Algebra Abstracta: Tarea #12

Jonathan Andrés Niño Cortés

28 de abril de 2015

1. El proposito de este problema es probar el siguiente resultado conocido como Teorema de extensión de isomorfismo

   Teorema 1. *Sea L/K una extensión algebraica y C/K_1 una extensión con C algebraicamente cerrado. Más aun suponga que existe un isomorfismo $\sigma : K \to K_1$. Entonces existe un homomorfismo $\tau : L \to C$ que extiende a σ i.e., tal que $\tau|_K = \sigma$.*

   La idea es utilizar el lema de Zorn de la siguiente forma:

   a) Pruebe el teorema en el caso que L/K es una extensión finita y simple. *(Esto lo hicimos en clase cuando probamos unicidad de cuerpos de descomposición).*

   Demostración. Por nuestra suposición tendriamos que $L = K(\alpha)$ donde α es la raíz de algún polinomo irreducible $f(x) \in K[x]$. Entonces podemos tomar $f'(x) \in K_1[x]$ el polinomio obtenodo a partir de $f(x)$ aplicando el isomorfismo σ a cada coeficiente. Entonces si tomamos β una raíz del polinomio $f'(x)$ tenemos por un teorema del Dummit que existe un isomorfismo $\tau : L \to K_1(\beta)$ tal que es una extensión de σ. Ahora si C es una extensión algrebraicamente cerrada de K_1 en particular tenemos que $\beta \in C$, luego $K_1(\alpha) \subseteq C$ y entonces podemos ver a τ como un homomorfismo $\tau : L \to C$. □

   b) Considere el conjunto de parejas

   $$\Sigma := \{(F; v) \mid K \subseteq F \subseteq L \text{ donde } v : F \to C \text{ extiende a } \sigma : K \to K_1\}$$

   dotado del orden parcial $(F, v) \preceq (F_1; \phi)$ si y sólo si $F \subseteq F_1$ y ϕ extiende a σ. Verifique que Σ es no vacío y que toda cadena en Σ es acotada.

   Demostración. El conjunto Σ es no vacío pues la pareja (K, σ) pertenece trivialmente a este conjunto. Ahora para verificar que toda cadena tiene cota superior considere una cadena $T = \{(F_i, v_i)\}_{i \in I} \subseteq \Sigma$. Entonces la pareja $(\bigcup_{i \in I} F_i, v)$ donde $v(\alpha) = v_i(\alpha)$ si $\alpha \in V_i$ es una cota para T. Primero $\bigcup_{i \in I} F_i \subseteq L$ pues todo F_i es tal que $F_i \subseteq L$. Además es un campo pues para cualesquiera dos elementos a, b

en la unión, como T es una cadena existe algún F_i tal que los contiene a los dos y esto nos basta para verificar todos los axiomas de campo.

Ahora para comprobar que v es un homomorfismo de campos que extiende a σ primero debemos ver que esta bien definida. Tomemos cualesquier elemento x y sean F_i y F_i' tales que $x \in F_i$, luego $v(x) = v_i(x) = v_{i'}(x)$ pues o bien v_i extiende a $v_{i'}$ o viceversa. Además v esta definido para todo elemento en la unión. Solo resta probar que es un homomorfismo de campos y esto se tiene pues para cualesquiera dos elementos x, y en la unión existe algún F_i que los contiene a ambos por ser una cadena y luego $v_(x) = v_i(x)$ y $v_(y) = v(x)$, de donde vemos que las condiciones de homomorfismo se derivan del hecho que v_i es un homomorfismo. □

c) Gracias al punto anterior, y al lema de Zorn, existe (F, τ) en Σ maximal con respecto al orden $\preceq$. *Muestre que $F = L$ y deduzca el resultado. Sugerencia: Si existiera $\alpha \in L/F$ utilice la parte (a) con la extensión $F(\alpha) = F$ para hallar una contradicción.*

Demostración. Suponga por contradicción que $F \neq L$. Entonces existe algún $\alpha \in L$ tal que $\alpha \notin F$ pero entonces podriamos considerar la extensión $F(\alpha) \supsetneq F$ que es finita y simple pues L es algebraico. Entonces por el punto (a) existiria una extensión τ' de τ, y por lo tanto la pareja $(F(\alpha), \tau')$ sería estrictamente mayor que (F, τ). Esto por lo tanto contradice el hecho que (F, τ) es maximal. Concluimos entonces que $F = L$. □

2. El proposito de este problema es probar la existencia y unicidad, módulo isomorfismo, de clausuras algebraicas. Sea K un cuerpo y sea $\Gamma := \{f \in K[x] : f(x) \text{ es irreducible y mónico}\}$ Sea $K[\{x_f\}]$ el anillo polinomial sobre K en las variables x_f indexadas por el conjunto Γ.

a) Sea $I \leq K[\{x_f\}]$ el ideal generado por el conjunto $\{f(x_f)\}_{f\in\Gamma}$. Muestre que I es un ideal propio. *Sugerencia: Si no lo fuera existirían $f_1, \cdots, f_n \in \Gamma$ y $h_1, \cdots, h_n \in K[\{x_f\}]$ tales que*

$$1 = f_1(x_{f_1})h_1 + \cdots + f_n(x_{f_n})h_n.$$

Si F/K es un cuerpo de descomposición de los $f_i (1 \leq i \leq n)$ muestre que la ecuación arriba se puede evaluar en F de tal forma que se obtenga una contradicción.

