Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Geometría sobre cuerpos finitos y aplicaciones combinatorias

Autor: Miguel Quintana Renedo

Tutor: José Enrique Marcos Naveira

Índice general

Introducción

Desde el mismo comienzo de la historia hay constancia de que el hombre se ha interesado por describir los objetos y formas que lo rodean, de esta forma surgió la geometría. Éste fue el propósito inicial de esta parte de las matemáticas y como lógica consecuencia, hasta ya entrado el siglo XIX la única geometría que el hombre fue capaz de concebir es la que describe el mundo en el que vivimos. A principios de dicho siglo fueron descubiertas las primeras geometrías no euclídeas, lo que hizo que rápidamente esta posición quedase obsoleta. Hoy en día son muchas de geometrías diferentes.

Una vez hemos dicho que existen muchas geometrías y no una única, hace falta dejar claro qué es una geometría. El matemático alemán David Hilbert nos dio en *"The foundations of Geometry"* (1899) una buena idea que seguir:

"Una geometría es el conjunto de teoremas que se de deducen de su sistema de axiomas."

Esta definición puede resultar muy abstracta y puede hacer que se empiece a construir demasiado lejos del mundo real o de las aplicaciones de la geometría. Buscando algo más concreto, una posible definición de geometría es la siguiente:

Una geometría es un par (Ω, I)*, donde* Ω *es un conjunto e* I *una relación sobre los objetos de* Ω *simétrica y reflexiva.*

La idea detrás de esta definición es que el conjunto Ω contenga todos los objetos geométricamente relevantes y la relación I describa si los objetos son incidentes entre sí. Parece que la relación de incidencia natural es la de contención, sin embargo, esta relación no es simétrica; esto se puede solucionar fácilmente añadiendo la posibilidad no sólo de contener si no de ser contenido.

Existen geometrías construidas sobre diversas estructuras, sin embargo nosotros trataremos principalmente con aquellas construidas sobre cuerpos. Uno de los teoremas más conocidos de la geometría clásica es el teorema de representación que nos asegura que a todo espacio afín o proyectivo, que cumpla el conocido teorema de Desargues, se le puede dotar de coordenadas sobre un cuerpo. Nosotros partiremos desde aquí, definiendo directamente estos espacios sobre estructuras vectoriales.

Se han estudiado a lo largo del grado en matemáticas el espacio afín y proyectivo sobre los cuerpos $\mathbb{R}$ y $\mathbb{C}$, nosotros trabajaremos sobre cuerpos finitos para acabar estudiando también algunas de las aplicaciones de la geometría en el campo de la combinatoria. Cabe resaltar que, aunque no se traten a lo largo del presente trabajo, las estructuras que estudiaremos tienen amplias aplicaciones en las telecomunicaciones actuales, tanto en el campo de la criptografía como en el de los códigos correctores.

Puesto que las geometrías con las que se va a tratar están construidas sobre **cuerpos finitos**, el trabajo comienza con un primer capítulo en el que se recopilan las propiedades más importantes a cerca de ellos y algunas propiedades que se utilizarán más adelante para por ejemplo, clasificar las formas bilineales.

En el segundo capítulo se introducen, partiendo de los espacios vectoriales $\mathbb{F}_q^n$, los espacios **proyectivo**, $\mathbb{P}^n(\mathbb{F}_q)$, y **afín**, $\mathbb{A}^n(\mathbb{F}_q)$. Se hace un conteo de los subespacios que los forman a través de los coeficientes gaussianos y se comprueba que cumplen los axiomas que habrían bastado para definirlos.

En los dos siguientes capítulos se introducirán las **aplicaciones bilineales**, las **formas cuadráticas** que siempre las acompañan y se hará una clasificación de las mismas. Aquí aparecerá una de las más significativas diferencias de los espacios que tratamos con los espacios construidos sobre $\mathbb{R}$ o $\mathbb{C}$; en espacios de dimensión mayor que dos siempre aparecen vectores ortogonales a sí mismos, luego estos espacios no pueden ser anisotrópicos como el euclídeo. Se ha separado en dos capítulos para tratar por separado aquellos cuerpos en los que no se puede dividir entre dos, puesto que pese a que la clasificación acaba siendo similar, es necesario tratarlos de diferente manera.

Puesto que bajo nuestros espacios proyectivos subyace una estructura vectorial, estas forma cuadráticas tratadas anteriormente, generan unos interesantes objetos en $\mathbb{P}^n(\mathbb{F}_q)$ llamados **cuádricas**. En el quinto capítulo estudiamos las propiedades de estos conjuntos, haciendo especial hincapié en los espacios de baja dimensión. Finalmente, en un guiño a la matemática patria clasificamos las cuádricas que parten de formas cuadráticas degeneradas como se hace en [San]; obra escrita por uno de los más importantes matemáticos españoles, Luis A. Santaló, que pese a ser español tuvo que exiliarse gran parte de su vida en Argentina.

Algunas de las cuádricas estudiadas no dejan de ser casos particulares de unos objetos que viven en el espacio proyectivo. Estos objetos se llaman **curvas** y a su estudio se dedica el sexto capítulo del trabajo. La parte más importante de este capítulo es el teorema de Segre, que afirma que en determinados casos, las cuádricas que hemos estudiado son las únicas curvas posibles.

Desde la segunda mitad del siglo XX hasta nuestros días la geometría proyectiva se ha enfocado en estudiar su relación con la combinatoria. Esto ha desembocado en el reto de describir una geometría a partir de sus parámetros combinatorios. A cerca de este tema versan los últimos dos capítulos.

En el séptimo capítulo se introducen los **diseños combinatorios** un tipo de estructura combinatoria que fue muy utilizada durante el siglo XX en el diseño de

experimentos. Estas estructuras existen de forma natural en la geometría finita, como analizamos en este capítulo. El avance más grande que se ha hecho en esta materia es el teorema de Bruck-Ryser que constituye el colofón de este séptimo capítulo.

En el último capítulo definimos una nueva geometría, los **planos inversivos** como un diseño combinatorio y analizamos su estrecha relación con la geometría afín y los **ovoides**, estructuras del espacio proyectivo.

Capítulo 1

Cuerpos finitos

Aunque existen geometrías apoyadas en estructuras que no son cuerpos, en este trabajo nos centraremos en las que sí lo están, concretamente en las que se basan en cuerpos finitos. En este capítulo desglosaremos las propiedades más elementales de los cuerpos finitos. Existe mucha literatura acerca de ellos, un buen libro es [Rom].

1.1. Estructura

Definición 1.1. *Un cuerpo* $(\mathbb{F}, +, \cdot)$ *es un conjunto no vacío,* $\mathbb{F}$*, con dos operaciones internas* $(+, \cdot)$*, a las que nos referiremos como suma y producto respectivamente, que cumplen las siguientes propiedades:*

I $(\mathbb{F}, +)$ *es un grupo abeliano cuyo elemento neutro denotamos por* 0*.*

II *Siendo* $\mathbb{F}^* = \mathbb{F} - \{0\}$*. Entonces* $(\mathbb{F}^*, \cdot)$ *es un grupo, cuyo elemento neutro es* 1*.*

III *Cumple la propiedad distributiva por ambos lados, es decir:*

$$(a+b)\cdot c = a\cdot c + b\cdot c \quad a\cdot(b+c) = a\cdot b + a\cdot c \quad a,b,c \in \mathbb{F}$$

Definición 1.2. *Dado un cuerpo* $\mathbb{F}$*, su característica es* $car(\mathbb{F}) = r$*, con* $r \in \mathbb{N}$*, si* r *es el menor natural de forma que* $\overbrace{1+\cdots+1}^{r \text{ veces}} = r1 = 0$*; se toma* $car(\mathbb{F}) = 0$ *si no existe dicho* r*.*

Teorema 1.3. *La característica de un cuerpo es* 0 *ó* p *siendo* p *un número primo. En particular la característica de un cuerpo finito es un número primo.*

Demostración. Sea $\mathbb{F}$ un cuerpo y $r = car(\mathbb{F})$, supongamos que r no es ni nulo ni un número primo, entonces $r = st$ para algún par de números naturales, quizá primos. Así que $0 = r1 = (s1)\cdot(t1)$ y por ser un cuerpo siempre dominio de integridad o bien $s1$, o bien $t1$ deben ser nulos y por lo tanto, r no es el menor número natural con $r1 = 0$.

□

De aquí en adelante todos los cuerpos serán finitos y conmutativos, esto es, $\mathbb{F}$ será un conjunto finito y $(\mathbb{F}^*, \cdot)$ será un grupo abeliano, por lo tanto, las dos relaciones distributivas de la definición de cuerpo serán la misma. Además, donde se pueda distinguir por el contexto omitiremos el símbolo"$\cdot$"para el producto.

Definición 1.4. *Dado un grupo $(G, \cdot)$:*

- *Llamamos orden del grupo $|G|$ a su cardinal.*
- *Sea $x \in G$ el orden de x, $o(x)$, es el mínimo $n \in \mathbb{N}$ que cumple $x^n = 1$.*
- *Decimos que $e \in \mathbb{N}$ es el exponente de G si e es el menor número natural que cumple $x^e = 1$ para cualquier $x \in G$.*

Definición 1.5. *Un grupo G es cíclico si existe $x \in G$ de forma que*

$$G = \{x^n : n = 0, 1 \ldots\}.$$

En tal caso x es un generador de G.

Proposición 1.6. *Dado un grupo finito y conmutativo G su exponente, e, coincide con el máximo de los órdenes de los elementos de G.*

Demostración. Es fácil ver que dado $x \in G$ se tiene $x^d = 1$ si y sólo si d resulta ser múltiplo del orden de x, $o(x)$. Por lo tanto, el exponente de G, e, será el mínimo común múltiplo de todos los órdenes $o(x_i)$ de elementos de G. Tenemos que ver que de hecho existe un elemento cuyo orden es e.

Podemos escribir e como producto de primos distintos con diferente multiplicidad $e = e_1^{g_1} \cdots e_t^{g_t}$. Por ser e el mínimo común múltiplo de los $o(x_i)$; para cada j, $1 \leq j \leq t$, existe un elemento $x_j \in G$ de forma que $e_j^{g_j}$ divide a $o(x_j)$.

Si existe un elemento de orden n entonces existen elementos de orden d para cada d divisor de n sin más que considerar el elemento $x^{n/d}$.

Consideramos ahora cada factor $e_j^{g_j}$. Existe para cada j con $1 \leq j \leq t$ un $y_j \in G$ de orden $e_j^{g_j}$. Por lo tanto, el elemento $y = y_1 \cdots y_t$ tiene orden e.

□

Proposición 1.7. *Dado un grupo finito y conmutativo G, es cíclico si y sólo si el exponente de G coincide con el orden de G.*

Demostración. Por un lado, si G es cíclico de orden n se escribe

$$G = \{1 = x^n, x, \ldots, x^{n-1}\},$$

por lo tanto, para cualquier potencia x^i con $i < n$ se tiene $x^i \neq 1$ y para cualquier elemento $a \in G$ existe un $j < n$ de forma que $a = x^j$ y $a^n = x^{jn} = 1$ lo que significa que n es el exponente de G.

Si G tiene exponente $|G| = n$, por la proposición anterior existe un elemento $x \in G$ de orden n y por lo tanto G contiene n elementos de la forma $x^i, \quad i = 1 \ldots n$, y estos son los que forman el grupo, por tanto, x genera G y es cíclico.

□

Teorema 1.8. *Dado un cuerpo finito $\mathbb{F}$ el grupo $(\mathbb{F}^*, \cdot)$ es un grupo cíclico.*

Demostración. El orden de $\mathbb{F}^*$ es $m-1$, y por lo tanto todos sus elementos son raíces de $p(X) = X^{m-1} - 1 \in \mathbb{F}[X]$. Por otra parte, $\mathbb{F}^*$ no puede tener un exponente $e < m-1$ porque entonces el polinomio $f(X) = X^e - 1$, de grado e, tendría $m-1$ raíces. Como el exponente de $\mathbb{F}^*$ coincide con su orden es cíclico.

□

Definición 1.9. *Dado un cuerpo $\mathbb{F}$, definimos lo siguiente:*

- *Un conjunto $\mathbb{K} \subset \mathbb{F}$ es un subcuerpo si, con las operaciones heredadas de $\mathbb{F}$, tiene estructura de cuerpo.*
- *Si $\mathbb{K} \subset \mathbb{F}$ es un subcuerpo se dice que $\mathbb{F}$ es una extensión de $\mathbb{K}$. Se denota $\mathbb{F}/\mathbb{K}$.*

Si $\mathbb{F}$ es una extensión de $\mathbb{K}$, podemos verlo como un $\mathbb{K}$-espacio vectorial con las operaciones esperadas: como suma de vectores la suma usual en $\mathbb{F}$ y como producto de un escalar de $\mathbb{K}$ por un vector de $\mathbb{F}$ también el producto usual en $\mathbb{F}$.

Definición 1.10. *Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos, se llama grado de la extensión y se denota $[\mathbb{F} : \mathbb{K}]$ a la dimensión de $\mathbb{F}$ como $\mathbb{K}$-espacio vectorial.*

Definición 1.11. *Dados dos cuerpos $\mathbb{F}, \mathbb{K}$; un homomorfismo de cuerpos es una aplicación $\phi : \mathbb{K} \to \mathbb{F}$ que cumple las siguientes propiedades:*

I $\phi(1_{\mathbb{K}}) = 1_{\mathbb{F}}$.

II $\phi(a) + \phi(b) = \phi(a+b)$ *para todos $a, b \in \mathbb{K}$.*

III $\phi(a)\phi(b) = \phi(ab)$ *para todos $a, b \in \mathbb{K}$.*

Nota. Un homomorfismo de cuerpos es un morfismo de anillos en el que los anillos son cuerpos. Luego la imagen de un homomorfismo de cuerpos es un cuerpo. Además, es siempre inyectivo, puesto que su núcleo es siempre $\{0\}$. Si $x \in ker(\phi)$ entonces $\phi(x) = 0$. Si suponemos que $x \neq 0$ entonces tiene un inverso, $y \in \mathbb{F}$ distinto de cero. Si aplicamos el homomorfismo a $xy = 1$ tenemos $1 = \phi(xy) = \phi(x)\phi(y) = 0$ así llegamos a un absurdo y podemos concluir que $x = 0$.

Teorema 1.12. *Sea $\mathbb{F}$ un cuerpo finito de característica p. La aplicación $\sigma : \mathbb{F} \to \mathbb{F}$ definida como $\sigma(x) = x^p$ es un isomorfismo de cuerpos.*

Demostración. Basta con ver que se trata de un homomorfismo de cuerpos, puesto que todos son inyectivos, y puesto que dominio e imagen tienen el mismo cardinal también será suprayectivo. Evidentemente para todos $x, y \in \mathbb{F}$ se cumple $\sigma(xy) = x^p y^p = \sigma(x)\sigma(y)$. Para comprobar la propiedad relativa a la suma escribimos:

$$\sigma(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

Como todos los elementos que forman los numeros combinatorios están en el cuerpo la expresión tiene sentido. En $\mathbb{F}$, por ser de característica p, se cumple $p = 0$ y por lo tanto se anulan todos los sumandos excepto los que tienen $i = 0$ o $i = p$. De esta forma hemos probado que $(x + y)^p = x^p + y^p$, lo que necesitábamos.

□

Definición 1.13. *Dado un cuerpo finito $\mathbb{F}$ de característica prima, p, el isomorfismo de grupos*

$$\begin{array}{rccc} \sigma: & \mathbb{F} & \to & \mathbb{F} \\ & x & \mapsto & \sigma(x) = x^p \end{array}$$

se denomina isomorfismo de Frobenius.

Recordamos que $\mathbb{Z}_p$, el anillo de los enteros módulo p, es un cuerpo para todo número p primo.

Proposición 1.14. *Si un cuerpo $\mathbb{F}$ tiene característica p, un número primo, existe un subcuerpo de $\mathbb{F}$ isomorfo a $\mathbb{Z}_p$.*

Demostración. Definimos un homomorfismo de cuerpos de la manera siguiente:

$$\begin{aligned} \phi : \mathbb{Z}_p &\longrightarrow \mathbb{F} \\ \bar{z} &\longmapsto z \cdot 1 = \overbrace{1 + \cdots + 1}^{z \text{ veces}}. \end{aligned}$$

El homomorfismo es inyectivo porque $\phi(\bar{z}) = z1 = 0 \Leftrightarrow z = pa$ donde $a \in \mathbb{Z}$ luego $\bar{z} = 0$. De esta forma, $\mathbb{Z}_p \cong Im(\phi) \subset \mathbb{F}$, que es un subcuerpo de $\mathbb{F}$.

□

Teorema 1.15. *Cada cuerpo finito $\mathbb{F}$ tiene orden $|\mathbb{F}| = p^n$, siendo p un número primo y $n \in \mathbb{N}$.*

Demostración. En primer lugar, veremos que si $\mathbb{F}/\mathbb{K}$ es una extensión de cuerpos finitos y $[\mathbb{F} : \mathbb{K}] = d$ entonces $|\mathbb{F}| = |\mathbb{K}|^d$. Para ello veamos que si la dimensión de $\mathbb{F}$ como espacio vectorial sobre $\mathbb{K}$ es d, entonces existe una base $\mathcal{B}$ con d elementos. De forma, cada elemento $x \in \mathbb{F}$ se escribe de manera única como combinación lineal de elementos de $\mathcal{B}$. Es decir, $x = \sum_{i=1}^{d} \alpha_i b_i$ con $b_i \in \mathcal{B}, \alpha_i \in \mathbb{F}$ y existen exactamente $|\mathbb{K}|^d$ combinaciones de este tipo.

Por la proposición 1.14 cada cuerpo finito se puede ver como una extensión de $\mathbb{Z}_p$ con p su característica, que debe ser un número primo.

□

Corolario 1.16. *Sea $\mathbb{F}$ de cardinal p^n y $\mathbb{K}$ un subcuerpo de de $\mathbb{F}$, entonces $|\mathbb{K}| = p^m$, siendo m un divisor de n.*

Demostración. Si $\mathbb{K}$ es un subcuerpo de $\mathbb{F}$ debe contener a $1_{\mathbb{F}}$. Como debe ser cerrado para la suma y hereda las operaciones de $\mathbb{F}$, fácilmente podemos deducir que la

característica de $\mathbb{K}$ debe ser también p. Por lo tanto, $|\mathbb{K}| = p^m$. Por otra parte, $\mathbb{F}$ es un $\mathbb{K}-$espacio vectorial, luego si llamamos $[\mathbb{F} : \mathbb{K}] = d$, podemos escribir:

$$p^n = |\mathbb{F}| = |\mathbb{K}|^d = p^{md},$$

de lo que se deduce que m divide a n.

□

Lema 1.17. *Sea $q = p^n$ una potencia de un primo. Sea $\mathbb{F}$ un cuerpo de orden q y $\mathbb{K}$ una extensión de $\mathbb{F}$ con $|\mathbb{K}| = q^d$. Entonces la aplicación $\sigma : \mathbb{K} \to \mathbb{K}$ definida como $\sigma(x) = x^q$ es un morfismo de cuerpos y además $\sigma(x) = x$ si y sólo si, $x \in \mathbb{F}$*

Demostración. La aplicación σ se define aplicando n veces el isomorfismo de Frobenius, luego es un morfismo de grupos. Dado $x \in \mathbb{F}$ podemos escribir $x^q = x^{q-1}x = 1 \cdot x$ porque $\mathbb{F}^*$ es un grupo cíclico de orden $q - 1$. Además el polinomio $X^q - X$ no puede tener más de q raíces, justamente los elementos de $\mathbb{F}$.

□

Lema 1.18. *Con la notación del lema anterior, las aplicaciones σ^i con $1 \leq i \leq d$ forman un grupo cíclico.*

Demostración. Como $\mathbb{K}$ es un cuerpo finito de cardinal q^d el menor i que cumple $x^i = x$ para todo $x \in \mathbb{K}$ es $i = q^d$ luego $\sigma^d(x) = x^{q^d}$ es la identidad y cualquiera de las potencias anteriores de σ no puede serlo, luego es un grupo cíclico de orden d.

□

Definición 1.19. *Dados un cuerpo finito de orden q y una extensión suya de orden q^d, $\mathbb{K}/\mathbb{F}$. Llamamos grupo de Galois $G(\mathbb{K}|\mathbb{F})$ al grupo cíclico que forman las potencias de la aplicación:*

$$\begin{array}{rccc} \sigma : & \mathbb{F} & \to & \mathbb{F} \\ & x & \mapsto & \sigma(x) = x^q. \end{array}$$

Definición 1.20. *Sea $\mathbb{F}$ un cuerpo de q elementos, $\mathbb{K}$ una extension de grado d y σ un generador del grupo de Galois $G(\mathbb{K}|\mathbb{F})$; la aplicación $tr : \mathbb{K} \to \mathbb{F}$ definida por:*

$$tr(x) = \sum_{i=1}^{d} \sigma^i(x), \quad \forall x \in \mathbb{K}$$

se denomina traza.

Proposición 1.21. *En las condiciones de la definición anterior, la aplicación traza está bien definida y viendo $\mathbb{K}$ como un $\mathbb{F}$-espacio vectorial es una aplicación lineal.*

Demostración. Hemos visto en 1.17 que $x \in \mathbb{F}$ si y sólo si, $\sigma(x) = x$. De la misma forma que se probó para el automorfismo de Frobenius, se puede ver que

$$\sigma(x + y) = \sigma(x) + \sigma(y). \tag{1.1}$$

Por lo tanto

$$\sigma(tr(x)) = \sum_{i=1}^{d} \sigma^{i+1}(x),$$

como los σ^i son todos los integrantes del grupo de Galois, esta nueva suma vuelve a incluirlos a todos y tenemos $\sigma(tr(x)) = tr(x)$, luego $tr(x) \in \mathbb{F}$. Para ver que es lineal sólo hace falta recordar la ecuación (1.1) y que para todo $\lambda \in \mathbb{F}$, $\lambda^q = \lambda$ luego para todo $x \in \mathbb{K}$, $\sigma(\lambda x) = \lambda^q x^q = \lambda\sigma(x)$.

□

1.2. Cuerpos de descomposición

Vamos a ver que los cuerpos de cardinal $q = p^n$ se pueden ver como un tipo especial de cuerpos, los cuerpos de descomposición, esto los dota de una estructura particular.

Nota. Recordamos que si $\mathbb{F}$ es un cuerpo y $f(X) \in \mathbb{F}[X]$ un polinomio irreducible entonces $\mathbb{F}[X]/(f(X))$, el anillo cociente de $\mathbb{F}[X]$ por el ideal engendrado por $f(X)$, es un cuerpo.

Proposición 1.22. *Sea $\mathbb{F}$ un cuerpo; dado $f(X) \in \mathbb{F}[X]$, existe una extensión $\mathbb{K}/\mathbb{F}$ en la que $f(X)$ tiene una raíz.*

Demostración. Podemos suponer que $f(X)$ es irreducible, si no es así, basta con coger uno de sus factores irreducibles. Si consideramos el siguiente cuerpo:

$$\mathbb{K} = \mathbb{F}/(f(X))$$

Podemos ver $\mathbb{F}$ embebido en él mediante el morfismo $\phi : \mathbb{F} \to \mathbb{K}$ que lleva $z \in \mathbb{F}$ en $\phi(z) = \bar{z}$ su clase en $\mathbb{K}$. En este cuerpo la clase $\bar{X}$ es una raíz de $f(X)$.

□

Corolario 1.23. *Dado un cuerpo $\mathbb{F}$ y un polinomio $f(X) \in \mathbb{F}[X]$ existe una extensión $\mathbb{K}/\mathbb{F}$ en la que $f(X)$ se descompone en factores lineales $f(X) = (X-\alpha_1)\cdots(X-\alpha_n)$*

Demostración. La demostración consiste en la aplicación reiterada de la proposición anterior.

□

Definición 1.24. *Si α es una raíz de $f(X) \in \mathbb{F}[X]$ su multiplicidad, n, es el máximo entero de forma que $(X-\alpha)^n$ divide a $f(X)$. Si $n > 1$ decimos que se trata de una raíz múltiple y si no, decimos que la raíz es simple.*

Definición 1.25. *Un polinomio $f(X) \in \mathbb{F}[X]$ irreducible es separable si no tiene raíces múltiples en ninguna extensión de $\mathbb{F}$.*

Definición 1.26. *Sea $\mathbb{F}$ un cuerpo y $f(X) \in \mathbb{F}[X]$ un polinomio. Un cuerpo de descomposición de $f(X)$ es una extensión $\mathbb{K}/\mathbb{F}$ que cumple:*

(I) *$f(X)$ se descompone en factores lineales.*

(II) *Es la extensión más pequeña que contiene a todas las raíces de* $f(X)$.

Definición 1.27. *Sea* $f(X) \in \mathbb{F}[X]$ *un polinomio con la forma*

$$f(X) = a_0 + a_1X + \cdots + a_nX^n,$$

su derivada formal es un polinomio $f'(X) \in \mathbb{F}[X]$ *con la forma*

$$f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Teorema 1.28. *Un polinomio* $f(X) \in \mathbb{F}[X]$ *no tiene raíces múltiples si y sólo si* $f(X)$ *y su derivada formal* $f'(X)$ *no tienen raíces en común.*

Demostración. Siempre existe; por el corolario 1.23 una extensión en la que:

$$f(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_n)^{e_n}$$

con $\alpha_i \neq \alpha_j$ si $i \neq j$. La derivada formal es:

$$f'(X) = \sum_{i=1}^{n} \left[e_i(X - \alpha_i)^{e_i - 1} \prod_{j \neq i} (X - \alpha_j)^{e_j} \right]$$

Si $X - \alpha_i$ divide a $f'(X)$, divide a todos los sumandos. Por lo tanto; no tienen raíces en común si y sólo si, $e_i = 1$ para todo i.

□

Corolario 1.29. *Un polinomio irreducible* $f(X)$ *es separable si y sólo si* $f'(X) \neq 0$.

Demostración. Como $deg(f') < deg(f)$ y $f(X)$ es irreducible, si $f'(X) \neq 0$ no pueden tener raíces en común.

□

Teorema 1.30. *Sea* $q = p^n$ *y* $\mathbb{F}_q$ *un cuerpo finito de* q *elementos, entonces* $\mathbb{F}_q$ *es el conjunto de raíces del polinomio* $g(X) = X^q - X \in \mathbb{F}_p$ *y en consecuencia es el cuerpo de descomposición de* $g(X)$ *sobre* $\mathbb{F}_q$.

