

República Dominicana
UNIVERSIDAD TECNOLÓGICA DEL CIBAO ORIENTAL
Universidad Patrimonio de la Comunidad



Facultad de Postgrado y Educación Continuada
Escuela de Postgrado

Trabajo de Postgrado para Optar por el Título de
Maestría en Matemática.

Título

Análisis del teorema de Hasse-Minkowski aplicado a ecuaciones

Sustentante

Julissa Díaz Hernández

Asesor

MA. Danny Daniel Manzueta Pérez

Cotuí, Provincia Sánchez Ramírez

Año académico, 2023.

Título

Análisis del teorema de Hasse-Minkowski aplicado a ecuaciones

Declaración de Autoría

Declaro que el presente trabajo de investigación, titulado Análisis del teorema de Hasse-Minkowski aplicado a ecuaciones, es el resultado de mi propio esfuerzo intelectual. Todas las fuentes utilizadas han sido debidamente citadas y referenciadas. Atestiguo que este trabajo no ha sido presentado anteriormente como requisito para la obtención de ningún otro título o grado académico. Asimismo, confirmo que todas las contribuciones de otros investigadores o autores han sido adecuadamente reconocidas y acreditadas. Asumo la responsabilidad total por el contenido y los resultados presentados en este trabajo.

Título

Análisis del teorema de Hasse-Minkowski aplicado a ecuaciones

Tesis presentada por **Julissa Díaz Hernández** para la obtención del grado de
Magister en Matemáticas.

Composición del tribunal evaluador

Jurado de metodología

Jurado de contenidos

Jurado de redacción

Lic. Yuderka Reyes

Directora de postgrado

CALIFICACIÓN FINAL:_____

Índice general

Declaración de autoría	III
Agradecimientos	VI
Dedicatorias	VII
Resumen	VIII
CAPÍTULO I: INTRODUCCIÓN	1
1.1. Antecedentes	1
1.1.1. Antecedentes históricos	1
1.1.2. Antecedentes académicos	2
1.2. Planteamiento del problema	3
1.3. Justificación	4
1.4. Objetivos	4
1.4.1. Objetivo general	4
1.4.2. Objetivos específicos	4
1.5. Alcances y límites	5
CAPÍTULO II: MARCO REFERENCIAL	6
2.1. Los números p -ádicos	6
2.1.1. La valuación, la norma p -ádica y la métrica p -ádica	6
2.2. Grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$	9
2.3. Formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$	10
2.3.1. Módulos cuadráticos	10
2.4. Teorema de Hasse-Minkowski a la solución de la ecuación p -ádica. . .	12
CAPÍTULO III: METODOLOGÍA	13
3.1. Método de investigación	13
3.2. Diseño de investigación	13
3.3. Tipo de investigación	13
3.4. Enfoque de investigación	13

3.5. Procedimiento de investigación	14
CAPÍTULO IV: PRESENTACIÓN DE LOS RESULTADOS	15
4.1. Solución racional mediante valuación, norma y métrica en una ecuación p-ádica	15
4.2. Grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$	17
4.3. Propiedades de los módulos cuadráticos para caracterizar las formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$	20
4.4. Teorema de Hasse-Minkowski a la solución de la ecuación p-ádica . .	22
CAPÍTULO V: CONCLUSIONES	26
5.1. Conclusiones	26
5.2. Lineas futuras de investigación	27
Referencias	28

Agradecimientos

A Dios: por haberme dado la vida y permitirme llegar a donde estoy, aportar la energía en mi cuerpo para poder soportar cada uno de esos viajes a la universidad, por poner la capacidad en mi cerebro de entender cada contenido impartido, por permitir que mi padres fueran el soporte tanto económicamente como emocional, por convencerme de que si yo podía llevar a cabo la meta propuesta ¡gracias mi Dios!

En especial a la UTECO, por brindarme la oportunidad de adquirir los conocimientos necesarios para poder culminar con gran éxito esta maestría y por ser el lugar donde me ayudaron a crecer en el ámbito humano e intelectual.

Al asesor Danny Manzueta: por estar al pendiente del desarrollo de esta investigación y bien corregir cada uno de los capítulos realizados.

Así mismo le agradezco a los profesores, por dejarme formar parte de sus enseñanzas ya que si no hubiese sido por sus grandes conocimientos y valores no estuviera alcanzando una de mis metas.

Dedicatorias

A mis padres: que fueron los pioneros para que esta meta fuera realizada, por estar ahí para entenderme , ayudarme , esperarme despierto, por estar siempre pendiente de mi motivándome , apoyándome , teniendo en cuenta las medicinas para mantener tanto mi cuerpo como mi salud mental, por enseñarme los valores y principios religiosos, por haberme dado esa buena crianza y yo hoy poder decir que escale otro peldaño profesionalmente gracias a ustedes , aunque tu mami ya no esté en esta tierra pero donde estés gracias por ser la buena madre que fuiste y darme esos buenos consejos que hoy han permitido que yo sea la persona que tu quería fuera.

A mis hermanos: por convencerme de que debía pensar en prepararme profesionalmente antes que cualquier otra cosa, por motivarme y hacerme ver que la vida es más fácil cuando estamos preparados , por bien aconsejarme y siempre querer lo mejor para mí , por hacerme sentir importante y confiar en que yo podía lograr cada objetivo propuesto.

A mi esposo: por estar pendiente de todo lo que necesitaba para alcanzar esta meta, por apoyarme y motivarme cuando más cansada me sentía.

A mis sobrinas: Natalia Gonzales y Rosmeri Rodríguez: por estar ahí cuando más necesitaba de alguien que me ayudara en la realización de algunas tareas, por apoyarme cuando más cansada me sentía. A mis compañeros de estudio: por hacer los días más llevaderos y hacer de ese espacio un lugar de alegría y un poco divertido, por ayudarnos mutuamente y ser buenos compañeros.

A mis amigas: Rosa María Adames, Candy María Rosario, Marileida Bautista, Sorivel veras, Lucia Bautista y Anyelina Suarez, por explicarme cada uno de los contenidos que no entendía y motivarme a continuar estudiando.

República Dominicana

UNIVERSIDAD TECNOLÓGICA DEL CIBAO ORIENTAL
(UTECO)

Facultad de Postgrado y Educación Continuada



MAESTRÍA EN MATEMÁTICA

Análisis del teorema de Hasse-Minkowski aplicado a ecuaciones

Julissa Díaz Hernández

Sustentante

MA. Danny Manzueta

Asesor

RESUMEN

El teorema de Hasse-Minkowski es un resultado importante en la teoría de ecuaciones que establece una condición necesaria y suficiente para la existencia de soluciones racionales en una variedad algebraica definida sobre un cuerpo global. En esta investigación se analiza el teorema de Hasse-Minkowski y su aplicación a ecuaciones, así como las diferentes generalizaciones y extensiones que existen.

Los objetivos de este estudio son: Identificar si una ecuación p -ádica tiene solución racional mediante valuación, norma y métrica. Caracterizar los grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$. Usar las propiedades de los módulos cuadráticos para caracterizar las formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$. Y, Describir los resultado de aplicar el teorema de Hasse-Minkowski a la solución de la ecuación p -ádica.

CAPÍTULO I

INTRODUCCIÓN

En este capítulo se abordan: Antecedentes, planteamiento del problema, así como también la justificación, objetivos y el alcance y límites del estudio, además, se presentarán los resultados existentes del teorema de Hasse-Minkowski y las posibles consecuencias de dicho teorema.

1.1. Antecedentes

1.1.1. Antecedentes históricos

Hay varias formas de abordar el estudio de los números p -ádicos. Una es la forma original, estudiándolos como series de Laurent. Esta es la más antigua, ya que fue así como nacieron estos números. Otra manera de estudiarlos es usando la teoría de valores absolutos. Por último, también pueden ser estudiados mediante el uso de límites proyectivos. Cada una de ellas tendrá ventajas y desventajas.