Demostración. Supongamos que I no es propio. Entonces tendriamos que existirian $f_1, \cdots, f_n \in \Gamma$ y $h_1, \cdots, h_n \in K[\{x_f\}]$ tales que

$$1 = f_1(x_{f_1})h_1 + \cdots + f_n(x_{f_n})h_n.$$

Entonces podemos extendernos al cuerpo de descomposición F de los f_i. Si evaluamos esta ecuación en F tomando $x_{f_i} = \alpha_i$ donde α_i es una raiz del polinomio f_i tendriamos que el polinomio es igual a 0, por lo tanto esta ecuación no puede ser igual a 1. □

b) Gracias al punto (a) existe un ideal maximal M que contiene a I. Muestre que $\hat{K} := K[\{x_f\}]/M$ es una extensión algebraica de K.

Demostración. Como M es maximal sabemos que $K[\{x_f\}]/M$ es un campo y sabemos que este campo contiene una copia isomorfa del campo K dada por los polinomios constantes. Solo nos resta demostrar que cada elemento es algebraico. Para probar esto considere los elementos de la forma $\overline{f(x_f)}$. Claramente tenemos que x_f como polinomio esta incluido en I y por lo tanto en M Luego $\overline{f(x_f)} = f(\overline{x_f}) = 0$ por lo que vemos que $\overline{x_f}$ es algebraico. Esto demuestrar que $K[\{x_f\}]/M$ es algebraico pues es generado por todos los $\{\overline{x_f}\}$. □

c) Defina inductivamente los cuerpos K_n de la siguiente manera: $K := K_0$ y $K_{n+1} := \hat{K}^n$. Sea $\mathcal{K} := [\bigcup_{n\geq 0} K_n$: Muestre que $\mathcal{K}/K$ es una extensión algebraica y que K es algebraicamente cerrado; en otras palabras $\mathcal{K}$ es una clausura algebraica de K.

Demostración. El hecho que es una extensión de K es similar a la demostración anterior sobre el Lema de Zorn, pues estos campos forman una cadena con el orden de contenencia. Para probar que es el agebraico basta con notar que para cualquier elemento en la unión hay algún K^n que lo contiene y cada K^n es algebraico pues se obtiene como una cadena finita de extensiones algebraicas entre si.

Para demostrar que es algebraicamente cerrado tome cualquier polinomio en $\mathcal{K}$. Podemos observar que todos los coeficientes deben pertenecer a algún K_n. Si este polinomio tiene una raiz en K_n ya ganamos. Si no tiene raices entonces este polinomio se puede ver como multiplicación de factores irreducibles de grado mayor o igual a 2. Por la definición de K_{n+1} debe existir alguna raiz de estos factores irreducibles en este campo. Luego vemos que el polinomio tiene una raiz en $\mathcal{K}$. □

d) Sean L, L_1 dos clausuras algebraicas de K, es decir dos cuerpos algebraicamente cerrados que son extensiones algebraicas de K. Muestre que $L \cong L_1$. *Sugerencia: Utilice el punto 1 de esta tarea.*

Demostración. El punto 1 nos permite concluir que existe un homomorfismo inyectivo entre L y L_1 y que también hay un homomorfismo inyectivo entre L_1 y L la existencia de estos dos homomorfismos nos dice que existe un isomorfismo entre L y L_1. □

3. Sean L/F y F/K extensiones de cuerpos.

a) Si L/K es separable muestre que L/F y F/K son separables.

Demostración. F/K es separable pues se puede ver como un subconjunto de L/K. Como en L/K todo sus elementos son separables concluimos que en F/K también todos sus elementos son separables y por lo tanto es separable.

Ahora para probar que L/F es separable tome cualquier elemento $\alpha \in L$. Y tome el polinomio irreducible $f(x) \in F[x]$. Pero si consideramos el polinomio irreducible $k(x)$ de α en $K[x]$ tenemos que $f(x)|k(x)$. Luego, como $k(x)$ no tiene raices repetidas concluimos que $f(x)$ tampoco. Por lo tanto L/F es separable. $\square$

b) Si L/K es normal muestre que L/F es normal. Concluya que si L/K es de Galois entonces L/F es de Galois. Muestre mediante un ejemplo que aunque L/K sea normal la extensión F/K no es necesariamente normal.

