Y. Kitaoka and H. Suzuki
Nagoya Math. J.
Vol. 142 (1996), 183–188

FINITE ARITHMETIC SUBGROUPS OF GL_n, IV

YOSHIYUKI KITAOKA AND HIROSHI SUZUKI

In this paper, we improve a result of the third paper of this series, that is we show

THEOREM. *Let K be a nilpotent extension of the rational number field $\mathbf{Q}$ with Galois group Γ, and G a Γ-stable finite subgroup of $GL_n(O_K)$. Then G is of A-type.*

Here, automorphisms in Γ act entry-wise on matrices in G, and G being Γ-stable means that $\sigma(g) \in G$ for every $\sigma \in \Gamma$ and $g \in G$. O_K stands for the ring of integers in K and G being of A-type means the following:

Let $L = \mathbf{Z}[e_1, \ldots, e_n]$ be a free module over $\mathbf{Z}$ and we make $g = (g_{ij}) \in G$ act on $O_K L$ by $g(e_i) = \sum_{j=1}^{n} g_{ij} e_j$. Then there exists a decomposition $L = \bigoplus_{i=1}^{k} L_i$ such that for every $g \in G$, we can take a root of unity $\varepsilon_i(g)\,(1 \le i \le k)$ and a permutation $s(g)$ so that $\varepsilon_i(g) g L_i = L_{s(g)(i)}$ for $i = 1, \ldots, k$. (The definition of A-type in the third paper [3] of this series is wrong, but the results in it are true in the above sense of A-type. See the correction at the end.) We denote the identity matrix of size n by 1_n, and the ring of rational integers by $\mathbf{Z}$.

LEMMA 1. *Let F be an abelian extension of $\mathbf{Q}$ with Galois group Γ, and $\mathfrak{J}$ an integral ideal ($\neq O_F$) of F. Let G be a Γ-stable finite subgroup of $GL_n(O_F)$. Then G is of A-type, and for a subgroup*

$$G(\mathfrak{J}) := \{g \in G \mid g \equiv 1_n \bmod \mathfrak{J}\},$$

there exists an integral matrix $T \in GL_n(\mathbf{Z})$ such that $\{TgT^{-1} \mid g \in G(\mathfrak{J})\}$ consists of diagonal matrices.

Proof. It is clear that

Received April 3, 1995.
Partially supported by Grand-in-Aid for Scientific Research, The Ministry of Education, Science, Sports and Culture, Japan.

$$S := \sum_{g \in G} g\,{}^t\bar{g}$$

is a rational integral positive definite matrix, where the bar denotes the complex conjugation. We introduce a lattice $L := \mathbf{Z}[e_1, \ldots, e_n]$ with bilinear form $(B(e_i, e_j)) := S$ and consider the scalar extension $O_F L$ with $B(\lambda x, \mu y) := \lambda\bar{\mu}\, B(x, y)$ for $\lambda, \mu \in O_F$ and $x, y \in L$. Then L, $O_F L$ are a positive definite quadratic lattice over $\mathbf{Z}$ and a positive definite Hermitian lattice over O_F, respectively. Let

$$L := L_1 \perp \cdots \perp L_a$$

be the decomposition to indecomposable lattices. We define an automorphism ϕ_g: $O_F L \to O_F L$ by

$$(\phi_g(e_1), \ldots, \phi_g(e_n)) := (e_1, \ldots, e_n)\,{}^t g \quad \text{i.e., } \phi_g(e_i) = \sum_{j=1}^{n} g_{ij} e_j.$$

Then ϕ_g is an isometry of $O_F L$ by $(B(\phi_g(e_i), \phi_g(e_j)) = gS\,{}^t\bar{g} = S$. Hence by [1], there exist a root of unity $\varepsilon_i \in F$ and a permutation $\sigma \in \mathfrak{S}_a$ such that

$$\varepsilon_i \phi_g(L_i) = L_{\sigma(i)} \quad \text{for } i = 1, \ldots, a, \tag{1}$$

which implies that G is of A-type. Here assuming $g \in G(\mathfrak{J})$, we have

$$\phi_g(x) \equiv x \bmod \mathfrak{J}L, \tag{2}$$

and hence the permutation σ in (1) is the identity. Now we take a basis $\{z_1, \ldots, z_s\}$ of L_k for an integer k with $1 \leq k \leq a$. Then there exist a root of unity $\varepsilon \in F$ and $A \in GL_s(\mathbf{Z})$ satisfying

$$(\varepsilon\phi_g(z_1), \ldots, \varepsilon\phi_g(z_s)) = (z_1, \ldots, z_s)\,{}^t A. \tag{3}$$

