ACTA ARITHMETICA
XXIV (1973)

Integral representations over local fields and the number of genera of quadratic forms

by

O. Körner (Ulm)

Dedicated to C. L. Siegel on his 75th birthday

We consider quadratic forms $f = \sum a_{ik}x_ix_k$ $(a_{ik} = a_{ki})$ with coefficients a_{ik} in a quotient field F of a Dedekind domain $\mathfrak{o}$ of characteristic $\neq 2$. The *determinant* and the *rank* of f are defined to be the corresponding quantities of the matrix (a_{ik}). The greatest common divisor (interpreted as fractional $\mathfrak{o}$-ideal of F) of all a_{ik} is called the *scale* and the greatest common divisor of all a_{ii} and all $2a_{ik}$ the *norm* of f. A quadratic form g is said to be a *representation* of f, if g is obtained by making a linear substitution of any number of new variables with coefficients in $\mathfrak{o}$ for the variables of f. If f is also a representation of g, then f and g are called *equivalent*. The set of forms equivalent to f is named the *equivalence class of f over* $\mathfrak{o}$.

One of the problems of the arithmetic theory of quadratic forms is to determine for given $\mathfrak{o}$ and f all representations of f by means of class invariants. Especially the case where $\mathfrak{o}$ is the ring of integers of a local field F is of interest. There the representation problem has been solved [2], [5] except when 2 is ramified in F and f is not modular. In this paper a solution is presented which covers the exceptional case for forms f of rank 2 (see Theorems 1 and 2). The result contains a solution of the equivalence problem over $\mathfrak{o}$ for binary forms (see Theorem 3) which is convenient for applications. It is of another shape than the solution given by O'Meara [4].

Applications of Theorem 3 are made in the last part of this paper which is devoted to the connection between local and global invariants of quadratic forms. There $\mathfrak{o}$ is the ring of integers of an algebraic number field F. If d is a non-zero number in F and $\mathfrak{n}$ and $\mathfrak{s}$ are fractional ideals of F and $\mathfrak{o}_\mathfrak{p}$, $\mathfrak{n}_\mathfrak{p}$ and $\mathfrak{s}_\mathfrak{p}$ the $\mathfrak{p}$-adic closures of $\mathfrak{o}$, $\mathfrak{n}$ and $\mathfrak{s}$ in a $\mathfrak{p}$-adic completion of F, we denote by $h_\mathfrak{p}$ the number of classes over $\mathfrak{o}_\mathfrak{p}$ of all binary quadratic forms with determinant d, norm $\mathfrak{n}_\mathfrak{p}$ and scale $\mathfrak{s}_\mathfrak{p}$ and by H the number of genera of all binary quadratic forms with determinant d, norm $\mathfrak{n}$, scale $\mathfrak{s}$ and of fixed index of inertia in each real archimedean completion of F. If $H > 0$ and F is the field of rational numbers, Gauss' classical relation reads

$$H = k \prod_{\mathfrak{p}} h_{\mathfrak{p}}, \tag{1}$$

where $\mathfrak{p}$ runs over all maximal ideals of $\mathfrak{o}$ and $k = 1$ if $-d$ is a square in F, and $k = 1/2$ otherwise. It is remarkable that (1) is not true in this simple form for all algebraic number fields F. For instance, for some F it happens that $k = 1$ although $-d$ is not a square in F. This is shown by generalizing (1) to all algebraic number fields and quadratic forms of rank 2, including those with vanishing determinants (see Theorem 6). Thereby an explicit evaluation of the $h_{\mathfrak{p}}$ by means of Theorem 3 and an extension of a classical result ([6], Theorem 43) on the existence of forms for given local invariants (see Theorem 5) are employed.

We use the terminology of [3], Chapters VIII–X. Exceptions to it are stated explicitly. In particular, we formulate our results on quadratic forms in terms of lattices with respect to $\mathfrak{o}$ in quadratic spaces over F with a bilinear form B and its associated quadratic form Q. Let $\mathfrak{o}$, F and f be as at the beginning. It is easy to see that for any given f of any number n of variables there exists a regular lattice L (in some suitable quadratic space) which is *related to* f; this means there are vectors $l_1, \ldots, l_n$ in L such that $L = \mathfrak{o}l_1 + \ldots + \mathfrak{o}l_n$ and $B(l_i, l_k) = a_{ik}$ $(i, k = 1, \ldots, n)$. Obviously $\dim L = \operatorname{rank} f$. Thus the problem of representation and equivalence of quadratic forms is reduced to the question of representation and isometry of related lattices which may be assumed regular.

1. Representations over dyadic fields.

Since the representation problem is solved in non-dyadic local fields [2], it is supposed in this section that F is a dyadic local field, $\mathfrak{o}$ its ring of integers, $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$ and π a fixed prime element of $\mathfrak{o}$. Let here the other notation be also the one of [3], Chapter IX, in particular dL, $\mathfrak{v}L$, $\mathfrak{n}L$, $\mathfrak{s}L$, $L^{\#}$, $S_{\mathfrak{p}}(FL)$ are the discriminant, volume, norm, scale and dual of a lattice L and the Hasse symbol of the quadratic space FL respectively. We use the abbreviations $\operatorname{ord} = \operatorname{ord}_{\mathfrak{p}}$, $e = \operatorname{ord} 2$ and $(\alpha, \beta)_{\mathfrak{p}} = \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$. The following properties ([3], § 63A) of the quadratic defect $\mathfrak{d}(\alpha)$ for $\alpha \in F$ are frequently applied: (i) $\mathfrak{d}(\alpha) = \alpha\mathfrak{o}$ if $\operatorname{ord}\alpha$ is odd, (ii) $\mathfrak{d}(\alpha) = 0$ if $\mathfrak{d}(\alpha) \subset 4\alpha\mathfrak{o}$, (iii) $\mathfrak{d}(\alpha) \subset \alpha\mathfrak{o}$ and $\operatorname{ord}\mathfrak{d}(\alpha)$ is odd if $\operatorname{ord}\alpha$ is even and $\mathfrak{d}(\alpha) \supset 4\alpha\mathfrak{o}$.

