ALGEBRA III (Doble grado Informática-Matemáticas)

Cuerpos Finitos

Sobre cuerpos de característica positiva.

Si F es un cuerpo cualquiera, como en cualquier anillo conmutativo, tenemos definido el producto na de enteros $n \geq 0$ por elementos $a \in F$: Si $n = 0$, entonces $0a = 0$, y si $n > 0$, entonces $na = \sum_{i=1}^{n} a = a + \overset{n}{\cdots} + a$ es la suma reiterada de ese elemento a consigo mismo n veces. Recordemos también que, para cualesquiera $m, n \geq 0$ y $a, b \in F$, se verifican (entre otras) las igualdades

(1) $1a = a$,
(2) $(m+n)a = ma + na$,
(3) $m(na) = (mn)a$,
(4) $(ma)(nb) = (mn)(ab)$.
(5) $(ma)b = m(ab) = a(mb)$.

Fijándonos en el caso en $a = 1 \in F$, los diferentes productos $n1 = 1 + \overset{n}{\cdots} + 1$, para $n \geq 0$, no tienen por qué ser todos distintos (por ejemplo, si F es finito no podrán serlo). En ese caso, existirán enteros $m > n \geq 0$ tales que $m1 = n1$. Pero entonces, si $m = n + k$, será $n1 + k1 = n1$ y $k1 = 0$. Luego existe un $k \geq 1$ tal que $k1 = 0$. Sea

$$p = \min\{k \geq 1 \mid k1 = 0\}.$$

Notemos que ha de ser $p \geq 2$, pues si fuese $p = 1$ sería $1 = 0$ en F, y en un cuerpo esto no se puede dar. Este número p **es primo**: Supongamos por el contrario que no es primo o, equivalentemente, que no es irreducible. Será $p = mn$, con $m, n < p$. Pero entonces $(m1)(n1) = (mn)1 = p1 = 0$. Como F es un cuerpo, será $m1_F = 0$ o $n1_F = 0$. Pero ninguna de estas igualdades puede darse al ser $m, n < p$. A este número primo p se le llama la **característica del cuerpo** F.

Por ejemplo, para cualquier número primo $p \geq 2$, $\mathbb{Z}_p$ es un cuerpo de característica p. Recordemos las operaciones de suma y producto en $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$: Si, para cualquier entero $n \in \mathbb{Z}$ denotamos por $\overline{n}$ al resto de dividir n entre p, entonces, $\overline{n} = n$ si $0 \leq n \leq p-1$ y la suma y producto en $\mathbb{Z}_p$ está determinada por que para cualesquiera $m, n \in \mathbb{Z}$

$$\overline{m} + \overline{n} = \overline{m+n}, \qquad \overline{m}\ \overline{n} = \overline{mn}.$$

En particular, si $1 \leq k < p$, en $\mathbb{Z}_p$, $k1 = \overline{k} = k \neq 0$, mientras que $p1 = \overline{p} = 0$. Así que la característica de $\mathbb{Z}_p$ es, en efecto, p. Si $F/\mathbb{Z}_p$ es cualquier extensión, entonces la característica de F es también p (tienen el mismo 1 y se suma consigo mismo en F como en $\mathbb{Z}_p$).

Lema 1. *Sea F un cuerpo de característica p. Para cualesquiera $m, n \geq 0$, se verifica que*

$$m1 = n1 \Leftrightarrow m \equiv n \mod (p) \Leftrightarrow \overline{m} = \overline{n}.$$

En particular,

(1) $m1 = \overline{m}\,1$.
(2) $m1 = 0 \Leftrightarrow p/n$.

Demostración. Supongamos $m \geq n$, $m = n + k$. Si $m \equiv n \mod (p)$, será $k = qp$. Entonces $m1 = n1 + q(p1) = n1$, pues $p1 = 0$. Y, recíprocamente, si $m1 = n1$, será $n1 + k1 = n1$ y $k1 = 0$. Pongamos $k = pq + r$, con $0 \leq r < p$. Entonces $r1 = 0$ y, como $r < p$, ha de ser $r = 0$. Así que $p \mid k$ y $m \equiv n \mod (p)$. □

Las conclusiones del lema anterior son válidas para cualquier elemento $0 \neq a \in F$:

Lema 2. *Sea F un cuerpo de característica p. Para cualesquiera $m, n \geq 0$ y $0 \neq a \in F$, se verifica que*

$$ma = na \Leftrightarrow m \equiv n \mod (p) \Leftrightarrow \overline{m} = \overline{n}.$$

En particular,

(1) $ma = \overline{m}\, a$.
(2) $ma = 0 \Leftrightarrow p/n$.

