New York Journal of Mathematics

New York J. Math. **13** (2007) 383–421.

Bounded generation of SL(n, A) (after D. Carter, G. Keller, and E. Paige)

Dave Witte Morris

Abstract. We present unpublished work of D. Carter, G. Keller, and E. Paige on bounded generation in special linear groups. Let n be a positive integer, and let $A = \mathcal{O}$ be the ring of integers of an algebraic number field K (or, more generally, let A be a localization $\mathcal{O}S^{-1}$). If $n = 2$, assume that A has infinitely many units.

We show there is a finite-index subgroup H of $\mathrm{SL}(n, A)$, such that every matrix in H is a product of a bounded number of elementary matrices. We also show that if $T \in \mathrm{SL}(n, A)$, and T is not a scalar matrix, then there is a finite-index, normal subgroup N of $\mathrm{SL}(n, A)$, such that every element of N is a product of a bounded number of conjugates of T.

For $n \geq 3$, these results remain valid when $\mathrm{SL}(n, A)$ is replaced by any of its subgroups of finite index.

Contents

Received June 16, 2006. Revised September 14, 2007.
Mathematics Subject Classification. 20H05; 11F06, 19B37.
Key words and phrases. Bounded generation, finite width, special linear group, elementary matrix, stable range, Mennicke symbol, nonstandard analysis.
Partially supported by a grant from the National Sciences and Engineering Research Council of Canada.

ISSN 1076-9803/07

1. Introduction

This paper presents unpublished work of David Carter, Gordon Keller, and Eugene Paige [CKP] — they should be given full credit for the results and the methods of proof that appear here (but the current author is responsible for errors and other defects in this manuscript). Much of this work is at least 20 years old (note that it is mentioned in [DV, p. 152 and bibliography]), but it has never been superseded.

If a set $\mathcal{X}$ generates a group G, then every element of G can be written as a word in $\mathcal{X} \cup \mathcal{X}^{-1}$. We are interested in cases where the length of the word can be bounded, independent of the particular element of G.

(1.1) **Definition.** A subset $\mathcal{X}$ of a group G *boundedly generates* G if there is a positive integer r, such that every element of G can be written as a word of length $\leq r$ in $\mathcal{X} \cup \mathcal{X}^{-1}$. That is, for each $g \in G$, there is a sequence $x_1, x_2, \ldots, x_\ell$ of elements of $\mathcal{X} \cup \mathcal{X}^{-1}$, with $\ell \leq r$, such that $g = x_1 x_2 \cdots x_\ell$.

A well-known paper of D. Carter and G. Keller [CK1] proves that if B is the ring of integers of a number field K, and $n \geq 3$, then the set of elementary matrices $E_{i,j}(b)$ boundedly generates $\mathrm{SL}(n,B)$. One of the two main results of [CKP] is the following theorem that generalizes this to the case $n = 2$, under an additional (necessary) condition on B. (For the proof, see Corollary 3.13(1) and Theorem 5.26.)

(1.2) **Theorem** (Carter–Keller–Paige [CKP, (2.4) and (3.19)])**.** *Suppose:*

- *B is the ring of integers of an algebraic number field K (or, more generally, B is any order in the integers of K),*
- *n is a positive integer,*
- *$\mathrm{E}(n,B)$ is the subgroup of $\mathrm{SL}(n,B)$ generated by the elementary matrices, and*
- *either $n \geq 3$, or B has infinitely many units.*

Then the elementary matrices boundedly generate $\mathrm{E}(n,B)$.

More precisely, there is a positive integer $r = r(n,k)$, depending only on n and the degree k of K over $\mathbb{Q}$, such that:

(1) *Every matrix in $\mathrm{E}(n,B)$ is a product of $\leq r$ elementary matrices.*
(2) $\#\big(\mathrm{SL}(n,B)/\,\mathrm{E}(n,B)\big) \leq r$.

(1.3) **Remark.** If B is (an order in) the ring of integers of a number field K, and B has only finitely many units, then K must be either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. In this case, the elementary matrices do not boundedly generate $\mathrm{SL}(2,B)$ [Ta1, Cor. of Prop. 8, p. 126]. (This follows from the fact [GS] that some finite-index subgroup of $\mathrm{SL}(2,B)$ has a nonabelian free quotient.) Thus, our assumption that $n \geq 3$ in this case is a necessary one.

The following result is of interest even when $\mathcal{X}$ consists of only a single matrix X.

(6.1′) **Theorem** (Carter–Keller–Paige [CKP, (2.7) and (3.21)]). *Let:*

- *B and n be as in Theorem* 1.2*,*
- *$\mathcal{X}$ be any subset of* $\mathrm{SL}(n,B)$ *that does not consist entirely of scalar matrices, and*
- $\mathcal{X}^{\triangleleft} = \left\{ T^{-1}XT \;\middle|\; \begin{matrix} X \in \mathcal{X}, \\ T \in \mathrm{SL}(n,B) \end{matrix} \right\}$.

Then $\mathcal{X}^{\triangleleft}$ boundedly generates a finite-index normal subgroup of $\mathrm{SL}(n,B)$*.*

(1.4) **Remark.**

(1) In the situation of Theorem 6.1′, let $\langle \mathcal{X}^{\triangleleft} \rangle$ be the subgroup generated by $\mathcal{X}^{\triangleleft}$. It is obvious that $\mathcal{X}^{\triangleleft}$ is a normal subgroup of $\mathrm{SL}(n,B)$, and it is well-known that this implies that $\mathcal{X}^{\triangleleft}$ has finite index in $\mathrm{SL}(n,B)$ (cf. 6.4, 6.5, and 6.11).

(2) The conclusion of Theorem 6.1′ states that there is a positive integer r, such that every element of $\mathcal{X}^{\triangleleft}$ is a product of $\leq r$ elements of $\mathcal{X}^{\triangleleft}$ (and their inverses). Unlike in (1.2), we do *not* prove that the bound r can be chosen to depend on only n and k. See Remark 6.2 for a discussion of this issue.

(3) We prove Thms. 1.2 and 6.1′ in a more general form that allows B to be replaced with any localization BS^{-1}. It is stated in [CKP] (without proof) that the same conclusions hold if B is replaced by an arbitrary subring A of any number field (with the restriction that A is required to have infinitely many units if $n = 2$). It would be of interest to establish this generalization.

(4) If Γ is any subgroup of finite index in $\mathrm{SL}(n,B)$, then Theorem 6.1(2) is a generalization of Theorem 1.2 that applies with Γ in the place of $\mathrm{SL}(n,B)$. For $n \geq 3$, Corollary 6.13 is a generalization of Theorem 6.1′ that applies with Γ in the place of $\mathrm{SL}(n,B)$.

Let us briefly outline the proof of Theorem 1.2. (A similar approach applies to Theorem 6.1′.) For n and B as in the statement of the theorem, it is known that the subgroup $\mathrm{E}(n,B)$ generated by the elementary matrices has finite index in $\mathrm{SL}(n,B)$ [BMS, Se, Va]. Theorem 1.2 is obtained by axiomatizing this proof:

(1) Certain ring-theoretic axioms are defined (for $n \geq 3$, the axioms are called $\mathsf{SR}_{1\frac{1}{2}}$, $\mathsf{Gen}(\mathsf{t},\mathsf{r})$, and $\mathsf{Exp}(\mathsf{t},\ell)$, where the parameters t, r, and ℓ are positive integers).

(2) It is shown that the ring B satisfies these axioms (for appropriate choices of the parameters).

(3) It is shown that if A is any integral domain satisfying these axioms, then $\mathrm{E}(n,A)$ is a finite-index subgroup of $\mathrm{SL}(n,A)$.

The desired conclusion is then immediate from the following simple consequence of the Compactness Theorem of first-order logic (see §2B):

(1.5) **Proposition.** *Let*

- *n be a positive integer, and*
- *$\mathcal{T}$ be a set of first-order axioms in the language of ring theory.*

Suppose that, for every commutative ring A satisfying the axioms in $\mathcal{T}$, the subgroup $\mathrm{E}(n, A)$ *generated by the elementary matrices has finite index in* $\mathrm{SL}(n, A)$*. Then, for all such A, the elementary matrices boundedly generate* $\mathrm{E}(n, A)$.

More precisely, there is a positive integer $r = r(n, \mathcal{T})$, such that, for all A as above, every matrix in $\mathrm{E}(n, A)$ *is a product of $\leq r$ elementary matrices.*

(1.6) **Example.** It is a basic fact of linear algebra that if F is any field, then every element of $\mathrm{SL}(n, F)$ is a product of elementary matrices. This yields the conclusion that $\mathrm{E}(n, F) = \mathrm{SL}(n, F)$. Since fields are precisely the commutative rings satisfying the additional axiom $(\forall x)(\exists y)(x \neq 0 \to xy = 1)$, then Proposition 1.5 implies that each element of $\mathrm{SL}(n, F)$ is the product of a bounded number of elementary matrices. (Furthermore, a bound on the number of elementary matrices can be found that depends only on n, and is universal for all fields.) In the case of fields, this can easily be proved directly, by counting the elementary matrices used in a proof that $\mathrm{E}(n, F) = \mathrm{SL}(n, F)$, but the point is that this additional work is not necessary — bounded generation is an automatic consequence of the fact that $\mathrm{E}(n, A)$ is a finite-index subgroup.

Because we obtain bounded generation from the Compactness Theorem (as in (1.5)), the conclusions in this paper do not provide any explicit bounds on the number of matrices needed. It should be possible to obtain an explicit formula by carefully tracing through the arguments in this paper and in the results that are quoted from other sources, but this would be nontrivial (and would make the proofs messier). The applications we have in mind do not require this.

(1.7) **Remark.** Assuming a certain strengthening of the Riemann Hypothesis, Cooke and Weinberger [CW] proved a stronger version of Theorem 1.2 that includes an explicit estimate on the integer r (depending only on n, not on k), under the assumption that B is the full ring of integers, not an order. For $n \geq 3$, the above-mentioned work of D. Carter and G. Keller [CK1, CK2] removed the reliance on unproved hypotheses, but obtained a weaker bound that depends on the discriminant of the number field. For $n = 2$, B. Liehl [Li] proved bounded generation (without explicit bounds), but required some assumptions on the number field K. More recently, for a localization $B_{\mathcal{S}}$ with $\mathcal{S}$ a sufficiently large set of primes, D. Loukanidis and V. K. Murty [LM, Mu] obtained explicit bounds for $\mathrm{SL}(n, B_{\mathcal{S}})$ that depend only on n and k, not the discriminant.

There is also interesting literature on bounded generation of other (arithmetic) groups, e.g., [AM, Bar, DV, ER1, ER2, LM, Mu, Ra, Sh, SS, Ta1, Ta2, vdK, Za].

Acknowledgments. This paper was written during a visit to the University of Auckland. I would like to thank the Department of Mathematics of that institution for its hospitality. I would also like to thank Jason Manning, Lucy Lifschitz, and Alex Lubotzky for bringing the preprint [CKP] to my attention, and an anonymous referee for reading the manuscript carefully and providing numerous corrections and helpful comments.

2. Preliminaries

(2.1) **Assumption.** All rings are assumed to have 1, and any subring is assumed to contain the multiplicative identity element of the base ring. (This is taken to be part of the definition of a ring or subring.)

§2A. Notation.

(2.2) **Definition.** Let B be an integral domain.

(1) A subset S of B is *multiplicative* if S is closed under multiplication, and $0 \notin S$.

(2) If S is a multiplicative subset of B, then

$$BS^{-1} = \left\{ \frac{b}{s} \;\middle|\; b \in B, s \in S \right\}.$$

This is a subring of the quotient field of B.

As usual, we use $\langle \mathcal{X} \rangle$ to denote the subgroup generated by a subset $\mathcal{X}$ of a group G. In order to conveniently discuss bounded generation, we augment this notation with a subscript, as follows.

(2.3) **Definition.** For any subset $\mathcal{X}$ of a group G, and any nonnegative integer r, we define $\langle \mathcal{X} \rangle_r$, inductively, by:

- $\langle \mathcal{X} \rangle_0 = \{1\}$ (the identity element of G).
- $\langle \mathcal{X} \rangle_{r+1} = \langle \mathcal{X} \rangle_r \cdot \big(\mathcal{X} \cup \mathcal{X}^{-1} \cup \{1\}\big)$.

That is, $\langle \mathcal{X} \rangle_r$ is the set of elements of G that can be written as a word of length $\leq r$ in $\mathcal{X} \cup \mathcal{X}^{-1}$. Thus, $\mathcal{X}$ boundedly generates G if and only if we have $\langle \mathcal{X} \rangle_r = G$, for some positive integer r.

(2.4) **Notation.** Let A be a commutative ring, $\mathfrak{q}$ be an ideal of A, and n be a positive integer.

(1) $\mathbb{I}_{n \times n}$ denotes the $n \times n$ identity matrix.

(2) $\mathrm{SL}(n, A; \mathfrak{q}) = \{\, T \in \mathrm{SL}(n, A) \mid T \equiv \mathbb{I}_{n\times n} \bmod \mathfrak{q} \,\}$.

(3) For $a \in A$, and $1 \leq i, j \leq n$ with $i \neq j$, we use $E_{i,j}(a)$ to denote the $n \times n$ *elementary matrix*, such that the only nonzero entry of $E_{i,j}(a) - \mathbb{I}_{n\times n}$ is the (i,j) entry, which is a. (We may use $E_{i,j}$ to denote $E_{i,j}(1)$.)

(4) $\mathrm{LU}(n, \mathfrak{q}) = \left\{ E_{i,j}(a) \;\middle|\; \begin{array}{c} a \in \mathfrak{q}, \\ 1 \leq i, j \leq n, \\ i \neq j \end{array} \right\}$. In other words, $\mathrm{LU}(n, A)$ is the set of all $n \times n$ elementary matrices, and $\mathrm{LU}(n, \mathfrak{q}) = \mathrm{LU}(n, A) \cap \mathrm{SL}(n, A; \mathfrak{q})$.

(5) $\mathrm{E}(n, \mathfrak{q}) = \langle \mathrm{LU}(n, \mathfrak{q}) \rangle$. Thus, $\mathrm{E}(n, A)$ is the subgroup of $\mathrm{SL}(n, A)$ generated by the elementary matrices.

(6) $\mathrm{LU}^{\triangleleft}(n, A; \mathfrak{q})$ is the set of $\mathrm{E}(n, A)$-conjugates of elements of $\mathrm{LU}(n, \mathfrak{q})$.

(7) $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q}) = \langle \mathrm{LU}^{\triangleleft}(n, A; \mathfrak{q}) \rangle$. Thus, $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$ is the smallest *normal* subgroup of $\mathrm{E}(n, A)$ that contains $\mathrm{LU}(n, \mathfrak{q})$.

(8) $W(\mathfrak{q}) = \left\{ (a,b) \in A \times A \;\middle|\; \begin{array}{c} (a,b) \equiv (1,0) \bmod \mathfrak{q} \\ \text{and} \\ aA + bA = A \end{array} \right\}$. Note that $(a,b) \in W(\mathfrak{q})$ if and only if there exist $c, d \in A$, such that $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(n, A; \mathfrak{q})$ [Ba2, Prop. 1.2(a), p. 283].

(9) $U(\mathfrak{q})$ is the group of units of $A/\mathfrak{q}$.

Note that $\mathrm{E}(n,A)$ is boundedly generated by elementary matrices if and only if $\mathrm{E}(n,A) = \langle \mathrm{LU}(n,A) \rangle_r$, for some positive integer r.

(2.5) **Remark.** The subgroup $\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q})$ is usually denoted $\mathrm{E}(n,A;\mathfrak{q})$ in the literature, but we include the superscript "$\triangleleft$" to emphasize that this subgroup is normalized by $\mathrm{E}(n,A)$, and thereby reduce the likelihood of confusion with $\mathrm{E}(n,\mathfrak{q})$.

(2.6) **Notation.** Suppose K is an algebraic number field. We use $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$ to denote the norm map from K to $\mathbb{Q}$.

§2B. The Compactness Theorem of first-order logic. The well-known Gödel Completeness Theorem states that if a theory in first-order logic is consistent (that is, if it does not lead to a contradiction of the form $\varphi \wedge \neg\varphi$), then the theory has a model. Because any proof must have finite length, it can quote only finitely many axioms of the theory. This reasoning leads to the following fundamental theorem, which can be found in introductory texts on first-order logic.

(2.7) **Theorem** (Compactness Theorem). *Suppose $\mathcal{T}$ is any set of first-order sentences (with no free variables) in some first-order language $\mathcal{L}$. If $\mathcal{T}$ does not have a model, then some finite subset $\mathcal{T}_0$ of $\mathcal{T}$ does not have a model.*

(2.8) **Corollary.** *Fix a positive integer n, and let $\mathcal{L}$ be a first-order language that contains:*

- *the language of rings $(+, \times, 0, 1)$,*
- *n^2 variables x_{ij} for $1 \le i, j \le n$,*
- *two n^2-ary relation symbols $X(x_{ij})$ and $H(x_{ij})$, and*
- *any number (perhaps infinite) of other variables, constant symbols, and relation symbols.*

Suppose $\mathcal{T}$ is a set of sentences in the language $\mathcal{L}$, such that, for every model

$$\big(A, (+, \times, 0, 1, X, H, \ldots)\big)$$

of the theory $\mathcal{T}$,

- *the universe A is a commutative ring (under the binary operations $+$ and $\times$), and*
- *letting*

$$X_A = \left\{ (a_{ij})_{i,j=1}^n \;\middle|\; \begin{array}{c} a_{ij} \in A, \\ X(a_{ij}) \end{array} \right\} \quad \text{and} \quad H_A = \left\{ (a_{ij})_{i,j=1}^n \;\middle|\; \begin{array}{c} a_{ij} \in A, \\ H(a_{ij}) \end{array} \right\},$$

  we have:
  - *H_A is a subgroup of $\mathrm{SL}(n,A)$, and*
  - *X_A generates a subgroup of finite index in H_A.*

Then, for every model $(A, \dots)$ of $\mathcal{T}$, the set X_A ***boundedly generates*** *a subgroup of finite index in H_A.*

More precisely, there is a positive integer $r = r(n, \mathcal{L}, \mathcal{T})$, such that, for every model $(A, \dots)$ of $\mathcal{T}$, $\langle X_A \rangle_r$ is a subgroup of H_A, and the index of this subgroup is $\leq r$.

Proof. This is a standard argument, so we provide only an informal sketch.

- Let $\mathcal{L}^+$ be obtained from $\mathcal{L}$ by adding constant symbols to represent infinitely many matrices $C_1, C_2, C_3, \dots$. (Each matrix requires n^2 constant symbols $c_{i,j}$.)
- Let $\mathcal{T}^+$ be obtained from $\mathcal{T}$ by adding first-order sentences specifying, for all $i, j, r \in \mathbb{N}^+$, with $i \neq j$, that
  - $C_i \in H_A$, and
  - $C_i^{-1} C_j \notin \langle X_A \rangle_{r-1}$.

