SURJECTIVE STABILITY IN DIMENSION 0
FOR $K_2$ AND RELATED FUNCTORS

BY

MICHAEL R. STEIN

ABSTRACT. This paper continues the investigation of generators and relations for Chevalley groups over commutative rings initiated in [14]. The main result is that if $A$ is a semilocal ring generated by its units, the groups $L(\Phi, A)$ of [14] are generated by the values of certain cocycles on $A^* \times A^*$. From this follows a surjective stability theorem for the groups $L(\Phi, A)$, as well as the result that $L(\Phi, A)$ is the Schur multiplier of the elementary subgroup of the points in $A$ of the universal Chevalley-Demazure group scheme with root system $\Phi$, if $\Phi$ has large enough rank. These results are proved via a Bruhat-type decomposition for a suitably defined relative group associated to a radical ideal. These theorems generalize to semilocal rings results of Steinberg for Chevalley groups over fields, and they give an effective tool for computing Milnor's groups $K_2(A)$ when $A$ is semilocal.

Let $\Phi_l$ be a reduced irreducible root system of rank $l$ and $A$ a commutative ring with 1. There is an exact sequence

$$1 \to L(\Phi_l, A) \to St(\Phi_l, A) \to E(\Phi_l, A) \to 1$$

where $St(\Phi_l, A)$ is the Steinberg group [14, (3.7)] and $E(\Phi_l, A)$ is the elementary subgroup of the points in $A$ of the universal Chevalley-Demazure group scheme with root system $\Phi_l$ [14, (3.3)]. If $\Phi_m$ is a second such root system, containing $\Phi_l$ as a subsystem generated by a connected subgraph of the Dynkin diagram of $\Phi_m$, there are induced homomorphisms $\theta(l, m): L(\Phi_l, A) \to L(\Phi_m, A)$, and Steinberg [17] has shown these are surjective for all $m \geq l \geq 1$ when $A$ is a field. In this paper I will prove that this is true for any semilocal ring $A$ with at most one residue field isomorphic to $F_2$. I will also show, in this case, that the groups $L(\Phi_l, A)$ are generated by the values of certain cocycles on $A^* \times A^*$ and that (1) is a central extension (and not just stably central; cf. [14, (5.1)]), theorems again due to Steinberg [17] when $A$ is a field. These results were announced in [13].

Received by the editors March 15, 1972.


Key words and phrases. Chevalley group, universal central extension, stability theorems, Steinberg group, commutators in Chevalley groups, $K_2$, second homology group, Bruhat decomposition.

Copyright © 1973, American Mathematical Society

165
In general one conjectures that $\theta(l, m)$ is surjective for all $m \geq l \geq d$, where $d$ is a fixed positive integer related to the dimension of the maximal ideal space of $A$; the theorem proved here may thus be thought of as the dimension 0 case of a surjective stability theorem for $L(\Phi_l, A)$. If $\Phi_l$ belongs to one of the infinite families $A, B, C, D$, one deduces, under the same hypotheses, the surjectivity of

$$\theta(l, \infty): L(\Phi_l, A) \rightarrow L(\Phi_{\infty}, A) = \lim_{l \rightarrow \infty} L(\Phi_l, A).$$

This reveals one motivation of the present research, since $L(A_{\infty}, A)$ is Milnor's algebraic $K_2$ functor [9].

The paper proceeds as follows. Let $q \subseteq A$ be an ideal, and write $(1 + q)^*$ for the units congruent to 1 modulo $q$. In §1 I define pairings ("relative Steinberg symbols")

$$\{ , \} : A^* \times (1 + q)^* \rightarrow L(\Phi_l, q)$$

and recall some of their properties. In §2 I prove, when $q \subseteq \text{rad } A$, a normal form for the relative group $St(\Phi, q)$ analogous to the Bruhat decomposition of the Chevalley groups over fields [17, 7.6]. This implies that the groups $L(\Phi_l, q)$ are generated by the relative symbols of §1, and, therefore, that $L(\Phi_l, q) \rightarrow L(\Phi_m, q)$ is surjective for all $m \geq l \geq 1$. Combining this with Steinberg's theorem for fields yields the above-mentioned results for semilocal rings. In addition the theorems of this section allow one to deduce a presentation for $E(\Phi, A)$ of such a semilocal ring.

In §3 I compute $L(\Phi_l, A)$ for various local rings, using the results of §§1 and 2. In §4 I apply these results to the problem of surjective stability for the maps

$$H_2(SL_2(A), \mathbb{Z}) \rightarrow H_2(E(\Phi_l, A), \mathbb{Z}).$$

The reader primarily interested in $K_2$ should note the following. Milnor's groups $E_{n+1}(A), St_{n+1}(A)$ are the groups $E(A_n, A), St(A_n, A)$ of this paper ($n \geq 2$), and $K_2(A) = L(A_{\infty}, A)$. The symbols $\{ , \}_a$ are always bilinear in this case. A positive root $\alpha \in A^*_n$ is to be identified with a pair $(ij)$, $1 \leq i < j \leq n + 1; -\alpha$ then corresponds to $(ji)$.

Milnor's $K_2$ theory exists for noncommutative rings as well, and most of the results of §2 remain true in this case, provided certain elements in $A^*$ lie in $[A^*, A^*]$. I have omitted a discussion of these points since the surjective stability theorem for $K_2$ of noncommutative semilocal rings has recently been obtained by Dennis [3], based on work of Silvester [12].

When $A = K$ is a field, Matsumoto [8] has shown that the maps $\theta(l, m)$ are injective as well. This injective stability theorem remains true for radical ideals in the semilocal rings considered here, and will be the subject of a subsequent paper [15].
I would like to thank Professor Hyman Bass, who directed the Columbia University doctoral thesis which contained a preliminary version of these results, for his advice and encouragement. I would also like to thank M. Léon Motchane and the Institut des Hautes Études Scientifiques for their hospitality during the first stages of this research.

**Notation and terminology.** The definitions, notations and terminology regarding root systems, Chevalley groups, Steinberg groups and their subgroups and relations are to be found in [14, §3]. However in this paper we always assume that the Chevalley-Demazure group schemes in question are universal [14, (3.3)]. If $\Phi_l \subseteq \Phi_m$ are reduced irreducible root systems, we say they are of the same type if they satisfy

(a) $\Phi_l$ is generated by a connected subgraph of the Dynkin diagram of $\Phi_m$.
(b) If $\Phi_m$ is symplectic, then $\Phi_l$ is also symplectic and at least one long root of $\Phi_m$ occurs in $\Phi_l$.

The inclusions $D_l \subseteq B_l$ violate (a) and the inclusions $A_{I-1} \subseteq C_I$, $l > 2$, violate (b).

The reader is reminded that the relative groups used in this paper differ from those of [9] and [16] (cf. the warnings following [14, (3.13)]). However the results of this paper do apply to the relative groups of [16], as follows from [16, (1.1), (2.5) and (2.6)].

All rings are commutative with 1; all homomorphisms preserve 1. If $A$ is a ring, $\text{rad } A$ is its *Jacobson radical* and $A^*$ is its multiplicative group of units. A *pair* $(A, q)$ consists of a ring $A$ together with an ideal $q \subseteq A$; if $q \subseteq \text{rad } A$ we say $(A, q)$ is a *radical pair*. We write $(1 + q)^* = (1 + q) \cap A^*$. If $T$ is a subset of $A$, the subring of $A$ generated by $T$ is denoted $\mathbb{Z}[T]$.

Let $G$ be a group. For $\sigma, \tau \in G$ we write $\tau \sigma = \tau \sigma \tau^{-1}$, $[\sigma, \tau] = \sigma \tau \sigma^{-1} \tau^{-1}$.

If $H, K$ are subgroups of $G$, $[H, K]$ is the subgroup generated by $[h, k]$, $h \in H$, $k \in K$; in particular the *commutator subgroup* of $G$ is $[G, G]$. We write $G^{ab} = G/[G, G]$. If $G$ is finite, $|G|$ is its order.

Finally, $\mathbb{Z}$ denotes the rational integers and $F_q$ a finite field with $q$ elements.

1. *Relative Steinberg symbols and the subgroup $L(\Phi, A) \cap \hat{R}(\Phi, q)$.* Recall [14, (3.12)] that $\hat{H}(\Phi, q)$ is the smallest normal subgroup of $\hat{R}(\Phi, A)$ containing all $\hat{b}_\alpha(v)$, $\alpha \in \Phi$, $v \in (1 + q)^*$. $\hat{H}(\Phi, q)$ is a subgroup of $St(\Phi, q)$ (cf. (2.7)(a)).

**Definition.** Let $\alpha \in \Phi$, $u, v \in A^*$, and set

\[
\{u, v\}_\alpha = \hat{b}_\alpha(uv)\hat{b}_\alpha(u)^{-1}\hat{b}_\alpha(v)^{-1}.
\]

The subgroup of $\hat{H}(\Phi, A)$ generated by all $\{u, w\}_\alpha$, $\{w, u\}_\alpha$, where $u \in A^*$, $w \in (1 + q)^*$ and $\alpha$ ranges over $\Phi$ is denoted $D(\Phi, q)$. $D(\Phi, q)$ is a subgroup of $St(\Phi, q)$ (cf. (2.7)(a)).
It follows from relation (R8) that for all $\alpha, \beta \in \Phi$,
\[
\{u^{(\beta, \alpha)}, v\}_{\beta} = [\hat{h}_\alpha(u), \hat{h}_\beta(v)].
\]
Thus if there is an $\alpha \in \Phi$ with $\langle \beta, \alpha \rangle = 1$, we have $\{u, v\}_{\beta} \in [\hat{H}(\Phi, A), \hat{H}(\Phi, q)] \subset \hat{H}(\Phi, q)$. This will be the case except when $\Phi$ is symplectic and $\beta$ is long.

The following proposition summarizes various well-known identities satisfied by $\{, \}$, $\{, \}_\alpha$. Proofs may be found in [8, 5.5–5.7], [10, 3.2, 3.9, Appendix] and [18, Lemma 39 and Theorem 12].

(1.1) **Proposition.** Let $\alpha \in \Phi$, $u, v, w \in A^*$. Then $\{u, v\}_{\alpha}^{-1} = \{v, u\}_{-\alpha}$. Writing $1, \varepsilon, \{, \}_\alpha$, the following identities hold in $D(\Phi, A)$:

1. $\{u, 1\} = \{1, u\} = 1$.
2. $\{u, v\} \{uv, w\} = \{u, vw\} \{v, w\}$.
3. $\{u, v\} = \{u^{-1}, v^{-1}\}$.
4. $\{u, v\} = \{uv, w\}$.
5. $\{u, v\} = \{u, (1 - u)v\}$ if $1 - u \in A^*$.
6. $\{u, v^2\} = \{u, v\} \{u, v\}$.
7. $\{u, v\} = \{u^{-1}, v^{-1}\}$.
8. $\{u, v^{2}\} = \{u, v\}$.
9. $\{u, v\} = \{v, u\}$.

Moreover, if $\Phi$ is nonsymplectic or if $\alpha$ is short,

1. $\{u, v\} = \{v, u\}$.
2. $\{u, v\} = \{v, u\}$.
3. $\{u, v\} = \{v, u\}$.

**Remarks.** 1. The above identities are not independent. For example, (S1)–(S4) imply (S6)–(S8), and if $\Phi$ is nonsymplectic or if $\alpha$ is short, (S1)(S5)(S°2) imply the others. (Cf. [10, Appendix].)