Let $\mathfrak{P}$ be a prime ideal dividing $\mathfrak{J}$ and p the rational prime number dividing $\mathfrak{P}$. At first, we claim that we can choose the matrix A so that

$$A \equiv 1_s \bmod p.$$

By virtue of (2), (3), we have

$$\varepsilon^{-1} A \equiv 1_s \bmod \mathfrak{P}, \tag{4}$$

which implies, by putting $A = (a_{ij})$

$$a_{ij} \equiv 0 \bmod p \text{ if } i \neq j, \quad a_{ii} \equiv \varepsilon \bmod \mathfrak{P} \text{ for every } i,$$

and then we have

(5) $$A \equiv a_{11} 1_s \bmod p.$$

Hence the claim is clear if $p = 2$, and hereafter we assume $p > 2$. $\varepsilon^{-1}A(\equiv 1_s \bmod \mathfrak{P})$ is of finite order, and the order is a power of p, say p^r. Then we have $\varepsilon^{p^r} 1_s = A^{p^r}$, which is a rational integral matrix. Thus $A^{p^r} = \pm 1_s$ is clear. If $A^{p^r} = -1_s$, then by replacing ε, A by $-\varepsilon$, $-A$ in (3), respectively, we may assume $A^{p^r} = 1_n$ and $\varepsilon^{p^r} = 1$. If $\varepsilon = 1$, (4) implies the claim. Otherwise, let $\mathfrak{p}$ be the prime ideal of $\mathbf{Q}(\varepsilon)$ under $\mathfrak{P}$; then (4) implies $a_{ii} \equiv \varepsilon \bmod \mathfrak{p}$. Now $\mathfrak{p} = (1 - \varepsilon)$ yields $a_{ii} \equiv 1 \bmod \mathfrak{p}$ and hence $a_{ii} \equiv 1 \bmod p$. Thus we have shown the claim.

Next we claim that we can take 1_s as A. Since A is of finite order, the claim above yields $A = 1_s$ if $p > 2$. Suppose $p = 2$. By virtue of $A \equiv 1_s \bmod 2$ and $x = (x + \varepsilon\phi_g(x))/2 + (x - \varepsilon\phi_g(x))/2$, we have $L_k = L_+ \perp L_-$, where $L_\pm = \{x \in L_k \mid \varepsilon\phi_g(x) = \pm x\}$. Since L_k is indecomposable, we have $L_k = L_+$ or L_-, which means $A = \pm 1_s$. If necessary, by replacing ε, A by $-\varepsilon$, $-A$ in (3), respectively, we may assume $A = 1_s$. Thus we have shown the claim. Hence we have only to take a matrix T as a transformation matrix from the original basis $\{e_1, \ldots, e_n\}$ of L to the one consisting of bases of L_k $(k = 1, \ldots, a)$. □

Definition. Let K be a Galois extension of $\mathbf{Q}$ with Galois group Γ and $\mathfrak{P}$ a prime ideal. Then we put, for a non-negative integer m

$$V_m(\mathfrak{P}; K/\mathbf{Q}) := \{u \in \Gamma \mid u(x) \equiv x \bmod \mathfrak{P}^{m+1} \text{ for } x \in O_K\}.$$

Lemma 2. *Let K be a Galois extension of $\mathbf{Q}$ with Galois group Γ, and $\mathfrak{P}$ a prime ideal of K, and suppose $\Gamma = V_1(\mathfrak{P}; K/\mathbf{Q})$. Let F be the maximal abelian extension of $\mathbf{Q}$ contained in K. Let G be a Γ-stable finite subgroup of $GL_n(O_K)$ and k a non-negative integer. Suppose that $G(\mathfrak{P}^{k+1})$ consists of diagonal matrices. Then we have $G(\mathfrak{P}^k) \subset GL_n(O_F)$.*

Proof. We take and fix an element $g \in G(\mathfrak{P}^k)$. Let us see, for $\sigma \in \Gamma$

$$\sigma(g) \equiv g \bmod \mathfrak{P}^{k+1}.$$

If $k = 0$, it is clear because of $\Gamma = V_1(\mathfrak{P}; K/\mathbf{Q})$. Suppose $k > 0$. Putting $g = 1_n + \pi^k A$ with $A \in M_n(O_\mathfrak{P})$, where π is a prime element in the completion $O_\mathfrak{P}$ of O_K at the prime $\mathfrak{P}$, we have

$$\sigma(\pi^k) \equiv \pi^k \bmod \mathfrak{P}^{k+1}, \quad \sigma(A) \equiv A \bmod \mathfrak{P}^2$$

and hence

$$\sigma(g) \equiv g \bmod \mathfrak{P}^{k+1} \quad \text{and} \quad \sigma(g)g^{-1} \in G(\mathfrak{P}^{k+1}).$$

