Contemporary Mathematics
Volume 55, Part II, 1986

CENTRAL EXTENSIONS OF SL_2 OVER DIVISION RINGS AND SOME METAPLECTIC THEOREMS

Ulf Rehmann

This paper contains essentially three theorems together with their proofs: The first is a generalization of Matsumoto's description [9] of central extensions of SL_2 over fields (cf. Theorem 2.1 and Theorem 4.9). The second describes the tame splitting of the Schur multiplier of $SL_2(D)$ of a non-archimedean local division algebra D (cf. Theorem 5.6, Corollary 5.7). The third, and probably most important result, describes all continuous central extensions of $SL_r(D)$ of a non-archimedean local division algebra, by proving that - without any exception - the topological fundamental group of $SL_r(D)$ for all $r \geq 2$, is isomorphic to the group $\mu(K)$ of roots of unity of the center K of D and that there is a uniform description of this phenomenon in terms of the local power norm residue symbol of K (cf. Theorem 6.8, Corollary 6.9). On the basis of this last result and the existing literature (see below) it seems to be conceivable that an analogous result is true for arbitrary semisimple groups of positive rank over non-archimedean local fields and that a general proof will soon be forthcoming.

Since this paper is rather technical, it might be reasonable to discuss some of its aspects in this introduction.

Theorem 2.1 describes central extensions of $G = SL_2(D)$ for arbitrary skew fields D under the assumption that G is perfect (which is true in all interesting cases, e.g., if the center K of D is infinite - cf. §1). The description is in terms of suitable central extensions of the commutator subgroup $D^{*1} = [D^*, D^*]$ of the units D^* of D and extends results previously obtained by the author in the case $G = SL_r$, $r \geq 3$ [14]. These extensions of D^{*1} are described by generators and relations, which are technically more complicated than in the case

$r \geq 3$. The only "inhomogeneous" relation 2.1 γ) (this is a relation which allows changing the parity of the number of letters in a given word) requires certain entries to be commutators rather than arbitrary units.

Nevertheless, as applications, the two other theorems can be derived from it.

This presentation immediately allows one to define the tame symbol of $SL_2(D)$ as a straightforward generalization of the corresponding symbol which is known in the commutative situation in case $r \geq 3$ (cf. §5). The analogues notion for $r \geq 3$ has been discussed by Bak-Rehmann [1; §4]. To show the splitting property in case $r = 2$ (Theorem 5.2) some additional arithmetic work is necessary, which essentially consists in extending certain results of Carroll [6] to the situation considered. As to my knowledge, these results have been unknown even in the commutative case, where they describe certain properties of the "symplectic K_2" (cf. [9]). The result is the following: The Schur multiplier of G is isomorphic to a product of the multiplicative group of the residue field of the valuation ring $\mathcal{O}_K$ of K (the "tame" part) and the canonical image of the Schur multiplier of $SL_2(\mathcal{O}_D)$. The corresponding result for $r \geq 3$ is proved in [1; §4], in which case, in addition, it is known that the Schur multiplier of $SL_r(\mathcal{O}_D)$ injects into that of G. I do not know whether this is true as well in case $r = 2$.

The determination of the topological fundamental group of semisimple algebraic groups has a long history, beginning with the work of Moore [10] and Matsumoto [9], both in 1969, and investigating essentially K-split groups, Deodhar [8] (1978) for quasi-split groups; and more recently it became possible to handle groups defined in terms of (non-split) division algebras also, at least in almost all cases: SL_r $(r \geq 3)$ has been investigated by Bak-Rehmann ([1], 1982), while Prasad-Raghunathan ([12], 1984) have results including all isotropic semisimple groups over local fields. However, these last results ([1], [12]) all have the same gap in common: in a special dyadic situation (if a non-split division algebra is involved) it was not possible to decide whether the fundamental group should be $\mu(K)$ or $\mu(K)/\{\pm 1\}$. (For example, the group SL_r $(r \geq 2)$ over the quaternions over $\mathbb{Q}_2$ is such a case, which, on the other hand, has been treated already in the appendix of [1] by an ad-hoc construction of a suitable central extension.) The reason for this gap is a functorial deficiency of the local power norm residue symbol: To distinguish elements in the fundamental group, say $\pi_1(G)$, $G = SL_r(D)$, a standard technique is to split the underlying division algebra by a suitable splitting field E and to look at its canonical image in $\pi_1(G_E)$, $G_E = SL_r(D \otimes_K E)$. This has been investigated by Rehmann-Stuhler [15; §3], 1978, and in [1; §3, cf. p.500f.] with the result that, in the exceptional cases, there is no algebraic splitting field of D which allows one distinguishing $\pm 1 \in \pi_1(G)$ in this way. Similar results are obtained in [12; §8].

Of course this point of view invites one to try transcendental splitting fields of D, and the best possibility, of course, is the generic splitting field $\tilde{E}$ of D, which is characterized by the property that every splitting field of D is an extension of a specialization of $\tilde{E}$. It is known that the center K of D is algebraically closed in $\tilde{E}$ [18], but then one has, by a result of Suslin [21], 1982, the injectivity of the natural map $K_2(K) \to K_2(\tilde{E})$, which almost immediately yields the desired result if one uses the transfer techniques of [15], together with the main result of §6 of this paper, which says: Everything in $\pi_1(G)$ lies in the canonical image of $\pi_1(SL_r(L))$, where $L \subseteq D$ is a maximal unramified commutative subextension of K. (For $r \geq 3$, this is already contained in [1].) This together with an argument derived from the Skolem-Noether theorem, gives $|\mu(K)|$ as an upper bound of $|\pi_1(G)|$, thereby concluding the proof.

I would like to thank the Department of Mathematics of Cornell University for its hospitality during the last year and the Fulbright Foundation for a travel grant which made this stay possible. This paper was written during that stay.

Part I: Arbitrary Skew Fields

1. The Steinberg group of rank 2 over a skew field.

Let D be any skew field. The elementary group $E_2(D)$ of rank 2 over D is the 2×2-matrix group generated by the elementary matrices $e_{12}(u) := \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, $e_{21}(v) := \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}$, where $u, v \in D$. It contains the matrices

$$m_{ij}(u) := e_{ij}(u)e_{ji}(-u^{-1})e_{ij}(u), \quad d_{ij}(u) := m_{ij}(u)m_{ij}(-1),$$

where $1 \leq i, j \leq 2$, $i \neq j$, $u \in D^* := \{u \in D | u \neq 0\}$. We have

$$m_{12}(u) = \begin{pmatrix} 0 & u \\ -u^{-1} & 0 \end{pmatrix}, \quad m_{21}(u) = \begin{pmatrix} 0 & -u^{-1} \\ u & 0 \end{pmatrix},$$

$$d_{12}(u) = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \quad d_{21}(u) = \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix}.$$

Moreover, we define, for $u,v \in D^*$ and $[u,v] := uvu^{-1}v^{-1}$, the matrices

$$d_1([u,v]) := d_{12}(u)d_{12}(v)d_{12}(vu)^{-1} = \begin{pmatrix} [u,v] & 0 \\ 0 & 1 \end{pmatrix},$$

$$d_2([u,v]) := d_{21}(u)d_{21}(v)d_{21}(vu)^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & [u,v] \end{pmatrix}.$$

More generally, if $\xi = \prod_{j=1}^{n} [u_j,v_j] \in [D^*,D^*]$ is arbitrary ($u_j,v_j \in D^*$ for $j = 1,\ldots,n, n \in \mathbb{N}$), then, for $i = 1,2$, we define

$$d_i(\xi) := \prod_{j=1}^{n} d_i(u_j,v_j).$$

There are many obvious relations between the elementary matrices over D, and the definition of the Steinberg group mimics some of them:

1.1 <u>Definition</u>: The Steinberg group of rank 2 over D is the group $St_2(D)$ defined by the following presentation: For $i,j \in \{1,2\}$, $i \neq j$, we have the generators $x_{ij}(u)$, $u \in D$, and $w_{ij}(u)$, $u \in D^*$ and the relations

R1 $\quad x_{ij}(u)x_{ij}(v) = x_{ij}(u+v) \quad (u,v \in D)$

R2 $\quad w_{ij}(u) = x_{ij}(u)x_{ji}(-u^{-1})x_{ij}(u) \quad (u \in D^*)$

R3 $\quad w_{ij}(u)x_{ij}(v)w_{ij}(u)^{-1} = x_{ji}(-u^{-1}vu^{-1}) \quad (u,v \in D^*)$.

By R2, the $x_{ij}(u)$ are already a set of generators of $St_2(D)$, and by some computation one verifies that there is a group epimorphism $\varphi: St_2(D) \to E_2(D)$ defined by $x_{ij}(u) \mapsto e_{ij}(u)$.

1.2 <u>Theorem</u>: $\varphi: St_2(D) \to E_2(D)$ is a central extension of $E_2(D)$, i.e., kernel(φ) is central in $St_2(D)$. Moreover, if $|D| \neq 2,3$, then $St_2(D)$ and $E_2(D)$ are perfect groups, and if the center $Z(D)$ of D is not of order 2,3,4,9 then $St_2(D)$ is the universal central extension of $E_2(D)$.

1.3 Remark: If D is commutative, the assertions of 1.2 will follow from [7, Théorème 3] and [20; §4].

The proof of 1.2 will be given in several steps. By 1.3, we may restrict our considerations to the non-commutative case, which implies $|D| = \infty$.

Let H denote the subgroup of $St_2(D)$ generated by all elements $w_{ij}(u)\cdot w_{ij}(v)$ ($1 \leq i,j \leq 2$, $i \neq j$, $u,v \in D^*$). Hence $\varphi(H)$ consists of diagonal matrices only.

1.4 Lemma: H normalizes the subgroups $\langle x_{ij}(u) | u \in D\rangle$, more precisely: If $h \in H$ and $\varphi(h) = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$, then

$$hx_{12}(u)h^{-1} = x_{12}(d_1ud_2^{-1}), hx_{21}(u)h^{-1} = x_{21}(d_2ud_1^{-1}).$$

The proof is a straightforward application of R3.

1.5 Lemma: For every $\xi \in St_2(D)$ there exist $u,v,w \in D$, $h \in H$ such that $\xi = x_{12}(u)x_{21}(v)x_{12}(w)h$.

Proof: It suffices to show: The set of all elements of this type is invariant under left multiplication by $x_{ij}(a)$. But this follows from R1 and

1.6 Lemma: Let $1 \leq i, j \leq 2$, $i \neq j$. For any $u,v,w \in D$, $h \in H$ there exist $u',v',w' \in D$, $h' \in H$ such that

$$x_{ij}(u)x_{ji}(v)x_{ij}(w)h = x_{ji}(u')x_{ij}(v')x_{ji}(w')h' .$$

Proof: If $w = 0$, take $u' = 0$, $v' = u$, $w' = v$, $h' = h$. Similarly, if $u = 0$. If $u \neq 0 \neq w$, then, by R1-R3, there are $u',v'',w'' \in D$, $a,b \in D^*$ such that

$$x_{ij}(u)x_{ji}(v)x_{ij}(w)h = x_{ji}(u')w_{ij}(a)x_{ji}(v'')w_{ij}(b)x_{ji}(w'')h.$$

An application of both R3 and 1.4 proves 1.6.

1.7 Corollary: $\varphi: St_2(D) \to E_2(D)$ is central, and $\operatorname{Ker} \varphi \subseteq H$.

Proof: Write $\xi \in \operatorname{Ker} \varphi$ as in 1.5, then $u = v = w = 0$, hence $\xi \in H$. By 1.4, ξ centralizes every $x_{ij}(u)$, q.e.d.

We now define $h_{ij}(u) := w_{ij}(u)w_{ij}(-1)$ and $c_i(u,v) := h_{ij}(u)h_{ij}(v)h_{ij}(vu)^{-1}$. Then we have

$$\varphi(h_{ij}(u)) = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \quad \varphi(c_1(u,v)) = \begin{pmatrix} [u,v] & 0 \\ 0 & 1 \end{pmatrix},$$

$$\varphi(c_2(u,v)) = \begin{pmatrix} 1 & 0 \\ 0 & [u,v] \end{pmatrix}.$$

Then 1.4 implies:

1.8 <u>Lemma</u>: If D is non-commutative and $u,v \in D$ such that $uv \neq vu$, then in $St_2(D)$ the following relations hold for every $w \in D$:

$$x_{ij}(w) = [c_i(u,v), x_{ij}(([u,v]-1)^{-1}w)].$$

Here and in the following we use the notation $[g,h] = ghg^{-1}h^{-1}$ for the commutator of two elements g, h of any group.

Hence if D is non-commutative $St_2(D)$ is generated by commutators. Together with 1.7 this proves the first two assertions of 1.2.

To prove the last one, we establish the more general result (cf. [20; 4.2] for the commutative version):

1.9 <u>Theorem</u>: Suppose the center $Z(D)$ of D is not of order 2,3,4,9. Let $\pi: E \twoheadrightarrow G$ be a central extension of any group G, let $\bar{\sigma}: St_2(D) \to G$ be any group homomorphism. Then there exists a unique group homomorphism $\sigma: St_2(D) \to E$ such that $\bar{\sigma} = \pi \circ \sigma$.

This theorem obviously implies the last assertion of 1.2. The proof of 1.9 is mutatis mutandis the same as the proof of 4.2 in [20]. Our assertions on the center of D guarantee the existence of central c, v as in [20; 9.1, 9.2c] which is necessary to mimic all arguments of the proof. I do not know whether or not the assertion of 1.9 is also true under the weaker condition $|D| \neq 2,3,4,9$.

2. Matsumoto's theorem and some generalizations.

It is known that a perfect group G always has a universal central extension $\tilde{G}$ which is unique up to isomorphism, and the corresponding kernel is isomorphic to the "Schur multiplier" $H_2(G,\mathbb{Z})$ of G. For the case that G is the group of K-rational points of a Chevalley group over an infinite field (these groups are perfect, cf. [20]). Matsumoto describes $H_2(G,\mathbb{Z})$ in terms of the underlying field K as follows [9; 5.11]: If G is <u>nonsymplectic</u>, then $H_2(G,\mathbb{Z})$ is isomorphic to the group presented by generators $c(u,v)$, $u,v \in K^*$, and relations

$$c(uv,w) = c(u,w)c(v,w),$$
$$c(u,vw) = c(u,v)c(u,w),$$
$$c(u,1-u) = 1 \quad (1-u \in K^*) .$$

If G is <u>symplectic</u>, then $H_2(G,\mathbb{Z})$ is isomorphic to the abelian group presented by generators $c(u,v), u,v \in K^*$, and relations

$$c(u,v)c(uv,w) = c(u,vw)c(v,w),$$
$$c(1,1) = 1,\ c(u,v) = c(u^{-1},v^{-1}),$$
$$c(u,v) = c(u,(1-u)v) \quad (1-u \in K^*).$$

E.g., $SL_n(K)$ is non-symplectic if $n \geq 3$ and symplectic if $n = 2$. Both presentations, in general, define different groups. If $K = \mathbb{Q}$ or $K = \mathbb{R}$, then $c(-1,-1)$ is of order 2 in the non-symplectic case, while it is of infinite order in the symplectic case.