2. Identity (S5), which is of great importance for computations when $A$ is a field, is valueless when $u \in (1 + q)^*$ (since in that case $1 - u \notin A^*$ if $q \notin A$). A new identity which can sometimes be used to replace (S5) in such computations when $q \subset \text{rad} A$ will be proved in (2.8).

(1.2) **Definition.** A relative Steinberg symbol on the pair $(A, q)$ with values in an abelian group $C$ is a mapping
\[
\{, \} : A^* \times (1 + q)^* \rightarrow C
\]
satisfying (S1)–(S5) of (1.1) and (2.8). When $q = A$, we call $\{, \}$ a Steinberg symbol. If (S°2) holds, we call $\{, \}$ a (relative) bilinear Steinberg symbol. We sometimes abbreviate "Steinberg symbol" to "symbol."

In this paper the word symbol will always refer to one of the symbols $\{, \}$ with values in $D(\Phi, q)$ constructed above.

Let $\hat{K}(\Phi, q)$ be the subgroup of $\text{St}(\Phi, q)$ generated by $D(\Phi, q)$ and all $\hat{h}_\alpha(v)$, $\alpha \in \Phi$, $v \in (1 + q)^*$. 
(1.3) **Proposition.** (a) $D(\Phi, q)$ is a central subgroup of $St(\Phi, A)$.
(b) $\hat{H}(\Phi, q) \subseteq \hat{K}(\Phi, q)$, and

$$[\hat{H}(\Phi, A), \hat{H}(\Phi, q)] \subseteq L(\Phi, A) \cap \hat{H}(\Phi, q) \subseteq L(\Phi, A) \cap \hat{K}(\Phi, q) \subseteq D(\Phi, q),$$

with equality if $\Phi$ is nonsymplectic or if every element of $(1 + q)^*$ is a square.

(c) $D(\Phi, q)$ is generated by all $\{u, v_\alpha^\beta, u \in A^*, v \in (1 + q)^* \}$ for any fixed long root $\alpha$. Hence if $\Phi_i \subseteq \Phi_m$ are reduced irreducible root systems of the same type, the homomorphism $D(\Phi_i, q) \to D(\Phi_m, q)$ is surjective for all $m \geq l \geq 1$, including $m = \infty$ if $\Phi$ is classical.

Since $H(A)$ is an abelian subgroup of $E(\Phi, A)$ [18, Lemma 28(b)], $D(\Phi, q)$ is a subgroup of $\hat{H}(\Phi, A) \cap L(\Phi, A)$, and the latter group is central in $St(\Phi, A)$ [18, p. 39, Corollary 1]. This also proves $[\hat{H}(\Phi, A), \hat{H}(\Phi, q)] \subseteq L(\Phi, A) \cap \hat{H}(\Phi, q)$, since $\hat{H}(\Phi, q)$ is normal in $\hat{H}(\Phi, A)$.

If $u \in A^*, v \in (1 + q)^*$, then

$$h(u)h(v)h(u)^{-1} = h(u^{(\beta, \alpha)}) h(v^{(\beta, \alpha)}) h(u^{(\beta, \alpha)})^{-1} \in \{u^{(\beta, \alpha)}, v^{(\beta, \alpha)} \} \subseteq \hat{K}(\Phi, q).$$

Since $D(\Phi, q)$ is central in $St(\Phi, q)$ by (a), this shows that $\hat{K}(\Phi, q)$ is a normal subgroup of $\hat{H}(\Phi, q)$; hence $\hat{H}(\Phi, q) \subseteq \hat{K}(\Phi, q)$. Thus $L(\Phi, A) \cap \hat{H}(\Phi, q) \subseteq L(\Phi, A) \cap \hat{K}(\Phi, q)$.

Given $h \in \hat{K}(\Phi, q)$, it follows from [17, 7.7] that we may write $h = d \hat{h}(u_1) \cdots \hat{h}(u_i)$ where $d \in D(q)$, $\hat{h}(u_i) = \hat{h}_\alpha(u_i)$, $\alpha_i \in \Delta$, and $u_i \in (1 + q)^*$. Then if

$$1 = \pi(h) = \hat{h}(u_1) \cdots \hat{h}(u_i)$$

we must have $u_i = 1$ for all $i$, since $E(\Phi, A)$ is a subgroup of a universal Chevalley group [18, Corollary to Lemma 28]. Hence $\hat{h}(u_i) = 1$ for all $i$; that is, $\hat{h} = d \in D(q)$ proving the last inclusion of (b).

Now if $\Phi$ is nonsymplectic, it follows from (2) that $D(\Phi, q) \subseteq [\hat{H}(\Phi, A), \hat{K}(\Phi, q)]$, and the inclusions in (b) are equalities. If $\Phi$ is symplectic, we may assume $\langle \beta, \alpha \rangle = 2$ and (2) becomes

$$\{u^2, v_\beta^\beta = [\hat{h}_\alpha(u), \hat{h}_\beta(v)].$$

By (1.1), $\{u^2, v_\beta^\beta = \{u, v^2\}_{\beta}$; thus it follows from (3) that if every $v \in (1 + q)^*$ is a square, again

$$D(\Phi, q) \subseteq [\hat{H}(\Phi, A), \hat{K}(\Phi, q)]$$

which completes the proof of (b).

For fixed $\beta$, let $D_\beta$ be the subgroup of $D(\Phi, q)$ generated by all $\{u, v_\beta^\beta, u \in A^*, v \in (1 + q)^* \}$. Let $\sigma = \sigma_\alpha$ be an element of the Weyl group of $\Phi$. Then relation (R5) and (a) imply
for some $\eta = \pm 1$. This proves $D_\beta \subseteq D_{\sigma \beta}$, and, by symmetry, $D_\beta = D_{\sigma \beta}$. Since the Weyl group acts transitively on roots of the same length, we have shown that if $\alpha$ and $\beta$ have the same length, $D_\alpha = D_\beta$.

Suppose then that $\beta$ is short and choose a long root $\alpha$ such that $\langle \beta, \alpha \rangle = 1$. Then by (2)

$$\{u, v\}_\beta = [\hat{b}_\alpha(u), \hat{b}_\beta(v)] = [\hat{b}_\beta(v), \hat{b}_\alpha(u)]^{-1} = \{u(\alpha, \beta) \cdot u \}_{\alpha}^{-1}$$

which proves $D_\beta \subseteq D_\alpha$. Since by (1.1)(S6) $\{u, u\}_\alpha = \{u, u\}_{\alpha}$, we have shown $D_\alpha = D(\Phi, q)$, proving the first part of (c); the rest of (c) is now an easy corollary.

Remark. In view of (1.3) we will usually write $\{, \}$ for $\{, u\}$; in that case it is to be understood that the symbol in question is taken with respect to a fixed long root $\alpha$.

2. The relative Bruhat decomposition for a radical ideal.

(2.1) Lemma. Let $\alpha \in \Delta$.

(a) $\hat{U}(\Phi, q) = \hat{U}(\Phi_+ - \{\alpha\}, q) \cdot \hat{U}(\alpha, q)$.

(a') $\hat{U}(\Phi_+ - \{\alpha\}, q)$ is normalized by $St_\alpha(\Delta)$.

(b) $\hat{U}(\Phi_+ - \{\alpha\}, q)$ is normalized by $St_\alpha(\Delta)$.

The set of roots $\Phi_+ - \{\alpha\}$ (resp. $\Phi_- - \{\alpha\}$) is an ideal in the closed sets of roots $\Phi_+$ and $(\Phi_+ - \{\alpha\}) \cup \{-\alpha\}$ (resp. $\Phi_-$ and $(\Phi_- - \{\alpha\}) \cup \{\alpha\}$). The lemma thus follows from [18, Lemmas 16, 17, 18, 36].

Definition. Set $\hat{M}(\Phi, q) = \hat{U}(\Phi, q)\hat{K}(\Phi, q)\hat{U}(\Phi, q)$, a subset of $St(\Phi, q)$ (cf. (2.7)). Recall from (1.3) that if $\Phi$ is nonsymplectic or if $(1 + q)^2 = (1 + q)^*$, then $\hat{K}(\Phi, q) = \hat{H}(\Phi, q)$, and that in any case, $\hat{K}(\Phi, q)$ is the product of the central subgroup $D(\Phi, q)$ with the group generated by all $\hat{b}_v(\nu), v \in (1 + q)^*$. Thus $\pi(\hat{K}(\Phi, q)) = H(\Phi, q)$.

(2.2) Lemma. $\hat{U}(\Phi, q)\hat{K}(\Phi, q)\hat{M}(\Phi, q) = \hat{M}(\Phi, q) = \hat{M}(\Phi, q)\hat{K}(\Phi, q)\hat{U}(\Phi, q)$.

This follows from relation (R6) which shows that $\hat{H}(\Phi, q)$, and therefore also $\hat{K}(\Phi, q)$, normalizes $\hat{U}(\Phi, q)$ and $\hat{U}(\Phi, q)$. 

\[\{u, v\}_\beta = \tilde{\omega}_\alpha(1) \cdot \{u, v\}_\beta \cdot \tilde{\omega}_\alpha(-1)\]

\[= \tilde{\omega}_\alpha(1) \cdot \hat{b}_\beta(\nu) \hat{b}_\beta(\nu)^{-1} \cdot \tilde{\omega}_\alpha(-1)\]

\[= \hat{b}_{\sigma \beta}(\eta \nu) \hat{b}_{\sigma \beta}(\eta)^{-1} \hat{b}_{\sigma \beta}(\eta \nu)^{-1} \hat{b}_{\sigma \beta}(\eta) \hat{b}_{\sigma \beta}(\eta \nu)^{-1}\]

\[= \hat{b}_{\sigma \beta}(\eta \nu) \hat{b}_{\sigma \beta}(\eta)^{-1} \hat{b}_{\sigma \beta}(\eta \nu)^{-1} \hat{b}_{\sigma \beta}(\eta) \hat{b}_{\sigma \beta}(\eta \nu)^{-1}\]

\[= \{\eta \nu, v\}_{\sigma \beta} \{\eta, \nu\}_{\sigma \beta}^{-1}\]
Theorem. (a) The product map \( \tilde{U}^{-}(\Phi, q) \times \tilde{k}(\Phi, q) \times \tilde{U}(\Phi, q) \to \tilde{St}(\Phi, q) \) is injective.

(b) \( L(\Phi, A) \cap \hat{M}(\Phi, q) \subset \hat{k}(\Phi, q) \).

(c) \( \hat{M}(\Phi, q) = \tilde{St}(\Phi, q) \) implies \( q \subset \text{rad } A \).

Suppose \( \hat{u}, \hat{u'} \in \tilde{U}(q), \hat{v}, \hat{v'} \in \tilde{U}^{-}(q) \) and \( \hat{k}, \hat{k'} \in \hat{k}(q) \). Then if \( \hat{v} \hat{k} \hat{u} = \hat{v'} \hat{k'} \hat{u'} \), we have

\[ \pi(\hat{v}^{-1} \hat{v'}) = \pi(\hat{k'} \hat{u'} \hat{u}^{-1} \hat{k}^{-1}) \in U^{-}(A) \cap U(A)H(A) = \{1\} \]

by [18, Lemma 21]. Hence \( \hat{v} = \hat{v'} \), since \( \pi|U^{-}(A) \) is an isomorphism [18, Lemma 36]. Similarly \( \hat{u} = \hat{u'} \), and therefore \( \hat{k} = \hat{k'} \), proving (a).

