MATEMATICA DISCRETA II

Cuerpos finitos

1.Definición :

Un cuerpo finito es un cuerpo que tiene una cantidad finita de elementos

Por ejemplo, los $\boldsymbol{Z}_p$, con p primo, son cuerpos finitos. Los $\boldsymbol{Z}_n$ con n no primo no son cuerpos. Por ejemplo, $\boldsymbol{Z}_4$ no es cuerpo, pues $2.2 = 0$ en $\boldsymbol{Z}_4$, con lo cual 2 no puede tener un inverso en $\boldsymbol{Z}_4$. En general, si $n = ab$, tendremos que $ab = 0$ en $\boldsymbol{Z}_n$ y ninguno tendra un inverso. Si bien $\boldsymbol{Z}_4$ no es cuerpo, ¿puede existir un cuerpo con 4 elementos? ¿puede haber uno con 6? ¿que estructura tienen? Veamos primero que no puede haber un cuerpo finito con 6 elementos, por ejemplo. Pero antes de ello, para facilidad de esxcritura en la prueba, intruduzcamos una notación y probemos algunas cosas:

2.Notación :

Dado un natural k, un cuerpo $\mathbb{F}$ y $\alpha \in \mathbb{F}$, denotamos a $\overbrace{\alpha + \cdots + \alpha}^{k}$ como $k.\alpha$, donde $+$ es la suma del cuerpo

3.Propiedad :

Si $\mathbb{F}$ es cuerpo, k, j son naturales, y $\alpha \in \mathbb{F}$ entonces $(k + j).\alpha = k.\alpha + j.\alpha$ y :

$$k.(j.\alpha) = (kj).\alpha$$

Prueba:

$$\begin{aligned} k.(j.\alpha) =& \overbrace{j.\alpha + \cdots + j.\alpha}^{k} \\ =& \overbrace{\overbrace{\alpha + \cdots + \alpha}^{j} + \cdots + \overbrace{\alpha + \cdots + \alpha}^{j}}^{k} \\ =& \overbrace{\alpha + \cdots + \alpha}^{kj} \\ =& (kj).\alpha \end{aligned}$$

La otra igualdad es mas fácil y se deja como ejercicio.

QED.

Ahora si, podemos probar el siguiente teorema, que en particular muestra que no hay cuerpos finitos con 6, 10 o 21 elementos.

4.Teorema :

Sea $(\mathbb{F}, +, .)$ un cuerpo finito. Entonces, existe un primo p y un natural r tal que $|\mathbb{F}| = p^r$. Mas aun, $(\mathbb{F}, +) \simeq (\mathbb{Z}_p^r)$

Prueba:

Sea $1_{\mathbb{F}}$ la unidad multiplicativa de $\mathbb{F}$. Como $\mathbb{F}$ es finito, no puede ser que todos los elementos $1_{\mathbb{F}}$, $2.1_{\mathbb{F}}$, $3.1_{\mathbb{F}}$, etc sean distintos. Por lo tanto, existen $i > j$ tal que $i.1_{\mathbb{F}} = j.1_{\mathbb{F}}$, es decir, $(i-j).1_{\mathbb{F}} = 0$. Sea entonces p el menor número tal que $p.1_{\mathbb{F}} = 0$. Probemos primero que p es primo. Supongamos que no. Entonces existen $a, b < p$ tales que $p = ab$. Sea $\alpha = a.1_{\mathbb{F}}$ y $\beta = b.1_{\mathbb{F}}$. Entonces:

$$\begin{aligned}
\alpha\beta =& (\overbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}^{a})\beta \\
=& \overbrace{\beta + \cdots + \beta}^{a} \\
=& a.\beta = a.(b.1_{\mathbb{F}}) \\
=& (ab).1_{\mathbb{F}} \\
=& p.1_{\mathbb{F}} \\
=& 0
\end{aligned}$$

Como $\mathbb{F}$ es cuerpo, esto dice que, o bien $\alpha = 0$ o bien $\beta = 0$. Es decir, tendriamos o bien $a.1_{\mathbb{F}} = 0$ o $b.1_{\mathbb{F}} = 0$, lo cual es absurdo porque p era el mas chico con $p.1_{\mathbb{F}} = 0$.

Hemos visto entonces que p es primo. Entonces $\mathbb{Z}_p$ es cuerpo. Podemos darle a $\mathbb{F}$ una estructura de $\mathbb{Z}_p$-espacio vectorial, definiendo la suma de vectores como la suma de $\mathbb{F}$, y el producto por escalares por $k.\alpha = \overbrace{\alpha + \cdots + \alpha}^{k}$.

