HIROSHIMA MATH. J.
43 (2013), 371–411

On integral quadratic forms having commensurable groups of automorphisms

Dedicated to Prof. José Manuel Rodríguez Sanjurjo in his 60th birthday

José María MONTESINOS-AMILIBIA

(Received February 21, 2012)
(Revised March 15, 2013)

ABSTRACT. We introduce two notions of equivalence for rational quadratic forms. Two n-ary rational quadratic forms are *commensurable* if they possess commensurable groups of automorphisms up to isometry. Two n-ary rational quadratic forms F and G are *projectivelly equivalent* if there are nonzero rational numbers r and s such that rF and sG are rationally equivalent. It is shown that if F and G have Sylvester signature $\{-,+,+,\dots,+\}$ then F and G are commensurable if and only if they are projectivelly equivalent. The main objective of this paper is to obtain a complete system of (computable) numerical invariants of rational n-ary quadratic forms up to projective equivalence. These invariants are a variation of Conway's p-excesses. Here the cases n odd and n even are surprisingly different. The paper ends with some examples.

1. Introduction

In the classical theory of rational quadratic forms, two n-ary, rational quadratic forms F and G are rationally equivalent if there is an $n \times n$ rational matrix T such that $T^tFT = G$. In particular, if T is integral and $\det T = \pm 1$, F and G are said to be integrally equivalent. This is a purely arithmetic definition. I want to introduce a "geometric" definition of equivalence.

Say that two n-ary rational quadratic forms F and G are "equivalent" if "they possess the same groups of automorphisms up to isometry". That is, there is a real $n \times n$ matrix T such that $T^tFT = G$ and $T^{-1}(\mathrm{Aut}\, F)T = \mathrm{Aut}\, G$, where $\mathrm{Aut}\, F$ denotes the subgroup of $\mathrm{GL}(n, \mathbf{Z})$ consisting of those matrices U such that $U^tFU = F$. In geometric terms, that means that, if F is hyperbolic, the two hyperbolic orbifolds, obtained as quotients of hyperbolic n-space $\mathbf{H}^n$ under the actions of $\mathrm{Aut}\, F$ and $\mathrm{Aut}\, G$, are isometric.

Supported by grant MTM2009-07030.

2010 *Mathematics Subject Classification*. 11E04, 11E20, 57M25, 57M50, 57M60.

Key words and phrases. Integral quadratic form, knot, link, hyperbolic manifold, volume, automorph, commensurability class.

Now, this definition is too strict for various reasons, which explain why the theory of arithmetic groups does not insist in Aut F and Aut G being equal up to isometry, but relax this condition to asking if Aut F and Aut G are commensurable up to isometry. That is, we will say that two n-ary, rational quadratic forms F and G are *commensurable* (see Definition 1) if there is a real $n \times n$ matrix T such that $T^t F T = \pm G$ and $T^{-1} H_F T = H_G$, where $H_F \leq \text{Aut } F$ and $H_G \leq \text{Aut } G$ are finite index subgroups. In geometric terms, that means that, if F is hyperbolic, the two hyperbolic orbifolds, obtained as quotients of $\mathbf{H}^n$ under the actions of Aut F and Aut G, have (up to isometry) a common finite orbifold-covering.

One reason why I introduce the above definition is that the restriction of the interesting automorphs of a rational quadratic form F to the ones with integral entries is somehow technical or artificial. Indeed, there are abundant examples of supergroups G of Aut F made up of real automorphs that still act properly and discontinuously on, say, $\mathbf{H}^3$. (For instance there is a supergroup of $\text{Aut}(\langle -1,1,4,4\rangle)$, made up of real automorphs of $\langle -1,1,4,4\rangle$, which is isomorphic to the Picard's group $\text{Aut}(\langle -1,1,1,1\rangle)$.) Necessarily then, the index of Aut F in G is finite, since $\mathbf{H}^3/G$ has finite volume. A second reason is that when one changes from one model of $\mathbf{H}^3$ to another one (say the upper half-space model), very often Aut F is sent to a group of homographies and antihomographies of $\mathbf{C}P^1$ whose entries are not algebraic integers. In these cases, Aut F possesses a finite index subgroup that is transfered to one with algebraic integer entries.

Note that the definition of commensurable, rational quadratic forms F and G is relevant only when the groups of automorphisms of the two forms are infinite (when F and G are hyperbolic, for instance). Two n-ary, *definite*, rational quadratic forms are always commensurable.

Clearly F and λF, $\lambda \in \mathbf{Q}\backslash\{0\}$, are commensurable. Moreover, any two, rationally equivalent, rational quadratic forms F and G are commensurable ([6]). This suggest to call two n-ary, rational quadratic forms F and G *projectivelly equivalent* (see Definition 2), denoted $F \overset{P}{\sim} G$, if there are nonzero rational numbers r and s, such that rF and sG are rationally equivalent.

This definition is the main topic in this paper. The relevance of it lies in the following theorem:

"If two n-ary, rational quadratic forms F and G are hyperbolic then F and G are commensurable if and only if they are projectivelly equivalent".

The main objective of this paper is to obtain (computable) numerical invariants of n-ary, rational quadratic forms, such that $F \overset{P}{\sim} G$ if and only if the invariants for F and G coincide. These invariants are variations of Conway's p-excesses ([7]). Here the cases n odd and n even are surprisingly different.

In sections 6 and 7, I offer a number of computed examples and I ask some questions.

In section 8, I give a geometric construction of an arithmetic group consisting of automorphs of an integral quadratic form, and I offer a historical perspective of rational quadratic forms, from a geometrical point of view, for the benefit of the more algebraically oriented reader.

In conclusion, I think that the definition $F \overset{P}{\sim} G$ corresponds perfectly to the geometric classification of quadratic forms. It would be very interesting to generalize this theory to quadratic forms over arbitrary number fields.

For the reader's sake, after some generalities on quadratic forms and the proof of the above theorem, I will review the invariants of rational equivalence (*Conway's p-excesses*), discovered by Conway ([7]), before using them to obtain the projective classification of quadratic forms.

I am very grateful to my brother Angel Montesinos-Amilibia. His help has been invaluable to understand the geometry of integral quadratic forms. Specially for having written a program that enabled me to perform a number of computations. I am also very much indebted to the editor of this journal for the many suggestions that made the paper more readable.

2. Quadratic forms: preliminaires

A general reference is [6] (see also [10] and [7]).

Let x be the column vector with coordinates $x_1, \ldots, x_n$ and F a symmetric $n \times n$ matrix. Then the expression

$$f(x) = x^t F x$$

is called the *n-ary quadratic form* with matrix F. We will make use also of the associated *bilinear form*

$$f(x, y) = x^t F y.$$

The *adjoint* of F, denoted Adj F, is the quadratic form $\det(F)F^{-1}$.

We call F a *rational quadratic form* if F is *rational*, that is, the matrix entries of F are rational numbers and the determinant of F is nonzero. We call F an *integral quadratic form* if F is *integral*, that is, the matrix entries of F are rational integers (i.e. if it is *classical integral* (Gauss), or integral as a symmetric bilinear form) and the determinant of F is nonzero.

We shall say that two n-ary, rational quadratic forms F and G are **Q**-*equivalent*, or that they are in the same **Q**-*class*, and write $F \overset{\mathbf{Q}}{\sim} G$, if there is an $n \times n$ rational matrix M such that $M^t F M = G$. In particular, if M is integral and $\det M = \pm 1$, we shall say that F and G are **Z**-*equivalent*, or that they are in the same **Z**-*class*, and write $F \overset{\mathbf{Z}}{\sim} G$.

An $n \times n$ matrix U with real entries is a *real automorph* of the rational quadratic form F if $U^t F U = F$. Then $\det U = \pm 1$. The real automorph U is *proper* if $\det U = +1$, *improper* if $\det U = -1$.

The group $O_{\mathbf{R}}(F)$ of real automorphs of F is called the *real orthogonal group* of the form F.

A real automorph U with integer entries is called an *automorph* (proper or improper) of F. The set of automorphs of F is the *automorphism group* $\mathrm{Aut}(F)$ of F. The subset $\mathrm{Aut}^+(F)$ of proper automorphs is the *proper automorphism group* of F. The group $\mathrm{Aut}^+(F)$ has index 1 or 2 in $\mathrm{Aut}(F)$.

We shall say that a rational quadratic form is *hyperbolic* if it is equivalent to $\{-,+,+,\ldots,+\}$ or $\{+,-,-,\ldots,-\}$ over the real field $\mathbf{R}$.

3. Commensurable and projectively equivalent forms

We want to investigate the relationship between the following two definitions.

DEFINITION 1. Two n-ary, rational quadratic forms F and G are *commensurable* if there is a real $n \times n$ matrix T such that $T^t F T = \pm G$ and $T^{-1} H_F T = H_G$, where $H_F \leq \mathrm{Aut}\, F$ and $H_G \leq \mathrm{Aut}\, G$ are finite index subgroups.

DEFINITION 2. Two n-ary, rational quadratic forms F and G are *projectivelly equivalent*, denoted $F \overset{P}{\sim} G$, if there are nonzero rational numbers r and s such that $rF \overset{\mathbf{Q}}{\sim} sG$.

This is an equivalence relation because

$$rF \overset{\mathbf{Q}}{\sim} sG, \qquad tG \overset{\mathbf{Q}}{\sim} uH \Rightarrow rtF \overset{\mathbf{Q}}{\sim} stG \overset{\mathbf{Q}}{\sim} suH$$

Of course $F \overset{\mathbf{Q}}{\sim} G$ implies $F \overset{P}{\sim} G$, but not viceversa.

PROPOSITION 1. *Let F and G be two n-ary rational quadratic forms. The following statements are equivalent.*

(1) $F \overset{P}{\sim} G$.

(2) *There is a nonzero, square-free integer a such that $F \overset{\mathbf{Q}}{\sim} aG$.*

(3) *There is a nonzero integer a and an integral matrix T such that $T^t F T = aG$.*

PROOF. If $F \overset{P}{\sim} G$ there are nonzero rational numbers r and s, such that $rF \overset{\mathbf{Q}}{\sim} sG$. Then

$$(T/m)^t (a/p) F (T/m) = (b/q) G,$$

where T is an integral matrix and m, a, b, p, q are non-zero integers. Hence $T^t(aqF)T = m^2 bpG$. Hence $F \overset{P}{\sim} G$ if and only if there are nonzero in-

tegers, a and b, and an integral matrix T, such that $T^t(bF)T = aG$. Then $T^t(bbF)T = baG$. Hence $(bT)^tF(bT) = baG$, which proves that (1) implies (3). Next, assume (3). Then if $a = p^2b$, where b is an square-free integer, we can write

$$(T/p)^tF(T/p) = bG.$$

Hence (3) implies (2). Obviously, (2) implies (1).

For instance:

COROLLARY 1. *Every integral quadratic form F is projectively equivalent to its adjoint* Adj F.

PROOF. Denote, for brevity, Adj F by G. Then

$$G^tFG = GFG = \det(F)^2F^{-1}FF^{-1} = \det(F)^2F^{-1} = \det(F)G.$$

As a non-trivial example of commensurable forms, note the following:

THEOREM 1. *Every integral quadratic form F is commensurable to its adjoint $G =$ Adj F. Even more, there is a real $n \times n$ matrix M such that $M^tFM = \pm G$ and M^{-1} Aut $FM =$ Aut G.*

PROOF. Let d denote the absolute value of $\det F$ and ε its sign $+1$ or -1. Let M be $\sqrt{d}F^{-1}$. Then $M^tFM = \varepsilon G$ and

$$M^{-1} \text{ Aut } FM = \text{Aut } G.$$

Indeed, let U be an automorph of F. Then $FUF^{-1} = (U^t)^{-1}$. That is, $M^{-1}UM = (U^{-1})^t$, which is integral (and therefore, an automorph of G). Conversely, Let V be an automorph of G. Then

$$GVG^{-1} = F^{-1}VF = (V^t)^{-1}.$$

Hence

$$MVM^{-1} = F^{-1}VF = (V^t)^{-1},$$

which is integral (and therefore, an automorph of F).

REMARK 1. It follows that the group Aut(Adj F) is the set of the transposes of the elements of Aut(F).

Note that *any rational quadratic form is projectivelly equivalent to an integral form*.

In [6] it is proved that **Q**-equivalent, integral forms are commensurable. Next, we show that, more generally, two rational forms are commensurable if they are projectively equivalent.

