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

HYMAN BASS
JOHN MILNOR
JEAN-PIERRE SERRE

Solution of the congruence subgroup problem for $SL_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$

Publications mathématiques de l'I.H.É.S., tome 33 (1967), p. 59-137

<http://www.numdam.org/item?id=PMIHES_1967__33__59_0>

SOLUTION OF THE CONGRUENCE SUBGROUP PROBLEM FOR SL_n ($n \geq 3$) AND Sp_{2n} ($n \geq 2$)

by H. BASS (1), J. MILNOR *and* J.-P. SERRE

CONTENTS

§ 1. Introduction.

Let k be a (finite) algebraic number field, and let $\mathcal{O}$ be its ring of integers. Suppose $n \geq 3$, and write $G = SL_n$, with the convention that $G_A = SL_n(A)$ for any commutative ring A. Set $\Gamma = G_{\mathcal{O}} \subset G_k$, and write, for any ideal $\mathfrak{q}$ in $\mathcal{O}$,

$$\Gamma_{\mathfrak{q}} = \ker(G_{\mathcal{O}} \to G_{\mathcal{O}/\mathfrak{q}}).$$

(1) Sloan Fellow. Research partially supported by the National Science Foundation under Grant N.S.F., GP-5303.

The subgroups of Γ containing some $\Gamma_\mathfrak{q}(\mathfrak{q}\neq 0)$ are called *congruence subgroups*. Since $\mathcal{O}/\mathfrak{q}$ is finite they are of finite index in Γ. One can pose, conversely, the

Congruence Subgroup Problem : Is every subgroup of finite index in Γ a congruence subgroup?

We shall present here a complete solution of this problem. While the response is, in general, negative, we can describe precisely what occurs. The results apply to function fields over finite fields as well as to number fields, and to any subring $\mathcal{O}$ of " arithmetic type ". Moreover the analogous problem is solved for the symplectic groups, $G=\mathrm{Sp}_{2n}$ $(n\geq 2)$. It appears likely that similar phenomena should occur for more general algebraic groups, G, e.g. for simply connected simple Chevalley groups of rank >1, and we formulate some conjectures to this effect in Chapter IV. Related conjectures have been treated independently, and from a somewhat different point of view, by Calvin Moore, and he has informed us of a number of interesting theorems he has proved in support of them. Chapter IV contains also some applications of our results (and conjectures) to vanishing theorems for the cohomology of arithmetic subgroups of G_k, and, in particular, to their " rigidity " (cf. Weil [24]).

Here, in outline, is how the problem above is solved for $G=\mathrm{SL}_n$ $(n\geq 3)$. There is a normal subgroup $E_\mathfrak{q}\subset\Gamma_\mathfrak{q}$, generated by certain " elementary " unipotent matrices, and it can be proved by fairly elementary arguments that: (i) Every subgroup of finite index contains some $E_\mathfrak{q}$ $(\mathfrak{q}\neq 0)$, and $E_\mathfrak{q}$ itself has finite index in Γ; (ii) $E_\mathfrak{q}$ is a congruence subgroup if and only if $E_\mathfrak{q}=\Gamma_\mathfrak{q}$; and (iii) $\Gamma_\mathfrak{q}$ is generated by $E_\mathfrak{q}$ together with the matrices $\begin{pmatrix}\alpha & 0\\ 0 & I_{n-2}\end{pmatrix}$ in $\Gamma_\mathfrak{q}$, where $\alpha=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(\mathcal{O})$.

From (i) and (ii) we see that an affirmative response to the congruence subgroup problem is equivalent to the vanishing of

$$C_\mathfrak{q}=\Gamma_\mathfrak{q}/E_\mathfrak{q}$$

for all ideals $\mathfrak{q}\neq 0$. If $\kappa:\Gamma_\mathfrak{q}\to C_\mathfrak{q}$ is the natural projection, then every element of $C_\mathfrak{q}$ is of the form $\kappa\begin{pmatrix}\alpha & 0\\ 0 & I_{n-2}\end{pmatrix}$, as in (iii), and, modulo elementary matrices, this element depends only on the first row, (a, b), of α. Denoting this image by $\begin{bmatrix}b\\ a\end{bmatrix}\in C_\mathfrak{q}$, we have a surjective function

$$[\ ]:W_\mathfrak{q}\to C_\mathfrak{q},$$

where $W_\mathfrak{q}=\{(a, b)\,|\,(a, b)\equiv(1, 0)\bmod\mathfrak{q};\ a\mathcal{O}+b\mathcal{O}=\mathcal{O}\}$, is the set of first rows of matrices α as above.

It was discovered by Mennicke [16] that this function has the following very pleasant properties:

MS1. $\begin{bmatrix}0\\ 1\end{bmatrix}=1$; $\begin{bmatrix}b+ta\\ a\end{bmatrix}=\begin{bmatrix}b\\ a\end{bmatrix}$ for all $t\in\mathfrak{q}$; and $\begin{bmatrix}b\\ a+tb\end{bmatrix}=\begin{bmatrix}b\\ a\end{bmatrix}$ for all $t\in\mathcal{O}$.

MS2. If $(a, b_1), (a, b_2)\in W_\mathfrak{q}$ then $\begin{bmatrix}b_1b_2\\ a\end{bmatrix}=\begin{bmatrix}b_1\\ a\end{bmatrix}\begin{bmatrix}b_2\\ a\end{bmatrix}$.

Accordingly, we call a function from W_q to a group satisfying MS1 and MS2 a *Mennicke symbol.* There is evidently a *universal* one, all others being obtained uniquely by following the universal one with a homomorphism.

The main theorem of Chapter II asserts that the Mennicke symbol, $[\ ] : W_q \to C_q$, above is universal. A more pedestrian way of saying this is that C_q has a presentation with generators W_q; and with relations MS1 and MS2. The principal content of this theorem is that C_q depends only on $\mathcal{O}$ and $\mathfrak{q}$, and not on n; recall that $G = SL_n$.

At this point we are faced with the problem of calculating, somehow directly, the universal Mennicke symbol on W_q. The multiplicativity (MS2) naturally suggests the power residue symbols. Specifically, suppose k contains μ_m, the m-th roots of unity. Then for $a, b \in \mathcal{O}$, with a prime to bm, there is a symbol

$$\left(\frac{b}{a}\right)_m \in \mu_m.$$

It is defined to be multiplicative in a, or rather in the principal ideal $a\mathcal{O}$, and for a prime ideal $\mathfrak{p}$ prime to m, with q elements in the residue class field, it is the unique m-th root of unity congruent, mod $\mathfrak{p}$, to $b^{q-1/m}$. This is evidently multiplicative in b and depends on b only modulo a.

Let $\mathfrak{q}$ be an ideal and suppose $(a, b) \in W_q$. If m divides $\mathfrak{q}$ then, since $a \equiv 1 \bmod \mathfrak{q}$, a is prime to m, so we can define $\left(\frac{b}{a}\right)_m$, provided $b \neq 0$. If $b = 0$ then a must be a unit, and we agree that $\left(\frac{0}{a}\right)_m = 1$ in this case. Then it is readily checked that

$$(-)_m : W_q \to \mu_m$$

satisfies all of the axioms for a Mennicke symbol except, possibly, the fact that $\left(\frac{b}{a}\right)_m$ depends on a only modulo b. For this we can try to use the " m-th power reciprocity law ". This says that $\left(\frac{b}{a}\right)_m = \pi_b \pi_m \pi_\infty$ where π_b is a product over primes $\mathfrak{p}$ dividing b, but not m, of $\left(\frac{a}{\mathfrak{p}}\right)_m^{\operatorname{ord}_{\mathfrak{p}}(b)}$, and where π_m and π_∞ are products over primes $\mathfrak{p}$ dividing m and ∞, respectively, of certain " local symbols ", $\left(\frac{a, b}{\mathfrak{p}}\right)_m$, which are bilinear functions on the multiplicative group of the local field $k_\mathfrak{p}$, with values in μ_m.

It is easily seen that π_b depends on a only modulo b, so we will have manufactured a non trivial Mennicke symbol, and thus shown that $C_q \neq \{1\}$, provided we can guarantee that $\pi_m = \pi_\infty = 1$. The factor π_m is easy to dispose of. For if we take $\mathfrak{q}$ highly divisible by m (e.g. by m^2) then since $a \equiv 1 \bmod \mathfrak{q}$, a will be very close to 1 in the topological group $k_\mathfrak{p}^*$, if $\mathfrak{p}$ divides m. Therefore a will be an m-th power in $k_\mathfrak{p}^*$, thus rendering $\left(\frac{a, b}{\mathfrak{p}}\right)_m = 1$ for any b.

If $\mathfrak{p}$ divides ∞ then $k_\mathfrak{p} = \mathbf{R}$ or $\mathbf{C}$, and everything is an m-th power in $\mathbf{C}^*$. If $k_\mathfrak{p} = \mathbf{R}$, however, we must have $m = 2$, and the local symbol at $\mathfrak{p}$ will be non trivial for any

choice of $\mathfrak{q}$. This, in broad outline, explains how we are led to the main theorem of Chapter I (Theorem 3.6):

If k has a real embedding then for all ideals $\mathfrak{q} \neq 0$ in $\mathcal{O}$, all Mennicke symbols on $W_{\mathfrak{q}}$ are trivial. Hence $C_{\mathfrak{q}} = \{1\}$ for all $\mathfrak{q}$.

If, on the other hand, k is totally imaginary, then for each ideal $\mathfrak{q} \neq 0$ in $\mathcal{O}$, there is an integer $r = r(\mathfrak{q})$ such that μ_r (the r-th roots of unity) belong to k, and such that

$$(-)_r : W_{\mathfrak{q}} \to \mu_r$$

is a universal Mennicke symbol on $W_{\mathfrak{q}}$. Hence $C_{\mathfrak{q}} \cong \mu_r$. If m is the number of roots of unity in k, and if m^2 divides $\mathfrak{q}$ then $r(\mathfrak{q}) = m$. (We give an explicit formula for r.)

To facilitate matters for the reader (and ourselves) we have included an " Appendix on Number Theory " at the end of Chapter I which contains statements of the results from class field theory which we require, together with either references or proofs in each case. The exposition in Chapter I is otherwise self contained.

Chapter III proves, for the symplectic groups, a result analogous to that of Chapter II on SL_n. Together with the results of Chapters I and II it gives a solution of the congruence subgroup problem for these groups.

Our results on SL_n give, in principle, a method for calculating the " Whitehead group ", $Wh(\pi)$, of a finite abelian group π. We include some simple applications of this type in § 4, though there remain some serious technical problems in completing this task.

It is worth mentioning also that the theorem of Chapter II is finally formulated, and proved, as a " stability theorem " for SL_n over an arbitrary commutative noetherian ring. An example of an application of this added generality is the following:

If $t_1, \ldots, t_m$ are indeterminates, and if $n \geq m + 4$, then $SL_n(\mathbf{Z}[t_1, \ldots, t_m])$ is a finitely generated group.

Next we shall explain, briefly, how the congruence subgroup problem is related to the work of Calvin Moore, mentioned above.

The congruence subgroups of Γ, and the subgroups of finite index, respectively, constitute bases for neighborhoods of the identity for two topologies on G_k. The latter refines the former so there is a continuous homomorphism,

$$\pi : \hat{G}_k \to \overline{G}_k,$$

between the corresponding completions, and it is easy to see that π is surjective. The congruence topology is the one induced by embedding $G_k \subset G_{(A_k^f)}$, where A_k^f is the ring of finite adèles of k, i.e. the adèle ring modulo the archimedean components. It is well known (cf. Bourbaki, *Alg. Comm.*, Chap. VII, § 2, n° 4, Prop. 4), that G_k is dense in $G_{(A_k^f)}$, o we can identify $\overline{G}_k = G_{(A_k^f)}$. In this way we obtain a topological group extension,

$$E(G_k) : 1 \to C(G_k) \to \hat{G}_k \xrightarrow{\pi} G_{(A_k^f)} \to 1,$$

and, since the right hand terms are both completions of G_k, the extension splits over $G_k \subset G_{(A_k^f)}$. The congruence subgroup problem asks whether the two topologies coincide,

i.e. whether π is an isomorphism, i.e. whether $C(G_k)=\{1\}$. The discussion above shows easily that

$$C(G_k)=\varprojlim \Gamma_q/E_q=\varprojlim C_q,$$

so we conclude that

$$C(G_k)=\begin{cases}\{1\} \text{ if } k \text{ has a real embedding,}\\ \mu_k, \text{ the roots of unity in } k, \text{ if } k \text{ is totally imaginary.}\end{cases}$$

We conjecture that this evaluation of $C(G_k)$ holds if G is any simply connected, simple, split group of rank >1 over k. The discrepancy between the real case and the imaginary one is nicely accounted for by the work of Calvin Moore, which suggests that one should expect an extension

$$1\to\mu_k\to\widetilde{G}_k\to G_{A_k}\to 1,$$

over the *full* adèle group, which splits over $G_k\subset G_{A_k}$, and which has order exactly $[\mu_k : 1]$ in $H^2(G_{A_k}, \mu_k)$. We cannot get at this when there are real primes because $G_{\mathbf{R}}$ is not generally simply connected, and the two sheeted covering sought by Moore in this case appears to depend essentially on the real primes. In contrast, $G_{\mathbf{C}}$ is simply connected, so it follows easily that the alleged $\widetilde{G}_k$ must be of the form $\hat{G}_k\times G_{k_\infty}$ if k is totally imaginary. $\widetilde{G}_k$ generalizes, in a natural way, the " metaplectic groups " of Weil [25].

Suppose that G is any semi-simple, simply connected, algebraic group defined over $\mathbf{Q}$, and let Γ be an arithmetic subgroup of G in the sense of Borel-Harish-Chandra [8]. If $\hat{\Gamma}$ is the " profinite completion " of Γ then there is a natural continuous homomorphism

$$\pi : \hat{\Gamma}\to G_{A_{\mathbf{Q}}^f},$$

(cf. discussion above). In § 16 of Chapter IV we prove:

Assume :

a) $\mathrm{im}(\pi)$ *is open in* $G_{A_{\mathbf{Q}}^f}$; *and*

b) $\ker(\pi)$ *is finite.*

Then if $f: \Gamma\to GL_n(\mathbf{Q})$ *is any group homomorphism there is there is a homomorphism*

$$F : G\to GL_n$$

of algebraic groups, defined over $\mathbf{Q}$, *such that* F *agrees with* f *on a subgroup of finite index of* Γ.

This conclusion easily implies that $H^1(\Gamma, V)=0$ for any finite dimensional vector space V over $\mathbf{Q}$ on which Γ operates. Taking for V the adjoint representation of G, this implies the triviality of all deformations of Γ in $G_{\mathbf{R}}$ (cf. Weil [24]). Vanishing and rigidity theorems of this type have already been proved in many cases by Borel, Garland, Kajdan and Raghunathan.

The hypothesis *a)* above corresponds to a form of the strong approximation theorem, and it has been proved for a wide class of groups by M. Kneser [13]. Hypothesis *b)* is a kind of " congruence subgroup theorem ". In the notation introduced above, and

applied to these more general groups G, it says that $C(G_{\mathbf{Q}})$ is finite. Therefore it is established here for certain G, and conjectured for others. For example, the case $\Gamma = SL_n(\mathbf{Z}) \subset G_{\mathbf{Q}} = SL_n(\mathbf{Q})$ $(n \geq 3)$, to which the theorem applies, is already rather amusing.

We shall close this introduction now with some historical remarks. The congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$ over $\mathbf{Q}$ was solved independently by Mennicke ([16] and [17]) and by Bass-Lazard-Serre [4]. Mennicke and Newman have, independently of us, solved the problem for SL_n over any *real* number field. Both Mennicke [16, p. 37] and Bass [18, p. 360 and p. 416] have announced incorrect solutions for arbitrary number fields.

Mennicke (unpublished) announced, and Matsumoto [15] outlined, a procedure for deducing an affirmative solution of the congruence subgroup problem for simply connected simple Chevalley groups of rank >1 from the two special cases, SL_3 and Sp_4. Their methods should probably suffice to prove at least the finiteness of $C(G_k)$, starting from the results proved here.

The research presented here was initiated by the first two named authors in [5]. A more definitive solution of the problem treated there was obtained using results of the third named author, and this appeared, again as a set of notes, in [6]. The content of [6] is embedded here in Chapter I and a small part of Chapters II and III.

We are grateful to T.-Y. Lam for a critical reading of the manuscript, and for the proofs of Lemma 2.11 and of Proposition 4.13, to M. Kervaire for Lemma 2.10, and to Mennicke and Newman for giving us access to some of their unpublished work.

Chapter I

DETERMINATION OF ARITHMETIC MENNICKE SYMBOLS

§ 2. Definition and Basic Properties of Mennicke Symbols.

Throughout this chapter, without explicit mention to the contrary, A *denotes a Dedekind ring and* $\mathfrak{q}$ *denotes a non zero ideal of* A. Nevertheless the definition of $W_\mathfrak{q}$, $\mathfrak{q}$-equivalence, and Mennicke symbols below make sense for any commutative ring and ideal, and they will sometimes be referred to in this generality. In particular lemmas 2.2 and 2.10 are valid without any hypothesis on A.

We write

$$W_\mathfrak{q} = \{(a, b) \in A^2 \mid (a, b) = (1, 0) \bmod \mathfrak{q}, \text{ and } aA + bA = A\}.$$

We call two pairs, (a_1, b_1) and (a_2, b_2) in A^2, $\mathfrak{q}$-*equivalent*, denoted

$$(a_1, b_1) \sim_\mathfrak{q} (a_2, b_2)$$

if one is obtained from the other by a finite sequence of transformations of the types

$$(a, b) \mapsto (a, b + ta) \qquad (t \in \mathfrak{q})$$

and

$$(a, b) \mapsto (a + tb, b) \qquad (t \in A)$$

(Note the asymmetry.) If we let $GL_2(A)$ operate on column vectors $\begin{pmatrix} a \\ b \end{pmatrix}$ by left multiplication, then the $\mathfrak{q}$-equivalence classes are the orbits of the group generated by all $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ $(t \in \mathfrak{q})$ and all $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ $(t \in A)$.

Lemma 2.1. — *Suppose* $A' = S^{-1}A$ *is a ring of fractions of* A, *and that* $\mathfrak{q}'$ *is a non zero ideal of* A'. *Then any* $(a', b') \in W_{\mathfrak{q}'}$ *is* $\mathfrak{q}'$*-equivalent to some* $(a, b) \in W_\mathfrak{q}$, *where* $\mathfrak{q} = \mathfrak{q}' \cap A$.

Proof. — Since A is a Dedekind ring it follows that, for any ideal $\mathfrak{a}' \neq 0$ in A', the composite $A \to A' \to A'/\mathfrak{a}'$ is surjective.

Now, for our problem we can first arrange that a' and b' are non zero. Then we can find $b \in A$ with $b = b' \bmod a'\mathfrak{q}'$, by the remark above. Write $bA = \mathfrak{b}_1\mathfrak{b}_2$ where $\mathfrak{b}_1 = bA' \cap A$. It follows from standard properties of rings of fractions, and the fact that A is Dedekind, that $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are relatively prime, and that $\mathfrak{b}_1 A' = bA'$. Choose $a_1 \in A$ such that $a_1 \equiv a' \bmod bA'$, using the remark above again. Then solve

$$a \equiv a_1 \bmod \mathfrak{b}_1$$
$$a \equiv 1 \bmod \mathfrak{b}_2$$

in A. The first congruence implies $a \equiv a_1 \equiv a' \bmod bA'$, since $bA' = \mathfrak{b}_1 A'$. Hence $(a', b') \sim_{\mathfrak{q}'} (a', b) \sim_{\mathfrak{q}'} (a, b)$, so $(a, b) \equiv (1, 0)$ modulo $\mathfrak{q}' \cap A = \mathfrak{q}$. The fact that $aA + bA = A$, and hence that $(a, b) \in W_{\mathfrak{q}}$, follows easily from the conditions $aA' + bA' = A'$ and $a \equiv 1 \bmod \mathfrak{b}_2$.

The following elementary remarks will be used repeatedly, without explicit reference: Suppose $aA + bA = A$. If A is semi-local then we can find a $t \in A$ such that $a + tb$ is a unit. For this is trivial if A is a field, so we can do this modulo each of the (finite number of) maximal ideals of A. Then we can use the " Chinese Remainder Theorem " to find a single t that works simultaneously for all of them.

Next suppose that A is a Dedekind ring, and that $\mathfrak{a}$ is a non zero ideal. Then, applying the preceding remark to the semi-local ring $A/\mathfrak{a}$, we conclude that we can find a $t \in A$ so that $a + tb$ is prime to $\mathfrak{a}$.

Lemma 2.2. — *Suppose* $(a, b) \in W_{\mathfrak{q}}$.

a) $(a, b) \sim_{\mathfrak{q}} (a, bq)$, *where* $q = 1 - a \in \mathfrak{q}$.

b) *If* a *is congruent to a unit* mod b, *or if* b *is congruent to a unit* mod a, *then* $(a, b) \sim_{\mathfrak{q}} (1, 0)$.

Proof. — a) $(a, b) \sim_{\mathfrak{q}} (a, b - ba) = (a, bq)$.

b) If $a = u - tb$ with u a unit, $t \in A$, then

$$(a, b) \sim_{\mathfrak{q}} (a + tb, b) = (u, b) \sim_{\mathfrak{q}} (u, b + u(u^{-1}(1 - b - u))) = (u, 1 - u) \sim_{\mathfrak{q}} (1, 1 - u) \sim_{\mathfrak{q}} (1, 0).$$

Next suppose $b = u + ta$, u a unit, $t \in A$. With $q = 1 - a$ we have

$$(a, b) \sim_{\mathfrak{q}} (a, bq) \sim_{\mathfrak{q}} (a, bq - a(tq)) = (a, uq) \sim_{\mathfrak{q}} (a + u^{-1}(uq), uq) = (1, uq) \sim_{\mathfrak{q}} (1, 0).$$

Lemma 2.3. — *Suppose* $\mathfrak{q}' \subset \mathfrak{q}$ *are non zero ideals in* A. *Then any* $(a, b) \in W_{\mathfrak{q}}$ *is* $\mathfrak{q}$*-equivalent to some* $(a', b') \in W_{\mathfrak{q}'}$.

Proof. — Passing to $B = A/\mathfrak{q}'$ and $\mathfrak{b} = \mathfrak{q}/\mathfrak{q}'$, we would like to show that an $(a, b) \in W_{\mathfrak{b}}$ is $\mathfrak{b}$-equivalent to $(1, 0)$, where now B is a semilocal ring. We can find $t \in B$ so that $a + tb$ is a unit, and then $(a, b) \sim_{\mathfrak{b}} (a + tb, b) \sim_{\mathfrak{b}} (1, 0)$, the last $\mathfrak{b}$-equivalence following as in Lemma 2.2 *b)*.

Lemma 2.4 (Mennicke-Newman). — *Given* $(a_1, b_1), \ldots, (a_n, b_n) \in W_{\mathfrak{q}}$, *we can find* $(a, c_1), \ldots, (a, c_n) \in W_{\mathfrak{q}}$ *such that* $(a, c_i) \sim_{\mathfrak{q}} (a_i, b_i)$, $1 \leq i \leq n$.

Proof. — Choose $q \neq 0$ in $\mathfrak{q}$, and use Lemma 2.3 to find $(a_i', a_i' q) \in W_q$ such that $(a_i', b_i' q) \sim_{\mathfrak{q}} (a_i, b_i)$, $1 \leq i \leq n$. We propose to find $(a, c_i q) \sim_q (a_i', b_i' q)$, $1 \leq i \leq n$, and this will clearly prove the lemma.

By induction on n (the case $n = 1$ being trivial) we can assume $n > 1$ and that $(a', c_i q) \sim_q (a_i', b_i' q)$, $1 \leq i < n$, have been found, and with all $c_i \neq 0$. Choose $c_n \equiv b_n' \bmod a_n'$ so that c_n is prime to $c_1 \ldots c_{n-1}$ (Lemma 2.2). Then $(a_n', b_n' q) \sim_q (a_n', c_n q)$, clearly.

Write $a' - a_n = dq$ and solve $d = rc_n - sc_1 \ldots c_{n-1}$. Then $a' - a_n = rc_n q - sc_1 \ldots c_{n-1}$ so $a_n' + rc_n q = a' + sc_1 \ldots c_{n-1} q$; call this element a. Clearly $(a', c_i q) \sim_q (a, c_i q)$, $1 \leq i < n$, and $(a, c_n q) \sim_q (a_n', c_n q)$, so the lemma is proved.

We now come to the principal object of study in this chapter.

Definition 2.5. — A *Mennicke symbol* on W_q is a function

$$[\ ] : W_q \to C; \qquad (a, b) \mapsto \left[\begin{matrix} b \\ a \end{matrix}\right],$$

where C is a group, which satisfies:

MS 1. $\left[\begin{matrix} 0 \\ 1 \end{matrix}\right] = 1$, and $\left[\begin{matrix} b_1 \\ a_1 \end{matrix}\right] = \left[\begin{matrix} b_2 \\ a_2 \end{matrix}\right]$ if $(a_1, b_1) \sim_q (a_2, b_2)$.

MS 2. If $(a, b_1), (a, b_2) \in W_q$ then $\left[\begin{matrix} b_1 b_2 \\ a \end{matrix}\right] = \left[\begin{matrix} b_1 \\ a \end{matrix}\right]\left[\begin{matrix} b_2 \\ a \end{matrix}\right]$.

This definition makes it clear that there is a *universal* Mennicke symbol,

$$[\ ]_q : W_q \to C_q,$$

such that all others are obtained, in a unique way, by composing $[\ ]_q$ with a homomorphism $C_q \to C$. We can take for C_q, for example, the free group with basis W_q modulo the relations dictated by MS 1 and MS 2.

If $q' \subset q$ then $W_{q'} \subset W_q$, and clearly a Mennicke symbol on W_q induces one on $W_{q'}$. In particular, therefore, there is a canonical homomorphism

$$C_{q'} \to C_q \tag{2.6}$$

Using Lemma 2.3, it follows just from MS 1 that this homomorphism is *surjective.*

We will now record some simple corollaries of the definition.

Lemma 2.7. — *Suppose* $[\ ] : W_q \to C$ *satisfies* MS 1. *Then :*

a) $\left[\begin{matrix} b \\ a \end{matrix}\right] = 1$ *if a is congruent to a unit* mod *b, or if b is congruent to a unit* mod *a.*

b) *If* $q' \subset q$ *then, given* $(a, b) \in W_q$, *we can find* $(a', b') \in W_{q'}$ *such that* $\left[\begin{matrix} b \\ a \end{matrix}\right] = \left[\begin{matrix} b' \\ a' \end{matrix}\right]$.

c) *If* $q \in \mathfrak{q}$ *and if* $a \equiv 1 \bmod q$, *then the map* $b \mapsto \left[\begin{matrix} bq \\ a \end{matrix}\right]$ *for* $b \in A$, *b prime to a, induces a map*

$$U(A/aA) \to C \tag{2.8}$$

whose composite with the homomorphism $U(A) \to U(A/aA)$ *is the constant map* 1.

d) *Any finite set of symbols* $\left[\begin{matrix} b_i \\ a_i \end{matrix}\right]$ *belong to the image of* (2.8) *for a suitable choice of q and a, and a can be chosen arbitrarily from a " progression "* $a + tcq$ $(t \in A)$ *for some c prime to a.*

Proof. — *a)* follows from Lemma 2.2 *b).*

b) follows from Lemma 2.3.

c) Clearly the q-equivalence class of (a, bq) depends on b only mod a, so (2.8) is well defined. If b is a unit then $a \equiv 1 \bmod bq$, so $\left[\begin{matrix} bq \\ a \end{matrix}\right] = 1$ by part *a).*

d) follows from *b)* and Lemma 2.4.

Lemma 2.9. — *Suppose* $[\ ] : W_q \to C$ *is a Mennicke symbol. Then :*

a) *The maps* (2.8) *are homomorphisms.*

b) *The image of* W_q *is an abelian subgroup of* C.

Proof. — *a)* For $a \equiv 1 \bmod q$ we have $\left[\begin{matrix} q \\ a \end{matrix}\right] = 1$ by Lemma 2.7 *a)*. Therefore for $b_1, b_2 \in A$ and prime to a we have

$$\left[\begin{matrix} b_1 b_2 q \\ a \end{matrix}\right] = \left[\begin{matrix} b_1 b_2 q \\ a \end{matrix}\right]\left[\begin{matrix} q \\ a \end{matrix}\right] = \left[\begin{matrix} b_1 q b_2 q \\ a \end{matrix}\right] = \left[\begin{matrix} b_1 q \\ a \end{matrix}\right]\left[\begin{matrix} b_2 q \\ a \end{matrix}\right],$$

so (2.8) is a homomorphism.

b) now follows from Lemma 2.7 *d)* and the fact that $U(A/aA)$ is an abelian group.

We have now established all the lemmas required for the theorems of Chapter I. The balance of this section contains material to be applied in Chapter II.

Lemma 2.10 (Kervaire " reciprocity "). — *Suppose* $a \equiv 1 \equiv d \bmod q$ *for some* $q \in \mathfrak{q}$, *and suppose* $aA + dA = A$. *Then if* $[\ ] : W_{\mathfrak{q}} \to C$ *is a Mennicke symbol we have*

$$\left[\begin{matrix} aq \\ d \end{matrix}\right] = \left[\begin{matrix} dq \\ a \end{matrix}\right]$$

Proof. — Write $d - a = qx$. Then $\left[\begin{matrix} dq \\ a \end{matrix}\right] = \left[\begin{matrix} dq - aq \\ a \end{matrix}\right] = \left[\begin{matrix} xq^2 \\ a \end{matrix}\right] = \left[\begin{matrix} xq \\ a \end{matrix}\right] = \left[\begin{matrix} xq \\ a + xq \end{matrix}\right] = \left[\begin{matrix} xq \\ d \end{matrix}\right]$.

On the other hand, $\left[\begin{matrix} aq \\ d \end{matrix}\right] = \left[\begin{matrix} aq - dq \\ d \end{matrix}\right] = \left[\begin{matrix} -q^2 x \\ d \end{matrix}\right] = \left[\begin{matrix} xq \\ d \end{matrix}\right]$.

Lemma 2.11 (Lam, Mennicke-Newman). — *If* $[\ ] : W_{\mathfrak{q}} \to C$ *is a Mennicke symbol, and if* $(a_1, b), (a_2, b) \in W_{\mathfrak{q}}$, *then*

$$\left[\begin{matrix} b \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} b \\ a_1 \end{matrix}\right]\left[\begin{matrix} b \\ a_2 \end{matrix}\right] \tag{2.12}$$

Remark. — This property was discovered and proved by Mennicke and Newman for the particular symbols constructed in Chapter II. Lam supplied the following axiomatic proof. Lam also has shown that MS 1 and (2.12) imply MS 2.

Proof. — Case 1. — There is a $q \in \mathfrak{q}$ such that $a_1 \equiv a_2 \equiv 1 \bmod q$.

Then $\left[\begin{matrix} q \\ a_1 a_2 \end{matrix}\right] = 1 = \left[\begin{matrix} q \\ a_i \end{matrix}\right]$, $i = 1, 2$, so it suffices to show that $\left[\begin{matrix} bq \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} bq \\ a_1 \end{matrix}\right]\left[\begin{matrix} bq \\ a_2 \end{matrix}\right]$. For this, neither side is altered if we vary $b \bmod a_1 a_2$, so we can arrange that b is prime to q. Then we can find b' solving

$$b_1 = b' b \equiv 1 \bmod q$$
$$b' \equiv 1 \bmod a_1 a_2.$$

Using Lemmas 2.7 and 2.9 we obtain

$$\left[\begin{matrix} b_1 q \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} b' q \\ a_1 a_2 \end{matrix}\right]\left[\begin{matrix} bq \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} bq \\ a_1 a_2 \end{matrix}\right]$$

and, for $i = 1, 2$,

$$\left[\begin{matrix} b_1 q \\ a_i \end{matrix}\right] = \left[\begin{matrix} b' q \\ a_i \end{matrix}\right] \quad \left[\begin{matrix} bq \\ a_i \end{matrix}\right] = \left[\begin{matrix} bq \\ a_i \end{matrix}\right]$$

Finally, we have from Lemma 2.10 and Lemma 2.9 *a)*,

$$\left[\begin{matrix} b_1 q \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} a_1 a_2 q \\ b_1 \end{matrix}\right] = \left[\begin{matrix} a_1 q \\ b_1 \end{matrix}\right]\left[\begin{matrix} a_2 q \\ b_1 \end{matrix}\right] = \left[\begin{matrix} b_1 q \\ a_1 \end{matrix}\right]\left[\begin{matrix} b_1 q \\ a_2 \end{matrix}\right]$$

General case. — Write $a_1 = 1 - q$. Neither side of (2.12) is altered if we replace b by $b_1 = b + t a_1 a_2$ for some $t \in \mathfrak{q}$. We can choose t so that q and b_1 generate $\mathfrak{q}$. For since $a_1 a_2$ is prime to b we can do this locally, clearly, and then use the Chinese Remainder Theorem to obtain a t that works at each prime dividing q. (If $q = 0$ our problem is trivial, so we can assume $q \neq 0$.) Next write $a_2 = 1 + q'$, $q' \in \mathfrak{q}$. Then $q' = r b_1 + sq$ for some $r, s \in A$. Neither side of the alleged equation,

$$\left[\begin{matrix} b_1 \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} b_1 \\ a_1 \end{matrix}\right]\left[\begin{matrix} b_1 \\ a_2 \end{matrix}\right],$$

is altered if we replace a_2 by $a_2' = a_2 - r b_1 = 1 + sq$. Therefore we have reduced the general case to case 1.

We close this section by showing how to extend a Mennicke symbol, $\left[\begin{matrix} b \\ a \end{matrix}\right]$ on $W_{\mathfrak{q}}$, to a symbol $\left[\begin{matrix} \mathfrak{b} \\ a \end{matrix}\right]$, where $\mathfrak{b}$ is an ideal. This result will not be needed in what follows, but it is perhaps worth pointing out.

Let

$$\overline{W}_{\mathfrak{q}} = \{(a, \mathfrak{b}) \mid a \equiv 1 \bmod \mathfrak{q};\ \mathfrak{b} \neq 0 \text{ is an ideal in } \mathfrak{q};\ aA + \mathfrak{b} = A\}.$$

Proposition 2.13. — *If* $(a, b) \mapsto \left[\begin{matrix} b \\ a \end{matrix}\right]$ *is a Mennicke symbol on* $W_{\mathfrak{q}}$, *then there is a unique function,* $(a, \mathfrak{b}) \mapsto \left[\begin{matrix} \mathfrak{b} \\ a \end{matrix}\right]$, *on* $\overline{W}_{\mathfrak{q}}$ *satisfying* :

M 0. — *If* $(a, b) \in W_{\mathfrak{q}}$, $b \neq 0$, *then* $\left[\begin{matrix} bA \\ a \end{matrix}\right] = \left[\begin{matrix} b \\ a \end{matrix}\right]$.

M 1. — *If* $(a, \mathfrak{b}) \in \overline{W}_{\mathfrak{q}}$ *then* $\left[\begin{matrix} \mathfrak{b} \\ 1 \end{matrix}\right] = 1$ *and* $\left[\begin{matrix} \mathfrak{b} \\ a + b \end{matrix}\right] = \left[\begin{matrix} \mathfrak{b} \\ a \end{matrix}\right]$ *for all* $b \in \mathfrak{b}$.

M 2. — *If* $(a, \mathfrak{b}_1), (a, \mathfrak{b}_2) \in W_{\mathfrak{q}}$ *then*

$$\left[\begin{matrix} \mathfrak{b}_1 \mathfrak{b}_2 \\ a \end{matrix}\right] = \left[\begin{matrix} \mathfrak{b}_1 \\ a \end{matrix}\right]\left[\begin{matrix} \mathfrak{b}_2 \\ a \end{matrix}\right]$$

M 3. — *If* $(a_1, \mathfrak{b}), (a_2, \mathfrak{b}) \in W_{\mathfrak{q}}$ *then* $\left[\begin{matrix} \mathfrak{b} \\ a_1 a_2 \end{matrix}\right] = \left[\begin{matrix} \mathfrak{b} \\ a_1 \end{matrix}\right]\left[\begin{matrix} \mathfrak{b} \\ a_2 \end{matrix}\right]$.

Proof. — Since an ideal in $\mathfrak{q}$ has $\mathfrak{q}$ as a factor we can write the elements of $\overline{W}_{\mathfrak{q}}$ in the form $(a, \mathfrak{b}\mathfrak{q})$, where $a \equiv 1 \bmod \mathfrak{q}$ and $aA + \mathfrak{b} = A$.