Demostración. Sabemos que $\mathbb{F}_q^*$ es cíclico de orden $q - 1$ luego todos sus elementos son raíces de $X^q - X$ y como 0 también lo es, todos los elementos de $\mathbb{F}_q$ lo son.

Por otra parte, $f'(X) = -1$ luego es separable y no existe ninguna extensión en la que tenga raíces múltiples, por lo tanto, es el cuerpo más pequeño en el que $g(X)$ descompone en factores líneales, es decir, el cuerpo de descomposición.

□

Definición 1.31. *Dado un cuerpo* $\mathbb{F}$*, decimos que* $a \in \mathbb{F}$ *es un cuadrado, si existe* $b \in \mathbb{F}$ *de forma que* $a = b^2$.

Proposición 1.32. *Dado un cuerpo finito* $\mathbb{F}$ *de característica distinta de 2:*

- *El único elemento de orden 2 es -1.*

- *-1 es un cuadrado si y sólo si* $q \equiv 1(mod\ 4)$.
- *Dados dos elementos* $a, b \in \mathbb{F}$ *que no son cuadrados, su producto* ab *es un cuadrado.*
- *Dados dos elementos* $a, b \in \mathbb{F}$ *si uno es un cuadrado y el otro no, entonces su producto no es un cuadrado.*

Demostración. Hemos visto en 1.8 que $\mathbb{F}^*$ es un grupo cíclico, luego existe un $a \in \mathbb{F}$ de forma que:

$$\mathbb{F} = \{0, a^{q-1} = 1, a, a^2, \ldots, a^{q-2}\}$$

Si tomamos un elemento a^l $(1 \leq l \leq q-2)$ de orden 2, entonces $a^{2l} = a^{q-1}$. Como $\mathbb{F}$ no tiene característica 2, q es un número impar y podemos deducir $l = \frac{q-1}{2}$. Por lo tanto existe un único elemento de orden dos y es $a^{\frac{q-1}{2}}$. Veamos ahora que -1, es decir, el opuesto de 1 para la suma, tiene orden 2:

$$0 = ((-1)+1)^2 = (-1)^2 + 1 - 1 - 1 = (-1)^2 - 1 \iff (-1)^2 = 1$$

Por lo tanto, el único elemento de orden dos es -1.
De la representación anterior de $\mathbb{F}$ podemos deducir que los cuadrados de $\mathbb{F}$ son exactamente los siguientes:

$$\{0, 1, a^2, a^4, \ldots, a^{2r}, \ldots, a^{q-3}\}$$

De lo que se deducen fácilmente los dos últimos puntos.

□

1.3. Aspectos prácticos

Una vez hemos explicado algunas de las propiedades más importantes de los cuerpos finitos; en esta última sección explicaremos brevemente como se opera con ellos. Hemos visto que todos los cuerpos tienen orden $q = p^n$ donde p es un número primo, evidentemente, si $n = 1$ se trabaja en el cuerpo de los enteros módulo p, es decir, $\mathbb{F}_p = \mathbb{Z}_p$.

Si por el contrario, $n \neq 1$ Sabemos que $\mathbb{Z}_{p^n}$ no es un cuerpo. En este caso, para trabajar con $\mathbb{F}_q$ necesitamos un polinomio irreducible de grado n en $\mathbb{F}_p[X]$, que siempre existe. De hecho, excepto en el caso de un polinomio de grado dos sobre $\mathbb{F}_2$ se pueden elegir varios polinomios, que producen cuerpos isomorfos. Una vez hemos elegido un polinomio, $p(X)$, irreducible de grado n, operar en el cuerpo se reduce a operar con las clases en $\mathbb{F}_p[X]/(p(X))$.

En la práctica, puesto que cualquier polinomio $f(X) \in \mathbb{F}_p[X]$ se puede escribir (gracias al algoritmo de división de Euclides) como $f(X) = q(X)p(X) + r(X)$ se opera con los polinomios de grado estrictamente menor que n con coeficientes en $\mathbb{F}_p$. La suma dentro de $\mathbb{F}_q$ es la suma usual y el producto es el resto de la división del producto

usual entre $p(X)$. Para facilitar este cálculo el polinomio $p(X)$ se suele tomar mónico y de forma que $p(X) - X^n$ tenga el menor grado posible.

Otro cálculo que puede resultar interesante es el del inverso de un elemento, para ello se utiliza el algoritmo de Euclides extendido.

Capítulo 2

Geometrías afín y proyectiva

En este capítulo introducimos las geometrías afín y proyectiva de dimensión n sobre el cuerpo finito de orden q, $\mathbb{F}_q$. Los espacios proyectivo y afín se definen adaptando las definiciones de los espacios sobre los cuerpos real y complejo que aparecen en [Cas], el conteo de subespacios y la equivalencia de los axiomas se hacen siguiendo [BeuRos] y [Hall].

Sobre estos dos espacios, $\mathbb{P}^n(\mathbb{F}_q)$ y $\mathbb{A}^n(\mathbb{F}_q)$, se asentará gran parte del resto del trabajo.

2.1. El espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$

Los espacios proyectivos se pueden construir de forma axiomática como más adelante comentaremos. Sin embargo, nosotros lo definiremos partiendo directamente de un espacio vectorial $\mathbb{F}_q^{n+1}$ que nos hará más fácil operar en el espacio.

Definición 2.1. *Un espacio proyectivo de dimensión $n \in \mathbb{N}$ sobre $\mathbb{F}_q$, $\mathbb{P}^n(\mathbb{F}_q)$, es un conjunto relacionado con $\mathbb{F}_q^{n+1}$ por una aplicación sobreyectiva*

$$\pi : \mathbb{F}_q^{n+1} - \{0\} \to \mathbb{P}^n(\mathbb{F}_q),$$

que cumple:

$$\pi(v) = \pi(w) \iff \text{existe } \lambda \in \mathbb{F}_q^* \quad \text{tal que} \quad v = \lambda w.$$

A los elementos de $\mathbb{P}^n(\mathbb{F}_q)$ se los llama puntos. Si $\pi(v) = p \in \mathbb{P}^n(\mathbb{F}_q)$ se dice que v es un representante de (o representa a) p.

A los subconjuntos de $\mathbb{P}^n(\mathbb{F}_q)$ que conservan las propiedades del espacio total se los denomina subespacios.

Definición 2.2. *Dado un subconjunto $L \subset \mathbb{P}^n(\mathbb{F}_q)$; se dice que es un subespacio proyectivo de $\mathbb{P}^n(\mathbb{F}_q)$ si existe un subespacio lineal $F \subset \mathbb{F}_q^{n+1}$ de forma que $L = \pi(F - \{0\})$. De nuevo, se dice que F representa a L.*

Nota. Si $\{v_1, \ldots, v_t\}$ es un conjunto de vectores en $\mathbb{F}_q^n$ denotaremos el subespacio vectorial que generan por: $\langle v_1 \ldots, v_t \rangle$.

De la definición de $\mathbb{P}^n(\mathbb{F}_q)$, podemos deducir que a cada punto $P \in \mathbb{P}^n(\mathbb{F}_q)$ lo representa el subespacio vectorial $\langle \pi^{-1}(P) \rangle$ y es por lo tanto un subespacio proyectivo, más adelante veremos que de dimensión 0.

Proposición 2.3. *Si un subespacio proyectivo $L \subset \mathbb{P}^n(\mathbb{F}_q)$ es representado por $F \subset \mathbb{F}_q^{n+1}$, entonces $F - \{0\} = \pi^{-1}(L)$*

Demostración. Sea $L \subset \mathbb{P}^n(\mathbb{F}_q)$ un subespacio proyectivo y F un subespacio vectorial en $\mathbb{F}_q^{n+1}$ que representa a L. Si $v \neq 0$ está en $\pi^{-1}(L)$ entonces, porque F representa a L, existe $w \in F - \{0\}$ de forma que $\pi(v) = \pi(w)$. Por la forma en que se define $\mathbb{P}^n(\mathbb{F}_q)$ sabemos que existe $\lambda \in \mathbb{F}_q^*$ tal que $v = \lambda w$ y por lo tanto, $v \in F - \{0\}$. Así probamos $F - \{0\} \supset \pi^{-1}(L)$. La otra contención, $F - \{0\} \subset \pi^{-1}(L)$, es evidente por la definición de representante.

□

Corolario 2.4. *Si $L_1 = \pi(F_1)$ y $L_2 = \pi(F_2)$ son dos subespacios proyectivos. Entonces $L_1 \subset L_2$ si y sólo si $F_1 \subset F_2$*

Demostración. Si $F_1 \subset F_2$ entonces $L_1 = \pi(F_1 - \{0\}) \subset \pi(F_2 - \{0\}) = L_2$. Recíprocamente, si $L_1 \subset L_2$ tenemos $F_1 = \pi^{-1}(L_1 - \{0\}) \subset \pi^{-1}(L_2 - \{0\}) = F_2$

□

La proposición 2.3 deja claro que cada subespacio lineal representa un único subespacio proyectivo. Parece entonces lógico, definir la dimensión de subespacio proyectivo relacionándola con la del subespacio lineal que lo representa.

Definición 2.5. *Dado un subespacio proyectivo $L \subset \mathbb{P}^n(\mathbb{F}_q)$; diremos que tiene dimensión d, si su representante F es un subespacio vectorial de dimensión $d+1$.*

- *Por convenio se define la dimensión de $\emptyset$ como -1.*
- *Cada punto es un subespacio de dimensión 0.*
- *Los subespacios proyectivos de dimensión 1 se denominan rectas.*
- *Los supespacios proyectivos de dimensión $n-1$ se denominan hiperplanos.*

Proposición 2.6. *Si $L \subset \mathbb{P}^n(\mathbb{F}_q)$ es un subespacio proyectivo de dimensión d, entonces es un espacio proyectivo de dimensión d.*

Demostración. Sea F el representante de L, entonces es un subespacio vectorial de dimensión $d+1$; por lo tanto, existe un isomorfismo lineal de F con ${\mathbb{F}_q}^{d+1}$:

$$\varphi : {\mathbb{F}_q}^{d+1} \to F$$

Componiendo φ con $\pi|_F$, la aplicación de la definción de espacio proyectivo restringida a F, tendremos una aplicación $\pi \circ \varphi : {\mathbb{F}_q}^{d+1} \to L$ que cumple las condiciones para definir un espacio proyectivo de dimensión d, veámoslo. Sean dos vectores $v, w \in {\mathbb{F}_q}^{d+1}$, de forma que $\pi \circ \varphi(v) = \pi \circ \varphi(w)$; entonces por las propiedades de π tenemos $\varphi(v) = \lambda\varphi(w)$ para algún $\lambda \in \mathbb{F}_q$. Finalmente, como φ es un isomorfismo, podemos deducir $v = \lambda w$.

□

Definición 2.7. *Dados tres números naturales $n, d, q \in \mathbb{N}$, el coeficiente gaussiano* $\begin{bmatrix} n \\ d \end{bmatrix}_q$ *se define como sigue:*

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{d-1})}{(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})}.$$

Proposición 2.8. *Dado un espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$; el numero exacto de subespacios proyectivos de dimensión d que contiene es* $\begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$.

Demostración. Como hemos visto, existe una correspondencia biunívoca entre los subespacios proyectivos de dimensión d contenidos en $\mathbb{P}^n(\mathbb{F}_q)$ y los subespacios lineales de dimensión $d+1$ de $\mathbb{F}_q^{n+1}$. Por lo tanto, para probar la proposición nos basta con contar estos últimos. Cada subespacio de dimensión $d+1$ queda definido por $d+1$ vectores linealmente independientes. Hay $q^{n+1}-1$ formas de elegir un vector no nulo en ${\mathbb{F}_q}^{n+1}$, $q^{n+1}-q$ formas de elegir un segundo vector independiente del anterior; de esta forma podemos ver que hay

$$\left(q^{n+1}-1\right)\left(q^{n+1}-q\right)\cdots\left(q^{n+1}-q^d\right)$$

formas de elegir estos $d+1$ vectores. Sin embargo, varias de estas elecciones pueden conducir al mismo subespacio. Siguiendo el mismo proceso que antes para elegir $d+1$ vectores linealmente independientes, pero ya en el interior de un subespacio de dimensión $d+1$, tenemos

$$\left(q^{d+1}-1\right)\left(q^{d+1}-q\right)\cdots\left(q^{d+1}-q^d\right)$$

formas de hacerlo, que definen el mismo subespacio. Por lo tanto, el número de subespacios proyectivos de dimensión d es:

$$\frac{\left(q^{n+1}-1\right)\left(q^{n+1}-q\right)\cdots\left(q^{n+1}-q^d\right)}{\left(q^{d+1}-1\right)\left(q^{d+1}-q\right)\cdots\left(q^{d+1}-q^d\right)}.$$

□

En particular, esta proposición da cuenta del número de puntos que contiene cada espacio proyectivo de dimensión n, tomando los puntos como los subespacios de dimensión 0 tenemos:

$$\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \cdots + 1.$$

Proposición 2.9. *Dado un subespacio proyectivo $L \subset \mathbb{P}^n(\mathbb{F}_q)$ de dimensión k existen* $\begin{bmatrix} n-k \\ d-k \end{bmatrix}_q$ *subespacios de dimensión d con $d \geq k$ que contienen a L.*

Demostración. Razonando como en la proposición anterior y apoyados en el corolario 2.4 tenemos que contar los subespacios de dimensión $d+1$ en $\mathbb{F}_q^{n+1}$ que contienen a $\pi^{-1}(L) \cup \{0\} = F$. Necesitamos elegir $d-k$ vectores en $\mathbb{F}_q^{n+1}$ de forma que ellos y el subespacio F, de dimensión $k+1$, sean linealmente independientes. Podemos elegir $\left(q^{n+1} - q^{k+1}\right)$ vectores fuera de F, después de esto podemos elegir $\left(q^{n+1} - q^{k+2}\right)$ linealmente independientes de F y el vector anterior. Así podemos definir un subespacio vectorial de dimensión $d+1$ que contenga a F de

$$\left(q^{n+1} - q^{k+1}\right)\left(q^{n+1} - q^{k+2}\right)\cdots\left(q^{n+1} - q^{d}\right)$$

formas. Sin embargo, igual que antes estamos contando subespacios repetidos, puesto que hay

$$\left(q^{d+1} - q^{k+1}\right)\left(q^{d+1} - q^{k+2}\right)\cdots\left(q^{d+1} - q^{d}\right)$$

formas de generar el mismo subespacio a partir de F. Por lo tanto el número de subespacios que contienen a F y tienen dimensión $d+1$ es:

$$\frac{\left(q^{n+1} - q^{k+1}\right)\left(q^{n+1} - q^{k+2}\right)\cdots\left(q^{n+1} - q^{d}\right)}{\left(q^{d+1} - q^{k+1}\right)\left(q^{d+1} - q^{k+2}\right)\cdots\left(q^{d+1} - q^{d}\right)}$$

Si ahora sacamos factor común a q^{k+1} en cada término tanto en numerador como en denominador:

$$\frac{\left(q^{n-k} - 1\right)\left(q^{n-k} - q\right)\cdots\left(q^{n-k} - q^{d-k-1}\right)}{\left(q^{d-k} - 1\right)\left(q^{d-k} - q\right)\cdots\left(q^{d-k} - q^{d-k-1}\right)} = \begin{bmatrix} n-k \\ d-k \end{bmatrix}_q$$

□

Utilizando esta proposición para calcular el número de rectas que contienen a un punto, es decir, $k=0$ y $d=1$ obtenemos:

$$\begin{bmatrix} n \\ 1 \end{bmatrix}_q = \frac{q^n - 1}{q-1} = q^{n-1} + q^{n-2} + \cdots + 1$$

Existen más espacios proyectivos que los que hemos definido. En general se puede definir espacio proyectivo como todo conjunto que cumple las condiciones que enunciamos en el siguiente teorema.

Teorema 2.10. *Dado un espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$ se cumple:*

I *Dados dos puntos diferentes $P, Q \in \mathbb{P}^n(\mathbb{F}_q)$ existe una única recta que llamaremos PQ que contiene a ambos.*

II *Dados cuatro puntos diferentes de forma que no haya tres en la misma recta $A, B, C, D \in \mathbb{P}^n(\mathbb{F}_q)$; si AB y CD tienen intersección no vacía y $P \in AB \cap CD$; entonces, AC y BD se intersecan en un punto Q.*

III *Cada recta tiene al menos 3 puntos*

Demostración. Demostraremos los puntos uno por uno:

I Dado $P \in \mathbb{P}^n(\mathbb{F}_q)$; existe $v \in \mathbb{F}_q^{n+1}$, de forma que $\pi(v) = P$ y ya hemos visto que $\pi^{-1}(P) = \langle v \rangle$. Como $Q \neq P$ dado $w \in \mathbb{F}_q^{n+1}$, representante de Q; no existe $\alpha \in \mathbb{F}_q$ de forma que se cumpla $v = \alpha w$, es decir, son linealmente independientes. Por lo tanto, v y w generan un subespacio lineal de dimensión 2. El subespacio vectorial $\langle v, w \rangle \subset \mathbb{F}_q^{n+1}$ es el único de dimensión 2 que contiene a los representantes de P y a los de Q. Luego, $\pi(\langle v, w \rangle - \{0\})$ es la única recta que contiene a ambos.

II Dados cuatro puntos distintos $A, B, C, D \in \mathbb{P}^n(\mathbb{F}_q)$; existen vectores v_A, v_B, v_C, v_D en $\mathbb{F}_q^{n+1}$ que son representantes de cada punto respectivamente. Además, los vectores v_A, v_B, v_C, v_D son independientes dos a dos, porque representan puntos distintos. Como hemos visto en la demostración anterior, el subespacio $\langle v_A, v_B \rangle$ representa a la recta AB y el subespacio $\langle v_C, v_D \rangle$ hace lo propio con CD. Como $P \in AB \cap CD$ si v_P es un representante de P tendremos que $v_P \in \langle v_A, v_B \rangle \cap \langle v_C, v_D \rangle$. Luego v_P se puede escribir de las formas siguientes:

$$v_P = \lambda_1 v_A + \lambda_2 v_B,$$
$$v_P = \alpha_1 v_C + \alpha_2 v_D,$$

Si ahora definimos $v_Q = \lambda_1 v_A - \alpha_1 v_C$ el punto $Q = \pi(v_Q)$ pertenece a la recta AC, también está en BD porque restando las dos expresiones para v_P tenemos $v_Q = \lambda_1 v_A - \alpha_1 v_C = \alpha_2 v_D - \lambda_2 v_B$. Ya hemos encontrado el punto que buscábamos.

III Si una recta $r \subset \mathbb{P}^n(\mathbb{F}_q)$ está representada por $\langle v_1, v_2 \rangle$, siendo v_1 y v_2 independientes al menos existen tres puntos en ella: $\pi(v_1), \pi(v_2)$ y $\pi(v_1 + v_2)$.

□

Coordenadas homogéneas

Para trabajar de forma más cómoda en $\mathbb{P}^n(\mathbb{F}_q)$ introducimos las referencias y las coordenadas. Comenzamos por generalizar la noción de puntos no alineados, la idea es poder conseguir un conjunto de puntos que tengan la menor relación posible entre ellos.

Definición 2.11. *Dado un conjunto de puntos $\{P_0, \ldots, P_t\} \subset \mathbb{P}^n(\mathbb{F}_q)$, se dice que es independiente si los vectores que los representan son linealmente independientes.*

Definición 2.12. *Dado un conjunto de puntos $\{P_0, \ldots, P_t\} \subset \mathbb{P}^n(\mathbb{F}_q)$ y un representante de cada uno $\{v_0, \ldots, v_t\} \subset \mathbb{F}_q^{n+1}$, se define el subespacio proyectivo generado por $P_0 \ldots, P_t$, como el subespacio proyectivo representado por $\langle v_0, \ldots, v_t \rangle$ y se denota:*

$$P_0 + \cdots + P_t = \pi(\langle v_0, \ldots, v_t \rangle).$$

De ahora en adelante el símbolo $\hat{\cdot}$ indicará que el elemento sobre el que está queda excluído de la expresión.

Definición 2.13. *Dado $\mathbb{P}^n(\mathbb{F}_q)$, un espacio proyectivo; un conjunto de $n+2$ puntos, $\Lambda = \{P_0, \ldots, P_n, A\}$ es una referencia proyectiva si cumple:*

I *El conjunto de puntos $\{P_0, \ldots, P_n\}$ es independiente.*

II *Para cada $i = 0, \ldots, n$, se tiene que $A \notin P_0 + \cdots + \hat{P}_i + \cdots + P_n$.*

Nota. Otra forma completamente equivalente de definir referencia es cambiar esas dos condiciones por:

"Dados $n+1$ puntos de Λ, son siempre independientes."

Definición 2.14. *Dada una base de $\mathbb{F}_q^{n+1}$, $\mathcal{B} = \{v_0, \ldots, v_n\}$; se dice que es una base adaptada a una referencia Λ si para cada $i = 0, \ldots, n$; el vector v_i es un representante de P_i y además $v_0 + \cdots + v_t$ es representante de A.*

Proposición 2.15. *Dada una referencia $\Lambda = \{P_0, \ldots, P_n, A\} \subset \mathbb{P}^n(\mathbb{F}_q)$ existe una base adaptada a ella.*

Demostración. Sea Λ una referenia proyectiva. La primera condición en 2.13 nos dice que si v_i es un representante de P_i para cada i, entonces los v_i forman una base de $\mathbb{F}_q^{n+1}$. De esta forma, dado v_A un representante de A; se puede escribir de manera única como combinación lineal de ellos, es decir, $v_A = \lambda_0 v_0 + \cdots \lambda_n v_n$. La segunda condición nos dice que ninguno de los coeficientes en dicha combinación puede ser nulo, de lo contrario, si existiese un $\lambda_i = 0$, podríamos expresar v_A como combinación lineal de v_j con $j \neq i$ por lo que A estaría en $P_0 + \cdots + \hat{P}_i + \cdots + P_n$. Si tomamos como nueva base $\mathcal{S} = \{\lambda_0 v_0, \ldots, \lambda_n v_n, \}$ es una base adaptada a Λ.

□

Proposición 2.16. *Dada en $\mathbb{P}^n(\mathbb{F}_q)$ una referencia $\Lambda = \{P_0, \ldots, P_n, A\}$, si $\mathcal{B} = \{v_0, \ldots, v_n\}$ y $\mathcal{S} = \{w_0, \ldots, w_n\}$ son dos bases adaptadas a Λ, entonces existe $\lambda \in \mathbb{F}_q^*$ de forma que $v_i = \lambda w_i$ para todo $I = 0, \ldots, n$.*

Demostración. Puesto que para cada P_i, v_i y w_i son representantes, para cada i existe $\lambda_i \in \mathbb{F}_q^*$ de forma que $v_i = \lambda_i w_i$. Por otra parte, si definimos $v_A = \sum_{i=0}^n v_i$; por ser $\mathcal{B}$ una base adaptada, es un representante de A, igual que antes, existe $\lambda \in \mathbb{F}_q^*$ de forma que $v_A = \lambda \sum_{i=0}^n w_i$. Juntando todo obtenemos:

$$v_a = \sum_{i=0} \lambda_i v_i = \lambda \sum_{i=1}^{n} w_i.$$

Como $\mathcal{S}$ es una base, la representación de v_A en ella debe ser única, es decir $\lambda_i = \lambda$ para todo i.

□

Ahora ya estamos en condiciones de definir las coordenadas de un punto en $\mathbb{P}^n(\mathbb{F}_q)$ con respecto a una determinada referencia.

Definición 2.17. *Dado un punto $P \in \mathbb{P}^n(\mathbb{F}_q)$, una referencia proyectiva Λ y una base adaptada a Λ, $\mathcal{B}$; decimos que el punto P tiene coordenadas $(x_0, \ldots, x_n)$ si el vector expresado con esas coordenadas en $\mathcal{B}$ es un representante de P.*

En particular, las coordenadas de los elementos de la base son:

$$\begin{aligned} p_0 &= (1, 0, \ldots, 0), \\ &\vdots \\ p_n &= (0, \ldots, 0, 1), \\ A &= (1, 1, \ldots, 1). \end{aligned}$$

De la misma forma que no había unicidad en las bases adaptadas no la hay en la en las coordenadas, pero igual que las bases, si un punto tiene dos coordenadas diferentes $(x_i, \ldots, x_n)$ y $(y_0, \ldots, y_n)$ existe $\lambda \in \mathbb{F}_q^*$ de forma que $x_i = \lambda y_i$. Resulta evidente entonces, que si con estas coordenadas en $\mathbb{F}_q^{n+1}$ se representa un subespacio lineal, L, ya sea con ecuaciones implícitas o explícitas, entonces en $\mathbb{P}^n(\mathbb{F}_q)$ representan el subespacio proyectivo que L representa, esto es, $\pi(L)$.

2.2. El espacio afín $\mathbb{A}^n(\mathbb{F}_q)$

Igual que en el caso proyectivo, definimos el espacio afín partiendo directamente de una estructura vectorial.

Definición 2.18. *La geometría afín de dimensión n sobre $\mathbb{F}_q$, $\mathbb{A}^n(\mathbb{F}_q)$; es un conjunto de q^n elementos, llamados puntos, relacionados entre sí por medio de una aplicación:*

$$\begin{aligned} \mathbb{A}^n(\mathbb{F}_q) \times {\mathbb{F}_q}^n &\to \mathbb{A}^n(\mathbb{F}_q) \\ (P, v) &\mapsto P + v, \end{aligned}$$

que cumple las siguientes propiedades:

I $P + (v + w) = (P + v) + w$ *para todo* $P \in \mathbb{A}^n(\mathbb{F}_q)$ *y* $v, w \in {\mathbb{F}_q}^n$.

II $P + 0 = P$ *para todo* $P \in \mathbb{A}^n(\mathbb{F}_q)$.

III *Para cada dos puntos* $P, Q \in \mathbb{A}^n(\mathbb{F}_q)$ *existe un único vector* $v \in {\mathbb{F}_q}^n$, *de forma que* $P + v = Q$, *se denota* $v = \vec{PQ}$.

Definición 2.19. *Sea $\mathbb{A}^n(\mathbb{F}_q)$ un espacio afín y $F \subset \mathbb{F}_q^n$ un subespacio vectorial de dimensión d; se dice que el conjunto L es un subespacio afín de dimensión d y F su subespacio director si:*

$$L = P + F := \{P + v : v \in F\}$$

- *Los puntos son subespacios afines de dimensión 0.*
- *A los subespacios afines de dimensión 1 se les llama rectas.*
- *A los subespacios afines de dimensión 2 se les llama planos.*

- *A los subespacios afines de dimensión $n-1$ se les llama hiperplanos.*

Nota. De la propiedad (III) de la definición de $\mathbb{A}^n(\mathbb{F}_q)$ se deduce que un subespacio de dimensión d tiene exactamente q^d puntos.