Proposition 2. *Let F and G be two n-ary, projectively equivalent, rational quadratic forms. Then F and G are commensurable. In fact, if T is an integral matrix and a is a nonzero integer such that $T^tFT = aG$, then $M^tFM = \varepsilon G$ and there is a finite index subgroup H of $\mathrm{Aut}(F)$ such that $M^{-1}HM = K$, where $M = T/\sqrt{|a|}$, $\varepsilon = \frac{a}{|a|}$ and $K \leq \mathrm{Aut}(G)$ is a finite index subgroup.*

Proof. Let m be the determinant of T. Then m is a rational integer. If $m = \pm 1$, then F and aG are $\mathbf{Z}$-equivalent and, therefore,

$$T^{-1}\,\mathrm{Aut}(F)T = \mathrm{Aut}(aG) = \mathrm{Aut}(G).$$

Assume $m \neq \pm 1$. Define the homomorphism ω, from $\mathrm{Aut}(F)$ into $\mathrm{GL}(n, \mathbf{Z}/m\mathbf{Z})$, by $\omega(U) = U \mod m$. Let

$$H := \{Q \in \mathrm{Aut}(F) : T^{-1}QT \in \mathrm{Aut}(G)\}.$$

Then $\ker \omega$ is a subgroup of H. In fact, if $U \in \ker \omega$, then $U = I \mod m$. That is, $U = I + mA$, where A is integral. Then

$$T^{-1}UT = T^{-1}(I + mA)T = I + mT^{-1}AT$$

is integral, because $mT^{-1} = \mathrm{Adj}(T)$ is integral. Hence $T^{-1}UT$ is an automorph of G, because

$$(T^{-1}UT)^t aG(T^{-1}UT) = T^tU^tFUT = T^tFT = aG.$$

Therefore $U \in H$. The group H is a finite index subgroup of $\mathrm{Aut}(F)$, because it contains $\ker \omega$ and $\mathrm{GL}(n, \mathbf{Z}/m\mathbf{Z})$ is a finite group. Now, $K := T^{-1}HT$ is a finite index subgroup of $\mathrm{Aut}(G)$, because it contains $\ker \eta$, where the homomorphism η, from $\mathrm{Aut}(G)$ into $\mathrm{GL}(n, \mathbf{Z}/m\mathbf{Z})$, is defined by $\eta(V) = V \mod m$. In fact, $K = \{P \in \mathrm{Aut}(G) : TPT^{-1} \in \mathrm{Aut}(F)\}$, and similar arguments as above apply. Defining $M = T/\sqrt{|a|}$, $\varepsilon = \frac{a}{|a|}$ we have

$$M^tFM = T^t(F/|a|)T = \varepsilon G$$

and

$$M^{-1}HM = (\sqrt{|a|}T^{-1})H(T/\sqrt{|a|}) = T^{-1}HT = K.$$

This concludes the proof.

Next, we will show that the converse is true for hyperbolic forms. It is probably true for all indefinite forms, $n \geq 3$.

Lemma 1. *Let h be an element of $\mathrm{GL}(n, \mathbf{R})$ with an eigenvalue λ such that the kernel of $h - \lambda I$ is a 1-dimensional (h-invariant) vector subspace V of $\mathbf{R}^n$. If z belongs to the centralizer of h in $\mathrm{GL}(n, \mathbf{R})$, then $z(V) = V$.*

PROOF. Assume that z belongs to the centralizer of h in $\mathrm{GL}(n,\mathbf{R})$ and let $v \in V$. Then $hz(v) = zh(v) = \lambda z(v)$. Hence $z(v) \in V$. Hence $z(V) = V$.

Recall that a *projective reference* in $\mathbf{R}^n$ is a set of 1-dimensional vector subspaces $\{V_1, \ldots, V_n; V_{n+1}\}$ such that $V_1, \ldots, V_n$ are linearly independent, and V_{n+1} is in general position with respect to $V_1, \ldots, V_n$. It is well known that an element of $\mathrm{GL}(n,\mathbf{R})$ fixes a projective reference if and only if it is of the form λI, where λ is a real number and I is the identity matrix.

Let F be an n-ary, hyperbolic quadratic form, $n \geq 3$. It represents a quadric Q_F in the real projective space $\mathbf{R}P^{n-1}$ that bounds a topological ball. The interior of this ball is a model (*Klein model*) of hyperbolic $(n-1)$-space $\mathbf{H}_F^{n-1}$, and its group of isometries is the orthogonal group (isomorphic to $\mathrm{O}(n,1)$) of the given quadratic form. A *hyperbolic (or loxodromic) isometry* is an orientation-preserving isometry with two fixed points "at infinity" (that is, on Q_F). Other orientation-preserving isometries are either *elliptic* (fixing a point inside Q_F) or parabolic (with just one fixed point "at infinity").

PROPOSITION 3. *Let F be an n-ary, hyperbolic, quadratic form, $n \geq 3$, and let h be a hyperbolic isometry of F. If $z \in \mathrm{GL}(n,\mathbf{R})$ commutes with h then $z(x) = x$ and $z(y) = y$, where x and y are the fixed points of h at infinity (in Q_F).*

PROOF. The isometry h is a hyperbolic isometry, that is, a hyperbolic translation along a geodesic γ_h of $(n-1)$-hyperbolic space $\mathbf{H}_F^{n-1}$ whose endpoints x and y are at infinity. That is, there is a 2-dimensional h invariant subspace W_h which is the direct sum of two 1-dimensional h-invariant subspaces V_h and V_h' with real eigenvalues $\lambda_h < 1$ and $\lambda_h' > 1$ such that $\lambda_h \lambda_h' = 1$; and there is a $(n-2)$-dimensional h-invariant subspace W_h' (the "polar" of xy) such that F, restricted to it, is definite, and, therefore, h, restricted to W_h', has no real eigenvalues different from ± 1. Hence the kernel of $h - \lambda_h I$ is equal to the 1-dimensional (h-invariant) vector subspace V_h of $\mathbf{R}^n$, and similarly, the kernel of $h - \lambda_h' I$ is equal to the 1-dimensional (h-invariant) vector subspace V_h'. Since z commutes with h, $z(x) = x$ and $z(y) = y$, by Lemma 1. This completes the proof.

COROLLARY 2. *Let F be an n-ary, hyperbolic, rational quadratic form, $n \geq 3$, and let H be a finite index subgroup of $\mathrm{Aut}(F)$. Then the centralizer of H in $\mathrm{GL}(n,\mathbf{R})$ is the set of diagonal matrices λI, where λ is a real number and I is the identity matrix.*

PROOF. The orbifold $\mathbf{H}_F^{n-1}/\mathrm{Aut}(F)$ is complete and of finite volume ([5]). It has a finite orbifold covering $\mathbf{H}_F^{n-1}/H$ that shares these two properties. Hence the limit set of H is Q_F ([15, Theorem 12.2.13]). This limit set is

the adherence of the set of fixed points of the hyperbolic isometries in H ([15, Theorem 12.2.4]). Hence this set contains a projective reference. By Proposition 3, z fixes the points of this reference. Hence $z = \lambda I$, where λ is a real number and I is the identity matrix. This concludes the proof (compare [15, Corollary 2 to Theorem 12.2.6]).

Proposition 4. *If F and G are two binary, hyperbolic, commensurable rational quadratic forms, then they are projectively equivalent.*

Proof. Here F and G are P-equivalent to diagonal matrices $\langle 1, -\Delta_F\rangle$ and $\langle 1, -\Delta_G\rangle$, respectively, where Δ_F and Δ_G are square-free positive integers. (In fact, F is $\mathbf{Q}$-equivalent to a diagonal matrix, say $\langle a, b\rangle$, which is P-equivalent to $a\langle a, b\rangle = \langle a^2, ab\rangle$, which is $\mathbf{Q}$-equivalent to $\langle 1, -\Delta_F\rangle$.) It is known (see [10]) that $\mathrm{Aut}^+(\langle 1, -\Delta_F\rangle)$ is isomorphic to $C_2 \times C_\infty$, where the cyclic group C_2 is generated by the automorph $\langle -1, -1\rangle$, and the infinite cyclic group C_∞ is generated by the automorph

$$\begin{bmatrix} p_0 & q_0\Delta_F \\ q_0 & p_0 \end{bmatrix},$$

where p_0 and q_0 are integers such that (i) $p_0^2 - q_0^2\Delta_F = 1$; (ii) $q_0 > 0$, $p_0 > 1$; and (iii) p_0 is minimal among the pairs (p, q) satisfying the conditions analogous to (i) and (ii). Since F and G are commensurable, $\langle 1, -\Delta_F\rangle$ and $\langle 1, -\Delta_G\rangle$ are commensurable, by Proposition 2. Thus, there is a real matrix such that

$$M^t\langle 1, -\Delta_F\rangle M = \pm\langle 1, -\Delta_G\rangle$$

and

$$M^{-1}\begin{bmatrix} p_1 & q_1\Delta_F \\ q_1 & p_1 \end{bmatrix} M = \begin{bmatrix} p_2 & q_2\Delta_G \\ q_2 & p_2 \end{bmatrix}$$

where q_1 and q_2 are non-zero integers. Since the eigenvalues $(p_1 - q_1\sqrt{\Delta_F}$, $p_1 + q_1\sqrt{\Delta_F})$ and $(p_2 - q_2\sqrt{\Delta_G}, p_2 + q_2\sqrt{\Delta_G})$ coincide, and Δ_F and Δ_G are square-free, it follows that $\Delta_F = \Delta_G$. This concludes the proof.

Theorem 2. *If F and G are n-ary, hyperbolic, rational quadratic forms, $n \geq 3$, such that there is a real $n \times n$ matrix M such that $M^tFM = \pm G$, and there is a finite index subgroup H of $\mathrm{Aut}(F)$ such that $M^{-1}HM$ is a finite index subgroup K of $\mathrm{Aut}(G)$, then $M = \sqrt{r}T$, where T is an integral matrix and r is a positive rational number. Hence F and G are projectively equivalent.*

Proof. Denote by $h_1, \ldots, h_m$ a system of generators of H ([5]). Then $k_i = M^{-1}h_iM$, $i = 1, \ldots, m$ generate K. The h_i and k_j are integral matrices. Denote by $X = (x_{ij})$ an $n \times n$ matrix with entries the n^2 variables x_{ij}. Then

$h_iX = Xk_i$, $i = 1, \ldots, m$ is a homogeneous system of mn^2 linear equations, with integer coefficients, in the variables x_{ij}. Denote by S the integral matrix of the system. This is an $mn^2 \times n^2$ integral matrix. Its rank is less than n^2 since $X = M$ is a solution. Let $X = T$ be another solution. Then $T^{-1}h_iT = k_i = M^{-1}h_iM$. Hence $(MT^{-1})h_i(TM^{-1}) = h_i$. Since h_i generate the subgroup of finite index H of $\mathrm{Aut}(F)$, MT^{-1} belongs to the centralizer of H in $\mathrm{GL}(n, \mathbf{R})$. Then, according to Corollary 2, $M = \lambda T$, where λ is a real number. Therefore, the rank of S is exactly $n^2 - 1$. Then, since S is integral, the solutions are of the form λN where N is an $n \times n$ integral matrix. In particular, $M = \rho N$ for some real number ρ that we can assume positive (otherwise change the sign of N). Then $M^tFM = \rho^2 N^tFN = \pm G$. Therefore ρ^2 is a positive rational number r and therefore $M = \rho N = \sqrt{r}N$, as we wanted to prove. Hence F and G are projectively equivalent. This concludes the proof.

We group together these results:

THEOREM 3. *Let F and G be two n-ary, hyperbolic, rational quadratic forms. Then they are commensurable if and only if they are projectively equivalent.*

EXAMPLE 1. *The diagonal, ternary, integral quadratic forms $F = \langle 1, 1, -8\rangle$ and $G = \langle -1, 1, 1\rangle$, with determinants -8 and -1 respectively, are commensurable. Even more,* $\mathrm{Aut}\, F$ *and* $\mathrm{Aut}\, G$ *both act in the hyperbolic plane* $\mathbf{H}^2$ *and the quotient hyperbolic orbifolds coincide, which implies that there is an isometry of* $\mathbf{H}^2$ *sending F to G and* $\mathrm{Aut}\, F$ *to* $\mathrm{Aut}\, G$. *This common hyperbolic orbifold is the hyperbolic asymptotic triangle t with angles $0, \frac{\pi}{2}, \frac{\pi}{4}$. We can be more specific. The reflections*

$$g_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \qquad g_2 = \langle 1, 1, -1\rangle, \qquad g_3 = \begin{bmatrix} 3 & 2 & -2 \\ -2 & -1 & 2 \\ 2 & 2 & -1 \end{bmatrix}$$

in the edges of t generate $\mathrm{Aut}(G)$. *Let M be $\frac{1}{\sqrt{2}}N$, where*

$$N = \begin{bmatrix} -4 & 0 & 12 \\ 3 & 1 & -8 \\ -3 & 1 & 8 \end{bmatrix}.$$

Then $M^tGM = F$ and, moreover, $M^{-1}g_iM$, $i = 1, 2, 3$, are the matrices

$$\langle 1, -1, 1\rangle, \begin{bmatrix} -8 & 3 & 24 \\ 3 & 0 & -8 \\ -3 & 1 & 9 \end{bmatrix}, \begin{bmatrix} -3 & 0 & 8 \\ 0 & 1 & 0 \\ -1 & 0 & 3 \end{bmatrix},$$

which generate $\mathrm{Aut}(F)$. *Since the forms* F *and* G *are commensurable, they must be projectively equivalent. In fact* $N^tGN = 2F$.

