Spiegelungssatz: a combinatorial proof for the 4-rank

Laurent Habsieger, Emmanuel Royer

▶ **To cite this version:**

Laurent Habsieger, Emmanuel Royer. Spiegelungssatz: a combinatorial proof for the 4-rank. International Journal of Number Theory, 2011, 7 (8), pp.2157-2170. 10.1142/S1793042111005106 . hal-00565894v2

HAL Id: hal-00565894
https://hal.science/hal-00565894v2

Submitted on 27 Apr 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SPIEGELUNGSSATZ: A COMBINATORIAL PROOF FOR THE 4-RANK

LAURENT HABSIEGER AND EMMANUEL ROYER

Abstract. The Spiegelungssatz is an inequality between the 4-ranks of the narrow ideal class groups of the quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-D})$. We provide a combinatorial proof of this inequality. Our interpretation gives an affine system of equations that allows to describe precisely some equality cases.

Contents

Introduction

Let $\mathbb{K}$ be a quadratic field. Let $\mathcal{I}_{\mathbb{K}}$ be the multiplicative group of fractional nonzero ideals of the ring of integers of $\mathbb{K}$ and $\mathcal{P}_{\mathbb{K}}$ be the subgroup of principal fractional ideals. We consider the subgroup $\mathcal{P}_{\mathbb{K}}^+$ of $\mathcal{P}_{\mathbb{K}}$, whose elements are the ones generated by an element with positive norm. The narrow class group $\mathcal{C}\ell_{\mathbb{K}}^+$ of $\mathbb{K}$ is the quotient $\mathcal{I}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}^+$. If $\mathbb{K}$ is imaginary, this is the usual class group $\mathcal{C}\ell_{\mathbb{K}} := \mathcal{I}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ whereas if $\mathbb{K}$ is real, the group $\mathcal{C}\ell_{\mathbb{K}}$ is a quotient of $\mathcal{C}\ell_{\mathbb{K}}^+$. We have $\mathcal{C}\ell_{\mathbb{K}}^+ = \mathcal{C}\ell_{\mathbb{K}}$ if and only if the fundamental unit of $\mathbb{K}$ has norm -1. Otherwise, the cardinalities of these two groups differ by a factor 2. For more details about the relations between $\mathcal{C}\ell_{\mathbb{K}}$ and $\mathcal{C}\ell_{\mathbb{K}}^+$ we refer to [FK10a, Section 3.1]. The narrow class-group being finite, we can define its p^k-rank for any power of a prime number p^k by

$$\mathrm{Rank}_{p^k}(\mathbb{K}) := \dim_{\mathbb{F}_p} \left(\mathcal{C}\ell_{\mathbb{K}}^+\right)^{p^{k-1}} \Big/ \left(\mathcal{C}\ell_{\mathbb{K}}^+\right)^{p^k}.$$

2010 *Mathematics Subject Classification.* 11R29,11R11,11A15,11T24,05E15.

Key words and phrases. 4-rank, Spiegelungssatz, combinatorial interpretation, reflection principle.

This research was partially supported by ANR grant *Modunombres*.

We would like to thank Étienne Fouvry for having introduced us to this problem.

In other words, $\mathrm{Rank}_{p^k}(\mathbb{K})$ is the number of elementary divisors of $\mathcal{C}\ell^+_{\mathbb{K}}$ divisible by p^k.

If $\mathbb{K} = \mathbb{Q}(\sqrt{\Delta})$, the *reflection* of $\mathbb{K}$ is the quadratic field $\mathbb{K}^{\#} := \mathbb{Q}(\sqrt{-\Delta})$. Assume that $\mathbb{K}$ is totally real, in [DP70, Théorèmes II.9 and II.10], Damey & Payan proved the following inequality (the so called *Spiegelungssatz* for the 4-rank, see [Leo58]):

$$\mathrm{Rank}_4(\mathbb{K}) \leq \mathrm{Rank}_4(\mathbb{K}^{\#}) \leq \mathrm{Rank}_4(\mathbb{K}) + 1.$$

In this article, we provide a combinatorial proof of this *Spiegelungssatz* using expressions involving character sums due to Fouvry & Kluners [FK07]. The letter D will always denote a positive, odd, squarefree integer.

Let $d_{\mathbb{K}}$ be the discriminant of the real quadratic field $\mathbb{K}$ and $d^{\#}_{\mathbb{K}}$ be the discriminant of the imaginary quadratic field $\mathbb{K}^{\#}$. The usual computation of the discriminant allows to consider three families of quadratic fields. This families are described table 1.

$d_{\mathbb{K}}$	$1 \pmod 4$	$0 \pmod 8$	$4 \pmod 8$
$d_{\mathbb{K}}$	D	$8D$	$4D$
$d^{\#}_{\mathbb{K}}$	$-4D$	$-8D$	$-D$
$d^{\#}_{\mathbb{K}}$	$4 \pmod 8$	$0 \pmod 8$	$1 \pmod 4$
D	$1 \pmod 4$		$-1 \pmod 4$
$\mathbb{K}$	$\mathbb{Q}(\sqrt{D})$	$\mathbb{Q}(\sqrt{2D})$	$\mathbb{Q}(\sqrt{D})$

TABLE 1. Link between D, $d_{\mathbb{K}}$ and their reflections.

