

ON NON-NORMAL SUBGROUPS OF $GL_n(A)$ WHICH ARE NORMALIZED BY ELEMENTARY MATRICES

BY

A. W. MASON

1. Introduction

Let A be a ring with identity, \mathfrak{q} a (two-sided) ideal in A (possibly $\mathfrak{q} = A$) and let $f : GL_n(A) \rightarrow GL_n(A/\mathfrak{q})$ be the natural homomorphism. We put

$$G = GL_n(A), \quad G(\mathfrak{q}) = \text{Ker } f \quad \text{and} \quad H(\mathfrak{q}) = f^{-1}(C),$$

where C is the centre of $GL_n(A/\mathfrak{q})$. (By definition

$$H(\mathfrak{q}) = \{X \in G : X \equiv xI \pmod{\mathfrak{q}}, \text{ where } x \in A \text{ is central (mod } \mathfrak{q})\}$$

and $H(A) = G(A) = G$.)

Let Δ be the subgroup of G generated by all the elementary matrices $I + aE_{ij}$, $a \in A$, $i \neq j$, $1 \leq i, j \leq n$, and let $\Delta(\mathfrak{q})$ be the *normal* subgroup of Δ generated by the \mathfrak{q} -elementary matrices, $I + qE_{ij}$, $q \in \mathfrak{q}$, $i \neq j$. (By definition $\Delta = \Delta(A)$.) Finally, if H, K are subgroups of G , $[H, K]$ is the subgroup generated by commutators $[h, k] = h^{-1}k^{-1}hk$, $h \in H$, $k \in K$.

Our starting point is the following:

THEOREM 1. *Assume that either*

(a) *A satisfies $SR_t(A)$, for some $t \geq 2$, and $n \geq \max(t, 3)$,*
or

(b) *A is finitely generated as a module over its centre and $n \geq 3$.*

If E is a subgroup of G normalized by Δ , then for some unique ideal \mathfrak{e} (called the level of E),

$$\Delta(\mathfrak{e}) \leq E \leq H(\mathfrak{e}).$$

Parts (a) and (b) are due to Bass [1, p. 240] and Vaserstein [11], respectively. Many special cases of this result have appeared over the last twenty years. Among the most important are those due to Brenner [3] ($A = \mathbb{Z}$, $n \geq 3$) and Golubchik [4] (A commutative, $n \geq 3$). The classical example of the modular group shows that the restriction $n \geq 3$ is necessary. It is known [5] that, if N is a normal subgroup of finite index in $GL_2(\mathbb{Z})$, then, with finitely many excep-

Received November 30, 1981.

tions, the commutator subgroup N' is a normal, non-central subgroup which contains $\Delta(\mathfrak{e})$ only when $\mathfrak{e} = 0$. (\mathbf{Z} satisfies $SR_3(\mathbf{Z})$.)

We assume throughout that A satisfies $SR_t(A)$ ($t \geq 2$) [1, p. 231] and that $n \geq \max(t, 3)$. This enables us to use results from algebraic K -theory, in particular the well-known stability theorem of Bass-Vaserstein [10]. As above let E be a subgroup of G , normalized by Δ , with level \mathfrak{e} . (From now on we abbreviate this to " E is a subgroup of level \mathfrak{e} ".) This paper is concerned with the following question (first raised by Bass in 1964): Is E a normal subgroup of G ? Now, since $[\Delta, \Delta(\mathfrak{e})] = \Delta(\mathfrak{e})$ [1, p. 223] we have, by Theorem 1,

$$\Delta(\mathfrak{e}) \leq [G, E] \leq [G, H(\mathfrak{e})].$$

It follows that, if $[G, H(\mathfrak{e})] = \Delta(\mathfrak{e})$, then E is normal. The most obvious question which arises from this is the following:

(*) Does $[G, H(\mathfrak{e})] \neq \Delta(\mathfrak{e})$ imply the existence of a non-normal subgroup of level \mathfrak{e} ?

It has been shown [7] that non-normal subgroups of this type exist for the case $A = \mathbf{Z}[i]$ if and only if n is even ($n \geq 3$). In this paper an example (in §4) is given which shows that in general the answer to (*) is no. In §2 however we do establish various conditions on A , \mathfrak{q} and n under which (*) has an affirmative answer. For example we show that if A contains central units of infinite order then (for any ideal \mathfrak{q}) non-normal subgroups of level \mathfrak{q} exist if and only if

$$[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q}) \quad (n \geq \max(t, 3)).$$

We also prove that a similar result holds for commutative A which have only units of finite order, provided certain finiteness hypotheses on A/\mathfrak{q} and $G(\mathfrak{q})/\Delta(\mathfrak{q})$ (together with related restrictions on n) are satisfied.

In §3 using the famous paper of Bass, Milnor and Serre [2] we apply the results of §2 to the case where A is Dedekind of arithmetic type ($t = 3$, $n \geq 3$). We show that the answer to (*) is always yes provided that either A is not totally imaginary or A contains units of infinite order. Different situations can arise when A is totally imaginary with only finitely many units. In §4 by considering the case

$$A = \mathbf{Z}[\varrho], \quad \text{where } \varrho^2 + \varrho + 1 = 0,$$

and $n \equiv 2 \pmod{4}$ ($n \geq 6$), we show that in general the answer to (*) is no. On the other hand we prove in §5 that, when $A = \mathbf{Z}[i]$ ($i^2 = -1$), every subgroup of level \mathfrak{q} is also normal (in $GL_n(\mathbf{Z}[i])$) if and only if $[G, H(\mathfrak{q})] = \Delta(\mathfrak{q})$ ($n \geq 3$).

2. Non-normal subgroups of level \mathfrak{q}

It is clear that, when $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$, the existence of a non-normal subgroup of level \mathfrak{q} is equivalent to the existence of such a subgroup which is also

cyclic (mod $\Delta(q)$). We note that, since $[\Delta, H(q)] = \Delta(q)$ [1, p. 240], the subgroup $\langle X, \Delta(q) \rangle$ has level q , for all $X \in H(q)$. This motivates the following lemma.