4. The Conway's invariants of Q-equivalence

Since $F \overset{P}{\sim} G$ if and only if there is a nonzero square-free integer a such that $F \overset{Q}{\sim} aG$, one expects that a system of invariants for projective equivalence will be obtain from known systems of invariants for rational equivalence. We will prove this expectation through the invariants introduced by J. Conway in [7]. For the sake of the reader, we start explaining carefully these invariants.

4.1. The Jacobi Symbol after Conway. Following Conway [7], it will be convenient to consider -1 as a prime number.

If S is a finite set, denote by Σ_S the group of bijections (or permutations) of S, and recall that a given permutation $\sigma \in \Sigma_S$ is called *even* (resp. *odd*) if, when written as a product of (non necessarily disjoint) cycles, the number of even cycles, in the product, is even (resp. odd). This defines a homomorphism $\mathscr{A} : \Sigma_S \to C_2$, where C_k is the cyclic group of order k, by setting $\mathscr{A}(\sigma) = 0$ if and only if σ is even.

Let a, n be two coprime integers, n odd (in particular, since -1 is prime, a and n are not both negative). Multiplication of $\mathbf{Z}$ by a defines a permutation σ_n^a of the set of classes of $\mathbf{Z} \bmod n$. Define the *Conway symbol* $\left[\frac{a}{n}\right]$ as $4\mathscr{A}(\sigma_n^a) \bmod 8$. That is:

$$\left[\frac{a}{n}\right] = \begin{cases} 0 \\ 4 \end{cases} \bmod 8, \text{ if } \sigma_n^a \text{ is } \begin{cases} \text{even} \\ \text{odd} \end{cases} \tag{4.1}$$

Then, by definition:

$$\left[\frac{a}{n}\right] = \left[\frac{a}{-n}\right] \tag{4.2}$$

(of course, formula (4.2) implies $a > 0$), and

$$\left[\frac{a + kn}{n}\right] = \left[\frac{a}{n}\right], \qquad k \in \mathbf{Z} \tag{4.3}$$

Moreover

$$\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right] + \left[\frac{b}{n}\right], \tag{4.4}$$

since $\mathscr{A}(\sigma_n^a.\sigma_n^b) = \mathscr{A}(\sigma_n^a) + \mathscr{A}(\sigma_n^b)$.

For example, $n = 11$, $a = -3$. Distribute the classes of $\mathbf{Z} \bmod 11$ into 5 negative classes, 1 zero class and 5 possitive classes as follows (5 is the integer part of $11/2$):

$$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$$

Then

$$\sigma_{11}^{-3} = \begin{pmatrix} -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & -2 & -5 & 3 & 0 & -3 & 5 & 2 & -1 & -4 \end{pmatrix}, \qquad (*)$$

which is the product of the even permutation:

$$\begin{pmatrix} -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 \\ -4 & -1 & -2 & -5 & -3 & 0 & 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

with the transpositions $(3, -3)$, $(1, -1)$ and $(4, -4)$. Therefore σ_{11}^{-3} is odd. Hence $\left[\frac{-3}{11}\right] = 4 \mod 8$.

In general $\left[\frac{a}{n}\right]$ *is* $4s_n^a \bmod 8$, *where* s_n^a *is the number of negative classes in the lower half right part of (*).*

For instance

$$\left[\frac{-1}{n}\right] = \begin{cases} 0 \\ 4 \end{cases} \mod 8 \text{ if } \begin{cases} n = 1 \mod 4 \\ n = -1 \mod 4 \end{cases}, \qquad (4.5)$$

because s_n^{-1} is the integer part of $n/2$, which is even if and only if $n = 1 \mod 4$.

It follows from (4.3) and (4.4) that

$$\left[\frac{a}{n}\right] = 0 \qquad \text{if } a = x^2 \mod n \qquad (4.6)$$

The converse is not true ($\left[\frac{-1}{9}\right] = 0$, but -1 is not a square mod 9). However, the converse is true if n is prime. In this case, it is well known that there is a *primitive root* $\bmod n$. This is an integer p, $0 < p < n$, such that σ_n^p is an $(n-1)$ cycle. Since this cycle is an even cycle, the permutation σ_n^p is odd. Hence $\left[\frac{p}{n}\right] = 4 \mod 8$. Then

$$\left[\frac{p^k}{n}\right] = k\left[\frac{p}{n}\right]$$

is zero if and only if k is even (4.4). (Note that the powers of p run over all nonzero classes of $\mathbf{Z} \bmod n$.) Hence, if $\left[\frac{a}{n}\right] = 0$, then $a = p^{2k} \mod n$. Hence a is a square $\bmod n$.

Thus, *if* n *is prime then* $\left[\frac{a}{n}\right] = 0$ *if and only if* a *is a square* $\bmod n$.

Remark 2. Jacobi defined $\left[\frac{a}{n}\right]$ for coprime a and n, n prime, to be 0 if and only if a is a square mod n, and extended this definition to $n = p_1 \dots p_k$, where $p_1, \dots, p_k$ are prime numbers, by setting

$$\left[\frac{a}{p_1 \dots p_k}\right] = \left[\frac{a}{p_1}\right] + \dots + \left[\frac{a}{p_k}\right] \tag{4.7}$$

Zolotarev gave meaning to $\left[\frac{a}{n}\right]$, for a general n, by defining $\left[\frac{a}{n}\right]$ as in the present section. Therefore, to show that Jacobi and Zolotarev definitions agree, (4.7) has to be proved. This follows from (4.4) and the so called Quadratic Reciprocity Law, to be proved later.

Next, we prove that

$$\left[\frac{a}{n}\right] = \left[\frac{a}{n + 4ka}\right], \qquad k \in \mathbf{Z}. \tag{4.8}$$

Consider the case $n = 11$, $a = 3$. Recall that $\left[\frac{3}{11}\right] = 4s_{11}^3 \mod 8$, where s_{11}^3 is the number of negative classes in the second row of

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ & & & \times 3 \downarrow & & \\ 0 & 3 & 6 & 9 & 12 & 15 \end{pmatrix}$$

The classes $6 = -5 \mod 11$ and $9 = -2 \mod 11$ are negative. Hence $s_{11}^3 = 2$. Hence $\left[\frac{3}{11}\right] = 0 \mod 8$.

Analyzing this process closely, we see that we divide the interval

$$3\left[0, \frac{11}{2}\right] = \left[0, 3\frac{11}{2}\right] = [0, 16.5]$$

into $a = 3$ parts

$$\left[0, \frac{11}{2}\right], \left[\frac{11}{2}, 2\frac{11}{2}\right], \left[2\frac{11}{2}, 3\frac{11}{2}\right]$$

to which we assign alternate signs $+, -, +$. A given class mod 11, falling in one particular interval, has the sign assigned to this interval. For instance, the classes 0, 3 fall in the first interval (+ sign); 6, 9 fall in the second (− sign); and 12, 15 fall in the third (+ sign).

Now, if we pass from $n = 11$, $a = 3$ to $n = 11 + 2 \times 3 = 17$, $a = 3$, the three intervals are now

$$\left[0, \frac{17}{2}\right], \left[\frac{17}{2}, 2\frac{17}{2}\right], \left[2\frac{17}{2}, 3\frac{17}{2}\right].$$

That is,

$$\left[0, \frac{11}{2}+3\right], \left[\frac{11}{2}+3, 2\frac{11}{2}+6\right], \left[2\frac{11}{2}+6, 3\frac{11}{2}+9\right],$$

and, now, in each interval fits one more class:

$$\{0,3,6\} \in \left[0, \frac{11}{2}+3\right]$$

$$\{9,12,15\} \in \left[\frac{11}{2}+3, 2\frac{11}{2}+6\right]$$

$$\{18,21,24\} \in \left[\frac{11}{2}+3, 2\frac{11}{2}+6\right].$$

Iterating this process once more (passing from $n=11$, $a=3$ to $n=11+4\times 3=23$, $a=3$), each one of the three intervals will contain *two* more classes than in case $n=11$, $a=3$. Thus, the number of negative classes mod 2 does not change: $s_{11}^3 = s_{11+4\times 3}^3 = s_{23}^3 \bmod 2$. Therefore, in general

$$\left[\frac{a}{n}\right] = \left[\frac{a}{n+4ka}\right], \qquad k \in \mathbf{Z},$$

as we wanted to prove.

For instance,

$$\left[\frac{2}{n}\right] = \left[\frac{2}{n+8k}\right],$$

and there are only two possibilities: $n = \pm 1 \bmod 8$ or $n = \pm 3 \bmod 8$. In the first case

$$\left[\frac{2}{n}\right] = \left[\frac{2}{\pm 1}\right] = \left[\frac{2}{1}\right] = 0 \bmod 8,$$

while in the second case

$$\left[\frac{2}{n}\right] = \left[\frac{2}{\pm 3}\right] = \left[\frac{2}{3}\right] = 4 \bmod 8,$$

because 2 is not a square mod 3. Therefore,

$$\left[\frac{2}{n}\right] = \begin{cases} 0 \\ 4 \end{cases} \bmod 8 \text{ if } \begin{cases} n = \pm 1 \bmod 8 \\ n = \pm 3 \bmod 8 \end{cases} \tag{4.9}$$

Theorem 4 (*Quadratic Reciprocity Law*). *Let m and n be two coprime odd integers. Then*

$$\left[\frac{m}{n}\right] + \left[\frac{n}{m}\right] = (m-1)(n-1) \mod 8$$

Proof. Case 1. $m = 1 \mod 4,\ n = -1 \mod 4$

Then $m + n = 0 \mod 4$. Write $m + n = 4a$. Assume $n > m$. Then $n > 0$ because m and n are coprime (in particular they cannot be both negative). Then $a > 0$. Then

$$\left[\frac{m}{n}\right] = \left[\frac{4a-n}{n}\right] \overset{(4.3)}{=} \left[\frac{4a}{n}\right] \overset{(4.4)}{=} \left[\frac{a}{n}\right] \overset{(4.2)}{=} \left[\frac{a}{-n}\right]$$
$$\overset{(4.8)}{=} \left[\frac{a}{-n+4a}\right] = \left[\frac{a}{m}\right] \overset{(4.4)}{=} \left[\frac{4a}{m}\right] \overset{(4.3)}{=} \left[\frac{4a-m}{m}\right] = \left[\frac{n}{m}\right] \qquad (**)$$

Case 2. $m = 1 \mod 4,\ n = 1 \mod 4$

One of m, n is > 0. Assume $m > 0$. Then

$$\left[\frac{m}{n}\right] \overset{(4.2)}{=} \left[\frac{m}{-n}\right] \overset{(**)}{=} \left[\frac{-n}{m}\right] \overset{(4.4)}{=} \left[\frac{-1}{m}\right] + \left[\frac{n}{m}\right] \overset{(4.5)}{=} \left[\frac{n}{m}\right]$$

Case 3. $m = -1 \mod 4,\ n = -1 \mod 4$

One of m, n is > 0. Assume $m > 0$. Then

$$\left[\frac{m}{n}\right] \overset{(4.2)}{=} \left[\frac{m}{-n}\right] \overset{(**)}{=} \left[\frac{-n}{m}\right] \overset{(4.4)}{=} \left[\frac{-1}{m}\right] + \left[\frac{n}{m}\right] \overset{(4.5)}{=} 4 + \left[\frac{n}{m}\right],$$

which is congruent with $\left[\frac{n}{m}\right] + (m-1)(n-1) \mod 8$. This completes the proof.

From this theorem, (4.7) follows. For instance, let a, p, q be odd integers. Then, from (4.4) and the Quadratic Reciprocity Law, we obtain:

$$\left[\frac{a}{pq}\right] = \left[\frac{a}{p}\right] + \left[\frac{a}{q}\right] + (pq + p + q - 3)(a-1) = \left[\frac{a}{p}\right] + \left[\frac{a}{q}\right] \mod 8,$$

because $a - 1 = 0 \mod 2$ and $(pq + p + q - 3) = 0 \mod 4$.

4.2. The Conway's *p*-excesses. Following Conway [7], we will define a set of invariants (*Conway's p-excesses*) that classify rational quadratic forms up to **Q**-equivalence.

