Capítulo 11

Anillos y cuerpos

1. Definiciones y propiedades
2. El anillo de los polinomios
3. Cuerpos finitos

En el capítulo anterior se ha estudiado la estructura algebraica más completa definida a partir de una operación, la estructura de grupo. En este capítulo iniciaremos el estudio de estructuras algebraicas definidas a partir de dos operaciones, los anillos y los cuerpos, introducidas en el primer capítulo de esta última parte.

Los sistemas de numeración algebraicamente más completos están construidos a partir de dos operaciones: la suma y el producto. Esto hace que sea importante el estudio de conjuntos que se comporten de forma similar desde el punto de vista algebraico.

La primera sección de este capítulo está dedicada al estudio de las propiedades básicas de los anillos y de los cuerpos. Se introducen las nociones de ideal y anillo cociente, que serán útiles más adelante. La segunda sección se dedica al estudio de un ejemplo importante de anillo, el anillo de los polinomios, que se utilizará para la construcción de cuerpos finitos en la última sección de este capítulo. Las aplicaciones basadas en estas estructuras se estudiarán en el último capítulo.

11.1 Definiciones y propiedades

Recordemos que un *anillo* $A = (A, \star, \circ)$ es una estructura algebraica en la cual A es un conjunto y '$\star$', '$\circ$' son operaciones binarias definidas sobre A que satisfacen las condiciones siguientes:

A1 $(A, \star)$ es un grupo abeliano.

A2 $(A, \circ)$ es un semigrupo.

A3 '$\circ$' es distributiva respecto de '$\star$'. Esto es, para todo $a, b \in A$,

$$\begin{cases} a \circ (b \star c) = (a \circ b) \star (a \circ c) \\ (a \star b) \circ c = (a \circ c) \star (b \circ c) \end{cases}$$

El ejemplo más sencillo y representativo de estructura de anillo lo encontramos en $(\mathbb{Z}, +, \cdot)$, el anillo de los enteros. De hecho, éste es un ejemplo de *anillo unitario*, es decir, admite elemento neutro respecto de la segunda operación. Hay, sin embargo, autores que incluyen dentro de los axiomas de anillo la existencia de este elemento neutro. Esto se debe al hecho de que la mayoría de los anillos más utilizados cumplen este requisito.

Por similitud con $(\mathbb{Z}, +, \cdot)$, cuando tratemos con un anillo unitario cualquiera, en general nos referiremos a la suma y al producto como primera y segunda operación respectivamente y utilizaremos el 0 y el 1 como neutros respectivos. Para abreviar la notación, escribiremos ab en lugar de $a \cdot b$.

Está claro que los axiomas de anillo son una abstracción del comportamiento de los números enteros respecto de las operaciones aritméticas elementales: la suma y el producto. Sin embargo, $(\mathbb{Z}, +, \cdot)$ tiene, además, otras propiedades referidas a la segunda operación que permiten refinar esta estructura. Así, la conmutatividad de esta segunda operación conlleva la estructura de *anillo abeliano*. Esta propiedad no la comparten, sin embargo, todos los anillos, como es el caso del anillo de las matrices cuadradas de orden 2 sobre $\mathbb{Z}$, $(M_2(\mathbb{Z}), +, \cdot)$.

Ejercicio 11.1. Demostrar que $(M_2(\mathbb{Z}), +, \cdot)$ es un anillo unitario no abeliano.

Una clase importante de anillos abelianos unitarios finitos es $(\mathbb{Z}_n, +, \cdot)$, el anillo de los enteros módulo n.

Ejercicio 11.2. Demostrar que $(\mathbb{Z}_n, +, \cdot)$ es un anillo unitario abeliano.

La *ley de simplificación* es otra propiedad importante que cumplen los números enteros, es decir, para todo $a, b, c \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ se verifica

$$ab = ac \Longrightarrow b = c$$

Esta propiedad está relacionada con la definición siguiente.

Diremos que el anillo $(A, +, \cdot)$ admite *divisores de cero* si existen $a, b \in A \setminus \{0\}$ tales que $ab = 0$.

Ejercicio 11.3. Demostrar que en un anillo A se verifica la ley de simplificación si y sólo si A no tiene divisores de cero.

El anillo $\mathbb{Z}$ de los enteros no tiene divisores de cero, pero es fácil encontrar ejemplos de anillos que sí tienen. En $\mathbb{Z}_6$, por ejemplo, se cumple que $[2][3] = [4][3] = [0]$ y por tanto $[2]$, $[3]$ y $[4]$ son divisores de cero. Cabe observar, sin embargo, que $[2] \neq [4]$. Por ello, en $\mathbb{Z}_6$ no es válida la ley de simplificación.

Se puede comprobar fácilmente que $\mathbb{Z}_3$ o $\mathbb{Z}_5$ no tienen divisores de cero. En el ejercicio siguiente hay clasificados los valores de n para los cuales $\mathbb{Z}_n$ admite la ley de simplificación.

Ejercicio 11.4. Demostrar que $(\mathbb{Z}_n, +, \cdot)$ admite divisores de cero si y sólo si n no es primo.

Un anillo abeliano sin divisores de cero se llama *anillo íntegro* o *anillo de integridad*. Si, además, el anillo es unitario diremos que se trata de un *dominio de integridad*. Así diremos que $(\mathbb{Z}, +, \cdot)$ es un dominio de integridad, mientras que $(\mathbb{Z}_n, +, \cdot)$ en general sólo tiene estructura de anillo unitario abeliano.

El hecho de que, en $\mathbb{Z}_n$, la clase de n sea la clase del cero

$$[n] = [\underbrace{1+1+\cdots+1}_{n}] = [0]$$

sugiere la siguiente abstracción relativa a los anillos unitarios abelianos en general.

Se define la *característica* de un anillo unitario abeliano A como el mínimo número natural n tal que

$$n \cdot 1 = \underbrace{1+1+\cdots+1}_{n} = 0$$

en A. Si este número no existe, se dice que el anillo tiene característica cero. De hecho, podríamos interpretar la característica de un anillo unitario abeliano como el orden del subgrupo aditivo generado por el 1.

Está claro que la característica de $\mathbb{Z}_n$ es n. Un ejemplo también claro de anillo de característica cero lo encontamos en $\mathbb{Z}$.

Proposición 11.5. La característica de un dominio de integridad es cero o es un número primo.

Demostración. Sea A un dominio de integridad de característica $n_0 \neq 0$. Si existiesen $a, b \in \mathbb{N}$ tales que $n_0 = ab$, entonces querría decir que

$$(\underbrace{1+\cdots+1}_{a})(\underbrace{1+\cdots+1}_{b}) = \underbrace{1+\cdots+1}_{n_0} = 0$$

y A tendría divisores de cero, en contra de lo que hemos supuesto. □

Ejercicio 11.6. Demostrar que si la característica de A es p, entonces

1. $n \cdot 1 = \underbrace{1+1+\cdots+1}_{n} = 0$ implica que p divide a n;
2. para todo $a \in A$, $p \cdot a = \underbrace{a+a+\cdots+a}_{p} = 0$.

Finalmente, si los elementos no nulos de un anillo tienen estructura de grupo abeliano respecto del producto, diremos que este anillo es un *cuerpo* y lo notaremos habitualmente con la letra K. Dicho de una otra manera, $(K,+,\cdot)$ es un cuerpo si $(K,+)$ y $(K^*,\cdot)$ son grupos abelianos y el producto es distributivo respecto de la suma.

Es fácil observar que en un cuerpo K no pueden existir elementos a y b de K^* tales que $ab = 0$, ya que, multiplicando por la izquierda por a^{-1}, deduciríamos que b tiene que ser cero, en contra de lo que hemos supuesto. Por tanto, podemos afirmar lo siguiente:

Proposición 11.7. Todo cuerpo es un dominio de integridad.

El ejemplo más pequeño de cuerpo lo encontramos en $\mathbb{Z}_2$. De hecho, es fácil obtener toda una familia de cuerpos finitos no triviales, como muestra el resultado siguiente:

Proposición 11.8. $(\mathbb{Z}_p,+,\cdot)$ es un cuerpo si y sólo si p es primo.

Demostración. Si $(\mathbb{Z}_p,+,\cdot)$ es un cuerpo, tiene que ser un dominio de integridad. Por el ejercicio 11.4, p tiene que ser primo. En este caso, basta con ver que cada elemento tiene inverso. Para cada $b \in \mathbb{Z}_p$, el conjunto $b\mathbb{Z}_p = \{bx, x \in \mathbb{Z}_p\}$ tiene p elementos diferentes, ya que se satisface la ley de simplificación. Como $b0 = 0$, existe $x \in \mathbb{Z}_p \setminus \{0\}$ tal que $bx = 1$ y por tanto x es inverso de b. □

Ejercicio 11.9. Adaptar esta última demostración para ver que todo dominio de integridad finito es un cuerpo.

Otros ejemplos bien conocidos de cuerpos no finitos de característica cero los encontramos en $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ o $(\mathbb{C},+,\cdot)$. En la última sección de este capítulo construiremos nuevas familias de cuerpos finitos de característica p a partir del ya conocido $\mathbb{Z}_p$. Para poder hacer estas construcciones es necesaria la noción de subanillo.

Se dice que un subconjunto B de un anillo $(A,+,\cdot)$ es un *subanillo* de A si con las operaciones '$+$' y '$\cdot$' restringidas a los elementos de B se satisfacen los axiomas de anillo. Así pues, B tiene que ser un subgrupo del grupo aditivo de A y una parte estable de A por la multiplicación.

Proposición 11.10. Sea $(A,+,\cdot)$ un anillo y $B \subset A$. Entonces para que $(B,+,\cdot)$ sea subanillo de $(A,+,\cdot)$ es necesario y suficiente que $(B,+)$ sea subgrupo de $(A,+)$ y que el producto sea cerrado en B.

Ejercicio 11.11. Demostrar que $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ considerado como anillo.

Ejercicio 11.12. Determinar los subanillos de $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

Ejercicio 11.13. Caracterizar en general los subanillos de $\mathbb{Z}_n$.

Es fácil observar que, si A es un anillo abeliano o íntegro, también lo es el subanillo B; pero A puede ser unitario sin que lo sea B, como muestra el resultado siguiente.

Proposición 11.14. Los subanillos de $(\mathbb{Z},+,\cdot)$ son los conjuntos $n\mathbb{Z}$.

Demostración. Tal como se vio en el capítulo anterior, los únicos subgrupos de $(\mathbb{Z},+)$ son los conjuntos $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$, conjunto de múltiplos de un entero n. Estos conjuntos son claramente estables por la multiplicación y por tanto son los únicos subanillos de $\mathbb{Z}$. □

Observar que para $n \geqslant 2$, $n\mathbb{Z}$ no es unitario.

Ideales y anillo cociente

Siguiendo un proceso paralelo al descrito en el capítulo anterior para la obtención de la estructura de grupo cociente, definiremos aquí la noción de anillo cociente. Por ello introducimos en primer lugar la noción de relación de equivalencia compatible con la estructura de anillo.

Diremos que una relación de equivalencia R es compatible por la derecha con la estructura de anillo si y sólo si R es compatible con la suma y el producto de este anillo. Es decir, para todo $a, b \in A$ y para cualquier elemento $x \in A$ se cumple que

$$aRb \iff \begin{cases} (a+x)R(b+x) \\ axRbx \end{cases}$$

De forma similar, R es compatible por la izquierda si la segunda condición es $xaRxb$. Sabemos que una relación R que cumpla la primera de estas condiciones tiene la forma $aRb \Leftrightarrow a-b \in B$, donde B es un subgrupo aditivo de $(A,+)$. Para la segunda de estas condiciones necesitamos también que $x(a-b)$ o $(a-b)x$ sean elementos de B para cualquier $x \in A$. Esto obliga a restringir las relaciones de equivalencia compatibles con la estructura de anillo a ciertos subgrupos del grupo aditivo, llamados *ideales por la izquierda* o *por la derecha* según sea la relación.

Un subconjunto $I \subset A$ es un *ideal* por la *derecha* del anillo A si $(I,+)$ es un subgrupo de $(A,+)$ y para todo $a \in I$ y para todo $x \in A$ se cumple $ax \in I$. El ideal es por la *izquierda* si esta segunda condición es $xa \in A$. Por ejemplo, $\{0\}$ es un ideal de cualquier anillo, como también lo es el anillo entero A. Los ideales diferentes de $\{0\}$ y A se llaman *ideales propios*.

De forma similar al caso de grupos, si un ideal por la izquierda coincide con el correspondiente ideal por la derecha, se dice que el ideal es *bilateral*. Los ideales bilaterales juegan en

los anillos un papel similar al de los subgrupos normales en los grupos. Observemos que si A es un anillo abeliano, sus ideales son bilaterales.

Es preciso tener en cuenta que es posible que un ideal tenga estructura de anillo no unitario, aunque provenga de un anillo con unidad. Este es el caso de los ideales de $\mathbb{Z}$, $n\mathbb{Z}$.

Ejercicio 11.15. Demostrar que $n\mathbb{Z}$ son los únicos ideales de $\mathbb{Z}$.

Hemos visto que las únicas relaciones de equivalencia compatibles con la estructura de anillo son de la forma $aRb \Leftrightarrow a-b \in I$, donde I es un ideal del anillo. Así, como en el caso de los grupos, las clases de equivalencia inducidas a partir de una de estas relaciones serán de la forma $a+I$ con $a \in A$ y las notaremos como $[a]_I = \{a+I, a \in A\}$ (o simplemente $[a]$ si la referencia al ideal se sobreentiende). El conjunto formado por estas clases se llama *conjunto cociente módulo I* y se representa por $A/I = \{[a], a \in A\}$. Si I es un ideal bilateral, el conjunto A/I tiene estructura de anillo con las operaciones inducidas de A y se llama *anillo cociente módulo I*. También se conoce como *anillo factor* de A respecto I.

Ejercicio 11.16. Si I es un ideal bilateral de un anillo A, comprobar que las operaciones siguientes están bien definidas, para todo $[a],[b] \in A/I$:

$$\begin{cases} [a]+_I[b] &= [a+b] \\ [a]\cdot_I[b] &= [ab] \end{cases}$$

La comprobación del resultado siguiente es rutinaria y la dejamos como ejercicio para el lector.

Proposición 11.17. Si I es un ideal bilateral de un anillo A, entonces $(A/I, +_I, \cdot_I)$ es un anillo.

Observar que los anillos cocientes de $\mathbb{Z}$ son justamente los $\mathbb{Z}_n$.

En lo que sigue consideraremos anillos abelianos, de manera que los ideales serán bilaterales y nos referiremos a ellos simplemente como ideales.

Como en el caso de subgrupos, la intersección de ideales es también un ideal. En particular tiene un interés especial considerar la intersección de todos los ideales que contienen un determinado subconjunto $X \subset A$. Entonces se dice que este ideal está *generado* por X y se denota por $I = (X)$. En otras palabras, el ideal generado por X es el ideal más pequeño que contiene a X. Los ideales generados por un solo elemento tienen un interés especial y se llaman *ideales principales*.

Observemos que el ideal generado por un solo elemento $a \in A$ tiene que contener los elementos de la forma na para cualquier $n \in \mathbb{Z}$, ya que tiene que ser subgrupo del grupo aditivo de A. También tiene que contener los elementos de la forma xa para todo $x \in A$. Por tanto,

tiene que contener todo elemento de la forma $na+xa$, con $n \in \mathbb{Z}$ y $x \in A$. Estos elementos son suficientes para formar un ideal, ya que

$$\begin{aligned}(na+xa)-(n'a+x'a) &= (n-n')a+(x-x')a\\ y(na+xa) &= (yn)a+(yx)a\end{aligned}$$

Observar que $n-n' \in \mathbb{Z}$ y que $(x-x'),\ yn,\ yx \in A$.

Si el anillo A es unitario podemos identificar $n \in \mathbb{Z}$ con $n \cdot 1 \in A$, que es el elemento que consiste en sumar n veces el neutro del producto de A. De donde, $na = (n \cdot 1)a \in Aa$. De aquí obtenemos el resultado siguiente:

Proposición 11.18. En un anillo unitario abeliano A, los ideales generados por $a \in A$ son de la forma aA.

En general, el ideal generado por un conjunto de elementos de un anillo unitario abeliano, $\{a_1, a_2, \ldots, a_n\} \subset A$ está descrito por los elementos de la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \qquad x_i \in A, \forall i$$

Así, por ejemplo, el ideal de $\mathbb{Z}$ generado por el 2 y por el 3 es de la forma

$$\{2x+3y,\ x,y \in \mathbb{Z}\}$$

Hay anillos en que todos sus ideales son principales. En este caso se dice que el *anillo* es *principal*. Este es el caso de $\mathbb{Z}$ que tomamos como ejemplo sencillo, reiterado e ilustrativo de la mayor parte de las cuestiones consideradas en esta sección. Cabe observar que la noción de anillo principal va ligada a los anillos unitarios abelianos, sobre los cuales, como hemos mencionado anteriormente, trabajaremos a partir de ahora.

Ejercicio 11.19. Demostrar que $\mathbb{Z}$ es un anillo principal.

Ejercicio 11.20. Demostrar que en $2\mathbb{Z}$, el ideal I generado por 4 no es $\{4x, x \in 2\mathbb{Z}\}$. ¿Por qué?

Está claro que si I es un ideal de un anillo A, también es ideal de todos los subanillos B de A que lo contengan. Sin embargo, es preciso observar que en sentido contrario no es cierto. Por ejemplo, $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$, pero no es un ideal de $\mathbb{Q}$.

Morfismos de anillos

Diremos que una aplicación f de un anillo A sobre un anillo A' es un *morfismo entre anillos*, o bien un *homomorfismo de anillos*, si y sólo si f respeta la suma y el producto. Es decir, para todo $a, b \in A$,

$$\begin{aligned}f(a +_A b) &= f(a) +_{A'} f(b)\\ f(a \cdot_A b) &= f(a) \cdot_{A'} f(b)\end{aligned}$$

Es preciso observar que, de hecho, no es necesario suponer que A' sea un anillo; es suficiente considerar A' como un conjunto con suma y producto, como pone de manifesto el ejercicio siguiente.

Ejercicio 11.21. Comprobar que si A es un anillo y $f : A \longrightarrow A'$ es un morfismo, donde A' es un conjunto con suma y producto, entonces

1. $f(A)$ es una parte estable de A';
2. $(f(A), +_{A'}, \cdot_{A'})$ es un anillo.

Es fácil comprobar que ciertas propiedades algebraicas de A se transmiten a través de f tal como se indica en los ejercicios siguientes.

Ejercicio 11.22. Demostrar que, si f es un morfismo entre los anillos A y $f(A)$, entonces

1. $f(0) = 0$ y $f(-a) = -f(a)$;
2. $f^{-1}(0)$ es un ideal de A, llamado *núcleo de* f.

Ejercicio 11.23. Demostrar que si A es un anillo unitario abeliano, entonces

1. $f(A)$ es también abeliano;
2. $f(1) = 1$;
3. $f(a^{-1}) = (f(a))^{-1}$, siempre que $a^{-1} \in A$.

Recordemos que los subgrupos normales están íntimamente relacionados con los morfismos entre grupos. En el caso de anillos, serán los ideales los que jugarán un papel similar.

Así, la aplicación $f : A \longrightarrow A/I$, donde I es un ideal de A tal que $f(x) = x + I$ para todo $x \in A$, es un homomorfismo exhaustivo o *epimorfismo*, llamado *homomorfismo canónico*.

Ejercicio 11.24. Demostrar que si $f : A \longrightarrow A/I$ es homomorfismo canónico, entonces el núcleo de f es el ideal I.

Un morfismo entre anillos es inyectivo si y sólo si $f^{-1}(0) = \{0\}$. En este caso se dice que f es un *monomorfismo*.

Además, como en el caso de grupos, si el morfismo es biyectivo se dice que los anillos son *isomorfos*.

Los homomorfismos conservan también los ideales en un cierto sentido, como se puede comprobar mediante el siguiente resultado que usaremos más adelante.

Proposición 11.25. Si $f : A \longrightarrow A'$ es un homomorfismo de anillos e I' es un ideal de A', entonces $I = f^{-1}(I')$ es un ideal de A que contiene al núcleo de f.

Demostración. Si $a, b \in I$, entonces $f(a-b) = f(a) - f(b) \in I'$ de manera que $a - b \in I$. Similarmente, para todo $x \in A$, $f(ax) = f(a)f(x) \in I'$ de manera que $ax \in I$, e I es un ideal de A que contiene a $f^{-1}(0)$. □

Ideales maximales y cuerpos

El hecho que $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ sea un anillo unitario abeliano, y que para determinados valores de n tenga estructura de cuerpo, no es un hecho particular de $\mathbb{Z}$, sino que lo comparte con cualquier anillo con las mismas características. Encontrar condiciones por las cuales un anillo cociente es un cuerpo es el objetivo que nos proponemos en esta parte.

Un ideal I en A se dice *maximal* si $I \neq A$ y no existe ningún otro ideal entre I y A.

Ejercicio 11.26. Demostrar que el ideal $(p) = p\mathbb{Z}$ es maximal en $\mathbb{Z}$ si y sólo si p es primo.

Una manera útil de obtener cuerpos a partir de un anillo unitario abeliano consiste en localizar sus ideales maximales y construir el correspondiente anillo cociente. Éste es justamente el argumento utilizado en la última sección de este capítulo para la construcción de cuerpos finitos. Por ello vemos primero cuáles son los ideales de un cuerpo.

