we shall consider the field $L\colon = k(\sqrt[\ell]{b}\,)$, where

$$b = p_1^{s_1} p_2^{s_2}, \qquad s_1 s_2 \not\equiv 0 \pmod{\ell}, \qquad b^{\ell-1} \equiv 1 \pmod{\ell^2}. \tag{3.2}$$

The extension L/k ramify in $\mathfrak{p}_1$, $\mathfrak{p}_2$, and the place v splits completely in it.

As it was shown in [1], Proposition 2.1, for a given triple of primes $p_1, p_2, p_3 \in \mathbb{P}_0$ there are $\ell - 2$ different fields K corresponding to this choice of r_1, r_2, r_3. On the contrary, the numbers p_1, p_2 define L uniquely. The next assertion is an analogue of Theorem 4.1 of [1].

Proposition 3.1. *The following equalities hold*: $\overline{T}_\ell(L_\infty) = T_\ell(L_\infty) = 0$, $\mathrm{Cl}(L)_\ell = \mathrm{Cl}_S(L)_\ell = 0$.

Proof. Consider an $\widetilde{H}$-module $\overline{T}_\ell(L_\infty)$. Let f be the minimal number of its generators as $\widetilde{H}$-module. Then f equals the minimal number of generators of the Abelian group $C := \overline{T}_\ell(L_\infty)/(\widetilde{\sigma} - 1)\overline{T}_\ell(L_\infty)$. As in [1], this implies that C is isomorphic to $\mathbb{F}_\ell^f$ as an Abelian group.

Let $\overline{N}$ be the extension of L_∞, whose Galois group is naturally isomorphic to the group $\overline{T}_\ell(L_\infty)$. Let $\overline{N}_0$ be the subfield of $\overline{N}$ fixed by the action of the Galois group $(\widetilde{\sigma}-1)\overline{T}_\ell(L_\infty)$, where $\widetilde{\sigma}$ is a generator of the group $\widetilde{H}$. Then, as in [1], we obtain that $G(\overline{N}_0/k_\infty)$ is an Abelian group of period ℓ and of order ℓ^{f+1}. To calculate f, we use the Kummer theory. Let M be a subfield of $\overline{N}_0$ of degree ℓ over L_∞. Then M is of the form $M = k_\infty(\sqrt[\ell]{\alpha}\,)$. Applying to the field M the same arguments that were used in the proof of Theorem 4.1 of [1], we get that the element α is defined uniquely up to raising in some power prime to ℓ and multiplication by some ℓ-th power. It means that $M = \overline{N}_0$. Then $\overline{N}_0 = L_\infty$ and $f = 0$. Therefore, $\overline{T}_\ell(L_\infty) = 0$. Since there are epimorphisms $\overline{T}_\ell(L_\infty) \to T_\ell(L_\infty)$, $\overline{T}_\ell(L_\infty) \to \mathrm{Cl}(L)_\ell$ and $\overline{T}_\ell(L_\infty) \to \mathrm{Cl}_S(L)_\ell$, we get $T_\ell(L_\infty) = 0$ and $\mathrm{Cl}(L)_\ell = \mathrm{Cl}_S(L)_\ell = 0$. This proves Proposition 3.1.

Remark. We can give more short but less direct proof of Proposition 3.1. Namely, we shall prove that $\overline{T}_\ell(L_\infty) = 0$. Applying the Riemann–Hurwitz formula to the extension L_∞/k_∞ (see, for example, [1], Theorem 1.1), we obtain $d(L_\infty) = \lambda'(L_\infty) = \lambda''(L_\infty) = r''(L_\infty) = 0$. Therefore, the module $\overline{T}_\ell(L_\infty)$ is at most finite and $D(L_\infty) = 0$ (the definition of $D(L_\infty)$ one can find in [1], § 6). Then the module $E'(L_\infty)$ defined in [1], Proposition 6.3, also vanishes. According to [2], Theorem 3.1, the module $E'(L_\infty)$ contains a submodule $E'_2(L_\infty)$, which is isomorphic to $\overline{T}_\ell(L_\infty)$. Hence, $\overline{T}_\ell(L_\infty) = 0$.

Our nearest goal is to study the groups of cohomologies $H^i(H, U(K))$ and $H^i(\widetilde{H}, U(L))$, and also the cohomologies of some subgroups and factorgroups of these groups of units. The exact sequence of H-modules

$$1 \to U(K) \to K^\times \to D_K^0 \to 1,$$

where D_K^0 is the group of principal divisors of K, induces an exact sequence of cohomologies

$$1 \to U(k) \to k^\times \to (D_K^0)^H \xrightarrow{\eta} H^1(H, U(K)) \to 1. \tag{3.3}$$

By Theorem 90 of Hilbert any element of $H^1(H, U(K))$ may be presented by a cocycle $f\colon H \to U(K)$ of the form $f = f_c$, where $f_c(h) = h(c)/c$, $c \in K^\times$ and the principal divisor (c) is fixed under the action of H. Any such (c) is of the form $(c) = a_1 a_2$, where $a_1 \in D(k)$ and a_2 is a product of some prime divisors of K ramified in K/k. In particular, the group $H^1(H, U(K))$ contains an element, which is presented by the cocycle $f_{\overline{a}}(h)$, where $\overline{a} = \sqrt[\ell]{a}$ and a is as in (3.1). Analogously, the group $H^1(\widetilde{H}, U(L))$ contains an element presented by $f_{\overline{b}}(h)$, where $\overline{b} = \sqrt[\ell]{b}$ and b is the element in (3.2). These cocycles take their values in the groups $\mu_\ell(K)$ and $\mu_\ell(L)$ respectively.

Proposition 3.2. *The inclusion $\mu_\ell(K) \hookrightarrow U(K)$ induces inclusions*

$$i_1\colon H^1(H, \mu(K)) \hookrightarrow H^1(H, U(K)), \qquad i_2\colon H^0(H, \mu_\ell(K)) \hookrightarrow H^0(H, U(K)). \tag{3.4}$$

Analogously, the inclusion $\mu_\ell(L) \hookrightarrow U(L)$ induces inclusions

$$j_1\colon H^1(\widetilde{H}, \mu_\ell(L)) \hookrightarrow H^1(\widetilde{H}, U(L)), \qquad j_2\colon H^0(\widetilde{H}, \mu_\ell(L)) \hookrightarrow H^0(\widetilde{H}, U(L)). \tag{3.5}$$

Proof. The class $\mathrm{cls}(f_{\overline{a}}(h))$ of the cocycle $f_{\overline{a}}(h)$ generates the group $H^1(H,\mu_\ell(K))$. Suppose that $i_1(\mathrm{cls}(f_{\overline{a}}(h)))=0$. It means that there is a unit $u\in U(K)$ such that $h(u)/u=h(\overline{a})/\overline{a}$ for any $h\in H$. Then $u/\overline{a}\in k^\times$, $u_1:=u^\ell\in k$ and $K=k(\sqrt[\ell]{u})$, but this is impossible. Indeed, the place v of K over ℓ splits completely in K/k, but any unit u_1 of K, which is an ℓ-th power in the local field k_v, is also an ℓ-th power in K (otherwise $k(\sqrt[\ell]{u_1})/k$ would be an unramified extension of degree ℓ). This proves that the map i_1 in (3.4) is an inclusion. The monomorphic character of j_1 in (3.5) may be proved in the same way.

To prove the monomorphic character of i_2 in (3.4), it is enough to check that ζ_0 is not a norm in the extension K/k. To do this, we note that $\mathfrak{p}_1=(p_1)$ ramifies in K/k and also in the extension of local fields $K_{\mathfrak{P}_1}/k_{\mathfrak{p}_1}$, where $\mathfrak{P}_1$ is a prime divisor of $\mathfrak{p}_1$ in K. By local class field theory it means that

$$\big(U(k_{\mathfrak{p}_1}):N(U(K_{\mathfrak{P}_1}))\big)=\ell, \tag{3.6}$$

where N means the norm map from $K_{\mathfrak{P}_1}$ into $k_{\mathfrak{p}_1}$. Since $\mathfrak{p}_1$ remains prime in k_∞, the field $k_{\mathfrak{p}_1}$ does not contain the primitive root of unity ζ_1 of degree ℓ^2, that is, the ℓ-component of $U(k_{\mathfrak{p}_1})$ is generated by ζ_0. Then (3.6) means that ζ_0 is not a norm in $K_{\mathfrak{P}_1}/k_{\mathfrak{p}_1}$ and, moreover, in K/k. This proves the monomorphic character of j_1 in (3.5). The monomorphic character of j_2 may be proved in the same way. This proves Proposition 3.2.