We introduce for any integers u and v coprime with D the cardinality

$$\mathcal{E}_D(u,v) := \#\{(a,b) \in \mathbb{N}^2 : D = ab,\ ua \equiv \square \pmod b,\ vb \equiv \square \pmod a\}$$

where $x \equiv \square \pmod y$ means that x is the square of an integer modulo y. Using table 1, we find in [FK07] (where what the authors note D is what we note $d_{\mathbb{K}}$ or $d^{\#}_{\mathbb{K}}$) the following expressions for the 4-rank of $\mathbb{K}$ and $\mathbb{K}^{\#}$.

1) If $d_{\mathbb{K}} \equiv 1 \pmod 4$, then

$$2^{\mathrm{Rank}_4(\mathbb{K})} = \frac{1}{2}\mathcal{E}_D(-1,1)$$

[FK07, Lemma 27] and

$$2^{\mathrm{Rank}_4(\mathbb{K}^{\#})} = \frac{1}{2}\left(\mathcal{E}_D(1,1) + \mathcal{E}_D(2,2)\right)$$

[FK07, Lemma 40] with $D \equiv 1 \pmod 4$.

2) If $d_{\mathbb{K}} \equiv 0 \pmod 8$, then

$$2^{\mathrm{Rank}_4(\mathbb{K})} = \frac{1}{2}\left(\mathcal{E}_D(-2,1) + \mathcal{E}_D(-1,2)\right)$$

[FK07, Lemma 38] and

$$2^{\mathrm{Rank}_4(\mathbb{K}^{\#})} = \mathcal{E}_D(2,1)$$

[FK07, Lemma 33].

3) If $d_{\mathbb{K}} \equiv 4 \pmod 8$, then

$$2^{\mathrm{Rank}_4(\mathbb{K})} = \frac{1}{2}\left(\mathcal{E}_D(-1,1) + \mathcal{E}_D(-2,2)\right)$$

[FK07, Lemma 42] and

$$2^{\mathrm{Rank}_4(\mathbb{K}^\#)} = \frac{1}{2}\mathcal{E}_D(1,1)$$

[FK07, Lemma 16] with $D \equiv 3 \pmod 4$.

Remark-- These expressions of $2^{\mathrm{Rank}_4(\mathbb{K})}$ and $2^{\mathrm{Rank}_4(\mathbb{K}^\#)}$ either have one term or are a sum of two terms. In case they have one term, it can not be zero and this term is a power of 2. In case they are sum of two terms, we will show that each of these terms is either zero or a power of two ; then considering the solutions of the equation $2^a = 2^b + 2^c$, we see that either one term (and only one) is zero or the two terms are equal.

To prove Damey & Payan *Spiegelungssatz*, we have then to prove the three following inequalities.

1) If $D \equiv 1 \pmod 4$ then

$$\mathcal{E}_D(-1,1) \le \mathcal{E}_D(1,1) + \mathcal{E}_D(2,2) \le 2\mathcal{E}_D(-1,1). \tag{1}$$

2) For any D,

$$\mathcal{E}_D(-2,1) + \mathcal{E}_D(-1,2) \le 2\mathcal{E}_D(2,1) \le 2\mathcal{E}_D(-2,1) + 2\mathcal{E}_D(-1,2). \tag{2}$$

3) If $D \equiv 3 \pmod 4$ then

$$\mathcal{E}_D(-1,1) + \mathcal{E}_D(-2,2) \le \mathcal{E}_D(1,1) \le 2\mathcal{E}_D(-1,1) + 2\mathcal{E}_D(-2,2). \tag{3}$$

In section 1, we establish a formula for $\mathcal{E}_D(u,v)$ involving Jacobi characters. We average this formula over a group of order 8 generated by three permutations. We deduce properties for $\mathcal{E}_D(u,v)$ from this formula. In section 2, we give an interpretation of $\mathcal{E}_D(u,v)$ in terms of the cardinality of an affine space. In particular, this shows that $\mathcal{E}_D(u,v)$ is either 0 or a power of 2. Finally, in section 3, we combine the character sum interpretation with the affine interpretation to deduce the *Spiegelungssatz*. We also prove the equality cases found by Uehara [Ueh89, Theorem 2] and give a new one.