Now suppose \( \pi(\hat{v} \hat{k} \hat{u}) = 1 \). Then \( \pi(\hat{v}) = \pi(\hat{u}^{-1} \hat{k}^{-1}) \in U^{-}(A) \cap U(A)H(A) = \{1\} \) implies \( \hat{v} = 1 \); hence \( \hat{u} = 1 \) also, proving (b).

Finally, it is easily checked in \( \text{SL}(2, A) \) that \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U^{-1}HU \implies a \in A^{*} \). Moreover, \( \phi_{a}^{-1}(U^{-1}HU) \subset U^{-1}HU \), where the decomposition on the right is in \( \text{SL}(2, A) \) and \( \phi_{a}: \text{SL}(2, A) \to E_{\alpha}(A) \) is the homomorphism of [14, (3.6)].

Applying these remarks to \( \begin{pmatrix} 1 + q & -q \\ q & 1 - q \end{pmatrix} \in \phi_{a}^{-1}(\pi(x_{\alpha}(1)x_{-\alpha}(q)x_{\alpha}(-1))) \) for any \( q \in q \), we see that \( \hat{M}(q) = \tilde{St}(q) \) implies \( (1 + q) \subset A^{*} \) and therefore, \( q \subset \text{rad } A \). This proves (c).

The key result of this section is the following partial converse to (2.3)(c):

(2.4) Theorem. Let \( (A, q) \) be a radical pair and assume \( A = \mathbb{Z}[A^{*}] \). Then \( \tilde{St}(\Phi, q) = \hat{M}(\Phi, q) \).

(2.5) Theorem. Let \( (A, q) \) be a radical pair with \( A = \mathbb{Z}[A^{*}] \), and suppose \( \Phi_{l} \subset \Phi_{m} \) are reduced irreducible root systems of the same type. Then \( L(\Phi_{m}, q) \) is generated by all \( \{u, v\}_{\alpha, \nu} \in A^{*}, \nu \in (1 + q)^{*} \) for any fixed long root \( \alpha \), and the homomorphisms \( L(\Phi_{l}, q) \to L(\Phi_{m}, q) \) are surjective for all \( m \geq l \geq 1 \), including \( m = \infty \) if \( \Phi_{m} \) is classical.

If, in addition, \( \Phi_{m} \) and \( A \) satisfy one of the hypotheses of [14, Theorem 5.3], \( \tilde{St}(\Phi_{m}, (0, q)) \) is the universal \( E(\Phi_{m}, A) \)-covering [14, §2] of \( E(\Phi_{m}, q) \).

This theorem is a corollary of (2.3)(b), (2.4) and (1.3).

Note. The hypothesis \( A = \mathbb{Z}[A^{*}] \) is innocent. It is fulfilled, for example, by semilocal rings having at most one residue field with 2 elements [14, (4.2)] (in particular, by local rings) and by group rings.

The proof of (2.4) will be based on a series of lemmas.
(2.6) Lemma. Let $\alpha \in \Delta$, $t \in A$. Then $x_\alpha(t)$ normalizes $\hat{M}(q)$ if and only if

$$x_\alpha(t) \hat{U}(-\alpha, q) x_\alpha(-t) \subseteq \hat{M}(q).$$

The "only if" is clear. For the converse, we assume $\alpha \in \Delta$ (the case $\alpha \in -\Delta$ is similar). By (2.1)(a−), we have

$$\hat{M}(q) = \hat{U}(\Phi_\alpha - \{\alpha\}, q) \cdot \hat{U}(-\alpha, q) \cdot \hat{K}(q) \cdot \hat{U}(q).$$

Since $x_\alpha(t)$ normalizes $\hat{U}(\Phi_\alpha - \{\alpha\}, q)$ by (2.1)(b−) and also normalizes $\hat{U}(q)$, it suffices to prove

$$x_\alpha(t) \cdot \hat{U}(-\alpha, q) \hat{K}(q) \cdot x_\alpha(-t) \subseteq \hat{M}(q)$$

and, in view of the hypothesis and (2.2), that would follow from

$$x_\alpha(t) \cdot \hat{K}(q) \cdot x_\alpha(-t) \subseteq \hat{K}(q) \cdot \hat{U}(q)$$

which is true since $\hat{K}(q) \subseteq \hat{H}(A)$ and $\hat{H}(A)$ normalizes $\hat{U}(q)$ by relation (R6).

(2.7) Proposition. Let $u, v \in A^*$, $\alpha \in \Phi$. The following identities hold in $St(\Phi, A)$:

$$\{ u, v \}_{\alpha} \alpha_{-\alpha}(v) \alpha_{-\alpha}(u)$$

(a) $$= x_\alpha(-u^{-1}(1 - v^{-1})) \cdot x_\alpha(-u^{-1}(u(v - 1))) \cdot x_\alpha(u(v - 1)^{-1}))$$

(b) $$= x_\alpha(-u^{-1}(v^{-1} - 1)) \cdot x_\alpha(u(1 - v^{-1}))$$

(c) $$= x_\alpha(-u^{-1}(u^{-1} - 1)) \cdot x_\alpha(u(1 - v^{-1}))$$

Proof. (a)

$$\{ u, v \}_{\alpha} \alpha_{-\alpha}(v) = \alpha_{-\alpha}(uv) \alpha_{-\alpha}(u^{-1}) = \alpha_{-\alpha}(uv) \alpha_{-\alpha}(uv^{-1})$$

$$= x_\alpha(-u^{-1}(1 - v^{-1})) \cdot x_\alpha(-u^{-1}(u(v - 1))) \cdot x_\alpha(u(v - 1)^{-1}))$$

(b) follows immediately from (a).
(c) In (b) exchange \( \alpha \) with \(-\alpha\) and \( u \) with \( u^{-1} \); then take the inverse of each side. The identities \( \hat{h}_{-\alpha}(v)^{-1} = \hat{h}_\alpha(v) \) and \( \left| u^{-1}, v \right|_{-\alpha} = \left| v^{-1}, u \right|_{\alpha} = \left| u, v \right|_{\alpha} \) complete the proof.

(2.8) Corollary. Let \( \alpha \in \Phi \), \( q \in \text{rad} \, A \). For all \( u, v, u', v' \in A^* \) such that \( u + v = u' + v' \), the symbol \( \left| u, v \right|_{\alpha} \) satisfies the identity

\[
\left| u, (1 + qz)/(1 + qv) \right|_{\alpha} \left| v, 1 + qv \right|_{\alpha}^{-1} \left| 1 + qv \right|_{\alpha}^{-1} \left| v', 1 + qv' \right|_{\alpha}^{-1} = \left| u', (1 + qz)/(1 + qv') \right|_{\alpha}^{-1} \left| v', 1 + qv' \right|_{\alpha}^{-1} \left| 1 + qv' \right|_{\alpha}^{-1}
\]

where \( z = u + v = u' + v' \). Moreover if \( z \in A^* \), both sides of (S9) equal \( |z, 1 + qz|_{\alpha} \).

Since \( u + v = u' + v' \), we must have

\[
\left| x_{\alpha}(-u)x_{\alpha}(-v), x_{\alpha}(-u')x_{\alpha}(-v') \right|_{\alpha} = \left| x_{\alpha}(-u)x_{\alpha}(qw^{-1})x_{\alpha}(-qz), x_{\alpha}(-u)x_{\alpha}(qw^{-1})x_{\alpha}(-qz) \right|_{\alpha}.
\]

We will use (2.7) to put (1) into \( \hat{M}(q) \); (S9) will then follow by comparing the terms in \( \hat{M}(q) \) which are uniquely determined according to (2.3)(a).

Write \( w = 1 - qv \in A^* \). Then \( \left| q, 1 - qw \right| = \left| q, 1 - qv \right|^{-1} \); applying (2.7)(c) with \( z = v, v' = z' ; v'' = z'' \) yields

\[
\left| x_{\alpha}(-u)x_{\alpha}(-v), x_{\alpha}(-u')x_{\alpha}(-v') \right|_{\alpha} = \left| x_{\alpha}(-u)x_{\alpha}(qw^{-1})x_{\alpha}(-qz), x_{\alpha}(-u)x_{\alpha}(qw^{-1})x_{\alpha}(-qz) \right|_{\alpha}.
\]

Similarly write \( x = 1 - quw^{-1} = u^{-1}(1 - x) \);\( x^{-1} = 1 - qz \) and we have

\[
\left| x_{\alpha}(u), x_{\alpha}(qw^{-1}), x_{\alpha}(q(1 - qz)^{-1}) \left| u, x_{\alpha}(x), x_{\alpha}(-qz^2(1 - qz)^{-1}) \right|_{\alpha} \right|_{\alpha}.
\]

Combining (2) and (3), and simplifying using relation (R6) and the definition of \( \left| u, v \right|_{\alpha} \) gives the identity

\[
\left| x_{\alpha}(-u)x_{\alpha}(-v), x_{\alpha}(-u')x_{\alpha}(-v') \right|_{\alpha} = \left| x_{\alpha}(-u)x_{\alpha}(qw^{-1})x_{\alpha}(1 - qz)x_{\alpha}(-qz^2(1 - qz)^{-1}) \right|_{\alpha}.
\]

(It should be noted that in deriving (4) we need only the weaker hypotheses \( u, v, 1 - qv, 1 - ku, 1 - qz \in A^* \); this will be important in (2.9) below.) We perform a similar calculation for \( \left| x_{\alpha}(-u)x_{\alpha}(-v), x_{\alpha}(-u')x_{\alpha}(-v') \right|_{\alpha} \); the identity follows by comparing the terms in \( \hat{K}(q) \) (noting that \( \hat{h}_{-\alpha}(1 - qz) \) depends only on \( z \)) and replacing \( q \) by \(-q\).

Finally if \( z \in A^* \), we may use (2.7)(c) to compute \( \left| x_{\alpha}(z), x_{\alpha}(-z) \right|_{\alpha} \) directly; comparing \( \hat{K}(q) \) terms, we see that \( |z, 1 + qz|_{\alpha} \) must equal both sides of (S9).

(2.9) Corollary. Let \( u, v \in A^* \), \( \alpha \in \Phi \) and write \( p = u - 1, q = v - 1 \). Then if \( pq = 0, q + 1, 1 + pq \in \Phi \), \( \left| [x_{-\alpha}(q), x_{-\alpha}(p)] \right|_{\alpha} \).

We will compute the right-hand side using (4) above. Make the substitutions

\[ -u = u, -v = v, -u' = u', -v' = v' \text{ in (4); then } z = p, 1 = qz = 1 - qp = 1, x^{-1} = w = 1 + q, \text{ and} \]

\[ \left| x_{\alpha}(-u)x_{\alpha}(-v), x_{\alpha}(-u')x_{\alpha}(-v') \right|_{\alpha} = \left| x_{\alpha}(-u)x_{\alpha}(qw^{-1})x_{\alpha}(1 - qz)x_{\alpha}(-qz^2(1 - qz)^{-1}) \right|_{\alpha}.
\]
\[ x_a(p) x_{-a}(-q) = x_a(u) x_{-a}(-1) \]
\[ x_{-a}(-q) = x_{-a}(-q) \]  \[ -u, x \}_{a}^{-1}, x \}_{a}^{-1}. \]
Therefore
\[ [x_{-a}(q), x_a(p)] = \{-u, x\}_{a}^{-1}, x \}_{a}^{-1}. \]
But (1.1) implies
\[ \{-u, x\}_{a}^{-1}, x \}_{a}^{-1} = \{-1, x\}_{a}^{-1}, x \}_{a}^{-1} \]
and therefore
\[ \{u^{-1}, x\}_{a}^{-1} = \{x, u^{-1}\}_{-a} = \{x^{-1}, u\}_{-a} = \{1 + q, 1 + pl_{-a} \}
\]
which yields the desired result by interchanging \( a \) and \( -a \).

