© Revista de Matemática: Teoría y Aplicaciones 2022 **29**(2) : 159–176
cimpa – ucr issn: 1409-2433 (Print), 2215-3373 (Online)
doi: https://doi.org/10.15517/rmta.v29i2.49254

GRUPOS ORTOGONALES SOBRE CUERPOS DE CARACTERÍSTICA POSITIVA

ORTHOGONAL GROUPS OVER FIELDS OF POSITIVE CHARACTERISTIC

Robin Zhang*

Received: 26/Nov/2021; Revised: 29/Apr/2022; Accepted: 30/May/2022

---

*Columbia University, Department of Mathematics, New York, United States of America. E-Mail: rzhang@math.columbia.edu

Resumen

Esta exposición examina la teoría de los grupos ortogonales y sus subgrupos sobre cuerpos de característica positiva, que recientemente se han utilizado como una herramienta importante en el estudio de las formas automórficas y la funcionalidad de Langlands. Presentamos la clasificación de grupos ortogonales sobre un cuerpo finito F utilizando la teoría de formas bilineales y formas cuadráticas en característica positiva. Usando el determinante y la norma del espinor cuando la característica de F es impar y usando la invariante de Dickson cuando la característica de F es par, también encontramos subgrupos especiales del grupo ortogonal.

Palabras clave: grupo ortogonal, característica positiva, forma bilineal, forma cuadrática, invariante de Arf, invariante de Dickson, núcleo espinorial

Abstract

This exposition examines the theory of orthogonal groups and their subgroups over fields of positive characteristic, which has recently been used as an important tool in the study of automorphic forms and Langlands functionality. We present the classification of orthogonal groups over a finite field using the theory of bilinear forms and quadratic forms in positive characteristic. Using the determinant and spinor norm when the characteristic of F is odd and using the Dickson invariant when the characteristic of F is even, we also look at special subgroups of the orthogonal group.

Keywords: orthogonal group, positive characteristic, bilinear form, quadratic form, Arf invariant, Dickson invariant, spinorial kernel

Mathematics Subject Classification: 11E04, 11E57, 11E88, 20D05, 11-02, 20-02.

1 Introducción

La teoría de los grupos ortogonales sobre los números complejos es muy conocida. La teoría de los grupos ortogonales sobre cuerpos de característica positiva no es tan conocida, incluso para cuerpos finitos. Estos grupos siguen siendo importantes en el estudio de la teoría de representaciónes, con importantes aplicaciones recientes en la teoría de formas automórficas y la functorialidad de Langlands (e.g. [10, 19, 14, 15, 5]).

Para un espacio vectorial V sobre un cuerpo general F, sea Q una forma cuadrática Q sobre V. En general, el grupo ortogonal de la forma Q es el grupo de aplicaciones lineales invertibles que conservan Q. Cuando la característica de

F es impar, podemos reemplazar la forma cuadrática Q con una forma bilineal simétrica no degenerada f sobre V.

Primero, desarrollamos la teoría de las formas bilineales para clasificar los grupos y subgrupos ortogonales sobre un cuerpo de característica impar. Luego pasamos a la teoría de las formas cuadráticas para clasificar los grupos y subgrupos ortogonales sobre un cuerpo de característica par. Sobre cuerpos finitos, gran parte del trabajo sobre estos grupos finitos de tipo Lie fue realizado a principios y mediados del siglo XX por Dickson, Chevalley, Dieudonné y muchos otros. Dependiendo de si la dimensión de V es par o impar, hay una o dos clases de equivalencia de tales formas sobre V. Entonces podemos clasificar los tipos de grupos ortogonales que existen sobre cuerpos de característica positiva. Esta clasificación está contenida esencialmente en las referencias de Suzuki [20, Sección 3.5] y Wilson [22, Capítulo 3]. Uno de los principales objetivos de este artículo expositivo es recopilar estos resultados en el siguiente teorema para beneficio del lector.

Teorema 1.1 (Clasificación de grupos ortogonales sobre un cuerpo finito)**.** *Sean F un cuerpo finito y n número entero al menos 2. Los grupos ortogonales sobre F son los siguientes:*

	n impar	*n par*
$\mathrm{car}(F)$ *impar*	$\mathrm{O}(n)$	$\mathrm{O}^{\pm}(n)$
$\mathrm{car}(F)$ *par*	$\mathrm{Sp}(n-1)$	$\mathrm{O}^{\pm}(n)$

Separamos los casos del Teorema 1.1 por característica del cuerpo F. Repasamos la teoría de formas bilineales en la Sección 2.1 y describimos los grupos ortogonales sobre cuerpos finitos de características impares en Sección 2.2. La fila superior del Teorema 1.1 se prueba en Proposición 2.11. De manera similar para cuerpos de característica par, repasamos la teoría de formas cuadráticas en Sección 3.1 y describimos los grupos ortogonales sobre cuerpos finitos de características pares en Sección 3.2. La fila inferior del Teorema 1.1 se prueba en Proposición 3.14.

También encontramos los subgrupos especiales de los grupos ortogonales. Cuando F es finito y la característica de F es impar, utilizaremos la norma determinante y la norma espinorial para definir el subgrupo ortogonal especial y el núcleo espinorial en Sección 4.1. Pero cuando la característica de F es par, el determinante es inútil y no tenemos la norma espinor. En cambio, utilizaremos la invariante de Dickson para definir el subgrupo ortogonal especial y el núcleo espinorial, los cuales coinciden en este caso, en Sección 4.2.

