

7.5 Isomorfismos de espacios con producto escalar

Sean $(\mathcal{E}, \langle \bullet \rangle)$ y $(\mathcal{F}, \langle \star \rangle)$ dos espacios con producto escalar. Una TL biyectiva $f : \mathcal{E} \rightarrow \mathcal{F}$ es un **isomorfismo de espacios con producto escalar** si f preserva el producto o sea si $\forall \mathbf{x}, \mathbf{y} \in \mathcal{E}$ se cumple que $\langle \mathbf{x} \bullet \mathbf{y} \rangle = \langle f(\mathbf{x}) \star f(\mathbf{y}) \rangle$.

La inversa de un isomorfismo es un isomorfismo. Si existe un isomorfismo entre $(\mathcal{E}, \langle \bullet \rangle)$ y $(\mathcal{F}, \langle \star \rangle)$ entonces se dice que los espacios con producto escalar son isomorfos. Si $\mathcal{E} = \mathcal{F}$ entonces, abusaremos del lenguaje y diremos que los productos escalares son isomorfos.

Ejercicio 1 Pruebe que la composición de isomorfismos de espacios con producto escalar es un isomorfismo. Lo mismo para la función inversa.

Ejercicio 2 Pruebe que los isomorfismos de espacios con producto escalar preservan la relación de perpendicularidad, los conjuntos ortogonales, la alternancia, la simetría y la antisimetría.

Si dos espacios son isomorfos entonces, o los dos son ortogonales o los dos son simplécticos. A un isomorfismo entre espacios ortogonales los llamaremos **isomorfismo ortogonal**. A un isomorfismo entre espacios simplécticos los llamaremos **isomorfismo simpléctico**.

Si $(\mathcal{E}, \langle \bullet \rangle)$ es un espacio ortogonal entonces el conjunto de todos sus automorfismos ortogonales es un subgrupo del grupo general lineal $GL(\mathcal{E})$ y se le llama **grupo ortogonal** de $(\mathcal{E}, \langle \bullet \rangle)$ y lo denotaremos por $O(\mathcal{E}, \langle \bullet \rangle)$ o por $O(\mathcal{E})$ si queda claro cual es el producto bilineal.

Si $(\mathcal{E}, \langle \bullet \rangle)$ es un espacio simpléctico entonces el conjunto de todos sus automorfismos simplécticos es un subgrupo del grupo general lineal $GL(\mathcal{E})$ y se le llama **grupo simpléctico** de $(\mathcal{E}, \langle \bullet \rangle)$ y lo denotaremos por $Sp(\mathcal{E}, \langle \bullet \rangle)$ o por $Sp(\mathcal{E})$ si queda claro cual es el producto bilineal.

Clasificación de productos bilineales. Caso simpléctico.

Ya sabemos como construir todos los productos bilineales posibles: sumando planos simplécticos o sumando espacios de dimensión 1. Sin embargo, es muy posible que al construir dos espacios con producto bilineal de diferentes formas obtengamos el mismo (salvo isomorfismos). En lo que sigue nos ocuparemos de este problema. El resultado más básico que usamos para probar que dos espacios son isomorfos es la “extensión bilineal”.

7.1

Si dos productos bilineales coinciden en una base entonces, son el mismo.

Prueba. Sea \mathbf{N} una base del espacio y $\mathbf{x} = \sum_{i \in \mathbf{N}} \alpha_i \mathbf{i}$, $\mathbf{y} = \sum_{j \in \mathbf{N}} \beta_j \mathbf{j}$ dos cualesquiera de sus vectores. Tenemos

$$\langle\langle \mathbf{x} \bullet \mathbf{y} \rangle\rangle = \langle\langle \sum_{i \in \mathbf{N}} \alpha_i \mathbf{i} \bullet \sum_{j \in \mathbf{N}} \beta_j \mathbf{j} \rangle\rangle = \sum_{i \in \mathbf{N}} \sum_{j \in \mathbf{N}} \alpha_i \beta_j \langle\langle \mathbf{i} \bullet \mathbf{j} \rangle\rangle$$

y por lo tanto $\langle\langle \mathbf{x} \bullet \mathbf{y} \rangle\rangle$ está definido a priori por los $\langle\langle \mathbf{i} \bullet \mathbf{j} \rangle\rangle$. ■