El matemático Hermann Minkowski (1864-1909) nació un 22 de junio. De gran talento matemático, con sólo 19 años obtuvo el Grand prix de l'Académie des sciences de Paris por una memoria sobre el número de maneras de escribir un entero como suma de cinco cuadrados.

Trabajó con David Hilbert en teoría de números. Se interesó por la física, desarrollando la idea de un espacio-tiempo de dimensión cuatro, que funda las bases matemáticas de la relatividad.

El matemático Helmut Hasse (1898-1979) nació un 25 de agosto. Trabajó en teoría algebraica de números: sus principales contribuciones fueron en teoría de cuerpos de clases, en la aplicación de los números p -ádicos a la teoría de cuerpos de clases locales y geometría diofántica-existe el llamado principio de Hasse-, y en el estudio de las funciones zeta locales.

En 1910, Ernst Steinitz publicó su trabajo fundamental sobre teoría de cuerpos, citando a los números p -ádicos como su mayor motivación. En ese mismo año, gracias a los trabajos de Maurice Fréchet, Frigyes Riesz y otros, las ideas topológicas se vuelven mas claras, esto permite tener un mejor entendimiento de los números p -ádicos. Aún así, en este trabajo se basa en los aspectos analíticos y algebraicos de los números p -ádicos, para ir perfilando al teorema de Hasse-Minkowski.

1.1.2. Antecedentes académicos

Arnalot (2020), en su estudio sobre “El Teorema de Hasse-Minkowski” el cual tiene como objetivo analizar el teorema de Hasse-Minkowski para resolver vectores en $\mathbb{R}^2$, en el cual se concluye que en todo cuerpo la cuadrática sobre K es un polinomio homogéneo de grado 2, es decir, una suma de monomios de grado 2.

En este sentido Ibáñez (2021), en su estudio sobre “Principio local-global” cuyo objetivo fue analizar el principio local-global de cuerpo locales en $\mathbb{R}$ y $\mathbb{Z}_p$, concluye que el principio local - global es aplicable a otras propiedades sobre el cuerpo de los racionales. También conocer bajo que condiciones funciona el principio local - global y en que casos no, en éste caso ver se observó porqué no funciona, y la posibilidad de formular el principio local - global, tomando como cuerpos locales a $\mathbb{R}$, y $\mathbb{Z}_p$, y como anillo global a $\mathbb{Z}$.

Hasse (2022) en su estudio sobre “Prefacio a la Tercera Edición. En Teoría de Números” cuyo objetivo fue analizar comparativamente si un número es p -ádico es solución de campos compltos. En el mismo se concluye que dos números p -ádicos están cerca cuando su diferencia es divisible por una potencia elevada de p : cuanto mayor es la potencia, más cerca están. Esta propiedad permitió que los números p -ádicos codifican la información de congruencia de una manera que resulta tener aplicaciones de gran alcance en teoría de números.

1.2. Planteamiento del problema

El teorema de Hasse-Minkowski es un resultado fundamental de la teoría de números que establece que dos formas cuadráticas sobre un cuerpo numérico son equivalentes si y solo si son equivalentes localmente en todos los lugares, condición que no siempre se tiene a mano, es decir, que sean equivalentes sobre cada terminación del campo (que puede ser real, complejo, o p -ádico).

Un resultado relacionado es que un espacio cuadrático sobre un campo numérico es isotrópico si y solo si es isótropo localmente en todas partes, o de manera equivalente, que una forma cuadrática sobre un cuerpo numérico representa cero de manera no trivial si y solo si esto se cumple para todos los complementos del cuerpo.

Esta situación de no reconocer de entrada que dos cuerpos sean localmente en todos los lugares en formas cuadráticas da lugar al teorema que fue probado en el caso del campo de números racionales por Hermann Minkowski (2019) y generalizado a campos numéricos por Helmut Hasse (2022). La misma afirmación es aún más general para todos los campos globales.

Dado que la importancia del teorema de Hasse-Minkowski radica en un paradigma novedoso para los residuos cuadráticos, se pretende responder a esta pregunta de manera general. ¿Cómo analizar el teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p -ádicas?. Por cierto, llegados a este punto, es importante responder a las siguientes preguntas:

1. ¿Cómo identificar si una ecuación p -ádica tiene solución racional mediante valuación, norma y métrica?
2. ¿Cómo caracterizar los grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$?
3. ¿Cómo usar las propiedades de los módulos cuadráticos para caracterizar las formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$?

4. ¿Cuál es el resultado de aplicar el teorema de Hasse-Minkowski a la solución de la ecuación p-ádica?

1.3. Justificación

A lo largo de los años los matemáticos han tratado de analizar como se presenta el teorema de Hasse-Minkowski en las ecuaciones p-ádicas, enfocándose más en las aplicaciones de dichas ecuaciones mediante valuación, norma y métrica.

La realización de esta investigación estriba en el hecho de realizar un análisis a los grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$, así como también usar las propiedades de los módulos cuadráticos para caracterizar formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$.

Este trabajo permitirá describir los resultado de aplicar el teorema de Hasse-Minkowski a la solución de la ecuación p-ádica y estará a disposición de estudiantes, profesionales y público interesado en el tema y el mismo será alojado en la Universidad Tecnológica del Cibao Oriental.

1.4. Objetivos

1.4.1. Objetivo general

Analizar el teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p-ádicas.

1.4.2. Objetivos específicos

1. Identificar si una ecuación p-ádica tiene solución racional mediante valuación, norma y métrica.
2. Caracterizar los grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$.

3. Usar las propiedades de los módulos cuadráticos para caracterizar las formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$.
4. Describir los resultado de aplicar el teorema de Hasse-Minkowski a la solución de la ecuación p-ádica.

1.5. Alcances y límites

Ésta investigación se limita al campo de la teoría algebraicas de números, la misma tiene como alcance, hacer un análisis del teorema de Hasse-Minkowski aplicado a las ecuaciones p-ádicas.

CAPÍTULO II

MARCO REFERENCIAL

En este capítulo se muestran algunos conceptos, definiciones, ejemplos y teoremas útiles para comprender la presente investigación y que serán utilizadas en la concreción de los capítulos IV y V.

2.1. Los números p -ádicos

Esta sección introduce la teoría de números p -ádicos. Hay varias formas equivalentes de definir este conjunto de números, dos de ellos se muestran a continuación. Los primeros son más útiles para comprender realmente lo que usará al construir números p -ádicos, mientras que el segundo es una representación más algebraica que, aunque es un poco más compleja de entender, permite un manejo más sencillo y formal de ellos. (Sada Allo, M., 2020)

Más formalmente según Chacón Cortés, L. F. (2020), para un primo p dado, el cuerpo $\mathbf{Q}_p$ de los números p -ádicos es un completado de los números racionales. El cuerpo $\mathbf{Q}_p$ también recibe una topología derivada de una métrica, que a su vez se deriva del orden p -ádico, una valoración alternativa en los números racionales. Este espacio métrico es completo en el sentido de que cada sucesión de Cauchy converge hasta un punto en $\mathbf{Q}_p$. Esto es lo que permite el desarrollo del cálculo en $\mathbf{Q}_p$, y es la interacción de esta estructura analítica y algebraica lo que le da a los sistemas numéricos p -ádicos su gran utilidad.