1. A character sum

Denote by $\left(\frac{m}{n}\right)$ the Jacobi symbol of m and n, for any coprime odd integers m and n. The letter p will always denote a prime number. For any integers s, t, u and v coprime with D, we introduce the sum

$$\sigma_D(s,t,u,v) = \sum_{ab=D} \prod_{p|b}\left(\left(\frac{s}{p}\right) + \left(\frac{ua}{p}\right)\right) \prod_{p|a}\left(\left(\frac{t}{p}\right) + \left(\frac{vb}{p}\right)\right).$$

We have

$$\sigma_D(1,1,u,v) = \sum_{ab=D} \prod_{p|b}\left(1 + \left(\frac{ua}{p}\right)\right) \prod_{p|a}\left(1 + \left(\frac{vb}{p}\right)\right) =: S_D(u,v).$$

This last sum is nonnegative and related to our problem by the easy equality

$$\mathcal{E}_D(u,v) = 2^{-\omega(D)} S_D(u,v) \tag{4}$$

where $\omega(D)$ stands for the number of prime divisors of D. The aim of this section is to establish some properties of σ_D.

We note the symmetry relation

$$\sigma_D(s,t,u,v) = \sigma_D(t,s,v,u)$$

which gives $S_D(u,v) = S_D(v,u)$. The factorisation

$$\sigma_D(s,t,u,v) = \sum_{ab=D} \left(\frac{s}{b}\right)\left(\frac{t}{a}\right) \prod_{p|b}\left(1+\left(\frac{sua}{p}\right)\right) \prod_{p|a}\left(1+\left(\frac{tvb}{p}\right)\right) \tag{5}$$

implies the upper bound

$$|\sigma_D(s,t,u,v)| \leq S_D(su,tv). \tag{6}$$

Finally, we shall use the elementary formula

$$2(-1)^{xy+yz+zx} = (-1)^x + (-1)^y + (-1)^z - (-1)^{x+y+z} \tag{7}$$

valid for any integers x, y and z.

We introduce the element $\beta(n) \in \mathbb{F}_2$ by

$$\left(\frac{-1}{n}\right) = (-1)^{\beta(n)}.$$

If m and n are coprime, the multiplicativity of the Jacobi symbol gives $\beta(m) + \beta(n) = \beta(mn)$. With this notation the quadratic reciprocity law reads

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\beta(m)\beta(n)}. \tag{8}$$

We shall combine (7) and (8) to get the linearisation formula

$$2\left(\frac{x}{y}\right)\left(\frac{y}{z}\right)\left(\frac{z}{x}\right)\left(\frac{x}{z}\right)\left(\frac{z}{y}\right)\left(\frac{y}{x}\right) = \left(\frac{-1}{x}\right)+\left(\frac{-1}{y}\right)+\left(\frac{-1}{z}\right)-\left(\frac{-1}{xyz}\right).$$

Lemma 1– *For any integers s, t, u, v coprime with D, the following equality*

$$\sigma_D(s,t,u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{s}{b}\right)\left(\frac{t}{a}\right)\left(\frac{u}{d}\right)\left(\frac{v}{c}\right)$$

holds.

Proof. By bimultiplicativity of the Jacobi symbol, equation (5) gives

$$\sigma_D(s,t,u,v) = \sum_{ab=D} \left(\frac{s}{b}\right)\left(\frac{t}{a}\right) \sum_{d|b}\left(\frac{usa}{d}\right) \sum_{c|a}\left(\frac{tvb}{c}\right).$$

By the change of variables $(a,b,c,d) = (\alpha\gamma, \beta\delta, \gamma, \delta)$, we get

$$\sigma_D(s,t,u,v) = \sum_{D=\alpha\beta\gamma\delta} \left(\frac{s}{\beta}\right)\left(\frac{u}{\delta}\right)\left(\frac{v}{\gamma}\right)\left(\frac{t}{\alpha}\right)\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right)\left(\frac{\alpha}{\delta}\right)\left(\frac{\beta}{\gamma}\right)$$

and we conclude using the quadratic reciprocity law (8) to $\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right)$. □

To build symmetry, we average the formula in lemma 1 over an order 8 group, namely the group generated by three permutations: the permutation (a,d), the permutation (b,c) and the permutation $((a,b),(d,c))$. The quadratic reciprocity law allows to factorise the term $(-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)$ in every transformed sum and then to see u and v as describing the action of each permutation.

Proposition 2– *For any integers* s,t,u,v *coprime with* D*, the following equality*

$$\begin{aligned}8S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\times\\ \Big[2\left(\frac{u}{d}\right)\left(\frac{v}{c}\right)+\left(\frac{u}{a}\right)\left(\frac{v}{c}\right)\left(\left(\frac{-1}{a}\right)+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)-\left(\frac{-1}{acd}\right)\right)\\ +\left(\frac{u}{d}\right)\left(\frac{v}{b}\right)\left(\left(\frac{-1}{b}\right)+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)-\left(\frac{-1}{bcd}\right)\right)\\ +\left(\frac{u}{a}\right)\left(\frac{v}{b}\right)\left(1+\left(\frac{-1}{ac}\right)+\left(\frac{-1}{bd}\right)-\left(\frac{-1}{D}\right)\right)\Big].\end{aligned}$$

holds.

