Quadratic forms in models of $I\Delta_0 + \Omega_1$, part II: Local equivalence

Paola D'Aquino and Angus Macintyre

June 4, 2009

Abstract

In this second paper of the series we do a local analysis of quadratic forms over completions of a non standard model of $I\Delta_0 + \Omega_1$.

1 Introduction

This paper is a sequel to [DM2], and has the same setting and conventions. For convenience we list the basic ingredients of the preceding paper.

$\mathcal{L}$ is the language of Arithmetic, containing the symbols $\{0, 1, +, \cdot, \leq\}$, and $I\Delta_0$ is the fragment of Peano Arithmetic (PA) where induction is applied only to bounded formulas (Δ_0-formulas). We will be working in an expansion of the language $\mathcal{L}$ which contains also the function symbol #, where $\#(x, y) = x^{[\log y]}$. We consider Δ_0-induction in the expanded language, getting a theory $I\Delta_0^{\#}$ which is bi-interpretable with $I\Delta_0 + \Omega_1$. The models of $I\Delta_0 + \Omega_1$ are discretely ordered rings, and they have proved to be a natural setting for developing basic elementary number theory ([Wo], [DM1], [BI], [DM2]).

We recall that in any model of $I\Delta_0$ the notions of prime and irreducible coincide. In [BI] it was proved that for any model $\mathcal{M}$ of $I\Delta_0 + \Omega_1$ and for any p in $\mathcal{M}$ the index of the squares in the multiplicative group of $\mathcal{M}/(p)$ have index at most 2. In [DM1] we showed that the quotient field $\mathcal{M}/(p)$ has a unique extension of each degree $n \in \mathbb{N}$. We still do not know if it is a pseudofinite field as in the case of models of PA (see [M]).

If $\mathcal{M}$ is a model of $I\Delta_0 + \Omega_1$, $\mathcal{K}$ is the fraction field of $\mathcal{M}$, and $\mathcal{K}_\infty$ is the real closure of $\mathcal{M}$. In the case of the standard model the real closure of $\mathbb{Z}$ gives the real closure of $\mathbb{Q}$ which is an elementary substructure of $\mathbb{R}$.

In [DM2] we studied the basic theory of equivalence of binary quadratic forms over models of $I\Delta_0 + \Omega_1$, with a view to proving some natural version of Quadratic Reciprocity law in $I\Delta_0 + \Omega_1$. We are using Gauss' second proof as presented in Cassels [C]. We now turn to local equivalence, something that Gauss did in terms of congruences, but which is nowadays presented in p-adic terms.

In the present paper we will consider for each prime p of $\mathcal{M}$ the p-adic valuation on $\mathcal{K}$, and its henselization $\mathcal{K}_p^h$. Note that for the standard model we do not get in this way $\mathbb{Q}_p$, but rather its elementary subfield, the algebraic p-adics (see [AK1], [AK2], [AK3] and [E] for the basics on model theory of such henselizations). We will make strong use of the results of Ax-Kochen and Ershov from [AK1], [AK2], [AK3] and [E], even for non standard p.

Here we want to complete the study of binary quadratic forms over the completions of such structures, as an essential step in proving a version of Gauss' classical result of quadratic reciprocity law in $I\Delta_0 + \Omega_1$. As in the previous paper we follow Cassels' book [C]. In what follows, unless otherwise specified, the quadratic forms are all binary. We recall that to each quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is associated a determinant $det(f) = ac - \frac{b^2}{2}$ and a discriminant $D(f) = -4det(f) = b^2 - 4ac$. In [DM2] we studied $\mathcal{M}$-equivalence of binary quadratic forms over $\mathcal{M}$, the exact analogue of the standard equivalence of forms over $\mathbb{Z}$ (see [C]). Moreover we gave a Δ_0-definition of the analogue of the standard group operation on $\mathcal{M}$-equivalence classes. The resulting group is $\mathcal{G}_D$.

2 Local groups

Now we consider appropriate equivalences of forms over $\mathcal{K}_\infty$ the real closure of $\mathcal{M}$, and over $\mathcal{K}_p^h$, the henselization of the fraction field of $\mathcal{M}$.

2.1 Equivalence over $\mathcal{K}_\infty$

First of all the real closure of $\mathcal{K}$ is uniquely determined since there is a unique order on $\mathcal{M}$ (by Lagrange theorem, see [BI]) and so also on its fraction field $\mathcal{K}$. In a natural way we extend the notion of equivalence to forms over the real closure $\mathcal{K}_\infty$ of $\mathcal{M}$. Because of elimination of quantifiers for real closed fields, for any formula $\varphi(\overline{x})$, there is a quantifier-free formula $\psi(\overline{x})$ such that for any $\overline{m} \in \mathcal{M}$

$$\mathcal{K}_\infty \models \varphi(\overline{m}) \qquad \text{iff} \qquad \mathcal{K}_\infty \models \psi(\overline{m}) \qquad \text{iff} \qquad \mathcal{M} \models \psi(\overline{m}).$$

Two quadratic forms f and g over $\mathcal{K}_\infty$ are $\mathcal{K}_\infty$-equivalent if there is an invertible matrix B with coefficients in $\mathcal{K}_\infty$ such that $g(x, y) = f(B(x, y))$. So this property is quantifier-free in the coefficients of f and g.

Clearly, forms not equivalent over $\mathcal{M}$ can become equivalent over $\mathcal{K}_\infty$. Quadratic forms can be diagonalized over $\mathbb{R}$, and since this is a first order property, they can be diagonalized also over $\mathcal{K}_\infty$. In fact, the representative of the proper equivalence classes are the following quadratic forms

$$x^2 + y^2, -(x^2 + y^2), x^2 - y^2, x^2, -x^2.$$

The first two forms are both of discriminant -4 but they are not equivalent since one is positive definite while the other is negative definite. The third form is indefinite, and the last two are singular and they cannot be equivalent to any of the previous ones.

We consider now only quadratic forms with a fixed non zero discriminant D, and we denote the set of equivalence classes by $\mathcal{G}_{D,\infty}$. In the future we will drop the subscript D if no ambiguity arises.

It turns out that the following two cases can occur.

1. If $D < 0$, i.e. the forms are definite, then there are only two classes whose representative are

$$x^2 - \frac{D}{4}y^2 \qquad \text{and} \qquad -x^2 + \frac{D}{4}y^2.$$

The first represents the positive definite forms of discriminant D, while the second represents the negative definite forms of discriminant D.