Since a rational quadratic form is **Q**-equivalent to a diagonal integral one, the p-excesses will be defined for these forms.

Start with an 1-ary such form $F = \langle a \rangle$. For each prime number p (-1 included), write $F = \langle p^x A \rangle$, where p and A are coprime (if $p = -1$, $A > 0$), and define the p-excess $e_p(F)$ as follows:

Case 1: $p = -1$. Define

$$e_{-1}(F) = p^x - 1 = \begin{cases} 0 \\ -2 \end{cases} \text{ if } \begin{cases} a > 0 \\ a < 0 \end{cases}$$

Case 2: $p = 2$. Define

$$e_2(F) = (1 - A) + \left[\frac{2^x}{A}\right] \mod 8 = \begin{cases} 1 - A \\ (1 - A) + \left[\frac{2}{A}\right] \end{cases} \mod 8, \text{ if } \begin{cases} x \text{ even} \\ x \text{ odd} \end{cases}$$

Case 3: p an odd prime. Define

$$e_p(F) = (p^x - 1) + \left[\frac{A}{p^x}\right] \mod 8 = \begin{cases} 0 \\ (p - 1) + \left[\frac{A}{p}\right] \end{cases} \mod 8, \text{ if } \begin{cases} x \text{ even} \\ x \text{ odd} \end{cases}$$

Next, let $F = \langle a_1, \ldots, a_m \rangle$ be an m-ary, diagonal, integral quadratic form. Define the Conway's p-excess as

$$e_p(F) = \sum_{i=1}^{m} e_p(\langle a_i \rangle) \mod 8$$

Among all the p-excesses, -1 included, the following *Global Relation* holds:

$$\sum_p e_p(F) = 0 \mod 8$$

The *reduced determinant* of an m-ary, diagonal, integral quadratic form F, written $\det_n F$, is obtained from $\det F = p_1^{x_1} \ldots p_k^{x_k}$ by reducing mod 2 the exponents $x_1, \ldots, x_k$ of the different primes $p_1, \ldots, p_k$ (-1 included) entering in the decomposition of $\det F$ in product of powers of prime numbers. It is well defined up to **Q**-equivalence.

The Conway's p-excesses and the reduced determinant of an m-ary, rational quadratic form F are, by definition, the Conway's p-excesses and the reduced determinant of any m-ary, diagonal, integral quadratic form F_1, **Q**-equivalent to F.

THEOREM 5 (*Conway's formulation of the Hasse-Minkowsky Theorem*). *Two m-ary, rational quadratic forms are rationally equivalent if and only if they have the same reduced determinants and the same Conway's p-excesses.*

We will call these invariants the *Conway invariants* $c(F)$ of F, and we will codify them as follows:

$$c(F) = [\Delta, (-1, e_{-1}(F)), (2, e_2(F)), (p_1, e_{p_1}(F)), \ldots, (p_k, e_{p_k}(F))],$$

where $\Delta = \det_n F$, and $p_1, \ldots, p_k$ are the odd primes, in increasing order, such that $e_{p_1}(F) \neq 0 \mod 8$. Note that the sequence $p_1, \ldots, p_k$ is finite, because, if an odd prime p fails to divide $\det F$, then there exists a diagonal integral quadratic form F_1, **Q**-equivalent to F, such that $p \nmid \det F_1$ [10] . This implies that $e_p(F) = e_p(F_1) = 0 \mod 8$.

EXAMPLE 2. $F = \langle -1, 7, 7, 7\rangle$, $G = \langle -7, 1, 1, 1\rangle$. *Here* $F \overset{\mathbf{Q}}{\sim} G$, *because*

$$c(F) = [-7, (-1, -2), (2, 0), (7, 2)] = c(G).$$

5. Invariants of projective equivalence

5.1. Binary forms. *The reduced determinant is the only invariant of projective equivalence of a binary, integral quadratic form.*

In fact, assume that two binary, diagonal, integral quadratic forms $F = \langle a_1, a_2\rangle$, $G = \langle b_1, b_2\rangle$ have the same reduced determinant Δ. Then $F \overset{P}{\sim} G$, because

$$\langle a_1, a_2\rangle \overset{P}{\sim} a_1\langle a_1, a_2\rangle \overset{\mathbf{Q}}{\sim} \langle 1, \Delta\rangle$$
$$\langle b_1, b_2\rangle \overset{P}{\sim} b_1\langle b_1, b_2\rangle \overset{\mathbf{Q}}{\sim} \langle 1, \Delta\rangle$$

On the other hand, if F and G are two binary, diagonal, integral quadratic forms such that $F \overset{P}{\sim} G$, then $\det_n F = \det_n G$, by Proposition 1.

5.2. Odd dimensional forms. Let F be an odd dimensional, integral quadratic form. Then, the dimension of F, together with the p-excesses of the integral quadratic form $(\det_n F)F$, constitute a complete system of invariants of projective equivalence:

PROPOSITION 5. *Two n-ary integral quadratic forms F and G, n odd, are projectively equivalent if and only if* $(\det_n F)F$ *and* $(\det_n G)G$ *are rationally equivalent.*

REMARK 3. Note that the reduced determinant of the form $(\det_n F)F$ is 1. From the relation (5.1) below, it follows also that two n-ary integral quadratic forms F and G, n odd, are projectively equivalent if and only if $(\det_n G)F$ and $(\det_n F)G$ are rationally equivalent.

PROOF. Assume $F \overset{P}{\sim} G$. Then $F \overset{\mathbb{Q}}{\sim} aG$, for some nonzero square-free integer a. Then $\det F = r^2 \det(aG)$, where r is a nonzero rational number. Since n is odd, this implies that $\det F = as^2 \det(G)$, where s is a nonzero rational number. Then

$$F \overset{\mathbb{Q}}{\sim} aG \overset{\mathbb{Q}}{\sim} (as^2 \det G \det G)G = (\det F \det G)G \tag{5.1}$$

But $(\det F \det G)G \overset{\mathbb{Q}}{\sim} (\det_n F \det_n G)G$, because $\det F = b^2 \det_n F$, for some integer b. From which it follows that $(\det_n F)F$ and $(\det_n G)G$ are rationally equivalent. Conversely, if $(\det_n F)F$ and $(\det_n G)G$ are rationally equivalent, then F and G are projectively equivalent, by definition.

We deduce the following important result:

COROLLARY 3. *Two n-ary integral quadratic forms F and G, n odd, are projectively equivalent if and only if their adjoints* Adj F *and* Adj G *are rationally equivalent.*

PROOF. Since every integral quadratic form F is projectively equivalent to its adjoint Adj F (Corollary 1), then $F \overset{P}{\sim} G$ if and only if Adj $F \overset{P}{\sim}$ Adj G. And by the above Proposition, Adj $F \overset{P}{\sim}$ Adj G if and only if $\det_n(\text{Adj } F)$ Adj $F \overset{\mathbb{Q}}{\sim} \det_n(\text{Adj } G)$ Adj G. Since the reduced determinants of Adj F and Adj G are 1, the corollary follows.

Therefore, a complete set of projective invariants of an n-ary, n odd, integral quadratic form F is the set of Conway's excesses for every odd prime p (-1 included) of the adjoint form Adj F. Now, if the odd prime $p \neq -1$ fails to divide $\det F$, then $e_p(\text{Adj } F) = 0 \mod 8$. But if p divides $\det F$, then the maximal power of p dividing $\det \text{Adj } F = (\det F)^{n-1}$ is even, and, therefore, $e_p(\text{Adj } F) = 0 \mod 4$ (compare with Proposition 7). Moreover

$$-2(n-1) \leq e_{-1}(\text{Adj } F) \leq 0$$

and $e_{-1}(\text{Adj } F) = 0 \mod 4$. Thus,

THEOREM 6. *A complete system of projective invariants of an n-ary, n odd, integral quadratic form F is $e_{-1}(\text{Adj } F)$, together with the set of odd primes $p > -1$, for which $e_p(\text{Adj } F) \neq 0 \mod 8$.*

A convenient way of offering these invariants is to write $inv_P F = [n; d; S]$, where

$$d = \frac{-e_{-1}(\text{Adj } F)}{4},$$

and where S is the product of the odd primes $p > -1$ for which $e_p(\text{Adj } F) \neq 0 \mod 8$.

Some of the implications of these invariants are studied in the forthcoming paper [14].

For instance, to see if the diagonal ternary forms $F = \langle -1, 1, 7\rangle$ and $G = \langle 1, -1, -3\rangle$ are projectively equivalent, we have to check if their adjoints $F_1 = \langle 7, -7, -1\rangle$ and $G_1 = \langle 3, -3, -1\rangle$ are rationally equivalent. And, indeed, they are, because their Conway invariants coincide:

$$c(F_1) = [1, (-1, -4), (2, 4)] = c(G_1)$$

On the other hand, the forms F and G are not **Q**-equivalent, because

$$c(F) = [-7, (-1, -2), (2, 4), (7, 6)]$$

and

$$c(G) = [3, (-1, -4), (2, 6), (3, 6)]$$

are different.

5.3. Even dimensional forms. The even dimensional case is more difficult than the odd one. Before finding a complete set of invariants, we need a number of definitions and of auxiliary results.

Since every diagonal, integral quadratic form is **Q**-equivalent to a *square-free* one (i.e. one with all its entries square-free), we start this section by repeating the definitions of the Conway's p-excesses when $F = \langle a\rangle$ is square-free:

Case 1: $p = -1$. Define

$$e_{-1}(F) = \begin{cases} 0 \\ -2 \end{cases} \text{ if } \begin{cases} a > 0 \\ a < 0 \end{cases} \tag{5.2}$$

Case 2: $p = 2$. Define

$$e_2(F) = \begin{cases} 1 - a \\ (1 - a/2) + \left[\frac{2}{a/2}\right] \end{cases} \bmod 8, \text{ if } a \text{ is } \begin{cases} \text{odd} \\ \text{even} \end{cases} \tag{5.3}$$

Case 3: p an odd prime. Define

$$e_p(F) = \begin{cases} 0 \\ (p-1) + \left[\frac{a/p}{p}\right] \end{cases} \bmod 8, \text{ if } \begin{cases} p \nmid a \\ p \mid a \end{cases} \tag{5.4}$$

5.3.1. Some definitions. Let F be a diagonal, integral quadratic form of even dimension $2d(F)$. Denote by $n(F)$ the set of odd primes (-1 included) dividing the reduced determinant $\det_n F$ of F (the letter n suggests "no-square").

The number $s(F)$ (resp. $t(F)$) is defined to be 0 if the number of elements $p \in n(F)$ such that $p = -1 \bmod 4$ (resp. $p = \pm 3 \bmod 8$) is even. Otherwise $s(F)$ (resp. $t(F)$) is defined to be 1.

We define another number $o(F)$ with values $\{0,1\}$: $o(F)$ is 0 if and only if $\det_n F$ is odd (the letter o suggests "odd").

If $\varepsilon_+(F)$ (resp. $\varepsilon_-(F)$) is the number of positive (resp. negative) diagonal entries of F, then the *Sylvester signature* of F is defined to be $\varepsilon_+(F) - \varepsilon_-(F)$. Note that $2d(F) = \varepsilon_+(F) + \varepsilon_-(F)$. Therefore, $2d(F)$, together with the Sylvester signature of F, determine $\varepsilon_+(F)$ and $\varepsilon_-(F)$. In these terms, the Conway's -1-excess of F is $e_{-1}(F) = -2\varepsilon_-(F)$. Let $\varepsilon(F)$ denote the smallest of the two numbers $\varepsilon_+(F)$ and $\varepsilon_-(F)$. Then $0 \le \varepsilon(F) \le d(F)$ will be called the *Sylvester partition* of F.

5.3.2. Projective invariants. Let F be a diagonal, integral quadratic form of even dimension $2d(F)$. In the remaining of the section we will prove that the following collection of numbers is a complete set of invariants of projective equivalence among forms of the same even dimension:

(1) The *reduced determinant* $\det_n F$ of F.
(2) The *Sylvester partition* $\varepsilon(F)$ of F.
(3) The 2-*excess* $e_2(F)$ of F, if $\det_n F = (-1)^{d(F)} \bmod 8$. Otherwise, this number $e_2(F)$ is not included among the invariants.
(4) The q-*excess* $e_q(F)$ of F, if $q \notin n(F)$ and $q \neq -1$ is an odd prime such that

$$2(q-1)d(F) + \left[\frac{\det_n F}{q}\right] = 0 \bmod 8$$

Otherwise, this number $e_q(F)$ is not included among the invariants. Note that if $q \nmid \det F$ then $e_q(F) = 0$. Therefore the set of nonzero $e_q(F)$'s is finite.

