LEYES DE RECIPROCIDAD CUADRÁTICA

Rubén Martínez Subías

Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Directores del trabajo: Fernando Montaner Frutos y Mª Paz Jiménez Seral

4 de septiembre de 2023

Preface

This work covers the various laws of quadratic reciprocity without delving into results that involve class field theory.
Law of quadratic reciprocity answers whether, given a polynomial f with coefficients in $\mathbb{Z}$, and a prime p, whether f modulo p is a product of distinct linear factors. We will focus on the classical laws of reciprocity, i.e. on monic polynomials of degree 2. That's why, among all the results that provide a solution to this problem, we will examine the quadratic reciprocity law of Gauss and Legendre. Additionally, we will also explore Hilbert's quadratic reciprocity law.
Before discussing the analysis and proofs of these results, we introduce a series of concepts about fields, rings, abelian groups, congruences, and isomorphism theorems upon which the results in the subsequent chapters are based.

- The first part, covered in Chapter 2, discusses the laws of quadratic reciprocity. The Legendre symbol is introduced, which encodes the information of an interger being a quadratic number residue modulo a natural number, and two of its properties are presented: Euler's criterion, which relates the Legendre symbol to the multiplicative structure of the set residues modulo the number on which the question of being a quadratic residue is posed, and secondly, Gauss's criterion, which provides a combinatorial interpretation, which will derive in a procedure of computation of the Legendre symbol. Finally, the Legendre and Gauss reciprocity laws are stated and proved, shedding light on the origin of the term reciprocity.

- In Chapter 3 we construct the field $\mathbb{Q}_p$ of p-adic numbers. We begin with the ring of quotients $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and by taking its projective limit, we obtain the ring of p-adic intergers $\mathbb{Z}_p$. Then, for $x \in \mathbb{Z}_p$, we examine how the mapping $x \to px$ behaves. The next step is to construct a field from $\mathbb{Z}_p$, so we need to find the invertible elements of $\mathbb{Z}_p$, which turn out to be the elements that are not multiples of p. We also prove that $\mathbb{Z} \subseteq \mathbb{Z}_p$, is an integral domain of zero characteristic, hence $\mathbb{Z}$ can be identified to the subring consisting of the interger multiples of the unit element of $\mathbb{Z}_p$. Moreover, we explore properties of the units, will help us establish that $\mathbb{Z}_p$ is a local ring and a principal ideal domain. Finally, we take the field of fractions of $\mathbb{Z}_p$ to obtain $\mathbb{Q}_p$.

- In Chapter 4 , the goal is twofold. Firstly, we aim to characterize the squares in $\mathbb{Q}_p$. To do this, we discuss the units of $\mathbb{Z}_p$ once again, and express $U = U(\mathbb{Z}_p) = U_1 \times \{x \in U \mid x^{p-1} = 1\}$, where $U_1 = 1 + p\mathbb{Z}_p$. if $p = 2$ then $U_1 = \pm 1 \times U_2$ and U_2 is isomorphic to $\mathbb{Z}_2$. If $p \neq 2$ then U_1 is isomorphic to $\mathbb{Z}_p$. This allows us to describe $\mathbb{Q}_p \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ for $p \neq 2$ and $\mathbb{Q}_2 \simeq \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ for $p = 2$. With this, we can characterize the squares in $\mathbb{Q}_p^*$ and $\mathbb{Q}_2^*$. This characterization of squares reveals that $\mathbb{Q}_p^*$ forms a group of type $(2,2)$, while the squares in $\mathbb{Q}_p^*$ constitute a group of type $(2,2,2)$.
  Additionally, in this section, we discuss p-adic equations. We explore how to relate polynomials with m variables in A_n, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ and their roots in A_n, $\mathbb{Z}_p$ and $\mathbb{Q}_p$. We also

state and prove the Chevalley-Warning theorem and its corollary, which tell us that if f is a polynomial with m variables in F_p, $\mathbb{Z}_p$ or $\mathbb{Q}_p$, if $gr(f) < m$ and f has no constant term, then, $f(x_1,\ldots,x_m) = 0$ has at least one non-trivial solution.

- In Chapter 5 we define the Hilbert symbol, a number whose value is 1 if the quadratic form $z^2 - ax^2 - by^2 = 0$ where $a,b \in \mathbb{Q}_p$ o $\mathbb{R}$ has no trivial zeros. To prove these results, we need the previous chapter. We also examine several properties, among which the most crucial are its bilinearity and non-degeneracy. Theorem 5.1 relates the Legendre and Hilbert symbols in the following way $\begin{cases} a = p^\alpha u \\ b = p^\beta v \end{cases}$ where $u,v \in U$. we have that

$$(a,b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \text{ if } p \neq 2$$

$$(a,b) = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} \text{ if } p = 2$$

  This result will help us prove Hilbert's reciprocity law whic is stated at the end of this section.

Resumen

Este trabajo recorre distintas leyes de reciprocidad cuadrática sin entrar en aquellos resultados que entren en teoría de cuerpos de clases.
Una ley de reciprocidad cuadrática da respuesta a si dado un polinomio f con coeficientes en $\mathbb{Z}$ y un un primo p si f módulo p es producto de distintos factores lineales. Nos centraremos en las leyes clásicas de reciprocidad, es decir, en polinomios mónicos de grado 2 y por eso entre todos los resultados que dan solución a este problema veremos la ley de reciprocidad cuadrática de Gauss y Legendre. Además, también veremos la ley de reciprocidad cuadrática de Hilbert.
Antes de entrar a discutir el análisis y las demostraciones de estos resultados introducimos una serie de conceptos sobre cuerpos, anillos, grupos abelianos, congruencias y teoremas de isomorfía sobre los cuales se basan los resultados de los capítulos siguientes.

- La primera parte que abarca el capítulo 2 habla sobre las leyes de reciprocidad cuadrática, se introduce el símbolo de legendre que codifica la información de un entero que es residuo cuadrático módulo un número natural y se presentan dos de sus propiedades. Por un lado el criterio de Euler que relaciona el símbolo de Legendre con congruencias. Por otro lado, el criterio de Gauss proporciona una interpretación combinatoria que nos llevará a un proceso de computación del símbolo de Legendre. Por último se enuncia y demuestra la ley de reciprocidad de Legendre y Gauss donde se observa de donde viene el nombre de reciprocidad.

- El capítulo 3 vamos construyendo el cuerpo $\mathbb{Q}_p$ de números p-ádicos, empezamos por el anillo de cocientes $A_n = \mathbb{Z}/p^n\mathbb{Z}$ que tomando su límite proyectivo conseguimos el anillo de enteros p-ádicos $\mathbb{Z}_p$. Luego, si $x \in \mathbb{Z}_p$ vemos como se comporta la aplicación que lleva $x \to px$. Lo siguiente es construir un cuerpo a partir de $\mathbb{Z}_p$ así que tenemos que encontrar los elementos invertibles de $\mathbb{Z}_p$, que resultan ser los elementos que no son múltiplos de p. Además, vemos propiedades de las unidades ya que nos ayudarán a ver que es dominio de integridad. Una vez, probado todo esto vemos que $\mathbb{Z} \subseteq \mathbb{Z}_p$ es un dominio de integración de característica cero, por lo tanto, $\mathbb{Z}$ puede identificarse con un subanillo que consiste en los múltiplos enteros del elemento unidad de $\mathbb{Z}_p$, que es un anillo local y dominio de ideales principales: Por último, tomamos el cuerpo de fracciones de $\mathbb{Z}_p$ y obtenemos $\mathbb{Q}_p$.

- El objetivo del capítulo 4 es doble primero queremos caracterizar los cuadrados en $\mathbb{Q}_p$ para ello volvemos a hablar sobre las unidades de $\mathbb{Z}_p$ y como podemos poner $U = U(\mathbb{Z}_p) = U_1 \times \{x \in U \mid x^{p-1} = 1\}$, donde $U_1 = 1 + p\mathbb{Z}_p$. Si p es 2 $U_1 = \pm 1 \times U_2$ y U_2 isomorfo a $\mathbb{Z}_2$. Si p no es 2 U_1 es isomorfo a $\mathbb{Z}_p$. Con esto $\mathbb{Q}_p \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ si $p \neq 2$ y $\mathbb{Q}_2 \simeq \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. Con esto podremos caracterizar los cuadrados en $\mathbb{Q}_p^*$ y los cuadrados en $\mathbb{Q}_2^*$. Esta caracterización de los cuadrados nos dirá que $\mathbb{Q}_p^*$ serán un grupo de tipo $(2,2)$ si $p \neq 2$ y los cuadrados en $\mathbb{Q}_2^*$ es un grupo de tipo $(2,2,2)$.
  Además, en esta sección se habla sobre ecuaciones p-ádicas. Como podemos relacionar polinomios de m variables en A_n, $\mathbb{Z}_p$ y $\mathbb{Q}_p$ y sus raices en A_n, $\mathbb{Z}_p$ y $\mathbb{Q}_p$. También, veremos

y probaremos el teorema de Chevalley-Warning y su corolario que nos dice que sea f un polinomio con m variables en F_p, $\mathbb{Z}_p$ o $\mathbb{Q}_p$ si $gr(f) < m$ y f no tiene término constante, entonces, $f(x_1,\ldots,x_m) = 0$ tiene al menos una solución no trivial.

- En el capítulo 5 se define el símbolo de Hilbert, un número cuyo valor es 1 si la forma cuadrática $z^2 - ax^2 - by^2 = 0$ donde $a,b \in \mathbb{Q}_p$ o $\mathbb{R}$ para probar estos resultados necesitamos el capítulo anterior. Además, se ven varias propiedades entre ellas las más importantes son su bilinealidad y que no es degenerado.
  El teorema 5.1 nos relaciona el símbolo de Legendre y el de Hilbert de la siguiente manera $\begin{cases} a = p^{\alpha}u \\ b = p^{\beta}v \end{cases}$ donde $u,v \in U$. Tenemos que:

$$(a,b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha} \text{ si } p \neq 2$$

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

  Este resultado nos ayudará a probar la ley de reciprocidad de Hilbert que se presenta al final de esta sección.