2. If $D > 0$, i.e. the forms are indefinite, then there is a unique class with represenatative

$$x^2 - \frac{D}{4}y^2.$$

2.2 Equivalence over $\mathcal{K}_p^h$

2.2.1 Preliminaries

Let p be any prime in $\mathcal{M}$. It is well-known that there is a Δ_0-definable valuation on $\mathcal{M}$ (see for example [D1])

$$\begin{array}{rccc} v_p: & \mathcal{M} & \longrightarrow & \mathcal{M} \\ & m & \mapsto & v_p(m) \end{array}$$

where $v_p(m)$ is the highest exponent to which p divides m for $m \neq 0$, and $v_p(0) = \infty$. As in the classical case we can extend v_p to $\mathcal{K}$ the fraction field of $\mathcal{M}$, by setting $v_p(\frac{n}{m}) = v_p(n) - v_p(m)$ for all $n, m \in \mathcal{M}$, $m \neq 0$. So $(\mathcal{K}, v_p)$ is a valued field, with valuation ring

$$\mathcal{V}_p = \{a \in \mathcal{K} : v_p(a) \geq 0\}$$

which is clearly Δ_0-definable since v_p is. In the classical case the valuation ring is a principal ideal domain, but in our setting only certain definable ideals inside the valuation ring are principal. The situation improves once we pass to the henselization of $(\mathcal{K}, v_p)$. The set

$$\mathcal{I}_p = \{a \in \mathcal{V}_p : v_p(a) > 0\}$$

is a maximal ideal since it is generated by the prime p. Hence $\mathcal{V}_p/\mathcal{I}_p$ is a field, the residue field of $\mathcal{K}$ relative to the valuation v_p, and we will denote it by $\mathbb{F}_p$. As in the classical case $\mathbb{F}_p$ is $\mathcal{M}/(p)$, hence for p standard $\mathbb{F}_p$ is the field with p elements and for p non standard is a characteristic 0 field. Clearly $\mathcal{M}$ is isomorphic to a subring of $\mathcal{V}_p$ (which is got by inverting elements prime to p).

The set $\Gamma_p = \{v_p(a) : a \in \mathcal{K} - \{0\}\}$ is the value group of $(\mathcal{K} - \{0\}, v_p)$ and it coincides with the Bennett segment $\mathbb{B}_p$ relative to the prime p, see [D1]. Notice that the value group depends on p, more precisely for standard primes p the $\mathbb{B}_p$'s coincide while if p is non standard the relative value group may be different. For both standard and non standard primes the value group is a $\mathbb{Z}$-group, since it is an initial segment of $\mathcal{M}$ closed under $+$. From the general theory of valued fields $(\mathcal{K}, v_p)$ has an henselization $(\mathcal{K}_p^h, v_p)$, which is the smallest algebraic extension of $(\mathcal{K}, v_p)$ where Hensel's Lemma holds, and the valuation on $\mathcal{K}_p^h$ extends the valuation of $\mathcal{K}$. Moreover, the valuation ring $\mathcal{M}_p$ of $\mathcal{K}_p^h$ is a ring extension of the valuation ring $\mathcal{V}_p$ of $\mathcal{K}$, and the residue fields and the value groups of $(\mathcal{K}, v_p)$ and of its henselization $(\mathcal{K}_p^h, v_p)$ coincide under the obvious induced embeddings.

Remark 2.1 Since $\mathcal{M}_p$ is a local ring for every non zero elements $x, y \in \mathcal{M}_p$ we have $x|y$ or $y|x$, where $|$ stands for divisibility relation. We say that x and y are coprime if at most one of them is not a unit, i.e. at most one is divisible by p. This notion can be extended to more than two elements and for our porposes it will be enough to know that three elements $x, y, z \in \mathcal{M}_p$ are coprime if at most two of them are divisible by p.

We recall results due to Ax, Kochen and Ershov to which we will appeal in order to extend some of the properties on equivalence of binary quadratic forms to our setting.

We will use refinements due to Basarab, et al. in the model theory of valued fields, and we will work in a many sorted language (see [B]) containing a constant t, and sorts for

1. elements of the starting valued field K,
2. elements of the value group Γ,
3. elements in the residue field k,
4. elements in the quotient rings $\mathcal{V}/(t^n)$ for $n = 2, \ldots$
5. elements of the multiplicative groups $\mathcal{K}^*/(1 + (t^n\mathcal{V}))$ for $n = 1, 2, \ldots$.

Note that this list is redundant, but it is more perspicuous to keep all the sorts in view.

On the field sort, and residue field sort we have the usual language for rings, on the value group sort the usual language of ordered abelian groups, and on $\mathcal{V}/(t^n)$ for $n = 2, 3, \ldots$ the language of rings. On the sort for elements of the groups $\mathcal{K}^*/(1 + (t^n\mathcal{V}))$ there is the multiplication induced by $\mathcal{K}^*$. In addition, we have cross-sort functions corresponding to:

- $v : \mathcal{K} \longrightarrow \Gamma$
- $- : \mathcal{V} \longrightarrow k$
- $-_n : \mathcal{V} \longrightarrow \mathcal{V}/(p^n)$
- $v : \mathcal{K}^*/(1 + (t^n\mathcal{V})) \longrightarrow \Gamma$ the induced valuations.
- $ac_n : \mathcal{K}^*/(1 + (t^n\mathcal{V})) \longrightarrow \mathcal{V}/(t^n\mathcal{V})$ the angular components.

In this language the main result which will be useful for us is due to Basarab [B]. He proves that for all unramified henselian valued fields every formula in the above language is equivalent to one with no quantifications over the field sort, i.e. for any formula $\phi(\overline{x})$ there is a quantifier-free (w.r.t sorts in $\mathcal{K}$) $\phi^*(\overline{x})$ such that for all tuples $\overline{m}$ (where $\overline{m}$ contains elements from $\mathcal{M}$, $\mathcal{K}$ and the valued group Γ)

$$\mathcal{K} \models \phi^*(\overline{m}) \qquad \text{iff} \qquad \mathcal{K}_p^h \models \phi(\overline{m})$$

relative to the diagram

$$\begin{tikzcd}
\mathcal{M} \arrow[r, phantom, "="] \arrow[d] & \mathcal{M} \arrow[r] \arrow[d] & \mathcal{M}_p \arrow[d] \\
\mathcal{K} \arrow[r] & \mathcal{V}_p \arrow[r] & \mathcal{K}_p^h
\end{tikzcd}$$

We will often use also the following fundamental result due to Ax, Kochen and Ershov (see [AK1], [AK2], [AK3] and [E]).

Theorem 2.2 *Let $(\mathcal{K}, v, k, \Gamma)$ be an henselian field of characteristic 0, where k is the residue field and Γ is the value group. If v is unramified then $Th(\mathcal{K}, v, k, \Gamma)$ is completely determined by $Th(k)$ and $Th(\Gamma)$.*

In our setting for p non standard the residue field has characteristic 0, and for p standard we have $v_p(p) = 1$, so the valuation is unramified. Hence we can apply Theorem 2.2 and the following holds.

Theorem 2.3 *Let $\mathcal{M}$ be a model of $I\Delta_0 + \Omega_1$ and p be a prime in $\mathcal{M}$.*

1. For p standard, $\mathcal{K}_p^h$ is elementarily equivalent to $\mathbb{Q}_p$ (the field of p-adic numbers), and $\mathcal{M}_p$ is elementarily equivalent to the ring of p-adic integers.

