Proceedings of the Edinburgh Mathematical Society (1987) 30, 341–349 ©

STANDARD SUBGROUPS OF $GL_2(A)$

by A. W. MASON

(Received 4th September 1985)

Introduction

Let R be a commutative ring and let $\mathbf{q}$ be an ideal in R. Let $E_n(R)$ be the subgroup of $GL_n(R)$ generated by the elementary matrices and let $E_n(\mathbf{q})$ be the normal subgroup of $E_n(R)$ generated by the $\mathbf{q}$-elementary matrices. The *order* of a subgroup S of $GL_n(R)$ is the ideal $\mathbf{q}_0$ in R generated by $x_{ij}, x_{ii}-x_{jj}$, where $(x_{ij})\in S$, with $1\leqq i, j\leqq n$ and $i\neq j$. The subgroup S is called a *standard* subgroup if $E_n(\mathbf{q}_0)\leqq S$. An *almost-normal* subgroup of $GL_n(R)$ is a non-normal subgroup which is normalized by $E_n(R)$.

It is known [1, Theorem 3.5, p. 239, Theorem 4.1(b), (c), p. 240] that if R is a Dedekind ring then the standard subgroups of $GL_n(R)$ are precisely those normalized by $E_n(R)$, where $n\geqq 3$. The restriction $n\geqq 3$ is necessary. It is known for example [6, 8] that, when $A=\mathbb{Z}$ or $K[x]$, where $\mathbb{Z}$ is the set of rational integers and K is a field, there are infinitely many normal, non-central subgroups of $SL_2(R)$ which contain $E_2(\mathbf{q})$ only when $\mathbf{q}=\mathbf{0}$. (By definition a subgroup has order $\mathbf{0}$ if and only if it is central.)

Using recent work of Liehl [4] we prove that if $R=A$, a Dedekind ring of arithmetic type with infinitely many units [2, p. 83], then every standard subgroup of $GL_2(A)$ is normalized by $E_2(A)$. We prove also that if the primes dividing 2 and the units of A satisfy some further conditions then every $E_2(A)$-normalized subgroup of $GL_2(A)$ is standard. (We provide examples to show that these conditions are necessary.) It follows for example that, when $A=\mathbb{Z}[\frac{1}{6}]$ or $\mathbb{Z}[\theta]$, where θ is a root of unity of order p^α, with p a prime greater than 3, a subgroup of $GL_2(A)$ is standard if and only if it is normalized by $E_2(A)$.

It seems natural to ask whether or not an $E_n(A)$-normalized subgroup of $GL_n(A)$ is a normal subgroup, especially when such a subgroup is standard. In this paper we provide examples of almost-normal subgroups of $GL_2(A)$, for various A. For a given R the existence of almost-normal subgroups of $GL_n(R)$ depends upon n. It is known [5, Corollary 4.2; 6] that almost-normal subgroups of $GL_n(\mathbb{Z})$ exist if and only if $n=2$. It is also known [5, Corollary 5.6] that, when $n\geqq 3$, almost-normal subgroups of $GL_n(\mathbb{Z}[i])$ exist if and only if n is even, where $i^2=-1$.

Liehl's results [4] do not apply to the case where A is a Dedekind ring of arithmetic type with only finitely many units and it appears that in this case the standard subgroups of $GL_2(A)$ have little in common with those normalized by $E_2(A)$. For example it is known [6] that there are infinitely many non-standard subgroups of $GL_2(\mathbb{Z})$ which are normalized by $E_2(\mathbb{Z})$. On the other hand it is clear from [11] that there are infinitely many standard subgroups of $GL_2(\mathbb{Z})$ (of order $\mathbf{q}=(6)$) which are not normalized by $E_2(\mathbb{Z})$.

Throughout this paper it will be assumed that A is a Dedekind ring of arithmetic type with infinitely many units. By the Dirichlet unit theorem this means that A has units of infinite order. For each prime ideal $\mathbf{p}$ in A we put $N(\mathbf{p}) = |A/\mathbf{p}|$.

