Y. Kitaoka
Nagoya Math. J.
Vol. 66 (1977), 139-149

SCALAR EXTENSION OF QUADRATIC LATTICES

YOSHIYUKI KITAOKA

Let E/F be a finite extension of algebraic number fields, O_E, O_F the maximal orders of E, F respectively. A classical theorem of Springer [6] asserts that an anisotropic quadratic space over F remains anisotropic over E if the degree $[E:F]$ is odd. From this follows that regular quadratic spaces U, V over F are isometric if they are isometric over E and $[E:F]$ is odd. Earnest and Hsia treated similar problems for the spinor genera [2, 3]. We are concerned with the quadratic lattices. Let L, M be quadratic lattices over O_F in regular quadratic spaces U, V over F respectively. Assume

(*) there is an isometry σ from $O_E L$ onto $O_E M$, where $O_E L, O_E M$ denote the tensor products of O_E and L, M over O_F respectively. Then our question is whether the assumption implies $\sigma(L) = M$ or not. The affirmative answer would imply that L, M are already isometric over O_F. Obviously the answer is negative if the quadratic space EU ($\cong EV$) is indefinite. Even if we suppose that EU is definite, the answer is still negative in general. However there are many cases in which the answer is affirmative if EU is definite. We give such examples in this paper.

Through this paper $Q(x), B(x, y)$ denote quadratic forms and corresponding bilinear forms ($2B(x, y) = Q(x + y) - Q(x) - Q(y)$). Notations and terminologies will be those of O'Meara [5].

THEOREM 1. *Let m be a natural number ≥ 2, and E be a totally real algebraic number field with degree m, and assume that L, M be definite quadratic lattices over the ring $\boldsymbol{Z}$ of rational integers. Then the assumption*[*] (*) implies $\sigma(L) = M$ if E does not intersect with a finite set of (explicitely determined) algebraic integers which are not dependent on L, M, but on m.*

THEOREM 2. *Let E be totally real, and L, M be definite quadratic*

Received May 20, 1976.

*) In Theorem 1, 2, and 3 F is the field $\boldsymbol{Q}$ of rational numbers.

lattices over $\boldsymbol{Z}$ *with rank* $L = \operatorname{rank} M \leq 5$. *The assumption**) (*) *implies* $\sigma(L) = M$ *if* E *does not contain any of* $\sqrt{2}$, $\sqrt{3}$ *and* $\sqrt{5}$ *in case of* $\operatorname{rank} L = \operatorname{rank} M = 5$.

COROLLARY. *Let* E, K *be a totally real algebraic number field and an imaginary quadratic field respectively whose discriminants are relatively prime. Then an ideal of* K *is principal if it is principal in the composite field* KE.

THEOREM 3. *Let* E *be a totally real algebraic number field with* $[E: \boldsymbol{Q}] \leq 5$, *and* L, M *be definite quadratic lattices over* $\boldsymbol{Z}$. *Then the assumption**) (*) *implies* $\sigma(L) = M$.

In case that $L = M$ and σ is associated with an orthogonal decomposition of $O_E L$ we have

THEOREM 4. *Let* E/F *be a Galois extension of totally real algebraic number fields. Assume that* F *is the only field between* E *and* F *which is unramified over* F. *If a definite quadratic lattice* L *over* O_F *is decomposable over* O_E, *i.e.*, $O_E L = L_1' \perp L_2'$, *then there is a decomposition of* $L, L = L_1 \perp L_2$, *with* $L_i' = O_F L_i$ $(i = 1, 2)$, *in other words, a definite indecomposable quadratic lattice over* O_F *remains indecomposable over* O_E.

COROLLARY. *Let* E *be a totally real algebraic number field, and* L *be a definite indecomposable quadratic lattice over* $\boldsymbol{Z}$. *Then* $O_E L$ *is also indecomposable.*

We give some other sufficient conditions to the affirmative answer of our question.

THEOREM 5. *Let* F *be totally real and* $E = F(\sqrt{a})$ *be a totally real quadratic extension, and let* L, M *be definite quadratic lattices over* O_F *and suppose that there is an isometry* σ *from* $O_E L$ *onto* $O_E M$. *Then, one of the following conditions on* O_E:

(i) $O_E = O_F + A\sqrt{a}$, *where* A *is an ideal of* F *such that* $A^2 a \neq O_F$,

(ii) $O_E = O_F + Ax$, *where* A *is an ideal of* F, $x^2 \notin F$, *and* $N_{E/F} x$ *is totally negative,*

implies $\sigma(L) = M$.