In case $G = SL_n(D)$, where $n \geq 3$ and D is a skew field, there is the following generalization of Matsumoto's theorem [14]:

Let U be the group presented by generators $c(u,v)$, $u,v \in D^*$, and relations

$$c(uv,w) = c({}^u v, {}^u w)c(u,w),$$
$$c(u,vw) = c(u,v)c({}^v u, {}^v w),$$
$$c(u,1-u) = 1 \quad (1-u \in D^*).$$

(We use the notation ${}^u v := uvu^{-1}$.) Then

$$c(u,v) \mapsto [u,v] := uvu^{-1}v^{-1}$$

defines a central extension of the group $D^{*1} := [D^*,D^*]$ with kernel isomorphic to $H_2(G,\mathbb{Z})$:

$$H_2(G,\mathbb{Z}) = \{\prod_{i=1}^{k} c(u_i,w_i) \in U \mid k \in \mathbb{N}, u_i,w_i \in D^* \text{ s.th. } \prod_{i=1}^{k} [u_i,w_i] = 1\}.$$

Obviously, if D is commutative, this gives Matsumoto's theorem for $G = SL_n(D)$, $n \geq 3$.

The main purpose of the first part of this paper is to prove the following $SL_2(D)$-analog of this theorem, which similarly generalizes the corresponding theorem of Matsumoto:

2.1 <u>Theorem</u>: Let D be a skew field such that $SL_2(D)$ is perfect. Let U be the group presented by generators $c(u,v)$, $u,v \in D^*$ and relations

α) $c(u,v)c(vu,w) = c(u,vw)c(v,w)$,

β) $c(u,v) = c(uvu,u^{-1})$,

γ) $c(x,y)c(u,v)c(x,y)^{-1} = c([x,y]u,v)c(v,[x,y])$,

δ) $c(u,v) = c(u,v(1-u)) \quad (1-u \in D^*)$.

Then $c(u,v) \mapsto [u,v]$ defines a central extension $\varphi_0 \colon U \to D^{*1}$ with kernel isomorphic to $H_2(SL_2(D),\mathbb{Z})$.

More precisely, the two correspondences

$$[u,v] \longmapsto d_1([u,v]),$$
$$c(u,v) \longmapsto h_{12}(u)h_{12}(v)h_{12}(vu)^{-1}$$

define group embeddings

$$D^{*1} \xhookrightarrow{i_E} E_2(D) \ ,$$

$$U \xhookrightarrow{i_{st}} St_2(D)$$

such that the following diagram commutes:

$$\begin{array}{ccc} U & \xrightarrow{\varphi_0} & D^{*1} \\ \downarrow{\scriptstyle i_{st}} & & \downarrow{\scriptstyle i_E} \\ St_2(D) & \xrightarrow{\varphi} & E_2(D) \end{array} .$$

Moreover, i_{st} induces an isomorphism of $Ker(\varphi_0)$ onto $Ker(\varphi)$.

The proof of 2.1 will be given in the next two sections. Here we will only give evidence for the centrality of $Ker(\varphi_0)$, thereby also proving that 2.1 implies Matsumoto's result for $SL_2(D)$ when D is commutative.

2.2 <u>Lemma</u>: If D, U, φ_0 is as in 2.1, then $Ker(\varphi_0)$ is central in U.

<u>Proof</u>: For $x = y = v = 1$, γ) gives

$$c(1,1)c(u,1)c(1,1)^{-1} = c(u,1)c(1,1)$$

for every $u \in D^*$. Taking $u = 1$ yields $c(1,1) = 1$.

Again by γ), with $x = y = 1$, u, v arbitrary, one obtains $c(v,1) = 1$ for every $v \in D^*$, hence by β) $c(1,v) = 1$ for every $v \in D^*$.

Another application of γ), with $u = 1$, then gives

$$c([x,y],v) = c(v,[x,y])^{-1} .$$

Now again applying γ) twice we get

$$\begin{aligned} &c(x',y')c(x,y)c(u,v)c(x,y)^{-1}c(x',y')^{-1} \\ &\quad = c(x',y')c([x,y]u,v)c([x,y],v)^{-1}c(x',y')^{-1} \\ &\quad = c([x',y'][x,y]u,v)c([x',y'][x,y],v)^{-1} . \end{aligned}$$

A straightforward induction on k shows: If $\prod_{i=1}^{k} [u_i,v_i] = 1$, then $\prod_{i=1}^{k} c(u_i,v_i)$ is central in U.

As a corollary to the preceding proof we state:

2.3 Corollary: In U, the following relations hold:

$$c(u,1) = c(1,v) = 1 \quad \text{for all} \quad u \in D^*, \text{ and}$$

$$c(u,v) = c(v,u)^{-1} \quad \text{for every} \quad u \in [D^*,D^*].$$

So far, we did not use relation δ).

2.4 Proposition: In U, the following relations hold:

δ') $c(u,v) = c(u(1-v),v)$,

ϵ) $c(u,v) = c(u,-vu)$,

ϵ') $c(u,v) = c(-uv,v)$.

Proof: By δ), α) we find

$$c(u,v) = c(u,v(1-u)) = c(u,v)c(vu,1-u)c(v,1-u)^{-1}$$

hence $c(v,1-u) = c(vu,1-u)$ which gives δ').

Applying δ), β) and again δ), β) we get

$$\begin{aligned} c(u,v) &= c(u,v(1-u)) = c(-uv(u^2-u),u^{-1}) \\ &= c(-uvu^2(1-u^{-1}),u^{-1}) = c(-uvu^2,u^{-1}) = c(u,-vu). \end{aligned}$$

This is ϵ), and ϵ') follows from ϵ) by an application of α).

We now state some easy consequences of β), ϵ):

2.5 Corollary: In U, the following relations hold:

$$c(u,v) = c(v^{-1},vuv) = c(u,-vu^{-1}) = c(-uv,u^{-1})$$
$$= c(-uv^{-1},v) = c(v^{-1},-vu) = c(v^{-1},vuv^{-1}).$$

Finally,

2.6 Remark: If D is commutative, then, in U, Matsumoto's symplectic relations hold. Conversely, from the calculations in [9] it is easy to verify relations α), β), γ), δ).

Proof: The only not completely obvious relation is

$$c(u,v) = c(u^{-1},v^{-1}).$$

But by 2.5, commutativity and ϵ) we have

$$c(u,v) = c(v^{-1},uv^2) = c(v^{-1},u).$$

Applying this twice we find what we want.

For later use, we prove the following statements:

2.7 Proposition: In U, the following relation holds:

γ') $$c(x,y)c(u,v)c(x,y)^{-1} = c([x,y],u)c(u,[x,y]v).$$

Proof: By 2.1 γ), the left hand side is

$$c([x,y]u,v)c(v,[x,y]).$$

By 2.3, $c([x,y],u) = c(u,[x,y])^{-1}$ and $c(v,[x,y]) = c([x,y],v)^{-1}$. Hence γ') follows as an application of 2.1 α).

2.8 Proposition: The correspondence

$$c(u,v) \mapsto c(v,u)$$

defines an anti-automorphism A of U. For every $\xi \in U$, $\xi \cdot A\xi$ is in Ker φ_0, hence central.

Moreover, in the definition of U, relation δ) can be replaced by

δ'') $$c(u,1-vu) = c(1-uv,v) \quad (uv \neq 1).$$

Proof: Clearly for every $c(u,v)$, $c(u,v)c(v,u) \in \text{Ker } \varphi_0$, since Ker φ_0 is central, $\xi \cdot A\xi \in \text{Ker } \varphi_0$ for every $\xi \in U$. The set of relations 2.1 α) is reproduced under A, if 2.1 β) is rewritten into an equivalent form

$$c(u,vu^{-1}) = c(uv,u^{-1}),$$

the same becomes obvious for this set.

The image of 2.1 γ) is 2.7 γ'), the image of 2.1 δ) is 2.4 δ').

To establish δ") we compute, using 2.5 and 2.1 δ):

$$c(1-uv,v) = c(1-uv,u^{-1}uv) = c(1-uv,u^{-1}) = c(u,v-u^{-1})$$
$$= c(u,1-vu).$$

Similarly, 2.1 δ) is derived from δ").

3. Proof of Theorem 2.1. First part.

The goal of this paragraph is to show that

$$c(u,v) \mapsto h_{12}(u)h_{12}(v)h_{12}(vu)^{-1}$$

defines a group homomorphism $i_{st}:U \to St_2(D)$, which is by no means obvious. In the next paragraph we then will see that i_{st} is in fact injective, which is the hardest part of the proof.

For $i = 1,2$, define in $St_2(D)$

$$c_i(u,v) = h_{ij}(u)h_{ij}(v)h_{ij}(vu)^{-1} \quad (u,v \in D^*),$$

where $j \in \{1,2\}$, $j \neq i$.

3.1 <u>Proposition</u>: In $St_2(D)$, relations α), β), γ), δ) from 2.1 hold with c replaced by c_i $(i = 1,2)$.

This of course shows that i_{st} is a group homomorphism.

The proof of 3.1 will be given by a series of lemmata as follows:

3.2 <u>Lemma</u>: In $St_2(D)$, the following relations hold:

R4 $\quad w_{ij}(u) = w_{ij}(-u)^{-1} = w_{ji}(-u^{-1}),$

R5 $\quad w_{ij}(u)w_{ij}(v) = w_{ij}(uv^{-1}u)w_{ij}(u) = w_{ij}(v)w_{ij}(vu^{-1}v),$

R6 $\quad h_{ij}(u)h_{ij}(v) = h_{ij}(uvu)h_{ij}(u^{-1}) = h_{ij}(v^{-1})h_{ij}(vuv),$

R7 $\quad h_{ij}(w)h_{ij}(v)^{-1} = h_{ij}(w(w^{-1}-v^{-1})w)h_{ij}(v-w)^{-1}$, if $v \neq w$.

<u>Proof</u>: By R1, R2, we have $w_{ij}(u)^{-1} = w_{ij}(-u)$. By R3, we get $w_{ij}(u)w_{ij}(v)w_{ij}(u)^{-1} = w_{ij}(-u^{-1}vu^{-1})$. In case $u = v$ this yields $w_{ij}(u) = w_{ji}(-u^{-1})$. This proves R4, R5. Now by R5:

$$\begin{aligned} h_{ij}(u)h_{ij}(v) &= w_{ij}(u)w_{ij}(-1)w_{ij}(v)w_{ij}(-1) \\ &= w_{ij}(u)w_{ij}(v^{-1})w_{ij}(-1)^2 \\ &= w_{ij}(uvu)w_{ij}(u)w_{ij}(-1)^2 \\ &= w_{ij}(uvu)w_{ij}(-1)w_{ij}(u^{-1})w_{ij}(-1) = h_{ij}(uvu)h_{ij}(u^{-1}). \end{aligned}$$

This proves one half of R6, and similarly one proves the second.

To prove R7, we replace w by vu. Then the right hand side is

$$\begin{aligned} &h_{ij}(vu-vu^2)h_{ij}(v-vu)^{-1} \\ &= w_{ij}(vu-vu^2)w_{ij}(v-vu)^{-1} \quad \text{by definition of } h_{ij} \\ &= x_{ij}(vu^2)x_{ij}(-vu^2)w_{ij}(vu(1-u))w_{ij}(v(1-u))^{-1} \quad \text{by R1} \\ &= x_{ij}(vu^2)w_{ij}(vu(1-u))w_{ij}(v(1-u))^{-1}x_{ij}(-v) \quad \text{by R3} \\ &= x_{ij}(vu)x_{ji}(-(1-u)^{-1}u^{-1}v^{-1})w_{ij}(v(1-u))^{-1}x_{ji}(-(1-u)^{-1}uv^{-1}) \\ &\qquad \cdot x_{ij}(-v) \quad \text{by R2, R3} \\ &= x_{ij}(vu)x_{ji}(-(1-u)^{-1}u^{-1}v^{-1})w_{ji}((1-u)^{-1}v^{-1}) \\ &\qquad \cdot x_{ji}(-(1-u)^{-1}uv^{-1})x_{ij}(-v) \quad \text{by R4} \\ &= x_{ij}(vu)x_{ji}(-u^{-1}v^{-1})x_{ij}(vu-v)x_{ji}(v^{-1})x_{ij}(-v) \quad \text{by R2} \\ &= w_{ij}(vu)x_{ij}(v)^{-1} = h_{ij}(vu)h_{ij}(v)^{-1}, \text{ by R2 and definition of } h_{ij}. \end{aligned}$$

This proves 3.2.

3.3 Corollary: In $St_2(D)$, the following relations hold:

$$c_i(u,v) = c_i(uvu,u^{-1}) \quad (u,v \in D^*),$$

$$c_i(u,v) = c_i(u,v(1-u)) \quad (u,v,1-v \in D^*) .$$

Proof: The first relations follow immediately from R6, for the second, we replace $w = vu$ and find

$$h_{ij}(vu)h_{ij}(v)^{-1} = h_{ij}(vu-vu^2)h_{ij}(v-vu)^{-1}$$

which obviously implies

$$c_i(u,v) = c_i(u,v(1-u)).$$

Hence to verify 3.1, we need to prove relations α), γ). We will do this in a slightly more general context, since this will be needed in the next paragraph.

Let $\hat{H}$ be the group presented by generators $\hat{h}(u)$, $u \in D^*$, and relations

H1 $$\hat{h}(u)\hat{h}(v) = \hat{h}(uvu)\hat{h}(u^{-1}).$$

Replacing uvu by u' and u^{-1} by v' we find

$$\hat{h}(u')\hat{h}(v') = \hat{h}(v'^{-1})\hat{h}(v'u'v'),$$

hence H1 is essentially R6 for a given pair i, j. We also define

$$\hat{c}(u,v) := \hat{h}(u)\hat{h}(v)\hat{h}(vu)^{-1}.$$

We have a surjective group homomorphism

$$\hat{\varphi}:\hat{H} \to EDiag_2(D) = \left\langle \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \middle| u \in D^* \right\rangle$$

of $\hat{H}$ onto the subgroup of elementary diagonal matrices in $E_2(D)$ with

$$\hat{\varphi}(\hat{c}(u,v)) = \begin{pmatrix} [u,v] & 0 \\ 0 & 1 \end{pmatrix}.$$

It will turn out that this homomorphism is a central group extension.