(2.10) Proposition. Let \((A, q)\) be a radical pair. Then \( \hat{M}(q) \) is a normal subgroup of \( St(\Phi, Z[A^*]) \).

Let us first show that (2.10) completes the proof of (2.4). The hypotheses of (2.4) imply that \( St(\Phi, A) = St(\Phi, Z[A^*]) \); thus by (2.10), \( \hat{M}(q) \) is a normal subgroup of \( St(\Phi, A) \) containing all \( \hat{U}(a, q) \). Therefore \( St(\Phi, q) \subseteq \hat{M}(q) \). But \( \hat{M}(q) \subseteq St(\Phi, q) \), whence (2.4).

Now let us prove (2.10). \( St(\Phi, Z[A^*]) \) is generated by all \( x_a(t), a \in \pm \Delta, t \in A^* \). By (2.6), the set \( \hat{M}(q) \) is normalized by \( St(\Phi, Z[A^*]) \) if and only if \( x_a(t) x_{-a}(q) \in \hat{M}(q) \) for all \( a \in \pm \Delta, t \in A^*, q \in q \). Since \( q \subseteq Z[A^*] \), this follows from (2.7)(b) and (c).

Now since \( \hat{U}^{-}(q) \subseteq St(\Phi, Z[A^*]) \), we have
\[ \hat{M}(q) = \hat{M}(q) \hat{U}^{-}(q) \hat{K}(q) \hat{U}(q) = \hat{U}^{-}(q) \hat{M}(q) \hat{K}(q) \hat{U}(q) = \hat{M}(q) \]
by (2.2). Therefore \( \hat{M}(q) \), being the monoid generated by 3 groups, is a group.

Remark. In showing \( \hat{M}(q) = St(\Phi, q) \) for a radical pair \((A, q)\), the restriction \( A = Z[A^*] \) was needed only in verifying (2.6). In \( SL(2, A) \), however, it is easy to show that
\[ e_a(t) U(-a, q) e_{-a}(-t) \subseteq U^{-}(q) H(q) U(q); \]
this is simply the matrix equation
\[ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} ^{-1} \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ u & 0 \end{pmatrix} \begin{pmatrix} 1 & -t^2 qu^{-1} \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \]
where \( u = 1 + t q \in A^* \), since \( q \subseteq rad A \). We conclude

(2.11) Corollary. Let \((A, q)\) be a radical pair. Then
\[ E(\Phi, q) = U^{-}(q) H(q) U(q). \]
(2.12) Lemma. If \( \text{rk } \Phi \geq 2 \), \( \text{St}(\Phi, \alpha) \) preserves finite products. If \( \text{rk } \Phi = 1 \), \( \text{St}(\Phi, B) \approx \text{St}(\Phi, A \times B)/C \), where \( C \) is the normal subgroup generated by all \( [x_{\alpha}((a, 0)), x_{-\alpha}((0, b))] \).

There is always a surjective homomorphism \( p: \text{St}(\Phi, A \times B) \to \text{St}(\Phi, A) \times \text{St}(\Phi, B) \) induced by the projections of \( A \times B \) onto its factors. Now \( \text{St}(\Phi, A) \times \text{St}(\Phi, B) \) is generated by all \( (x_{\alpha}(a), 1), (1, x_{\beta}(b)) \), and we may define a map \( s \) backwards by

\[
(x_{\alpha}(a), 1) \mapsto x_{\alpha}((a, 0)), \quad (1, x_{\beta}(b)) \mapsto x_{\beta}((0, b)).
\]

To show this defines an inverse isomorphism to \( p \), we must check that the defining relations of \( \text{St}(\Phi, A) \times \text{St}(\Phi, B) \) are preserved by \( s \). These relations are

(i) the defining relations of \( \text{St}(\Phi, A) \) applied to the generators \( (x_{\alpha}(a), 1) \),
(ii) the defining relations of \( \text{St}(\Phi, B) \) applied to the generators \( (1, x_{\beta}(b)) \),
(iii) \( [x_{\alpha}((a, 0)), x_{-\alpha}((0, b))] = 1 \) for all \( \alpha, \beta \in \Phi, a \in A, b \in B \).

It is clear that \( s \) preserves (i) and (ii). Moreover relation (R2) in \( \text{St}(\Phi, A \times B) \) shows that \( s \) preserves (iii) whenever \( \beta \neq -\alpha \). Hence the induced map \( s: \text{St}(\Phi, A) \times \text{St}(\Phi, B) \to \text{St}(\Phi, A) \times \text{St}(\Phi, B)/C \) is an isomorphism, since \( p(C) = 1 \). This completes the proof when \( \text{rk } \Phi = 1 \).

If \( \text{rk } \Phi \geq 2 \), there exist \( \beta, \gamma \in \Phi, \beta, \gamma \neq -\alpha \), such that

\[
x_{-\alpha}((0, b)) = [x_{\beta}((0, 1)), x_{\gamma}((0, b))]y
\]

where \( y \in \hat{U}(S, (0, B)) \), for some \( S \subset \Phi \) with \( -\alpha \notin S \). Hence

\[
[x_{\alpha}((a, 0)), x_{-\alpha}((0, b))] = [x_{\alpha}((a, 0)), [x_{\beta}((0, 1)), x_{\gamma}((0, b))]y] = 1
\]

which proves \( C = 1 \) and the lemma.

(2.13) Theorem. Let \( A \) be a semilocal ring with at most one residue field isomorphic to \( \mathbb{F}_2 \), and suppose \( \Phi \) is a reduced irreducible root systems of the same type. Then the homomorphisms \( \delta(l, m): L(\Phi, A) \to L(\Phi, A) \) are surjective for all \( m \geq l \geq 1 \), including \( m = \infty \) if \( \Phi \) is classical.

If \( l \geq 2 \), \( L(\Phi, A) \) is the central subgroup generated by all \( \{u, v\} \), \( u, v \in A^* \), for any fixed long root \( \alpha \). This is also true when \( l = 1 \), provided either that \( A \) has no residue field isomorphic to \( \mathbb{F}_2 \) or that \( A \) is a local ring.

If, in addition, \( \Phi \) and \( A \) satisfy one of the hypotheses of [14, Theorem 5.3], \( \text{St}(\Phi, A) \) is the universal covering of \( E(\Phi, A) \) and \( L(\Phi, A) \approx H_2(E(\Phi, A), \mathbb{Z}) \).

Write \( \overline{A} = A/\text{rad } A \), a finite product of fields. Steinberg [17] has shown that \( L(\Phi, k) = D(\Phi, k) \) when \( k \) is a field. Since \( E(\Phi, k) \) preserves finite products, it follows from (2.12) that \( L(\Phi, \overline{A}) = D(\Phi, \overline{A}) \) if \( \text{rk } \Phi \geq 2 \), and that \( L(\Phi, \overline{A}) \) is generated by \( D(\Phi, \overline{A}) \) and \( C \) when \( \text{rk } \Phi = 1 \), where \( C \) is the normal subgroup generated by all
(the appropriate generalization of the subgroup $C$ of (2.12) when $\bar{A}$ is a product of more than 2 factors).

Now suppose $rk \Phi = 1$. Then if $A$ is local, $L(\Phi, \bar{A}) = D(\Phi, \bar{A})$ by Steinberg [17]. If $A$ is semilocal but has no residue field isomorphic to $F_2$, we want to show $C \subset D(\Phi, \bar{A})$, and it clearly suffices to consider the case $\bar{A} = k \times k'$, a product of two fields. Then by (2.9),

$$[x_a((0, 0), x_{-a}((0, b))] = \{(1 + a, 1), (1, 1 + b)\}_a \in D(\Phi, \bar{A})$$

provided neither $a$ nor $b$ equals $-1$. But even if $a = -1$,

$$[x_{-a}((-1, 0)), x_a((0, b))] = [x_{-a}((0, b)), x_a((1, 0))]$$

and a similar argument applies if $b = -1$. Hence if $-1 \neq 1, C \subset D(\Phi, \bar{A})$.

Thus our hypotheses imply $L(\Phi, q) = D(\Phi, q)$ and the second part of the theorem follows from the exact sequence

$$1 \rightarrow L(\Phi, q) \rightarrow L(\Phi, A) \rightarrow L(\Phi, \bar{A}) \rightarrow 1$$

together with (1.3).

The first part of the theorem is a consequence of the second and (1.3), and the last part follows from [14, (5.3)].

(2.14) Corollary. Let $A$ be a semilocal ring with at most one residue field isomorphic to $F_2$. If $rk \Phi = 1$, assume further that either $A$ is local, or that $A$ has no residue field isomorphic to $F_2$. Then $E(\Phi, A)$ has a presentation by generators $e_\alpha(t), \alpha \in \Phi, t \in A$, and relations (R1), (R2) (resp. (R3)) if $rk \Phi = 1$ and

$$(C) b_\alpha(u)b_\alpha(v) = b_\alpha(uv), \quad u, v \in A^*, \alpha \in \Phi.$$ 

The proof is the same as [18, Theorem 8(b)] in view of (2.13).

Note. Theorems related to (2.14) have been proved by Silvester [11], [12], and Wardlaw [19].

(2.15) Proposition. Let $\mathfrak{p}, q$ be ideals of $A$.

(a) If $rk \Phi = 1$, assume $L(\Phi, q)$ is central in $St(\Phi, A)$. Then if $St(\Phi, q)$ is generated by $M(q)$,

$$[St(\Phi, A), [St(\Phi, q), St(\Phi, \mathfrak{p})]] \subset St(\Phi, \mathfrak{p} \cap q).$$
(b) Suppose \( r_k > 1 \) and that \( 2 \in A^* \) if \( \Phi = C_2 \). If either \( \text{St}(\Phi, q) \) is generated by \( \tilde{M}(q) \) or \( \text{St}(\Phi, \beta^2) \) is generated by \( \tilde{M}(\beta^2) \), then

\[
[\text{St}(\Phi, q), \text{St}(\Phi, \beta^2)] \subseteq \text{St}(\Phi, \beta q).
\]

Suppose \( M, N \) are normal subgroups of a group \( G \), and define

\[
(M : N) = \{ g \in G : [g, N] \subseteq M \}.
\]

It follows from the commutator formulas of [14, (2.1)] that \((M : N)\) is a normal subgroup of \( G \). The conclusions of the proposition are thus equivalent to

\[
\begin{align*}
(a') \quad & \text{St}(\beta^2) \subseteq ((\text{St}(p q) : \text{St}(A)) : \text{St}(q)), \\
(b') \quad & \text{St}(\beta^2) \subseteq (\text{St}(p q) : \text{St}(q)).
\end{align*}
\]

The groups on the right in \((a')\) and \((b')\) are normal in \( \text{St}(\Phi, A) \); therefore by [14, (2.1)] it suffices to prove

\[
\begin{align*}
(a'') \quad & \hat{U}(\alpha, \beta^2) \subseteq ([\hat{U}(\beta, p^2) : \hat{U}(\gamma, p) \cdot \hat{U}(S, p^2)]), \\
(b'') \quad & \hat{U}(\alpha, \beta^2) \subseteq (\text{St}(p q) : \text{St}(q))
\end{align*}
\]

for one root \( \alpha \) of each length.