For any $g \in G$ we put $[G, g] = \{[x, g] : x \in G\}$.

LEMMA 2. *Suppose that $[G, H(q)] \neq \Delta(q)$. Let $X \in H(q)$ satisfy $[G, X] \not\subseteq \Delta(q)$ and let $S = \langle X, \Delta(q) \rangle$. Then $S \triangleleft G$ implies that X has finite order (mod $\Delta(q)$).*

Proof. Since S has level q we have [6]

$$\Delta(q) \leq [G, S] \leq G(q).$$

Now $[G, G(q)] = \Delta(q)$ [10] and hence $[G, [G, S]] = \Delta(q)$ ($[\Delta, \Delta(q)] = \Delta(q)$). It follows that, for all $X_1, X_2 \in S$, and $Y_1, Y_2 \in G$,

$$[Y_1 Y_2, X_1] \equiv [Y_1, X_1] [Y_2, X_1] \pmod{\Delta(q)}$$

and

$$[Y_1, X_1 X_2] \equiv [Y_1, X_1] [Y_1, X_2] \pmod{\Delta(q)}.$$

It is clear then that $[G, S] = [G, X]\Delta(q)$.

Suppose now that $S \triangleleft G$, i.e., $(\Delta(q) \leq) [G, S] \leq S \cap G(q)$. Then $[G, S]$ is generated by X^s , say, (mod $\Delta(q)$), where $s > 0$. Let $Y \in G$ "generate" the image of the epimorphism $G \rightarrow [G, S] / \Delta(q)$, defined by

$$Y_1 \mapsto [Y_1, X]\Delta(q) \quad (Y_1 \in G).$$

This means that $[Y, X] \equiv X^s \pmod{\Delta(q)}$. Then by the above we have

$$I \equiv [Y, X^s] \equiv [Y, X]^s \equiv X^{s^2} \pmod{\Delta(q)}.$$

Before our first theorem we make the following definition.

DEFINITION. For any ideal q , the subgroup $Z(q)$ of G is defined by the property that $Z(q) / \Delta(q)$ is the centre of $G / \Delta(q)$.

LEMMA 3. (i) $G(q) \leq Z(q) \leq H(q)$.

(ii) $Z(q) = H(q)$ if and only if $[G, H(q)] = \Delta(q)$.

(iii) $uI \in Z(q)$, where u is any unit of A such that $ua \equiv au \pmod{q}$, for all $a \in A$.

Proof. Clearly $Z(q)$ has level q' , say. Since $[G, G(q)] = \Delta(q)$ [10], it follows that $G(q) \leq Z(q)$ and $q \leq q'$. On the other hand, by Theorem 1,

$$\Delta(q') = [\Delta, \Delta(q')] \leq [G, Z(q)] \leq \Delta(q).$$

And so $q' \leq q$. (i) follows from Theorem 1. (ii) follows from (i), and (iii) is trivial.

THEOREM 4. *Suppose that (the abelian group) $Z(\mathfrak{q})/\Delta(\mathfrak{q})$ has elements of infinite order. Then every subgroup of level \mathfrak{q} is also normal in G if and only if $[G, H(\mathfrak{q})] = \Delta(\mathfrak{q})$.*

Proof. We only have to show that when $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$ there exists a non-normal subgroup of level \mathfrak{q} .

Choose $X \in H(\mathfrak{q})$ such that $[G, X] \not\subseteq \Delta(\mathfrak{q})$ and let $S = \langle X, \Delta(\mathfrak{q}) \rangle$. If $[G, S] \leq S$, we are finished. Suppose then that $[G, S] \not\leq S$. By Lemma 2 it follows that X has finite order (mod $\Delta(\mathfrak{q})$). Now choose $U \in Z(\mathfrak{q})$ of infinite order (mod $\Delta(\mathfrak{q})$) and let $S_0 = \langle XU, \Delta(\mathfrak{q}) \rangle$. Clearly $[G, S_0] = [G, S] \neq \Delta(\mathfrak{q})$.

Suppose further that $[G, S_0] \leq S_0$. Then, again by Lemma 2, XU (and hence U) has finite order (mod $\Delta(\mathfrak{q})$). Therefore S_0 is the required non-normal subgroup of level \mathfrak{q} .

In particular we have (Lemma 3 (iii)):

COROLLARY 5. *Suppose that A has central units of infinite order. Then every subgroup of level \mathfrak{q} is also normal in G if and only if $[G, H(\mathfrak{q})] = \Delta(\mathfrak{q})$.*

We show later (§4) that Theorem 4 is not true in general if $Z(\mathfrak{q})/\Delta(\mathfrak{q})$ is torsion. However as we show later in this section Theorem 4 does hold for commutative A provided certain finiteness hypotheses are satisfied. Since A will be assumed to be commutative for most of the remainder of the paper it seems appropriate at this time to provide a non-commutative illustration of Theorem 4 and Corollary 5.

We refer to the example given in [8] (after Theorem 3.5) and we use the notation of this paper. It is shown that for this choice of A and \mathfrak{q} there is a unit ν in A such that (i) $\nu I \in H(\mathfrak{q})$ and (ii) the subset $[G, \nu I]$ of $G(\mathfrak{q})$ contains an element of infinite order (mod $\Delta(\mathfrak{q})$). It is easily verified that νI has infinite order (mod $G(\mathfrak{q})$). By Lemma 2 we conclude that $\langle \nu I, \Delta(\mathfrak{q}) \rangle$ is a non-normal subgroup of level \mathfrak{q} .

We require the following “minimal counterexample” lemma.

