Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Matemática

El Teorema de Hasse - Minkowski sobre Q

TESIS

Para optar el Título Profesional de Licenciado en Matemática

AUTOR

Luis Enrique ALEGRÍA ESPINOZA

ASESOR

Dr. Gabriel Armando MUÑOZ MÁRQUEZ

Lima, Perú

2023

Referencia bibliográfica

Alegría, L. (2023). *El Teorema de Hasse - Minkowski sobre Q*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Matemática]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Luis Enrique Alegría Espinoza
Tipo de documento de identidad	DNI
Número de documento de identidad	06765576
URL de ORCID	https://orcid.org/0009-0006-3567-8702
Datos de asesor	
Nombres y apellidos	Gabriel Armando Muñoz Márquez
Tipo de documento de identidad	DNI
Número de documento de identidad	44444774
URL de ORCID	https://orcid.org/0000-0001-5064-1250
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Alfonso Pérez Salvatierra
Tipo de documento	DNI
Número de documento de identidad	06445739
Miembro del jurado 1	
Nombres y apellidos	Leonardo Henry Alejandro Aguilar
Tipo de documento	DNI
Número de documento de identidad	43069051
Datos de investigación	
Línea de investigación	A.3.1.3. Álgebra

Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Coordenadas geográficas Latitud: -12.058333 Longitud: -77.083333
Año o rango de años en que se realizó la investigación	Mayo 2023 – octubre 2023
URL de disciplinas OCDE	Matemáticas puras https://purl.org/pe-repo/ocde/ford#1.01.01 Matemáticas aplicadas https://purl.org/pe-repo/ocde/ford#1.01.02

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE CIENCIAS MATEMÁTICAS
ESCUELA PROFESIONAL DE MATEMÁTICA

ACTA DE SUSTENTACIÓN DE TESIS PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE LICENCIADO(A) EN MATEMÁTICA (PROGRAMA DE TITULACIÓN PROFESIONAL 2023)

En la UNMSM – Ciudad Universitaria – Facultad de Ciencias Matemáticas, siendo las 09:15 horas del viernes 27 de octubre del 2023, se reunieron los docentes designados como Miembros del Jurado Evaluador (PROGRAMA DE TITULACIÓN PROFESIONAL 2023): Dr. Alfonso Pérez Salvatierra (PRESIDENTE), Dr. Leonardo Henry Alejandro Aguilar (MIEMBRO) y el Dr. Gabriel Armando Muñoz Márquez (MIEMBRO ASESOR), para la sustentación de la Tesis titulada: "**EL TEOREMA DE HASSE - MINKOWSKI SOBRE *Q***", presentado por el señor **Bachiller LUIS ENRIQUE ALEGRÍA ESPINOZA**, para optar el Título Profesional de Licenciado en Matemática.

Luego de la exposición de la Tesis, el Presidente invitó al expositor a dar respuesta a las preguntas formuladas.

Realizada la evaluación correspondiente por los Miembros del Jurado Evaluador, el expositor mereció la aprobación Sobresaliente, con un calificativo promedio de Dieciocho. (18)

A continuación, los Miembros del Jurado Evaluador dan manifiesto que el participante **Bachiller LUIS ENRIQUE ALEGRÍA ESPINOZA** en vista de haber aprobado la sustentación de su Tesis, será propuesto para que se le otorgue el Título Profesional de Licenciado en Matemática.

Siendo las 10:00 horas se levantó la sesión firmando para constancia la presente Acta.

Dr. Alfonso Pérez Salvatierra
PRESIDENTE

Dr. Leonardo Henry Alejandro Aguilar
MIEMBRO

Dr. Gabriel Armando Muñoz Márquez
MIEMBRO ASESOR

Yo Gabriel Armando Muñoz Márquez en mi condición de asesor acreditado con la Resolución Decanal N° 001561-2023-D-FCM/UNMSM de la tesis, cuyo título es EL TEOREMA DE HASSE – MINKOWSKI SOBRE Q, presentado por el bachiller Luis Enrique Alegría Espinoza para optar el título Profesional de Licenciado en Matemática de la Facultad de Ciencias Matemáticas.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 8 % de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del Asesor _____

DNI: 44444774

Nombres y apellidos del asesor:
Gabriel Armando Muñoz Márquez

Agradecimentos

Quiero agradecer en primer lugar a Dios y a la virgen de Guadalupe por cada día de existencia que me da para vivir junto a mi familia.

Agradezco a mi padre Juan (que lo llevo en la memoria) y a mi madre Zoila, porque me dieron su apoyo en mi época escolar y en la Universidad; también por su apoyo y cariño a mi querida esposa Nieves.

A mis hermanos Miguel, Susana, José y Milagros, que con sus palabras supieron darme aliento cuando me sentía desfallecer. Uno de los motivos para culminar esta tesis es mi hijo Nicolás Lunié, que es el motor y motivo de mi existencia en la vida.

A mis suegros Demetrio y Nieves, como a mis cuñadas Diana, Clemencia, Elvira y Jane por soportarme en mis noches de estudio y convivencia con ellos; motivo suficiente para sentirme en un lugar cómodo y agradable para el estudio.

A mis sobrinos Nicole, Alexandra, Fabrizio y Jean Pierre por verme como ejemplo en el estudio de las Matemáticas.

Largas fueron mis noches de estudio en el pre-grado y también para culminar esta Tesis; noches de las que guardo momentos imborrables en mi mente como cuando me quedaba dormido estudiando en el sillón y sentía que mi padre Juan me cubría con la colchita, tal como ellos lo hacía en mi niñez.

A todos mis profesores de la Facultad de Ciencias Matemáticas de la Universidad Nacional Mayor de San Marcos, que me formaron en esta dura disciplina que es la Matemática Pura y más aún en el álgebra abstracta.

Así mismo agradezco a mi asesor el Dr. Gabriel Muñoz Márquez por sus valiosas sugerencias y aportes para la redacción del presente trabajo.

Resumen

En este trabajo se estudia el teorema de Hasse-Minkowski sobre $\mathbb{Q}$ el cual establece que una forma cuadrática no degenerada de coeficientes racionales tiene solución no trivial si y solo sí, la forma cuadrática tiene solución no trivial sobre los números reales $\mathbb{R}$ y sobre cada cuerpo p-ádico $\mathbb{Q}_p$.

Para esto, en el Capítulo 1 se presentan algunos preliminares sobre el tema.

En el Capítulo 2, se estudian formas bilineales y formas cuadráticas.

En el Capítulo 3, se presentan generalidades sobre cuerpos locales, para lo cual los números racionales $\mathbb{Q}$, los números reales $\mathbb{R}$ y los campos p-ádicos $\mathbb{Q}_p$ (para p número primo) son casos especiales. El símbolo de Hilbert se define para determinar si una forma cuadrática de tres variables tiene soluciones enteras.

En el capítulo 4, se detalla la demostración del teorema de Hasse-Minkowski para formas cuadráticas de dos, tres, cuatro y al menos cinco variables; además de presentar algunas aplicaciones del teorema.

Palabras clave: forma cuadrática degenerada, vector isotrópico, cuerpos p-ádicos, símbolo de Hilbert.

Abstract

In this work, the Hasse-Minkowski theorem on $\mathbb{Q}$ is studied, which establishes that a non-degenerate quadratic form of rational coefficients has a non-trivial solution if and only if, the quadratic form has a non-trivial solution on the real numbers $\mathbb{R}$ and on every p-adic field $\mathbb{Q}_p$.

For this, in Chapter 1 some preliminaries on the subject are presented.

In Chapter 2, bilinear forms and quadratic forms are studied.

In Chapter 3, generalities about local fields are presented, for which the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$ (for p prime number) are special cases. The Hilbert symbol is defined to determine if a quadratic form of three variables has integer solutions.

In Chapter 4, the proof of the Hasse-Minkowski theorem for quadratic forms of two, three, four, and at least five variables is detailed; in addition to presenting some applications of the theorem.

Key words: degenerate quadratic form, isotropic vector, p-adic fields, Hilbert symbol.

Índice general

Capítulo 1

Introducción

En una línea de tiempo matemáticos como Fermat (1607-1665), Euler (1707-1783), Lagrange (1736-1815) y Gauss (1777-1783) trabajaron en teoría de números buscando soluciones enteras a ecuaciones polinómicas cuadráticas. Más tarde enfocaron tal búsqueda desde los números racionales $\mathbb{Q}$ por ser un cuerpo con una estructura más rica en propiedades, aunque no consiguieron mucho.

Entre los años 1897 a 1913 el matemático alemán Kurt Hensel (1861-1941) crea los números p-ádicos como un análogo de las series de potencia de funciones. En 1918 los números p-ádicos cobran relevancia cuando el matemático ucraniano Alexander Ostroswsky (1893-1986) lo utiliza para demostrar que las completaciones de $\mathbb{Q}$ son los números reales $\mathbb{R}$ o los cuerpos p-ádicos $\mathbb{Q}_p$. Más tarde, aproximadamente en 1921 un discípulo de Hensel, el matemático alemán Helmut Hasse (1898-1979) demostró en su tesis doctoral que los polinomios cuadráticos tenían solución no nula si también la poseían en los números reales $\mathbb{R}$ y en todos los cuerpos $\mathbb{Q}_p$.

Un aporte importante tuvo el matemático alemán Hermann Minkowski (1864-1909) quien desarrolló la teoría de las formas cuadráticas a finales del siglo XIX. Este gran resultado mancomunado se conoce como el Teorema de Hasse-Minkowski sobre $\mathbb{Q}$ y la idea de buscar soluciones en $\mathbb{Q}$ uniendo soluciones en $\mathbb{R}$ y $\mathbb{Q}_p$ se llama el principio local-global.

Las formas cuadráticas que son polinomios homogéneos de grado 2 serán usadas a lo largo de este tratado y cuando presenten términos mixtos sobre cuerpos de característica diferente de 2 podrán ser diagonalizadas mediante un cambio lineal de variables obte-

niéndose solo términos de variables cuadradas.

Ejemplo 1.0.1. *La forma cuadrática* $x^2 + xy + y^2$ *sobre* $\mathbb{Q}$ *puede escribirse como* $x'^2 + 3y'^2$ *donde* $x' = x + \frac{1}{2}y$ *y* $y' = \frac{1}{2}y$.

Así el estudio general de formas cuadráticas sobre $\mathbb{Q}$ sin perder generalidad, se centra en estudiar a las formas cuadráticas en su forma diagonal.

Los siguientes cuatro teoremas son famosos resultados sobre representación de números enteros por formas cuadráticas sobre $\mathbb{Z}$. Cursos elementales de Teoría de números pueden probar los primeros dos teoremas, pero los dos seguidos son un poco más avanzados.

Teorema 1.0.2. *(Fermat) Un primo* p *tiene la forma* $x^2 + y^2$ *con* x, y *en* $\mathbb{Z}$ *si y solo sí,* $p \equiv 1 \mod 4$ *o* $p = 2$.

Teorema 1.0.3. *(Fermat) Un primo* p *tiene la forma* $x^2 - 2y^2$ *con* x, y *en* $\mathbb{Z}$ *sí y solo sí* $p \equiv \pm 1 \mod 8$ *o* $p = 2$.

Teorema 1.0.4. *(Legendre) Sea un número entero positivo* n *en la forma* $4^a n'$ *con* $a \leq 0$ *y* $n' \not\equiv 0 \mod 4$ *Entonces* n *es una suma de tres enteros cuadrados sí y solo sí* $n' \not\equiv 7 \mod 8$.

Teorema 1.0.5. *(Lagrange) Cada entero positivo es suma de cuatro enteros cuadrados.*

Las forma cuadráticas sobre $\mathbb{Q}$ son algunas veces suficientes para responder preguntas sobre formas cuadráticas sobre $\mathbb{Z}$. Aquí hay dos resultados más al respecto.

Teorema 1.0.6. *Si un entero es suma de dos racionales cuadrados entonces es suma de dos enteros cuadrados.*

Teorema 1.0.7. *Si un entero es suma de tres racionales cuadrados entonces es suma de tres enteros cuadrados.*

La motivación de estudiar ecuaciones de coeficientes enteros son diversas.

Ejemplo 1.0.8. *La ecuación* $x^2 + y^2 = 1$ *tiene soluciones racionales cuando se toma la siguiente parametrización* $x = \dfrac{t^2-1}{t^2+1}$ *y* $y = \dfrac{2t}{t^2+1}$ *con* $t \in \mathbb{Q}$*. Por lo tanto, existen tantas soluciones como valores racionales tome* t*.*

En general, no siempre es posible obtener soluciones racionales de formas cuadráticas.

Ejemplo 1.0.9. *La ecuación* $x^2 + y^2 = 3$ *tiene muchas soluciones reales pero no tiene soluciones racionales.*
Supongamos que existan soluciones racionales, digamos que $a^2 + b^2 = 3$ *con* a *y* b *en* $\mathbb{Q}$
Por el teorema 1.0.6, 3 es suma de dos enteros cuadrados, lo cual es falso.

A continuación se detallan las fuentes teóricas de las que se obtuvo información.
El Capítulo 1 se cimentó teóricamente en

- The Hasse-Minkowski Theorem de Adam Gamzon [2].

El Capítulo 2 se cimentó teóricamente en

- Quadratic and Hermitian forms de Winfried Scharlau [7].
- The algebraic theory of quadratic forms de T.Y. Lam [5].

El Capítulo 3 se basó teóricamente en

- The Hasse-Minkowski Theorem de Adam Gamzon [2].
- Algebra de Serge Lang [8].
- Basic Algebra II de Nathan Jacobson [3].
- Algebraic extensions of fields de Paul McCarthy [6].
- A course in Arithmetic de J. P. Serre [9].
- Introducción a la Teoría de Números de Felipe Zaldívar [10]

El Capítulo 4 se cimentó teóricamente en

- The Hasse-Minkowski Theorem de Adam Gamzon [2].

- Number theory de Borevich and Shafarevich [1].
- Number theory: Fermat's dreams de Kato, Kurokawa and Saito [4].
- Introducción a la Teoría de Números de Felipe Salívar [10]

Capítulo 2

Teoría algebraica de Formas Bilineales y Cuadráticas

En este capítulo F denotará un cuerpo (conmutativo) de característica diferente de 2 y $F^\times$ denotará su grupo multiplicativo.
Todos los espacios vectoriales que se usen serán de dimensión finita sobre F.

2.1. Formas Bilineales

Definición 2.1.1. *Una* ***forma bilineal*** *sobre un espacio vectorial V de dimensión finita, es una función $b : V \times V \to F$ tal que:*

1. $b(x + x', y) = b(x, y) + b(x', y)$
2. $b(x, y + y') = b(x, y) + b(x, y')$
3. $b(\alpha.x, y) = b(x, \alpha.y) = \alpha.b(x, y)$

para todo x, x', y, y' en V y todo $\alpha \in F$, es decir, b es una función lineal en ambos argumentos.
b es llamada una ***forma bilineal simétrica****, si $b(x, y) = b(y, x)$.*

De la bilinealidad de una forma bilineal simétrica b se deduce fácilmente la siguiente relación:

$$b(x+y, x+y) = b(x,x) + b(y,y) + 2.b(x,y)$$

Si la característica de F es distinta de 2, se obtiene:

$$b(x,y) = \frac{1}{2}(b(x+y, x+y) - b(x,x) - b(y,y)) \tag{2.1}$$

para todo x, y en V.

La expresión (2.1) se conoce como la **identidad polar** y establece que una forma bilineal simétrica está determinada totalmente cuando se conoce la forma bilineal sobre la "diagonal" de $V \times V$.

Definición 2.1.2. *El par (V, b) es llamado un **espacio bilineal simétrico** (sobre F) o solamente, **espacio bilineal** para abreviar.*

Ejemplo 2.1.3. *Sea $b : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ el producto escalar usual sobre $\mathbb{R}^n$, definido por:*

$$b(x,y) = x.y = x_1.y_1 + x_2.y_2 + ... + x_n.y_n$$

donde $x = (x_1, x_2, ..., x_n)$ y $y = (y_1, y_2, ..., y_n)$, es una forma bilineal simétrica sobre $\mathbb{R}^n$.

Ejemplo 2.1.4. *Sea F un cuerpo y $b : F^n \times F^n \longrightarrow F$ una aplicación definida por*

$$b(x,y) = \sum_{i,j=1}^{n} a_{i,j} x_i y_j$$

donde $x = (x_1, x_2, ..., x_n)$ y $y = (y_1, y_2, ..., y_n)$ son n-dimensional y $a_{i,j} \in F$.

La aplicación b es una forma bilineal sobre K^n.

Ejemplo 2.1.5. *Sea $A = [a_{i,j}]$ una matriz de tipo $n \times n$ sobre un cuerpo F y sea $E = \{e_1, ..., e_n\}$ una base fijada de F^n.*

Definimos la aplicación $b_A : F^{n\times 1} \times F^{n\times 1} \longrightarrow F$ *por:*

$$\begin{aligned} b_A(x,y) &= [x]_E^t . A[y]_E \\ &= [x_1,...,x_n]_E . \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}_E \\ &= \sum_{i,j=1}^{n} a_{i,j} x_i y_j \end{aligned}$$

Por el ejemplo anterior, b_A *es una forma bilineal sobre* $F^{n\times 1}$.

b_A *denotará la* ***forma bilineal inducida por una matriz*** A *de tipo* $n \times n$.

Si la matriz A *es simétrica, el espacio bilineal inducido por* b_A *y por* A*, será denotado por* $\langle A \rangle$ *en lugar de* $(F^{n\times 1}, b_A)$.

El concepto de espacio bilineal es una generalización del concepto de espacio Euclidiano y algunos conceptos importantes de la geometría euclidiana pueden ser también introducidos en este contexto general.
En lo que sigue (V, b) siempre denotará un espacio bilineal simétrico.

Consideremos dos espacios vectoriales finitos dimensionales V y W sobre K. Sabemos por álgebra lineal que el conjunto de todas las transformaciones lineales de V en W es un espacio vectorial finito dimensional sobre F de un modo natural. Este conjunto será denotado por $L_F(V,W)$ o simplemente, $L(V,W)$. Cuando $V = W$, la composición de transformaciones lineales provee a $L(V,W)$ de una ley multiplicativa que le da una estructura de anillo con identidad, por lo que se usará la notación $L_F(V)$, $L_n(V)$ o $L(V)$ en lugar de $L_F(V,V)$ donde $n = dim(V)$. Los escalares y la ley de multiplicación en $L(V)$ son definidas así:

$$\alpha(\tau \circ \sigma) = (\alpha.\tau) \circ \sigma = \tau \circ (\alpha.\sigma)$$

para todo $\alpha \in F$ y para todo $\tau, \sigma \in L(V)$. Las transformaciones lineales invertibles en $L_F(V)$ forman un grupo llamado el **grupo lineal general** denotado por $GL_F(V)$, $GL_n(V)$ o $GL(V)$.

Definición 2.1.6. *Tenemos:*

1. *Dos* ***vectores*** x, y *en* V *son* ***ortogonales*** *(o perpendiculares a cada uno), si* $b(x, y) = b(y, x) = 0$.

2. *Dos* ***conjuntos*** X, Y *de* V *son llamados* ***ortogonales****, si sus respectivos elementos son todos ortogonales respecto a la forma bilineal* b *o equivalentemente:* $b(x, y) = 0 \ \forall x \in X, \forall y \in Y$

   Ortogonalidad lo denotaremos por $\perp$*:* $x \perp y, X \perp Y$*, etc.*

3. *Con cada subconjunto* X *de* V *está asociado su* ***espacio ortogonal***

$$X^{\perp} = \{x \in V / x \perp X\}.$$

   En la literatura, $X^{\perp}$ *es llamada después el* ***complemento ortogonal****, un término que usaremos solo en casos especiales.*

Lema 2.1.7. $X^{\perp}$ *es un subespacio de* V

Demostración. En efecto

- Para $\theta \in X$ y cualquier $x \in X$ se tiene

$$b(\theta + \theta, x) = b(\theta, x) + b(\theta, x)$$

  entonces, $b(\theta, x) = b(\theta, x) + b(\theta, x)$

  lo que implica que: $b(\theta, x) = 0 \quad \forall x \in X$

  O sea, $\theta \perp X$ entonces $\theta \in X^{\perp}$, por lo que $X^{\perp} \neq \emptyset$.

- Sean y, y' en $X^{\perp}$ entonces $b(y, x) = b(y', x) = 0, \quad \forall x \in X$

  luego $b(y + y', x) = \underbrace{b(y, x)}_{0} + \underbrace{b(y', x)}_{0} = 0$ con $x \in X$ cualquiera.

  por lo tanto, $y + y' \in X^{\perp}$.

- Sean $y \in X^{\perp}, \alpha \in K$ entonces $\alpha \in K$ y $b(y, x) = 0, \forall x \in X$

  luego $b(\alpha y, x) = \alpha . b(y, x) = \alpha . 0 = 0$ con $x \in X$ cualquiera

  por lo tanto, $\alpha . y \in X^{\perp}$.

□

Es claro de la definición que

1. $X \subset Y$ implica $Y^{\perp} \subset X^{\perp}$
2. $X \subset X^{\perp\perp}$

Demostración. 1. Supongamos que $X \subset Y$

$$\begin{aligned} z \in Y^{\perp} &\Rightarrow b(z,y) = 0 \text{ para todo } y \in Y \\ &\Rightarrow b(z,y) = 0 \text{ para todo } y \in X \\ &\Rightarrow z \in X^{\perp} \end{aligned}$$

Por lo tanto $Y^{\perp} \subset X^{\perp}$

2. Tenemos que:

$$\begin{aligned} z \in X &\Rightarrow b(z,y) = 0 \text{ para todo } y \in X^{\perp} \\ &\Rightarrow z \in (X^{\perp})^{\perp} = X^{\perp\perp} \end{aligned}$$

Por lo tanto $X \subset X^{\perp\perp}$

□

Si W es un subespacio de V entonces $(W, b|_{W\times W})$ es un espacio bilineal simétrico, subespacio de (V, b). En lugar de $(V, b|_{W\times W})$ por simplicidad escribiremos $b|_W$.

Definición 2.1.8. *Sean (V, b) y (V', b') espacios bilineales simétricos. Una transformación lineal inyectiva es llamada una* ***isometría*** *si*

$$b'(\sigma(x), \sigma(y)) = b(x, y), \quad \forall x, y \text{ en } V$$

Proposición 2.1.9. *La composición de isometrías es una isometría.*

Demostración. En efecto, sean $(V, b), (V', b')$ y (V'', b'') espacios bilineales simétricos tales que $\sigma : V \to V'$ y $\tau : V' \to V''$ son isometrías entonces, $\tau \circ \sigma : V \to V''$ es una transformación lineal inyectiva tal que para cualquier x, y en V se tiene que:

$$\begin{aligned} b''((\tau\circ\sigma)(x), (\tau\circ\sigma)(y)) &= b''((\tau(\sigma(x))), (\tau(\sigma(y)))) \\ &= b'(\sigma(x), \sigma(y)) && \ldots \ \tau \text{ es isometría} \\ &= b(x, y) && \ldots \ \sigma \text{ es isometría} \end{aligned}$$

Por lo tanto, $\tau \circ \sigma : V \to V''$ es una isometría. □

Definición 2.1.10. *Los* ***espacios*** (V, b) *y* (V', b') *son llamados* ***isométricos*** *o* ***isomorfos****, denotados por* $(V, b) \cong (V', b')$*, si existe una isometría biyectiva* $\sigma : V \to V'$*.*

Observación 2.1.11. *De la definición, se implica que los Espacios vectoriales* V *y* V' *son de la misma dimensión, pues siendo* σ *inyectiva y epiyectiva, se tiene que* $Ker(\sigma) = \{\theta\}$ *luego* $dim(V) = \underbrace{dim Ker(\sigma)}_{0} + dim \underbrace{Im(\sigma)}_{V'}$

Así: $dim(V) = dim(V')$*.*

La relación $\cong$ (isométrico) es de equivalencia.

Demostración. En efecto,

- reflexiva: Sea (V, b) un espacio bilineal simétrico luego $id_V : V \to V$ es isometría biyectiva entonces se tiene que $(V, b) \cong (V, b)$

- simétrica: Sean (V, b) y (V', b') espacios bilineales simétricos tales que $(V, b) \cong (V', b')$ entonces existe $\sigma : V \to V'$ isometría biyectiva
  luego $\sigma^{-1} : V' \to V$ es isomorfismo lineal tal que para cualquier x', y' en V', existen x, y en V tal que $\sigma(x) = x'$ y $\sigma(y) = y'$.
  Ahora,

$$\begin{aligned} b(\sigma^{-1}(x'), \sigma^{-1}(y')) &= b(\sigma^{-1}(\sigma(x)), \sigma^{-1}(\sigma(y))) && \dots \ \sigma \text{ es suryectiva} \\ &= b(\sigma^{-1} \circ \sigma)(x), \sigma^{-1} \circ \sigma)(y)) \\ &= b(x, y) \\ &= b'(\sigma(x), \sigma(y)) && \dots \ \sigma \text{ es isometría} \\ &= b'(x', y') && \dots \ \sigma \text{ es función} \end{aligned}$$

- transitiva: En efecto, sean $(V, b), (V', b')$ y (V'', b'') espacios bilineales simétricos tales que $(V, b) \cong (V', b')$ y $(V', b') \cong (V'', b'')$ entonces existen $\sigma : V \to V'$ y $\tau : V' \to V''$ isometrías biyectivas por lo que $\tau \circ \sigma : V \to V'$ es una isometría y a la vez, una función biyectiva ,por lo que $\tau \circ \sigma : V \to V'$ es isometría biyectiva, es decir, $(V, b) \cong (V'', b'')$

□

Con respecto a la composición de isometrías $\sigma : V \to V$, ellas forman un grupo llamado el **grupo ortogonal** o el **grupo de automorfismo** de (V, b). Este grupo será denotado por $O(V, b)$ o $Aut(V, b)$. Los elementos del grupo ortogonal son llamados **transformaciones ortogonales**.

Observación 2.1.12. *$O(V, b)$ es subgrupo de $GL(V)$*

Demostración. Tenemos que:

- Como $id : V \to V$ es isometría biyectiva, entonces $O(V, b) \neq \emptyset$
- $$\begin{aligned} \text{Sean } \sigma, \tau \in O(V, b) &\implies \sigma, \tau : V \to V \text{ son isometrías biyectivas} \\ &\implies \sigma \circ \tau : V \to V \text{ es isometría biyectiva} \\ &\implies \sigma \circ \tau \in O(V, b) \end{aligned}$$
- $$\begin{aligned} \text{Sea } \sigma \in O(V, b) &\implies \sigma : V \to V \text{ es una isometria biyectiva} \\ &\implies \sigma^{-1} : V \to V \text{ es una isometría biyectiva} \\ &\implies \sigma^{-1} \in O(V, b) \end{aligned}$$

□

Vectores ortogonales son llevados a vectores ortogonales, vía una isometría.

Demostración. En efecto, sean (V, b) y (V', b') dos espacios bilineales simétricos y $\sigma : V \to V'$ una isometría.
Si x, y son elementos cualesquiera de V tales que son ortogonales entonces:

$$b'(\underbrace{\sigma(x)}_{\in V'}, \underbrace{\sigma(y)}_{\in V'}) = \underbrace{b(x, y)}_{x \perp y} = 0$$

por lo que: $\sigma(x) \perp \sigma(y)$ en V' □

En particular, para cada subconjunto X de V, $\sigma(X^{\perp}) \subset [\sigma(X)]^{\perp}$

Demostración. En efecto, sea $z \in \sigma(X^{\perp})$ entonces existe $y \in X^{\perp}$ tal que $z = \sigma(y)$

entonces $z = \sigma(y) \quad \wedge \quad b(x,y) = 0, \quad \forall x \in X$

Para $y \in X^{\perp}$ y para cualquier $\sigma(x) \in \sigma(X)$, se tiene:

$$\begin{aligned} b'(\sigma(x), z) &= b'(\sigma(x), \sigma(y)) \\ &= b(x,y) \qquad\qquad \ldots \ \sigma \text{ es isometría} \\ &= 0 \end{aligned}$$

Por lo tanto, $z \in [\sigma(X)]^{\perp}$ □

Si σ es una isometría biyectiva se tiene que $\sigma(X^{\perp}) = (\sigma(X))^{\perp}$.

Dos de los problemas esenciales en la teoría de los espacios bilineales simétricos son:

1. Dado un cuerpo F, determinar las clases de isometrías de espacios bilineales simétricos sobre F y
2. determinar la estructura del grupo ortogonal (abeliano, de Sylow, etc)

Lema 2.1.13. *Si* $(V,b) \cong (V',b')$ *entonces* $O(V,b) \cong O(V',b')$

Demostración. Si $(V,b) \cong (V',b')$ entonces existe $\sigma : V \to V'$ isometría biyectiva.

Sea $\tau \in O(V,b)$ entonces $\tau : V \to V$ es isometría.

Definimos

$$\begin{aligned} \phi : O(V,b) &\to O(V',b') \\ \tau &\mapsto \phi(\tau) = \sigma \circ \tau \circ \sigma^{-1} \end{aligned}$$

$$\begin{array}{ccc} V & \xrightarrow{\tau} & V \\ {\scriptstyle \sigma^{-1}}\uparrow & & \downarrow{\scriptstyle \sigma} \\ V' & \xrightarrow[\sigma\circ\tau\circ\sigma^{-1}]{} & V' \end{array}$$

Buena definición Como σ es biyectiva (isometría)

$$\left.\begin{array}{ll} \sigma^{-1} : V' \to V & \text{isometría inyectiva} \\ \tau : V \to V & \text{isometría inyectiva} \\ \sigma : V \to V & \text{isometría inyectiva} \end{array}\right\} \text{ entonces } \sigma \circ \tau \circ \sigma^{-1} : V' \to V' \text{ es isometría}$$

biyectiva.

Por lo tanto, $\phi(\tau) \in O(V',b')$

ϕ es isomorfismo de grupos

- Sean $\theta, \gamma \in O(V,b)$ tales que $\phi(\theta) = \phi(\gamma)$ entonces

$$\sigma \circ \theta \circ \sigma^{-1} = \sigma \circ \gamma \circ \sigma^{-1}$$

aplicando elemento inverso de σ respecto a $\circ$ tenemos, $\quad \theta = \gamma$

- Dado $\gamma \in O(V',b')$ cualquiera, se tiene que $\gamma : V' \to V'$ es isometría biyectiva, por lo que $\sigma^{-1} \circ \gamma \circ \sigma \in O(V,b)$

$$\begin{array}{ccc} V' & \xrightarrow{\gamma} & V' \\ {\scriptstyle\sigma}\uparrow & & \downarrow{\scriptstyle\sigma^{-1}} \\ V & \xrightarrow[\sigma^{-1}\circ\gamma\circ\sigma]{} & V \end{array}$$

luego $\phi(\sigma^{-1} \circ \gamma \circ \sigma) = \sigma \circ (\sigma^{-1} \circ \gamma \circ \sigma) \circ \sigma^{-1} = \gamma$

- Sean $\theta, \gamma \in O(V,b)$ entonces

$$\begin{aligned} \phi(\theta \circ \gamma) &= \sigma \circ (\theta \circ \gamma) \circ \sigma^{-1} \\ &= (\sigma \circ \theta \circ \sigma^{-1}) \circ (\sigma \circ \gamma \circ \sigma^{-1}) \\ &= \phi(\theta) \circ \phi(\gamma) \end{aligned}$$

Por lo tanto, $O(V,b) \cong O(V',b')$ □

Definición 2.1.14. *Sea V un espacio vectorial sobre F. Una función $q : V \to V'$ es llamada una* ***forma cuadrática*** *sobre V si:*

1. $q(\alpha.x) = \alpha^2.q(x)$
2. $b_q(x,y) = \frac{1}{2}[q(x+y) - q(x) - q(y)]$ *es una forma bilineal (necesariamente simétrica).*

b_q es llamado la **forma bilineal asociado a** q.
El par (V,q) es llamado **el espacio cuadrático**.
Si b es una forma bilineal, b^t denota la **forma bilineal transpuesta** definida por $b^t(x,y) = b(y,x)$.
b es simétrica precisamente cuando $b = b^t$.