Proposición 11.27. Un anillo unitario abeliano K es un cuerpo si y sólo si sus únicos ideales son $\{0\}$ y K.

Demostración. Supongamos primero que K es un cuerpo e $I \neq \{0\}$ es un ideal de K. Entonces, si $a \in I$, $a^{-1}a = 1 \in I$ y por tanto $I = K$.

Recíprocamente, sea $I = (a)$ el ideal generado por $a \in K^* = K \setminus \{0\}$. Si $I = aK = K$, entonces existe $x \in K^*$ tal que $ax = 1$, de manera que x es el inverso de a. □

Esta última propiedad permite ver el resultado siguiente:

Proposición 11.28. Si M es un ideal maximal de un anillo unitario abeliano A, entonces A/M es un cuerpo.

Demostración. Consideremos el epimorfismo canónico $f : A \longrightarrow A/M$. Ya hemos visto en el ejercicio 11.23 que A/M es abeliano y unitario. Según la proposición 11.25, si $[J]$ es un ideal de A/I, entonces $I = f^{-1}([I])$ es un ideal de A que contiene a M. Por tanto, o bien $I = A$ y $[I] = A/M$, o bien $I = M$ y $[I] = [0]$. Así, A/M no tiene ideales propios y por tanto es un cuerpo. □

11.2 El anillo de los polinomios

En esta sección se estudia un ejemplo importante de anillo, el anillo de los polinomios, que se utilizará en la sección siguiente para la construcción de cuerpos de orden finito.

Normalmente se interpretan los polinomios como expresiones formales del tipo "$a_0+a_1x+\cdots+a_nx^n$" con "indeterminada" x. El origen de esta expresión se pondrá de manifesto al final de esta sección. De momento nos preguntamos, ¿qué representa esta x y cómo se hace para sumarla o multiplicarla? Podemos resolver esta cuestión introduciendo los polinomios de una manera aparentemente más formal, pero más precisa y más útil. La respuesta parte de una observación sencilla: un polinomio "$a_0+a_1x+\cdots+a_nx^n$" queda determinado por la secuencia $(a_0,a_1,\dots,a_n)$.

Definimos el conjunto de los *polinomios* sobre un anillo unitario abeliano A como el conjunto de todas las sucesiones de elementos de A que tienen un número finito de elementos no nulos

$$a=(a_0,a_1,\dots,a_n,0,0,\dots)$$

Diremos que $a_0,a_1,\dots,a_n$ son los *coeficientes* del polinomio a. Si n es el entero más grande para el cual $a_n\neq 0$, diremos que el polinomio a tiene *grado* n y lo notaremos escribiendo $gr(a)=n$. Si $a_n=1$ diremos que el polinomio a es *mónico*. A los polinomios de grado cero se los llama *constantes*. Es preciso observar que el polinomio nulo, el que tiene todos sus coeficientes cero, que denotaremos directamente como 0, no tiene grado según esta regla, pero se interpreta también como un polinomio constante y se dice, formalmente, que tiene grado $-\infty$.

Definiremos dos operaciones, la suma y el producto, que permitirán estructurar este conjunto como el propio anillo A sobre el cual se ha contruido.

Dados dos polinomios $a=(a_0,a_1,\dots)$ y $b=(b_0,b_1,\dots)$ con coeficientes en un anillo unitario abeliano A, definimos el *polinomio suma* y el *polinomio producto*

$$\begin{aligned} a+b &= (a_0+b_0,a_1+b_1,\dots)\\ ab &= (c_0,c_1,\dots), \qquad c_k=\sum_{i+j=k}a_ib_j=\sum_{i=0}^{k}a_ib_{k-i}\end{aligned}$$

Observar que, en general,

$$\begin{aligned} gr(a+b) &\leqslant \max\{gr(a),gr(b)\}\\ gr(ab) &\leqslant gr(a)+gr(b)\end{aligned}$$

Ejercicio 11.29. Si $a=(3,3,6,0,\dots)$ y $b=(3,-3,3,-1,0,\dots)$ son polinomios en $\mathbb{Z}_7[x]$, calcular los polinomios $a+b$ y ab. Repetir el cálculo si los polinomios a y b se consideran en $\mathbb{Z}_9[x]$.

La suma y el producto de polinomios involucra sólo sumas y productos de elementos del anillo de base A. Teniendo en cuenta esta observación, es fácil deducir que los polinomios respecto de la suma se comportan como grupo abeliano con el polinomio 0 como elemento neutro y que respecto del producto se comportan como un semigrupo abeliano con elemento neutro el polinomio constante $1 = (1, 0, \dots)$. La distributividad del producto respecto de la suma es también consecuencia directa de las observaciones anteriores. Así, el conjunto de polinomios con coeficientes en un anillo unitario abeliano tiene también estructura de anillo unitario abeliano.

La justificación de la notación clásica a que aludíamos al comienzo de esta sección descansa en el hecho de identificar el polinomio $(0, 1, 0, \dots)$ con x. De esta manera tenemos que, $x \cdot x = x^2 = (0, 0, 1, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, \dots)$ y así sucesivamente y, por convenio, $x^0 = (1, 0, \dots) = 1$. Por tanto, podemos escribir

$$a = (a_0, a_1, \dots, a_n, 0, \dots) = a_0 + a_1 x + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i$$

Cabe observar que ahora x no es una "indeterminada", sino un polinomio especial. Es habitual, como consecuencia de esta expresión, denotar el conjunto de los polinomios con coeficientes en A por $A[x]$ y los polinomios de $A[x]$ por $a(x)$, para diferenciarlos, si es necesario, de los propios elementos del anillo, $a \in A$. Observemos también que A se puede interpretar como el conjunto de los polinomios constantes, es decir, cada elemento $a \in A$ se asocia con el polinomio $a(x) = a + 0x + 0x^2 + \cdots \in A[x]$. Identificaremos por tanto los polinomios constantes con los elementos del anillo.

Los resultados siguientes nos garantizan en qué condiciones está permitida la ley de simplificación para los polinomios.

Lema 11.30. Si A es un dominio de integridad y $a(x), b(x) \in A[x]$, entonces $gr(a(x)b(x)) = gr(a(x)) + gr(b(x))$.

Demostración. Si $a(x)$ y $b(x)$ tienen grados $n, m \geqslant 0$ respectivamente, entonces el coeficiente de grado $m+n$ de $c(x) = a(x)b(x)$ es $c_{m+n} = a_n b_m \neq 0$, ya que a_n y b_m son no nulos y A no tiene divisores de cero. Si alguno de los grados es $-\infty$, entonces $a(x)b(x) = 0$ y también vale la igualdad. □

Cabe observar que en esta demostración ha sido útil la asignación de $-\infty$ como grado del polinomio nulo en lugar de asignarle grado cero, como haríamos con los otros polinomios constantes.

Proposición 11.31. Si A es un dominio de integridad, $A[x]$ también lo es.

Demostración. Sabemos que $A[x]$ es un anillo unitario abeliano. Tenemos que ver entonces que, si A es íntegro, también lo es $A[x]$. Si consideramos $a(x), b(x) \in A[x]$ tales que $a(x)b(x) = 0$, como $gr(ab) = gr(a) + gr(b)$, deducimos que $a(x) = 0$ o $b(x) = 0$. □

El resultado siguiente demuestra la imposibilidad de ampliar la estructura algebraica de los polinomios para obtener la estructura de cuerpo, demostrando la imposibidad de obtener inversos para todos los elementos de $A[x]$, independientemente de las propiedades de A.

Proposición 11.32. Si A es un anillo íntegro unitario, los únicos elementos invertibles de $A[x]$ son los elementos invertibles de A.

Demostración. $a(x), b(x) \in A[x]^* = A[x] \setminus \{0\}$ son inversos si y sólo si $a(x)b(x) = 1$. Como $gr(ab) = gr(a) + gr(b) = 0$, deducimos que $gr(a) = gr(b) = 0$ y por tanto $a(x) = a \in A$ y $b(x) = a^{-1}$. □

Divisibilidad en K[x]

Una vez definido y estructurado el conjunto de polinomios $A[x]$ con coeficientes sobre un anillo unitario abeliano A, nos interesa factorizar estos polinomios de forma similar a como factorizamos los números enteros, es decir, descomponiéndolos como productos de elementos tan "simples" como sea posible. En el caso de los enteros, sabemos que estos elementos son los números primos. Como veremos a continuación, en el caso de los polinomios, estos elementos "simples" se llaman también polinomios *primos*. Para ello necesitamos introducir las definiciones, las notaciones y las propiedades correspondientes al concepto de divisibilidad en el ámbito de $A[x]$, y observaremos que son similares a las propias en el caso de $\mathbb{Z}$.

Dados dos polinomios $a(x)$ y $b(x)$ de $A[x]$, diremos que $b(x)$ es un *divisor* de $a(x)$, o que $b(x)$ *divide* a $a(x)$, y lo denotaremos escribiendo

$$b(x)|a(x)$$

si y sólo si existe un polinomio $c(x) \in A[x]$ tal que $a(x) = b(x)c(x)$.

Observemos que los polinomios constantes correspondientes a los elementos invertibles de A, $U = \{u \in A,\ \exists u' \in A,\ uu' = 1\}$ son divisores de cualquier polinomio $a(x) \in A[X]$, ya que $a(x) = uu'a(x)$, donde u' es el inverso de u. Por el mismo motivo, $ua(x)$ es divisor de $a(x)$ para todo $u \in U$. Éstos se llaman *divisores triviales*. Es preciso observar que, sea cual sea A, exceptuando $\mathbb{Z}_2$, como mínimo se tienen asegurados ± 1 y $\pm a(x)$ como divisores triviales de $a(x)$. En $\mathbb{Z}[x]$ éstos son los únicos, mientras que si A es un cuerpo, cualquiera de sus elementos, salvo el cero, es un divisor trivial de $a(x)$. Por otra parte, si $gr(a) > gr(b) > 0$, diremos que $b(x)$ es un *divisor propio* de $a(x)$.

Todo polinomio que no tiene divisores propios, es decir, que no tiene otros divisores que los triviales, se dice que es *primo* o *irreductible*. Está claro que todo polinomio de grado 1 es irreductible. En el cuerpo de los números complejos $\mathbb{C}$, el *teorema fundamental del álgebra* nos garantiza que éstos son los únicos polinomios irreductibles de $\mathbb{C}[x]$. Desgraciadamente, no hay resultados teóricos tan sencillos para conocer los polinomios irreductibles en otros anillos de polinomios. Por ello, nos tendremos que conformar con resultados parciales que nos ayudarán a estudiar la situación en cada caso.

En nuestro contexto, nos interesan particularmente los polinomios definidos sobre un cuerpo y en especial sobre cuerpos finitos. En lo que sigue centraremos nuestra atención en el caso particular de estos polinomios.

A continuación enunciaremos un resultado teórico, el *teorema de factorización*, esencial para todo lo que sigue, cuya demostración evitaremos, ya que no tiene ningún interés práctico y es excesivamente laboriosa[1].

Teorema 11.33 (Teorema de factorización). Dado un cuerpo K, cada polinomio $k(x) \in K[x]$ admite una representación única de la forma

$$k(x) = kp_1(x)p_2(x)\cdots p_m(x)$$

con $k \in K$, $p_1(x), p_2(x), \ldots, p_m(x) \in K[x]$ polinomios mónicos irreductibles.

Esta descomposición en factores primos tiene en la práctica una dificultad fundamental: la inexistencia de métodos sencillos para encontrar en general estos polinomios irreductibles. Los conceptos y los resultados siguientes están dedicados al estudio de este problema.

Sea K un cuerpo. Para cualquier par de polinomios $a(x)$ y $b(x)$ de $K[x]$ se define su *máximo común divisor* como el polinomio de grado más grande que los divide a ambos. Es decir, $D(x) \in K[x]^* = K[x] \setminus \{0\}$ es un máximo común divisor de los polinomios $a(x)$ y $b(x)$, y escribimos $D(x) = \mathrm{mcd}(a(x), b(x))$ si se verifican las condiciones siguientes:

1. $D(x)|a(x)$ y $D(x)|b(x)$;
2. si $D'(x)|a(x)$ y $D'(x)|b(x)$, entonces $D'(x)|D(x)$.

Es preciso observar que, tal como está definido el máximo común divisor de dos polinomios, éste no es único, ya que si $D(x)$ es un máximo común divisor, entonces $kD(x)$ también lo es, para todo $k \in K$. Tiene sentido, por tanto, escoger el polinomio más sencillo que represente toda esta familia. Éste es el polinomio mónico correspondiente, que denotaremos como

$$d(x) = \mathrm{mcd}(a(x), b(x))$$

[1] El lector que esté interesado puede encontrar esta demostración en [3], por ejemplo.

Los factores en común que tienen dos polinomios en sus factorizaciones son los factores de su máximo común divisor. Diremos que dos polinomios $a(x), b(x) \in K^*[x]$ son *primos entre sí* o *coprimos* si $\mathrm{mcd}(a(x), b(x)) = 1$.

De forma similar, se define el *mínimo común múltiplo* entre $a(x)$ y $b(x)$, $M(x) = \mathrm{mcm}(a(x), b(x))$, si se verifican las condiciones siguientes:

1. $a(x)|M(x)$ y $b(x)|M(x)$;
2. si $a(x)|M'(x)$ y $b(x)|M'(x)$, entonces $M(x)|M'(x)$.

Como antes, se define $m(x) = \mathrm{mcm}(a(x), b(x))$ como el polinomio mónico de entre los que satisfacen las dos propiedades anteriores.

El teorema de factorización proporciona una manera teórica de encontrar el máximo común divisor de dos polinomios: sólo es preciso seleccionar los factores comunes de sus factorizaciones. En la práctica, sin embargo, resulta en general difícil encontrar estas factorizaciones. Es importante, por tanto, disponer de algoritmos eficientes que permitan la obtención directa de estos máximo común divisores. El teorema de Euclides, que enunciaremos a continuación, y una consecuencia inmediata de éste, conducirán a un algoritmo de estas características: el algoritmo de Euclides.

Teorema 11.34 (Euclides). Dados $a(x), b(x) \in K^*[x]$, existen dos únicos polinomios $q(x), r(x) \in K[x]$ tales que

$$a(x) = b(x)q(x) + r(x), \qquad gr(r) < gr(b)$$

La expresión anterior es la llamada *división euclídea*, de $a(x)$ por $b(x)$. En general, los anillos para los cuales es válida la división euclídea se llaman anillos *euclídeos*. La demostración del teorema anterior prueba la existencia de los polinomios $q(x), r(x) \in K[x]$, llamados respectivamente *cociente* y *resto*. Así, $K[x]$ es euclídeo. El resultado siguiente es una consecuencia importante del teorema anterior.

Corolario 11.35. $\mathrm{mcd}(a(x), b(x)) = \mathrm{mcd}(b(x), r(x))$.

Demostración. Si $d(x) = \mathrm{mcd}(a(x), b(x))$, significa que $a(x) = d(x)a_1(x)$ y $b(x) = d(x)b_1(x)$ para ciertos polinomios $a_1(x), b_1(x)$. De la igualdad del teorema de Euclides, $a(x) = b(x)q(x) + r(x)$, deducimos que $r(x) = d(x)(a_1(x) - b_1(x)q(x))$, de donde $d(x)|r(x)$. Por otra parte, de la misma igualdad se deduce que cualquier divisor común $d'(x)$ de $b(x)$ y $r(x)$ divide también a $a(x)$. □

Algoritmo de Euclides

En las condiciones del teorema de Euclides podemos usar el corolario anterior tantas veces como sea posible, es decir, hasta que obtengamos como resto el polinomio nulo. Esto es,

$$\begin{array}{lcll} a(x) & = & b(x)q_1(x)+r_1(x), & gr(r_1)<gr(b) \\ b(x) & = & r_1(x)q_2(x)+r_2(x), & gr(r_2)<gr(r_1) \\ r_1(x) & = & r_2(x)q_3(x)+r_3(x), & gr(r_3)<gr(r_2) \\ & \vdots & & \\ r_{n-2}(x) & = & r_{n-1}(x)q_n(x)+r_n(x), & gr(r_n)<gr(r_{n-1}) \\ r_{n-1}(x) & = & r_n(x)q_{n+1}(x)+0 & \end{array}$$

Aplicando reiteradamente el corolario anterior a las sucesivas expresiones, obtenemos

$$\mathrm{mcd}(a(x),b(x)) = \mathrm{mcd}(b(x),r_1(x)) = \cdots = \mathrm{mcd}(r_n(x),0) = r_n(x)$$

Es decir, el máximo común divisor es justamente el último resto diferente de cero.

Como ejemplo, podemos comprobar que $a(x) = x^4+3x^2-4x+1$ y $b(x) = x^2-3x$ son polinomios primos entre sí en $\mathbb{Z}_5$:

$$\begin{array}{rcl} x^4+3x^2+x+1 & = & (x^2+2x)(x^2+3x+2)+(2x+1) \\ x^2+2x & = & (2x+1)(3x+2)+3 \\ 2x+1 & = & 3(4x+2)+0 \end{array}$$

La simplicidad y la utilidad de este algoritmo son bien evidentes y hacen innecesario cualquier elogio. Una consecuencia directa también muy importante de este resultado es la llamada *identidad de Bézout*, que esencialmente consiste en "recorrer" el algoritmo de Euclides en sentido contrario, mediante substituciones sucesivas de los restos. Más concretamente, en el algoritmo anterior podemos escribir

$$r_n(x) = r_{n-2}(x) - r_{n-1}(x)q_n(x)$$

De la misma manera, cada resto $r_i(x)$ se puede expresar en términos de restos anteriores hasta obtener una expresión de $r_n(x)$ en términos de los polinomios iniciales $a(x)$ y $b(x)$.

Es preciso observar que el polinomio $r_n(x)$ que se obtiene en el algoritmo no es necesariamente mónico, de manera que tomaremos el correspondiente polinomio monico $d(x) = ur_n(x)$, donde u es el inverso del coeficiente de grado más grande de $r(x)$, como máximo común divisor. Con estas observaciones tenemos:

Teorema 11.36 (Identidad de Bézout). Dados $a(x),b(x) \in K[x]^*$ con $\mathrm{mcd}(a(x),b(x)) = d(x)$, existen dos polinomios $s(x),t(x) \in K[x]$ tales que

$$a(x)s(x)+b(x)t(x) = d(x)$$

Si tomamos como ejemplo los polinomios anteriores en $\mathbb{Z}_5[x]$, $a(x) = x^4 + 3x^2 - 4x + 1$ y $b(x) = x^2 - 3x$, obtenemos la identidad de Bézout a partir del máximo común divisor, que hemos calculado previamente a partir del algoritmo de Euclides, de la forma siguiente:

$$\begin{aligned} 3 &= (x^2+2x) - (2x+1)(3x+2) \\ &= (x^2+2x) - [(x^4+3x^2+x+1) - (x^2+2x)(x^2+3x+2)](3x+2) \\ &= (x^2+2x)[1+(x^2+3x+2)(3x+2)] - (x^4+3x^2+x+1)(3x+2) \\ &= (x^2+2x)(3x^3+x^2+2x) - (x^4+3x^2+x+1)(3x+2) \end{aligned}$$

Por tanto, multiplicando por 2 los dos lados de la igualdad, obtenemos:

$$1 = (x^2+2x)\underbrace{(x^3+2x^2+4x)}_{t(x)} + (x^4+3x^2+x+1)\underbrace{(4x+1)}_{s(x)}$$

Ejercicio 11.37. Usar el algoritmo de Euclides para encontrar el máximo común divisor $d(x)$ de los polinomios

$$\begin{aligned} a(x) &= 1+2x^2 \\ b(x) &= 1+2x+x^2 \end{aligned}$$

en $\mathbb{Z}_3[x]$. Obtener después los polinomios $s(x)$ y $t(x)$ que permiten escribir la identidad de Bézout $a(x)s(x) + b(x)t(x) = d(x)$.

Los ideales de K[x]

La noción de divisibilidad introducida aquí para los polinomios es válida también para otros anillos unitarios abelianos, en particular para $\mathbb{Z}$. La simplicidad de toda la teoría de la divisibilidad en $\mathbb{Z}$ proviene del hecho que $\mathbb{Z}$ es un anillo principal. Veremos en esta sección que $K[x]$ es también un anillo principal, siendo K un cuerpo.

En primer lugar es preciso encontrar una traducción del concepto de divisor en términos de ideales.

Proposición 11.38. En un anillo euclídeo,

$$b|a \Longleftrightarrow (a) \subset (b)$$

donde (a) y (b) son los ideales generados por a y b respectivamente.

Ejercicio 11.39. Demostrar la proposición anterior.

Es preciso observar que hemos traducido las nociones clásicas de divisibilidad en términos de inclusión de subconjuntos. Esta nueva manera de interpretar la divisibilidad tiene ventajas conceptuales que aprovecharemos en la sección siguiente.

La medida de proximidad, en cuanto a la divisibilidad, entre dos elementos de un anillo íntegro unitario A la da su máximo común divisor. En términos de ideales, la expresión de este máximo común divisor es muy simple.

Proposición 11.40. En un anillo euclídeo,

$$d = \mathrm{mcd}(a,b) \Longleftrightarrow (d) = (a,b)$$

Demostración. Observemos que el ideal generado por a y b está formado por los elementos de la forma $ax+by$, $x,y \in A$, y, por tanto, $(d) = (a,b) = (a) + (b)$. □

Observemos que de la demostración anterior se deduce de forma inmediata la identidad de Bézout.

