V. I. Yanchevskiĭ, Henselian division algebras and reduced unitary Whitehead groups for outer forms of anisotropic algebraic groups of the type A_n, *Sbornik: Mathematics*, 2022, Volume 213, Issue 8, 1096–1156

DOI: 10.4213/sm9660e

DOI: https://doi.org/10.4213/sm9660e

Henselian division algebras and reduced unitary Whitehead groups for outer forms of anisotropic algebraic groups of the type A_n

V. I. Yanchevskiĭ

Abstract. Some results on the structure of involutorial (that is, having an involution) Henselian tamely ramified division algebras are obtained. These results are then used to derive formulae for the computation of the reduced unitary Whitehead groups for outer forms of anisotropic algebraic groups of type A_n.

Bibliography: 46 titles.

Keywords: weakly ramified Henselian division algebras, unitary involutions, reduced Whitehead groups of anisotropic algebraic groups.

§ 1. Introduction and statements of the main results

Let K be an (infinite, for simplicity) field. Among the first important examples of infinite projectively simple (that is, containing no noncentral simple subgroups) groups provided by a linear algebra are the special linear groups $\mathrm{SL}_n(K)$, $n > 1$ (more generally, the special linear groups $\mathrm{SL}_n^+(D)$ over division rings; see [1] and [2]). These groups arise as the kernels of the determinant homomorphism of the general linear group $\mathrm{GL}_n(K)$, the group of nondegenerate K-linear automorphisms of the n-dimensional K-vector space $V_n(K)$. They can also be defined as the derived subgroups $\mathrm{GL}_n(K)'$ of the groups $\mathrm{GL}_n(K)$ (in what follows, for an arbitrary group G we denote by G' the derived subgroup of G). Other examples of this kind can be obtained with the use of classical linear groups. For example, suppose that $\operatorname{char} K \neq 2$ and the space $V_n(K)$ is equipped with a nondegenerate skew-symmetric bilinear form $f\colon V_n(K)\times V_n(K) \to K$ (which means that $f(v,w) = -f(w,v)$ for any pair $v, w \in V_n(K)$). Let $\mathrm{Sp}_n(K)$ be the symplectic group of the form f (see [1]–[3]):

$$\mathrm{Sp}_n(K) = \bigl\{s \in \mathrm{GL}_n(K) \mid f(s(v), s(w)) = f(v,w) \text{ for any pair } v, w \in V_n(K)\bigr\}.$$

Then $\mathrm{Sp}_n(K)$ is again a projectively simple group (see [1], Theorem 5.2). Note that $\mathrm{Sp}_n(K) = \mathrm{Sp}_n(K)'$ (this follows from [1], Theorem 5.1).

Leaving aside other examples of infinite projectively simple groups related to classical groups, we note that the range of such examples was significantly extended

This work was supported by the National Academy of Sciences of Belarus under the State Program of Scientific Research “Convergence-2025” (assignment no. 1.1.01) and by the Belarusian Republican Foundation for Fundamental Research (grant no. Φ21-054).

AMS 2020 *Mathematics Subject Classification.* Primary 16K20; Secondary 19B99.

by passing to semisimple linear algebraic groups, which gave rise to a number of interesting conjectures and results (particularly, in the arithmetic theory of algebraic groups). This approach has allowed distinguishing the general properties that characterize the phenomenon of projective simplicity. The definitions of all notions used in this paper (such as simple connectedness, simplicity, isotropy, parabolic subgroup and others) can easily be found in [4]–[7].

Let G be a simple linear algebraic group defined over a field K, which is not assumed to be algebraically closed, and G_K be the group of K-rational points of G. Consider in turn the cases when G is isotropic over K and when G is anisotropic. Recall that the group G is anisotropic if it has no proper parabolic subgroups defined over K. Here, a parabolic subgroup is a subgroup that contains some Borel subgroup. Denote by G_K^+ the normal subgroup of G_K generated by the rational (over K) elements of the unipotent radicals of K-defined parabolic subgroups. In this situation Tits established in 1964 the following important fact.

Theorem 1 (see [8]). *Suppose that K contains at least four elements. Then any subgroup of G_K normalized by the group G_K^+ is either central in G or contains G_K^+. In particular, G_K^+ is projectively simple.*

Thus, there arises a new class of projectively simple groups. It is natural to think of the structure of the group G_K as known if $G_K = G_K^+$. By the time Theorem 1 was proved this equality had already been known to hold for some special groups G and many fields K, so the following conjecture looked quite reasonable.

Conjecture (Kneser-Tits). For a K-simple simply connected group G that is isotropic over the field K, the equality $G_K^+ = G_K$ holds.

The Kneser-Tits conjecture is obviously true in the case when the field K is algebraically closed. Note also that É. Cartan proved this conjecture in the case when $K = \mathbb{R}$ and G is a simple, simply connected algebraic group. For a long time it was generally believed that the Kneser-Tits conjecture is true, since it was confirmed in a number of special cases. However, Platonov [9] showed in 1975 that this conjecture is false in general. As a result, Tits introduced the Whitehead groups $W(K,G) = G_K/G_K^+$ of reductive algebraic K-groups (further advances in this subject are presented in [10] and [11]).

As before, let G be a simply connected K-simple algebraic group. Then G belongs to one of the following classes: A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4 and G_2. Among the groups of these types the most interesting ones (and hardly amenable to investigation) are groups of type A_n. In particular, the groups G_K of K-rational points of simply connected groups of this type are exhausted by the following list (see [7], § 2.3, Propositions 17 and 18).

1) Inner forms: $\mathrm{SL}_m(D) = \{a \in M_m(D)\colon \mathrm{Nrd}_{M_m(D)}(a) = 1\}$, where $M_m(D)$ is the algebra of $m \times m$ K-matrices whose entries belong to the central division K-algebra D of index d and $\mathrm{Nrd}_{M_m(D)}\colon M_m(D) \to K$ is the reduced norm mapping and $n = md - 1$.

2) Outer forms: $\mathrm{SU}_m(D,f) = \{u \in U_m(D,f)\colon \mathrm{Nrd}_{M_m(D)}(u) = 1\}$, where D is a division algebra of index d endowed with a unitary involution τ (that is, with a nontrivial restriction to the centre of D). Here K coincides with the field

of τ-invariant elements of the centre of D, f is a nondegenerate m-dimensional Hermitian form, $U_m(D,f)$ is the unitary group of the form f and $n = md - 1$.

If the group G is an inner form of type A_n and it is K-isotropic, then it follows from the condition of K-isotropy that $m \geqslant 2$. Consider the subgroup $\mathrm{SL}_m^+(D)$ of the group $G_K = \mathrm{SL}_m(D)$ which is generated by the transvections, that is, by those matrices that, in a suitable basis of the space $V_n(K)$, have the form of an elementary matrix (see [1]). Since each elementary matrix is unipotent (and, moreover, lies in the unipotent radical of a suitable parabolic subgroup), $\mathrm{SL}_m^+(D)$ is contained in G_K^+. Moreover, the group $\mathrm{SL}_m^+(D)$ is a normal subgroup of $\mathrm{GL}_m(D)$, and therefore $G_K^+ = \mathrm{SL}_m^+(D)$ by Theorem 1. Hence the group G_K/G_K^+ is isomorphic to $\mathrm{SL}_m(D)/\mathrm{SL}_m^+(D)$. Now with the use of the Dieudonné determinant (see [1] and [2]) we conclude that the group $\mathrm{SL}_m(D)/\mathrm{SL}_m^+(D)$ is isomorphic to the reduced Whitehead group $\mathrm{SK}_1(D) = \mathrm{SL}_1(D)/D^{*\prime}$ of the algebra D. If G is an outer form of type A_n, then $G = \mathrm{SU}_m(D,f)$ for an appropriate nondegenerate m-dimensional Hermitian form over D with involution τ, whose restriction to the centre of D is nontrivial, and K coincides with the subfield of τ-invariant elements of the centre of D. The condition that G is K-isotropic means that the form f is isotropic, and in this case the group G_K^+ coincides with the subgroup $\mathrm{TU}_m(f)$ generated by the unitary transvections (see [2]); moreover, in almost all cases it coincides with the derived subgroup of the group $U_m(D,f)$. Now with the use of the Wall norm (see [2]) we obtain an isomorphism of the quotient group $\mathrm{SU}_m(D,f)/\mathrm{TU}_m(f)$ onto the reduced unitary Whitehead group $\mathrm{SUK}_1(D) = \Sigma'/\Sigma$, where Σ is the subgroup of D^* generated by the τ-invariant elements and Σ' consists of elements with τ-invariant reduced norms. This group is called the reduced unitary Whitehead group for the algebra D. In fact, it depends only on the restriction $\tau|_K$. Details can be found in [12].

There is a significant number of publications devoted to the computation of these groups (see [9], [10] and [12]–[29]).

Note that the inner forms of anisotropic groups of type A_n are related to the groups $\mathrm{SK}_1(D)$. As for outer forms of anisotropic groups, these are always unitary groups related to the anisotropic forms f. In this situation it is most important to consider first of all the groups $\mathrm{SU}_1(D,f)/U_1(D,f)'$. Although the first works on this subject date back to the early 2000s, such groups remains hardly tractable for investigation, and only a few basic results concerning these groups are known so far. Since such groups play the key role in this work, the following definition is quite important.

Definition 1. The group

$$\mathrm{SUK}_1^{\mathrm{an}}(D,\tau) = \mathrm{SU}_1(D,f)/U_1(D,f)'$$

is called the *special unitary Whitehead group of the anisotropic form* f (by analogy with the reduced isotropic Whitehead groups $\mathrm{SK}_1(D)$ and $\mathrm{SK}_1(D,\tau)$).

1. For quaternion division algebras possessing unitary involutions Sury [30] derived explicit formulae for the computation of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$.

2. In [31] Sethuraman and Sury proved that for the special symbol algebras D the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ is infinite.

3. In [32] this author showed that there exists an epimorphism of the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ onto $\mathrm{SUK}_1(D,\tau)$, which made it possible to solve the problem of nontriviality of the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ in the general case under the condition that the groups $\mathrm{SUK}_1(D,\tau)$ are nontrivial. Moreover, this relation shows that the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ is infinite, provided that the groups $\mathrm{SUK}_1(D,\tau)$ are too.

No significant results on the problem of the projective simplicity of outer forms of anisotropic groups of type A_n have been obtained to date; therefore, the computation of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ can be considered as an important step in gathering information for further studies on this problem.

Note that the first fundamental results related to the computation of nontrivial reduced Whitehead groups were obtained in the framework of the class of Henselian division algebras and were based on the idea of reducing the problem of the computation of these groups to determining certain special subgroups of the multiplicative groups of their residue algebras.

The structure of finite-dimensional general Henselian algebras was first described by Platonov and Yanchevskiĭ in [33]–[35]. A complete and extended proof of their results can be found in [36].

The purpose of this work is to derive formulae for the computation of reduced anisotropic unitary Whitehead groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ for Henselian algebras D using the idea of reduction mentioned above. The paper consists of two parts. In the first we establish a number of results on the structure of Henselian involutive division algebras. Some of these results can be formulated in terms of graded algebras (see [23]). However, we prefer remaining within the framework of Henselian situation, hence it seems appropriate to use the Henselian language here. In the second part we use the results obtained to describe the reduced anisotropic unitary Whitehead groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ for Henselian algebras D.

To formulate our results we need the following definitions.

In what follows $Z(R)$ denotes the centre of the ring R and $C_R(S)$ is the centralizer of the subring S of R. If $S\subseteq Z(R)$, then R is called an S-algebra. It is assumed that all rings have identity elements and that $1_S=1_R$ if S is a subring of R. Moreover, homomorphisms map the identity elements to each other. The kernel of a homomorphism f is denoted by $\mathrm{Ker}(f)$. By R^* we denote the multiplicative subgroup of the ring R. If $a\in R^*$, then we denote by i_a the inner automorphism of the ring R defined by the formula $r^{i_a}=a^{-1}ra$ for any $r\in R$. Occasionally, for the convenience of references i_a will mean the automorphism defined by the formula $r^{i_a}=ara^{-1}$ for $r\in R$ (however, it is always clear from the context which particular interpretation is meant). For a subalgebra E of a division algebra D we denote the dimension of D as a left vector space over E by $[D:E]$. All algebras below are assumed to be finite-dimensional.

Given a field K and a finite-dimensional central simple K-algebra A, we denote the class of A in the Brauer group $\mathrm{Br}(K)$ by $[A]$. By Wedderburn's theorem $A\cong M_n(D)$ for a K-central division algebra D, where $M_n(D)$ is the algebra of $n\times n$ matrices over D. The division algebra D is uniquely determined up to K-isomorphism and is called the underlying division algebra of A. Given K-algebras A and B, we write $A\sim B$ if their underlying algebras are K-isomorphic to each other. By definition the index $\operatorname{ind} A$ of the algebra A coincides with $\sqrt{[D:K]}$, the degree $\deg A$ is $n\cdot\operatorname{ind} A$, and the exponent $\exp A$ of the algebra A is the order of $[A]$

in $\mathrm{Br}(K)$. Moreover, we set

$$\mathcal{D}(K) = \{D\colon D \text{ is a central division } K\text{-algebra and } [D:K] < \infty\}.$$

For any field extension F/K and any $D \in \mathcal{D}(K)$ we denote the underlying algebra of the F-algebra $D \otimes_K F$ by $D_F \in \mathcal{D}(F)$. It is known that if $K \subset F \subset D$, then $D_F \cong C_D(F)$. Denote by $\mathrm{Br}(F/K)$ the kernel of the homomorphism of extension of scalars $\mathrm{Br}(F) \to \mathrm{Br}(K)$.

For any subextension L/K of the algebra $D \in \mathcal{D}(K)$ the following formula is valid: $\operatorname{ind} D = \operatorname{ind} C_D(L)[L:K]^2$.

Definition 2. A *unitary involution* of the algebra $D \in \mathcal{D}(K)$ is an antiautomorphism τ of D of order two that has a nontrivial restriction to K. For the field $k = \{a \in K \mid a^\tau = a\}$ K is a quadratic Galois extension. In this case τ is called a K/k-involution and the set of K/k-involutions of the algebra D is denoted by $\mathrm{Inv}_{K/k}(D)$.

Assume that the algebra D has a unitary involution τ and $k = \{a \in K \mid a^\tau = a\}$. In this case we write $\tau \in \mathrm{Inv}_{K/k}(D)$. Let $\mathrm{Nrd}_D\colon D \to K$ denote the reduced norm mapping of D. The unitary group $U(D,\tau)$ of the algebra D (with respect to τ) is $U(D,\tau) = \{d \in D^* \mid d^\tau d = 1\}$, and the special unitary group $\mathrm{SU}(D,\tau)$ is its subgroup $U(D,\tau) \cap \mathrm{SL}(D)$, where $\mathrm{SL}(D) := \mathrm{SL}_1(D)$. Moreover, given a finite field extension L/K, we denote the group $\{l \in L^* \mid N_{L/K}(l) = 1\}$ by $\mathrm{SL}(L/K)$. If, in addition, the extension L/K has an automorphism τ of order two such that $K^\tau = K$, then we denote the subgroup $\{l \in L^* \mid l^\tau l = 1\}$ by $U(L,\tau)$ and the subgroup $U(L,\tau) \cap \mathrm{SL}(L/K)$ by $\mathrm{SU}(L,\tau)$.

We also need some background on division algebras with valuations. Let $D \in \mathcal{D}(K)$. A *valuation* v of D is a function $v\colon D^* \to \Gamma$ (here Γ is a totally ordered Abelian group in additive notation) with the following properties: for all $a, b \in D^*$

(i) $v(ab) = v(a) + v(b)$;

(ii) $v(a+b) \geqslant \min(v(a), v(b))$ if $b \neq -a$.

Given a valuation v of D, one can define

- the valuation ring $V_D = \{d \in D^* \mid v(d) \geqslant 0\} \cup \{0\}$;
- the valuation ideal $M_D = \{d \in D^* \mid v(d) > 0\} \cup \{0\}$ (the unique two-sided maximal ideal of the ring V_D);
- the group of v-units $U_D = V_D \setminus M_D = V_D^*$ and its subgroup $1 + M_D = \{1 + m \mid m \in M_D\}$;
- the V_K/M_K-algebra $\overline{D} = V_D/M_D$ of the valuation v, and the group of values $\Gamma_D = v(D^*)$.

More generally, given an arbitrary subset $S \subset V_D$, we denote by $\overline{S}$ the set of images of the elements of S under the canonical homomorphism (reduction or residue homomorphism) from V_D to $\overline{D}$.

Since $V_D^\tau = V_D$ and $M_D^\tau = M_D$, along with the involution τ we can define its reduction $\overline{\tau}\colon \overline{D} \to \overline{D}$; here we have $(d + M_D)^{\overline{\tau}} = d^\tau + M_D$ for any $d \in V_D$.

If E is a K-subalgebra of the K-algebra D with a valuation (D, v), then the restriction $v|_E$ of the valuation v to E^* is a valuation of E. In this case the ramification index of the algebra D over E is defined as the index $|\Gamma_D : \Gamma_E|$ of the subgroup Γ_E in Γ_D.

For $d \in D^*$ the inner automorphism i_d maps V_D to V_D and M_D to M_D. Therefore, i_d induces a $\overline{K}$-automorphism $\overline{D}$. When restricted to $Z(\overline{D})$, it reduces to a $\overline{K}$-automorphism denoted below by $\overline{i_d}$. Finally, the mapping $d \mapsto \overline{i_d}$ defines a homomorphism $\alpha \colon D^* \to \mathrm{Gal}(Z(\overline{D})/\overline{K})$. For $u \in U_D$ the automorphism $\overline{i_u}$ acts as the conjugation by $\overline{u}$, so that $u \in \mathrm{Ker}(\alpha)$. Moreover, $K^* \subseteq \mathrm{Ker}(\alpha)$. Since $D^*/U_D K^* \cong \Gamma_D/\Gamma_K$, the mapping α induces a well-defined homomorphism $\theta_D \colon \Gamma_D/\Gamma_K \to \mathrm{Gal}(Z(\overline{D})/\overline{K})$ acting by the formula $\overline{v}(d) \mapsto \overline{i_d}$, where $\overline{v}(d) = v(d) + \Gamma_K$.

The following inequality is well known:

$$[D : E] \geqslant [\overline{D} : \overline{E}] \cdot [\Gamma_D : \Gamma_E]. \tag{1.1}$$

By the Ostrowski-Draxl theorem (see [21]) we have $[D:K] = q^r[\overline{D}:\overline{K}] \cdot |\Gamma_D:\Gamma_K|$, where $q = \mathrm{char}(\overline{D})$ for $\mathrm{char}(\overline{D}) \neq 0$, $q = 1$ for $\mathrm{char}(\overline{D}) = 0$, and r is a nonnegative integer. The algebra D is said to be *defectless over* K (with respect to v) if $[D : K] < \infty$ and $[D : K] = [\overline{D} : \overline{K}] \cdot |\Gamma_D : \Gamma_K|$, and it is said to be *unramified over* K if $[D : K] = [\overline{D} : \overline{K}] < \infty$ and $Z(\overline{D})$ is separable over $\overline{K}$. The term 'defectless (unramified) algebra D' means a 'defectless (respectively, unramified) algebra over $Z(D)$'. It is evident that when $\mathrm{char}(\overline{D}) = 0$ or $\mathrm{char}(\overline{D}) \nmid [D : K]$, the algebra D is defectless. The algebra $D \in \mathcal{D}(K)$ is said to be *totally ramified* if $[D : K] = [\Gamma_D : \Gamma_K]$. Finally, the algebra D/K is called *immediate* if $[\overline{D} : \overline{K}] \cdot |\Gamma_D : \Gamma_K| = 1$.

It is known that the reduction (residue) homomorphism defines an epimorphism θ_D of the group Γ_D/Γ_K onto the group of $\overline{K}$-automorphisms of the centre $Z(\overline{D})$ of the residue algebra $\overline{D}$ (see [36]).

The reduction homomorphism and the homomorphism θ_D are associated with the so-called reduction defect λ_D ($\lambda_D = \mathrm{ind}\, D/\mathrm{ind}\, \overline{D}[Z(\overline{D}) : \overline{K}]$). By abusing notation slightly, below we omit the subscript D and write λ instead of λ_D. Recall that a reduction is said to be *tame* if the extension $Z(\overline{D})/\overline{K}$ is separable and $\mathrm{char}(\overline{K})$ does not divide the order of $\mathrm{Ker}(\theta_D)$.

Our main interest is in weakly ramified algebras.

Definition 3. Let K be a Henselian field and let $D \in \mathcal{D}(K)$. An algebra D is said to be *weakly ramified* if (i) $\mathrm{char}(\overline{K}) = 0$ or (ii) $\mathrm{char}(\overline{K}) \neq 0$, and D is defectless and has a tame reduction. In what follows the set of weakly ramified over K division algebras is denoted by $\mathrm{TR}(K)$.

Remark 1. It follows immediately from the definition (see also [36], Lemma 6.1) that the elements of $\mathrm{Br}(K)$ represented by weakly ramified central division K-algebras form a subgroup of $\mathrm{Br}(K)$. Moreover, if the algebra A belongs to $\mathrm{TR}(K)$ and L/K is an extension of the field K, then $A_L \in \mathrm{TR}(K)$.

The following property of weakly ramified algebras is quite important.

Lemma 1. *Let $D \in \mathrm{TR}(K)$ and $D = D_1 \otimes_K D_2$, where D_1 and D_2 are central K-algebras of coprime indices. Then $D_1, D_2 \in \mathrm{TR}(K)$.*

Proof. If $\mathrm{char}\, \overline{K} = 0$, then this result follows directly from the definition of weakly ramified algebras. And if $\mathrm{char}\, \overline{K} \neq 0$, then it follows from Lemma 6.1, (i), in [36], since the indices of D_1 and D_2 are coprime.

For $D \in \mathrm{TR}(K)$ the ramification index of D over K, which is defined as the index of the group Γ_K in Γ_D, is the product of the upper ramification index, which coincides with λ_D^2, and the lower index, which coincides with $[Z(\overline{D}) : \overline{K}]$ (see [33]).

All the notation introduced above is also applicable to the case of an algebra D with unitary involution τ for a Henselian field k, since if k has a Henselian valuation v_k, then it extends uniquely to a valuation v_K of the field K and a valuation $v_D = v$ of the algebra $D \in \mathcal{D}(K)$ by the following rule: for any $d \in D^*$ put $v_D(d) = n^{-1} v_K(\mathrm{Nrd}_D(d))$, where $n = \operatorname{ind} D$. Thus, $\mathrm{SL}(D)$ is contained in U_D, and therefore the reduction homomorphism is defined on $\mathrm{SL}(D)$ (see [37]).

As mentioned already, the second part of this work is devoted to deriving formulae for the computation of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ in terms of subgroups of the multiplicative group of the residue algebra $\overline{D}^{\,*}$. The main assertion related to the computation of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ is formulated in terms of the following groups:

$$\begin{aligned}
&\mathrm{SL}^v(D) = \bigl\{d \in \mathrm{SL}(D) \mid N_{Z(\overline{D})/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{d})) = 1\bigr\};\\
&\mathrm{SU}^v(D,\tau) = \bigl\{d \in \mathrm{SU}(D,\tau) \mid N_{Z(\overline{D})/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{d})) = 1\bigr\};\\
&\mathrm{SUK}_1^v(D,\tau) = \overline{\mathrm{SU}^v(D,\tau)}/U(\overline{D},\overline{\tau})';\\
&E_\lambda = C_\lambda(\overline{K}) \cap N_{Z(\overline{D})/\overline{K}} \circ \mathrm{Nrd}_{\overline{D}}(\overline{D})^{\overline{\tau}-1}.
\end{aligned}$$

Here $C_\lambda(\overline{K})$ is the group of λth roots of unity belonging to the field $\overline{K}$.

At the end of this work we consider several important examples of the computation of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ for some special algebras D and $\overline{D}$, and special groups of values Γ_D.

The following theorem provides the main tool for computing $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$.

Theorem 2. *Let $D \in \mathrm{TR}(K)$, assume that $\operatorname{char} \overline{k} \neq 2$, and let $\tau \in \mathrm{Inv}_{K/k}(D)$, where k is Henselian. Then in the notation introduced above the following commutative diagram holds, in which the sequences in both rows and in the column are exact*:

$$\begin{tikzcd}
 & & & 1 \arrow[d] & & \\
1 \arrow[r] & E \arrow[r] & \mathrm{SU}^v(D,\tau)/(U(D,\tau))' \arrow[r] & \mathrm{SUK}_1^v(D,\tau) \arrow[r] \arrow[d] & 1, & (1)\\
1 \arrow[r] & E \arrow[r] & \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \arrow[r] & \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \arrow[r] \arrow[d] & 1. & (2)\\
 & & & E_\lambda \arrow[d] & & \\
 & & & 1 & &
\end{tikzcd}$$

Here $E = ((1 + M_D) \cap \mathrm{SU}(D,\tau))U(D,\tau)'/U(D,\tau)'$. *In addition, the following sequences are also exact*:

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \mathrm{SUK}_1^{v}(D,\tau) \to \mathrm{Nrd}_{\overline{D}}(\overline{U(D,\tau)}) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D,\tau)}) \to 1, \tag{3}$$

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \to \overline{\mathrm{SU}(D,\tau)}/\,\mathrm{SU}(\overline{D},\overline{\tau}) \to 1. \tag{4}$$

The proof of Theorem 2 is presented in § 6.

Remark 2. The exact sequences mentioned in the theorem and relating the subgroups of the groups D^* and $\overline{D}^*$ are realized by means of the reduction homomorphism, and the homomorphisms involved in these exact sequences are also induced by this homomorphism and can easily be recovered from the context; for brevity we leave it to the reader to describe these homomorphisms.

Thus, the problem of the computation of the above-mentioned groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ is reduced to the computation of the subgroups $\overline{D}^*$ and the group E, which is evidently isomorphic to $((1+M_D)\cap\mathrm{SU}(D,\tau))/(U(D,\tau)'\cap(1+M_D))$. It is clear that the last group is trivial when $((1 + M_D) \cap \mathrm{SU}(D,\tau)) \subset U(D,\tau)'$. If this condition is satisfied, then we say that the group $\mathrm{SU}(D,\tau)$ *satisfies the congruence theorem* or that the group $\mathrm{SU}(D,\tau)$ *has the congruence property.*

Remark 3. Note that similar assertions also hold for the groups $\mathrm{SL}_m(D)$ and the groups $\mathrm{SU}_m(D,f)$ of isotropic forms f (see [22] and [23]).

Below the congruence theorem is established for one-dimensional anisotropic forms f under some special, little restrictive assumptions.

More exactly, in what follows an important role will be played by the so-called cyclic involutions accompanied by unitary elements (cf. Definition 5).

Definition 4. Given a cyclic extension L/K of degree n with group $\mathrm{Gal}(L/K)$, a central K-algebra A is said to be *cyclic over the extension* L/K if it contains L as a maximal subfield. In this case there exists an element $u \in A^*$ such that the inner automorphism i_u induces on L a generator $\sigma \in \mathrm{Gal}(L/K)$. Then u^n is contained in K and the algebra A is usually denoted by (L,σ,a), where $a = u^n$. We shall also use the notation $\langle L,\sigma,u\rangle$ for the algebra A.

Definition 5. A unitary K/k-involution τ of the algebra $D \in \mathcal{D}(K)$ is said to be *cyclic* (and is denoted by τ_L) if $D = \langle L,\sigma,u\rangle$, $L^\tau = L$ and $L_\tau = \{l \in L \mid l^\tau = l\}$ is cyclic over k. A cyclic involution τ_L is called an *involution accompanied by a unitary element* if there exists an element $u \in U(D,\tau_L)$ such that the automorphism σ coincides with the inner automorphism i_u as restricted to the field L. Below we denote such an involution by $\tau_L(u)$ and call it an involution of the form $\tau_L(u)$.

Using this notation we can formulate the following important theorem.

Theorem 3. *Let* $D \in \mathrm{TR}(K)$ *and* $\tau \in \mathrm{Inv}_{K/k}(D)$. *Then the group* $\mathrm{SU}(D,\tau)$ *has the congruence property in the following two cases*:

(i) $\overline{D}$ *is a field*;

(ii) $\overline{D}$ *is not a field*, $(\mathrm{ind}\,D, \mathrm{char}\,\overline{k}) = 1$ (*provided that* $\mathrm{char}\,\overline{k} > 0$) *and* $\overline{\tau}$ *is accompanied by a unitary element.*

The proof is presented in § 7.

It turns out that the class of involutions of the form $\tau_L(u)$ is rather wide. For instance, we show below that the set of cyclic K/k-involutions τ_L of an algebra D with a fixed field L always contains an involution of the form $\tau_L(u)$. Moreover, for an arbitrary involution $\tau_L(u)$ we derive conditions for its 'duplication'.

Not every K/k-involution of the algebra D has the form $\tau_L(u)$ (neither is it cyclic, see [38]). However, there always exists a regular central extension N of the centre K such that the involution τ is extended to a unitary involution $\tau_E(v)$ for an appropriate field $E \subset D \otimes_K N$ and an element $v \in U(D \otimes_K N, \tau_E(v))$.

Recall the following definition.

Definition 6. Let ε_n be a primitive nth root of unity in the field K. For arbitrary $a, b \in K^*$ let $A(a, b; K, \varepsilon_n)$ denote the K-algebra generated by the elements i and j satisfying the relations $i^n = a$, $j^n = b$ and $ij = \varepsilon_n ji$. Such algebras are conventionally referred to as *symbol algebras*.

In our proof of the main result we use the following involutive analogue (Theorem 9) of a theorem of Draxl [21].

Let K/k be a weakly ramified extension, let the algebra $D \in \mathrm{TR}(K)$ be totally ramified ($D \neq K$), and let $\tau \in \mathrm{Inv}_{K/k}(D)$. Then there exists a positive integer r such that D has the form $D = D_1 \otimes_K \dots \otimes_K D_r$, where D_i is an appropriate tensor product of τ-invariant symbol algebras $A(a_{ij}, b_{ij}, K, \varepsilon_{p_i^{\alpha_j}})$, whose exponents coincide with their indices ($1 \leqslant i \leqslant r$, $j \in \mathbb{Z}$) and the corresponding canonical generators are τ-invariant, and the p_i are the prime divisors of the index $\operatorname{ind} D$. *In particular, the algebra D is the product of its τ-invariant primary components.*

The author dedicates this article to the memory of Academician A. N. Parshin.

§ 2. Unitary involutions of division algebras

In this section we describe special unitary involutions of division algebras D.

For any $N \subset D$ and any mapping $\mu\colon N \to N$ let $N_\mu = \{n \in N \mid n^\mu = n\}$. In particular, $S_\tau(D) = \{s \in D \mid s^\tau = s\}$. A criterion for the set $\mathrm{Inv}_{K/k}(D)$ being nonempty consists in the following: $\mathrm{Inv}_{K/k}(D)$ is nonempty if and only if the class of the algebra D in the Brauer group of the field K belongs to the kernel of the corestriction homomorphism $\mathrm{cor}_{K/k}\colon \mathrm{Br}(K) \to \mathrm{Br}(k)$. If $\mathrm{Inv}_{K/k}(D) \neq \varnothing$ and $\tau \in \mathrm{Inv}_{K/k}(D)$, then all other elements $\mu \in \mathrm{Inv}_{K/k}(D)$ have the form $\mu = \tau i_{s_\mu}$ for $s_\mu \in S_\mu(D)$.

The criterion formulated above yields a necessary and sufficient condition for the existence of K/k-involutions in special cyclic algebras.

Theorem 4 (Albert, [39]). *Let K/k be a quadratic separable extension with a nontrivial k-automorphism τ, E/k be a cyclic Galois extension, which is linearly disjoint from K over k, and let $L = E \otimes_k K$. Then the algebra $A = (L, \sigma, a)$ ($\langle\sigma\rangle =$* $\mathrm{Gal}(L/K)$) *has a K/k-involution extending* $\mathrm{id} \otimes \tau$ *if and only if $(E/k, \langle\sigma|_E\rangle, aa^\tau)$ is a trivial k-algebra (that is, $aa^\tau \in N_{E/k}(E^*)$).*

The following assertion also proves to be rather useful.

Theorem 5 (Kneser, [40]). *Let $D \in \mathcal{D}(K)$, $\tau \in \mathrm{Inv}_{K/k}(D)$, and let A be a K-subalgebra with a unitary involution μ_A such that $\mu_A|_K = \tau|_K$. Then there exists an involution $\mu \in \mathrm{Inv}_{K/k}(D)$ such that $\mu|_A = \mu_A|_A$.*

An important role in what follows is played by a certain special class of cyclic K/k-involutions.

The importance of the class of cyclic involutions is explained by the following lemma due to Sury.

Lemma 2. *Let $D \in \mathcal{D}(K)$ be an algebra of an odd prime index with an involution τ, and let $d \in \mathrm{SU}(D,\tau)$ and $d \notin K$. If $\tau = \tau_{K(d)}$, then $d = yay^{-1}a^{-1}$ for some $y \in D^*$ and $a \in U(D,\tau) \cap K(d)$.*

Remark 4. For cyclic involutions τ_L, in the case of odd $\operatorname{ind} D$ denote by δ some generator of the Galois group $\mathrm{Gal}(L/k)$ and set $\sigma = \delta^2$. It is evident that σ is a generator of the Galois group L/K and $\sigma|_{L_\tau}$ is a generator of $\mathrm{Gal}(L_\tau/k)$.

Remark 5. Algebras with cyclic involutions do exist. Indeed, let L/k be a cyclic extension of degree $2n$, where n is odd and greater than 1, and let μ be a generator of the Galois group. Set τ to be equal to μ^n and σ to be equal to μ^2. Let $a \in K$, $a, a^2, \dots, a^{n-1} \notin N_{L/K}(L^*)$ and $aa^\tau \in N_{L_\tau/k}$. Then $D = (L,\sigma,a)$ is a division algebra with a unitary K/k-involution. Moreover, by Theorem 5 the K/k-involution τ of the field L extends to a cyclic involution τ_L of the algebra D.

Lemma 3. *Let $D \in \mathcal{D}(K)$ be an algebra of odd index n with a cyclic involution τ_L. Then there exists an element $u \in D$ such that $u|_L$ generates the group $\mathrm{Gal}(L/K)$ and $u^{\operatorname{ind} D} \in U(K, \tau_L|_K)$.*

Proof. Since there exists an involution τ_L, the algebra D has the form $D = (L,\sigma,a)$. Then $D = (L,\sigma^2,a^2)$ because n is odd. Since D has a unitary K/k-involution, the following relations hold (see Theorem 4):

$$aa^\tau = N_{L_\tau/k}(\chi \quad \text{and} \quad a^2a^{2\tau} = N_{L_\tau/k}(\chi)^2,$$

where $\chi \in L_\tau$. Denote by b the value of $N_{L_\tau/k}(\chi)$. Then

$$a^{2\tau}b^{-1} = a^{-2}b \quad \text{and} \quad (a^2b^{-1})^\tau = (a^2b^{-1})^{-1}.$$

Thus, the element a^2b^{-1} is unitary and $D = (L,\sigma^2,a^2) = (L,\sigma^2,a^2b^{-1})$, since $b = N_{L_\tau/k}(\chi) = N_{L/K}(\chi)$. It follows from the last representation of D that it has an element u such that $u^n = a^2b^{-1} \in U(K,\tau)$ and the restriction of i_u to the field L coincides with σ. The proof is complete.