Índice general

Capítulo 1

Resultados Previos

El contenido de este capitulo se puede ver en [4].

Sea K un cuerpo. La imagen de $\mathbb{Z}$ en K es un dominio de integridad, por lo tanto es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/p\mathbb{Z}$ donde p es primo; su cuerpo de fracciones es isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}/p\mathbb{Z} = F_p$. En el primer caso, se dice que K tiene característica 0; en el segundo caso que tiene característica p.
La característica de K se denota como $char(K)$. Si $char(K) = p \neq 0$, entonces, p es el entero más pequeño tal que $p \cdot 1 = 0$.

Notación. $\mathbb{Z}/p\mathbb{Z} = F_p$ y no como $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ porque más adelante usaré $\mathbb{Z}_p$ para referirnos al anillo de enteros p-ádicos.

Si K es finito la característica es distinta de 0.

Definición. Un cuerpo L es una extensión de K si K es subcuerpo de L. En este caso, L es espacio vectorial sobre K y se denota como E/K.

Definición.

Sea $f \in K[x]$ y E/K una extensión decimos que f se escinde en E si existen $a, a_1, \ldots, a_n \in E$ tales que $f = a(x-a_1)\cdots(x-a_n)$. Además, si todos los a_i son distintos entonces decimos también que f es separable.

Teorema 1.1.

(a) Si K es finito tiene un subcuerpo que podemos identificar como F_p y si dimensión de K como F_p espacio vectorial es f, el número de elementos de K es $q = p^f$. Luego K es una extensión de F_p.

(b) Si $f \in K[x]$ entonces existe un cuerpo en el que se escinde f.

(c) Sea p un numero primo y $q = p^f\,(f \geq 1)$ una potencia de p. Existe un cuerpo Ω en el que se escinde $X^q - X$, que tiene q elementos, tiene característica p y que denotaremos por F_q.

Teorema 1.2. *El grupo multiplicativo F_q^* de un cuerpo finito F_q es cíclico de orden $q-1$.*

Proposición 1.2.1. Si A es un grupo abeliano (un anillo) e I es un subgrupo (un ideal) la proyección canónica es el homomorfismo de grupos (de anillos) $\varphi : A \to A/I$ tal que $\varphi(a) = a + I$. Es suprayectiva y su núcleo es I.

En lo que sigue denotaremos a los elementos de F_p como cualquiera de sus representantes en $\mathbb{Z}$.

Teorema 1.3. *Sea $f : G \to H$ un homomorfismo de grupos abelianos entonces $\bar{f} : G/Ker_f \to Imf$ tal que $\bar{f}(a+Ker_f) = f(a)$ con $a \in G$ es un isomorfismo.*
Sea $I \leq Ker_f$, entonces, existe $f^* : G/I \to H$ homomorfismo tal que $f^*(a+I) = f(a)$ con $a \in G$.

Teorema 1.4. *Sea G un grupo abeliano y N y H subgrupos de G entonces HN/N es isomorfo a $H/(H \cap N)$.*

Teorema 1.5. *Sea G un grupo abeliano y N y H subgrupos de G tal que $N \subseteq H$ entonces G/H es isomorfo a $(G/N)/(H/N)$.*

Definición. $q \in \mathbb{Z}$ es un residuo cuadrático de un número primo p si existe $x \in \mathbb{Z}$ tal que $x^2 \equiv q \pmod{p}$, es decir, $x^2 = q$ en F_p.

Definición. Una extensión K de un cuerpo F que tiene dimensión finita como F espacio vectorial esta formada por números algebraicos, esto quiere decir que para todo $a \in K$ existe $p \in F[x]$ tal que $p(a) = 0$. Si (p) es el núcleo del homomorfismo evaluación $F[x] \to K$ dada por $f \to f(a)$ a p se le llama polinomio mínimo de a sobre F.

Teorema 1.6. *Sea $F = K(\theta)$ el menor cuerpo que contiene a K y a θ, siendo θ un elemento algebraico sobre K. Además, sea L un cuerpo donde se escinde p, el polinomio mínimo de θ sobre K. Si p tiene grado n y es separable, entonces, hay exactamente n distintos homomorfismos $\sigma_i : F \longmapsto L$ y los elementos $\sigma_i(\theta) = \theta_i$ son los distintos ceros de p.*

Definición. Dada una K-base de $F = K(\theta)$, $\{\alpha_1, ..., \alpha_n\}$. Se define el discriminante de la base como:

$$\Delta[\alpha_1, ..., \alpha_n] = (det(\sigma_i(\alpha_j)))^2$$

Además, se define la norma de $\alpha \in F$ como:

$$NK(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

El conjunto de normas forman un grupo multiplicativo.

Teorema 1.7 (Teorema chino de los restos)**.** *Supongamos que $n_1, n_2, \ldots, n_k$ son enteros positivos coprimos dos a dos y $N = n_1...n_k$. Entonces, se tiene un isomorfismo entre un anillo y la suma directa de sus factores.*

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_k\mathbb{Z}$$

Una formulación más clásica, manteniendo las hipótesis ya planteadas.
Entonces para enteros dados $a_1, a_1, ..., a_k$ existe un entero x que resuelve el sistema de congruencias simultáneas.

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Más aún, todas las soluciones x de este sistema son congruentes módulo el producto N.

Lema 1.1. Sea p la característica de un cuerpo, si x e y son elementos de ese cuerpo, entonces $(x+y)^p = x^p + y^p$.

Definición. Si H es un subgrupo finito de G y $x \in G$ se llama coclase a izquierda a $xH = \{xh | h \in H\}$. Si k es el numero de coclases a izquierda de G módulo un subgrupo H entonces a k se le llama índice de H en G, se escribe $|G:H|$ y por el teorema de lagrange tenemos que $|G:H| = \frac{|G|}{|H|}$.

Proposición 1.7.1. $\forall n \geq 1$ y p primo $p^n\mathbb{Z}$ es un ideal de $\mathbb{Z}$, denotaremos estos ideales (p^n), los múltiplos de p^n. El anillo cociente $\mathbb{Z}/(p^n)$ tiene $x+(p^n)$ como unidad si p no divide a x. Denotamos como $U(\mathbb{Z}/(p^n))$ al grupo multiplicativo de las unidades de $\mathbb{Z}/(p^n)$ y se tiene que $|U(\mathbb{Z}/(p^n))| = p^{n-1}(p-1)$.

Proposición 1.7.2. Sea G un grupo abeliano donde $|G| = mn$ y m y n son coprimos, entonces existen únicos subgrupos A, B de G tal que $G = AB$ con $A \cap B = 1$, $|A| = m$ y $|B| = n$.

Proposición 1.7.3. El polinomio $x^n - 1 \in F_p[x]$ tiene n raices distintas en un cuerpo en el que se escinda si y solo si p no divide a n. Esas raíces forman un grupo cíclico llamado raíces de la unidad y a los generadores se les llama raíces primitivas.

Teorema 1.8 (pequeño teorema de Fermat)**.** *Si p es un número primo, entonces, para cada número natural a, con $a > 0$, coprimo con p , $a^{p-1} \equiv 1 \pmod{p}$.*

Definición. Sea una sucesión de conjuntos (A_i) y una sucesión de aplicaciones suprayectivas $\phi_n : A_n \to A_{n-1}$

$$\cdots\cdots A_n \to A_{n-1} \to \cdots \to A_2 \to A_1$$

Se llama límite proyectivo al subconjunto de $\prod_n A_n$ formado por las sucesiones

$$\mathbf{x} = (\cdots\cdots, x_n, x_{n-1}, \cdots\cdots, x_2, x_1)$$

tales que $x_n \in A_n$ y $\phi_n(x_n) = x_{n-1}$.
Este límite verifica que la proyección en cada componente es una aplicación suprayectiva.

Proposición 1.8.1. Sea una sucesión de conjuntos (A_i) que son grupos (o anillos) y una sucesión de aplicaciones suprayectivas $\phi_n : A_n \to A_{n-1}$ que son homomorfismos de grupos (o de anillos). Entonces el límite proyectivo es un subgrupo (o subanillo) de $\prod_n A_n$ Además, en este caso, un elemento del límite proyectivo tiene inverso en el límite proyectivo sí y solo si lo tiene en $\prod_n A_n$

Demostración. Sean

$$\mathbf{x} = (\cdots, x_n, x_{n-1}, \cdots, x_2, x_1)$$

$$\mathbf{y} = (\cdots, y_n, y_{n-1}, \cdots, y_2, y_1)$$

Veamos que si $\mathbf{x}, \mathbf{y}$ están en el límite proyectivo, $\mathbf{xy}$ también lo está.
$\phi_n(x_n y_n) = \phi_n(x_n)\phi_n(y_n) = x_{n-1}y_{n-1}$ luego el producto está en el límite. Análogamente para $+$.
Sea ahora $\mathbf{x}$ en el límite proyectivo y tal que existe $\mathbf{y} \in \prod_n A_n$ tal que $\mathbf{xy} = \mathbf{1}$. Se tiene que $x_n y_n = 1$ y $x_{n-1}y_{n-1} = 1$. De la primera igualdad obtenemos $\phi(x_n)\phi(y_n) = 1$ y $x_{n-1}\phi(y_n) = 1$ luego el inverso de x_{n-1} es exactamente $y_{n-1} = \phi(y_n)$ y esto prueba que $\mathbf{y}$ está en el límite proyectivo. □

Capítulo 2

Leyes de reciprocidad cuadrática

Dado un polinomio $f(x)$ con coeficientes en $\mathbb{Z}$, una ley de reciprocidad determina, para un primo p si $f(x)$ módulo p es producto de distintos factores lineales, en ese caso decimos que se separa.

2.1. Cuadrados en F_q

En este capítulo q es un potencia de un primo p.

Teorema 2.1.

(a) Si $p = 2$, entonces todos los elementos de F_q son cuadrados.

