PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

CALVIN C. MOORE

Group extensions of p-adic and adelic linear groups

Publications mathématiques de l'I.H.É.S., tome 35 (1968), p. 5-70

<http://www.numdam.org/item?id=PMIHES_1968__35__5_0>

GROUP EXTENSIONS OF p-ADIC AND ADELIC LINEAR GROUPS[1]

by CALVIN C. MOORE [2]

INTRODUCTION

If G is a group and A an abelian group such that G operates on A as a group of automorphisms (i.e., A is a G-module), then one has defined cohomology groups $H^n(G, A)$, $n \geq 0$, [17]. The group $H^1(G, A)$ represents the crossed homomorphisms of G into A modulo the principal ones, or simply Hom(G, A) if G operates trivially on A [17]. If A is a G-module, an extension of G by A is an exact sequence

$$1 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1$$

of groups such that the operation of G on A by inner automorphisms of E is the given operation of G on A. (If A is a trivial G-module, we speak of central extensions of G by the abelian group A.) One knows that $H^2(G, A)$ is isomorphic to the equivalence classes of extensions of G by the module A. Addition of cocycles corresponds to the Baer product of group extensions, and the neutral element of $H^2(G, A)$ to the semi-direct product of G and A (or the direct product when A is a trivial G-module) [17].

If G and A are locally compact (separable) topological groups, and if G acts on A as a topological transformation group of automorphisms, one may modify the definitions and arrive at cohomology groups $H^n(G, A)$ which take into account the topology [30]. The group $H^1(G, A)$ consists of the classes of continuous crossed homomorphisms of G to A modulo principal ones, and $H^2(G, A)$ classifies topological extensions of G by A. In this context a topological extension is an exact sequence of topological groups

$$1 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1$$

which is an extension of G by A as abstract groups with i a homeomorphism of A onto a closed subgroup of E and such that π induces an isomorphism of topological groups $E/i(A) \simeq G$. Occasionally we shall be dealing with a topological group G, and also with the same group G, but viewed as abstract group; we denote this group by G^a.

---

(1) Research supported in part by the National Science Foundation under grant no. GP-5585.
(2) Sloan Foundation Fellow.

Then if A is a G-module, $H^n(G, A)$ and $H^n(G^a, A)$ are both defined and there are natural homomorphisms from the former to the latter. (To be perfectly precise, one should write A^a for A viewed as an abstract G^a-module, but we shall not do this as no confusion will arise.) One of the most important cases is that of the circle group **T** viewed as trivial G-module; the group $H^2(G, \mathbf{T})$ arises naturally in the study of unitary representations of groups.

The object of this paper is the study of the groups $H^2(G, A)$ where G is a semi-simple algebraic linear p-adic or adelic group (e.g. $G = SL_2(k)$ or $SL_2(A)$ where k is a locally compact non-discrete field (a local field), or where A is the ring of adeles of a number field or a function field in one variable over a finite field). If G is such a group taken over the real or complex numbers instead, and if A is a trivial G-module, one knows that $H^2(G, A) \simeq \mathrm{Hom}(\pi_1(G), A)$ where $\pi_1(G)$ is the usual fundamental group of G [37]. We shall obtain very natural generalizations of these results, valid for all locally compact fields. The structure of these cohomology groups seems to have significant arithmetic interest since their determination turns out to be equivalent to solving the congruence subgroup problem [8], [9], [10]. (See Chapter IV.) Furthermore Weil, in his memoir [41], found certain cohomology classes of order two in $H^2(G, \mathbf{T})$ where G is the symplectic group over either a local field or the adèle ring of a global field, and he found moreover an intimate relation of these cohomology classes with (among other things) the quadratic reciprocity law. We will show that the complete group $H^2(G, \mathbf{T})$ has the same intimate relation with the higher reciprocity laws of Artin.

The results are organized as follows: Chapter I deals with certain preliminaries about the cohomology of groups which will serve as a framework for the sequel. Chapter II is devoted to uniqueness theorems in local and global class field theory. The determination of the cohomology groups (in Chapter III) is in terms of usual objects of class field theory (the norm residue symbols, and the reciprocity formula) and the unicity of these objects plays a key role in the determination of these cohomology groups. Chapter III contains the main results (the statements of which do not depend on Chapter II) and Chapter IV contains a brief discussion of the connection between the above and the congruence subgroup problem.

T. Kubota has obtained independently results which overlap with ours; see [23]. We would like here to acknowledge extremely useful conversations and correspondence about this work with G. P. Hochschild, S. Lang, A. Weil, B. Wyman, J.-P. Serre and H. Bass.

Chapter I

1) This chapter is devoted to the definition and the study of the " fundamental group " of certain abstract and topological groups. For topological groups, it need not coincide with the usual fundamental group, although it does in the most important cases (e.g. semi-simple Lie groups). Our notion is defined in terms of group extensions, and has of course a very close formal similarity to the usual fundamental group.

For the present, G will denote an abstract group. We say that G is simply connected if for every central extension

$$1 \to A \to E \xrightarrow{\pi} G \to 1$$

of G by any abelian group A, there exists a *unique* homomorphism φ of G to E with $\pi \circ \varphi = \mathrm{id}$ (in particular the extension splits). The analogy with the notion of simple connectivity for, say, Lie groups should be clear.

Lemma (1.1). — *The following are equivalent :*

(1) G *is simply connected.*

(2) $H^1(G, \mathbf{T}) = H^2(G, \mathbf{T}) = 0$ *where* $\mathbf{T}$ *is the circle group.*

(3) $H^1(G, A) = H^2(G, A) = 0$ *for any trivial* G*-module* A.

Proof. — If G is simply connected, any central extension of G by $\mathbf{T}$ is trivial so $H^2(G, \mathbf{T}) = 0$. Now if $H^1(G, \mathbf{T}) \neq 0$, then the trivial extension $E = \mathbf{T} \times G$ would have more than one splitting homomorphism of G into E. Thus (2) follows from (1). If (2) holds, we note that $H^1(G, S) = H^2(G, S) = (0)$ where S is any (possibly infinite) product of copies of $\mathbf{T}$. Now if A is any trivial G-module, we can find such an exact sequence

$$0 \to A \to S \to M \to 0$$

of trivial G-modules (the homomorphisms of A into $\mathbf{T}$ separate the points of A; from this fact it also follows that $H^1(G, A) = 0$). Now since $H^1(G, M) = H^2(G, S) = 0$, the exact sequence of cohomology for the above short exact sequence shows that $H^2(G, A) = 0$ also.

Finally, if (3) holds, and E is any extension of G by A with projection π from E to G, the vanishing of $H^2(G, A)$ implies the existence of a homomorphism φ of G to E with $\pi \circ \varphi = \mathrm{id}$. Any other homomorphism φ' with this property must clearly be of the form $\varphi' = \beta \circ \varphi$ with $\beta \in H^1(G, A) = \mathrm{Hom}(G, A)$. Since this group vanishes, $\beta = 1$, and $\varphi = \varphi'$.

We notice, of course, that $H^1(G, \mathbf{T}) = 0$ is equivalent to $[G, G] = G$ where $[G, G]$ always denotes the commutator subgroup. (When one discusses covering groups in the

usual topological sense, one always imposes an assumption of connectivity; the analogue of connectivity in the present situation is precisely the condition that $G=[G, G]$.)

If $E=[E, E]$, we shall say that E covers G (or more properly that a surjective homomorphism π from E to G is a covering homomorphism) if the kernel of π is central in E. Notice then that $[G, G]=G$ necessarily. We shall prove that any group with $[G, G]=G$ has a simply connected covering group. We first note that such a covering is unique.

Lemma (**1.2**). — *If* E_i, $i=1, 2$, *are two simply connected covering groups of* G, *then* $E_1 \simeq E_2$ *as group extensions of* G.

Proof. — Let A_i be the kernel of the projection π_i from E_i to G, and let $\alpha_i \in H^2(G, A_i)$ be the class of the extension. We inflate α_1 to a class in $H^2(E_2, A_1)$ be means of the projection π_2. We then have a central extension

$$1 \to A_1 \to E_{12} \xrightarrow{p_2} E_2 \to 1$$

of E_2 by A_1. By hypothesis we can find a unique homomorphism φ of E_2 into E_{12} with $p_2 \circ \varphi = \mathrm{id}$. Since the class of the extension E_{12} is the inflation to E_2 of the class of the extension E_1 of G, there is a homomorphism β of E_{12} onto E_1 such that $\pi_1 \circ \beta = \pi_2 \circ p_2$. Now let $\psi = \beta \circ \varphi$, which is a homomorphism of E_2 into E_1; then $\pi_1 \circ \psi = \pi_1 \circ (\beta \circ \varphi) = (\pi_2 \circ p_2) \circ \varphi = \pi_2$ by the above, and so ψ is a homomorphism of group extensions. We reverse the indices and construct a homomorphism ψ' of group extensions from E_2 to E_1. Then $\psi' \circ \psi = \gamma$ is a homomorphism of group extensions from E_1 to itself. Then $\gamma(x)x^{-1}$ is an element of A_1 and since A_1 is central this is a homomorphism of E_1 into A_1 which is therefore trivial since $[E_1, E_1]=E_1$. Thus $\gamma(x)=x$. One proves similarly that $(\psi \circ \psi')(y)=y$ for $y \in E_2$. Thus E_1 and E_2 are isomorphic as group extensions.

Lemma (**1.3**). — *If* $G=[G, G]$, *then* G *has a simply connected covering group.*

Proof. — The following is one of various ways of constructing such a covering. Let L be the free abelian group generated by objects $a(x, y)$, $x, y \in G \times G$. Let R be the subgroup generated by the elements $a(st, r)a(s, t)a(s, tr)^{-1}a(t, r)^{-1}$ and $a(1, s)$ and $a(s, 1)$ for all $s, t, r \in G$. Put $B_0 = L/R$, and let $\beta(s, t)$ be the image of $a(s, t)$ in this quotient group. Then it is absolutely clear that β as a function from $G \times G$ to B_0 is a two-cocycle of G with values in the trivial G-module B_0. Let E_0 be the group extension of G by B_0 defined by β; $E_0 = B_0 \times G$ as set and $(a, g)(b, h) = (ab\beta(g, h), gh)$ is the multiplication [17].

Now suppose that F is any central extension of G by an abelian group D. We choose a normalized cocycle γ representing this extension and view F as $D \times G$ with the multiplication defined just as above. Consider now the mapping ψ_1 from L to D given by $\psi_1(a(s, t)) = \gamma(s, t)$ on the generators. It is clear from the fact that γ is a normalized cocycle that $\psi_1(R)=(1)$, and hence ψ_1 defines a homomorphism ψ_0 of B_0 into D with $\psi_0(\beta(s, t)) = \gamma(s, t)$. In view of the definition of the group law in E_0 and F,

one sees that ψ_0 extends to a homomorphism of group extensions, again denoted by ψ_0, of E_0 into F. Thus E_0 has the first part of the universal property required for simple connectivity.

Now let $E=[E_0, E_0]$ be the commutator subgroup of E_0. Since $G=[G, G]$, the projection of E onto G is all of G so that E is a group extension of G

$$1 \to B \to E \to G \to 1$$

where $B=B_0 \cap E$. Now $E=B.E_0$ with B central so that $[E, E]=[E_0, E_0]=E_0$, and thus $H^1(E, \mathbf{T})=(0)$. If F is any central extension of G by D, we saw that there exists a homomorphism ψ_0 of group extensions of E_0 into F. Thus ψ, the restriction of ψ_0 to E, is also a homomorphism of group extensions. In terms of cohomology, this says exactly that the inflation homomorphism $H^2(G, D) \to H^2(E, D)$ is the zero map for every trivial G-module D.

We contend now that E is simply connected, and to do this, it suffices to show that $H^2(E, \mathbf{T})=0$. In view of the spectral sequence for the group extension E of G by B [21], it suffices to show first that the E_2^{11} term, $H^1(G, H^1(B, \mathbf{T}))$, is zero. But this group is zero since $H^1(B, \mathbf{T})$ is a trivial G-module and $G=[G, G]$. Then one must finally show that the restriction homomorphism $r : H^2(E, \mathbf{T}) \to H^2(B, \mathbf{T})$ is the zero map. This is contained in the following lemma.

Lemma (**1.4**). — *If* $E=[E, E]$ *and* B *is any central subgroup, then the restriction homomorphism* $H^2(E, \mathbf{T}) \to H^2(B, \mathbf{T})$ *is the zero map.*

Proof. — Let $\alpha \in H^2(E, \mathbf{T})$ and F be the corresponding extension of E by **T**. If $s \in G$ and $t \in B$, let s' and t' be representatives of s and t in F. Then the commutator $[s', t']$ depends only on s and t, and we denote it by $\varphi(s, t)$. We note that φ is a bilinear map from $E \times B$ into **T**, and since $E=[E, E]$, $\varphi(s, t)=1$.

Now let F′ be the inverse image of B in F. Then F′ is an extension of B by **T**. It is a corollary of the previous paragraph that F′ is an abelian group. Since **T** is divisible, this extension splits, and this says that the restriction of α to B is the trivial class as desired.

Thus we have shown that if $G=[G, G]$ we have a central extension

$$1 \to B \to E \to G \to 1$$

with E simply connected. Moreover we have seen that such an extension is unique up to isomorphism of group extensions, and so the abelian group B is determined uniquely. It is quite reasonable to call B the fundamental group of G, and to denote it by $\pi_1(G)$. Recall that a central extension F of G is a covering group of G if $[F, F]=F$; we shall call the extension E constructed above the universal covering of G.

Lemma (**1.5**). — *Let* F *be a covering group of* G. *Then the following are equivalent*:

(1) F *is the universal covering of* G.

(2) *inflation*: $H^2(G, A) \to H^2(F, A)$ *is the zero map for every trivial* G*-module* A.

(3) *inflation*: $H^2(G, \mathbf{T}) \to H^2(F, \mathbf{T})$ *is the zero map.*

Proof. — (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are clear from the definition. Finally 3 $\Rightarrow$ 1 follows from Lemma (1.4) and the remarks immediately preceding it.

The following shows that the universal covering is universal.

Lemma **(1.6).** — *If* F *is any covering group of* G, *then* F *is covered by the universal covering group* E *of* G *and so the universal covering group of* F *coincides with that of* G.

Proof. — By exactly the same argument as in Lemma (1.2) we may produce a homomorphism ψ of group extensions (of G) of E into F. Let $F' \subset F$ denote the range of ψ. Then F' is clearly a covering group of G. If $A \subset F$ is the kernel of the projection of F onto G, it follows that $F = A.F'$. Then as A is central, $[F, F] = [F', F'] = F'$, but $[F, F] = F$ since F is a covering group of G. Thus $F = F'$ and we are done.

We note that if $[G, G] = G$, the groups which G covers are exactly the groups G/D where D is a central subgroup of G. The following fact shows that there is a smallest group covered by G.

Corollary. — *If* $G = [G, G]$ *and* Z *is the center of* G, *then* G/Z *is centerless and covers only itself.*

Proof. — If Z'/Z is the center of G/Z, then G/Z covers G/Z', but by the lemma the universal covering of G/Z covers G/Z' and this says that Z' is central in G and hence that $Z' = Z$ as desired.

Let $G_i = [G_i, G_i]$, $i = 1, 2$, and let φ be a homomorphism of G_1 into G_2. If E_i is the universal covering of G_i, then the universal property of E_1 yields a homomorphism φ' of E_1 into E_2 compatible with φ. Then the restriction of φ' to $\pi_1(G_1) \subset E_1$ is a homomorphism φ_* of $\pi_1(G_1)$ into $\pi_2(G_2)$. It is clear that the assignment of $\pi_1(G)$ to G together with the induced maps φ_* is a covariant functor. If F is a covering group of G, then we have an induced homomorphism $\pi_1(F) \to \pi_1(G)$. Lemma (1.6) says that this homomorphism is injective.

Now if $G = [G, G]$, let E be the universal covering, and let $\pi_1(G)$ be the fundamental group. If A is any trivial G-module, the restriction-inflation sequence [21] yields, in view of the fact that $H^1(E, A) = H^2(E, A) = 0$, the following:

$$0 \to H^1(\pi_2(G), A) \xrightarrow{t} H^2(G, A) \to 0.$$

Here t is the transgression map [21]. Notice that $H^1(\pi_1(G), A) = \mathrm{Hom}(\pi_1(G), A)$.

Theorem **(1.1).** — *The transgression homomorphism is an isomorphism*:

$$\mathrm{Hom}(\pi_1(G), A) \simeq H^2(G, A)$$

for any trivial G*-module* A.

We want to note here an alternate construction for $\pi_1(G)$. Observe that the cochain complex $C^*(G, \mathbf{T})$ consists of compact topological groups with the topology of pointwise convergence. Moreover the differential d is continuous, and it follows that $H^n(G, \mathbf{T})$ becomes in a natural way a compact group. Now if $G = [G, G]$, a special case of Theorem (1.1) says that $H^2(G, \mathbf{T}) \simeq \mathrm{Hom}(\pi_1(G), \mathbf{T})$. We view $\pi_1(G)$ as a

discrete group so that then $H^2(G, \mathbf{T})$, viewed as the dual group, inherits a natural compact topology.

Theorem (**1.2**). — *The topology on* $H^2(G, \mathbf{T})$ *induced by pointwise convergence of cochains coincides with the topology of* $H^2(G, \mathbf{T})$ *viewed as the dual group of* $\pi_1(G)$.

Proof. — This is essentially implicit in [31]; the map from $\mathrm{Hom}(\pi_1(G), \mathbf{T})$ into $H^2(G, \mathbf{T})$ with the topology of convergence of cochains is clearly continuous, hence bicontinuous.

We shall be using this compact topology on $H^2(G, \mathbf{T})$ in the sequel. We note that if φ is a homomorphism $G \to H$, the induced map $\varphi^* : H^2(H, \mathbf{T}) \to H^2(G, \mathbf{T})$ is continuous as is clear from the definition of the topology.

If G is a finite group, the existence and some of the properties of its universal covering are well known from the work of Schur [35] in 1904.

We shall conclude this section with some facts about what one might call relative fundamental groups. Let $G = [G, G]$, and let $K = [K, K]$ be a subgroup, and denote by i the injection of K into G. Then we have a homomorphism i_* of $\pi_1(K)$ into $\pi_1(G)$. Let D be its range and let $\pi_1(G, K)$ denote the quotient group $\pi_1(G)/D$. Now if E is the universal covering of G, D is a central subgroup of E, and so $E_0 = E/D$ is a central extension of G by $\pi_1(G, K)$. Let us note that we have restriction maps $i^* : H^2(G, A) \to H^2(K, A)$ for any trivial G-module A. It is absolutely clear that the kernel of i^* in $H^2(G, \mathbf{T})$ is exactly the annihilator of the subgroup D of $\pi_1(G)$ where of course we view $H^2(G, \mathbf{T})$ as the dual group of $\pi_1(G)$.

Lemma (**1.7**). — *Let* α_0 *denote the class in* $H^2(G, \pi_1(G, K))$ *of the extension* E_0. *Then* $i^*(\alpha_0)$, *the restriction of* α_0 *to* K *is the trivial class.*

Proof. — By Theorem (1.1), $i^*(\alpha_0)$ corresponds to a homomorphism of $\pi_1(K)$ into $\pi_1(G, K)$. Also α_0 corresponds to a homomorphism of $\pi_1(G)$ into $\pi_1(G, K)$, which is, by definition of E_0, just the projection λ of $\pi_1(G)$ into $\pi_1(G, K)$. Then by the theory above, $i^*(\alpha_0)$ is represented by the homomorphism $\lambda \circ i_*$ which is zero by construction; hence $i^*(\alpha_0) = 0$.

In view of this lemma, there is a homomorphism i_0 of K into E_0 such that $\varphi_0 \circ i_0 = i$ where φ_0 is the natural projection of E_0 onto G. Moreover i_0 is unique subject to these conditions since $K = [K, K]$. We show that i_0 is universal in the following sense.

Theorem (**1.3**). — *Let* E_1 *be any central extension of* G *by an abelian group* A *with projection map* φ_1 *of* E_1 *onto* G. *Suppose that there is a homomorphism* i_1 *of* K *into* E_1 *such that* $\varphi_1 \circ i_1 = i$. *Then there exists a unique homomorphism* j *of* E_0 *into* E_1 *such that* $\varphi_1 \circ j = \varphi_0$. *Moreover* $j \circ i_0 = i_1$ *so that* j " *extends* " i_1.

Proof. — If E is the universal covering of G, there is a homomorphism of group extensions j' of E into E_1. If we can show that $j'(D) = 0$ where $E_0 = E/D$, then j' determines a homomorphism of group extensions of E_0 into E_1 which clearly satisfies our requirements. Moreover j is unique since $G = [G, G]$.

Now the class of the extension E_1 of G by A corresponds to a homomorphism λ of $\pi_1(G)$ into A which is clearly the restriction of j' to $\pi_1(G)$. But the restriction of the class of this extension to K, $i^*(\lambda)$, is trivial by hypothesis. On the other hand, $i^*(\lambda)$ corresponds to a homomorphism of $\pi_1(K)$ into A which is clearly exactly $\lambda \circ i_*$. Thus $\lambda \circ i_* = 0$, and this says that λ (and hence j') vanishes on D as desired.

Thus one may think of E_0 as being simply connected relative to its subgroup $i_0(K)$, and one could in fact formulate the above theorem in terms of central extensions of E_0 (instead of G) splitting on $i_0(K)$. We note that the topological analogue of the relative fundamental group $\pi_1(G, K)$ is just the topological fundamental group of the homogeneous space G/K, as can be seen from the exact homotopy sequence of a fibration [38].

We conclude with the following fact which is obvious by now.

Lemma (**1.9**). — *If* A *is any trivial* G*-module, the kernel of the restriction homomorphism* $i^* : H^2(G, A) \to H^2(K, A)$ *is isomorphic to* $\mathrm{Hom}(\pi_1(G, K), A)$ *viewed as a subgroup of* $\mathrm{Hom}(\pi_1(G), A) \simeq H^2(G, A)$.

In conclusion one might raise the rather natural question of whether these isomorphisms (say with $K = (e)$) $H^2(G, A) \simeq \mathrm{Hom}(\pi_1(G), A)$ are special cases of isomorphisms in all dimensions. We do not think that this is the case, but rather that it is more fruitful to think of these maps as analogues of the Hurewicz isomorphisms [38]. There one assumes vanishing of the first $n-1$ groups and obtains results about the n^{th} group. Here we assume vanishing of H^1 and obtain results about H^2. One may carry this further and show that if $H^1(G, A) = H^2(G, A)$ for all trivial G-modules A, then one obtains structural results similar to those here for $H^3(G, A)$, and so on in higher dimensions.

2) In this section we shall carry out the slight modifications of the above in order to make it apply to topological extensions. Let G be a locally compact separable group, and A a locally compact separable topological G-module. We have cohomology groups $H^n(G, A)$ defined (see above); at times we shall have to view G as abstract group, and we denote this group by G^a. The cohomology groups of G^a in A will be denoted by $H^n(G^a, A)$.

We say that G is simply connected if for every central topological extension

$$1 \to A \to E \xrightarrow{\pi} G \to 1$$

with A locally compact separable, there is a unique continuous homomorphism φ of G into E such that $\pi \circ \varphi = \mathrm{id}$. We can characterize simply connected groups as in Lemma (1.1), but the results are not quite as sharp.

Lemma (**2.1**). — G *is simply connected if and only if* $H^1(G, \mathbf{T}) = H^2(G, \mathbf{T}) = 0$ *where* **T** *is the circle group, and* $H^2(G, A) = 0$ *for any discrete abelian group.*

Proof. — It is clear just as in section 1 that G is simply connected if and only if $H^1(G, B) = H^2(G, B) = (0)$ for all trivial G-modules B. However the vanishing of $H^1(G, B)$ follows from the vanishing of $H^1(G, \mathbf{T})$ by duality theory. Now suppose that $H^2(G, \mathbf{T}) = 0$; then if S is any group which is a countable (or finite) product of

copies of **T** we clearly have $H^2(G, S)=0$. If B is any (separable) compact group viewed as trivial G-module, we can find an exact sequence

$$(*) \qquad 0\to B\to S\to S/B\to 0$$

with S as above. Since $H^1(G, S/B)=H^2(G, S)=(0)$, it follows from the exact cohomology sequence of (*) that $H^2(G, B)=(0)$.

Finally we suppose in addition that $H^2(G, D)=0$ for any discrete group D. Now if A is any trivial G-module, we can find an open subgroup B of A and a discrete subgroup D of B such that B/D is compact [29]. Then by hypothesis, $H^2(G, D)=H^2(G, A/B)=0$, and we have shown that $H^2(G, B/D)=0$. Then it follows from exact sequences of cohomology that $H^2(G, A)=0$.

Remark. — The final condition in the lemma above is annoying; we can show that it is implied by the first two conditions (hence giving an exact analogue of Lemma (1.1)) in a large number of special cases. However we know neither a proof nor counterexample in general.

If E is a central extension of G by A, we say that E covers G if [E, E] is dense in E. Note that the condition $H^1(E, \mathbf{T})=0$ of Lemma (2.1) is equivalent to the density of [E, E] in E.

Lemma **(2.2).** — *If* G *is locally compact (separable), then* G *has at most one simply connected covering group up to isomorphism of topological group extensions.*

Proof. — The argument of Lemma (1.2) applies without change.

It is perhaps possible that we have too weak a notion of covering group. One could instead of the density of [E, E] in E, demand that [E, E]=E. Lemma (2.2) remains true (of course) and moreover it is then true that a simply connected covering group of G (if it exists) covers any other covering of G. This statement is easily seen to be false with our present definition. However Lemma (2.3) (below) is true with the weaker definition.

In view of Lemma (2.2), one has at most one extension

$$1\to A\to E\to G\to 1$$

with E simply connected. Keeping in mind section 1, we should call A the fundamental group of G, and denote it by $\pi_1(G)$ whenever it exists. Note that $\pi_1(G)$ is now a topological group. Whenever E exists, $\pi_1(G)$ describes central extensions just as it should.

Lemma **(2.3).** — *If* $\pi_1(G)$ *exists, then* $H^2(G, A)\simeq \mathrm{Hom}(\pi_1(G), A)$ *for any locally compact (separable) trivial* G*-module* A. *(The " Hom " in this equation indicates of course continuous homomorphisms.)*

Proof. — This follows by the same argument as in Theorem (1.1). (See [30] for the restriction-inflation sequence in this context.)

We note that if a simply connected covering E of G exists, then E is a splitting group for G in the sense of [31]. Moreover the topology which $H^2(G, \mathbf{T})$ inherits as

the dual group of $\pi_1(G)$ by the above lemma is exactly the splitting group topology which is discussed at length in [31].

We have not yet treated any existence questions. The following two theorems concern this, but the hypotheses are of such a nature that they are never satisfied (except in cases where the results are essentially known) for the groups of interest to us in this paper. (Existence of $\pi_1(G)$ for groups of interest are corollaries of the main theorems in later sections.) Moreover the arguments are rather tedious and take us far afield and more properly belong in a forthcoming paper devoted to this and related questions. We mention them here with only a bare sketch of proof to indicate that the definitions above are not vacuous.

Theorem **(2.1).** — *If* G *is almost connected,* i.e. G/G_0 (G_0 *being the connected component*) *is compact, and if* $G=[G, G]$, *then* G *has a simply connected covering group.*

Theorem **(2.2).** — *If* G *is a connected Lie group with* $[G, G]=G$, *then* G *has a simply connected covering group* E *with* $[E, E]=E$. *Moreover* E *is a connected Lie group, and* $\pi_1(G)$ *is the direct sum of the usual fundamental group of* G, *and the dual vector space to* $H^2(\mathfrak{g}, \mathbf{R})$ *where* $\mathfrak{g}$ *is the Lie algebra of* G *and the group above is Lie algebra cohomology with coefficients in the trivial one dimensional* $\mathfrak{g}$*-module* **R**.

We remark in these theorems, the hypothesis that $[G, G]=G$ (not just that it is dense in G) is crucial. There are easy counterexamples if [G, G] is only dense. We note in Theorem 2 that if $H^2(\mathfrak{g}, \mathbf{R})=0$ (in particular if G is semi-simple) then $\pi_1(G)$ is the usual fundamental group. Moreover the extension described in Theorem (2.2), E, is exactly the ordinary topological universal covering group, as is implicit in the statement of Theorem (2.2). That this is the case for semi-simple groups was proved by A. Shapiro [37].

We sketch the idea of Theorem (2.1). By [31], we know that G has a splitting group E'; that is, a central extension of G by some A such that the transgression homomorphism: $H^1(A, \mathbf{T}) \to H^2(G, \mathbf{T})$ is surjective. Now we let E be the closure of the commutator group of E'. Then E covers G since $G=[G, G]$. (This is the point at which the argument fails if [G, G] is only dense in G.) One then proves that E is simply connected. The fact that $H^1(E, \mathbf{T})=H^2(E, \mathbf{T})=(0)$ follows just as in Lemma (1.3). The tedious part is to show that $H^2(G, D)=(0)$ for any discrete group. Let us note that Lemma (1.4) is valid for topological groups.

Lemma **(2.4).** — *If* G *is locally compact separable and* [G, G] *is dense in* G, *and if* Z *is a closed central subgroup, the restriction map:* $H^2(G, \mathbf{T}) \to H^2(Z, \mathbf{T})$ *is the zero map.*

Proof. — The argument in Lemma (1.4) applies directly if we note that a central extension (Z abelian)

$$1 \to \mathbf{T} \to E \to Z \to 1$$

splits if and only if E is abelian (as is evident by Pontrjagin duality), and if we note that the commutator function constructed in (1.4) is continuous in its arguments.

The above results suggest perhaps that one should assume that for this development that [G, G] is all of G and not just dense. In the following we want to compare the topological cohomology $H^2(G, A)$ with the cohomology $H^2(G^a, A)$ of G viewed as an abstract group. We noted before that we have natural homomorphisms of $H^n(G, A)$ into $H^n(G^a, A)$ for every n.

Theorem (**2.3**). — *If* $G=[G, G]$, *the natural map* i^a *of* $H^2(G, A)$ *into* $H^2(G^a, A)$ *is injective.*

Proof. — This assertion is equivalent to the (somewhat amazing) fact that if

$$1 \to A \to E \xrightarrow{\pi} G \to 1$$

is a topological extension of G by A which splits as extension of abstract groups, then it splits as extension of topological groups. In fact we shall show that if φ is a splitting homomorphism of G into E (i.e. $\pi\circ\varphi=\mathrm{id}$), then φ is necessarily continuous, and that $E=A\times G$ as topological groups.