For any ring R we let $U(R)$ denote its set of units and for each ideal $\mathbf{q}$ in R we put $GL_n(\mathbf{q}) = \mathrm{Ker}(GL_n(R) \to GL_n(R/\mathbf{q}))$ and $SL_n(\mathbf{q}) = GL_n(\mathbf{q}) \cap SL_n(R)$. We let $H_n(\mathbf{q})$ be the set of all matrices in $GL_n(R)$ which are scalar (mod $\mathbf{q}$). For each $r \in R$ and $u, v \in U(R)$ we put

$$T(r) = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad D(u, v) = \begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}.$$

To simplify the notation we put $G = GL_2(A)$, $\Gamma = SL_2(A)$, $\Gamma(\mathbf{q}) = SL_2(\mathbf{q})$, $\Delta(\mathbf{q}) = E_2(\mathbf{q})$, $H(\mathbf{q}) = H_2(\mathbf{q})$ and $G(\mathbf{q}) = GL_2(\mathbf{q})$, where $\mathbf{q}$ is an ideal in A. (By definition $\Gamma(A) = \Gamma$ and $G(A) = H(A) = G$.)

As usual if H, K are subgroups of a group L then $[H, K]$ is the subgroup of L generated by all the commutators $[h, k] = h^{-1}k^{-1}hk$, where $h \in H$ and $k \in K$.

1. Liehl's results

Bass, Milnor and Serre have shown that, for all $\mathbf{q}$ and for all $n \geqq 3$, $E_n(\mathbf{q})$ is a normal subgroup of $GL_n(A)$ and that the factor groups $C_n(\mathbf{q})$ and $C_m(\mathbf{q})$ are (naturally) isomorphic, for all $m \geqq n$, where $C_n(\mathbf{q}) = SL_n(\mathbf{q})/E_n(\mathbf{q})$. (See [**2**, Theorem 7.5(c), Theorem 11.1(b)].) (This is also true if A has only finitely many units.) Liehl [**4**] has proved the following.

Theorem 1.1. *Let* $\mathbf{q}$ *be any ideal in* A.

(i) $\Delta(\mathbf{q}) \lhd \Gamma(\mathbf{q})$.

(ii) *For each* $n \geqq 3$, *the map* $\phi_n : \Gamma(\mathbf{q})/\Delta(\mathbf{q}) \to C_n(\mathbf{q})$, *defined by*

$$\phi_n(g\Delta(\mathbf{q})) = \bar{g}E_n(\mathbf{q}) \qquad (g \in \Gamma(\mathbf{q})),$$

where $\bar{g} = g \oplus I_{n-2}$, *is an isomorphism.*

Proof. See [**4**, (20), (21)]. □

It follows that $\Gamma = \Delta(A)$, i.e. Γ is generated by elementary matrices, that $\Delta(\mathbf{q}) \lhd G$ and that $\Gamma(\mathbf{q})/\Delta(\mathbf{q})$ is a subgroup of the group of roots of unity in A. (A formula for $|\Gamma(\mathbf{q}) : \Delta(\mathbf{q})|$ is given on p. 166 of [**4**].) Moreover if A is *not* the ring of integers of a totally imaginary number field then $\Gamma(\mathbf{q}) = \Delta(\mathbf{q})$, for all $\mathbf{q}$, by [**4**, (19), (21)].

We now consider some immediate consequences of Liehl's results. If H is a group and m a positive integer we put $H^m = \langle h^m : h \in H \rangle$.

Theorem 1.2. *Let* $\mathbf{q}$ *be any ideal in* A.

(a) $[G, G(\mathbf{q})] \leqq \Delta(\mathbf{q})$.

(b) $[\Gamma, H(\mathbf{q})] \leqq \Delta(\mathbf{q})$.

(c) $[G, H(\mathbf{q})]^2 \leqq \Delta(\mathbf{q})$.

Proof. We note that $[G, H(\mathbf{q})] \leqq \Gamma(\mathbf{q})$. Let $g \in C$ and $k \in G(\mathbf{q})$. Then, with the above notation,

$$\phi_4([g,k]\Delta(\mathbf{q})) = g_0 E_4(\mathbf{q}),$$

where $g_0 = [g \oplus I_2, k \oplus I_2] = [g,k] \oplus I_2$. Now $g_0 \in [GL_4(A), GL_4(\mathbf{q})]$ and $[GL_4(A), GL_4(\mathbf{q})] = E_4(\mathbf{q})$ by [**2**, Theorem 11.1(a)]. Part (a) follows from Theorem 1.1.