(b) Si $p \neq 2$, entonces los cuadrados de F_q^* forman un subgrupo de índice 2 en F_q^*; este subgrupo es el kernel del homomorfismo $x \longmapsto x^{(q-1)/2}$ con valores en ± 1.

Demostración. El caso (a) se sigue del hecho $x \longmapsto x^2$ es un automorfismo en F_q porque la característica del grupo es 2 y por lo tanto $(x+y)^2 = x^2 + y^2$ por el lema 1.1, con la multiplicación no hay problemas. Es inyectiva porque si $x^2 = 0$ entonces $x = 0$ y es obvio que es suprayectiva. Luego es un automorfiso.
El caso (b), sea Ω un cuerpo de escisión del polinomio $y^2 = x$ en F_q. Sea $y \in \Omega$ y $x \in F_q^*$ tal que $y^2 = x$. Entonces como el homomorfismo $x \to x^2$ tiene núcleo $\{\pm 1\}$y su imagen son los cuadrados, los denotaremos $(F_q^*)^2$, entonces $|F_q^*|/2 = |(F_q^*)^2|$ como $(F_q^*)^2$ es subgrupo de F_q^* entonces $|F_q^*|||(F_q^*)^2|$, luego los cuadrados tienen índice 2. Como F_q^* e un grupo cíclico de orden $q-1$, entonces $x^{q-1} = 1$, luego $x^{(q-1)/2} = \pm 1$. Luego $(F_q^*)2$ es el kernel de la aplicación $x \longmapsto x^{(q-1)/2}$. □

Euler, interesado por el trabajo de Fermat, empezó una correspondecia con Goldbach donde intercambiaron ideas, entre otras cosas, sobre los divisores de los númeos de Fermat $(2^{2^n} + 1)$ y los números de Mersenne $(2^q - 1)$ lo que llevo a Euler a una ley de reciprocidad cuadrática. El teorema anterior nos permite justificar el siguiente enunciado.

Proposición 2.1.1 (Criterio de Euler)**.** Para enteros a y primos impares p tal que $p \nmid a$ tenemos que

$$a^{\frac{p-1}{2}} = \begin{cases} +1 \text{ en } F_p, \text{ si } a \text{ es un residuo cuadrático módulo p} \\ -1 \text{ en } F_p, \text{ si } a \text{ no es un residuo cuadrático módulo p} \end{cases}$$

Definición. Sea $p \neq 2$ primo y sea $x \in F_p^*$. El símbolo de Legendre de x se denota como $\left(\frac{x}{p}\right)$ y es ± 1 según si $x^{(p-1)/2} = \pm 1$ en F_p.
Conviene extender $\left(\frac{x}{p}\right)$ a todo F_p definiendo $\left(\frac{0}{p}\right) = 0$.

Observación.

(a) Si $x = x'$ en F_p, uno escribe $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.

(b) $\forall x, y \in \mathbb{Z}$, $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$.

2.1.1. Fórmulas complementarias

Para calcular $\left(\frac{x}{p}\right)$ para $x = 1, -1, 2$, vamos a introducir las siguientes funciones.
Si n es un entero impar, sea $\varepsilon(n)$ y $\omega(n)$ los elementos de $\mathbb{Z}/2\mathbb{Z}$ definidos de la siguiente manera

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

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

Notar que la funcion ε es un homomorfismo de $(\mathbb{Z}/4\mathbb{Z})^*$ en $\mathbb{Z}/2\mathbb{Z}$. De la misma manera ω es un homomorfismo de $(\mathbb{Z}/8\mathbb{Z})^*$ en $\mathbb{Z}/2\mathbb{Z}$.

Teorema 2.2.

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

(b) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$

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

Demostración. Demostremos (c) ya que (a) y (b) son inmediatos. Si α denota una raíz primitiva 8-ésima de la unidad en un cuerpo Ω donde estén todas las raíces 8-ésimas de la unidad, el elemento $y = \alpha + \alpha^{-1}$ verifica que $y^2 = 2$ ya que $y^2 = (\frac{\alpha^2+1}{\alpha})^2 = \frac{\alpha^4+2\alpha^2+1}{\alpha^2} = \frac{-1+1+2\alpha^2}{\alpha^2}$, esto se debe a que $\alpha^4 = -1$. Como estamos en un cuerpo de característica p por 1.1 tenemos que $y^p = \alpha^p + \alpha^{-p}$. Notar que si $p = a + \bar{8}$ donde $\bar{8}$ son múltiplos de 8 tenemos que $y^p = \alpha^a + \alpha^{-a}$, en nuestro caso nos interesa $a = 1$ y $a = 5$ porque si $a = 1$ entonces $y^p = \alpha + \alpha^{-1} = y$ y de este modo $\left(\frac{2}{p}\right) = y^{p-1} = 1$.
Si $a = 5$ tenemos que $y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y$ y de esta manera $\left(\frac{2}{p}\right) = y^{p-1} = -1$. □

2.1.2. Ley de reciprocidad cuadrática de Legendre y Gauss

Usando el criterio de Euler podemos conseguir otros criterios para el símbolo de Legendre. Vamos a escribir las unidades de F_p de la siguiente manera $U(F_p) = \{-(p-1)/2, \ldots, -2, -1, 1, 2, \ldots, (p-1)/2\} = N \cup P$ donde $P = \{1, 2, \ldots, (p-1)/2\}$ y podemos escribir $N = -1P$.

Proposición 2.2.1 (Criterio de Gauss)**.** Con la notación usada anteriormente, si $kP \cap N$ tiene v elementos entonces $\left(\frac{k}{p}\right) = (-1)^v$.

Demostración. Si k es una unidad, los elementos kP son distintos por lo tanto $|kP| = |P|$, es mas, si a, b son elementos distintos de P, podemos tomar $0 < a < b < (p-1)/2$ y no puede ocurrir que $ka = r$ y $kb = -r$ ya que esto implicaria que $k(a+b) = 0$ y como k es unidad entonces implicaría que $(a+b)$ es divisible por p, contradiciendo que $a, b < (p-1)/2$. Además los elementos de $kP = \{\pm 1, \ldots, \pm(p-1)/2\}$, luego el número de elementos negativos es el número de elementos de kP en N por lo tanto $k \cdot k2 \cdots k(p-1)/2 = (\pm 1) \cdots (\pm(p-1)/2)$ luego $k^{(p-1)/2} = (-1)^v$ donde $v = |kP \cap N|$, por lo tanto $k^{(p-1)/2} \equiv (-1)^v \pmod{p}$ y aplicando el criterio de Euler obtenemos que $\left(\frac{k}{p}\right) = (-1)^v$. □

Gracias a este criterio podemos calcular las formulas complementarias de otra forma.

Proposición 2.2.2.

(a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, luego -1 es residuo cuadrático módulo p si y solo si $p \equiv 1 \pmod{4}$

(b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, luego 2 es residuo cuadrático módulo p si y solo si $p \equiv \pm 1 \pmod{8}$

Demostración. (a) $-1P = N$, entonces $|-P \cap N| = p - 1/2$.
(b) $2P = 2, 4, ..., p-1$, luego $\nu = |2S \cap (-S)| = \frac{p-1}{2} - r$ donde r es el entero más grande tal que $2r \leq \frac{p-1}{2}$. Ahora la demostración se divide en dos casos:
Caso 1. $\frac{p-1}{2}$ es par y $2r = \frac{p-1}{2}$, por lo tanto, $\nu = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$, de este modo, $\left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$
Caso 2. $\frac{p-1}{2}$ es impar y $2r = \frac{p-1}{2} - 1$, por lo tanto, $\nu = \frac{p-1}{2} - \frac{p-1}{4} + \frac{1}{2} = \frac{p+1}{4}$, de este modo, $\left(\frac{2}{p}\right) = (-1)^{(p+1)/4}$
Podemos unir estos dos casos notando que en el primer caso $(p-1)/2$ es par si y solo si $(p+1)/2$ es impar y elevar $(-1)^n$ a una potencia impar no lo cambia. Luego tenemos para el caso 1 que

$$\left(\frac{2}{p}\right) = \left[(-1)^{(p-1)/4}\right]^{(p+1)/2} = (-1)^{(p^2-1)/8}$$

Para el caso 2. se sigue el mismo procedimiento pero elevando a una potencia impar $(p-1)/2$. □

Teorema 2.3 (Ley de reciprocidad cuadrática de Gauss y Legendre)**.** *Si p y l son primos impares distintos, entonces* $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{(p-1)(l-1)/4}$

Demostración. Gracias al criterio de Gauss 2.2.1 $\left(\frac{l}{p}\right) = (-1)^v$ donde v es el número elementos $1 \leq a \leq (p-1)/2$ tal que existe un elemento b que satisface $al = bp + r$ donde $-p/2 < r < 0$.

