ON THE GENERATORS OF ELEMENTARY SUBGROUPS OF GENERAL LINEAR GROUPS

by A. W. MASON

(Received 24 March, 1993)

Introduction. Let R be a ring with identity and let $E_{ij} \in M_n(R)$ be the usual $n \times n$ matrix units, where $n \geq 2$ and $1 \leq i, j \leq N$. Let $E_n(R)$ be the subgroup of $GL_n(R)$ generated by all $T_{ij}(r) = I_n + rE_{ij}$, where $r \in R$ and $i \neq j$. For each (two-sided) R-ideal $\mathfrak{q}$ let $E_n(R, \mathfrak{q})$ be the *normal* subgroup of $E_n(R)$ generated by $T_{ij}(q)$, where $q \in \mathfrak{q}$. The subgroup $E_n(R, \mathfrak{q})$ plays an important role in the theory of $GL_n(R)$. For example, Vaseršteĭn has proved that, for a larger class of rings $\mathscr{C}$ (which includes *all* commutative rings), every subgroup S of $GL_n(R)$, when $R \in \mathscr{C}$ and $n \geq 3$, contains the subgroup $E_n(R, \mathfrak{q}_0)$, where $\mathfrak{q}_0$ is the R-ideal generated by α_{ij}, $r\alpha_{ii} - \alpha_{jj}r$ $(i \neq j,\ r \in R)$, for all $(\alpha_{ij}) \in S$. (See [**13**, Theorem 1].) In addition Vaseršteĭn has shown that, for the same class of rings, $E_n(R, \mathfrak{q})$ has a simple set of generators when $n \geq 3$. Let $\hat{E}_n(R, \mathfrak{q})$ be the subgroup of $E_n(R, \mathfrak{q})$ generated by $T_{ij}(r)T_{ji}(q)T_{ij}(-r)$, where $r \in R$, $q \in \mathfrak{q}$. Then $\hat{E}_n(R, \mathfrak{q}) = E_n(R, \mathfrak{q})$, for all $\mathfrak{q}$, when $R \in \mathscr{C}$ and $n \geq 3$. (See [**13**, Lemma 8].)

In this paper we are concerned with the question: how are $\hat{E}_2(R, \mathfrak{q})$ and $E_2(R, \mathfrak{q})$ related? It is already known that Vaseršteĭn's result does not in general extend to $n = 2$. The author [**9**, Example 2.6] has shown that $\hat{E}_2(\mathbb{Z}, \mathfrak{q})$ is of infinite index in $E_2(\mathbb{Z}, \mathfrak{q})$, for all but finitely many $\mathbb{Z}$-ideals $\mathfrak{q}$, where $\mathbb{Z}$ is the ring of rational integers. On the other hand Menal and Vaseršteĭn [**10**, Theorem 5(a)] have proved that $\hat{E}_2(L, \mathfrak{q}) = E_2(L, \mathfrak{q})$, for all $\mathfrak{q}$, where L is a (possibly non-commutative) SR_2-ring. (We recall [**1**, p. 231] that an *SR_t-ring*, where $t \geq 2$, is one which satisfies Bass's "t-th stable range" condition. By [**1**, (3.5) Theorem, p. 239] fields and semi-local rings, for example, are SR_2-rings.) Menal and Vaseršteĭn's result however does not extend to SR_3-rings since every Dedekind ring (for example, $\mathbb{Z}$) is an SR_3-ring, again by [**1**, (3.5), Theorem, p. 239].

This paper elaborates on these results. It would appear that, unless R has "sufficiently many" units, $\hat{E}_2(R, \mathfrak{q})$ is likely to be of infinite index in $E_2(R, \mathfrak{q})$. For our first principal result, let O $(= O(d))$ be the ring of integers of $\mathbb{Q}(\sqrt{-d})$, where $\mathbb{Q}$ is the set of rational numbers and d is a positive integer. For each positive integer m, let O_m be the order of index m in O. (By definition, $O = O_1$.)

THEOREM A. *Suppose that* $(d, m) \neq (1,1), (2,1), (3,1), (3,2), (7,1), (11,1)$. *Then, for all but finitely many* $\mathfrak{q}$,

$$\hat{E}_2(O_m, \mathfrak{q}) \textit{ is of infinite index in } E_2(O_m, \mathfrak{q}).$$

Our proof is based on results of Cohn [**3**] and Fine [**5**].

