GyA - Tarea 2

Jose Antonio Lorencio Abril

3/04/2020

3.2.16. En el problema 2.1.12 se ha visto que el cardinal de un cuerpo finito K es una potencia de un número primo (de hecho una potencia de la característica de K). En este problema, fijado un entero primo positivo p, vamos a ver que existen cuerpos de cardinal $p^n, \forall n \in \mathbb{Z}^+$.

(1) Sea K un cuerpo de característica $p, n \in \mathbb{Z}^+$. Demostrar que el conjunto de las raíces en K del polinomio $x^{p^n} - x$ es un subcuerpo finito de K.

El ejercicio 2.1.11 nos dice que

$$\begin{aligned} f:\ & K \to K \\ & x \mapsto x^{p^n} \end{aligned}$$

es un endomorfismo de $K, \forall n \in \mathbb{Z}^+$.

Sea $A = \{a \in K :\ a^{p^n} - a = 0\}$

¿Es A un subcuerpo de K? Lo será si, y solo si, es un subanillo. Veámoslo.

- ¿$1 \in A$?

$$1^{p^n} - 1 = 1 - 1 = 0 \qquad \checkmark$$

- ¿$a, b \in A \implies a + b \in a$?

$$(a+b)^{p^n} - (a+b) = \sum_{k=0}^{p^n} \left(\begin{array}{c} p^n \\ k \end{array} \right) a^{p^n-k} b^k - (a+b) =$$

$$= a^{p^n} + \left(\begin{array}{c} p^n \\ 1 \end{array} \right) a^{p^n-1} b + ... + \left(\begin{array}{c} p^n \\ p^n - 1 \end{array} \right) a b^{p^n-1} + b^{p^n} - (a + b = *$$

Todos los factores entre a^{p^n}, b^{p^n} tienen al menos una p multiplicando, porque p es primo y, por tanto, p^n siempre dejará un factor p, pues su mayor divisor distinto de sí mismo es p^{n-1}. Por tanto

$$* = a^{p^n} + b^{p^n} - (a+b) = (a^{p^n} - a) + (b^{p^n} - b) = 0 - 0 = 0 \qquad \checkmark$$

- ¿$a, b \in A \implies a \cdot b \in A$?

Primero nótese que

$$a^{p^n} - a = 0 \iff a^{p^n} = a$$
$$b^{p^n} - b = 0 \iff b^{p^n} = b$$

Entonces

$$(ab)^{p^n} - ab = a^{p^n} b^{p^n} - ab = ab - ab = 0 \qquad \checkmark$$

Así, A es subanillo de K. Por lo que A es subcuerpo de K. Como K es finito, entonces A también lo es.

(2) Deducir que, $\forall n \in \mathbb{Z}^+$, existe un cuerpo de cardinal p^n.

Sea K un cuerpo de característica p.

$$x^{p^n} - x \in K[x] - K$$

Así, por el ejercicio 3.2.15, existe un cuerpo K' que contiene a K como subcuerpo y P es producto de polinomios de grado 1 con coeficientes en K.

Como el grado del polinomio es p^n, entonces será producto de p^n polinomios de grado 1. Es decir, tendrá p^n raíces.

Por el apartado 1, el conjunto A de estas raíces es un cuerpo. Al haber p^n raíces, $|A| = p^n$.

3.3.1. ¿Es cierto que, si D es un DFU y b es un elemento de D, entonces solo hay una cantidad finita de ideales de D que contienen a b? ¿Y si D es DIP?

Veamos primero el caso en que ***D* es DIP**, en particular, también es DFU.

Entonces

$$b = u \cdot p_1 \cdot ... \cdot p_n$$

De forma única. Esto quiere decir que

$$b \in (u) = D, (p_1), ..., (p_n)$$

y a sus intersecciones. Como D es DIP, estos son todos los ideales que lo contienen. En efecto, supongamos $I \lhd D$ distinto de los anteriores.

Entonces, como es DIP, $I = (a)$.

$$b \in (a) \iff up_1 \cdot ... \cdot p_n = b = c \cdot a \overset{D\ DFU}{\Longrightarrow} \begin{cases} c = u_c p_{c1} \cdot ... \cdot p_{cm} \\ a = v_a p_{a1} \cdot ... \cdot p_{ak} \\ m + k = n \end{cases}$$

En concreto, se tiene que, agrupando los factores repetidos, $(a) = (p_{a1}^{\alpha 1} \cdot ... \cdot p_{ak}^{\alpha k}) = (p_{a1}^{\alpha 1}) \cap ... \cap (p_{ak}^{\alpha k})$. Por lo que I es como los anteriores.

Si ***D* es DFU**. Vamos a ver un contraejemplo.

$$\mathbb{Z}\ DFU \iff \mathbb{Z}[x]\ DFU \iff \mathbb{Z}[x][y]\ DFU$$

Pero este último no es DIP, por la proposición 3.13.

Es más,

$$x \in (x, y), (x, y^2), (x, y^3), ...$$

Una cantidad infinita de ideales, distintos, pues $y^{n-1} \notin (x, y^n)$.

3.4.1. Sea D un DFU y sea $f = a_0 + a_1x + ... + a_nx^n$ un polinomio primitivo en $D[x]$. Demostrar que, si existe un irreducible $p \in D$ tal que

$$p|a_i \ \forall i > 0, \qquad p \nmid a_0, \qquad p^2 \nmid a_n$$

entonces f es irreducible en $D[x]$.

Pensemos $f = g \cdot h$. ¿Será $gr(g) = n$ ó $gr(f) = n$?

$$g = b_0 + ... + b_mx^m, \qquad h = c_0 + ... + c_kx^k, \qquad b_mc_k \neq 0$$

Por otro lado,

$$p^2 \nmid a_n = b_mc_k \implies p \nmid b_m \qquad \text{ó} \qquad p \nmid c_k$$

Supongamos que $p \nmid c_k$. Como f es primitivo, entonces $p \nmid g$, pues si
$p|g \overset{g|f}{\implies} p|f \implies f$ *no primitivo*, pero esto no es así.

Entonces, tomamos

$$i = \max\{j : p \nmid b_j\}$$

Consideremos ahora

$$a_{i+k} = \sum_{j=0}^{i+k-1} b_jc_{i+k-j} + b_{i+k}c_0$$

Como $gr(c) = k$, $c_{i+k-j} = 0 \, \forall j < i$. Por lo que

$$a_{i+k} = \sum_{j=i}^{i+k-1} b_jc_{i+k-j} + b_{i+k}c_0$$

Entonces, tenemos que $p|b_jc_{i+k-j}$, $\forall j > i$, ya que i es el máximo de los b_j que no son divisibles por p. Es decir, p divide a todos los sumandos de a_{i+k}, excepto a b_ic_k:

$$a_{i+k} = b_ic_k + S \cdot p$$

Donde S es lo que queda al sacar p factor común en todo el sumatorio. Tenemos, de esta manera, que $p \nmid a_{i+k}$, pero esto quiere decir que $i + k = 0$. Al ser ambos números no negativos, queda $i = 0 = k$. Es decir, $gr(h) = 0 \implies gr(g) = n$

Si hacemos el otro caso, $p \nmid b_m$, obtendremos $gr(h) = n$.

Tal y como queríamos ver, f es irreducible.