If \( \beta \neq -\alpha \), (R2) implies that

\[
[\hat{U}(\alpha, \beta), \hat{U}(\beta, q)] \subseteq \text{St}(\beta q).
\]

Suppose \( r_k \Phi > 1 \) and that \( 2 \in A^* \) if \( \Phi = C_2 \). Then (R2) implies the existence of \( \beta, \gamma \in \Phi \) such that

\[
\hat{U}(\alpha, \beta^2) \subseteq [\hat{U}(\beta, \beta), \hat{U}(\gamma, \beta) \cdot \hat{U}(S, \beta^2)],
\]

where \( S \subseteq \Phi \) and \( \alpha \notin S \). Therefore

\[
[\hat{U}(\alpha, \beta^2), \hat{U}(\gamma, \beta^2)] \subseteq [\hat{U}(\beta, \beta), \hat{U}(\gamma, \beta) \cdot \hat{U}(S, \beta^2), \hat{U}(\gamma, \beta^2) \subseteq \text{St}(\beta q)]
\]

(The last inclusion follows from [14, (2.1)] and (5).)

Finally, \( \hat{K}(\Phi, q) \) is generated by elements of the form \( \{ u, v \beta \} \tilde{h}_{\beta}(v), u \in A^*, v \in (1 + q)^* \). Therefore since \( \{ u, v \} \beta \) is central, relation (R6) implies

\[
[x_\alpha(p), [u, v] \beta \tilde{h}_{\beta}(v)] = [x_\alpha(p), \tilde{h}_{\beta}(v)] = x_\alpha(p' q')
\]

for some \( p' \in \beta, q' \in q \), which implies that

\[
[\hat{U}(\alpha, \beta), \hat{K}(q)] \subseteq \text{St}(\beta q).
\]

Clearly \((b'')\) is a consequence of \((5), (6), (7)\); this is true under either hypothesis of (b) since \((b')\) is equivalent to

\[
\text{St}(q) \subseteq (\text{St}(\beta q) : \text{St}(\beta^2)).
\]
From (5) and (7) we also conclude that

\[ [\hat{U}(\alpha, p), St(q)] = St(pq) \cdot [\hat{U}(\alpha, p), \hat{U}(-\alpha, q)]. \]

It is easily checked, moreover, that in \( SL(2, A) \)

\[ [U(\alpha, p), U(-\alpha, q)] \subseteq E(pq) \]

and therefore

\[ [\hat{U}(\alpha, p), St(q)] \subseteq St(pq) \cdot (L(\Phi, q) \cap St(A)). \]

Since \( L(\Phi, A) \cap St(A) \) is central in \( St(\Phi, A) \) (by [14, (5-1)] if \( \text{rk } \Phi > 1 \) and by hypothesis if \( \text{rk } \Phi = 1 \)), (a) is proved.

(2.16) Corollary. Let \((A, q)\) be a radical pair and assume \( A = Z[A^*] \). If \( p \subseteq A \) is an ideal such that \( pq = 0 \), then \([St(\Phi, p), St(\Phi, q)]\) is central in \( St(\Phi, A) \).

Moreover if \( \text{rk } \Phi > 1 \) and 2 \( \in A^* \) if \( \Phi = C_2 \), then for all \( i \geq 2 \),

\[ [St(\Phi, p^i), St(\Phi, q^i)] = [St(\Phi, p), St(\Phi, q)] = 1. \]

(2.17) Corollary. Let \((A, q)\) be as in (2.15) and suppose further that \( q^n + 1 = 0 \). Then \( \Gamma = [St(\Phi, q^n), St(\Phi, q)] \) is central in \( St(\Phi, A) \) if \( i + j \geq n + 1 \). If \( \text{rk } \Phi > 1 \) and if \( 2 \in A^* \) if \( \Phi = C_2 \), \( \Gamma \) is trivial when \( i + j \geq n + 2 \).

3. Some computations for local rings.

(3.1) Proposition. For any pair \((A, q)\), the sequence

\[ 1 \rightarrow L(\Phi, q) \rightarrow L(\Phi, A) \rightarrow L(\Phi, A/q) \]

is exact.

Except for the "1" on the left, this is just [16, (3.2)]. Exactness at the left holds because the group \( L(\Phi, q) \) used here is the image under the natural homomorphism of the group \( L(\Phi, q) \) of [16], and is therefore a subgroup of \( L(\Phi, A) \).

(3.2) Proposition [17, 3.3]. If \( k \) is an algebraic extension of a finite field, \( L(\Phi, k) = 1 \).

(3.3) Proposition. (a) For every positive integer \( m \) not divisible by 4, \( L(\Phi, Z/mZ) = 1 \), provided \( \text{rk } \Phi \geq 2 \).

(b) For every integer \( n \geq 2 \), the groups \( L(\Phi, Z/2^{n+1}Z) \) and \( L(\Phi, Z/2^nZ) \) are isomorphic and are generated by the symbol \( \{-1, -1\} \), which has order at most 2 if \( \Phi \) is nonsymplectic.

Proof. (a) Since \( L(\Phi, ) \) commutes with finite products, the Chinese remainder theorem implies we may assume \( m = p^n \), \( p \) a prime; we may further assume \( n > 1 \) and \( p \neq 2 \) by (3.2). Since \( Z/p^nZ \) satisfies the hypotheses of (2.13), it follows from (3.2) and from (3.1) with \( q = \text{rad}(Z/p^nZ) = pZ/p^nZ \) that \( L(\Phi, Z/p^nZ) \) is isomorphic.
to $L(\Phi, p\mathbb{Z}/p^n\mathbb{Z})$ which, according to (2.5), is generated by all $u, v, u \in (\mathbb{Z}/p^n\mathbb{Z})^*$, $v \in (1 + p\mathbb{Z}/p^n\mathbb{Z})$.

Now $(\mathbb{Z}/p^n\mathbb{Z})^*$ is a cyclic group of order $(p - 1)p^{n-1}$, isomorphic to the direct product $(\mathbb{Z}/p\mathbb{Z})^* \times (1 + p\mathbb{Z}/p^n\mathbb{Z})$. Hence (1.1)(S7), (S8) imply $\{u, v^2\} = 1$ ($u, v$ as above). Since $p$ is odd, every element of $1 + p\mathbb{Z}/p^n\mathbb{Z}$ is a square, which proves (a).

(b) Again the hypotheses of (2.13) are satisfied. It follows from (1.1)(S1) that $\{-1, -1\}$ is the only possibly nontrivial symbol in $L(\Phi, \mathbb{Z}/4\mathbb{Z})$, and if $\Phi$ is nonsymplectic, (1.1)(S6) implies that the order of this symbol is at most 2. Since $(\mathbb{Z}/2^{n+1}\mathbb{Z})^* \to (\mathbb{Z}/2^n\mathbb{Z})^*$ is surjective, we have, by (2.13) and (3.1), an exact sequence

$$1 \to L(\Phi, 2^n\mathbb{Z}/2^{n+1}\mathbb{Z}) \to L(\Phi, \mathbb{Z}/2^{n+1}\mathbb{Z}) \to L(\Phi, \mathbb{Z}/2^n\mathbb{Z}) \to 1$$

for all $n \geq 1$ and all $\Phi$. Thus to complete the proof of (b) it suffices to show

$$L(\Phi, 2^n\mathbb{Z}/2^{n+1}\mathbb{Z}) = 1 \quad \text{for } n \geq 2.$$

Let $n \geq 2$. According to (2.5), $L(\Phi, 2^n\mathbb{Z}/2^{n+1}\mathbb{Z})$ is generated by the symbols $1 + 2^n, u, u \in (\mathbb{Z}/2^{n+1}\mathbb{Z})^*$. Now $(\mathbb{Z}/2^{n+1}\mathbb{Z})^*$ is the direct product of the group $\{1\}$ with the cyclic group of order $2^{n-1}$ generated by the residue class of 5 modulo $2^{n+1}$. Moreover, an easy induction argument shows that for all $n \geq 2$,

$$1 + 2^n = 5^s \mod 2^{n+1}, \quad s = 2^{n-2}. \quad (1)$$

Now assume $n \geq 3$. Then $1 + 2^n$ is a square and (1.1)(S6) implies that $L(\Phi, 2^n\mathbb{Z}/2^{n+1}\mathbb{Z})$ is generated by the two symbols $\{1 + 2^n, -1\}$, $\{1 + 2^n, 5\}$; since $\{1 + 2^n, -1\} = \{1 + 2^n, 1 + 2^n\} = \{1 + 2^n, 5\}$ by (1), this group is generated by the single symbol $\{1 + 2^n, 5\}$. Again applying (1) and computing in $L(\Phi, \mathbb{Z}/2^{n+1}\mathbb{Z})$, we have $\{1 + 2^n, 5\} = \{5^s, 5\} = 1$ by (1.1)(S8).

Now suppose $n = 2$. Then it follows from (2.5) and (1.1)(S1) and (S4) that $L(\Phi, 4\mathbb{Z}/8\mathbb{Z})$ is also generated by $\{5, -1\}$. Take $q = 2, u = u' = -1, u' = v = 5$ in (2.8) to conclude that, in $L(\Phi, \mathbb{Z}/8\mathbb{Z})$, $1 = \{5, -1\}$.

Note. For the functor $K_2 = \lim_{\to \infty} L(A, t)$, this proposition was proved by Milnor [9] using his computation of $K_2(\mathbb{Z})$ (cf. [11], [19]) and results of Menicke, Bass, Lazard and Serre [1] on the congruence subgroup problem.

(3.4) Proposition. Let $A$ be an artinian ring such that $A^*$ is cyclic, and suppose $\text{rk } \Phi \geq 2$. Then $L(\Phi, A) = 1$, except possibly when $A$ has a direct factor isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Eldridge and Fischer [4] have shown that if $A$ is artinian and $A^*$ is finitely generated, then $A$ is finite. Moreover, a finite ring is a finite product of primary rings $A_1, \ldots, A_n$ (rings with a unique prime ideal); if $A^*$ is cyclic, $A_i^*$ must also be cyclic for $i = 1, \ldots, n$ with $|A_i^*|$ and $|A_j^*|$ relatively prime for $i \neq j$. Gilmer
[5] has determined all primary rings with cyclic groups of units; they are
(a) $F_q$, $q$ a prime power,
(b) $\mathbb{Z}/p^m\mathbb{Z}$, $p$ an odd prime, $m > 1$,
(c) $\mathbb{Z}/4\mathbb{Z}$,
(d) $F_p[x]/(x^2)$, $p$ prime,
(e) $F_2[x]/(x^3)$,
(f) $\mathbb{Z}[x]/(4, 2x, x^2 - 2)$.

Since $L(\Phi, A)$ commutes with finite products, it suffices to compute $L(\Phi, A)$
when $A$ is one of the rings in (a)—(f) and we may apply (2.13). Propositions 3.2
and 3.3 above settle cases (a)—(c). In (d), (e), (f) we let $x$ denote the residue
class of $X$ in $A$.

In (d) we use (3.1), with $q = \text{rad } A = 1 + Ax$, and (3.2) to conclude that
$L(\Phi, A) \approx L(\Phi, 1 + Ax)$. If $\zeta$ is a generator of $F_p^*$, $A^*$ is the product of the cy-
clic group $\langle \zeta \rangle$ of order $p - 1$ with the cyclic group $\langle 1 + x \rangle = 1 + Ax$ of order $p$.
If $p$ is odd, $1 + x$ is a square, and $L(\Phi, 1 + Ax)$ is generated by $\{\zeta, 1 + x\}$ and
$\{1 + x, 1 + x\}$ according to (2.5) and (1.1)(S6). That these symbols are trivial fol-
lows from (1.1)(S6), (S8).

