Y. Kitaoka
Nagoya Math. J.
Vol. 77 (1980), 137–143

FINITE ARITHMETIC SUBGROUPS OF GL_n, II

YOSHIYUKI KITAOKA

In [1] $\sim$ [6] the following question was treated: Let k be a totally real Galois extension of the rational number field $\boldsymbol{Q}$, O the maximal order of k and G a finite subgroup of $GL(n, O)$ which is stable under the operation of $G(k/\boldsymbol{Q})$. Then does $G \subset GL(n, \boldsymbol{Z})$ hold?

An aim of this paper is to generalize this. First we introduce a notion of A-type for finite subgroups of $GL(n, O)$. Let k be an algebraic number field, O the maximal order of k and G a finite subgroup of $GL(n, O)$. Put $L = \boldsymbol{Z}^n$ (row vectors) and operate G on $OL = O^n$ as product of matrices. Then we call G of A-type if there is a direct decomposition $L = \oplus_{i=1}^m L_i$ such that for each $g \in G$, there exist a root of unity $\varepsilon_i(g) \in O$ and a permutation $s(g) \in S_m$ satisfying $\varepsilon_i(g) g L_i = L_{s(g)i}$ for $i = 1, 2, \cdots, m$.

If ± 1 are all roots of unity in k, then we have $G \subset GL(n, \boldsymbol{Z})$ if G is of A-type. Now our question is following:

Let k be a Galois extension of $\boldsymbol{Q}$, O the maximal order of k and G a finite subgroup of $GL(n, O)$ which is stable under operation of $G(k/\boldsymbol{Q})$, that is, $g^\sigma \in G$ for every $g \in G$, $\sigma \in G(k/\boldsymbol{Q})$. Then is G of A-type?

It is shown that this is affirmative for abelian fields.

We denote by O_k the maximal order of an algebraic number field k and mean by a positive $\boldsymbol{Z}$-lattice a lattice on a positive definite quadratic space over the rational number field $\boldsymbol{Q}$.

Let k be a Galois extension of $\boldsymbol{Q}$ and assume that the complex conjugate induces an element of the center of $G(k/\boldsymbol{Q})$. Then O_k becomes a positive $\boldsymbol{Z}$-lattice with quadratic form $\mathrm{tr}_{k/\boldsymbol{Q}} |x|^2$, $(x \in O_k)$. In § 1 we prove that this positive $\boldsymbol{Z}$-lattice is of E-type in the sense of [5] if k is abelian. For positive $\boldsymbol{Z}$-lattices L, M, $O_k L$, $O_k M$ become cannonically positive definite Hermitian forms. In § 2 we show that if σ is an isometry from $O_k L$ on $O_k M$ and k is abelian, then there exist orthogonal decompositions $L = \perp_{i=1}^t L_i$, $M = \perp_{i=1}^t M_i$ and roots of unity ε_i in k such that $\varepsilon_i \sigma(L_i) = M_i$. As

Received February 6, 1979.

a corollary we can answer positively our question for abelian fields.

§ 1. Let k be a finite Galois extension of $\boldsymbol{Q}$ and assume that the complex conjugate induces an element of the center of $G(k/\boldsymbol{Q})$. Then O_k becomes a positive $\boldsymbol{Z}$-lattice with quadratic form $\mathrm{tr}_{k/\boldsymbol{Q}}|x|^2$, $(x \in O_k)$. This positive lattice is denoted by $\tilde{O}_k$. If $\tilde{O}_k$ is of E-type in the sense of [5], then we say that k is of E-type.

LEMMA 1. *Let k, $\tilde{O}_k$ be as above. Then we have* $\min_{\substack{x \in O_k \\ x \neq 0}} \mathrm{tr}_{k/\boldsymbol{Q}}|x|^2 = [k:\boldsymbol{Q}]$ *and* $\{x \in O_k \mid \mathrm{tr}_{k/\boldsymbol{Q}}|x|^2 = [k:\boldsymbol{Q}]\} = \{$*all roots of unity in* $k\}$.