Proof. From lemma 1 follows

$$S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{u}{d}\right)\left(\frac{v}{c}\right). \tag{9}$$

We permute a and d and use the quadratic reciprocity law (8) to obtain

$$\begin{aligned}S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{u}{a}\right)\left(\frac{v}{c}\right)\\ \times(-1)^{\beta(c)\beta(d)+\beta(d)\beta(a)+\beta(a)\beta(c)}.\end{aligned}$$

Formula (7) gives

$$\begin{aligned}2S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{u}{a}\right)\left(\frac{v}{c}\right)\\ \times\left(\left(\frac{-1}{a}\right)+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)-\left(\frac{-1}{acd}\right)\right).\end{aligned} \tag{10}$$

Similary, we permute b and c, then use the quadratic reciprocity law (8) and formula (7) to get

$$\begin{aligned}2S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{u}{d}\right)\left(\frac{v}{b}\right)\\ \times\left(\left(\frac{-1}{b}\right)+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)-\left(\frac{-1}{bcd}\right)\right).\end{aligned} \tag{11}$$

Finally, we permute (a,b) and (b,c), apply twice the quadratic reciprocity law (8) to get

$$2S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{u}{a}\right)\left(\frac{v}{b}\right) \times (-1)^{\beta(c)\beta(d)+\beta(b)\beta(a)+\beta(a)\beta(d)+\beta(b)\beta(c)}.$$

Since $\beta(c)\beta(d)+\beta(b)\beta(a)+\beta(a)\beta(d)+\beta(b)\beta(c) = \beta(ac)\beta(bd)$, using formula (7) with $z=0$ we get

$$2S_D(u,v) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{u}{a}\right)\left(\frac{v}{b}\right) \times \left(1+\left(\frac{-1}{ac}\right)+\left(\frac{-1}{bd}\right)-\left(\frac{-1}{D}\right)\right). \tag{12}$$

We obtain the result by adding twice (9) with the sum of (10), (11) and (12). □

When two expressions are equivalent under the action of the symmetry group, we get an identity. We give two such formulas in the next two corollaries.

***Corollary* 3–** *If* $D \equiv 1 \pmod 4$ *then* $S_D(-1,1) = S_D(1,1)$.

Proof. For any D, we obtain from proposition 2 the formula

$$8\,(S_D(1,1) - S_D(-1,1)) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right) \times \left(1-\left(\frac{-1}{D}\right)\right)\left(1+\left(\frac{-1}{b}\right)\right)\left(1+\left(\frac{-1}{c}\right)\right). \tag{13}$$

This gives the result since $\left(\frac{-1}{D}\right) = 1$ if $D \equiv 1 \pmod 4$. □

***Corollary* 4–** *If* $D \equiv 3 \pmod 4$ *then* $S_D(1,1) = 2S_D(-1,1)$.

Proof. For any D, proposition 2 gives

$$8S_D(1,-1) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left[2+\left(\frac{-1}{b}\right)+2\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)+\left(\frac{-1}{ac}\right)+\left(\frac{-1}{bd}\right)+\left(\frac{-1}{bc}\right)-\left(\frac{-1}{ad}\right)+\left(\frac{-1}{abc}\right)-\left(\frac{-1}{acd}\right)\right].$$

Thanks to (13), we deduce for any D the equality

$$-8\,(S_D(1,1) - S_D(-1,1) - S_D(1,-1)) = \sum_{abcd=D} (-1)^{\beta(c)\beta(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right) \times \left[1+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)+\left(\frac{-1}{ac}\right)+\left(\frac{-1}{bd}\right)+\left(\frac{-1}{abc}\right)+\left(\frac{-1}{abd}\right)+\left(\frac{-1}{D}\right)\right].$$

It follows that

$$-8\left(S_D(1,1)-S_D(-1,1)-S_D(1,-1)\right)=\sum_{abcd=D}(-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\times \left(1+\left(\frac{-1}{D}\right)\right)\left(1+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)+\left(\frac{-1}{ac}\right)\right).$$

This finishes the proof since $\left(\frac{-1}{D}\right)=-1$ if $D\equiv 3 \pmod 4$. □

Finally, after having dealt with equalities, we shall need the following inequalities.

***Lemma* 5–** *For any* D, *for any* u *coprime with* D, *the following inequalities*

$$S_D(u,1)\le S_D(-u,1)+S_D(u,-1)\le 2S_D(u,1)$$

hold.