Now let $x \in \Gamma$ and $y \in H(\mathbf{q})$. Then

$$\phi_4([x,y]\Delta(\mathbf{q})) = x_0 E_4(\mathbf{q}),$$

where $x_0 = [x,y] \oplus I_2 = [x \oplus I_2, y \oplus y]$. Clearly $x_0 \in [SL_4(A), H_4(\mathbf{q})]$ and $[SL_4(A), H_4(\mathbf{q})] = E_4(\mathbf{q})$ by [**1**, Theorem 4.1(b), p. 240] and [**2**, Corollary 4.3]. Part (b) follows from Theorem 1.1.

Finally, let $g \in G$ and $h \in H(\mathbf{q})$. Then by part (a) $[g,h]^2 \equiv [g,h^2] \pmod{\Delta(\mathbf{q})}$. Now by definition $h \equiv \alpha I_2 \pmod{\mathbf{q}}$, for some $\alpha \in A$, where $\alpha^2 \equiv \det h \pmod{\mathbf{q}}$. Thus $h^2 = h_1 g_1$, where $h_1 = u I_2$ and $g_1 \in \Gamma$ with $u = \det h$. Hence $[g,h^2] \equiv [g,g_1] \equiv 1 \pmod{\Delta(\mathbf{q})}$, by part (a). Part (c) follows. □

Corollary 1.3. *Every standard subgroup of G is normalized by* Γ.

Proof. Follows immediately from Theorem 1.2(b). □

As we shall see later the converse of Corollary 1.3 does not always hold. We now consider conditions under which the inequalities in Theorem 1.2(a),(b) become equalities.

Definition. A is said to have property (*) if it is equal to its ideal generated by $u^2 - 1$, where $u \in U(A)$.

Theorem 1.4. *Let A have property* (*).

(i) *If* $\mathbf{p}$ *is any prime ideal in A then* $N(\mathbf{p}) > 3$.

(ii) *If* $\mathbf{q}$ *is any ideal in A then*

$$[\Gamma, H(\mathbf{q})] = [G, G(\mathbf{q})] = \Delta(\mathbf{q}).$$

In particular ($\mathbf{q} = A$),

$$\Gamma' = G' = \Gamma.$$

Proof. For (i) if $N(\mathbf{p}) = 2$ or 3 then $u^2 - 1 \in \mathbf{p}$, for all $u \in U(A)$.

For (ii) it is sufficient to prove that $\Delta(\mathbf{q}) \leqq [\Gamma, \Delta(\mathbf{q})]$ by Theorem 1.2(a),(b). By (*) there exist $u_1, \ldots, u_t \in U(A)$ and $a_1, \ldots, a_t \in A$ such that

$$\sum_{i=1}^{t} (u_i^2 - 1) a_i = 1.$$

Now let $q \in \mathbf{q}$. Then

$$T(q) = \prod_{i=1}^{t} T(q(u_i^2 - 1)a_i) = \prod_{i=1}^{t} [D(u_i^{-1}, u_i), T(-qx_i)].$$

The result follows. □

Examples of A which have property (*) are not hard to find.

Theorem 1.5. *Let m be the order of the group of roots of unity in A. If $12|m$ or $p|m$, where p is a prime and $p \neq 2, 3$, then A has property (*).*

Proof. Let $\mathbf{q}^*$ be the ideal generated by $u^2 - 1$, where $u \in U(A)$ and let θ be a primitive pth root of unity, where p is an odd prime dividing m. Then $\theta \in A$ and $p \in \mathbf{q}^*$ since $(p) = (\theta^2 - 1)^{p-1}$ by [**12**, p. 173].

