Degree in Mathematics

Title: Exotic forms of weight 1

Author: Pol Torrent i Soler

Advisor: Jordi Quer Bosor

Department: Mathematics

Academic year: 2015/16

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Bachelor's degree thesis

Exotic forms of weight 1

Pol Torrent i Soler

Advisor: Jordi Quer Bosor

Department of Mathematics

Contents

Introduction

Many mathematical objects of great importance in Number Theory, such as number fields and elliptic curves, have associated a Dirichlet series: complex valued functions of the form $\sum_{n\geq 1} a_n n^{-s}$. For example, the Dirichlet series associated to the number field $\mathbb{Q}$ is the famous Riemann zeta function $\zeta(s) = \sum_{n\geq 1} n^{-s}$, which has been used for the study of the distribution of prime numbers, among other things. In some cases, the function $\sum a_n q^n$, with $q = e^{2\pi i z}$ and z in the upper half plane, is a modular form. Proving that for a given Dirichlet series the corresponding function is a modular form can be an extremely difficult problem. For example, for the Dirichlet series associated to elliptic curves this is the Shimura-Taniyama conjecture, proved by Wiles in his celebrated proof of Fermat's Last Theorem. But, in those cases, the modularity can be used to infer properties of the initial object. For this reason, modular forms are very relevant objects in Number Theory.

Dirichlet series can be also associated to Galois representations $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_m(\mathbb{C})$, linear representations of the Galois group of an extension of number fields L/K. In this case the coefficients a_n can be given in terms of the coefficients of the characteristic polynomial of the images by ρ of some elements of $\mathrm{Gal}(L/K)$, the so-called Frobenius elements. While is not known whether those Dirichlet series have an associated modular form in general, it has been proved that the answer is affirmative for $m = 2$ and $K = \mathbb{Q}$, the case that we will consider in this thesis.

We present a method that allows to obtain the modular form associated to a Galois representation $\rho : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ in the particular case where $\mathrm{Gal}(L/\mathbb{Q}) \cong \widetilde{\mathfrak{S}_4}$, a double cover of the symmetric group $\mathfrak{S}_4$. Since it is not easy to obtain such an extension directly, we obtain them as solutions to the quadratic embedding problem $\widetilde{\mathfrak{S}_4} \longrightarrow \mathfrak{S}_4 = \mathrm{Gal}(E/\mathbb{Q})$. A characterization of the solvability of this Galois embedding problem was first given by Serre in 1984 (see [**11**]) in terms of an equivalence of quadratic forms, but to obtain the corresponding modular form an explicit expression for the primitive element of that extension was needed. Crespo derived such an expression in 1989 (see, for instance, [**3**] and [**4**]), and finally Bayer and Frey in [**2**] gave the coefficients of the modular form in terms of the properties of a primitive element of the quadratic extension.

While those papers' proofs use techniques that are beyond the scope of this paper, our objective is to develop the basic theory of quadratic forms, Galois embedding problems and modular forms to understand their results, and to implement an algorithm that, given a field extension that has Galois group $\mathfrak{S}_4$ over $\mathbb{Q}$ (which can be given in terms of a polynomial of

degree 4), is able to decide whether the + embedding problem is solvable or not, and, if it is solvable, to compute a primitive element and the associated modular form. The software we will use for the implementation of that algorithm is SageMath.

This work is structured in four chapters, whose contents are listed in the following paragraphs:

Chapter 1. In this chapter we develop the basic theory of quadratic forms over the real, the p-adic and the rational numbers, reaching the Hasse-Minkowski theorem, that states that two quadratic forms are equivalent over the rational numbers if, and only if, they are equivalent over the p-adic numbers and the real numbers, and we give the tools that allow us to check the equivalence over those fields.

Chapter 2. Here we introduce the concept of group extension (with kernel cyclic of order two) and relate it to quadratic Galois extensions, developing the theory that allows the classification of those extensions.

Chapter 3. This chapter contains the statements of the theorems of Serre, Crespo and Bayer mentioned above, as well as some basic theory on modular forms and Galois representations.

Chapter 4. Finally we explain how the algorithm is implemented, describing the key methods and classes of SageMath that are used. We also present some examples of results obtained using our algorithm.

The commented source code of the algorithm can be found in the appendix.

I would like to thank my thesis advisor Jordi Quer for his support and unlimited patience, as well as for all the time he invested in explaining to me new concepts and checking all my work. Thanks to him the development of this thesis has been one of the greatest experiences I had as a college student.

Chapter 1
Quadratic forms

As we said in the introduction, quadratic forms and their equivalences turn out to play a major role in our problem. In this chapter, we aim to state the main results that will allow us to determine whether two rational quadratic forms are equivalent or not and, if they are, to find an explicit equivalence between them. This chapter is intended to develop the concepts and results that will lead to Hasse-Minkowski theorem, that states that two quadratic forms are equivalent over the rationals if, and only if, they are equivalent over all the completions of the rational numbers: the real numbers and the p-adic numbers. We will sketch the proof without proving a few technical results, but the interested reader can find those proofs in [**10**], where most of this theory is developed.

1. Generalities

Although we are mainly interested in quadratic forms with rational coefficients, we will begin by studying the basic properties of quadratic forms with coefficients in a field K which we will assume that has characteristic different of 2.

Definition 1 (Quadratic form). *A* quadratic form *in n variables with coefficients in a field K is an homogeneous polynomial of degree 2*

$$f(X_1, X_2, \ldots, X_n) \in K[X_1, X_2, \ldots, X_n]$$

Since K is not of characteristic 2, a quadratic form can be written in the form

$$f(X_1, X_2, \ldots, X_n) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j = \sum_{i=1}^{n} a_{ii} X_i^2 + \sum_{1 \leq i < j \leq n} 2a_{ij} X_i X_j,$$

with $a_{ij} = a_{ji}$. This leads to the following notation in terms of matrices, where the quadratic form f is represented in terms of a symmetric matrix $A_f = (a_{ij})$:

$$f(\mathbf{X}) = \mathbf{X}^t A_f \mathbf{X} = \begin{pmatrix} X_1 & X_2 & \cdots & X_n \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}$$

The *determinant* of the quadratic form is the determinant of its associated matrix $d(f) = \det(A_f)$. The form is called *regular* or *nonsingular* if $d(f) \neq 0$. The *rank* of the quadratic form is also defined as the rank of its associated matrix, so nonsingular forms have rank equal to their number of variables.

We can now define what does it mean for two quadratic forms to be equivalent:

DEFINITION 2 (Equivalent quadratic forms). *Two quadratic forms f and g are said to be* equivalent *if there exists a linear invertible change of variables which transforms one into the other one, i.e., if it exists an inverible matrix $M = (u_{ij}) \in \mathrm{GL}_n(K)$ such that*

$$g(X_1, \ldots, X_n) = f\left(\sum_{j=1}^{n} u_{1j}X_j, \ldots, \sum_{j=1}^{n} u_{nj}X_j\right).$$

Equivalently, in terms of the matrices A_f and A_g of the quadratic forms f and g, they are equivalent if there exists a matrix $M \in \mathrm{GL}_n(K)$ such that

$$A_g = M^t A_f M.$$

The relation $f \sim g$ if and only if f and g are equivalent quadratic forms is clearly an equivalence relation, and the property of being regular or singular is invariant modulo equivalence, as well as the rank of the quadratic form. The determinants of two equivalent quadratic forms differ in the square $\det(M)^2$, hence the determinant modulo invertible squares is also an invariant of the equivalence class.

A relevant problem that we will have to face is to determine solutions of the equation $f(X_1, \ldots, X_n) = a$ with $a \in K$. The nomenclature used is the following:

DEFINITION 3 (Representation of an element by a quadratic form). *We say that a quadratic form f* represents *an element $a \in K$ if there exists $(x_1, \ldots, x_n) \in K^n \setminus \{(0, \ldots, 0)\}$ such that $f(x_1, \ldots, x_n) = a$. Such a vector is called a* representation of a by f.

We notice that equivalent quadratic forms represent exactly the same elements of K. It is also clear that if a quadratic form represents a nonzero element $a \in K^*$ it also represents all the elements aK^{*2}, so it suffices to consider the elements zero and those in K^*/K^{*2}. Now we present an elementary result that will turn out to be really useful in our algorithm:

LEMMA 1. *Let $f = \sum_{1 \leq i,j \leq n} a_{ij}X_iX_j$ be a quadratic form. Then f represents all the elements a_{ii}. Additionally, if f represents an element $a \in K$ and $i \in \{1, \ldots, n\}$, then there exists a quadratic form $g = \sum b_{ij}X_iX_j$ equivalent to f such that $b_{ii} = a$.*

PROOF. For the first part, it is enough to consider the i-th element of the canonical base of K^n, $\mathbf{e_i} = (\delta_{ij})_{1 \leq j \leq n}$. Then $f(\mathbf{e_i}) = a_{ii}$.
For the second part let g be a form equivalent to f, and let M be the matrix that gives the equivalence between them. Let $\mathbf{u_i}$ be the i-th column of M. Then

$$f(\mathbf{u_i}) = f(M\mathbf{e_i}) = g(\mathbf{e_i}) = b_{ii},$$

so if we set the i-th column of M to be the representation of a by f and extend it to a base of the space K^n (we will always be able to do this since the representation is a nonzero vector) the resulting quadratic form g will fulfill $b_{ii} = f(\mathbf{u_i}) = a$, as desired. □

The following terms are used to describe which elements are represented by a quadratic form:

DEFINITION 4 (Isotropic and universal forms). *A regular quadratic form is said to be* isotropic *if it does represent zero, or* anisotropic *if it does not. We say that a form is* universal *if it represents all nonzero elements.*

Quadratic forms such that $a_{ij} = 0$ for $i \neq j$ are of interest because of their simpler structure,

$$f(X_1, \ldots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2.$$

Those forms are called *diagonal* quadratic forms since their associated matrices are diagonal. The shorter notation $\langle a_1, \ldots, a_n \rangle$ is often used to describe diagonal quadratic forms. The forms obtained by permuting the elements a_i or multiplying them by squares are equivalent to the original ones. This will allow us to deal with diagonal quadratic forms with integer coefficients instead of rational coefficients when working with equivalences of forms, since we can multiply each a_i by the square of its denominator.

A logical question is to ask which quadratic forms are equivalent to a diagonal quadratic form. The answer is pleasant: all quadratic forms are equivalent to a diagonal quadratic form. This result is an immediate consequence of the following lemma:

LEMMA 2. *Let f be a quadratic form in n variables that represents an element $a \in K^*$. Then f is equivalent to a form of the type $aX_1^2 + f_1(X_2, \ldots, X_n)$, where f_1 is a form in $n-1$ variables.*

PROOF. Let $\mathbf{x}$ be the representation of a by f. In particular, since $\mathbf{x}$ is not the zero vector we can extend it to a base of K^n. Setting the vectors of that base as the columns of a matrix M yields a transformation matrix, since $M \in \mathrm{GL}_n(K)$. Let $g = \sum\sum a_{ij} X^i X^j$ be the quadratic form equivalent to f obtained under the action of the matrix M. By the previous lemma, we will have $a_{11} = a$. Now define the form h to be

$$h(X_1, \ldots, X_n) = g\left(X_1 - \sum_{i=2}^{n} \frac{a_{1i}}{a} X_i, X_2, \ldots, X_n\right)$$

which corresponds to the matrix which is the identity matrix except for the first row, which is $(1, -a_{12}/a, \ldots, -a_{1n}/a)$, resulting in a matrix which is clearly nonsingular. If we apply this transformation to the explicit expression of the terms that contained X_1 in the form g, which are

$$aX_1^2 + \sum_{j=2}^{n} 2a_{1j} X_1 X_j,$$

we get

$$a\left(X_1 - \sum_{i=2}^{n} \frac{a_{1i}}{a} X_i\right)^2 + \sum_{j=2}^{n} 2a_{1j}\left(X_1 - \sum_{i=2}^{n} \frac{a_{1i}}{a} X_i\right) X_j =$$

$$= aX_1^2 - \sum_{i=2}^{n} 2a_{1i} X_1 X_j + \sum_{i,j=2}^{n} \frac{a_{1i} a_{ij}}{a} X_i X_j + \sum_{i=2}^{n} 2a_{1i} X_1 X_j - \sum_{i,j=2}^{n} \frac{2a_{1i} a_{ij}}{a} X_i X_j =$$

$$= aX_1^2 - \sum_{i,j=2}^{n} \frac{a_{1i}a_{ij}}{a} X_i X_j$$

which shows that the form $h \sim f$ is of the form $h(X_1, \ldots, X_n) = aX_1^2 + f_1(X_2, \ldots, X_n)$. □

PROPOSITION 1. *Each quadratic form is equivalent to a diagonal quadratic form.*

PROOF. We proceed by induction on the number of variables n. For $n = 1$ all quadratic forms are already diagonal. Now assume f is a form with n variables. If f only represents zero, then f is the zero form $f(X_1, \ldots, X_n) = 0$ which is diagonal. Otherwise, let $a \in K^*$ be a nonzero element represented by f. Then by the previous lemma $f \sim aX_1 + f_1(X_2, \ldots, X_n)$ and, by the inductive hypothesis, f_1 is equivalent to a diagonal quadratic form, hence f is equivalent to a diagonal form. □

DEFINITION 5 (Orthogonal sum). *Let f and g be quadratic forms in n and m variables respectively. We define its* orthogonal sum *as the quadratic form in $n + m$ variables*

$$(f \perp g)(X_1, \ldots, X_{n+m}) = f(X_1, \ldots, X_n) + g(X_{n+1}, \ldots, X_{n+m}).$$

It is easy to see that the matrix of the sum can be build as follows:

$$A_{f \perp g} = \begin{pmatrix} A_f & 0 \\ 0 & A_g \end{pmatrix}.$$

This implies $d(f \perp g) = d(f)d(g)$, i.e., the determinant is multiplicative with respect to the orthogonal sum, and that if $f_1 \sim g_1$ and $f_2 \sim g_2$ then $f_1 \perp g_1 \sim f_2 \perp g_2$. This operation is also clearly associative and, in terms of the equivalence classes, commutative ($f \perp g \sim g \perp f$). The orthogonal sum also has the property of cancellation:

THEOREM 1 (Witt cancellation theorem). *Let f_1, f_2, g_1 and g_2 be quadratic forms such that $f_1 \perp g_1 \sim f_2 \perp g_2$ and $f_1 \sim g_1$. Then $f_2 \sim g_2$.*

PROOF. First of all, we should notice that changing f_1 and f_2 by a form $f \sim f_1 \sim f_2$ we can assume without loss of generality that $f = f_1 = f_2$.
Assume both g_1 and g_2 are nondegenerate quadratic forms, and that f is the zero form. In this case, the equivalence $f \perp g_1 \sim f \perp g_2$ leads to the identity

$$\begin{pmatrix} 0 & 0 \\ 0 & A_{g_1} \end{pmatrix} = \begin{pmatrix} U^t & W^t \\ V^t & P^t \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & A_{g_2} \end{pmatrix} \begin{pmatrix} U & W \\ V & P \end{pmatrix}$$

where U, V, P, W and the zero matrices have the appropiate size according to the number of variables of g_1 (which is the same as the number of variables of g_2). The previous identity implies $A_{g_1} = P^t A_{g_2} P$. Since g_1 and g_2 are assumed to be nondegenerate, the matrix P is invertible and $g_1 \sim g_2$.
Now assume that f is a nondegenerated quadratic form in one variable, namely $f(X) = aX^2$ with $a \neq 0$. The following matrix identity holds:

$$\begin{pmatrix} a & 0 \\ 0 & A_{g_1} \end{pmatrix} = \begin{pmatrix} u & W^t \\ V^t & P^t \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & A_{g_2} \end{pmatrix} \begin{pmatrix} u & W \\ V & P \end{pmatrix}$$

where $u \in K$, V is a row vector, W a column vector and P a square matrix. Expanding the product we obtain

$$a = au^2 + W^t A_{g_2} W,$$
$$0 = uaV + W^t A_{g_2} P,$$
$$A_{g_1} = V^t a V + P^t A_{g_2} P.$$

Now let $R = P + \lambda WV$ for $\lambda \in K$. Using the previous relations one can get

$$R^t A_{g_2} R = A_{g_1} - a(1 + 2u\lambda + (u^2 - 1)\lambda^2) V^t V,$$

so if $1+2u\lambda+(u^2-1)\lambda^2 = 0$ we will have that $R^t A_{g_2} R = A_{g_1}$. If $u = \pm 1$, the (only) solution of the equation is $\lambda = -1/2u$. If $u^2 \neq 1$, the discriminant of the polynomial is $4 \in K^{*2}$ and the equation has always roots in K. Choosing λ such that the equation is fulfilled and using the fact that g_1 and g_2 are nondegenerate, we obtain $R^t A_{g_2} R = A_{g_1}$ with R invertible, so $g_1 \sim g_2$.

Now assume that f is any quadratic form (we are still assuming that g_1 and g_2 are regular). Then $f \sim \mathbf{0}_r \perp a_1 X_1^2 \perp \cdots \perp a_n X_n^2$, where $\mathbf{0}_r$ is the zero form in r variables and $a_i \neq 0$ for all i. Apply the previous cases to cancel out first the factor $\mathbf{0}_r$ and then each the factors $a_i X_i^2$ (notice that the cofactors will be regular in each cancellation).

Finally consider the general case, where g_1 and g_2 may be degenerate quadratic forms. In this case $g_i \sim \mathbf{0}_{s_i} \perp g_i'$, where g_1' and g_2' are nondegenerate. From the equivalence $f \perp g_1 \sim f \perp g_2$ one obtains that $s_1 = s_2 = s$. Then $f \perp \mathbf{0_s} \perp g_1' \sim f \perp \mathbf{0_s} \perp g_2'$, so $g_1' \sim g_2'$ and $g_1 \sim g_2$. □

The following result concerning representations of elements of the field K by an isotropic quadratic form is also remarkable.

PROPOSITION 2. *Every isotropic quadratic form is also universal, i.e., if a regular quadratic form represents zero, it represents all the elements of K.*

PROOF. Since equivalent quadratic forms represent exactly the same elements we may assume that the quadratic form is diagonal, $f(X_1, \ldots, X_n) = \sum a_i X_i^2$. Let $\mathbf{x} = (x_1, \ldots, x_n) \neq 0$ be a representation of zero by f, $f(\mathbf{x}) = 0$. Let i be such that $x_i \neq 0$ and let $\mathbf{y} = (y_1, \ldots, y_n) \in K^n$ with coordinates

$$y_i = x_i(1 + t),\ y_j = x_j(1 - t),\ j \neq i,\ t \in K.$$

Now we compute

$$f(\mathbf{y}) = a_i x_i^2 (1 + 2t + t^2) + \sum_{j \neq i} a_j x_j^2 (1 - 2t + t^2) = f(\mathbf{x})(1 + t)^2 + 4t x_i^2 a_i = 4t x_i^2 a_i.$$

Now we can solve $f(\mathbf{y}) = 4a_i t x_i^2 = a \in K^*$ for t, $t = a/4a_i x_i^2$, since K is not of characteristic 2, $x_i \neq 0$ by our choice of i and no a_i is zero since the form is regular. □

COROLLARY 1. *A regular form f represents a nonzero element $a \in K^*$ if, and only if, the form $g = \langle -a \rangle \perp f$ represents zero.*

PROOF. If $(x_1, \ldots, x_n)$ is a representation of a by f, then $(1, x_1, \ldots, x_n)$ is a representation of zero by g. Conversely, assume $(x_0, x_1, \ldots, x_n)$ is a representation of zero by f. Then,

if $x_0 \neq 0$, one has that $(x_1/x_0, \ldots, x_n/x_0)$ is a representation of a by f. If $x_0 = 0$ then $f(x_1, \ldots, x_n) = 0$ and f is isotropic and thus universal, and in particular represents a. □

Now we present some properties of binary quadratic forms, this is, quadratic forms in two variables, which will be useful as base cases in many proofs:

LEMMA 3 (Binary forms). (1) *A binary quadratic form represents zero if, and only if,* $d(f) = -1 \in K^*/K^{*2}$.

(2) *Two binary forms are equivalent if, and only if, they have the same determinant and they represent a common nonzero element.*

PROOF. If $ax^2 + by^2 = 0$ is a representation of zero then $xy \neq 0$ and

$$d = ab = -\left(\frac{by}{x}\right)^2 \equiv -1 \pmod{K^{*2}}.$$

Conversely, if $-d = -ab$ is a square, $(\sqrt{-ab}, a)$ is a representation of zero.
Now let f and g be binary quadratic forms. If $f \equiv g$ then both conditions are fulfilled trivially. Now assume $d(f) = d(g)$ and that they represent a common element $a \in K^*$. Since they represent a we can write $f \sim aX^2 + bY^2$ and $g \sim aX^2 + cY^2$. But $d(f) = ab = ac = d(g)$ and thus $b \equiv c \pmod{K^{*2}}$ and both quadratic forms are equivalent. □

THEOREM 2 (Witt's chain equivalence theorem). *Two equivalent diagonal quadratic forms can be connected through a chain of equivalences such that each term differs to the previous one in, at most, two coefficients.*

2. Hensel's lemma and the Hilbert symbol

Now we will advance towards studying equivalences of rational quadratic forms. To do so, we will see that we need to know whether the forms are equivalent as quadratic forms with coefficients in a completion of the field of rational numbers, namely $\mathbb{R}$ or $\mathbb{Q}_p$ (the field of p-adic numbers). Hence, in this section we will assume K is either $\mathbb{R}$ or $\mathbb{Q}_p$.

DEFINITION 6 (Hilbert symbol). *Let $a, b \in K^*$. We define their* Hilbert symbol (a, b) *as*

$$(a, b) = \begin{cases} 1 & \text{if } aX^2 + bY^2 - Z^2 \text{ represents zero over } K \\ -1 & \text{otherwise.} \end{cases}$$

From its definition and what we saw in the previous chapter it is obvious that the Hilbert symbol is symmetric and that does only depend on how a and b are modulo squares. This is, the Hilbert symbol defines an application

$$(\ ,\ ) : K^*/K^{*2} \times K^*/K^{*2} \longrightarrow \{\pm 1\}.$$

It is easy to see that the Hilbert symbol is 1 if and only if the conic $C_{a,b} : aX^2 + bY^2 = Z^2$ has a point in $\mathbb{P}^2(K)$, the projective plane over K. Equivalently, this happens if and only if $b \in K^*$ is a norm of the field $K(\sqrt{a})$ (or viceversa). Some elementary properties of the Hilbert symbol are introduced in the following proposition.

