Algebra Abstracta: Tarea #10

Jonathan Andrés Niño Cortés

9 de abril de 2015

1. Sea L/K una extensión de cuerpos.

   a) Sea p un primo y suponga que $[L : K] = p$. Muestre que L/K es una extensión simple.

   Demostración. Tome cualquier elemento $\alpha \in L$ tal que $\alpha \notin K$ y considere la extensión $K(\alpha)$. Por el lema de Torres tenemos que $p = [L : K] = [L : K(\alpha)][K(\alpha) : K]$. Así que $[K(\alpha) : K]$ es un divisor de p y como por nuestra suposición no es 1, concluimos que $[K(\alpha) : K] = p$ y que $[L : K(\alpha)] = 1$, es decir que $L = K(\alpha)$ lo que muestra que L es simple. □

   b) Muestre que no existe $L/\mathbb{C}$ tal que $[L : \mathbb{C}] = 2$.

   Demostración. Suponga por contradicción que existe $L/\mathcal{C}$ tal que $[L : \mathbb{C}] = 2$. Entonces debe existir algún elemento α tal que su polinomio minimal sea de grado 2. Pero se puede demostrar (sin necesidad del resultado más fuerte que $\mathbb{C}$ es algebraicamente cerrado) que todo polinomio de grado 2 en $\mathbb{C}$ es reducible.

   Esto es gracias a la ecuación cuadrática. Cualquier polinomio mónico de grado 2 $x^2 + ax + b$ en $\mathbb{C}$ se puede factorizar en dos polinomios mónicos de grado 1 como $(x - x_1)(x - x_2)$ donde

$$x_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

   $x_{1,2} \in \mathbb{C}$ porque en los complejos la función raiz se puede defenir para cualquier número complejo a diferencia de los reales donde las raíces de números negativos no estan definidas.

   Llegamos a una contradicción y concluimos que no puede existir dicha extensión. □

   c) Suponga que toda extensión finita de $\mathbb{R}$ es simple. Muestre que no existe L extensión finita $\mathbb{R}$ de grado $[L : \mathbb{R}]$ impar.

Demostración. De nuevo suponiendo por contradicción que L es una extensión finita de $\mathbb{R}$ de grado impar tendriamos que existe algún elemento $\alpha \in L$ tal que su polinomio mínimal es de grado impar.

Pero en $\mathbb{R}$ todo polinomio mónico impar tiene por lo menos una raiz lo que implica que es reducible. Para demostrar esto podemos utilizar el teorema de valor intermedio de cálculo. Sea $P(x)$ el polinomio irreducible. Como el polinomio es mónico de grado impar tenemos que su limite al infinito es igual a infinito y su limite a menos infinito es menos infinito. Entonces podemos tomar un valor a tal que $P(a) < 0$ y un valor b tal que $P(b) > 0$. Entonces por el teorema del valor intermedio existe un valor c entre a y b tal que $P(c) = 0$, es decir, que c es una raíz de $P(x)$. □

2. Sea L/K una extensión de cuerpos y sea $\alpha \in L$.

   a) Muestre que α es algebraico sobre K si y sólo si $K[\alpha] = K(\alpha)$. (Acá $K[\alpha]$ denota el sub-anillo de L generado por K y α.)

   Demostración. Una desigualdad siempre se cumple. Tenemos que $K[\alpha] \subseteq K(\alpha)$, pues cualquier elemento en $K[\alpha]$ se puede escribir como $a_n\alpha^n + \cdots + a_1\alpha + a_0$ donde $a_i \in K$ y claramente esto pertenece a $K(\alpha)$.

   Ahora sabemos que α es algebraico si y solo sí existe un polinomio mónico irreducible en K tal que α es raíz de este polinomio en $K(\alpha)$. Sea $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ este polinomio. Evaluando este polinomio por α obtenemos $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, luego $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha = -a_0$ y entonces factorizando α y multiplicando por el inverso de $-a_0$ obtenemos la expresión $\alpha * (-a_0)^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) = 1$, es decir que $\alpha^{-1} = (-a_0)^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1)$. Esto a su vez implica que $K(\alpha) \in K[\alpha]$ pues logramos escribir el inverso de α como un elemensto de $K[\alpha]$. □

   b) Muestre que α es trascendente sobre K si y sólo si $K[\alpha] \cong K[x]$.