In view of Lemma 3 it is natural to pose the following question: can the element u always be chosen in $U(D,\tau_L)$? This leads to considering involutions of the form $\tau_L(u)$, where $u \in U(D,\tau_L)$ (see Definition 5).

Note that the existence of an involution of the form $\tau_L(u)$ does not depend on the choice of a generator of the group $\mathrm{Gal}(L/K)$.

Since cyclic involutions $\tau_L(u)$ play an important role below, let us give a criterion for the existence of involutions $\mu_L(u)$ for a fixed cyclic involution τ_L.

Lemma 4. *Let $D \in \mathcal{D}(K)$ be a cyclic algebra (L,σ,γ) with a cyclic involution $\tau = \tau_L$, and let $\Gamma \in D$ be such that $i_\Gamma|_L = \sigma$ and $\Gamma^{\operatorname{ind} D} = \gamma$. Then the algebra D has a cyclic K/k-involution μ_L of the form $\mu_L(u)$ with the same restriction to L as τ if and only if $\mu_L = \tau i_a$, $a \in L_\tau$, and for an appropriate $l \in L^*$*

$$a^{-\sigma^{-1}}a = (\Gamma\Gamma^\tau)^{-1}N_{L/L_\tau}(l). \tag{2.1}$$

Proof. We set $\chi_\Gamma = \Gamma\Gamma^\tau$ and show that $\chi_\Gamma \in L_\tau$. Denote a primitive element L_τ over k by x. Then $\Gamma^{-1}x\Gamma = x^\sigma$ by the hypotheses of the lemma. Applying τ to both sides of this relation we obtain $\Gamma^\tau x^\tau \Gamma^{-\tau} = x^{\sigma\tau} = x^\sigma$. Note that, as σ and τ commute and x is fixed under the action of τ, this chain of equalities yields the relation $\Gamma^\tau x \Gamma^{-\tau} = x^\sigma$. With regard to what we said above, we obtain $\Gamma\Gamma^\tau x(\Gamma\Gamma^\tau)^{-1} = x$, which yields $\Gamma\Gamma^\tau = \chi_\Gamma \in L$, and since the element $\Gamma\Gamma^\tau$ is fixed by the action of τ, we have $\chi_\Gamma \in L_\tau$. It is evident that $\Gamma^\tau = \Gamma^{-1}\chi_\Gamma$.

Since $\Gamma^\tau = \Gamma^{-1}\chi_\Gamma$, equality (2.1) can be written in the following equivalent form: $a^{-\sigma^{-1}}a = \chi_\Gamma^{-1}N_{L/L_\tau}(l^{-1})$. Let $\mu_L = \tau i_a$ (note that the restriction of $i_{l\Gamma}$ to L coincides with $\sigma|_L$). In view of the relation $\Gamma^\tau = \Gamma^{-1}\chi_\Gamma$ and the equality $a^{-\sigma^{-1}}a = \chi_\Gamma^{-1}N_{L/L_\tau}(l^{-1})$ we have $la^{-\sigma^{-1}}a\chi_\Gamma l^\tau = 1$. Further, note that $la^{-\sigma^{-1}}a\chi_\Gamma l^\tau = l\Gamma a^{-1}\Gamma^{-1}a\chi_\Gamma l^\tau = (l\Gamma)a^{-1}\Gamma^{-1}\chi_\Gamma a l^\tau$. Since $\Gamma\Gamma^\tau = \chi_\Gamma$, the last expression can be written as $(l\Gamma)a^{-1}\Gamma^\tau a l^\tau$, which coincides with the product $l\Gamma(l\Gamma)^{\mu_L}$. Since we have started from the equality $la^{-\sigma^{-1}}a\chi_\Gamma l^\tau = 1$, the above computations show that $l\Gamma \in U(D,\mu_L)$, which means that the involution μ_L has the form $\mu_L(l\Gamma)$.

Conversely, suppose that the algebra D has an involution $\mu_L(u)$, where μ_L is a cyclic K/k-involution whose restriction μ_L to L coincides with $\tau|_L$ and $u \in U(D,\mu_L)$. It is evident that $\mu_L = \tau i_a$ for an appropriate $a \in L_\tau$. Next, as τ and μ_L have the same restriction to L, we can assume that $a^{\mu_L} = l\Gamma$ for some $l \in L$. In this notation, since $a^{\mu_L} = a$, the element $l\Gamma$ obeys the relation $(l\Gamma)(l\Gamma)^{\mu_L} = 1$. For the left-hand side of the last equality we have $(l\Gamma)(l\Gamma)^{\mu_L} = (l\Gamma)a^{-1}(l\Gamma)^\tau a = (l\Gamma)a^{-1}\Gamma^\tau l^\tau a = (l\Gamma)a^{-1}\Gamma^\tau a l^\tau$. Further, taking the relation $\Gamma^\tau = \Gamma^{-1}\chi_\Gamma$ into account we have $(l\Gamma)a^{-1}\Gamma^{-1}\chi_\Gamma a l^\tau$, which means that $l(\Gamma a^{-1}\Gamma^{-1})a\chi_\Gamma l^\tau = la^{-\sigma^{-1}}a\chi_\Gamma l^\tau$. Turning back to the equality $(l\Gamma)(l\Gamma)^{\mu_L} = 1$ we obtain $a^{-\sigma^{-1}}a\chi_\Gamma = l^{-1}l^{-\tau}$. Thus, $a^{-\sigma^{-1}}a = \chi_\Gamma^{-1}N_{L/L_\tau}(l^{-1})$. The proof is complete.

It turns out that each involution $\tau_L(v)$ generates a whole class of similar involutions.

Proposition 1. *If* $\tau = \tau_L(v)$, *then* $\tau i_{g^{-\tau}g^{-1}} = \tau_{gLg^{-1}}(gvg^{-1})$, *where* $g \in D^*$.

Proof. First note that the field gLg^{-1} is $\tau i_{g^{-\tau}g^{-1}}$-invariant. Indeed, as L is τ-invariant, we have

$$(gLg^{-1})^{\tau i_{g^{-\tau}g^{-1}}} = gg^\tau g^{-\tau}L^\tau g^\tau g^{-\tau}g^{-1} = gLg^{-1}.$$

Moreover, $gvg^{-1} \in U(D, \tau i_{g^{-\tau}g^{-1}})$, since $v \in U(D,\tau)$ and

$$(gvg^{-1})^{\tau i_{g^{-\tau}g^{-1}}} = gg^\tau g^{-\tau}v^{-1}g^\tau g^{-\tau}g^{-1} = (gvg^{-1})^{-1}.$$

By hypothesis, for any $l \in L$ we have $v^{-1}lv = l^\sigma$. Carrying over the generator σ to the extension gLg^{-1} gives the generator $\widetilde{\sigma}$ of the Galois group $\mathrm{Gal}(gLg^{-1}/K)$ that sends each element $glg^{-1} \in \mathrm{Gal}(gLg^{-1}/K)$ to $gl^\sigma g^{-1}$. Thus, to complete the proof of the proposition it remains to show that $(gvg^{-1})^{-1}(glg^{-1})(gvg^{-1}) = (glg^{-1})^{\widetilde{\sigma}}$. The proposition is proved.

Proposition 2. *Fix an involution* $\tau = \tau_L$ *of the form* $\tau_L(u)$. *Let* $\mu \in \mathrm{Inv}_{K/k}(D)$ *be such that* $\mu|_L = \tau_L(u)|_L$. *It is clear that* $\mu = \tau_L(u)i_a$, *where* $a \in L_\tau$. *If the index of* D *is odd, then the cyclic involution* μ *has the form* $\tau_L(v)$ *if and only if* $a = cb^\tau b$ *for some* $c \in k$ *and* $b \in L$.

Proof. Indeed, if a required v does exist, then, as the restrictions $i_v|_L$ and $i_u|_L$ coincide, the element v has the form uz, where $z \in L$. Since $v \in U(D,\mu)$, we have $(uz)^{\tau i_a} = z^{-1}u^{-1}$, $a^{-1}z^\tau u^\tau a = z^{-1}u^{-1}$, and since $a, z \in L$, we have $a^{-1}z^\tau u^\tau a = z^\tau a^{-1}u^{-1}a = z^{-1}u^{-1}$, which yields $z^\tau z = u^{-1}a^{-1}ua = a^{-\sigma}a = (a^{-1})^\sigma(a^{-1})^{-1}$. We apply the mapping $N_{L/K}$ to both sides of the last equality and obtain $N_{L/K}(z)N_{L/K}(z)^\tau = 1$. Hence, by Hilbert's Theorem 90 we have $z = t^{\theta-1}$, where θ is the generator of the group $\mathrm{Gal}(L/k)$ and $b \in L$. We can assume that $\theta = \sigma\tau$. Then $(t^{\theta-1})(t^{\theta-1})^\tau = (t^{\sigma\tau}t^{-1})(t^\sigma t^{-\tau}) = (t^{\tau+1})^\sigma(t^{\tau+1})^{-1} = (a^{-1})^\sigma(a^{-1})^{-1}$. This suggests the relation $(at^{\tau+1})^\sigma(at^{\tau+1})^{-1} = 1$, which in turn yields $at^{\tau+1} = c \in K$. Since a and $t^{\tau+1}$ belong to L_τ^*, we have $c \in k$. Putting $b = t^{-1}$ we obtain $a = cbb^\tau$.

Conversely, let $a = cb^\tau b$, where $c \in k$ and $b \in L$. Then $\tau i_a = \tau i_{cb^\tau b} = \tau i_{bb^\tau}$, hence τi_{bb^τ} has the form $\tau_{bLb^{-1}}(bub^{-1})$ in view of the above proposition. Since $b \in L$, we have $bLb^{-1} = L$ and τi_a has the form $\tau_L(v)$, where $v = bub^{-1}$. The proof is complete.

The following proposition is an adapted version of an observation made by Sury.

Proposition 3. *Let τ_L be a cyclic involution of an algebra $D \in \mathcal{D}(K)$ of odd index* ($\mathrm{char}\, k \neq 2$). *If τ_L has the form $\tau_L(u)$, then* $(\mathrm{SU}(D,\tau) \cap (L \setminus K)) \subset U(D,\tau)'$.

Proof. Consider the field $K(d)$, where $d \in \mathrm{SU}(D,\tau) \cap (L \setminus K)$. Then $\mathrm{Nrd}_D(d) = N_{L/K}(d) = 1$. By Hilbert's Theorem 90

$$d = b^{\sigma-1}$$

for some $b \in L$ and $\sigma = i_u|_L$. Since the group $\mathrm{Gal}(L/k)$ is Abelian, σ commutes with τ, and therefore $b^{-\sigma}b = d^{-1} = d^\tau = (b^\sigma b^{-1})^\tau = (b^\tau)^\sigma(b^\tau)^{-1}$. This yields the relation $(bb^\tau)^\sigma = bb^\tau$, which means that $bb^\tau \in K$. As bb^τ is τ-invariant, we have $bb^\tau = \lambda \in k$, or, which is the same, $\lambda = l_1^2 - \alpha l_2^2$ for some $l_1, l_2 \in L_\tau$. Moreover, since the cyclic K-algebra $(K, \tau|_K, \lambda)$ is a matrix algebra over K, the quadratic form $x^2 - \alpha y^2$ is isotropic over K, which means that there exist $t_1, t_2 \in K$ such that $t_1^2 - \alpha t_2^2 = \lambda$. Then it is easily seen that for $t = t_1 + \sqrt{\alpha}t_2$ we have $bt^{-1} \in U(1, L)$. Since the automorphism σ is induced by the restriction of the inner automorphism specified by the unitary element u, we have $d = u^{-1}(bt^{-1})u(bt^{-1})^{-1}$, which gives $d \in U(D,\tau)'$. The proof is complete.

For a division algebra with a unitary involution τ the following theorem establishes the existence of a regular extension of its centre such that the resulting division algebra has a unitary involution that extends the involution τ of the original algebra and has a special form.

Theorem 6. *Let $D \in \mathcal{D}(K)$ and $\tau \in \mathrm{Inv}_{K/k}(D)$, and assume that* $\mathrm{char}\, k \neq 2$. *Then there exist a regular extension N/K and an extension of τ to an involution $\widetilde{\tau}$ of the algebra $D_N = D \otimes_K N$ such that*:

1) *D_N is a cyclic division algebra*;
2) *$\widetilde{\tau}$ has the form $\tau_L(u)$ for appropriate $L \subset D_N$ and $u \in U(D_N, \widetilde{\tau})$.*

Proof. Let $n = \mathrm{ind}\, D$. By [41], Lemma 2.9, there exists a tower of extensions $k \subset R \subset T$ such that T/k is a finitely generated purely transcendental extension and

T/R is a cyclic Galois extension of degree n. Put $F = KR$ and $E = KT$, and let $A = (E(w)/F(w), \sigma, w)$ be a cyclic $F(w)$-algebra, where σ is a generator of the Galois group of the extension $E(z)/F(z)$, z is a variable that is transcendental over F and $w = (1 + z\sqrt{\alpha})/(1 - z\sqrt{\alpha})$. It is easily seen that both the exponent and index of this algebra are equal to n. Since $F(z) = F(w)$, A can be represented in the following form: $(E(z)/F(z), \sigma, w)$.

Further, note that $A \sim A \otimes_{F(z)} D^{\mathrm{op}}_{F(z)} \otimes_{F(z)} D_{F(z)}$, where the algebra $D^{\mathrm{op}}_{F(z)}$ is anti-isomorphic to the algebra $D_{F(z)}$.

Let M be the function field of the Severi-Brauer variety $\mathrm{SB}(A \otimes_{F(z)} D^{\mathrm{op}}_{K(z)})$. Then $A \otimes_{F(z)} M \sim D_{F(z)} \otimes_{F(z)} M$. Since $\deg(A \otimes_{F(z)} M) = \deg(D_{F(z)} \otimes_{F(z)} M)$, we have $A \otimes_{F(z)} M \cong D_{F(z)} \otimes_{F(z)} M$.

Further, let $\mu = \tau|_K$. Then the automorphism μ can be extended to an isomorphism between M and another regular extension of K, which we denote by M_μ. Consequently, we have the following commutative diagram:

$$\begin{tikzcd}
K \arrow[r] \arrow[d, "\mu"'] & M \arrow[d, "\mu"] \\
K \arrow[r] & M_\mu
\end{tikzcd}$$

Denote the free compositum MM_μ of the fields M and M_μ over K by N, and the natural extension of the automorphism μ to N by $\widetilde{\mu}$. Let $Q = T_{K/k}(N)$ be the transfer of the field N under the restriction of scalars K/k (that is, Q is the subfield of elements of N that are invariant under $\widetilde{\mu}$). As the extension N/K is regular (see [42]), the algebra D_N has the same index and exponent as D_M, moreover, D_N is a cyclic algebra with the unitary involution $\widetilde{\tau}$ defined by

$$\widetilde{\tau}(d \otimes n) = \tau(d) \otimes \widetilde{\mu}(n),$$

where $d \in D$ and $n \in N$. Thus, $\widetilde{\tau}$ is an extension of the involution τ to the algebra D_N. Note that the involution $\widetilde{\tau}$ has the form $\tau_L(u)$, since D_N contains a cyclic extension $(E(z)N)/F(z)N$ and an element w such that $\sigma = i_w$ and $w^{\widetilde{\tau}} = w^{-1}$. The proof of the theorem is complete.

In conclusion of this section we formulate a lemma that enables reducing many proofs of results on involutions $\tau_L(u)$ to the case of algebras of primary indices.

Lemma 5. *Let $D \in \mathcal{D}(K)$ and $\tau_L(u) \in \mathrm{Inv}_{K/k}(D)$. Let $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the canonical representation of the integer* $\mathrm{ind}\, D$*. Then D is the tensor product over K of algebras $D_1, \dots, D_s$, where each D_i has the primary index $p_i^{\alpha_i}$ and can be represented in the form $\langle L_i, u^{\mathrm{ind}\, D/p_i^{\alpha_i}} \rangle$, where L_i is the extension of the field K induced by the $p_i^{\alpha_i}$-part of the extension L_τ/k. In particular, the algebra D can be represented in the form $D = D_i \otimes_K T_i$, where*

$$T_i = \bigotimes_{j=1, j\neq i}^{s} D_j, \qquad \tau_L(u) = \tau_{L_i}(u^{\mathrm{ind}\, D/p_i^{\alpha_i}}) \otimes_K \Biggl(\prod_{j=1, j\neq i}^{s} \otimes_K \tau_{L_j}(u^{\mathrm{ind}\, D/p_j^{\alpha_j}}) \Biggr).$$

The proof of this lemma goes by direct computation based on the form of the algebra D and the involution $\tau_L(u)$.

Note also that the algebras D_i are $\tau_{L_i}(u^{\mathrm{ind}\, D/p_i^{\alpha_i}})$-invariant.

§ 3. Henselian finite-dimensional central division algebras

Below we need some notation and facts concerning finite-dimensional central simple algebras over Henselian fields.

The following well-known theorem often proves to be very useful.

Theorem 7 (Skolem-Noether). *Let $D \in \mathcal{D}(K)$, and let A and B be K-isomorphic K-subalgebras of D. Then there exists an inner automorphism of the algebra D that extends the K-automorphism between the algebras A and B.*

We will also often use the following theorem from [36].

Theorem 8. *Assume as above that F is a Henselian field and D is a division algebra over F. If $\widetilde{E}$ is an $\overline{F}$-subalgebra of the algebra $\overline{D}$ and the extension $Z(\widetilde{E})/\overline{F}$ is separable, then D contains an unramified lift of the algebra $\widetilde{E}/\overline{F}$ (this means that D contains an F-subalgebra E, unramified over F, with the residue algebra $\widetilde{E}$).*

The notion of an inertia algebra plays an important role in what follows.

Definition 7. Let $D \in \mathcal{D}(F)$ and let $Z(\overline{D})/\overline{F}$ be a separable extension. Then the unramified lift of the extension $\overline{D}/\overline{F}$ is called an *inertia algebra* of the algebra D.

Let us turn to the case of weakly ramified algebras. Clearly, the notion of a weakly ramified structure generalizes a similar notion for field extensions. It is easily seen that each weakly ramified central division algebra D has a maximal weakly ramified subfield. In turn, this fact readily yields the following

Proposition 4. *Suppose that $D \in \mathrm{TR}(K)$. Then $\mathrm{Nrd}_D(1 + M_D) = 1 + M_K$. Moreover, $(1 + M_K)^m = (1 + M_K)$, provided that $\mathrm{char}(\overline{K}) = 0$ or m is coprime to $\mathrm{char}(\overline{K})$ in the case when $\mathrm{char}(\overline{K}) \neq 0$.*

The residues (reductions) of the reduced values of elements of V_D in weakly ramified algebras are computed in the following way.

Proposition 5. *Let $d \in V_D$. Then $\overline{\mathrm{Nrd}_D(d)} = N_{Z(\overline{D})/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(d))^{\lambda}$.*

Lemma 6. *Let E be a weakly ramified extension of a field F. Then the equality $\mathrm{Ker}(N_{E/F})|_{(1+M_E)} = (1 + M_E)^{\tau-1}$ holds, where $\langle\tau\rangle = \mathrm{Gal}(E/F)$.*

Proof. By Hilbert's Theorem 90, for any $a \in \mathrm{Ker}(N_{E/F})(E^*)$ we have $a = b^{\tau-1}$, where $b = t^{\alpha}u$, $u \in U_E$, $\alpha \in \mathbb{Z}$ and $v(t) + \Gamma_F$ is a generator of the group Γ_E/Γ_F. Note that the element t can be taken equal to either 1 or $\sqrt{f}$, where f is an appropriate element of F such that $v(f) \in \Gamma_E \setminus \Gamma_F$. In the case when $t = 1$ we have $\overline{a} = \overline{u}^{\overline{\tau}-1}$, which means that $\overline{u}^{\overline{\tau}-1} = 1$. Hence $\overline{u} \in \overline{F}^*$, and therefore $u = c(1+m)$, where $c \in F^*$ and $m \in M_F$. This gives $a \in (1 + M_E)^{\tau-1}$.

It remains to consider the case of a weakly totally ramified extension E/F. In this case $(\sqrt{f})^{\tau} = -\sqrt{f}$. Then for odd α we have $a = -1(1 + m)^{\tau-1}$, where $m \in M_E$. However, the characteristic $\mathrm{char}\,\overline{F}$ is distinct from 2, and therefore $\overline{a} \neq 1$. Hence $\alpha \in 2\mathbb{Z}$, which reduces this case to the case when $t = 1$. Thus, we have established the inclusion $\mathrm{Ker}(N_{E/F})|_{(1+M_E)} \subset (1 + M_E)^{\tau-1}$. The reverse inclusion $(1 + M_E)^{\tau-1} \subset \mathrm{Ker}(N_{E/F})|_{(1+M_E)}$ is evident. The proof is complete.

The last proposition has the following consequence.

Corollary 1. *The relation $\overline{\mathrm{SL}(D)} = \{\,\widetilde{d} \in \overline{D} \mid N_{Z(\overline{D})/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\widetilde{d})^{\lambda}) = 1\,\}$ holds.*

§ 4. Henselian involutorial tamely totally ramified central division algebras

The main result of this section consists in the description of the structure of weakly totally ramified (that is, weakly ramified and totally ramified) Henselian division algebras D having unitary involutions. Note that in this case $\overline{D} = \overline{K}$. To obtain such a description we need the following preliminary assertions.

Lemma 7. *Let $D \in \mathcal{D}(K)$, let $\tau \in \operatorname{Inv}_{K/k}$ for a Henselian field k, and let $g \in D^*$. Then $g^\tau = ug$, where $u \in U_D$.*

Proof. It is easily seen that $\operatorname{Nrd}_D(g^\tau) = (\operatorname{Nrd}_D(g))^\tau$. Set $c = \operatorname{Nrd}_D(g)$. Then $v_K(c) = v_K(c^\tau)$. Consequently, $v_K(\operatorname{Nrd}_D(g)) = v_K((\operatorname{Nrd}_D(g))^\tau)$. This gives $v_D(g) = v_D(g^\tau)$, which yields $v_D(g^{\tau-1}) = 0$. Hence $g^{\tau-1} \in U_D$. The proof of the lemma is complete.

For the reader's convenience we present here the following well-known lemma. Recall that ε_e denotes a primitive eth root of unity in the field K.

Lemma 8. *Let k be a Henselian field, and let the integer e be coprime to $\operatorname{char} \overline{k}$ for $\operatorname{char} \overline{k} \neq 0$. If $K = k(\varepsilon_e)$ is a quadratic extension of the field k, then K/k is an unramified Galois extension.*

Lemma 9. *Let the algebra $D \in \operatorname{TR}(K)$ be totally ramified and the element $b \in D$ be such that $v_D(b^e) \in \Gamma_K$ for some e coprime to $\operatorname{char} \overline{k}$. Then there exist $\pi_K \in K^*$ and $m \in M_{K(b^e)}$ such that $b^e = \pi_K(1+m)^e$. Moreover, if K/k is weakly ramified, D has a unitary K/k-involution τ and b^e is a τ-invariant element, then $m \in M_{k(b^e)}$, so that $\pi_K \in k^*$.*

Proof. The proof of the first part of the lemma is presented in [21]. Now let b^e be a τ-invariant element, and let $v_D(b^e) \in \Gamma_K$. Then $b^e = \pi_K u$ for some appropriate elements π_K of K and u of $U_{K(b^e)}$.

If the extension K/k is unramified, then without loss of generality we can assume that π_K is an element of k^*, which means that the element $\pi_K^{-1} b^e$ is τ-invariant. In view of this we can conclude that $\overline{u}$ is $\overline{\tau}$-invariant. We consider its inverse image z in k and obtain $b^e = \pi_K z(1+q)$, where $q \in M_{K(b^e)}$. As $b^e \pi_K^{-1} z^{-1}$ is τ-invariant, the same is true of $1+q$. Since $D \in \operatorname{TR}(K)$, the field $k(b^e)$ contains $1+m$, an eth root of $1+q$.

In the case of a totally ramified extension K/k, for any $\Pi_K \in K \setminus k$ we have $\Pi_K = \delta_k \sqrt{\alpha}\, u$, where $u \in U_K$, $\delta_k \in k$, $K = k(\sqrt{\alpha})$ and $\sqrt{\alpha}^{\,\tau} = -\sqrt{\alpha}$. Since the extension K/k is totally ramified, we can assume without loss of generality that $u = 1+p$, where $p \in M_K$. As the element b^e is τ-invariant, by the first part of the lemma we obtain $\Pi_K^\tau (1+m^\tau)^e = \Pi_K (1+m)^e$. Since $\Pi_K = \delta_k \sqrt{\alpha}\,(1+p)$, we have $-\delta_k \sqrt{\alpha}\,(1+p^\tau)(1+m^\tau)^e = \delta_k \sqrt{\alpha}\,(1+m)^e$. Then $-(1+p^\tau)(1+m^\tau)^e = (1+p)(1+m)^e$. Passing to residues in the last equality leads to a contradiction since $\operatorname{char} \overline{k} \neq 2$ (recall that the extension K/k is weakly totally ramified). Consequently, $\pi_K \in k^*$ and $\pi_K^{-1} b^e$ is a τ-invariant element. Thus, $m \in M_{k(b^e)}$, as required. The proof is complete.

Proposition 6. *Let $D \in \mathrm{TR}(K)$ be a totally ramified algebra, let $\tau \in \mathrm{Inv}_{K/k}(D)$ and $e = \exp(\Gamma_D/\Gamma_K)$. Then there exist elements $s \in S_\tau(D)$ and $g \in D$ such that $s^e, g^e \in K$, the orders of the elements $v_D(s) + \Gamma_K$ and $v_D(g) + \Gamma_K$ are equal to e, $[s, g] = gsg^{-1}s^{-1}$ is a primitive eth root ε_e of unity and*

$$\Gamma_D/\Gamma_K = \Gamma_{K(g)}/\Gamma_K \oplus \Gamma_{C_D(K(s))}/\Gamma_K. \tag{4.1}$$

Proof. First of all, note that under the hypotheses of the proposition, by Theorem 3.10 in [33] we have $\varepsilon_e \in K$. Let us establish the existence of nonzero $s \in S_\tau(D)$ with the property that $v_D(s) + \Gamma_K \in \Gamma_D/\Gamma_K$ is an element of order e. Let $x \in D^*$ be such that $v_D(x) + \Gamma_K$ is an element of order e. Set $s = x$ if $x \in S_\tau(D)$. Otherwise, if $\mathrm{char}\,\overline{k} \neq 2$ and $x^\tau = xu$, $u \in U_D$ (Lemma 7), then at least one of the elements $1 - u$ or $1 + u$ is invertible in V_D. Then we set $s = x^\tau + x$ for $1 + u \in U_D$ and $s = x\sqrt{\alpha}\,(1 - u)$ otherwise, where, as usual, $K = k(\sqrt{\alpha})$, $\alpha \in U_k$. Finally, in the case when $\mathrm{char}\,\overline{k} = 2$, since the algebra D is tamely and totally ramified, the index e is odd. Then set $s = xx^\tau$. Without loss of generality we can assume that in all cases $s \in V_D$ (for this it suffices to consider s^{-1} instead of s if necessary).

Now, from Lemma 2 in [2] we obtain $s^e = \pi_K(1 + m)^e$ for appropriate elements π_K of K and m of $M_{K(s^e)}$. Taking now the element $s(1 + m)^{-1}$ instead of s we conclude that $s^e \in K$ and $K(s)/K$ is a cyclic extension of degree e since $\varepsilon_e \in K$.

Denote by φ a generator of the Galois group $K(s)/K$ such that $s^\varphi = s\varepsilon_e$. By the Skolem-Noether theorem there exists an element $g \in D$ such that $gsg^{-1} = s^\varphi$.

Since the group Γ_D/Γ_K has exponent e, we have $v_D(g^e) \in \Gamma_K$. Then from [21], Lemma 2, we obtain $g^e = \pi_K(1 + m)^e$ for some $\pi_K \in K$ and $m \in M_{K(g^e)}$. Taking now $g(1 + m)^{-1}$ instead of g we can assume that $g^e \in K$ and $K(g)/K$ is a cyclic extension of degree e. Without loss of generality let $g \in V_D$.

To establish equality (4.1) let us show that the intersection of the groups $\Gamma_{K(g)}/\Gamma_K$ and $\Gamma_{C_D(K(s))}/\Gamma_K$ coindides with Γ_K. Assume the opposite. Then for an appropriate positive integer m we have $g^m = c(1 + q)$, where $c \in C_D(K(s))$ and $q \in M_D$. Note that $g^m s g^{-m} = s\varepsilon_e^m$. On the other hand $g^m s g^{-m} = (1+q)s(1+q)^{-1}$, so that $s\varepsilon_e^m(1+q) = (1+q)s$, which implies that $s\varepsilon_e^m + s\varepsilon_e q = s + qs$. Consequently, $s(\varepsilon_e^m - 1) = qs - s\varepsilon_e q$. If $\varepsilon_e^m \neq 1$, then the left-hand side of the last equation has valuation $v_D(s)$, whereas a nonzero element with valuation greater than $v_D(s)$ is on the right-hand side. The contradiction obtained means that m is a multiple of e. Thus, $\Gamma_{K(g)}/\Gamma_K \cap \Gamma_{C_D(K(s))}/\Gamma_K = \Gamma_K$.

For reasons of dimension, the order of the group Γ_D/Γ_K is the product of the orders of $\Gamma_{K(s)}/\Gamma_K$ and $\Gamma_{C_D(K(s))}/\Gamma_K$. Since $\Gamma_{K(s)}/\Gamma_K$ and $\Gamma_{K(g)}/\Gamma_K$ have the same order, in view of the equality $\Gamma_{K(g)}/\Gamma_K \cap \Gamma_{C_D(K(s))}/\Gamma_K = \Gamma_K$ we can conclude that $\Gamma_D/\Gamma_K = \Gamma_{K(g)}/\Gamma_K \oplus \Gamma_{C_D(K(s))}/\Gamma_K$. The proof of the proposition is complete.

The following assertion is an analogue of Draxl's theorem in [21] in the case of algebras with unitary involutions.

Theorem 9. *Let K/k be a weakly ramified extension and the algebra $D \in \mathrm{TR}(K)$ ($D \neq K$) be totally ramified, and let $\tau \in \mathrm{Inv}_{K/k}(D)$. Then $D = D_1 \otimes_K \cdots \otimes_K D_r$ for some positive integer r, where D_i is an appropriate tensor product of τ-invariant symbol algebras $A(a_{ij}, b_{ij}, K, \varepsilon_{p_i^{\alpha_j}})$, $1 \leqslant i \leqslant r$, $j \in \mathbb{Z}$, whose exponents are equal* *to their indices, the corresponding canonical generators are τ-invariant, and the p_i are the prime divisors of the index* $\operatorname{ind} D$. *In particular, D is the product of its τ-invariant primary components.*

Proof. Denote $e = \exp(\Gamma_D/\Gamma_K)$ and let the elements $s \in S_\tau(D)$ and $g \in D$ be chosen as in Proposition 6. Thus, $g^e \in K$ and $K(g)/K$ is a cyclic extension of degree e.

Let us show that the element g can be chosen τ-invariant. Suppose that $g^\tau \neq g$. If $g^\tau = -g$, then instead of g we consider the element $\delta g \in S_\tau(D)$, where $\delta \in K$ and $\delta^\tau = -\delta$. Thus, we assume below that $g^\tau \neq \pm g$.

We set $g^\tau = ug$ and show that $u \in C_D(K(s))$. We have

$$g^\tau g s g^{-1} g^{-\tau} = g^\tau s g^{-\tau} \varepsilon_e = (g^{-1} s g)^\tau \varepsilon_e = s \varepsilon_e^{-\tau} \varepsilon_e, \tag{4.2}$$

which means that $(g^\tau g) s (g^\tau g)^{-1} = s\varepsilon_e^{-\tau}\varepsilon_e$. This yields the relation $usu^{-1} = s\varepsilon_e^{-(\tau+1)}$. As $u \in U_D$ and the algebra D is totally ramified, we can assume that $u = (1+m)u_K$, where $m \in M_D$ and $u_K \in U_K$. Then $s^{-1}usu^{-1} \in 1 + M_D$. Consequently, $\varepsilon_e^{-(\tau+1)} = 1$, that is, $\varepsilon_e^\tau = \varepsilon_e^{-1}$. Since $g^2 s g^{-2} = s\varepsilon_e^2$ and $(g^\tau g)s(g^\tau g)^{-1} = s\varepsilon_e^2$, we have $u \in C_D(K(s))$.

In view of equality (4.1) in Proposition 6, the order of the element $v_D(g+g^\tau)+\Gamma_K$ is the least common multiple of the orders of $v_D(g) + \Gamma_K$ and $v_D(1+u) + \Gamma_K \in \Gamma_{C_D(K(s))}$. Now it follows from the definition of e that the order of the element $v_D(g + g^\tau) + \Gamma_K$ equals e. Therefore, we can assume that $g \in S_\tau(D)$. Note also that $v_D(g^e) \in \Gamma_K$, since the exponent of the group Γ_D/Γ_K equals e.

By Lemma 9 and in view of the inclusion $g \in S_\tau(D)$ it follows that $g^e = \pi_k(1+m)^e$ for appropriate elements $\pi_k \in k$ and $m \in M_{k(g^e)}$. Since the elements of $k(g^e)$ commute with s, $1+m$ also commutes with s. Moreover, $1+m$ commutes with g, because it is an element of $k(g^e)$. Now going over from g to $g(1+m)^{-1}$ we can assume that $g^e \in k$ and $K(g)/K$ is a cyclic extension of degree e.

Consider the K-subalgebra A of the algebra D generated by the elements s and g. It is easily seen that A coincides with the symbol algebra $A(s^e, g^e, K, \varepsilon_e)$. Each $a \in A$ has the form $\sum_{l,r} c_{l,r} s^l g^r$, where $c_{l,r} \in K$, hence its τ-image a^τ coincides with $\sum_{l,r} c_{l,r}^\tau g^r s^l$. Since $c_{l,r}^\tau \in K$ and powers of s and g commute up to powers of the root ε_e, we have $a^\tau \in A$. Thus, the algebra A is τ-invariant. If A coincides with D, then D is a τ-invariant symbol algebra. Otherwise $D = A \otimes_K C_D(A)$. It is clear that $\operatorname{ind} C_D(A) < \operatorname{ind} D$. Repeating the above argument for the algebra $C_D(A)$ we arrive at the conclusion that D can be represented in the form of tensor products of τ-invariant symbol algebras over K whose canonical generators are τ-invariant. Now, to complete the proof of the theorem it suffices to take the following two remarks into account.

(i) Let $D = A(a, b, K, \varepsilon_{mn})$, where m and n are coprime, and let i and j be τ-invariant canonical generators of the algebra A.

Then $K\langle i^m, j^m\rangle = A(a, b, K, \varepsilon_{mn}^m)$, $K\langle i^n, j^n\rangle = A(a, b, K, \varepsilon_{mn}^n)$, the elements i^m, j^m and i^n, j^n are τ-invariant canonical generators of the first and second algebra, respectively, and $D = A(a, b, K, \varepsilon_{mn}^m) \otimes_K A(a, b, K, \varepsilon_{mn}^n)$.

(ii) Assume that the algebra $A = A(a, b, K, \varepsilon_q)$ is weakly totally ramified over K. Then its exponent coincides with the index. To prove this it is sufficient to make use of Proposition 6.9 in [36]. The proof of the theorem is complete.

