SOME NON-MAXIMAL ARITHMETIC GROUPS

by

Nelo D. ALLAN

Let $k$ be a non-finite Dedekind domain, and $\mathcal{O}$ be the ring of its integers. We shall assume that the ring $R = \mathcal{O}/(2)$ is finite. Let us denote by $M_n(k)$ (resp. $M_n(\mathcal{O})$) the ring of all $n$ by $n$ matrices with entries in $k$ (resp. in $\mathcal{O}$), and $GL_n(k)$ its group of units. We denote by $SL_n(k)$ the subgroup of $GL_n(k)$ whose elements $g$ have determinant, $\det g$, equal to one. Let $H \in M_n(\mathcal{O})$ be a symmetric matrix, i.e., $H = tH$ where $tH$ denotes the transpose matrix of $H$. We let $G = SO(H) = \{g \in SL_n(k) | t^gHg = H\}$, and we let $G_\mathcal{O} = G \cap M_n(\mathcal{O})$. We want to exhibit certain $H$ for which $G_\mathcal{O}$ is not maximal in $G$, in the sense that there exists a subgroup $\Delta$ of $G$ such that $\Delta$ contains $G_\mathcal{O}$ properly and $[\Delta : G_\mathcal{O}]$ is finite.

1. Preliminaries. Let $L$ be an order in $M_n(k)$; we shall denote by $L_{ij}$ the fractional ideal generated by all the $(i,j)$-entries of all the elements of $L$; we shall write

$$
L = \begin{pmatrix}
L_{11} & \cdots & L_{1n} \\
\vdots & \ddots & \vdots \\
L_{n1} & \cdots & L_{nn}
\end{pmatrix}.
$$

We shall say that $L$ is a direct summand if as an $\mathcal{O}$-module $L$ is a direct sum of $L_{ij}e_{ij}$ where $e_{ij}$ are the units of $M_n(k)$.

21
It is well known that in our case the maximal orders in $\mathbb{M}_n(k)$ are conjugate to the ones which are direct summands and $L_{nn} = L_{ij} = \epsilon^r$, $i,j \neq n$, and $L_{in} = \alpha^{-1}$, $L_{nj} = \alpha^r$, $i,j \neq n$, for some fractional ideal $\mathcal{U}$ of $k$, i.e.,

$$L = L(\mathcal{U}) = \left(\begin{array}{cccc}
\phi & \ldots & \phi \alpha^{-1} \\
\vdots & & \vdots \\
\phi & \ldots & \phi \alpha^{-1} \\
\alpha & \ldots & \alpha \phi
\end{array}\right)$$

If $L$ is one of such orders, then by looking at the expansion of $g^{-1}$, $g \in SL_n(k)$, we see that $L \mid SL_n(k)$ is a group. Consequently if $G \subset SL_n(k)$, then $\Delta = G \cap L$ is a group.

For our purposes we shall assume $\mathcal{U}$ to be integral.

**Lemma 1.** If $R = \mathcal{O}/\alpha$ is finite, then $\Delta$ is commensurable to $G_\mathcal{O}$, i.e., $\Delta \cap G_\mathcal{O}$ has finite index in both $G_\mathcal{O}$ and $\Delta$.