3.4 <u>Lemma</u>: In $\hat{H}$, the following relations hold:

H2 $\hat{c}(u,v) = \hat{h}(v^{-1}u^{-1})^{-1}\hat{h}(u^{-1})\hat{h}(v^{-1})$,

H3 $\hat{c}(u,v) = \hat{c}(uvu,u^{-1}) = \hat{c}(v^{-1},vuv)$,

H4 $\hat{c}(u,v)\hat{c}(vu,w) = \hat{c}(u,vw)\hat{c}(v,w)$
$= \hat{h}(u)\hat{c}(v,w)\hat{h}(u)^{-1}\hat{c}(u,wv)$,

H5 $\hat{c}(x,y)\hat{h}(u)\hat{c}(x,y)^{-1}$
$= \hat{h}([x,y]u)\hat{h}([x,y])^{-1} = \hat{c}(u,[x,y])^{-1}\hat{h}(u)$
$= \hat{h}([y,x])^{-1}\hat{h}(u[x,y]) = \hat{h}(u)\hat{c}([x,y]),u^{-1})^{-1}$,

H6 $\hat{c}(x,y)\hat{c}(u,v)\hat{c}(x,y)^{-1}$
$= \hat{c}(u,[x,y])^{-1}\hat{c}(u,[x,y]v)$
$= \hat{c}([x,y]u,v)\hat{c}([x,y],v)^{-1}$.

Moreover, $\hat{\varphi}:\hat{H} \to \mathrm{EDiag}_2(D)$ defines a central extension of groups with kernel contained in the subgroup generated by the elements $\hat{c}(u,v)$.

Proof: H2, H3 are straightforward consequences of H1. H4 requires some computation:

On the one hand, we have

$$\hat{c}(u,v)\hat{c}(vu,w) = \hat{h}(u)\hat{h}(v)\hat{h}(w)\hat{h}(wvu)^{-1},$$

on the other hand, by H2, H1, H1:

$$\begin{aligned}\hat{c}(u,vw)\hat{c}(v,w) &= \hat{h}(u)(\hat{h}(vw)\hat{h}(vwu)^{-1}\hat{h}(w^{-1}v^{-1})^{-1})\hat{h}(v^{-1})\hat{h}(w^{-1})\\ &= \hat{h}(u)\hat{h}(uw^{-1}v^{-1})^{-1}\hat{h}(v^{-1})\hat{h}(w^{-1})\\ &= \hat{h}(u)\hat{h}(v)\hat{h}(w)\hat{h}(wvu)^{-1}.\end{aligned}$$

This is the first half of H4. The second follows easily:

$$\begin{aligned}\hat{c}(u,v)\hat{c}(vu,w) &= \hat{h}(u)(\hat{h}(v)\hat{h}(w)\hat{h}(wv)^{-1})\hat{h}(u)^{-1}\hat{h}(u)\hat{h}(wv)\hat{h}(wvu)^{-1}\\ &= \hat{h}(u)\hat{c}(v,w)\hat{h}(u)^{-1}\hat{c}(u,vw).\end{aligned}$$

To prove H5, we use H1 to see, with $v = 1$:

$$\hat{h}(u) = \hat{h}(u^2)\hat{h}(u^{-1}) = \hat{h}(u^{-1})\hat{h}(u^2),$$

hence

$$\hat{h}(u^2)^{-1} = \hat{h}(u^{-1})\hat{h}(u)^{-1} = \hat{h}(u^{-2}).$$

This gives, again with H1:

$$\hat{h}(x)\hat{h}(u)\hat{h}(x)^{-1} = \hat{h}(xux)\hat{h}(x^2)^{-1}$$

and

$$\hat{h}(x)^{-1}\hat{h}(u)\hat{h}(x) = \hat{h}(x^{-1}ux^{-1})\hat{h}(x^{-2})^{-1} .$$

A repeated application of these formulae will prove H5, first half (together with the definition of $\hat{c}(u,[x,y])$. The second half is another application of H1. H6 is a consequences of H5, H4.

To prove the last statement of 3.4, we first observe that every element in H can be written in the form $\xi\hat{h}(w)$, where ξ is a product of $\hat{c}(u,v)$'s, and where $w \in D^*$ is uniquely determined by $\hat{\varphi}(\xi\hat{h}(w)) = \begin{pmatrix} w' & 0 \\ 0 & w^{-1}\end{pmatrix}$. Hence if $\xi\hat{h}(w) \in \operatorname{Ker}\hat{\varphi}$, then $w = 1$, hence $\hat{h}(w) = 1$.

Moreover, if $\xi = \prod_{i=1}^{k} \hat{c}(u_i,v_i)$, then we find by induction on k from H5:

$$\xi\hat{h}(u)\xi^{-1} = \hat{h}(\hat{\varphi}(\xi)u)\hat{h}(\hat{\varphi}(\xi))^{-1} .$$

Hence ξ is central if $\hat{\varphi}(\xi) = 1$.

This finishes the proof of 3.4. But also the proof of 3.1 is now complete:

Because of R7, we have a homomorphism $\hat{H} \to St_2(D)$, defined by $\hat{h}(u) \mapsto h_{12}(u)$, sending $\hat{c}(u,v)$ onto $c_1(u,v)$. By H4, H6, we find relations β), δ) holding for $c_1(u,v)$, and similarly for $c_2(u,v)$.

3.5 <u>Corollary</u>: If $h \in \hat{H}$ is such that $\hat{\varphi}(h) = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$, then

$$h\hat{h}(v)h^{-1} = \hat{h}(u_1vu_2^{-1})\hat{h}(u_1u_2^{-1})^{-1}.$$

<u>Proof</u>: By a repeated application of H5, this is true if $u_2 = 1$. In the proof of 3.4 we have seen

$$\hat{h}(x)\hat{h}(v)\hat{h}(x)^{-1} = \hat{h}(xux)\hat{h}(x^2)^{-1}.$$

Together this gives

$$\begin{aligned} h\hat{h}(v)h^{-1} &= \hat{h}(u_2^{-1})(\hat{h}(u_2^{-1})^{-1}h\hat{h}(v)h^{-1}\hat{h}(u_2^{-1}))\hat{h}(u_2^{-1})^{-1} \\ &= \hat{h}(u_2^{-1})(\hat{h}(u_2u_1v)\hat{h}(u_2u_1)^{-1})\hat{h}(u_2^{-1})^{-1} \\ &= \hat{h}(u_1vu_2^{-1})\hat{h}(u_1u_2^{-1})^{-1} . \end{aligned}$$

For later use in paragraph 4, we prove some more properties of $\hat{H}$:

3.6 <u>Proposition</u>: $\hat{H}$ has an automorphism of order 2, defined by $\hat{h}(u) \mapsto \hat{h}'(u) := \hat{h}(u^{-1})$. Under this automorphism, $\operatorname{Ker} \hat{\varphi}$ is pointwise fixed. If $\hat{c}'(u,v)$ denotes the image of $\hat{c}(u,v)$, the following relations hold in $\hat{H}$:

H7 $\quad \hat{h}'(u) = \hat{h}(u^{-1}) = \hat{h}(u)^{-1}\hat{c}(u,u^{-1})$,

H8 $\quad$ $$\begin{aligned} \hat{c}'(u,v) &= \hat{h}(u^{-1})\hat{h}(v^{-1})\hat{h}(u^{-1}v^{-1})^{-1} \\ &= \hat{h}(uv)^{-1}\hat{h}(u)\hat{h}(v) \\ &= \hat{h}(uv)^{-1}\hat{c}(u,v)\hat{h}(vu), \end{aligned}$$

H9 $\begin{cases} \hat{c}(x,y)\hat{h}(u) = \hat{h}([x,y]u)\hat{c}'(x,y) \\ \hat{c}'(x,y)\hat{h}(u) = \hat{h}(u[y,x])\hat{c}(x,y) \end{cases}$,

H10 $\hat{h}(w)^{-1} = \hat{h}(w^{-1})$ for every $w \in [D^*,D^*]$,

H11 $[\hat{h}([x,y]),\hat{c}(x,y)] = 1$,

H12 $\hat{c}(x,y)\hat{c}'(x,y)\hat{c}(u,v) = \hat{c}({}^{[x,y]}u, {}^{[x,y]}v)$.

Especially the relation

$$(*) \qquad [\hat{c}(x,y),\hat{c}(u,v)] = \hat{c}([x,y],[u,v])$$

is true if and only if

$$[\hat{c}(x,y),\hat{c}'(u,v)] = 1$$

holds.

Remark: The corresponding relations of course hold in $St_2(D)$, but the associated relations in $St_n(D)$, $n \geq 3$, seem to be much stronger. For example, (*) does always hold if $n \geq 3$ [14; §1, §2]. On the other hand, for $St_2(D)$, I do not know any example for which this equation fails. It would be very interesting to know whether such "noncommutative" contributions to $H_2(E_2(D),\mathbb{Z})$ exist.

Proof of 3.6: Relations H1 are kept invariant under $\hat{h}(u) \mapsto \hat{h}(u^{-1})$, hence $\hat{h}(u) \mapsto \hat{h}'(u)$ defines an automorphism of $\hat{H}$ of order ≤ 2. The invariance of $\operatorname{Ker} \hat{\varphi}$ will follow from H9: If $\prod_{i=1}^{k} \hat{c}(u_i,v_i) \in \operatorname{Ker} \hat{\varphi}$, then (by induction on k) we get from H9 for every $u \in D^*$:

$$\prod_{i=1}^{k} \hat{c}(u_i,v_i)\hat{h}(u) = \hat{h}(u)\prod_{i=1}^{k} \hat{c}'(u_i,v_i).$$

Taking $u = 1$ this yields

$$\prod_{i=1}^{k} \hat{c}(u_i,v_i) = \prod_{i=1}^{k} c'(u_i,v_i).$$

Hence we only have to prove the relations.

H7 is obvious by the definition of $\hat{c}(u,u^{-1})$. H8 follows immediately.

To verify each of H9, one has to apply R1 three times: We do only the first equation:

$$\hat{h}([x,y]u)\hat{h}(x^{-1})\hat{h}(y^{-1})\hat{h}(x^{-1}y^{-1})^{-1}$$
$$= \hat{h}(x)\hat{h}(y)\hat{h}(yx)^{-1}\hat{h}((yx)y^{-1}x^{-1}([x,y]u)x^{-1}y^{-1}(yx))$$
$$= \hat{c}(x,y)\hat{h}(u).$$

An application of H8 gives the result.

To prove H10, we use H9 (for $u = 1$):

$$\hat{h}([u,v])^{-1} = \hat{c}'(u,v)\hat{c}(u,v)^{-1}$$
$$= (\hat{c}(u,v)\hat{c}'(u,v)^{-1})^{1}$$
$$= \hat{h}'([u,v]) = \hat{h}([v,u]).$$

Repeating this argument we find H10.

From H5 we deduce

$$\hat{c}(x,y)\hat{h}([y,x]) = \hat{h}([x,y])^{-1}\hat{c}(x,y).$$

With H10 this yields H11.

H12 now results from R15 and the definition of $\hat{c}(u,v)$ if one observes that

$$\hat{c}(x,y)\hat{c}'(x,y)\hat{h}(u) = \hat{h}({}^{[x,y]}u)\hat{c}(x,y)\hat{c}'(x,y).$$

We can now prove the last statement of 3.6: By H9 $(u = 1)$ and H11 we have

$$\hat{c}'(x,y) = \hat{h}([y,x])\hat{c}(x,y) = \hat{c}(x,y)\hat{h}([y,x]),$$

hence by H4, H5:

$$\hat{c}'(x,y)\hat{c}(u,v) = {}^{\hat{c}(x,y)}(\hat{c}([y,x],[u,v])\hat{c}(u,v))$$
$$= \hat{c}([u,v],[x,y])[\hat{c}(x,y),\hat{c}(u,v)]\hat{c}(u,v).$$

This concludes the proof of 3.6.

Remark: In $St_2(D)$, the automorphism of H described in 3.6 is induced by conjugation with $w_{ij}(1)$.

4. Proof of Theorem 2.1. Second part.

In this paragraph we will show that the homomorphism

$$i_{st}: U \to St_2(D),\ c(u,v) \mapsto c_1(u,v)$$

is a monomorphism. We will do this by embedding the central extension $\varphi_0: U \to D'$ $(c(u,v) \mapsto [u,v])$ into a central extension of $E_2(D)$ via the embedding $D' \hookrightarrow E_2(D)([u,v] \mapsto d_1([u,v]))$. We use the ideas of [9; 14].

The first step is the construction of an appropriate extension of the diagonal matrices in $E_2(D)$.

We denote by M the associative monoid of words of elements $h(u)$ $(u \in D^*)$ and $\underline{\xi}$ $(\xi \in U)$. The empty word is the unit element, denoted by $\mathbb{1}$.

If, for $A, A' \in M$, we have decompositions

$$A = A_0 A_1 A_2,\ A' = A_0 A_1' A_2$$

in M, we say A' is obtained from A by the substitution $A_1 \to A_1'$. For $A, B \in M$ we define $A \succ B$, if B is obtained from A by an "admissible" substitution, which is the composition of a finite sequence of positive length of one of the following "elementary" substitutions:

(1)	$h(1) \to \mathbb{1}$	$1 \in D^*$
(2)	$\underline{1} \to \mathbb{1}$	$1 \in U$
(3)	$\underline{\xi}\ \underline{\eta} \to \underline{\xi\eta}$	$\xi, \eta \in U$
(4)	$h(u)\underline{\xi} \to \underline{c(u,\varphi_0\xi)\xi}h(u)$	$\xi \in U,\ u \in D^*$
(5)	$h(u)h(v) \to \underline{c}(u,v)h(vu)$	$u, v \in D^*$.

Here we have written $\underline{c}(u,v)$ for $\underline{c(u,v)}$ for simplicity. The number (*) $(* \in \{1,\ldots,5\})$ is the type of the elementary substitution.