The above proof suggests the following

Corollary 2. *There exist no weakly totally ramified noncommutative division algebras with unitary involutions such that* $\operatorname{char}\overline{k} = 2$ *and the extension* K/k *is not unramified.*

Proof. Since K/k is not unramified, by Lemma 8 for $e = \exp(\Gamma_D/\Gamma_K)$ we have $\varepsilon_e \in k$, in which case, as shown in the proof of the theorem, $\operatorname{ind} D$ is 2-primary. On the other hand, since $D \in \mathrm{TR}(K)$ and $\operatorname{char}\overline{k} = 2$, in view of Theorem 9 $\operatorname{ind} D$ is odd. This completes the proof of the corollary.

It turns out that the indices of the algebras D in Theorem 9 depend essentially on the form of the extension K/k.

Corollary 3. *Let D be the algebra considered in Theorem 9 and p be an odd prime such that* $\overline{\varepsilon_p} \in \overline{k}$*. Then* $(\operatorname{ind} D, p) = 1$.

Proof. Assume that p divides $\operatorname{ind} D$. By Theorem 9 the algebra D can be represented in the form $D_1 \otimes_K D_2$, where D_2 is τ-invariant and the algebra D_1 has a p-primary index which coincides with its exponent. Let L be the τ-invariant maximal subfield in D_2. Then the centralizer $C_D(L)$ is a τ-invariant L-algebra isomorphic to $D_1 \otimes_K L$. It is easily seen that the exponent and index of the last algebra are equal to each other and to the index of D_1. Thus, $C_D(L)$ is a symbol algebra $A(a_1, b_1, L, \varepsilon_{p^n})$, where $a_1, b_1 \in L_\tau^*$. Then the p^{n-1}th tensor power of this algebra is Brauer equivalent to the τ-invariant symbol algebra $A(a_1, b_1, L, \varepsilon_p)$. On the other hand $A(a_1, b_1, L, \varepsilon_p) = A(a_1, b_1, L_\tau, \varepsilon_p) \otimes_{L_\tau} L$. Since $A(a_1, b_1, L_\tau, \varepsilon_p)$ is τ-invariant and the restriction of τ to L_τ is the identity map, we have $\exp A(a_1, b_1, L_\tau, \varepsilon_p) = 2$, which contradicts the fact that the algebra $A(a_1, b_1, L, \varepsilon_p)$ has an odd index. The proof is complete.

Next, there is another corollary.

Corollary 4. *Let the algebra D be the same as in Theorem 9, and let* $\operatorname{char}\overline{k} \neq 2$ *and* $\varepsilon_{\operatorname{rad}(\operatorname{ind} D)} \in k$ *(here* $\operatorname{rad}(\operatorname{ind} D)$ *is the set of all prime divisors of* $\operatorname{ind} D$*). Then* $\operatorname{ind} D$ *is* 2*-primary. In particular, if τ is a cyclic involution, then* $\operatorname{ind} D$ *is* 2*-primary.*

Proof. Assume that $\operatorname{ind} D$ has an odd prime divisor. Take an appropriate 2-primary power of the algebra D and assume without loss of generality that $\operatorname{ind} D$ is odd. Consequently, $\operatorname{rad}(\operatorname{ind} D)$ is also odd, and therefore by Corollary 3 we have $(\operatorname{ind} D, p) = 1$ for any divisor $p \in \operatorname{rad}(\operatorname{ind} D)$, since $\varepsilon_{\operatorname{rad}(\operatorname{ind} D)} \in k$. The contradiction obtained means that the original algebra D is an algebra of a 2-primary index. The proof of the corollary is complete.

Corollary 5. *Let the algebra D be the same as in Theorem 9. If* $\overline{K} = \overline{k}$*, then D is the product of τ-invariant quaternion algebras $D_1, \dots, D_r$, where $D_i = A_i \otimes_k K$ and the A_i are quaternion τ-invariant k-algebras (cf. Lemma 8).*

Proof. Since $D \in \mathrm{TR}(K)$ and the algebra D is totally ramified, we have $\overline{\varepsilon}_e \in \overline{K}$ (see [33]), which means that $\varepsilon_e \in k$ in view of Lemma 8. By Theorem 9 each algebra $A(a_{ij}, b_{ij}, K, \varepsilon_{p_i^{\alpha_j}})$ can be written as a tensor product of a central k-algebra E_{ij} with canonical τ-invariant generators and an extension K/k. Then the algebras E_{ij} are

τ-invariant and $\exp E_{ij} = \operatorname{ind} E_{ij}$. Since the restriction of τ to k is the identity map, the algebra E_{ij} has an exponent and an index equal to 2. The proof is complete.

From the last corollary we easily derive the following.

Corollary 6. *In the above notation, for $\overline{K} = \overline{k}$ there exist no nontrivial weakly totally ramified algebras D/K whose indices are not* 2*-primary.*

Proof. In the case when $\overline{K} = \overline{k}$, by Corollary 5 the algebra D is a product of quaternion algebras, which contradicts the condition that the index of D is not 2-primary. The proof is complete.

The proof of Theorem 9 suggests the following description of weakly totally ramified division algebras.

Corollary 7. *Let the algebra D be as in Theorem* 9, *and let the index of D be coprime to* $\operatorname{char} \overline{k}$. *Then D is a radical K-algebra, which means that it has a finite system of generators over K which consists of τ-invariant radicals* (*recall that an element Δ is called a K-radical if $\Delta^n \in K$*; *τ-invariance means that $\Delta^\tau = \Delta$*).

§ 5. Henselian weakly ramified division algebras having unitary involutions

The main object of investigation in this section is a weakly ramified division algebra having unitary involutions. We assume below that k is a Henselian field, K/k is a quadratic separable extension, $D \in \mathrm{TR}(K)$ and $\tau \in \operatorname{Inv}_{K/k}(D)$ (so that $\operatorname{Inv}_{K/k}(D) \neq \varnothing$).

The structure of such K-algebras D can explicitly be described in terms of inertia algebras and generators with simple defining relations.

First, consider the case of unramified algebras D. The following assertion holds.

Lemma 10. *Let the algebra D be unramified over K and* $\operatorname{ind} D \neq 1$. *If $\operatorname{Inv}_{K/k}(D) \neq \varnothing$, then either the exponent of D equals* 2 *or K/k is unramified.*

Proof. Assume that the exponent of the algebra D is distinct from 2 and either $\overline{K} = \overline{k}$ or $\overline{K}/\overline{k}$ is purely inseparable. Then the restriction $\overline{\tau}|_{\overline{K}}$ is the identity map. Since the reduction $\overline{\tau}$ is an involution of the algebra $\overline{D}$ with trivial restriction to $\overline{K}$ and $\operatorname{ind} \overline{D} \neq 1$, the exponent of $\overline{D}$ equals 2. As soon as the algebra D is unramified over K, it has the same exponent as $\overline{D}$. This contradicts our assumption, and so either $\exp D = 2$ or K/k is unramified. The proof of the lemma is complete.

For algebras of odd indices we have the following.

Corollary 8. *Let the algebra D be unramified over K, and let* $\operatorname{ind} D$ *be odd. If $D \neq K$, then the extension K/k is unramified.*

Now let us describe the relation between the sets $\operatorname{Inv}_{K/k}(D)$ and $\operatorname{Inv}_{\overline{K}/\overline{k}}(\overline{D})$. To do this, note that we can introduce the following equivalence relation on the set $\operatorname{Inv}_{K/k}(D)$: two involutions $f_1, f_2 \in \operatorname{Inv}_{K/k}(D)$ are said to be equivalent ($f_1 \sim f_2$) if and only if their reductions $\overline{f_1}$ and $\overline{f_2}$ coincide.

The equivalence classes with respect to this relation are as follows.

Lemma 11. *For $f_1, f_2 \in \operatorname{Inv}_{K/k}(D)$* ($\operatorname{char} k \neq 2$) *the equivalence $f_1 \sim f_2$ holds if and only if there exists an element $m \in (1 + M_D) \cap S_{f_1}(D)K$ such that $f_2 = f_1 i_m$.*

Proof. First we show that $f_1 \sim f_2$ if and only if there exists an element $m \in (1 + M_D) \cap (S_{f_1}(D) \cup K_{f_1}(D))K$ such that $f_2 = f_1 i_m$, where $K_{f_1}(D) = \{d \in D\colon d^\tau = -d\}$. According to the above definition, $f_1 \sim f_2$ if and only if $\overline{f_1} = \overline{f_2}$. Since $f_1 f_2$ is a K-automorphism whose restriction to $\overline{D}$ is the identity map, by [43], Theorem 1, there exists an element $m \in (1 + M_D)$ such that $f_2 = f_1 i_m$. On the other hand, since f_1 and f_2 are K/k-involutions, we have $i_m = i_t$ for an appropriate $t \in S_{f_1}(D) \cup K_{f_1}(D)$, which yields the relation $m = st$, where $s \in K$. Note that $K_{f_1}(D) = \sqrt{\alpha}\, S_{f_1}(D)$, where $K = k(\sqrt{\alpha})$, $\alpha \in k$. Then by what we proved above we have $m \in (S_{f_1}(D) \cup \sqrt{\alpha}\, S_{f_1}(D))K$, that is, $m \in S_{f_1}(D)K$.

Conversely, if $f_2 = f_1 i_m$, then $\overline{f_1} = \overline{f_2}$, that is, $f_1 \sim f_2$. The proof is complete.

Remark 6. The claim of Lemma 11 can be refined in some special cases.

Suppose that $\operatorname{char} \overline{k} \neq 2$ and $\Gamma_K = \Gamma_k$. Note that $K_{f_1}(D) = \sqrt{\alpha}\, S_{f_1}(D)$ for some $\alpha \in U_k$. Taking the equality $K_{f_1}(D) = \sqrt{\alpha}\, S_{f_1}(D)$ into account we obtain $(S_{f_1}(D) \cup K_{f_1}(D))K = S_{f_1}(D)K$. Thus, we can assume that $f_2 = f_1 i_m = f_1 i_s$, where $m \in 1 + M_D$ and $s^{f_1} = s$. The fact that the automorphisms i_m and i_s coincide implies the equality $st = m$ for an appropriate $t \in K$. Since $\Gamma_K = \Gamma_k$, we can assume that $t = \pi_k u_K$ for $\pi_k \in k$ and $u_K \in U_K$. In view of the equality $m = st$ the element s has the form $\pi_k^{-1} u_s$, where $u_s \in U_D$, which yields $u_s^\tau = u_s$, and therefore we can assume from the very beginning that $s \in U_D$. Then it follows from the equality $su_K = m$ that $\overline{s}\,\overline{u_K} = 1$. Therefore, $\overline{s} \in \overline{K}$. Moreover, $\overline{s} \in \overline{k}$. However, in this case $\overline{u_K} \in \overline{k}$ as well. The element u_K has the form $u_K = u_k(1 + q)$ for some $u_k \in k$ and $q \in M_K$. Hence $m(1+q)^{-1} \in S_{f_1}(D)$. Therefore, $f_2 = f_1 i_{m(1+q)^{-1}} = f_1 i_{s\pi_k u_k}$. Thus, in the above definition of the equivalence of two involutions f_1 and f_2 it is sufficient to require that there exist an element $m \in (1 + M_D) \cap S_{f_1}(D)$.

Suppose as above that $\operatorname{char} \overline{k} \neq 2$ and Γ_k is a subgroup of index 2 in the group Γ_K and $K = k(\sqrt{\pi})$, where $\pi \in k$ and $v_k(\pi) \notin 2\Gamma_k$. Note that the element $v_K(\sqrt{\pi}) + \Gamma_k$ is a generator of the quotient group Γ_K/Γ_k. Since the algebra D/K is unramified, each element $d \in D$ has the form $\sqrt{\pi}^{\,n} u_d \delta_k$ for appropriate elements $u_d \in U_D$, $\delta_k \in k$ and $n \in \mathbb{Z}$. If $f_1 \sim f_2$, then by Lemma 11 there exists an element $m \in (1 + M_D) \cap S_{f_1}(D)K$ with the property that $f_2 = f_1 i_m$.

Let $m = st$, where $s \in S_{f_1}(D)$ and $t \in K$. It is easily seen that, as $v_D(m) = v_D(st) = 0$, we have $s = \sqrt{\pi}^{\,\beta} u_s \delta_s$ and $t = \sqrt{\pi}^{\,-\beta} u_t \delta_t$ for some $u_s \in U_D$, $u_t \in U_K$, $\delta_s, \delta_t \in k$ and $\beta \in \mathbb{Z}$.

Since $s \in S_{f_1}(D)$, depending on whether the integer β is even or odd, the element u_s has the property $u_s^{f_1} = \pm u_s$. Hence $m = st = \delta_s \delta_t u_t u_s$. Note that $\delta_s \delta_t u_t \in U_K$, and, passing to residues, we conclude that $\overline{u_s} \in \overline{K}$. Since $\overline{K} = \overline{k}$, we have $u_s = \delta_k(1 + p)$ for appropriate elements $\delta_k \in k$ and $1 + p \in 1 + M_D$. It is easy to see that $1 + p \in S_{f_1}(D) \cup K_{f_1}(D)$.

Since $i_{st} = i_{u_s} = i_{1+p}$, where $1 + p \in (1 + M_D) \cap (S_{f_1}(D) \cup K_{f_1}(D))$, there exists $n \in (1 + M_D) \cap (S_{f_1}(D) \cup K_{f_1}(D))$ such that $f_2 = f_1 i_n$.

Remark 7. The above considerations show that when $\operatorname{char} \overline{k} \neq 2$, our equivalence relation coincides with the one introduced in [43].

Let us make one more useful observation. Note that when passing to reductions the equivalence relation induces a mapping μ_D of the quotient space $\overline{\mathrm{Inv}_{K/k}(D)}$: $\mu_D\colon \overline{\mathrm{Inv}_{K/k}(D)} \to \mathrm{Inv}_{\overline{K}/\overline{k}}(\overline{D})$.

It is easily seen that μ_D is injective.

As for the surjectivity of μ_D, under sufficiently weak constraints on the extension K/k we establish the following theorem, in which we do not assume that $\operatorname{char}\overline{k} \neq 2$.

Theorem 10. *Let the algebra D be unramified over K and the extension $\overline{K}/\overline{k}$ be not purely inseparable. Then μ_D is a bijection.*

Remark 8. This theorem refines Theorem 2 in [43], where the same is proved in the case when $\operatorname{char}\overline{k} \neq 2$. Thus, below we also consider the case $\operatorname{char}\overline{k} = 2$.

Our proof uses the following two assertions.

Lemma 12. *Let $D \in \mathrm{TR}(K)$. Assume also that D has an involution τ and $\langle \tau|_K \rangle = \mathrm{Gal}(K/k)$. Then for each $\overline{\tau}$-invariant separable extension $\widetilde{Z}/\overline{K}$ the algebra D contains its unramified τ-invariant lift Z/K.*

Proof. If $\widetilde{Z} = \overline{K}$, then we can set $Z = K$.

Now, let $\widetilde{Z} \neq \overline{K}$ and $K_\tau = k$. Define an element $\widetilde{\beta} \in \widetilde{Z}$ in the following way: if K/k is unramified, then let $\widetilde{Z}_{\overline{\tau}} = \overline{k}(\widetilde{\beta})$. Otherwise, let $\overline{k}(\widetilde{\beta})/\overline{k}$ be the maximal separable subextension of the extension $\widetilde{Z}/\overline{k}$. Let β be the inverse image of $\widetilde{\beta}$ in D and let

$$E = \begin{cases} k(\beta + \beta^\tau) & \text{if } \operatorname{char}\overline{k} \neq 2, \\ k(\beta\beta^\tau) & \text{if } \operatorname{char}\overline{k} = 2. \end{cases}$$

Evidently, $\tau|_E = \mathrm{id}$. Let $N(E)$ be the maximal subfield of E unramified over k. Since $\overline{E} = \overline{N(E)}$, we have $\widetilde{\beta} \in \overline{N(E)}$. Indeed, if $\operatorname{char}\overline{k} \neq 2$, then $\overline{\beta + \beta^\tau} = 2\widetilde{\beta} \in \overline{N(E)}$, and in the case when $\operatorname{char}\overline{k} = 2$ we have $\widetilde{\beta}^2 = \overline{\beta}\,\overline{\beta}^{\tau} \in \overline{N(E)}$ and, moreover, in this case $\overline{k}(\widetilde{\beta}^2) = \overline{k}(\widetilde{\beta})$, since $\overline{k}(\widetilde{\beta})$ is at the same time purely inseparable and separable over $\overline{k}(\widetilde{\beta}^2)$. It is clear that the field $\overline{k}(\widetilde{\beta})$ lifts to $N(E)$ as an unramified extension $\widehat{Z}/k$. Now set $Z = \widehat{Z}K$. The proof is complete.

Lemma 13. *Let L/K be an unramified extension of Henselian fields with an involution τ, $\tau|_K \neq \mathrm{id}$ and $k = K_\tau$. If $\operatorname{char} k \neq 2$, then let $K = k(\sqrt{\alpha})$, and if $\operatorname{char} k = 2$, then let $K = k(\beta)$, where β is a root of a polynomial of the form $x^2 + x + b$, $b \in k$, which is irreducible over k. Let N/k be the maximal subextension of L/k unramified over k. Then the following possibilities hold for the extension L/L_τ.*

(i) *If K/k is unramified, then L/L_τ is unramified too.*

(ii) *If K/k is weakly totally ramified, then for $\tau|_N = \mathrm{id}$ the extension L/L_τ is weakly totally ramified. Otherwise L/L_τ is unramified.*

(iii) *If K/k is not weakly ramified, then for $\tau|_N \neq \mathrm{id}$ the extension L/L_τ is unramified. If $\tau|_N = \mathrm{id}$, then L/L_τ is not weakly ramified.*

The proof of the lemma consists in routine computations in the theory of Henselian Galois extensions and we leave it the reader as a simple exercise.

Proof of Theorem 10. In view of Remark 8 we can limit our considerations to the case when $\operatorname{char}\overline{k} = 2$.

Suppose that the algebra $\overline{D}$ has a $\overline{K}/\overline{k}$-involution $\widetilde{\tau}$. Then the argument of Theorem 2 in [43], which does not depend on the characteristic of $\overline{k}$, immediately establishes the existence of a K/k-involution σ of the algebra D. Since σ

is a K/k-involution, we have $\overline{\sigma}|_{\overline{K}} = \widetilde{\tau}|_{\overline{K}}$. Therefore, there exists an appropriate $\overline{\sigma}$-invariant element $\widetilde{h}$ such that $\overline{\sigma} = \widetilde{\tau} i_{\widetilde{h}}$. Consider the field $\overline{K}(\widetilde{h})$. We can assume that $\widetilde{h} \notin \overline{K}$. Otherwise $\widetilde{\tau}$ lifts to an involution σ. By Lemma 12 there is an unramified lift of the field $\overline{K}(\widetilde{h})$ to F that does not coincide with K. Now if we show that the element $\widetilde{h}$ is lifted to a σ-invariant element h of F, then the involution σi_h^{-1} is the lift of $\widetilde{\tau}$. To establish the existence of such h consider two cases: F/F_σ is not weakly ramified and F/F_σ is weakly ramified.

Let F/F_σ be not weakly ramified. Then by Lemma 13 the involution σ acts trivially on the maximal unramified subextension N/k of the extension F/k. Indeed, if we assume that $\sigma|_N \neq \mathrm{id}$, then by Lemma 13 the extension F/F_σ is unramified, which contradicts our assumption that F/F_σ is not weakly ramified. Note that, by the hypothesis of the theorem, $\overline{K}/\overline{k}$ is not purely inseparable and $\overline{N} = \overline{F}_{\overline{\sigma}}$ (since $\overline{N} \subset \overline{F}_{\overline{\sigma}}$). Hence the separability of the extension $\overline{F}/\overline{K}$ implies the separability of the extension $\overline{F}/\overline{k}$, which, in turn, yields $[\overline{F} : \overline{N}] = 1$, that is, $\overline{F}_{\overline{\sigma}} = \overline{N}$. Therefore, $\widetilde{h} \in \overline{N}$ and denoting the lift of the element $\widetilde{h}$ to the field N by h we obtain the required result.

Now consider the case of a weakly ramified extension F/F_σ. Let h be the lift of the element $\widetilde{h}$ to the field F. As $\widetilde{h}$ is $\overline{\sigma}$-invariant, we have $h^\sigma = h(1+m)$. We apply σ to both sides of the last equality and substitute the element $h(1+m)$ for h^σ. Then $h = (1+m)^\sigma h(1+m)$. Note that h and h^σ commute, so h and $(1+m)$ also commute. The last equality implies the relation $(1+m)^\sigma(1+m) = 1$, which is equivalent to $N_{F/F_\sigma}(1+m) = 1$. Hence, by Hilbert's Theorem 90 and the fact that the extension F/F_σ is weakly ramified we have $1+m = (1+p)^{\sigma-1}$ for an appropriate element $p \in M_F$. Taking the element $h(1+p)^{-1}$ as h we obtain the required result. Therefore, the mapping μ_D is surjective. The proof is complete.

Now we prove the following refinement of Corollary 8.

Theorem 11. *Let $D \in \mathrm{TR}(K)$ be an algebra of odd index and let $\tau \in \mathrm{Inv}_{K/k}(D)$. Then $D = K$ if $\overline{D}$ is a field and K/k is unramified if $\overline{D}$ is not a field.*

The proof of this theorem is based on the following assertions.

Lemma 14. *Let D be a totally ramified noncommutative algebra. Then any subfield L of the algebra D containing K is totally ramified over K. Moreover, the centralizer $C_D(L)$ is totally ramified.*

Proof. It is sufficient to apply the 'fundamental inequality' (1.1) from [36] and take into account that the algebra D is totally ramified over K. Indeed, since $[D : C_D(L)][C_D(L) : L][L : K] = [\Gamma_D : \Gamma_{C_D(L)}][\Gamma_{C_D(L)} : \Gamma_L][\Gamma_L : \Gamma_K]$, $[D : C_D(L)] \geqslant [\Gamma_D : \Gamma_{C_D(L)}]$, $[C_D(L) : L] \geqslant [\Gamma_{C_D(L)} : \Gamma_L]$ and $[L : K] \geqslant [\Gamma_L : \Gamma_K]$, all inequalities are in fact equalities, as required. The proof is complete.

Lemma 15. *Let the algebra D have an odd index and be weakly ramified over K. Then:*

(i) *any subfield L/K of D containing K and the centralizer $C_D(L)$ are weakly ramified over K and L, respectively;*

(ii) *any τ-invariant extension L of the field K is contained in a maximal τ-invariant subfield M_L.*

Proof. The proof of (i) is similar to the proof of Lemma 14 and is based on dimension considerations. Part (ii) is proved using induction on $\operatorname{ind} D$. First, suppose that $\operatorname{ind} D$ is a prime number. Then the claim of the lemma is evidently true. If $\operatorname{ind} D$ is composite, then we consider a noncentral τ-invariant element s and see that either $L(s)/K$ is maximal (and τ-invariant), or $C_D(L(s)) \neq L(s)$ and the index of $C_D(L(s))$ is less than that of the algebra $C_D(L)$. Repeating this step several times (if necessary) we obtain a tower of τ-invariant subfields in D, which starts with L and ends with a maximal τ-invariant subfield. The proof is complete.

Lemma 16. *Suppose that the extension K/k is not unramified. If* $\operatorname{ind} D$ *is odd*, D *is totally ramified and $\tau \in \operatorname{Inv}_{K/k}(D)$, then $D = K$.*

Proof. Assume the opposite. We can assume that D has a p-primary index. Next, by Theorem 9 we can assume that D is a symbol algebra, say, $D = A(a, b, K, \varepsilon_{p^m})$ with τ-invariant canonical generators A and B, where $\varepsilon_{p^m} \in K$ is a primitive p^mth root. As $D \in \mathrm{TR}(K)$ and $\operatorname{ind} D$ is primary, we have $(\operatorname{char} \overline{k}, p) = 1$. If $\varepsilon_{p^m} \notin k$, then the extension K/k must be unramified by Lemma 8, which is not the case by assumption. And if $\varepsilon_{p^m} \in k$, then the central k-algebra $\langle A, B, \varepsilon_{p^m} \rangle$ has an involution that acts trivially on k, and therefore its index is not greater than 2. On the other hand, the index of D is odd, which yields $D = K$. The proof is complete.

Proof of Theorem 11. We can assume that $\operatorname{ind} D$ is p-primary, since instead of τ we can consider $\mu \in \operatorname{Inv}_{K/k}(D)$ such that the primary components of the algebra D are μ-invariant.

Assume that the extension K/k is not unramified. Then $\overline{\tau}|_{\overline{K}} = \mathrm{id}$. By Corollary 8 we can assume that the K-algebra D is not unramified over K. Since the degree $[Z(\overline{D}) : \overline{K}]$ is odd, we have $\overline{\tau}|_{Z(\overline{D})} = \mathrm{id}$.

First, suppose that $\overline{D}$ is not a field. Then $\overline{\tau}|_{\overline{D}} \neq \mathrm{id}$, but $\overline{\tau}|_{Z(\overline{D})} = \mathrm{id}$. Therefore, $\exp D \leqslant 2$. On the other hand $\operatorname{ind} D$ is odd. Consequently, $\exp D = 1$.

Now suppose that $\overline{D}$ is a field and $\operatorname{ind} D = p$. If $\overline{D} = Z(\overline{D})$, then by Lemma 16 we have $D = K$, which contradicts the condition $\operatorname{ind} D = p$. Let $\overline{D} \neq \overline{K}$. As D/K is weakly ramified, $\overline{D}$ is a cyclic extension of degree p of the field $\overline{K}$. Let $Z(\overline{D})_s$ be the maximal subfield of $Z(\overline{D})$ separable over $\overline{k}$. It is evident that $Z(\overline{D})_s/\overline{k}$ is a cyclic extension of degree p. By Theorem 8 $Z(\overline{D})_s/\overline{k}$ lifts to the k-algebra D as an unramified τ-invariant cyclic extension X/k. Let $\widetilde{\beta}$ be a primitive element of the extension $\overline{X}/\overline{k}$ and β be its inverse image in X. Denote by $f_\beta(x)$ the minimal polynomial of β in the extension X/k. Since at the same time β is a primitive element of the extension XK/K, we have $\beta^\tau = g\beta g^{-1}$ for some $g \in D$. Therefore, $\beta^\tau(g + g^\tau) = (g + g^\tau)\beta$. In the case when $g + g^\tau = 0$ we set $\mu = \tau i_{g^{-1}}$. In the case when $g + g^\tau \neq 0$ we set $\mu = \tau i_{(g+g^\tau)^{-1}}$. Then $\mu \in \operatorname{Inv}_{K/k}(D)$ and $\beta^\mu = \beta$. Passing to the involution μ allows us to assume without loss of generality that the compositum XK has the form $X \otimes_k K$ and $\tau|_X = \mathrm{id}$.

Clearly, D is a cyclic algebra with maximal subfield $Z = X \otimes_k K$. It is evident that if φ is a generator of the Galois group $\operatorname{Gal}(X/k)$, then $\varphi \otimes_k \mathrm{id}$ is a generator of the Galois group $\operatorname{Gal}(Z/K)$. Let $\Gamma \in D$ have the property $i_\Gamma|_X = \varphi$. Set $\gamma = \Gamma^p$. Then $D = (Z, \varphi \otimes_K \mathrm{id}, \gamma)$. By Theorem 4, for the existence of a unitary involution that acts trivially on X it is necessary that the identity $\gamma\gamma^\tau = N_{X/k}(x)$ be satisfied for an appropriate $x \in X$. Without loss of generality we can assume that $\gamma \in V_K$. Let us show that then $\gamma \in M_K$. Indeed, let $\gamma \in U_K$. Then $\Gamma \in U_D$ and $\Gamma\beta\Gamma^{-1} = \beta^{\varphi}$. Passing to residues $\overline{\Gamma}\,\overline{\beta}\,\overline{\Gamma}^{-1} = \overline{\beta^{\varphi}} = \overline{\beta}^{\overline{\varphi}}$ gives a contradiction, since $\overline{D}$ is a field and $\overline{\beta} \neq \overline{\beta}^{\overline{\varphi}}$. Consequently, $\gamma \in M_K$. Note that $v_K(\gamma) \notin p\Gamma_K$. Indeed, let $v_K(\gamma) = pv_K(\delta)$ for some $\delta \in K$. Consider the element $\gamma\delta^{-p} \in U_K$. Since $D = (Z, \varphi \otimes_K \mathrm{id}, \gamma\delta^{-p})$, we arrive at the case $\gamma \in U_K$, which we have already considered. As the extension X/k is unramified, we have $v_K(N_{X/k}(x)) \in p\Gamma_K$. Since $(2,p) = 1$ and $v_K(\gamma) \notin p\Gamma_K$, we obtain $v_K(\gamma\gamma^{\tau}) = 2v_K(\gamma) \notin p\Gamma_K$, which gives a contradiction again. Therefore, there exists no algebra of odd prime index p with a K/k-involution.

Now we use induction on $\operatorname{ind} D$. Let D be a noncommutative K-algebra of index p^r $(r > 1)$ such that $\overline{D}$ is a field and suppose that there exist no weakly ramified algebras of index less than p^r, $r > 1$, with commutative residue algebras. Recall that $Z(\overline{D}) \neq \overline{K}$. Again, let $Z(\overline{D})_s$ be the maximal separable subextension of the extension $Z(\overline{D})/\overline{k}$. Then $Z(\overline{D})_s/\overline{k}$ is a $\overline{\tau}$-invariant extension. By Lemma 12 as applied to the k-algebra D and extension $Z(\overline{D})_s/\overline{k}$, there exists a τ-invariant unramified lift $\widehat{Z}$ of the last extension. Since the degree of $Z(\overline{D})_s/\overline{k}$ is odd, $\overline{\tau}$ is the identity automorphism of $Z(\overline{D})_s/\overline{k}$. Consequently, $\tau|_{\widehat{Z}} = \mathrm{id}$. Since the extension $\widehat{Z}/k$ is unramified, it is Abelian (because the residue field of the field $\widehat{Z}$ is Abelian over $\overline{k}$). Let $\widetilde{Z_p}/\overline{k}$ be a subextension of $Z(\overline{D})_s/\overline{k}$ such that $\widetilde{Z_p}/\overline{k}$ is a cyclic extension of degree p. Consider the τ-invariant unramified lift Z_p/k of $\widetilde{Z_p}/\overline{k}$. It is clear that $\widetilde{Z_p}$ is $\overline{\tau}$-invariant, and therefore by Lemma 12 there exists an unramified τ-invariant lift Z_p of the extension $\widetilde{Z_p}/\overline{k}$. Then the centralizer $C_D(Z_pK)$ is τ-invariant and weakly ramified over Z_pK, $\operatorname{ind} C_D(Z_pK) = p^{r-1}$, and we arrive at a contradiction with the assumption that $r > 1$. The proof of the theorem is complete.

In the general case, from Lemma 12 we immediately obtain the following.

Corollary 9. *In the algebra $D \in \mathrm{TR}(K)$ there is an unramified τ-invariant lift Z/K of the field $Z(\overline{D})$.*

Indeed, in the formulation of Lemma 12 we have $\widetilde{Z} = Z(\overline{D})$. Since $D \in \mathrm{TR}(K)$ the field $\widetilde{Z}$ is a separable extension of the field $\overline{K}$.

The following result plays a key role in what follows.

Theorem 12. *The algebra D has a τ-invariant inertia algebra.*

Proof. By Corollary 9 the extension $Z(\overline{D})/\overline{K}$ is separable. Let Z be an unramified τ-invariant lift of $Z(\overline{D})/\overline{K}$, which exists by virtue of Lemma 12. We can apply Corollary 2.11 in [36] to the τ-invariant algebra $C_D(Z)$. Therefore, $C_D(Z) = I \otimes_Z T$, where I is an inertia algebra of $C_D(Z)$ and T is a totally ramified Z-algebra. If T is a field, then $T = Z$ and the statement of the theorem is true. Let us show that this condition is satisfied for $\operatorname{char} \overline{k} = 2$. Indeed, since $D \in \mathrm{TR}(K)$, the index of T is odd. Next, it follows from $\overline{D} = \overline{I}$ that $\overline{I}$ has an involution $\overline{\tau}$. Then $\overline{I}$ contains a maximal separable $\overline{\tau}$-invariant extension, which can be lifted to a maximal τ-invariant unramified extension L/Z in I by Lemma 12. Consider the extension $C_D(Z) \otimes_Z L$ isomorphic to the L-algebra $(I \otimes_Z L) \otimes_L (T \otimes_Z L)$. By [36], Theorem 3.1, the algebra $T \otimes_Z L$ is totally ramified, has an odd index and has an involution induced by the natural involution of the algebra $C_D(Z) \otimes_Z L$. By Theorem 11 we have $\operatorname{ind}(T \otimes_Z L) = 1$, which coincides with $\operatorname{ind} T$.

Thus, in what follows we can assume that $\operatorname{char}\overline{k} \neq 2$ and the algebra T is noncommutative. In the case when $I^\tau = I$ the theorem is proved. Now suppose that $I^\tau \neq I$. Making use of Theorem 10 we lift $\overline{\tau}$ to an involution of the algebra I, which can be extended to an involution s of D (Theorem 5). Since $s|_K = \tau|_K$, we have $s = \tau i_g$ for a certain $g \in S_\tau(D)$. Then $i_g|_Z\colon Z \to gZg^{-1} = gZ^\tau g^{-1} = Z^s$. Since $I^s = I$, we also have $Z^s = Z$, and therefore $i_g|_Z \in \mathrm{Gal}(Z/K)$. As $\tau s = i_g$, we have $\overline{\tau s} = \overline{i_g}$, which yields $\overline{i_g}|_{\overline{Z}} = \mathrm{id}_{\overline{Z}} \in \mathrm{Gal}(\overline{Z}/\overline{K})$. Since the extension Z/K is unramified, we have $\mathrm{Gal}(Z/K) \cong \mathrm{Gal}(\overline{Z}/\overline{K})$. Hence $i_g|_Z = \mathrm{id}_Z$. Consequently, $g \in C_D(Z)$ and $v(g) \in \Gamma_T$.

Let $g = un^\tau$, where $u \in U_D$, $n^\tau \in T$ (note that $\Gamma_T = \Gamma_{T^\tau}$) and $v(n) = v(g)$. Then for $i \in I$ we have $i^s = gi^\tau g^{-1} = un^\tau i^\tau n^{-\tau} u^{-1} = u(n^{-1}in)^\tau u^{-1} = ui^\tau u^{-1}$. Thus, since $\overline{s} = \overline{\tau}$ and $s|_I = \tau i_u|_I$, we also have $\overline{i_u} = i_{\overline{u}} = \mathrm{id}_{\overline{I}}$. Consequently, $u = u_z(1+m)$ for appropriate $u_z \in U_Z$ and $m \in M_D$. Evidently, we can now assume that $u = 1+m$. We apply s to both sides of the equality $i^s = ui^\tau u^{-1}$. Then $i = (ui^\tau u^{-1})^s$. Since $ui^\tau u^{-1} \in I$, we have $i = (ui^\tau u^{-1})^s = (ui^\tau u^{-1})^{\tau i_u} = (uu^{-\tau})i(uu^{-\tau})^{-1}$. Thus, $i = (uu^{-\tau})i(uu^{-\tau})^{-1}$ and therefore $uu^{-\tau} \in T$ (because $T = C_D(I)$).

