Proc. Indian Acad. Sci. (Math. Sci.), Vol. 104, No. 1, February 1994, pp. 201–206.

Finite arithmetic subgroups of GL_n, III

YOSHIYUKI KITAOKA
Department of Mathematics, School of Science, Nagoya University, Japan

Dedicated to the memory of Professor K G Ramanathan

Abstract. Let G be an algebraic group in $GL_n(\mathbf{C})$ defined over $\mathbf{Q}$, and K an algebraic number field with the maximal order O_k. If the group $G(O_k)$ of rational points of G in $M_n(O_k)$ is a finite group and if it satisfies a certain condition, which is satisfied, for example, when K is a nilpotent extension of $\mathbf{Q}$ and 2 is unramified, then $G(O_k)$ is generated by roots of unity in K and $G(\mathbf{Z})$.

Keywords. Algebraic group; algebraic number field; quadratic form; finite arithmetic subgroup.

Let K be a Galois extension of the rational number field $\mathbf{Q}$ with Galois group $G(K/\mathbf{Q})$, and O_K the maximal order of K. Let G be a finite subgroup in $GL_n(O_K)$ such that G is stable under the action of $G(K/\mathbf{Q})$, that is $u(g) := (u(g_{ij})) \in G$ for every $g := (g_{ij}) \in G$ and $u \in G(K/\mathbf{Q})$. Our problem is whether G is of A- type in the sense of [2], that is, whether there is an element $h \in GL_n(\mathbf{Z})$ such that

$$\{hgh^{-1} | g \in G\} \subset \{\mathrm{diag}(\varepsilon_1 A_1, \ldots, \varepsilon_m A_m) | A_i \in GL_{n_i}(\mathbf{Z}),\ \varepsilon_i : \text{root of unity}\}.$$

Here $\mathrm{diag}(\varepsilon_1 A_1, \ldots, \varepsilon_m A_m)$ denotes the matrix in which $\varepsilon_1 A_1, \ldots, \varepsilon_m A_m$ are diagonally arranged. If, hence $\{\pm 1\}$ are the only roots of unity in K, then G being of A-type means $G \subset GL_n(\mathbf{Z})$.

The lattice-theoretic meaning is: Let L be a free module of rank n over $\mathbf{Z}$, and let $\mathcal{G}$ be a linear algebraic group in GL_n defined over $\mathbf{Q}$. Suppose that K is a Galois extension of $\mathbf{Q}$ and that $\mathcal{G}(O_K)$ is a finite group, which is canonically regarded as a subgroup of automorphisms of $O_K L$. Then $\mathcal{G}(O_K)$ being of A-type implies that there exists a direct sum decomposition $L = \bigoplus_{i=1}^{k} L_i$ so that every $\sigma \in \mathcal{G}(O_K)$ and for roots of unity $\varepsilon_i \in K$ dependent on σ, we have

$$\varepsilon_i \sigma(L_i) = L_i \text{ for } i = 1, \ldots, k.$$

We know that the above question is affirmative if either K is totally real and $G(K/\mathbf{Q})$ is nilpotent or $G(K/\mathbf{Q})$ is abelian ([1], [2]). The aim of this paper is to show that this is affirmative if $G(K/\mathbf{Q})$ is nilpotent and the complex conjugation induces an element of the center of $G(K/\mathbf{Q})$. In § 2, we give miscellaneous results.

1. Main result

Lemma 1. *Let $K/\mathbf{Q}$ be a Galois extension with Galois group $\Gamma := G(K/\mathbf{Q})$. Denote by W the set of all roots of unity in K. We fix an element $a_\sigma \in W$ for $\sigma \in \Gamma$. If $a_{\mu\sigma} = a_\mu \mu(a_\sigma)$*

holds for every $\sigma, \mu \in \Gamma$, then there exists an element $a \in K$ such that $a_\mu = \mu(a^{-1})a$ for $\mu \in \Gamma$ and $a^w \in \boldsymbol{Q}^\times$, where w is the cardinality of W.