2. For p non standard then $\mathcal{K}_p^h$ is elementary equivalent to $\mathbb{F}_p((t))$.

Proof: 1. In this case the valuations of $\mathcal{K}_p^h$ and $\mathbb{Q}_p$ are both unramified, the residue fields of $\mathcal{K}_p^h$ and $\mathbb{Q}_p$ coincide with $\mathbb{F}_p$ the field with p elements, and the value groups are both $\mathbb{Z}$-groups. Hence Theorem 2.2 gives the result.

2. In this case the characteristic of the residue field is 0 and so the valuation on $\mathcal{K}_p^h$ is unramified, and again from Theorem 2.2 it follows that $\mathcal{K}_p^h$ is elementarily equivalent to the field of power series over $\mathbb{F}_p$. □

Remark 2.4 1) Quite generally, the ordered value group Γ_p of $\mathcal{K}_p^h$ is uniformly interpretable in $\mathcal{K}_p^h$.

2) By Theorem 2.3 since all $\mathcal{K}_p^h$ are elementarily equivalent to models with value groups equal to $\mathbb{Z}$, it follows that all non empty subsets of $\{x : v_p(x) \geq 0\}$ definable in $\mathcal{K}_p^h$ in the many sorted language have a least element.

3) From 2) it follows easily that $\mathcal{M}_p$ is a definable PID, in the sense that any ideal $I \subseteq \mathcal{M}$, definable over $\mathcal{K}_p^h$ in the many sorted language, is principal.

2.3 Local equivalence of quadratic forms

In this section we will be mainly working in $\mathcal{M}_p$, the valuation ring of the henselization of the fraction of $\mathcal{M}$.

We now study the local theory of the equivalence relation between two forms over $\mathcal{M}_p$. We want a procedure, uniform in p, which allows us to define in $\mathcal{M}$ when two forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ over $\mathcal{M}$ are $\mathcal{K}_p^h$-equivalent or $\mathcal{M}_p$-equivalent. This will be done in terms of Hensel's Lemma.

Definition 2.5 *Let f and g be quadratic forms over $\mathcal{K}_p^h$. f and g are $\mathcal{M}_p$-equivalent if there is an invertible matrix T over $\mathcal{M}_p$ such that $f(\overline{x}) = g(T\overline{x})$.*

Notice that the discriminants of $\mathcal{M}_p$-equivalent forms differ by a factor which is the square of a unit in $\mathcal{M}_p$.

As usual we distinguish the cases for $p = 2$ and $p \neq 2$. For the case of $p = 2$ we will get the same results as for the classical case, since $\mathcal{K}_2^h \equiv \mathbb{Q}_2$, by Theorem 2.3 (some details will be given in Theorem 2.17).

Definition 2.6 *Fix a prime p. The vector $(a, b) \in \mathcal{M}_p^2$ is primitive if*

$$min(v_p(a), v_p(b)) = 0.$$

This is clearly a Δ_0-condition. Note that if $a, b \in \mathcal{M}$ then (a, b) is primitive if and only if p does not divide both a and b.

Lemma 2.7 *A necessary and sufficient condition that a vector* $(a, b) \in \mathcal{M}_p^2$ *forms a part of a basis is that it is primitive.*

Proof: This is a first order property true in any principal ideal domain. Hence it is true also in $\mathcal{M}_p$ for both p standard and non standard since the valuation rings are all elementary equivalent to a PID's. □

We now need a lemma analogous to Lemma 6.3 (*minimum principle*) of [DM2]. We will follow section 3 of chapter 8 of Cassels' [C], but we will replace his absolute values with valuations. We want to ensure that any regular form over $\mathcal{M}_p$ takes a minimum value with respect to the valuation.

Lemma 2.8 *(Minimum Principle) Let* $f(x, y)$ *be a regular quadratic form with coefficients in* $\mathcal{M}_p$*. Then there exists a primitive vector* (u, v) *such that* $v_p(f(u, v)) = min\{v_p(f(\overline{x})) : \overline{x} \in \mathcal{M}_p^2\}$.

Proof: By Remark 2.4 the set $\{v_p(f(\overline{x})) : \overline{x} \in \mathcal{M}_p^2\}$ has a least element. Then there is a vector $(a_1, a_2) \in \mathcal{M}_p^2$ on which f takes value with such minimum valuation. Notice that (a_1, a_2) is primitive. For if $(a_1, a_2) = p(c_1, c_2)$ then $v_p(f(c_1, c_2)) < v_p(f(a_1, a_2))$ a contradiction. □

Lemma 2.9 *Let* $f(x, y)$ *be a form over* $\mathcal{K}_p^h$*. Then* f *is* $\mathcal{M}_p$*-equivalent to a form* g *such that*

$$v_p(g(1, 0)) = min\{v_p(g(a, b)) : a, b \in \mathcal{M}_p\}.$$

Proof: Let (a_1, a_2) in $\mathcal{M}_p$ be primitive such that $v_p(f(a_1, a_2)) = min\{v_p(f(c_1, c_2)) : c_1, c_2 \in \mathcal{M}_p\}$. Complete (a_1, a_2) to a basis $(a_1, a_2), (b_1, b_2)$ using Lemma 2.7 above. Writing

$$T = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \tag{1}$$

we have $f(T(1, 0)) = f(a_1, a_2)$, and $g(\overline{x}) = f(T(\overline{x}))$. □

2.3.1 Canonical forms

It is convenient to use the rather general correspondence between quadratic forms over a unital commutative ring R of characteristic $\neq 2$ and quadratic spaces over R. Formally, assuming that 2 is invertible in R, one goes from a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ over R to a symmetric R-bilinear form $(\ , \ )_f$ on R^2 as follows

$$(\overline{u}, \overline{v})_f = \frac{1}{4}(f(\overline{u} + \overline{v}) - f(\overline{u} - \overline{v})).$$

If $\overline{u} = (x_1, y_1)$ and $\overline{v} = (x_2, y_2)$, then

$$(\overline{u}, \overline{v})_f = \frac{1}{4}(f(x_1 + x_2, y_1 + y_2) - f(x_1 - x_2, y_1 - y_2)) = ax_1x_2 + cy_1y_2 + \frac{1}{2}b(x_1y_2 + x_2y_1).$$

This is clearly R-bilinear and symmetric.

Conversely, one can go back from an R-bilinear form $(\ ,\ )_*$ on R^2 to a quadratic form f by

$$f(x,y) = (x\underline{e}_1 + y\underline{e}_2, x\underline{e}_1 + y\underline{e}_2)_* = x^2(\underline{e}_1,\underline{e}_1)_* + 2xy(\underline{e}_1,\underline{e}_2)_* + y^2(\underline{e}_2,\underline{e}_2)_*$$

where $\underline{e}_1 = (1,0)$ and $\underline{e}_2 = (0,1)$. One readily calculates that

$$(\ ,\ )_f = \frac{1}{4}(\ ,\ )_*,$$

for $(\underline{e}_1,\underline{e}_1)_f = \frac{1}{4}(\underline{e}_1,\underline{e}_1)_*$, with similar computations on the other basis elements of R^2.

