Teorema de Hasse-Minkowski

Jorge Bernués García

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: Fernando Montaner
5 de julio de 2016

Prólogo

La clasificación de las formas cuadráticas en los cuerpos de los complejos y los reales es algo que se estudia en el primer curso del grado en Matemáticas, en la asignatura de algebra lineal. Una cuestión que surge de modo natural es la de realizar una clasificación en otros cuerpos. Resolver dicho problema involucra el estudio de las propiedades aritméticas del cuerpo en cuestión. En este trabajo nuestro objetivo final será la clasificación de las formas cuadráticas en el cuerpo de los racionales. Que se deduce de la demostración del Teorema de Hasse-Minkowski. Para esto necesitaremos un estudio previo de las formas cuadráticas en los cuerpos finitos y en los cuerpos p-ádicos. Necesitaremos introducirnos en uno de los grandes temas de las Mátematicas, *La Teoría de Números* que comenzó a ser estudiada en profundidad por Fermat, quien escribió en el margen del libro *Aritmética* de Diofanto, la famosa cita:

"He sido el primero en descubrir un muy bonito teorema de la mayor generalidad, el siguiente: Cada número es o bien un número triangular o la suma de dos o tres números triangulares; cada número es un cuadrado o la suma de dos, tres, o cuatro cuadrados; cada número es un número pentagonal o la suma de dos, tres, cuatro, o cinco números pentagonales; y así hasta el infinito, para hexagonales, heptagonales y cualesquiera otros polígonos, el enunciado de este teorema hermoso y general debe variarse con el número de ángulos. La demostración que depende de variados y abstrusos misterios de los números no la puedo dar aquí, pues he decidido dedicar un trabajo completo y separado a este tema y con ello avanzar la aritmética en esta regiónde la investigación de manera extraordinaria más allá de sus límites antiguos y conocidos."(Fermat)

Sin embargo *La Teoría de Números* se empezó a consolidar con el estudio realizado por Gauss en su libro *Disquisitiones Arithmeticae*.

Para este trabajo nos hemos apoyado principalmente en la monografía del francés **Jean-Pierre Serre** mencionada en la bibliografía. En el se desarrolla toda la parte de la teoría de números necesaria para poder demostrar el Teorema de Hasse-Minkowski.

Comenzamos en este trabajo con una pequeña introducción recordando la deficinición de las formas cuadráticas y la clasificación en el cuerpo de los reales. En el segundo capítulo profundizamos en el estudio de las formas cuadráticas en cualquier cuerpo. Para finalizar en el último capítulo enunciaremos y demostraremos la clasificación en los cuerpo finitos, en los cuerpos $p-$ádicos y de esto deduciremos la clasificación en los números racionales.

Summary

Our aim is the Theory of quadratic forms over the rational field.
But first of all, let us give the general definition of a dorm over a field:

Definition: Let be K a field (characteristic $\neq 2$) and V his K-vectorial space . We say that the map $Q : V \longrightarrow K$ is a quadratic form if:

1. $Q(ax) = a^2 Q(x)$ for $a \in K$ and $x \in V$.
2. The map $(x,y) \mapsto Q(x+y) - Q(x) - Q(y)$ is a bilinear form.

The couple (V,Q) is a quadratic module. Let be $e_1,\ldots,e_n$ a basis of V, q is a quadratic form if and only if there exits a polynome $f(X_1,\ldots,X_n) = \sum_{i\leq j} a_{ij}X_iX_j \in K[X_1,\ldots,X_n]$ such that for each $x_1,\ldots,x_n \in K$ we have $q(x_1e_1 + \cdots + x_ne_n) = f(x_1,\ldots,x_n)$. The matrix $A = (a_{ij})$ is the matrix of the symetric bilinear form F belonging to q. F is the dot product associate to q, that is defined as follows:

$$F(x,y) = \tfrac{1}{2}[q(x+y) - q(x) - q(y)]$$

Next we review some of basic notions concerning quadratic modules.
We say that two elements of V x and y are orthogonal if the dot product is 0, i.e. $F(x,y) = 0$ from now on we are writting $(x \cdot y)$. The set of orthogonal elements to V is denoted by V^0, and is called the radical of V. If $V^0 = 0$ then we say that Q is not degenerated.
Let be an element x of (V,Q), if $Q(x) = 0$, then we define *x isotropic element.* An hyperbolic plane is a quadratic module that has a basis consisting of two isotropic elements x and y such that $(x \cdot y) \neq 0$.
If (V,Q) is not degenerated and has an isotropic element, then we have that $Q(V) = K$.
All quadratic modules have an orthogonal basis, so after a change of basis, we can write Q as $Q(x) = a_1x_1^2 + \cdots + a_nx_n$.
If we diagonalize (V,Q) so that Q has the form given above, then we writte $V \sim (a_1,\ldots,a_n)$. If there exists a second diagonalization such that $Q(x) = b_1x_1^2 + \cdots + b_nx_n$ then we write $(a_1,\ldots,a_n) \sim (b_1,\ldots,b_n)$.
The Witt's cancelation theorem asserts that if a quadratic module (V,Q) over a field K has:

$$(a_1,\ldots,a_r,b_1,\ldots,b_n) \sim (a_1,\ldots,a_r,c_1,\ldots,c_n)$$

with $a_1,\ldots,a_r \neq 0$ then:

$$(b_1,\ldots,b_n) \sim (c_1,\ldots,c_n)$$

.

After all that, we can rewritre the theory in terms of degree 2 polynomials
Let:

$$f(X) = \sum_{i=1}^{n} a_{ii}X_i^2 \; + \sum_{i<j} a_{ij}X_iX_j$$

be a quadratic form. The pair (K^n, f) is a quadratic module.
A quadratic form of two variables is called Hyperbolic if:

$$f \sim X_1X_2 \sim X_1^2 - X_2^2$$

we'll say that f represents an element a of K if there exists $x \in K^n$ such that $f(x) = a$. If f represents 0 and it is not degenerated then f represents all element in V and $f \sim f_2 \dot{+} g$ where f_2 is hyperbolic.

We now stress one of the most important results of the theory, that reads:
Let g and h be two non-degenerate quadratic forms and $f = g - h$. The followings assertions are equivalent:

1. f represents 0.
2. There exists an element $a \in K^*$ such that both g and h represent a.
3. There exists an element $a \in K^*$ such that both $g - a\mathbb{Z}^2$ and $h - a\mathbb{Z}^2$ represent 0.

Another important theorem, Witt's cancelation theorem, can be rewirtten in the following form:
Let be $f = g \dot{+} h$ and $f' = g' \dot{+} h'$ two non-degenerate quadratic forms. If $f \sim f'$ and $g \sim g'$ then $h \sim h'$.

Now we'll study the clasification the quadratic forms over finite fields (F_{p^n} with p prime).
Thanks to de Chevalley's Theorem we know that:

1. Let be f a polynomial with n variables and coefficients over $\mathbb{Z}$. If $degree(f) < 0$ and f doesn't have a constant term, then the congruence $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ has at least one not trivial solution for each p prime.
2. All quadratic form with at least 3 variables over F_{p^n} has a not trivial zero.

Chevalley's Theorem says:
Let q be a power of p and $f_i(x_1, \ldots, x_n) \in F_q[X_1, \ldots, X_n]$ be polynomials that have: $\sum degree(f_i) < n$. Let be V the set of common zeros of f_i over F_q^n, then:

$$|V| \equiv 0 \pmod{p}$$

For the clasification of the quadratic forms we need to choose an element $a \in F_{p^n}^*$ that is not a square. Any non-degenerate quadratic form with rank m over F_{p^n} is equivalent to:

$$X_1^2 + \cdots + X_{n-1}^2 + X_m^2 \quad \text{if the determinant is a square.}$$

or:

$$X_1^2 + \cdots + X_{n-1}^2 + aX_m^2 \quad \text{if the determinant is not a square.}$$

So two non-degenerate quadratic forms are equivalent if and only if they have the same **rank** and **determinant**.

Then we need to know whether the discriminant is not a square or it is a square in F_{p^n}.
But for all n this problem is the same problem as determining whether if the element is not a square or it is a square in F_p. So we introduce The **Legendre Symbol**:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a square in } F_p \\ -1 & \text{otherwise} \end{cases}$$

In short, the problem is to solve the congruence:

$$x^2 \equiv a \pmod{p}.$$

Later on we will need to solve all the congruences $x^2 \equiv a \pmod{p^n}$ for a in $\mathbb{Z}$ and any $n \geq 1$, to do that we'll introduce the $p-adic$ numbers. Because sommetimes the equation $x^2 - a = 0$ doesn't have integer solution but we have solutions (mod p^{n+1}) for all $n \geq 0$. We'll denote by $\mathbb{Q}_p$ the p-adic field. An element in $\mathbb{Q}_p$ is a sequence $(x_n)_n$ of solutios of the equation $x_n^2 - a \equiv 0 \pmod{p^{n+1}}$,
Let f be a quadratic form over $\mathbb{Q}_p$ with n variables, if:

$$f \sim a_1 X_1^2 + \cdots + a_n X_n^2$$

Then the invariants elements of the equivalence class of forms congruence are:

1. The discriminant $d(f) = a_1 \cdots a_n \quad$ (in $\mathbb{Q}_p^*/\mathbb{Q}_P^{*2}$).
2. $\varepsilon(f) = \prod_{i<j}(a_i, a_j) \quad$ (in $\{\pm 1\}$). Where (a_i, a_j) is the **Hilbert's Symbol** which is defined by:
   - $(a_i, a_j) = 1 \quad$ if $\quad z^2 - ax^2 - by^2 = 0$ has a not tirivial in $\mathbb{Q}_p^3$.
   - $(a_i, a_j) = -1 \quad$ if not.

So two quadratic forms over $\mathbb{Q}_p$ are equivalent if and only if they have the same rank, same discriminant and same invariant ε.

Now, we are able to classify the quadratic forms over the **Rational Field.**
First of all, we define the set V the union of the set of all the prime numbers and $\{\infty\}$.
Let f be a quadratic form over $\mathbb{Q}$ and f_v be the corresponding form over $\mathbb{Q}_v$ (note $\mathbb{Q} \subset \mathbb{Q}_v$) for $v \in V$.
Let's note that $Q_\infty = \mathbb{R}$.
If f is quadratic form over $\mathbb{Q}$ then we can associate the following invariants:

1. The *discriminant* $d(f) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, equal to $a_1 \cdots a_n$.
2. Let $v \in V$ and f_v be as before then we have the invariants $d_v(f)$ and $\varepsilon_v(f)$ that are the invariants of f_v.
3. The *signature (r,s)* of the real quadratic form f_∞.

The Hasse-Minkowski theorem asserts that:
f represents 0 if and only if $\forall v \in V$ the quadratic form f_v represents 0.

So the conclusion that we can obtein for the clasification is:
Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they are equivalent over $\mathbb{Q}_v$ $\forall v \in V$.

Índice general

Capítulo 1

Introducción

Nuestro objetivo es el de clasificar las formas cuadraticas en el cuerpo $\mathbb{Q}$.
Para esto necesitaremos un estudio previo de las formas cuadraticas en cuerpos finitos F_p y en los cuerpos p-ádicos $\mathbb{Q}_p$ (con p número primo).

Definición. Sea V un modulo sobre un anillo conmutativo A. Una aplicación Q:V$\longrightarrow$A se llama forma cuadrática de V si:

1. $Q(ax) = a^2Q(x)$ para $a \in A$ y $x \in V$.

2. La aplicación $(x,y) \mapsto Q(x+y) - Q(x) - Q(y)$ es una forma bilinial.

A la pareja (V,Q) se le denomina *módulo cuadrático*. Nosotros trataremos el caso particular en el que A es *un cuerpo K de característica* $\neq 2$; el A-módulo V es entonces un K-espacio vectorial que supondremos de dimensión finita.
Sea $e_1, \ldots, e_n$ una base de V, Q es una forma cudrática si y solo si existe un polinomio $f(X_1, \ldots, X_n) = \sum_{i \leq j} a_{ij} X_i X_j \in K[X_1, \ldots, X_n]$ de modo que para cada $x_1, \ldots, x_n \in K$, $Q(x_1e_1 + \cdots + x_ne_n) = f(x_1, \ldots, x_n)$
(Tomando$a_{ij} = Q(e_i, e_j)$ *si* $i < j$ *y* $a_{ii} = Q(e_i)$). La matriz A=(a_{ij}) es la matriz de la forma bliníal simétrica F correspondiente a Q. Donde F es el producto escalar asociado a Q y está definida de la siguiente manera:

$$\text{F(x,y)}=\tfrac{1}{2}[Q(x+y) - Q(x) - Q(y)].$$

Dieremos que una forma cuadrática q *representa* a $a \in K$ si existe $0 \neq v \in V$ con $q(v) = a$.

Recordaremos ahora la clasificación de las formas cuadráticas en el cuerpo $\mathbb{R}$, pero antes la terminología habitual de una forma cuadrática Q sobre el cuerpo $\mathbb{R}$ es:

- *Definida positiva* si $Q(a) > 0 \quad \forall a (\neq 0) \in \mathbb{R}$.
- *Semidefinida positiva* si $Q(a) \geq 0 \quad \forall a \in \mathbb{R}$.
- *Definida negativa* si $Q(a) < 0 \quad \forall a (\neq 0) \in \mathbb{R}$.
- *Semidefinida negativa* si $Q(a) \leq 0 \quad \forall a \in \mathbb{R}$.
- *Indefinida* si no se da ninguno de los casos, es decir si existen $a, b \in \mathbb{R}$ tales que $Q(a) < 0$ y $Q(b) > 0$.