Definición 2.1.15. *Si b es una forma bilineal sobre V entonces $q_b : V \to K$ definida por $q_b(x) = b(x, x)$ es una forma cuadrática (como es fácilmente comprobado con un simple cálculo).*

q_b es llamado la ***forma cuadrática asociada con*** *b.*

Lema 2.1.16. *Si b es una forma bilineal y q es una forma cuadrática sobre V entonces $b_{q_b} = \frac{1}{2}(b + b^t)$ y $q_{b_q} = q$.*
En particular, $b_{q_b} = b$ cuando b es simétrica.

Demostración. Tenemos:

$$\begin{aligned} b_{q_b}(x, y) &= \frac{1}{2}(q_b(x + y) - q_b(x) - q_b(y)) \\ &= \frac{1}{2}(b(x + y, x + y) - b(x, x) - b(y, y)) \\ &= \frac{1}{2}(b(x, y) + b(y, x)) \\ &= \frac{1}{2}(b(x, y) + b^t(x, y)) \\ &= \frac{1}{2}(b + b^t)(x, y) \end{aligned}$$

también

$$\begin{aligned} q_{b_q}(x) = b_q(x, x) &= \frac{1}{2}(q(x + x) - q(x) - q(x)) \\ &= \frac{1}{2}(q(2x) - 2.b(x)) \\ &= \frac{1}{2}(4.b(x) - 2.b(x)) \\ &= q(x) \end{aligned}$$

□

Observación 2.1.17. *Sobre las bases de este lema, se puede identificar formas cuadráticas (respectivamente espacios cuadráticos) con formas bilineales simétricas (respectivamente espacios bilineales simétricos) mediante las correspondientes inversas:*

$$(V, b) \to (V, q_b), (V, q) \to (V, b_q).$$

Por lo tanto, todos los conceptos de espacios bilineales simétricos pueden ser llevados a espacios cuadráticos y recíprocamente. Por ejemplo, dos vectores en un espacio cuadrático (V, q) son ortogonales cuando son ortogonales con respecto a b_q, etc.

El concepto de isometría tampoco produce nada nuevo: una isometría entre dos espacios cuadráticos (V, q) y (V', q') se define como una transformación lineal inyectiva $\sigma : V \to V'$ que satisface $q'(\sigma(x)) = q(x), \forall x \in V$.

Una transformación $\sigma : V \to V'$ es una isometría, precisamente cuando sea una isometría con respecto a b_q. Recíprocamente, una isometría de espacios bilineales simétricos es también una isometría de sus espacios cuadráticos asociados. A pesar que esto es después usado para distinguir entre los dos conceptos. Sobre los cuerpos de característica 2, las formas cuadráticas y formas bilineales simétricas son esencialmente diferentes.

2.2. Notación matricial

Supongamos que $dimV = n$ y sea $E = \{e_1, e_2, \cdots, e_n\}$ una base del espacio vectorial V.

Si b es una forma bilineal sobre V entonces:

$$B = B_{b,E} = (b(e_i, e_j)) = (b_{ij})$$

es llamado la **matriz de** b con **respecto a la base** E o simplemente **matriz de representación**. La matriz de b^t es claramente la matriz transpuesta B^t. En particular, b es simétrica precisamente cuando B es simétrica.

Para:

$$v = \sum_{i=1}^{n} x_i e_i, \quad w = \sum_{j=1}^{n} y_j . e_j$$

en V tenemos:

$$b(v, w) = b\left(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i b(e_i, e_j) y_j$$

$$b(v, w) = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}_E \begin{bmatrix} b(e_1, e_1) & b(e_1, e_2) & ... & b(e_1, e_n) \\ b(e_2, e_1) & b(e_2, e_2) & ... & b(e_2, e_n) \\ \vdots & \vdots & \ddots & \vdots \\ b(e_n, e_1) & b(e_n, e_2) & ... & b(e_n, e_n) \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}_E$$

o sea $b(v,w) = [v]_E^t.B.[w]_E$ donde identificamos a $[v]_E$ y $[w]_E$ con los correspondientes vectores columna coordenados de v y w respectivamente en la base E.

Observación 2.2.1. *La aplicación* $[.]_E : V \longrightarrow F^n$ *es un isomorfismo lineal, donde si*

$$v = \sum_{i=1}^{n} x_i e_i \Longrightarrow [v]_E = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Para $E' = \{e'_1, e'_2, \cdots, e'_n\}$ una segunda base de V y T la matriz cambio de base de E y E', tenemos

$$e'_j = \sum_{i=1}^{n} t_{ij} e_i$$

con $j = 1, 2, ..., n$ y $T = (t_{ij})$. Calculemos la matriz de b respecto a E'

Lema 2.2.2. *Siendo* T *la matriz cambio de base de* E *a* E'*, se tiene que* $B_{b,E'} = T^t.B_{b,E}.T$.

Demostración. Siendo $T = [t_{ij}]_{n\times n}$, sea $T^t = [r_{ij}]_{n\times n}$ con $r_{ij} = t_{ji}$ y $B_{b,E'} = [b(e'_i, e'_j)] \quad i,j = 1, 2, ..., n$ luego

$$\begin{aligned} b(e'_i, e'_j) &= b(\textstyle\sum_{k=1}^n t_{ki} e_k, \sum_{l=1}^n t_{lj} e_l) \qquad i,j = 1,2,...,n \\ &= \textstyle\sum_{k=1}^n \sum_{l=1}^n t_{ki}.t_{lj} b(e_k, e_l) \qquad i,j = 1,2,...,n \\ &= \textstyle\sum_{k=1}^n t_{ki} (\sum_{l=1}^n b(e_k, e_l) t_{lj}) \quad i,j = 1,2,...,n \end{aligned}$$

Hagamos un cambio ,

$$c_{kj} = \sum_{l=1}^{n} b(e_k, e_l) t_{lj}, \quad k,j = 1,2,...,n$$

Así,

$$\begin{aligned} B_{b,E'} &= [b(e'_i, e'_j)] && i,j = 1,2,...,n \\ &= [\textstyle\sum_{k=1}^{n} t_{ki}.c_{kj}] && i,j = 1,2,...,n \\ &= [\textstyle\sum_{k=1}^{n} r_{ik}.c_{kj}] && i,j = 1,2,...,n \\ &= [r_{ij}][c_{ij}] && i,j = 1,2,...,n \\ &= T^t.[\textstyle\sum_{l=1}^{n} b(e_k, e_l)t_{lj}] && i,j = 1,2,...,n \\ &= T^t.[b(e_i, e_j)][t_{ij}] && i,j = 1,2,...,n \\ &= T^t.B_{b,E}.T \end{aligned}$$

□

Como es conocido, dos matrices de orden $n \times n$, A y B son llamadas **congruentes** si existe una matriz invertible T tal que $B = T^t.A.T$. La matriz de un espacio bilineal (V, b) está entonces bien definida salvo congruencias.

Si (V, b) y (V', b') son dos espacios bilineales con bases $E = \{e_1, e_2, \cdots, e_n\}$ y $E' = \{e'_1, e'_2, \cdots, e'_m\}$ respectivamente entonces por el teorema de la existencia de las transformaciones lineales, una transformación lineal $\sigma : V \to V'$ es determinada por una matriz $S = [s_{ij}]$ de orden $m \times n$ donde

$$\sigma(e_j) = \sum_{i=1}^{m} s_{ij}.e'_i$$

Teorema 2.2.3. *Dos espacios bilineales son isomorfos si y solo si, sus matrices asociadas simétricas (con respecto a bases arbitrarias) son congruentes.*

Demostración. Supongamos que (V, b) y (V', b') sean espacios bilineales tales que $dimV = dimV' = n$ y que además E y E' sean sus bases respectivamente. ($\Rightarrow$)Supongamos que $(V, b) \cong (V', b')$ entonces existe una isometría biyectiva $\sigma : V \to V'$.
Siendo σ biyectiva, con respecto a las bases E y E', sea $S = [s_{ij}]$ su matriz asociada invertible, por lo que $[\sigma(x)]_{E'} = S[x]_E$.

Para x, y en V cualesquiera,

$$\begin{aligned}
[x]_E^t B_{b,E}[y]_E &= b(x,y) && \ldots \text{ def. de b} \\
&= b'(\sigma(x),\sigma(y)) && \ldots \ \sigma \text{ es isometría} \\
&= [\sigma(x)]_{E'}^t B_{b',E'}[\sigma(y)]_{E'} && \ldots \text{ def. de } b' \\
&= (S[x]_E)^t . B_{b',E'}(S[y]_{E'}) && \ldots \text{ def. de } \sigma \\
&= [x]_E^t . (S^t . B_{b',E'} . S)[y]_{E'} && \ldots \ \text{transpuesta}
\end{aligned}$$

luego $B_{b,E} = S^t . B_{b',E} . S$ con $S \in K^{n\times n}$ invertible

entonces $B_{b,E}$ y $B_{b',E}$ son congruentes.

($\Leftarrow$) Supongamos que las matrices asociadas de b y b' son congruentes entonces existe una matriz invertible $S \in F^{n\times n}$ que satisface $\quad B_{b,E} = S^t . B_{b',E} . S$.

Definimos la aplicación $\sigma : V \to V'$ por $[\sigma(x)]_{E'} = S[x]_E$, veamos que es una isometría biyectiva.

- <u>σ es isometría</u>
  - Consideremos el sistema lineal $S[x]_{E'} = \theta_{E'}$, como S es invertible $Ker(\sigma) = \theta_{E'}$
  - Se cumple que:

$$\begin{aligned}
b'(\sigma(x),\sigma(y)) &= [\sigma(x)]_{E'}^t B_{b',E'}[\sigma(y)]_{E'} \\
&= (S[x]_E)^t . B_{b',E'}(S[y]_E) \\
&= ([x]_E^t S^t) B_{b',E'}(S[y]_E) \\
&= [x]_E^t (S^t B_{b',E'} S)[y]_E \\
&= [x]_E^t B_{b,E}[y]_E \\
&= b(x,y)
\end{aligned}$$

- <u>σ es suryectiva</u> En efecto, para $[y]_{E'} \in V'$, existe $S^{-1}[y]_{E'}$ en V tal que $\sigma(S^{-1}[y]_{E'}) = S(S^{-1}[y]_{E'} = [y]_{E'}$

Así $\sigma : V \to V'$ es una isometría biyectiva, por lo tanto $(V, b) \cong (V', b')$ $\square$

Corolario 2.2.4. *Para $\sigma : V \to V$ y S su matriz asociada, se tiene que:*

$$O(V,b) \cong \{S \in F^{n\times n} / det(S) \neq 0 \wedge B = S^t B S\}$$

Demostración.

$$\begin{aligned} \sigma \in O(V,b) &\iff \sigma \text{ es isometría inyectiva} \\ &\iff \sigma \text{ es isometría biyectiva} \\ &\iff S \text{ es invertible} \qquad\qquad ... \quad L(V) \cong F^{n\times n} \\ &\iff det(S) \neq 0 \end{aligned}$$

Por la proposición anterior, tenemos que:
$(V,b) \cong (V,b) \iff B_{b,E} = S^t B_{b,E} S$ con $S \in F^{n\times n}$ y $det(S) \neq 0$ □

Tenemos así descrito el grupo ortogonal como un grupo de matrices. esto después lo usaremos para cálculos concretos.

Consideremos ahora el espacio vectorial $F^{n\times 1}$ de los vectores columna con coeficientes en F. Si B es una matriz simétrica de orden $n \times n$ entonces $b_B : F^{n\times 1} \times F^{n\times 1} \to F$ definido por: $b_B(x,y) = x^t B y$ es una forma bilineal simétrica.
El espacio bilineal $(F^{n\times 1}, b_B)$ será denotado por $\langle B \rangle$.
Si (V,b) es un espacio bilineal arbitrario, $E = \{e_1, ..., e_n\}$ una base de V y B la matriz asociada de b entonces $(V,b) \cong \langle B \rangle$.

Teorema 2.2.5. *Existe una correspondencia biyectiva canónica entre las clases isométricas de espacios bilineales simétricos y las clases de matrices simétricas congruentes.*

Demostración. Sean b y b' dos formas bilineales simétricas sobre F además sean B y B' sus respectivas matrices asociadas en diferentes bases de V $(dimV = n)$

$$\begin{aligned} (V,b) \cong (V,b') \quad &\Leftrightarrow \quad (F^{n\times 1}, b_B) \cong (F^{n\times 1}, b_{B'}) \\ &\Leftrightarrow \quad \langle B \rangle \cong \langle B' \rangle \\ &\underbrace{\Leftrightarrow}_{Teo2,2,3} \quad B \sim B' \end{aligned}$$

□

Cada problema sobre formas cuadráticas puede ser tratado en términos de matrices sobre los fundamentos de este hecho. Sea V un espacio vectorial, V^* denota su **espacio dual**, el espacio vectorial de todas las funcionales lineales de V en F. Si $\{e_1, e_2, \cdots, e_n\}$ es una base de V entonces $\{e_1^*, e_2^*, \cdots, e_n^*\}$ denota la base dual de V^* definido por:

$$e_i^*(e_j) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Definición 2.2.6. *Sea (V, b) un espacio bilineal entonces $\tilde{b} : V \to V^*$ definido por:*

$$(\tilde{b}(x))(y) = b(x, y)$$

es llamado la ***transformación adjunta****.*

Observación 2.2.7. *$\tilde{b}$ es una transformación lineal.*

Demostración. En efecto, sean a, c en F y x, y en V arbitrarios, entonces $ax + cy \in V$, por lo que $\tilde{b}(ax + cy) \in V^*$. Sea $z \in V$ cualesquiera fija, entonces:

$$\begin{aligned} (\tilde{b}(ax + cy))(z) &= b(ax + cy, z) \\ &= a.b(x, z) + c.b(y, z) \qquad \ldots \quad b \text{ es bilineal} \\ &= a(\tilde{b}(x))(z) + c(\tilde{b}(y))(z) \\ &= (a.\tilde{b}(x) + c.\tilde{b}(y))(z) \end{aligned}$$

Por lo que $\tilde{b}(ax + by) = a.\tilde{b}(x) + c.\tilde{b}(y)$ □

Lema 2.2.8. *Si $E = \{e_1, e_2, \cdots, e_n\}$ es una base de V y $E^* = \{e_1^*, e_2^*, \cdots, e_n^*\}$ es la base dual de V^* entonces la matriz asociada a $\tilde{b}$ con respecto a las bases E y E^* es la matriz $B_{b,E}$ de b con respecto a la base E.*

Demostración. Para cada $i = 1, 2, ..., n, \quad \tilde{b}(e_i) \in V^*$

entonces

$$\tilde{b}(e_i) = \sum_{j=1}^{n} (\tilde{b}(e_i))(e_j) e_j^*, \quad i = 1, 2, ..., n$$

luego

$$\tilde{b}(e_i) = \sum_{j=1}^{n} b(e_i, e_j) e_j^*, \quad i = 1, 2, ..., n$$

explícitamente, se tiene:

$$\begin{array}{rcccccc}
\tilde{b}(e_1) & = & b(e_1,e_1)e_1^* & + & b(e_1,e_2)e_2^* & +...+ & b(e_1,e_n)e_n^* \\
\tilde{b}(e_2) & = & b(e_2,e_1)e_1^* & + & b(e_2,e_2)e_2^* & +...+ & b(e_n,e_n)e_n^* \\
\vdots & & \vdots & & \vdots & \ddots & \vdots \\
\tilde{b}(e_n) & = & b(e_n,e_1)e_1^* & + & b(e_n,e_2)e_2^* & +...+ & b(e_n,e_n)e_n^*
\end{array}$$

así: $[\tilde{b}]_{E^*}^{E} = \begin{bmatrix} b(e_1,e_1) & b(e_1,e_2) & ... & b(e_1,e_n) \\ b(e_2,e_1) & b(e_2,e_2) & ... & b(e_2,e_n) \\ \vdots & \vdots & \ddots & \vdots \\ b(e_n,e_1) & b(e_n,e_2) & ... & b(e_n,e_n) \end{bmatrix}_{n\times n}$

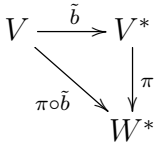
$[\tilde{b}]_{E^*}^{E} = B_{b,E} = B$ □

Lema 2.2.9. *Si W es un subespacio del espacio bilineal (V,b) entonces se tiene que $W^{\perp} = Ker(\pi \circ \tilde{b})$ donde $\pi : V^* \to W^*$ denota la proyección canónica.*

Demostración. Notemos que

$$\begin{array}{rccc} \pi: & V^* & \to & W^* \\ & g & \mapsto & \pi(g) = g|_W \end{array}$$, es decir, π restringe a W

Siguiendo el diagrama conmutativo



tenemos:

$$\begin{array}{rcl}
x \in W^{\perp} & \iff & b(x,y) = 0 \quad \forall y \in W \\
& \iff & (\tilde{b}(x))(y) = 0 \quad \forall y \in W \\
& \iff & \tilde{b}(x)|_W = \theta_{W^*} \quad \forall y \in W \\
& \iff & \pi(\tilde{b}(x)) = \theta_{W^*} \\
& \iff & (\pi \circ \tilde{b})(x) = \theta_{W^*} \\
& \iff & x \in Ker(\pi \circ \tilde{b})
\end{array}$$

Por lo tanto, $W^{\perp} = Ker(\pi \circ \tilde{b})$ □

2.3. Espacios Regulares y Descomposición Ortogonal

Definición 2.3.1. *Un **espacio bilineal simétrico** (V, b) es llamado **regular** (o **no degenerado** o **no singular**) si $V^{\perp} = \{\theta_V\}$, es decir, para cada vector $x \neq 0$, existe $y \in V$ tal que $b(x, y) \neq 0$; entonces en un espacio regular solo el vector cero es perpendicular a todos los otros vectores.*

*El subespacio $V^{\perp}$ es llamado el **radical** de (V, b) denotado por **rad V**.*

*Un **subespacio** W es llamado **regular**, si (W, b_W) es regular.*

*Si (V, b) no es regular se llama **singular**.*

Corolario 2.3.2. *(V, b) es regular precisamente cuando $\tilde{b}$ es un isomorfismo o equivalentemente cuando la matriz B de b (son respecto a una base arbitraria) es invertible.*

Demostración. ($\Rightarrow$) Ya sabemos que $\tilde{b} : V \to V^*$ es transformación lineal.

$$\begin{aligned} x \in Ker(\tilde{b}) &\implies \tilde{b}(x) = \theta_{V^*} \\ &\implies [\tilde{b}(x)](y) = 0, \quad \forall y \in V \\ &\implies b(x, y) = 0, \quad \forall y \in V \\ &\implies x \in V^{\perp} = \{\theta_V\} \quad \text{... hipótesis} \end{aligned}$$

Así $Ker(\tilde{b}) = \{\theta\}$

Como $\tilde{b}$ es mono (acabamos de probar), tenemos $dimV = dimIm(\tilde{b})$ entonces $dimIm(\tilde{b}) = dimV^*$, también se tiene que: $Im(\tilde{b}) \subseteq V^*$

luego, $V^* = Im(\tilde{b})$

Por lo tanto, $\tilde{b}$ es isomorfismo.

($\Leftarrow$)En el Lema 2.2.9 usamos $W = V$ subespacio de V y $\pi = id_{V^*}$

$$\begin{aligned} V^{\perp} &= Ker(id_{V^*} \circ \tilde{b}) \\ &= Ker(\tilde{b}) = \{\theta_V\} \end{aligned}$$

luego (V, b) es regular.

Para matrices: $\tilde{b}$ es isomorfismo $\iff [\tilde{b}]_{E,E^*}$ es invertible $\iff B_{b;E}$ es invertible $\square$

Si V es un espacio vectorial con subespacios $V_1, ..., V_n$ entonces decimos que V es

la **suma (interna) directa de** $V_1, ..., V_n$ y se escribe como $V = V_1 \oplus ... \oplus V_n$, en este caso $x \in V$ puede ser escrito de manera única como

$$x = \sum_{i=1}^{n} x_i, \quad x_i \in V_i$$

Para $n = 2$, esta condición significa que $V = V_1 + V_2$ y $V_1 \cap V_2 = \{\theta_V\}$, decimos entonces que V_1 y V_2 son **subespacios complemantarios de** V.
Este concepto tiene la siguiente analogía para espacios bilineales.

Definición 2.3.3. *Sean V_1 y V_2 dos subespacios de (V, b). Decimos que V es la **suma (interna) ortogonal de** V_1 y V_2 si $V = V_1 \oplus V_2$ y $V_1 \perp V_2$. En este caso decimos que V_1 y V_2 son **subespacios complementarios de** (V, b) y se denota como $V = V_1 \perp V_2$. Análogamente de un modo general, $V = V_1 \perp ... \perp V_n$ si $V = V_1 \oplus ... \oplus V_n$ y $V_i \perp V_j$ para $i \neq j$, dicha descomposición es llamada también **descomposición ortogonal de** (V, b).*

Lema 2.3.4. *Si W es un subespacio regular de (V, b) entonces se tiene que $V = W \perp W^{\perp}$.*

Demostración. Para $x \in W$ y para cada $y \in W^{\perp}$ se tiene que $b(x, y) = 0$, por lo que $W \perp W^{\perp}$.
Veamos que $V = W \oplus W^{\perp}$
Por el corolario 2.3.2, (W, b_W) es regular si y solo si $\tilde{b}_W : W \longrightarrow W^*$ es isomorfismo, entonces $Ker(\tilde{b}_W) = \{\theta_V\}$

$$\begin{aligned} \text{Sea } x \in W \cap W^{\perp} &\implies x \in W \text{ y } x \in W^{\perp} = \underbrace{Ker(\pi \circ \tilde{b})}_{\text{lema 2.2.9}} \\ &\implies x \in W \text{ y } x \in Ker(\pi \circ \tilde{b}) \\ &\implies x \in W \text{ y } x \in Ker(\tilde{b}_W) = \{\theta_V\} \\ &\implies x = \theta_V \end{aligned}$$

Por lo tanto, $W \cap W^{\perp} = \{\theta_V\}$

Es claro que $W + W^{\perp} \subseteq V$, debemos probar que $V \subseteq W + W^{\perp}$
Sea $x \in V$ cualquiera entonces $\tilde{b}(x) \in V^*$ luego $f = \tilde{b}(x)|_W \in W^*$.

Como W es regular, por corolario 2.3.2, $\tilde{b}_W : W \longrightarrow W^*$ es isomorfismo (en particular epiyectiva) entonces para $f \in W^*$ existe $y \in W$ tal que $\tilde{b}_W(y) = f$.

Para todo $z \in W$:

$$b(x,z) = [\tilde{b}(x)](z) = [\tilde{b}(x)|_W](z) = f(z) = [\tilde{b}_W(y)](z) = b(y,z)$$

luego $b(x-y,z) = 0$ para todo $z \in W$ entonces $x - y \in W^\perp$

Tenemos que $x = y + (x-y) \in W + W^\perp$, es decir $V \subseteq W + W^\perp$

Por lo tanto, $V = W + W^\perp$ □

Así por este lema, $W^\perp$ es llamado el **complemento ortogonal de** W.

Teorema 2.3.5. *Cada espacio bilineal simétrico (V,b) es la suma ortogonal de subespacios uni-dimensionales. En otras palabras V tiene una base de vectores ortogonales dos a dos (base ortogonal).*

Demostración.

- Caso I: $b \equiv \theta$

  Supongamos que $\{v_1, v_2, ..., v_n\}$ es una base de V entonces $b(v_i, v_j) = 0$ para $i \neq j$ y $1 \leq i, j \leq n$, además $V = \mathcal{L}\{v_1\} + \mathcal{L}\{v_2\} + ... + \mathcal{L}\{v_n\}$.

- Caso II: $b \not\equiv \theta$

  (Haciendo inducción sobre $dimV$)

  Si $dimV = 1$, sea $\{v\}$ una base de V entonces $V = \mathcal{L}\{v\}$

  Sea $n > 1$ y supongamos que el teorema se cumple para cualquier espacio vectorial de dimensión $n-1$ (hipótesis inductiva).

  Sea $dimV = n$, como $b \not\equiv \theta$, existen x, y en V tales que $b(x,y) \neq 0$

  equivalentemente, $\frac{1}{2}[b(x+y, x+y) - b(x,x) - b(y,y)] \neq 0$

  por lo que alguno de los sumandos no es nulo, así existe $v_1 \in V$ (que podría ser $x+y$, x ó y) tal que $b(v_1, v_1) \neq 0$.

  Consideremos el subespacio $W = \mathcal{L}\{v_1\}$

  Afirmación: (W, b_W) es regular.

  En efecto, sea $x \in W^\perp$ entonces $x \in W$ y $b_W(x, W) = 0$

por lo que $x = \alpha.v_1$ con $\alpha \in K$

En particular,

$$\begin{aligned} b_W(\alpha.v_1, \alpha.v_1) = 0 &\Rightarrow \alpha^2.b_W(v_1, v_1) = 0 \\ &\Rightarrow \alpha^2.b(v_1, v_1) = 0 \\ &\Rightarrow \alpha = 0 \text{ ... pues } b(v_1, v_1) \neq 0 \\ &\Rightarrow x = \theta \end{aligned}$$

por lo tanto, $W^\perp = \{\theta_V\}$

luego por el Lema 2.3.4, $V = W \perp W^\perp$ entonces

$\underbrace{dim(V)}_{n} = \underbrace{dim(W)}_{1} + dim(W^\perp)$, así $dim(W^\perp) = n - 1$

Aplicando la hipótesis inductiva, existe una base $\{v_2, ..., v_n\}$ de $W^\perp$ tal que $b(v_i, v_j) = 0$ para $i \neq j$, $2 \leqslant i, j \leqslant n$. Además por la definición de W, $b(v_1, v_j) = 0$ para $j = 2, ..., n$ luego el conjunto $\{v_1, v_2, ..., v_n\}$ es una base de V (pues $V = W \oplus W^\perp$) que tiene la propiedad pedida de $b(v_i, v_j) = 0$ para $i \neq j$.

Denotando $W_i = \mathcal{L}\{v_i\}$ tenemos que $dim(V_i) = 1$ y $W_i \perp W_j$ con $1 \leqslant i, j \leqslant n$

luego $V = W_1 \perp W_2 \perp .... \perp W_n$.

□

Corolario 2.3.6. *Cada matriz simétrica B es congruente a una matriz diagonal.*

Demostración. Por el teorema 2.3.5, escogemos una base ortogonal; digamos, $\{x_1, x_2, ..., x_n\}$ para el espacio bilineal $\langle B \rangle$ luego $[b_B(x_i, x_j)]$ es una matriz diagonal congruente con B por el Lema 2.2.2. □

Este resultado nos permite introducir una importante notación que será usada a lo largo de este tratado. De acuerdo con nuestra reciente notación, $\langle \alpha \rangle$ con $\alpha \in K$ será un espacio bilineal 1-dimensional con matriz $[\alpha]$. Para $\alpha_1, ..., \alpha_n$ en K definimos el espacio bilineal $\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle$ por

$$\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle := \langle A \rangle \text{ con } A = \begin{bmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha_n \end{bmatrix}$$

En particular, el último teorema asegura que cada espacio bilineal es isométrico a un espacio $\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle$. Así podemos siempre escribir un espacio arbitrario en esta forma, la cual es conveniente después para cálculos futuros. Usaremos el término **diagonalización** para referirnos al teorema 2.3.5 y corolario 2.3.6.

Lema 2.3.7. *Sea V un espacio vectorial con $dimV = n$*

1. *Si π es una permutación arbitraria de $1, 2, ..., n$ entonces*

$$\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle \cong \langle \alpha_{\pi(1)}, \alpha_{\pi(2)}, ..., \alpha_{\pi(n)} \rangle$$

2. *Para $\beta_i \in F^\times$ arbitrario se tiene:*

$$\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle \cong \langle \alpha_1\beta_1^2, \alpha_2\beta_2^2, ..., \alpha_n\beta_n^2 \rangle$$

Demostración. Sea $b : V \times V \longrightarrow F$ una forma bilineal.
Por el teorema 2.3.5, supongamos que $\{v_1, v_2, ..., v_n\}$ sea una base ortogonal de V donde $b(v_i, v_j) = 0$ con $i \neq j, \quad 1 \leq i, j \leq n$ y $b(v_r, v_r) = a_r$ con $r = 1, 2, ..., n$.

1. Por hipótesis, $\pi : I_n \longrightarrow I_n$ es una permutación entonces obtenemos otra base ordenada de V: $\{v_{\pi(1)}, v_{\pi(2)}...v_{\pi(n)}\}$.
   Si T es la matriz de pasaje de $\{v_1, v_2, ..., v_n\}$ a $\{v_{\pi(1)}, v_{\pi(2)}...v_{\pi(n)}\}$ entonces

$$[b(v_{\pi(i)}, v_{\pi(j)})] = T^t.[b(v_r, v_s)].T \text{ con } 1 \leq i, j \leq n \text{ y } 1 \leq r, s \leq n$$

   o sea,

$$\begin{bmatrix} a_{\pi(1)} & 0 & \dots & 0 \\ 0 & a_{\pi(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{\pi(n)} \end{bmatrix} = T^t. \begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{bmatrix} .T$$

   y siendo T no singular, tenemos que:

$$\langle a_1, a_2, ..., a_n \rangle \cong \langle a_{\pi(1)}, a_{\pi(2)}, ..., a_{\pi(n)} \rangle$$

   por el Teorema 2.2.3.

2. Tenemos:

$$\begin{bmatrix} \alpha_1.\beta_1^2 & 0 & \dots & 0 \\ 0 & \alpha_2.\beta_2^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha_n.\beta_n^2 \end{bmatrix} =$$

$$\begin{bmatrix} \beta_1 & 0 & \dots & 0 \\ 0 & \beta_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta_n \end{bmatrix}^t \cdot \begin{bmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha_n \end{bmatrix} \begin{bmatrix} \beta_1 & 0 & \dots & 0 \\ 0 & \beta_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta_n \end{bmatrix}$$

luego por Teorema 2.2.3,

$$\left(F^n, b\begin{bmatrix} \alpha_1.\beta_1^2 & 0 & \dots & 0 \\ 0 & \alpha_2.\beta_2^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha_n.\beta_n^2 \end{bmatrix}\right) \cong \left(F^n, b\begin{bmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha_n \end{bmatrix}\right)$$

por notación,

$$\langle \alpha_1\beta_1^2, \alpha_2\beta_2^2, ..., \alpha_n\beta_n^2 \rangle \cong \langle \alpha_1, \alpha_2, ..., \alpha_n \rangle$$

□

En el siguiente Teorema, reducimos el problema de clasificación de espacios bilineales a la consideración de espacios regulares.

Teorema 2.3.8. *Sea (V, b) un espacio bilineal tal que $V = V^\perp \oplus W$ entonces:*

1. *$V = V^\perp \perp W$*

2. *W es regular*

3. (W, b_W) *es determinado salvo isometrías (de espacios) por* (V, b).

Demostración. Se tiene

1. Sea $v \in V^\perp$ cualquiera, como $V = V^\perp + W$ se tiene que $v \perp W$ entonces $b(v, W) = 0$

   Siendo $v \in V^\perp$ arbitrario, $b(V^\perp, W) = 0$ es decir, $V^\perp \perp W$.

2. Debemos mostrar que $W^{\perp_{b_W}} = \{\theta\}$

   Sea $x \in W$ tal que $x \in W^{\perp_{b_W}}$ entonces $b_W(x, y) = 0$ para todo $y \in W$

   por lo que $b(x, y) = 0$ para todo $y \in W$

   por 1., $b(x, V^\perp) = 0$ es decir, $b(x, z) = 0$ para todo $z \in V^\perp$

   luego por la linealidad del segundo argumento y considerando las dos últimas igualdades $b(x, y + z) = 0$ para cualesquiera $y \in W$ y $z \in V^\perp$

   entonces $b(x, V^\perp \oplus W) = 0$

   entonces $b(x, V) = 0$ por lo que $x \in V^\perp$,

   sea, $x \in W \cap V^\perp = \{\theta\}$ entonces $x = \theta$

   Por lo tanto, (W, b_W) es regular.