4.1 <u>Lemma</u>: i) $(M, \succ)$ is a partially ordered set.

ii) For $A \in M$, $\{B \in M | A \succ B\}$ is a finite set.

iii) The subset H of M of minimal elements consists of the words of the form $\mathbb{1}$, $\underline{\xi}(\xi \in U\setminus\{1\})$, and $ah(u)$ with $u \in D^*$ and $a = \mathbb{1}$ or $a = \underline{\xi}$ for some $\xi \in U\setminus\{1\}$.

iv) For every $A \in M\setminus H$ there exists exactly one $B \in H$ with $A > B$.

Proof: To every $A \in M$, a unique natural number $r(A)$ is associated by the following definition: If $A = \prod_{i=1}^{k} a_i$ where $a_i \in \{h(u), \underline{\xi} | u \in D^*, \xi \in U\}$, then $(a_1,\ldots,a_k)$ is uniquely determined by A. We set $r(A) := k+r'(A)$, where $r'(A)$ is the number of pairs (a_i,a_j) with $i < j$ and $a_i = h(u)$ for some $u \in D^*$ and $a_j = \underline{\xi}$ for some $\xi \in U$. Clearly $r(\mathbb{1}) = 0$, and if $B \in M$ is obtained from A by an admissible substitution then $r(B) < r(A)$. Hence $A > B$ and $B > A$ cannot hold at the same time, which proves i). Also we have $H = \{A \in M | r(A) \leq 1\}$, and for every $A \notin H$, there is a finite number of $B \in M$ such that $A > B$. This proves ii) and iii).

To prove iv), we write $A \geq B$ if $A = B$ or $A > B$. We show: For every $A,B,C \in M$ with $A \geq B$, $A \geq C$ there exists $A' \in M$ with $B \geq A'$, $C \geq A'$. This will imply iv).

Of course it suffices to prove the existence of A' only for all cases in which B and C are obtained from A by an elementary substitution. The existence of A' is obvious if B and C are obtained from A by substitutions of disjoint words, or if at least one of them is obtained by a substitution of type (1) or (2).

Hence we may assume that both B and C are obtained from A by elementary substitutions of type (3), (4), (5) inside the same three-letter-subword of A, and the only nontrivial cases are those with $A > B$, $A > C$, $B \neq C$.

There are three cases which we have to consider:

1. Case: $A = h(u)\underline{\xi}\ \underline{\eta}$, $u \in D^*$, $\xi,\eta \in U$.
We may assume: $B = h(u)\underline{\xi\eta}$, $C = \overline{c(u,\varphi_0\xi)\xi h(u)}\underline{\eta}$. To verify the existence of A', it suffices to establish the relation $c(u,\varphi_0\xi\eta)\xi\eta = c(u,\varphi_0\xi)\xi c(u,\varphi_0\eta)\eta$ in U. A repeated application of 2.1 γ), 2.3 gives

$$\xi c(u,\varphi_0\eta) = c(\varphi_0\xi\cdot u,\varphi_0\eta)c(\varphi_0\xi,\varphi_0\eta)^{-1}\xi,$$

and we have to show (with $v = \varphi_0\xi$, $w = \varphi_0\eta$):

$$c(u,vw) = c(u,v)c(vu,w)c(v,w)^{-1}$$

which is simply 2.1 α).

2. Case: $A = h(u)h(v)\underline{\xi}$, $u, v \in D^*$, $\xi \in U$.
We may assume: $B = h(u)c(v,\varphi_0\xi)\xi h(v)$, $C = \underline{c}(u,v)h(vu)\xi$. Applying suitable admissible transformations we find

$$B \to \underline{c}(u,[v,\varphi_0\xi]\varphi_0\xi)\underline{c}(v,\varphi_0\xi)\underline{\xi}\underline{c}(u,v)h(vu),$$

$$C \to \underline{c}(u,v)\underline{c}(vu,\varphi_0\xi)\underline{\xi}h(vu).$$

We set $w = \varphi_0\xi$ and recall (from 2.1 γ)) that

$$\xi c(u,v) = c(wu,v)c(v,w)$$

hence we are done in this case if we can prove

$$c(u,vwv^{-1})c(v,w)c(wu,v)c(v,w) = c(u,v)c(vu,w).$$

By 2.1 α), this is equivalent to

$$(*) \qquad c(u,vwv^{-1})c(v,w)c(wu,v) = c(u,vw).$$

Since $w \in [D^*,D^*]$, we find, by 2.3 and 2.1 γ)

$$\begin{aligned} &c(u,vwv^{-1})c(v,w) \\ &\quad = (c(w,v)c(vwv^{-1},u))^{-1} \\ &\quad = (c(w,u)c(u,[w,v])c(w,v))^{-1} \\ &\quad = c(v,w)c([w,v],u)c(u,w). \end{aligned}$$

An application of 2.1 α) gives for the left hand side of (*)

$$\begin{aligned} &c(u,vwv^{-1})c(v,w)c(wu,v) \\ &\quad = c(v,w)c([w,v],u)c(u,wv)c(w,v) \\ &\quad = c(v,w)c([w,v],u)c(u,wv)c(w,v)^{-1}. \end{aligned}$$

We apply 2.1 γ) and 2.7 γ') to get

$$\begin{aligned} &{}^{c(v,w)}(c([w,v],u)c(u,wv)) \\ &\quad = c(u,[v,w])c([v,w],u)c(u,vw) \\ &\quad = c(u,vw), \end{aligned}$$

which proves (*).

3. Case: $A = h(u)h(v)h(w)$, $u, v, w \in D^*$.
We may assume: $B = h(u)\underline{c}(v,w)h(wv)$, $C = \underline{c}(u,v)h(vu)h(w)$.

Appropriate admissible substitutions give

$$B \to \underline{c}(v,w)\underline{c}([w,v],u)\underline{c}(u,wv)h(wvu)$$

$$C \to \underline{c}(u,v)\underline{c}(vu,w)h(wvu).$$

Hence, we have to establish in U:

$$c(v,w)c([w,v],u)c(u,wv) = c(u,v)c(vu,w).$$

By 2.1 γ), the right hand side equals $c(u,vw)c(v,w)$. But then everything follows from the last equation of the previous case.

This proves 4.1. We deduce

4.2 Corollary: H is a group under the following composition: For $a,b \in H$, $a\cdot b$ is the unique element of H below $ab \in M$. $\mathbb{1}$ is the unit element of H, and H contains an isomorphic image of the group U.

Proof: Obviously the composition is associative.

The inverse of $\xi h(u)$ is the minimal element lying under $\underline{c}(u^{-1},u)^{-1}h(u^{-1})\underline{\xi}^{-1} \in M$.

Everything else is obvious.

4.3 Corollary: In H, the following relations hold for all $u,v \in D^*$:

$$h(u)h(v) = h(uvu)h(u^{-1}),$$
$$h(v)h(vu)^{-1} = h(v-vu)h(vu-vu^2)^{-1} \quad (1-u \in D^*).$$

Proof: This is obvious from the definition of the composition law in H and from the defining relations 2.1 β), δ) of U.

4.4 Corollary: The correspondence $h(u) \mapsto h_{12}(u)$ defines a group homomorphism

$$i: H \to St_2(D).$$

Remark: The image of H in $St_2(D)$ is easily seen to be the subgroup of $St_2(D)$ which has been denoted by H in §1. It is our goal here to show that i is injective, which finally will prove our main theorem and will justify the notation. In this paragraph, however, H will always mean the group described in 4.2.

By 4.3, H is a homomorphic image of the group $\hat{H}$ defined in §3 (under $\hat{h}(u) \mapsto h(u)$). By 4.4, it is a central extension of

$\mathrm{EDiag}_2(D)$, hence, by 3.6, it has an automorphism $H \to H$ $(h \mapsto h')$ of order ≤ 2 defined by $h(u) \mapsto h(u^{-1})$.

We denote by W^* the semidirect product $\langle\omega\rangle \ltimes H$, where $\langle\omega\rangle \simeq \mathbb{Z}$ is a cyclic group of infinite order, operating on H by ${}^{\omega}h := h'$. The subgroup N of W^* generated by the element $(\omega^2, h(-1))$ is normal in W^*, as it is easily verified. Let $W = W^*/N$ denote the quotient, let $w_1 = \omega N$ be the canonical image of ω in W. Clearly H embeds into W, we denote its image by H also, similarly for its elements.

Then we have $w_1^2 = h(-1)^{-1}$ in W. Since, by definition, $h_{12}(-1) = w_{12}(-1)^2 = w_{12}(1)^{-2}$ and, by R5, $w_{12}(1)h_{12}(u)w_{12}(1)^{-1} = h_{12}(u^{-1})$, we find:

4.5 Lemma: i) The homomorphism $i: H \to St_2(D)$ extends, by $w_1 \mapsto w_{12}(-1)$, to a homomorphism, also denoted by i:

$$W \to St_2(D).$$

ii) If $h \in H$ is such that $\varphi i(h) = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$, then

$$hw_1h^{-1} = h(u_1u_2^{-1})w_1 .$$

Proof: i) is obvious.

ii) Assume first $u_2 = 1$. Then $h^{-1} = \prod_{i=1}^{k} c(y_i, x_i)$, for certain $x_i, y_i \in D^*$, with $\prod_{i=1}^{k} [x_i, y_i] = u_1$.

A repeated application of 3.6, H9 gives (if we observe $c'(y_i, x_i) = w_1 c(y_i, x_i) w_1^{-1}$):

$$w_1h^{-1}w_1^{-1} = h(u_1)h^{-1} .$$

By 3.6, H11 this gives

$$w_1h^{-1}w_1^{-1} = h^{-1}h(u_1)$$

which is ii) in this case.

We also have

$$w_1h(u)^{-1}w_1^{-1} = h(u^{-1})^{-1} ,$$

hence by 3.4, H3:

$$h(u)w_1h(u)^{-1} = h(u)h(u^{-1})^{-1}w_1$$
$$= c(u^2, u^{-1})^{-1}h(u^2)w_1 = h(u^2)w_1 ,$$

which proves ii) in case $h = h(u)$. Writing $h = h(u_2^{-1})\cdot h'$ and applying 3.5 we find

$$hw_1h = h(u_2^{-1})(h(u_2u_1)w_1)h(u_2^{-1})^{-1}$$
$$= h(u_1u_2^{-1})w_1 .$$

We now proceed like Matsumoto to prove the injectivity of i. Cf. [9, 14], see also [11].

Let T denote the group of strictly upper triangular matrices, and let M denote the group of monomial matrices in $E_2(D)$. There is a Bruhat decomposition of $E_2(D)$

$$E_2(D) = TMT = \bigcup_{m\in M} TmT$$

into pairwise disjoint double cosets, hence a map $\rho: E_2(D) \to M$ ($\rho(t'mt) := m$ for $t,t' \in T$, $m \in M$). We determine the value of ρ after multiplying a double coset by $m_{12}(\pm 1) = \varphi(w_{12}(\pm 1))$. We write $m \in M$ as $m = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$ if it is diagonal and as $m = \begin{pmatrix} 0 & u_2 \\ u_1 & 0 \end{pmatrix}$ if not. Then:

$$me_{ij}(v)m^{-1} = e_{k\ell}(u_ivu_j^{-1}) \quad \text{where} \quad k\ell = \begin{cases} ij & \text{if } m \text{ is diagonal,} \\ ji & \text{otherwise .} \end{cases}$$

4.6 Lemma: For $s \in E_2(D)$ let $\rho(s) = m$ be as above, assume $s = e_{12}(-u)me_{12}(v)$. Then the following is true:

i) If $u = 0$ or m diagonal then

$$m_{12}(1)s = m_{12}(1)me_{12}(-u_1^{-1}uu_2+v)$$

and

$$\rho(m_{12}(1)s) = m_{12}(1)m .$$

ii) If $u \neq 0$ and m not diagonal then

$$m_{12}(1)s = e_{12}(u^{-1})d_{12}(u)^{-1}me_{12}(-u_1^{-1}u^{-1}u_2+v)$$

and

$$\rho(m_{12}(1)s) = d_{12}(u)^{-1}m.$$

iii) If $v = 0$ or m diagonal then

$$sm_{12}(-1) = e_{12}(-u+u_1vu_2^{-1})mm_{12}(-1)$$

and

$$\rho(sm_{12}(-1)) = mm_{12}(-1).$$

iv) If $v \neq 0$ and m not diagonal, then

$$sm_{12}(-1) = e_{12}(-u+u_2v^{-1}u_1^{-1})md_{12}(v)e_{12}(-v^{-1})$$

and

$$\rho(sm_{12}(-1)) = md_{12}(v).$$

Proof: Straightforward computation.

On the set

$$X = \{(s,w) \in E_2(D) \times W \mid \rho(s) = \varphi i(w)\}$$

we now define permutations

$\lambda(h), \mu(t), \eta$ (resp. $\lambda^*(h), \mu^*(t), \eta^*$) where $h \in H$, $t \in T$,

by

$$\left.\begin{array}{l} \lambda(h)(s,w) := (\varphi i(h)s, hw) \\ (s,w)\lambda^*(h) := (s\varphi i(h), wh) \end{array}\right\} h \in H,$$

$$\left.\begin{array}{l} \mu(t)(s,w) := (ts,w) \\ (s,w)\mu^*(t) := (st,w) \end{array}\right\} t \in T,$$

$$\eta(s,w) := \begin{cases} (m(1)s, w_1w) \\ (m(1)s, h(u)^{-1}w) \end{cases} \text{if } \rho(m_{12}(1)s) = \begin{cases} m_{12}(1)m \\ d_{12}(u)^{-1}m \end{cases},$$

$$(s,w)\eta^* := \begin{cases} (sm(-1), ww_1^{-1}) \\ (sm(-1), wh(v)) \end{cases} \text{if } \rho(sm_{12}(-1)) = \begin{cases} mm_{12}(-1) \\ md_{12}(v) \end{cases}.$$

Let G (resp. G^*) be the group of automorphisms of X generated by

$\lambda(h), \mu(t), \eta$ (resp. by $\lambda^*(h), \mu^*(t), \eta^*$).

4.7 Lemma: For all $(s,w) \in X$, $g \in G$, $g^* \in G^*$ we have

$$(*) \qquad (g(s,w))g^* = g((s,w)g^*).$$

Proof: It suffices to show this for the generators of G and G^*.

The only nontrivial case is $g = \eta$, $g^* = \eta^*$, and one only has to compare the second components.

We write $s = e_{12}(-u)me_{12}(v)$, $m = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$ or $m = \begin{pmatrix} 0 & u_2 \\ u_1 & 0 \end{pmatrix}$ as in 4.6.