Proof. Take any non-zero element a in O_k. Then

$$\begin{aligned}\mathrm{tr}_{k/\boldsymbol{Q}}|a|^2 &= \sum_{g \in G(k/\boldsymbol{Q})} |g(a)|^2 \geq [k:\boldsymbol{Q}](\Pi\, |g(a)|^2)^{1/[k:\boldsymbol{Q}]} \\ &= [k:\boldsymbol{Q}](N_{k/\boldsymbol{Q}}|a|^2)^{1/[k:\boldsymbol{Q}]} \geq [k:\boldsymbol{Q}]\,.\end{aligned}$$

Suppose $\mathrm{tr}_{k/\boldsymbol{Q}}|a|^2 = [k:\boldsymbol{Q}]$, then $N_{k/\boldsymbol{Q}}|a|^2 = 1$ and $|g(a)|^2 = |a|^2$ for every $g \in G(k/\boldsymbol{Q})$. This implies $|g(a)| = 1$ for every $g \in G(k/\boldsymbol{Q})$. Hence a is a root of unity. Conversely a root of unity a in k satisfies $\mathrm{tr}_{k/\boldsymbol{Q}}|a|^2 = [k:\boldsymbol{Q}]$.

LEMMA 2. *Let k_1, k_2 be Galois extensions of $\boldsymbol{Q}$ and assume that the complex conjugate induces an element of the center of $G(k_i/\boldsymbol{Q})$, $(i = 1, 2)$. Then we have*

(i) *if $k_1 \supset k_2$ and k_1 is of E-type, then k_2 is also of E-type,*

(ii) *if the discriminants of k_1, k_2 are relatively prime and k_1, k_2 are of E-type, then the composite field k_1k_2 is also of E-type.*

Proof. Suppose $k_1 \supset k_2$. If $\tilde{O}_{k_1}$ is of E-type, then a submodule O_{k_2} of $\tilde{O}_{k_1}$ is also of E-type by virtue of Prop. 2 in [5] since $1 \in O_{k_2}$ is a minimal vector of $\tilde{O}_{k_1}$. For $x \in O_{k_2}$ we have $\mathrm{tr}_{k_1/\boldsymbol{Q}}|x|^2 = [k_1:k_2]\,\mathrm{tr}_{k_2/\boldsymbol{Q}}|x|^2$. Hence a submodule O_{k_2} of $\tilde{O}_{k_1}$ is similar to $\tilde{O}_{k_2}$ and so $\tilde{O}_{k_2}$ is also of E-type. Suppose the assumption of (ii), then $O_{k_1k_2} = O_{k_1} \otimes O_{k_2}$ and for $a_1, b_1 \in O_{k_1}$, $a_2, b_2 \in O_{k_2}$ we have $\mathrm{tr}_{k_1k_2/\boldsymbol{Q}}\, a_1a_2\overline{b_1b_2} = \mathrm{tr}_{k_1/\boldsymbol{Q}}\, a_1\overline{b_1} \cdot \mathrm{tr}_{k_2/\boldsymbol{Q}}\, a_2\overline{b_2}$ where the bar denotes the complex conjugate. Hence $\tilde{O}_{k_1k_2}$ is isometric to $\tilde{O}_{k_1} \otimes \tilde{O}_{k_2}$. Prop. 1 in [5] completes the proof.

LEMMA 3. *Let p be a prime and $L = \boldsymbol{Z}[u_1, \cdots, u_{p-1}]$ a quadratic lattice defined by $(u_i, u_j) = -1$ if $i \neq j$ and $(u_i, u_i) = p - 1$ for every i. Then L is a positive $\boldsymbol{Z}$-lattice and of E-type.*

Proof. Let N be a positive $\boldsymbol{Z}$-lattice. We use the same notations

$Q(x)$, (x, y) for the quadratic forms and bilinear forms associated to L, N and $L\otimes N$. For a non-zero element $x=\sum_{i=1}^{p-1} u_i\otimes w_i$, $(w_i\in N)$ in $L\otimes N$ we have

$$Q(x)=\sum_{i,j=1}^{p-1}(u_i, u_j)(w_i, w_j)$$
$$=\sum_{i=1}^{p-1}Q(w_i)+\sum_{i<j}Q(w_i-w_j)\,.$$