THEOREM 1. *Let L be a 2-dimensional regular lattice, $\gamma \in \dot{F}$ and $\lambda \in Q(L)$ with $\lambda\mathfrak{o} = \mathfrak{n}L$. Put $u = \operatorname{ord}\mathfrak{n}L$, $v = \operatorname{ord}\mathfrak{d}(-dL)$, $w = \operatorname{ord} dL$ and $t = \operatorname{ord}\gamma$. Then $\gamma \in Q(L)$ if and only if the following three conditions hold:*

$$t \geqslant u, \tag{2}$$

$$(\gamma, -dL)_{\mathfrak{p}} = (\lambda, -dL)_{\mathfrak{p}}, \tag{3}$$

$$\operatorname{ord}\mathfrak{d}(\gamma\lambda) \geqslant \begin{cases} w & \textit{if } w \textit{ is odd}, \\ \min\big(v,\, e + (u+w+t)/2\big) & \textit{otherwise}. \end{cases} \tag{4}$$

Proof. By suitably scaling, we may assume that $\mathfrak{s}L = \mathfrak{o}$. Since for unimodular L the assertion is contained in Lemma 6.13 of [5], we may assume that L is not modular. Hence $u = 0$, hence $\langle\lambda\rangle$ splits L by [3], 82:15, and we obtain $L \cong \langle\lambda\rangle \perp \langle\mu\rangle$ for some μ in $\mathfrak{o}$ with $\lambda\mu \cong d = dL$. Therefore $\gamma \in Q(L)$ if and only if the equation

$$\gamma\lambda = x^2 + dy^2 \tag{5}$$

can be solved by some x, y in $\mathfrak{o}$.

a) We prove the necessity of (2)–(4). Since (3) means that $\gamma \in Q(FL)$, the conditions (2) and (3) are immediate. Also (4) is clear if w is odd. Now suppose w to be even. We have $v > w$ and

$$-d \equiv z^2 \operatorname{mod} \mathfrak{p}^v \text{ for some } z \text{ with } \operatorname{ord} z = w/2. \tag{6}$$

From (5) and (6) we obtain

$$\gamma\lambda \equiv (x+zy)(x-zy) = (x+zy)^2 - 2yz(x+zy) \operatorname{mod} \mathfrak{p}^v. \tag{7}$$

Replacing z eventually by $-z$, we obtain from the first relation in (7) that $\operatorname{ord}(x+zy) \geqslant \min(v/2, t/2)$, hence from (7), (6) and (ii) that

$$\operatorname{ord}\mathfrak{d}(\gamma\lambda) \geqslant \min\big(v,\, e + w/2 + \min(v/2, t/2)\big) \geqslant \min(v,\, e + w/2 + t/2),$$

which proves (4).

b) Now to the sufficiency. If $\mathfrak{d}(\gamma\lambda) = 0$, there is obviously a solution x, y in $\mathfrak{o}$ for (5). Therefore we assume $\mathfrak{d}(\gamma\lambda) \neq 0$.

b$_1$) Let w be odd. By (3) there exist x, y in F that satisfy (5). If t is odd, (5) implies $t = w + 2\operatorname{ord} y < 2\operatorname{ord} x$, hence $\operatorname{ord} x > 0$, $\operatorname{ord} y \geqslant 0$, since $t \geqslant w$ by (4). If t is even, (5) implies $t = 2\operatorname{ord} x < w + 2\operatorname{ord} y$, hence $\operatorname{ord} x \geqslant 0$, but also $\operatorname{ord} y \geqslant 0$, since otherwise it would follow from (5) that $\operatorname{ord}\mathfrak{d}(\gamma\lambda) = \operatorname{ord} dy^2 < w$, contradicting (4). Hence always $\gamma \in Q(L)$.

b$_2$) Let w be even. Then $v > w$. If $t \geqslant w$, introduce the variable $x_0 = \pi^{-w/2}x$ in (5). The resulting equation can be solved by some x_0, y in $\mathfrak{o}$ in virtue of Lemma 6.13 of [5]. Now let $t < w$. Then t is even, since otherwise (4) would imply $t = \operatorname{ord}\mathfrak{d}(\gamma\lambda) > w$. Now (ii) and (4) imply $2e + t \geqslant \operatorname{ord}\mathfrak{d}(\gamma\lambda) \geqslant w$. We can assume that $-d = \pi^w(1 + \pi^{v-w}\varepsilon)$ and $\gamma\lambda = \pi^t(1 + \pi^s\eta)$ with $s = -t + \operatorname{ord}\mathfrak{d}(\gamma\lambda)$ for some units ε, η of $\mathfrak{o}$, under the convention $\pi^\infty = 0$. In the new variable $x_1 = \pi^{-w/2}x - \pi^{(t-w)/2}$ the equation (5) reads

$$(1 + \pi^{v-w}\varepsilon)y^2 = x_1^2 + 2\pi^{-(w-t)/2}x_1 - \pi^{s-w+t}\eta. \tag{8}$$

It suffices to find a solution x_1, y in $\mathfrak{o}$ for (8). First, let $v \leqslant e + (w+t)/2$. In view of the connection between (5) and (8), there exists a solution

x_1, y in F for (8). Assume $\operatorname{ord} x_1 < 0$. Then $x_1 = z^{-1}$ for some z in $\dot F$ with $\operatorname{ord} z > 0$, and (8) implies

$$(9)\qquad (1+\pi^{v-w}\varepsilon)(yz)^2 = 1+2\pi^{-(w-t)/2}z-\pi^{s-w+t}\eta z^2.$$