We call this set of numbers the *projective invariants* $p(F)$ *of* F, and we codify them as follows:

$$p(F) = [\Delta, \varepsilon(F), (2, e_2(F)) \text{ or } -, (q_1, e_{q_1}(F)), \ldots, (q_k, e_{q_k}(F))],$$

where $\Delta = \det_n F$, and the $q_1, \ldots, q_k$ are placed in increasing order, and the list contains only those with $e_q(F) \neq 0 \bmod 8$.

To prove that these numbers constitute, in fact, a complete set of projective invariants, we need some auxiliary results.

5.3.3. Auxiliary propositions.

PROPOSITION 6. *Let F be an integral quadratic form of even dimension $2d(F)$. Then $\det_n F = (-1)^{d(F)} \bmod 8$ if and only if*

$$(o(F), d(F) + s(F), t(F)) = (0,0,0) \bmod 2$$

Proof. By definition, the number $s(F)$ is 0 if the number of elements $p \in n(F)$ such that $p = -1 \mod 4$ is even. Hence $o(F) = 0$ and $s(F) = 0$ if and only if $\det_n F = 1 \mod 4$. Hence $o(F) = 0$ and $s(F) = d(F) \mod 2$ if and only if $\det_n F = (-1)^{d(F)} \mod 4$. On the other hand, the number $t(F)$ is 0 if the number of elements $p \in n(F)$ such that $p = \pm 3 \mod 8$ is even. Hence $o(F) = 0$ and $t(F) = 0$ if and only if $\det_n F = \pm 1 \mod 8$. Finally,

$$(o(F), d(F) + s(F), t(F)) = (0, 0, 0) \mod 2$$

if and only if $\det_n F = (-1)^{d(F)} \mod 8$. This concludes the proof.

Proposition 7. *Let F and G be two diagonal, integral quadratic forms of the same even dimension such that $n(F) = n(G)$. Then*

$$e_p(F) - e_p(G) = 0 \mod 4,$$

for all primes p (-1 included). Moreover, if p is an odd prime such that $p \notin n(F) = n(G)$ then

$$e_p(F) = e_p(G) = 0 \mod 4.$$

Proof. We can assume that F and G are square-free, because any F can be reduced to a $\mathbf{Q}$-equivalent, square-free, diagonal, integral quadratic form. Let p be an odd prime (-1 included). Let p^x (resp. p^y) the maximal power of p dividing $\det F$ (resp. $\det G$). Then $e_p(F) = x(p-1) \mod 4$ and $e_p(G) = y(p-1) \mod 4$. Since $n(F) = n(G)$ then $x = y \mod 2$. Hence

$$e_p(F) - e_p(G) = (x - y)(p - 1) = 0 \mod 4.$$

By the global relation,

$$e_2(F) = -\sum_{p \text{ odd}} e_p(F) \mod 8.$$

Hence

$$e_2(F) - e_2(G) = -\sum_{p \text{ odd}} (e_p(F) - e_p(G)) = 0 \mod 4.$$

If the odd prime $p \notin n(F) = n(G)$, then $x = y = 0 \mod 2$. Hence

$$e_p(F) = x(p-1) = 0 \mod 4$$

and

$$e_p(G) = y(p-1) = 0 \mod 4$$

This completes the proof.

PROPOSITION 8. *Let G be a diagonal, integral quadratic form of even dimension $2d$. Let b be a square-free, nonzero integer. Then*

(1) *The value of $e_{-1}(bG) - e_{-1}(G)$ is 0 if $b > 0$, and it is $4(\varepsilon_-(G) - d)$ if $b < 0$.*

(2) *For every odd prime p (-1 included), the value of $e_p(bG) - e_p(G)$ is*
   (a) $\left[\frac{b}{p}\right] \bmod 8$, *if $p \nmid b$ and $p \in n(G)$.*
   (b) $0 \bmod 8$, *if $p \nmid b$ and $p \notin n(G)$.*
   (c) $2(p-1)(1+d) + \left[\frac{b/p}{p}\right] + \left[\frac{\det_n G/p}{p}\right] \bmod 8$, *if $p|b$ and $p \in n(G)$.*
   (d) $2(p-1)d + \left[\frac{\det_n G}{p}\right] \bmod 8$, *if $p|b$ and $p \notin n(G)$.*

(3) *If b is odd, the value of $e_2(bG) - e_2(G)$* is

$$2(b-1)(d + s(G)) + o(G)\left[\frac{2}{b}\right] \bmod 8.$$

(4) *If $b = 2b_1$, b_1 odd, the value of $e_2(2b_1G) - e_2(G)$* is

$$2(b_1 - 1)(d + s(G)) + o(G)\left[\frac{2}{b_1}\right] + 4t(G) \bmod 8.$$

In particular

$$e_2(2G) - e_2(G) = 4t(G) \bmod 8$$

PROOF. We may assume that G is a diagonal, square-free, integral quadratic form. If $b > 0$, clearly $e_{-1}(bG) = e_{-1}(G)$. If $b < 0$, then

$$e_{-1}(bG) - e_{-1}(G) = -2(2d - \varepsilon_-(G)) - (-2\varepsilon_-(G)) = 4(\varepsilon_-(G) - d),$$

and this completes the proof of part (1).

If $p = -1$, it follows from (1) that the value of $e_{-1}(bG) - e_{-1}(G)$ is

$$\begin{cases} 0 \\ 4(1+d) \bmod 8 \\ 4d \end{cases} \text{ if } \begin{cases} b > 0 \\ b < 0 \text{ and } -1 \in n(G), \\ b < 0 \text{ and } -1 \notin n(G) \end{cases}$$

because $\varepsilon_-(G)$ is odd if and only if $-1 \in n(G)$, that is, if and only if $\det_n G < 0$. This proves part (2) for $p = -1$, because

$$\left[\frac{b/(-1)}{-1}\right] + \left[\frac{\det_n G/(-1)}{-1}\right] = 0 \bmod 8$$

if $b < 0$ and $\det_n G < 0$; and

$$\left[\frac{\det_n G}{-1}\right] = 0 \bmod 8$$

if $\det_n G > 0$.

If $p \neq -1$ is an odd prime, let p^x be the maximal power of p dividing $\det G$. If $p \nmid b$:

$$e_p(bG) - e_p(G) = x\left[\frac{b}{p}\right] \mod 8.$$

Hence, if $p \in n(G)$, x is odd and this proves $(2a)$, while if $p \notin n(G)$, x is even and this proves $(2b)$. Assume $p|b$, that is $b = pb_1$, where p and b_1 are coprime. Then, $e_p(bG) - e_p(G) \mod 8$ is:

$$e_p(pb_1G) - e_p(G) = (2d - 2x)(p-1) + (2d - x)\left[\frac{b_1}{p}\right] + \left[\frac{\det_n G/p^\alpha}{p}\right],$$

where $\alpha = 0$ if $p \notin n(G)$, and $\alpha = 1$ if $p \in n(G)$. Hence, if $p \in n(G)$, x is odd and $\alpha = 1$, and this proves $(2c)$, while if $p \notin n(G)$, x is even and $\alpha = 0$, and this proves $(2d)$.

By $(2a)$, $(2b)$ and the global relation, $e_2(2G) - e_2(G) \mod 8$ can be written:

$$-\sum_{p \text{ odd prime}} (e_p(2G) - e_p(G)) = \sum_{p \in n(G)} \left[\frac{2}{p}\right] = 4t(G) \mod 8,$$

because $\left[\frac{2}{p}\right] = 4 \mod 8$ if and only if $p = \pm 3 \mod 8$. This proves the particular case of part (4).

Next, we prove part (3) by induction in the number of (odd) prime numbers (-1 included), dividing b. Thus, assume, first, that $b \notin n(G)$ is an odd prime. By the global relation, $-e_2(bG) + e_2(G) \mod 8$ can be written as follows:

$$\sum_{p \neq b, \, odd} (e_p(bG) - e_p(G)) + (e_b(bG) - e_b(G)) \mod 8$$

Using $(2a)$ and $(2b)$:

$$\sum_{p \neq b, \, odd} (e_p(bG) - e_p(G)) = \sum_{p \in n(G)} \left[\frac{b}{p}\right] \mod 8.$$

And using $(2d)$:

$$e_b(bG) - e_b(G) = 2(b-1)d + \left[\frac{\det_n G}{b}\right] \mod 8.$$

Hence $-e_2(bG) + e_2(G) \mod 8$ is:

$$2(b-1)d + o(G)\left[\frac{2}{b}\right] + \sum_{p \in n(G)} \left(\left[\frac{b}{p}\right] + \left[\frac{p}{b}\right]\right) \mod 8.$$

By quadratic reciprocity:

$$\left[\frac{b}{p}\right] + \left[\frac{p}{b}\right] = (p-1)(b-1) \mod 8.$$

Hence $-e_2(bG) + e_2(G) \mod 8$ is:

$$(b-1)\left(2d + \sum_{p \in n(G)} (p-1)\right) + o(G)\left[\frac{2}{b}\right] \mod 8.$$

And, since $b - 1 = 0 \mod 2$, and

$$\sum_{p \in n(G)} (p-1) = \sum_{\substack{p \in n(G) \\ p = 1 \mod 4}} (p-1) + \sum_{\substack{p \in n(G) \\ p = -1 \mod 4}} (p-1) = 2s(G) \mod 4,$$

we have

$$-e_2(bG) + e_2(G) = 2(b-1)(d + s(G)) + o(G)\left[\frac{2}{b}\right] \mod 8.$$

Since the terms in the rigth-hand part of this formula are all zero mod 4, we can change their signs mod 8. This proves (3) if $b \notin n(G)$ is an odd prime.

Next, assume that $b \in n(G)$ is an odd prime. As before, using the global relation, (2*a*), (2*b*) and (2*c*), we can write $-e_2(bG) + e_2(G)$ as follows:

$$\sum_{p \in n(G) \setminus \{b\}} \left[\frac{b}{p}\right] + 2(b-1)(1+d) + \left[\frac{1}{b}\right] + \left[\frac{\det_n G/b}{b}\right] \mod 8.$$

Hence $-e_2(bG) + e_2(G)$ is:

$$2(b-1)(1+d) + o(G)\left[\frac{2}{b}\right] + \sum_{p \in n(G) \setminus \{b\}} \left(\left[\frac{b}{p}\right] + \left[\frac{p}{b}\right]\right) \mod 8.$$

Note that $2(b-1) = (b-1)^2 \mod 8$, because b is odd. Note also, that all the terms in the last expresion are zero mod 4. Then, quadratic reciprocity implies that $e_2(bG) - e_2(G)$ can be written as follows:

$$(b-1)\left(2d + \sum_{p \in n(G)} (p-1)\right) + o(G)\left[\frac{2}{b}\right] \mod 8.$$

As before:

$$e_2(bG) - e_2(G) = 2(b-1)(d + s(G)) + o(G)\left[\frac{2}{b}\right] \mod 8.$$

This proves (3) if $b \in n(G)$ is an odd prime.

Next, assume part (3) is true if b is a product of k odd primes (necessarily different from each other, because b is square-free). Take a new prime q and let us prove (3) for the number qb. We have

$$e_2(qbG) - e_2(G) = e_2(qbG) - e_2(bG) + e_2(bG) - e_2(G).$$

By the induction hypothesis, $e_2(qbG) - e_2(G) \mod 8$ is:

$$2(q-1)(d + s(bG)) + o(bG)\left[\frac{2}{q}\right] + 2(b-1)(d + s(G)) + o(G)\left[\frac{2}{b}\right].$$

Since $\det_n(bG) = \det_n G$, we have $s(bG) = s(G)$ and $o(bG) = o(G)$. Therefore,

$$e_2(qbG) - e_2(G) = 2(q + b - 2)(d + s(G)) + o(G)\left[\frac{2}{qb}\right] \mod 8.$$

Note that $q + b - 2 = qb - 1 \mod 4$, because $q = b = 1 \mod 2$. Hence part (3) is true, for an arbitrary odd number b.

Next, we prove part (4). Let $b = 2b_1$, where b_1 is odd. We have

$$e_2(2b_1G) - e_2(G) = e_2(2b_1G) - e_2(b_1G) + e_2(b_1G) - e_2(G).$$

Using the particular case of part (4), already proved, we can write $e_2(2b_1G) - e_2(G)$ as follows:

$$4t(b_1G) + 2(b_1 - 1)(d + s(G)) + o(G)\left[\frac{2}{b_1}\right] \mod 8.$$

Hence formula (4) follows, because $t(b_1G) = t(G)$. This completes the proof.

Remark 4. From parts (3) and (4), we have

$$d + s(G) = \frac{e_2(-G) - e_2(G)}{4} \mod 2,$$

$$t(G) = \frac{e_2(2G) - e_2(G)}{4} \mod 2.$$

Using Proposition 6, these two formulas provide a different expression of the third projective invariant.