Sea Q una forma cuadrática real, mediante un cambio de bases adecuado podemos llegar a escribirla en la forma: $Q = a_1X_1 + \cdots + a_nX_n$, se tiene entonces que Q es:

- *Definida positiva* si $a_i > 0$ para todo $i \in [1,n]$.
- *Semidefinida positiva* si $a_i \geq 0$ para todo $i \in [1,n]$.
- *Definida negativa* si $a_i < 0$ para todo $i \in [1,n]$.
- *Semidefinida negativa* si $a_i \leq 0$ para todo $i \in [1,n]$.
- *Indefinida* si existe un $a_i < 0$ y u $a_j > 0$ con $i, j \in [1,n]$.

Además como en $\mathbb{R}$ todo elemento positivo es un cuadrado, entonces los $a_i > 0$ los podremos sustituir por 1, mendiante la normalización de la base dividiendo por $\sqrt{a_i}$ el elemento i-ésimo de la base. En el caso de que a_j sea negativo podremos escribir $a_j = (-1)(-a_j)$ donde $(-a_j)$ es positivo y como hemos dicho antes podremos sustituirlo fácilmente por 1.
Por lo tanto toda forma cuadrática real podra escribirse de la forma $Q = a_1X_1 + \cdots + a_nX_n$ con $a_i \in \{-1,0,1\} \quad \forall i \in [1,n]$. El número de 1,0,-1 es único, no depende de la base que tomemos, es el invariante que caracteriza a la forma cuadrática.

En el caso que nosotros queremos estudiar (el cuerpo $\mathbb{Q}$), será más complejo. Necesitaremos la clasificación de las formas cuadráticas en los cuerpos $\mathbb{Q}_p$ y en el cuerpo $\mathbb{R} = \mathbb{Q}_\infty$ que introduciremos más tarde, ya que el teorema de **Hasse-Minkowski** nos dice que:
f una dorma cuadrática en $\mathbb{Q}$ representa a 0 si y solo si la imagen de f en el cuerpo $\mathbb{Q}_v$, (f_v), representa a 0 para toda valoracion v=v_p con p primo o $p = \infty$, correspondientes a la complecciones de $\mathbb{Q}$ en la métrica inducida por la valoración v_p.

Capítulo 2

Módulos Cuadráticos

En este cápitulos vamos a estudiar los módulos cuadráticos y veremos su traducción en las formas cuadráticas.

2.1. Otrogonalidad

Sea (V,Q) un módulo cuadrático sobre el cuerpo K. Dos elementos x,y de V se dicen ortogonales si F(x,y)=0 (a partir de ahora escribiremos simplemente (x·y) el producto escalar, en vez de F(x,y)). El conjunto de elementos ortogonales a un sub-espacio vectorial H de V se denota como H^0; que es un sub-espacio vectorial de V. Se dice que V_1 y V_2 son ortogonales si $V_1 \subset V_2^0$ i.e. para cuales quiera $x \in V_1,\ y \in V_2$ se tiene (x·y)=0.

El ortogonal V^0 de V entero se llama *radical* de V y se denota rad(V). Su dimensión se llama *rango* de Q. Si V^0=0 se dice que Q es *no degenerada*; esto equivale a que el discriminante de la matriz asociada a Q sea $\neq 0$.

Aunque este fuera de nuestro estudio, es interesante saber que si la característica de K fuera igual a 2 entonces deberiamos introducir el conjunto $radQ = \{v \in V^0 \mid Q(v) = 0\}$.

Si $CarK \neq 2$, $(rad(Q) = V^0)$, Q induce una forma cuadrática en V/V^0. Entonces $\dim(V/V^0)$ es el "número efectivo"de variables: existe una base de V en la que la forma cuadrática se representa por un polinomio en $\dim(V/V^0)$ variables.

Si $CarK = 2$, Q no induce una forma cuadrática en V/V^0. Por eso se introduce el *radical de Q*, y así Q induce $\overline{Q} : V/rad(Q) \mapsto K$ y $\dim(V/rad(Q))$ es el "número efectivo"de variables. Y la forma cuadrática Q se llamara también no degenerada si $rad(Q)$=0.

Ejemplo. Consideramos las forma cuadrática $q : K^3 \mapsto K$ dada (en la base canónica) por $f(x,y,z) = -3x^2 + 4y^2 - 2xy + 2xz + 2yz$

Si $CarK = p > 3$, la forma es no degenerada.

Si $CarK = 3$, $V^0 = K < (1,-1,-1) >$ y en la base $(1,0,0),(0,1,0),(-1,1,1)$ tiene polinomio $g(x,y) = y^2 - 2xy$.

Teorema 2.1. *Sea U un sub-espacio finito no degenerado de V y sea U^0 su complementario ortogonal. Entonces V es suma directa de U y de su complementario ortogonal U^0. ($V = U \oplus U^0$)*

Demostración. Primero haremos notar que como U es no degenerado entonces $U \cap U^0 = 0$. Por lo tanto solo nos queda demostrar que U y U^0 generan el espacio V. Sea x un elemento arbitrario de V. Tenemos que expresar x como suma de un elemento de U y otro elemento de U^0. Tomamos una base de U $(u_1,\ldots,u_n)$. Para resolver nuestro problema tenemos que buscar escalares $a_1,\ldots,a_n \in K$ y un elemento $y \in U^0$ de tal manera que:

$$x = a_1u_1 + \cdots + a_nx_n + y \tag{2.1}$$

Suponiendo que $(u_i \cdot u_j)$=c_{ij}. Utilizando la ecuacion (2.1) para el producto escalar de x con cada u_i y dado que $(y \cdot u_i)$=0 $\forall i \in 1,\ldots,n$, entonces encontramos:

$$\begin{aligned} c_{11}a_1 + c_{12}a_2 + \cdots + c_{1n}a_n &= (x,u_1) \\ c_{21}a_1 + c_{22}a_2 + \cdots + c_{2n}a_n &= (x,u_2) \\ &\vdots \\ c_{n1}a_1 + c_{n2}a_2 + \cdots + c_{nn}a_n &= (x,u_n) \end{aligned} \tag{2.2}$$

Estudiamos (2.2) como un sistema de n ecuaciones y n incognitas $a_1,\ldots,a_n$. La matriz de coeficientes (c_{ij}) es no singular ya que es la matriz del producto escalar de las base $(u_1,\ldots,u_n)$ de U y como U es no degenerado entonces la matriz tendra determinante distinto de 0. Luego el sistema (2.2) tiene una única solución.

□

Definición. Sean $U_1,\ldots,U_n$ sub-espacios vectoriales de V. Se dice que V es suma directa ortogonal de los U_i si estos son dos a dos otrogonales y si V es la suma directa de todos ellos. Entonces se escribe:

$$V \;=\; U_1 \oplus \ldots \oplus U_n$$

2.2. Vectores Isótropos

Definición. Un elemento x de un módulo cuadrático (V,Q) se dice isótropo si tenemos Q(x)=0. Un sub-espacio vectorial U de V se dice isótropo si todos sus elementos son isótropos. Tenemos evidentemente que:

$$U \text{ isótropo} \Leftrightarrow\; U \subset\; U^0 \;\Leftrightarrow Q \mid U = 0$$

Definición. Se llama plano *hiperbólico* a todo módulo cuadrático teniendo una base formada por dos elementos x, y isótropos tales que (x·y)≠0.

Podremos multiplicar por $(x \cdot y)^{-1}$ y así podremos suponer que (x·y)=1. Entonces la matriz asociada a la forma cuadrática respecto la base x, y será simplemente $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ y su discriminante es -1 (por lo tanto vemos que se trata de una forma cudrática no degenerada).

Proposición 1. *Sea x un elemento isótropo ≠0 de un módulo cudrático no degenerado (V,Q). Entonces existe un sub-espacio U de V contiene a x, que es un plano hiperbólico.*

Demostración. Ya que V es no degenerado entonces existe $z \in V$ tal que $(x \cdot y)$=1. Si tomamos el elemento $y = 2z - (z \cdot z)x$ es isótropo y además $(x \cdot y) = 2$. Entonces el sub-epacio U=$Kx + Ky$ corresponde al sub-espacio que buscabamos ya que es un plano hiperbólico. □

Corolario. *Si (V,Q) es no degenerado y contiene un elemento isótropo no nulo, tenemos que Q(V)=K.*

Demostración. Por la proposición anterior basta hacer la prueba en el caso en que V es un plano hiperbólico, con base formada por elementos isótropos x, y tales que $(x \cdot y)$=1. Si tomamos $\forall\, a \in K$ el elemento $x + \frac{a}{2}y$ entonces tenemos que Q($x + \frac{a}{2}y$)=a. De donde obtenemos el resultado buscado Q(V)=K. □

2.3. Bases ortogonales.

Definición. Una base $(e_1,\dots,e_n)$ de un módulo cuadrático (V,Q) se dice ortogonal si los elementos son dos a dos otrogonales; i.e. $V = Ke_1 \oplus \cdots \oplus Ke_n$.

Esto es lo mismo que decir que la matriz de Q respecto a dicha base es una matriz diagonal:

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}$$

Por lo tanto todo elemento de V se escribira de la forma $x = \sum x_i e_i$ y entonces tendremos:

$$Q(x) = a_1 x_1^2 + \cdots + a_n x_n^2.$$

Teorema 2.2. *Todo módulo cuadrático (V,Q) posee una base ortogonal.*

Demostración. Sea n=dim V, en el caso n=0,1 es trivial. Para n≥2, si V es isótropo entonces toda base de V es ortogonal. En caso contrario entonces existe un elemento $e_1 \in V$ tal que $(e_1 \cdot e_1) \neq 0$. Sea H el sub-espacio ortogonal, del sub-espacio Ke_1, es un hiperplano y como $e_1 \notin H$ tenemos $V = Ke_1 \oplus H$; H contiene una base $(e_2,\dots,e_n)$. Como H es no degenerado, al ser un hiperplano, podremos utilizar otra vez este procedimiento sobre su base $(e_2,\dots,e_n)$ y por recurrencia llegaremos a una base ortogonal, luego el teorema queda demostrado. □

Corolario. *Sea A una matriz simétrica con elementos en el cuerpo K. Entonces existe una matriz P no singular tal que PAP^0 es diagonal (donde P^0 es matriz ortogonal de P).*

Si diagonalizamos V con la base $(a_1,\dots,a_n)$, escribiremos V$\sim (a_1,\dots,a_n)$. Si además existe una segunda base $(b_1,\dots,b_n)$ que diagonalice V entonces escribiremos $(a_1,\dots,a_n) \sim (b_1,\dots,b_n)$.

Sean (V,Q) y (V',Q') dos módulos cuadráticos, diremos que V y V' son *equivalentes o isomorfos* V$\sim$V' si existe una transformación lineal inyectiva de V en V' que preserve los prodcutos escalares. Es decir: sean F y F' los productos escalares asociados a Q y Q' respectivamente, T la transformación lineal para que V$\sim$V' es necesario que $F'(Tx,Ty) = F(x,y)$. Diremos también que T es una isometria de V en V'.

2.4. Teorema de Cancelación de Witt

Teorema 2.3. *Sea x un elemento no isotrópico del módulo cuadrático (V,Q). Sea T la transformación lineal:*

$$Ty = -y + 2\tfrac{(x\cdot y)}{(x\cdot x)}x$$

Entonces T es una transformacion lineal ortogonal en V. Además T cumple que $Tx = x$ y $T^2 = Id_V$

Demostración. Las propiedades de T son evidentes. Dados $y,z \in V$ tenemos que demostrar que $(Ty\cdot Tz) = (y\cdot z)$. Tenemos:
$(Ty\cdot Tz) = (-y+2\frac{(x\cdot y)}{(x\cdot x)}x\cdot -z+2\frac{(x\cdot z)}{(x\cdot x)}x) = (y\cdot z) - (y\cdot 2\frac{(x\cdot z)}{(x\cdot x)}x) - (2\frac{(x\cdot y)}{(x\cdot x)}x\cdot z) + (2\frac{(x\cdot y)}{(x\cdot x)}x\cdot 2\frac{(x\cdot z)}{(x\cdot x)}x) = (y\cdot z) - 2\frac{(x\cdot z)}{(x\cdot x)}(y\cdot x) - 2\frac{(x\cdot y)}{(x\cdot x)}(x\cdot z) + 4\frac{(x\cdot z)}{(x\cdot x)}(y\cdot x)$ Como el producto escalar es simétrico entonces $(x\cdot y) = (y\cdot x)$ Entonces se anulan y tendremos el resultado buscado $(Ty\cdot Tz) = (y\cdot z)$. □

Teorema 2.4. *Sea (V,Q) un módulo cudrático. Sean y, z dos elemento de V con $(y\cdot y) = (z\cdot z) \neq 0$. Entonces existe una transformación lineal ortogonal en V que envia y a z.*

Demostración. El caso en el que $y+z$, $y-z$ son elementos nulos no se puede dar ya que si no:

$$\begin{aligned} 0 &= (y+z\cdot y+z)+(y-z\cdot y-z) \\ &= 2(y\cdot y)+2(z\cdot z) \\ &= 4(y\cdot y) \end{aligned}$$

Contradicción. Por lo que ahora supondremos que $x = y+z$ es un elemento de V no nulo. Tenemos $z = x-y$, entonces:

$$(z\cdot z) = (x\cdot x)-2(x\cdot y)+(y\cdot y)$$

Por lo tanto $(x\cdot x) = 2(x\cdot y)$. Utilizando las transformación del Teorema (2.3) encontramos que $Ty = -y+x = z$. Igualmente como $y-z$ es no nulo entonces sea T la reflexión de $y-z$ tendremos $T(-y) = -z$. Por lo que tenemos una transformación lineal que manda todo elemento de V en su negativo, por lo tanto es una transformación lineal ortogonal y además envia y a z lo que buscabamos y el teorema queda demostrado.