Algunas de las definiciones y resultados son válidos sobre cuerpos de característica 0. Cuando nos enfocamos en cuerpos finitos, muchos de los resultados también se generalizan a cuerpos infinitos. Sin embargo, los valores numéricos y las estructuras de los grupos ortogonales sobre cuerpos infinitos dependen de las propiedades del cuerpo, así que omitimos esas discusiones. Para el resto del artículo, F es un cuerpo de característica $\operatorname{car}(F) = p > 0$ y V es un espacio vectorial de dimensión $n < \infty$ sobre F. Damos pruebas para comodidad del lector, particularmente cuando usamos ligeras modificaciones de las referencias citadas.

2 Clasificación de grupos ortogonales para característica impar

2.1 Formas bilineales

Primero, recordamos algunos hechos sobre las formas bilineales.

Definición 2.1. *Una función $f : V \times V \to F$ es* una forma bilineal *si y solo si para todos $u, v, w \in V$ y $\lambda \in F$,*

$$f(\lambda u + v, w) = \lambda f(u, w) + f(v, w),$$
$$f(u, \lambda v + w) = \lambda f(u, v) + f(u, w).$$

Definición 2.2. *Sea $f : V \times V \to F$ una forma bilineal. Definimos* el radical *(*izquierdo*) de f,*

$$\operatorname{rad}(f) := \{v \in V \mid f(u, v) = 0, \quad \forall u \in V\}.$$

Además definimos:

- *f es* no singular *cuando* $\operatorname{rad}(f) = 0$.
- *f es* simétrica *cuando $f(u, v) = f(v, u)$ para todos $u, v \in V$.*
- *f es* anti-simétrica *cuando $f(u, v) = -f(v, u)$ para todos $u, v \in V$.*
- *f es* alternada *cuando $f(v, v) = 0$ para todo $v \in V$.*

Definición 2.3. *Una forma bilineal que es alternada y no singular se llama* una forma simpléctica*. Un espacio vectorial junto con una forma simpléctica se llama* un espacio vectorial simpléctico.

Observación 2.4 (cf. [7, Sección I.8], [20, Sección 3.5.6], [22, Sección 3.4.4])**.** *Un espacio vectorial simpléctico tiene dimensión par y una base $\{e_1, \dots e_{2m}\}$ tal que*

$$f(e_i, e_{i+m}) = -f(e_{i+m}, e_i) = 1,$$
$$f(e_i, e_j) = 0 \text{ si } i \neq j \pm m.$$

Los siguientes resultados son conocidos.

Observación 2.5 ([21, Capítulo 7], [22, Sección 3.4.1])**.** *Sea f una forma bilineal.*

(a) Si f es alternada, entonces f es anti-simétrica.

(b) Si f es anti-simétrica y $p \neq 2$, entonces f es alternada.

Demostración.

(a) Tenemos que

$$0 = f(u+v, u+v) = f(u, u)+f(u, v)+f(v, u)+f(v, v) = f(u, v)+f(v, u),$$

entonces $f(u, v) = -f(v, u)$.

(b) Tenemos que $f(v, v) = -f(v, v)$, entonces $2f(v, v) = 0$. Si $p \neq 2$, entonces $f(v, v) = 0$.

■

2.2 Los grupos ortogonales para F finito

Sea F un cuerpo finito de característica impar. Las dos primeras definiciones también son válidas para otros cuerpos, pero nos centramos en este caso. Describimos los grupos ortogonales sobre tal cuerpo F y demostramos la fila superior de Teorema 1.1.

Definición 2.6. *Sea $f : V \times V \to F$ una forma bilineal simétrica no singular. Definimos* el grupo ortogonal*,*

$$\mathrm{O}(V, f) := \{g : V \to V \textit{ lineal} \mid f\,(g(u), g(v)) = f(u, v), \quad \forall u, v \in V\}\,.$$

Definición 2.7. *Sea $f : V \times V \to F$ una forma simpléctica. Definimos* el grupo simpléctico*,*

$$\mathrm{Sp}(V, f) := \{g : V \to V \textit{ lineal} \mid f\,(g(u), g(v)) = f(u, v) \quad \forall u, v \in V\}\,.$$

Observación 2.8. *Podemos simplemente escribir* $\mathrm{Sp}(n) = \mathrm{Sp}(V, f)$ *porque existe una forma simpléctica canónica para $V \cong F^n$.*

Comenzamos con un hecho sobre las formas bilineales simÃ©tricas no singular cuando F es un cuerpo finito $\mathbb{F}_q$ de característica impar.

Lema 2.9 (cf. [22, Sección 3.4.6])**.** *Si F es un cuerpo finito de característica impar, entonces hay exactemente dos clases de equivalencia de formas bilineales simétricas no singulares (bajo la acción) de $\mathrm{GL}_n(F)$).*

Demostración. Sea f una forma bilineal simétrica sobre V. Hay vectores $u, v \in V$ tales que $f(u, v) \neq 0$, entonces hay un vector $x \in V$ ($x = u$, $x = v$, o $x = u + v$) tal que $f(x, x) \neq 0$. Escogemos $\alpha \in F$ no cuadrado. Entonces

1. si $f(x, x) = \lambda^2$ es un número cuadrado, $f(x', x') = 1$ para $x' := \lambda^{-1}x$;
2. si $f(x, x) = \lambda$ no es un número cuadrado, $f(x', x') = \alpha$ para $x' := \sqrt{\frac{\alpha}{\lambda}}x$ (porque ambos elementos no son residuos cuadráticos).

Restringimos f a $(x')^{\perp}$, continuamos hasta encontrar una base perpendicular $\{e_1, \ldots, e_n\}$ tal que $f(e_i, e_i) \in \{0, 1, \alpha\}$.