For local or global algebraic number field F we shall denote by $\overline{U}(F)$ the factor group $U(F)/\mu(F)$.

Proposition 3.3. *For $i=0,1$ the equalities hold*

$$|H^i(H,\overline{U}(K))|=\ell^{-1}|H^i(H,U(K))|, \tag{3.7}$$

$$|H^i(\widetilde{H},\overline{U}(L)|=\ell^{-1}|H^i(\widetilde{H},U(L))|. \tag{3.8}$$

Proof. The exact sequence of H-modules

$$1\to\mu(K)\to U(K)\to\overline{U}(K)\to 1$$

induces an exact sequence of cohomologies

$$\begin{aligned}\cdots\to H^0(H,\mu(K))\xrightarrow{\alpha}H^0(H,U(K))\to H^0(H,\overline{U}(K))\to H^1(H,\mu(K))\\ \xrightarrow{\beta}H^1(H,U(K))\to H^1(H,\overline{U}(K))\xrightarrow{\gamma}H^2(H,\mu(K))\to\cdots.\end{aligned} \tag{3.9}$$

Since $H^i(H,\mu(K))=H^i(H,\mu_\ell(K))$ for any i it follows from Proposition 3.2 that α and β are injections. So, for any i and any H-module A there is a natural isomorphism $H^i(H,A)\cong H^{i+2}(H,A)$. Hence the sequence (3.9) is periodic with period 2, and injectivity of α yields $\gamma=0$. Therefore, (3.9) induces short exact sequences

$$0\to H^0(H,\mu(K))\xrightarrow{\alpha}H^0(H,U(K))\to H^0(H,\overline{U}(K))\to 0,$$

$$0\to H^1(H,\mu(K))\xrightarrow{\beta}H^1(H,U(K))\to H^1(H,\overline{U}(K))\to 0,$$

whence it follows the assertion of the proposition for K. The proof for L is just the same. This proves Proposition 3.3.

Let F be an arbitrary algebraic number field, F_v the completion of F relative to some place v over ℓ and $F_{v,\infty}$ the cyclotomic $\mathbb{Z}_\ell$-extension of F_v. Put $\Gamma_v = G(F_{v,\infty}/F_v)$.

If the extension $F_{v,\infty}/F_v$ is purely ramified then by the local class field theory we have the canonical epimorphism $U^{(1)}(F_v) \to \Gamma_v$, whose kernel coincides with the group $\mathcal{U}(F_v)$ of universal norms from all groups $U^{(1)}(F_{v,n})$ in the extension $F_{v,\infty}/F_v$, that is, $\mathcal{U}(F_v) = \cap_n N_n(U^{(1)}(F_{v,n}))$, where N_n means the norm map from $F_{v,n}$ into F_v.

As in [2], § 3, we denote by $P(F)$ the kernel of the natural map $\chi_F : \prod_{v\in S}\Gamma_v \to \Gamma$, where $\Gamma = G(F_\infty/F)$, and Γ_v inserts in Γ as a decomposition subgroup of v. Thus, if all places over ℓ purely ramify in F_∞/F then there are exact sequences

$$1 \to P(F) \to \prod_{v\in S}\Gamma_v \xrightarrow{\chi_F} \Gamma \to 1, \tag{3.10}$$

$$1 \to \prod_{v\in S}\mathcal{U}(F_v) \to \prod_{v\in S}U^{(1)}(F_v) \xrightarrow{\pi_F} \prod_{v\in S}\Gamma_v \to 1. \tag{3.11}$$

If F is normal over $\mathbb{Q}$ then all groups entering (3.10) and (3.11) are $G(F/\mathbb{Q})$-modules.

The diagonal inclusion $U(F)[\ell] \hookrightarrow P(F)$ combined with (3.11) induce a map $\varphi_F : U(F)[\ell] \to P(F)$, whose kernel, which we denote by $U_2(F)$, – is the subgroup of all local universal norms from F_∞ in the group $U(F)[\ell]$. In particular, in the cases $F = K$ or $F = L$ we have the maps φ_K, φ_L and the groups $U_2(K)$, $U_2(L)$.

Proposition 3.4. *The maps φ_K and φ_L are epimorphisms. In other words, there are exact sequences*

$$1 \to U_2(K) \to U(K)[\ell] \to P(K) \to 1, \tag{3.12}$$

$$1 \to U_2(L) \to U(L)[\ell] \to P(L) \to 1. \tag{3.13}$$

Proof. For K the desired assertion was already proved in [2], Proposition 4.2. For L the proof is even simpler. Let M be the maximal Abelian ℓ-extension of L unramified out of ℓ, and such that for any $v \in S$ the field M_v contains in the cyclotomic $\mathbb{Z}_\ell$-extension of L_w, where w is a place of L under v. Then, taking into account, that $\mathrm{Cl}(L)_\ell = 0$ by Proposition 3.1 and applying the class field theory, we get that $G(M/L_\infty) \cong P(L)/\operatorname{Im}\varphi_L$, but according to Proposition 3.1 we have $\overline{T}_\ell(L_\infty) = 0$, whence it follows $M = L_\infty$. This proves Proposition 3.4.

In each of the extensions K/k and L/k the place $v \in S$ of K splits completely, hence (3.10) yields

$$P(K) \cong I_H, \qquad P(L) \cong I_{\widetilde{H}}, \tag{3.14}$$

where I_H and $I_{\widetilde{H}}$ are the ideals of augmentation of the group rings $\mathbb{Z}_\ell[H]$ and $\mathbb{Z}_\ell[\widetilde{H}]$ respectively. In particular, $H^0(H, P(K)) = 0$ and $H^{-1}(H, P(K)) \cong \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$. The analogous result holds for $P(L)$.

We put $\overline{U}_2(K) = U_2(K)/\mu_\ell(K)$ and $\overline{U}_2(L) = U_2(L)/\mu_\ell(L)$.

Proposition 3.5. *Let $\mathfrak{P}_1$ be a prime divisor in K (or in L) of the divisor $\mathfrak{p}_1 = (p_1)$, where p_1 is a prime number entering in a in (3.1) (or in b in (3.2)). Let the*

order of $\mathfrak{P}_1$ *in the group* $\mathrm{Cl}(K)$ (*respectively, in the group* $\mathrm{Cl}(L)$) *is prime to* ℓ. (*Note that the last condition always holds for* L *because of Proposition* 3.1.) *Then the following equalities hold*

$$|H^1(H,\overline{U}_2(K))| = \ell^{-1}|H^1(H,\overline{U}(K))|, \qquad |H^0(H,\overline{U}_2(K))| = |H^0(H,\overline{U}(K))|,$$
$$|H^1(\widetilde{H},\overline{U}_2(L))| = \ell^{-1}|H^1(\widetilde{H},\overline{U}(L))| = 1, \quad |H^0(\widetilde{H},\overline{U}_2(L))| = |H^0(\widetilde{H},\overline{U}(L))| = 1.$$

Proof. Let $x \in K^\times$ be such an element that $(x) = \mathfrak{P}_1^h$ for some h prime to ℓ. The element x is defined up to multiplication by an arbitrary unit in $U(K)$. Then x, as well as p_1, is a unit in the local field K_v for any v over ℓ. Therefore, under the diagonal inclusion $K^\times \hookrightarrow \prod_{v\in S} K_v^\times$ the elements x and p_1 go into $\prod_{v\in S} U(K_v)$, so, we can consider they as elements of the group $\prod_{v\in S} U(K_v)[\ell] = \prod_{v\in S} U^{(1)}(K_v)$. Obviously, $N_{K/k}(x) = p_1^h u$, where u is a unit in $U(K)$. Let $x_1 = \pi_k(x)$, where π_k is the map from (3.11) for K.

Since $\mathfrak{P}_1^\ell = \mathfrak{p}_1 = (p_1)$ we obtain that in the group Γ in (3.10) holds the relation $\chi_K(\pi_K(x)^\ell)) = \chi_K(\pi_K(p_1^h))$, but $\chi_K(\pi_K(p_1^h))$ generates the group Γ^ℓ. Hence the element $y = \chi_K(\pi_K(x))$ generates the group Γ. If y' is some lifting of y in $\prod_{v\in S}\Gamma_v$ then y' generates this group as an H-module.