PROPOSITION 3. *If all its entries are nonzero, the Hilbert symbol has the following properties:*

(1) $(a,-a)=(a,1-a)=1$.
(2) $(a,b)=1 \Longrightarrow (a,bb')=(a,b')$.
(3) $(a,b)=(a,-ab)=(a,(1-a)b)$.

PROOF. The first property holds since $(1,1,0)\in C_{a,-a}$ and $(1,1,1)\in C_{a,1-a}$. The second property follows by the multiplicativity of norms: if b is a norm of $K(\sqrt{a})$ then b' is a norm of that extension if an only if bb' is. The third property is a conseqüence of the other two. □

To state and understand the theorem that gives an explicit formula for the Hilbert symbol, we need Hensel's lemma for the p-adic numbers. We begin remembering the concept of p-adic valuation of a p-adic number along with its basic properties.

DEFINITION 7 (p-adic valuation). *Each nonzero element $\alpha\in\mathbb{Q}_p^*$ can be written uniquely as $\alpha=p^r\varepsilon$, with $r\in\mathbb{Z}$ and $\varepsilon\in\mathbb{Z}_p$. The integer r is called the* p-adic valuation *of α.*

PROPOSITION 4. *The p-adic valuation has the following properties:*

(1) $v_p(\alpha\beta)=v_p(\alpha)v_p(\beta)$.
(2) $v_p(\alpha^{-1})=-v_p(\alpha)$.
(3) $v_p(\alpha+\beta)\geq \min v_p(\alpha),v_p(\beta)$, *with equality if* $v_p(\alpha)\neq v_p(\beta)$.

PROOF. If $\alpha,\beta\in\mathbb{Q}_p^*$, we can write them uniquely as $\alpha=p^r\varepsilon$ and $\beta=p^s\eta$, with $\varepsilon,\eta\in\mathbb{Z}_p^*$. Then, since $\varepsilon\eta\in\mathbb{Z}_p^*$,

$$v_p(\alpha\beta)=v_p(p^{r+s}\varepsilon\eta)=r+s=v_p(\alpha)+v_p(\beta)$$

and since $\varepsilon^{-1}\in\mathbb{Z}_p^*$

$$v_p(\alpha^{-1})=v_p(p^{-r}\varepsilon^{-1})=-r=-v_p(\alpha).$$

The third property follows from the fact that, if $m=\min(r,s)$,

$$p^r\varepsilon+p^s\eta=p^m(p^{r-m}\varepsilon+p^{s-m}\eta)$$

and that if $r\neq s$, $p^{r-m}\varepsilon+p^{s-m}\eta$ is a p-adic unit since only one of the two terms is divisible by p. □

LEMMA 4. *Let $f(X)\in\mathbb{Z}_p[X]$. Given $\alpha\in\mathbb{Z}_p$ with*

$$v_p(f'(\alpha))=k \quad \textit{and } v_p(f(\alpha))>2k$$

let $\beta=\alpha-f(\alpha)/f'(\alpha)$. Then β is a p-adic integer and

$$v_p(\beta-\alpha)>k,\ v_p(f'(\beta))=k,\ \textit{and } v_p(f(\beta))>v_p(f(\alpha)).$$

PROOF. First of all, notice that β is well defined since $v_p(f'(\alpha))=k$ guarantees $f'(\alpha)$ is not zero. The first inequality can be shown as follows

$$v_p(\beta-\alpha)=v_p\left(\frac{f(\alpha)}{f'(\alpha)}\right)=v_p(f(\alpha))-v_p(f'(\alpha))>2k-k=k.$$

This implies $\beta-\alpha\in\mathbb{Z}_p$ and hence $\beta\in\mathbb{Z}_p$.

For the second property, we need to expand f' to first order, $f'(X) = f'(\alpha) + g(X)(X - \alpha)$ for some $g \in \mathbb{Z}_p[X]$. Evaluating $X = \beta$ and taking p-adic valuations we get

$$v_p(f'(\beta)) = v_p(f'(\alpha) + g(\beta)(\beta - \alpha))$$

Since $v_p(\beta - \alpha) > k$, $v_p(g(\beta)(\beta - \alpha)) = v_p(g(\beta)) + v_p(\beta - \alpha) > k$ so by the third property of the previous proposition we get $f'(\beta) = f'(\alpha) = k$. To get the third property, we expand f to second order, $f(X) = f(\alpha) + f'(\alpha)(X - \alpha) + h(X)(X - \alpha)^2$ for some $h(X) \in \mathbb{Z}_p[X]$. If we evaluate in β again we obtain (recalling the definition of β) $f(\beta) = h(\beta)(\beta - \alpha)^2$. Taking valuations yields

$$v_p(f(\beta)) \geq 2v_p(\beta - \alpha) = 2v_p(f(\alpha)) - 2v_p(f'(\alpha)) = v_p(f(\alpha)) + v_p(f(\alpha)) + 2k > v_p(f(\alpha)).$$

□

After this work, we are ready to prove Hensel's lemma, which reminds us to Newton's root finding method in $\mathbb{R}$, but turns out to have much nicer properties.

THEOREM 3 (Hensel's lemma). *Let $f(X) \in \mathbb{Z}_p[X]$. Given $\alpha \in \mathbb{Z}_p$ with*

$$v_p(f'(\alpha)) = k \text{ and } v_p(f(\alpha)) > 2k$$

exists $\gamma \in \mathbb{Z}_p$ such that $f(\gamma) = 0$ and $\gamma \equiv \alpha \pmod{p^{k+1}}$ that satisfies the following properties:

(1) *γ is the only root of f satisfying the congruence $\gamma \equiv \alpha \pmod{p^{k+1}}$,*
(2) *γ is a simple root of f, and*
(3) *γ is the limit of the recurrence*

$$\alpha_1 = \alpha,\ \alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}.$$

PROOF. Let $\{\alpha_n\}$ be the sequence defined in the statement. By the previous lemma, all $\alpha_n \in \mathbb{Z}_p$ and the following inequalities hold for $n \geq 1$:

$$v_p(\alpha_{n+1} - \alpha_n) > k,\ v_p(f'(\alpha_n)) = k \text{ and } v_p(f(\alpha_{n+1})) > v_p(f(\alpha_n)).$$

The first inequality tells us that the sequence is Cauchy in the p-adic metric (given by the absolute value $|\alpha|_p = p^{-v_p(\alpha)}$ which induces the distance $d(\alpha, \beta) = |\alpha - \beta|_p$). Since p-adic numbers are complete under that metric, the sequence converges to a limit γ, and polynomials are continous with the p-adic metric, $f(\gamma) = \lim f(\alpha_n)$. Since the valuations of $f(\alpha_n)$ are strictly increasing by the third inequality, $f(\gamma) = \lim f(\alpha_n) = 0$.
Now $v_p(\alpha_{n+1} - \alpha_n) \geq k + 1$ for $n \geq 1$ implies $v_p(\alpha_n - \alpha) \geq k + 1$ for $n \geq 1$. Let n be big enough so that $v_p(\gamma - \alpha_n) \geq k + 1$. Now the properties of the p-adic valuation $v_p(\gamma - \alpha) \geq \min\{v_p(\alpha_n - \alpha), v_p(\gamma - \alpha_n)\} \geq k + 1$ which is to say $\gamma \equiv \alpha \pmod{p^{k+1}}$.
Now only remains to show the uniqueness of γ and that it is a simple root of f. Consider $f(X) = (X - \gamma)f_1(X)$, $f_1 \in \mathbb{Z}_p[X]$. We need to show that f_1 does not have a root γ_1 which satisfies the congruence. This will also imply that γ is a simple root of f since otherwise γ would be a root of f_1. Taking derivatives and substituting $X = \alpha$ yields

$$f'(\alpha) = f_1(\alpha) + (\alpha - \gamma)f_1'(\alpha).$$

Since $v_p(f'(\alpha)) = k$ and $v_p(f_1'(\alpha)(\alpha - \gamma)) \geq v_p(\alpha - \gamma) = k + 1$ so taking the minimum yields $v_p(f_1(\alpha)) = k$. If γ_1 was a root of f_1 such that $\gamma_1 \equiv \alpha \pmod{()p^{k+1}}$ then we would have $f_1(\gamma_1) \equiv f_1(\alpha) \pmod{p^{k+1}}$ which is not possible since $v_p(f_1(\alpha)) = k$. □

The following application of Hensel's lemma is relevant for us since it tells which groups are $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$:

COROLLARY 2. *The subgroup $\mathbb{Q}_p^{*2}$ of the p-adic numbers that are squares has index 4 or 8 in the multiplicative group $\mathbb{Q}_p^*$ depending on whether $p \neq 2$ or $p = 2$, and a system of representatives of the quotient group is*

(1) $\mathbb{Q}_p^*/\mathbb{Q}_p^* = \{1, a, p, ap\}$ *where $a \in \mathbb{Z}$ is a nonquadratic residue modulo p, for odd p,*
(2) $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{\pm 1, \pm 2, \pm 5, \pm 10\}$ *for $p = 2$.*

PROOF. A nonzero p-adic number $\alpha = p^r\varepsilon$, $\varepsilon \in \mathbb{Z}_p^*$ is a square if and only if r is even and ε is a square (necessarily of a unit). Consider the polynomial $X^2 - \varepsilon \in \mathbb{Z}_p[X]$, which has derivative $2X$. Hensel's lemma tells us that this polynomial has a root in $\mathbb{Z}_p$ if and only if the congruence $X^2 \equiv \varepsilon \pmod{p}$ has a solution for odd p and the congruence $X^2 \equiv \varepsilon \pmod{8}$ for $p = 2$. This implies ε is a quadratic residue modulo p for odd p and that $\varepsilon \equiv 1 \pmod{8}$.

Hence if p is odd and a is a nonquadratic residue modulo p, then $a \notin \mathbb{Z}_p^{*2}$ and, for each unit ε, either ε or $a\varepsilon$ have a square root in $\mathbb{Z}_p$, so this proves the statement for odd p. For $p = 2$, for each unit ε exactly one of the four units $\pm\varepsilon$, $\pm 5\varepsilon$ is congruent to 1 modulo 8, and this finishes the proof. □

Now we turn our attention back to the Hilbert symbol. Let us introduce the following notation. which generalizes the notation used with the Legendre symbol. Recall that for $a \in \mathbb{Z}$ an p and odd prime we define the Legendre symbol as

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } a \not\equiv 0 \pmod{p}. \end{cases}$$

For $\mu \in \mathbb{Z}_2^*$ we define

$$\varepsilon(\mu) = \frac{\mu - 1}{2} \pmod{2} \text{ and } \omega(\mu) = \frac{\mu^2 - 1}{2} \pmod{8}.$$

For $\mu \in \mathbb{Z}_p^*$ and odd p, we define

$$\left(\frac{\mu}{p}\right) = \left(\frac{\mu \pmod{p}}{p}\right) = \left(\frac{a_1}{p}\right), \text{ if } \mu = \{a_n\} \in \mathbb{Z}_p^*.$$

As a conclusion of the previous result, we can see that the symbol we just defined tells us whether the p-adic unit μ is a square or not in $\mathbb{Q}_p^*$. Now we are ready to state the following theorem.

THEOREM 4 (Formulae for the Hilbert symbol). *If $K = \mathbb{R}$ the symbol $(a, b) = -1$ if and only if both a and b are negative. If $K = \mathbb{Q}_p$ and $a = p^r\mu$, $b = p^s\nu$ with $\mu, \nu \in \mathbb{Z}_p^*$, then*

(1) $(a,b) = (-1)^{rs\varepsilon(p)} \left(\frac{\mu}{p}\right)^s \left(\frac{\nu}{p}\right)^r$ *for odd* p, *and*
(2) $(a,b) = (-1)^{\varepsilon(\mu)\varepsilon(\nu)+s\omega(\mu)+r\omega(\nu)}$.

A straightforward manipulation of those formulae can be used to show that the Hilbert symbol is multiplicative. Notice that by symmetry it is enough to check that $(a_1a_2, b) = (a_1, b)(a_2, b)$ for all $a_1, a_2, b \in K^*$.

COROLLARY 3. *The Hilbert symbol is multiplicative in both variables.*

Hence fixing one of the variables induces a group homomorphism

$$\begin{array}{rccc} (\cdot, d): & K^*/K^{*2} & \longrightarrow & \{\pm 1\} \\ & x & \longmapsto & (x,d) \end{array}$$

LEMMA 5. *For* $d \neq 1$ *the homomorphism* $x \mapsto (x,d)$ *is surjective.*

PROOF. It suffices to find a $x \in K^*/K^{*2}$ such that $(x,d) = -1$, since $(1,d) = 1$ for all d.
If $K = \mathbb{R}$ then the only element of $\mathbb{R}/\mathbb{R}^2$ which is not 1 is -1, and $(-1,-1) = -1$.
If p is odd $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, p, ap, p\}$, where a is a unit which is not a quadratic residue modulo p. Then by the results above

$$(a,p) = (p,a) = (a,ap) = -1$$

Finally $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{1, \pm 2, \pm 5, \pm 10\}$ and

$$(-1,-1) = (5, \pm 2) = (2, \pm 5) = (2, \pm 10) = -1$$

□

3. Real quadratic forms

When $K = \mathbb{R}$ the study of quadratic forms is particulary simple, since modulo equivalences we can limit ourselves to diagonal quadratic forms with coefficients in $\mathbb{R}^*/\mathbb{R}^{*2} = \{-1, 1\}$. Hence all real quadratic forms which are regular are equivalent to a form of the type

$$\langle 1, 1, \ldots, 1, -1, \ldots, -1 \rangle$$

If r is the number of 1 and s the number of -1, the pair (r,s), which is called the *signature* of the quadratic form, classifies the equivalence class of the form once the number of variables is fixed.

A form is called *definite* if $rs = 0$, *positive* if $r = n$ and *negative* if $s = n$. The forms such that $rs \neq 0$ are *indefinite* forms. Notice that regular definite forms can only represent positive numbers if they are positive or negative numbers if they are negative, and hence they are not isotropic. Regular indefinite forms are trivially isotropic (putting a 1 in a variable that has 1 as a coefficient and another 1 in a variable which has -1 as a coefficient is a representation of zero) and hence universal.

4. p-adic quadratic forms

We will devote this section to study nonsingular quadratic forms over the p-adic numbers. First we introduce the Witt invariant (which sometimes is called Hasse-Witt invariant), which will play a crucial role in the study of p-adic forms.

DEFINITION 8 (Witt invariant). *Let f be a p-adic quadratic form and let $f \sim \langle a_1, a_2, \ldots, a_n \rangle$ be an equivalent diagonal form. We define the* Witt invariant *of f as the following product of Hilbert symbols*

$$w(f) = \prod_{i<j} (a_i, a_j) \in \{\pm 1\}.$$

The Witt invariant is well defined in the sense that it does not depend on the equivalent form taken, meaning that it is an invariant of the equivalence class of the quadratic form.

THEOREM 5. *The Witt invariant $w(f)$ does not depend on the diagonal form chosen to compute it.*

PROOF. If the forms have one variable the Witt invariant is an empty product. For $n = 2$ variables and $f \sim \langle a_1, a_2 \rangle$ we have $w(f) = (a_1, a_2)$. By definition of the Hilbert symbol $w(f)$ means whether that diagonal form (and hence f) represents or not 1, which does only depend on the equivalence class of the form f and not on the diagonal form.
For $n \geq 3$ variables we will proceed by induction. By a theorem of the first section two equivalent diagonal forms can be connected through a sequence of diagonal forms which share at least one coefficient, so it will suffice to show that the Witt invariant is mantained when passing from a diagonal form to another one which shares a coefficient with the original form (actually the theorem gives us a stronger condtion: it says that the two quadratic forms differ in at most 2 coefficients, which for $n \geq 3$ implies that they share at least one coefficient). Now let

$$f \sim \langle a_1, a_2, \ldots, a_n \rangle \sim \langle b_1, b_2, \ldots, b_n \rangle$$

where $a_1 = b_1$. Then Witt's cancellation theorem yields $\langle a_2, \ldots, a_n \rangle \sim \langle b_2, \ldots, b_n \rangle$, which, by the inductive hypothesis, have the same Witt invariant. Now taking into account that the product of the a_i and the b_i is the same modulo squares (and equal to the determinant of the quadratic form), that Hilbert symbols do only depend on classes modulo squares and that $(a, b) = (a, -ab)$,

$$\prod_{i<j} (a_i, a_j) = (a_1, a_2 \cdots a_n) \prod_{2 \leq i < j} (a_i, a_j) = (a_1, -d(f)) w(\langle a_2, \ldots, a_n \rangle) =$$

$$= (b_1, -d(f)) w(\langle b_2, \ldots, b_n) = (b_1, b_2 \cdots b_n) \prod_{2 \leq i < j} (b_i, b_j) = \prod_{i<j} (b_i, b_j),$$

so the Witt invariant for both diagonal forms coincide and we are done. □

Hence the Witt invariant and the determinant of the quadratic form are invariants of equivalence classes of quadratic forms. The following theorem, which we will not prove since it involves the study of many particular cases, tells us that the Witt invariant, the determinant

and the number of variables of a p-adic nonsingular quadratic form determine whether the form represents an element or not.

THEOREM 6. *Let f be a p-adic nonsingular quadratic form with invariants $d \in \mathbb{Q}_p^*/\mathbb{Q}_p^*$ and $w \in \{\pm 1\}$. Let n be the number of variables of the form. Then*

- *f represents zero if and only if*
  (1) *$n = 2$ and $-d = 1$,*
  (2) *$n = 3$ and $(-1, -d) = w$,*
  (3) *$n = 4$ and $d \neq 1$ or $d = 1$ and $w = (-1, -1)$,*
  (4) *$n \geq 5$.*
- *f represents $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ if and only if*
  (1) *$n = 1$ and $a = d$,*
  (2) *$n = 2$ and $(a, -d) = w$*
  (3) *$n = 3$ and $a \neq -d$ or $a = -d$ and $w = (-1, -d)$,*
  (4) *$n \geq 4$.*

Finally we arrive to the result that classifies the equivalence classes of p-adic quadratic forms in terms of its rank, its determinant and its Witt invariant:

THEOREM 7 (Classification of p-adic forms). *Two p-adic quadratic forms which are nondegenerate are equivalent if, and only if, they have the same rank, the same determinant and the same Witt invariant.*

PROOF. That the determinant, the rank, and the Witt invariant are invariants of the equivalence class has already been proved.
We will prove the converse by induction on the rank n (which since the form is nondegenerate is the number of variables). For $n = 1$ if $d(f) = d(g)$ then clearly $f \sim g$. Now let f and g be forms of rank $n \geq 2$ which have the same determinant and the same Witt invariant, and let $a \neq 0$ be an element represented by f. By the previous theorem, g also represents that element. Hence those forms are equivalent to $f \sim \langle a \rangle \perp f_1$ and $g \sim \langle a \rangle \perp g_1$, where f_1 and g_1 have rank $n - 1$ and invariants such that $d(f) = ad(f_1)$, $d(g) = ad(g_1)$ and $w(f) = (a, d(f_1))w(f_1)$, $w(g) = (a, d(g_1))w(g_1)$. Since f and g have the same invariants, we deduce that $d(f_1) = d_(g_1)$ and hence $w(f_1) = w(g_1)$. By induction $f_1 \sim g_1$ and this implies $f \sim g$. □

5. Global properties of the Hilbert symbol

We begin with a definition which will help us to treat jointly the p-adic and real cases.

DEFINITION 9 (Places of $\mathbb{Q}$). *The equivalence classes of absolute values over $\mathbb{Q}$ are called* places *of $\mathbb{Q}$, where we define two absolute values to be equivalent if they define the same topology on $\mathbb{Q}$.*

It is easy to see that an equivalent condition for two nontrivial absolute values $|\cdot|_1$ and $|\cdot|_2$ to be equivalent is that $|\cdot|_2 = |\cdot|_1^a$ for some $a > 0$.

Let V be the set of places of $\mathbb{Q}$. Ostrowski's theorem tells us we can identify V with the set which is the union of the prime numbers (which represent the p-adic numbers) and the symbol ∞ (representing the real numbers).

THEOREM 8 (Ostrowski). *Every nontrivial absolute value over $\mathbb{Q}$ is either equivalent exactly to one p-adic absolute value or to the real absolute value.*

PROOF. Let m, n be integers greater than 1 and let $|\cdot|$ be a nontrivial absolute value over $\mathbb{Q}$. Then we can write m in base n, $m = a_0 + a_1 n + \cdots + a_r n^r$ with $0 \leq a_i < n$ and $n^r \leq m$. Let $N = \max\{1, |n|\}$. By the triangle inequality we have

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq \sum_{i=0}^{r} |a_i| N^r$$

and since

$$r \leq \frac{\log(m)}{\log(n)}$$

where log is relative to some $e > 1$. Now we apply the triangle inequality again and use the fact that the a_i are nonnegative to get

$$|a_i| \leq a_i|1| = a_i \leq n.$$

Putting this into the first inequality yields

$$|m| \leq (1 + r) n N^r \leq \left(1 + \frac{\log(m)}{\log(n)}\right) n N^{\log(m)/\log(n)}$$

Now replace m with m^t, $t \in \mathbb{Z}$ and take t-th roots:

$$|m| \leq \left(1 + \frac{t \log m}{\log n}\right) n^{1/t} N^{\log m/\log n}.$$

Finally let $t \to \infty$ to get

$$|m| \leq N^{\log m/\log n}.$$

Now we distinguish two cases:

(1) For all integers $n > 1$, $|n| > 1$. In this case $N = |n|$ and

$$|m|^{1/\log m} \leq |n|^{1/\log n}.$$

By symmetry exchanging m and n tells us that we must have equality, so there exists $c > 1$ such that

$$c = |m|^{1/\log m} = |n|^{1/\log n}$$

for all $m, n > 1$. Hence

$$|n| = c^{\log n} = e^{\log c \log n} = n^{\log c}$$

for all $n > 1$. Now let $a = \log c$ and rewrite this as

$$|n| = |n|_\infty^a, \ \forall n > 1$$

where as usual $|\cdot|_\infty$ is the usual absolute value on $\mathbb{Q}$. Now since both $|\cdot|$ and $|\cdot|_\infty^a$ are group homomorphisms $\mathbb{Q}^* \to \mathbb{R}^+$ and they agree on a set of generators of $\mathbb{Q}^*$ (the primes and -1) this means that they agree on all $\mathbb{Q}^*$.