Pese a que en la definición de subespacio afín aparece un punto P, este no es el único que puede definir dicho espacio, de hecho cualquier punto contenido en el subespacio es válido.

Proposición 2.20. *Dados dos puntos $P, Q \in \mathbb{A}^n(\mathbb{F}_q)$ y un subespacio lineal $F \subset \mathbb{F}_q^n$; la igualdad $P + F = Q + F$ es cierta si y sólo si $Q \in P + F$.*

Demostración. Si $Q + F = P + F$ es evidente que $Q \in P + F$. Por otra parte, si $Q = P + v$ con $v \in F$ cualquier punto $A \in Q + F$ se puede escribir como $A = Q + w = P + v + w$ con $w \in F$. Luego $Q + F \subset P + F$. Para probar la contención contraria basta con observar que $Q = P + v \iff Q = P - v$.

□

Proposición 2.21. *Dados dos subespacios afines $L = P + F$ y $L' = P' + F'$; se cumple $L \subset L'$ si y sólo si $F \subset F'$ y además $L \cap L' \neq \emptyset$*

Demostración. Si tenemos $L \subset L'$ es evidente que la intersección de ambos conjuntos no será vacía. Si tomamos Q, un punto de dicha intersección, la proposición anterior nos dice que podemos escribir $L = Q + F$ y $L' = Q + F'$. Por lo tanto, si tomamos $v \in F$ el punto $Q + v$ pertenecerá a L luego $Q + v \in L'$ y por lo tanto $v \in F'$, es decir $F \subset F'$. Para probar el recíproco, tomamos de nuevo $Q \in L \cap L'$ y volvemos a expresar L y L' como antes. Sea $P \in L$ entonces $P = Q + v$ con $v \in L \subset L'$ luego $P \in L'$.

□

Proposición 2.22. *Sea $L = P + F \subset \mathbb{A}^n(\mathbb{F}_q)$ un subespacio afín de dimensión k; entonces existen $\begin{bmatrix} n-k \\ d-k \end{bmatrix}_q$ subespacios afines de dimensión d que lo contienen.*

Demostración. Por lo visto en las dos proposiciones, 2.20 y 2.21 nos basta con contar el número de subespacios lineales de dimensión d en $\mathbb{F}_q^n$, que contienen a F. Para hacerlo se procede igual que en la demostración de 2.9, pero ajustando la dimensión. Llegando a la conclusión de que el número exacto es:

$$\begin{bmatrix} n-k \\ d-k \end{bmatrix}_q = \frac{(q^{n-k}-1)(q^{n-k}-q)\cdots(q^{n-k}-q^{d-k-1})}{(q^{d-k}-1)(q^{d-k}-q)\cdots(q^{d-k}-q^{d-k-1})}.$$

□

Definición 2.23. *Dados dos subespacios afines $L, L' \subset \mathbb{A}^n(\mathbb{F}_q)$ con subespacios directores F y F' respectivamente, se dice que son paralelos si tienen intersección vacía y se tiene $F \subset F'$ ó $F' \subset F$.*

En la siguiente proposición se listan unas propiedades que cumplen los espacios afines.

Teorema 2.24. *Dado un espacio afín $\mathbb{A}^n(\mathbb{F}_q)$, cumple las siguientes afirmaciones:*

I *Dados dos puntos $P, Q \in \mathbb{A}^n(\mathbb{F}_q)$ existe una única recta que contiene a ambos.*

II *Dada una recta $r \subset \mathbb{A}^n(\mathbb{F}_q)$ y un punto $P \in \mathbb{A}^n(\mathbb{F}_q)$ no contenido en r, existe una única recta paralela a r que contenga a P.*

III *Una recta contiene al menos dos puntos.*

Demostración. Lo probaremos por separado:

I Sean $P, Q \in \mathbb{A}^n(\mathbb{F}_q)$ dos punos diferentes; por (III) en la definición de $\mathbb{A}^n(\mathbb{F}_q)$ existe un único vector, $v = \vec{PQ}$ de forma que $Q = P + v$. La recta $r = P + v$ contiene a ambos puntos. Si otra recta, l, contiene a ambos puntos, su subespacio director debe ser el generado por v, y evidentemente la intersección $r \cap l \neq \emptyset$, luego por 2.20 tendremos $r = l$.

II Sea una recta $r \subset \mathbb{A}^n(\mathbb{F}_q)$ y un punto $P \in \mathbb{A}^n(\mathbb{F}_q) - r$. Por la definición de subespacio paralelo y la proposición 2.20, dos rectas son paralelas si y sólo si comparten subespacio director y tienen un punto común. Por lo tanto el subespacio director de r y el punto P definen una única recta paralela a r que pase por P.

III Cualquier recta se puede representar como $P + \langle v \rangle$ con $v \in \mathbb{F}_q^n$ y $P \in \mathbb{A}^n(\mathbb{F}_q)$, por lo tanto, la recta contiene al menos a P y a $P + v$.

□

Esta lista de propiedades en muchos casos se toma como una serie de axiomas que debe cumplir una estructura para constituir un espacio afín.

Coordenadas afines

Definición 2.25. *En el espacio afín $\mathbb{A}^n(\mathbb{F}_q)$ una referencia $\mathcal{R} = \{O, \mathcal{B}\}$, está formada por un punto $O \in \mathbb{A}^n(\mathbb{F}_q)$ y una base vectorial $\mathcal{B} \subset \mathbb{F}_q^n$.*

Definición 2.26. *Dada una referencia afín $\mathcal{R} = \{O, \mathcal{B}\}$ de $\mathbb{A}^n(\mathbb{F}_q)$ se dice que un punto tiene coordenadas $(x_1, \ldots, x_n)$ en dicha referencia si el vector v que cumple $O + v = P$ tiene esas coordenadas en la base $\mathcal{B}$.*

Una vez fijamos una referencia afín $\mathcal{R}$ los puntos cuyas coordenadas son solución de un sistema de ecuaciones lineales independientes de la forma:

$$\begin{cases} a_1 &= a_1^1 x_1 + \cdots + a_1^n x_n, \\ a_2 &= a_2^1 x_1 + \cdots + a_2^n x_n, \\ & \vdots \\ a_{n-d} &= a_{n-d}^1 x_1 + \cdots + a_{n-d}^n x_n. \end{cases}$$

Forman un subespacio afín de dimensión d. Estas son sus ecuaciones implícitas. También se puede definir un subespacio con ecuaciones paramétricas. Si $(p_1, \ldots, p_n)_{\mathcal{R}} \equiv P$

es un punto y $\langle v^1, \dots v^d \rangle = L$ es un subespacio de dimensión d, todos los puntos de $P + L$ se pueden representar en coordenadas como sigue:

$$\begin{cases} x_1 &= p_1 + \lambda_1 v_1^1 + \lambda_2 v_1^2 + \cdots + \lambda_d v_1^d, \\ x_2 &= p_2 + \lambda_1 v_2^1 + \lambda_2 v_2^2 + \cdots + \lambda_d v_2^d, \qquad \textit{con } \lambda_i \in \mathbb{F}_q. \\ & \vdots \\ x_n &= p_n + \lambda_1 v_n^1 + \lambda_2 v_n^2 + \cdots + \lambda_d v_n^d, \end{cases}$$

2.3. Inmersión de $\mathbb{A}^n(\mathbb{F}_q)$ en $\mathbb{P}^n(\mathbb{F}_q)$

Vamos a ver como $\mathbb{A}^n(\mathbb{F}_q)$ se puede ver como una parte $\mathbb{P}^n(\mathbb{F}_q)$, de hecho vamos a ver que $\mathbb{A}^n(\mathbb{F}_q)$ es todo $\mathbb{P}^n(\mathbb{F}_q)$ excepto un hiperplano proyectivo al que llamaremos el hiperplano del infinito.

Lema 2.27. *Dado un hiperplano cualquiera $H_\infty \subset \mathbb{P}^n(\mathbb{F}_q)$, existe una referencia $\mathcal{R}$ en la que $P \in H_\infty$, si y sólo si, sus coordenadas en $\mathcal{R}$ cumplen la ecuación*

$$x_0 = 0.$$

Demostración. Sea H_∞ un hiperplano de $\mathbb{P}^n(\mathbb{F}_q)$, podemos elegir n puntos, $P_1, \dots, P_n$ en H_∞ independientes, porque el hiperplano lineal que lo representa tiene dimensión n. Para cada punto P_i podemos elegir un representante v_i. Como $\mathbb{F}_q^{n+1}$ tiene dimensión vectorial $n+1$, existen vectores independientes de los v_i, sea v_0 uno de estos vectores y P_0 el punto que representa, que evidentemente está fuera de H_∞. El conjunto $\mathcal{B} = \{v_0, \dots, v_n\}$ es una base de $\mathbb{F}_q^{n+1}$. Si además consideramos el punto $A = \pi(v_0 + \cdots + v_n)$, está claro que el conjunto $\{P_0, \dots, P_n, A\}$ es una referencia. Además, la ecuación del hiperplano vectorial que representa a H_∞ es $x_0 = 0$ en $\mathcal{B}$ y por lo tanto, representa a H_∞ en el espacio proyectivo.

□

Teorema 2.28. *Dados un espacio afín y uno proyectivo, ambos de la misma dimensión y sobre el mismo cuerpo, $\mathbb{A}^n(\mathbb{F}_q)$ y $\mathbb{P}^n(\mathbb{F}_q)$, y un hiperplano proyectivo $H_\infty \subset \mathbb{P}^n(\mathbb{F}_q)$; existe una aplicación $\Phi : \mathbb{A}^n(\mathbb{F}_q) \to \mathbb{P}^n(\mathbb{F}_q)$ inyectiva que cumple:*

I *$Im(\Phi) = \mathbb{P}^n(\mathbb{F}_q) - H_\infty$.*

II *Dado un subespacio afín F de dimensión d, existe un subespacio proyectivo, L, de la misma dimensión, de forma que $\Phi(F) \subset L$.*

Demostración. Dado un hiperplano H_∞ ya hemos visto en 2.27 que existe una referencia proyectiva, Λ, en la que

$$H_\infty \equiv \ x_0 = 0.$$

Fijamos ahora una referencia afín $\mathcal{R}$ en $\mathbb{A}^n(\mathbb{F}_q)$ y podemos definir la aplicacion:

$$\begin{array}{rccc} \Phi: & \mathbb{A}^n(\mathbb{F}_q) & \to & \mathbb{P}^n(\mathbb{F}_q) \\ & (x_1, \dots, x_n)_{\mathcal{R}} & \mapsto & (1, x_1, \dots, x_n)_\Lambda \end{array}$$

Para ver que es inyectiva, basta con darse cuenta de que las coordenadas $(x_0, \ldots, x_n)_\Lambda$ y las coordenadas $(y_0, \ldots, y_n)_\Lambda$ describen el mismo punto en $\mathbb{P}^n(\mathbb{F}_q)$ si y solo si, existe λ de forma que $(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$, como en dos puntos de la imagen se cumple $x_0 = y_0 = 1$ debe ser $\lambda = 1$ y por lo tanto $(x_1, \ldots, x_n)_\mathcal{R} = (y_1, \ldots, y_n)_\mathcal{R}$. Vamos a comprobar las otras dos propiedades:

I Resulta evidente que $Im(\Phi) \subset \mathbb{P}^n(\mathbb{F}_q) - H_\infty$, veamos la contención contraria. Si un punto $P \in \mathbb{P}^n(\mathbb{F}_q)$ no está en H_∞ entonces dadas unas coordenadas suyas en Λ, $(x_0, \ldots, x_n)$, sabemos que $x_0 \neq 0$ por lo tanto, $(1, x_1 x_0^{-1}, \ldots, x_n x_0^{-1})$ son también coordenadas de P por lo que éste está en la imagen de Φ.

II Sea $F = Q + T$ un subespacio afín de dimensión d, entonces dado un sistema de generadores de T, por ejemplo $\{v^1, \ldots, v^n\}$, y las coordenadas de $Q \equiv (q_1, \ldots, q_n)$ podemos expresar F en coordenadas paramétricas

$$\left(q_1 + \sum_{i=1}^{d} \alpha_i v_1^i, \ldots, q_n + \sum_{i=1}^{d} \alpha_i v_n^i \right)_\mathcal{R}$$

con $\alpha_i \in \mathbb{F}_q$. De esta forma se pueden expresar todos los puntos de F, vamos a ver como actúa Φ.

$$\Phi\left(\left(q_1 + \sum_{i=1}^{d} \alpha_i v_1^i, \ldots, q_n + \sum_{i=1}^{d} \alpha_i v_n^i \right)_\mathcal{R} \right) = \left(1, q_1 + \sum_{i=1}^{d} \alpha_i v_1^i, \ldots, q_n + \sum_{i=1}^{d} \alpha_i v_n^i \right)_\Lambda$$

Estas coordenadas en Λ describen los mismos puntos que ellas mismas multiplicadas por cualquier $\gamma \in \mathbb{F}_q^*$. De manera que todos los elementos de la forma:

$$\left(\gamma, \gamma q_1 + \sum_{i=1}^{d} \alpha_i \gamma v_1^i, \ldots, \gamma q_n + \sum_{i=1}^{d} \alpha_i \gamma v_n^i \right)_\Lambda$$

forman parte de $\Phi(F)$. En $\mathbb{F}_q^{n+1}$ estas coordenadas describen puntos contenidos en un subespacio vectorial de dimensión $d+1$ (si pudiese ser $\gamma = 0$ y renombrásemos $\gamma\alpha_i = \beta_i$ tendríamos unas ecuaciones paramétricas) por lo tanto, representa a un subespacio proyectivo de dimensión d en $\mathbb{P}^n(\mathbb{F}_q)$ en el que $\Phi(F)$ está contenido.

□

Capítulo 3

Aplicaciones bilineales simétricas

Analizaremos en este capítulo y en el siguiente las aplicaciones bilineales definidas sobre los espacios vectoriales $\mathbb{F}_q^d$. Las aplicaciones bilineales son un caso particular de las aplicaciones sesquilineales que se clasifican en [Ball]. Estas aplicaciones están íntimamente relacionadas con las formas cuadráticas que nos permiten definir las cuádricas en el espacio proyectivo y que trataremos más adelante.

Si bien las definiciones de aplicación bilineal o forma cuadrática son idénticas a las definidas sobre espacios vectoriales en un cuerpo cualquiera, a la hora de clasificarlas aparecen diferencias con las formas sobre los cuerpos real y complejo. Por ejemplo, veremos que en dimensión mayor que 2 es necesario que haya vectores sobre los que una forma cuadrática se anule, cosa que no ocurre en $\mathbb{R}$ ni en $\mathbb{C}$.

3.1. Aplicaciones bilineales.

Definición 3.1. *Una aplicación $(\cdot,\cdot) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, se dice que es una aplicación bilineal en $\mathbb{F}_q^n$ si cumple:*

I *Dados tres vectores $v, w, u \in \mathbb{F}_q^n$ se cumple $(v+w, u) = (v, u)+(w, u)$ y $(v, w+u) = (v, w) + (v, u)$.*

II *Dados dos vectores $v, w \in \mathbb{F}_q^n$ y $\lambda \in \mathbb{F}_q$ se cumple $(\lambda v, w) = (v, \lambda w) = \lambda(v, w)$.*

Definición 3.2. *Dada una aplicación bilineal; se dice que es no degenerada si cumple:*

- *El único vector, $v_0 \in \mathbb{F}_q^n$, que cumple $(v_0, w) = 0$ para todo $w \in \mathbb{F}_q^n$, es el vector nulo.*
- *El único vector $w_0 \in \mathbb{F}_q^n$ que cumple $(v, w_0) = 0$ para cualquier $v \in \mathbb{F}_q^n$, es el vector nulo.*

Definición 3.3. *Dada una aplicación bilineal $(\cdot,\cdot)$ y una base $\{e_1, \ldots, e_n\} = \mathcal{B}$ la matriz de Gram en $\mathcal{B}$, es la matriz que queda definida por las imágenes de los e_i de la siguiente manera: $A_{ij} = (e_i, e_j)$.*

Con la matriz de Gram en una base $\mathcal{B}$, la aplicación bilineal queda totalmente determinada puesto que la podemos escribir como sigue:

$$((x_1, \ldots, x_n)_{\mathcal{B}}, (y_1, \ldots, y_n)_{\mathcal{B}}) = \sum_{i,j} x_i y_j A_{ij}$$

De lo que fácilmente se deduce que una aplicación bilineal es no degenerada si y sólo si, su matriz de Gram es invertible. Si tenemos otra base de $\mathbb{F}_q^n$, $\mathcal{S} = \{v_1, \ldots, v_n\}$, en la cual la expresión de los elementos de $\mathcal{S}$ en $\mathcal{B}$ es:

$$v_i = \sum_{j=1}^{n} t_{ij} e_j$$

Podemos considerar una nueva matriz B, la matriz de Gram en la nueva base, cada coeficiente B_{ik} se puede obtener de la siguiente manera:

$$B_{ik} = (v_i, v_k) = (\sum_{j=1}^{n} t_{ij} e_j, \sum_{l=1}^{n} t_{kl} e_l) = \sum_{j,l} t_{ij} a_{jl} t_{kl}$$

Por lo tanto, si agrupamos los t_{ij} en la matriz de cambio de base, T, podemos deducir que $B = TAT^t$.

Esto nos permite discernir cuando dos aplicaciones bilineales son realmente distintas y no la misma aplicación expresada en diferentes bases.

Definición 3.4. *Dos matrices de Gram A y B, se dice que son equivalentes si existe una matriz de cambio de base, T, de forma que $B = TAT^t$.*

Definición 3.5. *Dos aplicaciones bilineales son equivalentes si lo son sus matrices de Gram.*

De entre todas las aplicaciones bilineales son especialmente interesantes aquellas que se comportan de forma similar a un producto escalar, es decir, aquellas que son simétricas

Definición 3.6. *Una aplicación bilineal se dice que es simétrica si $(v, w) = (w, v)$ para todo $v, w \in \mathbb{F}_q^n$ o equivalentemente, cuando su matriz de Gram es simétrica.*

Definición 3.7. *Dada una aplicación bilineal simétrica $(\cdot, \cdot)$ su radical es el subespacio vectorial definido como:*

$$Rad\left((\cdot, \cdot)\right) = \left\{v \in \mathbb{F}_q^n | (v, w) = 0 \ \forall w \in \mathbb{F}_q^n\right\}.$$

Definición 3.8. *Dada $(\cdot, \cdot)$ una aplicación bilineal simétrica; la aplicación*

$$\begin{array}{rccc} Q: & \mathbb{F}_q^n & \to & \mathbb{F}_q \\ & v & \mapsto & Q(v) = (v, v) \end{array},$$

se dice que es la forma cuadrática asociada a $(\cdot, \cdot)$. Además, decimos que la forma cuadrática es no degenerada cuando lo es su aplicación bilineal simétrica.

Es evidente que en una forma cuadrática se cumple $Q(\lambda v) = \lambda^2 Q(v)$, de hecho una forma cuadrática en $\mathbb{F}_q^n$ define, un polinomio homogéneo de grado 2 en n variables. Por otra parte, dados dos vectores $v, w \in \mathbb{F}_q^n$ podemos escribir:

$$Q(v+w) = (v,v) + (w,w) + 2(v,w) = Q(v) + Q(w) + 2(v,w)$$

Por lo tanto, si estamos en un cuerpo en el que se pueda dividir entre dos; es decir, un cuerpo de característica impar; podremos recuperar el valor de (v,w). Acabamos de ver que en un cuerpo de característica impar es equivalente definir una aplicación bilineal simétrica y definir directamente su forma cuadrática.

3.2. Ortogonalidad

Definición 3.9. *Dada una aplicación bilineal simétrica en $\mathbb{F}_q^n$, $(\cdot,\cdot)$; dos vectores $v, w \in \mathbb{F}_q^n$ se dice que son ortogonales si $(v,w) = 0$.*

Definición 3.10. *Dada una aplicación bilineal en $\mathbb{F}_q^n$ y un subconjunto $\Omega \subset \mathbb{F}_q^n$ se define el complemento ortogonal de Ω como sigue:*

$$\Omega^\perp = \{v \in \mathbb{F}_q^n | (v,\omega) = 0 \ \forall \omega \in \Omega\}$$

Una vez fijada una aplicación bilineal simétrica, cada $\omega_0 \in \Omega$ define una ecuación homogénea implícita $(v,\omega_0) = 0$. Los vectores que están en $\Omega^\perp$ son aquellos que cumplen todas estas ecuaciones y por lo tanto, forman un subespacio lineal.

Proposición 3.11. *Dada una aplicación bilineal simétrica no degenerada en $\mathbb{F}_q^n$, si $L \subset \mathbb{F}_q^n$ es un subespacio lineal, entonces:*

$$dim(L) + dim(L^\perp) = n.$$

Demostración. Dado un vector no nulo $v \in \mathbb{F}_q^n$, como la aplicación bilineal es no degenerada, existe $w \in \mathbb{F}_q^n$ de forma que $(v,w) \neq 0$ y por lo tanto $\{v\}^\perp \neq \mathbb{F}_q^n$. Veamos que $\{v\}^\perp$ es un hiperplano, es decir, $dim\left(\{v\}^\perp\right) = n-1$. Para demostrarlo, basta con probar que la intersección de $\{v\}^\perp$ con cualquier subespacio de dimensión 2 contiene algún vector distinto del nulo. Fijamos un subespacio de dimensión 2, $\langle w_1, w_2\rangle$. Denotamos a los valores (v,w_1) y (v,w_2) por λ y γ respectivamente. Si λ ó γ son 0, ellos mismos pertenecen a la intersección con $\{v\}^\perp$, si ninguno lo es, entonces $(v, \gamma w_1 - \lambda w_2) = 0$ y tenemos

$$0 \neq \gamma w_1 - \lambda w_2 \in \{v\}^\perp \cap \langle w_1, w_2\rangle.$$

Sea $\{e_1, \ldots, e_n\}$ una base de $\mathbb{F}_q^n$, entonces:

$$\langle e_1\rangle^\perp \supset \langle e_1, e_2\rangle^\perp \supset \cdots \supset \langle e_1, \ldots, e_n\rangle^\perp = \mathbb{F}_q^{n\perp} = \{0\}$$

Como $\langle e_1, \ldots e_t\rangle^\perp = \langle e_1, \ldots e_{t-1}\rangle^\perp \cap \langle e_t\rangle^\perp$ y $\langle e_t\rangle^\perp$ es un hiperplano; en la cadena anterior la dimensión decrece como mucho en una unidad por paso. En la cadena hay $n-1$ pasos y se llega a un subespacio de dimensión 0, entonces podemos deducir que de hecho en cada paso la dimensión decrece exactamente 1. Como la base puede ser cualquiera, tenemos que para cualquier subespacio $\langle e_1 \ldots, e_t\rangle$ de dimensión t, la dimensión de su complemento ortogonal es $n-t$.

□

3.3. Clasificación de las formas bilineales simétricas en cuerpos de característica impar.

Como se puede deducir del título, en esta sección nos centraremos en cuerpos de característica impar, por lo que en lo que resta de capítulo tendremos $q = p^n$ siendo p un número primo e impar.

Definición 3.12. *Dada una aplicación bilineal simétrica en $\mathbb{F}_q^n$:*

- *Un vector $v \in \mathbb{F}_q^n$ se dice que es isotrópico si es ortogonal a sí mismo, $(v, v) = 0$.*
- *Un subespacio lineal $L \subset \mathbb{F}_q^n$ se dice que es totalmente isotrópico si: $(v, w) = 0 \; \forall v, w \in L$.*
- *Se dice que la aplicación bilineal es anisotrópica si no existe ningún vector v distinto del nulo que cumpla (v, v).*

El producto escalar en el espacio euclídeo es un ejemplo de aplicación bilineal anisotrópica, por ello se dice que es un espacio anisotrópico. Veremos ahora que en espacios vectoriales sobre cuerpos finitos este tipo de aplicaciones no existen en espacios con dimensión superior a 2.

Definición 3.13. *Sea M una matriz $n \times n$ con coeficientes en $\mathbb{F}_q$; definimos el discriminante de M como sigue:*

$$disc(M) = \begin{cases} 1 & si \quad det(M) \text{ es un cuadrado} \\ -1 & si \quad det(M) \text{ no es un cuadrado} \end{cases}$$

Proposición 3.14. *El discriminante de una matriz de Gram es independiente de la base.*

Demostración. Sea A la matriz de Gram en una base, dada otra base hemos visto que la matriz de Gram en ella se puede escribir $B = TAT^t$, siendo T la matriz de cambio de base pertinente. Tomando determinantes tenemos $det(B) = det(A)det(T)^2$, vimos en la proposición 1.32 que el producto de un cuadrado por un no cuadrado es un no cuadrado y evidentemente, el producto de dos cuadrados es un cuadrado, luego $disc(B) = disc(A)$.

□

Aplicaciones bilineales simétricas en 1 dimensión

Teorema 3.15. *Dada una aplicación bilineal $(\cdot, \cdot)$ distinta de la aplicación nula en $\mathbb{F}_q$, sea Q su forma cuadrática; o bien $Q(x)$ es un cuadrado para todo $x \in \mathbb{F}_q$, o bien $Q(x)$ es no cuadrado para todo $x \in \mathbb{F}_q$.*

Demostración. Sea $x \in \mathbb{F}_q$, para todo $y \in \mathbb{F}_q$ existe $\lambda \in \mathbb{F}_q$ de forma que $y = \lambda x$, entonces $Q(y) = \lambda^2 Q(x)$. Por lo tanto, si $Q(x)$ es cuadrado, todos lo son y si no lo es, ninguno lo es.

□

Nota. Resulta obvio que multiplicando una forma bilineal simétrica por una constante, obtenemos otra forma bilineal simétrica. Por lo que para pasar de un caso al otro en el teorema anterior basta con multiplicar por un no cuadrado.