If such a φ exists, $E=A\times G'$ as abstract groups where $G'=\varphi(G)$. Since A is central and $G=[G, G]$, it is clear that G' is the commutator subgroup [E, E] of E. Now we claim that $G'=[E, E]$ is a Borel subset of E. In fact, if K_n is a sequence of compact sets exhausting G, then for each n, $L_n=\{k_1k_2k_1^{-1}k_2^{-1}, k_i\in K_n\}$ is compact and so the group E_n generated by L_n is a Borel set (an F_σ in fact). Clearly $G'=\bigcup_n E_n$ and so G' is a Borel subset, and in particular G' is a standard Borel space [26]. We consider the map h of $G'\times A$ into E given by $h(a, g')=ag'$; it is clear that h is a bijective Borel map of $G'\times A$ onto E. We deduce from Souslin's theorem ([26] or [6]) that h is a Borel isomorphism, and hence that the quotient Borel space E/G' is a standard Borel space (Borel isomorphic to A). It follows by [26], Theorem (7.2), that G' is in fact a closed subgroup, and hence locally compact. Thus $A\times G'$ is locally compact and $h : A\times G'\simeq E$ is continuous, so by [7], p. 25, h is a homeomorphism. That is, the extension E of G by A splits as topological extension.

We conclude this section with some remarks on the relative fundamental groups for topological groups. Let G and K be locally compact (separable) groups and let i be a continuous injection of K into G. We are not assuming that i is a homeomorphism onto $i(K)$ (equivalently that $i(K)$ is closed); in fact there will be applications when $i(K)$ is dense in G. Suppose that G and K have simply connected covering groups E_G and E_K, and let $\pi_1(G)$ and $\pi_1(K)$ be the fundamental groups. Then as we have noticed, i induces a continuous homomorphism i_* of $\pi_1(K)$ into $\pi_1(G)$. (This is the dual map to the restriction homomorphism $i^* : H^2(G, \mathbf{T}) \to H^2(K, \mathbf{T})$). Let D be the closure of the range of i_*; then D is also the annihilator, from duality, of the kernel of i_*. We form the group $E_0=E_G/D$ viewed as a group extension of G by $\pi_1(G)/D$, both groups with the quotient topology. Let φ and φ_0 respectively denote the homomorphisms of E and E_0 onto G. We denote $\pi_1(G)/D$ by $\pi_1(G, K)$, the relative fundamental group. (In all of our applications, the range of i_* will be closed so $D=i_*(\pi_1(K))$.)

Lemma (**2.7**). — *There is a unique continuous homomorphism* i_0 *of* K *into* E_0 *such that* $\varphi_0 \circ i_0 = i$.

Proof. — The uniqueness is clear since $H^1(K, \mathbf{T}) = (0)$. (K has a simply connected covering group.) For existence, one must show as in Lemma (1.7) that if $\alpha_0 \in H^2(G, \pi_1(G, K))$ is the class of E_0, then $i^*(\alpha_0)$, its restriction to K is trivial. This follows by the same argument as in Lemma (1.7).

Theorem (**2.4**). — (E_0, i_0) *is universal in the sense that if* E_1 *is any central extension of* G *by* A, *with projection* φ_1 *of* E_1 *onto* G, *such that there exists a continuous homomorphism* i_1 *of* K *into* E_1 *with* $\varphi_1 \circ i_1 = i$, *then there exists a unique (continuous) homomorphism j of group extensions of* E_0 *into* E_1. *Moreover we have* $j \circ i_0 = i_1$ *automatically so that j " extends " i*$_1$.

Proof. — The argument is identical with that in Theorem (1.3).

Finally the analogue of Lemma (1.9) comes over without change except that continuous homomorphisms are used instead of arbitrary ones.

Lemma (**2.8**). — *If* A *is any trivial (topological)* G*-module, then the kernel of the restriction map* $i^* : H^2(G, A) \to H^2(K, A)$ *is isomorphic to* $\mathrm{Hom}(\pi_1(G, K), A)$ *viewed as a subgroup of* $\mathrm{Hom}(\pi_1(G), A) \simeq H^2(G, A)$.

Chapter II

3) As we have indicated above, this chapter is devoted to certain uniqueness theorems in class field theory, which will be crucial in the following Chapter. These results say that the familiar objects of class field theory (the norm residue symbols and the reciprocity formula) are the only such objects satisfying appropriate axioms.

We shall begin with the local case; thus let k be a locally compact non-discrete field so that k is either a finite algebraic extension of $\mathbf{Q}_p$ the p-adic field, or is a field of formal power series over a finite field of constants (the non-Archimedian cases), or k is the real or complex field (the Archimedian case). We shall denote the multiplicative group $k-(0)$ by k^*. Let E_k be the group of roots of unity in k; then if $k \neq \mathbf{C}$, E_k is a finite group and hence cyclic of some order n_k ($=n$ if there is confusion about k).

The norm residue symbol $(\ ,\ )$ of local class field theory ([3], [33]), is a mapping $k^* \times k^* \to E_k$ such that

(1)′ $(\ ,\ )$ is bilinear.

(2)′ $(s, t)=(t, s)^{-1}$.

(3)′ $(s, t)=(s, -st)$.

(4)′ $(s, t)=(s, (1-s)t)$ if $s \neq 1$.

(5)′ $(\ ,\ )$ is continuous from $k^* \times k^*$ into E_k.

This function of course has many other properties, but the ones above (or rather weakenings of the ones described below) are the ones of interest to us. A corollary of our main theorem is that the norm residue symbol and its powers are the only functions satisfying (1)′-(5)′.

The weakening of these conditions which is of interest to us seems perhaps artificial without the motivation which is supplied by the following Chapter.

Definition **(3.1).** — *Let* A *be a locally compact separable abelian group and let* S(A) *denote the set of all functions* b *from* $k^* \times k^*$ *to* A *satisfying*

(1) $b(s, tr)b(t, r)=b(st, r)b(s, t)$, $b(1, s)=b(s, 1)=1$.

(2) $b(s, t)=b(t^{-1}, s)$.

(3) $b(s, t)=b(s, -st)$.

(4) $b(s, t)=b(s, (1-s)t)$ $s \neq 1$.

(5) b *is continuous.*

We shall call such functions *Steinberg cocycles.* If k is any field and A is any abelian group, then (1)-(4) above make sense. We shall call the group of such functions $S_k(A)$. (Note that (1) and (5) say that $b \in Z^2(k^*, A)$.) Our main theorem

in the local case describes the group S(A) completely. To be precise, let us define a subgroup $S_0(A)$ of S(A) as follows. If k is non-Archimedian, let $S_0(A)$ be the set of all functions from $k^*\times k^*$ into A of the form $b(s,t)=f((s,t))$ where $f\in\mathrm{Hom}(E_k, A)$, and $(\ ,\ )$ is the norm residue symbol. Since the range of $(\ ,\ )$ generates E_k, $S_0(A)\simeq\mathrm{Hom}(E_k, A)$. If $k=\mathbf{R}$, define a function b_0 from $k^*\times k^*$ to $\mathbf{Z}$ (the integers) by $b_0(s,t)=0$ unless s and t are both negative, and then $b_0(s,t)=1$. It may then be verified that $b_0\in S(\mathbf{Z})$. Then let $S_0(A)=\{b \mid b=f\circ b_0$ with $f\in\mathrm{Hom}(\mathbf{Z}, A)\}$. Notice that if $A=Z_2$, the integers mod 2 and f_2 is the natural projection of $\mathbf{Z}$ onto Z_2, then $f_2\circ b_0$ is the norm residue symbol for $\mathbf{R}$. Finally if $k=\mathbf{C}$, let $S_0(A)=(0)=\mathrm{Hom}((0), A)$.

Theorem (3.1). — *For all* k, $S_0(A)=S(A)$.

The remainder of our discussion for local fields (the next four sections) will be devoted to proving this fact. We note that $S_0(A)$ is of the form $\mathrm{Hom}(B_k, A)$ for some group B_k. The whole point of this is that in Chapter III we shall show that S(A) is isomorphic to $H^2(SL_2(k), A)$ where $SL_2(k)$ is the locally compact group of 2×2 unimodular matrices over k and A is viewed as a trivial module. Thus by Chapter I, we may identify B_k with the fundamental group $\pi_1(SL_2(k))$, so if k is non-Archimedian, $\pi_1(SL_2(k))=E_k$, whereas if k is real $\pi_1(SL_2(\mathbf{R}))=\mathbf{Z}$, and if k is complex $\pi_1(SL_2(\mathbf{C}))=0$; the latter two facts of course coincide with classical results. We shall investigate other matrix groups (the simply connected Chevalley groups), but the results are not yet complete in the general case. The results of [10] supply the complete answer for groups of type A_n and C_n.

We shall begin by drawing some consequences of (1)-(4) of the definition of S(A) (Definition (3.1)). In fact if k is an arbitrary field and A an abelian group, we consider the group $S_k(A)$. It should always be borne in mind that if b satisfies (1) of (3.1), then b defines a central extension of k^* by A

$$1\to A\to E\to k^*\to 1.$$

If $u, v\in k^*$, then let $\dot{u}$ and $\dot{v}$ be representatives for u and v in E. Then the commutator $[\dot{u}, \dot{v}]$ depends only on u and v and is denoted by $[u, v]$.

Lemma (3.1). — *If* b *is any cocycle defining the extension* E *above, then* $[u, v]=b(u, v)b(v, u)^{-1}$ *is a bilinear function of* u *and* v.

Proof. — It is clear that $[u, v]$ is a bilinear function of u and v (cf. Lemma (1.4)), and one may compute that it is given by the formula of the lemma.

The following will be crucial for us.

Lemma (3.2). — *If* $b\in S_k(A)$, *then,*

$$[t, s]=b(t, s)b(s, t)^{-1}=b(t^2, s)=b(s^2, t)^{-1}$$

is a bilinear function of s *and* t.

Proof. — We begin by observing that the identity

$$b(t^{-1}, t^2)b(t, s)b(t^{-1}, s)=b(t^{-1}, t^2 s)b(t^2, s)b(t^{-1}, s)$$

is (1) (the cocycle identity) multiplied by $b(t^{-1}, s)$. Now from (3) it follows that $b(t^{-1}, t^2)b(t^{-1}, s) = b(t^{-1}, t^2 s)$ and upon substitution of this into the above, we find that $b(t, s) = b(t^2, s)b(t^{-1}, s)$. Since $b(t^{-1}, s) = b(s, t)$ follows from (2), we see that $b(t^2, s) = b(t, s)b(s, t)^{-1}$ which is the first of our identities. The second follows by interchanging s and t.

Some other consequences of (1)-(4) are listed in the appendix but we shall not need them now. We also note that there is some redundancy in Definition (3.1). Namely if we assume (1) and (4), then (2) and (3) are equivalent to each other. We also note that if a function b is bilinear (as the most important examples are) then (1)-(4) can be replaced by a single identity, namely $b(s, (1-s)t)b(t, s) = 1$.

Our next result reduces Theorem (3.1) to the case of a single coefficient group. Remember that we are dealing with a fixed locally compact non-discrete field.

Lemma **(3.3).** — *If* $S_0(\mathbf{T}) = S(\mathbf{T})$, *then Theorem* (3.1) *follows*, i.e. $S_0(A) = S(A)$ *for any locally compact separable abelian group* A.

Proof. — Suppose that $b \in S(A)$; then if $\lambda \in \mathrm{Hom}(A, \mathbf{T})$ $(= \hat{A}$, the dual group of A) then $\lambda \circ b$, the composition of λ and b is clearly in $S(\mathbf{T}) = S_0(\mathbf{T})$. By definition $S_0(\mathbf{T}) \simeq \mathrm{Hom}(B, \mathbf{T})$ where B is a discrete (cyclic) group, finite or infinite. We have a distinguished element b_0 in $S_0(B)$ (the norm residue symbol if k is non-Archimedian, and as defined above for $k = \mathbf{R}$ or $\mathbf{C}$) such that $\gamma \to \gamma \circ b$ is this isomorphism of $S_0(A)$ with $\mathrm{Hom}(B, A)$. If $A = \mathbf{T}$, we give $S_0(\mathbf{T})$ the topology of pointwise convergence and observe that this is the same (compact) topology as that defined by $S_0(\mathbf{T}) \simeq \mathrm{Hom}(B, \mathbf{T}) = \hat{B}$, the dual group of $\hat{B}$. It is clear now that $\lambda \to \lambda \circ b$ is a continuous map from $\mathrm{Hom}(A, \mathbf{T}) = \hat{A}$ into $S_0(\mathbf{T}) \simeq \hat{B}$. Then we have a dual map φ, which is a continuous homomorphism of B into A. It is now clear from the definitions that $\lambda \circ b = \lambda(\varphi(b_0))$ for every $\lambda \in \hat{A}$. Since the elements of $\hat{A}$ separate the points of A, we must have $b = \boldsymbol{\varphi} \circ b_0$, and so $b \in S_0(A)$ by definition. This completes the proof.

We shall now conclude this section by disposing of Theorem (3.1) in the Archimedian case.

Theorem **(3.2).** — *If* k *is real or complex, then* $S_0(A) = S(A)$.

Proof. — By Lemma (3.3), it suffices to show that $S_0(\mathbf{T}) = S(\mathbf{T})$; or in other words, by definition it suffices to show that $S(\mathbf{T}) = (0)$ if $k = \mathbf{C}$, and that $S(\mathbf{T}) = \{\lambda \circ b_0; \lambda \in \mathrm{Hom}(\mathbf{Z}, \mathbf{T})\}$ where $b_0(s, t) = 0$ if either s or $t > 0$ and 1 otherwise if $k = \mathbf{R}$. The first step is to compute $H^2(k^*, \mathbf{T})$, the topological cohomology of k^* with coefficients in $\mathbf{T}$.

Lemma **(3.4).** — *If* k *is Archimedian,* $H^2(k^*, \mathbf{T}) = 0$.

Proof. — In both cases, k^* is the direct product $\mathbf{R} \times L$ where $\mathbf{R}$ is the additive reals and L is cyclic of order two or the circle group $\mathbf{T}$, respectively, in the two cases. One deduces from spectral sequences [30] or more directly if desired that

$$H^2(k^*, \mathbf{T}) \simeq H^2(\mathbf{R}, \mathbf{T}) \oplus H^1(\mathbf{R}, \mathrm{Hom}(L, \mathbf{T})) \oplus H^2(L, \mathbf{T}).$$

It is well known that $H^2(\mathbf{R}, \mathbf{T})=(0)$, and since $\mathrm{Hom}(L, \mathbf{T})=\hat{L}$ is discrete, and $\mathbf{R}$ is connected, $H^1(\mathbf{R}, \mathrm{Hom}(L, \mathbf{T}))=\mathrm{Hom}(\mathbf{R}, \hat{L})=(0)$. Finally it is also well known that $H^2(\mathbf{T}, \mathbf{T})=(0)$ and that $H^2(A, \mathbf{T})=(0)$ for any cyclic group A. Thus $H^2(k^*, \mathbf{T})=(0)$ as desired.

Now since any element of $S(\mathbf{T})$ represents an element of $H^2(k^*, \mathbf{T})$ we find that any b in $S(\mathbf{T})$ is a trivial cocycle. However we have observed in Lemma (2.4) that b is trivial if and only if it is symmetric. Thus $b(s, t)=b(t, s)$ and by Lemma (3.2), $b(s^2, t)=b(t, s^2)=1$ for any s and t. The following fact will be useful for us in the sequel.

Lemma **(3.5).** — *If* $b\in Z^2(B, A)$ *where* B *and* A *are abelian, and if* $b(s, t)=1$ *for* $s\in D$ *and* $t\in B$ *where* D *is some subgroup of* B, *then* $b(ds, t)=b(s, t)$ *for* $d\in D$ *and* $s, t\in B$. *Similarly, if* $b(s, t)=1$ *for all* $t\in D$, $b(s, td)=b(s, t)$ *if* $d\in D$.

Proof. — By the cocycle identity (1) of Definition (3.1), $b(ds, t)b(d, s)=b(d, st)b(s, t)$ and since the second and third terms are equal to 1 if $d\in D$, the result follows. The result for $b(s, td)$ follows similarly.

We combine this result with Lemma (3.4); take $B=k^*$, $A=\mathbf{T}$ with $D=(k^*)^2$ the group of squares in k^*. We find then that $b(s, t)$ depends on s and t only modulo squares. If $k=\mathbf{C}$, then $(k^*)^2=k^*$ so that $b(s, t)=b(1, 1)=1$ for all s and t as desired. If $k=\mathbf{R}$, then $b(s, t)$ depends only on the signs of s and t and this is clearly equivalent to the desired result (i.e. that $b(s, t)=1$ if either s or t is positive and $b(s, t)$ is some constant in $\mathbf{T}$ if s and t are both negative).

4) We now turn to the case of non-Archimedian fields k, where the situation is somewhat more subtle. Let $\mathfrak{O}$ be the ring of integers in k and let U be the group of units in $\mathfrak{O}$. Let π be a fixed generator of $\mathfrak{p}$, the maximal ideal of $\mathfrak{O}$. Then $k^*\simeq U\times\mathbf{Z}$ ($\mathbf{Z}$ is the integers) the isomorphism being $(u, n)\mapsto u\pi^n$.

We let $U_n=\{u : 1\equiv u \bmod \mathfrak{p}^n\}$ for $n\geq 1$. Then $U_n\supset U_{n+1}$; and each is an open and closed subgroup of the compact group U; moreover $\bigcap_n U_n=(1)$. Let k_r denote the residue class field $\mathfrak{O}/\mathfrak{p}$, and let $q=p^n$ be its cardinality where p is the characteristic of k_r. Then it is well known [33] that $U/U_1\simeq k_r^*$ is a cyclic group of order $q-1$ (prime to p). Moreover one can find a subgroup R of U such that $U=U_1\times R$. Moreover R is of course precisely the set of elements of $E_k=E$, the roots of unity in k, of order prime to p. Finally $U_n/U_{n+1}\simeq k_r$ for $n\geq 1$ so that U_1/U_r is a p-group, and hence U_1 is a pro-p group [34]. The first step in determining $S(\mathbf{T})$, as in the Archimedian case, is to investigate $H^2(k^*, \mathbf{T})$. The fact that this is non-zero if k is non-Archimedian accounts for some of our difficulties.

Lemma **(4.1).** — *We have an isomorphism*

$$H^2(k^*, \mathbf{T})\simeq \hat{U}\oplus H^2(U, \mathbf{T})\simeq \hat{R}\oplus\hat{U}_1\oplus H^2(U_1, \mathbf{T})$$

Proof. — Since $k^*=U\times\mathbf{Z}$, the spectral sequence of group extensions [30] gives $H^2(k^*, \mathbf{T})\simeq H^2(\mathbf{Z}, \mathbf{T})\oplus H^1(\mathbf{Z}, H^1(U, \mathbf{T}))\oplus H^2(U, \mathbf{T})$. The first term is zero and the

second is clearly $\hat{U}$, the dual group of U, and this gives the first statement. Furthermore, since $U = R \times U_1$, we obtain in the same way isomorphisms

$$H^2(U, \mathbf{T}) \simeq H^2(R, \mathbf{T}) \oplus H^1(R, H^1(U_1, \mathbf{T})) \oplus H^2(U_1, \mathbf{T}).$$

Now R is cyclic so $H^2(R, \mathbf{T}) = 0$, and the second term above is $\mathrm{Hom}(R, \hat{U}_1)$; but $\hat{U}_1$ is a p-primary torsion group, and R has order prime to p, so $\mathrm{Hom}(R, \hat{U}_1)$ vanishes. The second statement of the lemma follows immediately.

In addition to knowing the isomorphisms above it is perhaps well to know how they are implemented. Thus, given a cocycle $a \in Z^2(k^*, \mathbf{T})$ we want to know how to determine the components $\varphi_1(a)$ (resp. $\varphi_2(a)$) in $\hat{U} = \hat{U}_1 \times \hat{R}$ (resp. $H^2(U_1, \mathbf{T})$) of the class of a. It is clear that $\varphi_2(a)$ is the restriction of the class of a to U_1. Now recall that π is our fixed generator of $\mathfrak{p}$; then if $s \in U$, consider the function $s \mapsto a(\pi, s)a(s, \pi)^{-1}$. By our remarks above (Lemma (3.1)) this is an element of $\hat{U}$, and by the construction of the spectral sequence, it is exactly $\varphi_1(a)$ [30].

Corollary. — *The group* $H^2(k^*, \mathbf{T})$ *is a countable torsion group, and is the sum of a p-primary group and a cyclic group of order* $q-1$.

Proof. — Note that $\hat{U}_1$ and $H^2(U_1, \mathbf{T})$ are both p-primary torsion groups.

Now we of course have a map of $S(\mathbf{T})$ into $H^2(k^*, \mathbf{T})$ since $S(\mathbf{T}) \subset Z^2(k^*, \mathbf{T})$ by (1) and (5). The first step is the computation of the kernel of this map. We recall that a cocycle is trivial if and only if it is symmetric so we are looking for the symmetric elements of $S(\mathbf{T})$. At this point the whole argument divides into two cases — when p (the characteristic of k_r) is odd, and when it is two. The latter case is rather more involved.

Lemma **(4.2).** — *If* $p \neq 2$, *any symmetric element of* $S(\mathbf{T})$ *is of order dividing two and is in* $S_0(\mathbf{T})$; *hence the kernel of the map of* $S(\mathbf{T})$ *into* $H^2(k^*, \mathbf{T})$ *is of order* 2.

Proof. — The same result is true if $p = 2$, but the argument is best deferred. Now let b be a symmetric element of $S(\mathbf{T})$ with $p \neq 2$. Then by Lemma (3.2), $b(t, s^2) = b(s^2, t) = 1$, and so by Lemma (3.5), $b(s, t)$ depends only on the classes of s and t modulo $(k^*)^2$, the group of squares in k^*. Since p is odd, $(k^*)/(k^*)^2 = B$ is a group of order 4, and moreover $(k^*)^2 \supset U_1$. Let us fix a generator π of $\mathfrak{p}$, and note that the cyclic group R is of even order so that we can choose some $\varepsilon \in R - (k^*)^2$. Then 1, ε, π, and $\varepsilon\pi$ are coset representatives for $(k^*)^2$. We denote their classes in B by a_0, a_1, a_2, and a_3 respectively. We will abuse notation and simultaneously think of b as a function on $k^* \times k^*$ and on $B \times B$.

Steinberg [40] has observed that it is possible to find an element $\bar{x} \in k_r^*$ such that $\bar{x}$ and $1 - \bar{x}$ are both not squares in k_r. Let x be the corresponding element of $R \simeq k_r^*$; then x and $1 - x$ are both in the coset of ε modulo $(k^*)^2$, and so $1 = b(x, 1-x) = b(\varepsilon, \varepsilon) = 1$ by (4) of definition (3.1); or equivalently we have $b(a_1, a_1) = 1$.

At this point we must separate two cases, depending on whether or not $-1 \in (k^*)^2$. If $-1 \in (k^*)^2$, then $b(s, s) = b(s, -s^2)$ (by (3) of definition (3.1)) $= b(s, s^2) = 1$. Thus

we have $b(a_i, a_i)=1$ for all i. Also we find that $b(s, t)=b(s, -st)=b(s, st)$ for all s and t. In particular, $b(\pi, \varepsilon)=b(\pi, \pi\varepsilon)$ and $b(\pi\varepsilon, \varepsilon)=b(\pi\varepsilon, \pi\varepsilon^2)=b(\pi\varepsilon, \pi)$ and so $b(a_1, a_2)=b(a_1, a_3)=b(a_2, a_3)$. Now $b(a_1, a_1a_2)b(a_1, a_2)=b(a_1^2, a_2)b(a_1, a_1)$ by the cocycle identity (1). Since $a_1^2=1$, and $a_1a_2=a_3$, we see that $b(a_1, a_3)b(a_1, a_2)=b(a_1, a_2)^2=1$. By what we have shown above $b(a_i, a_j)^2=1$ so that b is of order two, and in fact b has been determined uniquely by the above formulas. Since $S_0(\mathbf{T})$ does contain an element of order two (as E_k has even order), the element b above must be this element and hence $b\in S_0(\mathbf{T})$.

Now suppose that $-1\notin(k^*)^2$. Then we may take $\varepsilon=-1$ to simplify the calculations. We observe that $b(\pi, -\pi)=b(\pi, \pi^2)=1$ by (3) of definition (3.1) so that $b(a_2, a_3)=1$. Also by (3) of definition (3.1), $b(\pi, \pi)=b(\pi, -\pi^2)=b(\pi, -1)$ and $b(-\pi, -\pi)=b(-\pi, -\pi^2)=b(-\pi, -1)$, or in other words $b(a_2, a_2)=b(a_2, a_1)$ and $b(a_3, a_3)=b(a_3, a_1)$. Moreover since we can choose $x\in R$ such that x and $1-x$ are both congruent to -1 mod $(k^*)^2$, $b(x, s)=b(x, (1-x)s)$ implies that $b(a_1, a_i)=b(a_1, a_ia_1)$ for all i. In particular, $b(a_1, a_2)=b(a_1, a_3)$ since $a_1a_2=a_3$. Thus since b is symmetric $b(a_2, a_2)=b(a_3, a_3)=b(a_1, a_2)=b(a_1, a_3)$.

By the cocycle identity,

$$b(a_2, a_3a_1)b(a_3, a_1)=b(a_2, a_3)b(a_2a_3, a_1),$$

and we have seen that that $b(a_2, a_3)=1=b(a_2a_3, a_1)=b(a_1, a_1)=1$. Since $a_3a_1=a_2$, we find that $b(a_2, a_2)b(a_3, a_1)=1$ or by the above $b(a_2, a_2)^2=1$. Thus b is of order 2 and its values have been uniquely determined and so it must be in $S_0(\mathbf{T})$ as we have argued above. This completes the proof of the lemma.

Corollary. — *The group* $S(\mathbf{T})$ *is a countable torsion group, which is the sum of a p-primary group and a group of order dividing* $2(q-1)$.

Proof. — We have a sequence

$$1\to A\to S(\mathbf{T})\to H^2(k^*, \mathbf{T})$$

where A is of order two. Our assertion follows from the Corollary to Lemma (4.1).

Since $S(\mathbf{T})$ is a torsion group, we can write $S(\mathbf{T})=S(\mathbf{T})_1+S(\mathbf{T})_p$ where $S(\mathbf{T})_p$ is p-torsion, and $S(\mathbf{T})_1$ has no elements of order p. According to the Corollary above we may write an exact sequence $0\to A\to S(\mathbf{T})_1\to\hat{R}$ where A is of order two and $\hat{R}$ is viewed as a subgroup of $H^2(k^*, \mathbf{T})$ by means of Lemma (4.1). Moreover the element $\varphi_1(b)\in\hat{R}$ corresponding to $b\in S(\mathbf{T})_1$ is given by $s\to b(\pi, s)b(s, \pi)^{-1}$ $(s\in R)$ (see the discussion following Lemma (4.1)).

Lemma **(4.3).** — *If* $b\in S(\mathbf{T})_1$, *then* $\varphi_1(b)$ *vanishes on* -1.

Proof. — According to the above, we must show that $b(\pi, -1)b(-1, \pi)^{-1}=1$ where π is a generator of p. However, $b(\pi, -1)b(-1, \pi)^{-1}=b((-1)^2, \pi)=b(1, \pi)=1$ by Lemma (3.2).

Corollary. — *The image of* $S(\mathbf{T})_1$ *in* $H^2(k^*, \mathbf{T})$ *has order dividing* $(q-1)/2$ *and hence* $S(T)_1$ *has order dividing* q.

Proof. — We observe that the image of $S(\mathbf{T})_1$ by definition must lie in the part of $H^2(k^*, \mathbf{T})$ prime to p; i.e. $\hat{R}$. Lemma (4.3) says this image in $\hat{R}$ must have index divisible by 2 in $\hat{R}$, and our assertions follows.

We finally note that $S_0(\mathbf{T})$ is a finite group isomorphic to $\hat{E}_k$ and hence the sum of a p-primary group $(S_0(\mathbf{T}))_p$ and a group $(S_0(\mathbf{T}))_1$ of order prime to p, which is necessarily isomorphic to $\hat{R}$ and hence of order $q-1$.

Theorem (4.1). — *If* $p \neq 2$, *we have* $S_0(\mathbf{T})_1 = S(\mathbf{T})_1$.

Proof. — We note that $S_0(\mathbf{T})_1 \subset S(\mathbf{T})_1$ and that both groups have order $q-1$.

Thus we have proved our result for $p \neq 2$ for the part of $S(\mathbf{T})$ prime to p. We now consider the p-primary component. The analysis is somewhat more subtle here.

5) The group E (roots of unity in k) splits as $R \times E_p$ where E_p is a cyclic group of order p^r contained in U_1. Our main problem is to discover how to compute the integer r; the results here will be valid for all p. It is reasonably easy to tell whether r is positive or not as follows. If k is of characteristic zero, it is a finite extension of $\mathbf{Q}_p$ the p-adic field and we denote by e the absolute degree of ramification of k over $\mathbf{Q}_p$ [33]. If k is of characteristic p, we let $e = \infty$ for notational purposes. Now if k has a p-th root of 1, it is known that $p-1$ divides e, and we define $l = \frac{e}{p-1} + e = \frac{pe}{p-1}$. In general let l be the greatest integer in $e/(p-1)+e$. Let $(k^*)^p$ be the (closed) subgroup of k^* consisting of p-th powers, and we observe that $k^*/(k^*)^p$ is a vector space over $\mathbf{Z}_p$ the integers mod p.

