J. Math. Soc. Japan
Vol. 21, No. 3, 1969

Class numbers of definite Hermitian forms

By Kenichi IYANAGA

(Received Nov. 22, 1968)

§ 0. Introduction.

G. Shimura has studied about the arithmetic of Hermitian forms over a quadratic extension K of an algebraic number field of finite degree k (cf. [7]). He proved that the special unitary class number of an indefinite Hermitian form is 1, and that the unitary class number of such a form can be described in terms of the class number of K.

Our purpose is to determine the (special unitary, and unitary) class numbers of definite Hermitian forms. In general, this problem does not seem to be easy. We have been able to get only very partial solutions.

M. Kneser has developed a method to determine the class numbers of definite quadratic forms in small numbers of variables with simple discriminants [4]. His method can be applied to determine the class numbers of certain families of Hermitian forms.

In particular, we get the following:

Let $K=\boldsymbol{Q}(\sqrt{-1})$, $k=\boldsymbol{Q}$. Take a vector space V over K with the bases $v_1, \cdots, v_n$. Let H be the Hermitian form determined by

$$H(v_i, v_j)=\delta_{ij}.$$

Let

$$L=\sum_{i=1}^{n} \boldsymbol{Z}[\sqrt{-1}]v_i$$

be the lattice in V.

In this case, it turns out that the unitary class number c_n of the lattice L and the special unitary class number c_n^1 of L, have the relation: $c_n \leqq c_n^1 \leqq (n, 4)\, c_n$ where $(n, 4)$ is the G.C.D. of n and 4; $c_n^1=1$ if $c_n=1$.

Moreover, we have $c_n>1$ if $n \geqq 5$, and $c_1=c_2=c_3=c_4=1$, $c_5=2$, $c_6=3$ and $c_7=4$. (In fact we can directly apply the results of M. Kneser [4] to get $c_i=1$ for $i=1, 2, 3, 4$.) $c_6^1=3$ or 4.

In § 1, we investigate the relations of the unitary class numbers and the special unitary class numbers. We will discuss about Kneser's method in § 2. In the last section, we will calculate the above c_n's.

I am grateful to Prof. M. Kneser and the referee of this paper who gave me helpful advice.

§ 1. Unitary class numbers and special unitary class numbers.

1.1. Let k be an algebraic number field of finite degree and K be a quadratic extension of k. We denote by $\mathcal{O}_k$ (resp. $\mathcal{O}_K$) the ring of integers in k (resp. K); and by σ the Galois involution of K/k.

Let V be a finite dimensional vector space over K supplied with a non-degenerate Hermitian form H which is sesqui-linear with respect to σ.

We put

$$G = SU(V, H), \qquad \tilde{G} = U(V, H)$$

and understand them to be k-rational points of algebraic groups defined over k.

Let L, M be $\mathcal{O}_K$-lattices in V (i.e. they are finitely generated $\mathcal{O}_K$-submodules of V and each of them contains a system of bases of V). We define

$$L \approx M \text{ (resp. } L \sim M)$$

if and only if there exists an element g of G (resp. of $\tilde{G}$) such that $L = gM$, and in that case we say that L and M belong to the same G (resp. $\tilde{G}$)-class.

For any prime ideal $\mathfrak{p}$ in k, we set

$$L_{\mathfrak{p}} = L \otimes \mathcal{O}_{\mathfrak{p}}, \qquad V_{\mathfrak{p}} = V \otimes k_{\mathfrak{p}},$$

where $\mathcal{O}_{\mathfrak{p}}$ is the ring of $\mathfrak{p}$-adic integers, and $k_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic number field.

By $G_{\mathfrak{p}}$ etc., we denote the $\mathfrak{p}$-adic completion of G etc..

Two lattices L and M are said to be of the same G (resp. $\tilde{G}$)-genus, if and only if $L_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$ belong to the same $G_{\mathfrak{p}}$ (resp. $\tilde{G}_{\mathfrak{p}}$)-class for each prime ideal $\mathfrak{p}$ in k. By $(L)_G$ (resp. $(L)_{\tilde{G}}$) we denote the set of all the lattices in V belonging to the same G (resp. $\tilde{G}$)-genus as L.

The number of G (resp. $\tilde{G}$)-classes among $(L)_G$ (resp. $(L)_{\tilde{G}}$) is known to be finite; we denote this number by $c^1(L, V)$ (resp. $c(L, V)$).

1.2. Given lattices L and M, it is known that there exist $\mathcal{O}_K$-ideals $\mathcal{A}_i$, $\mathcal{E}_i$ and elements e_i in V $(i = 1, \cdots, n)$ such that $\mathcal{E}_i \supset \mathcal{E}_{i+1}$,

$$L = \mathcal{A}_1 e_1 + \cdots + \mathcal{A}_n e_n$$

$$M = \mathcal{A}_1 \mathcal{E}_1 e_1 + \cdots + \mathcal{A}_n \mathcal{E}_n e_n .$$

The family of ideals $\{\mathcal{E}_1, \cdots, \mathcal{E}_n\}$ is uniquely determined by L and M (cf. [1] Ch. III, § 22). We denote

$$e(L, M) = \{\mathcal{E}_1, \cdots, \mathcal{E}_n\}$$

and call each of $\mathcal{E}_i$'s an elementary divisor of M with respect to L.