THEOREM 6. *Let* E/F *be a Galois extension of totally real algebraic number fields, and assume that* F *is the only field between* E *and* F

which is unramified over F. Let L, M be definite quadratic lattices over O_F and let σ be an isometry from $O_E L$ onto $O_E M$. Then we get $\sigma(L) = M$ if $\sigma(L) \subset M + 2O_E M$.

1.1. Let E be a totally real algebraic number field with degree m, and L be a positive definite quadratic lattice over $\boldsymbol{Z}$ with rank $n \leq m$.

LEMMA. *Let v_0 be an element in $O_E L$ such that $Q(v_0) = \min Q(v)$, where v runs over non-zero elements of $O_E L$ with $Q(v) \in \boldsymbol{Q}$. Then v_0 is in L if E does not intersect with a finite set of (explicitely determined) algebraic integers which are not dependent on L but m.*

Proof. We denote by $B(\ ,\ )$ the bilinear form associated with L as indicated in the introduction. There exists a $\boldsymbol{Z}$-basis $\{e_i\}$ of L such that $(B(e_i, e_j)) = D[T]$, where $D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$, $T = \begin{pmatrix} 1 & & t_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ satisfy $d_i \leq \frac{4}{3} d_{i+1}$, $(i = 1, \cdots, n-1)$, $|t_{ij}| \leq \frac{1}{2}$, $(i < j)$, (p. 20 in [1]). Put $v_0 = \sum x_i e_i$ $(x_i \in O_E)$, and $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & & t_{ij} \\ & \ddots & \\ & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = T\boldsymbol{x}$. Then $Q(v_0) = \sum d_i y_i^2 \leq d_1$ since $d_1 = Q(e_1)$ is a rational number. This implies $|y_i| \leq \sqrt{d_1/d_i}$ and so $\boldsymbol{x} = T^{-1}\boldsymbol{y}$ implies $|x_i| < c$, where c is explicitely calculated. Since $B(e_i, e_j) \in \boldsymbol{Q}$, taking a conjugate of the equation $Q(v_0) = (B(e_i, e_j))$ $[\boldsymbol{x}]$, we see $|x_i^{(j)}| < c$, where $x_i^{(j)}$ is a conjugate of x_i. Denote by S the set of algebraic integers x with $1 < [\boldsymbol{Q}(x) : \boldsymbol{Q}] \leq m$ such that the absolute values of conjugates of x is smaller than c. Then S is a finite set. If E contains no element of S, x_i is rational. Hence v_0 is in L.

For simplicity we call v_0 in Lemma an element which gives the rational minimum of $O_E L$.

1.2. *Proof of Theorem* 1. We may suppose that L, M are positive definite by scaling if necessary. We assume that E contains no element of S. We take an element v_0 of $O_E L$ which gives the rational minimum of $O_E L$. Let σ be an isometry from $O_E L$ onto $O_E M$; $\sigma(v_0)$ is an element which gives the rational minimum of $O_E M$. Let $O_E = \boldsymbol{Z}[\omega_1, \cdots, \omega_m]$ and put $v_0 = \sum \omega_i v_i$ and $L_0 = \boldsymbol{Z}[v_1, \cdots, v_m]$; the rank $L_0 \leq m$ and $v_0 \in O_E L_0$ is an element which gives the rational minimum of $O_E L_0$. Hence Lemma in 1.1 implies $v_0 \in L_0 \subset L$. Similarly we get $\sigma(v_0) \in M$. Now we have

https://doi.org/10.1017/S0027763000017773 Published online by Cambridge University Press

$\sigma(O_E(v_0^{\perp} \text{ in } L)) = \sigma(v_0^{\perp} \text{ in } O_E L) = \sigma(v_0)^{\perp} \text{ in } O_E M = O_E(\sigma(v_0)^{\perp} \text{ in } M)$. Theorem 1 is inductively proved.

2.1. The following lemma (Theorem 2.1 on p. 47 in [4]) is fundamental to prove Theorems 2, 3.

LEMMA. *Let a be a totally real algebraic integer such that the absolute values of the conjugates over $\boldsymbol{Q}$ are less than 2. Then a is of the form $2\cos r\pi$ $(r \in \boldsymbol{Q})$.*

Proof. Put $b = \sqrt{a^2/4 - 1}$; then the assumption implies that b^2 is totally negative. Since $a/2 + b$ satisfies the equation $x^2 - ax + 1 = 0$, $a/2 + b$ is an algebraic integer and the absolute values of the conjugates are 1. Hence $a/2 + b$ is a root of the unity. This completes the proof.