Formas bilineales simétricas en 2 dimensiones

Teorema 3.16. *Sea $(\cdot,\cdot)$ una aplicación bilineal no degenerada en $\mathbb{F}_q^2$, entonces hay dos opciones:*

- *Existe un vector no nulo $v \in \mathbb{F}_q^2$ que cumple $(v,v) = 0$ y es equivalente a una aplicación con matriz de Gram $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*
- *No existe ningún vector isotrópico y es equivalente a una aplicación cuya matriz de Gram es $\begin{pmatrix} 1 & 0 \\ 0 & -\gamma \end{pmatrix}$, donde γ es un no cuadrado.*

Demostración. Supongamos que existe un vector $v_1 \in \mathbb{F}_q^2$ isotrópico, como la aplicación es no degenerada, podemos encontrar $w \in \mathbb{F}_q^n$ de forma que cumpla $(v_1, w) \neq 0$, de hecho podemos elegir w de forma que (v_1, w)=1. Si definimos $\alpha = -2^{-1}(w,w)$ y además $v_2 = w + \alpha v_1$. Entonces v_1 y v_2 forman una base y cumplen:

$$(v_1, v_2) = 1,$$

$$(v_1, v_1) = 0,$$

$$(v_2, v_2) = (w + \alpha v_1, w + \alpha v_1) = (w,w) + 2\alpha = 0.$$

Por lo tanto, en esta base la matriz de Gram es la que dice el teorema, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Supongamos ahora que no existe ningún vector isotrópico. Vamos a ver por reducción al absurdo que no puede ser que (v,v) sea un cuadrado para todo v. Supongamos que (v,v) es un cuadrado para cualquier vector. Sea e_1 un vector no nulo, pusto que $dim(\langle e_1 \rangle^\perp) = 1$ y $e_1 \notin \langle e_1 \rangle^\perp$ porque no hay ningún vector isotrópico, lo podemos completar a una base de forma que $(e_1, e_2) = 0$. Además, como $(\lambda v, \lambda v) = \lambda^2 (v,v)$ y el inverso de un cuadrado es un cuadrado podemos elegir la base de forma que $(e_1, e_1) = 1$. Entonces, para cualesquiera $\alpha, \beta \in \mathbb{F}_q$ se cumple

$$(\alpha e_1 + \beta e_2, \alpha e_1 + \beta e_2) = \alpha^2 + \beta^2,$$

de lo que podemos deducir que la suma de cuadrados es un cuadrado. De esto podemos deducir, si la característica de $\mathbb{F}_q$ es p:

$$-1 = p - 1 = \overbrace{1 + \cdots + 1}^{p-1 \text{ veces}}$$

Por lo tanto, como el producto de dos cuadrados es un cuadrado y el inverso también, tenemos que los cuadrados de un cuerpo forman un subcuerpo. Si embargo, puesto que

el cardinal de un subcuerpo debe ser divisor de su cardinal q y el cardinal del conjunto de los cuadrados es $\frac{q-1}{2}+1 > \frac{q}{2}$, hemos llegado a una contradicción. Tampoco puede ser que (v,v) sea un no cuadrado para todos los vectores. Si fuese así, la aplicación bilineal simétrica $\eta(\cdot,\cdot)$, con $\eta \in \mathbb{F}_q$ no cuadrado, cumpliría por 1.32 que $\eta(v,v)$ es un cuadrado para todo v y acabamos de ver que eso es imposible.

Por lo tanto, tiene que haber un vector $v \in \mathbb{F}_q$ de forma que $(v,v) = a^2$. Definimos $e_1 = a^{-1}v$. Sabemos que existe e_2 ortogonal a e_1 y que además son linealmente independientes, puesto que si no lo fuesen, serían ambos isotrópicos. Supongamos que $-(e_2,e_2)$ es un cuadrado: $-(e_2,e_2) = b^2$, entonces el vector $be_1+e_2 \neq 0$ sería isotrópico. Por lo tanto, $\gamma = -(e_2,e_2)$ tiene que ser no cuadrado. Acabamos de encontrar la base que buscábamos $\mathcal{B} = \{e_1,e_2\}$ en la que la matriz es $\begin{pmatrix} 1 & 0 \\ 0 & -\gamma \end{pmatrix}$.

□

Las matrices del teorema anterior tienen determinante -1 y $-\gamma$ respectivamente, como γ es no cuadrado, $-\gamma$ será cuadrado si no lo es -1 y viceversa. Luego, una vez hemos determinado si en $\mathbb{F}_q$ -1 es cuadrado o no (recordemos 1.32) podemos distinguir en que caso de los anteriores nos encontramos por el discriminante de la matriz de Gram de la aplicación.

Definición 3.17. *Al plano $\mathbb{F}_q^2$ con un producto interno definido por una aplicación bilineal como la del primer caso se lo conoce como plano hiperbólico.*

Formas bilineales simétricas en dimensión $n > 2$

Proposición 3.18. *Sea $(\cdot,\cdot)$ una aplicación bilineal simétrica en $\mathbb{F}_q^n$ con $n > 2$; entonces existe un vector isotrópico distinto de 0.*

Demostración. Si la aplicación es degenarada, es obvio que existe. Si no, podemos elegir un vector v_0 que cumpla $(v_0,v_0) = 1$; para convencerse de esto, basta con ver que el espacio contiene algún subespacio de dimensión 2 y en cualquiera de las formas del teorema 3.16 existe un vector con esta propiedad. Por la proposición 3.11, $dim(\langle v_0\rangle^\perp) = n-1 \geq 2$ y de nuevo en ambas formas del teorema 3.16 podemos encontrar un vector v_1 que cumpla $(v_1,v_1) = -1$. Si consideramos ahora $v = v_0 + v_1$ tenemos:

$$\langle v,v\rangle = \langle v_0,v_0\rangle + \langle v_1+v_1\rangle = 0$$

Por lo tanto, ya hemos encontrado un vector isotrópico.

□

Teorema 3.19. *Sea $(\cdot,\cdot)$ una forma bilineal simétrica no degenerada sobre $\mathbb{F}_q^n$ con q impar y $n > 2$; entonces:*

- *Si n es par, entonces podemos descomponer $\mathbb{F}_q^n$ como sigue:*

$$\mathbb{F}_q^n = H_1 + \cdots + H_{n/2-1} + A$$

Donde los H_i son planos hiperbólicos y A es o bien, un plano hiperbólico, o bien, un plano anisotrópico. Además todos los subespacios de la descomposición son ortogonales entre sí.

- *Si n es impar, entonces podemos descomponer $\mathbb{F}_q^n$ así:*

$$\mathbb{F}_q^n = H_1 + \cdots + H_{(n-1)/2} + \langle v \rangle$$

Donde los H_i son planos hiperbólicos y o bien, $(v,v) = 1$, o bien; $(v,v) = \gamma$ con γ un no cuadrado. Además todos los subespacios de la descomposición son ortogonales entre ellos.

Demostración. En la proposición anterior hemos visto que existe un vector isotrópico no nulo, lo llamamos v_1. Como estamos ante una aplicación bilineal no degenerada, existe un $w_1' \in \langle v_1 \rangle^\perp$ de forma que $(v_1, w_1') \neq 0$ y podemos elegir que $(v_1, w_1') = 1$.

Definimos $\alpha = -2^{-1}(w_1', w_1')$ y $w_1 = w_1 + \alpha v_1$, de forma que $(w_1, w_1) = 0$. Entonces $H_1 = \langle v_1, w_1 \rangle$ es un plano hiperbólico. Como $(v_1, w_1) = 1$, tenemos

$$\langle v_1, w_1 \rangle \cap \langle v_1, w_1 \rangle^\perp = \emptyset,$$

y como por la proposición 3.11 $dim(\langle v_1, w_1 \rangle^\perp) = n - 2$ podemos deducir

$$\mathbb{F}_q^n = H_1 + H_1^\perp.$$

Si $dim(H_1^\perp) > 2$ podemos volver a realizar el mismo razonamiento restringiéndonos a $H_1^\perp$ y así hasta llegar a un subespacio de dimensión 1 si n es impar o de dimensión 2 si n es par y este último subespacio lo podemos clasificar de acuerdo con 3.15 y 3.16 respectivamente.

□

De nuevo, una vez hemos determinado si -1 es un cuadrado en en $\mathbb{F}_q$, podemos distinguir en qué caso de los dos anteriores nos encontramos gracias al discriminante. En el caso de n par, si todos los planos de la descomposición son hiperbólicos el determinante de la matriz de Gram vale $(-1)^{n/2}$ y si no $(-1)^{(n/2)-1}\gamma$ con γ un no cuadrado. Si al contrario, $n = 2m + 1$ el determinante será $(-1)^m$ o $(-1)^n\gamma$ dependiendo del caso en el que estemos.

Examinaremos a continuación un par de aplicaciones bilineales. Comenzamos por clasificar la forma cuadrática en $\mathbb{F}_5^3$ que viene dada por

$$Q((x_0, x_1, x_2)) = x_0x_2 - x_1^2.$$

Recordamos que los elementos en $\mathbb{F}_5$ son $\{0, 1, 2, 3, 4\}$. Puesto que el inverso de 2 en $\mathbb{F}_5$ es el 3 la aplicación bilineal simétrica que tiene asociada es

$$((x_0, x_1, x_2), (y_0, y_1, y_2)) = \frac{x_0y_2}{2} + \frac{x_2y_0}{2} - x_1y_1 = 3x_0y_2 + 3x_2y_0 + 4x_1y_1,$$

cuya matriz de Gram en esta base es

$$\begin{pmatrix} 0 & 0 & 3 \\ 0 & 4 & 0 \\ 3 & 0 & 0 \end{pmatrix},$$

y por lo tanto su determinante vale $-4 \cdot 4 \cdot 3$ que en $\mathbb{F}_5$ es la clase del 4 luego no es degenerada y además sabemos que tiene discriminante 1. Sabemos que existe una base en la que la matriz de Gram tiene la forma:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \eta \end{pmatrix},$$

vamos a buscarla. Para ello lo primero buscamos un vector isotrópico, por ejemplo $e_0 = (1, 0, 0)$. Buscamos ahora un segundo vector $e_1 = (y_0, y_1, y_2)$ también isotrópico y de forma que $(e_0, e_1) = 1$ para terminar de formar el plano hiperbólico. Estas dos condiciones se traducen en un sistema de dos ecuaciones

$$\begin{cases} Q(e_1) & = y_0 y_2 - y_1^2 = 0, \\ (e_0, e_1) & = 3y_2 = 1. \end{cases}$$

La segunda ecuación nos fuerza a tener $y_2 = 1/3 = 2$. Trasladando esto a la primera ecuación nos queda

$$2y_0 = y_1^2,$$

Esta ecuación tiene varias soluciones, sin embargo, la que más nos facilita los cálculos es $y_0 = y_1 = 0$, de forma que el segundo integrante de la base resulta ser $e_1 = (0, 0, 2)$. Finalmente, necesitamos un tercer miembro que sea ortogonal a estos dos, para ello, si denotamos $e_2 = (z_0, z_1, z_2)$ tenemos que imponer las dos condiciones

$$\begin{cases} (e_0, e_2) & = 3z_2 = 0, \\ (e_1, e_2) & = 6z_0 = 0. \end{cases}$$

Por lo tanto resulta obvio que el tercer elemento, una vez elegidos e_0 y e_1 debe ser $e_2 = (0, 1, 0)$. La forma bilineal tiene por matriz de Gram en la base $\mathcal{B} = \{(1, 0, 0), (0, 0, 2), (0, 1, 0)\}$ la forma canónica que buscábamos

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

En este caso hemos trabajado en 3 dimensiones, ahí una vez sabemos que la forma es no degenerada hay una única posibilidad, la forma permite descomponer en un plano hiperbólico y un subespacio ortogonal al plano de dimensión uno, aunque puede haber diferentes elecciones del plano. En 4 dimensiones hay dos posibilidades, puede que el espacio se descomponga en dos planos hiperbólicos ortogonales entre sí y por lo tanto exista una matriz de Gram con forma

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

o puede que se descomponga en un plano hiperbólico y un plano anisotrópico de forma que su matriz de Gram tenga la forma

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\gamma \end{pmatrix},$$

donde γ debe ser un no cuadrado.

Analizaremos la aplicación bilineal sobre $\mathbb{F}_3^4$ que viene dada por

$$((x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3)) = x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3.$$

En primer debemos determinar que tipo de aplicación bilineal simétrica es. En cuatro dimensiones, si se trata de suma ortogonal de dos planos hiperbólicos el discriminante de la matriz de Gram es 1 y si es un plano hiperbólico suma ortogonal con un plano anisotrópico el determinante de la matriz será γ, un no cuadrado, y por lo tanto su discriminante -1. Resulta evidente que la matriz de Gram de nuestra forma bilineal es la matriz identidad luego su discriminante es 1 y nos encontramos en el caso de dos planos hiperbólicos.

Vamos a buscar dos planos hiperbólicos ortogonales entre sí. Para ello buscamos un vector isotrópico, por ejemplo $l_0 = (1, 1, 1, 0)$, de la misma forma que antes buscamos un segundo vector $l_1 \in \mathbb{F}_3^4$ de forma que $Q(l_1) = 0$ y $(l_0, l_1) = 0$, lo que desemboca en el sistema:

$$\begin{cases} Q(l_1) & = y_0^2 + y_1^2 + y_2^2 + y_3^2 = 0, \\ (l_0, l_1) & = y_0 + y_1 + y_2 = 1. \end{cases}$$

Un vector solución del sistema es $l_1 = (2, 1, 1, 0)$, luego el primer plano hiperbólico será $\langle l_0, l_1 \rangle$. El segundo plano es el que definen las ecuaciones implícitas

$$\begin{cases} (l_0, v) & = z_0 + z_1 + z_2 = 0, \\ (l_1, v) & = 2z_0 + z_1 + z_2 = 0. \end{cases}$$

Si queremos completar la base en la que la matriz de Gram es la canónica necesitamos un tercer, l_2, vector que además de cumplir las dos ecuaciones anteriores sea isotrópico, es decir, que sea solución del sistema

$$\begin{cases} (l_0, l_2) & = z_0 + z_1 + z_2 = 0, \\ (l_1, l_3) & = 2z_0 + z_1 + z_2 = 0, \\ Q(l_2) & = z_0^2 + z_1^2 + z_2^2 + z_3^2 = 0. \end{cases}$$

Sumando las dos primeras ecuaciones lineales vemos que se debe cumplir la ecuación $z_1 + z_2 = 0$, restándolas vemos que debe ser $z_0 = 1$, proponemos el vector $(0, 2, 1, \xi)$ que cumple ambas condiciones, si además imponemos la tercera ecuación, nos queda $2^2 + 1^2 + \xi^2 = 2 + \xi^2 = 0$, una posible solución es $l_2 = (0, 2, 1, 1)$. Nos queda un único vector por encontrar, para hacerlo a las condiciones del último sistema hay que añadirles la condición $(l_2.l_3) = 1$, de forma que nos queda resolver el sistema

$$\begin{cases} (l_0, l_3) & = a_0 + a_1 + a_2 = 0, \\ (l_1, l_3) & = 2a_0 + a_1 + a_2 = 0, \\ Q(l_3) & = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 0, \\ (l_2, l_3) & = 2a_1 + a_2 + a_3 = 1. \end{cases}$$

Las dos condiciones $a_0 = 0$ y $a_1 + a_2 = 0$ siguen siendo vigentes, restando la última ecuación a la segunda nos queda $a_0 - a_3 = -1$, luego tenemos la condición $a_3 = 1$. Finalmente nos queda el vector $l_3 = (0, 1, 2, 1)$, de forma que la base

$$\mathcal{S} = \{(1, 1, 1, 0), (2, 1, 1, 0), (0, 2, 1, 1), (0, 1, 2, 1)\},$$

tiene por matriz de Gram la que estábamos buscando.

Capítulo 4

Formas cuadráticas en cuerpos de característica dos

En este capítulo trataremos los casos de característica par que evitamos en el anterior. Veremos que en general los resultados que se tienen en característica impar relativos a la clasificación de formas son ciertos o al menos tienen su equivalente en estos cuerpos. Sin embargo, las peculiaridades de estos cuerpos hacen que el tratamiento sea algo diferente, sin ir más lejos ya hemos visto que inevitablemente perdemos la equivalencia entre aplicación bilineal simétrica y forma cuadrática, lo que nos hará tener que redefinir algún concepto.

4.1. Aplicaciones simplécticas

Antes de centrarnos en la característica dos trataremos un tipo de aplicaciones bilineales que nos será útil al estudiar las formas cuadráticas en cuerpos característica par.

Definición 4.1. *Dada una aplicación bilineal $(\cdot,\cdot)$ en $\mathbb{F}_q^n$, se dice que es simpléctica si para todo $v \in \mathbb{F}_q^n$ se cumple $(v,v) = 0$.*

Definición 4.2. *Dada una aplicación bilineal $(\cdot,\cdot)$ en $\mathbb{F}_q^n$, se dice que es antisimétrica si para todos $v, w \in \mathbb{F}_q^n$ se cumple $(v,w) = -(w,v)$.*

Proposición 4.3. *Toda aplicación bilineal simpléctica es antisimétrica.*

Demostración. Sea $(\cdot,\cdot)$ una aplicación simpléctica, entonces dados $w, v \in \mathbb{F}_q^n$ tenemos:

$$0 = (v+w, v+w) = (v,v) + (w,w) + (v,w) + (w,v) = (v,w) + (w,v)$$

y por lo tanto, $(v,w) = -(w,v)$.

□

Evidentemente la matriz de Gram de una aplicación bilineal antisimétrica es antisimétrica. Podemos definir el complemento ortogonal de un subconjunto exactamente

igual que lo hicimos para aplicaciones bilineales simétricas. También se cumple, y de hecho se prueba de la misma forma que en aquel caso ,la siguiente proposición.

Proposición 4.4. *Sea $(\cdot,\cdot)$ una forma bilineal simpléctica no degenerada sobre $\mathbb{F}_q^n$ y $L \subset \mathbb{F}_q^n$ un subespacio vectorial de $\mathbb{F}_q^n$; entonces se cumple:*

$$dim(L) + dim(L^{\perp}) = n.$$

Vamos a ver que las aplicaciones simplécticas no degeneradas no pueden existir en cualquier dimensión.

Proposición 4.5. *Sea $(\cdot,\cdot)$ una forma bilineal simpléctica no degenerada sobre $\mathbb{F}_q^n$, entonces n es un número par. Además existe una base en la que su matriz de Gram está formada por bloques de la forma*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

situados sobre la diagonal.

Demostración. Tomamos un vector $v_1 \in \mathbb{F}_q^n$, como $(\cdot,\cdot)$ es una aplicación no degenerada, existe $w_1' \in \mathbb{F}_q^n$ de forma que $(v_1, w_1') = \lambda \neq 0$. Definimos $w_1 = \lambda^{-1} w_1'$, además v_1 y w_1 son linealmente independientes, porque de lo contrario tendríamos

$$(v_1, w_1) = \lambda(v_1, v_1) = 0.$$

Ningún vector de $\langle v_1, w_1\rangle$ es ortogonal a este mismo subespacio, luego gracias a la proposición 4.4 tenemos $\mathbb{F}_q^n = \langle v_1, w_1\rangle + \langle v_1, w_1\rangle^{\perp}$. Si ahora nos restringimos a $\langle v_1, w_1\rangle^{\perp}$ podremos realizar el mismo proceso hasta quedarnos únicamente con el subespacio $\{0\}$, en cuyo caso estaríamos en dimensión par, o con un subespacio de dimensión 1. Supongamos que llegamos a un subespacio de dimensión 1. Dado un vector u en este subespacio, u sería ortogonal a todos los vectores de los subespacios anteriores y, por ser $(\cdot,\cdot)$ simpléctica, a sí mismo. Acabamos de ver que $(v, u) = 0$ para todo $v \in \mathbb{F}_q^n$ luego la forma sería degenerada. En cada paso del proceso podemos obtener una base como $\{v_1, w_1\}$ adaptada a ese subespacio, $\{v_i, w_i\}$, de forma que la matriz de Gram de la aplicación restringida a ese espacio en esta base es la que buscamos.

□

4.2. Formas cuadráticas

En el capítulo anterior vimos que, en cuerpos de característica impar, las aplicaciones bilineales simétricas y las formas cuadráticas contienen la misma información. Vamos a analizar el caso de característica par, para ello comenzaremos definiendo forma cuadrática. De ahora en adelante en este capítulo, salvo que se indique lo contrario $\mathbb{F}_q$ será un cuerpo de característica 2, o lo que es lo mismo, tendremos $q = 2^n$.

Definición 4.6. *Una forma cuadrática en $\mathbb{F}_q^n$ es una aplicación $Q : \mathbb{F}_q^n \to \mathbb{F}_q$ que cumple:*

- $Q(\lambda x) = \lambda^2 Q(x) \quad \forall v \in \mathbb{F}_q^n,\ \forall \lambda \in \mathbb{F}_q$.
- *La aplicación* $(x, y) = Q(x + y) + Q(x) + Q(y)$ *es una aplicación bilineal.*

Puesto que, en cuerpos de característica dos, todo elemento es su propio opuesto, es fácil ver que la aplicación bilineal asociada a una forma cuadrática es simpléctica.

Nota. Como todo elemento es el opuesto de sí mismo, las formas simétricas y antisimétricas son exactamente las mismas.

A diferencia de en el caso de característica impar; aquí, pese a que una forma cuadrática define de forma inequívoca una aplicación bilineal simétrica asociada a ella, el recíproco no es cierto, puesto que de la forma bilineal no se pueden recuperar los valores de la forma cuadrática. Por ejemplo, si definimos en $\mathbb{F}_q^2$ la siguiente forma cuadrática:

$$Q((x_1, x_2)) = ax_1^2 + bx_2^2 + cx_1x_2$$

Su forma bilineal asociada es:

$$((x_1, x_2), (y_1, y_2)) =$$

$$a(x_1^2 + y_1^2 + (x_1 + y_1)^2) + b(x_2^2 + y_2^2 + (x_2 + y_2)^2) + c(x_1x_2 + y_1y_2 + (x_1 + y_1)(x_2 + y_2))$$

Es fácil ver que $x^2 + y^2 + (x + y)^2 = 0$ en característica par, además $x_1x_2 + y_1y_2 + (x_1 + y_1)(x_2 + y_2) = x_1y_2 + y_1x_2$ por lo tanto:

$$((x_1, x_2), (y_1, y_2)) = c(x_1y_2 + y_1x_2)$$

Luego dos formas cuadráticas diferentes pueden dar lugar a la misma aplicación bilineal aunque ellas sean distintas.

4.3. Clasificación formas cuadráticas

Puesto que la forma bilineal asociada a una forma cuadrática es simpléctica, la noción de ortogonalidad a sí mismo de un vector se tiene que definir directamente con la forma cuadrática. El concepto equivalente a vector isotrópico del capítulo anterior es el de vector singular.

Definición 4.7. *Dada una forma cuadrática* $Q : \mathbb{F}_q^2 \to \mathbb{F}_q$*, decimos que un vector* $v \in \mathbb{F}_q^n$ *es singular si* $Q(v) = 0$.

En característica impar hemos visto que una forma cuadrática es degenerada cuando lo es su forma bilineal asociada, es decir, cuando existen vectores distintos del nulo ortogonales a todo el espacio. Sin embargo, en el caso de característica 2 para cualquier forma bilineal asociada a una forma cuadrática se tiene $(v, v) = 0$. Por lo tanto hay que introducir la información de $Q(v)$ en la definición de degeneración.

Definición 4.8. *Sea* $Q : \mathbb{F}_q^2 \to \mathbb{F}_q$ *una forma cuadrática y* $(\cdot, \cdot)$ *su forma simpléctica asociada, decimos que* Q *es no degenerada si para todo* $v \in Rad((\cdot, \cdot)) - \{0\}$ *se cumple* $Q(v) \neq 0$.

Formas cuadráticas en característica par y dimensión 2

En un cuerpo de característica par, todos los elementos son cuadrados, luego es imposible hacer la distinción que se hacía en el caso de característica impar y dimensión 1. Por lo tanto, todas las formas cuadráticas son equivalentes en dimensión 1.

En un cuerpo de característica par, la aplicación que lleva x en x^2 es un isomorfismo, el isomorfismo de Frobenius, luego todos los elementos son cuadrados. El lema siguiente nos permite dividir los elementos de un cuerpo de característica par en dos grupos, con traza nula y con traza 1, de la misma forma que los elementos de un cuerpo de característica par se dividían en cuadrados y no cuadrados.

Lema 4.9. *Dado un cuerpo finito de característica 2 y un elemento $a \in \mathbb{F}_q$, existe $x \in \mathbb{F}_q$ de forma que $a = x + x^2$ si y sólo si, al considerar $\mathbb{F}_q$ como extensión de $\mathbb{F}_2$ y la aplicación traza definida como en 1.20, se cumple $tr(a) = 0$.*

Demostración. Sea $a \in \mathbb{F}_q$, supongamos que existe $x \in \mathbb{F}_q$ de forma que $a = x + x^2$. La aplicación que envía x en x^2 es un integrante del grupo de Galois de la extensión $[\mathbb{F}_q : \mathbb{F}_2]$, luego $tr(x) = tr(x^2)$. Por lo tanto, puesto que la traza es una aplicación lineal,

$$tr(a) = tr(x + x^2) = tr(x) + tr(x^2) = tr(x) + tr(x) = 0.$$

Sabemos, de la teoría de aplicaciones lineales, que dada una aplicación lineal $\phi : E \to V$ tenemos:

$$dim(Im(\phi)) + dim(ker(\phi)) = dim(V).$$

Como la traza es una aplicación lineal en $\mathbb{F}_2$; su núcleo, es decir, el subespacio de los elementos que cumple $tr(a) = 0$, es un hiperplano de $\mathbb{F}_q$ visto como $\mathbb{F}_2$-espacio vectorial. Por otra parte, la aplicación que definimos:

$$\begin{array}{rccc} \Phi: & \mathbb{F}_q & \to & \mathbb{F}_q \\ & x & \mapsto & x + x^2 \end{array}$$

es lineal sobre $\mathbb{F}_2$, veámoslo. Tenemos que

$$\Phi(\lambda x) = \lambda x + \lambda^2 x^2 = \lambda(x + x^2),$$

porque λ sólo puede ser 0 ó 1. Además,

$$\Phi(x + y) = x + y + (x + y)^2 = x + x^2 + y + y^2 = \Phi(x) + \Phi(y),$$

como vimos en el automorfismo de Frobenius. Como el único elemento que es igual a su cuadrado, y por lo tanto opuesto, es 1; sabemos que el núcleo de Φ es $\{0, 1\}$, un subespacio de dimensión 1. Por lo tanto la imagen de Φ es un hiperplano de $\mathbb{F}_q$. Hemos visto que $ker(tr) \subset Im(\Phi)$ al principio de la demostración y puesto que tienen la misma dimensión, son iguales. Así queda el lema demostrado.