For our second principal result let D be a k-ring with a degree function, where k is a field, as defined by Cohn [**3**, p. 21]. (The simplest examples of such rings are the polynomial rings in any number of indeterminates over k.)

THEOREM B. *Let* $\mathfrak{q}$ *be a proper D-ideal.*
(i) *If* $\dim_k (D/\mathfrak{q}) = 1$, *then*

$$\hat{E}_2(D, \mathfrak{q}) = E_2(D, \mathfrak{q}).$$

(ii) *Otherwise*,

$$\hat{E}_2(D, \mathfrak{q}) \textit{ is a non-normal subgroup of infinite index in } E_2(D, \mathfrak{q}).$$

Our proof is based on another result of Cohn [**3**].

Menal and Vaseršteın's result [**10**, Theorem 5(a)] does extend to other rings, including some SR_3-rings, provided the rings have "many" units. For example, when A is a Dedekind ring of arithmetic type with infinitely many units, it follows easily from a result of Liehl [**7**] that $\hat{E}_2(A, \mathfrak{q}) = E_2(A, \mathfrak{q})$, for all $\mathfrak{q}$. (The simplest examples of such rings are $\mathbb{Z}[1/p]$, where p is a prime, and $k[t, t^{-1}]$ is the Laurent polynomial ring over a *finite* field, k.

We conclude by determining precisely when $\hat{E}_2(\mathbb{Z}, \mathfrak{q}) = E_2(\mathbb{Z}, \mathfrak{q})$, which completes the results contained in [**9**, Example 2.6].

1. Orders in imaginary quadratic number fields. We begin by simplifying some of our notation.

We denote the set of units in a ring R by R^*. For each $r \in R$, $\alpha \in R^*$, we put

$$S(r) = T_{21}(r), \qquad T(r) = T_{12}(r), \qquad D(\alpha) = \mathrm{diag}(\alpha, \alpha^{-1}).$$

For each $x, y \in R$ we put

$$ST(x, y) = S(x)T(y)S(-x) \quad \text{and} \quad TS(x, y) = T(x)S(y)T(-x).$$

Then $\hat{E}_2(R, \mathfrak{q})$ is generated by $ST(r, q)$ and $TS(r, q)$, where $r \in R$ and $q \in \mathfrak{q}$.

Let d, O and O_m be as above. We may assume that d is square-free. Let

$$\omega = \begin{cases} \sqrt{-d}, & d \equiv 1, 2 \pmod 4, \\ (1 + \sqrt{-d})/2, & d \equiv 3 \pmod 4). \end{cases}$$

It is well-known that

$$O_m = \mathbb{Z} + \omega_m \mathbb{Z},$$

where $\omega_m = m\omega$. It follows that every non-zero O_m-ideal $\mathfrak{q}$ is a $\mathbb{Z}$-module of rank 2 and consequently is of finite index in O_m. We require a "canonical" set of $\mathbb{Z}$-generators for such a $\mathfrak{q}$.

LEMMA 1.1. *Let $\mathfrak{q}$ be a non-zero O_m-ideal. Then there exist unique $\alpha, \beta, \gamma \in \mathbb{Z}$ with the following properties*:

(i) $\mathfrak{q} = (\alpha\omega_m + \beta)\mathbb{Z} + \gamma\mathbb{Z}$;
(ii) $\alpha > 0$ *and* $0 \leq \beta < \gamma$;
(iii) $\alpha \mid \beta$ *and* $\alpha \mid \gamma$;
(iv) $|O_m : \mathfrak{q}| = \alpha\gamma$.

Proof. From the above $\mathfrak{q}$ has $\mathbb{Z}$-generators of the form

$$\omega_1 = \alpha'\omega_m + \beta' \quad \text{and} \quad \omega_2 = \alpha''\omega_m + \beta'',$$

where $\alpha', \beta', \alpha'', \beta'' \in \mathbb{Z}$, $(\alpha', \alpha'') \neq (0, 0)$ and $(\beta', \beta'') \neq (0, 0)$.

We now replace ω_1, ω_2 with ω_1', ω_2' where

$$\begin{bmatrix}\omega_1'\\ \omega_2'\end{bmatrix} = A\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix},$$

and $A \in GL_2(\mathbb{Z})$. In this way we can assume $\alpha'' = 0$, $\alpha', \beta'' > 0$ and $0 \leqslant \beta' < \beta''$. Let $\alpha' = \alpha$, $\beta'' = \gamma$ and $\beta' = \beta$.

