Sebastian Santos Bautista - 201816848
Álgebra Abstracta 2
MATE 3121

Parcial 2 - Parte 1

Carolina Benedetti
Martes 28 Abril, 2020

(1)

Sea $\mathbb{F}$ un cuerpo de característica p tal que $[\mathbb{F} : \mathbb{F}_p] = n$. Pruebe que $|\mathbb{F}| = p^n$.

Dem: En primera instancia, es importante notar que $\mathbb{F}$ efectivamente es una extensión de $\mathbb{F}_p$, debido a que $\mathbb{F}$ es un cuerpo de característica p y, por lo tanto, su cuerpo primo generado por la identidad debe ser $\mathbb{F}_p$.

Además, como $[\mathbb{F} : \mathbb{F}_p] = n$, tenemos que existe una base de n elementos de $\mathbb{F}$ visto como un $\mathbb{F}_p$ - espacio vectorial. Luego, existen $[v_i]_{i=1,...,n}$ tq' $v_i \in \mathbb{F}$ y todo $v \in \mathbb{F}$ puede ser escrito como una combinación lineal de la forma $v = a_1v_1 + ... + a_nv_n$ con coeficientes $a_i \in \mathbb{F}_p$.

Finalmente, vea que, como $a_i \in \mathbb{F}_p$, existen p elementos diferentes para colocar en n posiciones. En consecuencia, existen $p...p = p^n$ combinaciones lineales diferentes y, asimismo, elementos de $\mathbb{F}$.

(2)

Sea $\mathbb{F}_{p^n}$ un cuerpo finito con p^n elementos. Pruebe que $\mathbb{F}_{p^n}$ es el cuerpo de descomposición del polinomio $x^{p^n} - x$ sobre $\mathbb{F}_p$.

Dem: Primero, sabemos que f(x) $= x^{p^n} - x$ es separable en $\mathbb{F}_p$, pues $Df(x) = p^n x^{p^n-1} - 1 = -1$ en tanto que $p^n x^{p^n-1} = 0$ por ser $\mathbb{F}_p$ un cuerpo de característica p. Por lo tanto, claramente el máximo común divisor de ambos polinomios es 1. Lo anterior implica que f(x) y $Df(x)$ son primos relativos, lo que es equivalente a que f(x) es separable y, en consecuencia, tiene exactamente p^n raíces diferentes.

Vea que $x^{p^n} - x = x(x^{p^n-1} - 1)$ y $0 \in \mathbb{F}_{p^n}$ es una raíz de $f(x)$. Ahora bien, queremos demostrar que las otras $p^n - 1$ raíces de $x^{p^n-1} - 1$ coinciden con los $p^n - 1$ elementos de $\mathbb{F}_{p^n} - 0 = \mathbb{F}_{p^n}^*$. Para esto, utilizamos el hecho de que $\mathbb{F}_{p^n}^*$ es un grupo abeliano multiplicativo (asociativo, $1 \in \mathbb{F}_{p^n}^*$, inversos). De lo anterior, se sigue que se cumplen el teorema de Lagrange y sus corolarios. Específicamente, para todo $a \in \mathbb{F}_{p^n}^*$, $|a||p^n - 1$. Luego, también se cumple que, si $|a| = k$ y $kq = p^n - 1$, $a^{p^n-1} = a^{kq} = 1 \implies a^{p^n-1} - 1 = 0$.

Por lo tanto, los elementos de $\mathbb{F}_{p^n}^*$ coinciden con las raices de $x^{p^n-1} - 1$ y $\mathbb{F}_{p^n}$ es un cuerpo que posee las p^n raíces de $f(x)$. Finalmente, se puede concluir que $\mathbb{F}_{p^n}$ es efectivamente el cuerpo de descomposición, pues es imposible hallar un cuerpo mas pequeño y que posea todas las p^n raíces de $f(x)$ por la minimalidad de la cardinalidad de $\mathbb{F}_{p^n}$.