Además tiene que haber por lo menos una b para cada a, luego podemos reescribir v como el número de pares (a,b) que satisfacen (despejando r)

$$1 \leq a \leq (p-1)/2$$

$$-p/2 < al - bp < 0$$

De estas dos expresiones podemos deducir que

$$bp < al + p/2 \leq (p-1)l/2 + p/2 < pl/2 + p/2 = p(l+1)/2$$

luego $b < (l+1)/2$ y de $-p/2 < al - bp < 0$ obtenemos que $b \geq 1$, y por lo tanto $1 \leq b \leq (l-1)/2$, como esta desigualdad es consecuencia de los requisitos de v podemos añadirlo como otro requisito y de esta manera podemos cambiar los lugares de a y b y obtener que $\left(\frac{p}{l}\right) = (-1)^{\mu}$ donde μ es el el número de pares (a,b) que satisface

$$1 \leq a \leq (p-1)/2$$

$$1 \leq b \leq (l-1)/2$$

$-l/2 < bp - al < 0$ que se puede escribir como $0 < aq - bp < l/2$

Como l y q son dos primos distintos de los dos primeros requisitos obtenemos que $al - bp \neq 0$ luego $v + \mu$ es el número de pares (a,b) que satisfacen

$$1 \leq a \leq (p-1)/2$$

$$1 \leq b \leq (l-1)/2$$

$$-p/2 < al - bp < l/2$$

Ahora $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{v+\mu}$ luego el problema se reduce a encontrar el valor de $v+\mu$ módulo 2. Sea $R = \{(a,b) \in \mathbb{Z}^2 | 1 \leq a \leq (p-1)/2, 1 \leq b \leq (l-1)/2\}$ por lo tanto $|R| = (p-1)(l-1)/4$. Partimos R en tres subconjuntos

$$R_1 = \{(a,b) \in R | al - bp \geq -p/2\}$$

$$R_2 = \{(a,b) \in R | -p/2 < al - bp < l/2\}$$

$$R_3 = \{(a,b) \in R | l/2 < al - bp\}$$

Notar que R_2 es el conjunto de soluciones que cumple los requisitos que queremos, luego $|R_2| = v + \mu$. Sea $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ la aplicación dada por $f(a,b) = ((p+1)/2 - a, (l+1)/2 - b)$ luego restringiéndola a $f : R_1 \to R_3$ tenemos una biyección, entonces, $|R_1| = |R_3|$ y obtenemos que $|R| = |R_1| + |R_2| + |R_3| \equiv |R_2| \pmod 2$ y esto implica que $(p-1)(l-1)/4 = v + \mu$ y obtenemos que $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{(p-1)(l-1)/4}$. □

Esta ley motiva la siguiente observación.

Observación (Origen del nombre de reciprocidad)**.** Escribimos lRp si l es un cuadrado $\pmod p$, que es lo mismo que l sea un residuo cuadrático módulo p y de lo contrario lNp.
El teorema de Gauss quiere decir

$$lRp \Leftrightarrow pRl \text{ si } p \text{ o } l \equiv 1 \pmod 4$$

Que da el nombre de reciprocidad porque l sea un residuo cuadrático módulo p si y solo si p sea un residuo cuadrático módulo l. Esta ley de reciprocidad cuadrática fue formulada por Legendre y Gauss, aunque hemos visto en la introducción que su primera formulacion fue hecha por Fermat, que es la más conocida. Además, Gauss fue la primera persona en demostrar esta ley.

$$lRp \Leftrightarrow pNl \text{ si } p \text{ o } l \equiv -1 \pmod 4$$

Si tenemos que calcular que un numero k es un residuo cuadrático módulo m:

(a) Factorizaremos en primos m, gracias al teorema chino de los restos 1.7 y tendremos que ver si k es residuo cuadrático para cada primo de la factorización de m.

(b) Si alguno de los factores primos es 2, debemos mirar si 2^e es la mayor potencia de 2 que divide a m y tenemos tres casos:

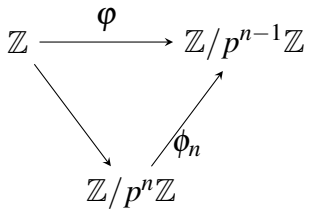
- Si $e = 1$ cualquier k es cuadrado.
- Si $e = 2$ debemos ver que $k \equiv 1 \pmod 4$.
- Si $e \geq 3$ debemos ver que $k \equiv 1 \pmod 8$.

(c) Para los factores primos impares aplicando las propiedades del símbolo de Legendre para ir calculando símbolos de Legendre para primos más pequeños y en ultimo caso aplicamos los criterios de Euler y Gauss.

Capítulo 3

Cuerpos p-ádicos

A partir de $\mathbb{Z}\ \forall n \geq 1$, sea $A_n = \mathbb{Z}/p^n\mathbb{Z}$ el anillo cociente de $\mathbb{Z}$ de clases de enteros $(\text{mód } p^n)$. Los elementos de A_n son de la siguiente forma $\bar{x_n} = x_n + (p^n)$ con $x_n \in \mathbb{Z}$ y (p^n) es ideal de los múltiplos de p^n.
Tenemos el siguiente diagrama conmutativo.



Donde los morfismo que salen de $\mathbb{Z}$ son las proyecciones canónica y como $p^n\mathbb{Z} \subset p^{n-1}\mathbb{Z} = Ker_\varphi$ ya que p^n es múltiplo de p^{n-1} entonces por 1.3 tenemos las ϕ_n. Recordemos que este homomorfismo

$$\phi_n : A_n \longmapsto A_{n-1}$$

lleva $x + (p^n) \to x + (p^{n-1})$ donde $x \in \mathbb{Z}$. Además, es suprayectivo y su kernel es $p^{n-1}A_n$.

Definición. $\mathbb{Z}_p$ es el límite proyectivo del conjunto de (A_i) con los homomorfismos ϕ_i. Recordemos que esto significa que $\mathbf{x} = (\ldots, \bar{x}_n, \bar{x}_{n-1}, \ldots, \bar{x}_1) \in \mathbb{Z}_p$ con $\bar{x}_n \in A_n$ si y solo si $\phi_n(\bar{x}_n) = \bar{x}_{n-1} \in A_{n-1}$.
Es anillo por lo visto en 1.8.1.
Sea $\varepsilon_n : \mathbb{Z}_\mathfrak{p} \longmapsto A_n$ la función que asocia a un entero p-ádico $\mathbf{x}$ su componente n-ésima $\bar{x}_n$

Proposición 3.0.1. $\mathbb{Z} \subseteq \mathbb{Z}_p$

Demostración. La aplicación de $\mathbb{Z}$ en $\mathbb{Z}_p$ dado por $a \to \mathbf{a}$ tal que $\varepsilon_n(\mathbf{a}) = a + (p)^n$ es un homomorfismo y si $0 < |a| < p^n$ se tiene $\varepsilon_n(\mathbf{a}) \neq 0$ luego $\mathbf{a} \neq 0$ y por tanto la aplicación es inyectiva. □

Hemos visto que ϕ_n lleva $x + (p^n) \to x + (p^{n-1})$ también podemos escribirlo de la siguiente manera $x_n + (p^n) \to x_{n-1} + (p^{n-1})$ donde x_{n-1} es el resto que queda de dividir x_n entre (p^{n-1}), esto se llama representación p-ádica. A continuación, vamos a ver cuatro ejemplos de representaciones p-ádicas.

Ejemplo. (a) Escribamos 103 como entero 3-ádico, primero tenemos que encontrar la potencia de 3 inmediatamente inferior a 103. De esta manera, la potencia inmediatamente superior a la que hemos tomado será mayor que 103 y no necesitamos calcular el resto,

esto también ocurrirá para todas las potencias más mayores. Para la potencia inmediatamente inferior en nuestro caso $3^4 = 81$ calculamos el resto de 103 entre 81 que es 22, vamos desciendendo potencias si el resto que hemos calculado es mayor que la siguiente potencia más pequeña aplicamos el algoritmo de la división para calcular el resto y, en el caso que sea más pequeño se deja así. Luego nos queda de la siguiente forma:
$\mathbf{103} = (\ldots, 103 + (3^6), 103 + (3^5), 22 + (3^4), 22 + (3^3), 4 + (3^2), 1 + (3))$.

(b) Escribamos p en $\mathbb{Z}_p$ que será $\mathbf{p} = (\ldots, p + (p^6), p + (p^5), p + (p^4), p + (p^3), p + (p^2), 0)$.

(b) Escribamos 1 en $\mathbb{Z}_p$ que será $\mathbf{1} = (\ldots, 1 + (p^6), 1 + (p^5), 1 + (p^4), 1 + (p^3), 1 + (p^2), 1 + (p))$

(b) Escribamos 0 en $\mathbb{Z}_p$ que será $\mathbf{0} = (\ldots, 0 + (p^6), 0 + (p^5), 0 + (p^4), 0 + (p^3), 0 + (p^2), 0)$

Proposición 3.0.2. Sea $\mathbf{x} \in \mathbb{Z}_p$ la aplicación que lleva $\mathbf{x} \to p\mathbf{x}$ multiplicar por p coordenada a coordenada es un homomorfismo inyectivo del grupo aditivo.

Demostración. Como podemos poner p como entero p-ádico y la multiplicacion es coordenada a coordenada, vemos que $p(\mathbf{x} + \mathbf{y}) = p\mathbf{x} + p\mathbf{y}$ por lo tanto homomorfismo. Podemos usar la notación de p-ádico como la de entero indistintamente porque la multiplicación es coordenada a coordenada. Veamos que es inyectiva, sea $\mathbf{x} \in \mathbb{Z}_p$ tal que $p\mathbf{x} = 0$, y veamos que $\mathbf{x} = \mathbf{0}$; es decir, que $\bar{x}_n = 0\ \forall n$.
Sabemos que $0 = p\bar{x}_{n+1} = px_{n+1} + (p^{n+1})$, es decir, $p^n | x_{n+1}$, así que $\bar{x}_n = \phi_{n+1}(\bar{x}_{n+1}) = x_{n+1} + (p^n) = 0$ y como era un n cualquiera por lo tanto son todos 0. □

Veamos como son las unidades de $\mathbb{Z}_p$.

Proposición 3.0.3. $\mathbf{x} \in \mathbb{Z}_p$ no es unidad $\Leftrightarrow \exists \mathbf{y} \in \mathbb{Z}_p$ tal que $\mathbf{x} = p\mathbf{y}$.

Demostración. ($\Leftarrow$) Inmediato porque si $\mathbf{x} = p\mathbf{y}$ tiene por lo menos un cero ya que $\bar{x}_1 = p\bar{y}_1$ y $\bar{x}_1 = py_1 + (p) = 0$ es múltiplo de p y entonces no puede ser unidad.
($\Rightarrow$)Las unidades de A_n son los elementos coprimos con p, luego si $\bar{x}_n \in A_n$ no es una unidad, entonces $\exists \bar{y}_n \in A_n$ tal que $\bar{x}_n = p\bar{y}_n$. Si esto ocurre para un n se cumple para los siguientes. Para un $n+1$ se tiene $\bar{x}_{n+1} = x_{n+1} + (p^{n+1})$ tal que $\phi_n(\bar{x}_{n+1}) = x_{n+1} + (p^n) = py_n + (p^n)$ y $x_{n+1} - py_n$ es múltiplo de p^n luego x_{n+1} es múltiplo de p y por inducción lo tenemos para cualquier m, entonces $\mathbf{x} = p\mathbf{y}$. □

Veamos que es un dominio de integridad, es decir, que no hay divisores de cero.