Now we have the usual notion of orthogonal complement $V^\perp$ for an R-subspace V of a quadratic R-space U. Cassels deals with the case of a field. We need also the case where $R = \mathcal{M}_p$ and $U = \mathcal{M}_p^2$, and we sketch the required changes.

Let f be a quadratic form over $\mathcal{M}_p$, and $(\ ,\ )_f$ the bilinear form associated to f.

Lemma 2.10 *($p \neq 2$) Let $\overline{b} \in \mathcal{M}_p^2$ be primitive, $f(\overline{b}) \neq 0$, and $v_p(f(\overline{b})) = min\{v_p(f(\overline{\beta})) : \overline{\beta} \in \mathcal{M}_p^2\}$. If $V =< \overline{b} >$ then $\mathcal{M}_p^2 = V \oplus V^\perp$.*

Proof: The following equalities and inequality hold

$$v_p((\overline{b},\overline{\beta})_f) = v_p\left(\frac{1}{4}(f(\overline{b}+\overline{\beta}) - f(\overline{b}-\overline{\beta}))\right) = v_p(f(\overline{b}+\overline{\beta}) - f(\overline{b}-\overline{\beta})) \geq v_p(f(\overline{b}) = v_p((\overline{b},\overline{b})_f).$$

The inequality implies that $(\overline{b},\overline{b})_f$ divides $(\overline{b},\overline{\beta})_f$ in $\mathcal{M}_p$ for all $\overline{\beta}$. By Lemma 2.7 there is $\overline{c} \in \mathcal{M}_p^2$ such that $\mathcal{M}_p = V \oplus < \overline{c} >$, and $(\overline{b},\overline{b})_f$ divides $(\overline{b},\overline{c})_f$ in $\mathcal{M}_p$. Let $\lambda \in \mathcal{M}_p$ such that

$$(\overline{b},\overline{c})_f = \lambda(\overline{b},\overline{b})_f = (\overline{b},\lambda\overline{b})_f.$$

It follows that $\overline{c} - \lambda\overline{b} \in V^\perp$, and it is easy to prove that $\mathcal{M}_p = V \oplus < \overline{c} - \lambda\overline{b} >$. Simple calculations show that $V^\perp =< \overline{c} - \lambda\overline{b} >$, hence the proof is completed. □

Following Cassels' (see page 113) we now consider the symmetry defined over $\mathcal{K}_p^h$ for $p \neq 2$

$$\tau_{\overline{b}} : \overline{x} \mapsto \overline{x} - \frac{2(\overline{b},\overline{x})_f}{f(\overline{b})}\overline{b}$$

where $(\cdot,\cdot)_f$ is the inner product associated to f, $f(\overline{b}) \neq 0$ and $2(\overline{b},\overline{x})_f = f(\overline{b}+\overline{x}) - f(\overline{b}) - f(\overline{x})$. It is immediate to verify that $\tau_{\overline{b}}(\overline{b}) = -\overline{b}$, and $\tau_{\overline{b}}(\overline{c}) = \overline{c}$ if $(\overline{b},\overline{c})_f = 0$.

As in the classical case $\tau_{\overline{b}}$ is a $\mathcal{K}_p^h$-automorphism of f, i.e. the coefficients of $\tau_{\overline{b}}$ are in $\mathcal{K}_p^h$ and $f(\tau_{\overline{b}}(\overline{u})) = f(\overline{u})$ for all $\overline{u} \in \mathcal{K}_p^h$.

Lemma 2.11 *($p \neq 2$) If $\overline{b} \in \mathcal{K}_p^h$ and $v_p(f(\overline{b})) = min\{v_p(f(\overline{a})) : \overline{a} \in \mathcal{M}_p^2\}$ then $\tau_{\overline{b}}$ is a $\mathcal{M}_p$-automorphism of f.*

Proof: The proof is formal as in [C] Lemma 3.2 of Chapter 8. It uses that $\tau_{\overline{b}}$ is of order 2, and that $v_p(2(\overline{b},\overline{u})_f) \geq v_p(f(\overline{b}))$. □

Notice that $\tau_{\overline{b}}$ is a $\mathcal{M}_p$-automorph of f with $det(\tau_{\overline{b}}) = -1$.

Lemma 2.12 *($p \neq 2$) Suppose $\overline{a}_1, \overline{a}_2 \in \mathcal{M}_p^2$ satisfy $f(\overline{a}_1) = f(\overline{a}_2)$, and $v_p(f(\overline{a}_1)) = v_p(f(\overline{a}_2)) = min\{v_p(f(\overline{a})) : \overline{a} \in \mathcal{M}_p^2\}$. Then there is an integral automorph σ of f such that $\sigma(\overline{a}_1) = \overline{a}_2$.*

Proof: The proof is formal as in [C] Lemma 3.3 of Chapter 8, and needs only algebraic calculations. □

Note. By inspection the proof gives σ as either $\tau_{\overline{b}}$ for $\overline{b} = \overline{a}_1 - \overline{a}_2$ or as $\tau_{\overline{b}}\tau_{\overline{a}_1}$ for $\overline{b} = \overline{a}_1 + \overline{a}_2$, so σ is the product of at most two symmetries.

Corollary 2.13 *($p \neq 2$) Let σ be any integral automorph of f. Then σ is the product of at most four automorphs $\tau_{\overline{b}}$ with $\overline{b}$ integral.*

Proof: Let $\overline{a_1}$ be such that $v_p(f(\overline{a_1})) = min\{v_p(f(\overline{a})) : \overline{a} \in \mathcal{M}_p^2\}$, and let $\overline{a_2} = \sigma(\overline{a_1})$. Lemma 2.12 implies the existence of an integral automorph σ_1 of f such that $\sigma_1(\overline{a_1}) = \overline{a_2}$, and because of the Note, σ_1 is a product of at most two $\tau_{\overline{b}}$ with $\overline{b}$ integral. Let $V =< \overline{a_1} >$, and consider the decomposition of $\mathcal{M}_p = V \oplus V^{\perp}$ as in Lemma 2.10. Let $\rho = \sigma_1^{-1}\sigma$, we have $\rho(\overline{a_1}) = \overline{a_1}$. Since ρ respects the associated $(\cdot,\cdot)_f$, ρ is an autoisometry of $V^{\perp}$, a $\mathcal{M}_p$-module of dimension 1. Let $V^{\perp} =< \overline{d} >$. Then $\rho(\overline{d}) = u\overline{d}$ where u is a unit, and $f(\overline{d}) = f(\rho(\overline{d}))$ in $V^{\perp}$. Lemma 2.12 applied to $V^{\perp}$ implies $\rho = \tau_{\overline{d}-u\overline{d}}$ or $\rho = \tau_{\overline{d}+u\overline{d}}\tau_{\overline{d}}$ on $V^{\perp}$. An easy calculation shows that both $\tau_{\overline{d}-u\overline{d}}$ and $\tau_{\overline{d}+u\overline{d}}\tau_{\overline{d}}$ fix $\overline{a_1}$, and hence $\rho = \tau_{\overline{d}-u\overline{d}}$ or $\rho = \tau_{\overline{d}+u\overline{d}}\tau_{\overline{d}}$ over $\mathcal{M}_p^2$. Then $\sigma = \sigma_1\rho$, and so we get that any integral automorph σ of f is the product of at most four $\tau_{\overline{b}}$ for $\overline{b}$ integral. □