Es facil chequear que $\mathbb{F}$ es un $\mathbb{Z}_p$-espacio vectorial con estas operaciones: las propiedades relativas a la suma las satisface obviamente, y $1.\alpha = \alpha$, $k.(\alpha + \beta) = k.\alpha + k.\beta$ son faciles de ver. La otra distributividad y la asociatividad del producto pueden dar lugar a alguna confusión, hagamos una. Denotemos las operaciones en $\mathbb{Z}_p$ como $\oplus$ y $\odot$ para distinguirlas de la suma y producto en $\mathbb{N}$. Sabemos que $k.(j.\alpha) = (kj).\alpha$ por lo que probamos antes, pero queremos el producto en $\mathbb{Z}_p$ ahi, no el producto de los naturales. Sea q tal que $kj = qp + k \odot j$. Entonces $(kj).\alpha = (qp + k \odot j).\alpha = q.(p.\alpha) + (k \odot j).\alpha = (k \odot j).\alpha$ puesto que $p.\alpha = \overbrace{\alpha + \cdots + \alpha}^{p} = \alpha.(\overbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}^{p}) = \alpha.0 = 0$

Similar para la distributividad.

Entonces, al ser $\mathbb{F}$ un $\mathbb{Z}_p$-espacio vectorial, tiene dimensión, la cual debe ser finita porque $\mathbb{F}$ lo es. Sea r la dimensión. Entonces, $\mathbb{F} \simeq \mathbb{Z}_p^r$ (como espacios vectoriales), por lo que

$|\mathbb{F}| = |\mathbb{Z}_p^r| = p^r$. Ademas, el isomorfismo de espacios vectoriales dice que $(\mathbb{F}, +) \simeq (\mathbb{Z}_p^r, +)$ (como grupos).

QED.

Por lo tanto, no hay grupos finitos de orden 6, 12, o 100. Mas aun, cualquier grupo finito de orden 4 que existiera, debe cumplir, con respeccto a la operaciom suma, que es isomorfo como grupo al grupo $\mathbb{Z}_2^2$. Querriamos saber si hay algun grupo finito de orden 4. Veamos como construir uno en general:

5.Teorema :

Sea $f(x) \in \mathbb{Z}_p[x]$ un polinomio irreducible (es decir, un polinomio que no se puede escribir como producto de dos polinomios de menor grado). Entonces $\mathbb{Z}_p[x]/f(x)$ es un cuerpo. (finito)

Prueba:
Sabemos que es un anillo, solo hace falta ver la inversibilidad de elementos no nulos. La prueba es la misma que para los $\mathbb{Z}_p$: Sea $g(x) \in \mathbb{Z}_p[x]/f(x)$, $g(x) \neq 0$. Si el grado de g es 0, entonces $g(x) = c$, una constante, y como $\mathbb{Z}_p$ es cuerpo y $c \neq 0$, tenemos que existe c^{-1}, asi que existe $g(x)^{-1}$. Supongamos ahora que el grado de g es mayor que cero. Como $f(x)$ es irreducible, el maximo comun divisor entre f y g es 1. Por lo tanto existen polinomios $q(x)$ y $t(x)$ tales que $1 = f(x)t(x) + g(x)q(x)$, con lo cual $g(x)q(x) \equiv 1_{f(x)}$, es decir, $q(x)$ es un inverso de $g(x)$ en $\mathbb{Z}_p[x]/f(x)$.

QED.

Por ejemplo, para construir un cuerpo de 4 elementos, podemos tomar el polinomio $f(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$. Es facil ver que $f(x)$ es irreducible, pues al ser de grado 2, los unicos factores pueden ser de grado 1, con lo cual f deberia tener raices. Pero $f(0) = 1 = f(1)$, asi que f no las tiene. El conjunto $\mathbb{Z}_2[x]/f(x)$ es el conmjunto $\{0, 1, x, 1 + x\}$. La suma es la suma usual de polinomios, y el producto viene dado, ademas de los productos obvios por 0 y por 1, por las ecuaciones:

$$x.x = 1 + x \qquad x.(1 + x) = 1 \qquad (1 + x).(1 + x) = x$$

(estas ecuaciones se deducen del hecho que, en $\mathbb{Z}_2[x]/f(x)$, se cumple $x^2 + x + 1 = 0$).
El siguiente teorema importante que deseamos probar requiere que probemos algunas cosas de teoria de grupos.
Recordemos que un grupo es un conjunto G junto con una operacion . tal que la operación es asociativa, tiene neutro y todo elemento tiene inverso. Si la operación es conmutativa, el grupo se dice abeliano. Denotemos por 1 el neutro.