Proof. We can take a non-zero element $u \in K$ such that $a := \Sigma_{\sigma \in \Gamma} a_\sigma \sigma(u) \neq 0$. For $\mu \in \Gamma$, we have $\mu(a) = \Sigma_{\sigma \in \Gamma} \mu(a_\sigma)\mu\sigma(u) = \Sigma_{\sigma \in \Gamma} a_\mu^{-1} a_{\mu\sigma} \mu\sigma(u) = a_\mu^{-1} a$, and hence $a_\mu = \mu(a^{-1})a$. $a_\mu \in W$ implies $a_\mu^w = 1$ and therefore $\mu(a^w) = a^w$. This yields $a^w \in \mathbf{Q}^\times$. ∎

Lemma 2. Let p be a prime number and let $A \in GL_n(\boldsymbol{Z})$ be of finite order and suppose that $A \equiv 1_n \bmod p$. If $p \neq 2$, then we have $A = 1_n$. If $p = 2$, then $A = T\begin{pmatrix} 1_r & \\ & -1_s \end{pmatrix} T^{-1}$ for some $T \in GL_n(\boldsymbol{Z})$.

Proof. This is due to Minkowski. But we give the proof for the convenience. For $B \in GL_n(\mathbf{Z})$ with $B \equiv 1_n \bmod p$, we write $B = 1_n + p^r C$, where C is integral and $C \not\equiv 0 \bmod p$. Then for a natural number h, the following is clear:

$$B^h = 1_n + hp^r C + \sum_{k=2}^{h} \binom{h}{k} (p^r C)^k. \tag{1}$$

Suppose that the order of A is not a power of p. Then some power B of A is of order h, where h is a prime different from p. Eqn. (1) implies $1_n \equiv 1_n + hp^r C \bmod p^{2r}$, which contradicts $C \not\equiv 0 \bmod p$. Thus the order of A is a power of p.

Suppose $p \neq 2$ and $A \neq 1_n$. Let B be a power of A whose order is p. Applying (1) with $h = p$, $1_n \equiv 1_n + p^{r+1} C \bmod p^{2r+1}$ follows from $r \geqslant 1$ and $\binom{p}{k} \equiv 0 \bmod p$ for $k \neq 0, p$. This contradicts $C \not\equiv 0 \bmod p$, and so we have $A = 1_n$ if $p \neq 2$.

Let us consider the case of $p = 2$.

Suppose that the order of $A = 1$ or 2. Let L be a $\mathbf{Z}$-module with basis $\{e_1, \ldots, e_n\}$ and define a linear mapping u by $(u(e_1), \ldots, u(e_n)) = (e_1, \ldots, e_n)A$. Then $A \equiv 1_n \bmod 2$ and $A^2 = 1_n$ imply $u(x) \equiv x \bmod 2L$ and $u^2 = id$. Hence $x = (x + u(x))/2 + (x - u(x))/2$ implies $L = \{x \in L \mid u(x) = x\} \oplus \{x \in L \mid u(x) = -x\}$. Therefore this completes the proof if $A^2 = 1_n$.

Lastly, supposing that the order of $A = 2^k$ $(k \geqslant 2)$, we will show the contradiction. Applying (1) for $B = A$, we have $A^2 \equiv 1_n \bmod 4$. Hence in the expression of $B := A^{2^{k-1}} = 1_n + 2^r C$, we have $r \geqslant 2$. Then we have $1_n = B^2 = 1_n + 2^{r+1} C + 2^{2r} C^2$, which yields the contradiction $C \equiv 0 \bmod 2^{r-1}$. Thus we have completed the proof. ∎

Lemma 3. Let $K/\boldsymbol{Q}$ be a Galois extension with Galois group $\Gamma := G(K/\boldsymbol{Q})$ and O_K the maximal order of K. Let G be a finite subgroup of $GL_n(O_K)$ which is stable under the action of Γ. Let Γ' be the commutator subgroup of Γ and K' be the maximal abelian subfiled of K corresponding to Γ'. Suppose the following conditions:

(I) *if F is a proper subfield of K and $F/\boldsymbol{Q}$ is a Galois extension, then $G \cap GL_n(F) \subset GL_n(K')$.*

(II) *At least two rational primes ramify in K.*

Then G is of A-type.