Demostración. $ma = na \Leftrightarrow (ma)a^{-1} = (na)a^{-1} \Leftrightarrow m(aa^{-1}) = n(aa^{-1}) \Leftrightarrow m1 = n1$, y basta aplicar el lema anterior. □

Teorema 3. *Sea F un cuerpo de característica p. La aplicación $\sigma : \mathbb{Z}_p \to F$ definida por*

$$\sigma(n) = n1, \qquad n = 0, 1, \ldots, p-1,$$

es una inmersión, y es la única que hay de $\mathbb{Z}_p$ en F.

Demostración. Claramente $\sigma(0) = 0$ y $\sigma(1) = 1$. Además, para cualesquiera $m, n \in \mathbb{Z}_p$,

$$\sigma(m) + \sigma(n) = (m1) + (n1) = (m+n)1 = \overline{m+n}\,1 = \sigma(\overline{m+n}),$$
$$\sigma(m)\,\sigma(n) = (m1)\,(n1) = (mn)1 = \overline{m\,n}\,1 = \sigma(\overline{m\,n}).$$

Si $\sigma' : \mathbb{Z}_p \to F$ es cualquier otra supuesta inmersión, para todo $0 \leq n \leq q-1$, será $\sigma'(n) = \sigma'(n1) = n\sigma'(1) = n1 = \sigma(n)$, luego $\sigma' = \sigma$. □

La inmersión $\sigma : \mathbb{Z}_p \to F$ es estándar, y la consideramos siempre como una inclusión. Con esta identificación en mente, tenemos demostrado la primera afirmación del siguiente

Teorema 4. (*i*) *Un cuerpo es de característica p si y solo si es una extensión de $\mathbb{Z}_p$.*

(*ii*) *Si F es un cuerpo de característica p, E es un cuerpo de característica q, y $p \neq q$, entonces no existe ninguna inmersión $F \to E$.*

(*iii*) *Si E, F son cuerpos de característica p, toda inmersión $\sigma : F \to E$ es una $\mathbb{Z}_p$-inmersión, esto es, $\sigma|_{\mathbb{Z}_p} = id$.*

Demostración. (*ii*) Si $\sigma : F \to E$ fuese un homomorfismo, tendríamos que $0 = \sigma(0) = \sigma(p1) = p\sigma(1) = p1 \in E$. Pero entonces $q \mid p$, lo que no es posible al ser primos positivos distintos.

(*iii*) Sea $\sigma : F \to E$ un homomorfismo, entonces, para cualquier $m \in \mathbb{Z}_p$,

$$\sigma(m) = \sigma(m1) = m\sigma(1) = m1 = m.$$

□

Existencia y unicidad de cuerpos finitos.

Un cuerpo finito necesariamente será de característica p, para p un primo positivo de $\mathbb{Z}$, y entonces una extensión, también necesariamente finita, de $\mathbb{Z}_p$. Esto nos limita las posibilidades del tamaño del cuerpo F a ser una potencia del primo p.

Teorema 5. *Si F un cuerpo finito, entonces $|F| = p^n$, donde p es su característica y $n = [F : \mathbb{Z}_p]$.*

Demostración. Sea $\{a_1, ..., a_n\}$ una base de F como espacio vectorial sobre $\mathbb{Z}_p$. Cada elemento $a \in F$ se escribe de forma única como $a = m_1 a_1 + ... + m_n a_n$, con $m_i \in \mathbb{Z}_p$. Consecuentemente, el número total de elementos de F es p^n. □

Lema 6. *Sea E un cuerpo de característica p donde el polinomio $x^{p^n} - x$ descompone totalmente. Entonces el subconjunto de E formado por todas las raíces de ese polinomio es un subcuerpo con p^n elementos.*