Now $\gamma\omega_m \in \mathfrak{q}$ and so $\alpha \mid \beta$ and $\alpha \mid \gamma$, The uniqueness of the α, β, γ follows, for example, from the fact that γ is the smallest positive integer in $\mathfrak{q}$. Part (iv) is obvious. □

NOTATION. We put

$$\mathfrak{q} = (\alpha, \beta^*, \gamma^*),$$

where $\beta = \alpha\beta^*$ and $\gamma = \alpha\gamma^*$. (Then $0 \leqslant \beta^* < \gamma^*$.)

The principal result of this section depends upon Cohn's theory of GL_2 over *discretely normed rings.* (See [**3**, § 5].)

To simplify our notation let

$$U = T(\omega_m), \qquad T = T(1), \qquad A = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, \qquad J = -I_2.$$

LEMMA 1.2. *Suppose* $(d, m) \neq (1,1), (2,1), (3,1), (3,2), (7,1), (11,1)$.

(i) $E_2(O_m) = \langle U, T, A : A^2 = (AT)^3 = J,\ J^2 = I_2,\ UT = TU,\ J \text{ central}\rangle$.

(ii) $E_2(O_m) = SL_2(\mathbb{Z}) *_C B$,

the amalgamated product of

$$SL_2(\mathbb{Z}) = \langle A; T : A^2 = (AT)^3 = J, J^2 = I_2, J \text{ central}\rangle,$$

and

$$B = \langle J, U, T : UT = TU, J^2 = I_2, J \text{ central}\rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^2,$$

over

$$C = SL_2(\mathbb{Z}) \cap B = \langle J, T : J^2 = I_2, JT = TJ\rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}.$$

Proof. Cohn [**3**, p. 16] has defined a *discretely normed ring* and Dennis [**4**, Theorem 3] has proved O_m is discretely normed precisely when (d, m) satisfies the above restrictions.

By virtue of [**5**, Theorem (5.2)] $E_2(O_m)$ has a presentation of the type described in [**3**, Theorem (2.2)]. Using an approach similar to that of Fine in [**5**, Theorem 4.8.1, p. 120] this presentation simplifies to that in (i) above.

Part (ii) follows immediately. (See also [**5**, Theorem 4.8.2 (1), p. 120].) □

NOTATION. Let $\mathfrak{q} = (\alpha, \beta^*, \gamma^*)$ as above. We put

$$E_2(O_m, \mathfrak{q}) = E_2(\alpha, \beta^*, \gamma^*).$$

It is clear that $E_2(\alpha, \beta^*, \gamma^*)$ is the normal subgroup of $E_2(O_m)$ generated by

$$U^\alpha T^{\alpha\beta^*} \quad \text{and} \quad T^{\alpha\gamma^*}.$$

https://doi.org/10.1017/S0017089500031189 Published online by Cambridge University Press

LEMMA 1.3. (i) *$E_2(\alpha, 0, 1)$ is of infinite index in $E_2(O_m)$, when $\alpha \geq 6$.*
(ii) *$E_2(1, \beta^*, \gamma^*)$ is of infinite index in $E_2(O_m)$, when $\gamma^* \geq 6$.*

Proof. (*i*) Let N be the normal subgroup of $E_2(O_m)$ generated by J and U and let $G = E_2(O_m)/N$. Then, by Lemma 1.2(i),

$$G = \langle a, t\colon a^2 = t^3 = 1\rangle \cong PSL_2(\mathbb{Z}),$$

where a (resp. t) is the image of A (resp. T) in G.

Now let M be the image of $E_2(\alpha, 0, 1)$ in G. Then G/M has a presentation of the form

$$G/M = \langle x, y\colon x^2 = y^2 = (xy)^\alpha\rangle,$$

which is one of the classical triangle groups. It is a classical result that this group is infinite when $\alpha \geq 6$. Part (i) follows.

For part (ii) we repeat the argument with N the normal subgroup of $E_2(O_m)$ generated by J and UT^{β^*}. □

COROLLARY 1.4. *When $\alpha \geq 6$ or $\gamma^* \geq 6$, $E_2(\alpha, \beta^*, \gamma^*)$ is of infinite index in $E_2(O_m)$.*

Proof. Follows from Lemma 1.3 since $E_2(\alpha, \beta^*, \gamma^*) \leq E_2(\alpha, 0, 1) \cap E_2(1, \beta^*, \gamma^*)$. □

We require one more lemma before our first principal result.