2.1.1. La valuación, la norma p -ádica y la métrica p -ádica

Sea p un número primo fijo. Para cada $a \in \mathbb{Z}$ existe un único $n \in \mathbb{Z}_{\geq 0}$ tal que $a = p^n r$, con $(r, p) = 1$. Esto permite, siguiendo las ideas en Baker, A. J. (2006), hacer la siguiente definición (Bellido Rojas, I. L., 2019):

Definición 2.1.1 Para Burgos Guerrero, V. M. (2019). Se define la valuación p -ádica de un número racional como:

- $v_p(x) = \max\{n \in \mathbb{Z} : p^n \mid x\} \geq 0$, si $x \in \mathbb{Z} \setminus \{0\}$
- $v_p(q) = v_p(a) - v_p(b)$, si $q = a/b \in \mathbb{Q}$.

Proposición 2.1.1 Sean $x, y \in \mathbb{Q}$. Entonces valen:

- a) $v_p(x) = \infty \iff x = 0$
- b) $v_p(xy) = v_p(x) + v_p(y)$
- c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, y si $v_p(x) \neq v_p(y)$ se da la igualdad.

Definición 2.1.2 Si p es un número primo fijo, se define en $\mathbb{Q}$ la norma p -ádica como $\|x\|_p = p^{-v_p(x)}$. (Bellido Rojas, I. L., 2019)

Obviamente, se define $\|0\|_p = 0$. Es fácil verificar que es efectivamente una norma en $\mathbb{Q}$. En particular, se ve que $\|\cdot\|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$. Valen las siguientes propiedades, análogas a las que valían para la valuación:

Proposición 2.1.2 Si $x \in \mathbb{Q}$, entonces se verifican:

- a) $\|x\|_p = 0 \iff x = 0$
- b) $\|xy\|_p = \|x\|_p \|y\|_p$
- c) $\|x + y\|_p \leq \max\{\|x\|_p, \|y\|_p\}$, y si $\|x\|_p \neq \|y\|_p$ se da la igualdad.

Definición 2.1.3 Se define en $\mathbb{Q}$ la métrica p -ádica, como $d_p(x, y) = v_p(x - y)$. (López Hernández, E. Y., 2023)

Definición 2.1.4 El cuerpo de números p -ádicos $\mathbb{Q}_p$ es la completación de $\mathbb{Q}$ con respecto a la métrica p -ádica. (Rocha Peña, L. J., 2021).

En $\mathbb{Q}_p$ se considera la topología inducida por la métrica p -ádica, según la cual resulta un espacio de Hausdorff localmente compacto. Obviamente, considerado como espacio métrico, $\mathbb{Q}_p$ resultará completo.

La segunda forma de la definición en $\mathbb{Z}_p$ y $\mathbb{Q}_p$ se verá desde el punto de vista algebraico como se muestra en Serre, J.P. (1996).

Para cada $n \geq 1$, denotemos por A_n al anillo de enteros módulo p^n , es decir, $A_n := \mathbb{Z}/p^n\mathbb{Z}$. Claramente a cada elemento $a \in A_n$ se le puede asociar uno en A_{n-1} tomando resto en la división por p^{n-1} . De esta forma queda siempre definido un epimorfismo $\phi_n : A_n \rightarrow A_{n-1}$, cuyo núcleo es $p^{n-1}A_n$. Con estos epimorfismos, resulta evidente que la sucesión

$$\dots \rightarrow A_n \rightarrow A_{n-1} \rightarrow \dots \rightarrow A_2 \rightarrow A_1$$

conforma un sistema proyectivo. De esta observación surge la idea para la segunda definición de los números p -ádicos.

Definición 2.1.5 Para Tuesta, N. C., Sotomayor, A. M., y Saldaña, M. E. S. (2022). Se define el anillo de enteros p -ádicos $\mathbb{Z}_p$ como el límite proyectivo del sistema (A_n, ϕ_n) definido previamente. Es decir,

$$\mathbb{Z}_p := \varprojlim (A_n, \phi_n)$$

Por definición de límite proyectivo (Aguilar Herrera, K. E., 2019), un elemento de $\mathbb{Z}_p$ es una sucesión $x = (\dots, x_n, \dots, x_1)$ con $x_n \in A_n$, y $x_n \equiv x_{n-1} \pmod{p^{n-1}}$. La suma y el producto en este anillo se definen coordenada a coordenada, es decir, se interpreta a $\mathbb{Z}_p$ como un subanillo del anillo producto $\prod_{n \geq 1} A_n$. Antes de llegar a la definición de $\mathbb{Q}_p$, observe algunas propiedades de los enteros p -ádicos.

Proposición 2.1.3 Sea $\varepsilon_n : \mathbb{Z}_p \rightarrow A_n$ la proyección de la n -ésima coordenada x_n de cada entero p -ádico x . Entonces, la sucesión de grupos abelianos

$$0 \rightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \rightarrow 0$$

es exacta.

Proposición 2.1.4 Un elemento de A_n o de $\mathbb{Z}_p$ es una unidad si y sólo si no es divisible por p . Además, todo elemento no nulo de $\mathbb{Z}_p$ se escribe de forma única como $p^n u$, con $u \in \mathcal{U}(\mathbb{Z}_p)$ y $n \geq 0$.

Definición 2.1.6 El conjunto de los números p-ádicos $\mathbb{Q}_p$ se define como el cuerpo de cocientes del anillo $\mathbb{Z}_p$. (Martín Ovejero, J. (2021).

Proposición 2.1.5 Todo $x \in \mathbb{Q}_p$ admite un único desarrollo de Hensel, es decir, se puede escribir de forma única como $x = \sum_{n \geq n_0} a_n p^n$, con $0 \leq a_n < p$, $a_{n_0} \neq 0$ y $n_0 \in \mathbb{Z}$.

2.2. Grupos multiplicativos y los diferentes stipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$

El propósito de esta sección es caracterizar de alguna manera el grupo multiplicativo y usar esta información para caracterizar los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$.

Lema 2.2.1 Sea $0 \rightarrow A \rightarrow E \rightarrow B \rightarrow 0$ una sucesión exacta de grupos abelianos, a, b los ordenes (finitos) de A, B , y tales que $\text{mcd}(a, b) = 1$. Si $B' := \{x \in E : bx = 0\}$, entonces $E \cong A \oplus B'$, y además B' es el único subgrupo de E isomorfo a B .

Proposición 2.2.1 Si $V := \{x \in U : x^{p-1} = 1\}$, entonces este es el único subgrupo de U isomorfo a F_p^* , $yU = V \times U_1$

Lema 2.2.2 Si $x \in U_n \setminus U_{n+1}$, con $n \geq 1$ ($y \geq 2$ si $p = 2$), entonces $x^p \in U_{n+1} \setminus U_{n+2}$.

Proposición 2.2.2 El grupo U_1 es isomorfo a:

- I) $\mathbb{Z}_p$, si $p \neq 2$.
- II) $\{\pm 1\} \times U_2 \cong \{\pm 1\} \times \mathbb{Z}_2$, si $p = 2$.

Teorema 2.2.1 El grupo $\mathbb{Q}_p^*$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/r\mathbb{Z}$, donde $r = p - 1$ si $p \neq 2$, y $r = 2$ si $p = 2$.

Teorema 2.2.2 Si $p \neq 2$, entonces para que un elemento $x = p^n u \in \mathbb{Q}_p^*$, con $n \in \mathbb{Z}$ y $u \in U^4$, sea un cuadrado perfecto, es necesario y suficiente que n sea par, y que la imagen de u en $F_p^* = U/U_1$ sea un cuadrado perfecto (resto cuadrático).⁵

Corolario 2.2.1 Si $p \neq 2$, el grupo Q_p^*/Q_p^{*2} es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, y se puede representar mediante $\{1, p, u, up\}$, siendo $u \in U$ un elemento tal que su imagen $\tilde{u}$ en F_p^* verifica $\left(\frac{\tilde{u}}{p}\right) = -1$ (es decir, no es un resto cuadrático mód p).

Teorema 2.2.3 Para que un elemento $x = p^n u \in \mathbb{Q}_2^*$ sea un cuadrado perfecto, es necesario y suficiente que n sea par y que $u \equiv 1 \pmod{8}$.