Proposition 9. *Let $p_1, \ldots, p_k$ be different, positive, odd prime numbers. Let $m_0, m_1, \ldots, m_k \in \{0, 4\}$. Then, there are infinitely many prime numbers b such that*

$$\left[\frac{2}{b}\right] = m_0$$

and

$$\left[\frac{b}{p_i}\right] = m_i, \qquad i = 1, \ldots, k$$

PROOF. For each index $i = 1, \ldots, k$, select an integer n_i such that

$$\left[\frac{n_i}{p_i}\right] = m_i, \qquad 0 < n_i < p_i,$$

and an integer n_0 such that

$$\left[\frac{2}{n_0}\right] = m_0.$$

By the Chinese theorem of rests, there is an integer b_1 such that

$$b_1 = n_i \mod p_i, \qquad i = 1, \ldots, k$$

and

$$b_1 = n_0 \mod 8.$$

Then b_1 and $8p_1 \ldots p_k$ are coprime. All the numbers b in the arithmetic progression

$$b_1 + h(8p_1 \ldots p_k), \qquad h = 1, 2, 3, \ldots$$

satisfy

$$\left[\frac{2}{b}\right] = m_0$$

and

$$\left[\frac{b}{p_i}\right] = m_i, \qquad i = 1, \ldots, k$$

By Dirichlet Theorem, this progression contains infinitely many prime numbers. This completes the proof.

5.3.4. Projective classification theorem.

THEOREM 7. *Two rational quadratic forms of the same even dimension are projectively equivalent if and only if they have identical projective invariants.*

PROOF. Before starting the proof, note that $F \overset{\mathbf{Q}}{\sim} G$ implies $p(F) = p(G)$, where $p(F)$ denotes the projective invariants of F. Since a rational quadratic form is **Q**-equivalent to a diagonal, square-free, integral quadratic form, we can

assume that the forms F and G, in the statement of the theorem, are diagonal, square-free integral quadratic forms.

We first prove that the condition in the theorem is necessary. That is, if $F \overset{P}{\sim} G$ then $p(F) = p(G)$.

Since $F \overset{\mathbb{Q}}{\sim} bG$, for some nonzero, square-free integer b, then the Sylvester signatures of F and bG coincide. But the Sylvester signature of G equals $\pm$ the Sylvester signature of bG according as if b is positive or negative. Hence

$$(\varepsilon_+(F), \varepsilon_-(F)) = (\varepsilon_+(G), \varepsilon_-(G))$$

or

$$(\varepsilon_+(F), \varepsilon_-(F)) = (\varepsilon_-(G), \varepsilon_+(G)).$$

In either case $\varepsilon(F) = \varepsilon(G)$. Let ε denote $\varepsilon(F) = \varepsilon(G)$.

On the other hand, $F \overset{\mathbb{Q}}{\sim} bG$ implies $r^2 \det F = b^{2d} \det G$, where $2d$ is the common dimension of F and G, and r is a rational number. Hence $\det_n F = \det_n G$. Let Δ_n denote this common reduced determinant. We also define:

$$n := n(F) = n(G)$$

$$s := s(F) = s(G)$$

$$t := t(F) = t(G)$$

$$o := o(F) = o(G)$$

Claim 1. *If $F \overset{\mathbb{Q}}{\sim} bG$, where b is a nonzero, square-free integer, and for some odd prime $q \neq -1$, $q \notin n$,*

$$2(q-1)d + \left[\frac{\Delta_n}{q}\right] = 0 \mod 8,$$

then

$$e_q(F) = e_q(G) \mod 8.$$

Proof. If $q \nmid b$, Proposition 8 implies

$$e_q(F) - e_q(G) = e_q(bG) - e_q(G) = 0 \mod 8.$$

If $q|b$, Proposition 8 implies

$$e_q(F) - e_q(G) = e_q(bG) - e_q(G) = 2(q-1)d + \left[\frac{\Delta_n}{q}\right] \mod 8,$$

and this is zero by hypothesis. This completes the proof of this claim.

CLAIM 2. *If* $F \overset{Q}{\sim} bG$, *where* b *is a nonzero, square-free integer, and* $\det_n F = (-1)^d \bmod 8$, *then* $e_2(F) = e_2(G)$.

PROOF. By Proposition 6, $\det_n F = (-1)^d \bmod 8$ if and only if

$$(o, d+s, t) = (0,0,0) \bmod 2.$$

If b is odd, Proposition 8 implies that $e_2(F) - e_2(G)$ is

$$e_2(bG) - e_2(G) = 2(b-1)(d+s) + o\left[\frac{2}{b}\right] \bmod 8,$$

and this is zero, because $b - 1 = d + s = o = 0 \bmod 2$. If $b = 2b_1$, b_1 odd, Proposition 8 implies that $e_2(F) - e_2(G)$ is

$$e_2(2b_1G) - e_2(G) = 2(b_1 - 1)(d+s) + o\left[\frac{2}{b_1}\right] + 4t \bmod 8,$$

and this is zero because $b_1 - 1 = d + s = o = t = 0 \bmod 2$. This completes the proof of this claim.

Therefore, we have proved that if $F \overset{P}{\sim} G$ then $p(F) = p(G)$. Next, we prove the converse.

Assume that the forms F and G are diagonal, square-free, integral quadratic forms of the same even dimension $2d$, and with the same projective invariants $p(F) = p(G)$. We want to prove that $F \overset{P}{\sim} G$.

Define $\Delta_n = \det_n F = \det_n G$ and

$$n := n(F) = n(G)$$

$$s := s(F) = s(G)$$

$$t := t(F) = t(G)$$

$$o := o(F) = o(G)$$

Step 1. Replacing, if necessary, G by $-G$, we can assume that $p(F) = p(G)$, and, moreover, that

$$e_{-1}(F) = e_{-1}(G).$$

Indeed, since $G \overset{P}{\sim} -G$

$$p(F) = p(G) = p(-G).$$

Step 2. Let a be the product of all the odd primes

$$r \neq -1, \qquad r \notin n$$

such that

$$e_r(G) - e_r(F) \neq 0 \mod 8$$

This is well defined, because it is a finite product. Indeed, if an odd prime r fails to divide both $\det F$ and $\det G$, then

$$e_r(G) = e_r(F) = 0 \mod 8.$$

Consider aG. Then $G \overset{P}{\sim} aG$ implies

$$p(F) = p(G) = p(aG).$$

Moreover, since $a > 0$,

$$e_{-1}(F) = e_{-1}(G) = e_{-1}(aG).$$

Next, we prove that

$$e_q(aG) - e_q(F) = 0 \mod 8,$$

for every odd prime $q \neq -1$, $q \notin n$.

In fact, if $q \nmid a$, then

$$e_q(aG) - e_q(G) = 0 \mod 8,$$

by Proposition 8, and

$$e_q(G) - e_q(F) = 0 \mod 8,$$

by definition of a. And, adding up these two relations, we obtain

$$e_q(aG) - e_q(F) = 0 \mod 8.$$

But if $q|a$, then by Proposition 8:

$$e_q(aG) - e_q(G) = 2(q-1)d + \left[\frac{\Delta_n}{q}\right] \mod 8$$

Now, this has the only possible values 0 or 4 mod 8 (Proposition 7). It cannot possibly be zero, otherwise both $e_q(G)$ and $e_q(F)$ would be part of the list of projective invariants of F and G, respectively, and as such they should coincide, which is not the case, since by definition of a,

$$e_q(G) - e_q(F) \neq 0 \mod 8.$$

Now, the value of this last formula is 4 by Proposition 7. Hence, adding up the last two relations, we finally obtain

$$e_q(aG) - e_q(F) = 0 \mod 8.$$

Therefore, by replacing, if necessary, aG by G, we can assume that our original forms F and G, besides having the same projective invariants $p(F) = p(G)$, they enjoy the following properties:

$$e_{-1}(F) = e_{-1}(G).$$

and

$$e_q(F) = e_q(G) \mod 8$$

for every odd prime $q \neq -1,\ q \notin n$.

Step 3. By Proposition 7, for every odd prime $p \neq -1,\ p \in n$,

$$e_p(G) - e_p(F) = 0 \mod 4.$$

Hence, by Proposition 9, there are infinitely many primes b such that $b > 2$, $b \not| \det F,\ b \not| \det G$ and

$$\left[\frac{b}{p}\right] = e_p(G) - e_p(F) \mod 8,$$

for every odd prime $p \neq -1,\ p \in n$.

For such numbers b, since $G \overset{p}{\sim} bG$,

$$p(F) = p(bG) \text{ and } e_{-1}(F) = e_{-1}(bG).$$

Next, we prove that

$$e_r(bG) - e_r(F) = 0 \mod 8,$$

for every odd prime $r \neq -1,\ r \neq b$. In fact,

$$e_r(bG) - e_r(F) = e_r(bG) - e_r(G) + e_r(G) - e_r(F) \mod 8.$$

And this is zero mod 8, because if $r \in n$, then, by definition of b and by Proposition 8:

$$e_r(G) - e_r(F) = \left[\frac{b}{r}\right] = e_r(bG) - e_r(G).$$

And, if $r \notin n,\ r \neq b$, then

$$e_r(bG) - e_r(G) = 0 \mod 8,$$

by Proposition 8, and

$$e_r(G) - e_r(F) = 0 \mod 8,$$

by hypothesis.

Remember that we have an infinitude of b's satisfying the previous conditions, and, since all such b's are odd, Proposition 8 implies

$$e_2(bG) - e_2(G) = 2(b-1)(d+s) + o\left[\frac{2}{b}\right] \mod 8,$$

and, if we can, we want to select b in such a way that

$$e_2(bG) - e_2(G) = e_2(G) - e_2(F) \mod 8.$$

There are three cases in which this selection can be made. There will be a remaining case, for which b must be defined *ex novo*.

Case 1. $e_2(G) - e_2(F) = 0 \mod 8$.

Select, as we can (Proposition 9), $b = 1 \mod 8$. Then

$$\left[\frac{2}{b}\right] = 0 \mod 8.$$

Therefore

$$e_2(bG) - e_2(G) = 0 \mod 8.$$

Case 2. $e_2(G) - e_2(F) = 4 \mod 8$, and $s + d = 1 \mod 2$.

Select (Proposition 9) $b = -1 \mod 8$. Then

$$\left[\frac{2}{b}\right] = 0 \mod 8.$$

Therefore,

$$e_2(bG) - e_2(G) = 2(b-1)(d+s) = 4 \mod 8,$$

because $s + d = 1 \mod 2$.

Case 3. $e_2(G) - e_2(F) = 4 \mod 8$, and $s + d = 0 \mod 2$, $o = 1$.

Select (Proposition 9) $b = 3 \mod 8$. Then

$$\left[\frac{2}{b}\right] = 4 \mod 8$$

Therefore,

$$e_2(bG) - e_2(G) = 4 \mod 8.$$

In cases 1, 2 and 3 we obtain

$$e_2(bG) - e_2(F) = e_2(bG) - e_2(G) + e_2(G) - e_2(F) = 0 \mod 8.$$

This, together with $e_{-1}(bG) = e_{-1}(F)$ and $e_r(bG) = e_r(F) \mod 8$, for every odd prime $r \neq b$, implies

$$e_b(bG) = e_b(F) \mod 8,$$

by the global relation. Hence $F \overset{\mathbb{Q}}{\sim} bG$, because $\det_n bG = \det_n G = \det_n F$. Hence $F \overset{P}{\sim} G$, as we wanted to prove.

Only remains

Case 4. $e_2(G) - e_2(F) = 4 \mod 8$, and $s + d = 0 \mod 2$, $o = 0$.

Here, t must be 1. Otherwise

$$(o, s + d, t) = (0, 0, 0) \mod 2,$$

and this implies (Proposition 6) that $e_2(F)$ and $e_2(G)$ are projective invariants of F and G, respectively. By hypothesis, they should coincide, and this is not the case. Hence $t = 1$.

Define b, *ex novo*, as a positive, odd prime number such that $b \nmid \det F$, $b \nmid \det G$ and

$$\left[\frac{b}{p}\right] = \left[\frac{2}{p}\right] + e_p(G) - e_p(F) \mod 8,$$

for every odd prime $p \neq -1$, $p \in n$ (Proposition 9 and Proposition 7). Then:

1: For every $p \neq -1$, $p \in n$, we can write $e_p(2bG) - e_p(F)$ as follows:

$$e_p(2bG) - e_p(bG) + e_p(bG) - e_p(G) + e_p(G) - e_p(F) \mod 8.$$

And this is zero, because (Proposition 8)

$$e_p(2bG) - e_p(bG) = \left[\frac{2}{p}\right],$$

and

$$e_p(bG) - e_p(G) = \left[\frac{b}{p}\right],$$

and

$$e_p(G) - e_p(F) = \left[\frac{b}{p}\right] + \left[\frac{2}{p}\right],$$

by definition of b.