Ejercicio 11.41. Sean a y b dos elementos primos entre sí en un anillo íntegro unitario. Encontrar la expresión correspondiente en términos de ideales.

La proposición anterior permite interpretar el anillo de polinomios sobre un cuerpo como un anillo principal.

Proposición 11.42. Si K es un cuerpo, $K[x]$ es un anillo principal.

Demostración. Tenemos que demostrar que los ideales de $K[x]$ son principales. Sea $I \neq \{0\}$ un ideal de $K[x]$ y $b(x)$ un polinomio de grado mínimo entre los polinomios de $I \setminus \{0\}$. Para cualquier $a(x) \in I$, la división euclídea permite escribir $a(x) = b(x)q(x) + r(x)$, para ciertos polinomios $b(x), r(x)$ y $gr(r(x)) < gr(b(x))$. Pero $r(x) = a(x) - b(x)q(x) \in I$, de manera que, siendo $b(x)$ el polinomio de grado mínimo de $I \setminus \{0\}$ tiene que ser $r(x) = 0$ y $a(x) \in (b(x))$. □

Podemos afirmar por tanto que los ideales I de $K[x]$ son de la forma $I = (a(x))$ con $a(x) \in K[x]$ mónico.

Para la construcción de los cuerpos finitos en la última sección, se usará el resultado siguiente, que ya hemos demostrado en general para cualquier anillo unitario abeliano.

Teorema 11.43. Si K es un cuerpo y $M(x)$ es un ideal maximal de $K[x]$, entonces $K[x]/M(x)$ es un cuerpo.

Es importante, por tanto, conocer cuáles son los ideales maximales de $K[x]$. Recordemos que, siguiendo también en este aspecto la similitud con el anillo de los enteros, los ideales maximales de $K[x]$ son justamente los generados por sus polinomios primos o irreductibles.

Proposición 11.44. Un ideal $(a(x))$ es maximal de $K(x)$ si y sólo si $a(x)$ es un polinomio primo.

Demostración. Ya hemos visto que todos los ideales de $K(x)$ son principales. Si $a(x)$ no es primo, se puede poner $a(x) = p(x)q(x)$, donde $p(x)$ y $q(x)$ son polinomios de grado mayor o igual que 1. Entonces, el ideal $(a(x))$ está estrictamente incluido en $(p(x))$, y no es maximal. Recíprocamente, si $a(x)$ no es maximal, $((a(x))$ está estrictamente incluido en $(p(x))$ para algún $p(x)$, de manera que $a(x) = p(x)q(x)$ y $a(x)$ no es primo. □

Raíces de un polinomio

Es frecuente pensar en funciones cuando se habla de polinomios. Esta es la razón que lleva a la notación clásica de los polinomios, a la que aludíamos al comienzo de esta sección. Pero, de hecho, no toda función polinómica está representada por un único polinomio, aunque sí sea cierto en sentido contrario. A continuación definiremos las funciones polinómicas y estudiaremos la relación entre sus ceros y la factorización de los polinomios correspondientes.

Sea K un cuerpo y $a(x) \in K[x]$, $a(x) = \sum_{i=0}^{n} a_i x^i$. Se define la *función polinómica* asociada al polinomio $a(x)$ como la aplicación

$$\begin{array}{rcl} \overline{a} : K & \longrightarrow & K \\ k & \longrightarrow & \overline{a}(k) = \displaystyle\sum_{i=0}^{n} a_i k^i \end{array}$$

Tomamos como ejemplo los polinomios $a(x) = x - 2$ y $b(x) = x^3 - 2$ en $\mathbb{Z}_3$. Las funciones polinómicas asociadas a estos dos polinomios son la misma, como se puede comprobar en la tabla siguiente:

$$\begin{array}{l} \overline{a}(0) = \overline{b}(0) = 1 \\ \overline{a}(1) = \overline{b}(1) = 2 \\ \overline{a}(2) = \overline{b}(2) = 0 \end{array}$$

En cambio, los dos polinomios no tienen los mismos coeficientes (no son el mismo). Comportamientos como el de este ejemplo son frecuentes en funciones polinómicas definidas sobre $\mathbb{Z}_p$, donde p es un número primo. De hecho, serán éstos los polinomios con los cuales trabajaremos. Se debe decir, sin embargo, que si el cuerpo es de característica cero, como por ejemplo $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, cada función polinómica tiene asociado un único polinomio y por tanto en estos casos no hay inconveniente en identificar los dos conceptos.

Se dice que $\alpha \in K$ es una *raíz* (o *cero*) del polinomio $a(x) \in K[x]$ si $\overline{a}(\alpha) = 0$, es decir, si es un cero de la función polinómica correspondiente.

El resultado siguiente da, mediante una condición muy sencilla, la herramienta clave que permite relacionar los ceros de una función polinómica con los factores de un polinomio.

Teorema 11.45. $\alpha \in K$ es una raíz de $a(x) \in K[x]$ si y sólo si $(x - \alpha) | a(x)$.

Demostración. Observemos en primer lugar que $gr(a) \geqslant 1$, ya que si $gr(a) = 0$ querría decir que $a(x)$ es un polinomio constante y por tanto no tiene raíces. Al hacer la división euclídea de $a(x)$ por $x-\alpha$ tenemos $a(x) = (x-\alpha)q(x)+r(x)$ con $gr(r) < 1$; como α es raíz de $a(x)$, $r(x) = 0$ y de aquí $(x-\alpha)|a(x)$. En sentido contrario sólo es preciso observar que si $(x-\alpha)|a(x)$, entonces existe un $q(x) \in K[x]$ tal que $a(x) = (x-\alpha)q(x)$ y, por tanto, α es raíz de $a(x)$. □

Se dice que $\alpha \in K$ es una raíz de *multiplicidad* $m \geqslant 1$ del polinomio $a(x) \in K[x]$ si y sólo si $(x-\alpha)^m$ divide a $a(x)$, pero no lo hace $(x-\alpha)^{m+1}$.

El teorema siguiente establece la relación entre el número de raíces de un polinomio y su grado. El resultado aparentemente inocente es esencial para tratar el problema central que nos ocupa, la factorización polinómica.

Teorema 11.46. Si el grado de $a(x) \in K[x]$ es n, entonces la suma de las multiplicidades de las raíces es como máximo n.

Demostración. Si $a(x)$ tiene raíces $\alpha_1, \ldots, \alpha_k$ con multiplicidades $m_1, \ldots, m_k$, entonces el polinomio $b(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k}$ divide a $a(x)$ y, por tanto, $gr(b(x)) = m_1 + \cdots + m_k \leqslant gr(a(x))$. □

A veces se utiliza una versión diferente de este teorema que dice que el número de raíces diferentes de un polinomio es como máximo igual a su grado.

11.3 Cuerpos finitos

Sabemos que $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo de p elementos si p es un número primo. ¿Existen cuerpos finitos de cualquier orden? Responder a esta cuestión es el primer objetivo que nos proponemos en esta sección. Estudiaremos, para comenzar, la estructura interna que deben tener estos cuerpos mediante el estudio de su grupo aditivo y multiplicativo. Describiremos de manera breve las razones de su existencia, que dependerá, como veremos, de la existencia de ciertos polinomios. Finalmente describiremos la manera general de obtenerlos mediante ejemplos ilustrativos y comentaremos, para acabar, también brevemente, que los cuerpos que hemos aprendido a construir son de hecho los únicos posibles.

Para comenzar recordemos que, si K es un cuerpo finito, su característica tiene que ser un número primo.

Teorema 11.47. Si K es un cuerpo de característica p, $|K| = p^n$, $n \in \mathbb{N}$.

Demostración. Demostraremos que el grupo aditivo de K es isomorfo al producto directo de n grupos cíclicos de orden p.

En primer lugar, observemos que el subgrupo cíclico de $(K,+)$ generado por un elemento $k \in K$ tiene orden p, como consecuencia directa de su característica. Es decir,

$$\langle k \rangle = \{k, k+k, \ldots, \underbrace{k+\cdots+k}_{p}\} = \{mk, m \in \mathbb{Z}_p\} \simeq \mathbb{Z}_p$$

Supongamos ahora que $\{g_1, g_2, \ldots, g_n\}$ sea un conjunto de generadores mínimo de K, es decir, que ningún subconjunto de éste genere todo K. Esto quiere decir que para cualquier elemento $k \in K$ existen n enteros $\{m_1, m_2, \ldots, m_n\}$, tales que

$$k = \sum_{i=1}^{n} m_i g_i$$

Demostraremos que las p^n posibles combinaciones de expresiones de esta forma son diferentes y dan lugar por tanto a p^n elementos diferentes de K. Supongamos que dos sumatorios diferentes diesen lugar al mismo elemento de K, es decir,

$$k = \sum_{i=1}^{n} m_i g_i = \sum_{i=1}^{n} m'_i g_i$$

Si j fuese la primera posición del sumatorio tal que $m_j \neq m'_j$, tendríamos que

$$(m_j - m'_j) g_j = \sum_{i=j+1}^{n} (m_i - m'_i) g_i$$

Ahora bien, como $(m_j - m'_j) = (m_j - m'_j) \cdot 1 \neq 0$ tiene inverso en K, obtendríamos

$$g_j = (m_j - m'_j)^{-1} \sum_{i=j+1}^{n} (m_i - m'_i) g_i$$

Esto contradice la hipótesis de que $\{g_1, g_2, \ldots, g_n\}$ es un conjunto de generadores mínimo.

Podemos asociar por tanto, de manera única, cada elemento $k = \sum_{i=1}^{n} m_i g_i$ de K con la n-tupla $\{m_1, m_2, \ldots, m_n\}$ de elementos de $\mathbb{Z}_p$. Esta asociación es por tanto una biyección de K en $\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n} = (\mathbb{Z}_p)^n$, que es de hecho un isomorfismo entre $(K,+)$ y $((\mathbb{Z}_p)^n,+)$. Por tanto,

$$(K,+) \simeq ((\mathbb{Z}_p)^n,+)$$

□

Acabamos de demostrar que el orden de cualquier cuerpo finito tiene que ser una potencia de un número primo, p^n. Esto lo hemos hecho estudiando la estructura de su grupo aditivo y

hemos visto que éste debe ser isomorfo a $((\mathbb{Z}_p)^n, +)$. Es, por tanto, razonable interpretar los elementos del cuerpo K como polinomios con coeficientes en $\mathbb{Z}_p$ de grado inferior a n. Sin embargo, si bien está claro que este conjunto es adecuado como modelo para el grupo aditivo del cuerpo, está claro también que no lo es para su grupo multiplicativo. Sólo es preciso observar que el producto no es cerrado en este conjunto, ya que el producto de dos polinomios sobre un cuerpo íntegro tiene por grado la suma de los grados de los polinomios correspondientes. Convendrá rectificar entonces el modelo, de manera que sea también compatible con el grupo multiplicativo. Antes de presentar un modelo apropiado con la estructura de cuerpo, estudiemos cómo tendría que ser su grupo multiplicativo.

Hemos visto que dos cuerpos finitos del mismo orden tienen sus grupos aditivos isomorfos. Veremos ahora que también son isomorfos sus grupos multiplicativos.

Teorema 11.48. El grupo multiplicativo de un cuerpo finito es cíclico.

Demostración. Supongamos que K es un cuerpo de orden p^n, con p primo y n un número natural. Como el orden de cualquier elemento diferente de cero de un grupo finito multiplicativo divide al orden del grupo, tenemos que, si $k \in K^*$, entonces $k^{p^n-1} = 1$. Esto es equivalente a decir que la ecuación

$$x^{p^n-1} - 1 = 0$$

tiene $p^n - 1$ ceros en K.

Por otra parte, está claro que el grupo multiplicativo de un cuerpo es abeliano y por tanto podemos utilizar el resultado siguiente, que es consecuencia (no directa) del teorema de Lagrange para grupos abelianos: "el exponente de un grupo es múltiplo de todos los órdenes de los elementos del grupo". De aquí que, si m es el exponente de $(K^*, \cdot)$, cada elemento de K^* satisface la ecuación $x^m - 1 = 0$, y por tanto, existen $p^n - 1$ raíces diferentes en esta ecuación. Pero, como cada polinomio de grado m tiene como máximo m raíces, deducimos que $m = p^n - 1$. Por tanto, el elemento que tiene orden m genera todo el grupo multiplicativo, es decir, el grupo $(K^*, \cdot)$ es cíclico. □

Hasta ahora hemos demostrado que, si existe un cuerpo finito K, debe cumplir las condiciones siguientes:

1. $|K| = p^n$;
2. $(K, +) \simeq ((\mathbb{Z}_p)^n, +)$;
3. $(K^*, \cdot)$ es cíclico.

La pregunta que nos formulamos a continuación tiene una apariencia sencilla, teniendo en cuenta la información de que disponemos, pero realmente no es así. Dado cualquier número primo p y cualquier número natural n, ¿existe un cuerpo de orden p^n?

Sabemos ya que, si en el anillo de los números enteros $(\mathbb{Z}, +, \cdot)$ definimos la relación de equivalencia módulo un número primo p, obtenemos el cuerpo $(\mathbb{Z}_p, +, \cdot)$ de orden p. De forma similar, si en el anillo de los polinomios $(\mathbb{Z}_p[x], +, \cdot)$ definimos la relación de equivalencia módulo un polinomio primo de grado n, obtendremos un cuerpo de orden p^n, llamado *cuerpo de Galois* de orden p^n en honor de Evariste Galois (1811–1832) y denotado por $GF(p^n)$ o simplemente $\mathbf{F}_q$, con $q = p^n$. Éste es entonces el modelo que aventurábamos anteriormente.

Teorema 11.49. Si $p(x) \in \mathbb{Z}_p[x]$ es un polinomio primo de grado n, entonces $\mathbb{Z}_p[x]/p(x)$ es un cuerpo de orden p^n, llamado cuerpo de Galois y denotado por $\mathbf{F}_{p^n}$.

Demostración. Por el hecho de ser $\mathbb{Z}_p[x]$ un anillo principal, sus ideales maximales están justamente generados por polinomios primos y por tanto $\mathbb{Z}_p[x]/p(x)$ es un cuerpo. □

El problema, entonces, consiste en asegurar la existencia de algún polinomio primo con coeficientes sobre cualquier cuerpo $\mathbb{Z}_p$ y de cualquier grado n. Demostrar la existencia de estos polinomios es laborioso y requiere la introducción de conceptos algebraicos que van más allá de los propósitos de este libro, pero alentamos al lector interesado y lo dirigimos a [3] [5].

Teorema 11.50. Para cualquier número natural n y cualquier número primo p, existe un polinomio primo $p(x) \in \mathbb{Z}_p[x]$ de grado n.

Muy esquemáticamente, la demostración consiste en caracterizar los elementos del cuerpo a partir de las raíces del polinomio $(x^{p^n-1} - 1)x = x^{p^n} - x$. Trivialmente, localizamos los elementos neutros del cuerpo como raíces de este polinomio. El resto de los elementos serán también raíces del polinomio y, por tanto, de los factores de su descomposición. Más concretamente: se caracterizan los elementos del cuerpo a partir de las raíces de los polinomios irreductibles de grado d, d divisor de n. Se demuestra que las raíces de un polinomio irreductible de grado d sobre $\mathbf{F}_p$ son las p-ésimas potencias de una de sus raíces α: $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$, para algún elemento α del cuerpo. A partir de este resultado se deduce que los factores de $x^{p^n} - x$ son todos los polinomios irreductibles sobre $\mathbf{F}_p$ de grado d. Finalmente se demuestra que, para $d = n$, el número de estos polinomios es como mínimo 1.

Sabiendo de su existencia, la obtención práctica de estos polinomios es también en general muy laboriosa. Por este motivo se han construido unas tablas con todos los polinomios irreductibles de grado n sobre $\mathbf{F}_p$ para valores razonablemente moderados de p y de n. En la tabla 11.1 presentamos una muestra que incluye los polinomios irreductibles sobre $\mathbf{F}_2$ y sobre $\mathbf{F}_3$ de grados 1, 2 y 3.

Tabla 11.1: Polinomios irreductibles de grado 1, 2 y 3 sobre $\mathbf{F}_p$

grado	$\mathbf{F}_2$	$\mathbf{F}_3$
1	x	x
	$x+1$	$x+1$
		$x+2$
2	x^2+x+1	x^2+1
		x^2+2x+2
		x^2+x+2
3	x^3+x+1	x^3+2x+1
	x^3+x^2+1	x^3+2x^2+1
		x^3+x^2+2
		x^3+2x^2+2
		x^3+x^2+x+2
		x^3+x^2+2x+1
		x^3+2x^2+x+1
		x^3+2x^2+2x+2

Observemos en primer lugar que se consideran sólo polinomios mónicos, ya que sabemos que un polinomio $p(x) \in \mathbf{F}_p[x]$ es irreductible si y sólo si lo es el polinomio $kp(x)$, para todo $k \in \mathbf{F}_p^*$.

Para los valores de p y n que aparecen en la tabla 11.1 es razonablemente sencillo deducir los posibles polinomios primos. Para ello, procedemos de forma similar a como lo haríamos para determinar si un número es primo. Claramente, los únicos polinomios irreductibles de grado 1 son los que figuran en la tabla. Los polinomios reducibles de grado 2 serán producto de dos polinomios irreductibles de grado 1; así tenemos que $x \cdot x = x^2$, $x(x+1) = x^2+x$ y $(x+1)(x+1) = x^2+1$ son los únicos polinomios reducibles de grado 2 sobre $\mathbb{Z}_2$ y por tanto x^2+x+1 representa el único polinomio irreductible de grado 2 sobre $\mathbb{Z}_2$. De hecho, hay cuatro polinomios de grado 3 que contienen únicamente factores de grado 1 y dos que contienen factores de grado 1 y de grado 2. Por tanto, sólo dos de los ocho posibles polinomios de grado 3 sobre $\mathbb{Z}_2$ son irreductibles. En general, es preciso observar que hay p^n polinomios mónicos de grado $n \geqslant 1$. Algunos de estos polinomios se obtienen como producto de factores de grado más pequeño, pero, de hecho, no existen p^n maneras diferentes de combinar polinomios irreductibles de grado menor que n para obtener uno de grado n.

Conociendo ya algunos polinomios irreductibles, pasamos a construir los cuerpos correspondientes.

Comenzamos con $\mathbf{F}_4$. Para ello, consideramos en $\mathbb{Z}_2[x]$ la relación de equivalencia módulo el único polinomio irreductible de grado dos que tenemos, $p(x) = x^2 + x + 1$. Las clases que se obtienen quedan representadas por los polinomios $\{0, 1, x, x+1\}$. Así,

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{[0], [1], [x], [x+1]\}$$

Recordemos que en general la suma y el producto de clases están definidos a partir de sus representantes. Por tanto,

$$\{[0], [1], [x], [x+1]\} = \{0, 1, [x], [x]+1\}$$

Si representamos la clase $[x] = \{x + (x^2 + x + 1)c(x), c(x) \in \mathbb{Z}_2[x]\}$ por α, las tablas 11.2 y 11.3 muestran el comportamiento de los elementos del cuerpo $\mathbb{Z}_2[x]/(x^2 + x + 1)$ respecto de la suma y el producto.

Tabla 11.2: Tabla de $(\mathbf{F}_4, +)$

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Tabla 11.3: Tabla de $(\mathbf{F}_4(\alpha), \cdot)$

$\cdot$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

Es preciso observar que mediante la relación de equivalencia definida se ha conseguido tener el producto cerrado en el conjunto de polinomios sobre $\mathbb{Z}_2$ de grado inferior a 2.

Es interesante observar también que, en este caso, α es un generador del grupo multiplicativo $(\mathbb{Z}_2^\star[x]/(x^2+x+1),\cdot) = (\mathbf{F}_4(\alpha),\cdot)$, es decir, podemos obtener todos los elementos del cuerpo salvo el cero, como las 2^2-1 potencias sucesivas de α:

$$\{\mathbb{Z}_2^\star[x]/(x^2+x+1)\} = \mathbf{F}_4(\alpha) = \{1,\alpha,\alpha+1\} = \{\alpha^3,\alpha,\alpha^2\}$$

Es interesante, para facilitar los cálculos en las tablas de multiplicar, obtener un generador simple. En general se dice que un generador del grupo multiplicativo del cuerpo es un *elemento primitivo*. Cabe observar que este elemento siempre existe (el grupo multiplicativo del cuerpo es siempre cíclico).

Para construir $\mathbf{F}_8$ tenemos dos posibles elecciones para el polinomio irreductible, x^3+x+1 o x^3+x^2+1.

En primer lugar, calculamos los 8 polinomios de grado inferior a 3 con coeficientes en $\mathbb{Z}_2$:

$$\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$$

Observemos que la tabla de sumar se obtiene directamente. Nos centraremos por tanto en la tabla de multiplicar.

Está claro que, multiplicando los representantes de cada clase y calculando los restos módulo x^3+x+1 o x^3+x^2+1, obtendremos unos representantes mónicos de los elementos de $\mathbb{Z}_2[x]/(x^3+x+1)$ y $\mathbb{Z}_2[x]/(x^3+x^2+1)$ respectivamente. Pero estos cálculos en general son tediosos y es por ello interesante encontrar un elemento primitivo del cuerpo.

