MATEMATICA DISCRETA II-2007
Cuerpos finitos

1.Definición :

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

Por ejemplo, los $\mathbb{Z}_p$, con p primo, son cuerpos finitos. Los $\mathbb{Z}_n$ con n no primo no son cuerpos. Por ejemplo, $\mathbb{Z}_4$ no es cuerpo, pues $2.2 = 0$ en $\mathbb{Z}_4$, con lo cual 2 no puede tener un inverso en $\mathbb{Z}_4$. En general, si $n = ab$, tendremos que $ab = 0$ en $\mathbb{Z}_n$ y ninguno tendra un inverso. Si bien $\mathbb{Z}_4$ 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:

2.Teorema :

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

Prueba:

Como $\mathbb{K}$ es finito, no puede ser que todos los elementos 1, $1+1$, $1+1+1$, etc sean distintos. Por lo tanto, existen $i > j$ tal que $\overbrace{1+\cdots+1}^{1} = \overbrace{1+\cdots+1}^{j}$, es decir, $\overbrace{1+\cdots+1}^{i-j} = 0$. Sea entonces p el menor número tal que $\overbrace{1+\cdots+1}^{p} = 0$. Probemos primero que p es primo. Supongamos que no. Entonces existen $a, b < p$ tales que $p = ab$. Sea $\alpha = \overbrace{1+\cdots+1}^{a}$ y $\beta = \overbrace{1+\cdots+1}^{b}$. Entonces:

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

Com $\mathbb{K}$ es cuerpo, esto dice que, o bien $\alpha = 0$ o bien $\beta = 0$. Es decir, tendriamos o bien $\overbrace{1+\cdots+1}^{a} = 0$ o $\overbrace{1+\cdots+1}^{b} = 0$, lo cual es absurdo porque p era el mas chico con $\overbrace{1+\cdots+1}^{p} = 0$.

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

$k\alpha = \overbrace{\alpha + \cdots + \alpha}^{k}$. Es facil chequear que $I\!K$ es un $\boldsymbol{Z}_p$-espacio vectorial con estas operaciones. Por ejemplo:

$$\begin{aligned} k(j\alpha) =& \overbrace{j\alpha + \cdots + j\alpha}^{k} \\ =& \overbrace{\overbrace{\alpha + \cdots + \alpha}^{j} + \cdots + \overbrace{\alpha + \cdots + \alpha}^{j}}^{k} \\ =& \overbrace{\alpha + \cdots + \alpha}^{kj} \\ =& \overbrace{\alpha + \cdots + \alpha}^{kj \mod p} \qquad \text{pues } \overbrace{\alpha + \cdots + \alpha}^{p} = \alpha(\overbrace{1 + \cdots + 1}^{p}) = 0 \\ =& (kj)\alpha \end{aligned}$$

Entonces, al ser $I\!K$ un $\boldsymbol{Z}_p$-espacio vectorial, tiene dimensión, la cual debe ser finita porque $I\!K$ lo es. Sea r la dimensión. Entonces, $I\!K \simeq \boldsymbol{Z}_p^r$ (como espacios vectoriales), por lo que $|I\!K| = |\boldsymbol{Z}_p^r| = p^r$. Ademas, el isomorfismo de espacios vectoriales dice que $(I\!K, +) \simeq (\boldsymbol{Z}_p^r, +)$ (como grupos). QED.

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

3.Teorema :

Sea $f(x) \in \boldsymbol{Z}_p[x]$ un polinomio irreducible (es decir, un polinomio que no se puede escribir como producto de dos polinomios de menor grado). Entonces $\boldsymbol{Z}_p[x]/f(x)$ 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 $\boldsymbol{Z}_p$: Sea $g(x) \in \boldsymbol{Z}_p[x]/f(x)$, $g(x) \neq 0$. Si el grado de g es 0, entonces $g(x) = c$, una constante, y como $\boldsymbol{Z}_p$ 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 $\boldsymbol{Z}_p[x]/f(x)$. QED.

Por ejemplo, para construir un cuerpo de 4 elementos, podemos tomar el polinomio $f(x) = 1 + x + x^2 \in \boldsymbol{Z}_2[x]$. 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 $\boldsymbol{Z}_2[x]/f(x)$ 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 $\boldsymbol{Z}_2[x]/f(x)$, se cumple $x^2 + x + 1 = 0$).