LEMMA 1.5. *For all ideals $\mathfrak{q}$, $\hat{E}_2(O_m, \mathfrak{q})$ is finitely generated.*

Proof. We may assume that $\mathfrak{q} \neq \{0\}$. Then from the above $O_m/\mathfrak{q}$ is finite and $\mathfrak{q}$ is a $\mathbb{Z}$-module of rank 2. Let $\{a_1, \ldots, a_S\}$ be a set of coset representatives of O_m (mod $\mathfrak{q}$) and let ω_1, ω_2 be a $\mathbb{Z}$-basis of $\mathfrak{q}$. Then $\hat{E}_2(O_m, \mathfrak{q})$ is generated by

$$ST(a_i, \omega_j) \quad \text{and} \quad TS(a_i, \omega_j),$$

where $1 \leq i \leq s$ and $j = 1, 2$. □

THEOREM 1.6. *For all but finitely many O_m-ideals $\mathfrak{q}$, $\hat{E}_2(O_m, \mathfrak{q})$ is of infinite index in $E_2(O_m, \mathfrak{q})$.*

Proof. We may assume that $\mathfrak{q} \neq \{0\}$. Let $\mathfrak{q} = (\alpha, \beta^*, \gamma^*)$ as above. By Lemma 1.5 it suffices to prove that $E_2(\alpha, \beta^*, \gamma^*)$ is infinitely generated when $\alpha \geq 6$ or $\gamma^* \geq 6$.

With the notation of Lemma 1.2(ii) we note that

$$|C\colon C \cap E_2(\alpha, \beta^*, \gamma^*)| < \infty,$$

since $T^{\alpha\gamma^*} \in E_2(\alpha, \beta^*, \gamma^*)$. Suppose that $E_2(\alpha, \beta^*, \gamma^*)$ is finitely generated, where $\alpha \geq 6$ or $\gamma^* \geq 6$. Then, combining Lemma 1.2(ii) with a result of Karrass and Solitar [**6**, Theorem 10], we conclude that

$$|E_2(O_m)\colon E_2(\alpha, \beta^*, \gamma^*)| < \infty,$$

which contradicts Corollary 1.4. The result follows. □

NOTES. (i) Theorem 1.6 is best possible in the sense that there are ideals $\mathfrak{q}$ for which $\hat{E}_2(O_m, \mathfrak{q}) = E_2(O_m, \mathfrak{q})$. (Trivially, $\hat{E}_2(O_m, \{0\}) = E_2(O_m, \{0\}) = \{I_2\}$ and $\hat{E}_2(O_m, O_m) = E_2(O_m, O_m) = E_2(O_m)$.)

(ii) By Lemma 1.1 it follows, for example, that Theorem 1.6 holds for all non-zero $\mathfrak{q}$ where $|O_m : \mathfrak{q}| > 125$.

(iii) The results for $\hat{E}_2(\mathbb{Z}, \mathfrak{q})$ are very similar to the above and will be described in detail in the last section.

2. k-rings with a degree function. Throughout this section D denotes a (commutative) k-ring with a degree function as defined by Cohn [**3**; p. 21], in which case $D^* = k^*$, where k is a field. Examples of such D include

(i) polynomial rings in any number of indeterminates over k,

(ii) the coordinate ring $C = C(\mathscr{C}, P, k)$ of the affine curve obtained by removing a closed point P from a projective curve $\mathscr{C}$ over k. (The simplest example of type (ii) is the polynomial ring $k[t]$.)

We begin with a "positive" result.

THEOREM 2.1. *Let* $\mathfrak{q}$ *be a* D*-ideal such that* $\dim_k (D/\mathfrak{q}) \leq 1$. *Then*

$$\hat{E}_2(D, \mathfrak{q}) = E_2(D, \mathfrak{q}) = E_2(D) \cap SL_2(D, \mathfrak{q}).$$

Proof. Since $\hat{E}_2(D, D) = E_2(D, D) = E_2(D)$ we may assume that $\dim_k(D/\mathfrak{q}) = 1$, i.e. $D/\mathfrak{q} \cong k$.