We further define

$$d(L, M) = \prod_{i=1}^{n} \mathcal{E}_i .$$

$d(L, M)$ is the $\mathcal{O}_K$-ideal generated by $\det(g)$ where g runs over the elements of endomorphisms of V sending L into M.

Note that $d(L, M)=\mathcal{O}_K$ if $L \approx M$.

Also, we put

$$\begin{aligned} C(K/k) &= \{\det(g) \mid g \in \tilde{G}\} \\ &= \{a \in K \mid N(a) = a \cdot a^{\sigma} = 1\} \\ C_L(K/k) &= \{\det(g) \mid g \in \tilde{G}_L\}\,, \end{aligned}$$

where $\tilde{G}_L$ (resp. G_L) is the subgroup of $\tilde{G}$ (resp. G) consisting of the elements which stabilize L.

Denoting by U_K the group of units in $\mathcal{O}_K$, we have:

1.3. LEMMA. *Suppose k is totally real and K is totally imaginary. Then we have*

$$U_K \cap C(K/k) = U_K^1 = \text{ the set of roots of unity in } K.$$

PROOF. Firstly, we shall see that given any isomorphism τ of K onto one of its conjugates, τ commutes with the complex conjugation σ. We may write $K=k(\sqrt{d})$, $d \in k \subset \boldsymbol{R}$, $d<0$. Given an element $\alpha=a+b\sqrt{d}$, $(a, b \in k)$, in K, we have $\alpha^{\tau}=a^{\tau}+b^{\tau}(\sqrt{d})^{\tau}$, $a^{\tau}, b^{\tau}, d^{\tau} \in \boldsymbol{R}$, $(\sqrt{d})^{\tau}=\varepsilon\sqrt{d^{\tau}}$, $\varepsilon=\pm 1$, and $\alpha^{\sigma}=a-b\sqrt{d}$. From this we get at once $\alpha^{\tau\sigma}=\alpha^{\sigma\tau}$.

Now suppose α belongs to $C(K/k)$. Then we have, for any τ,

$$|\alpha^{\tau}|^2 = \alpha^{\tau} \cdot (\alpha^{\tau})^{\sigma} = (\alpha \cdot \alpha^{\sigma})^{\tau} = 1\,.$$

Hence, if α is also an integer (in particular if $\alpha \in U_K$), then

$$\alpha \in U_K^1\,.$$

This completes the proof.

1.4. LEMMA. *Situation being the same as in the previous Lemma, the index $[U_K \cap C(K/k) : C_L(K/k)]$ divides the greatest common divisor* (dim V, $|U_K^1|$).

PROOF. Firstly, let us note that in general $C_L(K/k)$ is contained in $U_K \cap C(K/k)$. To see this, it is enough to show that

$$C_L(K/k) \subset U_K\,.$$

Let $g \in \tilde{G}_L$. Then $d(gL, L)=(\det g)=d(L, L)=\mathcal{O}_K$. Thus $\det g \in U_K$ as desired. Now, in virtue of the Lemma 1.3, it is enough to show that

$$(U_K^1)^n \subset C_L(K/k)\,, \qquad \text{where} \quad n=\dim V\,.$$

This is again obvious because if u is an element of U_K^1, then the linear transformation $u \cdot 1$ clearly belongs to $\tilde{G}_L$. This completes the proof.

Generally, we put

$$d_L = [U_K \cap C(K/k) : C_L(K/k)]\,.$$

Thus $d_L=1$ if, in the above,

$$(\dim V,\ |U_K^1|)=1\,.$$

1.5. PROPOSITION. *Suppose d_L is finite. Then among the lattices M such that $(L)_G=(M)_G$, $L\sim M$, there are at most d_L G-classes.*

PROOF. $(L)_G=(M)_G$ implies that $d(L, M)=\mathcal{O}_K$. And now we have $g\in\tilde{G}$ such that $M=gL$, therefore, $\mathcal{O}_K=(\det g)$. Hence

$$\det g\in U_K\cap C(K/k)\,.$$

Now suppose we have another such lattice M' and $M'=g'L$. If there exists an element $s\in\tilde{G}_L$ such that $\det g=\det g'\cdot\det s$, then

$$M'=g'\cdot s\cdot g^{-1}\cdot M\,,\qquad g'\cdot s\cdot g^{-1}\in G\,,$$

thus

$$M'\approx M\,.$$

This proves the proposition.

1.6. Suppose that

$$L=\mathcal{A}v\perp L'\quad\text{(orthogonal sum)}\,,$$

where $\mathcal{A}$ is an $\mathcal{O}_K$-ideal, v is an element of V, and L' is a sub-lattice of L. Then it is clear that we have

$$C_L(K/k)=U_K\cap C(K/k)\,.$$

1.7. Now, we decompose $(L)_{\tilde{G}}$ using an equivalence relation $\equiv$ defined by: For $M, M'\in(L)_{\tilde{G}}$, we put $M\equiv M'$ if and only if there exists an element g in $\tilde{G}$ such that

$$(gM)_G=(M')_G\,.$$

It was proved by G. Shimura [7] that, $(L)_{\tilde{G}}$ is decomposed into $s(L)$ $\equiv$-classes, where

$$s(L)=[C:C']\quad\text{or}\quad[C:C']\cdot[\tilde{C}(L):\tilde{U}(L)]$$

according as $\dim V$ is odd or even, where C is the group of ideal classes in K; C' is the subgroup of C consisting of the classes containing σ-invariant ideals; and

$$\tilde{C}(L)=\prod_{\mathfrak{q}}C(K_{\mathfrak{q}}/k_{\mathfrak{q}})/C_{L\mathfrak{q}}(K_{\mathfrak{q}}/k_{\mathfrak{q}})\,,$$

$\mathfrak{q}$ running over the ramifying ideals in k, $K_{\mathfrak{q}}=K\otimes k_{\mathfrak{q}}$; and

$$\tilde{U}(L)=\{(a_{\mathfrak{q}})\in\tilde{C}(L)\,|\,a_{\mathfrak{q}}=u\cdot C_{L\mathfrak{q}}(K_{\mathfrak{q}}/k_{\mathfrak{q}})\ \text{for}\ u\in U_K,\ N(u)=1\}$$

(cf. [7], 5.27, 5.28; Here we do not have to assume that (V, H) is indefinite.)