Demostración. Sea $F \subseteq E$ el subconjunto de todas las raíces de ese polinomio. Esto es, $F = \{\alpha \in E \mid \alpha^{p^n} = \alpha\}$. Notemos que el polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ tiene exactamente p^n raíces distintas en E, ya que no tiene raíces múltiples al ser su derivado $(x^{p^n} - x)' = -1$ primo relativo con él (notar que $px = 0$, pues $px = \sum_1^p x = (\sum_1^p 1)x = (p1)x = 0x = 0$). Veamos que F es un subcuerpo de E: Claramente $0, 1 \in F$. Puesto que E es de característica p, para cualesquiera $\alpha, \beta \in E$

$$(\alpha + \beta)^p = \sum_{i=0}^{p} \binom{p}{i} \alpha^i \beta^{p-i} = \sum_{i=0}^{p} \overline{\binom{p}{i}} \alpha^i \beta^{p-i} = \alpha^p + \beta^p,$$

de donde se deduce que $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$. Entonces, si $\alpha, \beta \in F$, es $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ y, por tanto $\alpha + \beta \in F$. Vemos también que $\alpha\beta \in F$, pues $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$. Además, si $0 \neq \alpha \in F$ entonces $-\alpha, \alpha^{-1} \in F$, pues $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = (-1)\alpha = -\alpha$ y $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. □

Puesto que siempre existe una extensión $E/\mathbb{Z}_p$ donde el polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ descompone totalmente, obtenemos el siguiente importante resultado.

Teorema 7. *Para cada primo p y cada entero $n \geq 1$ existe un cuerpo con p^n elementos.*

La obtención anterior de un cuerpo con p^n elementos cuyos elementos son todas las raíces del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ no es fruto de especial ingenio. Esa propiedad la tienen todos los cuerpos con p^n elementos.

Lema 8. *Si F es un cuerpo finito con p^n elementos, todos los elementos de F son raíces del polinomio $x^{p^n} - x$ y este polinomio tiene todas sus raíces en F, así que en $F[x]$ se tiene que $x^{p^n} - x = \prod_{\alpha \in F}(x - \alpha)$.*

Demostración. Puesto que $|F^\times| = p^n - 1$, y en un grupo finito el orden de cualquier elemento divide al orden del grupo, para todo $\alpha \in F^\times$, será $\alpha^{p^n-1} = 1$ y, por tanto, $\alpha^{p^n} = \alpha$ para todo $\alpha \in F$. □

El saber que los elementos de un cuerpo finito con p^n elementos son necesariamente las diferentes raíces del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ no nos dice mucho sobre la estructura de ese cuerpo, esto es, sobre como se representan sus elementos y sobre como se suman o multiplican estos entre si. Para poder precisar esto, nos ayuda el siguiente lema.

Lema 9. *Si K es un cuerpo, cualquier subgrupo finito del grupo multiplicativo $K^\times$ es cíclico.*

Demostración. Supongamos, por el contrario que $G \leq K^\times$ es un subgrupo finito que no es cíclico. Por el Teorema de Estructura de grupos abeliano finitos, sería $G \cong C_{d_1} \times \cdots \times C_{d_r}$, isomorfo a un producto de cíclicos de ordenes $d_1, \ldots, d_r$, donde cada $d_i \geq 2$, $d_i \mid d_{i+1}$ y $r > 1$. Pero entonces, para todo $\alpha \in G$, se tendría que $\alpha^{d_r} = 1$, y todo elemento de G sería una raíz del polinomio $x^{d_r} - 1$. Entonces $|G| \leq d_r$. Pero de la igualdad $d_1 \cdots d_r = |G|$, donde $d_1 \geq 2$ y $r > 1$, se deduce que $d_r < |G|$, lo que es una contradicción. □

Teorema 10. *Todo cuerpo finito de característica p es una extensión simple de $\mathbb{Z}_p$*

DEMOSTRACIÓN. El grupo $F^\times$ es cíclico. Supongamos que α es un generador de $F^\times$ y consideremos el subcuerpo $\mathbb{Z}_p(\alpha) \leq F$. Puesto que todo elemento no nulo de F es una potencia de α y pertenece a $\mathbb{Z}_p(\alpha)$, concluimos que $F = \mathbb{Z}_p(\alpha)$. □

Corolario 11. *Para todo número primo p y todo $n \geq 1$, existe un polinomio en $\mathbb{Z}_p[x]$ que es irreducible de grado n.*