We infer that $\operatorname{ord} yz = 0$, hence the quadratic defect of the left hand side of (9) is $\mathfrak{p}^{v-w}$, whereas the one of the right hand side is contained in $\mathfrak{p}^{e-(w-t)/2+1}+\mathfrak{p}^{s-w+t+2} \subset \mathfrak{p}^{v-w}$ by (4), which is impossible. Hence $\operatorname{ord} x_1 \geqslant 0$, and also $\operatorname{ord} y \geqslant 0$ by (8). This solves (8) in $\mathfrak{o}$. Secondly, let $v > e+(w+t)/2$. Then $s \geqslant e+(w-t)/2$ by (4). Put $x_1 = y$, $\alpha = 2^{-1}\pi^{v-(w+t)/2}\varepsilon$ and $\beta = 2^{-1}\pi^{s-(w-t)/2}\eta$. Then (8) is solved in $\mathfrak{o}$ if we can solve for arbitrary $k > 0$ the congruence $y-\alpha y^2 \equiv \beta \bmod \mathfrak{p}^k$ by some y in $\mathfrak{o}$; but this is easily done by induction on k, using only the facts $\operatorname{ord}\alpha > 0$ and $\operatorname{ord}\beta \geqslant 0$. This completes the proof.

Following Riehm [5], we define for non-zero fractional ideals $\mathfrak{a}$ of F and for regular lattices L the lattice $L_{\mathfrak{a}}$ as the lattice whose dual $L_{\mathfrak{a}}^{\#}$ is generated by all vectors $x \in L^{\#}$ with $Q(x) \in \mathfrak{a}$. It is evident that $L_{\mathfrak{a}}$ is a regular lattice with $FL_{\mathfrak{a}} = FL$, $L_{\mathfrak{a}}^{\#} \subseteq L^{\#}$ and $L \subseteq L_{\mathfrak{a}}$. If $\mathfrak{n}L^{\#} \subseteq \mathfrak{a}$, then $L_{\mathfrak{a}} = L$. Scaling L by any $a \in \dot F$ yields the formula $(L^a)_{\mathfrak{a}} = (L_{a\mathfrak{a}})^a$. In [5] it is shown that it is easy to compute $L_{\mathfrak{a}}$ for any given $\mathfrak{a}$ and L of dimension $\leqslant 2$, and that L is non-modular and $\mathfrak{n}L_{\mathfrak{a}}^{\#} \subseteq \mathfrak{a}$ if $L_{\mathfrak{a}}$ is 2-dimensional and non-modular.

Let the symbol $K \to L$ denote the representation of a lattice K by a lattice L. By the principle of duality one knows that the two statements

$$(10)\qquad K \to L \quad\text{and}\quad L^{\#} \to K^{\#}$$

are equivalent for any two regular lattices K and L of the same dimension. From (10) and the definition of $L_{\mathfrak{a}}$ one infers that the three statements

$$(11)\qquad K \to L, \quad L^{\#} \to K_{\mathfrak{a}}^{\#}, \quad K_{\mathfrak{a}} \to L$$

are pairwise equivalent for any two regular lattices K and L of the same dimension and any $\mathfrak{a}$ with $\mathfrak{n}L^{\#} \subseteq \mathfrak{a}$.

The following Theorem 2 reduces the problem of representation of 2-dimensional lattices by 2-dimensional ones to the question already answered in Theorem 1.

THEOREM 2. *Let M and N be 2-dimensional regular lattices and $\gamma \in Q(N^{\#})$ with $\gamma\mathfrak{o} = \mathfrak{n}N^{\#}$. Put $\mathfrak{m} = \mathfrak{n}N^{\#}$. Then $M \to N$ if and only if the following conditions hold:*

$$(12)\qquad FM \cong FN,$$

$$(13)\qquad \mathfrak{n}M_{\mathfrak{m}} \subseteq \mathfrak{n}N \quad\textit{and}\quad \mathfrak{v}M_{\mathfrak{m}} \subseteq \mathfrak{v}N,$$

$$(14)\qquad \gamma \in Q(M_{\mathfrak{m}}^{\#}).$$

Proof. In view of (11) the necessity of the conditions (12)–(14) is obvious. Now to their sufficiency! By scaling we may assume that $\mathfrak{s}N = \mathfrak{o}$. If $M_{\mathfrak{m}}$ is modular, we have $N^{\#} \to M_{\mathfrak{m}}^{\#}$ by Theorem 6.12 of [5], hence $M \to N$ by (11). Now let $M_{\mathfrak{m}}$ be non-modular. A Jordan splitting yields $M_{\mathfrak{m}}^{\#} \cong \langle\alpha\rangle \perp \langle\beta\rangle$ for some α, β in F with $\operatorname{ord}\mathfrak{m} \leqslant \operatorname{ord}\alpha < \operatorname{ord}\beta = -\operatorname{ord}\mathfrak{n}M_{\mathfrak{m}}$, since $\mathfrak{n}M_{\mathfrak{m}}^{\#} \subseteq \mathfrak{m}$ by the foregoing remarks. Furthermore N is also non-modular, since otherwise it would be unimodular, which would imply $\operatorname{ord}\mathfrak{m} = \operatorname{ord}\mathfrak{n}N \geqslant -\operatorname{ord}\mathfrak{n}N \geqslant -\operatorname{ord}\mathfrak{n}M_{\mathfrak{m}}$. Therefore $N^{\#}$ is non-modular, hence $\gamma\mathfrak{o} = \mathfrak{s}N^{\#}$, and $\langle\gamma\rangle$ splits $N^{\#}$ by [3], 82:15, which means $N^{\#} \cong \langle\gamma\rangle \perp \langle\delta\rangle$ for some δ in $\dot F$ with $\operatorname{ord}\gamma < \operatorname{ord}\delta$. By (14) we have $\mathfrak{n}N^{\#} \subseteq \mathfrak{n}M_{\mathfrak{m}}^{\#}$, hence $\operatorname{ord}\gamma = \operatorname{ord}\mathfrak{m} \geqslant \operatorname{ord}\mathfrak{n}M_{\mathfrak{m}}^{\#} = \operatorname{ord}\alpha \geqslant \operatorname{ord}\mathfrak{m}$, hence $\operatorname{ord}\gamma = \operatorname{ord}\alpha = \operatorname{ord}\mathfrak{n}M_{\mathfrak{m}}^{\#}$. From this, (14) and [3], 82:15 it follows that $\langle\gamma\rangle$ splits also $M_{\mathfrak{m}}^{\#}$, which means $M_{\mathfrak{m}}^{\#} \cong \langle\gamma\rangle \perp \langle\delta'\rangle$ for some δ' in $\dot F$. Taking discriminants in (12), we infer that $\delta'\delta^{-1} \in \dot F^2$, and by (13) that $\operatorname{ord}\delta' \leqslant \operatorname{ord}\delta$, hence $\langle\delta\rangle \to \langle\delta'\rangle$, hence $N^{\#} \to M_{\mathfrak{m}}^{\#}$, hence $M \to N$ by (11), q.e.d.