Since X_A generates a subgroup of finite index in H_A, we know that $\mathcal{T}^+$ is not consistent. From the Compactness Theorem, we conclude, for some r, that it is impossible to find $C_1, C_2, \dots, C_r \in H_A$, such that $C_i^{-1} C_j \notin \langle X_A \rangle_{r-1}$ for $i \neq j$. This implies the index of $\langle X_A \rangle$ is less than r. Also, we must have $\langle X_A \rangle_{r^2} = \langle X_A \rangle$ (otherwise, we could choose $C_i \in \langle X_A \rangle_{ir} \smallsetminus \langle X_A \rangle_{ir-1}$). □

Proof of Proposition 1.5. This is a standard compactness argument, so we provide only a sketch. Let $\mathcal{T}'$ consist of:

- the axioms in $\mathcal{T}$,
- the axioms of commutative rings,
- a collection of sentences that guarantees $X_A = \mathrm{LU}(n, A)$, and
- a collection of sentences that guarantees $H_A = \mathrm{SL}(n, A)$.

Then the desired conclusion is immediate from Corollary 2.8. □

§2C. Stable range condition SR_m. We recall the stable range condition SR_m of Bass. (We use the indexing of [HOM], not that of [Ba2].) For convenience, we also introduce a condition $\mathsf{SR}_{1\frac{1}{2}}$ that is intermediate between SR_1 and SR_2. In our applications, the parameter m will always be either 1 or $1\frac{1}{2}$ or 2.

(2.9) **Definition** ([Ba2, Defn. 3.1, p. 231], [HOM, p. 142], cf. [Ba1, §4])**.** Fix a positive integer m. We say that a commutative ring A satisfies the *stable range* condition SR_m if, for all $a_0, a_1, \dots, a_r \in A$, such that:

- $r \geq \mathsf{m}$ and
- $a_0 A + a_1 A + \cdots + a_r A = A$,

there exist $a_1', a_2', \dots, a_r' \in A$, such that:

- $a_i' \equiv a_i \bmod a_0 A$, for $1 \leq i \leq r$, and
- $a_1' A + \cdots + a_r' A = A$.

The condition SR_m can obviously be represented by a list of infinitely many first-order statements, one for each integer $r \geq \mathsf{m}$. It is interesting (though not necessary) to note that the single case $r = \mathsf{m}$ implies all the others [HOM, (4.1.7), p. 143], so a single statement suffices.

(2.10) **Definition.** We say a commutative ring A satisfies $\mathsf{SR}_{1\frac{1}{2}}$ if $A/\mathfrak{q}$ satisfies SR_1, for every nonzero ideal $\mathfrak{q}$ of A.

It is easy to see that $\mathsf{SR}_1 \Rightarrow \mathsf{SR}_{1\frac{1}{2}} \Rightarrow \mathsf{SR}_2$.

(2.11) **Remark.** If A satisfies SR_{m} (for some m), and $\mathfrak{q}$ is any ideal of A, then $A/\mathfrak{q}$ also satisfies SR_{m} [Ba1, Lem. 4.1]. Hence, A satisfies $\mathsf{SR}_{1\frac{1}{2}}$ if and only if A/qA satisfies SR_1, for every nonzero $q \in A$. This implies that $\mathsf{SR}_{1\frac{1}{2}}$ can be expressed in terms of first-order sentences.

(2.12) **Notation.** As is usual in this paper,

- K is an algebraic number field,
- $\mathcal{O}$ is the ring of integers of K,
- B is an order in $\mathcal{O}$, and
- S is a multiplicative subset of B.

The following result is well-known.

(2.13) **Lemma.** *BS^{-1} satisfies $\mathsf{SR}_{1\frac{1}{2}}$.*

Proof. Let $\mathfrak{q}$ be any nonzero ideal of BS^{-1}. Since the quotient ring $BS^{-1}/\mathfrak{q}$ is finite, it is semilocal. So it is easy to see that it satisfies SR_1 [Ba2, Prop. 2.8]. □

The following fundamental result of Bass is the reason for our interest in SR_{m}.

(2.14) **Theorem** (Bass [Ba1, §4])**.** *Let:*

- *A be a commutative ring,*
- *m be a positive integer, such that A satisfies the stable range condition SR_{m},*
- *$n > \mathsf{m}$, and*
- *$\mathfrak{q}$ be an ideal of A.*

Then:

(1) $\mathrm{SL}(n, A; \mathfrak{q}) = \mathrm{SL}(\mathsf{m}, A; \mathfrak{q})\, \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$.
(2) $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$ *is a normal subgroup of* $\mathrm{SL}(n, A)$.
(3) *If $n \geq 3$, then* $\big[\mathrm{E}(n, A), \mathrm{SL}(n, A; \mathfrak{q})\big] = \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$.

Applying the case $\mathsf{m} = 1$ of 2.14(1) to the quotient ring $A/\mathfrak{q}'$ yields the following conclusion:

(2.15) **Corollary.** *Let:*

- *A be a commutative ring,*
- *n be a positive integer, and*
- *$\mathfrak{q}$ and $\mathfrak{q}'$ be nonzero ideals of A, such that $\mathfrak{q}' \subseteq \mathfrak{q}$.*

If $A/\mathfrak{q}'$ satisfies SR_1, then $\mathrm{SL}(n, A; \mathfrak{q}) = \mathrm{SL}(n, A; \mathfrak{q}')\, \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$.

§2D. Mennicke symbols. We recall the definition and basic properties of Mennicke symbols, including their important role in the study of the quotient group $\mathrm{SL}(n, A; \mathfrak{q}) / \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$.

(2.16) **Definition** [BMS, Defn. 2.5]**.** Suppose A is a commutative ring and $\mathfrak{q}$ is an ideal in A. Recall that $W(\mathfrak{q})$ was defined in 2.4(8).

(1) A *Mennicke symbol* is a function $(a,b) \mapsto \begin{bmatrix} b \\ a \end{bmatrix}$ from $W(\mathfrak{q})$ to a group C, such that:

(MS1a) $\begin{bmatrix} b+ta \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$ whenever $(a,b) \in W(\mathfrak{q})$ and $t \in \mathfrak{q}$;

(MS1b) $\begin{bmatrix} b \\ a+tb \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$ whenever $(a,b) \in W(\mathfrak{q})$ and $t \in A$; and

(MS2a) $\begin{bmatrix} b_1 \\ a \end{bmatrix} \begin{bmatrix} b_2 \\ a \end{bmatrix} = \begin{bmatrix} b_1 b_2 \\ a \end{bmatrix}$ whenever $(a,b_1),(a,b_2) \in W(\mathfrak{q})$.

(2) It is easy to see that, for some group $C(\mathfrak{q})$ (called the *universal Mennicke group*), there is a *universal* Mennicke symbol

$$\left[\!\left[\quad \right]\!\right]_{\mathfrak{q}} : W(\mathfrak{q}) \to C(\mathfrak{q}),$$

such that any Mennicke symbol $\begin{bmatrix} \ \\ \ \end{bmatrix} : W(\mathfrak{q}) \to C$, for any group C, can be obtained by composing $\left[\!\left[\quad \right]\!\right]_{\mathfrak{q}}$ with a unique homomorphism from $C(\mathfrak{q})$ to C. The universal Mennicke symbol and the universal Mennicke group are unique up to isomorphism.

The following classical theorem introduces Mennicke symbols into the study of $\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q})$.

(2.17) **Notation.** For convenience, when $T \in \mathrm{SL}(2,A;\mathfrak{q})$, we use $\overline{T}$ to denote the image of T under the usual embedding of $\mathrm{SL}(2,A;\mathfrak{q})$ in the top left corner of $\mathrm{SL}(n,A;\mathfrak{q})$.

(2.18) **Theorem** [BMS, Thm. 5.4 and Lem. 5.5], [Ba2, Prop. 1.2(b), p. 283 and Thm. 2.1(b), p. 293]**.** *Let:*

- *A be a commutative ring,*
- *$\mathfrak{q}$ be an ideal of A,*
- *N be a normal subgroup of* $\mathrm{SL}(n,A;\mathfrak{q})$*, for some $n \geq 2$, and*
- *$C = \mathrm{SL}(n,A;\mathfrak{q})/N$,*

such that N contains both $\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q})$ *and* $\big[\mathrm{E}(n,A), \mathrm{SL}(n,A;\mathfrak{q})\big]$. *Then:*

(1) *The map* $\begin{bmatrix} b \\ a \end{bmatrix}_{\mathfrak{q}} : W(\mathfrak{q}) \to C$*, defined by*

$$(a,b) \mapsto \begin{bmatrix} b \\ a \end{bmatrix}_{\mathfrak{q}} = \overline{\begin{bmatrix} a & b \\ * & * \end{bmatrix}} N,$$

is well-defined.

(2) $\begin{bmatrix} \ \\ \ \end{bmatrix}_{\mathfrak{q}}$ *satisfies* (MS1a) *and* (MS1b).

(3) (Mennicke) *If $n \geq 3$, then* $\begin{bmatrix} \ \\ \ \end{bmatrix}_{\mathfrak{q}}$ *also satisfies* (MS2a)*, so it is a Mennicke symbol.*

Under the assumption that A is a Dedekind ring, Bass, Milnor, and Serre [BMS, §2] proved several basic properties of Mennicke symbols; these results appear in [Ba2] with the slightly weaker hypothesis that A is a Noetherian ring of dimension ≤ 1. For our applications, it is important to observe that the arguments of [Ba2] require only the assumption that $A/\mathfrak{q}$ satisfies the stable range condition SR_1, for every nonzero ideal $\mathfrak{q}$ of A.

(2.19) **Lemma** (cf. [BMS, §2], [Ba2, §6.1])**.** *Suppose:*

- *A is an integral domain that satisfies $\mathsf{SR}_{1\frac{1}{2}}$,*
- *$\mathfrak{q}$ is an ideal in A, and*
- *$\begin{bmatrix} \ \end{bmatrix} : W(\mathfrak{q}) \to C$ is a Mennicke symbol.*

Then:

(1) $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1$ *(the identity element of C).*

(2) *If $(a,b) \in W(\mathfrak{q})$, then $\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b(1-a) \\ a \end{bmatrix}$.*

(3) *If $(a,b) \in W(\mathfrak{q})$, and there is a unit $u \in A$, such that either $a \equiv u \bmod bA$ or $b \equiv u \bmod aA$, then $\begin{bmatrix} b \\ a \end{bmatrix} = 1$.*

(4) *If $(a,b) \in W(\mathfrak{q})$, and $\mathfrak{q}'$ is any nonzero ideal contained in $\mathfrak{q}$, then there exists $(a',b') \in W(\mathfrak{q}')$, such that $\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b' \\ a' \end{bmatrix}$.*

(5) *The image of the Mennicke symbol $\begin{bmatrix} \ \end{bmatrix}$ is an abelian subgroup of C.*

(6) (Lam) *If $\mathfrak{q}$ is principal, then*

$$\text{(MS2b)} \qquad \begin{bmatrix} b \\ a_1 \end{bmatrix} \begin{bmatrix} b \\ a_2 \end{bmatrix} = \begin{bmatrix} b \\ a_1 a_2 \end{bmatrix} \text{ whenever } (a_1,b),(a_2,b) \in W(\mathfrak{q}).$$

The following result provides a converse to Lemma 2.19(6). It will be used in the proof of Lemma 5.10.

(2.20) **Lemma.** *Suppose:*

- *A is a commutative ring,*
- *$\mathfrak{q}$ is an ideal in A,*
- *C is a group, and*
- *$\begin{bmatrix} \ \end{bmatrix} : W(\mathfrak{q}) \to C$ satisfies* (MS1a) *and* (MS1b).

Then:

(1) (Lam [Ba2, Prop. 1.7(a), p. 289]) *If $\begin{bmatrix} \ \end{bmatrix}$ satisfies* (MS2b), *then it also satisfies* (MS2a), *so it is a Mennicke symbol.*

(2) *If $\begin{bmatrix} \ \end{bmatrix}$ satisfies* (MS2b) *whenever $\begin{bmatrix} b \\ a_2 \end{bmatrix} = 1$, then it satisfies* (MS2a) *whenever $\begin{bmatrix} b_2 \\ a \end{bmatrix} = 1$.*

Proof. (1) Given $\begin{bmatrix} b_1 \\ a \end{bmatrix}, \begin{bmatrix} b_2 \\ a \end{bmatrix} \in W(\mathfrak{q})$, let $q = 1 - a \in \mathfrak{q}$. Note that, for any $b \in \mathfrak{q}$, we have

$$\text{(2.21)} \qquad \begin{bmatrix} bq^n \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} \text{ for every positive integer } n$$

(because the proof of 2.19(2) does not appeal to (MS2a)). Also, because

$$\begin{bmatrix} bq^2 \\ 1+bq \end{bmatrix} = \begin{bmatrix} bq^2 - q(1+bq) \\ 1+bq \end{bmatrix} = \begin{bmatrix} -q \\ 1+bq \end{bmatrix} = \begin{bmatrix} -q \\ 1 \end{bmatrix} = 1,$$

we have

$$\text{(2.22)}\qquad \begin{bmatrix} bq^2 \\ a \end{bmatrix} = \begin{bmatrix} bq^2 \\ a \end{bmatrix}\begin{bmatrix} bq^2 \\ 1+bq \end{bmatrix} = \begin{bmatrix} bq^2 \\ a(1+bq) \end{bmatrix} = \begin{bmatrix} bq^2 \\ a+abq \end{bmatrix}$$
$$= \begin{bmatrix} bq^2 \\ a+abq-bq^2 \end{bmatrix} = \begin{bmatrix} bq^2 \\ a+bq(a-q) \end{bmatrix}$$
$$= \begin{bmatrix} bq^2 \\ a+bq(1) \end{bmatrix} = \begin{bmatrix} bq^2-q(a+bq) \\ a+bq \end{bmatrix} = \begin{bmatrix} -aq \\ a+bq \end{bmatrix}.$$

Applying, in order, (2.21) to both factors, (2.22) to both factors, (MS2b), (MS1b), definition of q, (MS1b), (2.22), and (2.21), yields

$$\begin{bmatrix} b_1 \\ a \end{bmatrix}\begin{bmatrix} b_2 \\ a \end{bmatrix} = \begin{bmatrix} b_1q^2 \\ a \end{bmatrix}\begin{bmatrix} b_2q^2 \\ a \end{bmatrix} = \begin{bmatrix} -aq \\ a+b_1q \end{bmatrix}\begin{bmatrix} -aq \\ a+b_2q \end{bmatrix}$$
$$= \begin{bmatrix} -aq \\ (a+b_1q)(a+b_2q) \end{bmatrix} = \begin{bmatrix} -aq \\ a^2+b_1b_2q^2 \end{bmatrix}$$
$$= \begin{bmatrix} -aq \\ a(1-q)+b_1b_2q^2 \end{bmatrix} = \begin{bmatrix} -aq \\ a+b_1b_2q^2 \end{bmatrix}$$
$$= \begin{bmatrix} b_1b_2q^3 \\ a \end{bmatrix} = \begin{bmatrix} b_1b_2 \\ a \end{bmatrix}.$$

(2) The condition (MS2b) was applied only twice in the proof of (1).

- In the first application, the second factor is $\begin{bmatrix} bq^2 \\ 1+bq \end{bmatrix} = 1$.
- In the other application, the second factor is $\begin{bmatrix} -aq \\ a+b_2q \end{bmatrix} = \begin{bmatrix} b_2 \\ a \end{bmatrix}$, which is assumed to be 1.

Therefore, exactly the same calculations apply. □

The following useful result is stated with a slightly weaker hypothesis in [Ba2]:

(2.23) **Proposition** [Ba2, Thm. VI.2.1a, p. 293]**.** *If* $\begin{bmatrix} \ \end{bmatrix}$ *satisfies* (MS2a) *whenever* $\begin{bmatrix} b_2 \\ a \end{bmatrix} = 1$*, then it is a Mennicke symbol.*

Combining this with Lemma 2.20(2) yields the following conclusion:

(2.24) **Corollary.** *If* $\begin{bmatrix} \ \end{bmatrix}$ *satisfies* (MS2b) *whenever* $\begin{bmatrix} b \\ a_2 \end{bmatrix} = 1$*, then it is a Mennicke symbol.*

We conclude this discussion with two additional properties of Mennicke symbols.

(2.25) **Lemma.** *Let A, $\mathfrak{q}$, and* $\begin{bmatrix} \ \end{bmatrix}$ *be as in Lemma* 2.19*.*

(1) *If* $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, A; \mathfrak{q})$*, then* $\begin{bmatrix} b \\ a \end{bmatrix}^{-1} = \begin{bmatrix} c \\ a \end{bmatrix}$.

(2) *Suppose $\mathfrak{q} = qA$ is principal, and a, b, c, d, f, and g are elements of A, such that*
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \textit{ and } f\mathbb{I}_{2\times 2} + g\begin{bmatrix} a & b \\ c & d \end{bmatrix} \textit{ are in } \mathrm{SL}(2, A; qA).$$

Then

$$\begin{bmatrix} bg \\ f+ga \end{bmatrix}^2 = \begin{bmatrix} b \\ f+ga \end{bmatrix}^2.$$

Proof. (1) We have

$$\begin{aligned} \begin{bmatrix} b \\ a \end{bmatrix} \begin{bmatrix} c \\ a \end{bmatrix} &= \begin{bmatrix} bc \\ a \end{bmatrix} = \begin{bmatrix} bc(1-a) \\ a \end{bmatrix} \\ &= \begin{bmatrix} (bc-ad)(1-a) \\ a \end{bmatrix} = \begin{bmatrix} -(1-a) \\ a \end{bmatrix} = \begin{bmatrix} a-1 \\ 1 \end{bmatrix} = 1. \end{aligned}$$

(2) Note that, by assumption, a, d, and $f+ga$ are all congruent to 1 modulo qA. Also, working modulo gqA, we have

$$\begin{aligned} (f+ga)^2 &\equiv (f+g)^2 && \text{(since } a \equiv 1 \bmod qA\text{)} \\ &\equiv f^2 + (a+d)fg + g^2 && \text{(since } a+d \equiv 1+1 = 2 \bmod qA\text{)} \\ &= \det\left(f\mathbb{I}_{2\times 2} + g \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) \\ &= 1. \end{aligned}$$

Therefore

$$\begin{aligned} \begin{bmatrix} bg \\ f+ga \end{bmatrix}^2 &= \begin{bmatrix} bg \\ (f+ga)^2 \end{bmatrix} && \text{(by MS2b, see 2.19(6))} \\ &= \begin{bmatrix} bg \\ (f+ga)^2 \end{bmatrix} \begin{bmatrix} q \\ (f+ga)^2 \end{bmatrix} && \text{(since } (f+ga)^2 \equiv 1 \bmod qA\text{)} \\ &= \begin{bmatrix} b \\ (f+ga)^2 \end{bmatrix} \begin{bmatrix} gq \\ (f+ga)^2 \end{bmatrix} && \text{(by MS2a)} \\ &= \begin{bmatrix} b \\ f+ga \end{bmatrix}^2 && \text{(by MS2b and because } (f+ga)^2 \equiv 1 \bmod gqA\text{).} \end{aligned}$$

□

§2E. Nonstandard analysis.