2: For every odd prime $p \neq -1$, $p \notin n$, $p \neq b$ we have

$$e_p(2bG) - e_p(F) = e_p(2bG) - e_p(G) + e_p(G) - e_p(F) = 0 \mod 8,$$

because (Proposition 8)

$$e_p(2bG) - e_p(G) = 0 \mod 8,$$

and

$$e_p(G) - e_p(F) = 0 \mod 8,$$

by hypothesis.

3: $e_2(2bG) - e_2(F)$ can be written as follows:

$$e_2(2bG) - e_2(bG) + e_2(bG) - e_2(G) + e_2(G) - e_2(F) \mod 8.$$

And this is zero, because by Proposition 8

$$e_2(2bG) - e_2(bG) = 4t = 4 \mod 8;$$

and

$$e_2(bG) - e_2(G) = 2(b-1)(s+d) + o\left[\frac{2}{b}\right] = 0 \mod 8,$$

because

$$b - 1 = s + d = o = 0 \mod 2;$$

and

$$e_2(G) - e_2(F) = 4 \mod 8,$$

by the hypothesis of the present *Case* 4.

4: $\det_n 2bG = \det_n G = \det_n F$ and $e_{-1}(F) = e_{-1}(G) = e_{-1}(2bG)$.

Therefore, since F and $2bG$ have the same reduced determinant and the same p-excesses for all prime $p \neq b$, it follows (global relation) that also $e_b(F) = e_b(2bG)$. This implies that

$$F \overset{Q}{\sim} 2bG.$$

Hence $F \overset{P}{\sim} G$, as we wanted to prove.

This completes the proof of the theorem.

6. The projective classification of some particular even forms

Theorem 8. *There are at most two P-equivalence classes of* $2d$*-ary integral quadratic forms having the same square-free determinant* Δ *and Sylvester partition* a. *If* $\Delta \neq (-1)^d \mod 8$, *there is only one such P-class, namely* $\langle \Delta, \pm 1, \ldots, \pm 1 \rangle$, *where the appropriate signs are determined by* a. *If* $\Delta = (-1)^d \mod 8$ *and* $d \neq a \mod 2$, *there are exactly two such P-classes, but if* $d = a \mod 2$, *the number of P-classes migth be one or two. For instance, if* $|\Delta|$ *is prime, there is only one P-class.*

PROOF. Let F and G be two $2d$-ary integral quadratic forms with identic square-free determinant Δ and Sylvester partition a. Since $\det F = \det_n F$, the only P-invariants of F are $2d$, a, Δ, and the 2-excess $e_2(F)$ if

$$\Delta = (-1)^d \bmod 8.$$

In this case, F and G can only differ on the values of $e_2(F)$ and $e_2(G)$. But $e_2(F) = e_2(G) \bmod 4$, since $\det_n F = \Delta = \det_n G$ (Proposition 7). Hence $e_2(G) = e_2(F) \bmod 8$, or $e_2(G) = e_2(F) + 4 \bmod 8$. Therefore, there are at most two P-equivalence classes of $2d$-ary integral quadratic forms having the same square-free determinant Δ and Sylvester partition a. Note that, if

$$\Delta \neq (-1)^d \bmod 8,$$

there is only one such class.

Let D be a product of different positive odd primes. Let a, d be integers such that $0 \leq a \leq d$. Let s_1 be the number of primes dividing D, and congruent with $-1 \bmod 4$. Let t be the number of primes dividing D, and congruent with $\pm 3 \bmod 8$. Let $\Delta = (-1)^a D$, and let s be the number of primes (-1 included) dividing Δ, and congruent with $-1 \bmod 4$. Note that $s = s_1 + a \bmod 2$. Assume $s + d = 0 \bmod 2$ and $t = 0 \bmod 2$. We want to compare the following two $2d$-ary, square-free forms

$$F = \langle -1, \overset{a}{\ldots}, -1, 1, \ldots, 1, D \rangle$$

and

$$G = \langle -D, -1, \overset{a-1}{\ldots}, -1, 1, \ldots, 1 \rangle.$$

Here $e_{-1}(F) = e_{-1}(G)$ and $\det F = \det G = (-1)^a D = \Delta$. Moreover, $(o, s+d, t) = (0,0,0) \bmod 2$. These two forms F and G are, therefore, P-equivalent if and only if $e_2(G) = e_2(F) \bmod 8$. Now

$$e_2(F) = 2d - (-a + (2d - a - 1) + D) = 2a + 1 - D$$

and

$$e_2(G) = 2d - (-a + 1 + (2d - a) - D) = 2a - 1 + D.$$

Thus

$$F \overset{P}{\sim} G \Leftrightarrow D = 1 \bmod 4 \Leftrightarrow s_1 = 0 \bmod 2 \Leftrightarrow d = a \bmod 2,$$

because $s_1 = s + a \bmod 2$ and $d + s = 0 \bmod 2$, by hypothesis. Therefore, if $d \neq a \bmod 2$, the $2d$-ary forms F and G with the same square-free determinant

Δ and the same partition a are P-inequivalent. But if $d = a \mod 2$ and D is a positive odd prime number, the only possible $2d$-ary forms with the same square-free determinant $\Delta = (-1)^a D$ and the same partition a are just the two forms F and G above, and these two are P-equivalent. However, if D is not prime, anything can happen as the following examples show.

EXAMPLE 3. $F = \langle 1, 1, 1, 19 \times 11 \rangle$, $G = \langle 1, 1, 19, 11 \rangle$. *Here* $a = d = 0 \mod 2$ *and* $\Delta = 19 \times 11 = 1 \mod 8$. *However*

$$e_2(F) = 4 - (3 + 19 \times 11) = 0 \mod 8$$

but

$$e_2(G) = 4 - (2 + 19 + 11) = 4 \mod 8.$$

Thus F and G are P-inequivalent.

EXAMPLE 4. $\langle 1, 1, 1, 13 \times 5 \rangle$, $\langle 1, 1, 13, 5 \rangle$. *Here* $a = d = 0 \mod 2$ *and* $\Delta = 13 \times 5 = 1 \mod 8$. *However,*

$$e_2(F) = 4 - (3 + 13 \times 5) = 0 \mod 8$$

and

$$e_2(G) = 4 - (2 + 13 + 5) = 0 \mod 8,$$

and there is only one P-class of quaternary, integral quadratic forms with determinant 13×5 *and Sylvester partition* $a = 0$.

As an application of Theorem 8 we have:

COROLLARY 4. *There are exactly two P-equivalent classes of quaternary, hyperbolic, integral quadratic forms with square-free determinant $\Delta = -D$, $D > 0$, if and only if $\Delta = 1 \mod 8$. They are represented by $F = \langle -1, 1, 1, D \rangle$ and $G = \langle -D, 1, 1, 1 \rangle$.*

PROOF. Since $d = 2$, $a = 1$, there are exactly two P-classes if and only if $\Delta = (-1)^d = 1 \mod 8$.

It is very illustrative to compare the proof of P-inequivalence of F and G, implicit in this Corollary, with the following geometric one.

First, use congruences mod 8 to show that F represents 0 but G does not. This implies that the orbifold $\mathbf{G} := \mathbf{H}^3/\mathrm{Aut}(G)$ is compact, while $\mathbf{F} := \mathbf{H}^3/\mathrm{Aut}(F)$ is not compact. Then, it is imposible that both orbifolds $\mathbf{F}$ and $\mathbf{G}$ have a common finite orbifold-covering. It follows that $\mathrm{Aut}(F)$ and $\mathrm{Aut}(G)$

are not commensurable, and, as a consequence, F and G are P-inequivalent, by Theorem 3.

7. Quaternary, hyperbolic, integral quadratic forms with reduced determinant -1: the Picard form

Consider the projective classification of quaternary, integral quadratic forms with the same reduced determinant and Sylvester partition. If the determinant is square-free, this has been done in the previous section. Let us consider forms with reduced determinant -1, to understand the possibilities. For such forms, $d+s=1 \mod 2$. Hence, besides the invariants $d=2$, $a=1$ and $\det_n F=-1$, the only projective invariants are the p-excesses $e_p(F)$, where p runs over all positive odd primes such that

$$\left[\frac{\det_n F}{p}\right]=\left[\frac{-1}{p}\right]=0 \mod 8,$$

that is, such that $p=1 \mod 4$. Now, $e_p(F)=0 \mod 8$ if p fails to divide $\det F$. Hence we only need to consider the positive odd primes p dividing $\det F$ and such that $p=1 \mod 4$.

For instance, all the forms $F_b=\langle -1,1,b,b\rangle$ and $G_b=\langle -b,b,1,1\rangle$, b integer >0, are P-equivalent to the Picard form $\langle -1,1,1,1\rangle$, because, if $p|b$ and $p=1 \mod 4$, then

$$e_p(\langle -1,1,b,b\rangle)=2(p-1)+2\left[\frac{b/p}{p}\right]=0 \mod 8,$$

and

$$e_p(\langle -b,b,1,1\rangle)=2(p-1)+2\left[\frac{b/p}{p}\right]+\left[\frac{-1}{p}\right]=0 \mod 8.$$

In fact

$$T(2)^t F_2 T(2)=2F_1,$$

where

$$T(2)=\begin{bmatrix}2 & 1 & 1 & 0\\ 0 & 1 & -1 & 0\\ 1 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix},$$

and

$$T(b)^t F_b T(b)=bF_1, \qquad b>0 \text{ odd},$$

where

$$T(b) = \begin{bmatrix} \frac{b+1}{2} & \frac{b-1}{2} & 0 & 0 \\ \frac{b-1}{2} & \frac{b+1}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since the forms $F_b = \langle -1, 1, b, b \rangle$ are all mutually commensurable, it is interesting to find the rational number

$$v(b) = \frac{\mathrm{vol}(\mathbf{F}_b)}{\mathrm{vol}(\mathbf{F}_1)},$$

where $\mathrm{vol}(\mathbf{F}_b)$ denotes the volume of the hyperbolic orbifold $\mathbf{F}_b := \mathbf{H}^3/\mathrm{Aut}(F_b)$. I have calculated $v(b)$, for a number of values of b, obtaining the following results (to be published elsewhere):

(1) If $p = -1 \mod 4$ is a prime number, then $v(p) = \frac{p^2+1}{2}$, $3 \leq p < 100$.
(2) If $p = 1 \mod 4$ is a prime number, then $v(p) = \frac{(p+1)^2}{2}$, $3 \leq p \leq 101$.
(3) $v(2) = 3$, $v(2^2) = 2v(2)$, and $v(2^n) = 2^{2(n-2)}v(2)$, for $3 \leq n \leq 7$.
(4) $v(3^n) = 3^{2(n-1)}v(3)$, for $1 \leq n \leq 4$.
(5) $v(5^n) = 5^{2(n-1)}v(5)$, for $1 \leq n \leq 2$.
(6) $v(ab) = v(a)v(b)$, where a and b are coprime, and $ab < 22$.

The obvious conjectures remain open.

We end this section with another example.

Example 5. *Consider* $H_p = \langle -1, 3, p, 3p \rangle$, *p prime,* $p = 5 \mod 12$. *Here,* $\det_n H_p = -1$ *and, as before, we only need to consider the positive odd primes q dividing* $\det H_p$ *and such that* $q = 1 \mod 4$. *Hence, there is only one projective invariant of* H_p *to consider, namely*

$$e_p(H_p) = 2(p-1) + \left[\frac{3}{p}\right] = \left[\frac{3}{p}\right] \mod 8,$$

because $p = 1 \mod 4$. *Since*

$$\left[\frac{3}{p}\right] = \left[\frac{p}{3}\right] + 2(p-1) = \left[\frac{2}{3}\right] \mod 8 = 4 \mod 8,$$

because $p = 2 \mod 3$, *we deduce that all the forms* H_p *are pairwise P-inequivalent. There is an infinitude of them, due to the Dirichlet Theorem on primes in arithmetic progression. The first three such forms are* H_5, H_{17} *and* H_{29}.

8. Some historical comments

The theory of integral quadratic forms has geometric ramifications. In 1868 Beltrami ([1] and [2]) published the first models of the hyperbolic plane $\mathbf{H}^2$ (the *pseudosphere*, consisting on the interior of the plane circle of radius 1 together with a Riemannian metric of negative curvature) and of the hyperbolic 3-space $\mathbf{H}^3$. He also introduced the *upper half-space model* of $\mathbf{H}^3$, as the set of points $(u, z) \in \mathbf{C} \times \mathbf{R}$ such that $z > 0$. The group of direct isometries being the group $\mathrm{PSL}(2, \mathbf{C})$ of Moebius transformations.