Demostración. Debemos demostrar que L es el cuerpo de ruptura para algún polinomio en F. Pero sabemos que L/K es normal, luego L es el cuerpo de ruptura de algún polinomio $p(x)$ en $K[x]$, es decir, que todas sus raices estan contenidad en L. Pero si consideramos el mismo polinomio $p(x)$ embebido en $F[x]$ tenemos que también todas sus raices pertenecen a L. Luego, L se puede ver como el cuerpo de rutura para este polinomio en $F[x]$. Por lo tanto, L/F es normal.

Para demostrar que F/K no es necesariamente normal considere la extensión $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$. Esta extensión es precisamente el cuerpo de ruptura de $x^3 - 2$ y por lo tanto es normal. Sin embargo si consideramos la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ esta extensión no es normal. Pues el polinomio $x^3 - 2$ tiene una pero no todas sus raices pues las demás viven en $\mathbb{C}$. $\square$

c) Suponga que L/K es de Galois. Muestre que $\mathrm{Gal}(L/F)$ es un subgrupo de $\mathrm{Gal}(L/K)$ con indice

$$[\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)] = [F : K].$$

Demostración. Como L/K es de Galois tenemos que es separable y normal. Por los puntos anteriores tenemos que L/F es también separable y normal. Por lo tanto L/F también es de Galois.

Entonces sabemos que $|\mathrm{Gal}(L/K)| = [L : K]$. Y $|\mathrm{Gal}(L/F)| = [F : K]$. Finalmente por el Teorema de Lagrange tenemos que $[\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)] = [L : K]/[L : F]$ y por el lema de torres $[L : K]/[L : F] = [F : K]$. $\square$

d) Suponga que L/K es de Galois y que la extensión F/K es normal, en particular también de Galois. Muestre que $\mathrm{Gal}(L/F)$ es un subgrupo normal de $\mathrm{Gal}(L/K)$. Deduzca de esto que el homomorfismo de grupos, conocido como el *homomorfismo restricción*,

$$res_L^F : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K); \sigma \mapsto \sigma|_F$$

está bien definido y tiene a $\mathrm{Gal}(L/F)$ como Kernel. Concluya de esto, y de la parte (c), que

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K).$$

Demostración. Como la extensión F/K es normal tenemos que $\sigma|_F$ es un automorfismo de F a F. Luego el homomorfismo restricción esta bien definido y vemos que el kernel son todos los automorfismos que al restrigirlos en F son iguales a la

identidad. Esta es la definición de $\mathrm{Gal}(L/F)$. Por lo tanto, como $\mathrm{Gal}(L/F)$ es el kernel de un homomorfismo concluimos que es normal.

Finalmente tenemos por el primer teorema del homomorfismo que $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K) \cong res_L^F(\mathrm{Gal}(L/K))$. Entonces por Lagrange tenemos que $|res_L^F(\mathrm{Gal}(L/K))| = [L:K]/[L:F] = [F:K]$ pero por el punto (c) este es precisamente el orden de $\mathrm{Gal}(F/K)$. Luego $res_L^F(\mathrm{Gal}(L/K)) = \mathrm{Gal}(F/K)$. □

4. *a*) Sea G un grupo con $|G| \leq 7$. Muestre que existe $L/\mathbb{Q}$ extensión de Galois tal que

$$\mathrm{Gal}(L/\mathbb{Q}) \cong G.$$

Demostración. Tome $\mathbb{Q}(\zeta_{29})/\mathbb{Q}$. Ya demostramos que $\mathrm{Gal}(\mathbb{Q}(\zeta_{29})/\mathbb{Q}) = \mathbb{Z}/28\mathbb{Z}$. Pero tenemos que $H = \mathbb{Z}/7\mathbb{Z}$ es un subgrupo normal del anterior pues el anterior es abeliano. Luego, L^H sería la extensión que tendria asociada un subgrupo de Galois de orden 7. □

b) Sea $L := \mathbb{Q}(x_1, x_2)$ el cuerpo de funciones racionales en dos variables sobre $\mathbb{Q}$. Sean $s_1 := x_1 + x_2$ y $s_2 := x_1 x_2$.

Muestre que si $K = \mathbb{Q}(s_1, s_2)$ entonces $L = K(x_1)$ y la extensión L/K es de Galois con

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Demostración. Probemos que $L = K(x_1)$ por doble contenencia. $L \subseteq K(x_1)$ pues $x_1 \in K(x_1)$ y $x_2 = s_1 - x_1 \in K(x_1)$. Para probar que $K(x_1) \subseteq L$ observe que $x_1 \in L$, $s_1 = x_1 + x_2 \in L$ y $s_2 = x_1 x_2 \in L$.

Ahora tenemos que L/K es de Galois, pues es separable ya que $\mathbb{Q}$ tiene caracteristica 0. Además es normal pues $K(x_1)$ es el cuerpo de ruptura del polinomio $x^2 - s_1 x + s_2$.

Finalmente podemos probar que $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ pues el grado de la extensión es 2. Luego el grupo de Galois tiene orden 2 y este es el único grupo de orden 2 que existe módulo isomorfismos. □