3. Supongamos que también $V = V^\perp \oplus W_1$ entonces cada elemento de V, en particular $x \in W \subset V$ puede ser escrito de manera única como $x = y + \alpha(x)$ con $y \in V^\perp$ y $\alpha(x) \in W_1$ ...($\alpha(x)$ e y dependen de x).

   Definimos la aplicación

$$\begin{array}{rccc} \alpha: & W & \longrightarrow & W_1 \\ & \alpha & \longmapsto & \alpha(x) \end{array}$$

   <u>Afirmación:</u> α es transformación lineal

   Sea $\lambda \in F, x \in W$ entonces la descomposición de $\lambda.x \in W$ es: $\lambda.x = z + \alpha(\lambda.x)$, $z \in V^\perp$

   también $\lambda x = \lambda(y + \alpha(x))$ entonces $\lambda x = \lambda y + \lambda.\alpha(x))$

   por la unicidad de la escritura: $\alpha(\lambda.x) = \lambda.\alpha(x)$

   Sean $x, y \in W$ se tiene: $x = z_1 + \alpha(x)$ y $y = z_2 + \alpha(x)$

por lo que $x+y=\underbrace{(z_1+z_2)}_{\in V^\perp}+\underbrace{(\alpha(x)+\alpha(y))}_{\in W_1}$

también $x+y\in W$ entonces $x+y=\underbrace{z}_{\in V^\perp}+\underbrace{\alpha(x+y)}_{\in W_1}$

nuevamente por la unicidad de la escritura, $\alpha(x+y)=\alpha(x)+\alpha(y)$

α es inyectiva

Sean $x_1,x_2\in W$ tales que $\alpha(x_1)=\alpha(x_2)$ luego la descomposición de ellos es $x_1=z_1+\alpha(x_1)$ y $x_2=z_2+\alpha(x_2)$ con $z_1,z_2\in V^\perp$

entonces $x_1-x_2=(z_1-z_2)+\underbrace{(\alpha(x_1)-\alpha(x_2))}_{\theta\in W_1}$

luego $\underbrace{x_1-x_2}_{\in W}=\underbrace{z_1-z_2}_{\in V^\perp}$ por lo que $x_1-x_2\in W\cap V^\perp=\{\theta\}$

así: $x_1=x_2$

α es sobreyectiva

Es claro de la definición de α, pues como $dimW=dimW_1$ (V es suma directa) y α es inyectiva entonces α es sobreyectiva.

α es isometría

Sea $x'=y'+\alpha(x')$ con $y'\in V^\perp,\alpha(x')\in W_1$

luego para cualquier $x\in V$:

$$\begin{aligned} b(x,x') &= b(y+\alpha(x),y'+\alpha(x')) \\ &= \underbrace{b(y,y')}_{0}+\underbrace{b(y,\alpha(x'))}_{0}+\underbrace{b(\alpha(x),y')}_{0}+b(\alpha(x),\alpha(x')) \end{aligned}$$

por lo que $b(\alpha(x),\alpha(x'))=b(x,x')$

□

Definición 2.3.9. *: Las clases isométricas de (W,b_W) son llamadas la* ***componente regular*** *o* ***parte regular de*** *(V,b).*

Corolario 2.3.10. *Dos espacios bilineales son isométricos si y sólo si, ellos tienen la misma dimensión y las mismas componentes regular.*

Demostración. ($\Rightarrow$) Supongamos que (V,b) y (V_1,b') son isométricos entonces existe $\sigma:V\to V_1$ isometría biyectiva

luego tenemos que $dimV = \underbrace{dimKer(\sigma)}_{0} + dim\,\underbrace{\sigma(V)}_{V_1}$

entonces $dimV = dimV'$.

Como $V^\perp$ y $V_1^\perp$ son subespacios de V y V_1 respectivamente, entonces existen $W \subset V$ y $W_1 \subset V_1$ tales que $V = V^\perp \oplus W$ y $V_1 = V_1^\perp \oplus W_1$.

Consideremos $\tau = \sigma_{|W} : W \to \sigma(W)$, que es una isometría biyectiva.

Por el teorema 2.3.8, $V^\perp \perp W$, siendo σ una isometría: $\sigma(V^\perp) \perp \sigma(W)$ en V_1, además como $\sigma(V^\perp) = V_1^\perp$ entonces $\sigma(W) = W_1$

por lo que $\tau : W \to W_1$ es isometría biyectiva, es decir las componentes regular de (V, b) y (V_1, b') son ïguales"

($\Leftarrow$) Consideremos dos espacios bilineales (V, b) y (V_1, b') tales que $V = V^\perp \oplus W$ y $V_1 = V_1^\perp \oplus W_1$.

Por hipótesis, $dimV = dimV_1$...(1)

existe $\beta : W \to W_1$ isometría biyectiva ...(2)

de (1) y (2): $dim(V^\perp) + dim(W) = dim(V_1^\perp) + \underbrace{dim(W_1)}_{dim(W)}$

entonces $dim(V^\perp) = dim(V_1^\perp)$

en particular, existe una isometría biyectiva $\alpha : V^\perp \to V_1^\perp$

luego

$$\begin{array}{rccl} \alpha \oplus \beta : & V & \to & V_1 \\ & u + w & \mapsto & \alpha(u) + \beta(w) \end{array}$$

es isometría biyectiva.

En efecto:

buena definición: pues α y β son aplicaciones.

transformación lineal: pues α y β son transformaciones lineales.

$\alpha \oplus \beta$ es inyectiva: sean $u_1 + w_1, u_2 + w_2$ en $V = V^\perp \oplus W$ tal que:

$$\begin{array}{rcll}
(\alpha \oplus \beta)(u_1 + w_1) & = & (\alpha \oplus \beta)(u_2 + w_2) & \\
\alpha(u_1) + \beta(w_1) & = & \alpha(u_2) + \beta(w_2) & \\
\underbrace{\alpha(u_1 - u_2)}_{\in V_1^\perp} & = & \underbrace{\beta(w_2 - w_1)}_{\in W_1^\perp} & \\
\alpha(u_1 - u_2) & = & \beta(w_1 - w_2 = \theta_{V_1} & \text{... pues } V_1 = V_1^\perp \oplus W_1 \\
u_1 = u_2 & \text{y} & w_1 = w_2 & \text{... pues } \alpha \text{ y } \beta \text{ son mono} \\
u_1 + w_1 & = & u_2 + w_2 &
\end{array}$$

$\alpha \oplus \beta$ es epimorfismo: sabiendo que $\alpha \oplus \beta$, se tiene

$$\underbrace{dim(V)}_{dim(V_1) \text{ por (1)}} = 0 + dim(Im(\alpha \oplus \beta))$$

además $Im(\alpha \oplus \beta) \subseteq V_1$, se tiene $Im(\alpha \oplus \beta) = V_1$

$\alpha \oplus \beta$ es isometría: Sean $u = u_1 + w_1$, $v = u_2 + w_2$ en $V = V^\perp \oplus W$ cualquiera

$$b_1((\alpha \oplus \beta)(u), (\alpha \oplus \beta)(v)) = b_1(\alpha(u_1) + \beta(w_1), \alpha(u_2) + \beta(w_2))$$

$$= b_1(\underbrace{\alpha(u_1)}_{\in V_1^\perp}, \underbrace{\alpha(u_2)}_{\in V_1^\perp}) + \underbrace{b_1(\underbrace{\alpha(u_1)}_{\in V_1^\perp}, \underbrace{\beta(w_2)}_{\in W_1})}_{0} + \underbrace{b_1(\underbrace{\beta(w_1)}_{\in W_1}, \underbrace{\alpha(u_2)}_{\in V_1^\perp})}_{0} + b_1(\underbrace{\beta(w_1)}_{\in W_1}, \underbrace{\beta(w_2)}_{\in W_1})$$

$$= b_1|_{V_1^\perp}(\alpha(u_1), \alpha(u_2)) + b_1|_{W_1}(\beta(w_1), \beta(w_2)) = b(u_1, u_2) + b(w_1, w_2)$$

$$b(u_1 + w_1, u_2 + w_2) = b(u, v)$$

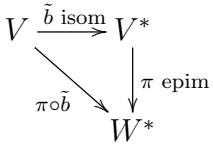
Por lo tanto $V \cong V_1$ □

Lema 2.3.11. *Sea (V, b) un espacio regular y W un subespacio de V entonces se tiene que $dimW + dimW^\perp = dimV$.*

Demostración. Como V es regular, la aplicación adjunta $\tilde{b} : V \to V^*$ es isomorfismo y la aplicación canónica

$$\begin{array}{rccc}
\pi : & V^* & \to & W^* \\
& f & \mapsto & f_{|W}
\end{array}$$

es sobreyectiva



luego $\pi \circ \tilde{b}$ es sobreyectiva entonces

$$\begin{aligned} dimV &= dimKer(\pi \circ \tilde{b}) + dimIm(\pi \circ \tilde{b}) \\ dimV &= dimW^{\perp} + dimW^* && \text{... lema 2.2.9 y } \pi \circ \tilde{b} \text{ es epim} \\ dimV &= dimW^{\perp} + dimW && \text{... } dimW^* = dimW \end{aligned}$$

□

Corolario 2.3.12. *Bajo las mismas condiciones,* $(W^{\perp})^{\perp} = W$

Demostración. Si $x \in W$ entonces $b(x, y) = 0$ para todo $y \in W^{\perp}$ por lo que se tiene que $x \in W^{\perp\perp}$

Por lo tanto, $W \subset W^{\perp\perp}$ ...(1)

Por otro lado, como $W^{\perp}$ es subespacio de V por el lema 2.3.11,

$dimV = dimW^{\perp} + dimW^{\perp\perp}$

entonces $dimV = dimW^{\perp} + dimW^{\perp\perp} = dimW + dimW^{\perp}$

en consecuencia $dimW + dimW^{\perp\perp}$ ...(2).

De (1) y (2), se obtiene $W = W^{\perp\perp}$. □

En esta sección hemos discutido la descomposición de un espacio bilineal como la suma ortogonal de subespacios. Naturalmente el proceso inverso está estrechamente relacionado. De dos espacios bilineales podemos formar un espacio bilineal nuevo: su suma (externa) ortogonal. Cuando consideramos el producto cartesiano $V \times W$ de dos espacios vectoriales V y W, identificaremos a V y W como subespacios de $V \times W$ vía la inclusión canónica y escribimos $V \oplus W$ en vez de $V \times W$.

Definición 2.3.13. *Si* (V, b) *y* (V', b') *son dos* ***espacios bilineales*** *entonces escribimos* $(V, b) \perp (V', b')$ *para el espacio bilineal simétrico cuyo espacio vectorial fundamental es la* ***suma directa*** $V \oplus V'$ *y cuya forma bilineal* $b \perp b'$ *está definida por:*

$$\begin{aligned} b \perp b' : \ & (V \oplus V') \times (V \oplus V') \longrightarrow F \\ & (b \perp b')((x, x'), (y, y')) = b(x, y) + b'(x', y') \end{aligned}$$

$(V,b) \perp (V',b')$ es llamado la suma(externa) ortogonal de (V,b) y (V',b'). Definimos la suma ortogonal de n espacios bilineales, análogamente. La construcción de sumas ortogonales es naturalmente asociativa. La notación $\perp$ es consistente para $V \perp V'$ en $(V,b) \perp (V',b')$ en el sentido de la definición 2.3.3.

En lo siguiente denotaremos a los espacios bilineales por las letras Φ, Ψ, etc. Ahora, numeramos algunas propiedades básicas de la suma ortogonal.

Lema 2.3.14. *Sean $\Phi, \Psi, \Phi_1, \Psi_1$ espacios bilineales*

1. $\Phi \perp \Psi \cong \Psi \perp \Phi$.
2. *Si $\Phi \cong \Phi_1$ y $\Psi \cong \Psi_1$ entonces $\Phi \perp \Psi \cong \Phi_1 \perp \Psi_1$.*
3. $\Phi \perp \Psi$ *es regular si y sólo sí, Φ y Ψ son ambos regular.*
4. *Si B es la matriz de Φ y B' es la matriz de Ψ entonces la suma ortogonal $\Phi \perp \Psi$ tiene la matriz:* $\begin{bmatrix} B & \Theta \\ \Theta & B' \end{bmatrix}$

En la parte final de esta sección, regresamos al grupo ortogonal y definimos el determinante de un espacio bilineal.

Lema 2.3.15. *Si (V,b) es un espacio bilineal regular y $\alpha \in O(V,b)$ entonces $det\alpha = \pm 1$*

Demostración. Escogemos una base de V y sea B la matriz asociada a (V,b) en la base escogida, por corolario 2.3.2 se tiene $detB \neq 0$.
Como $\alpha \in O(V,b)$, sea A su matriz asociada entonces por el isomorfismo consecuencia de 2.2.3, $detA \neq 0$ y $A^t.B.A = B$
entonces $detA^t.detB.detA = detB$ entonces $(detA)^2 = 1$
por lo que $detA = \pm 1$ luego $det\alpha = \pm 1$. □

Definición 2.3.16. *El determinante induce un homomorfismo*

$$det : O(V,b) \longrightarrow \{1,-1\}$$

El núcleo de este homomorfismo: las isometrías de determinante 1, es llamado el **grupo ortogonal especial** y será denotado por $SO(V, b)$.
Sea $F^{\times^2}$ el grupo de cuadrados del grupo multiplicativo de $F^{\times}$ de nuestro cuerpo original F. Si b tiene matriz B con respecto a alguna base entonces b tiene matriz $B' = A^t BA$ con respecto a otra base, donde A es la matriz cambio de base. Como A es invertible entonces $detB' = \underbrace{detA^t}_{detA}.detB.detA$ por lo que $detB' = detB.(detA)^2$ o sea, $detB'$ y $detB$ difieren solo en un elemento de $F^{\times^2}$. De los resultados de la Sección 2 tenemos inmediatamente que: (V, b) es singular si y solo si $detB = 0$.

Definición 2.3.17. *El escalar $detB$, el cual es bien definido salvo cuadrados, es llamado* ***el determinante*** *de (V, b). Más precisamente, si (V, b) es singular entonces $det(V, b) = 0$. Si (V, b) es no singular(regular) entonces $det(V, b)$ es un elemento de $F^{\times}/F^{\times^2}$ representado por $detB$.*

Como los espacios isométricos tienen las matrices asociadas congruentes, la igualdad del determinante es necesaria para isometrías. De la igualdad

$$det \begin{bmatrix} B_1 & \Theta \\ \Theta & B_2 \end{bmatrix} = det(B_1).det(B_2)$$

se implica inmediatamente

$$det(\Phi \perp \Psi) = det(\Phi).det(\Psi)$$

En términos de formas cuadráticas tenemos

Definición 2.3.18. *La* ***dimensión*** *de una* ***forma cuadrática*** *q sobre V denotado por $dim(q)$, es igual a la dimensión de V.*

Definición 2.3.19. *El* ***discriminante*** *de una* ***forma cuadrática*** *q es igual al determinante de la matriz asociada a la forma cuadrática q, denotada por $disc(q)$.*

En las siguientes secciones y capítulos haremos uso continuo de los determinantes.

2.4. Isotropía y Espacios hiperbólicos

En esta sección todos los espacios serán regular.

Definición 2.4.1. *Tenemos:*

1. *Un* ***vector*** $x \neq \theta$ *en un espacio bilineal* (V, b) *es llamado* ***isotrópico*** *si* $b(x, x) = 0$. *En caso contrario,* x *es llamado* ***anisotrópico****.*

2. (V, b) *es llamado* ***Espacio bilineal isotrópico*** *si contiene un vector isotrópico. También diremos que* (V, b) *representa al cero, en caso contrario,* (V, b) *es llamado Espacio bilineal anisotrópico.*

3. *Un* ***subespacio*** W *de* V *es llamado* ***totalmente isotrópico*** *si*

$$b(W, W) = 0 \text{ o } b(x, y) = 0 \text{ para todo } x, y \text{ en } W$$

Teorema 2.4.2. *Cualquier forma cuadrática degenerada tiene un vector isotrópico.*

Demostración. Supongamos que la forma cuadrática q es degenerada entonces su forma bilineal simétrica asociada b es degenerada por lo que existe algún vector $v \in V$ tal que $b(v, w) = 0$ para todos los $w \in V$. En particular se tiene $b(v, v) = q(v) = 0$ □

Sea V un K-espacio vectorial y V^* su espacio dual. Sobre el espacio vectorial $V \oplus V^*$, consideremos la siguiente bilineal simétrica

$$\hat{b} := \hat{b}_V : (V \oplus V^*) \times (V \oplus V^*) \longrightarrow F$$

definido por

$$\hat{b}((x, f), (y, g)) = f(y) + g(x)$$

Lema 2.4.3. *Se tiene que:*

1. $(V \oplus V^*, \hat{b}_V)$ *es regular.*

2. V *y* V^* *son subespacios totalmente isotrópicos.*

Demostración. 1. Sea $(x, f) \in V \oplus V^*$ cualquiera no nulo.

Si $x \neq \theta$ entonces existe $g \in V^*$ tal que $g(x) \neq 0$ por lo tanto, existe (θ, g) tal que $\hat{b}((x, f), (\theta, g)) = g(x) \neq 0$.

Si $f \neq \theta_{V^*}$, existe $y \in V$ tal que $f(y) \neq 0$ luego $\hat{b}((x, f), (y, 0)) = f(y) \neq 0$.

Por lo tanto, dado $(x, f) \in V \oplus V^*$ no nulo, existe (y, g) tal que $\hat{b}((x, f), (y, 0)) \neq 0$.

2. $V \cong \{(x, \theta_{V^*}) / x \in V\} \subset V \oplus V^*$

$V^* \cong \{(\theta_{V^*}, f) / f \in V^*\} \subset V \oplus V^*$.

Sean (x, θ_{V^*}) y (y, θ_{V^*}) en V se tiene

$$\hat{b}((x, \theta_{V^*}), (x, \theta_{V^*})) = \theta_{V^*}(y) + \theta_{V^*}(x) = 0$$

Análogamente, sean (θ_{V^*}, f) y (θ_{V^*}, g) en V^* cualesquiera, luego

$$\hat{b}((\theta_V, f), (\theta_V, g)) = f(\theta_V) + g(\theta_V) = 0$$

□

Definición 2.4.4. *El espacio bilineal simétrico regular $(V \oplus V^*, \hat{b})$ será denotado por $\mathbb{H}(V)$ y llamado el* ***espacio hiperbólico*** *sobre V.*

De una manera natural esta construcción asocia a un espacio bilineal regular con cada espacio vectorial. De una manera análoga, podemos asociar una isometría con cada isomorfismo de espacios vectoriales:

Lema 2.4.5. *Sea $\alpha : V \to W$ un isomorfismo de espacios vectoriales y $\alpha^* : W^* \to V^*$ su isomorfismo dual, entonces*

$$\mathbb{H}(\alpha) = \alpha \oplus (\alpha^*)^{-1} : \mathbf{H}(V) \to \mathbb{H}(W)$$

es una isometría biyectiva.

Demostración. Tenemos que:

$$\begin{array}{rccl} \mathbb{H}(\alpha): & \mathbb{H}(V) & \to & \mathbb{H}(W) \\ & (u, f) & \mapsto & \mathbb{H}(\alpha)(u, f) = (\alpha(u), (\alpha^*)^{-1}(f)) \end{array}$$

- $\mathbb{H}(\alpha)$ es transformación lineal

  Sean a, b en K, además $(u, f), (v, g)$ en $\mathbb{H}(\alpha)$.

$$\begin{aligned}
[\mathbb{H}(\alpha)]\,(a(u,f)+b(v,g)) &= [\mathbb{H}(\alpha)]\,(au+bv, af+bg)\\
&= (\alpha(au+bv), (\alpha^*)^{-1}(af+bg))\\
&= (a\alpha(u)+b\alpha(v), a(\alpha^*)^{-1}(f)+b(\alpha^*)^{-1}(g))\\
&= a(\alpha(u), (\alpha^*)^{-1}(f))+b(\alpha(v), (\alpha^*)^{-1}(g))\\
&= a\,[\mathbb{H}(\alpha)]\,(u,f)+b\,[\mathbb{H}(\alpha)]\,(v,g)
\end{aligned}$$

- $\mathbb{H}(\alpha)$ es inyectiva

  Sean (u, f) y (v, g) en $\mathbb{H}(V)$

$$\begin{aligned}
[\mathbb{H}(\alpha)]\,(u,f) = [\mathbb{H}(\alpha)]\,(v,g) &\Rightarrow (\alpha(u), (\alpha^*)^{-1}(f)) = (\alpha(v), (\alpha^*)^{-1}(g))\\
&\Rightarrow [\alpha(u)=\alpha(v) \text{ y } (\alpha^*)^{-1}(f)=(\alpha^*)^{-1}(g)]\\
&\Rightarrow [\alpha(u-v)=\theta_W \text{ y } (\alpha^*)^{-1}(f-g)=\theta_{W^*}]\\
&\Rightarrow [u-v\in Ker(\alpha)=\{\theta_V\} \text{ y}\\
&\quad\ f-g=(\alpha^*)^{-1}(\theta_{W^*})=\{0_{V^*}\}]\\
&\Rightarrow [u=v \text{ y } f=g]
\end{aligned}$$

  Por lo tanto $(u, f) = (v, g)$

- $\mathbb{H}(\alpha)$ es epiyectiva

  Dado (w, g) en $\mathbb{H}(W)$ cualquiera, se tiene que $w \in W$ y $g \in W^*$

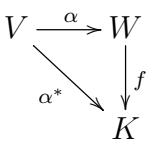
  Como α es epiyectiva, existe $u \in V$ tal que $\alpha(u) = w$.

  Como $(\alpha^*)^{-1}$ es epiyectiva, existe $f \in V^*$ tal que $(\alpha^*)^{-1}(f) = g$. Así existe $(u, f) \in \mathbb{H}(V)$ tal que

  $[\mathbb{H}(\alpha)]\,(u, f) = (\alpha(u), (\alpha^*)^{-1}(f)) = (w, g)$

- $\mathbb{H}(\alpha)$ es isometría

  Recordemos que:



$$\begin{aligned}
\alpha^*: \ W^* &\to V^*\\
f &\mapsto \alpha^*(f) = f\circ\alpha
\end{aligned}$$

Sean (u,f) y (v,g) en $\mathbb{H}(V)$ cualesquiera

$$\begin{aligned}
\hat{b}_W(\mathbb{H}(\alpha)(u,f),\mathbb{H}(\alpha)(v,g)) &= \hat{b}_W((\underbrace{\alpha(u)}_{\in W},\underbrace{(\alpha^*)^{-1}(f)}_{\in W^*}),(\underbrace{\alpha(v)}_{\in W},\underbrace{(\alpha^*)^{-1}(g)}_{\in W^*}) \\
&= ((\alpha^*)^{-1}(f))(\alpha(v)) + ((\alpha^*)^{-1}(g))(\alpha(u)) \\
&= (\underbrace{((\alpha^*)^{-1}(f))}_{\in W^*}\circ\alpha)(v) + (\underbrace{((\alpha^*)^{-1}(g))}_{\in W^*}\circ\alpha)(u) \\
&= (\alpha^*((\alpha^*)^{-1}(f))(v) + ((\alpha^*)^{-1}(g))(u) \\
&= ((\alpha^*\circ(\alpha^*)^{-1})(f))(v) + ((\alpha^*\circ(\alpha^*)^{-1})(g))(u) \\
&= ((1_{V^*})(f))(v) + ((1_{V^*})(g))(u) \\
&= f(v) + g(u) \\
&= \hat{b}_V((u,f),(v,g))
\end{aligned}$$

□

Sea $GL(V) = Aut(V)$ que denota el **grupo de endomorfismos invertibles** de V. Más aún, se verifica que

$$\begin{aligned}
\mathbb{H}: \quad GL(V) &\to O(\mathbb{H}(\mathbb{V})) \\
\alpha &\mapsto \alpha \oplus (\alpha^*)^{-1}
\end{aligned}$$

es un homomorfismo de grupos inyectivo.

En efecto,

- buena definición de $\mathbb{H}$

  Sea $\alpha \in GL(V)$, ó $\alpha \oplus (\alpha^*)^{-1} \in O(\mathbb{H}(V))$

  Por el lema 2.4.5 y tomando $V = W$ tenemos que

  $\alpha \oplus (\alpha^*)^{-1} : \mathbb{V} \to \mathbb{H}(V)$ es isometría biyectiva, por lo tanto

  $\alpha \oplus (\alpha^*)^{-1} \in O(\mathbb{H}(V))$.

- $\mathbb{H}$ es homomorfismo de grupos

  Sean α, β en $GL(V)$ entonces $\mathbb{H}(\alpha,\beta) \in O(\mathbb{H}(V))$.

  Sean $(u,f) \in \mathbb{H}(V)$ cualquiera, entonces

$$\begin{aligned}
\mathbb{H}(\alpha\circ\beta)(u,f) &= ((\alpha\circ\beta)\oplus((\alpha\circ\beta)^*)^{-1})(u,f)\\
&= ((\alpha\circ\beta)(u),((\alpha\circ\beta)^*)^{-1}(f))\\
&= (\alpha(\beta(u)),((\beta^*\circ\alpha^*)^{-1})(f))\\
&= (\alpha(\beta(u)),((\beta^*)^{-1}\circ(\beta^*)^{-1})(f))\\
&= (\alpha(\beta(u)),(\alpha^*)^{-1}((\beta^*)^{-1}(f)))\\
&= (\alpha\oplus(\alpha^*)^{-1})(u))\circ(\beta(u),(\beta^*)^{-1}(f))\\
&= (\alpha\oplus(\alpha^*)^{-1})(u))\circ((\beta\oplus(\beta^*)^{-1})(f))\\
&= ((\alpha\oplus(\alpha^*)^{-1})\circ(\beta\oplus(\beta^*)^{-1}))(f)\\
&= (\mathbb{H}(\alpha)\circ\mathbb{H}(\beta))(f)
\end{aligned}$$

Por lo tanto $\mathbb{H}(\alpha\circ\beta)=\mathbb{H}(\alpha)\circ\mathbb{H}(\beta)$

- $\mathbb{H}$ es inyectivo

  Sean α, β en $GL(V)$ cualesquiera tal que

$$\begin{aligned}
\mathbb{H}(\alpha)=\mathbb{H}(\beta) &\Rightarrow \mathbb{H}(\alpha)(u,f)=\mathbb{H}(\beta)(u,f) \text{ con } (u,f) \text{ en } V\oplus V^*\\
&\Rightarrow ((\alpha\oplus(\alpha^*)^{-1})(u,f)=(\beta\oplus(\beta^*)^{-1})(u,f)\\
&\Rightarrow (\alpha(u),(\alpha^*)^{-1}(f))=(\beta(u),(\beta^*)^{-1}(f))\\
&\Rightarrow [\alpha(u)=\beta(u) \text{ y } (\alpha^*)^{-1}(f)=(\beta^*)^{-1}(f)]\\
&\Rightarrow [(\alpha-\beta)(u)=\theta_V \text{ para todo } u\in V \text{ y}\\
&\quad ((\alpha^*)^{-1}-(\beta^*)^{-1})(f)=\theta_{V^*} \text{ para todo } f\in V^*]\\
&\Rightarrow \alpha-\beta=\theta_{GL(V)}\\
&\Rightarrow \alpha=\beta
\end{aligned}$$

.

Teorema 2.4.6. *Sea (V,b) un espacio bilineal regular $2n$-dimensional. Las siguientes condiciones son equivalentes:*

i. $(V,b)\cong\mathbb{H}(W)$ *para un espacio vectorial n-dimensional.*

ii. V *contiene un subespacio totalmente isotrópico W de dimensión n.*

iii. $(V,b)\cong\langle B\rangle$ *con* $B=\begin{pmatrix}\theta & C\\ C^t & D\end{pmatrix}$ *donde θ,C y D son matrices $n\times n$ con $det(C)\neq 0$.*

iv. $(V,b) \cong \langle B \rangle$ *con* $B = \begin{pmatrix} \theta & E \\ E^t & \theta \end{pmatrix}$ *donde* E *denota la matriz identidad* $n \times n$.

v. $(V,b) \cong \langle B \rangle$ *con* $B = \begin{pmatrix} A & \theta \\ \theta & -A \end{pmatrix}$ *donde* A *es una matriz invertible* $n \times n$.

vi. $(V,b) \cong \langle 1, \ldots, 1, -1, \ldots, -1 \rangle \cong \langle 1, -1, \ldots, 1, -1 \rangle$

Demostración. i) $\Rightarrow$ ii) W es un subespacio totalmente isotrópico de $\mathbb{H}(W)$

ii) $\Rightarrow$ iii) Se completa la base arbitraria $\{e_1, \cdots, e_n\}$ de W a una base de V. La matriz de b respecto a esa base tiene la forma requerida.

iii) $\Longleftrightarrow$ iv) Se obtiene del teorema 2.2.3 de la siguiente ecuación matricial:

$$\begin{pmatrix} C & 0 \\ A^t & E \end{pmatrix} \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix} \begin{pmatrix} C^t & A \\ 0 & E \end{pmatrix} = \begin{pmatrix} 0 & C \\ C^t & D \end{pmatrix}, A = \frac{1}{2}D.$$

iv) $\Longleftrightarrow$ v) Se obtiene de la siguiente ecuación matricial:

$$\begin{pmatrix} E & E \\ X^t & -X^t \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & -A \end{pmatrix} \begin{pmatrix} E & X \\ E & -X \end{pmatrix} = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}, X = \frac{1}{2}A^{-1}.$$

iv) $\Longleftrightarrow$ vi) Este es un caso especial de iv) $\Longleftrightarrow$ v)

iv) $\Longrightarrow$ i) Sea $\{e_1, ..., e_n, e'_1, ..., e'_n\}$ la base de V respecto a la matriz de b que tiene la forma $\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}$. Sea $\{e_1, ..., e_n\}$ la base de W y $\{e_1^*, ..., e_n^*\}$ la base dual de W^* Entonces $\alpha : V \to V \oplus W^*$ definido por $\alpha(e_i) = e_i, \alpha(e'_i) = e_i^*$ es una forma isometríca de (V,b) a $\mathbb{H}(W)$. Para probar que α es una isometría primero debemos notar que α se comporta como una isometría sobre los vectores base y el resultado se obtiene por una combinación lineal arbitraria de los vectores bases. □

Corolario 2.4.7. *Sea* (V,b) *un espacio bilineal regular* 2*-dimensional. Las siguientes condiciones son equivalentes:*

i. $(V, b$ *es isotrópico.*

ii. $(V,b) \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$

iii. $(V,b) \cong \langle 1,-1\rangle \cong \langle \alpha,-\alpha\rangle$, $\alpha \neq 0$

iv. $(V,b) \cong \left\langle \begin{pmatrix} 0 & \alpha \\ \alpha & \gamma \end{pmatrix} \right\rangle$, $\alpha \neq 0$

v. $det(V,b) \equiv -1 mod \dot{K}^2$

Demostración. Como (V,b) es isotrópico, existe $u \in V$ no nulo tal que $b(u,u) = 0$. Considerando $W = \mathcal{L}_F\{u\}$, tenemos que W es un subespacio totalmente isotrópico 1-dimensional de V por lo que se cumplen las equivalencias del Teorema 2.4.6: (i)⇔(ii)⇔(iii)⇔(iv)

(ii) Tomar $E = \langle 1\rangle$ en Teorema 2.4.6 (iv).

(iii) Tomar $A = \langle \alpha\rangle$ $(\alpha \neq 0)$ en el Teorema 2.4.6 (v) entonces $(V,b) \cong \langle \alpha,-\alpha\rangle$ y del Teorema 2.4.6 (vi), $(V,b) \cong \langle 1,-1\rangle$.

Por lo tanto, $(V,b) \cong \langle 1,-1\rangle \cong \langle \alpha,-\alpha\rangle$ con $\alpha \neq 0$.

(iv) del Teorema 2.4.6 (iii), $(V,b) \cong \begin{pmatrix} 0 & \alpha \\ \alpha & \gamma \end{pmatrix}$ con $\alpha \neq 0$.