Proof. We prove first the inequality

$$S_D(-u,1)+S_D(u,-1)\le 2S_D(u,1). \tag{14}$$

With proposition 2, we write

$$\begin{aligned}8\left(S_D(-u,1)+S_D(u,-1)\right)=\sum_{abcd=D}(-1)^{\beta(c)\beta(d)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\times\\ \left[2\left(\frac{u}{d}\right)\left(1+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)+\left(\frac{-1}{bd}\right)\right)\right.\\ +\left(\frac{u}{a}\right)\left(2+\left(\frac{-1}{a}\right)+\left(\frac{-1}{b}\right)+\left(\frac{-1}{c}\right)+\left(\frac{-1}{d}\right)+2\left(\frac{-1}{ac}\right)\right.\\ \left.\left.+\left(\frac{-1}{abd}\right)+\left(\frac{-1}{abc}\right)-\left(\frac{-1}{acd}\right)-\left(\frac{-1}{bcd}\right)\right)\right].\end{aligned}$$

Using

$$\left(\frac{-1}{xyz}\right)=\left(\frac{-1}{D}\right)\left(\frac{-1}{t}\right) \tag{15}$$

for any $\{x,y,z,t\}=\{a,b,c,d\}$ together with (9) and lemma 1 we deduce

$$\begin{aligned}8\left(S_D(-u,1)+S_D(u,-1)\right)&=2\left(S_D(u,1)+S_D(u,-1)+S_D(-u,1)\right)\\ &+2\left(\sigma_D(-1,1,-u,1)+\sigma_D(1,u,1,1)+\sigma_D(1,-u,1,-1)\right)\\ &+\left(1-\left(\frac{-1}{D}\right)\right)\left(\sigma_D(1,-u,1,1)+\sigma_D(-1,u,1,1)\right)\\ &+\left(1+\left(\frac{-1}{D}\right)\right)\left(\sigma_D(1,u,1,-1)+\sigma_D(1,u,-1,1)\right).\end{aligned}$$

Since $1-\left(\frac{-1}{D}\right)$ and $1+\left(\frac{-1}{D}\right)$ are nonnegative, the upper bound (6) gives

$$8\left(S_D(-u,1)+S_D(u,-1)\right)\le 4\left(2S_D(u,1)+S_D(u,-1)+S_D(-u,1)\right)$$

hence (14). We prove next the inequality

$$S_D(u,1)\le S_D(-u,1)+S_D(u,-1). \tag{16}$$

As for (14), we use equation (15), proposition 2, equation (9) and lemma 1 to get

$$\begin{aligned}8S_D(u,1) = {} & 2S_D(u,1) + S_D(u,-1) + S_D(-u,1) \\ & + \sigma_D(1,-u,1,1) + \sigma_D(1,u,1,-1) + \sigma_D(1,u,-1,1) + \sigma_D(-1,1,u,1) \\ & + \left(1+\left(\frac{-1}{D}\right)\right)\sigma_D(1,-u,1,-1) + \left(1-\left(\frac{-1}{D}\right)\right)\sigma_D(1,u,1,1) \\ & - \left(\frac{-1}{D}\right)\left(\sigma_D(-1,u,1,1) + \sigma_D(1,-1,u,1)\right).\end{aligned}$$

Then (6) leads to

$$8S_D(u,1) \leq 4\left(S_D(u,1) + S_D(u,-1) + S_D(-u,1)\right)$$

hence (16). □

2. An affine interpretation

We write $p_1 < \cdots < p_{\omega(D)}$ for the prime divisors of D and define a bijection between the set of divisors a of D and the set of sequences $(x_i)_{1\leq i\leq \omega(D)}$ in $\mathbb{F}_2^{\omega(D)}$ by

$$x_i = \begin{cases} 1 & \text{if } p_i \mid a \\ 0 & \text{otherwise.}\end{cases}$$

Let a and b satisfy $D = ab$ and u and v two integers coprime with D. We extend the notation of the previous section writing

$$\left(\frac{a}{b}\right) = (-1)^{\alpha(a,b)} = (-1)^{\beta_a(b)}$$

with $\alpha(a,b) = \beta_a(b) \in \mathbb{F}_2$. The condition that vb is a square modulo a is equivalent to $\left(\frac{vb}{p}\right) = 1$ for any prime divisor p of a, that is

$$\left(\frac{v}{p_i}\right)\prod_{j:\, x_j=0}\left(\frac{p_j}{p_i}\right) = 1$$

for any i such that $x_i = 1$. With our notation, this gives

$$\forall i,\ x_i = 1 \Longrightarrow (-1)^{\beta_v(p_i)}(-1)^{\sum_{j:\, x_j=0}\alpha(p_j,p_i)} = 1.$$

We rewrite it

$$\forall i,\ x_i = 1 \Longrightarrow (-1)^{\beta_v(p_i)}(-1)^{\sum_{j\neq i}(1-x_j)\alpha(p_j,p_i)} = 1$$

and so

$$\forall i,\ x_i\beta_v(p_i) + \sum_{j\neq i} x_i(1-x_j)\alpha(p_j,p_i) = 0. \tag{17}$$

Similary, the condition that ua is a square modulo b is equivalent to

$$\forall i,\ (1-x_i)\beta_u(p_i) + \sum_{j\neq i}(1-x_i)x_j\alpha(p_j,p_i) = 0. \tag{18}$$

Since x_i is either 0 or 1, equations (17) et (18) are equivalent to their sum. We deduce the following lemma.