Let z be the image of $(\sigma - 1)(x)$ in $\overline{U}(K)$. Then z defines some element of the group $H^{-1}(H,\overline{U}(K))$, moreover, $\pi_K(z)$ generates the group $H^{-1}(H,P(K)) \cong H^1(H,P(K))$. Therefore, the natural map $H^{-1}(H,\overline{U}(K)[\ell]) \to H^{-1}(H,P(K))$, induced by the map φ_K of (3.11), is an epimorphism. Then the exact cohomological sequence for (3.12) yields exact sequences

$$0 = H^{-2}(H,P(K)) \to H^{-1}(H,\overline{U}_2(K)) \to H^{-1}(H,\overline{U}(K)[\ell] \to H^{-1}(H,P(K)) \to 0,$$
$$0 \to H^0(H,\overline{U}_2(K)) \to H^0(H,\overline{U}(K)[\ell]) \to H^0(H,P(K)) = 0.$$

This proves the proposition for K. The proof for L is quite analogous (with using the exact sequence (3.13)). This proves Proposition 3.5.

Theorem 3.1. *There are two possibilities for* K.

(A) *All three divisors* $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ *have an order prime to* ℓ *in the group* $\mathrm{Cl}(K)$. *In this case*

$$|H^0(H,\overline{U}_2(K))| = |H^1(H,\overline{U}_2(K))| = \ell.$$

This case always take place if $|\mathrm{Cl}_\ell(K)| < \ell^{\ell-1}$.

(B) *At least, one of the divisors* $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ *present non-zero element in* $\mathrm{Cl}(K)_\ell$. *Then*

$$|H^0(H,\overline{U}_2(K))| = |H^1(H,\overline{U}_2(K))| = 1 \quad \textit{and} \quad |\mathrm{Cl}(K)_\ell| = \ell^{\ell-1}.$$

For the field L *we always have*

$$H^0(\widetilde{H},\overline{U}_2(L)) = H^1(\widetilde{H},\overline{U}_2(L)) = 0.$$

Proof. Let $\mathfrak{A} = \mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\mathfrak{P}_3^{m_3}$ be a product of prime divisors, which ramify in K/k. If $\mathfrak{A}$ is a principal divisor then by (3.3) the element $\mathfrak{A} \in (D_K^0)^H$ determines some element $\eta(\mathfrak{A})$ in the group $H^1(H,U(K))$. Put

$$\mathcal{A} = (\mathbb{Z}\mathfrak{P}_1 \oplus \mathbb{Z}\mathfrak{P}_2 \oplus \mathbb{Z}\mathfrak{P}_3)/(\mathbb{Z}\mathfrak{p}_1 \oplus \mathbb{Z}\mathfrak{p}_2 \oplus \mathbb{Z}\mathfrak{p}_3) \cong (\mathbb{Z}/\ell\mathbb{Z})^3.$$

Then there is an exact sequence

$$0 \to (D_K^0)^H/D_k \to \mathcal{A} \xrightarrow{\psi} \mathrm{Cl}(K)_\ell^H. \tag{3.15}$$

It follows from [1], Theorem 4.1, that $\mathrm{Cl}(K)_\ell$ is a cyclic H-module, that vanishes under the norm map N_H, therefore, by [1], Lemma 3.1, the group $\mathrm{Cl}(K)_\ell^H$ is of order ℓ.

So, it follows from (3.15) that the group $H^1(H, U(K)) = (D_K^0)^H/D_k$ is of order ℓ^2 if $\psi \neq 0$, or of order ℓ^3 if $\psi = 0$.

In the case (A) we have $\psi = 0$, that is, $|H^1(H, U(K))| = \ell^3$. Calculating the Herbrand index $h(U(K))$ via Dirichlet theorem, we obtain

$$h(U(K)) = |H^0(H, U(K))|/|H^1(H, U(K))| = \ell^{-1}, \text{ that is, } |H^0(H, U(K))| = \ell^2.$$

Then by Proposition 3.2 we get $|H^1(H, \overline{U}(K))| = \ell^2$ and $|H^0(H, \overline{U}(K))| = \ell$. The condition $\psi = 0$ means that the assumptions of Proposition 3.5 hold, that is,

$$|H^1(H, U_2(K))| = \ell \quad \text{and} \quad |H^0(H, U_2(K))| = \ell.$$

Consider the lower central series of the H-module $\mathrm{Cl}(K)_\ell$. The first factor of this series is isomorphic to $\mathbb{F}_\ell(1)$ as a Δ-module. Then [1], Lemma 3.2, yields that in the case $|\mathrm{Cl}(K)_\ell| < \ell^{\ell-1}$ this central series has no factors isomorphic to $\mathbb{F}_\ell(0)$ as a Δ-module. This is the situation of the case (A).

Now we turn to the case (B). If one of the divisors $\mathfrak{P}_i$, $\mathfrak{P}_1$ for example, presents a non-zero element of $\mathrm{Cl}(K)$ then this element is fixed under the action of G. Then, applying Lemma 3.2 of [1] again and taking into account that $\mathrm{Cl}(K)_\ell/(\sigma - 1)\,\mathrm{Cl}(K)_\ell \cong \mathbb{F}_\ell(1)$ as a Δ-module, we obtain that the length of the lower central series of the H-module $\mathrm{Cl}(K)_\ell$ is at least $\ell - 1$, but its length cannot be bigger, since the group $\mathrm{Cl}(K)_\ell$ is of period ℓ by Corollary 3.1 of [2]. Therefore, in this case we have $|\mathrm{Cl}(K)_\ell| = \ell^{\ell-1}$.

Since $\psi \neq 0$ in (3.15) we get

$$|H^1(H, U(K))| = \ell^2 \quad \text{and} \quad |H^0(H, U(K))| = \ell.$$

Now, it follows from Proposition 3.2 that $|H^1(H, \overline{U}(K))| = \ell$ and $|H^0(H, \overline{U}(K))| = 1$. This completes the proof of the theorem for K.

The proof for L is analogous. We can write down an analogue of Formula (3.15) for the field L again, but in this case we have $\mathrm{Cl}(L)_\ell^H = 0$ by Proposition 3.1, and $\mathcal{A} \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, so, $|H^1(\widetilde{H}, U(L))| = \ell^2$ and $|H^0(\widetilde{H}, U(L))| = \ell$. By virtue of Proposition 3.2 we have $|H^1(\widetilde{H}, \overline{U}(L))| = \ell$ and $|H^0(\widetilde{H}, \overline{U}(L))| = 1$. Then Proposition 3.5 yields that $H^1(\widetilde{H}, U_2(L)) = H^0(\widetilde{H}, U_2(L)) = 0$. This proves Theorem 3.1.

§ 4. Structure of certain groups of units of the field L

Let $\mathcal{A}(L) = \prod_{v \in S} U^{(1)}(L_v)$ and $\overline{\mathcal{A}}(L) = \prod_{v \in S} \overline{U}^{(1)}(L_v)$ be the maximal $\mathbb{Z}_\ell$-free factor module of $\mathcal{A}(L)$. Our nearest goal is to characterize $\mathcal{A}(L)$ as a $\mathbb{Z}_\ell[\widetilde{G}]$-module. To do this, we need some general results on $\mathbb{Z}_\ell[\widetilde{G}]$-modules, which are analogous to those in [1], § 3. Since the groups $G = G(K/\mathbb{Q})$ and $\widetilde{G} = G(L/\mathbb{Q})$ are isomorphic we shall formulate these general results for the case of G-modules.

We shall consider a Noetherian G-module A that is free as a $\mathbb{Z}_\ell[H]$-module. These conditions on A are equivalent to simultaneous fulfilment of the following two conditions:

(i) A is Noetherian and has no torsion over $\mathbb{Z}_\ell$;

(ii) A is a cohomologically trivial $\mathbb{Z}_\ell[H]$-module.

As in [1], we assume that some section $f\colon \Delta \to G$ is fixed. Let $\delta' = f(\delta)$ be a fixed generator of $f(\Delta)$ and e_i the idempotent of $\mathbb{Z}_\ell[f(\Delta)]$ corresponding to the character ω^i, where ω is the Teichmüller character. For $a \in A$ we denote by $a[i]$ the element $e_i a$. Let σ be a fixed generator of H.

As in [1], let $F_1 = \mathbb{Z}_\ell[G]$ be a free G-module of rank 1. Then we have

$$F_1/(\ell, (\sigma - 1))F_1 \cong \bigoplus_{i=0}^{\ell-2} \mathbb{F}_\ell(i).$$

If $a \in F_1$ is a generator of G-module F_1 then $a = \sum_{i-0}^{\ell-2} a[i]$ and thus

$$F_1 = Q(0) + Q(1) + \cdots + Q(\ell - 2), \quad \text{where } Q(i) = \mathbb{Z}_\ell[H]a[i]. \tag{4.1}$$

Any of $Q(i)$ is a G-module and has the rank at most ℓ as a $\mathbb{Z}_\ell$-module. Then it follows from (4.1) that the rank is exactly ℓ, and (4.1) defines a decomposition of F_1 into a direct sum of G-modules $Q(i)$ for $i = 0, 1, \ldots, \ell - 2$. Therefore, each of the modules $Q(i)$ is projective as a G-module.