Si consideramos $\mathbb{Z}_2[x]/(x^3+x+1)$, por ejemplo, podemos comprobar que las 2^3-1 potencias sucesivas de x dan lugar a toda una familia de representantes del grupo multiplicativo del cuerpo y, por tanto, del propio cuerpo.

$$\{x,x^2,x^3,x^4,x^5,x^6,x^7\} = \{x,x^2,x+1,x^2+x,x^2+x+1,x^2+1,1\}$$

Consecuentemente, podemos representar los elementos del cuerpo por las sucesivas potencias de $[x]$:

$$\{[x],[x]^2,[x]^3=[x]+1,[x]^4=[x]^2+[x],[x]^5=[x]^2+[x]+1,[x]^6=[x]^2+1,[x]^7=1\}$$

Igual que en el ejemplo anterior, la clase de $[x]$, que denotaremos también por α, es un elemento primitivo del cuerpo que ahora denotamos por $\mathbf{F}_8(\alpha)$. Así, para construir la tabla 11.4 usaremos las potencias de α. Para encontrar los polinomios correspondientes a las potencias de α sólo es preciso deshacer los cambios que figuran a la derecha en la tabla 11.4.

Si utilizamos x^3+x^2+1 para construir $\mathbf{F}_8$, podemos comprobar, también en este caso, que a partir de las 2^3-1 potencias sucesivas de x obtenemos toda una familia de representantes de los elementos del cuerpo diferentes de cero. Pero en este caso las relaciones son las siguientes:

$$\{[x],[x^2],[x^3]=[x^2+1],[x^4]=[x^2+x+1],[x^5]=[x+1],[x^6]=[x^2+x],[x^7]=1\}$$

Tabla 11.4: Tabla de $(\mathbf{F}_8(\alpha),\cdot)$

$\cdot$	α	α^2	α^3	α^4	α^5	α^6	1
α	α^2	α^3	α^4	α^5	α^6	1	α
α^2	α^3	α^4	α^5	α^6	1	α	α^2
α^3	α^4	α^5	α^6	1	α	α^2	α^3
α^4	α^5	α^6	1	α	α^2	α^3	α^4
α^5	α^6	1	α	α^2	α^3	α^4	α^5
α^6	1	α	α^2	α^3	α^4	α^5	α^6
1	α	α^2	α^3	α^4	α^5	α^6	1

$\alpha^1 = [x]$
$\alpha^2 = [x]^2$
$\alpha^3 = [x]+1$
$\alpha^4 = [x]^2+[x]$
$\alpha^5 = [x]^2+[x]+1$
$\alpha^6 = [x]^2+1$
$\alpha^7 = 1$

Igual que en el ejemplo anterior, la clase de $[x]$, que denotaremos ahora por β, es un elemento primitivo del cuerpo, denotado por $\mathbf{F}_8(\beta)$. Y, también igual que antes, construimos la tabla del producto a partir de las potencias de β (Tabla 11.5).

Tabla 11.5: Tabla de $(\mathbf{F}_8(\beta),\cdot)$

$\cdot$	β	β^2	β^3	β^4	β^5	β^6	1
β	β^2	β^3	β^4	β^5	β^6	1	β
β^2	β^3	β^4	β^5	β^6	1	β	β^2
β^3	β^4	β^5	β^6	1	β	β^2	β^3
β^4	β^5	β^6	1	β	β^2	β^3	β^4
β^5	β^6	1	β	β^2	β^3	β^4	β^5
β^6	1	β	β^2	β^3	β^4	β^5	β^6
1	β	β^2	β^3	β^4	β^5	β^6	1

$\beta^1 = [x]$
$\beta^2 = [x]^2$
$\beta^3 = [x]^2+1$
$\beta^4 = [x]^2+[x]+1$
$\beta^5 = [x]+1$
$\beta^6 = [x]^2+[x]$
$\beta^7 = 1$

Si comparamos las tablas 11.4 y 11.5, vemos que son evidentemente idénticas. Sin embargo, después de substituir en estas tablas las sucesivas potencias por los polinomios correspondientes, las tablas no coinciden. Es fácil comprobar que $\beta+1$ es, de hecho, otro elemento primitivo de x^3+x+1. Esto quiere decir que existe un isomorfismo ϕ de $(\mathbb{Z}_2[x]/(x^3+x+1)$ en $(\mathbb{Z}_2[x]/(x^3+x^2+1)$

$$\phi : \mathbf{F}_8(\alpha) \longrightarrow \mathbf{F}_8(\beta)$$

tal que $\phi(\alpha) = \beta+1$.

Este hecho no es casual. En general, se demuestra que todos los posibles cuerpos de un mismo orden son isomorfos. De hecho, hemos visto ya que todos los cuerpos de orden p^n tienen sus grupos aditivos isomorfos a $((\mathbb{Z}_p)^n, +)$ y sus grupos multiplicativos son cíclicos de orden $p^n - 1$. Queda, por tanto, por ver que la estructura del cuerpo no depende del generador que escogemos ni en particular, entonces, del polinomio irreductible escogido. Por razones similares a las aludidas cuando planteábamos la existencia de un polinomio irreductible de cualquier grado sobre cualquier $\mathbb{Z}_p$ con p primo, prescindiremos de presentar aquí la demostración formal sobre la existencia en general de un isomorfismo entre dos cuerpos cualesquiera del mismo orden y recomendamos, al lector interesado en esta cuestión, la misma bibliografía.

El teorema siguiente recoge de manera concisa el resultado que acabamos de mencionar.

Teorema 11.51. Para cada número primo p y para cada número natural n, hay un único cuerpo, salvo isomorfismos, de orden p^n llamado cuerpo de Galois, $\mathbf{GF}(p^n)$.

Notas bibliográficas

Aunque la parte introductoria de este capítulo, es decir, la que se refiere a las definiciones y primeras propiedades de los anillos, se puede encontrar en cualquier libro introductorio de álgebra, nosotros preferimos recomendar, incluso para esta parte, libros de cariz aplicado, ya que éste será nuestro último interés y es conveniente no dispersar los objetivos en cuestiones extremadamente teóricas. En este sentido el libro de Birkhoff y Bartee [2] puede ser de gran ayuda. Es interesante tener más de una referencia, y tanto el libro del Stone [5] como el de Childs [4] pueden también ser útiles en esta primera parte. Para la última parte, la que corresponde a los cuerpos finitos, recomendamos el libro de Lindl [3], teniendo en cuenta que, si bien su calidad es indudable, su nivel es superior al de este libro. Para compensar este desnivel, el libro de Biggs [1] es ideal. También se encuentra explicado este tema a un nivel intermedio en los otros libros recomendados para la primera parte.

Bibliografía

[1] N. L. Biggs. *Matemática Discreta*, Vicens Vives, 1993.

[2] G. Birkhoff, T. C. Bartee. *Modern Applied Algebra*, McGraw-Hill, 1970.

[3] R. Lidl, G. Pilz. *Applied Abstract Algebra*, Springer-Verlag, 1984.

[4] L. Childs. *A Concrete Introduction to Higher Algebra*, Springer-Verlag, 1988.

[5] H. S. Stone. *Discrete Mathematical Structures and their Applications*, Science Research Asociates, SRA, 1973.

Problemas

1. Demostrar que el producto en un anillo A es conmutativo si y sólo si para todo $a,b \in A$,
$$(a+b)^2 = a^2 + 2ab + b^2$$

2. Comprobar que el conjunto de aplicaciones de un anillo A sobre él mismo, $F(A)$, tiene estructura de anillo con la suma y el producto de aplicaciones, es decir, que para toda $f,g \in F(A)$ y para todo $x \in A$ se define:
$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (fg)(x) &= f(x)g(x)\end{aligned}$$

3. Demostrar, de forma general, que el conjunto de aplicaciones de un conjunto cualquiera X sobre un anillo A, $F(X,A)$, tiene con las mismas operaciones del ejercicio anterior, estructura de anillo.

4. Sea $(G,+)$ un grupo abeliano. Demostrar que el conjunto de aplicaciones de G en G con la suma y la composición de aplicaciones, $(End(G),+,\circ)$, es un anillo unitario. ¿Tiene divisores de cero? Estudiar el caso de $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

5. Demostrar que si un anillo $(A \neq \{0\},+,\cdot)$ es unitario, entonces los elementos neutros de la suma y el producto son diferentes.

6. Un anillo A en el cual todo elemento $a \in A$ es independiente de la segunda operación, es decir, $a^2 = a$, se llama *anillo de Boole*. Demostrar que
   (a) A es de característica 2 y es abeliano;
   (b) para todo $a,b \in A$ se cumple que $ab(a+b) = 0$;
   (c) si A es íntegro, entonces $A = \{0\}$ o bien $A \simeq \mathbb{Z}_2$;
   (d) sólo hay un anillo de Boole de cuatro elementos.

7. Si X es un conjunto cualquiera, demostrar que $(P(X),\triangle,\cap)$ es un anillo de Boole, con la llamada *diferencia simétrica*, $\triangle$, como primera operación. Es decir, para todo $C,D \subseteq X$
$$C \triangle D = (C \cup D) - (C \cap D)$$

8. Consideremos en el producto cartesiano de dos anillos A_1 y A_2 las operaciones suma y producto siguientes:
$$\begin{aligned}(a_1,a_2)+(b_1,b_2) &= (a_1+b_1,a_2+b_2)\\ (a_1,a_2)(b_1,b_2) &= (a_1b_1,a_2b_2)\end{aligned}$$

(a) Demostrar que $(A_1 \times A_2, +, \cdot)$ es un anillo, llamado *producto cartesiano*.

(b) Estudiar cómo se trasladan la conmutatividad, la integridad y la existencia de unidad de A_1 y A_2 a $A_1 \times A_2$.

9. El conjunto de elementos de un anillo A que conmutan con todos los elementos de A

$$Z(A) = \{x \in A \mid xa = ax, \forall a \in A\}$$

se llama *centro* de A. Demostrar que es un subanillo de A.

10. Dado un anillo unitario A y un elemento $a \in A$, demostrar que la aplicación $\phi : A \longrightarrow A$ definida por $\phi(x) = axa^{-1}$ es un automorfismo de A.

11. Demostrar que el conjunto de elementos invertibles de un anillo unitario A

$$U(A) = \{u \in A \mid \exists a \in A, au = ua = 1\}$$

es un subgrupo del grupo multiplicativo A^*. Calcular $U(\mathbb{Z})$, $U(\mathbb{Z}_3)$, $U(\mathbb{Z}_6)$ y en general $U(\mathbb{Z}_n)$.

12. Demostrar que la imagen homomórfica de un cuerpo es un cuerpo.

13. Dado un cuerpo K, demostrar que la aplicación $f : K \longrightarrow K$ tal que $f(k) = k^p$ es un automorfismo si K tiene característica p.

14. Dado un subconjunto propio Y de un anillo A, consideremos el llamado *anulador por la izquierda* de Y. Éste es el conjunto X de elementos de A tal que

$$X(Y) = \{x \in A \mid xy = 0, \forall y \in Y\}$$

Demostrar que es un ideal por la izquierda de A.

15. Si A es un anillo unitario, consideremos el producto cartesiano $\mathbb{Z} \times A$ con las operaciones siguientes:

$$\begin{aligned} (n,a)+(m,b) &= (n+m, a+b) \\ (n,a)(m,b) &= (nm, nb+ma+ab) \end{aligned}$$

(a) Demostrar que $\mathbb{Z} \times A$ es un anillo unitario.

(b) Demostrar que $\{0\} \times A$ es un ideal bilateral de $\mathbb{Z} \times A$.

16. Dar ejemplos de polinomios $a(x)$ y $b(x)$ de $\mathbb{Z}_6[x]$ tales que $gr(ab) < gr(a) + gr(b)$. ¿Hay polinomios con estas condiciones en $\mathbb{Z}_5[x]$? ¿Por qué?

17. Comprobar que en $\mathbb{Z}_{12}[x]$ la igualdad siguiente es cierta:

$$(x+1)(x+11) = (x+7)(x+5)$$

¿Es cierta también en $\mathbb{Z}_{13}[x]$? ¿Por qué?

18. Encontrar un polinomio $a(x) \in \mathbb{Z}_n[x]$ no nulo tal que su función polinómica $\bar{a}(x)$ sea nula.

19. Demostrar que en $\mathbb{Z}_p[x]$ (p es primo) los polinomios

$$\begin{cases} a(x) &= x^p \\ b(x) &= x \end{cases}$$

definen la misma función polinómica.

20. ¿Se puede efectuar la divisió euclídea en $\mathbb{Z}[x]$ de

$$\begin{cases} a(x) &= 5x^3 + 2x - 1 \\ b(x) &= x^2 - 3x + 11 \ ? \end{cases}$$

¿Por qué?

21. Sean $a(x), b(x) \in K[x]$ dos polinomios primos entre sí. Demostrar que

$$a(x)|b(x)c(x) \Rightarrow a(x)|c(x)$$

22. Comprobar que $(x+1)^3 = x^3 + 1$ en $\mathbb{Z}_3[x]$. Encontrar para qué valores de n es cierto en $\mathbb{Z}_n[x]$ que

$$(x+1)^n = x^n + 1$$

23. Sea $a(x) \in \mathbb{Z}_p[x]$. Demostrar que, en general, si p es primo, entonces se cumple

(a) $(a(x))^p = a(x^p)$

(b) $(a(x))^{p^n} = a(x^{p^n})$

24. Demostrar que los polinomios $a(x) = x^2 + 1$ y $b(x) = 2x$ son polinomios primos entre sí en $\mathbb{Z}[x]$. Deducir que $\mathbb{Z}[x]$ no es principal.

25. Demostrar que en $\mathbb{Z}[x]$ el ideal generado por $x^2 + 1$ es primo pero no es maximal. ¿Por qué?

26. Factorizar $3x^2 + 2x - 1$ en $\mathbb{Q}[x]$, $\mathbb{Z}_3[x]$ y $\mathbb{Z}[x]$.

27. Encontrar un polinomio irreductible de grado tres en $\mathbb{Z}_5[x]$.

28. Demostrar que ax^2+bx+c es irreductible en $\mathbb{Z}_p[x]$ (p es primo), si y sólo si b^2-4ac no es un cuadrado en $\mathbb{Z}_p$.

29. Demostrar que el grupo aditivo de $\mathbf{F}_9$ no es cíclico.

30. Construir dos representaciones de $\mathbf{F}_9$ y comprobar que son isomórficas.

Capítulo 12

Estructuras combinatorias

1. Diseños combinatorios
2. Geometrías finitas
3. Cuadrados latinos

Las estructuras combinatorias estudian de manera sistemática la selección de objetos según unas reglas específicas, o bien, de forma equivalente, las relaciones de incidencia entre determinados objetos y ciertos subconjuntos de estos objetos. La construcción de estas estructuras depende en gran medida de las estructuras algebraicas que se han descrito en los capítulos anteriores, aunque están relacionadas también con otras ramas de la matemática, como por ejemplo la teoría de números o las geometrías finitas entre otros.

Este capítulo pretende dar una visión general sobre estas estructuras, y dedica una atención especial a algunas de ellas como ejemplos ilustrativos importantes. La primera sección está dedicada a introducir los diseños combinatorios como modelos generales de estructuras combinatorias. En la segunda sección se introducen las geometrías finitas y se particulariza el estudio en los planos proyectivos y los planos afines como modelos geométricos de ciertos diseños combinatorios. El capítulo finaliza con el estudio de los cuadrados latinos como modelo combinatorio útil para contrastar diferentes aspectos de un mismo fenómeno.

12.1 Diseños combinatorios

Un *diseño combinatorio* es un par $D = (V, B)$ formado por un conjunto de elementos $V = \{x_1, x_2, \ldots, x_v\}$, llamado conjunto de *variedades*, y una familia de subconjuntos de estas variedades $B = \{B_i, B_i \subset V\}$, llamados *bloques* del diseño.

El número de variedades de un diseño D se denota por $|V| = v$ y el número de sus bloques por $b = |B|$.

Un diseño es, entonces, un sistema general de incidencia que nos dice cuándo un elemento (variedad) $x_i \in V$ está en un determinado subconjunto (bloque) $B_j \in B$. Una forma útil y sencilla de representar el sistema es a partir de lo que se llama su *matriz de incidencia*.

$$A = (a_{ij})_{v \times b}, \quad a_{ij} = \begin{cases} 1, & \text{si } x_i \in B_j \\ 0, & \text{si } x_i \notin B_j \end{cases}$$

Por ejemplo,

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

corresponde a la matriz de incidencia de un diseño $D = (V, B)$, con conjunto de variedades $V = \{1, 2, 3, 4, 5\}$ y conjunto de bloques:

$$B = \{\{4\}, \{4\}, \{2, 4\}, \{2, 3, 4\}\}$$

Observar que se admite la posibilidad que B tenga bloques repetidos. Cuando éste no es el caso, se dice que el diseño es *simple*.

Se dice que dos diseños $D = (V, B)$ y $DE = (V', B')$ son *isomorfos* si se puede obtener uno del otro reordenando variedades o bloques. Es decir, sus matrices de incidencia, A y A', se obtienen una de la otra intercambiando filas (variedades) o columnas (bloques). Más concretamente, D es isomorfo a D' si existen matrices de permutaciones P y Q (de dimensiones $v \times v$ y $b \times b$ respectivamente) tales que,

$$A' = PAQ$$

Por ejemplo, el diseño D' que tiene por matriz de incidencia

$$A' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

es isomorfo al diseño D descrito anteriormente, ya que existen dos matrices de permutaciones P y Q tales que:

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = PAQ$$

Esto corresponde a intercambiar las variedades y los bloques según las biyecciones siguientes:

$$\begin{array}{lcl} x_1 & \to & x_1 = x'_1 \\ x_2 & \to & x_4 = x'_2 \\ x_3 & \to & x_3 = x'_3 \\ x_4 & \to & x_5 = x'_4 \\ x_5 & \to & x_2 = x'_5 \end{array} \qquad \begin{array}{lcl} B_1 & \to & B_4 = B'_1 \\ B_2 & \to & B_3 = B'_2 \\ B_3 & \to & B_2 = B'_3 \\ B_4 & \to & B_1 = B'_4 \end{array}$$

Hay diversas maneras de utilizar un diseño $D = (V, B)$ para construir otros diseños relacionados con él. Quizá la más sencilla de todas es la que corresponde al llamado *diseño dual*, en el cual las funciones de las variedades y de los bloques se intercambian. De forma más precisa, si denotamos el diseño dual de $D = (V, B)$ por

$$D^T = (V^T, B^T) = (B, V)$$

entonces cada variedad $x \in V$ corresponde a un bloque de B^T y cada bloque $B \in B$ corresponde a una variedad de V^T. Las incidencias en D^T vienen dadas por la regla siguiente: una variedad $B \in V^T$ está en el bloque $x \in B^T$ si y sólo si $x \in V$ es de $B \in B$.

Por ejemplo, dado el diseño $D = (V, B)$, con $V = \{1, 2, 3, 4, 5, 6\}$ y el conjunto B formado por los bloques:

$$\begin{array}{ll} B_1 = \{1, 2, 3\} & B_5 = \{2, 4, 5\} \\ B_2 = \{1, 4, 5\} & B_6 = \{2, 4, 6\} \\ B_3 = \{1, 2, 6\} & B_7 = \{3, 4, 5\} \\ B_4 = \{1, 3, 6\} & B_8 = \{3, 5, 6\} \end{array}$$

su diseño dual $D^T = (V^T, B^T)$ tiene como conjunto de variedades $V^T = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y como conjunto de bloques B^T el formado por

$$\begin{array}{ll} B_1 = \{1, 2, 3, 4\} & B_4 = \{2, 5, 6, 7\} \\ B_2 = \{1, 3, 5, 6\} & B_5 = \{2, 5, 7, 8\} \\ B_3 = \{1, 4, 7, 8\} & B_6 = \{3, 4, 6, 8\} \end{array}$$

A partir de la definición está claro que el diseño dual del diseño dual es el propio diseño, $(D^T)^T = D$. Se puede demostrar como ejercicio la relación entre las matrices de incidencia de un diseño y su dual:

Proposición 12.1. Si A es la matriz de incidencia de un diseño D, entonces la matriz transpuesta A^T es la matriz de incidencia del diseño dual D^T.

A partir de un diseño $D = (V, B)$ también se puede definir la estructura que se obtiene al reemplazar cada bloque $B_i \in B$ por su complemento $\bar{B}_i = V \setminus B_i$. De esta manera se obtiene otro diseño sobre el mismo conjunto de variedades con el mismo número de bloques, llamado *diseño complementario* de D y que denotaremos por

$$\bar{D} = (\bar{V}, \bar{B}) = (V, B)$$

Por ejemplo, la matriz

$$\bar{A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

es la matriz de incidencia del diseño complementario del primer diseño considerado. Los respectivos conjuntos de bloques figuran a continuación:

$$\begin{aligned} B &= \{\{4\},\{4\},\{2,4\},\{2,3,4\}\} \\ \bar{B} &= \{\{1,2,3,5\},\{1,2,3,5\},\{1,3,5\},\{1,5\}\} \end{aligned}$$

Diseños regulares

El estudio sistemático de estas estructuras hace necesaria la consideración de ciertas restricciones sobre las relaciones de incidencia. Las más básicas son las que figuran a continuación y caracterizan los diseños que las cumplen.

Se dice que un diseño $D = (V, B)$ es

a) *incompleto* si existe algún bloque $B_i \in B$ tal que, $|B_i| < v$;

b) *uniforme* si cada bloque tiene el mismo número (k) de variedades;

c) *regular* si cada variedad pertenece al mismo número (r) de bloques.