1. Case: m is diagonal.
We set $u' = u-u_1vu_2^{-1}$. If $u' = 0$, then $(*)$ is obvious. Otherwise, by 4.6, we have to show:

$$h(u')^{-1}ww_1^{-1} = w_1wh(-u_1^{-1}u'u_2).$$

For this we remember

$$1 = c(-x,x^{-1}) = h(-x)h(x^{-1})h(-1)^{-1},$$

hence

$$(*) \qquad w_1h(x)w_1^{-1} = h(x^{-1}) = h(-x)^{-1}h(-1).$$

We compute

$$\begin{aligned} w_1wh(-u_1^{-1}u'u_2) &= w_1h(-u')h(u_1u_2^{-1})^{-1}w && (3.5) \\ &= h(u')^{-1}h(-u_1u_2^{-1})w_1w && ((*)) \\ &= h(u')^{-1}h(-u_1u_2^{-1})h(u_1u_2^{-1})^{-1}ww_1 && (4.5\text{ ii})) \\ &= h(u')^{-1}h(-u_1u_2^{-1})h(u_1u_2^{-1})^{-1}wh(-1)^{-1}w_1^{-1} && \\ &= h(u')^{-1}ww_1^{-1} && (3.5) \end{aligned}$$

Hence this case is settled.

2. Case: m is non-diagonal.
Since $u = v = 0$ is trivial, we may assume that at least one of both is not zero.

If $u \neq 0 = v$, we have to show (by 4.6):

$$w_1ww_1^{-1} = h(u)^{-1}wh(-u_1^{-1}u^{-1}u_2).$$

If $u = 0 \neq v$, we have to show:

$$h(-u_2 v^{-1} u_1^{-1})^{-1} w h(v) = w_1 w w_1^{-1} .$$

If $u \neq 0 \neq v$, but $u' = u - u_2 v^{-1} u_1^{-1} = 0$, we have to show

$$w_1 w h(v) = h(u)^{-1} w w_1^{-1} .$$

All these three cases are easily done by 3.5 and 4.5 ii).

If $u \neq 0 \neq v$, $u' \neq 0$, then also $v' = v - u_1^{-1} u^{-1} u_2 \neq 0$, and we have to show:

$$h(u')^{-1} w h(v) = h(u)^{-1} w h(v').$$

By 3.5, this is equivalent to

$$w_1 h(-u_1 v' u_2^{-1}) h(-u_1 v u_2^{-1})^{-1} w_1^{-1} = h(u) h(u')^{-1}.$$

Using (*) we find equivalently

$$h(u_1 v' u_2^{-1})^{-1} h(u_1 v u_2^{-1}) = h(u) h(u')^{-1},$$

which means that we have to show

$$h(u_1 v u_2^{-1}) h(u') = h(u_1 v' u_2^{-1}) h(u).$$

We replace $x := u_1 v u_2^{-1}$, $y = u$ and find

$$h(x) h(y - x^{-1}) = h(x - y^{-1}) h(y)$$

to show.

This means that we have to establish:

$$c(x, y - x^{-1}) = c(x - y^{-1}, y).$$

But this is an easy consequence of 2.8 δ'').

4.8 <u>Proposition</u>: G (resp. G^*) operates simply transitive on X and is a central extension of $E_2(D)$ with kernel φ_0. Moreover, there is exactly one epimorphism $St_2(D) \to E_2(D)$ over $E_2(D)$.

<u>Proof</u>: For the transitivity, see the arguments in [9]. The fact that G operates simply transitive follows from 4.7. For the rest of the arguments see [14, p.100].

Hence we have proved:

4.9 Theorem: The central extensions of $E_2(D)$ below $St_2(D)$ are classified by central extensions $\varphi_0: U \to [D^*, D^*]$ of the following type: U has a set of generators $c(u,v)$ such that $\varphi_0 c(u,v) = [u,v]$, for $u,v \in D^*$, and among these generators relations α), β), γ), δ) from 2.1 are valid.

If U is such an extension of $[D^*, D^*]$, then there is a central extension $p: G \to E_2(D)$ and exactly one homomorphism $\psi: St_2(D) \to G$, lying over $E_2(D)$, such that

$$c(u,v) \mapsto \psi(h_{12}(u)h_{12}(v)h_{12}(vu)^{-1})$$

defines an isomorphism of U onto a subgroup of G and such that $Ker(\varphi_0)$ is mapped isomorphically onto $Ker(p)$. Conversely, every central extension of $E_2(D)$ which is a quotient of $St_n(D)$ is obtained in this way.

By the well-known properties of universal central extensions of perfect groups all the statements of 2.1 will follow.

Part II: Local Division Algebras

5. The tame symbol of SL_2 of a local division algebra.

Let K be a non-archimedean local field with integers $\mathfrak{o}$, prime π and prime ideal $\mathfrak{p}$. Let $v: K \to \mathbb{Z}$ denote its discrete valuation, hence $v(\pi) = 1$, $v(\mathfrak{o}) = \mathbb{N} \cup \{0\}$, $v(\mathfrak{p}) = \mathbb{N}$. Let D be a finite dimensional central K-algebra. The structure of D as a K-algebra is as follows (cf. [17]): There is an $n \in \mathbb{N}$ such that $n^2 = \dim_K D$, and D contains an unramified extension L of K of degree n as a maximal commutative subfield. Let $q = |\mathfrak{o}/\mathfrak{p}|$. L is a cyclotomic extension $L = K(\omega)$ of K, where ω is a (q^n-1)-th root of unity, hence cyclic over K. There is an element $\Pi \in D$ with $\Pi^n = \pi$ and a generator σ of the Galois group of $L:K$ such that $\Pi\omega = {}^{\sigma}\omega\Pi$, hence

$$D = L \oplus L\Pi \oplus \ldots \oplus L\Pi^{n-1}.$$

We define

$$\mathfrak{o}_D = \mathfrak{o}_L \oplus \mathfrak{o}_L \Pi \oplus \ldots \oplus \mathfrak{o}_2\Pi^{n-1} ,$$

where $\mathfrak{o}_L \subseteq L$ is the ring of integers of L. $\mathfrak{o}_D$ is the ring of integers of D. In fact $\mathfrak{o}_D$ is a valuation ring which is, as an extension of $\mathfrak{o}$ (or $\mathfrak{o}_L$), ramified of index n. Its residue class skew field $\mathfrak{o}_D/\Pi_D$ is canonically isomorphic to $\mathfrak{o}_L/\pi\mathfrak{o}_L$ which, as a finite extension of $\mathfrak{o}/\mathfrak{p}$, is generated by the canonical image of ω, which we denote by the same letter. Hence $\mathfrak{o}_D/\Pi\mathfrak{o}_D$ is commutative.

Let $N:D \to K$ denote the reduced norm of D over K. This has the property that its restriction to any maximal commutative sub-K-algebra of D is the usual field norm. Obviously then $N(\Pi) = (-1)^{n-1}\pi$, and together with the well-known fact that, in any unramified extension of local fields, every unit of the ground field is a norm [19; p. 89], this shows the surjectivity of N. We also have $N(\mathfrak{o}_D) = \mathfrak{o}$ and for $k > 1$

$$N(1+\Pi^k\mathfrak{o}_D) = 1+\pi^{\{k/n\}}\mathfrak{o} = (1+\Pi^k\mathfrak{o}_D) \cap \mathfrak{o}$$

where $\{k/n\}$ is the smallest integer $\geq k/n$ [19; p. 89].

As in the commutative case and in the case of $SL_r(D)$ $(r \geq 3)$, there is a tame symbol

$$t: U \to \mathfrak{o}_D/\Pi\mathfrak{o}_D$$

for the group U defined in 2.1 with respect to D. This is defined as follows (cf. [1; 4.2]). Let, for $i \in \mathbb{N} \cup \{0\}$,

$$p_i: \mathfrak{o}_D^* \to \mathfrak{o}_D^*/(1+\Pi\mathfrak{o}_D) \cong (\mathfrak{o}_D/\Pi\mathfrak{o}_D)^*$$

be obtained recursively as follows: For $u \in \mathfrak{o}_D^*$,

$$p_0(u) := 1, \ p_{i+1}(u) := \bar{u}p_i(\overline{\Pi u \Pi^{-1}}).$$

(Here, for $u \in \mathfrak{o}_D$, we write $\bar{u} := u+\Pi\mathfrak{o}_D$.)

5.1 Proposition: Let U be as in 2.1. If $x,y \in D^*$, let $x = u\Pi^i$, $y = v\Pi^j$, where $u,v \in \mathfrak{o}_D^*$ and $i,j \in \mathbb{Z}$. Then

$$c(x,y) \longmapsto (-1)^{ij}p_j(u)p_i(v)^{-1}$$

induces a surjective homomorphism (the "tame symbol")

$$t: U \to (\mathfrak{o}_D/\Pi\mathfrak{o}_D)^* \simeq (\mathfrak{o}_L/\pi\mathfrak{o}_L)^*.$$

Proof: A straightforward verification shows that U maps onto $U(D)$ as it is defined in [1; 4.1]. The same reference then shows the truth of 5.1.

5.2 Theorem: The tame symbol has a splitting s given by $s(\omega^k) := c(\omega^k, \Pi)$.

The proof of this theorem is much more complicated than the proof of the corresponding statement for SL_n $(n \geq 3)$ in [1].

In 5.6 we will show more precisely that U is a semidirect product, where $c(\omega, \Pi)$ generates the non-normal factor.

Proof: It is straightforward to verify $ps = id$. The theorem now will follow if we show:

$$s(\omega^k) = s(\omega)^k.$$

We do this in several steps:

5.3 Proposition: If K is a local field, q the order of its residue class field and ω a primitive $(q-1)$-th root of unity in K, then in $K_2(2,K) = H_2(SL_2(K), \mathbb{Z})$,

$$c(\omega^k, \omega^\ell) = 1$$

holds for all k, ℓ.

Remark: The corresponding statement for $K_2(n,K)$, $n \geq 3$, is due to Carroll [6; Thm. 1].

Proof of 5.3: By 2.1 (or by Matsumoto's theorem), $K_2(2,K)$ is just the group U of Theorem 2.1 for the division algebra K. We use the relations

i) $c(u,v)c(vu,w) = c(u,vw)c(v,w)$ (2.1 α))

ii) $c(u,v) = c(u,-vu^{-1}) = c(-uv^{-1},v) = c(uvu,u^{-1})$ (2.1 β), 2.5)

iii) $c(u,v) = c(u,v(1-u))$ (2.1 δ))

By ii), we find

$$c(\omega^k,\omega^\ell) = c(\omega^k,-\omega^{\ell-k}) = c(-\omega^{k-\ell},\omega^\ell).$$

Euclid's algorithm then yields

$$c(\omega^k,\omega^\ell) = c(\omega^{(k,\ell)},(-1)^\varepsilon), \quad \varepsilon = 0 \quad \text{or} \quad \varepsilon = 1.$$

Especially we have

$$c(\omega,\omega^k) = c(\omega,(-1)^k).$$

By i), we get

$$c(\omega^{k+1},-1) = c(\omega,\omega^k)^{-1}c(\omega,-\omega^k)c(\omega^k,-1)$$
$$= c(\omega,(-1)^k)^{-1}c(\omega,-(-1)^k)c(\omega^k,-1).$$

Induction on k gives

iv) $c(\omega^{2\ell+1},-1) = c(\omega,-1)$,

v) $c(\omega^{2\ell},-1) = c(1,-1) = 1$.

Hence it remains to show: $c(\omega,-1) = 1$.

If $2 \mid q$, then ω is of odd order, and this follows from iv). We may henceforth assume that $2 \nmid q$.

If $-1 = \omega^{2\ell}$ for some ℓ, then by v)

$$c(-1,-1) = c(\omega^{2\ell},-1) = 1,$$

hence by ii)

$$c(\omega,-1) = c(\omega,\omega^{2\ell}) = c(\omega,+1) = 1.$$

If $-1 \neq \omega^{2\ell}$ for every ℓ, then $q \equiv 3 \bmod 4$, and -1 is an odd power of ω. By iv), we find

$$c(\omega,-1) = c(-1,-1),$$

and in this case we must only show that $c(-1,-1) = 1$.

To do this we show first:

5.4 <u>Lemma</u>: Under the assumptions of 2.1, let $x,y \in D^*$ be such that $xy = yx$. Then

$$c(-1,-1)c(x^2,-y^2) = c(-x^2,-y^2).$$

<u>Proof of 5.4</u>: By 2.1 α), β), δ), we have

$$c(-1,y^2) = c(-1,y)c(-y,y)c(y,y)^{-1} = 1$$

and

$$c(-1,-x^2)c(x^2,-y^2) = c(-1,(xy)^2)c(-x^2,-y^2).$$

Hence $(x = 1)$:

$$c(-1,-1) = c(-1,-y^2) \quad \text{for every } y \in D^*.$$

Putting these observations together proves the Lemma.

To finish the proof of 5.3 we write $\omega^s = -1$, with $2 \nmid s$ since we have $q \equiv 3 \bmod 4$.

Because -1 is a sum of two squares in the residue class field of K, an application of Hensel's Lemma shows the existence of $k \in \mathbb{N}$ and $v \in K^*$ such that $\omega^{2k}+v^2 = -1$.

By 5.4 $(x = 1)$ we find

$$c(-1,-1) = c(-1,-v^2) = c((-\omega^{2k})^s,-v^2) = c((1+v^2)^s,-v^2).$$

This is 1 by iii).

We now return to the proof of 5.2.

Applying relation 2.1 α) and 5.3 we find

$$c(\omega^{k+1},\Pi) = c(\omega,\omega^k\Pi)c(\omega^k,\Pi). \qquad (*)$$

We use $\Pi\omega = {}^{\sigma}\omega\Pi = \omega^{q^v}\Pi$ for some v with $(n,v) = 1$ and 2.5 to deduce, for every $\ell \in \mathbb{N}$:

$$c(\omega,\omega^k\Pi) = c(\omega,(-1)^{\ell}\omega^{k-\ell\cdot q^v}\Pi).$$

If ℓ is a solution of $k-\ell q^v \equiv 0 \bmod q^n-1$ (which obviously always exists) this yields

$$c(\omega,\omega^k\Pi) = c(\omega,(-1)^{\ell}\Pi).$$

If $2|q$ then we can always find an even solution ℓ for any k, hence in this case we have, for any k

$$c(\omega,\omega^k\Pi) = c(\omega,\Pi).$$

If $4|q^n-1$, then $-1 = \omega^{2k}$ holds for some natural k, and

$$c(\omega,-\Pi) = c(\omega,\omega^{2k-2\ell q^v}\Pi)$$

holds for every $\ell \in \mathbb{N}$. Taking ℓ such that $k \equiv \ell q^v \bmod q^n-1$ yields

$$c(\omega,-\Pi) = c(\omega,\Pi).$$

An induction on k using (*) now shows:

If $2|q$ or $4|q^n-1$ then

$$c(\omega^k,\Pi) = c(\omega,\Pi)^k$$

Hence in these cases 5.2 is shown.