LEMMA 6. *Suppose that $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$ and let*

$$q = \min\{|\langle X, \Delta(\mathfrak{q}) \rangle : \Delta(\mathfrak{q}) \mid : X \in H(\mathfrak{q}), [G, X] \not\subseteq \Delta(\mathfrak{q}), \langle X, \Delta(\mathfrak{q}) \rangle \triangleleft G\}.$$

Then $q = p^\alpha$, for some prime p and integer $\alpha \geq 2$. Further, if $q = p^\alpha$ is “attained” by $X_0 \in H(\mathfrak{q})$, then

- (i) $X_0^p \in Z(\mathfrak{q})$, and
- (ii) $[G, \langle X_0, \Delta(\mathfrak{q}) \rangle] / \Delta(\mathfrak{q})$ is generated by $X_0^{p^{\alpha-1}} \pmod{\Delta(\mathfrak{q})}$.

Moreover, if A is commutative, then p divides n .

Proof. By Lemma 2, q is well-defined. Put $T = \langle X_0, \Delta(\mathfrak{q}) \rangle$. As in the proof of Lemma 2, let $Y \in G$ “generate” the image of the epimorphism

$$G \rightarrow [G, T] / \Delta(\mathfrak{q})$$

defined by

$$Y_1 \mapsto [Y_1, X_0] \Delta(\mathfrak{q}).$$

($[G, T] = [G, X_0] \Delta(\mathfrak{q})$ and $[G, T] \leq T$.) It is clear that, for any integer f , we have

(1) $X'_0 \in Z(\mathfrak{q})$ if and only if $[Y, X'_0]^f \equiv I \pmod{\Delta(\mathfrak{q})}$.

Let $T \cap Z(\mathfrak{q}) = \langle X_0^d, \Delta(\mathfrak{q}) \rangle$ and $[G, T] = \langle X_0^e, \Delta(\mathfrak{q}) \rangle$, where $d|e$ and $e|q$ with $d, e > 1$. (X_0 has order $q \pmod{\Delta(\mathfrak{q})}$ and $[G, T] \leq Z(\mathfrak{q})$.) It follows from (1) that $q = de$, since, by definition,

$$[Y, X_0] \equiv X_0^e \pmod{\Delta(\mathfrak{q})}.$$

Suppose that $d = d_1 d_2$, with $1 < d_1 < d$. Then $X_0^{d_1} \notin Z(\mathfrak{q})$ and so by (1),

$$[Y, X_0^{d_1}] \equiv [Y, X_0]^{d_1} \not\equiv I \pmod{\Delta(\mathfrak{q})}.$$

But $X_0^{d_1}$ has order $q/d_1 < q \pmod{\Delta(\mathfrak{q})}$ and $\langle X_0^{d_1}, \Delta(\mathfrak{q}) \rangle \triangleleft G$, since

$$[Y, X_0^{d_1 k}] \equiv [Y, X_0]^{d_1 k} \pmod{\Delta(\mathfrak{q})}, \text{ for all } k.$$

This contradicts the minimality of q unless $d = p$, prime, say.

Let p' be the largest divisor of q prime to p . Clearly $X_0^{p'} \notin Z(\mathfrak{q})$ and so, again by (1), $[G, X_0^{p'}] \subseteq \Delta(\mathfrak{q})$. By considering the subgroup $\langle X_0^{p'}, \Delta(\mathfrak{q}) \rangle$ we deduce as above that $p' = 1$.

The last part follows from the fact [7, Theorem 2.1] that when A is commutative the abelian group $[G, H(\mathfrak{q})] / \Delta(\mathfrak{q})$ has exponent n .

THEOREM 7. *Suppose that A is commutative and that A, \mathfrak{q} and n satisfy the following:*

(a) *There exists $h > 0$ (assumed minimal) such that, for all $a \in A$ prime to \mathfrak{q} , $a^h \in U(A) + \mathfrak{q}$, where $U(A)$ is the group of units in A .*

(b) *The (abelian) group $G(\mathfrak{q}) / \Delta(\mathfrak{q})$ has (minimum) exponent $k (> 0)$, say.*

(c) *hk divides n .*

Then non-normal subgroups of level \mathfrak{q} exist if and only if $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$.

Before the proof of Theorem 7 we make some remarks about the hypotheses.

(i) Clearly h is independent of n . This is also true of k (modulo the basic assumption that $n \geq \max(t, 3)$.) More precisely the Bass-Vaserstein stability theorem [10] states that the groups $G(\mathfrak{q}) / \Delta(\mathfrak{q})$ are all isomorphic when $n \geq \max(t, 3)$.

(ii) If A is a Dedekind ring of arithmetic type [2, p. 83] and $\mathfrak{q} \neq 0$, (a) and (b) are both satisfied. (A/\mathfrak{q} is finite and $|G(\mathfrak{q}) : \Delta(\mathfrak{q})|$ divides m^2 , where m is the order of the group of roots of unity in A .) Theorem 7 will then hold in this case provided n is divisible, for example, by $m^2 h_0$, where $h_0 = |U(A/\mathfrak{q})|$.

Proof of Theorem 7. We need only prove that, if (a), (b), (c) are satisfied and if $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$, then there exists a non-normal subgroup of level \mathfrak{q} .

We may suppose then that $X_0 \in H(\mathfrak{q})$ satisfies the statement of Lemma 6, for some prime p dividing n . Then

$$X_0 \equiv x_0 I \pmod{\mathfrak{q}},$$

where $x_0 \in A$ and

$$x_0^n \equiv \det(X_0) \pmod{\mathfrak{q}}.$$

As in Lemma 6, let $p^\alpha = \text{ord}_{\Delta(\mathfrak{q})}(X_0)$ ($\alpha \geq 2$). Clearly $x_0^{p^\alpha} \equiv 1 \pmod{\mathfrak{q}}$. Let p^β be the smallest positive integer such that $x_0^{p^\beta} \in U(A) + \mathfrak{q}$. By definition

$$X_0^{p^\beta} = uX',$$

say, where $u \in U(A)$, $u \equiv x_0^{p^\beta} \pmod{\mathfrak{q}}$ and $X' \in G(\mathfrak{q})$. Hence $X_0^{p^\beta} \in Z(\mathfrak{q})$ by Lemma 3. Now, from Lemma 6, $X_0 \notin Z(\mathfrak{q})$ and $x_0^{p^{\alpha-1}} \equiv 1 \pmod{\mathfrak{q}}$. We conclude that $0 < \beta < \alpha$. Further p^β divides h by (a) and hence n by (c).