Es fácil comprobar que los subconjuntos de $V = \{1,2,3,4,5,6\}$

$$\begin{array}{ll} B_1 = \{1,2,3\} & B_5 = \{2,4,5\} \\ B_2 = \{1,4,5\} & B_6 = \{2,4,6\} \\ B_3 = \{1,2,6\} & B_7 = \{3,4,5\} \\ B_4 = \{1,3,6\} & B_8 = \{3,5,6\} \end{array}$$

constituyen los bloques de un diseño que cumple estas condiciones.

Estas restricciones en las relaciones de un diseño se traducen en la correspondiente matriz de incidencia en las condiciones siguientes:

a) existe alguna columna con algún 0;

b) cada columna tiene el mismo número (k) de 1;

c) cada fila tiene el mismo número (r) de 1.

La matriz de incidencia del diseño anterior es:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Ejercicio 12.2. Demostrar que si $A \in M_{v\times b}(\mathbb{Z}_2)$ es la matriz de incidencia de un diseño uniforme y regular, entonces, si J_n denota la matriz $n \times n$ con todos los términos iguales a 1, se cumple:

b) $J_v A = kJ_{v\times b}$

c) $AJ_b = rJ_{v\times b}$

Éstas fueron las condiciones que propuso R. A. Fisher en 1940 para obtener un buen modelo estadístico para comparar diferentes marcas de un mismo producto. En este caso, un determinado número de personas, b, tiene que probar v marcas de un determinado producto de manera que cada persona tiene que probar el mismo número, k, de marcas y cada marca tiene que ser probada por el mismo número, r, de personas. Está claro que si cada persona prueba todas las marcas, entonces el problema tiene solución, considerando, por ejemplo, la relación de parámetros, $b = v = k = r$. Pero esta solución es demasiado costosa y es conveniente buscar otras con $k < v$.

Esta sección la dedicaremos al estudio de este tipo de estructuras, a las que nos referiremos como diseños regulares, o directamente como diseños, e indicaremos sus parámetros con (v,k,r). El número de bloques de un (v,k,r) diseño no es arbitrario. Es inmediato comprobar que si existe un diseño regular, sus parámetros tienen que cumplir la relación siguiente:

Proposición 12.3. En todo diseño regular de parámetros (v,k,r) se cumple:

$$bk = rv$$

Demostración. Es suficiente observar que el número (n) de incidencias se puede contar de dos maneras diferentes:

1. $n = bk$, ya que hay b bloques con k variedades;
2. $n = rv$, ya que cada variedad pertenece a r bloques.

□

Ejercicio 12.4. Demostrar que si una matriz $A \in M_{v\times b}(\mathbb{Z}_2)$ cumple las condiciones del ejercicio 12.2, entonces A es la matriz de incidencia de un diseño regular con parámetros (v,k,r).

t-diseños

Se puede aumentar la regularidad de un diseño exigiendo que cada t-subconjunto de variedades, donde $1 \leqslant t \leqslant k \leqslant v$, esté contenido en el mismo número (λ) de bloques. En este caso, el sistema correspondiente se llama *t-diseño* y se denota por

$$t\text{-}(v,k,\lambda)$$

Los diseños regulares son por tanto 1-diseños, tomando $t = 1$ y $\lambda = r$. La proposición 12.3 se puede obtener también como caso particular del teorema siguiente, que nos dice cuál es la relación que tienen que mantener los parámetros de cualquier t-diseño. Su demostración es también una generalización del razonamiento utilizado en el caso de diseños regulares.

Teorema 12.5. El número de bloques de un t-(v,k,λ) diseño es

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}$$

Demostración. Sea (V,B) un t-(v,k,λ) diseño. Para obtener el resultado contaremos de dos maneras diferentes el número de pares (T,B), donde T es un t-subconjunto de V y $B \in B$ es un bloque que contiene el subconjunto T.

El número de t-subconjuntos contenidos en un bloque es $\binom{k}{t}$ y por tanto hay $b\binom{k}{t}$ de estos pares. Por otra parte, $\binom{v}{t}$ es el número de t-subconjuntos de V y λ es el número de bloques que contienen T y por tanto el número de pares (T,B) es también $\lambda\binom{v}{t}$. □

Esta condición, contrariamente al caso de los 1-diseños, no es suficiente para la existencia del diseño correspondiente. Por ejemplo, se ha demostrado la no existencia de ningún diseño con parámetros 2-$(43,7,1)$ o 10-$(16,72,1)$. Es necesario, por tanto, encontrar recursos que faciliten la obtención en general de t-diseños, o al menos, que nos aseguren su no existencia.

Siguiendo el mismo tipo de razonamiento, se puede generalizar el resultado anterior:

Teorema 12.6. El número de bloques, λ_s, de un t-(v,k,λ_t) diseño que contienen un determinado s-subconjunto $S \subset V$, con $s \leqslant t$, es

$$\lambda_s = \lambda_t \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$$

Demostración. Sea (V,B) un t-(v,k,λ) diseño. Contemos ahora de dos maneras diferentes el número de pares (T,B), donde T es un t-subconjunto de V que contiene un determinado s-subconjunto S, y $B \in B$ es un bloque que contiene T.

El número de t-subconjuntos que contienen S y están contenidos en un determinado bloque es $\binom{k-s}{t-s}$, y el número de bloques que contienen S es λ_s. Por otra parte, el número de t-subconjuntos que contienen S es $\binom{v-s}{t-s}$, y el número de veces (bloques) que aparece cada t-subconjunto es λ_t. De donde:

$$\lambda_s \binom{k-s}{t-s} = \lambda_t \binom{v-s}{t-s}$$

□

Observemos que el valor λ_s, obtenido en el teorema anterior, no depende del conjunto S que se ha considerado: todos los subconjuntos de tamaño s están contenidos en λ_s bloques. Como consecuencia inmediata deducimos que un t-diseño tiene que ser también un s-diseño para $1 \leqslant s \leqslant t$.

Corolario 12.7. Todo t-diseño es también un s-diseño, para todo $1 \leqslant s \leqslant t$.

Por ejemplo, los subconjuntos de $\{1,2,3,4,5,6,7,8\}$

$$\begin{array}{ll} \{1,2,3,5\} & \{2,3,4,7\} \\ \{1,2,4,8\} & \{2,3,6,8\} \\ \{1,2,6,7\} & \{2,4,5,6\} \\ \{1,3,4,6\} & \{2,5,7,8\} \\ \{1,3,7,8\} & \{3,4,5,8\} \\ \{1,4,5,7\} & \{3,5,6,7\} \\ \{1,5,6,8\} & \{4,6,7,8\} \end{array}$$

constituyen los bloques de un 3-$(8,4,1)$ diseño , ya que, como es fácil comprobar, cualquier 3-subconjunto aparece una única vez. Es fácil comprobar también que cualquier 2-subconjunto aparece en tres bloques diferentes, por ejemplo el par $\{1,3\}$ aparece en los bloques $\{1,2,3,5\}$, $\{1,3,4,6\}$ y $\{1,3,7,8\}$. Así, estos bloques son también bloques de un 2-$(8,4,3)$ diseño y también de un 1-$(8,4,7)$ diseño. Es inmediato comprobar, sin embargo, que no constituyen un 4-diseño, ya que no aparece, por ejemplo, el 4-subconjunto $\{1,2,3,4\}$.

A causa de la dificultad que supone la construcción de un t-diseño en general, es interesante como mínimo poder obtener algunos diseños a partir de otros conocidos. En este sentido, el teorema anterior (12.6) nos proporciona también un recurso útil.

Dado un t-diseño $D = (V,B)$ y un s-subconjunto S de V, con $s \leqslant t$, se define lo que llamaremos diseño *s-derivado* de D respecto de S y que denotaremos por

$$D_S = (V_S, B_S)$$

donde $V_S = V \setminus S$ y

$$B_S = \{B_i \setminus S, B_i \in B : S \subset B_i\}$$

Es decir, un diseño s-derivado es el que se obtiene de un t-diseño suprimiendo $s \leqslant t$ variedades de V y de cada uno de los bloques de D que contienen cada una de estas s variedades. Si S sólo tiene un elemento, entonces se dice que D_S es una *contracción* de D respecto del 1-subconjunto S.

Por ejemplo, los diseños s-derivados del diseño 3-$(8,4,1)$ descrito anteriormente son los diseños 2-$(7,3,1)$ y el 1-$(6,2,1)$, que figuran a continuación y que se obtienen suprimiendo de 3-$(8,4,1)$ los subconjuntos $S = \{8\}$ y $S = \{7,8\}$ respectivamente.

$$\{1,2,4\},\ \{2,3,6\},\ \{1,3,7\},\ \{2,5,7\},\ \{1,5,6\},\ \{3,4,5\},\ \{4,6,7\}$$
$$\{1,3\},\ \{2,5\},\ \{4,6\}$$

Cabe observar que 2-$(7,3,1)$ es una contracción de 3-$(8,4,1)$.

Es inmediato comprobar, como consecuencia del teorema 12.6, que D_S es efectivamente un t-diseño con los parámetros que figuran a continuación.

Corolario 12.8. Si existe un t-(v,k,λ) diseño, existe también el diseño s-derivado con parámetros $(t-s)$-$(v-s,k-s,\lambda)$, para todo $1 \leqslant s \leqslant t$.

En el mismo sentido se puede definir lo que llamaremos diseño *s-residual* de un t-diseño, $D=(V,B)$ respecto de un s-subcunjunto S de V, con $s \leqslant t$,

$$D^S = (V^S, B^S)$$

donde $V^S = V \setminus S$ y

$$B^S = \{B_i \in B : B_i \cap S = \emptyset\}$$

Es decir, un diseño s-residual es el que se obtiene de un t-diseño suprimiendo un subconjunto de cardinal inferior a t del conjunto de variedades V y como bloques se consideran los del diseño original que no contienen ningún elemento de este subconjunto.

Por ejemplo, los diseños s-residuales que se obtienen del diseño 3-$(8,4,1)$ descrito anteriormente suprimiendo del conjunto de variedades los subconjuntos $S=\{8\}$ y $S=\{7,8\}$ son respectivamente los que figuran a continuación:

$$\{1,2,3,5\},\ \{1,2,6,7\},\ \{1,3,4,6\},\ \{1,4,5,7\},\ \{2,3,4,7\},\ \{2,4,5,6\},\ \{3,5,6,7\}$$
$$\{1,2,3,5\},\ \{1,3,4,6\},\ \{2,4,5,6\}$$

Cabe observar que a diferencia de los diseños s-derivados, los diseños s-residuales tienen todos la misma uniformidad, es decir, los bloques que se obtienen son todos del mismo tamaño que los originales.

La proposición siguiente permite deducir que esta construcción proporciona efectivamente un nuevo t-diseño.

Proposición 12.9. El número de bloques de un t-(v,k,λ_t) diseño que no contienen ninguna variedad de un determinado s-subconjunto $S \subset V$, con $s \leqslant t$, es

$$\lambda^s = \lambda_t \frac{\binom{v-s}{k}}{\binom{v-t}{k-t}}$$

Teorema 12.10. Si existe un t-(v,k,λ) diseño, existe también el diseño s-residual con parámetros $(t-s)$-$(v-s,k,\mu)$, para todo $1 \leqslant s < t$.

Ejercicio 12.11. Demostrar el teorema 12.10 usando la proposición 12.9.

Se puede demostrar sin excesiva dificultad que el diseño complementario de un t-diseño es también un t-diseño. Al final de esta sección se deducirán los parámetros del complementario

de un 2-diseño. Usando el mismo tipo de razonamiento, se pueden deducir los parámetros del complementario de un t-diseño en general.

Desgraciadamente no existen resultados generales que faciliten la obtención de t-diseños. Un breve repaso histórico dará una idea de la dificultad del problema y de su estado actual.

Es preciso mencionar que, para $t > 4$, se conocen muy pocos t-diseños. Por ejemplo, no fue hasta 1976 que se obtuvieron los primeros 5-diseños de parámetros

$$5\text{-}(12,6,1), \quad 5\text{-}(24,6,1), \quad 5\text{-}(28,6,1), \quad 5\text{-}(48,6,1), \quad 5\text{-}(84,6,1)$$

En 1978, W. Mills construyó un $5\text{-}(72,6,1)$ diseño y desde entonces hasta 1986, en que D. Kreher y S. Radziszowski encontraron el primer 6-diseño, $6\text{-}(14,7,4)$, no se obtuvo nada nuevo. De hecho, los especialistas en el tema conjeturaban la no existencia de tales diseños. Fue L. Teirlinck, en el año 1987, quien contradijo esta sospecha demostrando la existencia de un t-diseño para cualquier valor de t. Pero los diseños que se obtienen a partir de su demostración tienen unos parámetros extraordinariamente grandes y, por tanto, la obtención de ejemplos pequeños es aún un problema abierto.

Dentro de la clasificación general de los t-diseños hay, sin embargo, dos casos especialmente importantes de los cuales es más fácil obtener información. Éstos son, de hecho, los que dieron origen a esta teoría de diseños y que están relacionados, cronológicamente hablando, con problemas geométricos surgidos en el siglo pasado (J. Steiner, 1844) y con problemas estadísticos tratados en este siglo (R. A. Fisher, 1940):

1. Los llamados *sistemas de Steiner* son t-diseños en los cuales $\lambda = 1$ y se denotan habitualmente por

$$S(t,k,v)$$

2. Los llamados *BIBD* (abreviación de su denominación inglesa *Balanced Incomplete Block Design*) son 2-diseños, es decir, $t = 2$. En este caso se dice que λ es el parámetro que mide el equilibrio del diseño y el 2-diseño correspondiente se llama *equilibrado* y se denota normalmente por

$$(v,b,r,k,\lambda)\text{-BIBD}$$

¿Existen diseños para cualquier valor de estos parámetros? La respuesta a esta cuestión no es hoy en día aún del todo satisfactoria, como veremos a continuación.

Sistemas de Steiner

Cualquier sistema de Steiner, además de las condiciones generales como t-diseño, cumple la condición adicional siguiente:

Teorema 12.12. En cualquier sistema de Steiner, $S(t,k,v)$, se cumple:

$$v \geqslant (t+1)(k-t+1)$$

Demostración. Sea (V,B) un $S(t,v,k)$ diseño. En primer lugar, observemos que en cualquier sistema de Steiner dos bloques diferentes tienen como máximo $(t-1)$ variedades en común.

Observemos también que debe existir algún $(t+1)$-subconjunto que no esté en ningún bloque. Sea X alguno de estos $(t+1)$-subconjuntos.

Para cada uno de los $(t+1)$ t-subconjuntos $T \subset X$ de V, existe un único bloque, $B_T \in B$, que contiene T. Cada uno de estos B_T bloques contiene $k-t$ variedades que no son de X y cada variedad de $V \setminus X$ está contenida como máximo en uno de estos B_T bloques, ya que estos B_T bloques tienen siempre $t-1$ variedades de X en común.

Deducimos, por tanto, que la unión de todos estos B_T bloques contiene

$$v \geqslant |\cup B_T| = |X| + \sum_{T \subset X} |B_T \setminus X| = (t+1) + (t+1)(k-t)$$

variedades, como queríamos demostrar. □

Como consecuencia de este teorema podemos deducir, por ejemplo, la no existencia del 10-diseño que hemos mencionado anteriormente, $S(10,16,72)$, ya que $72 < 11 \cdot 7$.

Los sistemas de Steiner más conocidos y más sencillos son los llamados *sistemas triples de Steiner* constituidos por bloques de tamaño tres, es decir, $S(2,3,v)$ y que habitualmente se denotan por

$$\mathrm{STS}(v)$$

Como ejemplo consideremos $\mathrm{STS}(9)$, que tiene por bloques los que figuran a continuación:

$$\begin{array}{ll} \{1,2,3\} & \{2,4,8\} \\ \{1,4,7\} & \{2,5,9\} \\ \{1,5,8\} & \{2,6,7\} \\ \{1,6,9\} & \{3,4,9\} \\ \{4,5,6\} & \{3,5,7\} \\ \{7,8,9\} & \{3,6,8\} \end{array}$$

Como consecuencia del teorema 12.5, el número de *triplos* (bloques) de un sistema triple de Steiner es $b = v(v-1)/6$ y ésta es por tanto una condición sencilla para deducir la no existencia de un $\mathrm{S}(2,3,v)$. Por ejemplo, no existe ningún $\mathrm{S}(2,3,8)$. Esta expresión nos permite deducir también que el sistema triple de Steiner más pequeño es el $\mathrm{STS}(7)$ descrito a continuación:

$$\begin{array}{ll} \{1,2,4\} & \{2,3,5\} \\ \{1,3,7\} & \{2,6,7\} \\ \{1,5,6\} & \{3,4,6\} \\ & \{4,5,7\} \end{array}$$

Proposición 12.13. El número de bloques en un sistema triple de Steiner, STS(v) es

$$b = v(v-1)/6$$

Ejercicio 12.14. Demostrar que no existe ningún STS(v) para valores de $v = 4, 5, 6$.

Los 2-sistemas de Steiner son un caso particular de BIBD y los trataremos en el apartado siguiente. Un ejemplo de 3-sistema de Steiner está descrito en 12.1. Los sistemes de Steiner más interesantes son los que corresponden a valores de $t > 3$ y son también los de más difícil obtención. Por ejemplo, para $t \geqslant 4$, únicamente se conocen las contracciones de los 5-diseños mencionados anteriormente (12.1):

$$\mathrm{S}(4,5,11), \quad \mathrm{S}(4,5,23), \quad \mathrm{S}(4,5,27), \quad \mathrm{S}(4,5,47), \quad \mathrm{S}(4,5,83)$$

BIBD

Si centramos ahora la atención en los 2-diseños (BIBD), el problema en general de su obtención es también un problema abierto, pero en este caso hay más resultados parciales y de más fácil tratamiento, como veremos a continuación.

En primer lugar sabemos que en cualquier 2-(v,k,λ) diseño se cumple:

1. $bk = vr$
2. $r(k-1) = \lambda(v-1)$

La primera de estas condiciones es consecuencia de la regularidad del diseño y la segunda se obtiene del teorema 12.6 tomando $s = 1$.

Estas condiciones necesarias, sin embargo, sabemos también que no son suficientes. En particular, no existe ningún $(43,7,1)$-BIBD.

El siguiente teorema, conocido como *desigualdad de Fisher*, proporciona una condición muy sencilla para la no existencia de BIBD. Este resultado se obtiene teniendo en cuenta el comportamiento de las matrices de incidencia de estos diseños.

Proposición 12.15. Si A es la matriz de incidencia de un (v,b,r,k,λ)-BIBD, entonces

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

Demostración.

$$AA^T = (c_{ij})_{v\times v}, \qquad \begin{cases} c_{ii} &= \sum_{h=1}^{b} a_{ih}^2 = \sum_{h=1}^{b} a_{ih} = r \\ c_{ij} &= \sum_{h=1}^{b} a_{ih}a_{jh} = \lambda \end{cases}$$

Observar que los elementos de la diagonal de AA^T son todos iguales a r como consecuencia de la regularidad del diseño, y el resto son todos iguales a λ como consecuencia de su equilibrio. Así,

$$AA^T = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & & \cdots & r \end{pmatrix}$$

□

Teorema 12.16. El número b de bloques de un (v,b,r,k,λ)-BIBD es como mínimo igual al número v de variedades:

$$b \geqslant v$$

Demostración. Calculamos de forma inmediata el determinante de AA^T, restando la primera fila de las otras filas y sumando a la primera columna la suma del resto de columnas, para obtener

$$|AA^T| = \begin{vmatrix} (r+(v-1)\lambda) & \lambda & \cdots & \lambda \\ 0 & (r-\lambda) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (r-\lambda) \end{vmatrix}, \quad |AA^T| = (r+(v-1)\lambda)(r-\lambda)^{v-1}$$

Usando la condición que proporciona el equilibrio del diseño y teniendo en cuenta que $r > \lambda$, deducimos que

$$|AA^T| = (r+(k-1)r)(r-\lambda)^{v-1} = rk(r-\lambda)^{v-1} \neq 0$$

Finalmente, se obtiene el resultado teniendo en cuenta que

$$v = rang(AA^T) \leqslant rangA \leqslant \min(v,b)$$

□

Si se considera el caso límite de la desigualdad de Fisher, es decir, igual número de bloques que de variedades, se obtienen los llamados *diseños simétricos*, que se denotan habitualmente por

$$(v,k,\lambda)\text{-SD}$$

De la igualdad $bk = vr$, deducimos que en un diseño simétrico, $k = r$.

El ejemplo más pequeño y también más conocido de diseño simétrico es el $(7,3,1)$-SD, que ya hemos considerado anteriormente como sistema triple de Steiner y que trataremos de nuevo en la sección siguiente como ejemplo importante de geometría finita.

La simetría de los diseños es una característica que se pierde con facilidad cuando se manipulan estos diseños para obtener otros. Por ejemplo, el dual de un diseño simétrico no siempre es simétrico.

Ejercicio 12.17. Buscar un ejemplo de un diseño simétrico tal que su dual no lo sea.

Es fácil comprobar, sin embargo, que el diseño complementario de un diseño simétrico es también simétrico.

Proposición 12.18. El diseño complementario de un diseño simétrico (v,k,λ)-SD es también un diseño simétrico de parámetros $(v, v-k, b-2r+\lambda)$-SD, si $b-2r+\lambda > 0$.