Proof. First we give a remark on elements in $G' := G \cap GL_n(K')$. Putting $P := \Sigma_{g \in G'} {}^t g \bar{g}$, ${}^t\bar{P} = P$ is a positive definite Hermitian matrix. Since K' is an abelian extension and $\mu(G') = G'$ for $\mu \in G(K'/\mathbf{Q})$, we have $\mu(P) = \Sigma_{g \in G'} {}^t\mu(g)\overline{\mu(g)} = P$ for $\mu \in G(K'/\mathbf{Q})$. Hence P is an integral positive definite symmetric matrix. Put $L := \mathbf{Z}^n$ (column vectors) and

for $x, y \in O_{K'}$ $L = (O_{K'})^n$ we introduce an inner product by $(x, y) := {}^t x P \bar{y}$. Note that $x, y \in L$ implies $(x, y) \in \mathbf{Z}$. Let $L = \perp_{i=1}^{m} L_i$ be an orthogonal decomposition of L to indecomposable submodules. Then $O_{K'} L_i$ is also indecomposable with respect to the inner product by Lemma on p. 142 in [2]. Every $g \in G'$ satisfies ${}^t g P \bar{g} = P$ and hence $x \mapsto gx$ induces an isometry σ of $O_{K'} L$. From theorems on p. 140 and p. 141 it follows that there exist roots of unity ε_i in K' such that $\varepsilon_i \sigma(L_i) = L_i$.

Take any element $g \in G$. We will show $g \in GL_n(K')$.

Let q be a rational prime which ramifies in K. We take a rational prime p different from q which also ramifies in K. Let $\tilde{p}, \tilde{q}$ be prime ideals of K on p, q respectively. First, let us show that for every element μ in the inertia group $T(\tilde{q})$, there is an integral matrix $T \in GL_n(\mathbf{Z})$ dependent only on the above decomposition $L = \perp L_i$ of L such that

$$g_1 := \mu(g) g^{-1} = T D_\mu T^{-1}$$

for a diagonal matrix D_μ whose diagonal elements are roots of unity in K'. $g_1 \equiv 1_n \bmod \tilde{q}$ follows from the definition and hence $\sigma(g_1) = g_1$ for $\sigma \in T(\tilde{p})$ by Lemma 7.5.2 in [3]. Considering other prime ideals lying on p, g_1 is fixed by the subgroup Γ_1 generated by inertia subgroups of prime ideals lying on p. Since Γ_1 is normal in Γ and $\Gamma_1 \neq \{1\}$, the condition (I) yields $g_1 \in GL_n(K')$. By the remark at the beginning of the proof, there exist roots of unity ε_i such that $\varepsilon_i \eta(L_i) = L_i$, where $\eta(x) := g_1 x$. Put $\mu := \varepsilon_i \eta$. Then $\mu(L_i) = L_i$ implies $\eta(O_{K'} L_i) = O_{K'} L_i$ and then $g_1 \equiv 1_n \bmod \tilde{q}$ implies $\eta(x) \equiv x \bmod \tilde{q} L i$ for $x \in L_i$ and so $\mu(x) \equiv \varepsilon_i x \bmod \tilde{q} L_i$ for $x \in L_i$. Comparing the coordinates, ε_i is congruent to some rational integer a modulo $\tilde{q}$. Since ε_i is a unit, a and q are relatively prime, and there is a rational integer b such that $ab \equiv 1 \bmod q$. Hence $\eta(x) \equiv x \bmod \tilde{q} L$ for $x \in L$ implies $\mu(x) \equiv ab\mu(x) \equiv ab\varepsilon_i x \equiv a^2 bx \equiv ax \bmod \tilde{q} L_i$ for $x \in L_i$, and hence $\mu(x) \equiv ax \bmod q L_i$ for $x \in L_i$. Let $\{f_1, \ldots, f_m\}$ be a basis of L_i and define a matrix $B \in GL_m(\mathbf{Z})$ by $(\mu(f_1), \ldots, \mu(f_m)) = (f_1, \ldots, f_m) B$. Then $B \equiv a 1_m \bmod q$ and the order k of μ and hence B is finite. Put $S = \Sigma_{r \bmod k} {}^t B^r B^r$, and take an integer s such that $S_0 := q^{-s} S$ is integral and is not congruent to $0 \bmod q$. If q is odd, then there is a $\mathbf{Z}$-vector x such that ${}^t x S_0 x \not\equiv 0 \bmod q$. Hence we have ${}^t x S_0 x = {}^t(Bx) S_0 (Bx) \equiv a^2 {}^t x S_0 x \bmod q$ and hence $a^2 \equiv 1 \bmod q$, which yields $a \equiv \pm 1 \bmod q$. This is true even for $q = 2$, since $(a, q) = 1$. Thus we have $\mu(x) \equiv \pm x \bmod q L_i$ for $x \in L_i$. Since $\mu = \varepsilon_i \eta$ is of finite order, $\mu = \pm id$ on L_i follows from Lemma 2 and the indecomposability of L_i. If $\mu = -id$, then taking $-\varepsilon_i$ instead of ε_i, we may assume that $\varepsilon_i \eta$ is id on L_i. Taking the union of bases of L_i's as a basis of L, and denoting the base change matrix by $T \in GL_n(\mathbf{Z})$, we can conclude that $g_1 = \mu(g) g^{-1} = T D_\mu T^{-1}$ for a diagonal matrix whose diagonal entries are roots of unity in K. Thus (1) has been proved.

