Revista Colombiana de Matemáticas
Volumen II, 1968, págs. 21- 28

SOME NON-MAXIMAL ARITHMETIC GROUPS

by

Nelo D. ALLAN

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

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

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

It is well known that in our case the maximal orders in $M_n(k)$ are conjugate to the ones which are direct summands and $L_{nn} = L_{ij} = \mathfrak{o}$, $i,j \neq n$, and $L_{in} = \mathfrak{a}^{-1}$, $L_{nj} = \mathfrak{a}$, $i,j \neq n$, for some fractional ideal $\mathfrak{a}$ of k, i.e.,

$$L = L(\mathfrak{a}) = \begin{pmatrix} \mathfrak{o} & \dots & \mathfrak{o} & \mathfrak{a}^{-1} \\ \vdots & & \vdots & \vdots \\ \mathfrak{o} & \dots & \mathfrak{o} & \mathfrak{a}^{-1} \\ \mathfrak{a} & \dots & \mathfrak{a} & \mathfrak{o} \end{pmatrix}$$

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

For our purposes we shall assume $\mathfrak{a}$ to be integral.

LEMMA 1. <u>If</u> $R = \mathfrak{o}/\mathfrak{a}$ <u>is finite, then</u> Δ <u>is commensurable to</u> $G_{\mathfrak{o}}$, i.e., $\Delta \cap G_{\mathfrak{o}}$ <u>has finite index in both</u> $G_{\mathfrak{o}}$ <u>and</u> Δ.

Proof: We shall follow Ramanathan's proof [1]. First we consider the subgroup $\Delta(\mathfrak{a}) = \{ g \in G_{\mathfrak{o}} \mid g \equiv E \bmod \mathfrak{a}\}$. The index $[G_{\mathfrak{o}} : \Delta(\mathfrak{a})]$ is finite because it is at most the order of the group $G\ell_n(R)$, which is clearly finite. Suppose that $g, g' \in \Delta$ and that $\mathfrak{a}(g_{ij} - g'_{ij})$ is divisible by $\mathfrak{a}^2$ for all (i,j), i.e., $g' = g + V$, $V = (v_{ij})$ and $v_{ij} \equiv 0$ modulo $\mathfrak{a}$ for all (i,j); hence $g^{-1}g' = E + g^{-1}V$, and it is easy to see that $g^{-1}V \in M_n(\mathfrak{o})$. Consequently $g^{-1}g' \in G_{\mathfrak{o}} \cap \Delta$. Now there is only finitely many classes $\mathfrak{a}L$ modulo $\mathfrak{a}^2$, hence only finitely many classes Δ modulo $\Delta \cap G_{\mathfrak{o}}$, i.e., $[\Delta : \Delta \cap G_{\mathfrak{o}}]$ is finite. Next as $G_{\mathfrak{o}} \supset \Delta \cap G_{\mathfrak{o}} \supset \Delta(\mathfrak{a})$, it follows that $[G_{\mathfrak{o}} : \Delta \cap G_{\mathfrak{o}}]$ 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 $\mathfrak{p}^\alpha | 2$, $\mathfrak{p}$ prime, α a positive integer, we say that H is $\mathfrak{p}^\alpha$-even, if for any integral 1 by n matrix x, ${}^t xHx \equiv 0$ (modulo $\mathfrak{p}^\alpha$). (As $\mathfrak{p}^\alpha | 2$, to say that H is $\mathfrak{p}^\alpha$-even is equivalent to say that $\mathfrak{p}^\alpha$ divides all the diagonal entries of H, where $H = (h_{ij})$, since mod 2, and _a fortiori_ modulo $\mathfrak{p}^\alpha$, ${}^t xHx \equiv x_1^2 h_{11} + \dots + x_n^2 h_{nn}$.) We shall denote by $J(a)$, $a \in \mathfrak{o}$, the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}.$$

We may assume that $2 \nmid a$, otherwise we can replace $J(a)$ by ${}^t SJ(a)S = J(a + 2\lambda) = J(0)$ **where**

$$S = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

$a = -2\lambda$, $\lambda \in \mathfrak{o}$: under such replacement, the maximality or not of $G_{\mathfrak{o}}$, for $H = V \perp J(a)$, is not affected.

LEMMA 2. _Let_ $G = SO(H)$, $H = V \perp J(a)$. _If_ V _is_ $\mathfrak{p}^\alpha$_-even, and_ $\mathfrak{p}^\alpha \nmid a$, _then the_ $\mathfrak{o}$_-ring generated by_ $G_{\mathfrak{o}}$ _in_ $M_n(k)$ _is contained in the order_ $L(\mathfrak{p})$.

Proof: Since $G_{\mathfrak{o}} \subset M_n(\mathfrak{o})$, it suffices to prove that for all $j = 1, \dots, n-1$, $\mathfrak{p} | g_{nj}$. If we write $g \in G_{\mathfrak{o}}$ as

$$g = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

A being $n-2$ by $n-2$ and D being 2 by 2, then

${}^t gHg = H$ implies that ${}^t AVA + {}^t CJ(a)C = V$ and ${}^t BVB + {}^t DJ(a)D = J(a)$. Let us write $V = (v_{ij})$; now V is $\mathfrak{p}^\alpha$-even, so that $\mathfrak{p}^\alpha | v_{ii}$ 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

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

$$({}^t BVB)_{jj} + {}^t y_j J(a) y_j = \delta_{j2} a, \quad j=1,2, \ \delta_{12}=0, \ \delta_{22}= 1.$$

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

$$ {}^t zJ(a)z \equiv 0 \quad (\text{modulo } \mathfrak{p}^\alpha).$$

Writting ${}^t z = {}^t(z_1, z_2)$, this implies that

$$2z_1 z_2 + az_2^2 \equiv 0 \ (\text{modulo } \mathfrak{p}^\alpha)$$

or

$$az_2^2 \equiv 0 \ (\text{modulo } \mathfrak{p}^\alpha),$$

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

q.e.d.