We now assume: q odd and $4 \nmid q^n-1$.

Again by 2.1 α) and 5.3 we obtain:

$$c(\omega,\Pi) = c(-\omega,-\Pi)c(-1,\Pi),$$

$$c(\omega,-\Pi) = c(-\omega,\Pi(c(-1,-\Pi).$$

Another application of 2.5 gives

$$c(-\omega,-\Pi) = c(-\omega,-(-1)^{\ell}(-\omega)^{-\ell q^v}\Pi).$$

The order of $-\omega$ is $s := (q^n-1)/2$ which is odd by assumption, hence any odd solution ℓ of $\ell q^v \equiv 0 \bmod (q^n-1)/2$ yields

$$c(-\omega,-\Pi) = c(-\omega,\Pi).$$

It remains to show $c(-1,\Pi) = c(-1,-\Pi)$.

By Hensel's Lemma, we may find $k \in \mathbb{N}$, $v \in K^*$, hence v central in D, with $\omega^{2k}+v^2 = -1$. Using 2.1 δ) we find:

$$c(-\Pi,-v^2) = c((-\omega^{2k})^s\Pi,-v^2) = c((1+v^2)^s\Pi,-v^2) = c(\Pi,-v^2).$$

By 2.1 α) we get

$$c(-v^2,\Pi) = c(v^2,-1)^{-1}c(v^2,-\Pi)c(-1,\Pi),$$

$$c(-v^2,-\Pi) = c(v^2,-1)^{-1}c(v^2,\Pi)c(-1,-\Pi).$$

By Matsumoto [9, Prop. 5.7] the pairing $(x,y) \mapsto c(x^2,y)$ is bimultiplicative when restricted to a commutative subfield of D, hence $c(v^2,-\Pi) = c(v^2,-1)c(v^2,\Pi)$. By 5.3, 5.4, $c(v^2,-1) = 1$. Putting together these equations we obtain $c(-1,\Pi) = c(-1,-\Pi)$, as desired. This proves Theorem 5.2.

In the following we use the notation ${}^ab := aba^{-1}$ for elements a, b of any group.

5.5 <u>Lemma</u>: Let $i,j \in \mathbb{N} \cup \{0\}$, $i+j > 0$, and $\alpha,\beta \in \mathcal{O}_D$. Assume that $\beta \neq 0$, $1-\alpha\Pi^i$, $1-\beta_1\Pi^j \in \mathcal{O}_D^*$ for $\beta_1 := {}^{\Pi^j}\!\beta(1-\alpha\Pi^i)^{-1}$. Then if $\alpha_1 := {}^{\Pi^i}\!\alpha\, {}^{\Pi^{i+j}}\!\beta_1(1-\beta_1\Pi^j)^{-1}$, the following relation holds in U:

$$c(1-\alpha\Pi^i,1-\beta\Pi^j) = c(1-\alpha_1\Pi^{i+j},\beta_1\Pi^j).$$

(It is useful to remark that, for every pair α_1, $\beta_1 \in \mathcal{O}_D$, not both $\equiv 1 \bmod \Pi$ in case $i = 0$, with β_1, $1-\beta_1\Pi^j \in \mathcal{O}_D^*$ there exist $\alpha,\beta \in \mathcal{O}_D$ such that the above assumptions hold.)

<u>Proof</u>: We apply relations δ), δ'), δ'') from §2 (2.1, 2.4, 2.8):

δ) $\quad c(x,y) = c(x,y(1-x))$,

δ') $\quad c(x,y) = c(x(1-y),y)$,

δ'') $\quad c(1-xy,y) = c(x,1-yx)$.

With $x := 1-\alpha\Pi^i$ we have

$$\begin{aligned} c(x,1-\beta\Pi^j) &= c(x,1-\beta_1\Pi^j x) \\ &= c(1-x\beta_1\Pi^j,\beta_1\Pi^j) && \text{(by } \delta''\text{))} \\ &= c((1-\beta_1\Pi^j+\alpha^{\Pi^i}\beta_1\Pi^{i+j})(1-\beta_1\Pi^j)^{-1},\beta_1\Pi^j) && \text{(by } \delta'\text{))} \\ &= c(1-\alpha_1\Pi^{i+j},\beta_1\Pi^j). \end{aligned}$$

5.6 Theorem: Let U_1 be the subgroup of U generated by all $c(x,y)$, where $x,y \in \mathcal{O}_D^*$ and at least one congruent to 1 modulo Π. Then U_1 is a normal subgroup of U, and U is a semidirect product of a cyclic subgroup of order q^n-1 and U_1 as follows:

$$U = \langle c(\omega,\Pi)\rangle \ltimes U_1 .$$

Hence U_1 is the kernel of the tame symbol.

Proof: Normality follows from 2.1 γ) respective 2.7 γ'): If $u,v \in D^*$, then $[u,v] \in \mathcal{O}_D^*$, hence e.g.:

$$c(u,v)_{c(1+\alpha\Pi,y)} = c([u,v]\ ,1+\alpha\Pi)c(1+\alpha\Pi,[u,v]y).$$

It remains to show: Every $c(x,y)$ can be written as a product of an element in U_1 and a power of $c(\omega,\Pi)$.

If $x = \Pi^i u$, $y = \Pi^j v$, $i,j \in \mathbb{Z}$, $u,v \in \mathcal{O}_D^*$, an application of 2.7 together with Euclid's algorithm gives

$$c(x,y) = c(\Pi^k u',v') \quad \text{or} \quad = c(u',\Pi^k v')$$

for some $k \in \mathbb{N}$, $u',v' \in \mathcal{O}_D^*$. Hence we may assume that both entries of c are in $\mathcal{O}_D$ and at most one is divisible by Π.

By using 2.1 α), 2.7, we will show that we may assume that Π occurs only in the first power:

$$\begin{aligned} c(u,\Pi^{k+1}v) &= c(u,\Pi)c(\Pi u,\Pi^k v)c(\Pi,\Pi^k v)^{-1} \\ &= c(u,\Pi)c(\Pi u,(-1)^k v')c(\Pi,(-1)^k v'')^{-1}, \end{aligned}$$

for $u,v \in \mathcal{O}_D^*$ and suitable $v',v'' \in \mathcal{O}_D^*$.

We now may write $u = u_1\omega^i$, $v = v_1\omega^j$ with $i,j \in \mathbb{N}$, $u_1,v_1 \equiv 1$ modulo Π. 2.1 α) gives

$$c(u,\Pi v) = c(\omega^i,u_1)^{-1}c(\omega^i,u_1\Pi v)c(u_1,\Pi v),$$

where the first and the last factor are in U_1 by definition resp. by 5.5.

For the second factor we obtain, by 2.1 α):

$$\begin{aligned} c(\omega^i, u_1\Pi v) &= c(\omega^i, u_1\Pi v_1\omega^j) \\ &= c(\omega^i, \omega^j\Pi w_1) \quad \text{for some } w_1 \in 1+\Pi\mathcal{O}_D, \\ &= c(\omega^i, \omega^j\Pi)c(\omega^j\Pi\omega^i, w_1)c(\omega^j\Pi, w_1)^{-1}. \end{aligned}$$

Again, by 5.5 (using the antiautomorphism A of U), the last two factors are in U_1, while, by 2.1 α), we find for the first, using 5.2, 5.3,

$$c(\omega^i, \omega^j\Pi) = c(\omega^{i+j}, \Pi)c(\omega^j, \Pi)^{-1} = c(\omega, \Pi)^i.$$

This proves 5.6.

5.7 <u>Corollary</u>: The Schur multiplier of $Sl_2(D)$ has a splitting

$$H_2(SL_2(D), \mathbb{Z}) = \langle c(\omega_0, \Pi)\rangle \times (U_1 \cap H_2(SL_2(D), \mathbb{Z}),$$

where ω_0 is a generator of the subgroup of the (q-1)-th roots of unity of the center K of D. Moreover, $c(\omega_0, \Pi) = c(\omega, \pi)$, where $\pi = \Pi^n \in K$, and ω_0 is the reduced norm of ω.

The only non-obvious part of this statement is the last relation, which is a special case of

5.8 <u>Proposition</u>: In U, the following is true for any $k \in \mathbb{N}$:

$$c(\omega, \Pi^k) = c(\prod_{j=0}^{k-1} {}^{\Pi^j}\omega, \Pi).$$

<u>Proof</u>: We have

$$\begin{aligned} c(\omega, \Pi^{k+1}) &= c(\omega, \Pi^k)c(\Pi^k\omega, \Pi)c(\Pi^k, \Pi)^{-1} \\ &= c(\omega, \Pi^k)c({}^{\Pi^k}\omega\cdot(-1)^k, \Pi)c((-1)^k, \Pi)^{-1} \\ &= c(\omega, \Pi^k)c({}^{\Pi^k}\omega, \Pi). \end{aligned}$$

An induction on k gives the result.

6. Continuous central extensions of $SL_2(D)$.

We keep the notations of the preceding paragraph.

Every $u \in D^*$ can be written uniquely as

$$u = \Pi^i \omega^j (1+\alpha\Pi^\ell),$$

where $i \in \mathbb{Z}$, $j \in \mathbb{Z}/(q-1)\mathbb{Z}$, $\alpha \in \mathcal{O}_D^*$ and $\ell \in \mathbb{N}$.

For $m \in \mathbb{N}$ we define the subgroup U_m of U to be generated by $c(u,v)$ with $u,v \in \mathcal{O}_D^*$ and at least one of the two arguments in $1+\Pi^m\mathcal{O}_D$. Hence, by §5, U_1 is exactly the kernel of the tame symbol. Moreover, the first argument in the proof of 5.6 shows that U_m is normal in U.

We will investigate the quotients U_m/U_{m+1}.

6.1 <u>Lemma</u>: If $u,v \in \mathcal{O}_D^*$, then $c(u,v) \in U_1$, and its value in U/U_{m+1} depends only on the classes of u and v in $\mathcal{O}_D^*/1+\Pi^{m+1}\mathcal{O}_D$.

<u>Proof</u>: The first statement follows from the properties of the tame symbol. For the second, we write $v = v_1(1+\gamma\Pi^{m+1})$ (with $\gamma \in \mathcal{O}_D$) and apply 2.1 α):

$$c(u,v) = c(u,v_1)c(v_1u,1+\gamma\Pi^{m+1})c(v_1,1+\gamma\Pi^{m+1}) .$$

6.2 <u>Lemma</u>: If $i,j \geq 1$ then for $\alpha,\beta \in \mathcal{O}_D$ we have

$$\xi := c(1+\alpha\Pi^i,1+\beta\Pi^j) \in c(1+\mathcal{O}_D\Pi^{i+j-1},1+\mathcal{O}_D\Pi)U_{i+j} ,$$

and the value of ξ modulo U_{i+j} depends only on the classes of α, β module $\Pi\mathcal{O}_D$.

<u>Proof</u>: Obviously, $c(1\pm\alpha\Pi^i,1\pm\beta\Pi^j) \in U_1$ for all $\alpha,\beta \in \mathcal{O}_D$. We write $m := i+j$. By 5.5, 2.1 α) we obtain, for $\alpha,\beta \in \mathcal{O}_D$ and suitable $\alpha_1,\beta_1 \in \mathcal{O}_D$,

$$\text{i)}\quad c(1-\alpha\Pi^i,1-\beta\Pi^j) = c(1-\alpha_1\Pi^m,\beta_1\Pi^j)$$
$$\equiv c(\beta_1(1-\alpha_1\Pi^m),\Pi^j)c(\beta_1,\Pi^j)^{-1} \text{ modulo } U_m.$$

We also have, in case $j > 1$, with $u := 1-\alpha_1\Pi^m$:

$$\text{ii)}\quad c(u,\beta_1\Pi^j) = c(u,\beta_1\Pi^{j-1})c(\beta_1\Pi^{j-1}u,\Pi)c(\beta_1\Pi^{j-1},\Pi)^{-1} \quad \text{(by 2.1 } \alpha))$$

$$= c(u,\beta_1\Pi^{j-1})c(\beta_2u',\Pi)c(\beta_2,\Pi)^{-1} \quad \text{(by 2.5)}$$

$$\equiv c(u,\beta_1\Pi^{j-1})c(u',\beta_2\Pi) \quad \text{modulo } U_m,$$

with $\beta_2 = (-1)^{j-1}\beta_1$, $u' = \Pi^{j-1}u$; for the last congruence we used i) (in the case $j = 1$) backwards. An induction on j proves the first statement of the lemma. To prove the second, we first assume $n \nmid j$. We then can write

$$1-\beta\Pi^j = [\omega, 1-\omega^k\Pi^j]\cdot v,\ v \in \mathcal{O}_D,\ v \equiv 1 \bmod \Pi^m,\ k \in \mathbb{N}.$$

(This simply requires to solve the congruence

$$-\beta \equiv \omega^k(\omega^{\Pi^j}\omega^{-1}-1) \bmod \Pi$$

which is possible if $n \nmid j$.)

By 2.7 γ') we have

$$c(1-\alpha\Pi^i, 1-\beta\Pi^j) = c(1-\alpha\Pi^i,[\omega,1-\omega^k\Pi^j])^{c(\omega,1-\omega^k\Pi^j)}c(1-\beta\Pi^j,v).$$

The last factor is in U_m by the first part of this lemma, hence the second statement is true in case $n \nmid j$.

Using the antiautomorphism A, we obtain the corresponding result in case $n|i$ for the first variable of c. To prove the statement in general we use ii) above together with 5.5 which yields, in case $n|j$, say, a congruence module U_m

$$c(1-\alpha\Pi^i, 1-\beta\Pi^j) \equiv c(1-\alpha'\Pi^{i+1}, 1-\beta'\Pi^{j-1})c(1-\alpha''\Pi^{i+j-1}, 1-\beta''\Pi)$$

where the class of β', β'' modulo Π are uniquely determined by the class of β modulo Π. This and the corresponding symmetric result proves 6.2.

