

UNA NOTA SOBRE EL NUMERO DE SOLUCIONES DE ECUACIONES
CON COEFICIENTES MATRICIALES

por

Víctor S. ALBIS GONZALEZ

Consideremos el anillo

$$A = \left\{ \begin{pmatrix} \lambda & \alpha \\ 0 & \lambda \end{pmatrix} \in M_2(\mathbb{F}_p) : \alpha, \lambda \in \mathbb{F}_p \right\}$$

donde \mathbb{F}_p designa el cuerpo $\mathbb{Z}/(p)$. Es claro que A_p es un anillo conmutativo finito con elemento unidad. Sean ahora $A_p[t]$ el anillo de los polinomios en la indeterminada t con coeficientes en A_p y

$$f(t) = \sum_{k=0}^n a_k t^k \in A_p[t] \quad , \quad a = \begin{bmatrix} \lambda_k & \alpha_k \\ 0 & \lambda_k \end{bmatrix} ,$$

un polinomio de grado n . Usando el siguiente teorema [1]

TEOREMA 1.- Sean B un anillo conmutativo finito con elemento unidad y k un cuerpo finito. Sea $\mu : B \rightarrow k$ un epimorfismo de anillos y $N = \text{card}[ker \mu]$. Entonces, si $f(t) = \sum_{k=0}^n a_k t^k$ es tal que $a_k \notin ker \mu$, para algún $k=0, 1, \dots, n$, $f(t)$ tiene a lo más n/N raíces distintas o no en B .

obtenemos el

TEOREMA 2.- Sea $f(t) = \sum_{k=0}^n a_k t^k \in A_p[t]$ un polinomio de grado n tal que $\lambda_k \neq 0$ para algún $k=0, 1, \dots, n$. Entonces $f(t)$ tiene a lo más pn raíces de la forma

$$\begin{pmatrix} \lambda & \alpha \\ 0 & \lambda \end{pmatrix}$$

Demostración: La aplicación $\mu : A_p \rightarrow \mathbb{F}_p$ definida por

$$\begin{pmatrix} \lambda & \alpha \\ 0 & \lambda \end{pmatrix} \longmapsto \lambda$$

es un epimorfismo ; como

$$\mu = \left\{ \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} ; \lambda \in \mathbb{F}_p \right\}$$

y $\text{card}[ker \mu] = p$, resulta el teorema 2.

Por otra parte, consideremos el polinomio

$$f(t) = \sum_{k=0}^n \begin{pmatrix} \lambda_k & \alpha_k \\ 0 & \lambda_k \end{pmatrix} \cdot t^k \in A_p[t]$$

Es fácil comprobar que

$$\begin{pmatrix} \lambda & \alpha \\ 0 & \lambda \end{pmatrix} \in A_p$$

es una raíz de $f(t)$ si y sólo si $b(\lambda) = 0$ y $\alpha b'(\lambda) + g(\lambda) = 0$, donde $g(t) = \sum_{k=0}^n \alpha_k t^k$ y $b(t) = \sum_{k=0}^n \lambda_k t^k$. Ahora bien existen a lo más n valores de λ en F_p tales que $b(\lambda) = 0$, a menos que $b(t) \equiv 0$. Así mismo α está determinado de manera única por λ a menos que $b'(\lambda) = 0$. Esto muestra que la cota p^n sirve para todos los polinomios $f(t) \in A_p[t]$.

Dado un polinomio $f(t) \in A_p[t]$ no hay que pensar que todas sus raíces en $\mathfrak{M}_2(F_p)$ pertenecen a A_p . Por ejemplo,

$$f(t) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} t^2 \in A_p[t]$$

tiene como raíz en $\mathfrak{M}_2(F_p)$ a

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

Sería interesante investigar bajo qué condiciones $f(t) \in A_p[t]$ tiene todas sus raíces en A_p . Quiero agradecer aquí al profesor R. MacRae algunas sugerencias que han mejorado la presentación de esta nota.

REFERENCIAS

- [1]. V. ALBIS, "A certain class of rings and the number of roots of polynomials with coefficients in these rings", (to appear)

Departamento de Matemáticas y Estadística
 Universidad Nacional de Colombia
 Bogotá, Colombia, S. A.
 (Recibido en abril de 1969)