Proposición 3.0.4. Si U denota el grupo de elementos invertibles de $\mathbb{Z}_p$ todo elemento no nulo de $\mathbb{Z}_p$ puede escribirse de manera única de la forma $p^n\mathbf{u}$ donde $\mathbf{u} \in U$ (Un elemento de U se llama unidad p-ádica) y $n \geq 0$.

Demostración. Por lo visto en 1.8.1 para que $\mathbb{Z}_p$ tenga una unidad es suficiente tenerla en $\prod_{n\geq 1} A_n$.
Tenemos dos casos que ya sea una unidad y en ese caso $n = 0$ o que no. Sea $\mathbf{x} \notin U$ y $\mathbf{x} \neq 0$, entonces, existe un n lo más grande posible tal que $\varepsilon_n(\mathbf{x}) = \bar{x}_n = 0$ y $\varepsilon_{n+1}(\mathbf{x}) = \bar{x}_{n+1} \neq 0$ es decir, $\bar{x}_n$ es múltiplo de p^n y todos los demás también lo serán, luego $\mathbf{x} = p^n\mathbf{u}$ donde $\mathbf{u}$ no es divisible por p luego es una unidad. □

Como para todo elemento no nulo $\mathbf{x} \in \mathbb{Z}_p$ $\mathbf{x} = p^n\mathbf{u}$, si tomase otro elemento de $\mathbb{Z}_p$ y lo multiplicase no podría ser 0 porque la multiplicación de dos unidades no puede ser 0.

Observación. Si I es un ideal propio de en $\mathbb{Z}_p$ contiene elementos de la forma $p^n u$ para algún $n \in \mathbb{N}$. Sea $n \in \mathbb{N}$ lo más pequeño posible tal que existe $p^n u \in I$, entonces, $p^n \in I$ y si $y \in I$ $y = p^m u$ se tendrá que $m \geq n$, luego $y \in (p^n)$ y se tiene la igualdad. Luego los ideales de $\mathbb{Z}_p$ son de la forma (p^n) y por lo tanto todos los ideales son principales y $\mathbb{Z}_p$ es un dominio de ideales principales. Además, para cualquier $n \in \mathbb{N}$ $(p^n) \subseteq (p)$ luego este es el único ideal maximal y $\mathbb{Z}_p$ es un anillo local.

Esta proposición motiva la siguiente definición.

Definición. Sea x un elemento no nulo de $\mathbb{Z}_p$, escribimos x en la forma $p^n u$ donde $u \in U$. El entero n se llama valoración p-ádica de x y se denota como $v_p(x)$, es decir, cual es la primera posición que es 0 en la secuencia Extendemos la definición al cero $v_p(0) = +\infty$ y tenemos las siguientes propiedades

$$v_p(xy) = v_p(x) + v_p(y)$$
$$v_p(x+y) \geq inf(v_p(x), v_p(y))$$

Definición. El cuerpo de números p-ádicos, se denota por $\mathbb{Q}_p$, es el cuerpo de fracciones del anillo $\mathbb{Z}_p$, es decir, el cuerpo más pequeño que contiene al dominio de integridad $\mathbb{Z}_p$.
Ahora nos encontramos en el mejor caso posible, tenemos conmutatividad, asociatividad, elementos neutros y todos los elementos tienen inverso para la suma y la multiplicación y distribución respecto de la suma.

Todo elemento $x \in \mathbb{Q}_p^*$ puede ser escrito de forma única como $p^n u$ donde $n \in \mathbb{Z}$ y $u \in U$ y $n \in \mathbb{Z}$ que es una evaluación p-ádica. Por lo tanto $v_p(x) \geq 0$ si y solo si $x \in \mathbb{Z}_p$.

Capítulo 4

El grupo multiplicativo $\mathbb{Q}_p$ y Ecuaciones p-ádicas

4.1. Grupo multiplicativo de $\mathbb{Q}_p$

$\varepsilon_n : U \to U(A_n)$ es un homomorfismo suprayectivo de grupos multiplicativos. Si llamamos U_n al núcleo del homomorfismo, es decir, es de la forma $U_n = 1 + p^n\mathbb{Z}_p$, se tiene que $U/U_n \simeq U(A_n)$ luego para todo n, $|U/U_n| = p^{n-1}(p-1)$ ver 1.7.1. En particular

$$|U/U_1| = (p-1)$$

Para cada n se tiene que U_1/U_n es un subgrupo de U/U_n luego es finito y aplicando 1.5 $|\frac{U/U_n}{U_1/U_n}| = |U/U_1| = p-1$ luego $\frac{p^{n-1}(p-1)}{|U_1/U_n|} = p-1$ y se tiene que $|U_1/U_n| = p^{n-1}$.

Observación. En U_1 no hay elementos distintos de 1 de orden divisor de $p-1$. Supongamos que existe $1 \neq x \in U_1$ de orden divisor de $p-1$. Por ser distinto de 1, existe n tal que $x \notin U_n$ y el orden de xU_n en U_1/U_n es a la vez divisor de $p-1$ y potencia de p, luego no puede ser.

Proposición 4.0.1. $U = V \times U_1$ donde $V = \{x \in U \mid x^{p-1} = 1\}$ es el único subgrupo de U isomorfo a F_p^*

Demostración. Para cada n, como $U(A_n)$ tiene orden $p^{n-1}(p-1)$ por la proposición 1.1.(a) hay un único subgrupo V_n de orden $p-1$ y que contiene a todos los elementos de orden divisor de $p-1$.
Las correspondientes restricciones de ϕ_n son homorfismos $V_n \to V_{n-1}$ suprayectivos . El límite proyectivo es un subgrupo V de U cuyos elementos tienen orden divisor de $p-1$ y tiene al menos $p-1$ elementos.
Por la observación anterior $V \cap U_1 = 1$ y se tiene por 1.4 que

$$V \simeq \frac{U_1 \times V}{U_1} \leq U/U_1 \tag{4.1}$$

y por los órdenes se tiene la igualdad $U = U_1 \times V$. □

Corolario 4.0.1. El cuerpo $\mathbb{Q}_p$ contiene a las $(p-1)$ raices de la unidad.

Observación. El grupo V se llama el el grupo multiplicativo de representantes de los elementos de F_p^*.

Lema 4.1. Sea $x \in U_n - U_{n+1}$ donde $n \geq 1$ si $p \neq 2$ y $n \geq 2$ si $p = 2$ entonces $x^p \in U_{n+1} - U_{n+2}$.

Demostración. Por hipótesis $x = 1 + kp^n$ con $k \not\equiv 0 \pmod{p}$ y por el binomio de Newton será $x^p = 1 + kp^{n+1} + \ldots k^p p^{np}$ y sus exponentes en los términos que nos hemos escrito son $\geq 2n+1$, por lo tanto también $\geq n+2$. Además, $np \geq n+2$, ya que $n \geq 2$ si $p = 2$. Esto nos muestra que $x^p \equiv 1 + kp^{n+1} \pmod{p^{n+2}}$ por lo tanto $x^p \in U_{n+1} - U_{n+2}$.

□

Proposición 4.0.2.

(a) Si $p \neq 2$, entonces U_1 es isomorfo a $\mathbb{Z}_p$.

(b) Si $p = 2$, $U_1 = \{\pm 1\} \times U_2$ y U_2 es isomorfo a $\mathbb{Z}_2$.

Demostración. Consideramos primero el caso $p \neq 2$. Elegimos un elemento $\alpha \in U_1 - U_2$, tomamos $\alpha = 1 + p$. Por el lema 4.1, tenemos que $\alpha^p \in U_2 - U_3$, luego elevando sucesivamente a p tenemos que $\alpha^{p^i} \in U_{i+1} - U_{i+2}$.
Queremos ver que U_1/U_n es un grupo cíclico, ya sabemos que su orden es p^{n-1}, sea α_n la imagen de α en U_1/U_n, es decir, $\alpha_n = \alpha U_n$, entonces, $(\alpha_n)^{p^{n-2}} \in U_{n-1} - U_n$ y $(\alpha_n)^{p^{n-1}} \in U_n - U_{n+1}$, luego $(\alpha_n)^{p^{n-2}} \neq 1$ en U_1/U_n y $(\alpha_n)^{p^{n-1}} = 1$ en U_1/U_n. Luego U_1/U_n es cíclico y generado por α_n Ahora denotamos por $\theta_{n,\alpha}$ el isomorfismo $z \to \alpha_n^z$ de $\mathbb{Z}/p^{n-1}\mathbb{Z}$ en U_1/U_n como U_1/U_n es cíclico la isomorfía es inmediata . El siguiente diagrama es conmutativo, donde ψ_n es multiplicar por p.

$$\begin{array}{ccc} (\mathbb{Z}/p^n\mathbb{Z}, +) & \xrightarrow{\theta_{n+1,\alpha}} & U_1/U_{n+1} \\ \downarrow \phi_n & & \downarrow \psi_n \\ (\mathbb{Z}/p^{n-1}\mathbb{Z}, +) & \xrightarrow[\theta_{n,\alpha}]{} & U_1/U_n \end{array}$$