Corolario 2.2.2 El grupo Q_2^*/Q_2^{*2} es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, y se puede representar mediante $\{\pm 1, \pm 5, \pm 2, \pm 10\}$

2.3. Formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$

El objetivo de esta sección es estudiar y caracterizar formas cuadráticas sobre los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$. Para ello se estudian las propiedades de los módulos cuadráticos generales y luego se estudia el lenguaje actual de los módulos cuadráticos. Mientras se completan las propiedades básicas y los teoremas importantes de los números representados por formas cuadráticas, aunque se dedica más tiempo al estudio de estas propiedades en $\mathbb{Q}_p$ y $\mathbb{R}$.

2.3.1. Módulos cuadráticos

Definición 2.3.1 Sea V un A -módulo, con A un anillo conmutativo. Una función $Q : V \rightarrow A$ es una forma cuadrática sobre V si se satisfacen las siguientes condiciones:

- I) $Q(ax) = a^2 Q(x) \forall a \in A, x \in V$;
- II) La función $B(x, y) = Q(x + y) - Q(x) - Q(y)$ es una forma bilineal. (Rodríguez Guzmán, F. P., 2021).

Un par (V, Q) con dichas propiedades se llama módulo cuadrático.

Definición 2.3.2 Si (V, Q) y (V', Q') son dos módulos cuadráticos, una función $f : V \rightarrow V'$ es un morfismo de módulos cuadráticos (o morfismo métrico, para simplificar) si $Q' \circ f = Q$. (Castillo, S. L. S., 2019).

Definición 2.3.3 Sean $U_1, \dots, U_m$ subespacios de V . Diremos que V es la suma directa ortogonal de ellos si son todos ortogonales entre sí, y además V es suma directa de ellos. Se nota como:

$$V = U_1 \hat{\oplus} \dots \hat{\oplus} U_m$$

Proposición 2.3.1 Sea (V, Q) un módulo cuadrático no degenerado. Entonces,

- i) Todos los morfismos métricos que partan de V son inyectivos.
- ii) Para todo subespacio U de V se tiene que

$$U^{00} = U, \dim U + \dim U^0 = \dim V, \text{rad}(U) = \text{rad}(U^0) = U \cap U^0$$

Definición 2.3.4 Dado un módulo cuadrático (V, Q) , diremos que un elemento x es isotrópico si $Q(x) = 0$. Un subespacio U es isotrópico si todos sus elementos lo son. Finalmente, diremos que el módulo cuadrático es isotrópico si existe algún elemento isotrópico no nulo $x \in V$. (Cuadrado Chica, M. A. (2021).

Definición 2.3.5 Un módulo cuadrático que tiene una base formada por dos elementos isotrópicos x, y no ortogonales es llamado un plano hiperbólico.

Proposición 2.3.2 Sea $x \in V$ un elemento isotrópico no nulo, donde (Q, V) es no-degenerado. Entonces existe un subespacio U de V que contiene a x y es un plano hiperbólico.

Corolario 2.3.1 Si (V, Q) es isotrópico, entonces $Q(V) = k$.

Teorema 2.3.1 Todo módulo cuadrático (V, Q) admite una base de elementos ortogonales dos a dos (base ortogonal).

Definición 2.3.6 Dos bases ortogonales de un mismo módulo cuadrático (V, Q) se dicen contiguas si tienen algún elemento en común (si las bases son $(e_1, \dots, e_n)$ y $(e'_1, \dots, e'_n)$, deben existir i, j tal que $e_i = e'_j$)

Teorema 2.3.2 Sea (V, Q) un módulo cuadrático no degenerado de dimensión $n \geq 3$, y sean $e = (e_1, \dots, e_n)$ y $e' = (e'_1, \dots, e'_n)$ dos bases ortogonales de V . Entonces existe una sucesión finita de bases ortogonales $e^{(0)}, e^{(1)}, \dots, e^{(m)}$ tales que $e^{(0)} = e$, $e^{(m)} = e'$ y $e^{(j)}$ es contigua a $e^{(j+1)}$ para todo $j = 0, \dots, m-1$.

Teorema 2.3.3 Si (V, Q) y (V', Q') son isomorfos (como módulos cuadráticos) y no degenerados, entonces todo morfismo métrico inyectivo $s : U \rightarrow V$, de cualquier subespacio U de V , puede ser extendido a una isometría de V en V' .

2.4. Teorema de Hasse-Minkowski a la solución de la ecuación p-ádica.

Teorema 2.4.1 (Teorema de Hasse-Minkowski) Una forma cuadrática con coeficientes racionales representa 0 en $\mathbb{Q}$ si y sólo si representa 0 en todos los cuerpos $\mathbb{Q}_p$, para todo primo p , incluido $p = \infty$.

Teorema 2.4.2 Una forma cuadrática con coeficientes racionales representa a un número racional r en $\mathbb{Q}$ si y sólo si representa a r en todos los cuerpos $\mathbb{Q}_p$, para todo primo p , incluido $p = \infty$.

Definición 2.4.1 Si f y g son dos formas cuadráticas sobre un cuerpo K con m y n variables respectivamente, llamaremos suma directa de f y g a la forma cuadrática dada por

$$(f \oplus g)(x_1, \dots, x_{m+n}) = f(x_1, \dots, x_m) + g(x_{m+1}, \dots, x_{m+n}).$$

Claramente la suma directa de formas cuadráticas regulares es de nuevo una forma cuadrática regular (su determinante es el producto de los determinantes).

Teorema 2.4.3 (Teorema de Witt) Sean f, g, h formas cuadráticas regulares en un cuerpo K . Si $f \oplus g$ es equivalente a $f \oplus h$, entonces g es equivalente a h .

Teorema 2.4.4 Dos formas cuadráticas regulares con coeficientes racionales son racionalmente equivalentes si y sólo si son equivalentes en $\mathbb{Q}_p$ para todo primo p , incluido $p = \infty$.

CAPÍTULO III METODOLOGÍA

En este capítulo se describen los aspectos metodológicos que enmarcan el desarrollo de este estudio. Presenta la metodología, diseño, tipos, métodos y procedimientos de este trabajo.

3.1. Método de investigación

Esta investigación adopta el método deductivo, y como expresan Palella y Martins (2006) el método deductivo se basa en generalizaciones establecidas, reglas, leyes o principios diseñados para resolver un problema específico.

3.2. Diseño de investigación

Esta investigación corresponde al diseño no experimental, ya que, no se manipulan variables, sino que se analizó el teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p -ádicas. El diseño no experimental es aquel que se realiza sin manipular deliberadamente variables (Hernández-Sampieri, Fernández y Baptista, 2014).

3.3. Tipo de investigación

La presente investigación es descriptiva, ya que recopila información que puede lograr los objetivos planteados; y exploratoria, porque analiza teorías poco conocidas. Hernández-Sampieri, Fernández y Baptista (2014), sostienen que la investigación descriptiva es aquella que busca medir o recopilar información y especificar atributos de un sujeto de investigación específico.

3.4. Enfoque de investigación

Este estudio es cualitativo, y se utilizan definiciones, proposiciones y teoremas para intentar dar respuesta a la pregunta de investigación. Según, Hernández Sampieri, Fernández, y Baptista (2014), el enfoque cualitativo se basa en la recolección y

análisis de datos con el fin de refinar las preguntas de investigación, responderlas o formular otras nuevas

3.5. Procedimiento de investigación

1. Con la finalidad de comprender los conocimientos existentes, establecer antecedentes y limitaciones del tema a estudiar, se realizó la lectura de documentos relacionados con el mismo.
2. Luego, se desarrolló la estructura del enfoque del contenido de la investigación y su análisis.
3. Se realizó visitas a Universidades nacionales en busca de revisión de literatura.
4. Se realizaron encuentros con el asesor de la investigación, para que orientara el proceso.
5. Se realizaran las observaciones por parte de los jurados y el asesor.
6. Se entregó el anteproyecto al departamento de postgrado.