4.Teorema del Elemento Primitivo :

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

Prueba:

Dado un elemento $\alpha \neq 0$ de $I\!K$, definimos el orden (multiplicativo) de α ($ord(\alpha)$ como el menor natural a tal que $\alpha^a = 1$. (como $I\!K$ es cuerpo finito, a debe existir). Observemos que, si $\alpha^t = 1$, entonces $ord(\alpha)|t$, pues si $t = ord(\alpha)q + r$, con $r < ord(\alpha)$, entonces $1 = \alpha^t = (\alpha^{ord(\alpha)})^q\alpha^r = \alpha^r$. Como $ord(\alpha)$ es el menor numero natural a con $\alpha^a = 1$,concluimos que r no es natural, i.e., $r = 0$.

Otra propiedad del orden es que, si el maximo comun divisor entre $ord(\alpha)$ y $ord(\beta)$ es 1, entonces $ord(\alpha\beta) = ord(\alpha)ord(\beta)$. Probemos esto: Sea $a = ord(\alpha)$, $b = ord(\beta)$. Entonces $(\alpha\beta)^{ab} = (\alpha^a)^b(\beta^b)^a = 1.1 = 1$, por lo tanto, $ord(\alpha\beta) \leq ab$.

Por otro lado, $(\alpha\beta)^{ord(\alpha\beta)} = 1 \Rightarrow \alpha^{ord(\alpha\beta)} = (\beta^{-1})^{ord(\alpha\beta)}$ con lo cual $\alpha^{b.ord(\alpha\beta)}((\beta^b)^{-1})^{ord(\alpha\beta)} = 1$, por lo tanto $a|b.ord(\alpha\beta)$. Como $mcd(a,b) = 1$, obtenemos que $a|ord(\alpha\beta)$. De la misma forma $b|ord(\alpha\beta)$ y usando otra vez que $mcd(a,b) = 1$, obtenemos que $ab|ord(\alpha\beta)$. Como habiamos visto que $ord(\alpha\beta) \leq ab$, concluimos que son iguales.

Habiendo probado estas propiedades de ord, podemos continuar: tomemos α un elemento no nulo de orden el mayor posible. (como $I\!\!K$ es finito, existe tal α) y sea $a = ord(\alpha)$. Por definición de orden, el conjunto $\{\alpha, \alpha^2, ..., \alpha^{a-1}, \alpha^a = 1\}$ tiene todos los elementos distintos. Es decir, alli hay a elenementos, y como eso es un subconjunto de $I\!\!K - \{0\}$, concluimos que $a \leq q-1$. Querriamos ver que ese conjunto es todo $I\!\!K$, es decir, que vale la igualdad.

Sea β otro elemento no nulo, y sea $b = ord(\beta)$. Quiero probar que $b|a$, asi que supongamos que no y lleguemos a un absurdo.

Si $b \not| a$, entonces en la descomposicion prima de b existe algun primo cuyo exponente en la misma es mayor que el exponente que tiene en la descomposicion prima de a. Es decir, existe un primo t y un exponente e tal que $t^e|b$, $t^{e-1}|a$ pero $t^e \not| a$.

Es facil ver que $ord(\gamma^k) = \frac{ord(\gamma}{mcd(ord(\gamma),k)}$. Por lo tanto $ord(\alpha^{t^{e-1}} = \frac{a}{mcd(a,t^{e-1})} = \frac{a}{t^{e-1}}$ mientras que $ord(\beta^{\frac{b}{t^e}}) = \frac{b}{mcd(b,\frac{b}{t^e})} = \frac{b}{\frac{b}{t^e}} = t^e$.

Por lo tanto, $mcd(ord(\alpha^{t^{e-1}}, ord(\beta^{\frac{b}{t^e}})) = mcd(\frac{a}{t^{e-1}}, t^e) = 1$.

Con lo cual $ord(\alpha^{t^{e-1}}\beta^{\frac{b}{t^e}}) = \frac{a}{t^{e-1}}t^e = at$, absurdo, pues a era el mayor orden de cualquier elemento.

Este absurdo provino de suponer que $b \not| a$, por lo que tenemos que $b|a$. En particular, $\beta^a = 1$. Es decir, TODO elemento no nulo es raiz del polinomio $x^a - 1$. Pero en un cuerpo, un polinomio de grado n no puede tener mas de n raices. Como hemos dicho que todo elemento no nulo de $I\!\!K$ es raiz de $x^a - 1$, concluimos que $I\!\!K - \{0\}| \leq a$, es decir, $q - 1 \leq a$, que era lo que queriamos. QED.