Sea G un grupo finito. Dado un elemento $x \neq 0$ de G, definimos el orden de x ($ord(x)$) como el menor natural a tal que $x^a = 1$. (como G es finito, a debe existir). ("natural" significa "entero positivo").

==========

6.LEMA :

Propiedades del orden (LO): Sea G un grupo finito. Entonces:

i) $x^t = 1$ si y sólo si $ord(x)|t$.
ii) Si $k|ord(x)$, entonces $ord(x^k) = \frac{ord(x)}{k}$.
iii) Si G es abeliano, y $ord(x), ord(y)$ son coprimos entonces $ord(xy) = ord(x)ord(y)$

==========

Prueba:
i) Claramente si $ord(x)|t$, entonces $t = q.ord(x)$ y $x^t = (x^{ord(x)})^q = 1^q = 1$ Para el otro lado, supongamos ahora $x^t = 1$, y dividamos: $t = ord(x)q + r$, con $r < ord(x)$, entonces $1 = x^t = (x^{ord(x)})^q x^r = x^r$. Como $ord(x)$ es el menor numero natural a con $x^a = 1$, concluimos que r no es natural, i.e., $r = 0$.
ii) Sea $a = ord(x)$, $b = ord(x^k)$.
Como $(x^k)^{\frac{a}{k}} = x^a = 1$, tenemos que $b = ord(x^k) \leq \frac{a}{k}$.
Por otro lado $1 = (x^k)^b = x^{kb} \Rightarrow a \leq kb$, es decir $\frac{a}{k} \leq b$.
iii) Sea $a = ord(x)$, $b = ord(y)$, $m = ord(xy)$. Entonces $(xy)^{ab} = (x^a)^b(y^b)^a = 1.1 = 1$, por lo tanto, $m = ord(xy) \leq ab$.
Por otro lado, $(xy)^m = 1 \Rightarrow x^m = (y^{-1})^m$ con lo cual
$x^{bm} = ((y^b)^{-1})^m = (1^{-1})^m = 1$, por lo tanto $a|bm$ (por i). Como $mcd(a, b) = 1$, obtenemos que $a|m$. De la misma forma $b|m$ y usando otra vez que $mcd(a, b) = 1$, obtenemos que $ab|m$. Como habiamos visto que $m \leq ab$, concluimos que son iguales.

QED.

Lo principal que quiero probar es lo siguiente, lo cual sale como un corolario fácil de un teorema llamado el teorema de estructuras de grupos finitos, pero la demostración de ese teorema es mas complicada que lo que necesitamos probar, asi que la prueba es mas directa:

==========

7.LEMA DEL MAXIMO ORDEN (LMO) :

Sea G grupo abeliano finito y sea m el máximo de todos los ordenes de los elementos de G. Entonces $x^m = 1$ para todo $x \in G$.

==========

Prueba: Sean $x \in G$ y $a = ord(x)$. Como m es el máximo orden, existe $y \in G$ tal que $m = ord(y)$. Si $a|m$, entonces por LO i) tenemos que $x^m = 1$ que es lo que queremos probar. Supongamos entonces que $a \not| m$. Esto dice que en la descomposición prima de a existe algún primo cuyo exponente en la misma es mayor que el exponente que tiene en la descomposición prima de m. Es decir, existe un primo p y un exponente e tal que $p^e|m$; $p^{e+1} \not| m$ y $p^{e+1}|a$. Sea $t = \frac{a}{p^{e+1}}$.
Por el LO ii), $ord\left(y^{p^e}\right) = \frac{m}{p^e}$ mientras que $ord\left(x^t\right) = \frac{a}{t} = p^{e+1}$. Como $p^{e+1} \not| m$, entonces $\frac{m}{p^e}$ y p^{e+1} son coprimos, por lo tanto por el LO iii) tenemos que $ord(x^t y^{p^e}) = p^{e+1}\frac{m}{p^e} = pm$, absurdo, pues m era el mayor orden de cualquier elemento.
Este absurdo provino de suponer que $a \not| m$, por lo que tenemos que $a|m$ y $x^m = 1$

QED.