(2) Exists $n > 1$ such that $|n| \leq 1$. For this n, $N = 1$ and the previous inequality implies $|m| \leq 1$ for all integers m. Then the absolute value is nonarchimedean. Let $\mathfrak{a} = \{a \in \mathbb{Z} : |a| < 1\}\}$. Since $|m| \leq 1$ for all $\mathbb{N}$, $\mathfrak{a}$ is an ideal of $\mathbb{Z}$.
If $|p| = 1$ for all primes p, then $|\cdot|$ would be a trivial absolute, hence exists p such that $|p| \leq 1$, i.e., $p \in \mathfrak{a}$. This means $p\mathbb{Z} \subseteq \mathfrak{a} \subsetneq \mathbb{Z}$ and we deduce $p\mathbb{Z} = \mathfrak{a}$. Now let

$$s = -\frac{\log |p|}{\log |p|}$$

and take $a = p^m b/c \in \mathbb{Q}$, with $m, b, c \in \mathbb{Z}$ with b and c not multiple of p. Then $|b| = |c| = 1$, and

$$|a| = \left| p^m \frac{b}{c} \right| = |p^m| = p^{-ms} = |a|_p^s$$

where $|\cdot|_p$ is the p-adic absolute value. This (and the fact that $\mathfrak{a} = p\mathbb{Z}$) proves that $|\cdot|$ is equivalent to exactly one p-adic absolute value.

□

Now let $a, b \in \mathbb{Q}^*$ be nonzero rational numbers. For each place $v \in V$ we define $(a, b)_v$ as the Hilbert symbol of the rationals a and b seen as elements of the fields $\mathbb{Q}_v$. We will use this notation from now on even if $a, b \in \mathbb{Q}_v$, although the v would not be strictly necessary in this case.

THEOREM 9 (Product formula, Hilbert). *If $a, b \in \mathbb{Q}^*$ then $(a, b)_v = 1$ for almost all v and*

$$\prod_{v \in V} (a, b)_v = 1.$$

That is, the number of places such that the Hilbert symbol is -1 is finite and even.

PROOF. The finiteness of the number of places where the Hilbert symbol is -1 follows from the fact that for all odd primes p such that $v_p(a) = v_p(b) = 0$ both a and b are p-adic units and hence $(a, b)_p = 1$.
Since Hilbert symbols are bilinear we just need to prove the result in the cases where a and b are either prime or -1. In the rest of the proof p and q will be odd primes. If we apply the formula for the Hilbert symbol we gave in section 2 and the quadratic reciprocity laws we obtain

- $(-1, -1)_v = -1 \iff v = 2, \infty$.
- $(-1, 2)_v = (2, 2)_v = 1$ at all places $v \in V$.
- $(-1, p)_v = (p, p)_v = 1$ at all places different from 2 and p, and $(-1, p)_2(-1, p)_p = (-1)^{\varepsilon(p)} \left(\frac{-1}{p}\right) = 1$.
- $(2, p)_v = 1$ at all places $v \neq 2, p$, and $(2, p)_2(2, p)_p = (-1)^{\omega(p)} \left(\frac{2}{p}\right) = 1$.
- If $p \neq q$, $(p, q)_v = 1$ at all places $v \neq 2, p, q$, and $(p, q)_2(p, q)_p(p, q)_q = (-1)^{\varepsilon(p)\varepsilon(q)} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1$.

In fact, we have shown that the product formula is equivalent to the quadratic reciprocity law. □

The following propositions are technical results that we will need to prove the Hasse principle.

PROPOSITION 5. *Let $f(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ be a polynomial with rational coefficients and let $S \subset V$ a finite subset of the places of $\mathbb{Q}$. For each $v \in S$, let $\alpha_v \in \mathbb{Q}_v^*$ be a element of the form $\alpha_v = f(x_{1,v}, \ldots, x_{n,v})$ with $x_{i,v} \in \mathbb{Q}_v$. Then there exist rational numbers $x_1, \ldots, x_n$ such that*

$$f(x_1, \ldots, x_n) \in \alpha_v \mathbb{Q}_v^{*2} \text{ for all } v \in S$$

PROPOSITION 6. *Let $\{a_i\}_{1 \leq i \leq n}$ be a finite family of nonzero rationals, and let $\varepsilon_{i,v} \in \{\pm 1\}$ be signs for each i and place $v \in V$ such that*

1. *for each index i only a finite and even number of signs $\varepsilon_{i,v}$ is -1, so $\prod_{v \in V} \varepsilon_{i,v} = 1$ for all i, and*
2. *for each place $v \in V$ there exists $\alpha_v \in \mathbb{Q}_v^*$ such that $(a_i, \alpha_v)_v = \varepsilon_{i,v} \in \{\pm 1\}$ for all i.*

Then there exists a nonzero rational x such that $(a_i, x)_v$ for all i and place v.

6. Rational quadratic forms

Let f be a nonsingular quadratic form of rank n. Its determinant $d(f)$ is an invariant defined modulo squares. For each place $v \in V$ we define the *local Witt invariant* $w_v(f)$ as the Witt invariant of the form f seen as a form with coefficients in $\mathbb{Q}_v$. By Hilbert's product formula,

$$\prod_{v \in V} w_v(f) = 1.$$

We will call $d_v(f) \in \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ the determinant of the quadratic form considered as a form in $\mathbb{Q}_v$, which coincides with the determinant $d(f)$ seen as an element of $\mathbb{Q}_v$.

THEOREM 10 (Legendre). *Let a, b be nonzero rational numbers. The conic*

$$aX^2 + bY^2 = Z^2$$

has rational points if, and only if, it has points in all the completions $\mathbb{Q}_v$.

PROOF. Only one direction is nontrivial, since the existence of rational points obviously implies the existence of points in the completions.

Assume the conic has points in all the completions $\mathbb{Q}_v$. By multiplying the variables by nonzero rationals if it is necessary, we can assume that a and b are squarefree integers, and by exchanging X and Y we can assume $|a| \leq |b|$, since these transformations do not change the properties of the statement.
We will proceed by induction on the value of $|a| + |b|$. If $|a| + |b| = 2$ then both a and b must be either 1 or -1. Since the conic has a real point they cannot be both equal to -1, and then the conic has the rational point $(1, 0, 1)$ if $a = 1$ and $(0, 1, 1)$ if $b = 1$.

Now assume $|a|+|b|>2$, and hence $|b|\geq 2$. For each odd prime dividing p, the existence of points in $\mathbb{Q}_p$ implies that $(a,b)_p=1$. If $p\nmid a$,

$$\left(\frac{a}{p}\right)=(a,b)_p=1$$

Hence a is a quadradic residue modulo each odd prime dividing b, even if $p\nmid a$, which is the trivial case. a is also a quadratic residue modulo 2 since all integers are. Applying the chinese remainder theorem yields that a is a quadratic residue modulo b.
Let $t\in\mathbb{Z}$ be a square root of a modulo b and q be the integer such that $t^2=a+bq$. Changing the sign of t if necessary, we can assume $|t|\leq|b|/2$. If $q=0$ then $a=1$ since a is squarefree, and the conic has the rational point $(1,0,1)$. Otherwise let $q=b'u^2$ with b' an squarefree integer and $u\neq 0$. Then

$$bb'=\frac{t^2}{u^2}-\frac{a}{u^2}$$

implies that the element bb' is a norm of the extension $\mathbb{Q}_v(\sqrt{a})$. Now we recall that

$$|b'|\leq|b'u^2|=\left|\frac{t^2-a}{b}\right|\leq\left|\frac{t^2}{b}\right|+\left|\frac{a}{b}\right|\leq\frac{|b|^2/4}{|b|}+1\leq\frac{b}{4}+\frac{b}{2}\leq b$$

and consider the new conic $aX^2+b'Y^2=Z^2$. Since $aX^2+bY^2=Z^2$ has points in $\mathbb{Q}_v$, b is a norm of the extension $\mathbb{Q}_v(\sqrt{a})$. Since bb' was also a norm of that extension, we get that b' is a norm of $\mathbb{Q}_v(\sqrt{a})$ for all v and hence the new conic has points in all completions $\mathbb{Q}_v$. Applying the hypothesis of induction the new conic has rational points, since $|a|+|b'|<|a|+|b|$.
Hence since both b' (the conic $aX^2+b'Y^2=Z^2$ has rational points) and bb' (the same identity as in the completions applies) are norms of $\mathbb{Q}(\sqrt{a})$, b is also a norm of that extension and hence the conic has rational points. □

We finally arrive to the main result in equivalences of rational quadratic forms:

THEOREM 11 (Hasse-Minkowski). *A regular quadratic form f with rational coefficients represents zero over $\mathbb{Q}$ if, and only if, it represents zero over all the completions $\mathbb{Q}_v$.*

PROOF. Let n be the rank of the quadratic form. If $n=1$ then the form never represents zero. If $n=2$ the form represents zero over a field if, and only if, $-d$ is a square of that field. We claim that a nonzero rational $r\in\mathbb{Q}^*$ is a square if and only if it is a square locally in all $\mathbb{Q}_v$. To prove this, we write r as

$$r=\pm\prod p_i^{m_i}.$$

The fact that r is a square in $\mathbb{R}$ implies $r>0$, and since r is a square of $\mathbb{Q}_{p_i}$ for all p_i the p_i-adic valuation $v_{p_i}(r)=m_i$ must be an even number and hence r is a square of $\mathbb{Q}$.
For $n=3$ the result is Legendre's theorem, that we have already proved.
For $n=4$ we write f as $f\sim\langle a_1,a_2,-a_3,-a_4\rangle$ with $a_i\in\mathbb{Q}^*$. Then f represents zero if, and only if, the forms $\langle a_1,a_2\rangle$ and $\langle a_3,a_4\rangle$ represent a common nonzero element. By hypothesis those forms represent a common nonzero element $\alpha_v\in\mathbb{Q}_v^*$ for all $v\in V$. Then by theorem 6 of the fourth section

$$(\alpha_v,-a_1a_2)=(a_1,a_2)_v,\text{ and }(\alpha_v,-a_3a_4)=(a_3,a_4).$$

Hilbert's product formula yields

$$\prod_{v\in V}(a_1,a_2)_v=\prod_{v\in V}(a_3,a_4)_v=1$$

and if we define $\varepsilon_{1,v}=(a_1,a_2)$ and $\varepsilon_{2,v}=(a_3,a_4)$ then by the results of the previous section there exists $x\in\mathbb{Q}^*$ such that

$$(x,-a_1a_2)_v=(a_1,a_2)_v,\text{ and }(x,-a_3a_4)_v=(a_3,a_4)_v$$

for all $v\in V$. Again by theorem 6 of the fourth section both $\langle a_1,a_2\rangle$ and $\langle a_3,a_4\rangle$ represent x over all $\mathbb{Q}_v$ and by this same result for lower n they represent x over $\mathbb{Q}$.
Finally let $n\geq 5$. We will proceed by induction over n. Let $f\sim\langle a_1,a_2\rangle\perp\langle -a_3,\ldots,a_n\rangle=h\perp -g$ where $g=\langle a_3,\ldots,a_n\rangle$ is a form in $n-2\geq 3$ variables. Let S be the set of places consisting of ∞, 2, and all odd primes p such that $v_p(a_i)\neq 0$ for some $i\geq 3$. The places which are not in S are odd primes p such that $d_p(g)$ is a unit and $w_p(g)=1$. For each place $v\in S$, f represents zero over $\mathbb{Q}_v$ and thus there exists a nonzero element α_v represented by both g and $h=\langle a_1,a_2\rangle$. Let $a_1x_{1,v}+a_2x_{2,v}=\alpha_v$ be a representation for each $v\in S$. Then by a result of the previous section there exist rationals $x_1,x_2\in\mathbb{Q}$ such that $a_1x_1^2+a_2x_2^2=x\in\mathbb{Q}^*$ is a rational with $x=\alpha_v\beta_v^2$ for all $v\in S$. The form g also represents x over each $\mathbb{Q}_v$ since it represents α_v for $v\in S$. But g represents x even if $v\notin S$: if g has four or more variables, then it represents all nonzero elements, in particular x, and if g has three variables then $(-1,-d_p(g))=1$ since $d_p(g)$ is a p-adic unit and $w_p(g)=1$ since all a_i are p-adic units for $i\geq 3$. Then by the theorem 6 of the fourth section tells us that g represents all nonzero elements and thus it represents x. Hence the form $\langle -x\rangle\perp g$, which has $n-1$ variables, represents zero over all completions $\mathbb{Q}_v$. By induction, it represents zero over $\mathbb{Q}$ and hence g represents x over $\mathbb{Q}$ and finally f represents zero over $\mathbb{Q}$. □

Corollary 4. *A quadratic form over $\mathbb{Q}$ represents a rational a over $\mathbb{Q}$ if, and only if, if represents a locally at all the completions $\mathbb{Q}_v$.*

Proof. This is equivalent to say that $\langle -a\rangle\perp f$ represents zero over $\mathbb{Q}$ if, and only if, it represents zero over all the completions, which is Hasse-Minkowski theorem. □

Corollary 5 (Equivalence of rational quadratic forms). *Two quadratic forms over $\mathbb{Q}$ are equivalent if, and only if, they are equivalent over all the completions $\mathbb{Q}_v$. Equivalently, two rational quadratic forms are equivalent if an only if they have the same determinant modulo squares, the same signature and the same local Witt invariants.*

Proof. We proceed by induction on the number of variables n. If $n=1$ then we need to prove that an element is a square of $\mathbb{Q}$ if, and only if, it is a square of all completions $\mathbb{Q}_v$, but this has already been done during the proof of the theorem.
Now let $n>1$. Assume that $f\sim g$ over all $\mathbb{Q}_v$. Let $a\in\mathbb{Q}^*$ be a rational represented by f over $\mathbb{Q}$ (and thus over all $\mathbb{Q}_v$). The local equivalence implies that g also represents a over all $\mathbb{Q}_v$, and by the previous corollary g represents a over $\mathbb{Q}$. Then $f\sim\langle a\rangle\perp f_1$ and $g\sim\langle a\rangle\perp g_1$. By the cancellation theorem $f_1\sim g_1$ over all $\mathbb{Q}_v$, and by induction $f_1\sim g_1$ over $\mathbb{Q}$, and thus $f\sim g$ over $\mathbb{Q}$. □

Chapter 2
Quadratic embedding problems

1. Group extensions with kernel $\mathbb{Z}/2\mathbb{Z}$

Let Q be a group and let G be an *extension* of Q with kernel $\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$. This is to say that we have an exact sequence of groups

$$1 \longrightarrow \{\pm 1\} \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

Note that the image of $\{\pm 1\}$ inside G is a normal subgroup which, since it has two elements, belongs to the center $Z(G)$ of G.

Definition 10 (Equivalent group extensions). *Let G_1, G_2 be two extensions of Q with kernel $\{\pm 1\}$. The two extensions are said to be* equivalent *if it exists an isomorphism $\varphi : G_1 \to G_2$ which makes the following diagram commutative:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \{\pm 1\} & \xrightarrow{i} & G_1 & \xrightarrow{\pi} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & \{\pm 1\} & \xrightarrow{i} & G_2 & \xrightarrow{\pi} & Q & \longrightarrow & 1 \end{array}$$

Now we consider a section of $s : Q \to G$ of the canonical projection $\pi : G \twoheadrightarrow Q$, i.e., a map such that $\pi \circ s = \mathrm{Id}_Q$. Any other section is of the form $t(\sigma) = u_\sigma s(\sigma)$, with $\sigma \mapsto u_\sigma$ being a map $Q \to \{\pm 1\}$. For each $\sigma, \tau \in Q$ we define $c(\sigma, \tau) \in \{\pm 1\}$ as the sign that verifies the identity

$$s(\sigma)s(\tau) = c(\sigma, \tau)s(\sigma\tau).$$

Lemma 6. *The map*

$$\begin{array}{rccc} c(.,.) : & Q \times Q & \longrightarrow & \{\pm 1\} \\ & (\sigma, \tau) & \longmapsto & c(\sigma, \tau) \end{array}$$

satisfies the identity

$$c(\tau, \mu)c(\sigma, \tau\mu) = c(\sigma, \tau)c(\sigma\tau, \mu)$$

for all $\sigma, \tau, \mu \in Q$.

PROOF. We will compute $s(\sigma)s(\tau)s(\mu)$ in two different ways:

$$s(\sigma)s(\tau)s(\mu) = c(\sigma,\tau)s(\sigma\tau)s(\mu) = c(\sigma,\tau)c(\sigma\tau,\mu)s(\sigma\tau\mu)$$

and

$$s(\sigma)s(\tau)s(\mu) = s(\sigma)s(\tau\mu)c(\tau,\mu) = c(\sigma,\tau\mu)c(\tau,\mu)s(\sigma\tau\mu).$$

Equating both results and cancelling $s(\sigma\tau\mu) \neq 0$ yields the result. □

One should notice that the definition of c that we have given depends on the section s considered. The following lemma tells us the relation between the maps obtained by considering two different sections:

LEMMA 7. *Let $s, t : Q \to G$ be sections of π, with $s(\sigma) = u_\sigma t(\sigma)$, and let c_s, c_t be the corresponding maps. Then*

$$c_t(\sigma,\tau) = c_s(\sigma,\tau)u_\sigma u_\tau u_{\sigma\tau}.$$

PROOF. Since $t(\sigma) = u_\sigma s(\sigma)$,

$$t(\sigma)t(\tau) = u_\sigma u_\tau s(\sigma)s(\tau)$$

but

$$t(\sigma)t(\tau) = c_t(\sigma,\tau)t(\sigma\tau) = c_t(\sigma,\tau)u_{\sigma\tau}s(\sigma\tau)$$

and

$$s(\sigma)s(\tau) = c_s(\sigma,\tau)s(\sigma\tau),$$

hence we have

$$c_t(\sigma,\tau)u_{\sigma\tau}s(\sigma\tau) = u_\sigma u_\tau c_s(\sigma,\tau)s(\sigma\tau)$$

and this finishes the proof. □

Until this point we have defined some maps from a group extension. Now we will try to go the other way around, i.e., consider the maps that verify an identity that we have proved true in the case where the maps come from a group extension and try to define a group extension from those maps.

DEFINITION 11 (2-cocycle). *Let Q be a group. We define $Z^2(Q, \{\pm 1\})$ as the set of the maps $c : G \times G \to \{\pm 1\}$ that verify*

$$c(\tau,\mu)c(\sigma,\tau\mu) = c(\sigma,\tau)c(\sigma\tau,\mu)$$

for all $\sigma, \tau, \mu \in Q$. We will call a 2-cocycle *such a map.*

LEMMA 8. *$Z^2(Q, \{\pm 1\})$ is a group with the operation corresponding to operate with the images of the 2-cocycles, this is, $cc'(\sigma,\tau) = c(\sigma,\tau)c'(\sigma,\tau)$ for $c, c' \in Z^2(Q, \{\pm 1\})$. In fact, $Z^2(Q, \{\pm 1\}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$.*

PROOF. $Z^2(Q,\{\pm1\})$ is closed under this map since clearly cc' is an map $Q\times Q\to\{\pm1\}$ and

$$cc'(\tau,\mu)cc'(\sigma,\tau\mu)=cc'(\sigma,\tau)cc'(\sigma\tau,\mu)$$

because c,c' satisfy their corresponding identities (we just need to split the product, apply those identities and regroup).
Associativity and commutativity are trivial because the product of ±1 is associative and commutative.
The neutral element is the map that is identically one, $(\sigma,\tau)\mapsto 1: Q\times Q\to\{\pm1\}$.
Finally, we consider $cc(\sigma,\tau)=c(\sigma,\tau)c(\sigma,\tau)=(c(\sigma,\tau))^2=1$ and hence each element has order 2 and it's its own inverse, and hence $Z^2(Q,\{\pm1\})\simeq(\mathbb{Z}/2\mathbb{Z})^n$.
These last things are a consequence of the fact that the set of maps from a set to a group inherits a group structure when it is equipped with the operation corresponding to operate with the images of those maps. In this case, since all elements of $\{\pm1\}$ have order at most 2, the maps will also have order at most 2. □

DEFINITION 12 (2-coboundary). *Let $\sigma\mapsto u_\sigma: Q\to\{\pm1\}$ be a map and define $c_u(\sigma,\tau)=u_\sigma u_\tau u_{\sigma\tau}$. Those maps will be called* 2-coboundaries. *We will denote by $B^2(Q,\{\pm1\})$ the set of 2-coboundaries.*

LEMMA 9. *Each 2-coboundary is a 2-cocycle and they form a subgroup $B^2(Q,\{\pm1\})\subseteq Z^2(Q,\{\pm1\})$.*

PROOF. Let c_u be a 2-coboundary. First of all, we compute

$$c_u(\tau,\mu)c_u(\sigma,\tau\mu)=u_\tau u_\mu u_\sigma u_{\tau\mu}^2 u_{\sigma\tau\mu}$$

and

$$c_u(\sigma,\tau)c_u(\sigma\tau,\mu)=u_\sigma u_\tau u_\mu u_{\sigma\tau}^2 u_{\sigma\tau\mu}$$

which are equal since $u_{\tau\mu}^2=u_{\sigma\tau}^2=1$, so all 2-coboundaries are 2-cocycles.
If c_u and c_v are 2-coboundaries, then $c_uc_v=c_{uv}$ is also a 2-coboundary and hence the set $B^2(Q,\{\pm1\})$ is closed under the operation product of images. The neutral element of the group $Z^2(Q,\{\pm1\})$ belongs to $B^2(Q,\{\pm1\})$ since it is a coboundary for the map $\sigma\mapsto u_\sigma=1$, and since all elements are their own inverse $B^2(Q,\{\pm1\})$ is also closed under inversion of elements and hence a subgroup of $Z^2(Q,\{\pm1\})$. □