Uniqueness. — Choose $\mathfrak{c}$ prime to $\mathfrak{b}\mathfrak{q}$ so that $\mathfrak{c}\mathfrak{b}\mathfrak{q} = dA$ is principal, and choose a' solving

$$(*) \qquad \begin{aligned} a' &\equiv a \bmod \mathfrak{b}\mathfrak{q} \\ a' &\equiv 1 \bmod \mathfrak{c} \end{aligned}$$

Since $a \equiv 1 \bmod \mathfrak{q}$ we have $a' \equiv 1 \bmod \mathfrak{cq}$ so M 1 implies $\left[\begin{smallmatrix}\mathfrak{cq}\\ a'\end{smallmatrix}\right] = 1 = \left[\begin{smallmatrix}\mathfrak{q}\\ a'\end{smallmatrix}\right]$. Therefore

$$\begin{aligned}\left[\begin{smallmatrix}\mathfrak{bq}\\ a\end{smallmatrix}\right] &= \left[\begin{smallmatrix}\mathfrak{bq}\\ a'\end{smallmatrix}\right]\left[\begin{smallmatrix}\mathfrak{cq}\\ a'\end{smallmatrix}\right] \\ &= \left[\begin{smallmatrix}\mathfrak{cbq}^2\\ a'\end{smallmatrix}\right] \qquad \text{(M 2)} \\ &= \left[\begin{smallmatrix}\mathfrak{cbq}\\ a'\end{smallmatrix}\right]\left[\begin{smallmatrix}\mathfrak{q}\\ a'\end{smallmatrix}\right] \qquad \text{(M 2)} \\ &= \left[\begin{smallmatrix}d\\ a'\end{smallmatrix}\right] \qquad \text{(M 0 and M 1)}\end{aligned}$$

Existence. — Define $\left[\begin{smallmatrix}\mathfrak{bq}\\ a\end{smallmatrix}\right] = \left[\begin{smallmatrix}d\\ a'\end{smallmatrix}\right]$ as above. We must check that this is independent of the choices: $\mathfrak{c}$, then d, then a'. The congruences $(*)$ determine $a' \bmod d\mathrm{A} = \mathfrak{cbq}$ so $\left[\begin{smallmatrix}d\\ a'\end{smallmatrix}\right]$ does not depend on the choice of a'. Neither does it depend on d, which is determined by $\mathfrak{c}$ up to a unit factor.

Finally, suppose $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are prime to $\mathfrak{b}$ (hence to $\mathfrak{bq}$) and that $\mathfrak{c}_i\mathfrak{bq} = d_i\mathrm{A}$, $i = 1, 2$. Choose $\mathfrak{b}'$ prime to $\mathfrak{bq}$ so that $\mathfrak{c}_i\mathfrak{b}'\mathfrak{q} = e_i\mathrm{A}$, $i = 1, 2$; just take $\mathfrak{b}'$ in the ideal class of $\mathfrak{b}$. Then

$$e_1d_2\mathrm{A} = \mathfrak{c}_1\mathfrak{b}'\mathfrak{q}\,\mathfrak{c}_2\mathfrak{bq} = \mathfrak{c}_2\mathfrak{b}'\mathfrak{q}\,\mathfrak{c}_1\mathfrak{bq} = e_2d_1\mathrm{A}.$$

Choose an a' solving

$$\begin{aligned}a' &\equiv a \bmod \mathfrak{bq} \\ a' &\equiv 1 \bmod \mathfrak{c}_1\mathfrak{c}_2\mathfrak{b}'.\end{aligned}$$

Then $a' \equiv 1 \bmod \mathfrak{c}_1\mathfrak{c}_2\mathfrak{b}'\mathfrak{q} = e_1\mathfrak{c}_2 = e_2\mathfrak{c}_1$, so $\left[\begin{smallmatrix}e_i\\ a'\end{smallmatrix}\right] = 1$, $i = 1, 2$. We must show that $\left[\begin{smallmatrix}d_1\\ a'\end{smallmatrix}\right] = \left[\begin{smallmatrix}d_2\\ a'\end{smallmatrix}\right]$. But

$$\begin{aligned}\left[\begin{smallmatrix}d_1\\ a'\end{smallmatrix}\right] &= \left[\begin{smallmatrix}d_1\\ a'\end{smallmatrix}\right]\left[\begin{smallmatrix}e_2\\ a'\end{smallmatrix}\right] = \left[\begin{smallmatrix}d_1e_2\\ a'\end{smallmatrix}\right] \\ &= \left[\begin{smallmatrix}d_2e_1\\ a'\end{smallmatrix}\right] = \left[\begin{smallmatrix}d_2\\ a'\end{smallmatrix}\right]\left[\begin{smallmatrix}e_1\\ a'\end{smallmatrix}\right] = \left[\begin{smallmatrix}d_2\\ a'\end{smallmatrix}\right]\end{aligned}$$

Now that $\left[\begin{smallmatrix}\mathfrak{b}\\ a\end{smallmatrix}\right]$ is well defined M 0 is clear. If $a = 1$ we can choose a' above equal to 1, so $\left[\begin{smallmatrix}\mathfrak{b}\\ 1\end{smallmatrix}\right] = \left[\begin{smallmatrix}d\\ 1\end{smallmatrix}\right] = 1$.

Replacing a by $a + b$, $b \in \mathfrak{bq}$, we can make the same choices of $\mathfrak{c}$, d, a' above, so M 1 follows.

Suppose $(a, \mathfrak{b}_1\mathfrak{q}), (a, \mathfrak{b}_2\mathfrak{q}) \in \overline{\mathrm{W}}_{\mathfrak{q}}$. Choose $\mathfrak{c}_i$ prime to $\mathfrak{b}_1\mathfrak{b}_2$ such that $\mathfrak{c}_i\mathfrak{b}_i\mathfrak{q} = d_i\mathrm{A}$, $i = 1, 2$. Then choose a' so that

$$\begin{aligned}a' &\equiv a \bmod \mathfrak{b}_1\mathfrak{b}_2\mathfrak{q} \\ a' &\equiv 1 \bmod \mathfrak{c}_1\mathfrak{c}_2\end{aligned}$$

Since $(\mathfrak{c}_1\mathfrak{c}_2)(\mathfrak{b}_1\mathfrak{q}\mathfrak{b}_2\mathfrak{q}) = d_1 d_2 \mathrm{A}$ we have

$$\left[\begin{matrix}\mathfrak{b}_1\mathfrak{q}\mathfrak{b}_2\mathfrak{q}\\ a\end{matrix}\right] = \left[\begin{matrix}d_1 d_2\\ a'\end{matrix}\right] = \left[\begin{matrix}d_1\\ a'\end{matrix}\right]\left[\begin{matrix}d_2\\ a'\end{matrix}\right] = \left[\begin{matrix}\mathfrak{b}_1\\ a\end{matrix}\right]\left[\begin{matrix}\mathfrak{b}_2\\ a\end{matrix}\right].$$

Finally, to prove M 3, suppose $(a_1, \mathfrak{b}\mathfrak{q}), (a_2, \mathfrak{b}\mathfrak{q}) \in \mathrm{W}_\mathfrak{q}$. Choose $\mathfrak{c}$, d, and a_i' as above, $i = 1, 2$. Then $\mathfrak{c}$, d, and $a' = a_1' a_2'$ clearly serve to define the symbol for $(a_1 a_2, \mathfrak{b}\mathfrak{q})$. Hence

$$\left[\begin{matrix}\mathfrak{b}\mathfrak{q}\\ a_1 a_2\end{matrix}\right] = \left[\begin{matrix}d\\ a_1' a_2'\end{matrix}\right] = \left[\begin{matrix}d\\ a_1'\end{matrix}\right]\left[\begin{matrix}d\\ a_2'\end{matrix}\right] \qquad \text{(Lemma 2.11)}$$

$$= \left[\begin{matrix}\mathfrak{b}\mathfrak{q}\\ a_1\end{matrix}\right]\left[\begin{matrix}\mathfrak{b}\mathfrak{q}\\ a_2\end{matrix}\right]$$

Remark. — The symbol $\left[\begin{matrix}b\\ a\end{matrix}\right]$ is trivial whenever a is a unit. We shall exhibit examples in § 4 for which $\left[\begin{matrix}\mathfrak{b}\\ a\end{matrix}\right] \neq 1$ even when a is a unit. In this way we can get a non trivial pairing of the units of A with the ideal class group of A.

§ 3. Determination of arithmetic Mennicke symbols.

Throughout this section A denotes a Dedekind ring of arithmetic type defined by a finite set, S_∞, of primes in a global field k. This terminology as well as that to follow, is taken from the appendix on number theory, to which frequent reference will be made here.

We shall call A *totally imaginary* if S_∞ consists of complex primes. This means that k is a totally imaginary number field, and that A is its ring of algebraic integers.

For an integer $m \geq 1$ we shall write μ_m for the group of all m-th roots of unity (in some algebraic closure of k). It will be understood, when we write μ_m, that m is prime to $\mathrm{char}(k)$, so that μ_m is a cyclic group of order m.

Here is the first example of a non trivial Mennicke symbol.

Proposition 3.1. — *Suppose that* A *is totally imaginary and that* $\mu_m \subset k$. *Let* $\mathfrak{q}$ *be an ideal such that, for all primes* $\mathfrak{p}$ *dividing* m, *if* p *is the rational prime over which* $\mathfrak{p}$ *lies, we have*

$$\frac{\mathrm{ord}_\mathfrak{p}(\mathfrak{q})}{\mathrm{ord}_\mathfrak{p}(p)} - \frac{1}{p-1} \geq \mathrm{ord}_p(m).$$

Then $(a, b) \mapsto \left(\frac{b}{a}\right)_m$ $(= 1$ *if* $b = 0)$ *is a Mennicke symbol*

$$(-)_m : \mathrm{W}_\mathfrak{q} \to \mu_m.$$

Remarks. — 1. For the definition of the power residue symbol $\left(\frac{b}{a}\right)_m$, see formula A.20 of the Appendix. Note that the hypothesis makes a prime to m, so that $\left(\frac{b}{a}\right)_m$ is defined if $b \neq 0$; when $b = 0$ we have made the convention that $\left(\frac{b}{a}\right)_m = 1$.

2. The main result of this chapter, Theorem 3.6 below, says that Proposition 3.1 accounts for all non trivial Mennicke symbols of arithmetic type.

Proof. — It follows immediately from the definition (A.20) that $\left(\frac{b}{a}\right)_m$ is bimultiplicative and depends on b only modulo a. (Note that b can be zero only when a is a unit, in which case $\left(\frac{b}{a}\right)_m = 1$ for all b's.) These remarks establish all the axioms for a Mennicke symbol except the fact that $\left(\frac{b}{a}\right)_m$ depends on a only modulo b. This is trivial if $b=0$ so suppose otherwise, and apply the reciprocity formula, (A.21):

$$\left(\frac{b}{a}\right)_m = \prod_{\mathfrak{p}\nmid a} \left(\frac{a, b}{\mathfrak{p}}\right)_m$$

If $\mathfrak{p}\nmid abm$ then either $\mathfrak{p}$ is finite and $\left(\frac{a, b}{\mathfrak{p}}\right)_m = 1$ by (A.16), or $\mathfrak{p}$ is complex (by hypothesis). Therefore, using (A.16) again,

$$\left(\frac{b}{a}\right)_m = \prod_{\mathfrak{p}\mid b,\ \mathfrak{p}\nmid m} \left(\frac{a}{\mathfrak{p}}\right)_m^{\mathrm{ord}_{\mathfrak{p}}(b)} \cdot \prod_{\mathfrak{p}\mid m} \left(\frac{a, b}{\mathfrak{p}}\right)_m .$$

The first factors clearly depend on a only modulo b. Finally, suppose $\mathfrak{p}\mid m$ and set $h=\mathrm{ord}_{\mathfrak{p}}(\mathfrak{q})$ and $e=\mathrm{ord}_{\mathfrak{p}}(p)$, where p is the rational prime $\mathfrak{p}$ divides. We have assumed that

$$\frac{h}{e} - \frac{1}{p-1} \geq n = \mathrm{ord}_p(m).$$

With this we conclude from (A.18) that $\left(\frac{a, b}{\mathfrak{p}}\right)_{p^n}$ depends on a only modulo b for $(a, b)\in W_{\mathfrak{q}}$. Writing $m=p^n m'$ with m' prime to p we have

$$\left(\frac{a, b}{\mathfrak{p}}\right)_m = \left(\left(\frac{a, b}{\mathfrak{p}}\right)_{p^n}\right)^r \left(\left(\frac{a, b}{\mathfrak{p}}\right)_{m'}\right)^s$$

for suitable integers r and s (independent of a and b), and $\left(\frac{a, b}{\mathfrak{p}}\right)_m = \left(\frac{a}{\mathfrak{p}}\right)_{m'}^{\mathrm{ord}_{\mathfrak{p}}(b)}$ depends on a only modulo b. This completes the proof.

Let p be a rational prime and let μ_{p^n} be the group of *all* p-th power roots of unity in k. (If $\mathrm{char}(k)=p$ then $n=0$.) This notation will be fixed in the next two theorems.

Theorem 3.2. — *Given* $(a, b)\in W_{\mathfrak{q}}$, *we can find an* $(a_1, b_1)\sim_{\mathfrak{q}}(a, b)$ *such that* $a_1 A = \mathfrak{p}_1\mathfrak{p}_2$, *a product of distinct primes, which satisfy* $\mathbf{N}\mathfrak{p}_i \not\equiv 1 \bmod p^{n+1}$, $i=1, 2$. *In case* k *is a number field we can choose the* $\mathfrak{p}_i$ *prime to* p; *moreover, if* $\mathfrak{q}\subset p^{n+1}A$ *and* $b\neq 0$ *then we can find* $a_1\equiv a \bmod b$ *with this property.*

Proof. — *Number field case:* Suppose first that A is the ring of algebraic integers in k. Let $P=\{\mathfrak{p}\notin S_\infty \mid \mathbf{N}\mathfrak{p}\not\equiv 1 \bmod p^{n+1}\}$. Our hypothesis, together with (A.8), implies that P is *infinite.*

Using Lemma 2.3 we see that it suffices to prove the theorem for ideals divisible by $p^{n+1}A$, so assume $\mathfrak{q} \subset p^{n+1}A$. We may also arrange that $b \neq 0$. Then the theorem will be proved if we find $a_1 \equiv a \bmod bA$ satisfying the conditions of the theorem, for then clearly $(a_1, b) \sim_{\mathfrak{q}} (a, b)$.

Since $b \neq 0$ and P is infinite we can choose a $\mathfrak{p}_1 \in P$ prime to b. Then we can apply the Dirichlet Theorem (A.11) to find $a_1 \equiv a \bmod b$ such that a_1 is positive at the real primes, and such that $a_1 A = \mathfrak{p}_1 \mathfrak{p}_2$ for some prime $\mathfrak{p}_2$. It remains only to be shown that $\mathfrak{p}_2 \in P$, i.e. that $\mathbf{N}\mathfrak{p}_2 \not\equiv 1 \bmod p^{n+1}$.

$\mathbf{N}\mathfrak{p}_1 \mathbf{N}\mathfrak{p}_2 = \operatorname{card}(A/a_1 A) = |N_{k/\mathbf{Q}} a_1|$, since A is the ring of integers of k. Since a_1 is positive at the real primes, and since $a_1 \equiv 1 \bmod \mathfrak{q}$ with $\mathfrak{q} \subset p^{n+1}A$, we have

$$|N_{k/\mathbf{Q}} a_1| = N_{k/\mathbf{Q}} a_1 \equiv 1 \bmod p^{n+1}\mathbf{Z}.$$

Since $\mathbf{N}\mathfrak{p}_1 \not\equiv 1 \bmod p^{n+1}\mathbf{Z}$ the desired conclusion now follows.

Next suppose A′ is some other Dedekind ring of arithmetic type in k. Then $A' = A[s^{-1}]$ for some $s \in A$, where A is as above. The theorem for A′ follows by using Lemma 2.1 to replace (a, b) by a $\mathfrak{q}$-equivalent pair in $W_{\mathfrak{q} \cap A}$, and then applying the argument above, making sure that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not divide s. This is possible since we have infinitely many choices for each of them.

Function field case. — First suppose $p \neq \operatorname{char}(k)$. Let $\mathbf{F}_q$ be the constant field of k, and let m be the least positive integer such that $p^{n+1} | q^m - 1$. The hypothesis of the theorem implies that $m > 1$. Let $P = \{\mathfrak{p} \notin S_\infty \mid \deg(\mathfrak{p}) \text{ is prime to } m\}$. Then (A.9) says P is infinite. Moreover, if $\mathfrak{p} \in P$, then $\mathbf{N}\mathfrak{p} \equiv 1 \bmod p^{n+1}$. To see this write $\mathbf{N}\mathfrak{p} = q^d$, where $d = \deg(\mathfrak{p})$ is prime to m. If $I = (q^m - 1)\mathbf{Z} + (q^d - 1)\mathbf{Z} \subset (q-1)\mathbf{Z}$ then, modulo I, $q^m \equiv 1 \equiv q^d$, so $q \equiv 1$; i.e. g.c.d.$(q^m - 1, q^d - 1) = q - 1$. Therefore if p^{n+1} divides $q^d - 1$ it also divides $q - 1$, contradicting our hypothesis.

Given $(a, b) \in W_{\mathfrak{q}}$ (we can assume $b \neq 0$) choose a $\mathfrak{p}_1 \in P$ prime to b. This is possible because P is infinite. Now use the Dirichlet Theorem (A.12) to find $a_1 \equiv a \bmod b$ such that $\operatorname{ord}_{\mathfrak{p}}(a_1) \equiv 0 \bmod m$ at all $\mathfrak{p} \in S_\infty$ and such that $a_1 A = \mathfrak{p}_1 \mathfrak{p}_2$ for some prime $\mathfrak{p}_2 \neq \mathfrak{p}_1$. The product formula (A.3) yields

$$\begin{aligned} 0 &= \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(a_1) \deg(\mathfrak{p}) \\ &= \deg(\mathfrak{p}_1) + \deg(\mathfrak{p}_2) + \sum_{\mathfrak{p} \in S_\infty} \operatorname{ord}_{\mathfrak{p}}(a_1) \deg(\mathfrak{p}) \\ &\equiv \deg(\mathfrak{p}_1) + \deg(\mathfrak{p}_2) \quad \bmod m\mathbf{Z} \end{aligned}$$

Since $\mathfrak{p}_1 \in P$ this implies $\mathfrak{p}_2 \in P$ also, and since $(a_1, b) \sim_{\mathfrak{q}} (a, b)$, the theorem now follows from the fact, proved above, that $\mathbf{N}\mathfrak{p} \not\equiv 1 \bmod p^{n+1}$ for $\mathfrak{p} \in P$.

Finally, if $\operatorname{char}(k) = p$ we can take any $a_1 \equiv a \bmod b$ which is a product of two distinct primes, and the conclusion of the theorem is automatic. This concludes the proof of Theorem 3.2.

Before stating the next result we must introduce some further notation. Recall that μ_{p^n} is the group of all p-th power roots of unity in k.

Suppose that A is totally imaginary and let $\mathfrak{q}$ be a non zero ideal in A. We define

$$j_p(\mathfrak{q}) = \min_{\mathfrak{p}|p} \left[\frac{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{q})}{\mathrm{ord}_{\mathfrak{p}}(p)} - \frac{1}{p-1} \right]_{[0,n]} \tag{3.3}$$

For $x \in \mathbf{R}$, $[x]_{[0,n]}$ denotes the nearest integer in the interval $[0, n]$ to the largest integer $\leq x$. I.e. $[x]_{[0,n]} = \inf(\sup(0, [x]), n)$.

Lemma 3.4. — a) *With* $j = j_p(\mathfrak{q})$, *there is a prime* $\mathfrak{p}_0$ *dividing* p, *a* $u \equiv 1 \bmod \mathfrak{q}$, *and a* $v \in U_{\mathfrak{p}_0}$, *such that* $\left(\frac{u, v}{\mathfrak{p}_0}\right)_{p^n}$ *generates* $\mu_{p^{n-j}}$.

b) $(-)_{pj} : W_{\mathfrak{q}} \to \mu_{pj}$ *is a Mennicke symbol.*

Proof. — *a)* $j = \left[\frac{\mathrm{ord}_{\mathfrak{p}_0}(\mathfrak{q})}{\mathrm{ord}_{\mathfrak{p}_0}(p)} - \frac{1}{p-1} \right]_{[0,n]}$ for some $\mathfrak{p}_0$ dividing p, and (A.17) tells us that

$$\mu_{p^{n-j}} = \left(\frac{U_{\mathfrak{p}_0}(h), U_{\mathfrak{p}_0}}{\mathfrak{p}_0} \right)_{p^n}$$

where $h = \mathrm{ord}_{\mathfrak{p}_0}(\mathfrak{q})$, hence the result.

b) follows from Proposition 3.1 if $j > 0$, and it is obvious if $j = 0$.

Theorem 3.5. — *Suppose* $(a, b) \in W_{\mathfrak{q}}$. *Let* p *be a prime number, and let* n *be the largest integer such that* k *contains* μ_{p^n}. *Then there exist* $q \in \mathfrak{q}$, $a_1 \equiv 1 \bmod q$, *and* $c \in A$, *such that* $(a, b) \sim_{\mathfrak{q}} (a_1, c^{p^n} q)$, *except in the following case:* A *is totally imaginary and* $\left(\frac{b}{a}\right)_{pj} \neq 1$, *where* $j = j_p(\mathfrak{q})$.

(Lemma 3.4 guarantees that $\left(\frac{b}{a}\right)_{pj}$ above is defined.)

Proof. — We shall call two non zero elements " close at $\mathfrak{p}$ " if they are multiplicatively congruent modulo p^n-th powers. Note that this is a congruence relation modulo an open subgroup of finite index.

Case 1. — A *is not totally imaginary.*

Then there is a non-complex (i.e. either real or finite) $\mathfrak{p}_\infty \in S_\infty$, and the non degeneracy of the Hilbert symbol shows that we can find $u, v \in k^*_{\mathfrak{p}_\infty}$ such that $\left(\frac{u, v}{\mathfrak{p}_\infty}\right)_{p^n}$ generates μ_{p^n}.

Choose a principal ideal $q\mathrm{A} \subset \mathfrak{q}$, and, with the aid of Lemma 2.3, an $(a', b'q) \in W_q$ which is $\mathfrak{q}$-equivalent to (a, b). We can take $b' \neq 0$, and, altering a' mod $b'q$, arrange that a' is prime to p in the number field case.

Now the Dirichlet theorem (A.10) gives us a prime $b_1\mathrm{A}$, where b_1 satisfies

$b_1 \equiv b' \bmod a'$

b_1 is close to v at $\mathfrak{p}_\infty$

b_1 is close to 1 at all $\mathfrak{p} \in S_\infty - \{\mathfrak{p}_\infty\}$, and at all $\mathfrak{p} \notin S_\infty$ which divide p, in the number field case.

The last condition makes $b_1\mathrm{A}$ prime to p in the number field case.

Since $\left(\frac{u, v}{\mathfrak{p}_\infty}\right)_{p^n}$ generates μ_{p^n} we can solve $\left(\frac{a', b_1}{b_1 \mathrm{A}}\right)_{p^n} \cdot \left(\frac{u, v}{\mathfrak{p}_\infty}\right)_{p^n}^{i} = 1$ for some $i > 0$. Use Dirichlet now to find a prime $a_1 \mathrm{A}$, prime to p in the number field case, so that

$$a_1 \equiv a' \bmod b_1 q$$
$$a_1 \text{ is close to } u^i \text{ at } \mathfrak{p}_\infty$$

Now we apply the reciprocity formula (A.21):

$$\left(\frac{b_1}{a_1}\right)_{p^n} = \prod_{\mathfrak{p} \nmid a_1} \left(\frac{a_1, b_1}{\mathfrak{p}}\right)_{p^n}.$$

On the right our conditions on b_1 exclude any contribution from S_∞ except at $\mathfrak{p}_\infty$, as well as any from the primes dividing p in the number field case. Using (A.16) to eliminate most of the finite primes, therefore, we have

$$\left(\frac{b_1}{a_1}\right)_{p^n} = \left(\frac{a_1, b_1}{b_1 \mathrm{A}}\right)_{p^n} \cdot \left(\frac{a_1, b_1}{\mathfrak{p}_\infty}\right)_{p^n}.$$

Since $b_1 \mathrm{A}$ is not p-adic the first factor depends on a_1 only modulo b_1, so our approximations, and choice of i, leave us with

$$\left(\frac{b_1}{a_1}\right)_{p^n} = \left(\frac{a', b_1}{b_1 \mathrm{A}}\right)_{p^n} \cdot \left(\frac{u^i, v}{\mathfrak{p}_\infty}\right)_{p^n} = 1.$$

Thus b_1 is a p^n-th power modulo a_1, say $b_1 \equiv c^{p^n} \bmod a_1$. Then

$$(a, b) \sim_{\mathfrak{q}} (a', b'q) \sim_q (a', b_1 q) \sim_q (a_1, b_1 q) \sim_q (a_2, c^{p^n} q),$$

and the proof is complete.

Case 2. — A *is totally imaginary, but* $\mathfrak{q}$ *is not divisible by every prime dividing* p.

Let $\mathfrak{q}' \subset \mathfrak{q}$ be the largest ideal in $\mathfrak{q}$ which is so divisible. Then $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{q}') = 1$ for at least one $\mathfrak{p}$ dividing p, so it follows that $j_p(\mathfrak{q}') = j_p(\mathfrak{q}) = 0$ (see (3.3)). Use Lemma 2.3 to find an $(a', b') \in \mathrm{W}_{\mathfrak{q}'}$ which is $\mathfrak{q}$-equivalent to (a, b). Then, since $j_p(\mathfrak{q}') = 0$, this case follows now from:

Case 3. — A *is totally imaginary,* $\mathfrak{q}$ *is divisible by every prime dividing* p, *and* $\left(\frac{b}{a}\right)_{pj} = 1$.

We recall from Lemma 3.4 that $(-)_{pj}$ is a Mennicke symbol on $\mathrm{W}_{\mathfrak{q}}$.

Choose $q \in \mathfrak{q}$ such that $\mathrm{ord}_{\mathfrak{p}}(q) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{q})$ for all $\mathfrak{p} \mid p$. Clearly then $j_p(q) = j_p(\mathfrak{q})$, and we can find an $(a', b'q) \in \mathrm{W}_q$ which is $\mathfrak{q}$-equivalent to (a, b). Then

$$1 = \left(\frac{b}{a}\right)_{pj} = \left(\frac{b'q}{a'}\right)_{pj} = \left(\frac{b'}{a'}\right)_{pj} \left(\frac{q}{a'}\right)_{pj} = \left(\frac{b'}{a'}\right)_{pj}$$

because $(-)_{pj}$ is a Mennicke symbol on $\mathrm{W}_{\mathfrak{q}}$, and because $a' \equiv 1 \bmod q$.

Choose a $\mathfrak{p}_0$, u, and v as in Lemma 3.4 *a)*. If $h = \mathrm{ord}_{\mathfrak{p}_0}(\mathfrak{q})$ then $u \equiv 1 \bmod \mathfrak{p}_0^h$, $v \in \mathrm{U}_{\mathfrak{p}_0}$, and $\left(\frac{u, v}{\mathfrak{p}_0}\right)_{p^n}$ generates $\mu_{p^{n-j}}$.

We now use the Dirichlet theorem (A.10) to find a $b_1 \in A$ such that

$b_1 \equiv b' \bmod a'$
b_1 is close to v at $\mathfrak{p}_0$
b_1 is close to 1 at all other $\mathfrak{p}$ dividing p,

and such that $b_1 A$ is a prime, prime to q. Since $a' \equiv 1 \bmod q$, a' is prime to p, so these congruences are compatible.

Since $(-)_{pj}$ is a Mennicke symbol on W_q, we obtain, with the reciprocity formula (A.21):

$$1 = \left(\frac{b}{a}\right)_{pj} = \left(\frac{b'}{a'}\right)_{pj} = \left(\frac{b_1}{a'}\right)_{pj} = \prod_{\mathfrak{p} \nmid a'} \left(\frac{a', b_1}{\mathfrak{p}}\right)_{pj}.$$

Since A is totally imaginary, and since b_1 is close to 1 at all p-adic $\mathfrak{p}$ other than $\mathfrak{p}_0$, we are left with

$$1 = \left(\frac{a', b_1}{b_1}\right)_{pj} \left(\frac{a', b_1}{\mathfrak{p}_0}\right)_{pj}.$$

Since $\left(\frac{a', b_1}{\mathfrak{p}_0}\right)_{p^n} \in \left(\frac{U_{\mathfrak{p}_0}(h), U_{\mathfrak{p}_0}}{\mathfrak{p}_0}\right)_{p^n} = \mu_{p^{n-j}}$ (see (A.17)) we have $\left(\frac{a', b_1}{\mathfrak{p}_0}\right)_{pj} = 1$, hence also $\left(\frac{a', b_1}{b_1}\right)_{pj} = 1$. Therefore $\left(\frac{a', b_1}{b_1}\right)_{p^n} \in \mu_{p^{n-j}}$, so we can find $i \geq 0$ such that

$$\left(\frac{u, v}{\mathfrak{p}_0}\right)_{p^n}^{i} \left(\frac{a', b_1}{b_1}\right)_{p^n} = 1.$$

Now choose a prime a_1 such that

$a_1 \equiv a' \bmod b_1 q$
a_1 is close to u^i at $\mathfrak{p}_0$.

Since $u \equiv 1 \bmod \mathfrak{p}_0^h$, $h = \mathrm{ord}_{\mathfrak{p}_0}(q)$, the same is true of u^i, so these congruences are compatible since b_1 is prime to q. Moreover,

$$(a_1, b_1 q) \sim_q (a', b_1 q) \sim_q (a', b' q) \sim_q (a, b).$$

We conclude the proof now by showing that b_1 is a p^n-th power modulo a_1.

From reciprocity,

$$\left(\frac{b_1}{a_1}\right)_{p^n} = \prod_{\mathfrak{p} \nmid a_1} \left(\frac{a_1, b_1}{\mathfrak{p}}\right)_{p^n} = \left(\frac{a_1, b_1}{b_1}\right)_{p^n} \left(\frac{a_1, b_1}{\mathfrak{p}_0}\right)_{p^n}$$

using the fact that A is totally imaginary, and eliminating most finite primes with the aid of (A.16). The latter shows also that $\left(\frac{a_1, b_1}{b_1}\right)_{p^n} = \left(\frac{a_1}{b_1}\right)_{p^n}$ depends on a_1 only modulo b_1 so $\left(\frac{a_1, b_1}{b_1}\right)_{p^n} = \left(\frac{a', b_1}{b_1}\right)_{p^n}$. At $\mathfrak{p}_0$ our approximations imply

$\left(\frac{a_1, b_1}{\mathfrak{p}_0}\right)_{p^n} = \left(\frac{u^i, v}{\mathfrak{p}_0}\right)_{p^n}$. Hence $\left(\frac{b_1}{a_1}\right)_{p^n} = \left(\frac{a', b_1}{b_1}\right)_{p^n}\left(\frac{u^i, v}{\mathfrak{p}_0}\right)_{p^n} = 1$, so b_1 is indeed a p^n-th power modulo a_1. Q.E.D.

We are now prepared to prove the main theorem of this chapter.

Theorem 3.6. — *If* A *is not totally imaginary then, for all ideals* $\mathfrak{q} \neq 0$, *all Mennicke symbols on* $W_\mathfrak{q}$ *are trivial*; i.e. $C_\mathfrak{q} = \{1\}$.

Suppose A *is totally imaginary, and let m denote the number of roots of unity in k. If* $\mathfrak{q}$ *is a non zero ideal define the divisor* $r = r(\mathfrak{q})$ *of m by* $\mathrm{ord}_\mathfrak{p}(r) = j_\mathfrak{p}(\mathfrak{q})$, *for each prime* $\mathfrak{p}$, *where*

$$j_\mathfrak{p}(\mathfrak{q}) = \min_{\mathfrak{p}\,|\,p}\left[\frac{\mathrm{ord}_\mathfrak{p}(\mathfrak{q})}{\mathrm{ord}_\mathfrak{p}(p)} - \frac{1}{p-1}\right]_{[0,\,\mathrm{ord}_\mathfrak{p}(m)]}$$

as in (3.3). *Then* $(-)_r : W_\mathfrak{q} \to \mu_r$

is a universal Mennicke symbol in $W_\mathfrak{q}$, *so* $C_\mathfrak{q} \cong \mu_r$. *If* $\mathfrak{q} \subset \mathfrak{q}'$ *and if* $r' = r(\mathfrak{q}')$, *then the natural homomorphism* $C_\mathfrak{q} \to C_{\mathfrak{q}'}$ *corresponds to the* (r/r')*-th power map,* $\mu_r \to \mu_{r'}$.

Remark. — In the totally imaginary case it follows already from Proposition 3.1 that $(-)_r$ is a Mennicke symbol on $W_\mathfrak{q}$. The point now being made is its universality. The last assertion follows simply from the formula,

$$(-)_{r'} = ((-)_r)^{r/r'}$$

Proof. — Let $[\ ] : W_\mathfrak{q} \to C$ be a universal Mennicke symbol. We shall use the notation and assertions of Lemmas 2.7 and 2.3. In the homomorphism (2.8) we can use (2.7) *d)* and the Dirichlet Theorem to make aA prime. Then $U(A/aA)$ is cyclic, so we conclude from (2.7) *d)* that:

(i) Every finite subset of C lies in a finite cyclic subgroup.

Suppose $m = p^n m'$ with p a rational prime and m' prime to p. Given $(a, b) \in W_\mathfrak{q}$ we can find $(a_1, b_1) \sim_\mathfrak{q} (a, b)$ as in Theorem 3.2. This implies that $U(A/a_1A)$ has no elements of order p^{n+1}. If $q = 1 - a_1 \in \mathfrak{q}$ then $(a_1, b_1) \sim_\mathfrak{q} (a_1, b_1 - b_1 a_1) = (a_1, b_1 q)$ so $\left[\frac{b}{a}\right] = \left[\frac{b_1 q}{a_1}\right]$ lies in a homomorphic image of $U(A/a_1A)$. Consequently C has no elements of order p^{n+1}. Letting p range now over all rational primes we conclude from this and (i) that C has exponent m, i.e. $x^m = 1$ for all $x \in C$. It follows easily from this and (i) that:

(ii) C is a cyclic group of order dividing m.

Again write $m = p^n m'$ as above. Suppose $(a, b) \sim_\mathfrak{q} (a_1, c^{p^n} q)$ for some $q \in \mathfrak{q}$ with $a_1 \equiv 1 \bmod q$ and $c \in A$. Then $\left[\frac{b}{a}\right] = \left[\frac{c^{p^n} q}{a_1}\right] = \left[\frac{cq}{a_1}\right]^{p^n}$, so it follows from (ii) that $\left[\frac{b}{a}\right]$ has order prime to p. If A is not totally imaginary then we can invoke Theorem 3.5 and apply this remark, for every p, and conclude:

(iii) $C = \{1\}$ if A is not totally imaginary.

Now suppose that A is totally imaginary. Since [ ] was chosen universal, and since $(-)_r$ is a Mennicke symbol on W_q (Remark 2 above) there is a homomorphism $f: C \to \mu_r$ rendering

$$\begin{array}{ccc} & [\,] \nearrow & C \\ W_q & & \downarrow f \\ & (-)_r \searrow & \mu_r \end{array}$$

commutative. Clearly f is surjective, so if we show that $[C : 1] \leq r$ the theorem will be proved. It suffices to do this on the p-primary components C_p for each prime p. Writing $m = p^n m'$ and $r = p^j r'$, with m' and r' prime to p, and $j = j_p(q)$, the passage to p-primary components can be achieved by replacing m by p^n, r by p^j, and C by C_p. Then if $\begin{bmatrix} b \\ a \end{bmatrix} \in C_p \cap \ker f$ we have $\left(\frac{b}{a}\right)_{p^j} = 1$, so it follows from Theorem 3.5 that $(a, b) \sim_q (a_1, c^{p^n} q)$. As above, we see that $\begin{bmatrix} b \\ a \end{bmatrix} = 1$ since it is a p^n-th power in the group C_p which has exponent p^n, according to (ii). Q.E.D.

The next theorem is required to handle some technical problems that arise in connection with the symplectic groups where we obtain a symbol $\{\ \}$ for which we cannot directly verify all the axioms for a Mennicke symbol.

Theorem 3.7. — Suppose we have a commutative diagram

$$\begin{array}{ccc} & \{\,\} \nearrow & D \\ W_q & & \downarrow f \\ & [\,]_q \searrow & C_q \end{array}$$

where

a) *f is a homomorphism of abelian groups,*

b) *$[\,]_q$ is a universal Mennicke symbol on W_q, and*

c) *$\{\,\}$ is a surjective map.*

Let $\begin{bmatrix} b \\ a \end{bmatrix}$ be $\begin{Bmatrix} b^2 \\ a \end{Bmatrix}$, and make the following assumptions:

(i) *$(a, b) \mapsto \begin{Bmatrix} b \\ a \end{Bmatrix}$ and $(a, b) \mapsto \begin{bmatrix} b \\ a \end{bmatrix}$ satisfy* MS 1, *and*

(ii) *if $(a, b_1), (a, b_2) \in W_q$, then*

$$\begin{Bmatrix} b_1 \\ a \end{Bmatrix} \begin{bmatrix} b_2 \\ a \end{bmatrix} = \begin{Bmatrix} b_1 b_2^2 \\ a \end{Bmatrix}.$$

Then f is an isomorphism, so $\{\,\}$ is a universal Mennicke symbol on W_q.

Proof. — Evidently *c)* (i) and *c)* (ii) imply that [ ] satisfies MS 1 and MS 2, so [ ] is a Mennicke symbol on W_q. Therefore its image is a cyclic subgroup, D′, of D, whose order divides m (the same m as in Theorem 3.6).