Nextly, we put

$$\tilde{c}(L, V)=\text{the number of }\tilde{G}\text{-classes among }\{M\in(L)_{\tilde{G}}\,|\,M\equiv L\}\,.$$

If L_j's form a system of representatives of $\equiv$-classes, we have:

$$c(L,\ V)=\sum_{j=1}^{s(L)}\tilde{c}(L_j,\ V)\,.$$

Hence, by Proposition 1.5, 1.4, we obtain the following:

1.8. Proposition.

(1) *We have, in general,*

$$c(L,\ V)\leqq\sum_{j=1}^{s(L)}c^1(L_j,\ V)\,.$$

(2) *If we have* $C_M(K/k)=U_K\cap C(K/k)$ *for all* $M\in(L)_{\tilde{G}}$*, then,*

$$c(L,\ V)=\sum_{j=1}^{s(L)}c^1(L_j,\ V)\,.$$

(3) *If* K *is totally imaginary and* k *is totally real, then we have*

$$(\dim V,\ |U_K^1|)c(L,\ V)\geqq\sum_{j=1}^{s(L)}c^1(L_j,\ V)\,.$$

§ 2. Class numbers of modular normal lattices.

2.1. Let us recall some definitions. We denote by

$$\mu(L)=\text{the } \mathcal{O}_K\text{-ideal generated by } H(x)=H(x,x),\ x\in L\,,$$

$$\mu_0(L)=\text{the } \mathcal{O}_K\text{-ideal generated by } H(x,y),\ x,y\in L\,.$$

L is said to be *normal* if and only if $\mu(L)=\mu_0(L)$.

We put

$$L^{\#}=\{x\in V\,|\,H(L,x)\subset\mathcal{O}_K\}\,.$$

L is said to be ($\mu_0(L)$—) modular if and only if $L=\mu_0(L)L^{\#}$. (cf. [**6**].)

The following proposition is known [**2**].

2.2. Proposition. *Given modular lattices* L *and* M*. Then* $(L)_{\tilde{G}}=(M)_{\tilde{G}}$ *if and only if* $\mu_0(L)=\mu_0(M)$, $\mu(L)=\mu(M)$.

2.3. Proposition. *Suppose* $\dim V\geqq 3$, $C=C'$, *and* L *is normal. Let* $M\in(L)_{\tilde{G}}$, *and* $\mathfrak{p}$ *be any prime ideal in* k*. Let* $\tilde{\mathfrak{p}}=\mathfrak{p}\mathcal{O}_K$*. Then there exists an element* g *in* $\tilde{G}$ *such that all the elementary divisors of* M *with respect to* gL *are* $\tilde{\mathfrak{p}}$*-powers.*

Proof. It is known that if L is normal then $\tilde{C}(L)=\tilde{U}(L)$ (cf. [**2**]). Hence, in the above, we have $s(L)=1$. Therefore, in view of 1.7, there exists an element g in $\tilde{G}$ such that $(gL)_G=(M)_G$.

Also by the assumption, $V_{\mathfrak{p}}$ is indefinite. Hence, by the Strong Approximation Theorem for G [**5**], we get the above result.

2.4. From now on we assume that

$$h(K)=\text{the class number of } K=1\,.$$

Any lattice L has a base as $\mathcal{O}_K$-module; say $\{v_1, \cdots, v_n\}$. We define

$$d(L) = \det(H(v_i, v_j))\mathrm{N}U_K .$$

We see at once that

$$d(M) = \mathrm{N}(d(L, M)) \cdot d(L) .$$

From this we get easily the following lemma:

2.5. LEMMA. *Suppose we have*

$$L \supset M, \qquad d(L) = d(M) .$$

Then we have

$$L = M .$$

2.6. LEMMA. *Suppose we have*

$$(L)_{\widetilde{G}} = (M)_{\widetilde{G}} .$$

Then we have

$$d(L) = d(M) .$$

PROOF. We have

$$d(M) = \mathrm{N}(d(L, M)) \cdot d(L) .$$

Let us put

$$\mathrm{N}(d(L, M)) = (a) .$$

By the assumption we have

$$a \in \mathrm{N}U_{\mathfrak{p}} \qquad \text{for all the prime ideal } \mathfrak{p} \text{ in } k .$$

Hence we have

$$a \in U_k \cap \mathrm{N}K .$$

Therefore, our assertion is reduced to the following lemma.