If $p = 2$ in (d), $\zeta = 1$ and $L(\Phi, 1 + Ax)$ is generated by
$$\{1 + x, 1 + x\} = \{1 + x, - (1 + x)\} = 1$$
by (S4) of (1.1).

In (e) and (f), $A^*$ is cyclic of order 4, generated by $1 + x$, and $L(\Phi, A)$ is
generated by $\{1 + x, 1 + x\}$. In (e) we have
$$\{1 + x, 1 + x\} = \{1 + x, - (1 + x)\} = 1,$$
and in (f)
$$\{1 + x, 1 + x\} = \{1 + x, (1 + x)^{-1}\} = \{1 + x, - (1 + x)\} = 1,$$
which completes the proof of (3.4).

Our next objective is to generalize Proposition 3.3. Throughout the rest of
this section we will assume $A$ is a local ring whose maximal ideal $\mathfrak{p}$ is principal
and generated by $\mu$. We further assume that $A/\mathfrak{p}$ is a finite field containing $q =
p^s$ elements.

For $n \geq 0$, the group of units $(A/p^{n+1})^*$ is the direct product $\langle \zeta \rangle \times (1 +
p/p^{n+1})$, where $\zeta \in (A/p^{n+1})^*$ is of order $q - 1$ and maps to a generator of $(A/p)^*$
$\approx (F_q)^*$. Since $A$ and $A/p^{n+1}$ are local, they are generated by their units.

(3.5) Lemma. For all $n \geq 0$ and $1 \leq i \leq n + 1$, the additive group $\mathfrak{p}^i/p^{n+1}$
and the multiplicative group $1 + \mathfrak{p}^i/p^{n+1}$ have exponent $p^{n-i+1}$. Hence if $p$
is odd, every element of $1 + \mathfrak{p}^{n+1}$ is a square.

The map $a \mapsto \bar{a}\mu^n$ induces, for all $n \geq 0$, an isomorphism of additive groups
$$A/\mathfrak{p} \cong \mathbb{Z}/p^n/\mathbb{Z}[x]/(x^2 - 2).$$
where we write $\bar{a}$ for the residue class of $a \in A$ modulo $p^{n+1}$. Since $(p^n/p^{n+1})^2 = 0$, $1 + p^n/p^{n+1} \approx p^n/p^{n+1}$ and both, therefore, have exponent $p$. The lemma follows by descending induction on $i$ and the exact sequences

$$0 \rightarrow \frac{p^{i+1}}{p^{n+1}} \rightarrow \frac{p^i}{p^{n+1}} \rightarrow \frac{p^i}{p^i+1} \rightarrow 0,$$

$$1 \rightarrow (1 + \frac{p^{i+1}}{p^{n+1}}) \rightarrow (1 + \frac{p^i}{p^{n+1}}) \rightarrow (1 + \frac{p^i}{p^i+1}) \rightarrow 1.$$

(3.6) Lemma. Let $k$ be a finite field. Every element of $k$ is a sum of squares. Every element of $k$ is a sum of fourth powers if and only if $k \neq \mathbb{F}_q$.

Let $k = \mathbb{F}_q$, $q = p^n$, and let $d$ be a positive nonzero integer. The subset $S$ of $k$ consisting of sums of $d$th powers is closed under addition, multiplication and subtraction, since $-1 = p - 1 = 1 + \cdots + 1$. Hence, $S$, being a subdomain of a finite field, is a subfield of $k$, and $S = \mathbb{F}_r$, $r = p^m$ for some $m$ dividing $n$. In particular, $p^m - 1$ divides $p^n - 1$ with quotient $c$.

Choose an $x \in k^*$ of order $p^n - 1$. Then $x^d \in S$ and thus $x^d(p^m-1) = 1$, which implies $p^n - 1 | d(p^m - 1)$. Hence $c(p^m - 1) | d(p^m - 1)$ and $c | d$. If $d = 2$, then $c = 1$ or $2$. If $c = 2$, then $2p^m - 2 = p^n - 1$, $p^m(2 - p^n - m) = 1$, $p = 1$.

Thus $c = 1$ and $n = m$.

If $d = 4$ we must have $c = 1$, 2 or 4, and we have seen above that $c = 2$ leads to a contradiction. If $c = 4$, then $p^m(4 - p^n - m) = 3$, $p = 3, m = 1, n = 2$.

and it is easily checked that $(\mathbb{F}_3)^4 = \mathbb{F}_3$.

Note. I would like to thank Armand Brumer who supplied the neat proof of this lemma.

(3.7) Corollary. The symbols $\{1 + s, 1 + t, s \in \frac{\mathbb{F}^*}{p^{n+1}}, t \in \frac{p^n}{p^{n+1}}$ generate $D(\Phi, \frac{\mathbb{F}}{p^{n+1}})$.

Recall from (1.3) that $D(\Phi, \frac{\mathbb{F}}{p^{n+1}})$ is the subgroup of $L(\Phi, \frac{\mathbb{F}}{p^{n+1}})$ generated by all $\{u, 1 + t, u \in (\mathbb{F}/p^{n+1})^*, t \in \frac{p^n}{p^{n+1}}$. Write $u = \zeta^i(1 + s)$, $s \in \frac{\mathbb{F}}{p^{n+1}}$, where $\zeta$ is of order $q - 1$. Then if $p$ is odd, $1 + s$ is a square by (3.5), and if $p = 2$, $\zeta^i$ is a square. In either case $(1.1)(S6)$ implies

$$\{u, 1 + t\} = \{\zeta^i, 1 + t\} \{1 + s, 1 + t\}$$

and we must show $\{\zeta^i, 1 + t\} = 1$. Suppose $1 + t$ is a square and let $v \in 1 + \frac{p^n}{p^{n+1}}, v^2 = 1 + t$. Then $v$ has exponent $p$ by (3.5) and $\zeta^i$ has order prime to $p$. Hence $\zeta^i$ and $v$ generate a cyclic subgroup of $(\mathbb{F}/p^{n+1})^*$ and $\{\zeta^i, 1 + t\} = 1$ by (1.1)(S7) and (S8). If $1 + t$ is not a square, we must have $p = 2$ and $\zeta^i$ is a square; a similar argument applied to $(\zeta^i)^{1/2}$ and $1 + t$ again yields $\{\zeta^i, 1 + t\} = 1$. 


Lemma. If \( \text{rk } \Phi = 1 \), assume \( A/p \not\cong F_{9} \). Then \( L(\Phi, \mathfrak{p}^{n}/\mathfrak{p}^{n+1}) \) is generated by all

\[
\{ 1 + u\overline{\mu}^{i}, 1 + u\overline{\mu}^{n} \}, \quad 1 \leq i \leq n,
\]

where \( u \) is a power of \( \zeta \) and \( \overline{\mu} \) denotes the image of \( \mu \) in \( A/\mathfrak{p}^{n+1} \).

Moreover if \( \Phi \not\cong \Phi_{1}, C_{2} \), or if \( \Phi = C_{2} \) and \( p \) is odd, then these symbols are trivial except possibly when \( i = 1 \).

We begin by proving that the additive group \( \mathfrak{p}^{m}/\mathfrak{p}^{n+1} \) is generated by all \( \zeta^{k}, m \leq k \leq n \), where \( \zeta \) is an even power of \( \zeta \) (resp. \( \zeta \) is a fourth power of \( \zeta \) if \( A/\mathfrak{p} \not\cong F_{9} \)). By (3.6) this is true if \( m = n \), for \( \mathfrak{p}^{m}/\mathfrak{p}^{n+1} \) is isomorphic to \( A/\mathfrak{p} \). By definition of \( \zeta \), \( \mathfrak{p}^{m-1}/\mathfrak{p}^{n+1} \) is generated by all \( v\overline{\mu}^{k}, m - 1 \leq k \leq n \), where \( v \) is a power of \( \zeta \). According to (3.6), \( v \equiv a_{1} + \cdots + a_{n} \) modulo \( \mathfrak{p}/\mathfrak{p}^{n+1} \) where the \( a_{i} \) are even (resp. fourth) powers of \( \zeta \). Therefore \( v\overline{\mu}^{k} = a_{1}\overline{\mu}^{k} + \cdots + a_{n}\overline{\mu}^{k} + b \) for some \( b \in \mathfrak{p}^{m}/\mathfrak{p}^{n+1} \); by descending induction on \( m \), \( b \) is of the desired form.

Our hypothesis on \( p \) assures us, by (2.5), that \( L(\Phi, \mathfrak{p}^{n}/\mathfrak{p}^{n+1}) = D(\Phi, \mathfrak{p}^{n}/\mathfrak{p}^{n+1}) \) and is generated, according to (3.7), by all

\[
\{ 1 + s, 1 + \zeta^{m-n} \}_{\alpha}, \quad s \in \mathfrak{p}/\mathfrak{p}^{n+1},
\]

where \( \zeta = b_{1} + \cdots + b_{r} \) is a sum of even (resp. fourth) powers of \( \zeta \), and \( \alpha \) is any fixed long root. (The \( \langle \text{"resp."} \rangle \) statements hold under the hypothesis \( A/\mathfrak{p} \not\cong F_{9} \).)

Now if \( \Phi \) is nonsymplectic, there is a \( \beta \in \Phi \) with \( \langle \alpha, \beta \rangle = 1 \), where \( \alpha \) is the root occurring in (2). We now show that the same is true if \( \Phi = C_{I}, I \geq 2 \), and \( p \) is odd. In that case \( 1 + s = (1 + s')^{2} \) for some \( s' \in \mathfrak{p}/\mathfrak{p}^{n+1} \) by (3.5), and we have, by (4) of §1 and (1.1)(S°3),

\[
\{ 1 + s, 1 + \zeta^{m-n} \}_{\alpha} = \{ (1 + s')^{2}, 1 + t \}_{\alpha}
\]

\[
\{ 1 + t, 1 + s' \}_{\gamma}^{-1} = \{ 1 + s', 1 + t \}_{\gamma}
\]

where \( \gamma \in \Phi \) is a short root such that \( \langle \alpha, \gamma \rangle = 2 \), \( \langle \gamma, \alpha \rangle = 1 \). Replacing \( \alpha \) by \( \gamma \) in (2), we are done.

Because \( (\mathfrak{p}/\mathfrak{p}^{n+1})(\mathfrak{p}^{n}/\mathfrak{p}^{n+1}) = 0 \), we may apply (2.9), (2.17), and the commutator identities of \( [14, (2.1)] \) to conclude

\[
\{ 1 + s, 1 + \zeta^{m-n} \}_{\alpha} = [x_{-\alpha}(s), x_{\alpha}(\zeta^{m-n})]
\]

\[
= [x_{-\alpha}(s), x_{\alpha}(b_{1}\overline{\mu}^{n}) \cdots x_{\alpha}(b_{n}\overline{\mu}^{n})]
\]

\[
= [x_{-\alpha}(s), x_{\alpha}(b_{1}\overline{\mu}^{n})] \cdots [x_{-\alpha}(s), x_{\alpha}(b_{n}\overline{\mu}^{n})]
\]

\[
= \{ 1 + s, 1 + b_{1}\overline{\mu}^{n} \}_{\alpha} \cdots \{ 1 + s, 1 + b_{n}\overline{\mu}^{n} \}_{\alpha}
\]

which shows we may assume in (2) that \( \zeta \) itself is an even (resp. fourth) power of \( \zeta \) (and not just a sum of such powers).
Conjugating

$\{1 + s, 1 + \xi \mu^n \}_a = [x_{-a}(s), x_a(\xi \mu^n)]$

by $\hat{h}_a(\xi^{1/2})$ yields

$\{1 + s, 1 + \xi \mu^n \}_a = [x_{-a}(\xi s), x_a(\mu^n)] = \{1 + \xi s, 1 + \mu^n \}_a,$

and $L(\Phi, p^n/p^n+1)$ is thus generated by all

(4)

$\{1 + s, 1 + \mu^n \}_a, \quad s \in \mathbb{p}^{n+1}.$

Now we may write $s = a_1 \mu + \cdots + a_n \mu^n$, where each $a_i$ is a sum of even (resp. fourth) powers of $\zeta$. Arguing as for (3) above, we have

(5)

$\{1 + a_i \mu, 1 + \mu^n \}_a = [x_{-a}(a_i \mu), x_a(\mu^n)], \quad 1 \leq i \leq n,$

where $a$ is an even (resp. fourth) power of $\zeta$.