If A is not totally imaginary, and if $\mathrm{char}(k)\neq 2$, then we can apply Theorem 3.5 to any $(a, b)\in W_{\mathfrak{q}}$ to find an $(a_1, c^2q)\sim_{\mathfrak{q}}(a, b)$ with $q\in\mathfrak{q}$, $a_1\equiv 1 \bmod q$, and $c\in A$. (We take $p=2$ in Theorem 3.5). Since $(a_1, q)\sim_{\mathfrak{q}}(1, 0)$ we conclude, using *c)* (i) and *c)* (ii), that

$$\left\{\frac{b}{a}\right\}=\left\{\frac{c^2q}{a_1}\right\}=\left\{\frac{c^2q}{a_1}\right\}\left[\frac{q}{a_1}\right]=\left\{\frac{(cq)^2q}{a_1}\right\}=\left\{\frac{q}{a_1}\right\}\left[\frac{cq}{a_1}\right]=\left[\frac{cq}{a_1}\right]\in D'.$$

If $\mathrm{char}(k)=2$ we find $(a_1, b_1q)\sim_{\mathfrak{q}}(a, b)$ with $q\in\mathfrak{q}$, $a_1\equiv 1 \bmod q$, and a_1A prime, using the Dirichlet Theorem. A/a_1A is then a finite field of characteristic 2 so $b_1\equiv c^2 \bmod a_1$ for some c, and we can argue again as above. Thus, if A is not totally imaginary then we have $D=D'$, and, by Theorem 3.6, $D'=\{1\}$.

Now assume that A is totally imaginary. Then we can realize $[\ ]_{\mathfrak{q}}$ by $(-)_r : W_{\mathfrak{q}}\to\mu_r$, as in Theorem 3.6. We want to show that the (surjective) homomorphism $f : D\to\mu_r$ is an isomorphism, and we shall do this by showing that $[D : 1]\leq r$. We know $[D' : 1]\,|\,r$.

Write $m=2^nm'$ with m' odd. If r is odd, i.e. if $j_2(\mathfrak{q})=0$, then we always have the hypotheses of Theorem 3.5, and we can argue as above to prove that $D=D'$.

Henceforth, therefore, we can assume r is even. We claim that $[D' : 1]\,|\,\frac{r}{2}$. To see this we first note that, since $[\ ] : W_{\mathfrak{q}}\to D'$ is a Mennicke symbol, there is a necessarily surjective homomorphism $g : \mu_r\to D'$ such that

$$\left\{\frac{b^2}{a}\right\}=\left[\frac{b}{a}\right]=g\left(\frac{b}{a}\right)_r.$$

We want to show that $g(-1)=1$. If $-1=\left(\frac{b}{a}\right)_r$ then $\left(\frac{b^2}{a}\right)_r=1$, so we have $\left(\frac{b^2}{a}\right)_{2^j}=1$, $j=j_2(\mathfrak{q})$. Hence we can apply Theorem 3.5 and find an $(a_1, c^{2^n}q)\sim_{\mathfrak{q}}(a, b^2)$ with $q\in\mathfrak{q}$, $a_1\equiv 1 \bmod q$, $c\in A$. Then we have

$$\begin{aligned}
g(-1)&=\left\{\frac{b^2}{a}\right\}=\left\{\frac{c^{2^n}q}{a_1}\right\}\left[\frac{q}{a_1}\right]\\
&=\left\{\frac{(c^{2^{n-1}}q)^2q}{a_1}\right\} \qquad \text{(using } c) \text{ (ii))}\\
&=\left[\frac{c^{2^{n-1}}q}{a_1}\right]\left\{\frac{q}{a_1}\right\} \qquad \text{(using } c) \text{ (ii))}\\
&=\left[\frac{cq}{a_1}\right]^{2^{n-1}}\in(D')^{2^{n-1}}.
\end{aligned}$$

If $j<n$ this implies $g(-1)=1$. Now suppose $j=n$, i.e. that $2^n\,|\,r$. We can use Theorem 3.2 to find an $a\equiv 1 \bmod \mathfrak{q}$ such that $aA=\mathfrak{p}_1\mathfrak{p}_2$ where the $\mathfrak{p}_i$ are distinct odd primes such that $N_i=\mathbf{N}\mathfrak{p}_i\not\equiv 1 \bmod 2^{n+1}$, $i=1, 2$. Choose a $b\in\mathfrak{q}$ such that $b\equiv -1 \bmod \mathfrak{p}_1$ and $b\equiv 1 \bmod \mathfrak{p}_2$. Then $b^2\equiv 1 \bmod a$, and we have

$\left(\frac{b}{a}\right)_r = \left(\frac{-1}{\mathfrak{p}_1}\right)_r \left(\frac{1}{\mathfrak{p}_2}\right)_r = (-1)^{(N_1-1)/r}$. Since $2^n | r$ and since $2^{n+1} \nmid N_1 - 1$, it follows that $(N_1-1)/r$ is odd, so $\left(\frac{b}{a}\right)_r = -1$. Setting $q = 1-a$ we have

$$(a, b^2) \sim_{\mathfrak{q}} (a, b^2 - b^2 a) = (a, b^2 q) \sim_{\mathfrak{q}} (a, q) \sim_{\mathfrak{q}} (1, 0),$$

so $\left\{\frac{b^2}{a}\right\} = 1$. Therefore $g(-1) = g\left(\frac{b}{a}\right)_r = \left\{\frac{b^2}{a}\right\} = 1$, as claimed. This completes the proof that $[D' : 1] \mid \frac{r}{2}$ when r is even.

The proof of the theorem will be concluded now by showing that $[D : D'] \leq 2$. (Note that, at this point, we have not even shown that D is finite). For since we have just shown that $[D' : 1] \mid \frac{r}{2}$ it will follow that $[D : 1] \leq r$, as we were required to show.

Given any $(a_1, b_1), \ldots, (a_n, b_n) \in W_{\mathfrak{q}}$ we can use Lemmas 2.3 and 2.4 to choose $q \in \mathfrak{q}$ and $(a, c_i q) \in W_q$, such that $(a_i, b_i) \sim_{\mathfrak{q}} (a, c_i q)$, $1 \leq i \leq n$. We can further arrange that the c_i are non-zero, and then, by varying a mod $c_1 \ldots c_n q$, arrange that aA is a prime ideal. Let U be the finite cyclic group U(A/aA). Then we have the map defined in (2.8),

$$h : U \to D,$$

defined by $b \mapsto \left\{\frac{bq}{a}\right\}$ for $b \in A$ and prime to a, and the image of h contains each of the given elements $\left\{\frac{b_1}{a_1}\right\}, \ldots, \left\{\frac{b_n}{a_n}\right\}$. From *c)* (ii) we have the functional equation,

$$h(u^2 v) = h(u^2) h(v) \qquad \text{for } u, v \in U.$$

Let $H = h(U^2) \subset D'$, and let b generate U. Then $U = U^2 \cup bU^2$ so

$$h(U) = H \cup h(b) H \subset D' \cup h(b) D'.$$

In conclusion, this discussion shows that any finite set of symbols $\left\{\frac{b_1}{a_1}\right\}, \ldots, \left\{\frac{b_n}{a_n}\right\}$ lie in the union of D' and of one of its cosets in D. Finally, since $\{\} : W_{\mathfrak{q}} \to D$ is surjective, by hypothesis, it follows immediately that $[D : D'] \leq 2$. Q.E.D.

We shall conclude this chapter now by describing the functoriality of the isomorphism in Theorem 3.6.

Let A be the ring of integers in a totally imaginary number field k. Then Theorem 3.6 supplies an isomorphism

$$\varprojlim_{\mathfrak{q}} C_{\mathfrak{q}} \cong \mu_k, \tag{3.8}$$

where μ_k denotes the group of roots of unity in k, and where the limit is taken over all non zero ideals $\mathfrak{q}$ of A. In fact, if $m = [\mu_k : 1]$, the limit is already reached by any $\mathfrak{q}$ divisible by $m \cdot \prod_{p \mid m} \mathfrak{p}^{1/(p-1)}$, and *a fortiori* by any $\mathfrak{q}$ divisible by m^2. (k contains a primitive p-th root of unity, w_p, and $1 - w_p$ generates the ideal whose $(p-1)$-st power is (p). The symbol $\mathfrak{p}^{1/(1-p)}$ above denotes this ideal.)

Let k_1 be an extension of k of degree $d=[k_1:k]$, and with integers A_1. If $\mathfrak{q}$ is an ideal of A then the inclusion $W_{\mathfrak{q}} \subset W_{\mathfrak{q}A_1}$ induces a homomorphism $C_{\mathfrak{q}} \to C_{\mathfrak{q}A_1}$. The ideals $\mathfrak{q}A_1$ are cofinal in A_1, so, passing to the limit, (3.8) induces a homomorphism

$$\varphi : \mu_k \to \mu_{k_1}.$$

The nature of the identification (3.8) shows that φ is characterized by the fact that, for $\mathfrak{q}$ highly divisible by $m_1=[\mu_{k_1}:1]$, and for any $(a,b)\in W_{\mathfrak{q}}$,

$$\varphi\left({}_k\left(\frac{b}{a}\right)_m\right) = {}_{k_1}\left(\frac{b}{a}\right)_{m_1}.$$

The left subscripts here designate the fields to which the symbols apply.

This φ has been determined in (A.23); it is defined by the formula:

$$\varphi(\zeta)=\zeta^e, \qquad \text{where } e=\left(1+\frac{m}{2}+\frac{m_1}{2}\right)\frac{dm}{m_1}. \tag{3.9}$$

APPENDIX ON NUMBER THEORY

This appendix presents, in a form convenient for our applications in § 3, the statements of several fundamental theorems from algebraic number theory. Most of the statements are simply given with a reference to the literature from which they are drawn. In other cases we have deduced certain " well known " corollaries from the latter. The following references will be used:

[AT] E. Artin and J. Tate, *Class Field Theory*, Harvard notes (1961).

[H] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II Teil, *Jahr. Deut. Math. Ver.*, Erg. VI Band, Teubner, 1930.

[L] S. Lang, *Algebraic Numbers*, Addison Wesley (1964).

[O'M] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer (1963).

[S] J.-P. Serre, *Corps Locaux*, Hermann (1962).

Let k be a global field, i.e. a finite number field or a function field in one variable over a finite field. If $\mathfrak{p}$ is a prime (or place) of k then there is a normalized absolute value, $|\ |_{\mathfrak{p}}$, on the local field $k_{\mathfrak{p}}$ at $\mathfrak{p}$. (See [L, p. 24] where it is denoted $\|\ \|_{\mathfrak{p}}$.) If $\mathfrak{p}$ is finite then the residue class field $k(\mathfrak{p})$ is finite with $\mathbf{N}\mathfrak{p}$ elements, and $|x|_{\mathfrak{p}}=\mathbf{N}\mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(x)}$. If k is a function field with constant field $\mathbf{F}_q$ then $\mathbf{N}\mathfrak{p}=q^{\deg(\mathfrak{p})}$, where $\deg(\mathfrak{p})=[k(\mathfrak{p}):\mathbf{F}_q]$.

For finite $\mathfrak{p}$ write $U_{\mathfrak{p}}$ for the group of local units at $\mathfrak{p}$, and

$$U_{\mathfrak{p}}(n)=\{u\in U_{\mathfrak{p}} \mid \mathrm{ord}_{\mathfrak{p}}(1-u)\geq n\}$$

Thus $U_{\mathfrak{p}}(0)=U_{\mathfrak{p}}$ and $U_{\mathfrak{p}}(n)=1+\mathfrak{p}^n$ for $n>0$. The group $U_{\mathfrak{p}}(n)$ is an open subgroup of finite index in $U_{\mathfrak{p}}$. If $\mathfrak{p}$ is infinite we can set $U_{\mathfrak{p}}=k_{\mathfrak{p}}^*$, the multiplicative group of $k_{\mathfrak{p}}$.

Let J be the idèle group of k (see [L, Ch. VI] or [O'M, Ch. III]). J has a topo-

logy making it a locally compact group and inducing the product topology on the open subgroup $\prod_{\mathfrak{p}} U_{\mathfrak{p}}$. The group k^* is embedded diagonally as a discrete subgroup of J.

If $x=(x_{\mathfrak{p}})$ is an idèle then $|x_{\mathfrak{p}}|_{\mathfrak{p}}=1$ for almost all $\mathfrak{p}$. Let $||x||=\prod_{\mathfrak{p}}|x_{\mathfrak{p}}|_{\mathfrak{p}}$. The map $||\ ||: J\to \mathbf{R}^*$ is a continuous homomorphism whose kernel we denote by J^0. It is clear from the definitions that

$$(A.1) \qquad J/J^0 \cong \begin{cases} \mathbf{R} & \text{if } k \text{ is a number field.} \\ \mathbf{Z} & \text{if } k \text{ is a function field.} \end{cases}$$

(A.2) *Product Formula* (See [L, Ch. V] or [O'M, § 33 B]).

$$k^* \subset J^0.$$

I.e. $\prod_{\mathfrak{p}}|x|_{\mathfrak{p}}=1$ for $x\in k^*$.

In function fields this is usually written additively:

(A.3) *If k is a function field and if $x\in k^*$ then*

$$\sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(x)\deg(\mathfrak{p})=0.$$

Write $C=J/k^*$, the group of *idèle classes*, and $C^0=J^0/k^*$.

(A.4) *Class Number-Unit Theorem* (See [L, Ch. VI, Theorem 4]).

C^0 *is compact.*

Let $\mathfrak{p}_0$ be a finite prime. An idèle $t=(t_{\mathfrak{p}})$ is called *prime at* $\mathfrak{p}_0$ if $t_{\mathfrak{p}}=1$ for $\mathfrak{p}\neq\mathfrak{p}_0$, and if $t_{\mathfrak{p}_0}$ is a local parameter (i.e. generates the maximal ideal) at $\mathfrak{p}_0$.

(A.5) *Artin Reciprocity and Existence Theorem.* (See [AT, Ch. 8, § 1]). *Let K/k be a finite abelian extension. Then there is a continuous epimorphism $r: C\to \mathrm{Gal}(K/k)$ such that, if $\mathfrak{p}$ is a finite prime of k, unramified in K, and if t is a prime idèle at $\mathfrak{p}$, then $r(t.k^*)=(\mathfrak{p}, K/k)$, the Artin symbol. Every open subgroup of finite index in C is the kernel of r for a suitable (and uniquely determined) K.*

For the Artin symbol see, e.g., [S, Ch. I, § 8].

(A.6) " *Čebotarev Theorem for abelian extensions* ". (See [H], § 24). *Let K/k be a finite abelian extension; given $\sigma\in\mathrm{Gal}(K/k)$ there are infinitely many primes $\mathfrak{p}$ of k, unramified in K, such that $(\mathfrak{p}, K/k)=\sigma$.* (See also A. Weil, *Basic number theory*, p. 289.)

In view of (A.5) we see that this Čebotarev Theorem is equivalent to the:

(A.7) *Density Theorem.*

If U is an open subgroup of finite index in C then every coset of C/U contains infinitely many prime idèle classes.

(A.8) *Corollary. — Let ζ be a primitive m-th root of unity and suppose that $\zeta\notin k$. Then there exist infinitely many primes ζ such that $\mathbf{N}\mathfrak{p}\equiv 1 \bmod m$. If $k(\zeta)/k$ is cyclic we can even arrange that $k(\mathfrak{p})$ contains no more m-th roots of unity than k does.*

Proof. — Choose $\sigma\neq 1$ in $\mathrm{Gal}(k(\zeta)/k)$, a generator in the cyclic case. By the Čebotarev Theorem there are infinitely many primes $\mathfrak{p}$, prime to m in the number field case, and hence unramified in $k(\zeta)$, such that $(\mathfrak{p}, k(\zeta)/k)=\sigma$. Thus the Frobenius

automorphism in the extension $k(\mathfrak{p})(\zeta)/k(\mathfrak{p})$ is not trivial, so $\zeta \notin k(\mathfrak{p})$. (We identify ζ with its image modulo $\mathfrak{p}$.)

In the cyclic case we even have $[k(\mathfrak{p})(\zeta) : k(\mathfrak{p})] = \text{order of } \sigma$. Suppose $\zeta^i \in k(\mathfrak{p})$. Then, by Hensel's lemma, $\zeta^i \in k_\mathfrak{p}$, so $[k_\mathfrak{p}(\zeta) : k_\mathfrak{p}]$ is dominated by $[k(\zeta) : k(\zeta^i)]$. The inequalities

$$[k(\zeta) : k] = [k(\mathfrak{p})(\zeta) : k(\mathfrak{p})] \leq [k_\mathfrak{p}(\zeta) : k_\mathfrak{p}] \leq [k(\zeta) : k(\zeta^i)]$$

now imply that $\zeta^i \in k$.

(A.9) *Corollary.* — *If k is a function field then, given $n > 1$, there are infinitely many primes $\mathfrak{p}$ of degree prime to n.*

For if $\mathbf{F}_q$ is the constant field of k we can take $m = q^n - 1$ in the corollary above. The extension $k(\zeta)/k$ is certainly cyclic, and it is easy to see that a finite extension of $\mathbf{F}_q$ having only $q-1$ m-th roots of unity must have degree prime to n.

Let S_∞ be a finite, non empty, set of primes of k, containing all archimedean primes when k is a number field, and let

$$A = \{x \in k \mid \mathrm{ord}_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S_\infty\}.$$

A is called the *Dedekind ring of arithmetic type* defined by the set S_∞ of primes in k. (A is a " Hasse domain " in the terminology of O'Meara.) A is, indeed, a Dedekind domain, and we can canonically identify the maximal ideals of A with the primes outside S_∞. With this convention we have $k(\mathfrak{p}) = A/\mathfrak{p}$ for $\mathfrak{p} \notin S_\infty$. If A′ is defined by $S'_\infty \supset S_\infty$ then it follows easily from the finiteness of class number that A′ is a ring of fractions of A; in fact $A' = A[a^{-1}]$ for a suitable $a \in A$.

(A.10) *Dirichlet Theorem.* — *Suppose we are given: non zero $a, b \in A$ such that $aA + bA = A$; a finite set S_0 of primes outside S_∞ and prime to b; for each $\mathfrak{p} \in S_0 \cup S_\infty$ an open subgroup $V_\mathfrak{p} \subset k_\mathfrak{p}^*$ and an $x_\mathfrak{p} \in k_\mathfrak{p}^*$ such that, for $\mathfrak{p} \in S_0$, $e_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(x_\mathfrak{p}) \geq 0$. Suppoxe also that, for at least one $\mathfrak{p} \in S_\infty$, $V_\mathfrak{p}$ has finite index in $k_\mathfrak{p}^*$.*

Then there exist infinitely many primes $\mathfrak{p}_0 \notin S_0 \cup S_\infty$ such that there is a $c \in A$ satisfying

$$c \equiv a \bmod bA$$

$$c \in x_\mathfrak{p} V_\mathfrak{p} \text{ for all } \mathfrak{p} \in S_0 \cup S_\infty$$

and

$$cA = \mathfrak{p}_0 \mathfrak{a}$$

where

$$\mathfrak{a} = \prod_{\mathfrak{p} \in S_0} \mathfrak{p}^{e_\mathfrak{p}}.$$

Proof. — For $\mathfrak{p} \in S_0$ we can, by making the $V_\mathfrak{p}$ smaller, if necessary, assume $V_\mathfrak{p} \subset U_\mathfrak{p}$. For $\mathfrak{p} \notin S_0 \cup S_\infty$ define

$$V_\mathfrak{p} = U_\mathfrak{p}(\mathrm{ord}_\mathfrak{p}(b)) = \{u \in U_\mathfrak{p} \mid \mathrm{ord}_\mathfrak{p}(1-u) \geq \mathrm{ord}_\mathfrak{p}(b)\}.$$

Then $V_\mathfrak{p} = U_\mathfrak{p}$ for almost all $\mathfrak{p}$, so $V = \prod_\mathfrak{p} V_\mathfrak{p}$ is an open subgroup of J. Therefore $W = Vk^*/k^*$ is an open subgroup of $C = J/k^*$, so C/W is discrete. To show that it is finite we need only observe that it is compact. Since C^0 is compact (see (A.4)) it suffices to show that $C/C^0.W = ||C||/||W||$ is finite. Since $||C|| \cong \mathbf{R}$ or $\mathbf{Z}$ (see (A.1))

and since $||W||$ is an open subgroup, it suffices to observe that $||W|| \neq \{1\}$. But this follows immediately from the fact that $V_\mathfrak{p}$ has finite index in $k_\mathfrak{p}^*$ for some $\mathfrak{p} \in S_\infty$.

Now it follows from the Density Theorem that each coset of $J/V \cdot k^*$ contains infinitely many prime idèles. To apply this we first construct some idèles from the data of the theorem. Write S_b for the set of primes dividing b, and define idèles $\bar{a}$ and $\bar{x}$ by:

$$\bar{a}: \quad \bar{a}_\mathfrak{p} = \begin{cases} a \text{ if } \mathfrak{p} \in S_b \\ 1 \text{ if } \mathfrak{p} \notin S_b \end{cases}$$

$$\bar{x}: \quad \bar{x}_\mathfrak{p} = \begin{cases} x_\mathfrak{p} \text{ if } \mathfrak{p} \in S_0 \cup S_\infty \\ 1 \quad \text{otherwise} \end{cases}$$

Now the Density Theorem gives us infinitely many primes $\mathfrak{p}_0 \notin S_b \cup S_\infty$ such that there is a prime idèle r at $\mathfrak{p}_0$ satisfying $r \equiv \bar{a}\,\bar{x}^{-1} \bmod Vk^*$. Thus we can find $d \in k^*$ and $v \in V$ such that

$$(*) \qquad r\bar{x}v = \bar{a}d$$

We claim that $\mathfrak{p}_0$ and $c = ad$ satisfy the conclusions of the theorem. To verify this we study the equation $(*)$ at each $\mathfrak{p}$.

$$\begin{array}{lll} \mathfrak{p} \notin \{\mathfrak{p}_0\} \cup S_b \cup S_0 \cup S_\infty: & v_\mathfrak{p} = ad, & \text{so } \operatorname{ord}_\mathfrak{p}(c) = 0 \\ \mathfrak{p} = \mathfrak{p}_0: & r_{\mathfrak{p}_0} v_{\mathfrak{p}_0} = ad, & \text{so } \operatorname{ord}_{\mathfrak{p}_0}(c) = 1 \\ \mathfrak{p} \in S_0: & x_\mathfrak{p} v_\mathfrak{p} = ad, & \text{so } cx_\mathfrak{p}^{-1} \in V_\mathfrak{p} \subset U_\mathfrak{p} \end{array}$$

and, in particular, $\operatorname{ord}_\mathfrak{p}(c) = \operatorname{ord}_\mathfrak{p}(x_\mathfrak{p}) = e_\mathfrak{p}$.

$$\mathfrak{p} \in S_b: \qquad v_\mathfrak{p} = d \qquad \text{so } d \in V_\mathfrak{p} = U_\mathfrak{p}(\operatorname{ord}_\mathfrak{p}(b))$$

and therefore $c = ad \equiv a \bmod \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(b)}$.

These conclusions already show that $c \in A$, that $c \equiv a \bmod bA$, and that $cA = \mathfrak{p}_0 \mathfrak{a}$, as well as that $cx_\mathfrak{p}^{-1} \in V_\mathfrak{p}$ for $\mathfrak{p} \in S_0$. There remains only the condition at S_∞.

$$\mathfrak{p} \in S_\infty: \qquad x_\mathfrak{p} v_\mathfrak{p} = ad, \qquad \text{so } cx_\mathfrak{p}^{-1} \in V_\mathfrak{p}. \qquad \text{Q.E.D.}$$

The following special cases of this theorem suffice for most applications.

(A.11) *Suppose k is a number field. Given non zero $a, b \in A$ and a non zero ideal $\mathfrak{a}$ such that $aA + bA = A = \mathfrak{a} + bA$, then there are infinitely many primes $\mathfrak{p}_0 \notin S_\infty$ such that $\mathfrak{p}_0 \mathfrak{a} = cA$ for some $c \equiv a \bmod bA$, and we can prescribe the signs of c at the real primes.*

We take $V_\mathfrak{p}$ = the positive reals, at real $\mathfrak{p}$, to obtain the last condition.

(A.12) *Suppose k is a function field, and that we are given a, b and $\mathfrak{a}$ as in* (A.11) *above. Suppose also given, for each $\mathfrak{p} \in S_\infty$, integers $n_\mathfrak{p} > 0$ and $m_\mathfrak{p}$. Then we have the same conclusion as above, where the condition at real primes is replaced by:*

$$\operatorname{ord}_\mathfrak{p}(c) \equiv m_\mathfrak{p} \bmod n_\mathfrak{p}\mathbf{Z}$$

for all $\mathfrak{p} \in S_\infty$.

Here we take for $V_\mathfrak{p}$, $\mathfrak{p} \in S_\infty$, the set of $x \in k^*$ such that $\operatorname{ord}_\mathfrak{p}(x) \equiv 0 \bmod n_\mathfrak{p}$.

We shall now give a description of the power reciprocity laws, following [AT, Ch. 12] and [S, Ch. XIV].

We fix an integer $m \geq 1$ and we shall be discussing fields k which contain the group, μ_m, of all m-th roots of unity. This will always be understood to imply that $\mathrm{char}(k) \nmid m$, so that μ_m is cyclic of order m.

First suppose k is a *local field*, i.e. a local completion of some global field, and assume $\mu_m \subset k$. If k_a is the maximal abelian extension of k, then there is a *reciprocity map*, which is a continuous homomorphism

$$k^* \to \mathrm{Gal}(k_a/k)$$
$$a \to (a, k_a/k),$$

(See [S, Ch. XI, § 3]). For example, in the non-archimedean case, the restriction of $(a, k_a/k)$ to the unramified part is the Artin symbol, i.e. the $\mathrm{ord}(a)$ power of the lifting of the Frobenius automorphism. If $a, b \in k^*$ then, since $\mu_m \subset k$, $k(a^{1/m})/k$, is an abelian extension on which $\sigma = (b, k_a/k)$ operates, so we can define

$$\left(\frac{a, b}{k}\right)_m = \frac{\sigma a^{1/m}}{a^{1/m}} \in \mu_m$$

and it is easy to see that this is independent of the choice of $a^{1/m}$. (In case our field is $k_\mathfrak{p}$, where k now denotes some global field, then we shall write $\left(\frac{a, b}{\mathfrak{p}}\right)_m$ instead.) This definition agrees with those of [H] and [S], and is reciprocal to that of [A-T].

(A.13) $$\left(\frac{\ ,\ }{k}\right)_m : k^* \times k^* \to \mu_m$$

factors through $(k^*/k^{*m}) \times (k^*/k^{*m})$, *on which it defines a non-degenerate, antisymmetric, bilinear form. Moreover,*

$$\left(\frac{a, 1-a}{k}\right)_m = 1 \qquad \textit{whenever } a, 1-a \in k^*$$

and, if $n \mid m$,

$$\left(\left(\frac{a, b}{k}\right)_m\right)^n = \left(\frac{a, b}{k}\right)_{m/n}.$$

This result and (A.16) below summarize the results of [S, Ch. XIV, §§ 1-3] and of [AT, Ch. 12, § 1].

We shall now discuss the evaluation of these symbols. In the archimedean case the symbol is uniquely characterized by (A.13):

(A.14) *If* $k \cong \mathbf{C}$ *then* $k^* = k^{*m}$ *so* $\left(\frac{a, b}{\mathbf{C}}\right)_m = 1$ *for all* a *and* b.

(A.15) *If* $k \cong \mathbf{R}$ *then* $m \leq 2$ *and we have*

$$\left(\frac{a, b}{\mathbf{R}}\right)_2 = \begin{cases} -1 & \text{if } a, b < 0 \\ 1 & \text{otherwise} \end{cases}.$$

Suppose next that k is non archimedean, with prime $\mathfrak{p}$ and suppose $\mathbf{N}\mathfrak{p} = q$ is prime to m. Since $\mu_m \subset k$ we have $q \equiv 1 \bmod m$. Therefore, if $a \in U_\mathfrak{p}$, $a^{\frac{q-1}{m}}$ becomes an m-th root of unity mod $\mathfrak{p}$, so there is a unique element $\left(\frac{a}{\mathfrak{p}}\right)_m \in \mu_m$ such that

$$a^{\frac{q-1}{m}} \equiv \left(\frac{a}{\mathfrak{p}}\right)_m \bmod \mathfrak{p}.$$

This is called the m-th *power residue symbol* at $\mathfrak{p}$.

(A.16) (See [S, p. 217]). *Suppose k is non archimedean with prime $\mathfrak{p}$ and residue characteristic prime to m. Then for $a \in U_\mathfrak{p}$ and $b \in k_\mathfrak{p}^*$*

$$\left(\frac{a, b}{\mathfrak{p}}\right)_m = \left(\frac{a}{\mathfrak{p}}\right)_m^{\mathrm{ord}_\mathfrak{p}(b)}$$

Thus $\left(\frac{a, b}{\mathfrak{p}}\right)_m = 1$ if b is also a unit. Note that when $\mathrm{char}\, k > 0$ we are automatically in the case covered by (A.16). It remains to discuss the much more complicated case when the residue characteristic divides m. The information we require in these cases is contained in the following two propositions.

k now denotes a finite extension of $\mathbf{Q}_p$, with prime $\mathfrak{p}$, and we suppose $m = p^n$. We shall write

$$e = \mathrm{ord}_\mathfrak{p}(p),$$

the absolute ramification index.

For $x \in \mathbf{R}$ write $[x]$ for the largest integer $\leq x$, and for $a \in \mathbf{Z}$ write $a_{[0,n]}$ for the nearest integer to a in the interval $[0, n]$.

(A.17) *Let h be a non negative integer. Then*

$$\left(\frac{U_\mathfrak{p}(h), U_\mathfrak{p}}{\mathfrak{p}}\right)_{p^n} = \left(\frac{U_\mathfrak{p}(h+1), k^*}{\mathfrak{p}}\right)_{p^n} = \mu_{p^{n-j}}$$

where

$$j = \left[\frac{h}{e} - \frac{1}{p-1}\right]_{[0,n]}.$$

(A.18) *If $a \in U_\mathfrak{p}(h)$ and if $\mathrm{ord}_\mathfrak{p}(b) \geq h$, then $\left(\frac{a, b}{\mathfrak{p}}\right)_{p^j}$ depends on a only modulo b, where j has the same meaning as in* (A.17); *it equals* 1 *if* $\mathrm{ord}_\mathfrak{p}(b) = h$.

Remark. — When $a \in U_\mathfrak{p}(h)$, $b \in k_\mathfrak{p}^*$, the value of $\left(\frac{a, b}{\mathfrak{p}}\right)_{p^j}$ may be given explicitly, as follows:

When $j=0$, this symbol is of course equal to 1.

When $j\geq 1$, let w be a primitive p-th root of unity, and let $\alpha=(a-1)/p^j(w-1)$. Since $a\in U_{\mathfrak{p}}(h)$, α is $\mathfrak{p}$-integral; let $\overline{\alpha}$ be its image in $k(\mathfrak{p})$, and let $S(\alpha)$ be the image of $\overline{\alpha}$ by the trace $\mathrm{Tr}: k(\mathfrak{p})\to \mathbf{F}_p$. With these notations, one has:

$$\left(\frac{a, b}{\mathfrak{p}}\right)_{p^j}=w^{-S(\alpha)\mathrm{ord}_{\mathfrak{p}}(b)}.$$

(If $j=1$ this is [S, Prop. 6, p. 237]. The general case is proved by induction on j, writing a as a p-th power.)

Proof of (A.17). — Write

$$\mu(h, n)=\left(\frac{U_{\mathfrak{p}}(h+1), k_{\mathfrak{p}}^*}{\mathfrak{p}}\right)_{p^n}$$

and

$$\mu'(h, n)=\left(\frac{U_{\mathfrak{p}}(h), U_{\mathfrak{p}}}{\mathfrak{p}}\right)_{p^n}$$

We shall reason by induction on n. Setting $j'=\left[\frac{h}{e}-\frac{1}{p-1}\right]$, j' is defined by the inequalities

$$e\left(j'+\frac{1}{p-1}\right)\leq h<e\left(j'+1+\frac{1}{p-1}\right),$$

and j is the nearest integer to j' in the interval $[0, n]$.

The case $n=1$. — Since the groups μ and μ' decrease as h increases it suffices to show that, for $h=e\left(1+\frac{1}{p-1}\right)=\frac{ep}{p-1}$ (which is an integer because $p^{n-1}(p-1)$ divides e),

$$\mu(h, 1)=\{1\}, \qquad \mu(h-1, 1)=\mu_p,$$
$$\mu'(h, 1)=\{1\}, \qquad \mu'(h-1, 1)=\mu_p.$$

If $x\in U_{\mathfrak{p}}(h)$ and $y\in k_{\mathfrak{p}}^*$ the evaluation of $\left(\frac{x, y}{\mathfrak{p}}\right)_p$ is made in [S, p. 237, Prop. 6]. From this one deduces the first three formulas

$$\left(\frac{U_{\mathfrak{p}}(h+1), k_{\mathfrak{p}}^*}{\mathfrak{p}}\right)_p=\{1\}=\left(\frac{U_{\mathfrak{p}}(h), U_{\mathfrak{p}}}{\mathfrak{p}}\right)_p, \text{ and } \left(\frac{U_{\mathfrak{p}}(h), k_{\mathfrak{p}}^*}{\mathfrak{p}}\right)_p=\mu_p.$$

The last formula, $\left(\frac{U_{\mathfrak{p}}(h-1), U_{\mathfrak{p}}}{\mathfrak{p}}\right)_p=\mu_p$ follows from the evaluation of the symbol given in [S, p. 237, Exercise 3]. Rather than appeal to an exercise we can argue directly, as follows. Take $x\in U_{\mathfrak{p}}(h-1)$, $x\notin U_{\mathfrak{p}}(h)$. If $\left(\frac{x, U_{\mathfrak{p}}}{\mathfrak{p}}\right)_p=\{1\}$, the reciprocity map $k^*\to \mathrm{Gal}(k(x^{1/p})/k)$ is trivial on $U_{\mathfrak{p}}$, and hence the extension $k(x^{1/p})/k$ is unra-

mified [S, p. 205, Cor. to Prop. 13]. Then ord_p on k agrees with ord on $k(x^{1/p})$. Writing $x^{1/p}=1+y$ we have

$$x=1+py\left(1+\frac{p-1}{2}y+\dots\right)+y^p$$

so
$$h-1=\frac{ep}{p-1}-1=e+\frac{e}{p-1}-1=\mathrm{ord}(x-1)$$
$$\geq\min(e+\mathrm{ord}(y),\, p\,\mathrm{ord}(y)),$$

with equality when these two numbers differ. Since $h-1$ is not a multiple of p, therefore, we cannot have $p\,\mathrm{ord}(y)<e+\mathrm{ord}(y)$, so $\mathrm{ord}(y)\geq\frac{e}{p-1}$, and $h-1\geq e+\mathrm{ord}(y)\geq e+\frac{e}{p-1}$; contradiction.

The case $n\geq 2$. — Let $\pi\colon \mu_{p^n}\to\mu_{p^{n-1}}$ be the p-th power map. Since

$$(*)\qquad \left(\frac{x,y}{\mathfrak{p}}\right)_{p^{n-1}}=\pi\left(\frac{x,y}{\mathfrak{p}}\right)_{p^n}=\left(\frac{x^p,y}{\mathfrak{p}}\right)_{p^n}$$

we see that $\mu(h,n-1)=\pi(\mu(h,n))$, and similarly for μ'.

(i) Suppose first that $j=\left[\frac{h}{e}-\frac{1}{p-1}\right]_{[0,n]}\leq n-2$. Then, by induction we have $\mu(h,n-1)=\mu_{p^{n-1-j}}\neq\{1\}$, and the only subgroup of μ_{p^n} having this image under π is $\mu_{p^{n-j}}$. Therefore this case follows from the remark above.

(ii) Suppose that $\left[\frac{h}{e}-\frac{1}{p-1}\right]\geq n-1$. The argument above shows now that $\pi(\mu(h,n))=\{1\}$, so $\mu(h,n)\subset\mu_p$, and similarly for μ'. As in the case $n=1$, it suffices to show that, if $h_n=e\left(n+\frac{1}{p-1}\right)$, then

$$\mu(h_n,n)=\{1\},\qquad \mu(h_n-1,n)=\mu_p,$$
$$\mu'(h_n,n)=\{1\},\qquad \mu'(h_n-1,n)=\mu_p.$$

Since $n\geq 2$ and since e is divisible by $(p-1)p^{n-1}\geq 2$ it follows that $h_n-1>e\left(1+\frac{1}{p-1}\right)$. Now it follows from [S, p. 219, Prop. 9] that, for $m>e\left(1+\frac{1}{p-1}\right)$, the p-th power map sends $U_{\mathfrak{p}}(m-e)$ isomorphically onto $U_{\mathfrak{p}}(m)$. Taking $m=h_n-1$, $m=h_n$, and $m=h_n+1$, and using the formula $(*)$ above, we obtain

$$\mu(h_n,n)=\mu(h_{n-1},n-1)$$
$$\mu'(h_n,n)=\mu'(h_{n-1},n-1)$$
$$\mu(h_n-1,n)=\mu(h_{n-1}-1,n-1)$$
$$\mu'(h_n-1,n)=\mu'(h_{n-1}-1,n-1)$$

The proof is now completed by the induction hypothesis.

Proof of (A.18). — Since $\left(\frac{a, b}{\mathfrak{p}}\right)_{pj} = \left(\left(\frac{a, b}{\mathfrak{p}}\right)_{p^n}\right)^{p^{n-j}}$ it follows from part (i) that

$$\left(\frac{U_{\mathfrak{p}}(h), U_{\mathfrak{p}}}{\mathfrak{p}}\right)_{pj} = \{1\} = \left(\frac{U_{\mathfrak{p}}(h+1), k_{\mathfrak{p}}^*}{\mathfrak{p}}\right)_{pj}.$$

This shows first that $\left(\frac{a, b}{\mathfrak{p}}\right)_{pj}$ depends only on the class of a mod $U_{\mathfrak{p}}(h+1)$, i.e. mod $\mathfrak{p}^{h+1}$.