THEOREM 3. *Let K and L be 2-dimensional regular lattices, $\varkappa \in Q(K)$, $\lambda \in Q(L)$ with $\mathfrak{o}\varkappa = \mathfrak{n}K$ and $\mathfrak{o}\lambda = \mathfrak{n}L$. Then $K \cong L$ if and only if the following conditions hold:*

$$(15)\qquad \mathfrak{s}K = \mathfrak{s}L, \quad dK \cong dL,$$

$$(16)\qquad (\varkappa, -dK)_{\mathfrak{p}} = (\lambda, -dL)_{\mathfrak{p}},$$

$$(17)\qquad \varkappa \cong \lambda \bmod \begin{cases} dL(\mathfrak{n}L)^{-1} & \textit{if } \operatorname{ord} dL \textit{ is odd},\\ \mathfrak{d}(-dL)(\mathfrak{n}L)^{-1}+2\mathfrak{p}^{(\operatorname{ord} dL)/2} & \textit{otherwise}.\end{cases}$$

Proof. Since (16) is a consequence of $FK \cong FL$ and since (17) follows from $\varkappa \in Q(L)$ and Theorem 1, the necessity of the conditions (15)–(17) is clear. Now to their sufficiency! It suffices to prove that the lattices $M = K^{\#}$ and $N = L^{\#}$ satisfy (12)–(14) with respect to $\mathfrak{m} = \mathfrak{n}L$, since then $M \to N$ by Theorem 2, hence $L \to K$ by (10), and also $K \to L$ by the symmetry of (15)–(17) in K and L, hence $K \cong L$. Condition (12) is a consequence of (15) and (16). By (17) we have $\mathfrak{m} = \mathfrak{n}K$, hence $M_{\mathfrak{m}} = M$, and therefore (13) is satisfied in virtue of (15). Finally, Theorem 1 and (15)–(17) show the validity of (14), q.e.d.

We say that two lattices (not necessarily in the same space) are in the *same class* if they are isometric. Similarly, two elements α and β of $\dot F$ are said to be in the same *class* or in the same *class modulo* $\mathfrak{a}$ (where $\mathfrak{a}$ is any fractional ideal of F) if $\alpha \cong \beta$ or $\alpha \cong \beta \bmod \mathfrak{a}$ respectively. For any non-zero fractional ideal $\mathfrak{n}$ and any $d \in \dot F$ define the ideal $\mathfrak{b}(d, \mathfrak{n})$ to be $d\mathfrak{n}^{-1}$ if $\operatorname{ord} d$ is odd, and to be $\mathfrak{d}(-d)\mathfrak{n}^{-1}+2\mathfrak{p}^{(\operatorname{ord} d)/2}$ otherwise. If L is a regular lattice, we denote by $q(L)$ any $\lambda \in F$ with $\lambda \in Q(L)$ and $\lambda\mathfrak{o} = \mathfrak{n}L$.

Put $\chi_{\mathfrak{p}}(L) = \big(-q(L), -dL\big)_{\mathfrak{p}}$. Then Theorem 3 shows that for any 2-dimensional regular lattice L the quantities $\mathfrak{s}L$, class of dL, $\chi_{\mathfrak{p}}(L)$ and class of $q(L)$ modulo $\mathfrak{b}(dL, \mathfrak{n}L)$ form a complete set of class invariants. The relations between these invariants will be exhibited in the next theorem. The invariant nature of $\chi_{\mathfrak{p}}(L)$ can also be seen from the relation

$$\chi_{\mathfrak{p}}(L) = (-1, -1)_{\mathfrak{p}} S_{\mathfrak{p}}(FL). \tag{18}$$

Denote by $h_{\mathfrak{p}}(d, \mathfrak{n}, \mathfrak{s})$ the number of classes of all 2-dimensional regular lattices L with $dL \cong d$, $\mathfrak{n}L = \mathfrak{n}$ and $\mathfrak{s}L = \mathfrak{s}$.