Lemma (5.1). — *If k is of characteristic zero, one always has* $U_{l+1} \subset (k^*)^p$. *Moreover* $r > 0$ *if and only if the characteristic of k is zero,* $p-1 \mid e$, *and the projection of* U^l *into* $k^*/(k^*)^p$ *is non-zero, in which case it is one dimensional; i.e. it is cyclic of order p.*

Proof. — These are essentially well known facts, but for completeness we include proofs. We consider the map $\varphi : x \mapsto x^p$ on U_1. If $x \in U_n$, $x = 1 + u\pi^n$ with $u \in \mathfrak{O}$ and π a fixed generator of $\mathfrak{p}$, the maximal ideal of $\mathfrak{O}$. Now $\varphi(x) = 1 + up\pi^n + u^p\pi^{np} + B(x)$. Now by definition of e, p is a generator of the ideal $\mathfrak{p}^e$ and so $p = \pi^e u_0$ where $u_0 \in U$. Thus $\varphi(x) = 1 + uu_0\pi^{n+e} + u^p\pi^{np} + B(x)$ and from inspection of the terms of $B(x)$, we see that $B(x) \in \mathfrak{p}^{a(n)+1}$ where $a(n) = \min(n+e, np)$. Thus $\varphi(U_n) \subset U_{a(n)}$ and hence φ induces a map $\varphi : U_n/U_{n+1} \to U_{a(n)}/U_{a(n)+1}$. For every k, U_n/U_{n+1} is isomorphic (not canonically) to k_r the additive group of the residue class field, and in fact the isomorphism is induced by the map $1 + u\pi^n \mapsto u$ (u mod $\mathfrak{p}$). In terms of these identifications, φ_n viewed as map from k_r tok_r is the map $u \mapsto \dot{u}_0 u$ if $n+e < np$, and the map $u \mapsto u^p$ if $np < n+e$, where $\dot{u}_0$ is non-zero. Thus φ_k is an isomorphism if $np \neq n+e$. If on the other hand $np = n+e$, then φ_n becomes the map $u \mapsto \dot{u}_0 u + u^p$. The kernel of this map is at most cyclic of order p (o and the at most $p-1$ solutions of the equation $u^{p-1} = -\dot{u}_0$). We notice that if $np = n+e$ then $n = e/(p-1)$ so that $p-1$ necessarily divides e.

We now consider the proof of the lemma proper, and observe that if $n > l-e$, then $n > e/(p-1)$ and so $n+e > np$. Then φ_n is necessarily an isomorphism. Thus taking $n = l-e+1$, we see that φ maps U_{l-e+1} into U_{l+1}. One proves by induction

on s that $\varphi(u_{l-e+1}).U_s=U_{l+1}$ for every $s\geq l+1$ using the fact that φ_n is an isomorphism if $n>l-e$. This says that $\varphi(U_{l-e+1})$ is dense in U_{l+1}, but this group is also closed since U_{l-e+1} is compact. This proves the first statement of the lemma, and even more, namely that every element of U_{l+1} is the p-th power of some element of U_{l-e+1}.

Now suppose that $r>0$ so that k does have a primitive p-th root of unity, x. Then k is of characteristic zero (essentially by definition of a primitive p-th root of unity). Then $x\in U_n-U_{n+1}$ for some n and since $\varphi(x)=1$, it follows that φ_n is not one-one and hence that $n=e/(p-1)$ and so $p-1$ divides e. Now let us look at $U_l\cap(k^*)^p$; it is clear that if $u\in U_l$, then whether or not u is a p-th power depends only on its class $\dot{u}$ in U_l/U_{l+1}. However by our discussion above it is perfectly clear that u is a p-th power if and only if $\dot{u}\in\varphi_s(U_s/U_{s+1})$ $(s=e/(p-1)=l-e)$. Since φ_s has kernel cyclic of order p, the index of $\varphi_s(U_s/U_{s+1})$ in U_l/U_{l+1} is clearly p. Thus the index of $(k^*)^p\cap U_l$ in U_l is p and this gives the final assertion.

Conversely suppose that k is of characteristic zero and that $l=e/(p-1)+e$ and that $(k^*)^p\cap U_l\neq U_l$; then by reversing the above argument, we see that it is exactly of index p, and that φ_s $(s=l-e)$ is not injective. Then we choose $x\in U_s$ such that $\varphi_s(\dot{x})=0$, or in other words $\varphi(x)\in U_{l+1}$. But by the first statement of the lemma, $\varphi(x)=x^p=y^p$ for some $y\in U_{s+1}$. Then $xy^{-1}=u$ is in U_s but not U_{s+1}; moreover, $u^p=1$ so that k has a primitive p-th root of one.

The following is really a corollary of the argument above.

Corollary. — *k has a p-th root of 1 if and only if k is of characteristic zero, and $l=e/(p-1)+e$ and φ_s $(s=l-e=e/(p-1))$ is not one-one. Moreover if this p-th root of unity exists, it is in U_s-U_{s+1}.*

If k does have a p-th root of 1, we shall call any element v of U_l $(l=e/(p-1)+e)$ which is not in $(k^*)^p$, *unramified.* We observe that if v is such an element, then $k((v)^{1/p})$ is an unramified extension of k.

Now if π is a generator of the maximal ideal $\mathfrak{p}$ of $\mathfrak{O}$, let $H(\pi)$ be the smallest closed subgroup of U_1 containing all elements of the form $1-u\pi^t$ where $u\in R$ (the multiplicative residue class system) and t is a positive integer prime to p. Our main result is the following.

Theorem (5.1). — *The group U_1 is the closure of the group generated by $H(\pi)$ and v where v is any unramified element with the understanding that $H(\pi)=U_1$ if k has no p-th roots of unity. Moreover the index of $H(\pi)$ is divisible by p^r where p^r is the order of E_p. Finally there exists π such that the index of $H(\pi)$ in U_1 is exactly p^r.*

Proof. — Let W denote the smallest closed subgroup containing $H(\pi)$ and v, where v is a fixed unramified element. We will show by induction on t that $W.U_t=U_1$ for $t\geq 1$. This is true for $t=1$ so let us assume that it holds for all integers less than or equal to some $t>1$. Then we consider $(W\cap U_t).U_{t+1}$; if we can show that this is U_t, then $W.U_{t+1}\supset U_t$ and since $W.U_{t+1}\supset W$, $WU_{t+1}\supset W.U_t=U_1$ by the inductive assumption.

Thus we must show that $(W\cap U_t).U_{t+1}=U_t$, or in other words that W contains an

element of each coset of U_{t+1} in U_t. If t is prime to p, then W contains $1-u\pi^t$ for all $u\in R$, and these are representatives of every non-zero coset of U_{t+1} in U_t so we are done in this case. If $p|t$, we choose m such that $a(m)=\min(m+e, pm)=t$. This is clearly possible, and then, by induction, W contains coset representatives x_i of every coset of U_{m+1} in U_m. Then W contains the elements $\varphi(x_i)=x_i^p$, and so if $\varphi_m : U_m/U_{m+1} \to U_t/U_{t+1}$ is an isomorphism, the $\varphi(x_i)$ are coset representatives of every coset of U_{t+1} in U_t and we are done. Thus if k has no p-th roots of unity (so that φ_m is always an isomorphism), then $W=H(\pi)$ satisfies $W.U_{t+1}=U_1$ for all t. If however k has a p-th root of unity, φ_m fails to be an isomorphism only for $m=s=e/(p-1)$. In this case $t=e/(p-1)+e=l$ and the range of φ_m in U_l/U_{l+1} is of index p. Moreover the image of v (any unramified element) in U_l/U_{l+1} is not in the range of φ_m. Thus the elements $\varphi(x_i)v^k=x_i^p v^k$ $(k=1, \ldots, p)$ are representatives of the cosets of U_l in U_{l+1} and are all in W. Thus $(W\cap U_t).U_{t+1}=U_t$ for all t and as we have remarked, it follows then that $W.U_t=U_1$ for all t.

The statement that $W.U_t=U_1$ for all t says exactly that W is dense in U_1, but since W is closed by its definition, $W=U_1$, and this proves the first part of the theorem. Now if K is the extension field of k generated by the p^r-th roots of π, K is a totally non-tamely ramified Kummer extension of k [33]. (Recall that p^r is the order of E_p, the p-primary component of the roots of unity of k.) Now it is more or less clear from the properties of the norm residue symbol that every element of the form $1-u\pi^t$, $u\in R$, t prime to p, is a norm from K. (This is a special case of an argument to be given in more detail shortly.) Thus $H(\pi)$ is contained in N(K), the norm group from K. Now it follows from local class field theory that the index of $N(K)\cap U_1$ in U_1 is exactly p^r [33]. Our second assertion then follows.

It remains to show the existence of at least one π such that the index of $H(\pi)$ in U_1 is p^r. (This is the same thing as showing that $H(\pi)=U_1\cap N(K)$ by the above comments.) If $r=0$, that is, if k has no p-th roots of unity, we are done. Thus assume that $r>0$, and let x be any primitive p^r-th root of unity. Then $x\notin(k^*)^p$ and so if y is a p-th root of x, $L=k(y)\neq k$. Now let π be any generator of $\mathfrak{p}$ such that π is not a norm from L. Such elements clearly exist (otherwise every element of k is a norm from L), and by class field theory $N(L)\neq k^*$. Then we claim that $H(\pi)$ is of index p^r in U_1, or equivalently that v^n $(n=p^r)$ is in $H(\pi)$ where v is any unramified element.

Let $\dot{H}$ be the projection of $H(\pi)$ into U_1/U_{l+1} where $l=pe/(p-1)$ as usual. If $\dot{v}$ is the image of v in U_1/U_{l+1}, it is a corollary of the first part of the theorem that $\dot{H}$ and $\dot{v}$ generate U_1/U_{l+1}. Then if $\dot{x}$ is the image of x in U_1/U_{l+1}, $\dot{x}=\dot{h}(\dot{v})^m$ with $\dot{h}\in\dot{H}$ and m an integer. Since $\dot{v}$ has order p in U_1/U_{l+1}, either $\dot{x}\in\dot{H}$ in which case $m\equiv 0 \pmod p$, or m is prime to p. If $\dot{x}\in\dot{H}$, it follows that $x\in H(\pi).U_{l+1}$. However $H(\pi)$ is contained in the norm group from $K=k(z)$ where z is a p^r-th root of π. Thus $H(\pi)$ is contained in the norm group from $M=k(w)$ where w is a p-th root of π. Since $U_{l+1}\subset(k^*)^p$, every element of U_{l+1} is a norm from M since M is of degree p over k. Thus the assumption that $\dot{x}\in\dot{H}$ implies that x is a norm from M. By the skew symmetry of the norm

residue symbol (cf. definition (3.1)), this implies that π is a norm from $L=K(y)$ where y is a p-th root of x and this is contrary to our choice of π.

Thus we find that $\dot{x}=\dot{h}\dot{v}^m$ where m is prime to p, or in other words $x=hv^m y$ where $y\in U_{l+1}$. We now take $n=p^r$-th powers of this to find that $1=h^n v^{nm} y^n$ (recall that x is a p^r-th root of unity). Moreover, $w=y^n\in U_{l+re+1}$ by our computations about p-th powers, and we deduce that $v^{nm}\in(H(\pi)\cap U_{l+re})\cdot U_{l+re+1}$. Since U_{l+re}/U_{l+re+1} is a p-group and m is prime to p we see that $v^n\in(H(\pi)\cap U_{l+re})\cdot U_{l+re+1}$ $(n=p^r)$. The same inductive argument utilized in the first part of the theorem may be used again to show that $H(\pi)\supset U_{l+re}$. (That is, one shows that $(H(\pi)\cap U_t)\cdot U_{t+1}=U_t$ for all $t\geq l+re$.) Then it follows that $v^n\in H(\pi)$ as desired.

Remark. — The content of this theorem is that for suitable π, the group $N(K)\cap U_1$ where K is $k(z)$, z a p^r-th root of π, is generated by the elements $1-u\pi^t$, which are all obviously norms from K. These objects are obviously norms by virtue of formal properties of the norm residue symbol which in addition are part of the definition of $S(\mathbf{T})$ (Definition (3.1)). For these reasons it is clear that this theorem will play a key role in the proof of Theorem (3.1).

We now complete the proof of Theorem (3.1) in the case when p (=characteristic of the residue class field) is odd. Recall that $S(\mathbf{T})_p$ is the subgroup of $S(\mathbf{T})$ of elements of order a power of p.

Lemma **(5.2).** — *Let p be odd and $b\in S(\mathbf{T})_p$, and let π be a generator for* $\mathfrak{p}$ *and let v be an unramified element (it it exists). If $b(\pi, v)=1$, then $b=1$. If there is no unramified element, $b=1$.*

Proof. — We first note that every element of U_1 is a square since p is odd, and so by Lemma (3.2), $b(x, u)$ and $b(u, x)$ are bilinear functions of u and x when $u\in U_1$. Now if $s\in R$ (the multiplicative residue class system), and $u\in U$, $b(s, u)$, being continuous, has order a power of p since U_1 is a pro-p-group, but it also has order prime to p since R has order prime to p. Thus $b(s, u)=1$, and by the same argument, $b(u, s)=1$ $(u\in U_1, s\in R)$.

Now we will show that $b(\pi, u)=b(u, \pi)=1$ for all $u\in U_1$ under our assumptions. Let $u=1-s\pi^n$ with $s\in R$ and n prime to p; then $1=b(s\pi^n, 1)=b(s\pi^n, 1-s\pi^n)$ (by definition (3.1)) $=b(s\pi^n, u)=b(s, u)b(\pi, u)^n$ by bilinearity established above. But also $b(s, u)=1$, and so $b(\pi, u)^n=1$. Now n is prime to p and $b(\pi, u)$ has order prime to p so that $b(\pi, u)=1$. By linearity and continuity, $b(\pi, x)=1$ for all $x\in H(\pi)$, and since $b(\pi, v)=1$ where v is some fixed unramified element by assumption, it follows, again by linearity and continuity and Theorem (5.1) that $b(\pi, x)=1$ for all $x\in U_1$. Moreover, if k has no unramified elements then it follows that $b(\pi_1, x)=1$ for any generator π_1 of $\mathfrak{p}$ and any $x\in U_1$.

Our next step is to prove that $b(\pi_1, x)=1$ for any π_1 and any $x\in U_1$ when k does have a p-th root of one. We may write the unramified element v of the statement in the form $v=1-su\pi^l$ where $s\in R$, $u\in U_1$ and $l=e/(p-1)+e$. If π_1 is any generator of $\mathfrak{p}$ then $\pi_1=tu_1\pi$ with $t\in R$, $u_1\in U_1$. Now let us form $v_1=1-su_1\pi^l$; then $v_1\equiv v \bmod U_{l+1}$ so that v_1 is also unramified. Moreover, $1=b(x, 1)=b(x, 1-x)$ by definition (3.1), and

putting $v_1 = 1 - x$, we see that $1 = b(1-v_1, v_1) = b(su_1\pi^l, v_1) = b(s, v_1)b(\pi, v_1)^l b(u_1, v_1)$ by linearity. On the other hand, we have seen that $b(s, v_1) = 1$ since $s \in R$ and $v_1 \in U_1$, and we have shown that $b(\pi, v_1) = 1$. We then conclude that $b(u_1, v_1) = 1$, and finally that $b(\pi_1, v_1) = b(\pi, v_1)b(t, v_1)b(u_1, v_1)$ again by bilinearity since $v_1 \in U_1$. We have shown that all terms are equal to 1, and hence $b(\pi_1, v_1) = 1$. Our previous argument now applies since v_1 is unramified, and shows that $b(\pi_1, u) = 1$ for any $u \in U_1$. Since $b(\pi_1, u) = b(u^{-1}, \pi_1)$ by definition (3.1), we can conclude from the hypotheses of the lemma that $b(\pi_1, u) = b(u, \pi_1) = 1$ whenever π_1 is an arbitrary generator of p and u is an arbitrary element of U_1.

Now if $u_1 \in U_1$ and $u \in U_1$ and π is any generator of $\mathfrak{p}$, $b(\pi u, u_1) = b(u_1, \pi u) = 1$, and so by linearity, and the fact that $b(\pi, u_1) = b(u_1, \pi) = 1$, we see that $b(u, u_1) = b(u_1, u) = 1$. Thus the cohomology class of b in $H^2(k^*, \mathbf{T})$ must vanish upon restriction to U_1. Now according to Lemmas (4.1) and (4.2), b, as an element of $S(\mathbf{T})$, must have order dividing $2(q-1)$, q being the cardinality of the residue class field, and hence b must have order prime to p since p is odd. However b is assumed to have order dividing p, and so $b = 1$ as desired.

We can now complete the proof of Theorem (3.1) when p, the characteristic of the residue class field, is odd. We have shown that $S(\mathbf{T})$ is a torsion group, and that its component of order prime to p is contained in $S_0(\mathbf{T})$. We want to show that its p-primary component $S(\mathbf{T})_p$ is contained in $S_0(\mathbf{T})$. Since the p-primary component of $S_0(\mathbf{T})$ is cyclic of order p^r (the order of E_p, the p-primary component of the group of roots of unity of k), it suffices to estimate the order of $S(\mathbf{T})_p$.

Lemma **(5.3).** — *The group* $S(\mathbf{T})_p$ *is cyclic of order* p^r *and hence* $S(\mathbf{T}) = S_0(\mathbf{T})$.

Proof. — If $r = 0$, lemma (5.2) says that $S(\mathbf{T})_p = (1)$ and we are done. If $r > 0$, so that there exist unramified elements, choose an unramified element v and a generator π of the maximal ideal $\mathfrak{p}$ such that the final statement of Theorem (5.1) is valid. Then we define a map φ of $S(\mathbf{T})_p$ into $\mathbf{T}$ by $\varphi(b) = b(\pi, v)$. By the preceding lemma, φ is injective. Moreover since $b(\pi, u)$ is linear in u when $u \in U$, $\varphi(b)^n = b(\pi, v)^n = b(\pi, v^n)$ for any n. We take $n = p^r$ and use the fact that $v^n \in H(\pi)$ by Theorem (5.1). On the other hand the argument of the preceding lemma showed that $b(\pi, u) = 1$ if $u \in H(\pi)$, and hence we deduce that $\varphi(b)^n = b(\pi, v^n) = 1$. Thus since φ is injective, $S(\mathbf{T})_p$ is cyclic of order dividing $n = p^r$. Since it clearly contains a cyclic group of order p^r ($S_0(\mathbf{T})_p$) its order is exactly p^r.

6) We are now left with the case when p (the characteristic of the residue class field) is two. Our first result is the extension of Lemma (4.2) to this case.

Theorem **(6.1).** — *If* $b \in S(\mathbf{T})$ *is symmetric, then* $b \in S_0(\mathbf{T})$ *and hence* b *has order dividing two.*

Proof. — Since b is symmetric, $b(x^2, y) = b(x, y^2) = 1$ for all x and y by Lemma (3.2), and hence $b(x, y)$ depends only on the classes of x and y mod $(k^*)^2$, the group of squares. The group R is cyclic of order $q-1$ prime to 2 and hence $R \subset (k^*)^2$. Now let π be any generator of $\mathfrak{p}$, and let n be an odd positive integer, $s \in R$, and $x \in k^*$;

then $b(\pi, x)=b(s\pi^{n-1}\pi, x)=b(s\pi^n, x)=b(s\pi^n, (1-s\pi^n)x)=b(\pi, (1-s\pi^n)x)$. Therefore, by continuity, $b(\pi, x)$ depends only on the coset of x modulo $H(\pi)$ ($H(\pi)$ is defined in Theorem (5.1)), and hence $b(\pi, x)$ depends only on the coset of x modulo $H(\pi).(k^*)^2$.

Now let us suppose that k has characteristic two. Then by Theorem (5.1), $H(\pi)$ is all of U_1 and hence $H(\pi)(k^*)^2$ is of index two in k^*. Moreover π is in the non-trivial coset, and $b(\pi, \pi)=b(\pi, -\pi^2)=b(\pi, 1)=1$, so that we conclude that $b(\pi, x)=b(x, \pi)=1$ for any π and all x. (The last statement follows since b is symmetric.) Finally let $x=u\pi^n$ and $y=v\pi^m$ be arbitrary elements of k^* with u and $v\in U$. If either n or m is odd, say n, then $b(x, y)=b(u\pi, y)=1$ since $u\pi$ is a generator of $\mathfrak{p}$. If n and m are even, $b(x, y)=b(u, v)$, and since $b(u, v)$ depends on the classes of u and v modulo squares, if either u or v is not a square, say u, we can assume that $u=1-u'\pi^n$, $u'\in U$ where n is an odd integer. Then $b(u, v)=b(u, (1-u)v)=b(u, u'v\pi^n)=b(u, u'v\pi)$ since n is odd. Since $u'v\pi$ is a generator of $\mathfrak{p}$ we see that $b(u, v)=1$. Thus we have shown that $b(x, y)=1$ for all x and y in k^*, and this gives our assertion when k has characteristic two.

We assume now that k has characteristic zero; then there exists an unramified element v since k has a square root of 1. If π is any generator of $\mathfrak{p}$, then by Lemma (5.1) and Theorem (5.1), $(H(\pi).(k^*)^2)\cap U_1$ is of index two in U_1, and any unramified element v is in the non-trivial coset. We complete the argument in the following lemmas.

Lemma **(6.1)**. — *Let k be of characteristic zero and b be symmetric. If $b(\pi, v)=1$ for some π and some unramified element v, then $b=1$.*

Proof. — By our preceding discussion $b(\pi, x)$ depends only on the coset of x modulo $H(\pi).(k^*)^2$ and hence by our hypothesis, $b(\pi, x)=1$ for all $x\in U_1$. Since $R\subset(k^*)^2$, we see at once that $b(\pi, x)=1$ if $x\in U$ also.

If $u\in U$, then for suitable $s\in R$, the element $v'=1-su^{-1}\pi^{2e}$ is unramified where e is the absolute degree of ramification (cf. Lemma (5.1), $2e=e/(p-1)+e=l$ since $p=2$). Then $b(\pi u, v')=b(\pi u(1-v'), v')=b(\pi s\pi^{2e}, v')=b(\pi, v')=1$ since $s\pi^{2e}\in(k^*)^2$. Since πu is the most general generator of $\mathfrak{p}$ and v' is unramified, we deduce from the above that $b(\pi', u')=1$ for any generator π' of $\mathfrak{p}$ and any $u'\in U$. We can argue essentially as in the case when k has characteristic two that $b(x, y)=1$ for all x and $y\in k^*$. The only modification is that not every element u of U can be written as $1-u'\pi^n$, n odd, $u'\in U$, modulo squares. We must allow the case when u is unramified. Then if v any element of U, we can write u in the form $u=1-sv\pi^{2e}$ for appropriate $s\in R$. Then we must show that $b(u, v)=1$, but $1=b(u, 1)=b(u, 1-u)=b(u, sv\pi^{2e})=b(u, v)$ since $s\pi^{2e}\in(k^*)^2$. This remark concludes the proof of the lemma.

We want to show that $b\in S_0(\mathbf{T})$ and is of order two. We note that $S_0(\mathbf{T})$ contains a symmetric element of order two, b_0 (the Hilbert symbol), and that $b_0(\pi, v)\neq 1$ by the preceding lemma since $b_0\neq 1$. Suppose that we could show that our symmetric element b is of order two. Then if $b\neq 1$, $b(\pi, v)\neq 1$ and then necessarily $b(\pi, v)=b_0(\pi, v)$, and hence $b_0=b$ by the preceding lemma. Thus it suffices to show any symmetric element of $S(\mathbf{T})$ is of order two and by the lemma above, it suffices to show that $b(\pi, v)^2=1$ for any π and any unramified element v.

Lemma **(6.2)**. — *If b is symmetric, then* $b(\pi, v)^2 = 1$.

Proof. — First we note that if v and v' are unramified, then $v \equiv v' \bmod (k^*)^2$ by Lemma (5.1), so that $b(\pi, v) = b(\pi, v')$. Furthermore if $u \in U$, then $v' = 1 - su^{-1}\pi^{2e}$ is unramified for suitable $s \in R$, so that $b(\pi u, v') = b(\pi, v')$ as above. Thus $b(\pi, v)$ does not depend on the choice of either π or v. In our proof then we are free to choose π and v at will.

Just as in Lemma (4.2), we must consider two cases depending on whether -1 is unramified or not. If -1 is not unramified, that is $-1 \not\equiv v \bmod (k^*)^2$, we claim that we can choose π so that $-1 \in H(\pi).(k^*)^2$. If $-1 \in (k^*)^2$, this is clear, and if not $-1 \equiv 1 - su\pi^n \bmod (k^*)^2$ where n is either odd or $n = 2e$ by the local square theorem with $u \in U_1$ and $s \in R$. However, if $n = 2e$, $-1 \equiv v \bmod (k^*)^2$ contrary to hypothesis. Thus $-1 \equiv 1 - su\pi^n \bmod (k^*)^2$ with n odd. Since U_1 is a pro-2-group, $u = z^n$ for appropriate z and $-1 \equiv 1 - s(z\pi)^n \bmod (k^*)^2$. Thus if we replace π by $z\pi$, we have $-1 \in H(\pi).(k^*)^2$. Let us fix such a π.

We now consider the subgroup A of $k^*/(k^*)^2$ consisting of the classes of 1, v, π, and $v\pi$ which we denote by a_0, a_1, a_2, and a_3 respectively. As in Lemma (4.2), we may with slight abuse of notation, view b as a cocycle on A and denote its values by $b(a_i, a_j)$. Now $b(a_2, a_2) = b(\pi, \pi) = b(\pi, -\pi^2) = b(\pi, -1) = 1$ since $-1 \in H(\pi).(k^*)^2$. On the other hand, we claim that $H(\pi).(k^*)^2 = H(v\pi).(k^*)^2$, for if n is odd, $1 - s(v\pi)^n \equiv 1 - s\pi^n$ modulo $\mathfrak{p}^{2e+1}$ since $v \equiv 1$ modulo p^{2e}. Thus as $U_{2e+1} \subset (k^*)^2$ by Lemma (5.1), we see that $1 - s(v\pi)^n \equiv 1 - s\pi^n$ modulo $(k^*)^2$ for n odd, and this proves our assertion. Thus in particular $b(a_3, a_3) = b(v\pi, v\pi) = b(v\pi, -1) = 1$ since $-1 \in H(v\pi).(k^*)^2$. We finally note that $v' = 1 - sv\pi^{2e}$ is unramified for suitable $s \in R$, and hence $v \equiv v' \bmod (k^*)^2$. Thus for any t, $b(v', t) = b(v', (1 - v')t) = b(v', vs\pi^{2e}t) = b(v', vt)$, and in particular $b(v', v) = b(a_1, a_1) = 1$. Therefore we have shown that $b(a_i, a_i) = 1$ for all i.

Moreover, $b(a_3, a_1) = b(v\pi, v) = b(\pi, v) = b(a_2, a_1)$ since $b(\pi, v)$ is independent of the choice of π. Also $b(a_3, a_2) = b(v\pi, \pi) = b(v\pi, -v\pi^2) = b(v\pi, -v) = b(v\pi, v) = b(a_3, a_1)$ since $-1 \in H(v\pi).(k^*)^2$. Thus we have a symmetric cocycle b on A (the Klein four group) with $b(a_i, a_i) = 1$ and $b(a_1, a_2) = b(a_2, a_3) = b(a_1, a_3)$. It follows just as in lemma (4.2) that $b(a_2, a_1)^2 = b(\pi, v)^2 = 1$ as desired. This completes the argument when -1 is not unramified. If -1 is unramified, the argument proceeds in exactly the same fashion as the second of the two cases considered in Lemma (4.2). It is clear that the argument above is the analogue of the first of the two cases considered in Lemma (4.2), and it shows the way. We omit the details.

Corollary 1. — *The map* $S(\mathbf{T}) \to H^2(k^*, \mathbf{T})$ *has kernel of order two if the characteristic of k is zero, and is injective if the characteristic of k is two.*

Corollary 2. — *The group* $S(\mathbf{T})$ *is a countable torsion group and* $S(\mathbf{T})_1$, *the sum of the components of order prime to two, is cyclic of order dividing $q - 1$ where q is the cardinality of the residue class field k_r.*

Proof. — This follows from Corollary 1 and the Corollary to Lemma (4.1).

Corollary 3. — *If* $(S_0(\mathbf{T}))_1$ *is the sum of the components of* $S_0(\mathbf{T})$ *of order prime to two, then* $S_0(\mathbf{T})_1 = S(\mathbf{T})_1$.

Proof. — Since $S_0(\mathbf{T})_1 \subset S(\mathbf{T})_1$ and $S_0(\mathbf{T})_1$ is cyclic of order $q-1$, the result follows from Corollary 2.

We are now reduced to the study of $S(\mathbf{T})_2$, the two-primary component of $S(\mathbf{T})$.

Lemma **(6.3).** — *If* $b \in S(\mathbf{T})_2$, *then* $b(sx, y) = b(x, sy) = b(x, y)$ *for* $s \in R$ *and* $x, y \in k^*$.

Proof. — We recall that R is cyclic of odd order $q-1$ so that $s = t^2$. Then $b(x, t^2)$ and $b(t^2, x)$ are bilinear in x and t by lemma (3.2), and hence $b(x, t^2)^n = b(t^2, x)^n = 1$ for n odd. But b has 2-power order and so with $s = t^2$, $b(x, s) = b(s, x) = 1$ for all $x \in k^*$. Our result follows now from Lemma (3.5).

The next step is the following fact.

Lemma **(6.4).** — *If the characteristic of k is two,* $S(\mathbf{T})_2 = (1)$; *if k is of characteristic zero, and* π *is a generator of* $\mathfrak{p}$, *and v an unramified element, then* $b(\pi, v^2) = 1$ *implies that b is symmetric.*

Proof. — Let us say that x and y commute if $b(x, y) = b(y, x)$. By Lemma (3.2), this is equivalent to any one of the following: $b(x^2, y) = b(y, x^2) = b(y^2, x) = b(x, y^2) = 1$. Furthermore if E is the extension of k^* by $\mathbf{T}$ defined by b, this also means that coset representatives of x and y in E commute with each other.

First let us note that $1 = b(s\pi^n, 1) = b(s\pi^n, 1 - s\pi^n)$ and that

$$1 = b(1, s\pi^n) = b(1 - s\pi^n, s\pi^n)$$

if $s \in R$, by definition (3.1) and a substitution of variables. We conclude by Lemma (6.3) that $1 = b(\pi^n, 1 - s\pi^n) = b(1 - s\pi^n, \pi^n)$, and hence that π^n commutes with $1 - s\pi^n$. If n is odd it follows since b has order a power of two that π commutes with $1 - s\pi^n$ for all $s \in R$, and n odd. Since the set of elements commuting with π is a closed subgroup, we deduce that π commutes with $H(\pi)$.

Thus if k has characteristic two, $H(\pi) = U_1$ so that π commutes with U_1. On the other hand, Lemma (6.2) implies that π commutes with R, and hence that π commutes with $U = U_1 \times R$. Since π clearly commutes with itself, this shows that π commutes with all of k^*. If $u \in U$, this also says that πu commutes with k^* and hence that u does. Finally we deduce that any element of k^* commutes with any other element; this says that b is symmetric and then Theorem (6.1) says then that b is identically equal to one.