Hence L is positive definite. For each permutation $s\in S_{p-1}$, $u_i\mapsto u_{s(i)}$ gives an isometry of L. Hence we may assume that $w_1,\cdots,w_k\neq 0$, $w_{k+1}=\cdots=w_{p-1}=0$ without changing the value of $Q(x)$. Since $w_1,\cdots,w_k$, $w_1-w_{k+1},\cdots,w_1-w_{p-1}$ are not zero, we get $Q(x)\geq(p-1)m(N)$ where $m(N)$ denotes the minimum of $Q(y)$, $(y\in N, y\neq 0)$. If we take a special lattice $\langle 1\rangle$ as N, then $Q(x)\geq p-1$ for any non-zero x in L. Hence we have $m(L)=p-1$ and $m(L\otimes N)\geq m(L)m(N)$. Suppose that $Q(x)=(p-1)m(N)$. Then w_i-w_j, $(i<j)$, should be zero if $(i,j)\neq(1,k+1),\cdots,(1,p-1)$, since $(p-1)m(N)=Q(x)\geq\sum_{i=1}^{k}Q(w_i)+\sum_{k=k+1}^{p-1}Q(w_1-w_j)\geq(p-1)m(N)$. Hence we have $w_2=\cdots=w_{p-1}$. If $w_2=0$, then $x=u_1\otimes w_1$. If $w_2\neq 0$, then $k\geq 2$ implies $w_1=w_2$ and $x=(\sum u_i)\otimes w_1$. Therefore by definition L is of E-type.

LEMMA 4. *Let ζ be a primitive p^n-th root of unity where p is prime and $n\geq 2$. Then $\boldsymbol{Q}(\zeta)$ is of E-type.*

Proof. It is well known that

$$\operatorname{tr}_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}}\zeta^m=\begin{cases}p^{n-1}(p-1) & \text{if } p^n\,|\,m\,,\\ -p^{n-1} & \text{if } p^{n-1}\,\|\,m\,,\\ 0 & \text{if } p^{n-1}\nmid m\,.\end{cases}$$

As an integral basis of $\boldsymbol{Z}[\zeta]$ we can take $v_i=\zeta^{i-1}$, $(1\leq i\leq p^{n-1}(p-1))$. Then $\operatorname{tr}_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}}v_i\overline{v_j}=\operatorname{tr}_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}}\zeta^{i-j}$. Let $L=\boldsymbol{Z}[u_1,\cdots,u_{p-1}]$ be a quadratic lattice defined by $(u_i, u_i)=p-1$, $(u_i, u_j)=-1$ for $i\neq j$. By Lemma 3, L is positive definte and of E-type. We define another positive $\boldsymbol{Z}$-lattice $M=\boldsymbol{Z}[w_1,\cdots,w_{p^{n-1}}]$ by $(w_i, w_j)=p^{n-1}\delta_{ij}$. Then $M=\perp\langle p^{n-1}\rangle$ is also of E-type by Prop. 1 in [5]. We determine a basis $\{z_i\}$ of $L\otimes M$ by $z_i=u_{b+1}\otimes w_a$, $(i=a+bp^{n-1},\ 1\leq a\leq p^{n-1})$. Put $i=a+bp^{n-1}$, $j=a'+b'p^{n-1}$, $(1\leq a, a'\leq p^{n-1})$, then $(z_i, z_j)=(u_{b+1}, u_{b'+1})\times(w_a, w_{a'})$. Hence we have $(z_i, z_i)=p^{n-1}(p-1)$. Suppose $i\neq j$. If $i\equiv j\bmod p^{n-1}$, then $(z_i, z_j)=-p^{n-1}$. $i\not\equiv j\bmod p^{n-1}$ implies $(z_i, z_j)=0$. Therefore we have $\operatorname{tr}_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}}v_i\overline{v_j}$

$=(z_i, z_j)$, $(1 \leq i, j \leq p^{n-1}(p-1))$. Since $L \otimes M$ is of E-type, $\tilde{O}_{Q(\zeta)}$ is also of E-type.