***Lemma* 6–** *The cardinality $\mathcal{E}_D(u,v)$ is the cardinality of the affine space $\mathcal{F}_D(u,v)$ in $\mathbb{F}_2^{\omega(D)}$ of equations*

$$\left(\beta_u(p_i)+\beta_v(p_i)+\sum_{j\neq i}\alpha(p_j,p_i)\right)x_i+\sum_{j\neq i}\alpha(p_j,p_i)x_j=\beta_u(p_i)$$

for all $i\in\{1,\dots,\omega(D)\}$.

Remark-- In particular, lemma 6 shows that $\mathcal{E}_D(u,v)$ if not zero is a power of 2, the power being the dimension of the direction of $\mathcal{F}_D(u,v)$. This is not *a priori* obvious.

Remark-- This interpretation slightly differs from the one found by Redei [Red34, Ger84]. The matrix with coefficients in $\mathbb{F}_2$ associated to our affine space is $(a_{ij})_{1\leq i,j\leq\omega(D)}$ with

$$a_{ij}=\begin{cases}\alpha(p_j,p_i) & \text{if } i\neq j\\ \beta_u(p_i)+\beta_v(p_i)+\sum_{\ell\neq i}\alpha(p_\ell,p_i) & \text{if } i=j\end{cases}$$

whereas the matrix considered by Redei is $(\widetilde{a}_{ij})_{1\leq i,j\leq\omega(D)}$ with

$$\widetilde{a}_{ij}=\begin{cases}\alpha(p_j,p_i) & \text{if } i\neq j\\ \omega(D)+1+\sum_{\ell\neq i}\alpha(p_\ell,p_i) & \text{if } i=j.\end{cases}$$

***Corollary* 7–** *For any D, we have $S_D(1,1)\neq 0$ and, either $S_D(2,2)=0$ or $S_D(2,2)=S_D(1,1)$.*

Proof. The affine space $\mathcal{F}_D(2,2)$ has equations

$$\left(\sum_{j\neq i}\alpha(p_j,p_i)\right)x_i+\sum_{j\neq i}\alpha(p_j,p_i)x_j=\beta_2(p_i)$$

for all $i\in\{1,\dots,\omega(D)\}$. The affine space $\mathcal{F}_D(1,1)$ has equations

$$\left(\sum_{j\neq i}\alpha(p_j,p_i)\right)x_i+\sum_{j\neq i}\alpha(p_j,p_i)x_j=0$$

for all $i\in\{1,\dots,\omega(D)\}$. Hence, both spaces have the same direction, and same dimension. The space $\mathcal{F}_D(1,1)$ is not empty: it contains $(1,\dots,1)$. Its cardinality is then $2^{\dim_{\mathbb{F}_2}\mathcal{F}_D(1,1)}$. The affine space $\mathcal{F}_D(2,2)$ might be empty and, if it is not, then its cardinality is $2^{\dim_{\mathbb{F}_2}\mathcal{F}_D(2,2)}=2^{\dim_{\mathbb{F}_2}\mathcal{F}_D(1,1)}$. It follows that $\mathcal{E}_D(1,1)\neq 0$ and, either $\mathcal{E}_D(2,2)=0$ or $\mathcal{E}_D(2,2)=\mathcal{E}_D(1,1)$. We finish the proof thanks to (4). □

***Corollary* 8–** *For any D, we have $S_D(-1,1)\neq 0$ and, either $S_D(-2,2)=0$ or $S_D(-2,2)=S_D(-1,1)$.*

Proof. Since $\beta_{-2}(p_i) + \beta_2(p_i) = \beta_{-1}(p_i)$, the affine space $\mathcal{F}_D(-2,2)$ has equations

$$\left(\beta_{-1}(p_i) + \sum_{j\neq i} \alpha(p_j,p_i)\right) x_i + \sum_{j\neq i} \alpha(p_j,p_i)x_j = \beta_{-2}(p_i)$$

for all $i \in \{1,\dots,\omega(D)\}$. The affine space $\mathcal{F}_D(-1,1)$ has equations

$$\left(\beta_{-1}(p_i) + \sum_{j\neq i} \alpha(p_j,p_i)\right) x_i + \sum_{j\neq i} \alpha(p_j,p_i)x_j = \beta_{-1}(p_i)$$

for all $i \in \{1,\dots,\omega(D)\}$. Hence, both spaces have the same direction, and same dimension. The space $\mathcal{F}_D(-1,1)$ is not empty: it contains $(1,\dots,1)$. It follows that $\mathcal{E}_D(-1,1) \neq 0$ and, either $\mathcal{E}_D(-2,2) = 0$ or $\mathcal{E}_D(-2,2) = \mathcal{E}_D(-1,1)$. We finish the proof thanks to (4). □

3. Damey-Payan Spiegelungssatz

3.1. **Proof of the Spiegelungssatz.** We have to prove (1), (2) and (3).