Case $\mathrm{ord}_{\mathfrak{p}}(b) \geq h+1$. — It is then clear that $\left(\frac{a, b}{\mathfrak{p}}\right)_{pj}$ depends only on a mod b.

Case $\mathrm{ord}(b) = h$. — If $a \in U_{\mathfrak{p}}(h+1)$ we have $\left(\frac{a, b}{\mathfrak{p}}\right)_{pj} = 1$ by one of the formulae above. If $a \notin U_{\mathfrak{p}}(h+1)$, $\mathrm{ord}_{\mathfrak{p}}(1-a) = h$, and we have $b = (1-a)v$ with $v \in U_{\mathfrak{p}}$. Hence:

$$\left(\frac{a, b}{\mathfrak{p}}\right)_{pj} = \left(\frac{a, 1-a}{\mathfrak{p}}\right)_{pj}\left(\frac{a, v}{\mathfrak{p}}\right)_{pj}.$$

But $\left(\frac{a, 1-a}{\mathfrak{p}}\right)_{pj} = 1$ by (A.13), and $\left(\frac{a, v}{\mathfrak{p}}\right)_{pj} = 1$ by one of the formulae above. Hence $\left(\frac{a, b}{\mathfrak{p}}\right)_{pj} = 1$. Q.E.D.

Now let k be a *global* field containing μ_m.

(A.19) *m-th power reciprocity law: If* $a, b \in k^*$ *then* $\left(\frac{a, b}{\mathfrak{p}}\right)_m = 1$ *for almost all* $\mathfrak{p}$, *and*

$$\prod_{\mathfrak{p}} \left(\frac{a, b}{\mathfrak{p}}\right)_m = 1$$

The first assertion follows from (A.16), since a and b are both units at almost all finite $\mathfrak{p}$. The product formula is [AT, Ch. 12, Theorem 13].

Suppose that A is the ring of algebraic integers in a number field k. Let b be a non zero element of A, and let $\mathfrak{a}$ be an ideal of A prime to bm. The *m-th power residue symbol*, $\left(\frac{b}{\mathfrak{a}}\right)_m$, is defined by

$$\left(\frac{b}{\mathfrak{a}}\right)_m = \prod_{\mathfrak{p} \mid \mathfrak{a}} \left(\frac{b}{\mathfrak{p}}\right)_m^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}. \tag{A.20}$$

When $\mathfrak{a} = a\mathrm{A}$ we write simply $\left(\frac{b}{a}\right)_m$. This is evidently a bimultiplicative function on the pairs $(\mathfrak{a}, b)$ for which it is defined. According to (A.16) we can write $\left(\frac{b}{\mathfrak{p}}\right)_m^{\mathrm{ord}_{\mathfrak{p}}(a)} = \left(\frac{b, a}{\mathfrak{p}}\right)_m$ so the reciprocity law, and the antisymmetry of the local symbols, gives us

$$\left(\frac{b}{a}\right)_m = \prod_{\mathfrak{p} \nmid a} \left(\frac{a, b}{\mathfrak{p}}\right)_m. \tag{A.21}$$

If $\mathfrak{p} \nmid mab\infty$ then (A.16) implies $\left(\frac{a, b}{\mathfrak{p}}\right)_m = 1$. Therefore we can rewrite (A.21), using (A.16), as:

$$\left(\frac{b}{a}\right)_m = \prod_{\substack{\mathfrak{p}\mid b \\ \mathfrak{p}\nmid m}} \left(\frac{a}{\mathfrak{p}}\right)_m^{\mathrm{ord}_{\mathfrak{p}}(b)} \cdot \prod_{\mathfrak{p}\mid m} \left(\frac{a, b}{\mathfrak{p}}\right)_m \cdot \prod_{\mathfrak{p}\mid \infty} \left(\frac{a, b}{\mathfrak{p}}\right)_m \tag{A.21}$$

Note that the third factor disappears if k is totally imaginary; if $(b, m)=1$ the first factor is just $\left(\frac{a}{b}\right)_m$.

The following fact from Artin-Tate [AT, Ch. 12, Theorem 8] is used in the proof of Proposition 4.15. It can also be deduced from the remark following (A.18).

(A.22) *Let p be an odd prime, let $k=\mathbf{Q}(\zeta)$ with ζ a primitive p-th root of unity, and let $\lambda=1-\zeta$. Then* $\left(\frac{1-\lambda^p, \lambda}{(\lambda)}\right)_p \neq 1$.

We shall now discuss a functorial property of the power residue symbols. Changing notation slightly we shall write μ_k for the group of all roots of unity in a number field k.

(A.23) *Let $k \subset k_1$ be an extension of number fields of degree $d=[k_1 : k]$, and write $m=[\mu_k : 1]$ and $m_1=[\mu_{k_1} : 1]$ for the orders of their groups of roots of unity.*

a) *There is a unique homomorphism $\varphi=\varphi_{k_1/k} : \mu_k \to \mu_k$ making the triangle*

$$\begin{array}{ccc} & \mu_{k_1} & \\ {\scriptstyle m_1/m}\swarrow & & \searrow{\scriptstyle N_{k_1/k}} \\ \mu_k & \xrightarrow[\varphi]{} & \mu_k \end{array}$$

commutative, and, if $k_1 \subset k_2$, $\varphi_{k_2/k}=\varphi_{k_2/k_1} \circ \varphi_{k_1/k}$.

b) $\varphi(\zeta)=\zeta^e$, *where* $e=\left(1+\frac{m}{2}+\frac{m_1}{2}\right) dm/m_1$.

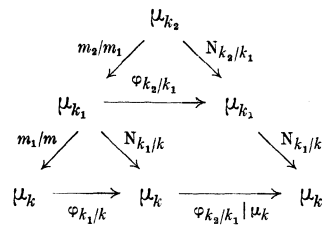
This makes sense because dm/m_1 has denominator prime to m.

c) *Let b be an algebraic integer of k, and let $\mathfrak{a}$ be an ideal of k which is prime to $m_1 b$; identify $\mathfrak{a}$ with the corresponding ideal of k_1. Then*

$$\left(\frac{b}{\mathfrak{a}}\right)_{m_1} = \varphi\left(\left(\frac{b}{\mathfrak{a}}\right)_m\right),$$

where the left subscript denotes the field in which the symbol is defined.

Proof. — a) The existence and uniqueness of φ follows because $\mu_{k_1} \xrightarrow{m_1/m} \mu_k$ is an epimorphism of cyclic groups, and because $N_{k_1/k}(\mu_{k_1}) \subset \mu_k$. The functoriality follows from uniqueness and the commutativity of the diagram



(The parallelogram commutes because φ_{k_2/k_1} is the multiplication by some integer.)

Suppose we know *b)* for $\varphi_{k_1/k}$ and φ_{k_2/k_1}, and write $d_1=[k_2:k_1]$. Then

$$\left(1+\frac{m}{2}+\frac{m_1}{2}\right)\frac{dm}{m_1}\left(1+\frac{m_1}{2}+\frac{m_2}{2}\right)\frac{d_1m_1}{m_2}=\left(1+\frac{m}{2}+\frac{m_1}{2}\right)\left(1+\frac{m_1}{2}+\frac{m_2}{2}\right)\frac{[k_2:k]m}{m_2}$$

so the formula for $\varphi_{k_2/k}=\varphi_{k_2/k_1}\circ\varphi_{k_1/k}$ will follow if we show that

$$\left(1+\frac{m}{2}+\frac{m_1}{2}\right)\left(1+\frac{m_1}{2}+\frac{m_2}{2}\right)\equiv\left(1+\frac{m}{2}+\frac{m_2}{2}\right)\bmod m.$$

Write $m_1=mn_1$ and $m_2=m_1n_2$. Then the difference of the left and right side is

$$m_1+\frac{1}{4}(mm_1+mm_2+m_1^2+m_1m_2)\equiv\frac{m^2n_1}{4}(1+n_2+n_1+n_1n_2)\bmod m$$

$$\equiv m.\frac{m}{2}.\frac{n_1(1+n_1)}{2}.(1+n_2)\equiv 0 \bmod m.$$

Similarly *c)* follows if we know it for each layer of $k\subset k_1\subset k_2$. Using this we can prove *b)* and *c)* in the layers of $k\subset k(\mu_{k_1})\subset k_1$, and we can further break up the bottom into layers such that the order of μ_k increases by a prime factor in each one. Therefore it suffices to treat the following three cases.

Case 1. — $m_1=m$. Then $\mu_{k_1}\subset k$ so clearly $\varphi(\zeta)=\zeta^d$, which is *b)*. For *c)* it suffices to show that if $\mathfrak{p}$ is a prime of k, prime to m_1, and if $b\notin\mathfrak{p}$, then $\left(\frac{b}{\mathfrak{p}}\right)_{k_1,m}=\left(\frac{b}{\mathfrak{p}}\right)_{k,m}^{d}$. If $\mathfrak{p}=\prod_i\mathfrak{P}_i^{e_i}$ where $\mathfrak{P}_i$ has degree f_i over $\mathfrak{p}$, and if $\mathbf{N}\mathfrak{p}=q$, then $\mathbf{N}\mathfrak{P}_i=q^{f_i}$. Therefore $\left(\frac{b}{\mathfrak{P}_i}\right)_{k_1,m}\equiv b^{\frac{q^{f_i}-1}{m}}=b^{\frac{(q-1)}{m}(1+q+\ldots+q^{f_i-1})}\equiv\left(\frac{b}{\mathfrak{p}}\right)_{k,m}^{(1+q+\ldots+q^{f_i-1})}=\left(\frac{b}{\mathfrak{p}}\right)_{k,m}^{f_i}\bmod\mathfrak{P}_i$. Thus

$$\left(\frac{b}{\mathfrak{p}}\right)_{k_1,m}=\prod_i\left(\frac{b}{\mathfrak{P}_i}\right)_{k_1,m}^{e_i}=\left(\frac{b}{\mathfrak{p}}\right)_{k,m}^{\Sigma e_if_i}=\left(\frac{b}{\mathfrak{p}}\right)_{k,m}^{d}.$$

Case 2. — $k_1=k(\mu_{k_1})$ and $m_1=mp$ where p is a prime not dividing m. Then p must be odd so $\frac{m}{2}+\frac{m_1}{2}=m.\frac{1+p}{2}\equiv 0 \bmod m$, so *b)* becomes $\varphi(\zeta)=\zeta^{d/p}$. Thus we must

show $N_{k_1/k}(\zeta)=(\zeta^p)^{d/p}$ for $\zeta\in\mu_{k_1}$. This is clear for $\zeta\in\mu_k$, and if ζ has order p, and hence for a set of generators of μ_{k_1}.

For *c)* we note that $\left(\frac{b}{\mathfrak{p}}\right)_{mp}\in\mu_k$ because it is fixed under the galois group. Moreover,

$$\left(\frac{b}{\mathfrak{p}}\right)_{mp}^{p}=\left(\frac{b}{\mathfrak{p}}\right)_{m}=\left(\frac{b}{\mathfrak{p}}\right)_{m}^{d},$$

by the same calculation as in case 1. Hence

$$\left(\frac{b}{\mathfrak{p}}\right)_{mp}=\left(\frac{b}{\mathfrak{p}}\right)_{m}^{d/p}=\varphi\left(\left(\frac{b}{\mathfrak{p}}\right)_{m}\right).$$

Case 3. — As in Case 2, but now assume p divides m. Then $d=[k_1:k]=p$, and

$$\frac{m}{2}+\frac{m_1}{2}=m\frac{1+p}{2}\equiv\begin{cases}0 & \text{if } p\neq 2\\ \frac{m}{2} & \text{if } p=2\end{cases}\quad \bmod m.$$

We are in a Kummer extension of degree p, so the norm of a root of unity not in μ_k is its p-th power times the product of all p-th roots of unity. Therefore, for $\zeta\in\mu_{k_1}$

$$N_{k_1/k}(\zeta)=\begin{cases}\zeta^p & \text{if } p\neq 2\\ \zeta^{2+m} & \text{if } p=2.\end{cases}$$

These remarks prove *b)*.

It remains to prove *c)*. Let b an element of A, and let $\mathfrak{p}$ be a prime ideal of A which divides neither b nor m_1. Then $\mathfrak{p}$ is unramified in the galois extension k_1/k, so $p=[k_1:k]=fg$, where f is the degree of a prime $\mathfrak{P}$ over $\mathfrak{p}$, and g is the number of primes over $\mathfrak{p}$. Write $q=\mathbf{N}\mathfrak{p}$, so $q^f=\mathbf{N}\mathfrak{P}$.

The case $f=1$. — Set $\zeta=\left(\frac{b}{\mathfrak{P}}\right)_{mp}$. Then

$$\zeta^p=\left(\frac{b}{\mathfrak{P}}\right)_{m}\equiv b^{(q-1)/m}\equiv\left(\frac{b}{\mathfrak{p}}\right)_{m}\bmod\mathfrak{P}$$

and

$$N_{k_1/k}(\zeta)=\prod_{\sigma\in\mathrm{Gal}(k_1/k)}\left(\frac{b}{\sigma\mathfrak{P}}\right)_{mp}=\left(\frac{b}{\mathfrak{p}}\right)_{mp}.$$

Hence $\varphi\left(\left(\frac{b}{\mathfrak{p}}\right)_{m}\right)=\varphi(\zeta^p)=\varphi(\zeta^{m_1/m})=N_{k_1/k}(\zeta)=\left(\frac{b}{\mathfrak{p}}\right)_{mp}$ by part *a)*.

The case $f=p$. — Then $q\equiv 1 \bmod m$ but $q\not\equiv 1 \bmod mp$. Write $q=1+am$; then $a^{p-1}\equiv 1 \bmod p$. We can write $q^p-1=pam(1+amb)+a^pm^p$ for some integer b. Setting $(q^p-1)/mp=h(q-1)/m$, we have

$$h=\frac{1+q+\ldots+q^{p-1}}{p}=\frac{q^{p-1}}{p(q-1)}=1+amb+\frac{a^{p-1}m^{p-1}}{p}$$

$$\equiv 1+\frac{m^{p-1}}{p} \bmod m.$$

$$\equiv \begin{cases} 1 & \text{if } p\neq 2 \\ 1+\dfrac{m}{2} & \text{if } p=2 \end{cases} \bmod m.$$

Now

$$\left(\frac{b}{\mathfrak{p}}\right)_{mp}=\left(\frac{b}{\mathfrak{P}}\right)_{mp}\equiv b^{(q^p-1)/mp} \bmod \mathfrak{P}$$

$$=b^{h(q-1)/m}$$

$$\equiv\left(\frac{b}{\mathfrak{p}}\right)_m^h \bmod \mathfrak{P}$$

$$=\varphi\left(\left(\frac{b}{\mathfrak{p}}\right)_m\right). \quad \text{Q.E.D.}$$

CHAPTER II

MENNICKE SYMBOLS ASSOCIATED WITH SL_n

§ 4. Statement of the main theorem. Examples and Applications.

Let A be a commutative ring and let $\mathfrak{q}$ be an ideal of A. $E_n(A)$ denotes the subgroup of $SL_n(A)$ generated by all " elementary " matrices, $I + te_{ij}$ $(t \in A, i \neq j)$, and $E_n(A, \mathfrak{q})$ denotes the *normal* subgroup of $E_n(A)$ generated by those with $t \in \mathfrak{q}$. This is a subgroup of

$$SL_n(A, \mathfrak{q}) = \ker(SL_n(A) \to SL_n(A/\mathfrak{q})).$$

We shall consider $SL_n(A) \subset SL_{n+m}(A)$ by identifying $\alpha \in SL_n(A)$ with $\begin{pmatrix} \alpha & 0 \\ 0 & I_m \end{pmatrix}$.

If $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(A, \mathfrak{q})$, then it is easy to see (Lemma 5.3 below) that $\alpha \mapsto (a, b)$ defines a surjective map $SL_2(A, \mathfrak{q}) \xrightarrow{1^{st} \text{ row}} W_{\mathfrak{q}}$,

where $W_{\mathfrak{q}}$ is defined in § 2.

The aim of this chapter is to prove:

Theorem 4.1. — *Let* A *be a Dedekind ring, let* $\mathfrak{q}$ *be an ideal of* A, *and suppose* $n \geq 3$.

a) $E_n(A, \mathfrak{q}) = [SL_n(A), SL_n(A, \mathfrak{q})]$.

b) *Write* $C_{\mathfrak{q}}(n) = SL_n(A, \mathfrak{q})/E_n(A, \mathfrak{q})$, *and let*

$$\kappa : SL_n(A, \mathfrak{q}) \to C_{\mathfrak{q}}(n)$$

be the natural epimorphism. Then there is a unique map $[\ ] : W_{\mathfrak{q}} \to C_{\mathfrak{q}}(n)$ *such that*

$$\begin{array}{ccc} SL_2(A, \mathfrak{q}) & \xrightarrow{\text{incl.}} & SL_n(A, \mathfrak{q}) \\ \Big\downarrow{\scriptstyle 1^{st} \text{ row}} & & \Big\downarrow{\scriptstyle \kappa} \\ W_{\mathfrak{q}} & \xrightarrow[[\ ]]{} & C_{\mathfrak{q}}(n) \end{array}$$

is commutative, and $[\ ]$ *is a Mennicke symbol.*

c) *This Mennicke symbol is universal.*

Part *a)* is a slight improvement of well known results (cf. part *d)* of Theorem 7.5 and part *a)* of Theorem 11.1 below). Parts *b)* and *c)* can be stated equally well as follows:

Let C be any group. Then the commutative squares

$$\begin{array}{ccc} SL_2(A, \mathfrak{q}) & \longrightarrow & SL_n(A, \mathfrak{q}) \\ \Big\downarrow{\scriptstyle 1^{st}\ row} & & \Big\downarrow{\scriptstyle \kappa} \\ W_{\mathfrak{q}} & \xrightarrow[[\ ]]{} & C \end{array}$$

define a bijection between Mennicke symbols, [ ], and homomorphisms κ satisfying $\kappa(\tau\sigma\tau^{-1}) = \kappa(\sigma)$ for $\sigma \in SL_n(A, \mathfrak{q})$ and $\tau \in SL_n(A)$.

Part *b)* says that, given $\kappa : SL_n(A, \mathfrak{q}) \to C$ as above, its restriction to $SL_2(A, \mathfrak{q})$ factors through a unique map $[\ ] : W_{\mathfrak{q}} \to C$, and [ ] is a Mennicke symbol. The theorem of Mennicke in § 5 contains this fact.

Part *c)* says that, given a Mennicke symbol $[\ ] : W_{\mathfrak{q}} \to C$, we can construct a unique κ as above. This implies, first of all, that the composite

$$SL_2(A, \mathfrak{q}) \xrightarrow{1^{st}\ row} W_{\mathfrak{q}} \xrightarrow{[\ ]} C$$

is a homomorphism. This not at all obvious fact is the Theorem of Kubota in § 6. After this there remains the problem of extending a homomorphism $\kappa_n : SL_n(A, \mathfrak{q}) \to C$, satisfying certain conditions, to a homomorphism $\kappa_{n+1} : SL_{n+1}(A, \mathfrak{q}) \to C$, satisfying analogous conditions. The (rather complicated) solution of this problem occupies §§ 8-10, and it is done in a setting more general than that of Theorem 4.1.

Before embarking on the proofs of these results we shall now record some of the principal corollaries of Theorem 4.1. Further results and applications are stated in § 11.

Corollary 4.2. — For $n \geq 3$ the natural maps

$$C_{\mathfrak{q}}(n) \to C_{\mathfrak{q}}(n+1)$$

are isomorphisms.

The next corollary solves the " congruence subgroup problem " (see Chapter IV) for $SL_n(A)$.

Corollary 4.3. — Suppose that A is of arithmetic type and that $n \geq 3$.

a) $SL_n(A)$ *is equal to* $E_n(A)$ *and it is a finitely generated group, equal to its own commutator subgroup.*

b) *If A is not totally imaginary then $C_{\mathfrak{q}} = \{1\}$ for all $\mathfrak{q}$.*

c) *If A is totally imaginary, and if m is the number of roots of unity in A, then there is a canonical isomorphism*

$$C_{\mathfrak{q}} \cong \mu_r \qquad \textit{(the r-th roots of unity)}$$

where $r = r(\mathfrak{q})$, is defined by

$$\mathrm{ord}_p(r) = \min_{p \mid \mathfrak{q}} \left[\frac{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{q})}{\mathrm{ord}_{\mathfrak{p}}(p)} - \frac{1}{p-1} \right]_{[0,\ \mathrm{ord}_p(m)]}$$

for each prime p (cf. (3.3)).

If $\mathfrak{q} \subset \mathfrak{q}'$, *and if* $r' = r(\mathfrak{q}')$, *then the homomorphism* $C_{\mathfrak{q}} \to C_{\mathfrak{q}'}$ *corresponds to the* (r/r')*-th power map* $\mu_r \to \mu_{r'}$.

d)

$$\varprojlim_{\mathfrak{q}} C_{\mathfrak{q}} \cong \begin{cases} \{1\} & \text{if A is not totally imaginary,} \\ \mu_m & \text{if A is totally imaginary.} \end{cases}$$

Parts *b)* and *c)* follow from Theorem 4.1 combined with Theorem 3.6. These imply $C_A = \{1\}$ in all cases, and this, together with remarks (5.2) below, is part *a)*. Part *d)* is an immediate consequence of parts *b)* and *c)*.

When A is a ring of algebraic integers the finite generation of $SL_n(A)$ was proved by Hurwitz [12] in 1895, and the finite generation of all " arithmetic groups " was finally proved by Borel-Harish-Chandra [8] in 1962. In the function field case, however, finite generation of $SL_n(A)$ $(n \geq 3)$ was only recently proved by O'Meara [20], and he points out that $SL_2(A)$ may fail to be finitely generated. The statements about generation by elementary matrices, and about the commutator subgroups, can fail for $SL_2(A)$ even in the number field case. For example, if $A = \mathbf{Z}[\sqrt{-5}]$, then Swan (unpublished) has determined a presentation of $SL_2(A)$ from which it follows that $SL_2(A)/H \cong \mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$ where H is the subgroup generated by all commutators and all elementary matrices. Thus H doesn't even have finite index in $SL_2(A)$.

In § 11 we show that $SL_n(A)$ is finitely generated for certain finitely generated $\mathbf{Z}$-algebras A, provided n is sufficiently large relative to the Krull dimension of A.

In the balance of this section we shall use Theorem 4.1 to produce some further examples of non trivial Mennicke symbols, and finally apply Corollary 4.3 to the calculation of some " Whitehead groups " of finite abelian groups.

Example 4.4. — (Cf. [18, § 1, Ex. 1.7, and p. 422].) Let $A = \mathbf{R}[x, y]$ where x and y are subject to the single relation, $x^2 + y^2 = 1$. Viewing A as a ring of functions on the circle, S^1, with x and y the coordinate functions, an element of $SL_n(A)$ defines a map $S^1 \to SL_n(\mathbf{R})$. Taking homotopy classes we obtain a homomorphism

$$SL_n(A) \to \pi_1(SL_n(\mathbf{R})) \cong \{\pm 1\} \qquad (n \geq 3).$$

Since $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ represents a generator of this homotopy group we obtain a Mennicke symbol (for the ideal $\mathfrak{q} = A$) such that $\left[\begin{matrix} y \\ x \end{matrix}\right] = -1$. Let $\mathfrak{p}_i$ be the ideal generated by y and $x - i$, $i = \pm 1$. Then $x \equiv i \bmod \mathfrak{p}_i$ and $\mathfrak{p}_1 \mathfrak{p}_{-1} = yA$. Hence, using Proposition 2.13, we have

$$-1 = \left[\begin{matrix} y \\ x \end{matrix}\right] = \left[\begin{matrix} \mathfrak{p}_1\mathfrak{p}_{-1} \\ x \end{matrix}\right] = \left[\begin{matrix} \mathfrak{p}_1 \\ x \end{matrix}\right]\left[\begin{matrix} \mathfrak{p}_{-1} \\ x \end{matrix}\right] = \left[\begin{matrix} \mathfrak{p}_1 \\ 1 \end{matrix}\right]\left[\begin{matrix} \mathfrak{p}_{-1} \\ -1 \end{matrix}\right] = \left[\begin{matrix} \mathfrak{p}_{-1} \\ -1 \end{matrix}\right].$$

The orthogonal group in the plane operates as automorphisms of A. Applying them to the above equation we find that

$$\left[\begin{matrix} \mathfrak{p} \\ -1 \end{matrix}\right] = -1$$

for any prime $\mathfrak{p}$ corresponding to a point of S^1. This should be contrasted with the fact that $\left[\begin{matrix} b \\ u \end{matrix}\right] = 1$ whenever u is a unit.

It can be shown that the symbol above is universal, i.e. that $SL_n(A)/E_n(A) \cong \{\pm 1\}$ for $n \geq 3$.

Example 4.5 (Stallings). — Let $A = \mathbf{R}[t]$ be a polynomial ring in one variable t. Then A is euclidean, so $SL_n(A) = E_n(A)$ for all $n \geq 2$. Let $\mathfrak{q} = (t^2 - t)A$; $\mathfrak{q}$ consists of polynomials vanishing at 0 and 1. Therefore, if $[0, 1]$ denotes the unit interval, an element of $SL_n(A, \mathfrak{q})$ defines a function $[0, 1] \to SL_n(\mathbf{R})$ sending 0 and 1 to the identity matrix. It is easy to see that this induces, for $n \geq 3$, a homomorphism

$$(*) \qquad SL_n(A, \mathfrak{q})/E_n(A, \mathfrak{q}) \to \pi_1(SL_n(\mathbf{R})) \cong \{\pm 1\}.$$

Let
$$\tau(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}\begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 1-t^2 & -t \\ 2t-t^3 & 1-t^2 \end{pmatrix}$$

For $t = 1$, $\tau(t) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is a 90° rotation.

Let $\sigma(t)$ be the rotation by $\pi t/2$. One has $\sigma(0) = \tau(0)$ and $\sigma(1) = \tau(1)$. Moreover the paths σ and τ are homotopic; to see this it suffices to verify that the paths $\sigma(t)(e_2)$ and $\tau(t)(e_2)$ in $\mathbf{R}^2 - \{0\}$ are homotopic, which is clear. It follows that σ^4 and τ^4 are homotopic loops in $SL_2(\mathbf{R})$. Since σ^4 is evidently a generator of $\pi_1(SL_2(\mathbf{R}))$ it follows that τ^4 is likewise. Consequently the map $(*)$ above is surjective, and we obtain a non trivial Mennicke symbol

$$[\,] : W_{\mathfrak{q}} \to \{\pm 1\}.$$

If $(a, b) \in W_{\mathfrak{q}}$ then (a, b) defines a function from $[0, 1]$ to $\mathbf{R}^2 - \{0\}$ sending 0 and 1 to the point $(1, 0) \in \mathbf{R}^2$. Viewed as a function from the circle to the punctured plane, $\left[\begin{matrix} b \\ a \end{matrix}\right] \in \{1\}$ is just the parity of the degree of this function.

We close this section now with some calculations of Whitehead groups. For an ideal $\mathfrak{q}$ in a commutative ring A we shall write

$$SK_1(A, \mathfrak{q}) = \lim_{n \to \infty} SL_n(A, \mathfrak{q})/E_n(A, \mathfrak{q}),$$

and $SK_1A = SK_1(A, A)$.

It is clear that we have an exact sequence (cf. [1, Ch. III]),

$$(4.6) \qquad SK_1(A, \mathfrak{q}) \to SK_1A \to SK_1(A/\mathfrak{q}).$$

Moreover, it follows from [1, Corollary 5.2] that:

(4.7) *If* $\mathfrak{q} \subset \mathfrak{q}'$ *are ideals such that* $A/\mathfrak{q}$ *is semi-local then* $SK_1(A, \mathfrak{q}) \to SK_1(A, \mathfrak{q}')$ *is surjective.*

Let π be a finite abelian group, and let $A = \mathbf{Z}\pi$. We are interested in determining $SK_1\mathbf{Z}\pi$. Let $\bar{A}$ denote the integral closure of A in $\mathbf{Q}\pi$. The ring $\bar{A}$ is a direct product of rings A_χ indexed by the subgroups χ of π for which π/χ is cyclic. A_χ is generated

over $\mathbf{Z}$ by the projection of π, which is, say, the m_χ-th roots of unity. The kernel of this projection is χ, and we write $k_\chi = [\chi : 1]$; thus $[\pi : 1] = k_\chi m_\chi$.

Let $\mathfrak{c} = \{a \in \bar{A} \mid a\bar{A} \subset A\}$ be the conductor from $\bar{A}$ to A; it is the largest ideal of $\bar{A}$ lying in A. Since $\mathfrak{c}$ is an ideal of $\bar{A}$ it is the direct sum of its components, $\mathfrak{c}_\chi$ in the various factors A_χ. The $\mathfrak{c}_\chi$'s have been determined in [7, Prop. 8.6]:

$$\mathfrak{c}_\chi = k_\chi \cdot \prod_{p \mid m_\chi,\ p \text{ prime}} (p)^{1/(p-1)} \tag{4.8}$$

Here $(p)^{1/(p-1)}$ is the ideal whose $(p-1)$-st power is (p), and it is generated by $1-w$ for any primitive p-th root of unity w. If $\mathfrak{p} \mid p$ in A_χ then $\operatorname{ord}_\mathfrak{p}((p)^{1/(p-1)}) = p^{\operatorname{ord}_p(m_\chi)-1}$.

It follows from Corollaries 4.2 and 4.3 that

$$SK_1(A_\chi, \mathfrak{c}_\chi) \cong \mu_r,$$

the r-th roots of unity, where $r = r(\mathfrak{c}_\chi)$ is 1 if A_χ is not totally imaginary, i.e. if $m_\chi \leq 2$, and otherwise we have, for a prime p,

$$\operatorname{ord}_p(r) = \min_{\mathfrak{p} \mid p} \left[\frac{\operatorname{ord}_\mathfrak{p}(\mathfrak{c}_\chi)}{\operatorname{ord}_\mathfrak{p}(p)} - \frac{1}{p-1} \right]_{[0,\ \operatorname{ord}_p(m'_\chi)]}. \tag{4.9}$$

We use the notation of Corollary 4.3 here, and m'_χ denotes the number of roots of unity in A_χ. Thus $m'_\chi = m_\chi$ if m_χ is even, and $m'_\chi = 2m_\chi$ otherwise.

Proposition 4.10. — For a prime p the p-primary part of $SK_1(A_\chi, \mathfrak{c}_\chi)$ is cyclic of order p^j, where:

If $p = 2$ and if m_χ is odd and > 2 then

$$j = \begin{cases} 1 & \text{if } 4 \mid [\pi : 1] \\ 0 & \text{if } 4 \nmid [\pi : 1] \end{cases}$$

Otherwise,

$$j = \begin{cases} \min(\operatorname{ord}_p(k_\chi), \operatorname{ord}_p(m_\chi)) & \text{if } m_\chi > 2 \\ 0 & \text{if } m_\chi \leq 2 \end{cases}$$

Proof. — If $m_\chi \leq 2$ then A_χ is not totally imaginary so $j = 0$. If $m_\chi > 2$ then $j = \operatorname{ord}_p(r)$ as in (4.9).

Suppose $p \mid m_\chi$. Then if $\mathfrak{p} \mid p$, we have $\operatorname{ord}_\mathfrak{p}(m'_\chi) = \operatorname{ord}_\mathfrak{p}(m_\chi)$, and,

$$\operatorname{ord}_\mathfrak{p}(p) = \varphi(p^{\operatorname{ord}_p(m_\chi)}) = (p-1)p^{(\operatorname{ord}_p(m_\chi)-1)}.$$

Further it follows from (4.8) that $\operatorname{ord}_\mathfrak{p}(\mathfrak{c}_\chi) = \operatorname{ord}_\mathfrak{p}(k_\chi) + p^{(\operatorname{ord}_p(m_\chi)-1)}$. Consequently

$$\begin{aligned} \frac{\operatorname{ord}_\mathfrak{p}(\mathfrak{c}_\chi)}{\operatorname{ord}_\mathfrak{p}(p)} - \frac{1}{p-1} &= \frac{\operatorname{ord}_\mathfrak{p}(k_\chi)}{\operatorname{ord}_\mathfrak{p}(p)} + \frac{1}{p-1} - \frac{1}{p-1} \\ &= \operatorname{ord}_p(k_\chi) \geq 0, \end{aligned}$$

so

$$\left[\frac{\operatorname{ord}_\mathfrak{p}(\mathfrak{c}_\chi)}{\operatorname{ord}_\mathfrak{p}(p)} - \frac{1}{p-1} \right]_{[0,\ \operatorname{ord}_p(m_\chi)]} = \min(\operatorname{ord}_p(k_\chi), \operatorname{ord}_p(m_\chi)).$$

If $p \nmid m'_\chi$ there are no p-th roots of unity in A_χ, so $j=0$. Thus the formulas are verified except in the case m_χ is odd and >2 and $p=2$. In this case, if $\mathfrak{p}|2$, $\mathrm{ord}_\mathfrak{p}(2)=1$ and $\mathrm{ord}_\mathfrak{p}(\mathfrak{c}_\chi)=\mathrm{ord}_\mathfrak{p}(k_\chi)$ so

$$j=\left[\frac{\mathrm{ord}_\mathfrak{p}(k_\chi)}{1}-\frac{1}{2-1}\right]_{[0,\,1]}=(\mathrm{ord}_2(k_\chi)-1)_{[0,\,1]}$$
$$=\begin{cases}1 & \text{if } \mathrm{ord}_2(k_\chi)\geq 2\\ 0 & \text{if } \mathrm{ord}_2(k_\chi)<2.\end{cases}$$

This completes the proof of Proposition 4.10.

Corollary 4.11. — *We have* $\mathrm{SK}_1(A_\chi, \mathfrak{c}_\chi)=\mu_{r(\chi)}$ *where:*

$r(\chi)=1$ *if* $m_\chi\leq 2$;

$r(\chi)=2$ g.c.d. (m_χ, k_χ) *if* $4|k_\chi$ *and* m_χ *is odd and* ≥ 3;

$r(\chi)=$ g.c.d. (m_χ, k_χ) *otherwise.*

Since $A/\mathfrak{c}$ is a finite ring it follows from (4.7) that

$$\mathrm{SK}_1(A, \mathfrak{c}) \to \mathrm{SK}_1 A \quad \textit{is surjective.}$$

Moreover, it follows from [7, Lemma 10.5] that *if* $\mathfrak{a}$ *is an* $\overline{A}$*-ideal contained in* A *then*

$$\mathrm{SK}_1(A, \mathfrak{a}) \xrightarrow{\cong} \mathrm{SK}_1(\overline{A}, \mathfrak{a}). \tag{4.12}$$

These two facts combine to show that $\mathrm{SK}_1 A$ is a quotient of

$$\mathrm{SK}_1(\overline{A}, \mathfrak{c})=\coprod_\chi \mathrm{SK}_1(A_\chi, \mathfrak{c}_\chi).$$

Corollary 4.13. — $\mathrm{SK}_1(\mathbf{Z}\pi)=0$ *if* π *is an elementary 2-group.*

For in this case all m_χ's are ≤ 2.

Proposition 4.14. — *If the p-primary part of* π *is cyclic then* $\mathrm{SK}_1(\mathbf{Z}\pi)$ *has no p-torsion.*

Proof. — We argue by induction on $n=\mathrm{ord}_p[\pi : 1]$. The case $n=0$ is trivial, so assume $n>0$. Let π_0 be *the* subgroup of π of order p, and write $\pi'=\pi/\pi_0$. Let $\mathfrak{b}=\ker(A\to A')$, where $A'=\mathbf{Z}\pi'$. Then from (4.6) we have an exact sequence $\mathrm{SK}_1(A, \mathfrak{b}) \to \mathrm{SK}_1(A) \to \mathrm{SK}_1(A')$, and, by induction, $\mathrm{SK}_1(A')$ has no p-torsion. We shall finish the proof by showing that $\mathrm{SK}_1(A, \mathfrak{b})$ has no p-torsion.

Write $\overline{A}=\overline{A}'\times\overline{A}''$ where $\overline{A}'$ is the integral closure of A', and where $\overline{A}''$ is the product of all A_χ for which χ does not contain π_0. If A'' is the projection of A into $\overline{A}''$ then $A\subset A'\times A''$ and $\mathfrak{b}$ is the kernel of the projection of A in the first factor. In particular, $\mathfrak{b}$ is an $(A'\times A'')$-ideal, and is identical with its projection into A''. It follows therefore from [7, Lemma 10.5] that $\mathrm{SK}_1(A, \mathfrak{b})=\mathrm{SK}_1(A'\times A'', \mathfrak{b})$, and the latter is clearly equal to $\mathrm{SK}_1(A'', \mathfrak{b})$.

Let $\mathfrak{a}$ denote the projection of $\mathfrak{c}$ into $\overline{A}''$. Then we can identify $\mathfrak{a}$ with an ideal of $\overline{A}''$, which has finite index in $\overline{A}''$, and which is contained in $\mathfrak{b}$. Now (4.7) implies

that $SK_1(A'', \mathfrak{a}) \to SK_1(A'', \mathfrak{b})$ is surjective, and from [7, Lemma 10.5] again, we deduce that $SK_1(A'', \mathfrak{a}) \cong SK_1(\bar{A}'', \mathfrak{a})$. The latter is just the direct sum of all $SK_1(A_\chi, \mathfrak{c}_\chi)$ for which χ does not contain π_0. Hence the Proposition will be proved if we show that each of these has no p-torsion.