Podemos reducir el número de i tal que $f(e_i, e_i) = \alpha$ en dos: si hay e_i y e_j tales que $f(e_i, e_i) = f(e_j, e_j) = \alpha$ y $f(e_i, e_j) = 0$, podemos elegir λ y μ tales que $\lambda^2 + \mu^2 = \frac{1}{\alpha}$ (no cuadrado). Entonces $e'_i := \lambda e_i + \mu e_j$ y $e'_j := \mu e_i + \lambda e_j$ son una base ortonormal para el espacio generado por e_i y e_j.

Por lo tanto, siempre podemos encontrar una base $\{e_1, \ldots e_n\}$ ortogonal tal que

1. $\{e_1, \ldots, e_n\}$ es ortonormal, o
2. $\{e_1, \ldots e_{n-1}\}$ es ortonormal y $f(e_n, e_n) = \alpha$.

Entonces hay dos clases de equivalencia. ∎

Lema 2.9 implica que hay hasta dos grupos ortogonales de dimensión fija sobre un cuerpo finito de característica impar. Cuando hay dos grupos ortogonales distintos, se distinguen por vectores isotrópicos.

Definición 2.10. *Un vector $v \in V \backslash \{0\}$ es* un vector isotrópico *para la forma bilineal $f : V \times V \to F$ si $f(v, v) = 0$. Un subespacio $W \subset V$ es* totalmente isotrópico *si $f(u, w) = 0$ para todos $u, w \in W$.*

Por ejemplo (cf. [22, Sección 3.4.6]), sean $n = 2$ y las dos formas diferentes f_1 y f_2 tal que existe una base ortogonal $\{x_0, x_1\}$ con

$$f_1(x_0, x_0) = 1,$$
$$f_1(x_1, x_1) = 1,$$
$$f_2(x_0, x_0) = 1,$$
$$f_2(x_1, x_1) = \alpha \notin (F^{\times})^2.$$

Si $-1 \in (F^{\times})^2$ (i.e. $|F| \equiv 1 \pmod 4$), entonces

$$f_1(x_0 + ix_1, x_0 + ix_1) = 0$$
$$f_2(x_0 + \lambda x_1, x_0 + \lambda x_1) = 1 + \lambda^2\alpha \neq 0.$$

Si $-1 \notin (F^{\times})^2$ (i.e. $|F| \equiv 3 \pmod 4$), entonces $-\alpha \in (F^{\times})^2$ y exista una λ tal que $-\alpha = \lambda^{-2}$, por lo que entonces

$$f_1(x_0 + ix_1, x_0 + ix_1) \neq 0$$
$$f_2(x_0 + \lambda x_1, x_0 + \lambda x_1) = 1 + \lambda^2\alpha = 0.$$

En ambos casos, exactamente una de las dos f_i tiene un vector isotrópico. Esta es una distinción geométrica que diferencia los dos grupos ortogonales.

Para n par en general, exactamente una de las dos f_i tiene un subespacio totalmente isotrópico de dimension $\frac{n}{2}$, mientras que el otra tiene un subespacio totalmente isotrópico de dimension $\frac{n}{2} - 1$. Escribimos $\mathrm{O}^+(n)$ para $\mathrm{O}(V, f)$ si existe un subespacio totalmente isotrópico de dimension $\frac{n}{2}$, y $\mathrm{O}^-(n)$ de lo contrario.

Para completar la prueba de la fila superior de Teorema 1.1, demostramos que tenemos exactamente uno o exactamente dos grupos ortogonales diferentes dependiendo de la paridad de la dimensión n.

Proposición 2.11 (cf. [20, Sección 3.5.8])**.**

1. *Si n es impar, entonces hay solo un grupo ortogonal (excepto por isomorfismo)* $\mathrm{O}(n)$

2. *Si n es par, entonces hay dos grupos (excepto por isomorfismo)* $\mathrm{O}^{\pm}(n)$

Demostración.

1. Sean f y f' dos formas bilineales simétricas no singulares. Escribimos $n = 2m + 1$. Usando un proceso similar al de la prueba de Lema 2.9, hay $\alpha, \beta \in F^{\times}$ y bases $\{e_1, \dots, e_{2m+1}\}, \{e'_1, \dots, e'_{2m+1}\} \subset V$ tales que

$$\begin{aligned}
f(e_{2i-1}, e_{2i}) &= 1 && \text{si } 1 \leq i \leq m \\
f(e_{2m+1}, e_{2m+1}) &= \alpha && \\
f(e_i, e_j) &= 0 && \text{para otros } (i, j), \\
f'(e'_{2i-1}, e'_{2i}) &= 1 && \text{si } 1 \leq i \leq m \\
f'(e'_{2m+1}, e'_{2m+1}) &= \beta && \\
f'(e'_i, e'_j) &= 0 && \text{para otros } (i, j).
\end{aligned}$$

Definimos $\sigma \in \mathrm{GL}(V)$ por

$$\begin{aligned} e_{2i-1} &\mapsto e'_{2i-1}, && \text{si } 1 \leq i \leq m), \\ e_{2i} &\mapsto \alpha^{-1}\beta e'_{2i} && \text{si } 1 \leq i \leq m), \\ e_{2m+1} &\mapsto e'_{2m+1}. \end{aligned}$$

Entonces $f' = \alpha^{-1}\beta f^{\sigma}$, con $f^{\sigma}(u,v) := f\left(\sigma^{-1}(u), \sigma^{-1}(v)\right)$. La multiplicación por una constante y la acción de $\mathrm{GL}(V)$ no cambia el grupo ortogonal (cf. [20, Sección 3.5.3]).