Suppose that $\operatorname{char}\overline{k} \neq 2$. Then $\overline{u + u^\tau} = \overline{2}$ and so $u + u^\tau \in U_D$. Then $u + u^\tau = (t^{-1}+1)u$, where $t = uu^{-\tau}$. For $i \in I$ we have

$$i^s = (t^{-1}+1)^{-1} i^s (t^{-1}+1) = (t^{-1}+1)ui^\tau u^{-1}(t^{-1}+1)^{-1}.$$

But $(t^{-1}+1)u = u + u^\tau$. Hence

$$i^s = (u+u^\tau)i^\tau(u+u^\tau)^{-1} = \frac{u+u^\tau}{2} i^\tau \left(\frac{u+u^\tau}{2}\right)^{-1}.$$

It is clear that $\overline{((u+u^\tau)/2)} = \overline{1}$. Set $(u+u^\tau)/2 = 1+p$. Then $1+p \in (1+M_D)\cap S_\tau(D)$ and $i^s = (1+p)i^\tau(1+p)^{-1}$. Since the extension K/k is weakly ramified, the extension $K(1+p)/k(1+p)$ is too. Then the element $1+p$ is the value of some element $1+q \in 1+M_{K(1+p)}$, which means that $1+p = (1+q)(1+q)^\tau$. Set $J = (1+q)^{-1}I(1+q)$. Then

$$J^\tau = (1+q)^\tau I^\tau (1+q)^{-\tau} = (1+q)^\tau(1+p)^{-1}I^s(1+p)(1+q)^{-\tau} = (1+q)^{-1}I(1+q).$$

Hence J is a τ-invariant inertia algebra of the algebra D. The proof of the theorem is complete.

Theorem 12 can be improved by using the following two assertions.

Lemma 17. *Let A be a subalgebra of an F-algebra D with involution τ, let A be an unramified τ-invariant division F-algebra, let $F \subset Z(A)$, where $F^\tau = F$, and let $\widetilde{R}$ be a central $\overline{\tau}$-invariant $\overline{F}$-algebra such that $\overline{A} = \widetilde{R} \otimes_{\overline{F}} \widetilde{L}$, where $\widetilde{L}$ is a separable extension of the field $\overline{F}$. Then there exists an unramified τ-invariant lift of the $\overline{F}$-algebra $\widetilde{R}$ to A.*

Proof. By Theorem 8 the algebra A has the form $A = \widehat{R} \otimes_F L$, where $\widehat{R}$ is an unramified algebra over F with residue algebra $\widetilde{R}$ and L is a τ-invariant unramified extension of the field F. Suppose that $\widehat{R}^\tau \neq \widehat{R}$. We lift $\overline{\tau} \mid \widetilde{R}$ to an involution of the algebra $\widehat{R}$, which, in turn, can be extended to an involution s of the algebra A

by letting it act on L in the same way as τ. Since $s|_{Z(A)} = \tau|_{Z(A)}$, we have $s = \tau i_g$ for some $g \in A$. As the $Z(A)$-algebra A is unramified, we have $g = \pi_{Z(A)}u$, where $\pi_{Z(A)} \in M_{Z(A)}$ and $u \in U_A$. The rest of the proof repeats the argument in the proof of Theorem 12. More exactly, for an arbitrary $r \in \widehat{R}$ we have

$$r^s = gr^\tau g^{-1} = u\pi^\tau_{Z(A)} r^\tau \pi^{-\tau}_{Z(A)} u^{-1} = u(\pi^{-1}_{Z(A)} r \pi_{Z(A)})^\tau u^{-1} = ur^\tau u^{-1}.$$

In view of the equalities $\overline{s} = \overline{\tau}$ and $s|_{\widehat{R}} = \tau i_u|_{\widehat{R}}$ we have $\overline{i_u} = i_{\overline{u}}$ and therefore the last automorphism is the identity automorphism of the residue algebra of $\widehat{R}$. Consequently, $u = u_l(1+m)$ for some $u_l \in U_L$ and $m \in M_A$. Now it can clearly be assumed that $u = 1+m$. We apply s to both sides of the equality $r^s = ur^\tau u^{-1}$ and obtain $r = (ur^\tau u^{-1})^s$. Since $ur^\tau u^{-1} \in \widehat{R}$, we have $r = (ur^\tau u^{-1})^s = (ur^\tau u^{-1})^{\tau i_u} = (uu^{-\tau})r(uu^{-\tau})^{-1}$. Thus, $r = (uu^{-\tau})r(uu^{-\tau})^{-1}$, and therefore $uu^{-\tau} \in C_A(\widehat{R})$.

Since char $\overline{Z(A)} \neq 2$ and the residue of $u + u^\tau$ is $\overline{2}$, we have $u + u^\tau \in U_A$. Set $t = uu^{-\tau}$. Then $u + u^\tau = (t^{-1}+1)u$. Moreover,

$$r^s = (t^{-1}+1)^{-1} r^s (t^{-1}+1) = (t^{-1}+1)ur^\tau u^{-1}(t^{-1}+1)^{-1},$$

but $(t^{-1}+1)u = u + u^\tau$. Consequently,

$$r^s = (u+u^\tau)r^\tau(u+u^\tau)^{-1} = \frac{u+u^\tau}{2} r^\tau \left(\frac{u+u^\tau}{2}\right)^{-1}.$$

It is clear that $\overline{((u+u^\tau)/2)} = \overline{1}$. Set $(u+u^\tau)/2 = 1+p$. Then $1+p \in (1+M_A)\cap S_\tau(A)$,

$$r^s = (1+p)r^\tau(1+p)^{-1}.$$

Since the extension $Z(A)/Z(A)_\tau$ is weakly ramified, the extension $Z(A)(1+p)/Z(A)_\tau(1+p)$ is too. Then the element $1+p$ is the value of some element $1+q \in 1+M_{Z(A)(1+p)}$, which means that $1+p = (1+q)(1+q)^\tau$. Denote the algebra $(1+q)^{-1}\widehat{R}(1+q)$ by J. It is τ-invariant:

$$J^\tau = (1+q)^\tau \widehat{R}^\tau (1+q)^{-\tau} = (1+q)^\tau(1+p)^{-1}\widehat{R}^s(1+p)(1+q)^{-\tau} = (1+q)^{-1}\widehat{R}(1+q).$$

Hence J is a τ-invariant lift of the algebra $\widetilde{R}$ in A. The proof is complete.

Lemma 18. *Let A be an unramified division algebra, let $\tau \in \mathrm{Inv}_{K/k}(A)$, and let F be a τ-invariant subfield of the field $Z(A)$. Then for any $\overline{\tau}$-invariant algebra $\widetilde{S}$ that is a subalgebra of $\overline{A}$ such that $Z(\widetilde{S})$ is a separable extension of the field $\overline{F}$, there exists a τ-invariant unramified lift of the algebra $\widetilde{S}$ to the algebra A.*

Proof. Consider $\overline{Z(A)}Z(\widetilde{S})$, the $\overline{Z(A)}$-linear hull of the field $Z(\widetilde{S})$. Clearly, it is a $\overline{\tau}$-invariant extension of the field $\overline{Z(A)}$. Its centralizer in $\overline{A}$ is also $\overline{\tau}$-invariant. Hence $C_{\overline{A}}(\overline{Z(A)}Z(\widetilde{S})) = \widetilde{S} \otimes_{Z(\widetilde{S})} \overline{Z(A)}Z(\widetilde{S})$, which allows us to reduce the proof of the lemma to an application of Lemma 17. The lemma is proved.

Theorem 13. *Each $\overline{\tau}$-invariant $\overline{K}$-subalgebra $\widetilde{E} \subset \overline{D}$ such that the centre $Z(\widetilde{E})$ of $\widetilde{E}$ is separable over $\overline{K}$ has a τ-invariant unramified lift $\widehat{E} \subset D$ (over K).*

Proof. The proof of the theorem can be reduced to the case when D is an unramified K-algebra. Indeed, by Theorem 12 the algebra D contains a τ-invariant inertia algebra I. Denote the $Z(\overline{I})$-linear hull of the algebra $\widetilde{E}$ by $\widetilde{E'}$. Clearly, $\widetilde{E'} \subset \overline{I}$. Note that $Z(\widetilde{E'})$ is a separable extension of the field $Z(\overline{I})$ (as the compositum of the fields $Z(\widetilde{E})$ and $Z(\overline{I})$). Hence $Z(\overline{I})Z(\widetilde{E'}) \subset \widetilde{E'} \subset \overline{I}$. Now, instead of the algebra D consider the algebra I, which is unramified over $Z(I)$. First we establish the existence of an E'-unramified τ-invariant lift of $\widetilde{E'}$ to I (Lemma 18) and then the existence of an $\widehat{E}$-unramified τ-invariant lift to E' (Lemma 17). By Lemma 12 there exists a τ-invariant lift of the field $Z(\overline{I})Z(\widetilde{E})$ to I. Hence we arrive at the case when the K-algebra D is unramified over K.

In view of Lemma 12 the extension $Z(\widetilde{E})/\overline{K}$ has a τ-invariant unramified lift Z to the algebra D. By Theorem 8 the algebra $\widetilde{E}$ has an unramified lift E/K. Note that since $Z(E^\tau) = Z^\tau$ and $Z^\tau = Z$, the algebras E and E^τ have the same centre. We assume that $E^\tau \neq E$ and lift $\overline{\tau}$ to an involution of E (see [43]), which, in turn, can be extended to an involution s of the algebra D (Theorem 5). Since the involutions s and τ have the same restriction to K, we have $s = \tau i_g$ for an appropriate element $g \in D$. As the algebra D is unramified over K, we have $g = \pi_K u$, where $\pi_K \in K \setminus U_K$ and $u \in U_D$. The rest of the proof follows the lines of the proofs of Theorem 12 and Lemma 17. More exactly, for an arbitrary $e \in E$ we have

$$e^s = ge^\tau g^{-1} = u\pi_K^\tau e^\tau \pi_K^{-\tau} u^{-1} = u(\pi_K^{-1} e \pi_K)^\tau u^{-1} = ue^\tau u^{-1}.$$

Thus, since $\overline{s} = \overline{\tau}$ and $s|_E = \tau i_u|_E$, we also have $\overline{i_u} = i_{\overline{u}} = \mathrm{id}_{\overline{E}}$. Consequently, $u = u_z(1+m)$ for some $u_z \in U_Z$ and $m \in M_D$. Now it can obviously be assumed without loss of generality that $u = 1+m$. We apply s to both sides of the equality $e^s = ue^\tau u^{-1}$ and obtain $e = (ue^\tau u^{-1})^s$. Since $ue^\tau u^{-1} \in E$, we have $e = (ue^\tau u^{-1})^s = (ue^\tau u^{-1})^{\tau i_u} = (uu^{-\tau})e(uu^{-\tau})^{-1}$. Using the same argument as in the proof of Lemma 17 we obtain $uu^{-\tau} \in C_D(E)$. Moreover, it is easily seen that $u + u^\tau \in U_D$. Further, we have $(u+u^\tau)/2 = 1+p$, where $1+p \in (1+M_D) \cap S_\tau(D)$ and $e^s = (1+p)e^\tau(1+p)^{-1}$. Since the extension $K(1+p)/k(1+p)$ is weakly ramified, $1+p$ is the value of some element $1+q \in 1+M_{K(1+p)}$, which means that $1+p = (1+q)(1+q)^\tau$. Denote the algebra $(1+q)^{-1}E(1+q)$ by J. It is τ-invariant:

$$J^\tau = (1+q)^\tau E^\tau (1+q)^{-\tau} = (1+q)^\tau (1+p)^{-1} E^s (1+p)(1+q)^{-\tau} = (1+q)^{-1}E(1+q).$$

Hence J is a τ-invariant lift of the algebra $\widetilde{E}$ to D. The proof of the theorem is complete.

Let I be the τ-invariant inertia algebra of the algebra D. Then the centre Z of this algebra is τ-invariant and $(C_D(Z))^\tau = C_D(Z)$. Note that the algebra $C_D(Z)$ is defectless over Z, and therefore by Corollary 2.11 in [36] we have $C_D(Z) = T \otimes_Z I$, where T is totally ramified over Z. Since $C_D(Z)$ and I are τ-invariant, T is also τ-invariant (because $T = C_D(I)$).

One aim of this section is to carry over to weakly ramified algebras with unitary involutions the main fact about the structure of a finite weakly ramified extension of a Henselian field: each extension of this kind can be represented as a tower of totally ramified (radical) extensions of a maximal unramified subextension.

To formulate the main theorem about the decomposition into a τ-invariant radical tower over a τ-invariant inertia algebra I we find a system of generators of the algebra D that are roots of elements of $C_D(Z)$ that generate totally ramified extensions.

In the general case we also need information about the existence of outer automorphisms of the algebra $C_D(Z)$. Now let us say a few words about generalized dihedral groups.

Definition 8. Let n be an odd integer greater than 1. A group G of order $2n$ is called a *generalized dihedral group* if it has an Abelian subgroup H of order n and an element a of order 2 with the defining relations $aha^{-1} = h^{-1}$ for any $h \in H$.

It is easily seen that this definition can be reformulated in the following equivalent way.

Definition 9. Let n be an odd integer greater than 1. A group G of order $2n$ is called a *generalized dihedral group* if it has an Abelian subgroup H such that $[G : H] = 2$ and any element of $G \setminus H$ has order 2.

In this notation the following assertion holds.

Proposition 7. *Let $Z(\overline{D}) \neq \overline{K}$ and I be the τ-invariant inertia algebra for D. Then in D there exist an unramified τ-invariant Abelian extension Z/K (for example, $Z = Z(I)$) and a system of τ-invariant elements $\{\Pi_1, \dots, \Pi_r\} \subset M_D$ such that*

(i) $\overline{Z} = Z(\overline{D})$;

(ii) $Z = Z_1 \times \dots \times Z_r$ *(the direct compositum of $Z_1, \dots, Z_r$ over K), where Z_j/K is a τ-invariant cyclic extension with Galois group generated by $i_{\Pi_j}|_{Z_j}$, $j = 1, \dots, r$;*

(iii) $(\tau|_{Z_j} \circ i_{\Pi_j}|_{Z_j})^2 = \mathrm{id}_{Z_j}$, *that is, $\mathrm{Gal}(Z_j/k)$ is either a generalized dihedral group, or an Abelian group of exponent 2.*

Proof. Since the algebra I is τ-invariant and unramified over K, its centre $Z(I)$ has the same properties. Moreover, $\overline{Z(I)} = Z(\overline{D})$. Set $Z = Z(I)$. It is clear that $Z^\tau = Z$. Since the extension $Z(\overline{D})/\overline{K}$ is Abelian and Z/K is its unramified lift in D, Z/K is also Abelian and its Galois group is the cross product of the cyclic groups $\langle\varphi_j\rangle$, $j = 1, \dots, r$, where $\langle\varphi_j\rangle$ is the cyclic group generated by φ_j. By the Skolem-Noether theorem the automorphism φ_j can be extended to an inner automorphism i_{Π_j}; moreover, replacing φ_j by φ_j^{-1} (if necessary) we can assume that $\Pi_j \in M_D$.

Note that $\Pi_j^\tau = u_j\Pi_j$, where $u_j \in U_D$. Replacing Π_j (if necessary) by an appropriate element $\Pi_j v_j$, where $v_j \in U_Z$, allows one to assume without loss of generality that $u_j + 1 \in U_D$. Indeed, let $u_j + 1 \in M_D$ and let $(\Pi_j v_j)^\tau = w_j\Pi_j v_j$ for any $v_j \in U_Z$, where $w_j + 1 \in M_D$. Then $v_j^\tau \Pi_j^\tau = w_j \Pi_j v_j$. Since $\Pi_j^\tau = u_j\Pi_j$ and $\Pi_j v_j \Pi_j^{-1} = v_j^{\varphi_j}$, we obtain $v_j^\tau u_j = w_j v_j^{\varphi_j}$. Adding $v_j^{\varphi_j} + v_j^\tau$ to both sides of this equality gives $v_j^\tau(u_j + 1) + v_j^{\varphi_j} = (w_j + 1)v_j^{\varphi_j} + v_j^\tau$. Since $u_j + 1 \in M_D$ and $w_j + 1 \in M_D$, we have $v_j^{\varphi_j} = v_j^\tau + m$, where $m \in M_D$. This yields the equality $\overline{v_j}^{\overline{\varphi_j}} = \overline{v_j}^{\overline{\tau}}$. Now let $v_j \in U_{Z_\tau}$. Then $\overline{v_j}^{\overline{\varphi_j}} = \overline{v_j}$. Since $\overline{\varphi_j}$ is a nontrivial automorphism of the field $\overline{Z_\tau}$, this field contains an element $\widetilde{v_j}$ such that $\widetilde{v_j}^{\overline{\varphi_j}} \neq \widetilde{v_j}$. If v_j is the inverse image of $\widetilde{v_j}$ in Z_τ, then we arrive at a contradiction. Hence we may assume that $u_j + 1 \in U_D$.

Consider the restriction to $\overline{Z}$ of the reduction of the involution $\tau i_{\Pi_j^\tau+\Pi_j}$. Then

$$\overline{\tau i_{\Pi_j^\tau+\Pi_j}}|_{\overline{Z}} = \overline{\tau}|_{\overline{Z}}\,\overline{i_{\Pi_j^\tau+\Pi_j}}|_{\overline{Z}} = \overline{\tau}|_{\overline{Z}}\,\overline{i_{(u_j+1)\Pi_j}}{}_{\overline{Z}} = \overline{\tau}|_{\overline{Z}}(\overline{i_{\Pi_j}}|_{\overline{Z}}\,\overline{i_{u_j+1}}|_{\overline{Z}}).$$

Since $\overline{i_{u_j+1}}|_{\overline{Z}}$ is the identity mapping of $\overline{Z}$, the restriction of the reduction $\overline{\tau}|_{\overline{Z}}\,\overline{i_{\Pi_j}}|_{\overline{Z}}$ is an involution in $\mathrm{Gal}(Z(\overline{D})/\overline{k})$, which means that $(\overline{\tau}|_{Z(\overline{D})}\,\overline{\varphi}_j)^2 = 1$ or $\overline{\tau}_{Z(\overline{D})}\overline{\varphi}_j\overline{\tau}_{Z(\overline{D})} = \overline{\varphi}_j^{-1}$. Hence $\mathrm{Gal}(Z(\overline{D})/\overline{k})$ is either a generalized dihedral group in case $\overline{\tau}|_{Z(\overline{D})} \neq \mathrm{id}_{Z(\overline{D})}$, or an Abelian group of exponent 2.

If K/k is an unramified extension, then $\overline{\tau} \neq \mathrm{id}_{Z(\overline{D})}$, and therefore the Galois group $\mathrm{Gal}(Z/k)$ is a generalized dihedral group, since Z/k is an unramified lift of $Z(\overline{D})/\overline{k}$.

If the extension K/k is totally ramified, then $Z = Z_\tau \times K$ is the direct compositum of the fields Z_τ/k and K/k and therefore $\mathrm{Gal}(Z/k) = \mathrm{Gal}(Z_\tau/k) \times \mathrm{Gal}(K/k)$ is again a generalized dihedral group.

Consider the equality $\Pi_j z \Pi_j^{-1} = z^{\varphi_j}$, where $z \in Z$. We apply τ to both sides. Since $\mathrm{Gal}(Z/k)$ is a generalized dihedral group, we have

$$\Pi_j^{-\tau} z^\tau \Pi_j^\tau = z^{\varphi_j\tau} = z^{\tau\varphi_j^{-1}} = \Pi_j^{-1} z^\tau \Pi_j.$$

As $Z^\tau = Z$, we have $z = \Pi_j^\tau\Pi_j^{-1} z \Pi_j \Pi_j^{-\tau}$. Thus, $\Pi_j^\tau = c_j\Pi_j$, where $c_j \in C_D(Z) \cap U_D$. It is easily seen that $i_{\Pi_j+\Pi_j^\tau}|_Z = i_{\Pi_j}|_Z$, and thus we can assume without loss of generality that $\Pi_j^\tau = \Pi_j$.

Let Φ_j be the subgroup of $\mathrm{Gal}(Z/K)$ generated by the φ_i, $i \in \{1, 2, \ldots, r\} \setminus \{j\}$. Denote by Z_j the field of invariants of the group Φ_j. Then Z_j/K is a Galois extension with group $\langle \varphi_j|_{Z_j}\rangle$. Let us show that $Z_j^\tau = Z_j$. For $z \in Z_j$ and any $g \in \Phi_j$ we have $z^g = z$. Applying τ to both sides of the last equality gives $z^{g\tau} = z^\tau$. However, $g = \varphi_1^{\alpha_1} \cdots \varphi_r^{\alpha_r}$, where $\alpha_j = 0$. Then $z^{g\tau} = z^{\tau g^{-1}} = z^\tau$. As g runs through the group Φ_j, so does g^{-1} as well. Hence z^τ belongs to the field of invariants of the group Φ_j. Consequently, $Z_j^\tau \subseteq Z_j$. The inverse is evident. The proof of the proposition is complete.

Lemma 19. *Again, let* D, τ, I, Z *and* $\Pi_1, \ldots, \Pi_r$ *be as in Proposition* 7. *If* $C_D(Z) = T \otimes_Z I$ *and* $i_{\Pi_j}|_Z \in \mathrm{Gal}(Z/K)$, *then for any* $j \in \{1, 2, \ldots, r\}$ *there exists a* τ*-invariant element* Γ_j *such that* $I^{i_{\Gamma_j}} = I$ *and* $i_{\Gamma_j}|_Z = i_{\Pi_j}|_Z$.

Proof. Let $i_{\Pi_j}|_Z \in \mathrm{Gal}(Z/K)$. Consider the reduction of the involution τi_{Π_j}. This reduction lifts to an involution $\widehat{\mu}_j$ of the algebra I, which, in turn, can be extended to a K/k-involution μ_j of D. Then $\mu_j = \tau i_{\Gamma_j}$, where $\Gamma_j^\tau = \Gamma_j$. The elements $\Gamma_1, \ldots, \Gamma_r$ possess the required properties. The proof is complete.

Lemma 20. *If* $C_D(Z) = T \otimes_Z I$ *and* $i_{\Gamma_j}|_Z \in \mathrm{Gal}(Z/K)$, *then there exist* $\tau\varphi_j$*-invariant elements* $i_j \in I$ *and* $t_j \in T$ *such that* $\Gamma_j^{e_j} = t_j i_j$.

Proof. Let $i_{\Gamma_j}|_Z \in \mathrm{Gal}(Z/K)$ and $I^{i_{\Gamma_j}} = I$ (see Lemma 19). Then $i_{\Gamma_j^{e_j}}|_Z = \mathrm{id}_Z$. Hence $i_{\Gamma_j^{e_j}}|_I = i_{i_j}|_I$ for some $i_j \in I$. Consequently, $i_{\Gamma_j^{e_j} i_j^{-1}}|_I = \mathrm{id}_I$, and therefore $\Gamma_j^{e_j} = i_j t_j$, where $t_j \in C_D(I) = T$.

We show that we can choose t_j and i_j to be $\tau\varphi_j$-invariant. Indeed,

$$i_jt_j = \Gamma_j^{e_j} = (\Gamma_j^{e_j})^{\varphi_j^{-1}} = i_j^{\varphi_j^{-1}} t_j^{\varphi_j^{-1}} \quad \text{and} \quad i_jt_j = \Gamma_j^{e_j} = (\Gamma_j^{e_j})^{\tau} = i_j^{\tau} t_j^{\tau}.$$

The last equality implies that $i_j^\tau t_j^\tau = i_j^{\varphi_j^{-1}} t_j^{\varphi_j^{-1}}$. Applying τ to both sides gives $i_jt_j = i_j^{\varphi_j^{-1}\tau} t_j^{\varphi_j^{-1}\tau}$. However, $\varphi_j^{-1}\tau = \tau\varphi_j$. Consequently, $t_j^{\tau\varphi_j} t_j^{-1} = (i_j^{\tau\varphi_j})^{-1} i_j \in Z$.

Let $z_j = \delta_j^{\tau\varphi_j - 1}$, $\delta_j \in Z$. Then the elements $t_j\delta_j^{-1}$ and $i_j\delta_j$ are $\tau\varphi_j$-invariant. The proof is complete.

Note that by Theorem 9 any central algebra T which is totally ramified over Z has the form $T = \langle \Delta_1, \dots, \Delta_s, Z\rangle$, where Δ_i, $i = 1, \dots, s$, are τ-invariant radicals over $Z(I)$. Then the following assertions hold.

Theorem 14. *Let $Z(\overline{D}) \neq \overline{K}$ and let I be a τ-invariant inertia algebra of the algebra D. Then $D = \langle \Gamma_1, \dots, \Gamma_r, \Delta_1, \dots, \Delta_s, I\rangle$.*

Theorem 15. *Let $Z(\overline{D}) \neq \overline{K}$ and let I be a τ-invariant inertia algebra of the algebra D. Then $D = \langle \Gamma_1, \dots, \Gamma_r, C_D(Z(I))\rangle$.*

Corollary 10. *In the notation of Theorem 14 the following equalities hold*:

$$D^* = (\Gamma_1^{\alpha_1} \cdots \Gamma_r^{\alpha_r})(\Delta_1^{\beta_1} \cdots \Delta_s^{\beta_s}) I^*(1 + M_D),$$
$$V_D = (\Gamma_1^{\alpha_1} \cdots \Gamma_r^{\alpha_r})(\Delta_1^{\beta_1} \cdots \Delta_s^{\beta_s}) V_I(1 + M_D) \quad \textit{and} \quad U_D = U_I(1 + M_D).$$

These assertions are used to prove a stronger version of Theorem 12.

Theorem 16. *Let $D \in \mathrm{TR}(K)$ be a τ-invariant division algebra as in Lemma 12. Then for any τ-invariant subalgebra M in D unramified over K there exists a τ-invariant inertia algebra of D containing M.*

Proof. Suppose that D is a field. Since $D \in \mathrm{TR}(K)$ is a τ-invariant algebra and the extension M/K is unramified, M is contained in a maximal subextension N/K contained in D and unramified over K, which is an inertia algebra of D (over K). Finally, note that $N^\tau = N$ in view of the equality $D^\tau = D$. This completes the proof of the theorem in the case of a commutative algebra D.

Suppose that D is not a field. Let us show that we can limit our considerations to the case when $K = Z(D)$. Indeed, assume that K is distinct from $Z(D)$. Consider $MZ(D)$, the compositum of M and $Z(D)$ over K, which coincides with the $Z(D)$-linear hull of the field M. Then, as M and $Z(D)$ are τ-invariant unramified extensions of K, their compositum has the same properties. Now if we show that $MZ(D)$ is contained in a τ-invariant inertia algebra of the algebra D, then we can assume without loss of generality that $K = Z(D)$.

First suppose that $\overline{D}$ is a field. Note that in the case when $\overline{D} = \overline{K}$ we have $M = K$, and so the theorem is true in view of Theorem 12. Now suppose that $\overline{D} \neq \overline{K}$. Then by the commutativity of $\overline{D}$ we have $\overline{D} = Z(\overline{D})$, and thus $\overline{D} = Z(\overline{I})$, where I is a τ-invariant inertia algebra of D. Clearly, $Z(I)$ is a τ-invariant extension of the field K. By Lemma 12 there exists an intermediate field $\widetilde{M}$ ($K \subset \widetilde{M} \subset Z(I)$) which is τ-invariant and unramified over K and $\overline{\widetilde{M}} = \overline{M}$. In view of a $\overline{K}$-isomorphism between $\overline{M}$ and $\overline{\widetilde{M}}$ the fields M and $\widetilde{M}$ are K-isomorphic. We can assume that

$\widetilde{M}$ does not coincide with $Z(I)$. Otherwise M is a maximal subfield in D and the claim of the theorem obviously holds. Let us show that among the K-isomorphisms between the fields $\widetilde{M}$ and M there exists an isomorphism induced by an inner automorphism of the algebra D and specified by an element of $1+M_D$. Let $v \in D$ be such that the restriction of the automorphism i_v to $\widetilde{M}$ induces a K-isomorphism φ between $\widetilde{M}$ and M. Note that i_v also induces an isomorphism of $Z(I)$ onto $vZ(I)v^{-1}$ which is the lift of φ. Let $v = gu_Z\Pi$, where $g \in 1+M_D$ and $u_Z \in Z(I)$, and let Π be an appropriate product of powers of the elements $\Delta_1, \dots, \Delta_s$ and $\Gamma_1, \dots, \Gamma_r$ from Theorem 14. In view of the relation $vZ(I)v^{-1} = gZ(I)g^{-1}$ we obtain the desired K-isomorphism between $\widetilde{M}$ and M induced by i_g.

Assume that the claim of the theorem does not hold for an algebra M. Then we can assume that M is not contained in any larger τ-invariant algebra $\widehat{M}$ unramified over K. This assumption leads to a contradiction. Indeed, define an element $\widetilde{\beta} \in Z(\overline{I})$ as follows. If $\widetilde{M}/\overline{M}_\tau$ is unramified, then let $Z(\overline{I})_{\overline{\tau}} = \overline{\widetilde{M}}(\widetilde{\beta})$. Otherwise let $\overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta})/\overline{\widetilde{M}}_{\overline{\tau}}$ be the maximal separable subextension of the extension $Z(\overline{I})/\overline{\widetilde{M}}_{\overline{\tau}}$. It is easily seen that $\overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta})$ is a $\overline{\tau}$-invariant extension of $\overline{\widetilde{M}}_{\overline{\tau}}$. Denote the inverse image of $\widetilde{\beta}$ in $Z(I)$ by β and set

$$E = \begin{cases} \widetilde{M}_\tau(\beta + \beta^\tau) & \text{if } \operatorname{char} \overline{k} \neq 2, \\ \widetilde{M}_\tau(\beta \cdot \beta^\tau) & \text{if } \operatorname{char} \overline{k} = 2. \end{cases}$$

It is clear that $\tau|_E = \mathrm{id}$. Let $N(E)$ be the maximal subfield of E unramified over $\widetilde{M}_\tau$. Since $\overline{E} = \overline{N(E)}$, we have $\widetilde{\beta} \in \overline{N(E)}$. Indeed, in the case when $\operatorname{char} \overline{k} \neq 2$ we have $\overline{\beta + \beta^\tau} = 2\widetilde{\beta} \in \overline{N(E)}$, and in the case when $\operatorname{char} \overline{k} = 2$ we have $\widetilde{\beta}^2 = \overline{\beta}\,\overline{\beta^\tau} \in \overline{N(E)}$. Moreover, in this case $\overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta}^2) = \overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta})$, since $\overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta})$ is at the same time purely unseparable and separable over $\overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta}^2)$. Now it is clear that the field $\overline{\widetilde{M}}_{\overline{\tau}}(\widetilde{\beta})$ lifts to $N(E)$ as an unramified extension $Z(I)_\tau/\widetilde{M}_\tau$. This yields the relation $Z(I) = Z(I)_\tau\widetilde{M}$.

Let $\widetilde{\beta}$ be a primitive element of the unramified extension $Z(I)/\widetilde{M}$. Then the element β^{i_g} generates an unramified extension of M of degree $[Z(I) : \widetilde{M}]$. Put $s = \widetilde{\beta}^{i_g} + \widetilde{\beta}^{i_g\tau}$. Since $g \in 1+M_D$, we have $\overline{s} = 2\overline{\widetilde{\beta}}$ and therefore, for $\operatorname{char} \overline{k} \neq 2$ the extension $M(s)$ contains the field $\overline{M}(\overline{\widetilde{\beta}})$ as residues. Since $M(s)$ is τ-invariant, we arrive at a contradiction. And if $\operatorname{char} \overline{k} = 2$, then instead of the extension $M(s)$ we take the extension by the element $\widetilde{\beta}^{i_g}\widetilde{\beta}^{i_g\tau}$. Thus, we have dealt with the case when $\overline{D}$ is a field.

Now let $\overline{D}$ be not a field. We demonstrate that the claim of the theorem holds for algebras with prime indices. Since D is weakly ramified and $\overline{D}$ is not a field, D is an unramified algebra. Therefore, it is an inertia algebra of itself because its index is a prime number. This yields the validity of the theorem.

Let $\operatorname{ind} D$ be a composite integer and suppose that the theorem holds for subalgebras whose indices divide $\operatorname{ind} D$ and are less than $\operatorname{ind} D$. Since the indices of all subalgebras considered below are divisors of $\operatorname{ind} D$, the last condition reduces to the assumption that their indices are strictly less than $\operatorname{ind} D$. Now consider the possible cases for D and M one by one.

Recall that if $Z(M)/K$ is unramified, then $\overline{Z(M)} = Z(\overline{M})$ and the extension $Z(\overline{D})/\overline{K}$ is $\overline{\tau}$-invariant and separable. Moreover, if M^τ coincides with M, then $Z(M) = Z(M)^\tau$. Clearly, $Z(M) \subset C_D(M)$.

Note that M is contained in some inertia algebra A of the algebra D. Indeed, consider the algebra $\overline{M} \subset \overline{D}$. In view of Theorem 2.9 in [36] as applied to an arbitrary inertia algebra J of D and the algebra $\overline{M}$, there exists an unramified lift $\widetilde{M} \subset J$. By [36], Theorem 2.8, there exists an isomorphism between $\widetilde{M}$ and M, which can be extended to an automorphism φ of the algebra D by Theorem 5. Then J^φ is an inertia algebra of D containing the algebra M, and we have $M \subset J^\varphi$.

In the case when $A^\tau = A$ the claim of the theorem is proved. Suppose that $A^\tau \neq A$. In view of the inequality $[D : K] < \infty$ we can assume that the K-algebra M satisfies the following condition:

(a) *there exists no K-subalgebra $\widehat{M}$ of D that is distinct from M, contains M and is τ-invariant and unramified over K.*

Further, note that two cases are possible for the fields $Z(\overline{M})$ and $Z(\overline{D})$:

(1) $Z(\overline{M})Z(\overline{D}) = Z(\overline{M})$;

(2) $Z(\overline{D})Z(\overline{M}) \neq Z(\overline{M})$.

Suppose that M is not a field. Then the algebra $C_D(M)$ is noncommutative. Indeed, if $C_D(M)$ is a field, then $C_D(M) = Z(M)$, since otherwise the centre of the algebra $C_D(Z(M))$, which coincides with $C_D(M)$, is also distinct from $Z(M)$, which is not the case. Hence $C_D(M)$ is not a field.

Consider the centralizer of $C_D(Z(M))$ and apply Theorem 3.1 in [36] to the algebra D and the unramified extension $Z(M)/K$. Then we obtain $Z(\overline{C_D(Z(M))}) \cong Z(\overline{D})Z(\overline{M})$, and by our assumptions we have $Z(\overline{D})Z(\overline{M}) \neq Z(\overline{M})$. On the other hand, if the algebra $C_D(M)$ were totally ramified over $Z(M)$, then by [36], Proposition 1.4, we would have $\overline{C_D(Z(M))} = \overline{M}$. Thus, with due regard to the fact that $C_D(M)$ is τ-invariant and noncommutative, by Theorem 12 there exists a τ-invariant inertia algebra I of the algebra $C_D(M)$, which contradicts the maximality of M in the sense of condition (a) (it suffices to consider the I-hull of the algebra M).

Suppose that M is a field and case (2) takes place. Then the compositum $Z(\overline{D})Z(\overline{M})$ over $\overline{K}$ is separable. Denote a primitive element of this extension by $\widetilde{\alpha}$. Since $Z(M)$ is a τ-invariant extension of K, the $Z(M)$-algebra $C_D(Z(M))$ is also τ-invariant. By Lemma 12 there exists an element α of $C_D(Z(M))$ such that $\overline{\alpha} = \widetilde{\alpha}$ and the extension $Z(M)(\alpha)/Z(M)$ is τ-invariant and unramified. Since M is a field, we have $Z(M) = M$. Thus we have proved the existence of an extension $M(\alpha)$ that contains M strictly and does not coincide with D, which contradicts condition (a) for M. Hence we are in case (1). Thus, we can assume that $Z(\overline{M})Z(\overline{D}) = Z(\overline{M})$.