Ejercicio 3 Sean $(\mathcal{E}, \langle\langle \bullet \bullet \rangle\rangle)$ y $(\mathcal{F}, \langle\langle * * \rangle\rangle)$ dos espacios con producto bilinear con bases \mathbf{N} y \mathbf{M} respectivamente. Pruebe que si $f : \mathbf{N} \rightarrow \mathbf{M}$ es una función biyectiva tal que $\forall \mathbf{i}, \mathbf{j} \in \mathbf{N}$, $\langle\langle \mathbf{i} \bullet \mathbf{j} \rangle\rangle = \langle\langle f(\mathbf{i}) * f(\mathbf{j}) \rangle\rangle$ entonces, la extensión lineal de f es un isomorfismo de espacios con producto bilinear.

Esto nos da inmediatamente que existe “un solo” espacio simpléctico.

7.2

Cualesquiera dos espacios simplécticos de la misma dimensión finita son isomorfos.

Prueba. Sean $(\mathcal{E}, \langle\langle \bullet \bullet \rangle\rangle)$ y $(\mathcal{F}, \langle\langle * * \rangle\rangle)$ dos espacios simplécticos de la misma dimensión finita. Entonces, $\mathcal{E} = P_1 \oplus \dots \oplus P_n$ y $\mathcal{F} = Q_1 \oplus \dots \oplus Q_m$ donde los P_i y los Q_j son planos simplécticos (todos de dimensión 2). Luego $2n = 2m = \dim \mathcal{E} = \dim \mathcal{F}$ y por lo tanto $n = m$. Cada plano simpléctico tiene una base $\{\mathbf{x}, \mathbf{y}\}$ de dos vectores isotrópicos tales que $\langle\langle \mathbf{x} \bullet \mathbf{y} \rangle\rangle = -\langle\langle \mathbf{y} \bullet \mathbf{x} \rangle\rangle = 1$. Sean $\{\mathbf{x}_i, \mathbf{y}_i\} \subseteq P_i$ y $\{\mathbf{x}'_i, \mathbf{y}'_i\} \subseteq Q_i$ para $i \in \{1, \dots, n\}$ las bases de estos planos simplécticos. Los conjuntos $\mathbf{N} = \bigcup_{i=1}^n \{\mathbf{x}_i, \mathbf{y}_i\}$ y $\mathbf{M} = \bigcup_{i=1}^n \{\mathbf{x}'_i, \mathbf{y}'_i\}$ son bases de \mathcal{E} y \mathcal{F} respectivamente. Como la sumas son perpendiculares entonces, para $i \neq j$ tenemos que

$$\begin{aligned} \langle\langle \mathbf{x}_i \bullet \mathbf{x}_j \rangle\rangle &= \langle\langle \mathbf{x}_i \bullet \mathbf{y}_j \rangle\rangle = \langle\langle \mathbf{y}_i \bullet \mathbf{x}_j \rangle\rangle = \langle\langle \mathbf{y}_i \bullet \mathbf{y}_j \rangle\rangle = 0 \\ \langle\langle \mathbf{x}'_i * \mathbf{x}'_j \rangle\rangle &= \langle\langle \mathbf{x}'_i * \mathbf{y}'_j \rangle\rangle = \langle\langle \mathbf{y}'_i * \mathbf{x}'_j \rangle\rangle = \langle\langle \mathbf{y}'_i * \mathbf{y}'_j \rangle\rangle = 0 \end{aligned}$$

y por lo tanto, la función $f : \mathbf{N} \ni \mathbf{a} \rightarrow \mathbf{a}' \in \mathbf{M}$ es una biyección entre las bases que preserva el producto bilinear. ■



Los espacios simplécticos a pesar de (o tal vez, debido a) su simplicidad tienen amplias aplicaciones en la física (óptica geométrica, mecánica clásica, termodinámica, cuantización geométrica, etc) y en la matemática aplicada (teoría de control). En matemáticas (como ya vimos) ellos surgen naturalmente y son importantes para muchos problemas del análisis y el álgebra.