Necesitamos tambien el siguiente hecho fundamental sobre cuerpos, que ya que estamos lo pruebo:

==========

8.LEMA DE POLINOMIOS SOBRE UN CUERPO (LPC) :

En un cuerpo, un polinomio de grado n que se mire como función no puede tener mas de n raices distintas

==========

Prueba:
Sea $f(x)$ es un polinomio de grado x, mirado como función. Sean $r_1, r_2, ..., r_t$ raices distintas de $f(x)$. Como r_1 es raiz, entonces existe $q(x)$ tal que $f(x) = (x - r_1)q(x)$. Como r_2 es raiz, entonces $0 = f(r_2) = (r_2 - r_1)q(r_2)$. Por estar en un cuerpo, entonces o bien $r_2 - r_1 = 0$, o bien $q(r_2) = 0$. Como estamos suponiendo que $r_1 \neq r_2$, tenemos que debe ser $q(r_2) = 0$, es decir, r_2 es raiz de $q(x)$. Podemos escribir entonces $q(x) = (x - r_2)q_2(x)$ y por lo tanto $f(x) = (x - r_1)(x - r_2)q_2(x)$. Con el mismo argumento concluimos que r_3 es raiz de $q_2(x)$, etc, con lo cual concluimos que existe algún polinomio $q_t(x)$ tal que $f(x) = (x - r_1)(x - r_2)\dots(x - r_t)q_t(x)$. Pero entonces el grado de f debe ser mayor o igual que t.

QED.

(Nota al margen: esto no vale en general en un anillo: Por ejemplo, el polinomio $f(x) = x^2 + x$ tiene CUATRO raices en $\boldsymbol{Z}_6 : 0, 2, 3$ y 5).
Ahora si, el teorema principal:

9.Teorema del Elemento Primitivo :

Sea $\mathbb{F}$ un cuerpo finito. Entonces, existe un elemento primitivo en $\mathbb{F}$, es decir, existe un α tal que $\mathbb{F} - \{0\} = \{\alpha, \alpha^2, ..., \alpha^{q-1}\}$, donde $q = |\mathbb{F}|$. En otras palabras $(\mathbb{F} - \{0\}, .) \simeq (\mathbb{Z}_{q-1}, +)$

Prueba:
Como $\mathbb{F}$ es cuerpo, entonces $\mathbb{F} - \{0\}$ es un grupo finito abeliano. Por lo tanto, si m denota el mayor orden, tenemos por LMO que $\beta^m = 1 \ \forall \beta \in \mathbb{F} - \{0\}$. Como hay $q-1$ elementos en $\mathbb{F} - \{0\}$ concluimos que el polinomio $x^m - 1$ tiene $q-1$ raices distintas, asi que por el LPC tenemos que $q - 1 \leq m$.
Por otro lado, sea α tal que $ord(\alpha) = m$.
Entonces el conjunto $< \alpha >= \{\alpha, \alpha^2, ..., \alpha^{a-1}, \alpha^m = 1\}$ tiene m elementos distintos. Como es un subconjunto de $\mathbb{F} - \{0\}$, concluimos que $m \leq q-1$. Por esto y lo anterior, $m = q-1$, con lo cual $< \alpha >= \mathbb{F} - \{0\}$ que es lo que queriamos probar.

QED.

Volvamos ahora a códigos:
==========

10.Propiedad :

Sea $\{\alpha_1, ..., \alpha_r\}$ un conjunto de r elementos no nulo de $GF(p^r)$ Sea $g(x) = (x-\alpha_1)...(x-\alpha_r)$ y $n = p^r - 1$. Entonces $g(x)|(x^n - 1)$ y por lo tanto es el generador de algún código ciclico

==========

Prueba:
Por el teorema del elemento primitivo, como $n = p^r - 1 = \mathbb{F} - \{0\}$ tenemos que $\alpha^n = 1$ para todo $\alpha \in \mathbb{F} - \{0\}$. En particular todos los α_i son raices del polinomio $x^n - 1$ y por la demostración del LPC obtenemos que $(x - \alpha_1)...(x - \alpha_r)|(x^n - 1)$.

QED.

==========

11.Definición :

Un código de Reed-Solomon $RS(p^r, d)$ es el código cíclico de longitud $n = p^r - 1$ generado por $g(x) = (x - \beta^{t+1})(x - \beta^{t+2})...(x - \beta^{t+d-1})$, donde β es un elemento primitivo de $GF(p^r)$. (t es un parametro a elegir)

==========
Un código de Reed-solomon tiene entonces longitud $p^r - 1$ y si k es su dimensión tiene p^{rk} palabras.

Lo importante de estos códigos yace en que podemos saber cuanto vale δ.