□

Lema 4.10. *Dada una forma cuadrática $Q : \mathbb{F}_q^2 \to \mathbb{F}_q$; si su aplicación bilineal asociada es la aplicación nula, entonces Q es degenerada.*

Demostración. Sea $(\cdot,\cdot)$ la aplicación bilineal asociada a Q. Supongamos que es la aplicación nula, por lo que $rad((\cdot,\cdot)) = \mathbb{F}_q^2$. Entonces

$$0 = (v,w) = Q(v) + Q(w) + Q(v+w); \quad \forall v, w \in \mathbb{F}_q^2$$

y como estamos en un cuerpo de característica 2, podemos deducir $Q(v+w) = Q(v) + Q(w)$.

Tenemos una aplicación de $\mathbb{F}_q^2$, un espacio de q^2 elementos, en $\mathbb{F}_q$, un cuerpo de q elementos. Existen por lo tanto dos opciones:

- Existe algún vector $v \neq 0$ en $\mathbb{F}_q^2$ de forma que $Q(v) = 0$, en cuyo caso Q es degenerada y habríamos terminado.
- No existe dicho vector, veamos que esto es imposible:

Si no existe, quiere decir que de los $q^2 - 1$ vectores no nulos de $\mathbb{F}_q^2$, todos tienen imagen por Q no nula. Existen $q-1$ escalares no nulos en $\mathbb{F}_q$, luego al menos dos vectores distintos, w_1 y w_2, deben tener la misma imagen $Q(w_1) = Q(w_2) = \nu \neq 0$. Sin embargo, hemos visto que $Q(w_1 + w_2) = Q(w_1) + Q(w_2) = \nu + \nu = 0$ y como $w_1 \neq w_2$ sabemos $w_1 + w_2 \neq 0$.

□

Estamos ya en condiciones de clasificar las formas bilineales de cuerpos en característica par. El siguiente teorema divide las formas cuadráticas sobre cuerpos de característica par de forma similar a como el teorema 3.16 diferenciaba entre planos anisotrópicos e hiperbólicos.

Teorema 4.11. *Dada una forma cuadrática $Q : \mathbb{F}_q^2 \to \mathbb{F}_2$ no degenerada, existen dos opciones:*

- *Existe una base $\{v_1, v_2\}$ de forma que $Q(v_1) = Q(v_2) = 0$ y $Q(v_1 + v_2) = 1$.*
- *No existe ningún vector no nulo con $Q(v) = 0$ y existe una base $\{v_1, v_2\}$ con $Q(v_1) = 1$, $Q(v_2) = a$ con $tr(a) = 1$, siendo la traza relativa al grupo de Galois $G(\mathbb{F}_q|\mathbb{F}_2)$.*

Demostración. Sea $(\cdot,\cdot)$ la forma simpléctica asociada a Q; por lo visto en 4.5 debe ser o la aplicación nula o no degenerada, si no fuese así quedaría un subespacio de dimensión 1 (impar) en el que $(\cdot,\cdot)$ restringida a él sería no degenerada. Hemos visto en lema 4.10 que si su aplicación bilineal asociada es nula, entonces Q es degenerada. Vamos con la primera opción:

Sea $v_1 \in \mathbb{F}_q^2$ no nulo de forma que $Q(v_1) = 0$, como Q es no degenerada v_1 no está en el radical de la forma bilineal, por lo que existe w de forma que $(v,w) \neq 0$; dividiendo por una constante adecuada podemos tomar $(v,w) = 1$. Sea $v_2 = w + \eta v$, entonces $(v_1, v_2) = 1$. Evaluando la forma cuadrática:

$$Q(v_2) = Q(w) + \eta^2 Q(v) + \eta(v,w) = Q(w) + \eta.$$

Si elegimos $\eta = Q(w)$ tenemos $Q(v_2) = 0$ y la base $\{v_1, v_2\}$ cumplirá lo que estipula el teorema, puesto que $Q(v_1 + v_2) = Q(v_1) + Q(v_2) + (v_1, v_2) = 1$.

Pasamos ahora al caso en el que no existe ningún vector singular. Como en característica par todos los elementos de un cuerpo son cuadrados podemos elegir sin problema un vector v, de forma que $Q(v) = 1$. Dado que la aplicación bilineal asociada a Q es no degenerada y $(v, v) = 0$, existirá $w \in \mathbb{F}_q^2$, independiente de v, de forma que $(v, w) \neq 0$ y de nuevo lo podemos elegir de forma que $(v, w) = 1$. Supongamos que $Q(w) = a$, evaluamos la forma cuadrática en un vector arbitrario:

$$Q(\alpha v + \beta w) = \alpha^2 Q(v) + \beta^2 Q(w) + \alpha\beta = \alpha^2 + \beta^2 a + \alpha\beta.$$

Como no hay ningún vector singular, esta última expresión tiene que ser distinta de 0 siempre que lo sean α y β. Cualquier vector $\alpha v + \beta w$ es proporcional a uno de la forma $\gamma v + w$ luego nos podemos restringir a este caso sin pérdida de generalidad. Necesitamos por lo tanto que $\gamma^2 + \gamma + a \neq 0$. Según el lema 4.9 esto se dará si y sólo si, al considerar la extensión $[\mathbb{F}_q : \mathbb{F}_2]$ la traza de a es 1.

□

Nota. El plano dotado de la forma cuadrática del primer caso tiene la misma estructura que el plano hiperbólico en característica y par y por lo tanto, también es denominado plano hiperbólico.

Clasificación de característica 2 y dimensión > 2

De nuevo aparece una similitud con los cuerpos de característica impar. Igual que entonces vimos la imposibilidad de que existieran espacios anisotrópicos de dimensión superior a 2, ahora vemos que necesariamente existen vectores singulares en cualquier espacio de dimensión 3 o mayor.

Proposición 4.12. *Dado un espacio vectorial, $\mathbb{F}_q^n$, con $n \geq 3$ y Q una forma cuadrática en él, existe un vector $v \neq 0$ de forma que $Q(v) = 0$.*

Demostración. Sea $v \in \mathbb{F}_q^n$ no nulo, por 4.4 sabemos que $dim(\langle v \rangle^\perp) \geq 2$ y por lo tanto existe $w \in \langle c \rangle^\perp$ independiente de v de forma que $(v, w) = 0$. Sea el vector $v + \eta w$ evaluando Q:

$$Q(v + \eta w) = Q(v) + \eta^2 Q(w).$$

Si $Q(w) = 0$ ya hemos terminado, en caso contrario fijando $\eta = Q(v)Q(w)^{-1}$ hemos encontrado el vector que queríamos.

□

Procediendo de manera idéntica a como se hizo en característica impar, se puede probar el siguiente teorema:

Teorema 4.13. *Dada Q, una forma cuadrática no degenerada en $\mathbb{F}_q^n$; el espacio vectorial se puede descomponer de la siguiente manera:*

$$\mathbb{F}_q^n = H_1 + \cdots + H_{m-1} + R.$$

Donde los H_i son planos hiperbólicos y para R existen las siguientes opciones:

- *Si $n = 2m$ entonces R puede tener la forma de cualquiera de las opciones de 4.11.*
- *Si $n = 2m - 1$ entonces R es un subespacio de dimensión 1 no degenerado.*

Analizaremos una forma cuadrática de la que ya hablamos en el capítulo anterior

$$Q((x_0, x_1, x_2, x_3)) = x_0^2 + x_1^2 + x_2^2 + x_3^2,$$

pero esta vez en el cuerpo $\mathbb{F}_2$. En primer lugar vamos a buscar la expresión de su forma bilineal asociada, sean dos vectores $v = (x_0, x_1, x_2, x_3)$ y $w = (x_0, x_1, x_2, x_3)$, entonces

$$\begin{gathered}(v, w) = Q(v) + Q(w) + Q(v + w) = \\ x_0^2 + x_1^2 + x_2^2 + x_3^2 + y_0^2 + y_1^2 + y_2^2 + y_3^2 + \\ (x_0 + y_0)^2 + (x_1 + y_1)^2 + (x_2 + y_2)^2 + (x_3 + y_3)^2 = 0,\end{gathered}$$

por lo tanto, como consecuencia del lema 4.10 la forma es degenerada. Llama la atención que una forma pueda ser degenerada o no en función del cuerpo sobre el que sea estudiada.

Capítulo 5

Cuádricas en el espacio proyectivo

Fijada una referencia proyectiva en $\mathbb{P}^n(\mathbb{F}_q)$ podemos establecer unas coordenadas homogéneas basadas en las coordenadas usuales en $\mathbb{F}_q^n$. Examinaremos en este capítulo los conjuntos de ceros de las formas cuadráticas entendiéndolos como parte del espacio proyectivo. Veremos que las diferentes formas cuadráticas que aparecen en las clasificaciones dan lugar a conjuntos de puntos con propiedades realmente diferentes.

5.1. Definiciones y conteo

Definición 5.1. *Fijadas una referencia proyectiva en $\mathbb{P}^n(\mathbb{F}_q)$ y una forma cuadrática Q sobre $\mathbb{F}_q^{n+1}$. Si q es impar decimos que un punto $P \in \mathbb{P}^n(\mathbb{F}_q)$ es isotrópico si lo es el subespacio vectorial que lo representa. Si q es par decimos que un punto $P \in \mathbb{P}^n(\mathbb{F}_q)$ es singular si lo son los vectores que lo representan.*

Clasificaremos ahora los diferentes tipos de puntos isotrópicos en función de las diferentes formas cuadráticas que los generan, ver teoremas 3.19 y 4.13.

Definición 5.2. *En las condiciones de la definicion anterior:*

- *Si q es impar (resp. par) denotamos por $Q(2m, q) \subset \mathbb{P}^{2m}(\mathbb{F}_q)$ y llamamos cuádrica parabólica al conjunto de puntos isotrópicos (resp. singulares) de una forma cuadrática no degenerada en $\mathbb{F}_q^{2m+1}$.*

- *Si q es impar (resp. par) denotamos por $Q^+(2m-1, q) \subset \mathbb{P}^{2m-1}(\mathbb{F}_q)$ y llamamos cuádrica hiperbólica al conjunto de puntos isotrópicos (resp. singlares) de una forma cuadrática no degenerada en $\mathbb{F}_q^{2m}$ que permite descomponer el espacio en suma de planos hiperbólicos.*

- *Si q es impar (resp. par) denotamos por $Q^-(2m-1, q) \subset \mathbb{P}^{2m-1}(\mathbb{F}_q)$ y llamamos cuádrica elíptica al conjunto de puntos isotrópicos (resp. singulares) de una forma cuadrática no degenerada en $\mathbb{F}_q^{2m}$ que permite descomponer el espacio en la suma de $m-1$ planos hiperbólicos y un plano anisotrópico (resp. asingular).*

De ahora en adelante no distinguiremos entre el caso de q par o impar, trataremos el caso impar, pero si no se dice lo contrario el resultado también es válido en característica par intercambiando los conceptos de isotrópico y singular. Vamos a ver cuantos puntos contiene cada una de las cuádricas descritas.

Teorema 5.3. *Dada una cuádrica hiperbólica $Q^+(2m-1,q) \subset \mathbb{P}^{2m-1}(\mathbb{F}_q)$, su número de puntos es:*

$$|Q^+(2m-1,q)| = \frac{(q^m-1)(q^{m-1}+1)}{q-1}.$$

Demostración. Trataremos en primer lugar el caso de $m=1$. En este caso la cuádrica está generada por una forma cuadrática, Q, en $\mathbb{F}_q^2$ que da lugar a un plano hiperbólico. Denotaremos por $h_1(\lambda)$ al número de vectores de $v \in \mathbb{F}_q^2$ que cumplen $Q(v)=\lambda$. Si Q es una forma cuadrática hiperbólica y la multiplicamos por una constante seguimos teniendo una forma cuadrática hiperbólica, por lo tanto, cualquier constante $\lambda \neq 0$ debe tener el mismo $h_1(\lambda)$. Por otra parte, vimos en 3.16 que existe una base $\{e_1,e_2\}$ en la que la matriz asociada a la forma bilineal es $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, de esta forma podemos ver que los únicos vectores que cumplen $Q(v)=0$ son los múltiplos de e_1 y los múltiplos de e_2. Acabamos de ver $h_1(0)=2q-1$. En $\mathbb{F}_q^2$ hay q^2 vectores, por lo tanto, quedan $q^2-2q+1=(q-1)^2$ vectores con $Q(v)\neq 0$ por lo tanto, para todo $\lambda \neq 0$ tenemos $h_1(\lambda)=q-1$.

Supongamos ahora que tenemos una forma cuadrática, Q, en $\mathbb{F}_q^{2m}$ de forma que $\mathbb{F}_q^{2m}$ se puede descomponer en suma de m planos hiperbólicos. Sea $h_m(\lambda)$ el número de vectores que cumplen $Q(v)=\lambda$ en $\mathbb{F}_q^{2m}$. Podemos descomponer $\mathbb{F}_q^{2m}$ en un plano hiperbólico, H, y la suma ortogonal de otros $m-1$ planos hiperbólicos, V. Sabemos que dados $v \in H$ y $u \in V$ se cumple $(v,u)=0$, por lo que $Q(v+u)=Q(v)+Q(u)$. Podemos obtener un vector isotrópico de dos formas, suma de uno isotrópico en H con uno isotrópico en V o suma de un vector anisotrópico en H con otro de V también anisotrópico con su valor opuesto. De la primera forma podemos encontrar $h_{m-1}(0)h_1(0)$ vectores. En V hay $q^{2(m-1)}-h_{m-1}(0)$ vectores anisotrópicos, dado un vector con $Q(v)=\alpha$ en V existen en H $h_1(-\alpha)=q-1$ vectores, u, que hacen que $v+u$ sea isotrópico. Por lo tanto, acabamos de encontrar una relación recursiva para los vectores isotrópicos en $\mathbb{F}_q^{2m}$.

$$h_m(0) = h_{m-1}(0)h_1(0) + (q^{2(m-1)} - h_{m-1}(0))h_1(1) = qh_{m-1}(0) + (q-1)q^{2(m-1)}.$$

Veamos por inducción que $h_m(0)=q^{m-1}(q^m+q-1)$. Supongámoslo cierto para $m-1$, entonces:

$$h_m(0) = qq^{m-2}(q^{m-1}+q-1)+(q-1)q^{2(m-1)} = q^m-q^{m-1}+q2m-1 = q^{m-1}(q^m+q-1).$$

Ahora para contar los puntos isotrópicos de $\mathbb{P}^{2m-1}(\mathbb{F}_q)$ tenemos que recordar que el 0 no representa ningún punto en el espacio proyectivo y que cada punto tiene $q-1$ coordenadas distintas. Por lo tanto, el número de puntos isotrópicos es:

$$\frac{h_m(0)-1}{q-1},$$

por lo que finalmente nos queda:

$$|Q^+(2m-1,q)| = \frac{(q^m-1)(q^{m-1}+1)}{q-1}.$$

□

Teorema 5.4. *Dada una cuádrica elíptica $Q^-(2m-1,q) \subset \mathbb{P}^{2m-1}(\mathbb{F}_q)$, su número de puntos es:*

$$|Q^-(2m-1,q)| = \frac{(q^m+1)(q^{m-1}-1)}{q-1}.$$

Demostración. El razonamiento es similar al de la prueba anterior. Sin embargo, $\mathbb{F}_q^{2m}$ se descompone en suma ortogonal de $m-1$ planos hiperbólicos y un plano anisotrópico. Por lo tanto, la relación que podemos utilizar ahora es:

$$e_m(0) = h_{m-1}(0)e_1(0) + (q^{2(m-1)} - h_{m-1}(0))e_m(1),$$

donde $e_m(0)$ representa el número de vectores con $Q(v)=0$ de $\mathbb{F}_q^{2m}$ cuando Q es una forma cuadrática elíptica, y $e_m(1)$ representa el número de vectores con $Q(v)=1$, que ya sabemos que es el mismo número que para cualquier otra constante no nula. Por definición de plano anisotrópico, resulta evidente que el único vector sobre el que la forma cuadrática se anula es el vector 0, luego $e_1(0)=1$, por lo tanto

$$e_m(1) = q^2 - 1/q - 1 = q+1,$$

de forma que conocemos todos los valores necesarios y podemos escribir:

$$e_m(0) = h_{m-1}(0) + (q^{2(m-1)} - h_{m-1}(0))(q+1) = q^{2m-1} - q^m + q^{m-1}.$$

De nuevo el 0 no representa ningún punto en $\mathbb{P}^{2m-1}(\mathbb{F}_q)$ y cada punto es representado por $q-1$ vectores diferentes, por lo tanto:

$$|Q^-(2m-1,q)| = \frac{(q^m+1)(q^{m-1}-1)}{q-1}.$$

□

Teorema 5.5. *Dada una cuádrica $Q(2m,q) \subset \mathbb{P}^{2m}(\mathbb{F}_q)$, su número de puntos es:*

$$|Q(2m,q)| = \frac{q^{2m}-1}{q-1}.$$

Demostración. En este caso tenemos que contar el número de vectores isotrópicos en $\mathbb{F}_q^{2m+1}$ asociados a una forma cuadrática, Q, que permite descomponer $\mathbb{F}_q^{2m+1}$ en la suma de m planos hiperbólicos, V, y un subespacio unidimensional no degenerado, R. En 3.15 vimos que en el caso de q impar había dos formas diferentes, sin embargo, esto no hace diferencia alguna en los ceros de Q puesto que se pasa de una a otra sin más que multiplicar por un no cuadrado. Suponemos entonces que los valores que toma Q en R son todos cuadrados. Dados $v \in V$ y $u \in R$, las formas de que $u+v$ sea isotrópico son, por un lado que v sea isotrópico y u también, sólo hay un vector en R con $Q(u) = 0$ y es el vector nulo, por lo tanto, hay tantos vectores de este tipo en $\mathbb{F}^{2m+2}$ como en V, es decir, $h_m(0)$. La otra opción es que $Q(u)$ sea el opuesto de $Q(v)$. En V tenemos $q^{2m} - h_m(0)$ vectores no isotrópicos, sin embargo, la única opción de encontrar su opuesto en $Q(R)$ es dicho opuesto sea un cuadrado, luego nos tenemos que quedar con la mitad de esos números. Por otra parte en $Q(R)$, cada elemento de $\mathbb{F}_q$ cuadrado está dos veces. El número de vectores w con $Q(w) = 0$ en $\mathbb{F}_q^{2m+1}$ es por lo tanto:

$$h_m(0) + \frac{q^{2m} - h_m(0)}{2} 2 = q^{2m},$$

Teniendo en cuenta que el 0 no representa ningún punto de $\mathbb{P}^{2m}(\mathbb{F}_q)$ y que cada punto es representado por $q-1$ vectores el cardinal de nuestra cuádrica será:

$$|Q(2m, q)| = \frac{q^{2m} - 1}{q - 1}.$$

□

Trataremos en la siguiente sección las cuádricas no degeneradas en espacios proyectivos de dimensión 2 y 3.

5.2. Cuádricas en $\mathbb{P}^2(\mathbb{F}_q)$

Estudiamos la cuádricas el el plano proyectivo, cuya denominación común es la de cónicas. Mantenemos la denominación de cuádricas por homogeneidad con el resto de la memoria.

Nos encontramos ante una cuádrica parabólica como la descrita en el terorema 5.5 en el caso $m = 1$. Por lo tanto, sabemos que $Q(2, q) \subset \mathbb{P}^2(\mathbb{F}_q)$ tiene exactamente $q + 1$ puntos. La misma cantidad de puntos que tiene una recta en $\mathbb{P}^2(\mathbb{F}_q)$, como vimos en 2.9. Sin embargo, sabemos que $Q(2, q)$ no es una recta porque esto implicaría que la forma cuadrática que la genera se anula en todo un plano de $\mathbb{F}_q^3$ y sabemos que es imposible, puesto que resultaría una forma degenerada. Consecuencia de ésto es la siguiente proposición.

Proposición 5.6. *Sea Q una forma cuadrática no degenerada en $\mathbb{F}_q^3$ y $Q(2, q)$ la cuádrica que genera en $\mathbb{P}^2(\mathbb{F}_q)$. Dada una recta $r \subset \mathbb{P}^2(\mathbb{F}_q)$, r tiene como mucho 2 puntos en común con $Q(2, q)$.*

Demostración. Sea $(\cdot,\cdot)$ la aplicación bilineal asociada a Q. Supongamos que existen tres puntos distintos P_1, P_2 y P_3 en $r \cap Q(2,q)$. Estos puntos están representados por tres vectores diferentes v_1, v_2 y v_3, independientes dos a dos y todos ellos contenidos en un mismo plano vectorial en $\mathbb{F}_q^3$. Vamos a ver que entonces Q se anula en todo este plano, lo que es imposible. Podemos escribir v_3 como combinación lineal de los otros dos $v_3 = \alpha v_1 + \beta v_2$, siendo α y β no nulos. Consideramos la base del plano $\{e_1 = \alpha v_1, e_2 = \beta v_2\}$. Puesto que Q se anula sobre v_1 y v_2, para cualquier vector del plano tenemos

$$Q(\lambda e_1 + \gamma e_2) = \lambda\gamma(e_1, e_2),$$

pero como también $(e_1, e_2) = \frac{1}{2}Q(e_1 + e_2) = \frac{1}{2}Q(v_3) = 0$ la forma cuadrática se anula en todo el plano de forma que llegamos a un absurdo.

□

Definición 5.7. *Una recta $l \subset \mathbb{P}^2(\mathbb{F}_q)$, se dice que es tangente a $Q(2,q)$ si en $l \cap Q(2,q)$ hay un único punto.*

Proposición 5.8. *Dada una cuádrica $Q(2,q) \subset \mathbb{P}^2(\mathbb{F}_q)$, por cada punto $P \in Q(2,q)$ pasa una única tangente. Además, si $v_P \in \mathbb{F}_q^3$ es el vector que representa a P, el subespacio que representa a la tangente a $\mathcal{O}$ por P es $\langle v_P\rangle^\perp$.*

Demostración. Sea Q la forma cuadrática que genera la cuádrica y $(\cdot,\cdot)$ la aplicación bilineal asociada. Dado un punto $P \in Q(2,q)$ existe un subespacio $\langle v_P\rangle \subset \mathbb{F}_q^3$ que lo representa, evidentemente $Q(v_P) = 0$. Si consideramos $\langle v_P\rangle^\perp$ por 4.4 es un subespacio de dimensión dos, que contiene a v_P porque es un vector isotrópico. Dado un vector $w \in \langle v\rangle^\perp$ no puede ser isotrópico porque si no $(\cdot,\cdot)$ se anularía en todo el plano $\langle v_P\rangle^\perp$ y esto no se puede dar.

□

Al final del tercer capítulo analizamos la forma cuadrática $Q((x_0,x_1,x_2)) = x_0x_2 - x_1^2$. Ahora analizaremos la cuádrica parabólica a la que da lugar en un plano proyectivo sobre un cuerpo finito de característica impar arbitrario, $\mathbb{F}_q$

$$Q(2,q) = \{(x_0,x_1,x_2)_\Lambda \in \mathbb{P}^2(\mathbb{F}_q) : Q((x_0,x_1,x_2)) = 0\},$$

donde Λ es una referencia proyectiva ya fijada. Si consideramos la recta del infinito r_∞ la que viene determinada por la ecuación $x_0 = 0$, su única intersección con los puntos de $Q(2,q)$ es el punto $P_\infty = (0,0,1)_\Lambda$. Por lo tanto, el resto de puntos de la cuádrica tienen su primera coordenada no nula y para evitar la indeterminación propia de las coordenadas homogéneas la podemos fijar como $x_0 = 1$. El resto de puntos deben cumplir la ecuación $x_2 = x_1^2$, luego dependerán de un único parámetro más, $\lambda \in \mathbb{F}_q$, de forma que para cada valor que tome λ habrá un punto más en $Q(2,q)$ al que denotaremos $P_\lambda = (1,\lambda,\lambda^2)_\Lambda$.
De esta forma acabamos de demostrar que

$$Q(2,q) = \{(1,\lambda,\lambda^2)_\Lambda \in \mathbb{P}^2(\mathbb{F}_q) \mid \lambda \in \mathbb{F}_q\} \cup \{(0,0,1)_\Lambda\}.$$

Resulta evidente que la recta tangente a $Q(2,q)$ en P_∞ es la propia recta del infinito. Veamos que sucede en el resto de puntos de la cuádrica. Ya vimos que la forma bilineal asociada a esta forma cuadrática tiene la forma

$$((x_0,x_1,x_2),(y_0,y_1,y_2)) = \frac{x_0y_2}{2} + \frac{x_2y_0}{2} - x_1y_1,$$

además sabemos que si un punto P_λ es representado por un vector v_λ, su recta tangente es representada por el subespacio $\langle v_\lambda\rangle^\perp$. Para calcular la ecuación implícita que representa a la recta tangente a $Q(2,q)$ por P_λ a la que llamamos r_λ basta con sustituir las coordenadas de P_λ en la forma bilineal simétrica e iguala a cero de lo que obtenemos

$$r_\lambda \equiv \quad ((x_0,x_1,x_2),(1,\lambda,\lambda^2)) = \frac{\lambda^2}{2}x_0 - \lambda x_1 + \frac{1}{2}x_2 = 0.$$

5.3. Cuádricas en $\mathbb{P}^3(\mathbb{F}_q)$

Cuádrica elíptica en $\mathbb{P}^3(\mathbb{F}_q)$

Nos centraremos primero en el caso expuesto en el teorema 5.4 con la particularidad de $m = 2$, por lo tanto, $Q^-(3,q)$ contiene q^2+1 puntos. Al igual que en el caso de las cuádricas en $\mathbb{P}^2(\mathbb{F}_q)$, una forma cuadrática Q que induzca una cuádrica elíptica no se puede anular en un subespacio vectorial de dimensión 2, esto resulta en propiedades similares que se prueban de forma similar.

Proposición 5.9. *Dada una cuádrica elíptica $Q^-(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$ y una recta $r \subset \mathbb{P}^3(\mathbb{F}_q)$, su intersección tiene como mucho 2 puntos.*

Demostración. La prueba es la misma que la de la proposición 5.6, el hecho de Q se anule en tres puntos de una linea en $\mathbb{P}^3(\mathbb{F}_q)$ obliga a que Q se anule sobre todo un plano de $\mathbb{F}_q^4$.

□

Definición 5.10. *Un plano $\pi \subset \mathbb{P}^3(\mathbb{F}_q)$ se dice que es tangente a $Q^-(3,q)$ si la intersección $\pi \cap Q^-(3,q)$ tiene un único punto.*

Proposición 5.11. *Dada una cuádrica elíptica $Q^-(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$, por cada punto $P \in Q^-(3,q)$ pasa un único plano tangente. Si P es representado por el subespacio $\langle v_P\rangle \subset \mathbb{F}_q^4$ el plano tangente a $Q^-(3,q)$ en P es representado por el subespacio $\langle v_P\rangle^\perp$.*

Demostración. De nuevo, vuelve a ser muy similar a la prueba de la proposición 5.8, con la diferencia de que ahora $\langle v_P\rangle^\perp$ tiene dimensión tres y por lo tanto representa a un plano proyectivo.