DEMOSTRACIÓN. Sea F un cuerpo con p^n elementos. Será $F = \mathbb{Z}_p(\alpha)$ para algún $\alpha \in F$. Como $[F : \mathbb{Z}_p] = n$, el polinomio $Irr(\alpha, \mathbb{Z}_p)$ será de grado n. □

La anterior propiedad es cierta para $\mathbb{Q}$ (considerar los polinomios $(x^n - 2)$, pero claramente no es cierta para todos los cuerpos, por ejemplo en $\mathbb{C}[x]$ o en $\mathbb{R}[x]$. En este segundo caso no hay irreducibles de grado ≥ 3: Si f fuese un tal polinomio, que podemos suponer mónico, este tendría una raíz α en $\mathbb{C}$, sería $f = Irr(\alpha, \mathbb{R})$ y $[\mathbb{R}(\alpha) : \mathbb{R}] \geq 3$. Pero desde la torre $\mathbb{R} \leq \mathbb{R}(\alpha) \leq \mathbb{C}$, vemos que $[\mathbb{R}(\alpha) : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$.

La siguientes observaciones ya nos prepara para precisar como describir los cuerpos finitos.

Lema 12. *Sea $p \geq 2$ un primo. Cualquier polinomio $f \in \mathbb{Z}_p[x]$ irreducible de grado n es un divisor de $x^{p^n} - x$.*

DEMOSTRACIÓN. Podemos suponer que f es mónico. Sea $E/\mathbb{Z}_p$ una extensión donde f descompone totalmente. Sea $\beta \in E$ una raíz de f, y sea $F = \mathbb{Z}_p(\beta) \leq E$. Puesto que $f = Irr(\beta, \mathbb{Z}_p)$, será $[F : \mathbb{Z}_p] = n$ y, por tanto, F es un cuerpo con p^n-elementos. Entonces β es una raíz de $x^{p^n} - x$ en F, y ha de ser $f \mid x^{p^n} - x$ en $\mathbb{Z}_p[x]$. □

Corolario 13. *Sea F un cuerpo con $|F| = p^n$. Cualquier polinomio $f \in \mathbb{Z}_p[x]$ irreducible de grado n descompone totalmente en F.*

DEMOSTRACIÓN. Sabemos que $x^{p^n} - x$ tiene todas sus raíces F. Como f es un divisor suyo, f también las tiene. □

Teorema 14. *Sea F un cuerpo con $|F| = p^n$ y $f \in \mathbb{Z}_p[x]$ cualquier polinomio mónico e irreducible de grado n. Si designamos por α cualquier raíz de f en F, entonces*

(1) $F = \mathbb{Z}_p(\alpha)$.
(2) *Los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, forman una base de $F/\mathbb{Z}_p$. Por tanto,*
$$F = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}_p\},$$
donde la expresión de cada elemento de F de tal forma es única.
(3) *Todo elemento de F es expresable como $g(\alpha)$, para algún polinomio $g \in \mathbb{Z}_p[x]$. Si $g \in K[x]$ es cualquier polinomio tal que $g(\alpha) = \beta$, entonces la expresión de β en función de la base es*
$$\beta = r(\alpha) = \textstyle\sum_{i=0}^{n-1} c_i\alpha^i,$$
donde $r = \sum_{i=0}^{n-1} c_i x^i$ es el resto de dividir g entre f.
(4) *Si $g, h \in K[x]$ son polinomios tal que $g(\alpha) = \beta$ y $h(\alpha) = \gamma$, entonces*
$$\begin{cases} \beta + \gamma = (g + h)(\alpha), \\ \beta\gamma = (gh)(\alpha). \end{cases}$$
Además, si $0 \neq \beta = g(\alpha)$, existen polinomios $u, v \in K[x]$ tal que $1 = gu + fv$ y se verifica que
$$\beta^{-1} = u(\alpha).$$

*La descripción anterior del cuerpo F solo depende del polinomio f y del símbolo α usado para referirnos a una de sus raíces en F. Nos referimos a esta como "***La descripción de F en la clave (α, f)***"*