Demostración. Sea $D = (V,B)$ un diseño simétrico de parámetros (v,k,λ)-SD. Es inmediato comprobar, a partir de la definición, que el diseño complementario $\bar{D} = (\bar{V},\bar{B})$ cumple $|\bar{V}| = v$, $|\bar{B}| = b = v$ y que todo $\bar{B} \in \bar{B}$ tiene cardinal $|\bar{B}| = v-k$.

El parámetro de equilibrio de $\bar{D}$, $\bar{\lambda}$, se obtiene descontando del número de bloques b de B aquellos que contienen una determinada pareja $\{x,y\}$ de V, λ, y también aquellos bloques que sólo contienen alguno de los elementos x o y, r. Tenemos, por tanto:

$$\bar{\lambda} = b - 2(r-\lambda) - \lambda = b - 2r + \lambda$$

□

Como ejemplo, el diseño $(7,4,2)$-SD que figura a continuación es complementario del $(7,3,1)$-SD descrito anteriormente como sistema triple de Steiner.

$$\begin{array}{ll} \{3,5,6,7\} & \{1,4,6,7\} \\ \{2,4,5,6\} & \{1,3,4,5\} \\ \{2,3,4,7\} & \{1,2,5,7\} \\ & \{1,2,3,6\} \end{array}$$

Se pueden obtener 2-diseños de dos maneras especiales a partir de diseños simétricos, considerando en los dos casos como punto de referencia un bloque del diseño original. Estas construcciones aparecen como generalizaciones de ciertas construcciones geométricas que veremos en la próxima sección. La denominación de estas construcciones puede llevar a confusión, ya que son similares a otras introducidas por t-diseños.

Dado un diseño simétrico $D = (V, B)$, se define el diseño *derivado* de D respecto de un bloque $B \in B$,

$$D_B = (V_B, B_B)$$

como el diseño que tiene por conjunto de variedades el propio B, $V_B = B$ y como conjunto de bloques el que se obtiene de intersectar todos los otros bloques de B con el propio B:

$$B_B = \{B_i \cap B,\ B_i \in B \setminus B\}$$

Si consideramos el diseño $(15, 7, 3)$-SD, con conjunto de bloques

$$\begin{array}{lcllcl}
B_1 & = & \{1,2,3,4,5,6,7\} & B_8 & = & \{2,4,6,8,10,12,14\} \\
B_2 & = & \{1,2,3,8,9,10,11\} & B_9 & = & \{2,4,6,9,11,13,15\} \\
B_3 & = & \{1,2,3,12,13,14,15\} & B_{10} & = & \{2,5,7,8,10,13,15\} \\
B_4 & = & \{1,4,5,8,9,12,13\} & B_{11} & = & \{2,5,7,9,11,12,14\} \\
B_5 & = & \{1,4,5,10,11,14,15\} & B_{12} & = & \{3,4,7,8,11,12,15\} \\
B_6 & = & \{1,6,7,8,9,14,15\} & B_{13} & = & \{3,4,7,9,10,13,14\} \\
B_7 & = & \{1,6,7,10,11,12,13\} & B_{14} & = & \{3,5,6,8,11,13,14\} \\
 & & & B_{15} & = & \{3,5,6,9,10,12,15\}
\end{array}$$

su diseño derivado respecto el bloque B_1 es el diseño que tiene como conjunto de variedades $V_B = B_1 = \{1,2,3,4,5,6,7\}$ y tiene por bloques

$$\begin{array}{lcllcl}
B_1 & = & \{1,2,3\} & B_8 & = & \{2,4,6\} \\
B_2 & = & \{1,2,3\} & B_9 & = & \{2,5,7\} \\
B_3 & = & \{1,4,5\} & B_{10} & = & \{2,5,7\} \\
B_4 & = & \{1,4,5\} & B_{11} & = & \{3,4,7\} \\
B_5 & = & \{1,6,7\} & B_{12} & = & \{3,4,7\} \\
B_6 & = & \{1,6,7\} & B_{13} & = & \{3,5,6\} \\
B_7 & = & \{2,4,6\} & B_{14} & = & \{3,5,6\}
\end{array}$$

Comprobar que identificando los bloques iguales el diseño que se obtiene es isomorfo al diseño simétrico $(7, 3, 1)$-SD.

Se define también el *residual* de D respecto de un bloque $B \in B$,

$$D^B = (V^B, B^B)$$

como el diseño que tiene por conjunto de variedades el que se obtiene suprimiendo B de V, $V^B = V \setminus B$ y como conjunto de bloques el que se obtiene suprimiendo los elementos de B de todos los otros bloques:

$$B^B = \{B_i \setminus B,\ B_i \in B \setminus B\}$$

Como ejemplo, consideremos el diseño residual del diseño $(7,3,1)$-SD respecto del bloque $B = \{3,4,6\}$. Así tenemos $V^B = \{1,2,5,7\}$ y como conjunto de bloques se obtiene

$$B^B = \{\{1,2\},\{2,5\},\{5,7\},\{5,1\},\{7,2\},\{7,1\}\}$$

Se puede comprobar sin dificultad que en los dos casos se obtienen BIBD con los parámetros que figuran a continuación:

Proposición 12.19. Dado un diseño simétrico de parámetros (v,k,λ)-SD, su diseño derivado tiene parámetros $(k, v-1, k-1, \lambda, \lambda-1)$-BIBD.

Proposición 12.20. Dado un diseño simétrico de parámetros (v,k,λ)-SD, su diseño residual tiene parámetros $(v-k, v-1, k, k-\lambda, \lambda)$-BIBD.

Los diseños simétricos constituyen la clase más estudiada de diseños. En particular cumplen una condición muy simple respecto de lo que se llama *orden* del diseño, que se define como $k-\lambda$. Esta condición fue obtenida por Bruch, Ryser y Chowla en 1950 y se conoce directamente como la condición BRC.

Teorema 12.21. Si el número v de variedades de un (v,k,λ)-SD es par, entonces el orden del diseño, $k-\lambda$, es un cuadrado.

Demostración. La matriz de incidencia del diseño (v,k,λ)-SD es cuadrada y entonces

$$|AA^T| = |A|^2 = (r+(v-1)\lambda)(r-\lambda)^{v-1} = k^2(k-\lambda)^{v-1}$$

por tanto, $(k-\lambda)^{v-1}$ debe ser un cuadrado. Si v es par, entonces $k-\lambda$ es un cuadrado. □

Los mismos autores obtuvieron también una condición necesaria para la existencia de un diseño simétrico con un número impar de variedades. La demostración en este caso es más complicada y usa resultados de teoría de números que no tienen cabida en este libro.

Teorema 12.22. Si el número v de variedades de un (v,k,λ)-SD es impar, entonces existen tres números enteros x,y,z tales que

$$z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$$

No se conoce ningún conjunto de parámetros que cumpla las condiciones de los teoremas 12.21 o 12.22 para el cual no exista el diseño simétrico correspondiente. Pero la suficiencia de este resultado es aún un problema abierto. Por ejemplo, no se ha podido determinar la existencia de un diseño de parámetros $(111,11,1)$-SD.

12.2 Geometrías finitas

Una *geometría finita* es un sistema particular de incidencia en el cual, a partir de una determinada axiomática, se define una cierta familia de subconjuntos de un conjunto finito de elementos llamados puntos. En particular, una geometría finita es un diseño combinatorio en el que se consideran las variedades como puntos.

En función de la axiomática definida aparecen diferentes estructuras geométricas. Unas de las más sencillas son las llamadas *geometrías lineales finitas*, en las cuales la axiomática se refiere a propiedades que deben cumplir ciertos subconjuntos de puntos llamados líneas o rectas. Así, si $P = \{p_1, p_2, \ldots, p_v\}$ representa un conjunto de puntos, el conjunto de líneas será un determinado subconjunto de las partes de P, $L = \{l_1, l_2, \ldots, l_b\} \subset \mathcal{P}(P)$ y la correspondiente geometría se representa por

$$G = (P, L)$$

El número de puntos de una línea $l \in L$ lo notaremos por $|l| = |\{p \in P, p \in l\}|$. Como veremos a continuación, es útil considerar el conjunto de líneas que contienen un determinado punto p. Representamos este conjunto por $L_p = \{l \in L \mid p \in l\}$.

De hecho son las *geometrías casi-lineales* las que tienen la axiomática más simple:

QL0 Para todo $l \in L$, $|l| \geqslant 2$

QL1 Para todo $p, q \in P$, $|L_p \cap L_q| \leqslant 1$

El primero de estos axiomas no es propio de estas geometrías, sino que lo comparten todas las geometrías finitas no triviales. El segundo es por tanto el que las caracteriza y asegura que dos puntos cualesquiera están como máximo en una línea. Si imponemos que haya exactamente una línea que los contenga, obtenemos la axiomática propia de una *geometría lineal finita*:

L0 Para todo $l \in L$, $|l| \geqslant 2$

L1 Para todo $p, q \in P$, $|L_p \cap L_q| = 1$

Planos proyectivos

La geometría proyectiva tiene sus orígenes en el siglo IV (Pappus de Alejandría) pero no fue hasta el siglo XVI, mediante los pintores flamencos, que se le dio importancia, y aún se demoró tres siglos más para hacer sistemático y riguroso su estudio (Boole, Cayley, Sylvester, siglo XIX). La versión finita de las geometrías proyectivas tiene múltiples aplicaciones en combinatoria relacionadas con la construcción de ciertos diseños simétricos y también con la obtención de lo que se llaman *cuadrados latinos*, que estudiaremos en la próxima sección.

Añadiendo condiciones a las descritas anteriormente para geometrías lineales, se obtienen tipos especiales de geometrías lineales finitas. En particular si se considera que dos líneas diferentes siempre tienen un único punto en común, y que existen como mínimo cuatro puntos no colineales tres a tres (esto, como veremos, evita casos triviales), se obtiene lo que se llama *plano proyectivo finito*. Así, un plano proyectivo es una geometría lineal finita que cumple los axiomas siguientes:

P0 Para todo $l \in L$, $|l| \geqslant 2$

P1 Para todo $p, q \in P$, $|L_p \cap L_q| = 1$

P2 Para todo $l, l' \in L$, $|l \cap l'| = 1$

P3 Existen $p, q, s, t \in P$, no colineales tres a tres

Observar que en un plano proyectivo todas las rectas se cortan, de manera que no se satisface el axioma de Euclides, que afirma que por un punto exterior a una recta pasa una única paralela.

El plano proyectivo más pequeño es el plano de Fano que aparece en la figura 12.1.

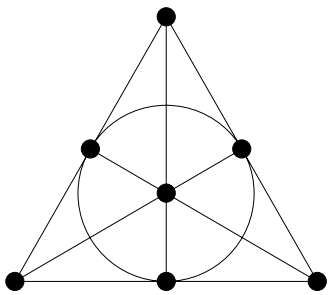


Figura 12.1: Plano de Fano

¿Existen planos proyectivos con cualquier número de puntos? Comprobaremos que la respuesta a esta pregunta es negativa si descartamos los casos llamados *degenerados* que se muestran en la figura 12.2.

Ejercicio 12.23. Comprobar que no existe ningún plano proyectivo no degenerado de cuatro puntos.

Es preciso observar en primer lugar que el axioma **P3** se impone para eliminar los casos degenerados. Es preciso observar también que **P1** y **P2** son condiciones duales, es decir, que se obtienen una de la otra intercambiando puntos por líneas. En particular, también se verifica el dual de **P3**.

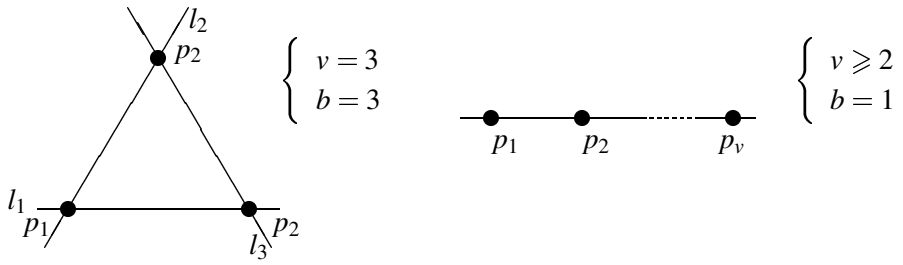


Figura 12.2: Planos proyectivos degenerados

Proposición 12.24. En un plano proyectivo hay al menos cuatro líneas tales que tres cualesquiera de ellas no contienen un mismo punto.

Demostración. Sean $p, q, r, s \in P$ cuatro puntos no colineales tres a tres. Entonces tres de las líneas $l_{pq}, l_{qr}, l_{ps}, l_{rs}$ no tienen ningún punto en común. Por ejemplo, si l_{pq}, l_{ps}, l_{rs} tuviesen un punto t en común, las líneas l_{pqt}, l_{pst} y l_{rst} coincidirían, ya que las dos primeras y las dos últimas tendrían dos puntos en común y psr serían colineales. □

Este resultado junto con los tres axiomas **P1**, **P2** y **P3** hacen que cualquier resultado sobre planos proyectivos tenga su dual (intercambiando puntos por líneas). Se dice por tanto que los planos proyectivos verifican lo que se llama *principio de dualidad*.

El comportamiento regular de los planos proyectivos se evidencia mediante los siguientes resultados que ponen de manifiesto al mismo tiempo este principio de dualidad.

Teorema 12.25. En un plano proyectivo, todas las líneas contienen el mismo número de puntos y cada punto pertenece al mismo número de líneas.

Demostración. Para demostrar que cada línea contiene el mismo número de puntos, establecemos una biyección entre los puntos de dos líneas diferentes l y l'. Para ello, consideremos $x \in P$ tal que no sea un punto de $l \cup l'$.

La *proyección* sobre l' de cada punto $p \in l$ respecto al punto x es el punto $p' \in l'$ que se obtiene como intersección de la línea l_{xp} con l':

$$p' = l' \cap l_{xp}$$

tal como se puede ver en la figura 12.3.

Observar que si $p, q \in l$, $p \neq q$, entonces $p' \neq q'$ (axioma **P2**). Por tanto, la proyección es una biyección.

Por el principio de dualidad, también es cierto que cada punto pertenece al mismo número de líneas. □

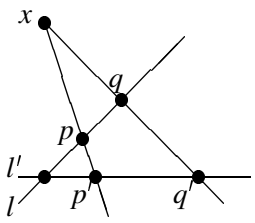


Figura 12.3: Proyección respecto a x

Teorema 12.26. En un plano proyectivo, el número de puntos que contiene cada línea es igual al número de líneas que pasan por cada punto.

Demostración. Sea (P,L) un plano proyectivo. Consideremos $l \in L$ y $x \in P \setminus l$. Entonces la aplicación que a cada punto $p \in l$ le asigna la línea l_{px} es una biyección entre el conjunto de puntos de l y el conjunto de líneas que pasa por x. □

Teorema 12.27. Un plano proyectivo con $m+1$ puntos en cada línea tiene m^2+m+1 puntos.

Demostración. Si v es el número de puntos de un plano proyectivo, entonces

$$v = (m+1)m+1$$

donde $(m+1)$ es $|L_p|$, es decir, el número de líneas que contienen un determinado punto $p \in P$, y m es $|l|-1$, $l \in L_p$.

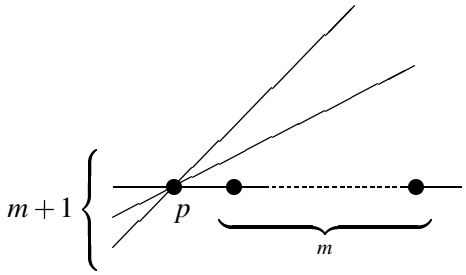


Figura 12.4: Número de puntos de un plano proyectivo

Observemos que éstos son efectivamente todos los puntos del plano, ya que, si existiese algún punto q que no fuese de L_p, también tendría que existir (axioma **P1**) la línea $l_{pq} \in L_p$ que lo une a p. □

El principio de dualidad nos garantiza que el número de líneas de un plano proyectivo es el mismo que el número de puntos, es decir, m^2+m+1.

En particular, no existen planos proyectivos con 5 o 6 puntos. Observar también que para $m = 1$, el plano que se obtiene es degenerado. Por tanto, tal como se ha comentado anteriormente, el plano proyectivo más pequeño es el plano de Fano con $m = 2$. Para $m = 3$ se obtiene un plano proyectivo con 13 puntos, que está representado en la figura 12.5.

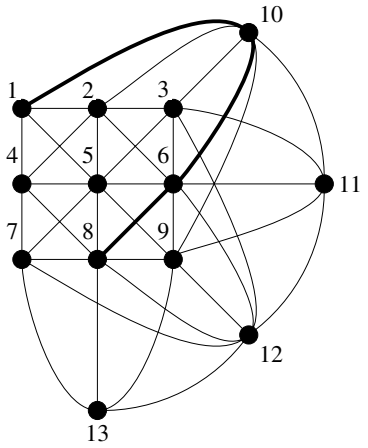


Figura 12.5: Plano proyectivo de 13 puntos

Al número m se le dice *orden* del plano proyectivo. Un plano proyectivo de orden m se denota habitualmente por

$$PG(2,m)$$

De momento sabemos que cualquier plano proyectivo debe tener m^2+m+1 puntos; sin embargo, ¿existe un plano proyectivo para cualquier valor de m? Podemos obtener la respuesta identificando los planos proyectivos con unos ciertos diseños simétricos. Si se consideran los puntos de $PG(2,m)$ como variedades y las líneas como bloques, se obtiene un 2-diseño simétrico con los parámetros que figuran a continuación:

$$\begin{array}{rcl} (V,B) & \leftrightarrow & (P,L) \\ (m^2+m+1,m+1,1)\text{-SD} & \leftrightarrow & PG(2,m) \\ v=b & \leftrightarrow & m^2+m+1 \\ k=r & \leftrightarrow & m+1 \\ \lambda & \leftrightarrow & 1 \end{array}$$

Se puede observar como consecuencia del axioma **P1** que $\lambda = 1$, y se puede comprobar también que se cumplen las condiciones de regularidad de todo diseño simétrico. Por ejemplo,

el plano proyectivo de la figura 12.5 corresponde al diseño $(13,4,1)$-SD, cuyos bloques figuran a continuación:

$$\begin{array}{lcllcl} B_1 & = & \{1,2,3,11\} & B_8 & = & \{3,5,7,10\} \\ B_2 & = & \{1,4,7,13\} & B_9 & = & \{3,6,9,13\} \\ B_3 & = & \{1,5,9,12\} & B_{10} & = & \{3,12,8,4\} \\ B_4 & = & \{1,10,6,8\} & B_{11} & = & \{4,5,6,11\} \\ B_5 & = & \{2,6,12,7\} & B_{12} & = & \{7,8,9,11\} \\ B_6 & = & \{2,4,10,9\} & B_{13} & = & \{10,11,12,13\} \\ B_7 & = & \{2,5,8,13\} & & & \end{array}$$

Está claro, por tanto, que todo plano proyectivo es una representación geométrica de un determinado diseño simétrico. En sentido contrario también es cierto, es decir, cualquier $(m^2+m+1,m+1,1)$-SD cumple los axiomas de plano proyectivo, como veremos a continuación:

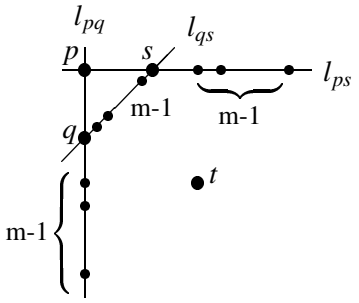
Teorema 12.28. $PG(2,m)$ existe si y sólo si existe el diseño simétrico

$$(m^2+m+1,m+1,1)\text{-SD}$$

Demostración. Es suficiente demostrar que los axiomas de los planos proyectivos se cumplen en el diseño $(m^2+m+1,m+1,1)$-SD para todo $m \geqslant 2$.

Los dos primeros axiomas se deducen directamente a partir de la propia definición de los parámetros k y λ, y **P2** se cumple como consecuencia de la simetría del diseño, que en términos geométricos equivale a la dualidad de **P1**.

Para demostrar que también se cumple el axioma **P3**, será preciso encontrar cuatro puntos no colineales tres a tres. Para ello, consideremos la única línea ($\lambda = 1$) que contiene dos puntos cualesquiera $p,q \in P$, $l_{pq} \in L$. Como el diseño es incompleto, existe $s \in P \setminus l_{pq}$ y por tanto



podemos considerar las líneas que unen el punto s con los puntos p y q, l_{sp} y l_{sq} (observar que

son únicas, ver la figura 12.2). Entonces,

$$|l_{pq} \cup l_{sp} \cup l_{sq}| = 3(m-1)+3 = 3m < m^2+m+1$$

De donde deducimos que

$$\exists t \in P \setminus l_{pq} \cup l_{sp} \cup l_{sq}$$

□

El resultado siguiente nos proporciona condiciones sencillas para determinar la no existencia de planos proyectivos para determinados órdenes.

Teorema 12.29. Si existe un diseño $(m^2+m+1, m+1, 1)$-SD con $m \equiv 1,2 \pmod 4$, entonces existe $a, b \in \mathbb{Z}$ tal que $m = a^2+b^2$.

En particular, no existen planos proyectivos de orden 6, 14, 21, 22, ... La demostración de este resultado es consecuencia del teorema 12.22 para diseños simétricos en general. Esquemáticamente,

$$v-1 = m(m+1) \equiv 0 \pmod 2$$

de donde, claramente, v es impar para todo valor de m, y el teorema 12.22 asegura en este caso la existencia de una terna de números enteros $(x,y,z) \in (\mathbb{Z}^3)^*$ tal que

$$z^2 = \underbrace{(k-\lambda)}_{m} x^2 + (-1)^{(v-1)/2} \underbrace{\lambda}_{1} y^2$$

Si $m \equiv 1,2 \pmod 4$, se obtiene que $z^2+y^2 = mx^2$ y un resultado de teoría de números asegura que, en este caso, existe $a, b \in \mathbb{Z}$ tal que $m = a^2+b^2$.