CAPÍTULO IV

PRESENTACIÓN DE LOS RESULTADOS

En este capítulo, luego de hacer un análisis minucioso de las definiciones y teoremas, que sirven de sustento para; Analizar el teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p-ádicas, pues se presentan en este apartado dichos detalles de manera minuciosa con la intención de que se logren las preguntas que se han propuesto al inicio del estudio.

4.1. Solución racional mediante valuación, norma y métrica en una ecuación p-ádica

En matemáticas, la solución racional mediante valuación, norma y métrica en una ecuación p-ádica implica utilizar números p-ádicos, que son una generalización de los números racionales, para resolver ecuaciones. La valuación p-ádica asigna un valor absoluto a cada número, la norma p-ádica mide la magnitud de un número y la métrica p-ádica define la distancia entre dos números. Estos conceptos se utilizan en conjunto para encontrar soluciones racionales en ecuaciones p-ádicas.

Un ejemplo de una ecuación p-ádica sería: $3x + 2 = 0$, donde p es un número primo. Utilizando la solución racional mediante valuación, norma y métrica en una ecuación p-ádica, se pueden encontrar los valores de x que satisfacen la ecuación.

Ahora si se consideran mas formalidad en el valor de p . Suponga si p es un número primo fijo. Se sabe, que para cada $a \in \mathbb{Z}$ existe un único $n \in \mathbb{Z}_{\geq 0}$ tal que $a = p^n r$, con $(r, p) = 1$. Esto permite, hacer la siguiente definición:

Definición 4.1.1 Se define la valuación p-ádica de un número racional como:

- $v_p(x) = \max \{n \in \mathbb{Z} : p^n \mid x\} \geq 0$, si $x \in \mathbb{Z} \setminus \{0\}$
- $v_p(q) = v_p(a) - v_p(b)$, si $q = a/b \in \mathbb{Q}$

Por convención se toma $v_p(0) = \infty$. Note que $v_p : \mathbb{Q} \rightarrow \mathbb{Z}$, y además está bien definida, pues si $a/b = a'/b'$ entonces $ab' = a'b$, y claramente $v_p(a) + v_p(b') = v_p(a') + v_p(b)$ de donde $v_p(a/b) = v_p(a'/b')$.

Proposición 4.1.1 Sean $x, y \in \mathbb{Q}$. Entonces valen:

a) $v_p(x) = \infty \iff x = 0$

b) $v_p(xy) = v_p(x) + v_p(y)$

c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, y si $v_p(x) \neq v_p(y)$ se da la igualdad.

Demostración: Probaremos únicamente el ítem (c) que es el no trivial. Para eso, supongamos que x, y son no nulos (si alguno de ellos lo fuera, se da la igualdad trivialmente). Entonces podemos escribir

$$x = p^r \frac{a}{b}, y = p^s \frac{c}{d}$$

con $r, s \in \mathbb{Z}$, y $a, b, c, d \in \mathbb{Z}$ no divisibles por p . Es claro que $v_p(x) = r, v_p(y) = s$. Supongamos sin pérdida de generalidad que $s \geq r$, y sea $t = s - r \geq 0$. Entonces,

$$x + y = p^r \left(\frac{a}{b} + p^t \frac{c}{d} \right) = p^r \left(\frac{ad + p^t bc}{bd} \right)$$

de donde se deduce inmediatamente la desigualdad a probar. Si suponemos $v_p(x) \neq v_p(y)$, es equivalente a tomar $t \geq 1$ con lo cual se ve claramente que p no divide ni al numerador ni al denominador de la fracción que acompaña a p^r (pues por hipótesis p no dividía a ninguno de los enteros a, b, c, d). $\square$

Esta valuación p -ádica nos permite definir la norma p -ádica, de la siguiente manera:

Definición 4.1.2 Si p es un número primo fijo, se define en $\mathbb{Q}$ la norma p -ádica como $\|x\|_p = p^{-v_p(x)}$.

Obviamente, definimos $\|0\|_p = 0$. Es fácil verificar que es efectivamente una norma en $\mathbb{Q}$. En particular, se ve que $\|\cdot\|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$. Valen las siguientes propiedades, análogas a las que valían para la valuación:

Proposición 4.1.2 Si $x \in \mathbb{Q}$, entonces se verifican:

1. $\|x\|_p = 0 \iff x = 0$

2. $\|xy\|_p = \|x\|_p \|y\|_p$
3. $\|x + y\|_p \leq \max\{\|x\|_p, \|y\|_p\}$, y si $\|x\|_p \neq \|y\|_p$ se da la igualdad.

Como bien es sabido, toda norma N en un espacio induce una distancia, mediante la definición $d(x, y) = N(x - y)$. Así, suena lógico presentar la siguiente definición:

Definición 4.1.3 Se define en $\mathbb{Q}$ la métrica p -ádica, como $d_p(x, y) = v_p(x - y)$. Es usual interpretar a los números reales $\mathbb{R}$ como la completación de $\mathbb{Q}$ de acuerdo a la métrica standard $d(x, y) = |x - y|$. Inspirados en esta interpretación, se define lo siguiente:

Definición 4.1.4 El cuerpo de números p -ádicos $\mathbb{Q}_p$ es la completación de $\mathbb{Q}$ con respecto a la métrica p -ádica.

En $\mathbb{Q}_p$ se considera la topología inducida por la métrica p -ádica, según la cual resulta un espacio de Hausdorff localmente compacto. Obviamente, considerado como espacio métrico, $\mathbb{Q}_p$ resulta completo.

4.2. Grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$

El objetivo de esta sección es caracterizar de cierta forma los grupos multiplicativos y, con esta información, los diferentes tipos de restos cuadráticos en cada uno de los cuerpos $\mathbb{Q}_p$.

Llamaremos $U = \mathbb{Z}_p^*$ al grupo multiplicativo (o de unidades) de los enteros p -ádicos. Para cada $n \geq 1$, notamos $U_n = 1 + p^n \mathbb{Z}_p$, es decir, el núcleo de la aplicación $\varepsilon_n : U \rightarrow (\mathbb{Z}/p^n \mathbb{Z})^*$. En particular, como $U_1 = \ker(\varepsilon_1)$ y $(\mathbb{Z}/p \mathbb{Z})^* = \text{Im}(\varepsilon_1)$, U/U_1 se puede pensar como $(\mathbb{Z}/p \mathbb{Z})^* \cong F_p^*$ (grupo multiplicativo del cuerpo de p elementos), y luego es cíclico y de orden $p - 1$. Además, es claro que los U_n forman una sucesión decreciente (según inclusión) de subgrupos abiertos de U (pues $U/U_n \cong (\mathbb{Z}/p^n \mathbb{Z})^*$),

y se tiene que $U = \lim U/U_n$.

Consideremos ahora para cada $n \geq 1$ el morfismo de grupos abelianos $\phi : U_n \rightarrow \mathbb{Z}/p\mathbb{Z}$, dado por $(1 + p^n x) \mapsto x \text{ mód } p$. Entonces $U_n/\ker(\phi) \cong \text{Im}(\phi)$. Pero $\ker(\phi) = U_{n+1}$, $\text{Im}(\phi) = \mathbb{Z}/p\mathbb{Z}$, luego $U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$. Así, se puede ver por inducción que U_1/U_n tiene orden p^{n-1} .

Veamos ahora el siguiente Lema de teoría de grupos:

Lema 4.2.1 Sea $0 \rightarrow A \rightarrow E \rightarrow B \rightarrow 0$ una sucesión exacta de grupos abelianos, a, b los ordenes (finitos) de A, B resp., y tales que $\text{mcd}(a, b) = 1$. Si $B' := \{x \in E : bx = 0\}$, entonces $E \cong A \oplus B'$, y además B' es el único subgrupo de E isomorfo a B .