Now let k have characteristic zero. Then our hypothesis is that some fixed π commutes with some fixed unramified element v. Now as above, π commutes with $H(\pi)$ and hence with U_1 by Theorem (5.1), the same argument as above shows that then π commutes with all of k^*.

Now if u is an arbitrary element of U, then $v' = 1 - su^{-2}\pi^{2e}$ is unramified for suitable $s \in R$. Then $b(v', \pi^2 u^2) = b(v', (1 - v')\pi^2 u^2) = b(s\pi^{2e+2}, v') = b(\pi^2, v')^{e+1} = 1$ by definition (3.1), Lemma (3.2) and Lemma (6.3). Therefore πu commutes with v' and the first part of the argument shows then that πu commutes with k^*. Thus u commutes with k^* and it follows as above that b is symmetric as desired.

We now need the converse of Theorem (6.1).

Lemma **(6.5).** — *Any element of* $S(\mathbf{T})_2$ *or order two is symmetric.*

Proof. — We may assume by Lemma (6.4) that k has characteristic zero. Let 2^r be the order of the two primary component of E and hence the order of $S_0(\mathbf{T})_2$. By Theorem (5.1), we can choose a generator π such that $H(\pi)$ has index 2^r in U_1; now let v be an unramified element, and let us assume that $r=1$; we see then that $v^2\in H(\pi)$.

It was shown in the preceding lemma that π commutes with $H(\pi)$ or in other words that $b(\pi^2, x)=1$ if $x\in H(\pi)$. We claim now that $b(\pi, x)=1$ if $x\in H(\pi)$. First let us take $x=\prod_{i=1}^{m} x_i$ with $x_i=1-s_i\pi^{n_i}$, $s_i\in R$, n_i odd. If $y=\prod_{i=2}^{m} x_i$, then we may assume inductively on m that $b(\pi, y)=1$. For simplicity, we write $x_1=1-s\pi^n$, and then $b(s\pi^n, y)=b(s\pi^n, 1-s\pi^n y)=b(s\pi^n, x)$. By Lemma (6.3) we can drop the factor of s so that $b(\pi^n, y)=b(\pi^n, x)$.

In view of the fact that b is of order two,

$$b(z^4, w)=b(z^2, w)^2=1=b(z, w^4)=b(z, w^2)^2=1$$

by Lemma (3.2). Then by Lemma (3.5), $b(z, w)$ depends only on the classes of x and y mod$(k^*)^4$. Now if n above is congruent to 1 mod 4, the equation $b(\pi^n, y)=b(\pi^n, x)$ becomes $b(\pi, x)=b(\pi, y)=1$. On the order hand if $n\equiv 3 \bmod 4$, we see that $b(\pi^3, x)=b(\pi^3, y)$. However for any z we have by the cocycle identity,

$$b(\pi^3, z)b(\pi^2, \pi)=b(\pi^2, \pi z)b(\pi, z).$$

By Lemma (3.2), $b(\pi^2, \pi)=1$ and $b(\pi^2, \pi z)=b(\pi^2, \pi)b(\pi^2, z)=b(\pi^2, z)$, and we find then that $b(\pi^3, z)=b(\pi^2, z)b(\pi, z)$. Now if $z\in H(\pi)$, $b(\pi^2, z)=1$ by our remark above. Thus if we apply this to the equation $b(\pi^3, x)=b(\pi^3, y)$, we deduce that $b(\pi, x)=b(\pi, y)=1$.

This shows that $b(\pi, x)=1$ for any x in the semi-group generated by the elements $1-s\pi^n$, and hence that $b(\pi, x)=1$ for any x in the closure of the semi-group since b is continuous. Since U_1 is compact, the closure of this semi-group is a group, and of course is exactly $H(\pi)$. Thus $b(\pi, x)=1$ for any $x\in H(\pi)$. Now under our hypothesis that $r=1$, and our choice of π, $v^2\in H(\pi)$ where v is any unramified element. Thus $b(\pi, v^2)=1$ and our result follows from Lemma (6.4) when $r=1$.

Now we assume that $r>1$ where p^r is the order of p-primary component of E, the roots of unity in E. In this case $S_0(\mathbf{T})_2\subset S(\mathbf{T})_2$ contains an element c of order exactly four, which is moreover bilinear. Now $c(\pi, v^2)=c(\pi, v)^2=-1$. (It is of order two in the circle group $\mathbf{T}$ and it is not $+1$ for then c would be symmetric by Lemma (6.4).) Now let b be an element of order two in $S(\mathbf{T})$. If $b(\pi, v^2)=1$ for some generator π and some unramified v, we are done by Lemma (6.3), so we can assume that $b(\pi, v^2)=-1$ since b has order two. Then we form $d=bc$, an element of $S(\mathbf{T})_2$, and observe that $d(\pi, v^2)=1$ so that d is symmetric by Lemma (6.4), and hence of order two by Theorem (6.1). Thus $1=d^2=b^2c^2=c^2$ which contradicts the fact that c has order four. This completes the proof of Lemma (6.5).

The following lemma will then complete the proof of Theorem (3.1).

Lemma **(6.6).** — *We have* $S(\mathbf{T})_2 = S_0(\mathbf{T})_2$.

Proof. — Recall that $S_0(\mathbf{T})_2$ is cyclic of order p^r and is contained in $S(\mathbf{T})_2$. We may assume that k has characteristic zero, and also that $r>0$, by virtue of the first statment of Lemma (6.4). Now let $b\in S(\mathbf{T})_2$ and choose π so that $H(\pi)$ has index $n=2^r$ in U_1 by Theorem (5.1). If v is an unramified element, then $(v^2)^m = v^n \in H(\pi)$ where $m=2^{r-1}$.

By the argument of Lemma (6.4), π commutes with $H(\pi)$, so that

$$b(\pi, x^2) = b(\pi^2, x) = 1$$

if $x\in H(\pi)$ (cf. Lemma (3.2)). We contend in fact that $b(\pi, x)=1$ if $x\in H(\pi)$. Let us first note that formula (7) of the appendix, $b(yz^2, x) = b(y, x)b(z^2, x)$, holds for any b. In particular, if $x\in H(\pi)$ and $a=2c+1$ is odd, and $s\in R$, $b(s\pi^a, x) = b(s\pi, x)b((\pi^2)^c, x) = b(\pi, x)b(\pi^2, x)^c = b(\pi, x)$. In order to prove that $b(\pi, x)=1$ if $x\in H(\pi)$, it clearly suffices to show that $b(\pi, x)=1$ if $x=\prod_{i=1}^{r}(1-s_i\pi^{n(i)})$, $n(i)$ odd, $s_i\in R$. We proceed by induction on r starting at $r=0$ (in which case $x=1$). Let $x_0=1-s\pi^a$, a odd, and assume $b(\pi, x)=1$. Then by the above, we have $1 = b(\pi, x) = b(s\pi^a, x) = b(s\pi^a, x_0x) = b(\pi, x_0x)$ which completes the induction.

Returning to our argument, we have $v^n=(v^2)^m\in H(\pi)$, so that

$$b(\pi, v^n) = b(\pi, v^2)^m = 1.$$

Therefore b^m is symmetric by Lemma (6.4) and hence of order two by Theorem (6.1). Thus $b^n=(b^m)^2=1$, and we have shown that any element of $S(\mathbf{T})_2$ has order dividing $n=2^r$.

On the other hand, Lemma (6.5) and Theorem (6.1) together say that the subgroup of $S(\mathbf{T})_2$ of elements with $b^2=1$ is exactly of order two. It follows by elementary group theory that $S(\mathbf{T})_2$ is cyclic of order dividing $n=2^r$. This completes the proof of the Lemma and hence finally the proof of Theorem (3.1).

7) We now turn to uniqueness questions in global class field theory. By a global field k, we shall mean either a finite algebraic extension of the field of rational numbers, or a function field in one variable over a finite field of constants. We denote by v an exponential valuation of k, and k_v the completion of k with respect to v. Then k_v is either Archimedian and hence the real or complex field, or if non-Archimedian is one of the fields discussed in sections 3 through 6. In any case we normalize (as usual) v, as a valuation of k_v as follows: if k_v is real, v is usual absolute value; if k_v is complex, v is the square of the usual absolute value; if k_v is non-Archimedian, and π is a generator of the maximal ideal of the ring of integers in k_v, the normalization of v is determined by $v(\pi)$ which we set equal to $1/q$ where $q=p^n$ is the cardinality of the residue class field of k_v.

Then one has the classical product formula ([2], [5]), $\prod_v v(a)=1$ if $a\in k^*$, where the product is taken over all normalized valuations. One might inquire whether there exists any other such formula; the fact that this is the only such formula is implicit in [5],

but the proof below is rather short so that we shall present it, even though the result is not used later. Namely let us suppose that

$$\prod_v v(a)^{n(v)}=1 \qquad \text{for } a\in k^*$$

where $n(v)$ is a non-negative real number for each valuation v.

Theorem (7.1). — *If* $\prod_v v(a)^{n(v)}=1$ *for* $a\in k^*$, *then* $n(v)=n$ *is independent of* v.

Proof. — Let I be the idèle group of k, i.e. the restricted product [3] of the locally compact groups k_v^* with respect to their compact open subgroups U_v (the units in the ring of integers in k_v). If v is Archimedian, U_v is undefined but this is irrelevant since there are only a finite number of Archimedian v. If $n(v)\geq 0$ for each v, we see that the map φ defined by $\varphi(\alpha)=\prod_v v(a_v)^{n(v)}$, if $\alpha=(a_v)$, of I into the positive multiplicative reals $\mathbf{R}_+^*$ is a continuous homomorphism. Let I_1 denote the closed subgroup of idèles of norm one, (i.e., $\alpha=(a_v)\in I_1$ if and only if $\prod_v v(a_v)=1$). Now $k^*\subset I_0$ by the product formula, and it is basic that k^* is closed and that I_1/k^* is compact. (This is equivalent to the finiteness of class number and the Dirichlet theorem ([2], [3]).) Now our hypothesis is that $\varphi(k^*)=(1)$ and since I_1/k^* is compact, it follows that $\varphi(I_1)=(1)$ since $\mathbf{R}_+^*$ has no non-trivial compact subgroups. Thus we can interpret φ as a homomorphism φ' of I/I_1 into $\mathbf{R}_+^*$. However if $\varphi_0(\alpha)=\prod_v v(a_v)$ when $\alpha=(a_v)$, then φ_0 defines in the same way a homomorphism φ_0' of I/I_1 into $\mathbf{R}_+^*$ which is injective by definition of I_1. On the other hand, the image of φ_0' is all of $\mathbf{R}_+^*$ if k is a number field or the group $\{(p^n)^m,\ m\in\mathbf{Z}\}$ if k is a function field and p is the characteristic of the constant field. In either case φ_0' is a topological isomorphism onto its range, and it is absolutely clear that any other continuous homomorphism φ' of I/I_1 into $\mathbf{R}_+^*$ is of the form $\varphi'=(\varphi_0')^n$ for some non-negative real number n. It is now clear that $n=n(v)$ where $\varphi(\alpha)=\prod_v v(a_v)^{n(v)}$, as desired.

Remark. — This proof makes it evident that the compacity of the group I_1/k^* is the key factor in the uniqueness of the product formula, since a compact group, or more generally a locally compact group which is a union of compact subgroups, admits no non-trivial continuous homomorphisms into $\mathbf{R}_+^*$.

The uniqueness theorems which will be of interest to us in the sequel concern the reciprocity law of global class field theory. The fundamental result in the local case applied to each completion k_v is the existence of a continuous homomorphism (the reciprocity homomorphism) φ_v of k_v^* into G_v^a, the Galois group of the maximal abelian extension of k_v [33], such that the range of φ_v is dense, and φ_v has kernel equal to the connected component of k_v^*. Then one notes that if G^a is the Galois group of the maximal abelian extension of k, our global field, then G_v^a may be viewed as a subgroup of G^a [3]. Moreover if $\alpha\in I$, one may define $\varphi(\alpha)=\prod_v \varphi_v(a_v)$ if $\alpha=(a_v)$ since only a finite number of terms are unequal to 1. It is clear that φ_v vanishes on the connected component of k_v^* and hence that φ vanishes on the connected component I_0 of I. The Artin reciprocity law ([3], [33]), says that $\varphi(k^*)=(1)$ where $k^*\subset I$, and moreover that φ defines a continuous

injection of $C = I/\overline{I_0 . k^*}$ into G^a. In characteristic zero, this map is a topological isomorphism. Also in this case, $I = I_0 . I_1$, so that $C = I_1/\overline{(I_0 \cap I_1) . k^*}$ is the connected component of I_1/k^*, so that C is compact totally disconnected. In characteristic $p \neq 0$, $I_0 = (0)$, and the range of φ is dense in G^a. More precisely φ is a topological isomorphism of I_1/k^* onto the subgroup of G^a fixing the algebraic closure of the finite field of constants in k, and φ maps I/I_1, which as a group is the integers, onto the obvious dense subgroup of the Galois group of the algebraic closure of the constant field.

Now we let E_v be the group of roots of unity in k_v, and we let $n(v)$ denote its order with obvious conventions if k_v is complex. Then Kummer theory [3] yields an isomorphism, s_v, of $(k_v^*)/(k_v^*)^{n(v)}$ onto $\mathrm{Hom}(G_v^a, E_v)$; if $a, b \in k_v^*$, $(a, b)_v = s_v(\dot{b})(\varphi_v(a))$, where $\dot{a}$ is the class of a in $k_v^*/(k_v^*)^{n(v)}$, is a bilinear function from $k_v^* \times k_v^*$ into E_v which is by definition the norm residue symbol we have discussed previously. Let E denote the group of roots of unity in the global field k, and let n be its order. Since $E \subset E_v$ for all v, $n \mid n(v)$ and so define $m(v) = n(v)/n$; we observe that the map $f(v)$ of raising to the power $m(v)$ in E_v, maps E_v onto E. We let $b_v(x, y) = f(v)((x, y)_v)$ so that b_v is a map of $k_v^* \times k_v^*$ into E. A corollary of the reciprocity law is the reciprocity formula which says that $\prod_v b_v(x, y) = 1$ if $x, y \in k^*$ [33]. We shall be simultaneously concerned with the uniqueness of the reciprocity map φ of I into G^a and with the uniqueness of the reciprocity formula.

Theorem **(7.2).** — *Let $p(v)$ be an integer for each completion v of k and let $g(v)$ be the map of* E *into itself of raising to the power $p(v)$. Then if $\prod_v g(v)(b_v(x, y)) = 1$, there exists p so that $p(v) \equiv p \pmod{n}$ for all non-complex places.* (i.e. *$g(v) = g$ is independent of v for all non-complex places. Note that $b_v = 1$ if v is complex so that the value of $p(v)$ is irrelevant.)*

Theorem **(7.3).** — *Let φ_v be the local reciprocity map of k_v^* into G_v^a and let $p(v)$ an integer for each v. Then let $\varphi'(\alpha) = \prod_v (\varphi_v(a_v))^{p(v)}$ be the corresponding homomorphism of* I *into* G^a. *If $\varphi'(k^*) = (1)$, then there exists an integer p such that $p(v) = p$ for all non-Archimedian v and $p(v) \equiv p \pmod{2}$ for real v. (Again the value $p(v)$ for v complex is irrelevant as $\varphi_v = 1$ in this case.)*

We note that Theorem (7.3) says that the only global reciprocity mapping that can be constructed out of the local ones are the powers of the usual global reciprocity homomorphism. Theorem (7.2) says similarly that the only identities relating the norm residue symbols $b_v(x, y)$ for n^{th} roots of unity in the various completions of k, are powers of the known one. One may raise a more general uniqueness question concerning the norm residue symbols. That is, suppose that $h(v)$ is a homomorphism of E_v into the circle group **T**, and suppose that $\prod_v h(v)((a, b)_v) = 1$, $a, b \in k^*$, where $(\ ,\ )_v$ is the norm residue symbol for $n(v)^{\text{th}}$ roots of unity in k_v. Theorem (7.2) treats the case when $h(v) = g(v)f(v)$ where $f(v)$ is the map $E_v \to E$ given by raising to the power $m(v) = n(v)/n$ and where $g(v)$ is a homomorphism of E into **T**, where we view E as a subgroup of **T**. The general theorem is also valid.

Theorem **(7.4).** — *If $\prod_v \varphi(v)((a, b)_v) = 1$ for all $a, b \in k^*$, then $\varphi(v) = g(v)f(v)$ for some homomorphisms $g(v)$ of* E *into itself (equivalently into* **T***), and hence $g(v)$ is the map of raising to the m^{th} power for some m for every non-complex v (by Theorem* (7.2)).

This result says that the only relations among the norm residue symbols for $n(v)^{\text{th}}$ roots of unity for the various completions are the powers of the reciprocity formula. The proof of Theorem (7.4) involves in an essential way the ideas of [9] and [10]. We note here that Theorems (7.2) and (7.4) are the results that allow us to compute the relative fundamental groups $\pi_1(\mathrm{SL}_2(\mathrm{A}), \mathrm{SL}_2(k))$ where A is the ring of adeles of the global field k.

We now proceed to the proofs of Theorems (7.2) and (7.3). In both cases we are given integers $p(v)$, one for each completion k_v of k. We form the mapping ψ of I into I given on an idèle $\alpha=(a_v)$ by $\psi(\alpha)=(a_v^{p(v)})$. It is clear that ψ is a continuous homomorphism of I into itself. Clearly I_0, the connected component of I is sent into itself by ψ. On the other hand, the multiplicative group k^* of k is a subgroup of I, and it is absolutely clear that the hypothesis of Theorem (7.3) is equivalent to the assertion that $\psi(k^*)\subset\overline{k^*.\mathrm{I}_0}$ in view of the Artin reciprocity law (i.e., that $\mathrm{C}=\mathrm{I}/\overline{\mathrm{I}_0.k^*}$ is injected into G^a by the Artin reciprocity map).

Furthermore, let us denote by I_m the subgroup of I consisting of m^{th} powers where m is an integer. It is well known that $\overline{\mathrm{I}_0.k^*}=\bigcap_m(\mathrm{I}_m.k^*)$ since $\mathrm{I}_m.k^*$ is closed in I [3]. Thus the hypothesis of Theorem (7.3) is also equivalent to the assertion that $\psi(k^*)\subset k^*.\mathrm{I}_m$ for every m. We claim now that the hypothesis of Theorem (7.2), namely that $\prod_v b_v(x,y)^{p(v)}=1$ for x and $y\in k^*$, is equivalent to the assertion that $\psi(k^*)\subset k^*.\mathrm{I}_n$ where n is the order of E, the group of roots of unity in k. Indeed, let $x\in k^*$, and let λ be any element of $\mathrm{Hom}(\mathrm{G}^a, \mathrm{E})$. Now as above, Kummer theory yields an isomorphism s of $k^*/(k^*)^n$ onto $\mathrm{Hom}(\mathrm{G}^a, \mathrm{E})$ so that λ is of the form $s(\dot{y})$ for some $y\in k^*$, where the dot indicates the class of y mod n^{th} powers. Now if φ is the global reciprocity map of I into G^a, it is perfectly clear from the definition of b_v above and class field theory [3], that

$$1=\prod_v b_v(x,y)^{p(v)}=\prod_v b_v(x^{p(v)},y)$$
$$=s(\dot{y})(\varphi(\psi(x)))=\lambda(\varphi(\psi(x))).$$

Therefore every character of order dividing n of G^a vanishes on $\varphi(\psi(x))$, and so $\varphi(\psi(x))$ is an n^{th} power in G^a. Since φ is an injective map of C into G^a and $\mathrm{G}^a/\varphi(\mathrm{C})$ is torsion free, this says that $\psi(x)\in k^*.\mathrm{I}_n$ as desired.

Now we let $\mathrm{C}^m=\mathrm{I}/k^*.\mathrm{I}_m$ for any m, and observe that C^m is exactly C modulo the subgroup C_m of its m^{th} powers. If $\psi(k^*)\subset k^*.\mathrm{I}_m$, then clearly $\psi(k^*.\mathrm{I}_m)\subset k^*.\mathrm{I}_m$ so that ψ induces a homomorphism ψ_m of C^m into itself.

Lemma (7.1). — *Suppose that* $\psi(k^*)\subset \mathrm{I}_m.k^*$ *so that* ψ_m *is defined. Then if* U *is any closed subgroup of finite index in* $\mathrm{C}^m=\mathrm{I}/\mathrm{I}_m.k^*$, $\psi(\mathrm{U})\subset\mathrm{U}$.

Proof. — Let U′ be the inverse image of U in C so that U′ is a closed subgroup of finite index (dividing m) in C. Then by the existence theorem, there exists a (unique) finite abelian extension K of k such that U′ consists of the norms from K to k. Now for each completion k_v we have an abelian extension K_v of k_v which is a completion of K. The norm group $\mathrm{N}_v\subset k_v^*$ of norms from K_v is independent of the choice of K_v; moreover

from the definitions of global class field theory, $U' = k^*.(\prod_v N_v)/k^*.I_0$. In order to show that $\psi_m(U) \subset U$ it clearly suffices to show that $\psi(k^*.\prod_v N_v) \subset k^*.\prod_v N_v$, and this is clear since $\prod_v N_v \supset I_m$ (K_v is of degree dividing m over k_v), and since $\psi(k^*) \subset k^*.I_m$, and since $\psi(\prod_v N_v) = \prod_v N_v^{p(v)} \subset \prod_v N_v$.

Thus we must study a homomorphism ψ_m of C^m such that ψ_m maps every closed subgroup of finite index into itself. In other words we have an endomorphism α of a pro-finite abelian group A such that $\alpha(U) \subset U$ for every closed subgroup of finite index. We note that any such A is a $\mathbf{Z}^*$-module where $\mathbf{Z}^*$ denotes the compact ring of supernatural numbers (the completion of the integers $\mathbf{Z}$ at all ideals). We write this action as $(n, x) \mapsto x^n$, $x \in A$, $n \in \mathbf{Z}^*$, and note that the continuous endomorphism $x \mapsto x^n$ sends every closed subgroup of finite index of A into itself. The following lemma says that these are the only such continuous endomorphisms with this property.

Lemma (7.2). — *Let* A *be a profinite abelian group and* α *a continuous endomorphism such that* $\alpha(U) \subset U$ *for every closed subgroup of finite index in* A. *Then there exists a supernatural number* n *such that* $\alpha(x) = x^n$.

In order not to interrupt the continuity of argument, we defer this proof until the end and proceed with the proofs of Theorems (7.2) and (7.3). Then Lemmas (7.1) and (7.2) tell us that whenever ψ_m is defined, $\psi_m(x) = x^s$ for some supernatural number s. Since C^m is a torsion group (of exponent m), it follows that we can choose s to be an integer, whose residue modulo m is uniquely determined. Thus if ψ_m is defined, $\psi_m(x) = x^s$ for some integer s, for all $x \in C^m$.

Now we have seen that the hypotheses of Theorem (7.2) imply that ψ_n is defined where n is the order of E, the roots of unity in k. We lift the previous result back to the idèle group I, and deduce that if $\alpha \in I$, then $\psi(\alpha) = \alpha^s.x^n.t_\alpha$ for some $x \in I$, and $t_\alpha \in k^*$. Now if $\alpha = (a_v)$, recall that $\psi(\alpha) = (a_v^{p(v)})$ so that $a_v^{p(v)} = a_v^s x_v^n.t_\alpha$ with $t_\alpha \in k^*$. We are trying to show that $p(v) \equiv p \pmod n$ for some p and every non-complex place v; we in fact claim that $p(v) \equiv s \pmod n$. Suppose that $p(v) \not\equiv s \pmod n$ for some non-Archimedian v. Now define an idèle α, by $a_v = \pi$ where π is a generator of the maximal ideal $\mathfrak{p}_v$, and $a_u = 1$ if $u \neq v$. Then by the above, for every $u \neq v$, we have $1 = 1.x_u^n.t_\alpha$ and so the element t_α has an n^{th} root in all completions k_u for $u \neq v$. Since n is the order of E, Grünwald's theorem ([3], p. 96) applies with no exceptional case, and it follows that t_α has an n^{th} root in k. However in the completion k_v, $\pi^{p(v)} = \pi^s.x_v^n.t_\alpha$ and since $p(v) \not\equiv s \bmod n$, it is clear that t_α does not have an n^{th} root in k_v. This contradiction shows that $p(v) \equiv s \pmod n$ for all non-Archimedian v.

If k_v is a real completion of k, it follows necessarily that $n = 2$. Then if $p(v) \not\equiv s \bmod 2$, we define an idèle α by $a_v = -1$ and $a_u = 1$ if $u \neq v$. The same argument as above leads to the same contradiction, and hence Theorem (7.2) is proved.

We now consider Theorem (7.3); we have seen that the hypotheses of this theorem imply that ψ_m is defined for all m, and hence that for each m, there exists an integer $s(m)$ such that $\psi(x) = x^{s(m)}$ for $x \in C^m$, or equivalently that for each $\alpha = (a_v) \in I$,

$a_v^{p(v)} = a_v^{s(m)} . x^m . t_\alpha$ with $x \in \mathrm{I}$ and $t_\alpha \in k^*$. If m is odd, and k_v non-Archimedian, we claim that $p(v) \equiv s(m) \pmod m$, for if not, define an idèle α by $a_v = \pi$, a generator of the maximal ideal, and $a_u = 1$ if $u \neq v$. It follows as before that t_α has an m^{th} root in all completions k_u except for $u = v$. Since m is odd, Grünwald's theorem ([3], p. 96) applies with no exceptional case, and says that t_α has an n^{th} root in k. We obtain the same contradiction as before in the completion k_v. Thus we conclude that $p(v) \equiv s(m) \pmod m$ if v is non-Archimedian; hence if v and v' are non-Archimedian, $p(v) \equiv p(v') \pmod m$ for every odd integer m. It follows immediately that $p(v) = p(v')$, and hence that $p(v) = p$ for some integer p for every non-Archimedian v. It remains to see that $p(v) \equiv p \pmod 2$ if k_v is real, and this is proved in exactly the same way as in Theorem (7.2).

We conclude this argument with the proof of Lemma (7.2); this lemma was stated without proof in the course of the argument above. We remark that in a sense this lemma is a version of the fundamental theorem of projective geometry. We have now a profinite abelian group A and a continuous endomorphism α such that $\alpha(\mathrm{U}) \subset \mathrm{U}$ for any closed subgroup U of finite index in A. We want to know that $\alpha(x) = x^t$ for some supernatural number $t \in \mathbf{Z}^*$. We denote by B the dual group of A, and by β the dual endomorphism defined by $\beta(b)(a) = b(\alpha a)^{-1}$ for $b \in \mathrm{B} = \hat{\mathrm{A}}$. Then B is a discrete torsion group and the hypothesis on α translates by duality into the hypothesis that $\beta(\mathrm{F}) \subset \mathrm{F}$ for every finite subgroup F of B. We notice that B, being a torsion group, is a module for $\mathbf{Z}^*$ and that this module structure is compatible with duality. Thus it suffices to show that $\beta(b) = b^t$ for some $t \in \mathbf{Z}^*$.

Now if $x \in \mathrm{B}$, the group generated by x is a finite cyclic group of order $o(x)$. It follows then that $\beta(x) = x^{m(x)}$ for some integer $m(x)$ which is uniquely determined mod $o(x)$. Let B_n denote the subgroup of all elements in B of order dividing $n!$ so that B_n is a group of finite exponent $k(n)$ dividing $n!$. Let x be an element of order $k(n)$; then $\beta(x) = x^m$ for some integer $m = m(x)$ unique modulo $k(n)$. If y is a power of x, then of course $\beta(y) = y^m$. On the other hand if $y \in \mathrm{B}_n$ is not a power of x, then the finite group F generated by x and y has a basis of two elements, one of which can be chosen to be x and the other to be of the form $z = x^a y$. Every element of F is of the form $x^s y^t$ and $x^s z^t = 1$ if and only if $s \equiv 0 \bmod k(n)$ and $t \equiv 0 \pmod{o(z)}$, the order of z. Now $\beta(xz) = (xz)^{m(xz)} = x^{m(xz)} z^{m(xz)} = \beta(x)\beta(z) = x^m z^{m(z)}$. Thus we must have $m(xz) \equiv m \bmod k(n)$, and $m(xz) \equiv m(z) \pmod{o(z)}$. Thus $m \equiv m(z) \pmod{o(z)}$ since $o(z) \mid k(n)$, and consequently $\beta(z) = z^m$. Now $y = zx^{-a}$, so $\beta(y) = z^m x^{-am} = y^m$ and hence $\beta(y) = y^m$ for any $y \in \mathrm{B}_n$.

Note that $\mathrm{B}_n \subset \mathrm{B}_{n+1}$ and that $\bigcup_n \mathrm{B}_n = \mathrm{B}$ since B is a torsion group. Moreover $k(n) \mid k(n+1)$; we have shown above that there is for each n an integer $m(n)$, unique modulo $k(n)$, such that $\beta(x) = x^{m(n)}$ for $x \in \mathrm{B}_n$. Now as $\mathrm{B}_n \subset \mathrm{B}_{n+1}$, we also have $\beta(x) = x^{m(n+1)}$ for $x \in \mathrm{B}_n$ and hence $m(n+1) \equiv m(n) \pmod{k(n)}$. It follows essentially from the definition of $\mathbf{Z}^*$ that there exists at least one supernatural number t such

that $t=m(n)$ modulo the ideal $k(n)\mathbf{Z}^*$ of $\mathbf{Z}^*$ for every n. (Note that t will be unique if and only if the sequence $k(n)$ is cofinal in the sense of divisibility; that is every integer a eventually divides $k(n)$.) It follows that if $x\in B_n$, $\beta(x)=x^{m(n)}=x^t$ since $t\equiv m(n) \pmod{k(n)}$, and hence $\beta(x)=x^t$ for all $x\in B$. This completes the proof of the lemma.

We conclude now with the proof of Theorem (7.4). Recall that we are given a global field k with completions k_v and homomorphisms $\varphi(v)$ of E_v (the roots of unity in k_v) into the circle group $\mathbf{T}$ such that $\prod_v \varphi(v)((a, b)_v)=1$, $a, b\in k^*$, where $(\ ,\ )_v$ is the norm residue symbol for $n(v)^{\text{th}}$ roots of unity in k_v ($n(v)$ being the order of E_v). For notational convenience let us agree that $E_v=(0)$ if v is complex so that we are really dealing with E_v modulo its maximal divisible subgroup. Let n be the order of E, the roots of unity in k. We want to show that $\varphi(v)^n=1$ so that $\varphi(v)$ takes values in a cyclic subgroup of order n.