**Proof:** We shall follow Ramanathan's proof (1). First we consider the subgroup $\Delta(\alpha) = \{ g \in G_\mathcal{O} \mid g \equiv \epsilon \mod \mathcal{U}\}$. The index $[G_\mathcal{O} : \Delta(\alpha)]$ is finite because it is at most the order of the group $GL_n(R)$, which is clearly finite. Suppose that $g$, $g' \in \Delta$ and that $\mathcal{U}(g_{ij} - g'_{ij})$ is divisible by $\mathcal{U}^2$ for all $(i,j)$, i.e., $g' = g + V$, $V = (v_{ij})$ and $v_{ij} \equiv 0$ modulo $\mathcal{U}$ for all $(i,j)$; hence $g^{-1}g' = E + g^{-1}V$, and it is easy to see that $g^{-1}V \in M_n(\mathcal{O})$. Consequently $g^{-1}g' \in G_\mathcal{O} \cap \Delta$. Now there is only finitely many classes $\alpha L$ modulo $\mathcal{U}^2$, hence only finitely many classes $\Delta$ modulo $\Delta \cap G_\mathcal{O}$, i.e., $[\Delta : \Delta \cap G_\mathcal{O}]$ is finite. Next as $G_\mathcal{O} \supset \Delta \cap G_\mathcal{O} \supset \Delta(\alpha)$, it follows that $[G_\mathcal{O} : \Delta \cap G_\mathcal{O}]$ is finite. q.e.d.
2. MAIN RESULT. We shall use the block notation for the matrices and write
\[ H = \begin{pmatrix} V & 0 \\ 0 & W \end{pmatrix}, \]
where \( V \) is \( r \) by \( r \) and \( W \) is \( s \) by \( s \), \( r + s = n \); such \( H \) we shall denote sometimes by \( V \perp W \). If \( p^a \nmid 2 \), \( p \) prime, \( \alpha \) a positive integer, we say that \( H \) is \( p^\alpha \)-even, if for any integral \( 1 \) by \( n \) matrix \( x \),
\[ t^x H x \equiv 0 \pmod{p^\alpha}. \]
(As \( p^\alpha \nmid 2 \), to say that \( H \) is \( p^\alpha \)-even is equivalent to say that \( p^\alpha \) divides all the diagonal entries of \( H \), where \( H = (h_{ij}) \), since mod 2, and a fortiori modulo \( p^\alpha \), \( t^x H x \equiv x_1^2 h_{11} + \ldots + x_n^2 h_{nn} \).) We shall denote by \( J(a), a \in \mathcal{O} \), the matrix
\[ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}. \]
We may assume that \( 2 \nmid a \), otherwise we can replace \( J(a) \) by \( t S J(a) S = J(a + 2\lambda) = J(0) \) where
\[ S = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \]
a = 2\lambda, \( \lambda \in \mathcal{O} \): under such replacement, the maximality or not of \( G_{\mathcal{O}} \), for \( H = V \perp J(a) \), is not affected.

LEMMA 2. Let \( G = \text{SO}(H), H = V \perp J(a) \). If \( V \) is \( p^\alpha \)-even, and \( p^\alpha \nmid a \), then the \( \mathcal{O} \)-ring generated by \( G_{\mathcal{O}} \) in \( M_n(k) \) is contained in the order \( L(p) \).

Proof: Since \( G_{\mathcal{O}} \subset M_n(\mathcal{O}) \), it suffices to prove that for all \( j = 1, \ldots, n-1 \), \( p \mid g_{nj} \). If we write \( g \in G_{\mathcal{O}} \) as
\[ g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \]
A being \( n-2 \) by \( n-2 \) and \( D \) being 2 by 2, then
$tgHg = H$ implies that $tAVA + tCJ(a)C = V$ and $tBVB + tDJ(a)D = J(a)$. Let us write $V = (v_{ij})$; now $V$ is $p^\alpha$-even, so that $p^\alpha | v_{ii}$ for all $i = 1, \ldots, n-2$. Let us write $C = (x_1, \ldots, x_{n-2})$, where $x_j$ are the column vectors of $C$, and similarly $D = (y_1, y_2)$. We have

$$(tAVA)_{jj} + tx_j J(a)x_j = v_{jj}, \quad j = 1, \ldots, n-2,$$

$$(tBVB)_{jj} + ty_j J(a)y_j = \delta_j x_j, \quad j = 1, 2, \delta_{12} = 0, \delta_{22} = 1.$$

Consequently if $z = x_1, \ldots, x_{n-2}, y_1$, then

$$tzJ(a)z \equiv 0 \pmod{p^\alpha}.$$ 

Writing $z = (z_1, z_2)$, this implies that

$$2z_1z_2 + az_2^2 \equiv 0 \pmod{p^\alpha}$$

or

$$az_2^2 \equiv 0 \pmod{p^\alpha},$$

and as $p^\alpha | a$, thus $p | z_2$. This means precisely that the last row of $C$ is divisible by $p$, as well as the entry $(2,1)$ of $D$.

q.e.d.