Equivalencia cuadrática

La clasificación de los espacios ortogonales es mucho más compleja que la de los espacios simplécticos.

Diremos que un escalar no nulo ω es un **cuadrado** si existe β tal que $\omega = \beta^2$. Diremos que dos escalares no nulos α y γ son **cuadráticamente equivalentes** si existe otro escalar β tal que $\alpha = \beta^2 \gamma$. En otras palabras, si $\alpha \gamma^{-1}$ es un cuadrado.

Clasificación de los espacios ortogonales en dimensión 1

7.3

Sean $\langle\langle \bullet \bullet \rangle\rangle$ y $\langle\langle * \rangle\rangle$ dos productos bilineales definidos en un espacio vectorial \mathcal{E} de dimensión 1. Sea \mathbf{x} una base de \mathcal{E} . Denotemos $\alpha \stackrel{\text{def}}{=} \langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle \neq 0$ y $\gamma \stackrel{\text{def}}{=} \langle\langle \mathbf{x} * \mathbf{x} \rangle\rangle \neq 0$. Entonces, los productos $\langle\langle \bullet \bullet \rangle\rangle$ y $\langle\langle * \rangle\rangle$ son isomorfos si y solo si α y γ son cuadráticamente equivalentes.

Prueba. Si α y γ son cuadráticamente equivalentes entonces para cierto β tenemos que $\langle\langle \mathbf{x} * \mathbf{x} \rangle\rangle = \beta^2 \alpha$. La homotecia $f : \mathbf{x} \mapsto \beta \mathbf{x}$ cumple que

$$\langle\langle \mathbf{x} * \mathbf{x} \rangle\rangle = \beta^2 \alpha = \beta^2 \langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle = \langle\langle \beta \mathbf{x} \bullet \beta \mathbf{x} \rangle\rangle = \langle\langle f(\mathbf{x}) \bullet f(\mathbf{x}) \rangle\rangle$$

lo que muestra que $\langle\langle \bullet \bullet \rangle\rangle$ y $\langle\langle * \rangle\rangle$ son isomorfos.

Recíprocamente, supongamos que f es un operador tal que $\langle\langle \mathbf{x} * \mathbf{x} \rangle\rangle = \langle\langle f(\mathbf{x}) \bullet f(\mathbf{x}) \rangle\rangle$. Como todo operador en dimensión 1 es una homotecia, existe β tal que $f(\mathbf{x}) = \beta \mathbf{x}$ y por lo tanto

$$\gamma \stackrel{\text{def}}{=} \langle\langle \mathbf{x} * \mathbf{x} \rangle\rangle = \langle\langle f(\mathbf{x}) \bullet f(\mathbf{x}) \rangle\rangle = \langle\langle \beta \mathbf{x} \bullet \beta \mathbf{x} \rangle\rangle = \beta^2 \langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle = \beta^2 \alpha$$

lo que demuestra que α y γ son cuadráticamente equivalentes. ■

La equivalencia cuadrática depende mucho del campo. Por ejemplo en \mathbb{C} todo número es un cuadrado y por lo tanto dos complejos cualesquiera son cuadráticamente equivalentes. En \mathbb{R} los cuadrados son los números positivos y por lo tanto hay dos clases de equivalencia cuadrática: los positivos y los negativos. En \mathbb{Q} los cuadrados son los productos y cocientes de cuadrados de números primos y por lo tanto hay infinitas clases de equivalencia cuadrática, una por cada racional de la forma $p^{\pm 1} q^{\pm 1} \dots r^{\pm 1}$ donde p, q, \dots, r son primos todos diferentes.

Clasificación de espacios ortogonales

Sea $(\mathcal{E}, \langle\langle \bullet \bullet \rangle\rangle)$ un espacio ortogonal sobre \mathbb{K} y \mathbf{N} una de sus bases ortogonales. A la \mathbf{N} -ada $\alpha_{\mathbf{N}} : \mathbf{N} \ni \mathbf{i} \mapsto \langle\langle \mathbf{i} \bullet \mathbf{i} \rangle\rangle \in \mathbb{K}$ la llamaremos la **huella** del espacio ortogonal en la base \mathbf{N} . Como la base es ortogonal sabemos que $\forall \mathbf{i}, \mathbf{j} \in \mathbf{N}$ se cumple que $(\mathbf{i} \neq \mathbf{j}) \Rightarrow (\langle\langle \mathbf{i} \bullet \mathbf{j} \rangle\rangle = 0)$ y por lo tanto la huella define completamente el producto bilineal. La huella no es otra cosa que la diagonal de la matriz del producto bilineal en la base \mathbf{N} .