But if $\pi_0 \notin \chi$ then $k_\chi = [\chi : 1]$ is prime to p. Proposition 4.10 says the p-torsion in $SK_1(A_\chi, \mathfrak{c}_\chi)$ is cyclic of order p^j, where $j = \min(\mathrm{ord}_p(k_\chi), \mathrm{ord}_p(m_\chi))$, so $j = 0$ as claimed.

Proposition 4.15(T.-Y. Lam). — *Let* $\pi = (x, y / x^p = y^p = [x, y] = 1)$ *be a direct product of two cyclic groups of order p. Then* $SK_1\mathbf{Z}\pi = 0$.

Proof. — We can assume $p > 2$ thanks to Corollary 4.13. We shall write f_χ for the projection $\mathbf{Z}\pi \to A_\chi$, and $f_0 = f_{\chi_0}$, where χ_0 is the subgroup generated by x. Let $c = \prod_{i=0}^{p-1}(x^i - y)$, $a = 1 - c$, and $b = (1-y)c$. Then if $\chi \neq \chi_0$ we have $f_\chi(x^i) = f_\chi(y)$ for some i, so $f_\chi(a) = 1$. Moreover, if $\lambda = 1 - f_0(y)$ then $f_0(a) = 1 - \lambda^p$ and $f_0(b) = \lambda^{p+1}$. This shows that b and c belong to the conductor $\mathfrak{c}$.

Let $[\ ]_\mathfrak{c}$ be the Mennicke symbol associated with $\mathfrak{c}$ in $\mathbf{Z}\pi$ or in $\bar{A}$. It exists thanks to Theorem 5.4 below, and (4.12) implies that it is insensitive to the difference between $\mathbf{Z}\pi$ and $\bar{A}$. In the decomposition

$$SK_1(\bar{A}, \mathfrak{c}) = \coprod_\chi SK_1(A_\chi, \mathfrak{c}_\chi),$$

$\left[\begin{matrix} b \\ a \end{matrix}\right]_\mathfrak{c}$ has zero coordinate at each $\chi \neq \chi_0$, and at χ_0 it has a coordinate which corresponds, via Corollary 4.3, to the power residue symbol

$$\left(\frac{\lambda^{p+1}}{1-\lambda^p}\right)_p = \left(\frac{\lambda}{1-\lambda^p}\right)_p = \left(\frac{1-\lambda^p,\ \lambda}{(\lambda)}\right)_p \tag{A.21}$$

$$\neq 1. \tag{A.22}$$

The map $SK_1(A, \mathfrak{c}) \to SK_1(A)$ is an epimorphism of modules over

$$G = \mathrm{Aut}(\pi) \cong GL_2(\mathbf{Z}/p\mathbf{Z}),$$

and G operates transitively on the non trivial characters χ. Consequently $\left[\begin{matrix} b \\ a \end{matrix}\right]_\mathfrak{c}$ generates $SK_1(A, \mathfrak{c})$ as a G-module, and if we show that $\left[\begin{matrix} b \\ a \end{matrix}\right]_\mathfrak{c}$ has trivial image in SK_1A the proposition will be proved. If $[\ ]$ is the Mennicke symbol for SK_1A, i.e. for the unit ideal in A, then the image of $\left[\begin{matrix} b \\ a \end{matrix}\right]_\mathfrak{c}$ is just $\left[\begin{matrix} b \\ a \end{matrix}\right]$. Write $d = 1 - y$. Then $b = dc$ and $a = 1 - \prod_{i=0}^{p-1}(x^i - y) = 1 - de$, so

$$\left[\begin{matrix} b \\ a \end{matrix}\right] = \left[\begin{matrix} dc \\ a \end{matrix}\right] = \left[\begin{matrix} d \\ a \end{matrix}\right]\left[\begin{matrix} c \\ a \end{matrix}\right] = 1.$$

because $a \equiv 1 \bmod d$ and $a \equiv 1 \bmod c$. Q.E.D.

§ 5. The theorem of Mennicke.

Let A be a commutative ring and let $\mathfrak{q}$ and $\mathfrak{q}'$ be ideals. The commutator formula $[I+te_{ij}, I+se_{jk}]=I+tse_{ik}$, for i, j, and k distinct, shows that

$$\mathrm{E}_n(\mathrm{A}, \mathfrak{q}'\mathfrak{q}) \subset [\mathrm{E}_n(\mathrm{A}, \mathfrak{q}'), \mathrm{E}_n(\mathrm{A}, \mathfrak{q})]$$

for $n\geq 3$. For $\mathfrak{q}'=\mathrm{A}$ this yields

$$\mathrm{E}_n(\mathrm{A}, \mathfrak{q})=[\mathrm{E}_n(\mathrm{A}), \mathrm{E}_n(\mathrm{A}, \mathfrak{q})] \quad \textit{for} \quad n\geq 3. \tag{5.1}$$

The commutator formula also easily implies (see [1, Corollary 1.5]) that:

(5.2) *If* A *is a finitely generated* **Z***-algebra then* $\mathrm{E}_n(\mathrm{A})$ *is a finitely generated group, for* $n\geq 3$.

The subgroup generated by $\mathrm{E}_n(\mathrm{A}, \mathfrak{q})$ together with the diagonal matrices in $\mathrm{GL}_n(\mathrm{A}, \mathfrak{q})$ will be denoted

$$\mathrm{GE}_n(\mathrm{A}, \mathfrak{q}).$$

Lemma 5.3. — *Let* N *denote the group of all matrices* $\begin{pmatrix} 1 & 0 \\ q & u \end{pmatrix}$ *in* $\mathrm{GL}_2(\mathrm{A}, \mathfrak{q})$, *and let* SN *denote those with* $u=1$. *The map* $\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a, b)$ *defines bijections* $\mathrm{N}\backslash\mathrm{GL}_2(\mathrm{A}, \mathfrak{q})\to \mathrm{W}_{\mathfrak{q}}$ *and* $\mathrm{SN}\backslash\mathrm{SL}_2(\mathrm{A}, \mathfrak{q})\to \mathrm{W}_{\mathfrak{q}}$.

Proof. — Since $u=ad-bc$ is a unit it is clear that $(a, b)\in \mathrm{W}_{\mathfrak{q}}$. Suppose $\alpha'=\begin{pmatrix} a & b \\ c' & d' \end{pmatrix}$. Then $\alpha'\alpha^{-1}=\begin{pmatrix} a & b \\ c' & d' \end{pmatrix}\cdot\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}u^{-1}=\begin{pmatrix} u & 0 \\ * & * \end{pmatrix}u^{-1}\in \mathrm{N}$. We conclude the proof by showing that every $(a, b)\in \mathrm{W}_{\mathfrak{q}}$ is the first row of an $\alpha\in \mathrm{SL}_2(\mathrm{A}, \mathfrak{q})$. Write $1=ax+by$ $(x, y\in \mathrm{A})$ and then set $c=-by^2\in\mathfrak{q}$ and $d=x+bxy$. Then

$$ad-bc=a(x+bxy)+b^2y^2=ax+by(ax+by)=1.$$

Hence $d\equiv 1 \bmod \mathfrak{q}$ since $a\equiv 1 \bmod \mathfrak{q}$, and so $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathrm{A}, \mathfrak{q})$.

Theorem 5.4 (Mennicke). — *Let* A *be a commutative ring, and let* $\mathfrak{q}$ *be an ideal of* A. *Suppose, for some* $n\geq 3$, *that we are given a homomorphism* $\kappa : \mathrm{SL}_n(\mathrm{A}, \mathfrak{q})\to \mathrm{C}$ *such that* $\kappa(\tau\sigma\tau^{-1})=\kappa(\sigma)$ *whenever* $\tau\in \mathrm{E}_n(\mathrm{A})$ *and* $\sigma\in \mathrm{SL}_n(\mathrm{A}, \mathfrak{q})$. *Then there is a unique map* $[\,] : \mathrm{W}_{\mathfrak{q}}\to \mathrm{C}$ *rendering*

$$\begin{array}{ccc} \mathrm{SL}_2(\mathrm{A}, \mathfrak{q}) & \longrightarrow & \mathrm{SL}_n(\mathrm{A}, \mathfrak{q}) \\ \Big\downarrow{\scriptstyle 1^{\mathrm{st}}\text{ row}} & & \Big\downarrow{\scriptstyle \kappa} \\ \mathrm{W}_{\mathfrak{q}} & \longrightarrow & \mathrm{C} \end{array}$$

commutative, and $[\,]$ *is a Mennicke symbol.*

Remarks. — 1) When A is a Dedekind ring this establishes part *b)* of Theorem 4.1.

2) The proof of Theorem 5.4 is developed directly from Mennicke's arguments in [16].

3) In view of the results of Chapter I this theorem is already sufficient to obtain the portion of Corollary 4.3 applying to A of arithmetic type, but not totally imaginary. In case A is the ring of algebraic integers in a real number field this application was obtained independently by Mennicke and Newman in unpublished work. They follow closely Mennicke's original argument [16] for the case $A=\mathbf{Z}$.

Proof. — Since $n\geq 3$ it follows from the hypotheses of the theorem and (5.1) that

$$\ker(\kappa)\supset [E_n(A), SL_n(A, \mathfrak{q})]\supset E_n(A, \mathfrak{q}).$$

Therefore, if $\kappa_2 : SL_2(A, \mathfrak{q})\to C$ is the restriction of κ to $SL_2(A, \mathfrak{q})$, the existence of [ ] satisfying MS 1 follows from the next lemma, which will be used again in Chapter III for the symplectic group.

Lemma 5.5. — *Let* $\kappa_2 : SL_2(A, \mathfrak{q})\to C$ *be a homomorphism whose kernel contains* $E_2(A, \mathfrak{q})$ *and* $[E_2(A), SL_2(A, \mathfrak{q})]$. *Then* κ_2 *factors, via* $SL_2(A, \mathfrak{q})\xrightarrow{1^{st}\text{ row}} W_{\mathfrak{q}}$, *through a unique map* $[\,] : W_{\mathfrak{q}}\to C$, *and* [ ] *satisfies* MS 1.

Proof. — The group SN in Lemma 5.3 clearly lies in $E_2(A, \mathfrak{q})$, so [ ] exists, thanks to Lemma 5.3, and, moreover, $\begin{bmatrix}0\\1\end{bmatrix}=1$ because κ_2 kills SN. If $t\in\mathfrak{q}$ then $\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}\in E_2(A, \mathfrak{q})$ so, for $\alpha=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(A, \mathfrak{q})$,

$$\begin{bmatrix}b\\a\end{bmatrix}=\kappa\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\kappa\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}\right)=\kappa\begin{pmatrix}a & b+ta\\ * & *\end{pmatrix}=\begin{bmatrix}b+ta\\a\end{bmatrix}.$$

If $t\in A$ then $\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix}\in E_2(A)$, so

$$\begin{bmatrix}b\\a\end{bmatrix}=\kappa\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\kappa\left(\begin{pmatrix}1 & 1\\ -t & 0\end{pmatrix}\cdot\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix}\right)=\kappa\begin{pmatrix}a+tb & b\\ * & *\end{pmatrix}=\begin{bmatrix}b\\a+tb\end{bmatrix}.$$

We have thus shown the existence of [ ] satisfying MS 1.

Proof of MS 2. — If (a, b_1), $(a, b_2)\in W_{\mathfrak{q}}$ we have to show that $\begin{bmatrix}b_1b_2\\a\end{bmatrix}=\begin{bmatrix}b_1\\a\end{bmatrix}\begin{bmatrix}b_2\\a\end{bmatrix}$. By restricting κ to $SL_3(A, \mathfrak{q})$ we may as well assume that $n=3$. Choose $\alpha_i=\begin{pmatrix}a & b_i\\ c_i & d_i\end{pmatrix}\in SL_2(A, \mathfrak{q})$, $i=1, 2$, which we view, as usual, as elements of $SL_3(A, \mathfrak{q})$. Setting $\varepsilon_1=\begin{pmatrix}0 & -1 & 0\\ 0 & 0 & -1\\ 1 & 0 & 0\end{pmatrix}\in E_3(A)$, we have:

$$\alpha_1\varepsilon_1\alpha_2\varepsilon_1^{-1}=\begin{pmatrix}a & b_1 & 0\\ c_1 & d_1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}d_2 & 0 & -c_2\\ 0 & 1 & 0\\ -b_2 & 0 & a\end{pmatrix}=\begin{pmatrix}ad_2 & b_1 & -ac_2\\ c_1d_2 & d_1 & -c_1c_2\\ -b_2 & 0 & a\end{pmatrix}$$

Left multiplication by $\varepsilon_2=\begin{pmatrix}1&0&c_2\\0&1&0\\0&0&1\end{pmatrix}$ gives $\begin{pmatrix}1&b_1&0\\c_1d_2&d_1&-c_1c_2\\-b_2&0&a\end{pmatrix}$.

Left multiplication by $\varepsilon_3=\begin{pmatrix}1&0&0\\-c_1d_2&1&0\\b_2&0&1\end{pmatrix}$ gives $\begin{pmatrix}1&b_1&0\\0&d'&-c_1c_2\\0&b_1b_2&a\end{pmatrix}$,

where $d'=d_1-b_1c_1d_2$.

Right multiplication by $\varepsilon_4=\begin{pmatrix}1&-b_1&0\\0&1&0\\0&0&1\end{pmatrix}$ gives $\alpha'=\begin{pmatrix}1&0&0\\0&d'&-c_1c_2\\0&b_1b_2&a\end{pmatrix}$.

With $\varepsilon_5=\begin{pmatrix}0&0&1\\0&1&0\\-1&0&0\end{pmatrix}\in E_3(A)$ we have

$\varepsilon_5\alpha'\varepsilon_5^{-1}=\begin{pmatrix}a&b_1b_2&0\\-c_1c_2&d'&0\\0&0&1\end{pmatrix}$. Now since $\varepsilon_i\in E_3(A)$ for $i=1, 5$ and $\varepsilon_i\in E_3(A, \mathfrak{q})$ for $i=2, 3, 4$, we have

$$\begin{bmatrix}b_1b_2\\a\end{bmatrix}=\kappa(\varepsilon_5\alpha'\varepsilon_5^{-1})=\kappa(\alpha')=\kappa(\varepsilon_3\varepsilon_2\alpha_1(\varepsilon_1\alpha_2\varepsilon_1^{-1})\varepsilon_4)=\kappa(\alpha_1)\kappa(\alpha_2)=\begin{bmatrix}b_1\\a\end{bmatrix}\begin{bmatrix}b_2\\a\end{bmatrix}.$$ Q.E.D

§ 6. Kubota's Theorem.

Theorem 6.1 (Kubota, cf. [14]). — *Let* A *be a Dedeking ring, let* $\mathfrak{q}$ *be an ideal of* A, *and let* $[\ ]: W_{\mathfrak{q}}\to C$ *be a Mennicke symbol. Let* κ *be the composite map,*

$$GL_2(A, \mathfrak{q}) \xrightarrow{1^{st}\text{ row}} W_{\mathfrak{q}} \xrightarrow{[\,]} C,$$

so that $\kappa\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{bmatrix}b\\a\end{bmatrix}$. *Then* κ *is a homomorphism, and its kernel contains* $GE_2(A, \mathfrak{q})$ *and* $[GE_2(A), GL_2(A, \mathfrak{q})]$. *If* $\mathfrak{q}'$ *is a non zero ideal contained in* $\mathfrak{q}$, *then* κ *and* $\kappa|SL_2(A, \mathfrak{q}')$ *have the same image. Hence, if* $[\ ]$ *is not trivial, then* $\ker(\kappa)$ *contains no congruence subgroup* $SL_2(A, \mathfrak{q}')$, $\mathfrak{q}'\neq 0$.

Kubota proved this in the following case: A is of arithmetic type and totally imaginary, A contains $C=\mu_m$, $\mathfrak{q}$ is highly divisible by m, and $[\ ]=(-)_m$, which, according to Proposition 3.1, is a Mennicke symbol under these circumstances. The proof we give for the above generalization is inspired directly by Kubota's.

Proof. — We shall give the proof in several steps. $\alpha=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ always denotes an element of $GL_2(A, \mathfrak{q})$. We assume $\mathfrak{q}\neq 0$; otherwise the theorem is trivial. Lemma 2.11 will be used without explicit reference.

1) $\kappa(\alpha)=\begin{bmatrix}c\\d\end{bmatrix}=\begin{bmatrix}b\\d\end{bmatrix}^{-1}$. *In particular,* $\kappa({}^T\alpha)=\kappa(\alpha)^{-1}$, *where* ${}^T\alpha$ *denotes the transpose of* α.

For since $ad-bc$ is a unit, ad is congruent to a unit mod b, and bc is congruent to a unit mod d, so using Lemma 2.7 *a)*,

$$\kappa(a)=\begin{bmatrix}b\\a\end{bmatrix}=\begin{bmatrix}b\\ad\end{bmatrix}\begin{bmatrix}b\\d\end{bmatrix}^{-1}=\begin{bmatrix}b\\d\end{bmatrix}^{-1}=\begin{bmatrix}b\\d\end{bmatrix}^{-1}\begin{bmatrix}bc\\d\end{bmatrix}=\begin{bmatrix}c\\d\end{bmatrix}.$$

2) *If* $\varepsilon\in GE_2(A)$, *then* $\kappa(\varepsilon\alpha\varepsilon^{-1})=\kappa(\alpha)$.

It suffices to check this for a set of generators of $GE_2(A)$, so we can take ε either elementary or diagonal. If $\varepsilon=\begin{pmatrix}1&0\\t&1\end{pmatrix}$ then $\varepsilon\alpha\varepsilon^{-1}=\begin{pmatrix}a-tb&b\\*&*\end{pmatrix}$, so $\kappa(\varepsilon\alpha\varepsilon^{-1})=\begin{bmatrix}b\\a-tb\end{bmatrix}=\begin{bmatrix}b\\a\end{bmatrix}$. If $\varepsilon=\begin{pmatrix}1&t\\0&1\end{pmatrix}$ then $\varepsilon\alpha\varepsilon^{-1}=\begin{pmatrix}a_1&b_1\\c&d-tc\end{pmatrix}$, so, using (1), $\kappa(\varepsilon\alpha\varepsilon^{-1})=\begin{bmatrix}c\\d-tc\end{bmatrix}=\begin{bmatrix}c\\d\end{bmatrix}=\kappa(\alpha)$. If $\varepsilon=\begin{pmatrix}u&0\\0&v\end{pmatrix}$ then $\varepsilon\alpha\varepsilon^{-1}=\begin{pmatrix}a&uv^{-1}b\\vu^{-1}c&d\end{pmatrix}$ so

$$\kappa(\varepsilon\alpha\varepsilon^{-1})=\begin{bmatrix}uv^{-1}b\\a\end{bmatrix}=\begin{bmatrix}uv^{-1}bq\\a\end{bmatrix}=\begin{bmatrix}uv^{-1}q\\a\end{bmatrix}\begin{bmatrix}b\\a\end{bmatrix}=\begin{bmatrix}b\\a\end{bmatrix}=\kappa(\alpha),$$

where $q=1-a$, and we have used Lemma 2.2.

3) *If* $\varepsilon\in GE_2(A,\mathfrak{q})$ *then* $\kappa(\alpha\varepsilon)=\kappa(\alpha)$.

If ε is elementary or diagonal this follows from simple direct calculations very similar to those just above. Clearly

$$H=\{\varepsilon\in GL_2(A,\mathfrak{q})\,|\,\kappa(\alpha\varepsilon)=\kappa(\alpha)\quad\text{for all}\quad\alpha\in GL_2(A,\mathfrak{q})\}$$

is a group. Therefore, since H contains elementary and diagonal matrices, it will contain $GE_2(A,\mathfrak{q})$ provided it is normalized by $GE_2(A)$. So suppose $\tau\in GE_2(A)$ and $\varepsilon\in H$. Then

$$\begin{aligned}\kappa(\alpha\tau\varepsilon\tau^{-1})&=\kappa(\tau^{-1}\alpha\tau\varepsilon)&&\text{(by 2))}\\&=\kappa(\tau^{-1}\alpha\tau)&&(\varepsilon\in H)\\&=\kappa(\alpha)&&\text{(by 2)).}\end{aligned}$$

4) *Suppose* $\alpha=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ *and* $\alpha'=\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}$ *in* $GL_2(A,\mathfrak{q})$ *are such that* $d\equiv 1\equiv a'$ mod q *for some* $q\in\mathfrak{q}$, *and such that* $dA+a'A=A$. *Then*

$$\kappa(\alpha'\alpha)=\kappa(\alpha')\kappa(\alpha).$$

We shall use the following remark: If $x\in A$ and $y\in\mathfrak{q}$ are prime to a' then $\begin{bmatrix}xy\\a'\end{bmatrix}=\begin{bmatrix}xq\\a'\end{bmatrix}\begin{bmatrix}y\\a'\end{bmatrix}$, and similarly for d. For $\begin{bmatrix}q\\a'\end{bmatrix}=1$, so $\begin{bmatrix}xy\\a'\end{bmatrix}=\begin{bmatrix}xy\\a'\end{bmatrix}\begin{bmatrix}q\\a'\end{bmatrix}=\begin{bmatrix}xyq\\a'\end{bmatrix}=\begin{bmatrix}xq\\a'\end{bmatrix}\begin{bmatrix}y\\a'\end{bmatrix}$.

Now $\alpha'\alpha=\begin{pmatrix}a'a+b'c&a'b+b'd\\*&*\end{pmatrix}$, so

$$\kappa(\alpha'\alpha)=\begin{bmatrix}a'b+b'd\\ a'a+b'c\end{bmatrix}$$

$$=\begin{bmatrix}a'b+b'd\\ (a'a+b'c)d\end{bmatrix}\begin{bmatrix}a'b+b'd\\ d\end{bmatrix}^{-1} \qquad (d \text{ is prime to } a')$$

$$=\begin{bmatrix}a'b+b'd\\ a'u+c(a'b+b'd)\end{bmatrix}\begin{bmatrix}a'b\\ d\end{bmatrix}^{-1} \qquad (u=ad-bc)$$

$$=\begin{bmatrix}a'b+b'd\\ a'u\end{bmatrix}\begin{bmatrix}a'q\\ d\end{bmatrix}^{-1}\begin{bmatrix}b\\ d\end{bmatrix}^{-1} \qquad \text{(remark above)}$$

$$=\begin{bmatrix}b'd\\ a'u\end{bmatrix}\begin{bmatrix}a'q\\ d\end{bmatrix}^{-1}\kappa(\alpha) \qquad \text{(by 1))}$$

$$=\begin{bmatrix}b'd\\ u\end{bmatrix}\begin{bmatrix}b'\\ a'\end{bmatrix}\begin{bmatrix}dq\\ a'\end{bmatrix}\begin{bmatrix}a'q\\ d\end{bmatrix}^{-1}\kappa(\alpha) \qquad \text{(remark above)}$$

$$=\kappa(\alpha')\kappa(\alpha) \qquad \text{(Lemma 2.10; } u \text{ is a unit).}$$

5) κ *is a homomorphism.*

Given $\alpha, \alpha' \in GL_2(A, \mathfrak{q})$ we must show that $\kappa(\alpha'\alpha)=\kappa(\alpha')\kappa(\alpha)$. If $\alpha=\alpha_1\alpha_2$ with $\alpha_2 \in GE_2(A, \mathfrak{q})$ then, using 3), we have $\kappa(\alpha'\alpha)=\kappa(\alpha'\alpha_1)$, and $\kappa(\alpha)=\kappa(\alpha_1)$, so it suffices to deal with α_1. In this way we can first arrange that $\alpha \in SL_2(A, \mathfrak{q})$.

Write $a'=1+q$. If $q=0$ then our assertion follows from 4). If $q\neq 0$ then A/qA is semi-local, so it follows from [1, Corollary 5.2] that $SL_2(A, \mathfrak{q})=SL_2(A, qA).E_2(A, \mathfrak{q})$. Hence we can find an $\varepsilon_1 \in E_2(A, \mathfrak{q})$ such that $\alpha\varepsilon_1=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\in SL_2(A, qA)$. Since $d_1A+c_1A=A=d_1A+c_1^2A$ we can find a $d_2=d_1+tc_1^2$ $(t\in A)$ which is prime to a' (see remark before (2.2)). Setting $\varepsilon_2=\begin{pmatrix}1 & c_1t\\ 0 & 1\end{pmatrix}\in E_2(A, qA)$, we have now achieved the hypotheses of 4) for $\alpha\varepsilon_1\varepsilon_2$ and α'. Applying 3) and 4) therefore, we have

$$\kappa(\alpha'\alpha)=\kappa(\alpha'\alpha\varepsilon_1\varepsilon_2)=\kappa(\alpha')\kappa(\alpha\varepsilon_1\varepsilon_2)=\kappa(\alpha')\kappa(\alpha).$$

6) $\ker \kappa \supset GE_2(A, \mathfrak{q})$ *and* $[GE_2(A), GL_2(A, \mathfrak{q})]$.

This follows respectively from 3) and 2).

The last assertion of Kubota's Theorem follows from Lemma 2.3, so its proof is now complete.

§ 7. Review of the stable structure of $GL_n(A)$.

Let A be a commutative ring, and let $\mathfrak{q}$ be an ideal in A. We call an element $(a_1, \ldots, a_m)\in A^m$ $\mathfrak{q}$-unimodular if $(a_1, a_2, \ldots, a_m)\equiv(1, 0, \ldots, 0) \bmod \mathfrak{q}$, and if

$$\sum_i Aa_i = A.$$

When $\mathfrak{q}=A$ we just say *unimodular.* When $m=2$ the $\mathfrak{q}$-unimodular elements are just the elements of $W_{\mathfrak{q}}$. Thus, it follows immediately from Lemma 5.3, that:

(7.1) $SL_2(A, \mathfrak{q})$ *operates transitively on the* $\mathfrak{q}$*-unimodular elements in* A^2.

Throughout the balance of this chapter we shall deal extensively with the following condition, some of whose implications we shall record in this section.

$(7.2)_n$ *If* $m \geq n$, *if* $\mathfrak{q}$ *is an ideal in* A, *and if* $(a_1, \ldots, a_m)$ *is* $\mathfrak{q}$*-unimodular in* A^m, *then there exist* $a_i' = a_i + t_i a_m$, *with* $t_i \in \mathfrak{q}$, $1 \leq i < m$, *such that* $(a_1', \ldots, a_{m-1}')$ *is* $\mathfrak{q}$*-unimodular in* A^{m-1}.

Clearly this condition is reasonable only for $n \geq 2$. If we require $(7.2)_n$ only for the unit ideal, $\mathfrak{q} = A$, then $(7.2)_n$ becomes the condition that " $n-1$ defines a stable range for GL(A) " in the sense of [1, § 4].

Lemma 7.3. — *If we require* $(7.2)_n$ *only for* $\mathfrak{q} = A$ *then it follows for all ideals* $\mathfrak{q}$.

Proof. — If $(a_1, \ldots, a_m)$ is $\mathfrak{q}$-unimodular then clearly $(a_1, \ldots, a_{m-1}, a_m^2)$ is still unimodular. By hypothesis, therefore, we can find $a_i' = a_i + t_i a_m^2$, $1 \leq i < m$, such that $(a_1', \ldots, a_{m-1}')$ is unimodular. It is automatically $\mathfrak{q}$-unimodular, so we solve our problem with the $s_i = t_i a_m \in \mathfrak{q}$, $1 \leq i < m$.

By virtue of this lemma it now follows from [1, Theorem 11.1] that:

Theorem 7.4. — *If the maximal ideal space of* A *is a noetherian space of dimension* $\leq d$ (e.g. *if* A *is a noetherian ring of Krull dimension* $\leq d$) *then* A *satisfies* $(7.2)_n$ *for all* $n \geq d+2$.

The force of $(7.2)_n$ derives largely from the following theorem [1, Theorem 4.2], which we will strengthen in § 11.

Theorem 7.5. — *Assume* $(7.2)_n$. *For all ideals* $\mathfrak{q}$, *and for all* $m \geq n$:

a) $E_m(A, \mathfrak{q})$ *operates transitively on each congruence class modulo* $\mathfrak{q}$ *of unimodular elements in* A^m.

b) $GL_m(A, \mathfrak{q}) = GL_{n-1}(A, \mathfrak{q}) \cdot E_m(A, \mathfrak{q})$.

c) $E_m(A, \mathfrak{q})$ *is a normal subgroup of* $GL_m(A)$.

d) $[GE_m(A), GL_m(A, \mathfrak{q})] \subset E_m(A, \mathfrak{q})$. *In case* $m \geq 3$ *we have*

$$E_m(A, \mathfrak{q}) = [E_m(A), E_m(A, \mathfrak{q})],$$

so the above inclusion becomes equality. If moreover, $m \geq 2(n-1)$, *then*

$$[GL_m(A), GL_m(A, \mathfrak{q})] = E_m(A, \mathfrak{q}).$$

Suppose $m \geq n$ *and* $m \geq 3$:

e) *If* $H \subset GL_m(A)$ *is a subgroup normalized by* $E_m(A)$ *then there is a unique ideal* $\mathfrak{q}$ *such that* $E_m(A, \mathfrak{q}) \subset H$ *and such that* H *maps into the center of* $GL_m(A/\mathfrak{q})$.

This differs in formulation from [1, Theorem 4.2] only in part *d)*. The proof of [1, Theorem 4.2] proves *d)* as stated provided we replace $GE_m(A)$ above by $E_m(A)$. The fact that we can put $GE_m(A)$ there follows immediately from part *b)* plus the fact that $GE_m(A)$ is generated by $E_m(A)$ and the matrices $\mathrm{diag}(1, \ldots, 1, u)$, u a unit, because the latter commute with $GL_{n-1}(A, \mathfrak{q})$.

§ 8. The construction of κ_{n+1}.

To prove part *c)* of Theorem 4.1 we want to extend the homomorphism $\kappa_2 : GL_2(A, \mathfrak{q}) \to C$ given by Kubota's Theorem, to a homomorphism $\kappa_n : GL_n(A, \mathfrak{q}) \to C$. Once this is accomplished part *a)* of Theorem 4.1 will follow easily from the results

quoted in § 7. We shall extend κ_2 in two steps. First we shall show that it extends to a homomorphism $\kappa_3 : GL_3(A, \mathfrak{q}) \to C$ which satisfies several conditions. Then we shall show, in a rather general setting, that a homomorphism $\kappa_n : GL_n(A, \mathfrak{q}) \to C$, satisfying such conditions, extends to a homomorphism $\kappa_{n+1} : GL_{n+1}(A, \mathfrak{q}) \to C$ which satisfies analogous conditions. Before stating our results we must enumerate the conditions in question.

Two of the conditions will be imposed on A and n. The first is condition $(7.2)_n$ of the last section, and the second is:

$(8.1)_n$ *For every ideal* $\mathfrak{q}$, $GL_n(A, \mathfrak{q})$ *operates transitively on the* $\mathfrak{q}$*-unimodular elements of* A^n.

By virtue of Theorem 7.5 *a)* we have $(7.2)_n \Rightarrow (8.1)_m$ for $m \geq n$, but we shall require $(7.2)_n$ together with $(8.1)_{n-1}$.

Next we shall consider conditions on a homomorphism $\kappa_n : GL_n(A, \mathfrak{q}) \to C$. It is assumed throughout that $n \geq 2$.

$(8.2)_n$ $\kappa_n(\varepsilon) = 1$ *if* ε *lies in* $[GE_n(A), GL_n(A, \mathfrak{q})]$ *or in* $E_n(A, \mathfrak{q})$.

If $n \geq 3$ then (5.1) permits us to delete $E_n(A, \mathfrak{q})$ in this condition. Conversely, assuming $(7.2)_n$, Theorem 7.5 *d)* permits us to delete $[GE_n(A), GE_n(A, \mathfrak{q})]$.

$(8.3)_n$ *If* $\kappa_n(\sigma) = 1$ *then* $\kappa_n({}^T\sigma) = 1$.

Here ${}^T\sigma$ denotes the transpose of σ.

To state the last condition we make a definition. Let $\alpha, \alpha' \in GL_n(A, \mathfrak{q})$ and let $t \in \mathfrak{q}$. We shall say that α' is $(\mathfrak{q}, t)$*-related to* α if α' can be written in the form

$$\alpha = \begin{pmatrix} 1 + ta'_{11} & a'_{12} & \dots & a'_{1n} \\ ta'_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ ta'_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \quad \text{and} \quad \alpha' = \begin{pmatrix} 1 + ta'_{11} & ta'_{12} & \dots & ta'_{1n} \\ a'_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a'_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

with $a'_{11} \in \mathfrak{q}$. Note that this is not a symmetric relation.

Our last condition is:

$(8.4)_n$ If $t \in \mathfrak{q}$ and if α' is $(\mathfrak{q}, t)$-related to α in $GL_n(A, \mathfrak{q})$ then $\kappa_n(\alpha') = \kappa_n(\alpha)$.

Proposition 8.5. — Suppose we have the assumptions of Kubota's theorem (Theorem 6.1). Then A *satisfies* $(7.2)_n$ *for* $n \geq 3$ *and* $(8.1)_n$ *for* $n \geq 2$. *Moreover the homomorphism* $\kappa_2 : GL_2(A, \mathfrak{q}) \to C$ *constructed in Kubota's theorem extends uniquely to a homomorphism* $\kappa_3 : GL_3(A, \mathfrak{q}) \to C$ *satisfying* $(8.2)_3$, *and* κ_3 *also satisfies* $(8.3)_3$ *and* $(8.4)_3$.

Proposition 8.6. — Let A *be a commutative ring satisfying* $(7.2)_n$ *and* $(8.1)_{n-1}$, *and let* $\mathfrak{q}$ *be an ideal of* A. *Then given a homomorphism* $\kappa_n : GL_n(A, \mathfrak{q}) \to C$ *satisfying* $(8.2)_n$, $(8.3)_n$, *and* $(8.4)_n$, *it has a unique extension* $\kappa_{n+1} : GL_{n+1}(A, \mathfrak{q}) \to C$ *satisfying* $(8.2)_{n+1}$, *and* κ_{n+1} *also satisfies* $(8.3)_{n+1}$ *and* $(8.4)_{n+1}$.

Proposition 8.6 does not apply to κ_2 in Kubota's Theorem because A need not satisfy $(7.2)_2$. However it does apply to the κ_3 supplied by Proposition 8.5, and to all the κ_n thereafter. Hence the proof of part *c)* of Theorem 4.1 will be achieved with the proof of these two propositions. This proof occupies §§ 8-10. The two propositions

will be proved simultaneously, except for the very last stage of the argument. This is made possible because of:

Lemma 8.7. — Let A *be a Dedekind ring.*

a) A *satisfies* $(7.2)_n$ *for* $n\geq 3$ *and* $(8.1)_n$ *for* $n\geq 2$.

b) *The homomorphism* K_2 *constructed in Kubota's theorem satisfies* $(8.2)_2$, $(8.3)_2$, *and* $(8.4)_2$.

Proof. — a) A Dedekind ring is a noetherian ring of Krull dimension ≤ 1, so Theorem 7.4 implies A satisfies $(7.2)_n$ for $n\geq 3$, and hence, by Theorem 7.5 *a)*, it satisfies $(8.1)_n$ for $n\geq 3$. Condition $(8.1)_2$ follows from (7.1).

b) The statement of Kubota's Theorem contains $(8.2)_2$, and step (1) of its proof implies $(8.3)_2$. For $(8.4)_2$, suppose $t\in\mathfrak{q}$ and suppose $\alpha'=\begin{pmatrix}1+ta' & tb'\\ c' & d\end{pmatrix}$ is $(\mathfrak{q}, t)$-related to $\alpha=\begin{pmatrix}1+ta' & b'\\ tc' & d\end{pmatrix}$ in $GL_2(A, \mathfrak{q})$. Then

$$K_2(\alpha')=\begin{bmatrix}tb'\\ 1+ta'\end{bmatrix}=\begin{bmatrix}t\\ 1+ta'\end{bmatrix}\begin{bmatrix}b'\\ 1+ta'\end{bmatrix}=\begin{bmatrix}b'\\ 1+ta'\end{bmatrix}=K_2(\alpha).\quad \text{Q.E.D.}$$

Henceforth until the end of § 10 A may be any commutative ring, and $\mathfrak{q}$ any ideal in A. The following lemma will help us verify $(8.4)_{n+1}$ for K_{n+1}.

Lemma 8.8. — Suppose $t\in\mathfrak{q}$ *and suppose* α' *and* β' *are* $(\mathfrak{q}, t)$*-related to* α, *resp.* β. *Then*

a) $\alpha'\beta'$ *is* $(\mathfrak{q}, t)$*-related to* $\alpha\beta$.

b) $\alpha^{-1}\alpha'\in[E_{n+1}(A), GL_{n+1}(A, \mathfrak{q})]$. *In particular,* $\det\alpha'=\det\alpha$.