COROLLARY. *Let a be a totally real algebraic integer such that the absolute values of the conjugates are less than $\frac{16}{9}$. Then $a = 0, \pm 1, \pm\sqrt{2}, \pm(1 \pm \sqrt{5})/2$ or $\pm\sqrt{3}$.*

Proof. Lemma implies Corollary immediately.

2.2. Let E be a totally real algebraic number field and L be a positive definite quadratic lattice over $\boldsymbol{Z}$ with rank $L \leq 5$.

LEMMA. *If v_0 is an element of $O_E L$ which gives the rational minimum of $O_E L$, then v_0 is in L if E does not contain any of $\sqrt{2}, \sqrt{3}$ and $\sqrt{5}$ in case of* rank $L = 5$.

Proof. Put $n = \operatorname{rank} L$; then there is a basis $\{u_i\}$ of L such that $(B(u_i, u_j)) = D[T]$, where $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ with $d_i/d_{i+1} \leq \frac{4}{3}$ $(1 \leq i \leq n-1)$, $T = \begin{pmatrix} 1 & & t_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ $(|t_{ij}| \leq \frac{1}{2})$. Put $v_0 = \sum \omega_i u_i$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = T \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$; then $\sum d_i x_i^2 = Q(v_0) \leq d_1 = Q(u_1)$. Since $Q(v_0)$ and $B(u_i, u_j)$ are rational, we have $\sum d_i x_i'^2 = Q(v_0) \leq d_1$, where $\begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix} = T \begin{pmatrix} \omega_1' \\ \vdots \\ \omega_n \end{pmatrix}$ and $\{\omega_i'\}$ is any conjugate of $\{\omega_i\}$. Let $n = 2$; then we get $d_2 x_2^2 \leq d_1$. Hence $|\omega_2| = |x_2| \leq \sqrt{d_1/d_2} \leq 2/\sqrt{3}$. Corollary in 2.1 implies $\omega_2 = 0$ or ± 1. If $\omega_2 = 0$, then $\omega_1 = x_1$

https://doi.org/10.1017/S0027763000017773 Published online by Cambridge University Press

and $d_1\omega_1^2 \leq d_1$. Therefore $\omega_1 = 0$ or ± 1, and $v_0 \in L$. If $\omega_2 = \pm 1$, then $d_1x_1^2 \leq d_1 - d_2$. This yields $|x_1| \leq \sqrt{1 - d_2/d_1} \leq \frac{1}{2}$, and $|\omega_1| = |x_1 - t_{12}x_2| \leq \frac{1}{2} + \frac{1}{2} = 1$. Hence $\omega_1 = 0$ or ± 1 and v_0 is in L. Let $n = 3$; then $d_3x_3^2 \leq d_1$ implies $|\omega_3| = |x_3| \leq \sqrt{d_1/d_3} \leq \frac{4}{3}$. Hence $\omega_3 = 0$ or ± 1. If $\omega_3 = 0$, then v_0 is a vector which gives the rational minimum of $O_E[u_1, u_2]$, and so v_0 is in $\boldsymbol{Z}[u_1, u_2] \subset L$. Suppose $\omega_3 = \pm 1$; then $d_2x_2^2 \leq d_1 - d_3$ implies $|x_2| \leq \sqrt{d_1/d_2 - d_3/d_2} \leq \sqrt{\frac{4}{3} - \frac{3}{4}} = \sqrt{\frac{7}{12}}$. Since $\omega_2 = x_2 - t_{23}\omega_3$, $|\omega_2| \leq \sqrt{\frac{7}{12}} + \frac{1}{2}$. Hence we get $\omega_2 = 0$ or ± 1, and v_0 is a vector which gives the rational minimum of $O_E[u_1, \omega_2u_2 + \omega_3u_3]$. Hence $v_0 \in \boldsymbol{Z}[u_1, \omega_2u_2 + \omega_3u_3] \subset L$. Let $n = 4$; then $|\omega_4| \leq \sqrt{d_1/d_4} \leq \sqrt{(\frac{4}{3})^3}$. Hence $\omega_4 = 0$, ± 1 or $\pm\sqrt{2}$. As above we may assume $\omega_4 \neq 0$. Since $|x_3| \leq \sqrt{d_1/d_3 - d_4\omega_4^2/d_3} \leq \sqrt{\frac{16}{9} - \frac{3}{4}\omega_4^2}$, we have $|\omega_3| \leq \sqrt{\frac{16}{9} - \frac{3}{4}\omega_4^2} + \frac{1}{2}|\omega_4|$. Hence $\omega_4 = \pm 1$ implies $\omega_3 = 0$, ± 1 or $\pm\sqrt{2}$, and $\omega_4 = \pm\sqrt{2}$ implies $\omega_3 = 0$ or ± 1. As above we may exclude the cases $\omega_3 = 0$, and $|\omega_3| = |\omega_4| = 1$. Therefore we assume either $|\omega_3| = \sqrt{2}$, $|\omega_4| = 1$ or $|\omega_3| = 1$, $|\omega_4| = \sqrt{2}$. Since $x_2^2 \leq d_1/d_2 - d_3x_3^2/d_2 - d_4x_4^2/d_2 \leq \frac{4}{3} - \frac{3}{4}(\omega_3 + t_{34}\omega_4)^2 - \frac{9}{16}\omega_4^2$, we get $x_2^2 \leq -\frac{11}{12} + \frac{3}{4}\sqrt{2}$. Hence $|\omega_2| = |x_2 - t_{23}\omega_3 - t_{24}\omega_4| \leq \sqrt{\frac{3}{4}\sqrt{2} - \frac{11}{12}} + \frac{1}{2}(1 + \sqrt{2}) \leq 1.59$. This implies $\omega_2 = 0$, ± 1 or $\pm\sqrt{2}$. If $\omega_2 = 0$ or ± 1, then v_0 is a vector which gives the rational minimum of $O_E[u_1, \omega_2u_2 + \omega_3u_3, u_4]$ ($|\omega_4| = \sqrt{2}$) or $O_E[u_1, \omega_2u_2 + \omega_4u_4, u_3]$ ($|\omega_4| = 1$), and so v_0 is in L. If $|\omega_2| = \sqrt{2}$, then v_0 is in $O_E[u_1, u_3, 1/\sqrt{2}(\omega_2u_2 + \omega_4u_4)]$ ($|\omega_4| = \sqrt{2}$) or $O_E[u_1, u_4, 1/\sqrt{2}(\omega_2u_2 + \omega_3u_3)]$ ($|\omega_4| = 1$), and v_0 is in L. Let $n = 5$; then $d_5x_5^2 \leq d_1$ implies $|\omega_5| = |x_5| \leq \frac{16}{9}$. From the assumption follows $\omega_5 = 0$ or ± 1. We may exclude $\omega_5 = 0$. Hence $x_4^2 \leq d_1/d_4 - d_5/d_4 \leq (\frac{4}{3})^3 - \frac{3}{4}$ and $|\omega_4| \leq |x_4 - t_{45}\omega_5| \leq \sqrt{(\frac{4}{3})^3 - \frac{3}{4}} + \frac{1}{2} \leq \frac{16}{9}$, and so $\omega_4 = 0$ or ± 1. This yields $v_0 \in L$. Thus, we have completed the proof.