□

Teorema 2.5. ***Cancelación de Witt***

Sobre el cuerpo K y (V,Q) su módulo cuadrático supongamos que:

$$(a_1,\ldots,a_r,b_1,\ldots,b_n) \sim (a_1,\ldots,a_r,c_1,\ldots,c_n)$$

Con $a_1,\ldots,a_r \neq 0$ *Entonces:*

$$(b_1,\ldots,b_n) \sim (c_1,\ldots,c_n)$$

Demostración. Por iteración reducimos la prueba al caso r=1 y simplificamos la notacion remplazando a_1 por a.
Sea la primera base ortogonal de V $(u,u_1,\ldots,u_n)$ con $(u\cdot u) = a$, $(u_i\cdot u_i) = b_i$ y la segunda base ortogonal de V es $(v,v_1,\ldots,v_n)$ con $(v\cdot v) = a$, $(v_i\cdot v_i) = c_i$ Por el teorema anterior (2.4) sabemos que existe una transformación lineal ortogonal T que lleva u a v. Necesariamente T lleva el complementario ortogonal de u en el complementario ortogonal de v. Lo que quiere decir que T lleva el subespacio generado por los $u_i's$ en el espacio generado por los $v_i's$. Por lo que tenemos:

$$(b_1,\ldots,b_n) \sim (c_1,\ldots,c_n)$$

□

2.5. Traducción

Sea

$$f(X) = \sum_{i=1}^{n} a_{ii}X_i^2 \; + \sum_{i<j} a_{ij}X_iX_j$$

una forma cuadrática a n variables sobre K. Tomamos $a_{ij} = a_{ji}$ si $i > j$, de manera que la matriz $A = (a_{ij})$ es simétrica. La pareja (K^n,f) es un módulo cuadrático, que se dice *asociado* a f o a la matriz A.

Definición. Dos formas cudráticas f y f' se dicen equivalentes si los modulos correspondientes son isomorfos.

Entonces se escribe $f \sim f'$. Si A y A' son las matrices de f y f', entonces que f y f' sean equivalentes es lo mismo que decir que existe una matriz inversible X tal que $A' = XAX^t$. Sean $f(X_1, \cdots, X_n)$ y $g(X_1, \cdots, X_m)$ dos formas cuadráticas; escribiremos $f \dot{+} g$ a la forma cuadrática de $n+m$ variables:

$$f(X_1, \cdots, X_n) \dot{+} g(X_{n+1}, \cdots, X_{n+m})$$

Esta operación corresponde a la suma ortogonal. (También escribiremos $f + g$ si no hay confusión alguna). A la resta tambien la denotaremos como $f - g$ que representa a $f \dot{+} (-g)$

Definición. Una forma $f(X_1, X_2)$ de dos variables se dice hiperbólica si tenemos:

$$f \sim X_1 X_2 \sim X_1^2 - X_2^2$$

(Esto sigfinica que el módulo (K^2, f), corresponde a un plano hiperbólico.)

Proposición 2. *Si f representa 0 y es no degenerado, entonces $f \sim f_2 \dot{+} g$, donde f_2 es hiperbólica. Además f representa todo elemento de K.*

Es la traducción a la proposición (1) y su corolario.

De modo general, podremos tener un resultado identico incluso si f es degenerada:

Lema. *Sea $f : V \longmapsto K$ es una forma cuadrática. Si existe $v \in V \backslash V^0$ con $f(v) = 0$, entonces f representa a todo $a \in K$.*

Demostración. Puesto que $f(v) = 0$ y $v \notin V^0$, y existe u con$(v \cdot u) \neq 0$. Tomando $(v \cdot u)^{-1} u$ en vez de u podremos suponer que $(v \cdot u) = 1$.
Y tomando $2u - (u \cdot u)v$ en vez de u, podremos suponer que $f(u) = 0$. Entonces si $a \in K$, $f(v + \frac{a}{2}u) = a$. □

Corolario. *Sean g y h dos formas cudráticas no degeneradas de rango $\geq$ 1, y sea $f = g - h$. Las propiedades siguientes son equivalentes:*
a) f representa 0.
b) Existe un $a \in K^*$ tal que g y h lo representan.
c) Existe un $a \in K^*$ tal que $g - a\mathbb{Z}^2$ y $h - a\mathbb{Z}^2$ representen 0.

Demostración. La equivalencia b) $\Leftrightarrow$ c) resulta del lema anterior. La implicación b) $\Rightarrow$ a) es trivial. Demostremos ahora que a) $\Rightarrow$ b). Un cero no trivial de f puede escribirse de la forma (x, y), con $g(x) = h(y)$. Si el elemento $a = g(x) = h(y)$ es $\neq 0$, es claro que se verifica b). Si $a = 0$, una de las formas g por ejemplo, representa 0, por lo tanto también representa a todo elemento de K, y en particular a todo valor no nulo que toma h. □

Teorema. ***(2.2)'.*** *Sea f una forma cuadrática en n variables. Entonces existen $a_1, \cdots, a_n \in K$ tales que $f \sim a_1 X_1^2 + \cdots + a_n X_n^2$.*

El *rango* de f es el numero de indices i tales que $a_i \neq 0$. Es igual a n si y sólo si el *discriminante* $a_1 \ldots a_n$ de f es $\neq 0$ (lo que equivale a que f es no degenerada).

Y finalemente del teorema de Witt traducimos que:

Teorema 2.6. *Sea $f = g \dot{+} h$ y $f' = g' \dot{+} h'$ dos formas cudráticas no degeneradas. Si $f \sim f'$ y $g \sim g'$, entonces $h \sim h'$*

Corolario. *Si f es no degenerada tenemos:*

$$f \sim g_1 \dot{+} \cdots \dot{+} g_m \dot{+} h$$

Donde $g_1, \cdots, g_m$ son hiperbólicas y h no representa 0. Esta descomposición es única, salvo por las equivalencias.

La existencia resulta de la proposición 2 y la unicidad del Teorema (2.6).

Capítulo 3

Clasificación Formas Cuadráticas

Primero clasificaremos las formas cuadráticas en los cuerpos finitos. Estudiaremos como encontrar ceros de la forma cuadrática modulo p^n (con p primo) e intentaremos ir subiendo el exponene, introduciremos los números *p-ádicos* y haremos la clasificación en los cuerpos *p-ádicos* $\mathbb{Q}_p$. Y como consecuencia finalmente pasaremos al estudio en el cuerpo $\mathbb{Q}$.

3.1. Cuerpos Finitos F_q

Teorema 3.1. *i) La característica de un cuerpo finito K es un número primo p ≠0; si r = [K : F_p], el cardinal de K es q = p^r.*
ii) Sea p un número primo y sea q = p^r (r ≥ 1) una potencia de p. Sea Ω un cuerpo algebraico cerrado de característica p. Existe un sub-cuerpo F_q de Ω y uno solo que tenga q elementos; Es el conjunto de raices del polinomio $X^q - X$.
iii) Todo cuerpo finito de q = p^r elementos es isomorfo a F_q.

Demostración. i) Si K es finito, entonces no contiene a $\mathbb{Q}$; su característica es por lo tanto un número primo p. Si r es el grado de la extensión K/F_p, es claro que $|K| = p^r$.
ii) Si Ω es algebraicamente cerrado de característica p, tenemos que la aplicación $x \longmapsto x^q$ es un automorphismo de Ω ; ya que es la potencia *r-ésima* del automorfismo $\sigma : x \longmapsto x^p$ (notar que σ es sobreyectiva ya que Ω es algebraicamente cerrado). Los elementos $x \in \Omega$ invariantes por $x \longmapsto x^q$ forman un sub-cuerpo F_q de Ω.
Veamos ahora que este cuerpo tienes q elementos. En efecto, la derivada del polinomio $X^q - X$ es:

$$qX^{q-1} - 1 = p \cdot p^{r-1}X^{q-1} - 1 = -1$$

y no se anula. Por lo tanto (ya que Ω es algebraicamente cerrado) $X^q - X$ tiene q raices distintas. Entonces tenemos $|F_q| = q$.
Inversamente, si K es un sub-cuerpo de Ω con q elementos, el grupo multiplicativo K^* tienes q-1 elementos; Por lo tanto tenemos $x^{q-1} = 1$ si $x \in K^*$, vemos entonces que $x^q = x$ si $x \in K$ lo que demuestra que K esta contenido en F_q. Y como

$$|K| = |F_q|$$

tenemos la igualdad $K = F_q$.
iii) Resulta del apartado *ii)* y del hecho que todo cuerpo de p^r elementos puede considerarse en Ω, ya que este es algebraicamente cerrado.

□

Teorema 3.2. *El grupo multiplicativo $F_{p^n}^*$ del cuerpo finito F_{p^n} es cíclico de orden $p^n - 1$.*

Demostración. Si d es un entero ≥ 1, recordamos que escribimos $\varphi(d)$ al indicador de Euler de d, es decir el número de enteros x, $1 \leq x \leq d$, que son coprimos con d. Está claro que el número de generadores de un grupo cíclico de orden d es igual a $\varphi(d)$.

Lema. *Si n es un entero ≥ 1, entonces tenemos $n = \sum_{d|n} \varphi(d)$.*

Lema. *Sea H un grupo de orden finito n. Suponemos que, para todo divisor d de n, el conjunto de los $x \in H$ tales que $x^d = 1$ tiene a lo más d elementos. Entonces H es cíclico.*

Demostración. Sea d un divisor de n. Si existe $x \in H$ de orden d, el sub-grupo $(x) = 1, x, \ldots, x^{d-1}$ generado por x es cíclico de orden d, por la hipótesis todo elemento $y \in H$ tal que $y^d = 1$ pertenece a (x). En particular los únicos elemetnos de H de orden d son los generadores de (x), y de estoy hay $\varphi(d)$. Asi el número de elementos de H de orden d es 0 o $\varphi(d)$. Si fuese 0 por un valor de d, la formula $n = \sum_{d|n} \varphi(d)$ muestra que el número de elementos de H es < n, contradiciendo a la hipótesis del enunciado. En particular existe un elementos $x \in H$ de orden n y H coincide con el grupo cíclico (x). □

Así pues el teorema (3.2) resulta del lema precedente aplicado a $H = F_{p^n}^*$ y $n = q - 1$.

□

Lema. ***(Elevación de Soluciones)***

Sea f$\in \mathbb{Z}[X]$, $p \in \mathbb{Z}$ y $n \in \mathbb{Z}^*$. Supongamos que:

$$f(x) \equiv 0 \pmod{p^n}.$$
$$v_p(f'(x)) = k \quad con\ 0 \leq 2k < n.$$

Entonces existe $y \in \mathbb{Z}$, con $x \equiv y \pmod{p^{n-k}}$ cumpliendo $f(y) \equiv 0 \pmod{p^{n+1}}$.

Demostración. Pongamos $y = x + zp^{n-k}$ y busquemos z para que se satisfaga $f(y) \equiv 0 \ [p^{n+1}]$. Se tiene:

$$f(x + zp^{n-k}) = f(x) + f'(x)zp^{n-k} + g(x, zp^{n-k})z^2 p^{2n-2k}$$

(aplicando el desarrollo de *Taylor*, para un cierto $g \in \mathbb{Z}[X,Y]$). Sea $g(x, zp^{n-k})z^2 = h(z)$. Como $v_p(f'(x)) = k$, $f'(x) = bp^k$ para un cierto $b \in \mathbb{Z}$ con $mcd(p,b) = 1$ y como $f(x) \equiv 0 \ [p^n], f(x) = cp^n$ para un cierto $c \in \mathbb{Z}$.
Es decir, buscamos $z \in \mathbb{Z}$ con:

$$p^n c + bzp^n + h(z)p^{2n-2k} \equiv 0 \pmod{p^{n+1}}.$$

es decir,

$$c + bz + h(z)p^{n-2k} \equiv 0 \pmod{p}.$$

Pero $n > 2k \Rightarrow n - 2k \geq 1$ y basta que z cumpla

$$c + bz \equiv 0 \pmod{p}.$$

Lo que siempre es posible ya que $mcd(p,b) = 1$ y por lo tanto por la identidad de Bezout tenemos el resultado.

□

Este resultado se puede generalizar para el caso de funciones en varias variables.