(2.26) **Remark.** Many of the results and proofs in §5 use the theory of nonstandard analysis, in the language and notation of [SL]. This enables us to express some of the arguments in a form that is less complicated and more intuitive. In particular, it is usually possible to eliminate phrases of the form "for every ideal $\mathfrak{q}$, there exists an ideal $\mathfrak{q}'$," because the nonstandard ideal $\mathcal{Q}$ (see Definition 5.2) can be used as $\mathfrak{q}'$ for any choice of the ideal $\mathfrak{q}$ of A. (Thus, $\mathcal{Q}$ plays a role analogous to the set of infinitesimal numbers in the nonstandard approach to Calculus.)

As an aid to those who prefer classical proofs, Remark 5.1 provides classical reformulations of the nonstandard results. It is not difficult to prove these versions, by using the nonstandard proofs as detailed hints. Doing so yields a proof of Theorem 5.26 without reference to nonstandard analysis.

The unpublished manuscript [CKP] uses nonstandard models much more extensively than we do here, in place of the Compactness Theorem (2.7), for example (cf. 2.29). We have employed them only where they have the most effect.

(2.27) **Notation** (cf. [SL])**.**
- For a given ring A, we use ${}^*\!A$ to denote a (polysaturated) nonstandard model of A.
- If X is an entity (such as an ideal, or other subset) that is associated to A, we use ${}^*X$ to denote the corresponding standard entity of ${}^*\!A$.
- For an element a of A, we usually use a (instead of ${}^*a$) to denote the corresponding element of ${}^*\!A$.

Recall that the $*$-transform of a first-order sentence is obtained by replacing each constant symbol X with ${}^*X$ [SL, Defn. 3.4.2, p. 27]. For example, the $*$-transform of $\forall a \in A, \exists b \in B, (a = b^2)$ is $\forall a \in {}^*\!A, \exists b \in {}^*B, (a = b^2)$.

(2.28) **Leibniz' Principle** [SL, (3.4.3), p. 28]**.** *A first-order sentence with all quantifiers bounded is true in A if and only if its $*$-transform is true in ${}^*\!A$.*

The following result of nonstandard analysis could be used in place of the Compactness Theorem (2.7) in our arguments.

(2.29) **Lemma** [CKP, (2.1)]**.** *Suppose G is a group and $\mathcal{X}$ is a subset of G. The following are equivalent:*

(1) *$\mathcal{X}$ boundedly generates $\langle \mathcal{X} \rangle$.*
(2) *$\langle {}^*\mathcal{X} \rangle = {}^*\langle \mathcal{X} \rangle$.*
(3) *$\langle {}^*\mathcal{X} \rangle$ is of finite index in ${}^*\langle \mathcal{X} \rangle$.*
(4) *There exists a $*$-finite subset Ω of ${}^*G$ with ${}^*\langle \mathcal{X} \rangle \subseteq \langle {}^*\mathcal{X} \rangle \, \Omega$.*

Proof. (1) $\Rightarrow$ (2) If $\mathcal{X}$ boundedly generates $\langle \mathcal{X} \rangle$, then there exists a positive integer r, such that $\langle \mathcal{X} \rangle = \langle \mathcal{X} \rangle_r$. Then

$$ {}^*\langle \mathcal{X} \rangle = {}^*\langle \mathcal{X} \rangle_r = \langle {}^*\mathcal{X} \rangle_r \subseteq \langle {}^*\mathcal{X} \rangle \, . $$

(2) $\Rightarrow$ (3) $\Rightarrow$ (4) Obvious.

(4) $\Rightarrow$ (1) Let $\Omega' = \Omega \cap {}^*\langle \mathcal{X} \rangle$. Since Ω' is $*$-finite, there exists $\omega \in {}^*\mathbb{N}$, such that $\Omega' \subseteq {}^*\langle \mathcal{X} \rangle_\omega$. For any infinite $\tau \in {}^*\mathbb{N}$, we have $\langle {}^*\mathcal{X} \rangle \subseteq {}^*\langle \mathcal{X} \rangle_\tau$. Therefore, letting $r = \omega + \tau$, we have "There exists $r \in {}^*\mathbb{N}$, such that ${}^*\langle \mathcal{X} \rangle = {}^*\langle \mathcal{X} \rangle_r$". By Leibniz' Principle, "There exists $r \in \mathbb{N}$, such that $\langle \mathcal{X} \rangle = \langle \mathcal{X} \rangle_r$." □

§2F. Two results from number theory. Our proofs rely on two nontrivial theorems of number theory. The first of these is a version of Dirichlet's Theorem on primes in arithmetic progressions. It is a basic ingredient in our arguments (cf. few generators property (3.2)). The second theorem is used only to establish the claim in the proof of Lemma 4.6.

(2.30) **Theorem** [BMS, (A.11), p. 84]**.** *Let:*
- *$\mathcal{O}$ be the ring of integers of an algebraic number field K, and*
- *$\mathrm{N}\colon K \to \mathbb{Q}$ be the norm map.*

For all nonzero $a, b \in \mathcal{O}$, such that $a\mathcal{O} + b\mathcal{O} = \mathcal{O}$, there exist infinitely many $h \in a + b\mathcal{O}$, such that:

(1) *$h\mathcal{O}$ is a maximal ideal of $\mathcal{O}$, and*
(2) *$\mathrm{N}(h)$ is positive.*

(2.31) **Remark.** The fact that $\mathrm{N}(h)$ can be assumed to be positive is not essential to any of the arguments in this paper. However, it simplifies the proof of

Lemma 3.8(2), by eliminating the need to consider absolute values. (Also, if $\mathrm{N}(h)$ were not assumed to be positive, then a factor of 2 would be lost, so $(16k)!$ would replace $(8k)!$ in the conclusion, but that would have no impact on the main results.)

(2.32) **Theorem** [Os, p. 57]. *Let r and m be any positive integers, such that $\gcd(r,m) = 1$. Then there exists $M \in \mathbb{Z}$, such that if t is an integer greater than M, and $t \equiv 3r \bmod m$, then $t = p_1 + p_2 + p_3$, where each p_i is a rational prime that is congruent to r modulo m.*

We do not need the full strength of Theorem 2.32, but only the following consequence:

(2.33) **Corollary.** *Let r and m be any positive integers, with $\gcd(r,m) = 1$. If $t \in m\mathbb{Z}$, then t can be written in the form*

$$t = p_1 + p_2 + p_3 - p_4 - p_5 - p_6,$$

where each p_i is a rational prime that is congruent to r modulo m.

In fact, the arguments could be carried through with a weaker result that uses more than 6 primes: if we assume only that every $t \in m\mathbb{Z}$ can be written in the form

$$t = p_1 + p_2 + \cdots + p_c - p_{c+1} - p_{c+2} - \cdots - p_{2c},$$

then the only difference would be that the constant $7k$ in the conclusion of Lemma 4.6 would be replaced with $(2c+1)k$. This would have no effect at all on the main results.

3. First-order properties and bounded generation when $n \geq 3$

In §3A and §3B, we define certain first-order properties that any particular ring may or may not have. They are denoted $\mathsf{Gen}(\mathsf{t},\mathsf{r})$, and $\mathsf{Exp}(\mathsf{t},\ell)$, for positive integers t, r, and ℓ. (In order to apply the Compactness Theorem (2.7), it is crucial that, for fixed values of the parameters t, r, and ℓ, these properties can be expressed by first-order sentences.) We also show that the number rings BS^{-1} of interest to us satisfy these properties for appropriate choices of the parameters (see 3.5 and 3.9). In §3C, we show that these properties (together with the stable range condition $\mathsf{SR}_{1\frac{1}{2}}$) imply that the order of the universal Mennicke group is bounded (see 3.11). Finally, in §3D, we establish that if $n \geq 3$, then the elementary matrices boundedly generate a finite-index subgroup of $\mathrm{SL}(n, BS^{-1})$ (see 3.13(1)).

(3.1) **Notation.** Throughout this section,

- K is an algebraic number field,
- k is the degree of K over $\mathbb{Q}$,
- $\mathcal{O}$ is the ring of integers of K,
- B is an order in $\mathcal{O}$,
- S is a subset of $B \setminus \{0\}$ that is closed under multiplication, and
- $\mathrm{N}\colon K \to \mathbb{Q}$ is the norm map.

§3A. Few generators property $\mathsf{Gen}(\mathsf{t},\mathsf{r})$. We write down a simple first-order consequence of Dirichlet's Theorem (2.30) on primes in arithmetic progressions. It will be used to bound the number of generators of the universal Mennicke group (see Step 2 of the proof of Theorem 3.11). In addition, the special case $\mathsf{Gen}(2,1)$ also plays a key role in the proof of Proposition 5.7.

(3.2) **Definition** [CKP, (1.2)]**.** For fixed positive integers t and r, a commutative ring A is said to satisfy $\mathsf{Gen}(\mathsf{t},\mathsf{r})$ if and only if: for all $a, b \in A$, such that $aA + bA = A$, there exists $h \in a + bA$, such that

$$\frac{U(hA)}{U(hA)^{\mathsf{t}}} \text{ can be generated by } \mathsf{r} \text{ or less elements.}$$

(Recall that $U(hA)$ denotes the group of units in A/hA.)

(3.3) **Lemma.** *If $b \in B$ and $s \in S$, with $b \neq 0$, then:*

1. *$B \subseteq bBS^{-1} + sB$.*
2. *$B + bBS^{-1} = BS^{-1}$.*
3. *The natural homomorphism from B to BS^{-1}/bBS^{-1} is surjective.*

Proof. (1) Because B/bB is finite, and $\{s^n B\}$ is a decreasing sequence of ideals, there exists $n \in \mathbb{Z}^+$, such that $bB + s^n B = bB + s^{n+1}B$. Hence $s^n \in bB + s^{n+1}B$, so

$$1 \in s^{-n}(bB + s^{n+1}B) = s^{-n}bB + sB \subseteq bBS^{-1} + sB.$$

(2) For any $s_0 \in S$, we know, from (1), that $1 \in bBS^{-1} + s_0B$. Therefore $1/s_0 \in bBS^{-1} + B$.

(3) This is immediate from (2). □

(3.4) **Proposition** [CKP, (4.1)]**.** *Let:*

- *$a \in BS^{-1}$ and $b \in B$, such that $b \neq 0$ and $aBS^{-1} + bBS^{-1} = BS^{-1}$, and*
- *γ be any nonzero element of $\mathcal{O}$, such that $\gamma\mathcal{O} \subset B$.*

Then:

1. *There exists $a_0 \equiv a \bmod bBS^{-1}$, such that $a_0B + b\gamma^2B = B$.*
2. *For any a' in $\mathcal{O}$ with $a' \equiv a_0 \bmod b\gamma^2\mathcal{O}$,*
   (a) *the natural homomorphism $BS^{-1} \to \mathcal{O}S^{-1}/a'\mathcal{O}S^{-1}$ is surjective, and has kernel $a'BS^{-1}$,*
   (b) *$BS^{-1}/a'BS^{-1}$ is isomorphic to a quotient of $\mathcal{O}/a'\mathcal{O}$, and*
   (c) *$a' \in B$.*

Proof. (1) From 3.3(3), the natural homomorphism $B \to BS^{-1}/bBS^{-1}$ is surjective, so we may choose $a_1 \in B$ with $a_1 \equiv a \bmod bBS^{-1}$. Since a is a unit in BS^{-1}/bBS^{-1}, then a_1 is a unit in $B/(B \cap bBS^{-1})$; thus, there exist $x \in B$ and $y \in B \cap bBS^{-1}$, such that $a_1x + y = 1$. Since $B/b\gamma^2B$ is semilocal (indeed, it is finite), there exists $a_0 \in a_1 + yB$, such that a_0 is a unit in $B/b\gamma^2B$. Then $a_0 \equiv a_1 \equiv a \bmod bBS^{-1}$ and $a_0B + b\gamma^2B = B$.

(2c) We have $a' \in a_0 + b\gamma^2\mathcal{O} \subseteq B + b\gamma B = B$.

(2a) Let $\varphi\colon BS^{-1} \to \mathcal{O}S^{-1}/a'\mathcal{O}S^{-1}$ be the natural homomorphism. Because $b\gamma^2\mathcal{O} \subseteq b\gamma B$, we have

$$a'B + \gamma B \supseteq a'B + b\gamma B = a_0B + b\gamma B \supseteq a_0B + b\gamma^2B = B.$$

Therefore
$$a'BS^{-1} + \gamma BS^{-1} = BS^{-1}.$$
Hence $a'\mathcal{O}S^{-1} + \gamma\mathcal{O}S^{-1} = \mathcal{O}S^{-1}$ (which implies $a'\mathcal{O}S^{-1} + BS^{-1} = \mathcal{O}S^{-1}$ — that is, φ is surjective). In other words, a' is relatively prime to γ, so
$$a'\mathcal{O}S^{-1} \cap \gamma\mathcal{O}S^{-1} = a'\gamma\mathcal{O}S^{-1} \subseteq a'BS^{-1}.$$
The kernel of φ is
$$\begin{aligned} a'\mathcal{O}S^{-1} \cap BS^{-1} &= a'\mathcal{O}S^{-1} \cap (a'BS^{-1} + \gamma BS^{-1}) \\ &= a'BS^{-1} + (a'\mathcal{O}S^{-1} \cap \gamma BS^{-1}) \\ &\subseteq a'BS^{-1} + (a'\mathcal{O}S^{-1} \cap \gamma\mathcal{O}S^{-1}) \\ &= a'BS^{-1}. \end{aligned}$$

(2b) From (2a), we see that $BS^{-1}/a'BS^{-1} \cong \mathcal{O}S^{-1}/a'\mathcal{O}S^{-1}$. On the other hand, the natural homomorphism $\mathcal{O} \to \mathcal{O}S^{-1}/a'\mathcal{O}S^{-1}$ is surjective (see 3.3(3)) and has $a'\mathcal{O}$ in its kernel, so $\mathcal{O}S^{-1}/a'\mathcal{O}S^{-1}$ is isomorphic to a quotient of $\mathcal{O}/a'\mathcal{O}$. The desired conclusion follows. □

(3.5) **Corollary** (cf. [CKP, (4.4)]). *BS^{-1} satisfies $\mathsf{Gen}(\mathsf{t}, 1)$, for every positive integer t.*

Proof. Proposition 3.4(1) yields $a_0 \equiv a \bmod bBS^{-1}$, such that $a_0B + b\gamma^2B = B$. Then $a_0\mathcal{O} + b\gamma^2\mathcal{O} = \mathcal{O}$, so Dirichlet's Theorem (2.30) yields $h \in a_0 + b\gamma^2\mathcal{O}$, such that $h\mathcal{O}$ is a maximal ideal. Therefore $\mathcal{O}/h\mathcal{O}$ is a finite field.

From 3.4(2b), we know that BS^{-1}/hBS^{-1} is isomorphic to a quotient of $\mathcal{O}/h\mathcal{O}$; thus, BS^{-1}/hBS^{-1} is either trivial or a finite field. In either case, the group of units is cyclic, so the quotient $U\big(hBS^{-1}\big)/U\big(hBS^{-1}\big)^{\mathsf{t}}$ is also cyclic. □

§3B. Exponent property $\mathsf{Exp}(\mathsf{t}, \ell)$. We now introduce a rather technical property that is used to bound the exponent of the universal Mennicke group (see Step 1 of the proof of Theorem 3.11). Theorem 3.9 shows that this property holds in number rings BS^{-1}.

(3.6) **Definition** [CKP, (1.3)]. Let t be a nonnegative integer and let ℓ be a positive integer. A commutative ring A is said to satisfy $\mathsf{Exp}(\mathsf{t}, \ell)$ if and only if for every q in A with $q \neq 0$ and every $(a, b) \in W(qA)$, there exists $a', c, d \in A$ and $u_i, f_i, g_i, b_i', d_i' \in A$ for $1 \le i \le \ell$, such that:

(1) $a' \equiv a \bmod bA$.

(2) $\begin{bmatrix} a' & b \\ c & d \end{bmatrix}$ is in $\mathrm{SL}(2, A; qA)$.

(3) $\begin{bmatrix} a' & b_i' \\ c & d_i' \end{bmatrix}$ is in $\mathrm{SL}(2, A; qA)$ for $1 \le i \le \ell$.

(4) $f_iI + g_i \begin{bmatrix} a' & b_i' \\ c & d_i' \end{bmatrix}$ is in $\mathrm{SL}(2, A; qA)$ for $1 \le i \le \ell$.

(5) $(f_1 + g_1a')^2(f_2 + g_2a')^2 \cdots (f_\ell + g_\ell a')^2 \equiv (a')^{\mathsf{t}} \bmod cA$.

(6) u_i is a unit in A and $f_i + g_ia' \equiv u_i \bmod b_i'A$ for $1 \le i \le \ell$.

(3.7) **Remark.** Assume t is even, and let A be an arbitrary commutative ring.

(1) It is easy to satisfy all of the conditions of Definition 3.6 *except* the requirement that u_1 is a unit: simply choose $f_1, g_1 \in A$, such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{\mathsf{t}/2} = f_1 \mathbb{I}_{2\times 2} + g_1 \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

and let $f_i = 1$ and $g_i = 0$ for $i > 1$.

(2) If $a = 0$, then it is easy to satisfy all the conditions of Definition 3.6: choose f_i, g_i as in (1), and, because $b_i = b$ is a unit, we may let $u_i = 1$ for all i.

(3) If $b = 0$, then it is easy to satisfy all the conditions of Definition 3.6. This is because a must be a unit in this case, so we may let $u_1 = a^{\mathsf{t}/2}$ (and $u_i = 1$ for $i > 1$).

Recall that k is the degree of K over $\mathbb{Q}$ (see 3.1).

(3.8) **Lemma** [CKP, (4.3)]**.**

(1) *For any rational prime p and positive integer r, let N_{p^r} be the homomorphism from $U(p^r\mathcal{O})$ to $U(p^r\mathbb{Z})$ induced by the norm map $\mathrm{N}\colon K \to \mathbb{Q}$. If $p^r > 8k$, then the image of N_{p^r} has more than 2 elements.*

(2) *If $f, g \in BS^{-1}$ with $fBS^{-1} + gBS^{-1} = BS^{-1}$, then, for any positive integer n and any nonzero $h \in BS^{-1}$, there exists $f' \equiv f \bmod gBS^{-1}$, such that:*

(a) $\gcd\bigl(\mathrm{e}(f'BS^{-1}), n\bigr)$ *is a divisor of* $(8k)!$, *where* $\mathrm{e}(f'BS^{-1})$ *is the exponent of* $U\bigl(f'BS^{-1}\bigr)$.

(b) $f'BS^{-1} + hBS^{-1} = BS^{-1}$.