6.3 <u>Lemma</u>: If $\alpha \in \mathcal{O}_D$ and $\beta' = \beta(1-\alpha\Pi^{m+1}) \in \mathcal{O}_D^*$, then for any $\gamma \in \mathcal{O}_D$ the following is true:

$$c(\beta',\gamma\Pi) \equiv c(\beta,\gamma\Pi) \quad \text{modulo } U_m.$$

This follows from i) in the proof of 6.2, with m replaced by $m+1$, $j = 1$, $i = m$.

6.4 Lemma: If $i, j \geq 0$, $n \nmid i+j$, then we have

$$c(1+\mathfrak{o}_D\Pi^i, 1+\mathfrak{o}_D\Pi^j) \subseteq U_{i+j}.$$

Proof: We may assume $i,j \geq 1$ and, by 6.2, $j = 1$. We write $m := i+j = i+1$. According to 5.5 and to step i) in the proof of 6.2 we have, for $\alpha,\beta,\gamma \in \mathfrak{o}_D^*$:

$$c(1-\alpha\Pi^i, 1-\beta\gamma\Pi^j) = c(1-\alpha_1\Pi^m, \beta\gamma_1\Pi^j)$$

$$\equiv c(\beta(1-\alpha_1\Pi^m), \gamma_1\Pi^j)c(\beta,\gamma_1\Pi^j)^{-1} \quad \text{modulo} \quad U_m,$$

with $\beta\gamma_1 = \beta\gamma^{\Pi^j}(1-\alpha\Pi^i)^{-1}$, $\alpha_1 = \alpha^{\Pi^i}(\beta\gamma_1)^{\Pi^m}(1-\beta\gamma_1\Pi^j)^{-1}$. Using $n \nmid m$, we find $\gamma' \in \mathfrak{o}_D$, $\beta' \in \mathfrak{o}_D^*$, $\beta' \equiv \beta$ mod $1+\mathfrak{o}_D\Pi^{m+1}$, such that

$$\beta(1-\alpha_1\Pi^m) = [\omega, 1+\gamma'\Pi^m]\beta'$$

similarly as in the proof of 6.2.

Hence we obtain modulo U_m:

$$c(\beta(1-\alpha_1\Pi^m), \gamma_1\Pi^j) = c([\omega,1+\gamma'\Pi^m]\beta', \gamma_1\Pi^j)$$

$$\equiv c(\beta',\gamma_1\Pi^j)c([\omega,1+\gamma'\Pi^m],\gamma_1\Pi^j) \qquad \text{(by 2.1 } \gamma))$$

$$\equiv c(\beta,\gamma_1\Pi^j)c([\omega,1+\gamma'\Pi^m],\gamma_1\Pi^j) \qquad \text{(by 6.3)}$$

$$\equiv c([\omega,1+\gamma'\Pi^m],[\beta,\gamma_1\Pi^j]\gamma_1\Pi^j)c(\beta,\gamma_1\Pi^j) \qquad \text{(by 2.7 } \gamma'))$$

$$\equiv c({}^{\beta}(1-\alpha_1\Pi^m), {}^{\beta}(\gamma_1\Pi^j))c(\beta,\gamma_1\Pi^j) \qquad \text{(by 6.3)}$$

This yields

$$c(1-\alpha_1\Pi^m, \beta\gamma_1\Pi^j) \equiv c({}^{\beta}(1-\alpha_1\Pi^m), {}^{\beta}(\gamma_1\Pi^j)) \text{ mod } U_m,$$

equivalently:

$$c(1-\alpha_1\Pi^m, \beta\gamma_1\Pi^j) \equiv c(1-\beta\alpha_1{}^{\Pi^m}\beta^{-1}\cdot\Pi^m, \beta\gamma_1{}^{\Pi^j}\beta^{-1}\cdot\Pi^j) \text{ mod } U_m.$$

Since β was arbitrary (in $\mathfrak{o}_D^*$), we may write this as

(*) $$c(1-\alpha_1\Pi^m, \beta_1\Pi^j) \equiv c(1-\varepsilon\alpha_1{}^{\Pi^m}\varepsilon^{-1}\cdot\Pi^m, \beta_1{}^{\Pi^j}\varepsilon^{-1}\cdot\Pi^j) \text{ mod } U_m.$$

We now use 5.5 and 6.2 several times:

$$c(1-\varepsilon\alpha\Pi^{i}, 1-\beta\,{}^{\Pi^{j}}\varepsilon^{-1}\Pi^{j})$$

$$\equiv c(1-\varepsilon\alpha\,{}^{\Pi^{i}}(\beta_1\,{}^{\Pi^{j}}\varepsilon^{-1})\Pi^{m}, \beta_1\,{}^{\Pi^{j}}\varepsilon^{-1}\Pi^{j}) \qquad (5.5,\ 6.2)$$

$$\equiv c(1-\varepsilon\alpha\,{}^{\Pi^{i}}\beta_1\,{}^{\Pi^{m}}\varepsilon^{-1}\Pi^{m}, \beta_1\,{}^{\Pi^{j}}\varepsilon^{-1}\Pi^{j}) \qquad \text{(trivially)}$$

$$\equiv c(1-\alpha\,{}^{\Pi^{i}}\beta_1\Pi^{m}, \beta_1\Pi^{j}) \qquad \text{(by (*) above)}$$

$$\equiv c(1-\alpha\Pi^{i}, 1-\beta\Pi^{j}) \qquad \text{(by 5.5)} .$$

This yields the two relations modulo U_m ($\varepsilon \in \mathscr{O}_D^*$ arbitrary):

$$c(1-\varepsilon\alpha\Pi^{i}, 1-\beta\Pi^{j}) \equiv c(1-\alpha\Pi^{i}, 1-\beta\Pi^{j}\varepsilon),$$

$$c(1-\alpha\Pi^{i}\varepsilon, 1-\beta\Pi^{j}) \equiv c(1-\alpha\Pi^{i}, 1-\varepsilon\beta\Pi^{j}),$$

the second being obtained from the first by means of the anti-automorphism A and by interchanging i and j. We apply this to the special case $i = m-1$, $j = 1$ to obtain

$$c(1-\alpha\Pi^{i}, 1-\beta\Pi) \equiv c(1-\Pi^{i}, 1-\beta\,{}^{\Pi}\alpha\Pi) \equiv c(1-\Pi^{i}, 1-{}^{\Pi^{-i}}\alpha\cdot\beta\Pi) .$$

With $\gamma = {}^{\Pi^{-i}}\alpha$ this implies, for every $\beta \in \mathscr{O}_D^*$,

$$c(1-\Pi^{i}, 1-\beta\gamma\Pi) \equiv c(1-\Pi^{i}, 1-{}^{\Pi^{m}}\gamma\beta\Pi).$$

Now, by 6.2, we may replace all entries by powers of ω, hence β, γ, ${}^{\Pi^{m}}\gamma$ commute with each other.

We write $[\omega, 1+\varepsilon\Pi] \equiv 1+\beta\gamma\Pi \bmod 1+\mathscr{O}_D\Pi^2$ with suitable $\varepsilon \in \mathscr{O}_D^*$ and obtain, using the above relation, 6.2, and relations 2.1 γ), 2.7 γ'):

$$c(1-\Pi^{i}, 1+\beta(\gamma-{}^{\Pi^{m}}\gamma)\Pi)$$

$$\equiv c(1-\Pi^{i}, 1+\beta\gamma\Pi)^{c(\omega,1+\varepsilon\Pi)} c(1-\Pi^{i}, 1-\beta\,{}^{\Pi^{m}}\gamma\Pi)$$

$$\equiv c(1-\Pi^{i}, 1+\beta\gamma\Pi)^{c(\omega,1+\varepsilon\Pi)} c(1-\Pi^{i}, 1-\beta\gamma\Pi)$$

$$\equiv c(1-\Pi^{i}, 1+\beta\gamma\Pi)^{c(\omega,1+\varepsilon\Pi)} c(1-\Pi^{i}, (1+\beta\gamma\Pi)^{-1})$$

$$\equiv 1 \text{ modulo } U_m.$$

Since this is true for arbitrary β, this concludes the proof of Lemma 6.4.

6.5 Lemma: Let U_m' be the subgroup of U generated by U_m and by all $c(1+\mathfrak{o}_D\Pi^i, 1+\mathfrak{o}_D\Pi^j)$, $i+j = m$. (By 6.4: $U_m' = U_m$ if $n \nmid m$.) Then we have: Every element of U_m can be represented, modulo U_{m+1}', by $c(\omega, 1+\alpha\Pi^m)$, $\alpha \in \mathfrak{o}_D$.

Proof: Up to A-symmetry, we may write an arbitrary generator of U_m in the form

$$c(\omega^k u, v),\ k \in \mathbb{N},\ u, v \in \mathfrak{o}_D^*,\ u \equiv 1 \bmod \Pi,\ v \equiv 1 \bmod \Pi^m.$$

Up to an element of norm one in $1+\mathfrak{o}_D\Pi$, which is a product of commutators, u can be replaced by an element w in $\mathfrak{o}_L \cap 1+\mathfrak{o}_D\Pi$ [19; p.89], [12]. Hence we may write

$$\omega^k u = u_1\omega^k w,\ N(u_1) = 1,\ w \in \mathfrak{o}_L,\ u_1 \equiv w \equiv 1 \bmod \Pi.$$

If ξ is a preimage of u_1 in U_1 we obtain by

$$c(\omega^k u, v) = {}^{\xi}c(\omega^k u_1, v)c(u_1, v) \quad \text{(by 2.1 } \gamma))$$

$$\equiv {}^{\xi}c(\omega^k u_1, v) \qquad \text{modulo } U_{m+1}' .$$

Now 2.1 γ) and 2.7 γ') show that U_m/U_{m+1}' is central in U_1/U_{m+1}', hence we obtain modulo U_{m+1}':

$$c(\omega^k u, v) \equiv c(\omega^k u_1, v),\ u^k u_1 \in \mathfrak{o}_L^* .$$

If $n|m$, then v may be replaced by $1+\alpha\Pi^m$ with $\alpha \in \mathfrak{o}_L$, hence $1+\alpha\Pi^m \in \mathfrak{o}_L$. But then $c(\omega^k u_1, 1+\alpha\Pi^m)$ lies in the natural image of $H_2(SL_2(L), \mathbb{Z})$, which is, by [9; 11.1], bimultiplicative when evaluated modulo U_{m+1}. This gives

$$c(\omega^k u, v) \equiv c(\omega, (1+\alpha\Pi^m)^k) \bmod U_{m+1} .$$

Hence we may assume $n \nmid m$. Then we may choose $\beta \in \mathfrak{o}_D$ such that

$$u_1 v u_1^{-1} \equiv [\omega, 1+\beta\Pi^m] \bmod 1+\mathfrak{o}_D\Pi^{m+1}.$$

We then obtain by 2.1 α), modulo U_{m+1}':

$$c(\omega^k u, v) \equiv c(\omega^k u_1, v)$$
$$\equiv c(u_1,\omega^k)^{-1} c(\omega^k, [\omega, 1+\beta\Pi^m] u_1)$$
$$\equiv c(u_1,\omega^k)^{-1} c(\omega^k, [\omega, 1+\beta\Pi^m])^{c(\omega, 1+\beta\Pi^m)} c(\omega^k, u_1)$$
$$\equiv c(\omega^k, [\omega, 1+\beta\Pi^m]),$$

the last result is due to the centrality of $c(u_1,\omega^k)$ in U. By 2.1 γ), $c(\omega^k,[x,y])^{-1} = c([x,y],\omega^k)$, hence we have proved that every generating element is represented by some $c(\omega^k,u)$, $u \equiv 1 \mod \Pi^{m+1}$.

We use induction together with 2.1 α) and 5.3 to reduce to $k = 1$:

$$c(\omega^{k+1},u) = c(\omega,\omega^k u) c(\omega^k,u)^{-1}$$

since $\omega^k u \omega^{-k}$ can be written as a commutator, we find by 2.1 γ):

$$c(\omega,\omega^k u) = c(\omega,u).$$

Now if $u, v \in 1+\mathcal{O}_D\Pi^m$, we may write $u = [\omega, 1+\gamma\Pi^m]$ with some $\gamma \in \mathcal{O}_D$ to obtain from 2.1 γ):

$$c(\omega,uv) = c(\omega,u)^{c(\omega,1+\gamma\Pi^m)} c(\omega,v)$$
$$\equiv c(\omega,u)c(\omega,v) \quad \text{modulo } U'_{m+1},$$

the latter argument using again the centrality of U_m/U'_{m+1} in U_1/U'_{m+1}, which follows from 2.1 γ), 2.7 γ').

Hence $c(\omega,u)$ is multiplicative in u and Lemma 6.5 is proved.

6.6 <u>Lemma</u>: If $n|m$, then every element of U'_m can be represented, modulo U_m, by

$$c(\Pi, 1+\alpha\Pi^m), \ \alpha \in \mathcal{O}_L.$$

<u>Proof</u>: Let $c(1-\alpha\Pi^i, 1-\beta\Pi^j) \in U'_m$, $\alpha,\beta \in \mathcal{O}_D^*$, $i+j = m$. Then, by 6.2, we may assume that $\alpha,\beta \in \langle\omega\rangle \subseteq \mathcal{O}_L^*$. We first assume that the reduced trace $S(\alpha_1)$ of $\alpha_1 := a^{\Pi^i}\beta$ is congruent 0 mod Π. Then

$$1-\alpha_1\Pi^m \equiv [1+\Pi, 1+\gamma\Pi^{m-1}] \mod 1+\mathcal{O}_D\Pi^{m+1}$$

for some $\gamma \in \mathfrak{o}_L^*$. We write $\beta = \delta\epsilon$ for some $\delta, \epsilon \in \langle\omega\rangle$ and obtain, modulo U_m:

$$c(1-\alpha\Pi^i, 1-\beta\Pi^j) \equiv c(1-\alpha_1\Pi^m, \delta\epsilon\Pi^j) \qquad (5.5)$$

$$\equiv c([1+\Pi, 1+\gamma\Pi^{m-1}]\delta, \epsilon\Pi^j)c(\delta, \epsilon\Pi^j)^{-1} \qquad (2.1\ \alpha))$$

$$\equiv c(\delta, \epsilon\Pi^j)c([1+\Pi, 1+\gamma\Pi^{m-1}], \epsilon\Pi^j)c(\delta, \epsilon\Pi^j)^{-1} \qquad (2.1\ \gamma))$$

$$\equiv c(1-\alpha_1\Pi^m, {}^{\Pi^j}\delta^{-1}(\delta\epsilon)\Pi^j) \qquad (2.7\ \gamma'))$$

$$\equiv c(1-\alpha\delta\,\Pi^i, 1-{}^{\Pi^j}\delta^{-1}\beta\Pi^j). \qquad (5.5)$$

We may state this result as follows:

i) If $\alpha, \beta, \gamma \in \langle\omega\rangle$ are such that $\alpha^{\Pi^i}(\beta\gamma)$ has reduced trace 0, then we have, modulo U_m:

$$c(1-\alpha\Pi^i, 1-\beta\gamma\Pi^j) \equiv c(1-\alpha^{\Pi^i}\beta\Pi^i, 1-\gamma\Pi).$$

We now denote by V the subgroup of U_m' generated by U_m and by all elements $c(1-\alpha\Pi^{m-1}, 1-\Pi)$. We claim that $V = U_m'$. By 6.2, we have to show that every element $d(\alpha,\beta) := c(1-\alpha\Pi^{m-1}, 1-\beta\Pi)$ is in V. This is obvious from i) in case $S(\alpha^{\Pi^i}\beta) = 0$, hence we may assume $S({}^{\Pi}\alpha\cdot\beta) \neq 0$ (S denoting the reduced trace). From 2.1 α) it follows immediately that $d(\alpha,\beta+\gamma) \equiv d(\alpha,\beta)d(\alpha,\gamma)$, $d(\alpha+\beta,\gamma) \equiv d(\alpha,\gamma)d(\beta,\gamma)$ modulo U_m.