Corollary 2.14 *($p \neq 2$) Let f be an integral and primitive form. If the determinant of f is a unit in $\mathcal{M}_p$ then any integral automorph σ of f is a product of $\tau_{\overline{b}}$'s where $\overline{b}$ is integral and $f(\overline{b})$ is a unit in $\mathcal{M}_p$.*

Proof: The proof proceeds as in the previous lemma. Simple calculations give the existence of $\overline{a_1} \in \mathcal{M}_p^2$ such that $v_p(f(\overline{a_1})) = 0$. If we know that there is a $\overline{d}$ in $< \overline{a_1} >^{\perp}$ (with respect to $(\cdot,\cdot)_f$) with $f(\overline{d})$ a unit in $\mathcal{M}_p$, then the proof of the preceding lemma gives the integral vectors $\overline{b}$'s with $f(\overline{b})$'s units in $\mathcal{M}_p$.

In general it is easy to see that there is a matrix T over $\mathcal{M}_p$ with determinant a unit, so that

$$f\left(T\left(\begin{array}{c} x \\ y \end{array}\right)\right)$$

is one of the forms x^2+y^2, $x^2+\gamma y^2$, $\gamma(x^2+y^2)$, where $v_p(\gamma)=0$, and γ is not a square. For each of these $g(\overline{x})=f(T(\overline{x}))$ we have $g(1,0)$ is a unit, so let $\overline{a_1}=(1,0)$. It is clear that $(0,1)\in<\overline{a_1}>^{\perp}$ with respect to $(\cdot,\cdot)_g$, and $g(0,1)$ is a unit. The result is then true for g.

Now let σ be an $\mathcal{M}_p$-automorph of f, so $f(\sigma\overline{x})=f(\overline{x})$. Thus

$$g(T^{-1}\sigma T(\overline{x}))=f(TT^{-1}\sigma T(\overline{x}))=f(\sigma T(\overline{x}))=f(T(\overline{x}))=g(\overline{x}),$$

so $T^{-1}\sigma T$ is an $\mathcal{M}_p$-automorph of g. Hence from our observation early in the proof, $T^{-1}\sigma T=\tau_{\overline{b_1}}\ldots\tau_{\overline{b_j}}$ with $j\leq 4$, where $\overline{b_i}$'s are in $\mathcal{M}_p^2$ and $g(\overline{b_i})$'s are units in $\mathcal{M}_p$ (and the symmetries τ's are with respect to $(\cdot,\cdot)_g$). Thus

$$\sigma=T(\tau_{\overline{b_1}}\ldots\tau_{\overline{b_j}})T^{-1}=(T\tau_{\overline{b_1}}T^{-1})T\ldots T^{-1}(T\tau_{\overline{b_j}}T^{-1}).$$

Since

$$(\overline{w_1},\overline{w_2})_g=\frac{1}{4}(g(\overline{w_1}+\overline{w_2})-g(\overline{w_1}-\overline{w_2}))=\frac{1}{4}(f(T\overline{w_1}+T\overline{w_2})-f(T\overline{w_1}-T\overline{w_2}))=(T\overline{w_1},T\overline{w_2})_f,$$

we have $T\tau_{\overline{b_i}}=\tau_{T\overline{b_i}}T$ with τ's in the right hand side with respect to $(\cdot,\cdot)_f$. We then get $\sigma=\tau_{T\overline{b_1}}\ldots\tau_{T\overline{b_j}}$, with $j\leq 4$ and $f(T\overline{b_i})=g(\overline{b_i})$, so $f(T\overline{b_i})$'s are units in $\mathcal{M}_p$. □

We first show that any quadratic form over $\mathcal{M}_p$ is $\mathcal{M}_p$-equivalent to a canonical form. We need the following

Lemma 2.15 *($p\neq 2$) Let u_1,u_2 be units in $\mathcal{M}_p$. Then $u_1x^2+u_2y^2$ is $\mathcal{M}_p$-equivalent to $x^2+u_1u_2y^2$.*

Proof: Using that the squares have index 2 in $\mathbb{F}_p^*$ the equation

$$u_1x^2+u_2y^2\equiv 1(\text{mod } p) \qquad (2)$$

can be reduced to a norm type equation, a generalization of a Pell equation. Using the same techniques of [D3] we can show that (2) has a solution in $\mathbb{F}_p$. This solution can be lifted up to a solution (a_1,a_2) in $\mathcal{M}_p$, using Hensel's lemma which is available in $\mathcal{K}_p^h$. Since (a_1,a_2) is primitive we can extend it to a basis (a_1,a_2), (b_1,b_2) where b_1 is divisible by u_2 and b_2 is divisible by u_1. In this basis the form is written as $x^2+u_1u_2y^2$. □

We have now all the ingredients to prove the following classification theorem for quadratic forms over $\mathcal{M}_p$, for $p\neq 2$.

Theorem 2.16 *($p \neq 2$) Let r_p be a quadratic non-residue modulo p with $v_p(r_p) = 0$. Then every non-singular quadratic form f over $\mathcal{K}_p^h$ is $\mathcal{M}_p$-equivalent to one of the following forms*

1. $p^e(x^2 + y^2)$
2. $p^e(x^2 + r_p y^2)$
3. $p^{e_1}x^2 + p^{e_2}y^2$
4. $p^{e_1}r_p x^2 + p^{e_2}r_p y^2$
5. $p^{e_1}x^2 + p^{e_2}r_p y^2$
6. $p^{e_1}r_p x^2 + p^{e_2}y^2$

with $e_1 < e_2$, and $e, e_1, e_2 \in \mathbb{B}_p$. Moreover, none of the forms are $\mathcal{M}_p$-equivalent.