Theorem 1. Let $V$ be $p^\alpha$-even and let $p^\alpha | a$. Suppose that we can find in $\theta$ a unit $\eta$ and an element $b$ such that $(ba/2)$ lies in $p^{-1}$ but is not integral and $\eta^2 + b\eta = 1$. Then $G_\theta$ is not maximal in $G$, in the sense explained before.

Proof: As $\theta/(2)$ is finite, we have $\theta/p$ finite and $\Delta = L(p) \cap G$ is commensurable to $G_\theta$. It suffices to show that $\Delta$ contains $G_\theta$ properly. We consider $g = E_2 \bot g^*$ with
Clearly \( g \in L(\mu) \), and it is easy to see that
\[
g' = \begin{bmatrix} \eta^{-1} & ab/2 \\ 0 & \eta \end{bmatrix}
\]
Therefore \( g \in L(\mu) \cap G \) and \( g \notin G_{\phi} \).

q.e.d.

**COROLLARY.** Let \( W \) be any unimodular matrix, i.e., \( W \in M_{n-2}(\phi) \) and \( \det W \) is a unit, and let \( c \in \phi^\times \). Let us assume also the existence of \( \eta \) and \( b \) like in the theorem. If \( H = W \perp cJ(a) \), then \( G_{\phi} \) is not maximal.

Proof: First of all, we observe that if \( \det H \neq 0 \) then \( g \in SO(H) \) if and only if \( t g \in SO(H^{-1}) \), for as \( g^{-1} \in SO(H) \), \( t g^{-1} H g^{-1} = H \) if and only if \( g H^{-1} g = H^{-1} \). Now the mapping \( g \mapsto t g \) maps subgroups onto subgroups, and preserves integrality of matrices and indices; hence \( SO(H)_{\phi} \) is not maximal if and only if \( SO(H^{-1})_{\phi} \) is not maximal. Now \( H^{-1} = W^{-1} \perp c^{-1} J(a)^{-1} \), or \( c H^{-1} = c W^{-1} \perp J(a)^{-1} \). As before our situation does not change if we replace \( J(a)^{-1} \) by \( J(0) J(a)^{-1} J(0) = J(-a) \). Hence \( SO(H)_{\phi} \) is not maximal if and only if \( SO(H')_{\phi} \) is not maximal where \( H' = c W^{-1} \perp J(-a) \). Finally it is easy to see that \( c W^{-1} \) is \( \phi^2 \)-even, consequently \( SO(H')_{\phi} \) is not maximal. Therefore, \( SO(H)_{\phi} \) is not maximal.

q.e.d.

**3. APPLICATIONS.** We shall look first into the case where \( k \) is a dyadic local field with residue class field having more than two elements. We observe the fol-
lowing trivial lemma.

**Lemma 3.** Let \( \mathfrak{p} \) be the prime of \( \mathfrak{o} \) and let \( (2) = \mathfrak{p}^\alpha, \alpha > 1 \). If \( a \in \mathfrak{p} \), then the equation \( x^2 + ax + 1 = 0 \) is always solvable in \( \mathfrak{o} \), and its solution is a unit.

Proof: In \( \mathfrak{o} / \mathfrak{p} \) our equation become \( x^2 - 1 = 0 \). By Hensel's lemma \( x^2 + ax - 1 = 0 \) is always solvable in \( \mathfrak{o} \), \( a \in \mathfrak{p} \), and its solution does not lie in \( \mathfrak{p} \).

q.e.d.

Now we discuss the unramified case:

**Theorem 2.** If \( k \) is an unramified dyadic field, then \( G_{\mathfrak{p}} \) is not maximal in \( G \) for \( H = V \downarrow cJ(e) \) if

a) \( V \) is even, \( 2 \uparrow e \) and \( c = 1 \).

b) \( V \) is unimodular, \( c = 2 \) and \( 2 \uparrow e \).