Proof. (1) It is well-known that $U(p^r\mathbb{Z})$ has a cyclic subgroup of order $(p-1)p^{r-1}$ if p is odd, or of order p^{r-2} if $p = 2$. Thus, in any case, $U(p^r\mathbb{Z})$ has a cyclic subgroup C of order $\geq p^r/4 > 2k$. For $c \in \mathbb{Z}$ and, in particular, for $c \in C$, we have $\mathrm{N}(c) = c^k$. Therefore

$$\#\,\mathrm{N}_{p^r}\bigl(U(p^r\mathcal{O})\bigr) \geq \#\,\mathrm{N}_{p^r}(C) \geq \frac{\#C}{\gcd\bigl(k, \#C\bigr)} > \frac{2k}{k} = 2.$$

(2) We may assume $h = n$, by replacing n with $n\,|\,\mathrm{N}(hs)|$, for some $s \in S$ with $hs \in B$. We consider two cases.

Case 1. *Assume $BS^{-1} = \mathcal{O}$.* Choose $f_0 \equiv f \bmod g\mathcal{O}$, such that $f_0\mathcal{O} + (8k)!\,ng\mathcal{O} = \mathcal{O}$.

Let P be the set of rational prime divisors of n. We may assume (by replacing n with the product $\mathrm{N}(g)\,n$) that P contains every prime divisor of $\mathrm{N}(g)$. For each p in P, let

$$r(p) \text{ be the largest integer such that } p^{r(p)} \text{ divides } (8k)!.$$

From (1), we know that the image of $\mathrm{N}_{p^{r(p)+1}}$ has more than 2 elements. Therefore, $\mathrm{N}_{p^{r(p)+1}}(f_0)$ (or any other element of the image) can be written as a product of two elements of the image, neither of which is trivial. This implies that there exist $x(p), y(p) \in \mathcal{O}$, such that:

- $x(p)\,y(p) \equiv f_0 \bmod p^{r(p)+1}\mathcal{O}$ and
- neither $\mathrm{N}\bigl(x(p)\bigr)$ nor $\mathrm{N}\bigl(y(p)\bigr)$ is is congruent to 1 modulo $p^{r(p)+1}$.

Now, by Dirichlet's Theorem (2.30) and the Chinese Remainder Theorem, pick

- $f_1 \in \mathcal{O}$, such that
  - $f_1 \equiv x(p) \bmod p^{r(p)+1}\mathcal{O}$, for each p in P,
  - $f_1\mathcal{O}$ is maximal,
  - $n \notin f_1\mathcal{O}$, and
  - $\mathrm{N}(f_1) > 0$; and
- $f_2 \in \mathcal{O}$, such that
  - $f_1 f_2 \equiv f_0 \bmod \left(\prod_{p \in P} p^{r(p)+1}\right) g\,\mathcal{O}$,
  - $f_2\mathcal{O}$ is maximal,
  - $f_1\mathcal{O} + f_2\mathcal{O} = \mathcal{O}$, and
  - $\mathrm{N}(f_2) > 0$.

Set $f' = f_1 f_2$, so $f' \equiv f_0 \equiv f \bmod g\mathcal{O}$.

The Chinese Remainder Theorem implies that $U(f_1 f_2\mathcal{O}) \cong U(f_1\mathcal{O}) \times U(f_1\mathcal{O})$. Also, since $f_j\mathcal{O}$ is maximal, for $j = 1, 2$, we know that $U(f_j\mathcal{O})$ is cyclic of order

$$\#U(f_j\mathcal{O}) = \#(\mathcal{O}/f_j\mathcal{O}) - 1 = \#\,\mathrm{N}(f_j) - 1 = \mathrm{N}(f_j) - 1.$$

Therefore

$$\mathrm{e}(f'\mathcal{O}) = \mathrm{e}(f_1 f_2\mathcal{O}) = \mathrm{lcm}\big(\mathrm{e}(f_1\mathcal{O}), \mathrm{e}(f_1\mathcal{O})\big) = \mathrm{lcm}\big(\mathrm{N}(f_1) - 1, \mathrm{N}(f_2) - 1\big).$$

For each p in P, we have

$$f_1 f_2 \equiv f_0 \equiv x(p)\, y(p) \equiv f_1\, y(p) \bmod p^{r(p)+1}\mathcal{O},$$

so $f_2 \equiv y(p) \bmod p^{r(p)+1}\mathcal{O}$. Thus, our selection of $x(p)$ and $y(p)$ guarantees that

$$\gcd\big(\mathrm{N}(f_j) - 1, n\big) \text{ is a divisor of } (8k)! \text{ for } j = 1, 2.$$

Therefore

$$\gcd\big(\mathrm{e}(f'\mathcal{O}), n\big) = \mathrm{lcm}\Big(\gcd\big(\mathrm{N}(f_1) - 1, n\big), \gcd\big(\mathrm{N}(f_2) - 1, n\big)\Big)$$

is a divisor of $(8k)!$.

Case 2. *The general case.* We may assume $g \in B$, by replacing g with sg, for some appropriate $s \in S$. (Note that, since elements of S are units in BS^{-1}, we have $sgBS^{-1} = gBS^{-1}$.) Let γ be a nonzero element of $\mathcal{O}$, such that $\gamma\mathcal{O} \subseteq B$. By 3.4(1), there exists $f_0 \in B$, such that $f_0 \equiv f \bmod gBS^{-1}$ and $f_0 B + gn\gamma^2 B = B$. From Case 1, we get $f' \equiv f_0 \bmod gn\gamma^2\mathcal{O}$, such that

$$\gcd\big(\mathrm{e}(f'\mathcal{O}), n\big) \text{ is a divisor of } (8k)!.$$

From 3.4(2b), we see that $U\big(f'BS^{-1}\big)$ is isomorphic to a quotient of $U(f'\mathcal{O})$, so (2a) holds. Also, we have $f' \equiv f_0 \equiv f \bmod gBS^{-1}$ and

$$\begin{aligned} f'BS^{-1} + nBS^{-1} &\supseteq f'BS^{-1} + gn\gamma^2\mathcal{O}S^{-1} = f_0 BS^{-1} + gn\gamma^2\mathcal{O}S^{-1} \\ &\supseteq f_0 BS^{-1} + gn\gamma^2 BS^{-1} = BS^{-1}. \end{aligned}$$ □

(3.9) **Theorem** (cf. [CKP, (4.5)]). BS^{-1} *satisfies* $\mathsf{Exp}\big(2(8k)!, 2\big)$.

Proof. Let:

- q be any element of BS^{-1} with $q \neq 0$,
- (a, b) be any element of $W(qBS^{-1})$ with $a \neq 0$ and $b \neq 0$ (see 3.7(2,3)),
- $c, d \in BS^{-1}$, such that $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, BS^{-1}; qBS^{-1})$,
- $a' = a$, $b'_1 = b$, $d'_1 = d$,

- $u_i = 1$ for $i = 1, 2$,
- $b_0 = b/q \in BS^{-1}$,
- α_1 be the exponent of a modulo bBS^{-1},
- $b' \equiv b_0 \bmod aBS^{-1}$, such that (see 3.8(2)):
  - the exponent $\alpha_2 = \mathrm{e}(b'BS^{-1})$ has the property that $\gcd(\alpha_1, \alpha_2)$ is a divisor of $(8k)!$, and
  - $b'BS^{-1} + qBS^{-1} = BS^{-1}$,
- $b_2' = b'q$,
- $d_2' \in BS^{-1}$, such that $\begin{bmatrix} a & b_2' \\ c & d_2' \end{bmatrix} \in \mathrm{SL}(2, BS^{-1}; qBS^{-1})$, that is,

$$d_2' = d + \frac{(b_2' - b)c}{a} = d + \frac{q(b' - b_0)c}{a},$$

- $t_1, t_2 \in \mathbb{Z}$, such that $\alpha_1 t_1 + \alpha_2 t_2 = (8k)!$, and
- $f_i, g_i \in BS^{-1}$ (for $i = 1, 2$) be defined by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{\alpha_1 t_1} = f_1 \mathbb{I}_{2\times 2} + g_1 \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

$$\begin{bmatrix} a & b_2' \\ c & d_2' \end{bmatrix}^{\alpha_2 t_2} = f_2 \mathbb{I}_{2\times 2} + g_2 \begin{bmatrix} a & b_2' \\ c & d_2' \end{bmatrix}.$$

Now, by multiplying matrices modulo cBS^{-1}, we see that

$$a^{2(8k)!} = (a^{\alpha_1 t_1})^2 (a^{\alpha_2 t_2})^2 \equiv (f_1 + g_1 a)^2 (f_2 + g_2 a)^2 \bmod cBS^{-1}.$$

Similarly,

$$f_1 + g_1 a \equiv a^{\alpha_1 t_1} \equiv 1 = u_1 \bmod bBS^{-1}.$$

Finally, because

- $f_2 + g_2 a \equiv a^{\alpha_2 t_2} \bmod b_2' BS^{-1}$ (by a similar calculation),
- $a^{\alpha_2 t_2} \equiv 1^{t_2} = 1 \bmod b'BS^{-1}$ (by definition of α_2),
- $a^{\alpha_2 t_2} \equiv 1^{\alpha_2 t_2} = 1 \bmod qBS^{-1}$ (since $(a, b) \in W(qBS^{-1})$), and
- $b_2' = b'q$ with b' relatively prime to q,

we conclude that

$$f_2 + g_2 a \equiv a^{\alpha_2 t_2} \equiv 1 = u_2 \bmod b_2' BS^{-1}. \qquad \square$$

(3.10) **Remark.** The function $2(8k)!$ in the conclusion of Theorem 3.9 is much larger than necessary, but reducing the order of magnitude would not yield any improvement in the main results — all that matters is that the function depends only on k. However, it would be of interest to replace $2(8k)!$ with a function that is bounded on an infinite subset of $\mathbb{N}$. For example, perhaps there is a constant t (independent of k), such that BS^{-1} satisfies $\mathsf{Exp}(\mathsf{t}, 2)$ whenever k is odd. If so, then the bound r in Theorem 1.2 could be chosen to depend only on n, when k is odd and $n \geq 3$.

§3C. Bounding the order of the universal Mennicke group. The properties $\mathsf{Gen}(\mathsf{t}, \mathsf{r})$ and $\mathsf{Exp}(\mathsf{t}, \ell)$ were specifically designed to be be what is needed in the proof of the following theorem.

(3.11) **Theorem** [CKP, (1.8)]. *Let:*

- t, r, *and* ℓ *be positive integers,*
- A *be an integral domain satisfying* $\mathsf{SR}_{1\frac{1}{2}}$, $\mathsf{Gen}(\mathsf{t},\mathsf{r})$, *and* $\mathsf{Exp}(\mathsf{t},\ell)$, *and*
- $\mathfrak{q}$ *be an ideal in* A.

Then the universal Mennicke group $C(\mathfrak{q})$ *is finite, and its order is bounded by* t^{r}.

Proof. To bound the order of the abelian group $C(\mathfrak{q})$, it suffices to bound both the exponent and the number of generators needed. We assume $\mathfrak{q} \neq 0$ (because the desired conclusion is obvious otherwise). Note that, for any nonzero $q \in \mathfrak{q}$, the natural homomorphism $C(qA) \to C(\mathfrak{q})$ is surjective (see 2.19(4)), so we may assume $\mathfrak{q} = qA$ is principal.

Step 1. (cf. [Li, (2.4)]) *The exponent of* $C(\mathfrak{q})$ *is a divisor of* t. (*I.e., if* z *is in* $C(\mathfrak{q})$, *then* $z^{\mathsf{t}} = 1$.) Let $\left[\!\left[\begin{smallmatrix} b \\ a \end{smallmatrix} \right]\!\right]_{qA}$ be an arbitrary element of $C(qA)$. Because, by assumption, A satisfies the exponent property $\mathsf{Exp}(\mathsf{t},\ell)$, there exist $a', c, d \in A$ and $u_i, f_i, g_i, b_i', d_i' \in A$ (for $1 \le i \le \ell$) satisfying the conditions of (3.6). Applying, in order, 3.6(1)+(MS1b), 2.25(1), (MS2b)+3.6(5), 2.25(2), 2.25(1), 2.25(2), 3.6(6)+(MS1b), and 2.19(3), we have

$$\begin{aligned}
\left[\!\left[\begin{matrix} b \\ a \end{matrix} \right]\!\right]_{qA}^{-\mathsf{t}} &= \left[\!\left[\begin{matrix} b \\ a' \end{matrix} \right]\!\right]_{qA}^{-\mathsf{t}} = \left[\!\left[\begin{matrix} c \\ a' \end{matrix} \right]\!\right]_{qA}^{\mathsf{t}} = \prod_i \left[\!\left[\begin{matrix} c \\ f_i + g_i a' \end{matrix} \right]\!\right]_{qA}^{2} \\
&= \prod_i \left[\!\left[\begin{matrix} c g_i \\ f_i + g_i a' \end{matrix} \right]\!\right]_{qA}^{2} = \prod_i \left[\!\left[\begin{matrix} b_i' g_i \\ f_i + g_i a' \end{matrix} \right]\!\right]_{qA}^{-2} \\
&= \prod_i \left[\!\left[\begin{matrix} b_i' \\ f_i + g_i a' \end{matrix} \right]\!\right]_{qA}^{-2} = \prod_i \left[\!\left[\begin{matrix} b_i' \\ u_i \end{matrix} \right]\!\right]_{qA}^{-2} = \prod_i 1^{-2} = 1.
\end{aligned}$$

Step 2. $C(\mathfrak{q})$ *can be generated by* r *or less elements.* Because of Step 1, it suffices to show, for each prime divisor p of t, that the rank of $C(\mathfrak{q})/C(\mathfrak{q})^p$ is $\le \mathsf{r}$.

- Let $\left[\!\left[\begin{smallmatrix} b_i \\ a_i \end{smallmatrix} \right]\!\right]_{qA} \in C(qA)$, for $1 \le i \le \mathsf{r}+1$.
- By repeated application of $\mathsf{SR}_{1\frac{1}{2}}$, we can inductively construct a sequence $a_1', \ldots, a_{\mathsf{r}+1}'$ of elements of A, such that:
  - $a_i' \equiv a_i \bmod b_i A$, for $1 \le i \le \mathsf{r}+1$, and
  - $a_i'A + a_j'A = A$ for $1 \le i < j \le \mathsf{r}+1$.
- By the Chinese Remainder Theorem, choose $y \in A$ with:
  - $y \equiv 1 \bmod qA$ and
  - $y \equiv b_i \bmod a_i'A$ for $1 \le i \le \mathsf{r}+1$.
- Now $yA + a_1'a_2' \cdots a_{\mathsf{r}+1}' qA = A$, so $\mathsf{Gen}(\mathsf{t},\mathsf{r})$ implies that there exists

  $h \equiv y \bmod a_1'a_2' \cdots a_{\mathsf{r}+1}' qA$, such that $U(hA)/U(hA)^p$ has rank $\le \mathsf{r}$.

- Hence, there exists $\alpha \in A$ and integers $e_1, e_2, \ldots, e_{\mathsf{r}+1}$, with $e_i \not\equiv 0 \bmod p$ for some i, such that

$$\prod_{i=1}^{\mathsf{r}+1} (a_i')^{e_i} \equiv \alpha^p \bmod hA.$$

- Since $h \equiv y \equiv 1 \bmod qA$, we have $hA + qA = A$. Therefore, we can choose $\beta \in A$ with
$$\beta \equiv \alpha \bmod hA \quad \text{and} \quad \beta \equiv 1 \bmod qA.$$

We have $\beta^p \equiv \alpha^p \bmod hA$ and $\beta^p \equiv 1 \bmod qA$. Hence
$$\beta^p \equiv \prod_{i=1}^{\mathsf{r}+1} (a_i')^{e_i} \bmod hqA.$$
Now, since $h \equiv y \equiv b_i \bmod a_i'A$, we have
$$\llbracket \begin{smallmatrix} b_i \\ a_i \end{smallmatrix} \rrbracket_{qA} = \llbracket \begin{smallmatrix} b_i \\ a_i' \end{smallmatrix} \rrbracket_{qA} = \llbracket \begin{smallmatrix} b_i \\ a_i' \end{smallmatrix} \rrbracket_{qA} \llbracket \begin{smallmatrix} q \\ a_i' \end{smallmatrix} \rrbracket_{qA} = \llbracket \begin{smallmatrix} b_i q \\ a_i' \end{smallmatrix} \rrbracket_{qA} = \llbracket \begin{smallmatrix} hq \\ a_i' \end{smallmatrix} \rrbracket_{qA}.$$
Hence
$$\begin{aligned} \prod_{i=1}^{\mathsf{r}+1} \llbracket \begin{smallmatrix} b_i \\ a_i \end{smallmatrix} \rrbracket_{qA}^{e_i} = \prod_{i=1}^{\mathsf{r}+1} \llbracket \begin{smallmatrix} hq \\ a_i' \end{smallmatrix} \rrbracket_{qA}^{e_i} &= \llbracket \begin{smallmatrix} hq \\ \prod_{i=1}^{t+1} (a_i')^{e_i} \end{smallmatrix} \rrbracket_{qA} \\ &= \llbracket \begin{smallmatrix} hq \\ \beta^p \end{smallmatrix} \rrbracket_{qA} = \llbracket \begin{smallmatrix} hq \\ \beta \end{smallmatrix} \rrbracket_{qA}^{p} \in C(qA)^p. \end{aligned}$$
Since $\llbracket \begin{smallmatrix} b_1 \\ a_1 \end{smallmatrix} \rrbracket_{qA}, \ldots, \llbracket \begin{smallmatrix} b_{\mathsf{r}+1} \\ a_{\mathsf{r}+1} \end{smallmatrix} \rrbracket_{qA}$ are arbitrary elements of $C(qA)$, and some e_i is nonzero modulo p, we conclude that the rank of $C(qA)/C(qA)^p$ is $\leq \mathsf{r}$. □

§3D. Bounded generation in $\mathrm{SL}(n, A)$ for $n \geq 3$. The preceding results enable us to establish Theorem 1.2 in the case where $n \geq 3$ (see 3.13(1)).

(3.12) **Theorem.** *Let:*

- $n \geq 3$,
- t, r, *and* ℓ *be positive integers,*
- A *be an integral domain satisfying* $\mathsf{SR}_{1\frac{1}{2}}$, $\mathsf{Gen}(\mathsf{t}, \mathsf{r})$, *and* $\mathsf{Exp}(\mathsf{t}, \ell)$, *and*
- $\mathfrak{q}$ *be an ideal in* A.

Then $\mathrm{SL}(n, A; \mathfrak{q}) / \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$ *is finite, and its order is bounded by* t^{r}.

Proof. By combining Thms. 2.14 and 2.18 (with $\mathsf{m} = 2$ and $N = \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$), we see that $\mathrm{SL}(n, A; \mathfrak{q}) / \mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$ is isomorphic to a quotient of the universal Mennicke group $C(\mathfrak{q})$. From Theorem 3.11, we know that $\#C(\mathfrak{q}) \leq \mathsf{t}^{\mathsf{r}}$, so the desired conclusion is immediate. □

Applying the Compactness Theorem (see 2.8) to this finiteness result yields bounded generation. In the particular case of number rings, we obtain the following conclusions.

(3.13) **Corollary** (cf. [CKP, (2.4)])**.** *Let:*

- n *be a positive integer* ≥ 3,
- K *be an algebraic number field,*
- k *be the degree of* K *over* $\mathbb{Q}$,
- B *be an order in* K,
- S *be a multiplicative subset of* B, *and*
- $\mathfrak{q}$ *be an ideal in* BS^{-1}.