If $\beta \in K \cap \langle\omega\rangle$ then we may find a $\beta' \in \langle\omega\rangle$, $\beta' \notin K$ such that $S({}^{\Pi}\alpha\beta') = 0$, hence $S({}^{\Pi}\alpha(\beta+\beta')) = S({}^{\Pi}\alpha\beta)$ and

$$d(\alpha,\beta+\beta') \equiv d(\alpha,\beta)d(\alpha,\beta') \equiv d(\alpha,\beta) \bmod U_m \quad (\text{by i})).$$

Hence we may assume $S({}^{\Pi}\alpha\cdot\beta) \neq 0$ and $\beta \in \langle\omega\rangle$, $\beta \notin K$. Comparing dimensions of vector spaces over $\mathfrak{o}_K/\mathfrak{p}_K$ and using the non-degeneracy of the bilinear form defined by the trace of separate extensions, we find that there exists a $\xi \in \langle\omega\rangle$ such that

$$S({}^{\Pi}\xi\cdot\beta) = 0, \ S(\xi) \neq 0.$$

Hence we find a $\lambda \in \langle\omega\rangle \cap K$ such that

$$\lambda S(\xi) = S({}^{\Pi}\alpha\cdot(\beta-1)),$$

which implies

ii) $$S((\alpha+\lambda\xi)^{\Pi^{-1}}(1-\beta)) = 0.$$

Therefore we may compute, modulo V, using i) several times:

$$\begin{aligned} d(\alpha,\beta) &\equiv d(\alpha+\lambda\xi,\beta) && (\text{since } S(\lambda\xi^{\Pi^{-1}}\beta) = 0) \\ &\equiv d(\alpha+\lambda\xi,\beta+(1-\beta)) && (\text{since ii) holds}) \\ &\equiv d(\alpha+\lambda\xi,1). \end{aligned}$$

This proves $V = U'_m$, and moreover, by the bilinearity of d, that every element of U'_m is of the shape

$$c(1+\alpha\Pi^{m-1},1+\Pi)^{-1} = c(1+\Pi,1+\alpha\Pi^{m-1}).$$

An application of the symmetric version of 5.5 gives Lemma 6.6.

6.7 <u>Corollary</u>: If $n|m$, then every element of $U'_m \cap \operatorname{Ker}\varphi_0$ is, modulo U_m, of the form

$$c(\Pi,1+\alpha\pi^{\frac{m}{n}}),\ \alpha\in\mathcal{O}_L.$$

(Recall $\pi = \Pi^n \in \mathcal{O}_L$.)

<u>Proof</u>: If $c(\Pi,1+\alpha\Pi^m) \in U'_m \cap \operatorname{Ker}\varphi_0$ then

$$1 = [\Pi,1+\alpha\Pi^m] \equiv 1+({}^{\Pi}\alpha-\alpha)\Pi^m \bmod \Pi^{m+1},$$

hence (since we may take $\alpha \in \langle\omega\rangle$) $\alpha \in \mathcal{O}_K$. On the other hand, we have, in U'_m/U_m:

$$\begin{aligned} &c(1+\gamma\Pi^m,\Pi^{k+1}) \\ &= c(1+\gamma\Pi^m,\Pi^k)c(\Pi^k(1+\gamma\Pi^m),\Pi)c(\Pi^k,\Pi)^{-1} && (2.1\ \alpha)) \\ &= c(1+\gamma\Pi^m,\Pi^k)c((-1)^k(1+{}^{\Pi^k}\gamma\Pi^m),\Pi)c((-1)^k,\Pi)^{-1} && (2.5) \\ &= c(1+\gamma\Pi^m,\Pi^k)c(1+{}^{\Pi^k}\gamma\Pi^m,(-1)^k\Pi). && (2.1\ \alpha)) \end{aligned}$$

By 5.5, the second factor is independent from the sign of Π, hence we obtain, by induction on k:

$$c(1+\gamma\Pi^m,\Pi^k) = c(1+\sum_{i=0}^{k-1}\Pi^i\gamma\Pi^m,\Pi).$$

Since the trace of finite extensions of finite field is surjective, the case $k = n$ yields the corollary.

6.8 Theorem: Let D be a non-archimedean local division algebra with center K. Let $r \in \mathbb{N}$, $r \geq 2$ and

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} SL_r(D) \longrightarrow 1$$

be the universal topological central extension of $SL_r(D)$.

Then A is isomorphic to the group $\mu(K)$ of roots of unity of K.

Remark: The existence of a universal topological central extension follows from the work of Moore [10]. G is a second countable locally compact group, A is central and closed in G, and φ is continuous.

Proof: We first consider the case $r = 2$.

We identify G with a quotient of $St_2(D)$, hence A becomes a quotient of $H_2(SL_2(D),\mathbb{Z})$. The natural images of various elements of $St_2(D)$ defined in §1 will be denoted by the same symbols as their corresponding preimages, hence we consider $x_{ij}(u)$, $h_{ij}(u)$, $c(u,v) = h_{12}(u)h_{12}(v)h_{12}(vu)^{-1}$ to be elements of G. Since φ restricted to the subgroup $\{x_{ij}(u) | u \in D\}$ is injective one obtains, using the usual Bruhat-decomposition of $St_2(D)$, that $u \mapsto x_{ij}(u)$ is a continuous map, hence the pairing

$$c: D^* \times D^* \to U = \langle c(u,v) \in G | u,v \in D^* \rangle$$

is continuous.

If $\xi \in \operatorname{Ker}\varphi$, then, by Theorem 2.1, $\xi \in U$, and it follows from 5.7, 6.5 and 6.7 that

$$\xi = c(\pi,\alpha)c(\omega,\beta)\eta$$

where $\pi,\alpha,\beta \in \mathcal{O}_L$, π a prime of K, and $\eta \in \bigcap_{m\in\mathbb{N}} U_m$. Since the U_m form a system of closed normal subgroups which is cofinal in the topology of U their intersection is trivial since G is Hausdorff. Hence ξ is in the canonical image of $H_2(SL_2(L),\mathbb{Z})$. Since the Galois operation of the cyclic extension $L:K$ is - in D - induced by inner automorphisms, the centrality of A implies that the kernel of the canonical map

$$H_2(SL_2(L),\mathbb{Z}) \to A$$

vanishes on all elements ${}^{\sigma}\xi\cdot\xi^{-1}$, $\sigma \in G(L:K)$. Clearly it also factors through the topological fundamental group of $SL_2(L)$, which is, by Matsumoto [9; 11.1] or by Moore [11], isomorphic to $\mu(L)$. Hence A is a quotient of $\mu(L)/{}^{\sigma-1}\mu(L) \simeq \mu(K)$.

On the other hand, say by 2.1 and by [14], the canonical map

$$H_2(SL_2(D),\mathbb{Z}) \to H_2(SL_n(D),\mathbb{Z})$$

is surjective for arbitrary skew fields, and the groups on the right are known to be independent from n and isomorphic to $K_2(D)$. An analogues observation holds for the corresponding topological fundamental groups in case of a topological D, which, for $n \geq 3$, are $K_2^{top}(D)$. Hence we get the composite map

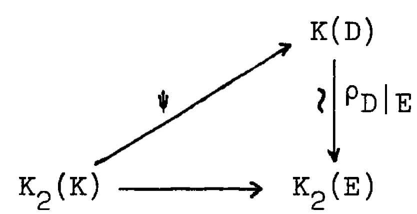
$$\mu(L)/{}^{(\sigma-1)}\mu(L) \to A \to K_2^{top}(D),$$

and it can be deduced from [15; Theorem 3.1 ii)] that the image of this map contains a subgroup isomorphic to $\mu(K)$ except if $char(K) = 0$, the residue characteristic of K is 2, $\mu(K) = \{\pm 1\}$ and D has no algebraic splitting field such that -1 is a norm of a root of unity from that field. (The latter condition requires that D is of even index.) In the exceptional case (as well as in all other cases also) the proof now can be concluded using a theorem of Suslin [21] and results of [15] as follows:

By [15; 2.4] there exists a homomorphism

$$\psi : K_2(K) \to K_2(D)$$

defined by $\psi(c(\alpha,\beta)) := c(\alpha,b)$, where $\alpha,\beta \in K^*$ and $b \in D^*$ such that $Nb = \beta$, such that, for every splitting field E of D, the diagram



commutes, where $\rho_{D|E}$ is the natural transfer map (factoring through $K_2(D \otimes_K E)$).

By [21; 3.6], the natural map $K_2(K) \to K_2(E)$ is injective if K is algebraically closed in E. This property holds for the generic splitting field of E (which is characterized by the property that every splitting field of D contains a specialization of E and which always exists, cf. [18]). Since the topological fundamental group of $SL_r(K)$, $r \geq 2$, is a factor (isomorphic to $\mu(K)$) of $K_2(K)$ [9, 10], which can be generated by a symbol $c(\pi,\epsilon)$, where π is a prime and ϵ a unit of K [11], and since L/K is unramified, there is a unit $e \in L$ with $Ne = \epsilon$, hence it follows now that the natural image of $H_2(SL_2(L),\mathbb{Z})$ in A is of order at least $|\mu(K)|$, which concludes the proof.

The theory of fundamental groups of $SL_n(D)$ $(n \geq 2)$ for local non-archimedean D now can be described in a completely satisfactory and uniform way in terms of the norm residue symbol

$$(\ ,\ ): K^* \times K^* \to \mu(K)$$

of the center K of D:

6.9 Corollary: For any D as in 6.8, and any $r \geq 2$, the topological fundamental group of $SL_r(D)$ is isomorphic to the group $\mu(K)$ of roots of unity of K. More precisely:

If $G \xrightarrow{\varphi} SL_r(D)$ is a univeral topological extension and if $h_{12}(u) \in G$ is defined as in §1 $(r = 2)$ resp. as in [14] $(r \geq 3)$, then there is an isomorphism

$$i: \mu(K) \xrightarrow{\sim} \operatorname{Ker} \varphi$$

such that

$$i((\alpha,\beta)) = c(\alpha,b) = h_{12}(\alpha)h_{12}(b)h_{12}(b\alpha)^{-1},$$

where $b \in D^*$ is any element of reduced norm β.

Proof: This follows from the last part of the proof of 6.8.

BIBLIOGRAPHY

1. A. Bak and U. Rehmann, The congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras, J. Algebra 78 (1982), 475-547.

2. A. Bak and U. Rehmann, K_2-analogs of Hasse's norm theorems, Comment. Math. Helv. 59 (1984), 1-11.

3. A. Bak and U. Rehmann, Remarks on the congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras, to appear.

4. H. Bass, J. Milnor, and J.-P. Serre, Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, Publ. I.H.E.S. 33 (1967), 59-137.

5. N. Bourbaki, Algèbre. Paris 1967.

6. J. E. Carroll, On the torsion in K_2 of local fields, Lecture Notes in Math. 342, Springer-Verlag, Berlin/Heidelberg/New York (1973), 464-473.

7. C. Chevalley, Sur certain groupes simples, Tôhoku Math. J. 7 (1955), 14-66.

8. V. V. Deodhar, On central extensions of rational points of algebraic groups, Amer. J. Math. 100 (1978), 303-386.

9. H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semisimple déployés, Ann. Ecole Nat. Sup. Sér. 4, 2 (1969), 1-62.

10. C. C. Moore, Group extensions of p-adic and adelic linear groups, Publ. Math. I.H.E.S. 35 (1969), 5-70.

11. J. Milnor, Introduction to algebraic K-theory, Ann. Math. Studies 72, Princeton Univ. Press, Princeton, N.J. (1971).

12. T. Nakayama and Y. Matsushima, Über die multiplikative Gruppe einer p-adischen Divisionsalgebra, Proc. Imp. Acad. Japan 19 (1943), 622-628.

13. G. Prasad and M. S. Raghunathan, Topological central extensions of semisimple groups over local fields, Annals of Math. 119 (1984), 143-201.

14. U. Rehmann, Zentrale Erweiterungen der speziellen linearen Gruppe eines Schiefkörpers, J. reine u. angew. Math. 301 (1978), 77-104.

15. U. Rehmann and U. Stuhler, On K_2 of finite dimensional division algebras over arithmetical fields, Inv. Math. 50 (1978), 75-90.

16. U. Rehmann, Die Kommutatorfaktorgruppe der Normeinsgruppe einer p-adischen Divisionsalgebra, Arch. Math. 32 (1979), 318-322.

17. I. Reiner, Maximal orders, Academic Press, New York, 1975.

18. P. Roquette, On the galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras, Math. Ann. 150 (1963), 411-439.

19. J.-P. Serre, Corps locaux, Actualités scientifiques et industrielles 1296, Hermann, Paris, 1962.

20. R. Steinberg, Générateurs, relations et revêtements de groupes algébriques, Colloq. théorie des groupes algébriques, CBRM, Bruxelles (1962), 113-127.

21. A. A. Suslin, Torsion in K_2 of fields, Lomi preprints E-2-82, USSR Acad. Sciences, Steklov Math. Institute, Leningrad Department, Leningrad (1982).