Proof: We first observe that in theorem 1 we can take \( b = \mathfrak{q} - \mathfrak{q} \) and \( x = \mathfrak{q} \). It remains to show that we can always choose \( \eta \) such that \( 2 \uparrow b \). Now \( \mathfrak{o} / \mathfrak{p} \) is a finite dimensional vector space over the prime field, hence its group of units has odd order, i.e., if \( \eta \neq 1 \) (modulo 2), then \( \eta^2 \neq 1 \) (modulo 2).

q.e.d.

**Theorem 3.** Let \( k \) be a dyadic ramified field. Then \( G_{\mathfrak{p}} \) is not maximal in \( G \), for \( H = V \downarrow cJ(a) \), if

a) \( V \) is \( \pi^\lambda \)-even, \( c = 1 \), \( a = e\pi^\beta \), \( e \) unit and \( \alpha > \lambda > \beta > 0 \).

b) \( V \) is unimodular, \( c = \pi^\lambda \), \( a = e\pi^\beta \), \( e \) unit and \( \alpha > \lambda > \beta > 0 \).
Proof: In order to verify our assertion we find a solution \( \eta \) of \( x^2 + \pi^{d-\beta-1}x = 1 \) and set \( b = \pi^{d-\beta-1} \) and \( \eta = x \) in the proof of theorem 1, in the case where \( d > \beta + 1 \). In the case where \( d = \beta + 1 \), we consider the equation \( x^2 + bx = 1 \), \( b = \eta^{-1} - \eta \), \( x = \eta \) where \( \eta \) is a unit such that \( \mathfrak{p} \mid \eta^{-1} \eta \). It is always possible to find such unit because \( \mathfrak{O}/\mathfrak{p} \) has more than two elements. The case b) follows from the corollary and from a).

q.e.d.

Now we shall study some consequences for the case \( k \) is an algebraic number field.

**Theorem 4.** Suppose that 2 is unramified in \( k \) and that there exists a unit \( \eta \in \mathfrak{O} \) such that \( \eta \neq 1 \) (modulo 2). Then \( \mathfrak{O} \) is not maximal in \( G \) for \( H = V \perp \text{cJ(a)} \) in the following cases:

a) \( V \) is even, \( c = 1 \), \( a = \text{unit} \).

b) \( V \) is unimodular, \( c = 2 \), \( a = \text{unit} \).

Proof: Clearly the case b) follows from a) by corollary of theorem 1. Next we observe that we can sharpen lemma 2, to get the \( \mathfrak{O} \)-ring generated by \( G \) contained in \( L(2) \); as \( V \) is even, we can work all congruences of that lemma modulo 2, and from the last congruence \( az^2 \equiv 0 \) (modulo 2) we get that \( z^2 \equiv 0 \) (modulo 2), because if \( \mathfrak{p} \mid 2 \), then \( \mathfrak{p}^2 \mid 2 \). Hence \( 2 \mid g_{nj} \), \( j \neq n \), for all \( g = (g_{ij}) \in G \). Now in the proof of theorem 1 it suffices to take \( b = \eta^{-1} - \eta \), \( x = \eta \), and it is easily seen that \( ab \) is relatively prime to 2.

q.e.d.

**Corollary.** If \( k \) is a quadratic number field with
discriminant \ a, \ a \equiv 5 \text{(modulo } 8), \text{ and if the basic unit of } k \text{ is } \omega = (m + n\sqrt{a})/2, \ m,n \text{ being odd integers, then we have the same conclusion as in theorem 4.}

Proof: For \ \omega^{-1} - \omega = -m \text{ or } \sqrt{a} \text{ and in both cases } 2\n\omega^{-1} - \omega.

We close this note observing that our last corollary applies to the case where

\[ a = -3, 5, 13, 21, 29, 53, 61, 69, 77, 85, 93. \]

(See table 1, (2)).

REFERENCES


Departamento de Matemáticas
y Estadística
Universidad Nacional de Colombia
(Recibido en febrero de 1968)

ERRATA: Lines 12 and 13, page 23, should read: "2, and \_fortiori \ modulo } f^\omega x, \ t_x h = x_1^2 h_1 + ... + x_n^2 h_n, \text{ where } t_x = (x_1, ..., x_n)."