Let $X \in E_2(D) \cap SL_2(D, \mathfrak{q})$. Then

$$X = T(x_1)S(y_1) \ldots T(x_n)S(y_n),$$

where $x_1, y_1, \ldots, x_n, y_n \in D$. Now

$$x_i = q_i + \alpha_i \quad \text{and} \quad y_i = \hat{q}_i + \beta_i,$$

for some $q_i, \hat{q}_i \in \mathfrak{q}$ and $\alpha_i, \beta_i \in k$, where $1 \leq i \leq n$. It is clear that X can be written in the form $X = X_1 X_2$, where (i) X_1 is a product of matrices of the type $YT(q)Y^{-1}$, with $Y \in SL_2(k)$ and $q \in \mathfrak{q}$, and (ii) $X_2 \in SL_2(k)$. (Note that $AT(x)A^{-1} = S(-x)$.) Clearly $X_1 \in SL_2(D, \mathfrak{q})$. Hence $X_2 \in SL_2(D, \mathfrak{q})$ and so $X_2 = I_2$. It suffices therefore to prove that

$$YT(q)Y^{-1} \in \hat{E}_2(D, \mathfrak{q}).$$

Let

$$Y = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

There are two possibilities.

(a) $\alpha \neq 0$: In this case

$$Y = S(\alpha^*)D(\alpha)T(\beta^*),$$

where $\alpha^* = \gamma\alpha^{-1}$ and $\beta^* = \beta\alpha^{-1}$, in which case

$$YT(q)Y^{-1} = ST(\alpha^*, \alpha^2 q).$$

(b) $\alpha = 0$: In this case

$$YT(q)Y^{-1} = S(-\gamma^2 q).$$

The result follows. □

For the simplest case, namely $D = k[t]$, Theorem 2.1 says that

$$\hat{E}_2(k[t], \mathfrak{q}) = E_2(k[t], \mathfrak{q})$$

where $\mathfrak{q} = R$ or $(t - \alpha)R$, for some $\alpha \in k$ $(R = k[t])$.

The situation when $\dim_k(D/\mathfrak{q}) > 1$ is completely different. We require another result [**3**] of Cohn.

Definition. Let R be a ring. For each $r \in R$ we put

$$E(r) = \begin{bmatrix} r & 1 \\ -1 & 0 \end{bmatrix}.$$

Let $r, s \in R$ and $\alpha \in R^*$. The following identities are easily verified

$$E(r)E(0)E(s) = -E(r+s),$$

$$E(r)D(\alpha) = D(\alpha^{-1})E(r\alpha^2),$$

$$E(r)E(\alpha^{-1})E(s) = E(r-\alpha)D(\alpha^{-1})E(s-\alpha).$$

Now each element X of $E_2(D)$ is by definition a product of matrices of the type $S(r)$ and $T(S)$ and, since $S(r) = -E(0)E(r)$ and $T(s) = -E(-s)E(0)$, X is then a product of matrices of the type $E(r)$. If such an $E(r)$, where $r \in D^* \cup \{0\}$, occurs in this product the above identities can be used to reduce its "length". Cohn's result says that after all such eliminations we are left with a unique *standard form* for X.

Lemma 2.2. *Let $X \in E_2(D)$. Then X can be written uniquely in the following standard form*

$$X = D(\alpha)E(a_1)\ldots E(a_n),$$

where $\alpha \in k^*$ and $a_1, \ldots, a_n \in D$ such that

(i) *$a_i \notin k$, where $1 < i < n$, when $n > 2$ or*
(ii) *$(a_1, a_2) \neq (0,0)$, when $n = 2$.*

Proof. See [**3**, Theorem (7.1)]. □

Theorem 2.3. *Let $\mathfrak{q}$ be a non-zero D ideal, where $\dim_k(D/\mathfrak{q}) > 1$. Then $\hat{E}_2(D, \mathfrak{q})$ is a non-normal subgroup of infinite index in $E_2(D, \mathfrak{q})$.*

Proof. Choose $x \in D$, where $x \notin \mathfrak{q} \oplus k$ and let $Y = S(x)T(x)$. Let $q \in \mathfrak{q}$, with $q \neq 0$. It suffices to prove that for each positive integer n

$$Y^n S(q) Y^{-n} \notin \hat{E}_2(D, \mathfrak{q}).$$

By means of the above identities it is clear that the standard form (Lemma 2.2) of $Y_nS(q)Y^{-n}$ is

$$D(-1)E(0)E(x)E(-x)\ldots E(x)E(-x)E(q)E(x)E(-x)\ldots E(x)E(-x) \qquad (1)$$

(There are $2n+2$ terms in this product.)