□

Proposición 5.12. *Sea $Q^-(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$ una cuádrica elíptica. Dado un plano $\pi \subset \mathbb{P}^3(\mathbb{F}_q)$ no tangente a $Q^-(3,q)$ su intersección con dicha cuádrica tiene $q+1$ puntos.*

Demostración. Sea Q la forma cuadrática que genera la cuádrica elíptica y $(\cdot,\cdot)$ la aplicación bilineal asociada. Sea π un plano proyectivo y $L \subset \mathbb{F}_q^4$ el subespacio lineal que lo representa. Si la restricción de Q a L es no degenerada, sabemos que $Q_{|L}$ genera una cuádrica $Q(2,q)$ en L de $q+1$ puntos. Veamos que si π no es tangente, la restricción a L es no degenerada. Para ello supongamos que es degenerada y veamos que entonces π es tangente. Sabemos que Q y $(\cdot,\cdot)$ se pueden anular por completo como mucho en un subespacio vectorial de dimensión 1. Sea $\langle v\rangle \subset L$ el subespacio en el que las restricciones se anulan, entonces $L \subset \langle v\rangle^\perp$ y como por la proposición 3.11 tienen la misma dimensión son iguales, pero hemos visto que $\langle v\rangle^\perp$ es justo el subespacio que representa al plano tangente a $Q^-(3,q)$ que pasa por el punto que representa $\langle v\rangle$.

□

Cuádrica hiperbólica en $\mathbb{P}^3(\mathbb{F}_q)$

Trataremos ahora un caso diferente a los dos anteriores, puesto que la la forma cuadrática que genera $Q^+(3,q)$ permite descomponer $\mathbb{F}_q^4$ en 2 planos hiperbólicos, ahora existen subespacios vectoriales de dimensión 2 sobre los que tanto Q como su forma bilineal asociada, $(\cdot,\cdot)$ se anulan. Por lo tanto, hay rectas en $\mathbb{P}^3(\mathbb{F}_q)$ contenidas en $Q^+(3,q)$. Veamos cuantas:

Proposición 5.13. *Sea $Q^+(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$ una cuádrica hiperbólica. Por cada punto $P \in Q^+(3,q)$ pasan 2 rectas contenidas en $Q^+(3,q)$. En una cuádrica hiperbólica en $\mathbb{P}^3(\mathbb{F}_q)$ hay $2(q+1)$ líneas diferentes.*

Demostración. Sean Q y $(\cdot,\cdot)$ la forma cuadrática y la aplicación bilineal que generan nuestra cuádrica hiperbólica. Sea $P \in Q^+(3,q)$ y sea $\langle v\rangle$ el subespacio lineal que representa a P; como $(v,v)=0$, podemos completar una base de $\mathbb{F}_q^4$, $\mathcal{B}=\{v,v_1,v_2,v_3\}$ en la que la matriz de $(\cdot,\cdot)$ sea

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Buscamos las coordenadas de $\langle v\rangle^\perp$ en dicha base:

$$(a,b,c,d)\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \quad b=0,$$

por lo tanto $\langle v\rangle^\perp$ es la suma ortogonal de $\langle v\rangle$ y un plano hiperbólico, $\langle v_2,v_3\rangle$. De esta forma podemos ver que en $\langle v\rangle^\perp$ hay dos planos completamente isotrópicos, $\langle v,v_2\rangle$ y $\langle v,v_3\rangle$ y por lo tanto, por P pasan dos rectas, representadas por estos subespacios, totalmente contenidas en $Q^+(3,q)$.

Si por cada punto de $Q^+(3,q)$ pasan 2 rectas, el cardinal de la cuádrica es $|Q^+(3,q)| = (q+1)^2$ y en cada recta hay $q+1$ puntos. El número de rectas diferentes es:

$$2\frac{(q+1)^2}{q+1} = 2(q+1).$$

□

Estas rectas que forman $Q^+(3,q)$ tienen una determinada estructura.

Proposición 5.14. *Sea $Q^+(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$ una cuádrica hiperbólica. Las $2(q+1)$ rectas que contiene se dividen en dos grupos de $q+1$ rectas de forma que si dos rectas pertenecen al mismo grupo no tienen intersección entre ellas.*

Demostración. Sea Q la forma cuadrática en
F_q^4 que genera $Q^+(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$ y l una recta contenida en la cuádrica. Consideramos los $q+1$ puntos que según la proposición 2.8 contiene, $l = \{P_0, P_1, \ldots, P_q\}$ representados por $\langle v_i \rangle$. Llamamos g_i a la otra recta que pasa por P_i. Cada recta g_i es representada por $\langle v_i, w_i \rangle$. Supongamos que g_i y g_j se intersecan en un punto representado por $\langle v_i, w_i \rangle \cap \langle v_j, w_j \rangle$, entonces Q se anula sobre el subespacio $\langle v_i, v_j, w_i \rangle$. Sin embargo, Q no se puede anular sobre un subespacio de dimensión mayor que 2 y por lo tanto g_i y g_j no se pueden intersecar. Luego el conjunto de rectas $\{g_0, \ldots, g_q\}$ no presenta intersecciones entre sí.

□

5.4. Cuádricas descomponibles en $\mathbb{P}^2(\mathbb{F}_q)$.

Hemos analizado las cuádricas en el espacio proyectivo con ayuda de la clasificación que hicimos de las formas bilineales simétricas, sin embargo, una cuádrica no deja de ser el conjunto de puntos representados por ceros de polinomios homogéneos de segundo grado. En [San] las cuádricas en $\mathbb{P}^2(\mathbb{F}_q)$ como tal son tratadas y se separan en dos grupos; *cónicas no descomponibles*, que se corresponde con el grupo de cuádricas no degeneradas que ya hemos tratado, y *cónicas descomponibles*. Estas últimas se llaman así porque la ecuación de segundo grado que las define se puede factorizar en producto de dos términos lineales. Vamos a ver como podemos llegar a esta conclusión desde nuestro punto de vista.

Trataremos las cuádricas en $\mathbb{P}^2(\mathbb{F}_q)$ sobre cuerpos de característica impar, es fácil llegar a un resultado equivalente en los cuerpos de característica par.

Teorema 5.15. *La expresión de una forma cuadrática degenerada sobre $\mathbb{F}_q^3$ no nula puede ser factorizada en dos términos lineales. Dependiendo del caso se puede dar:*

- *Dos facotres lineales con coeficientes en una extensión $\mathbb{K}$ de $\mathbb{F}_q$.*
- *Dos factores lineales diferentes con coeficientes en $\mathbb{F}_q$.*
- *Un factor lineal elevado al cuadrado con coeficientes en $\mathbb{F}_q$.*

Demostración. Una forma cuadrática está definida a partir de una forma bilineal simétrica. Supongamos ahora que esta forma, $(\cdot,\cdot)$, es degenerada y que su radical tiene dimensión 1. Supongamos que $rad\,((\cdot,\cdot)) = \langle v_1\rangle$. Si completamos v_0 hasta formar una base de $\mathbb{F}_q^3$, la restricción de la forma bilineal al subespacio bidimensional generado por los otros dos vectores debe ser no degenerado, el teorema 3.16 nos dice que este plano puede ser o bien anisotrópico o bien hiperbólico.

Supongamos que estamos en el primer caso y este subespacio es anisotrópico, como consecuencia del teorema 3.16, v_0 se puede completar hasta una base $\mathcal{B} = \{v_0, v_1, v_2\}$ en la que la matriz asociada a la aplicación sea

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\eta \end{pmatrix},$$

donde recordemos que η es un no cuadrado. Consecuencia de esto la forma en esta base de la forma cuadrática es

$$Q\left((x_0, x_1, x_2)_{\mathcal{B}}\right) = x_1^2 - \eta x_2^2.$$

Evidentemente en $\mathbb{F}_q$ esta ecuación no se puede descomponer en factores lineales puesto que el polinomio $x_1^2 - \eta x_2^2$ no tiene raíces, esto se puede ver teniendo en cuenta que ηx_2^2 es siempre un no cuadrado y x_1^2 es, obviamente, un cuadrado luego no se puede dar $x_1^2 = \eta x_2^2$. Sin embargo, en una extensión de $\mathbb{F}_q$ en la que $\xi^2 = \eta$ tenga solución, tendremos la descomposición $x_1^2 - \eta x_2^2 = (x_1 + \xi x_2)(x_1 - \xi x_2) = 0$.

Si por el contrario el subespacio es hiperbólico, según el teorema 3.16, existirá una base que complete a v_0, $\mathcal{S} = \{\tilde{v}_0, \tilde{v}_1, \tilde{v}_2\}$ en la cual la matriz de Gram de la aplicación es

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Resulta evidente entonces que la expresión explícita en esta base de la forma cuadrática será

$$Q\left((x_0, x_1, x_2)_{\mathcal{S}}\right) = 2\, x_2 x_1,$$

producto de dos factores lineales, x_1 y x_2.

En el caso en el que el radical tenga dimensión 2, es consecuencia de 3.15 que existe una base $\mathcal{G} = \{\hat{v}_0, \hat{v}_1, \hat{v}_2\}$ en la que la forma cuadrática tenga la forma

$$Q\left((x_0, x_1, x_2)_{\mathcal{G}}\right) = \gamma x_2^2,$$

donde γ puede ser cuadrado o no, pero a efectos prácticos es equivalente a la ecuación $x_2^2 = 0$ es decir el producto de un factor lineal consigo mismo.

Es fácil ver que los factores en los que se ha descompuesto cada forma no dejan de ser lineales en ninguna base, pues las coordenadas x_1 y x_2 son combinaciones, también lineales, de las coordenadas en la otra base.

□

Corolario 5.16. *Las cuádricas en $\mathbb{P}^2(\mathbb{F}_q)$ que definen las formas cuadráticas en $\mathbb{F}_q^3$ explicadas en el teorema anterior están formadas en cada caso por:*

- *un único punto,*
- $2q+1$ *puntos situados sobre 2 rectas,*
- *los $q+1$ puntos de una recta.*

Demostración. Siguiendo con la notación de la demostración anterior, con la expresión $Q\left((x_0, x_1, x_2)_{\mathcal{B}}\right) = x_1^2 - \eta x_2^2$, los únicos vectores para los que Q se anula son los representados por $(\lambda, 0, 0)$, es decir los que están en el subespacio $\langle v_0 \rangle \subset \mathbb{F}_q^3$ que representa a un único punto en el plano proyectivo.

En el segundo caso los vectores sobre los Q se anula son los que están en los planos $x_1 = 0$ y $x_2 = 0$, cada uno de ellos representa una recta diferente, ambas se cortan en el punto representado por $\langle v_0 \rangle$.

Finalmente, en el tercer caso los únicos vectores con imagen nula son los que están contenidos en el plano vectorial $x_2 = 0$ que representa una recta en el plano proyectivo.

□

Corolario 5.17. *La expresión de una forma cuadrática no degenerada en $\mathbb{F}_q^3$ no se puede descomponer en factores lineales.*

Demostración. Hemos visto que si la expresión se descompusiese en factores lineales, esta se anularia sobre todo un plano y por lo tanto la cuádrica $Q(2, q) \subset \mathbb{P}^2(\mathbb{F}_q)$ contendría una recta, pero sabemos que esto último no es cierto.

□

Este último corolario nos revela que la denominación de cónica no descomponible es acertada.

Capítulo 6

Curvas

Hemos tratado las cuádricas en el capítulo anterior, algunas de ellas constituyen un caso particular de unos conjuntos del espacio proyectivo, $\mathbb{P}^n(\mathbb{F}_q)$, llamados curvas. Analizaremos estos objetos más generales y en particular trataremos con los óvalos, un tipo de curvas en el plano proyectivo. Veremos en que caso los óvalos son curvas maximales y como, si q es impar, en $\mathbb{P}^2(\mathbb{F}_q)$ los únicos óvalos que existen son las cuádricas $Q(2,q)$ como ya vio Segre en 1955, [Seg].

6.1. Curvas en el espacio proyectivo

Definición 6.1. *Una curva, $\mathcal{A} \subset \mathbb{P}^n(\mathbb{F}_q)$, es un conjunto de al menos $n+1$ puntos de los cuales hay como mucho n contenidos en un mismo hiperplano.*

Consideramos en $\mathbb{P}^n(\mathbb{F}_q)$ el conjunto definido en coordenadas homogéneas como sigue:

$$\mathcal{A} = \{(1, \xi, \xi^2, \ldots, \xi^n) : \xi \in \mathbb{F}_q\} \cup \{(0, 0, \ldots, 0, 1)\},$$

dado un hiperplano, H, se puede definir por una ecuación

$$a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0,$$

si se cumple $a_n = 0$, entonces el punto $(0, 0, \ldots, 0, 1)$ está en el hiperplano; puesto que el polinomio

$$a_0 + a_1t + a_2t^2 + \cdots + a_{n-1}t^{n-1},$$

tiene como mucho $n-1$ raíces diferentes, se cumple $|\mathcal{A} \cap H| \leq n$. Por el contrario, si $a_n \neq 0$, entonces $(0, 0, \ldots, 0, 1)$ no está en el hiperplano y el polinomio

$$a_0 + a_1t + \cdots + a_nt^n,$$

tiene a lo sumo n soluciones. Por lo tanto, dado un hiperplano cualquiera nunca hay más de n puntos de $\mathcal{A}$ en él, luego el conjunto $\mathcal{A}$ es una curva en $\mathbb{P}^n(\mathbb{F}_q)$.

Proposición 6.2. *Si $n \geq q-1$, entonces una curva en $\mathbb{P}^n(\mathbb{F}_q)$ tiene como mucho $n+2$ puntos.*

Demostración. Supongamos que tenemos una curva con $n+2$ puntos. Por definición no hay ningún hiperplano que contenga a $n+1$ puntos, luego si elegimos $n+1$ puntos en la curva son independientes, por lo que estamos en las mismas condiciones que en la definición de referencia proyectiva 2.13. Existe por lo tanto una referencia en la que los $n+2$ puntos que contiene la curva se pueden expresar como:

$$(1,0,\dots,0),\ (0,1,0,\dots,0),\dots,\ (0,\dots,0,1),\ (1,\dots,1)$$

Elegimos otro punto cualquiera, $P \in \mathbb{P}^n(\mathbb{F}_q)$. Podemos escribir $P = (x_0,\dots,x_n)$ en sus coordenadas en la referencia anterior y como $n+1 \geq q$ tenemos dos opciones:

- Hay una coordenada de P nula, en cuyo caso el hiperplano $x_i = 0$ tendría $n+1$ puntos.
- Hay dos coordenadas x_i y x_j iguales, en este caso el hiperplano $x_i = x_j$ tendría $n+1$ puntos.

Sabemos que la igualdad es posible por el ejemplo anterior.

□

6.2. Curvas en el plano

Si nos restringimos al plano, la condición de que un hiperplano no contenga más de n puntos se traduce en que en una misma recta no puede haber más de dos puntos de la misma curva. Esta propiedad es la misma que tiene la cuádrica $Q(2,q)$ que estudiamos en el anterior capítulo, ¿habrá curvas distintas de $Q(2,q)$ en $\mathbb{P}^2(\mathbb{F}_q)$?.

Vamos a analizar cual es el tamaño máximo de una curva $\mathcal{A} \subset \mathbb{P}^2(\mathbb{F}_q)$. Sea un punto $P \in \mathcal{A}$, vimos en 2.9 que por él pasan $q+1$ rectas y en cada una de éstas hay, como mucho, un punto más contenido en $\mathcal{A}$, por lo tanto $|\mathcal{A}| \leq q+2$. Sabemos que las cónicas tienen $q+1$ puntos, estudiamos a continuación la existencia de curvas más grandes.

Definición 6.3. *Un conjunto $\mathcal{O} \subset \mathbb{P}^2(\mathbb{F}_q)$ es un óvalo si es una curva de $q+1$ puntos.*

Sabemos por la proposición 2.9, que por un punto de $\mathbb{P}^2(\mathbb{F}_q)$ pasan $q+1$ rectas. Por lo tanto, dado un punto en un óvalo $P \in \mathcal{O}$, de esas $q+1$ rectas, q quedan definidas por el resto de puntos de $\mathcal{O}$ y la recta restante únicamente insterseca a $\mathcal{O}$ en un punto. Por lo que por cada punto de un óvalo pasa un una única recta tangente a él. Vamos a ver que en el caso en el que el cuerpo sobre el que trabajamos tenga caracaterística 2 existe siempre una curva que contiene al óvalo.

Proposición 6.4. *Sea $q = 2^n$ y $\mathcal{O} \subset \mathbb{P}^2(\mathbb{F}_q)$ un óvalo, entonces dado un punto $P \notin \mathcal{O}$ por él pasan ó una tangente a $\mathcal{O}$ ó $q+1$ tangentes a $\mathcal{O}$.*

Demostración. Dado un punto $P \notin \mathcal{O}$, por él pasan $q+1$ rectas. Como q es un número par, $q+1$ es impar y puesto que en una recta puede haber, a lo sumo, dos puntos de $\mathcal{O}$, tiene que haber al menos una tangente a $\mathcal{O}$ que pase por P. Sabemos que por

cada punto de un óvalo pasa exactamente una tangente. Tenemos por lo tanto que por cada punto de $\mathbb{P}^2(\mathbb{F}_q)$ pasa al menos una tangente y existen $q+1$ tangentes. Es decir:

$$\mathbb{P}^2(\mathbb{F}_q) = \bigcup_{r \text{ tangente a } \mathcal{O}} r.$$

Dado un conjunto de l rectas diferentes contenidas en un plano proyectivo, su unión contiene al máximo número posible de puntos si y sólo si todas ellas tienen el mismo punto en común. En este caso el numero de puntos de la unión es $ql+1$, cada recta aporta q puntos diferentes, a los que añadimos el punto común. Tenemos entonces un grupo de $q+1$ rectas cuya unión forma $\mathbb{P}^2(\mathbb{F}_q)$ que como vimos en la proposición 2.8 tiene q^2+q+1 puntos. Luego todas las rectas deben concurrir en el mismo punto.

Sabemos por lo tanto que por cada punto pasa al menos una recta tangente a $\mathcal{O}$ y existe un punto, N, por el que pasan todas. Supongamos que por un punto fuera de $\mathcal{O}$ pasan dos rectas, esas dos rectas también pasan por N, luego tienen que ser iguales. □

Definición 6.5. *Dado un óvalo en un plano proyectivo sobre un cuerpo de característica 2, $\mathbb{P}^2(\mathbb{F}_q)$; el punto por el que pasan las $q+1$ tangentes a él se denomina núcleo del óvalo.*

La unión de un óvalo, $\mathcal{O} \subset \mathbb{P}^2(\mathbb{F}_{2^n})$, y su núcleo N sigue siendo una curva con la particularidad de que no tiene ninguna recta tangente.

Definición 6.6. *Una curva en $\mathbb{P}^2(\mathbb{F}_q)$ con $q+2$ puntos es un hiperóvalo.*

Proposición 6.7. *Sea q impar y $\mathcal{O}$ un óvalo en $\mathbb{P}^2(\mathbb{F}_q)$. Por cada punto $P \notin \mathcal{O}$ pasan o bien 2 tangentes o ninguna.*

Demostración. Llamamos x_i al número de puntos no contenidos en $\mathcal{O}$ por los que pasan i tangentes. Podemos contar el número de pares (P,t), donde P es un punto no contenido en $\mathcal{O}$ y t es una tangente que pasa por P de dos formas. Por un lado tenemos $q+1$ tangentes y cada una tiene q puntos fuera de $\mathcal{O}$. Por otro, por cada punto contado en x_i pasan i tangentes diferentes. Por lo tanto:

$$q(q+1) = \sum_{i}^{q+1} i x_i. \tag{6.1}$$

Ahora contamos de nuevo de dos formas distintas las ternas (P,t,l) formadas por un punto P y dos tangentes distintas cuya intersección es P. Por un lado, dadas dos tangentes distintas se cortan en un punto fuera de $\mathcal{O}$, ya que por cada punto de $\mathcal{O}$ pasa una única tangente. Por otro lado, si por un punto pasan i tangentes en ese punto hay $i(i-1)$ ternas distintas. Podemos escribir:

$$q(q+1) = \sum_{i}^{q+1} x_i i(i-1) \tag{6.2}$$

Restando la ecuación (6.1) a la ecuación (6.2) nos queda la expresión

$$\sum_i i(i-2)x_i = 0.$$

Como q es impar $q+1$ es par, luego el número de puntos en $\mathcal{O}$ es par y el número de líneas que pasan por un punto es par. Por tanto, dado un punto $P \notin \mathcal{O}$ por él sólo puede pasar un número par de tangentes a $\mathcal{O}$. De esto se deduce que $x_i = 0$ si i es impar y por lo tanto todos los términos de la serie son mayores o iguales que cero luego todos deben ser 0. De esto deducimos que x_i sólo puede ser distinto de 0 si i es 0 ó 2.

□

Proposición 6.8. *Sea q impar, entonces no existen hiperóvalos en $\mathbb{P}^2(\mathbb{F}_q)$.*

Demostración. Todo hiperóvalo contiene un óvalo, por lo tanto para formar un hiperóvalo podemos partir de un óvalo. Sea $\mathcal{O}$ un óvalo en un plano proyectivo sobre un cuerpo $\mathbb{F}_q$ con q impar y sea $P \notin \mathcal{O}$. Por la proposición anterior por P pasan 0 ó 2 tangentes a $\mathcal{O}$ por lo que siempre tienen que pasar secantes a $\mathcal{O}$ así vemos que no podemos añadir otro punto y seguir teniendo una curva, puesto que tendríamos tres puntos alineados.

□

6.3. Teorema de Segre

Vamos a ver que los únicos óvalos que existen en planos proyectivos sobre cuerpos de característica impar son las cuádricas $Q(2,q)$ estudiadas en el capítulo anterior. Esto fue originalmente demostrado por Beniamino Segre en 1955, un matemático italiano nacido en Turin en 1903. Segre fue uno de los pioneros en el estudio de la geometría finita. La prueba original aparece en [Seg], sin embargo, nosotros seguimos una posterior en [Cam].

Teorema 6.9 (**Teorema de Segre**)**.** *Sea q impar y $\mathcal{O}$ un óvalo en $\mathbb{P}^2(\mathbb{F}_q)$, entonces existe una forma cuadrática, Q, de forma que $\mathcal{O}$ es el conjunto de puntos isotrópicos de Q, la cuádrica $Q(2,q)$.*

Demostración. Estructuramos la prueba en pasos:

Paso 1. El producto de todos los elementos en $\mathbb{F}_q^*$ es -1.

Todos los elementos excepto 1 y -1 (que son sus propios inversos) aparecen multiplicados por su inverso, los únicos que prevalecen en el producto son precisamente 1 y -1 luego:

$$\prod_{a \in \mathbb{F}_q^*} a = -1.$$

Paso 2. Dados tres puntos no alineados; P_1, P_2 y P_3; podemos elegir una referencia de forma que las coordenadas en ella de estos puntos sean $(1,0,0)$, $(0,1,0)$ y $(0,0,1)$.

Además, en esta referencia se tiene que las rectas r_i, definidas por pasar por los puntos P_j y P_k con $i \neq j$, $k \neq j$ y $i \neq k$, tienen ecuación $x_i = 0$.

Paso 3. Dadas tres rectas l_1, l_2 y l_3 que pasan por P_1, P_2 y P_3 respectivamente y se cortan en un mismo punto, si sus puntos de corte con r_1, r_2 y r_3 son $(0, 1, a)$, $(b, 0, 1)$ y $(1, c, 0)$; entonces $abc = 1$.

Para demostrarlo, hay a ver que las ecuaciones de l_1, l_2 y l_3 son $x_3 = ax_2$, $x_1 = bx_3$ y $x_2 = cx_1$. Sustituyendo tenemos:

$$x_3 = ax_2 = acx_1 = abcx_3,$$

luego por el paso 1 tenemos $abc = 1$.

Paso 4. Sea $\mathcal{O}$ un óvalo en $\mathbb{P}^2(\mathbb{F}_q)$. Supongamos que los tres puntos (P_1, P_2 y P_3) están sobre $\mathcal{O}$ y las tangentes al óvalo por ellos tienen ecuaciones $x_3 = ax_2$, $x_1 = bx_3$ y $x_2 = cx_1$ respectivamente; entonces abc=-1.

Primero veamos que las tangentes pueden tener esas ecuaciones. Una recta que pasa por P_1 tiene ecuación

$$\alpha x_2 + \beta x_3 = 0,$$

si $\alpha = 0$ la recta pasa por P_2, de hecho es es r_3, y no es tangente y si $\beta = 0$ entonces pasa por P_3, es r_2 y no es tangente tampoco, luego la ecuación está bien definida y $a \neq 0$. Además, corta a r_1 en $(0, 1, a)$.

En $\mathcal{O}$ hay otros $q - 2$ puntos, $p_1, p_2, \ldots, p_{q-2}$, podemos suponer que la recta que pasa por P_1 y p_i tiene ecuación $x_3 = a_i x_2$, por lo tanto corta a r_1 en $(0, 1, a_i)$. Como la recta tangente y estas $q - 2$ rectas son distintas, también lo son a y los a_i, entonces constituyen los $q - 1$ elementos de $\mathbb{F}_q^*$ y por el paso 1 tenemos

$$a \prod_{i=1}^{q-2} a_i = -1.$$

Podemos hacer las mismas construcciones desde P_2 y P_3 obteniendo

$$b \prod_{i=1}^{q-2} b_i = c \prod_{i=1}^{q-2} c_i = -1,$$

por lo tanto:

$$abc \prod_{i=1}^{q-2} a_i b_i c_i = -1.$$

Las rectas que pasan por P_1, P_2 y P_3 y se cortan en p_i cumplen las condiciones del paso 3 y por lo tanto $a_i b_i c_i = 1$ y $abc = -1$.

Paso 5. Dados tres puntos de $\mathcal{O}$ existe una cónica que pasa por ellos y con las mismas tangentes que $\mathcal{O}$ en estos puntos.