Now, by [9, p. 332] there exists $X_1 \in SL_{p^\beta}(A)$ such that

$$X_1 \equiv x_0 I \pmod{\mathfrak{q}}.$$

Let $X_2 \in SL_n(A)$ be the "diagonal" matrix consisting of n/p^β blocks, each of which is X_1 , "along its main diagonal". Then

$$X_0 = X_2 Y,$$

where $Y \in G(\mathfrak{q})$. Now $X_1^{p^\beta} \equiv uI \pmod{\mathfrak{q}}$ and so, by repeated applications of the Whitehead lemma [1, p. 226], we see that

$$X_2^{p^\beta} \equiv uX_3^{n/k^\beta} \pmod{\Delta(\mathfrak{q})},$$

where X_3 is $u^{-1}X_1^{p^\beta}$ ($\equiv I \pmod{\mathfrak{q}}$) embedded in G in the "upper left hand corner." Now kh divides n , by (c), and so k divides n/p^β . We deduce from (b) that

$$X_0^{p^\beta} \equiv uY^{p^\beta} \pmod{\Delta(\mathfrak{q})}.$$

(Recall from Lemma 3(i) that $Y \in G(\mathfrak{q})$ and so is central $\pmod{\Delta(\mathfrak{q})}$.)

Let $p^\gamma = \text{ord}_{\mathfrak{q}}(x_0)$. Then from the above $0 < \beta \leq \gamma < \alpha$ and $u^{p^{\gamma-\beta}} \equiv 1 \pmod{\mathfrak{q}}$. Again by Whitehead lemma and (c) it follows that $\forall I \in G(\mathfrak{q})^n \leq \Delta(\mathfrak{q})$ where $\nu = u^{p^{\gamma-\beta}}$. We deduce that

$$X_0^{p^\gamma} \equiv Y^{p^\gamma} \pmod{\Delta(\mathfrak{q})}.$$

Now consider the subgroup $\langle X_4, \Delta(\mathfrak{q}) \rangle$ of level \mathfrak{q} , where $X_4 = X_0 Y^{-1}$. By the above $X_4^{p^\gamma} \in \Delta(\mathfrak{q})$ and, by Lemma 6, $[G, X_4] \equiv [G, X_0] \neq I \pmod{\Delta(\mathfrak{q})}$. The minimality of p^α then implies that $\langle X_4, \Delta(\mathfrak{q}) \rangle$ is non-normal.

We show later (§4) that, for a given pair h, k , hypothesis (c) is, in a sense, "best possible". Of course (a) and (b) can be replaced by weaker (but more complicated) hypotheses.

3. Dedekind rings of arithmetic type

From now on we assume that A is a Dedekind ring of arithmetic type as defined in [2, p. 83] ($t = 3$ and $n \geq 3$). The basic reference in this connection is of course the Bass, Milnor, Serre paper [2]. For our purposes however the most convenient reference is [7]. We make frequent use of the notation in these papers. A is said to be *totally imaginary* if it is the ring of integers of an algebraic number field which cannot be embedded in \mathbf{R} .

We begin by recalling some of the basic results of [2]. For any ideal \mathfrak{q} , let

$$\Gamma(\mathfrak{q}) = G(\mathfrak{q}) \cap SL_n(A) \quad \text{and} \quad C(\mathfrak{q}) = \Gamma(\mathfrak{q}) / \Delta(\mathfrak{q}).$$

(When A satisfies $SR_t(A)$ and $n \geq \max(t, 3)$, $\Delta(\mathfrak{q}) \triangleleft G$ [1, p. 240].) Since A satisfies $SR_3(A)$ each element of $C(\mathfrak{q})$ can be represented by a unimodular pair

$$(a, b) \equiv (1, 0) \pmod{\mathfrak{q}}.$$

The pair (a, b) is the first row of a 2×2 matrix in $\text{Ker}(SL_2(A) \rightarrow SL_2(A/\mathfrak{q}))$, embedded in G in the usual way.

(a) When A is not totally imaginary, $C(\mathfrak{q}) = 1$, for all \mathfrak{q} .

(b) When A is totally imaginary the situation is much more complicated. Let m be the order of the group of roots of unity in such on A . Throughout \mathfrak{p} denotes a prime ideal in A and p the rational prime over which it lies. For any real x and positive integer y , μ_y is the cyclic group of order y and $[x]_{[0,y]}$ is the nearest integer in the range $[0, y]$ to the integral part $[x]$ of x .

It can be shown that for some divisor r , say, of m ,

$$C(\mathfrak{q}) \cong \mu_r,$$

where r is given by

$$\text{ord}_p(r) = \min_{p|p} \left[\frac{h}{e} - \frac{1}{p-1} \right]_{[0, \text{ord}_p(m)]},$$

with $h = \text{ord}_p(\mathfrak{q})$ and $e = \text{ord}_p(p)$. When $r > 1$, the mapping $C(\mathfrak{q}) \rightarrow \mu_r$ is given by

$$(a, b) \mapsto \begin{cases} \left(\frac{b}{a} \right)_r, & b \neq 0 \\ 1 & , b = 0 \end{cases}$$

where $(a, b) \equiv (1, 0) \pmod{\mathfrak{q}}$, $aA + bA = A$ and

$$\left(\frac{b}{a} \right)_r \in \mu_r$$

is the r -th power residue symbol. Clearly $r = 1$ when \mathfrak{q} is prime to m and $r = m$ when m^2 divides \mathfrak{q} (see [7, §4]).

Our next theorem covers the situation where $[G, H(\mathfrak{q})]$ is always equal to $\Delta(\mathfrak{q})$. We note that in general $\Delta(\mathfrak{q}) \leq [G, H(\mathfrak{q})] \leq \Gamma(\mathfrak{q})$ [9, Theorem 3.1].