Since $Z^2(Q,\{\pm1\})\simeq(\mathbb{Z}/2\mathbb{Z})^n$ and, in particular, $Z^2(Q,\{\pm1\})$ is an abelian group, all subgroups are normal subgroups, so we can consider the quotient group of the 2-cocycles modulo the 2-coboundaries:

DEFINITION 13 (Second cohomology group). *The* second cohomology group *of G with values in $\{\pm1\}$ is the quotient group*

$$H^2(Q,\{\pm1\})=Z^2(Q,\{\pm1\})/B^2(Q,\{\pm1\}).$$

DEFINITION 14 (Normalized cocycle). *A* normalized cocycle *is a cocycle such that $c(\sigma,1)=c(1,\sigma)=c(1,1)=1$ for all $\sigma\in Q$.*

LEMMA 10. *Each 2-cocycle is equivalent (modulo coboundaries) to a normalized cocycle.*

PROOF. First of all we will compute $c(\sigma, 1)$ using the defining identity of a 2-cocycle, by setting $\tau = \mu = 1$:

$$c(\sigma,1)c(\sigma,1) = c(1,1)c(\sigma,1) \Longrightarrow c(\sigma,1) = c(1,1).$$

We repeat this procedure to compute $c(1, \sigma)$,

$$c(1,\sigma)c(1,\sigma) = c(1,1)c(1,\sigma) \Rightarrow c(1,\sigma) = c(1,1).$$

We have checked that $c(\sigma, 1) = c(1, \sigma) = c(1, 1)$. Now we have to see that this cocycle is equivalent modulo coboundaries to one that satisfies $c(1, 1) = 1$. Consider $u : Q \to \{\pm 1\}$ such that $u_1 = c(1, 1)$. Then $cc_u(1, 1) = c(1, 1)u_1u_1u_1 = (c(1, 1))^4 = 1$ and we are done. □

LEMMA 11. *If Q is abelian, the classes of the symmetric 2-cocycles (i.e. those such that $c(\sigma, \tau) = c(\tau, \sigma)$) are a subgroup of the second cohomology group $H^2(Q, \{\pm 1\})$ which will be called $\mathrm{Ext}^2(Q, \{\pm 1\})$.*

PROOF. A sufficient condition for a subset H to be a subgroup is that $gh^{-1} \in H$ for any two elements $g, h \in H$.
Since all 2-cocycles are their own inverse in $Z^2(Q, \{\pm 1\})$ and so are their equivalence classes, we only need to show that the product of two symmetric cocycles is equivalent to another symmetric cocycle. Let c, c' be symmetric cocycles. Then

$$cc'(\sigma,\tau) = c(\sigma,\tau)c'(\sigma,\tau) = c(\tau,\sigma)c'(\tau,\sigma) = cc'(\tau,\sigma)$$

□

Now, as we said earlier, we will try to build a group extension G of Q given a 2-cocycle $c \in Z^2(Q, \{\pm 1\})$. We define the group G (as a set) in a quite natural way, $G = \{\pm 1\} \times Q$, so that the natural inclusion and projection are easily defined so as to give a group extension of Q with kernel $\{\pm 1\}$. The operation of G is defined as $(u, \sigma)(v, \tau) = (c(\sigma, \tau)uv, \sigma\tau)$, that is, taking the product of components and modifying the first component depending on the value which takes the 2-cocycle c evaluated in the two second components.

PROPOSITION 7. *The set $G = \{\pm 1\} \times Q$ equipped with the operation $(u, \sigma)(v, \tau) = (c(\sigma, \tau)uv, \sigma\tau)$ is indeed a group, and it is an extension of Q with kernel $\{\pm 1\}$.*

PROOF. If we assume that G is a group it is trivial that it is an extension of Q with kernel $\{\pm 1\}$ by taking i as the inclusion into the first compontent of $G = \{\pm 1\} \times Q$ and π as the projection onto the second component.
We need to check that G is a group with the operation that we defined. Since $c(\sigma, \tau) \in \{\pm 1\}$ for all $\sigma, \tau \in Q$, it is obvious that the group is closed under the operation. Associativity is also trivial since the operation in Q is associative.
For the neutral element, we recall that $c(\sigma, 1) = c(1, \sigma) = c(1, 1)$. Then

$$(u,\sigma)(c(1,1),1) = (c(1,1)^2u,\sigma) = (c(1,1),1)(u,\sigma)$$

and hence $(c(1, 1), 1)$ is the neutral element of the group (since we will end up working with equivalence classes modulo coboundaries we will always be able to take a normalized cocycle

such that $c(1,1) = 1$ so the neutral element will be $(1,1)$).
Finally we need to we need to find the inverse of an element (u,σ). Notice that

$$(u,\sigma)(uc(\sigma,\sigma^{-1})c(1,1),\sigma^{-1}) = (u^2c(\sigma,\sigma^{-1})^2c(1,1),\sigma\sigma^{-1}) = (c(1,1),1)$$

and hence $(u,\sigma)^{-1} = (uc(\sigma,\sigma^{-1})c(1,1),\sigma^{-1})$. □

A natural question that we may ask now is under which conditions two 2-cocycles yield equivalent group extensions in the sense that we defined above. We discover that there is a natural bijection between the equivalence classes of the 2-cocycles modulo 2-coboundaries and the equivalence classes of group extensions of Q with kernel $\{\pm 1\}$:

PROPOSITION 8. *There is a bijection between $H^2(Q,\{\pm 1\})$ and the equivalence classes the group extensions of Q with kernel $\{\pm 1\}$.*

PROOF. Let G_1 and G_2 be groups that give equivalent extensions of Q, and let $s : Q \to G_1$ and $t : Q \to G_2$ be sections of the canonical projections for G_1 and G_2 respectively. We have to see that the corresponding cocycles are equivalent modulo coboundaries. By the commutativity of the diagram, $s(\sigma) = u_\sigma t(\sigma)$ for $\sigma \in Q$ and some sign $u_\sigma \in \{\pm 1\}$. As in lemma 7 one can proof that the corresponding cocycles are equivalent modulo the coboundary $c_u(\sigma,\tau) = u_\sigma u_\tau u_{\sigma\tau}$.
Conversely, let c and c' be two equivalent cocycles and let G_1 and G_2 be the corresponding extensions obtained using the procedure described above, giving a group structure to the cartesian product $\{\pm 1\} \times Q$. Let $\sigma \mapsto u_\sigma$ be a map such that the equivalence between the cocicles is given by $c'(\sigma,\tau) = c(\sigma,\tau)u_\sigma u_\tau u_{\sigma\tau}^{-1}$. Then the map $(u,\sigma) \mapsto (u, u_\sigma\sigma)$ is an isomorphism between the groups G_1 and G_2 that produces the equivalence between the two group extensions. □

We should note that this result tells us that we can give a group structure to the equivalence classes of the group extensions of Q with kernel $\{\pm 1\}$. If Q is abelian, some of the extensions that we defined using the 2-cocycles could be also abelian. Those commutative extensions are classified by the subgroup $\mathrm{Ext}^2(Q,\{\pm 1\})$ that we defined earlier, since for Q abelian the fact that $(u,\sigma)(v,\tau) = (v,\tau)(u,\sigma)$ is equivalent to $c(\sigma,\tau) = c(\tau,\sigma)$.

In this section we considered group extensions considering as a kernel the group $\{\pm 1\}$. The theory can be developed in a very similar way considering instead any abelian group K, although in that case the extensions that are classified by the second cohomology group $H^2(Q,K)$ are the *central extensions*: the ones such that $i(K) \subseteq Z(G)$.
More generally, if we consider abelian kernels K, an extension determines an action G over K obtained by defining ${}^\sigma k = s(\sigma)ks(\sigma)^{-1}$, and the map $c(\sigma,\tau)$ satisfies the 2-cocycle condition modified by the action

$${}^\sigma c(\tau,\mu)c(\sigma,\tau\mu) = c(\sigma,\tau)c(\sigma\tau,\mu),\ \forall\sigma,\tau,\mu \in Q.$$

Once we fix an action $Q \to \mathrm{Aut}(K)$ which gives K a structure of G-module it can be shown that $H^2(Q,K)$ classifies the equivalence classes of extensions of Q which kernel K which yield the action we fixed.
Since only the trivial action can be considered over $\mathbb{Z}/2\mathbb{Z}$ (and hence $i(\{\pm 1\}) \subseteq Z(G)$)

to study the extensions in which the kernel is the group $\{\pm 1\}$ we do not need to consider actions.

2. The field embedding problem

Let char$K \neq 2$. Let F/K be a Galois extension with Galois group $Q = \mathrm{Gal}(F/K)$. In this section we will study quadratic extensions E/F such that the extension E/K is Galois. This corresponds to an exact sequence

$$1 \longrightarrow \mathrm{Gal}(E/F) \xrightarrow{incl} \mathrm{Gal}(E/K) \xrightarrow{res} \mathrm{Gal}(F/K) \longrightarrow 1$$

which gives us the group $\mathrm{Gal}(E/K)$ as a group extension of $\mathrm{Gal}(F/K)$ with kernel $\{\pm 1\}$. Since char$K \neq 2$ all the quadratic extensions of F are of the form $E = F(\sqrt{\gamma})$, where γ is not a square of F. The following proposition gives a necessary and sufficient condition for the extension E/K being Galois where $E = F(\sqrt{\gamma})$:

PROPOSITION 9. *Let $\gamma \in F^*$ and let $E = F(\sqrt{\gamma})$. Then E/K is Galois if, and only if, for all $\sigma \in Q$ there exists an element $b_\sigma \in F^*$ such that ${}^\sigma\gamma = b_\sigma^2\gamma$.*

PROOF. Assume that E/K is Galois. Obviously if γ is a square in F^* then $E = F$ and the extension is Galois by hypothesis, and if $\gamma = a^2$ then ${}^\sigma\gamma = ({}^\sigma a)^2 = ({}^\sigma a/a)^2\gamma$ which satisfies the condition for $b_\sigma = {}^\sigma a/a$.
Now assume $\gamma \notin F^{*2}$. The extension E/K is if, and only if, for any K-embedding σ of E into and algebraic closure ${}^\sigma E = E$, which is equivalent to ${}^\sigma\sqrt{\gamma} = a + b\sqrt{\gamma}$ with $a, b \in F$. Then ${}^\sigma\gamma = a^2 + \gamma b^2 + 2ab\sqrt{\gamma}$, but since $\gamma \in F$ and F/K is normal then ${}^\sigma\gamma \in F$ and we must have $2ab = 0$. Since char$K \neq 2$ then either $a = 0$ or $b = 0$.
If $b = 0$ then ${}^\sigma\sqrt{\gamma} = a$, but this would mean that $\sqrt{\gamma} \in F$, but we assumed that γ was not a square in F. This means $a = 0$ and hence ${}^\sigma\gamma = b^2\gamma$.
Conversely, we need to prove that if such b_σ exist then E/K is Galois. The only thing that is not trivial is that the extension E/K is normal. Let σ be a K-embedding of E into an algebraic closure. We have to check that ${}^\sigma E = E$ and again since F/K is normal in suffices to check that ${}^\sigma\sqrt{\gamma} \in E$.
But ${}^\sigma(\sqrt{\gamma})^2 = (b_\sigma\sqrt{\gamma})^2$, and this equation for ${}^\sigma\sqrt{\gamma}$ has only the solutions $b_\sigma\sqrt{\gamma} \in E$ and $-b_\sigma\sqrt{\gamma} \in E$ (since it is a polynomic equation of degree 2 in a field), and since both belong to E we conclude that ${}^\sigma E = E$ and that the extension is normal and hence Galois. □

For the rest of the section assume that the hypothesis of the previous proposition is fulfilled. We will now define a 2-cocycle of $Z^2(Q, \{\pm 1\})$ using the elements b_σ that we defined in the previous proposition:

PROPOSITION 10. *The map*

$$\begin{array}{rccc} c: & Q \times Q & \longrightarrow & \{\pm 1\} \\ & (\sigma, \tau) & \longmapsto & b_\sigma {}^\sigma b_\tau b_{\sigma\tau}^{-1} \end{array}$$

is a 2-cocycle of $Z^2(Q, \{\pm 1\})$.

PROOF. We have to see that $c(\sigma,\tau) \in \{\pm 1\}$ for all $\sigma, \tau \in Q$ and that in verifies the 2-cocycle identity. For the first part, we compute

$$b_{\sigma\tau}^2 \gamma = {}^{\sigma\tau}\gamma = {}^{\sigma}({}^{\tau}\gamma) = {}^{\sigma}(b_\tau^2 \gamma) = {}^{\sigma} b_\tau^{2\sigma} \gamma = {}^{\sigma} b_\tau^2 b_\sigma^2 \gamma$$

and hence $b_{\sigma\tau}^2 = {}^{\sigma} b_\tau^2 b_\sigma^2$ and $c(\sigma,\tau) = b_\sigma {}^{\sigma} b_\tau b_{\sigma\tau}^{-1} \in \{\pm 1\}$.
To see that they are a 2-cocycle, we write explicitly the condition for being a 2-cocycle in terms of the b_σ:

$$\left(b_\tau {}^{\tau} b_\mu b_{\tau\mu}^{-1}\right)\left(b_\sigma {}^{\sigma} b_{\tau\mu} b_{\sigma\tau\mu}^{-1}\right) = \left(b_\sigma {}^{\sigma} b_\tau b_{\sigma\tau}^{-1}\right)\left(b_{\sigma\tau} {}^{\sigma\tau} b_\mu b_{\sigma\tau\mu}^{-1}\right).$$

Now since all of the terms inside of the parentheses are either 1 or -1 (and hence belong to the base field K), they are fixed by the K-automorphisms of the Galois group Q, i.e., $\left(b_\tau {}^{\tau} b_\mu b_{\tau\mu}^{-1}\right) = {}^{\sigma}\left(b_\tau {}^{\tau} b_\mu b_{\tau\mu}^{-1}\right) = \left({}^{\sigma} b_\tau {}^{\sigma\tau} b_\mu {}^{\sigma} b_{\tau\mu}^{-1}\right)$. This is

$$\left({}^{\sigma} b_\tau {}^{\sigma\tau} b_\mu {}^{\sigma} b_{\tau\mu}^{-1}\right)\left(b_\sigma {}^{\sigma} b_{\tau\mu} b_{\sigma\tau\mu}^{-1}\right) = \left(b_\sigma {}^{\sigma} b_\tau b_{\sigma\tau}^{-1}\right)\left(b_{\sigma\tau} {}^{\sigma\tau} b_\mu b_{\sigma\tau\mu}^{-1}\right)$$

which is trivally true after cancelling terms. □

This 2-cocycle only depends on the extension and not on the element γ used:

LEMMA 12. *Let γ, γ' be such that $F(\sqrt{\gamma}) = F(\sqrt{\gamma'})$. Then both γ and γ' give the same 2-cocyle, defined as in the previous proposition.*

PROOF. We know that $F(\sqrt{\gamma}) = F(\sqrt{\gamma'})$ if, and only if, $\gamma = a^2\gamma'$ with $a \in F^*$. Then

$$b_\sigma^2 a^2 \gamma' = b_\sigma^2 \gamma = {}^{\sigma}\gamma = {}^{\sigma}(a^2\gamma') = {}^{\sigma}(a^2) {}^{\sigma}\gamma'$$

so $b'_\sigma = b_\sigma a / {}^{\sigma} a$ for all $\sigma \in Q$. Substituting this into the expression of the 2-cocycle for γ' yields

$$b'_\sigma {}^{\sigma} b'_\tau b'^{-1}_{\sigma\tau} = \frac{a \cdot {}^{\sigma} a \cdot {}^{\sigma\tau} a}{{}^{\sigma} a \cdot {}^{\sigma\tau} a \cdot a} b_\sigma {}^{\sigma} b_\tau b_{\sigma\tau}^{-1} = b_\sigma {}^{\sigma} b_\tau b_{\sigma\tau}^{-1}$$

and hence both 2-cocycles coincide over all $Q \times Q$ and must be the same. □

This means that every solution $E = F(\sqrt{\gamma})$ of the embedding problem determines an element of $Z^2(Q, \{\pm 1\})$ which corresponds to the group extension given by the exact sequence of Galois groups.

The next problem we have to adress is to determine in terms of the element γ that generates the quadratic extension when two extensions are equivalent. To do this, we will need to introduce some results. Recall that in a Galois extension E/K (with Galois group G) we define the *norm* and the *trace* of an element $\alpha \in E$ as

$$N_{E/K}(\alpha) = \prod_{\sigma \in G} {}^{\sigma}\alpha, \quad \mathrm{Tr}_{E/K}(\alpha) = \sum_{\sigma \in G} {}^{\sigma}\alpha.$$

The norm is a group homomorphism $E^* \to K^*$ and the trace is a K-linear map $E \to K$. Let S be a set. Then the set of the maps $S \to K$ equipped with the sum and the product by scalars is a K-vector space. We will say that a collection of such maps is *linearly independent* when they are linearly independent in that vector space.

THEOREM 12 (Linear independence of characters). *Let G be a group and let $\{\chi_i\}_{i\in I}$ be a collection of characters (group homomorphisms) $G \to K^*$ from G to the multiplicative group of a field K. If the χ_i are different maps, they are independent (as maps $G \to K$).*

PROOF. Assume that they are not independent. Let $\Sigma a_i\chi_i$, with $a_i \in K$ and almost all zero, be a nontrivial linear combination that is identically zero and that has the minimum number of nonzero coefficients among all the nontrivial linear combinations that are identically zero. Since the maps χ_i take values in K^*, at least two of the coefficients are nonzero. Let those coefficients be a_j and a_k. Given any two $g, h \in G$,

$$\sum a_i\chi_i(h)\chi_i(h^{-1}g) = \sum a_i\chi_i(g) = 0, \forall g \in G.$$

Since the action by translation of a group acting on itself is transitive, when g runs through G, $h^{-1}g$ does it as well. Hence we have a new linear combination that is identically zero, $\sum a_i\chi_i(h)\chi_i$. If we multiply the original combination by $\chi_j(h)$ and substract this one to it, we obtain the combination

$$\sum b_i\chi_i = \sum a_i(\chi_j(h) - \chi_i(h))\chi_i,$$

that is also identically zero. Notice that this combination has more zero coefficients that the original one, since $a_i = 0 \Rightarrow b_i = 0$ and $b_j = a_j(\chi_j(h) - \chi_j(h)) = 0$ (recall that we took $a_j \neq 0$), and thus it must be the trivial combination. Then since $a_k \neq 0$ we have that $\chi_j(h) = \chi_k(h)$ for all $h \in G$ and this implies that $\chi_j = \chi_k$, which is a contradiction since we assumed that no two characters were equal. □

COROLLARY 6 (Linear independence of homomorphisms). *Let K and L be fields, and let $\{\sigma_i\}_{i\in I}$ be field embeddings $\sigma_i : K \to L$. If they are different, they are L-independent.*
In particular, given different embeddings $\sigma_1, \ldots, \sigma_n$ from K to L and nonzero elements $\alpha_1, \ldots, \alpha_n \in L$, there exists an element $x \in K$ such that ${\alpha_1}^{\sigma_1}x + \cdots + {\alpha_n}^{\sigma_n}x \neq 0$.

PROOF. It is enough to apply the previous theorem to the characters $\sigma_i|_{K^*} : K^* \to L^*$. If $\sum a_i\sigma_i = 0$ then $\sum a_i(\sigma_i|_{K^*}) = 0$ and the theorem tells us that all coefficients must be zero. □

Now we will give some definitions which are analogous to the ones we gave for 2-cocycles and 2-coboundaries:

DEFINITION 15. *Let G be a group and M be a G-module. A* 1-cocycle *of G in M is a collection $\{\alpha_\sigma\} \subset M$ such that*

$$\alpha_{\sigma\tau} = {\alpha_\sigma}^{\sigma}\alpha_\tau$$

for all $\sigma, \tau \in G$. It is easy to check that they form a group with the product element by element that we will call $Z^1(G, M)$.
A 1-coboudary *of G in M is a collection of elements $\{\alpha_\sigma\}_{\sigma\in G}$ such that there exists some $\beta \in M$ for which*

$$\alpha_\sigma = \frac{{}^{\sigma}\beta}{\beta}$$

for every $\sigma \in G$. It is not difficult either to check that they form a subgroup of $Z^1(G, M)$ that we shall denote $B^1(G, M)$.
Finally, we define the first cohomology group *of G in M as the quotient group*

$$H^1(G, M) = Z^1(G, M)/B^1(G, M).$$

THEOREM 13 (Hilbert's theorem 90). *Let F/K be a Galois extension and let $Q = \mathrm{Gal}(F/K)$ acting on F with the Galois action. Then $H^1(Q, F^*)$ is the trivial group, i.e., each 1-cocycle of Q in F^* is a 1-coboundary.*

PROOF. Let $\{\alpha_\sigma\}_{\sigma\in G}$ be a 1-cocycle of Q in F^*. Since all the α_τ are nonzero (they belong to F^*), the following linear combination is not the zero map (by the theorem of linear independence)

$$\sum_{\tau\in Q} \alpha_\tau \tau : F \to F$$

this is, it exists $\theta \in F$ such that

$$\beta = \sum_{\tau\in Q} \alpha_\tau{}^\tau\theta \neq 0.$$

But then for each $\sigma \in Q$

$$^\sigma\beta = \sum_{\tau\in Q} {}^\sigma\alpha_\tau{}^{\sigma\tau}\theta = \sum_{\tau\in Q} \alpha_\sigma^{-1}\alpha_{\sigma\tau} \cdot {}^{\sigma\tau}\theta = \alpha_\sigma^{-1} \sum_{\tau\in Q} \alpha_{\sigma\tau} \cdot {}^{\sigma\tau}\theta = \alpha_\sigma^{-1}\beta.$$

Hence $\alpha_\sigma = \beta/{}^\sigma\beta$. Setting $\gamma = \beta^{-1}$ gives $\alpha_\sigma = {}^\sigma\gamma/\gamma$. □

Now we are ready to determine when two extensions are equivalent in the sense of the group extensions:

PROPOSITION 11. *Two elements γ, γ' give equivalent extensions if, and only if, $\gamma' = a\gamma$ modulo squares of F, with $a \in K^*$.*

PROOF. If $\gamma' = a\gamma$, ${}^\sigma\gamma' = {b'_\sigma}^2\gamma'$ leads to ${}^\sigma\gamma = {b'_\sigma}^2\gamma$ (since ${}^\sigma a = a$ because $a \in K$ and $\sigma \in Q = \mathrm{Gal}(F/K)$ fixes the elements of the base field), and hence the b_σ and b'_σ elements coincide and the extensions are equivalent.
Now assume that the extensions are equivalent, i.e., that the corresponding 2-cocycles are equivalent modulo coboundaries. This is to say that b_σ/b'_σ is a 1-cocycle. By Hilbert's theorem 90, it is a 1-coboundary, this is, there exists $\beta \in F^*$ such that

$$\frac{b_\sigma}{b'_\sigma} = \frac{{}^\sigma\beta}{\beta}$$

Then, since ${}^\sigma\gamma = b_\sigma^2\gamma$ and ${}^\sigma\gamma' = {b'_\sigma}^2\gamma'$,

$${}^\sigma\left(\frac{\gamma}{\gamma'}\right) = \left(\frac{b_\sigma}{{b_\sigma}'}\right)^2 \frac{\gamma}{\gamma'} = \left(\frac{{}^\sigma\beta}{\beta}\right)^2 \frac{\gamma}{\gamma'}$$

Then

$${}^\sigma\left(\frac{\gamma}{\gamma'\beta^2}\right) = \frac{\gamma}{\gamma'\beta^2}$$

and since $\sigma \in \mathrm{Gal}(F/K)$ and the element $\gamma/(\gamma'\beta^2)$ is fixed by all $\sigma \in \mathrm{Gal}(F/K)$, we must have $\gamma/(\gamma'\beta^2) \in K$. This is to say that γ/γ' is a square of F^* times an element of K, and since multiplying by a square of F^* gives the same extension we have finished the proof. □

This allows us to classify the embedding problems in terms of extension equivalence classes, so that for each extension F/K with Galois group isomorphic to Q and each element of $H^2(Q, \{\pm 1\})$ (that represents a class of extensions) one can study the solvability of the corresponding embedding problem. But solving the embedding problems is equivalent to finding the appropiate b_σ elements, as shown in the following proposition.