(ii)⇒(v) Por definición 2.3.17,

$det(V,b) = det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times a^2$ con $a \in F^\times$

⇔ $\det(V,b) = -1 \times a^2$, $a \in F^\times$ ⇔ $\det(V,b) \equiv -1 mod({F^\times}^2)$

(v)⇒(i): Por Teorema 2.3.5 b es ortogonal, tomemos $\{x,y\}$ una base ortogonal de V y por Corolario 2.3.6, sea $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$ su matriz diagonal asociada. Como $det(V,b) \equiv -1 mod({F^\times}^2)$ entonces $\alpha_1.\alpha_2 = -\gamma^2$ con algún $\gamma \in F^\times$.

Afirmación: el vector $x + y\gamma\alpha_2^{-1}$ es isotrópico.

$$
\begin{aligned}
b(x+y\gamma\alpha_2^{-1}, x+y\gamma\alpha_2^{-1}) &= b(x, y\gamma\alpha_2^{-1}) + b(x,x) + b(y\gamma\alpha_2^{-1}, y\gamma\alpha_2^{-1}) + b(y\gamma\alpha_2^{-1}, x) \\
&= \gamma\alpha_2^{-1}.\underbrace{b(x,y)}_{0} + \underbrace{b(x,x)}_{\alpha_1\neq 0} + \gamma^2\alpha_2^{-2}.\underbrace{b(y,y)}_{\alpha_2\neq 0} + \gamma\alpha_2^{-1}.\underbrace{b(y,x)}_{0} \\
&= \alpha_1 + \gamma^2\alpha_2^{-1} \\
&= \alpha_1 + (-\alpha_1.\alpha_2)\alpha_2^{-1} \\
&= \alpha_1 - \alpha_1 \\
&= 0
\end{aligned}
$$

Además $x+y\gamma\alpha_2^{-1} \neq \theta$ pues en caso contrario, x e y serán linealmente dependientes. □

Definición 2.4.8. *Cualquier espacio bilineal que satisface las condiciones del teorema 2.4.6 será llamado* ***espacio bilineal hiperbólico****. Si satisface las condiciones del corolario 2.4.7 será llamado* ***plano hiperbólico****. En particular, los espacios hiperbólicos sobre espacios vectoriales 1-dimensionales son planos hiperbólicos.*

Definición 2.4.9. *Dos vectores x e y con $b(x,x) = b(y,y) = 0$ y $b(x,y) = 1$ son llamados* ***par hiperbólico****.*

Por el Corolario 2.4.7 ii. cada plano hiperbólico tiene una base que es par hiperbólico. El plano hiperbólico después será denotado por $\mathbb{H}$.

Corolario 2.4.10. *Un espacio hiperbólico es la suma ortogonal de planos hiperbólicos.*

Corolario 2.4.11. *Si (V,b) es regular y x es isotrópico entonces existe un vector y tal que x, y es un par hiperbólico entonces V tiene una descomposición $V = W \perp W^{\perp}$ donde (W, b_W) es un plano hiperbólico.*

Demostración. Como (V,b) es regular, dado $x \neq 0$ en V, existe $z \in V$ tal que $\alpha = b(x,z) \neq 0$ entonces $b(x, \alpha^{-1}z) = 1$.

Tomando $u = \alpha^{-1}z$, tenemos que $b(x,u) = 1$, consideremos el siguiente vector $y = u - \frac{1}{2}.b(u,u)x$

Afirmación: x e y es par hiperbólico

En efecto, tenemos que:

$$
\begin{aligned}
b(x,x) &= 0 \text{ ... pues } x \text{ es isotrópico} \\
b(y,y) &= b(u-\tfrac{1}{2}.b(u,u)x, u-\tfrac{1}{2}.b(u,u)x) \\
&= b(u,u) - \tfrac{b(u,u)}{2}b(u,x) - \tfrac{b(u,u)}{2}b(x,u) - \tfrac{[b(u,u)]^2}{4}\underbrace{b(x,x)}_{0} \\
&= b(u,u) - b(u,u).b(u,x) \\
&= b(u,u)(1-b(u,x)) \\
&= b(u,u),0 = 0 \\
b(x,y) &= b(x, u-\tfrac{1}{2}.b(u,u)x) \\
&= \underbrace{b(x,u)}_{1} - \tfrac{b(u,u)}{2}\underbrace{b(x,x)}_{0} \\
&= 1
\end{aligned}
$$

Tomando $W = \mathcal{L}\{x,y\}$ se obtiene el plano hiperbólico buscado. □

Definición 2.4.12. *Un **espacio bilineal** (V,b) **representa a** $\alpha \in F$, si existe $x \in V$, $x \neq \theta$ tal que $b(x,x) = \alpha$.*

*El **espacio** (V,b) es llamado **universal** si (V,b) representa a todos los $\alpha \in F^{\times}$.*

En términos de una forma cuadrática q tenemos la siguiente

Definición 2.4.13. *Una **forma cuadrática representa** un elemento $\alpha \in F$ si existe un $x \neq 0$ en F^n tal que $q(x) = \alpha$.*

Decimos que q representa al cero solo de manera trivial si $q(x) = 0$ para $x = 0$.

Definición 2.4.14. *Una **forma cuadrática** q es **isotrópica** si existe $x \in F^n$ no nulo tal que $q(x) = 0$, o sea, la forma q representa a cero de manera no trivial.*

Lema 2.4.15. *Cada espacio bilineal isotrópico es universal.*

Demostración. Sea $x \in V$ isotrópico entonces por el Corolario 2.4.11, existe $y \in V$ tales que x, y es un par hiperbólico.

Siendo $\alpha \in F$ cualquiera, tenemos

$$
\begin{aligned}
b(x+\tfrac{1}{2}\alpha y, x+\tfrac{1}{2}\alpha y) &= \underbrace{b(x,x)}_{0} + \tfrac{\alpha}{2}.\underbrace{b(x,y)}_{1} + \tfrac{\alpha}{2}\underbrace{b(y,x)}_{1} + \tfrac{\alpha^2}{4}.\underbrace{b(y,y)}_{0} \\
&= \tfrac{\alpha}{2} + \tfrac{\alpha}{2} = \alpha
\end{aligned}
$$

□

Ejemplo 2.4.16. *La forma cuadrática $q(x,y) = x^2 - y^2$ sobre F^2 es universal sobre F porque para cada $a \in F$ se tiene que $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$.*

Teorema 2.4.17. *Sea $a \in F^\times$. La forma cuadrática $q(x,y) = x^2 - ay^2$ sobre F^2 tiene un vector isotrópico sí y solo sí a es un cuadrado en $F^\times$, en este caso q es universal.*

Demostración. ($\Rightarrow$) Si a es un cuadrado en $F^\times$, digamos $a = c^2$ para algún $c \in F$ entonces $q(c,1) = (c)^2 - a(1)^2 = (a) - a = 0$ por lo que $(c,1)$ es un vector isotrópico para q.

($\Leftarrow$) Sea $(x_0, y_0) \in F^2$ un vector isotrópico para q. Así $x_0^2 = ay_0^2$ y $(x_0, y_0) \neq (0,0)$ Entonces x_0 y y_0 ambos no deberían ser nulos a la vez (pues $a \neq 0$) así $a = (x_0/y_0)^2$ es un cuadrado en $F^\times$. Por lo tanto, $q(x,y) = x^2 - (cy)^2$ donde $c = x_0/y_0$ y este es universal por el cálculo de Ejemplo 2.4.16. □

Teorema 2.4.18. *Sea q una forma cuadrática no degenerada sobre F^n. Si q tiene un vector isotrópico entonces q es universal sobre F.*

Demostración. Primera prueba: Sea $f(x_1, x_2, ..., x_n) = a_1x_1^2 + a_2x_2^2 + ... + a_nx_n^2$ una forma cuadrática no degenerada.

Supongamos que $(\alpha_1, \alpha_2, .., \alpha_n) \in F^n$ un vector isotrópico de q entonces se tiene que

$$a_1\alpha_1^2 + a_2\alpha_2^2 + ... + a_n\alpha_n^2 = 0 \tag{2.2}$$

Sin pérdida de generalidad podemos suponer que $\alpha_1 \neq 0$.

Sea γ cualquier elemento de F.

Consideremos el elemento $(x_1, x_2, x_3, ..., x_n)$ de F^n en términos de una variable $t \in F$ del siguiente modo:

$$\begin{aligned} x_1 &= \alpha_1(1+t) \\ x_2 &= \alpha_2(1-t) \\ x_3 &= \alpha_3(1-t) \\ \vdots &\quad \vdots \\ x_n &= \alpha_n(1-t) \end{aligned}$$

Sustituyendo en la forma cuadrática q, tenemos:

$q(x_1, x_2, ..., x_n) = a_1\alpha_1^2(1+t)^2 + a_2\alpha_2^2(1-t)^2 + ... + a_n\alpha_n^2(1-t)^2$

$= (a_1\alpha_1^2 + a_2\alpha_2^2 + ... + a_n\alpha_n^2) + 2t(a_1\alpha^2 - a_2\alpha_2^2 - ... - a_n\alpha_n^2) + t^2(a_1\alpha_1^2 + a_2\alpha_2^2 + ... + a_n\alpha_n^2)$

$= (0) + 2t(a_1\alpha_1^2 - a_2\alpha_2^2 - ... - a_n\alpha_n^2) + t^2(0)$

$= 2t(2a_1\alpha_1^2 - (a_1\alpha_1^2 + a_2\alpha_2^2 + ... + a_n\alpha_n^2))$

$= 2t(2a_1\alpha_1^2 - (0)) = 4ta_1\alpha_1^2.$

Si $q(x_1, x_2, ..., x_n) = \gamma$ entonces $4ta_1\alpha_1^2 = \gamma$, debe ocurrir que $t = \dfrac{\gamma}{4a_1\alpha_1^2}$

Por lo tanto, q representa a γ.

Segunda Prueba: Supongamos que $dimV \geq 2$ puesto que una forma cuadrática 1-dimensional no degenerada no puede tener un vector isotrópico.

Note que para cualesquiera vectores v, $w \in V$ y escalares α, $\beta \in F$,

$$\begin{aligned} q(\alpha v + \beta w) &= q(\alpha v) + q(\beta w) + 2b(\alpha v, \beta w) \\ &= \alpha^2 q(v) + \beta^2 q(w) + 2\alpha\beta b(v, w) \end{aligned} \tag{2.3}$$

Sea v_0 un vector isotrópico para q. Si podemos encontrar otro vector isotrópico w_0 tal que $b(v_0, w_0) \neq 0$ entonces v_0 y w_0 son linealmente independientes (si $w_0 = cv_0$, entonces $b(v_0, w_0) = cb(v_0, v_0) = 0$). Además, tendríamos

$$q(\alpha v_0 + \beta w_0) = 2\alpha\beta b(v_0, w_0). \tag{2.4}$$

Así, si fijamos $\beta = 1$ y dejamos variar a α en F entonces el lado derecho de (2.4) toma todos los valores en F, así q es universal.

Ahora encontraremos tal w_0. Por la no degeneración, $b(v_0, v_0') \neq 0$ para algún v_0'. Entonces multiplicando por escalares a v_0' podemos suponer $b(v_0, v_0') = 1$. Así $\{v_0, v_0'\}$ es linealmente independiente y

$$q(\alpha v_0 + v_0') = q(v_0') + 2\alpha \tag{2.5}$$

por (2.3). El lado derecho de (2.5) es cero cuando $\alpha = -\dfrac{v_0'}{2}$ (recuerde que $char(F) \neq 2$). Por lo tanto, podemos usar $w_0 = -q(\dfrac{v_0'}{2})v_0 + v_0'$ como nuestro segundo vector isotrópico. □

Observación 2.4.19. *En la segunda prueba del Teorema 2.4.18, podemos multiplicar por escalares a* w_0 *así* $b(v_0, w_0) = 1$. *Entonces* $q(v_0 + \frac{1}{2}w_0) = 1$ *y* $q(v_0 - \frac{1}{2}w_0) = -1$. *Así en el plano generado por* $v_0 + \frac{1}{2}w_0$, $v_0 - \frac{1}{2}w_0$,

$$q(x(v_0 + \frac{1}{2}w_0) + y(v_0 - \frac{1}{2}w_0)) = x^2 - y^2.$$

Esto significa que q *tiene un vector isotrópico sí y solo sí* V *contiene un plano en el cual* q *es* $x^2 - y^2$.

Corolario 2.4.20. *Sea* $q(x_1, ..., x_n)$ *una forma cuadrática no degenerada sobre* F^n. *Para* $r \in F^\times$, *los siguientes enunciados son equivalentes:*
1) $q(a_1, ..., a_n) = r$ *es soluble para algún* $(a_1, ..., a_n) \in F^n$
2) la forma cuadrática $q(x_1, ..., x_n) - rx_{n+1}^2$ *sobre* F^{n+1} *tiene un vector isotrópico.*

Demostración. 1) $\Rightarrow$ 2) Supongamos que $q(a_1, ..., a_n) = r$ es soluble para algún $(a_1, ..., a_n) \in F^n$ entonces $q(a_1, ..., a_n) - rx_{n+1}^2 = r - rx_{n+1}^2$, por lo que $(a_1, ..., a_n, 1)$ es un vector isotrópico para $q(a_1, ..., a_n) - rx_{n+1}^2$.
2) $\Rightarrow$ 1) Supongamos que $(a_1, ..., a_n, a_{n+1})$ sea un vector isotrópico de $q(x_1, ..., x_n) - rx_{n+1}^2$. Si $a_{n+1} \neq 0$ entonces

$$r = \frac{1}{a_{n+1}^2} q(a_1, ..., a_n) = q(\frac{a_1}{a_{n+1}}, ..., \frac{a_n}{a_{n+1}}).$$

Así q representa a r en F^n.
Si $a_{n+1} = 0$, entonces $(a_1, ..., a_n) \neq 0$ desde que $(a_1, ..., a_n, a_{n+1}) \neq 0$ Entonces q tiene un vector isotrópico $(a_1, ..., a_n)$, así por el teorema 2.4.18 q es universal sobre F^n. En particular, q representa a r en F^n □

Ejemplo 2.4.21. *Se puede describir un contraejemplo para la recíproca del Teorema 2.4.18 sobre* $\mathbb{Q}$. *La forma cuadrática* $x^2 + y^2 + z^2 - 7t^2$ *sobre* $\mathbb{Q}^4$ *no tiene un vector isotrópico: si es ocurre entonces 7 es suma de tres cuadrados racionales por el Corolario 2.4.20. Así 7 es una suma de tres cuadrados enteros por el Teorema 1.0.7 pero esto es falso. Aún así Veremos en la Sección 4.5 que la forma cuadrática es universal sobre* $\mathbb{Q}^4$ *por el Teorema de Hasse-Minkowski.*

Corolario 2.4.22. *Sean q_1 y q_2 dos formas cuadráticas no degeneradas sobre V tal que q sea la forma cuadrática sobre $V \oplus V$:*

$$q(v, w) = q_1(v) - q_2(w)$$

Entonces q_1 y q_2 tienen un valor común no nulo sobre V sí y solo sí q tiene un vector isotrópico sobre V.

Demostración. ($\Rightarrow$) Si q_1 y q_2 tienen un valor común no nulo sobre V es claro que q tiene un vector isotrópico.
($\Leftarrow$) Supongamos que q_1 o q_2 tiene un vector isotrópico v_0 Entonces $(v_0, 0)$ o $(0, v_0)$ es un vector isotrópico de q. Esto significa que al menos uno de q_1 y q_2 es universal desde que ellos son no degenerados, sin pérdida de generalidad supongamos que q_1 es universal. Entonces q_1 y q_2 representan un valor común no nulo sobre F desde que q_2 es no degenerado y además, toma algún valor no nulo sobre F. Notemos que q tenga un vector isotrópico juega un rol importante en este caso.
Ahora supongamos que q tiene un vector isotrópico y que ninguno de los dos, q_1 ni q_2 tienen vectores isotrópicos. Desde que q tiene un vector isotrópico, digamos (v_0, w_0), tenemos

$$q_1(v_0) = q_2(w_0) \tag{2.6}$$

y $(v_0, w_0) \neq (0, 0)$. El valor común de q_1 y q_2 en (2.6) es no nulo desde que $q_1(v_0) \neq 0$ si $v_0 \neq 0$ y $q_2(w_0) \neq 0$ si $w_0 \neq 0$. □

Teorema 2.4.23. *Para un espacio 2-dimensional (V, q), son equivalentes:*
1) (V, q) es un plano hiperbólico.
2) (V, q) es no degenerada y contiene un vector isotrópico.
3) $disc(q) \sim -1$

Demostración. (2) $\Rightarrow$ (1): Proviene de la observación 2.4.19.
(1) $\Rightarrow$ (3): Sea (V, q) un plano hiperbólico. Por definición, $q(xe_1 + ye_2) = x^2 - y^2$ en alguna base $\{e_1, e_2\}$. Así $disc(q) \sim -1$.

(3) $\Rightarrow$ (2): El espacio cuadrático (V, q) es no degenerado desde que $disc(q) \neq 0$. Escogemos $v \in V$ tal que $q(v) \neq 0$. Extendemos v a una base ortogonal $\{v, w\}$ de V. Relativo a la base $\{v, w\}$

$$q(xv + yw) = q(v)x^2 + q(w)y^2 = cx^2 + q(w)y^2$$

donde $c = q(v)$. Entonces $disc(q) = cdisc(q) \sim -1$ por nuestra hipótesis, lo que significa que

$$q(w) \sim \frac{-1}{c} \sim -c$$

desde que $c \neq 0$. Entonces multiplicando por escalares a w, podemos suponer que $q(w) = -c$. Así $q(v + w) = c - c = 0$. Por lo tanto, $v + w$ es un vector isotrópico. $\square$

2.5. Teorema de Witt

En esta sección daremos algunos de los teoremas básicos de la teoría de formas bilineales simétricas.
(V, b) siempre denotará un espacio bilineal simétrico regular.

Definición 2.5.1. *Sea $x \in V$ un vector anisotrópico y $W = \{x\}^{\perp}$ entonces la **aplicación lineal***

$$\begin{aligned} \tau_x : V &\rightarrow V \\ y &\mapsto \tau_x(y) = y - 2\frac{b(x,y)}{b(x,x)}x \end{aligned}$$

*es llamado **reflexión en el hiperplano** W ortogonal a x.*

El nombre es sugerido por la propiedad (1) del siguiente

Lema 2.5.2. *Se cumplen:*

1. $\tau_x(x) = -x$, $\tau_x|_W = id_W$
2. τ_x *es una isometría de* (V, b)
3. $\tau_x \circ \tau_x = id$

4. $det\tau_x = -1$

Demostración. Se tiene que:

1. $\tau_x(x) = x - 2.\dfrac{b(x,x)}{b(x,x)}x = x - 2x = -x$

   Por otro lado, supongamos $w \in W$ cualesquiera entonces $w \in \{x\}^{\perp}$ por lo tanto

   $b(x,w) = 0$

   luego $\tau_x(w) = w - 2\dfrac{b(x,w)}{b(x,x)}w = w = id_W(w)$

   Por lo tanto, $\tau_x|_W = id_W$

2. $\underline{\tau_x \text{ es t.l.}}$

$$\begin{aligned}
\tau_x(ay+cz) &= (ay+cz) - 2\frac{b(x,ay+cz)}{b(x,x)}x \\
&= (ay+cz) - 2\frac{b(x,ay}{b(x,x)}x - 2\frac{b(x,cz}{b(x,x)}x \\
&= \left(ay - 2a\frac{b(x,y)}{b(x,x)}x\right) + \left(cz - 2c\frac{b(x,z)}{b(x,x)}x\right) \\
&= a\left(y - 2\frac{b(x,y)}{b(x,x)}x\right) + c\left(z - 2\frac{b(x,z)}{b(x,x)}x\right) \\
&= a\tau_x(y) + c\tau_x(z)
\end{aligned}$$

   $\underline{\tau_x \text{ es inyectiva}}$

   Si $\tau_x(y) = \theta$ entonces $y - 2\dfrac{b(x,y)}{b(x,x)}x = \theta$ por lo que $y = 2\dfrac{b(x,y)}{b(x,x)}x$

   luego

$$\begin{aligned}
b(x,y) &= b\left(x, 2\frac{b(x,y)}{b(x,x)}x\right) \\
&= 2\frac{b(x,y)}{b(x,x)}b(x,x) \\
&= 2b(x,y) \quad \text{... pues } b(x,x) \neq 0
\end{aligned}$$

$$b(x,y) = 0$$

   entonces $y \in V^{\perp} = \{\theta_V\}$ por lo que $y = \theta_V$

   $\underline{\tau_x \text{ es isometría}}$

   Ya vimos que τ_x es transformación lineal inyectiva.

$$\begin{aligned} b(\tau_x(y),\tau_x(z)) &= b\left(y-2\frac{b(x,y)}{b(x,x)}x, z-2\frac{b(x,z)}{b(x,x)}x\right) \\ &= b(y,z)-2\frac{b(x,z)}{b(x,x)}b(y,x)-2\frac{b(x,y)}{b(x,x)}b(x,z)+4\frac{b(x,y)b(x,z)}{[b(x,x)]^2}b(x,x) \\ &= b(y,z)-4\frac{b(x,y).b(x,z)}{b(x,x)}+4\frac{b(x,y).b(x,z)}{b(x,x)} \\ &= b(y,z) \quad \text{para todo } y,z \text{ en } V \end{aligned}$$

Por lo tanto τ_x es una isometría de (V,b).

3. Sea $y \in V$ cualquiera

$$\begin{aligned} (\tau_x \circ \tau_x)(y) &= \tau_x(\tau_x(y)) \\ &= \tau_x\left(y-2\frac{b(x,y)}{b(x,x)}x\right) \\ &= \left(y-2\frac{b(x,y)}{b(x,x)}x\right)-2\frac{b\left(x, y-2\frac{b(x,y)}{b(x,x)}x\right)}{b(x,x)}x \\ &= y-2\frac{b(x,y)}{b(x,x)}x-2\frac{b(x,y)}{b(x,x)}x+4\frac{b(x,y)}{b(x,x)}.\frac{b(x,x)}{b(x,x)}x \\ &= y-4\frac{b(x,y)}{b(x,x)}x+4\frac{b(x,y)}{b(x,x)}x \\ &= y \\ &= id(y) \end{aligned}$$

Por lo tanto $\tau_x \circ \tau_x = id_W$

4. Sea $\{e_2, e_3, ..., e_n\}$ una base de W y completamos a una base de V con $e_1 = x$ obteniendo $\{x, e_2, e_3, ..., e_n\}$ luego

$$\begin{aligned} \tau_x(x) &= -x \\ \tau_x(e_i) &= e_i - 2\frac{b(x,e_i)}{b(x,x)}x \quad i = 1,2,3,... \\ &= e_i \text{ pues } b(x,e_i) = 0 \end{aligned}$$

por lo tanto la matriz asociada a τ_x en esta base tiene la forma:

$$\begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

el cual tiene determinante igual a -1.

□

Ahora formulamos dos teoremas básicos. Solo se dará una prueba de una forma débil del segundo teorema, se puede leer a Artin: Geometric Algebra o a Dieudonné para una prueba completa.

Teorema 2.5.3. *(Witt) Sea (V, b) un espacio bilineal simétrico regular. Sea W un subespacio de V y $\sigma : W \to V$ una isometría entonces existe una isometría $\Sigma : V \to V$ que extiende a σ, es decir $\Sigma|_W = \sigma$.*

Teorema 2.5.4. *(Cartan-Dieudonné) Sea (V, b) un espacio lineal simétrico regular entonces cada isometría $\sigma \in O(V, b)$ es un producto de a lo más n reflexiones donde $n = dim_F V$.*

Probaremos el siguiente resultado el cual es obviamente un desprendimiento de 2.5.4 tomando $W = V$ y que implica una forma débil del Teorema 2.5.3 tomando $W = V$.

Teorema 2.5.5. *Sea (V, b) un espacio bilineal simétrico regular. Sea W un subespacio de V y $\sigma : W \to V$ una isometría entonces existe un producto de reflexiones Σ que extiende a σ.*

Para la prueba necesitamos el siguiente lema trivial.

Lema 2.5.6. *Supongamos que W no es totalmente isotrópico entonces existe un vector anisotrópico $x \in W$.*

Demostración. Como W no es totalmente isotrópico entonces existen los vectores y, z en W tales que $b(y, z) \neq 0$.
Como $b(y, z) = \frac{1}{2}\{b(y + z, y + z) - b(y, y) - b(z, z)\}$ entonces alguno de los sumandos del las llaves no es cero por lo que $y + z$ ó y ó z es vector anisotrópico. □

Demostración. Del Teorema 2.5.5. Consideremos primero el caso especial $W = xF$, donde x es anisotrópico.
Sea $y = \sigma(x)$ entonces

$$b(x + y, x + y) + b(x - y, x - y) = 4b(x, x).$$

Como $\text{char}(F) \neq 2$ entonces o $x+y$ o $x-y$ es anisotrópico. En el primer caso ponemos $\Sigma = \tau_{x-y}$ y en el segundo caso, ponemos $\Sigma = \tau_{x+y}\tau_x$. Se puede verificar fácilmente que $\Sigma(x) = y = \sigma(x)$, así que Σ extiende a σ. □

Observación 2.5.7. *Si el espacio (V, b) es anisotrópico nuestros argumentos dan una prueba del Teorema 2.5.4: Sea $\sigma : V \to V$ una isometría y escogemos un vector $x \neq \theta$. Si $\sigma(x) = x$ entonces $\sigma(x^\perp) = x^\perp$ y por hipótesis inductiva σ es un producto de a lo más $n-1$ reflecciones. Si $y = \sigma(x) - x \neq 0$, entonces y es anisotrópico y $\tau_y(\sigma(x)) = x$. Así σ es un producto de a lo más n reflecciones.*

Ahora derivamos algunas consecuencias del Teorema de Witt.

Corolario 2.5.8. *(Cancelación de Witt) Sean (V, b) y (V', b') espacios isométricos con descomposición ortogonal $V = W_1 \perp W_2$, $V' = W_1' \perp W_2'$ tales que W_1 y W_1' son regulares e isométricos entonces W_2 y W_2' son isométricos.*

Corolario 2.5.9. *Todos los subespacios isotrópicos totalmente maximal de (V, b) tienen la misma dimensión.*

Definición 2.5.10. *La dimensión común de los subespacios isotrópicos totalmente maximal de un espacio regular (V, b) es llamado el* ***índice de Witt*** *de (V, b) y será denotado por $ind(V, b)$.*

Corolario 2.5.11. *(Descomposición de Witt) Supongamos que el espacio (V, b) tenga índice de Witt igual a m. Entonces*

$$V = H_1 \perp ... \perp H_m \perp V_1$$

donde H_i son planes hiperbólicos y V_1 es anisotrópico. V_1 es únicamente determinada salvo isometrías.

Definición 2.5.12. *(V_1, b_{V_1}) es llamado la componente anisotrópico o parte anisotrópica (o le forma kernel) de (V, b). Dos espacios bilineales ϕ, ψ son llamadas similar (o Witt equivalente) si ellos tienen componentes isométricas anisotrópicas. Esto es,*

$\phi \perp \mathbb{H}(F^n) \cong \psi \perp \mathbb{H}(F^m)$ para adecuados n, m. La parte isotrópica de ϕ será denotada después por ϕ_{an}. Similarmente será denotada por $\sim$. Los resultados de esta sección nos dicen que cada espacio bilineal simétrico es similar a un espacio anisotrópico el cual es únicamente determinado salvo isometría.

Capítulo 3

Cuerpos locales

El capítulo está diseñado considerando un cuerpo F local como una generalización de $\mathbb{Q}$. De esta manera se puede ver el teorema de Hasse-Minkowski sobre cualquier cuerpo global, donde en general los cuerpos locales puedan jugar un rol importante como cuerpo p-adico en el teorema de Hasse-Minkowski sobre $\mathbb{Q}$.

3.1. Generalidades

Nuestro objetivo en esta sección es tomar lo que el lector debe saber sobre los cuerpos $\mathbb{Q}_p$ y examinar resultados análogos en un contexto más general. Mucho de los resultados pueden ser establecidos sin una prueba desde que las pruebas p-ádicas se aplican sin un cambio significante. En esta sección $\mathbb{F}$ denota cualquier cuerpo finito (posiblemente de característica 2).
En esta sección F es un cuerpo completo con respecto a un valor absoluto no Arquimediano $|\cdot|$. El anillo entero de F es $\mathcal{O} = \{x \in F : |x| \leq 1\}$ cuyo grupo unitario es $\mathcal{O}^\times = \{x \in F : |x| = 1\}$. El complemento de $\mathcal{O}^\times$ en $\mathcal{O}$ es $\mathfrak{m} = \{x \in F : |x| < 1\}$ el cual es un ideal maximal. El cuerpo $\mathcal{O}/\mathfrak{m}$ es llamado el cuerpo residual de F.

Ejemplo 3.1.1. *Si $F = \mathbb{Q}_p$ entonces $\mathcal{O} = \mathbb{Z}_p$ y $\mathfrak{m} = p\mathbb{Z}_p$. Más aún,*

$$\mathcal{O}/\mathfrak{m} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

Definición 3.1.2. *Un **valor absoluto** sobre un cuerpo F es una función $|\cdot| : F \to \mathbb{R}$ tal que:*

1. $|x| \geq 0$ *y* $|x| = 0$ *sí y solo sí* $x = 0$.

2. $|xy| = |x||y|$ *para todo* $x, y \in F$.

3. $|x + y| \leq |x| + |y|$ *para todo* $x, y \in F$. *(La desigualdad triangular)*

Definición 3.1.3. *Un* ***valor absoluto*** *sobre* F *es llamado* ***No arquimediano*** *si satisface la* ***desigualdad ultramétrica****:* $|x + y| \leq \text{máx}\{|x|, |y|\}$ *para todo* $x, y \in F$*; en caso contrario, diremos que es* ***arquimediana****.*

Recordemos que existe un valor absoluto en $\mathbb{Q}$ correspondiente a cada número primo p: para $r \in \mathbb{Q}$,

$$|r|_p = \begin{cases} p^{-ord_p(r)}, & \text{para } r \in \mathbb{Q}^\times \\ 0, & \text{para } r = 0 \end{cases} \tag{3.1}$$

donde $ord_p(r)$ es el exponente de p en r. Completando $\mathbb{Q}$ con respecto a estos valores absolutos se generan los cuerpos $\mathbb{Q}_p$ mientras que completando $\mathbb{Q}$ con respecto al valor absoluto usual:

$$|r|_\infty = \begin{cases} r, & \text{para } r \geq 0 \\ -r, & \text{para } r \leq 0 \end{cases} \tag{3.2}$$

se genera $\mathbb{R}$.

Observación 3.1.4. *Como una convención usamos* v *como el nombre de un valor absoluto general no trivial sobre* $\mathbb{Q}$ *como en (3.1), (3.2). La notación* $\mathbb{Q}_v$ *(donde* $\mathbb{Q}_\infty = \mathbb{R}$ *y* $|\cdot|_\infty$ *denota el usual valor absoluto arquimediano sobre* $\mathbb{Q}$*) es usado para representar cualquier completación de* $\mathbb{Q}$*. De esta manera se puede escribir todas esas completaciones de una manera común.*

Los valores absolutos de $\mathbb{Q}$ que fueron descritos son una lista completa de valores absolutos no triviales salvo equivalencias en el siguiente sentido.

Definición 3.1.5. *Dos* ***valores absolutos*** *sobre un cuerpo son* ***equivalentes*** *cuando ellos definen la misma topología.*

Observación 3.1.6. *De la definición 3.1.5, cualquier vecindad esférica de un punto definido por uno de esos valores absolutos es también una vecindad esférica definido por el otro valor absoluto.*

Teorema 3.1.7. *Si $|\cdot|_1$ y $|\cdot|_2$ son valores absolutos equivalentes sobre un cuerpo F entonces $|\cdot| = |\cdot|_2^t$ para algún $t > 0$. En particular, cada una de las propiedades $|x| < 1$, $|x| = 1$, $|x| > 1$ no cambia si el valor absoluto $|\cdot|$ es reemplazado por un valor absoluto equivalente.*

Demostración. Si $|a|_1 < |b|_1 \Rightarrow \dfrac{|a|_1}{|b|_1} < 1 \Rightarrow |\dfrac{a}{b}|_1 < 1 \Rightarrow |\dfrac{a}{b}|_2 < 1$

$\Rightarrow \dfrac{|a|_2}{|b|_2} < 1 \Rightarrow |a|_2 < |b|_2$

Por lo tanto, $|a|_1 > 1 = |1|_1$ implica que $|a|_2 > |1|_2 = 1$.