Sean $\alpha_{\mathbf{N}} \in \mathbb{K}^{\mathbf{N}}$ y $\beta_{\mathbf{M}} \in \mathbb{K}^{\mathbf{M}}$. Diremos que $\alpha_{\mathbf{N}}$ y $\beta_{\mathbf{M}}$ son **cuadráticamente equivalentes** si existe otra \mathbf{M} -ada $\gamma_{\mathbf{M}} \in \mathbb{K}^{\mathbf{M}}$ y una biyección $\phi : \mathbf{M} \rightarrow \mathbf{N}$ tal que $\forall \mathbf{j} \in \mathbf{M}$ se cumple que $\alpha_{\phi(\mathbf{j})} = \gamma_{\mathbf{j}}^2 \beta_{\mathbf{j}}$.

7.4

Sean $(\mathcal{E}, \langle\langle \bullet \bullet \rangle\rangle)$ y $(\mathcal{F}, \langle\langle * \rangle\rangle)$ dos espacios ortogonales sobre \mathbb{K} . Sean \mathbf{N} y \mathbf{M} bases ortogonales de \mathcal{E} y \mathcal{F} respectivamente. Si la huella de \mathcal{E} en la base \mathbf{N} es cuadráticamente equivalente a la huella de \mathcal{F} en la base \mathbf{M} entonces los espacios son isomorfos.

Prueba. Sean $\alpha_{\mathbf{N}}$ y $\beta_{\mathbf{M}}$ las dos huellas mencionadas. Sean $\gamma_{\mathbf{M}} \in \mathbb{K}^{\mathbf{M}}$ y una biyección

$\phi : M \rightarrow N$ tal que $\alpha_{\phi(j)} = \gamma_j^2 \beta_j$. Sea $f : \mathfrak{F} \rightarrow \mathfrak{E}$ el operador lineal no singular tal que $f(j) = \gamma_j^{-1} \phi(j)$. Tenemos $\forall j \in M$

$$\langle\langle j \star j \rangle\rangle = \beta_j = \gamma_j^{-2} \alpha_{\phi(j)} = \langle\langle \gamma_j^{-1} \phi(j) \bullet \gamma_j^{-1} \phi(j) \rangle\rangle = \langle\langle f(j) \bullet f(j) \rangle\rangle$$

y por lo tanto f es un isomorfismo de espacios ortogonales. ■

Para ver que el recíproco de este resultado NO es cierto consideremos el producto bilineal en \mathbb{Q}^2 definido por $\langle\langle (x, y) \star (x', y') \rangle\rangle = 5xx' + 5yy'$. Sea además $\langle\langle (x, y) \bullet (x', y') \rangle\rangle = xx' + yy'$ el producto escalar canónico. A pesar que la huella (5, 5) no es cuadráticamente equivalente en \mathbb{Q}^2 a (1, 1) tenemos que el operador lineal definido por $f(x, y) = (x + 2y, y - 2x)$ cumple que

$$\begin{aligned} \langle\langle f(x, y) \bullet f(x', y') \rangle\rangle &= (x + 2y)(x' + 2y') + (y - 2x)(y' - 2x') = \\ &= 5xx' + 5yy' = \langle\langle (x, y) \star (x', y') \rangle\rangle \end{aligned}$$

por lo que \mathbb{Q}^2 on el producto $\langle\langle \star \rangle\rangle$ es isomorfo a \mathbb{Q}^2 con el producto escalar canónico.

La clasificación de los espacios ortogonales sobre \mathbb{Q} y muchos otros campos es un problema complicado. Por esto nos conformaremos con estudiar los casos más sencillos.

Si en el campo hay una sola clase de equivalencia cuadrática por ejemplo \mathbb{C} entonces 7.4 nos da que solo puede haber salvo isomorfismos un solo producto ortogonal y podemos pensar que este es el producto escalar canónico en cierta base ortogonal.