2.3. *Proof of Theorem* 2. Without the loss of generality we may assume that L, M are positive definite. If v_0 is an element which gives the rational minimum of O_EL, then $\sigma(v_0)$ is an element which gives the rational minimum of O_EM, where σ is an isometry from O_EL onto O_EM, so that Lemma in 2.2 implies $v_0 \in L$, $\sigma(v_0) \in M$. By induction with respect to rank L = rank M as in the proof of Theorem 1, we complete the proof of Theorem 2.

2.4. *Proof of Theorem* 3. Let E be a totally real algebraic number field with $[E: \boldsymbol{Q}] \leq 5$, and L, M be definite quadratic lattices over $\boldsymbol{Z}$. As in 2.3 we may assume that L, M are positive definite. To prove Theorem

https://doi.org/10.1017/S0027763000017773 Published online by Cambridge University Press

3 it suffices to show that an element which gives the rational minimum of $O_E L, O_E M$ is in L, M respectively. Let $N = L$ or M and v_0 be an element which gives the rational minimum of $O_E N$. Take a Z-basis $\{\omega_1, \cdots, \omega_n\}$ of O_E and put $v_0 = \sum \omega_i v_i$, where $v_i \in N$. Since v_0 is an element which gives the rational minimum of $O_E N_0$, $N_0 = Z[v_1, \cdots, v_n]$, and rank $N_0 \leq 5$, Lemma in 2.2 implies $v_0 \in N_0 \subset N$.

2.5. *Remark.* If Lemma in 2.2 is true without the restriction on the rank of L, our assumption (*) implies $\sigma(L) = M$ under the situation that E is totally real, F is the field Q of rational numbers, and L, M are positive definite quadratic lattices over Z. The author knows no counterexamples.