2.7. LEMMA. *If $h(K) = 1$, then we have*

$$U_k \cap \mathrm{N}K = \mathrm{N}U_K .$$

PROOF. It is enough to show that if $N(a) = \mathcal{O}_k$ then $\mathrm{N}a \in \mathrm{N}U_K$. But $\mathrm{N}(a) = \mathcal{O}_k$ implies that

$$(a) = \mathcal{A}_1^{1-\sigma} \qquad \text{for an ideal } \mathcal{A}_1 \text{ in } K .$$

Now we have $\mathcal{A}_1 = (a_1)$ so that

$$a = a_1^{1-\sigma} \cdot u ,$$

for an element u in U_K. Therefore,

$$\mathrm{N}a = \mathrm{N}u .$$

This completes the proof.

2.8. Now we are going to introduce 'Kneser's method'. For that purpose we need the following conditions besides $h(K) = 1$:

1) $\dim V \geqq 3$,

2) L is modular and normal,

3) There exists a prime ideal $\mathfrak{P}_0$ in K such that $\mathfrak{P}_0^\sigma = \mathfrak{P}_0$, $\mathrm{N}_{K/Q}(\mathfrak{P}_0) = (2)$. We put $N(\mathfrak{P}_0) = \mathfrak{p}_0$. $\mathfrak{p}_0$ is a prime ideal in k.

2.9. Let M be a lattice belonging to $(L)_{\tilde{G}}$ $(M \neq L)$. Our purpose is to find out a way to see if $L \sim M$. We are going to build a 'chain' connecting L and M. In view of Proposition 2.3, we may assume that all the elementary divisors of M with respect to L are $\mathfrak{P}_0$-powers. In view of Lemmas 2.5, 2.6, we may assume that there exists an element x_0 contained in $L^c \cap M \cap \mathfrak{P}_0^{-1} L$, where L^c is the set-theoretical complement of L in V. Let us put

$$\hat{L} = \{ y \in L \mid H(x_0, y) \in \mu_0(L) \} ,$$

$$L' = \mathcal{O}_K x_0 + \hat{L} .$$

L' is the first 'link' in our chain.

2.10. PROPOSITION. *Situations being same as in* 2.9, *we have*

$$d(L) = d(L') ,$$

$$[L' : L' \cap M] = \frac{1}{2} [L : L \cap M] .$$

PROOF. We give a proof although the argument runs parallel to that of M. Kneser in [4].

By the assumption in 2.8, we have:

$$\text{Suppose } (a) = (b) = \mathfrak{P}_0^{-1}, \text{ then } a + b \in \mathcal{O}_K .$$

Hence, if $x, x' \in L \cap \hat{L}^c$ then we have $x + x' \in \hat{L}$.

Also we have

$$L \supset \hat{L} \supset \mathfrak{P}_0 L .$$

Therefore there exists a base $\{v_1, \cdots, v_n\}$ of L such that

$$\hat{L} = \mathcal{O}_K v_1 + \cdots + \mathcal{O}_K v_i + \mathfrak{P}_0 v_{i+1} + \cdots + \mathfrak{P}_0 v_n .$$

So, by what was said above, we get:

$$d(L, \hat{L}) \supset \mathfrak{P}_0 .$$

Hence

$$[L : \hat{L}] \leqq 2 .$$

Using the assumption that L is modular, we get:

$$[L : \hat{L}] = 2 , \qquad d(L, \hat{L}) = \mathfrak{P}_0 .$$

Similarly we get

$$d(L', \hat{L}) = \mathfrak{P}_0 .$$

($\mathfrak{P}_0 x_0 \in \hat{L}$ because $M \in (L)_{\tilde{G}}$, $\mu_0(M) = \mu_0(L)$. So, we can use a similar argument as above.)

Hence

$$d(L', L) = \mathcal{O}_K\,,$$

and so,

$$d(L) = d(L')\,.$$

Also, by definition,

$$L \cap M = \hat{L} \cap M\,,$$

this implies that

$$\begin{aligned}[L' : L' \cap M] &= [\hat{L} : \hat{L} \cap M] \\ &= [\hat{L} : L \cap M] \\ &= \frac{1}{2}[L : L \cap M]\,.\end{aligned}$$

This completes the proof.

2.11. If L' is again modular and $\mu_0(L') = \mu_0(L)$, then we can continue the above process and build the next link. Especially, if L is unimodular (i. e. $\mathcal{O}_K$-modular), then we have $d(L) = d(L') = \mathrm{N}U_K$. And as $\mu_0(L') \subset \mathcal{O}_K$, it turns out that L' is also unimodular (cf. 4.2 in [2]). In this case, if we can show somehow that $L \sim L'$, $L' \sim L''$ (= the second link) etc., then it follows that $L \sim M$.

2.12. The following facts will be used later to simplify the process of building the chain:

1) If there exists an element x in L such that $H(x_0, x) \in \mu_0(L)$, then we may replace x_0 by $x_0 - x$.

2) If $g \in \tilde{G}_L$, then we may replace x_0 by gx_0.

3) Suppose we have $\mathfrak{P}_0 = (\alpha_0)$, $\mathrm{N}(1 - \alpha_0) = 1$.

If there exists an element t in V such that $t \equiv x_0 \bmod L$, and $\alpha_0 H(x_0, t) \equiv 1 \bmod \mathfrak{P}_0$, $H(t) = 1$, then we have $L \sim L'$.

Proof for 3): Let $s_{\alpha_0, t}$ be an element of $GL(V)$ defined by

$$s_{\alpha_0, t}(z) = z - \alpha_0 \frac{H(z, t)}{H(t)} t\,.$$

Then $s_{\alpha_0, t}$ belongs to $\tilde{G}$, and we have

$$s_{\alpha_0^\sigma, t} \cdot s_{\alpha_0, t} = 1\,.$$

And we have

$$s_{\alpha_0, t}(L') = L\,.$$

This completes the proof.