Lemma 1. a) *All units ε, η of $\mathfrak{o}$ with $\mathfrak{d}(\varepsilon)\mathfrak{d}(\eta) \subset 4\mathfrak{o}$ satisfy $(\varepsilon, \eta)_{\mathfrak{p}} = 1$. b) If ε is a unit of $\mathfrak{o}$ with $\mathfrak{d}(\varepsilon) \supset 4\mathfrak{o}$, there exists a unit η of $\mathfrak{o}$ with $\mathfrak{d}(\varepsilon)\mathfrak{d}(\eta) = 4\mathfrak{o}$ and $(\varepsilon, \eta)_{\mathfrak{p}} = -1$.*

Proof. Part a) is proved in [4], pp. 174. As for part b), we choose an α in $\mathfrak{o}$ with $(\alpha, \varepsilon)_{\mathfrak{p}} = -1$ by [3], 63 : 13. Consider the quadratic space $V \cong \langle 1\rangle \perp \langle -\varepsilon\rangle$. Then $\alpha \notin Q(V)$. By [5], Lemma 3.7, there exists a unit η in $\mathfrak{o}$ such that $\mathfrak{d}(\varepsilon)\mathfrak{d}(\eta) = 4\mathfrak{o}$ and $\alpha\eta \in Q(V)$, hence $(\varepsilon, \eta)_{\mathfrak{p}} = -1$, q.e.d.

Theorem 4. *Given any non-zero fractional ideals $\mathfrak{n}, \mathfrak{s}$ of F and any elements d, μ of $\dot{F}$ with $\mu\mathfrak{o} = \mathfrak{n}$ and any number $\varepsilon \in \{1, -1\}$. Put $u = \operatorname{ord}\mathfrak{n}$, $s = \operatorname{ord}\mathfrak{s}$, $v = \operatorname{ord}\mathfrak{b}(-d)$ and $w = \operatorname{ord} d$.*

(a) *There exists a 2-dimensional regular lattice L with $\mathfrak{s}L = \mathfrak{s}$, $dL \cong d$, $\chi_{\mathfrak{p}}(L) = \varepsilon$ and $q(L) \cong \mu \bmod \mathfrak{b}(d, \mathfrak{n})$ if and only if the following conditions hold:*

$$w \geqslant 2s; \tag{19}$$

$$u = s \textit{ if } w > 2s;\ s \leqslant u \leqslant \min(e+s, [v/2]) \textit{ if } w = 2s; \tag{20}$$

$$\varepsilon = (-\mu, -d)_{\mathfrak{p}} \textit{ if } w \geqslant 2e+2s \textit{ or } u = e+s \textit{ or } v > e+u+w/2. \tag{21}$$

(b) *$h_{\mathfrak{p}}(d, \mathfrak{n}, \mathfrak{s}) > 0$ if and only if (19) and (20) are satisfied, and then*

$$h_{\mathfrak{p}}(d, \mathfrak{n}, \mathfrak{s}) = \begin{cases} 1 & \textit{if} \quad u \geqslant e+s, \\ 2(N\mathfrak{p})^{[v/2]-u} & \textit{if} \quad u < e+s,\ w < 2e+2s,\ 2 \mid w, \\ & \qquad v \leqslant e+u+w/2, \\ (N\mathfrak{p})^{[(e-u+w/2)/2]} & \textit{if} \quad u < e+s,\ w < 2e+2s,\ 2 \mid w, \\ & \qquad v > e+u+w/2, \\ 2(N\mathfrak{p})^{[w/2]-s} & \textit{if} \quad w < 2e+2s,\ 2 \nmid w, \\ (N\mathfrak{p})^{e} & \textit{if} \quad w = 2e+2s, \\ 2(N\mathfrak{p})^{e} & \textit{if} \quad w > 2e+2s. \end{cases}$$

Proof. By scaling we may assume that $s = 0$.

1) We prove the necessity of (19)–(21). The condition (19) is obvious, also (20) for $w > 0$. If $w = 0$, the condition (20) is clear by [3], 93 : 17. As for (21), we observe that $\varepsilon = (-\mu, -d)_{\mathfrak{p}} k$, where $k = \big(q(L)\mu^{-1}, -d\big)_{\mathfrak{p}}$. If $w \geqslant 2e$ or $v > e+u+w/2$ and if w is odd, we have $u = 0$ and $\mathfrak{b}(d, \mathfrak{n}) \subset 4\mathfrak{o}$, hence $\mathfrak{d}\big(q(L)\mu^{-1}\big) = 0$, hence $k = 1$. If $w \geqslant 2e$ or $v > e+u+w/2$ and if w is even, then $\mathfrak{b}(d, \mathfrak{n}) \subset 4\mathfrak{p}^{w-v+u}$, hence $k = 1$ by Lemma 1. Finally, if $u = e$, then $w = 0$ and $v \geqslant 2e$ by (19) and (20), hence $k = 1$ again by Lemma 1. Thus (21) is proved.

2) Now to the sufficiency of (19)–(21) for part a)! First, let $w > 0$. We show that there is a unit $\eta \cong 1 \bmod \mathfrak{b}(d, \mathfrak{n})$ with $(\eta, -d)_{\mathfrak{p}} = -1$ if $w < 2e$ and $v \leqslant e+w/2$. If w is odd, we have $\mathfrak{b}(d, \mathfrak{n}) \supset 4\mathfrak{o}$, and therefore every unit η of quadratic defect $4\mathfrak{o}$ has the desired properties by [3], 63 : 11a. If w is even, we observe that $\mathfrak{d}(-d\pi^{-w}) \supset 4\mathfrak{o}$ so that we can find a unit η by Lemma 1 with $(\eta, -d)_{\mathfrak{p}} = -1$ and $\mathfrak{d}(\eta) = \mathfrak{p}^{2e-v+w} \subseteq \mathfrak{b}(d, \mathfrak{n})$. Now the lattice $L \cong \langle\mu\rangle \perp \langle d\mu^{-1}\rangle$ satisfies the assertion, unless $(-\mu, -d)_{\mathfrak{p}} = -\varepsilon$, $w < 2e$ and $v \leqslant e+w/2$. But in the latter case the lattice $L \cong \langle\mu\eta\rangle \perp \langle d(\mu\eta)^{-1}\rangle$ (with the unit η constructed before) has the required type. Secondly, let $w = 0$. Then $-d \cong 1-\delta$ for some δ in $\mathfrak{o}$ with $\mathfrak{d}(1-\delta) = \delta\mathfrak{o} = \mathfrak{p}^{v}$. The lattice $L \cong \langle A(\mu, \delta\mu^{-1})\rangle$ meets the requirements, unless $(-\mu, -d)_{\mathfrak{p}} = -\varepsilon$, $u < e$ and $v \leqslant e+u$. But in the latter case $v < 2e$, hence Lemma 1 implies the existence of a unit η with $(\eta, -d)_{\mathfrak{p}} = -1$ and $\mathfrak{d}(\eta) = \mathfrak{p}^{2e-v} \subseteq \mathfrak{b}(d, \mathfrak{n})\mathfrak{n}^{-1}$, and the lattice $L \cong \langle A\big(\mu\eta, \delta(\mu\eta)^{-1}\big)\rangle$ satisfies the assertion.