2.6. *Proof of Corollary of Theorem* 2. Let A be an ideal of K such that A is principal in the composite field KE. Since discriminants of K, E are relatively prime, $O_{KE} = O_K O_E$. Hence we get $O_{KE}A = O_E A = \lambda O_E O_K$, where λ is an element of KE. Putting $A = Z[u_1, u_2]$, $O_K = Z[v_1, v_2]$, we have $(\lambda v_1, \lambda v_2) = (u_1, u_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, O_E)$. Let $x, y \in O_E$ and NA be the norm of A in K; then

$$\begin{aligned} &NA^{-1}|(xa + yb)u_1 + (xc + yd)u_2|^2 \\ &\quad = NA^{-1}|\lambda(v_1 x + v_2 y)|^2 = |\lambda|^2 NA^{-1}|v_1 x + v_2 y|^2 . \end{aligned}$$

On the other hand, the discriminants of binary quadratic forms $NA^{-1}|xu_1 + yu_2|^2$, $|v_1 x + v_2 y|^2$ are equal to the discriminant of K. Comparing the both sides of the above equation, we have $(ad - bc)^2 = (|\lambda|^2 NA^{-1})^2$. Put $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \sqrt{|\lambda|^{-2} NA}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; then $a'd' - b'c' = \pm 1$ and $NA^{-1}|(xa' + yb')u_1 + (xc' + yd')u_2|^2 = |v_1 x + v_2 y|^2$. Moreover $|\lambda|^2$ is totally positive since $|\lambda|^2 = \alpha^2 + \delta\beta^2$ where $\lambda = \alpha + \sqrt{-\delta}\beta$, $K = Q(\sqrt{-\delta})$. In other words, the binary positive definite quadratic forms associated with the ideal A, O_K are equivalent over $O_{E(\sqrt{|\lambda|^2 NA^{-1}})}$. From Theorem 2 follows that they are equivalent over Z. This means that A is principal.

3. *Proof of Theorem* 5. Without the loss of generality we may assume that L, M be positive definite at each infinite place by scaling.

Suppose that O_E satisfies the first condition (i). Regarding $O_E L$ as a quadratic lattice over O_F with bilinear form $\mathrm{tr}_{E/F} B(x, y)$, $O_E L$ has the orthogonal decomposition to indecomposable quadratic lattices $O_E L = L_1$

$\perp \cdots \perp L_m \perp A\sqrt{a}L_1 \perp \cdots \perp A\sqrt{a}L_m$, where $L = L_1 \perp \cdots \perp L_m$ is the orthogonal decomposition of L to indecomposable quadratic lattices. Let $M = M_1 \perp \cdots \perp M_n$ be the orthogonal decomposition of M to indecomposable quadratic lattices. The isometry σ gives an isometry from $O_E L$ onto $O_E M$, which are regarded as definite quadratic lattices over O_F as above, and so $n = m$. If $\sigma L_1 = M_i$, then $\sigma(O_E(\perp_{i\geq 2} L_i)) = O_E(\perp_{j\neq i} M_j)$, and Lemma is inductively proved. Hence we may assume $\sigma(L_i) = A\sqrt{a}M_{\alpha(i)}$, where $\alpha(i)$ is a permutation of the set $\{1, 2, \cdots, m\}$. Thus we have $\sigma(L) = A\sqrt{a}M$. Comparing the volumes of the both sides, $(A\sqrt{a})^2 = O_F$. This is a contradiction. Next we suppose the second condition (ii) on O_E. Put $\sigma(v) = \varphi_1(v) + x\varphi_2(v)$, where $v \in L$, $\varphi_1(v) \in M$, $\varphi_2(v) \in AM$. We may assume $x = \sqrt{a} + b$ $(0 \neq b \in F)$. Since $Q(v) = Q(\sigma(v)) = Q(\varphi_1(v)) + 2xB(\varphi_1(v), \varphi_2(v)) + x^2Q(\varphi_2(v)) \in F$, we get $Q(v) = Q(\varphi_1(v)) + 2bB(\varphi_1(v), \varphi_2(v)) + (a + b^2)Q(\varphi_2(v))$, $B(\varphi_1(v), \varphi_2(v)) + bQ(\varphi_2(v)) = 0$. Thus $Q(v) = Q(\varphi_1(v)) + (a - b^2)Q(\varphi_2(v)) = Q(\varphi_1(v)) - N_{E/F}(x)Q(\varphi_2(v))$, and we see that φ_1 is injective. From our assumption follows that $Q(v) - Q(\varphi_1(v))$ is zero or totally positive. Similarly we get an injective mapping φ_1' from M to L such that $Q(v) - Q(\varphi_1'(v))$ is zero or totally positive if $v \in M$. Put $\varphi = \varphi_1'\varphi_1$; then φ is an injective endomorphism of L such that $Q(v) - Q(\varphi(v))$ is zero or totally positive. Let $\{v_i\}$ be elements of L such that $[L : O_F[\cdots, v_i, \cdots]] < \infty$. From the property of φ follows that there is a natural number k such that $Q(\varphi^k(v_i)) = Q(\varphi^{k+1}(v_i))$ for any index i. Since φ is monomorphism, we may suppose that v_i themselves satisfy $[L; O_F[\cdots, v_i, \cdots]] < \infty$ and $Q(v_i) = Q(\varphi(v_i))$ instead of $\varphi^k(v_i)$. Thus