Es decir, $\mathrm{O}(V,f') = \mathrm{O}(V,\alpha^{-1}\beta f^{\sigma}) = \mathrm{O}(V,f)$.

2. Si $n = 2m$, hay una base $\{e_1, \ldots, e_{2m}\} \subset V$ tal que

$$\begin{aligned} f(e_{2i-1}, e_{2i}) &= 1 && \text{si } 1 \leq i \leq m-1 \\ f(e_i, e_j) &= 1 && \text{para otros } (i,j). \end{aligned}$$

Hay dos casos, que corresponden a a la existencia de un subespacio totalmente isotrópico de dimension m:

(a) $f(e_{2m-1}, e_{2m-1}) = f(e_{2m}, e_{2m}) = 0$ y $f(e_{2m-1}, e_{2m}) = 1$, o

(b) $f(e_{2m-1}, e_{2m-1}) = -\alpha f(e_{2m}, e_{2m}) \neq 0$ y $f(e_{2m-1}, e_{2m}) = 0$.

En el caso (a), hay un subespacio totalmente isotrópico de dimensión m y el orden del grupo ortogonal $\mathrm{O}(V,f) = \mathrm{O}^{+}(n)$ es

$$\left|\mathrm{O}^{+}(n)\right| = 2(q^m - 1)q^{m(m-1)} \prod_{i=1}^{m-1} (q^{2m-2i} - 1).$$

En el caso (b), no hay un subespacio totalmente isotrópico de dimension m y el orden del grupo ortogonal $\mathrm{O}(V,f) = \mathrm{O}^{-}(n)$ es

$$\left|\mathrm{O}^{-}(n)\right| = 2(q^m + 1)q^{m(m-1)} \prod_{i=1}^{m-1} (q^{2m-2i} - 1).$$

Los dos grupos claramente no son isomorfos porque sus órdenes son diferentes.

■

3 Clasificación de grupos ortogonales para característica 2

3.1 Formas cuadráticas

De manera similar con las formas bilineales, podemos definir grupos ortogonales en términos de formas cuadráticas. Para cuerpos de característica impar, esto es equivalente a la formulación que utiliza formas bilineales simétricas. Cuando trabajemos con cuerpos de característica 2, solo usaremos formas cuadráticas.

Sean F un cuerpo de característica p (no necesariamente par) y V un espacio vectorial sobre F de dimensión n.

Definición 3.1. *Una función $Q : V \to F$ es* una forma cuadrática *cuando para todos $u, v \in V$ y $\lambda \in F$,*

$$Q(\lambda u + v) = \lambda^2 Q(u) + \lambda f_Q(u, v) + Q(v),$$

donde $f_Q : V \times V \to F$ es una forma bilineal simétrica.

Una forma cuadrática $Q : V \to F$ determina una forma bilineal simétrica f_Q. De hecho, f_Q es alternada cuando $p = 2$ porque

$$0 = Q(2v) = 2Q(v) + f_Q(v, v) = f_Q(v, v).$$

Dada una forma bilineal simétrica $f : V \times V \to F$, tambiÃ©n podemos obtener una forma cuadrática $Q_f(v) := \frac{f(v,v)}{2}$, pero solo cuando $p \neq 2$. Por lo tanto, solo existe una equivalencia entre la teoría de formas bilineales simétricas y la teoría de formas cuadráticas cuando la caracteristíca de F no es 2.

Definición 3.2. *Sea $Q : V \to F$ una forma cuadrática. Definimos* el radical *de Q,*

$$\operatorname{rad}(Q) := \{v \in \operatorname{rad}(f_Q) \mid Q(v) = 0\},$$

y el álgebra de Clifford*,*

$$\operatorname{Cl}(V, Q) := \bigoplus_{n \geq 0} V^{\otimes n} / \langle v \otimes v - Q(v) \otimes \mathbb{1} \rangle .$$

Además definimos:

- *Q es* no singular *cuando* $\operatorname{rad}(Q) = 0$.
- *Q es* no degenerada *cuando f_Q es no singular.*

Introducimos la invariante de Arf para describir las formas cuadráticas sobre cuerpos de característica par. Mencionamos la invariante de Arf porque las formas cuadráticas no singulares sobre un espacio vectorial sobre F están determinadas por la invariante de Arf y el álgebra de Clifford. Para el resto de la sección, F es un cuerpo de característica par

Sea Q una forma cuadrática no degenerada (entonces n es par). Definimos la relación de equivalencia $\sim$: $Q \sim Q'$ cuando existe $C \in \mathrm{GL}_n(F)$ tal que $Q(v) = Q'(Cv)$. Por un teorema de Arf [1, Satz 2] (cf. [16, Sección 4]), existen formas cuadráticas binarias Q_i tales que

$$Q \sim \bigoplus_{i}^{r} Q_i.$$

Definición 3.3 (cf. [16, Sección 7])**.** *Sea U el subgrupo aditivo de F definido por*

$$U := \left\{ u^2 + u \mid u \in F \right\}.$$

Definimos la invariante de Arf *por*

$$\mathrm{Arf}(ax^2 + xy + by^2) := ab + U \in F/U.$$

Para una forma cuadrática no degenerada Q, definimos la invariante de Arf *(o* el pseudodeterminante *[8]) de Q por*

$$\mathrm{Arf}(Q) := \sum_{i=1}^{r} \mathrm{Arf}(Q_i).$$

Observación 3.4. *Para cualquier forma cuadrática binaria Q, existen a y b en F tales que $Q(x, y) \sim ax^2 + xy + by^2$. La invariante de Arf está bien definido porque si $ax^2 + xy + by^2 \sim a'x^2 + xy + b'y^2$, existe $u \in F$ tal que $ab - a'b' = u^2 + u$.*

Teorema 3.5 ([1, Teoremas 11-12], [2])**.** *Si F es perfecto, una forma cuadrática no singular Q está determinada únicamente por el par $(\mathrm{Arf}(Q), n)$.*

Si F no es perfecto y $[F : F^2] \leq 2$, una forma cuadrática no singular Q está determinada únicamente por el triplete $(\mathrm{Arf}(Q), n, \mathrm{Cl}(V, Q))$ donde $\mathrm{Cl}(V, Q)$ es el álgebra de Clifford.