De este modo tomando el subconjunto del anillo de producto directo $\prod_{n\geq 1} A_n$ tal que si $\bar{x}_n \in A_n$, entonces $\phi_n(\bar{x}_n) = (\bar{x}_{n-1}$, que sabemos que dicho conjunto es $\mathbb{Z}_p$. Por otro lado, tomando el subconjunto del grupo producto $\prod_{n\geq 1} U_1/U_n$ tal que si $x \in U_1/U_n$ entonces $\psi_n(x) = \theta_{n-1,\alpha}(x) \in U_1/U_{n-1}$, este subconjunto será subgrupo y sera U_1, luego los $\theta_{n,\alpha}$ define un isomorfismo θ de $\mathbb{Z}_p$ en U_1 y tenemos probada la primera parte.
Suponemos ahora que $p = 2$, elegimos $\alpha \in U_2 - U_3$, esto es $\alpha \equiv 5 \pmod{8}$. Definimos los siguientes isomorfismos

$$\theta_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \to U_2/U_n$$

Por lo tanto el isomorfismo $\theta_\alpha : \mathbb{Z}_2 \to U_2$. Por otro lado, el homomorfismo $U_1 \to U_1/U_2 \equiv \mathbb{Z}/2\mathbb{Z}$ induce un isomorfismo de $\{\pm 1\}$ en $\mathbb{Z}/2\mathbb{Z}$ y de aquí obtenemos que $U_1 = \{\pm 1\} \times U_2$ □

Teorema 4.1. *El grupo $\mathbb{Q}_p^*$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ si $p \neq 2$. Si $p = 2$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.*

Demostración. Todo elemento de $\mathbb{Q}_p^*$ puede escribirse de forma única como $x = p^n u$ donde $n \in \mathbb{Z}$ y $u \in U$. Por lo tanto, $\mathbb{Q}_p^* \cong (\mathbb{Z}, +) \times U$, es más, por la proposición 4.0.1 prueba que $U = V \times U_1$, donde V es cíclica de orden $p-1$ y la estructura de U_1 nos la da la proposicion 4.0.2. □

4.2. Cuadrados en $\mathbb{Q}_p^*$

Teorema 4.2. *Suponemos $p \neq 2$ y $x = p^n u$ un elemento de $\mathbb{Q}_p^*$ donde $n \in \mathbb{Z}$ y $u \in U$. x es un cuadrado si y solo si esa n es par y la imagen de $\bar{u}$ de u en $F_p^* = U/U_1$ es un cuadrado.*

Demostración. Descomponemos u de la forma $u = vu_1$ donde $v \in V$ y $u_1 \in U_1$ juntando el teorema 4.1 y la proposición 4.0.1 tenemos que $\mathbb{Q}_p^* \cong Z \times V \times U_1$ y al elemento x le corresponde (n, v, u_1). x es un cuadrado si y solo si n es par y v y u_1 son cuadrados. pero U_1 es isomorfo a $(\mathbb{Z}_p, +)$ para saber si u_1 es cuadrado tenemos en cuenta que el isomorfismo transforma $u_1^2 \to 2a$ y 2 es invertible en $\mathbb{Z}_p$, entonces todos los elementos de U_1 son cuadrados. como V es isomorfo a F_p^* se sigue el teorema. □

Observación. La condición que dice que la imagen de $\bar{u}$ de u en $F_p^* = U/U_1$ es un cuadrado significa que $\left(\frac{\bar{u}}{p}\right) = 1$.
A partir de ahora nos referiremos a $\left(\frac{\bar{u}}{p}\right)$ también como $\left(\frac{u}{p}\right)$.

Corolario 4.2.1. Si $p \neq 2$ el grupo $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ es un grupo de tipo $(2,2)$ que tiene como representantes $\{1, p, u, pu\}$ donde $u \in U$ tal que $\left(\frac{u}{p}\right) = -1$.

Teorema 4.3. *$x = p^n u$ de $\mathbb{Q}_2^*$ es un cuadrado si y solo si n es par y $u \equiv 1 \pmod 8$.*

Demostración. La descomposición $U = \{\pm 1\} \times U_2$ nos dice que u es un cuadrado si y solo si $u \in U_2$ y es un cuadrado en U_2. Ahora el isomorfismo $\theta : \mathbb{Z}_2 \longmapsto U_2$ construido en la demostración de la proposición 4.0.2 lleva $2^n\mathbb{Z}_2$ a U_{n+2}. Tomando $n = 1$ vemos que el conjunto de cuadrados de U_2 es igual a U_3, por lo tanto un elemento $u \in U$ es un cuadrado si y solo si es congruente a 1 módulo 8. □

Corolario 4.3.1. El grupo $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ es un grupo de tipo $(2,2,2)$ que tiene como representantes $\{\pm 1, \pm 5, \pm 2, \pm 10\}$

Observación. Para $p = 2$ definimos $\varepsilon, \omega : U/U_3 \longmapsto \mathbb{Z}/2\mathbb{Z}$ esto nos lleva a las formulas

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

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

ε define un isomorfismo de U/U_2 en $\mathbb{Z}/2\mathbb{Z}$ y ω define un isomorfismo de U_2/U_3 en $\mathbb{Z}/2\mathbb{Z}$. Por lo tanto el par (ε, ω) forman un isomorfismo de U/U_3 en $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En particular una unidad 2-ádica es un cuadrado si y solo si $\varepsilon(z) = \omega(z) = 0$.

4.3. Ecuaciones p-ádicas

Vamos a introducir la siguiente notación.
Si $f \in \mathbb{Z}_p[X_1, ..., X_m]$ es un polinomio suyos coeficientes en $\mathbb{Z}_p$ y si n es un entero ≥ 1, denotamos como f_n el polinomio con coeficientes en A_n se deduce de f por reducción $\pmod{p^n}$.

Proposición 4.3.1. Sea $f^{(i)} \in \mathbb{Z}_p[X_1, ..., X_m]$ polinomios con coeficientes enteros p-ádicos. Los siguientes resultados son equivalentes:

(a) Los $f^{(i)}$ tiene un cero común en $(\mathbb{Z}_p)^m$.

(b) $\forall n > 1$ los polinomios $f_n^{(i)}$ tiene un cero común en $(A_n)^m$.

Demostración. La aplicación $\varepsilon_n : \mathbb{Z}_p \to A_n$. Sea $f \in \mathbb{Z}_p[x_1,\ldots,x_m]$ si $f(\mathbf{x_1},\ldots,\mathbf{x_m}) = 0$, entonces, $0 = \varepsilon_n(f(\mathbf{x_1},\ldots,\mathbf{x_m})) = \varepsilon_n(f)(\varepsilon_n(\mathbf{x_1}),\ldots,\varepsilon_n(\mathbf{x_m})) = f_n(\varepsilon_n(\mathbf{x_1}),\ldots,\varepsilon_n(\mathbf{x_m}))$. Luego, los f_n^i tienen un cero común en $(A_n)^m$.
Reciprocamente llamamos D_n el conjuntos de ceros comunes de $f_n^{(i)}$, $D_n \subset (A_n)^m$ $A_n[x_1,\ldots,x_m] \to A_{n-1}[x_1,\ldots,x_m]$ dado por $f_n \to \phi_n(f_n) = f_{n-1}$. Si $fn(\bar{x}_1,\ldots,\bar{x}_m) = 0$, entonces:
$f_{n-1} = \phi_n(f_n)(\phi_n(\bar{x}_1),\ldots,\phi_n(\bar{x}_m)) = 0$ luego $\phi_n : D_n \to D_{n-1}$ sea $d_n \in D_n$, $d_n = (d_n^1,\ldots,d_n^m)$. Tomamos el subanillo del producto directo de anillos $\prod_{i\geq 1} D_i$ donde $\phi_n(d_n) = d_{n-1} = (d_{n-1}^1,\ldots,d_{n-1}^m)$ y lo llamamos D que es el conjunto de ceros comunes en $(\mathbb{Z}_p)^m$. D es no vació porque los D_i son finitos. □

Definición. Un punto $x = (x_1,...,x_m)$ de $(\mathbb{Z}_p)^m$ se llama primitivo si uno de los x_i es invertible, es decir que no sea divisible por p. Uno define de manera similar los elementos primitivos de $(A_n)^m$.

Proposición 4.3.2. Sea $f^{(i)} \in \mathbb{Z}_p[X_1,...,X_m]$ polinomios homogéneos. Los siguientes resultados son equivalentes:

(a) Los $f^{(i)}$ tiene un cero común no trivial en $(\mathbb{Q}_p)^m$.

(b) Los $f^{(i)}$ tiene un cero común primitivo en $(\mathbb{Z}_p)^m$.

(c) $\forall n > 1$ los polinomios $f_n^{(i)}$ tiene un cero común primitivo en $(A_n)^m$.

Demostración. Notar que solo hay que probar la equivalencia de (a) y (b) porque la de (b) y (c) esta probada por la proposición anterior.
$(b) \Rightarrow (a)$ es trivial por la definición de primitivo.
$(a) \Rightarrow (b)$ si $x = (x_1,...,x_n)$ es un cero común de $f^{(i)}$, ponemos

$$h = inf(v_p(x_1),...,v_p(x_n)) \text{ y } y = p^{-h}x.$$

Esta claro que y es un elemento primitivo de $(\mathbb{Z}_p)^m$. □

Teorema 4.4 (Chevalley-Warning)**.** *Sea q una potencia de un primo p, y sean $f_i(x_1,\ldots,x_m) \in F_q[X_1,\ldots,X_m]$ polinomios cumpliendo que $\sum gr(f_i) < m$. Sea D el conjunto de ceros comunes de los f_i en F_q^m, entonces $|D| \equiv 0 \pmod{p}$.*

Demostración. Pongamos $P(x_1,...,x_m) = \prod(1 - f_i^{q-1})$. Notamos que $\forall a \in F_q^*$, $a^{q-1} = 1$, se tiene

$$P(x_1,\ldots,x_m) = \begin{cases} 0 \text{ si } (x_1,\ldots,x_m) \notin D \\ 1 \text{ si } (x_1,\ldots,x_m) \in D \end{cases}$$

es decir P es la función característica de D.
Pongamos para $h \in F_q[x_1,\ldots,x_l]$, $s(h) = \sum_{x\in F_q^l} h(x)$, como P es la función característica de D,entonces, $s(P)$ será la cantidad de elementos de F_q que hay en D, entonces, se tiene que $|D| = s(P)$, con lo que basta ver que $s(P) = 0$.
Ahora P es combinación lineal de monomios $x_1^{\alpha_1},\ldots,x_m^{\alpha_m}$ con $\alpha_1 + \cdots + \alpha_m \leq gr(P) \leq (\sum gr(f_i))(q-1) < m(q-1)$. Por lo tanto basta ver que $s(x_1^{\alpha_1},\ldots,x_m^{\alpha_m}) = 0$ si $\alpha_1 + \cdots + \alpha_m < m(q-1)$ luego basta ver que $s(x_1^{\alpha_1},\ldots,x_m^{\alpha_m}) = 0$ si $\alpha_i < q-1$ para algún i. Pero, $s(x_1^{\alpha_1},\ldots,x_m^{\alpha_m}) =$

$s(x_1^{\alpha_1}) \cdot \cdots \cdot (x_m^{\alpha_m})$ y basta ver que $s(x^l) = 0$ si $l < q-1$. Ahora, sea $H = \{x^l | x \in F_q^*\}$, H es subgrupo de F_q^* y $s(x^l) = \sum_{x \in H} x$. Por otro lado, como $l < q-1$, $H \neq 1$ luego $\exists y \in H$ distinto de 1 y $s(x^l) = \sum_{x \in H} x = \sum_{x \in H} yx = ys(x^l)$ luego $(1-y)s(x^l) = 0$ y como $(1-y) \neq 0$, entonces $s(x^l) = 0$. □

Notar que gracias a 4.3.2 el resultado es equivalente en $(\mathbb{Z}_p)^m$ y $(\mathbb{Q}_p)^m$.