   Demostración. Tenemos que el homomorfismo $\phi : K[x] \to K[\alpha]$ donde ϕ es evaluación por α es un homomorfismo sobreyectivo. Lo único que resta es demostrar que este homomorfismo es inyectivo si y solo sí α es trascendente.

   De hecho sabemos que α es trascendente si y solo sí α no es algebraico, es decir, si y solo si no existe un polinomio $P(x)$ distinto al polinomio 0 tal que $P(x) = 0$. Pero esto es equivalente a que el kernel de ϕ es igual a $\{0\}$, lo que significa que el homomorfismo es además inyectivo y por lo tanto es un isomorfismo. □

3. *a*) Sean M/L y L/K extensiones de cuerpos, y suponga que ambas extensiones son algebraicas. Muestre que M/K es una extensión algebraica.

   Demostración. Esto es equivalente a demostrar que $[K(\alpha) : K] < \infty$ para cualquier $\alpha \in M$.

Primero como M/L es algebráico tenemos que $[L(\alpha) : L] < \infty$ para todo $\alpha \in M$. Es decir que existe algún polinomio $x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, con coeficientes en L tal que α es raíz de este polinomio.

Entonces si consideramos la extensión $K(a_0, a_1, \cdots, a_{n-1})$ esta es una expansión finita porque es finitamente generada por elementos que son algebraicos en K. El polinomio minimal de α pertenece a esta extensión por lo que $[K(a_0, a_1, \cdots a_{n-1})(\alpha) : K(a_0, a_1, \cdots a_{n-1})] < \infty$. Finalmente, por lema de las torres tenemos que $[K(a_0, a_1, \cdots a_{n-1})(\alpha) : K] = [K(a_0, a_1, \cdots a_{n-1})(\alpha) : K(a_0, a_1, \cdots a_{n-1})][K(a_0, a_1, \cdots a_{n-1}) : K] < \infty$. Pero también tenemos que $[K(a_0, a_1, \cdots a_{n-1})(\alpha) : K] = [K(a_0, a_1, \cdots a_{n-1})(\alpha) : K(\alpha)][K(\alpha) : K] < \infty$ lo que implica que $[K(\alpha) : K] < \infty$, es decir, que α es algebraico en K. $\square$

b) En clase vimos que si L/K es una extensión finita entonces la extensión es algebraica. Pruébelo de nuevo acá.

Demostración. Tome cualquier $\alpha \in L$. Por hipotesis tenemos que $[L : K] < \infty$. Además tenemos que $K(\alpha) \subseteq L$. Luego por el lema de torres tenemos que $[L : K] = [L : K(\alpha)][K(\alpha) : K] < \infty$ lo que implica que $[K(\alpha) : K] < \infty$, es decir, que α es algebraico en K. $\square$

c) Muestre mediante el siguiente ejemplo que el converso del anterior no es cierto. Sea S el sub-conjunto de los números reales dado por la raíces primas de 2 i.e.,

$$S := \{2^{1/p} : p \text{ es primo}\}.$$

Muestre que $\mathbb{Q}(S) = \mathbb{Q}$ es una extensión algebraica tal que $[\mathbb{Q}(S) : \mathbb{Q}] = \infty$.

Demostración. Primero para demostrar que $\mathbb{Q}(S)$ es algebraico solo basta demostrar que los elementos en S son algebraicos, porque los demás elementos en $\mathbb{Q}(S)$ se pueden ver como sumas, multiplicaciones o divisiones finitas de elementos de $\mathbb{Q}$ y S que por lo tanto también son algebraicos. Y cualquier elemento $2^{1/p} \in S$ es algebraico en $\mathbb{Q}$ porque el polinomio $x^p - 2$ tiene como raíz a $2^{1/p}$.