Now let $\psi = \theta^i$, where $1 \leq i \leq p-1$. Then $1 + \psi + \cdots + \psi^{p-1} = 0$ and, since p is odd, $u = 1 + \psi \in U(A)$. Since $(u^2 - 1) = (2 + \psi)$ it follows that

$$\sum_{i=1}^{p-1} \{2 + \theta^i\} = 2p - 3 \in \mathbf{q}^*.$$

Note that if $4|m$ then $i \in A$, where $i^2 = -1$, and so $2 \in \mathbf{q}^*$. The result follows. □

Examples of A which have property (*) include $A = \mathbb{Z}[\frac{1}{6}]$ and $A = \mathbb{Z}[\theta]$, where θ is a primitive mth root of unity and m is divisible by a prime greater than 3. (See [**12**, p. 269].) When θ is a primitive mth root of unity, where $m = 2^\alpha$ or 3^β, then $\mathbb{Z}[\theta]$ has a prime $\mathbf{p}$ with $N(\mathbf{p}) = 2$ or 3 and so does not have property (*) by Theorem 1.4(i). (See [**12**, p. 173].)

2. Standard subgroups

In this section we obtain a partial converse to Corollary 1.3. We require the following lemma.

Lemma 2.1. *Let L be a local ring with maximal ideal $\mathbf{m}$ and suppose that either $\frac{1}{2} \in L$ or $|L/\mathbf{m}| > 2$. Then the centre of $PSL_2(L)$ is trivial.*

Proof. Let $X \in SL_2(L)$ map into the centre of $PSL_2(L)$. Then there exist $\lambda, \mu \in U(L)$, with $\lambda^2 = \mu^2 = 1$, such that

$$XT(1) = \lambda T(1)X \tag{1}$$

and

$$XY = \mu YX, \tag{2}$$

where $Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Suppose first that $\frac{1}{2} \in L$. Then $\lambda, \mu = \pm 1$. If $\lambda = -1$ then $c = d = 0$. But $ad - bc = 1$. Hence $\lambda = 1$ and so $c = 0$ and $a = d$. From (2) we deduce that $b = 0$.

Suppose now that $2 \in \mathbf{m}$ and that $|L/\mathbf{m}| > 2$. From (1) we have $c + d = \lambda d$ and so $c(2d + c) = 0$. It follows that $c \in \mathbf{m}$ and hence that $a, d \in U(L)$.

From (2) we deduce that $a = \mu d$ and $b = -\mu c$. Hence $ac + bd = 0$. Now repeat the argument with $D(u, u^{-1})XD(u^{-1}, u)$, where $u \in U(L)$. We deduce that $ac + bdu^4 = 0$ and hence that $b(u^4 - 1) = 0$. The hypothesis $|L/\mathbf{m}| > 2$ ensures the existence of $u \in U(L)$ such that $u^2 - 1 \in U(L)$. For such a case $u^4 - 1 \in U(L)$ and so $b = 0$. Hence $c = 0$. Now repeat the argument with $T(-1)XT(1) = T(-1)D(a, d)T(1)$. It follows that $a = d$. □

Definition. A rational prime p is *unramified* in A if $p \notin U(A)$ and $(p) = \prod_{i=1}^{t} \mathbf{p}_i$, where $\mathbf{p}_1, \ldots, \mathbf{p}_t$ are distinct prime ideals.

Definition. The *level* of a subgroup of G is the largest ideal $\mathbf{q}$ such that $\Delta(\mathbf{q}) \leqq S$.

The level is well-defined since $\Delta(\mathbf{q}_1) \cdot \Delta(\mathbf{q}_2) = \Delta(\mathbf{q}_1 + \mathbf{q}_2)$, for all $\mathbf{q}_1, \mathbf{q}_2$. Clearly the order of a subgroup divides its level and they coincide if and only if the subgroup is standard.

Theorem 2.2. *Let A have property (*) and suppose that $2 \in U(A)$ or 2 is unramified in A. Then the standard subgroups of G are precisely those normalized by Γ.*

Proof. By Corollary 1.3 it is sufficient to prove that if N is a subgroup of G normalized by Γ then N is standard. By [**13**, Proposition 2, p. 492] the level $\mathbf{q}$ of N is *non-zero*. It is sufficient to prove that $N \leqq H(\mathbf{q})$.

We prove first that $M = [\Gamma, N] \cdot \Gamma(\mathbf{q})$ is contained in $\Theta(\mathbf{q})$, where $\Theta(\mathbf{q}) = \Gamma \cap H(\mathbf{q})$. Now $\Delta(\mathbf{q}) \leqq M$ and if $\Delta(\mathbf{q}') \leqq N$ then by Theorem 1.4(ii)

$$\Delta(\mathbf{q}') = [\Gamma, \Delta(\mathbf{q}')] \leqq [\Gamma, N][\Gamma, \Gamma(\mathbf{q})] \leqq N \cdot \Delta(\mathbf{q}) = N.$$

It follows that M has level $\mathbf{q}$. Now let $\mathbf{q} = \mathbf{q}_0\mathbf{q}_1$, where $\mathbf{q}_0 = \mathbf{p}^\alpha$, with $\mathbf{p}$ prime, and $\mathbf{q}_1$ is prime to $\mathbf{p}$.