Corolario 4.4.1. Sea f un polinomio con m variables en F_p, $\mathbb{Z}_p$ o $\mathbb{Q}_p$ si $gr(f) < m$ y f no tiene término constante entonces, $f(x_1, \ldots, x_m) = 0$ tiene al menos una solución no trivial para cada primo p.

Capítulo 5

Símbolo de Hilbert

En este capítulo nos vamos a referir como K tanto a $\mathbb{Q}_p$ como a $\mathbb{R}$.

5.1. Definición y primeras propiedades

Definición (símbolo de Hilbert)**.** Sea $a,b \in K^*$, entonces, $(a,b) = 1$ si $z^2 - ax^2 - by^2 = 0$ tiene una solución no trivial en K^3 en otro caso $(a,b) = -1$.
Al número $(a,b) = \pm 1$ se le llama símbolo de Hilbert de a y b relativo a K.
Esa claro que (a,b) no cambia cuando a y b son multiplicados por cuadrados. Por lo tanto el símbolo de Hilbert define una aplicación $K^*/K^{*2} \times K^*/K^{*2} \longmapsto \{\pm 1\}$

Proposición 5.0.1. Sea $a,b \in K^*$, β la raiz cuadrada de b y $K_b = K(\beta)$. $(a,b) = 1$ si y solo si a pertenece al grupo NK_b^* de norma de los elementos de K_b^*.

Demostración. Si b es un cuadrado de un elemento c, la ecuación $z^2 - ax^2 - by^2 = 0$ tiene $(c,0,1)$ como solución por lo tanto $(a,b) = 1$ y la proposición es clara en es sentido como $K_b = K$ y $NK_b^* = K^*$. Por otra parte, K_b es cuadrático sobre K, todo elemento $\xi \in K_b$ puede escribirse como $\xi = z + \beta y$ donde $y,z \in K$ y la norma $N(\xi)$ de ξ es igual a $z^2 - by^2$ ya que tendríamos los ismorfismos identidad y $\sigma(\beta) = -\beta$ y entonces $N(\xi) = (z+\beta y)(z-\beta y) = z^2 - by^2$. Si $a \in NK_b^*$, entonces $\exists y,z \in K$ tal que $a = z^2 - by^2$ por lo tanto la forma cuadrática $z^2 - ax^2 - by^2$ tiene un cero en $(z,1,y)$ y tenemos $(a,b) = 1$. Recíprocamente si $(a,b) = 1$, esta forma tiene un cero no trivial . $x \neq 0$ ya que de lo contrario b sería un cuadrado. De aquí obtenemos que a es la norma de $\frac{z}{x} + \frac{y}{x}$. □

Proposición 5.0.2. El símbolo de Hilbert satisface las siguientes propiedades:

(a) $(a,b) = (b,a)$ y $(a,c^2) = 1$.

(b) $(a,-a) = 1$ y $(a,1-a) = 1$.

(c) $(a,b) = 1$, entonces, $(aa',b) = (a',b)$.

(d) $(a,b) = (a,-ab) = (a,(1-a)b)$.

Demostración. (a) Cambiar los papeles de a y b no cambian que tenga solución no trivial. Si $b = c^2$ entonces tiene un cero en $(1,0,1/c)$.
(b) Si $b = -a$ entonces tiene un cero en $(0,1,1)$ y si $b = 1-a$ lo tiene en $(1,1,1)$, por lo tanto ambos símbolos de Hilbert son 1.

(c) Usamos 5.0.1 para probarlo. Sabemos que la norma del producto de dos elementos es el producto de sus normas luego $NK_{a'}(aa') = NK_{a'}(a)NK_{a'}(a')$, esto nos lleva a la siguiente ecuación

$$(a,a') = 1 \Leftrightarrow NK_{a'}(a)NK_{a'}(a') = 1 \Leftrightarrow NK_{a'}(a)NK_{a'}(a') = NK_{a'}(a')^{-1}$$

Esto nos dice que $(aa',b) = (a,b)(a',b)$ y si $(a,b) = 1$ entonces $(aa',b) = (a',b)$.
(d) Se sigue de las tres anteriores. □

Teorema 5.1.

(a) Si $K = \mathbb{R}$, tenemos que $(a,b) = 1$ si a o b es > 0 y $(a,b) = -1$ si $a,b < 0$

(b) Si $K = \mathbb{Q}_p$ y si escribimos $\begin{cases} a = p^\alpha u \\ b = p^\beta v \end{cases}$ *donde $u,v \in U$. Tenemos que:*

$$(a,b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \text{ si } p \neq 2$$

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

Para demostrar este teorema tendremos que introducir antes una serie de resultados que nos ayudaran en la demostración.

Teorema 5.2. *El símbolo de Hilbert es una forma bilineal no degenerada en el F_2-ev K^*/K^{*2}.*

Demostración. Notar que la bilinealidad viene de que $(aa',b) = (a',b)(a,b)$ y que $(a+b,c) = (a,c)+(b,c)$ esto se sigue de que la suma de las ecuaciones $z^2 - ax^2 - by^2 = 0$ y $(z')^2 - a(x')^2 - b(y')^2 = 0$ tiene solución notrivial si las originales la tenían, el que sea no degenerada quiere decir que si $b \in K^*$ tal que $(a,b) = 1\ \forall a \in K^*$ uno tiene $b \in K^{*2}$. □

Corolario 5.2.1. Si b no es un cuadrado, el grupo NK_b^* definido en la proposición 5.0.1 es un subgrupo de índice 2 en K^* .

Demostración. El homomorfismo $\phi_b : K^* \longmapsto \{\pm 1\}$ definido por $\phi_b(a) = (a,b)$ tiene como núcleo NK_b^* por la proposición 5.0.1. Es más ϕ_b es suprayectiva porque (a,b) es no degenerada. Por lo tanto por el primer teorema de isomorfía ϕ_b define un isomorfismo $K^*/NK_b^* \longmapsto \{\pm 1\}$. □

Lema 5.1. Sea $v \in U$. Si la ecuación $z^2 - ax^2 - by^2 = 0$ tiene solución no trivial en $\mathbb{Q}_p$, entonces tiene una solución (z,x,y) tal que $z,y \in U$ y $x \in \mathbb{Z}_p$.

Demostración. Por la proposición 4.3.2 la ecuación dada tiene una solución primitiva (z,x,y). Veamos que esra solución tiene la propiedad deseada.
Reduccion al absurdo: Suponemos que no tiene dicha propiedad, entonces tendríamos $y \equiv 0 \pmod p$ o $z \equiv 0 \pmod p$, como $z^2 - vy^2 \equiv 0 \pmod p$ y $v \not\equiv 0 \pmod p$, tendremos tanto $y \equiv 0 \pmod p$ y $z \equiv 0 \pmod p$. Por lo tanto, $px^2 \equiv 0 \pmod{p^2}$ que significa que $x \equiv 0 \pmod p$ que es contrario al carácter primitivo de (z,x,y). □

Demostración Teorema 5.1. El caso $K = \mathbb{R}$ es trivial. Notar que K^*/K^{*2} es un campo vectorial de dimensión 1 sobre el cuerpo F_2 con $\{\pm 1\}$ como representantes.
Primero suponemos que $p \neq 2$. Esta claro que los exponentes α y β vienen solo por su residuo módulo 2, luego $\alpha,\beta \in \{0,1\}$; Por la simetría del símbolo de Hilbert, solo hay tres casos que considerar:

1) $\alpha = 0, \beta = 0$. Debemos comprobar que $(u,v) = 1$. Ahora la ecuación:

$$z^2 - ux^2 - vy^2 = 0$$

Tiene solución no trivial módulo p por 4.4.1. Por lo tanto $(u,v) = 1$.

2) $\alpha = 1, \beta = 0$. Debemos comprobar que $(pu,v) = \left(\frac{v}{p}\right)$. Como $(u,v) = 1$ tenemos por la propiedad (c) que $(pu,v) = (p,v)$, esto es suficiente para comprobar que $(p,v) = \left(\frac{v}{p}\right)$ ya que si v es un cuadrado, los dos términos iguales a 1.
En caso contrario $\left(\frac{v}{p}\right) = -1$. Por lo tanto por el lema 5.1 $z^2 - ux^2 - vy^2 = 0$ no tiene solución no trivial,entonces, $(p,v) = -1$.