THEOREM 8. *Let A be Dedekind of arithmetic type and suppose that either A is not totally imaginary or A is totally imaginary and $(n, m) = 1$.*

Then, for any subgroup E of G , $E \triangleleft G$ if and only if $[E, SL_n(A)] \leq E$.

Proof. When A is Dedekind of arithmetic type, $\Delta = SL_n(A)$ [2, Corollary 4.3]. The proof follows from Theorem 1 and the fact that for the above cases, $[G, H(\mathfrak{q})] = \Delta(\mathfrak{q})$, for all \mathfrak{q} [7, Corollaries 4.2, 4.4]. (In fact, when A is not totally imaginary, $[G, H(\mathfrak{q})] = \Delta(\mathfrak{q}) = \Gamma(\mathfrak{q})$, for all \mathfrak{q} .)

By Corollary 5 we have:

THEOREM 9. *Let A be totally imaginary with infinitely many units. Then non-normal subgroups of G of level \mathfrak{q} exist if and only if $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$.*

There remain to consider therefore the totally imaginary number fields with only finitely many units. By the Dirichlet unit theorem these are precisely the rings of integers of the imaginary quadratic extensions of \mathbf{Q} . We will consider the cases $A = \mathbf{Z}[\varrho]$, $\mathbf{Z}[i]$, where $\varrho^2 + \varrho + 1 = 0$ and $i^2 = -1$. Before dealing with them we require the following (technical) lemma.

LEMMA 10. *Let A be totally imaginary and let \mathfrak{q} be an ideal such that $|C(\mathfrak{q})| = 2^s$, for some $s \geq 1$. Suppose that n is even ($n \geq 4$) and that for some prime $\alpha \in A$, $\alpha^2 = 1 - q$, where $q \in \mathfrak{q}$. Put*

$$X = \sum_{i=1}^{\frac{n}{2}} \{ \alpha(1+q)E_{2i-1, 2i-1} + q(E_{2i-1, 2i} - E_{2i, 2i-1}) + \alpha E_{2i, 2i} \}.$$

Then $X \in H(\mathfrak{q}) \cap SL_n(A)$, $X^2 \in \Gamma(\mathfrak{q})$ and the order of $X^2 \pmod{\Delta(\mathfrak{q})}$ is

$$\frac{1}{2} (3 - (-1)^\beta), \quad \text{where } \beta = \frac{(N(\alpha) - 1)n}{2^{s+1}}.$$

($N(\alpha)$ is the (absolute) norm of α .)

Proof. Clearly $X \equiv \alpha I \pmod{\mathfrak{q}}$ and $\det X = 1$. Our first task is to find a unimodular pair $(a, b) \equiv (1, 0) \pmod{\mathfrak{q}}$ representing X^2 in $C(\mathfrak{q})$.

Since $[\Delta, H(\mathfrak{q})] = \Delta(\mathfrak{q})$ [1, p. 240],

$$X^2 \equiv YXY^{-1}X \pmod{\Delta(\mathfrak{q})},$$

where $Y = I + \sum_{i=1}^{n/2} \alpha E_{2i, 2i-1}$. By repeated applications of the Whitehead lemma [1, p. 226] we deduce that

$$X^2 \equiv \begin{bmatrix} 1 - 2q^2 & 2\alpha q \\ * & * \end{bmatrix}^{n/2} \pmod{\Delta(\mathfrak{q})},$$

where the 2×2 matrix is identified with its usual embedding in $\Gamma(q)$. It remains therefore to evaluate the symbol

$$\left(\frac{b}{a}\right)_r,$$

for the case $r = 2^s$, $a = 1 - 2q^2$ and $b = 2\alpha q$.

Using standard notation [7, p. 125] we have

$$\left(\frac{b}{a}\right)_r = \prod_{\substack{p|b \\ p \nmid r}} \left(\frac{a}{p}\right)_r^{\text{ord}_p(b)} \prod_{p|r} \left(\frac{a, b}{p}\right)_r$$

Now let $r = 2^s$, $a = 1 - 2q^2$ and $b = 2\alpha q$. For any $p|2$,

$$\text{ord}_p(a - 1) = f + 2 \text{ord}_p(q) \geq f + 2 \text{ord}_p(q),$$

where $f = \text{ord}_p(2)$. Since $|C(q)| = 2^s$, the formula for $|C(q)|$ implies that

$$\text{ord}_p(q) \geq f(s + 1).$$

Hence $\text{ord}_p(a - 1) \geq f(2s + 3) > f(s + 1)$. It follows that in this case

$$\left(\frac{a, b}{p}\right)_r = 1 \quad [9, \text{p. 344}].$$

We note that α is prime, that $p|2q \implies a \equiv 1 \pmod{q}$, and that $a \equiv -1 \pmod{\alpha}$. It follows from the definition of the symbol

$$\left(\frac{a}{p}\right)_r,$$

(called the r -th power residue symbol at p) and the above that, in this case,

$$\left(\frac{b}{a}\right)_r = (-1)^{(N(\alpha)-1)/2^s}.$$

The result follows.

4. The case $A = \mathbf{Z}[\varrho]$

In this case the units of A are $\pm 1, \pm \varrho, \pm \varrho^2 (\varrho^3 = 1)$ and so $m = 6$. Our counterexample is based on the ideal (4). Now 2 is prime and it follows from the formula given in the previous section that $|C(4)| = 2$. (We have modified the notation slightly.) When $n (\geq 3)$ is odd it follows from [7, Corollary 4.4] that $[G, H(4)] = \Delta(4)$. In this case then every subgroup of level (4) is normal in G . The situation when n is even is however more complicated.