Observación 3.6. *Para una excelente revisión de la historia de los teoremas de Arf y la corrección de sus errores, consulte [16, Sección 9].*

Ejemplo 3.7. *Si k es un cuerpo perfecto, entonces $F = k(t)$ y $F = k((t))$ son cuerpos tales que F no es perfecto y $[F : F^2] \leq 2$.*

3.2 Los grupos ortogonales para F finito

Sea F un cuerpo finito de característica 2. La primera definicion también es válida para otros cuerpos, pero nos centramos en este caso. Describimos los grupos ortogonales sobre tal cuerpo F y demostramos la fila inferior de Teorema 1.1.

Definición 3.8. *Sea $Q : V \to F$ una forma cuadrática no singular. Definimos* el grupo ortogonal *de V sobre Q como*

$$\mathrm{O}(V, Q) := \{g : V \to V \textit{ lineal} \mid Q\left(g(v)\right) = Q(v), \quad \forall v \in V\}.$$

Los siguientes resultados son conocidos (cf. [22, Sección 3.4.7 y Sección 3.8]).

Lema 3.9. *Si $Q : V \to F$ es una forma cuadrática degenerada y no singular, entonces* $\dim \mathrm{rad}(f) = 1$.

Demostración. La forma bilineal simétrica f_Q es alternada porque $\mathrm{car}(F) = 2$. Si $u, v \in \mathrm{rad}(f)$,

$$Q(\lambda u + v) = \lambda^2 Q(v) + Q(w),$$

entonces $Q|_{\mathrm{rad}(f)}$ es una aplicación semilineal a F y $\mathrm{rad}(Q)$ es un subespacio de codimensión 0 o 1 de $\mathrm{rad}(f)$. Pero $\mathrm{rad}(f) \neq 0$ y $\mathrm{rad}(Q) = 0$ porque Q es degenerada y no singular, entonces $\dim \mathrm{rad}(f) = 1$. ∎

Lema 3.10. *Si $Q : V \to F$ es una forma cuadrática degenerada no singular, entonces f_Q induce una forma simpléctica sobre $V/\mathrm{rad}(f_Q)$ tal que* $\mathrm{O}(V, Q) \cong \mathrm{O}(V/\mathrm{rad}(f_Q), f'_Q)$.

Demostración. Para el complemento $W \cong V/\mathrm{rad}(f_Q)$ de $V/\mathrm{rad}(f_Q)$ en V, $V = W \oplus \mathrm{rad}(f_Q)$. Para $g \in \mathrm{O}(V, Q)$ y $w, w' \in W$,

$$\begin{aligned}
Q(w) + f_Q(w, w') + Q(w') &= Q(w + w') \\
&= Q(g|_W(w + w')) \\
&= Q(g|_W(w)) + f_Q(g|_W(w), g|_W(w')) + Q(g|_W(w')) \\
&= Q(w) + f_Q(g|_W(w), g|_W(w')) + Q(w').
\end{aligned}$$

Entonces, $f_Q(w, w') = f_Q(g|_W(w), g|_W(w'))$ para todos $w, w' \in W$. Usando $g|_W$ y el isomorfismo $W \cong V/\mathrm{rad}(f_Q)$, hay $g' \in \mathrm{O}(V/\mathrm{rad}(f_Q), f'_Q)$.

El elemento de $\mathrm{O}(V/\mathrm{rad}(f_Q), f'_Q)$ obtenido de cada $g \in \mathrm{O}(V, Q)$ es único. Sean $g_1, g_2 \in \mathrm{O}(V, Q)$ tales que $g'_1 = g'_2 \in \mathrm{O}(V/\mathrm{rad}(f_Q), f'_Q)$.

La dimensión de $\mathrm{rad}(f_Q)$ es 1, entonces podemos escribir $\mathrm{rad}(f_Q) = \langle u \rangle$. Sean $v \in V$ y $w \in W$.

$$\begin{aligned} f_Q(v, g_1(w) + g_2(w)) &= f_Q(v, g_1'(w) + g_2'(w)) \\ &= f_Q(v, 0) = 0. \\ Q(g_1(w) + g_2(w)) &= Q(g_1(w)) + f_Q(g_1(w), g_2(w)) + Q(g_2(w)) \\ &= 2Q(w) + f_Q(g_1'(w), g_2'(w)) \\ &= f_Q(g_1'(w), g_1'(w)) \\ &= 0. \end{aligned}$$

Entonces, $g_1(w) + g_2(w) \in \mathrm{rad}(Q) = \{0\}$ y $g_1(w) = g_2(w)$ para todos $w \in W$. Solo necesito verificar que $g_1|_{\langle u \rangle} = g_2|_{\langle u \rangle}$ porque $g_1|_W = g_2|_W$. Pero, $g_i(u) \in \langle u \rangle$ porque g_i es lineal. Además,

$$\begin{aligned} Q(g_i(u) + u)) &= Q(g_i(u)) + f_Q(g_i(u), u) + Q(u) \\ &= 2Q(u) + f_Q(g_i(u), u) \\ &= 0. \end{aligned}$$