Also, let us note that to construct L', we do not have to use the existence of M. We just have to pick up an element $x_0 \in \mathfrak{P}_0^{-1} L \cap L^c$ such that $H(x_0) \in \mathcal{O}_K$ and put $L' = \mathcal{O}_K x_0 + \hat{L}$, as in 2.9.

§ 3. Calculation of c_n $(n \leqq 7)$.

3.1. In this section we put

$$k=\boldsymbol{Q}, \quad K=\boldsymbol{Q}(\sqrt{-1}), \quad \mathfrak{P}_0=(1-\sqrt{-1}),$$
$$V=V_n=\{v_1, \cdots, v_n\}_K,$$
$$H(v_i, v_j)=\delta_{ij}, \quad L=L_n=\sum_{i=1}^{n} \mathcal{O}_K v_i.$$

L is unimodular and normal. Also in view of 1.5, 1.8, we have

$$c(L, V_n)=c^1(L, V_n),$$

if $\dim V$ is odd; and in general, $c(L, V_n) \leqq c^1(L, V_n) \leqq (n, 4)c(L, V_n)$. We denote

$$c(L, V_n)=c_n$$
$$c^1(L, V_n)=c_n^1.$$

3.2. It is known that $(M)_{\tilde{G}}=(L)_{\tilde{G}}$ if and only if M is unimodular and normal (cf. [2]).

Also, generally, if the Hermitian vector space V is definite, then any lattice M can be decomposed uniquely into orthogonal sum of indecomposable sublattices [3]. Hence, if $c_n=1$ then $c_m=1$ for $m<n$. (Because if M is of rank m, unimodular, normal, then we have

$$M \perp L_{n-m} \sim L_n.)$$

3.3. Now we are going to apply Kneser's method to determine c_n's for $n \leqq 7$. Firstly let us note that the residue class of $\mathfrak{P}_0^2=(2)$ is represented by $\{0, 1, 1-\sqrt{-1}, \sqrt{-1}\}$.

Using 2.12 1), we may assume that

$$x_0=\frac{1}{1-\sqrt{-1}} \sum_{j=1}^{s} \eta_j v_j, \quad \eta_j=1 \text{ or } \sqrt{-1}.$$

By 2.12 2), we may further put

$$x_0=\frac{1}{1-\sqrt{-1}} \sum_{i=1}^{s} v_i.$$

As $H(x_0) \in \mathcal{O}_K$, we have $s \equiv 0 \bmod 2$.

We look at several possible cases:

1) $s=2$:—

In this case, we have $L' \sim L$.

PROOF. Put

$$e_1=x_0$$
$$e_2=\frac{1}{1-\sqrt{-1}}(v_1-v_2)=x_0-(1+\sqrt{-1})v_2$$

and

$$e_i = v_i \quad \text{for} \quad i \geqq 3\,.$$

e_i's are all elements of L'. We have $H(e_i, e_j) = \delta_{ij}$. Hence by Lemma 2.5, we have $\sum_{i=1}^{n} \mathcal{O}_K e_i = L'$, i.e. $L' \sim L$.

This implies that $c_3 = 1$, and therefore $c_1 = c_2 = 1$.

2) $s = n = 4 \cdot s_1$:—

This time L' is not normal and does not belong to the same genus as L.

PROOF. Let $z = ax_0 + y \in L'$, $y \in \hat{L}$. Then

$$y = \sum a_i v_i \quad \text{such that} \quad \sum a_i \in \mathfrak{P}_0\,.$$

And we have

$$\begin{aligned} H(z) &\equiv H(ax_0) + H(y) \mod 2 \\ &\equiv H(ax_0) + \mathrm{N}(\sum a_i) \mod 2 \\ &\equiv 0 \mod 2\,. \end{aligned}$$

As we have

$$\mu(L') \subset \mu_0(L') \subset \frac{1}{2}\mu(L')\,,$$

so we have

$$\mu(L') = (2)\,.$$

This completes the proof.

3) $s = n = 2 \cdot s_1$, s_1 is odd, $s_1 \geqq 3$:—

In this case we have $(L')_{\tilde{G}} = (L)_{\tilde{G}}$ and $L' \not\sim L$. Hence $c_n > 1$.

PROOF. $H(x_0) = s_1$, but as $v_1 + v_2$ belongs to L' $(H(v_1 + v_2) = 2)$, we have $\mu(L') = \mathcal{O}_K$. So in view of Proposition 2.2, we have $(L')_{\tilde{G}} = (L)_{\tilde{G}}$. Now let $z = ax_0 + y$ be an element of L', where

$$y = \sum a_i v_i\,, \qquad \sum a_i \in \mathfrak{P}_0\,.$$

It follows that

$$\begin{aligned} H(z) &= \sum \mathrm{N}\Big(\frac{a}{1-\sqrt{-1}} + a_i\Big) \\ &= \frac{1}{2} \sum \mathrm{N}(a + a_i(1-\sqrt{-1}))\,. \end{aligned} \tag{i}$$

Here, if $a + a_i(1-\sqrt{-1}) = 0$ for any i, then $z \in L$; and so $z \in \hat{L}$ which implies that $H(z) \equiv 0 \mod 2$.