Proposition 4.1. *Let A be a Noetherian G-module, which is free as a $\mathbb{Z}_\ell[H]$-module. Then there is a (non-canonical) isomorphism of G-modules*

$$A \cong \bigoplus_{i=0}^{\ell-2} Q(i)^{r_i}, \tag{4.2}$$

where the exponents r_i are defined uniquely by the module A. In particular, if A is a cyclic H-module then $A \cong Q(i)$ for some i.

Proof The proof of this proposition is completely analogous to that of Proposition 3.1 of [1].

Corollary 4.1. *Suppose that we have an exact sequence of Noetherian $\mathbb{Z}_\ell[G]$-modules*

$$0 \to A \to B \to C \to 0,$$

such that A, B, C are free as $\mathbb{Z}_\ell$-modules. If any two modules of this sequence are projective then so is the third one.

So, if A is a free $\mathbb{Z}_\ell[H]$-module of rank 1 then by Proposition 4.1we have $A \cong Q(i)$ for some i. In this case $A/(\ell, (\sigma-1))A \cong \mathbb{F}_\ell(i)$. In general, if $A/(\ell, (\sigma-1))A \cong \mathbb{F}_\ell(i)$ then we say that A begins at $\mathbb{F}_\ell(i)$. Under the same assumption, if A is finite and $A^H \cong \mathbb{F}_\ell(k)$ then we say that A ends at $\mathbb{F}_\ell(k)$.

Put $A \cong Q(i)$ and $B = A/\ell A$. Then B is a cohomologically trivial $\mathbb{F}_\ell[H]$-module, and there is a lower central series

$$B = B_0 \supset B_1 \cdots \supset B_\ell = 0, \quad \text{where} \quad B_j/B_{j+1} \cong \mathbb{F}_\ell(i + j)$$

for $j = 0, 1, \ldots, \ell - 1$, as it follows easily from Lemma 3.2 of [1]. The next Proposition is an analogue of Proposition 4.1 for the case $\mathbb{F}_\ell[G]$-modules and may be proved by the same arguments.

Proposition 4.2. *Let $\mathscr{A}$ be a Noether G-module, which is free as a $\mathbb{F}_\ell[H]$-module. Then there is a (non-canonical) isomorphism of G-modules*

$$\mathscr{A} \cong \bigoplus_{i=0}^{\ell-2} \mathscr{Q}(i)^{r_i}, \tag{4.3}$$

where $\mathscr{Q}(i) = Q(i)/\ell Q(i)$ and the exponents r_i are defined uniquely by $\mathscr{A}$. In particular, if $\mathscr{A}$ is a cyclic H-module then $\mathscr{A} \cong \mathscr{Q}(i)$ for some i.

Corollary 4.2. *Let an exact sequence of $\mathbb{F}_\ell[G]$-modules be given*

$$0 \to \mathscr{A} \to \mathscr{B} \to \mathscr{C} \to 0.$$

If any two modules of this sequence are projective in the category of Noetherian $\mathbb{F}_\ell[G]$-modules then so is the third one.

Proposition 4.3. *Let an exact sequence of Noetherian $\mathbb{Z}_\ell[G]$-modules be given*

$$0 \to A \to B \to C \to 0,$$

and these modules are free as $\mathbb{Z}_\ell$-modules. If the G-module A is projective then there is a decomposition into a direct sum $B \cong A' \oplus C'$, where $A \cong A'$ and $C \cong C'$.

Proof. Put $A^0 = \mathrm{Hom}_{\mathbb{Z}_\ell}(A, \mathbb{Z}_\ell)$ and let B^0 and C^0 be of analogous meaning. Let A^0, B^0 and C^0 has a standard structure of left G-modules, as it is explained in [3]. Then there is an exact sequence of G-modules

$$0 \to C^0 \to B^0 \to A^0 \to 0$$

with projective A^0. Therefore, it splits, that is, $B^0 \cong C^0 \oplus \widetilde{A}^0$, where $\widetilde{A}^0 \cong A^0$. Thus $B \cong (B^0)^0 \cong (C^0 \oplus \widetilde{A}^0)^0 \cong C^{00} \oplus \widetilde{A}^{00} \cong C \oplus \widetilde{A} \cong A \oplus C$. This proves Proposition 4.3.

Let $M(L)$ be the kernel of the natural map $\mathcal{A}(L) \to \overline{\mathcal{A}}(L)$. Hence, $M(L) = \prod_{v \in S} \mu_\ell(L_v)$.

Proposition 4.4. *The module $M(L)$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^\ell$ as an Abelian group. It is cyclic and cohomologically trivial as a $\widetilde{H}$-module, where $\widetilde{H} = G(L/k)$. The module $M(L)$ begins at $\mathbb{F}_\ell(1)$ and ends at $\mathbb{F}_\ell(1)$. So, taking into account the notions introduced above, we get an isomorphism of $\widetilde{G}$-modules $M(L) \cong \mathscr{Q}(1)$.*

Proof. The first assertion is obvious. The group $\widetilde{H}$ substitutes the factor $\mu_\ell(L_v)$, hence $M(L)$ is an induced $\widetilde{H}$-module. Therefore, it is cohomologically trivial. The norm map $N_{L/k}$ is a Δ-homomorphism that maps $M(L)$ onto $M(k) = \mu_\ell(k) \cong \mathbb{F}_\ell(1)$. Therefore, $M(L)$ begins at $\mathbb{F}_\ell(1)$. This proves Proposition 4.4.

We see that the $\widetilde{G}$-module $\overline{\mathcal{A}}(L)$ is induced as a $\widetilde{H}$-module. Therefore it is cohomologically trivial as a $\widetilde{H}$-module, and by Proposition 4.1 it has a decomposition of the form (4.2). Note that every direct summand $Q(i)$ enters this decomposition with multiplicity 1, since $N_{L/k}$ induces an isomorphism

$$\overline{\mathcal{A}}(L)/(\widetilde{\sigma}-1)\overline{\mathcal{A}}(L) \cong \overline{\mathcal{A}}(k) \cong \bigoplus_{i=0}^{\ell-2} \mathbb{Z}_\ell(i), \tag{4.4}$$

where $\widetilde{\sigma}$ is a generator of $\widetilde{H}$ and $\mathbb{Z}_\ell(i)$ denotes a $\widetilde{G}$-module, which is isomorphic to $\mathbb{Z}_\ell$ as an Abelian group with trivial action of $\widetilde{H}$, while Δ acts on it by multiplication by ω^i.

In sequel we need the decomposition of $\mathcal{A}(L)$ with some additional properties.

Proposition 4.5. *$\widetilde{G}$-module $\mathcal{A}(L)$ has a decomposition into the direct sum of $\widetilde{G}$-modules $\mathcal{A}(L) = \bigoplus_{i=0}^{\ell-2} \mathcal{A}[i]$, where $\mathcal{A}[i] \cong Q(i)$ as a $\widetilde{G}$-module, and the following conditions hold*:

1) $\mathcal{A}[2i] \subset U_2(L)$ *for* $i = 1, \dots, (\ell-3)/2$;

2) *the direct summand* $\mathcal{A}[0]$ *has a generator* $\mathbf{a}_0$ *such that* Δ *acts trivially on* $\mathbf{a}_0$ *and* $(\widetilde{\sigma}-1)\mathbf{a}_0 \in \overline{U}(L)$.

Proof. The cohomological triviality of $\overline{U}_2(L)$ (see Theorem of 3.1) yields that $\overline{U}_2(L)/(\widetilde{\sigma}-1)\overline{U}_2(L) \cong \overline{U}(k)$, hence

$$\overline{U}_2(L) \cong \bigoplus_{i=1}^{(\ell-3)/2} Q(2i). \tag{4.5}$$

Then $\widetilde{G}$-module $\overline{\mathcal{A}}(L)/\overline{U}_2(L)$ is projective by Corollary 4.1, hence there is a decomposition into the direct sum $\overline{\mathcal{A}}(L) \cong (\overline{\mathcal{A}}(L)/\overline{U}_2(L)) \oplus \overline{U}_2(L)$. Then we put $\overline{\mathcal{A}}[2i] = Q(2i)$, where $Q(2i)$ are the components of $\overline{U}_2(L)$ in the decomposition (4.5).