Then:

(1) $\mathrm{LU}(n, BS^{-1})$ *boundedly generates* $\mathrm{E}(n, BS^{-1})$.

(2) $\mathrm{LU}^{\triangleleft}(n, BS^{-1}; \mathfrak{q})$ *boundedly generates* $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q})$.

More precisely, there is a positive integer r*, depending only on* k *and* n*, such that*

$$\left\langle \mathrm{LU}(n, BS^{-1}) \right\rangle_r = \mathrm{E}(n, BS^{-1}) \text{ and } \left\langle \mathrm{LU}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}) \right\rangle_r = \mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}).$$

A generalization of 3.13(2) that applies to all normal subgroups, not merely the one subgroup $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q})$, can be found in §6. It is proved by combining this result (and an analogous result for the case $n = 2$) with the Sandwich Condition (6.4).

4. Additional first-order properties of number rings

We define two properties ($\mathsf{Unit}(\mathsf{r}, \mathsf{x})$ and $\mathsf{Conj}(\mathsf{z})$), and show they are satisfied by number rings BS^{-1} that have infinitely many units (see 4.4 and 4.6). As in §3, it is crucial that these properties can be expressed by first-order sentences (for fixed values of the parameters r, x, and z).

(4.1) **Notation.** Throughout this section,

- K is an algebraic number field,
- k is the degree of K over $\mathbb{Q}$,
- $\mathcal{O}$ is the ring of integers of K,
- B is an order in $\mathcal{O}$, and
- S is a multiplicative subset of B.

§4A. Unit property $\mathsf{Unit}(\mathsf{r}, \mathsf{x})$.

(4.2) **Notation.** If u is a unit in a ring A, then $H(u) = \begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix}$.

(4.3) **Definition** (cf. [CKP, (3.1)]). Let r and x be positive integers. A commutative ring A satisfies the *unit property* $\mathsf{Unit}(\mathsf{r}, \mathsf{x})$ if and only if:

(1) For each nonzero $q \in A$, there exists a unit u in A, such that $u \equiv 1 \bmod qA$ and $u^4 \neq 1$.

(2) There exists a unit u_0 in A with $u_0^2 \neq 1$, such that whenever
  - $\mathfrak{q}$ is an ideal in A with $\leq \mathsf{r}$ generators, and
  - $T \in \mathrm{SL}(2, A; \mathfrak{q})$,

  there exist $E_1, E_2, \ldots, E_{\mathsf{x}} \in \mathrm{LU}(2, \mathfrak{q})$, such that

$$H(u_0)^{-1}\, T\, H(u_0) = E_1 T E_2 E_3 \cdots E_{\mathsf{x}}.$$

(4.4) **Lemma** [CKP, (4.6)]. *If* BS^{-1} *has infinitely many units, then* BS^{-1} *satisfies the unit property* $\mathsf{Unit}(\mathsf{r}, 5)$*, for any* r.

Proof. Let q be any nonzero element of BS^{-1}. Since, by assumption, BS^{-1} has infinitely many units, there is a unit u in BS^{-1} that is not a root of unity. Some power of u satisfies the requirements of 4.3(1).

Let $u_0 = u^{(8k)!}$, $\mathfrak{q}$ be any ideal of BS^{-1}, and $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any element of $\mathrm{SL}(2, A; \mathfrak{q})$. We may assume $\mathfrak{q} \neq 0$, for otherwise $T = \mathbb{I}_{2\times 2}$, so the conclusion of 4.3(2) is trivially true.

- By 3.8(2a), there exists $a' \equiv a \bmod b^2 BS^{-1}$, such that

$$\gcd\big(\mathrm{e}(aBS^{-1}), \mathrm{e}(a'BS^{-1})\big) \text{ is a divisor of } (8k)!,$$

  where $\mathrm{e}(aBS^{-1})$ denotes the exponent of $U\big(aBS^{-1}\big)$.

- Choose $z \in BS^{-1}$, such that $a' = a + zb^2$.
- Choose $t, t' \in BS^{-1}$, such that $t\,\mathrm{e}(aBS^{-1}) + t'\,\mathrm{e}(a'BS^{-1}) = (8k)!$.
- Let $u^{2t\,\mathrm{e}(aBS^{-1})} = ax + 1$ and $u^{-2t\,\mathrm{e}(aBS^{-1})} = ay + 1$.

We have

$$\begin{aligned} H(u^{-t\,\mathrm{e}(aBS^{-1})})T\,H(u^{t\,\mathrm{e}(aBS^{-1})}) &= \begin{bmatrix} a & u^{-2t\,\mathrm{e}(aBS^{-1})}b \\ u^{2t\,\mathrm{e}(aBS^{-1})}c & d \end{bmatrix} \\ &= \begin{bmatrix} a & (ay+1)b \\ (ax+1)c & d \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ xc & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & yb \\ 0 & 1 \end{bmatrix} \\ &= E_{2,1}(*)\,T\,E_{1,2}(*). \end{aligned}$$

Letting $T' = T \begin{bmatrix} 1 & 0 \\ zb & 1 \end{bmatrix} = \begin{bmatrix} a' & b \\ * & d \end{bmatrix}$, the same calculation shows that

$$H(u^{-t'\,\mathrm{e}(a'BS^{-1})})T'\,H(u^{t'\,\mathrm{e}(a'BS^{-1})}) = E_{2,1}(*)\,T'\,E_{1,2}(*).$$

Therefore

$$\begin{aligned} &H(u_0)^{-1}T\,H(u_0) \\ &\quad = H(u^{-t'\,\mathrm{e}(a'BS^{-1})})\,E_{2,1}(*)\,T\,E_{1,2}(*)\,H(u^{t'\,\mathrm{e}(a'BS^{-1})}) \\ &\quad = H(u^{-t'\,\mathrm{e}(a'BS^{-1})})\,E_{2,1}(*)\,T'\,E_{2,1}(*)\,E_{1,2}(*)\,H(u^{t'\,\mathrm{e}(a'BS^{-1})}) \\ &\quad = E_{2,1}(*)\,T'\,E_{1,2}(*)\,E_{2,1}(*)\,E_{1,2}(*) \\ &\quad = E_{2,1}(*)\,T\,E_{2,1}(*)\,E_{1,2}(*)\,E_{2,1}(*)\,E_{1,2}(*), \end{aligned}$$

with each of the elementary matrices in $\mathrm{LU}(2,\mathfrak{q})$. Hence, 4.3(2) is satisfied with $\mathsf{x} = 5$. □

§4B. Conjugation property $\mathsf{Conj}(\mathsf{z})$. The following property will be used to control the image of the other elementary matrices under conjugation by $E_{1,2}$ (see 5.17).

(4.5) **Definition.** Let z be a positive integer, and let A be a commutative ring.

- For ideal $\mathfrak{q}$ of A, let
$$\mathcal{M}_{\mathfrak{q}} = \left\{ y \in \mathfrak{q} \;\middle|\; \begin{array}{c} \text{there exists } z \equiv \pm 1 \bmod \mathfrak{q}, \text{ and} \\ \text{units } u_1, u_2 \text{ in } A, \text{ such that} \\ 1 + yzu_1^2 = u_2^2 \end{array} \right\}.$$
- The ring A is said to satisfy $\mathsf{Conj}(\mathsf{z})$ if, for every nonzero $q \in A$, there is a nonzero $q' \in A$, such that every element of $q'A$ is a sum of $\le \mathsf{z}$ elements of $\mathcal{M}_{qA}$.

Most of the proof of the following theorem appears in [Va, p. 327] and [Li, pp. 519–521], but [CKP] modified the argument to avoid Liehl's assumption that the prime p splits completely in K. This eliminates the need to place restrictions on K (as in [Li]).

(4.6) **Theorem** (cf. [CKP, (4.7)]). *If BS^{-1} has infinitely many units, then BS^{-1} satisfies $\mathsf{Conj}(7k)$.*

Proof. For convenience, let us use $[j]\mathcal{M}_{qA}$ to denote the set of elements of BS^{-1} that are a sum of j elements of $\mathcal{M}_{qA}$.

Claim. *It suffices to find*

- *nonzero* $q', q'' \in A$,
- *positive integers* r, m, *with* $\gcd(r, m) = 1$, *and*
- *a finite subset* D *of* B, *such that* $\#D \leq k+1$, *and the* $\mathbb{Z}$*-span of* D *contains* $q'B$,

such that $pdq'' \in \mathcal{M}_{qA}$, *for*

- *every rational prime* p *that is congruent to* r *modulo* m, *and*
- *every* $d \in D$.

We show that if there exist such q', q'', r, m, and D, then the principal ideal $q'q''mBS^{-1}$ is contained in $[7k]\mathcal{M}_{qA}$. To this end, let b be any nonzero element of B and $s \in S$. By assumption on D, we may write $q'b = \sum_{i=1}^{k+1} b_i d_i$ with $b_i \in \mathbb{Z}$ and $d_i \in D$. For each i,

- $b_i m$ is a signed sum of 6 rational primes that are congruent to r modulo m (see 2.33),
- $pd_iq'' \in \mathcal{M}qA$, for each of these primes p, and
- $-\mathcal{M}_{qA} = \mathcal{M}_{qA}$ (because z can be replaced by $-z$),

so $b_imd_iq'' \in [6]\mathcal{M}_{qA}$. Hence

$$q'bmq'' = \sum_{i=1}^{k+1} b_imd_iq'' \in [6(k+1)]\mathcal{M}_{qA} \subseteq [7k]\mathcal{M}_{qA}.$$

Since it is clear from the definition that $\mathcal{M}_{qA}$ is closed under multiplication by s^{-2} (this is the reason for including the unit u_1), we see that $q'mq''(b/s^2) \in [7k]\mathcal{M}_{qA}$. Since b/s^2 is an arbitrary element of BS^{-1}, we conclude that $q'mq''BS^{-1} \subseteq [7k]\mathcal{M}_{qA}$, as desired.

This completes the proof of the claim. □

We now find q', q'', r, m, and D as described in the Claim. We begin by establishing notation.

- To prove the result for a particular value of q, it suffices to prove it for some nonzero multiple of q. Therefore, we may assume q is a rational integer, such that:
  - the exponent e of $U(q\mathbb{Z})$ is divisible by $k!$,
  - $q\mathcal{O} \subseteq B$, and
  - the discriminant of K divides q.
- Furthermore, we may assume there exists $t \in \mathbb{Z}$, such that $t^e - 1 \equiv aq \bmod q^2\mathbb{Z}$, with $\gcd(a, q) = 1$. (To achieve, this, let $q = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ be the prime factorization. By carefully enlarging q, we may assume, for $i \neq j$, that $p_i^{e_i}$ does not divide $\phi(p_j^{e_j})$. Choose t so that, for each i, its image in $U\big(p_i^{e_i+2}\mathbb{Z}\big)$ is an element of maximal order.)
- Let $D = \big\{\, t^{e-1}(a + qd_0) \bigm| d_0 \in D_0 \cup \{0\} \,\big\}$, where D_0 is some basis for B as a $\mathbb{Z}$-module. (Note that $\#D \leq k+1$, and the $\mathbb{Z}$-span of D contains $t^{e-1}qB$.)
- Let $b = t^{e-1}a \prod_{d_0 \in D_0}(a + qd_0)$. (Note that every element of D is a divisor of b, and b is relatively prime to q.)

- Because BS^{-1} has infinitely many units, there is some unit u that is not a root of unity. Multiplying by an element of S, we may assume $u \in B$. Furthermore, by replacing u with an appropriate power, we may assume that $u \equiv 1 \bmod q^2bB$ (and $u^2 \neq 1$).
- Let $y = u^2 - 1 \in q^2bB$, so $\mathrm{N}(y) \in (q^2bB) \cap \mathbb{Z}$.
- Let $q'' = qy(1+y)^{-1} = qy/u^2 \in BS^{-1}$.
- Write $\mathrm{N}(y) = n_0n_1$, where $\gcd(q, n_0) = 1$, and any (rational) prime dividing n_1 divides q.
- Let r be a rational integer with:
  - $r \equiv t \bmod q^2$ and
  - $r \equiv 1 \bmod n_0$.

Let d be any element of D, and let p be any rational prime that is congruent to r, modulo $\mathrm{N}(y)$. We will show that $pdq'' \in \mathcal{M}_{qA}$, which, by the Claim, completes the proof.

- Since $y^{p^e-1} \equiv 0 \bmod dq^2BS^{-1}$, and $p \equiv r \bmod q^2dBS^{-1}$, and $td = t^e(a + qd_0) \equiv a \bmod qBS^{-1}$, we have
  - $y^{p^e-1} + p^e - pdq - 1 \equiv 0 + r^e - 0 - 1 \equiv 0 + 1^e - 0 - 1 = 0 \bmod dBS^{-1}$, and
  - $y^{p^e-1} + p^e - pdq - 1 \equiv 0 + (t^e - 1) - tdq \equiv 0 + aq - aq = 0 \bmod q^2BS^{-1}$,

  so $y^{p^e-1} + p^e - pdq - 1 \equiv 0 \bmod dq^2BS^{-1}$. Therefore
  $$y^{p^e} + p^e y - pdqy - y$$
  is divisible by dq^2y. Since $k!$ divides e (and because p, being relatively prime to q, does not divide the discriminant of K), we know that $y^{p^e} \equiv y \bmod pBS^{-1}$, so the displayed expression is also divisible by p.
- Therefore $y^{p^e} + p^e y \equiv pdqy + y \bmod pdq^2yBS^{-1}$.
- Hence $(1+y)^{p^e} \equiv 1 + p^e y + y^{p^e} \equiv 1 + y + pdqy \bmod pdq^2yBS^{-1}$.
- Thus (recalling that $q'' = qy(1+y)^{-1}$), we have
  $$(1+y)^{p^e-1} \equiv 1 + pdq'' \bmod pdqq''BS^{-1},$$
  so we may write $(1+y)^{p^e-1} = 1 + pdq''z$ with $z \equiv 1 \bmod qBS^{-1}$.
- Since $(1+y)^{p^e-1} = (u^{p^e-1})^2$ is the square of a unit, we conclude that $pdq'' \in \mathcal{M}_{qA}$ (taking $u_1 = 1$).

By the Claim, this completes the proof. □

5. Bounded generation in SL(2, A)

In this section, we establish Theorem 1.2 in the case where $n = 2$ (see 5.26(1)). This complements Theorem 3.13(1), which dealt with the case where $n \geq 3$.

(5.1) **Remark** (nonstandard analysis)**.** In this section, we frequently use the theory of nonstandard analysis (cf. §2E). As an aid to the reader who wishes to construct a classical proof, we point out that:

- Corollary 5.20 is simply a restatement of Lemma 5.19 in nonstandard terms.
- Lemma 5.4 is a technical result that should be omitted from a classical presentation of this material.
- Proposition 5.21 asserts the existence of an ideal $\mathfrak{q}'$ of A, such that
  $$[\mathrm{SL}(2,K), \mathrm{SL}(2,A;\mathfrak{q}')] \subseteq \mathrm{E}(2,\mathfrak{q}).$$

- Lemma 5.24 states, for any nonzero $y \in A$, that there is a nonzero ideal $\mathfrak{q}'$ of A, such that $\mathfrak{q}' \subseteq \mathfrak{q}$, and $\begin{bmatrix} by^2 \\ a \end{bmatrix}_{\mathfrak{q}} = \begin{bmatrix} b \\ a \end{bmatrix}_{\mathfrak{q}}$ for all $(a,b) \in W(\mathfrak{q}')$.

(5.2) **Notation.** Let

$$\mathcal{Q} = \bigcap_{\substack{\mathfrak{q} \text{ is an} \\ \text{ideal in } A}} {}^*\mathfrak{q} = \bigcap_{q \in A} q\, {}^*\!A.$$

This is an (external) ideal of ${}^*\!A$.

§5A. Preliminaries.

(5.3) **Definition** (cf. [Va])**.** If $\mathfrak{q}$ is an ideal in a commutative ring A, then

$$\mathrm{SSL}(2, A; \mathfrak{q}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, A) \;\middle|\; \begin{matrix} a, d \equiv 1 \bmod \mathfrak{q}^2 \\ b, c \equiv 0 \bmod \mathfrak{q} \end{matrix} \right\}.$$

This is a subgroup of $\mathrm{SL}(2, A; \mathfrak{q})$ that contains $\mathrm{E}(2, \mathfrak{q})$ and $\mathrm{SL}(2, A; \mathfrak{q}^2)$.

(5.4) **Lemma.** *The ideal $\mathcal{Q}$ is nonzero, and we have $\mathcal{Q}^2 = \mathcal{Q}$. Therefore,*

$$\mathrm{SSL}(2, A; \mathcal{Q}) = \mathrm{SL}(2, A; \mathcal{Q}).$$

Proof. If F is any finite set of nonzero elements of A, then (because A is an integral domain) there is some nonzero $y \in A$, such that y is a multiple of every element of F. Since ${}^*\!A$ is assumed to be polysaturated, this implies that there is some nonzero $z \in {}^*\!A$, such that z is a multiple of every element of A. Then $z \in \mathcal{Q}$, so $\mathcal{Q} \neq \{0\}$.

Now, for any fixed element z of $\mathcal{Q}$, consider the internal binary relation $R_z \subseteq {}^*\!A \times {}^*\!A$ given by

$$R_z = \{\, (x, y) \mid y \in {}^*\!Ax \text{ and } z \in {}^*\!Ay^2 \,\}.$$

Since $z \in \mathcal{Q}$, it is easy to see that if F is any finite set of nonzero elements of A, then there is a nonzero element y of A, such that $(x, y) \in R_z$ for all $x \in F$. By polysaturation, there is some nonzero $y_0 \in {}^*\!A$, such that $(x, y_0) \in R_z$ for every nonzero $x \in A$. Therefore $y_0 \in \mathcal{Q}$ and $z \in {}^*\!Ay_0^2 \subseteq \mathcal{Q}^2$. Since z is an arbitrary element of $\mathcal{Q}$, we conclude that $\mathcal{Q}^2 = \mathcal{Q}$. $\square$

(5.5) **Lemma** (Vaserstein [Va])**.** *Let A be a commutative ring and u be a unit in A.*

(1) *Suppose $u \equiv 1 \bmod q^2 A$ for some q in A. Then $u = 1 + xy$ with x, y in qA, and we have*

$$H(u) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \begin{bmatrix} 1 & -u^{-1}x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -uy & 1 \end{bmatrix}.$$

(2) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} H(u) \begin{bmatrix} 1 & 1 - u^{-2} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = H(u).$

(3) *For x in A, we have* $H(u)^{-1} \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} H(u) = \begin{bmatrix} 1 & 0 \\ xu^2 & 1 \end{bmatrix}.$

(4) *For $y, z \in A$, set*

$$M(y, z) = \begin{bmatrix} 1 & z-1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.$$

Suppose u^2-1 is in $(1+yz)A$, and $(1+yz)w = u^2-1$. Set $c = w(1-z+yz)$. Then
$$M(y,z)H(u)^{-1}\begin{bmatrix}1 & c\\ 0 & 1\end{bmatrix}M(y,z)^{-1}H(u) = \begin{bmatrix}1 & 0\\ -wy & 1\end{bmatrix}.$$

An argument similar to the proof of Corollary 2.15 establishes the following result.