Además, por el criterio de Einsenstein $x^p - 2$ es irreducible en $\mathbb{Q}$ para cualquier p primo en $\mathbb{Z}$ por lo que este polinomio es el minimal. Ahora para demostrar que $[\mathbb{Q}(S) : \mathbb{Q}] = \infty$ suponga por contradicción que $[\mathbb{Q}(S) : \mathbb{Q}] = n < \infty$. Entonces todo elemento en $\mathbb{Q}(S)$ deberia ser raiz de algún polinomio irreducible $\mathbb{Q}$ de grado menor o igual a $\ltimes$, pero sabemos que el conjunto de primos es infinito. Luego, podemos encontrar algún primo $p > n$ y entonces el elemento $2^{1/p} \in S$ cuyo polinomio minimal es $x^p - 2$ y por lo tanto no hay ningún polinomio de grado menor o igual a n para el que $2^{1/p}$ es raíz. Por lo tanto llegamos a una contradicción. $\square$

4. Para esta pregunta asuma que $e := \sum_{n=0}^{\infty} \frac{1}{n!}$ y $\pi := \int_0^{\infty} \frac{2}{1+x^2} dx \in \mathbb{R}$ son trascendentes sobre $\mathbb{Q}$. Sean $\alpha = e + \pi$ y $\beta = e\pi$. Muestre que al menos uno entre α y β no es

algebráico sobre $\mathbb{Q}$. (Nota: En principio uno de ellos puede ser algebraico, pero es un problema abierto decidir si los dos son trascendentes, de hecho no sé sabe si quiera si son irracionales.)

Demostración. Considere el polinomio $x^2 - \alpha x + \beta$. Efectivamente este polinomi se puede descomponer en $\mathbb{R}$ como $(x - \pi)(x - e)$. La fórmula cuadrática nos da una expresión para calcular las raices de este polinomio.

$$x_{1,2} = \frac{\alpha \pm \sqrt{\alpha^2 - 4\beta}}{2}$$

Donde x_1 y x_2 van a ser π o e. Sabemos que la suma, resta y división de algebraicos es algebraico. Tan solo falta demostrar que la raiz de algebraicos es algebraica y esto es así. Suponiendo que la raiz no esta contenida en una extension algebraica podemos hacer una extensión de grado 2 sobre esta extensión para agregarla (partiendo el anillo de polinomios por el polinomio $x^2 - \alpha$, por ejemplo) y la extensión vista desde $\mathbb{Q}$ seguiria siendo algebraica por el punto 3(a) de esta tarea.

Pero esto implicaria que tanto e como π son algebráicos lo cual es una contradicción. Concluimos que por lo menos uno de los dos entre α y β son trascendentes. $\square$

5. Sean p_1 y p_2 primos distintos. Suponga que m_i, para $i = 1, 2$, son enteros positivos tales que m_i no es una potencia p_i-ésima perfecta. Sean μ_i los reales positivos definidos por las dos ecuaciones $\mu_i^{p_i} = m_i (i = 1; 2)$.

   a) Fije $i \in \{1, 2\}$ y sea F un subcuerpo de $\mathbb{R}$ que no contiene a μ_i. Si $\mu_i^n \in F$ para algún entero no negativo n, muestre que $p_i | n$.

   Demostración. Vamos a demostrar primero que para cualquier $\alpha \in F$ se tiene que si $\alpha^n \in F$ y $\alpha^m \in F$ entonces $\alpha^{g.c.d(n,m)} \in F$. La demostración es utilizando la identidad de Bezout, que nos dice que existen $a, b \in \mathbb{Z}$ tales que $am + bn = g.c.d(m, n)$. Note que si $a = -c$ es negativo entonces se toma $\alpha^a = (\alpha^{-1})^c$ Entonces tenemos que $(\alpha^m)^a (\alpha^n)^b = \alpha^{an+bm} = (\alpha^{g.c.d(m,n)} \in F$.
   Ahora la otra cosa que cabe notar es que por nuestra suposición $\mu_i^{p_i} = m_i \in \mathbb{Z} \subseteq \mathbb{Q}$. En una tarea anterior demostramos que todo campo de caracteristica 0, como $\mathbb{R}$ contiene una copia de $\mathbb{Q}$. Entonces cualquier subcampo F contiene a $\mathbb{Q}$ por lo que concluimos que $\mu_i^{p_i} = m_i \in F$.
   Entonces si suponemos por contradicción que existe n tal que $p_i \not| n$ y $\mu_i^n \in F$ tendriamos primero que $g.c.d(n, p_i) = 1$ y por lo discutido anteriormente concluimos que $\alpha^1 = \alpha \in F$ lo cual es una contradicción. $\square$

