ON THE NUMBER OF INEQUIVALENT BINARY UNIMODULAR FORMS

SAMSON M. ROSENZWEIG

1. **Introduction.** In [1] and [2], O. T. O'Meara has given necessary and sufficient conditions for equivalence of binary unimodular forms in the ring of integers of a local field. The purpose of this paper is to use these results to compute the number of inequivalent binary unimodular forms in such a ring.

Let F be a local field [2, §32] in which 2 is not a unit, $\mathfrak{O}$ the ring of integers of F, $\mathfrak{O}^2$ the set of squares of elements of $\mathfrak{O}$, π a prime element of $\mathfrak{O}$, e the ramification index, with $2=\pi^e g$, and f the residue class degree. The residue class field $\overline{F}$ then has $2^f=q$ elements, and thus is a finite field of characteristic 2. Two elementary facts about such fields are of importance: (i) If $a\in\overline{F}$, there is a unique $b\in\overline{F}$ such that $b^2=a$. (ii) If $a, b\in\overline{F}$ and $a, b\neq 0$, then the set $\{ax^2+bx; x\in\overline{F}\}$ is an additive subgroup of index 2 in $\overline{F}$. We will also use the following result: If $r\leqq 2e$, $a, b\in\mathfrak{O}$, and $a^2\equiv b^2 \pmod{\pi^r}$, then $a\equiv b \pmod{\pi^s}$, where $s=[(r+1)/2]$.

If L is a binary unimodular lattice over $\mathfrak{O}$, then L is equivalent to a lattice generated by η, ω with $\eta^2=a$, $\eta\cdot\omega=1$, $\omega^2=b$; following O'Meara, we denote such a lattice by $A(a, b)$. For given L, let ν be the smallest integer such that ord $\alpha^2=\nu$ for some $\alpha\in L$; we will call ν the (integer) norm of L, and observe that $\nu\leqq e$. If L is a lattice of norm ν, and ord $\alpha^2=\nu$, let μ be the largest integer (or ∞) such that there exists $\beta\in L$ with $\alpha\cdot\beta=1$ and ord $\beta^2=\mu$; O'Meara has shown [1, Lemma 14.1] that ν and μ are invariants under equivalence, and that either $\mu+\nu\geqq 2e$ or $\mu+\nu$ is odd.

In what follows, it should be mentioned that many of the partial results are stated or closely implied in [1, §14] and [2, §§63 and 93]. The following sets of necessary and sufficient conditions for equivalence of binary unimodular lattices K and L will be used:

(A) [1, Theorem 14.3]: $\nu(K)=\nu(L)$; K and L have the same discriminant; for some unit c, K and L both represent $c\pi^\nu$.

(B) [2, Theorem 93.16]: K and L are lattices in the same quadratic space (that is, they have the same discriminant and Hasse symbol); K and L have the same norm group.

2. **Units and unit squares in $\mathfrak{O}$.** We denote the group of units by U, the group of unit squares by U^2, and, for each $n>0$, the group

Received by the editors July 8, 1965.

$\{1+\pi^n x;\ x\in\mathfrak{O}\}$ by U_n (with $U_0=U$). The groups U^2, U_n, U_nU^2, $U_n\cap U^2$ are all subgroups of U, and we require some index theorems. Note that $a\in U_nU^2$ if and only if there exists $b\in U$ such that $a\equiv b^2 \pmod{\pi^n}$.

LEMMA. (i) $(U_{2e+1}U^2\colon U^2)=1$.
(ii) $(U_{2e}U^2\colon U_{2e+1}U^2)=2$.
(iii) *If* $0\leqq n<2e$ *and* n *is even, then* $(U_nU^2\colon U_{n+1}U^2)=1$.
(iv) *If* $0\leqq n<2e$ *and* n *is odd, then* $(U_nU^2\colon U_{n+1}U^2)=q$.

PROOF. (i) Let $a\in U_{2e+1}U^2$. Then $a=b^2+\pi^{2e+1}c$ for some $b\in U$, $c\in\mathfrak{O}$. Let $b_1=b+\pi^{e+1}x$. Then $b_1^2=a$ is equivalent to $gx+\pi x^2=c$. Since this equation is solvable by Hensel's Lemma, $a\in U^2$.