PROPOSITION 12. *Let $\{b_\sigma\}_{\sigma\in Q}$ be a collection of elements of F^* such that $b_\sigma{}^\sigma b_\tau b_{\sigma\tau}^{-1} \in \{\pm 1\}$. Then the map $(\sigma, \tau) \mapsto b_\sigma{}^\sigma b_\tau b_{\sigma\tau}^{-1}$ is a 2-cocycle. Moreover, there exist elements $x \in F^*$ such that*

$$\gamma = \sum_{\sigma\in Q} \frac{{}^\sigma x}{b_\sigma^2} \neq 0,$$

and all those γ elements are solutions to the corresponding embedding problem.

PROOF. The fact that the map is a 2-cocycle has already been proven (since we only used this hypothesis when proving that the elements $b_\sigma{}^\sigma b_\tau b_{\sigma\tau}^{-1}$ with ${}^\sigma\gamma = b_\sigma^2\gamma$ were a 2-cocycle). The existence of elements x such that the resulting γ is nonzero is guaranteed by the theorem of linear independence of field homomorphisms (since otherwise we would have a linear combination of all the elements of Q that is identically zero).
To see that if γ is defined in this way it is a solution of the embedding problem, it is enough to compute

$${}^\sigma\gamma = \sum_{\tau\in Q} \frac{{}^{\sigma\tau}x}{{}^\sigma b_\tau^2} = \sum_{\tau\in Q} \frac{{}^{\sigma\tau}x \cdot b_\sigma^2}{b_{\sigma\tau}^2} = b_\sigma^2 \sum_{\sigma\tau\in Q} \frac{{}^{\sigma\tau}x}{b_{\sigma\tau}^2} = b_\sigma^2\gamma$$

and hence by the equivalent condition we proved before, if we let $E = F(\sqrt{\gamma})$, the extension E/K is Galois and a solution of the embedding problem. □

3. Some examples

We will devote this section to solve all the quadratic embedding problems where the Galois group Q of the extension F/K is the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. That extension has three different quadratic subextensions, $K(\sqrt{a_i})$ for $i = 1, 2, 3$. In this case, the second cohomology group $H^2(V_4, \{\pm 1\}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ has order 8, so there are eight different embedding problems, seven of which are nontrivial. The following result will be useful to solve problems involving the V_4 group.

PROPOSITION 13 (Biquadratic extensions). *Let $K \subset F \subset E$ be fields such that the extension E/K is a tower of two quadratic extensions, $[F : K] = [E : F] = 2$. Then $F = K(\sqrt{a}), a \in K^*/K^{*2}$ and $E = F(\sqrt{\alpha})$, with $\alpha = b + c\sqrt{a} \in F^*/F^{*2}$ and $b, c \in K$. We define $\beta = b - c\sqrt{a} \in F^*$ and $d = b^2 - ac^2 \in K^*$. Then the extension E/K behaves as follows:*

(1) *If $d \in K^{*2}$ the extension E/K is Galois and* $\mathrm{Gal}(E/K) = V_4$. *The quadratic subextensions are $K(\sqrt{a})$, $K(\sqrt{b})$ and $K(\sqrt{ab})$ if $c = 0$, and $K(\sqrt{a})$, $K(\sqrt{\alpha} + \sqrt{\beta})$ and $K(\sqrt{\alpha} - \sqrt{\beta})$ if $c \neq 0$.*
(2) *If $ad \in K^{*2}$ the extension E/K is Galois and* $\mathrm{Gal}(E/K) = C_4$ *and has a single quadratic subextension, $K(\sqrt{a})$.*
(3) *If none of the two conditions are fulfilled then the extension is not Galois and the normal closure N has Galois group* $\mathrm{Gal}(N/K) = D_8$.

We will not give the proof of this last proposition since it is too technical and can be found in any course on Galois theory. Let us begin by considering the embedding problem where the group $\mathrm{Gal}(E/K)$ is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

PROPOSITION 14. *Let F/K be a Galois extension with* $\mathrm{Gal}(F/K) = V_4$ *and let $K(\sqrt{a_i})$, $i = 1, 2, 3$ be its three quadratic subextensions.Consider the embedding problem $\pi_i : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Gal}(F/K)$ where $K(\sqrt{a_i})$ is the fixed field of $\pi_i(0, 1)$. Then*

(1) *The embedding problem π_i has a solution if, and only if, a_i is a sum of two squares of K.*
(2) *If two of the embedding problems π_i have a solution, then the third one also has a solution.*

PROOF. Assume the problem is solvable. Let $a = a_i$ and define the elements b, d, α, β as in the previous proposition. The subgroup lattice of $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is shown in Figure 1.
Then we have that $\mathrm{Gal}(K(\sqrt{\alpha})/K) = \mathbb{Z}/4\mathbb{Z}$ and hence $ad = u^2, u \in K^*$. This means that $b^2a - (ca)^2 = u^2$. If $b = 0$, then -1 is a square of K and hence all the elements of K are squares. Then the result follows easily. If $b \neq 0$, then

$$a = \left(\frac{u}{b}\right)^2 + \left(\frac{ca}{b}\right)^2$$

and we are done.
Conversely, assume $a_i = a = x^2 + y^2$ with $x, y \in K^*$. Then, taking $\alpha = a + x\sqrt{a}$, we have that $d = a^2 - x^2a = ay^2$ so $ad \in K^{*2}$ and $\mathrm{Gal}(K(\sqrt{\alpha})) = C_4$. Thus, if $i \neq j$, $\mathrm{Gal}(K(\sqrt{\alpha}, \sqrt{a_j})) = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Finally we have to prove that if two of the embedding problems are solvable then the third one is also solvable. Assume that $\{i, j, k\} = \{1, 2, 3\}$ and that the embedding problems π_i and π_j are have a solution. Then $a_i = x^2 + y^2$ and $a_j = z^2 + t^2$, with $x, y, z, y \in K$. Then it can be easily checked that (this result is know as Brahmagupta's identity)

$$a_ia_j = (xz + yt)^2 + (xt - yz)^2,$$

and since $a_k = u^2a_ia_j$, $u \in K$, a_k is a a sum of two squares of K and hence the third embedding problem has a solution. □

The previous result implies that the number of embedding problems that could have a solution for a given extension is either zero, one or three:

(1) If $a_1 = -2$, $a_2 = 3$ and $a_3 = a_1a_2 = -6$, none of the problems have a solution since none of those numbers are a sum of two squares.

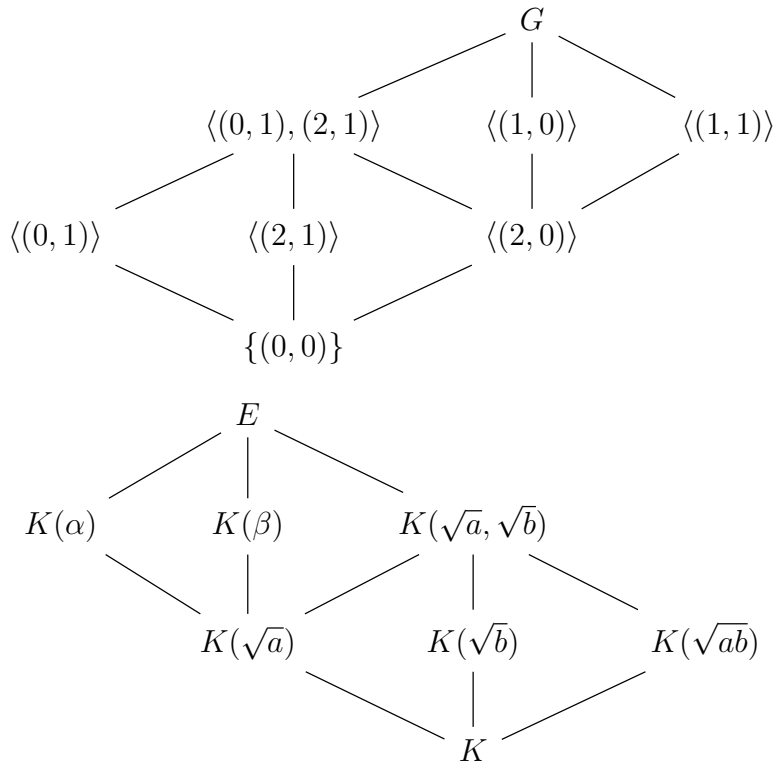

FIG. 1. Lattice of subgroups and subfields corresponding to Proposition 14.

(2) If $a_1 = 2$, $a_2 = -1$ and $a_3 = a_1a_2 = -2$, only π_1 is solvable ($2 = 1^2 + 1^2$).
(3) If $a_1 = 2$, $a_2 = 5$ and $a_3 = a_1a_2 = 10$, all three problems have a solution: $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$ and $10 = 3^2 + 1^2$.

Another problem that can be solved quite easily is obtained by considering $\mathrm{Gal}(E/K) = D_8$ and again $Q = \mathrm{Gal}(F/K) = V_4$:

PROPOSITION 15. *Let F/K be a Galois extension with $\mathrm{Gal}(F/K) = V_4$ and let $K(\sqrt{a_i})$, $i = 1, 2, 3$ be its three quadratic subextensions. Consider the embedding problem $\pi_i : D_8 \to \mathrm{Gal}(F/K)$, where $K(\sqrt{a_i})$ is the fixed field of $\pi_i(r)$. This problem is solvable if, and only if, the equation $a_jX^2 + a_kY^2 = Z^2$ has a nontrivial solution in the field K.*

PROOF. We will use the same notation as in the other propositions of this section. The subgroup/subfield lattice is presented in Figure 2.

Assume that the problem has a solution. Then $a = a_ju^2$ and $d = a_kv^2$, $u, v \in K^*$. Since $d = b^2 - c^2a$, we have that $a_ju^2 = b^2 - a_k(cv)^2$ and the equation has a solution.

Conversely, assume that there exists a nontrivial solution $a_jx^2 + a_ky^2 = z^2$. Then define $a = a_j$, $\alpha = z + x\sqrt{a_j}$. Then $d = z^2 - a_jx^2 = a_ky^2$ is not a square, and neither is $ad = a_ja_k^2 = a_iw^2y^2$, where we have set $w^2a_i = a_ja_k$. Hence the extension is not Galois and, according to the proposition above, its normal closure is a Galois extension with Galois group D_8, which solves the embedding problem. □

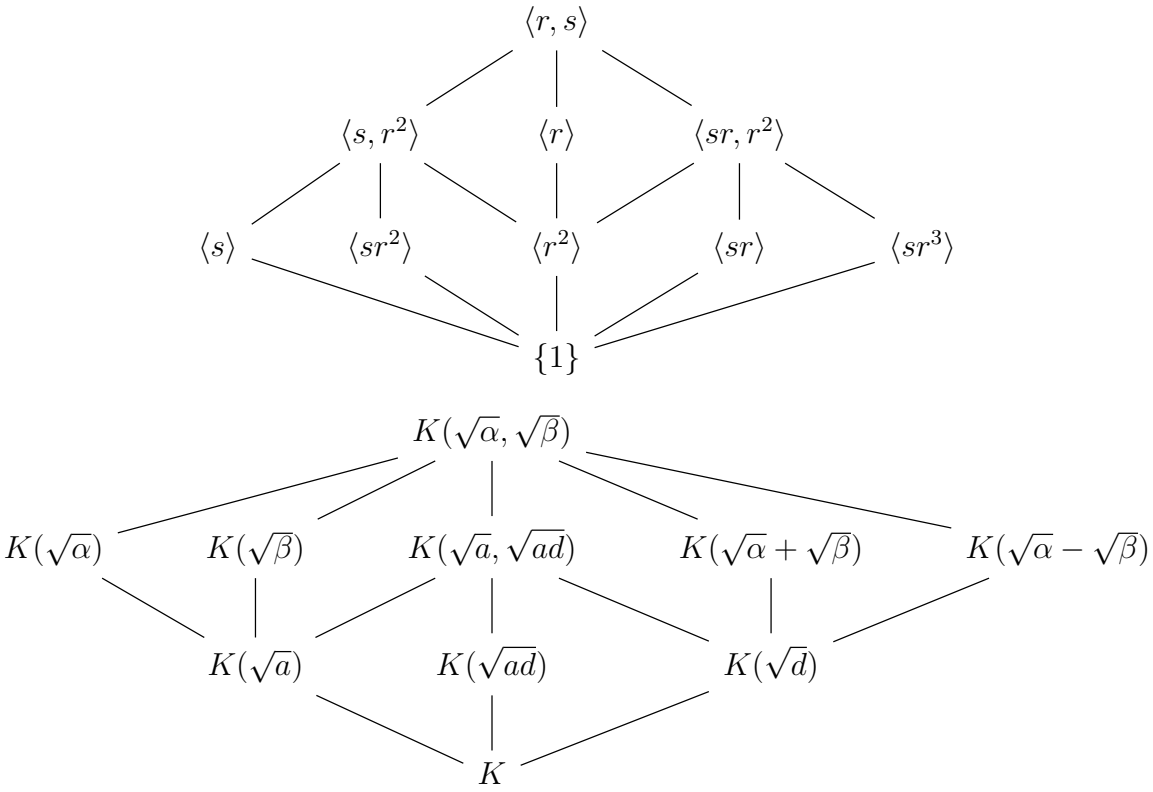

FIG. 2. Lattice of subgroups and subfields corresponding to Proposition 15.

This time, each of the three problems behaves independently of the other two in terms of having a solution (the existence of the solution of the equation $aX^2 + bY^2 = Z^2$ is given by Legendre's theorem):

- If $a_1 = 2$, $a_2 = 5$, $a_3 = a_1a_2 = 10$, none of the problems have a solution.
- If $a_1 = 2$, $a_2 = 3$, $a_3 = a_1a_2 = 6$, only the first problem has a solution ($3\cdot 1^2 + 6\cdot 1^2 = 3^2$).
- If $a_1 = 2$, $a_2 = -1$, $a_3 = a_1a_2 = -2$, the second and the third problems have a solution, but not the first one ($2 \cdot 1^2 - \cdot 1^2 = 1^2$ and $3 \cdot 1^2 - 1 \cdot 1^2 = 4^2$).
- If $a_1 = 5$, $a_2 = 29$, $a_3 = a_1a_2 = 145$ all three problems have a soltuion.

The other nonabelian group of order 8 is the quaternion group Q_8 (we will consider again $\mathrm{Gal}(F/K) = V_4$). In this case there is a single embedding problem, and we can give an equivalent condition for that problem in terms of an equivalence of quadratic forms as proved by Witt in 1936. This Witt result was the inspiration for the more sophisticated cases that we will introduce in the following chapter.

PROPOSITION 16. *Let F/K be a Galois extension with $\mathrm{Gal}(F/K) = V_4$ and let $K(\sqrt{a_i})$, $i = 1, 2, 3$ be its three quadratic subextensions. The embedding problem $\pi : Q_8 \to \mathrm{Gal}(F/K)$ has a solution if, and only if, the quadratic form $\langle a_1, a_2, a_3\rangle$ is equivalent to $\langle 1, 1, 1\rangle$. Moreover, if the matrix $P = (p_{ij}) \in GL_3(K)$ is such that*

$$P^t \cdot \mathrm{diag}(a_1, a_2, a_3)P = \mathrm{Id}_3$$

the solutions of the embedding problems are the extensions

$$F\left(\sqrt{r(1+p_{11}\sqrt{a_1}+p_{22}\sqrt{a_2}+p_{33}\sqrt{a_3}}\right), r \in K^*.$$

PROOF. Let $F = K(\sqrt{a}, \sqrt{b})$ with $a, b \in K^*$ and assume that the three quadratic subextensions of F are $K(\sqrt{a})$, $K(\sqrt{b})$ and $K(\sqrt{ab})$ (hence $a_1 = a$, $a_2 = b$, $a_3 = ab$). Let $G = \mathrm{Gal(F/K)} \cong V_4 = \{1, \sigma, \tau, \sigma\tau\}$, where σ is the nontrivial automorphism that fixes $K(\sqrt{a})$ and τ is the nontrivial automorphism that fixes $K(\sqrt{b})$ (and hence $\sigma\tau$ is the nontrivial automorphism that fixes $K(\sqrt{ab})$). Consider the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = -1$ and $ij = k = -ji$. The embedding problem in terms of extensions of groups is given by an exact sequence of groups

$$1 \longrightarrow \{\pm 1\} \longrightarrow Q_8 \longrightarrow V_4 \longrightarrow 1.$$

Out of the eight extensions of the Klein group which have kernel of order 2, only one has group isomorphic to Q_8. It is characterized by the fact that the preimages of all nontrivial elements of the Klein group have order 4: the preimages of σ, τ and $\sigma\tau$ are i, j and k, in some order. In terms of the associated cocycle, this extension is characterized by the fact that $c(\sigma, \sigma) = c(\tau, \tau) = c(\sigma\tau, \sigma\tau) = -1$.
We fix the epimorphism $Q_8 \to \mathrm{Gal}(F/K)$ such that $i \mapsto \sigma$, $j \mapsto \tau$ and to compute the 2-cocycle associated to the extension we take i, j and $k = ij$ as preimages of σ, τ and $\sigma\tau$.
Giving a solution of the embedding problem is equivalent to finding an element $\gamma \in F^*$ and elements $\beta_s \in F^*$ for each four elements $s \in G$ such that ${}^s\gamma = \beta_s^2\gamma$ for all γ and such that $\beta_s^s\beta_s = -1$ for all $s \neq 1$. To avoid confusion with the element b of the number field, we will use the notation β_s instead of b_s along this proof. The first condition implies that the extension $F(\sqrt{\gamma})/K$ is Galois and the second one that the Galois group $\mathrm{Gal}(F(\sqrt{\gamma})/K)$ is isomorphic to the quaternion group. Notice that the condition $\langle a, b, ab\rangle \sim \langle 1, 1, 1\rangle$ is equivalent to the fact that there exists a matrix

$$S = \begin{pmatrix} p_{11}\sqrt{a} & p_{12}\sqrt{a} & p_{13}\sqrt{a} \\ p_{21}\sqrt{b} & p_{22}\sqrt{b} & p_{23}\sqrt{b} \\ p_{31}\sqrt{ab} & p_{32}\sqrt{ab} & p_{33}\sqrt{ab} \end{pmatrix} \in \mathrm{GL}_3(F)$$

such that $S^tS = \mathrm{Id}_3$.
We can always take $\beta_1 = 1$ so we only need to find β_s for $s \neq 1$. The conditions for the β_s lead to the following conditions for $\gamma\beta_s$:

$$(\gamma\beta_s)^2 = \gamma\,{}^s\gamma,\ \frac{(\gamma\beta_s)\,{}^s(\gamma\beta_s)}{(\gamma\beta_s)^2} = c(s, s)$$

and the second condition, for $s \neq 1$ is equivalent to $(\gamma\beta_s)\,{}^s(\gamma\beta_s) = -(\gamma\beta_s)^2$.