(3)

Muestre que $\mathbb{F}_{p^n}/\mathbb{F}_p$ es Galois y que $\mathbb{F}_{p^n}$ es una extensión simple sobre $\mathbb{F}_p$. Describa el grupo Gal$(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Dem: Primero, demostraremos los primeros dos puntos:

- $\mathbb{F}_{p^n}/\mathbb{F}_p$ es Galois: Como $\mathbb{F}_{p^n}$ es cuerpo de descomposición de un polinomio separable sobre $\mathbb{F}_p$, luego, por teorema, esto es equivalente a que $\mathbb{F}_{p^n}/\mathbb{F}_p$ es Galois
- $\mathbb{F}_{p^n}$ es simple: $\mathbb{F}_{p^n}$ es una extensión finita y separable, pues todos sus p^n elementos son raíces del polinomio separable $f(x)$ sobre $\mathbb{F}_p$. Luego, por teorema del elemento primitivo, se concluye que $\mathbb{F}_{p^n}$ es una extensión simple sobre $\mathbb{F}_p$.

A continuación, pasamos a describir el grupo G = Gal$(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Inicialmente, sabemos que $|G| = n$, debido a que, por el primer ejercicio, existe una base de n elementos para generar el cuerpo $\mathbb{F}_{p^n}$ como un $\mathbb{F}_p$-espacio vectorial y, además, como $\mathbb{F}_{p^n}/\mathbb{F}_p$ es Galois, $|G|$ debe ser igual al grado de esta extensión.

Ahora bien, sabemos que todo $\varphi \in G$ es tal que para todo $\alpha \in \mathbb{F}_{p^n}$ algebraico (Note que todo elemento en $\mathbb{F}_{p^n}$ es algebraico, pues es raíz de $f(x)$ y, por lo tanto, su polinomio minimal debe ser un divisor irreducible de $f(x)$ con grado n) se cumple que $\varphi(\alpha)$ es también una raíz del polinomio minimal de α en $\mathbb{F}_p$. En este orden de ideas, vea que el homomorfismo de Frobenius $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ tq' $a \mapsto a^p$ debe pertenecer a G. Primero, es claro que φ fija a todo elemento perteneciente a $\mathbb{F}_p$, por ser este un cuerpo cíclico de orden p. Por otro lado, verificamos que es un homomorfismo de anillos:

$$\begin{aligned} \varphi(xy) &= (xy)^p \\ &= x^p y^p \end{aligned} \tag{1}$$

$$\begin{aligned} \varphi(x+y) &= (x+y)^p \\ &= x^p + y^p \end{aligned} \tag{2}$$

donde la última igualdad es valida por ser un cuerpo finito de característica p.

Mas aún, φ es 1-1, pues $x^p = 0 \leftrightarrow x = 0$ debido a que $\mathbb{F}_{p^n}$ es un cuerpo y no tiene divisores de cero. Luego, como $\mathbb{F}_{p^n}$ es finito, φ es un automorfismo de anillos.

Finalmente, se puede ver $\varphi^i(x) = x^{p^i}$ es un automorfismo también perteneciente a G para $i = 0, ..., n-1$, donde $\varphi^0(x) = Id(x) = x$. Sin embargo, φ^n vuelve a ser la identidad, pues $\varphi^n(x) = x^{p^n} = x^{p^n-1}x = x$ para $x \in \mathbb{F}_{p^n}^*$ y $\varphi^n(0) = 0$. Por lo tanto, esto nos hace concluir que G es el grupo de n elementos generados por φ de tal forma que $G = \{Id, \varphi, \varphi^2, ..., \varphi^{n-1}\}$.