THEOREM 11. *Let $A = \mathbf{Z}[\varrho]$, where $\varrho^2 + \varrho + 1 = 0$, and suppose that n is even ($n \geq 4$). Then $[G, H(4)] = \Gamma(4) (\neq \Delta(4))$.*

- (i) *When $4|n$, there exist non-normal subgroups of level (4).*
- (ii) *When $n \equiv 2 \pmod{4}$, every subgroup of level (4) is normal in G .*

Proof. Let $\alpha = 1 + 2\varrho$. Then α is prime, $N(\alpha) = 3$ and $\alpha^2 \equiv 1 \pmod{4}$. Define $X \in H(4)$ as in Lemma 10. By [7, Theorem 4.6] (with $u = -1$, $\alpha^* = 1 + 2\varrho$) we deduce that commutator $[I - 2E_{11}, X] \notin \Delta(4)$. Hence

$$[G, H(4)] = \Gamma(4),$$

since $|\Gamma(4) : \Delta(4)| = 2$. ($[G, H(4)] \leq \Gamma(4)$.)

Now it is easily verified that $A/(4)$ has 12 units and that if $\beta \in A$ is prime to 2, then

$$\beta \equiv u(1 + 2\varrho)^j \pmod{4},$$

where $j = 0, 1$ and $u \in U(A) = \{\pm 1, \pm \varrho, \pm \varrho^2\}$. Part (i) then follows from Theorem 7 with $h = k = 2$.

For part (ii) we note first of all that, by Lemma 10 (with $\alpha = 1 + 2\varrho$, $N(\alpha) = 3$, $s = 1$, $n \equiv 2 \pmod{4}$), $X^2 \in \Gamma(4) \setminus \Delta(4)$. It follows that

$$\Gamma(4) = \langle X^2, \Delta(4) \rangle.$$

Now let $Y \in H(4)$. Then, by the above,

$$Y = uX^jT,$$

where $u \in U(A)$, $j = 0$ or 1 and $T \in G(4) = \Gamma(4)$. Now, since $[G, G(4)] = \Delta(4)$, we deduce that

$$[G, Y] \equiv [G, X^j] \pmod{\Delta(4)}.$$

Let $S = \langle Y, \Delta(4) \rangle$ and recall that $\Delta(4) \leq [G, S] \leq \Gamma(4)$.

If $j = 0$, $[G, S] = \Delta(4) \leq S$ and so S is normal. On the other hand, if $j = 1$,

$$Y^6 \equiv u^6 X^6 T^6 \equiv X^2 \pmod{\Delta(4)}.$$

($G(4)$ is central (mod $\Delta(4)$) by Lemma 3(i).) Hence

$$S \geq \langle X^2, \Delta(4) \rangle = \Gamma(4) \geq [G, S]$$

and so S is normal in G . This completes the proof.

Theorem 11 shows that in general hypothesis (c) of Theorem 7 (for a given pair h, k) cannot be weakened.

5. The case $A = \mathbf{Z}[i]$

The object of this section is to show that (in the context of this paper) some imaginary quadratic number fields “behave nicely”. In this case the units are $\pm 1, \pm i$ and so $m = 4$. Throughout \mathfrak{p} will denote the ideal $(1 + i)$ and \mathfrak{q} will always be non-zero. As in [7] we put

$$\theta(\mathfrak{q}) = H(\mathfrak{q}) \cap SL_n(A), \quad \overline{GH}(\mathfrak{q}) = [G, H(\mathfrak{q})]/\Delta(\mathfrak{q})$$

and

$$\overline{G\theta}(q) = [G, \theta(q)] / \Delta(q).$$

For any $\alpha \in A$, $N(\alpha) = |\alpha|^2$ is the *norm* of α .

Since $(2) = p^2$, the structure of $C(q)$ depends entirely on the “ p -component” of q . We recall the following [7, Theorem 5.1].

THEOREM 12. *Let $x = \text{ord}_p(q)$. Then*

$$C(q) \cong C(p^x) \cong \begin{cases} 1, & x \leq 3 \\ C(p^4), & x = 4, 5 \\ C(p^6), & x \geq 6 \end{cases},$$

and

$$|C(p^x)| = \begin{cases} 1, & x \leq 3 \\ 2, & x = 4, 5 \\ 4, & x \geq 6 \end{cases}$$

We will show that when $[G, H(q)] \neq \Delta(q)$ non-normal subgroups of level q always exist. We begin by determining precisely when $[G, H(q)] \neq \Delta(q)$. This has been done for $n = 4$ in [7, Theorem 5.15]. When n is odd it is known [7, Theorem 5.2(i)] that $[G, H(q)] = \Delta(q)$, for all q . We require the following lemmas.

LEMMA 13. *Let $\alpha \in A$ be prime to p . Then*

- (i) $\text{ord}_p(\alpha^4 + 1) = 2$,
- (ii) $\alpha^2 \equiv \pm 1 \pmod{p^6}$,
- (iii) $\alpha^{2^x} \equiv 1 \pmod{p^x}$, where

$$s = \left\lfloor \frac{x-1}{2} \right\rfloor + 1,$$

for all $x \geq 6$.

Proof. (i) and (ii) are trivial. (iii) follows by induction.

LEMMA 14. (a) *Under the natural isomorphism*

$$C(q) \cong C(p^x) \quad \text{where } x = \text{ord}_p(q),$$

$\overline{GH}(q)$ embeds into $\overline{GH}(p^x)$ and

$$\overline{G\theta}(q) \cong \overline{G\theta}(p^x).$$

(b) *Under the natural isomorphism $C(p^{x+1}) \cong C(p^x)$, where $x \leq 4$ or $x \geq 6$,*

$$\overline{GH}(p^{x+1}) \quad (\text{resp. } \overline{G\theta}(p^{x+1}))$$

embeds into

$$\overline{GH}(p^x) \quad (\text{resp. } \overline{G\theta}(p^x)).$$

(c) If $\text{ord}_2(n) \geq 2$ and $\text{ord}_p(q) \geq 3$, then $H(q) = \theta(q)$.

Proof. We recall that if $q_1 \leq q_2$, then

$$H(q_1) \leq H(q_2) \quad \text{and} \quad \theta(q_1) \leq \theta(q_2).$$

(a) follows from Theorem 12 and the fact that

$$[G, \theta(p^x)] = [G, \theta(q)]\Delta(p^x)$$

(See the proof of [7, Theorem 5.3].) (b) again follows from Theorem 12.