Es preciso mencionar, sin embargo, que este teorema no proporciona condiciones suficientes para la existencia de planos proyectivos de estos órdenes. Por ejemplo, se ha mencionado ya la falta de información sobre la existencia de un diseño de parámetros $(111, 11, 1)$-SD, que evidentemente cumple las condiciones del teorema. Por tanto, la existencia del plano proyectivo de orden 10, $PG(2,10)$, es un problema por resolver.

Si $m \equiv 0,3 \pmod 4$, del mismo teorema 12.22 se obtiene que $z^2-y^2 = mx^2$ y por ejemplo los puntos $(1,(m-1)/2,(m+1)/2)$ y $(1,(m-4)/4,(m+4)/4)$ son soluciones de esta ecuación, con lo que no se puede concluir nada sobre la existencia o no de un plano proyectivo con estos órdenes.

En cuanto a resultados concretos de existencia de planos proyectivos, al final de la sección dedicada a cuadrados latinos se verá un procedimiento constructivo que asegura la existencia de $P(2,m)$ cuando m es una potencia de un número primo. Esta construcción está basada en los cuerpos de Galois.

Planos afines

La geometría afín está intrínsecamente relacionada con la geometría proyectiva, aunque, de hecho, la geometría afín sigue los postulados de la geometría euclídea, mientras que en la geometría proyectiva, como ya hemos visto, no es así. La relación que hay entre las dos se pondrá de manifiesto, como veremos, a través del diseño residual del diseño simétrico asociado a un plano proyectivo.

Se dice que una geometría finita $G = (P,L)$ es un *plano afín* si cumple las condiciones siguientes:

A0 Para todo $l \in L$, $|l| \geqslant 2$

A1 Para todo $p,q \in P$, $|L_p \cap L_q| = 1$

A2 Para todo $l \in L$, y para todo $p \in P \setminus l$, existe una única línea $l' \in L_p$ tal que $|l \cap l'| = 0$

A3 Existen $p,q,s \in P$, no colineales

Los axiomas de planos afines y planos proyectivos difieren sólo en los dos últimos y, de hecho, la diferencia substancial es entre los axiomas **P2** y **A2**. Cabe observar que son los axiomas **P2** y **A2** los que contraponen estas geometrías lineales respecto de la geometría euclídea.

Denotamos por $G^{l^*} = G^* = (P^*, L^*)$ el diseño residual que se obtiene suprimiendo una línea $l^* \in L$ y sus puntos del diseño $G = (P,L) = (m^2+m+1, m+1, 1)$-SD. Demostraremos que este diseño residual es un plano afín. En primer lugar, los parámetros del diseño que se obtiene son los siguientes:

$$\begin{array}{rcl} G = (P,L) & \leftrightarrow & G^* = (P^*, L^*) \\ (m^2+m+1, m+1, 1)\text{-SD} & \leftrightarrow & (m^2, m^2+m, m, m+1, 1)\text{-BIBD} \end{array}$$

$$\begin{array}{rcl} |P| = m^2+m+1 & \leftrightarrow & |P^*| = m^2 \\ |L| = m^2+m+1 & \leftrightarrow & |L^*| = m^2+m \\ |l| = m+1 & \leftrightarrow & |l| = m \\ |L_p| = m+1 & \leftrightarrow & |{L^*}_p| = m+1 \\ |L_p \cap L_q| = 1 & \leftrightarrow & |{L^*}_p \cap {L^*}_q| = 1 \end{array}$$

Ejercicio 12.30. Comprobar que los parámetros del diseño residual de un plano proyectivo $PG(2,m)$ son efectivamente los que se han descrito.

Teorema 12.31. El diseño residual de un plano proyectivo es un plano afín.

Demostración. Comprobemos que $G^* = (P^*, L^*)$ cumple los axiomas de plano afín. Los dos primeros se deducen directamente a partir de la definición de diseño residual.

A0 Para todo $l \in L^*$, $|l| = m \geqslant 2$

A1 Para todo $p, q \in P^*$, $|L_p^* \cap L_q^*| = 1$

A2 Para que se cumpla este axioma es preciso comprobar que para todo $l \in L^*$, y para todo $p \in P^* \setminus l$, existe una única línea $l_p \in L_p^*$ tal que $|l \cap l_p| = 0$.

Para ello, consideremos la única línea $l_{pp^*} \in L$, donde p^* es el punto $l^* \cap l$ (véase la figura 12.6). Como $l \cap l_{pp^*} = p^*$ en G, entonces, $l \cap l_{pp^*} = \emptyset$ en G^*.

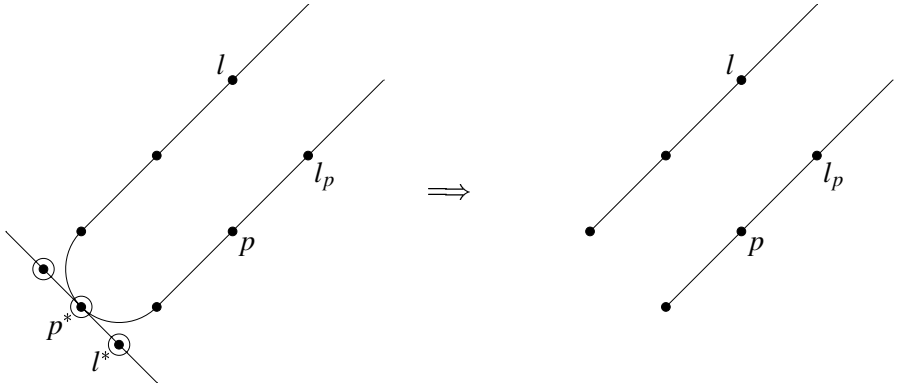


Figura 12.6: Obtención de un plano afín a partir del plano proyectivo

A3 este axioma es consecuencia directa de **P3**, teniendo en cuenta que suprimiendo una línea en un plano proyectivo siempre quedan como mínimo tres puntos no colineales.

□

Denotamos por $AG(2,m)$ el plano afín de orden m, es decir, el plano afín que tiene m puntos en cada línea.

Podemos invertir el proceso que hemos seguido para obtener un plano afín a partir de un plano proyectivo, añadiendo al plano afín la línea l^*, formada por los puntos correspondientes a las intersecciones entre líneas que no tienen intersección en $AG(2,m)$. Así,

$$G = G^* \cup l^*$$

En la figura 12.7 hay representado el plano afín de orden dos y el correspondiente plano proyectivo.

Ejercicio 12.32. Comprobar que efectivamente $PG(2,m) = AG(2,m) \cup l^*$.

Teorema 12.33. $AG(2,m)$ existe si y sólo si existe $PG(2,m)$.

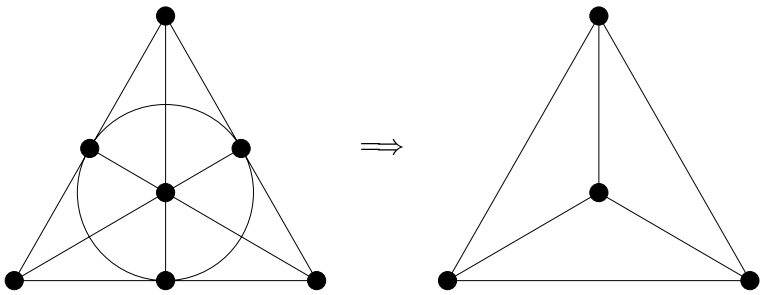


Figura 12.7: $AG(2,2)$ y $PG(2,2)$

12.3 Cuadrados latinos

Un *cuadrado latino* de orden n es una matriz de orden $n \times n$ cuyos términos son elementos de un conjunto cualquiera S de tamaño n, de manera que cada fila y cada columna contenga todos los elementos de S.

Por ejemplo, la matriz

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

es un cuadrado latino de orden 3.

Está claro que cada fila y cada columna de un cuadrado latino es una permutación de los elementos de S. También está claro que un cuadrado latino es un diseño completo simétrico con n bloques repetidos, cada uno de ellos igual a S.

Es fácil ver que existen cuadrados latinos de cualquier orden. Sólo es preciso identificar S con un grupo G del mismo orden y considerar como cuadrado latino Q, la tabla de su operación, de manera que a $q_{ij} \in Q$ le corresponda $g_k \in G$ si y sólo si $g_k = g_i g_j$. Cabe observar que, de esta manera, ningún elemento se repite en ninguna fila ni en ninguna columna. Por ejemplo, los dos cuadrados latinos siguientes se corresponden con las tablas de los grupos $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ (en este último se identifica $(0,0)$ con 0, $(0,1)$ con 1, $(1,0)$ con 2 y $(1,1)$ con 3):

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{array} \qquad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array}$$

Dos cuadrados latinos de tamaño n son *equivalentes* si es posible deducir uno del otro mediante una permutación de los símbolos. Por ejemplo, los cuadrados que figuran a continuación

son equivalentes:

$$\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array} \qquad \begin{array}{cc} 2 & 1 \\ 1 & 2 \end{array}$$

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{array}$$

En general, las tablas de grupos no isomorfos proporcionan ejemplos de cuadrados latinos no equivalentes.

Como el nombre de los elementos de S es irrelevante, supondremos que $S = \{1, 2, \ldots, n\}$. Un cuadrado latino $Q = (q_{ij})$ de orden n se dice *normalizado* si los términos de la primera columna aparecen en el orden natural, es decir, para todo i, $q_{i1} = i$. Observemos que siempre podemos obtener cuadrados latinos normalizados permutando los nombres de los símbolos.

Un cuadrado latino $Q = (q_{ij})$ de orden n se llama *idempotente* si los términos de la diagonal aparecen en el orden natural, es decir, para todo i, $q_{ii} = i$.

Cuadrados latinos mutuamente ortogonales

El llamado *problema de los 36 oficiales* (L. Euler, 1782) dio origen a lo que se conoce hoy en día por *cuadrados latinos mutuamente ortogonales*.

El problema consistía en encontrar, dadas 6 graduaciones y 6 regimientos, una formación de 6×6 oficiales tal que en cada fila y en cada columna hubiese un oficial de cada regimiento y de cada graduación.

Una posible ordenación de los oficiales de manera que en cada fila y en cada columna haya sólo un oficial de cada graduación es la que figura a continuación:

$$\begin{array}{cccccc} G_1 & G_6 & G_2 & G_5 & G_3 & G_4 \\ G_4 & G_2 & G_6 & G_3 & G_1 & G_5 \\ G_2 & G_5 & G_3 & G_6 & G_4 & G_1 \\ G_5 & G_3 & G_1 & G_4 & G_6 & G_2 \\ G_6 & G_1 & G_4 & G_2 & G_5 & G_3 \\ G_3 & G_4 & G_5 & G_1 & G_2 & G_6 \end{array}$$

Una posible ordenación de los oficiales de manera que en cada fila y en cada columna haya sólo un oficial de cada regimento es la que figura a continuación:

$$\begin{array}{cccccc} R_1 & R_2 & R_3 & R_4 & R_5 & R_6 \\ R_3 & R_1 & R_2 & R_6 & R_4 & R_5 \\ R_2 & R_3 & R_1 & R_5 & R_6 & R_4 \\ R_4 & R_5 & R_6 & R_1 & R_2 & R_3 \\ R_6 & R_4 & R_5 & R_3 & R_1 & R_2 \\ R_5 & R_6 & R_4 & R_2 & R_3 & R_1 \end{array}$$

Es preciso observar que cada fila y cada columna de estas ordenaciones contiene todas las graduaciones (regimientos) o, equivalentemente, ninguna fila o columna contiene ninguna graduación (regimiento) más de una vez.

El problema tendrá solución si, superponiendo las dos ordenaciones, cada par (G_i, R_j) aparece en la formación una única vez. En este caso, esto no es así, como se puede observar en el cuadro siguiente:

$$\begin{array}{cccccc} 11 & 62 & 23 & 54 & 35 & 46 \\ 43 & 21 & 62 & 36 & 14 & 55 \\ 22 & 53 & 31 & 65 & 46 & 14 \\ 54 & 35 & 16 & 41 & 62 & 23 \\ 66 & 14 & 45 & 23 & 51 & 32 \\ 35 & 46 & 54 & 12 & 23 & 61 \end{array}$$

Por ejemplo, la pareja 62 aparece tres veces, mientras que las parejas 33 o 44, entre otras, no aparecen.

Euler usaba el alfabeto griego para denotar las graduaciones y el alfabeto romano para denotar los regimientos, y por ello denominaba greco-romanos a estos cuadrados. Esta es también la razón por la cual los cuadrados latinos se denominan de esta manera.

¿Es posible obtener alguna ordenación de manera que este problema tenga solución?

Euler conjeturó que si $n \equiv 2 \pmod 4$, entonces no existe ningún cuadrado greco-romano de orden n. En esta sección trabajaremos sobre esta conjetura.

El problema de los 36 oficiales es un problema que exige la existencia de dos cuadrados latinos tales que superponiéndolos aparezcan todas las posibles parejas o, de forma equivalente, no se repita ninguna. Para comenzar definiremos este concepto.

Dos cuadrados latinos $A = (a_{ij})$ y $B = (b_{ij})$ de tamaño n son *ortogonales* si los n^2 pares ordenados $(a_{ij}, b_{ij}) \in A \times B$ son todos diferentes. Lo denotaremos escribiendo

$$A \perp B \qquad (\text{o } B \perp A)$$

En primer lugar es preciso observar que no existen cuadrados latinos ortogonales de tamaño 2. Si tomamos $n = 3$, podemos considerar un ejemplo clásico introducido por Fisher (1926). De hecho, fue Fisher quien recuperó y utilizó de forma sistemática los cuadrados latinos para tratar esencialmente experimentos sobre agricultura. En su ejemplo se trataba de estudiar la incidencia conjunta de tres fertilizantes $\{f_1, f_2, f_3\}$ y tres insecticidas $\{i_1, i_2, i_3\}$ sobre un campo dividido en tres parcelas $\{P_1, P_2, P_3\}$, durante tres años consecutivos, $\{A_1, A_2, A_3\}$. Por ello, es preciso combinar en cada año y cada parcela una pareja formada por un fertilizante y un insecticida de manera que todas las parejas hayan sido probadas.

Las figuras 12.8 y 12.9 muestran que las dos condiciones son compatibles en el sentido de que es posible obtener todas las combinaciones, es decir, existen dos cuadrados latinos ortogonales de tamaño tres.

	A_1	A_2	A_3
P_1	f_1	f_2	f_3
P_2	f_2	f_3	f_1
P_3	f_3	f_1	f_2

	A_1	A_2	A_3
P_1	i_1	i_2	i_3
P_2	i_3	i_1	i_2
P_3	i_2	i_3	i_1

Figura 12.8: Cuadrados latinos de tamaño tres

	A_1	A_2	A_3
P_1	11	22	33
P_2	23	31	12
P_3	32	13	21

Figura 12.9: Cuadrados latinos ortogonales de tamaño tres

En la figura 12.10 hay un ejemplo de tres cuadrados latinos ortogonales dos a dos de orden 4. Desde el punto de vista del diseño de experimentos, se pueden interpretar como tres aspectos diferentes de un mismo fenómeno que se quieren contrastar dos a dos. Es inmediato comprobar que estos tres cuadrados son mutuamente ortogonales. Esto nos lleva a la definición siguiente.

Se dice que una familia $A_1, A_2, \ldots, A_k$ de cuadrados latinos del mismo orden constituye un conjunto de *MOLS* (*Mutually Orthogonal Latin Squares*) si $A_i \perp A_j$ para todo i, j, $i \neq j$.

Es natural plantearse la cuestión siguiente. ¿En qué condiciones existe una familia de MOLS? En esta sección trataremos este problema y daremos un método constructivo para encontrar familias de MOLS para ciertos valores de orden n.

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	3	4	2
2	4	3	1
3	1	2	4
4	2	1	3

1	4	2	3
2	3	1	4
3	2	4	1
4	1	3	2

Figura 12.10: Cuadrados latinos mutuamente ortogonales

Proposición 12.34. Si A y B son cuadrados latinos ortogonales, los correspondientes cuadrados normalizados también lo son.

Demostración. Sean $A = (a_{ij})$ y $B = (b_{ij})$ dos cuadrados latinos ortogonales. Si efectuamos las permutaciones σ_1 y σ_2 de $\{1,2,\ldots,n\}$ en A y B respectivamente, cada par (a_{ij}, b_{ij}) se transforma en $(\sigma_1(a_{ij}), \sigma_2(b_{ij}))$, de manera que continúa habiendo todos los pares y la condición de ortogonalidad se mantiene. Sólo es preciso entonces efectuar las permutaciones necesarias para normalizar cada uno de los cuadrados. □

Proposición 12.35. Si existe una familia de k MOLS de orden n, entonces $k \leqslant n-1$.

Demostración. Sea $A_1, A_2, \ldots, A_k$ una familia de MOLS normalizada de orden n. Si $A_p = (a_{ij}^p)$ y $A_q = (a_{ij}^q)$ son dos cuadrados cualesquiera de esta familia, sólo es preciso observar que

$$(a_{12}^p, a_{12}^q) \neq (i,i), \qquad 1 \leqslant i \leqslant n$$

ya que, si no, $(a_{12}^p, a_{12}^q) = (a_{1i}^p, a_{1i}^q)$, cosa que contradice la condición de ortogonalidad entre A_p y A_q. Por tanto,

$$a_{12}^1, a_{12}^2, \ldots, a_{12}^k$$

son todos diferentes y, consecuentemente, $k \leqslant n-1$. □

Un *conjunto completo de MOLS* de orden n es un conjunto de $n-1$ MOLS de orden n.

Si $N(n)$ representa el número máximo de MOLS de orden n, sabemos que $N(2) = 1$, $N(3) = 2$ y $N(4) = 3$.

¿Para qué valores de n, $N(n) = n-1$? Es decir, ¿para qué valores de n existe un conjunto completo de MOLS de orden n?

El teorema siguiente, debido a Bose (1938), garantiza la existencia de un conjunto completo de MOLS para cualquier potencia de un número primo. La demostración es constructiva y consiste esencialmente en identificar el conjunto de variedades con los elementos de un cuerpo del mismo orden.

Teorema 12.36. Si p es un número primo, $N(p^k) = p^k - 1$, para todo $k \in \mathbb{N}$.

Demostración. Identifiquemos el conjunto de $p^k = n$ variedades con el cuerpo de Galois del mismo orden.

$$V \leftrightarrow GF(n) = \{f_0 = 0, f_1 = 1, f_2, \ldots, f_{n-1}\}$$

donde $f_i = \alpha^{i-1}$, $2 \leqslant i \leqslant n-1$, siendo α un elemento primitivo del cuerpo.

A partir de los elementos del cuerpo definimos la familia siguiente de matrices:

$$\begin{array}{rcll} A_l & = & (a^l_{ij}) & 1 \leqslant l < n-1 \\ a^l_{ij} & = & f_l f_j + f_i & 0 \leqslant i, j \leqslant n-1 \end{array}$$

(aquí los índices van de 0 a $n-1$ en lugar de ir de 1 a n como es habitual). En primer lugar, demostraremos que estas matrices son cuadrados latinos. Para ello, comprobemos que los elementos de cada fila y de cada columna son todos diferentes. Si $a^l_{ij} = a^l_{ik}$, entonces $f_l f_j + f_i = f_l f_k + f_i$ y, como $f_l \neq 0$, deducimos que $f_j = f_k$ y por tanto $j = k$. Razonando de forma similar, se demuestra que los elementos de cualquier columna son todos diferentes.