Let S_∞ be the set of Archimedian places, and let S be a finite non-void subset of V, the set of all places, which contains S_∞. We let $\mathfrak{O}(S)=\{x \mid x\in k, v(x)\leq 1 \text{ for } v\notin S\}$. Then $\mathfrak{O}(S)$ is a Dedekind domain, and its maximal ideals are in one-one correspondence with the places v not in S; to be precise $\mathfrak{p}_v=\{y \mid y\in\mathfrak{O}(S), v(y)<1\}$ is the maximal ideal corresponding to v [10]. Now let $\mathfrak{q}$ be a non-zero ideal in $\mathfrak{O}(S)$ and let W_q be the set $\{(a, b) : a, b\in\mathfrak{O}(S), (a, b)\equiv(1, 0) \bmod q, \text{ and } a.\mathfrak{O}(S)+b.\mathfrak{O}(S)=\mathfrak{O}(S)\}$, (see [10]). A Mennicke symbol [10] is a function $M(a, b)$ defined on W_q into a group C such that the following conditions hold:

MS 1. *a)* $M(1, 0)=1$.
b) $M(a, b)=M(a, b+ta)$ if $t\in\mathfrak{q}$.
c) $M(a, b)=M(a+tb, b)$ if $t\in\mathfrak{O}(S)$.

MS 2. $M(a, b_1)M(a, b_2)=M(a, b_1b_2)$.

The following line of argument is really just a trivial modification of the technique in [10]. If $a\in\mathfrak{O}(S)$, let $D(a)$ denote the set of its prime factors; that is, those v dividing a, or $v(a)>1$. Given the hypotheses of the theorem and an ideal $\mathfrak{q}$, define for $(a, b)\in W_q$, $M(a, b)=\prod_v \varphi(v)((b, a)_v)$ $(v\in D(a))$, with the convention that $M(a, 0)=1$. This is a function from W_q into the circle group which we claim will be a Mennicke symbol under appropriate conditions. To be precise, let F be the finite set of places where E_v has order divisible by the characteristic of the residue class field at v. ($F=\emptyset$ for function fields.) We claim that there is an ideal $\mathfrak{q}$ containing only primes in F such that if $v\notin S$, and x and y are elements of $\mathfrak{O}(S)$ which are units at v (i.e. $v(x)=v(y)=1$) with $x\equiv y \bmod(\mathfrak{q}\cap\mathfrak{p}_v)$, then $(x, z)_v=(y, z)_v$ for all z. Indeed if $v\notin F$, it is clear that if $x\equiv 1 \bmod \mathfrak{p}_v$ then $(x, z)_v=1$. If $v\in F$, it is clear that we can find an integer $a(v)\geq 1$ such that if $x\equiv 1 \bmod a(v)$, then $(x, z)_v=1$. Thus it suffices to take $\mathfrak{q}=\prod_v \mathfrak{p}_v^{a(v)}$ $(v\in F)$, and in particular $\mathfrak{q}=\mathfrak{O}(S)$ is the unit ideal if k is a function field.

Lemma **(7.3)**. — *If* $\mathfrak{q}$ *is as above and if* $\varphi(v)=1$ *for* $v\in S$, *and if the hypothesis of Theorem* (7.4) *holds, then* M *is a Mennicke symbol on* $W_\mathfrak{q}$.

Proof. — MS 1 *a)* is clear by definition, and MS 2 is also clear from the formula for M. Also if $a, b \in W_q$, and $t \in q$, then $M(a, b+ta) = \prod_v \varphi(v)((b+ta, a)_v)$ $(v \in D(a))$. Now if $v \in D(a)$, b is a unit at v since a and b are relatively prime and since $a \in \mathfrak{p}_v$, and $D(a) \cap F = \emptyset$, $ta \in q\mathfrak{p}_v = q \cap \mathfrak{p}_v$. Thus by the choice of q, $(b+ta, a)_v = (b, a)_v$ and MS 1 *b)* is established.

Finally we consider MS 1 *c)*. By the assumed " reciprocity formula " of the hypothesis of the theorem and skew symmetry of $(a, b)_v$, $M(a, b) = \prod_v \varphi(v)((a, b)_v)$, $v \in V - D(a)$. We decompose $V - D(a)$ into the disjoint union $V - D(a) = (D(b) - F) \cup F \cup S \cup H$ where H is the complement of the first three sets. (Note that $D(a) \cap D(b) = \emptyset$ since a and b are relatively prime.) Then $M(a, b) = M_1 . M_2 . M_3 . M_4$ where the four factors represent the products taken over the four sets above. If $v \in H$, a and b are units at v and $v \notin F \cup S$ so that $(a, b)_v = 1$ so $M_4 = 1$. If $v \in S$, then $\varphi(v) = 1$ by the hypothesis of the lemma so that $M_3 = 1$. Finally if $v \in F$, $a \equiv 1 \bmod q$ and since $q = q \cap \mathfrak{p}_v$ as $\mathfrak{p}_v \supset q$ (recall that F is void for a function field), we see that $(a, b)_v = 1$. Thus $M_2 = 1$, and we see that $M(a, b) = \prod_v \varphi(v)((a, b)_v)$ $(v \in D(b) - F)$, with obvious conventions if $b = 0$.

If $t \in \mathfrak{O}(S)$ then

$$M(a+tb, b) = \prod_v \varphi(v)((a+tb, b)_v) \quad (v \in D(b) - F).$$

But now if $v \in D(b) - F$, a is a unit at v and $b \in \mathfrak{p}_v$ and also $b \in q$ by definition of W_q. Thus $a + tb \equiv a \bmod q \cap \mathfrak{p}_v$ and so $(a+tb, b)_v = (a, b)_v$. Now MS 1 *c)* is established, and so the lemma is proved.

We now turn to the proof proper of Theorem (7.4). Let k be a number field; and let $S = S_\infty$. If k is totally imaginary $\varphi(v) = 1$ for all $v \in S$ automatically so that M is a Mennicke symbol on W_q. It is shown in [9] (see also [10]) that any such symbol has order dividing n, the order of the roots of unity in k. Thus $M^n = 1$. If now k is not totally imaginary, then E_v has order dividing two for each $v \in S$, and upon replacing $\varphi(v)$ by $\varphi(v)^2$ for every v, we see that the hypothesis of the lemma is satisfied. Thus M^2 is a Mennicke symbol on W_q. However, it is shown in [9] (see also [10]) that any such Mennicke symbole is trivial. Thus $M^2 = 1$, but we note that $n = 2$ since k has a real place so that $N = M^n = 1$ for a number field.

Thus if we set $\psi(v) = \varphi(v)^n$, we see that $N(a, b) = \prod_v \psi(v)((a, b))_v = 1$ $(v \in D(a))$ for every $a, b \in W_q$. We shall deduce that $\psi(v) = 1$, which will prove our theorem for number fields. The Dirichlet theorem will be useful here and we refer to [10], A.10, for a convenient formulation of this result. Since $\psi(v) = 1$ if $v \in S$, by construction, we fix a $v \notin S$ with $v \notin F$. We can find by the Dirichlet theorem a $u \notin F$ $(u \neq v)$ such that $\mathfrak{p}_u \mathfrak{p}_v = a . \mathfrak{O}(S)$ is a principal ideal, and such that a is congruent to 1 modulo q. Thus $D(a)$ consists of the points u and v so if b is a unit at u and v and is in q, $(a, b) \in W_q$ and we see that $\psi(v)((a, b)_v)\psi(u)((a, b)_u) = 1$. Again by the Dirichlet theorem we can find a $b \in q$ such that $b \equiv 1 \bmod \mathfrak{p}_u$ and such that the image of b in $\mathfrak{O}(S)/\mathfrak{p}_v$ is a generator of the multiplicative group of this field. Then $(a, b)_u = 1$ by construction since $u \notin F$,

and so $\psi(v)((a, b)_v)=1$. However by construction and properties of the local symbol, $(a, b)_v$ is a primitive $n(v)^{\text{th}}$ root of 1 in E_v. Thus $\psi(v)=1$ for $v\notin F$.

Now the n^{th} power of the alleged reciprocity formula in the statement of the theorem reads $\prod_v \psi(v)((a, b)_v)=1$ $(v\in F)$. Let k_F^* denote the product of the local fields k_v^*, $v\in F$. Then k^* is injected diagonally into k_F^*, and the image is dense by the Dirichlet theorem (i.e. weak approximation). Since $\psi(v)((a, b)_v)$ is continuous on $k_v^*\times k_v^*$, it follows by density that $\prod_v \psi(v)((a_v, b_v)_v)=1$ $(v\in F)$ where a_v and b_v are arbitrary elements of k_v^*. It is clear now that $\psi(v)=1$ for $v\in F$ as desired. This completes the proof for number fields.

Now let k be a function field. We choose S to consist of a single point v and denote by $n(v)$ the order of E_v. We now define $\psi(w)=\varphi(w)^{n(v)}$ for all $w\in V$. Then the lemma applies to $M(a, b)^{n(v)}$ with $\mathfrak{q}=\mathfrak{O}(S)$ the unit ideal since $\psi(v)=1$. Now it is shown in [9] (see also [10]) that any Mennicke symbol on $W_{(1)}$ is trivial so that we deduce that $M(a, b)^{n(v)}=1$. We can apply exactly the same argument using the Dirichlet theorem as in the case of a number field. The conclusion is that $\psi(w)=\varphi(w)^{n(v)}=1$ for $v\neq w$. (Note that F is void, and note that $\varphi(v)^{n(v)}=1$ by construction.) Now if $m=\text{g.c.d.}(n(v))$, $\varphi(v)^{n(v)}=1$ implies that $\varphi(v)^m=1$ for all v. On the other hand $m=n$ is the order of E the roots of unity in k, see [3], p. 12. This completes the proof of the theorem.

CHAPTER III

8) Let k be a field and let G be a simply connected simple Chevalley group ([12], [15], [1]). We denote by G_k the group of points of G in k. Among these groups one has SL_n, the unimodular group, Sp_n the group of $2n \times 2n$ matrices preserving a non-degenerate skew-two form, and $Spin_n$, the spin group of a quadratic form of maximal Witt index. With the exception of $SL_2(Z_2)$, $SL_2(Z_3)$, $Sp_2(Z_2)$ and $G_2(Z_2)$ [15], where Z_n is the field of n elements, all of the groups G_k are equal to their own commutator subgroups. Therefore G_k with these exceptions has a fundamental group, $\pi_1(G_k)$. We note that the groups G_k are simply connected as algebraic groups; that is, they have no algebraic coverings, but they certainly might have non-trivial covering groups as abstract groups; or when k is a topological field, they may have non-trivial topological coverings. One point of view is then that $\pi_1(G_k)$ will reflect properties of the field k, and the fact that it might be non-zero reflects some properties of k. Note that if $k = \mathbf{C}$ the complex numbers, then $G_{\mathbf{C}}$ is simply connected as topological group, whereas if k is the real field $G_{\mathbf{R}}$ is not simply connected. In [40], Steinberg shows that $\pi_1(G_k) = 0$ if k is a finite field, at least if we exclude a few fields of low cardinality.

In fact in [40], Steinberg gives an explicit construction for the universal covering group $E(G_k)$ of G_k if one excludes again some small finite fields (to be precise, the cardinality of k must be greater than 4, and in an addition unequal to 9 if $G = SL_2$). He constructs these groups as extensions of G_k/Z where Z is the center of G_k, but in fact the same group $E(G_k)$ will be the universal covering of G_k by Lemma (1.6). These results of Steinberg clearly supplied the motivation for the general discussion in Chapter I (1).

By construction of G as group scheme over $\mathbf{Z}$ [16] we have a split Cartan subgroup H of G_k; we also fix an ordering on the roots of G_k with respect to H. Thus we have distinguished nilpotent subgroups U_+ corresponding to the positive roots, and U_- corresponding to the negative roots. To be precise, each root α determines a one dimensional unipotent subgroup of G_k : $\{x_\alpha(t),\ t \in k\}$, so that $t \mapsto x_\alpha(t)$ is a homomorphism of k into G_k ([12], [15]). Then $U_\pm$ is the group generated by $x_\alpha(t)$, $\alpha > 0$ (resp. $\alpha < 0$). Now G_k is generated by the elements $x_\alpha(t)$, $\alpha \in \Sigma$ (the root system) and $t \in k$. Moreover, one has

A) $x_\alpha(t+s) = x_\alpha(t)x_\alpha(s)$ and

B) $[x_\alpha(t), x_\beta(s)] = \prod x_{i\alpha+j\beta}(N_{\alpha,\beta,i,j}t^i s^j)$ if $\alpha + \beta \neq 0$, where the product is taken of all roots of the form $i\alpha + j\beta$ arranged in dictionary order and $N_{\alpha,\beta,i,j}$ are certain integers.

---

(1) In fact an appropriate title for this entire paper would be " Variations on a theme of Steinberg ".

If $G=SL_2$, then B) is vacuous and is replaced by B') below. For any root α, define $w_\alpha(t)=x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$ and then

B') $w_\alpha(t)x_\alpha(s)w_\alpha(t)^{-1}=x_{-\alpha}(-st^{-2})$ if $G=SL_2$.

One defines $h_\alpha(t)=w_\alpha(t)w_\alpha(1)^{-1}$ and then

C) $h_\alpha(t)h_\alpha(s)=h_\alpha(ts)$ holds.

Now Steinberg [40] shows that in fact G_k is the group generated by $x_\alpha(t)$ subject to exactly these relations A), B) (B') if $G=SL_2$) and C). Then one defines the group $E(G_k)$ to be the group generated by objects which we denote by $x'_\alpha(t)$ subject to the same relations A) and B) (or B')), but not C). There is clearly a unique homomorphism φ of $E(G_k)$ onto G_k such that $\varphi(x'_\alpha(t))=x_\alpha(t)$ for every $\alpha\in\Sigma$ and $t\in k$. Steinberg [4] shows that $E(G_k)$ is simply connected and that the kernel of φ is central in E_k. Hence $E(G_k)$ is the universal covering group of G_k and the kernel of φ is just $\pi_1(G_k)$.

Let $U'_\pm$ denote the subgroup of $E(G_k)$ generated by the elements $x'_\alpha(t)$, $\alpha>0$, (resp. $x'_\alpha(t)$, $\alpha<0$). Then Steinberg shows that φ restricted to $U'_\pm$ is an isomorphism onto $U_\pm$. Moreover we have elements $w'_\alpha(t)$, $h'_\alpha(t)$ of $E(G_k)$ defined by the same formulas, and we let H' be the subgroup generated by the elements $h'_\alpha(t)$, $\alpha\in\Sigma$, $t\in k^*$, and N' be the subgroup generated by the elements $w'_\alpha(t)$, $\alpha\in\Sigma$, $t\in k^*$. Then H is normal in N [40], and $W=N'/H'\simeq N/H$, where N is the group generated by $w_\alpha(t)$, $\alpha\in\Sigma$, $t\in k^*$. Then W is the Weyl group of G relative to H, and we choose representatives $w'(\sigma)$ ($\sigma\in W$) for the cosets of H' in N', and for simplicity if σ is a reflection in a positive root α, we take $w'(\sigma)=w'_\alpha(1)$. Let $\varphi(w'(\sigma))=w(\sigma)$ be the images of these elements in G_k. Now let Π denote the set of simple roots in our ordering on Σ. Then every element of H can be uniquely written as $\prod_\alpha h_\alpha(t_\alpha)$ ($\alpha\in\Pi$, $t_\alpha\in k^*$) ([40], p. 122).

On the basis of these choices we want to define a cross section s of G_k into $E(G_k)$, that is $s(g)$ will be an element of $E(G_k)$ such that $(\varphi\circ s)(g)=g$. If $\sigma\in W$, let U_σ be the subgroup of U_+ generated by the $x_\alpha(t)$ such that $\alpha>0$ and $\sigma(\alpha)<0$. Then G_k has a Bruhat decomposition ([15], [40]); namely each element g is uniquely of the form $g=u_\sigma.w(\sigma).h.u$ where $u_\sigma\in U_\sigma$, $h\in H$, and $u\in U_+$. For fixed σ, the set of such elements is the double coset $Bw(\sigma)B$ where $B=H.U_+$. Now we observed that $\varphi: E(G_k)\to G_k$ is an isomorphism of U'_+ onto U_+. We denote its inverse on U_+ by s. Also $h=\prod_\alpha h_\alpha(t_\alpha)$, $\alpha\in\Pi$, $t_\alpha\in k^*$, and we define $s(h)=\prod_\alpha h'_\alpha(t_\alpha)\in H'$. Then one defines for $g=u_\sigma.h.w(\sigma).u$, $s(g)=s(u_\sigma)s(h)w'(\sigma)s(u)$ so that s is a well defined map of G_k into $E(G_k)$ with $\varphi\circ s=\mathrm{id}$.

Now for g_1 and $g_2\in G$, $b(g_1,g_2)=s(g_1)s(g_1g_2)^{-1}$ is an element of the kernel of φ, that is $\pi_1(G_k)$, and moreover b is an element of $Z^2(G_k,\pi_1(G_k))$ whose class is the universal covering $E(G_k)$ of G_k. If A is any abelian group and if λ is a homomorphism of $\pi_1(G_k)$ into A, then $\lambda\circ b$ is clearly an element of $Z^2(G_k,A)$, and by Chapter I, if $(\lambda\circ b)'$ is the class of $\lambda\circ b$, the map $\lambda\mapsto(\lambda\circ b)'$ is the isomorphism of $\mathrm{Hom}(\pi_1(G_k),A)$ with $H^2(G_k,A)$ described in Theorem (1.1). We shall call the cocycles $\lambda\circ b$, *Steinberg cocycles* on G.

Recall that H' is the subgroup of $E(G_k)$ generated by the elements $h'_\alpha(t)$, and recall that Steinberg [40] shows that $\pi_1(G_k)\subset H'$. Now for any $\alpha\in\Sigma$, let

$h'_\alpha(t)h'_\alpha(s)=b_\alpha(t,s)h'_\alpha(ts)$; it is evident from the defining relation C) for G_k that $b_\alpha(s,t)$ is in $\pi_1(G_k)$ and that in fact $b_\alpha(s,t)=b(h_\alpha(s),h_\alpha(t))$ is the restriction of the Steinberg cocycle b to the subgroup $\{h_\alpha(t);\ t\in k^*\}$. We are interested in the structure of $\pi_1(G_k)$ and the following fact will be very useful.

Lemma (**8.1**). — *The group* $\pi_1(G_k)$ *is generated by* $b_\alpha(s,t)$ *for* $\alpha\in\Pi$ *(the fundamental roots) and* $s,t\in k^*$.

Proof. — Let H'_α denote the subgroup of H' generated by $h'_\alpha(t)$, $t\in k^*$. Then by ([40], (7.7)), H'_α is normal in H' and $H'=\prod_\alpha H'_\alpha$. Thus if $h\in H'$, $h=\prod_\alpha h^\alpha$ with $h^\alpha\in H'_\alpha$, and by (8.2) of [40], $h\in\pi_1(G_k)$ if and only if each $h^\alpha\in\pi_1(G_k)$. Thus it suffices to show that $H'_\alpha\cap\pi_1(G_k)$ is generated by the elements $b_\alpha(s,t)$. But if $h=\prod_{i=1}^n h'_\alpha(t_i)$, then by (8.2) of [40], $h\in\pi_1(G_k)$ if an only if $\prod_{i=1}^n t_i=1$. We proceed by induction on n to show our result, the case $n=1$ being trivial. Now if $n>1$, observe that $h'_\alpha(t_1)h'_\alpha(t_2)=b_\alpha(t_1,t_2)h'_\alpha(t_1t_2)$ so that $\prod_{i=1}^n h_\alpha(t_i)=1$ implies that

$$h'=(b_\alpha(t_1,t_2))^{-1}h=h'_\alpha(t_1t_2)\prod_{i=3}^n h'_\alpha(t_i)\in\pi_1(G_k).$$

Thus by induction, h' is in the group generated by the $b_\alpha(s,t)$, and hence so is h, by the definition of h' above.

Theorem (**8.1**). — *A Steinberg cocycle* $c=\lambda\circ b$ *is uniquely determined by its restriction to* $H\times H$.

Proof. — In view of our construction, it suffices to show that if $c(h_1,h_2)=1$ for all $h_i\in H'$, then $c=1$. Let c take values in the abelian group A, and let F be the extension of G by A defined by c. Then by the universal property of $E(G_k)$, there is a unique homomorphism of group extensions j of $E(G_k)$ into F. The restriction of j to $\pi_1(G_k)$ is clearly λ by Chapter I. Let s be the canonical cross section chosen from G_k into $E(G_k)$ and let $v(g)=(j\circ s)(g)$. Then if we let $y_\alpha(t)=v(x_\alpha(t))$ it is clear from the construction of $E(G_k)$ that the relations A) and B) (or B')) are satisfied by the elements $y_\alpha(t)$. Moreover if we let $l_\alpha(t)=v(h_\alpha(t))$ for $\alpha\in\Sigma$, and $t\in k^*$, then $l_\alpha(t)l_\alpha(s)l_\alpha(ts)^{-1}=j(b_\alpha(t,s))=\lambda(b_\alpha(t,s))=c(h_\alpha(t),h_\alpha(s))=1$. Thus the elements $y_\alpha(t)$ satisfy relation C) above, and since G_k has only the relations A), B) and C), it follows that j is a homomorphism of G_k into F. Hence the class of the cocycle c is trivial, and hence $c=1$ by Chapter I.

Definition (**8.1**). — $S(G_k,A)$ *is the group of all restrictions of cocycles of the form* $\lambda\circ b$, $\lambda\in\mathrm{Hom}(\pi_1(G_k),A)$, *to* $H\times H$. *An element of this group is called a Steinberg cocycle (on* H).

By Theorem (8.1), it is clear that $S(G_k,A)$ is isomorphic to

$$H^2(G_k,A)\simeq\mathrm{Hom}(\pi_1(G_k),A).$$

A Steinberg cocycle c may be thought of on the one hand as a function from $H\times H$ into A satisfying certain identities; on the other hand, since $\pi_1(G_k)$ is generated by the

elements $b_\alpha(s, t)$, the homomorphism λ of $\pi_1(G_k)$ into A corresponding to c is uniquely determined by $\lambda(b_\alpha(s, t))=c(h_\alpha(s), h_\alpha(t))$. Then it becomes absolutely clear that the identities that c must satisfy in order to belong to $S(G_k, A)$ are exactly the relations among the generators $b_\alpha(s, t)$. Thus determining necessary and sufficient conditions for a function c to be belong to $S(G_k, A)$ is exactly the same thing as determining all the relations between the generators $b_\alpha(s, t)$ of $\pi_1(G_k)$.

Our next observation is that one may reduce substantially the number of generators required for $\pi_1(G_k)$. Since G is simple, it is known that the roots $\alpha\in\Sigma$ can have at most two distinct lengths. Moreover the ratio between the squared lengths of any pair of roots is either 1, 2, 3 1/2 or 1/3. Thus if there are two lengths of roots we may speak of long roots and short roots; if there is only one length for the roots, any root is long by convention.

Lemma **(8.2).** — *The group* $\pi_1(G_k)$ *is generated by* $b_\beta(s, t)$, $s, t\in k^*$, *for any fixed long root* β.

Proof. — Let D_α be the group generated by the elements $b_\alpha(s, t)$. Now if $\sigma\in W$ (the Weyl group) let $\beta=\sigma(\alpha)$; then β is a root, and we claim that $D_\alpha=D_\beta$. Since W is generated by reflections in positive roots, it suffices to consider the case when σ is reflection in a positive root γ. Then by (7.3) *b)* of [40], we have $w'_\gamma(1)h'_\alpha(t)w'_\gamma(-1)=h'_\beta(\eta t)h'_\beta(\eta)$ where $\eta=\pm 1$, independently of t. Then as $w'_\gamma(-1)=w'_\gamma(1)^{-1}$,

$$w'_\gamma(1)h'_\alpha(t)h'_\alpha(s)w'_\gamma(1)^{-1}=h'_\beta(\eta t)h'_\beta(\eta)h'_\beta(\eta s)h'_\beta(\eta). \tag{1}$$

But now the left hand side is exactly $b_\alpha(t, s)w'_\gamma(1)h'_\alpha(ts)w'_\gamma(1)^{-1}$ since $b_\alpha(t, s)$ is central in $E(G_k)$. However let us apply the same formula above to $h'_\alpha(ts)$; this yields

$$b_\alpha(t, s)w'_\gamma(1)h'_\alpha(ts)w'_\gamma(1)^{-1}=b_\alpha(t, s)h'_\beta(\eta ts)h'_\beta(\eta). \tag{2}$$

Then we see by equating (1) and (2) and solving for $b_\alpha(t, s)$ that

$$b_\alpha(t, s)=h'_\beta(\eta t)h'_\beta(\eta)h'_\beta(\eta s)h'_\beta(\eta ts)^{-1}.$$

Then by relation C) in G_k, and Lemma (8.1) it is clear that the right hand side is in D_β. Thus $D_\alpha\subset D_\beta$ and by symmetry $D_\beta\subset D_\alpha$, hence $D_\alpha=D_\beta$ as asserted.

Now suppose that there is only one length of root in Σ. Then all roots are conjugate under W and so $D_\alpha=D_\beta$ for all α and β and hence $\pi_1(G_k)=D_\alpha$ for any α by Lemma (8.1). Now if there are two lengths of roots, let β be a long root. Since β is conjugate to any long root under W, it will suffice to show that $D_\alpha\subset D_\beta$ for any short root α. We may replace α by any conjugate under W and hence assume that $(\alpha, \beta)>0$ since G is simple. Since β is long, the Cartan integer $2(\alpha, \beta)/(\beta, \beta)$ is one and $2(\alpha, \beta)/(\alpha, \alpha)=d$ where $d=2$ or 3. Then by (7.3) *e)* of [40]

$$\begin{aligned} h'_\alpha(t)h'_\beta(s)h'_\alpha(t)^{-1}h'_\beta(s)^{-1}&=h'_\beta(t^d s)h'_\beta(t^d)^{-1}h'_\beta(s)^{-1}\\ &=b_\beta(s, t^d)^{-1}. \end{aligned} \tag{3}$$

Furthermore we find from the same formula that

$$h'_\beta(s)h'_\alpha(t)h'_\beta(s)^{-1}h'_\alpha(t)^{-1}=b_\alpha(t, s)^{-1}. \tag{4}$$

Since the left hand sides of (3) and (4) are clearly inverses of each other we see that $b_\alpha(t, s) = b_\beta(s, t^d)^{-1}$ which shows that $D_\alpha \subset D_\beta$ as desired.

The argument in the preceding proof simultaneously yields an important set of relations satisfied by $b_\alpha(s, t)$.

Lemma **(8.3)**. — *Let* $\alpha \in \Sigma$ *and suppose there exists a root* β *such that* $2(\beta, \alpha)/(\beta, \beta) = 1$. *Then* $b_\alpha(t, s)$ *is a bilinear function of* s *and* t.

Proof. — If our hypothesis is satisfied, formula (4) of the argument above holds, and we simply observe that the right hand side is bilinear in s and t by Lemma (3.2) (cf. Lemma (1.4)).

We note that by inspection of the root systems of simple Lie algebras that the hypothesis on α in Lemma (8.3) is satisfied for every root in every simple algebra except for the long roots of the algebras of type C_n, $n \geq 1$. Also in this particular case $b_\alpha(s, t)$ may fail to be bilinear.

We denote by H_α the subgroup of $H \subset G_k$ generated by the elements h_α; then Lemma (8.2) yields the following fact.

Lemma **(8.4)**. — *If* α *is a long root, any Steinberg cocycle on* G_k *is determined uniquely by its restriction to* H_α.

Proof. — As before, let c be a Steinberg cocycle such that $c(h_1, h_2) = 1$ if $h_1, h_1 \in H_\alpha$. We must show that $c = 1$. Now c restricted to H is of the form $\lambda \circ b$ where λ is a homomorphism of $\pi_1(G_k)$ into A, and b is the fixed cocycle describing the universal covering $E(G_k)$ of G_k. The hypothesis that $c = 1$ on H_α is clearly equivalent to the hypothesis that $\lambda(b_\alpha(s, t)) = 1$ and hence that $\lambda = 1$ on D_α, the group generated by $b_\alpha(s, t)$, $s, t \in k^*$. Then by Lemma (8.2), $D_\alpha = \pi_1(G_k)$ and hence $\lambda = 1$ on $\pi_1(G_k)$ and hence $c = 1$ by Theorem (8.1).

It is possible to view this result in a slightly different way; namely if α is any root, there is an injective homomorphism i_α of $SL_2(k)$ into G_k such that if $\overline{x}_\pm(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ $\left(\text{resp. } \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\right)$ then $i_\alpha(\overline{x}_\pm(t)) = x_{\pm\alpha}(t)$. There is a corresponding homomorphism e_α of the universal covering $\overline{E}_k$ of $SL_2(k)$ into $E(G_k)$, and the restriction of e_α to $\pi_1(SL_2(k))$ maps this group into $\pi_1(G_k)$, and is of course the induced homomorphism $(i_\alpha)_*$ on fundamental groups (see Chapter I). The dual map $(i_\alpha)^*$ of $\mathrm{Hom}(\pi_1(G_k), A) = H^2(G_k, A)$ into $\mathrm{Hom}(\pi_1(SL_2(k)), A)$ for any A is of course the restriction map in cohomology.

Lemma **(8.5)**. — *The map* $(i_\alpha)_*$ *is surjective, and hence the restriction homomorphisms* $(i_\alpha)^*$ *are injective for any* A, *and* α *a long root.*

Proof. — It is clear that $\pi_1(G_k)$ is generated by elements $\overline{b}_\alpha(s, t)$ defined in the same way from the elements $\overline{x}_\pm(t)$ of $SL_2(k)$. Moreover it is clear from our construction that $e_\alpha(\overline{b}_\alpha(s, t)) = (i_\alpha)_*(\overline{b}_\alpha(s, t)) = b_\alpha(s, t)$. Hence by Lemma (8.1), the range of $(i_\alpha)_*$ contains D_α and hence is equal to $\pi_1(G_k)$. This establishes the lemma.

This lemma indicates the key role played by the group of rank one, $SL_2(k)$. The next section is devoted to the detailed treatment of this group.