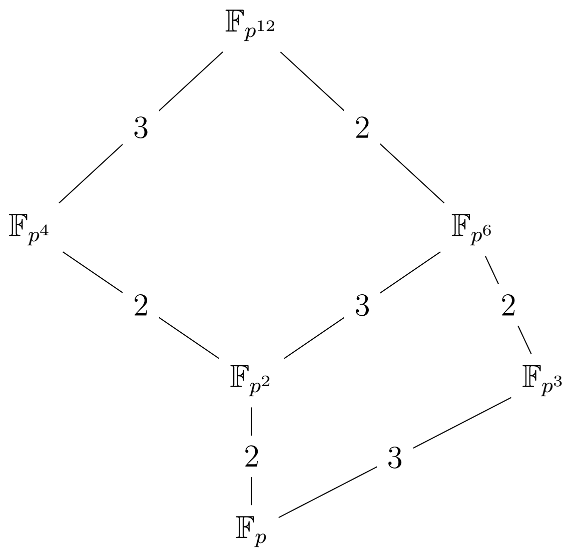
(4)

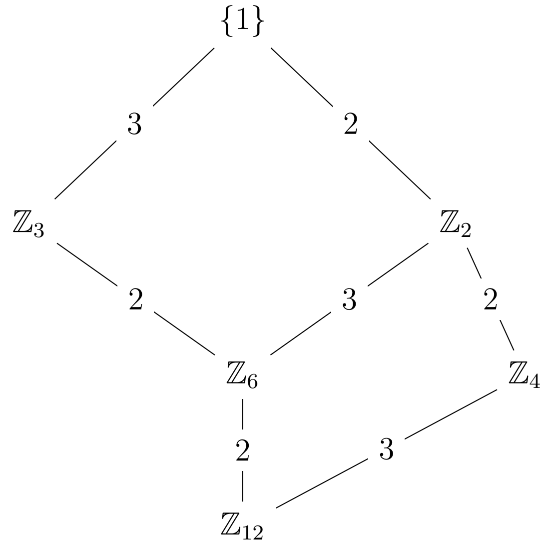
Muestre que un subcuerpo de $\mathbb{F}_{p^n}$ tiene orden p^d donde $d|n$ y existe un subcuerpo para cada tal d.

Dem: Por el ejercicio anterior, sabemos que $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es un grupo cíclico de n elementos. Por resultados de teoría de grupos, sabemos que tenemos un subgrupo H tq' $|H| = d$ por cada $d|n$

Ahora bien, por el teorema fundamental de Galois, sabemos a hay una biyección entre subgrupos de G y subcuerpos de $\mathbb{F}_{p^n}$. Mas aun, a cada subcuerpo E de $\mathbb{F}_{p^n}$ le corresponde un único subgrupo H de G que lo fija y viceversa. Además, por el mismo teorema, también sabemos que $[E : \mathbb{F}_p] = |G : H|$. Por lo tanto, sea $k \leq n$ arbitrario tq' $ke = n$, tenemos que existe $H \leq G$ de k elementos y, por teo. de Galois, tenemos que $E = K^H$ es tal que $[E : \mathbb{F}_p] = \frac{n}{k} = e$. Luego, aplicando el resultado obtenido en el primer ejercicio, $|E| = p^e$. De manera similar, si queremos obtener ahora el subcuerpo con p^k elementos basta con tomar $H \leq G$ tq' $|H'| = e$ y determinar su subcuerpo fijo $E' = K^{H'}$, el cual tendrá cardinalidad p^k por los mismos argumentos ya explicados. De manera similar, se pueden obtener los demas subcuerpos de $\mathbb{F}_{p^n}$ a partir de los divisores de n.

Finalmente, llegamos a que, por el teorema de Galois, todos los subcuerpos de $\mathbb{F}_{p^n}$ deben ser subcuerpo fijo de algún subgrupo de G. Luego, por lo mostrado, cada uno es de la forma $\mathbb{F}_{p^d}$ y existe un único de ellos por cada $d|n$.





(5)

Dibuje el Diagrama de subcuerpos de $\mathbb{F}_{p^{12}}$ y el diagrama de subgrupos de $\mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p)$

Para el diagrama anterior, hacemos la siguiente simplificación. Sabemos que el grupo cíclico de 12 elementos de $\mathbb{F}_{p^{12}}$ es isomorfo a $\mathbb{Z}_{12}$. Además, se encuentra ordenado para que el subgrupo coincida con su subcuerpo fijo del diagrama de subcuerpos.