Thus $D_\sigma := \sigma(g)g^{-1}$ is diagonal and it is easy to see

$$D_{\mu\sigma} = \mu(D_\sigma)D_\mu \quad \text{for } \sigma, \mu \in \Gamma.$$

By Lemma 1 in [3], there exists a diagonal matrix $D \in GL_n(K)$, which satisfies

$$D^w \in GL_n(\mathbf{Q}) \quad \text{and} \quad D_\sigma = \sigma(D^{-1})D,$$

where w is the number of roots of unity in K. Then $\sigma(g)g^{-1} = \sigma(D^{-1})D$ for every $\sigma \in \Gamma$ yields $h := Dg \in GL_n(\mathbf{Q})$. We choose a rational diagonal matrix h_1 so that the greatest common divisor of entries of each row of $h_1 h$ is 1. Since $g = D^{-1}h = (h_1 D)^{-1}h_1 h$ and $g \in GL_n(O_K)$, all diagonal entries of the diagonal matrix $h_1 D$ are units in O_K. Moreover we know that $(h_1 D)^w = h_1^w D^w$ is rational, and so all diagonal entries of $(h_1 D)^w$ are ± 1, which means that all diagonal entries of $h_1 D$ are roots of unity in K. Thus we have $g = (h_1 D)^{-1}h_1 h \in GL_n(F)$. □

LEMMA 3. *Keeping everything in Lemma 2, we have $G \subset GL_n(O_F)$.*

Proof. By Lemma 1, we may assume that $G(\mathfrak{P}) \cap M_n(F)$ consists of diagonal matrices. We take a sufficiently large integer k so that $G(\mathfrak{P}^k) = \{1_n\}$; then Lemma 2 yields $G(\mathfrak{P}^{k-1}) \subset G(\mathfrak{P}) \cap M_n(F)$ and then $G(\mathfrak{P}^{k-1})$ consists of diagonal matrices, too. By iterating this operation, we see that $G(\mathfrak{P})$ consists of diagonal matrices and then Lemma 2 yields $G \subset GL_n(O_F)$.

LEMMA 4. *Let K be a nilpotent extension of $\mathbf{Q}$ with Galois group Γ and suppose that 2 is the only ramified rational prime. Denoting a prime ideal of K lying over 2 by $\mathfrak{P}$, we have $\Gamma = V_1(\mathfrak{P}; K/\mathbf{Q})$.*

Proof. Let $\Phi(\Gamma)$ be the Frattini subgroup of Γ. Then it contains the commutator subgroup and the subfield $F\,(\neq \mathbf{Q})$ corresponding to $\Phi(\Gamma)$ is an abelian extension of $\mathbf{Q}$ and 2 is the only ramified prime number. Let $\mathfrak{p}$ be a prime ideal of F lying over 2. Then $V_0(\mathfrak{p}; F/\mathbf{Q})$ is induced by $V_0(\mathfrak{P}; K/\mathbf{Q})$ and hence $V_0(\mathfrak{P}; K/\mathbf{Q})\Phi(\Gamma)/\Phi(\Gamma) = V_0(\mathfrak{p}; F/\mathbf{Q})$. $V_0(\mathfrak{p}; F/\mathbf{Q}) = \mathrm{Gal}(F/\mathbf{Q})$ yields $V_0(\mathfrak{P}; K/\mathbf{Q})\cdot\Phi(\Gamma) = \Gamma$ and the property of the Frattini subgroup implies $V_0(\mathfrak{P}; K/\mathbf{Q}) = \Gamma$. Hence $\mathfrak{P}$ is fully ramified and the order of the quotient group $V_0(\mathfrak{P}; K/\mathbf{Q})/V_1(\mathfrak{P}; K/\mathbf{Q})$ divides $N\mathfrak{P} - 1 = 1$, which means $V_0(\mathfrak{P}; K/\mathbf{Q}) = V_1(\mathfrak{P}; K/\mathbf{Q})$. □

Proof of Theorem. We use induction on the degree $[K:\mathbf{Q}]$. By virtue of Lemma 3 in [3], we may assume that the number of ramified rational prime number is one, and let it be p. We claim that G is contained in $GL_n(F)$, where F is the maximal abelian subfield of K. Then Theorem on p. 142 in [1] completes the proof. If p is odd, then K is a cyclic extension of $\mathbf{Q}$ as in [3] and so the claim is obvious. Suppose $p = 2$; then Lemma 3 and Lemma 4 yield that G is contained in $GL_n(F)$.