Proof: From the choice of r_p we have that r_p is invertible. By Lemma 2.11 f is $\mathcal{M}_p$-equivalent to a diagonal form $g(x, y) = a_1x^2 + a_2y^2$ with $v_p(a_1) \leq v_p(a_2)$. If $v_p(a_1) = v_p(a_2) = e$ for some $e \in \mathcal{M}$, then by Lemma 2.15 g is $\mathcal{M}_p$-equivalent to $p^e(x^2 + uy^2)$ where u is invertible. Then either $u = v^2$ or $u = r_p v^2$ for some unit v and we get the first two forms. We argue in an analogous way if $e_1 = v_p(a_1) < v_p(a_2) = e_2$ since now g is $\mathcal{M}_p$-equivalent to $p^{e_1}u_1x^2 + p^{e_2}u_2y^2$ with u_1, u_2 invertible, and we have the other four cases according to u_i, $i = 1, 2$ being a square or not.

It is left as an exercise to show that no two distinct forms among 1) to 6) are $\mathcal{M}_p$-equivalent. □

An analogous classification theorem holds for $p = 2$.

Theorem 2.17 *Every regular quadratic form over $\mathcal{K}_2^h$ is $\mathcal{M}_2$-equivalent to a standard finite sum of forms of the following type:*

1. $2^e x^2$, $2^e(3x^2)$, $2^e(5x^2)$, $2^e(7x^2)$
2. $2^e(2xy)$
3. $2^e(2x^2 + 2xy2y^2)$

with $e \in \mathbb{B}_2$

Proof: We are only interested at the case of $n = 2$ of Lemma 4.1 of [C]. The proof there gives an absolute standard finite bound on the length of the sum of forms of a certain type, and in our case this is 2. If we replace 2^e in the proof of [C] by $v_2(a) = e$ for some $a \in \mathcal{M}_2$, then we can express the theorem in a first-order statement in the language of valued fields, true in $\mathbb{Q}_2$, so true also in $\mathcal{K}_2^h$ thanks to Theorem 2.2. To go back from elements of value e to 2^e is then a triviality. □

2.4 Approximations theorems

Our next goal is to show that the $\mathcal{M}_p$-equivalence relation on quadratic forms over $\mathcal{M}$ is uniformly Δ_0-definable.

Cassels in his Lemma 5.1 of Chapter 8 proves that if f is a form of discriminant D and g is a form whose coefficients are equivalent to those of f modulo $p^{v_p(D)+1}$ for $p \neq 2$, or modulo $p^{v_p(D)+3}$ for $p = 2$, then the two forms are $\mathbb{Z}_p$-equivalent. We will show that the same holds in our context. We need the following result.

Lemma 2.18 *Let A be a 2×2 matrix over $\mathcal{M}_p$. If A is invertible modulo p then A is invertible also in $\mathcal{M}_p$.*

Proof: Let $\overline{A}$ be the reduced matrix modulo p. By hypothesis there is a 2×2 matrix $\overline{B}$ modulo p such that $det(\overline{AB}) = 1$. Pull back $\overline{B}$ to $\mathcal{M}_p$, and get a matrix B such that $det(AB) = u$ with u invertible in $\mathcal{M}_p$ and $u \equiv 1(\text{mod } p)$. A simple calculation shows that $u^{-1}B$ is the inverse of A in $\mathcal{M}_p$. □

Lemma 2.19 *Let $f(x, y) = a_1x^2 + a_2xy + a_3y^2$ and $g(x, y) = c_1x^2 + c_2xy + c_3y^2$ be two forms over $\mathcal{M}_p$, and let D be the discriminant of f.*

(i) If $p \neq 2$ and $c_i \equiv a_i(mod\ p^{v_p(D)+1})$ for $i = 1, 2, 3$ then f and g are $\mathcal{M}_p$-equivalent.

(ii) If $p = 2$ and $c_i \equiv a_i(mod\ 2^{v_2(D)+3})$ for $i = 1, 2, 3$ then f and g are $\mathcal{M}_p$-equivalent.

Proof: (i) If we replace $c_i \equiv a_i(\text{mod } p^{v_p(D)+1})$ by $v_p(c_i - a_i) \geq v_p(D) + 1$ for $i = 1, 2, 3$ then the statement of the theorem is first-order in the many sorted language, and hence from Lemma 5.1 of Chapter 8 of [C] and Theorem 2.3 in this paper, it is true also for $\mathcal{M}_p$ with standard p's. In the case of p non standard we notice that the statement is true for $\mathbb{F}_p((t))$ and from elementary equivalence of $\mathcal{K}_p^h$ and $\mathbb{F}_p((t))$ we have the result.

(ii) Replacing $c_i \equiv a_i(\text{mod } 2^{v_2(D)+3})$ by $v_2(c_i - a_i) \geq v_2(D) + 3$ for $i = 1, 2, 3$ we get again the result from the elementary equivalence of $\mathcal{K}_2^h$ and $\mathbb{Q}_2$, and of $\mathcal{M}_2$ with $\mathbb{Z}_2$. □

This lemma says that if two forms have coefficients p-adically close in $\mathcal{M}$ then actually the forms are $\mathcal{M}_p$-equivalent.

Theorem 2.20 *Let f be a quadratic form over $\mathcal{M}_p$ of discriminant $D \neq 0$. A form g is $\mathcal{M}_p$-equivalent to f iff g is equivalent to f modulo $p^{v_p(D)+1}$ for $p \neq 2$, and modulo $p^{v_p(D)+3}$ for $p = 2$.*

Proof: ($\Rightarrow$) Let $p \neq 2$. If T is an invertible matrix in $\mathcal{M}_p$ giving the equivalence between f and g then by reducing T modulo $p^{v_p(D)+1}$ we get f and g equivalent modulo $p^{v_p(D)+1}$. For $p = 2$ it follows from standard case and Theorem 2.2.

($\Leftarrow$) Let $p \neq 2$. If f and g are equivalent modulo $p^{v_p(D)+1}$ then there is an invertible matrix S modulo $p^{v_p(D)+1}$ giving $F = S^t G S$. So the coefficients of F and $S^t G S$ are equivalent modulo $p^{v_p(D)+1}$, and by Lemma 2.19 we have that F and $S^t G S$ are $\mathcal{M}_p$-equivalent, and so also F and G are $\mathcal{M}_p$-equivalent. Analogously for $p = 2$. As usual, Ax-Kochen-Ershov takes care of case $p = 2$. $\square$

Corollary 2.21 *$\mathcal{M}_p$-equivalence is Δ_0-definable uniformly in p.*

We emphasize the difference between the global analysis of equivalence of quadratic forms in [DM2] where we showed that equivalence being Δ_0-definable was strictly connected to solvability of a Pell equation.

3 The nature of $\mathcal{G}_{D,p}$

Let $\mathcal{G}_{D,p}$ denote the set of equivalence classes of forms of discriminant $D \neq 0$ under $\mathcal{M}_p$-equivalence.

Lemma 3.1 *Let p be a prime different from 2*

1) If $p \not| D$ then $\mathcal{G}_{D,p}$ is trivial.