Corolario. *Sea $f(X_1,\ldots,X_n)\in\mathbb{Z}[X_1,\ldots,X_n]$. Si $\overline{f}\in F_p[X_1\ldots X_n]$ tiene un cero simple en F_p^n, $(\overline{x_1},\ldots,\overline{x_n})\in F_p^n$, entonces $f(x_1,\ldots,x_n)\equiv 0 \pmod{p^m}$ tiene un cero simple $(y_1,\ldots,y_n)\in\mathbb{Z}^n$ con $\overline{y_i}=\overline{x_i}$, para cada m.*

Teorema 3.3. ***[Chevalley].***
Sea q una potencia de p primo y sea $f_i(x_1,\ldots,x_n)\in F_q[X_1,\ldots,X_n]$ polinomios cumpliendos: $\sum grad(f_i)<n$. Sea V el conjunto de ceros comunes de los f_i en F_q^n, entonces:

$$|V|\equiv 0 \pmod{p}$$

Demostración. Pongamos $P(x_1,\ldots,x_n)=\Pi(1-f_i^{q-1})$. Notando que $\forall a\in F_q^*$, $a^{q-1}=1$ se tiene:

$$P(x_1,\ldots,x_n)=0 \text{ si } (x_1,\ldots,x_n)\notin V$$
$$P(x_1,\ldots,x_n)=1 \text{ si } (x_1,\ldots,x_n)\in V$$

es decir, P es la función característica de V. Pongamos para $h\in\mathbb{Z}[X_1,\ldots,X_n]$, $S(h)=\sum_{x\in F_q^n} h(x)$. Tenemos por lo tanto:

$$|V|\equiv S(P) \pmod{p},$$

Luego basta demostrar que $S(P)=0$.
La hipótesis $\sum deg(f_i)<n$ implica:

$$deg(P)<n(q-1);$$

por lo que P es combinación lineal de los monomios.

$$X^u=X_1^{u_1}\ldots X_n^{u_n}$$

con $\sum u_i\leq grad(P)\leq\sum grad(f_i)(q-1)\leq n(q-1)$; Es sufucuiente probar que $S(X_1^{u_1}\ldots X_n^{u_n})=0$ si $\sum u_i\leq n(q-1)$. Luego basta ver que $S(X_1^{u_1}\ldots X_n^{u_n})=0$ si $u_i\leq q-1$ para algún i (su existencia es segura debido a la desigualdad anterior). Pero $S(X_1^{u_1}\ldots X_n^{u_n})=S(X^{u_1})\ldots S(X^{u_n})$. Sea $l=u_i$ tal que $l<q-1$ entonces basta probar que $S(X^l)=0$.

Si $l=0$, por convenio escribiremos $X^l=1$, luego todos los terminos de la suma $S(X^l)=\sum_{x\in F_q} x^l$ son 1 por lo tanto $S(X^l)=q\cdot 1=0$ ya que la característica de F_q es p. Si $l\neq 0$ como $l<q-1$ entonces l no es divisible por $q-1$, (haremos notar que $S(X^l)=\sum_{x\in F_q^*} x^l$ ya que el único elemento que pertenece a $F_q\backslash F_q^*$ es 0). Como F_q^* es cíclico de orden $q-1$ existe un elemento $y\in F_q^*$ tal que $y^l\neq 1$ entonces:

$$S(X^l)=\sum_{x\in F_q^*} x^l=\sum_{x\in F_q^*} y^l x^l=y^l S(X^l)$$

de donde obtenemos $(1-y^l)S(X^l)=0$, y como teníamos $y^l\neq 1$ entonces $S(X^l)=0$.

Luego obtenemos el resultado que buscabamos y entonces:

$$|V|\equiv 0 \pmod{p}.$$

Y así el teorema queda demostrado. □

Corolario. *Sea f un polinomio en n variables con coeficientes en $\mathbb{Z}$. Si grad(f) < n y f no tienes término constante, la congruencia $f(x_1,\ldots,x_n)\equiv 0 \pmod{p}$ tiene al menos una solución no trivial para cada primo p.*

Demostración. 0 es la solución no trivial y si fuese la única enotnces $|V|=1$ pero el teorema anterior nos dice que $p\mid|V|$ y como p es un número primo entonces $p\geq 2$ por lo tanto $p\nmid 1$ entonces tenemos una contradiccón. Luego 0 no es la unica solución, con lo que existe una solucón no trivial. □

Corolario. *Toda forma cuadrática de almenos 3 variables sobre F_{p^n} tiene un cero no trivial.*

Geometricamente este corolario nos dice que: toda cónica sobre un cuerpo finito tiene almenos un punto.

Notemos que el Teorema de Chevalley sólo se aplica a polinomios sin termino constante, luego a la representación del 0. El truco que utilizamos para obtener un resultado general es:

Sea $q : V \longmapsto F_{p^n}$ una forma cuadrática y sea $a \in F_{p^n}$. Definimos en $V \oplus F_{p^n}$ la forma cuadrática $q+a : V \oplus F_{p^n} \longmapsto F_{p^n}$ dada por $(q+a)(v+t) = q(v)+at^2$. Se tiene entonces:

Lema. *Sea $q : V \longmapsto F_{p^n}$ es una forma cuadrática y $a \in F_{p^n}^*$. Si q es no degenerada, $q+(-a)$ representa $0 \Leftrightarrow$ q representa a a.*

Demostración. Sea $(q+(-a))(v+t) = q(v)-at^2 = 0$. Si $t \neq 0$, $q(t^{-1}v) = a$, ya está. Si t=0, $q(v) = 0$ y puesto que q es no degenerada representa a todos los elementos de $F_{p^n}^*$.

□

Notemos que si $q : V \longmapsto F_{p^n}$ es una forma cuadrática, la forma inducida $\overline{q} : V/V^0 \longmapsto F_{p^n}$ respresenta a los mismo elementos de F_{p^n} que q y por lo tanto podemos aplicar el siguiente resultado:

Lema. *Sea $q : V \longmapsto F_{p^n}$ una forma cuadrática, $e_1, \ldots, e_n$ una base de V y $f(X_1 \ldots, X_n) \in F_{p^n}[X_1, \ldots, X_n]$ el polinomio asociado:*

- *q induce una forma cuadrátia $\overline{q} : V/V^0 \mapsto F_{p^n}$ que es no degenerada, y existe una base de V en la que el polinomio que representa a q tiene $dimV/V^0$ variables, y este número es el menor posible.*

Proposición 3. *Sea q una forma cuadrática sobre V, y F_{p^n} el cuerpo finito.*

1. *Si $dimV/V^0 \geq 2$, q representa a todo $a \in F_{p^n}^*$.*
2. *Si $dimV/V^0 \geq 3$, q representa a todo $a \in F_{p^n}$.*

Demostración. $\overline{q} : V \longmapsto F_{p^n}$ se expresa mediante un polinomio en $dimV/V^0$ variables, lo que da 2) ya que por el corolario del teorema de Chevalley tenemos que existe un cero no trivial y por lo tanto $\overline{q}$ representa a 0 luego q representa a 0 y así también representa a todo elemento de F_{p^n}.
Para obtener 1) consideramos $\overline{q}+(-a)\ \forall a \in F_{p^n}^*$ y aplicamos 2) entonces $\overline{q}+(-a)$ representa a 0 y por el lema visto anteriormente tenemos que $\overline{q}$ representa a a. Por lo tanto q representa a $a \in F_{p^n}^*$. □

Podemos ver que en realidad lo importante no es el número de variables sino el rango de q, donde $rang(q) = dimV/V^0$.

Elegimos $a \in F_{p^n}^*$ un elemento que no es un cuadrado.

Proposición 4. *Toda forma cuadrática no degnerada de rango m sobre F_{p^n} es equivalente a:*

$$X_1^2 + \cdots + X_{n-1}^2 + X_m^2$$

o bien a

$$X_1^2 + \cdots + X_{n-1}^2 + aX_m^2$$

según si su discriminante es o no un cuadrado respectivamente.

Demostración. Para m=1 es claro. Si $n \geq 2$, la proposición (3) muestra que la forma q representa 1. Entonces es equivalente a $X_1^2 \dot{+} g$, donde g es una forma de $m-1$ variables, y aplicamos la hipotesis de recurrencia a g, y el ultimo paso obtendremos X_m^2 si su discriminante es un cuadrado sino será aX_n^2 □

Corolario. *Para que dos formas cuadráticas no degenradas sobre F_{p^n} sean equivalentes, es necesario y suficiente que tengan el mismo **rango** y mismo **discriminante**.*

Ahora veremos como estudiar si un elemento $a \in F_{p^n}$ es o no un cuadrádo.

A partir de ahora q es una potencia de un numero primo $p \neq 2$. Recordemos que la característica de F_{p^n} es diferente de 2.

Teorema 3.4. *Los cuadrados de F_q^* forman un sub-grupo de índice 2 de F_q^*. Este sub-grupo es el núcleo del homomorfismo $x \longmapsto x^{(q-1)/2}$ con valores en ± 1.*

Demostración. Sea Ω una clausura algebraica de F_q; si $x \in F_q^*$ sea $y \in \Omega$ tal que $y^2 = x$. Tenemos:

$$y^{q-1} = x^{(q-1)/2} = \pm 1.$$

ya que $x^{q-1} = 1$.

Para que x sea un cuadrado en F_q, es necesario y suficiente que y pertenezca a F_q, es decir $y^{q-1} = 1$. Por lo tanto F_q^{*2} es el núcleo de $x \longmapsto x^{(q-1)/2}$. Ademas como F_q^* es cíclico de orden $q-1$, el índice de F_q^{*2} es igual a 2. □

Lema. *Si p es un número primo impar, sea d un entero tal que mcd(d,p)=1 y $r \geq 1$, d es un residuo cuadrático módulo $p^r \iff$ es un residuo cuadrático módulo p.*

Demostración. Si d es un residuo cuadráticpo módulo p^r es obvio que también lo es módulo p.
Ahora demostraremos el recíproco. Sea $f(x) = x^2 - d$, d es un residuo cuadrático mód p, existe un $a \in \mathbb{Z}$ con $a^2 \equiv d \pmod{p}$; i.e. $f(a) \equiv 0 \pmod{p}$. Claramente $mcd(p,d) = 1 \Longrightarrow p \nmid a$, luego $v_p(f'(a)) = v_p(2a) = 0$ y la solución es simple. Esto implica que existe solución mód p^r $\forall r$. □

Es lo mismo estudiar si d es un cuadrado en F_{p^r} que en F_p $\forall r \geq 2$.
Luego estudiaremos si un elemento x del grupo multiplicativo de F_p es un residuo cuadrático o no. Para ello definimos el **Símbolo de Legendre**:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si x es un residuo cuadrático mód p} \\ -1 & \text{si no} \end{cases}$$

La definición se extiende al caso $p|x$ siendo $\left(\frac{x}{p}\right) = 0$.
Es claro que $\left(\frac{x}{p}\right)$ depende sólo de la clase de x (módp). $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$ si $x' \equiv x \pmod{p}$. Si $p \nmid xy$ entonces $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
Si $x \in F_p^*$ tiene por raiz cuadrada y en una clausura algebraica de F_p. Tenemos entonces $\left(\frac{x}{p}\right) = y^{q-1}$.

Vamos a calcular el valor de $\left(\frac{x}{p}\right)$ para $x = 1, -1, 2$.
Primero definimos para un entero *n impar*, $\varepsilon(n)$ y $\omega(n)$ los elemento de F_2 por:

$$\varepsilon(n) \equiv \tfrac{n-1}{2} \pmod{2} = \begin{cases} 0 & si \quad n \equiv 1 \pmod{4} \\ 1 & si \quad n \equiv -1 \pmod{4} \end{cases}$$

$$\omega(n) \equiv \tfrac{n^2-1}{8} \pmod{2} = \begin{cases} 0 & si \quad n \equiv \pm 1 \pmod{8} \\ 1 & si \quad n \equiv \pm 5 \pmod{8} \end{cases}$$

Tenemos los siguientes resultados:

1. $\left(\frac{1}{p}\right) = 1$
2. $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$
3. $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$

Los dos primeros resultados son triviales solo para el último es necesario una demostración.

Sea α una raiz primitiva 8ª de la unidad en una clausura algebraica Ω de F_p, el elemento $y = \alpha + \alpha^{-1}$ verifica que $y^2 = 2$, ya que $\alpha^4 = -1$ de donde obtenemos $\alpha^2 + \alpha^{-2} = 0$. Tenemos:

$$y^p = \alpha^p + \alpha^{-p}.$$

Si $p \equiv \pm 1 \pmod 8$, esto conlleva que $y^p = y$ y por lo tanto $y \in F_p$ de donde $(\frac{2}{p}) = 1$.

Si $p \equiv \pm 5 \pmod 8$, tenemos que:

$$y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y$$

Por lo tanto tenemos que $y^{p-1} = -1$ entonces $y \notin F_p$ luego $(\frac{2}{p}) = -1$.
La formula queda demostrada.

Ahora estudiaremos la **Ley de Recirpocidad Cuadrática**.

Teorema 3.5. ***(Gauss)***.
Sean l y p dos primos distintos y diferentes a 2. Tenemos $(\frac{l}{p}) = (\frac{p}{l})(-1)^{\varepsilon(l)\varepsilon(p)}$.