Let $\overline{\mathcal{A}}_2(L)$ be the subgroup of local universal norms (of L_∞) in the group $\overline{\mathcal{A}}(L)$, so, that there is a natural isomorphism

$$\overline{\mathcal{A}}(L)/\overline{\mathcal{A}}_2(L) \cong \prod_{v\in S} \Gamma_v, \tag{4.6}$$

where $\prod_{v\in S}\Gamma_v$ has the same meaning, as in (3.9) and(3.10). Thus $\overline{\mathcal{A}}(L)/\overline{\mathcal{A}}_2(L)$ is a cohomologically trivial $\widetilde{H}$-module of $\mathbb{Z}_\ell$ rank ℓ. This module admits a natural $\widetilde{G}$-epimorphism $\varphi\colon \overline{\mathcal{A}}(L)/\overline{\mathcal{A}}_2(L) \to \Gamma = G(L_\infty/L)$. Therefore by Proposition 4.2 we have $\overline{\mathcal{A}}(L)/\overline{\mathcal{A}}_2(L) \cong Q(0)$.

Now consider a $\widetilde{G}$-module $\overline{\mathcal{A}}(L)/\overline{U}_2(L)$. By Proposition 4.2 and formulae (4.3), (4.5) we have an isomorphism $B := \mathcal{A}(L)/\overline{U}_2(L) \cong \bigoplus_{i=0}^{(\ell-3)/2} Q(2i+1) \oplus Q(0)$. Let $C = \mathcal{A}_2(L)/U_2(L)$ and $P(L)$ be of the same meaning as in (3.12). Then we can consider C and $P(L)$ as submodules of B, where $C \cong \bigoplus_{i=0}^{(\ell-3)} Q(2i+1)$. Taking into account that C and $P(L)$ have zero intersection in B, we obtain an exact sequence

$$0 \to C \oplus P(L) \to B \to \Gamma \to 0 \tag{4.7}$$

with a projective $\widetilde{G}$-module C, whence, taking factor-module with respect to $P(L)$, we get an exact sequence

$$0 \to C \to B/P(L) \to \Gamma \to 0$$

with projective C. Applying Proposition 4.3 to this sequence, we see that $B/P(L)$ contains a submodule Γ', which is isomorphic to Γ as a $\widetilde{G}$-module, that is, Γ' is isomorphic to $\mathbb{Z}_\ell$ as an Abelian group and $\widetilde{G}$ acts trivially on Γ'. Thus, we have an exact sequence

$$0 \to \Gamma' \xrightarrow{\chi} B/P(L) \to C' \to 0,$$

where $C' \cong C$. Let a' be a generator of Γ'. Then, lifting a' up to some element $a'' \in B$, we obtain an element $a'' \in B$ such that $b := (\widetilde{\sigma} - 1)a'' \in P(L)$. If a $\widetilde{H}$-submodule generated by b would be a proper submodule of $P(L)$ then , after replacing b by some $b' = b + x$ for a suitable $x \in P(L)$, we should obtain $\widetilde{\sigma}(b') = b'$. It means that $B \cong C \oplus P(L) \oplus \mathbb{Z}_\ell b'$ as an $\widetilde{H}$-module. But this contradicts to projectivity of B.

Finally, we put $\mathbf{a} = a''[0]$. Obviously, a'' and $\mathbf{a}$ are equal modulo $P(L)$, $\mathbf{a}$ generates a submodule of B, which is isomorphic to $Q(0)$, and $\mathbf{a}$ is fixed under the action of Δ. This completes the proof of Proposition 4.5.

Using Proposition 4.5, we shall obtain some special decomposition for $\mathscr{B}(L) := \overline{\mathcal{A}}(L)/\ell\overline{\mathcal{A}}(L)$ that we need in the next section. We shall construct a decomposition into the direct sum $\mathscr{B}(L) = \bigoplus_{i=0}^{\ell-2} \mathscr{B}[i]$, where for $i \neq 1$ we put $\mathscr{B}[i] = \mathcal{A}[i]/\ell\mathcal{A}[i]$ and for $i = 1$ we define the component $\mathscr{B}[1]$ as follows.

Let L_v be the completion of L at the place v over ℓ. The group $U(L_v)$ contains ℓ-primary elements, that is, such elements u_v, that $L_v(\sqrt[\ell]{u_v})$ is an unramified extension of L_v of degree ℓ. We shall consider u_v as an element of the group $\overline{U}(L_v)/(\overline{U}(L_v))^\ell$. Thus, there are $\ell - 1$ primary elements, which together with the unity form a subgroup denoted by $\mathcal{P}_v$ of the group $\overline{U}(L_v)/\overline{U}(L_v)^\ell$. We put $\mathscr{B}[1] = \prod_{v \in S} \mathcal{P}_v$ and consider this group as a subgroup of $\mathscr{B}$. Obviously, $\mathscr{B}[1]$ is a Galois submodule in $\mathscr{B}(L)$.

The group $\widetilde{H}$ substitutes the components $\mathcal{P}_v$ of $\mathscr{B}[1]$, so, $\mathscr{B}[1] \cong \mathbb{F}_\ell[\widetilde{H}]$ as an $\widetilde{H}$-module.

Proposition 4.6. *We have an isomorphism of the Galois modules*

$$\mathscr{B}[1] \cong \mathscr{Q}(1).$$

Proof. Put $G_v^{\mathrm{un}} = G(L_v(\sqrt[\ell]{u_v})/L_v)$. Then by the local class field theory there is a canonical isomorphism $G_v^{\mathrm{un}} \cong L_v^\times/(L_v^\times)^\ell U(L_v)$. Thus, if D_S is the group of divisors of L with supports in S then $D := \prod_{v \in S} G_v^{\mathrm{un}} \cong D_S/D_S^\ell$. This defines a structure of Galois module on D. Since there is an epimorphism of Galois modules $D \to \mathbb{F}_\ell(0)$ induced by the norm map, we get that $D \cong \mathscr{B}[0]$, that is D starts with $\mathbb{F}_\ell(0)$ and ends with $\mathbb{F}_\ell(0)$. On the other hand, by Kummer theory there is a non-degenerate pairing between D and $\mathscr{B}[1]$, hence $\mathscr{B}[1]$ starts with $\mathbb{F}_\ell(1)$ and ends with $\mathbb{F}_\ell(1)$. This proves Proposition 4.6.

Proposition 4.7. *The Galois module $\mathscr{B}(L)$ has a decomposition into the direct sum*

$$\mathscr{B}(L) = \bigoplus_{i=0}^{I=\ell-2} \mathscr{B}[i], \tag{4.8}$$

where if $i \neq 1$ then $\mathscr{B}[i] = \mathcal{A}[i]$ and $\mathcal{A}[i]$ has the same meaning as in Proposition 4.5, and if $i = 1$ then $\mathscr{B}[1]$ has the same meaning as in Proposition 4.6.

Proof. Put

$$\mathscr{B}'(L) = \bigoplus_{i=0,\, i\neq 1}^{i=\ell-2} \mathscr{B}[i]. \tag{4.9}$$

To prove the formula (4.8) it is enough to check that in the group $\mathscr{B}(L)$ we have $C := \mathscr{B}'(L) \cap \mathscr{B}[1] = 0$. To do this, it is enough to check that $C^{\widetilde{H}} = 0$. Obviously, $C^{\widetilde{H}} = \mathscr{B}'(L)^{\widetilde{H}} \cap \mathscr{B}[1]^{\widetilde{H}}$, but we have $\mathscr{B}'(L)^{\widetilde{H}} \cong \bigoplus_{i=0,\, i\neq 1}^{\ell-2} \mathscr{B}[i]^{\widetilde{H}} \cong \bigoplus_{i=0,\, i\neq 1}^{i=\ell-2} \mathbb{F}_\ell(i)$, while $\mathscr{B}[1]^{\widetilde{H}} \cong \mathbb{F}_\ell(1)$. This proves the existence of the decomposition (4.8).

The main results of this section we can formulate as a following theorem.

Theorem 4.1. *For the field L, the Galois module $\mathcal{A}(L)/\mathcal{A}(L)^\ell$ contains in the split exact sequence of Galois modules*

$$0 \to M(L) \to \mathcal{A}(L)/\mathcal{A}(L)^\ell \to \mathscr{B}(L) \to 0, \tag{4.10}$$

where the structure of $M(L)$ is given in Proposition 4.4, and the structure of $\mathscr{B}(L)$ is given in Proposition 4.7.

This result may be presented in another form, taking into account that $M(L)$ and $\mathscr{B}[1]$ are defined canonically as submodules of $\mathcal{A}(L)/\mathcal{A}(L)^\ell$. Namely, there is a split exact sequence of Galois modules

$$0 \to \mathscr{B}[1] \oplus M(L) \to \mathcal{A}(L)/\mathcal{A}(L)^\ell \to \mathscr{B}'(L) \to 0, \tag{4.11}$$

where $\mathscr{B}'(L)$ was defined in the proof of Proposition 4.7.