Entonces $g_i(u) + u \in \mathrm{rad}(Q) = \{0\}$ y $g_i(u) = u$ para cada $i \in \{1, 2\}$. ■

Proposición 3.11. *Si $Q : V \to F$ es una forma cuadrática no singular, entonces*

$$\begin{aligned} &\mathrm{O}(V, Q) \cong \mathrm{Sp}(n-1) && \textit{si } n \textit{ es impar}, \\ &\mathrm{O}(V, Q) \leq \mathrm{Sp}(n) && \textit{si } n \textit{ es par}. \end{aligned}$$

Demostración. Sea $g \in \mathrm{O}(V, Q)$ y $u, v \in V$. Tenemos las igualdades,

$$\begin{aligned} Q(u) + f_Q(u, v) + Q(v) &= Q(u + v) \\ &= Q(g(u + v)) \\ &= Q(g(u) + g(v)) \\ &= Q(g(u)) + f_Q(g(u), g(v)) + Q(g(v)) \\ &= Q(u) + f_Q(g(u), g(v)) + Q(v). \end{aligned}$$

Entonces, $f_Q(u, v) = f_Q(g(u), g(v))$ para todos $u, v \in V$ y $g \in \mathrm{O}(V, f_Q)$. Por lo tanto, $\mathrm{O}(V, Q) \leq \mathrm{Sp}(n)$.

Si n es impar, $\mathrm{rad}(f_Q) \neq 0$ (de lo contrario f_Q es simpléctica). Por Lema 3.9, $\dim \mathrm{rad}(f_Q) = 1$. Por Lema 3.10, $\mathrm{O}(V, Q) \cong \mathrm{O}(V/\mathrm{rad}(f_Q), f_Q)$. La forma bilineal alternada f_Q induce una forma simpléctica sobre $V/\mathrm{rad}(f_Q)$, entonces $\mathrm{O}(V/rad(f_Q), f_Q') \cong \mathrm{Sp}(n-1)$. ■

Proposición 3.11 da la esquina inferior izquierda de Teorema 1.1. Para completar la demostración de la fila inferior de Teorema 1.1, solo necesitamos contar el número de grupos ortogonales de dimensión par. Como en la Sección 2.2, usamos vectores isotrópicos.

Definición 3.12. *Un vector* $v \in V \setminus \{0\}$ *es* un vector isotrópico *para la forma cuadrática* $Q : V \to F$ *si* $Q(v) = 0$.

Lema 3.13 (cf. [20, Sección 3.5.9], [22, Sección 3.4.7])**.** *Hay exactemente dos clases de equivalencia de formas cuadráticas no singulares.*

Demostración. Construimos una base de la misma manera que la base simpléctica en Observación 2.4, pero con $Q(e_i) = Q(f_i) = 0$ cuando sea posible. Si $n > 2$ y $Q(e_i) \neq 0$, podemos reemplazar e_i par

$$e_i' = \left(\frac{Q(f_i)}{Q(e_i)}\right)^{\frac{|F|}{2}} e_i + f_i,$$

si $Q(e_i) \neq 0$ (en cuyo caso $Q(e_i') = 0$). Si $Q(e_i) = 0$, podemos reemplazar f_i par $f_i' = f_i + Q(f_i)e_i$ para garantizar que $Q(f_i') = 2Q(f_i) = 0$.

Pero para los dos primeros elementos de la base, podemos elegir e_1 y f_1 tal que $Q(e_1) = f(e_1, f_1) = 1$, $f(e_1, f_1 + \lambda e_1) = 1$ y $Q(f_1 + \lambda e_1) = Q(f_1) + \lambda^2 + \lambda$. Podemos reemplazar f_1 par $f_1' = f_1 + \lambda e_1$. Hay exactamente dos clases de equivalencia de formas cuadráticas no singulares, dependiendo de si Q tiene un vector isotrópico (i.e. si $Q(f_1') = \lambda^2 + \lambda + Q(f_1) = 0$ tiene una solución en F). ■

Como en Proposición 2.11, las dos clases de equivalencia de formas cuadráticas no singulares en Lema 3.13 producen dos clases de isomorfismo de grupos ortogonales con diferentes ordenes.

Proposición 3.14 (cf. [20, Sección 3.5.10])**.**

1. *Si* n *es impar, entonces hay solo un grupo ortogonal (excepto por isomorfismo)* $\mathrm{O}(n) \cong \mathrm{Sp}(n-1)$

2. *Si* n *es par, entonces hay dos grupos (excepto por isomorfismo)* $\mathrm{O}^{\pm}(n)$

Demostración.