Para la demostración necesitamremos introducir la suma de Gauss junto a ciertos lemas técnicos. Sea Ω una clausura algebraica de F_p, y sea $\omega \in \Omega$ una raiz primitiva $l-$ésima de la unidad. Si $x \in F_p$, el elemento ω^x tiene sentido, ya que $\omega^l = 1$. Por lo que podemos definir la suma de **Gauss**:

$$y = \sum_{x \in F_p} (\frac{x}{l})\omega^x.$$

Lema. *$y^2 = (-1)^{\varepsilon(l)} l$ donde, por abuso de notación, l se identifica con su imagen en F_p.*

Demostración. En efecto:

$$y^2 = \sum_{t,z} (\frac{tz}{l})\omega^{t+z} = \sum_{u \in F_p} \omega^u (\sum_{t \in F_p} (\frac{t(u-t)}{l})).$$

Si $t \neq 0$:

$(\frac{t(u-t)}{l}) = (\frac{-t^2}{l})(\frac{1-ut^{-1}}{l}) = (-1)^{\varepsilon(l)}(\frac{1-ut^{-1}}{l})$. Entonces nos queda que:

$$(-1)^{\varepsilon(l)} y^2 = \sum_{u \in F_p} C_u \omega^u.$$

Donde

$$C_u = \sum_{t \in F_l^*} (\frac{1-ut^{-1}}{l}).$$

Si $u = 0$, $C_0 = \sum_{t \in F_l^*} (\frac{1}{l}) = l - 1$; Si no $s = 1 - ut^{-1}$ describre todos los elementos de $F_l - \{1\}$, y tendremos:

$$C_u = \sum_{s \in F_l} (\frac{s}{l}) - (\frac{1}{l}) = -(\frac{1}{l}) = -1.$$

Ya que en F_l^* hay tanto elementos que son resíduos cuadráticos como elementos que no lo son. Entonces nos queda:

$$\sum_{u \in F_p} C_u \omega^u = l - 1 - \sum_{u \in F_p^*} = l$$

Y el lema queda demostrado. □

Lema. $y^{p-1} = (\frac{p}{l})$.

Demostración. Ya que Ω es de característica p, tenemos:
$y^p = \sum_{x\in F_p} (\frac{x}{l})\omega^{xp} = \sum_{z\in F_l} (\frac{zp^{-1}}{l})\omega^z = (\frac{p^{-1}}{l})y = (\frac{p}{l})y.$
De donde obtenemos el resultado $y^{p-1} = (\frac{p}{l})$. □

Así el Teorema(3.5) resulta de estos Lemas. De los dos lemas obtenemos:

$$(\frac{(-1)^{\varepsilon(l)}l}{p}) = y^{p-1} = (\frac{p}{l}).$$

Y como $(\frac{(-1)^{\varepsilon(l)}}{p}) = (\frac{(-1)}{p})^{\varepsilon(l)} = (-1)^{\varepsilon(p)\varepsilon(l)}$. Así el Temorema de **Gauss** queda demostrado.

Ejemplo. Comprobaremos si 29 es un residuo cuadrático en F_{47}:
$(\frac{29}{47}) = (-1)^{14\cdot 23}(\frac{47}{29}) = (\frac{18}{29}) = (\frac{3^2}{29})(\frac{2}{29}) = (\frac{2}{29}) = (-1)^{\omega(29)} = -1.$
Por lo tanto no lo es.

3.2. Cuerpos p-ádicos $\mathbb{Q}_p$

El problema principal en la clasificación de las formas cuadráticas en los cuerpos finitos se trata de resolver las congruencias:

$$x^2 \equiv a \pmod{p}.$$

También es natural plantearse la ecuación $x^2 = a$ en $\mathbb{Z}$ o $\mathbb{Q}$, una solución lo es, obviamente, de todas las congruencias $x^2 \equiv a \pmod{p^n}$ $\forall p$ primo y $\forall n \in \mathbb{N}$. Un problema que surge de modo natural es si el recíproco es cierto, es decir si una solución de todas las congruencias es también solución en $\mathbb{Z}$ o $\mathbb{Q}$. En general esto no es cierto y esto nos lleva a la introducción de los números *p-ádicos*. Sea x una solucion entera de la ecuación $x^2 - a = 0$. Si x_n es una solución de la ecuación anterior módulo p^{n+1}. Basta tomar $x_n \equiv x \pmod{p^{n+1}}$ eligiendo x_n entre los representantes de $F_{p^{n+1}}$, así x determina una única solucion $x_0, \dots, x_n, x_{n+1}, \dots$
Con $x_n \equiv x \pmod{p^{n+1}}$ y por lo tanto con $x_n \equiv x_{n+1} \pmod{p^{n+1}}$ Ademas la sucesión de los x_n determina a x, si $x_n \equiv y \pmod{p^{n+1}}$ $\forall n$, entonces $x \equiv y \pmod{p^{n+1}}$ $\forall n \Longrightarrow p^{n+1} \mid x - y$ $\forall n$, luego $x - y = 0$.

Si consideramos la ecuación $x^2 + 1 \equiv 0 \pmod{5^{n+1}}$ $\forall n \geq 0$, para cada n por el proceso de *elevación de soluciones* , podemos encontrar una raiz de $f(x) = x^2 + 1$ módulo 5^{n+1}; por ejemeplo:
$x_0 = 2, x_1 = 7, x_2 = 57, \dots$ y se cumple que $x_n \equiv x_{n+1} \pmod{5^{n+1}}$. El resultado es una sucesión como la introducida antes, pero está no corresponde a ningún entero ya que la ecuación $f(x) = 0$ no tiene solución.

Entonces nuestra intencion es de hacer que esa sucesión corresponda a algun elemento *"entero extendido"*, es decir queremos un anillo A con $\mathbb{Z} \subseteq A$ de modo que los elementos de A correspondan con las sucesiones del tipo anterior.

Este anillo lo denotaremos como $\mathbb{Z}_p$ *enteros p-ádicos*. Ponemos $A_n = \mathbb{Z}/p^n\mathbb{Z}$, definimos el homeomorfismo sobreyectivo, de núcleo $p^n A_{n+1}$

$$\varphi_n : A_{n+1} \longmapsto A_n$$

Entonces $\mathbb{Z}_p$ es el limite proyectivo del sistema (A_n, φ_n). [$\mathbb{Z}_p = \varprojlim(A_n, \varphi_n)$]. Daremos ahora una construcción del anillo $\mathbb{Z}_p$, sea $S \subseteq \prod_{n\geq 0} \mathbb{Z}$ el conjunto de sucesiones $(x_n)_{n\geq 0}$ con $x_n \equiv x_{n+1} \pmod{p^{n+1}}$ $\forall n$. Definimos en S la relación de equivalencia $(x_n) \sim (y_n)$ si $\forall n$ $x_n \equiv y_n \pmod{p^{n+1}}$. Sea $I = \{\xi \in S \mid \xi \sim 0\}$. Si

$\xi = (x_n) \in I$, $\zeta = (y_n) \in S$ se tiene $x_n \equiv 0 \pmod{p^{n+1}}$ $\forall n$ luego $x_n y_n \equiv 0 \pmod{p^{n+1}}$ y $\xi\zeta = (x_n y_n) \in I$ luego $I \rhd S$ es un ideal. Así S/I es un anillo y definimos $\mathbb{Z}_p := S/I$.
Definimos la aplicación $\varepsilon_n : Z_p \mapsto A_n$ la proyección asociando a un entero p-ádico x su componente x_{n-1}.

Proposición 5. *La sucesión* $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ *es exacta.*

Demostración. La multiplicación por p y entonces también por p^n es inyectiva en $\mathbb{Z}_p$; ya que sea $x = (x_n)$ un entero p-ádico tal que $px = 0$, tenemos px_{n+1}=0 para todo n, lo que conlleva que x_{n+1} es de la forma $p^n y_{n+1}$ con $y_{n+1} \in A_{n+1}$; como $x_n = \varphi(x_{n+1})$, vemos que x_n es también divisible por p^n, luego nulo.
Es claro que el núcleo de ε_n contiene a $p^n Z_p$. Reciprocamente si $x = (x_m)$ pertenece a $Ker(\varepsilon_n)$, tenemos $x_m \equiv 0 \pmod{p^n}$ para todo $m \geq n$. Lo que significa que hay un elemento y_{m-n} bien definido en A_{m-n} tal que $x_m = p^n y_{n-m}$. Los y_i definen un elemento $y \in \mathbb{Z}_p$ y por lo tanto $x = p^n y$ Luego $Ker(\varepsilon_n) = p^n\mathbb{Z}_p$ y asi obtenemos el resultado buscado para tener una sucesión exacta. □

Proposición 6. *1. Para que un elemento de $\mathbb{Z}_p$ sea inversible, es suficiente y necesario que no sea divisible por p.*

2. Si U designa el grupo multiplicativo de $\mathbb{Z}_p$, todo elemento de $\mathbb{Z}_p$ diferente de cero se escrive de forma única como producto $p^n u$, con $u \in U$ y $n \geq 0$.

Demostración. Basta probar a) para los A_n y el resultado en $\mathbb{Z}_p$ será una consecuencia. Si $x \in A_n$ no pertenece a pA_n, su imagen en A_1 no es nula, por lo tanto inversible; existen $y, z \in A_n$ tales que $xy = 1 - pz$, de donde obtenemos $xy(1 + px + \cdots + p^{n-1}z^{n-1} = 1)$ por lo tanto x es inversible.
Por otra parte, si $x \in \mathbb{Z}_p$ es no nulo, existe un maximo entero n tal que $x_n = \varepsilon_n(x)$ sea nulo. Entonces $x = p^n u$ con $p \nmid u$ luego $u \in U$. La unicidad es evidente. □

Podemos definir la siguiente aplicación.

$$v_p : \mathbb{Z}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$$

con $v_p(0) = \infty$ y $v_p(\xi) = n$ si $\xi = \omega p^n$ con $\omega \in U(\mathbb{Z}_p)$ y $n \geq 0$. Se conoce como la *Valoración p-ádica*. Se tiene:

$$v_p(\xi\zeta) = v_p(\xi) + v_p(\zeta)$$
$$v_p(\xi + \zeta) \geq min\{v_p(\xi), v_p(\zeta)\}$$

Des esto resulta que $\mathbb{Z}_p$ es un anillo integro.
Podemos definir la topología de $\mathbb{Z}_p$ dada por la métrica.

$$d(\xi, \zeta) = \lambda^{v_p(\xi - \zeta)} \text{ con } |\lambda| < 1.$$

$v_p(\xi) = \infty \Longleftrightarrow \xi = 0$. Además tenemos que $v_p(\xi) \leq v_p(\zeta) \Longleftrightarrow \xi | \zeta$ y $\alpha \in U(\mathbb{Z}_p) \Longleftrightarrow v_p(\alpha) = 0$.

Definición. Llamaremos cuerpo de los números p-ádicos a $\mathbb{Q}_p$, al cuerpo de fracciones del anillo integro $\mathbb{Z}_p$.

La aritmética de $\mathbb{Q}_p$ es muy sencilla: todo elemento $0 \neq \alpha \in \mathbb{Q}_p$ se escribe de la forma $\alpha = \omega p^k$ con únicos $\omega \in U$, $k \in \mathbb{Z}$. Por lo tanto esto permite extender v_p a $\mathbb{Q}_p$.

$$v_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

Y de nuevo tomando $0 < \lambda < 1$, se tiene una aplicación llamada *valor absoluto p-ádico*:

$$|\cdot|_p : \mathbb{Q}_p \longmapsto \mathbb{R}, \alpha \longmapsto |\alpha|_p = \lambda^{v_p(\alpha)}$$

que cumple:
$|\alpha|_p = 0 \Longleftrightarrow \alpha = 0$
$|\alpha\beta|_p = |\alpha|_p|\beta|_p$
Propiedead no arqumediana: $|\alpha+\beta|_p \leq \text{máx}\ \{|\alpha|_p, |\beta|_p\} \leq |\alpha|_p + |\beta|_p$.

Por lo tanto se puede extender la métrica de $\mathbb{Z}_p$ a $\mathbb{Q}_p$. Así $(\mathbb{Q}_p, |\cdot|_p)$ es un espacio métrico. Luego $\mathbb{Q}_p$ tiene la topología inducida por dicha métrica.

Teorema. *Si $p \neq 2$, sea $x = p^n u$ un elemento de $\mathbb{Q}_p^*$ con $n \in \mathbb{Z}$ y $u \in U$. Para que x sea un cuadrado, es suficiente y necesario que n sea par, y que la imagen de u en F_p^* sea un cuadrado.*

Teorema. *Para que un elemento $x = 2^n u$ de $\mathbb{Q}_2^*$ sea un cuadrado, es suficiente y necesario que n sea par y que $u \equiv 1$ (mód 8).*

La clasificación de las formas cuadráticas sobre $\mathbb{Q}_p$ depende de dos invariantes y del rango.
Sea (V, Q) un módulo cuadrático sobre $\mathbb{Q}_p$, el primer invariante será el discriminate, que denotaremos como $d(Q)$ un elemento de $\mathbb{Q}_p/\mathbb{Q}_p^2$. Si $e = (e_1, \ldots, e_n)$ es una base ortogonal de V, si tomamos $a_i = e_i \cdot e_i$ tendremos:

$$d(Q) = a_1 \cdots a_n$$

El siguiente invariante es:

$$\varepsilon(e) = \prod_{i<j} (a_i, a_j)$$

Donde (a_i, a_j) representa el *el símbolo de Hilbert*, el cual se define de la siguiente manera:

Definición. Sean a, b $\in \mathbb{Q}_p^*$ entonces:
(a,b)=1 si $z^2 - ax^2 - by^2 = 0$ tiene una solución no tirivial en $\mathbb{Q}_p^3$.
(a,b)=-1 si no.

Para el cálculo de este símbolo necesitaremos ver ciertas propiedades.

Proposición 7. *El símnolo de Hilbert satisface las formulas:*
i) $(a,b) = (b,a)$ *y* $(a,c^2) = 1$;
ii) $(a,-a) = 1$ *y* $(a,1-a) = 1$*;*
iii) $(a,b) = 1 \Longrightarrow (aa',b) = (a',b)$*;*
iv) $(a,b) = (a,-ab) = (a,(1-a)b)$.