Consider the subgroup $M_0 = [M \cap \Gamma(\mathbf{q}_1)] \cdot \Gamma(\mathbf{q}_0)$. Clearly $\Gamma(\mathbf{q}_0) \leqq M_0$. If $\Delta(\mathbf{q}') \leqq M_0$, where $\mathbf{q}'$ divides $\mathbf{q}_0$, then $\Gamma(\mathbf{q}') = \Delta(\mathbf{q}') \cdot \Gamma(\mathbf{q}_0)$ is also contained in M_0. (See [**1**, Corollary 9.3, p. 267].) Hence

$$\Gamma(\mathbf{q}'\mathbf{q}_1) = \Gamma(\mathbf{q}') \cap \Gamma(\mathbf{q}_1) \leqq M_0 \cap \Gamma(\mathbf{q}_1) = [M \cap \Gamma(\mathbf{q}_1)] \cdot \Gamma(\mathbf{q}) \leqq M.$$

It follows that $\mathbf{q}_0\mathbf{q}_1$ divides $\mathbf{q}'\mathbf{q}_1$ and hence that $\mathbf{q}' = \mathbf{q}_0$. We conclude that M_0 has level $\mathbf{q}_0$.

Let $L = A/\mathbf{q}_0$. Then L is a local ring and so $\Gamma/\Gamma(\mathbf{q}_0)$ is naturally isomorphic to $SL_2(L)$ and $M_0/\Gamma(\mathbf{q}_0)$ is mapped onto a normal subgroup $\bar{M}$, say, of $SL_2(L)$. (See [**1**, Corollary 9.3, p. 267].) Let $\mathbf{m}$ be the maximal ideal of L. Since A has property (*) and 2 is unramified it is clear by Theorem 1.4(i) that either ($\mathbf{m} = (2)$ and $|A/\mathbf{m}| > 2$) or ($\frac{1}{2} \in L$ and $|A/\mathbf{m}| > 3$). Suppose that $\bar{M}$ is a non-central subgroup of $SL_2(L)$. Then by [**3**, Satz 3] together with the proof of [**9**, Corollary 2.2] it follows that $\bar{M}$ contains $\mathrm{Ker}(SL_2(L) \to SL_2(L/\mathbf{r}))$, for some non-zero ideal $\mathbf{r}$ in L. It follows that M_0 contains $\Delta(\mathbf{q}_2)$ for some $\mathbf{q}_2$ dividing $\mathbf{q}_0$, where $\mathbf{q}_2 \neq \mathbf{q}_0$. This contradicts the maximality of $\mathbf{q}_0$. Hence $\bar{M}$ is central and so $M \cap \Gamma(\mathbf{q}_1) \leqq \Theta(\mathbf{q}_0)$.

Again by [1, Corollary 9.3, p. 267] we have $\Gamma=\Gamma(\mathbf{q}_0)\cdot\Gamma(\mathbf{q}_1)$ and so $M\cdot\Theta(\mathbf{q}_0)/\Theta(\mathbf{q}_0)$ is a central subgroup of $\Gamma/\Theta(\mathbf{q}_0)\cong PSL_2(L)$. We now apply Lemma 2.1 and conclude that $M\leqq\Theta(\mathbf{q}_0)$. By [10, Theorem 2.2(a)] it follows that

$$M\leqq\bigcap_{\mathbf{p}^\alpha\|\mathbf{q}}\Theta(\mathbf{p}^\alpha)=\Theta(\mathbf{q}).$$