Si consideramos los puntos y las tangentes del paso anterior la cónica definida como

$$\mathcal{C} \equiv x_2x_3 - cx_3x_1 + cax_1x_2 = 0,$$

lo cumple. Tanto, $(1,0,0)$ como $(0,1,0)$ y $(0,0,1)$ están en $\mathcal{C}$, además si consideramos la recta $x_3 = ax_2$. La única solución del sistema:

$$\begin{cases} 0 &= x_2x_3 - cx_3x_1 + cax_1x_2 \\ x_3 &= ax_2, \end{cases}$$

distinta de la nula es $(1,0,0)$ así que esta recta es efectivamente una tangente. Lo mismo ocurre con la recta $x_2 = cx_1$. Si añadimos la condición del paso 4 ($abc = -1$) a la recta $x_1 = bx_3$ también le ocurre lo mismo.

Paso 6. Dados 3 puntos de $\mathcal{O}$ y una cuádrica que pase por ellos y tenga las mismas tangentes en dichos puntos $\mathcal{O}$, pasa por el resto de puntos del óvalo con la tangente correcta.

Para demostrarlo consideramos 4 puntos de $\mathcal{O}$; P_1, P_2, P_3 y P_4, representados por los vectores v_1, v_2, v_3 y v_4, con tangentes t_1, t_2, t_3 y t_4 representados por los subespacios $L_1 = \langle v_1, w_1\rangle$, $L_2 = \langle v_2, w_2\rangle$, $L_3 = \langle v_3, w_3\rangle$ y $L_4 = \langle v_4, w_4\rangle$. Consideramos tres formas cuadráticas Q_1, Q_2 y Q_3 que generan las cuádricas que pasan por $\{P_1, P_2, P_3\}$, $\{P_1, P_2, P_4\}$ y $\{P_1, P_3, P_4\}$ respectivamente. Estas formas cuadráticas están determinadas salvo un factor constante. Hemos visto en 5.8 que $L_i = \langle v_i\rangle^\perp$. Todas las matrices tienen la misma tangente t_1 en P_1. Por lo tanto, la matriz de Q_j en L_1 es $\begin{pmatrix} 0 & 0 \\ 0 & \alpha_j \end{pmatrix}$, luego multiplicando por una constante adecuada las tres formas cuadráticas coinciden en L_1.

Consideramos ahora las restricciones de Q_2 y Q_3 a L_4 Razonando igual que antes, la restricción de las formas a este espacio en la base $\{v_4, w_4\}$ tiene forma $\begin{pmatrix} 0 & 0 \\ 0 & \beta_i \end{pmatrix}$, sin embargo, coinciden en $L_1 \cap L_4$, luego tienen que ser iguales. De la misma forma Q_1 y Q_2 coinciden en L_2 y Q_1 coincide con Q_3 en L_3. De esta forma hemos visto que Q_2 y Q_3 coinciden en L_1, L_4 y $L_2 \cap L_3$, lo que las obliga a ser iguales.

□

Capítulo 7

Diseños combinatorios

Los diseños combinatorios se utilizan en experimentos en los que la cantidad de muestras a analizar es muy grande. La idea es conseguir dividir estas muestras de forma efectiva. Por ejemplo, si estamos en una cata de quesos y el objetivo es ser capaces de distinguir de entre dos quesos cual es el mejor, las muestras se dividen en bloques de k elementos cada uno, de forma que cada *fromelier* pruebe las muestras de un bloque. Si conseguimos que dados 2 quesos distintos siempre haya λ bloques en los que estén podremos consultar la opinión de los λ expertos que han probado ambos. Esta estructura es un 2-(v, k, λ) diseño.

Otra situación en la que los diseños son útiles es a la hora de realizar pruebas de alergias. Se pueden elaborar v muestras de forma que en cada una de ellas se encuentren k posibles alérgenos disueltos. Si conseguimos que dadas 2 muestras distintas siempre nos lleven a una sustancia concreta, las dos muestras que mayor reacción produzcan nos conducirán al alérgeno al que más sensibles somos.

7.1. Definición y parámetros

Comenzaremos por definir de manera formal lo que es un diseño.

Definición 7.1. *Dado un conjunto Ω de v elementos, un t-(v, k, λ) diseño es una familia, $\mathcal{D} = \{B_1, \ldots, B_b\}$, de subconjuntos de Ω llamados bloques, que cumple las propiedades:*

- *Cada bloque B_i tiene cardinal k.*
- *Cada subconjunto de Ω de t elementos está contenido en exactamente λ bloques.*

Un caso frecuente en geometría es el de $\lambda = 1$, por ejemplo dos puntos definen una única recta.

Definición 7.2. *Un t-$(v, k, 1)$ diseño es un $S(t, k, v)$ sistema de Steiner.*

Vamos a estudiar dos parámetros que tienen gran importancia a la hora de estudiar los diseños: en cuantos bloques está cada elemento de Ω y cuantos bloques hay en un diseño $\mathcal{D}$.

Proposición 7.3. *Sea $\mathcal{D}$ un t-(v,k,λ) diseño en Ω; cada elemento $\omega \in \Omega$ está en r bloques con:*

$$r = \lambda \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}. \tag{7.1}$$

Demostración. Cada subconjunto de Ω de t elementos, por definición determina λ bloques. Fijado un elemento $\omega \in \Omega$, hay $v-1$ formas de completar ω a una pareja en Ω, $\binom{v-1}{2}$ formas de completarlo a un trío, de la misma forma hay $\binom{v-1}{t-1}$ formas de completar un subconjunto de t elementos. Sin embargo, cada uno de estos bloques puede ser determinado por otro subconjunto de t elementos, veamos cuantas veces estamos contando cada bloque. Dado ω, dentro de un bloque hay $\binom{k-1}{t-1}$ formas de elegir otros $t-1$ elementos dentro del mismo. Por lo tanto:

$$r = \lambda \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}} = \lambda \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}.$$

□

Proposición 7.4. *Un t-(v,k,λ) diseño $\mathcal{D}$ tiene b bloques con:*

$$b = \lambda \frac{v(v-1)(v-2)\cdots(v-t+1)}{k(k-1)(k-2)\cdots(k-t+1)}. \tag{7.2}$$

Demostración. La demostración es muy similar a la anterior, la diferencia es que ahora no partimos de un elemento, pues nuestro objetivo es contar todos los bloques y no sólo los que contienen a un elemento fijado. Ahora tenemos $\binom{v}{2}$ formas de elegir una pareja, $\binom{v}{3}$ formas de elegir una terna y $\binom{v}{t}$ formas de elegir t elementos. Cada subconjunto de t elementos determina λ bloques distintos. Dentro de un bloque hay k elementos, por lo tanto, un subconjunto de t elementos se puede elegir dentro de él de $\binom{v}{t}$ formas diferentes, es decir, estamos contando cada bloque todas esas veces. Finalmente el número total de bloques será:

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}} = \lambda \frac{v(v-1)(v-2)\cdots(v-t+1)}{k(k-1)(k-2)\cdots(k-t+1)}.$$

□

El parámetro r se denomina *parámetro de replicación*. Dividiendo una la ecuacion (7.2) entre (7.1) obtenemos una relación entre los parámetros del diseño:

$$kb = rv,$$

la interpretación combinatoria de esta relación es fácil, por un lado kb es el número de bloques por el número de elementos que contiene cada uno y por el otro, rv es el número de puntos en Ω por el número de bloques en el que está cada uno. De forma que kb y rv son dos formas de contar la misma cantidad.

7.2. Ejemplos conocidos

Las estructuras geométricas son proclives a formar diseños combinatorios. Un claro ejemplo de esto es que dos puntos determinan una única recta o que en un espacio de dimensión n, precisamente n puntos determinan un hiperplano. A lo largo del trabajo ya nos hemos cruzado con varias estructuras que dan lugar a diseños combinatorios, muchos de estos ejemplo aparecen en [Ball] o [LiWi].

Proposición 7.5. *Sea n un número natural y q una potencia entera de un número primo:*

- *El conjunto de las rectas del espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$ es un $S\left(2, q+1, \frac{q^{n+1}-1}{q-1}\right)$ sistema de Steiner.*
- *El conjunto de las rectas del espacio afín $\mathbb{A}^n(\mathbb{F}_q)$ es un $S\,(2, q, q^n)$ sistema de Steiner.*

Demostración. Está claro que dos puntos definen una única recta. Las rectas tienen $q+1$ y q puntos en $\mathbb{P}^n(\mathbb{F}_q)$ y $\mathbb{A}^n(\mathbb{F}_q)$ respectivamente según las proposiciones 2.8 y 2.22. Por otra parte, en el primer caso el espacio ambiente es el espacio proyectivo con $|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}$ y en el segundo, $\Omega = \mathbb{A}^n(\mathbb{F}_q)$ con $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$.

□

Proposición 7.6. *Sea n un número natural y q una potencia entera de un número primo:*

- *El conjunto de hiperplanos del espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$ es un 2-$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^n-1}{q-1}\right)$ diseño.*
- *El conjunto de hiperplanos del espacio afín $\mathbb{A}^n(\mathbb{F}_q)$ es un 2-$\left(q^n, q^{n-1}, \frac{q^{n-1}-1}{q^{n-2}-1}\right)$. diseño*

Demostración. En el primer caso se tiene $\Omega = \mathbb{P}^n(\mathbb{F}_q)$, por lo tanto contiene $v = \frac{q^{n+1}-1}{q-1}$ puntos (elementos). Dos puntos definen una recta que según la proposición 2.9 está contenida en $\frac{q^{n-1}}{q-1}$ hiperplanos distintos. Por otra parte los hiperplanos son subconjuntos de $\frac{q^n-1}{q-1}$ elementos, tal y como dice la proposición 2.8.

En el segundo caso $\Omega = \mathbb{A}^n(\mathbb{F}_q)$, ocurre lo mismo, dos puntos definen una recta que está contenida en $\frac{q^{n-1}-1}{q^{n-2}-1}$ hiperplanos según la proposición 2.22. Añadiendo a esto el tamaño del espacio, $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$ y que el cardinal de los hiperplanos es q^{n-1}, podemos terminar.

□

Podemos considerar sistemas en espacios ambiente más pequeños, por ejemplo en la cuádrica $Q^-(3, q) \subset \mathbb{P}^3(\mathbb{F}_q)$, estudiada en el capítulo quinto. Los diseños con esta estructura se conocen como *planos inversivos* y los estudiaremos en profundidad más adelante.

Proposición 7.7. *Sea $Q^-(3,q) \subset \mathbb{P}^3(\mathbb{F}_q)$ una cuádrica elíptica. Consideramos las intersecciones de planos no tangentes a $Q^-(3,q)$ con la propia cuádrica como bloques. Estos constituyen un $S(3, q+1, q^2+1)$ sistema de Steiner.*

Demostración. Sabemos por el teorema 5.4 que la cuádrica elíptica en $\mathbb{P}^3(\mathbb{F}_q)$ tiene q^2+1 puntos. Dados tres puntos cualesquiera de $Q^-(3,q)$ nunca están alineados, luego definen un único plano en $\mathbb{P}^3(\mathbb{F}_q)$ que evidentemente no es tangente a $Q^-(3,q)$ y cuya intersección con la cuádrica tiene $q+1$ puntos según la proposición 5.12. Luego tres puntos en $Q^-(3,q)$ bastan para determinar un bloque y cada bloque tiene $q-1$ puntos.

□

Introducimos ahora un par de nuevos ejemplos asociados a la conocida estructura de plano afín $\mathbb{A}^2(\mathbb{F}_q)$.

Proposición 7.8. *Dado un plano afín $\mathbb{A}^2(\mathbb{F}_q)$, la familia de los conjuntos formados por pares de lineas paralelas constituye un $2-(q^2, 2q, 2q-1)$ diseño.*

Demostración. Veamos que dos puntos están en $2q-1$ bloques. Tomamos dos puntos $P, Q \in \mathbb{A}^2(\mathbb{F}_q)$. Fijado un punto, P, en el plano afín, por él pasan $q+1$ rectas tal y como se vio en la proposición 2.22. Por lo tanto, por P pasan exactamente q rectas que no contienen a Q; podemos, como vimos en 2.24, identificar una recta paralela a cada una de estas que pase por Q, existen por lo tanto q bloques de este tipo. Por otra parte, si consideramos la recta PQ, podemos tomar una recta secante a ella, s. Por cada uno de los $q-1$ puntos de s distintos del punto de corte con PQ, pasa una recta paralela a la propia PQ, formamos así $q-1$ nuevos bloques. En total, fijados dos puntos, existen exactamente $2q-1$ bloques de los descritos en la proposición que contengan a ambos.

Puesto que una recta contiene q puntos, un bloque contiene $2q$.

□

En [Cag] se dan condiciones necesarias y suficientes para determinar si un cierto $2-(n^2, 2n, 2n-1)$ diseño puede verse como parte de un plano afín.

Proposición 7.9. *Sea q impar. En el plano afín $\mathbb{A}^2(\mathbb{F}_q)$ existen $q+1$ direcciones diferentes, las agrupamos en $\frac{q+1}{2}$ parejas, si dos direcciones están emparejadas decimos que son perpendiculares. El conjunto de bloques formado por las uniones de dos rectas perpendiculares excepto el punto de su intersección constituye un $2-(q^2, 2q-2, 2q-3)$ diseño.*

Demostración. Tomamos dos puntos $P, Q \in \mathbb{A}^2(\mathbb{F}_q)$. Igual que antes, estos puntos pueden estar en un bloque de dos formas distintas. Por una parte la recta PQ define una dirección, por cada uno de los $q-2$ puntos de la recta que son distintos de P y de Q pasa una recta perpendicular a la dirección de PQ, existen por tanto $q-2$ bloques de este tipo. En segundo lugar podemos hacer que por Q pase una recta, r, con una dirección distinta de las definidas por PQ y su perpendicular, de forma que por P pase otra con dirección perpendicular a la de r. Podemos elegir $q-1$ bloques de

este tipo, uno por cada una de las direcciones que no intervienen en los bloques de la primera forma. Por lo tanto, sumando los bloques de ambos tipos tenemos $\lambda = 2q-3$.

Dadas dos rectas que se intersecan en punto, tienen en total $2q-1$ puntos, si a este conjunto le quitamos el punto de la intersección, nos quedan bloques con cardinal $2q-2$.

□

7.3. Planos proyectivos

Dentro de los diseños hay unos muy particulares, su interés reside en que tienen propiedades muy similares a las de los planos proyectivos, son los $S(2, m+1, m^2+m+1)$ sistemas de Steiner. Los bloques tienen $m+1$ elementos, los mismos que tiene una recta proyectiva en un plano de orden m y el espacio total tiene m^2+m+1 puntos, los mismos que un plano proyectivo de orden m. La diferencia estriba en que aquí, en teoría m no está forzado a ser la potencia de un primo, sin embargo, no se conoce ningún diseño de orden compuesto; su existencia es un problema abierto. La principal diferencia con los planos que nosotros hemos tratado, $\mathbb{P}^2(\mathbb{F}_q)$, está en el hecho de que si el orden de estos diseños es compuesto no pueden tener la estructura vectorial detrás que define $\mathbb{P}^2(\mathbb{F}_q)$. Las similitudes entre ambos objetos motivan la siguiente definición:

Definición 7.10. *Un $S(2, n+1, n^2+n+1)$ sistema de Steiner es un plano proyectivo de orden n. A los bloques del diseño los llamamos rectas.*

Gracias a la proposición 7.4 sabemos que el número de bloques es n^2+n+1, es decir, el mismo que el número de puntos. A los diseños con esta propiedad se los conoce como *diseños simétricos*. Puesto que conocemos la relación $kb = rv$, un diseño es simétrico si y sólo si, se tiene la igualdad $k = r$. Por lo tanto, cada punto está en tantos bloques como puntos contiene un bloque, en nuestro caso $n+1$.

Pese a que la existencia de determinados planos proyectivos es un problema abierto, sí que conocemos ciertos límites que han de cumplir, recogidos en el teorema de Bruck-Ryser, 7.18. Antes de proceder con la prueba de este teorema vamos a explicar ciertos conceptos y algún resultado de teoría de números que nos hará falta, los resultados son sencillos, pero una buena referencia para estos hechos de teoría de números es [HaWr].

Definición 7.11. *Dado un sistema de Steiner con v elementos, $a_1, \ldots, a_v$ y b bloques, $B_1, \ldots, B_b$, su matriz de incidencia $A \in \mathcal{M}_{v\times b}$ queda definida por:*

$$A_{ij} = \begin{cases} 1 & si \quad a_i \in B_j \\ 0 & si \quad a_i \notin B_j \end{cases}.$$

Proposición 7.12. *Dado un $2-(v,k,\lambda)$ diseño si A es su matriz de incidencia se cumple:*

$$AA^T = B = (r-\lambda)I + \lambda J,$$

donde r es el parámetro de replicación, I la matriz identidad y J una matriz con todo unos, ambas cuadradas con b columnas.

Demostración. El elemento b_{ii} de B es el producto escalar de la fila i-ésima de A consigo misma, luego cuenta el número de bloques en los que se encuentra el elemento a_i, esto es, r. Por otra parte, el elemento b_{ij} es el producto escalar de la fila $i-$ésima de A con la j-ésima, es decir, cuenta el número de bloques en los que coinciden el elemento a_i y a_j, el parámetro λ.

□

El siguiente lema se debe a Leonard Euler y se cumple en cualquier anillo conmutativo, es conocido como la identidad de los cuatro cuadrados.

Lema 7.13. *Se satisface la siguiente igualdad:*

$$(a_1^2 + a_2^2 + a_3^2 + a_4^4)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

donde

$$\begin{aligned} y_1 &= a_1x_1 - a_2x_2 - a_3x_3 - a_4x_4, \\ y_2 &= a_1x_2 + a_2x_1 + a_3x_4 - a_4x_3, \\ y_1 &= a_1x_3 + a_3x_1 + a_4x_2 - a_2x_4, \\ y_1 &= a_1x_4 + a_4x_3 + a_2x_3 - a_3x_2. \end{aligned}$$

Proposición 7.14. *Sea p un número primo e impar y x_1, x_2, dos enteros, al menos uno de llos no divisible por p, de forma que*

$$x_1^2 + x_2^2 \equiv 0 \text{ (mód } p),$$

entonces p es la suma de dos enteros elevados al cuadrado.

Demostración. Por hipótesis, sabemos que $x_1^2 + x_2^2 = rp$ para algún r positivo. Tomamos una expresión del tipo

$$x_1'^2 + x_2'^2 = rp, \tag{7.3}$$

con r lo más pequeño posible. Si $r = 1$ hemos terminado. Veamos que no puede ser $r > 1$. Elegimos dos enteros u_1, u_2 de forma que $u_1 \equiv x_1$ (mód r) y $u_2 \equiv -x_2$ (mód r). Podemos tomar $|u_i| < r/2$. Evidentemente $x_1^2 + x_2^2 \equiv 0$ (mód r) y por lo tanto:

$$u_1^2 + u_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \text{ (mód } r),$$

luego tenemos la igualdad $u_1^2 + u_2^2 = rs$, como hemos elegido $|u_i| < r/2$, podemos acotar $rs = u_1^2 + u_2^2 < r^2/2$, y por lo tanto, $s < r$. Poniendo todo en común:

$$r^2sp = (x_1^2 + x_2^2)(u_1^2 + u_2^2) = (x_1uu_1 - x_2u_2)^2 + (x_1u_2 + x_2u_1)^2.$$

Puesto que $x_1 \equiv u_1$ (mód r) y $-x_2 \equiv u_2$ (mód r) se cumple:

$$\begin{aligned} (x_1u_1 - x_2u_2) &\equiv (x_1^2 + x_2^2) \equiv 0 \text{ (mód } r), \\ (x_1u_2 + x_2u_1) &\equiv x_1x_2 - x_2x_1 \equiv 0 \text{ (mód } r). \end{aligned}$$

Por lo tanto, $(x_1u_1 - x_2u_2) = ra$ y $(x_1u_2 + x_2u_1) = rb$. Podemos escribir una expresión con la forma de (7.3),

$$sp = a^2 + b^2,$$

que contraviene la elección de r lo más pequeño posible llegando a un absurdo.

□

Proposición 7.15. *Sea p un número primo e impar y x_1, x_2, x_3, x_4 enteros, al menos uno de ellos no divisible por p de forma que*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \ (\text{mód} p),$$

entonces p es la suma de 4 cuadrados.

Demostración. Se prueba de forma muy similar a la anterior. □

Proposición 7.16. *Cualquier entero positivo se puede escribir como la suma de cuatro cuadrados de enteros no negativos.*

Demostración. Gracias al lema 7.13 sabemos que si dos números son la suma de 4 cuadrados su producto también lo es. Por lo tanto, nos basta con probarlo para números primos. Para el 2 podemos escribir $2 = 1^2 + 1^2 + 0^2 + 0^2$ de forma que nos podemos centrar en los primos impares.

Sea p un primo impar, denotaremos durante esta demostración por a a un entero y por $\overline{a}$ a su clase en $\mathbb{F}_p \cong \mathbb{Z}/(p)$. Existen dos casos, -1 es un cuadrado en $\mathbb{F}_p$ o no lo es.

Supongamos que es un cuadrado, entonces existe a de forma que $\overline{a}^2 = -1$, es decir, $a^2 + 1 \equiv 0 \ (\text{mód } p)$ y por 7.14 p es la suma de 2 cuadrados.

Si por el contrario, -1 no es un cuadrado. Sea m el entero más pequeño de forma que $\overline{m}$ no es un cuadrado. Entonces $\overline{-m}$ es un cuadrado por ser producto de no cuadrados y $\overline{m-1}$ también. Por lo tanto, existen x e y de forma que $\overline{x}^2 = \overline{m-1}$ e $\overline{y}^2 = \overline{-m}$. Es decir, $x^2 \equiv m - 1 \ (\text{mód } p)$ e $y^2 \equiv -m \ (\text{mód } p)$, juntándolo todo $x^2 + y^2 + 1^2 \equiv 0 \ (\text{mód } p)$ y de nuevo aplicando 7.15, p es suma de 4 cuadrados.

□

Proposición 7.17. *Dado un entero n, si la ecuación $x^2 + y^2 = nz^2$, tiene soluciones enteras con $(x, y, z) \neq (0, 0, 0)$, entonces n es la suma de dos cuadrados.*

Demostración. Sea $n = p_1^{e_1} \cdots p_t^{e_t}$ la descomposición en primos distintos de n. Podemos suponer que $1 = e_1 = \cdots = e_t$, en caso contrario $n = mu^2$, donde m no tiene ningún factor cuadrado. Si se cumple $m = a^2 + b^2$, entonces $n = (au)^2 + (bu)^2$.

Podemos suponer por tanto $n = p_1 \cdots p_t$, siendo todos los p_i primos y distintos entre sí. Podemos también suponer que x, y y z no tienen factores comunes. Entonces no existe p_i que divida a x e y a la vez, si existiese ó p_i^2 dividiría a n ó p_i dividiría a z. Por la proposición 7.14 para cualquier i el número p_i es la suma de dos cuadrados. Aplicando la igualdad $(x_1^2+x_2^2)(u_1^2+u_2^2) = (x_1u_1-x_2u_2)^2+(x_1u_2+x_2u_1)^2$ repetidamente podemos concluir.

□

Estamos ya en condiciones de probar el teorema de Bruck-Ryser, probado en 1949 por estos dos matemáticos, [BrRy].

Teorema 7.18 (**Bruck-Ryser**). *Si $n \equiv 1$ ó 2 (mód 4) y existe un plano proyectivo de orden n, entonces n es la suma de los cuadrados de dos enteros.*

Demostración. El número de puntos del plano será $N = n^2 + n + 1$, puesto que $n \equiv 1$ ó 2 (mód 4), sabemos que $N \equiv 3$ (mód 4). El parámetro de replicación, r, en un plano proyectivo es $n + 1$, además es un $2 - (n^2 + n + 1, n + 1, 1)$ diseño, luego tal y como vimos en la proposición 7.12, si A es la matriz de incidencia del plano tenemos $AA^T = nI + J$.

Consideramos $x_1, \ldots, x_N$ indeterminadas y definimos $x = (x_1, \ldots, x_N)$. Definimos también $z = xA = (z_1, \ldots, z_n)$, de forma que las z_i son combinaciones lineales de las x_i con coeficientes enteros. Multiplicando z por su traspuesto tenemos:

$$zz^T = nxx^T + xJx^T,$$

que podemos expresar explícitamente como:

$$z_1^2 + \cdots + z_N^2 = n(x_1^2 + \cdots + x_N^2) + w^2, \tag{7.4}$$

donde $w = x_1 + \cdots + x_N$. Consideramos una nueva indeterminada x_{N+1} y añadimos nx_{N+1}^2 a ambos lados de (7.4), resultando:

$$z_1^2 + \cdots + z_N^2 + nx_{N+1}^2 = n(x_1^2 + \cdots + x_{N+1}^2) + w^2, \tag{7.5}$$

El número $N + 1$ es congruente con 0 módulo 4, luego es un múltiplo de 4 y podemos dividir las x_i en grupos de 4. Por la proposición (7.16), sabemos que n se puede escribir como la suma de 4 cuadrados, $n = c_1^2 + c_2^2 + c_3^2 + c_4^2$ y por el lema (7.13) sabemos que el producto de cuatro cuadrados por otros cuatro vuelve a ser la suma de cuatro cuadrados, en particular:

$$n(x_{4l+1}^2 + \cdots + x_{4l+4}^2) = y_{4l+1}^2 + \cdots + y_{4l+4}^2,$$

Donde los y_i vuelven a ser combinaciones lineales enteras de los x_i, de forma que llegamos a la igualdad:

$$z_1^2 + \cdots + z_N^2 + nx_{N+1}^2 = y_1^2 + \cdots + y_{N+1}^2 + w^2, \tag{7.6}$$

Las transformaciones lineales que llevan las x_i en las z_i y en las y_i son ambas invertibles, luego podemos añadir restricciones a la igualdad (7.6) y si éstas son compatibles con dicha ecuación seguiremos teniendo una igualdad. Podemos suponer sin pérdida de generalidad que tanto y_1 como z_1 dependen de x_1. Si no lo hacen con el mismo coeficiente, podemos añadir la restricción $y_1 = z_1$, si el coeficiente es el mismo en ambas combinaciones lineales añadimos la restricción $z_1 = -y_1$ para evitar incompatibilidades; en ambos casos tenemos $z_1^2 = y_1^2$, simplificándose la igualdad (7.6) a:

$$z_2^2 + \cdots + z_N^2 + nx_{N+1}^2 = y_2^2 + \cdots + y_{N+1}^2 + w^2.$$

Podemos repetir este proceso hasta quedarnos con la igualdad:

$$nx_{N+1}^2 = y_{N+1}^2 + w^2$$

Donde y_{N+1} y w son múltiplos racionales de x_{N+1}, podemos por lo tanto, elegir para x_{N+1} un valor entero de forma que y_{N+1} y w sean también enteros. Para cumplirse esa igualdad, por la proposición 7.17, se tiene que dar que n sea la suma de dos cuadrados enteros.