(ii) Let $a\in U_{2e}U^2$. Then $a=b^2+\pi^{2e}c$ for some $b\in U$, $c\in\mathfrak{O}$. If $a\equiv b_1^2 \pmod{\pi^{2e+1}}$, then $b_1\equiv b \pmod{\pi^e}$; so put $b_1=b+\pi^e x$. Then $b_1^2\equiv a \pmod{\pi^{2e+1}}$ is equivalent to $gx+x^2\equiv c \pmod{\pi}$, and the result follows from property (ii) of $\overline{F}$.

(iii) Let $n=2m$, and $a=b^2+\pi^{2m}c$ as before. Pick $x\in\mathfrak{O}$ with $x^2\equiv c \pmod{\pi}$; then $(b+\pi^m x)^2\equiv a \pmod{\pi^{n+1}}$. Thus, if $a\in U_nU^2$, then $a\in U_{n+1}U^2$.

(iv) Let $n=2m-1$. It is sufficient (because $\overline{F}$ has q elements) to show that, if $a\equiv c \pmod{\pi^n}$ and a, $c\in U_{n+1}U^2$, then $a\equiv c \pmod{\pi^{n+1}}$. But, if $a\equiv b^2 \pmod{\pi^{n+1}}$ and $c\equiv d^2 \pmod{\pi^{n+1}}$, then $b^2\equiv d^2 \pmod{\pi^{2m-1}}$; thus $b\equiv d \pmod{\pi^m}$ and $a\equiv c \pmod{\pi^{2m}}$.

THEOREM 1. (i) $(U\colon U_nU^2)=q^{[n/2]}$ *if* $0\leqq n\leqq 2e$,

$$(U\colon U^2) = 2q^e.$$

(ii) $(U_n\colon U_n\cap U^2)=2q^{e-[n/2]}$ *if* $0\leqq n\leqq 2e$.

PROOF. (i) We have

$$(U\colon U_nU^2) = (U\colon U_1U^2)(U_1U^2\colon U_2U^2)\cdots(U_{n-1}U^2\colon U_nU^2),$$

and the result follows immediately from the lemma.

(ii) $(U_n\colon U_n\cap U^2)=(U_nU^2\colon U^2)=(U\colon U^2)/(U\colon U_nU^2)=2q^e/q^{[n/2]}$.

3. **The number of inequivalent forms.** Fixing ν, we investigate the number of inequivalent forms of norm ν. The case $\nu=e$ is easily settled, as follows: If L is any lattice of norm e, then L is equivalent to $A(a\pi^e,\ b\pi^e)$ for some $a\in U$, $b\in\mathfrak{O}$. Since the discriminant of any such lattice is represented by $-1+d\pi^{2e}$ for some $d\in\mathfrak{O}$, there are $(U_{2e}\colon U_{2e}\cap U^2)=2$ possible discriminants; and since, for any $a\in U$, $A(a\pi^e,\ b\pi^e)$ represents π^e (because the equation $ax^2+gxy+by^2=1$ can be solved by picking x with $ax^2\equiv 1 \pmod{\pi}$ and using Hensel's

Lemma to solve for y), it follows from (A) that there are 2 inequivalent forms of norm e. These may be taken as $A(\pi^e, 0)$ and $A(\pi^e, b\pi^e)$, where $1+b\pi^{2e}$ is not a square.

Now assume $0 \leqq \nu < e$, and put $\lambda = e - \nu$. We consider lattices of two types:

(I) Here we discuss all lattices equivalent to $A(a\pi^\nu, c\pi^{e+1})$ for some $a \in U$, $c \in \mathfrak{O}$. Any such lattice has a discriminant represented by $-1+d\pi^{\nu+e+1}$, so there are $(U_{\nu+e+1}: U_{\nu+e+1} \cap U^2) = 2q^{[\lambda/2]}$ possible discriminants.

THEOREM 2. *For each discriminant as described, the number of inequivalent forms of type* I *having that discriminant is* $q^{[\lambda/2]}$; *and thus the total number of inequivalent forms of type* I *is* $2q^{2[\lambda/2]}$.