§ 5. Certain ℓ-extensions of the field L

In this section we assume that the field $L = k(\sqrt[\ell]{b})$ defined as in (3.2) is fixed. In particular, we fix the pair of primes $p_1, p_2 \in \mathbb{P}_0$ such that $b = p_1^{s_1} p_2^{s_2}$. Let $p_3 \in \mathbb{P}_0$, where p_3 has the same meaning as in (3.1). Let $N = N(p_3)$ be the maximal Abelian ℓ-extension of L such that the Galois group $G(N/L)$ is of period ℓ, and only prime divisors of p_3 may ramify in the extension N/L. We wish to obtain the spectrum of all possible values of degree $[N : L]$. Note that we have always $[N : L] > 1$ since $N \supseteq K \cdot L$. To avoid plenty of indices, we shall denote p_3 by q in this section. By $(\mathfrak{q})$ we denote the principal divisor of q, which is a prime divisor in $\mathbb{Q}$ or in K.

Proposition 5.1. *If $q \neq p_1, p_2$ then $\mathfrak{q}$ splits completely in the extension L/k.*

Proof. If $\mathfrak{q}$ remains prime in L/k then $\mathfrak{q}$ remains prime in $L/\mathbb{Q}$. It means that $\widetilde{G} = G(L/\mathbb{Q})$ coincides with the decomposition subgroup of $\mathfrak{q}$. But $\mathfrak{q}$ does not ramify in $L/\mathbb{Q}$, hence its decomposition subgroup must be cyclic hence it cannot coincide with $\widetilde{G}$. This concludes the proof.

Let, as in the beginning of § 3 some section $f\colon \Delta \to \widetilde{G}$ is fixed. Since there are exactly ℓ subgroups of order $\ell - 1$ in $\widetilde{G}$ and all these subgroups are mutually conjugate, we may assume that the prime divisors $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ are enumerated in such a way that $f(\Delta)$ coincides with the decomposition subgroup of $\mathfrak{q}_1$.

Since the Galois group $G(N/L)$ is of period ℓ we can use the Kummer theory for description of N. Suppose that $L(\sqrt[\ell]{\alpha}) \subseteq N$. This means that all divisors prime to q enter α with exponents divisible by ℓ.

Let h be the class number of L, which is prime to ℓ by Proposition 3.1, and $\mathbf{h}$ is such number that $\mathbf{h} \equiv 0 \pmod{h}$ and $\mathbf{h} \equiv 1 \pmod{\ell}$. Then, putting $\alpha' = \alpha^{\mathbf{h}}$, we get $L(\sqrt[\ell]{\alpha}) = L(\sqrt[\ell]{\alpha'})$.

If α contains a prime divisor distinct from $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$, the divisor $\mathfrak{p}^{r_\mathfrak{p}}$, for example, then $r_\mathfrak{p} \equiv 0 \pmod{\ell}$ and (α') contains $\mathfrak{p}$ with exponent $r_\mathfrak{p}\mathbf{h}$. But the divisor $\mathfrak{p}^{\mathbf{h}}$ is principal, hence, multiplying α' by some ℓ-th power if necessary, we may assume that α' contains only the prime divisors $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$.

Thus, we have to characterize all the elements $\alpha' \in L$ such that (α') contains only prime divisors $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ while all the places $v \in S$ split or remain unramified in $L(\sqrt[\ell]{\alpha'})/L$.

Proposition 5.2. *Let $\alpha_1, \alpha_2 \in L$ be such elements that $L_1 := L(\sqrt[\ell]{\alpha_1}) \subseteq N$ and $L_2 := L(\sqrt[\ell]{\alpha_2}) \subseteq N$. Then the equality of the divisors $(\alpha_1) = (\alpha_2)$ yields that $L_1 = L_2$ and $\alpha_1 = \alpha_2 u^\ell$, where u is a unit of L.*

Proof. Put $u_1 = \alpha_1\alpha_2^{-1}$. Then u_1 is a unit of L and $L(\sqrt[\ell]{u_1}) \subseteq N$. The extension $L(\sqrt[\ell]{u_1})/L$ cannot have ramification out of S, but it cannot have ramification in S by definition of N. Therefore, the extension $L(\sqrt[\ell]{u_1})/L$ is unramified, but then it follows from Proposition 3.1 that $L(\sqrt[\ell]{u_1}) = L$, that is, $u_1 = u^\ell$ for some unit $u \in U(L)$. This proves Proposition 5.2.

Let $\beta_1 \in L^\times$ be such an element that $(\beta_1) = \mathfrak{q}_1^{\mathbf{h}}$. In this case the element $u := \beta^{1-\delta}$ is a unit. Since $H^{-1}(\Delta, U(L)[\ell]) = 0$ we get that there are units u_1 and u_2 such that $u = u_1^{1-\delta}u_2^\ell$. Then, putting $\beta = \beta_1 u^{-1}$, we obtain such an element β that

$$(\beta) = \mathfrak{q}_1^{\mathbf{h}} \text{ and } \beta^{1-\delta} = u_2^\ell \quad \text{for some } u_2 \in U(L)[\ell]. \tag{5.1}$$

Any divisor with support in $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ may be written (in additive notation) in the form $\eta(\beta)$ for some $\eta \in \mathbb{Z}_\ell[\widetilde{H}]$. The element $\eta\beta$ is a unit in the local field L_v for all $v \in S$, so, we can consider $\eta\beta$ as an element of $\mathcal{A}(L)$. By $\pi(\eta\beta)$ we denote the image of $\eta\beta$ in $\mathcal{A}(L)/\ell\mathcal{A}(L)$.

Using the exact sequence (4.11), we can transform $\pi(\eta\beta)$ into the element $\pi'(\eta\beta) \in \mathscr{B}'(L)$. Then it follows from (4.9) that $\pi'(\eta\beta) = \bigoplus_{i=0,\, i\neq 1}^{i=\ell-2} \pi_i(\eta\beta)$, where $\pi_i(\eta\beta) \in \mathscr{B}[i]$. Formula 4.5 and the definition of the component $\mathscr{B}[i]$ yield that

$$\bigoplus_{i=1}^{(\ell-3)/2} \mathscr{B}[2i] \cong \overline{U}_2(L)/\ell\overline{U}_2(L),$$

so, after multiplying β by some suitable unit in the group $\overline{U}_2(L)$, we may assume and we shall assume in further that $\pi_i(\beta) = 0$ for $i = 2, 4, \dots, \ell - 3$. Then the same property have the elements $\pi(\eta\beta)$ for any η and $i = 2, 4, \dots, \ell - 3$.

So, we can assume that some element $\beta \in L^{\times}$ is chosen such that $\pi(\beta)^{\delta} = \pi(\beta)$, moreover, $\pi_i(\beta) = 0$ for $i = 2, 4, \dots, \ell - 3$. We shall consider a system $\eta_1, \dots, \eta_{\ell^{\ell}} \in \mathbb{Z}_{\ell}[\widetilde{H}]$ that presents all the elements of $\mathbb{F}_{\ell}[\widetilde{H}]$, and we have to determine all η_j such that $L(\sqrt[\ell]{\eta_j\beta}\,) \subseteq N$. The elements $\eta_j\beta$ must satisfy the following condition

$$\pi_i(\eta_j\beta) = 0 \text{ for } i = 2, \dots, \ell - 2 \quad \text{and} \quad \pi_M(\eta_j\beta) = 0, \tag{5.2}$$

where the projection $\pi_M \colon \mathcal{A}(L)/\ell\mathcal{A}(L) \to M(L)$ is defined by the split exact sequence (4.10). Herein we can assume that the conditions (5.2) hold already for even $i > 0$. The conditions that appear in the case $i = 0$, we shall discuss below (see Proposition 5.3).

Obviously, the images of those representatives of $\eta_1, \dots, \eta_{\ell^{\ell}}$ that satisfy the condition (5.2) form an ideal I of $\mathbb{F}_{\ell}[\widetilde{H}]$, and $I = I(q)$ is of the form $I = I_{\max}^{i}$, where $I_{\max}$ is the maximal ideal of $\mathbb{F}_{\ell}[\widetilde{H}]$.

Proposition 5.3. *For any q we have $I \neq 0$.*

Proof. Indeed, there is always the extension KL/L, that corresponds to $\eta = \sum_{h \in \widetilde{H}} h$, hence I always contains the ideal $\mathbb{F}_{\ell}(\sum_{h \in \widetilde{H}} h)$.