   b) De nuevo, si $\mathbb{R}/F$ es tal que $\mu_i \notin F$ muestre que $[F(\mu_i) : F] = p_i$. Deduzca de lo anterior que el polinomio $x^{p_i} - m_i \in F[x]$ es irreducible. (Sugerencia para la primera parte: Considere el término constante del polinomio minimal de μ_i sobre F.)

Demostración. Sabemos que μ_i es una raiz del polinomio $x^{p_i} - m_i$. Luego el polinomio minimal de μ_i divide a este polinomio. Si nos extendemos al campo algebraicamente cerrado $\mathbb{C}$ podemos factorizar el polinomio minimal como $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$ donde m es el grado de este polinomio que debe ser menor o igual a p_i.

Ahora las otras raices de $x^{p_i} - m_i$ estan dadas por $\mu_i\omega_j$ donde ω_j es una p_i-ésima raiz de la unidad.

Ahora si consideramos el término constante del polinomio minimal este debe ser igual a $\alpha_1 \cdots \alpha_m = \mu^m(\omega_1 \cdots \omega_m) \in F$. Pero recordemos que F es un subcampo de los reales, luego como $\mu \in \mathbb{R}$ concluimos que $(\omega_1 \cdots \omega_m) \in \mathbb{R}$. Además, se puede observar que $(\omega_1 \cdots \omega_m)_i^p = 1 \cdots 1 = 1$, pero las únicas raices de la unidad reales son 1 o -1. Por lo tanto, el término constante es μ^m o $-\mu^m$. En cualquier caso, por el punto anterior tenemos que $p_i | m$ y por lo tanto m debe ser igual a p_i. Como este es el grado del polinomio minimal concluimos finalmente que $[F(\alpha) : F] = p_i$. □

c) Sea K el sub-cuerpo de R dado por $K = \mathbb{Q}[\mu_1 + \mu_2]$. Muestre que $[K : \mathbb{Q}] = p_1 p_2$

Demostración. Tenemos que μ_1 y μ_2 son algebraicos, luego su suma es algebraica y por el punto 2 tenemos que $\mathbb{Q}[\mu_1+\mu_2] = \mathbb{Q}(\mu_1+\mu_2)$. Ahora por lo demostrado anteriormente tenemos que ni μ_1 ni μ_2 pertenecen a $\mathbb{Q}$. Luego $[K(\mu_1) : K] = p_1$ y además $\mu_2 \notin \mathbb{Q}$ puesto que si estuviera entonces p_2 deberia dividir a p_1 lo cual es una contradicción. Luego tenemos que $[K(\mu_1, \mu_2) : K(\mu_1)] = p_2$ y por el lema de las torres tenemos que $[K(\mu_1, \mu_2) : K] = p_1 p_2$.