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

Proof: As $\mathfrak{o}/(2)$ is finite, we have $\mathfrak{o}/\mathfrak{p}$ finite and $\Delta = L(\mathfrak{p}) \cap G$ is commensurable to $G_{\mathfrak{o}}$. It suffices to show that Δ contains $G_{\mathfrak{o}}$ properly. We consider $g = E_{n-2} \perp g'$ with

$$g' = \begin{bmatrix} \eta^{-1} & ab/2 \\ 0 & \eta \end{bmatrix}$$

Clearly $g \in L(\mathfrak{p})$, and it is easy to see that

$${}^t g' J(a) g' = J(ab\eta + \eta^2 a) = J(a(b\eta + \eta^2)) = J(a).$$

Therefore $g \in L(\mathfrak{p}) \cap G$ and $g \notin G_{\mathfrak{o}}$.

q.e.d.

COROLLARY. *Let W be any unimodular matrix, i.e.,* $W \in M_{n-2}(\mathfrak{o})$ *and* $\det W$ *is a unit, and let* $c \in \mathfrak{p}^{\alpha}$. *Let us assume also the existence of* η *and* b *like in the theorem. If* $H = W \perp cJ(a)$, *then* $G_{\mathfrak{o}}$ *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 $gH^{-1}g = H^{-1}$. Now the mapping $g \rightsquigarrow {}^t g$ maps subgroups onto subgroups, and preserves **integrality** of matrices and indices; hence $SO(H)_{\mathfrak{o}}$ is not maximal if and only if $SO(H^{-1})_{\mathfrak{o}}$ is not maximal. Now $H^{-1} = W^{-1} \perp c^{-1}J(a)^{-1}$, or $cH^{-1} = cW^{-1} \perp J(a)^{-1}$. As before our situation does not change if we replace $J(a)^{-1}$ by $J(0)J(a)^{-1}J(0) = J(-a)$. Hence $SO(H)_{\mathfrak{o}}$ is not maximal if and only if $SO(H')_{\mathfrak{o}}$ is not maximal where $H' = cW^{-1} \perp J(-a)$. Finally it is easy to see that cW^{-1} is $\mathfrak{p}^{\alpha}$-even, consequently $SO(H')_{\mathfrak{o}}$ is not maximal. Therefore, $SO(H)_{\mathfrak{o}}$ 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 $(2) = \mathfrak{p}^{\alpha}$, $\alpha \geq 1$. 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 $G_{\mathfrak{o}}$ is not maximal in G for $H = V \perp cJ(\varepsilon)$ if

a) V is even, $2 \nmid \varepsilon$ and $c = 1$.

b) V is unimodular, $c = 2$ and $2 \nmid \varepsilon$.

Proof: We first observe that in theorem 1 we can take $b = \eta^{-1} - \eta$ and $x = \eta$. It remains to show that we can always choose η such that $2 \nmid b$. 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 $\eta \not\equiv 1$(modulo 2), then $\eta^2 \not\equiv 1$(modulo 2).

q.e.d.

THEOREM 3. Let k be a dyadic ramified field. Then $G_{\mathfrak{o}}$ is not maximal in G, for $H = V \perp cJ(a)$, if

a) V is π^{λ}-even, $c = 1$, $a = \varepsilon\pi^{\beta}$, ε unit and $\alpha \geq \lambda > \beta > 0$.

b) V is unimodular, $c = \pi^{\lambda}$, $a = \varepsilon\pi^{\beta}$, ε unit and $\alpha \geq \lambda > \beta > 0$.

Proof: In order to verify our assertion we find a solution η of $x^2 + \pi^{\alpha-\beta-1}x = 1$ and set $b = \pi^{\alpha-\beta-1}$ and $\eta = x$ in the proof of theorem 1, in the case where $\alpha > \beta + 1$. In the case where $\alpha = \beta + 1$, we consider the equation $x^2 + bx = 1$, $b = \eta^{-1} - \eta$, $x = \eta$ where η is a unit such that $\mathfrak{p} \nmid \eta^{-1} - \eta$. 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 $\eta \not\equiv 1$ (modulo 2). Then $G_{\mathfrak{o}}$ is not maximal in G for $H = V \perp cJ(a)$ in the following cases:

a) V is even, $c = 1$, $a =$ unit.

b) V is unimodular, $c = 2$, $a =$ 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 $az_2^2 \equiv 0$ (modulo 2) we get that $z_2 \equiv 0$ (modulo 2), because if $\mathfrak{p} | 2$, then $\mathfrak{p}^2 \nmid 2$. Hence $2 | g_{nj}$, $j \neq n$, for all $g = (g_{ij}) \in G_{\mathfrak{o}}$. 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, $a \equiv 5$ (modulo 8), and if the basic unit of k is $\omega = (m + n\sqrt{a})/2$, m,n being odd integers, then we have the same conclusion as in theorem 4.

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

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

1. K. RAMANATHAN, Discontinuos Groups F, Goeth. Nach. (1964), 145-164.

2. Z. BOREVICH, I. SHAFAREVICH, Number Theory, Academic Press, 1966, New York.

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 *a fortiori* modulo $\mathfrak{p}^{\alpha}$, ${}^{t}xHx \equiv x_1^2 h_{11} + \ldots + x_n^2 h_{nn}$, where ${}^{t}x = (x_1, \ldots, x_n)$.)"