9) If $G_k = SL_2(k)$, the split Cartan subgroup H may be taken to be k^*, the multiplicative group of the field k. There are two roots $\pm\alpha$, and we denote the corresponding one parameter groups by $x(t)$ and $y(t)$. We take the representative for the Weyl reflection in G_k and $E(G_k)$ to be $w(1) = w_{+\alpha}(1)$ and $w'(1) = w'_{+\alpha}(1)$. Then $h(t) = w(t)w(1)^{-1}$, and $\pi_1(G_k)$ is generated by elements $b_\alpha(s, t)$ which we denote for simplicity by $b(s, t)$.

Now every element of G_k is uniquely of the form $g_1(u, t) = x(u)h(t)$, $u \in k$, $t \in k^*$ or of the form $g_2(u, t, v) = x(u)w(t)x(v)$, $u, v \in k$, $t \in k^*$ by the Bruhat decomposition. We have elements $g'_1(u, t)$, $g'_2(u, t, v)$ in $E(G_k)$ defined by the same formulas with primes. The canonical cross section s of section 8 of G_k into $E(G_k)$ is then $s(g_1(u, t)) = g'_1(u, t)$, $s(g_2(u, t, v)) = g'_2(u, t, v)$. The Steinberg cocycle b on $G_k \times G_k$ into $\pi_1(G_k)$ is defined by $s(a_1)s(a_2) = b(a_1, a_2)s(a_1a_2)$ if $a_i \in G_k$. Then Theorem (8.1) says in principle that $b(a_1, a_2)$ can be computed from its values on $k^* \times k^*$, $b(h(s), h(t)) = b(s, t)$. In this simple case it is possible by simple calculations to make this explicit. We omit the routine details and record the results.

(1) $$b(g_2(u, t, v), g_2(u', t', v')) = b(tw^{-1}, w^{-1})^{-1} b(tw^{-1}, t') \qquad (\text{if } w = -(v + u') \neq 0)$$

and $= b(-t, -t')^{-1}$ if $w = 0$.

(2) $$b(g_2(u, t, v), g_1(u', t')) = b(t, t'^{-1})$$

(3) $$b(g_1(u, t), g_2(u', t', v')) = b(t, t')$$

(4) $$b(g_1(u, t), g_1(u', t')) = b(t, t').$$

Lemma **(9.1).** — *If $d \in S(G_k, A)$ is any Steinberg cocycle on $G_k = SL_2(k)$ with values in A, then d can be calculated from its values $d(h'(s), h'(t)) = d(s, t)$ on $k^* \times k^*$ by substituting d for b in formulas (1)-(4) above.*

Proof. — By definition d is of the form $\lambda \circ b$ for some homomorphism of $\pi_1(G_k)$ into A, and the result is immediate.

Now the function b in the formulas above is a normalized cocycle; i.e.

$$b(a_1a_2, a_3)b(a_1, a_2)b(a_1, a_2a_3)^{-1}b(a_2, a_3)^{-1} = 1, \quad b(1, 1) = 1.$$

Then if we rewrite these expressions using (1)-(4), we obtain words $W(a_1, a_2, a_3)$ in the generators $b(s, t)$ of $\pi_1(G_k)$.

Theorem **(9.1).** — *The relations $W(a_1, a_2, a_3) = 1$ and $b(1, 1) = 1$ hold for the generators $b(s, t)$ of $\pi_1(G_k)$. Moreover these relations generate all relations so that $\pi_1(G_k)$ is the free group on generators $b(s, t)$ subject to relations $W(a_1, a_2, a_3) = 1$ and $b(1, 1) = 1$.*

Proof. — It is clear that these relations hold; now let F be the free group on objects $\bar{b}(s, t)$ subject to these relations. There is clearly a surjective homomorphism ψ of F onto $\pi_1(G_k)$ sending generators to generators. Then $\bar{b}(s, t)$ is a function from $k^* \times k^*$ into F. We extend $\bar{b}$ to a function from $G_k \times G_k$ to F by formulas (1)-(4), and it is

absolutely clear that it is a normalized cocycle with values in F. Let K be the group extension of G_k by F which $\bar{b}$ defines. Then by the universal property of $E(G_k)$ there is a unique homomorphism j of group extensions of $E(G_k)$ into K. It is clear from the definition of $\bar{b}$ that $j(b(s, t))=\bar{b}(s, t)$ and since $b(s, t)=\psi(\bar{b}(s, t))$, it follows that $j\psi=\mathrm{id}$, and hence that ψ is injective, and hence an isomorphism as desired.

The problem then is to reduce the relations in Theorem (9.1) to a more usable form. This is simply a routine but tedious calculation; see the appendix for the details.

Theorem **(9.2).** — *If* $G_k=SL_2(k)$, *then* $\pi_1(G_k)$ *is the free group generated by* $b(s, t)$, $s, t\in k^*$ *subject to the following relations*

(1) $$b(st, r)b(s, t)=b(s, tr)b(t, r), \quad b(1, s)=b(s, 1)=1$$

(2) $$b(s, t)=b(t^{-1}, s)$$

(3) $$b(s, t)=b(s, -st)$$

(4) $$b(s, t)=b(s, (1-s)t).$$

We note that (1) is the normalized cocycle identity. Also Steinberg showed that a special case of (4) holds in $\pi_1(G_k)$ (see the calculation at the bottom of p. 121 of [40]). We note of course that these properties are exactly the first four parts of definition (3.1) of Chapter II, so that Theorem (9.2) serves as the motivation for the discussion in Chapter II.

We recall that $S(G_k, A)$ consists of all Steinberg cocycles from $k^*\times k^*$ into A, or equivalently all functions of the form $(\lambda\circ b)(s, t)$ where λ is a homomorphism from $\pi_1(G_k)$ into A.

Corollary. — *The group* $S(G_k, A)$ *for* $G_k=SL_2(k)$ *consists of all functions* d *from* $k^*\times k^*$ *satisfying* (1)-(4) *of Theorem* (9.2) *with* b *replaced by* d.

Proof. — If $d\in S(G_k, A)$, $d=\lambda\circ b$ so that d satisfies (1)-(4) of Theorem (9.2). Conversely if d satisfies these properties, then the map $b(s, t)\mapsto d(s, t)$ defines a homomorphism λ of $\pi_1(G_k)$ into A by Theorem (9.2). We clearly have $d=\lambda\circ b$ so our assertion is established.

We note that then $S(G_k, A)$ is the group we denoted by $S_k(A)$ in Chapter II. Our real interest is the subgroup S(A) consisting of the continuous functions in $S_k(A)$ when k is a topological field and when A is a topological group.

10) Let k be a locally compact non-discrete field (a local field), and let G_k denote the set of points of an arbitrary simply connected simple Chevalley group in k. Since G_k can be realized as an algebraic group of matrices, G_k is a locally compact (separable) topological group; also $G_k=[G_k, G_k]$. In accordance with Chapter I we denote by G_k^a the group G_k viewed as an abstract group, and by $E(G_k^a)$ its universal covering group, and by $\pi_1(G_k^a)$ the fundamental group of G_k^a.

Let A be any locally compact separable abelian group and let E be a central topological extension of G_k by A. By the universal property of $E(G_k^a)$, there is a unique

homomorphism of group extensions ψ of $E(G_k^a)$ into E. Recall that s denotes the distinguished cross section of G_k^a into $E(G_k^a)$; then we define $\sigma(g)=\psi(s(g))$ which is a cross section of G_k into E. The Steinberg cocycle d of the extension E is then defined by the equation $\sigma(g_1)\sigma(g_2)=d(g_1, g_2)\sigma(g_1g_2)$; also $d=\psi\circ b$ where b is the Steinberg cocycle of $E(G_k^a)$. We want to show first that the fact that E is a topological extension implies certain topological properties of σ and d.

Recall that $U_\pm$ is the subgroup of G_k generated by the elements $x_\alpha(t)$, $\alpha\in\Sigma^\pm$, $t\in k$.

Lemma (**10.1**). — *If* E *is a topological extension, then* σ *is a continuous function on* U_+ *and* U_-.

Proof. — It is always possible [25], [26] to choose a Borel map σ' of G_k into E such that $\varphi\circ\sigma'=\mathrm{id}$ where φ is the projection of E onto G_k. The commutator $[\sigma'(a), \sigma'(b)]\in E$ depends only on a and b and not on the choice of σ' since E is a central extension of G_k by A; moreover it is clear that $[\sigma'(a), \sigma'(b)]$ is a Borel function of a and b. Now if α is a root, and if $n\in k^*$ with $n^2=c\neq 1$ (such an n exists if we omit the fields of 2 or 3 elements), then $\sigma(x_\alpha(t))=[\sigma'(h_\alpha(n)), \sigma'(x_\alpha(t((c-1))))]$ by [40], p. 123 where σ is the distinguished cross section of our lemma. Thus it follows that σ is a Borel function when restricted to the subgroup U_α of elements of the form $x_\alpha(t)$. Since U_α is clearly a closed subgroup of G_k, U_α is locally compact separable, and it follows by a classical theorem of Banach [7], p. 25 that σ is continuous on U_α.

Every element u of the group U can be written uniquely as $u=\prod_\alpha x_\alpha(t_\alpha)$, $\alpha\in\Sigma^+$, $t_\alpha\in k^*$, where the product is taken in lexicographic order. It is also known that the map $u\mapsto(x_\alpha(t_\alpha))$ is a homeomorphism onto the product $\prod_\alpha U_\alpha$. Thus since σ is known to be a homomorphism on U, $\sigma(u)=\sigma(\prod_\alpha x_\alpha(t_\alpha))=\prod_\alpha\sigma(x_\alpha(t_\alpha))$ is clearly a continuous function of u, as desired.

By definition, we have $\sigma=\psi\circ s$, where s is the distinguished section of G_k^a into $E(G_k^a)$, and ψ is the projection of $E(G_k^a)$ into E. Also we know that for any α, $w'_\alpha(t)=s(x_\alpha(t))s(x_\alpha(t^{-1}))s(x_\alpha(t))$ and that $h'_\alpha(t)=w'_\alpha(t)w'_\alpha(-1)$. If α is a fundamental root, we defined $s(h_\alpha(t))=h'_\alpha(t)$, and hence

$$\sigma(h_\alpha(t))=\sigma(w_\alpha(t))\sigma(w_\alpha(-1))=\sigma(x_\alpha(t))\sigma(x_\alpha(t^{-1}))\sigma(x_\alpha(t))\sigma(w_\alpha(-1))$$

so that $\sigma(h_\alpha(t))$ is a continuous function of t by the previous lemma.

Corollary 1. — *The cross section* σ *is continuous on* H.

Proof. — Every element h of H can be written uniquely as $h=\prod_\alpha h_\alpha(t_\alpha)$ $(\alpha\in\Pi)$ where Π is the set of simple roots ([40], p. 122). Then we defined $s(h)=\prod_\alpha h_\alpha(t_\alpha)$ and hence $\sigma(h)=\prod_\alpha\sigma(h_\alpha(t_\alpha))$. Since H is isomorphic as topological group to the product $\prod_\alpha k^*$ by the map $h\mapsto(t_\alpha)$, it is clear from the preceding paragraph that σ is continuous on H.

Now if $a\in W$, the Weyl group, let $D(a)=Bw(a)B$ be the corresponding double coset of B in G_k where $w(a)$ is the representative of a in N chosen in section 8.

Corollary 2. — *The cross section* σ *is continuous on each double coset* $D(a)$.

Proof. — Each element g of $D(a)$ can be uniquely represented as $u_a.w(a).h.u$ with $u_a \in U_a$, $h \in H$, $u \in U$. Moreover the map $g \mapsto (u_a, h, u)$ is a homeomorphism, as is well known. Since by definition $\sigma(g) = \sigma(u_a)w(a)\sigma(h)\sigma(u)$, the result follows from Lemma (10.1) and Corollary 1.

Now if $a_1, a_2, a_3 \in W$, let $A(a_1, a_2, a_3)$ be the subset of $G_k \times G_k$ of all pairs g_1, g_2 such that $g_1 \in D(a_1)$, $g_2 \in D(a_2)$ and $g_1 g_2 \in D(a_3)$. Since each set $D(a_i)$ is locally closed (the intersection of an open and a closed set) it follows at once that $A(a_1, a_2, a_3)$ is locally closed.

Corollary 3. — *If* E *is a topological extension of* G_k *by* A, *and if* c *is the Steinberg cocycle of this extension, then* c *is continuous on each set* $A(a_1, a_2, a_3)$, *and hence* c *is a Borel function on* $G_k \times G_k$.

Proof. — We have by definition $c(g_1, g_2) = \sigma(g_1)\sigma(g_2)\sigma(g_1 g_2)^{-1}$, and the result follows immediately from Corollary 2. Since $G_k \times G_k = \bigcup A(a_1, a_2, a_3)$ and each is a Borel set, and since c is a Borel function on each $A(a_1, a_2, a_3)$, c is a Borel function.

Now if as before, A is a separable locally compact abelian group, it follows from Theorem (2.3) that the natural homomorphism of $H^2(G_k, A)$ into $H^2(G_k^a, A)$ is injective since $[G_k, G_k] = G_k$. Thus we can view $H^2(G_k, A)$ as a subgroup of $H^2(G_k^a, A)$, and to each class $\alpha \in H^2(G_k^a, A)$, there is associated a Steinberg cocycle c_α which we view as a function on $G_k \times G_k$ or on $H \times H$ since the values of c_α on $H \times H$ determine c_α uniquely by Theorem (8.1). (By Chapter I, α determines a unique homomorphism λ of $\pi_1(G_k^a)$ into A and $c_\alpha = \lambda \circ b$ where b is the Steinberg cocycle for the universal covering $E(G_k^a)$ of G_k^a.) We are now in a position to say which Steinberg cocycles belong to classes in $H^2(G_k, A)$ in terms of their restrictions to $H \times H$.

Theorem **(10.1).** — *The following are equivalent for a Steinberg cocycle* c :

(1) c *is continuous on* $H_\alpha \times H_\alpha$ *for some long root* α.

(2) c *is continuous on* $H \times H$.

(3) c *is a Borel function on* $H \times H$.

(4) c *is a Borel function on* $G_k \times G_k$.

(5) *The class of* c *is in* $H^2(G_k, A)$.

Proof. — (2) $\Rightarrow$ (3) is clear since any continuous function is a Borel function. Also (5) $\Rightarrow$ (1) is a consequence of Corollary 3 above applied to the set $A(1, 1, 1)$. Now if (4) holds, there is by [25] a topological extension E of G_k by A with c as a cocycle representative. Then c belongs to a class in $H^2(G_k, A)$ as desired, so (4) $\Rightarrow$ (5) holds.

Suppose now that (1) holds. We make use of the formulas developed in Lemma (8.2) and the general case of (7.3) *e)* of [40], and one may obtain an expression for $c(h_1, h_2)$, $h_i \in H$, in terms of its values $c(h_\alpha(s), h_\alpha(t))$ with α a long root. We omit the details, but the result is that this formula exhibits c as a continuous function on $H \times H$ provided it is continuous of $H_\alpha \times H_\alpha$ so (1) $\Rightarrow$ (2) holds.

It remains to consider (3) $\Rightarrow$ (4). If $G = SL_2$ then the explicit formulas (1)-(4) preceding Lemma (9.1) show immediately that c is a Borel function on $SL_2(k) \times SL_2(k)$.

For a general group G_k one knows in principle that one can compute the values of c on $G_k \times G_k$ from its values on $H \times H$, but explicit formulas seem too formidable; however, the same basic idea will work. It clearly suffices to show that c is a Borel function on each set $G_k \times D(\beta)$ for each $\beta \in W$. Now any element w of W may be written as a product of reflections in fundamental roots [22], and let us call the minimal number of reflections needed $l(w)$. We shall prove our statement above by induction on $l(\beta)$. Suppose that $l(\beta) \geq 1$; then any element g of the double coset $D(\beta)$ may be written uniquely as $g = u_\beta w(\beta) hu$ with $u_\beta \in U_\beta$, $h \in H$, $u \in U$ where $w(\beta)$ is the representative of β chosen. Now by the construction of Steinberg cocycles it is absolutely clear that $c(x, yu) = c(x, y)$ when $u \in U$ (see the formulas (1)-(4) of Lemma (9.1)). Thus it suffices to show that $c(x, u_\beta w(\beta) h)$ is a Borel function of its variables. Now we can find a reflection, α, in a fundamental root such that $\beta = \gamma\alpha$ and $l(\gamma) = l(\beta) - 1$. Let w be the representative for α in G_k. Since any element $w(t)$, $t \in W$, normalizes H, it follows that if $g = u_\beta w(\beta) h$ is the second variable above, $g = g'w$ where g' is a Borel function of g, and where $g \in D(\gamma)$ with $l(\gamma) = l(\beta) - 1$. Now by the cocycle identity,

$$c(x, g) = c(x, g'w) = c(g', w)^{-1} c(xg', w) c(x, g').$$

Now $g \in D(\gamma)$ and $l(\gamma) < l(\beta)$ so that the third term on the right is a Borel function of x and g', and hence of x and g. It is quite evident now that it suffices to show that $c(x, w)$ is a Borel function of x, w being a reflection in a fundamental root, and to treat the case when $l(\beta) = 0$; that is to show that $c(x, g)$ is a Borel function of x and g when $g \in B$, the Borel subgroup of G_k. In both of these cases one may write down formulas for the relevant values of the cocycle c in terms of its values on $H \times H$ quite analogous to the formulas (1)-(4) of Lemma (9.1). These formulas, which we omit, show immediately that c is a Borel function. This completes the proof of the Theorem.

Remark. — The description of topological extensions by Borel cocycles, rather than by some other class of cocycles (e.g. those continuous at (e, e) in $G \times G$ or those continuous in a neighborhood of (e, e) in $G \times G$) is well adapted to this discussion, since the rather natural selection of the Steinberg cocycle to represent a class leads to a cocycle that clearly is a Borel function, but in general is not even continuous at (e, e) in $G_k \times G_k$. Notice that any Steinberg cocycle is continuous on a dense open set in $G_k \times G_k$ by Corollary 3 of Lemma (10.1).

We change notation slightly from section 8 and denote by $S(G_k^a, A)$ the set of all Steinberg cocycles of G_k with values in A viewed as functions on $H \times H$. Then $S(G_k^a, A) \simeq H^2(G_k^a, A)$ for any A. Then if A is locally compact separable, $S(G_k, A)$ will denote all such functions corresponding to topological extensions. By Theorem (10.1), $S(G_k, A)$ consists of the continuous functions in $S(G_k^a, A)$. If now $G_k = SL_2(k)$, we have an explicit description of $S(SL_2(k)^a, A)$ by Theorem (9.2), and its Corollary. Now $S(SL_2(k), A)$, the continuous functions in the former group, will be denoted by $S(A)$.

Theorem **(10.2).** — *The group* $S(A)$ *consists of all functions from* $k^* \times k^*$ *into* A *satisfying* (1)-(4) *of Theorem* (9.2) *which in addition are continuous.*

We remember now that Theorem (3.1) of Chapter II describes the group S(A) completely (cf. Definition (3.1)). Thus since $S(A) \simeq H^2(SL_2(k), A)$ for any A, we have an explicit description of this group of extensions. Recall that there is a cyclic group B_k such that $S(A) \simeq \mathrm{Hom}(B_k, A)$ and that $B_{\mathbf{C}} = (0)$, $B_{\mathbf{R}} = \mathbf{Z}$, and $B_k = E_k$, the roots of unity in k if k is non-Archimedian. Thus $H^2(SL_2(\mathbf{C}), A) = 0$ and $H^2(SL_2(\mathbf{R}), A) \simeq \mathrm{Hom}(\mathbf{Z}, A)$, both of which are well known results (cf. Chapter I). Moreover we find the following fact.

Theorem **(10.3).** — *If k is non-Archimedian, then* $H^2(SL_2(k), A) \simeq \mathrm{Hom}(E_k, A)$ *for any separable locally compact abelian group viewed as a trivial* $SL_2(k)$*-module.*

It is clear then that if $SL_2(k)$ as topological group has a fundamental group in the sense of Chapter I, this group must be E_k. Our main result in the local case includes this and more (see Theorem (10.5)). It is really a matter of putting the pieces together.

Theorem **(10.4).** — *If k is a local field, and G is a simple, simply connected Chevalley group, then G_k, as locally compact group, has a universal covering group $E(G_k)$. Moreover $E(G_k) = [E(G_k), E(G_k)]$ so that $E(G_k)$ is a covering group of G_k as abstract group. If $k = \mathbf{C}$, $\pi_1(G_{\mathbf{C}}) = 0$ and if $k = \mathbf{R}$, $\pi_1(G_{\mathbf{R}}) = Z_2$ (the integers* mod 2*) unless G is of type C_n (the symplectic groups), in which case $\pi_1(G_{\mathbf{R}}) = \mathbf{Z}$. If k is non-Archimedian, $\pi_1(G_k)$ is a finite cyclic group of order dividing the order of E_k, the roots of unity in k, and finally $\pi_1(SL_2(k)) \simeq E_k$.*

Proof. — If $k = \mathbf{C}$, the complex numbers, it is well known that $G_{\mathbf{C}}$ is simply connected. If $k = \mathbf{R}$, the real number field, then $G_{\mathbf{R}}$ has a simply connected covering group $E(G_{\mathbf{R}})$ equal to its commutator subgroup by Theorem (2.2); moreover $E(G_{\mathbf{R}})$ is the usual topological universal covering group of $G_{\mathbf{R}}$. That $\pi_1(SL_2(\mathbf{R})) = \mathbf{Z}$ follows from Theorem (3.1) and Theorem (10.2), not to mention the usual classical proof of this fact. If G is arbitrary, let α be a long root of G, and let i_α be the corresponding injection of SL_2 into G (see Lemma (8.5)). In view of Lemma (8.5) and Lemma (2.5), the induced map $(i_\alpha)_* : \pi_1(SL_2(\mathbf{R})) \to \pi_1(G_{\mathbf{R}})$ is surjective. Thus $\pi_1(G_{\mathbf{R}})$ is cyclic and generated by $(i_\alpha)_*(x)$ where x is a generator of $\pi_1(SL_2(\mathbf{R}))$. Now by Theorem (3.1), Theorem (9.2), and Theorem (10.2), $\pi_1(SL_2(\mathbf{R}))$ is generated by $x = b(-1, -1)$. Now by Lemma (8.5), $(i_\alpha)_*(b(-1, -1)) = b_\alpha(-1, -1)$, but by Lemma (8.3) which is valid for the long roots of any group other than those of type C_n, $b_\alpha(s, t)$ is bilinear in s and t. Hence $b_\alpha(-1, -1)^2 = 1$, and $\pi_1(G_{\mathbf{R}})$ has order at most two if G is not a symplectic group. Now if G is of type C_n so $G_{\mathbf{R}} = Sp_n(\mathbf{R})$, it is well known that $\pi_1(G_{\mathbf{R}}) = \mathbf{Z}$. Moreover an inspection of a list of simple groups reveals that $\pi_1(G_{\mathbf{R}}) = Z_2$ in all other cases. We of course do not need this elaborate theory at all here, but we feel it is significant in that it " explains " the empirically observed facts about $\pi_1(G_{\mathbf{R}})$.

Suppose now that k is non-Archimedian. If $G_k = SL_2(k)$, then $\pi_1(G_k^a)$ is generated by the elements $b(s, t)$ subject to the relations of Theorem (9.2). We define a homomorphism α of $\pi_1(G_k^a)$ onto the roots of unity E_k by sending $b(s, t)$ into (s, t), the norm residue symbol in k. It is well known (cf. Chapter II) that (s, t) satisfies all relations

satisfied by the elements $b(s, t)$ so that α is well defined and surjective. By Chapter I, $\alpha \in \mathrm{Hom}(\pi_1(G_k^a), E_k)$ defines an element α' of $H^2(G_k^a, E_k)$ and so a central extension $E(G_k^a)$ of G_k^a. The Steinberg cocycle of this extension is $c(s, t) = \alpha(b(s, t)) = (s, t)$ and is a continuous function on $k^* \times k^*$ and hence $E(G_k)$ is a topological extension of $SL_2(k)$ by Theorem (10.1). Let D be the kernel of α in $\pi_1(SL_2(k)^a)$. Then if G is any simple simply connected Chevalley group, let β be a long root of G. Then by Lemma (8.2), the map $b(s, t) \mapsto b_\beta(s, t)$ defines a surjective homomorphism $(i_\beta)_*$ of $\pi_1(SL_2(k)^a)$ into $\pi_1(G_k^a)$ (the induced map defined by the inclusion $i_\beta : SL_2(k) \to G_k$). Let $(i_\beta)_*(D) = D_G$ be the image of D. Then $L_k = \pi_1(G_k^a)/D_G$ is a finite cyclic group of order dividing the order of E_k and in fact a quotient group of E_k. If α_G is the natural projection of $\pi_1(G_k^a)$ into L_k, then there is a unique $\gamma \in \mathrm{Hom}(E_k, L_k)$ such that $\gamma \circ \alpha = \alpha_G \circ (i_\beta)_*$. Since $\alpha_G \in \mathrm{Hom}(\pi_1(G_k)^a, L_k)$, it defines a central extension $E(G_k)$ of G_k^a by L_k. The Steinberg cocycle c of this extension is simply $\alpha_G \circ b_G$ where b_G is the Steinberg cocycle of $E(G_k^a)$. Now if $h = h_\beta(t)$ and $h' = h_\beta(s)$ are in $H_\beta \subset H$, then $b(h, h') = b_\beta(t, s)$ and hence $c(h, h') = (\alpha_G \circ b)(h, h') = \alpha_G(b_\beta(t, s)) = \alpha_G(i_\beta)_*(b(t, s)) = \gamma(\alpha(b(t, s)) = \gamma((t, s))$ where (t, s) is the norm residue symbol since $\gamma\alpha = \alpha_G(i_\beta)_*$ by construction. This shows that the Steinberg cocycle c is continuous on $H_\beta \times H_\beta$ and hence by Theorem (10.1), $E(G_k)$ is a topological extension. This extension could have easily been constructed by the techniques in [31].

We contend now that $E(G_k)$ is simply connected as topological group. We first consider the inflation homomorphism $j : H^2(G_k, A) \to H^2(E(G_k), A)$ for any A. We view $H^2(G_k, A)$ and $H^2(E(G_k), A)$ as subgroups of $H^2(G_k^a, A)$ and $H^2(E(G_k^a), A)$ respectively. Since $H^2(G_k^a, A) \simeq \mathrm{Hom}(\pi_1(G_k^a), A)$ and $E(G_k)$ is a covering group of G_k as $E(G_k) = E(G_k^a)/D_G$ ($D_G \subset \pi_1(G_k^a)$), it is clear from Theorem (1.1) that the kernel of the inflation map j viewed as a subgroup of $\mathrm{Hom}(\pi_1(G_k^a), A)$ consists of exactly those homomorphisms vanishing on D_G. Now if $a \in H^2(G_k, A)$, let d be its Steinberg cocycle. We consider the restriction d' of d to $SL_2(k)$ so that d' is the Steinberg cocycle of the restriction a' of a to $SL_2(k)$. Then viewing d' as a function on $H_\beta \times H_\beta$ (β is the long root defining the injection of $SL_2(k)$ into G_k and H_β is a split Cartan subgroup of the image of $SL_2(k)$) and hence on $k^* \times k^*$, d' is the Steinberg cocycle of a topological extension. Hence $d \in S(A)$ (cf. Theorems (10.1) and (10.2)) and then by Theorem (3.1), $d \in S_0(A) = S(A)$. But $S_0(A)$ consists of all functions on $k^* \times k^*$ into A of the form $\varphi((s, t))$ where (s, t) is the norm residue symbol and $\varphi \in \mathrm{Hom}(E_k, A)$. Thus d' viewed now as the homomorphism of $\pi_1(SL_2(k)^a)$ into A which sends $b(s, t)$ into $d'(s, t) = d(h'_\beta(s), h'_\beta(t))$ vanishes on D, the kernel of the projection α of $\pi_1(SL_2(k)^a)$ into E_k. Since d' is the restriction of d to $H_\beta = k^*$, it is clear that d viewed as a homomorphism of $\pi_1(G_k)$ into A vanishes on $(i_\beta)_*(D) = D_G$. It follows then that the class of d, which is an arbitrary class of $H^2(G_k, A) \subset H^2(G_k^a, A)$ is in the kernel of the inflation homomorphism j to $H^2(E(G_k), A) \subset H^2(E(G_k^a), A)$. We have shown the following.

Lemma **(10.2).** — *The inflation homomorphism* $j : H^2(G_k, A) \to H^2(E(G_k), A)$ *is the zero map.*

This is the first step in showing that $E(G_k)$ is simply connected. We consider the spectral sequence for the group extension $E(G_k)$ of G_k by L_k. The E_2^{11} term is $H^1(G_k, H^1(L_k, A))$ which is trivial since $G_k = [G_k, G_k]$ acts trivially on the coefficient module $H^1(L_k, A)$. Thus the restriction-inflation sequence [30]:

$$(*) \qquad 0 \to H^1(B_k, A) \xrightarrow{t} H^2(G_k, A) \xrightarrow{j} H^2(E(G_k), A) \xrightarrow{r} H^2(B_k, A)$$

is exact where t is the transgression and r is the restriction. If $A = \mathbf{T}$ is the circle group, r is the zero map since $[E(G_k), E(G_k)] = E(G_k)$ by Lemma (2.4), and so $H^2(E(G_k), \mathbf{T}) = (0)$. Since $H^1(E(G_k), \mathbf{T}) = 0$, we have already verified the first part of the hypotheses of Lemma (2.1).

Now let A be any discrete abelian group. It will suffice to show that $H^2(E(G_k), A) = (0)$. By the exact sequence $(*)$ $H^2(E(G_k), A) \subset H^2(L_k, A)$ via the restriction homomorphism. Let $\alpha \in H^2(E(G_k), A)$ and let $r(\alpha)$ be its image in $H^2(L_k, A)$. Since L_k is finite, there exists a finitely generated subgroup A′ of A, or an exact sequence,

$$0 \to A' \xrightarrow{a} A \xrightarrow{b} A'' \to 0$$

such that $b^*(r(\alpha)) = 0$ and hence that $b^*(\alpha) \in H^2(E(G_k), A'')$ is zero. Thus there exists a class $\beta \in H^2(E(G_k), A'')$ with $a^*(\beta) = \alpha$, and so it suffices to show that $H^2(E(G_k), A) = (0)$ if A is finitely generated. In this case $A = \prod_i A_i$ where A_i is cyclic (finite or infinite) and so it suffices to show that $H^2(E(G_k), A) = 0$ if A is cyclic. We have seen that if $H^1(E(G_k, \mathbf{T}) = H^2(E(G_k), \mathbf{T}) = (0)$, then $H^2(E(G_k), B) = 0$ for any compact B, and hence for any finite group B. Thus it finally suffices to show that $H^2(E(G_k), \mathbf{Z}) = (0)$ where $\mathbf{Z}$ is the integers.