Como $|.|_1$ es no trivial, para algún $a_0 \neq 0$ se tiene $|a_0| > 1$ entonces $|a_0|_2 > 1$.

Sea a cualquier elemento tal que $|a|_1 > 1$ y por lo tanto, $|a|_2 > 1$.

Sea $t = \dfrac{log|a|_1}{log|a_0|_1}$ entonces $t > 0$ y por definición de logaritmos, $|a|_1 = |a_0|_1^t$.

Afirmación: $|a|_2 = |a_0|_2^t$

Análogamente, tenemos $|a|_2 = |a_0|_2^{t'}$ con $t' > 0$

Si $t' \neq t$ entonces existe un número racional tal que $t < r < t'$ o $t' < r < t$.

En el primer caso, $|a_0|_2^r < |a|_2$ y en el segundo caso, $|a_0|_2^r > |a|_2$. Por lo tanto nuestra afirmación puede probarse demostrando que si r es un número racional mayor que t entonces $|a_0|_2^r > |a|_2$ y si r es un número racional positivo menor que t entonces $|a_0|_2^r > |a|_2$. Sea $r = \dfrac{m}{n} > t$ donde m y n son enteros positivos entonces $|a|_1 < |a_0|_1^{m/n}$ se tiene que $|a^n|_1 < |a_0^m|_1$ se implica que $|a^n|_2 < |a_0^m|_2$ entonces $|a|_2 < |a_0|_2^{m/n}$.

Similarmente, si $r = \dfrac{m}{n}$ entonces $|a|_2 > |a_0|_2^{m/n}$. Por lo tanto, $|a|_2 = |a_0|_2^t$ y

$$t = \frac{log|a|_2}{log|a_0|_2} = \frac{log|a|_1}{log|a_0|_1}$$

entonces

$$t = \frac{log|a|_2}{log|a|_1} = \frac{log|a_0|_2}{log|a_0|_1}$$

Entonces $|a|_2 = |a|_1^s$ con $s = \dfrac{log|a_0|_2}{log|a_0|_1} > 0$ y esto se cumple para todo a tal que $|a|_1 > 1$.

Si $|a|_1 < 1$ tenemos que $|a_1^{-1}| > 1$ entonces $|a^{-1}|_2 = |a^{-1}|_1^s$ lo que implica que $|a|_2 = |a|_1^s$.

Por lo tanto, $|a|_2 = |a|_1^s$ y hemos probado que esto implica la equivalencia de los valores absolutos.

□

Teorema 3.1.8. *Un valor absoluto $|\cdot|$ de un cuerpo F es no arquimediano sí y solo sí $|n1| \leq 1$ para todo $n \in \mathbb{Z}$.*

Demostración. ($\Rightarrow$) Como $|n| = |-n|$ podemos suponer que $n \geq 1$.

$$|n1| = |\underbrace{1 + \cdots + 1}_{n \quad veces}| \leq max\{|1|, ..., |1|\} = 1$$

entonces $|n1| \leq 1$ para todo $n \in \mathbb{Z}$.

($\Leftarrow$) Sean $a, b \in F$ entonces para cualquier entero positivo n se tiene

$$\begin{aligned}
|a+b|^n &= |a^n + \tbinom{n}{1}a^{n-1}b + \tbinom{n}{2}a^{n-2}b^2 + \cdots + b^n| \\
&\leq |a^n| + \tbinom{n}{1}|a^{n-1}b| + \tbinom{n}{2}|a^{n-2}b^2| + \cdots + |b^n| \\
&\leq |a^n| + |\tbinom{n}{1}||a^{n-1}||b| + |\tbinom{n}{2}||a^{n-2}||b^2| + \cdots + |b^n| \\
&\leq (1)|a^n| + (1)|a^{n-1}||b| + (1)|a^{n-2}||b^2| + \cdots + (1)|b^n| \\
&\leq \underbrace{(\text{máx}\{|a|, |b|\})^n + (\text{máx}\{|a|, |b|\})^n + \cdots + (\text{máx}\{|a|, |b|\})^n}_{(n+1) \quad veces} \\
&= (n+1)(\text{máx}\{|a|, |b|\})^n
\end{aligned}$$

Entonces extrayendo raíz n-ésima $|a+n| \leq \sqrt[n]{n+1}(\text{máx}\{|a|, |b|\})$.

Como $\lim_{n\to\infty} \sqrt[n+1]{n} = 1$ en $\mathbb{R}$, $|a+n| \leq \text{máx}\{|a|, |b|\})$. □

Teorema 3.1.9. *(Ostrowski) Se tiene que:*

a) Cualquier valor absoluto arquimediano sobre $\mathbb{Q}$ es equivalente a $|\cdot|_\infty$.

b) Cualquier valor absoluto no trivial no arquimediano sobre $\mathbb{Q}$ es equivalente a $|\cdot|_p$ para algún primo p.

Demostración. (a) Supongamos que n y n' sean enteros mayor que 1.

Si $n' = a_0 + a_1 n + \cdots + a_k n^k$ donde $0 \leq a_i < n$. entonces

$$|n'| < n(1 + |n| + \cdots + |n|^k) \leq n(k+1)\,\text{máx}\{1, |n|^k\}$$

Como $n' \geq n^k$, $log(n') \geq log(n^k)$, $k \leq \dfrac{log(n')}{log(n)}$

entonces

$$|n'| < n\left(\frac{log(n')}{log(n)} + 1\right)\text{máx}\{1, |n|^{\frac{log(n')}{log(n)}}\}$$

Reemplazando n' por n'^r donde r es cualquier entero positivo, obtenemos

$$|n'^r| < n\left(\frac{log(n'^r)}{log(n)} + 1\right) \text{máx}\{1, |n|^{\frac{log(n'^r)}{log(n)}}\}$$

$$|n'^r| < n\left(\frac{rlog(n')}{log(n)} + 1\right) \text{máx}\{1, |n|^{\frac{rlog(n')}{log(n)}}\}$$

Extrayendo la raíz r-ésima:

$$|n'| < \sqrt[r]{n\left(\frac{rlog(n')}{log(n)} + 1\right)} \text{máx}\{1, |n|^{\frac{log(n')}{log(n)}}\}$$

Para cualesquiera números reales a y b, $\lim_{r\to\infty}(ra+b)^{\frac{1}{r}} = 1$ porque se tiene que $\lim_{r\to\infty} \frac{1}{r}(ra+b) = 0$, por lo tanto se tiene que

$$|n'| \leq \text{máx}\{1, |n|^{\frac{log(n')}{log(n)}}\} \tag{3.3}$$

para cualesquiera enteros n, n' tales que $n, n' > 1$.

Como $|\cdot|$ es arquimediano por el Teorema 3.1.8 existe un n' tal que $|n'| > 1$ entonces $|n'| \leq |n|^{\frac{log(n')}{log(n)}}$ para $|n| > 1$ para todo $n > 1$. Entonces 3.3 se cumple para cualesquier n, n' tales que $n, n' > 1$. Por lo tanto,

$$|n'|^{\frac{1}{log(n')}} \leq |n|^{\frac{1}{log(n)}}$$

para todo $n, n' > 1$. Por simetría, tenemos

$$|n'|^{\frac{1}{log(n')}} = |n|^{\frac{1}{log(n)}}$$

Entonces aplicando logaritmos $\frac{log|n'|}{log(n')} = \frac{log|n|}{log(n)}$ y tomando $s = \frac{log|n'|}{log(n')} > 0$ se tiene que $s = \frac{log|n|}{log(n)}$ por lo que $|n| = n^s$ para todos los enteros $n > 1$. De ahí se sigue que $|a| = |a|_\infty^s$ para todo $a \neq 0$ en $\mathbb{Q}$ y por lo tanto, $|\cdot|$ es equivalente a $|\cdot|_\infty$

(b) Tenemos que $|n| \leq 1$ para cada entero n.

Si $|n| = 1$ para todo $n \neq 0$ en $\mathbb{Z}$ entonces $|\cdot|$ es trivial, lo cual es una contradicción. Por lo tanto el conjunto $P = \{b \in \mathbb{Z}/|b| < 1\}$ contiene elementos no nulos. Ahora P es un

ideal en $\mathbb{Z}$ desde que $|b_1+b_2| \leq \text{máx}\{|b_1|,|b_2|\} < 1$ si $b_i \in P$ y $|nb| = |n||b| < 1$ si $n \in \mathbb{Z}$ y $b \in P$. También P es ideal primo desde que $|n| = 1$ y $|n'| = 1$ implica que $|nn'| = 1$. Por lo tanto, $P = (p)$ para algún primo $p > 0$. Ahora, sea $\gamma = |p|$ donde $0 < \gamma < 1$. Si $r \in \mathbb{Q}$, podemos escribir $r = p^k \dfrac{a}{b}$ donde $k \in \mathbb{Z}$ y $a, b \notin (p)$ entonces $|a| = 1 = |b|$ y $|r| = \gamma^k = \gamma^{v_p(p)}$. Por lo tanto, $|\cdot|$ es el valor absoluto p-ádico definido por γ. □

Los siguientes dos resultados enlazan a todos los valores absolutos sobre cada elemento de $\mathbb{Q}$ y $\mathbb{F}(T)$ como en (3.1) y (3.2).

Teorema 3.1.10. *Para $r \in \mathbb{Q}^\times$, $|r|_v \neq 1$ para un número finito de v y*

$$\prod_v |r|_v = 1.$$

Demostración. Sea $r = \pm p_1^{e_1} ... p_m^{e_m}$ donde los p_i son distintos primos. Entonces

$$\prod_{p_i} |r|_{p_i} = p_1^{-e_1} ... p_m^{-e_m},$$

para $p \neq p_i$: $|r|_p = 1$ y para $|r|_\infty = p_1^{e_1} ... p_m^{e_m}$, así

$$\prod_v |r|_v = 1.$$

□

Retornamos al escenario general. El siguiente teorema juega un rol importante en el teorema de Hasse-Minkowski para dimensión al menos 5.

Teorema 3.1.11. *Sean $|\cdot|_1, ..., |\cdot|_n$ valores absolutos no equivalentes no triviales sobre F entonces para cualquier k, $1 \leq k \leq n$ existe un $a_k \in F$ tal que*

$$|a_k|_k > 1, \quad |a_k|_l < 1 \quad si \quad l \neq k. \tag{3.4}$$

Demostración. Sin pérdida de generalidad supongamos que $k = 1$, tenemos que mostrar que existe un $a \in F$ tal que $|a|_1 > 1$ y $|a|_l < 1$ para cada $l > 1$. Haremos inducción sobre n.

Sea $n = 2$. Por el Teorema 3.1.8 existe $b \in F$ tal que $|b|_1 < 1$ y $|b|_2 \geq 1$ y $c \in F$ tal que $|c|_2 < 1$ y $|c|_1 \geq 1$ Entonces si tomamos $a = cb^-1$ tenemos que $|a|_1 > 1$ y $|a|_2 < 1$, por

lo tanto el enunciado se cumple para $n = 2$. Supongamos que se cumple para $n-1 \geq 2$. Entonces tenemos elementos b y c tales que

$$|b|_1 > 1, \quad |b|_2 < 1, ..., \quad |b|_{n-1} < 1,$$

$$|c|_1 > 1, \quad |c|_n < 1.$$

Distinguimos dos casos:

Caso I: $|b|_n \leq 1$. Consideremos $a_r = b^r c$. Tenemos $|a_r|_k = |b_k^r||c|_k$. Esto es > 1 si $k = 1$ y < 1 si $k > 1$ y r es suficientemente grande. Para cualquiera tal r pongamos $a = a_r$ Entonces se cumple (3.4).

Caso II: $|b|_n > 1$. Tomamos $a_r = \dfrac{b^r c}{1 + b^r}$. Si $2 \leq k \leq n-1$, $|b|_k < 1$ así $|b^r|_k \to_{r\to\infty} 0$ Entonces $|a_r| \to 0_{r\to\infty}$ y $|a_r|_k < 1$ para r suficientemente grande.

Sea $k = 1$ o n entonces $|b|_k > 1$ y por lo tanto, $|\dfrac{b^r}{1 + b^r}|_k = |\dfrac{1}{1 + \dfrac{1}{b^r}}|_k \to 1$ y $|a_r|_k \to c$.

Como $|c|_1 > 1$ y $|c|_n < 1$, tenemos que $|a_r|_1 > 1$ y $|a_r|_n < 1$ para r suficientemente grande. Por lo tanto, para un adecuado $a = a_r$ tenemos que $|a|_1 > 1$, $|a|_2 < 1$,...,$|a|_n > 1$. □

Teorema 3.1.12. *(Teorema de Aproximación) Sean $|\cdot|_1, ..., |\cdot|_n$ valores absolutos no equivalentes no triviales sobre un cuerpo F. Si $a_1, ..., a_n$ son elementos de F y ε un número real positivo Entonces existe un $a \in F$ tal que*

$$|a - a_k|_k < \varepsilon \text{ para todo } 1 \leq k \leq n. \tag{3.5}$$

Demostración. Sean $|\cdot|_1, ..., |\cdot|_n$ valores absolutos no equivalentes no triviales sobre un cuerpo F. Si $a_1, ..., a_n$ son elementos de F, para cada k con $1 \leq k \leq n$ aplicamos el Teorema 3.1.11 para obtener un elemento b_k tal que $|b_k|_k > 1$ y $|b_k|_l$ para todo $l \neq k$. Entonces

$$|\frac{b_k^r}{1 + b_k^r}|_k \to 1$$
$$|\frac{b_k^r}{1 + b_k^r}|_l \to 0 \quad \text{si } l \neq k.$$

Por lo tanto, $|\frac{a_k b_k^r}{1+b_k^r}|_k \to a_k$ y $|\frac{a_k b_k^r}{1+b_k^r}|_l \to 0$ *si* $l \neq k$.

Entonces

$$|\sum_{k=1}^{n} \frac{a_k b_k^r}{1+b_k^r}|_l \to a_j \text{ para cada } j, 1 \leq j \leq n.$$

Por lo tanto, para cualquier $\varepsilon > 0$ podemos tomar

$$a_k = \frac{a_k b_k^r}{1+b_k^r}$$

para r suficientemente grande y tenemos la relación requerida $|a - a_k|_k < \varepsilon$, $1 \leq k \leq n$. □

Sobre cuerpos con un valor absoluto no arquimediano no trivial existe una analogía del método de Newton para encontrar raíces reales de polinomios; este es el siguiente teorema.

Teorema 3.1.13. *(Lema de Hensel) Sea* $f(X) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$ *un polinomio con coeficientes en* $\mathcal{O}$. *Supongamos que existe* $\alpha_0 \in \mathcal{O}$ *tal que:*

$$|f(\alpha_0)| < |f'(\alpha_0)|^2,$$

donde f' *es la derivada (formal) de* f. *Entonces existe un* $\alpha \in \mathcal{O}$ *tal que* $\alpha \equiv \alpha_0$ mód $\mathfrak{m}$ *y* $f(\alpha) = 0$.

Demostración. Ver Proposición 7.6 del Capítulo XII de [8] o Sección 9.11 de [3]. □

Ejemplo 3.1.14. *Si el cuerpo residual no es de característica* 2 *entonces* $a \in \mathcal{O}^\times$ *es un cuadrado en* F *si y solo si* a *es un cuadrado en* $\mathcal{O}/\mathfrak{m}$. *Consideremos el polinomio* $X^2 - a$ *y aplicamos el lema de Hensel donde* $\alpha_0^2 \equiv a \mod \mathfrak{m}$. *Note que* 2 *está en* $\mathcal{O}^\times$.

Ejemplo 3.1.15. *Si* $\mathcal{O}/\mathfrak{m}$ *tiene característica 2 y* F *tiene característica* 0 *(por ejemplo* $F = \mathbb{Q}_2$*) entonces* $a \in \mathcal{O}^\times$ *es un cuadrado en* F *si y solo si* a *es un cuadrado módulo* $4\mathfrak{m}$. *Otra vez, considerar el polinomio* $f(X) = X^2 - a$. *Para* $\alpha_0 \in \mathcal{O}^\times$, $|f'(\alpha_0)|^2 = |4|$. *Así el lema de Hensel se aplica cuando* a *es congruente a un cuadrado módulo* $4\mathfrak{m}$.

El siguiente resultado es una versión multivariable del lema de Hensel.

Teorema 3.1.16. *Sea $g(X_1, ..., X_n)$ un polinomio con coeficientes en $\mathcal{O}$. Supongamos que existen $\gamma_1, ..., \gamma_n$ en $\mathcal{O}$ tal que para algún i,*

$$|g(\gamma_1, ..., \gamma_n)| < |\frac{\partial g}{\partial X_i}(\gamma_1, ..., \gamma_n)|^2.$$

Entonces existe $\alpha \in \mathcal{O}$ tal que $g(\gamma_1, ..., \alpha, ..., \gamma_n) = 0$.

Demostración. Sea $f(X) = g(\gamma_1, ..., \gamma_{i-1}, X, \gamma_{i+1}, ..., \gamma_n)$ Entonces

$$f'(X) = \frac{\partial g}{\partial X_i}(\gamma_1, ..., \gamma_{i-1}, X, \gamma_{i+1}, ..., \gamma_n).$$

Aplicando el lema de Hensel a f con $\alpha_0 = \gamma_i$ da una raíz de g. □

Definición 3.1.17. *Cuando $\mathfrak{m}$ es principal, un **uniformizador** de F es cualquier elemento π que genera a $\mathfrak{m}$: $\mathfrak{m} = (\pi) = \pi\mathcal{O}$.*

Observación 3.1.18. *Cuando F es discretamente valuado y $|F^\times| = c^{\mathbb{Z}}$ con $c > 1$, un uniformizador π puede ser equivalentemente definido como cualquier elemento de mayor valor absoluto menor que 1: $|\pi| = \frac{1}{c}$.*

Ejemplo 3.1.19. *En $\mathbb{Q}_p$, la selección usual del uniformizador es p. Aunque, se puede escoger cualquier elemento con valor absoluto $1/p$; por ejemplo, $-p$ también satisface.*

Proposición 3.1.20. *Sea π un uniformizador de F. Cada $x \in F^\times$ es $\pi^m u$ para único $m \in \mathbb{Z}$ y $u \in \mathcal{O}^\times = \{x \in F : |x| = 1\}$. Más aún, cualesquiera dos uniformalizadores son iguales salvo para un múltiplo unitario y $x \in \mathcal{O}$ si y solo si $m \geq 0$.*

Definición 3.1.21. *Sea π ser un uniformizador de F. Para $x \in F$ **la valuación** de x es el exponente de π en x. Esto es, si $x = \pi^m u$ para $u \in \mathcal{O}^\times$ entonces la valuación de x es m. Esto es independiente de la elección de π. La valuación de x se denota como ord(x).*

Usando la función valuación y asignando $c = |\pi|^{-1} > 1$, tenemos:

$$|x| = |\pi|^m = \begin{cases} c^{-ord(x)}, & \text{para } x \in F^\times \\ 0, & \text{para } x = 0 \end{cases}$$

Ahora estamos listos para definir un cuerpo local.

Definición 3.1.22. *Un **cuerpo local** es un cuerpo que es completo con respecto a un valor absoluto discreto (no arquimediano) y que tiene un cuerpo residual finito.*

Entonces, ¿cómo son los elementos de un cuerpo local F? Fijando un uniformalizador π y un conjunto S de representantes para $\mathcal{O}/\mathfrak{m}$ (usando el 0 para representar la clase de 0), cualquier x en $\mathcal{O}$ tiene un única expansión π-ádica:

$$x = c_0 + c_1\pi + c_2\pi^2 + ... \tag{3.6}$$

donde $c_i \in S$ y los c_i son únicamente determinados por x (S es fijado). ¿Qué pasa si $x \in F$ pero x no está en $\mathcal{O}$? Entonces x puede ser escrito como $x = \dfrac{y}{\pi^m}$ donde $m \geq 1$ y $y \in \mathcal{O}$. Escribiendo a y como una expansión π-ádica y dividendo por π^m da

$$x = c_0\pi^{-m} + c_1\pi^{-m+1} + ... + c_{m-1}\pi^{-1} + c_m + c_{m+1}\pi + ... \tag{3.7}$$

donde $c_i \in S$ y los c_i son únicamente determinados por x.

Teorema 3.1.23. *Sea F un cuerpo completo con respecto a un valor absoluto no trivial no arquimediano. Las siguientes proposiciones son equivalentes:*

1. *F es localmente compacto (cada punto tiene una vecindad compacta).*
2. *$\mathcal{O}$ es compacto.*
3. *F es un cuerpo local.*

Demostración. (2) $\Rightarrow$ (1): Elegimos $a \in F$. Desde que $\mathcal{O}$ es una vecindad compacta de cero y el mapeo $f(x) = a+x$ es un homeomorfismo de F consigo mismo, $a+\mathcal{O}$ es una vecindad compacta de a.

(1) $\Rightarrow$ (2): Supongamos que existe una vecindad compacta A de cero. Escogemos $\alpha \in \mathcal{O}$ con $0 < |\alpha| < 1$, así $\alpha^n \to 0$ cuando $n \to \infty$. Como A es una vecindad de 0, para n suficientemente grande el conjunto $\alpha^n\mathcal{O} = \{x : |x| \leq |\alpha|^n\}$ está contenido en A. Más aún, $\alpha^n\mathcal{O}$ es un subconjunto cerrado de A por lo que es compacto. Definimos $g : \alpha^n\mathcal{O} \to \mathcal{O}$ por $g(x) = x\alpha^{-n}$ entonces g es un homeomorfismo por lo tanto $\mathcal{O}$ es compacto.

(2) $\Rightarrow$ (3): El ideal $\mathfrak{m}$ es abierto en $\mathcal{O}$, así los conjuntos cocientes $x + \mathfrak{m}$ para $x \in \mathcal{O}$ forman un cubrimiento abierto de $\mathcal{O}$. Aunque solo un número finito de los conjuntos cocientes de $\mathfrak{m}$ son necesitados para cubrir $\mathcal{O}$ desde que $\mathcal{O}$ es compacto. Por lo tanto, $\mathcal{O}/\mathfrak{m}$ es finito. Para probar que $|F^\times|$ es discreto, supongamos lo contrario. Entonces existe una sucesión en $\mathcal{O}$ tal que

$$|x_1| < |x_2| < ... < 1$$

con $|x_i| \to 1$ cuando $i \to \infty$. Como $\mathcal{O}$ es compacto, existe una subsucesión convergente con un punto límite, digamos x, tal que $|x| = 1$. Así, si $|x - x_i| < 1$ entonces $|x_i| = 1$ por el valor absoluto no arquimediano, pero $|x_i| < 1$ para todo i con lo que se llega a una contradicción.

(3) $\Rightarrow$ (2): Mostraremos que $\mathcal{O}$ es secuencialmente compacto, lo cual es lo mismo que compacidad desde que F es un espacio métrico. Sea S un conjunto de conjuntos cocientes representativos de $\mathfrak{m}$ y sea π un uniformalizador. Sea A_n una sucesión infinita en $\mathcal{O}$. De (3.6), un número finito de términos de A_n deben tener algún c_0 común como el primer coeficiente de su expansión π-ádica desde que S es finita. Similarmente, un número infinito de términos de A_n que tiene a c_0 como el coeficiente inicial de su expansión π-ádica también tiene algún c_1 común como segundo coeficiente de su expansión π-ádica desde que S es finita. Continuando de esta manera infinitas veces vemos que A_n contiene una sucesión de Cauchy la cual converge a un punto límite en $\mathcal{O}$ porque F es completo y $\mathcal{O}$ es cerrado en F.

□

Teorema 3.1.24. *Los cuerpos locales son extensiones de cuerpos finitos de $\mathbb{Q}_p$.*

Demostración. Ver Capítulo 9, teorema 9.16 de [3] □

Observación 3.1.25. *Note que en el Teorema 3.1.24, $\mathbb{F}$ puede tener característica 2.*

Observación 3.1.26. *Las extensiones finitas de $\mathbb{Q}_p$ después serán referenciados como cuerpos p-ádicos. Por ejemplo, una extensión finita de $\mathbb{Q}_2$ es llamado un cuerpo 2-ádico.*

Una bonita aplicación del lema de Hensel cuando F es un cuerpo local es que podemos encontrar un conjunto lleno de $(q-1)$-avas raíces de la unidad en F donde q es el tamaño del cuerpo residuo de F. Para hacer esto, consideremos el polinomio $f(X) = X^{q-1} - 1$. Entonces para cada $a \in \mathcal{O}^\times$, $|f(a)| < 1$ mientras que $|f'(a)| = 1$ así el lema de Hensel da una raíz ζ de $f(X)$ tal que $\zeta \equiv a \mod \mathfrak{m}$. Así cada conjunto cociente no nulo de $\mathfrak{m}$ tiene una raíz de f. Más aún, estos deben ser todas las raíces desde que

$$grd(f) = q - 1 = \#(\mathcal{O}/\mathfrak{m})^\times.$$

Note que $\mu_{q-1} = \{\zeta : \zeta^{q-1} = 1\}$ es un subgrupo de $\mathcal{O}^\times$. Ahora usamos esto para analizar la estructura de $\mathcal{O}^\times$.

Teorema 3.1.27. *Para cualquier cuerpo local F tenemos un isomorfismo de grupos $\mathcal{O}^\times \cong \mu_{q-1} \times (1 + \mathfrak{m})$, donde $q = \#(\mathcal{O}/\mathfrak{m})$.*

Demostración. Para $a \in \mathcal{O}^\times$, sea $\zeta \in \mu_{q-1}$ tal que $\zeta \equiv a \mod \mathfrak{m}$. Sea $u = a/\zeta$. Así $u \in \mathcal{O}^\times$ y $u \equiv 1 \mod \mathfrak{m}$. Esto es, $u \in 1 + \mathfrak{m}$ y $a = \zeta u$. Así $\mathcal{O}^\times = \mu_{q-1}(1 + \mathfrak{m})$. Más aún, μ_{q-1} y $1 + \mathfrak{m}$ son subgrupos de $\mathcal{O}^\times$ que se intersectan trivialmente. Así $\mathcal{O}^\times \cong \mu_{q-1} \times (1 + \mathfrak{m})$. □

Observación 3.1.28. *Los elementos de $\mu_{q-1} \cup \{0\}$ son llamados representantes Teichmuller; ellos algunas veces son los conjuntos más naturales de representantes para usar por $\mathcal{O}/\mathfrak{m}$.*

No solo el Teorema 3.1.27 da una estructura a $\mathcal{O}^\times$ pero eso también muestra que

$$F^\times \cong \pi^{\mathbb{Z}} \times \mu_{q-1} \times (1 + \mathfrak{m}). \tag{3.8}$$

Concluimos esta sección con una desigualdad índice que será usada en la Sección 3.3 (Teorema 3.3.20).

Teorema 3.1.29. *Sea F un cuerpo local con característica diferente de 2 Entonces:*

$$[F^\times : F^{\times^2}] \geq 4.$$

Demostración. Desde que $F^\times \cong \pi^{\mathbb{Z}} \times \mathcal{O}^\times$,

$$F^\times / F^{\times^2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathcal{O}^\times / \mathcal{O}^{\times^2}.$$

Eso es suficiente para mostrar que $\mathcal{O}^\times \neq \mathcal{O}^{\times^2}$. Si F tiene una característica de cuerpo residual impar usamos un no cuadrado en μ_{q-1}. Si F tiene un cuerpo residual de característica 2 entonces $\mu_{q-1} = \mu_{q-1}^2$, así nosotros encontramos un no cuadrado en $1+\mathfrak{m}$. Colocamos $u = 1+\pi$ donde π es un uniformalizador de F. Supongamos que u es un cuadrado en $\mathcal{O}^\times$. Entonces $u = c^2$ para algún $c \in \mathcal{O}^\times$. Así $c \equiv 1 \mod \pi$ desde que elevar al cuadrado es inyectivo en característica 2 ($car(\mathcal{O}/\mathfrak{m}) = 2$) Entonces $c = 1+d\pi$ para algún $d \in \mathcal{O}$. El cuadrado resulta:

$$1 + \pi = 1 + 2d\pi + d^2\pi^2. \tag{3.9}$$

Esto es falso, sin embargo, desde que el lado derecho de (3.9) es $1 \mod \pi^2$ porque 2 es $0 \mod \pi$ mientras que el lado izquierdo es $1+\pi \mod \pi^2$. Así u es un no cuadrado en $\mathcal{O}^\times$. □

3.2. Formas Cuadráticas sobre Cuerpos locales

Usamos los hechos establecidos sobre Cuerpos locales en la Sección 3.1 y la discusión de formas cuadráticas en el Capítulo 1 para examinar formas cuadráticas sobre cuerpos locales. Para toda esta sección sea F un cuerpo local de característica diferente de 2, $\mathcal{O}$ es el anillo entero y π sea un uniformizador para F. La característica del cuerpo residual podría ser 2.

Teorema 3.2.1. *Sea q una forma cuadrática no degenerada sobre F Entonces en alguna base*

$$q(x_1, ..., x_n) = a_1x_1^2 + \cdots + a_rx_r^2 + \pi(a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2) \tag{3.10}$$

donde los a_i son unidades.

Demostración. Supongamos que q es diagonal, escribiéndolo

$$q(x_1, ..., x_n) = a_1'x_1^2 + \cdots + a_n'x_n^2$$

con los a_i' en $F^\times$ Entonces ocurre que $a_i' = \pi^{2e_i}a_i$ o $a_i' = \pi^{2e_i+1}a_i$ donde a_i es una unidad. Por un cambio lineal de variables (pongamos $x_i' = \pi^{ei}x_i$ y entonces organizando

los vectores base) se tiene

$$q(x_1, ..., x_n) = a_1x_1^2 + \cdots + a_rx_r^2 + \pi(a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2)$$

como se quería probar. □

Cualquier vector en F^n se puede multiplicar por escalares para que sea un vector en $\mathcal{O}^n$. Estos vectores en $\mathcal{O}^n$ el cual no se reduce a 0 en $(\mathcal{O}/\mathfrak{m})^n$ tiene un nombre especial:

Definición 3.2.2. *Un* ***vector*** $(\alpha_1, ..., \alpha_n)$ *en* $\mathcal{O}^n$ *es llamado* ***primitivo*** *si al menos uno de los* α_i *es no nulo en el cuerpo residual.*

Lema 3.2.3. *Si* $v = (\alpha_1, ..., \alpha_n)$ *en* F^n *y* $v \neq 0$ *entonces* cv *es primitivo para algún* $c \in F^\times$.

Demostración. Sea $max_{1\leq i\leq n}|\alpha_i| = |\alpha_{i_0}|$ Entonces $(1/\alpha_{i_0})v$ es primitivo: $|\alpha_i/\alpha_{i_0}| \leq 1$ para todo i y $\alpha_{i_0}/\alpha_{i_0} = 1$. □

Teorema 3.2.4. *Cualquier forma cuadrática sobre un cuerpo local que tiene un vector isotrópico también tiene un vector isotrópico primitivo.*

Demostración. Sea q una forma cuadrática sobre un cuerpo local F que tiene un vector isotrópico v. Por el Lema 3.2.3, cv es primitivo para algún $c \in F^\times$ y

$$q(cv) = c^2q(v) = 0$$

□

Teorema 3.2.5. *Cuando* F *tiene un cuerpo residual de característica impar, la ecuación*

$$a_1x_1^2 + \cdots + a_rx_r^2 + \pi(a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2) = 0 \tag{3.11}$$

con todos los $a_i \in \mathcal{O}^\times$ *tiene una solución no trivial sobre* F *si y solo si al menos uno de*

$$a_1x_1^2 + \cdots + a_rx_r^2$$

y

$$a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2$$

tiene una solución no trivial sobre F.