Now if $\Phi$ is nonsymplectic, or if $p$ is odd and $p = 2$, take $\beta$ so that $\langle \alpha, \beta \rangle = 1$ and let $\nu$ be a power of $\zeta$ such that $\nu^2 = a$. If $\Phi = A_1$, or if $p = 2$ and $\Phi = A_1$, $l \geq 2$, take $\beta = \alpha$ and let $\nu$ be a power of $\zeta$ such that $\nu^4 = a$ (these choices are possible by our hypotheses and the previous discussion). Conjugating (6) by $\hat{h}_\beta(\nu)$ yields

$\{1 + a_i \mu, 1 + \mu^n \}_a = [x_{-a}(u \mu^i), x_a(u \mu^n)], \quad 1 \leq i \leq n,$

where $u = \nu^{(\alpha, \beta)}$ is a power of $\zeta$ as desired.

Finally if $\Phi \neq A_1, C_2$, or if $\Phi = C_2$ and $p$ is odd, it follows from (2.9) and (2.17) that for $i > 1$,

(3.9) Lemma. For every $u \in A^*$ and all $n \geq 1$,

$\{1 + u \mu^k \}_a = [x_{-a}(u \mu^k), x_a(u \mu^n)] = 1.$

If $p \neq 2$, this congruence holds for $k = 1$ as well.

If $k = n$ the congruence is clearly true, and we will prove the remaining cases by induction on $(n - k, n + 1)$ (lexicographically ordered).
Our induction hypothesis implies
\[(1 + \mu_k^p)^{n-k-1} \equiv 1 + \mu^{n-k-1} \mu^k \pmod{\mathfrak{p}^n}\]
and, therefore, for some \(s \in \mathfrak{p}^n/\mathfrak{p}^{n+1},\)
\[(1 + \mu_k^p)^{n-k-1} \equiv 1 + \mu^{n-k-1} \mu^k + s \equiv (1 + \mu^{n-k-1} \mu^k)(1 + s) \pmod{\mathfrak{p}^{n+1}}\]
since \(s \mu^k = 0.\)

Thus modulo \(\mathfrak{p}^{n+1}\) we have
\[(1 + \mu_k^p)^{n-k} \equiv ((1 + \mu_k^p)^{n-k-1})^p \equiv (1 + \mu^{n-k-1} \mu^k)^p (1 + s)^p \equiv (1 + \mu^{n-k-1} \mu^k)^p\]
\[\equiv 1 + \mu^{n-k-1} \mu^k + \sum_{i=2}^{p} \binom{p}{i} (\mu^{n-k-1} \mu^k)^i\]
since \(1 + \mathfrak{p}^n/\mathfrak{p}^{n+1}\) has exponent \(p\) by (3.5), and it suffices to show
\[\binom{p}{i} \mu^{ni-ki-i} \mu^i \equiv 0 \pmod{\mathfrak{p}^{n+1}}\]
for \(2 \leq i \leq p.\)

According to (3.5), \(\mathfrak{p}^{ki}/\mathfrak{p}^{n+1}\) has additive exponent \(p^{n-ki+1}.\) Since \(\binom{p}{i}\) is divisible by \(p\) if \(2 \leq i \leq p-1,\) we must have
\[ni - ki - i + 1 \geq n - ki + 1, \quad 2 \leq i \leq p - 1,\]
\[np - kp - p \geq n - kp + 1.\]
That is, we must have
\[i \geq n/(n-1), \quad 2 \leq i \leq p - 1,\]
\[p \geq (n + 1)/(n-1).\]
These identities are satisfied except when \(n = 1\) (in which case the lemma is trivial) and when \(p = 2, n = 2.\)

This completes the proof when \(p\) is odd. If \(p = 2,\) the lemma holds for \(n = 2, k = 2\) and hence by induction for all \((n, k)\) with \(n \geq 2, k \geq 2.\) The cases \((n, 1),\) \(n \geq 1\) are true exceptions.

(3.10) Theorem. Let \(A\) be a local ring whose residue field is a finite field with \(q = p^s\) elements and whose maximal ideal \(\mathfrak{p}\) is principal, generated by \(\mu,\) the image of \(p\) in \(A.\) If \(rk \Phi = 1,\) assume that \(A/\mathfrak{p} \neq F_q.\) Then for all \(n \geq 0\)
and all odd primes \(p,\) \(L(\Phi, A/\mathfrak{p}^{n+1}) = 1.\) Moreover, if \(p = 2,\) the groups \(L(\Phi, A/\mathfrak{p}^{n+1})\) and \(L(\Phi, A/\mathfrak{p}^{n})\) are isomorphic for all \(n \geq 2\) and are generated by the \(2^s - 1\) symbols \(\{1 + \zeta^i \mu, 1 + \zeta^i \mu^k\}, 1 \leq i \leq 2^s - 1,\) where \(\zeta \in (A/\mathfrak{p}^{n+1})^*\) has
order $2^s - 1$ and maps to a generator of $A/p$. Each of these symbols has order at most 2.

Since $\bar{p} = \bar{\mu}$ generates $\mathbb{Z}/p^{n+1}$ (we identify $\bar{p} \in A$ with its image in $A/p^{n+1}$), (3.9) implies, for $p$ odd, that

$$1 + u\bar{p}^n = 1 + u\bar{\mu}^n = (1 + u\bar{\mu})\bar{p}^{n-1}$$

and it follows from (3.8) that $L(\Phi, \mathbb{Z}/p^{n+1})$ is generated by all

$$(7) \quad \{1 + u\bar{\mu}^i, (1 + u\bar{\mu})\bar{p}^{n-i} \mid 1 \leq i \leq n, \}$$

where $u$ is a power of $\zeta$. Since $p$ is odd, (3.5) implies that $1 + u\bar{\mu}^i$ is a square, and

$$(8) \quad \{1 + u\bar{\mu}^i, (1 + u\bar{\mu})\bar{p}^{n-i} \mid 1 \leq i \leq n, \} = \{1 + u\bar{\mu}^i, 1 + u\bar{\mu}i\bar{p}^{n-i} = 1$$

by (1.1)(S6), (S7) and (S8). The first part of the theorem now follows by induction on $n$ from (3.2) and the exact sequence

$$(8) \quad 1 \to L(\Phi, \mathbb{Z}/p^{n+1}) \to L(A/p^{n+1}) \to L(A/p^n) \to 1.$$
Thus \( \{1 + 4u, 1 + 4u\}^2 = 1 \) for any \( u \in A^* \). Now \( L(\Phi, \mathfrak{p}^2/\mathfrak{p}^3) \) is generated by the symbols \( \{1 + 4u, 1 + 4u\}, \{1 + 2u, 1 + 4u\} \). But

\[
\{1 + 4u, 1 + 4u\} = [x_{-\alpha}(4u), x_\alpha(4u)]^2 = 1 + 2u, 1 + 4u^2
\]

and we may take the symbols \( \{1 + 2u, 1 + 4u\}, u = \zeta^{2k} \), as generators. But (9), (10), (11) then imply

\[
\{1 + 2\zeta^{2k}, 1 + 4\zeta^{2k}\}^2 = \{1 + 4\zeta^{4k}, -1\}^{-1}
\]

(See that the last 3 lines of this computation follow from (9) by substituting \( 2k \) for \( k \).)

Thus by (8), \( L(\Phi, A/\mathfrak{p}^{n+1}) \cong L(\Phi, A/\mathfrak{p}^n) \) for all \( n \geq 2 \) as stated. If \( n = 1 \), then (8) and (3.2) imply \( L(\Phi, A/\mathfrak{p}^2) \cong L(\Phi, \mathfrak{p}/\mathfrak{p}^2) \) is generated by the symbols \( \{1 + u\bar{\mu}, 1 + u\bar{\mu}\} \) where \( u = \zeta^i, 1 \leq i \leq 2^s - 1 \). Since the characteristic of \( A/\mathfrak{p}^2 \) is 4, an argument similar to (10) shows that each of these symbols has order at most 2.

(3.11) Corollary. Under the hypothesis of (3.10) assume further that \( \mathfrak{p} \) is nilpotent. Then if \( p \) is odd, \( L(\Phi, A) = 1 \), and if \( p = 2 \), \( L(\Phi, A) \) is generated by the \( 2^s - 1 \) symbols \( \{1 + \zeta^i \bar{\mu}, 1 + \zeta^i \bar{\mu}\}, 1 \leq i \leq 2^s - 1 \), which have order at most 2.

The corollary follows from the theorem, since if \( \mathfrak{p}^n+1 = 0, A/\mathfrak{p}^{n+1} = A \).

(3.12) Corollary. Let \( \mathcal{O} \) be the ring of integers in an algebraic number field and let \( 0 \neq \mathfrak{p} \subset \mathcal{O} \) be a prime ideal which is unramified over \( \mathfrak{p}Z = \mathfrak{p} \cap \mathbb{Z} \). If \( \text{rk} \Phi = 1 \), assume that \( \mathcal{O}/\mathfrak{p} \neq \mathbb{F}_9 \). Then if \( p \) is odd, \( L(\Phi, \mathcal{O}/\mathfrak{p}^{n+1}) = 1 \) for all \( n \geq 0 \). Moreover, if \( p = 2 \), the groups \( L(\Phi, \mathcal{O}/\mathfrak{p}^{n+1}) \) are isomorphic for all \( n \geq 1 \) and are generated by the \( 2^s - 1 \) symbols \( \{1 + 2\zeta^i, 1 + 2\zeta^i\}, 1 \leq i \leq 2^s - 1 \), where \( |\mathcal{O}/\mathfrak{p}| = 2^s \) and \( \zeta \in (\mathcal{O}/\mathfrak{p}^{n+1})^* \) has order \( 2^s - 1 \) and maps to a generator of \( (\mathcal{O}/\mathfrak{p})^* \). These symbols have order at most 2.

This follows from (3.11) with \( A = \mathcal{O}/\mathfrak{p}^{n+1} \).

Note. For the groups of type \( A_1, l \geq 2 \), this corollary is due to Christofides [2].

4. Stability for \( H_2(E(\Phi, A), \mathbb{Z}) \). Throughout this section, \( A \) denotes a local ring with maximal ideal \( \mathfrak{p} \). We set \( k = A/\mathfrak{p} \), but do not assume that \( k \) is finite or that \( \mathfrak{p} \) is principal, as in §3.

We fix an \( l > 1 \) (depending on \( \Phi \) and \( A \)) such that \( L(\Phi, A) \cong H_2(E(\Phi, A), \mathbb{Z}) \).
and write $\Phi = \Phi$. It follows from [14, Theorem 5.3] that for a given $A$ and $\Phi$ there is an $l_0 \geq 1$ such that every $l \geq l_0$ satisfies this condition, and it is clear that $l_0$ depends only on $\Phi$ and $A/\text{rad} A = k$.