Demostración. Puesto que será $f = Irr(\alpha, \mathbb{Z}_p)$. Tendremos entonces que $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n = [F : \mathbb{Z}_p]$, de donde se deduce que $F = \mathbb{Z}_p(\alpha)$, y todo lo anunciado ya nos es conocido. □

Corolario 15. *Sean F y F' dos cuerpos con p^n elementos. Supongamos que F está descrito por la clave (α, f). Entonces, para cualquier raíz α' de f en F' hay un isomorfismo $\varphi : F \cong F'$ tal que $\varphi(\alpha) = \alpha'$.*

Demostración. Si describimos F' en la clave (α', f), resulta obvio que la aplicación $\psi : F \to F'$ definida por

$$\psi(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = (a_0 + a_1\alpha' + \cdots + a_{n-1}\alpha'^{n-1})$$

es un isomorfismo (el único que hay tal que $\psi(\alpha) = \alpha'$). □

Teorema 16. *Dos cuerpos finitos con el mismo cardinal son isomorfos.*

Demostración. Sean F y F' cuerpos con p^n elementos. Sea $f \in \mathbb{Z}_p[x]$ cualquier mónico irreducible de grado n. Por el teorema anterior existen raíces $\alpha \in F$ y $\alpha' \in F'$ de f. Entonces, por el corolario anterior, hay un isomorfismo $\varphi : F \cong F'$ tal que $\varphi(\alpha) = \alpha'$ □.

Usualmente, se denota por

$$\mathbb{F}_{p^n}$$

al único (salvo isomorfismo) cuerpo con p^n elementos. En particular $\mathbb{F}_p = \mathbb{Z}_p$.

El retículo de subcuerpos de $\mathbb{F}_{p^n}$.

Para describir el retículo de subcuerpos $Sub(\mathbb{F}_{p^n}) = Sub(\mathbb{F}_{p^n}/\mathbb{F}_p)$, usaremos el siguiente lema:

Lema 17. *(i) Para cualesquiera enteros $m \geq 2$ y $\ell \geq k \geq 1$, se verifica que*

$$m^k - 1 \mid m^\ell - 1 \Leftrightarrow k \mid \ell.$$

(ii) Sea K es un cuerpo. Para cualesquiera enteros $\ell \geq k \geq 1$, se verifica que

$$x^k - 1 \mid x^\ell - 1 \text{ en } K[x] \Leftrightarrow k \mid \ell$$

y para $m \geq 2$ se verifica que

$$x^{m^k} - x \mid x^{m^\ell} - x \text{ en } K[x] \Leftrightarrow k \mid \ell.$$

Demostración.

(i) Notemos que, obviamente, $m^k \equiv 1 \mod (m^k - 1)$. Si $k \mid \ell$, poniendo $\ell = qk$, tenemos que $m^\ell - 1 = (m^k)^q - 1 \equiv 1^q - 1 = 0 \mod (m^k - 1)$. Por tanto $m^k - 1 \mid m^\ell - 1$. Recíprocamente, supongamos que $m^k - 1 \mid m^\ell - 1$, o sea que $m^\ell - 1 \equiv 0 \mod (m^k - 1)$, y que $k \nmid \ell$. Poniendo $\ell = qk + r$, con $0 < r < k$, tenemos que

$$m^\ell - 1 = (m^k)^q m^r - 1 \equiv m^r - 1 \mod (m^k - 1),$$

luego ha de ser $m^r - 1 \equiv 0 \mod (m^k - 1)$, o sea que $m^k - 1 \mid m^r - 1$. Pero esto implica que $m^k - 1 \leq m^r - 1$, o sea que $m^k \leq m^r$, lo que no es posible pues $0 < r < k$ y $m \geq 2$.

(ii) Es similar: Pongamos $\ell = qk + r$ con $0 \leq r < k$. Como, obviamente, $x^k \equiv 1 \mod (x^k - 1)$, tenemos que $x^\ell - 1 = (x^k)^q x^r - 1 \equiv x^r - 1 \mod (x^k - 1)$. Entonces

$$x^k - 1 \mid x^\ell - 1 \Leftrightarrow x^\ell - 1 \equiv 0 \mod (x^k - 1) \Leftrightarrow x^r - 1 \equiv 0 \mod (x^k - 1)$$
$$\Leftrightarrow x^k - 1 \mid x^r - 1 \Leftrightarrow r = 0 \Leftrightarrow k \mid \ell.$$