Let $\bar{\Gamma}$ and $\bar{N}$ be the images of Γ and N, respectively, in $GL_2(A/\mathbf{q})$. By the above $[\bar{\Gamma},\bar{N}]$ is central and $\bar{\Gamma}=SL_2(A/\mathbf{q})$, since $A/\mathbf{q}$ is semi-local. By Theorem 1.4(ii) we have $\bar{\Gamma}=[\bar{\Gamma},\bar{\Gamma}]$ and so we may apply [1, Lemma 5.1, p. 245]. We conclude that $[\bar{\Gamma},\bar{N}]=1$. Since $\bar{N}$ is centralized by the elementary matrices it is central. Hence $N\leqq H(\mathbf{q})$. □

Theorem 2.2 applies for example to $A=\mathbb{Z}[\frac{1}{6}]$ or $\mathbb{Z}[\theta]$, where θ is a root of unity of order p^α, with p a prime greater than 3. (See [12, p. 174].)

Example 2.3. Our first example shows that Theorem 2.2 does not hold when $2\notin U(A)$ and 2 is not unramified. Suppose that 2 is divisible by $\mathbf{p}^2$, for some prime ideal $\mathbf{p}$ in A.

Now $2\mathbf{p}^2\leqq\mathbf{p}^4$ and so $\Gamma(\mathbf{p}^2)/\Gamma(\mathbf{p}^4)$ is an elementary 2-abelian group in which each element is uniquely representable by a matrix of the form

$$\begin{bmatrix}1+a & b\\ c & 1+a\end{bmatrix},$$

where $a,b,c\in\mathbf{p}^2/\mathbf{p}^4$. (See [10, Theorem 4.1].)

Let $\Lambda=\{k^2+\mathbf{p}^4:k\in\mathbf{p}\}$ and define a subgroup $N(\Lambda)$ of $\Gamma(\mathbf{p}^2)$, containing $\Gamma(\mathbf{p}^4)$, by

$$N(\Lambda)/\Gamma(\mathbf{p}^4)\cong\left\{\begin{bmatrix}1+a & b\\ c & 1+a\end{bmatrix}:a\in\mathbf{p}^2/\mathbf{p}^4,\ b,c\in\Lambda\right\}.$$

Then $N(\Lambda)$ is a well-defined, normal subgroup of Γ. (See [9, Theorem 2.4].) Moreover the order of $N(\Lambda)$ is $\mathbf{p}^2$ since $\mathbf{p}^2$ is principal $(\operatorname{mod}\mathbf{p}^4)$. ($A$ is a Dedekind ring.)

Suppose that $\Delta(\mathbf{p}^3)\leqq N(\Lambda)$ and let h be a generator of $\mathbf{p}^3$ $(\operatorname{mod}\mathbf{p}^4)$. Then there exists $k\in\mathbf{p}$ such that

$$k^2\equiv h(\operatorname{mod}\mathbf{p}^4).$$

Hence the level of $N(\Lambda)$ is $\mathbf{p}^4$ and so $N(\Lambda)$ is not standard.

Example 2.4. Our next example shows that Theorem 2.2 does not hold if A has not property (*) even if 2 is unramified. Suppose that A has a prime $\mathbf{p}$ with $N(\mathbf{p})=3$. (Consider for example $A=\mathbb{Z}[\theta]$, where θ has order 3^α with $\alpha>1$, [12, p. 174].)

By [1, Corollary 9.3, p. 267] we have $\Gamma/\Gamma(\mathbf{p})\cong SL_2(F_3)$, where $F_3=A/\mathbf{p}$ is the field of order 3. From the well-known structure of $SL_2(F_3)$ it is clear that, if $\Gamma_0=\Gamma(\mathbf{p})\cdot\Gamma'$, then Γ/Γ_0 is cyclic of order 3, "generated" by $T(1)$. Now let $u\in U(A)$ be of infinite order with

$u \equiv 1 \pmod{\mathbf{p}}$ and let

$$N = \langle D(u,1)T(x), \Gamma_0 \rangle,$$

where $x = 0, \pm 1$. It is easily verified that N is normalized by Γ.

Now $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})'$ and so Γ' and hence N has order A. (See for example [**13**, Lemme 13, p. 522].) It can also be shown that $M \cap \Gamma = \Gamma_0$ from which it follows that N has level $\mathbf{p}$. We conclude that N is not standard.

Anticipating the next section we note that N is not normal in G when $x = \pm 1$. This follows from the fact that $[D(-1,1), D(u,1)T(x)] = T(2x)$.