For (c) we note that if $\alpha^4 \equiv u \pmod{p^x}$, where $u = \pm 1, \pm i$ and $x \geq 3$, then $u = 1$ by Lemma 13(ii).

THEOREM 15. Let $x = \text{ord}_p(q)$ and $y = \text{ord}_2(n)$, with $y > 0$.

(a) $[G, H(q)] = \Delta(q)$, when $x \geq 2y + 6$.

(b) $[G, \theta(q)] = \Gamma(q)$, when $x \leq 2y + 3$.

(c) $|\Gamma(q) : [G, H(q)]| = |[G, H(q)] : \Delta(q)| = 2$, when $x = 2y + 4$ or $2y + 5$.

Proof. By Theorem 12 we may assume that $x \geq 4$. We treat the cases $y = 1$ and $y > 1$ separately.

Case where $y = 1$. For (a) it is sufficient to prove that $\overline{GH}(p^8) = 1$, by Lemma 14. By [7, Lemma 4.7] we have to consider those $\alpha \in A$ such that

$$\alpha^2 \equiv u \pmod{p^8},$$

where $u = \pm 1, \pm i$. By Lemma 13(ii) we have $u = \pm 1$ and it is easily verified that $N(\alpha) \equiv 1 \pmod{16}$. It follows by [7, Theorem 4.6] that $\overline{GH}(p^8) = 1$. (We can assume by the Dirichlet theorem on primes in an arithmetic progression that α is prime.)

For (b), consider $\alpha = 1 + 2i$. Clearly $\alpha^2 \equiv 1 \pmod{p^5}$ and α is prime, with $N(\alpha) = 5$. We deduce again by [7, Theorem 4.6] and Theorem 12, that $[G, \theta(p^5)] = \Gamma(p^5)$. (b) then follows from Lemma 14.

For (c) consider $\alpha = 5 + 4i$. Clearly $\alpha^2 \equiv 1 \pmod{p^7}$ and α is prime with $N(\alpha) = 41$. By [7, Theorem 4.6] it follows that $\overline{GH}(p^7) \neq 1$. But by [7, Theorem 4.3(a)] $|\overline{GH}(q)|$ always divides 2. Hence $|\overline{GH}(p^7)|$ and similarly $|\overline{GH}(p^6)|$ is equal to 2. The general case follows from Lemma 14.

Case where $y > 1$. By [7, Lemma 4.7] and Lemma 14(c) we are concerned with these $\alpha \in A$ for which $\alpha^{2^y} \equiv 1 \pmod{p^x}$. (We may assume again by Dirichlet's theorem on primes in an arithmetic progression that any such α is prime.)

For (a) it is sufficient to prove that $[G, H(p^{2y+6})] = \Delta(p^{2y+6})$, by Lemma 14. If $\alpha^{2^y} \equiv 1 \pmod{p^{2y+6}}$, then

$$\alpha^4 \equiv 1 \pmod{p^{10}}$$

by Lemma 13(i). (Note that $\alpha^{2^y} - 1 = (\alpha^{2^{y-1}} - 1)(\alpha^{2^{y-1}} + 1)$.) It follows by direct calculation that $N(\alpha) \equiv 1 \pmod{16}$, which implies that $\overline{GH}(\mathfrak{p}^{2y+6}) = 1$ by [7, Theorem 4.6].

For (b) we note that if $x \leq 2y + 3$ then, by Lemma 13, $\alpha^{2^y} \equiv 1 \pmod{\mathfrak{p}^x}$, for all α prime to \mathfrak{p} . Now choose any rational prime $p \equiv 5 \pmod{8}$ and write it in the form $p = a^2 + b^2$, where $a, b \in \mathbb{N}$. Let $\alpha_0 = a + ib$. Then $\alpha_0^{2^y} \equiv 1 \pmod{\mathfrak{p}^x}$, α_0 is prime and

$$N(\alpha_0) \equiv 5 \pmod{8}.$$

It follows from [7, Theorem 4.6] that $[G, \theta(\mathfrak{p}^x)] = \Gamma(\mathfrak{p}^x)$ and hence by Lemma 14(a) that $[G, \theta(\mathfrak{q})] = \Gamma(\mathfrak{q})$.

For (c) consider $\alpha_1 = 5 + 4i$. Now α_1 is prime, with

$$N(\alpha_1) = 41 \quad \text{and} \quad \alpha_1^4 \equiv 1 \pmod{\mathfrak{p}^9}.$$

It follows that $\alpha_1^{2^y} \equiv 1 \pmod{\mathfrak{p}^{2y+5}}$ and hence by [7, Theorem 4.6] that

$$\overline{G\theta}(\mathfrak{p}^{2y+5}) \neq 1.$$

On the other hand for any $\alpha \in A$ such that $\alpha^{2^y} \equiv 1 \pmod{\mathfrak{p}^{2y+5}}$, we have, by Lemma 13(i), $\alpha^4 \equiv 1 \pmod{\mathfrak{p}^9}$ which implies that $N(\alpha) \equiv 1 \pmod{8}$. We deduce from [7, Theorem 4.6] that $|\overline{G\theta}(\mathfrak{p}^{2y+5})|$ divides 2. Hence $|\overline{G\theta}(\mathfrak{p}^{2y+5})|$ and similarly $|\overline{G\theta}(\mathfrak{p}^{2y+4})|$ are equal to 2. The general case follows from Lemma 14.

We now come to the main result of this section.

THEOREM 16. *When $A = \mathbb{Z}[i]$, non-normal subgroups of level \mathfrak{q} exist if and only if $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})(n \geq 3)$.*

Moreover, if $\text{ord}_{\mathfrak{p}}(\mathfrak{q}) \leq 5$ and $[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$, then, for each $Y \in H(\mathfrak{q})$ such that $[G, Y] \not\subseteq \Delta(\mathfrak{q})$, the subgroup $\langle Y, \Delta(\mathfrak{q}) \rangle$ (of level \mathfrak{q}) is not normal in G .