3) It remains to compute $h_{\mathfrak{p}} = h_{\mathfrak{p}}(d, \mathfrak{n}, \mathfrak{s})$ under the conditions (19) and (20). Denote by G the number of classes modulo $\mathfrak{b}(d, \mathfrak{n})$ within the set of all elements μ of F satisfying $\operatorname{ord}\mu = u$. By part a) and Theorem 3 we have $h_{\mathfrak{p}} = 2G$ if $w < 2e$, $u < e$ and $v \leqslant e+u+w/2$, and $h_{\mathfrak{p}} = G$ otherwise. It is easy to see that G equals the number of solutions ξ modulo $\mathfrak{p}^{g}$ of the congruence $\xi^2 \equiv 1 \bmod \mathfrak{p}^{g}$ in $\mathfrak{o}$, where $g = -u + \operatorname{ord}\mathfrak{b}(d, \mathfrak{n})$. Therefore by [1], p. 236 we obtain $G = (N\mathfrak{p})^{[g/2]}$ or $2(N\mathfrak{p})^{e}$ according as $g \leqslant 2e$ or not. This yields the assertion for $h_{\mathfrak{p}}$.

2. Isometry over non-dyadic local fields. The terminology of the preceding section is kept throughout this section, except that here F is supposed to be a non-dyadic local field. To this case the definition of $h_{\mathfrak{p}}(d, \mathfrak{n}, \mathfrak{s})$, $q(L)$ and $\chi_{\mathfrak{p}}(L)$ for 2-dimensional regular lattices L can be carried over, (18) remains true. For d in $\dot{F}$ and for non-zero fractional ideals $\mathfrak{n}$ of F put $\mathfrak{b}(d, \mathfrak{n}) = \mathfrak{n}$ or $\mathfrak{n}\mathfrak{p}$ according as $d\mathfrak{n}^{-2} = \mathfrak{o}$ or not.

Lemma 2. *Let K and L be 2-dimensional regular lattices. Then $K \cong L$ if and only if $dK \cong dL$ and $q(K) \cong q(L) \bmod \mathfrak{b}(dL, \mathfrak{n}L)$.*

Proof. Clear by [3], 92 : 2b.

Lemma 3. *Given any non-zero fractional ideals* $\mathfrak{n}, \mathfrak{s}$ *of* F *and any elements* d, μ *of* $\dot{F}$ *with* $\mu\mathfrak{o} = \mathfrak{n}$.

a) *There exists a 2-dimensional regular lattice* L *with* $\mathfrak{s}L = \mathfrak{s}$, $dL \cong d$ *and* $q(L) \cong \mu \bmod \mathfrak{b}(d, \mathfrak{n})$ *if and only if*

$$(22) \qquad \mathfrak{n} = \mathfrak{s} \quad \textit{and} \quad d\mathfrak{n}^{-2} \subseteq \mathfrak{o}.$$

holds.

b) $h_\mathfrak{p}(d, \mathfrak{n}, \mathfrak{s}) > 0$ *if and only if* (22) *holds, and then* $h_\mathfrak{p}(d, \mathfrak{n}, \mathfrak{s}) = 1$ *or* 2 *according as* $d\mathfrak{n}^{-2} = \mathfrak{o}$ *or not.*

Proof. The necessity of (22) is obvious. The sufficiency of part a) follows from the fact that the lattice $L \cong \langle\mu\rangle \perp \langle d\mu^{-1}\rangle$ meets the requirements. As for part b), we note that Lemma 2 and part a) imply $h_\mathfrak{p}(d, \mathfrak{n}, \mathfrak{s}) = G$, where G denotes the number of classes modulo $\mathfrak{b}(d, \mathfrak{n})$ within the set of all elements μ of $\dot{F}$ with $\mu\mathfrak{o} = \mathfrak{n}$. Now $G = 1$ or 2 according as $\mathfrak{b}(d, \mathfrak{n})\mathfrak{n}^{-1} = \mathfrak{o}$ or not, q. e. d.

The following remark will be useful later. If L is a 2-dimensional regular lattice with $\operatorname{ord}\mathfrak{n}L = u$ and $\operatorname{ord} dL = w$, we have by the properties of the Hilbert symbol

$$(23) \qquad \chi_\mathfrak{p}(L) = (-1)_\mathfrak{p}^{uw}\big(-\pi^{-u}q(L)\big)_\mathfrak{p}^{w}(-\pi^{-w}dL)_\mathfrak{p}^{u},$$

where $(\alpha)_\mathfrak{p}$ denotes the quadratic residue symbol modulo $\mathfrak{p}$ for α in $\mathfrak{o}$.

3. Isometry over complete archimedean fields. In this section let $\mathfrak{o} = F$ and either $F = R$ or C, where R denotes the field of real and C the field of complex numbers. Let $\mathfrak{p}$ be the spot at which F is complete. We state known results in a form convenient for our later purposes.