Suppose that $Z = Y^nS(q)Y^{-n}$ belongs to $\hat{E}_2(D, \mathfrak{q})$. Then

$$Z = Y_1 \ldots Y_S,$$

where $Y_i = ST(a_i, q_i)$ or $TS(a_i, q_i)$ for some $a_i \notin \mathfrak{q}$ and $q_i \in \mathfrak{q}$ $(1 \leqslant i \leqslant s)$, where $s \geqslant 1$. It is clear that $s > 1$. We note that

$$ST(a_i, q_i) = E(0)E(a_i)E(-q_i)(E(-a_i)$$

and

$$TS(a_i, q_i) = E(-a_i)(E(q_i)E(a_i)E(0).$$

From the above identities it follows that

$$X(r, s_1)X(r, s_2) = X(r, s_1 + s_2),$$

where $X = ST$ or TS. We may therefore assume that if $Y_i = X(a_i, \tau_i)$ and $Y_{i+1} = X(a_{i+1}, q_{i+1})$, where $X = ST$ or TS, and $1 \leqslant i < s$, then $a_i \neq a_{i+1}$. In addition, from the standard form of Z, we conclude that at least one $a_i \notin \mathfrak{q} \cup k$ (otherwise $Z \in E_2(\mathfrak{q} \oplus k)$). Assume from now on that j is the largest integer with this property.

We now write Z as a product of matrices of the type $E(x)$. Then

$$Z = \pm E(a) \ldots E(\pm a_j)E(\mp q_j)E(\mp a_j)Y_0,$$

where $Y_0 \in E_2(\mathfrak{q} \oplus k)$ and Y_0 or $-E(0)Y_0 \in SL_2(D, \mathfrak{q})$. Reducing this to standard form and comparing its last terms with those of (1) we conclude by Lemma 2.2 that $Y_0 = E(q_0)$ or $-E(0)E(q_0)$, for some $q_0 \in \mathfrak{q}$ and hence that

$$E(x)E(-x) = E(\mp q_j + \lambda)E(\mp a_j + q_0),$$

for some $\lambda \in k$. Again by Lemma 2.2 it follows that $x = \mp q_j + \lambda$ which contradicts the fact that $x \notin \mathfrak{q} \oplus k$. $\square$

3. Dedekind rings of arithmetic type. Throughout this section A denotes a *Dedekind ring of arithmetic type* [**2**, p. 83]. By a classical theorem of Dirichlet it is known that A^* is finite if and only if $A = \mathbb{Z}$, $A = O = O(d)$, for some d, or $A = C(\mathscr{C}, P, k)$, for some finite k. The preceding results (together with these of the last section) show that for most A of this type the subgroup $\hat{E}_2(A, \mathfrak{q})$ is nearly always of infinite index in $E_2(A, \mathfrak{q})$.

When A^* is infinite however the situation is completely different.

THEOREM 3.1. *Let A be as above and suppose that A^* is infinite. Then, for all A-ideals $\mathfrak{q}$, $\hat{E}_2(A, \mathfrak{q}) = E_2(A, \mathfrak{q})$.*

Proof. Let $X \in E_2(A, \mathfrak{q})$. Liehl [**7**, (20), p. 164] has proved that

$$X = S(a_1)T(q_1) \ldots S(a_n)T(q_n),$$

for some $a_1, \dots, a_n \in A$ and $q_1, \dots, q_n \in \mathfrak{q}$. Then

$$X = ST(a_1^*, q_1) \dots ST(a_n^*, q_n)S(a_n^*),$$

where

$$a_i^* = a_1 + \dots + a_i \qquad (1 \leq i \leq n).$$

Now $X \equiv I_2 \pmod{\mathfrak{q}}$ and so $a_n^* \in \mathfrak{q}$. Hence $X \in \hat{E}_2(A, \mathfrak{q})$. $\square$

4. The modular group. We conclude by determining precisely when $\hat{E}_2(\mathbb{Z}, \mathfrak{q}) = E_2(\mathbb{Z}, \mathfrak{q})$. This completes the results contained in [**9**, Example 2.6]. Now $\mathfrak{q} = m\mathbb{Z}$, for some $m \geq 0$. We may assume that $m > 0$.