Demostración. ($\Rightarrow$) trivial

($\Leftarrow$) Sea

$$F_1(x_1, ..., x_r) = a_1x_1^2 + \cdots + a_rx_r^2$$

y

$$F_2(x_{r+1}, ..., x_n) = a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2$$

Supongamos que existe una solución no trivial sobre F para (3.11), digamos $(\alpha_1, ..., \alpha_n)$. Por el Teorema 3.2.4, supongamos que cada α_i está en $\mathcal{O}$ y que al menos uno de ellos esté en $\mathcal{O}^\times$. Supongamos que $\alpha_i \not\equiv 0 \mod \pi$ para algún $i \leq r$. Entonces

$$F_1(\alpha_1, ..., \alpha_n) \equiv 0 \mod \pi$$

y

$$\frac{\partial F_1}{\partial x_i}(\alpha_1, ..., \alpha_n) = 2a_i\alpha_i \not\equiv 0 \mod \pi.$$

Así existe una solución no trivial para $F_1(x_1, ..., x_r) = 0$ sobre F por el Teorema 3.1.16. De otro lado, si $\alpha_1, ..., \alpha_r$ son todos divisibles por π entonces, al menos uno de los $\alpha_{r+1}, ..., \alpha_n$ debe estar en $\mathcal{O}^\times$. Por lo tanto, $F_1(\alpha_1, ..., \alpha_r) \equiv 0 \mod \pi^2$ así podemos dividir la congruencia

$$a_1\alpha_1^2 + \cdots + a_r\alpha_r^2 + \pi(a_{r+1}\alpha_{r+1}^2 + \cdots + a_n\alpha_n^2) \equiv 0 \mod \pi^2$$

por π para ver que

$$F_2(\alpha_{r+1}, ..., \alpha_n) \equiv 0 \mod \pi.$$

Supongamos, sin pérdida de generalidad que $\alpha_{r+1} \in \mathcal{O}^\times$ Entonces

$$\frac{\partial F_2}{\partial x_{r+1}}(\alpha_{r+1}, ..., \alpha_n) \not\equiv 0 \mod \pi$$

aplicando el Teorema 3.1.16 otra vez nos da una solución no trivial para

$$F_2(x_{r+1}, ..., x_n) = 0$$

sobre F. □

Corolario 3.2.6. *Cuando F tiene un cuerpo residual de característica impar, la forma cuadrática diagonal en (3.10) tiene un vector isotrópico si y solo si la ecuación (3.11) tiene una solución primitiva módulo π^2.*

Demostración. Se sigue de la prueba del Teorema 3.2.5. □

Observación 3.2.7. *El Corolario 3.2.6 da una secuencia finita de pasos para decidir cuando una formas cuadrática no degenerada sobre F tiene un vector isotrópico desde que $\mathcal{O}/\pi^2\mathcal{O}$ es finito.*

Teorema 3.2.8. *Cuando F tiene un cuerpo residual de característica impar y α, β y γ están en $\mathcal{O}^\times$, la forma cuadrática $\alpha x^2 + \beta y^2 + \gamma z^2$ tiene un vector isotrópico en F^3.*

Demostración. Supongamos que q sea el tamaño de $\mathcal{O}/\mathfrak{m}$, por lo que q es impar. Consideremos la congruencia

$$\alpha x^2 = -\beta y^2 - \gamma z^2 \mod \pi.$$

Tomando $z = 1$, ambos miembros de la congruencia toman $\frac{q+1}{2}$ valores pues x e y recorren $\mathcal{O}/\mathfrak{m}$. Así, para algún x_0, y_0 en $\mathcal{O}/\mathfrak{m}$, los dos miembros toman un valor común. Más aún, π no divide a ambos x_0 e y_0 pues $\gamma \not\equiv 0 \mod \pi$. Sin pérdida de generalidad supongamos que $x_0 \not\equiv 0 \mod \pi$ Entonces

$$x_0^2 \equiv \frac{-\beta}{\alpha} y_0^2 - \frac{\gamma}{\alpha} \mod \pi$$

porque α es invertible modulo π. Por el lemma de Hensel existe una raíz $\tilde{x}_0$ para el polinomio $X^2 - (-\frac{\beta}{\alpha} y_0^2 - \frac{\gamma}{\alpha})$. Por lo tanto, $(\tilde{x}_0, y_0, 1)$ es un vector isotrópico para $\alpha x^2 + \beta y^2 + \gamma z^2$. □

Ejemplo 3.2.9. *La forma cuadrática $x^2 + y^2 + z^2$ tiene un vector isotrópico sobre cualquier cuerpo local con cuerpo residual de característica impar por el Teorema 3.2.8.*

Corolario 3.2.10. *Cuando F tiene un cuerpo residual de característica impar, cualquier forma cuadrática sobre F con dimensión al menos 5, tiene un vector isotrópico.*

Demostración. Por el Teorema 2.4.2, es suficiente centrarse en formas cuadráticas no degeneradas. Sea $q = q_1 + \pi q_2$ donde q_1 y q_2 son diagonales con coeficientes en $\mathcal{O}^\times$ (Teorema 3.2.1). Ocurre que q_1 o q_2 es al menos 3-dimensional puesto que $dim(q_1) + dim(q_2) = dim(q) \geq 5$. Para la q_i que es al menos 3-dimensional, establezcamos que todas las variables menos 3 de ellas sean iguales a 0 entonces usando el Teorema 3.2.8 para conseguir un vector isotrópico para esta q_i. □

Observación 3.2.11. *Veremos más adelante (Teorema 3.3.20) que el Corolario 3.2.10 es también cierto cuando F es un cuerpo 2-ádico.*

El Corolario 3.2.6 da una condición necesaria y suficiente para formas cuadráticas sobre cuerpos locales con cuerpo residual de característica impar para tener un vector isotrópico. Sobre cuerpos locales de característica 0 que tienen un cuerpo residual de característica 2 (es decir, cuerpos 2-ádicos) la teoría es un poco más sutil. Los siguientes teoremas dan una condición necesaria y suficiente para decidir cuando una forma cuadrática sobre un cuerpo 2-ádico tiene un vector isotrópico.

Teorema 3.2.12. *Sea F un cuerpo 2-ádico. La forma cuadrática q en (3.10) tiene un vector isotrópico si y solo si la congruencia $q \equiv 0 \mod 4\pi^2$ tiene una solución primitiva.*

Demostración. Supongamos que $dim(q) = n$ y

$$q(x_1, ..., x_n) = a_1x_1^2 + \cdots + a_rx_r^2 + \pi(a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2)$$

con $a_i \in \mathcal{O}^\times$

($\Leftarrow$) Se sigue del Teorema 3.2.4

($\Rightarrow$) Supongamos que $q(\alpha_1, ..., \alpha_n) \equiv 0 \mod 4\pi^2$ con $\alpha_i \in \mathcal{O}$ donde al menos uno de los α_i es unitario. Supongamos que $\alpha_i \not\equiv 0 \mod \pi$ para algún $i \leq r$. Esto implica que

$$\frac{\partial q}{\partial x_i}(\alpha_1, ..., \alpha_n) = 2a_i\alpha_i \not\equiv 0 \mod 2\pi.$$

Así

$$|q(\alpha_1, ..., \alpha_n)| \leq |4\pi^2| < |4| = |\frac{\partial q}{\partial x_i}(\alpha_1, ..., \alpha_n)|^2,$$

asi que q tiene un vector isotrópico por el Teorema 3.1.16. Note que solo necesitamos la congruencia $q(\alpha_1, ..., \alpha_n) \equiv 0 \mod 4\pi$, no módulo $4\pi^2$.

Ahora supongamos que α_i es divisible por π para $1 \leq i \leq r$ y escribimos $\alpha_i = \pi\eta_i$ para ese i. Así por nuestra suposición

$$\pi^2 \sum_{i=1}^{r} a_i\eta_i^2 + \pi \sum_{i=r+1}^{n} a_i\alpha_i^2 \equiv 0 \mod 4\pi^2 \tag{3.12}$$

donde al menos uno de los $\alpha_{r+1}, ..., \alpha_n$ es unitario. Dividiendo (3.12) por π da

$$\sum_{i=r+1}^{n} a_i\alpha_i^2 + \pi \sum_{i=1}^{r} a_i\eta_i^2 \equiv 0 \mod 4\pi \tag{3.13}$$

Usando (3.13) y el mismo razonamiento como antes, la forma cuadrática

$$\frac{1}{\pi} q(\pi x_1, ..., \pi x_r, x_{r+1}, ..., x_n)$$

tiene un vector isotrópico. Entonces trivialmente Q tiene un vector isotrópico. □

Corolario 3.2.13. *Para cualquier cuerpo 2-ádico F, la ecuación $a_1x_1^2 + \cdots + a_nx_n^2 = 0$ donde cada a_i está en $\mathcal{O}^\times$ tiene una solución no trivial en F si y solo si la congruencia*

$$a_1x_1^2 + \cdots + a_nx_n^2 \equiv 0 \mod 4\pi$$

tiene una solución primitiva.

Demostración. Este corolario se sigue de la prueba del Teorema 3.2.12. □

Ejemplo 3.2.14. *Consideremos la forma cuadrática $x^2 + y^2 + z^2$ del Ejemplo 3.2.9. Consideremos la congruencia en $\mathbb{Z}_2$*

$$x^2 + y^2 + z^2 \equiv 0 \mod 8\mathbb{Z}.$$

No existe soluciones primitivas para esta congruencia así que $x^2 + y^2 + z^2$ no tiene vectores isotrópicos en $\mathbb{Q}_2^3$.

3.3. El símbolo de Hilbert

En esta sección definimos el símbolo de Hilbert sobre un cuerpo local y discutimos algunas de su propiedades y aplicaciones. En el capítulo 4 juega un papel muy importante en la prueba del teorema de Hasse-Minkowski sobre $\mathbb{Q}$. Para esta sección F es un cuerpo local de característica diferente de 2 (note que F podría tener un cuerpo residual de característica 2, es decir, podría ser un cuerpo 2-ádico).

Definición 3.3.1. *Sea F un cuerpo local de característica diferente de 2. Para $a, b \in F^\times$, **el símbolo de Hilbert** es*

$$(a,b)_K = \begin{cases} 1, & \text{si } b = x^2 - ay^2 \text{ para algún } a, b \in F, \\ -1, & \text{otro caso} \end{cases}$$

Ejemplo 3.3.2. *Para a, b, c en $F^\times$ tenemos:*

- $(a, -a)_F = 1$,
- $(1, b)_F = 1$,
- $(a, bc^2)_F = (ac^2, b)_F = (a, b)_F$.

Lema 3.3.3. *Sea F cualquier cuerpo. Para $a \in F^\times$,*

$$\{x^2 - ay^2 \neq 0 : x, y \in F\}$$

es un subgrupo de $F^\times$.

Demostración. Si a es un cuadrado en F entonces $x^2 - ay^2$ es universal por el Teorema 2.4.17. Así $\{x^2 - ay^2 \neq 0 : x, y \in F\}$ es $F^\times$.
Si a no es un cuadrado en F entonces $F(\sqrt{a})$ es una extensión cuadrática de F. Para cualquier $\alpha \in F(\sqrt{a})$ escribimos $\alpha = x + y\sqrt{a}$. Así la norma $N_{F(\sqrt{a})/F}(\alpha)$ es $x^2 - ay^2$. En particular, $\{x^2 - ay^2 \neq 0 : x, y \in F\}$ es la imagen de la función norma sobre $F(\sqrt{a})^\times$. Por lo tanto, es un subgrupo de $F^\times$. □

Teorema 3.3.4. *Sobre un cuerpo F de característica diferente de 2 con a y b en $F^\times$, las siguientes afirmaciones son equivalentes:*

1) $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$ *tiene un vector isotrópico sobre* F.

2) $b = x^2 - ay^2$ *para algún* $x, y \in F$.

3) $ax^2 + by^2 - z^2$ *tiene un vector isotrópico sobre* F.

Demostración. Si a es un cuadrado en F entonces (1) y (3) son trivialmente verdaderos y (2) es verdadero por el Teorema 2.4.17. Sea α no un cuadrado en F. Supongamos

$$x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 0$$

no trivialmente Entonces

$$x_1^2 - ax_2^2 = b(x_3^2 - ax_4^2)$$

donde $x_1^2 - ax_2^2$ y $x_3^2 - ax_4^2$ son no nulos desde que α no es un cuadrado en F. Por lo tanto, $b = x^2 - ay^2$ para algún x, y en F porque $\{x^2 - ay^2 \neq 0 : x, y \in F\}$ es un subgrupo de $F^\times$ (Lema 3.3.3).
Ahora supongamos que $b = x^2 - ay^2$ para algún $x, y \in F$ entonces renombrando las variables, $ax^2 + by^2 - z^2$ tiene un vector isotrópico sobre F (sea $y = 1$).
Si $ax^2 + by^2 - z^2$ tiene un vector isotrópico (x_0, y_0, z_0) sobre F entonces es claro que $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$ también lo tiene: $x_1 = z_0, x_2 = x_0, x_3 = y_0$ y $x_4 = 0$. □

Las propiedades algebraicas del símbolo de Hilbert serán seguidas del próximo resultado. Este es el hecho clave desde donde se construirá la teoría de formas cuadráticas sobre cuerpos locales.

Teorema 3.3.5. *Sea* L *una extensión cuadrática de un cuerpo local* F *de característica diferente de 2 Entonces:* $[F^\times : N_{L/F}(L^\times)] = 2$.

Demostración. Ver Apendice B de [2]. □

Observación 3.3.6. *El teorema 3.3.5 también es verdadero cuando* L/F *es una extensión cuadrática de Galois de un cuerpo local de característica 2.*

Corolario 3.3.7. *Sea* F *un cuerpo local de característica diferente de 2. El símbolo de Hilbert sobre* F *tiene las siguientes propiedades:*

1) $(a,b)_F = (b,a)_F$,

2) Si a *no es un cuadrado en* F *entonces existe algún* b *tal que* $(a,b)_F = -1$,

3) $(a,bb')_F = (a,b)_F(a,b')_F$ *y* $(aa',b)_F = (a,b)_F(a',b)_F$

Demostración. A través de la prueba, sean a, b en $F^\times$.

(1) Por el teorema 3.3.4, $(a,b)_F = 1$ exactamente cuando $ax^2 + by^2 - z^2 = 0$ es no trivialmente soluble sobre F. Similarmente, $(b,a)_F = 1$ cuando $bx^2 + ay^2 - z^2 = 0$ es no trivialmente soluble sobre F. Claramente $ax^2 + by^2 - z^2$ y $bx^2 + ay^2 - z^2$ son formas cuadráticas equivalentes (solo se permuta los vectores base de una de las formas para conseguir la otra) así $(a,b)_F = 1$ si y solo si $(b.a)_F = 1$. Por lo tanto, $(a,b)_F = (b,a)_F$.

(2) Si a no es un cuadrado en F entonces $L = F(\sqrt{a})$ es una extensión cuadrática de F por lo que $N_{L/F}(x + y\sqrt{a}) = x^2 - ay^2$. Por el Teorema 3.3.5, existen $a, b \notin N_{L/F}(L^\times)$. Así $(a,b)_F \neq 1$

(3) Por (1) es suficiente mostrar que $(a,bb')_F = (a,b)_F(a,b')_F$. Supongamos que a es un cuadrado entonces $x^2 - ay^2$ es universal. Así la ecuación es trivialmente verdadera desde que $(a,b)_F = 1$ para todo $b \in F^\times$.

Si a no es un cuadrado, sea $L = F(\sqrt{a})$. Supongamos que $(a,b)_F = 1$ y $(a,b')_F = 1$ entonces $b \in N_{L/F}(L^\times)$ y $b' \in N_{L/F}(L^\times)$. Así bb' está en $N_{L/F}(L^\times)$ desde que $N_{L/F}(L^\times)$ es un grupo. Por lo tanto, $(a,bb')_F = 1$.

Supongamos que o $(a,b)_F$ o $(a,b')_F$ es -1. Sin pérdida de generalidad supongamos que $(a,b)_F = -1$ y $(a,b')_F = 1$ entonces $b \notin N_{L/F}(L^\times)$ y $b' \in N_{L/F}(L^\times)$. Supongamos que $bb' \in N_{L/F}(L^\times)$ entonces $b = bb'/b' \in N_{L/F}(L^\times)$ lo cual es una contradicción, por lo tanto $(a,bb')_F = -1$.

Supongamos que $(a,b)_F = -1$ y $(a,b')_F = -1$ entonces $bb' \in N_{L/F}(L^\times)$ desde que $N_{L/F}(L^\times)$ tiene índice 2 en $F^\times$ por el Teorema 3.3.5, por lo tanto $(a,bb')_F = 1$.

□

Como $[\mathbb{R}^\times : N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)] = [\mathbb{R}^\times : \mathbb{R}^{\times 2}] = 2$ podemos asignar $F = \mathbb{R}$ en la Definición 3.3.1 (aunque $\mathbb{R}$ no es cuerpo local) y el símbolo resultante $(\cdot,\cdot)_{\mathbb{R}}$ tendrá las mismas propiedades algebraicas como los símbolos de Hilbert sobre cuerpos locales del Corolario 3.2.5. Denotamos el símbolo de Hilbert sobre $\mathbb{R}$ por $(a,b)_{\mathbb{R}}$ para $a, b \in \mathbb{R}^\times$.

Ejemplo 3.3.8. *El símbolo de Hilbert $(-1,-1)_F$ es 1 cuando F es un cuerpo local de un cuerpo residual de característica impar (Teorema 3.2.8). Cuando $F = \mathbb{R}$ o $F = \mathbb{Q}_2$, sin embargo, $(-1,-1)_F$ es -1 (mirar la ecuación $-x^2-y^2-z^2 = 0$ y recordar el Ejemplo 3.2.14). Por el Corolario 3.2.13, $(-1,-1)_F = 1$ cuando F es un cuerpo 2-ádico sí y solo sí $x^2+y^2+z^2 \equiv 0 \mod 4\pi$ tiene una solución primitiva.*

Ejemplo 3.3.9. *Las propiedades algebraicas del símbolo de Hilbert muestran que $(a,1)_F = (1,a)_F = 1$ y lo que es más importante para cálculos posteriores*

$$\begin{aligned}(a,a)_F &= (a,-a)_F(a,-1)_F \\ &= (a,-1)_F\end{aligned}$$

para cualquier cuerpo local F ($car(F) \neq 2$) y para $F = \mathbb{R}$.

El siguiente resultado ofrece una fórmula para calcular el símbolo de Hilbert sobre cuerpos locales con cuerpo residual de característica impar.

Teorema 3.3.10. *Sea F un cuerpo local con un cuerpo residual de característica impar y π un uniformalizador. Para $a, b \in F^\times$ escribimos $a = \pi^m\varepsilon$ y $b = \pi^n\delta$ para m, n en $\mathbb{Z}$ y ε, δ en $\mathcal{O}^\times$ Entonces:*

$$(a,b)_F = (-1)^{mn(q-1)/2}\chi(\overline{\varepsilon})^n\chi(\overline{\delta})^m$$

donde q es el tamaño del cuerpo residual y $\chi : (\mathcal{O}_F/\mathfrak{m}_F)^\times \to \{\pm 1\}$ es la característica cuadrática sobre el cuerpo residual.

Demostración. Denotemos el miembro derecho de la fórmula como $\langle a,b\rangle_F$. Primero verificaremos que $\langle a,b\rangle_F$ como una función de a y de b tiene la primera y la tercera propiedades algebraica del símbolo de Hilbert en el Corolario 3.3.7. La simetría es obvio

por lo que solo verificaremos que $\langle a,b\rangle_F$ es multiplicativa en a. Sean a,a',b están en $F^\times$. Escribimos $a=\pi^m\varepsilon$, $a'=\pi^{m'}\varepsilon'$ y $b=\pi^n\delta$ Entonces

$$\begin{aligned}\langle a,b\rangle_F\langle a',b\rangle_F &= (-1)^{mn(q-1)/2}\chi(\overline{\varepsilon})^n\chi(\overline{\delta})^m(-1)^{m'n(q-1)/2}\chi(\overline{\varepsilon'})^n\chi(\overline{\delta})^{m'}\\ &= (-1)^{(m+m')n(q-1)/2}(\chi(\overline{\varepsilon})\chi(\overline{\varepsilon'}))^n\chi(\overline{\delta})^{m+m'}\\ &= (-1)^{(m+m')n(q-1)/2}\chi(\overline{\varepsilon}\overline{\varepsilon'})^n\chi(\overline{\delta})^{m+m'}\\ &= \langle aa',b\rangle_F\end{aligned}$$

así la fórmula es multiplicativa. Ahora vamos a mostrar que $(a,b)_F=\langle a,b\rangle_F$ para todo $a,b\in F^\times$. Por las propiedades algebraicas recientemente probadas, es suficiente verificar la ecuación para a,b igual a π o a unidades. Así tenemos tres casos para verificar.

Caso 1: (a,b son unidades) Sean $a=\varepsilon$ y $b=\delta$ entonces $(\varepsilon,\delta)_F=1$ por el Teorema 3.2.8. En el miembro derecho,

$$\langle\varepsilon,\delta\rangle_F=(-1)^0\chi(\overline{\varepsilon})^0\chi(\overline{\delta})^0=1$$

Así la fórmula es válida para dos unidades.

Caso 2: ($a=\pi$ y $b=\varepsilon$ es una unidad) Tenemos que $(\pi,\varepsilon)_F=1$ sí y sólo sí la ecuación $\pi x^2+\varepsilon y^2-z^2=0$ tiene una solución no trivial. Pero por el Teorema 2.4.17 y el Teorema 3.2.5, esta ecuación tiene una solución trivial sí y solo sí ε es un cuadrado en F. Este último enunciado es equivalente a que ε es un cuadrado en el cuerpo residual. Similarmente,

$$\langle\pi,\varepsilon\rangle_F=(-1)^0\chi(1)^0\chi(\overline{\varepsilon})=\chi(\overline{\varepsilon}),$$

el cual es 1 sí y solo sí ε es un cuadrado en el cuerpo residual. Así la fórmula se satisface en este caso también.

Caso 3: ($a=b=\pi$) En este caso, $(\pi,\pi)_F=(\pi,-1)_F=\langle\pi,-1\rangle_F$ por el Ejemplo 3.3.9 y el caso 2. Mas aún,

$$\langle\pi,-1\rangle_F=\chi(-1)=(-1)^{(q-1)/2}=\langle\pi,\pi\rangle_F$$

así $\langle\pi,\pi\rangle_K=\langle\pi,\pi\rangle_F$. □

Teorema 3.3.11. *Para $a, b \in \mathbb{R}^\times$,*

$$(a,b)_{\mathbb{R}} = \begin{cases} 1, & si\ a > 0\ o\ b > 0 \\ -1, & si\ a < 0\ o\ b < 0 \end{cases}$$

Demostración. Esto se consigue con un cálculo directo. □

Para una fórmula explicita para $(a,b)_F$ cuando $F = \mathbb{Q}_2$ ver en [9]. Nosotros no necesitamos tal fórmula en nuestro trabajo.
Discutimos algunas aplicaciones del símbolo de Hilbert.
Dos invariantes para formas cuadráticas son la dimensión y el discriminante, con estas se puede clasificar formas cuadráticas no degeneradas sobre $\mathbb{C}$ y $\mathbb{F}$. La clasificación de formas cuadráticas no degeneradas sobre $\mathbb{R}$ necesita una invariante adicional (el número de coeficientes positivos en una diagonalización) Aquí introducimos una invariante para formas cuadráticas sobre cuerpos locales usando el símbolo de Hilbert.

Definición 3.3.12. *Sea F un cuerpo local de característica diferente de 2 o $F = \mathbb{R}$. Supongamos que q sea una forma cuadrática n-dimensional no degenerada sobre F que es equivalente a la forma diagonal*

$$a_1 x_1^2 + \cdots + a_n x_n^2$$

Entonces

$$c_F(q) = \prod_{i<j} (a_i, a_j)_F \in \{\pm 1\}$$

*Es llamado el **invariante de Hasse** de q. Si q es 1-dimensional entonces se hace la convención que $c_F(q) = 1$.*

Observación 3.3.13. *Notemos que el invariante de Hasse es definido solamente para formas cuadráticas no degeneradas puesto que el símbolo de Hilbert $(a,b)_K$ no es definido si a o b es 0.*

Antes de usar el invariante de Hasse, mostraremos que solo depende de la clase de equivalencia de la forma cuadrática y no de una diagonalización en particular. Los siguientes dos lemas son necesarios para esta tarea.

Lema 3.3.14. *Sea q una forma cuadrática no degenerada sobre un espacio vectorial V. Sea $E = \{e_1, ..., e_n\}$ y $E' = \{e'_1, ..., e'_n\}$ cualquier par de bases ortogonales de V Entonces existe una sucesión de bases ortogonales $E_i = \{e_{i1}, ..., e_{in}\}$ para $i = 1, ..., m$ tal que:*

1) $E_1 = E$ y $E_m = E'$

2) para cada i, las bases E_i, E_{i+1} tienen al menos $n-2$ elementos en común (es decir, $e_{ij} = e_{(i+1)j}$ para al menos $n-2$ valores de j).

Demostración. Sea F un cuerpo sobre el cual V es un espacio vectorial. Si E' es una permutación de E entonces el Lema 3.3.14 es trivialmente cierto puesto que todas las permutaciones son productos de transposiciones. Por lo tanto, no tenemos que tomar en cuenta el orden de una base.

Procedemos por inducción sobre la dimensión de V. Cuando $dimV = 1$ o 2, el lema trivialmente se satisface. Para $n \geq 3$, supongamos que esto es verdadero cuando $dimV < n$. Queremos mostrar que existe una sucesión del tipo deseado de E a una base ortogonal $\{e'_1, e^*_2, ..., e^*_n\}$ para algún $e^*_i \in V$. Para hacerlo, sea $\{f_1, ..., f_n\}$ una base ortogonal tal que existe una sucesión desde E para que se ajuste a la segunda condición del lema y que e'_1 es una combinación lineal de menor número posible de vectores base. Mostraremos que ese mínimo es 1.

Supongamos sin pérdida de generalidad que e'_1 es una combinación lineal de los primeros J vectores base, explícitamente

$$e'_1 = \sum_{i=1}^{J} a_i f_i$$

donde cada $a_i \neq 0$.

Supongamos que $J > 1$. Primero mostramos que existen dos de estos vectores tal que $q(a_j f_j + a_k f_k) \neq 0$. Supongamos sin perder la generalidad que

$$\begin{aligned} 0 &= q(a_1 f_1 + a_2 f_2) = a_1^2 q(f_1) + a_2^2 q(f_2), \\ 0 &= q(a_1 f_1 + a_3 f_3) = a_1^2 q(f_1) + a_3^2 q(f_3), \\ 0 &= q(a_2 f_2 + a_3 f_3) = a_2^2 q(f_2) + a_3^2 q(f_3). \end{aligned}$$

Entonces $q(f_1) = q(f_2) = q(f_3) = 0$, esto es una contradicción puesto que $q(f_i) \neq 0$ (V es no degenerada). Por lo tanto, existe siempre un par de vectores f_j, f_k con $1 \leq j < k \leq J$ tal que $q(a_j f_j + a_k f_k) \neq 0$. Por permutación de los vectores base, podemos suponer que $q(a_1 f_1 + a_2 f_2) \neq 0$.

Ahora queremos encontrar un vector ortogonal no nulo a $a_1 f_1 + a_2 f_2$ y a $f_3, ..., f_n$. Para desconocidos b_1 y b_2 en F, supongamos que

$$\begin{aligned} 0 &= b(a_1 f_1 + a_2 f_2, b_1 f_1 + b_2 f_2) \\ &= a_1 b_1 q(f_1) + a_2 b_2 q(f_2) \end{aligned}$$

donde b es la forma bilineal asociada a q. Tomando $b_1 = a_2 q(f_2)$ y $b_2 = -a_1 q(f_1)$ encontramos el deseado vector isotrópico. Sea

$$\begin{aligned} \tilde{f}_1 &= a_1 f_1 + a_2 f_2 \\ \tilde{f}_2 &= a_2 q(f_2) f_1 - a_1 q(f_1) f_2 \\ \tilde{f}_j &= f_j \text{ para } j = 3, ..., n. \end{aligned}$$

Entonces $b(\tilde{f}_i, \tilde{f}_j) = 0$ para todo $i \neq j$ en $\{1, ..., n\}$ y notemos que

$$\begin{aligned} q(\tilde{f}_2) &= q(a_2 Q(f_2) f_1 - a_1 q(f_1) f_2) \\ &= q(f_1) q(f_2)(a_1^2 q(f_1) + a_2^2 q(f_2)) \\ &= q(f_1) q(f_2) q(a_1 f_1 + a_2 f_2) \\ &\neq 0 \end{aligned}$$

así $\{\tilde{f}_1, ..., \tilde{f}_n\}$ es una base ortogonal. Por lo tanto, $e_1' = \tilde{f}_1 + \sum_{i=3}^{J} a_i \tilde{f}_i$ (la suma es vacía si $J = 2$), un total de $J - 1$ vectores, contradiciendo la suposición de que J es mínimal. Por lo tanto, $J = 1$. Así existe una sucesión del tipo deseado empezando con E y terminando con una base ortogonal $\{e_1', e_2^*, ..., e_n^*\}$ para algún $e_i^* \in V$.

El paso inductivo viene ahora. Desde que Fe_1' es un subespacio no degenerado de V, $e_1'^{\perp}$ es también no degenerado (porque V es no degenerado). Más aún, $e_1'^{\perp}$ es un subespacio $(n-1)$-dimensional de V generado por $\{e_2^*, ..., e_n^*\}$. Por la hipótesis inductiva, existe una sucesión de bases ortogonales de $e_1'^{\perp}$ empezando con $\{e_2^*, ..., e_n^*\}$ y terminando con $\{e_2', ..., e_n'\}$ ajustando las condiciones necesarias. Agregando e_1' a esta sucesión de bases nos da el tipo de sucesión deseada de $\{e_1', e_2^*, ..., e_n^*\}$ a E' y así de E a E'. □

Lema 3.3.15. *Sea F un cuerpo local de característica diferente de 2 o $F = \mathbb{R}$. Sea q una forma cuadrática no degenerada 2-dimensional sobre F Entonces para $b \in F^\times$, q toma el valor de b sobre F sí y sólo sí $(b, -disc(q))_F = c_F(q)$.*

Demostración. Sin pérdida de generalidad, podemos suponer que q es diagonal:

$$q(x_1, x_2) = a_1x_1^2 + a_2x_2^2$$

para $a_i \in F^\times$. Entonces $q(x_1, x_2) = b$ es soluble sobre F si y solo sí la forma cuadrática $q(x_1, x_2) - bx_3^2$ tiene un vector isotrópico. Este último enunciado es equivalente a la condición $(a_1/b, a_2/b)_F = 1$.

Usando las propiedades algebraicas del símbolo de Hilbert (Corolario 3.3.7 y Ejemplo 3.3.9),

$$\begin{aligned}(a_1/b, a_2/b)_F &= (b, a_2)_F(b, a_1)_F(b, b)_F(a_1, a_2)_F \\ &= (b, -a_1a_2)_F(a_1, a_2)_F \\ &= (b, -disc(q))_F(a_1, a_2)_F\end{aligned}$$

Por lo tanto, $(a_1/b, a_2/b)_F = 1$ sí y solo sí $(b, -disc(q))_F = (a_1, a_2)_F$. □

Observación 3.3.16. *El Lema 3.3.15 nos dice que $c_F(q)$ es independiente de la elección de la diagonalización cuando $dim(q) = 2$ porque $(b, -disc(q))_F$ no depende de una diagonalización en particular.*

Teorema 3.3.17. *Sea F un cuerpo local de característica diferente de 2 o $F = \mathbb{R}$. Si*

$$q(x_1, ..., x_n) = a_1x_1^2 + \cdots + a_nx_n^2$$

es una forma cuadrática diagonalizada no degenerada que es equivalente a

$$q'(x_1, ..., x_n) = b_1x_1^2 + \cdots + b_nx_n^2$$

entonces $c_F(q) = c_F(q')$.