If on the other hand $a + a_i(1-\sqrt{-1}) \neq 0$ for all i, then they are positive integers and so in (i), we have $H(z) > 1$.

Thus $H(z)$ is never equal to 1.

This proves that $L' \not\sim L$.

In particular, $c_n > 1$, if $n \geqq 6$.

3.4. Proceeding to the next step, we will construct our second link L''

starting from L'. Now we have

$$L_n'' = L'' = \mathcal{O}_K y_0 + \hat{L}' ,$$

where

$$y_0 \in \mathfrak{P}_0^{-1} L' \cap M \cap L'^c ,$$
$$\hat{L}' = \{ z \in L' \mid H(y_0, z) \in \mathcal{O}_K \} .$$

We have the following possibilities:

a) $y_0 \in \mathfrak{P}_0^{-1}L$.

In this case we may assume that $n = s$. And we have two possible cases:

1) $y_0 = \dfrac{1}{1-\sqrt{-1}} \sum_1^m v_i$, $m \equiv 0 \bmod 2$, $m \leqq n/2$, and $L_n'' \sim L_m' \perp L_{n-m}'$.

2) $y_0 = \dfrac{1}{1-\sqrt{-1}} \sum_1^m v_i + v_{m+1}$, $m \equiv 0 \bmod 2$, $m \geqq n/2$.

b) $y_0 \notin \mathfrak{P}_0^{-1}L$. Then

$$y_0 = \frac{1}{2}\Big(\sum_1^{s-1} v_i + \tau v_s \Big) + \frac{1}{1-\sqrt{-1}} \sum_{s+1}^m v_j \ (+v_{m+1}) ,$$

where $\tau = 1, 3, 1-2\sqrt{-1}, -(1+2\sqrt{-1})$. And if in this case $n = s$, then $n \equiv 0$ (4).

PROOF. If $y_0 = v_1$, then $L'' = L$. Because, if $z \in \hat{L}'$, $z = ax_0 + y$, $y \in \hat{L}$, then $H(v_1, ax_0) = a/(1-\sqrt{-1}) \in \mathcal{O}_K$. Hence $z \in L$, and $L'' \subset L$. So, in view of Lemma 2.5, we have $L'' = L$.

Now we have $L' \ni v_1 - v_i$, therefore by 2.12. 1), we may replace y_0 by v_1 if $y_0 \in L$. Hence we may assume that $y_0 \notin L$.

Suppose that $y_0 \in \mathfrak{P}_0^{-1}L$.

To show that we get 1) or 2) in this case, we can use an argument which is almost identical with the one used by M. Kneser in [4]. For the sake of completeness, however, we sketch an outline of the argument.

Using 2.12, we have

$$y_0 = \frac{1}{1-\sqrt{-1}} \sum_1^m \eta_i v_i \ (+v_{m+1}) \quad \text{or} \quad \frac{1}{1-\sqrt{-1}} \sum_1^n \eta_i v_i ,$$

where $\eta_i = 1$ or $\sqrt{-1}$.

We can interchange 1 and $\sqrt{-1}$ at even number of places. Thus

$$y_0 = \frac{1}{1-\sqrt{-1}} \sum_1^m v_i \ (+v_{m+1}) \quad \text{or} \quad \frac{1}{1-\sqrt{-1}} \Big(\sum_1^{n-1} v_i + \eta_n v_n \Big) .$$

From this, in view of 2.12. 1), we may assume that $n = s$ in this case.

The latter case may be eliminated because if $\eta_n = 1$, then $y_0 \in L'$ contradicting the assumption that $y_0 \notin L'$, while if $\eta_n = \sqrt{-1}$, then putting $t = v_n$, and using 2.12 3), we get $L' \sim L''$.

m is even because $H(y_0) \in \mathcal{O}_K$.

In case

$$y_0=\frac{1}{1-\sqrt{-1}}\sum_1^m v_i\,, \quad \text{we have} \quad \frac{1}{1-\sqrt{-1}}\sum_1^n v_i\in \hat{L}'\,.$$

Subtracting the latter from y_0 if necessary, we get 1).

On the other hand if

$$y_0=\frac{1}{1-\sqrt{-1}}\sum_1^m v_i+v_{m+1}\,, \qquad m<n/2\,,$$

then we have

$$\frac{1}{1-\sqrt{-1}}\sum_1^m v_i-v_m+v_{m+1}-(1+\sqrt{-1})^{-1}\sum_{m+1}^n v_i\in \hat{L}'\,.$$

Subtracting this from y_0 and changing the order of the base, we get 2). Nextly, let $y_0=\frac{1}{2}\sum_1^s a_iv_i+y_1$ ($\notin \mathfrak{P}_0^{-1}L$), where y_1 is a linear combination of v_j's for $j=s+1, \cdots, n$. Then $\mathfrak{P}_0 y_0 \subset L'$. Therefore none of a_i $(i=1, \cdots, s)$ is divisible by $\mathfrak{P}_0$. Also we have

$$(1-\sqrt{-1})y_0 \quad \text{and} \quad \frac{1}{1-\sqrt{-1}}\sum_1^s v_i\in L'\,.$$

Therefore $\sum_1^s a_i\in(2)$. So, $a_i\equiv 1$ or $\sqrt{-1}$ mod 2.

Subtracting vectors of the form av_i+bv_s, where a and b are suitable integers, we can put

$$y_0=\frac{1}{2}\Big(\sum_1^{s-1} c_iv_i+\tau v_s\Big)+y_1$$

where c_i is 1 or $\sqrt{-1}$.