3) $\alpha = 1, \beta = 1$. Debemos comprobar que $(pu,pv) = (-1)^{(p-1)/2}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. En base a las propiedades (a) y (c) del símbolo de Hilbert:

$$(pu,pv) = (pu,-pu)(pu,pv) = (pu,-p^2uv) = (pu,-p^2)(pu,pv) = (pu,-uv)$$

Por lo que acabamosde ver que $(pu,pv) = \left(\frac{-uv}{p}\right)$, por lo que el resultado se sigue ya que $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Ahora suponemos que $p = 2$, por lo mismo expuesto anteriormente solo hay tres casos:

1) $\alpha = 0, \beta = 0$. Debemos comprobar que $(u,v) = 1$ si u o v es congruente a 1 módulo 4 y $(u,v) = -1$ en otro caso. Suponemos primero que $u \equiv 1 \pmod 4$.
Entonces $u \equiv 1 \pmod 8$ o $u \equiv 5 \pmod 8$. En el primer caso u es un cuadrado por el teorema 4.3 y por lo tanto tenemos que $(u,v) = 1$. En el segundo caso tenemos que $u + 4v \equiv 1 \pmod 8$ por lo tanto $\exists w \in U$ tal que $w^2 = u + 4v$, la forma $z^2 - ux^2 - vy^2$ tiene por lo tanto $(w,1,2)$ es un cero y tenemos que $(u,v) = 1$.
Supongamos ahora que $u \equiv v \equiv -1 \pmod 4$; si (z,x,y) es una solución primitiva de $z^2 - ux^2 - vy^2 =$, entonces $z^2 + x^2 + y^2 \equiv 0 \pmod 4$; pero los cuadrados $\mathbb{Z}/4\mathbb{Z}$ son 0 y 1, esta congruencia implica sque $x,y,z \equiv 0 \pmod 2$, lo que contradice la hipótesis de primitividad. Por lo tanto, $(u,v) = -1$.

2) $\alpha = 1, \beta = 0$. Debemos comprobar que $(2u,v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$. Primero veamos que $(2,v) = (-1)^{\omega(v)}$, es decir, que $(2,v) = 1$ es equivalente a $v \equiv \pm 1 \pmod 8$. Por el lema 5.1 si $(2,v) = 1$, entonces $\exists x,y,z \in \mathbb{Z}_2$ tal que $z^2 - 2x^2 - vy^2 = 0$ y $y,z \not\equiv 0 \pmod 8$. Pero los únicos cuadrados módulo 8 son $0,1$ y 4. De aquí obtenemos que $v \equiv \pm 1 \pmod 8$. En cambio, si $v \equiv 1 \pmod 8$, v es u cuadrado y $(2,v) = 1$; si $v \equiv -1 \pmod 8$, la ecuación $z^2 - 2x^2 - vy^2 = 0$ tiene $(1,1,1)$ es una solución módulo 8 y por el teorema chino de los restos 1.7 y por la proposición 4.3.2 tiene también solución en $\mathbb{Q}_p^3$. Por lo tanto, tenemos que $(2,v) = 1$.
Ahora veremos que $(2u,v) = (2,v)(u,v)$, por las propiedades del símbolo de Hilbert, esto es cierto si $(2,v) = 1$ o $(u,v) = 1$. El caso que queda es $(2,v) = (u,v) = -1$, esto quiere decir que, $v \equiv 3 \pmod 8$ y $u \equiv 3$ o $-1 \pmod 8$; despues de multiplicar u y v por cuadrados, podemos suponer que $u = -1$, $v = 3$ o $u = 3$,$v = -5$; ahora las ecuaciones

$$z^2 + 2x^2 - 3y^2 = 0 \text{ y } z^2 - 6x^2 + 5y^2 = 0$$

tienen por solución $(1,1,1)$, por lo tanto tenemos que $(2u,v) = 1$

3) $\alpha = 1, \beta = 1$. Debemos comprobar que $(2u,2v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)}$. Por las propiedades (a) y (b) del símbolo de Hilbert y su binealidad tenemos:

$$(2u,2v) = (2u,2v)(2u,-2u) = (2u,-4uv) = (2u,-uv)(2u,4) = (2u,-uv)$$

pero acabamos de ver que $(2u,2v) = (-1)^{\varepsilon(u)\varepsilon(-uv)+\omega(-uv)}$ ya que $\varepsilon(-1) = 1$, $\omega(-1) = 0$ y $\varepsilon(u)(1+\varepsilon(u)) = 0$, el exponente $\varepsilon(u)\varepsilon(-uv)+\omega(-uv) = \varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)$. Lo que prueba el teorema. La bilinealidad de (a,b) se sigue de la fórmula dada por este símbolo, ya que ε y ω son homomorfismos. Que sea no degenerado se comprueba por los representantes $\{u,2u\}$ donde $u = 1,5,-1$. De hecho, tenemos que $(5,2u) = -1$ y $(-1,-1) = (-1,-5) = -1$.

□

5.2. Propiedades globales

El cuerpo $\mathbb{Q}$ es el cuerpo primo, intersección de todos los subcuerpos, de cada subcuerpo en cada uno de los cuerpos $\mathbb{Q}_p$ y $\mathbb{R}$. Si $a,b \in \mathbb{Q}^*$, $(a,b)_p$(respectivamente $(a,b)_\infty$) denota lo símbolos de Hilbert de sus imágenes en $\mathbb{Q}_p$ (respectivamente $\mathbb{R}$). Definimos V como el conjunto de primos junto con el símbolo ∞ y tomamos la convención de que $\mathbb{Q}_\infty = \mathbb{R}$.

Teorema 5.3 (Ley de reciprocidad de Hilbert)**.** *Si $a,b \in \mathbb{Q}^*$, tenemos que $(a,b)_p = 1$ para casi todos $v \in V$ y*

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

Demostración. Ya que los símbolos de Hilbert son bilineales, es suficiente para probar el teorema que cuando a o b son iguales a -1 o a un numero primo. En cada caso, el teorema 5.1 nos da el valor de $(a,b)_v$.

1) $a = -1$, $b = -1$. $(-1,-1)_\infty = (-1,-1)_2 = -1$ y $(-1,-1)_p = 1$ si $p \neq 2,\infty$. Luego, el producto es igual a 1.

2) $a = -1$, $b = l$ donde l es primo. Si $l = 2$ entonces $(-1,2)_v = 1\ \forall v \in V$.
Si $l \neq 2$ entonces $(-1,l)_v = 1$ si $v \neq 2,l$ y $(-1,l)_2 = (-1,l)_l = (-1)^{\varepsilon(l)}$. El producto es igual a 1.

3) $a = l$, $b = l'$ donde l y l' son primos, Si $l = l'$ entonces por las propiedades del símbolo de Hilbert tenemos que $(l,l)_v = (-1,l)_v\ \forall v \in V$ y estamos en el caso ya estudiado.
Si $l \neq l'$ y si $l' = 2$, uno tiene que $(l,2)_v = 1$ para $v \neq 2,l$ y

$$(l,2)_2 = (-1)^{\omega(l)},\ (l,2)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)} \text{ Por el teorema 2.2}$$

Si $l \neq l' \neq 2$, entonces, $(l,l')_v = 1$ para $v \neq 2,l,l'$ y

$$(l,l')_2 = (-1)^{\varepsilon(l)\varepsilon(l')},\ (l,l')_l = \left(\frac{l'}{l}\right) \text{ y } (l,l')'_l = \left(\frac{l}{l'}\right) \text{ Por el teorema } \textbf{??}\text{(Gauss)}$$

Entonces $\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right) = (-1)^{\varepsilon(l)\varepsilon(l')}$. Por lo tanto, el producto es igual a 1.

□

Observación. El interés de esta ley de reciprocidad cuadrática viene del hecho de que lo extiende a todos los cuerpos de números algebraicos.

Teorema 5.4. *Los siguientes resultados son equivalentes*

(a) Para enteros, coprimos e impares $a,b>0$, tenemos que:

$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right)(-1)^{(a-1)(b-1)/4}$$

(b) Para enteros impares $a,a',b,b'>0$, tenemos que:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=\left(\frac{a'}{b'}\right)\left(\frac{b'}{a'}\right)$$

Cuando $a\equiv a'\pmod 4$, $b\equiv b'\pmod 4$ y $(a,b)=(a',b')=1$

(c) $\forall a,b\in\mathbb{Q}^*$, tenemos que:

$$\prod_p (a,b)_p=1$$

Demostración.

$(a)\Rightarrow(b)$ Es claro ya que $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{(a-1)(b-1)/4}$ y el segundo miembro depende de que a sea módulo 4 y b sea módulo 4.

$(b)\Rightarrow(a)$ Si $a\equiv 1\pmod 4$, entonces nos dice que $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=\left(\frac{1}{b}\right)\left(\frac{b}{1}\right)=1$ si $a\equiv b\equiv 3\pmod 4$, entonces, $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=\left(\frac{3}{7}\right)\left(\frac{7}{3}\right)=-1$.

$(a)\Leftrightarrow(c)$ Ya lo hemos probado en la ley de Reciprocidad de Hilbert.

□

Observación. El segundo resultado se llama ley de reciprocidad de Eisenstein.

Hay mas leyes de reciprocidad cuadráticas como la de Artin que se generaliza en la llamada teoría de cuerpos de clases. Por ejemplo el noveno problema de Hilbert que solicita encontrar la ley de reciprocidad más general para los residuos de la norma del k-ésimo orden en un cuerpo de números algebraicos general, donde k es una potencia prima. Para saber más ver [4] [6].

Bibliografía

[1] J.P. SERRE, *A course in arithmethic (New York Springer-Verlag 1973)*

[2] FRANZ LEMMERMEYER, *Reciprocity laws from euler to Eisenstein (Springer-Verlag Berlin Heidelberg 2000)*

[3] IAN STEWART Y DAVID TALL, *Algebraic number theory and Fermat's last theorem (CRC Press 2016)*

[4] SERGE LANG, *Algebra (Springer-Verlag New York, Inc 2002)*

[5] JARED WEINSTEIN, *Reciprocity laws and Galois representations: recent breakthrougs (Bull Amer Math. Soc, New series, 53, 2016. 1-39)*

[6] I.R. SHAFAREVICH, *Ley de reciprocidad general y sus aplicaciones en la teoría de campos numéricos algebraicos (Tr. I Congr. Matemáticos húngaros edición, Budapest, 1952. 291-298)*