Let $Z \subset Z(M)$ be a τ-invariant lift of the extension $Z(\overline{D})/\overline{K}$ which is unramified over K (note that such an extension does exist due to the equality $Z(\overline{M})Z(\overline{D}) = Z(\overline{M})$). Let us show that Z can be assumed to be equal to K. Indeed, assume that $Z \neq K$. Consider the centralizer $C_D(Z)$. It is easily seen that the Z-algebra $C_D(Z)$ is a τ-invariant central algebra over Z. For this algebra there are *a priori* two cases depending on whether $C_D(Z)$ is commutative or noncommutative. In the first case we note that, since $Z \subset Z(M)$, we have $M \subset C_D(Z)$, and $C_D(Z)$, considered as a K-algebra, is an inertia algebra of D. Thus, we find ourselves in the framework of the earlier considerations for Z-algebras $C_D(Z)$ and M, where $\operatorname{ind} C_D(Z)$ divides $\operatorname{ind} D$. In the case when $C_D(Z)$ is noncommutative, it can be represented in the form $C_D(Z) = I \otimes_Z T$, where I is an inertia algebra of the algebra $C_D(Z)$ and T is a totally ramified subalgebra of $C_D(Z)$. It is clear that the index of $C_D(Z)$ divides $\operatorname{ind} D$. In other words, the product of the indices of T and I divides $\operatorname{ind} D$, which means that either $\operatorname{ind} I$ is less than $\operatorname{ind} D$ or these indices coincide. In the latter case D is unramified over K, and we arrive at the case considered above. If $\operatorname{ind} I < \operatorname{ind} C_D(Z)$, then, as the index of $C_D(Z)$ is less than that of D and $\operatorname{ind} I < \operatorname{ind} D$, we arrive at the case of subalgebras of smaller index, when it is sufficient to verify the theorem for divisors with prime indices (again, we find ourselves in the case of algebras of smaller indices, for which the inductive hypothesis holds true). Hence we can assume that $Z = K$.

Note that the theorem is true in the case when $\operatorname{char} \overline{k} = 2$. Indeed, since $D \in \mathrm{TR}(K)$, the index of T is odd. By Theorem 12 some inertia algebra I of D is τ-invariant. Then $D = I \otimes_K E$, where E is a totally ramified τ-invariant algebra over K. Now, applying Theorem 11 to E we obtain $\operatorname{ind} T = \operatorname{ind} E = 1$. Hence the algebra D is unramified, and therefore M is contained in a τ-invariant inertia algebra of D.

Now suppose that $\operatorname{char} \overline{k} \neq 2$. Then by virtue of [36], Corollary 2.11, D is the tensor product over K of some inertia algebra of D and a totally ramified central K-algebra. Since all inertia algebras are conjugate, it can be assumed without loss of generality that $D = A \otimes_K T$, where T is a totally ramified central K-algebra. Using Theorem 10 we lift $\overline{\tau}|_{\overline{A}}$ to an involution μ of A. Now we apply Theorem 5 to the algebra A with the involution μ and the subalgebra M with the involution $\tau|_M$ and conclude that there exists a K/k-involution δ of A such that $\delta|_M = \tau|_M$. Applying again Theorem 5 to D with the involution τ and the subalgebra A with the involution δ we see that there exists a K/k-involution $s\colon D \to D$ such that $s|_M = \tau|_M$. Since $s|_K = \tau|_K$, we have $s = \tau i_g$ for an appropriate element $g \in S_\tau(D)$. Moreover, $v_D(g) \in \Gamma_T$.

Now, as in the proof of Theorem 12, let $g = un^\tau$, where $u \in U_D$, $n^\tau \in T$ (note that $\Gamma_T = \Gamma_{T^\tau}$) and $v_D(n) = v_D(g)$. Then for $a \in A$ we have $a^s = ga^\tau g^{-1} = un^\tau a^\tau n^{-\tau} u^{-1} = u(n^{-1}an)^\tau u^{-1} = ua^\tau u^{-1}$. Since $\overline{s} = \overline{\tau}$ and $s|_A = \tau i_u|_A$, we also have $\overline{i_u} = i_{\overline{u}} = \mathrm{id}_{\overline{A}}$. Consequently, $u = u_z(1+m)$ for some elements $u_z \in U_{Z(A)}$ and $m \in M_D$. We can assume that $u = 1+m$. Applying s to both sides of the equality $a^s = ua^\tau u^{-1}$ gives $a = (ua^\tau u^{-1})^s$. Since $ua^\tau u^{-1} \in A$, we have $a = (ua^\tau u^{-1})^s = (ua^\tau u^{-1})^{\tau i_u} = (uu^{-\tau})a(uu^{-\tau})^{-1}$. Hence $a = (uu^{-\tau})a(uu^{-\tau})^{-1}$, and therefore $uu^{-\tau} \in T$ (because $T = C_D(A)$). Note that $\overline{u + u^\tau} = \overline{2}$, which yields $u + u^\tau \in U_D$. Set $t = uu^{-\tau}$. Then $u + u^\tau = (t^{-1}+1)u$. For any $a \in A$ we have $a^s = (t^{-1}+1)^{-1}a^s(t^{-1}+1) = (t^{-1}+1)ua^\tau u^{-1}(t^{-1}+1)^{-1}$. Next, in view of the equality $(t^{-1}+1)u = u + u^\tau$ we have

$$a^s = (u+u^\tau)a^\tau(u+u^\tau)^{-1} = \frac{u+u^\tau}{2}a^\tau\left(\frac{u+u^\tau}{2}\right)^{-1}.$$

It is clear that $\overline{((u+u^\tau)/2)} = \overline{1}$. Set $(u+u^\tau)/2 = 1+p$. Then $1+p \in (1+M_D) \cap S_\tau(D)$ and $a^s = (1+p)a^\tau(1+p)^{-1}$. As the extension K/k is weakly ramified, the extension $K(1+p)/k(1+p)$ is weakly ramified too. Then $1+p$ is the value of some element $1+q \in 1+M_{K(1+p)}$, which means that $1+p = (1+q)(1+q)^\tau$.

Let $I = (1+q)^{-1}A(1+q)$. Then

$$I^\tau = (1+q)^\tau A^\tau (1+q)^{-\tau} = (1+q)^\tau (1+p)^{-1} A^s (1+p)(1+q)^{-\tau} = (1+q)^{-1}A(1+q).$$

Hence I is a τ-invariant inertia algebra of the algebra D.

It follows from what we said above that $1+p$ commutes with elements of M. Evidently, all elements of the field $K(1+p)$ commute with elements of M, so $1+q$ also commutes with them. Consequently, $(1+q)^{-1}M(1+q) = M$, hence it is a subalgebra of the τ-invariant algebra I. The proof of Theorem 16 is complete.

Let $D \in \mathrm{TR}(K)$ and Z be a τ-invariant lift of $Z(\overline{D})$. Then $C_D(Z) = T \otimes_Z I$. In this notation the following proposition is valid.

Proposition 8. *If* $\operatorname{char} \overline{k} = 2$ *and the extension* Z/Z_τ *is not unramified, then* $\lambda_D = 1$.

Indeed, recall that the algebra T is τ-invariant and weakly totally ramified. Then the proposition follows from Corollary 2 since $\lambda_D = \lambda_{C_D(Z)} = \lambda_T$.

Another relevant assertion looks as follows.

Lemma 21. *If* $\operatorname{char} k \neq 2$, *while* $\operatorname{char} \overline{k} = 2$, *and* K/k *is not unramified, then* $\lambda_D = 1$.

Proof. First suppose that $Z(\overline{D}) = \overline{K}$. By [36], Corollary 2.11, we have $D = T \otimes_K I$, where the algebra T/K is totally ramified and I is an inertia algebra of D.

If $\overline{D}$ is a field, then $I = K$, and therefore $D = T$. This means that D is weakly totally ramified. Hence by Corollary 2 we have $D = K$, which yields $\lambda_D = 1$. If $\overline{D}$ is not a field, then let $\widetilde{E}$ be the maximal subfield of $\overline{D}$ separable over $\overline{K}$. Consider the maximal separable subextension $\widetilde{L}/\overline{k}$ of the extension $\widetilde{E}/\overline{k}$ and denote by L the unramified lift of $\widetilde{L}$ to the algebra I as a $\overline{k}$-algebra. The extension L/k does not contain K (since K/k is not weakly ramified). Let b be a primitive element of L/k. Since $[K(b) : K] = [k(b) : k]$, the coefficients of the minimal polynomial of b over K belong in fact to the field k. Hence $b^\tau = gbg^{-1}$ for an appropriate $g \in D$. Let us show that there exists an involution μ that has the same restriction to K as τ and satisfies $b^\mu = b$. Note that $b^\tau(g+g^\tau) = (g+g^\tau)b$. If $g + g^\tau = 0$, then we take $\mu = \tau i_{\sqrt{\alpha} g}$, where $\sqrt{\alpha} \in K$ and $(\sqrt{\alpha})^\tau = -\sqrt{\alpha}$ (recall that $\operatorname{char} k \neq 2$). If $g + g^\tau \neq 0$, then let $\mu = \tau i_{(g+g^\tau)^{-1}}$. In either case the element b is μ-invariant, so the field L is μ-invariant.

It is easily seen that KL is a maximal μ-invariant subfield of the algebra I. Indeed, KL is μ-invariant, because K and L are μ-invariant and their elements commute. Now, since $\overline{KL} = \widetilde{E}$ is a maximal subfield in $\overline{I}$, KL is a maximal subfield of I (because the algebra I is unramified over K). Thus, KL is a maximal μ-invariant subfield of I. It is clear that $C_D(KL) = T \otimes_K KL$ and $C_D(KL)$ is a μ-invariant weakly totally ramified KL-algebra. Since $\operatorname{char} \overline{k} = 2$ and $KL/(KL)_\mu$ is not unramified, by Corollary 2 we have $\operatorname{ind}(T \otimes_K KL) = 1$, which yields $\operatorname{ind} T = 1$.

Thus, in this case $D = I$ is an unramified K-algebra and therefore $\lambda_D = 1$.

Let $Z(\overline{D}) \neq \overline{K}$. Since the extension $Z(\overline{D})/\overline{K}$ is separable, there exists a maximal separable subextension $\widetilde{L}/\overline{k}$ of the extension $Z(\overline{D})/\overline{k}$. Denote the unramified lift of $\widetilde{L}$ to the algebra I as a $\overline{k}$-algebra by L. As above, note that K is not contained in L as the extension L/k is unramified. Using the same argument as above we show that there exists a central τ-invariant involution μ such that $L^\mu = L$. This, in turn, means that the compositum Z of the fields K and L over k is μ-invariant and, moreover, the extension Z/K is unramified and $\overline{Z} = Z(\overline{D})$. Hence $C_D(Z) = T \otimes_Z I$, where the algebra T/Z is totally ramified, the algebra I/Z is unramified and $\lambda_D = \lambda_{C_D(Z)}$. The centre $Z(\overline{C_D(Z)})$ coincides with $\overline{Z}$ and we arrive at the case considered at the beginning of the proof. Hence $\lambda_D = \lambda_{C_D(Z)} = 1$. The proof of the lemma is complete.

§ 6. The groups $U(D,\tau)$, $\mathrm{SU}(D,\tau)$, $\mathrm{SU}^v(D,\tau)$, $U(D,\tau)'$ and their reductions

In this section we describe the structure of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$. First we compute the reductions of the groups $U(D,\tau)$, $\mathrm{SU}(D,\tau)$, $U(D,\tau)'$ and $\mathrm{SU}^v(D,\tau) = \{d \in \mathrm{SU}(D,\tau) \mid N(\overline{d}) = 1\}$, where N denotes the composition $N_{Z(\overline{D})/\overline{K}} \circ \mathrm{Nrd}_{\overline{D}}$.

Below $D \in \mathrm{TR}(K)$, k is a Henselian field, and the extension K/k is weakly ramified (this is so in the case when $\mathrm{char}\,\overline{k} \neq 2$, which we assume below for definiteness). For brevity we write λ instead of λ_D.

Note that $\overline{Z} = \overline{Z(D)}$. Then the following proposition is valid.

Proposition 9. *The equality* $\overline{U(D,\tau)} = U(\overline{D},\overline{\tau})$ *holds and, for* $N = N_{\overline{Z}/\overline{K}} \circ \mathrm{Nrd}_{\overline{D}}$,

$$\overline{\mathrm{SU}(D,\tau)} = U(\overline{D},\overline{\tau}) \cap \overline{\mathrm{SL}(D)} = \{\widetilde{d} \in U(\overline{D},\overline{\tau}) \mid N(\widetilde{d})^\lambda = 1\}.$$

Proof. It is clear that $\overline{U(D,\tau)} \subseteq U(\overline{D},\overline{\tau})$, and therefore to prove the first claim of the proposition it is sufficient to establish the inverse inclusion. Let $\widetilde{d} \in U(\overline{D},\overline{\tau}) \cap \overline{\mathrm{SL}(D)}$ and let d be the inverse image of $\widetilde{d}$ in D. Then $dd^\tau = 1 + m$, where $m \in M_{K(dd^\tau)_\tau}$. Since $K(dd^\tau) = (K(dd^\tau))^\tau$, the extension $K(dd^\tau)/K(dd^\tau)_\tau$ is quadratic and separable. As $dd^\tau \in 1 + M_{K(dd^\tau)_\tau}$ and since the extension $K(dd^\tau)/k(dd^\tau)$ is weakly ramified, there exists an element $c \in 1 + M_{K(dd^\tau)}$ such that $N_{K(dd^\tau)/K(dd^\tau)_\tau}(c) = dd^\tau$. Hence $cc^\tau = dd^\tau$. Consequently, $c^{-1}d \in U(D,\tau)$ and $\overline{c^{-1}d} = \widetilde{d}$. Thus, $U(\overline{D},\overline{\tau}) \subseteq \overline{U(D,\tau)}$, which yields $\overline{U(D,\tau)} = U(\overline{D},\overline{\tau})$.

Let us show that $\overline{\mathrm{SU}(D,\tau)} \subset U(\overline{D},\overline{\tau}) \cap \overline{\mathrm{SL}(D)}$. To do this, note that $\overline{U(D,\tau)} \subset U(\overline{D},\overline{\tau})$ and $\overline{\mathrm{SL}(D)} = \{\widetilde{d} \in \overline{D} \mid N(\widetilde{d})^\lambda = 1\}$ (see, for example, [37]). In the case when $\overline{D}$ is a field we have $\overline{\mathrm{SL}(D)} = \{\widetilde{d} \in \overline{D} \mid N_{\overline{Z(D)}/\overline{K}}(\widetilde{d})^\lambda = 1\}$. Taking the residue $\overline{d} \in \overline{D}$ of an element $d \in \mathrm{SU}(D,\tau)$ gives the required inclusion.

Let us prove the reverse inclusion $\overline{SU(D,\tau)} \supset U(\overline{D},\overline{\tau}) \cap \overline{SL(D)}$. Suppose that $\overline{D}$ is not a field. By Theorem 12 there exists a τ-invariant inertia algebra I of D. Let $Z = Z(I)$. Then I is at the same time an inertia algebra of $C_D(Z)$. By what we established above, we have $\overline{U(I,\tau|_I)} = U(\overline{D},\overline{\tau})$. Let b be the inverse image of $\widetilde{d}$ in the group $U(I,\tau|_I)$. Since $\widetilde{d} \in U(\overline{D},\overline{\tau}) \cap \overline{\mathrm{SL}(D)}$, we have $N_{Z/K}(\mathrm{Nrd}_I(b))^\lambda = (1+m)^{\tau-1}$, where $m \in M_K$. As $(\lambda, \mathrm{char}\,\overline{k}) = 1$, we can assume that $1+m = (1+e)^\lambda$, $e \in M_K$. Then $N_{Z/K}(\mathrm{Nrd}_I(b)) = (1+e)^{\tau-1}$. Recall that by virtue of Proposition 4 we have $\mathrm{Nrd}_D(1 + M_D) = 1 + M_K$. Moreover, the mapping $N_{Z/K} \circ \mathrm{Nrd}_I$ sends $1+M_I$ to $1+M_K$. Let $p \in M_I$ have the property $N_{Z/K}(\mathrm{Nrd}_I(1+p)) = 1+e$. Then $b(1+p)^{1-\tau} \in \mathrm{SU}(D,\tau)$ and $\overline{b(1+p)^{1-\tau}} = \widetilde{d}$. If $\overline{D}$ is a field, then the argument is similar. The proof of the proposition is complete.

Proposition 9 suggests a description of the reduction of the group $\mathrm{SU}^v(D,\tau)$.

Corollary 11. *The following equality holds*:

$$\overline{\mathrm{SU}^v(D,\tau)} = \{\widetilde{d} \in U(\overline{D},\overline{\tau}) \mid N(\widetilde{d}) = 1\} = U(\overline{D},\overline{\tau}) \cap \overline{\mathrm{SL}^v(D)}.$$

Here $\mathrm{SL}^v(D) = \{d \in \mathrm{SL}(D) \mid N(\overline{d}) = 1\}$.

Proof. The inclusion $\overline{\mathrm{SU}^v(D,\tau)} \subseteq \{\widetilde{d} \in U(\overline{D},\overline{\tau}) \mid N(\widetilde{d}) = 1\}$ follows from the definition of the group $\mathrm{SU}^v(D,\tau)$. Conversely, let $\widetilde{d} \in U(\overline{D},\overline{\tau})$ and $N(\widetilde{d}) = 1$. Then $N(\widetilde{d})^\lambda = 1$. By Proposition 9, in the group $\mathrm{SU}(D,\tau)$ we can find an inverse image of the element $\widetilde{d}$, which belongs in fact to $\mathrm{SU}^v(D,\tau)$. The proof of the corollary is complete.

Finally, let us establish the following lemma.

Lemma 22. *The equality* $\overline{U(D,\tau)'} = U(\overline{D},\overline{\tau})'$ *holds.*

Proof. The inclusion $\overline{U(D,\tau)'} \subseteq U(\overline{D},\overline{\tau})'$ is evident. Conversely, let $a, b \in U(\overline{D},\overline{\tau})$. Then by the argument used in the proof of Proposition 9 the elements a and b have inverse images $u, v \in U(D,\tau)$, respectively. It is clear that $uvu^{-1}v^{-1} \in U(D,\tau)'$ and $\overline{uvu^{-1}v^{-1}} = aba^{-1}b^{-1}$, which proves the reverse inclusion. The proof is complete.

Let $UK_1^{\mathrm{an}}(D,\tau) = U(D,\tau)/U(D,\tau)'$. Then, as above, we obtain $\overline{UK_1^{\mathrm{an}}(D,\tau)} \cong UK_1^{\mathrm{an}}(\overline{D},\overline{\tau})$.

Next, let $E = ((1 + M_D) \cap \mathrm{SU}(D,\tau))U(D,\tau)'/U(D,\tau)'$.

The group $\mathrm{SUK}_1^v(D,\tau) = \overline{\mathrm{SU}^v(D,\tau)}/(U(\overline{D},\overline{\tau}))'$ plays an important role below. Denote $E_\lambda = N(\overline{\mathrm{SU}(D,\tau)})$. Then we have the following lemma.

Lemma 23. *The following exact sequence holds*:

$$1 \to \mathrm{SUK}_1^v(D,\tau) \to \overline{\mathrm{SU}(D,\tau)}/(U(\overline{D},\overline{\tau}))' \to E_\lambda \to 1.$$

The group E_λ *is computed in the following way*:

(i) $E_\lambda = 1$ *if* K/k *is totally ramified*;

(ii) *if* K/k *is unramified, then*

$$E_\lambda = C_\lambda(\overline{K}) \cap N(\overline{D})^{\overline{\tau}-1}, \tag{6.1}$$

where $C_\lambda(\overline{K})$ *is the group of* λ*th roots of unity in* $\overline{K}$.

Proof. Note that $U(\overline{D},\overline{\tau})' \subseteq \overline{\mathrm{SU}^v(D,\tau)}$. Let $[\widetilde{a},\widetilde{b}]$, where $\widetilde{a}$, $\widetilde{b} \in U(\overline{D},\overline{\tau})$. By Proposition 9 the elements $\widetilde{a}$ and $\widetilde{b}$ have inverse images a and b in $U(D,\tau)$. Then $[a,b] \in \mathrm{SU}(D,\tau)$. Next, $\overline{[a,b]} = [\widetilde{a},\widetilde{b}]$. Moreover, $N([\widetilde{a},\widetilde{b}]) = N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}([\widetilde{a},\widetilde{b}])) = N_{\overline{Z}/\overline{K}}(1) = 1$. Thus, $[\widetilde{a},\widetilde{b}] \in \overline{\mathrm{SU}^v(D,\tau)}$. By definition $\overline{\mathrm{SU}^v(D,\tau)} \subset \overline{\mathrm{SU}(D,\tau)}$. Thus, we have a sequence of subgroups

$$U(\overline{D},\overline{\tau})' \subseteq \overline{\mathrm{SU}^v(D,\tau)} \subset \overline{\mathrm{SU}(D,\tau)}.$$

Since $\overline{\mathrm{SU}^v(D,\tau)}$ is the kernel of the restriction of the homomorphism N to $\overline{\mathrm{SU}(D,\tau)}$, we have $\overline{\mathrm{SU}(D,\tau)}/\overline{\mathrm{SU}^v(D,\tau)} \cong E_\lambda$, which gives the exact sequence of the lemma.

In the proof of (6.1) we consider two cases:

(i) K/k is totally ramified;

(ii) K/k is unramified.

Case (i). Consider the case of a totally ramified extension K/k. Then for $s \in \mathrm{SU}(D, \tau)$ we have $N(\overline{s}) = N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{s}))$, where we can assume without loss of generality that s belongs to $U(I, \tau|_I)$. We use Merkurjev's formula $\mathrm{Nrd}_I(U(I, \tau|_I)) = \mathrm{Nrd}_I(I)^{\tau-1}$ (see [44], Proposition 6.1) and obtain $\mathrm{Nrd}_I(s) = \mathrm{Nrd}_I(i)^{\tau-1}$, where $i \in I$. Passing to residues gives the equality $\overline{\mathrm{Nrd}_I(s)} = \mathrm{Nrd}_{\overline{D}}(\overline{s}) = \mathrm{Nrd}_{\overline{D}}(\overline{i})^{\overline{\tau}-1}$. Applying the homomorphism $N_{\overline{Z}/\overline{K}}$ to the right- and left-hand sides of this equality gives $N(\overline{s}) = N(\overline{i})^{\overline{\tau}-1}$. Since the restriction of $\overline{\tau}$ to $\overline{K}$ is the identity map, we have $N(\overline{s}) = 1$. This yields $E_\lambda = 1$.

Case (ii) Let $\varepsilon \in C_\lambda(\overline{K}) \cap N(\overline{D})^{\overline{\tau}-1}$ be a primitive μth root dividing λ. Then by the equality $(\lambda, \mathrm{char}\,\overline{k}) = 1$ the root ε has a unique inverse image $\widehat{\varepsilon}$ in K, which is a primitive μth root of unity. Note that, since $N_{\overline{K}/\overline{k}}(\varepsilon) = 1$, we have $N_{K/k}(\widehat{\varepsilon}) = 1 + m_K$, where $m_K \in M_K$. Further, $(1 + m_K)^\lambda = 1$, hence in view of the equality $(\lambda, \mathrm{char}\,\overline{k}) = 1$ we obtain $m_K = 0$. Therefore, $N_{K/k}(\widehat{\varepsilon}) = 1$ and so $\widehat{\varepsilon} = (\widehat{u})^{\tau-1}$. Denote the composition $N_{Z/K} \circ \mathrm{Nrd}_I$ by $\widehat{N}$. It follows from the equality $\varepsilon = N(d)^{\overline{\tau}-1}$ that $\widehat{\varepsilon} = \widehat{N}(\widehat{d})^{\tau-1}(1 + m_K)$, where $\widehat{d}$ is the inverse image of d in I. The last equality suggests that $N_{K/k}(1 + m_K) = (1 + n_K)^{\tau-1}$. Consequently, $\widehat{\varepsilon} = (\widehat{N}(\widehat{d})(1 + n_K))^{\tau-1}$. It is clear that $1 + n_K = N_{Z/K}(1 + v_K)$, where $v_K \in M_Z$. Because I/Z is unramified, this yields $1 + v_K \in \mathrm{Nrd}_I(I)$. Finally, we obtain $\widehat{\varepsilon} = \widehat{N}(i)^{\tau-1} = N_{Z/K}(\mathrm{Nrd}_I(i))^{\tau-1}$ for an appropriate $i \in I$. Using Merkurjev's formula $\mathrm{Nrd}_I(I)^{\tau-1} = \mathrm{Nrd}_I(U(I, \tau|_I))$ (see [44], Proposition 6.1) we obtain $N_{Z/K}(\mathrm{Nrd}_I(i))^{\tau-1} = N_{Z/K}(\mathrm{Nrd}_I(u))$ for some $u \in U(I, \tau|_I) \subset U(D, \tau)$. Note that the above argument is also valid when I is a field. Then Nrd_I is the identity mapping, and therefore $\mathrm{Nrd}_I(i)^{\tau-1} = i^{\tau-1} \in U(I, \tau|_I)$, which means that $\mathrm{Nrd}_I(i)^{\tau-1} = \mathrm{Nrd}_I(u)$ for $u \in U(D, \tau)$. In addition, we have $\mathrm{Nrd}_D(u) = N_{Z/K}(\mathrm{Nrd}_I(u))^\lambda = 1$, which means that $u \in \mathrm{SU}(D, \tau)$. This yields $C_\lambda(\overline{K}) \cap N(\overline{D})^{\overline{\tau}-1} \subset E_\lambda$.

Conversely, suppose that $e \in E_\lambda$. Then $e = N(\overline{s})$ for an appropriate $s \in \mathrm{SU}(D, \tau)$ (by Proposition 9). Since $e = N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{s}))$, where $s \in \mathrm{SU}(D, \tau)$, we have $s \in U(D, \tau)$ and $\overline{s} \in U(\overline{D}, \overline{\tau})$. Now let u be a preimage of $\overline{s}$ in $U(I, \tau|_I)$. It follows from Merkurjev's formula that $e \in N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{D}))^{\overline{\tau}-1}$. Moreover, $e^\lambda = (N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{s}))^{\overline{\tau}-1})^\lambda = \overline{\mathrm{Nrd}_D(s)} = 1$, which means that $e \in C_\lambda(\overline{K})$. Hence $E_\lambda \subset C_\lambda(\overline{K}) \cap N(\overline{D})^{\overline{\tau}-1}$.

The proof of the lemma is complete.

For the group $\mathrm{SUK}_1^v(D, \tau)$ we have the following result.

Proposition 10. *The following sequence is exact*:

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D}, \overline{\tau}) \to \mathrm{SUK}_1^v(D, \tau) \to \mathrm{Nrd}_{\overline{D}}(U(\overline{D}, \overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)}) \to 1.$$

Proof. Note that

$$\mathrm{Nrd}_{\overline{D}}(U(\overline{D}, \overline{\tau}) \cap \overline{\mathrm{SL}^v(D)}) = \mathrm{Nrd}_{\overline{D}}(U(\overline{D}, \overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)}).$$

Indeed, it is evident that

$$\mathrm{Nrd}_{\overline{D}}(U(\overline{D}, \overline{\tau}) \cap \overline{\mathrm{SL}^v(D)}) \subseteq \mathrm{Nrd}_{\overline{D}}(U(\overline{D}, \overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)}).$$

Conversely, if $d \in \mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)})$, then there exists $u \in U(\overline{D},\overline{\tau})$ such that $\mathrm{Nrd}_{\overline{D}}(u) = d$ and $N(u) = 1$, because $d \in \overline{\mathrm{SL}^v(D)}$.

Let us also show that the kernel of the restriction of the homomorphism $\mathrm{Nrd}_{\overline{D}}$ to the group $\overline{\mathrm{SU}^v(D,\tau)}$ is the group $\mathrm{SU}(\overline{D},\overline{\tau})$. Indeed, by Corollary 11 we have $\mathrm{SU}(\overline{D},\overline{\tau}) \subseteq \overline{\mathrm{SU}^v(D,\tau)}$. Evidently, $\mathrm{SU}(\overline{D},\overline{\tau})$ belongs to the kernel. On the other hand, let d be an element of this kernel. Then $\mathrm{Nrd}_{\overline{D}}(d) = 1$, and since $d \in \overline{\mathrm{SU}^v(D,\tau)}$, we have $d \in \mathrm{SU}(\overline{D},\overline{\tau})$. Thus,

$$\overline{\mathrm{SU}^v(D,\tau)}/\,\mathrm{SU}(\overline{D},\overline{\tau}) \cong \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SU}^v(D,\tau)}).$$

In addition, both groups $\overline{\mathrm{SU}^v(D,\tau)}$ and $\mathrm{SU}(\overline{D},\overline{\tau})$ contain the commutator subgroup $U(\overline{D},\overline{\tau})'$, and therefore (see Lemma 22) we have

$$\big(\overline{\mathrm{SU}^v(D,\tau)}/U(\overline{D},\overline{\tau})'\big)/\big(\mathrm{SU}(\overline{D},\overline{\tau})/U(\overline{D},\overline{\tau})'\big) \cong \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SU}^v(D,\tau)}).$$

To complete the proof of the proposition is remains to note that $\mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SU}^v(D,\tau)}) = \mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)})$. The proposition is proved.

Further, since $(U(\overline{D},\overline{\tau}))' \subset \mathrm{SU}(\overline{D},\overline{\tau}) \subset \overline{\mathrm{SU}(D,\tau)}$, we have the following evident short exact sequence:

$$\begin{aligned} 1 &\to \mathrm{SU}(\overline{D},\overline{\tau})/(U(\overline{D},\overline{\tau}))' \to \overline{\mathrm{SU}(D,\tau)}/(U(\overline{D},\overline{\tau}))' \\ &\to (\overline{\mathrm{SU}(D,\tau)}/(U(\overline{D},\overline{\tau}))')/(\mathrm{SU}(\overline{D},\overline{\tau})/(U(\overline{D},\overline{\tau}))') \to 1. \end{aligned}$$

From the isomorphism theorem we obtain

$$(\overline{\mathrm{SU}(D,\tau)}/(U(\overline{D},\overline{\tau}))')/(\mathrm{SU}(\overline{D},\overline{\tau})/(U(\overline{D},\overline{\tau}))') \cong \overline{\mathrm{SU}(D,\tau)}/\,\mathrm{SU}(\overline{D},\overline{\tau}).$$

Taking this into account we obtain the following exact sequence:

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \to \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \to 1.$$

Recall the formulation of Theorem 2.

Let $D \in \mathrm{TR}(K)$, *assume that* $\mathrm{char}\,\overline{k} \neq 2$, *and let* $\tau \in \mathrm{Inv}_{K/k}(D)$, *where the field* k *is Henselian. Then in the notation introduced above the following commutative diagram holds, in which the sequences in the rows and the column are exact*:

$$\begin{tikzcd}
 & & & 1 \arrow[d] & & \\
1 \arrow[r] & E \arrow[r] & \mathrm{SU}^v(D,\tau)/(U(D,\tau))' \arrow[r] & \mathrm{SUK}_1^v(D,\tau) \arrow[r] \arrow[d] & 1, & (1) \\
1 \arrow[r] & E \arrow[r] & \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \arrow[r] & \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \arrow[r] \arrow[d] & 1, & (2) \\
 & & & E_\lambda \arrow[d] & & \\
 & & & 1 & &
\end{tikzcd}$$

where $E = ((1 + M_D) \cap \mathrm{SU}(D,\tau))U(D,\tau)'/U(D,\tau)'$. *Moreover, the following sequences are also exact*:

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \mathrm{SUK}_1^{v}(D,\tau) \to \mathrm{Nrd}_{\overline{D}}(\overline{U(D,\tau)}) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^{v}(D,\tau)}) \to 1, \tag{3}$$

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \to \overline{\mathrm{SU}(D,\tau)}/\,\mathrm{SU}(\overline{D},\overline{\tau}) \to 1. \tag{4}$$

Proof of Theorem 2. Consider the homomorphism

$$\pi\colon\ \mathrm{SU}(D,\tau)/(U(D,\tau))' \to \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})'$$

defined by the following rule: for $s \in \mathrm{SU}(D,\tau)$ let $\pi(s(U(D,\tau))') = \overline{s}U(\overline{D},\overline{\tau})'$. It is clear that π is onto and its kernel by Lemma 22 coincides with the group E. By the isomorphism theorem we have $E \cong ((1+M_D)\cap \mathrm{SU}(D,\tau))/((1+M_D)\cap U(D,\tau)')$. Thus, we obtain the following exact sequence:

$$\begin{aligned} 1 &\to ((1+M_D)\cap \mathrm{SU}(D,\tau))/((1+M_D)\cap (U(D,\tau))') \\ &\to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})' \to 1. \end{aligned}$$

Combining all the above and taking due account of the relation $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)/E \cong \overline{\mathrm{SU}(D,\tau)}/U(\overline{D},\overline{\tau})'$, one easily establishes the validity of Theorem 2.

Remark 9. The group $\mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^{v}(D)})$ is computed with the use of the following subgroups of the groups $\overline{D}^{\,*}$:

$$\Sigma_{\mathrm{Nrd}_{\overline{D}}} = \mathrm{Nrd}_{\overline{D}}(\overline{D}^{\,*})_{\overline{\tau}} \quad \text{and} \quad \Sigma^1_{\mathrm{Nrd}_{\overline{D}}} = \{z \in \mathrm{Nrd}_{\overline{D}}(\overline{D}^{\,*}) \mid N_{\overline{Z}/\overline{K}}(z) \in \overline{k}\},$$

where $\overline{Z} = Z(\overline{D})$.

Proposition 11. *The following sequence is exact*:

$$1 \to \Sigma_{\mathrm{Nrd}_{\overline{D}}} \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}} \xrightarrow{\overline{\tau}-1} (\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1} \to 1.$$

Moreover, $\mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^{v}(D)}) = (\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1}$.

Proof. Let us prove that the sequence is exact. The mapping $\overline{\tau}-1$ is a homomorphism of the group $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}$ onto the group $(\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1}$. It is clear that $\mathrm{Ker}(\overline{\tau}-1) = \Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Indeed, if $x \in \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}$ and $x^{\overline{\tau}-1} = 1$, then $x \in S_{\overline{\tau}}(\overline{D})$, and therefore $x \in \Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Conversely, if $y \in \Sigma_{\mathrm{Nrd}_{\overline{D}}}$, then $y^{\overline{\tau}-1} = 1$ and also $N_{\overline{Z}/\overline{K}}(y) \in \overline{k}$, since $\overline{Z}/\overline{k}$ is a generalized dihedral (or Abelian) Galois extension. This implies the inclusion $y \in \mathrm{Ker}(\overline{\tau}-1)$. Hence $(\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1} \cong \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$.