Proof. — a) Write $\alpha=\begin{pmatrix}\alpha_{11} & \alpha_{12}\\ t\alpha_{21} & \alpha_{22}\end{pmatrix}$ and $\alpha'=\begin{pmatrix}\alpha_{11} & t\alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{pmatrix}$ in block form, with $\alpha_{11}=1+ta'_{11}$, $\alpha_{22}=\begin{pmatrix}a_{22} & \cdots & a_{2n}\\ \vdots & & \vdots\\ a_{n2} & \cdots & a_{nn}\end{pmatrix}$, etc. Similarly write

$$\beta=\begin{pmatrix}\beta_{11} & \beta_{12}\\ t\beta_{21} & \beta_{22}\end{pmatrix}\qquad\text{and}\qquad\beta'=\begin{pmatrix}\beta_{11} & t\beta_{12}\\ \beta_{21} & \beta_{22}\end{pmatrix}.$$

Then
$$\alpha\beta=\begin{pmatrix}\alpha_{11}\beta_{11}+t\alpha_{12}\beta_{21} & \alpha_{11}\beta_{12}+\alpha_{12}\beta_{22}\\ t(\alpha_{21}\beta_{11}+\alpha_{22}\beta_{21}) & t\alpha_{21}\beta_{12}+\alpha_{22}\beta_{22}\end{pmatrix}$$

and
$$\alpha'\beta'=\begin{pmatrix}\alpha_{11}\beta_{11}+t\alpha_{12}\beta_{21} & t(\alpha_{11}\beta_{12}+\alpha_{12}\beta_{22})\\ \alpha_{21}\beta_{11}+\alpha_{22}\beta_{21} & t\alpha_{21}\beta_{12}+\alpha_{22}\beta_{22}\end{pmatrix}.$$

b) The first column of α is $\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}+t\gamma$, where $\gamma=\begin{pmatrix}a'_{11}\\ \vdots\\ a'_{n1}\end{pmatrix}$. Set $\bar{\alpha}=\begin{pmatrix}\alpha & -\gamma\\ 0 & 1\end{pmatrix}$, and $\varepsilon=\begin{pmatrix}0 & 0 & 1\\ 0 & I_{n-1} & 0\\ -1 & 0 & t\end{pmatrix}\in E_{n+1}(A)$. A direct calculation shows that

$$\bar{\alpha}^{\varepsilon}=\varepsilon^{-1}\bar{\alpha}\varepsilon=\bar{\alpha}'=\begin{pmatrix}\alpha' & 0\\ \rho & 1\end{pmatrix},$$

where $\rho=(a'_{11}, \ldots, a'_{1n})$. Hence $\bar{\alpha}^{-1}\bar{\alpha}'=[\bar{\alpha}, \varepsilon]\in[E_{n+1}(A), GL_{n+1}(A, \mathfrak{q})]$. Evidently if we write $\alpha=\bar{\alpha}\varepsilon_1$ and $\alpha'=\bar{\alpha}'\varepsilon_2$ then $\varepsilon_1, \varepsilon_2\in E_{n+1}(A, \mathfrak{q})$, and since $n+1\geq 3$, (5.1) implies $E_{n+1}(A, \mathfrak{q})\subset[E_{n+1}(A), GL_{n+1}(A, \mathfrak{q})]$. Therefore

$$\alpha^{-1}\alpha'=\varepsilon_1^{-1}\bar{\alpha}^{-1}\bar{\alpha}'\varepsilon_2\in[E_{n+1}(A), GL_{n+1}(A, \mathfrak{q})].$$

The construction of κ_{n+1} will be based upon the next lemma. We shall say an element σ of $GL_{n+1}(A)$ is of *type* L if its last row is $(0, \ldots, 0, 1)$, and of *type* R if its first column is $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$. One of type L thus looks like

$$\bar{\alpha}=\begin{pmatrix}\alpha & \gamma\\ 0 & 1\end{pmatrix}$$

with $\alpha\in GL_n(A)$, γ an n-column; etc. Similarly a type R has the form

$$\bar{\beta}=\begin{pmatrix}1 & \rho\\ 0 & \beta\end{pmatrix}$$

with $\beta\in GL_n(A)$, ρ an n-row, etc.

Lemma 8.9. — *Assume* $(7.2)_{n+1}$ *and* $(8.1)_n$.

a) *Any* $\sigma\in GL_{n+1}(A, \mathfrak{q})$ *can be factored in* $GL_{n+1}(A, \mathfrak{q})$ *as*

$$\sigma=\bar{\alpha}\varepsilon\bar{\beta}$$

where $\bar{\alpha}$ *is of type* L, $\varepsilon=I+te_{n+1,1}$ *for some* $t\in\mathfrak{q}$, *and* $\bar{\beta}$ *is of type* R. *We shall call such a representation a " standard form " for* σ.

b) *Suppose* $t\in\mathfrak{q}$ *and suppose that* σ' *is* $(\mathfrak{q}, t)$*-related to* σ *in* $GL_{n+1}(A, \mathfrak{q})$. *Then* $\sigma^{-1}\sigma'\in E_{n+1}(A, \mathfrak{q})$.

Remark. — The ε in part *a)* is unique because t is the coefficient $a_{n+1,1}$ of σ.

Proof. — *a)* Say σ has first column $\sigma_1=\begin{pmatrix}a_1\\\vdots\\a_{n+1}\end{pmatrix}$. Using $(7.2)_{n+1}$ we can find $\bar{\gamma}=\begin{pmatrix}I_n & \gamma\\ 0 & 1\end{pmatrix}\in E_{n+1}(A, \mathfrak{q})$ such that $\bar{\gamma}\sigma_1=\begin{pmatrix}a'_1\\\vdots\\a'_n\\a_{n+1}\end{pmatrix}$ with $\sigma'_1=\begin{pmatrix}a'_1\\\vdots\\a'_n\end{pmatrix}$ $\mathfrak{q}$-unimodular. Then $(8.1)_n$ gives us an $\alpha_1\in GL_n(A, \mathfrak{q})$ such that $\alpha_1\sigma'_1=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$. Set $\bar{\alpha}_1=\begin{pmatrix}\alpha_1 & 0\\ 0 & 1\end{pmatrix}$ and $\varepsilon=I+a_{n+1}e_{n+1,1}$. Then $\varepsilon^{-1}\bar{\alpha}_1\bar{\gamma}\sigma_1=\varepsilon^{-1}\begin{pmatrix}1\\0\\\vdots\\0\\a_{n+1}\end{pmatrix}=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$, so $\bar{\beta}=\varepsilon^{-1}\bar{\alpha}_1\bar{\gamma}\sigma=\begin{pmatrix}1 & \rho\\ 0 & \beta\end{pmatrix}$ is of type R. Finally, $\sigma=\bar{\alpha}\varepsilon\bar{\beta}$, where $\bar{\alpha}=\bar{\gamma}^{-1}\bar{\alpha}_1^{-1}=\begin{pmatrix}\alpha_1^{-1} & -\gamma\\ 0 & 1\end{pmatrix}$ is of type L and in $GL_{n+1}(A, \mathfrak{q})$.

b) We are given a σ' that is $(\mathfrak{q}, t)$-related to σ. Thus, in the argument above, σ_1 is actually $(t\mathfrak{q})$-unimodular, so we can choose $\bar{\gamma}$ and $\bar{\alpha}_1$ in $\mathrm{GL}_{n+1}(A, t\mathfrak{q})$. The result will be a standard form, $\sigma = \bar{\alpha}\varepsilon\bar{\beta}$, in which $\bar{\alpha}$ and $\varepsilon = I + a_{n+1}e_{n+1,1}$ have $(t\mathfrak{q})$-unimodular first columns. This permits us to define $\bar{\alpha}' = \begin{pmatrix} \alpha' & \gamma' \\ 0 & 1 \end{pmatrix}$ and $\varepsilon' = I + a'_{n+1}e_{n+1,1}$ which are $(\mathfrak{q}, t)$-related to $\bar{\alpha}$, resp. ε. Similarly, $\bar{\beta}' = \begin{pmatrix} 1 & t\rho \\ 0 & \beta \end{pmatrix}$ is $(\mathfrak{q}, t)$-related to $\bar{\beta}$, so Lemma 8.8 *a)* implies that $\bar{\alpha}\varepsilon'\bar{\beta}'$ is $(\mathfrak{q}, t)$-related to $\sigma = \bar{\alpha}\varepsilon\bar{\beta}$.

Our hypothesis $(7.2)_{n+1}$, and Theorem 7.5, imply that $\mathrm{E}_{n+1}(A, \mathfrak{q})$ is a normal subgroup of $\mathrm{GL}_{n+1}(A)$ containing $[\mathrm{GE}_{n+1}(A), \mathrm{GL}_{n+1}(A, \mathfrak{q})]$. It is clear that $\varepsilon' \equiv \varepsilon$ and $\bar{\beta}' \equiv \bar{\beta}$ modulo $\mathrm{E}_{n+1}(A, \mathfrak{q})$, and it follows from Lemma 8.8 *b)* that $\bar{\alpha}' \equiv \alpha' \equiv \alpha$ modulo $\mathrm{E}_{n+1}(A, \mathfrak{q})$. Therefore $\bar{\alpha}'\varepsilon'\bar{\beta}' \equiv \bar{\alpha}\varepsilon\bar{\beta} = \sigma$ modulo $\mathrm{E}_{n+1}(A, \mathfrak{q})$.

Now σ' and $\bar{\alpha}'\varepsilon'\bar{\beta}'$ are both $(\mathfrak{q}, t)$-related to σ, so they differ at most in the first row. (They may differ if t is a zero divisor.) Hence $\bar{\alpha}'\varepsilon'\bar{\beta}'(\sigma')^{-1}$ differs from I_{n+1} at most in the first row. Since, by Lemma 8.8 *b)*, $\det \sigma' = \det \sigma = \det(\bar{\alpha}'\varepsilon'\bar{\beta}')$, it follows that $\bar{\alpha}'\varepsilon'\bar{\beta}'(\sigma')^{-1} \in \mathrm{E}_{n+1}(A, \mathfrak{q})$, so $\sigma' \equiv \sigma$ modulo $\mathrm{E}_{n+1}(A, \mathfrak{q})$.

Corollary 8.10 (Uniqueness). — *Assume* $(7.2)_{n+1}$ *and* $(8.1)_n$, *and let*

$$\kappa_n : \mathrm{GL}_n(A, \mathfrak{q}) \to C$$

be a homomorphism satisfying $(8.3)_n$. *Then there is at most one homomorphism*

$$\kappa_{n+1} : \mathrm{GL}_{n+1}(A, \mathfrak{q}) \to C$$

extending κ_n *and satisfying* $(8.2)_{n+1}$. *Moreover* κ_{n+1} *must also satisfy* $(8.3)_{n+1}$ *and* $(8.4)_{n+1}$.

Proof. — $(7.2)_{n+1}$ and Theorem 7.5 *b)* imply that

$$\mathrm{GL}_{n+1}(A, \mathfrak{q}) = \mathrm{GL}_n(A, \mathfrak{q}) \cdot \mathrm{E}_{n+1}(A, \mathfrak{q}).$$

The map κ_{n+1} agrees with κ_n on $\mathrm{GL}_n(A, \mathfrak{q})$, and, by $(8.2)_{n+1}$, annihilates $\mathrm{E}_{n+1}(A, \mathfrak{q})$; hence it is unique. To verify $(8.3)_{n+1}$, i.e. that $\kappa_{n+1}({}^T\sigma) = \kappa_{n+1}(\sigma)$, it is enough to do so for generators of $\mathrm{GL}_{n+1}(A, \mathfrak{q})$. On $\mathrm{GL}_n(A, \mathfrak{q})$ this follows from $(8.3)_n$, and if $\sigma \in \mathrm{E}_{n+1}(A, \mathfrak{q})$ then likewise for ${}^T\sigma$. Finally, $(8.4)_{n+1}$ follows immediately from $(8.2)_{n+1}$ and Lemma 8.9 *b)*, which our hypotheses permit us to invoke.

Henceforth we shall assume we are given A, $\mathfrak{q}$, and $\kappa_n : \mathrm{GL}_n(A, \mathfrak{q}) \to C$ satisfying $(7.2)_{n+1}$, $(8.1)_n$, $(8.2)_n$, $(8.3)_n$, and $(8.4)_n$. (Recall that $(7.2)_{n+1}$ and $(8.1)_n$ are both consequences of $(7.2)_n$.) We seek to construct a homomorphism $\kappa_{n+1} : \mathrm{GL}_{n+1}(A, \mathfrak{q}) \to C$ which extends κ_n and satisfies $(8.2)_{n+1}$. Once this is done it will follow from Corollary 8.10 that we have proved both Proposition 8.5 and 8.6.

Lemma 8.11 (Definition of κ_{n+1}*).* — *Suppose* $\sigma \in \mathrm{GL}_{n+1}(A, \mathfrak{q})$ *has a standard form* $\sigma = \bar{\alpha}\varepsilon\bar{\beta}$ *with*

$$\bar{\alpha} = \begin{pmatrix} \alpha & \gamma \\ 0 & 1 \end{pmatrix} \qquad \textit{and} \qquad \bar{\beta} = \begin{pmatrix} 1 & \rho \\ 0 & \beta \end{pmatrix}.$$

Then

$$\kappa_{n+1}(\sigma)=\kappa_n(\alpha)\kappa_n(\beta)$$

depends only on σ, *and* $\kappa_{n+1}|\mathrm{GL}_n(A, \mathfrak{q})=\kappa_n$.

Proof. — Suppose $\bar{\alpha}_1\varepsilon_1\bar{\beta}_1=\sigma=\bar{\alpha}_2\varepsilon_2\bar{\beta}_2$ are two standard forms. We claim that $\kappa_n(\alpha_1)\kappa_n(\beta_1)=\kappa_n(\alpha_2)\kappa_n(\beta_2)$, i.e. that $\kappa_n(\alpha)=\kappa_n(\beta)$, where $\alpha=\alpha_2^{-1}\alpha_1=(a_{ij})$ and $\beta=\beta_2\beta_1^{-1}=(b_{ij})$. Setting $\bar{\alpha}=\bar{\alpha}_2^{-1}\bar{\alpha}_1=\begin{pmatrix}\alpha & \gamma\\ 0 & 1\end{pmatrix}$ and $\bar{\beta}=\bar{\beta}_2\bar{\beta}_1^{-1}=\begin{pmatrix}1 & \rho\\ 0 & \beta\end{pmatrix}$ we have $\bar{\alpha}\varepsilon_1=\varepsilon_2\bar{\beta}$. Say $\varepsilon_1=I+te_{n+1,1}$, $\varepsilon_2=I+se_{n+1,1}$, $\gamma=\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$, and $\rho=(r_1, \ldots, r_n)$.

$$\bar{\alpha}\varepsilon_1=\begin{pmatrix}\alpha+\gamma(t, 0, \ldots, 0) & \gamma\\ t\ 0\ .\ .\ .\ 0 & 1\end{pmatrix}=\begin{pmatrix}a_{11}+c_1t & a_{12}\ \ldots\ a_{1n} & c_1\\ \vdots & \vdots\ \ \vdots & \vdots\\ a_{n1}+c_nt & a_{n2}\ \ldots\ a_{nn} & c_n\\ t & 0\ \ldots\ 0 & 1\end{pmatrix}.$$

$$\varepsilon_2\bar{\beta}=\begin{pmatrix}1 & & \rho\\ 0 & & \\ \vdots & & \\ 0 & \beta+\begin{pmatrix}0\\ \vdots\\ 0\\ s\end{pmatrix}\cdot\rho & \\ s & & \end{pmatrix}=\begin{pmatrix}1 & r_1\ .\ .\ .\ r_n\\ 0 & b_{11}\ .\ .\ .\ b_{1n}\\ \vdots & \cdot\ \ \ \cdot\\ 0 & \cdot\ \ \ \cdot\\ s & b_{n1}+sr_1\ \ldots\ b_{nn}+sr_n\end{pmatrix}$$

Therefore $s=t$ and $c_1=r_n$, and if we set $a'_{i1}=-c_i$ $(1<i\leq n)$ and $a'_{1j}=r_j$ $(1\leq j<n)$ we have

$$\alpha=\begin{pmatrix}1-c_1t & r_1\ \ldots\ r_{n-1}\\ -c_2t & a_{22}\ \ \ a_{2n}\\ \vdots & \\ -c_nt & a_{n2}\ \ \ a_{nn}\end{pmatrix}=\begin{pmatrix}1+ta'_{11} & a'_{12}\ \ldots\ a'_{1n}\\ ta'_{21} & a_{22}\ \ldots\ a_{2n}\\ \vdots & \vdots\ \ \ \vdots\\ ta'_{n1} & a_{n2}\ \ldots\ a_{nn}\end{pmatrix}$$

and

$$\beta=\begin{pmatrix}a_{22}\ \ldots\ a_{2n} & c_2\\ \vdots\ \ \ \vdots & \\ a_{n2}\ \ldots\ a_{nn} & c_n\\ -tr_1\ \ldots\ -tr_{n-1} & 1-tr_n\end{pmatrix}=\begin{pmatrix}a_{22}\ \ldots\ a_{2n} & -a'_{21}\\ \\ a_{n2}\ \ldots\ a_{nn} & -a'_{n1}\\ -ta'_{12}\ \ldots\ -ta'_{1n} & 1+ta'_{11}\end{pmatrix}$$

With $\pi=\begin{pmatrix}0 & \cdots & 0 & -1\\ 1 & 0\cdots & \cdot & 0\\ \cdot & 1 & \cdot\ \cdot & \cdot\\ \cdot & \cdot & \cdot\ \cdot & \cdot\\ 0 & \cdots 0 & 1 & \cdot\ 0\end{pmatrix}\in\mathrm{GE}_n(A)$ we have

$$\pi\beta\pi^{-1}=\begin{pmatrix}1+ta'_{11} & ta'_{12}\ \ldots\ ta'_{1n}\\ a'_{21} & a_{22}\ \ldots\ a_{2n}\\ \vdots & \vdots\ \ \ \vdots\\ a'_{n1} & a_{n2}\ \ldots\ a_{nn}\end{pmatrix},$$ which is $(\mathfrak{q}, t)$-related to α.

Therefore $\kappa_n(\beta)=\kappa_n(\pi\beta\pi^{-1})$ by $(8.2)_n$, and $\kappa_n(\pi\beta\pi^{-1})=\kappa_n(\alpha)$ by $(8.4)_n$. Finally, the fact that κ_{n+1} extends κ_n is clear.

We close this section with a corollary of the definition of κ_{n+1}.

Lemma 8.12. — *If* $\overline{\alpha}_1, \sigma, \overline{\beta}_1 \in GL_{n+1}(A, \mathfrak{q})$ *with* $\overline{\alpha}_1$ *of type* L *and* $\overline{\beta}_1$ *of type* R, *then*

$$\kappa_{n+1}(\overline{\alpha}_1\sigma\overline{\beta}_1) = \kappa_{n+1}(\overline{\alpha}_1)\kappa_{n+1}(\sigma)\kappa_{n+1}(\overline{\beta}_1).$$

Proof. — If $\sigma = \overline{\alpha}\varepsilon\overline{\beta}$ in standard form then, with an obvious choice of notation,

$$\overline{\alpha}_1\overline{\alpha} = \begin{pmatrix} \alpha_1\alpha & * \\ 0 & 1 \end{pmatrix}$$

is of type L, and

$$\overline{\beta}\,\overline{\beta}_1 = \begin{pmatrix} 1 & * \\ 0 & \beta\beta_1 \end{pmatrix}$$

is of type R. Hence $\overline{\alpha}_1\sigma\overline{\beta}_1 = (\overline{\alpha}_1\overline{\alpha})\varepsilon(\overline{\beta}\,\overline{\beta}_1)$ is a standard form for $\overline{\alpha}_1\sigma\overline{\beta}_1$, so $\kappa_{n+1}(\overline{\alpha}_1\sigma\overline{\beta}_1) = \kappa_n(\alpha_1\alpha)\kappa_n(\beta\beta_1) = \kappa_n(\alpha_1)\kappa_n(\alpha)\kappa_n(\beta)\kappa_n(\beta_1) = \kappa_{n+1}(\overline{\alpha}_1)\kappa_{n+1}(\sigma)\kappa_{n+1}(\overline{\beta}_1)$.

§ 9. The normalizer of κ_{n+1}.

Given A, $\mathfrak{q}$, and a homomorphism $\kappa_n : GL_n(A, \mathfrak{q}) \to C$, satisfying $(7.2)_{n+1}$, $(8.1)_n$, $(8.2)_n$, $(8.3)_n$ and $(8.4)_n$, we have constructed (Lemma 8.11) a map, $\kappa_{n+1} : GL_{n+1}(A, \mathfrak{q}) \to C$, extending κ_n. We seek to show, under the hypotheses of either Proposition 8.5 or Proposition 8.6, that the map κ_{n+1} is a homomorphism satisfying $(8.2)_{n+1}$. The remarks after Corollary 8.10 show that this will suffice to prove Propositions 8.5 and 8.6.

Write

$$H = \{\sigma \in GL_{n+1}(A, \mathfrak{q}) \mid \kappa_{n+1}(\sigma\sigma') = \kappa_{n+1}(\sigma)\kappa_{n+1}(\sigma') \text{ for all } \sigma' \in GL_{n+1}(A, \mathfrak{q})\}$$

and

$$N = \{\tau \in GL_{n+1}(A) \mid \kappa_{n+1}(\tau\sigma\tau^{-1}) = \kappa_{n+1}(\sigma) \text{ for all } \sigma \in GL_{n+1}(A, \mathfrak{q})\}.$$

The condition that κ_{n+1} be a homomorphism is that $H = GL_{n+1}(A, \mathfrak{q})$. Since $n+1 \geq 3$, condition $(8.2)_{n+1}$ just means that $GE_{n+1}(A) \subset N$.

Lemma 9.1. — a) H *is a group, and it contains all matrices of type* L *in* $GL_{n+1}(A, \mathfrak{q})$.

b) N *is a group, and it normalizes* H.

Proof. — *a)* If $\sigma \in H$ then

$$1 = \kappa_{n+1}(\sigma\sigma^{-1}) = \kappa_{n+1}(\sigma)\kappa_{n+1}(\sigma^{-1}) \qquad \text{so} \qquad \kappa_{n+1}(\sigma^{-1}) = \kappa_{n+1}(\sigma)^{-1}.$$

Hence, if $\sigma' \in GL_{n+1}(A, \mathfrak{q})$, then $\kappa_{n+1}(\sigma') = \kappa_{n+1}(\sigma\sigma^{-1}\sigma') = \kappa_{n+1}(\sigma)\kappa_{n+1}(\sigma^{-1}\sigma')$, so $\kappa_{n+1}(\sigma^{-1}\sigma') = \kappa_{n+1}(\sigma)^{-1}\kappa_{n+1}(\sigma') = \kappa_{n+1}(\sigma^{-1})\kappa_{n+1}(\sigma')$; i.e. $\sigma^{-1} \in H$. Suppose $\sigma_1 \in H$ also. Then $\kappa_{n+1}(\sigma_1\sigma\sigma') = \kappa_{n+1}(\sigma_1)\kappa_{n+1}(\sigma\sigma') = \kappa_{n+1}(\sigma_1)\kappa_{n+1}(\sigma)\kappa_{n+1}(\sigma') = \kappa_{n+1}(\sigma_1\sigma)\kappa_{n+1}(\sigma')$, so $\sigma_1\sigma \in H$. This shows that H is a group. Lemma 8.12 implies that H contains all $\sigma \in GL_{n+1}(A, \mathfrak{q})$ of type L.

It is clear that N is a group.

If $\tau \in N$, $\sigma \in H$, and $\sigma' \in GL_{n+1}(A, \mathfrak{q})$, then

$$\kappa_{n+1}((\tau^{-1}\sigma\tau)\sigma') = \kappa_{n+1}(\sigma\tau\sigma'\tau^{-1}) = \kappa_{n+1}(\sigma)\kappa_{n+1}(\tau\sigma'\tau^{-1})$$
$$= \kappa_{n+1}(\sigma)\kappa_{n+1}(\sigma') = \kappa_{n+1}(\tau^{-1}\sigma\tau)\kappa_{n+1}(\sigma');$$

hence $\tau^{-1}\sigma\tau \in H$.

Lemma 9.2. — *A subgroup* $K \subset GL_{n+1}(A, \mathfrak{q})$ *which contains all matrices of type* L, *and which is normalized by* $E_{n+1}(A)$, *is all of* $GL_{n+1}(A, \mathfrak{q})$.

Proof. — The matrices of type L contain $GL_n(A, \mathfrak{q})$ and, therefore, all matrices $I + te_{12}$ $(t \in \mathfrak{q})$. The smallest group containing the latter and normalized by $E_{n+1}(A)$ is $E_{n+1}(A, \mathfrak{q})$. Therefore K contains $GL_n(A, \mathfrak{q}) . E_{n+1}(A, \mathfrak{q})$, which is all of $GL_n(A, \mathfrak{q})$ thanks to Theorem 7.5 *b)* and our hypothesis $(7.2)_{n+1}$ above.

Corollary 9.3. — *If* $GE_{n+1}(A) \subset N$ *then* κ_{n+1} *is a homomorphism satisfying* $(8.2)_{n+1}$.

This follows immediately from Lemmas 9.1, 9.2, and the remarks preceding Lemma 9.1. The rest of our arguments will be concerned with showing that $GE_{n+1}(A) \subset N$.

Lemma 9.4. — N *contains all matrices of the form*

$$\tau = \begin{pmatrix} u & * & * \\ 0 & \nu & * \\ 0 & 0 & v \end{pmatrix}$$

where u and v are units and $\nu \in GE_{n-1}(A)$.

Proof. — These matrices form a group, of which those of the types

$$\tau_1 = \operatorname{diag}(u_1, \ldots, u_{n+1}), \qquad \tau_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \nu & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \text{and} \qquad \tau_3 = I + te_{ij},$$

where the u_i are units, $\nu \in GE_{n-1}(A)$, $t \in \mathfrak{q}$, and $(i, j) = (1, 2)$ or $(n, n+1)$, form a set of generators. It therefore suffices to show that, for τ one of these types, and for $\sigma \in GL_{n+1}(A, \mathfrak{q})$, that $\kappa_{n+1}(\tau\sigma\tau^{-1}) = \kappa_{n+1}(\sigma)$.

If $\sigma = \bar{\alpha}\varepsilon\bar{\beta}$ in standard form, then, for $\tau = \tau_1$ or τ_2, $\tau\sigma\tau^{-1} = (\tau\bar{\alpha}\tau^{-1})(\tau\varepsilon\tau^{-1})(\tau\bar{\beta}\tau^{-1})$ is still in standard form, and it follows easily from hypothesis $(8.2)_n$ that

$$\kappa_{n+1}(\tau\sigma\tau^{-1}) = \kappa_{n+1}(\sigma).$$

Suppose next, say, that $\tau = I + te_{12}$, $t \in A$. Then $\bar{\alpha}' = \tau\bar{\alpha}\tau^{-1} = \begin{pmatrix} \alpha' & \gamma' \\ 0 & 1 \end{pmatrix}$ is still of type L, with $\alpha' = \tau\alpha\tau^{-1}$. Moreover $\bar{\beta}' = \tau\bar{\beta}\tau^{-1} = \begin{pmatrix} 1 & \rho' \\ 0 & \beta \end{pmatrix}$ is still of type R. Finally, if $\varepsilon = I + se_{n+1,1}$, then $\tau\varepsilon\tau^{-1} = I + se_{n+1,1} - ste_{n+1,2} = \varepsilon(I - ste_{n+1,2}) = \varepsilon\bar{\beta}_1$. Here $\bar{\beta}_1 = \begin{pmatrix} 1 & 0 \\ 0 & \beta_1 \end{pmatrix}$ is of type R with $\beta_1 \in E_n(A, \mathfrak{q})$. Therefore $\tau\sigma\tau^{-1} = \bar{\alpha}'\varepsilon(\bar{\beta}_1\bar{\beta}')$ is in standard form, so $\kappa_{n+1}(\tau\sigma\tau^{-1}) = \kappa_n(\alpha')\kappa_n(\beta_1\beta) = \kappa_n(\alpha)\kappa_n(\beta_1)\kappa_n(\beta) = \kappa_{n+1}(\sigma)$, by virtue of $(8.2)_n$.

In case $\tau = I + te_{n,n+1}$ the argument is similar, except that this time we have $\tau\varepsilon\tau^{-1} = \bar{\alpha}_1\varepsilon$, where $\bar{\alpha}_1$ is a factor of type L that can be absorbed with $\tau\bar{\alpha}\tau^{-1}$.

At this point we shall use condition $(8.3)_n$ for the first time. This says that $\ker(\kappa_n)$ is invariant under transposition. Consequently the map $\sigma \mapsto {}^T\sigma$ on $GL_n(A, \mathfrak{q})$ induces an antiautomorphism, $x \mapsto {}^Tx$, on $\operatorname{im}(\kappa_n) \subset C$. It is defined by the formula

$${}^T\kappa_n(\sigma) = \kappa_n({}^T\sigma).$$

Let $\varphi=\begin{pmatrix}0 & 0 & 1\\ 0 & I_{n-1} & 0\\ 1 & 0 & 0\end{pmatrix}\in GE_{n+1}(A)$. Note that $\varphi=\varphi^{-1}={}^{T}\varphi$. For $\sigma\in GL_{n+1}(A)$ write

$$\tilde{\sigma}={}^{T}(\varphi\sigma\varphi^{-1})=\varphi({}^{T}\sigma)\varphi^{-1}.$$

It is easy to see that $\sigma\mapsto\tilde{\sigma}$ is an antiautomorphism of $GL_{n+1}(A)$, preserving $GL_{n+1}(A, \mathfrak{q})$, and that $\tilde{\tilde{\sigma}}=\sigma$.

Suppose $\bar{\alpha}=\begin{pmatrix}\alpha & \gamma\\ 0 & 1\end{pmatrix}$ is of type L. Then a direct calculation shows that $\tilde{\bar{\alpha}}=\begin{pmatrix}1 & \gamma_1\\ 0 & {}^{T}\alpha_1\end{pmatrix}$ is of type R. Here $\alpha_1=\pi\alpha\pi^{-1}$, where $\dot{\pi}=\begin{pmatrix}0 & 1 & \cdots & 0\\ \vdots & 0 & & \vdots\\ 0 & & \ddots & 1\\ 1 & 0 & \cdots & 0\end{pmatrix}\in GE_n(A)$.

Similarly, if $\bar{\beta}=\begin{pmatrix}1 & \rho\\ 0 & \beta\end{pmatrix}$ if of type R then $\tilde{\bar{\beta}}=\begin{pmatrix}{}^{T}\beta_1 & \rho_1\\ 0 & 1\end{pmatrix}$ is of type L, where $\beta_1=\pi^{-1}\beta\pi$.

Finally, if $\varepsilon=I+te_{n+1,1}$, then $\tilde{\varepsilon}=\varepsilon$.

Suppose $\sigma\in GL_{n+1}(A, \mathfrak{q})$ has a standard form $\sigma=\bar{\alpha}\varepsilon\bar{\beta}$. The discussion above shows that $\tilde{\sigma}=\tilde{\bar{\beta}}\tilde{\varepsilon}\tilde{\bar{\alpha}}$ is a standard form for $\tilde{\sigma}$, so $\kappa_{n+1}(\tilde{\sigma})=\kappa_n({}^{T}\beta_1)\kappa_n({}^{T}\alpha_1)$, in the notation above. Thus

$$\begin{aligned}\kappa_{n+1}(\tilde{\sigma})&={}^{T}\kappa_n(\beta_1)\,{}^{T}\kappa_n(\alpha_1)\\ &={}^{T}(\kappa_n(\pi\alpha\pi^{-1})\kappa_n(\pi^{-1}\beta\pi))\\ &={}^{T}(\kappa_n(\alpha)\kappa_n(\beta))\\ &={}^{T}\kappa_{n+1}(\sigma).\end{aligned}$$

Now suppose that $\tau\in N$; we claim that $\tilde{\tau}\in N$ also. For

$$\begin{aligned}\kappa_{n+1}(\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1})&=\kappa_{n+1}((\tau^{-1}\tilde{\sigma}\tau)\tilde{\ })\\ &={}^{T}\kappa_{n+1}(\tau^{-1}\tilde{\sigma}\tau)\\ &={}^{T}\kappa_{n+1}(\tilde{\sigma})\\ &=\kappa_{n+1}(\sigma)\end{aligned}$$

We have thus proved:

Lemma 9.5. — *If* $\tau\in N$ *then* $\tilde{\tau}\in N$.

Lemma 9.6. — *A subgroup of* $GL_{n+1}(A)$ *containing all the matrices in Lemma 9.4, invariant under* $\tau\mapsto\tilde{\tau}$, *and containing*

$$\pi=\begin{pmatrix}I_{n-1} & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$$

contains $GE_{n+1}(A)$.

Proof. — $GE_{n+1}(A)$ is generated by diagonal matrices and by elementary matrices. Lemma 9.4 gives us all diagonal matrices and all elementary matrices $I+te_{ij}$ except those with $i=n+1$ or $j=1$.

But $\pi(I+te_{n,n+1})\pi^{-1}=I+te_{n+1,n}$, and $[I+te_{n+1,n}, I+e_{nj}]=I+te_{n+1,j}$ for $j\neq n, n+1$. Hence we have all $I+te_{ij}$ with $j\neq 1$. Next note that $(I+te_{n+1,j})\tilde{\ }=I+te_{j1}$ for $j\neq 1, n+1$, so we lack only $I+te_{n+1,1}$. We obtain the latter as $[I+te_{n+1,n}, I+e_{n,1}]$.

§ 10. Proof that $\pi \in N$.

We want to show that $GE_{n+1}(A) \subset N$, and Lemmas 9.4, 9.5 and 9.6 make it sufficient to show that $\pi \in N$, where

$$\pi = \begin{pmatrix} I_{n-1} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

This amounts to showing that

$$\kappa_{n+1}(\pi\sigma\pi^{-1}) = \kappa_{n+1}(\sigma) \tag{10.1}$$

for $\sigma \in GL_{n+1}(A, \mathfrak{q})$.

Lemma 10.2. — a) *The matrices σ for which* (10.1) *holds are stable under right multiplication by matrices β_1 of type* R, *and under left multiplication by matrices*

$$\bar{\alpha}_1 = \begin{pmatrix} \alpha_1' & \gamma_1 \\ 0 & I_2 \end{pmatrix}. \tag{10.3}$$

b) *It suffices to prove* (10.1) *for σ of the form $\sigma = \bar{\alpha}\varepsilon$, where $\varepsilon = I + te_{n+1,1}$, and where $\bar{\alpha} = \begin{pmatrix} \alpha & \gamma \\ 0 & 1 \end{pmatrix}$ is of type* L. *If we further assume $(7.2)_n$ and $(8.1)_{n-1}$ then we can even restrict α to have the form*

$$\alpha = \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n-1,2} & \dots & a_{n-1,n} \\ a_{n1} & a_{n2} & & a_{nn} \end{pmatrix}. \tag{10.4}$$

Proof. — *a)* If $\bar{\beta}$ is of type R then so is $\pi\bar{\beta}_1\pi^{-1}$, clearly, and $(8.2)_n$ implies $\kappa_{n+1}(\pi\bar{\beta}_1\pi^{-1}) = \kappa_{n+1}(\bar{\beta}_1)$. Similarly, if $\bar{\alpha}_1$ is as in (10.3) then $\pi\bar{\alpha}_1\pi^{-1}$ is of the same type, and $\kappa_{n+1}(\pi\bar{\alpha}_1\pi^{-1}) = \kappa_{n+1}(\bar{\alpha}_1)$, clearly. Now if $\kappa_{n+1}(\pi\sigma\pi^{-1}) = \kappa_{n+1}(\sigma)$ then, using Lemma 8.12,

$$\kappa_{n+1}(\pi\bar{\alpha}_1\sigma\bar{\beta}_1\pi^{-1}) = \kappa_{n+1}(\pi\bar{\alpha}_1\pi^{-1})\kappa_{n+1}(\pi\sigma\pi^{-1})\kappa_{n+1}(\pi\bar{\beta}_1\pi^{-1})$$
$$= \kappa_{n+1}(\bar{\alpha}_1)\kappa_{n+1}(\sigma)\kappa_{n+1}(\bar{\beta}_1) = \kappa_{n+1}(\bar{\alpha}_1\sigma\bar{\beta}_1).$$

b) Using *a)*, in order to verify (10.1) for a given σ, we are free to first modify σ on the right by factors of type R, and on the left by factors of type (10.3). The former permits us to render σ of the form $\sigma = \bar{\alpha}\varepsilon$, as indicated in the lemma. If we assume $(7.2)_n$ and $(8.1)_{n-1}$ then it follows from Lemma 8.9 *a)* that we can write $\alpha = \alpha_1\varepsilon_1\beta_1$, a standard form in $GL_n(A, \mathfrak{q})$. Since $\alpha_1 = \begin{pmatrix} \alpha_1' & \gamma_1' \\ 0 & 1 \end{pmatrix}$ it follows that $\bar{\alpha}_1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & 1 \end{pmatrix}$ is a matrix of type (10.3). Replacing σ by $\bar{\alpha}_1^{-1}\sigma$, therefore, which we can do thanks to part *a)*, we can assume above that $\alpha = \varepsilon_1\beta_1$, a standard form in $GL_n(A, \mathfrak{q})$. This implies that α has the form (10.4) above. Q.E.D.

Proof of Proposition 8.6 (concluded):

Since $(7.2)_n$ and $(8.1)_{n-1}$ are part of the hypotheses of Proposition 8.6, we can now finish the proof of that proposition by verifying (10.1) for $\sigma=\bar{\alpha}\varepsilon$ where $\varepsilon=I+te_{n+1,1}$, $t\in\mathfrak{q}$, and where $\bar{\alpha}=\begin{pmatrix}\alpha & \gamma\\ 0 & 1\end{pmatrix}$ with α as in (10.4).

Note first that if $\varepsilon_1=I-a_{n1}e_{n1}\in E_n(A,\mathfrak{q})$ then $\varepsilon_1\alpha=\begin{pmatrix}1 & *\\ 0 & \alpha'\end{pmatrix}$, where

$$\alpha'=\begin{pmatrix} a_{22} & \cdots & a_{2n}\\ \vdots & & \\ a_{n-1,2} & \cdots & a_{n-1,n}\\ a_{n2}-a_{n1}a_{12} & \cdots & a_{nn}-a_{n1}a_{1n}\end{pmatrix}.$$

Hence, if $\kappa_{n-1}=\kappa_n|GL_{n-1}(A,\mathfrak{q})$ then

$$\kappa_{n+1}(\sigma)=\kappa_n(\alpha)=\kappa_{n-1}(\alpha'),$$

clearly. Thus we must show that $\kappa_{n+1}(\pi\sigma\pi^{-1})=\kappa_{n-1}(\alpha')$.