Demostraremos ahora que la familia de matrices definida constituye un conjunto completo de MOLS. Para ello es preciso demostrar que cualquier par de estas matrices son ortogonales. Supongamos que no lo son. Entonces, existen dos pares iguales ocupando posiciones diferentes, es decir,

$$(a^l_{ij}, a^m_{ij}) = (a^l_{hk}, a^m_{hk})$$

de donde

$$\left\{ \begin{array}{rcl} f_l f_j + f_i & = & f_l f_k + f_h \\ f_m f_j + f_i & = & f_m f_k + f_h \end{array} \right.$$

Restando estas dos igualdades deducimos que $f_j = f_k$ y, por tanto, $j = k$ e $i = h$. □

Como ejemplo de aplicación del teorema anterior, veamos cómo se construyen conjuntos completos de MOLS de órdenes tres y cuatro. Para los de orden tres, consideramos $GF(3) = (\mathbb{Z}_3, +, \cdot)$ y obtenemos los dos cuadrados ortogonales a partir de las igualdades:

$$\begin{array}{rclrcl} a^1_{0j} & = & j & a^2_{0j} & = & 2j \\ a^1_{1j} & = & j+1 & a^2_{1j} & = & 2j+1 \\ a^1_{2j} & = & j+2 & a^2_{2j} & = & 2j+2 \end{array}$$

de donde

$$A_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

Para los de orden cuatro, consideremos $GF(4) = (\mathbb{Z}_2[x]/(x^2+x+1), +, \cdot)$, donde

$$\mathbb{Z}_2[x]/(x^2+x+1) = \{f_0 = 0,\ f_1 = 1,\ f_2 = x,\ f_3 = x+1\}$$

En este caso, los cuadrados ortogonales se obtienen a partir de las igualdades siguientes:

$$\begin{array}{lll} a^1_{0j} = f_j & a^2_{0j} = f_2 f_j & a^3_{0j} = f_3 f_j \\ a^1_{1j} = f_j + 1 & a^2_{1j} = f_2 f_j + 1 & a^3_{1j} = f_3 f_j + 1 \\ a^1_{2j} = f_j + f_2 & a^2_{2j} = f_2 f_j + f_2 & a^3_{2j} = f_3 f_j + f_2 \\ a^1_{3j} = f_j + f_3 & a^2_{3j} = f_2 f_j + f_3 & a^3_{3j} = f_3 f_j + f_3 \end{array}$$

$$A_1 = \begin{pmatrix} 0 & 1 & x & x+1 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & x & x+1 & 1 \\ 1 & x+1 & x & 0 \\ x & 0 & 1 & x+1 \\ x+1 & 1 & 0 & x \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0 & x+1 & 1 & x \\ 1 & x & 0 & x+1 \\ x & 1 & x+1 & 0 \\ x+1 & 0 & x & 1 \end{pmatrix}$$

Para simplificar la notación, podemos expresar las anteriores matrices identificando $f_2 = x$ con 2 y $f_3 = x+1$ con 3, y obtener

$$A_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix} \qquad A_3 = \begin{pmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \end{pmatrix}$$

Realmente no es necesario hacer todos estos cálculos. Los conjuntos completos de MOLS que proporciona el teorema 12.36 siguen un comportamiento general sencillo que explicitamos a continuación:

Método constructivo de un conjunto completo de $n-1$ MOLS para $n = p^k$, p primo.

1. A_1 es la tabla del grupo aditivo $(GF(n), +)$, ya que $f_1 = 1$ y, por tanto, $a^1_{ij} = f_j + f_i$
2. Todos los cuadrados tienen la primera columna igual, ya que $f_0 = 0$ y, por tanto, $a^l_{i0} = f_i$

3. Las columnas restantes de cada A_i se obtienen haciendo la permutación cíclica $(23\ldots n)$ de las columnas del cuadrado anterior A_{i-1}. Este comportamiento se debe al carácter cíclico de $(GF(n)^*,\cdot)$, como demostramos a continuación. Si α es un elemento primitivo de $GF(n)$,

$$f_i = \alpha^{i-1} \qquad 1 \leqslant i \leqslant n-1$$

Entonces, para $2 \leqslant j \leqslant n-1$ y $l \geqslant 2$,

$$a_{ij}^{l+1} = f_{l+1}f_j + f_i = \alpha^l\alpha^{j-1} + f_i = \alpha^{l-1}\alpha^j + f_i = f_l f_{j+1} + f_i = a_{i(j+1)}^l$$

Es preciso mencionar que Wernicke (1910) enunció el recíproco del teorema anterior, es decir, si existe un conjunto completo de MOLS de orden n, entonces n es una potencia de un primo. Se detectaron errores en la demostración de este resultado y hasta ahora continúa siendo un problema abierto.

Una manera de obtener nuevas familias de MOLS a partir de otras la proporciona el resultado siguiente, obtenido por MacNeish (1922).

Teorema 12.37. Si existen dos familias de k MOLS de órdenes respectivos n y m, entonces existe una nueva familia de k MOLS de orden nm.

Demostración. Sean F_1 y F_2 dos familias de k MOLS de órdenes respectivos n y m:

$$\begin{aligned} F_1 &= \{A_1, A_2, \ldots, A_k\} \\ F_2 &= \{B_1, B_2, \ldots, B_k\} \end{aligned}$$

Definimos una nueva familia $F_3 = \{C_1, C_2, \ldots, C_k\}$ de orden nm a través del producto cartesiano de las matrices de las familias anteriores:

$$C_l = A_l \times B_l = \begin{pmatrix} (a_{11}^l, B_l) & \cdots & (a_{1n}^l, B_l) \\ \vdots & \ddots & \vdots \\ (a_{n1}^l, B_l) & \cdots & (a_{nn}^l, B_l) \end{pmatrix}$$

donde

$$(a_{ij}^l, B_l) = \begin{pmatrix} (a_{ij}^l, b_{11}^l) & \cdots & (a_{ij}^l, b_{1m}^l) \\ \vdots & \ddots & \vdots \\ (a_{ij}^l, b_{m1}^l) & \cdots & (a_{ij}^l, b_{mm}^l) \end{pmatrix}$$

Es preciso demostrar que F_3 es una familia de MOLS.

En primer lugar, comprobemos que los elementos de F_3 son cuadrados latinos. Para ello sólo es preciso observar que dos elementos cualesquiera de una fila (columna) de C_l, $1 \leqslant l \leqslant k$ son diferentes ya que A_l y B_l son cuadrados latinos:

$$\begin{cases} (a^l_{ij}, b^l_{uv}) & \neq & (a^l_{ij'}, b^l_{uv'}) \\ (a^l_{ij}, b^l_{uv}) & \neq & (a^l_{i'j}, b^l_{u'v}) \end{cases}$$

Comprobemos ahora que los elementos de F_3 son mutuamente ortogonales. Para ello, supongamos que existen dos parejas de elementos iguales a $(C_l, C_h) \in F_3 \times F_3$,

$$((a^l_{ij}, b^l_{uv}), (a^h_{ij}, b^h_{uv})) = ((a^l_{i'j'}, b^l_{u'v'}), (a^h_{i'j'}, b^h_{u'v'}))$$

Entonces, igualando componentes y teniendo en cuenta que $A_l \perp A_h$ y $B_l \perp B_h$, deducimos que las posiciones también tienen que coincidir. □

Como consecuencia directa de este teorema tenemos el resultado siguiente:

Teorema 12.38. Si $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ es la descomposición en factores primos de n, entonces

$$N(n) \geqslant \min\{p_i^{n_i} - 1, 1 \leqslant i \leqslant s\}$$

El único caso en que el más pequeño de los $p_i^{n_i}$ en la descomposición en factores primos de n es 2 se da cuando n es par pero no divisible por cuatro. Así pues,

Corolario 12.39. Si $n \not\equiv 2 \pmod 4$, entonces $N(n) \geqslant 2$.

Teniendo en cuenta este resultado, deducimos por ejemplo que hay como mínimo dos cuadrados latinos de orden 12 mutuamente ortogonales, $N(12) \geqslant 2$. Si $n = 2m$, donde m es un número impar, sólo deducimos que $N(n) \geqslant 1$. Recordemos que la conjetura de Euler decía que, en este caso, $N(n) = 1$. Para $m = 1$, está claro que $N(2) = 1$. Para $m = 3$, Terry obtuvo en 1901 todas las posibles parejas de cuadrados latinos de orden 6 (9.408, considerando sólo cuadrados latinos normalizados) y no encontró ninguno que fuese ortogonal. Por tanto, el problema de los 36 oficiales no tiene solución y parte de la conjetura de Euler es cierta. Pero no fue hasta 1960 que Bose, Parker y Shrikhande demostraron, mediante diseños experimentales, que la conjetura es falsa, excepto justamente en los casos conocidos $n = 2, 6$.

Teorema 12.40. $N(n) \geqslant 2, \quad n \equiv 2 \pmod 4, \quad n \neq 2, 6.$

La demostración de este resultado es muy larga y, por este motivo, se ha intentado encontrar demostraciones más sencillas, pero de momento no se ha conseguido.

MOLS y planos proyectivos

La existencia de un conjunto completo de MOLS, tal como veremos a continuación, equivale a la existencia de un plano proyectivo. La demostración de este resultado es constructiva y pensamos que muy instructiva. En particular, proporciona un método para construir los planos proyectivos de orden $n = p^k$, p primo, a partir de la familia completa de MOLS que se ha descrito en el teorema 12.36 del apartado anterior.

Teorema 12.41. Existe un plano proyectivo de orden m, si y sólo si existe un conjunto completo de MOLS de orden m.

Demostración. Sea $PG(2,m)$ un plano proyectivo de orden m. Consideramos una línea cualquiera l de $PG(2,m)$ y escogemos dos puntos arbitrarios p y q de l. Consideramos ahora las intersecciones entre los conjuntos de líneas siguientes:

$$\begin{aligned} L_p \setminus l &= \{l_p^1, l_p^2, \ldots, l_p^m\} \\ L_q \setminus l &= \{l_q^1, l_q^2, \ldots, l_q^m\} \end{aligned}$$

que denotamos por

$$p_{ij} = l_p^i \cap l_q^j$$

y $p_1, \ldots, p_{m-1}$ son los puntos de l diferentes de p y q.

Definimos la familia de matrices de orden $m \times m$,

$$F = \{A_k = (a_{ij}^k),\ 1 \leqslant k \leqslant m-1\}$$

de manera que a_{ij}^k representa la línea de $PG(2,m)$ que pasa por los puntos p_{ij} y $p_k \in l \setminus \{p,q\}$.

Demostraremos que F es un conjunto completo de MOLS. En primer lugar, es preciso comprobar que los elementos de F son cuadrados latinos. Cualquier matriz A_k sólo tiene m elementos diferentes, ya que por p_k sólo pasan $(m+1)$ rectas, y de éstas la recta l no intersecta con p_{ij}. Por otra parte, los elementos de una fila (columna) son todos diferentes. Efectivamente, si $a_{ij}^k = a_{ij'}^k$ ($a_{ij}^k = a_{i'j}^k$), entonces $p_{ij} = p_{ij'}$ ($p_{ij} = p_{i'j}$), ya que $a_{ij}^k, a_{ij'}^k \in L_{p_k}$ ($a_{ij}^k, a_{i'j}^k \in L_{p_k}$), y, por tanto, $j = j'$ ($i = i'$).

Es preciso comprobar también que los elementos de F son mutuamente ortogonales. Supongamos lo contrario, es decir, que $A_k, A_k' \in F$ son tales que alguna pareja, $(a_{ij}^k, a_{ij}^{k'})$, aparece más de una vez, o sea

$$(a_{ij}^k, a_{ij}^{k'}) = (a_{i'j'}^k, a_{i'j'}^{k'})$$

Entonces, igualando componentes, obtenemos que los puntos p_k, p_{ij} y $p_{i'j'}$ están en una misma línea l', y, de forma similar, los puntos $p_{k'}$, p_{ij} y $p_{i'j'}$ están sobre otra línea l'', de manera que $l' \cap l'' = \{p_{ij}, p_{i'j'}\}$, lo que contradice el axioma **P2**.

En sentido contrario, sea ahora $F = \{A_1, A_2, \ldots, A_{m-1}\}$ un conjunto completo de MOLS. Podemos construir un plano proyectivo de orden n de la forma siguiente.

Consideremos una malla cuadrada de tamaño $m \times m$ y definamos el conjunto de líneas formado por las líneas horizontales y las líneas verticales, es decir, $2m$ líneas. Definamos también el conjunto de puntos formado por las intersecciones de las líneas de la malla, más los puntos x e y que se obtienen de intersectar las líneas horizontales entre ellas y las verticales entre ellas. De esta manera tenemos $m^2 + 2$ puntos.

Consideremos ahora, para cada cuadrado latino $A_i \in F$, el conjunto L_i formado por todas las líneas que se obtienen al unir las diferentes posiciones que ocupa un mismo elemento de A_i y denotemos por x_i el punto, exterior a la malla, donde hacemos intersectar estas líneas. Observemos que, por el hecho de ser A_i un cuadrado latino, $|L_i| = m$, y que, por el hecho de ser F una familia de MOLS, $x_i \neq x_j$ si $i \neq j$. Finalmente añadimos una nueva línea que contiene los $(m-1)$ puntos x_i y además el x y el y.

De esta manera tenemos un conjunto de puntos P y un conjunto de líneas L tales que:

$$\begin{cases} |P| & = & m^2 + |\{x,y\}| + |\{x_i \mid 1 \leqslant i \leqslant m\}| = m^2 + m + 1 \\ |L| & = & 2m + (m-1)m + 1 = m^2 + m + 1 \\ |l| & = & m+1, \forall l \in L \\ |L_p| & = & m+1, \forall p \in P \\ |L_p \cap L_q| & = & 1, \forall p, q \in P \end{cases}$$

Éste es un 2-diseño simétrico con parámetros $(m^2 + m + 1, m + 1, 1)$-SD y, por tanto, un plano proyectivo de orden m, $PG(2,m)$. □

En la figura 12.11 se muestra por ejemplo la construcción del plano proyectivo de orden tres, $PG(2,3)$, a partir del siguiente conjunto completo de MOLS:

$$A_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

Como consecuencia del teorema anterior, deducimos que existe un plano proyectivo de orden cualquier potencia de un primo. De la misma manera, se podría haber relacionado la existencia de un conjunto completo de MOLS de orden m con la de un plano afín del mismo orden (recordemos que hay un plano proyectivo de orden m si y sólo si hay un plano afín del mismo orden).

Corolario 12.42. Si $m = p^k$, con p primo, entonces existen $PG(2,m)$ y $AG(2,m)$.

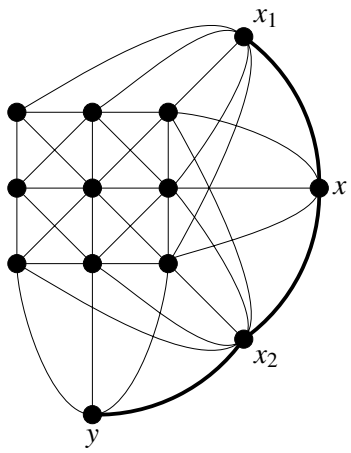


Figura 12.11: $PG(2,3)$

Notas bibliográficas

Son muchos los libros de combinatoria que dedican una parte importante al estudio de los diseños, y hay otros más específicos que se dedican exclusivamente al estudio de los diseños. Aquí hemos escogido una muestra que creemos suficiente para cubrir un margen amplio de niveles de exigencia.

El texto de Anderson [1] presenta una visión global de las posibilidades del tema que puede ser útil en un nivel básico. En el libro de Wallis [6] se tratan todos los aspectos básicos relacionados con el tema de forma clara y más extensa. El texto de Street y Street [4] puede ser un libro complementario y presenta diferentes métodos para la construcción explícita de diseños que no han tenido un espacio en este libro. En este sentido recomendamos también el libro de Hall [2], que además contiene de forma muy comprensible toda la información básica sobre esta teoría. Los lectores más interesados se pueden dirigir a [3] o a [5]. En el primero se tratan todas estas cuestiones desde un punto de vista más formal, mientras que, en el segundo, el estilo es más conciso pero hay más información. Ambos textos son de un nivel más exigente que los anteriores.

Bibliografía

[1] I. Anderson. *A First Course in Combinatorial Mathematics*, Oxford University Press, 1979.

[2] M. Hall. *Combinatorial Theory*, John Wiley & Sons, 1986.

[3] D. R. Hughes, F. C. Piper. *Design Theory*, Cambridge University Press, 1988.

[4] A. P. Street, D. J. Street. *Combinatorics of Experimental Designs*, Oxford Science, 1986.

[5] J. H. van Lint, R. M. Wilson. *A Course in Combinatorics*, Cambridge University Press, 1993.

[6] W. D. Wallis. *Combinatorial Designs*, Marcel Dekker, 1988.

Problemas

1. Estudiar los valores de $r = \lambda_1, \lambda_2$ y λ_3 en la siguiente estructura combinatoria E definida sobre el conjunto $V = \{1,2,3,4,5,6,7\}$ y que tiene por conjunto de bloques los que figuran a continuación:

$$\begin{array}{lcllcl} B_1 & = & \{1,2,4\} & B_8 & = & \{1,2,4\} \\ B_2 & = & \{1,3,7\} & B_9 & = & \{1,3,7\} \\ B_3 & = & \{1,5,6\} & B_{10} & = & \{1,5,6\} \\ B_4 & = & \{2,3,5\} & B_{11} & = & \{2,3,5\} \\ B_5 & = & \{2,6,7\} & B_{12} & = & \{2,6,7\} \\ B_6 & = & \{3,4,6\} & B_{13} & = & \{3,4,6\} \\ B_7 & = & \{4,5,7\} & B_{14} & = & \{4,5,7\} \end{array}$$

   Comprobar que si se define la relación de equivalencia R que identifica bloques iguales, entonces, E/R es isomorfo a STS(7).

2. Comprobar que el conjunto de bloques que figuran a continuación, obtenidos a partir del conjunto $V = \{1,2,3,4,5,6,7\}$, no es un 2-diseño:

$$\begin{array}{lcllcl} B_1 & = & \{1,2,4\} & B_8 & = & \{1,2,4\} \\ B_2 & = & \{1,3,7\} & B_9 & = & \{1,3,7\} \\ B_3 & = & \{1,5,6\} & B_{10} & = & \{1,5,6\} \\ B_4 & = & \{2,3,5\} & B_{11} & = & \{2,3,6\} \\ B_5 & = & \{2,6,7\} & B_{12} & = & \{2,5,7\} \\ B_6 & = & \{3,4,6\} & B_{13} & = & \{3,4,5\} \\ B_7 & = & \{4,5,7\} & B_{14} & = & \{4,6,7\} \end{array}$$

   Comprobar también que la estructura definida en este ejercicio no es isomorfa a la definida en el ejercicio anterior.

3. Estudiar los parámetros de la estructura siguiente e interpretarla como una 2-estructura y también como una 1-estructura:

$$V = \{1,2,3,4,5,6,7\} \qquad \begin{aligned} B_1 &= \{1,2,3,6\} \\ B_2 &= \{1,2,5,7\} \\ B_3 &= \{1,3,4,5\} \\ B_4 &= \{1,4,6,7\} \\ B_5 &= \{2,3,4,7\} \\ B_6 &= \{2,4,5,6\} \\ B_7 &= \{3,5,6,7\} \end{aligned}$$

   Comparar la matriz de incidencia de esta estructura con la matriz de incidencia de $\mathrm{STS}(7)$.

4. Demostrar, de forma constructiva, que la condición de la proposición 12.3, $bk = rv$ es también suficiente para la existencia de un diseño regular con parámetros (v,k,r).

5. Un diseño regular $D = (V,B)$ con parámetros (v,k,r) se dice *trivial* si cada k-subconjunto de V está contenido como mínimo en un bloque de B. Demostrar que un diseño D es trivial si y sólo si D es un t-diseño para todo t tal que $0 \leqslant t \leqslant k$.

6. Demostrar que un 2-diseño con $v = 8$ y $k = 3$ es trivial.

7. Demostrar que no puede existir un sistema de Steiner con parámetros $S(5,7,13)$.

8. Demostrar que si existe un sistema de Steiner $S(3,4,v)$, entonces $v = 6n+2$, o bien, $v = 6n+4$, para algún natural n. (Se demuestra que éstas son también condiciones suficientes.)

9. Demostrar que no puede existir ningún 4-diseño con parámetros $(11,7,2)$.

10. Demostrar que para el diseño 5-$(24,8,1)$, todos los λ_4, λ_3, λ_2 y λ_1 son enteros.

11. Demostrar que si D es un 2-diseño con parámetros (v,k,λ), entonces son equivalentes las afirmaciones siguientes:

    (a) $b = v$;

    (b) $k = r$;

    (c) D^T es un 2-diseño;

    (d) D y D^T son diseños simétricos con parámetros (v,k,λ)-SD.

12. Demostrar que no existen 2-diseños simétricos con parámetros:

(a) $(4,7,1)$-SD

(b) $(22,7,2)$-SD

(c) $(29,8,2)$-SD

13. Demostrar que hay un único 3-$(8,4,1)$ diseño (salvo isomorfismos).

14. Examinar todos los posibles conjuntos de parámetros para un diseño simétrico con $\lambda = 1$ y $k \leqslant 24$. Decidir cuándo:

    (a) existe algún diseño simétrico con estos parámetros;

    (b) no existe diseño simétrico con estos parámetros;

    (c) no se puede decidir.

15. Examinar todos los posibles conjuntos de parámetros con $\lambda = 2$ y $k \leqslant 16$. Decidir cuándo:

    (a) no puede existir ningún diseño simétrico $(v,k,2)$-SD;

    (b) el teorema BRC no dá información para la existencia de diseños simétricos con estos parámetros.

16. Demostrar que, si un cuadrado latino de tamaño n tiene un subcuadrado latino de tamaño $m < n$, entonces $2m \leqslant n$.

17. Demostrar que el siguiente cuadrado latino no se corresponde con la tabla multiplicativa de ningún grupo finito.

1	2	3	4	5
2	1	5	3	4
3	4	1	5	2
4	5	2	1	3
5	3	4	2	1

18. Demostrar que no existe ningún cuadrado latino ortogonal con

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

19. Demostrar que el único cuadrado latino normalizado de orden 4 que admite cuadrados latinos ortogonales es

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

20. Usando el ejercicio anterior, demostrar que, salvo isomorfismos, existe sólo un plano afín y un plano proyectivo de orden 4.

21. De forma similar al ejercicio anterior, demostrar que los planos afines y proyectivos de orden 3 son únicos.

22. Un cuadrado latino se dice *auto-ortogonal* si es ortogonal a su propio transpuesto.

    (a) Demostrar que, en un cuadrado latino auto-ortogonal, los elementos de la diagonal tienen que estar ordenados consecutivamente, es decir: 1, 2, 3, ...

    (b) Demostrar que no existen cuadrados latinos auto-ortogonales de tamaño 3.

    (c) Encontrar cuadrados latinos auto-ortogonales de tamaño 4 y tamaño 5.