In conclusion let us show that $\mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^{v}(D)}) = (\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1}$. In view of the relations $(\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1} \subset \mathrm{Nrd}_{\overline{D}}(\overline{D}^{\,*})^{\overline{\tau}-1}$ and $\mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) = \mathrm{Nrd}_{\overline{D}}(\overline{D}^{\,*})^{\overline{\tau}-1}$ for $\operatorname{char}\overline{k} \neq 2$ (see [44], Proposition 6.1) it is sufficient to prove that $(\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1} \subseteq \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^{v}(D)})$. Let the element $\widetilde{x} \in \overline{D}$ be such that $N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\widetilde{x})) \in \overline{k}$. Then $\mathrm{Nrd}_{\overline{D}}(\widetilde{x})^{\overline{\tau}-1} \in (\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1}$. Let x be an inverse image of $\widetilde{x}$ in D and consider the element $x^{\tau-1}(1+m)$, where $m \in M_D$. Note that $\overline{x^{\tau-1}(1+m)} = \widetilde{x}^{\overline{\tau}-1}$. It is clear that $N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(\overline{x^{\tau-1}(1+m)})) = 1$. We show that for some $m \in M_D$ we have $x^{\tau-1}(1+m) \in \mathrm{SL}^v(D)$. Indeed, $N(\overline{x^{\tau-1}(1+m)}) = N(\widetilde{x})^{\overline{\tau}-1} = \overline{1}$. Consider the chain of equalities $\overline{\mathrm{Nrd}_D(x^{\tau-1}(1+m))} = N(\overline{x^{\tau-1}(1+m)})^{\lambda_D} = \overline{1}$. Then $\mathrm{Nrd}_D(x^{\tau-1}(1+m)) = 1+p$, where $p \in M_K$, which yields $\mathrm{Nrd}_D(x^{\tau-1}) = 1+q$, where $q \in M_K$. Since $D \in \mathrm{TR}(K)$, the element $1+q$ is the reduced value of some element $1+c$, where $c \in M_D$. Then $\mathrm{Nrd}_D(x^{\tau-1}(1+c)^{-1}) = 1$. Hence $x^{\tau-1}(1+c)^{-1} \in \mathrm{SL}(D)$ and it is easily seen that $\mathrm{Nrd}_{\overline{D}}(\overline{x^{\tau-1}(1+c)^{-1}}) = \overline{1}$, which prove the inclusion $(\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1} \subseteq \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)})$.

Conversely, let $y \in \mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)})$. Then for an appropriate $d \in \overline{D}$ we have $y = \mathrm{Nrd}_{\overline{D}}(d)^{\overline{\tau}-1}$, and since $y \in \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)})$, it follows that $1 = N_{\overline{Z}/\overline{K}}(y) = N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(d)^{\overline{\tau}-1})$, Hence $N_{\overline{Z}/\overline{K}}(\mathrm{Nrd}_{\overline{D}}(d)) \in \overline{k}$. Then $\mathrm{Nrd}_{\overline{D}}(U(\overline{D},\overline{\tau})) \cap \mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)}) \subseteq (\Sigma^1_{\mathrm{Nrd}_{\overline{D}}})^{\overline{\tau}-1}$. The proof is complete.

It follows from Theorem 2 that the group E is quite important for computations. The group $\mathrm{SU}(D,\tau)$ is said to satisfy the congruence property if $E=1$. This is equivalent to the following condition.

Theorem 17 (congruence theorem). *Let $D \in \mathcal{D}(K)$ be a weakly ramified algebra and let $\tau \in \mathrm{Inv}_{K/k}(D)$. Then $(1+M_D) \cap \mathrm{SU}(D,\tau) \subset U(D,\tau)'$.*

Now we focus on several particular cases of Theorem 2.

(i) $E=1$. Then Theorem 2 implies that the following sequences are exact:

$$1 \to \mathrm{SUK}^{\mathrm{an}}_1(\overline{D},\overline{\tau}) \to \mathrm{SUK}^{v}_1(D,\tau) \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to 1, \tag{6.2}$$

$$1 \to \mathrm{SUK}^{v}_1(D,\tau) \to \mathrm{SUK}^{\mathrm{an}}_1(D,\tau) \to E_\lambda \to 1. \tag{6.3}$$

Consequently, $\mathrm{SUK}^{\mathrm{an}}_1(D,\tau)$ is the extension of the Abelian group $\mathrm{SUK}^{v}_1(D,\tau)$ by some subgroup of λth roots belonging to the field K, and $\mathrm{SUK}^{v}_1(D,\tau)$ is the extension of the group $\mathrm{SUK}^{\mathrm{an}}_1(\overline{D},\overline{\tau})$ by the group $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$.

(ii) $E_\lambda = 1$. In this case the following sequences are exact:

$$1 \to E \to \mathrm{SUK}^{\mathrm{an}}_1(D,\tau) \to \mathrm{SUK}^{v}_1(D,\tau) \to 1, \tag{6.4}$$

$$1 \to \mathrm{SUK}^{\mathrm{an}}_1(\overline{D},\overline{\tau}) \to \mathrm{SUK}^{v}_1(D,\tau) \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to 1. \tag{6.5}$$

(iii) $E = E_\lambda = 1$. Then the following sequence is exact:

$$1 \to \mathrm{SUK}^{\mathrm{an}}_1(\overline{D},\overline{\tau}) \to \mathrm{SUK}^{\mathrm{an}}_1(D,\tau) \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to 1. \tag{6.6}$$

§ 7. Congruence property for the groups $\mathrm{SU}(D,\tau)$. The case of commutative residue algebras

Let $D \in \mathrm{TR}(K)$ $(\mathrm{char}\,\overline{k} \neq 2)$, $\tau \in \mathrm{Inv}_{K/k}(D)$, and let Z be an unramified τ-invariant lift of the field $Z(\overline{D})$. Then $C_D(Z) = I \otimes_Z T$, where I is a τ-invariant inertia algebra and the algebra T is totally ramified over Z. Suppose also that $\overline{D}$ is a field.

To obtain the main result (Proposition 12) we establish two lemmas. In the first lemma $\overline{D}$ is not assumed to be a field.

Lemma 24. *Let $D \in \mathcal{D}(K)$ be a quaternion algebra, let $\tau \in \mathrm{Inv}_{K/k}(D)$ and $\varepsilon_2 \in \overline{k}$. Then $(1+M_D) \cap \mathrm{SU}(D,\tau) \subseteq U(D,\tau)'$.*

Proof. Since $\operatorname{char} k \neq 2$, there exists a quaternion algebra $A \in \mathcal{D}(k)$ such that $D = A \otimes_k K$ and τ is induced by the canonical involution on A and a nontrivial automorphism of the extension K/k (see [39] and [45]).

It was shown in [30] that $\mathrm{SU}(D,\tau)$ coincides with the set $\{x \otimes 1 \mid x \in \mathrm{SL}(A)\}$. By Proposition 1.3 in [30] for the group $G = \{a \in A^* \mid \mathrm{Nrd}_A(a) \in N_{K/k}(K)\}$, the surjective homomorphism $\pi\colon\ \mathrm{SU}(D,\tau) \to \mathrm{SL}(A)/G'$ defined by $x \otimes 1 \mapsto xG'$ induces an isomorphism between the groups $\mathrm{SU}(D,\tau)/U(D,\tau)'$ and $\mathrm{SL}(A)/G'$. Hence, to establish the congruence property of the group $\mathrm{SU}(D,\tau)$ it suffices to show that for any $x \otimes 1 \in \mathrm{SU}(D,\tau) \cap (1+M_D)$ $(x \in \mathrm{SL}(A))$ the image $\pi(x)$ belongs to G'. This is evident if $x \in k$. Next, as $\mathrm{Nrd}_A(x) = 1$, we have $x = b^{\sigma-1}$, where $b \in k(x)$ and σ is the generator of the Galois group $\mathrm{Gal}(k(x)/k)$. If $b \in U_A$, then $\overline{b}^{\overline{\sigma}} = \overline{b}$, and therefore $b = u_k(1+p)$, where $u_k \in U_k$ and $p \in M_A$. Since $b \notin U_A$, we have $b = \sqrt{q}^{\,\beta} u$ for some $q \in M_k$ and $u \in U_{K(x)}$. Then $b^{\sigma-1} = (-1)^{\beta} u^{\sigma-1} = x$ and $\overline{u}^{\overline{\sigma}} = (-1)^{\beta}\overline{u}$. Thus, if the element $\overline{u}$ is $\overline{\tau}$-invariant, then $u \in k$. Clearly, we can assume that $b \in 1+M_D$. On the other hand, if $\overline{u}^{\overline{\tau}} = -\overline{u}$, then the extension $k(b)/k$ is unramified, and therefore $b\delta \in U_D$ for an appropriate $\delta \in k$.

Hence $x = b^{\sigma-1}$, where $b \in 1 + M_A$. Let σ be the restriction of some automorphism i_g, $g \in A$. Then $x = gbg^{-1}b^{-1} = gg^{-i_b}$. Using similar arguments for b we establish that $g \in 1 + M_A$.

Since $A \in \mathrm{TR}(k)$ and the extension K/k is weakly ramified, we have

$$\mathrm{Nrd}_A(1+M_A) = 1 + M_k = N_{K/k}(1+M_K).$$

Then $1 + M_A \subset G$, hence $x = gbg^{-1}b^{-1} \in G'$. Therefore, $x \in \operatorname{Ker}\pi = U(D,\tau)'$, which yields the congruence property for $\mathrm{SU}(D,\tau)$. The proof is complete.

Below we also need another lemma.

Lemma 25. *Let F be a Henselian field* ($\operatorname{char}\overline{F} \neq 2$), *$E$ be its quadratic weakly ramified or immediate extension, and let $a \in (1+M_E) \cap \mathrm{SL}(1, E/F)$. Then $a = b^{\tau-1}$ for some $b \in 1 + M_E$ and a generator τ of the group* $\mathrm{Gal}(E/F)$.

Proof. First, suppose that E/F is weakly totally ramified. By Hilbert's Theorem 90 we have $a = c^{\tau-1}$, where $c \in E$. Since the extension E/F is weakly totally ramified, there exists an element $\pi \in M_F$ such that $v_F(\pi) \notin 2\Gamma_F$, and then $E = F(\sqrt{\pi})$. As the extension is quadratic, we have $c^{\tau} = \alpha - \beta\sqrt{\pi}$, where $\alpha + \beta\sqrt{\pi} = c$. We can assume that $\alpha, \beta \in V_E$. Since $[\Gamma_E : \Gamma_F] = 2$, we have $v(\alpha) \neq v(\beta\sqrt{\pi})$, where v is a valuation of the field E. Let $v(\alpha) > v(\beta\sqrt{\pi})$. Then

$$a = c^{\tau-1} = (\alpha - \beta\sqrt{\pi})(\alpha + \beta\sqrt{\pi})^{-1} = \left(\frac{\alpha}{\beta\sqrt{\pi}} - 1\right)\left(\frac{\alpha}{\beta\sqrt{\pi}} + 1\right)^{-1}.$$

Since $\alpha/(\beta\sqrt{\pi}) \in M_E$, we have $\overline{a} = -1$ and thus we arrive at a contradiction, because $\overline{a} = 1$ and $\operatorname{char}\overline{E} \neq 2$.

Now suppose that $v(\alpha) < v(\beta\sqrt{\pi})$. Then

$$a = (\alpha - \beta\sqrt{\pi})(\alpha + \beta\sqrt{\pi})^{-1} = \left(1 - \frac{\beta\sqrt{\pi}}{\alpha}\right)\left(1 + \frac{\beta\sqrt{\pi}}{\alpha}\right)^{-1}.$$

Since $\beta\sqrt{\pi}/\alpha \in M_E$, we have $a = b^{\tau}/b$, where $b = 1 + \beta\sqrt{\pi}/\alpha \in 1 + M_E$.

If the extension E/F is unramified, then $a = b^{\tau-1}$ by Hilbert's Theorem 90. Replacing b (if necessary) by an appropriate element of V_F, we can assume that b is invertible in V_E. Passing to residues in the equality $a = b^{\tau-1}$ gives $1 = \overline{b^\tau}\,\overline{b}^{-1} = \overline{b}^{\overline{\tau}}\overline{b}^{-1}$. This implies that $\overline{b} \in \overline{F}$. Let e be an inverse image of $\overline{b}$ in F. Then $b = e(1+m)$, where $m \in M_E$, which yields the equality $a = (1+m)^{\tau-1}$. The proof of the lemma is complete.

Recall that the ramification index of $e(D/K)$ is equal to $\lambda_D^2 r(D/K)$, where $r(D/K) = [Z(\overline{D}) : \overline{K}]$.

Proposition 12. *Let* $D \in \mathrm{TR}(K)$, *let* $\overline{D}$ *be a field and assume that* $\operatorname{char}\overline{k} \neq 2$. *Then*

$$(1 + M_D) \cap \mathrm{SU}(D, \tau) \subseteq U(D, \tau)'.$$

Proof. Note that by Theorem 11 the index $\operatorname{ind} D$ is 2-primary. Indeed, if $\operatorname{ind} D$ is divisible by an odd integer greater than 1, then D can be written as $D_1 \otimes_K D_2$, where $\operatorname{ind} D_1$ is odd and $\operatorname{ind} D_2 = 2^m$. Moreover, D_1, $D_2 \in \mathrm{TR}(K)$ and are μ-invariant under an appropriate K/k-involution. Then $\operatorname{ind} D_1 = 1$ by virtue of Theorem 11. Recall that $\operatorname{char}\overline{k} \neq 2$, and therefore $(\operatorname{ind} D, \operatorname{char}\overline{k}) = 1$.

Let $a \in (1 + M_D) \cap \mathrm{SU}(D, \tau)$. If $a \in K$, then $1 = a^{\operatorname{ind} D} \in 1 + M_K$. In this case $a = 1$ because $(\operatorname{ind} D, \operatorname{char}\overline{k}) = 1$, and therefore $a \in U(D, \tau)'$.

Thus, in what follows we assume that $a \notin K$. Let M/K be a subextension of D/K and $M^\tau = M$. Let us show that M contains a cyclic quadratic subextension L/K such that $L^\tau = L$. Since M/K is 2-primary, the general situation reduces to the following two cases:

(i) M/K is totally ramified;

(ii) $\overline{M} \neq \overline{K}$.

In case (i) let $\gamma \in \Gamma_M$ be such that $\gamma + \Gamma_K$ is an element of order 2 in the group Γ_M/Γ_K and let $b \in M$ satisfy $v_M(b) = \gamma$. Then the extension $K(b)/K(b^2)$ is weakly totally ramified and $v_M(b^2) \in \Gamma_K$. Hence $b^2 = tu$, where $u \in V_M$. Since M/K is a totally ramified extension, we can assume that $u = 1+m$, where $m \in M_M$. In view of the condition $(\operatorname{ind} D, \operatorname{char}\overline{k}) = 1$ we can conclude that $u = c^2$ for an appropriate $c \in 1 + M_M$. Considering the element bc^{-1} instead of b from the very beginning, allows us to assume that $b^2 \in K$. If $b^2 \in k$, then $L = K(b)$ is a τ-invariant extension of the field K, and it is cyclic over K. On the other hand, if $b^2 \notin k$, then consider the τ-invariant extension $K(b^{\tau-1})$. Note that $[K(b^{\tau-1}) : K] \leqslant 2$ due to the choice of the value of the element u. Moreover, $K(b^{\tau-1}) \neq K$ (otherwise $K(b)^\tau = K(b)$). We set $L = K(b^{\tau-1})$.

Now suppose that $\overline{M} \neq \overline{K}$. Passing to the maximal unramified subextension M/K (which is τ-invariant since $M^\tau = M$), we can assume that M/K is an unramified extension. Since $\overline{M} \subseteq Z(\overline{D})$, the extension M/K is Abelian. Then there exists a cyclic quadratic extension E/K, $E \subseteq M$, which has the form $E = K(\sqrt{\beta})$, where $\beta \in K$. If $\beta^{\tau-1} = c^2$, $c \in K$, then $K(\sqrt{\beta})$ is τ-invariant. Let $L = K(\sqrt{\beta})$. In the case when $\beta^{\tau-1} \neq c^2$ we have $[K(\sqrt{\beta^{\tau-1}}) : K] = 2$ and $(\sqrt{\beta^{\tau-1}})^\tau = \sqrt{\beta^{1-\tau}}\varepsilon_2^m$. Now let $L = K(\sqrt{\beta^{\tau-1}})$. Thus, in this case L is also τ-invariant.

Since $K(a)^\tau = K(a)$, the above result about the extension M/K is also applicable to the extension $K(a)/K$. Clearly, $L(a)/L(a)_\tau$ is weakly ramified.

Note that for $\operatorname{ind} D = 2$ the proposition was established in Lemma 24. Let $\operatorname{ind} D$ be composite. Suppose that the congruence theorem is valid for K-subalgebras of the algebra D of 2-primary indices less than $\operatorname{ind} D$, and let us establish the existence of an element $l \in (1 + M_L) \cap \mathrm{SU}(C_D(L), \tau|_{C_D(L)})$ such that $\mathrm{Nrd}_D(l) = 1$ and $\mathrm{Nrd}_{C_D(L)}(a) = \mathrm{Nrd}_{C_D(L)}(l)$. For such l we have $\mathrm{Nrd}_{C_D(L)}(al^{-1}) = 1$ and $L(al^{-1}) = L(a)$. Since $\operatorname{ind} C_D(L) < \operatorname{ind} D$ and is 2-primary, our assumption is applicable to the element al^{-1}. Hence $al^{-1} \in U(C_D(L), \tau|_{C_D(L)})'$. Let us show that $l \in U(D, \tau)'$.

Let $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. By Theorem 7 there exists $g \in D$ such that $i_g|_L = \sigma$, and we can assume that $g^\tau \neq -g$. Note that L/k is separable. Put $L_\tau = k(\beta)$. Then $g\beta g^{-1} = \beta^\sigma$. Applying τ to both sides of the last equality we obtain $g^{-\tau}\beta g^\tau = \beta^{\sigma\tau}$. For the Galois group $\mathrm{Gal}(L/k)$ we have $\mathrm{Gal}(L/k) \cong C_2 \times C_2$, where C_2 is a group of order 2, which yields $\beta^{\sigma\tau} = \beta^{\sigma^{-1}} = g^{-1}\beta g$. Hence $g^\tau g^{-1} \in C_D(L)$. Consequently, $g^\tau = cg$ for some $c \in C_D(L)$. Note that σ extends to an automorphism of the whole centralizer $C_D(L)$, since the conjugation by g maps the field L to itself. Consider the element $g^\tau + g = (c+1)g$. Then $(g^\tau + g)^2 = (c+1)g(c+1)g = (c+1)(c+1)^\sigma g^2$. Let $C = (c+1)(c+1)^\sigma \in C_D(L)$. Then the algebra $A = \langle L(Cg^2), g^\tau + g \rangle$ is a τ-invariant quaternion algebra. If $l \in (1 + M_L) \cap \mathrm{SL}(1, D)$, then

$$\mathrm{Nrd}_D(l) N_{L/K}(\mathrm{Nrd}_{C_D(L)}(l)) = N_{L/K}(l)^{\operatorname{ind} C_D(L)} = 1 \in 1 + M_K.$$

It follows from the equality $(\operatorname{ind} C_D(L), \operatorname{char} \overline{k}) = 1$ that $N_{L/K}(l) = 1$. Further,

$$N_{L/K}(l) = N_{L(Cg^2)/K(Cg^2)}(l) = 1.$$

Otherwise, the fact that the extension L/K is quadratic yields $L(Cg^2) = K(Cg^2)$, but this contradicts the fact that $g^\tau + g$ acts nontrivially on L and trivially on Cg^2 by the construction of this element. Hence $l \in \mathrm{SU}(A, \tau|_A) \cap (1 + M_A)$, and therefore we can apply Lemma 24 to the algebra A and the element l, which gives $l \in U(D, \tau)'$.

We complete the proof of the proposition by establishing the existence of l with the indicated properties.

Let M be a maximal subfield of D containing a, and let $K(a) \subset M$. Then

$$\mathrm{Nrd}_{C_D(L)}(a) = N_{M/L}(a) = N_{L(a)/L}(N_{M/L(a)}(a)) = N_{L(a)/L}(a)^{[M:L(a)]}.$$

Since $aa^\tau = 1$, we have $N_{L(a)/L(a)_\tau}(a) = 1$ and by Hilbert's Theorem 90 we have $a = t^{\tau-1}$ and $t \in L(a)$. In view of Lemma 25 as applied to the extension $L(a)/L(a)_\tau$ it can be assumed that $t \in 1 + M_{L(a)}$. Since $L(a)^\tau = L(a)$, we have $N_{L(a)/L}(t^{\tau-1}) = N_{L(a)/L}(t)^{\tau-1}$. Let $e = N_{L(a)/L}(t)$ and set $l = \sqrt[{[L(a):L]}]{e^{\tau-1}}$. Then l is the required element. Indeed,

$$\begin{aligned}
\mathrm{Nrd}_{C_D(L)}(al^{-1}) &= N_{L(a)/L}(al^{-1})^{[M:L(a)]} = \bigl(N_{L(a)/L}(a) N_{L(a)/L}(l)^{-1}\bigr)^{[M:L(a)]} \\
&= \bigl(e^{\tau-1} l^{-[L(a):L]}\bigr)^{[M:L(a)]} = \bigl(e^{\tau-1} e^{1-\tau}\bigr)^{[M:L(a)]} = 1, \\
\mathrm{Nrd}_D(l) &= N_{M/K}(l) = N_{L/K}(N_{M/L}(l)) = N_{L/K}(\mathrm{Nrd}_{C_D(L)}(l)) = \\
&= N_{L/K}(\mathrm{Nrd}_{C_D(L)}(a)) = \mathrm{Nrd}_D(a) = 1.
\end{aligned}$$

The proof of the proposition is complete.

Remark 10. As noted above, each division algebra $D \in \mathrm{TR}(K)$ $(\mathrm{char}\,\overline{k} \neq 2)$ possessing a unitary K/k-involution has a 2-primary index.

Moreover, the following corollary holds.

Corollary 12. *Assume that the algebra* $D \in \mathrm{TR}(K)$ *is totally ramified and* $(\mathrm{char}\,\overline{k} \neq 2)$. *Then the congruence theorem holds for the group* $\mathrm{SU}(D,\tau)$.

Indeed, $\overline{D} = \overline{K}$.

Corollary 13. *Assume that* $D \in \mathrm{TR}(K)$ $(\mathrm{char}\,\overline{k} \neq 2)$ *and* D *has a maximal totally ramified extension. Then the congruence property holds for* $\mathrm{SU}(D,\tau)$.

Proof. Let L/K be a maximal totally ramified extension of fields in D and let $n{=}\mathrm{ind}\,D$. Then $n^2 = [D : L] \cdot n$, and therefore $n = [D : L]$. On the other hand, in view of inequality (1.1) we have $[\overline{D} : \overline{L}][\Gamma_L : \Gamma_K] \leqslant [D : L]$, which implies that $n = [\overline{D} : \overline{L}] \leqslant 1$, In other words, $\overline{D}$ is a field and we can apply Proposition 12. The proof of the corollary is complete.

The following assertion is also valid (including in the case when $\lambda_D = 1$).

Proposition 13. *Assume that* $D \in \mathrm{TR}(K)$, K/k *is weakly ramified and*, *in the case when* $\mathrm{char}\,\overline{k} = 2$ *and* K/k *is unramified*, *let* $\varepsilon_{\mathrm{rad}\,\lambda_D} \in \overline{k}$ $(\mathrm{rad}\,\lambda_D$ *is the product of all distinct prime divisors of the integer* $\lambda_D)$. *Then* $\lambda_D = 2^m$.

Proof. Let T be the totally ramified part of the centralizer $C_D(Z)$, where Z/K is a τ-invariant unramified lift of the extension $Z(\overline{D})/\overline{K}$. Since $\lambda_D = \lambda_T$, it is sufficient to establish that $\mathrm{ind}\,T$ is 2-primary. Thus, the proposition holds for $\mathrm{char}\,\overline{k} \neq 2$, since $\mathrm{ind}\,D$ is 2-primary (as shown in the beginning of the proof of Proposition 12).

Consequently, it remains to consider the case when $\mathrm{char}\,\overline{k} = 2$ and $\mathrm{ind}\,T$ is not 2-primary. Since $\mathrm{ind}\,T$ is not 2-primary (for otherwise the proposition is valid again), T has the form $T_o \otimes_Z T_e$, where $\mathrm{ind}\,T_o$ is nontrivial and odd, and $\mathrm{ind}\,T_e$ is 2-primary in view of the relation $\lambda_T = \lambda_{T_o} \cdot \lambda_{T_e}$. To complete the proof of the proposition we demonstrate that $\lambda_{T_o} = 1$. Assume the contrary, that is, let $\lambda_{T_o} > 1$. We represent T_o in the form $T_1 \otimes_Z \cdots \otimes_Z T_s$, where $T_1, \dots, T_s$ have primary pairwise coprime indices. As the index λ_{T_o} is assumed to be nontrivial, there exists i, $1 \leqslant i \leqslant s$, such that $\lambda_{T_i} > 1$. Set $\mathrm{ind}\,T_i = p_i^{\alpha_i}$. Since $\varepsilon_{\mathrm{rad}\,\lambda_D} \in \overline{k}$, we have $\varepsilon_{p_i} \in \overline{k}$. Consider the extension $k(\varepsilon_i)/k$, where ε_i is a primitive $\exp(\Gamma_{T_i}/\Gamma_Z)$th root of unity. Then for an appropriate m the element $\varepsilon_i^m \in k$ is a primitive p_ith root of unity. Assume that $\varepsilon_i \notin Z_\tau$. Then $\varepsilon_i^m = (\varepsilon_i^m)^\tau = \varepsilon_i^{-m}$, and therefore $\varepsilon_{p_i}^2 = \varepsilon_i^{2m} = 1$, which contradicts the fact that ε_{p_i} is a primitive p_ith root of unity, because p_i is odd. Consequently, $\varepsilon_i \in Z_\tau$. Therefore, $T_i = A_i \otimes_{Z_\tau} Z$, where A_i is a τ-invariant central division Z_τ-algebra. This contradicts the facts that the algebra A_i is τ-invariant, the index of A_i is odd and the restriction of τ to Z_τ is trivial. Consequently, $\lambda_{T_i} = 1$. Thus, $\lambda_{T_o} = \lambda_{T_1}\lambda_{T_2} \cdots \lambda_{T_s} = 1$. The proof is complete.

§ 8. Congruence property for the groups $\mathrm{SU}(D,\tau)$ of unramified algebras with involutions of the form $\tau_L(u)$

As above, we assume that $\mathrm{char}\,\overline{k} \neq 2$ and the extension K/k is weakly ramified. First consider the case of unramified algebras D.

Lemma 26. *Let $D \in \mathcal{D}(K)$ be an unramified algebra and let $\tau = \tau_L \in \mathrm{Inv}_{K/k}(D)$. Then the representation of the involution τ_L in the form $\tau_L(u)$ is equivalent to the representation of the involution $\overline{\tau}$ in the form $\overline{\tau}_{\overline{L}}(v)$ for some $v \in U(\overline{D}, \overline{\tau}_{\overline{L}})$ (in the case when K/k is totally ramified $\overline{\tau}_{\overline{L}}(v)$, for an appropriate $v \in U(\overline{D}, \overline{\tau}_{\overline{L}})$, means an involution on $\overline{D}$ that acts on $\overline{L}$ as $\overline{\tau}$ and is such that $i_v|_{\overline{L}}$ is a generator of the group* $\mathrm{Gal}(\overline{L}/\overline{k})$*).*

Proof. Let $D = \langle L, \sigma, u\rangle$, where $\langle\sigma\rangle = \mathrm{Gal}(L/K)$. Taking an appropriate element which is L-proportional to u we can assume that $\overline{D} = \langle \overline{L}, \overline{\sigma}, \overline{u}\rangle$. This means that $\overline{\tau}$ has the form $\overline{\tau}_{\overline{L}}(\overline{u})$. Conversely, by the hypothesis of the lemma there exists $v \in U(\overline{D}, \overline{\tau})$ such that $\overline{D} = \langle \overline{L}, \overline{\sigma}, v\rangle$, and we can assume without loss of generality that $\overline{u} = v$. Note that for any $l \in L$ we have $u^{-1}lu = l^{\sigma}$ and $u^{\tau}l^{\tau}u^{-\tau} = l^{\sigma\tau}$. In view of the relation $\sigma\tau = \tau\sigma$ the last equality implies that $u^{\tau}lu^{-\tau} = l^{\sigma}$. This means that $uu^{\tau} \in L$. Moreover, passing to residues gives $\overline{uu^{\tau}} = \overline{1}$. Hence $uu^{\tau} \in 1 + M_L$, and since the element uu^{τ} is τ-invariant, it actually belongs to $1 + M_{L_\tau}$. As the extension L/L_τ is weakly ramified, there exists $y \in L$ such that $yy^{\tau} = uu^{\tau}$. This means that $(y^{-1}u)(u^{\tau}y^{-\tau}) = 1$. Passing from u to $y^{-1}u$ we see that the involution τ_L has the form $\tau_L(y^{-1}u)$. The proof of the lemma is complete.

Note that not every cyclic involution τ_L has the form $\tau_L(u)$.

Lemma 27. *Let K/k be a weakly ramified extension, D be an unramified K-algebra and $\tau_L \in \mathrm{Inv}_{K/k}(D)$ be a cyclic involution of the algebra D. Denote by L_2 the extension of K that lies in L and is such that $[L : L_2] = 2$. Suppose that $L_2/L_{2\tau}$ is totally ramified. Then $\tau_L \neq \tau_L(u)$ for all $u \in U(D, \tau_L)$ in the following two cases*:

(1) $-1 \in L^2_{2_\tau}$;

(2) $-1 \notin D^2$.

Proof. First consider case (1), that is, let $-1 \in L^2_{2_\tau}$. Assume that $\tau_L = \tau_L(u)$. Then $\mathrm{ind}\, D$ is 2-primary by Lemma 10. Since L/K is unramified, $\overline{L}/\overline{K}$ is a cyclic extension with Galois 2-group. As $\overline{K} = \overline{k}$, the extension $\overline{L}/\overline{k}$ is a cyclic extension with Galois 2-group. Consider the extension $L_2/L_{2\tau}$. Note that the centralizer $C_D(L_2)$ is a quaternion L_2-algebra such that the restriction of τ to this centralizer is an involution of the form $\tau_L(u)$. Since $L_2/L_{2\tau}$ is totally ramified, it is sufficient to prove the lemma in the case when $\mathrm{ind}\, D = 2$, K/k is totally ramified and $-1 \in k^2$. Since $\mathrm{char}\, \overline{k} \neq 2$, we can assume that $D = (\alpha, \beta) \otimes_k k(\sqrt{\pi})$, where (α, β) is a τ-invariant unramified quaternion k-algebra the restriction of τ to which is as follows: $\sqrt{\alpha}^{\,\tau} = -\sqrt{\alpha}$, $\sqrt{\beta}^{\,\tau} = -\sqrt{\beta}$, $\sqrt{\pi}^{\,\tau} = -\sqrt{\pi}$, and $\pi \in M_k$ is such that $v_k(\pi) \notin 2\Gamma_k$. Since the algebra (α, β) is unramified, we can assume without loss of generality that $\alpha, \beta \in U_K$ and $(\overline{\alpha}, \overline{\beta})$ is a division $\overline{k}$-algebra. Our aim is to prove that τ_L cannot be an involution of the form $\tau_L(u)$. Assume the opposite: let τ_L be a cyclic involution of the form $\tau_L(u)$, where $u \in U(D, \tau)$. Since $\{1, \sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha}\sqrt{\beta}\}$ is the canonical basis of the quaternion algebra (α, β), we have $\sqrt{\beta}^{\,-1}\sqrt{\alpha}\sqrt{\beta} = -\sqrt{\alpha}$ and $u^{-1}\sqrt{\alpha}u = -\sqrt{\alpha}$. This yields $\sqrt{\beta}^{\,-1}\sqrt{\alpha}\sqrt{\beta} = u^{-1}\sqrt{\alpha}u$, which, in turn, implies that $u\sqrt{\beta}^{\,-1} \in k(\sqrt{\pi}, \sqrt{\alpha})$. This means that $u\sqrt{\beta}^{\,-1} = a + b\sqrt{\alpha}$, where $a, b \in k(\sqrt{\pi})$. Consequently, since $u \in U(D, \tau)$, we have $1 = uu^{\tau} = -\beta(a + b\sqrt{\alpha})(a^{\tau} - b^{\tau}\sqrt{\alpha})$. Finally, we conclude that $-\beta^{-1} = (aa^{\tau} - \alpha bb^{\tau}) + (-ab^{\tau} + ba^{\tau})\sqrt{\alpha}$. Since $\beta^{-1}, aa^{\tau} - \alpha bb^{\tau} \in k$, the relation $-ab^{\tau} + ba^{\tau} = 0$ holds. This means that $a/b \in S_\tau(D)$. It follows from the above that $\beta^{-1} = (\alpha bb^{\tau} - aa^{\tau}) + (ab^{\tau} - ba^{\tau})\sqrt{\alpha}$. Note that the situation where a is an integer and b is not (or b is an integer and a is not) cannot occur. In the first case it follows from the previous equality that αbb^{τ} is not an integer, but it is equal to $b^{-1} + aa^{\tau}$, which is a contradiction. The second case is considered similarly. Thus, a and b are either integers or not simultaneously.

Consider the case when a and b are integers. Then $\overline{\beta}^{-1} = \overline{\alpha}\,\overline{b}\,\overline{b}^{\overline{\tau}} - \overline{a}\,\overline{a}^{\overline{\tau}}$. As the extension $k(\sqrt{\pi})/k$ is weakly totally ramified, we have $\overline{b^{\tau}} = \overline{b}$. Similarly, $\overline{a^{\tau}} = \overline{a}$, which yields $\overline{\beta}^{-1} = \overline{\alpha}\,\overline{b}^{2} - \overline{a}^{2}$. With due regard to the condition $-1 \in \overline{k}^{2}$ we obtain $(\overline{\alpha}, \overline{\beta}) = (\overline{\alpha}, \overline{\beta}^{-1})$. This means that $(\overline{\alpha}, \overline{\beta})$ is not a division algebra, which is not the case.

Suppose that both a and b are not integers and we have $a = u_a/(\sqrt{\pi})^m$ and $b = u_b/(\sqrt{\pi})^n$, where $u_a, u_b \in U_{k(\sqrt{\pi})}$. Then $\beta^{-1} = \alpha u_b u_b^{\tau}/((\sqrt{\pi})^n((\sqrt{\pi})^n)^{\tau}) - u_a u_a^{\tau}/((\sqrt{\pi})^m((\sqrt{\pi})^m)^{\tau})$. If $m \neq n$, then we multiply both sides of this equality by a smaller power of $\sqrt{\pi}$ and arrive at the case considered above. Consequently, it remains to consider the case when $m = n$. Raising the denominators on both sides of the equality and passing to residues gives $\overline{u_a}^{2} - \overline{\alpha}\,\overline{u_b}^{2} = 0$. Thus, $\overline{\alpha} \in \overline{k}^{2}$, which contradicts the fact that $(\overline{\alpha}, \overline{\beta})$ is a division algebra and completes the consideration of the case when $-1 \in L_{2_{\tau}}^{2}$.