(5.6) **Lemma** (Vaserstein's Lemma 1, cf. [Va, Lem. 1])**.** *Let:*

- *A be a commutative ring, and*
- *$\mathfrak{q}$ and $\mathfrak{q}'$ be nonzero ideals of A, such that $\mathfrak{q}' \subseteq \mathfrak{q}^2$.*

If $A/\mathfrak{q}'$ satisfies SR_1, then $\mathrm{SSL}(2,A;\mathfrak{q}) = \mathrm{SL}(2,A;\mathfrak{q}')\,\mathrm{E}(2,\mathfrak{q})$.

Proof. By modding out $\mathfrak{q}'$, we may assume that A satisfies SR_1, and we wish to show that $\mathrm{E}(2,\mathfrak{q}) = \mathrm{SSL}(2,A;\mathfrak{q})$. It suffices to show that if $a,b \in A$, with

(1) $a \equiv 1 \bmod \mathfrak{q}^2$,
(2) $b \in \mathfrak{q}$, and
(3) $aA + bA = A$,

then there exists $E \in \mathrm{E}(2,\mathfrak{q})$, such that $(a,b)E = (1,0)$.

Since $a \equiv 1 \bmod \mathfrak{q}$, and $aA+bA = A$, we know that $aA+b\mathfrak{q} = A$; so SR_1 implies that there exists $q \in \mathfrak{q}$, such that $a+bq$ is a unit. Thus, by replacing (a,b) with $(a,b)E_{2,1}(q)$, we may assume
$$a \text{ is a unit.}$$
Then, by replacing (a,b) with $(a,b)E_{1,2}(-a^{-1}b)$, we may assume
$$b = 0.$$
Write
$$1 - a = x_1y_1 + \cdots + x_ry_r$$
with $x, y \in \mathfrak{q}$, and r minimal. The remainder of the proof is by induction on r.

Base case. Assume $a = 1 + xy$ with $x, y \in \mathfrak{q}$. Applying $E_{1,2}\big(a^{-1}x\big)$, $E_{1,2}(-y)$, and $E_{1,2}(-x)$ sequentially, we have
$$(a,0) \to (a,x) \to (1,x) \to (1,0).$$

Induction step. Let $\mathfrak{q}'' = x_1y_1A + \cdots + x_{r-1}y_{r-1}A$. Now
$$1 - a = x_1y_1 + \cdots + x_ry_r \equiv x_ry_r \bmod \mathfrak{q}'',$$
so, by applying the base case to the ring $A/\mathfrak{q}''$, we know there is some $E \in \mathrm{E}(2,\mathfrak{q})$, such that $(a,0)E \equiv (1,0) \bmod \mathfrak{q}''$. We may also assume, by the argument above, that $(a,0)E = (u,0)$, for some unit u (because the transformations will not change the congruence class of $(a,0)E$ modulo $\mathfrak{q}''$). By the induction hypothesis, then there exists $E' \in \mathrm{E}(2,\mathfrak{q})$, such that $(a,0)EE' = (1,0)$. □

§5B. A sufficient condition for a Mennicke symbol. Because Mennicke's Theorem 2.18(3) does not apply when $n = 2$, we prove the following result that yields a Mennicke symbol.

(5.7) **Proposition.** *Suppose:*

- *A is an integral domain,*
- *$\mathfrak{q}$ is an ideal of A, and*
- *N is a normal subgroup of* $\mathrm{SL}(2,A;\mathfrak{q})$,

such that:

- *A satisfies* $\mathsf{SR}_{1\frac{1}{2}}$ *and* $\mathsf{Gen}(2,1)$,
- $\bigl[\mathrm{E}(2,A), \mathrm{SL}(2,A;\mathfrak{q})\bigr] \subseteq N$,
- $\mathrm{E}^{\triangleleft}(2,A;\mathfrak{q}) \subseteq N$,
- $C = \mathrm{SL}(2,A;\mathfrak{q})/N$,
- $\begin{bmatrix} \ \end{bmatrix} : W(\mathfrak{q}) \to C$ *is defined by* $\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} a & b \\ * & * \end{bmatrix} N$, *and*
- ${}^{*}\!\begin{bmatrix} by^2 \\ a \end{bmatrix} = {}^{*}\!\begin{bmatrix} b \\ a \end{bmatrix}$ *for all* $(a,b) \in W(\mathcal{Q})$ *and all nonzero* $y \in A$.

Then $\begin{bmatrix} \ \end{bmatrix}$ *is a well-defined Mennicke symbol.*

(5.8) **Remark.** From Theorem 2.18, we know that $\begin{bmatrix} \ \end{bmatrix}$ is well-defined, and satisfies (MS1a) and (MS1b). The problem is to establish (MS2a).

We begin with a useful calculation.

(5.9) **Lemma** (cf. [Va, Case 1, p. 331])**.** *Let* $(a_1,b),(a_2,b) \in W(\mathfrak{q})$, *and suppose* $\begin{bmatrix} a_2 & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,A;\mathfrak{q})$. *Then*

$$\begin{bmatrix} b \\ a_1 a_2 \end{bmatrix} \begin{bmatrix} b \\ a_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_2 b(1-a_1) \\ 1 + a_2 d(a_1 - 1) \end{bmatrix}.$$

Proof. Because $bc = a_2 d - 1$, we have

$$\begin{aligned}
\begin{bmatrix} a_1 a_2 & b \\ * & * \end{bmatrix} \begin{bmatrix} a_2 & b \\ c & d \end{bmatrix}^{-1} &= \begin{bmatrix} a_1 a_2 & b \\ * & * \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a_2 \end{bmatrix} \\
&= \begin{bmatrix} a_1 a_2 d - bc & -a_1 a_2 b + b a_2 \\ * & * \end{bmatrix} \\
&= \begin{bmatrix} 1 + a_2 d(a_1 - 1) & a_2 b(1-a_1) \\ * & * \end{bmatrix}.
\end{aligned}$$

□

Let us show that it suffices to consider principal ideals.

(5.10) **Lemma** [CKP, (3.13)]**.** *Suppose A, $\mathfrak{q}$, N, C, and* $\begin{bmatrix} \ \end{bmatrix}$ *are as in the statement of Proposition* 5.7. *If the restriction of* $\begin{bmatrix} \ \end{bmatrix}$ *to $W(qA)$ is a Mennicke symbol, for every nonzero $q \in \mathfrak{q}$, then* $\begin{bmatrix} \ \end{bmatrix}$ *is a Mennicke symbol.*

Proof. By (5.8) and Lam's Theorem 2.20(1), we need only establish (MS2b). Given

$$(a_1,b),(a_2,b) \in W(\mathfrak{q}),$$

we know, by assumption, that

$$\text{the restriction of } \begin{bmatrix} \ \end{bmatrix} \text{ to } W(qA) \text{ is a Mennicke symbol} \tag{5.11}$$

we have

$$\begin{aligned}
\begin{bmatrix} b \\ a_1a_2 \end{bmatrix} \begin{bmatrix} b \\ a_2 \end{bmatrix}^{-1} &= \begin{bmatrix} a_2b(1-a_1) \\ 1+a_2d(a_1-1) \end{bmatrix} && (5.9) \\
&= \begin{bmatrix} a_2b(1-a_1) \\ 1+a_2d(a_1-1) \end{bmatrix} \begin{bmatrix} 1-a_1 \\ 1+a_2d(a_1-1) \end{bmatrix} && \text{(2nd is trivial)} \\
&= \begin{bmatrix} a_2b(1-a_1)^2 \\ 1+a_2d(a_1-1) \end{bmatrix} && (5.11) \\
&= \begin{bmatrix} a_2(1-a_1) \\ 1+a_2d(a_1-1) \end{bmatrix} \begin{bmatrix} b(1-a_1) \\ 1+a_2d(a_1-1) \end{bmatrix} && (5.11) \\
&= 1 \cdot \begin{bmatrix} b(1-a_1) \\ 1+(1+bc)(a_1-1) \end{bmatrix} && \text{(MS1b)} \\
&= \begin{bmatrix} b(1-a_1) \\ a_1+bc(a_1-1) \end{bmatrix} \\
&= \begin{bmatrix} b(1-a_1) \\ a_1 \end{bmatrix} && \text{(MS1b)} \\
&= \begin{bmatrix} b \\ a_1 \end{bmatrix} && \text{(MS1a).}
\end{aligned}$$

□

Proof of Proposition 5.7. By Lemma 5.10, we may assume $\mathfrak{q} = qA$ is principal. Also, by (2.24), it suffices to show that if $(a_1, bq), (a_2, bq) \in W(\mathfrak{q})$, and either $\begin{bmatrix} bq \\ a_1 \end{bmatrix} = 1$ or $\begin{bmatrix} bq \\ a_2 \end{bmatrix} = 1$, then

$$\begin{bmatrix} bq \\ a_1 \end{bmatrix} \begin{bmatrix} bq \\ a_2 \end{bmatrix} = \begin{bmatrix} bq \\ a_1a_2 \end{bmatrix}. \tag{5.12}$$

Note that the elements $\begin{bmatrix} bq \\ a_1 \end{bmatrix}$ and $\begin{bmatrix} bq \\ a_2 \end{bmatrix}$ commute with each other (because one of them is trivial). Thus, there is no harm in interchanging a_1 with a_2 if it is convenient. (That is why we do not assume it is $\begin{bmatrix} bq \\ a_2 \end{bmatrix}$ that is trivial; it is better to allow ourselves some flexibility.)

Case 1. *Assume that either a_1 or a_2 is a square modulo bqA.* Because there is no harm in interchanging a_1 with a_2, we may assume it is a_2 that is a square modulo bqA.

Applying (MS1a) and (MS1b) allows us to make some simplifying assumptions:

- By adding a multiple of bq to a_2, we may assume $a_2 = y^2$, for some y in A.
- By adding a multiple of a_1a_2 to b, we may assume $b{}^*\!A + \mathcal{Q} = {}^*\!A$ (because ${}^*\!A/\mathcal{Q}$ satisfies SR_1).
- By adding a multiple of bq to a_1, we may assume $a_1 \equiv 1 \bmod \mathcal{Q}$. (To see this, let $t \in {}^*\!A$, such that $tb \equiv 1 \bmod \mathcal{Q}$, and then replace a_1 with $a_1 + (1-a_1)tb$.)

We have

$$\begin{aligned}
\begin{bmatrix} bq \\ a_1a_2 \end{bmatrix} \begin{bmatrix} bq \\ a_2 \end{bmatrix}^{-1} &= \begin{bmatrix} a_2bq(1-a_1) \\ 1+a_2d(a_1-1) \end{bmatrix} && (5.9) \\
&= \begin{bmatrix} bq(1-a_1) \\ 1+a_2d(a_1-1) \end{bmatrix} && (\text{by assumption, since } 1-a_1 \in \mathcal{Q}) \\
&= \begin{bmatrix} bq(1-a_1) \\ a_1 \end{bmatrix} && (a_2d = 1+bqc \equiv 1 \bmod bq) \\
&= \begin{bmatrix} bq \\ a_1 \end{bmatrix} && (2.19(2)).
\end{aligned}$$

Case 2. *The general case.* Because there is no harm in interchanging a_1 with a_2, we may assume it is $\begin{bmatrix} bq \\ a_2 \end{bmatrix}_{\mathfrak{q}}$ that is equal to 1.

Let $T = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. It is not difficult to see that the hypotheses of the proposition are satisfied with $T^{-1}NT$ in the place of N (because conjugation by T is an automorphism that fixes $\mathrm{E}(2,A)$, $\mathrm{SL}(2,A;\mathfrak{q})$, and $\mathrm{E}^{\triangleleft}(2,A;\mathfrak{q})$, and because $(a,-b) \in W(\mathcal{Q})$ for all $(a,b) \in W(\mathcal{Q})$.) Therefore, the hypotheses are also satisfied with $(T^{-1}NT) \cap N$ in the place of N, so we may assume that T normalizes N. Then conjugation by T induces an automorphism of C, so

$$\begin{bmatrix} bq \\ a_2 \end{bmatrix} = 1 = T^{-1}1T = T^{-1}\begin{bmatrix} bq \\ a_2 \end{bmatrix} T = \begin{bmatrix} -\,bq \\ a_2 \end{bmatrix}.$$

Adding a multiple of a_1a_2 to b does not change any of the terms in (5.12), so, since $\mathsf{Gen}(2,1)$ holds in A, we may assume that $U(bA)\,/U(bA)^2$ is cyclic.

Let $\begin{bmatrix} a_2 & -bq \\ c & d \end{bmatrix} \in \mathrm{SL}(2,A;\mathfrak{q})$. Then, by assumption and by the formula for the inverse of a 2×2 matrix, we have

$$\begin{bmatrix} bq \\ a_2 \end{bmatrix}_{\mathfrak{q}}^{-1} = \begin{bmatrix} -\,bq \\ a_2 \end{bmatrix}_{\mathfrak{q}}^{-1} = \begin{bmatrix} bq \\ d \end{bmatrix}_{\mathfrak{q}}.$$

If either a_1 or a_2 is a square mod bqA, then $\begin{bmatrix} bq \\ a_1 \end{bmatrix}\begin{bmatrix} bq \\ a_2 \end{bmatrix} = \begin{bmatrix} bq \\ a_1a_2 \end{bmatrix}$ by Case 1.

If not, then a_1a_2 is a square mod bqA, so, appealing to Case 1 again, we have

$$\begin{bmatrix} bq \\ a_1a_2 \end{bmatrix}_{\mathfrak{q}} \begin{bmatrix} bq \\ a_2 \end{bmatrix}_{\mathfrak{q}}^{-1} = \begin{bmatrix} bq \\ a_1a_2 \end{bmatrix}_{\mathfrak{q}} \begin{bmatrix} bq \\ d \end{bmatrix}_{\mathfrak{q}} = \begin{bmatrix} bq \\ a_1a_2d \end{bmatrix}_{\mathfrak{q}} = \begin{bmatrix} bq \\ a_1 \end{bmatrix}_{\mathfrak{q}}$$

(because $a_2d \equiv a_2d + bqc = 1 \bmod bq$). $\square$

§5C. Finiteness of $\mathrm{SL}(2,A;\mathfrak{q})/\,\mathrm{E}^{\triangleleft}(2,A;\mathfrak{q})$**.** We now prove the following theorem.

(5.13) **Theorem** (cf. [CKP, (3.19)])**.** *Suppose:*

- r, x, ℓ, t, *and* z *are positive integers,*
- *A is an integral domain satisfying:*
  - *the stable range condition* $\mathsf{SR}_{1\frac{1}{2}}$,
  - *the few generators properties* $\mathsf{Gen}(2,1)$ *and* $\mathsf{Gen}(\mathsf{t},\mathsf{r})$,
  - *the exponent property* $\mathsf{Exp}(\mathsf{t},\ell)$,
  - *the unit property* $\mathsf{Unit}(1,\mathsf{x})$, *and*

∘ *the conjugation property* $\mathsf{Conj}(\mathsf{z})$*, and*

- $\mathfrak{q}$ *is any nonzero ideal in* A.

Then $\mathrm{SL}(2, A; \mathfrak{q}) / \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q})$ *is finite.*

(5.14) **Remark.** The proof will show that the order of the quotient group is bounded by t^{r}.

(5.15) **Assumption.** Throughout §5C, r, x, ℓ, t, z, A, and $\mathfrak{q}$ are as in the statement of Theorem 5.13.

(5.16) **Notation.** For $(a, b) \in W(\mathfrak{q})$, we set

$$\begin{bmatrix} b \\ a \end{bmatrix}_{\mathfrak{q}} = \begin{bmatrix} a & b \\ * & * \end{bmatrix} \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q}) \in \mathrm{SL}(2, A; \mathfrak{q}) / \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q}).$$

The key to the proof is showing that $\begin{bmatrix} \ \end{bmatrix}_{\mathfrak{q}}$ is a well-defined Mennicke symbol. For this, we use Proposition 5.7, so it suffices to show that

$$\big[\mathrm{E}(2, A), \mathrm{SL}(2, A; \mathfrak{q})\big] \subseteq \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q})$$

and that ${}^{*}\begin{bmatrix} by^2 \\ a \end{bmatrix}_{\mathfrak{q}} = {}^{*}\begin{bmatrix} b \\ a \end{bmatrix}_{\mathfrak{q}}$ for all $(a, b) \in W(\mathcal{Q})$ and all nonzero $y \in A$. These assertions are established in (5.23) and (5.24), respectively.

Combining Vaserstein's identity 5.5(4) with the conjugation property $\mathsf{Conj}(\mathsf{z})$ yields the following lemma.

(5.17) **Lemma.** *There is a nonzero ideal* $\mathfrak{q}'$ *of* A*, such that*

$$E_{1,2}^{-1} \, \mathrm{LU}(2, \mathfrak{q}') \, E_{1,2} \subseteq \langle \mathrm{LU}(2, \mathfrak{q}) \rangle_{50\mathsf{z}} .$$

Proof ([Va, Lem. 4], [CKP, (4.7)]). Fix some nonzero $q \in \mathfrak{q}$. For convenience, let

$$\mathrm{LU}^{\#} = E_{1,2} \, \mathrm{LU}(2, A; qA) E_{1,2}^{-1}$$

and

$$E_{2,1}^{\#}(a) = E_{1,2} \, E_{2,1}(a) E_{1,2}^{-1}, \text{ for } a \in A.$$

From the unit property 4.3(1), there is a unit u in A, such that $u^2 \neq 1$. Since A satisfies $\mathsf{Conj}(\mathsf{z})$ (and $E_{1,2}$ normalizes $\{E_{1,2}(*)\}$),

$$\text{it suffices to show } E_{2,1}\big({-(u^2 - 1)y}\big) \in \left\langle \mathrm{LU}^{\#} \right\rangle_{50}, \text{ for every } y \in \mathcal{M}_{qA}.$$

From 5.5(2) and 5.5(3), we see, for any unit v, that

$$H(v)^{-1} E_{2,1}^{\#}(*) H(v) = E_{1,2}(*) \, E_{2,1}^{\#}(*) \, E_{1,2}(*) \in \left\langle \mathrm{LU}^{\#} \right\rangle_3 .$$

Since $H(v)$ normalizes $\{E_{1,2}(*)\}$, this implies that

$$H(v)^{-1} \left\langle \mathrm{LU}^{\#} \right\rangle_j H(v) \subseteq \left\langle \mathrm{LU}^{\#} \right\rangle_{3j} \text{ for all } j. \tag{5.18}$$

Because $y \in \mathcal{M}_{qA}$, we have $y \in qA$, and there exist $z \equiv \pm 1 \bmod qA$ and units u_1 and u_2, such that $1 + yzu_1^2 = u_2^2$. By replacing y with $-y$ if necessary, let us assume $z \equiv 1 \bmod qA$. It is obvious that $u^2 - 1$ is a multiple of $1 + yzu_1^2$ (since everything is a multiple of any unit). In the notation of 5.5(4), with $y' = yu_1^2$ in the role of y, we have

$$M(y', z) \in \left\langle \mathrm{LU}^{\#} \right\rangle_2 \text{ and } E_{1,2}(c) M(y', z)^{-1} \in \left\langle \mathrm{LU}^{\#} \right\rangle_3,$$

so

$$E_{2,1}(-wy') \in \left\langle \mathrm{LU}^{\#} \right\rangle_{2+3\times 3} = \left\langle \mathrm{LU}^{\#} \right\rangle_{11}.$$

Since

$$-wy' = -\frac{(u^2-1)yu_1^2}{1+yzu_1^2} = -\frac{(u^2-1)yu_1^2}{u_2^2},$$

conjugating by $H(u_2/u_1)$ yields the conclusion that

$$\begin{aligned} E_{2,1}\bigl(-(u^2-1)y\bigr) &= H(u_2/u_1)^{-1} E_{2,1}(-wy')\, H(u_2/u_1) \\ &\in \left\langle \mathrm{LU}^{\#} \right\rangle_{3\times 11} \subseteq \left\langle \mathrm{LU}^{\#} \right\rangle_{50}, \end{aligned}$$

as desired. $\square$

(5.19) **Corollary** [CKP, (3.3)]**.** *For each element T of $\mathrm{GL}(2,K)$, there is a nonzero ideal $\mathfrak{q}'$ of A, such that $T^{-1}\,\mathrm{LU}(2,\mathfrak{q}')\,T \subseteq \langle \mathrm{LU}(2,\mathfrak{q})\rangle_{(50\mathsf{z})^2}$.*

Proof. Any matrix in $\mathrm{GL}(2,K)$ is a product involving only diagonal matrices, the permutation matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and the elementary matrix $E_{1,2}$, with the elementary matrix appearing no more than twice. (This is a consequence of the "Bruhat decomposition.")