Now assume that such an $S \in \mathrm{GL}_3(F)$ exists. We can assume without loss of generality that $\det(S) = 1$, since if $\det(S) = -1$ changing the sign of a row or a column of the matrix $P = (p_{ij})$ leads to a matrix S with positive determinant. In this case we take

$$\gamma\beta_\sigma = p_{23}\sqrt{b} - p_{32}\sqrt{ab},\ \gamma\beta_\tau = p_{13}\sqrt{a} - p_{31}\sqrt{ab},\ \gamma\beta_{\sigma\tau} = p_{12}\sqrt{a} - p_{21}\sqrt{b}.$$

We must check that they fulfill the conditions. The second condition is obvions since applying s to $\gamma\beta_s$ makes it change its sign and hence $c(s,s) = -1$ in all three cases.
We will now check the first condition. The fact that the matrix S is orthogonal tells us that their rows and columns are all vectors of norm 1 with respect to the standard quadratic form (corresponding to the sum of squares), and, since $\det(S) = 1$, we have that $S^t = S^{-1} = (\det(S))^{-1}(S^*)^t$ and hence $S = S^*$, where S^* is the adjoint matrix of S.
We have to check, for instance, that

$$\gamma\,{}^{\sigma}\gamma = (1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{ab})(1 + p_{11}\sqrt{a} - p_{22}\sqrt{b} - p_{33}\sqrt{ab} = \\ = 1 + p_{11}^2 a - p_{22}^2 p_{33}^2 ab + (p_{11} - bp_{22}p_{33})\sqrt{a}$$

equals

$$(\gamma\beta_\sigma)^2 = p_{23}^2 b + p_{32}^2 ab - 2bp_{23}p_{32}\sqrt{a}.$$

The equality of the coefficients of $\sqrt{a}$ follows from the fact that $S = S^*$. Considering the position $(1,1)$ of both matrices

$$p_{11}\sqrt{a} = \begin{vmatrix} p_{22}\sqrt{b} & p_{23}\sqrt{b} \\ p_{32}\sqrt{ab} & p_{33}\sqrt{ab} \end{vmatrix} \Rightarrow p_{11} = bp_{22}p_{33} - bp_{23}p_{32}.$$

The equality between the rest of the terms is obtained, by, for instance, substracting to $p_{23}^2 b + p_{32}^2 ab$ the sum of the squares of the second and the third row of S (equivalent to substracting 2, since the matrix is orthogonal), and adding to it the sum of the squares of first column of S plus 1 (so we add 2 to compensate). The result is $1 + p_{11}^2 a - p_{22}^2 b - p_{33}^2 ab$, as desired. The other two cases are checked in the same way.

Conversely, assume that the problem is solvable and let β_σ, β_τ and $\beta_{\sigma\tau}$ be the elements of F corresponding to a solution. Let $\alpha = 1 + \beta_\sigma^2 + \beta_\tau^2 + \beta_{\sigma\tau}^2$. The matrix

$$S = \alpha^{-1} \begin{pmatrix} \frac{1}{2}(1 + \beta_\sigma^2 - \beta_\tau^2 - \beta_{\sigma\tau}^2) & \beta_\sigma\beta_\tau - \beta_{\sigma\tau} & \beta_\sigma\beta_{\sigma\tau} + \beta_\tau \\ \beta_\sigma\beta_\tau + \beta_{\sigma\tau} & \frac{1}{2}(1 - \beta_\sigma^2 + \beta_\tau^2 - \beta_{\sigma\tau}^2) & \beta_{\sigma\tau}\beta_\tau - \beta_\sigma \\ \beta_\sigma\beta_{\sigma\tau} - \beta_\tau & \beta_{\sigma\tau}\beta_\tau + \beta_\sigma & \frac{1}{2}(1 - \beta_\sigma^2 - \beta_\tau^2 + \beta_{\sigma\tau}^2) \end{pmatrix} \in \mathrm{M}_3(F)$$

is orthogonal and has the desired form for the matrix S. The fact that it is orthogonal does not depend on the β_s and can be easily checked by direct computation. To see that it has the correct form, we have to see that all entries are an element of K times $\sqrt{a}$, $\sqrt{b}$ or $\sqrt{ab}$, depending on the row. The final step is to prove that the elements of the matrix times γ are an element of K times the corresponding square root. Notice that $\gamma\alpha = \mathrm{Tr}(\gamma) \in K$. For instance, if we let $x = 1 + \beta_\sigma^2 - \beta_\tau^2 - \beta_{\sigma\tau}$ and $\gamma = u + v\sqrt{a} + w\sqrt{b} + k\sqrt{ab}$, then $\gamma x = 4v\sqrt{a}$. For the elements off the diagonal, one must also use the relation $\beta_s^s\beta_t = c(s,t)\beta_{st}$ for $s, t \in \{\sigma, \tau, \sigma\tau\}$. The γ factor of the elements of the matrix cancels out with the γ factor of α, giving the matrix S above. $\square$

Chapter 3
Galois covers of symmetric and alternating groups

In this chapter we will consider quadratic extensions of fields K which have symmetric or alternating groups as Galois group over $\mathbb{Q}$. We will be especially interested in the cases where $G = \mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}_4, \mathfrak{A}_4, \mathfrak{A}_5$ for their interest in the construction of modular forms of weight 1, as we will explain later on. The exact sequence of the corresponding group extension will be

$$1 \longrightarrow \{\pm 1\} \xrightarrow{i} 2G \xrightarrow{\pi} \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1 \ .$$

This extension is said to be a *Galois double cover* of the group $G = \mathrm{Gal}(K/\mathbb{Q})$. Many proofs will be omitted since they use concepts that are beyond the scope of this thesis, such as Clifford algebras and spinor norms. Appropiate references will be mentioned in each section. We will work mostly in the case where $G = \mathfrak{S}_4$ for simplicity, but most of the results that we present are more general.

1. Solvability of the embedding problem for $\mathfrak{S}_4$

Let us define the following notation for the polynomials and fields that will be used in the sections 1 and 2 of this chapter: let $f \in \mathbb{Q}[x]$ be a polynomial whose Galois group over $\mathbb{Q}$ is isomorphic to $\mathfrak{S}_4$, and let x_1, x_2, x_3, x_4 be the roots of f. Let g be the cubic resolvent of f, and let $y_1 = x_1x_2 + x_3x_4$, $y_2 = x_1x_3 + x_2x_4$ and $y_3 = x_1x_4 + x_2x_3$ be its roots. We define the following field extensions (see figure 1):

- $K = \mathbb{Q}(x_1)$ is the number field obtained when one adds to $\mathbb{Q}$ a root of the polynomial f (it has degree 4 over $\mathbb{Q}$).
- $F = \mathbb{Q}(y_1)$ is the number field obtained by adding to $\mathbb{Q}$ a root of the cubic resolvent g (it has degree 3 over $\mathbb{Q}$).
- $E = \mathbb{Q}(x_1, x_2, x_3, x_4)$ is a decomposition field of the polynomial f (it has degree 24 over $\mathbb{Q}$).
- $\widetilde{E} = E(\sqrt{\gamma})$ will a quadratic extension of E that is a solution to the embedding problem that will be explained in this chapter.

It is a well known result that the second cohomology groups of the symmetric and alternating groups are $H^2(\mathfrak{S}_4, \{\pm 1\}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $H^2(\mathfrak{A}_4, \{\pm 1\}) = \mathbb{Z}/2\mathbb{Z}$ (this is general for $\mathfrak{S}_n$

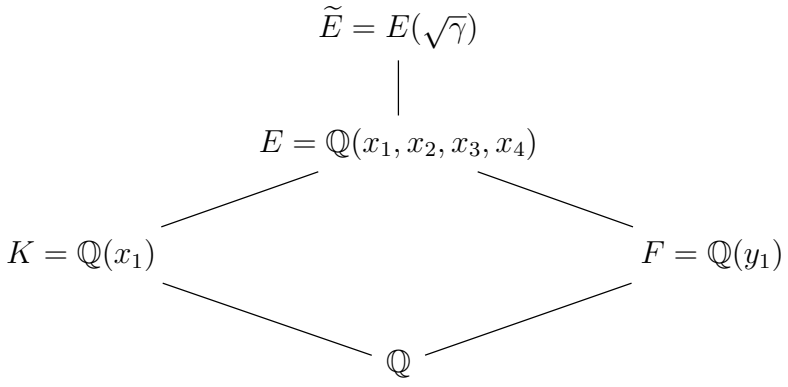

FIG. 1. Diagram of the number fields that will be used in this chapter

and $\mathfrak{A}_n$, with $n \geq 4$). This leads to four different equivalence classes for $\mathfrak{S}_4$ of group extensions according to the previous chapter, two of those reduce to the unique non-trivial double cover $\widetilde{\mathfrak{A}_4}$ of the alternating group $\mathfrak{A}_4$. The four extensions of $\mathfrak{S}_4$ are classified according to the order that have the elements resulting of lifting transpositions and disjoint products of transpositions. Those lifted elements can have either order 2 or order 4. The trivial extension (the cartesian product of the groups $\mathfrak{S}_4$ and $\{\pm 1\}$) lifts both types of elements to elements of order two. Let $\widetilde{\mathfrak{S}_4}$ be the non-trivial double cover of $\mathfrak{S}_4$ in which transpositions lift to involutions (and since we assume that this is the non-trivial double cover the products of disjoint transpositions lift to elements of order 4). The remaining two extensions, which we will not study here, lift transpositions to elements of order 4 and the products of disjoint transpositions to elements of order 2 or 4, respectively.
In [**11**] Serre studied the solvability of the embedding problem

$$\widetilde{\mathfrak{S}_4} \longrightarrow \mathfrak{S}_4 = \mathrm{Gal}(K/\mathbb{Q})$$

and gave a solution in terms of an equivalence of quadratic forms. Given the polynomial $f \in \mathbb{Q}[X]$, we define its associated *trace quadratic form* $\mathrm{Tr}_{K/\mathbb{Q}}(X^2)$ as the quadratic form $x \mapsto \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(x^2)$. Let $T = (T_{ij}) = (\mathrm{Tr}(x_1^i x_1^j))$ be its associated matrix. It can be shown that this matrix can also be computed as

$$T = M^T M, \text{ where } M = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}.$$

It is important to notice that while the matrix M has entries over E, the matrix T has rational entries, and hence we can study the $\mathbb{Q}$-equivalence of the quadratic form $\mathrm{Tr}_{K/\mathbb{Q}}(X^2)$ and other rational quadratic forms.

THEOREM 14 (Serre, [**11**], Th. 1). *The embedding problem*

$$\widetilde{\mathfrak{S}_4} \longrightarrow \mathfrak{S}_4 = \mathrm{Gal}(E/\mathbb{Q})$$

has a solution if, and only if, $w(\mathrm{Tr}_{K/\mathbb{Q}}(X^2)) = (2, d)$ *over all places of* $\mathbb{Q}$*, where* w *is the Witt invariant,* $(\cdot,\cdot)$ *the Hilbert symbol and* d *is the discriminant of the polynomial* f*.*

Using the characterization of the equivalence of quadratic forms over the rational numbers we gave in chapter 1, the previous condition is clearly equivalent to the following one, since $(2, 2d) = (2, -4d) = (2, -d) = (2, d)$:

COROLLARY 7. *The embedding problem*

$$\widetilde{\mathfrak{S}_4} \longrightarrow \mathfrak{S}_4 = \mathrm{Gal}(K/\mathbb{Q})$$

has a solution if, and only if, the quadratic froms $\mathrm{Tr}_{K/\mathbb{Q}}(X^2)$ *and* $\langle 1, 1, 2, 2d\rangle$ *are* $\mathbb{Q}-$*equivalent, where* d *is the discriminant of the polynomial* f*.*

2. Explicit construction of the solutions

While Serre gave an equivalent condition for the solvability of the embedding problem, he left open the problem of finding an explicit form for the element γ such that $E(\sqrt{\gamma})$ is a solution of the embedding problem. This question was addressed by T. Crespo in [**3**] and [**4**].

THEOREM 15 (Crespo). *Assume that the quadratic forms* $\mathrm{Tr}_{K/\mathbb{Q}}(X^2)$ *and* $\langle 1, 1, 2, 2d\rangle$ *are* $\mathbb{Q}$*-equivalent. Let* $P \in \mathrm{GL}_4(\mathbb{Q})$ *be such that*

$$P^T T P = \mathrm{diag}(1, 1, 2, 2d)$$

and define R *as*

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & \sqrt{d}/2 & -\sqrt{d}/2 \end{pmatrix}.$$

Then P *can be chosen such that*

$$\gamma = \det(MPR + \mathrm{Id}) \neq 0$$

and the field $K(\sqrt{\gamma})$ *is a solution of the embedding problem*

$$\widetilde{\mathfrak{S}_4} \longrightarrow \mathfrak{S}_4 = \mathrm{Gal}(K/\mathbb{Q}).$$

The formula above gives an expression of γ in terms of x_1, x_2. But, in fact, one can show that γ can be expressed only in terms of x_1. The following proposition gives an explicit formula to get the expression of γ in terms of x_1:

PROPOSITION 17. *Let* M_f *be the matrix of the trace quadratic form* $\mathrm{Tr}_{K/\mathbb{Q}}(X^2)$*, and let* M_g *be the matrix of the trace quadratic form of the cubic resolvent* $\mathrm{Tr}_{F/\mathbb{Q}}(X^2)$ *(notice that* $M_f \in \mathrm{M}_4(\mathbb{Q})$ *but* $M_g \in \mathrm{M}_3(\mathbb{Q})$*).*
Assume that the quadratic forms $\mathrm{Tr}_{K/\mathbb{Q}}(X^2)$ *and* $\langle 1\rangle \perp \mathrm{Tr}_{F/\mathbb{Q}}(X^2)$ *are* $\mathbb{Q}$*-equivalent. Let* T_f

and T_g be their associated matrices, and let $P \in \mathrm{GL}_4(\mathbb{Q})$ a matrix such that $P^T T_f P = T_g$. Define R as the matrix

$$R = \begin{pmatrix} 1 & 0 \\ 0 & -M_g^{-1} \end{pmatrix}.$$

Then P can be chosen such that

$$\gamma = \det(M_f P R + \mathrm{Id}) \neq 0.$$

Then γ and is a solution of the embedding problem and $\gamma \in \mathbb{Q}(x_1)$.

Proof. The proof of this proposition can be done with the same arguments that Crespo used, whch are beyond the scope of our work. We will prove the fact that this γ only depends on x_1. Consider the subgroup of the Galois group that contains the elements that fix x_1:

$$H = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) :^{\sigma} x_1 = x_1\}$$

We need to show that γ is in the fixed field of that subgroup $K^H = \mathbb{Q}_{\mathbb{k}}$: take any $\sigma \in H$ and compute

$${}^{\sigma}\gamma =^{\sigma} \det(M_f P R + \mathrm{Id}) = \det({}^{\sigma}M_f P^{\sigma} R + \mathrm{Id})$$

Since $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ it acts as a permutation on the roots of the polynomial, and since it fixes x_1 it acts as a permutation on the set $\{x_2, x_3, x_4\}$. By construction, the rows of ${}^{\sigma}M_f$ are a permutation of the rows of M_f (the first one is always fixed since σ fixes x_1). This implies ${}^{\sigma}M_f = EM_f$, where E is a product of elementary (row exchanging) matrices. It is easy to check that σ is also a permutation of the roots of the cubic resolvent and that it permutates the rows of the matrix M_g in the exacty as the last theree rows of M_f. This leads to ${}^{\sigma}R = RE^{-1}$, and finally

$$\begin{aligned} {}^{\sigma}\gamma &= \det(EM_f P R E^{-1} + \mathrm{Id}) = \det(EM_f P R E^{-1} + EE^{-1}) \\ &= \det(M_f P R + \mathrm{Id})\det(E)\det(E)^{-1} = \gamma \end{aligned}$$

so γ is fixed by σ and we are done. □

3. Galois representations and modular forms

3.1. Dedekind domains and Frobenius elements. There are two faithful representations of $\widetilde{\mathfrak{S}}_4$ into $\mathrm{GL}_2(\mathbb{C})$. Choose one of them. Consider a Galois representation of the Galois group of the extension, i.e., an injective map

$$\rho : \mathrm{Gal}(K(\sqrt{\gamma})/\mathbb{Q}) \cong \widetilde{\mathfrak{S}_4} \to \mathrm{GL}_2(\mathbb{C}).$$

L-series of this representation depend only on the characteristic polynomial of the images of certain elements Frob_p. This leads to the results that we will present later, that tell us that the modular form associated to this representation does only depend on the conjugacy classes of the Frobenius elements $\mathrm{Frob}_p \in \mathrm{Gal}(K(\sqrt{\gamma})/\mathbb{Q})$ in $\widetilde{\mathfrak{S}}_4$. We will now present some concepts and results which will be useful to understand what the Frobenius element Frob_p is.

Definition 16 (Dedekind domain). *A Dedekind domain R is an integral domain where every nonzero proper ideal factors into prime ideals.*

It is easy to see that, in a Dedekind domain, all nonzero prime ideals are maximal. While some of the results we will give are more general, we will work with extensions of the rational numbers $E/\mathbb{Q}$. We denote by $\mathcal{O}_E$ the ring of integers of E, i.e., the set of elements whose irreducible polynomial has integer coefficients. It is a Dedekind domain. Clearly the ring of integers of $\mathbb{Q}$ is the ring of the integer numbers $\mathbb{Z}$.

PROPOSITION 18. *Let $E/\mathbb{Q}$ be a finite Galois extension of number fields and let $\mathcal{O}_E$ be the ring of integers of E. Let p be a prime of $\mathbb{Z}$. Then the ideal $p\mathcal{O}_E$ has the following unique factorization*

$$p\mathcal{O}_E = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$$

where $\{\mathfrak{P}_i\}$ is a set of distinct prime ideals of $\mathcal{O}_E$ and e is called the ramitication index *of (p), the principal ideal generated by p. If $e = 1$ we say that the prime ideal (p) is* unramified *in E. Otherwise we say that the prime ideal (p) is* ramified *in E.*

DEFINITION 17. *Let $E/\mathbb{Q}$ be a finite Galois extension of number fields and let $\mathcal{O}_E$ be the ring of integers of E. Let p be a prime of $\mathbb{Z}$ and $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_E$.*

(1) *p is a prime* below *$\mathfrak{P}$ if $(p) = \mathfrak{P} \cap \mathbb{Z}$. If this condition holds we also say that $\mathfrak{P}$ is a prime ideal lying* over *p.*
(2) *The* decomposition group *$D_{\mathfrak{P}}$ at $\mathfrak{P}$ is defined as the following subgroup of* $\mathrm{Gal}(E/\mathbb{Q})$*:*

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(E/\mathbb{Q}) \mid {}^{\sigma}\mathfrak{P} = \mathfrak{P}\}$$

The following theorem proves the existence of the Frobenius element, which will be defined after the theorem, in the Galoius group of a finite Galois extension. Notice that the $\mathbb{Z}/(p)$ is a finite field, and the extension $(\mathcal{O}_E/\mathfrak{P})/(\mathbb{Z}/(p))$ is a finite cyclic extension of finite fields.

THEOREM 16. *Let $E/\mathbb{Q}$ be a finite Galois extension of number fields and let $\mathcal{O}_E$ be the ring of integers of E. Let $\mathfrak{P}$ be a prime ideal of E. Define p to be a prime below $\mathfrak{P}$ in $\mathbb{Z}$, $(p) = \mathfrak{P} \cap \mathbb{Z}$, and let $D_{\mathfrak{P}}$ be the decomposition group at $\mathfrak{P}$. Then the natural homomorphism*

$$\phi : D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/(\mathbb{Z}/(p)))$$

is surjective.

The order of the kernel of the surjective homomorphism ϕ is the ramification index of p. If p is unramified, the ramification index is 1, so the kernel is trivial. This implies that ϕ is injective and hence an isomorphism. That isomorphism gives the defininition of the Frobenius element.

DEFINITION 18 (Frobenius element). *Let ϕ be the homomorphism defined in the previous theorem, and assume that p is unramified. Define* $\mathrm{Frob}(\mathfrak{P}/(p)) \in D_{\mathfrak{P}}$ *as the element such that* $\phi(\mathrm{Frob}(\mathfrak{P}/(p)))$ *is the Frobenius automorphism in* $\mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/(\mathbb{Z}/(p)))$*, i.e., the generator of* $\mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/(\mathbb{Z}/(p)))$ *charaterized by*

$$\phi(\mathrm{Fr}(\mathfrak{P}/(p))(x) \equiv x^q \pmod{\mathfrak{P}}$$

for every $x \in \mathcal{O}_E$, where $q = |A/(p)|$.

Since in fact we are only interested in the conjugacy class of the Frobenius element, it is of great interest to know the cycle decomposition of the Frobenius element seen as an element of the Galois group, when viewing the Galois group as a group of permutations.

THEOREM 17 (Dedekind). *Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and let $E = \mathbb{Q}(x_1, \ldots, x_n)$ be the splitting field of f over $\mathbb{Q}$, where $x_1, \ldots, x_n$ are the roots of $f(X)$. Choose a prime $p \in \mathbb{Z}$ such that $p \nmid d$, the discriminant of f. Let $B = \mathbb{Z}[x_1, x_2, \ldots, x_n]$ and let $\mathfrak{P}$ be a prime ideal of B lying over (p), i.e., $\mathfrak{P} \cap \mathbb{Z} = (p)$. Denote $f \pmod p$ as $\overline{f}$. If $\overline{f} = \prod_{i=1}^{r} \overline{f_i}$, where $\overline{f_i} = f_i \pmod p$ are irreducible polynomials over $\mathbb{F}_p$ of degree n_i, then $\mathrm{Frob}(\mathfrak{P}/(p))$, when viewed as a permutation of roots of f, has the cycle decomposition $\delta_1 \cdots \delta_r$, each δ_i with length n_i.*

Once we have a Galois representation and we know what the Frobenius element is, we can now talk about the Artin L-functions. Consider the element $\rho(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbb{C})$ for each unramified prime p, where we have written $\mathrm{Frob}_p = \mathrm{Frob}(\mathfrak{P}/(p))$. For each of those p, let $c_p(t)$ be the characteristic polynomial of $(\rho(\mathrm{Frob_p}))$. Multiplying the inverses of $c_p(N(p)^{-s})$ for each p prime (for ramified primes the construction has to be modified using inertia subgroups, but we will not enter into those details) to obtain a complex valued function $L(\rho, s)$. It can be shown, in a way that resembles the relation between the Riemann zeta function and the infinite product running over all primes discovered by Euler, that the L-function can be written as

$$L(\rho, s) = \prod_{p \,\mathrm{prime}} \frac{1}{1 - \mathrm{Tr}(\rho(\mathrm{Frob}_p))p^{-s} + \left(\frac{D}{p}\right) p^{1-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

3.2. Modular forms. Theorems by Deligne-Serre and Weil-Langlands give a 1-1 correspondence between those L-series and modular forms of weight 1 which are eigenvectors of certain Hecke operators (in fact those modular forms span the whole vector space of modular forms of weight 1). The study of modular forms is a very relevant topic in number theory and a detailed treatment is beyond the scope of this thesis. We will limit ourselves to the basic definition.
We define the *modular group* Γ as the quotient group $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$, where $\mathrm{SL}_2(\mathbb{Z})$ is the group of squared matrices of size 2 with integer entries and determinant 1. Recall that the group

$$\mathrm{SL}_2(\mathbb{R}) = \{M \in M_2(\mathbb{R}),\, \det(M) = 1\}$$

acts in the complex upper half plane $\mathbb{H}$ by fractional linear transformations as follows: if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

then for any $z \in \mathbb{H}$ we have

$$f\left(\frac{az+b}{cz+d}\right) \in \mathbb{H}.$$

Notice that the matrix $-\mathrm{Id}$ acts trivially on $\mathbb{H}$, hence it is natural to consider the quotient group Γ.