Consider the case $d_{\mathbb{K}} \equiv 1 \pmod 4$. Recall that $D = d_{\mathbb{K}}$. Thanks to (4), equation (1) is

$$S_D(-1,1) \leq S_D(1,1) + S_D(2,2) \leq 2S_D(-1,1)$$

for any $D \equiv 1 \pmod 4$. By corollary 3, this inequality is equivalent to $S_D(2,2) \leq S_D(1,1)$ and this last inequality is implied by corollary 7.

Consider the case $d_{\mathbb{K}} \equiv 0 \pmod 8$. Recall that $D = d_{\mathbb{K}}/8$. Thanks to (4), equation (2) is

$$S_D(2,1) \leq S_D(-2,1) + S_D(2,-1) \leq 2S_D(2,1)$$

for any D. This is implied by lemma 5 with $u = 2$.

Finally, consider the case $d_{\mathbb{K}} \equiv 4 \pmod 8$. Recall that $D = d_{\mathbb{K}}/4$. Thanks to (4), equation (3) is

$$S_D(-1,1) + S_D(-2,2) \leq S_D(1,1) \leq 2S_D(-1,1) + 2S_D(-2,2)$$

for any $D \equiv 3 \pmod 4$. By corollary 4, this inequality is equivalent to $S_D(-2,2) \leq S_D(-1,1)$ and this last inequality is implied by corollary 8.

3.2. **Some equality cases.** It is clear from our previous computations that

- if $d_{\mathbb{K}} \equiv 1 \pmod 4$ then

$$\mathrm{Rank}_4(\mathbb{K}^{\#}) = \begin{cases} \mathrm{Rank}_4(\mathbb{K}) & \text{if } \mathcal{E}_D(2,2) = 0 \\ \mathrm{Rank}_4(\mathbb{K}) + 1 & \text{otherwise;} \end{cases}$$

- if $d_{\mathbb{K}} \equiv 4 \pmod 8$ then

$$\mathrm{Rank}_4(\mathbb{K}^{\#}) = \begin{cases} \mathrm{Rank}_4(\mathbb{K}) + 1 & \text{if } \mathcal{E}_D(-2,2) = 0 \\ \mathrm{Rank}_4(\mathbb{K}) & \text{otherwise.} \end{cases}$$

We do not have such clear criterium in the case $d_{\mathbb{K}} \equiv 0 \pmod 8$. The reason is that our study of the cases $d_{\mathbb{K}} \equiv 1 \pmod 4$ and $d_{\mathbb{K}} \equiv 4 \pmod 8$ rests on equalities (corollaries 3, 4, 7 and 8) whereas, our study of the case $d_{\mathbb{K}} \equiv 0 \pmod 8$ rests on inequalities (lemma 5 and mainly equation (6)). We study more explicitely special cases in proving the following proposition due to Uehara [Ueh89, Theorem 2] (the case c seems to be new).

***Theorem* 9**– *Let* $\mathbb{K}$ *be a real quadratic field of discriminant* $d_{\mathbb{K}}$ *and* D *be described in table 1. Suppose that every prime divisors of* D *is congruent to* ± 1 *modulo* 8. *Then*

a) If $d_{\mathbb{K}} \equiv 1 \pmod 4$, *then* $\mathrm{Rank}_4(\mathbb{K}^{\#}) = \mathrm{Rank}_4(\mathbb{K}) + 1$.
b) If $d_{\mathbb{K}} \equiv 0 \pmod 8$ *and* $D \equiv -1 \pmod 4$, *then* $\mathrm{Rank}_4(\mathbb{K}^{\#}) = \mathrm{Rank}_4(\mathbb{K}) + 1$.
c) If $d_{\mathbb{K}} \equiv 0 \pmod 8$ *and* $D \equiv 1 \pmod 4$, *then* $\mathrm{Rank}_4(\mathbb{K}^{\#}) = \mathrm{Rank}_4(\mathbb{K})$.
d) If $d_{\mathbb{K}} \equiv 4 \pmod 8$, *then* $\mathrm{Rank}_4(\mathbb{K}) = \mathrm{Rank}_4(\mathbb{K}^{\#})$.

Proof. Since every prime divisors of D is congruent to ± 1 modulo 8, we have $\beta_2(p_i) = 0$ for any i.