(a) Let $F = C$. For given $d \in \dot{F}$ there exists up to isometry exactly one 2-dimensional regular lattice L with $dL \cong d$, and then

$$S_\mathfrak{p}(L) = (-1, -1)_\mathfrak{p} = 1.$$

(b) Let $F = R$. For regular lattices L put $t(L) = \operatorname{ind}^+ L$, where ind^+ is defined as in [3], § 61A. For given $d \in \dot{F}$ and $t \in \{0, 1, 2\}$ there exists a 2-dimensional regular lattice L with $t(L) = t$ and $dL \cong d$ if and only if

$$(24) \qquad d \cong (-1)^t,$$

and then L is uniquely determined up to isometry, furthermore

$$(25) \qquad S_\mathfrak{p}(L) = (-1, -1)_\mathfrak{p}(-1)^{t(t-1)/2}.$$

4. The number of genera. Throughout this section $\mathfrak{o}$ is the ring of integers of an algebraic number field F. Let Ω be the set of all spots on F, let S be the subset of all non-archimedean spots and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ the real archimedean spots on F. For F, quadratic spaces V, lattices L and fractional ideals $\mathfrak{a}$ of F as usual $F_\mathfrak{p}, V_\mathfrak{p}, L_\mathfrak{p}$ and $\mathfrak{a}_\mathfrak{p}$ denote the corresponding localisations at the spot $\mathfrak{p} \in \Omega$. For $\mathfrak{p} \in S$ we write $\mathfrak{p} \mid 2$ or $\mathfrak{p} \nmid 2$ according as $\operatorname{ord}_\mathfrak{p} 2 > 0$ or not. By $\pi_\mathfrak{p}$ we denote any prime element of $\mathfrak{o}_\mathfrak{p}$ and by $\mathfrak{d}_\mathfrak{p}(\beta)$ the quadratic defect of any β in $F_\mathfrak{p}$.

Theorem 5. *Let* n *be any natural number. Given an* n*-dimensional regular* $\mathfrak{o}_\mathfrak{p}$*-lattice* $K_{(\mathfrak{p})}$ *for each* $\mathfrak{p}$ *in* Ω, *there exists a regular lattice* L *with* $L_\mathfrak{p} \cong K_{(\mathfrak{p})}$ *for all* $\mathfrak{p}$ *in* Ω *if and only if the following conditions hold:*

$$(26) \qquad K_{(\mathfrak{p})} \textit{ is } \mathfrak{o}_\mathfrak{p}\textit{-modular for almost all } \mathfrak{p} \in S;$$

$$(27) \qquad \prod_{\mathfrak{p} \in \Omega} S_\mathfrak{p}(F_\mathfrak{p}K_{(\mathfrak{p})}) = 1;$$

$$(28) \qquad \textit{there exists an } \alpha \in \dot{F} \textit{ with } d(F_\mathfrak{p}K_{(\mathfrak{p})}) = \alpha \textit{ for all } \mathfrak{p} \in \Omega.$$

Proof. (a) Necessity. We have

$$(29) \qquad \mathfrak{n}K_{(\mathfrak{p})} = (\mathfrak{n}L)_\mathfrak{p}, \quad \mathfrak{v}K_{(\mathfrak{p})} = (\mathfrak{v}L)_\mathfrak{p} \quad \text{for all } \mathfrak{p} \in S,$$

hence (26) is satisfied. The conditions (27) and (28) are clear by [3], 72 : 1.

(b) Sufficiency. (26) implies that $S_\mathfrak{p}(F_\mathfrak{p}K_{(\mathfrak{p})}) = 1$ for almost all $\mathfrak{p}$ in Ω, hence by (27), (28) and [3], 72 : 1 there exists a regular quadratic space V over F with $V_\mathfrak{p} \cong F_\mathfrak{p}K_{(\mathfrak{p})}$ for all $\mathfrak{p}$ in Ω. Take any lattice M on V. Then

$$(30) \qquad F_\mathfrak{p}M_\mathfrak{p} \cong F_\mathfrak{p}K_{(\mathfrak{p})} \quad \text{for all } \mathfrak{p} \in \Omega.$$

Applying (26), (30) and [3], 92 : 1 to $\mathfrak{p} \nmid 2$, we obtain

$$(31) \qquad M_\mathfrak{p} \cong K_{(\mathfrak{p})} \quad \text{for almost all } \mathfrak{p} \in S.$$

By (30), (31) and [3], 81 : 14 we find a lattice L on V with $L_\mathfrak{p} \cong K_{(\mathfrak{p})}$ for all $\mathfrak{p}$ in S. But for $\mathfrak{p}$ in $\Omega - S$ we have then $L_\mathfrak{p} = M_\mathfrak{p} \cong K_{(\mathfrak{p})}$ by (30). This completes the proof.

We say that two lattices K and L (not necessarily in the same space) are in the same *genus* if $K_\mathfrak{p} \cong L_\mathfrak{p}$ for all $\mathfrak{p}$ in Ω.

Theorem 6. *Given any* α *in* $\dot{F}$, *any non-zero fractional ideals* $\mathfrak{v}, \mathfrak{n}, \mathfrak{s}$ *of* F *and any numbers* $t_1, \ldots, t_r$ *in* $\{0, 1, 2\}$. *Denote by* $H = H(\alpha, \mathfrak{v}, \mathfrak{n}, \mathfrak{s}, t_1, \ldots$ $\ldots, t_r)$ *the number of genera of all 2-dimensional regular lattices* L *satisfying* $d(FL) = \alpha$, $\mathfrak{v}L = \mathfrak{v}$, $\mathfrak{n}L = \mathfrak{n}$, $\mathfrak{s}L = \mathfrak{s}$ *and* $t(L_{\mathfrak{p}_i}) = t_i$ $(i = 1, \ldots, r)$. *Put*