PROOF. We show that, if a, $b \in U$, then a lattice $A(a\pi^\nu, c\pi^{e+1})$ represents b if and only if $ab^{-1} \in U_\lambda U^2$. In order for the equation $ax^2 + \pi^\lambda gxy + \pi^{\lambda+1} cy^2 = b$ to have a solution, the condition $ab^{-1} \in U_\lambda U^2$ is certainly necessary; while, if it is satisfied, the equation is solved by picking x with $ax^2 \equiv b \pmod{\pi^\lambda}$ and using Hensel's Lemma to solve for y. Since, for any discriminant $-1+d\pi^{\nu+e+1}$ and any unit a, the lattice $A(a\pi^\nu, a^{-1}d\pi^{e+1})$ has that discriminant, the number of inequivalent lattices per discriminant is $(U: U_\lambda U^2) = q^{[\lambda/2]}$, and the theorem is proved.

(II) Here we discuss all remaining lattices; and it is sufficient to examine lattices $A(a\pi^\nu, b\pi^\mu)$, with a, $b \in U$, $\nu < \mu \leqq e$, and $\mu+\nu$ odd. It is sufficient to look for the number of inequivalent forms for each pair ν, μ satisfying the conditions. Put $\lambda = e - \nu$, $2\tau + 1 = \mu - \nu$.

The discriminant of any form of type II is represented by $-1+d\pi^{\mu+\nu}$, where $d \in U$; it follows that the number of different discriminants for given ν, μ is

$$(U_{\mu+\nu}: U_{\mu+\nu} \cap U^2) - (U_{\mu+\nu+1}: U_{\mu+\nu+1} \cap U^2),$$

since the first term is the number of discriminants represented by $-1+d\pi^{\mu+\nu}$ with $d \in \mathfrak{O}$, and the second the number with $d \equiv 0 \pmod{\pi}$. There are thus

$$\begin{aligned} 2q^{e-[(\mu+\nu)/2]} - 2q^{e-[(\mu+\nu+1)/2]} &= 2q^{e-(\mu+\nu-1)/2} - 2q^{e-(\mu+\nu+1)/2} \\ &= 2q^{\lambda-\tau}(q-1) \end{aligned}$$

discriminants.

Next, no form of type II can represent 0; and it follows [2, Theorem 63.22] that, for each discriminant, we can get a binary space over F with either Hasse symbol, and it is easily seen that any such space can be represented as (α, β), where $\alpha^2 = a\pi^\nu$, $\alpha \cdot \beta = 1$, $\beta^2 = b\pi^\mu$ and

a, $b \in U$. There are thus $4q^{\lambda-\gamma}(q-1)$ different spaces.

A general discussion of norm groups can be found in [2, §93]. For our purposes, it suffices to say that the norm group of a lattice of type II is $\{a\pi^\nu\mathfrak{O}^2+\pi^\mu\mathfrak{O}\}$, where $a \in U$ and the lattice represents $a\pi^\nu$. Since it is evident that $\{a\pi^\nu\mathfrak{O}^2+\pi^\mu\mathfrak{O}\}=\{c\pi^\nu\mathfrak{O}^2+\pi^\mu\mathfrak{O}\}$ if and only if $ac^{-1}\in U_{\mu-\nu}U^2$, there are $(U: U_{\mu-\nu}U^2)=q^{\tau-1}$ possible norm groups.

The discussion will be complete when it is shown that each space supports a lattice with any of the norm groups.

LEMMA. *Let $a, b \in U$, and let the space V have basis α, β, with $\alpha^2=a\pi^\nu$, $\alpha\cdot\beta=1$, $\beta^2=b\pi^\mu$, and let $c \in U$. Then there exists $d \in U$ such that $d\pi^\nu \equiv c\pi^\nu$ (mod π^e) and V represents $d\pi^\nu$.*

PROOF. It is sufficient to find $x, y \in F$ such that

$$a\pi^\nu x^2 + b\pi^\mu y^2 \equiv c\pi^\nu \pmod{\pi^e}.$$

Putting $y=\pi^{-\tau}v$, this becomes

$$ax^2 + b\pi v^2 \equiv c \pmod{\pi^{e-\nu}}.$$

This last congruence can even be solved in $\mathfrak{O}$, as follows: Set $x=\sum_{i=0}^\infty v_{2i}\pi^i$, $v=\sum_{i=0}^\infty v_{2i+1}\pi^i$, where the v_i are to be chosen from (say) a fixed set of residues mod π. Substituting, we obtain

$$\sum_{i=0}^{\infty} av_{2i}^2\pi^{2i} + \sum_{i=0}^{\infty} bv_{2i+1}^2\pi^{2i+1} \equiv c \pmod{\pi^{e-\nu}}.$$