1. Por Proposición 3.11.

2. Las dos clases de equivalencia de formas cuadráticas no singulares en Lema 3.13 se distinguen por diferentes números de vectores isotrópicos. Como en Proposición 2.11, el orden del grupo ortogonal $\mathrm{O}(V,Q)=\mathrm{O}^+(n)$ en un caso es

$$\left|\mathrm{O}^+(n)\right| = 2(q^m-1)q^{m(m-1)}\prod_{i=1}^{m-1}(q^{2m-2i}-1).$$

En el otro caso, el orden del grupo ortogonal $\mathrm{O}(V,Q)=\mathrm{O}^-(n)$ es

$$\left|\mathrm{O}^-(n)\right| = 2(q^m+1)q^{m(m-1)}\prod_{i=1}^{m-1}(q^{2m-2i}-1).$$

■

4 Subgrupos de grupos ortogonales

4.1 Los subgrupos para característica impar

Sea F un cuerpo finito de característica impar. Todos los elementos del grupo ortogonal tienen determinante ± 1. Por lo tanto tenemos *el grupo ortogonal especial* $\mathrm{SO}^{(\pm)}(n)$, el subgrupo de $\mathrm{O}^{(\pm)}(n)$ de índice 2 definido como el núcleo del determinante. Al igual que con el grupo ortogonal en Teorema 1.1, hay una clase de isomorfismo de grupos ortogonales especiales $\mathrm{SO}(n)$ si n es impar y hay dos clases de isomorfismo de grupos ortogonales especiales $\mathrm{SO}^{\pm}$ si n es par.

También $\pm\mathrm{Id} \in \mathrm{O}^{(\pm)}(n)$ (con $-\mathrm{Id} \in \mathrm{SO}^{(\pm)}(n)$ si y solo si n es par), entonces tenemos los grupos de cocientes $\mathrm{PO}^{(\pm)}(n) := \mathrm{O}^{(\pm)}(n)/\left\{\pm\mathrm{Id}\right\}$ y $\mathrm{PSO}^{(\pm)}(n) := \mathrm{SO}^{(\pm)}(n)/\left\{\pm\mathrm{Id}\right\}$ llamados respectivamente *el grupo ortogonal proyectivo* y *el grupo ortogonal especial proyectivo*.

Definición 4.1. *Para una forma bilineal simétrica $f: V\times V\to F$ y un vector $v\in V$ tal que $f(v,v)\neq 0$, definimos la reflexión*

$$r_v : x \mapsto x - 2\frac{f(x,v)}{f(v,v)}v.$$

Un elemento g del $\mathrm{SO}^{(\pm)}(n)$ *tiene* la norma espinor 1 *cuando g es un producto de un número par de reflexiones de vectores de norma* 1 *y un número par de reflexiones de vectores de norma no cuadrada. Un elemento g del* $\mathrm{SO}^{(\pm)}(n)$ *tiene la norma espinor -1 de lo contrario.*

Usando el núcleo de la norma espinor $\mathrm{sn} : \mathrm{SO}^{(\pm)}(n) \to \{\pm 1\}$, definimos los subgrupos de índice 2

$$\begin{aligned}\Omega^{(\pm)}(n) &:= \ker(\mathrm{sn}) \leq \mathrm{SO}^{(\pm)}(n),\\ \mathrm{P}\Omega^{(\pm)}(n) &:= \ker\left(\mathrm{sn}|_{\mathrm{PSO}^{(\pm)}}\right) \leq \mathrm{PSO}^{(\pm)}(n).\end{aligned}$$

4.2 Los subgrupos para característica 2

En esta sección, F es cuerpo de característica 2. Podemos considerar que F es finito, pero las siguientes definiciones y resultados también son válidos para cuerpos infinitos.

Para característica 2, el determinante es inútil y no tenemos la norma espinor (cf. Definición 4.1). Sea $Q : V \to F$ una forma cuadrática no singular. Definimos la transvección ortogonal («la reflexión »)

$$t_v : x \mapsto x + \frac{f_Q(x,v)}{f_Q(v,v)} v$$

para $v \in V$ tal que $f_Q(v,v) \neq 0$. El transvección t_v es lineal y conserva Q porque

$$Q\left(x + f(x,v)v\right) = Q(x) + f_Q(x,v)^2 + f_Q(x,v)^2 Q(v) = Q(x).$$

Teorema 4.2 (Cartan–Dieudonné–Kneser)**.** *El grupo ortogonal* $\mathrm{O}(V,Q)$ *es generado por* $\{t_v\}_{v\in V}$*, excepto cuando* $F = \mathbb{F}_2$ *y* $n = 4$*.*

Observación 4.3. *Wilson [22, Capítulo 3] no menciona la única excepción dada por Cartan–Dieudonné–Kneser (cf. [3, Teorema I.5.1], [7, pp.20–22], [12], [13, Teorema 6.3.4], y [21, Teorema 11.42]).*

Definición 4.4. *Definimos* la invariante de Dickson *para*

$$g = \prod_{i=1}^{r} t_{v_i},$$

como

$$D(g) := \begin{cases} 1 & r \textit{ es impar,}\\ 0 & r \textit{ es par.}\end{cases}$$

Equivalente, $D(g) = \mathrm{rango}\,(\mathrm{Id} - g)$ (*módulo* 2).

La invariante de Dickson también se le conoce como *el cuasideterminante* o *el pseudodeterminante* porque son esencialmente el mismo que el determinante en característica impar.

Teorema 4.5 ([9, Teorema 2], cf. [21, Teorema 11.43])**.** *La invariante de Dickson es un homomorfismo*

$$D : \mathrm{O}(V, Q) \to \mathbb{Z}/2\mathbb{Z}.$$

Además para característica diferente a 2*,*

$$\det(g) = (-1)^{D(g)}.$$

Entonces en este caso, el determinante es equivalente a la invariante de Dickson.

Podemos usar la invariante de Dickson como determinante para definir subgrupos.

Definición 4.6. *Definimos* el grupo ortogonal especial *como el núcleo de* D*,*

$$\mathrm{SO}(V, Q) := \{g \in \mathrm{O}(V, Q) \mid D(g) = 0\}.$$

Este grupo tambiÃ©n se conoce como el núcleo espinorial $\Omega(V, Q)$.