We consider now the exact sequence

$$(**) \qquad 0 \to \mathbf{Z} \to \mathbf{R} \to \mathbf{T} \to 0$$

as an exact sequence of $E(G_k)$-modules. Since $H^1(E(G_k), \mathbf{T}) = H^2(E(G_k), \mathbf{T}) = (0)$, we find from the exact cohomology sequence of $(**)$ that

$$0 \to H^2(E(G_k), \mathbf{Z}) \to H^2(E(G_k), \mathbf{R}) \to 0.$$

However $H^2(E(G_k), \mathbf{R})$ is a vector space, and $H^2(E(G_k), \mathbf{Z})$, being isomorphic to a subgroup of $H^2(L_k, \mathbf{Z})$, with L_k a finite cyclic group, is a finite group. Thus $H^2(E(G_k), \mathbf{Z}) = (0)$ as desired. This shows that $E(G_k)$ is simply connected, and hence identifies $\pi_1(G_k)$ as described in the theorem. We have already observed that $E(G_k)$ is equal to its own commutator subgroup.

The authors in [10] have remarked that via the connection of this theory with the problem of congruence subgroups (cf. Chapter IV), one may deduce the following.

Theorem **(10.5).** — *If* $G_k = SL_n(k)$, *or* $G_k = Sp_n(k)$ *for any* n, *then* $\pi_1(G_k) \simeq E_k$ *if* k *is of characteristic zero.*

Remark. — There seems to be considerable evidence now that $\pi_1(G_k) \simeq E_k$ for any simple simply connected Chevalley group for non-Archimedian k [1]. Part of this comes from the observed regularity of the fundamental groups $\pi_1(G_k)$ for $k = \mathbf{R}$, the real field, when they are incidentally isomorphic to $E_{\mathbf{R}}$ the roots of unity in $\mathbf{R}$, if G is not of type C_n. The anomaly for the symplectic groups is explained in Lemma (8.3), and is a phenomenon which is not expected to occur in the non-Archimedian case, since Steinberg cocycles even for $SL_2(k)$ are already bilinear by Theorem (3.1).

We note two additional results which are obvious at this point.

Corollary 1. — *If α is a long root, the injection i_α of $SL_2(k)$ in G_k induces a surjective map of $\pi_1(SL_2(k))$ into $\pi_1(G_k)$.*

Let H be the fixed Cartan subgroup we have been using. Then we have the restriction homomorphism $r : H^2(G_k, \mathbf{T}) \to H^2(H, \mathbf{T})$.

Corollary 2. — *If the characteristic of k is not two and if G is of type C_n ($n \geq 1$), then the kernel of r is of order two. Otherwise r is injective.*

Proof. — If $G = SL_2$, then the result follows from Lemma (4.2). If G is not of type C_n, the result follows from Lemma (8.2) and (8.3). Finally if G is of type C_n, it follows from Lemma (8.2), that any element of order two in $H^2(G_k, \mathbf{T})$ is in the kernel of r and that conversely any element of the kernel of r is of order two. It then suffices to know that if k is not of characteristic two, then $H^2(G_k, \mathbf{T})$ ($G = C_n$) has a non-trivial element of order two. However Weil's classes [41] are non-trivial elements of order two, and we are done.

Remark. — It seems to be more than an accident that the metaplectic coverings found by Weil in [41] are characterized by Corollary 2 above.

11) In addition to information about G_k, k a local field, we shall also need some facts about $G_{\mathfrak{O}}$ where $\mathfrak{O}$ is the ring of integers in k. By definition we shall denote by $G_{\mathfrak{O}}$ the subgroup of G_k generated by the elements $x_\alpha(t)$, $\alpha \in \Sigma$, $t \in \mathfrak{O}$. We shall recall some well known facts about this group. View G as a group scheme defined over the integers $\mathbf{Z}$ as in [16] or [1] (lecture I-D, I-D'). Then we have a faithful representation ρ of G_k (defined over $\mathbf{Z}$) on a vector space V_k and an admissible lattice L in V_k such that $\rho(x_\alpha(t))(L) = L$ for every $\alpha \in \Sigma$ and $t \in \mathfrak{O}$ (*op. cit.*, [14], [22]). Let K be the subgroup of G_k of all elements g such that $\rho(g)(L) = L$. Then it is well known that K is an open compact subgroup ([14], [22]). Also let K_i be the subgroup of all elements of K such that $\rho(g)$ induces the identity transformation on $L/\mathfrak{p}^i L$ where $\mathfrak{p}$ is the maximal ideal of L. These are clearly the " congruence subgroups " of K of level i. We recall some well-known facts.

Lemma (**11.1**). — $K = G_{\mathfrak{O}}$ *is a compact subgroup and K/K_1 is isomorphic to G', the group of points of G in the residue class field k_r. Moreover K_1 is a pro-p-group where p is the characteristic of k_r. If k_r has at least four elements, then $K = [K, K]$.*

---

[1] Added in proof : H. Matsumoto has shown that this is in fact true; see [42].

Proof. — As we have observed each of the generators $x_\alpha(t)$ of $G_\mathfrak{O}$, $t\in\mathfrak{O}$, is contained in K and so $G_\mathfrak{O}\subset K$. But $G_\mathfrak{O}$ is known to be a maximal compact subgroup ([14], p. 36, and [22]), and so $G_\mathfrak{O}=K$. It is known by the construction of the group scheme G over $\mathbf{Z}$ ([16], [1]) that K/K_1 is G′, the group of points of G in k_r. We note that K_1 is a subgroup of the group H of all endomorphisms of V leaving the lattice L fixed and inducing the trivial map on L/pL. We observe that H is a pro-p-group and hence that K_1 is a pro-p-group.

Finally if k_r, the residue class field, has at least four elements we can find $d\in R$ the residue class system (which is cyclic or order at least three) such that $c=d^2\neq 1$. Then $c-1$ and c are units in $\mathfrak{O}$ and by [41], p. 123, $x_\alpha(t)=[h_\alpha(d), x_\alpha(t/(c-1))]$ for any $t\in k$. By the definition of $w_\alpha(x)$ and $h_\alpha(x)$, it is clear that $h_\alpha(x)\in G_\mathfrak{O}=K$ if x is a unit in $\mathfrak{O}$. Thus if $t\in\mathfrak{O}$, $(t/(c-1))\in\mathfrak{O}$ and c is a unit, hence $x_\alpha(t)\in[K, K]$, and so $K=[K, K]$ since K is generated by elements $x_\alpha(t)$, $t\in\mathfrak{O}$.

It is appropriate to consider at this point when a compact group K has a fundamental group $\pi_1(K)$. The following is more than we shall need.

Lemma (**11.2**). — *If* K *is compact and* [K, K] *is dense in* K, *then* K *has a simply connected covering group. Moreover* $\pi_1(K)$ *is a compact totally disconnected group* (i.e. *a profinite group*).

Proof. — This almost follows from Theorem (2.1), but we notice that in essence, we have already constructed explicitly in [31], p. 380, the universal covering E of K, and observed that the kernel of the projection of E onto K is profinite. The only problem is to show that E is simply connected. The commutator subgroup of E is dense for if not then $\overline{[E, E]}$ covers K since E is compact, contrary to the properties of E in [31]. We showed in [31] that the inflation map: $H^2(K, \mathbf{T})\to H^2(E, \mathbf{T})$ is the zero map, and this combined with the fact that [G, G] is dense in G and Lemma (2.4) shows that $H^2(E, \mathbf{T})=0$. It suffices then to show that $H^2(E, D)=0$ for any discrete group, but exactly as in the proof of Theorem (10.4) and Lemma (2.2) of [30], it suffices to consider the case when $D=\mathbf{Z}$. We consider $0\to\mathbf{Z}\to\mathbf{R}\to\mathbf{T}\to 0$ as an exact sequence of E-modules and observe that $H^1(E, \mathbf{T})=0$ by the above, and also that $H^2(E, \mathbf{R})=0$ so that it follows that $H^2(E, \mathbf{Z})=0$ as desired.

We shall apply these results to the case when $K=G_\mathfrak{O}$, the group of integral points of a simple connected Chevalley group in the integers $\mathfrak{O}$ of a local field k.

Lemma (**11.3**). — *If* $K=[K, K]$, *in particular if* k_r *has at least four elements,* $\pi_1(K)$ *is a pro-p-group.*

Proof. — Since $\pi_1(K)$ is the dual group of $H^2(K, \mathbf{T})$, it suffices to show that $H^2(K, \mathbf{T})$ is a p-torsion group. If K_1 is the principal congruence subgroup of level one as above, K_1 is a pro-p-group and $K/K_1=G'$, the group of points in G in the residue class field. We have a spectral sequence E_r^{ij} for the group extension of G′ by K_1, and it suffices to prove that E_2^{ij}, $i+j=2$, are p-torsion groups. Now $E_2^{0,2}$ is a subgroup of $H^2(K_1, \mathbf{T})$, and since $K_1=\varprojlim K_1/K_i$ it follows from [30] that $H^2(K_1, \mathbf{T})=\varinjlim H^2(K_1/K_i, \mathbf{T})$. Since K_1/K_i is a finite p-group for each i, it follows that $H^2(K_1, \mathbf{T})$ is a p-torsion group.

Now $E_2^{11}=H^1(G', \mathrm{Hom}(K_1, \mathbf{T}))$ and since $\mathrm{Hom}(K_1, \mathbf{T})$ is a p-torsion group, and G' is finite, it follows that E_2^{11} is a p-torsion group. Finally $E_2^{2,0}=H^2(G', \mathbf{T})$, and if one excludes a finite number of examples where the residue class field k_r has low cardinality, Steinberg [40] shows that $H^2(G', \mathbf{T})=(0)$. In all cases Steinberg shows that any projective representation of G' over a field of characteristic p, is equivalent to an ordinary representation. Now if $\alpha\in H^2(G', \mathbf{T})$ is of order prime to p, α may be viewed as a cocycle with values in Z_n the cyclic group or order n with n prime to p. We may find a finite field L of characteristic p such that Z_n may be identified to a subgroup L^*, the multiplicative group of L. Then we view α as a cohomology class of G' with values in L^*. Since $G'=[G', G']$ it suffices to show that $\alpha=1$ as a class in $H^2(G', L^*)$. Now we can find a modular projective representation π of G' in a finite dimensional vector space over L whose associated cohomology class is α. (The left regular α-representation, for instance.) Since π is equivalent to an ordinary representation, α is the trivial class. This shows that the finite group $H^2(G', \mathbf{T})$ has no elements of order prime to p, and hence is a finite p-group. This completes the proof of the Lemma.

12) We shall begin our discussion of the global or adèlic situation with a discussion of the cohomology of restricted products of groups. Thus let G_α be a countable family of separable locally compact groups and let K_α be a compact open subgroup of G_α which is defined for almost all α (i.e. except for a finite number of α). If one changes or leaves undefined the group K_α for a finite set of α, the entire construction which follows is unchanged. We denote by G the subgroup of the complete Cartesian product $\prod_\alpha G_\alpha$ consisting of elements $g=(g_\alpha)$ such that $g_\alpha\in K_\alpha$ for almost all α. This group is called the restricted product of the groups G_α relative to (K_α) and it can be given a separable locally compact topology such that it is a topological group [11]. If F is a finite set of indices containing the exceptional set where K_α is undefined, let $G_F=\prod_\alpha G_\alpha$ $(\alpha\in F)$ and let $K_F^*=\prod_\alpha K_\alpha$ $(\alpha\notin F)$. Then $G_F\times K_F^*\subset G$ and is locally compact with the product topology. We topologize G by declaring that $G_F\times K_F^*$ is an open subgroup with the relative topology. (This is independent of the choice of F.) We denote by G_F^* the restricted product of the groups G_α $(\alpha\notin F)$ so that then $G=G_F\times G_F^*$.

Our object is to determine the fundamental group of G if it exists, in terms of the fundamental groups of the factors G_α, assuming that they exist. It will be necessary to also assume that almost all K_α have fundamental groups, but in view of Lemma (11.2) it will suffice to assume that $[K_\alpha, K_\alpha]$ is dense in K_α for almost all α.

Now for almost all α the injection of K_α into G_α induces a continuous homomorphism j_α of $\pi_1(K_\alpha)$ into $\pi_1(G_\alpha)$. The range D_α of j_α is compact since $\pi_1(K_\alpha)$ is profinite, hence closed and in fact totally disconnected. The quotient group $\pi_1(G_\alpha)/D_\alpha$ is by definition the relative fundamental group $\pi_1(G_\alpha, K_\alpha)$, and we assume that it is discrete for almost all α or in other words, that D_α is open. We will see that this is a necessary condition for the existence of $\pi_1(G)$. It is quite a reasonable hypothesis and may always be true; in any case if K_α is normal in G_α it is automatically satisfied. Let E_α be the

universal covering of G_α and let L'_α be the universal covering of K_α. By the universal property of L'_α, there is for almost all α a unique continuous homomorphism d_α of L'_α into E_α compatible with the inclusion of K_α in G_α. The image L_α of L'_α is a compact subgroup and $L_\alpha/D_\alpha \simeq K_\alpha$. Moreover L_α is open since K_α is open in G_α and D_α is open in $\pi_1(G_\alpha)$ for almost all α by hypothesis.

Theorem (**12.1**). — *If* G_α *has a universal covering group* E_α *for all* α, *and if* $[K_\alpha, K_\alpha]$ *is dense in* K_α *for almost all* α *and if* D_α *(above) is open in* $\pi_1(G_\alpha)$ *for almost all* α, *then the restricted product* E *of the groups* E_α *relative to their compact open subgroups* L_α *is simply connected and covers* G. *Hence* G *has a fundamental group, and moreover* $\pi_1(G)$ *is isomorphic to the restricted product of the groups* $\pi_1(G_\alpha)$ *relative to their compact open subgroups* D_α.

Proof. — Let us notice that the product of two simply connected groups C and D is simply connected since $H^1(C\times D, A) = H^1(C, A)\times H^1(D, A)$ and

$$H^2(C\times D, A) \simeq H^2(C, A)\times H^2(D, A)\times H^1(C, H^1(D, A))$$

for any trivial module A (see Chapter I), and all terms vanish since C and D are simply connected. Thus the same holds for any finite product. So if F is any finite set of indices α, $E = E_F \times E_F^*$ where E_F is the product of E_α ($\alpha\in F$) and E_F^* is the restricted product of the remaining factors, it suffices to show that E_F^* is simply connected. Thus we are free to drop any finite set of indices, and consequently we may assume that the hypotheses of the theorem hold for all α.

If $\lambda\in H^1(E, \mathbf{T})$, let λ_α be its restriction to E_α viewed as a subgroup of E. Then $\lambda_\alpha = 1$ as $[E_\alpha, E_\alpha]$ is dense in E_α. Since the group generated by the E_α is dense in E, $\lambda = 1$ on a dense subgroup and hence $\lambda = 1$ so $H^1(E, \mathbf{T}) = 1$. Now let A be any abelian Lie group viewed as trivial E-module, and let $a\in H^2(E, A)$. Let $L = \prod_\alpha L_\alpha$ be our compact open subgroup of E and let b denote the restriction of a to L. Then $L = L_F \times L_F^*$ where $L_F = \prod_\alpha L_\alpha$ ($\alpha\in F$) and $L_F^* = \prod_\alpha L_\alpha$ ($\alpha\notin F$). Then as $[L_\alpha, L_\alpha]$ is dense in L_α, the same is true of L_F and L_F^* and so

$$(*) \qquad H^2(L, A) \simeq H^2(L_F, A)\times H^2(L_F^*, A).$$

On the other hand it is clear that L is the projective limit of the groups L_F relative to the obvious projection maps. Then by Theorem (2.3) of [30], $H^2(L, A)$ is the inductive limit of the groups $H^2(L_F, A)$ or in view of our special situation, $H^2(L, A) = \bigcup_F H^2(L_F, A)$ where $H^2(L_F, A)$ is viewed as a subgroup of $H^2(L, A)$ by (*). Thus if we choose F such that $b\in H^2(L_F, A)$ it is clear that the restriction of b to $H^2(L_F^*, A)$ will be the zero class. Also the restriction of b to L_H^* for any $H\supset F$ is zero.

Now suppose that H is any finite set of indices containing F. We form the group $E^H = E_H \times L_H^*$. Since E_H is simply connected, $H^2(E^H, A) \simeq H^2(L_H^*, A)$ by the restriction homomorphism. Now we started with a class $a\in H^2(E, A)$ and showed that there existed an F such that if $H\supset F$, the restriction of a to L_H^* is zero. Thus the restriction a^H of a to E^H is the zero class for all $H\supset F$. On the other hand, $E = \bigcup_H E^H$ ($H\supset F$), and this

is a countable union. We fix a Borel cocycle representative α of a; then if $H \supset F$ there is a (normalized) Borel one-cochain β^H on E^H, such that $\alpha^H = \delta(\beta^H)$ on $E^H \times E^H$ where δ is the coboundary operator. Since $H^1(E^H, A) = 0$ and A is a trivial module, it follows that δ is injective and hence the cochain β^H is unique. Hence if $M \supset H \supset F$, β^H is the restriction of β^M to $E^H \times E^H$, and so we may define a unique function β on E by $\beta(y) = \beta^H(y)$ if $y \in E^H$. Now each E^H is a Borel subset of E and each β^H is a Borel function and since $E = \bigcup_H E^H$ is a countable union, it follows that β is a Borel function for which $\alpha = \delta(\beta)$. Thus α is a coboundary, and so the original class a is trivial.

We have shown then that $H^2(E, A) = (0)$ for any Lie group A. However to show that E is simply connected it is enough to show that $H^2(E, T) = H^2(E, D) = 0$ for the circle group **T** and for any discrete group D, both of which are Lie groups. This completes the proof of Theorem (12.1).

We now apply Theorem (12.1) to the number theoretic situation at hand. Let k be a global field (i.e. a finite extension of the rational field or a function field in one variable over a finite field), and let k_v denote its completions. Then the fields k_v are local fields, and if G is a simple, simply connected Chevalley group over k, denote by G_v its points in k_v. Let K_v denote the group of points of G in $\mathfrak{O}_v$ the ring of integers in k_v, which is defined for non-Archimedian v, and in particular for almost all v. The restricted product of the groups G_v relative to their compact open subgroups K_v is the group of points G_A of G in the adèle ring A of k. More generally if S is any set of places (possibly void), then G(S) will denote the restricted product of the groups G_v, $v \notin S$. If $S = \emptyset$, $G(S) = G_A$ is the adèle group of G.

Theorem **(12.2).** — *The topological group* G(S) *has a fundamental group* $\pi_1(G(S))$. *Moreover* $\pi_1(G(S)) \simeq \coprod_v \pi_1(G_v)$ $(v \notin S)$ *(where* $\coprod$ *denotes direct sum), the isomorphism being effected by the maps* $\pi_1(G_v) \to \pi_1(G(S))$ *induced by the inclusions* $G_v \subset G(S)$.

Proof. — Since G_v has a discrete fundamental group for each v by Theorem (10.4), it suffices to show by Theorem (12.1), that for almost all v, $[K_v, K_v] = K_v$ and that for almost all v, the induced map $\pi_1(K_v) \to \pi_1(G_v)$ is the zero map.

First we note there are only a finite number of places v such that the residue class field k_v has cardinality less than four and so $[K_v, K_v] = K_v$ for almost all v by Lemma (11.1). Finally we observe that $\pi_1(G_v)$ is a quotient group of E_v the roots of unity in k_v for non-Archimedian v. If k is a number field, it is classical [3] that almost all k_v are absolutely unramified and hence that E_v is of order prime to p_v, the characteristic of the residue class field of k_v, for almost all v. If k is a function field E_v is always of order prime to p, the characteristic of k and k_v. Thus as $\pi_1(K_v)$ is a p_v-primary torsion group for almost all v by Lemma (11.3) and the comments at the beginning of the proof, the induced map $\pi_1(K_v) \to \pi_1(G_v)$ is the zero map for almost all v. This completes the proof.

Now the group of points of G with coefficients in k, G_k, is injected into each completion G_v by a map i_v. Moreover if $g \in G_k$, then $i_v(g)$ which we can view as a matrix with

coefficients in k (cf. Lemma (11.1)), will clearly have integral entries for almost all v. Hence $i_v(g) \in K_v$ for almost all v and we can define an injection i of G_k into $G(S)$ for any S. We view G_k as a discrete group; then $[G_k, G_k] = G_k$ so that G_k has a fundamental group $\pi_1(G_k)$. Moreover (the continuous map) i induces a homomorphism i_* of $\pi_1(G_k)$ into $\pi_1(G(S))$. Since $\pi_1(G(S))$ is discrete, the range is closed, and the cokernel of i_* is exactly the relative group $\pi_1(G(S), G_k)$.

Lemma (**12.1**). — *If* $x \in \pi_1(G_k)$, $(i_v)_*(x) = 0$ *for almost all* v *and* $i_*(x)$ *viewed as an element of* $\pi_1(G(S)) \simeq \coprod_v \pi_1(G_v)$ *has components* $(i_v)_*(x)$.

Proof. — Let p_v denote the projection of $G(S)$ onto the v^{th} factor G_v. Then $p_v \circ i = i_v$ so that $(i_v)_* = (p_v)_* \circ i_*$. However it is clear from Theorem (12.2) that $(p_v)_*$ is just the projection of $\pi_1(G(S)) \simeq \coprod_v \pi_1(G_v)$ onto the v^{th} factor. Thus the v^{th} component of $i_*(s)$ is $(i_v)_*(x)$ which is zero for almost all v.

We now have to discover in more detail what these induced maps are. Let G be as above and let α be a fixed long root and consider the corresponding subgroup isomorphic to SL_2 as embedded in G. We have natural generators $b(s, t)$, $s, t \in k^*$, for the fundamental group of $SL_2(k)$ (Lemma (8.1)). The induced homomorphism $\gamma : \pi_1(SL_2(k))$ into $\pi_1(G_k)$ is surjective as we have shown and sends the generators $b(s, t)$ onto elements we denoted by $b_\alpha(s, t)$. Moreover by Theorem (10.2), $\pi_1(G_v)$ is generated by elements $b^v_\alpha(s, t)$, $s, t \in k_v^*$ and $(i_v)_* b_\alpha(s, t) = b^v_\alpha(s, t)$ as is perfectly clear. We also have induced maps $\psi_v : \pi_1(SL_2(k_v)) \to \pi_1(G_v)$, and if $b^v(s, t)$, $s, t \in k_v^*$, denotes the canonical generators of $\pi_1(SL_2(k_v))$, $\psi_v(b^v(s, t) = b^v_\alpha(s, t)$ by construction. Moreover $\pi_1(SL_2(k_v))$ for v non-Archimedian is identified with E_v the roots of unity in k_v by $b^v(s, t) \mapsto (s, t)_v$ where $(s, t)_v$ denotes the norm residue symbol for $n(v)^{\text{th}}$ roots of unity ($n(v)$ is the order of E_v). Finally we let E denote the roots of unity in k and we denote by n its order.

Our main result below follows from the above and the global uniqueness theorems in Chapter II.

Theorem (**12.3**). — *Let* k *be a global field and* S *be a set of places, and* G *a simple, simply connected Chevalley group. Then the relative group* $\pi_1(G(S), G_k)$ *is zero if* S *contains a non-complex place. If* S *consists entirely of complex places* $\pi_1(G(S), G_k)$ *is cyclic of order dividing* n *(the order of* E, *the roots of unity in* k*). If* $G = SL_2$, *and* S *consists entirely of complex places,* $\pi_1(SL_2(S), SL_2(k)) \simeq E$.

Proof. — If α is a long root of G, then the map $\pi_1(SL_2(S)) \to \pi_1(G(S))$ is surjective, since the local maps at each completion are surjective. Moreover, the map $\pi_1(SL_2(k)) \to \pi_1(G_k)$ is surjective by Lemma (8.1). It follows that $\pi_1(G(S), G_k)$ is a quotient group of $\pi_1(SL_2(S), SL_2(k))$ and hence it suffices to prove our assertions for $G = SL_2$.

Let L(S) be the subgroup of homomorphisms of $\pi_1(SL_2(S))$ into **T** (the circle group) vanishing on the image of $\pi_1(SL_2(k))$. Then L(S) is simply the dual group of $\pi_1(SL_2(S), SL_2(k))$. Any homomorphism φ of $\pi_1(SL_2(S)) \simeq \coprod_v \pi_1(SL_2(k_v))$ $(v \notin S)$ into **T**

is uniquely determined by a family $\varphi(v)$ of homomorphisms of $\pi_1(SL_2(k_v))$ into **T**. Then to say that φ vanishes on $i_*(SL_2(k))$ is to say that $1=\varphi(i_*(b(s,t)))$ for $s, t\in k^*$ or equivalently by Lemma (12.1), $1=\prod_v \varphi(v)(i_v)_*(b(s,t))=\prod_v \varphi(v)(b^v(s,t))$ $(v\notin S)$. For non-Archimedian v we identify $\pi_1(SL_2(k_v))$ with E_v by the map $b^v(s,t)\mapsto(s,t)_v$. We denote by V the infinite places. Then we have $1=\prod_{v\in V-S}\varphi(v)(b^v(s,t)).\prod_{v\notin S\cup V}\varphi(v)((s,t)_v)$. We notice now that since the second factor on the right is bilinear in s and t, the first factor $\prod_v \varphi(v)(b^v(s,t))$ $(v\in V-S)$ is bilinear in s and t. Now the image of k^* in $\prod_{v\in V} k_v^*$ is dense as is well known, and since $\varphi(v)(b^v(s,t))$ is continuous for $s, t\in k_v^*$, it is immediately clear that $\prod_v \varphi(v)(b^v(s_v,t_v))$, $s_v, t_v\in k_v^*$, is bilinear and hence that $\varphi(v)b^v(.,.)$ is bilinear for $v\in V-S$. In that case, $\varphi(v)(b^v(s,t))$ is of the form $\varphi'(v)((s,t)_v)$ where φ' is a homomorphism of E_v into **T** by Chapter III. (If v is complex this is automatic since $b^v(s,t)=1$ so the only content here is for real places.) We change notation and call $\varphi'(v)$, $\varphi(v)$ so that in all cases, $\varphi(v)$ is a homomorphism from E_v into **T**. Then our formula reads $1=\prod_v \varphi(v)((s,t)_v)$ $(v\notin S)$. *Thus it is absolutely clear that the group* L(S) *is the group of all "reciprocity laws" with no contribution from* S.

If $\varphi=(\varphi(v))$, $v\notin S$, satisfies the above, we may define $\varphi(v)=1$ for $v\in S$, and then we have $1=\prod_v \varphi(v)((s,t)_v)$ with the product taken over all completions. Theorem (7.4) concerns exactly this situation; to be precise, let us embed the cyclic group E in the circle group by some map j and let us denote by $\psi(v)$ the map of E_v onto E of raising to the power $n(v)/n$ with obvious conventions if v is complex. Then Theorem (7.4) says that $\varphi(v)=j(\psi(v))^m$ for some integer m uniquely determined modulo n, with say $\varphi(v)=1$ if v is complex. Thus if we know $\varphi(v)$ for some non-complex v, φ is completely determined. Now suppose that S contains a non-complex place v; since $\varphi(v)=1$ if $v\in S$ by definition this says that $\varphi(w)=1$ for all w and hence that $\varphi=1$. Thus $L(S)=(1)$ and hence its dual group $\pi_1(SL_2(S), SL_2(k))$ is trivial. If on the other hand, S contains only complex places, let $\varphi(v)=1$ for v complex, and $\varphi(v)=j(\psi(v))^m$ for $m=0, 1, \ldots, n-1$. Then $\prod_v \varphi(v)((s,t))_v=1$ is the classical Artin reciprocity formula or a power of it ([3], [33]). Since these are the only possible choices for $\varphi(v)$, it follows that L(S) is cyclic of order n, and hence that $\pi_1(SL_2(S), SL_2(k))$ is cyclic of order n. This completes the proof.

A more careful analysis of the surjective homomorphism $\pi_1(SL_2(S))\to\pi_1(G(S))$ for any G mentioned in the first sentence of the proof together with the argument of the above theorem for SL_2 yields a formula for the order of the relative group $\pi_1(G(S), G_k)$ in terms of local data alone. Namely let $l(v)$ denote the order of $\pi_1(G_v)$, so that $l(v)\,|\,n(v)$. It is absolutely clear by global class field theory [3] that $n=$ g.c.d.$(n(v))$, v not complex. Then let $l=$ g.c.d.$(l(v))$ v not complex so that l divides n.

Theorem (**12.4**). — *If every v in* S *is complex* $\pi_1(G(S), G_k)$ *has order l.*

We noted in Theorem (10.5) that the authors in [10] show that $l(v)=n(v)$ if G is of type A_n or C_n (the special linear or symplectic groups) and k_v is of characteristic zero.

Theorem (**12.5**). — *If* G *is of type* A_n *or* C_n, *and if every* v *in* S *is complex, and if* k *is a number field*

$$\pi_1(G(S), G_k) \simeq E.$$

The argument in [10] proceeds by showing by completely different methods that for any totally imaginary number field and S consisting of all complex places, $\pi_1(G(S), G_k) \simeq E$ for G of type A_n or C_n ($n \geq 2$). If one has a given local field k' the authors in [10] remark that one can find a totally imaginary field k such that k' is a completion of k and k and k' have the same roots of unity.

Remarks. — 1) We remark that the determination of the kernel of the map $i_* : \pi_1(G_k) \to \pi_1(G(S))$ seems to be somewhat deeper. We have no information about it.

2) It seems a reasonable conjecture that the relative group $\pi_1(G(S), G_k)$ is isomorphic to E, the roots of unity in k if every $v \in S$ is complex for any G. This conjecture follows if one can solve the local problem. We note that this is exactly the " metaplectic " conjecture posed in [10] with slightly different notation.