We can now solve this by a method of successive congruences; that is, we choose v_i so that the congruence will be satisfied mod π^{i+1}. Explicitly, let A_i denote a if i is even, b if i is odd; choose v_0 such that $av_0^2\equiv c$ (mod π), v_1 such that $b\pi v_1^2\equiv c-av_0^2$ (mod π^2), and, for $0\leqq k \leqq e-\nu-1$, v_k such that

$$A_k\pi^k v_k^2 \equiv \left(c - \sum_{i=0}^{k-1} A_i\pi^i v_i^2\right) \pmod{\pi^{k+1}}.$$

It follows by induction and property (i) of $\bar{F}$ that these choices can be made, and, taking $v_i=0$ for $i\geqq e-\nu$, the resulting x and v satisfy the congruence.

THEOREM 3. (i) *For each appropriate pair ν, μ, the number of inequivalent forms is* $4q^{\lambda-1}(q-1)$,

(ii) *For each ν, the number of inequivalent forms of norm ν is*

$$4\left[\frac{\lambda+1}{2}\right]q^{\lambda-1}(q-1) + 2q^{2[\lambda/2]}.$$

PROOF. (i) if V is any of the spaces arising from lattices of type II, and $a \in U$, the lemma shows that V represents some $c\pi^\nu$ with $a\pi^\nu \equiv c\pi^\nu \pmod{\pi^e}$. Hence V supports a lattice $A(c\pi^\nu, b\pi^\mu)$, and the norm group of this lattice is $\{c\pi^\nu \mathfrak{O}^2 + \pi^\mu \mathfrak{O}\} = \{a\pi^\nu \mathfrak{O}^2 + \pi^\mu \mathfrak{O}\}$. It follows, using conditions (B), that the number of inequivalent forms is obtained by multiplying the number of spaces by the number of possible norm groups, and (i) follows.

(ii) For each ν, the number of appropriate μ in type II is $[(\lambda+1)/2]$. Combining Theorems 2 and 3(i), the result follows.

(Forms of type II can also be handled using conditions (A). The number of discriminants has already been obtained, and the key question is to determine, for given a, $b \in U$, those units c for which

$$a\pi^\nu x^2 + \pi^e gxy + b\pi^\mu y^2 = c\pi^\nu$$

has a solution in $\mathfrak{O}$. Clearly a necessary condition is $ac^{-1} \in U_{\mu-\nu}U^2$; putting $c = az^2 + \pi^{\mu-\nu}d$, with z determined uniquely mod $\pi^{\gamma+1}$, we see that x must have the form $z + \pi^{\gamma+1}u$. We then set $y = \sum_{i=0}^{\infty} y_{2i}\pi^i$, $u = \sum_{i+0}^{\infty} y_{2i+1}\pi^i$, substitute, and pick the y_i by successive congruences as in the proof of the lemma to Theorem 3; but now the cross-product terms cannot be ignored, and the expressions become quite formidable. It turns out that property (i) of $\overline{F}$ can be used to obtain y_i uniquely in solving the congruence mod $\pi^{\mu+i+1}$ as long as $0 \leqq i < 2(e-\mu)$; with this done, the equation takes the form

$$by_{2r}^2 + gzy_{2r} = C_1 + \pi C_2,$$

where C_1 depends on the given numbers and the y_i for $i < 2r$, and $r = e - \mu$. The nature of this equation, property (ii) of $\overline{F}$, Hensel's Lemma, and (A) can now be used to show that the number of inequivalent forms per discriminant is $2(U\colon U_{\mu-\nu}U^2)$. The author is indebted to the referee for suggesting the alternate approach using (B).)

BIBLIOGRAPHY

1. O. T. O'Meara, *Quadratic forms over local fields*, Amer. J. Math. **77** (1955), 87–116.

2. ———, *Introduction to quadratic forms*, Springer-Verlag, Berlin, 1963.

DOUGLASS COLLEGE, RUTGERS, THE STATE UNIVERSITY