3. Almost-normal subgroups

Theorem 3.1. *Let A have a property* (*) *and suppose that $2 \in U(A)$ or 2 is unramified in A. If A is not the ring of integers of a totally imaginary number field then G has no almost-normal subgroups.*

Proof. Let N be a subgroup of G of order $\mathbf{q}$ which is normalized by Γ. Then N is standard by Theorem 2.2 and so $[G,N] \leqq \Gamma(\mathbf{q})$. But $\Gamma(\mathbf{q}) = \Delta(\mathbf{q})$ (see §1) and so $[G,N] \leqq N$. □

Theorem 3.1 applies for example to $A = \mathbb{Z}[\frac{1}{6}]$ or $\mathbb{Z}[\rho]$, where $\rho^2 - \rho - 1 = 0$. (By [**12**, p. 77] the ring of integers of the number field $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}[\rho]$. Clearly $\mathbb{Z}[\rho]$ has property (*) and 2 is unramified in $\mathbb{Z}[\rho]$ by [**12**, p. 171].)

Example 2.4 (for the cases $x = \pm 1$) is an almost-normal subgroup of G which is not standard. We now consider the existence of almost-normal subgroups which are standard.

Theorem 3.2. *Almost-normal, standard subgroups of order* $\mathbf{q}$ *exist if and only if* $[G, H(\mathbf{q})] \nleqq \Delta(\mathbf{q})$.

Proof. The proof is an adaptation of that of [7, Lemma 2]. The condition is clearly necessary. Suppose then that $[G, H(\mathbf{q})] \nleqq \Delta(\mathbf{q})$ and choose $x \in H(\mathbf{q})$ such that $[G, x] \nleqq \Delta(\mathbf{q})$. If $\det x$ is a root of unity replace x with xx_0, where $x_0 = uI_2$ and u is a unit of infinite order in A. We may assume therefore that $\det x$ has infinite order.

Let $S = \langle x, \Delta(\mathbf{q}) \rangle$. Then S is a standard subgroup and is therefore normalized by Γ by Corollary 1.3. Now $[G,S] \leqq \Gamma(\mathbf{q})$ and so by Theorem 1.2(a) we have

$$[g_1 g_2, s] \equiv [g_1, s][g_2, s] \pmod{\Delta(\mathbf{q})}$$

and

$$[g, s_1 s_2] \equiv [g, s_1][g, s_2] \pmod{\Delta(\mathbf{q})},$$

for all $g, g_1, g_2 \in G$ and $s, s_1, s_2 \in S$.

Suppose now that $S \lhd G$. Then $[G,S] \leqq S$ and so there exists $g_0 \in G$ and an integer $m \neq 0$ such that

$$[g_0, x] \equiv x^m (\text{mod}\, \Delta(\mathbf{q})).$$

But $[G,[G,S]] \leqq \Delta(\mathbf{q})$ by Theorem 1.2(a) and so

$$1 \equiv [g_0, x^m] \equiv [g_0, x]^m \equiv x^{m^2} \quad (\text{mod}\, \Delta(\mathbf{q})).$$

We conclude that S is not normal in G. □

Corollary 3.3. *If $|\Gamma(\mathbf{q}):\Delta(\mathbf{q})|$ is odd then G has no almost-normal subgroups of order* $\mathbf{q}$ *which are standard.*

Proof. We recall from §1 that $\Gamma(\mathbf{q})/\Delta(\mathbf{q})$ is a finite cyclic group. Let $M(\mathbf{q}) = [G, H(\mathbf{q})] \cdot \Delta(\mathbf{q})$. Clearly $M(\mathbf{q}) \leqq \Gamma(\mathbf{q})$. If G has a standard, almost-normal subgroup of order $\mathbf{q}$ then $M(\mathbf{q}) \neq \Delta(\mathbf{q})$ by Theorem 3.2. Hence $M(\mathbf{q})/\Delta(\mathbf{q})$ is cyclic of order 2 by Theorem 1.2(c). □

From the above it is clear that if N is an almost-normal subgroup of order $\mathbf{q}$ which is standard then $|\Gamma(\mathbf{q}) \cap N : \Delta(\mathbf{q})|$ must be even.