Chapter IV

13) We want to indicate briefly in this final chapter the connection of the relative fundamental groups $\pi_1(G(S), G_k)$ with the problem of congruence subgroups ([8], [9], [10], [27], [28]). This connection is set forth in [10] and we briefly recall it here. Let k be a global field and let S be a finite *non-void* set of places containing S_∞, the Archimedian places. Let $\mathfrak{O}(S)=\{x \mid x\in k,\ v(x)\leq 1, x\notin S\}$. Then $\mathfrak{O}(S)$ is a Dedekind domain [10] and k is its field of fractions; if k is a number field and $S=S_\infty$, then $\mathfrak{O}(S)$ is simply the ring of integers in k. We choose a faithful matrix representation of the group scheme G over the integers $\mathbf{Z}$ as in section 11. Then $x_\alpha(t)$ is a matrix with entries polynomials in t with integral coefficients. We let $G_{\mathfrak{O}(S)}$ be the points in G_k with coefficients in $\mathfrak{O}(S)$. If $\mathfrak{p}$ is an ideal in $\mathfrak{O}(S)$, one has the congruence subgroup $G_{\mathfrak{O}(S)}(\mathfrak{p})$ of matrices congruent to the unit matrix mod $\mathfrak{p}$. One defines a topology then on G_k by taking as neighborhoods of 1, the congruence subgroups. Then G_k is a topological group, and we denote by $\overline{G}_k$ the completion with respect to this topology. On the other hand, an S-arithmetic subgroup H of G_k is by definition a subgroup such that $H\cap G_{\mathfrak{O}(S)}$ is of finite index in both $G_{\mathfrak{O}(S)}$ and H. One defines a topology of G_k by choosing the arithmetic subgroups as neighborhoods of 1, and completes G_k in the topology and arrives at a group $\hat{G}_k$. Since every congruence subgroup is arithmetic, the identity map $G_k\to G_k$ induces a continuous homomorphism π of the completions: $\hat{G}_k\to\overline{G}_k$. It is shown in [10] that π is surjective and that $\overline{G}_k$, $\hat{G}_k$, and the kernel $C(G_{\mathfrak{O}(S)})$ of π are locally compact and that $C(G_{\mathfrak{O}(S)})$ is in fact pro-finite. The congruence subgroup problem then is to determine $C(G_{\mathfrak{O}(S)})$. It is shown in [10] that $C(G_{\mathfrak{O}(S)})$ is central in $\hat{G}_k$ if G is of type A_n or C_n and $n\geq 2$, and presumably the argument of Matsumoto in [1] (lecture I-H) would show that this is true for any G other than SL_2 (1).

Thus if G is of type A_n or C_n, $n\geq 2$, we have a central extension

$$1\to C(G_{\mathfrak{O}(S)})\to\hat{G}_k\to\overline{G}_k\to 1$$

and moreover the natural injection of G_k into $\overline{G}_k$ lifts to an injection of G_k into $\hat{G}_k$ since $\hat{G}_k$ is a completion of G_k. Since $[G_k, G_k]=G_k$, it is clear that the commutator subgroups of $\overline{G}_k$ and $\hat{G}_k$ are dense, and so we are in the context of relative fundamental groups, since the class of the extension $\hat{G}_k$ of $\overline{G}_k$ splits upon restriction to G_k. More generally we may factor $\hat{G}_k$ by $[C(G_{\mathfrak{O}(S)}), \hat{G}_k]^-$ which will turn $\hat{G}_k$ modulo this subgroup into a central extension of the same type for any G. We consider then an arbitrary G.

---

(1) Added in proof : Matsumoto has proved this ; see [42]. Serre has settled the problem for SL_2.

One observes then from [10] that the natural injection of G_k into $G(S)$ is a homeomorphism for the congruence topology and hence one may identify $\overline{G}_k$ with the closure of G_k in $G(S)$. If k is a number field, the authors in [10] observe that $\overline{G}_k = G(S)$ by theorems on strong approximation. (See Kneser's lectures in [1] if $G \neq E_8$.) We observe that this is always the case.

Lemma (**13.1**). — *If* S *a non-void set of places, containing all infinite places,* G_k *is dense in* $G(S)$ *if* G *is a simple simply connected Chevalley group.*

Proof. — We denote by $A(S)$ the adèle ring of k associated to the set S, so that $A(S)$ is the restricted product of the additive groups k_v relative to their rings of integers $\mathfrak{O}_v$ for $v \notin S$. The natural diagonal injection of k into $A(S)$ is dense in $A(S)$ — this is strong approximation for the Dedekind domain $\mathfrak{O}(S)$, or essentially the Chinese remainder theorem. Let us consider the elements $x_\alpha(t)$, $t \in k$, $\alpha \in \Sigma$ (the root system of G) of G_k. Let $x_\alpha(t_v)$ denote the corresponding elements of G_v, $t_v \in k_v$. It is clear by strong approximation in $A(S)$, that the closure of the one parameter group $x_\alpha(t)$ in $G(S)$ consists of all elements $x = (x_\alpha(t_v))$, $v \notin S$, with t_v an arbitrary element of k_v almost all of which belong to $\mathfrak{O}_v$. If we fix v, and take all $t_w = 0$ except for $w = v$, the elements $x_\alpha(t_v)$ fo G_v viewed as a subgroup of $G(S)$ lie in the closure of G_k. However these elements generate G_v and so $\overline{G}_k \supset G_v$ for all $v \notin S$. Hence $\overline{G}_k \supset G_F = \prod_v G_v$ $(v \in F)$ for any finite set F. Since the union of the groups G_F is dense in $G(S)$, our result follows.

Thus we have an exact sequence

$$(*) \qquad 1 \to C(G_{\mathfrak{O}(S)}) \to \hat{G}_k \to G(S) \to 1$$

with $C(G_{\mathfrak{O}(S)})$ central at least if G is of type A_n or C_n $(n \geq 2)$. Moreover this extension splits upon restriction to G_k. We know from Theorem (12.2) and Chapter I that $G(S)$ has a universal covering split on G_k which is an extension of $G(S)$ by $\pi_1(G(S), G_k)$

$$(**) \qquad 1 \to \pi_1(G(S), G_k) \to E \to G(S) \to 1.$$

We now factor $\hat{G}_k$ by the closure of the subgroup $[\hat{G}_k, C(G_{\mathfrak{O}(S)})]$ so that we convert $(*)$ into a central extension (if it is not so already),

$$(***) \qquad 1 \to B(G_{\mathfrak{O}(S)}) \to \hat{G}'_k \to G(S) \to 1$$

with $B(G_{\mathfrak{O}(S)}) \simeq C(G_{\mathfrak{O}(S)}) / [\hat{G}_k, C(G_{\mathfrak{O}(S)})]^-$. The following result serves to tie up the material of the first three Chapters with the theory of congruence subgroups. We are deeply indebted to J.-P. Serre for pointing out this connection to us. The formulation of the theorems in the first three Chapters was strongly influenced by this.

Theorem (**13.1**). — *The group extensions* $(**)$ *and* $(***)$ *are isomorphic, and hence* $B(G_{\mathfrak{O}(S)}) \simeq \pi_1(G(S), G_k)$ *and if* $C(G_{\mathfrak{O}(S)})$ *is central,* $C(G_{\mathfrak{O}(S)}) \simeq \pi_1(G(S), G_k)$.

Proof. — By the universal property of the extension E in $(**)$, there is a (unique) homomorphism φ of group extensions of $(**)$ into $(***)$. Since G_k is dense in $\hat{G}'_k$, the range of φ is dense. Let K_v be the maximal compact subgroup of integral matrices

in G_v for $v \notin S$, and let $K = \prod_v K_v$ so that K is compact open subgroup. Then viewing G_k as a subgroup of G(S), $G_{\mathfrak{D}(S)} = G_k \cap K$ since an element of k is in $\mathfrak{D}(S)$ if and only if it is local integer at all $v \notin S$. It is moreover clear that $G_{\mathfrak{D}(S)}$ is dense in K. Now let L be the inverse image in E of K; it is clear that $i(G_{\mathfrak{D}(S)}) \subset L$ where i is the injection of G_k into E assured by the definition of E. Let M be the closure of $i(G_{\mathfrak{D}(S)})$ in L. Since $\pi_1(G(S), G_k)$ is finite, and K is profinite, L and hence M are profinite. Moreover since the projection of $i(G_{\mathfrak{D}(S)})$ into G(S) is dense in K, it follows that M is also open in E.

Now let N be an open subgroup of M and π_N the projection onto the finite group M/N. Then $\pi_N \circ i$ is a surjective homomorphism of $G_{\mathfrak{D}(S)}$ into the finite group M/N and hence its kernel is an arithmetic subgroup of G_k. Since the subgroups N of M define the topology of E (M is open), it is clear that the closure of $i(G_k)$ in E is a completion of G_k relative to a family of arithmetic groups containing all the congruence subgroups. Also M is open in E so that the closure of $i(G_k)$ is open in E, and it follows immediately that the closure of $i(G_k)$ in E is all of E (the projection of the closure of G_k into G(S) is open and contains the dense subgroup G_k and is hence all of G(S). Then the closure of $i(G_k)$ is a central extension of G(S) splitting on G_k and by the universal property of E, must be all of E.)

Since $\hat{G}_k$ is the completion of G_k with respect to all arithmetic subgroups, there is a continuous homomorphism ψ of $\hat{G}_k$ into E, which is in fact surjective (since the image contains M, an open subgroup of E) and is clearly seen to be a homomorphism of group extensions. Since E is a central extension of G(S), it is clear that $\psi([\hat{G}_k, C(G_{\mathfrak{D}(S)})]) = 1$ so that ψ becomes a homomorphism ψ' of $\hat{G}'_k$ onto E (as central group extensions of G(S)). On the other hand we have already constructed a homomorphism φ of group extensions of E into $\hat{G}'_k$. It follows immediately that $\varphi \circ \psi'$ and $\psi' \circ \varphi$ are the identity maps since [E, E] and $[\hat{G}'_k, \hat{G}'_k]$ are dense in E and $\hat{G}'_k$ respectively. This completes the proof os the Theorem.

Now we can make use of the results in [10]; in particular it is shown that if G if of type A_n or C_n ($n \geq 2$), then $C(G_{\mathfrak{D}(S)})$ is central in $\hat{G}_k$, and moreover that $C(G_{\mathfrak{D}(S)}) \simeq E$, the roots of unity in k provided that S consists entirely of complex places, and that $C(G_{\mathfrak{D}(S)}) = (0)$ otherwise. This then yields Theorem (12.5), and together with Theorem (12.4) it also yields Theorem (10.5) so that all of the statements are completely proved.

APPENDIX

We shall concern ourselves here with the proof of Theorem (9.2) of Chapter III, which characterizes Steinberg cocycles as those functions b on $k^*\times k^*$ into an abelian group satisfying:

* (1) $b(st, r)b(s, t)=b(s, tr)b(t, r), \quad b(s, 1)=b(1, s)=1$

(2) $b(s, t)=b(t^{-1}, s)$

(3) $b(s, t)=b(s, -ts)$

(4) $b(s, t)=b(s, t(1-s))$.

Let us first establish that these conditions are first of all necessary, it being clear that (1) is necessary. Now for (3), we take $r=s$ in Lemma (7.3 *a*) of [40] and this becomes in our notation $w(u)w(t)w(u)^{-1}=w(t^{-1}u^2)$. Then we use the substitution $w(x)w(y)=h(x)h(-y)^{-1}=b(-xy^{-1}, -y)^{-1}h(-xy^{-1})$ and find that $b(-st^{-1}, -t)=b(-st^{-1}, -s)$ which is (3) with a change of variables. We note also that (1) and (3) yield

(5) $$b(vx, -x^{-1})b(v, x)=b(v, -1).$$

We put $x=-v^{-1}$ in (5) and find that $b(-1, v)b(v, -v^{-1})=b(v, -1)$. Since $b(v, -v^{-1})=1$ by (3), $b(-1, v)=b(v, -1)$. By (5) and (3),

$$b(st, -t^{-1})^{-1}b(s, -1)=b(s, t)=b(s, -st)=b(s^2t, (st)^{-1})^{-1}b(s^2t, -1)$$

and since $b(-1, x)b(-1, -x)=b(-1, -1)$ by (1), and since $b(x, -1)=b(-1, x)$, the above becomes

$$b(-1, -s)b(st, -t^{-1})=b(-1, -s^2t)b(s^2t, s^{-1}t^{-1}).$$

We transform the right hand side by (1) and use the fact derived from (3) that $b(st, -t^{-1})=b(st, -s^2t)$, and find that $b(st, -s^2t)=b(-s^2t, s^{-1}t^{-1})$ which is (2).

Finally we note that the same argument *verbatim* as on the bottom of p. 121 of [40] shows that $h(av-av^2)h(a-av)^{-1}=h(av)h(a)^{-1}$ or in other words that $b(v, a(1-v))=b(v, a)$ which is (4). This establishes the necessity. We also note that by (2) and (3), $b(vx, -x^{-1})=b(v, -x^{-1})$ so that (5) becomes

(6) $$b(v, x)b(v, -x^{-1})=b(v, -1).$$

Moreover we showed in Lemma (3.2) that $b(z^2, xy)=b(z^2, x)b(z^2, y)$ follows from (1)–(3). Now from (1), $b(z^2, x)b(z^2x, y)=b(z^2, xy)b(x, y)$, and substituting in the above, we see that

(7) $$b(z^2x, y)=b(z^2, y)b(x, y)$$

is a consequence of (1)–(3).

For sufficiency, we begin with a function b from $k^*\times k^*$ into an abelian group A satisfying (1)-(4), and we extend it to a function from $\mathrm{SL}_2(k)\times\mathrm{SL}_2(k)$ into A by the formulas preceding Lemma (9.1). We must simply show that this function again denoted by b is a cocycle. (That it is then the Steinberg cocycle of the corresponding group extension is implicit in Theorem (9.1).) In the language of Theorem (9.1) it must be shown that each relation $W(a_1, a_2, a_3)=1$, $a_i\in\mathrm{SL}_2(k)$ is a consequence of (1)—(4). Further examination shows that this decomposes into consideration of fifteen special cases depending on the position of the a_i. However, there is one case which we may speak of as generic. Recall that each $g\in\mathrm{SL}_2(k)$ is uniquely of the form $x(u)w(t)x(v)$ or $x(u)h(t)$. The latter set forms a subgroup B and the former its complement U which is in fact the double coset $Bw(1)B$. We say that a_1, a_2, a_3 are generic if a_1, a_2, a_3, a_1a_2, a_2a_3, $a_1a_2a_3$ all are in U.

Lemma (A.1). — *If* a_1, a_2, a_3 *are generic, then* $W(a_1, a_2, a_3)=1$ *if* b *satisfies* (1)-(4).

Proof. — If $a_i=x(u_i)w(t_i)x(v_i)$, it is evident from

$$(**)\qquad b(a_1, a_2)=b(t_1\omega^{-1}, \omega)^{-1}b(t_1\omega^{-1}, t_2)\qquad (\text{if } \omega=-(v_1+u_2)\neq 0)$$

that $W(a_1, a_2, a_3)$ does not depend on u_1 or v_3 and depends only on t_i and v_1+u_2 and (v_2+u_3). Thus it is no loss of generality to take $u_1=v_3=u_2=v_2=0$. To say that (a_1, a_2, a_3) is generic means that $v_1\neq 0$, $u_3\neq 0$, and that $1-t_2^2v_1^{-2}u_3^{-1}\neq 0$. We simplify our notation and take $a_1=w(s)x(-u^{-1})$, $a_2=w(t)$, $a_3=x(-v^{-1})w(r)$ and put $z=1-t^2uv$. Then $W(a_1, a_2, a_3)=1$ becomes by (**)

$$(A)\qquad b(su, u^{-1})^{-1}b(su, t)b(stuvz^{-1}, v^{-1}z)^{-1}b(sutvz^{-1}, r)$$
$$=b(tv, v^{-1})^{-1}b(tv, r)b(suz^{-1}, u^{-1}z)^{-1}b(suz^{-1}, tvr).$$

The second and fourth terms on the right may be replaced using (1) by $b(sutvz^{-1}, r)b(suz^{-1}, tv)$, and the first of these cancels out. Now we place the third term on the left on the right side and use (1) to replace it times $b(suz^{-1}, tv)$ by $b(suz^{-1}, tz)b(tv, v^{-1}z)$. Finally we use the identities $b(suz^{-1}, u^{-1}z)=b(-s, u^{-1}z)$ and $b(suz^{-1}, tz)=b(-sut, tz)$ which are derived from (2) and (3) to write (A) as

$$(B)\qquad b(su, u^{-1})^{-1}b(su, t)=b(tv, v^{-1})^{-1}b(tv, v^{-1}z)b(-s, u^{-1}z)^{-1}b(-sut, tz).$$

Now by (1) we have

$$b(-s, u^{-1}z)^{-1}=b(-s, u^{-1})^{-1}b(-su^{-1}, z)^{-1}b(u^{-1}, z)$$
$$b(-sut, tz)=b(-sut, t)b(-sut^2, z)b(t, z)^{-1}$$
$$b(tv, v^{-1}z)=b(tv, v^{-1})b(t, z)b(v^{-1}, z)^{-1},$$

and we may replace $b(-s, u^{-1})$ and $b(-sut, t)$ by $b(su, u^{-1})$ and $b(su, t)$ respectively using (2) and (3). With these substitutions and the resulting cancellations, (B) becomes

$$(C)\qquad 1=b(v^{-1}, z)^{-1}b(u^{-1}, z)b(-su^{-1}, z)^{-1}b(-sut^2, z).$$

Now by (7) above the final two terms may be replaced by $b(u^2t^2, z)$ and this in turn may be combined with the second term so that (C) becomes

$$(D)\qquad 1=b(v^{-1}, z)^{-1}b(ut^2, z).$$

Finally by (2) and (4) we may write this as

$$1 = b(v^{-1}(1-z), z)^{-1} b(ut^2, z), \tag{E}$$

and recalling that $z = 1 - t^2uv$, we observe that $v^{-1}(1-z) = ut^2$. Thus (E) reduces to $1 = 1$ and the lemma is proved. We observe incidentally that this also provides a proof of the necessity of condition (4).

One could complete the proof by considering each of the remaining fourteen special cases, but this does not seem profitable even through none are as involved as the above. There is however another method which avoids most of these calculations and has some independent interest.

Theorem (A.1). — *Let* G *be a group and* U *a subset of* G *such that* $U = U^{-1}$ *and* $\bigcap_{i=1}^{n} a_i U \neq \emptyset$ *for any finite set of points* a_i *in* G. *Let* b *be a function defined on the set of points* X *consisting of all pairs* $(s, t) \in G \times G$ *with* $s, t, st \in U$, *taking values in an abelian group* A *satisfying* $b(s, tr)b(t, r) = b(st, r)b(s, t)$ *whenever* $s, t, r, st, tr, str \in U$. *There exists an extension* c *of* b *to* $G \times G$ *which is a cocycle. Moreover, any two extensions differ by a coboundary.*

Proof. — We can find a complex vector space W and a faithful representation of A on W; we shall now simply view A as a subgroup of GL(W). Now if f and g are two functions on G, we shall say that $f = g$ almost everywhere (a.e.) if $f = g$ on a set of the form $\bigcap_{i=1}^{n} a_i U$. This is clearly an equivalence relation, and we denote by V the set of equivalence classes of functions from G into W. Then V is a vector space which is non zero under our hypothesis; we shall with the usual abuse write the same symbol f for a function and its class. If a is function defined a.e. in G with values in A, and $g \in G$, then $(Mf)(x) = a(x)f(gx)$ is a well defined linear operator M on V. We let H denote the group of all such transformations, and note that A is naturally a subgroup of the center of H.

Now for each $s \in U$, we defined an element $L(s)$ of H by $(L(s)f)(x) = b(s, s^{-1}x)f(s^{-1}x)$ where b is the function of the theorem. A simple calculation shows that

$$(L(s)L(t)f)(x) = b(s, t)(L(st)f)(x)$$

for all s, t, x such that $s, t, st \in U$ and $x \in sU \cap U$ and hence that $L(s)L(t) = b(s, t)L(st)$ if $(s, t) \in X$. If p is the natural projection of H into H/A, and $J(s) = p(L(s))$, then $J(s)J(t) = J(st)$ for $(s, t) \in X$. It follows from Lemma 6 of [41] that J extends uniquely to a homomorphism of G into H/A. (The lemma in question asserts that G is naturally isomorphic to the free group on symbols (s), $s \in U$, subject to the relations $(s)(t) = (st)$ for all $(s, t) \in X$.) We denote this extension by J, and choose for each $s \in G$ an element $K(s)$ of H with $p(K(s)) = J(s)$ and with $K(s) = L(s)$ if $s \in U$. Then we must have $K(s)K(t) = c(s, t)K(st)$ for all $(s, t) \in G \times G$ with $c(s, t) \in A$. Evidently $c = b$ on X and c is a cocycle extending b.

Finally, if d is any extension of b as a cocycle to $G \times G$, let us define $(M(s)f)(x) = d(s, s^{-1}x)f(s^{-1}x)$. Then evidently, $M(s)M(t) = d(s, t)M(st)$ and so if $N(s) = p(M(s))$, $N(s)N(t) = N(st)$; but on the other hand, if $s \in U$, $d(s, s^{-1}x) = b(s, s^{-1}x)$ a.e.,

and so $M(s)=L(s)$, and hence $N(s)=J(s)$. By unicity, $N=J$, and it follows that $M(s)=a(s).K(s)$ where K is as above, and a is some function from G into A. We find then that $a(s)a(t)K(s)K(t)=d(s,t)a(st)K(st)$ and hence that c and d differ by the coboundary of a. This completes the proof.

We note that a unique class in $H^2(G, A)$ is determined by the above, and hence an extension of G by A. It is absolutely clear from the proof that this extension E is simply the subgroup of H generated by $L(s)$, $s\in U$, and A. This extension is equipped with a partial cross section defined on U, namely $s\mapsto L(s)$.

We now apply the Theorem above to the situation of Lemma (A.1), taking U to be the complement of the subgroup B. The hypothesis are fulfilled whenever B has infinite index in $SL_2(k)$; i.e. whenever k is infinite. (If k is finite, it follows from [40] that any function satisfying (1)-(4) is identically one so there is nothing to prove in this case anyway.) The proof of Theorem (9.2) will be complete once we show that b as function on $k^*\times k^*$ is the Steinberg cocycle of the extension E produced by Lemma (A.1) and Theorem (A.2).

The Steinberg cocycle of any extension is computed as follows. We choose representatives $B(x(t))$ and $B(h(s))$ for $x(t)$ and $h(s)$, and then the commutator $[B(h(s)), B(x(t))]=D(x(s^2t-t))$ is a representative for $x(s^2t-t)$ independent of our choices. Now if $B(w(1))$ represents $w(1)$, let $D(y(t))=B(w(1))D(x(-t))B(w(1))^{-1}$ and $D(w(t))=D(x(t))D(y(-t^{-1}))D(x(t))$, and finally $D(h(t))=D(w(t))D(w(-1))$. Then the Steinberg cocycle c is defined by the equation $D(h(s))D(h(t))=c(s,t)D(h(st))$. At this point we need to know in more detail some of the operators $L(s)$ $s\in U$ defined by Lemma (A.1) and Theorem (A.1). If $g=x(u)w(t)y(v)$, let $x(g)=u$, $w(g)=t$, and then a simple calculation shows that for $s\in U$,

$$(L(s)f)(g)=b((x(g)-x(t))w(s)^{-1}, -w(s))^{-1}b((x(g)-x(t))w(s)^{-1}, -w(g))f(s^{-1}g).$$

Now clearly we may choose $B(x(t))=L(w(-1))L(w(1)x(t))$ and by using (2), (3) and (1), this becomes $(B(x(t))f)(g)=f(x(-t)g)$. Also we may take $B(h(s))=L(w(s))L(w(-1))$ which upon simplification yields $(B(h(s))f)(g)=b(s, -w(g))f(h(s)^{-1}g)$. Then computation of the commutator above shows at once that $D(x(t))=B(x(t))$. Furthermore using the fact that $b(x(t)s, y)=b(s, y)=b(sx(t), x(-t)y)$ for $(s, y)\in X$, we see that $D(x(t))L(s)=L(x(t)s)$ and $L(s)D(x(t))=L(sx(t))$ if $s\in U$. Since $B(h(1))=1$, $L(w(1))^{-1}=L(w(-1))$ and then we see that

$$D(y(t))=L(w(1))D(x(-t))L(w(1))^{-1}=D(x(t^{-1}))L(w(t^{-1}))D(x(t^{-1}))$$

and hence that $D(w(t))=L(w(t))$. Finally we see that

$$(D(h(s))f)(g)=(B(h(s))f)(g)=b(s, -w(g))f(h(s)^{-1}g).$$

Then calculation of $D(h(s))D(h(t))D(h(st))^{-1}$ yields $b(s, t)$ and the proof is complete.

REFERENCES

[1] American Mathematical Society, *Notes on the Boulder Conference on Algebraic Groups and Discontinuous Subgroups*, Summer 1965.

[2] E. Artin, *Algebraic Number Theory* (Notes by G. Wurges), Göttingen.

[3] — and J. Tate, *Class Field Theory* (Harvard), 1961.

[4] — and G. Whaples, Axiomatic characterization of fields by the product formula, *Bull. Amer. Math. Soc.*, vol. 51 (1945), pp. 469-492.

[5] — and G. Whaples, A note on the axiomatic characterization of fields, *Bull. Amer. Math. Soc.*, vol. 52 (1946), pp. 245-247.

[6] L. Auslander and C. Moore, Unitary representations of solvable Lie groups, *American Math. Soc.*, Memoir n° 62 (1966).

[7] S. Banach, Théorie des opérations linéaires, *Monogr. Mat.*, t. I, Warsaw, 1932.

[8] H. Bass, M. Lazard and J.-P. Serre, Sous-groupes d'indice fini dans SL(n, $\mathbf{Z}$), *Bull. Amer. Math. Soc.*, vol. 70 (1964), pp. 385-392.

[9] H. Bass and J. Milnor, *On the congruence subgroup problem for* SL_n ($n \geq 3$) *and* Sp_n ($n \geq 2$) (Notes, Institute for Advanced Study).

[10] H. Bass, J. Milnor and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n ($n \geq 3$) *and* Sp_n ($n \geq 2$), *Inst. des Hautes Études Scient.*, n° 33 (1967).

[11] A. Borel, Some finiteness properties of adèle groups over number fields, *Inst. des Hautes Études Scient.*, n° 16 (1963).

[12] — and J. Tits, Groupes réductifs, *Inst. des Hautes Études Scient.*, n° 27 (1965).

[13] Bourbaki, *Topologie générale*, chap. IX, 2e éd., Paris, Hermann, 1958.

[14] F. Bruhat, Sur une classe de sous-groupes compacts maximaux des groupes p-adiques, *Inst. des Hautes Études Scient.*, n° 23 (1964).

[15] C. Chevalley, Sur certains groupes simples, *Tôhoku Journal of Math.* (2), vol. 7 (1955), pp. 14-62.

[16] —, Sur certains schémas de groupes semi-simples, *Séminaire Bourbaki*, Exposé 219.

[17] S. Eilenberg and S. Mac Lane, Cohomology theory in abstract groups, I, *Ann. of Math.* (2), vol. 48 (1947), pp. 51-78.

[18] —, Cohomology theory in abstract groups, II, *Ann. of Math.* (2), vol. 48 (1947), pp. 326-341.

[19] R. Godement, Groupes linéaires algébriques sur un corps parfait, *Séminaire Bourbaki*, Exposé 206.

[20] S. Helgason, *Differential Geometry and Symmetric Spaces*, New York, Academic Press, 1962.

[21] G. Hochschild and J.-P. Serre, Cohomology of group extensions, *Trans. Amer. Math. Soc.*, vol. 74 (1953), pp. 110-134.

[22] N. Iwahori and H. Matsumoto, On some Bruhat decomposition and the structure of the Hecke ring of p-adic Chevalley groups, *Inst. des Hautes Études Scient.*, n° 25 (1965).

[23] T. Kubota, Topological covering of SL(2) over a local field, *Jour. Math. Soc. Japan*, vol. 19 (1967), pp. 114-121.

[24] M. Lazard, Groupes analytiques p-adiques, *Inst. des Hautes Études Scient.*, n° 26 (1965).

[25] G. W. Mackey, Les ensembles boréliens et les extensions des groupes, *J. Math. Pures et Appl.*, vol. 36 (1957), pp. 171-178.

[26] —, Borel structures in groups and their duals, *Trans. Amer. Math. Soc.*, vol. 85 (1957), pp. 134-165.

[27] J. Mennicke, Finite factor groups of the unimodular group, *Ann. of Math* (2), vol. 81 (1965), pp. 31-37.

[28] —, Zur Theorie der Siegelische Modulgruppe, *Math. Ann.*, vol. 159 (1965), pp. 115-129.

[29] D. Montgomery and L. Zippin, *Topological transformation groups*, Interscience, New York, 1955.

[30] C. C. Moore, Extensions and low dimensional cohomology theory of locally compact groups, I, *Trans. Amer. Math. Soc.*, vol. 113 (1964), pp. 40-63.

[31] —, Extensions and low dimensional cohomology theory of locally compact groups, II, *Trans. Amer. Math. Soc.*, vol. 113 (1964), pp. 63-86.
[32] —, Decomposition of unitary representations defined by discrete subgroups of nilpotent groups, *Ann. of Math.*(2), vol. 82 (1965), pp. 146-182.
[33] J.-P. SERRE, *Corps locaux*, Paris, Hermann, 1962.
[34] —, *Cohomologie galoisienne*, Berlin, Springer, 1964.
[35] I. SCHUR, Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.*, vol. 127 (1904), pp. 20-50.
[36] *Séminaire « Sophus Lie »*, Paris, 1954.
[37] A. SHAPIRO, Group extensions of compact Lie groups, *Ann. of Math.* (2), vol. 50 (1949), pp. 581-585.
[39] STEENROD, *Topology of Fiber Bundles*, Princeton Univ. Press, Princeton, 1951.
[39] R. STEINBERG, Variations on a theme of Chevalley, *Pacific J. of Math.*, vol. 9 (1959), pp. 875-891.
[40] —, *Générateurs, relations et revêtements de groupes algébriques*, Colloque de Bruxelles (1962), pp. 113-127.
[41] A. WEIL, Sur certains groupes d'opérateurs unitaires, *Acta Math.*, vol. 111 (1964), pp. 143-211.
[42] H. MATSUMOTO, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*, Thèse, Univ. de Paris, 1968.

Manuscrit reçu le 8 janvier 1968.