Klein, following work by Cayley, developed a projective-geometric theory that generalized Beltrami's pseudosphere model. Namely, an $(n+1)$-ary real quadratic form F with Sylvester signature $n-1$ (a *hyperbolic form*, in this article) represents a hyperquadric in the real projective n-space $\mathbf{R}P^n$ that bounds a topological ball. The interior of this ball is a model (*Klein model*) of hyperbolic n-space $\mathbf{H}^n$, and its group of isometries is the orthogonal group (isomorphic to $\mathrm{O}(n, 1)$) of the given quadratic form. The three dimensional half-space model of $\mathbf{H}^3$ is related to the Klein model of the diagonal form $\langle -1, 1, 1, 1 \rangle$ via stereographic projection ([11]; see the proof and comments by Bianchi in [3]).

Motivated, perhaps, by Clifford's discovery of a flat 2-torus inside spherical 3-space, Klein stated the problem of enumerating all the (so called) *forms of Clifford-Klein*. In actual language they can be identified with the *geometric orbifolds of constant curvature, complete and with finite volume* (see [15]). A number of illustrious geometers (Hermite, Picard, Klein, Fricke, Dick, Bianchi, Poincaré, and later Hopf, Seifert and Threlfall among them) started the investigation and the construction of these forms. The first noneuclidean examples are the quotients of properly discontinuous groups acting upon spherical and hyperbolic planes. The book by Fricke-Klein is one of the best references. The heritage of Picard, Klein, Bianchi, etc. is the theory of arithmetic groups, developed by Borel and Harish-Chandra and many others (see [12] and [8]).

These groups are called arithmetic, because they are constructed using arithmetic methods. For instance, in dimension three, the idea is to define a subgroup G of $\mathrm{PSL}(2, \mathbf{C})$ (half-space model), or of $\mathrm{O}(3, 1)$ (Klein model), such that the entries of the matrices in G belong to a discrete subset of $\mathbf{C}$ (resp. $\mathbf{R}$). For instance, in dimension three, Bianchi, following work by Picard, considered the set of homographies and antihomographies whose coefficients are Gauss integers and with determinant 1 or i. This group (that we call *Picard's group*) is sent, via stereographic projection, to a subgroup of $\mathrm{O}(3, 1)$ conjugate to the discrete subgroup formed by all the 4×4 integral matrices T such that $T^t F T = F$, where F is the diagonal integral quadratic form

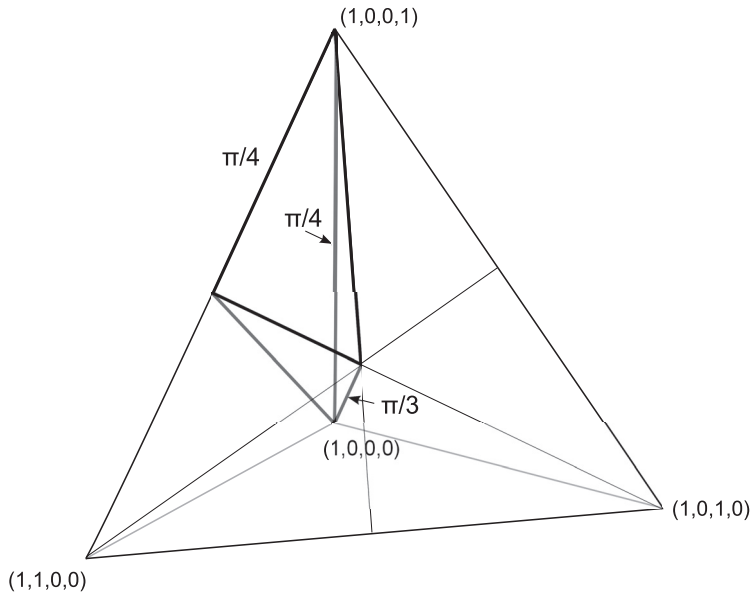

Fig. 1. The 3-orbifold Q

$\langle -1,1,1,1\rangle$ (the group Aut F of *automorphisms* of F). It is readily found that the quotient of the action of Picard group on the ball of radius 1 is the hyperbolic 3-orbifold Q depicted in solid lines in Fig. 1. The underlying space of Q is a hyperbolic asymptotic tetrahedron with only one cusp-point $(1,0,0,1)$; the faces of the tetrahedron are mirrors; and the dihedral angles are all right angles, excepted the indicated three angles.

W. Thurston discovered in 1976 that the topology and geometry of 3-manifolds and 3-orbifolds (concept that he reintroduced and popularized) are intimately related. Let us illustrate this by constructing, in an elementary way, a finite index subgroup G of Picard's group such that the quotient orbifold $\mathbf{H}^3/G$ is a complete, finite volume, hyperbolic manifold, homeomorphic to the exterior of the Borromean rings. This will show that the group $\pi(S^3\backslash B) \approx G$ of the Borromean rings (Fig. 2) is *arithmetic* (compare [9]).

The octant of Fig. 1 is the union of six copies of Picard's orbifold Q. The eigth octants form an asymptotic regular octahedron O, which is the union of 48 copies of Q. Reflect, through each face of O, the cone with apex the center of O and base the face of reflection. We obtain an asymptotic regular rombododecahedron R, having its tetravalent vertices at infinity. Its dihedral angles are all right angles. Thus R is the union of 96 copies of Q. Identifying the faces of R as depicted, one obtains the exterior E of the Borromean rings [18]. The natural map from E to Q is a 96-fold orbifold covering (Fig. 3).

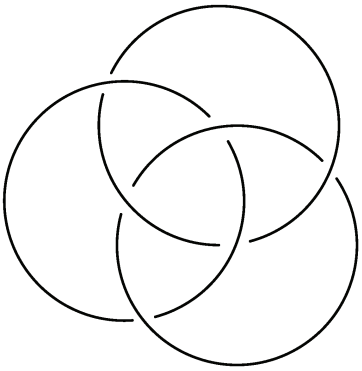

Fig. 2. Borromean rings

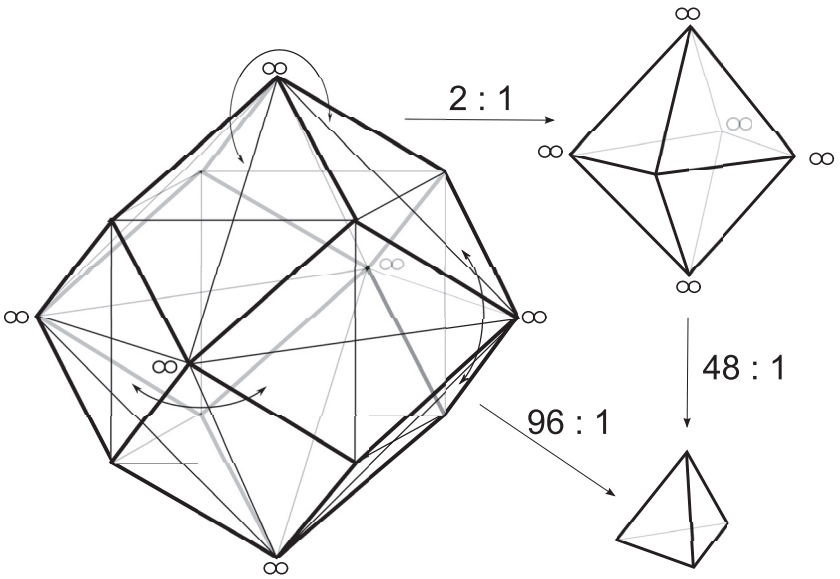

Fig. 3. The map from E to Q

Therefore (see [18] and [13]), the group $\pi(S^3 \backslash B) \approx G$ of the Borromean rings acts properly and discontinuously on $\mathbf{H}^3$ in such a way that $\mathbf{H}^3/G$ is a complete, finite volume hyperbolic manifold homeomorphic to the exterior E of the Borromean rings. Moreover, G is a subgroup of index 96 of the Picard group. The volume of Q can be calculated to be

$$\mathrm{vol}(Q) = 0.07633046618143491\ldots$$

Therefore, the volume of E is 96 times the volume of Q:

$$\mathrm{vol}(E) = 7.3277247534177521204\ldots$$

Due to a celebrated theorem of Mostow, the metric invariants of hyperbolic 3-orbifolds are in fact topological invariants, because the hyperbolic structures of such orbifolds are unique, up to isometry. Thus the volume of E is a topological invariant of the Borromean rings. This is one of the various reasons which makes the theory of Thurston enormously important.

Just for the record, the set of tetravalent vertices of R is

$$(1,1,0,0),\ (1,0,1,0),\ (1,0,0,1),\ (1,0,0,-1),\ (1,0,-1,0),\ (1,-1,0,0)$$

and the set of trivalent vertices is

$$(2,1,-1,1),\ (2,-1,1,1),\ (2,1,1,-1),\ (2,1,-1,-1),$$
$$(2,1,1,1),\ (2,-1,1,-1),\ (2,-1,-1,1),\ (2,-1,-1,-1)$$

and the parabolic automorphisms of $\langle -1,1,1,1\rangle$, identifying faces, are

$$x = \begin{bmatrix} 3 & -2 & 0 & -2 \\ 2 & -1 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ -2 & 2 & 0 & 1 \end{bmatrix}, \quad y = \begin{bmatrix} 3 & -2 & 2 & 0 \\ -2 & 1 & -2 & 0 \\ -2 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad z = \begin{bmatrix} 3 & 0 & 2 & -2 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & -2 \\ 2 & 0 & 2 & -1 \end{bmatrix}$$

They satisfy the relations of the Wirtinger presentation of the link group G. Namely:

$$[x,[y^{-1},z]] = [y,[z^{-1},x]] = [z,[x^{-1},y]] = 1$$

References

[1] E. Beltrami, Saggio di interpretazione della geometria non-euclidea, Gior. Mat., **6** (1868), 248–312.

[2] E. Beltrami, Teoria fondamentale degli spazii di curvatura constante, Annali di Mat. Serie II, **2** (1868), 232–255.

[3] L. Bianchi, Ricerche sulle forme quaternarie quadratiche e sui gruppi poliedrici, Annali di Matematica Pura e applicata (2), **21** (1893), 237–288.

[4] L. Bianchi, Complemento alle ricerche sulle forme quaternarie quadratiche e sui gruppi poliedrici, Annali di Matematica Pura e applicata (2), **23** (1894), 1–44.

[5] A. Borel, Harish-Chandra, Arithmetic subgroups of algebraic groups, Annals of Math., **75** (1962), 485–535.

[6] J. W. S. Cassels, Rational Quadratic Forms, Academic Press, London, New York, San Francisco, 1978.

[7] John H. Conway, assisted by Francis Y. C. Fung, The sensual (quadratic) form, Carus Math. Monographs No. 26, MAA, Washington, 1977.

[8] J. Elstrodt, F. Grunewald, J. Mennicke, Groups Acting on Hyperbolic Space, Springer monographs in Math., Springer-Verlag, New York, 1997.
[9] Hugh M. Hilden, M. T. Lozano, José M. Montesinos-Amilibia, On the Borromean orbifolds: geometry and arithmetic, Topology '90 (Columbus, OH, 1990), 133–167, Ohio State Univ. Math. Res. Inst. Publ., 1, de Gruyter, Berlin, 1992.
[10] B. W. Jones, The Arithmetic Theory of Quadratic Forms, Carus Math. Monographs No. 10, MAA, Baltimore, 1950.
[11] F. Klein, Über die sogennante nicht-Euklidische Geometrie, Math. Ann. **4** (1871), 573–625.
[12] C. Maclachlan, A. W. Reid, The Arithmetic of Hyperbolic 3-Manifolds, Graduate Texts in Math., 219, Springer-Verlag, New York, 2003.
[13] Y. Matsumoto, J. M. Montesinos-Amilibia, A proof of Thurston's uniformization theorem of geometric orbifolds, Tokyo J. Math., **14** (1) (1991), 181–196.
[14] J. M. Montesinos-Amilibia, On the integral and projective equivalence of odd rank integral quadratic forms, (in preparation).
[15] J. G. Ratcliffe, Foundations of Hyperbolic Manifolds (Second Edition), Graduate Texts in Math., 149, Springer Verlag, New York, 2006.
[16] W. Scharlau and H. Opolka, From Fermat to Minkowski, Springer Verlag, New York, 1985.
[17] J. Stillwell, Elements of Number Theory, Springer Verlag, New York, 2003.
[18] W. P. Thurston, The geometry and topology of three-manifolds, Princeton University Lectures, 1976–77, available at http://library.msri.org/books/gt3m/

José María Montesinos-Amilibia
Facultad de Matemáticas
Universidad Complutense
28040 *Madrid*
Spain
E-mail: montesin@mat.ucm.es