==========

12.TEOREMA Reed-Solomon :

Un código $RS(p^r, d)$ tiene $\delta = d$, $k = p^r - d$ y es un códigos MDS

==========

Prueba:

Como el grado del generador es $d-1$, tenemos que $k = n - (d-1) = n + 1 - d = p^r - d$.

Recordemos que un código es MDS si $k = n+1-\delta$. Como acabamos de ver que $k = n+1-d$ concluimos que si probamos que $d = \delta$, habremos tambien probado que el código es MDS.

Una cota esta clara, justamente por la cota Singleton: $\delta \leq n - k + 1 = d$.

Para ver la otra desigualdad, basta dar una matriz de chequeo tal que cualquier conjunto de $d-1$ columnas sea LI.

Sea

$$H = \begin{bmatrix} 1 & \beta^{t+1} & (\beta^{t+1})^2 & ... & (\beta^{t+1})^{n-1} \\ 1 & \beta^{t+2} & (\beta^{t+2})^2 & ... & (\beta^{t+2})^{n-1} \\ \vdots & \vdots & ... & \vdots & \\ 1 & \beta^{t+d-1} & (\beta^{t+d-1})^2 & ... & (\beta^{t+d-1})^{n-1} \end{bmatrix}$$

que es una matriz $(d-1) \times n$. Si expandimos el polinomio generador $g(x) = g_0 + g_1 x + \cdots + g_{d-1}x^{d-1}$ y miramos $g = (g_0, g_1, ..., g_{d-1}, 0, ..., 0)$ tenemos que tenemos que

$$\begin{aligned} Hg^t &= \begin{bmatrix} g_0 + g_1\beta^{t+1} + g_2(\beta^{t+1})^2 + \cdots + g_{d-1}(\beta^{t+1})^{d-1} + 0 + \cdots + 0 \\ g_0 + g_1\beta^{t+2} + g_2(\beta^{t+2})^2 + \cdots + g_{d-1}(\beta^{t+2})^{d-1} + 0 + \cdots + 0 \\ \vdots \\ g_0 + g_1\beta^{t+d-1} + g_2(\beta^{t+d-1})^2 + \cdots + g_{d-1}(\beta^{t+d-1})^{d-1} + 0 + \cdots + 0 \end{bmatrix} \\ &= \begin{bmatrix} g(\beta^{t+1}) \\ g(\beta^{t+2}) \\ \vdots \\ g(\beta^{t+d-1}) \end{bmatrix} \\ &= 0 \end{aligned}$$

la ultima ecuación porque los β^{t+i} son raices de g. Como $g(x)$ es el generador de C entonces $Hv^t = 0$ para todo $v \in C$.

Veamos ahora que $d-1$ columnas cualesquiera de H son LI:

tomemos columnas $H^{(j_1)}, H^{(j_2)}, ..., H^{(j_{d-1})}$.

$$\det\left[\begin{array}{cccc} H^{(j_1)} & ... & H^{(j_{d-1})} \end{array}\right] = \det\begin{bmatrix} (\beta^{t+1})^{j_1} & (\beta^{t+1})^{j_2} & ... & (\beta^{t+1})^{j_{d-1}} \\ (\beta^{t+2})^{j_1} & (\beta^{t+2})^{j_2} & ... & (\beta^{t+2})^{j_{d-1}} \\ \vdots & \vdots & ... & \vdots \\ (\beta^{t+d-1})^{j_1} & (\beta^{t+d-1})^{j_2} & ... & (\beta^{t+d-1})^{j_{d-1}} \end{bmatrix}$$

$$= \beta^{(t+1)j_1}\beta^{(t+1)j_2}...\beta^{(t+1)j_{d-1}} \det\begin{bmatrix} 1 & ... & 1 \\ \beta^{j_1} & ... & \beta^{j_{d-1}} \\ (\beta^{j_1})^2 & ... & (\beta^{j_{d-1}})^2 \\ (\beta^{j_1})^{d-2} & ... & (\beta^{j_{d-1}})^{d-2} \end{bmatrix}$$

Esta ultima es una matriz de VanderMonde, que es invertible, por lo tanto el determinante no es cero. Esto dice que $\det\left[\begin{array}{cccc} H^{(j_1)} & H^{(j_2)} & ... & H^{(j_{d-1})} \end{array}\right] \neq 0$ y por lo tanto $\left[\begin{array}{cccc} H^{(j_1)} & H^{(j_2)} & ... & H^{(j_{d-1})} \end{array}\right]$ es invertible, asi que sus columnas son LI.

QED.