$$Q(v_i) - Q(\varphi(v_i)) = Q(v_i) - Q(\varphi_1(v_i)) + Q(\varphi_1(v_i)) - Q(\varphi_1'\varphi_1(v_i)) = 0$$

implies $Q(v_i) = Q(\varphi_1(v_i))$ and $Q(\varphi_2(v_i)) = 0$. Hence we get $\varphi_2(v_i) = 0$ and $\varphi_2 = 0$. This means $\sigma(L) \subset M$. Similarly we get $\sigma^{-1}(M) \subset L$. Hence $\sigma(L) = M$.

4. *Proof of Theorem* 4. Let E/F be a Galois extension of totally real algebraic number fields satisfying the assumption in Theorem 4, and L be an indecomposable definite quadratic lattice over O_F. It suffices to prove $O_E L$ is still indecomposable. Suppose that $O_E L$ is not indecomposable, i.e., $O_E L = L_1 \perp \cdots \perp L_m$ $(m > 1)$, where each L_i is indecomposable. Denote by G the Galois group $G(E/F)$ and operate G on $O_E L$ as follows: $g(av) = g(a)v$ for $a \in O_E$, $v \in L$, $g \in G$. Then $gB(x, y) = B(g(x), g(y))$ $(x, y \in O_E L)$ implies $O_E L = g(L_1) \perp \cdots \perp g(L_m)$ for $g \in G$. From the

https://doi.org/10.1017/S0027763000017773 Published online by Cambridge University Press

uniqueness of the orthogonal decomposition of a definite quadratic lattice to indecomposable lattices follows $g(L_i) = L_{g(i)}$, where $g(i)$ stands for a permutation. If G does not operate on the set $\{L_i\}$ transitively, then there is a decomposition $O_E L = L_1' \perp L_2'$, where L_i' is G-invariant as a set. Let v be an element of L; then $v = v_1 + v_2$ ($v_1 \in L_1'$, $v_2 \in L_2'$). Since $v = gv = g(v_1) + g(v_2)$ and $g(v_i) \in L_i'$ for any g in G, $gv_i = v_i$ for any g in G. This implies $v_i \in L$. Hence $L = (L_1' \cap L) \perp (L_2' \cap L)$. This contradicts our assumption. Thus G operates on the set $\{L_i\}$ transitively. Put $H = \{g \in G; gL_1 = L_1\}$ and $g_i L_1 = L_i$, $G = \bigcup_{i=1}^m g_i H$. From our assumption $m > 1$ follows $H \neq G$. Put $K = \{a \in E; h(a) = a$ for any h in $H\}$, and $M_1 = \{v \in L_1; h(v) = v$ for any h in $H\}$. Let $v = \tilde{v}_1 + \tilde{v}_2$ be an element in $O_K L$ ($\tilde{v}_1 \in L_1$, $\tilde{v}_2 \in \perp_{i \geq 2} L_i$); then $v = h(v) = h(\tilde{v}_1) + h(\tilde{v}_2)$ implies $h(\tilde{v}_i) = \tilde{v}_i$ ($i = 1, 2$) for any h in H. Hence $O_K L = M_1 \perp (O_K L \cap \perp_{i \geq 2} L_i)$. This implies $L_1 = O_E M_1$. Let $M_1 = O_K v_1 \oplus \cdots \oplus O_K v_{r-1} \oplus A v_r$, where A is an ideal of K such that A and the relative discriminant $D(E/F)$ of E/F are relatively prime. Similarly let $L = O_F u_1 \oplus \cdots \oplus O_F u_{n-1} \oplus B u_n$ ($n = mr$), where B is an ideal of F such that B and $D(E/F)$ are relatively prime. Put $v_i = \sum_{j=1}^n a_{ij} u_j$ ($a_{ij} \in E$), and $u_i = \sum_{j=1}^m g_j(w_{j,i})$, where $w_{j,i}$ is an element of L_1. Since v_i is fixed by H and $gu_i = u_i$ ($g \in G$), a_{ij} is an element of K, and $u_i = \sum_j g_j(w_{j,i}) = \sum_j g g_j(w_{j,i})$ ($g \in G$). Comparing the components in L_1, we get $w_{1,i} = h(w_{j,i})$ ($h \in H$). Thus u_j is written as $\sum_{k=1}^m g_k(w_j)$ ($w_j \in M_1$). Putting $w_j = \sum_{t=1}^r b_{jt} v_t$ ($b_{jt} \in K$), we have $v_i = \sum_{j=1}^n a_{ij} u_j = \sum_{j=1}^n \sum_{k=1}^m a_{ij} g_k(w_j) = \sum_{j=1}^n \sum_{k=1}^m \sum_{t=1}^r a_{ij} g_k(b_{jt}) g_k(v_t)$. Thus $v_i = \sum_{j=1}^n \sum_{t=1}^r a_{ij} b_{jt} v_t$, $\sum_{j=1}^n \sum_{t=1}^r a_{ij} g_k(b_{jt}) g_k(v_t) = 0$ if $k > 1$. If we put $a_j = a_{1,j}$, $b_j = b_{j,1}$, then $\sum_{j=1}^n a_j b_j = 1$ and $\sum_{j=1}^n g(a_j) b_j = 0$ if $g \notin H$. From our assumption on ideals A, B follows that a_i, b_i are $\mathfrak{p}$-adic integers of K if $\mathfrak{p} | D(E/F)$. Let $O_K = O_F \omega_1 \oplus \cdots \oplus O_F \omega_{m-1} \oplus C\omega_m$, where C is an ideal of F such that C and $D(E/F)$ are relatively prime, and $a_i = \sum_{j=1}^m c_{ij} \omega_j$, $b_i = \sum_{t=1}^m d_{it} \omega_t$ and $f_{jt} = \sum_{i=1}^n c_{ij} d_{it}$; then $\sum_{j,t=1}^m f_{jt} \omega_j \omega_t = 1$, $\sum_{j,t=1}^m f_{jt} g(\omega_j) \omega_t = 0$ ($g \notin H$), and f_{ij} is a $\mathfrak{p}$-adic integer of F if $\mathfrak{p} | D(E/F)$. Putting $\Omega = (\omega_1, \cdots, \omega_m)$, ${}^t\Omega' = (\sum_{t=1}^m f_{1t} \omega_t, \cdots, \sum_{t=1}^m f_{mt} \omega_t)$, we have $\Omega\Omega' = 1$, $g(\Omega)\Omega' = 0$ if $g \notin H$. Hence we get