THEOREM. *Abelian extensions of* $\boldsymbol{Q}$ *are of E-type.*

Proof. Any abelian extension of $\boldsymbol{Q}$ is contained in $\boldsymbol{Q}(\zeta)$ for some root of unity ζ. Hence Lemma 2 and 4 complete the proof.

§ 2. Through this section we denote by k a Galois extension of $\boldsymbol{Q}$ and assume that the complex conjugate induces an element of the center of $G(k/\boldsymbol{Q})$. For a positive $\boldsymbol{Z}$-lattice L the associated bilinear form (,) can be generalized to $O_k L$ as follows:

For $a, b \in O_k$ and $x, y \in L$, $(ax, by) = a\bar{b}(x, y)$, where $\bar{b}$ is the complex conjugate of b. Hereafter $O_k L$ means this positive definite Hermitian form.

LEMMA. *Let M, N be positive $\boldsymbol{Z}$-lattices and σ an isometry from $O_k M$ on $O_k N$. Assume that there exist submodules $\perp_{i=1}^m M_i$ of M and $\perp_{i=1}^m N_i$ of N such that $[M: \perp_{i=1}^m M_i]$, $[N: \perp_{i=1}^m N_i] < \infty$ and $\varepsilon_i \sigma(M_i) = N_i$, $(1 \leq i \leq m)$, for some root of unity ε_i in k.* Then there exist orthogonal decompositions $M = \perp_{i=1}^n M'_i$, $N = \perp_{i=1}^n N'_i$ such that $\varepsilon'_i \sigma(M'_i) = N'_i$, $(1 \leq i \leq n)$ for some root of unity ε'_i in k.