(1) For a diagonal matrix $T = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, we have

$$T^{-1}\,\mathrm{LU}(2, a^{-1}b\mathfrak{q} \cap b^{-1}a\mathfrak{q} \cap A)\,T \subseteq \mathrm{LU}(2,\mathfrak{q}).$$

(2) Conjugation by the permutation matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ interchanges $E_{1,2}(*)$ with $E_{2,1}(*)$, so $\mathrm{LU}(2,\mathfrak{q})$ is invariant.

(3) For $E_{1,2}$, see (5.17).

$\square$

Lemma 5.19 can be restated very cleanly in the terminology of nonstandard analysis:

(5.20) **Corollary** [CKP, (3.6)]**.** $\mathrm{GL}(2,K)$ *normalizes* $\mathrm{E}(2,\mathcal{Q})$*.*

Proof. For any $T \in \mathrm{GL}(2,K)$, Lemma 5.19 implies that

$$T^{-1}\,\mathrm{LU}(2,\mathcal{Q})\,T \subseteq \langle \mathrm{LU}(2, {}^*\mathfrak{q})\rangle_{(50\mathsf{z})^2}.$$

Since $\mathfrak{q}$ is an arbitrary ideal of A, we conclude, from polysaturation, that

$$T^{-1}\,\mathrm{LU}(2,\mathcal{Q})\,T \subseteq \langle \mathrm{LU}(2,\mathcal{Q})\rangle_{(50\mathsf{z})^2} \subseteq \mathrm{E}(2,\mathcal{Q}),$$

as desired. $\square$

Hence, the action of $\mathrm{GL}(2,K)$ on $\mathrm{SL}(2, {}^*\!A; \mathcal{Q})$ induces an action on the coset space $\mathrm{SL}(2, {}^*\!A; \mathcal{Q}) / \mathrm{E}(2,\mathcal{Q})$. It can be shown that this is a trivial action of $\mathrm{GL}(2,K)$ (see 5.25), but we now establish this only for $\mathrm{SL}(2,K)$.

(5.21) **Proposition** [CKP, (3.7)]**.** $[\mathrm{SL}(2,K), \mathrm{SL}(2, {}^*\!A; \mathcal{Q})] \subseteq \mathrm{E}(2,\mathcal{Q})$.

Proof. Let T be an arbitrary element of $\mathrm{SL}(2, {}^*\!A; \mathcal{Q})$. Applying (5.19), with ${}^*\!A$ in the role of A, yields a nonzero ideal $\mathcal{Q}' \subseteq \mathcal{Q}$, such that

$$T^{-1}\,\mathrm{E}(2, \mathcal{Q}')\,T \subseteq \mathrm{E}(2, \mathcal{Q}). \tag{5.22}$$

We may assume $\mathcal{Q}'$ is principal, by passing to a smaller ideal. We may write $T = XE$, with $X \in \mathrm{SL}(2, {}^*\!A; \mathcal{Q}')$ and $E \in \mathrm{E}(2, \mathcal{Q})$ (by Vaserstein's Lemma 1 (5.6) and the fact that $\mathrm{SL}(2, {}^*\!A; \mathcal{Q}) = \mathrm{SSL}(2, {}^*\!A; \mathcal{Q})$ (see 5.4)). Let u_0 be a unit in A satisfying the unit property 4.3(2) (with $\mathsf{r} = 1$), so there exist $E_1, \dots, E_{\mathsf{x}} \in \mathrm{LU}(2, \mathcal{Q}')$, such that

$$H(u_0)^{-1} X H(u_0) = E_1 X E_2 \cdots E_{\mathsf{x}} \in E_1 T\,\mathrm{E}(2, \mathcal{Q}) = T\,\mathrm{E}(2, \mathcal{Q}).$$

Then

$$H(u_0)^{-1} T H(u_0) = \big(H(u_0)^{-1} X H(u_0)\big)\big(H(u_0)^{-1} E H(u_0)\big) \in T\,\mathrm{E}(2, \mathcal{Q}).$$

Hence, $H(u_0)$ is in the kernel of the action on $\mathrm{SL}(2, {}^*\!A; \mathcal{Q})/\,\mathrm{E}(2, \mathcal{Q})$. Since $\mathrm{SL}(2, K)$ is the smallest normal subgroup of $\mathrm{GL}(2, K)$ containing $H(u_0)$, this implies that all of $\mathrm{SL}(2, K)$ is in the kernel. □

(5.23) **Corollary** [CKP, (3.10)]**.** *We have:*

(1) $\big[\mathrm{E}(2, A), \mathrm{SL}(2, A; \mathfrak{q})\big] \subseteq \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q})$.

(2) $\mathrm{E}^{\triangleleft}(2, A; \mathfrak{q})$ *is normal in* $\mathrm{SL}(2, A; \mathfrak{q})$.

Proof. (1) We have $\mathrm{SL}(2, {}^*\!A; {}^*\mathfrak{q}) = \mathrm{E}^{\triangleleft}(2, {}^*\!A; {}^*\mathfrak{q})\,\mathrm{SL}(2, {}^*\!A; \mathcal{Q})$ (see 2.15). For $T \in \mathrm{E}(2, A)$, we have

$$\begin{aligned}
[T, {}^*\,\mathrm{SL}(2, A; \mathfrak{q})] &\subseteq [\mathrm{E}(2, A), \mathrm{SL}(2, {}^*\!A; {}^*\mathfrak{q})] \\
&= [\mathrm{E}(2, A), \mathrm{E}^{\triangleleft}(2, {}^*\!A; {}^*\mathfrak{q})][\mathrm{E}(2, A), \mathrm{SL}(2, {}^*\!A; \mathcal{Q})] \\
&\subseteq \mathrm{E}^{\triangleleft}(2, {}^*\!A; {}^*\mathfrak{q})]\,\mathrm{E}(2, \mathcal{Q}) && \text{(by 5.21)} \\
&= \mathrm{E}^{\triangleleft}(2, {}^*\!A; {}^*\mathfrak{q}) \\
&\subseteq {}^*\mathrm{E}^{\triangleleft}(2, A; \mathfrak{q}).
\end{aligned}$$

By Leibniz' Principle, then $[T, \mathrm{SL}(2, A; \mathfrak{q})] \subseteq \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q})$. This completes the proof of the first half of the corollary.

(2) Since $\mathrm{E}^{\triangleleft}(2, A; \mathfrak{q}) \subseteq \mathrm{E}(2, A)$, part (1) implies

$$[\mathrm{E}^{\triangleleft}(2, A; \mathfrak{q}), \mathrm{SL}(2, A; \mathfrak{q})] \subseteq \mathrm{E}^{\triangleleft}(2, A; \mathfrak{q}),$$

so $\mathrm{E}^{\triangleleft}(2, A; \mathfrak{q})$ is normal. □

(5.24) **Corollary** [CKP, (3.11)]**.** *If y is a nonzero element of A, and $(a, b) \in W(\mathcal{Q})$, then*

$$\begin{bmatrix} by^2 \\ a \end{bmatrix}_{\mathcal{Q}} = \begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}}.$$

Proof. Because $\mathrm{E}(2, \mathcal{Q}) \subseteq \mathrm{E}^{\triangleleft}(2, {}^*\!A; \mathcal{Q})$, we see, from (5.21), that

$$[\mathrm{SL}(2, K), \mathrm{SL}(2, {}^*\!A; \mathcal{Q})] \subseteq \mathrm{E}^{\triangleleft}(2, {}^*\!A; \mathcal{Q}).$$

Therefore

$$\begin{aligned}
\begin{bmatrix} by^2 \\ a \end{bmatrix}_{\mathcal{Q}} &\equiv \begin{bmatrix} a & by^2 \\ * & * \end{bmatrix} = \begin{bmatrix} y & 0 \\ 0 & y^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ * & * \end{bmatrix} \begin{bmatrix} y^{-1} & 0 \\ 0 & y \end{bmatrix} \\
&\equiv \begin{bmatrix} a & b \\ * & * \end{bmatrix} \equiv \begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}} \bmod \mathrm{E}^{\triangleleft}(2, {}^*\!A; \mathcal{Q}).
\end{aligned}$$

□

Proof of Theorem 5.13. We have:
- $\big[\mathrm{E}(2,A), \mathrm{SL}(2,A;\mathfrak{q})\big] \subseteq \mathrm{E}^{\triangleleft}(2,A;\mathfrak{q})$ (see 5.23) and
- ${}^*\!\begin{bmatrix} by^2 \\ a \end{bmatrix}_{\mathfrak{q}} = {}^*\!\begin{bmatrix} b \\ a \end{bmatrix}_{\mathfrak{q}}$ for all $(a,b) \in W(\mathcal{Q})$ and all nonzero $y \in A$ (see 5.24),

so Proposition 5.7 implies that $\begin{bmatrix} \ \end{bmatrix}_{\mathfrak{q}}$ is a well-defined Mennicke symbol. Therefore, its range $\mathrm{SL}(2,A;\mathfrak{q}) / \mathrm{E}^{\triangleleft}(2,A;\mathfrak{q})$ is isomorphic to a quotient of the universal Mennicke group $C(\mathfrak{q})$, so the desired conclusion is immediate from Theorem 3.11. □

(5.25) **Remark** [CKP, (3.18)]**.** For $T = \begin{bmatrix} y^{-1} & 0 \\ 0 & 1 \end{bmatrix}$, the fact that $\begin{bmatrix} \ \end{bmatrix}_{\mathcal{Q}}$ is a Mennicke symbol (cf. proof of Theorem 5.13) implies

$$T^{-1}\begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}} T = \begin{bmatrix} by \\ a \end{bmatrix}_{\mathcal{Q}} = \begin{bmatrix} by(1-a) \\ a \end{bmatrix}_{\mathcal{Q}} = \begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}} \begin{bmatrix} y(1-a) \\ a \end{bmatrix}_{\mathcal{Q}}$$
$$= \begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}} \left(T^{-1} \begin{bmatrix} a-1 \\ a \end{bmatrix}_{\mathcal{Q}} T \right) = \begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}} (T^{-1}\, 1\, T) = \begin{bmatrix} b \\ a \end{bmatrix}_{\mathcal{Q}},$$

so T acts trivially on $\mathrm{SL}(2, {}^*\!A; \mathcal{Q}) / \mathrm{E}(2,\mathcal{Q})$. Combining this with (5.21) yields the conclusion that all of $\mathrm{GL}(2,K)$ acts trivially.

§5D. Bounded generation in $\mathrm{SL}(2, BS^{-1})$**.** We now deduce Theorem 1.2 under the assumption that $n = 2$. (See Theorem 3.13 for the case $n \geq 3$.)

(5.26) **Theorem** (cf. [CKP, (3.19)])**.** *Let:*
- *K be an algebraic number field,*
- *k be the degree of K over $\mathbb{Q}$,*
- *B be an order in K,*
- *S be a multiplicative subset of B, and*
- *$\mathfrak{q}$ be an ideal in BS^{-1}.*

If BS^{-1} has infinitely many units, then:
1. $\mathrm{LU}(2, BS^{-1})$ *boundedly generates* $\mathrm{E}(2, BS^{-1})$.
2. *The set* $\mathrm{LU}^{\triangleleft}(2, BS^{-1}; \mathfrak{q})$ *boundedly generates* $\mathrm{E}^{\triangleleft}(2, BS^{-1}; \mathfrak{q})$.

More precisely, there is a positive integer r, depending only on n and k, such that

$$\big\langle \mathrm{LU}(2, BS^{-1}) \big\rangle_r = \mathrm{E}(2, BS^{-1}) \text{ and } \big\langle \mathrm{LU}^{\triangleleft}(2, BS^{-1}) \big\rangle_r = \mathrm{E}^{\triangleleft}(2, BS^{-1}; \mathfrak{q}).$$

To establish the above result, note that Theorem 5.13 applies to the above situation (by 3.5, 3.9, 4.4, and 4.6), so the desired conclusion follows from the Compactness Theorem (see 2.8).

6. Bounded generation of normal subgroups

(6.1) **Theorem** (cf. [CKP, (2.7) and (3.21)])**.** *Let:*
- *n be a positive integer,*
- *K be an algebraic number field,*
- *k be the degree of K over $\mathbb{Q}$,*
- *B be an order in K, and*
- *S be a multiplicative subset of B.*

Assume that either $n \geq 3$ or BS^{-1} has infinitely many units.

(1) *If $\mathcal{X}^{\triangleleft}$ is any subset of* $\mathrm{SL}(n, BS^{-1})$, *such that* $g^{-1}\mathcal{X}^{\triangleleft}g = \mathcal{X}^{\triangleleft}$, *for every* $g \in \mathrm{E}(n, BS^{-1})$ (*and $\mathcal{X}^{\triangleleft}$ does not consist entirely of scalar matrices*), *then $\mathcal{X}^{\triangleleft}$ boundedly generates a finite-index subgroup of* $\mathrm{SL}(n, BS^{-1})$.

(2) *For any finite-index subgroup Γ of* $\mathrm{SL}(n, BS^{-1})$, *the set* $\mathrm{LU}(n, BS^{-1}) \cap \Gamma$ *of elementary matrices in Γ boundedly generates a subgroup of finite index in Γ.*

(6.2) **Remark.** In the situation of part (1) of the above theorem, we have $\langle \mathcal{X}^{\triangleleft} \rangle_r = \langle \mathcal{X}^{\triangleleft} \rangle$, for some r that depends on k, n, $\#(A/\mathfrak{q})$, and the minimal number of generators of $\mathfrak{q}$, where $\mathfrak{q} = \mathfrak{q}(\mathcal{X}^{\triangleleft})$ is a certain ideal defined in the statement of Proposition 6.7 below. (The minimal number of generators of $\mathfrak{q}$ is certainly finite, since BS^{-1} is Noetherian. In the situation of Theorem 6.1′ of the introduction, the minimal number of generators of $\mathfrak{q}(\mathcal{X}^{\triangleleft})$ is bounded by $n^2 \cdot \#\mathcal{X}$.)

(6.3) **Remark.** We will use the Compactness Theorem to establish Theorem 6.1, but a more straightforward proof can be obtained by applying nonstandard analysis. All of the cases are very similar, so let us describe only the proof of 6.1(1) when $n \geq 3$. There is some nonzero (principal) ideal $\mathfrak{q}'$ of ${}^*BS^{-1}$, such that $\langle {}^*\mathcal{X}^{\triangleleft} \rangle$ contains $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q}')$ (see Theorem 6.4 below). From Theorem 3.12, we know that $\mathrm{SL}(n, {}^*A; \mathfrak{q}') / \mathrm{E}^{\triangleleft}(n, {}^*A; \mathfrak{q}')$ is finite. Furthermore, since $\mathrm{SL}(n, A) / \mathrm{SL}(n, A; \mathfrak{q})$ is finite, for every nonzero ideal $\mathfrak{q}$ of A, Leibniz' Principle implies that $\mathrm{SL}(n, {}^*A) / \mathrm{SL}(n, {}^*A; \mathfrak{q}')$ is $*$-finite. Therefore, the coset space $\mathrm{SL}(n, {}^*A) / \mathrm{E}^{\triangleleft}(n, {}^*A; \mathfrak{q}')$ is $*$-finite, which means there is a $*$-finite set Ω, such that $\mathrm{E}^{\triangleleft}(n, {}^*A; \mathfrak{q}')\Omega = \mathrm{SL}(n, {}^*A)$. Then

$$^*\langle \mathcal{X}^{\triangleleft} \rangle \subseteq \mathrm{SL}(n, {}^*A) = \mathrm{E}^{\triangleleft}(n, {}^*A; \mathfrak{q}')\Omega \subseteq \langle {}^*\mathcal{X}^{\triangleleft} \rangle\, \Omega,$$

so the desired bounded generation follows from $(4 \Rightarrow 1)$ of Proposition 2.29.

§6A. Part 1 of Theorem 6.1. When $n \geq 3$, the proof of 6.1(1) is based on the following description of normal subgroups of $\mathrm{SL}(n, A)$.

(6.4) **Theorem** (Sandwich Condition [Ba1, Thm. 4.2e], [HOM, 4.2.9, p. 155])**.** *Suppose:*

- *A is a commutative ring that satisfies the stable range condition* SR_2,
- *$n \geq 3$, and*
- *N is a subgroup of* $\mathrm{SL}(n, A)$ *that is normalized by* $\mathrm{E}(n, A)$.

Then there is an ideal $\mathfrak{q}$ of A, such that:

(1) *N contains* $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$.

(2) *Each element of N is congruent to a scalar matrix, modulo $\mathfrak{q}$.*

As a replacement for the Sandwich Condition when $n = 2$, we have the following elementary observation, essentially due to Serre.

(6.5) **Lemma** ([CoK, Lem. 1.3], cf. [Se, pp. 492–493])**.** *Suppose:*

- *A is a commutative ring,*
- *N is a subgroup of* $\mathrm{SL}(2, A)$ *that is normalized by* $\mathrm{E}(2, A)$,
- $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *is any element of N, and*
- *u is a unit in A, such that* $u^2 \equiv 1 \bmod cA$.

Then $\mathrm{E}^{\triangleleft}\big(2, A; (u^4 - 1)A\big) \subseteq N$.

Now 6.1(1) is obtained by applying the Compactness Theorem (see 2.8) to the following proposition.