$$\begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix} \Omega' = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \boldsymbol{e} .$$

We define a permutation matrix M_i by

$$\begin{pmatrix} g_i g_1(\Omega) \\ \vdots \\ g_i g_m(\Omega) \end{pmatrix} = M_i \begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix}.$$

Then $M_i \begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix} g_i(\Omega') = \boldsymbol{e}$ implies

$$\begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix} (g_1(\Omega'), \cdots, g_m(\Omega')) = (M_1^{-1}\boldsymbol{e}, \cdots, M_m^{-1}\boldsymbol{e}) .$$

If $g(\Omega') = \Omega'$, then $g \in H$ since $\Omega\Omega' = 1$ and $g(\Omega)\Omega' = 1$. If $M_i^{-1}\boldsymbol{e} = M_j^{-1}\boldsymbol{e}$, then $\begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix} g_i(\Omega') = \begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix} g_j(\Omega')$ and $g_i(\Omega') = g_j(\Omega')$. Therefore $i = j$, and this means that $(M_1^{-1}\boldsymbol{e}, \cdots, M_m^{-1}\boldsymbol{e})$ is a permutation matrix. Thus we have

$$\det \begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix} \cdot \det (g_1(\Omega'), \cdots, g_m(\Omega')) = \pm 1 .$$

From our assumption follows that both components on the left side are $\mathfrak{p}$-adic integers if $\mathfrak{p} | D(E/F)$. Hence $\det \begin{pmatrix} g_1(\Omega) \\ \vdots \\ g_m(\Omega) \end{pmatrix}$ is a $\mathfrak{p}$-adic unit if $\mathfrak{p} | D(E/F)$, and this implies that K is unramified over F. This is a contradiction.

4.1. *Proof of Corollary of Theorem* 4. If E is a totally real algebraic number field, then there is a totally real algebraic number field $\tilde{E}$ which is a Galois extension of $\boldsymbol{Q}$ and contains E. If $O_E L$ is decomposable, then $O_{\tilde{E}} L$ is also decomposable. This contradicts Theorem 4.