LEMMA 4.1. *$\hat{E}_2(\mathbb{Z}, m\mathbb{Z})$ is (finitely) generated by $ST(a, m)$ and $TS(a, m)$, where $0 \leq a \leq m-1$*

Proof. Obvious. $\square$

LEMMA 4.2. (i) *When $3 \leq m \leq 5$, $E_2(\mathbb{Z}, m\mathbb{Z})$ is a free group of rank*

$$1 + \frac{\mu}{12},$$

where $\mu = |SL_2(\mathbb{Z}) : SL(\mathbb{Z}, m\mathbb{Z})|$.

(ii) *When $m \geq 6$, $E_2(\mathbb{Z}, m\mathbb{Z})$ is a free group of infinite rank.*

Proof. We denote the embedding of a subgroup S of $SL_2(\mathbb{Z})$ in $PSL_2(\mathbb{Z})$ by PS. Now, for all $m \geq 3$,

$$E_2(\mathbb{Z}, m\mathbb{Z}) \cong PE_2(\mathbb{Z}, m\mathbb{Z}),$$

and, by [**11**, Theorem VIII.6, p. 143], $PE_2(\mathbb{Z}, m\mathbb{Z})$ is a free group.

When $1 \leq m \leq 5$ it is well-known that

$$PE_2(Z, mZ) = PSL_2(\mathbb{Z}, m\mathbb{Z}).$$

(See, for example, [**12**, Theorem (i)].) It is known [**11**, Theorem VIII.7, p. 144] that the rank of $E_2(\mathbb{Z}, m\mathbb{Z})$ is

$$1 + \frac{\rho}{6},$$

where $\rho = |PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}, m\mathbb{Z})\|$ with $1 \leq m \leq 5$. Part (i) follows.

For part (ii) it is well-known that, when $m \geq 6$, $PE_2(\mathbb{Z}, m\mathbb{Z})$ is of infinite index in $PSL_2(\mathbb{Z})$. (See, for example, [**12**, Theorem (ii)].) Now $PSL_2(\mathbb{Z})$ is a (non-trivial) free product. (See, for example, [**11**, Theorem VIII.1, p. 139].) Part (ii) follows from [**6**, Theorem 10]. $\square$

We now come to our final result.

THEOREM 4.3. (i) *$\hat{E}_2(\mathbb{Z}, m\mathbb{Z}) = E_2(\mathbb{Z}, m\mathbb{Z})$, when $1 \leq m \leq 4$.*

(ii) *When $m \geq 5$, $\hat{E}_2(\mathbb{Z}, m\mathbb{Z})$ is a non-normal subgroup of infinite index in $E_2(\mathbb{Z}, m\mathbb{Z})$.*

Proof. Suppose first that $m \geq 6$. By Lemmas 4.1 and 4.2(ii) $\hat{E}_2(\mathbb{Z}, m\mathbb{Z})$ is a finitely generated subgroup of $E_2(\mathbb{Z}, m\mathbb{Z})$, a free group of infinite rank. Hence $\hat{E}_2(\mathbb{Z}, m\mathbb{Z})$ is of infinite index in $E_2(\mathbb{Z}, m\mathbb{Z})$ and is consequently non-normal in $E_2(\mathbb{Z}, m\mathbb{Z})$ by [**8**, Proposition 3.11, p. 17].

By Lemma 4.2(i) and [**11**, Theorem VII.15, p. 115] $E_2(\mathbb{Z}, 5\mathbb{Z})$ is free of rank 11. By Lemma 4.1, $\hat{E}_2(\mathbb{Z}, 5\mathbb{Z})$ is free of rank r, where $r \leqslant 10$. Hence $\hat{E}_2(\mathbb{Z}, 5\mathbb{Z})$ is of infinite index in $E_2(\mathbb{Z}, 5\mathbb{Z})$ by [**8**, Proposition 3.9, p. 16]. Again by [**8**, Proposition 3.11, p. 17] and Lemma 4.1, $\hat{E}_2(\mathbb{Z}, 5\mathbb{Z})$ is non-normal in $E_2(\mathbb{Z}, 5\mathbb{Z})$. Part (ii) follows.

For part (i) we treat the cases $m = 2, 3, 4$, separately. (The case $m = 1$ is trivial.)