Demostración: Como a y b son coprimos, existen $r, s \in \mathbb{Z}$ tales que $ar + bs = 1$. Veamos primero que $A \cap B' = 0$. Sea $x \in A \cap B'$. Entonces por ser a el orden de A , $ax = 0$. Y $bx = 0$ por definición de B' , luego $x = (ar + bs)x = r(ax) + s(bx) = 0$ y entonces $A \cap B' = 0$. Ahora bien, tomemos $x \in E$ y escribamoslo como $x = arx + bsx$. Sean f el monomorfismo de A a E y g el epimorfismo de E a B . Entonces $g(bsx) = bg(sx) = 0$ ya que $g(sx) \in B$ y b es el orden de ese grupo. Luego, $bsx \in \ker g = \text{Im } f \cong A$ pues f es mono. Entonces, $bsx \in A$ (abuso de notación; en realidad está en un subgrupo de E isomorfo a A). Resta ver que $arx \in B'$, pero para esto hacemos $b(arx) = a(brx)$, se ve de forma análoga a la anterior que $brx \in A$, y luego $abrx = 0$ con lo cual $arx \in B'$. Por lo tanto, $E \cong A \oplus B'$. El epimorfismo $g : E \rightarrow B$ define un isomorfismo entre B y B' , puesto que en los elementos de A da 0. Si tuviéramos un $B'' \subseteq E$ isomorfo a B entonces por una cuestión de orden (de este subgrupo), $bB'' = 0$ luego $B'' \subseteq B'$ por definición de B' . Y al tener el mismo orden, resulta que $B' = B''$. $\square$

Proposición 4.2.1 El grupo U_1 es isomorfo a.

I) $\mathbb{Z}_p$, si $p \neq 2$.

II) $\{\pm 1\} \times U_2 \cong \{\pm 1\} \times \mathbb{Z}_2$, si $p = 2$.

Demostración: (i) Sea $\alpha \in U_1 \setminus U_2$, por ejemplo $\alpha = 1 + p$. Por el Lema anterior, $\alpha^{p^i} \in U_{i+1} \setminus U_{i+2}$. Sea α_n la imagen de α en U_1/U_n . De lo mencionado anteriormente (tomando $i = n - 2$ y $i = n - 1$) se deduce que $\alpha^{p^{n-2}} \in U_{n-1} \setminus U_n$ y $\alpha^{p^{n-1}} \in U_n$, luego $(\alpha_n)^{p^{n-2}} \neq 1$ y $(\alpha_n)^{p^{n-1}} = 1$ (recordar que los grupos se notan multiplicativamente).

Al ser U_1/U_n un grupo de orden p^{n-1} , resulta que el orden de α_n es exactamente p^{n-1} , con lo cual es un generador. Esto implica que se puede definir un isomorfismo $\theta_{n,\alpha}$ entre $\mathbb{Z}/p^{n-1}\mathbb{Z}$ y U_1/U_n .

Pasando al límite, queda entonces definido un isomorfismo θ entre $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ y $U_1 = \varprojlim U_1/U_n$, con lo cual queda probado el caso $p \neq 2$.

ii) Tomando $\alpha \in U_2 \setminus U_3$ obtenemos de la misma forma que antes los isomorfismos $\theta_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \rightarrow U_2/U_n$, y por lo tanto se tiene un isomorfismo $\theta : \mathbb{Z}_2 \rightarrow U_2$. Por otro lado, como $U_1/U_2 \cong \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$ se ve inmediatamente que $U_1 \cong \{\pm 1\} \times U_2$. $\square$

Con estos resultados, ya estamos en condiciones de caracterizar el grupo multiplicativo de $\mathbb{Q}_p$ de la siguiente manera:

Teorema 4.2.1 El grupo $\mathbb{Q}_p^*$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/r\mathbb{Z}$, donde $r = p - 1$ si $p \neq 2$, y $r = 2$ si $p = 2$.

Demostración: Se sabe que todo elemento $x \in \mathbb{Q}_p^*$ se escribe de forma única como $x = p^n u$, con $n \in \mathbb{Z}$ y $u \in U$. Luego, $\mathbb{Q}_p^* \cong \mathbb{Z} \times U$. Pero además, $U \cong V \times U_1$, y $V \cong \mathbb{Z}/(p-1)\mathbb{Z}$ si $p \neq 2$ (V es trivial si $p = 2$), luego usando la estructura para U_1 probada en la Proposición anterior se deduce inmediatamente lo que quería probar. $\square$

4.3. Propiedades de los módulos cuadráticos para caracterizar las formas cuadráticas en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$

El objetivo de esta sección es estudiar y caracterizar las formas cuadráticas sobre los cuerpos $\mathbb{Q}_v$ y $\mathbb{Q}$. Para eso, estudiaremos las propiedades de los módulos cuadráticos en general, y luego las traduciremos al lenguaje corriente de formas cuadráticas. Al terminar con las propiedades básicas y los importantes teoremas de representación de un número a través de una forma cuadrática.

Sea $f(X) = \sum_{i=1}^n a_{ii}X_i^2 + 2\sum_{i<j} a_{ij}X_iX_j$ una forma cuadrática en n variables sobre k . Suponemos que $a_{ij} = a_{ji}$, de esta forma, la matriz de $fA = (a_{ij})$ resulta simétrica. Entonces, (k^n, f) resulta un módulo cuadrático; será llamado de hecho el módulo cuadrático asociado a f (o a su matriz A).

Definición 4.3.1 Diremos que dos formas cuadráticas f y f' son equivalentes si los correspondientes módulos cuadráticos son isomorfos. Lo notaremos como

$$f \sim f'$$

Si $f(X_1, \dots, X_n)$ y $g(X_1, \dots, X_m)$ son dos formas cuadráticas, definimos la suma (también conocida como suma ortogonal) de f y g mediante la forma cuadrática

$$f \dot{+} g := (X_1, \dots, X_n) + g(X_1, \dots, X_m)$$

en $n + m$ variables (en realidad se realiza la suma directa de los módulos cuadráticos, definiendo la forma cuadrática allí canónicamente). De manera natural, definiremos

$$f \dot{-} g := f \dot{+} (-g)$$

En general, se omitirá el puntito por comodidad de notación (siempre y cuando no haya problemas).

Definición 4.3.2 Se dice que una forma cuadrática f representa a un determinado elemento $a \in k$ si existe $x \in (k^n)^*$ tal que $f(x) = a$.

Observar que f representa a 0 si y sólo si su módulo cuadrático correspondiente es isotrópico.

Definición 4.3.3 Una forma cuadrática $f(X_1, X_2)$ se dice hiperbólica si se tiene

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

En ese caso, también se tendría que $f \sim X_1 X_2$.

Y si interpretamos en este contexto se obtienen los siguientes resultados, que traducen todos los problemas relativos a números representables por cierta forma cuadrática, a entender cuáles son las formas cuadráticas isotrópicas.

Corolario 4.3.1 Si g es una forma cuadrática en $n - 1$ variables, y $a \in k^*$, entonces las propiedades son equivalentes:

- I) g representa a a ;
- II) $g \sim h + aZ^2$, donde h es una forma cuadrática en $n - 2$ variables;
- III) La forma cuadrática $f = g - aZ^2$ representa a 0.

Demostración:

(i) $\Leftrightarrow$ (ii): La vuelta es trivial, pues $g(0, \dots, 0, 1) = a$. Para ver su recíproca, si suponemos que g representa a a entonces el módulo cuadrático V correspondiente a g tendrá un elemento x tal que $x.x = a$ (ya que $x \cdot x = g(x)$ en dicho módulo cuadrático). Sea H el complemento ortogonal de x ; tenemos que $V = H \hat{\oplus} kx$. O lo que es equivalente, $g \sim h + aZ^2$, donde h es la g restringida a H (es claro, dado que $x.x = a$, que g restringida a kx es aZ^2).