Demostración. El teorema es evidentemente verdadero para $n = 1$.

Para $n = 2$ es verdadero por el Lema 3.3.15.

Supongamos que $n > 2$. Por el Lema 3.3.14 existe una sucesión de bases ortogonales

que van de $q(x_1, ..., x_n)$ a $q'(x_1, ..., x_n)$ tal que cada base difiere de la anterior en al menos dos vectores. Si podemos mostrar que $c_F(q)$ es invariante después del primer paso de tal sucesión, entonces esto será invariante a través de todos los pasos en la sucesión. Desde que los coeficientes en una diagonalización de una forma cuadrática son sus valores sobre las bases ortogonales es suficiente suponer que a_i no es igual a algún b_j para al menos dos valores de i. Lo que es más, $\prod_{i<j}(a_i, a_j)_F$ es independiente de cualquier permutación de $a_1, ..., a_n$. Así sin pérdida de generalidad podemos asumir que $a_i = b_i$ para $i > 2$. Entonces $a_1x_1^2 + a_2x_2^2$ es equivalente a $b_1x_1^2 + b_2x_2^2$ por la cancelación de Witt, así $a_1a_2 \sim b_1b_2$ y

$$(a_1, a_2)_F = (b_1, b_2)_F$$

del caso $n = 2$ de este teorema. Ahora calculamos el invariante de Hasse de q y q':

$$c_F(q) = (a_1, a_2)_F \prod_{2<i} (a_1a_2, a_i)_F \prod_{2<i<j} (a_i, a_j)_F$$

$$c_F(q) = (b_1, b_2)_F \prod_{2<i} b_1b_2, b_i)_F \prod_{2<i<j} (b_i, b_j)_F$$

$$c_F(q) = c_F(q')$$

Así el invariante de Hasse es independiente de una elección particular de diagonalización. □

El Lema 3.3.15 ya ilustró cómo el invariante de Hasse juega un importante rol en encontrar condiciones necesarias y suficientes condiciones para cuando una forma cuadrática 2-dimensional sobre un cuerpo local representa un valor particular en el cuerpo. Como resulta, el invariante de Hasse también juega un mayor rol en el siguiente análogo 3-dimensional del Lema 3.3.15.

Teorema 3.3.18. *Sea F un cuerpo local de característica diferente de 2 o $F = \mathbb{R}$. Una forma cuadrática no degenerada 3-dimensional q sobre F toma un valor $b \in F^\times$ sí y solo sí la forma cuadrática 4-dimensional $q - bx^2$ satisface al menos una de las siguientes condiciones:*

1) $disc(q - bx^2) \notin F^{\times^2}$,

2) $c_F(q - bx^2) = (-1, -1)_F$.

Demostración. Sin pérdida de generalidad supongamos que q es diagonalizado. Escribimos $b = a_4$ y $q = a_1x_1^2 + a_2x_2^2 - a_3x_3^2$, así

$$q(x_1, x_2, x_3) - a_4x_4^2 = q_1(x_1, x_2) - q_2(x_3, x_4)$$

donde

$$q(x_1, x_2) = a_1x_1^2 + a_2x_2^2$$

y

$$q(x_3, x_4) = a_3x_3^2 + a_4x_4^2.$$

Para simplificar, escribimos: $(a, b)_F = (a, b)$.

Caso 1: $-disc(q_1)$ o $-disc(q_2)$ es un cuadrado en $F^{\times^2}$

Sin pérdida de generalidad podemos suponer que $-disc(q_1)$ es un cuadrado en $F^\times$ entonces q_1 tiene un vector isotrópico así $q - a_4x_4^2$ también tiene un vector isotrópico. Así q tiene el valor $a_4 = b$. Ahora mostramos que $q - a_4x_4^2$ satisface al menos uno de (1) y (2). Puesto que $-disc(q_1)$ está en $F^{\times^2}$ tenemos que

$$disc(q - a_4x_4^2) = disc(q_1)disc(q_2) \sim -disc(q_2).$$

Supongamos que $-disc(q_2)$ también es un cuadrado en $F^\times$. En otro caso, (1) es satisfecho. Mostraremos que $c_F(q - a_4x_4^2)$ es $(-1, -1) = (-1, -1)_F$.

Por un cálculo directo,

$$\begin{aligned} c_F(q - a_4x_4^2) &= (a_1, a_2)(a_1, -a_3)(a_1, -a_4)(a_2, -a_3)(a_2, -a_4)(-a_3, -a_4) \\ &= (a_1, a_2)(a_1, a_3a_4)(a_2, a_3a_4)(-a_3, -a_4) \\ &= (a_1, a_2)(a_1a_2, a_3a_4)(-a_3, -a_4). \end{aligned}$$

Cuando $-disc(q_1) = -a_1a_2$ y $-disc(q_2) = -a_3a_4$ están en $F^{\times^2}$,

$$\begin{aligned} c_F(q - a_4x_4^2) &= (a_1, a_2)(a_1a_2, a_3a_4)(-a_3, -a_4) \\ &= (a_1, -a_1)(-1, -1)(-a_3, a_3) \\ &= (-1, -1) \end{aligned}$$

como lo queríamos.

Caso 2: $-disc(q_1)$ y $-disc(q_2)$ no son cuadrados en $F^\times$.

Mostramos este caso probando la equivalencia de las negaciones: es decir, $q - bx^2$ no tiene un vector isotrópico si y solo si $q - bx^2$ no satisface ni (1) ni (2).

Por el Corolario 2.4.22, $q - a_4x_4^2$ tiene un vector isotrópico sí y solo sí q_1 y q_2 toman un valor común no nulo. Del Lema 3.3.15 tenemos que q_1 y q_2 representan un valor común no nulo, digamos $d \in F^\times$ sí y solo sí

$$(d, -disc(q_1)) = (a_1, a_2) \tag{3.14}$$

y

$$(d, -disc(q_2)) = (a_3, a_4). \tag{3.15}$$

Desde que $-disc(q_1)$ y $-disc(q_2)$ no están en $F^{\times^2}$, $F(\sqrt{-a_1a_2})$ y $F(\sqrt{-a_3a_4})$ son extensiones cuadráticas de F con $x^2 + disc(q_1)y^2$ y $x^2 + disc(q_2)y^2$ como sus respectivas formas norma. Por la definición y simetría del símbolo de Hilbert,

$$(d, -disc(q_i)) = 1$$

sí y solo sí la forma norma $x^2 + disc(q_i)y^2$ representa a d para algún $x, y \in F$. Por el Teorema 3.3.5 el subgrupo de valores representado por cada una de estas formas norma tienen índice 2 en $F^\times$. Así el conjunto de los d satisfaciendo cada uno de (3.14) y (3.15) se encuentra exactamente en la mitad de las clases laterales de $F^{\times^2}$. Por lo tanto, $q - a_4x_4^2$ no tiene vector isotrópico es equivalente a los conjuntos d satisfaciendo (3.14) y (3.15) siendo complementos. Si

$$disc(q_1) \sim disc(q_2) \tag{3.16}$$

y

$$(a_1, a_2) = -(a_3, a_4) \tag{3.17}$$

entonces es claro que los conjuntos de d que satisfacen (3.16) y (3.17) son complementarios.

Ahora probaremos la recíproca.

Supongamos que $(a_1, a_2) = (a_3, a_4)$ entonces cuando $d = 1$,

$$(d, -disc(q_1)) = (d, -disc(q_2)).$$

Así para $d = 1$, cualquiera de (3.14) y (3.15) son verdaderos o ambos son falsos. Por lo tanto, $(a_1, a_2) = -(a_3, a_4)$ si los conjuntos de d satisfaciendo (3.14) o (3.15) son complementarios. Si $disc(q_1) \not\sim disc(q_2)$ entonces $disc(q_1)/disc(q_2)$ no es un cuadrado en $F^\times$. Esto significa que existe algún d_0 tal que $(d_0, disc(q_1)/disc(q_2)) = -1$ por (2) del Corolario 3.3.7. Así $(d_0, -disc(q_1)) = -(d_0, -disc(q_2))$ mientras que $(a_1, a_2) = -(a_3, a_4)$. Así para $d = d_0$ cualquiera de (3.14) y (3.15) son verdaderos o ambos son falsos. Por lo tanto los conjuntos de d que satisfacen (3.14) y (3.15) siendo complementarios es equivalente a (3.16) y (3.17) siendo verdaderos.

Ahora tenemos que $q - a_4x_4^2$ no tiene un vector isotrópico sí y solo sí (3.16) y (3.17) son satisfechas. Mostraremos que (1) y (2) fallan sí y solo sí (3.16) y (3.17) se satisfacen. Esto es, $a_1a_2a_3a_4 \sim 1$ y $c_F(q - a_4x_4^2) = -(-1, -1)$ sí y solo sí (3.16) y (3.17) son verdaderos. Asumamos que $a_1a_2a_3a_4 \sim 1$ y mostremos que $c_F(q - a_4x_4^2) = -(-1, -1)$ sí y solo sí $(a_1, a_2) = -(a_3, a_4)$. De antes,

$$c_F(q - a_4x_4^2) = (a_1, a_2)(a_1a_2, a_3a_4)(-a_3, -a_4)$$

Desde que $a_1a_2a_3a_4 \sim 1$,

$$\begin{aligned}
(a_1, a_2)(a_1a_2, a_3a_4)(-a_3, -a_4) &= (a_1, a_2)(a_3a_4, a_3a_4)(-a_3, -a_4) \\
&= (a_1, a_2)(-1, a_3a_4)(-a_3, -a_4) \\
&= (a_1, a_2)(-1, a_3)^2(-1, a_4)^2(-1, -1)(a_3, a_4) \\
&= (a_1, a_2)(-1, -1)(a_3, a_4),
\end{aligned}$$

el cual es $-(-1, -1)$ sí y solo sí $(a_1, a_2) = -(a_3, a_4)$. □

Corolario 3.3.19. *Sea F un cuerpo local de característica diferente de 2 o $F = \mathbb{R}$. Una forma cuadrática no degenerada 3-dimensional sobre F toma todos los valores excepto posiblemente en una clase lateral de $F^\times/F^{\times^2}$.*

Demostración. Sea q una forma cuadrática no degenerada 3-dimensional sobre F. Si q no toma algún valor, digamos b entonces $q - bx^2$ no tiene un vector isotrópico y por lo tanto, $disc(q - bx^2) = -bdisc(q)$ es un cuadrado en $F^\times$. Así los únicos valores que q no podría tomar están en la misma clase cuadrada de $-disc(q)$. Para $F = \mathbb{R}$ este corolario es trivial desde que $\mathbb{R}/\mathbb{R}^{\times^2}$ tiene tamaño 2. □

Podemos extender el Corolario 3.2.10 a cuerpos 2-ádico. Nuestro argumento dará un tratamiento uniforme para todos los cuerpos locales de característica diferente de 2.

Teorema 3.3.20. *Sea F un cuerpo local de característica diferente de 2. Cada forma cuadrática de dimensión ≥ 5 sobre F tiene un vector isotrópico.*

Demostración. Sea q una forma cuadrática sobre F de dimensión $n \geq 5$. Podemos suponer que q es no degenerada desde que cualquier forma cuadrática no degenerada tiene un vector isotrópico (Teorema 2.4.2). Además, podemos suponer que q es diagonalizado.
Para $n = 5$, escribimos

$$q(x_1, x_2, x_3, x_4, x_5) = q_1(x_1, x_2, x_3) - q_2(x_4, x_5)$$

donde

$$q_1(x_1, x_2, x_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$$

y

$$q_2(x_4, x_5) = -a_4x_4^2 - a_5x_5^2$$

para $a_i \in F^\times$. Entonces esto es equivalente por el Corolario 2.4.22 a mostrar que q_1 y q_2 toman un valor común no nulo. Por el Corolario 3.3.19, q_1 toma todos los valores de $F^\times$ excepto posiblemente en una clase lateral de $F^\times/F^{\times^2}$. Si $-disc(q_2)$ es un cuadrado en $F^\times$ entonces q_2 es universal por el Lema 3.3.15. De otro lado, si $-disc(q_2)$ no es cuadrado en $F^\times$ entonces $-a_4q_2$ es equivalente a la forma norma de una extensión cuadrática de F. Por el Teorema 3.3.5 el conjunto de los valores no nulos de $-a_4q_2$ es un subgrupo de índice 2 en $F^\times$. Por lo tanto, no importa cuál sea el valor de $-disc(q_2)$,

q_2 toma todos los valores en al menos la mitad de las clases de $F^\times/F^{\times^2}$. En cualquier cuerpo local, $[F^\times/F^{\times^2}] > 2$ por el Teorema 3.1.29 (esto es falso para $F = \mathbb{R}$) así q_1 y q_2 deben tomar un valor común no nulo.

Para $n > 5$, el conjunto de todos pero cinco de las variables igual a cero, se reducen al caso $n = 5$. □

Observación 3.3.21. *Un resultado bonito del Teorema 3.3.20 es que cada forma cuadrática no degenerada sobre un cuerpo local de dimensión más grande o igual a cuatro es universal. Esto es falso para formas cuadráticas sobre* $\mathbb{R}$*, una suma de cuadrados no es universal sobre* $\mathbb{R}$*.*

El último teorema en este capítulo caracteriza a las formas cuadráticas no degeneradas sobre cuerpos locales salvo equivalencias usando el invariante de Hasse junto con la dimensión y el discriminante.

Teorema 3.3.22. *La dimensión, el discriminante y el invariante de Hasse determinan una forma cuadrática no degenerada sobre un cuerpo local salvo equivalencias.*

Demostración. Sean q_1 y q_2 formas cuadráticas no degeneradas n-dimensionales sobre F tal que $disc(q_1) \sim disc(q_2)$ y $c_F(q_1) = c_F(q_2)$. Mostraremos que $q_1 \cong q_2$ haciendo inducción sobre la dimensión.

Cuando $n = 1$ el teorema es trivialmente verdadero.

Supongamos que $n > 1$. Queremos mostrar que q_1 y q_2 toman un valor común. Una vez se mostrado, diagonalizaremos usando inducción.

Para $n = 2$, q_1 y q_2 toma los mismos valores por el Lema 3.3.15. Para $n > 2$, la forma cuadrática $q_1 \perp -q_2$ tiene dimensión $2n > 5$ así que por el Corolario 2.4.22 y el Teorema 3.3.20, q_1 y q_2 toman un valor común no nulo, digamos d entonces la diagonalización es

$$q_1(x_1, ..., x_n) = dx_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$$

y (en un conjunto de coordenadas posiblemente diferentes)

$$q_2(y_1, ..., y_n) = dy_1^2 + b_2y_2^2 + \cdots + b_ny_n^2$$

donde $a_i, b_i \in F^\times$. Denotemos $a_2x_2^2 + \cdots + a_nx_n^2$ por q_1' y $b_2y_2^2 + \cdots + b_ny_n^2$ por q_2'. Es claro que q_1' y q_2' tienen dimensión $n-1$. Por lo tanto, $disc(q_1') \sim disc(q_2')$ puesto que

$$da_2 \cdots a_n \sim db_2 \cdots b_n$$

(solo cancelamos las d). Finalmente mostramos que $c_F(q_1') = c_F(q_2')$. El invariante de Hasse de q_1 es

$$c_F(q_1) = \prod_i (d, a_i)_F \prod_{i<j} (a_i, a_j)_F$$
$$c_F(q_1) = (d, disc(q_1'))_F c_F(q_1')$$

y el invariante de Hasse de q_2 es

$$c_F(q_2) = \prod_i (d, b_i)_F \prod_{i<j} (b_i, b_j)_F$$
$$c_F(q_2) = (d, disc(q_2'))_F c_F(q_2')$$

Así $c_F(q_1') = c_F(q_2')$ desde que $c_F(q_1) = c_F(q_2)$ y $disc(q_1') \sim disc(q_2')$ Entonces por inducción $q_1' \cong q_2'$ y por lo tanto, $q_1 \cong q_2$. □

Capítulo 4

Hasse-Minkowski sobre $\mathbb{Q}$

Estamos preparados para probar el teorema de Hasse-Minkowski sobre $\mathbb{Q}$. Después haremos algunas de sus aplicaciones: Rescatamos el teorema de Hasse-Minkowski

Teorema 4.0.1. *Sea $q(x_1, ..., x_n)$ una forma cuadrática no degenerada sobre $\mathbb{Q}$. La ecuación $q(x_1, ..., x_n) = 0$ es soluble no trivialmente sobre $\mathbb{Q}$ si y sólo si ella es soluble no trivialmente sobre $\mathbb{R}$ y cada $\mathbb{Q}_p$.*

La prueba de Hasse-Minkowski usa inducción matemática sobre n la dimensión de la forma cuadrática. El caso $n = 1$ es trivial, por lo que empezamos con $n = 2$. Recordemos que la colección de completaciones de $\mathbb{Q}$ son denotados por $\mathbb{Q}_v$ con v igual a un número primo p en $\mathbb{Z}$ o $v = \infty$ ($\mathbb{Q}_\infty = \mathbb{R}$).

4.1. $n = 2$

Lema 4.1.1. *Sobre cualquier cuerpo F (de característica diferente de 2) la forma cuadrática no degenerada $ax^2 + by^2$ tiene un vector isotrópico sobre F si y sólo si $-\frac{b}{a} \in F^{\times 2}$.*

Demostración. Supongamos que la ecuación $ax^2 + by^2 = 0$ es soluble no trivialmente sobre F. Sea (x_0, y_0) una solución no trivial. Si $x_0 = 0$ entonces $by_0^2 = 0$ por lo que $y_0 = 0$. Así x_0 y y_0 son ambos no nulos entonces

$$\frac{x_0^2}{y_0^2} = -\frac{b}{a}$$

por lo que $-\frac{b}{a}$ está en $F^{\times 2}$.
Recíprocamente, si $-\frac{b}{a} = c^2$ para algún $c \in F^\times$ entonces $(c, 1)$ es un vector isotrópico.

□

Así nuestra prueba se reduce al siguiente resultado, llamado el teorema del Cuadrado.

Teorema 4.1.2. *Supongamos que $c \in \mathbb{Q}^\times$. c es un cuadrado en $\mathbb{Q}$ si y sólo si c es un cuadrado en todos los $\mathbb{Q}_v$.*

Demostración. ($\Rightarrow$) Supongamos que c es un cuadrado en $\mathbb{Q}$

$$\begin{aligned} &\Rightarrow \quad c = p_1^{2e_1}...p_r^{2e_r} \text{ para distintos primos } p_i \\ &\Rightarrow \quad ord_{p_i}(c) = 2e_i \text{ para todo } i \\ &\Rightarrow \quad c \text{ es un cuadrado para todo } \mathbb{Q}_v \end{aligned}$$

($\Leftarrow$) Supongamos que c es un cuadrado en todos los $\mathbb{Q}_v$ entonces sea $c = \pm p_1^{e_1}...p_r^{e_r}$ para distintos números primos p_i.
Si $c \in (\mathbb{Q}_{p_i}^\times)^2$ para todo primo p_i

$$\begin{aligned} &\Rightarrow \quad ord_{p_i}(c) \text{ es par para todo primo } p_i \\ &\Rightarrow \quad e_i \text{ es par para todo } i \end{aligned}$$

Si $c \in (\mathbb{Q}_\infty^\times)^2 = (\mathbb{R}^\times)^2$ entonces $c > 0$.
Por lo tanto, c es un cuadrado en $\mathbb{Q}$. □

Teorema 4.1.3. *Para a, b en $\mathbb{Q}^\times$ la ecuación $ax^2 + by^2 = 0$ es soluble no trivialmente sobre $\mathbb{Q}$ si y sólo si es soluble no trivialmente sobre todo $\mathbb{Q}_v$.*

Demostración. Se tienen las siguientes equivalencias Lema 4.1.1 $\Leftrightarrow$ Teorema 4.1.2 $\Leftrightarrow$ Lema 4.1.1, es decir:
La forma cuadrática no degenerada $ax^2 + by^2$ tiene un vector isotrópico sobre $\mathbb{Q}$ sí y solo sí $-\frac{b}{a} \in \mathbb{Q}^{\times 2}$ sí y solo sí $-\frac{b}{a} \in \mathbb{Q}_v^{\times 2}$ para cada v sí y solo sí la forma cuadrática $ax^2 + by^2$ tiene un vector isotrópico sobre cada $\mathbb{Q}_v$. □

4.2. $n = 3$

Queremos probar que para a, b, c en $\mathbb{Q}^\times$ que si $ax^2+by^2+cz^2 = 0$ es no trivialmente soluble sobre todos los $\mathbb{Q}_v$ entonces $ax^2+by^2+cz^2 = 0$ es no trivial sobre $\mathbb{Q}$. La recíproca es consecuencia de que $\mathbb{Q}$ está incluida en sus completaciones. Primero haremos una serie de reducciones. Los coeficientes a, b y c pueden ser tomados todos números enteros pues si fuesen números racionales multiplicando a todos por el común denominador de los coeficientes no se afecta la existencia de una solución racional no trivial. Si alguno de los coeficientes tiene un factor cuadrático entonces por un cambio lineal de variables podemos conseguir que a, b y c sean libres de cuadrados. Por ejemplo, si un entero cuadrado m^2 es un factor de a, digamos que $a = a'm^2$ entonces hagamos el cambio $x' = mx$, así

$$ax^2 + by^2 + cz^2 = a'(mx)^2 + +by^2 + cz^2 = a'x'^2 + by^2 + cz^2.$$

Desde que $ax^2+by^2+cz^2 = 0$ tiene una solución no trivial en $\mathbb{R}$, uno de los coeficientes debería tener diferente signo de los otros dos. Sin pérdida de generalidad, podemos suponer que $a > 0, b > 0$ y $c < 0$. Reescribimos c como $-c$ con $c > 0$, así nuestra forma cuadrática se transforma en $ax^2 + by^2 - cz^2$. Finalmente podemos multiplicar por c y entonces usar un cambio lineal de variables para conseguir los coeficientes de x y y para ser coeficientes libres de cuadrados otra vez mientras que el coeficiente de z es -1. Así podemos suponer que nuestra forma cuadrática $ax^2 + by^2 - z^2$ donde a y b son enteros libres de cuadrados. Ahora daremos una prueba por inducción para el valor de los coeficientes.

Teorema 4.2.1. *Sean a y b enteros libres de cuadrados. Si $ax^2 + by^2 = z^2$ tiene una solución no trivial sobre cada $\mathbb{Q}_v$ sí y solo sí $ax^2 + by^2 = z^2$ tiene una solución no trivial racional.*

Demostración. ($\Leftarrow$) Se sigue de que $\mathbb{Q} \subset \mathbb{Q}_v$

($\Rightarrow$) Haremos inducción sobre $|a| + |b|$.

Si $|a| + |b| = 2$ entonces $|a| = |b| = 1$ por lo que las ecuaciones que satisfacen estas condiciones son:

- $x^2 + y^2 - z^2 = 0$ la cual tiene solución $(1, 0, 1)$,
- $x^2 - y^2 - z^2 = 0$ la cual tiene solución $(1, 0, 1)$,
- $-x^2 + y^2 - z^2 = 0$ la cual tiene solución $(1, 1, 0)$,
- $-x^2 - y^2 - z^2 = 0$ la cual tiene solución $(0, 0, 0)$ en $\mathbb{R}$ y en $\mathbb{Q}_2$ como se mostró en el Ejemplo 3.2.14. (Por el Ejemplo 3.2.9 hay soluciones no triviales en $\mathbb{Q}_p$ para todos los impares p.)

Supongamos que $|a| + |b| > 2$ y que el teorema sea verdadero para todos los valores menores que $|a| + |b|$.

Sin pérdida de generalidad, supongamos que $|a| \leq |b|$, así $|b| \geq 2$.

Afirmación 1: a es un cuadrado mod b.

Como b es libre de cuadrados, supongamos que $b = \pm p_1 ... p_k$ donde los $p_1, ..., p_k$ son primos distintos.

Por hipótesis, para cada primo $p \in \{p_1, ..., p_k\}$ existe una solución no trivial $(x_p, y_p, z_p) \in \mathbb{Q}_p^3$ tal que $ax_p^2 + by_p^2 = z_p^2$. Multiplicando por escalares podemos suponer que (x_p, y_p, z_p) es una solución primitiva (esto significa que x_p, y_p y $z_p \in \mathbb{Z}_p$ y que al menos uno de ellos es no nulo en $\mathbb{Z}_p$).

Mostraremos que x_p está en $\mathbb{Z}_p^\times$. En efecto, si $p|x_p$

$$\begin{aligned} &\Rightarrow \quad p|ax_p^2 \\ &\Rightarrow \quad p|(z_p^2 - by_p^2) \text{ y } p|b \\ &\Rightarrow \quad p|z_p^2 \\ &\Rightarrow \quad p|z_p \end{aligned}$$

Entonces tenemos que $p|x_p$ y $p|z_p$

$$\begin{aligned}
&\Rightarrow \quad p^2|x_p^2 \text{ y } p^2|z_p^2 \\
&\Rightarrow \quad p^2|(z_p^2 - ax_p^2) \\
&\Rightarrow \quad p^2|by_p^2 \\
&\Rightarrow \quad p^2|y_p^2 \text{ ... pues } b \text{ es libre de cuadrados.} \\
&\Rightarrow \quad p|y_p^2 \\
&\Rightarrow \quad p|y_p
\end{aligned}$$

Por lo tanto, $p|x_p$, $p|y_p$ y $p|z_p$ lo que contradice la suposición de que (x_p, y_p, z_p) es una solución primitiva entonces debe ocurrir que p no divide a x_p es decir $x_p \not\equiv 0 \mod p$ por lo que $x_p \in \mathbb{Z}_p^\times$.

Desde que p divide a b en $ax_p^2 + by_p^2 = z_p^2$,

$$\begin{aligned}
&\Rightarrow \quad ax_p^2 \equiv z_p^2 \mod p \text{ y } x_p \in \mathbb{Z}_p^\times \\
&\Rightarrow \quad a \equiv \frac{z_p^2}{x_p^2} \mod p \\
&\Rightarrow \quad a \equiv \left(\frac{z_p}{x_p}\right)^2 \mod p.
\end{aligned}$$

Tenemos que

$$\begin{cases}
a \equiv \left(\frac{z_{p_1}}{x_{p_1}}\right)^2 \mod p_1 \\
\vdots \quad \vdots \quad \vdots \\
a \equiv \left(\frac{z_{p_k}}{x_{p_k}}\right)^2 \mod p_k
\end{cases}$$

Por el Teorema chino del resto,

$$a \equiv m^2 \mod b \text{ en } \mathbb{Z}/b\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}$$

Por lo tanto, a es un cuadrado módulo b.

Como a es un cuadrado módulo b existen m y q en $\mathbb{Z}$ tales que $m^2 = a + bq$ para algún $q \in \mathbb{Z}$. Sin perder generalidad podemos suponer que $|m| \leq \frac{|b|}{2}$. (Si $|m| > \frac{|b|}{2}$ entonces $\frac{|b|}{2} - |m| < 0$ entonces $|b| - |m| < \frac{|b|}{2}$ entonces $(|b| - |m|)^2 \equiv a \mod b$ entonces $|b|^2 - 2|b||m| + |m|^2 \equiv a \mod b$ entonces $m^2 \equiv a \mod b$).

Sabemos que a es libre de cuadrados y el caso $a = 1$ es trivial, así que $q \neq 0$. (Si $q = 0$

entonces $m^2 = a + (0)b$ entonces $a = m^2$ entonces a es cuadrado).

Supongamos que $q = cd^2$ donde c es un entero libre de cuadrados.

Dividiendo a $a + bcd^2 = m^2$ por $(cd)^2$ se obtiene

$$\begin{aligned}
\frac{a + bcd^2}{c^2d^2} &= \frac{m^2}{c^2d^2} \\
\frac{a}{c^2d^2} + \frac{b}{c} &= \frac{m^2}{c^2d^2} \\
\frac{b}{c} &= \frac{m^2}{(cd)^2} - \frac{a}{(cd)^2} \\
\frac{b}{c} &= \left(\frac{m}{cd}\right)^2 - a\left(\frac{1}{cd}\right)^2
\end{aligned}$$

$$\Rightarrow \frac{b}{c} \in \{x^2 - ay^2 \neq 0 : x, y \in \mathbb{Q}\} \tag{4.1}$$

$$\Rightarrow \frac{b}{c} \in \{x^2 - ay^2 \neq 0 : x, y \in \mathbb{Q}_v\}. \tag{4.2}$$

Por la hipótesis, $ax^2 + by^2 = z^2$ tiene solución no trivial en cada $\mathbb{Q}_v$ entonces por el Teorema 3.3.4, $b = x_v^2 - ay_v^2$ en cada $\mathbb{Q}_v$, así por (4.2) y porque $\{x^2 - ay^2 \neq 0 : x, y \in \mathbb{Q}_v\}$ es un subgrupo de $\mathbb{Q}_v^\times$ se tiene que c tiene la misma forma en cada $\mathbb{Q}_v$ entonces nuevamente por el Teorema 3.3.4) existen soluciones no triviales para $ax^2 + cy^2 = z^2$ en todos los $\mathbb{Q}_v$

Afirmación 2: $|a| + |c| < |a| + |b|$

Como $|a| \leq |b|$ y $a + bcd^2 = m^2$ entonces

$$\begin{aligned}
|c| \leq |cd^2| &= |\frac{m^2 - a}{b}| \\
&\leq |\frac{m^2}{b}| + |\frac{a}{b}| \\
&= |m|^2\frac{1}{|b|} + |\frac{a}{b}| \\
&\leq \frac{|b|^2}{4}\frac{1}{|b|} + 1 \text{ ... pues } |m| \leq \frac{|b|}{2} \text{ y } |\frac{a}{b}| \leq 1 \\
&\leq \frac{|b|}{4} + 1 \\
&< |b|
\end{aligned}$$

(Si $\frac{|b|}{4} + 1 \geq |b|$ entonces $|b| + 4 \geq 4|b|$ entonces $|b| \leq \frac{4}{3}$ ... contradicción)

Así si $|c| < |b|$ entonces $|a| + |c| < |a| + |b|$

Tenemos que $ax^2 + cy^2 = z^2$ tiene solución no trivial en cada $\mathbb{Q}_v$ entonces por hipótesis inductiva existe una solución racional no trivial para $ax^2 + cy^2 = z^2$.
Por el Teorema 3.3.4, se tiene que $c = r^2 - as^2$ para algún $r, s \in \mathbb{Q}$. Otra vez por (4.1), b tiene la forma $x^2 - ay^2$ para algún $x, y \in \mathbb{Q}$. Por lo tanto, por el Teorema 3.3.4, $ax^2 + by^2 = z^2$ tiene una solución racional no trivial. □

4.3. $n = 4$

La prueba para el caso $n = 4$ del teorema de Hasse-Minkowski sobre $\mathbb{Q}$ requiere los dos siguientes teoremas. El primero será citado sin prueba.

Teorema 4.3.1. *(Dirichlet) Para a y m en $\mathbb{Z}$ con $(a, m) = 1$, existen infinitos números primos p tales que $p \equiv a \mod m$.*

Recordemos la definición 3.3.1 del Símbolo de Hilbert. Para el resto de este capítulo $(a, b)_{\mathbb{Q}_v}$ será denota por $(a, b)_v$ con la convención que $(a, b)_\infty = (a, b)_{\mathbb{R}}$

Teorema 4.3.2. *Sean a, b en $\mathbb{Q}^\times$*

1. *Hay un número finito de v tales que $(a, b)_v = -1$.*
2. *$\prod_v (a, b)_v = 1$. En otras palabras, $\#\{v : (a, b)_v = -1\}$ es par.*

Demostración.

1. Ya lo sabemos por el teorema 3.2.8. Más precisamente, esto significa que el único v para el cual $(a, b)_v$ puede ser -1 son ∞, 2 y los primos impares para el cual a y b no están en $\mathbb{Z}_p^\times$.

