AYUDANTÍA XVIII

GRUPOS Y ANILLOS (PRIMAVERA 2016)

En esta ayudantía comenzaremos a estudiar la estructura de cuerpos. Nos enfocaremos en la adición de elementos en un cuerpo.

1.- Problema 1:

Sea L una extensión finita de K un cuerpo. Pruebe que para todo $\alpha \in L$ existe $p(x) \in K[x]$ no nulo tal que $p(\alpha) = 0$.

Demostración: Considere $\alpha \in L$ elemento cualquiera y supongamos que $[L : K] = \dim_K L = n < \infty$. Observe que el conjunto $X = \{1, \alpha, \dots, \alpha^n\}$ tiene $n + 1$ elementos. Por lo tanto X es un conjunto linealmente dependiente. Luego existen $a_0, \dots, a_n$ no todos nulos tales que $p(\alpha) = \sum_{i=0}^n a_i \alpha^i = 0$, donde $p(x) = \sum_{i=0}^n a_i x^i \in K[x]$ es un polinomio no nulo.

i.- **Ejercicio:** Encuentre una extensión L de $\mathbb{Q}$ de grado infinito tal que para todo $\alpha \in L$ existe $p(x) \in \mathbb{Q}[x]$ no nulo que cumple con $p(\alpha) = 0$.

2.- Problema 2:

Considere $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.

- i.- Pruebe que $L = \mathbb{F}_2[x]/(p(x))$ es un cuerpo. Determine su grado sobre $\mathbb{F}_2$.
- ii.- Calcule el inverso de $\bar{x} + \bar{1} \in L$.
- iii.- Pruebe que si L es una extensión de $\mathbb{F}_2$ tal que $[L : \mathbb{F}_2] = 2$ y $L = \mathbb{F}_2(\theta)$ entonces $L \cong \mathbb{F}_2[x]/(p(x))$.

Desarrollo:

- i.- Observe que $(p(x)) \subset \mathbb{F}_2[x]$ es un ideal maximal. Esto se debe a que $p(x)$ no tiene raíces en $\mathbb{F}_2$ y fue analizado en el problema 3 de la ayudantía XII. Luego $L = \mathbb{F}_2[x]/(p(x))$ es un cuerpo. Por último tenemos que $[L : \mathbb{F}_2] = \dim_{\mathbb{F}_2} \mathbb{F}_2[x]/(p(x)) = \deg(p(x)) = 2$.
- ii.- Tenemos que encontrar polinomios $s(x), t(x) \in \mathbb{F}_2[x]$ tales que $p(x)s(x) + (x+1)t(x) = 1$, pues en este caso $\overline{(x+1)}^{-1} = t(x)$. En efecto $p(x) - x(x+1) = 1$. Luego $\overline{(x+1)}^{-1} = \bar{x}$.
- iii.- Considere $L = \mathbb{F}_2(\theta)$ una extensión de grado 2 de $\mathbb{F}_2$. Considere el homomorfismo de anillos $\phi : \mathbb{F}_2[x] \rightarrow L$ definida por $\phi(s(x)) = s(\alpha)$. Entonces $\ker(\phi) = (t(x))$, para cierto $t(x) \in \mathbb{F}_2[x]$. Luego $\mathbb{F}_2[x]/(t(x)) \hookrightarrow L$. Comparando el grado sobre $\mathbb{F}_2$ tenemos que $\deg(t(x)) \leq 2$. Supongamos que $\deg(t(x)) = 1$, entonces $t(x) = x - a_0$, con $a_0 \in \mathbb{F}_2$. Por lo tanto, como $t(\alpha) = 0$ tenemos que $\alpha = a_0 \in \mathbb{F}_2$. Luego $L = \mathbb{F}_2$, lo que contradice el hecho de que $[L : \mathbb{F}_2] = 2$. Por lo tanto $\deg(t(x)) = 2$ y por igualdad en la dimensión tenemos que $L \cong \mathbb{F}_2[x]/(t(x))$, en donde ambos anillos son cuerpos. Por lo tanto $t(x)$ es un polinomio irreducible de grado 2 en $\mathbb{F}_2$. Los polinomios de grado dos en $\mathbb{F}_2[x]$ son $\{x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$ en

donde $p(x) = x^2 + x + 1$ es el único irreducible. Por lo tanto $t(x) = p(x)$. Esto concluye lo pedido.

2.- **Ejercicio:** Demuestre que $p(x) = x^3 - x + 1$ es un polinomio irreducible en $\mathbb{F}_3[x]$. Concluya que $L = \mathbb{F}_3[x]/(p(x))$ es cuerpo.

3.- **Problema 3:**

Considere $L = \mathbb{Q}(\sqrt[n]{2}) \subset \mathbb{C}$. Pruebe que $[L : \mathbb{Q}] = n$.

Demostración: Considere el homomorfismo $\phi : \mathbb{Q}[x] \rightarrow L$ definido por $\phi(x) = \sqrt[n]{2}$. Entonces como $p(x) = x^n - 2$ es un polinomio tal que $p(\sqrt[n]{2}) = 0$ tenemos que existe un homomorfismo $\bar{\phi} : \mathbb{Q}[x]/(p(x)) \rightarrow L$. Observe que por criterio de Eisenstein tenemos que $p(x)$ es irreducible sobre $\mathbb{Q}$. Por lo tanto $\mathbb{Q}[x]/(p(x)) \subset \mathbb{C}$ es un cuerpo que contiene a $\sqrt[n]{2}$. Por lo tanto $L \hookrightarrow \mathbb{Q}[x]/(p(x))$. Por otro lado como $\bar{\phi}$ es un homomorfismo no nulo, cuyo dominio es un cuerpo, tenemos que $\mathbb{Q}[x]/(p(x)) \hookrightarrow L$. Por lo tanto $L \cong \mathbb{Q}[x]/(p(x))$. Luego $[L : \mathbb{Q}] = \deg(p(x)) = n$.

4.- **Problema 4:**

Sea $L = K(\alpha) \cong K[x]/(p(x))$, donde $p(x) \in K[x]$ es un polinomio irreducible.

- i.- Muestre que existe $\sigma : L \rightarrow L$ automorfismo tal que $\sigma|_K = id$.
- ii.- Pruebe que $\sigma = id$ si $\{a \in L : p(x) = 0\} = \{\alpha\}$.
- iii.- Pruebe que existe $\sigma \neq id$ si $|\{a \in L : p(x) = 0\}| > 1$.

Desarrollo:

- i.- Observe que todo elemento $\alpha' \in L$ tal que $irr_{\alpha'}(x) = p(x)$ cumple con que $\phi : K[x]/(p(x)) \rightarrow L$, $\phi(x) = \alpha'$ es un isomorfismo, pues inyectivo, ya que $p(x)$ es irreducible y sobreyectivo pues $[L : K] = \deg(p(x)) = [K[x]/(p(x)) : K]$. Además $\phi|_K = id$. Por lo tanto existe $\sigma : L \rightarrow K[x]/(p(x)) \rightarrow L$ definida por $\sigma(\alpha) = \alpha'$ homomorfismo inyectivo entre espacios de igual dimensión. Por ello σ es un isomorfismo tal que $\sigma|_K = id$.
- ii.- Observe que para todo $\sigma : L \rightarrow L$ automorfismo tal que $\sigma|_K = id$, se tiene que $p(\sigma(\alpha)) = \sigma(p(\alpha)) = \sigma(0) = 0$. Luego $\sigma(\alpha) \in L$ es una raíz de $p(x)$. Luego si $\{a \in L : p(x) = 0\} = \{\alpha\}$ tenemos que $\phi(\alpha) = \alpha$. Por ello $\phi = id$, esto ya que $K(\alpha) = K \oplus K\alpha \oplus \dots \oplus K\alpha^t$, donde $\deg(p(x)) = t + 1$, pues $K(\alpha) \cong K[x]/(p(x))$.
- iii.- Por lo dicho en [i], si $|\{a \in L : p(x) = 0\}| > 1$, tenemos que $\sigma : L \rightarrow L$ definida por $\sigma(\alpha) = \alpha'$ define un isomorfismo de cuerpos, donde α' otra raíz de $p(x)$ en L . Esto prueba que existe σ no trivial.

4.- **Ejercicio:** Sea $d \in \mathbb{Z}$ elemento libre de cuadrado. Muestre que existen solamente dos automorfismos $\sigma : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}(\sqrt{d})$ tales que $\sigma|_{\mathbb{Q}} = id$.