Proof. As before, let $x = \text{ord}_{\mathfrak{p}}(\mathfrak{q})$ and $y = \text{ord}_2(n)$. We assume that

$$[G, H(\mathfrak{q})] \neq \Delta(\mathfrak{q})$$

and so n must be even (i.e., $y > 0$) by [7, Theorem 5.2(i)]. By Theorem 15 we may also assume that $4 \leq x \leq 2y + 5$.

Case 1. $x \geq 6$. Consider $\alpha = 5 + 4i$. α is prime, with $N(\alpha) = 41$, and

$$\alpha^{2^y} \equiv 1 \pmod{\mathfrak{p}^{2y+5}}.$$

Use the Chinese remainder theorem to find $Y \in \theta(\mathfrak{q})$ such that $Y \equiv \alpha I \pmod{\mathfrak{p}^x}$. Now construct $X \in \theta(\mathfrak{p}^6)$ as in Lemma 10 with $\alpha = 5 + 4i$ ($s = 1$). Since $X \equiv \alpha I \pmod{\mathfrak{p}^6}$ we have $Y = XT$, for some $T \in \Gamma(\mathfrak{p}^6)$.

Now, by Theorem 12, $C(\mathfrak{q}) \cong C(\mathfrak{p}^6)$. Choose $T_0 \in \Gamma(\mathfrak{q})$ such that $T_0 \equiv T \pmod{\Delta(\mathfrak{p}^6)}$ and consider the subgroup $S = \langle YT_0^{-1}, \Delta(\mathfrak{q}) \rangle$. If S is normal in G then so is

$$\langle YT_0^{-1}, \Delta(\mathfrak{p}^6) \rangle = \langle X, \Delta(\mathfrak{p}^6) \rangle.$$

An argument identical to that used in the proof of [7, Theorem 5.5] shows that $\langle X, \Delta(\mathfrak{p}^6) \rangle$ is not normal in G .

Case 2. $x = 4, 5$. In this case we have

$$C(\mathfrak{q}) \cong C(\mathfrak{p}^4)$$

by Theorem 12 and

$$[G, \theta(\mathfrak{q})] = \Gamma(\mathfrak{q})$$

by Theorem 15(b). Let $S = \langle Y, \Delta(\mathfrak{q}) \rangle$, where $Y \in H(\mathfrak{q})$ and $[G, Y] \not\subseteq \Delta(\mathfrak{q})$. If S is normal in G then $\Gamma(\mathfrak{q}) \leq S$. ($|C(\mathfrak{p}^4)| = 2$, by Theorem 12.)

We prove that $S \cap \Gamma(\mathfrak{q}) = \Delta(\mathfrak{q})$.

Now $Y \in H(\mathfrak{p}^4)$ and $[G, Y] \not\subseteq \Delta(\mathfrak{p}^4)$ since, by Theorem 12, $\Delta(\mathfrak{p}^4) \cap \Gamma(\mathfrak{q}) = \Delta(\mathfrak{q})$. It follows that $Y \equiv u(1 - 2i)I \pmod{\mathfrak{p}^4}$, where $u = \pm 1, \pm i$. (See the first part of the proof of Theorem 15.) Construct $X \in \theta(\mathfrak{p}^4)$ as in Lemma 10 with $\alpha = 1 + 2i$ ($s = 1$). Then by Lemma 10, $X^2 \in \Delta(\mathfrak{p}^4)$. Now $Y = uXT_1$, for some $T_1 \in \Gamma(\mathfrak{p}^4)$, from which we deduce that $Y^2 \equiv u^2I \pmod{\mathfrak{p}^4}$ ($\Gamma(\mathfrak{p}^4)$ is central $\pmod{\Delta(\mathfrak{p}^4)}$ and $|C(\mathfrak{p}^4)| = 2$). Hence, for any s , $Y^s \equiv uY^j \pmod{\Delta(\mathfrak{p}^4)}$, where $u = \pm 1, \pm i$, and $j = 0, 1$.

It follows that $Y^s \in \Gamma(\mathfrak{q})$ if and only if $Y^s \in \Delta(\mathfrak{q})$. This completes the proof of the theorem.

REFERENCES

1. H. BASS, *Algebraic K-theory*, Benjamin, New York, 1968.
2. H. BASS, J. MILNOR, J.-P. SERRE, *Solution of the congruence subgroup problem for SL_n , ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Publ. Math. I.H.E.S., vol. 33 (1967), pp. 59-137.
3. J.L. BRENNER, *The linear homogeneous group, III*, Ann. of Math., vol. 71 (1960), pp. 210-223.
4. J. GOLUBCHIK, *On the general linear group over an associative ring*, Uspekhi Mat. Nauk., vol. 28:3 (1973), pp. 179-180 (in Russian).
5. A.W. MASON, *Lattice subgroups of free congruence groups*, Glasgow Math. J., vol. 10 (1969), pp. 106-115.
6. ———, *A note on subgroups of $GL(n, A)$ which are generated by commutators*, J. London Math. Soc. (2), vol. 11 (1975), pp. 509-512.
7. ———, *On subgroups of $GL(n, A)$ which are generated by commutators. II*, J. Reine Angew. Math., vol. 322 (1981), pp. 118-135.
8. ———, *A further note on subgroups of $GL(n, A)$ which are generated by commutators*, Arch. Math., vol. 37 (1981), pp. 401-405.
9. A.W. MASON and W.W. STOTHERS, *On subgroups of $GL(n, A)$ which are generated by commutators*, Invent. Math., vol. 23 (1974), pp. 327-346.
10. L.N. VASERSTEIN, *On the stabilization of the general linear group over a ring*, Math. USSR Sbornik, vol. 8 (1969), pp. 383-400.
11. ———, *On the normal subgroups of GL_n over a ring*, Lecture Notes in Mathematics, vol. 854, Springer-Verlag 1981, 456-465.

UNIVERSITY OF GLASGOW,
GLASGOW, SCOTLAND