Si en el campo \mathbb{K} hay exactamente dos clases de equivalencia cuadrática entonces podemos asumir que las coordenadas de las huellas son iguales a $\mathbf{1}$ o a un elemento de \mathbb{K} fijo ρ que no sea un cuadrado. Este tipo de huellas está está predeterminada por la cantidad de $\mathbf{1}$ en ellas ya que las demás forzosamente son iguales a ρ . Esta cantidad de $\mathbf{1}$ puede ser desde cero hasta la dimensión del espacio por lo que obtenemos.

7.5

En un espacio \mathfrak{E} sobre un campo con dos clases de equivalencia cuadrática se pueden definir a lo más $1 + \dim \mathfrak{E}$ productos ortogonales diferentes.

El lector debe observar el “a lo más” ya que es muy posible que algunos de estos productos sean isomorfos. En lo que sigue inmediatamente veremos que sobre \mathbb{R} los $1 + \dim \mathfrak{E}$ productos son efectivamente diferentes.

Ley de inercia de Silvestre

Un **ordenamiento** de un campo \mathbb{K} es un subconjunto $P \subseteq \mathbb{K} \setminus \{0\}$ cerrado para la suma y el producto y tal que $P \cup -P = \mathbb{K} \setminus \{0\}$. A los elementos de P se les llama **positivos** y a los de $-P$ **negativos**. Observase que P y $-P$ son necesariamente disjuntos ya que si $x, -x \in P$ entonces $x + (-x) \in P$ lo que contradice que $0 \notin P$. Escribiremos $x > y$ si $x - y \in P$.

El producto de dos negativos es positivo ya que si $x, y \in P$ entonces $(-x)(-y) = xy \in P$. En particular, cualquier cuadrado es positivo y como $1^2 = 1$ tenemos que $1 > 0$. De aquí, $1 + \dots + 1 > 0$ por lo que un campo ordenado tiene necesariamente característica cero, o sea, contiene a \mathbb{Q} . Cualquier campo \mathbb{K} tal que $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{R}$ se

puede ordenar pero estos no son los únicos.



Una bonita y útil caracterización de los campos que se pueden ordenar es el Teorema de Artin - Schreier: *Un campo se puede ordenar si y solo si -1 no es suma de cuadrados.*

Se dice que un producto bilineal ortogonal definido en un espacio vectorial sobre un campo ordenado es **definido positivo** si para cualquier vector $\mathbf{x} \neq \mathbf{0}$ se tiene que $\langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle > 0$. También diremos que el espacio con producto bilineal es **definido positivo**. Análogamente se definen que un producto bilineal es **definido negativo** si para cualquier vector $\mathbf{x} \neq \mathbf{0}$ se tiene que $\langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle < 0$.

7.6

La suma perpendicular de espacios definidos positivos es definida positiva.

Prueba. Si $(\mathbf{x}, \mathbf{y}) \in \mathfrak{E} \oplus \mathfrak{F}$ entonces, $\langle\langle (\mathbf{x}, \mathbf{y}) \bullet (\mathbf{x}, \mathbf{y}) \rangle\rangle = \langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle + \langle\langle \mathbf{y} \bullet \mathbf{y} \rangle\rangle > 0$.

■

Evidentemente, hay un resultado similar para los espacios definidos negativos. De aquí, vemos que un producto es definido positivo (negativo) si y solo si existe una base ortogonal tal que $\langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle > (<) 0$ para cualquier vector en la base.

Ley de inercia de Silvestre

7.7

Todo espacio ortogonal sobre un campo ordenado es suma perpendicular de un subespacio definido positivo con otro definido negativo. Si el espacio es finito dimensional entonces, las dimensiones de estos dos subespacios están definidas a priori por el producto bilineal.