Demostración. i) es evidente.
Para ii) tenemos que $b = -a$ entonces nos queda la forma cuadrática $z^2 - ax^2 + ay^2$ que tiene por cero la solución (0,1,1) y para $b = 1-a$ entonces tenemos la solución (1,1,1) y por lo tanto en ambos (a,b)=1.
En iii) necesitamos definir el cuerpo $\mathbb{Q}_p(\sqrt{b})$ que se obtiene al añadir una raiz cuadrada de b al cuerpo de inicio $\mathbb{Q}_p$ y $N\mathbb{Q}_p(\sqrt{b})^*$ el grupo de normas de elementos de $\mathbb{Q}_p(\sqrt{b})^*$. Para que (a,b) sea igual a 1 entonces es suficiente y necesario que a pertenezca a $N\mathbb{Q}_p(\sqrt{b})^*$. Luego como en la hipotesis (a,b)=1 tenemos que a pertenece a $N\mathbb{Q}_p(\sqrt{b})^*$ así que:

$$a' \in N\mathbb{Q}_p(\sqrt{b})^* \Longleftrightarrow aa' \in N\mathbb{Q}_p(\sqrt{b})^*$$

y queda demostrado.
La propiedad iv) es consecuencia de las tres anteriores. □

Teorema 3.6. *Calculo de (a,b), si ecribimos a, b en la forma $p^\alpha u$, $p^\beta v$ donde u y v pertenecen al grupo de unidades p-ádicas U. Tendremos:*

$$(a,b) = (-1)^{\alpha\beta\varepsilon(p)}(\tfrac{u}{p})^{\beta}(\tfrac{v}{p})^{\alpha}, \quad si\ p \neq 2.$$
$$(a,b) = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}, \quad si\ p = 2.$$

Para la demostración de este *Teorema* necesitaremos la ayuda de ciertas proposiciones y lemas.

Proposición 8. *Sean $f^{(i)} \in \mathbb{Z}_p[X_1,\ldots,X_m]$ polinomios homogeneos con coeficientes enteros p-ádicos. Hay una equivalencia entre:*

1. *Los $f^{(i)}$ tienen un ceo común no trivial en $(\mathbb{Q}_p)^m$.*
2. *Los $f^{(i)}$ tienen un ceo común no trivial en $(\mathbb{Z}_p)^m$.*
3. *para todo $n \geq 1$, los $f^{(i)}$ tienen un ceo común no trivial en $(A_n)^m$.*

Demostración. La implicación $b \Rightarrow a$ es trivial. Reciprocamente si $x = (x_1,\ldots,x_m)$ esun cero común no trivial de los $f^{(i)}$, tomamos:

$$h = \text{ínf}(v_p(x_1),\ldots,v_p(x_m)), \text{ y} \quad y = p^{-h}x.$$

Es claro que y es un elemento primitivo de $(\mathbb{Z}_p)^m$, y que es un cero comun de los $f^{(i)}$, por lo que ya tenemos la equivalencia. La equivalencia de $b \Leftrightarrow c$ vienen dada por que si $X = \varprojlim X_n$ y los X_n son finitos y no vacios, entonces X es no vacio, luego aplicamos esto al caso particular de $\mathbb{Z}_p$ que es el limite proyectivo de los (A_n) que son finitos y no vacios.

□

Lema. *Sea $v \in U$ una unidad p-ádica. Si la ecuación $z^2 - px^2 - vy^2 = 0$ tiene una solución no trivial en $\mathbb{Q}_p$, entonces tiene una solución (x,y,z) tal que $z,y \in U$, $x \in \mathbb{Z}_p$.*

Demostración. Por la proposición anterior la ecuación tiene una solución *primitiva* (x,y,z). Demostremos que es la solución necesaria. Sino tendriamos, $y \equiv 0 \pmod p$ o $z \equiv 0 \pmod p$, ya que $z^2 - v^2y \equiv 0 \pmod p$, y $v \not\equiv 0 \pmod p$, o tendríamos a la vez $y \equiv 0 \pmod p$, $z \equiv 0 \pmod p$, de donde obtendríamos $px^2 \equiv 0 \pmod{p^2}$, lo que conlleva $x \equiv 0 \pmod p$ lo que contradice que la solución (x,y,z) sea primitiva. □

Volviendo a la demostración del *Teorema*. Podemos ver que en realidad los exponentes α y β sólo intervienen por su residuo módulo 2; por la simetría del símbolo, tenemos tres casos a considerar:

1) $\alpha = 0, \beta = 0$. Hay que verificar que $(u,v) = 1$. Lo que es lo mismo que la ecuación $z^2 - ux^2 - vy^2 = 0$ tiene una solución no trivial módulo p, como el discriminante de la forma cuadrática es una unidad p-ádica, entonces lleva a una solución p-ádica y así $(u,v) = 1$. Esto es debido a los siguientes resultados:

Lema. *Sea $f \in \mathbb{Z}_p[X]$, y sea f' su derivada. Sea $x \in \mathbb{Z}_p$, $n,k \in \mathbb{Z}$ tales que $0 \leq 2k < n$ $f(x) \equiv 0$ (mód p^n), $v_p(f'(x)) = k$. Entonces existe $y \in \mathbb{Z}_p$ tal que :*

$$f(y) \equiv 0 \ (\text{mód } p^{n+1})$$
$$v_p(f'(y)) = k,\ y \equiv x \ (\text{mód } p^{n-k}).$$

Demostración. Tomemos y de la forma $x + p^{n-k}z$, con $z \in \mathbb{Z}_p$. Gracias a la formula de Taylor obtenemos: $f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a$, con $a \in \mathbb{Z}_p$.
Por hipótesis tenemos que $f(x) = p^n b$ y $f'(x) = p^k c$, con $b \in \mathbb{Z}_p$ y $c \in U$, por lo que podemos elegir z de manera que:

$$b + zc \equiv 0 \pmod{\text{p}}.$$

Por lo tanto tenemos ya que $f(y) \equiv 0 \pmod{p^{n+1}}$. Y la formula de Taylor aplicada a f' nos da que $f'(y) \equiv p^k c \pmod{p^{n-k}}$ y como $n-k > k$ se deduce que $v_p(f'(y)) = k$

□

Teorema 3.7. *Sean $f \in \mathbb{Z}_p[X_1,\dots,X_m]$, $x=(x_i)\in(\mathbb{Z}_p)^m$, $n,m\in\mathbb{Z}$ y j un entero comprendido entre 1 y m. Suponemos que $0\le 2k<n$ y que $f(x)\equiv 0 \pmod{p^n}$ y $v_p(\frac{\partial f}{\partial X_j}(x))=k$. Entonces existe un cero y de f en $(\mathbb{Z}_p)^m$ que es congruente a x módulo p^{n-k}*

Demostración. Supongamos primero que $m=1$. Aplicando el lema anterior a $x^{(0)}=x$, obtenemos que $x^{(1)}\in\mathbb{Z}_p$, congruente con $x^{(0)}$ módulo p^{n-k} y tal que:
$f(x^{(1)})\equiv 0 \pmod{p^{n+1}}$, $v_p(f'(x^{(1)}))=k$.
Podemos aplicar el lema a $x^{(1)}$, remplazando n por $n+1$. Paso a paso construiremos una sucesión $x^{(0)},\dots,x^{(q)},\dots$, tal que:
$x^{(q+1)}\equiv x^{(q)} \pmod{p^{n+q-k}}$, $f(x^{(q)})\equiv 0 \pmod{p^{n+q}}$.
Es una sucesión de Cauchy; si denotamos y su limite, tenemos evidentemente $f(y)=0$ y $y\equiv x \pmod{p^{n-k}}$ el resultado buscado.
El caso de $m>1$ es un corolario del caso anterior. Ya que solo se modifica x_j. Más en concreto, sea $\widetilde{f}\in\mathbb{Z}_p[X_j]$, polinomio en una variable remplazando los X_i cuando $i\neq j$ por los x_i. Entonces podemos aplicar lo que acabamos de demostrar a $\widetilde{f}$ y x_j. Deduciremos la existencia del $y_j\equiv x_j \pmod{p^{n-k}}$ tal que $f(y_j)=0$, tomando entonces $y_i=x_i$ obtendremos el elemento que buscabamos $y=(y_i)$.

□

2) $\alpha=1$, $\beta=0$. Hay que verificar que (pu,v)=$(\frac{v}{p})$. Como (u,v)=1 tenemos que $(pu,v)=(p,v)$ por lo tanto se trata de demostrar que $(p,v)=(\frac{v}{p})$. Es claro que si v es un cuadrado entonces los dos son igual a 1. Si no lo es tenemos $(\frac{v}{p})=-1$ y por lo tanto la ecuación $z^2-px^2-vy^2=0$ no tiene una solución con $z,y\in U$ y entonces no tiene un cero trivial en $\mathbb{Q}_p$, luego $(p,v)=-1$.

3) $\alpha=1$, $\beta=1$. Tenemos que demostrar:
$(pu,pv)=(-1)^{(p-1)/2}(\frac{u}{p})(\frac{v}{p})$.
Por las propiedades del símbolo de Hilbert tenemos que $(pu,pv)=(pu,-p^2uv)=(pu,-uv)$. Y por 2) tenemos que $(pu,-uv)=(\frac{-uv}{p})$.

El caso $p=2$ no lo demostraremos, es el caso más complejo.

Corolario. *El símbolo de Hilbert es una forma bilineal sobre el F_2-espacio vectorial $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$*

Veamos que es cierto que $\varepsilon(e)$ es un invariante ya que no depende de la elección de la base.

Teorema 3.8. *El número $\varepsilon(e)$ no depende de la elección de la base ortogonal e*

Demostración. Si $n=1$, tenemos $\varepsilon(e)=1$. Si $n=2$, tendremos $\varepsilon(e)=1$ si y solo si la forma $Z^2-a_1X^2-a_2Y^2$ representa 0, que dicho de otra manera es que $a_1X^2+a_2Y^2$ representa 1. Esto quiere decir que existe un elemento $x\in V$ tal que $Q(x)=1$, y esto no depende de la base e. Para $n\ge 3$, utilizaremos recurrencia sobre n. Como $n\ge 3$ podemos aplicar que si e y e' son dos bases ortogonales de V, entonces existe una sucesión de bases $e^{(0)},e^{(1)},\dots,e^{(n)}$ de bases ortogonales de V tales que $e^{(0)}=e$, $e^{(n)}=e'$ y las bases $e^{(i)},e^{(i+1)}$ son contigüas para $0\le i<n$. Por lo tanto basta probar $\varepsilon(e)=\varepsilon(e')$. Debido a la simetría del símbolo de Hilbert, $\varepsilon(e)$, no cambia por la permutación de los e_i. Por lo tanto podemos suponer $e'=(e'_1,\dots e'_n)$ tal que $e'_1=e_1$. Tomamos $a'_i=(e'_i\cdot e'_i)$, tendremos $a'_1=a_1$. Podemos escribir $\varepsilon(e)$ de la forma:

$$\varepsilon(e)=(a_1,\dots,a_n)\prod_{2\le i<j}(a_i,a_j)=(a_1,d(Q)a_1)\prod_{2\le i<j}(a_i,a_j).$$

Igualmente :

$$\varepsilon(e')=(a_1,d(Q)a_1)\prod_{2\le i<j}(a'_i,a'_j).$$

Y la hipótesis de recurrencia, aplicado al ortogonal de e_1, nos da:

$$\prod_{2\leq i<j}(a_i,a_j)=\prod_{2\leq i<j}(a'_i,a'_j)$$

Y obtenemos el resultado que buscabamos. □

Volviendo a la clasificación de las formas cuadráticas en $\mathbb{Q}_p$, recapitulando tenemos que si f es una forma cuadrática de n variables y si:

$$f\sim a_1X_1^2+\cdots+a_nX_n^2,$$

los dos elementos:

$$d(f)=a_1\cdots a_n \quad (\text{en } \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}).$$
$$\varepsilon(f)=\prod_{i<j}(a_i,a_j) \quad (\text{en } \{\pm 1\}).$$

Son los **invariantes** de la clase de equivalencia de f.
A partir de ahora denotaremos por $d=d(f)$ y $\varepsilon=\varepsilon(f)$ sus dos invariantes.
Ahora estudiaremos la representacion de un elemento de $\mathbb{Q}_v$ por una forma cuadrática.

Teorema 3.9. *Para que f represente a 0, es suficiente y necesario que se de una de las siguientes situaciones:*

1. *n=2 y* $d=-1$ *(en* $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$*).*
2. *n=3 y* $(-1,-d)=\varepsilon$.
3. *n=4 y , o* $d\neq 1$*, o d=1 y* $\varepsilon=(-1,-1)$
4. $n\geq 5$

Demostración. Escribimos f en la forma $f\sim a_1X_1^2+\cdots+a_nX_n^2$, consideraremos por separado los casos de $n=2,3,4$ y ≥ 5.

1. Para $n=2$. La forma f representa 0 si y solo si $-a_1/a_2$ es un cuadrado; pero $-a_1/a_2=-a_1a_2=-d$ en $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ por lo tanto debemos tener $-d=1$ lo que es igual a tener $d=-1$.

2. Para $n=3$. La forma f representa 0 si y solo si la forma

$$a_3f\sim -a_3a_1X_1^2-a_3a_2X_2^2-X_3^2$$

representa 0. Así la forma representa 0 si y solo si el símbolo de Hilbert $(-a_3a_1,-a_3a_2)=1$ Por ser bilineal encontramos:
$(-1,-1)(-1,a_1)(-1,a_2)(-1,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3)(a_3,a_3)=1$
y como $(a_3,a_3)=(-1,a_3)$ podemos rescribir lo anterior como:
$(-1,-1)(-1,a_1a_2a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3)=1$
Lo que es lo mismo:
$(-1,-d)\varepsilon=1$ entonces $(-1,-d)=\varepsilon$.