Proposition 5.4. *For the field L we have always a strict inclusion $I \subset \mathbb{F}_{\ell}[\widetilde{H}]$.*

Proof. We suppose that (q) remains prime in the extension k_{∞}/k. This means that the Artin symbol of divisor (q) is a generator of $\Gamma = G(k_{\infty}/k)$. The map of restriction of automorphisms from L_{∞} to k_{∞} maps isomorphically $\Gamma_1 := G(L_{\infty}/L)$ onto Γ. This map agree with the norm map $N_{L/k}$, which sends $\mathfrak{q}_1$ into (q). It means that for any $\beta \in L^{\times}$ such that $(\beta) = \mathfrak{q}_1^{\mathbf{h}}$, there is a place $v \in S$ of L such that the inclusion $v \colon L \hookrightarrow L_v$ sends the element β into a generator of Γ_v, where Γ_v is of the same meaning as in (3.10). It is known by local class field theory that the extension $L(\sqrt[\ell]{\beta}\,)/L$ is ramified for such β, hence, for example, $1 \notin I$. This proves Proposition 5.4.

Remark. Consider an element $\eta\beta$ such that $\eta \in I_{\max}$. Then $\pi_0(\eta\beta)$ belongs to $\pi_0(P(L))$, where $P(L)$ has the same meaning as in (3.10). This means that, multiplying β by some unit in $P(L)$, we always may assume that $\pi_0(\eta\beta) = 0$ (under assumption that $\eta \in I_{\max}$).

Now we consider the restrictions that yields the equality $\pi_i(\eta\beta) = 0$ for some odd $i = 3, 5, \dots, \ell - 2$. Remind that we use additive notation for multiplication. The lower central series of the Galois module $\mathscr{B}[i]$ starts with $\mathbb{F}_{\ell}(i)$. Meanwhile, the element β is fixed under the action of Δ. If $\pi_i(\beta) = 0$, then there appear no obstructions connected with the projection π_i. If $\pi_i(\beta) \neq 0$ then, applying Lemma 3.2 of [1] in this case, we obtain that π_i sends β into a generator of $\mathscr{B}[i]^{(\widetilde{\sigma}-1)^{\ell-1-i}}$ (Δ acts identically on β and the module $\mathscr{B}[i]^{(\widetilde{\sigma}-1)^{\ell-1-i}}$ starts with $\mathbb{F}_{\ell}(0)$). Then the element $\pi_i(\beta)$ generates in $\mathscr{B}[i]$ a submodule of order ℓ^{i+1}. Thus, in this case we have $\pi_i(\eta\beta) = 0$ if and only if $\eta \in I_{\max}^{i+1}$.

We have to consider two particular cases else: the behavior of $\pi_1(\beta)$ and the behavior of the element $\pi_M(\beta)$. In the case $i = 1$ we, repeating all preceding considerations, obtain that $\pi_1(\beta)$ generates a submodule of order ℓ^2 in $\mathscr{B}[1]$. But since I is a proper ideal, we have either $\pi_1(\eta\beta) = 0$, which corresponds to the

extension $L(\sqrt[\ell]{\eta\beta})/L$, where all places over ℓ completely split, or $\pi_1(\eta\beta) \neq 0$, and this corresponds to the case when all places over ℓ of the field L remain unramified in the extension $L(\sqrt[\ell]{\eta\beta})/L$.

At last, let us consider $\pi_M(\beta)$. Since M starts by $\mathbb{F}_\ell(1)$ and ends by $\mathbb{F}_\ell(1)$, we obtain, as in the case $i = 1$, that $\pi_M(\eta\beta) \in M^{\widetilde{H}} = \mu_\ell(L)$, hence, after multiplying the element $\eta\beta$ by a suitable root of unity in $\mu_\ell(L)$, we can assume that $\pi_M(\eta\beta) = 0$.

We can formulate the results of our study in the form of the following theorem.

Theorem 5.1. *Let $X := 3, 5, \ldots, \ell - 2$ and X_1 be the subset of those $i \in X$, for which $\pi_i(\beta) \neq 0$. Let i_0 be the maximal index in X_1. Then*

$$I(q) = I_{\max}^{i_0+1}. \tag{5.3}$$

If X_1 is empty then $I(q) = I_{\max}$. Here either all places over ℓ split completely in N/L, or each of them has inertia degree ℓ.

Proof. Any odd index $i > 1$, that is, any $i \in X_1$ must satisfy the condition $I(q) \subseteq I_{\max}^{i+1}$, whence it follows (5.3). If X_1 is empty then any element $\eta\beta$ is admissible, that is $I(q) = I_{\max}$. If $\pi_1(\eta\beta) = 0$ for any η then all places over ℓ split in the extension N/L. Otherwise, all places over ℓ have non-unit inertia degree, which, as man can check easily is equal to ℓ. This proves Theorem 5.1.

Corollary 5.1. *We have always $[N : L] = \ell^{r(q)}$ with even $r(q)$.*

Indeed, $|(I(q))|$ is the order of the Kummer group of the extension N/L, which coincides with $I(q)$. The index i_0 is odd by definition, $|(I_{\max})| = \ell^{\ell-1}$, so it follows from (5.3) that $|I(q)|$ is an even power of ℓ. Then the degree $[N : L]$ is equal to $\ell^{r(q)}$, where $r(q) = \ell - i_0 - 2$ is even. In the case $\ell = 3$ the set X_1 is empty, therefore, $[N : L] = 9$, and all the places over ℓ either split completely (if $\pi_1(\beta) = 0$), or have inertia degree 3 (if $\pi_1(\beta) \neq 0$).

Till now we studied how the properties of the field $N(q)$, in particular, its degree over L depend on q. Now we shall treat the inverse problem: to prove the existence of prime q such that the field $N(q)$ has a given properties. Namely, the following theorem holds.

Theorem 5.2. *Assume that for the set of indices $i = 1, 2, \ldots, \ell - 2$ a collection of elements $\alpha_i \in \mathscr{B}[i]$ is given such that α_i are fixed under the action of $f(\Delta)$. Then there are infinitely many prime divisors (q) of $\mathbb{Q}$ such that (q) remains prime in k_∞, (q) splits completely in L/k and (q) has the following additional property: Let $\mathfrak{q}_1$ be a prime divisor of (q) in L fixed by the action of $f(\Delta)$. Then there is $\beta = \beta(\mathfrak{q}_1)$ such that the principal divisor of β is equal to $\mathfrak{q}_1$, and the following properties hold:*

1) $\pi_0(\beta(\mathfrak{q}_1)) \notin P(L)/\ell P(L)$;
2) $\pi_i(\beta(\mathfrak{q}_1)) = \alpha_i$ *for* $i = 1, 2, \ldots, \ell - 2$.

Proof. Consider the finite Galois module $\mathscr{B}(L) = \mathcal{A}/\ell\mathcal{A}$. Let $\widetilde{U}(L)$ be an image of $U(L)/\ell U(L)$ in the group $\mathscr{B}(L)$. As it was shown in Propositions 4.5 and 4.6, in $\widetilde{U}(L)$ there is a subgroup $U_2(L)/\ell U_2(L)$ and there is a subgroup $P(L)/\ell P(L)$ that contains in the component $\mathscr{B}_0$.

According to the global class field theory, man can interpret the group $R(L) := \mathscr{B}(L)/\widetilde{U}(L)$ as a Galois group of some Abelian extension $F_1(L)/L$. Put $F(L) = F_1(L)^{M(L)}$. Then the element $\varphi := \prod_{i=1}^{\ell-2} \alpha_i^{-1}$ may be considered as an element of the group $R(L)$, that is, as an automorphism φ of $F(L)/L$. By the Chebotarev density theorem there are infinitely many prime divisors $\mathfrak{q}_1'$ of L such that φ coincides with Frobenius automorphism that corresponds to $\mathfrak{q}_1'$.

The divisor $\mathfrak{q}_1'$, that we have constructed, has the desired projections α_i^{-1}, but we have to check if the divisor (q) under $\mathfrak{q}_1$ remains prime in k_∞? This condition is equivalent to the claim that (q) remains prime simultaneously in the extension $\mathbb{Q}_\infty/\mathbb{Q}$ and in $k/\mathbb{Q}$. The fact that (q') remains prime in $\mathbb{Q}_\infty/\mathbb{Q}$ follows from the fact that $\pi_0(\beta(q_1'))$ does not contain in the group $P(L)/\ell P(L) \subset \mathscr{B}[0]$. We have already discussed this situation in detail during the proof of Proposition 5.4.