Prueba. Sea \mathbf{A} una base ortogonal y

$$\mathfrak{A}^+ \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbf{A} \mid \langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle > 0\} \quad \mathfrak{A}^- \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbf{A} \mid \langle\langle \mathbf{x} \bullet \mathbf{x} \rangle\rangle < 0\}$$

Los subespacios $\mathfrak{E}^+ = \langle \mathfrak{A}^+ \rangle$ y $\mathfrak{E}^- = \langle \mathfrak{A}^- \rangle$ son perpendiculares y definidos positivo y negativo respectivamente. Luego $\mathfrak{E} = \mathfrak{E}^+ \oplus \mathfrak{E}^-$ es la descomposición buscada.

Si \mathfrak{F} es un subespacio definido positivo arbitrario entonces $\mathfrak{F} \cap \mathfrak{E}^- = \{\mathbf{0}\}$. Por la igualdad modular tenemos que

$$\dim \mathfrak{F} + \dim \mathfrak{E}^- = \dim (\mathfrak{F} + \mathfrak{E}^-) \leq \dim \mathfrak{E}$$

y por lo tanto

$$\dim \mathfrak{F} \leq \dim \mathfrak{E} - \dim \mathfrak{E}^- = \dim \mathfrak{E}^+$$

Esto quiere decir que $\dim \mathfrak{E}^+$ se puede caracterizar como la dimensión más grande posible de un subespacio definido positivo y por lo tanto está definida a priori por el producto bilineal. ■

En \mathbb{R}^n la ley de inercia de Silvestre tiene como consecuencia que los $n+1$ productos bilineales posibles son diferentes ya que las dimensiones de los subespacios definidos positivos maximales son todas diferentes.

Equivalencia cuadrática en campos finitos

7.8

En cualquier campo finito hay tantas clases de equivalencia cuadrática como raíces cuadradas de la unidad.

Prueba. Recalquemos (véase la solución al ejercicio ?? el Teorema de Lagrange para grupos finitos: si F es un subgrupo de G entonces, las clases laterales $xF = \{xy \mid y \in F\}$ forman una partición del grupo y todas tienen el mismo número de elementos. En particular $|F|$ es un divisor de $|G|$ y el número de clases laterales es igual a $|G| \div |F|$. Al conjunto de todas estas clases laterales lo denotaremos por G/F .

En nuestro caso G es el grupo multiplicativo del campo y F es el subgrupo de todos los cuadrados no nulos. El lector deberá observar que una clase de equivalencia cuadrática no es más que xF para cierto $x \in G$. Luego, $|G/F| = |G| \div |F|$ es el número de clases de equivalencia cuadrática.

Sea $H = \{x \in G \mid x^2 = 1\}$ el conjunto de raíces cuadradas de la unidad. Obsérvese que H es otro subgrupo de G y que la función

$$f: G/H \ni xH \mapsto x^2 \in F$$

es evidentemente sobreyectiva. Para ver que f es inyectiva supongamos que $x^2 = y^2$ entonces, $x^{-2}y^2 = 1$ y por lo tanto $x^{-1}y \in H$. Luego

$$(x^{-1}yH = H) \Rightarrow (yH = xH).$$

Como f es una biyección, por el Teorema de Lagrange obtenemos que $|G| \div |H| = |F|$ y por lo tanto $|G| \div |F| = |H|$. ■

Como en un campo cualquiera el número de raíces del polinomio $x^2 - 1$ es ≤ 2 y en un campo de característica $\neq 2$ los números $+1$ y -1 son dos raíces cuadradas de la unidad, obtenemos que, en un campo de finito de característica $\neq 2$ hay exactamente dos clases de equivalencia cuadrática: aquellos que son cuadrados y aquellos que no lo son. Para los campos de característica 2 tenemos el siguiente:

7.9

En un campo finito de característica 2 todo elemento es un cuadrado.

Prueba. En cualquier campo de característica 2 tenemos que

$$(x - 1)^2 = x^2 - 2x + 1 = x^2 + 1 = x^2 - 1$$

y por lo tanto las raíces cuadradas de 1 son las raíces del polinomio $(x - 1)^2$ el cual tiene como única raíz a 1 . Aplicando 7.8 terminamos la prueba. ■

Este resultado nos dice en un espacio vectorial sobre un campo finito de característica 2 , dos huellas cualesquiera son cuadráticamente equivalentes y por lo tanto hay un solo producto ortogonal.