(ii) $\Rightarrow$ (iii): Por la hipótesis (ii) tenemos que $f \sim h + aY^2 - aZ^2$, luego $f(0, \dots, 0, 1, 1) = 0$ entonces f representa a 0.

(iii) $\Rightarrow$ (i): Supongamos que $f \sim g - aZ^2$ y $f(x_1, \dots, x_{n-1}, z) = 0$, con $(x_1, \dots, x_{n-1}, z) \neq 0$. Entonces: o bien $z = 0$, en cuyo caso $g(x_1, \dots, x_{n-1}) = 0$ con $(x_1, \dots, x_{n-1}) \neq 0$, o sea que g representa a 0 y luego a a ; o bien $z \neq 0$, que implica $g(x_1/z, \dots, x_{n-1}/z) = a$ por lo tanto g representa a a (observar que no es necesario pedir que algún x_j sea no nulo, pues si todos fueran 0 entonces $a = 0$, absurdo). $\square$

4.4. Teorema de Hasse-Minkowski a la solución de la ecuación p-ádica

Basándose en los resultados previos se estudian ahora las formas cuadráticas sobre $\mathbb{Q}$, para llegar así al resultado principal de nuestro trabajo.

Como antes, V denotará el conjunto de números primos junto con el símbolo ∞ , y se denota $\mathbb{Q}_\infty = \mathbb{R}$. Sea $f \sim a_1X_1^2 + \dots + a_nX_n^2$ una forma cuadrática en $\mathbb{Q}$ de rango n . Considere los siguiente invariantes, llame invariantes locales de f :

- a) El discriminante de f , $d(f) = a_1 \dots a_n \in \mathbb{Q}^*/\mathbb{Q}^{*2}$
- b) Para cada $v \in V$, consideramos a f como una forma cuadrática f_v en $\mathbb{Q}_v$, lo cual nos permite definir el invariante $\varepsilon_v(f)$ para cada $v \in V$ de la siguiente manera:

$$\varepsilon_v(f) = \prod_{i < j} (a_i, a_j)_v$$

de donde se tiene que

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

- c) La signatura (r, s) de la forma cuadrática pensada en $\mathbb{R}$. Se está ahora en condición de presentar el Teorema que nos dice que es equivalente la existencia de soluciones en $\mathbb{Q}$ a la existencia de soluciones en cada $\mathbb{Q}_v$.

Teorema 4.4.1 (Hasse-Minkowski). Sea f una forma cuadrática sobre $\mathbb{Q}$. Entonces f representa a 0 si y sólo si para todo $v \in V$ la forma cuadrática f_v representa a 0.

Demostración: Es obvio que si f representa a 0, su imagen en $\mathbb{Q}_v$ también, para todo v . Para probar la vuelta, escribamos a f en la forma usual:

$$f \sim a_1 X_1^2 + \dots + a_n X_n^2, a_i \in \mathbb{Q}^*$$

Y supongamos sin pérdida de generalidad que $a_1 = 1$ (reemplazando f por $a_1 f$). Dividir la prueba en casos: $n = 2, 3, 4$ y ≥ 5

I) $n = 2$

Tenemos $f = X_1^2 - aX_2^2$. El hecho de que f_∞ represente a 0 nos dice que $a > 0$.

Escribamos

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

y como f_p representa a 0 para todo p , se tiene que si (x_1, x_2) es una solución no trivial de $f_p = 0$ entonces $a = (x_1/x_2)^2$, y entonces es un cuadrado en cada $\mathbb{Q}_p$. Esto implica que $v_p(a)$ es par, para todo p . Pero entonces a es un cuadrado en $\mathbb{Q}$, con lo cual f representa a 0.

II) $n = 3$ (Legendre)

Se tiene $f = X_1^2 - aX_2^2 - bX_3^2$, y podemos suponer que a y b son enteros libres de cuadrados (si no fueran enteros, multiplicamos por los denominadores al cuadrado, obteniendo una forma equivalente; luego para que sean libres de cuadrados, hacemos que las variables absorban todos los factores cuadrados de a y de b). Esto se traduce en que $v_p(a), v_p(b) \in \{0, 1\}$ para todo p primo. Supongamos sin pérdida de generalidad que $|a| \leq |b|$. Probemos el resultado por inducción en $m := |a| + |b|$.

Para $m = 2$, $f = X_1^2 \pm X_2^2 \pm X_3^2$. Pero no pueden ser todos signos positivos por el hecho de que f_∞ representa a 0. Entonces, es claro que f representa a 0. Supongamos ahora que $m > 2$. Esto implica que $|b| \geq 2$ (pues es el más grande de los dos). Escribamos a b como

$$b = \pm p_1 \dots p_k$$

donde los p_i son primos distintos (por la suposición hecha de que b es libre de cuadrados). Sea p cualquiera de los p_i , veamos que a es un cuadrado módulo p . Si a es múltiplo de p , esto es trivial. En caso contrario, a es una unidad en $\mathbb{Q}_p$. Por hipótesis, sabemos que existe $(x, y, z) \in (\mathbb{Q}_p)^3$ tal que $z^2 - ax^2 - by^2 = 0$. Podemos suponer, que (x, y, z) es primitiva (que $x, y, z \in \mathbb{Z}_p$ y hay alguno no múltiplo de p). Se tiene que $z^2 - ax^2 \equiv 0 \pmod{p}$ ya que $p \mid b$.

Si p dividiera a x , entonces también a z . Pero como $v_p(b) = 1$, p dividiría también a y , absurdo. Luego x no es múltiplo de p , entonces multiplicando por su inverso mód p en la ecuación de antes, se ve que $a \equiv (zx^{-1})^2 \pmod{p}$ entonces es cuadrado módulo p .

Esto vale para cualquier p_i que divide a b , luego como $\mathbb{Z}/b\mathbb{Z} = \prod \mathbb{Z}/p_i\mathbb{Z}$, tenemos que a es un cuadrado módul b . Es decir, existen t, b' tales que

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

Se puede suponer que $|t| \leq |b|/2$. Observar que $bb' = t^2 - a$ luego bb' es la norma de un elemento de $k(\sqrt{a})$. Entonces, $(a, bb') = 1$. Luego $(a, b) = 1$ sii $(a, b') = 1$, por linealidad. Así, recordando la definición del símbolo de Hilbert, tenemos que nuestra forma f representa a 0 en k ($= \mathbb{Q}$ o a $\mathbb{Q}_p$) si lo hace la forma

$$f' := X_1^2 - aX_2^2 - b^6X_3^2$$

Por hipótesis, f representa a 0 en cada $\mathbb{Q}_p$, entonces f' también. Pero observar que

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

pues $|b| \geq 2$. Si escribimos $b' = ub''$, con b'' libre de cuadrados, entonces es claro que $|b''| < |b|$. Por hipótesis inductiva, la forma cuadrática $f'' = X_1^2 - aX_2^2 - b''X_3^2$ representa a 0. Luego f' también, y en consecuencia nuestra f .

III) $n = 4$

Por comodidad, escribamos $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Sea $v \in V$. Como

f_v representa a 0, se tiene que existe un $x_v \in \mathbb{Q}_v^*$ representado por las formas $aX_1^2 + bX_2^2$ y $cX_3^2 + dX_4^2$. Esto equivale, para $\mathbb{Q}_\infty = \mathbb{R}$, a decir que

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

Y esto vale para todo $v \in V$. Como $\prod_{v \in V} (a, b)_v = \prod_{v \in V} (c, d)_v = 1$, y obtenemos así un $x \in \mathbb{Q}^*$ que verifica

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

para todo $v \in V$.