We abbreviate the functors $\text{St}(A, \Phi)$ and $L(A, \Phi)$ by $\text{St}_1(\Phi)$ and $L_1(\Phi)$ and we write $H_i(G)$ for the homology groups $H_i(G, Z)$ of the group $G$, $i = 1, 2$. Recall that the functor $E(A, \Phi)$ is $\text{SL}_2(\Phi)$.

(4.1) Theorem. $H_2(\text{SL}_2(A)) \rightarrow H_2(E(\Phi, A))$ is surjective whenever $|k| \geq 4$.

Apply the homology spectral sequence [6] to the diagram of group extensions

$1 \rightarrow L_1(A) \rightarrow \text{St}_1(A) \rightarrow \text{SL}_2(A) \rightarrow 1$

to obtain the following commutative diagram with exact rows:

$H_2(\text{SL}_2(A)) \rightarrow H_2(E(\Phi, A)) \rightarrow H_2(E(Q, A)) \rightarrow L_0(A, \Phi)$

The surjectivity of $L_1(A) \rightarrow L(\Phi, A)$ is a consequence of (2.13). If $|k| \geq 4$, there exists $u \in A^*$ with $u^2 - 1 \in A^*$ and by [14, (4.4)], $\text{St}_1(A)_{ab} = 0$. Thus the theorem follows from (1).

We shall require the following unpublished result of Bass.

(4.2) Lemma. Let $q \subseteq A$ be the ideal generated by all $u^2 - 1$, $u \in A^*$. If $k = F_2$, assume that $p$ is principal, generated by $\mu$. Then $\text{St}_1(A)_{ab} \approx \text{St}_1(A/q)_{ab}$ and both groups are quotients of $A/q$. Moreover, $q = A$ except in the following cases:

$k = F_2, q = p, A/q = F_3$

Denote the image in $\text{St}_1(A)_{ab}$ of $g \in \text{St}_1(A)$ by $[g]$, and set $\langle t \rangle = [x_\alpha(t)]$ for $t \in A$. It follows from relation (R1) that $t \mapsto \langle t \rangle$ is a homomorphism $A^+ \rightarrow \text{St}_1(A)_{ab}$. By relation (R3)

$[\hat{\alpha}(u), x_\alpha(t)] = x_\alpha((u^2 - 1)t)$

we have $\{x_\alpha(t)\} = \{-u^2t\}$; hence $t \mapsto \langle t \rangle$ is surjective. Moreover by (R6)
and therefore \( (t) = 0 \) for \( t \in q \). This proves that \( \text{St}_1(A)^{ab} \) is a quotient of \( A/q \) and that \( \text{St}_1(q) \subseteq [\text{St}_1(A), \text{St}_1(A)] \). Hence there is a surjective homomorphism 
\( \text{St}_1(A/q) \rightarrow \text{St}_1(A)^{ab} \) which factors through \( \text{St}_1(A/q)^{ab} \); the projection \( \text{St}_1(A)^{ab} \rightarrow \text{St}_1(A/q)^{ab} \) is an inverse to this induced homomorphism.

Now let us determine the ideal \( q \). Since \( A \) is local, \( q = A \) if and only if \( |k| \geq 4 \). If \( k = F_3 \), we have \( A^* = \{1 + x, x - 1, x \in p\} \). Hence if \( u \in A^*, u^2 - 1 = x(2 + x) \) or \( x(x - 2) \) for some \( x \in p \); since \( 2 + x, 2 - x \in A^* \), this proves \( q = p \).

If \( k = F_2 \), write \( 2A = \mu eA \) with \( e = \infty \) if \( 2A = 0 \). If \( e = 1 \) we may assume \( \mu = 2 \), and \( (1 + 2x)^2 - 1 = 4x + 4x^2 = 0 \) mod \( 8A \). Taking \( x = 1 \), we see that \( q = 8A \) and, therefore, that \( A/q \approx Z/2^nZ, n = 1, 2 \) or 3. If \( c > 1 \), write \( 2 = \mu e^v \), \( v \in A^* \). Then
\[
(1 + \mu)^2 - 1 = 2\mu + \mu^2 = \frac{\mu(e + 1)}{\mu(e - 1)} = \frac{\mu^2(1 + \mu^{-1})}{(1 + \mu^{-1})}.
\]
Since \( 1 + \mu^{-1} \in A^*, q = \mu^2A \) and \( A/q \approx F_2[X]/(X^2) \) as desired.

(4.3) Theorem. The map 
\[
H_2(\text{SL}_2(A)) \rightarrow H_2(\text{E}(\Phi, A)).
\]
is surjective if \( k \approx F_3 \).

It suffices, by (1), to show that \( L_1(A) \rightarrow \text{St}_1(A)^{ab} \) is 0, and this map factors, by (4.2), as
\[
\begin{array}{ccc}
L_1(A) & \rightarrow & \text{St}_1(A)^{ab} \\
\downarrow & & \downarrow \\
\text{St}_1(A/q) & \rightarrow & \text{St}_1(A/q)^{ab}
\end{array}
\]
But \( L_1(A/q) = L_1(F_3) = 1 \) by (3.2).

(4.4) Lemma. Let \( \{u, v\} \in L_1(A) \). Then \( \{u, v\} = (3(u - 1)(v - 1)) \) in 
\( \text{St}_1(A)^{ab} \). Moreover, \( \{u, v\} \) lies in the image of \( H_2(\text{SL}_2(A)) \) if and only if \( \{u, v\} = 1 \).

Since \( [x_{-a}(t)] = (-u^{-t}) \) (cf. the proof of (4.2)), taking \( t = -u^{-1} \), we have 
\( [\tilde{w}_a(-u^{-1})] = (u) \). Hence \( [\tilde{w}_a(u)] = [x_{-a}(u)x_{-a}(-u^{-1})x_{-a}(u)] = (3u) \) and 
\( [\tilde{b}_a(u)] = [\tilde{w}_a(u)\tilde{w}_a(-1)] = (3(u - 1)) \). Finally,
\[
\{u, v\} = [\tilde{b}_a(uv)\tilde{b}_a(u)^{-1}\tilde{b}_a(v)^{-1}] = (3(uv - 1) - 3(u - 1) - 3(v - 1)) = (3(u - 1)(v - 1)).
\]

Now consider the commutative diagram
\[
\begin{array}{cccc}
1 & \rightarrow & L_1(A) & \rightarrow & \text{St}_1(A) & \rightarrow & \text{SL}_2(A) & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \rightarrow & L_1(A)/\phi(H_2(\text{SL}_2(A))) & \rightarrow & \text{St}_1(A)^{ab} & \rightarrow & \text{SL}_2(A)^{ab} & \rightarrow & 1
\end{array}
\]
Its columns and top row are clearly exact. Since the bottom row is obtained by factoring out the image of \( H_2(SL_2(A)) \) from the top row of (1), it too is exact. The second part of the lemma follows easily from (2).

(4.5) Proposition. The map \( H_2(SL_2(Z/2^nZ)) \rightarrow L_1(Z/2^nZ) \) is surjective for \( n = 1, 2 \) but not for \( n \geq 3 \). Therefore the map

\[
H_2(SL_2(Z/4Z)) \rightarrow H_2(E(\Phi, Z/4Z))
\]

is surjective.

It is clear from (1) that the second statement is implied by the first. For \( n = 1 \), the first assertion is trivial since \( L_1(Z/2Z) = 1 \) by (3.2). Now \( L_1(Z/4Z) \) is generated by the symbol \( [1-1, -1] \) whose image in \( St_1(Z/4Z)^{ab} \) is \( (3(-1-1)(-1-1)) = 1 \). This completes the proof for \( n = 2 \) by (4.4).

Now suppose \( n \geq 3 \). According to (4.2), \( St_1(Z/2^nZ)^{ab} \approx St_1(Z/8Z)^{ab} \) for all \( n \geq 3 \); thus (1) implies that

\[
\phi: H_2(SL_2(Z/2^nZ)) \rightarrow L_1(Z/2^nZ)
\]

is surjective for \( n = 3 \) if and only if \( \phi \) is surjective for all \( n \geq 3 \).

Suppose that this is the case. Then from (1) we have

\[
St_1(Z/2^nZ)^{ab} \approx SL_2(Z/2^nZ)^{ab}
\]

for all \( n \geq 3 \), and the same must be true for the 2-adic integers

\[
St_1(\hat{Z}_2)^{ab} \approx SL_2(\hat{Z}_2)^{ab}.
\]

Hence \( H_2(SL_2(\hat{Z}_2)) \rightarrow L_1(\hat{Z}_2) \rightarrow L_\infty(\hat{Z}_2) = K_2(\hat{Z}_2) \) is surjective by (1) and (2.13).

Dualizing, we have

\[
\text{Hom}(H_2(SL_2(\hat{Z}_2)), Q/Z) \approx H^2(SL_2(\hat{Z}_2), Q/Z)
\]

by the universal coefficient theorem [7, p. 77]. But \( H^2(SL_2(\hat{Z}_2), Q/Z) = 0 \) [1, Proposition 2]. Therefore if \( \phi \) is surjective, we conclude that \( K_2(\hat{Z}_2) = 0 \); in particular \( \{1, -1\} = 0 \) in \( K_2(\hat{Q}_2) \). But it follows from results of Moore [10] and Matsumoto [8] that \( \{1, -1, -1\} \neq 0 \) in \( K_2(\hat{Q}_2) \), whence the proposition.

(4.6) Corollary. The symbol \( \{1, -1\} \) is nontrivial in \( L_1(Z/4Z) \).

Since \( \{1, -1\} \) generates \( L_1(Z/4Z) \), if it is 1 we conclude from (3.1) that \( L_1(Z/8Z) \approx L_1(4Z/8Z) \) is generated by the symbols \( \{1 + 4a, 1 + 2b\}, a, b \in Z \).

But in \( St_1(Z/8Z)^{ab} \), \( \{1 + 4a, 1 + 2b\} = (3(4a)(2b)) = 0 \), which implies that \( H_2(SL_2(Z/8Z)) \rightarrow L_1(Z/8Z) \) is surjective by (4.4). This contradicts (4.5).

Note. Despite (4.6), we cannot conclude that \( \{1, -1\} \neq 0 \) in \( K_2(Z/4Z) \) since \( K_2(Z/4Z) \) is a quotient of \( L_1(Z/4Z) \) by (2.13).
Added in proof. Much more extensive information on the functor $K_2 = \lim_{l \to \infty} L(A_l)$ has been obtained since this paper was written. Dennis ([20], [21]) has proved the conjecture of the Introduction, showing that when $\Phi$ is of type $A_l$, the maps $\theta(l, m)$ are surjective for all $m \geq l \geq d + 3$, where $d$ is the dimension of the maximal ideal space of $A$.

The results concerning $K_2$ of a semilocal ring (Theorem 2.13) have been completed by Stein and Dennis [24]. They have also proved ([22], [23]) that for nonsymplectic $\Phi$, the maps $\theta(l, m)$ are injective (and hence isomorphisms) when $A$ is a discrete valuation ring or a quotient thereof, and they have given a presentation of the $K_2$ of such a ring. These papers also compute $K_2$ of a ring of algebraic integers modulo any nonzero ideal, generalizing the results of §3. Among the consequences of this computation is the nontriviality of the symbol $\{−1, −1\} \in K_2(\mathbb{Z}/4\mathbb{Z})$ (see the Note at the end of §4).

REFERENCES

3. R. K. Dennis, Universal GE rings and the functor $K_2$ (unpublished manuscript; see [24]).


