Algebra Abstracta: Tarea #11

Jonathan Andrés Niño Cortés

17 de abril de 2015

1. *a*) Muestre que el polinomio $x^3 - 3x + 1 \in \mathbb{Q}[x]$ es irreducible

   Demostración. Sea $p(x) = x^3 - 3x + 1$. Por el Lema de Gauss tenemos que si el polinomio es irreducible en $\mathbb{Z}$ entonces es irreducible en $\mathbb{Q}$.Ahora para demostrar que es irreducible en $\mathbb{Z}$ como el polinomio es mónico basta demostrar que el polinomio es irreducible en $(\mathbb{Z}/2\mathbb{Z})[x]$. Como el polinomio es de grado 3, ser irreducible es equivalente a no tener una raíz. El polinomio reducido es $p(x) = x^3 + x + 1$ y vemos que $p(0) = 1$ y $p(1) = 1$. Por lo tanto, no tiene raices, es irreducible es $\mathbb{Z}/2\mathbb{Z}[x]$ y por lo es irreducible en $\mathbb{Z}$ y en $\mathbb{Q}$. $\square$

   b) Utilice la identidad trigonométrica $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ para verificar que $2\cos\left(\frac{2\pi}{9}\right)$ es una raíz de $x^3 - 3x + 1$.

   Demostración. Evaluemos $p\Bigg(2\cos\left(\frac{2\pi}{9}\right)\Bigg)$.

$$\begin{aligned} p\Bigg(2\cos\left(\frac{2\pi}{9}\right)\Bigg) &= 8\cos\left(\frac{2\pi}{9}\right)^3 - 6\cos\left(\frac{2\pi}{9}\right) + 1 \\ &= 2(4\cos^3\left(\frac{2\pi}{9}\right) - 3\cos\left(\frac{2\pi}{9}\right)) + 1 \end{aligned}$$

   Entonces por identidad trigonométrica en el enunciado tenemos que $4\cos^3\left(\frac{2\pi}{9}\right) - 3\cos\left(\frac{2\pi}{9}\right) = \cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2}$.
   Luego,

$$\begin{aligned} p\Bigg(2\cos\left(\frac{2\pi}{9}\right)\Bigg) &= 2(\cos\left(\frac{2\pi}{3}\right)) + 1 \\ &= 2(-\frac{1}{2}) + 1 \\ &= 0 \end{aligned}$$

$\square$

c) Muestre que el poligono regular de 9 lados, Eneágono, no se puede construir con regla y compas. Equivalentemente el ángulo $\frac{2\pi}{3}$ no puede ser trisecado.

Demostración. Los dos puntos anteriores nos permiten concluir que $\alpha = 2\cos\left(\frac{2\pi}{9}\right) \notin \mathbb{Q}$ porque es una raíz del polinomio pero ya vimos que este polinomio no tiene ráices en $\mathbb{Q}$.

Por lo tanto tenemos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Pero esto implica que el punto no puede contruirse con regla y compas, porque no es posible que ella una cadena de extensiones de grado 2 entre esta extensión y $\mathbb{Q}$. ☐

2. Sea K un cuerpo algebraicamente cerrado. Muestre que K es infinito.

Demostración. Vamos a demostrar que níngun cuerpo finito puede ser algebraicamente cerrado. Suponga por contradicción que hay un campo finito F de tamaño n algebraicamente cerrado. Si es finito entonces su caracteristica es $p > 0$ porque si su caracteristica fuera cero entonces necesariamente sería infinito.

Entonces considere el polinomio $P(x) = (x - \alpha_0)(x - \alpha_1) \cdots (x - \alpha_n) + 1$, donde α_i es el elemento i del campo. Este polinomio no tiene ninguna raíz porque si evaluamos en cualquier elemento de $\alpha \in F$ tenemos que $P(\alpha) = 0 + 1 = 1$. Pero esto es una contradicción porque si F fuera algebraicamente cerrado todo polinomio de grado >0 deberia tener una raiz. ☐

3. Sea K un cuerpo de característica $p > 0$. Muestre que la función $\mathrm{Frob}_p : K \to K$ definida por $x \mapsto x^p$ es un monomorfismo de anillos. A éste homorfismo se le conoce como el homomorfismo de Frobenious.

Demostración. Primero probemos que Frob_p es un homomorfismo.

$$\mathrm{Frob}_p(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Pero si $0 < k < p$ entonces $p | \binom{p}{k}$.

Por la definición del coeficiente binomial tenemos que $\binom{p}{k} k!(p-k)! = p!$. Ahora vamos a probar que p es primo relativo con $k!(p-k)!$ porque la restricción sobre k asegura que tanto k como $p-k$ son menores estrictamente a p. Y por lo tanto como todo número menor a p es primo relativo con p se cumple que tanto $k!$ como $(p-k)!$ son primos relativos con p y luego $(p-k)!k!$ es primo relativo con p. Ahora claramente $p | p!$, luego concluimos que $p | \binom{p}{k}$. Pero como el cuerpo es de caracteristica p tenemos que $p = 0$, por lo tanto

$$
\begin{aligned}
\mathrm{Frob}_p(x+y) &= \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k. \\
&= \binom{p}{0} x^p + \binom{p}{p} y^p \\
&= x^p + y^p \\
&= \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y)
\end{aligned}
$$

Por otra parte $\mathrm{Frob}_p(xy) = (xy)^p$, pero como en un campo la multiplicación es conmutativa tenemos que $(xy)^p = x^p y^p = \mathrm{Frob}_p(x)\mathrm{Frob}_p(y)$.