2. De la bimultiplicidad y simetría del símbolo de Hilbert (Corolario 3.3.7), es suficiente ver que 2. es verdadero cuando a y b son -1 o primos, Desde que $(a, a)_v = (a, -1)_v$, no tenemos que comprobar el caso cuando a y b son el mismo número primo.

   Supongamos $a = b = -1$ entonces $(-1, -1)_v = 1$ para $v \notin \{2, \infty\}$ mientras que $(-1, -1)_\infty = (-1, -1)_2 = -1$ del Ejemplo 3.3.8.

   Si $a = -1$ y $b = 2$ entonces $(-1, 2)_v = 1$ para todos los v puesto que $2 = 1^2 + 1^2$.

Recordemos la fórmula para el símbolo de Hilbert sobre un Cuerpo local F con un cuerpo residual de característica impar:

$$(a,b)_F = (\pi^m\varepsilon, \pi^n\delta)_F = (-1)^{\frac{mn(q-1)}{2}}\chi(\overline{\varepsilon})^n\chi\left(\overline{\delta}\right)^m \tag{4.3}$$

donde π es un uniformalizador, ε y δ son unidades, q es el tamaño del cuerpo residual y $\chi : (\mathcal{O}_F/\mathfrak{m}_F)^\times \to \{\pm 1\}$ es la característica cuadrática sobre el Cuerpo residual. Usamos esta fórmula en los casos restantes para $\mathbb{Q}_p$ donde p es impar. La característica cuadrática sobre el Cuerpo residual de $\mathbb{Q}_p$ es el símbolo de Legendre $\left(\frac{\cdot}{p}\right)$.

Supongamos que $a = -1$ y $b = l$ para algún primo l entonces $(-1,1)_v = 1$ para impar $v \neq l$ y $v = \infty$. Sobre $\mathbb{Q}_l$, $(-1,l)_l = \left(\frac{-1}{l}\right)$ por (4.3). Sobre $\mathbb{Q}_2$, la ecuación $-x^2 + ly^2 - z^2 = 0$ tiene una solución no trivial (por Corolario 3.2.13) si y sólo si existe una solución primitiva para la congruencia

$$-x^2 + ly^2 - z^2 \equiv 0 \mod 8.$$

Si l es $1 \mod 4$ (así $l \equiv 1$ o $5 \mod 8$) entonces claramente existe una solución primitiva. Si l es $3 \mod 4$ entonces un cálculo tedioso muestra que hay una solución primitiva. Por lo tanto, tenemos que $(-1,l)_2 = (-1)^{\frac{l-1}{2}}$. Así

$$\prod_v (-1,l)_v = (-1,l)_l(-1,l)_2 = \left(\frac{-1}{l}\right)(-1)^{\frac{l-1}{2}},$$

el cual es 1 si y sólo sí la primera propiedad suplementaria de la reciprocidad cuadrática es verdadera. Ahora supongamos que $a = 2$ y $b = l$ donde l es un primo impar. Así antes $(2,l)_v = 1$ para todo primo impar $v \neq l$ y $v = \infty$. También, $(2,l)_l = \left(\frac{2}{l}\right)$ usando (4.3). Sobre $\mathbb{Q}_2$, podemos considerar la congruencia

$$2x^2 + ly^2 - z^2 \equiv 0 \mod 8.$$

Si l es 1 o $7 \mod 8$ entonces es claro que $(2,l)_2 = 1$ puesto que la congruencia proviene de

$$2x^2 + y^2 - z^2 \equiv 0 \mod 8.$$

o

$$2x^2 - y^2 - z^2 \equiv 0 \quad \text{mód } 8.$$

Si $l \equiv 3$ o $5 \mod 8$ un cálculo muestra que no hay soluciones primitivas para la congruencia. Así $(2,l)_2 = (-1)^{\frac{l^2-1}{8}}$, así

$$\prod_v (2,l)_v = (2,l)_l (2,l)_2 = \left(\frac{2}{l}\right)(-1)^{\frac{l^2-1}{8}}$$

el cual es 1 sí y sólo sí la segunda ley suplementaria de la reciprocidad cuadrática es verdadera.

Finalmente supongamos que $a = l$ y $b = l'$ para distintos primos impares l, l' Entonces $(a,b)_v = 1$ para todos los v distintos de l, l' y 2. La fórmula (4.3) del simbolo de Hilbert muestra que $(l,l')_l = \left(\frac{l'}{l}\right)$ y $(l',l)_{l'} = \left(\frac{l}{l'}\right)$. En una manera similar a la anterior, la congruencia

$$lx^2 + l'y^2 - z^2 \equiv 0 \quad \text{mód } 8$$

tiene soluciones primitivas cuando al menos uno de l, l' es $1 \mod 4$, pero no tiene soluciones primitivas cuando ambos l y l' son $3 \mod 4$. Así

$$(l,l')_2 = \begin{cases} 1 & \text{si } l \text{ o } l' \equiv 1 \mod 4 \\ -1 & \text{si } l, l' \equiv 3 \mod 4 \end{cases} = (-1)^{\frac{l-1}{2}\frac{l'-1}{2}}$$

Así tenemos

$$\prod_v (l,l')_v = (l,l')_l (l,l')_{l'} (l,l')_2 = \left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right)(-1)^{\frac{l-1}{2}\frac{l'-1}{2}},$$

el cual es 1 sí y sólo sí la ley principal de la reciprocidad cuadrática se satisface.

□

Observación 4.3.3. *El segundo enunciado en el Teorema 4.3.2 es conocido como la Reciprocidad de Hilbert. Como se puede ver de la demostración del teorema, los casos no triviales de la reciprocidad de Hilbert son equivalentes a la reciprocidad cuadrática sin ningún papel especial para 2 o para la positividad como en el enunciado clásico de la reciprocidad cuadrática. Todos los primos (incluyendo a ∞) están en pie de igualdad. Por otra parte, la reciprocidad de Hilbert generaliza a todos los Cuerpos globales.*

Observación 4.3.4. *La reciprocidad de Hilbert dice que* $(a,b)_v = -1$ *para un número par de* v*. Por ejemplo, recordemos que la ecuación* $-x^2 - y^2 - z^2 = 0$ *en la prueba del caso* $n = 3$ *de Hasse-Minkowski tiene una solución no trivial en* $\mathbb{Q}_v$ *para todos los* v *excepto* $v = 2$ *y* $v = \infty$*.*

Corolario 4.3.5. *Para cualquier forma cuadrática no degenerada* q *sobre* $\mathbb{Q}$*,* $c_v(q) = -1$ *para un número finito de* v *y* $\prod_v c_v(q) = 1$*.*

Demostración. Diagonalizar q y usar la reciprocidad de Hilbert. □

Corolario 4.3.6. *Sean* a, b, c *en* $\mathbb{Q}^\times$*. Si* $ax^2+by^2+cz^2 = 0$ *tiene soluciones no triviales en* $\mathbb{Q}_v$ *para todo* v *excepto quizás un* v_0*, entonces también se tiene una solución no trivial sobre* $\mathbb{Q}_{v_0}$*.*

Demostración. Teniendo una solución no trivial para $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Q}_v$ es equivalente a tener una solución no trivial para $-\frac{a}{c}x^2 - \frac{b}{c}y^2 - z^2 = 0$ en $\mathbb{Q}_v$, el cual es equivalente a $\left(-\frac{a}{c}, -\frac{b}{c}\right)_v = 1$. Por hipotesis $\left(-\frac{a}{c}, -\frac{b}{c}\right)_v = 1$ para todo $v \neq v_0$. Así la recíprocidad de Hilbert implica $\left(-\frac{a}{c}, -\frac{b}{c}\right)_v = 1$ también. □

Cuando Legendre probó primero el caso $n = 3$ del teorema de Hasse-Minkowski sobre $\mathbb{Q}$, él uso congruencias de potencias primas en lugar de números p-adicos. Curiosamente, su demostración ignora las congruencias módulo potencias de 2 (es decir, el caso 2-adico). También es posible probarlo sin poner atención a la existencia de soluciones reales; para la prueba ver Rational Quadratic forms de J.W. Cassels - 1978, pág 79-81. El Corolario 4.3.6 explica por qué esto es posible. Ahora estamos preparados para probar el caso $n = 4$ del teorema de Hasse-Minkowski sobre $\mathbb{Q}$.

Teorema 4.3.7. *Para* a, b, c, d *no nulos en* $\mathbb{Q}$*, la ecuación*

$$ax^2 + by^2 + cz^2 + dt^2 = 0$$

tiene una solución no trivial sobre $\mathbb{Q}$ *sí y sólo sí tiene una solución no trivial sobre todos los* $\mathbb{Q}_v$*.*

Demostración. ($\Rightarrow$) Se sigue de $\mathbb{Q} \subset \mathbb{Q}_v$

($\Leftarrow$) Supongamos que la forma cuadrática $ax^2+by^2+cz^2+dt^2$ tiene solución no trivial sobre cada $\mathbb{Q}_v$. Multiplicando por escalares adecuados podemos asumir que a, b, c y d están en $\mathbb{Z}$. Puesto que existe una solución sobre $\mathbb{R}$, sin perdida de generalidad supongamos que $a > 0$ y que $d < 0$.

Consideremos las formas $q_1(x,y) = ax^2 + by^2$ y $q_2(z,t) = -cz^2 - dt^2$ tales que

$$q_1(x,y) - q_2(z,t) = ax^2 + by^2 + cz^2 + dt^2 \tag{4.4}$$

Por el Corolario 2.4.22, q_1 y q_2 toman un valor común $\alpha_p \in \mathbb{Q}_p^\times$ para cada número primo p.

El propósito es usar estos valores comunes para encontrar nuestra deseada solución no trivial sobre $\mathbb{Q}$ (La solubilidad sobre los números reales fue usada para arreglar a q_1 y q_2 de tal manera que cada uno tenga un coeficiente positivo). Multiplicando por escalares, podemos suponer que α_p está en $\mathbb{Z}_p^\times$ o está en $p\mathbb{Z}_p^\times$. (Si $\alpha_p = 0$ entonces por lo menos una de las formas q_1 o q_2 es isotrópico, digamos q_1, entonces por el Teorema 2.4.18, q_1 es universal. Por lo tanto, existe un valor no nulo de $F^\times$ que es representado tanto por q_1 como por q_2 a la vez.)

Para los primos positivos impares $p \in \{p_1, ..., p_s\}$ que dividen a a, b, c y d y para el número primo 2, escogemos un entero positivo r tal que satisface el sistema de congruencias:

$$\begin{cases} r & \equiv & \alpha_2 (\mod 16) \\ r & \equiv & \alpha_{p_1} (\mod p_1^2) \\ r & \equiv & \alpha_{p_2} (\mod p_2^2) \\ \vdots & \vdots & \vdots \\ r & \equiv & \alpha_{p_s} (\mod p_s^2) \end{cases}$$

donde por el Teorema chino de resto, r es determinado de manera única módulo $m = 16p_1^2p_2^2 \dots p_s^2$.

Como α_{p_i} es divisible a lo más por la primera potencia de p_i entonces $|\frac{\alpha_{p_i}}{r}|_{p_i} = 1$ es

decir, $\frac{\alpha_{p_i}}{r}$ es una unidad p_i-ádica y se tiene que $\frac{\alpha_{p_i}}{r} \equiv 1 mod(p_i)$. Por lo tanto, $\frac{\alpha_{p_i}}{r}$ es un residuo cuadrático módulo $p\mathbb{Z}$ entonces $\frac{\alpha_{p_i}}{r}$ es un cuadrado p_i-ádico.

Por otro lado, como α_2 no es divisible por ninguna potencia superior de 2 y solo es divisible por 2, se tiene que $\frac{\alpha_2}{r} \equiv 1 mod(8)$ y $\frac{\alpha_2}{r}$ es un cuadrado 2-adico.

Del hecho que α_p y r difieren por un factor cuadrático en todos los $\mathbb{Q}_p$ para todos los $p \in \{2, p_1, p_2, \ldots, p_s\}$ entonces $\frac{\alpha_p}{r}$ está en $\mathbb{Q}_p^{\times^2}$. Así q_1 y q_2 ambos toman el valor r en este $\mathbb{Q}_p$.

Dicho de otra manera, las formas cuadráticas 3-dimensional

$$q_1'(x, y, w_1) = q_1(x, y) - rw_1^2$$

y

$$q_2'(z, t, w_2) = q_2(z, t) - rw_2^2$$

tienen vectores isotrópicos en $\mathbb{Q}_p^3$ para todo $p \mid 2abcd$. Más aún, q_1' y q_2' tienen coeficientes racionales, por lo que si podemos encontrar soluciones no triviales para $q_1' = 0$ y para $q_2' = 0$ sobre cada $\mathbb{Q}_v$, entonces podemos aplicar el teorema de Hasse-Minkowsky para $n = 3$ para conseguir las soluciones no triviales para $q_1' = 0$ y $q_2' = 0$ sobre $\mathbb{Q}$.

Las ecuaciones $q_1' = 0$ y $q_2' = 0$ tienen soluciones no triviales sobre $\mathbb{R}$ desde que $a, r, -d > 0$. Por el Teorema 3.2.8 para los p que no dividen a $2abcdr$ siempre existen soluciones no triviales sobre $\mathbb{Q}_p$ para q_1' y q_2'.

Mostraremos que es posible encontrar un entero positivo r' que se adapte a todas las condiciones impuestas sobre r, y que cada factor primo de r' excepto uno de ellos divida a $2abcd$.

Observe que r sólo importa a través de su positividad y su clase de congruencia módulo $m = 16p_1^2p_2^2...p_s^2$ y posiblemente $MCD(r, m) \neq 1$ desde que alguno de los α_p puede tener $ord_p(\alpha_p) > 0$. Sea $\delta = MCD(r, m)$ entonces $MCD(\frac{r}{\delta}, \frac{m}{\delta}) = 1$. Por el teorema de Dirichlet existen infinitos números primos l tales que

$$l \equiv \frac{r}{\delta} \mod \frac{m}{\delta}.$$

Elegir un l tal que no divide a $2abcd$ y sea $r' = l\delta$. Entonces $r' > 0$ y $r' \equiv r \mod m$, así r' se ajusta a todas las condiciones impuestas sobre r y cada primo que divide a

r' también divide a $2abcd$ excepto l. Por lo tanto, la sustitución de r con r' en q_1' y q_2', existen soluciones no triviales para $q_1' = 0$ y $q_2' = 0$ sobre cada $\mathbb{Q}_v$ con la posible excepción de $\mathbb{Q}_l$. El Corolario 4.3.6 implica que existen también soluciones no triviales para estas ecuaciones sobre $\mathbb{Q}_l$.

Usando el caso $n = 3$ de Hasse-Minkowski, existe una solución no trivial para $q_1' = 0$ y $q_2' = 0$ sobre $\mathbb{Q}$. Así existen soluciones para $q_1(x, y) = r'$ y $q_2(z, t) = r'$ sobre $\mathbb{Q}$. Así por (4.4) existe una solución no trivial para $ax^2 + by^2 + cz^2 + dt^2 = 0$ sobre $\mathbb{Q}$. □

4.4. $n \geq 5$

La prueba para $n \geq 5$ se sigue por inducción.

Teorema 4.4.1. *Sea $n \geq 5$, sea $q(x_1, ..., x_n) = a_1x_1^2 + ... + a_nx_n^2$ con $a_i \in \mathbb{Q}^\times$. Entonces $q(x_1, \cdots, x_n) = 0$ tiene una solución no trivial en $\mathbb{Q}$ si y solo si tiene una solución no trivial sobre todos los $\mathbb{Q}_v$.*

Demostración. ($\Rightarrow$) Se sigue de $\mathbb{Q} \subset \mathbb{Q}_v$

($\Leftarrow$) Sea $q = q_1 - q_2$ donde

$$q_1(x_1, x_2) = a_1x_1^2 + a_2x_2^2$$

y

$$q_2(x_3, ..., x_n) = -a_3x_3^2 - \cdots - a_nx_n^2.$$

Sea S el conjunto que consiste de los $v = 2$, $v = \infty$ y v tales que no cada $a_i \in \mathbb{Z}_v^\times$ para $i \geq 3$. Para todo $v \in S$, q_1 y q_2 representan algún valor común diferente de cero α_v sobre $\mathbb{Q}_v$ desde que q tiene un vector isotrópico sobre $\mathbb{Q}_v$ (Corolario 2.4.22). Es decir,

$$q_1(x_{1,v}, x_{2,v}) = \alpha_v = q_2(x_{3,v}, ..., x_{n,v})$$

para $x_{i,v} \in \mathbb{Q}_v$. El conjunto de cuadrados no nulos $\mathbb{Q}_v^{\times^2}$ es abierto, así el cociente de $\mathbb{Q}_v^{\times^2}$ que contiene a α_v es un conjunto abierto. La forma cuadrática q_1 es continua (es polinomial) así la imagen inversa del cociente que contiene a α_v es un conjunto abierto

A_v en $\mathbb{Q}_v \times \mathbb{Q}_v$. Por el teorema de aproximación (Teorema 3.1.12) existen $x_1, x_2 \in \mathbb{Q}$ tal que $(x_1, x_2) \in A_v$ para todo $v \in S$. Así $a := q_1(x_1, x_2)$ está en $\mathbb{Q}$ y $a/\alpha_v \in \mathbb{Q}_v^{\times^2}$ para todo $v \in S$. Consideremos la forma cuadrática $q' = at^2 - q_2$. Existe una solución no trivial para $q' = 0$ sobre cada $\mathbb{Q}_v$ para $v \in S$ puesto que $a/\alpha_v \in \mathbb{Q}_v^{\times^2}$ para todo $v \in S$. Más aun, la ecuación $q' = 0$ tiene una solución no trivial sobre cada $\mathbb{Q}_v$ donde v no está en S puesto que q_2 es universal sobre $\mathbb{Q}_v$ por el teorema 3.2.8 ($n-2$ es al menos 3). Así existe una solución no trivial para $q' = 0$ sobre $\mathbb{Q}$ por la hipótesis inductiva puesto que q' es una forma cuadrática $(n-1)$-dimensional. Esto significa que la ecuación $q_2 = a$ tiene una solución sobre $\mathbb{Q}$. Ahora tenemos soluciones sobre $\mathbb{Q}$ para $q_1 = a$ y $q_2 = a$, así

$$q = q_1 - q_2 = 0$$

tiene una solución no trivial sobre $\mathbb{Q}$. □

4.5. Aplicaciones

Una consecuencia interesante del Teorema 3.3.20 es que cada forma cuadrática indefinida (no todos los términos en una diagonalización tienen el mismo signo) de dimensión mayor o igual a 5 sobre $\mathbb{Q}$ tiene un vector isotrópico. Como un resultado, cuando q es una forma cuadrática 4-dimensional sobre $\mathbb{Q}$, la ecuación $q = r$ para $r \in \mathbb{Q}^\times$ es soluble si y solo si la forma cuadrática 5-dimensional $q - rx^2$ es indefinida. Por ejemplo, la forma cuadrática $x^2 + y^2 + z^2 - 7t^2 - ru^2$ del ejemplo 2.4.21 es universal sobre $\mathbb{Q}$ puesto que para cualquier $r \in \mathbb{Q}^\times$,

$$x^2 + y^2 + z^2 - 7t^2 - ru^2$$

es indefinida.

Proposición 4.5.1. *Si $x \in \mathbb{Z}$ y $x^2 \equiv r \mod 8$ entonces $r \in \{0, 1, 4\}$*

Demostración. Caso 1: Si x es par entonces para algún s en $\mathbb{Z}$

$$\begin{aligned}
\Rightarrow \quad & x = 2(2s) \quad o \quad x = 2(2s+1) \\
\Rightarrow \quad & x = 4s \quad o \quad x = 4s+2 \\
\Rightarrow \quad & x^2 = 16s^2 \quad o \quad x^2 = 16s^2 + 16s + 4 \\
\Rightarrow \quad & x^2 \equiv 0 \mod 8 \quad o \quad x^2 \equiv 4 \mod 8
\end{aligned}$$

Caso 2: Si x es impar entonces para algún s en $\mathbb{Z}$

$$\begin{aligned}
\Rightarrow \quad & x = 2s+1 \\
\Rightarrow \quad & x^2 = 4s^2 + 4s + 1 \\
\Rightarrow \quad & x^2 = 4s(s+1) + 1 \\
\Rightarrow \quad & x^2 \equiv 1 \mod 8
\end{aligned}$$

Por lo tanto $r \in \{0, 1, 4\}$. □

Retornamos a los teoremas del Capítulo 1 sobre enteros como suma de enteros cuadrados. Reafirmamos el Teorema 1.0.4 y lo probamos.

Teorema 4.5.2. *(Legendre) Sea n un número entero positivo de la forma $4^a n'$ con $a \geq 0$ y $n' \not\equiv 0$ mod 4 Entonces n es una suma de tres enteros cuadrados si y solo si $n' \not\equiv 7$ mod 8.*

Demostración. Si $n = x^2 + y^2 + z^2$ para algunos x, y, z en $\mathbb{Z}$ entonces

$$\begin{aligned}
4^a n' &= x^2 + y^2 + z^2 \\
n' &= \left(\frac{x}{2^a}\right)^2 + \left(\frac{y}{2^a}\right)^2 + \left(\frac{z}{2^a}\right)^2 \\
n' &= x'^2 + y'^2 + z'^2
\end{aligned}$$

donde $x' = \dfrac{x}{2^a}$, $y' = \dfrac{y}{2^a}$ y $z' = \dfrac{z}{2^a}$ están en $\mathbb{Q}$. Por el teorema 1.0.7, n' es la suma de

tres enteros cuadrados entonces $n' = u^2 + v^2 + w^2$ con u, v, w en $\mathbb{Z}$

$$
\begin{aligned}
n' &\equiv u^2 + v^2 + w^2 \quad \text{mód } (8) \\
n' &\equiv (u^2 \quad \text{mód } (8)) + (v^2 \quad \text{mód } (8)) + (w^2 \quad \text{mód } (8)) \\
n' &\equiv \underbrace{(u^2 \quad \text{mód } (8))}_{0,1,4} + \underbrace{(v^2 \quad \text{mód } (8))}_{0,1,4} + \underbrace{(w^2 \quad \text{mód } (8))}_{0,1,4} \text{... por Proposición 4.5.1} \\
n' &\equiv 0 + 1 + 4 = 5 \equiv 5 \quad \text{mód } (8) \\
n' &\equiv 0 + 0 + 1 = 1 \equiv 1 \quad \text{mód } (8) \\
n' &\equiv 0 + 0 + 0 = 0 \equiv 0 \quad \text{mód } (8) \\
n' &\equiv 1 + 1 + 0 = 2 \equiv 2 \quad \text{mód } (8) \\
n' &\equiv 1 + 1 + 4 = 6 \equiv 6 \quad \text{mód } (8) \\
n' &\equiv 1 + 4 + 4 = 9 \equiv 1 \quad \text{mód } (8) \\
n' &\equiv 1 + 1 + 1 = 3 \equiv 3 \quad \text{mód } (8)
\end{aligned}
$$

Por lo tanto $n' \not\equiv 7 \bmod (8)$.

Recíprocamente, supongamos que $n' \not\equiv 7 \bmod 8$. Entonces n' es 1, 2, 3, 5 o 6 modulo 8 porque 4 no debe dividir a n'. Ahora mostramos que n' es la suma de tres cuadrados racionales usando el teorema de Hasse-Minkowski.

Por el teorema 3.2.8 y para todos los primos impares p, la forma cuadrática $x^2+y^2+z^2$ tiene un vector isotrópico sobre $\mathbb{Q}_p$ y por el teorema 2.4.18, $x^2 + y^2 + z^2$ es universal sobre $\mathbb{Q}_p$.

Sobre $\mathbb{R}$, $x^2 + y^2 + z^2$ representa n', es decir, $n' = x^2 + y^2 + z^2$ puesto que $n' > 0$.

Sobre $\mathbb{Q}_2$, mostramos que n' es congruente a $x^2 + y^2 + z^2 \bmod 8$:

- Si $n' \equiv 1 \bmod 8$, cuando $(x, y, z) = (1, 0, 0)$,
- Si $n' \equiv 2 \bmod 8$, cuando $(x, y, z) = (1, 1, 0)$,
- Si $n' \equiv 3 \bmod 8$, cuando $(x, y, z) = (1, 1, 1)$,
- Si $n' \equiv 5 \bmod 8$, cuando $(x, y, z) = (1, 2, 0)$,
- Si $n' \equiv 6 \bmod 8$, cuando $(x, y, z) = (1, 1, 2)$.

Por lo tanto, la forma cuadrática $x^2+y^2+z^2-n't^2$ tiene una solución primitiva módulo 8 en $\mathbb{Z}_2$ y por el Corolario 3.2.13 también una solución 2-ádica. Así $x^2+y^2+z^2$ representa n' sobre $\mathbb{Q}_2$. Por lo tanto, $x^2+y^2+z^2$ representa a n' en $\mathbb{R}$ y en cada cuerpo p-ádico $\mathbb{Q}_p$ entonces por el Teorema de Hasse-Minkowski para tres variables, $x^2+y^2+z^2$ representa a n' en $\mathbb{Q}$, es decir n' es la suma de tres racionales cuadrados. Por el teorema 1.0.7 se implica que n' es una suma de tres enteros cuadrados, digamos:
$n' = s_1^2 + s_2^2 + s_3^2$ con s_1, s_2 y s_3 en $\mathbb{Z}$ entonces:

$$\begin{aligned} 4^a n' &= 4^a s_1^2 + 4^a s_2^2 + 4^a s_3^2 \\ n &= (2^a s_1)^2 + (2^a s_2)^2 + (2^a s_3)^2 \\ n &= (\underbrace{2^a s_1}_{\in\mathbb{Z}})^2 + (\underbrace{2^a s_2}_{\in\mathbb{Z}})^2 + (\underbrace{2^a s_3}_{\in\mathbb{Z}})^2 \end{aligned}$$

Por lo tanto, n es una suma de tres enteros cuadrados. □

Ahora reafirmamos y probamos el Teorema 1.0.5 como consecuencia del Teorema 4.5.2.

Teorema 4.5.3. *(Lagrange). Cada entero positivo es una suma de cuatro enteros cuadrados.*

Demostración. Sea $n \in \mathbb{Z}^+$ tal que $n = 4^a n'$ con 4 no dividendo a n' y $a \geq 0$.
Si $n' \not\equiv 7 \bmod 8$ por el Teorema 4.5.2, n es la suma de tres cuadrados enteros. Tomando al número cero como cuarto sumando tenemos que n es la suma de cuatro enteros cuadrados.
Si n' es 7 módulo 8 entonces

$$\begin{aligned} n'-1 &\equiv 6 \quad \text{mód } (8) \\ n'-1 &\not\equiv 7 \quad \text{mód } (8). \end{aligned}$$

También $n' \equiv 7 \ \text{ mód } (8)$ entonces

$$\begin{aligned} n' &\equiv 7 \quad \text{mód } (4) \\ n' &\equiv 3 \quad \text{mód } (4) \\ n'-1 &\equiv 2 \quad \text{mód } (4) \\ n'-1 &\not\equiv 0 \quad \text{mód } (4) \end{aligned}$$

Nuevamente por el Teorema 4.5.2 se tiene:

$4^a(n'-1) = x_0^2 + y_0^2 + z_0^2$ para algún x_0, y_0, z_0 en $\mathbb{Z}$ entonces

$$\begin{aligned} 4^a(n'-1) &= x_0^2 + y_0^2 + z_0^2 \\ 4^a n' - 4^a &= x_0^2 + y_0^2 + z_0^2 \\ 4^a n' &= x_0^2 + y_0^2 + z_0^2 + 4^a \\ n &= x_0^2 + y_0^2 + z_0^2 + (2^a)^2 \end{aligned}$$

Por lo tanto n es la suma de cuatro enteros cuadrados. □

El siguiente teorema está relacionado al teorema de Hasse-Minkowski.

Teorema 4.5.4. *Dos formas cuadráticas no degeneradas con coeficientes racionales son equivalentes sobre $\mathbb{Q}$ si y solo si ellas son equivalentes en cada $\mathbb{Q}_v$.*

Demostración. Como en la prueba del teorema de Hasse-Minkowski es claro que solo una dirección necesita probarse. Supongamos que dos formas cuadráticas no degeneradas con coeficientes racionales q_1 y q_2 son equivalentes sobre todo $\mathbb{Q}_v$. Mostraremos que $q_1 \cong q_2$ sobre $\mathbb{Q}$ por inducción sobre la dimensión n.

Sea $n = 1$ entonces $q_1 = ax^2$ y $q_2 = bx^2$ para $a, b \in \mathbb{Q}^\times$. Como $q_1 \cong q_2$ sobre $\mathbb{Q}_v$, $\frac{a}{b} \in \mathbb{Q}_v^{\times^2}$, el teorema 4.1.2 implica que $\frac{a}{b} \in \mathbb{Q}^{\times^2}$. Por lo tanto, $q_1 \cong q_2$ sobre $\mathbb{Q}$.

Sea $n > 1$ y supongamos que el teorema se satisface para todas las dimensiones menores de la forma cuadrática no degenerada con coeficientes racionales. Sea w un vector sobre $\mathbb{Q}$ tal que $q_1(w) = a$ donde $a \in \mathbb{Q}^\times$. Entonces $q_2(w_v) = a$ para algún vector w_v sobre cada $\mathbb{Q}_v$ puesto que $q_1 \cong q_2$ sobre todo $\mathbb{Q}_v$, así $q_2(w') = a$ para algún vector w' sobre $\mathbb{Q}$ por el teorema de Hasse-Minkowski. Así,

$$q_1 \cong ax_1^2 + Q_1'$$

y

$$q_2 \cong ay_1^2 + Q_2'$$

sobre $\mathbb{Q}$ donde q_1' y q_2' son formas cuadráticas $(n-1)$-dimensional. Como $q_1 \cong q_2$ sobre cada $\mathbb{Q}_v$ y $ax_1^2 \cong ay_1^2$ sobre $\mathbb{Q}$ (y cada $\mathbb{Q}_v$), la cancelación de Witt dice que $q_1' \cong q_2'$ sobre $\mathbb{Q}$ por la hipótesis inductiva. Por lo tanto, $q_1 \cong q_2$ sobre $\mathbb{Q}$. □

Observación 4.5.5. *El teorema 4.5.4 es referido como el teorema débil de Hasse-Minkowski. Hasse originalmente lo probó sin hacer uso de la cancelación de Witt o del teorema de Hasse-Minkowski. El usual teorema de Hasse-Minkowski es llamado (en comparación) el teorema fuerte de Hasse-Minkowski. Mas aun, el teorema fuerte de Hasse-Minkowski puede ser derivado del teorema débil de Hasse-Minkowski.*

Capítulo 5

Conclusiones

Las conclusiones del estudio del Teorema de Hasse-Minkowski sobre $\mathbb{Q}$ son:

- Los números p-ádicos le dieron a los números racionales $\mathbb{Q}$ una base para crear nuevos cuerpos numéricos.
- La clasificación de las formas cuadráticas.
- Un criterio para saber cuando una forma cuadrática no degenerada tiene solución no trivial sobre $\mathbb{Q}$.
- Un criterio para saber cuando una forma cuadrática no degenerada tiene solución no trivial sobre los números reales $\mathbb{R}$ y cada cuerpo p-ádico $\mathbb{Q}_p$.

Bibliografía

[1] Zenon Ivanovich Borevich and Igor Rostislavovich Shafarevich. *Number theory*. Academic press, 1986.

[2] Adam Gamzon. The hasse-minkowski theorem. 2006.

[3] Nathan Jacobson. Basic algebra ii, 1989, 1989.

[4] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saitō. *Number Theory: Fermat's dream*. AMS Bookstore, 2000.

[5] Tsit-Yuen Lam. The algebraic theory of quadratic forms. *W.A. Benjamin, Inc*, 1973.

[6] Paul J McCarthy. *Algebraic extensions of fields*. Courier Corporation, 1991.

[7] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270. Springer Science & Business Media, 2012.

[8] Lang Serge. *Algebra*. Springer, 2002.

[9] JP Serre. A course in arithmetic springer verlag. *Berlin etc*, 1973.

[10] Felipe Zaldívar. *Introducciión a la teoría de números*. Fondo de Cultura Económica, 2014.