Example 3.4. For our last example let $A = \mathbb{Z}[\theta]$, where θ is a unit of order p^α, with p an odd prime. (We must have $\alpha > 1$ when $p = 3$ to ensure that $\mathbb{Z}[\theta]$ has infinitely many units.) We obtain an almost-normal, standard subgroup of G of order $\mathbf{q} = (4)$. In this case $|\Gamma(\mathbf{q}):\Delta(\mathbf{q})| = 2$ by the formula on p. 166 of [**4**].

For each $a \in A$ let $N(a)$ be the norm of a in A (usual definition [**12**, p. 184]). Then $N(a)$ is a non-negative integer, for all $a \in A$. Let ϕ be a primitive p-th root of unity. We use the Dirichlet theorem on primes in an arithmetic progression [**2**, (A.10), p. 83] to choose a prime element $\alpha \in A$ such that $\alpha \equiv 1 + 2\phi$ (mod $\mathbf{q}$). Then $N(\alpha) \equiv N(1+2\phi)$ (mod 4) and by [**12**, p. 185] we have $N(1+2\phi) = b^m$, where $m = p^{\alpha-1}$ and

$$b = \prod_{j=1}^{p-1} \{1 + 2\phi^j\}.$$

(In fact b is the norm of $1+2\phi$ in $\mathbb{Q}(\phi)$.) It follows that $N(\alpha) \equiv -1$ (mod 4).

Now $\alpha^2 \equiv 1$ (mod $\mathbf{q}$) and so we can choose $X \in \Theta(\mathbf{q}) = \Gamma \cap H(\mathbf{q})$ such that $X \equiv (1+2\phi)I_2$ (mod $\mathbf{q}$). (See [**10**, p. 332].) We consider the element $g = [D(-1,1), X]$ of $[G, H(\mathbf{q})]$. Clearly $g \in \Gamma(\mathbf{q})$ and under the natural isomorphism from $\Gamma(\mathbf{q})/\Delta(\mathbf{q})$ to $SL_3(\mathbf{q})/E_3(\mathbf{q})$ the element $g\Delta(\mathbf{q})$ is mapped to $\bar{g}E_3(\mathbf{q})$, where $\bar{g} = g \oplus 1$. (See Theorem 1.1(ii).) By [**5**, Theorem 4.6] and the formula following it $\bar{g} \notin E_3(\mathbf{q})$. Hence $g \notin \Delta(\mathbf{q})$ and so $[G, H(\mathbf{q})] \nleqq \Delta(\mathbf{q})$. By Theorem 3.2 therefore almost-normal, standard subgroups of order $\mathbf{q}$ exist.

By the proof of Theorem 3.2 it follows that $\langle uX, \Delta(\mathbf{q}) \rangle$ is such a subgroup, where u is any unit of infinite order in A. (We could take $u = 1 + \theta$, for example.)

REFERENCES

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

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

3. W. Klingenberg, Lineare Gruppen über lokalen Ringen, *Amer. J. Math.* **83** (1961), 137–153.

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

5. A. W. Mason, On subgroups of $GL(n, A)$ which are generated by commutators II, *J. Reine Angew. Math.* **322** (1981), 118–135.

6. A. W. Mason, Anomalous normal subgroups of the modular group, *Comm. Algebra* **11** (1983), 2555–2573.

7. A. W. Mason, On non-normal subgroups of $GL_n(A)$ which are normalized by elementary matrices, *Illinois J. Math.* **28** (1984), 125–138.

8. A. W. Mason, Anomalous normal subgroups of $SL_2(K[x])$, *Quart. J. Math. (Oxford) Ser. (2)*, **36** (1985), 345–358.

9. A. W. Mason, On GL_2 of a local ring in which 2 is not a unit, *Canad. Math. Bull*, to appear.

10. A. W. Mason and W. W. Stothers, On subgroups of $GL(n, A)$ which are generated by commutators, *Invent. Math.* **23** (1974), 327–346.

11. M. Newman, A complete description of the normal subgroups of genus one of the modular group, *Amer. J. Math.* **86** (1964), 17–24.

12. P. Ribenboim, *Algebraic Numbers* (Wiley-Interscience, New York, 1972).

13. J.-P. Serre, Le problème des groupes de congruence pour SL_2, *Ann. of Math.* **92** (1970), 489–527.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW