ALGEBRA II

Licenciatura en Ciencias Matemáticas

1. Probar que si p es un primo y $p \geq 3$ entonces

$$p \text{ divide a } 2^{2p-1} - 2.$$

Solución.
Se tiene que

$$2^{p-1} \equiv 1 \bmod(p),$$

elevando al cuadrado

$$2^{2(p-1)} \equiv 1 \bmod(p)$$

y multiplicando por 2:

$$2^{2p-1} \equiv 2 \bmod(p),$$

de donde el enunciado.

2. Sean A y B dos anillos y $f : A \to B$ un morfismo entre ellos. Sea p un ideal de B y denotemos con q al ideal de A siguiente:

$$q = f^{-1}(p) = \{a \in A : f(a) \in p\}.$$

a) Probar que si p es primo entonces q también lo es.
b) ¿Es cierto lo anterior sutituyendo primo por maximal? Pruébese o propóngase un contraejemplo.

Solución.
El apartado a) está resuelto en la colección "Problemas de ideales".
Construyamos un contraejemplo al apartado b).
Consideremos la inyección de anillos

$$i : Z[T] \hookrightarrow Q[T];$$

entonces el ideal $p = (T)$ es maximal en $Q[T]$ pues $Q[T]/(T) \simeq Q$, pero en cambio, el ideal $q = i^{-1}(p)$, que no es otro que (T) en $Z[T]$, NO es maximal pues en cociente $Z[T]/(T)$ aunque es el anillo íntegro Z, no es un cuerpo.

3. Sea T una indeterminada sobre $\mathbb{Q}$ y sea

$$H = \frac{T^4 - 2T^3 - 3T^2 + 12T - 12}{T^3 - 2T - 4}.$$

a) Calcular el polinomio mínimo de T sobre $\mathbb{Q}(H)$.
b) Calcular los grados de transcendencia siguientes:

gr. trans. $(\mathbb{Q}(T)/\mathbb{Q})$, gr. trans. $(\mathbb{Q}(H)/\mathbb{Q})$, gr. trans. $(\mathbb{Q}(T)/\mathbb{Q}(H))$.

Solución.

El problema es muy similar a [GR, 59] o a [FL, 135].

Como $T^4 - 2T^3 - 3T^2 + 12T - 12 = (T-2)(T^3 - 3T + 6)$ y $T^3 - 2T - 4 = (T-2)(T^2+2T+2)$ y $mcd(T^3-3T+6, T^2+2T+2) = 1$ (ambos son irreducibles, por Eisenstein), de la demostración del teorema de Lüroth se deduce que el polinomio mínimo de T sobre $\mathbb{Q}(H)$ es

$$(X^2 + 2X + 2)H - (X^3 - 3X + 6).$$

En particular, la extensión de cuerpos

$$Q(H) \hookrightarrow Q(T)$$

es finita y $[Q(T) : Q(H)] = 3$.

b) Como T es una indeterminada sobre Q, entonces $gr.trans.(Q(T)/Q) = 1$.

Por otra parte, como $Q(H)/Q$ es una subextensión no trivial de $Q(T)/Q$, el teorema de Lüroth afirma que $Q(H)/Q$ es también simple transcendente y por tanto $gr.trans.(Q(H)/Q) = 1$. Por último, como $Q(T)/Q(H)$ es finita, se tiene $gr.trans.(Q(T)/Q(H)) = 0$.

4. Sea E/K una extensión finita de cuerpos. Definir los conceptos $[E : K]$ y $G(E : K)$. Establecer con detalle el teorema del elemento primitivo para E/K y probar que:

$$\text{orden } G(E : K) \leq [E : K].$$

Solución.

El grado $[E : K]$ está definido en [GR, definición 1.4 pág. 249]. El grupo $G(E : K)$ está definido en [GR, pág. 312].

El enunciado del teorema del elemento primitivo está en [GR, proposición 3.9, pág. 276].

Una vez establecidos estos conceptos, la prueba de que orden $G(E : K) \leq [E : K]$ está incluida en el apartado 1.4 "Grupo de automorfismos de una extensión finita" pág. 316.