2) If $p|D$ then $\mathcal{G}_{D,p}$ has exactly two elements represented by $x^2 - \frac{D}{4}y^2$ and $rx^2 - r^{-1}Dy^2$, where r is a unit not in $((\mathcal{K}_p^h)^*)^2$.

Proof: 1) Suppose $p \not| D$. From Theorem 2.16 the only way to get $v_p(D) = 0$ is when the form is one of the following type

$$x^2 + y^2 \qquad \text{or} \qquad x^2 + r_p y^2 \tag{3}$$

where r_p is a quadratic non-residue modulo p. If f and g are $\mathcal{M}_p$-equivalent then $det(f)$ and $det(g)$ are in the same coset modulo the squares of $(\mathcal{K}_p^h)^*$. For if f and g correspond to the matrices A and B then $B = C^T A C$ for some invertible matrix C in $\mathcal{M}_p$. Thus if f is $\mathcal{M}_p$-equivalent to some form h then $v_p(det(h)) = 0$.

The two forms in (3) cannot be $\mathcal{M}_p$-equivalent since they have discriminants in different classes modulo the squares of $(\mathcal{K}_p^h)^*$. Hence $\mathcal{G}_{D,p}$ has only one element corresponding to the class of $x^2 + y^2$ if D is a square modulo p, and to the class of $x^2 + r_p y^2$ if D is not a square modulo p.

2) Let $\delta = v_p(D)$. Again from Theorem 2.16 we have this time that $2e = \delta$ or $e_1 + e_2 = \delta$, and primitivity gives the only possibility $e_1 = 0$ and $e_2 = \delta$. Thus the forms can only be one of the following

$$x^2 + p^\delta y^2, \quad x^2 + p^\delta r_p y^2, \quad r_p x^2 + p^\delta y^2, \quad r_p x^2 + p^\delta r_p y^2$$

where r_p is a quadratic non-residue modulo p. Again, considerations of cosets modulo the squares of $(\mathcal{K}_p^h)^*$ show that at most two classes can occur, given D. The forms

$$x^2 - \frac{D}{4}y^2 \quad \text{and} \quad r_p x^2 - r_p^{-1}\frac{D}{4}y^2$$

are not $\mathcal{M}_p$-equivalent, since $x^2 - \frac{D}{4}y^2$ represent 1, and $r_px^2 - r_p^{-1}\frac{D}{4}y^2$ does not. For if $r_px^2 - r_p^{-1}\frac{D}{4}y^2 = 1$, $v_p(x) = 0$ and $v_p(r_p^{-1}\frac{D}{4}y^2) > 0$, so r_p would be a square modulo p, a contradiction. □

Now we consider the most delicate case, $p = 2$.

Lemma 3.2 *a) If* $2 \not| D$ *then* $\mathcal{G}_{D,2}$ *is trivial.*

b) If $2|D$ *then* $D = 4d$ *where* $d \in \mathcal{M}^2$*, and there are the following cases:*

i)$_b$ $d \equiv 1(mod\ 4)$ *then* $\mathcal{G}_{D,2}$ *is trivial.*

ii)$_b$ $d \equiv -1(mod\ 4)$ *then* $\mathcal{G}_{D,2}$ *is a two element group.*

iii)$_b$ $2|d$ *but* $2^3 \not| d$ *then* $\mathcal{G}_{D,2}$ *is a two element group.*

iv)$_b$ $2^3|d$ *then* $\mathcal{G}_{D,2}$ *is a four element group.*

In each case we have Δ_0 *in* D *explicit reprentatives of* $\mathcal{G}_{D,2}$.

Proof: Note that in this lemma D need only be in $\mathcal{M}_p$. The explicit description of the elements of $\mathcal{G}_{D,2}$, and their multiplicative relations is a set of first-order sentences true in $\mathbb{Z}_2$, so true in $\mathcal{M}_2$ by [AK1], [AK2], [AK3] and [E]. Notice that in the cases when $\mathcal{G}_{D,2}$ is trivial a representative of the unique class is $x^2 - \frac{D}{4}y^2$. In the other cases the representatives come from the list

$$f_u(x, y) = ux^2 - u^{-1}dy^2 \qquad \text{where } u = 1, 3, 5, 7,$$

and $f_u \sim f_v$ if and only if f_u represents v modulo 8. □

We have already shown in Section 2.1 that if $p = \infty$ then $\mathcal{G}_{D,\infty}$ is trivial if $D > 0$ with representative $x^2 - \frac{D}{4}y^2$, and $\mathcal{G}_{D,\infty}$ has only two elements if $D < 0$ with representative $x^2 - \frac{D}{4}y^2$ and $-x^2 + \frac{D}{4}y^2$.

Notice that we have not yet discussed the group structure over $\mathcal{G}_{D,\infty}$ and $\mathcal{G}_{D,p}$. Once we do it, Cassels' clause that in (iv) $\mathcal{G}_{D,2}$ is not cyclic will follow too by appealing again to the results of Ax, Kochen and Ershov.

Cassels considers the following product of finite groups

$$\prod_{\substack{p=\infty \\ p|D}} \mathcal{G}_{D,p}.$$

In $I\Delta_0$ there are many restrictions on *counting* cardinalities of sets, because of the non totality of the exponential function (see [Pa]). In [Wo] it was shown that for every $m \in \mathcal{M}$ where $\mathcal{M}$ is a model of $I\Delta_0$ it is possible to count in a Δ_0-way the number of prime divisors of m. For any given D we can give a Δ_0-meaning in $\mathcal{M}$ to the product of the finite local groups over the primes p dividing D including $p = \infty$. We have given above canonical representatives (Δ_0 in D and p, uniformly) with coefficients in $\mathcal{M}$ (we should interpret r_p^{-1} as the least positive element of $\mathcal{M}$ representing this class modulo p). In all cases the elements are in diagonal form and by using a polynomial pairing function we give, Δ_0 uniformly in D and p, a linear order of the above elements of $\mathcal{G}_{D,p}$ (including $p = \infty$). Let $n_{D,p}$ be the cardinality of $\mathcal{G}_{D,p}$, where $1 \leq n_{D,p} \leq 4$. Then the function

$$(D, p) \mapsto n_{D,p}$$

is uniformly Δ_0-definable in D and p. Now the size $c(D)$ of

$$\prod_{\substack{p=\infty \\ p|D}} \mathcal{G}_{D,p}$$

is roughly

$$c(D) = \prod_{\substack{p=\infty \\ p|D}} n_{D,p} \leq 2^3 2^k$$

where k is the number of primes which divide D, and $k \leq [log_2 D]$. So,

$$c(D) \leq 8(2^{[log_2 D]}) \leq 8D.$$

It is now routine, using our Δ_0-definitions for the local equivalence, to define a Δ_0-map σ from the set of primitive binary forms over $\mathcal{M}$ (coded by their triples of coefficients) to $c(D)$ so that

$$\sigma(f) = \sigma(g) \text{ if and only if } f \text{ and } g \text{ are } \mathcal{M}_p\text{-equivalent.}$$

We have the set

$$\prod_{\substack{p=\infty \\ p|D}} \mathcal{G}_{D,p}$$

lying on an initial segment of $\mathcal{M}$.