□

Remark. It is a problem to consider a general algebraic number field as a base field instead of $\mathbf{Q}$. Let K/F be a Galois extension of algebraic number fields, and G a $\mathrm{Gal}(K/F)$-stable finite subgroup of $GL_n(O_K)$. If K is totally real, then one generalization of the notion of being A-type is that G is already in $GL_n(O_F)$. But this is not adequate because there exists a counter-example when K/F is unramified. Nevertheless, it seemed not necessarily to be off the point, since the existence of a certain kind of element in G induces the existence of a proper intermediate subfield of K unramified over F. So, we asked the role of the existence of an unramified proper intermediate field. (c.f. p. 261 in [2].) But D. A. Malinin gave a following example in [4]: Set

$$K = \mathbf{Q}(\alpha, \beta),\ F = \mathbf{Q}(\alpha\beta) \quad \text{for } \alpha = \sqrt{2 + \sqrt{2}},\ \beta = \sqrt{3 + \sqrt{2}}.$$

Then K/F is not unramified and for

$$g = (g_{ij}),\ g_{11} = -g_{22} = -\beta,\ g_{21} = -g_{12} = -\alpha,$$

$G = \{\pm 1_2, \pm g\}$ is a $\mathrm{Gal}(K/F)$-stable subgroup of $GL_2(O_K)$. This seems to be the first example such that K/F is not umramified and G is not in $GL_n(O_F)$ up to roots of unity, although it is $\mathrm{Gal}(K/F)$-stable.

We can give another example: Let n be a natural number and F an algebraic number field containing nth roots of unity, and ε a unit in F, which is not a root of unity. Put $K := F(\varepsilon^{1/n})$, which is a not necessarily unramified but abelian extension of F. For a cyclic permutation $\sigma := (1,2,\ldots, n) \in \mathfrak{S}_n$ and for $a_1 = \cdots = a_{n-1} = \varepsilon^{1/n}$ and $a_n = (\varepsilon^{1/n})^{1-n}$, we put

$$S = (a_i \delta_{\sigma(i),j}),$$

where δ_{ij} denotes Kronecker's delta function. Then $S^n = 1_n$ is easy and

$$G := \left\{ \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix} S^i \;\middle|\; \varepsilon_i : n\text{th root of unity} \right\}$$

is a $\mathrm{Gal}(K/F)$-stable finite subgroup of $GL_n(O_K)$. G is not contained in

$GL_n(O_F)$ up to roots of unity.

Is there an example of a $\mathrm{Gal}(K/F)$-stable finite subgroup G in $GL_n(O_K)$ such that G is not contained in $GL_n(O_L)$ for the maximal abelian subfield L of K over F, or what can we expect?

Malinin announced good results in [5], but the details are not available yet.

REFERENCES

[1] Y. Kitaoka, Finite arithmetic subgroups of GL_n, II, Nagoya Math. J., **77** (1980) 137–143

[2] ——, Arithmetic of quadratic forms, Cambridge University Press, 1993

[3] ——, Finite arithmetic subgroups of GL_n, III, Proc. Indian Acad. Sci., **104** (1994) 201–206

[4] D. A. Malinin, Isometries of positive definite quadratic lattices, ISLC Mathematical College Works. Abstracts, Lie-Lobachevsky Colloquium. Tartu. October 26–30, 1992

[5] ——, Lecture Notes in Mannheim, 1994

Corrections to [3]

As stated in the introduction, the definition of A-type in [3] is not adequate, and we should adopt the definition in this paper. Then the results are true with the following minor modifications in the proof of Lemma 3:

Page 203, line 6: $\varepsilon_i\sigma(L_i) = L_i$ should be "$\varepsilon_i\sigma(L_i) = L_{s(i)}$ for some permutation $s \in \mathfrak{S}_m$".

Page 203, line 12: The displayed equation is numbered by (2).

Page 203, line 18: $\varepsilon_i\eta(L_i) = L_i$ should be "$\varepsilon_i\eta(L_i) = L_{s(i)}$ for some permutation $s \in \mathfrak{S}_m$".

Page 203, line 19: $\mu(L_i) = L_i$ should be $\mu(L_i) = L_{s(i)}$.

Page 203, line 19: $\eta(O_{K'}L_i) = O_{K'}L_i$ should be $\eta(O_{K'}L_i) = O_{K'}L_{s(i)}$.

Pabe 203, line 19-line 20: Insert "that the permutation s is the identity and" between implies and $\eta(x)$.

Page 203, line 35: (1) should be (2).

Theorem 2 on p. 205 is improved as follows:

Page 205, line 9: $GL_n(O_K)$ should be "$GL_m(O_K)$ for any natural number m,".

Graduate School of Polymathematics
Nagoya University
Chikusa-ku, Nagoya 464-01
Japan