(6.6) **Definition.** The *level ideal* of a subset $\mathcal{X}$ of $\mathrm{SL}(n,A)$ is the smallest ideal $\mathfrak{q}$ of $\mathrm{SL}(n,A)$, such that the image of $\mathcal{X}$ in $\mathrm{SL}(n,A;\mathfrak{q})$ consists entirely of scalar matrices.

(6.7) **Proposition.** *Suppose:*

- $\mathsf{j}, \mathsf{m}, \mathsf{r}, \ell, \mathsf{r}, \mathsf{z}$ *are positive integers.*
- *A is an integral domain satisfying* $\mathsf{SR}_{1\frac{1}{2}}$, $\mathsf{Gen}(2,1)$, $\mathsf{Gen}(2\mathsf{t},\mathsf{r})$, *and* $\mathsf{Exp}(2\mathsf{t},\ell)$.
- *$\mathcal{X}^{\triangleleft}$ is any (nonempty) subset of* $\mathrm{SL}(n,A)$, *such that* $g^{-1}\mathcal{X}^{\triangleleft}g = \mathcal{X}^{\triangleleft}$, *for every* $g \in \mathrm{E}(n,A)$ *(and X does not consist entirely of scalar matrices).*
- *If $n \geq 3$, then:*
  - $\mathfrak{q}$ *is the level ideal of* $\mathcal{X}^{\triangleleft}$.
  - *There is a* j*-element subset* $\mathcal{X}_0$ *of* $\mathcal{X}^{\triangleleft}$, *such that* $\mathfrak{q}$ *is the level ideal of* $\mathcal{X}_0$.
- *If $n = 2$, then:*
  - *A satisfies* $\mathsf{Unit}(\mathsf{r},\mathsf{x})$ *and* $\mathsf{Conj}(\mathsf{z})$.
  - $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{X}^{\triangleleft}$.
  - *u is a unit in A, such that* $u^2 \equiv 1 \bmod cA$.
  - $\mathfrak{q} = (u^4 - 1)A$.
- $\#(A/\mathfrak{q}) \leq \mathsf{m}$.

Then $\mathcal{X}^{\triangleleft}$ generates a finite-index subgroup of $\mathrm{SL}(n,A)$.

Proof. Since $\langle \mathcal{X}^{\triangleleft} \rangle$ is obviously normalized by $\mathrm{E}(n,A)$, we know, from (6.4) or (6.5), that $\langle \mathcal{X}^{\triangleleft} \rangle$ contains $\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q})$. Thus,

$$\#\frac{\mathrm{SL}(n,A)}{\langle \mathcal{X}^{\triangleleft} \rangle} \leq \#\frac{\mathrm{SL}(n,A)}{\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q})} \leq \#\mathrm{SL}(n,A/\mathfrak{q}) \cdot \#\frac{\mathrm{SL}(n,A;\mathfrak{q})}{\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q})} < \infty,$$

by (3.12) or (5.13). □

§6B. Part 2 of Theorem 6.1. In preparation for the proof of 6.1(2), we establish some preliminary results. (We need only the corollary that follows.) The following theorem is only a special case of a result that is valid for all Chevalley groups, not only $\mathrm{SL}(n,A)$.

(6.8) **Theorem** (Tits [Ti, Prop. 2]). *If $n \geq 3$ and $\mathfrak{q}$ is any ideal of any commutative ring A, then* $\mathrm{E}^{\triangleleft}(n,A;\mathfrak{q}^2) \subseteq \mathrm{E}(n,\mathfrak{q})$.

See Definition 5.3 for the definition of $\mathrm{SSL}(2,A;\mathfrak{q})$.

(6.9) **Lemma** [CKP, (3.8) and (3.20)]. *Suppose:*

- *A is as in the statement of Theorem* 5.13, *and*
- $\mathfrak{q}$ *is a nonzero ideal in A.*

Then:

(1) $\mathrm{E}(2,\mathfrak{q})$ *is a normal subgroup of* $\mathrm{SSL}(2,A;\mathfrak{q})$.

(2) *If $A/\mathfrak{q}^2$ is finite, then* $\mathrm{E}(2,\mathfrak{q})$ *contains* $\mathrm{E}^{\triangleleft}(2,A;\mathfrak{q}')$, *for some nonzero ideal* $\mathfrak{q}'$.

Proof. We use nonstandard analysis. (See Notation 5.2 for the definition of the ideal $\mathcal{Q}$.)

(1) Let $T \in \mathrm{SSL}(2,A;\mathfrak{q})$ and $E_1 \in \mathrm{LU}(2,\mathfrak{q})$. By Vaserstein's Lemma 1 (5.6), we may write $T = XE$ with $X \in \mathrm{SSL}(2,{}^*\!A;\mathcal{Q})$ and $E \in \mathrm{E}(2,{}^*\mathfrak{q})$. Then

$$[T,E_1] = [XE,E_1] = E^{-1}[X,E_1]E_1^{-1}EE_1.$$

It is obvious that $E_1, E \in \mathrm{E}(2, {}^*\mathfrak{q})$, and, by (5.21), we have

$$[X, E_1] \in \mathrm{E}(2, \mathcal{Q}) \subseteq \mathrm{E}(2, {}^*\mathfrak{q}).$$

Hence

$$[T, E_1] \in \mathrm{E}(2, {}^*\mathfrak{q}) \subseteq {}^*\mathrm{E}(2, \mathfrak{q}).$$

By Leibniz' Principle, $[T, E_1] \in \mathrm{E}(2, \mathfrak{q})$.

(2) Let $w_1, \ldots, w_r$ be coset representatives for $\mathrm{SL}(2, A; \mathfrak{q}^2)$ in $\mathrm{SL}(2, A)$. For each i, we have $\mathrm{LU}(2, q_i A) \subseteq w_i^{-1}\,\mathrm{E}(2, \mathfrak{q}) w_i$, for some nonzero q_i (see 5.19), so

$$H = \bigcap_{i=1}^{r} \left(w_i^{-1}\,\mathrm{E}(2, \mathfrak{q}) w_i \right) \text{ contains } \mathrm{LU}(2, q_1 q_2 \cdots q_r A).$$

From (1) (and because $\mathrm{SL}(2, A; \mathfrak{q}^2) \subseteq \mathrm{SSL}(2, A; \mathfrak{q})$), we see that H is the intersection of all of the conjugates of $\mathrm{E}(2, \mathfrak{q})$, so H is normal. Therefore H contains $\mathrm{E}^{\triangleleft}(2, A; q_1 q_2 \cdots q_r A)$. □

(6.10) **Corollary.** *Assume the situation of Theorem* 6.1*. If $\mathfrak{q}$ is any nonzero ideal of BS^{-1}, then there exist a nonzero ideal $\mathfrak{q}'$ of BS^{-1} and a positive integer r, such that* $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}') \subseteq \langle \mathrm{LU}(n, \mathfrak{q}) \rangle_r$.

Proof (sketch)**.** We apply a compactness argument to Lemma 6.9(2) (if $n = 2$) or Theorem 6.8 (if $n \geq 3$). These results show (under appropriate hypotheses) that there is an ideal $\mathfrak{q}'$ of A, such that

$$\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q}') \subseteq \mathrm{E}(n, \mathfrak{q}) = \langle \mathrm{LU}(n, \mathfrak{q}) \rangle .$$

By bounded generation of $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q}')$ and $\mathrm{E}(n, A)$ (cf. 3.13 and 5.26), there is some positive integer r_0, such that

$$\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q}') = \left\langle \bigcup_{E \in \langle \mathrm{LU}(n, A) \rangle_{r_0}} E^{-1}\,\mathrm{LU}(n, \mathfrak{q}') E \right\rangle_{r_0} .$$

Thus, the desired result is a consequence of the Compactness Theorem (2.7). □

Proof of Theorem 6.1(2). Because Γ has finite index, there is some nonzero ideal $\mathfrak{q}$ of BS^{-1}, such that $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}) \subset \Gamma$. From Theorem 5.13 (if $n = 2$) or Theorem 3.12 (if $n \geq 3$), and the fact that $\mathrm{SL}(n, BS^{-1}) / \mathrm{SL}(n, BS^{-1}; \mathfrak{q})$ is finite, we see that

(6.11) $\quad \mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q})$ is a subgroup of finite index in $\mathrm{SL}(n, BS^{-1})$.

Thus, we may assume $\Gamma = \mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q})$, so

$$\mathrm{LU}(n, BS^{-1}) \cap \Gamma = \mathrm{LU}(n, \mathfrak{q}).$$

We have $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}') \subseteq \langle \mathrm{LU}(n, \mathfrak{q}) \rangle_r$, for some nonzero ideal $\mathfrak{q}'$ of BS^{-1} and some positive integer r (see 6.10). Since $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}')$ has finite index in $\mathrm{SL}(n, BS^{-1})$ (see 6.11), this implies $\langle \mathrm{LU}(n, \mathfrak{q}) \rangle = \langle \mathrm{LU}(n, \mathfrak{q}) \rangle_{r'}$, for some positive integer r'. □

For $n \geq 3$, the bounded generation of normal subgroups also remains valid when the group $\mathrm{SL}(n, BS^{-1})$ is replaced by a subgroup of finite index (see 6.13).

(6.12) **Theorem** (Bak [Bak, Cor. 1.2])**.** *Let:*

- $n \geq 3$,
- *A be a commutative ring satisfying the stable range condition* SR_2,

- $\mathfrak{q}$ *be a nonzero ideal of* A*, and*
- N *be a noncentral subgroup of* $\mathrm{SL}(n, A)$.

If N *is normalized by* $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q})$*, then* N *contains* $\mathrm{E}^{\triangleleft}(n, A; \mathfrak{q}')$*, for some nonzero ideal* $\mathfrak{q}'$ *of* A*.*

(6.13) **Corollary.** *Let:*

- $n \geq 3$*,*
- K*,* k*,* B*, and* S *be as in Theorem* 6.1*,*
- Γ *be any subgroup of finite index in* $\mathrm{SL}(n, BS^{-1})$*, and*
- $\mathcal{X}^{\triangleleft}$ *be is any subset of* Γ*, such that* $g^{-1}\mathcal{X}^{\triangleleft}g = \mathcal{X}^{\triangleleft}$*, for every* $g \in \Gamma$ *(and* $\mathcal{X}^{\triangleleft}$ *does not consist entirely of scalar matrices).*

Then $\mathcal{X}^{\triangleleft}$ *boundedly generates a finite-index subgroup of* Γ*.*

Proof. Applying a compactness argument (as in the proof of Corollary 6.10) to the theorem yields the conclusion that there exist a nonzero ideal $\mathfrak{q}'$ of BS^{-1} and a positive integer r, such that $\mathrm{E}^{\triangleleft}(n, BS^{-1}; \mathfrak{q}') \subseteq \langle \mathcal{X}^{\triangleleft} \rangle_r$. The proof is completed by arguing as in the final paragraph of the proof of Theorem 6.1(2), with $\mathcal{X}^{\triangleleft}$ in the place of $\mathrm{LU}(n, \mathfrak{q})$. □

References

[AM] Adian, S. I.; Mennicke, J. On bounded generation of $\mathrm{SL}_n(\mathbb{Z})$. *Internat. J. Algebra Comput.* **2** (1992), no. 4, 357–365. MR1189668 (93m:20064), Zbl 0794.20061.

[Bak] Bak, Anthony. Subgroups of the general linear group normalized by relative elementary groups. *Algebraic K-Theory, Part*II (Oberwolfach, 1980), 1–22, Lecture Notes in Math., 967, *Springer, New York*, 1982. MR0689387 (84f:20049), Zbl 0536.20030.

[Bar] Bardakov, V. G. On the decomposition of automorphisms of free modules into simple factors. *Izv. Ross. Akad. Nauk Ser. Mat.* **59** (1995), no. 2, 109–128; translation in *Izv. Math.* **59** (1995) 333–351. MR1337161 (96f:20067), Zbl 0896.20031.

[Ba1] Bass, H. K-theory and stable algebra. *Inst. Hautes Études Sci. Publ. Math.* **22** (1964) 5–60. MR0174604 (30 #4805), Zbl 0248.18025.

[Ba2] Bass, Hyman. Algebraic K-theory. *Benjamin, New York*, 1968. MR0249491 (40 #2736), Zbl 0174.30302.

[BMS] Bass, H.; Milnor, John W.; Serre, Jean-Pierre Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* **33** (1967) 59–137. MR0244257 (39 #5574), Zbl 0174.05203.

[CK1] Carter, David; Keller, Gordon. Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$ *Amer. J. Math.* **105** (1983) 673–687. MR0704220 (85f:11083), Zbl 0525.20029.

[CK2] Carter, David; Keller, Gordon. Elementary expressions for unimodular matrices. *Comm. Algebra* **12** (1984) 379–389. MR0737253 (86a:11023), Zbl 0572.20030.

[CKP] Carter, David; Keller, Gordon; Paige, Eugene. Bounded expressions in $\mathrm{SL}(n, A)$. Unpublished.

[CW] Cooke, George; Weinberger, Peter J. On the construction of division chains in algebraic number rings, with applications to SL_2. *Comm. Algebra* **3** (1975) 481–524. MR0387251 (52 #8094), Zbl 0315.12001.

[CoK] Costa, Douglas L.; Keller, Gordon E. On the normal subgroups of $\mathrm{SL}(2, A)$. *J. Pure Appl. Algebra* **53** (1988) 201–226. MR0961360 (89h:20069), Zbl 0654.20051.

[DV] Dennis, R. K.; Vaserstein, L. N. On a question of M. Newman on the number of commutators. *J. Algebra* **118** (1988) 150–161. MR0961333 (89k:20062), Zbl 0649.20048.

[ER1] Erovenko, Igor V.; Rapinchuk, Andrei S. Bounded generation of some S-arithmetic orthogonal groups. *C. R. Acad. Sci. Paris Sér. I Math.* **333** (2001), no. 5, 395–398. MR1859225 (2002g:20083), Zbl 1010.20033.

[ER2] Erovenko, Igor V.; Rapinchuk, Andrei S. Bounded generation of S-arithmetic subgroups of isotropic orthogonal groups over number fields. Preprint, 2005.

[GS] GRUNEWALD, FRITZ J.; SCHWERMER, JOACHIM. Free nonabelian quotients of SL_2 over orders of imaginary quadratic numberfields. *J. Algebra* **69** (1981) 298–304. MR0617080 (82i:10027), Zbl 0461.20026.

[HOM] HAHN, ALEXANDER J.; O'MEARA, O. TIMOTHY. The classical groups and K-theory. With a foreword by J. Dieudonné. Grundlehren der Mathematischen Wissenschaften, 291. *Springer, New York*, 1989. MR1007302 (90i:20002), Zbl 0683.20033.

[Li] LIEHL, BERNHARD. Beschränkte Wortlänge in SL_2. *Math. Z.* **186** (1984) 509–524. MR0744962 (86b:11034), Zbl 0523.20028.

[LM] LOUKANIDIS, D.; MURTY, V. K. *Bounded generation for* SL_n $(n \geq 2)$ *and* Sp_n $(n \geq 1)$. Preprint.

[Mu] MURTY, V. KUMAR. Bounded and finite generation of arithmetic groups. *Number theory* (Halifax, NS, 1994), 249–261, CMS Conf. Proc., 15, *Amer. Math. Soc., Providence, RI*, 1995. MR1353937 (96g:11039), Zbl 0851.11026.

[Os] OSTMANN, HANS-HEINRICH. Additive Zahlentheorie. 2. Spezielle Zahlenmengen. Ergebnisse der Mathematik und ihrer Grenzgebiete, 11. *Springer, Berlin*, 1956. MR0268112 (42 #3011), Zbl 0072.03102.

[Ra] RAPINCHUK, A. S. The congruence subgroup problem for arithmetic groups of bounded generation (Russian). *Dokl. Akad. Nauk SSSR* **314** (1990) 1327–1331; translation in *Soviet Math. Dokl.* **42** (1991), no. 2, 664–668. MR1088588 (92b:20053).

[Se] SERRE, JEAN-PIERRE. Le problème des groupes de congruence pour SL_2. *Ann. of Math.* (2) **92** (1970) 489–527. MR0272790 (42 #7671).

[Sh] SHALOM, YEHUDA. Bounded generation and Kazhdan's property (T). *Inst. Hautes Études Sci. Publ. Math.* **90** (1999) 145–168. MR1813225 (2001m:22030), Zbl 0980.22017.

[SS] SIVATSKI, A. S.; STEPANOV, A. V. On the word length of commutators in $\mathrm{GL}_n(R)$. *K-Theory* **17** (1999) 295–302. MR1706109 (2001b:20081), Zbl 0935.20037.

[SV] STEPANOV, ALEXEI; VAVILOV, NIKOLAI. Decomposition of transvections: a theme with variations. *K-Theory* **19** (2000) 109–153. MR1740757 (2000m:20076), Zbl 0944.20031.

[SL] STROYAN, K. D.; LUXEMBURG, W. A. J. Introduction to the theory of infinitesimals. Pure and Applied Mathematics, No. 72. *Academic Press, New York*, 1976. MR0491163 (58 #10429), Zbl 0336.26002.

[Ta1] TAVGEN', O. I. Bounded generation of Chevalley groups over rings of algebraic S-integers (Russian). *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), no. 1, 97–122, 221–222; translation in *Math. USSR-Izv.* **36** (1991), no. 1, 101–128. MR1044049 (91e:20036), Zbl 0709.20024.

[Ta2] TAVGEN', O. I. Finite width of arithmetic subgroups of Chevalley groups of rank ≥ 2 (Russian). *Dokl. Akad. Nauk SSSR* **310** (1990), no. 4, 802–806; translation in *Soviet Math. Dokl.* **41** (1990), no. 1, 136–140. MR1047534 (91h:11029), Zbl 0716.20026.

[Ti] TITS, JACQUES. Systèmes générateurs de groupes de congruence. *C. R. Acad. Sci. Paris, Sér. A* **283** (1976) 693–695. MR0424966 (54 #12924), Zbl 0408.20028.

[vdK] VAN DER KALLEN, WILBERD. $\mathrm{SL}_3\big(\mathbb{C}[X]\big)$ does not have bounded word length. *Algebraic K-Theory, Part* I (Oberwolfach, 1980), 357–361, Lecture Notes in Math., 966, *Springer, New York*, 1982. MR0689383 (84b:20037), Zbl 0935.20501.

[Va] VASERŠTEĬN, L. N. On the group SL_2 over Dedekind rings of arithmetic type (Russian). *Mat. Sb.* (N.S.) **89(131)** (1972), 313–322, 351; translation in *Math. USSR Sb.* **18** (1972), 321–332. MR0435293 (55 #8253), Zbl 0359.20027.

[Za] ZAKIR'YANOV, K. KH. Symplectic groups over rings of algebraic integers have finite width over the elementary matrices. *Algebra i Logika* **24** (1985) 667–673, 748; translation in *Algebra Logic* **24** (1985) 436-440. MR0853775 (87j:20077), Zbl 0603.20043.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE, LETHBRIDGE, ALBERTA T1K 3M4, CANADA
Dave.Morris@uleth.ca http://people.uleth.ca/˜dave.morris/

This paper is available via http://nyjm.albany.edu/j/2007/13-17.html.