□

Consecuencia inmediata de este teorema es que no existen planos proyectivos de orden 6, 14, 21 e infinitos valores. Un año después de ser probado, en 1950, este teorema fue extendido por el propio Ryser y Chowla a todo tipo de diseños simétricos, [ChoRy].

El primer valor que no es potencia de primo y que el teorema de Bruck-Ryser no descarta es el 10. En 1985 la existencia de un plano proyectivo de orden 10 se redujo a la existencia de cierta configuración de 19 puntos y finalmente en 1989 fue descartada con uso exhaustivo de ordenador, [LaThSw]. Este el único avance que se ha hecho desde 1950.

Capítulo 8

Planos inversivos y ovoides.

Hemos estudiado espacios afines y proyectivos, existen otro tipo de configuraciones geométricas. En este capítulo estudiaremos los planos inversivos, una geometría íntimamente relacionada con los planos afines y cuya estructura combinatoria es muy similar a la del diseño que estudia la proposición 7.7, que utiliza como espacio ambiente los puntos de una cuádrica $Q^-(3,q)$.

8.1. Planos inversivos

En el capítulo anterior analizamos en la proposición 7.7 como podemos inducir un diseño en el espacio ambiente $Q^-(3,q)$ tomando como bloques sus intersecciones con planos de $\mathbb{P}^3(\mathbb{F}_q)$ no tangentes a la cuádrica. De dicha construcción brotaba un $S(3,q+1,q^2+1)$ sistema de Steiner, esta familia de sistemas de Steiner tiene una denominación particular.

Definición 8.1. *Un $S(3,n+1,n^2+1)$ sistema de Steiner se denomina plano inversivo o plano de Moebius de orden n. Sus bloques se denominan circunferencias.*

Por definición, si dos circunferencias tienen tres puntos en común tienen que ser el mismo, por lo tanto, dos circunferencias diferentes se pueden intersecar en 0, 1 ó 2 puntos.

Definición 8.2. *Dado $\mathcal{I}$ un plano inversivo, sean $C, D \subset \Omega$ dos circunferencias:*

- *Si $|C \cap D = 0|$, se dice que los dos circunferencias son paralelas.*
- *Si $|C \cap D = 1|$, se dice que los dos circunferencias son tangentes.*
- *Si $|C \cap D = 2|$, se dice que los dos circunferencias son secantes.*

Con estas definiciones trataremos dos tipos de conjuntos de circunferencias estudiados en [Dem2].

Definición 8.3. *Sea $\mathcal{I}$ un plano inversivo. Dados dos puntos, $P, Q \in \mathcal{I}$ su haz, $\mathcal{B}(P,Q)$ es el conjunto de todas los circunferencias secantes en P y Q.*

Proposición 8.4. *Sea $\mathcal{I}$ un plano inversivo y P, Q dos puntos. El haz $\mathcal{B}(P,Q)$ tiene $q+1$ circunferencias.*

Demostración. Existen q^2-1 puntos en $\mathcal{I}$ distintos de P y Q, cada uno de ellos basta para definir una circunferencia por el que pasen P y Q, sin embargo, cada circunferencia de estas contiene $q-1$ puntos distintos de P y Q luego estamos contando cada circunferencia de $\mathcal{B}(P,Q)$ $q-1$ veces. Por lo tanto

$$|\mathcal{B}(P,Q)| = \frac{q^2-1}{q-1} = q+1.$$

□

Definición 8.5. *Sea $\mathcal{I}$ un plano inversivo y $P \in \mathcal{I}$ un punto. Un haz, $\mathcal{P}(P)$, es un conjunto maximal de circunferencias de forma que dadas dos circunferencias en $\mathcal{P}(I)$ son tangentes en P.*

Nota. Pese a que ambos conjuntos son definidos como haces esto no induce confusión alguna puesto que el primer tipo de haces esta generado de por dos puntos y el segundo por un único punto.

Proposición 8.6. *Sea $\mathcal{I}$ un plano inversivo y $P \in \mathcal{I}$ un punto. Si $\mathcal{P}(P)$ es un haz, entonces hay q circunferencias contenidas en él.*

Demostración. Puesto que el conjunto $\mathcal{P}(P)$ es maximal y por cada punto pasan varias circunferencias tiene que haber al menos una circunferencia $C \in \mathcal{P}(P)$. Sea Q un punto en $\mathcal{I}$ no contenido en C. En el haz $\mathcal{B}(P,Q)$ hay $q+1$ circunferencias de las cuales únicamente una se corta con C sólo en P. De esta forma cada uno de los q^2-q puntos fuera de C define una nueva circunferencia de $\mathcal{P}(P)$, sin embargo, puesto que en cada circunferencia hay q puntos distintos de P, estamos contando cada circunferencia q veces. De esta forma tenemos

$$\frac{q^2-q}{q} = q-1,$$

puntos distintos de C en $\mathcal{P}(P)$ luego en total tenemos q.

□

En el capítulo anterior vimos como los planos proyectivos se pueden definir también como diseños pese a que en la práctica los únicos que conocemos son los que están construidos sobre cuerpos. Lo mismo ocurre con los planos afines.

Definición 8.7. *Un $S(2,n,n^2)$ sistema de Steiner es un plano afín. Los bloques son rectas.*

Las propiedades enumeradas en el teorema 2.24 siguen siendo ciertas con esta definición de plano afín. Vamos a analizar la relación que tiene un plano afín y un plano inversivo.

Proposición 8.8. *Sea $\mathcal{I}$ un plano inversivo de orden n y $P \in \mathcal{I}$ un punto. Si $\mathcal{C}_P$ es el conjunto de las circunferencias que contienen a P. El conjunto $\Omega - \{P\}$ con los bloques $C - \{P\}$ con $C \in \mathcal{C}_P$ es un plano afín de orden n.*

Demostración. Evidentemente $\mathcal{A} = \Omega - \{P\}$ tiene cardinal q^2. Nos falta probar que cada dos puntos de $\mathcal{A}$ definen una recta. Sean dos puntos $Q, M \in \mathcal{A}$, entonces existe una única circunferencia en Ω que contenga a P, Q y M, sea C dicha circunferencia, entonces $C - \{P\}$ es la recta en $\mathcal{A}$ que buscamos. Hemos probado que $\mathcal{A}$ con los bloques definidos es un $S(2, q^2, q)$ sistema de Steiner y por lo tanto un plano afín. □

Se puede ver como de esta forma los haces $\mathcal{P}(P)$ dan lugar a conjuntos de rectas paralelas entre sí y como los haces $\mathcal{B}(P, Q)$ dan lugar a los conjuntos de rectas que pasan por Q en el plano afín. Veremos a continuación como esta relación entre los planos afines y los planos inversivos se puede ver en alguna ocasión de una forma más explícita.

Dentro del plano complejo, 2 puntos definen una recta y 3 puntos determinan una única circunferencia. Si a $\mathbb{C}$ le añadimos un punto, ∞, y denotamos $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Por medio de la conocida proyección estereográfica podemos identificar una esfera con $\bar{\mathbb{C}}$, esta construcción es la esfera de Riemman. En la esfera tres puntos siempre definen una circunferencia. Si dada una recta $r \subset \mathbb{C}$ definimos en $\bar{\mathbb{C}}$ una circunferencia generalizada como $r \cup \{\infty\}$ tres puntos en $\bar{\mathbb{C}}$ siempre determinan una circunferencia. En el caso de que los tres puntos pertenezcan a $\mathbb{C}$ y no estén alineados la circunferencia que determinan en $\mathbb{C}$ es la que determinan en $\bar{\mathbb{C}}$. Si dos de los puntos pertenecen a $\mathbb{C}$ y el tercero es ∞ ó se trata de tres puntos alineados en $\mathbb{C}$, la circunferencia que definen en $\bar{\mathbb{C}}$ es la circunferencia generalizada correspondiente.

De forma análoga al caso complejo que acabamos de exponer, se puede completar un plano afín finito, $\mathbb{A}^2(\mathbb{F}_q)$, para formar un plano inversivo. La expresión de una circunferencia a la que estamos acostumbrados es:

$$\{(x, y) \in \mathbb{R}^2 | (x - a)^2 + (y - b)^2 = r^2;\ r \neq 0\},$$

veamos que en el caso de geometrías finitas se puede tratar de forma similar.

Lema 8.9. *Dados tres puntos $A, B, C \in \mathbb{A}^2(\mathbb{F}_q)$ y fijada una referencia afín, $\mathcal{R}$; existe una única ecuación con la forma*

$$(x - a)^2 + (y - b)^2 = \rho; \quad a, b \in \mathbb{F}_q;\ \rho \in \mathbb{F}_q^*,$$

que sea satisfecha por las coordenadas de los tres puntos en $\mathcal{R}$.

Demostración. La ecuación $(x - a)^2 + (y - b)^2 = \rho$ se desarrolla de la forma

$$\alpha x + \beta y + \gamma = -(x^2 + y^2), \tag{8.1}$$

donde $\alpha = -2a$, $\beta = -2b$ $\gamma = a^2 + b^2 - \lambda$. Sustituyendo las coordenadas de A, B y C en la ecuación (8.1) obtenemos un sistema lineal de ecuaciones. Puesto que los tres

puntos no están alineados, obtenemos una solución única para los coeficientes α, β y γ a partir de los cuales podemos obtener, de nuevo de forma única los coeficientes originales, a, b y ρ.

□

Analizaremos ahora bajo que condiciones este tipo de ecuaciones da efectivamente lugar a bloques de $q+1$ elementos.

Proposición 8.10. *Siempre que $\mathbb{F}_q$ sea un cuerpo en el que -1 no es cuadrado el conjunto de puntos afines*

$$\{(x,y) \in \mathbb{A}^2(\mathbb{F}_q) | (x-a)^2 + (y-b)^2 = \rho;\ a,b \in \mathbb{F}_q;\ \rho \in \mathbb{F}_q^*\}$$

tiene cardinal $q+1$.

Demostración. Basta con probarlo para la ecuación $x^2+y^2=\rho$, puesto que el paso a otras ecuaciones es una mera traslación. Recordando la inmersión afín en el espacio proyectivo que hicimos en 2.28, podemos ver $\mathbb{A}^2(\mathbb{F}_q)$ embebido en $\mathbb{P}^2(\mathbb{F}_q)$. Utilizaremos en el plano proyectivo unas coordenadas (x,y,z), en las que la recta del infinito r_∞ sea representada por la ecuación $z=0$.

La forma cuadrática $Q((x,y,z)) = x^2+y^2-\rho z^2$, es no degenerada y por lo tanto representa $q+1$ puntos en $\mathbb{P}^2(\mathbb{F}_q)$. Los $q+1$ puntos estarán en $\mathbb{A}^2(\mathbb{F}_q)$ si y sólo si, no hay ninguno sobre r_∞, es decir, si y sólo si, no hay soluciones de la ecuación

$$Q((x,y,z)) = x^2+y^2-\rho z^2 = 0, \tag{8.2}$$

compatibles con $z=0$. Esto es cierto si y sólo si, la ecuación

$$x^2+y^2=0,$$

no tiene solución alguna en $\mathbb{F}_q$, lo que se cumple si y sólo si -1 no es un cuadrado en $\mathbb{F}_q$.

En este caso, todos los puntos que sean solución de (8.2) tendrán su tercera coordenada distinta de 0, por lo tanto, todos los puntos admitirán un única representación de la forma $(x,y,1)$. Lo que significa que la ecuación se puede transformar en

$$x^2+y^2=\rho,$$

y ya sabemos que tiene $q+1$ soluciones que son los puntos afines representados en el enunciado de la proposición.

□

Nota. Recordamos que en los cuerpos de característica par $-1=1$ y por lo tanto, siempre es un cuadrado. Por otra parte, los cuerpos de característica impar en los que -1 es cuadrado son aquellos en los que q es de la forma $q=4t+1$ como vimos en la proposición 1.32. Por lo tanto los cuerpos en los que esto funciona es los que q tiene la forma $q=4t-1$.

Definición 8.11. *Sea $\mathbb{A}^2(\mathbb{F}_q)$ un plano afín sobre un cuerpo, $\mathbb{F}_q$ en el que -1 no es un cuadrado. Entonces el conjunto de $q+1$ puntos*

$$\{(x,y) \in \mathbb{A}^2(\mathbb{F}_q) | (x-a)^2 + (y-b)^2 = \rho;\ a,b \in \mathbb{F}_q;\ \rho \in \mathbb{F}_q^*\},$$

es una circunferencia.

Proposición 8.12. *Sea $\mathbb{F}_q$ un cuerpo en el que -1 no es un cuadrado. El conjunto $\mathbb{A}^2(\mathbb{F}_q) \cup \{\infty\}$ con las circunferencias de $\mathbb{A}^2(\mathbb{F}_q)$ y los conjuntos $r \cup \{\infty\}$; con $r \subset \mathbb{A}^2(\mathbb{F}_q)$ una recta; actuando como circunferencias, es un plano inversivo.*

Demostración. El plano afín tiene q^2 puntos, a los que añadimos el punto del infinito, luego en total hay q^2+1 puntos. Dados tres puntos, si los tres están en $\mathbb{A}^2(\mathbb{F}_q)$ y no están alineados, por el lema 8.9 hay una única ecuación del tipo

$$(x-a)^2 + (y-b)^2 = \rho; \quad a,b \in \mathbb{F}_q;\ \rho \in \mathbb{F}_q^*,$$

que los representa. Además puesto que -1 no es un cuadrado, por la proposición 8.10 esta ecuación define una circunferencia de $q+1$ puntos. Si por el contrario los tres puntos están en $\mathbb{A}^2(\mathbb{F}_q)$ pero alineados o uno de ellos es ∞, definen de forma evidente un único bloque del tipo $r \cup \{\infty\}$, que también tiene $q+1$ puntos.

□

En los teoremas 2.10 y 2.24 se expusieron una serie de propiedades de los espacios proyectivo y afín respectivamente, de hecho ambas estructuras se pueden construir axiomáticamente a partir de dichas propiedades. Lo mismo ocurre con los planos inversivos.

Teorema 8.13. *Sea $\mathcal{I}$ un plano inversivo y $\mathcal{C}$ el conjunto de sus circunferencias. Entonces se cumplen las siguientes propiedades:*

I *Dados tres puntos distintos existe una única circunferencia en $\mathcal{C}$ que contenga a todos.*

II *Sean $P,Q \in \mathcal{I}$ y $C \in \mathcal{C}$ de forma que $P \in C$ y $Q \notin C$, entonces existe una única circunferencia $D \in \mathcal{C}$ de forma que $Q \in D$ y $C \cap D = \{P\}$.*

III *Hay al menos dos circunferencias y al menos tres puntos en cada circunferencia.*

Demostración. La primera propiedad es consecuencia directa de la definición de sistema de Steiner. Para probar la segunda nos apoyamos en el mismo argumento que hemos utilizado en la prueba de la proposición 8.6. En el haz $\mathcal{B}(P,Q)$ hay $q+1$ circunferencias, q de ellos están definidos por P, Q y cada uno de los q puntos de C distintos de P, la circunferencia restante es nuestra circunferencia D. La tercera propiedad es simplemente una condición para evitar casos degenerados. □

8.2. Ovoides

La definición de ovoide se puede escribir en cualquier dimensión, sin embargo, únicamente existen en espacios proyectivos de dimensión inferior a 4 [Ball]. Nosotros trabajaremos desde el principio en $\mathbb{P}^3(\mathbb{F}_q)$ puesto que nuestro objetivo es llegar a los planos inversivos, estructuras con las que están intimamente relacionadas.

Definición 8.14. *Un ovoide es un subconjunto $\mathcal{O} \subset \mathbb{P}^3(\mathbb{F}_q)$ que cumple con las propiedades:*

I *Cada linea de $\mathbb{P}^3(\mathbb{F}_q)$ interseca a $\mathcal{O}$ en 2 puntos como máximo.*

II *Dado un punto $P \in \mathcal{O}$ la unión de todas las rectas cuya intersección con $\mathcal{O}$ es exactamente $\{P\}$ es un plano, al que llamamos plano tangente a $\mathcal{O}$ por P.*

Las cuádricas elípticas $Q^-(3,q)$ que ya estudiamos en quinto capítulo constituyen un ejemplo de ovoide en $\mathbb{P}^3(\mathbb{F}_q)$ puesto que cumplen ambas condiciones de la definición, como vimos en las proposiciones 5.9 y 5.11 respectivamente. Otras propiedades de estas cónicas, relativas a su cardinal y a su relación con los planos proyectivos, que ya fueron estudiadas en las proposiciones 5.4 y 5.12 se hacen extensivas a todos los ovoides de $\mathbb{P}^3(\mathbb{F}_q)$ como reflejan las dos proposiciones siguientes.

Proposición 8.15. *Un ovoide $\mathcal{O} \subset \mathbb{P}^3(\mathbb{F}_q)$ contiene q^2+1 puntos.*

Demostración. Sea $P \in \mathcal{O}$, las rectas que pasan por él deben cortar al ovoide en uno ó dos puntos. Las rectas que lo cortan en punto forman un plano, sabemos que dentro de un plano pasan por un punto $q+1$ rectas gracias a la proposición 2.8. Por lo tanto, el resto de las $\frac{q^3-1}{q-1} = q^2+q+1$ rectas de $\mathbb{P}^3(\mathbb{F}_q)$ que pasan por P tienen que cortar a $\mathcal{O}$ en dos puntos luego definen un punto distinto cada una. En total tenemos el punto P más los q^2 puntos que acabamos de definir, luego:

$$|\mathcal{O}| = q^2+1$$

.

□

Proposición 8.16. *Sea $\mathcal{O} \subset \mathbb{P}^3(\mathbb{F}_q)$ un ovoide. Dado un plano $\pi \subset \mathbb{P}^3(\mathbb{F}_q)$ existen dos opciones:*

- *O bien $\pi \cap \mathcal{O}$ es un óvalo en π.*
- *O bien $\pi \cap \mathcal{O}$ es un único punto y π es el plano tangente a $\mathcal{O}$ en él.*

Demostración. Sea $\mathcal{O}$ un ovoide en $\mathbb{P}^3(\mathbb{F}_q)$. Sabemos por la proposición 2.8 que hay q^3+q^2+q+1 planos en $\mathbb{P}^3(\mathbb{F}_q)$. Sea $P \in \mathcal{O}$ un punto, por P pasa exactamente un plano tangente π_P, en el que están contenidas todas las rectas cuyo único punto de corte con $\mathcal{O}$ es P. Sabemos por 2.9 que por P pasan q^2+q+1 planos, sea π un plano de ellos distinto de π_P. Veamos que $\pi \cap \mathcal{O}$ es un óvalo en π. Puesto que el espacio ambiente es un plano, la condición de curva exige que no haya más de dos puntos

en una misma recta de π, esto es inmediato de la definición de ovoide, si vemos que además el cardinal de la intersección es $q+1$ sabremos que efectivamente se trata de un óvalo.

La proposición 2.9 nos dice que por P pasan exactamente $q+1$ rectas contenidas en π, además su unión es el propio π

$$\bigcup_{i=0}^{q} r_i = \pi.$$

Una de estas rectas, por ejemplo r_0, es la intersección $\pi \cap \pi_P$ y su único punto en común con $\mathcal{O}$ es el propio P. Existen por lo tanto q rectas $\{r_1, \dots r_q\}$ en la expresión anterior de π, que cortan a $\mathcal{O}$ en dos puntos de forma que cada una define un punto, P_i, distinto de P en $\mathcal{O}$, estos q puntos unidos a P conforman el total de la intersección $\pi \cap \mathcal{O}$.

Veamos cuantos planos hay de este tipo. Para definir un plano de este tipo nos hacen falta 3 puntos en $\mathcal{O}$, luego hay $\binom{q^2+1}{3}$ formas de definir un plano con 3 puntos del ovoide, sin embargo, cada uno de estos planos tiene $q+1$ puntos en $\mathcal{O}$ luego hay $\binom{q+1}{3}$ formas de definir el mismo plano. En definitiva hay

$$\frac{\binom{q^2+1}{3}}{\binom{q+1}{3}} = \frac{(q^2+1)q(q^2-1)}{(q+1)q(q-1)} = q^3+q,$$

planos de este tipo. Sumando los q^2+1 planos tangentes a estos q^3+q tenemos el número total de planos en $\mathbb{P}^3(\mathbb{F}_q)$, q^3+q^2+q+1, luego no hay otro tipo de planos. □

En el quinto capítulo vimos que los óvalos en planos proyectivos sobre cuerpos de característica impar eran siempre cuádricas $Q(2,q)$, este resultado es el teorema de Segre. Por lo expuesto en la anterior proposición sabemos que dado un ovoide $\mathcal{O} \subset \mathbb{P}^3(\mathbb{F}_q)$, su intersección con un plano no tangente al ovoide, π, se puede identificar con los ceros de una cuádrica en el subespacio que represente a π. Uniendo todas estas cuádricas, en 1955, Barlotti y Panela, de forma independiente, consiguieron extender el teorema de Segre llegando al siguiente teorema [Bar], [Pan].

Teorema 8.17 (Barlotti-Panella). *Sea q impar y $\mathcal{O}$ un ovoide en $\mathbb{P}^3(\mathbb{F}_q)$. Existe una forma cuadrática elíptica, Q, en $\mathbb{F}_q^4$ de forma que su conjunto de puntos isotrópicos, la cuádrica $Q^-(3,q)$, es igual a $\mathcal{O}$.*

Por lo tanto, queda descartada la existencia de ovoides diferentes de los que ya conocíamos en espacios proyectivos sobre cuerpos de característica impar. Esto no es así en cuerpos de característica par, en los cuerpos de orden $q = 2^{2l-1}$ se conoce otro tipo de ovoide, el ovoide de Tits. Este objeto fue descubierto por Jacques Tits en 1962, [Tit] como ya hemos comentado sólo existe en cuerpos en los que q es una potencia impar de 2. La representación de este ovoide en coordenadas homogéneas dada una referencia $\mathcal{R}$ es:

$$\{(d, t, s^\sigma + st + t^{\sigma+2}, 1)_\mathcal{R} : s, t \in \mathbb{F}_q\} \cup \{(0, 0, 1, 0)_\mathcal{R}\},$$

donde α^σ representa el morfismo de cuerpos dado por

$$t \mapsto t^\sigma = t^{2^l}.$$

Recordemos que estamos trabajando en cuerpos con orden $q = 2^{2l-1}$.

Se conocen en la actualidad dos familias de ovoides en espacios proyectivos $\mathbb{P}^3(\mathbb{F}_q)$; las cuádricas elípticas, que existen para todos los cuerpos y los ovoides de Tits que únicamente existen en espacios sobre cuerpos de determinado orden. La existencia o no de otros ovoides a día de hoy es un problema abierto.

Igual que ocurre en el caso de las cuádricas $Q^-(3, q)$ cualquier ovoide en $\mathbb{P}^3(\mathbb{F}_q)$ define un plano inversivo.

Proposición 8.18. *Sea $\mathcal{O} \subset \mathbb{P}^3(\mathbb{F}_q)$ un ovoide. Consideramos las intersecciones de planos no tangentes a $\mathcal{O}$ con la propia cuádrica como circunferencias. El ovoide $\mathcal{O}$ con estos bloques constituye un plano inversivo.*

Demostración. Dados tres puntos de $\mathcal{O}$ definen un plano no tangente y por 8.16 su intersección con $\mathcal{O}$ tiene exactamente $q + 1$ puntos, luego tres puntos de $\mathcal{O}$ definen una circunferencia de $q + 1$ elementos. Por la proposición 8.15 $\mathcal{O}$ tiene $q^2 + 1$ puntos. □

De hecho es posible que todos los planos inversivos sean isomorfos a estructuras de este tipo. En 1963 Peter Dembowsky probo un resultado parcial para esto, [Dem1].

Teorema 8.19. *Todo plano inversivo de orden par n es isomorfo a la estructura de incidencia de puntos e intersecciones por planos de un ovoide en un espacio proyectivo de orden n.*

En particular esto implica que si existe un plano inversivo de orden par n, entonces n es una potencia de 2. No se conocen planos inversivos de orden impar que no provengan de cuádricas elípticas en $\mathbb{P}^3(\mathbb{F}_q)$.

Bibliografía

[Ball] Simeon Ball, Finite geometry and combinatorial applications, Cambridge University Press, (2015).

[Bar] Barlotti, A. (1955). "Un'estensione del teorema di Segre-Kustaanheimo". Bollettino dell'Unione Matematica Italiana. 3rd ser. 10, 498–506.

[BeuRos] A. Beutelspacher, U. Rosenbaum, Projective Geometry, Cambridge University Press (1998).

[BrRy] Bruck, R.H.; Ryser, H.J.,"The nonexistence of certain finite projective planes", Canadian Journal of Mathematics, 1 (1949) 88–93.

[Cag] Andrea Caggegi "$2-(n^2, 2n, 2n-1)$ designs obtained from affine planes", Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica. 1 (2006) 31-34.

[Cam] P. J. Cameron, Combinatorics: topics, techniques, algorithms, Cambridge University Press, (1994).

[Cas] Eduardo Casas-Alvero, Analytic Projective Geometry, European Mathematical Society (2014).

[ChoRy] Chowla, S.; Ryser, H.J., "Combinatorial problems", Canadian Journal of Mathematics, 2 (1950) 93–99.

[Dem1] P. Dembowski, "Inversive planes of even order", Bull. Amer. Math. Soc., 69 850– 854 (1963).

[Dem2] Peter Dembowsky, "Finite Geometries", Springer (1968).

[Hall] M. Hall Jr., Combinatorial Theory, John Wiley & Sons (1986).

[HaWr] Hardy G.H.; Wright E.M, Introduction to the theory of numbers, Oxford University Press, (1938).

[LaThSw] C. Lam, L. Thiel, S.Swierz, "The non-existence of finite projective planes or order 10", Canadian Journal of Mathematics, 6(1989) 1117-1123.

[LiWi] J.H. van Lint & R.M. Wilson, A course in combinatorics, Cambridge University Press, (1994).

[Pan] Panella, G. . "Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito". Bollettino dell'Unione Matematica Italiana. 3rd ser. 10 (1995) 507–513.

[Rom] S. Roman, Field Theory, 2^{nd} edition, Springer (2006).

[San] Luis A. Santaló, Geometría proyectiva, Editorial universitaria de Buenos Aires (1977).

[Seg] B. Segre, Ovals in a finite projective plane, Canad. J. Math. 7 (1955) 414–416.

[Tit] J. Tits, Ovoïdes et groupes de Suzuki, Arch. Math 13 (1962), 187-198.