Definition 19 (Weakly modular function). *A* weakly modular function of weight $k \in \mathbb{Z}$ *is a meromorphic function on* $\mathbb{H}$ *such that for all* $\gamma \in \Gamma$ *and* $z \in \mathbb{H}$

$$f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right), \text{ if } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Since it can be checked that the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

generate Γ, so to show that a meromorphic function f on the upper half plane is weakly modular it suffices to show that for all $z \in \mathbb{H}$ it holds

$$f(z+1) = f(z) \text{ and } f\left(-\frac{1}{z}\right) = z^k f(z).$$

Assume f is weakly modular. By the fact that f is periodic of period 1 and hence has a Fourier expansion we can express f as a function of $q = e^{2\pi i z}$, function which we will denote by $\tilde{f}$; it is meromorphic in the disc $|q| < 1$ with the origin removed. If $\tilde{f}$ extends to a meromorphic (resp. holomorphic) function at the origin, we say that f is meromorphic (resp. holomorphic) at infinity. This means that $\tilde{f}$ admits a Laurent expansion in a neightbourhood of the origin

$$\tilde{f}(q) = \sum_{n=m}^{\infty} a_n q^n$$

where $m = 0$ in the holomorphic case.

Definition 20 (Modular function). *A weakly modular function is called modular if it is meromorphic at infinity.*

Definition 21 (Modular form). *A modular function which is holomorphic everywhere, including infinity, is called a* modular form*. If such a function is zero at infinity, it is called a* cusp form*.*

Hence a modular form of weight k is given by a series

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

which converges for $|q| < 1$ (i.e. $\mathrm{Im}(z) > 0$) and verifies $f(-1/z) = z^k f(z)$. It is a cusp form if $a_0 = 0$.

Requiring modular functions to satisfy the functional equation for all matrices of the modular group Γ is a very restrictive condition. In fact, the cusp form of lowest weight according to the definitions we gave is the discriminant function

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n,$$

where $\tau(n)$ is known as the Ramanujan tau function and $q = e^{2\pi iz}$, which is a cusp form of weight 12. It has been proved that the Ramanujan tau function is multiplicative, but there are still some open questions involving the tau function, such as if $\tau(n) \neq 0$ for all $n \geq 1$ (Lehmer's conjecture). Deligne proved in 1974 Ramanujan's conjecture, which stated that $|\tau(p)| \leq 2p^{11/2}$ for all primes p.

To get cusp forms of weight 1 as the ones we will get using the Galois representation ρ, we cannot ask modular forms to fulfill the functional equation for all matrices of the modular group. Now we will consider functions that fulfill the functional equations for the matrices that belong to certain subgroups of Γ. Given an integer $N > 1$, we define the *principal congruence subgroup of level N* as

$$\Gamma(N) = \left\{ M \in \Gamma : M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

We will say that a subgroup $\gamma \subseteq \Gamma$ is a *congruence subgroup* if it exists $N > 1$ such that $\Gamma(N) \subseteq \gamma$. The smallest such N is called the *level* of γ. The following examples of congruence subgroups are of fundamental importance in the study of modular forms:

$$\Gamma_0(N) = \left\{ M \in \Gamma : M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ M \in \Gamma : M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where $*$ represents any number of $\mathbb{Z}/N\mathbb{Z}$. We can also attach a character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ to a modular form.
We define a modular form of weight k, level N, and character ε as an holomorphic function in $\mathbb{H}$ (including infinity) such that

$$f(z) = \varepsilon(d)(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right), \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Notice that the modular forms that we defined previously were modular forms of weight k, level 1 and trivial character and that since the matrix $T \in \Gamma_0(N)$ for all $N > 1$, the same Fourier expansion that we obtained in that case applies here.

3.3. Modular forms of weight one obtained from a Galois representation of $\widetilde{\mathfrak{S}_4}$. What is actually relevant for us is that a modular form is determined by its Fourier coefficients a_n. In our case, thanks to some multiplicative properties, it will be enough to determine the coefficients a_p for prime p. Those coefficients were obtained in terms of the elements γ and b_σ of the extension in our case by Bayer and Frey in [**2**] and revisited by Crespo in [**5**].

PROPOSITION 19. *Let p be a prime not dividing the discriminant of the polynomial f (the polynomial whose splitting field E is used as a base field for the quadration extension $\widetilde{E} = E(\sqrt{\gamma})$). Then the p-th coefficient to the modular form associated to the Galois representation ρ is $a_p = \mathrm{Tr}(\rho(\mathrm{Frob}_p))$.*

Let us denote by $\widetilde{\pi}_p$ and π_p the conjugation class of the Frobenius in $\widetilde{\mathfrak{S}_4}$ and $\mathfrak{S}_4$ respectively. Now, π_p is determined by the reduction modulo p of the polynomial realizing $\mathfrak{S}_4$ over $\mathbb{Q}$ and the five conjugation classes of $\mathfrak{S}_4$ lift to eight conjugation classes in $\widetilde{\mathfrak{S}_4}$. On the other hand, the character table of $\mathfrak{S}_4$ gives the value of a_p for each $\widetilde{\pi}_p$.

Decomposition Type	π_p	$\widetilde{\pi}_p$	a_p
$P_1P_1'P_1''P_1'''$	1A	1A	2
		2A	-2
P_2P_2'	2A	4A	0
$P_1P_1'P_2$	2B	2B	0
P_1P_3	3A	3A	-1
		6A	1
P_4	4A	8A	$i\sqrt{2}$
		8B	$-i\sqrt{2}$

The notation of the congruence classes is the standard one, where the number stands for the order or the elements of the congruence class in the group and the letter enumerates the congruence classes of the same order.
In the cases 2A and 2B $\widetilde{\pi}_p$ and hence a_p are determined by the decomposition of the polynomial. The following proposition gives conditions to determine the sign of a_p in the cases in which π_p lifts to two different conjugation classes.

PROPOSITION 20. *The sign of a_p when π_p is either 1A, 3A or 4A is determined as follows.*

(1) *If $\pi_1 = 1A$ (resp. 3A), we have*
   (a) *$a_p = 2$ (resp. -1) if γ is a square in the completion $E_{\mathfrak{P}}$ for $\mathfrak{P}|p$.*
   (b) *$a_p = -2$ (resp. 1), otherwise.*
(2) *If p is an odd prime and $\pi_p = 4A$, we have*
   (a) *$a_p = i\sqrt{2}$ if $\gamma^{(p-1)/2} \equiv b_\sigma \pmod{\mathfrak{P}}$ where $\mathfrak{P}|p$ and $\sigma \in S_4$ is the the transposition $(1\,2)$,*
   (b) *$a_o = -i\sqrt{2}$ otherwise.*

The property of being a square in the completion $K_{\mathfrak{P}}$ can be checked by reducing modulo the prime ideal $\mathfrak{P}$ and checking if the element γ is a square in the resulting finite field.
To obtain the values of the Fourier coefficients a_n for non-prime n, the following rules apply:

- $a_{mn} = a_m a_n$ if $(m, n) = 1$.
- $a_{p^r} = a_{p^{r-1}} a_p - \left(\frac{D}{p}\right) a_{p^{r-2}}$ for p prime, where D is the discriminant of the extension and $\left(\frac{D}{p}\right)$ is the Legendre symbol.

Those formulas are obtained by imposing that the resulting modular forms are eigenvectors of the Hecke operators.

Chapter 4
Implementation of the algorithm

The software used for all the computations of this thesis is SageMath [**9**], a mathematical software that is widely used in many areas of mathematics, and particularly useful in number theory. It allows to code in a Python-like syntax while having access to many open-source mathematical packages, such as GAP (group theory) or PARI (number theory). A good reference to learn the basic aspects of Sage is [**1**], but the documentation of the software itself contains a comprehensive list of all available classes and functions. The code that was developed in this thesis can be found in the appendix.

1. Building number fields

To begin we have to define a polynomial ring over the rational numbers (`QQ[]`). Then one can load the polynomial. Our aim is to create a number field that contains all the roots of the polynomial. The objects that are of the type Polynomial have a method called `splitting_field()`, but this method returns a `NumberField` that is expressed in terms of a primitive element (that in our case has degree 24 over $\mathbb{Q}$). To get a field in terms of the different roots of the polynomial, we build a tower of fields adding in each step a root of the polynomial. To do so, we start by creating a `NumberField` using its constructor (one has to specify the name of the generator and a polynomial, with the syntax `K.<x1> = NumberField(p)`. This creates the `NumberField` $\mathbb{Q}(x_1)$, where x_1 is a root of the polynomial p.
The next thing we have to do is to add the rest of the roots of the polynomial. We can get the polynomial $p(X)/(X - x_1)$ by creating another `PolynomialRing` over K, `R.<X> = PolynomialRing(K)`. Once we have the quotient polynomial q, we can use the `extension()` method of number fields to get the field $\mathbb{Q}(x_1, x_2)$, `K2.<x2> = K.extension(q)`. Repeating this process one can get a number field $N = \mathbb{Q}(x_1, x_2, x_3, x_4)$ where the expressions are evaluated in terms of the four roots of the polynomial.
It is important to notice that the use of the `extension()` method significantly decreases the performance of the algorithm, since doing arithmetic in towers of relative extensions is much slower than in absolute fields (using the primitive element of the extension). In the particular case where the field is an splitting field of a polynomial, a much faster implementation could be done, but using the method `extension()` we treat the different steps of the extension as if they had nothing in common.

2. Quadratic forms

Quadratic forms in Sage are implemented in the class `QuadraticForm`. The constructor of this class accepts many ways of defining a quadratic form, but the one we will use is `QuadraticForm(QQ, M)`, where `M` is the matrix of the quadratic form and `QQ` indicates that we are creating a rational quadratic form. Nevertheless, diagonal quadratic forms have their own constructor, `DiagonalQuadraticForm`, which can be created via a tuple that contains the elements of the diagonal of the quadratic form's (Gram) matrix. When dealing with their matrices, these two different ways of creating a `QuadraticForm` object can lead to a confusion. If, for instace, we create the object `DiagonalQuadraticForm(QQ, [1, 1])` and we ask for its matrix using the `matrix()` method, we obtain the matrix $\mathrm{diag}(2, 2)$. To get the identity matrix, we have to use the method `Gram_matrix()`. However, if we create the object `QuadraticForm(QQ, identity_matrix(2))`, the method `matrix()` returns the identity matrix, and the method `Gram_matrix()` returns $\mathrm{diag}(1/2, 1/2)$.
Now our aim is to determine whether two rational quadratic forms are $\mathbb{Q}$-equivalent or not. Using the Hasse-Minkowski theorem, it is enough to check if they have the same rank, the same signature, the same determinant modulo squares and the same local Witt invariants. The signature of a quadratic form can be obtained with the method `signature()`, and their determinant with the methods `det()` (for the determinant of the Hessian matrix, the one obtained with the method `matrix()`) or `Gram_det()` (for the determinant of the Gram matrix). Notice that to compare them we will have to use the method `squarefree_part()`. To check the equality of all local Witt invariants, it is enough to check if the Hasse conductors (i.e. the product of all primes where the Witt invariant is -1) is equal. The Hasse conductor is obtained with the method `hasse_conductor()`. It is worth to say that one must be really careful at this point, since mixing the two constructors `QuadraticForm` and `DiagonalQuadraticForm` could lead to an error in the computation of the Hasse-Witt invariant at $p = 2$.
Finally, if we have determined that two quadratic forms are equivalent, we need an explicit equivalence between those two quadratic forms. The method `rational_diagonal_form()` returns a diagonal form that is $\mathbb{Q}$-equivalent to the current matrix along with the transformation matrix T. Once we have a rational diagonal form, we can multiply by the squares of the denominators and take the square free part of each coefficient. Therefore we can restrict ourselves from now on to diagonal quadratic forms which have squarefree integers as coefficients. When doing those transformations, the matrix T has to be modified accordingly. All this process is done in the function `squarefree_diag` of our code, which takes a quadratic form as an input and returns a $\mathbb{Q}$-equivalent diagonal quadratic form with squarefree integers as coefficients along with the corresponding transformation matrix.
The remaining problem is to give an explicit equivalence matrix for two diagonal quadratic forms $Q_1 = \langle a_1, \ldots, a_n \rangle$ and $Q_2 = \langle b_1, \ldots, b_n \rangle$ with integer coefficients. The algorithm (implemented in the function `diag_qf_equiv`) reads as follows:

(1) Let $b = b_1$ and let $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$ be a representation of b by Q_1 (such a representation exists since we assume the two forms to be equivalent). The vector x is found using the method `solve()`. Our implementation tries to represent b using subforms to get a representation that has as many zeros as possible. To do so, we try

to represent the number using smaller subforms and, if we do not succeed, we increase the size of the subform and repeat the process.

(2) Let i be the minimum number such that $x_i \neq 0$. Let S be the identity matrix except for the i-th row, whose value is the vector x. If M is the matrix of Q_1, the matrix $S^T M S$ corresponds to a quadratic form $\hat{Q}_1$ that is equivalent to Q_1 and has b in its upper left corner.

(3) Diagonalize (using the function `squarefree_diag`) the quadratic form $\hat{Q}_1$. The resulting form is the diagonal form $\tilde{Q}_1 = \langle b, c_2, \ldots, c_n \rangle$. Let T be the transformation matrix given by `squarefree_diag`. Then $\tilde{S} = T^T S$ transforms Q_1 into $\tilde{Q}_1$.

(4) Now the forms $\tilde{Q}_1 = \langle b, c_2, \ldots, c_n \rangle$ and $Q_2 = \langle b, b_2, \ldots, b_n \rangle$ agree in their first coefficient. Then we can call recursively this same method to get an equivalence for the subforms $\langle b_2, \ldots, b_n \rangle$ and $\langle c_2, \ldots, c_n \rangle$. If the resulting matrix is P, then the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} \tilde{S}$$

gives the desired equivalence.

3. Computing γ and its irreducible polynomial

Once one has the explicit equivalence matrix and the traces matrix, computing the elements γ described by the theorems of the previous section is straightforward. The only thing that has to be taken into account is that when one uses `set_block` to set a block of a matrix, both the matrix and the submatrix need to have the same parent.
Let $\phi(X) = \mathrm{Irr}(\gamma, \mathbb{Q}; X)$ be the irreducible polynomial of γ over $\mathbb{Q}$, that can be obtained using the method `absolute_minpoly()`. The minimum polynomial for $\sqrt{\gamma}$ can be obtained easily, since it is $\phi(X^2)$. Once one creates the number field $E = \mathbb{Q}(\sqrt{\gamma})$, the method `optimized_representation()` can be used to get this extension in terms of an element that has a simpler irreducible polynomial.

We also tried to compute the coefficients of the modular form associated to the embedding problem. To do so, one can use the method `factor_mod(prime)` to get the factorization of the polynomial modulo primes. Then one can determine the possible values for a_p according to the table of the previous chapter. The two cases in which the value of a_p depends on whether the element γ is a square in the completion $E_{\mathfrak{P}}$ can be treated using the method `ideal.residue_symbol(gamma, 2)`. The cases where one needs the explicit expression for b_σ are more difficult. The program includes an expression that allows to compute b_σ from the minors of the matrix MPR extracted from the work of Crespo. We could compute directly $\gamma^{(p-1)/2}$ and b_σ reduce them modulo the prime ideal, using the method `reduce()`, or we could work in the residue field obtained with the method `residue_field`. We have not succeeded in getting to the correct results in that last case, so we do not include the results obtained for the coefficients of the modular form in the examples we will give in the following section. Nevertheless, one can find our approach in the end of the code that can be found in the appendix.