Suppose that $-1 \notin D^2$ and D has an involution of the form $\tau_L(u)$ for $u \in U(D, \tau)$. Then $\tau_L(u)$ can be extended to an involution $\tau_L(i)$ of the algebra $D(i) = D \otimes_K K(i)$, where $i^2 = -1$, by letting $i^{\tau} = i$. Since $-1 \notin D^2$ and $\operatorname{char} \overline{k} \neq 2$, $k(i)/k$ is unramified and $K(i)/k(i)$ is totally ramified. Moreover, $L \otimes_K K(i)$ is the maximal cyclic subfield of this algebra and $u \otimes_K 1 \in U(D(i), \tau_L(i))$. This means that $\tau_{L(i)}$ has the form $\tau_{L(i)}(u \otimes_K 1)$. Note that the algebra $D(i)$ is unramified over $K(i)$ and $K(i)/K(i)_{\tau_{L(i)}}$ is a totally ramified extension. Thus, if we assume that the extension $L(i)_2/L(i)_{2_{\tau_L(i)}}$ is totally ramified, then we find ourselves in the framework of case (1). This yields that there is no involution of the form $\tau_{L(i)}(u \otimes_K 1)$ on $D(i)$, which is a contradiction. The proof is complete.

The following technical proposition will be used repeatedly both for extensions of fields K and for extensions of fields $\overline{K}$.

Let N/F be a Galois extension of an infinite field F ($\operatorname{char} F \neq 2$) such that the group $\operatorname{Gal}(N/F)$ is a direct product $G \times G_2$ of two groups, where G is Abelian and G_2 is a group of order two. Suppose that $G_2 = \langle \widetilde{\mu} \rangle$ and let $\mu = \mathrm{id}_G \otimes \widetilde{\mu}$. Note that if $E = N_G$, then $N = N_{\mu} \otimes_F E$. Then the following proposition holds.

Proposition 14. *Let $E = F(\sqrt{\beta})$. Then the exists a primitive element z of the extension N_{G_2}/F such that, among the elements of the form $v_z = \big((1 + z\sqrt{\beta})/(1 - z\sqrt{\beta})\big)^{\gamma - 1}$, $\gamma \in \operatorname{Gal}(N/E)$, there is a primitive element of N/E.*

Proof. First of all note that for an arbitrary intermediate subfield L such that $E \subset L \subseteq N$ and any prime divisor p of degree $[L : E]$ there exists a subextension T_p such that $T_p \subset L$ and $[L : T_p] = p$. Indeed, if $G_L = \operatorname{Gal}(L/E)$ and G_p is a subgroup of G_L of prime order p, then let T_p be the field of invariants of the group G_p in N. It is easily seen that $[N : T_p] = p$ and N/T_p is a cyclic extension of degree p.

The element v_z can obviously be written in the form

$$v_z = \frac{1 - z^{\gamma} z\beta + (z^{\gamma} - z)\sqrt{\beta}}{1 - z^{\gamma} z\beta + (z - z^{\gamma})\sqrt{\beta}}.$$

Set $A = 1 - z^\gamma z\beta$ and $B = z^\gamma - z$. Then

$$E(v_z) = E\biggl(1 + \frac{2B\sqrt{\beta}}{A - B\sqrt{\beta}}\biggr) = E\biggl(\frac{A}{B\sqrt{\beta}}\biggr) = E\biggl(\frac{1 - z^\gamma z\beta}{z^\gamma - z}\biggr).$$

Assume that for any primitive element z of the extension N_μ/F the element $(1 - z^\gamma z\beta)/(z^\gamma - z)$ is not primitive for the extension N/E. Then it belongs to some field T_p. We restrict our consideration to the case when $\langle\gamma\rangle = \mathrm{Gal}(N/T_p)$ and N_{G_2}/F is cyclic.

Let $p = 2$. Since $z^\gamma z = N_{N|T_2}(z) \in T_2$, we have $1 - z^\gamma z\beta \in T_2$ and therefore $z^\gamma - z \in T_2$. Then either $z \in T_2$, which is not the case because z is primitive in the extension N/T_2, or z is a root of an irreducible polynomial of degree 2 with coefficients in T_2. However, in the last case $z^\gamma - z$ cannot belong to T_2, because $[N : T_2] = 2$.

Now suppose that $p \neq 2$ and $(1 - z^\gamma z\beta)/(z^\gamma - z) \in T_p$. By our assumptions, for any $m \in F$ the element $\bigl(1 - (z+m)^\gamma (z+m)\beta\bigr)/(z^\gamma - z)$ also belongs to T_p. Then so does also the quotient of these two elements. Hence

$$\frac{1 - (z+m)^\gamma (z+m)\beta}{1 - z^\gamma z\beta} = 1 - \frac{(m + z^\gamma + z)m\beta}{1 - z^\gamma z\beta} \in T_p, \quad \text{that is,} \quad \frac{m + z^\gamma + z}{1 - z^\gamma z\beta} \in T_p.$$

Similarly, we have $(n + z^\gamma + z)/(1 - z^\gamma z\beta) \in T_p$ for $n \in F$ and $n \neq m$. Taking the quotient of these two elements we obtain $(m + z^\gamma + z)/(n + z^\gamma + z) \in T_p$. Since

$$\frac{m + z^\gamma + z}{n + z^\gamma + z} = \frac{m - n + n + z^\gamma + z}{n + z^\gamma + z} = 1 + \frac{m - n}{n + z^\gamma + z},$$

we have $(m - n)/(n + z^\gamma + z) \in T_p$, which yields $z^\gamma + z \in T_p$. Let $z^\gamma = -z + t$, $t \in T_p$. Then $(1 - z^\gamma z\beta)/(z^\gamma - z)$ transforms into $(1 - (t - z)z\beta)/(t - z - z) = (1 + z^2\beta - tz\beta)/(t - 2z)$. Since this element belongs to T_p, we obtain the equality $\widetilde{t} = (1 + z^2\beta - tz\beta)/(t - 2z)$, where $\widetilde{t} \in T_p$. This immediately implies that z is a root of a polynomial of degree 2 with coefficients in T_p. On the other hand, since z is a primitive element of the extension N_μ/F, it is a primitive element of N/E and, in particular, a primitive element of the extension N/T_p. Hence we arrive at a contradiction, since $[N : T_p] = p$ and $N = T_p(z)$. The proof is complete.

Corollary 14. *Assume that the algebra $D \in \mathcal{D}(K)$ is unramified, $\tau \in \mathrm{Inv}_{K/k}(D)$ and $\overline{D}$ contains a maximal subfield N satisfying the conditions formulated before Proposition 14 for $F = \overline{k}$, $E = \overline{K}$, $\mu = \overline{\tau}|_N$ and $\beta = \overline{\alpha}$, where $\alpha \in U_k$ and $\overline{K} = \overline{k}(\sqrt{\overline{\alpha}}\,)$. Then there exist an unramified τ-invariant lift L of the extension $N/\overline{k}$, an element $z \in U_{L_\tau}$ and $\gamma \in \mathrm{Gal}(L/K)$ such that $\bigl((1 + \overline{z}\sqrt{\overline{\alpha}})/(1 - \overline{z}\sqrt{\overline{\alpha}})\bigr)^{\gamma - 1}$ is a primitive element of the extension $N/\overline{K}$.*

Proof. Denote the τ-invariant unramified lift of the extension $N/\overline{k}$ by L/k. By virtue of the last proposition the extension $N/\overline{K}$ contains a primitive element of the form $\bigl((1 + \widetilde{t}\sqrt{\overline{\alpha}})/(1 - \widetilde{t}\sqrt{\overline{\alpha}})\bigr)^{\gamma - 1}$, where $\widetilde{t}$ is some primitive element of the extension $N_{\overline{\tau}}/\overline{k}$.

Let z be the inverse image of $\widetilde{t}$ in L_τ. Then the element $\bigl((1+\overline{z}\sqrt{\overline{\alpha}})/(1-\overline{z}\sqrt{\overline{\alpha}})\bigr)^{\gamma-1}$ is primitive for the extension $N/\overline{K}$. The proof of the corollary is complete.

If λ is the lift of the automorphism γ to the field L, then the following remark is valid.

Remark 11. The inclusion

$$\left(\frac{1+z\sqrt{\alpha}}{1-z\sqrt{\alpha}}\right)^{\lambda-1}\in \mathrm{SU}(D,\tau)$$

holds.

Corollary 15. *If $\lambda=i_u|_L$, where $u\in U(D,\tau)$, then $\big((1+z\sqrt{\alpha})/(1-z\sqrt{\alpha})\big)^{\lambda-1}\in U(D,\tau)'$.*

Proof. We have $d=(1+z\sqrt{\alpha})/(1-z\sqrt{\alpha})\in U(D,\tau)$, which implies that $d^{\lambda-1}=udu^{-1}d^{-1}\in U(D,\tau)'$. The proof is complete.

Let us formulate a sufficient condition for the group $\mathrm{SU}(D,\tau)$ to exhibit the congruence property.

Proposition 15. *Let $D\in\mathcal{D}(K)$ be an unramified algebra of an odd index and $\tau_L\in\mathrm{Inv}_{K/k}(D)$. Suppose that the involution $\overline{\tau}=\overline{\tau}_{\overline{L}}$ has the form $\overline{\tau}_{\overline{L}}(\widetilde{u})$. Then the group $\mathrm{SU}(D,\tau)$ has the congruence property.*

Proof. Let $a\in(\mathrm{SU}(D,\tau)\cap(1+M_D))\setminus K$. Note that $\overline{D}=\langle\overline{L},\overline{\sigma},\widetilde{u}\rangle$, where $\langle\overline{\sigma}\rangle=\mathrm{Gal}(\overline{L}/\overline{K})$ and $\widetilde{u}\in U(\overline{D},\overline{\tau})$. Also note that $\overline{\tau}|_{\overline{L}}$ commutes with the elements of $\mathrm{Gal}(\overline{L}/\overline{K})$.

Let $N=\overline{L}$, $E=\overline{K}$, $\mu=\overline{\tau}|_{\overline{L}}$ and $F=\overline{k}$. By Proposition 14 there exists a primitive element $\widetilde{z}$ of the extension $\overline{L}_{\overline{\tau}}/\overline{k}$ such that $\widetilde{d}_{\widetilde{z}}=\big((1+\widetilde{z}\sqrt{\overline{\alpha}})/(1-\widetilde{z}\sqrt{\overline{\alpha}})\big)^{\gamma-1}$ is a primitive element of the extension $\overline{L}/\overline{K}$.

For the lift λ of the automorphism $\overline{\sigma}$ in L let $d_z=\big((1+z\sqrt{\alpha})/(1-z\sqrt{\alpha})\big)^{\lambda-1}$, where $\overline{z}=\widetilde{z}$. By Lemma 26 there exists an element $u\in U(D,\tau)$ such that $i_u|_L=\lambda$. Then $d_z\in U(D,\tau)'$ by Corollary 15.

Denote the field $K(d_za)$ by L'. As $\overline{d_za}=\widetilde{d}_{\widetilde{z}}$ is a primitive element of the extension $\overline{L}/\overline{K}$, we have $\overline{L'}=\overline{L}$. Since $\overline{D}=\langle\overline{L'},\widetilde{\sigma},\widetilde{u}\rangle$, where $\langle\widetilde{\sigma}\rangle=\mathrm{Gal}(\overline{L'}/\overline{K})$, by the last lemma we have $D=\langle L',\sigma',u\rangle$, where $\langle\sigma'\rangle=\mathrm{Gal}(L'/K)$, $\overline{\sigma'}=\widetilde{\sigma}$ and $u\in U(D,\tau)$. Applying Proposition 3 to the last algebra and the element d_za gives $d_za\in U(D,\tau)'$. Hence $a\in U(D,\tau)'$.

Now suppose that $a\in\mathrm{SU}(D,\tau)\cap(1+M_D)\cap K$ and let d_z be the element mentioned above. Consider d_za. We have $d_za\in(L'\setminus K)$. Again, $d_za\in U(D,\tau)'$ by Proposition 3, which implies that $a=(d_za)d_z^{-1}\in U(D,\tau)'$. The proof of the proposition is complete.

We need the following proposition below.

Proposition 16. *Let $D\in\mathcal{D}(K)$ be an unramified algebra of 2-primary index, let $\tau\in\mathrm{Inv}_{K/k}(D)$, $\tau=\tau_L(u)$, and assume that $\operatorname{char}\overline{k}\neq 2$. Then the group $\mathrm{SU}(D,\tau)$ has the congruence property.*

Proof. If D is a quaternion algebra, then $\mathrm{SU}(D,\tau)$ has the congruence property by Lemma 24. Suppose that $\operatorname{ind}D>2$ and that the special unitary groups of cyclic subalgebras of D with involutions satisfying the hypotheses of the proposition posses the congruence property.

By Proposition 14 there exists a primitive element $\widetilde{z}$ of the extension $\overline{L}_{\overline{\tau}}/\overline{k}$ such that $\widetilde{d} = \big((1+\widetilde{z}\sqrt{\overline{\alpha}})/(1-\widetilde{z}\sqrt{\overline{\alpha}})\big)^{\gamma-1}$ is a primitive element of the extension $\overline{L}/\overline{K}$.

Next, let $\widetilde{E}$ be a quadratic extension of k containing in L_τ. Let $E = \widetilde{E} \times_k K$. Then E/K is a τ-invariant quadratic extension of K. For the inverse image z of the element $\widetilde{z}$ in L_τ let $d_z = \big((1+z\sqrt{\alpha})/(1-z\sqrt{\alpha})\big)^{\nu-1}$, where ν is an inverse image of γ.

Since $\overline{L} = \overline{K}(\widetilde{d}) \subset \overline{K(d_z)}$, L is a maximal field and the algebra D/K is unramified, we have $K(d_z) = L$; furthermore, $d_z \in U(D,\tau)'$ because $(1+z\sqrt{\alpha})/(1-z\sqrt{\alpha}) \in U(D,\tau)$ and $\nu = i_u|_L$, $u \in U(D,\tau)$.

Next, let $a \in (1+M_D) \cap \mathrm{SU}(D,\tau) \setminus K$ and let $L' = K(d_za)$. Since the extension $\overline{K}(\overline{d_z})/\overline{K}$ is maximal and $\overline{K}(\overline{d_z}) \subset \overline{K(d_za)}$, we obtain $\overline{L'} = \overline{L}$. The identity automorphism of the fields $\overline{L'}$ and $\overline{L}$ is the restriction of the identity automorphism of $\overline{D}$. Denote by φ the K-automorphism of D sending L' to L and such that $\overline{\varphi}|_{\overline{L'}} = \mathrm{id}_{\overline{L'}}$. Then, since the algebra D is unramified, we conclude from [43] that $\varphi = i_{(1+m)^{-1}}$, where $m \in M_D$. Consequently, $L' = (1+m)^{-1}L(1+m)$. We apply τ to both sides of the last equality and obtain $L'^{\tau} = (1+m)^{\tau}L^{\tau}(1+m)^{-\tau}$. Since $L' = K(d_za)$, the field L' is τ-invariant (in view of the fact that $d_za \in U(D,\tau)$). Hence $L' = (1+m)^{\tau}L(1+m)^{-\tau}$. This implies that $(1+m)^{-1}L(1+m) = (1+m)^{\tau}L(1+m)^{-\tau}$, which, in turn, yields $L = (1+m)(1+m)^{\tau}L((1+m)(1+m)^{\tau})^{-1}$. Then the restriction of the automorphism $i_{(1+m)(1+m)^{\tau}}$ is an automorphism of L with an identity reduction. Therefore, $(1+m)(1+m)^{\tau} \in C_D(L) = L$. Note that $(1+m)(1+m)^{\tau} \in 1+M_L$; hence for an appropriate $1+p \in 1+M_L$ we have $(1+m)(1+m)^{\tau} = N_{L/L_\tau}(1+p) = (1+p)(1+p)^{\tau}$, since L/L_τ is weakly ramified. Consequently, $(1+p)^{-1}(1+m) \in U(D,\tau)$, and we may assume without loss of generality that $(1+m) \in (1+M_D) \cap U(D,\tau)$ because $1+p$ is a central element of $C_D(L)$.

To complete the proof of the proposition we demonstrate that $b = (1+m)^{-1}(d_za)(1+m)$ belongs to $U(D,\tau)'$. To do this we show that there exists an element $e \in (1+M_E) \cap \mathrm{SU}(C_D(E), \tau|_{C_D(E)})$ such that $\mathrm{Nrd}_{C_D(E)}(b) = \mathrm{Nrd}_{C_D(E)}(e)$ and, in addition, $\mathrm{Nrd}_D(e) = 1$. For such e we have $E(be^{-1}) = E(b)$ and $\mathrm{Nrd}_{C_D(E)}(be^{-1}) = 1$, which means that $be^{-1} \in (1+M_{C_D(E)}) \cap \mathrm{SU}(C_D(E), \tau|_{C_D(E)})$. Since $\operatorname{ind} C_D(E) < \operatorname{ind} D$, we can apply the inductive hypothesis to be^{-1} and obtain $be^{-1} \in U(C_D(E), \tau|_{C_D(E)})'$.

Now we establish that $e \in U(D,\tau)'$, which implies that $b \in U(D,\tau)'$.

Let $\langle\sigma\rangle = \mathrm{Gal}(E/K)$. By Theorem 7 there exists an element $g \in D$ such that $i_{g^{-1}}|_E = \sigma$. Let $E_\tau = k(\beta)$. Then $g\beta g^{-1} = g^{\sigma}$. We apply τ to both sides of this equality and obtain $g^{-\tau}\beta g^{\tau} = \beta^{\sigma\tau}$. Since $\mathrm{Gal}(E/k) = C_2 \times C_2$, we have $\beta^{\sigma\tau} = \beta^{\sigma^{-1}} = g^{-1}\beta g$. This yields $g^{\tau}g^{-1} \in C_D(E)$. Hence $g^{\tau} = cg$ for some $c \in C_D(E)$. Note that σ extends to an automorphism of the whole centralizer $C_D(E)$, because the conjugation by g maps the field E to itself. We can assume without loss of generality that $g^{\tau} \neq -g$. Otherwise, instead of g we can consider the element αg, where $K = k(\alpha)$. We look at $g^{\tau}+g = (c+1)g$. We have $(g^{\tau}+g)^2 = (c+1)g(c+1)g = (c+1)(c+1)^{\sigma}g^2$. Denote the element $(c+1)(c+1)^{\sigma} \in C_D(E)$ by C. Then the algebra $A = \langle E(Cg^2), g^{\tau}+g\rangle$ is a τ-invariant central algebra of index 2 over $K(Cg^2)$. Note that

$$N_{E/K}(\mathrm{Nrd}_{C_D(E)}(e)) = N_{E/K}(e)^{\operatorname{ind} C_D(E)} = 1 \in 1+M_K.$$

Since $\operatorname{ind} C_D(E)$ is coprime to $\operatorname{char}\overline{k}$, we have $N_{E/K}(e) = 1$. It is easily seen that $N_{E/K}(e) = N_{E(Cg^2)/K(Cg^2)}(e) = 1$. Otherwise, since the extension E/K is quadratic, we have $E(Cg^2) = K(Cg^2)$, which contradicts the fact that $i_{g^\tau+g}$ acts nontrivially on E and trivially on Cg^2 by the construction of this element. Thus, $e \in \mathrm{SU}(A, \tau|_A) \cap (1 + M_A)$, and therefore Lemma 24 applies to the algebra A and the element e. Hence $e \in U(D, \tau)'$.

It remains to prove that there exists an element e with the indicated properties. Now,

$$\mathrm{Nrd}_{C_D(E)}(b) = N_{L/E}(b) = N_{E(b)/E}(N_{L/E(b)}(b)) = N_{E(b)/E}(b)^{[L:E(b)]}.$$

Since $bb^\tau = 1$, we have $N_{E(b)/E(b)_\tau}(b) = 1$ and by Hilbert's Theorem 90 we have $b = t^{\tau-1}$, where $t \in E(b)$. In view of Lemma 25 as applied to the extension $E(b)/E(b)_\tau$, we can assume without loss of generality that $t \in 1 + M_{E(b)}$. Let $r = N_{E(b)/E}(t)$. We set $e = \sqrt[{[E(b):E]}]{r^{\tau-1}}$ and show that e is the required element. Indeed,

$$\begin{aligned}\mathrm{Nrd}_{C_D(E)}(be^{-1}) &= N_{E(b)/E}(be^{-1})^{[L:E(b)]} = \big(N_{E(b)/E}(b)N_{E(b)/E}(e)^{-1}\big)^{[L:E(b)]}\\ &= \big(r^{\tau-1}e^{-[E(b):E]}\big)^{[L:E(b)]} = \big(r^{\tau-1}r^{1-\tau}\big)^{[L:E(b)]} = 1\end{aligned}$$

and

$$\begin{aligned}\mathrm{Nrd}_D(e) &= N_{L/K}(e) = N_{E/K}(N_{L/E}(e)) = N_{E/K}(\mathrm{Nrd}_{C_D(E)}(e))\\ &= N_{E/K}(\mathrm{Nrd}_{C_D(E)}(b)) = \mathrm{Nrd}_D(b) = 1.\end{aligned}$$

The proof of Proposition 16 is complete.

Theorem 18. *Suppose that $D \in \mathcal{D}(K)$ is an unramified algebra and $\tau = \tau_L(u)$ is a cyclic involution in $\mathrm{Inv}_{K/k}(D)$. Then the group $\mathrm{SU}(D,\tau)$ has the congruence property. In particular, the assumptions of the theorem are satisfied when D is a quaternion algebra unramified over K.*

Proof. As above, we note that the element $a \in (1 + M_D) \cap \mathrm{SU}(D,\tau) \cap K$ belongs to $U(D,\tau)'$.

Now let $a \in (\mathrm{SU}(D,\tau) \cap (1 + M_D)) \setminus K$. Note that $\overline{D} = \langle \overline{L}, \widetilde{\sigma}, \overline{u}\rangle$, where $\langle\widetilde{\sigma}\rangle = \mathrm{Gal}(\overline{L}/\overline{K})$. Moreover, the restriction $\overline{\tau}|_{\overline{L}}$ commutes with all elements of $\mathrm{Gal}(\overline{L}/\overline{K})$.

Let $N = \overline{L}$, $E = \overline{K}$, $\mu = \overline{\tau}|_{\overline{L}}$ and $F = \overline{k}$. By Proposition 14 there exists a primitive element $\widetilde{z}$ of the extension $\overline{L}_{\overline{\tau}}/\overline{k}$ such that for some $\gamma \in \mathrm{Gal}(\overline{L}/\overline{K})$ the element $\widetilde{d}_{\widetilde{z}} = \big((1+\widetilde{z}\sqrt{\overline{\alpha}})/(1-\widetilde{z}\sqrt{\overline{\alpha}})\big)^{\gamma-1}$ is a primitive element of the extension $\overline{L}/\overline{K}$.

For the lift of the $\overline{K}$-automorphism γ to a K-automorphism λ of the field L set $d_z = \big((1+z\sqrt{\alpha})/(1-z\sqrt{\alpha})\big)^{\lambda-1}$, where $\overline{z} = \widetilde{z}$. By Lemma 26 there exists an element $u \in U(D,\tau)$ such that $i_u|_L = \lambda$. Then $d_z \in U(D,\tau)'$ by Corollary 15.

Denote the field $K(d_z a)$ by L'. Since $\overline{d_z a} = \widetilde{d}_{\widetilde{z}}$ is a primitive element of $\overline{L}/\overline{K}$, we have $\overline{L'} = \overline{L}$. Consequently, $\overline{D} = \langle\overline{L'}, \widetilde{\sigma}, \overline{u}\rangle$ and by Lemma 26 we have $D = \langle L', \sigma', u\rangle$, where $\langle\sigma'\rangle = \mathrm{Gal}(L'/K)$ and $u \in U(D,\tau)$. Applying Proposition 3 we obtain $d_z a \in U(D,\tau)'$. Hence $a \in U(D,\tau)'$. The proof is complete.

§ 9. Congruence property for the groups $\mathrm{SU}(D,\tau)$. The mixed case

Let $D \in \mathrm{TR}(K)$ and assume that $\operatorname{char} \overline{k} \neq 2$. The main result of this section is Theorem 3. We recall its formulation.

Let $\tau \in \mathrm{Inv}_{K/k}(D)$. Then the group $\mathrm{SU}(D,\tau)$ has the congruence property in the following two cases:

(i) *$\overline{D}$ is a field;*

(ii) *$\overline{D}$ is not a field (if $\operatorname{char}\overline{k} > 0$, then $(\operatorname{ind} D, \operatorname{char}\overline{k}) = 1$) and the involution $\overline{\tau}$ is cyclic and accompanied by a unitary element.*

Remark 12. In case (i) Theorem 3 has already been established (see Proposition 12).

We preface the proof of Theorem 3 in case (ii) by the following lemma.

Lemma 28. *Assume that D obeys the conditions of case* (ii) *and I is a τ-invariant inertia algebra of D. Then $\tau|_I$ is a cyclic involution of I accompanied by a unitary element and having the form $(\tau|_I)_L$ and $L/Z(I)$ is an appropriate τ-invariant cyclic extension of the field $Z(I)$. In this case there exists $l \in (1+M_L) \cap \mathrm{SU}(D,\tau)$ such that $\overline{L} = \overline{K(l)}$ and $l \in U(D,\tau)'$.*

Proof. It is clear that both in the case when $\operatorname{char}\overline{k} = 0$ and in the case when $\overline{k}$ has a positive characteristic, in view of the condition $(\operatorname{ind} D, \operatorname{char}\overline{k}) = 1$ all K-extensions containing in D are weakly ramified.

Let I be a τ-invariant inertia algebra of D. It follows from the hypothesis of the lemma that $\overline{\tau|_I} = (\overline{\tau}|_{\overline{I}})_{\widetilde{L}}(\widetilde{u})$, where $\widetilde{L}$ is an appropriate cyclic extension of the field $Z(\overline{I})$ and $\widetilde{u} \in U(\overline{I}, \overline{\tau|_I})$. Denote the unramified τ-invariant lift of the extension $\widetilde{L}/\overline{Z(I)}$ by $L/Z(I)$. Then $\tau|_I$ is a cyclic involution of $(\tau|_I)_L$. However, in this case, in view of conditions (ii) and Lemma 26 the involution $\tau|_I$ has the form $(\tau|_I)_L(u)$ for an appropriate $u \in U(I, \tau|_I)$.

Let us show that there exists an element l mentioned in the formulation of the lemma. It is easily seen that there exists a primitive τ-invariant element $s \in U_L$ such that $\widetilde{L} = \overline{K}(\overline{s})$. Denote a primitive element of the extension $\widetilde{L}_{\overline{\tau}}/\overline{Z(I)}_{\overline{\tau}}$ by $\widetilde{s_1}$ and a primitive element of $\overline{Z(I)}_{\overline{\tau}}/\overline{k}$ by $\widetilde{s_2}$. Let s_1 be the inverse image of $\widetilde{s_1}$ in L and s_2 be the inverse image of $\widetilde{s_2}$ in $Z(I)$. Then $s_1 + s_1^\tau$ and $s_2 + s_2^\tau$ are τ-invariant primitive elements in L and $Z(I)$, respectively. Note that there exists an element $\widetilde{c} \in \overline{k}$ such that $\widetilde{s_1} + \widetilde{c}\widetilde{s_2}$ is a primitive element of $\widetilde{L}/\overline{K}$. Let

$$s = (s_1 + s_1^\tau) + 2c(s_2 + s_2^\tau),$$

where c is the inverse image of the element $\widetilde{c}$ in k. In view of the condition $\operatorname{char}\overline{k} \neq 2$ and the equality $(\operatorname{ind} D, \operatorname{char}\overline{k}) = 1$, the element s is as required. In the case of a totally ramified extension $K = k(\sqrt{\pi})$, $\pi \in M_k$, let $l' = (1+\sqrt{\pi}s)/(1-\sqrt{\pi}s)$. Then $l' \in U(D,\tau)$. Set $l = (\sqrt[\operatorname{ind} D]{\mathrm{Nrd}_D(l')})^{-1} l'$. Then it is clear that $l \in (1+M_L) \cap \mathrm{SU}(D,\tau)$. In the case when K/k is unramified, for $q \in U_K$ such that $\overline{q} \neq \overline{k}$ and $q^\tau = -q$ we set $l' = (1+\pi q s)/(1-\pi q s)$. Then, as in the case of a totally ramified extension K/k, we show that $l' \in U(D,\tau)$. Let $l = (\sqrt[\operatorname{ind} D]{\mathrm{Nrd}_D(l')})^{-1} l'$. Then l is again the desired element.

Now denote by N a cyclic τ-invariant extension of the field K of prime degree which is contained in $Z(I)$ if $Z(I) \neq K$, while in the case when $Z(I) = K$ let N be a cyclic extension of $Z(I)$ of prime degree that is contained in L.

Note that L is a maximal subfield in D and

$$\mathrm{Nrd}_{C_D(N)}(l) = N_{L/N}(l) = N_{N(l)/N}(N_{L/N(l)}(l)) = N_{N(l)/N}(l)^{[L:N(l)]}.$$

Since $ll^\tau = 1$, we have $N_{N(l)/N(l)_\tau}(l) = 1$ and by Hilbert's Theorem 90 $l = t^{\tau-1}$, $t \in N(l)$. Since the extension $N(l)/N(l)_\tau$ is weakly ramified, we can assume without loss of generality that $t \in 1 + M_{N(l)}$. Since $N(l)$ is a τ-invariant field, we have $N_{N(l)/N}(t^{\tau-1}) = N_{N(l)/N}(t)^{\tau-1}$. Note that $[N(l) : N]$ divides the index of the algebra D, which is coprime to $\mathrm{char}\,\overline{k}$. We take $m = N_{N(l)/N}(t)$ and $c = \sqrt[{[N(l):N]}]{m^{\tau-1}} \in 1 + M_N$ and show that c satisfies the following conditions:

$$\begin{aligned}\mathrm{Nrd}_{C_D(N)}(lc^{-1}) &= N_{N(l)/N}(lc^{-1})^{[L:N(l)]} = \bigl(N_{N(l)/N}(l)N_{N(l)/N}(c)^{-1}\bigr)^{[L:N(l)]}\\ &= \bigl(m^{\tau-1}c^{-[N(l):N]}\bigr)^{[L:N(l)]} = \bigl(m^{\tau-1}m^{1-\tau}\bigr)^{[L:N(l)]} = 1, \qquad (9.1)\\ \mathrm{Nrd}_D(c) &= N_{L/K}(c) = N_{N/K}(N_{L/N}(c)) = N_{N/K}(\mathrm{Nrd}_{C_D(N)}(c))\\ &= N_{N/K}(\mathrm{Nrd}_{C_D(N)}(l)) = \mathrm{Nrd}_D(l) = 1.\end{aligned}$$

Thus, $\mathrm{Nrd}_{C_D(N)}(lc^{-1}) = 1$ and $\mathrm{Nrd}_D(c) = 1$. Taking these two equalities into account, the proof of the lemma is completed as follows. If lc^{-1} and c belong to $U(D,\tau)'$, then the same is true of l. To prove the lemma we use induction on $\mathrm{ind}\,D$. When $\mathrm{ind}\,D$ is a prime number, Theorem 3 holds true and the lemma holds too. Now let $\mathrm{ind}\,D$ be distinct from a prime. Consider the algebra $D' = C_D(N)$ and the element $l' = lc^{-1}$. By the inductive hypothesis Theorem 3 holds true for D', whose index is less than $\mathrm{ind}\,D$; hence, in particular, $lc^{-1} \in U(D', \tau|_{D'})'$. Now, to complete the proof of the lemma is suffices to show that $c \in U(D,\tau)'$.

Let $\langle\sigma\rangle = \mathrm{Gal}(N/K)$. Recall that N/k is a separable extension because $\mathrm{char}\,\overline{k} \neq 2$ and $\mathrm{ind}\,D$ and $\mathrm{char}\,\overline{k}$ are coprime. Then there exists $g \in D$ such that $i_{g^{-1}}|_N = \sigma$. Let $N_\tau = k(\beta)$. Then $g\beta g^{-1} = \beta^\sigma$. We apply τ to both sides of this equality: $g^{-\tau}\beta g^\tau = \beta^{\sigma\tau}$. Since $\mathrm{Gal}(N/k)$ is either a generalized dihedral group or a direct product of groups of order 2, we have $\beta^{\sigma\tau} = \beta^{\sigma^{-1}} = g^{-1}\beta g$. It follows from this that $g^\tau g^{-1} \in C_D(N)$. Hence $g^\tau = rg$ for some $r \in C_D(N)$. Note that σ can be extended to an automorphism of the whole centralizer $C_D(N)$, since the conjugation by g maps the field N to itself. Consider the element $g^\tau + g = (r+1)g$. Note that $(g^\tau + g)^p = (r+1)g(r+1)g\cdots(r+1)g = (r+1)(r+1)^\sigma\cdots(r+1)^{\sigma^{p-1}}g^p$. Let $r \neq -1$. Denote the element $(r+1)(r+1)^\sigma\cdots(r+1)^{\sigma^{p-1}} \in C_D(N)$ by R. Consider the τ-invariant ramified algebra $A = \langle N(Rg^p), g^\tau + g\rangle$ of prime index that is central over $K(Rg^p)$. (If $r = -1$, then let $A = \langle NK(g^p), g\rangle$.) Note that $c \in \mathrm{SU}(A, \tau|_A) \cap (1 + M_A)$. Indeed, first of all, let us show that $N_{N(Rg^p)/K(Rg^p)}(c) = 1$. To do this we establish the equality $N_{N/K}(c) = 1$. From (9.1) we obtain $N_{N/K}(\mathrm{Nrd}_{C_D(N)}(c)) = 1$, and since $\mathrm{Nrd}_{C_D(N)}(l) = \mathrm{Nrd}_{C_D(N)}(c)$, we have $N_{N/K}(\mathrm{Nrd}_{C_D(N)}(c)) = 1$, which yields $(N_{N/K}(c))^{\mathrm{ind}\,C_D(N)} = 1 \in 1 + M_K$. In view of the equality $(\mathrm{ind}\,C_D(N), \mathrm{char}\,\overline{k}) = 1$ we have $N_{N/K}(c) = 1$. Moreover, it follows from $c = \sqrt[{[N(l):N]}]{e^{\tau-1}}$ that $c^{[N(l):N]} = e^{\tau-1}$. Then $(N_{N/N_\tau}(c))^{[N(l):N]} = 1 \in 1 + M_{N_\tau}$. Consequently, $N_{N/N_\tau}(c) = 1$, which means that $c \in U(D,\tau)$. Thus, $c \in \mathrm{SU}(A, \tau|_A) \cap (1 + M_A)$. Note also that the algebra A is ramified over $K(Rg^p)$ (over $K(g^p)$, respectively), and therefore by Proposition 12 (for ramified algebras of prime index) the congruence theorem holds for the algebra A and the element c. Hence $c \in U(D,\tau)'$. The proof is complete.

Proof of Theorem 3. First recall Remark 12. Let $a \in (1+M_D) \cap \mathrm{SU}(D,\tau)$. If $a \in K$ and $n = \operatorname{ind} D$, then $a^n = 1$, which means that a is an nth root of unity. Then it follows from $(\operatorname{ind} D, \operatorname{char} \overline{k}) = 1$ that $a = 1$. The case when $\operatorname{char} \overline{k} = 0$ is considered similarly. Thus, we assume below that $K(a) \neq K$.

In the proof of the theorem we can restrict our considerations to the case when a has the property $\overline{K(a)} \neq \overline{K}$. Indeed, if the extension $K(a)/K$ is totally ramified, then consider a τ-invariant inertia algebra I containing the element l mentioned in Lemma 28. Note that $a = (al)l^{-1}$, where $al \in \mathrm{SU}(D,\tau)$ and $\overline{K(al)}$ contains $\overline{K(l)}$ and therefore $\overline{K(al)} = \overline{K(l)} = \widetilde{L}$. Thus, if we prove that $al \in U(D,\tau)'$, then $a = (al)l^{-1}$ will imply that $a \in U(D,\tau)'$. Hence we can assume without loss of generality that $\overline{K(a)} \neq \overline{K}$.