3. Para $n=4$. f representa 0 si y solo si existe un $x\in\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ el cual esta representado por las dos formas:
$a_1X_1^2+a_2X_2^2$ y $-a_3X_3^2-a_4X_a^2$ Por lo tanto debido a la demostración de $n=2$ obtenemos como corlario que x queda caracterizado de la siguiente manera:
$(x,-a_1a_2)=(a_1,a_2)$ y $(x,-a_3a_4)=(a_3,a_4)$.
Sea A la parte de Q_p^*/Q_p^{*2} definida por la primera condición y B la definida por la segunda. Para que f no represente 0, es suficiente y necesario que A∩B=∅. Ya que A y B son evidentemente no vacios. Esto equivale a tener las siguientes condiciones:
$a_1a_2=a_3a_4$ y $(a_1,a_2)=-(a_3,a_4)$
La primera condición significa que $d=1$. Si se cumple entonces tendremos:

$$\varepsilon = (a_1,a_2)(a_3,a_4)(a_3a_4,a_3a_4) = (a_1,a_2)(a_3,a_4)(-1,a_3a_4) = (a_1,a_2)(-a_3,-a_4)(-1,-1);$$

Por lo tanto la segunda condición es $\varepsilon = -(-1,-1)$ de donde obtenemos la demostración.

4. Para $n \geq 5$. Basta con tratar el caso en el que $n = 5$. Como habiamos dicho antes de la demostración de rango 2 obtenemos un corolario en el que si f representa a un elemento x entonces $(x,d) = \varepsilon$ y si $d = 1$ entonces existen 2^r elementos cumpliendo esto, si $d \neq 1$ existen 2^{r-1}. Por lo tanto una forma de rango 2 representa almenos 2^{r-1} elementos. Este resultado se puede deducir *a fortiori* para formas de rango ≥ 2. Como $2^{r-1} \geq 2$, f representa almenos un elemento diferente de d. Tendremos:

$$f \sim aX^2 \dot{+} g$$

Donde g es una forma de rango 4. El discriminante de g est igual a d/a. Por lo tanto es diferente de 1 y por la demostración 3) tenemos que g representa a 0. Y entonces tenemos que f representa también 0.

□

Ahora enunciaremos el corolario que hemos utilizado en la demostración del Teorema pero para todos los rangos.

Corolario. *Sea $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Para que f represente a, es suficiente y necesario que se de una de las siguientes situaciones:*

1. $n = 1$ *y* $a = d$.
2. $n = 2$ *y* $(a,d) = \varepsilon$.
3. $n = 3$ *y, o* $a \neq -d$, *o* $a = d$ *y* $(-1,-d) = \varepsilon$.
4. $n \geq 4$.

Teorema 3.10. *Dos formas cuadráticas sobre $\mathbb{Q}_p$ son equivalentes si y solo si tienen el mismo rango, mismo discriminante y mismo invariante ε.*

Demostración. Que dos formas equivalentes tengan los mismos invariantes resulta de la definición de equivalencia (Capítulo 2). El recíproco se demuestra por recurrencia sobre el rango n de dos formas f y g consideradas. El caso $n = 0$ es trivial. El corolario anterior muestra que f y g representan los mismos elementos de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Por lo que podemos encontrar un $a \in \mathbb{Q}_p^*$ que está representado por f y g a la vez, por lo tanto podemos escribir:

$$f \sim a\mathbb{Z}^2 \dot{+} f' \text{ y } g \sim a\mathbb{Z}^2 \dot{+} g'$$

donde f', g' son dos formas de rango $n-1$. Tenemos:
$d(f') = ad(f) = ad(g) = d(g')$
$\varepsilon(f') = \varepsilon(f)(a,d(f')) = \varepsilon(g)(a,d(g')) = \varepsilon(g')$
Luego f', g' tienen los mismo invariantes. Por la hipótesis de recurrencia tenemos que $f' \sim g'$ y entonces también obtenemos $f \sim g$.

□

Proposición 9. *Sea $n \geq 1$, $d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ y $\varepsilon = \pm 1$. Para que exista una forma cuadrática f de rango n tal que $d(f) = d$ y $\varepsilon(f) = \varepsilon$, es suficiente y necesario que tengamos:*
$n = 1$, $\varepsilon = 1$; o $n = 2$, $d \neq -1$; o $n = 2$, $\varepsilon = 1$; o $n \geq 3$.

Demostración. El caso $n = 1$ es trivial. Si $n = 2$ tenemos $f \sim aX^2 + bY^2$ y si $d(f) = -1$, $\varepsilon(f)(a,b) = (a,-ab) = 1$. así que no podemos tener simultaneamente $d(f) = -1$ y $\varepsilon(f) = -1$. Inversamente si $d = -1$, $\varepsilon = 1$ tomamos $f = X^2 - Y^2$, si $d \neq -1$ entonces existe $a \in \mathbb{Q}_p^*$ tal que $(a,-d) = \varepsilon$ y tomamos $f = aX^2 + adY^2$. Si $n = 3$, elegimos $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ distinto de $-d$, por lo que acabamos de ver existe una forma g de rango 2 tal que $d(g) = ad$, $\varepsilon(g) = \varepsilon(a,-d)$ y entonces la forma $a\mathbb{Z}^2 \dot{+} g$ es la qu cumple el enunciado. El caso $n \geq 4$ se deduce del caso anteior tomando la forma f como:
$g(X_1,X_2,X_3) + X_4^2 + \cdots + X_n^2$
donde g tiene los invarientes requeridos. □

Corolario. *El número de clases de formas cuadráticas de rango n sobre $\mathbb{Q}_p$, es igual a 4 si n=1, a 7 si n=2 y a 8 si $n \geq 3$.*

3.3. Cuerpo de los Racionales $\mathbb{Q}$

Denotaremos V la unión del conjunto de números primos y del símbolo $\{\infty\}$. Sea $f \sim a_1X_1^2 + \cdots + a_nX_n^2$ una forma cuadrática sobre $\mathbb{Q}$ de rango n. Sea $v \in V$ podremos considerar gracias a la inyección $\mathbb{Q} \mapsto \mathbb{Q}_v$ la forma cuadrática f_v. A la forma cuadrática f le asociaremos los siguiente invariantes:

1. El discriminante $d(f) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, que será igual a $a_1 \cdots a_n$.
2. Los invariantes de la imagen de f sobre $\mathbb{Q}_v$ f_v que denominamos $d_v(f)$ y $\varepsilon_v(f)$. Es claro que $d_v(f)$ es la imagen de $d(f)$ por $\mathbb{Q}^*/\mathbb{Q}^{*2} \mapsto \mathbb{Q}_v/\mathbb{Q}_v^{*2}$ y $\varepsilon_v(f) = \prod_{i<j}(a_i,a_j)_v$ donde $(a_i,a_j)_v$ representa el símbolo de Hilbert de las imagnenes de a_i, a_j en $\mathbb{Q}_v$.
3. La *signatura* (r,s) de la forma real f_∞.

Los invariantes $d_v(f)$, $\varepsilon_v(f)$ y (r,s) son llamados los invariantes *locales* de f.
Un resultado interesante es la formula del producto que nos da el Teorema de Hilbert.

Teorema 3.11. ***(Hilbert)***. *Si a, $b \in \mathbb{Q}^*$, tenemos $(a,b)_v = 1$ para casi todo $v \in V$, y :*

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

Demostración. Como el símbolo de Hilbert es bilineal, entonces nos basta con demostrar el teorema en los caso en los que a y b son -1 o son un número primo. Lo que tendremos que hacer en cada caso es calcular $(a,b)_v$.

1. $a = -1$, $b = -1$ Entonces tendremos:
   $(-1,-1)_\infty = (-1,-1)_2 = -1$ y $(-1,-1)_v = 1$ con $v \neq 2$. Por lo tanto el producto para todo $v \in V$ es 1.
2. $a = -1$, $b = l$ con l un primo. Si $l = 2$ entonces $(-1,2)_v = 1$ $\forall v \in V$.
   Si $l \neq 2$ tendremos:
   $(-1,l)_v = 1$ si $v \neq 2,l$
   $(-1,l)_2 = (-1,l)_l = (-1)^{\varepsilon(l)}$.
   Por lo tanto el producto es siempre igual a 1.
3. $a = l$, $a = p$ con l, p números primos. Si $l = p$ tendremos $(l,l)_v = (-1.l)_v$, para todo $v \in V$, lo que nos lleva al caso 2).
   Ahora si $l \neq p$. Si $p = 2$ tendremos $(l,2)_v = 1$ para todo $v \neq 2,l$, $(-1,2)_2 = (l,2)_l = (\frac{2}{l}) = (-1)^{\omega(l)}$. Si los dos son diferentes a 2 entonces $(l,p)_v = 1$ para todo $v \neq 2,l,p$ y $(l,p)_2 = (-1)^{\varepsilon(l)\varepsilon(p)}$ $(l,p)_l = (\frac{p}{l})$ y $(l,p)_p = (\frac{l}{p})$. Además gracias a la ley de reciprocidad cuadrática tenemos $(\frac{p}{l})(\frac{l}{p}) = (-1)^{\varepsilon(l)\varepsilon(p)}$ Luego tenemos que el producto es igual a 1 para todo $v \in V$.

□

Por lo tanto tendremos: $\prod_{v\in V}\varepsilon_v(f)=1$.

Teorema 3.12. ***(Hasse-Minkowski)*** *Para que f represente 0, es suficiente y necesario, que para todo $v\in V$ la forma f_v represente 0.*

Demostración. La necesidad es trivial. Pero tendremos que demostrar que si es suficiente también vale. Escribimos f bajo la forma:

$$f=a_1X_1^2+\cdots+a_nX_n^2,\quad a_i\in\mathbb{Q}^*.$$

Si remplazamos f por a_1f podemos suponer que $a_1=1$. Estudiaremos los distintos caso $n=2,3,4,\geq 5$.

1. Caso $n=2$:
   Tenemos $f=X_1^2-aX_2^2$. Como f_∞ representa 0 entonces $a>0$. Si escribimos a bajo la forma:

   $$a=\sum_p p^{v_p(a)}$$

   El hecho de que f_p represente 0 implica que a es un cuadrado en $\mathbb{Q}_p$ por lo tanto $v_p(a)$ es par. Entonces a es un cuadrado en $\mathbb{Q}$ luego f representa 0.

2. Caso $n=3$:
   Tenemos $f=X_1^2-aX_2^2-bX_3^2$. Si multiplicamos a,b por cuadrados, podremos suponer que a,b son enteros sin factores cuadrados (i.e $v_p(a),v_p(b)$ son iguales a 0 o a 1 para todo primo p). Podemos suponer también que $|a|\leq|b|$. Razonamos por recurrencia sobre el valor $m=|a|+|b|$. Si $m=2$, tendremos:

   $$f=X_1^2\pm X_2^2\pm X_3^2$$

   El caso $X_1^2+X_2^2+X_3^2$ queda excluido ya que f_∞ representa a 0. En los otros caso es claro que f representa a 0.
   Supongamos ahora que $m>2$, por lo tanto $|b|\geq 2$ y escribimos b como $b=\pm p_1,\ldots,p_k$. donde los p_i son primos distintos. Sea p un de los p_i, veremos que a es un cuadrado módulo p. Es evidente si $a\equiv 0 \pmod p$. Si no a es una unidad p-ádica. Por hipótesis, existe $(x,y,z)\in(\mathbb{Q}_p)^3$ tal que:

   $$z^2-ax^2-by^2=0$$

   y podemos suponer que (x,y,z) es solucion primitiva. Tenemos $z^2-ax^2=0 \pmod p$. De donde podemos concluir que si $x\equiv 0 \pmod p$ entonces z y by^2 son divisibles por p^2, como $v_p(b)=1$ tendremos $y\equiv 0 \pmod p$ que contradice el hecho de que (x,y,z) es una solución primitiva. Por lo que tenemos $x\not\equiv 0 \pmod p$, lo que demuestra que a es un cuadrado módulo p. Como tenemos $\mathbb{Z}/b\mathbb{Z}=\prod\mathbb{Z}/p_i\mathbb{Z}$, tendremos también que a es un cuadrado módulo b. Por lo que existen enteros t,b' tales que:

   $$t^2=a+b'b$$

   y podemos elegir t de manera que $|t|\leq|b|/2$. La formula $b'b=t^2-a$ demuestra que $b'b$ es una norma de la extension $k(\sqrt{a})/k$, (donde $k=\mathbb{Q}$ o $k=\mathbb{Q}_v$). Entonces conluimos que f representa a 0 en k si y solo si $f'=X_1^2-aX_2^2-b'X_3^2$ también. En particular, f' representa 0 en cada uno de los $\mathbb{Q}_v$, pero tenemos:
   $|b'|=|\frac{t^2-a}{b}|\leq\frac{|b|}{4}+1<|b|$ ya que $|b|\geq 2$.
   Escribimos b' de la forma $b''u^2$ con b'',u enteros y b'' sin factores cuadrados; tenemos *a fortriori* $|b''|<|b|$. La hipótesis de recurrencia se aplica entonces a la forma: $f''=X_1^2-aX_2^2-b''X_3^2$ que es equivalente a f'. Vemos claramente por la recurrencia que f'' representa a 0 ya que $|b''|<|b|$ y por lo tanto tambien f' y como consecuencia final f también representa a 0.