Ahora también tenemos que $K(\mu_1, \mu_1 + \mu_2) = K(\mu_2, \mu_1 + \mu_2) = K(\mu_1, \mu_2)$. Valiendonos de nuevo del lema de torres tenemos que $p_1 p_2 = [K(\mu_1, \mu_1+\mu_2) : K] = [K(\mu_1, \mu_1+\mu_2) : K(\mu_1+\mu_2)][K(\mu_1+\mu_2 : K]$ y $p_1 p_2 = [K(\mu_2, \mu_1+\mu_2) : K] = [K(\mu_1, \mu_1+\mu_2) : K(\mu_1+\mu_2)][K(\mu_1+\mu_2 : K]$. Ahora $[K(\mu_1, \mu_1+\mu_2) : K(\mu_1+\mu_2)]$ puede ser 1 o p_2 dependiendo de sí μ_1 esta contenido o no y de igual manera con $[K(\mu_2, \mu_1+\mu_2) : K(\mu_1+\mu_2)]$. Si alguno de estos es 1 entonces concluiriamos por el lema de las torres que $[K(\mu_1+\mu_2) : K] = p_1 p_2$, pero si suponemos que ninguno de los 2 es 1 llegariamos rapidamente a una contradicción porque el lema de las torres nos permitiria concluir que $[K(\mu_1+\mu_2) : K] = p_1$ y $[K(\mu_1+\mu_2) : K] = p_2$ al mismo tiempo. Luego $[K(\mu_1+\mu_2) : K] = p_1 p_2$ □

6. Sea L/K una extensión de cuerpos. Un subconjunto $T \subseteq L$ se dice algebraicamente independiente sobre K si para todos $t_1, \cdots, t_n \in T$ se tiene que si $p(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ es tal que $p(t_1, \cdots, t_n) = 0$ entonces $p(x_1, \cdots, x_n)$ es el polinomio 0.

   a) Muestre que si $T = \{t\}$ consiste de un solo elemento entonces T es algebraicamente independiente sobre K si y sólo si t es trascendente sobre K.

   Demostración. Por nuestra suposición que solamente hay un elemento evaluar sobre un polinomio de x_n variables es equivalente a evaluar sobre un polinomio de una sola variable que se obtiene sustituyendo cada una de las variables x_i por el indeterminado x. Efectivamente tenemos que t es trascendente si y solo si no existe un polinomio con coeficientes en K tal que t sea raíz de este polinomio Por lo anterior, concluimos que T es algebraicamente independiente. □

b) Muestre que toda extensión L/K contiene un subconjunto algebraicamente independiente maximal T.

Demostración. Vamos a utilizar el Lema de Zorn sobre la colección de subconjuntos alg ind de L. Esta colección es no vacía si tomamos en cuenta el vacío, que por vacuidad cumple todas las condiciones de subconjuntos alg ind. Ahora sea C una cadena de colecciones alg ind. Vamos a demostrar que $B = \bigcup_{A \in C} A$ es una cota para la cadena C. Claramente $A \subseteq B$ para cualquier $A \in C$. Entonces solo resta demostrar que B es un conjunto alg ind. Entonces tome cualesquiera $t_1, \cdots, t_n \in T$. Por cada t_i existe un A_i en la cadena y como son finitos yo puedo tomar algun A_n tal que los contenga a todos. Luego como A_n es un conjunto alg ind concluimos que no hay ningun polinomio distinto de 0 que al evaluarlo con estos parametros de 0. Por lo tanto, concluimos que B es una cota y luego podemos utilizar el Lema de Zorn para concluir que debe existir algún subconjunto alg ind máximal. □

c) Sea T un conjunto alg ind maximal para la extensión L/K. Muestre que la extensión $L/K(T)$ es algebráica.

Demostración. Si suponemos por contradicción que $L/K(T)$ no es algebraico entonces existiría al menos un elemento $\alpha \in L$ trascendente en $L/K(T)$. Claramente $\alpha \notin T$ porque cualquier elemento en T es algebraico en $L/K(T)$. Entonces si tomamos el conjunto $T \cup \{\alpha\}$ este es alg ind. Si esto no fuera así es porque existe algún polinomio sobre $K(T)$ tal que α es raíz, pero entonces no sería trascendente. Llegamos pues a una contradicción con la maximalidad de T. □

Se puede mostrar que dada una extensión L/K cuales quiera dos conjuntos alg ind maximales (conocidos como bases de trascendencia) tienen el mismo cardinal. A éste cardinal se le conoce como el grado de trascendencia de L sobre K y se denota por trdeg (L/K).