Campos finitos de característica diferente de 2

Sabemos que si la característica es diferente de 2 entonces, en el campo hay exactamente dos clases de equivalencia cuadrática.

En lo que sigue \mathbb{K} es un campo finito de característica diferente de 2 y ρ es un elemento de \mathbb{K} que no es un cuadrado.



Es un error que pensar que podemos tomar $\rho = -1$. Hay campos finitos de característica diferente de 2 en los cuales -1 es un cuadrado, por ejemplo, en \mathbb{Z}_5 tenemos $2^2 = 4 = -1$.

7.10

Los productos ortogonales en \mathbb{K}^2 con huellas $\{1, 1\}$ y $\{\rho, \rho\}$ son isomorfos.

Prueba. Sea $\{\mathbf{a}, \mathbf{b}\}$ una base de \mathbb{K}^2 y $\langle\langle \bullet \bullet \rangle\rangle$ el producto ortogonal para el cual

$$\begin{aligned}\langle\langle \mathbf{a} \bullet \mathbf{a} \rangle\rangle &= \langle\langle \mathbf{b} \bullet \mathbf{b} \rangle\rangle = \rho \\ \langle\langle \mathbf{a} \bullet \mathbf{b} \rangle\rangle &= \langle\langle \mathbf{b} \bullet \mathbf{a} \rangle\rangle = 0\end{aligned}$$

Sea $A \stackrel{\text{def}}{=} \{\alpha^2 \rho \mid \alpha \in \mathbb{K}\}$. El conjunto A esta formado por el cero y por todos los elementos no nulos de \mathbb{K} cuadráticamente equivalentes a ρ . Como \mathbb{K} tiene exactamente dos clases de equivalencia cuadrática, tenemos

$$|A| = \frac{|\mathbb{K}| - 1}{2} + 1 = \frac{|\mathbb{K}| + 1}{2}$$

Como la función $\mathbb{K} \ni x \mapsto 1 - x \in \mathbb{K}$ es una biyección entonces $|1 - A| = |A|$ y por lo tanto

$$|(1 - A) \cap A| = |1 - A| + |A| - |(1 - A) \cup A| \leq 2|A| - |\mathbb{K}| = 1.$$

los conjuntos $|1 - A|$ y $|A|$ tienen intersección no vacía. Esto quiere decir que existen dos elementos del campo α y β tales que $\alpha^2 \rho = 1 - \beta^2 \rho$ o lo que es lo mismo $\alpha^2 \rho + \beta^2 \rho = 1$. Obsérvese que como ρ no es un cuadrado entonces, ambos α y β son diferentes de cero.

Sea $\mathbf{c} \stackrel{\text{def}}{=} \alpha \mathbf{a} + \beta \mathbf{b}$. El conjunto $\{\mathbf{c}, \mathbf{b}\}$ una base de \mathbb{K}^2 ya que $\alpha \neq 0$ y tenemos que

$$\begin{aligned}\langle\langle \mathbf{c} \bullet \mathbf{c} \rangle\rangle &= \alpha^2 \rho + \beta^2 \rho = 1 & \langle\langle \mathbf{b} \bullet \mathbf{b} \rangle\rangle &= \rho \\ \langle\langle \mathbf{c} \bullet \mathbf{b} \rangle\rangle &= \langle\langle \mathbf{b} \bullet \mathbf{c} \rangle\rangle = \beta \rho\end{aligned}$$

Lo malo de esta base es que no es ortogonal. Definamos $\mathbf{d} \stackrel{\text{def}}{=} \mathbf{b} - \beta \rho \mathbf{c}$. El conjunto $\{\mathbf{c}, \mathbf{d}\}$ una base de \mathbb{K}^2 y ahora tenemos que

$$\begin{aligned}\langle\langle \mathbf{c} \bullet \mathbf{c} \rangle\rangle &= 1 & \langle\langle \mathbf{d} \bullet \mathbf{d} \rangle\rangle &= \rho(1 - \beta^2 \rho) = \alpha^2 \rho^2 \\ \langle\langle \mathbf{c} \bullet \mathbf{d} \rangle\rangle &= \langle\langle \mathbf{d} \bullet \mathbf{c} \rangle\rangle = 0\end{aligned}$$