Writing $\gamma=\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$ we have

$$\sigma=\bar{\alpha}\varepsilon=\begin{pmatrix}\alpha+\gamma(t,0,\ldots,0) & \gamma\\ t\quad 0\ \cdots\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1+tc_1 & a_{12} & \cdots & a_{1n} & c_1\\ tc_2 & a_{22} & \cdots & a_{2n} & c_2\\ \vdots & \vdots & & \vdots & \\ tc_{n-1} & a_{n-1,2} & \cdots & a_{n-1,n} & c_{n-1}\\ a_{n1}+tc_n & a_{n2} & \cdots & a_{nn} & c_n\\ t & 0 & \cdots & 0 & 1\end{pmatrix}.$$

Writing $\tau=\pi\sigma\pi^{-1}$ we have

$$\tau=\begin{pmatrix} 1+tc_1 & a_{12} & \cdots & a_{1,n-1} & c_1 & a_{1n}\\ tc_2 & a_{22} & \cdots & a_{2,n-1} & c_2 & a_{2n}\\ \vdots & \vdots & & \vdots & \vdots & \vdots\\ tc_{n-1} & a_{n-1,1} & \cdots & a_{n-1,n-1} & c_{n-1} & a_{n-1,n}\\ t & 0 & \cdots & 0 & 1 & 0\\ a_{n1}+tc_n & a_{n2} & \cdots & a_{n,n-1} & c_n & a_{nn}\end{pmatrix}.$$

We now proceed to put τ in standard form, so that we can evaluate $\kappa_{n+1}(\tau)$.

Set $\bar{\alpha}_1=\begin{pmatrix}\alpha_1 & 0\\ 0 & 1\end{pmatrix}$, where $\alpha_1=I-(\sum_{i=1}^{n-1}c_ie_{in})$. Then

$$\bar{\alpha}_1\tau=\begin{pmatrix} 1 & a_{12} & \cdots & a_{1,n-1} & 0 & a_{1n}\\ 0 & a_{22} & \cdots & a_{2,n-1} & 0 & a_{2n}\\ \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & a_{n-1,2} & \cdots & a_{n-1,n-1} & 0 & a_{n-1,n}\\ t & 0 & \cdots & 0 & 1 & 0\\ a_{n1}+tc_n & a_{n2} & \cdots & a_{n,n-1} & c_n & a_{nn}\end{pmatrix}.$$

Set $\bar{\alpha}_2 = \pi\varepsilon^{-1}\pi^{-1} = \begin{pmatrix} \alpha_2 & 0 \\ 0 & I \end{pmatrix}$, where $\alpha_2 = I - te_{n1}$, and set $\varepsilon_1 = I + se_{n+1,1}$, where $s = a_{n1} + tc_n$. Then

$$\bar{\beta} = \varepsilon_1^{-1}\bar{\alpha}_2\bar{\alpha}_1\tau = \begin{pmatrix} I & \rho \\ 0 & \beta \end{pmatrix}$$

is of type R, where

$$\beta = \begin{pmatrix} a_{22} & \cdots & a_{2,n-1} & 0 & a_{2n} \\ \vdots & & \vdots & \vdots & \vdots \\ -ta_{12} & \cdots & -ta_{1,n-1} & I & -ta_{1n} \\ a_{n2} - sa_{12} & \cdots & a_{n,n-1} - sa_{1,n-1} & c_n & a_{nn} - sa_{1n} \end{pmatrix}.$$

Therefore $\tau = (\bar{\alpha}_2\bar{\alpha}_1)^{-1}\varepsilon_1\bar{\beta}$ is a standard form, so $\kappa_{n+1}(\tau) = \kappa_n((\alpha_2\alpha_1)^{-1})\kappa_n(\beta) = \kappa_n(\beta)$, since clearly $\alpha_1, \alpha_2 \in E_n(A, \mathfrak{q})$.

In $GL_n(A, \mathfrak{q})$ set $\delta = I + (\sum_{j=1}^{n-2} ta_{ij+1}e_{n-1,j}) + ta_{1n}e_{n-1,n}$. Then since

$$a_{nj} - sa_{ij} + ta_{ij}c_n = a_{nj} - (a_{n1} + tc_n)a_{ij} + ta_{ij}c_n = a_{nj} - a_{n1}a_{ij},$$

we have

$$\beta\delta = \begin{pmatrix} a_{22} & \cdots & a_{2,n-1} & 0 & a_{2n} \\ \vdots & & \vdots & \vdots & \vdots \\ a_{n-1,2} & \cdots & a_{n-1,n-1} & 0 & a_{n-1,n} \\ 0 & & 0 & I & 0 \\ a_{n2} - a_{n1}a_{12} & \cdots & a_{n,n-1} - a_{n1}a_{1,n-1} & c_n & a_{nn} - a_{n1}a_{1n} \end{pmatrix}.$$

Now $\beta\delta$ is conjugate, by a permutation matrix, to

$$\beta' = \begin{pmatrix} & & 0 \\ & \alpha' & \vdots \\ & & 0 \\ & & c_n \\ 0 & \cdots\ 0 & I \end{pmatrix}.$$

Therefore, since $\delta \in E_n(A, \mathfrak{q})$, it follows from $(8.2)_n$ that

$$\kappa_n(\beta) = \kappa_n(\beta\delta) = \kappa_n(\beta') = \kappa_{n-1}(\alpha'),$$

and so $\kappa_{n+1}(\tau) = \kappa_n(\beta) = \kappa_{n-1}(\alpha')$, as was to be shown. This concludes the proof of Proposition 8.6.

Proof of Proposition 8.5 (concluded):

Now it remains to prove (10.1) in the setting of Proposition 8.5. Thus $n = 2$ and κ_2 is given by a Mennicke symbol, $\kappa_2\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$. Again it is enough, by Lemma 10.2 *b)*, to treat σ of the form $\sigma = \bar{\alpha}\varepsilon$.

Writing $\bar{\alpha} = \begin{pmatrix} \alpha & \gamma \\ 0 & I \end{pmatrix}$ with $\alpha = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $\gamma = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$, we can modify σ on the left by a factor of type (10.3) to arrange that $a_{11} \neq 0$. (This is automatic if $\mathfrak{q} \neq A$.)

With $\tau=\pi\sigma\pi^{-1}$ we have

$$\tau=\begin{pmatrix} a_{11}+tc_1 & c_1 & a_{12} \\ t & 1 & 0 \\ a_{21}+tc_2 & c_1 & a_{22}\end{pmatrix}.$$

Set $\bar{\alpha}_1=\begin{pmatrix}\alpha_1 & 0\\ 0 & 1\end{pmatrix}$ with $\alpha_1=\begin{pmatrix}1 & -c_1\\ 0 & 1\end{pmatrix}$, as above, so that

$$\bar{\alpha}_1\tau=\begin{pmatrix} a_{11} & 0 & a_{12} \\ t & 1 & 0 \\ a_{21}+tc_2 & c_2 & a_{22}\end{pmatrix}.$$

Since $a_{11}\neq 0$, $A/a_{11}A$ is semi-local, so we can find an $s\in\mathfrak{q}$ such that $t+s(a_{21}+tc_2)$ is prime to a_{11} (see remark above Lemma 2.2). We can further arrange that $c=1+sc_2\neq 0$, and write $t+s(a_{21}+tc_2)=sa_{21}+tc$. Then with $\delta=I+se_{23}$ we have

$$\delta\bar{\alpha}_1\tau=\begin{pmatrix} a_{11} & 0 & a_{12} \\ sa_{21}+tc & c & sa_{22} \\ a_{21}+tc_2 & c_2 & a_{22}\end{pmatrix}.$$

Since $(a_{11}, sa_{21}+tc)$ is $\mathfrak{q}$-unimodular we can use (7.1) to find an

$$\omega=\begin{pmatrix} w_{11} & w_{12}\\ w_{21} & w_{22}\end{pmatrix}\in \mathrm{SL}_2(A,\mathfrak{q})$$

such that

$$\omega\begin{pmatrix} a_{11} & 0\\ sa_{21}+tc & c\end{pmatrix}=\begin{pmatrix} 1 & x\\ 0 & y\end{pmatrix} \tag{10.5}$$

for some x, y. Setting $\bar{\omega}=\begin{pmatrix}\omega & 0\\ 0 & 1\end{pmatrix}$ we have

$$\bar{\omega}\delta\bar{\alpha}_1\tau=\begin{pmatrix} 1 & x & w_{11}a_{12}+sw_{12}a_{22} \\ 0 & y & w_{21}a_{12}+sw_{22}a_{22} \\ a_{21}+tc_2 & c_2 & a_{22}\end{pmatrix}.$$

Therefore if $\varepsilon_1=I+ue_{31}$, $u=a_{21}+tc_2$, then

$$\bar{\beta}=\varepsilon_1^{-1}\bar{\omega}\delta\bar{\alpha}_1\tau=\begin{pmatrix}1 & \rho\\ 0 & \beta\end{pmatrix}$$

is of type R, where $\beta=\begin{pmatrix} y & w_{21}a_{12}+sw_{22}a_{22}\\ c_2-ux & a_{22}-u(w_{11}a_{12}+sw_{12}a_{22})\end{pmatrix}$.

Finally $\tau=(\bar{\omega}\delta\bar{\alpha}_1)^{-1}\varepsilon_1\bar{\beta}$ is a standard form for τ, because

$$\bar{\omega}\delta\bar{\alpha}_1=\begin{pmatrix}\omega\alpha_1 & & \omega\begin{pmatrix}0\\ s\end{pmatrix}\\ 0 \quad 0 & & 1\end{pmatrix}$$

is of type L. Since $\alpha_1=I-c_1e_{12}\in \mathrm{E}_2(A,\mathfrak{q})$ we have

$$\begin{aligned}\kappa_3(\tau)&=\kappa_2((\omega\alpha_1)^{-1})\kappa_2(\beta)\\ &=\kappa_2(\omega)^{-1}\kappa_2(\beta).\end{aligned}$$

To evaluate this we solve for ω from (10.5):

$$\begin{pmatrix} w_{11}a_{11}+w_{12}(sa_{21}+tc) & w_{12}c \\ w_{21}a_{11}+w_{22}(sa_{21}+tc) & w_{22}c \end{pmatrix}=\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}.$$

Since $\det \omega = 1$, (10.5) shows that $y=a_{11}c$, and hence $a_{11}c=w_{22}c$. But $c\neq 0$ by our choice of s above, so $a_{11}=w_{22}$. Therefore $0=w_{21}a_{11}+a_{11}(sa_{21}+tc)$, and since $a_{11}\neq 0$ (by construction) we have $w_{21}=-(sa_{21}+tc)$. The other coordinates give $x=w_{12}c$ and $1=w_{11}a_{11}+w_{12}(sa_{21}+tc)$.

Now we can write $$\omega=\begin{pmatrix} w_{11} & w_{12} \\ -(sa_{21}+tc) & a_{11} \end{pmatrix}$$

and $$\beta=\begin{pmatrix} a_{11}c & -(sa_{21}+tc)a_{12}+sa_{11}a_{22} \\ * & * \end{pmatrix}=\begin{pmatrix} a_{11}c & sd-tca_{12} \\ * & * \end{pmatrix}$$

where $d=\det \alpha$.

Using step (1) of the proof of Kubota's Theorem we have

$$\begin{aligned} \kappa_2(\omega)^{-1}&=\begin{bmatrix} -(sa_{21}+tc) \\ a_{11} \end{bmatrix}^{-1}=\begin{bmatrix} (sa_{21}+tc)a_{12} \\ a_{11} \end{bmatrix}^{-1}\begin{bmatrix} a_{12} \\ a_{11} \end{bmatrix} \\ &=\begin{bmatrix} s(a_{11}a_{22}-d)+tca_{12} \\ a_{11} \end{bmatrix}^{-1}\kappa_2(\alpha) \\ &=\begin{bmatrix} tca_{12}-sd \\ a_{11} \end{bmatrix}^{-1}\kappa_2(\alpha). \end{aligned}$$

Next $$\begin{aligned} \kappa_2(\beta)&=\begin{bmatrix} sd-tca_{12} \\ a_{11}c \end{bmatrix}=\begin{bmatrix} sd-tca_{12} \\ c \end{bmatrix}\begin{bmatrix} sd-tca_{12} \\ a_{11} \end{bmatrix} \\ &=\begin{bmatrix} sd \\ c \end{bmatrix}\begin{bmatrix} sd-tca_{12} \\ a_{11} \end{bmatrix}=\begin{bmatrix} sd-tca_{12} \\ a_{11} \end{bmatrix} \end{aligned}$$

because d is a unit and $c=1+sc_2$. Finally, we have

$$\begin{aligned} \kappa_3(\tau)&=\kappa_2(\omega)^{-1}\kappa_2(\beta) \\ &=\kappa_2(\alpha)\begin{bmatrix} tca_{12}-sd \\ a_{11} \end{bmatrix}^{-1}\begin{bmatrix} sd-tca_{12} \\ a_{11} \end{bmatrix} \\ &=\kappa_2(\alpha)=\kappa_3(\sigma). \end{aligned}$$ Q.E.D.

This concludes the proof of Proposition 8.5, and hence of part *c)* of Theorem 4.1. Part *b)* of Theorem 4.1 was proved in § 5 (Theorem 5.1). Part *a)* will be deduced in the following section.

§ 11. Further conclusions.

Theorem 11.1. — *Let* A *be a commutative ring, let* $\mathfrak{q}$ *be an ideal of* A, *and assume they satisfy* $(7.2)_n$ *and* $(8.1)_{n-1}$ *for some* $n\geq 3$. *Then for all* $m\geq n$:

a) $E_m(A,\mathfrak{q})=[GL_m(A), GL_m(A,\mathfrak{q})]$; *and*

b) *The natural homomorphism*

$$\mathrm{GL}_n(A, \mathfrak{q})/\mathrm{E}_n(A, \mathfrak{q}) \to \mathrm{GL}_m(A, \mathfrak{q})/\mathrm{E}_m(A, \mathfrak{q})$$

is an isomorphism.

Proof. — $(7.2)_n$ and Theorem 7.5 *c)* imply that $\mathrm{E}_m(A, \mathfrak{q})$ is normal in $\mathrm{GL}_m(A)$. In particular we can define $\mathrm{C}_m = \mathrm{GL}_m(A, \mathfrak{q})/\mathrm{E}_m(A, \mathfrak{q})$. Theorem 7.5 *b)* implies that $\mathrm{C}_n \to \mathrm{C}_m$ is surjective. Let $\kappa_n : \mathrm{GL}_n(A, \mathfrak{q}) \to \mathrm{C}_n$ be the natural projection. This satisfies $(8.2)_n$ because of Theorem 7.5 *d)*, and it satisfies $(8.3)_n$ because $\mathrm{E}_n(A, \mathfrak{q})$ is clearly stable under transposition. Finally the hypotheses $(7.2)_n$ and $(8.1)_{n-1}$ make Lemma 8.9 *b)* available, and the latter confirms $(8.4)_n$. We now have all the hypotheses of Proposition 8.6, so we obtain an extension of κ_n to a homomorphism $\kappa_{n+1} : \mathrm{GL}_{n+1}(A, \mathfrak{q}) \to \mathrm{C}_n$ whose kernel contains $\mathrm{E}_{n+1}(A, \mathfrak{q})$. The map κ_{n+1} therefore induces $\mathrm{C}_{n+1} \to \mathrm{C}_n$ such that the composite $\mathrm{C}_n \to \mathrm{C}_{n+1} \to \mathrm{C}_n$ is the identity. Since, as already remarked, $\mathrm{C}_n \to \mathrm{C}_{n+1}$ is surjective, it follows that $\mathrm{C}_n \to \mathrm{C}_{n+1}$ is an isomorphism.

Since $(7.2)_n \Rightarrow (7.2)_m$ and $(8.1)_m$ for all $m \geq n$, by virture of Theorem 7.5 *a)*, we can repeat the above argument, and prove part *b)* of the theorem by induction.

According to Theorem 7.5 *d)* we have $[\mathrm{GL}_m(A), \mathrm{GL}_m(A, \mathfrak{q})] \subset \mathrm{E}_m(A, \mathfrak{q})$ for sufficiently large m. Hence

$$[\mathrm{GL}_n(A), \mathrm{GL}_n(A, \mathfrak{q})] \subset \mathrm{E}_m(A, \mathfrak{q}) \cap \mathrm{GL}_n(A, \mathfrak{q}) = \mathrm{E}_n(A, \mathfrak{q}),$$

the last equality expressing the fact that $\mathrm{C}_n \to \mathrm{C}_m$ is a monomorphism. Since $n \geq 3$ it follows now from (5.1) that

$$\mathrm{E}_n(A, \mathfrak{q}) = [\mathrm{E}_n(A), \mathrm{E}_n(A, \mathfrak{q})] = [\mathrm{GL}_n(A), \mathrm{GL}_n(A, \mathfrak{q})].$$

Since our hypotheses carry over for all $m \geq n$, this proves *a)*, and completes the proof of the theorem.

Theorem 11.2. — *Suppose the maximal ideal space of* A *is a noetherian space of dimension* $\leq d$. *Then* A *satisfies* $(7.2)_n$ *and* $(8.1)_n$ *for all ideals* $\mathfrak{q}$ *and all* $n \geq d+2$.

Proof. — This follows directly from Theorem 7.4 and Theorem 7.5 *a)*.

Write

$$\mathrm{GL}(A, \mathfrak{q}) = \bigcup_{n \geq 1} \mathrm{GL}_n(A, \mathfrak{q}) \qquad \text{and} \qquad \mathrm{E}(A, \mathfrak{q}) = \bigcup_{n \geq 1} \mathrm{E}_n(A, \mathfrak{q}) = [\mathrm{GL}(A), \mathrm{GL}(A, \mathfrak{q})]$$

(see [1, Ch. I]). Then there are canonical maps

$$\mathrm{GL}_n(A, \mathfrak{q})/\mathrm{E}_n(A, \mathfrak{q}) \to \mathrm{K}_1(A, \mathfrak{q}) = \mathrm{GL}(A, \mathfrak{q})/\mathrm{E}(A, \mathfrak{q}).$$

The next corollary affirms, for commutative A, the conjecture of [1, § 11], except for the probably unnecessary requirement of $(8.1)_{n-1}$.

Corollary 11.3. — *Under the hypotheses of Theorem 11.2, the map*

$$\mathrm{GL}_n(A, \mathfrak{q})/\mathrm{E}_n(A, \mathfrak{q}) \to \mathrm{K}_1(A, \mathfrak{q})$$

is an isomorphism of groups for all $n \geq d+3$ (*and for all* $n \geq 3$ *if* $d = 1$). *Moreover* $\mathrm{E}_n(A, \mathfrak{q}) = [\mathrm{E}_n(A), \mathrm{E}_n(A, \mathfrak{q})] = [\mathrm{SL}_n(A), \mathrm{SL}_n(A, \mathfrak{q})] = [\mathrm{GL}_n(A), \mathrm{GL}_n(A, \mathfrak{q})]$.

Proof. — The first assertion, as well as the equality $E_n(A, \mathfrak{q}) = [GL_n(A), GL_n(A, \mathfrak{q})]$, follows from Theorem 11.1 and Theorem 11.2 if $d > 1$. The case $d = 1$ and $n = 3$ works because condition $(8.1)_2$ is supplied by (7.1).

The equality $E_n(A, \mathfrak{q}) = [E_n(A), E_n(A, \mathfrak{q})]$ is (5.1) and the insertion of SL_n follows from this and the equation above.

The last assertion of Corollary 11.3 contains part *a)* of Theorem 4.1. Thus, *the proof of Theorem 4.1 is now concluded.*

According to (5.2), $E_n(A)$ is a finitely generated group if A is a finitely generated $\mathbf{Z}$-algebra, and $n \geq 3$. Hence:

Corollary 11.4. — Let A *be a finitely generated commutative* $\mathbf{Z}$*-algebra of Krull dimension* $\leq d$. *If* K_1A *is a finitely generated abelian group, then* $GL_n(A)$ *and* $SL_n(A)$ *are finitely generated groups for all* $n \geq d+3$ (*and all* $n \geq 3$ *if* $d = 1$).

Examples. — Let A be a Dedekind ring of arithmetic type, and let T be a free abelian group or monoid. Then it follows from the results of [3] that $K_1A[T]$ is finitely generated. Therefore, for example, if $t_1, \ldots, t_d$ are indeterminates, then

$$SL_n(\mathbf{Z}[t_1, \ldots, t_d])$$

is a finitely generated group if $n \geq d+4$, *and, if k is a finite field,*

$$SL_n(k[t_1, \ldots, t_d])$$

is a finitely generated group if $n \geq d+3$.

One cannot generalize these results too hastily, as the following example shows. Let $A = \{a + 2ib \mid a, b \in \mathbf{Z}\}$, a subring of the Gaussian integers, or, say, $k[t^2, t^3] \subset k[t]$ with k a finite field and t an indeterminate. Then if T is a free abelian group of rank ≥ 2, $SL_n(A[T])$ is not a finitely generated group for any $n \geq 6$. This can be deduced from results of [3] and [7].

CHAPTER III

MENNICKE SYMBOLS ASSOCIATED WITH Sp_{2n}

§ 12. Statement of the main theorem.

Let A be a commutative ring and let ε denote the $2n\times 2n$ matrix, $\varepsilon=\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. Then ${}^{\mathrm{T}}\varepsilon=-\varepsilon$, where the superscript denotes transpose. The *symplectic group* is defined by

$$\mathrm{Sp}_{2n}(\mathrm{A})=\{\alpha\in\mathrm{GL}_{2n}(\mathrm{A})\mid \alpha\varepsilon{}^{\mathrm{T}}\alpha=\varepsilon\}.$$

This is the group of automorphisms of A^{2n} leaving invariant the standard alternating form in $2n$ variables.

Writing a $2n\times 2n$ matrix in $n\times n$ blocks, we can express membership in $\mathrm{Sp}_{2n}(\mathrm{A})$ by the condition:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} {}^{\mathrm{T}}\delta & -{}^{\mathrm{T}}\beta \\ -{}^{\mathrm{T}}\gamma & {}^{\mathrm{T}}\alpha \end{pmatrix}=I_{2n}.$$

From this we deduce three immediate consequences. First

$$\mathrm{Sp}_2(\mathrm{A})=\mathrm{SL}_2(\mathrm{A}).$$

Second, Sp_{2n} contains all matrices

$$\text{(12.1)}\qquad \begin{pmatrix} I & \sigma \\ 0 & I \end{pmatrix} \quad\text{and}\quad \begin{pmatrix} I & 0 \\ \sigma & I \end{pmatrix} \quad\text{with}\quad \sigma={}^{\mathrm{T}}\sigma.$$

The subgroup generated by these will be denoted

$$\mathrm{Ep}_{2n}(\mathrm{A}).$$

Finally, there is a homomorphism,

$$\text{(12.2)}\qquad \mathrm{GL}_n(\mathrm{A})\to\mathrm{Sp}_{2n}(\mathrm{A}),\qquad \alpha\mapsto\begin{pmatrix} \alpha & 0 \\ 0 & \widetilde{\alpha} \end{pmatrix},$$

where $\widetilde{\alpha}=({}^{\mathrm{T}}\alpha)^{-1}={}^{\mathrm{T}}(\alpha^{-1})$. It is also known that $\mathrm{Sp}_{2n}(\mathrm{A})\subset\mathrm{SL}_{2n}(\mathrm{A})$.

We shall agree to identify $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\in\mathrm{Sp}_{2n}(\mathrm{A})$ with $\begin{pmatrix} \delta & 0 & \beta & 0 \\ 0 & I_m & 0 & 0 \\ \gamma & 0 & \delta & 0 \\ 0 & 0 & 0 & I_m \end{pmatrix}\in\mathrm{Sp}_{2(m+n)}(\mathrm{A})$.

This gives us the vertical map in the diagram of monomorphisms,

$$\begin{array}{ccccc} & & \mathrm{SL}_2(A)=\mathrm{Sp}_2(A) & & \\ & & \downarrow f_1 & & \\ \mathrm{GL}_n(A) & \xrightarrow{(12.2)} & \mathrm{Sp}_{2n}(A) & \xrightarrow{\text{incl.}} & \mathrm{SL}_{2n}(A). \end{array} \tag{12.3}$$

It is clear that the embedding $\mathrm{SL}_2(A)\to\mathrm{SL}_{2n}(A)$ induced by f_1 differs from the inclusion defined in Chapter II, § 4, only by conjugation by a permutation matrix.

Let $\mathfrak{q}$ be an ideal of A. Then we write

$$\mathrm{Sp}_{2n}(A,\mathfrak{q})=\ker(\mathrm{Sp}_{2n}(A)\to\mathrm{Sp}_{2n}(A/\mathfrak{q})),$$

and denote by $\mathrm{Ep}_{2n}(A,\mathfrak{q})$

the *normal* subgroup of $\mathrm{Ep}_{2n}(A)$ generated by all those matrices (12.1) for which σ has coordinates in $\mathfrak{q}$.

We can now state an analogue, for Sp_{2n}, of Theorem 4.1 on SL_n.

Theorem 12.4. — *Let* A *be a Dedekind ring of arithmetic type, let* $\mathfrak{q}$ *be a nonzero ideal of* A, *and suppose* $n\geq 2$. *Then* $\mathrm{Ep}_{2n}(A,\mathfrak{q})$ *is a normal subgroup of* $\mathrm{Sp}_{2n}(A)$, *so we can define* $\mathrm{Cp}_{\mathfrak{q}}=\mathrm{Sp}_{2n}(A,\mathfrak{q})/\mathrm{Ep}_{2n}(A,\mathfrak{q})$, *and the natural projection,* $\kappa:\mathrm{Sp}_{2n}(A,\mathfrak{q})\to\mathrm{Cp}_{\mathfrak{q}}$. *There is a unique map* $\{\}:W_{\mathfrak{q}}\to\mathrm{Cp}_{\mathfrak{q}}$ *rendering*

$$\begin{array}{ccc} \mathrm{SL}_2(A,\mathfrak{q})=\mathrm{Sp}_2(A,\mathfrak{q}) & \xrightarrow{f_1} & \mathrm{Sp}_{2n}(A,\mathfrak{q}) \\ \downarrow{\scriptstyle 1^{\text{st}}\text{ row}} & & \downarrow{\scriptstyle \kappa} \\ W_{\mathfrak{q}} & \xrightarrow[\{\}]{} & \mathrm{Cp}_{\mathfrak{q}} \end{array}$$

commutative, and $\{\}$ *is a universal Mennicke symbol.*

Invoking Theorem 3.6, where the universal Mennicke symbols are calculated arithmetically, we obtain the following corollary:

Corollary 12.5. — $\mathrm{Sp}_{2n}(A)$ *is generated by the matrices* (12.1). $\mathrm{Cp}_{\mathfrak{q}}$ *is independent of* n, *and the natural map* $\mathrm{Cp}_{\mathfrak{q}}\to\mathrm{Cp}_{\mathfrak{q}'}$, *is an epimorphism of finite groups whenever* $0\neq\mathfrak{q}\subset\mathfrak{q}'$. *Moreover,*

$$\lim_{\leftarrow\mathfrak{q}}\mathrm{Cp}_{\mathfrak{q}}\cong\begin{cases}\text{the roots of unity in A, if A is totally imaginary;}\\ \{1\}\text{ otherwise.}\end{cases}$$

Remark. — Using the fact that $\mathrm{Sp}_{2n}(A)$ is generated by the matrices (12.1) it is not difficult to show that $\mathrm{Sp}_{2n}(A)$ is finitely generated (cf. [22]). (This is even trivial in the number field case.) Moreover the commutator factor group of $\mathrm{Sp}_{2n}(A)$ is trivial for $n\geq 3$, and is a finite group of exponent 2 for $n=2$.

§ 13. Proof of Theorem 12.4.

Lemma 13.1. — *The diagram* (12.3) *induces diagrams*

$$\begin{array}{ccccc} & & \mathrm{SL}_2(A,\mathfrak{q}) & & \\ & & \downarrow f_1 & & \\ \mathrm{SL}_n(A,\mathfrak{q}) & \xrightarrow{(12.2)} & \mathrm{Sp}_{2n}(A,\mathfrak{q}) & \longrightarrow & \mathrm{SL}_{2n}(A,\mathfrak{q}) \end{array}$$

and

$$\begin{array}{ccccc} & & \mathrm{E}_2(A,\mathfrak{q}) & & \\ & & \downarrow f_1 & & \\ \mathrm{E}_n(A,\mathfrak{q}) & \xrightarrow{(12.2)} & \mathrm{Ep}_{2n}(A,\mathfrak{q}) & \longrightarrow & \mathrm{E}_{2n}(A,\mathfrak{q}). \end{array}$$

Proof. — The only assertion here that does not follow immediately from the definitions is that $\begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix}\in \mathrm{Ep}_{2n}(A,\mathfrak{q})$ if $\alpha\in \mathrm{E}_n(A,\mathfrak{q})$. From the way these groups are defined it is easily seen that it suffices to prove this when α is an elementary matrix. α is then an element of some SL_2, so we can carry out the calculation in Sp_4. Say $\alpha=\begin{pmatrix}1 & 0\\ q & 1\end{pmatrix}$. Set $\sigma=\begin{pmatrix}0 & q\\ q & 0\end{pmatrix}$ and $\tau=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$. Then $\sigma\tau=\begin{pmatrix}0 & 0\\ q & 0\end{pmatrix}$, $\tau\sigma=\begin{pmatrix}0 & q\\ 0 & 0\end{pmatrix}$, $\sigma\tau\sigma=\begin{pmatrix}0 & 0\\ 0 & q^2\end{pmatrix}$, and $\tau\sigma\tau=0$. Hence

$$\begin{pmatrix}I & 0\\ \tau & I\end{pmatrix}^{-1}\begin{pmatrix}I & \sigma\\ 0 & I\end{pmatrix}\begin{pmatrix}I & 0\\ \tau & I\end{pmatrix}=\begin{pmatrix}I+\sigma\tau & \sigma\\ 0 & I-\tau\sigma\end{pmatrix}=\begin{pmatrix}\alpha & \sigma\\ 0 & \tilde{\alpha}\end{pmatrix},$$

and $\begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix}=\begin{pmatrix}I & \sigma^{\mathrm{T}}\alpha\\ 0 & I\end{pmatrix}\begin{pmatrix}\alpha & \sigma\\ 0 & \tilde{\alpha}\end{pmatrix}$.

Proposition 13.2. — *Let* A *be a Dedekind ring, let* $\mathfrak{q}$ *be an ideal of* A, *and suppose* $n\geq 2$.

a) $\mathrm{Sp}_{2n}(A,\mathfrak{q})=\mathrm{Sp}_2(A,\mathfrak{q})\cdot\mathrm{Ep}_{2n}(A,\mathfrak{q})$.

b) $\mathrm{Ep}_{2n}(A,\mathfrak{q})\supset[\mathrm{Sp}_{2n}(A),\mathrm{Sp}_{2n}(A,\mathfrak{q})]\supset\mathrm{Ep}_{2n}(A,\mathfrak{q}'\cdot\mathfrak{q})$, *where* $\mathfrak{q}'=A$ *if* $n\geq 3$, *and* $\mathfrak{q}'$ *is generated by all* t^2-t, $t\in A$, *if* $n=2$.

c) *Every subgroup of finite index in* $\mathrm{Sp}_{2n}(A)$ *contains* $\mathrm{Ep}_{2n}(A,\mathfrak{q})$ *for some* $\mathfrak{q}\neq 0$.

This is a special case of results proved in [2, Ch. II].

It follows from part *b)* that $\mathrm{Ep}_{2n}(A,\mathfrak{q})$ is normal in $\mathrm{Sp}_{2n}(A)$ so we can introduce the canonical projection,

$$\kappa:\mathrm{Sp}_{2n}(A,\mathfrak{q})\to \mathrm{Cp}_{\mathfrak{q}}=\mathrm{Sp}_{2n}(A,\mathfrak{q})/\mathrm{Ep}_{2n}(A,\mathfrak{q}).$$

We have $$f_1:\mathrm{SL}_2(A,\mathfrak{q})=\mathrm{Sp}_2(A,\mathfrak{q})\to\mathrm{Sp}_{2n}(A,\mathfrak{q}),$$

and we further introduce $$f_2:\mathrm{SL}_2(A,\mathfrak{q})\to\mathrm{Sp}_{2n}(A,\mathfrak{q})$$

which is the composite of the inclusion, $\mathrm{SL}_2(A,\mathfrak{q})\subset\mathrm{GL}_n(A)$, with the homomorphism (12.2): $\mathrm{GL}_n(A)\to\mathrm{Sp}_{2n}(A)$. From Lemma 13.1 we see that $\mathrm{E}_2(A,\mathfrak{q})\subset\ker(\kappa f_i)$

for both $i=1$ and 2. Moreover (13.2) *b)* implies that $[E(A), SL_2(A, \mathfrak{q})] \subset \ker(\kappa f_i)$ as well, for $i=1$ and 2.

Now it follows from Lemma 5.5 that there exist unique maps $\{\ \}, [\ ] : W_\mathfrak{q} \to Cp_\mathfrak{q}$ rendering

$$\begin{array}{ccc} SL_2(A, \mathfrak{q}) & \xrightarrow{f_1} & Sp_{2n}(A, \mathfrak{q}) \\ \downarrow{\scriptstyle 1^{st}\ row} & & \downarrow{\scriptstyle \kappa} \\ W_\mathfrak{q} & \xrightarrow[\{\ \}]{} & Cp_\mathfrak{q} \end{array}$$

and

$$\begin{array}{ccc} SL_2(A, \mathfrak{q}) & \xrightarrow{f_2} & Sp_{2n}(A, \mathfrak{q}) \\ \downarrow{\scriptstyle 1^{st}\ row} & & \downarrow{\scriptstyle \kappa} \\ W_\mathfrak{q} & \xrightarrow[[\ ]]{} & Cp_\mathfrak{q} \end{array}$$

commutative, and they both satisfy axiom MS1 for a Mennicke symbol.

Lemma 13.3. — If $(a, b_1), (a, b_2) \in W_\mathfrak{q}$ *then*

$$\begin{bmatrix} b_1 \\ a \end{bmatrix} \begin{Bmatrix} b_2 \\ a \end{Bmatrix} = \begin{Bmatrix} b_1^2 b_2 \\ a \end{Bmatrix}.$$

Before proving this we shall use it to conclude the proof of Theorem 12.4; this will be accomplished by supplying the hypotheses of Theorem 3.7 for $\{\ \}$.

If $(a, b) \in W_\mathfrak{q}$ then

$$\begin{bmatrix} b \\ a \end{bmatrix} = \begin{Bmatrix} b^2 \\ a \end{Bmatrix}.$$

For if $q = 1 - a \in \mathfrak{q}$ we have $(a, q) \sim_\mathfrak{q} (1, 0)$ so MS1 implies $\begin{Bmatrix} q \\ a \end{Bmatrix} = 1$. Using Lemma 13.3, therefore,

$$\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} \begin{Bmatrix} q \\ a \end{Bmatrix} = \begin{Bmatrix} b^2 q \\ a \end{Bmatrix} = \begin{Bmatrix} b^2 q + b^2 a \\ a \end{Bmatrix} = \begin{Bmatrix} b^2 \\ a \end{Bmatrix}.$$

In particular, $(a, b) \mapsto \begin{Bmatrix} b^2 \\ a \end{Bmatrix}$ satisfies MS1.

Next let $$f : Cp_\mathfrak{q} \to C_\mathfrak{q}$$

be the homomorphism induced by the inclusion $Sp_{2n}(A, \mathfrak{q}) \to SL_{2n}(A, \mathfrak{q})$. The composite $f \circ \{\ \} = [\ ]_\mathfrak{q} : W_\mathfrak{q} \to C_\mathfrak{q}$ is just the map denoted $[\ ]$ in Theorem 4.1. This is because, as remarked above, the composite

$$SL_2(A, \mathfrak{q}) \xrightarrow{f_1} Sp_{2n}(A, \mathfrak{q}) \longrightarrow SL_{2n}(A, \mathfrak{q})$$

differs from the embedding used in Chapter II only by conjugation by a permutation matrix, whereas $C_\mathfrak{q} \subset \text{center}(SL_{2n}(A)/E_{2n}(A, \mathfrak{q}))$.

Thanks to Theorem 4.1, we have now shown that the maps in the commutative diagram

$$\begin{array}{ccc} & \{\,\} \nearrow & \mathrm{Cp}_q \\ \mathrm{W}_q & & \downarrow f \\ & [\,]_q \searrow & \mathrm{C}_q \end{array}$$

satisfy all the hypotheses of Theorem 3.7, so the latter implies f is an isomorphism and that $\{\,\}$ is a universal Mennicke symbol on W_q. This proves Theorem 12.4, modulo the:

Proof of Lemma 13.3. — If $\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathrm{A}, \mathfrak{q})$ then

$$f_1\alpha=\begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad f_2\alpha=\begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix}$$

where $\tilde{\alpha}={}^{\mathrm{T}}\alpha^{-1}=\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\alpha\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}$. The symbols $\left\{\begin{matrix} b \\ a \end{matrix}\right\}$ and $\left[\begin{matrix} b \\ a \end{matrix}\right]$ are the classes modulo $\mathrm{Ep}_{2n}(\mathrm{A}, \mathfrak{q})$ of $f_1\alpha$ and $f_2\alpha$, respectively. Hence it suffices to prove the lemma in Sp_4. Moreover since $[\mathrm{Sp}_{2n}(\mathrm{A}), \mathrm{Sp}_{2n}(\mathrm{A}, \mathfrak{q})]\subset \mathrm{Ep}_{2n}(\mathrm{A}, \mathfrak{q})$ we can replace α by $\tilde{\alpha}$ without changing the symbols.