3.1 The group structure on $\prod \mathcal{G}_{D,p}$

Recall from [DM2] the development in $I\Delta_0 + \Omega_1$ of the group $\mathcal{G}_D$. We now develop, uniformly in p and ∞, the group structures on $\mathcal{G}_{D,p}$ generalizing those in Chapter 14 of [C].

$\mathcal{G}_D$ is the quotient of the set of primitive forms over $\mathcal{M}$ by the relation of proper $\mathcal{M}$-equivalence. The latter relation is not in general Δ_0 (see [DM2]), though is obviously definable. Thus $\mathcal{G}_D$ is not an easy set to understand in terms of counting in $\mathcal{M}$. The group operation on $\mathcal{G}_D$ is a little closer to Δ_0, in the sense that there is a Δ_0 operation on the set of primitive $\mathcal{M}$-forms which descends (through proper $\mathcal{M}$-equivalence) to the group operation on $\mathcal{G}_D$. That operation is defined (first-order in $\mathcal{M}$) in the last section of [DM2], and the reader may find it useful to have that paper to hand.

For the local versions we initially work in $\mathcal{M}_p$ (p a prime or $p = \infty$), with the set of primitive $\mathcal{M}_p$-forms. The notion of primitive is clear when p is a prime, and all forms are primitive when $p = \infty$. The relation of equivalence to be considered on the $\mathcal{M}_p$-forms is simply $\mathcal{M}_p$-equivalence, for p prime and unimodular equivalence for $p = \infty$.

If one now looks at Section 7 of [DM2], one sees that Lemmas 7.1 and 7.3 go through verbatim, with $\sim$ interpreted as the equivalence given above. The Definitions 7.3 (concordance) and 7.4 (composition of primitive concordant forms of discriminant D) make good sense. ($\mathcal{M}_p$, for p prime, is a valuation ring, and $\mathcal{M}_\infty$ is a field.)

Lemma 7.5 of [DM2] refers to proper equivalence in the original setting, but this can be dropped in the case of p a prime, and replaced by unimodularity for $p = \infty$.

The same considerations apply to Lemma 7.6. Now exactly as for $\mathcal{M}$ we get an abelian group structure on $\mathcal{G}_{D,p}$. Moreover, the natural map

$$\mathcal{G}_D \longrightarrow \mathcal{G}_{D,p}$$

induced by the inclusion $\mathcal{M} \to \mathcal{M}_p$ is evidently a group homomorphism.

Note. One should not forget that in the p-adic case $\mathcal{M}$-equivalent forms need not have the same discriminant. In general their discriminants will differ by the square of a unit. Of course unimodular equivalence preserves discriminants.

For future reference we need to put a Δ_0-group structure on $\prod_{p,\infty} \mathcal{G}_{D,p}$. The essential point is that for prime p the groups $G_{D,p}$ are uniformly Δ_0 in D, p.

For $p \neq 2$, the structure of $G_{D,p}$ is completely explicit (see Lemma 3.1). Their units are given in a Δ_0-way. It is a Δ_0-condition that the group is trivial, and when it is not the other element is given.

For $p = 2$, the structure of the groups is slightly more complicated (see Lemma 3.2). But the argument in the proof of Lemma 3.2 gives the Δ_0-structure.

From Section 2.1 it is immediate to understand the group structure on $\mathcal{G}_{D,\infty}$. In both cases $D > 0$ and $D < 0$ the class of $x^2 - \frac{D}{4}y^2$ is the unit of the group. Thus it is clear that the structure on $\mathcal{G}_{D,\infty}$ is uniformly Δ_0 in D.

Acknowledgments. The authors would like to thank the Hausdorff Research Institute for Mathematics in Bonn where this work was completed in the spring 2009 during the trimester in Diophantine equations.

References

[AK1] Ax J. and Kochen S., Diophantine problems over local fields. I. American Journal of Mathematics, 87 (1965), 605–630.

[AK2] Ax J. and Kochen S., Diophantine problems over local fields II, in American Journal of Mathematics , 87 (1965), pp. 631648

[AK3] Ax J. and Kochen S., Diophantine problems over local fields. III. Decidable fields. Annals of Mathematics, (2) 83 (1966), 437–456.

[B] Basarab S.A., Relative elimination of quantifiers for Henselian valued fields. Annals of Pure and Applied Logic 53 (1991), pp. 51-74

[BI] Berarducci A. and Intrigila B., Combinatorial principles in elementary number theory, Annals of Pure and Applied Logic, vol. 55 (1991), pp. 35-50.

[C] Cassels J.W.S., Rational Quadratic Forms, Academic Press, 1978.

[D1] D'Aquino P., Local behaviour of Chebyshev theorem in models of $I\Delta_0$, Journal of Symbolic Logic, vol.57, (1992), n. 1, pp. 12-27.

[D2] D'Aquino P., Pell equations and exponentiation in fragments of arithmetic, Annals of Pure and Applied Logic, vol. 77 (1996), pp.1-34.

[D3] D'Aquino P., Solving Pell equations locally in models of $I\Delta_0$, Journal of Symbolic Logic, vol. 63, (1998), n. 2, pp. 402-410.

[DM1] D'Aquino P. and A. Macintyre, Non standard finite fields over $I\Delta_0 + \Omega_1$, in Israel Journal of Mathematics 117, (2000), pp. 311-333.

[DM2] D'Aquino P. and A. Macintyre, Quadratic forms in models of $I\Delta_0 + \Omega_1$, I, Annals of Pure and Applied Logic, 148, (2007), pp. 31-48.

[E] Ershov Yu.L., On the elementary theory of maximal normed fields, in Soviet Math. Dokl. , 6 (1965) pp. 1390-1393. (In Russian)

[G] Gauss C. F., Disquisitiones Arithmeticae, English edition, Springer, 1986.

[H] Hungerford W.H., Algebra, Springer, 1974.

[K] Kitaoka Y., Arithmetic of Quadratic Forms, Cambridge University Press, 1993.

[M] Macintyre A., Residue fields of models of P. Logic, methodology and philosophy of science, VI (1979), Stud. Logic Found. Math., 104, pp. 193–206, North-Holland, 1982.

[Pa] Parikh R., Existence and feasibility in arithmetic, Journal of Symbolic Logic, vol. 36 (1976), no. 3, pp. 494-508.

[PWW] Paris J., Wilkie A. and Woods A., Provability of the Pigeonhole Principle and the existence of infinitely many primes, Journal of Symbolic Logic 53, no. 4, (1988), pp. 1235-1244.

[Wo] Woods A., Some problems in logic and number theory and their connections, Ph.D. thesis, Manchester University, 1981.