Una consecuencia de la segunda parte del Teorema 4.5, que en realidad funciona para un cuerpo general F, explica el nombre grupo ortogonal especial.

Corolario 4.7. *Si* F *es un cuerpo de característica* 0 *o impar, el núcleo de* D *es isomorfo al subgrupo de elementos de determinantes* 1 *en* $\mathrm{O}(V, Q)$ *y también al subgrupo de elementos de norma espinorial* 1 *en* $\mathrm{O}(V, Q)$.

Teorema 4.8 ([11, 17, 4, 18])**.** *El subgrupo commutador*

$$\mathrm{O}(V, Q)^{(1)} := [\mathrm{O}(V, Q), \mathrm{O}(V, Q)]$$

es isomorfo al $\Omega(V, Q)$.

Observación 4.9. *Si* F *es un cuerpo global o local, la afirmación del Teorema 4.8 sigue siendo cierto con una sola excepción: si* F *es un cuerpo local de característica impar,* $n = 4$*, y* V *es anisotrópico. En este caso, Pollak [17] demostró que* $[\Omega(V, Q) : \mathrm{O}(V, Q)^{(1)}] = 2$.

Agradecimientos

Estas notas se basan en una charla impartida en el taller de Casa Matemática Oaxaca–Banff International Research Station (CMO–BIRS), «Teoría de números en América », en agosto de 2019. Agradecemos su apoyo, así como las discusiones con Lea Beneish, Michael Harris, Luis Lomelí y Alberto Mínguez. También agradecemos a los árbitros anónimos por sus útiles comentarios.

Financiamiento

El autor fue apoyado por la National Science Foundation Graduate Research Fellowship Program, Grant No. DGE-1644869. Todas las opiniones, hallazgos y conclusiones o recomendaciones expresadas en este material pertenecen al autor y no reflejan necesariamente los puntos de vista de la National Science Foundation.

Referencias

[1] C. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. I*, J. Reine Angew. Math. **183** (1941), 148–167. Doi: 10.1515/crll.1941.183.148

[2] R. Baeza, *Comparing u-invariants of fields of characteristic* 2, Bol. Soc. Brasil. Mat. **13** (1982), no. 1, 105–114. Doi: 10.1007/BF02584739

[3] C. Chevalley, *The Algebraic Theory of Spinors*, Columbia University Press, New York, 1954. Doi: 10.7312/chev93056

[4] E.A. Connors, *The structure of* O'/Ω *over local fields of characteristic* 2, Proc. Amer. Math. Soc. **22** (1969), 596–599. Doi: 10.2307/2037439

[5] H. del Castillo, *Langlands functoriality conjecture for* SO^* *(2n) in positive characteristic*, Ph.D. Thesis, Université Paris-Saclay; Pontificia Universidad Católica de Valparaíso, 2021. Available from: Link

[6] L. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, Dover Publications, Inc., New York, 1958. Doi: 10.5962/bhl.title.22174

[7] J. Dieudonné, *Sur les Groupes Classiques*, Hermann et Cie., Paris, 1948.

[8] J. Dieudonné, *Pseudo-discriminant and Dickson invariant*, Pacific J. Math. **5** (1955), 907–910. Available from: Link

[9] R. Dye, *A geometric characterization of the special orthogonal groups and the Dickson invariant*, J. London Math. Soc. (2) **15** (1977), no. 3, 472–476. Doi: 10.1112/jlms/s2-15.3.472

[10] Benedict. Gross, M. Reeder, *From Laplace to Langlands via representations of orthogonal groups*, Bull. Amer. Math. Soc. **43** (2006), no. 2, 163–205. Doi: 10.1090/S0273-0979-06-01100-1

[11] M. Kneser, *Orthogonale Gruppen über algebraischen Zahlkörpern*, J. Reine Angew. Math. **196** (1956), 213–220. Doi: 10.1515/crll.1956.196.213

[12] M. Kneser, *Witts Satz über quadratische Formen und die Erzeugung orthogonaler Gruppen durch Spiegelungen*, Math.-Phys. Semesterber. **17** (1970), 33–45.

[13] M.A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 294, Springer-Verlag, Berlin, 1991, Doi: 10.1007/978-3-642-75401-2

[14] L.A. Lomelí, *Functoriality for the classical groups over function fields*, Int. Math. Res. Not. IMRN (2009), no. 22, 4271–4335. Doi: 10.1093/imrn/rnp089

[15] L.A. Lomelí, *Rationality and holomorphy of Langlands-Shahidi L-functions over function fields*, Math. Z. **291**(2019), no. 1-2, 711–739. Doi: 10.1007/s00209-018-2100-7

[16] F. Lorenz, P. Roquette, *Cahit Arf and his invariant*, Mitt. Math. Ges. Hamburg **30** (2011), 87–126. Available from: Link

[17] B. Pollak, 4-*dimensional orthogonal groups over algebraic number fields*, J. Reine Angew. Math. **211** (1962), 176–178. Doi: 10.1515/crll.1962.211.176

[18] B. Pollak, *Orthogonal groups over global fields of characteristic* 2, J. Algebra **15** (1970), no. 4, 589-595. Doi: 10.1016/0021-8693(70)90055-4

[19] M. Reeder, *On the restriction of Deligne-Lusztig characters*, J. Amer. Math. Soc. **20**(2007), no. 2, 573–602. Doi: 10.1090/S0894-0347-06-00540-6

[20] M Suzuki, *Group Theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin-New York, 1982.

[21] D. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

[22] R. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009. Doi: 10.1007/978-1-84800-988-2