Let us show that when the extension $K(a)/K$ is unramified, we can assume without loss of generality that $Z(\overline{D}) \neq \overline{K}$. Indeed, if $Z(\overline{D}) = \overline{K}$, then, since $K(a)/K$ is unramified (by Theorem 16) there exists a τ-invariant inertia algebra I containing $K(a)$. By assumption $D = I \otimes_K T$, where T is a weakly totally ramified algebra. Since $\mathrm{Nrd}_D(a) = 1$ and

$$1 = \mathrm{Nrd}_D(a) = (\mathrm{Nrd}_I(a))^{\lambda_D},$$

it immediately follows from the coprimality of $\operatorname{ind} D$ and $\operatorname{char} \overline{k}$ that $\mathrm{Nrd}_I(a) = 1$, and therefore $a \in U(I, \tau|_I)'$, because I is an unramified $Z(I)$-algebra.

Thus, if $K(a)/K$ is unramified, then we can assume that $Z(\overline{D}) \neq \overline{K}$. To prove the theorem in this case we use induction on $\operatorname{ind} D$. As above, let $a \in (\mathrm{SU}(D,\tau) \cap (1 + M_D)) \setminus K$. It is easily seen that the theorem holds in the case when D has a prime index.

Let I be a τ-invariant inertia algebra such that $K(a) \subset I$, which exists because the field $K(a)$ is τ-invariant. Denote by N/K an unramified τ-invariant cyclic extension of prime degree which is contained in $Z(I)$. Then the element $a \in C_D(N)$ commutes with the elements of N. Since $\mathrm{Nrd}_D(a) = 1$ and $(\operatorname{ind} D, \operatorname{char} \overline{k}) = 1$, we obtain $N_{K(a)/K}(a) = 1$ (recall that $a \in 1+M_D$). This implies that $N_{N(a)/N}(a) = 1$. Consider the centralizer $C_D(N)$. Note that $\operatorname{ind} C_D(N) < \operatorname{ind} D$ and $\tau|_{C_D(N)}$ satisfies again a condition similar to condition (ii) in Theorem 3. If we assume that our assertion holds for algebras of index less than $\operatorname{ind} D$, then it follows from the above that $a \in U(D,\tau)'$.

Now we prove the theorem in the case when $K(a)$ is ramified over K. We use induction on $\operatorname{ind} D$. If $\operatorname{ind} D$ is a prime number, then by Proposition 12 the group $\mathrm{SU}(D,\tau)$ has the congruence property. Suppose that $\operatorname{ind} D$ is not a prime. Denote the maximal τ-invariant unramified extension K contained in $K(a)$ by N_a. Then $N_a/K(a)$ is a totally ramified extension. Consider the centralizer $C_D(N_a)$ and note that $N_a \neq K$, because otherwise we arrive at the situation where $K(a)/K$ is a totally ramified extension, which we considered above. Since N_a is τ-invariant, we have $C_D(N_a)^\tau = C_D(N_a)$. Moreover, $\operatorname{ind} C_D(N_a) < \operatorname{ind} D$ and $\mathrm{Nrd}_{C_D(N_a)}(a) = 1$. The last equality follows from the fact that $a \in 1 + M_D$ and

$$\mathrm{Nrd}_D(a) = N_{N_a/K}(\mathrm{Nrd}_{C_D(N_a)}(a)) = (\mathrm{Nrd}_D(a))^{[N_a:K]} = 1.$$

Since $[N_a : K]$ divides $\operatorname{ind} D$ and therefore is coprime to $\operatorname{char} \overline{k}$, we have $\mathrm{Nrd}_{C_D(N_a)}(a) = 1$. Applying now the inductive hypothesis to $C_D(N_a)$ and the element a we obtain $a \in U(D,\tau)'$.

§ 10. Special cases of the computation of the groups $\mathbf{SUK}_1^{\mathrm{an}}(\boldsymbol{D},\boldsymbol{\tau})$

In conclusion consider several examples of the computation of the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$.

We assume below that $D \in \mathrm{TR}(K)$, $\operatorname{char}\overline{k} \neq 2$ and k is Henselian.

For unramified algebras D the following theorem is valid.

Theorem 19. *Suppose that the algebra D is unramified. Then the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ and $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau})$ are isomorphic if the involution $\overline{\tau}$ has the form $\overline{\tau}_{\overline{L}}(u)$, where $u \in U(\overline{D},\overline{\tau})$.*

The last condition holds for quaternion algebras D.

Proof. Since the algebra D is unramified, we have $\lambda_D = 1$, and since the column of the diagram in Theorem 2 is exact, we have $\mathrm{SUK}_1^{v}(D,\tau) \cong \overline{\mathrm{SU}(D,\tau)}/\overline{U'}$. Note that in our case $\mathrm{Nrd}_{\overline{D}}(\overline{\mathrm{SL}^v(D)}) = 1$, and therefore it follows from the exactness of the sequence (3) in Theorem 2 that the groups $\mathrm{SUK}_1^{v}(D,\tau)$ and $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau})$ are isomorphic, which yields that the sequence

$$1 \to E \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to 1$$

is exact. Thus (see Theorem 3), if the involution $\overline{\tau}$ has the form $\overline{\tau}_L(u)$ for $u\in U(\overline{D},\overline{\tau})$, then $E = 1$. This implies that $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \cong \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau})$. In the case when D is a quaternion algebra the condition concerning the involution $\overline{\tau}$ holds by to a result due to Albert [39]. The proof of the theorem is complete.

We assume below that the algebra D has a nontrivial ramification.

For commutative algebras $\overline{D}$ the following theorem holds.

Theorem 20. *Let $\overline{D}$ be a field. Then $E = 1$ and the following sequence is exact*:

$$1 \to \{\overline{z} \in \overline{Z} \mid N_{\overline{Z}/\overline{K}}(\overline{z}) \in \overline{k}\}/\overline{Z}^*_{\overline{\tau}} \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to E_\lambda \to 1.$$

In particular, if $E_\lambda = 1$, then $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \cong \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$.

Proof. By Proposition 12 we have $E = 1$. First of all, note that $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) = \mathrm{SU}(\overline{D},\overline{\tau}) = 1$ since $\mathrm{Nrd}_{\overline{D}} = \mathrm{id}_{\overline{D}}$. Hence, taking the relation $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) = 1$ and the exact sequence (6.2) into account, we obtain $\mathrm{SUK}_1^{v}(D,\tau) \cong \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. In view of this isomorphism, taking the sequence (6.3) into account we conclude that the following sequence is exact:

$$1 \to \{\overline{z} \in \overline{Z} \mid N_{\overline{Z}/\overline{K}}(\overline{z}) \in \overline{k}\}/\overline{Z}^*_{\overline{\tau}} \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to E_\lambda \to 1.$$

The proof is complete.

Now consider the case when the upper ramification index of the algebra D is trivial.

Theorem 21. *If $\lambda = 1$, then the following sequence is exact*:

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to 1.$$

Proof. Suppose that $\lambda = 1$. Then $E_\lambda = 1$. Since, in addition $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau) = \mathrm{SUK}_1^{v}(D,\tau)$, it follows from the exactness of the sequence (6.5) that the following sequence is also exact:

$$1 \to \mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to 1.$$

The proof is complete.

Now we consider special fields $\overline{k}$.

Proposition 17. *Let $\overline{k}$ be a field such that* $\dim\overline{k} \leqslant 1$ (*see* [46], *Ch.* 2, § 3). *Then the following sequence is exact*:

$$1 \to \mathrm{SL}(\overline{Z}/\overline{K}))/(\mathrm{SL}(\overline{Z}/\overline{K})) \cap \overline{Z}^*_{\overline{\tau}}) \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to E_\lambda \to 1.$$

Proof. Since $\dim\overline{k} \leqslant 1$, for any L of finite degree of $\overline{k}$ the Brauer group $\mathrm{Br}(L)$ is trivial, and therefore $\overline{D}$ is a field. Hence the group E is trivial. As shown above, in this case the following sequence is exact:

$$1 \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to E_\lambda \to 1.$$

The proof is complete.

Thus, the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ is an extension of $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ by the subgroup E_λ of the group of λth roots of unity belonging to the field K. Consider the group $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Note that $\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ coincides with the multiplicative group $\overline{Z}^*_{\overline{\tau}}$ of the field $\overline{Z}_{\overline{\tau}}$ and $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}} = \overline{Z}^*_{\overline{\tau}}\,\mathrm{SL}(\overline{Z}/\overline{K})$. Consequently,

$$\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} = (\overline{Z}^*_{\overline{\tau}}\,\mathrm{SL}(\overline{Z}/\overline{K}))/\overline{Z}^*_{\overline{\tau}},$$

which implies that

$$\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \cong \mathrm{SL}(\overline{Z}/\overline{K}))/(\mathrm{SL}(\overline{Z}/\overline{K})) \cap \overline{Z}^*_{\overline{\tau}})$$

by the isomorphism theorem for groups.

Now consider the case of finite $\overline{k}$. Since computations for the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ are closely related to the groups E, E_λ and $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$, which are defined in terms of the residue algebras $\overline{D}$, we preface these computations by a description of the structure of $\overline{D}$. Since $\dim\overline{k} \leqslant 1$, we have $\overline{D} = \overline{Z}$. Let us show that the degree $[\overline{Z}:\overline{K}]$ is not greater than 2. Namely, we show that if $[\overline{Z}:\overline{K}] \neq 1$, then $[\overline{Z}:\overline{K}] = 2$. In the case when $[\overline{Z}:\overline{K}] \neq 1$ we can apply Proposition 7 to the algebra D. Let us show that there are no generalized dihedral groups among the groups $\mathrm{Gal}(Z_j/k)$ listed in the formulation of Proposition 7.

Suppose that the extension K/k is unramified. Then Z/k is also unramified. This implies that $\mathrm{Gal}(Z/k) \cong \mathrm{Gal}(\overline{Z}/\overline{k})$. By Proposition 7 $\mathrm{Gal}(\overline{Z}/\overline{k})$ is a direct product of groups $\mathrm{Gal}(\overline{Z}_j/\overline{k})$, which are either generalized dihedral groups or groups of exponent 2. Suppose that, among the groups $\mathrm{Gal}(\overline{Z}_j/\overline{k})$, $1 \leqslant j \leqslant r$, there is a group $\mathrm{Gal}(\overline{Z}_{j_0}/\overline{k})$ that is a generalized dihedral group. On the other hand, since $\overline{k}$ is finite, this group must be cyclic. Hence there are no dihedral groups among the groups $\mathrm{Gal}(\overline{Z}_j/\overline{k})$.

Now suppose that K/k is totally ramified and $\mathrm{Gal}(Z_{j_0}/k)$ is a generalized dihedral group. Then $\mathrm{Gal}(Z_{j_0}/K)$ has an odd order. By Theorem 13 there exists a τ-invariant unramified lift N/k of the extension $\overline{Z}_{j_0}/\overline{k}$ to Z_{j_0}/k. Since $\overline{Z}_{j_0}/\overline{k}$ is a Galois extension, N/k is a Galois extension too. Now it is easily seen that Z_{j_0}/k is isomorphic to $(N \otimes_k K)/k$, and therefore Z_{j_0}/k is Abelian. This means that there are no generalized dihedral groups among the groups $\mathrm{Gal}(Z_j/k)$.

Hence all groups $\mathrm{Gal}(Z_j/k)$ have exponent 2. Since $Z = Z_1 \times \cdots \times Z_r$ by Proposition 7 and $\mathrm{Gal}(Z/K)$ is a subgroup of the Galois group $\mathrm{Gal}(Z/k)$, this group also has exponent 2. The extension Z/K is unramified, so $\mathrm{Gal}(\overline{Z}/\overline{K})$ is a group of exponent 2. Assume that $r > 1$. Then $\mathrm{Gal}(\overline{Z}/\overline{K})$ contains a subfield that is a direct compositum of quadratic extensions Q_1 and Q_2. As the field $\overline{k}$ is finite, the field $Q_1 \times Q_2$ contains divisors of zero, which is impossible. Therefore, $r = 1$. Thus, $[\overline{Z} : \overline{K}] = 2$.

As a result, $\overline{D}$ is a field such that $[\overline{D} : \overline{K}] \leqslant 2$.

Now consider the groups $\mathrm{SUK}_1^{\mathrm{an}}(D, \tau)$. Note that $E = 1$, because $\overline{D}$ is a field. As concerns the group E_λ, below we consider the cases of a totally ramified and an unramified extension K/k separately.

Let K/k be totally ramified. In this case $E_\lambda = 1$ (Lemma 23). Let K/k be an unramified extension. Since D has a unitary involution, we have $D = D_1 \otimes_k K$, where D_1 is an appropriate quaternion k-algebra. Note that $\overline{D}_1$ contains no unramified quadratic extensions over k. Otherwise the algebra $\overline{D}_1 \times_{\overline{k}} \overline{K}$ has divisors of zero. Hence $\overline{D} = \overline{Z} = \overline{K}$. We show that in this case we also have $E_\lambda = 1$. In view of the relation $\overline{D} = \overline{Z} = \overline{K}$, (6.1) assumes the form $E_\lambda = C_\lambda(\overline{K}) \cap \overline{K}^{\overline{\tau}-1}$.

To apply Theorem 2 we also need to compute the groups $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D}, \overline{\tau})$ and $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Since $\overline{D}$ is a field, we have $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D}, \overline{\tau}) = \mathrm{SU}(\overline{D}, \overline{\tau}) = 1$.

Consider the groups $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. First suppose that $\overline{D} = \overline{Z} = \overline{K}$. Then $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}} = \{z \in \overline{Z} \mid N_{\overline{Z}/\overline{K}}(z) \in \overline{k}\} = \overline{Z}_{\overline{\tau}}$ and $\Sigma_{\mathrm{Nrd}_{\overline{D}}} = \overline{Z}_{\overline{\tau}}$. This implies that $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}} = \overline{Z}_{\overline{\tau}}$, which coincides with $\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Hence $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} = 1$. As noted above, in the case when $[\overline{Z} : \overline{K}] = 2$ the extension K/k must be totally ramified. In this situation the group $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}$ coincides with $\overline{Z}^*$ since $\overline{K} = \overline{k}$, and $\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ coincides with $\overline{Z}^*_{\overline{\tau}}$. Hence $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} = \overline{Z}^*/\overline{Z}^*_{\overline{\tau}}$.

Applying Theorem 2 to the case when K/k is a totally ramified extension we obtain $\mathrm{SUK}_1^{\mathrm{an}}(D, \tau) \cong \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Finally,

$$\mathrm{SUK}_1^{\mathrm{an}}(D, \tau) = \begin{cases} 1 & \text{if } \overline{Z} = \overline{K}, \\ \overline{Z}^*/\overline{Z}^*_{\overline{\tau}} & \text{if } [\overline{Z} : \overline{K}] = 2. \end{cases}$$

Consider the case of an unramified K/k. Then the following sequences are exact:

$$1 \to \mathrm{SUK}_1^v(D, \tau) \to \mathrm{SUK}_1^{\mathrm{an}}(D, \tau) \to C_\lambda(\overline{K}) \cap \overline{K}^{\overline{\tau}-1} \to 1$$

and

$$1 \to \mathrm{SUK}_1^v(D, \tau) \to \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \to 1.$$

Since $\overline{D} = \overline{Z} = \overline{K}$, the same arguments as in the case of totally ramified K/k prove that $\mathrm{SUK}_1^v(D, \tau) \cong \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$. Finally, $\mathrm{SUK}_1^v(D, \tau) = 1$. Thus, $\mathrm{SUK}_1^{\mathrm{an}}(D, \tau) \cong C_\lambda(\overline{K}) \cap \overline{K}^{\overline{\tau}-1}$.

The following proposition summarizes the above discussion.

Proposition 18. *Let $\overline{k}$ be a finite field*, $\operatorname{char}\overline{k} \neq 2$, *and assume that a central algebra $D \in \mathrm{TR}(K)$ has a unitary involution τ. Then the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ can be computed in the following way*: *if K/k is totally ramified, then always $[\overline{Z} : \overline{K}] \leqslant 2$ and*

$$\mathrm{SUK}_1^{\mathrm{an}}(D,\tau) = \begin{cases} 1 & \text{if } \overline{Z} = \overline{K}, \\ \overline{Z}^{\,*}/\overline{Z}^{\,*}_{\overline{\tau}} & \text{if } [\overline{Z} : \overline{K}] = 2, \end{cases}$$

whereas if K/k is unramified, then $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \cong C_\lambda(\overline{K}) \cap \overline{K}^{\,\overline{\tau}-1}$.

Remark 13. The above argument can also be used in the case of an infinite field $\overline{k}$. For example, if $\overline{k}$ is the field of formal power series in one variable with coefficients in an algebraically closed field of characteristic 0, then very much the same argument as in the case of a finite field $\overline{k}$ produces similar final results on the computation of $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ in this case.

Remark 14. Note that if k is a local field (a finite extension of the field of p-adic numbers or the field of formal power series in one variable with finite field of constants), then the computation of the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ can be reduced to the case considered above. Indeed, since $\overline{k}$ is a Henselian field with finite residue field, the algebra D has a Henselian valuation with finite residue field (namely, a valuation composed of the original valuation and the valuation of the field $\overline{k}$).

Consider another example, where $\overline{k}$ is a real closed field. In this case the argument is similar to the reasoning carried out above, so we present only the formulations and sketches of proofs of the corresponding assertions. First we describe the algebras $\overline{D}$.

Proposition 19. *Let $\overline{k}$ be real closed. Then the structure of the residue algebra $\overline{D}$ is as follows.*

1. *If $\overline{D}$ is not a field*, *then $\overline{Z} = \overline{K}$.*
2. *If $\overline{D}$ is a field*, *then $\overline{D} = \overline{Z}$ and the following possibilities hold for the fields $\overline{Z}$*, *$\overline{K}$ and $\overline{k}$*:
   i) $\overline{Z} = \overline{K} = \overline{k}$;
   ii) $\overline{Z} \neq \overline{K} = \overline{k}$;
   iii) $\overline{Z} = \overline{K} \neq \overline{k}$.

The proof is evident since $\overline{k}$ is real closed and the extensions $\overline{K}/\overline{k}$, $\overline{Z}/\overline{k}$ and $\overline{D}/\overline{k}$ are finite.

Consider the groups $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$. We make use of Theorem 2.

It turns out that for all algebras listed above we have $E = 1$. In case 1 we have $E = 1$ by Theorem 18, while in all other cases $\overline{D}$ is a field and the result that $E = 1$ follows from Proposition 12.

For all algebras listed above, except the ones in case 2, iii), we have $E_\lambda = 1$, since in all these cases the extension K/k is totally ramified. In case 2, iii) the composition of homomorphisms $N_{\overline{Z}/\overline{K}} \circ \mathrm{Nrd}_{\overline{D}}$ is the identity homomorphism. Bearing in mind that $\overline{s} = 1$ for $s \in \mathrm{SU}(D,\tau)$, this gives $E_\lambda = 1$ in this case too.

Now we compute the groups $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau})$. If $\overline{D}$ is not a field, then the algebra $\overline{D}$ contains a quaternion $\overline{k}$-algebra A such that $\overline{D} = A \otimes_{\overline{k}} \overline{K}$ and the restriction of $\overline{\tau}$ to A is the standard quaternion conjugation. Note that $U(\overline{D},\overline{\tau}) = \{u \in \overline{D} \mid uu^{\overline{\tau}} = 1\}$. On the other hand the equation $uu^{\overline{\tau}} = 1$ is equivalent to $\mathrm{Nrd}_{\overline{D}}(u) = 1$. Hence $\mathrm{SU}(\overline{D},\overline{\tau}) = \mathrm{SL}_1(\overline{D})$. By definition we have

$$\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) = \mathrm{SU}(\overline{D},\overline{\tau})/U(\overline{D},\overline{\tau})' = \mathrm{SL}_1(\overline{D})/\,\mathrm{SL}_1(\overline{D})'.$$

Moreover,

$$\overline{D}' \subset \mathrm{SL}_1(\overline{D})'.$$

Indeed, for $a, b \in \overline{D}^*$

$$[a,b] = [\mathrm{Nrd}_{\overline{D}}(a)^{-1}a, \mathrm{Nrd}_{\overline{D}}(b)^{-1}b].$$

Since the group $\mathrm{SK}_1(\overline{D})$ is trivial, it follows from the inclusion $\overline{D}' \subseteq \mathrm{SL}_1(\overline{D})'$ that the group $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau})$ is trivial.

Suppose that $\overline{D}$ is a field. Then $U(\overline{D},\overline{\tau})' = 1$. Therefore, in all remaining cases we have $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) = \mathrm{SU}(\overline{D},\overline{\tau})$. Let $s \in \mathrm{SU}(\overline{D},\overline{\tau})$, which means that $\mathrm{Nrd}_{\overline{D}/\overline{Z}}(s) = 1$. Since $\overline{D} = \overline{Z}$, we have $s = 1$. Thus, $\mathrm{SUK}_1^{\mathrm{an}}(\overline{D},\overline{\tau}) = 1$ in all cases.

Let us compute the groups $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ in cases 1)—2, iii) of Proposition 19.

Case 1. $\overline{D}$ is not a field. In this case the reduced values of the elements in $\overline{D}$ are zeros of the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ in the variables x_1, x_2, x_3, x_4 over $\overline{K}$ and, since $\overline{K} = \overline{k}$, of the quadratic form in these variables over $\overline{k}$. This implies that $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}} = \Sigma_{\mathrm{Nrd}_{\overline{D}}}$, which means that $\Sigma^1\mathrm{Nrd}_{\overline{D}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ is trivial.

Case 2, i). $\mathrm{Nrd}_{\overline{D}} = \mathrm{id}$, and since $\overline{Z} = \overline{K} = \overline{k}$, we have $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}} = \overline{k}^*$. This means that $\mathrm{Nrd}_{\overline{D}}(\overline{D}_{\overline{\tau}})$ also coincides with $\overline{k}^*$.

Case 2, ii). In this case the fact that the element $z \in \overline{Z}$ belongs to $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}$ means that $N_{\overline{Z}/\overline{K}}(z) \in \overline{k}$, since $\overline{K} = \overline{k}$ $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}$ coincides with $\overline{Z}^*$. The group $\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ coincides with $\overline{Z}^*_{\overline{\tau}}$. Hence $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \cong \overline{Z}^*/\overline{Z}^*_{\overline{\tau}}$.

Case 2, iii). In this case for $z \in \overline{Z}$ we have $\mathrm{Nrd}_{\overline{D}}(z) = z$, therefore, the condition that z belongs to the group $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}$ means that z belongs to $\overline{k}$. Note that $\mathrm{Nrd}_{\overline{D}}(\overline{D})^*_{\overline{\tau}} = \overline{Z}^*_{\overline{\tau}}$. Consequently, $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}} \cong \overline{Z}^*/\overline{Z}^*_{\overline{\tau}}$, which in view of the equality $\overline{Z} = \overline{K}$ implies that the groups $\Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ and $\overline{K}^*/\overline{k}$ are isomorphic.

The results obtained above, in combination with Theorem 2, establish the following proposition.

Proposition 20. *Suppose that $\overline{k}$ is real closed. Then the group $\mathrm{SUK}_1^{\mathrm{an}}(D,\tau)$ is trivial, except for the cases* 2, ii) *and* 2, iii), *where it is isomorphic to $\overline{Z}^*/\overline{Z}^*_{\overline{\tau}}$ and $\overline{K}^*/\overline{k}^*$, respectively.*

Consider one more important example of the field $\overline{k}$.

Proposition 21. *Let $\overline{k}$ be an extension of an algebraically closed field with transcendence degree* 1. *Then $\mathrm{SUK}_1^{v}(D,\tau) \cong \Sigma^1_{\mathrm{Nrd}_{\overline{D}}}/\Sigma_{\mathrm{Nrd}_{\overline{D}}}$ and the following sequence is exact*:

$$1 \to \mathrm{SUK}_1^{v}(D,\tau) \to \mathrm{SUK}_1^{\mathrm{an}}(D,\tau) \to E_\lambda \to 1,$$

where

$$E_\lambda = \begin{cases} 1 & \text{if } K/k \text{ is totally ramified,} \\ 1 & \text{if } K/k \text{ is unramified, } \lambda \text{ is odd,} \\ 1 & \text{if there exists no element } s \in \mathrm{SU}(D,\tau) \text{ such that } N_{\overline{Z}/\overline{K}}(\overline{s}) = \overline{-1}, \\ \mathbb{Z}/2 & \text{otherwise.} \end{cases}$$

Theorem 2 allows one to obtain simple formulae in the case of a field $\overline{k}$ of algebraic numbers and algebras D of odd indices, which we do not present here because their proofs are exceedingly lengthy.

The author is profoundly grateful to the referee, who read the preliminary version of the paper attentively and made a lot of useful comments.

Bibliography

[1] E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York–London 1957, x+214 pp.

[2] J. A. Dieudonné, *La géométrie des groupes classiques*, 3ème éd., Ergeb. Math. Grenzgeb., vol. 5, Springer-Verlag, Berlin–New York 1971, viii+129 pp.

[3] N. Bourbaki, "Ch. 7: Modules sur les anneaux principaux", *Éléments de mathématique. Livre* II: *Algèbre*, Ch. 6: Groupes et corps ordonnés. Ch. 7: Modules sur les anneaux principaux, Actualités Sci. Indust., vol. 1179, Hermann, Paris 1952; Ch. 8: Modules et anneaux semi-simples, vol. 1261, 1958, 189 pp.; Ch. 9: Formes sesquilinéaires et formes quadratiques, vol. 1272, 1959, 211 pp.

[4] A. Borel, *Linear algebraic groups*, Math. Lecture Note Ser., W. A. Benjamin, Inc., New York–Amsterdam 1969, xi+398 pp.

[5] T. A. Springer, *Linear algebraic groups*, 2nd ed., Progr. Math., vol. 9, Birkhäuser Boston, Inc., Boston, MA 1998, xiv+334 pp.

[6] J. E. Humphreys, *Linear algebraic groups*, Grad. Texts Math., vol. 21, Springer-Verlag, New York–Heidelberg 1975, xiv+247 pp.

[7] V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory*, Nauka, Moscow 1991, 656 pp.; English transl., Pure Appl. Math., vol. 139, Academic Press, Inc., Boston, MA 1994, xii+614 pp.

[8] J. Tits, "Algebraic and abstract simple groups", *Ann. of Math.* (2) **80**:2 (1964), 313–329.

[9] V. P. Platonov, "On the Tannaka-Artin problem", *Dokl. Akad. Nauk SSSR* **221**:5 (1975), 1038–1041; English transl. in *Soviet Math. Dokl.* **16** (1975), 468–473.

[10] Ph. Gille, "Le problème de Kneser-Tits", *Séminaire N. Bourbaki*, vol. 2007/2008, Astérisque, vol. 326, Soc. Math. France, Paris 2009, pp. vii, 39–81, Exp. No. 983.

[11] J. Tits, "Groupes de Whitehead de groupes algébriques simples sur un corps", d'après V. P. Platonov et al., *Séminaire N. Bourbaki*, vol. 1976/1977, Lecture Notes in Math., vol. 677, Springer, Berlin 1978, pp. 218–236, Exp. No. 505.

[12] V. I. Yanchevskii, "Reduced unitary K-theory and division rings over discretely valued Hensel fields", *Izv. Akad. Nauk SSSR Ser. Mat.* **42**:4 (1978), 879–918; English transl. in *Izv. Math.* **13**:1 (1979), 175–213.

[13] V. P. Platonov and V. I. Yanchevskii, "On the Kneser-Tits conjecture for unitary groups", *Dokl. Akad. Nauk SSSR* **225**:1 (1975), 48–51; English transl. in *Soviet Math. Dokl.* **16** (1975), 1456–1460.

[14] V. P. Platonov and V. I. Yanchevskii, "SK_1 for division rings of noncommutative rational functions", *Dokl. Akad. Nauk SSSR* **249**:5 (1979), 1064–1068; English transl. in *Soviet Math. Dokl.* **20** (1979), 1393–1397.

[15] V. P. Platonov, "The Tannaka-Artin problem and reduced K-theory", *Izv. Akad. Nauk SSSR Ser. Mat.* **40**:2 (1976), 227–261; English transl. in *Izv. Math.* **10**:2 (1976), 211–243.

[16] V. P. Platonov, "Birational properties of the reduced Whitehead group", *Dokl. Akad. Nauk. Bel. SSR* **21**:3 (1977), 197–198; English transl. in *Selected papers in K-theory*, Amer. Math. Soc. Transl. Ser. 2, vol. 154, Amer. Math. Soc., Providence, RI 1992, pp. 7–9.

[17] V. I. Yanchevskii, "Division rings over Hensel discretely valued fields and the Tannaka-Artin problem", *Dokl. Akad. Nauk SSSR* **226**:2 (1976), 281–283; English transl. in *Soviet Math. Dokl.* **17** (1976), 113–116.

[18] V. I. Yanchevskii, "A converse problem in reduced unitary K-theory", *Mat. Zametki* **26**:3 (1979), 475–482; English transl. in *Math. Notes* **26**:3 (1979), 728–731.

[19] V. I. Yanchevskii, "A converse problem in reduced unitary K-theory", *Mat. Sb.* **110(152)**:4(12) (1979), 579–596; English transl. in *Sb. Math.* **38**:4 (1981), 533–548.

[20] P. Draxl, "SK_1 von Algebren über vollständig diskret bewerteten Körpern und Galoiskohomologie abelscher Körpererweiterungen", *J. Reine Angew. Math.* **1977**:293/294 (1977), 116–142.

[21] P. Draxl, "Ostrowski's theorem for Henselian valued skew fields", *J. Reine Angew. Math.* **1984**:354 (1984), 213–218.

[22] R. Hazrat and A. R. Wadsworth, "SK_1 of graded division algebras", *Israel J. Math.* **183** (2011), 117–163.

[23] R. Hazrat and A.Ṙ. Wadsworth, "Unitary SK_1 of graded and valued division algebras", *Proc. Lond. Math. Soc.* (3) **103**:3 (2011), 508–534.

[24] A. S. Merkurjev, "Generic element in SK_1 for simple algebras", *K-Theory* **7**:1 (1993), 1–3.

[25] V. P. Platonov, "Algebraic groups and reduced K-theory", *Proceedings of the international congress of mathematicians* (Helsinki 1978), Acad. Sci. Fennica, Helsinki 1980, pp. 311–317.

[26] A. Suslin, "SK_1 of division algebras and Galois cohomology revisited", *Proceedings of the St. Petersburg Mathematical Society*, vol. XII, Amer. Math. Soc. Transl. Ser. 2, vol. 219, Amer. Math. Soc., Providence, RI 2006, pp. 125–147.

[27] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Transl. Math. Monogr., vol. 179, Amer. Math. Soc., Providence, RI 1998, xiv+218 pp.

[28] A. R. Wadsworth and V. I. Yanchevskiĭ, "Unitary SK_1 for a graded division ring and its quotient division ring", *J. Algebra* **352**:1 (2012), 62–78.

[29] A. R. Wadsworth, "Unitary SK_1 of semiramified graded and valued division algebras", *Manuscripta Math.* **139**:3–4 (2012), 343–389.

[30] B. Sury, "On $\mathrm{SU}(1,D)/[\mathrm{U}(1,D),\mathrm{U}(1,D)]$ for a quaternion division algebra D", *Arch. Math. (Basel)* **90**:6 (2008), 493–500.

[31] B. A. Sethuraman and B. Sury, "A note on the special unitary group of a division algebra", *Proc. Amer. Math. Soc.* **134**:2 (2006), 351–354.

[32] V. I. Yanchevskii, "Reduced Whitehead groups and the conjugacy problem for special unitary groups of anisotropic Hermitian forms", *Questions of the theory of representations of algebras and groups*. 23, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov (POMI), vol. 400, St Petersburg Department of Steklov. Mathematical Institute, St Petersburg 2012, pp. 222–245; English transl. in *J. Math. Sci. (N.Y.)* **192**:2 (2013), 250–262.

[33] V. P. Platonov and V. I. Yanchevskii, "Dieudonné's conjecture on the structure of unitary groups over a division ring, and Hermitian K-theory", *Izv. Akad. Nauk SSSR Ser. Mat.* **48**:6 (1984), 1266–1294; English transl. in *Izv. Math.* **25**:3 (1985), 573–599.

[34] V. P. Platonov and V. I. Yanchevskii, "On the theory of Henselian division algebras", *Dokl. Akad. Nauk SSSR* **297**:2 (1987), 294–298; English transl. in *Dokl. Math.* **36**:3 (1988), 468–472.

[35] V. P. Platonov and V. I. Yanchevskii, "Finite-dimensional Henselian division algebras", *Dokl. Akad. Nauk SSSR* **297**:3 (1987), 542–547; English transl. in *Dokl. Math.* **36**:3 (1988), 502–506.

[36] B. Jacob and A. Wadsworth, "Division algebras over Henselian fields", *J. Algebra* **128**:1 (1990), 126–179.

[37] Yu. L. Ershov, "Henselian valuations of division rings and the group SK_1", *Mat. Sb.* **117(159)**:1 (1982), 60–68; English transl. in *Sb. Math.* **45**:1 (1983), 63–71.

[38] A. V. Prokopchuk and V. I. Yanchevskiĭ, "Noncyclic unitary involutions of Henselian discretely normed algebras with division", *Isv. Nats. Akad. Nauk Belarusi Ser. Fiz.-Mat. Nauk*, 2014, no. 1, 51–53. (Russian)

[39] A. A. Albert, "Involutorial simple algebras and real Riemann matrices", *Ann. of Math.* (2) **36**:4 (1935), 886–964.

[40] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions*, Amer. Math. Soc. Colloq. Publ., vol. 44, Amer. Math. Soc., Providence, RI 1998, xxii+593 pp.

[41] U. Rehmann, S. V. Tikhonov and V. I. Yanchevskiĭ, "Prescribed behavior of central simple algebras after scalar extension", *J. Algebra* **351**:1 (2012), 279–293.

[42] P. Roquette, "Isomorphisms of generic splitting fields of simple algebras", *J. Reine Angew. Math.* **1984**:214/215 (1964), 207–226.

[43] S. V. Tikhonov and V. I. Yanchevskii, "Homomorphisms and involutions of unramified Henselian division algebras", *Questions of the theory of representations of algebras and groups*. 26, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov (POMI), vol. 423, St Petersburg Department of the Steklov Mathematical Institute, St Petersburg 2014, pp. 264–275; English transl. in *J. Math. Sci.* (*N.Y.*) **209**:4 (2015), 657–664.

[44] A. S. Merkur'ev (Merkurjev), "Norm principle for algebraic groups", *Algebra i Analiz* **7**:2 (1995), 77–105; English transl. in *St. Petersburg Math. J.* **7**:2 (1996), 243–264.

[45] A. A. Albert, *Structure of algebras*, Reprint of 1939 ed., Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, RI 1961, xi+210 pp.

[46] J.-P. Serre, *Cohomologie galoisienne*, Cours au Collège de France, 1962–1963, 2ème éd., Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin–Heidelberg–New York 1964, vii+212 pp. (not consecutively paged).

Vyacheslav I. Yanchevskiĭ
Institute of Mathematics of the National Academy
of Sciences of Belarus, Minsk, Belarus
E-mail: yanch@im.bas-net.by

Received 27/AUG/21 and 21/APR/22
Translated by A. PANKRAT'EV