Consider a tower of fields $F(L) \supset L \supset \mathbb{Q}$. The group $G(L/\mathbb{Q})$ contains the subgroup $f(\Delta)$, which fixes the divisor $\mathfrak{q}_1'$. Since $G(L/\mathbb{Q})$ acts on $F(L)$ by conjugation, we obtain that $\varphi \in G(F(L)/L)$ commutes with the generator $\widetilde{\delta}$ of $f(\Delta)$. Then the product of these two commuting elements φ and $\widetilde{\delta}$ generates in $G(F(L)/\mathbb{Q})$ a cyclic subgroup C of order $\ell(\ell-1)$. By the Chebotarev density theorem for any $\mathfrak{q}_1'$ there are infinitely many prime divisors $\mathfrak{Q}_1$ of $F(L)$ such that the decomposition subgroup of $\mathfrak{Q}_1$ coincides with C. Let φ_1 be a Frobenius automorphism in $G(F(L)/\mathbb{Q})$ that corresponds to $\mathfrak{Q}_1$. Without restricting the generality, we can assume that $\varphi_1^{\ell-1} = \varphi$. The divisor $\mathfrak{Q}_1$ remains prime in the extension $F(L)/F(L)^{\varphi}$, that is, $\mathfrak{Q}_1$ is a prime divisor of the field $F(L)^{\varphi}$. Let $\mathfrak{q}_1$ be a prime divisor of L under $\mathfrak{Q}_1$. Then $N(\mathfrak{Q}_1) = \mathfrak{q}_1$, where N is the norm in the extension $F(L)^{\varphi}/L$. So, for the element $\beta_1 = \beta_1(\mathfrak{q}_1)$ such that the principal divisor (β_1) is equal to $\mathfrak{q}_1$, we obtain that the projections $\pi_i(\beta^{\ell-1})$ are equal to α_i, that is, $\mathfrak{q}_1^{\ell-1}$ is a suitable divisor. This proves Theorem 5.2.

Corollary 5.2. *For any pair of distinct prime numbers $p_1, p_2 \in \mathbb{P}_0$ there are infinitely many primes $p_3 = q \in \mathbb{P}_0$ such that $[N : L] = \ell^i$ for any even i, where $2 \leqslant i \leqslant \ell - 1$.*

Corollary 5.3. *For any pair of distinct prime numbers $p_1, p_2 \in \mathbb{P}_0$ there are infinitely many primes $p_3 = q \in \mathbb{P}_0$ such that $[N : L] = \ell^{\ell-1}$, and all the places over ℓ split completely in the extension N/L, and infinitely many primes $p_3 = q \in \mathbb{P}_0$ such that all the places over ℓ have inertia degree ℓ in the extension N/L.*

§ 6. Application to arithmetic of K

Proposition 6.1. *Assume that $\ell > 3$, $p_3 = q$ and $N = N(q)$ has the same meaning as in § 5. Then the following three conditions are equivalent*:

(i) $d(\mathrm{Cl}_S(K)_\ell) \geqslant 2$;
(ii) $d(\mathrm{Cl}_S(LK)_\ell) \geqslant 1$;
(iii) $d(G(N/L)) \geqslant 2$.

Proof. (i) $\Rightarrow$ (ii). Let $d(\mathrm{Cl}_S(K)_\ell) \geqslant 2$. This means that there is an unramified extension N_1/K of K, with the Galois group $(\mathbb{Z}/\ell\mathbb{Z})^2$ such that all places over ℓ split completely in this extension. Then N_1L/LK is an unramified Abelian ℓ-extension, and all places over ℓ split in it, that is, $d(\mathrm{Cl}_S(LK)_\ell) \geqslant 1$.

(ii) $\Rightarrow$ (iii). Let N_2 be the maximal Abelian unramified ℓ-extension of LK, in which all places over ℓ completely split. Then the Galois group $G(KL/L) \cong \mathbb{Z}/\ell\mathbb{Z}$ acts by conjugation on the Abelian ℓ-group $G(N_2/KL)$. Hence there is a non-trivial factorgroup $C = G(N_2/KL)/B$ with identical action of $G(KL/L)$. Put $N_3 = N_2^B$. Then the Galois group $G(N_3/KL)$ contains in the exact sequence

$$1 \to C \to G(N_3/L) \to G(KL/L) \to 1, \tag{6.1}$$

whence it follows that $G(N_3/L)$ is an Abelian ℓ-group of order at least ℓ^2. Only the places $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ over q may be ramified in the extension N_3/L, and $G(N_3/L)$ is generated by the inertia subgroups of these place. Each of these subgroups is of order ℓ or 1. Therefore, $N_3 \subseteq N$ and $G(N_3/L)$ is of period ℓ, so $d(G(N/L)) \geqslant d(G(N_3/L)) \geqslant 2$.

(iii) $\Rightarrow$ (i). Since $K \subseteq N$ the condition $d(G(N/L)) \geqslant 2$ yields $[N : KL] \geqslant \ell$. Thus, $[N : K] \geqslant \ell^2$. Let N_4 be the maximal Abelian unramified extension of KL, such that all the places over ℓ split completely in it. Then, using the same method, that we have used above to construct the field N_3, and an analogue of the exact sequence (6.1), which in the present case has the form

$$1 \to C' \to G(N_5/K) \to G(KL/K) \to 1,$$

where C' is the maximal factorgroup of $G(N_4/KL)$ with trivial action of $G(KL/K)$, we obtain an Abelian unramified ℓ-extension N_5/K of degree $\geqslant \ell^2$ such that all places over ℓ split completely in it. By Theorem 4.1 of [1] the H-module $G(N_5/K)$ is cyclic. So, by Theorem 3.1 of [1], if the period of $\mathrm{Cl}_S(K)_\ell$ is greater ℓ, then $d(\mathrm{Cl}_S(K)_\ell) \geqslant \ell - 1$. So, the condition $[N_5 : K] \geqslant \ell^2$ yields $d(\mathrm{CL}_S(K)_\ell) \geqslant 2$. This proves Proposition 6.1.

The following theorem 6.1 is an immediate consequence of Corollary 5.2 and Proposition 6.1.

Theorem 6.1. *Assume that $\ell > 3$ and K is of the form (3.1). In this case we have always $d(\mathrm{Cl}_S(K)_\ell) \geqslant 2$.*

In the case $\ell = 3$ we need the following variant of Proposition 6.1.

Proposition 6.2. *Under conditions of Proposition 6.1 assume that $\ell = 3$. Let N_6 be the maximal Abelian ℓ-extension of L unramified out of the prime divisors $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\mathfrak{q}_3$, over $(q) = (p_3)$ and such that $G(N_6/L)$ is of period ℓ. We assume additionally that all the places over ℓ, must be unramified, but we do not assume that they split completely in N_6/L. Then the following three conditions are equivalent*:

(i) $d(\mathrm{Cl}(K)_\ell) \geqslant 2$;
(ii) $d(\mathrm{Cl}(KL)_\ell) \geqslant 1$;
(iii) $d(G(N_6/L)) \geqslant 2$.

Proof of this Proposition is completely equivalent to that of Proposition 6.1.

The next theorem is an immediate consequence of Corollary 5.2, Theorem 6.1 and Proposition 6.2.

Theorem 6.2. *Let $\ell = 3$ and K be of the form (3.1). Then for any pair $p_1, p_2 \in \mathbb{P}_0$ there are infinitely many $p_3 \in \mathbb{P}_0$ such that $d(\mathrm{Cl}_S(K)_\ell) = 1$ and infinitely many p_3 such that $d(\mathrm{Cl}_S(K)_\ell) > 1$.*

Bibliography

[1] L. V. Kuz'min, "Arithmetic of certain ℓ-extensions ramified at three places", *Algebra, number theory, and algebraic geometry*, Collected papers. Dedicated to the memory of Academician Igor Rostislavovich Shafarevich, Trudy Mat. Inst. Steklova, vol. 307, Steklov Mathematical Institute of RAS, Moscow 2019, pp. 78–99; English transl., *Proc. Steklov Inst. Math.* **307** (2019), 65–84.

[2] L. V. Kuz'min, "Arithmetic of certain ℓ-extensions ramified at three places. II", *Izv. Ross. Akad. Nauk Ser. Mat.* **85**:5 (2021), 132–151; English transl., *Izv. Math.* **85**:5 (2021), 953–971.

[3] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, NJ 1956; Russian transl., Inostr. Lit., Moscow 1960.

Leonid V. Kuz'min
National Research Centre
"Kurchatov Institute", Moscow, Russia
E-mail: lvkuzmin@mail.ru

Received 9/JUL/21
5/JAN/22
Translated by THE AUTHOR