Proof. We use induction on rank M. Lemma is obvious in case of rank $M = 1$. Suppose rank $M > 1$. Since $\varepsilon_1 \sigma$ is also an isometry from $O_k M$ on $O_k N$, we may assume $\varepsilon_1 = 1$ without loss of generality. Take any non-zero element u in M_1, then $\sigma(u) = v \in N_1$ and $\sigma(O_k u^\perp) = O_k v^\perp$. Applying induction to $\sigma(O_k u^\perp) = O_k v^\perp$, we may assume that $M_1 = \boldsymbol{Z}[u]$, $N_1 = \boldsymbol{Z}[v]$, $\varepsilon_1 = 1$, $M_1^\perp = M_2 \perp \cdots \perp M_m$, $N_1^\perp = N_2 \perp \cdots \perp N_m$ and that M_1, N_1 are direct summands of M, N respectively. Hence $M/\perp_{i=1}^m M_i$, $N/\perp_{i=1}^m N_i$ are finite cyclic groups and $[M: \perp_{i=1}^m M_i] = [OM: \perp_{i=1}^m OM_i]^{1/[k:Q]} = [ON: \perp_{i=1}^m ON_i]^{1/[k:Q]}$ $= [N: \perp_{i=1}^m N_i] = r$ (say). Let $x = r^{-1}(\mathrm{au} + \sum_{i=2}^m m_i)$ $y = r^{-1}(a'v + \sum_{i=2}^m n_i)$ be generators of $M/\perp_{i=1}^m M_i$, $N/\perp_{i=1}^m N_i$ respectively where $a, a' \in \boldsymbol{Z}$, $m_i \in M_i$ and $n_i \in N_i$. If $p^s \| r$, $p^s | a$, $(s \geqq 1)$, then $p^{-s}rx - p^{-s}au = p^{-s}\sum_{i=2}^m m_i$ is in M. Hence we have $p^{-s}m_i \in M_i$ since $\perp_{i=2}^m M_i$ is a direct summand of M. This implies $p^{-s}rx \in \perp_{i=1}^m M_i$ and it contradicts the definition of x. Thus $p^s \| r$, $(s \geq 1)$ yields $p^s \nmid a$ and similarly $p^s \nmid a'$. Suppose that $m_j \equiv 0$ (rM_j) for some $j \geq 2$; then any element m in M can be written as $m = cx + \sum_{i=1}^m m'_i$, $(c \in \boldsymbol{Z}, m'_i \in M_i)$ and $m = (c(x - r^{-1}m_j) + \sum_{i \neq j} m'_i) + (m'_j + cr^{-1}m_j)$. Hence we have $M = M_j \perp M_j^\perp$. From $\sigma(O_kM_j) = O_kN_j$ follows $\sigma(O_kM_j^\perp) = O_kN_j^\perp$. Applying induction to $\sigma(O_kM_j^\perp) = O_kN_j^\perp$, we complete the proof in this case. Now we suppose $m_j \not\equiv 0(rM_j)$ for every $j \geq 2$. There is an element $b \in O_k$ such that $\sigma(x) \equiv by \bmod O_k(\perp_{i=1}^m N_i)$. This is equivalent to $a \equiv a'b \bmod rO_k$ and $\sigma(m_i) \equiv bn_i \bmod rO_kN_i$. Since there is $b' \in O_k$ such that $\sigma(b'x) \equiv y \bmod O_k(\perp_{i=1}^m N_i)$, b is a unit modulo rO_k. Hence we have $(a, r) = (a', r) = a''$ and $r/a'' \equiv 0(p)$ if $r \equiv 0(p)$. From this follows that b is congruent to a rational integer modulo pO_k for each prime $p | r$. Fix $j \geq 2$ and any prime p such that $p^s \| r$, $m_j \notin p^sM_j$. Take a basis $w_1, w_2, \cdots$ of N_j so that $n_j = cw_1$, $\varepsilon_j\sigma(m_j) = dw_1 + ew_2$, $(c, d, e \in Z)$. Then $\sigma(m_j) \equiv bn_j \bmod rO_kN_j$ implies $d \equiv \varepsilon_j bc \bmod rO_k$ and $e \equiv 0(r)$. $m_j \notin p^sM_j$ yields $\varepsilon_j\sigma(m_j) = dw_1 + ew_2 \notin p^sN_j$ since $\varepsilon_j\sigma(M_j) = N_j$. Therefore we have $d \not\equiv 0(p^s)$ and $\varepsilon_j^{-1} \equiv f \bmod p$ for some $f \in Z$. Then $f^2 \equiv \varepsilon_j^{-1}\overline{\varepsilon_j^{-1}} \equiv 1 \bmod p$ implies $f \equiv \pm 1 \bmod p$ and $\pm\varepsilon_j \equiv 1 \bmod pO_k$, and from this follows easily $\varepsilon_j = \pm 1$ and $\sigma(M_j) = N_j$ for each $j \geq 1$. Hence we have $\sigma(QM)$ and QN and $\sigma(O_kM) = O_kN$ imply $\sigma(M) = N$. This completes the proof.

THEOREM. *Let M, N be positive Z-lattices and σ an isometry from O_kM on O_kN. Assume that k is of E-type or* rank $M \leq 42$. *Then there exist orthogonal decompositions $M = \perp_{i=1}^t M_i$, $N = \perp_{i=1}^t N_i$ and roots of unity ε_i in k such that $\varepsilon_i\sigma(M_i) = N_i$. Especially M, N are isometric.*

Proof. Denote by $\widetilde{O_kM}$ O_kM as a Z-module with bilinear form $\mathrm{tr}_{k/Q}(\ ,\ )$. Then $\widetilde{O_kM}$ is isometric to $\tilde{O}_k \otimes M$. Since $\tilde{O}_k$ or M is of E-type, any minimal vector of $\tilde{O}_k \otimes M$ is of form $\varepsilon \otimes m$ by Lemma 1 in § 1 where ε is a root of unity in k and m is a minimal vector m of M. Hence for a minimal vector m of M we have $\sigma(m) = \varepsilon n$ where ε is a root of unity in k and n is a minimal vector of N, compairing minimal vectors in $\tilde{O}_k \otimes M$, $\tilde{O}_k \otimes N$. Putting $\sigma' = \varepsilon^{-1}\sigma$, we get an isometry σ' from O_kM on O_kN such that $\sigma'(m) = n$ and $\sigma'(O_km^\perp) = O_kn^\perp$. Applying induction on rank M to $\sigma'(O_km^\perp) = O_kn^\perp$, we complete the proof by virtue of Lemma.