If $\mu_i \in G(K/\mathbf{Q})$ $(i = 1, 2)$ satisfies $\mu_i(g) g^{-1} = T D_{\mu_i} T^{-1}$, then we have $\mu_1 \mu_2(g) g^{-1} = \mu_1(T D_{\mu_2} T^{-1} g) g^{-1} = T \mu_1(D_{\mu_2}) T^{-1} (T D_{\mu_1} T^{-1}) = T \mu_1(D_{\mu_2}) D_{\mu_1} T^{-1}$ and $\mu_1(D_{\mu_2}) D_{\mu_1}$ is also a diagonal matrix whose diagonal elements are roots of unity in K. Noting that $G(K/\mathbf{Q})$ is generated by inertia subgroups of all ramified prime ideals, we have $\mu(g) g^{-1} = T D_\mu T^{-1}$ for $\mu \in G(K/\mathbf{Q})$, where D_μ is a diagonal matrix whose diagonal entries are roots of unity in K. Since $D_{\mu_1 \mu_2} = \mu_1(D_{\mu_2}) D_{\mu_1}$ for $\mu_1, \mu_2 \in G(K/\mathbf{Q})$, Lemma 1 implies the existence of diagonal matrix $D = \operatorname{diag}(d_1, \ldots, d_n) \in M_n(K)$ such that $D_\mu = \mu(D^{-1}) D$ and $d_i^w \in \mathbf{Q}^\times$, where w is the order of the group of roots of unity in K. Hence $\mu(g) g^{-1} = T D_\mu T^{-1} = T \mu(D^{-1}) D T^{-1}$ yields $\mu(D T^{-1} g) = D T^{-1} g$ for $\mu \in G(K/\mathbf{Q})$. This means $h := D T^{-1} g \in M_n(\mathbf{Q})$. Taking a rational diagonal matrix h' so that the numbers on any row of $h'h$ are relatively prime integers, then $T^{-1} g = (h' D)^{-1} h' h \in M_n(O_K)$ implies that the diagonal matrix $\tilde{D} := (h' D)^{-1}$ is in $M_n(O_K)$. Moreover

the fact that $\det(T^{-1}g)(=\det(\tilde{D})\det(h'h))$ is in $O_K^\times$ yields that diagonal entries $\tilde{d}_i$ of $\tilde{D}$ are also in $O_K^\times$ by $h'h \in M_n(\mathbf{Z})$. Thus we have $\tilde{d}_i \in O_K^\times$ and $\tilde{d}_i^w \in \mathbf{Q}^\times$ by $d_i^w \in \mathbf{Q}^\times$ and hence $\tilde{d}_i$ is a root of unity. Thus we have proved that $T^{-1}g = \tilde{D}h'h = (h'D)^{-1}h'h$ and hence g is in $GL_n(K')$. Thus G is in $GL_n(O_{K'})$ and hence it is of A-type by Theorem on p. 141 in [2]. ∎