Como $\langle\langle \mathbf{d} \bullet \mathbf{d} \rangle\rangle$ es un cuadrado entonces, podemos normalizar definiendo $\mathbf{e} = \mathbf{d}/\alpha \rho$. En la base ortogonal $\{\mathbf{c}, \mathbf{e}\}$ la huella del producto bilineal es $\{1, 1\}$. ■

El resultado anterior nos permite afirmar las posible huellas para un producto bilineal sobre \mathbb{K} son $\{\rho, 1, \dots, 1\}$ y $\{1, 1, \dots, 1\}$. Solo falta probar que estos dos productos son diferentes. Para esta prueba lo más sencillo es usar el Teorema de Witt sobre

isomorfismos entre espacios con producto bilineal sobre cualquier campo.

Teorema de cancelación de Witt

7.11

Sea \mathcal{E} un espacio ortogonal. Sean \mathfrak{F} y \mathfrak{G} dos subespacios de \mathcal{E} . Si \mathfrak{F} es isomorfo a \mathfrak{G} entonces, \mathfrak{F}^\perp es isomorfo a \mathfrak{G}^\perp .

La prueba de este resultado nos llevaría lejos en el estudio del grupo ortogonal y esto sale fuera de los objetivos de este libro.

Ejercicio 4 Pruebe usando el Teorema de Witt que los productos con huellas $\{1, \rho\}$ y $\{1, 1\}$ no son isomorfos. [9]

Ejercicio 5 Pruebe lo mismo, pero sin usar el Teorema de Witt. [9]

Ejercicio 4 (Sección 7.5 página 8) Supongamos que son isomorfos. Sean $\{\mathbf{a}, \mathbf{b}\}$ y $\{\mathbf{c}, \mathbf{d}\}$ bases ortogonales en las cuales el producto bilineal tiene huellas $\{1, 1\}$ y $\{1, \rho\}$ respectivamente. Tenemos que los subespacios $\langle \mathbf{a} \rangle$ y $\langle \mathbf{c} \rangle$ son isomorfos pero los subespacios $\langle \mathbf{a} \rangle^\perp = \langle \mathbf{b} \rangle$ y $\langle \mathbf{c} \rangle^\perp = \langle \mathbf{d} \rangle$ por Clasificación de los espacios ortogonales en dimensión 1 (7.3) no lo son. Esto contradice el Teorema de Witt.

Ejercicio 5 (Sección 7.5 página 8) Sean $\{\mathbf{a}, \mathbf{b}\}$ y $\{\mathbf{c}, \mathbf{d}\}$ bases ortogonales en las cuales el producto bilineal tiene huellas $\{1, 1\}$ y $\{1, \rho\}$ respectivamente. Sean α, β, γ y ω escalares tales que $\mathbf{c} = \alpha\mathbf{a} + \beta\mathbf{b}$ y $\mathbf{d} = \gamma\mathbf{a} + \omega\mathbf{b}$. Tenemos

$$\begin{aligned} \langle\langle \mathbf{c} \bullet \mathbf{d} \rangle\rangle &= \alpha\gamma + \beta\omega = 0 \\ \langle\langle \mathbf{c} \bullet \mathbf{c} \rangle\rangle &= \alpha^2 + \beta^2 = 1 \\ \langle\langle \mathbf{d} \bullet \mathbf{d} \rangle\rangle &= \gamma^2 + \omega^2 = \rho \end{aligned}$$

De $\alpha = 0$ obtenemos que $\beta = 1$, $\omega = 0$ y $\gamma^2 = \rho$ lo que contradice que ρ no es un cuadrado. Luego, podemos suponer que $\alpha \neq 0$. Multiplicando la tercera igualdad por α^2 y usando las dos primeras obtenemos que

$$\alpha^2\rho = \alpha^2\gamma^2 + \alpha^2\omega^2 = \beta^2\omega^2 + \alpha^2\omega^2 = (\beta^2 + \alpha^2)\omega^2 = \omega^2$$

y de aquí obtenemos que ρ es el cuadrado de ω/α . Esto contradice que ρ no es un cuadrado.

Guía *de estudio*

1. Definición de productos definidos positivos.
2. Ley de inercia de Silvestre