§ 3. Let k be an algebraic number field and G a finite subgroup in $GL(n, O_k)$. Denote by L Z^n (row vectors); then G operates on $O_kL = O_k^n$ from the left as product of matrices. Then we call G A-type if there is a direct decomposition $L = \oplus_{i=1}^m L_i$ such that for each $g \in G$, there exist roots of unity $\varepsilon_i(g)$ in k and a permutation $s(g) \in S_m$ satisfying $\varepsilon_i(g)gL_i = L_{s(g)i}$ for $i = 1, 2, \cdots, m$.

LEMMA. *Let k be a Galois extension of $\boldsymbol{Q}$ and assume that the complex conjugate induces an element of the center of $G(k/\boldsymbol{Q})$. For an indecomposable positive $\boldsymbol{Z}$-lattice L, O_kL is also indecomposable.*

Proof. For a positive $\boldsymbol{Z}$-lattice M O_kM is a positive definite (at every infinite prime) Hermitian lattice and for such lattices the uniqueness of decompositions to indecomposable ones holds as 105: 1 in [7]. Hence this lemma is proved quite similarly to Theorem 4 in [4].

THEOREM. *Let k be a Galois extension and assume that the complex conjugate induces an element of the center of $G(k/\boldsymbol{Q})$. Then every $G(k/\boldsymbol{Q})$-stable finite subgroup G in $GL(n, O_k)$ is of A-type if k is of E-type or $n \leq 42$.*

Proof. Put $A = \sum_{g\in G} {}^t g\bar{g}$ where the bar denotes the complex conjugate; then A is a positive definite symmetric matrix with rational entries. Put $L = \boldsymbol{Z}^n$ (row vectors) and $(x, y) = {}^t xA\bar{y}$ for $x, y \in O_kL$. For $g \in G$ we have $(gx, gy) = (x, y)$ and $gO_kL = O_kL$. Hence $g \in G$ induces an isometry of O_kL. Since L is a positive $\boldsymbol{Z}$-lattice by (,), there is the orthogonal decomposition $L = \perp_{i=1}^m L_i$ where L_i is indecomposable. By Lemma $O_kL = \perp_{i=1}^m O_kL_i$ is the decomposition to indecomposable lattices. Hence for $g \in G$ there is a permutation $s \in S_m$ such that $g(O_kL_i) = O_kL_{s(i)}$, $(i = 1, \cdots, m)$. Applying Theorem in § 2, there is a root of unity $\varepsilon_i \in O_k$ such that $\varepsilon_i gL_i = L_{s(i)}$. This completes the proof.

Remark. By using this theorem, we can show a lemma corresponding to Lemma 2 in [3] without the assumption that the complex conjugate induces an element of the center of $G(k/\boldsymbol{Q})$.

REFERENCES

[1] H.-J. Bartels, Zur Galoiskohomologie definiter arithmetischer Gruppen, J. reine angew. Math. **298** (1978), 89–97.
[2] H.-J. Bartels, Definite arithmetische Gruppen, J. reine angew. Math. **301** (1978), 27–29.
[3] H.-J. Bartels and Y. Kitaoka, Endliche arithmetische Untergruppen der GL_n, to appear.
[4] Y. Kitaoka, Scalar extension of quadratic lattices, Nagoya Math. J. **66** (1977), 139–149.
[5] ——, Scalar extension of quadratic lattices II, Nagoya Math. J. **67** (1977), 159–164.

[6] Y. Kitaoka, Tensor products of positive definite quadratic forms IV, to appear.
[7] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, Berlin, 1963.

Department of Mathematics
Nagoya University