Theorem 1. *Let K be an algebraic number field such that* (i) *$K/\mathbf{Q}$ is a nilpotent extension, and* (ii) *if H is a subfield of K such that H is a Galois extension over $\mathbf{Q}$ and 2 is the only rational prime that ramifies in H, then the complex conjugation induces an element of the center of $G(H/\mathbf{Q})$. Let G be a finite subgroup of $GL_n(O_K)$ which is stable under the action of $G(K/\mathbf{Q})$. Then G is of A-type.*

Proof. We use induction on $[K:\mathbf{Q}]$. When $[K:\mathbf{Q}] = 1$, we have nothing to do. We note that for a proper subfield F of K which is a Galois extension of $\mathbf{Q}$, the conditions (i) and (ii) are satisfied. Suppose that there are at least two rational primes which ramify in K. Lemma 3 completes the proof, since the condition (I) in Lemma 3 is satisfied by the induction assumption. Hence we may suppose that there is only one rational prime p that ramifies in K. To complete the proof, we have only to claim that K is abelian by induction on $[K:\mathbf{Q}]$, assuming (i) and (ii), since the theorem is proved for every abelian field K.

Let Z be the center of $G(K/\mathbf{Q})$. Then we have $Z \neq \{1\}$ and $G(K/\mathbf{Q})/Z$ is nilpotent, and the subfield of K corresponding to Z satisfies the conditions (i) and (ii). By the induction assumption, $G(K/\mathbf{Q})/Z$ is abelian and the complex conjugation is trivial by (ii) if $p = 2$. Thus $G(K/\mathbf{Q})/Z$ is cyclic and hence $G(K/\mathbf{Q})$ is abelian. ∎

2. Miscellaneous results

Lemma 4. *Let n be a natural number. Then there exists a finite set S_n of algebraic numbers with $S_n \cap \mathbf{Q} = \phi$ which satisfies the following:*

Let K be a Galois extension of degree n of $\mathbf{Q}$ and suppose that $S_n \cap K = \phi$ and the complex conjugation is in the center of $G(K/\mathbf{Q})$. Then the maximal order O_K is a positive lattice of E-type with respect to the quadratic form $\mathrm{tr}_{K/\mathbf{Q}}|x|^2$ in the sense of [3].

Proof. Denote by S_n the set of non-rational algebraic integers x satisfying that $[\mathbf{Q}(x):\mathbf{Q}] \leqslant n$ and the square of the absolute value of every conjugate of x over $\mathbf{Q}$ is less than $(4/3)^{n-2} + 1/4$. Then S_n is a finite set of algebraic integers and $S_n \cap \mathbf{Q} = \phi$. Let K be the field in the statement of Lemma. Then $\mathrm{tr}_{K/\mathbf{Q}}|x|^2 \geqslant 0$ for $x \in O_K$ and the equality occurs if and only if $x = 0$. For $x \in O_K$ $(x \neq 0)$, we have $\mathrm{tr}_{K/\mathbf{Q}}|x|^2 \geqslant n(\Pi_{\sigma \in G(K/\mathbf{Q})}|\sigma(x)|^2)^{1/n} = n|N_{K/\mathbf{Q}}(x)|^{2/n} \geqslant n$ and $\mathrm{tr}_{K/\mathbf{Q}}|1|^2 = n$ is clear. If $x \in O_K$ is not in $\mathbf{Z}$, then $S_n \cap K = \phi$ implies that the absolute value of some conjugate of x^2 is larger than $(4/3)^{n-2} + 1/4$ and hence $\mathrm{tr}_{K/\mathbf{Q}}|x|^2 > (4/3)^{n-2} + 1/4$. Let $v_1 = 1, v_2, \ldots, v_n$ be a basis of O_K over $\mathbf{Z}$ such that the matrix $(\mathrm{tr}_{K/\mathbf{Q}} v_i \bar{v}_j)$ is in the Siegel domain $S_{4/3,\,1/2}$, that is $(\mathrm{tr}_{K/\mathbf{Q}} v_i \bar{v}_j) = A[N]$, where $A = \mathrm{diag}(a_1, \ldots, a_n)$ with $a_i/a_{i+1} \leqslant 4/3$ and $N = (n_{ij})$ satisfying $n_{ij} = 0$ if $i > j$, $= 1$ if $i = j$ and $|n_{ij}| \leqslant 1/2$ if $i < j$. Then we have