3. Caso $n = 4$
   $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$.
   Sea $v \in V$, f_v representa a 0, entonces tenemos que existe un elemento $x_v \in \mathbb{Q}_v^*$ que está representado a la vez por las formas $aX_1^2 + bX_2^2$ y por $cX_3^2 + dX_4^2$, lo que es lo mismo que decir que:

   $$(x_v, -ab)_v = (a,b) \quad \text{y} \quad (x_v, -cd)_v = (c,d)_v.$$

   Como $\prod_{v\in V}(a,b)_v = \prod_{v\in V}(c,d)_v = 1$, entonces existe un elemento $x \in \mathbb{Q}^*$ tal que:

   $$(x, -ab)_v = (a,b) \quad \text{y} \quad (x, -cd)_v = (c,d)_v \quad \forall v \in V.$$

   Por lo tanto la forma $aX_1^2 + bX_2^2 - x\mathbb{Z}^2$ representa 0 en cada uno de los Q_v, por lo tanto en $\mathbb{Q}$ por lo que hemos visto para $n = 3$. Entonces x esta representado en $\mathbb{Q}$ por la forma $aX_1^2 + bX_2^2$ y usando el mismo argumento encontraremos que también esta representado por la forma $cX_3^2 + dX_4^2$ y finalmente vemos que f representa 0.

4. Caso $n \geq 5$:
   Razonaremos por recurrencia sobre n. Escribiremos f de la forma: $f = h - g$ con $h = a_1X_1^2 + a_2X_2^2$, $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$ Sea S un subconjunto de V formado por ∞, 2 y de números primos p tales que $v_p(a_i) \neq 0$, para un $i \geq 3$ (es un conjunto finito). Sea $v \in S$, ya que f_v representa 0, existe un $a_v \in \mathbb{Q}_v^*$ que esta representado a la vez por h y g en $\mathbb{Q}_v$. Por lo tanto existe $x_i^v \in \mathbb{Q}_v$, $i = 1, \ldots, n$ tal que :

   $$h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v)$$

   Recordamos que $\mathbb{Q}_v$ es un espacio métrico cuya métrica induce la topología. El conjunto de cuadrados de $\mathbb{Q}_v^*$ es abierto. Y ya que la imagen de $\mathbb{Q}$ en $\prod_{v\in S}\mathbb{Q}_v$ es denso en dicho producto tenemos la existencia de $x_1, x_2 \in \mathbb{Q}$ tales que, si $a = h(x_1, x_2)$. Tendremos $a/a_v \in \mathbb{Q}_v^{*2}$ para todo $v \in S$. Consideramos ahora la forma: $f_1 = a\mathbb{Z}^2 - g$. Si $v \in S$, g representa a_v en $\mathbb{Q}_v$, entonces también a ya que $a/a_v \in \mathbb{Q}_v^{*2}$. Por lo tanto f_1 representa 0 en $\mathbb{Q}_v$. Si $v \notin S$, los coeficientes $-a_3, \ldots, -a_n$ de g son unidades v-ádicas, luego $d_v(g)$ también, y ya que $v \neq 2$, tenemos $\varepsilon_v(g) = 1$. Como el rango de g es ≥ 3, por el teorema (3.9) vemos que g representa a 0. Por lo tanto hemos demostrado que en todos los casos f_1 representa a 0 en $\mathbb{Q}_v$. Como el rango de f_1 es $n-1$ por la hipótesis de recurrencia tendremos que f_1 representa 0 en $\mathbb{Q}$. Luego g representa a en $\mathbb{Q}$ y como h representa a, deducimos que finalmente f representa 0 en $\mathbb{Q}$.

□

Corolario. *Sea $a \in \mathbb{Q}^*$. Para que f represente a en $\mathbb{Q}$, es necesario y suficiente que lo represente en cada $\mathbb{Q}_v$*

Corolario. *Una forma cuadrática f de rango ≥ 5 representa 0 si y solo si es indefinida(i.e. si representa a 0 en $\mathbb{R}$)*

Teorema 3.13. *Sean f y f' dos formas cuadráticas sobre $\mathbb{Q}$. Para que f y f' sean equivalentes sobre $\mathbb{Q}$ es necesario y suficiente que lo sean en cada uno de los $\mathbb{Q}_v$.*

Demostración. La necesidad es trivial. Para probar la suficiencia, razonaremos por recurrencia sobre el rango n de f y f'. Si $n = 0$, no hay nada que demostrar. Si no existe un $a \in \mathbb{Q}^*$ representado por f, por lo que también por f'. Tendremos $f \sim a\mathbb{Z}^2 + g$, $f' \sim a\mathbb{Z}^2 + g'$. Luego para todo $v \in V$ tendremos que $g \sim g'$ en $\mathbb{Q}_v$. La hipótesis de recurrencia demuestra que $g \sim g'$ en $\mathbb{Q}$ (ya que su rango es $n-1$) y por lo tanto lo serán también $f \sim f'$. □

Corolario. *Sean (r,s) y (r',s') las signaturas de f y de f'. Para que f y f' sean equivalentes, es necesario y suficiente que tengamos:*

$$d(f)=d(f'),\ (r,s)=(r',s')\ y\ \varepsilon_v(f)=\varepsilon_v(f')\ para\ todo\ v\in V.$$

En efecto estas condiciones expresan simplemente que f y f' son equivalente en cada uno de los $\mathbb{Q}_v$.

Algo a destacar es que los invariantes $d=d(f)$, $\varepsilon_v(f)=\varepsilon_v$ y (r,s) no son arbitrarios. Si no que verifican las siguientes relaciones:

1. $\varepsilon_v=1$ para casi todo $v\in V$, y $\prod_{v\in V}\varepsilon_v=1$.
2. $\varepsilon_v=1$ si $n=1$, o si $n=2$ y si la imagen de d_v de d en $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ es igual a -1.
3. $r,s\geq 0$ y $r+s=n$.
4. $d_\infty=(-1)^s$.
5. $\varepsilon_\infty=(-1)^{s(s-1)/2}$.

Inversamente también tendremos:

Proposición 10. *Sean d, $(\varepsilon_v)_{v\in V}$ y (r,s) verificando las relaciones anteriores. Entonces existe una forma cuadrática de rango n sobre $\mathbb{Q}$, que tiene por invariantes d, $(\varepsilon_v)_{v\in V}$ y (r,s).*

Demostración. El caso $n=1$ es trivial. Supongamos que $n=2$. Sea $v\in V$,como el símbolo de Hilbert es no degenerado y de la condición 2) se demuestra que existe $x_v\in\mathbb{Q}_v^*$ tal que $(x_v,-d)=\varepsilon_v$. De aquí y de la condición 1) obtenemos la existencia de $x\in\mathbb{Q}^*$ tal que $(x,-d)_v=\varepsilon_v\quad\forall v\in V$. La forma xX^2+xdY^2 convendría.
Supongamos ahora que $n=3$. Sea S el conjunto de $v\in V$ tales que $(-d,-1)_v=-\varepsilon_v$ (es un conjunto finito). Si $v\in S$, elijamos un elemento c_v en $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ distinto de la imagen de $-d_v$ de $-d$. Como $\mathbb{Q}$ es denso en $\prod_{v\in S}\mathbb{Q}_v$ existe un $c\in\mathbb{Q}^*$ el cual su imagen en cada uno de los $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ es c_v. Por lo que acabamos de demostrar, existe una forma g de rango 2 tal que:
$d(g)=cd,\quad \varepsilon_v(g)=(c,-g)_v\varepsilon_v$ para todo $v\in V$. Luego la forma $f=c\mathbb{Z}^2+g$ conviene.
Cuando $n\geq 4$ lo demostraremos por recurrencia sobre n. Primero supongamos que $r\geq 1$. Por medio de la hipótesis de recurrencia vemos que existe una forma g de rango $n-1$ que tiene por invariantes d, $(\varepsilon_v)_{v\in V}$ y $(r-1,s)$, luego la forma X^2+g es la buscada. Cuando $r=0$ construimos una forma h de rango $n-1$ teniendo por invariantes, $-d$, $\varepsilon_v(-1,-d)_v$ y $(0,n-1)$, por lo tanto la forma que necesitabamos es $-X^2+h$. □

Apéndice A

Suma de Tres Cuadrados

Gracias al estudio que hemos realizado de la clasificación de las formas cuadráticas, podremos saber cuando un entero positivo n es suma de p cuadrados, donde $p \in \mathbb{N}^*$. En este caso diremos que n está representado en el anillo $\mathbb{Z}$ por la forma cuadrática $X_1^2 + \cdots + X_p^2$, i.e. si existen enteros $n_1, \ldots, n_p$ tales que:

$$n = n_1^2 + \cdots + n_p^2.$$

Teorema. ***Gauss.*** *Para que un entero positivo n sea suma de tres cuadrados, es necesario y suficiente que no sea de la forma* $4^a(8b-1)$*, con* $a, b \in \mathbb{Z}$

Ejemplo. Si n no es divisible por 4, entonces n es suma de tres cuadrados si y solo si tenemos que n es congruente a $1,2,3,5,6$ módulo 8. $19 = 3^2 + 3^2 + 1^2$

Demostración. Podemos suponer que n es no nulo. La condicion de que n es de la forma $4^a(8b-1)$ equivale a decir que n es un cuadrado en $\mathbb{Q}_2$. Ahora bien, tenemos el resultado siguiente:

Lema. *A. Sea* $a \in \mathbb{Q}^*$*. Para que a sea representado en* $\mathbb{Q}$ *por la forma cuadrática* $f = X_1^2 + X_2^2 + X_3^2$*, es suficiente y necesario que a>0 y que -a no sea un cuadrado en* $\mathbb{Q}_2$*.*

Ahora tenemos que pasar de la representación en $\mathbb{Q}$ a la representación en $\mathbb{Z}$. Esto lo conseguimos gracias al siguiente lema:

Lema. *B. Sea la forma cuadrática:*
$f(X) = \sum_{i,j=1}^{p} a_{ij} X_i X_j$
Definida positiva, la matriz $(a_{ij}$ *es simétrica y con coeficientes enteros. Haremos la siguiente hipótesis: Para todo* $x = (x_1, \ldots, x_p) \in \mathbb{Q}^p$*, existe* $y \in \mathbb{Z}^p$ *tal que* $f(x-y) < 1$*.*
Entonces si $n \in \mathbb{Z}$ *es representado por* f *en* $\mathbb{Q}$*, n es representado por* f *en* $\mathbb{Z}$ *también.*

Por lo que ahora para demostrar el Teorema bastara con verificar que la forma $f = X_1^2 + X_2^2 + X_3^2$ satisface la hipótesis del lema anterior. Esto es inmediato ya que si $(x_1, x_2, x_3) \in \mathbb{Q}^3$ elegimos $(y_1, y_2, y_3) \in \mathbb{Z}^3$ tal que $|x_i - y_i| \leq 1/2$ para todo i. Tenemos $\sum (x_i - y_i)^2 \leq 3/4 < 1$

□

Corolario. *(Lagrange) Todo entero positivo es suma de cuatro cuadrados.*

Demostración. Sea n un entero >0. Podremos escribirlo de la forma $4^a m$, donde m no es divisible por 4. Si $m \equiv 1,2,3,5,6 \pmod 8$, m es suma de tres cuadrados y por lo tanto también n. Si no, tendremos $n \equiv -1 \pmod 8$ y así $m-1$ es suma de tres cuadrados, luego m es suma de cuatro cuadrados y entonces n también. □

Corolario. *(Gauss). Todo entero positivo es suma de tres números triangulares. (llamaremos números triangulares a todo número de la forma* $\frac{m(m+1)}{2}$*), donde m es un entero)*

Demostración. Sea n un entero ≥ 0. Aplicando el teorema a $8n+3$ vemos que existen enteros x_1, x_2, x_3 tales que:
$x_1^2 + x_2^2 + x_3^2 = 8n+3$.
Por lo tanto:
$x_1^2 + x_2^2 + x_3^2 \equiv 3 \pmod 8$.
Pero los únicos cuadrados en $\mathbb{Z}/8\mathbb{Z}$ son 0,1,4, por lo tanto una suma de tres cuadrados en $\mathbb{Z}/8\mathbb{Z}$ puede ser igual a 3 solo si los terminos son igual a 1. Podemos entonces deducir que los x_i son impares, luego podemos escribirlos de la forma $2m_i+1$, con m_i entero. Tenemos:
$$\sum_{i=1}^{i=3} \frac{m_i(m_i+1)}{2} = \frac{1}{8}(\sum_{i=1}^{i=3}(2m_i+1)^2 - 3) = \frac{1}{8}(8n+3-3) = n$$ □

Bibliografía

[1] JEAN-PIERRE SERRE, *Cours d'Arithmétique*, 9–82.
Presses Universitaires de France.

[2] F. MONTANER, *Curso Teoría de Números 1996-1997*, 13–53.

[3] Y. AMICE, *Les nombre p-ádiques*, 15-35.
Presses Universitaires de France.

[4] I. KAPLANSKY, *Linear Algebra And Geometry*, 1–26.

[5] Texto de Fermat. `http://personal.us.es/arias/TAN2003-4/03-Diofanto.pdf`

[6] P.RIBENBOM, *L'Arithmétique Des Corps*.
Hermann Paris.

[7] William Stein, Elementary Number Theory: Primes, Congruences, and Secrets.
`http://wstein.org/ent/ent.pdf`