Interchanging $\sqrt{-1}$ and 1 at even number of places, we may further assume:

$$y_0=\frac{1}{2}\Big(\sum_1^{s-1} v_i+\tau v_s\Big)+y_1\,.$$

We have

$$s-1+\tau=0 \bmod 2\,,$$

$$s\equiv 0 \bmod 2\,.$$

Hence,

$$\tau\equiv 1 \bmod 2\,.$$

Hence,

$$\tau=(1-\sqrt{-1})^2\tau_1+1\,, \qquad \tau_1\in\{0,\ 1,\ 1-\sqrt{-1},\ \sqrt{-1}\}\,.$$

If $y_1\in L_{n-s}$, then $L''=L''_s\perp L_{n-s}$.

Generally, we have $y_1=\frac{1}{1-\sqrt{-1}}\sum_{s+1}^m \eta_jv_j$. By the argument as above, we may put

$$y_1 = \frac{1}{1-\sqrt{-1}} \sum_{s+1}^{m} v_j \ (+v_{m+1}) .$$

Now if $n = s$, then we have

$$H(y_0) = \frac{1}{4}(n-1+\mathrm{N}\tau) .$$

But

$$\mathrm{N}\tau \equiv 1 \bmod 4 .$$

Therefore

$$n \equiv 0 \bmod 4 .$$

This completes the proof.

3.5. In case $y_0 = \frac{1}{1-\sqrt{-1}} \sum_{1}^{m} v_i + v_{m+1}$, $m \equiv 0 \bmod 2$, and $n = m+2$ we have $L'' \sim L'$.

PROOF. Put

$$t = \frac{1}{1-\sqrt{-1}} (-\sqrt{-1} \cdot v_{n-1} - v_n) .$$

Then

$$y_0 - t = \frac{1}{1-\sqrt{-1}} \sum_{1}^{n-2} v_i + v_{n-1} - t$$
$$= \frac{1}{1-\sqrt{-1}} \sum_{1}^{n} v_i = x_0 ,$$
$$H(t) = 1 ,$$
$$(1-\sqrt{-1})H(y_0, t) = -\sqrt{-1} \equiv 1 \bmod \mathfrak{P}_0 .$$

Therefore, using 2.12 3), we are done.

3.6. Suppose $n = 4$, $y_0 = \frac{1}{2}\left(\sum_{1}^{3} v_i + \tau v_4\right)$. In this case, we have the following possibilities:

1) If $\tau = 1$ or 3, then $L'' \sim L$,

2) If $\tau = 1-2\sqrt{-1}$ or $-(1+2\sqrt{-1})$, then $L'' \sim L'$, and $\mu(L'') = (2)$.

PROOF. 1)—i) :—Case $\tau = 1$. Put

$$t = \frac{1}{2} \sum_{1}^{4} v_i .$$

Then

$$H(t) = 1 , \qquad 2H(y_0, t) = 1 .$$

Hence, if we put

$$S_t(z) = z - 2\frac{H(z, t)}{H(t)} t ,$$

for any element z in V, then

$$S_t \in G$$

and

$$S_t(y_0)=v_4\,.$$

If we have

$$z=\sum a_i v_i \in L''\,,$$

then

$$\sum a_i \equiv 0 \bmod 2\,.$$

Therefore,

$$2H(z,\,t)\equiv 0 \bmod 2\,,$$

$$S_t(z)\in L\,,\quad \text{i.e.}\quad S_t(L'')\subset L\,.$$

Hence, by Lemma 2.5, we have $S_t(L'')=L$.

1)—ii):—Case $\tau=3$.

In this case we set

$$e_1=y_0-v_1-v_4\,,\qquad e_2=y_0-v_2-v_4\,,$$
$$e_3=y_0-v_3-v_4\,,\qquad e_4=-y_0+(1-\sqrt{-1})x_0\,.$$

Then all the e_i's belong to L'' and moreover we have

$$(H(e_i,\,e_j))=1_4\,.$$

Hence, by Lemma 2.5, we have $L''\sim L$.

2):—

If $\tau=1-2\sqrt{-1}$, put

$$e_1=\sqrt{-1}(v_2+v_3)\,,\quad e_2=v_1+v_2\,,\quad e_3=v_1+v_3\,,\quad e_4=y_0\,.$$

Then all the e_i's belong to L''.

If $\tau=-(1+2\sqrt{-1})$, put

$$f_i=e_i\quad (i=1,2,3)\,,\qquad f_4=\sqrt{-1}\,y_0\,.$$

We have

$$f_i\in L''\qquad \text{for all}\quad i\,.$$

Also we put

$$g_1=(1-\sqrt{-1})^{-1}\cdot(v_1+v_2+\sqrt{-1}\,v_3-\sqrt{-1}\,v_4)\,,$$
$$g_2=(1-\sqrt{-1})^{-1}\cdot(-v_1-\sqrt{-1}\,v_2-\sqrt{-1}\,v_3+v_4)\,,$$
$$g_3=2(1-\sqrt{-1})^{-1}\cdot v_4=(1+\sqrt{-1})v_4\,,$$
$$g_4=(1-\sqrt{-1})^{-1}\sum_1^4 v_i\,.$$

Then all the g_i's belong to L' and we have

$$(H(e_i,\,e_j))=(H(f_i,\,f_j))=(H(g_i,\,g_j))$$

$$=\begin{pmatrix} 2 & -i & -i & 1 \\ i & 2 & 1 & i \\ i & 1 & 2 & 1 \\ 1 & -i & 1 & 2 \end{pmatrix} \qquad (i=\sqrt{-1}).$$

$$\det(H(e_i, e_j))=1.$$

This implies that $\{e_i\}$, $\{f_i\}$, $\{g_i\}$ are all bases of the corresponding lattices. And it is clear from the form of the above matrix that $\mu(L'')=(2)$.