The case $m = 2$: $E_2(\mathbb{Z}, 2\mathbb{Z})$ is generated by $-I_2$, $S(2)$ and $T(2)$. (See, for example, [**12**, p. 149].) Now

$$-I_2 = T(2)S(-2)(TS(1,2))^{-1}$$

and so

$$\hat{E}_2(\mathbb{Z}, 2\mathbb{Z}) = E_2(\mathbb{Z}, 2\mathbb{Z}).$$

The case $m = 3$: It is known [**12**, p. 149] that $E_2(\mathbb{Z}, 3\mathbb{Z})$ is generated by $T(3)$, $P^{-1}T(3)P$, $P^{-2}T(3)P^2$, where

$$P = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

Now $P^{-1}T(3)P = TS(-1, -3)$ and $P^{-2}T(3)P^2 = ST(-1, -3)$ and so

$$\hat{E}_2(\mathbb{Z}, 3\mathbb{Z}) = E_2(\mathbb{Z}, 3\mathbb{Z}).$$

The case $m = 4$: By [**11**, Exercises and problems, p. 137] a complete set of right coset representatives for $SL_2(\mathbb{Z}, 2\mathbb{Z})$ (modulo $SL_2(\mathbb{Z}, 4\mathbb{Z})$) is

$$\pm I_2, \qquad \pm T(2), \qquad \pm S(2) \quad \text{and} \quad \pm T(2)S(2).$$

From the above $SL_2(\mathbb{Z}, 2\mathbb{Z}) = E_2(\mathbb{Z}, 2\mathbb{Z})$ is generated by $-I_2$, $S(2)$ and $T(2)$ and so by a Reidemeister–Schreier type argument $SL_2(\mathbb{Z}, 4\mathbb{Z}) = E_2(\mathbb{Z}, 4\mathbb{Z})$ is generated by

$$S(4), \qquad TS(2,4), \qquad T(4), \qquad S(2)T(2)S(-2)T(-2) \quad \text{and} \quad T(2)S(2)T(2)S(-2).$$

From the above $[TS(1,2)]^2 = T(2)S(-2)T(2)S(-2)$ and so

$$T(2)S(2)T(2)S(-2) = TS(2,4)[TS(1,2)]^2.$$

In addition

$$S(2)T(2)S(-2)T(-2)TS(2,4)[TS(1,2)]^2 = ST(2,4).$$

It follows that

$$\hat{E}_2(\mathbb{Z}, 4Z) = E_2(Z, 4Z). \quad \square$$

REFERENCES

1. H. Bass, *Algebraic K-theory* (Benjamin, 1968).

2. H. Bass, J. Milnor and J-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geqslant 3$) and Sp_{2n} ($n \geqslant 2$), *Publ. Math. Inst. Hautes Étud. Sci.* **33** (1967), 59–137.

3. P. M. Cohn, On the structure of the GL_2 of a ring, *Publ. Math. Inst. Hautes Étud. Sci.* **30** (1966), 5–53.

4. R. K. Dennis, The GE_2-property of discrete subrings of $\mathbb{C}$, *Proc. Amer. Math. Soc.* **50** (1975), 77–82.

5. B. Fine, *Algebraic Theory of the Bianchi groups* (Marcel Dekker, 1989).

6. A. Karrass and D. Solitar, The subgroups of a free product of two groups with an amalgamated subgroup, *Trans. Amer. Math. Soc.* **150** (1970), 227–255.

7. B. Liehl, On the groups SL_2 over orders of arithmetic type, *J. Reine Angew. Math.* **323** (1981), 153–171.

8. R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory* (Springer-Verlag, 1977).

9. A. W. Mason, Congruence hulls in SL_n, *J. Pure Appl. Algebra.* **89** (1993) 255–272.

10. P. Menal and L. N. Vaserštein, On the structure of GL_2 over stable range one rings, *J. Pure Appl. Algebra* **64** (1990), 149–162.

11. M. Newman, *Integral Matrices* (Academic Press, 1972).

12. R. A. Rankin, Subgroups of the modular group generated by parabolic elements of constant amplitude, *Acta Arith.* **18** (1971), 145–151.

13. L. N. Vaserštein, On the normal subgroups of GL_n over a ring, *Lecture Notes in Mathematics* **854** (Springer-Verlag, 1981), 456–465.

14. K. Wohlfahrt, An extension of F. Klein's level concept, *Illinois J. Math.* **8** (1964), 529–535.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland

e-mail: awm@MATHS.GLA.AC.UK.