- If $d_{\mathbb{K}} \equiv 1 \pmod 4$, then $D \equiv 1 \pmod 4$. By lemma 6, we know that $\mathcal{E}_D(2,2)$ is the cardinality of an affine space having equations
$$\sum_{j \neq i} \alpha(p_j, p_i)(x_i + x_j) = 0 \quad (1 \leq i \leq \omega(D))$$
hence it is non zero ($x_i = 1$ for any i gives a solution).
- If $d_{\mathbb{K}} \equiv 0 \pmod 8$, then
$$2^{\mathrm{Rank}_4(\mathbb{K}^{\#}) - \mathrm{Rank}_4(\mathbb{K})} = \frac{2\mathcal{E}_D(2,1)}{\mathcal{E}_D(-2,1) + \mathcal{E}_D(-1,2)}.$$
Since $\beta_{-2}(p_i) = \beta_{-1}(p_i)$ for any i, lemma 6 shows that $\mathcal{E}_D(-2,1) = \mathcal{E}_D(-1,2) = \mathcal{E}_D(-1,1)$. Lemma 6 also shows that $\mathcal{E}_D(2,1) = \mathcal{E}_D(1,1)$, hence
$$2^{\mathrm{Rank}_4(\mathbb{K}^{\#}) - \mathrm{Rank}_4(\mathbb{K})} = \frac{\mathcal{E}_D(1,1)}{\mathcal{E}_D(-1,1)}.$$
If $D \equiv -1 \pmod 4$, corollary 4 implies that
$$2^{\mathrm{Rank}_4(\mathbb{K}^{\#}) - \mathrm{Rank}_4(\mathbb{K})} = 2$$
whereas, if $D \equiv 1 \pmod 4$, corollary 3 implies that
$$2^{\mathrm{Rank}_4(\mathbb{K}^{\#}) - \mathrm{Rank}_4(\mathbb{K})} = 1.$$
- If $d_{\mathbb{K}} \equiv 4 \pmod 8$, then $D \equiv -1 \pmod 4$. By lemma 6, we know that $\mathcal{E}_D(-2,2)$ is the cardinality of an affine space having equations
$$\beta_{-1}(p_i)x_i + \sum_{j \neq i} \alpha(p_j, p_i)(x_i + x_j) = \beta_{-1}(p_i) \quad (1 \leq i \leq \omega(D))$$
hence it is non zero ($x_i = 1$ for any i gives a solution).

□

Remark-- Probabilistic results have been given by Gerth[Ger01] and, for a more natural probability by Fouvry & Kluners in [FK10b]. Among other results, Fouvry & Kluners prove that

$$\lim_{X\to+\infty} \frac{\#\left\{d_{\mathbb{K}} \in \mathcal{D}(X):\ \mathrm{Rank}_4(\mathbb{K}^{\#}) = s \middle| \mathrm{Rank}_4(\mathbb{K}) = r\right\}}{\#\mathcal{D}(X)} = \begin{cases} 1-2^{-r-1} & \text{if } r = s \\ 2^{-r-1} & \text{if } r = s-1 \\ 0 & \text{otherwise.} \end{cases}$$

where $\mathcal{D}(X)$ is the set of fundamental discriminants in $]0, X]$.

References

[DP70] Pierre Damey and Jean-Jacques Payan, *Existence et construction des extensions galoisiennes et non-abéliennes de degré* 8 *d'un corps de caractéristique différente de* 2, J. Reine Angew. Math. **244** (1970), 37–54. MR MR0280466 (43 #6186)

[FK07] Étienne Fouvry and Jurgen Kluners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), no. 3, 455–513. MR MR2276261 (2007k:11187)

[FK10a] ———, *On the negative Pell equation*, Ann. of Math. (2) **172** (2010), no. 3, 2035–2104. MR 2726105

[FK10b] ———, *On the Spiegelungssatz for the 4-rank*, Algebra Number Theory **4** (2010), no. 5, 493–508. MR 2679097

[Ger84] Frank Gerth, III, *The* 4*-class ranks of quadratic fields*, Invent. Math. **77** (1984), no. 3, 489–515. MR 759260 (85j:11137)

[Ger01] ———, *Comparison of 4-class ranks of certain quadratic fields*, Proc. Amer. Math. Soc. **129** (2001), no. 9, 2547–2552 (electronic). MR 1838376 (2002c:11149)

[Leo58] Heinrich-Wolfgang Leopoldt, *Zur Struktur der* l*-Klassengruppe galoisscher Zahlkorper*, J. Reine Angew. Math. **199** (1958), 165–174. MR 0096633 (20 #3116)

[Red34] L. Redei, *Arithmetischer Beweis des Satzes uber die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkorper.*, J. Reine Angew. Math. **171** (1934), 55–60 (German).

[Ueh89] Tsuyoshi Uehara, *On the* 4*-rank of the narrow ideal class group of a quadratic field*, J. Number Theory **31** (1989), no. 2, 167–173. MR 987569 (90e:11170)

Université de Lyon, CNRS, Université Lyon 1, INSA, Ecole Centrale de Lyon, UMR5208, Institut Camille Jordan, 43 blvd du 11 novembre 1918, F-69622 Villeurbanne-Cedex, France

E-mail address: laurent.habsieger@math.univ-lyon1.fr

Emmanuel Royer, Clermont Université, Université Blaise Pascal, Laboratoire de mathématiques, BP 10448, F-63000 Clermont-Ferrand, France

Current address: Emmanuel Royer, Université Blaise Pascal, Laboratoire de mathématiques, Les Cézeaux, BP 80026, F-63171 Aubière Cedex, France

E-mail address: emmanuel.royer@math.univ-bpclermont.fr