Esto implica que la forma cuadrática $aX_1^2 + bX_2^2 - xZ^2$ representa a 0 en cada $\mathbb{Q}_v$, y entonces representa a 0 en $\mathbb{Q}$ por el caso anterior. O sea que $x \in \mathbb{Q}^*$ es representado por $aX_1^2 + bX_2^2$. Análogamente, x es representado por $cX_3^2 + dX_4^2$. Aplicando ahora otra implicación, deducimos que f representa a 0 en $\mathbb{Q}$.

IV) $n \geq 5$

Probaremos el resultado por inducción en n . Pensemos a f como $f = h - g$, donde $h = a_1X_1^2 + a_2X_2^2$ y $g = -(a_3X_3^2 + \dots + a_nX_n^2)$. Sea S el subconjunto de V dado por los elementos $\infty, 2$, y los primos p tales que $v_p(a_i) \neq 0$ para algún $i \geq 3$ (i.e., primos que dividen a alguno de los coeficientes de g). Claramente, S es finito. Sea $v \in S$. Como f_v representa a 0, existirá un $a_v \in \mathbb{Q}_v^*$ representado (en $\mathbb{Q}_v$) por h y g . Esto es, existen $x_i^v \in \mathbb{Q}_v, i = 1, \dots, n$ tales que

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

Como los cuadrados de $\mathbb{Q}_v^*$ forman un abierto, si utilizamos el conjunto S , deducimos que existen $x_1, x_2 \in \mathbb{Q}$ tales que si $a = h(x_1, x_2)$, entonces $a/a_v \in \mathbb{Q}_v^{*2}$ para todo $v \in S$. □

CAPÍTULO V

CONCLUSIONES

Luego de analizar los resultados presentados en el capítulo IV, se muestran las conclusiones pertinentes para dar respuesta a los objetivos de investigación planteado en el capítulo I. Específicamente se basó en analizar el teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p -ádicas.

5.1. Conclusiones

En esta sección se realiza un análisis de los resultados encontrados en esta tesis, presentando así los más pertinentes de la misma. De forma específica se realizó un análisis del teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p -ádicas, obteniendo conclusiones relevantes.

- Luego de analizar el teorema de Hasse-Minkowski aplicado a la solución de ecuaciones p -ádicas, se concluye que este teorema es una herramienta poderosa para investigar la existencia y no existencia de soluciones en el ámbito de las ecuaciones p -ádicas.

Además, se destaca la versatilidad del teorema de Hasse-Minkowski al aplicarse a diferentes contextos y tipos de ecuaciones p -ádicas. Su utilidad no se limita a un caso específico, sino que puede ser empleado en una amplia gama de problemas matemáticos. Esto demuestra su robustez y relevancia en la resolución de ecuaciones p -ádicas, brindando a los investigadores y matemáticos una herramienta poderosa para abordar estos desafíos.

En cuanto a los objetivos específicos se llegó a las siguientes conclusiones:

- a) La solución racional mediante valuación, norma y métrica en una ecuación p -ádica proporcionó un enfoque poderoso y eficiente para resolver problemas matemáticos complejos en este contexto específico. La norma p -ádica proporcionó una medida de tamaño relativo basada en la valuación p -ádica. La métrica p -ádica permitió definir distancias entre números p -ádicos.

- b) En cuanto al estudio de los grupos multiplicativos y los diferentes tipos de residuos cuadráticos en cada campo $\mathbb{Q}_p$, se logró comprender las propiedades aritméticas de los números p-ádicos. Estos conceptos permitieron analizar la estructura y las propiedades de los elementos en estos campos, así como resolver ecuaciones y problemas relacionados con los residuos cuadráticos. El estudio de estos temas tiene aplicaciones en diversas áreas como la teoría de números, la criptografía y la geometría algebraica.
- c) El estudio de las propiedades de los módulos cuadráticos en los dominios $\mathbb{Q}_v$ y $\mathbb{Q}$ fue fundamental para caracterizar y analizar las formas cuadráticas en estos contextos. Estas propiedades permitieron comprender la estructura y las propiedades de las formas cuadráticas, así como resolver ecuaciones y problemas relacionados con ellas.
- d) Finalmente, el teorema de Hasse-Minkowski es una herramienta poderosa para abordar la solución de ecuaciones p-ádicas. Este teorema estableció que una ecuación tiene solución en los números racionales si y solo si tiene solución en los números p-ádicos para todos los primos p. Esto permitió utilizar el enfoque p-ádico para resolver ecuaciones y analizar propiedades aritméticas de manera más general.

5.2. Líneas futuras de investigación

Luego de presentar las conclusiones pertinentes, se propone algunas líneas futuras para otros maestrante que le interese el tema en cuestión o que sirvan para otras generaciones de la comunidad y el país, entre ellos:

1. Investigación sobre la generalización del teorema de Hasse-Minkowski para ecuaciones cúbicas y mayores.
2. Estudio de las implicaciones del teorema de Hasse-Minkowski en la teoría de números y la geometría algebraica.

Referencias

- Abreu, J. (2015). Analisis al metodo de investigacion. Daena: International Journal of Good Conscience.
- Aguilar Herrera, K. E. (2019). Caso clínico trastorno límite de personalidad.
- Arnaldot Farràs, J. (2020). El Teorema de Hasse-Minkowski.
- Baker, A. J. (2006)“An Introduction to p -adic numbers and p -adic Analysis.”
- Bellido Rojas, I. L. (2019). Algunas propiedades del cuerpo de los números P-ÁDICOS.
- Burgos Guerrero, V. M. (2019). Funciones Zeta Locales de Igusa y Operadores Pseudodiferenciales sobre campos p -ádicos.
- Castillo, S. L. S. (2019). Criterio de Euler-Ley de Rec. Matemática Discreta.
- Chacón Cortés, L. F. (2020). Una introducción a los números p -ádicos y sus Aplicaciones. In IV Encuentro Internacional de Matemáticas, Estadística y Educación Matemática.
- Cuadrado Chica, M. A. (2021). Ley de reciprocidad cuadrática y cuestiones relacionadas con cuadrados.
- Hasse, H. (2022). Prefacio a la Tercera Edición. En Teoría de Números (págs. XII-XII). De Gruyter.
- Hernández-Sampieri, R., Fernández, C. y Baptista, P. (2014). Metodología de la Investigación Científica. McGraw-Hill / Interamericana editores, S. A. de C.V., México.
- Ibáñez Rojas, L. P. (2021, March). Principio local-global. In ENCuentro Facultad de

CIENCIAS-2020.

López Hernández, E. Y. (2023). p-adic string amplitudes and AdS/CFT correspondence=
Amplitudes de cuerdas p-ádicas y correspondencia AdS/CFT.

Martín Ovejero, J. (2021). Móduli de fibrados principales y teoría algebraica de solitones.

Minkowski, F.S.H. (2019). Cómo Minkowski podría haber descubierto el espacio-tiempo de seis dimensiones.

Palella, S., y Martins, F. (2006). Metodología de la investigación cuantitativa. Caracas: FE-DUPEL.

Rocha Pen?a, L. J. (2021). Ecuacio?n Funcional de la Funcio?n ζ de Riemann. In ENCUESTRO FACULTAD DE CIENCIAS-2020.

Rodríguez Guzmán, F. P. (2021). Polinomios cuadráticos que generan primos.

Sada Allo, M. (2020). Los números p-ádicos: Principales propiedades.

Serre, J.-P. (1996) “A Course in Arithmetic,” Springer-Verlag.

Tuesta, N. C., Sotomayor, A. M., & Saldaña, M. E. S. (2022). Los enteros p-ádicos como un cociente de un anillo de series de potencias. *Pesquimat*, 25(1), 50-58.