4.2. If E/F is an unramified extension of totally real algebraic number fields, then we will show that there is an indecomposable definite quadratic lattice over O_F which is decomposable over O_E. We take an unramified Galois extension K/F where K is totally real and contains E. Denote by $G = \{g_1 = 1, g_2, \cdots, g_m\}$ the Galois group of K/F. Let V be

https://doi.org/10.1017/S0027763000017773 Published online by Cambridge University Press

an m-dimensional quadratic space over F with orthonormal basis $\{v_i\}$. We define the operation of G to KV by $g_i(av_1) = g_i(a)v_i$ $(a \in K)$. Put $\tilde{L} = O_K v_1 \perp \cdots \perp O_K v_m (\subset KV)$ and $L = \{\sum_{i=1}^m g_i(a)v_i ; a \in O_K\}$. By definition, G operates trivially on L. Since K/F is unramified, there are elements $a_1, \cdots, a_m$ in O_K such that $(g_i(a_j))$ is a unimodular matrix at a given prime. Hence $\tilde{L} = O_K L$. If L is decomposable, and $L = L_1 \perp L_2$, then $O_K L_1$ is an orthogonal sum of a proper subset of $\{O_K v_i\}$. Thus $O_K L_1$ is not closed under the operation of G. This is a contradiction because G operates trivially on L_1. Denote the subgroup of G corresponding to E by H. Let $G = \bigcup Hh_i$ (coset decomposition) and put $\tilde{L}_i = \perp_{h \in H} O_K hh_i(v_1)$ which is closed under the operation of H; then $\tilde{L} = \perp_i \tilde{L}_i$. Decompose an element u in $O_E L$ as $u = \sum u_i$, $u_i \in \tilde{L}_i$. By definition $u = h(u) = \sum h(u_i)$ for h in H. Hence we get $h(u_i) = u_i$ and $O_E L = \perp (\tilde{L}_i \cap O_E L)$. Thus $O_E L$ is decomposable.

5. *Proof of Theorem* 6. Put $N = L \perp M$ and $\tilde{\sigma}$ be an isometry of $O_E N$ defined as $\tilde{\sigma}(u + m) = \sigma(u) + \sigma^{-1}(m)$ for $u \in O_E L$, $m \in O_E M$. If $\tilde{\sigma}(v) \equiv v \bmod 2O_E N$ for $v \in O_E N$, then $v = (v + \tilde{\sigma}(v))/2 + (v - \tilde{\sigma}(v))/2 \in N_+ \perp N_-$, where $N_\pm = \{u \in O_E N ; \tilde{\sigma}(u) = \pm u\}$. Thus $N_+ \perp N_- = \{v \in O_E N ; \tilde{\sigma}(v) \equiv v \bmod 2O_E N\}$. Since $v = u_1 + \sigma(u_2)$ $(u_1, u_2 \in O_E L)$ is in $N_+ \perp N_-$ if and only if $u_1 \equiv u_2 \bmod 2O_E L$, we get $N_+ \perp N_- = O_E\{u + \sigma(u) ; u \in L\} + 2O_E M$. Our assumption implies $\sigma(u) = m_u + 2v$ for $u \in L$, where $m_u \in M$, $v \in O_E M$. Thus $N_+ \perp N_- = O_E\{\{u + m_u ; u \in L\} + 2M\}$. By virtue of Theorem 4, there are sublattices $\tilde{N}_+, \tilde{N}_-$ of N such that $\{u + m_u ; u \in L\} + 2M = \tilde{N}_+ \perp \tilde{N}_-$ and $N_+ = O_E \tilde{N}_+$, $N_- = O_E \tilde{N}_-$. So, $\tilde{\sigma} = \pm 1$ on $N_\pm$ implies $\tilde{\sigma}(\tilde{N}_+) = \tilde{N}_+$, $\tilde{\sigma}(\tilde{N}_-) = \tilde{N}_-$. Thus $\tilde{\sigma}(FL \perp FM) = FL \perp FM$. Therefore $\tilde{\sigma}(L \perp M) = L \perp M$. This yields $\sigma L = M$.

6. *Remark.* Theorems 2, 3 are fairly improved by a different method which will appear in a subsequent paper.

References

[1] A. Borel, Introduction aux groupes arithmétiques, Hermann, Paris, 1967.
[2] A. G. Earnest and J. S. Hsia, Springer-type theorems for spinor genera of quadratic forms, Bull. Amer. Math. Soc., **81** (1975), 942–943.
[3] A. G. Earnest and J. S. Hsia, Spinor genera under field extension (to appear in Acta Arith.).
[4] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Warszawa, 1974.
[5] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, Berlin, 1963.

[6] T. A. Springer, Sur les formes quadratiques d'indice zéro, C. R. Acad. Sci., **234** (1952), 1517–1519.

Department of Mathematics
Nagoya University