Given $(a, b_1), (a, b_2)\in \mathrm{W}_\mathfrak{q}$ choose $\alpha_i=\begin{pmatrix} a & b_i \\ c_i & d_i \end{pmatrix}\in \mathrm{SL}_2(\mathrm{A}, \mathfrak{q})$, $i=1, 2$, and set $\beta_1=f_2\tilde{\alpha}_1$, $\beta_2=f_1\alpha_2$. Then $\left[\begin{matrix} b_1 \\ a \end{matrix}\right]\left\{\begin{matrix} b_2 \\ a \end{matrix}\right\}$ is the image modulo $\mathrm{Ep}_{2n}(\mathrm{A}, \mathfrak{q})$ of

$$\beta_1\beta_2=\begin{pmatrix} d_1 & -c_1 & 0 & 0 \\ -b_1 & a & 0 & 0 \\ 0 & 0 & a & b_1 \\ 0 & 0 & c_1 & d_1 \end{pmatrix}\begin{pmatrix} a & 0 & b_2 & 0 \\ 0 & 1 & 0 & 0 \\ c_2 & 0 & d_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$=\begin{pmatrix} d_1a & -c_1 & d_1b_2 & 0 \\ -b_1a & a & -b_1b_2 & 0 \\ ac_2 & 0 & ad_2 & b_1 \\ c_1c_2 & 0 & c_1d_2 & d_1 \end{pmatrix}.$$

Right multiplication by $\varepsilon_1=\begin{pmatrix} 1 & 0 & 0 & 0 \\ b_1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -b_1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

gives $\begin{pmatrix} 1 & -c_1 & d_1b_2 & -b_1b_2d_1 \\ 0 & a & -b_1b_2 & b_1^2b_2 \\ ac_2 & 0 & ad_2 & -b_1b_2c_2 \\ c_1c_2 & 0 & c_1d_2 & d_1-b_1c_1d_2 \end{pmatrix}$.

Left multiplication by $\varepsilon_2=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -ac_2 & -c_1c_2 & 1 & 0 \\ -c_1c_2 & 0 & 0 & 1 \end{pmatrix}$

gives $\begin{pmatrix} 1 & -c_1 & d_1b_2 & -b_1b_2d_1 \\ 0 & a & -b_1b_2 & b_1^2b_2 \\ 0 & 0 & 1 & 0 \\ 0 & c_1^2c_2 & e & d_3 \end{pmatrix}$, where

$$e=c_1d_2-c_1c_2d_1b_2 \qquad \text{and} \qquad d_3=d_1-b_1c_1d_2+c_1c_2b_1b_2d_1.$$

Right multiplication by $\varepsilon_3=\begin{pmatrix} 1 & c_1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -c_1 & 1 \end{pmatrix}$

gives $\begin{pmatrix} 1 & 0 & ad_1^2b_2 & -b_1b_2d_1 \\ 0 & a & -ad_1b_1b_2 & b_1^2b_2 \\ 0 & 0 & 1 & 0 \\ 0 & c_1^2c_2 & e-c_1d_3 & d_3 \end{pmatrix}$.

Right multiplication by $\varepsilon_4=\begin{pmatrix} 1 & 0 & -ad_1^2b_2 & b_1b_2d_1 \\ 0 & 1 & b_1b_2d_1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

gives $\gamma=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b_1^2b_2 \\ 0 & 0 & 1 & 0 \\ 0 & c_1^2c_2 & 0 & d_3 \end{pmatrix}$.

If $\alpha_3=\begin{pmatrix} a & b_1^2b_2 \\ c_1^2c_2 & d_3 \end{pmatrix}$ then γ is evidently conjugate in $\mathrm{Sp}_4(A, \mathfrak{q})$ to $f_1\alpha_3$, so $\begin{pmatrix} b_1^2b_2 \\ a \end{pmatrix}$ is the image mod $\mathrm{Ep}_{2n}(A, \mathfrak{q})$ of $\gamma=\varepsilon_2\beta_1\beta_2\varepsilon_1\varepsilon_3\varepsilon_4$. Since each $\varepsilon_i\in\mathrm{Ep}_{2n}(A, \mathfrak{q})$ (thanks to Lemma 13.1 for $i=1, 3$) it follows that $\begin{pmatrix} b_1^2b_2 \\ a \end{pmatrix}$ is the image of $\beta_1\beta_2$ mod $\mathrm{Ep}_{2n}(A, \mathfrak{q})$, and this proves the lemma.

Chapter IV

THE CONGRUENCE SUBGROUP CONJECTURE. APPLICATIONS

§ 14. First variations of the problem.

The results of the preceding chapters solve, for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, what we describe below as the " congruence subgroup problem ". There is strong evidence that similar phenomena should be witnessed for more general semi-simple algebraic groups, so we shall formulate the question in this more general setting.

In this section we fix a global field k and a finite non empty set S of primes of k containing all archimedean primes. We shall call S *totally imaginary* if all $\mathfrak{p} \in S$ are complex. This means k is a totally imaginary number field and S is just its set of archimedean primes. Departing slightly from our earlier notation we shall write

$$\mathcal{O} = \mathcal{O}^S = \{x \in k \mid \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \qquad \text{for all } \mathfrak{p} \notin S\}.$$

A_k denotes the adèle ring of k, and A_k^S the ring of S-adèles of k, i.e. the restricted product of the completions $k_{\mathfrak{p}}$ at all $\mathfrak{p} \notin S$. For any field F, μ_F denotes the group of roots of unity in F.

Let G be a linear algebraic group over k, and let $\Gamma = G_k \cap GL_n(\mathcal{O})$, with respect to some faithful representation $G \to GL_n$ defined over k. The questions we shall pose turn out to be independent of the choice of this representation. We write $\Gamma_{\mathfrak{q}} = \Gamma \cap GL_n(\mathcal{O}, \mathfrak{q})$ for $\mathfrak{q}$ an ideal of $\mathcal{O}$, and call a subgroup of Γ which contains $\Gamma_{\mathfrak{q}}$, for some $\mathfrak{q} \neq 0$, an S-*congruence subgroup* of Γ. These are evidently of finite index in Γ, and one can ask, conversely:

Congruence Subgroup Problem: *Is every subgroup of finite index in* Γ *an* S-*congruence subgroup?*

Two subgroups of G_k are called commensurable if their intersection has finite index in each of them. The subgroups commensurable with Γ will be called S-*arithmetic subgroups*. In case k is a number field and S is the set of archimedean primes then these are just the arithmetic subgroups of G_k in the sense of Borel-Harish-Chandra [8]. We obtain two Hausdorff topologies on G_k, the S-*congruence topology*, and the S-*arithmetic topology*, by taking as a base for neighborhoods of 1 the S-congruence subgroups of Γ, and the S-arithmetic subgroups respectively. Since the latter topology refines the former there is a canonical continuous homomorphism

$$\hat{G}_k \xrightarrow{\pi} \bar{G}_k$$

between the corresponding completions of G_k. Write $\hat{\Gamma}$ and $\overline{\Gamma}$ for the closure of Γ in $\hat{G}_k$, respectively, $\overline{G}_k$. Clearly $\hat{\Gamma}$ is just the profinite completion of Γ, so it is a *compact* and open subgroup of $\hat{G}_k$. It follows that $\pi(\hat{\Gamma}) = \overline{\Gamma}$, an open subgroup of $\overline{G}_k$. Therefore $\pi(\hat{G}_k)$ is an open and dense subgroup of $\overline{G}_k$ so π is *surjective*. Writing

$$C^S(G_k) = \ker(\pi) = \ker(\pi | \hat{\Gamma})$$

we see that $C^S(G_k)$ is a profinite group, and we have a topological group extension,

$$E^S(G_k) : 1 \to C^S(G_k) \to \hat{G} \xrightarrow{\pi} \overline{G}_k \to 1.$$

Since both the right hand terms are constructed as completions of G_k the inclusion $G_k \subset \hat{G}_k$ can be viewed as a *splitting* of $E^S(G_k)$ when restricted to the subgroup $G_k \subset \overline{G}_k$.

The congruence subgroup problem asks whether the two topologies above coincide, or, equivalently, whether π is an isomorphism. Thus we can restate it:

Congruence Subgroup Problem: Is $C^S(G_k) = \{1\}$?

The S-congruence topology on G is clearly just the topology induced by the embedding $G_k \to G_{(A_k^S)}$, which comes from the diagonal embedding of k in its ring of S-adèles. Therefore *we can identify* $\overline{G}_k$ *with the closure of* G_k *in* $G_{(A_k^S)}$. In this connection we have the:

Strong Approximation Theorem (M. Kneser [13]). — *Suppose k is a number field and let* G *be simply connected and (almost) simple, but not of type* E_8. *Then, if* $G_{k_\mathfrak{p}}$ *is not compact for some* $\mathfrak{p} \in S$, G_k *is dense in* $G_{(A_k^S)}$. *I.e.* $\overline{G}_k = G_{(A_k^S)}$.

Here " simply connected " is taken in the algebraic sense. It is equivalent to the condition that for some (and therefore for every) embedding $k \to \mathbf{C}$, the corresponding Lie group $G_\mathbf{C}$ is a simply connected topological group.

Congruence Subgroup Conjecture. — *Let* G *be a simply connected, simple, Chevalley group of rank* > 1, *and let*

$$E^S(G_k) : 1 \to C^S(G_k) \to \hat{G}_k \to \overline{G}_k \to 1$$

be the extension constructed above. Then this extension is central, and

$$C^S(G_k) \cong \begin{cases} \mu_k & \text{if S is totally imaginary} \\ \{1\} & \text{otherwise.} \end{cases}$$

Recall that G is a Chevalley group if it has a split k-torus of dimension equal to the rank of G.

Theorem 14.1. — *The congruence subgroup conjecture is true for* $G = SL_n$ $(n \geq 3)$ *and for* $G = Sp_{2n}$ $(n \geq 2)$.

Proof. — First consider $G = SL_n$ $(n \geq 3)$, and write $E_\mathfrak{q} = E_n(\mathcal{O}, \mathfrak{q}) \subset \Gamma_\mathfrak{q} = SL_n(\mathcal{O}, \mathfrak{q})$, in the notation of Chapter II. It follows from Corollary 4.3 that $E_\mathfrak{q}$ has finite index in Γ (for $\mathfrak{q} \neq 0$), and it follows from Theorem 7.5 *e)* that every subgroup of finite index

in Γ contains an E_q for some $q \neq 0$. Therefore the E_q are a cofinal family of subgroups of finite index so $\hat{\Gamma} = \varprojlim \Gamma/E_q$. Since $\bar{\Gamma} = \varprojlim \Gamma/\Gamma_q$ we have

$$C = C^S(SL_n(k)) = \ker(\pi \mid \hat{\Gamma}) = \varprojlim \Gamma_q/E_q = \varprojlim C_q,$$

where $C_q = \Gamma_q/E_q$ is the group occuring in Theorem 4.1. Now the conjectured evaluation of C follows from Corollary 4.3. Since G is simply connected, it is known that G_k is generated by its unipotent subgroups, and hence has no finite quotients $\neq \{1\}$. Therefore it must centralize the finite group C.

By density, therefore, $C \subset$ center $\hat{G}_k$.

The proof for $G = Sp_{2n}$ $(n \geq 2)$ is similar. For E_q we take $Ep_{2n}(\mathcal{O}, q)$, and use Corollary 12.5 and Proposition 13.2 *c)* to verify that the E_q are a cofinal family of subgroups of finite index. Then the theorem follows as above, this time with the aid of Corollary 12.5.

Remarks. — 1) Matsumoto [15] outlined a method for proving that $C^S(G_k) = \{1\}$, starting from the assumption that this is so for SL_3 and Sp_4. Mennicke (unpublished) has also announced such a procedure. It seems likely that these methods might be used, in conjunction with Theorem 14.1, to prove at least the finiteness of $C^S(G_k)$, and perhaps even that it is a quotient of μ_k.

2) To prove the opposite " inequality " in the totally imaginary case the following observation is useful: If $\rho : G \to G'$ is a homomorphism of algebraic groups defined over k there is an induced homomorphism $C^S(\rho_k) : C^S(G_k) \to C^S(G'_k)$, since ρ_k is automatically continuous in both topologies. Now if we use the κ_n in Chapter II to identify $C^S(SL_n(k)) = \mu_k$, then every representation $\rho : G \to SL_n$ defined over k gives us a homomorphism $\bar{\rho} : C^S(G_k) \to \mu_k$. If we write the group $\mathrm{Hom}(C^S(G_k), \mu_k)$ additively then $\rho \to \bar{\rho}$ defines an additive map

$$R_k(G) \to \mathrm{Hom}(C^S(G_k), \mu_k),$$

where $R_k(G)$ is the k-representation ring of G. The behavior under multiplication is given by

$$\overline{\rho \otimes \sigma} = (\dim \rho)\bar{\sigma} + \bar{\rho}(\dim \sigma).$$

We thus obtain a pairing $R_k(G) \times C^S(G_k) \to \mu_k$; using subgroups of G isomorphic to SL_2 this can be used to give lower bounds for $C^S(G_k)$.

§ 15. Relationship to the work of C. Moore. The " Metaplectic Conjecture ".

Let L be a locally compact group (we shall understand this to mean separable also) and let M be a locally compact L-module, i.e. a locally compact abelian group with a continuous action $L \times M \to M$. If N is another such module we write $\mathrm{Hom}_L(M, N)$ for the continuous L-homomorphisms from M to N. C. Moore [19] has defined cohomology groups $H^n(L, M)$, $n \geq 0$, which have the usual formal properties, and the usual

interpretations in low dimensions if one suitably accounts for the topological restrictions. In particular $H^2(L, M)$ classifies group extensions

$$1 \to M \xrightarrow{i} E \xrightarrow{p} L \to 1,$$

inducing the given action of L on M, and where p and i are continuous homomorphisms which induce topological isomorphisms $M \to iM$ and $E/iM \to L$.

Examples of these are the extensions

$$E^S(G_k) : 1 \to C^S(G_k) \to \hat{G}_k \to \bar{G}_k \to 1$$

constructed in the last section, provided we assume $C^S(G_k)$ is in the center of $\hat{G}_k$. If we put $C = C^S(G_k)$, and write $e = (E^S(G_k)) \in H^2(\bar{G}_k, C)$, then the fact that $E^S(G_k)$ splits over $G_k \subset \bar{G}$ can be written

$$e \in \ker(H^2(\bar{G}_k, C) \xrightarrow{\text{restr}} H^2(G_k, C)),$$

where we view $G_k \to \bar{G}_k$ as a homomorphism of locally compact groups, giving G_k the discrete topology. Now if $f : C \to M$ is a continuous homomorphism of locally compact $\bar{G}_k$-modules then

$$f(e) \in \ker(H^2(\bar{G}_k, M) \xrightarrow{\text{restr}} H^2(G_k, M)).$$

Theorem 15.1. — *Let* M *be a profinite* $\bar{G}_k$*-module. Then*

$$\mathrm{Hom}_{\bar{G}_k}(C, M) \longrightarrow \ker(H^2(\bar{G}_k, M) \xrightarrow{\text{restr}} H^2(G_k, M)),$$

by $f \mapsto f(e)$, *is surjective. If* $\bar{G}_k$ *acts trivially on* C *and on* M, *and if* G_k *has no non-trivial finite abelian quotients, then it is bijective.*

Proof. — If $x \in \ker(H^2(\bar{G}_k, M) \to H^2(G_k, M))$ let

$$1 \to M \to E \xrightarrow{p} \bar{G}_k \to 1$$

be an extension representing x. By assumption there is a section $s : G_k \to E$ such that $ps(\gamma) = \gamma$ for $\gamma \in G_k$.

Write $\bar{\Gamma}$ for the closure of Γ in $\bar{G}_k$, and set $F = p^{-1}(\bar{\Gamma})$, so that we have an induced extension

$$1 \to M \to F \to \bar{\Gamma} \to 1.$$

This shows that F is compact and totally disconnected, since M and $\bar{\Gamma}$ are, so F is a profinite group. Consequently $s \mid \Gamma$ extends to a continuous homomorphism $\hat{s} : \hat{\Gamma} \to F$. Therefore $s : G_k \to E$ is continuous for the S-arithmetic topology, since it is continuous in a neighborhood of 1. The completeness of E now allows us to extend s to a continuous homomorphism $\hat{s} : \hat{G}_k \to E$. Now the square

$$\begin{array}{ccc} E & \xrightarrow{p} & \bar{G}_k \\ \uparrow & & \| \\ \hat{G}_k & \xrightarrow{\pi} & \bar{G}_k \end{array}$$

commutes on $G_k \subset \hat{G}_k$, so it commutes because G_k is dense in $\hat{G}_k$ and the arrows are continuous. Thus we have constructed a morphism

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & \overline{G}_k & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle \hat{s}} & & \| & & \\ 1 & \longrightarrow & C & \longrightarrow & \hat{G}_k & \longrightarrow & \overline{G}_k & \longrightarrow & 1 \end{array}$$

of group extensions, and f is therefore the required $\overline{G}_k$-homomorphism for which $f(e)=x$.

Now suppose given $f: C \to M$. Factor f into $C \xrightarrow{g} C/\ker f \xrightarrow{h} M$. Then $g(e)$ corresponds to the extension

$$1 \to C/\ker f \to \hat{G}_k/\ker f \to \overline{G}_k \to 1.$$

If it splits and if $C \subset$ center $\hat{G}_k$ then $C/\ker f$ is an abelian quotient of $\hat{G}_k/\ker f$. If G_k has no non trivial finite abelian quotients then, by density, neither does $\hat{G}_k$, so $C/\ker f = 0$. This shows, under the hypotheses of the theorem, that $f \neq 0 \Rightarrow g(e) \neq 0$. Now if, further, $\overline{G}_k$ acts trivially on M then $H^1(\overline{G}_k, \text{coker } h) = \text{Hom}(\overline{G}_k, \text{coker } h) = 0$, so the cohomology sequence of $0 \to C/\ker f \xrightarrow{h} M \to \text{coker } h \to 0$ yields

$$0 = H^1(\overline{G}_k, \text{coker } h) \to H^2(\overline{G}_k, C) \xrightarrow{h} H^2(\overline{G}_k, M).$$

Hence $f(e) = h(g(e)) \neq 0$. Q.E.D.

We can now restate the congruence subgroup conjecture cohomologically. We can even generalize it in a natural way by no longer requiring that the set S contain the archimedean primes, and even allowing S to be empty, in which case $A_k^S = A_k$. For reasons to be explained below we shall call this generalization the:

Metaplectic Conjecture. — Let k be a global field and let S *be any finite set of primes of k (possibly empty). Let* G *be a simply connected, simple, Chevalley group of rank* >1. *Then for any profinite abelian group* M *on which* $G_{(A_k^S)}$ *acts trivially, there is a natural isomorphism*

$$\ker(H^2(G_{(A_k^S)}, M) \xrightarrow{\text{restr}} H^2(G_k, M)) \cong \begin{cases} \text{Hom}(\mu_k, M) & \text{if all } \mathfrak{p} \in S \text{ are complex} \\ \{1\} & \text{otherwise.} \end{cases}$$

More concretely, this means that there exists a central extension

$$1 \to \mu_k \to \widetilde{G} \to G_{A_k} \to 1, \tag{15.2}$$

which splits over $G_k \subset G_{A_k}$, and that any other such, say

$$1 \to M \to E \to G_{A_k} \to 1,$$

with profinite kernel M, is induced by a unique homomorphism $\mu_k \to M$. Moreover, for any non complex prime $\mathfrak{p}$, the restriction of (15.2) to the factor $G_{k_\mathfrak{p}} \subset G_{A_k}$ has order exactly $[\mu_k : 1]$ in $H^2(G_{k_\mathfrak{p}}, \mu_k)$.

The last assertion is deduced as follows: Let $x \in H^2(G_{A_k}, \mu_k)$ be the class of the

extension (15.2). For any $\mathfrak{p}$, $G_{A_k} = G_{k_\mathfrak{p}} \times G_{(A_k^\mathfrak{p})}$, and $H^1(G_{k_\mathfrak{p}}, \mu_k) = 0$ because G_k is generated by unipotents. Therefore if the restriction of x to $H^2(G_{k_\mathfrak{p}}, \mu_k)$ is killed by n then it follows from the Künneth formula that nx is the inflation of an element of $H^2(G_{(A_k^\mathfrak{p})}, \mu_k)$ which splits on G_k. But, according to the conjecture, the group of such elements is zero if $\mathfrak{p}$ is not complex, and hence $nx = 0$.

The existence of (15.2) has been suggested by C. Moore as a natural generalization of Weil's " metaplectic " groups [25]. The latter are certain two sheeted coverings in the case $G = Sp_{2n}$. We might thus call the alleged $\widetilde{G}$ the " metaplectic group of G " over k. Moore, in unpublished work, has proved a number of interesting theorems in support of the metaplectic conjecture, and he suggests that we allow an arbitrary locally compact M in its formulation. His procedure, contrary to ours, is local to global. This seems to be the most natural approach since we obtain no direct construction of the local extensions (over the $G_{k_\mathfrak{p}}$'s) and because our method gives us no access to $\widetilde{G}$ when there are real primes or when k is a function field. On the other hand:

Theorem 15.3. — *If k is a totally imaginary number field then the congruence subgroup conjecture for G_k is equivalent to the metaplectic conjecture for G_k, plus the conjecture that $C^S(G_k)$ lies always in the center of $\hat{G}_k$. In particular all these conjectures are true in this case for $G = SL_n$ $(n \geq 3)$ and $G = Sp_{2n}$ $(n \geq 2)$.*

Proof. — In view of Theorem 15.1 we see that the congruence subgroup conjecture is obtained from the metaplectic conjecture simply by requiring the sets S to contain all archimedean primes. We must therefore show that this restriction costs us nothing when k is totally imaginary.

Given any finite set S let T be the union of S and the set of archimedean primes. Then

$$A_k^T \cong A_k^S \times \mathbf{C}^r$$

for some $r \geq 0$, since k is totally imaginary. Therefore

$$G_{(A_k^T)} \cong G_{(A_k^S)} \times G_{\mathbf{C}^r}.$$

Now $G_\mathbf{C}$ is a complex semi-simple Lie group which, by hypothesis, is simply connected. It follows that

$$H^1(G_{\mathbf{C}^r}, M) = H^2(G_{\mathbf{C}^r}, M) = 0$$

for any profinite abelian group M on which $G_\mathbf{C}$ acts trivially. From this it follows that the projection

$$G_{(A_k^T)} \to G_{(A_k^S)}$$

induces an isomorphism $H^2(G_{(A_k^S)}, M) \xrightarrow{\text{inf}} H^2(G_{(A_k^T)}, M)$. The projection is compatible with the embeddings of G_k, so we have now a natural isomorphism

$$\ker(H^2(G_{(A_k^S)}, M) \xrightarrow{\text{restr}} H^2(G_k, M))$$
$$\cong \ker(H^2(G_{(A_k^T)}, M) \xrightarrow{\text{restr}} H^2(G_k, M)).$$

Thus the metaplectic conjecture for S is equivalent to the same for T, and T contains the archimedean primes, so the theorem is proved.

In case there are real primes the argument above decidedly fails, since, e.g., $\pi_1(G_{\mathbf{R}}) \cong \mathbf{Z}/2\mathbf{Z}$ if G is not of type C_n. However, by a slight artifice, we can still deduce a partial local result at the finite primes of any number field.

Theorem 15.4. — Let k be a number field and let q *be a finite prime of k. Suppose* G *is a simply connected, simple, Chevalley group for which the congruence subgroup conjecture holds over all number fields* (for instance SL_n, $n \geq 3$, or Sp_{2n}, $n \geq 2$). *Then* $H^2(G_{k_q}, \mu_{k_q})$ *contains an element of order* $[\mu_{k_q} : 1]$.

Proof. — Choose a totally imaginary number field L which contains μ_{k_q} and which has a finite prime p such that $L_p \cong k_q$; this is quite easy to do. Clearly then $\mu_L = \mu_{k_q}$. Let S be the set of archimedean primes of L. Then, by the congruence subgroup conjecture, we obtain a central extension

$$1 \to \mu_L \to \hat{G}_L \to G_{A_L^S} \to 1$$

whose restriction to G_{L_p} has order $[\mu_L : 1]$, as we have seen above. Q.E.D.

§ 16. Recovery of G-representations from those of an arithmetic subgroup.

Let G be a semi-simple, simply connected, algebraic group defined over $\mathbf{Q}$, and let Γ be an arithmetic subgroup of $G_{\mathbf{Q}}$. In the notation of § 14 this is an S-arithmetic subgroup where $S = \{\infty\}$. We will write A^f for the ring of *finite* adèles of $\mathbf{Q}$. (This is $A_{\mathbf{Q}}^{\{\infty\}}$ in our previous notation.) The closure of Γ in G_{A^f} is a profinite group, so there is a canonical continuous homomorphism

$$\pi : \hat{\Gamma} \to G_{A^f},$$

where $\hat{\Gamma}$ is the profinite completion of Γ. The main theorem of this section will invoke the following hypothesis:

(16.1)
a) $\pi(\hat{\Gamma})$ is open in G_{A^f}.
b) $\ker(\pi)$ is finite.

It is easy to see that these conditions depend only on G over $\mathbf{Q}$, and not on the choice of Γ. Moreover *a)* follows from Kneser's strong approximation theorem whenever the latter applies. This requires, essentially, that all factors of G be not of type E_8 and non compact over $\mathbf{R}$. Part *b)* is a qualitative form of the conclusions of the congruence subgroup conjecture. It says, in the notation of § 14, that $C^{\{\infty\}}(G_{\mathbf{Q}})$ is a finite group. In particular it has been proved above for certain G.

Conjecture. — (16.1) *is true if* G *is simple relative to* $\mathbf{Q}$, *and of* $\mathbf{Q}$*-rank* (in the sense of Borel-Tits [9]) ≥ 2.

Theorem 16.2. — *With the hypothesis* (16.1), *suppose given a group homomorphism* $f : \Gamma \to \mathrm{GL}_n(\mathbf{Q})$. *Then there is a homomorphism of algebraic groups*

$$F : G \to \mathrm{GL}_n,$$

defined over $\mathbf{Q}$, *which coincides with* f *on a subgroup of finite index of* Γ.

Corollary 16.3. — *If* V *is a finite* $\mathbf{Q}$*-dimensional* $\mathbf{Q}[\Gamma]$*-module there is a lattice in* V *stable under* Γ.

Proof. — Say $F : G \to \mathrm{GL}(V)$ agrees with f on $\Gamma' \subset \Gamma$, a subgroup of finite index. Then one knows that $F(\Gamma')$ is an arithmetic subgroup of $F(G)_{\mathbf{Q}}$, so $F(\Gamma')$ leaves some lattice, say L', invariant. Then $L = \sum_{s \in \Gamma/\Gamma'} sL'$ is stable under Γ.

Corollary 16.4. — *Every exact sequence*

$$0 \to V \to V' \to V'' \to 0$$

of finite $\mathbf{Q}$*-dimensional* $\mathbf{Q}[\Gamma]$*-modules splits. In particular* $H^1(\Gamma, V) = 0$.

Proof. — Passing to a subgroup Γ' of finite index in Γ, this becomes a sequence of Γ'-modules induced by an exact sequence of " algebraic " G-modules over $\mathbf{Q}$. Since G is semi-simple this sequence splits, and therefore it splits over Γ'. If $g' : V'' \to V'$ is a Γ'-splitting then $g(x) = \frac{1}{[\Gamma : \Gamma']} \sum_{s \in \Gamma/\Gamma'} sg'(s^{-1}x)$ defines a Γ-splitting.

The vanishing of $H^1(\Gamma, V)$ corresponds to the case $V'' = \mathbf{Q}$ with trivial action.

Corollary 16.5. — *If* Γ *operates on a finitely generated* $\mathbf{Z}$*-module* M *then* $H^1(\Gamma, M)$ *is finite.*

Proof. — Since Γ is finitely generated $H^1(\Gamma, M)$ is a finitely generated $\mathbf{Z}$-module. Now tensor with $\mathbf{Q}$ and apply the last corollary.

Remark. — The vanishing of $H^1(\Gamma, \mathrm{ad})$, where ad is the adjoint representation of G, implies the " rigidity " of Γ, i.e. the triviality of deformations of Γ in $G_{\mathbf{R}}$ (see Weil [24]). Garland has proved that $H^1(\Gamma, \mathrm{ad}) = 0$ for Chevalley groups, and Borel proved rigidity when G is semi-simple of $\mathbf{Q}$-rank ≥ 2 and such that every simple factor has $\mathbf{Q}$-rank ≥ 1. Finally, Raghunathan [21] proved the vanishing of $H^1(\Gamma, V)$ for these G and for any *faithful, irreducible* rational G-module V. On the other hand D. Kajdan has obtained vanishing of H^1 for the trivial representation in some cases.

Corollary 16.6. — *Assume* (16.1) *and that* $G_{\mathbf{Q}}$ *is generated by unipotents. Then every group homomorphism* $f : G_{\mathbf{Q}} \to \mathrm{GL}_n(\mathbf{Q})$ *is algebraic.*

Proof. — It follows from Theorem 16.2 that there is an algebraic homomorphism $F : G \to \mathrm{GL}_n$, defined over $\mathbf{Q}$, such that F and f agree on an arithmetic subgroup, Γ, of $G_{\mathbf{Q}}$. To show that F and f agree on all of $G_{\mathbf{Q}}$ it suffices, by hypothesis, to show that they agree on each abelian unipotent algebraic subgroup U of $G_{\mathbf{Q}}$. Since F is algebraic, F(U) is unipotent in $\mathrm{GL}_n(\mathbf{Q})$. The group U is isomorphic to a vector space over $\mathbf{Q}$, and $\Gamma \cap U$ is a lattice of maximal rank in U. Hence, if we show that $f(U)$ is unipotent then it will follow from Lemma 16.7 below, that f and F agree on U, since they agree on the lattice $\Gamma \cap U$.

Suppose $x \in \mathrm{GL}_n(\mathbf{Q})$ is such that some power of x is unipotent. Then the eigenvalues of x are roots of unity as well as roots of a polynomial of degree n over $\mathbf{Q}$. It follows that they are N-th roots of unity for some N depending only on n, and hence x^N is unipotent.

Now suppose $x \in U$. Then $x = y^N$ for some $y \in U$. Some power of y lies in $\Gamma \cap U$, so some power of $f(y)$ lies in $f(\Gamma \cap U) = F(\Gamma \cap U)$, which is unipotent. Therefore $f(x) = f(y)^N$ is unipotent, as was to be shown.

Lemma 16.7. — Let k be a field of characteristic zero, and suppose $x, y \in \mathrm{GL}_n(k)$ are unipotent and that $x^m = y^m$ for some $m > 0$. Then $x = y$.

Proof. — We can write a unipotent x uniquely as $x = \exp(X)$ with $X (= \log(x))$ nilpotent, the " series " exp and log here being in fact polynomials. Hence if $x^m = y^m$ then $mX = mY$, so $X = Y$ and therefore $x = y$.

Proof of Theorem 16.2. — Since Γ is finitely generated there exists a prime p such that all elements of $f(\Gamma)$ are p-integral. (For each generator γ_i of Γ choose a common denominator for $f(\gamma_i)$ and $f(\gamma_i^{-1})$, and take p prime to all these denominators.) Then f extends continuously to

$$f_p : \hat{\Gamma} \to \mathrm{GL}_n(\mathbf{Z}_p).$$

Replacing Γ by a subgroup of finite index, if necessary, we can identify $\hat{\Gamma}$ with an open subgroup of $G_{\mathbf{A}f}$ of the form $\prod_q U_q$, where U_q is a compact open subgroup of $G_{\mathbf{Q}_q}$, equal to $G_{\mathbf{Z}_q}$ for almost all q. Then if $q \neq p$ it is easy to see that the image of the q-adic group U_q in the p-adic group $\mathrm{GL}_n(\mathbf{Z}_p)$ must be finite.

Since $\mathrm{GL}_n(\mathbf{Z}_p)$ has " no small finite subgroups ", i.e. since it has a neighborhood of the identity containing no non trivial finite subgroups, it follows by continuity of f_p that $f_p(U_q) = \{1\}$ for almost all q.

Passing again to a subgroup of finite index in Γ, therefore, we can arrange that $f_p(U_q) = 1$ for all $q \neq p$. Thus f factors as the composite

$$\Gamma \to U_p \xrightarrow{\varphi} \mathrm{GL}_n(\mathbf{Z}_p),$$

where φ is a continuous homomorphism. Now by the theory of p-adic Lie groups (see [23, III (3.2.3.1)]) φ is analytic, and its tangent map at the identity is a homomorphism

$$L(\varphi) : \mathfrak{g} \otimes_{\mathbf{Q}} \mathbf{Q}_p \to \mathfrak{gl}_n(\mathbf{Q}_p)$$

of the associated Lie algebras over $\mathbf{Q}_p$. Since G is semi-simple and simply connected there is a unique homomorphism of algebraic groups, $F : G \to \mathrm{GL}_n$, defined over $\mathbf{Q}_p$, with tangent map $L(\varphi)$. Therefore F agrees locally over $\mathbf{Q}_p$ with f_p, so F coincides with f on a subgroup, Γ', of finite index in Γ. It remains only to be seen that F is defined over $\mathbf{Q}$. This follows from the fact that $F(\Gamma') = f(\Gamma') \subset \mathrm{GL}_n(\mathbf{Q})$, and the fact that Γ' is Zariski-dense in G.

REFERENCES

[1] BASS (H.), K-theory and stable algebra, *Publ. I.H.E.S.*, n° 22 (1964), 5-60.

[2] —, *Symplectic modules and groups* (in preparation).

[3] BASS (H.), HELLER (A.) and SWAN (R.), The Whitehead group of a polynomial extension, *Publ. I.H.E.S.*, n° 22 (1964), 61-79.

[4] BASS (H.), LAZARD (M.) and SERRE (J.-P.), Sous-groupes d'indice fini dans SL(n, **Z**), *Bull. Am. Math. Soc.*, 385-392.

[5] BASS (H.) and MILNOR (J.), *Unimodular groups over number fields* (mimeo. notes), Princeton University (1965).

[6] —, *On the congruence subgroup problem for* $\mathrm{SL}_n(n \geq 3)$ *and* $\mathrm{Sp}_{2n}(n \geq 2)$. (Notes, Inst. for Adv. Study.)

[7] BASS (H.) and MURTHY (M. P.), Grothendieck groups and Picard groups of abelian group rings, *Ann. of Math.*, 86 (1967), 16-73.

[8] BOREL (A.) and HARISH-CHANDRA, Arithmetic subgroups of algebraic groups, *Ann. of Math.*, 75 (1962), 485-535.

[9] BOREL (A.) and TITS (J.), Groupes réductifs, *Publ. I.H.E.S.*, n° 27 (1965), 55-151.

[10] CHEVALLEY (C.), Sur certains schémas de groupes semi-simples, *Sém. Bourbaki* (1961), exposé 219.

[11] HIGMAN (G.), On the units of group rings, *Proc. Lond. Math. Soc.*, 46 (1940), 231-248.

[12] HURWITZ (A.), Die unimodularen Substitutionen in einem algebraischen Zahlkörpen (1895), *Mathematische Werke*, vol. 2, 244-268, Basel (1933).

[13] KNESER (M.), Strong approximation, I, II, Algebraic groups and discontinuous subgroups, *Proc. Symp. Pure Math.*, IX, A.M.S., 1966, p. 187-196.

[14] KUBOTA (T.), Ein arithmetischer Satz über eine Matrizengrouppe, *J. reine angew. Math.*, 222 (1965), 55-57.

[15] MATSUMOTO (H.), Subgroups of finite index of arithmetic groups. Algebraic groups and Discontinuous Subgroups, *Proc. Symp. Pure Math.*, IX, A.M.S., 1966, p. 99-103.

[16] MENNICKE (J.), Finite factor groups of the unimodular group, *Ann. of Math.*, 81 (1965), 31-37.

[17] —, Zur theorie der Siegelsche Modulgruppe, *Math. Ann.*, 159 (1965), 115-129.

[18] MILNOR (J.), Whitehead torsion, *Bull. Am. Math. Soc.*, 7 (1966), 358-426.

[19] MOORE (C.), Extensions and low dimensional cohomology of locally compact groups, I, *Trans. Am. Math. Soc.*, 113 (1964), 40-63.

[20] O'MEARA (O. T.), On the finite generation of linear groups over Hasse domains, *J. reine angew. Math.*, 217 (1963).

[21] RAGHUNATHAN (M. S.), A vanishing theorem for the cohomology of arithmetic subgroups of algebraic groups (to appear).

[22] REGE (N.), Finite generation of classical groups over Hasse domains (to appear).

[23] LAZARD (M.), Groupes analytiques p-adiques, *Publ. I.H.E.S.*, n° 26 (1965), 5-219.

[24] WEIL (A.), Remarks on the cohomology of groups, *Ann. of Math.*, 80 (1964), 149-157.

[25] —, Sur certains groupes d'opérateurs unitaires, *Acta Math.*, 111 (1964), 143-211.

Manuscrit reçu le 17 mai 1967.