$$\begin{pmatrix} 1 & \mathrm{tr}\,\bar{v}_2 \\ \mathrm{tr}\,v_2 & \mathrm{tr}|v_2|^2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}\left[\begin{pmatrix} 1 & n_{12} \\ 0 & 1 \end{pmatrix}\right]$$

and hence $a_1 = 1, \operatorname{tr} \overline{v_2} = a_1 n_{12} = n_{12}, \operatorname{tr}|v_2|^2 = n_{12}^2 + a_2 \leqslant 1/4 + a_2$. $v_2 \notin \mathbf{Q}$ implies $\operatorname{tr}_{K/\mathbf{Q}}|v_2|^2 > (4/3)^{n-2} + 1/4$ and hence $a_2 > (4/3)^{n-2}$. Thus O_K is of E-type by Exercise 4 in §4 of Chapter 7 in [3]. ■

Remark. By Theorem 7.1.1 in [3], we can assume $S_n = \phi$ if $n \leqslant 43$.

Theorem 2. *Let n be a natural number. Then there exists a finite set S_n of non-rational algebraic integers which satisfies the following:*

Let K be a Galois extension of degree n over $\mathbf{Q}$ with $S_n \cap K = \phi$ and assume that the complex conjugation is in the center of $G(K/\mathbf{Q})$. If G is a finite group of $GL_n(O_K)$ which is stable under the action of $G(K/\mathbf{Q})$, then G is of A-type.

Proof. Let S_n be the set given in Lemma 4. Then O_K is a positive lattice of E-type by Lemma 4 and hence Theorem on p. 141 in [2] completes the proof. ■

Remark. The set S_n constructed in Lemma 1 contains r-th roots of unity for $r \leqslant n$. Therefore in Theorem 2 the conclusion "G is of A-type" is replaced by "$G \subset GL_n(\mathbf{Z})$".

Lemma 5. Let K be a Galois extension of $\mathbf{Q}$. Let G be a subgroup of $GL_n(O_K)$ stable under the action of $G(K/\mathbf{Q})$. For a prime ideal I of K, we put $V_t(I, K/\mathbf{Q}) := \{u \in G(K/\mathbf{Q}) | u(x) \equiv x \bmod I^{t+1}$ for every $x \in O_K\}$ and $G(I^i) := \{g \in G | g \equiv 1_n \bmod I^i\}$. Suppose $G(I^r) \neq \{1_n\}$ and $G(I^{r+1}) = \{1_n\}$ for a natural number $r \geqslant 1$. If t, m are integers satisfying $t \geqslant 0, m \geqslant 1$ and $t + m \geqslant r + 1$, then $V_t(I, K/\mathbf{Q})$ acts trivially on $G(I^m)$, and $G(I^s)$ is abelian if $2s \geqslant r + 1$.

Proof. Take an integer $\pi \in O_K$ so that πI^{-1} is an integral ideal relatively prime to I. Let a, b be non-negative rational integers. We claim

$$u(\pi)^a \equiv \pi^a \bmod I^{a+b} \text{ if } u \in V_b(I, K/\mathbf{Q}).$$

When $a = 1$, this is contained in the definition. Suppose $u(\pi)^a \equiv \pi^a \bmod I^{a+b}$ for $a \geqslant 1$. Write $u(\pi) = \pi + x, u(\pi)^a = \pi^a + y$ where $x \in I^{b+1}$, $y \in I^{a+b}$. Then $u(\pi)^{a+1} = (\pi + x)(\pi^a + y) = \pi^{a+1} + x\pi^a + y\pi + xy \equiv \pi^{a+1} \bmod I^{a+b+1}$ is clear. Thus we have completed the proof of the above claim.