4. Examples

We present the detailed output of our algorithm, showing intermediate computations, such as the representation of elements by quadratic forms or the equivalence matrices obtained. There are five examples and in three of them the embedding problem has a solution.

```
------------------------ BEGIN EXAMPLE --------------------
Polynomial  x^4 + x^3 - 12*x^2 + 10*x - 2
Polynomial after adding one root  x^3 + (x0 + 1)*x^2 + (x0^2 + x0 - 12)*x
+ x0^3 + x0^2 - 12*x0 + 10
Polynomial after adding two roots  x^2 + (x1 + x0 + 1)*x + x1^2 + (x0 + 1)*x1
+ x0^2 + x0 - 12
Polynomial after adding three roots  x + x2 + x1 + x0 + 1
Traces matrix
[    4    -1    25   -67]
[   -1    25   -67   385]
[   25   -67   385 -1441]
[  -67   385 -1441  6781]
Discriminant  29268
--------- SOLVABILITY OF THE EMBEDDING PROBLEM
The embedding problem has a solution
Equivalence class invariants: Determinant  813 , Signature  4 , Hasse conductor  1
--------- COMPUTATION OF GAMMA (METHOD 1)
Looking for an equivalence between the diagonal forms
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 2 0 ]
[ * * * 58536 ]
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 11 0 0 ]
[ * * 2409 0 ]
[ * * * 19783 ]
Representation of  1  by the quadratic form
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 2 0 ]
[ * * * 58536 ]
is  [1, 0, 0, 0]
Representation of  11  by the quadratic form
Quadratic form in 3 variables over Rational Field with coefficients:
[ 1 0 0 ]
[ * 2 0 ]
```

```
[ * * 1626 ]
is  [3, 1, 0]
Representation of  2409  by the quadratic form
Quadratic form in 2 variables over Rational Field with coefficients:
[ 22 0 ]
[ * 1626 ]
is  [81/208, 253/208]
Equivalence matrix for METHOD 1
[         1          0          0          0]
[         0          3          1          0]
[         0    -81/104    243/208   253/1248]
[         0   6233/104 -18699/208      9/416]
The equivalence matrix is correct:  True
Gamma for METHOD 1
(23/52*x0^2 - 183/104*x0 + 77/104)*x1^2 + (23/26*x0^3 - 47/104*x0^2 - 713/104*x0
+ 317/88)*x1 + 77/104*x0^2 - 4813/3432*x0 + 5011/1716
--------- COMPUTATION OF GAMMA (METHOD 2)
Traces matrix of the cubic resolvent
[    3   -12   108]
[  -12   108 -1074]
[  108 -1074 10920]
Looking for an equivalence between the diagonal forms
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 15 0 ]
[ * * * 4065 ]
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 11 0 0 ]
[ * * 2409 0 ]
[ * * * 19783 ]
Representation of  1  by the quadratic form
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 15 0 ]
[ * * * 4065 ]
is  [1, 0, 0, 0]
Representation of  11  by the quadratic form
Quadratic form in 3 variables over Rational Field with coefficients:
[ 3 0 0 ]
[ * 15 0 ]
[ * * 4065 ]
is  [-5/9, -11/15, -1/45]
```

```
Representation of  2409  by the quadratic form
Quadratic form in 2 variables over Rational Field with coefficients:
[ 1 0 ]
[ * 8943 ]
is  [-627/16, -5/16]
Equivalence matrix for METHOD 2
[            2             0             0             0]
[         -1/2         -25/6          -7/3          -1/6]
[         25/2        307/22        153/22         25/44]
[        -67/2 -973585/14454 -508835/14454  -74699/28908]
The equivalence matrix is correct  True
Gamma for METHOD 2
-1649/1606*x0^3 - 2702/2409*x0^2 + 194831/14454*x0 - 27596/7227
Minimum polynomial of sqrt(gamma) over Q
x^8 - 12*x^6 + 198678131/5803281*x^4 - 576311091443/45753067404*x^2 +
3967186389151039/3637231599415788
Optimized representation
x^8 - 3*x^7 - 10272*x^6 + 24213*x^5 + 35258346*x^4
- 76517709*x^3 - 46666774044*x^2 + 63802319883*x + 20858753256609
Different primes between the original polynomial and the one for sqrt(gamma)  1
Different primes between the original polynomial and the one
of the extension K(sqrtgamma) 1
------------------------ END EXAMPLE ----------------------


------------------------ BEGIN EXAMPLE --------------------
Polynomial  x^4 - 6*x^2 + 2*x + 2
Polynomial after adding one root  x^3 + x0*x^2 + (x0^2 - 6)*x + x0^3 - 6*x0 + 2
Polynomial after adding two roots  x^2 + (x1 + x0)*x + x1^2 + x0*x1 + x0^2 - 6
Polynomial after adding three roots  x + x2 + x1 + x0
Traces matrix
[  4   0  12  -6]
[  0  12  -6  64]
[ 12  -6  64 -60]
[ -6  64 -60 372]
Discriminant  21200
--------- SOLVABILITY OF THE EMBEDDING PROBLEM
The embedding problem has a solution
Equivalence class invariants: Determinant  53 , Signature  4 , Hasse conductor  1
--------- COMPUTATION OF GAMMA (METHOD 1)
Looking for an equivalence between the diagonal forms
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 2 0 ]
[ * * * 42400 ]
```

```
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 1 0 ]
[ * * * 159 ]
Representation of  1  by the quadratic form
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 2 0 ]
[ * * * 42400 ]
is  [1, 0, 0, 0]
Representation of  3  by the quadratic form
Quadratic form in 3 variables over Rational Field with coefficients:
[ 1 0 0 ]
[ * 2 0 ]
[ * * 106 ]
is  [1, 1, 0]
Representation of  1  by the quadratic form
Quadratic form in 2 variables over Rational Field with coefficients:
[ 6 0 ]
[ * 106 ]
is  [5/16, 1/16]
Equivalence matrix for METHOD 1
[     1      0      0      0]
[     0      1      1      0]
[     0   -5/8   5/16  1/320]
[     0   53/8 -53/16   3/64]
The equivalence matrix is correct:  True
Gamma for METHOD 1
(3/16*x0^2 - 9/20*x0 - 27/80)*x1^2 + (3/8*x0^3 - 27/40*x0^2 - 9/8*x0 + 33/40)*x1
- 3/8*x0^3 - 9/80*x0^2 + 7/10*x0 + 159/40
--------- COMPUTATION OF GAMMA (METHOD 2)
Traces matrix of the cubic resolvent
[   3   -6   52]
[  -6   52 -204]
[  52 -204 1328]
Looking for an equivalence between the diagonal forms
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 10 0 ]
[ * * * 1590 ]
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
```

```
[ * 3 0 0 ]
[ * * 1 0 ]
[ * * * 159 ]
Representation of  1  by the quadratic form
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 10 0 ]
[ * * * 1590 ]
is  [1, 0, 0, 0]
Representation of  3  by the quadratic form
Quadratic form in 3 variables over Rational Field with coefficients:
[ 3 0 0 ]
[ * 10 0 ]
[ * * 1590 ]
is  [1, 0, 0]
Representation of  1  by the quadratic form
Quadratic form in 2 variables over Rational Field with coefficients:
[ 10 0 ]
[ * 1590 ]
is  [49/160, -1/160]
Equivalence matrix for METHOD 2
[     2      0      0      0]
[     0      2      0      0]
[     6  27/16  17/32  -3/32]
[    -3 295/48  23/32  11/32]
The equivalence matrix is correct  True
Gamma for METHOD 2
15/16*x0^3 + 9/8*x0^2 - 45/16*x0 + 33/32
Minimum polynomial of sqrt(gamma) over Q
x^8 - 12*x^6 + 11961/512*x^4 - 2835/4096*x^2 + 4293/1048576
Optimized representation
x^8 - 42*x^6 + 558*x^4 - 2700*x^2 + 4293
Different primes between the original polynomial and the one for sqrt(gamma)  1
Different primes between the original polynomial and the one
of the extension K(sqrtgamma) 1
------------------------- END EXAMPLE ----------------------


------------------------- BEGIN EXAMPLE --------------------
Polynomial  x^4 - 8*x^2 + 2*x + 10
Polynomial after adding one root  x^3 + x0*x^2 + (x0^2 - 8)*x + x0^3 - 8*x0 + 2
Polynomial after adding two roots  x^2 + (x1 + x0)*x + x1^2 + x0*x1 + x0^2 - 8
Polynomial after adding three roots  x + x2 + x1 + x0
Traces matrix
[  4   0  16  -6]
```

```
[  0  16  -6  88]
[ 16  -6  88 -80]
[ -6  88 -80 556]
Discriminant  53840
--------- SOLVABILITY OF THE EMBEDDING PROBLEM
The embedding problem has a solution
Equivalence class invariants: Determinant  3365 , Signature  4 , Hasse conductor  1
--------- COMPUTATION OF GAMMA (METHOD 1)
Looking for an equivalence between the diagonal forms
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 2 0 ]
[ * * * 107680 ]
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 87 0 ]
[ * * * 292755 ]
Representation of  1  by the quadratic form
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 2 0 ]
[ * * * 107680 ]
is  [1, 0, 0, 0]
Representation of  1  by the quadratic form
Quadratic form in 3 variables over Rational Field with coefficients:
[ 1 0 0 ]
[ * 2 0 ]
[ * * 6730 ]
is  [1, 0, 0]
Representation of  87  by the quadratic form
Quadratic form in 2 variables over Rational Field with coefficients:
[ 2 0 ]
[ * 6730 ]
is  [133/22, 1/22]
Equivalence matrix for METHOD 1
[       1        0        0        0]
[       0        1        0        0]
[       0        0   133/22     1/88]
[       0        0 -3365/22   133/88]
The equivalence matrix is correct:  True
Gamma for METHOD 1
(3/44*x0^2 - 3/11)*x1^2 + (3/22*x0^3 - 3/11*x0^2 - 6/11*x0 + 18/11)*x1
```

```
+ 1/11*x0^3 - 5/11*x0^2 - 27/22*x0 + 11/2
--------- COMPUTATION OF GAMMA (METHOD 2)
Traces matrix of the cubic resolvent
[   3   -8  144]
[  -8  144 -500]
[ 144 -500 7168]
Looking for an equivalence between the diagonal forms
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 69 0 ]
[ * * * 77395 ]
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 1 0 0 ]
[ * * 87 0 ]
[ * * * 292755 ]
Representation of  1  by the quadratic form
Quadratic form in 4 variables over Rational Field with coefficients:
[ 1 0 0 0 ]
[ * 3 0 0 ]
[ * * 69 0 ]
[ * * * 77395 ]
is  [1, 0, 0, 0]
Representation of  1  by the quadratic form
Quadratic form in 3 variables over Rational Field with coefficients:
[ 3 0 0 ]
[ * 69 0 ]
[ * * 77395 ]
is  [2/9, 1/9, 0]
Representation of  87  by the quadratic form
Quadratic form in 2 variables over Rational Field with coefficients:
[ 23 0 ]
[ * 77395 ]
is  [118/161, -5/161]
Equivalence matrix for METHOD 2
[       2        0        0        0]
[       0     16/9      1/3        0]
[       8 3064/207 -194/483    -5/14]
[      -3 -1237/69  404/161      4/7]
The equivalence matrix is correct  True
Gamma for METHOD 2
66/161*x0^3 + 83/161*x0^2 - 394/161*x0 + 250/161
Minimum polynomial of sqrt(gamma) over Q
x^8 - 12*x^6 + 1282720/25921*x^4 - 317976900/4173281*x^2 + 16733808500/671898241
```

```
Optimized representation
x^8 - 2*x^7 - 10830*x^6 + 24124*x^5 + 13861180*x^4 + 30051088*x^3 -
4848462832*x^2 - 8798856976*x + 522956254328
Different primes between the original polynomial and the one for sqrt(gamma)  1
Different primes between the original polynomial and the one
of the extension K(sqrtgamma) 1
------------------------ END EXAMPLE ----------------------

------------------------ BEGIN EXAMPLE --------------------
Polynomial  x^4 - 7*x^2 + 2*x + 1
Polynomial after adding one root  x^3 + x0*x^2 + (x0^2 - 7)*x + x0^3 - 7*x0 + 2
Polynomial after adding two roots  x^2 + (x1 + x0)*x + x1^2 + x0*x1 + x0^2 - 7
Polynomial after adding three roots  x + x2 + x1 + x0
Traces matrix
[  4   0  14  -6]
[  0  14  -6  94]
[ 14  -6  94 -70]
[ -6  94 -70 656]
Discriminant  33424
--------- SOLVABILITY OF THE EMBEDDING PROBLEM
The embedding problem has no solutions
First quadratic form : Determinant  2089 , Signature  4 , Hasse conductor  1
Second quadratic form : Determinant  2089 , Signature  4 , Hasse conductor  2
------------------------ END EXAMPLE ----------------------

------------------------ BEGIN EXAMPLE --------------------
Polynomial  x^4 - 9*x^2 + 2*x + 12
Polynomial after adding one root  x^3 + x0*x^2 + (x0^2 - 9)*x + x0^3 - 9*x0 + 2
Polynomial after adding two roots  x^2 + (x1 + x0)*x + x1^2 + x0*x1 + x0^2 - 9
Polynomial after adding three roots  x + x2 + x1 + x0
Traces matrix
[  4   0  18  -6]
[  0  18  -6 114]
[ 18  -6 114 -90]
[ -6 114 -90 822]
Discriminant  158112
--------- SOLVABILITY OF THE EMBEDDING PROBLEM
The embedding problem has no solutions
First quadratic form : Determinant  122 , Signature  4 , Hasse conductor  1
Second quadratic form : Determinant  122 , Signature  4 , Hasse conductor  2
------------------------ END EXAMPLE ----------------------
```

References

[1] G. Bard, *Sage for Undergraduates (online version)* http://www.gregorybard.com/Sage.html [last visited 19/5/16].

[2] P. Bayer and G. Frey, *Galois representations of octahedral type and* 2*-coverings of elliptic curves*, Math. Zeitschrift 207 (1991), 395-408.

[3] T. Crespo, *Explicit construction of* A_n *type fields*, J. Algebra 127 (1989), 452-461.

[4] T. Crespo, *Explicit construction of* $2\mathfrak{S}_n$ *Galois extensions*, J. Algebra 129 (1990), 312-319.

[5] T. Crespo, *Galois representations, embedding problems and modular forms*, Collect. Math. 48, 1-2 (1997), 63-68.

[6] J. Milne, Class Field Theory, v4.02 (2013). Available at http://www.jmilne.org/math/.

[7] J. Milne, Fields and Galois Theory, v4.51 (2015). Available at http://www.jmilne.org/math/.

[8] S-W. Park, *Existence of the Frobenius element and its applications*, http://math.uchicago.edu/ may/REUDOCS/Park.pdf [last visited the day 18/5/16].

[9] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 6.10)*, 2015, http://www.sagemath.org.

[10] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, Fifth printing, 1996.

[11] J-P. Serre, *L'invariant de Witt the la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984), 651-676.

Appendix A
Code developed

```
############################################### AUXILIAR FUNCTIONS ############

def squarefree_diag( QF1 ):
"""Returns a diagonal quadratic form equivalent to QF1 such that the elements in
the diagonal are squarefree integers"""

H = QF1.Gram_matrix();
dim = H.dimensions();
size = dim[0];

# Get an equivalent rational form
QF1d, T = QF1.rational_diagonal_form(return_matrix=True);
H = QF1d.Hessian_matrix();

diag_entries = [];
factor = copy(identity_matrix(QQ, size));

# clear denominators and square factors
for i in range(0, size):
new_entry = (H[i][i]*((H[i][i]).denominator()^2)).squarefree_part();
factor[i,i] = sqrt(new_entry/H[i][i]);
diag_entries = diag_entries + [new_entry];

QF1d = DiagonalQuadraticForm(QQ, diag_entries);

T = T*factor;
# print "This should be diagonal form";
# print T.transpose() * QF1.matrix() * T;

return QF1d, T;

########################
```

```
def diag_qf_equiv ( QF1, QF2, total_length ):

"""Gives an explicit equivalence between the two diagonal (equivalent) quadratic forms
QF1 and QF2
(total_length is the rank of the quadratic forms QF1 and QF2 the first time that this
method is called)."""
H1 = QF1.Gram_matrix();
dim = H1.dimensions();
size1 = dim[0];

H2 = QF2.Gram_matrix();
dim = H2.dimensions();
size2 = dim[0];

if (size1 != size2):
raise RuntimeError('QF sizes do not match');

if (size1 == 1):
# BASE CASE: size = 1. The equivalence exists iff in this step H1[0][0]== H2[0][0]
if (H1[0][0] != H2[0][0]):
raise RuntimeError('Final numbers do not match');
return identity_matrix(QQ, total_length);
else:
# Represent the first element of the second quadratic form using the first
# quadratic form.
a = H2[0][0];
r = -1;

l = H1.nrows();
i = 0; # start trying smaller subforms
while (i in range(0, l) and r == -1):
try:
subform = [];
for j in range(0, i):
subform = subform + [H1[j][j]];
tempQF = DiagonalQuadraticForm (QQ, subform);
r = tempQF.solve(a);
except ArithmeticError:
r = -1;
i = i + 1;

if (r != -1):
r = list(r);
for i in range(0, l - len(r)):
r = r + [0];
```

```
else:
r = list(QF1.solve(a));

print "Representation of ",
print a,
print " by the quadratic form "
print QF1;
print "is ",
print r;

# Create the equivalence matrix
S = matrix.identity(QQ, len(r));
first_nonzero = -1;
for i in range(0, len(r)):
if (r[i] != 0 and first_nonzero == -1):
first_nonzero = i;

# Swap rows if the first element of the representation is zero
S[first_nonzero] = S[0];
S[0] = r;

# Equivalent quadratic form
M = QF1.Gram_matrix();
QF1 = QuadraticForm(QQ, S*M*S.transpose());

# Diagonalize the resulting quadratic form
QF1, T = squarefree_diag(QF1);
M = QF1.Gram_matrix();
S = T.transpose()*S;

n = S.ncols();
Sext = identity_matrix(QQ, total_length);
Sext.set_block(total_length - n, total_length - n, S);


# Select the subform of size n - 1 x n - 1
if (M[0][0] != H2[0][0]):
raise RuntimeError('Upper diagonal numbers do not match');

diag1 = [];
diag2 = [];
for i in range(1, len(r)):
diag1 = diag1 + [M[i][i]];
diag2 = diag2 + [H2[i][i]];
```

```
    # Recursive call
Ssub = diag_qf_equiv(DiagonalQuadraticForm(QQ, diag1),
        DiagonalQuadraticForm(QQ, diag2), total_length)

# Computation of the total equivalence matrix
P = Ssub*Sext;

return P;

def o2m ( M, i1, i2, j1, j2 ):
""" Computes the order 2 minor |i1 i2; j1 j2| of
the matrix M """
return M[i1 - 1][j1 - 1]*M[i2 - 1][j2 - 1] - M[i1 - 1][j2 - 1]*M[i2 - 1][j1 - 1];


############################################### MAIN FUNCTION ############
def gamma ( p ):
print "------------------------ BEGIN EXAMPLE -------------------";
print "Polynomial ",
print p;

total_length = p.degree();

# Builds the tower of extensions to get the splitting field of the polynomial p
# in terms of its roots.
K1r.<x0> = NumberField(p);
R.<x> = PolynomialRing(K1r);
q = p/(x - x0);

print "Polynomial after adding one root ",
print q;

q = q.numerator();

K2r.<x1> = K1r.extension(q);
R.<x> = PolynomialRing(K2r);
q = q/(x - x1);
q = q.numerator();

print "Polynomial after adding two roots ",
print q;


N.<x2> = K2r.extension(q); # N is the splitting field of p.
R.<x> = PolynomialRing(N);
```

```
q = q/(x - x2);
q = q.numerator();

print "Polynomial after adding three roots ",
print q;

x3 = -q.constant_coefficient();


# FIRST METHOD
QF1 = DiagonalQuadraticForm(QQ, [1, 1, 2, 2*p.discriminant()]);
QF1qf = QuadraticForm(QQ, QF1.Gram_matrix());

Mf = matrix([[1, x0, x0^2, x0^3], [1, x1, x1^2, x1^3],
    [1, x2, x2^2, x2^3], [1, x3, x3^2, x3^3]]);
TrF = Mf.transpose() * Mf; # Traces matrix

TrF = matrix(QQ, TrF)

print "Traces matrix ";
print TrF;
print "Discriminant ",
print p.discriminant();

print "--------- SOLVABILITY OF THE EMBEDDING PROBLEM";

QF2 = QuadraticForm(QQ, TrF);

# Check if the two quadratic forms are equivalent. Fails sometimes when calculating
# Hasse-Witt symbol at p = 2.
if (QF1qf.signature() == QF2.signature() and
    QF1qf.hasse_conductor() == QF2.hasse_conductor() and
    TrF.determinant().squarefree_part() == p.discriminant().squarefree_part()):
print "The embedding problem has a solution";
print "Equivalence class invariants: Determinant ",
print TrF.determinant().squarefree_part(),
print ", Signature ",
print QF1qf.signature(),
print ", Hasse conductor ",
print QF1qf.hasse_conductor();
else:
print "The embedding problem has no solutions";
print "First quadratic form : Determinant ",
print TrF.determinant().squarefree_part(),
print ", Signature ",
```

```
print QF1qf.signature(),
print ", Hasse conductor ",
print QF1qf.hasse_conductor();
print "Second quadratic form : Determinant ",
print p.discriminant().squarefree_part(),
print ", Signature ",
print QF2.signature(),
print ", Hasse conductor ",
print QF2.hasse_conductor();


#Get the explicit equivalence matrix
QF2d, T = squarefree_diag( QF2 );

print "--------- COMPUTATION OF GAMMA (METHOD 1)";

print "Looking for an equivalence between the diagonal forms";
print QF1;
print QF2d;

P = diag_qf_equiv(QF1, QF2d, total_length);

print "Equivalence matrix for METHOD 1 ";
print P;

# Check it is indeed an equivalence matrix
P = T.transpose().inverse()*P;
print "The equivalence matrix is correct: ",
print P*QF1.Gram_matrix()*P.transpose() == QF2.matrix();

# Compute gamma using the first method
d = p.discriminant();
sqd = (x0 - x1)*(x0 - x2)*(x0 - x3)*(x1 - x2)*(x1 - x3)*(x2 - x3);
R = matrix([[1, 0, 0, 0], [0, 1, 0, 0],
    [0, 0, 1/2, 1/2], [0, 0, -sqd/(2*d), +sqd/(2*d)]]);
P = P.inverse().transpose();

MPR = Mf*P*R;
gamma = (MPR + identity_matrix(4)).determinant();

print "Gamma for METHOD 1 ";
print gamma;

# METHOD OF THE CUBIC RESOLVENT
print "--------- COMPUTATION OF GAMMA (METHOD 2)";
```

```
# cubic resolvent roots
y1 = x0*x1 + x2*x3;
y2 = x0*x2 + x1*x3;
y3 = x0*x3 + x1*x2;

#Traces matrix of the cubic resolvent
Mg = matrix([[1, y1, y1^2], [1, y2, y2^2], [1, y3, y3^2]]);
TrG = Mg.transpose() * Mg;
TrG = matrix(QQ, TrG);

print "Traces matrix of the cubic resolvent ";
print TrG;

TrGExt = identity_matrix(QQ, 4);
TrGExt.set_block(1, 1, TrG);
QFg = QuadraticForm(QQ, TrGExt);


# Get the explicit equivalence between the quadratic forms
QFgd, Tg = squarefree_diag( QFg );

print "Looking for an equivalence between the diagonal forms";
print QFgd;
print QF2d;

Pg2 = diag_qf_equiv(QFgd, QF2d, total_length);
Pg = T.transpose().inverse()*Pg2*Tg.transpose();

print "Equivalence matrix for METHOD 2";
print Pg;

# Check that the equivalence is correct
print "The equivalence matrix is correct ",
print Pg*QFg.matrix()*Pg.transpose() == QF2.matrix();


# Compute gamma
Rg = -Mg.inverse();

Rext = identity_matrix(N, 4);
Rext.set_block(1, 1, Rg);

MPRg = Mf*Pg.inverse().transpose()*Rext;
gammaCR = (MPRg + identity_matrix(4)).determinant();
```

```
print "Gamma for METHOD 2 ";
print gammaCR;


# Compute the absolute polynomial for sqrt(gamma) over QQ.
minPoly = gammaCR.absolute_minpoly();
coefs = minPoly.list()
R.<x> = QQ[];
sqMinPoly = coefs[0] + x^2*coefs[1] + x^4*coefs[2] + x^6*coefs[3] + x^8*coefs[4];

print "Minimum polynomial of sqrt(gamma) over Q ",
print sqMinPoly;

# Optimize the polynomial
E.<sqgamma> = NumberField(sqMinPoly);
Eo, fromE, toE = E.optimized_representation();
print "Optimized representation "
print Eo.polynomial();

# Compare the primes of the discriminants
print "Different primes between the original polynomial and the one for sqrt(gamma) ",
print (d/sqMinPoly.discriminant()).squarefree_part().factor();
print "Different primes between the original polynomial and the one
    of the extension K(sqrtgamma)",
print (d/Eo.discriminant()).squarefree_part().factor();

print "------------------------- END EXAMPLE ----------------------"


"""
This part of the program is intended to compute the
coefficients of the modular form, but presents some
problems in the case 4A.

print "--------- COEFFICIENTS OF THE MODULAR FORM";

# Odd primes that are less than 100.
primes = [ 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
    67, 71, 73, 79, 83, 89, 97]
coefs = [] # Coefficients of the quadratic form

# Get gamma as an element of K1r.
gamma2 = list(gammaCR)[0];
gammaBase = list(gamma2)[0];
```

```
# Compute bs.
bs = MPRg[0][2] - MPRg[0][3] - MPRg[1][2] + MPRg[1][3] - MPRg[2][0]
    + MPRg[2][1] + MPRg[3][0] - MPRg[3][1];
bs = bs - o2m(MPRg, 1, 2, 1, 3) + o2m(MPRg, 1, 2, 1, 4)
    - o2m(MPRg, 1, 2, 2, 3) + o2m(MPRg, 1, 2, 2, 4);
bs = bs + o2m(MPRg, 1, 3, 1, 2) + o2m(MPRg, 1, 3, 3, 4)
    + o2m(MPRg, 2, 3, 1, 2) - o2m(MPRg, 2, 3, 3, 4);
bs = bs/2;

# Multiply by a rational, it gives the same extension.
bs = bs*gammaCR.denominator();
gammaCR = gammaCR*gammaCR.denominator();

print gammaCR;
print bs;


# For each prime compute the corresponding coefficient.
for prime in primes:
pmod = p.factor_mod(prime);
if len(pmod) == 1: # 4A
fact = N.factor(prime);
ideal = fact[0][0];
gammaR = gammaCR^((prime - 1)/2);
if ideal.reduce(gammaR) == ideal.reduce(bs):
coefs = coefs + [2*i];
else:
coefs = coefs + [-2*i];
elif len(pmod) == 2: # 3A or 2A
if pmod[0][1] == 2 and pmod[1][1] == 2: # 2A
coefs = coefs + [0];
else: # 3A
fact = K1r.factor(prime);
ideal = fact[0][0];
try:
sign = ideal.residue_symbol(gammaBase, 2);
if sign == 1:
coefs = coefs + [-1];
else:
coefs = coefs + [1];
except ValueError:
coefs = coefs + [9999];
elif len(pmod) == 3: # 3B
coefs = coefs + [0];
```

```
else: # 1A
fact = K1r.factor(prime);
ideal = fact[0][0];
try:
sign = ideal.residue_symbol(gammaBase, 2);
if sign == 1:
coefs = coefs + [2];
else:
coefs = coefs + [-2];
except ValueError:
coefs = coefs + [3333];

print coefs;

"""
```