3.7. Summarizing the above, we get $c_4=1$. (Because L_4' is not normal.) For $n=5$, the above process yields two classes of unimodular and normal lattices: L_5 and $L_4'\perp L_1$. Namely $c_5=2$. For $n=6$, we saw in 3.3 that L_6' is unimodular normal but $L_6\not\sim L_6'$. The second step (3.4) yields:

1) $$y_0=(1-\sqrt{-1})^{-1}(v_1+v_2), \qquad L_6''\sim L_2'\perp L_4'\sim L_2\perp L_4'\not\sim L_6.$$

This L_6'' is again unimodular and normal, which has element x such that $H(x)=1$. Hence $L_6''\not\sim L_6'$.

2) $$y_0=(1-\sqrt{-1})^{-1}\sum_1^4 v_i+v_5, \qquad L_6''\sim L_6' \text{ (cf. 3.5)}.$$

Hence in this case we have $c_6=3$.

From the above we can conclude that $c_6^1=3$ or 4.

To see this let us decompose $(L_6)_{\tilde{G}}$ into three $\tilde{G}$-classes C_1, C_2, C_3 represented by L_6, L_6', L_6'' respectively. We have $C_i\cap(L_6)_G\neq\emptyset$ for $i=1, 2, 3$ (cf. 1.7, 1.8, and note that $s(L_6)=1$ now). In view of 1.6, it is clear that $C_i\cap(L_6)_G$ consists of only one G-class for $i=1, 3$. The number of G-class in $C_2\cap(L_6)_G$ is one or 2 ($2=(6, 4)=(\dim V_6, |U_K^1|)$. cf. 1.5). Thus $c_6^1=3$ or 4. Also, from the above, it is clear that if $c_n=1$ then $c_n^1=1$.

Likewise for $n=7$, we get besides three classes among unimodular and normal lattices:

$$L_7, \quad L_1\perp L_6', \quad L_1\perp L_2\perp L_4', \quad L_3\perp L_4',$$

the lattice L_7'' which corresponds to the case:

$$y_0=\frac{1}{2}\sum_1^6 v_i+\frac{1}{1-\sqrt{-1}}v_7.$$

We can show that if $x\in L_7''$, then $H(x)>1$. Hence $c_7=4$. In fact, let $x=\alpha y_0+z$, $z\in\hat{L}'$. If $\alpha=0$, then in view of 3.3, we have $H(x)>1$. If $\alpha\neq0$, then writing $x_i=\sum_1^7 a_iv_i$, we see that none of a_i is 0. Furthermore, $\mathrm{N}a_i\geqq\frac{1}{2}$ for $i=1, \cdots, 6$. This implies that $H(x)>1$. This completes the proof.

Thus we get the following Theorem:

3.8. THEOREM. *Situations being as in* 3.1, *we have*

1) $c_n > 1$, $c_n^1 > 1$ *if* $n \geqq 5$; $c_n = c_n^1$ *if* n *is odd*, $c_n \leqq c_n^1 \leqq (n, 4)c_n$ *in general.*

2) $c_1 = c_2 = c_3 = c_4 = 1$, $c_5 = 2$, $c_6 = 3$, $c_7 = 4$; $c_1^1 = c_2^1 = c_3^1 = c_4^1 = 1$, $c_5^1 = 2$, $c_6^1 = 3$ or 4, $c_7^1 = 4$.

REMARKS (due to M. Kneser).

1. $c_i = 1$ for $i = 1, \cdots, 4$ follows at once from Satz 1 of [4]. Because the lattice L_n can be identified with the lattice of rank $2n$ (with discriminant 1) in the quadratic vector space of $\dim 2n$ (with the form given by 1_{2n}). Then the above mentioned Satz implies that there exists an element x in L_n $(n \leqq 4)$ such that $H(x) = 1$. This obviously leads to the desired result.

2. The lattices obtained above correspond to the ones in the respective quadratic spaces as follows: $L_4' = K_8$, $L_6' = K_{12}$, $L_7'' = M_{14}$ (cf. [4] Satz 1).

International Christian University

References

[1] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience Publ., New York, London, 1962.

[2] K. Iyanaga, Arithmetic of special unitary groups and their symplectic representations, J. Fac. Sci. Univ. Tokyo, **15** (1968), 35-69.

[3] M. Kneser, Zur Theorie der Kristallgitter, Math. Ann., **127** (1954), 105-106.

[4] M. Kneser, Klassenzahlen definiter quadratischer Formen, Arch. Math., **8** (1957), 241-250.

[5] M. Kneser, 'Strong approximation', in Proc. Sympos. Pure Math., Vol. 9, Amer. Math. Soc., Providence, R. I., 1966.

[6] O. T. O'Meara, Introduction to Quadratic Forms, Academic Press, New York, 1963.

[7] G. Shimura, Arithmetic of unitary groups, Ann. of Math., (2), **79** (1964), 369-409.