Werk

Titel: Some non-maximal arithmetic groups

Autor: Allan, N.

Jahr: 1968

PURL: https://resolver.sub.uni-goettingen.de/purl?320387429_0002|log12

Kontakt/Contact

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 ele-
ments 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 $G =$
$SO(H) = \left\{ g \in Sl_n(k) \mid {}^tgHg = H \right\}$, 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 sub-
group Δ of G such that Δ contains $G_{\mathcal{O}}$ properly and
$[\Delta : G_{\mathcal{O}}]$ is finite.

1. <u>Preliminaries</u>. 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 $\mathcal{O}$-mo-
dule 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 $L_{nn} = L_{ij} = \mathcal{O}$, $i,j \neq n$, and $L_{in} = \mathcal{U}^{-1}$, $L_{nj} = \mathcal{U}$, $i,j \neq n$, for some fractional ideal $\mathcal{U}$ of k, i.e.,

$$L = L(\mathcal{U}) = \begin{pmatrix} \mathcal{O} & \cdots & \mathcal{O} & \mathcal{U}^{-1} \\ \vdots & & \vdots & \vdots \\ \mathcal{O} & \cdots & \mathcal{O} & \mathcal{U}^{-1} \\ \mathcal{U} & \cdots & \mathcal{U} & \mathcal{O} \end{pmatrix}$$

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 $L \parallel S\ell_n(k)$ 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 $\mathcal{U}$ to be integral.

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

Proof: We shall follow Ramanathan's proof [1]. First we consider the subgroup $\Delta(\mathcal{U}) = \{ g \in G_{\mathcal{O}} \mid g \equiv E \bmod \mathcal{U} \}$. The index $[G_{\mathcal{O}}: \Delta(\mathcal{U})]$ 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 $\mathcal{U}(g_{ij} - g'_{ij})$ 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 aL modulo $\mathcal{U}^2$, hence only finitely many classes Δ modulo $\Delta \cap G_{\mathcal{O}}$, i.e., $[\Delta : \Delta \cap G_{\mathcal{O}}]$ is finite. Next as $G_{\mathcal{O}} \supset \Delta \cap G_{\mathcal{O}} \supset \Delta(\mathcal{U})$, 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 $p^\alpha | 2$, p prime, α a positive integer, we say that H is p^α-even, if for any integral 1 by n matrix x, $^t x H x \equiv 0 (\mathrm{modulo}\ p^\alpha)$. (As $p^\alpha | 2$, to say that H is p^α-even is equivalent to say that p^α divides all the diagonal entries of H, where $H = (h_{ij})$, since mod 2, and a fortiori modulo p^α, $^t x H x \equiv x_1^2 h_{11} + \ldots + x_n^2 h_{nn}$.) 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 $G = SO(H)$, $H = V \perp J(a)$. If V is p^α-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 $j = 1, \ldots, n-1$, $p | g_{nj}$. 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

$^t gHg = H$ implies that $^tAVA + {}^tCJ(a)C = V$ and $^tBVB + {}^tDJ(a)D = J(a)$. Let us write $V = (v_{ij})$; now V is $\not p^\alpha$-even, so that $\not p^\alpha | v_{ii}$ 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

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

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

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

$$^tzJ(a)z \equiv 0 \quad (\text{modulo } \not p^\alpha).$$

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

$$2z_1 z_2 + az_2^2 \equiv 0 \quad (\text{modulo } \not p^\alpha)$$

or

$$az_2^2 \equiv 0 \quad (\text{modulo } \not p^\alpha),$$

and as $\not p^\alpha \nmid a$, thus $\not p | z_2$. This means precisely that the last row of C is divisible by $\not p$, as well as the entry $(2,1)$ of D.

<div align="right">q.e.d.</div>

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

Proof: As $\mathcal{O}/(2)$ is finite, we have $\mathcal{O}/\not p$ finite and $\Delta = L(\not q) \cap G$ is commensurable to $G_{\mathcal{O}}$. It suffices to show that Δ contains $G_{\mathcal{O}}$ properly. We consider $g = E_{n-2} \perp g'$ with

<div align="left">24</div>

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

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 $g \notin G_{\mathscr{O}}$.

<div align="right">q.e.d.</div>

COROLLARY. Let W <u>be any unimodular matrix,i.e$;$,</u> $W \in M_{n-2}(\mathscr{O})$ <u>and</u> det W <u>is a unit, and let</u> $c \in \mathfrak{p}^\alpha$. <u>Let us assume also the existence of</u> η <u>and</u> b <u>like in the theorem</u>. <u>If</u> $H = W \perp cJ(a)$, <u>then</u> $G_{\mathscr{O}}$ <u>is not maximal.</u>

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 $SO(H)_{\mathscr{O}}$ is not maximal if and only if $SO(H^{-1})_{\mathscr{O}}$ 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 $SO(H)_{\mathscr{O}}$ is not maximal if and only if $SO(H')_{\mathscr{O}}$ 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 $SO(H')_{\mathscr{O}}$ is not maximal. Therefore, $SO(H)_{\mathscr{O}}$ is not maximal.

<div align="right">q.e.d.</div>

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 $\mathcal{O}$ 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 $\mathcal{O}$, and its solution is a u-nit.

Proof: In $\mathcal{O}/\mathfrak{p}$ our equation become $x^2 - 1 = 0$. By Hensel's lemma $x^2 + ax - 1 = 0$ is always solvable in $\mathcal{O}$, $a \in \mathfrak{p}$, 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 $G_{\mathcal{O}}$ 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 $\mathcal{O}/\mathfrak{p}$ is a finite dimensional vector space over the prime field, hence its group of units has odd order, i.e., if $\eta \not\equiv 1 (\text{modulo } 2)$, then $\eta^2 \not\equiv 1 (\text{modulo } 2)$.

q.e.d.

THEOREM 3. Let k be a dyadic ramified field. Then $G_{\mathcal{O}}$ 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 $\alpha \geq \lambda > \beta > 0$.

26

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 $\not{p} \uparrow \eta^{-1} - \eta$. It is always possible to find such unit because $\mathscr{O}/\not{p}$ 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 $\eta \in \mathscr{O}$ such that $\eta \not\equiv 1$ (modulo 2). Then $G_{\mathscr{O}}$ 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 $\mathscr{O}$-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 $\not{p}|2$, then $\not{p}^2 \dagger 2$. Hence $2|g_{nj}$, $j \neq n$, for all $g = (g_{ij}) \in G_{\mathscr{O}}$. 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), <u>and if the basic</u>
<u>unit of</u> k <u>is</u> $\omega = (m + n\sqrt{a})/2$, m,n <u>being odd inte-</u>
<u>gers,</u> <u>then we have the same conclusion as in theorem</u>
<u>4</u>.

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, Acade-
      mic Press, 1966, New York.

Departamento de Matemáticas
y Estadística
Universidad Nacional de Colombia

ERRATA: Lines 12 and 13, page 23, should read: " 2, and <u>a</u>
<u>fortiori</u> modulo φ^α, ${}^t xHx = x_1^2 h_{11} + \ldots + x_n^2 h_{nn}$, where
${}^t x = (x_1, \ldots, x_n).)$ "