$w(\mathfrak{p}) = \mathrm{ord}_\mathfrak{p}\mathfrak{v}$, $u(\mathfrak{p}) = \mathrm{ord}_\mathfrak{p}\mathfrak{n}$ *and* $T = [t_1(t_1-1)+\ldots+t_r(t_r-1)]/2$. *For* $H > 0$ *the following three conditions are necessary:*

$$\alpha(-1)^{t_i} \in \dot{F}^2_{\mathfrak{p}_i} \quad (i = 1, \ldots, r); \tag{32}$$

$$\mathrm{ord}_\mathfrak{p}\,\alpha \equiv w(\mathfrak{p}) \bmod 2 \textit{ for all } \mathfrak{p} \in S; \tag{33}$$

$$\prod_{\mathfrak{p}\in S} (\pi_\mathfrak{p}, -\alpha)_\mathfrak{p}^{u(\mathfrak{p})} = (-1)^T \textit{ if } \alpha \textit{ satisfies} \tag{34}$$

$$2\,|\,\mathrm{ord}_\mathfrak{p}\,\alpha \textit{ for all } \mathfrak{p} \in S,\ \mathfrak{d}_\mathfrak{p}(-\alpha) \subseteq 4\alpha\mathfrak{o}_\mathfrak{p} \textit{ for all } \mathfrak{p}\,|\,2. \tag{A}$$

Under the conditions (32)–(34) *we have*

$$H = k \prod_{\mathfrak{p}\in S} h_\mathfrak{p}(d_\mathfrak{p}, \mathfrak{n}_\mathfrak{p}, \mathfrak{s}_\mathfrak{p}), \tag{35}$$

where $k = 1$ *or* $1/2$ *according as* α *satisfies* (A) *or not, and where*

$$d_\mathfrak{p} = \alpha\pi_\mathfrak{p}^{g(\mathfrak{p})} \textit{ with } g(\mathfrak{p}) = w(\mathfrak{p}) - \mathrm{ord}_\mathfrak{p}\,\alpha. \tag{36}$$

The quantities $h_\mathfrak{p}$ *are computed for* $\mathfrak{p}\,|\,2$ *in Theorem* 4 *and for* $\mathfrak{p} \nmid 2$ *in Lemma* 3.

Proof. By (24) and (29), the conditions (32) and (33) are clear. The condition (34) follows from (27), using the formulas (18), (23), (25), Lemma 1 and the reciprocity law for the Hilbert norm residue symbol. Now we compute H. We may assume the validity of (32)–(34) and the existence of 2-dimensional regular $\mathfrak{o}_\mathfrak{p}$-lattices $K_{(\mathfrak{p})}$ with $dK_{(\mathfrak{p})} = d_\mathfrak{p}$, $\mathfrak{n}K_{(\mathfrak{p})} = \mathfrak{n}_\mathfrak{p}$, $\mathfrak{s}K_{(\mathfrak{p})} = \mathfrak{s}_\mathfrak{p}$ for all $\mathfrak{p}$ in S and with $dK_{(\mathfrak{p})} = \alpha$ for $\mathfrak{p} \in \Omega - S$, $t(K_{(\mathfrak{p}_i)}) = t_i$ $(i = 1, \ldots, r)$, where $d_\mathfrak{p}$ is defined by (36). Namely, this definition is necessary (up to equivalence) and sufficient for the validity of (26), (28) and $\mathfrak{v}K_{(\mathfrak{p})} = \mathfrak{v}_\mathfrak{p}$. From Theorem 5, (18) and (25) we infer that H equals the number of sets $\{K_{(\mathfrak{p})}\}_{\mathfrak{p}\in\Omega}$ satisfying

$$\prod_{\mathfrak{p}\in S} \chi_\mathfrak{p}(K_{(\mathfrak{p})}) = (-1)^T, \tag{37}$$

where for each $\mathfrak{p} \in \Omega$ the lattice $K_{(\mathfrak{p})}$ is of the kind described before and restricted to a fixed system of representatives for the $\mathfrak{o}_\mathfrak{p}$-isometry classes. If α satisfies (A), the condition (37) holds for all such sets in virtue of (34), hence (35) is true for $k = 1$. Assume now that α does not satisfy (A). Then there exists a spot $\mathfrak{p}$ in S which violates (A). By applying the Theorems 3 and 4, Lemma 1 and [3], 63 : 11a to the case $\mathfrak{p}\,|\,2$ and the Lemmas 2 and 3 and (23) to the case $\mathfrak{p} \nmid 2$, we see that for this $\mathfrak{p}$ the invariant $\chi_\mathfrak{p}(K_{(\mathfrak{p})})$ takes on any given sign as $K_{(\mathfrak{p})}$ varies within the limits defined before. Therefore here (35) is satisfied with $k = 1/2$, q.e.d.

In concluding, we remark that if F is the field of rational numbers, the property (A) simply amounts to the condition $-\alpha \in \dot{F}^2$, and then (34) becomes superfluous. But in general, as examples show, this remark does not apply to fields F of degree > 1.

References

[1] H. Hasse, *Zahlentheorie*, 2nd ed., Berlin 1963.

[2] O. T. O'Meara, *The integral representations of quadratic forms over local fields*, Amer. J. Math. 80 (1958), pp. 843–878.

[3] — *Introduction to Quadratic Forms*, Berlin Göttingen, Heidelberg 1963.

[4] — *Integral equivalence of quadratic forms in ramified local fields*, Amer. J. Math. 79 (1957), pp. 157–186.

[5] C. Riehm, *On the integral representations of quadratic forms over local fields*, Amer. J. Math. 86 (1964), pp. 25–62.

[6] G. L. Watson, *Integral quadratic forms*, Cambridge Tract No 51 (1960).

ABTEILUNG FÜR MATHEMATIK IV DER UNIVERSITÄT ULM

Received on 4. 11. 1972 (341)