Let t, m, r be rational integers such that $t \geqslant 0, m \geqslant 1$ and $t + m \geqslant r + 1$. For $g \in G(I^m)$, we write $g = 1_n + \pi^m A$ for $A \in M_n(O_I)$, where O_I denotes the I-adic completion of O_K. If $u \in V_t(I, K/\mathbf{Q})$, then we have

$$\begin{aligned} u(g) &= 1_n + u(\pi)^m u(A) \\ &= 1_n + (\pi^m \bmod I^{m+t})(A \bmod I^{t+1}) \\ &\equiv 1_n + \pi^m A \bmod I^{t+m} \\ &\equiv g \bmod I^{t+m}, \end{aligned}$$

which implies $u(g)g^{-1} \in G(I^{t+m}) \subset G(I^{r+1}) = \{1_n\}$ and hence $u(g) = g$. Thus $V_t(I, K/\mathbf{Q})$ acts trivially on $G(I^m)$.

Let s be a rational integer such that $2s \geqslant r + 1$, and $g, h \in G(I^s)$. Writing $g = 1_n + \pi^s A$,

$h = 1_n + \pi^s B(A, B \in M_n(O_I))$, we have $gh - hg = \pi^{2s}(AB - BA) \equiv 0 \bmod I^{r+1}$. Hence $ghg^{-1}h^{-1} \equiv 1_n \bmod I^{r+1}$ which means $ghg^{-1}h^{-1} \in G(I^{r+1}) = \{1_n\}$. Thus $G(I^s)$ is abelian. ■

Theorem 3. *Let K be a totally real Galois extension of $\mathbf{Q}$ and suppose that there is a rational prime p which is totally ramified in K. If G is a finite subgroup of $GL_n(O_K)$ stable under the action of $G(K/\mathbf{Q})$, then G is in $GL_n(\mathbf{Z})$.*

Proof. First we note that the inertia subgroup $V_0(I, K/\mathbf{Q})$ for the prime ideal I of K over p is equal to $G(K/\mathbf{Q})$, and $N_{K/\mathbf{Q}}(I) = p$ is clear. If $p = 2$, then the order of the inertia group is a power of 2 and hence K is nilpotent. Therefore Theorem 3 follows from Theorem 1.

Suppose $p \neq 2$. Define an integer $r \geqslant 0$ by the condition $G(I^r) \neq \{1_n\}, G(I^{r+1}) = \{1_n\}$. Suppose $r \geqslant 1$; then by Lemma 5, $V_1(1, K/\mathbf{Q})$ acts trivially on $G(I^r)$. Hence $G(I^r) \subset GL_n(O_F)$, where F is the subfield of K corresponding to $V_1(I, K/\mathbf{Q})$, which is normal in $V_0(I, K/\mathbf{Q})$. Since $V_0(I, K/\mathbf{Q})/V_1(I, K/\mathbf{Q})$ is cyclic, F is abelian over $\mathbf{Q}$. Since p is totally ramified in K, p is also totally ramified in F and $G(F/\mathbf{Q}) = V_0(I, K/\mathbf{Q})/V_1(I, K/\mathbf{Q})$ acts on $G(I^r)(\subset GL_n(O_F))$. By Theorem 1, we have $G(I^r) \subset G(\mathbf{Z})$ and hence by Lemma 2 we have $G(I^r) = \{1_n\}$, which is the contradiction. Thus we have $r = 0$ and hence $G(I) = \{1_n\}$. For $g \in G$ and $u \in G(K/\mathbf{Q}) = V_0(I, K/\mathbf{Q})$, we have $u(g) \equiv g \bmod I$ and hence $u(g)g^{-1} \in G(I) = \{1_n\}$. Thus $G(K/\mathbf{Q})$ acts trivially on G. ■

References

[1] Bartels H -J and Kitaoka Y, Endliche arithmetische Untergruppen der GL_n, *Reine Angew. Math.* **313** (1980), 151–156

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

[3] Kitaoka Y, *Arithmetic of quadratic forms*, (Cambridge: Cambridge University Press) 1993