La tercera afirmación es consecuencia de las partes anteriores: Tenemos que

$$x^{m^k} - x \mid x^{m^\ell} - x \Leftrightarrow x^{m^k-1} - 1 \mid x^{m^\ell-1} - 1 \Leftrightarrow m^k - 1 \mid m^\ell - 1 \Leftrightarrow k \mid \ell.$$

□

Teorema 18. *Sea p un primo.*

(1) *Para cada divisor positivo d de n, el cuerpo $\mathbb{F}_{p^n}$ contiene exactamente un subcuerpo con p^d elementos, $\mathbb{F}_{p^d}$, y estos son sus únicos subcuerpos. Esto es,*

$$\mathrm{Sub}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{\mathbb{F}_{p^d},\ \textit{donde } d \geq 1,\ \textit{y } d \mid n\}.$$

(2) *Para cada $d \mid n$, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = \frac{n}{d}$.*

(3) *Si $d_1, d_2 \mid n$, se tiene que $\mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p^{d_2}} \Leftrightarrow d_1 \mid d_2$.*

Demostración. (1) Si $F \leq \mathbb{F}_{p^n}$, será $|F| = p^d$, para un cierto $d \geq 1$. La torre de extensiones $\mathbb{F}_p \leq F \leq \mathbb{F}_{p^n}$, nos asegura que $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : F][F : \mathbb{F}_p] = [\mathbb{F}_{p^n} : F]\, d$, de donde necesariamente $d \mid n$.

Supongamos que $d \mid n$. Entonces $x^{p^d} - x \mid x^{p^n} - x$ en $\mathbb{Z}_p[x]$. Como $x^{p^n} - x$ descompone totalmente en $\mathbb{F}_{p^n}$, $x^{p^d} - x$ también lo hace. Sabemos entonces que las diferentes raíces de este polinomio en $\mathbb{F}_{p^n}$ forman un subcuerpo con p^d elementos. Podemos denotar a este por $\mathbb{F}_{p^d}$, ya que es el único subcuerpo de $\mathbb{F}_{p^n}$ de tal orden: si $F \leq \mathbb{F}_{p^n}$ es cualquier supuesto subcuerpo con $|F| = p^d$, sabemos que todo elemento de F es raíz del polinomio $x^{p^d} - x$ y, por tanto, $F \subseteq \mathbb{F}_{p^d}$, de donde concluimos que $F = \mathbb{F}_{p^d}$ por cardinalidad.

(2) La torre $\mathbb{F}_p \leq \mathbb{F}_{p^d} \leq \mathbb{F}_{p^n}$ nos dice que

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]\,[\mathbb{F}_{p^d} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]\, d$$

de donde la conclusión es clara.

(3) Sean $d_1, d_2 | n$. Si $\mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p_2^d}$, tomando grados en la torre $\mathbb{F}_p \leq \mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p^{d_2}}$, deducimos que $d_1 | d_2$. Y recíprocamente, si $d_1 | d_2$ entonces $\mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p^{d_2}}$ pues $x^{p^{d_1}} - x \mid x^{p^{d_1}} - x$. □

Una interesante consecuencia es la siguiente:

Proposición 19. (1) *Si $m \mid n$, entonces todo polinomio irreducible de grado m en $\mathbb{F}_p[x]$ descompone totalmente en $\mathbb{F}_{p^n}$.*

(2) *Si $m \nmid n$, entonces un polinomio irreducible de grado m en $\mathbb{F}_p[x]$ no tiene ninguna raíz en $\mathbb{F}_{p^n}$.*

Indicación de solución: (1) Sabemos que todo polinomio irreducible de grado m en $\mathbb{F}_p[x]$ descompone totalmente en $\mathbb{F}_{p^m}$. Si $m \mid n$, entonces $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$ y la conclusión es clara.

(2) Si $f \in \mathbb{F}_p[x]$ es irreducible de grado m y tiene una raíz α en $\mathbb{F}_{p^n}$, entonces $\mathbb{F}_p(\alpha) \leq \mathbb{F}_{p^n}$ es un subcuerpo. Pero como $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$, sería $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$. Luego tendríamos que $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$, lo que no puede ser ya que $m \nmid n$.