Ahora para probar que es inyectivo solo basta demostrar que el homomorfismo es diferente del homomorfismo 0, pues estamos en un campo y este es el caso porque por ejemplo si consideramos el elemento 1, $\mathrm{Frob}_p(1) = 1^p = 1$. $\square$

4. Sea p un primo y sea $\mathbb{F}_p$ el cuerpo de p elementos. Sea n un entero positivo y sea $f_n(x) := x^{p^n} - x \in \mathbb{F}_p[x]$.

   a) Muestre que $f_n(x)$ no tiene raíces repetidas.

   Demostración. Tome la derivada del polinomio $f_n(x)$.

$$
f'(x) = p^n x^{p^n - 1} - 1 = -1
$$

   Lo anterior es porque la caracteristica del polinomio es p, luego $p^n = 0$. Y como $f'(x)$ no tiene raíces en particular no hay raices comunes entre $f(x)$ y $f'(x)$ y por lo tanto el polinomio $p(x)$ no tiene raices repetidas. $\square$

   b) Sea $\mathbb{F}_{p^n}$ el cuerpo de descomposición de $f_n(x)$ y sea $S \subseteq \mathbb{F}_{p^n}$ el conjunto de las raíces de $f_n(x)$. Muestre que S es un cuerpo y concluya que $S = \mathbb{F}_{p^n}$.

   Demostración. Como primera observación tenemos que $1 \in S$ puesto que $1^{p^n} = 1$. Todas las raíces α de f_n cumplen que $\alpha^{p^n} = \alpha$. Para probar que S es un campo basta probar que para cualesquiera α, β y $\gamma \in S$, $\alpha - \beta/\gamma \in S$.
   En efecto,

$$
(\alpha - \beta/\gamma)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{k} \alpha^{p^n - k} (\beta/\gamma)^k \tag{1}
$$

   Pero por un argumento similar al dado en la demostración del segundo punto todos los coeficientes entre 1 y $k-1$ son divisibles por p y por lo tanto son iguales a 0. Luego los únicos factores sobrevivientes son los correspondientes a 0 y a p^n. Entonces,

$$
\begin{aligned}
(\alpha - \beta/\gamma)^{p^n} &= \sum_{i=0}^{p^n} \binom{p^n}{k} \alpha^{p^n-k}(-\beta/\gamma)^k \\
&= \alpha^{p^n} + (-\beta/\gamma)^{p^n}
\end{aligned}
$$

Ahora, debemos considerar dos casos. Si p es impar entonces $(-\beta/\gamma)^{p^n} = -(\beta/\gamma)^{p^n}$. Si $p = 2$ entonces $(-\beta/\gamma)^{p^n} = (\beta/\gamma)^{p^n}$. Sin embargo como la característica del campo es dos tenemos que $-1 = 1$, pues $1+1 = 0$. Por lo tanto, en ambos casos $(-\beta/\gamma)^{p^n} = -(\beta/\gamma)^{p^n}$.

Finalmente por nuestra suposición que α, β y γ son raices tenemos que $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$ y $\gamma^{p^n} = \gamma$.

Por lo tanto,

$$
\begin{aligned}
(\alpha - \beta/\gamma)^{p^n} &= \alpha^{p^n} + (-\beta/\gamma)^{p^n} \\
&= \alpha^{p^n} - (\beta/\gamma)^{p^n} \\
&= \alpha^{p^n} - \beta^{p^n}/\gamma^{p^n} \\
&= \alpha - \beta/\gamma
\end{aligned}
$$

Que era el resultado que estabamos buscando. Por lo tanto S es un campo y como contiene a todas las raices del polinomo $f_n(x)$ entonces debe coincidir con el campo de descomposición $\mathbb{F}_{p^n}$ puesto que por definición es el mínimo campo que contiene a todas las raíces del polinomio dado. □

c) Muestre que $|\mathbb{F}p^n| = p^n$ y que más aun F_{p^n} es el único cuerpo, módulo isomorfismo, con esta cardinalidad. En otras palabras muestre que si L es un cuerpo tal que $|L| = p_n$ entonces $F_{p^n} \cong L$.

Demostración. Como el polinomio no tiene raíces repetidas su número de raíces es igual a su grado, es decir, $|\mathbb{F}^{p^n}| = p^n$. Ahora para demostrar que cualquier otro campo L con tamaño p^n es esencialmente el mismo campo solo basta demostrar que para cualquier $\alpha \in L$ se cumple que $(\alpha)^{p^n} = \alpha$.

Debemos considerar dos casos. Si $\alpha = 0$ entonces $0^{p^n} = 0$. Si $\alpha \neq 0$ entonces $\alpha \in L^*$. Ya tenemos un teorema que nos dice que L^* es un grupo cíclico de tamaño $p^n - 1$. Por lo tanto, por el teorema de Lagrange tenemos que $\alpha^{p^n-1} = 1$. Finalmente multiplicando por α a ambos lados obtenemos la expresión deseada. □

(*Sugerencia: Muestre que si* $\alpha \in L$ *entonces* $(\alpha)^{p^n} = \alpha$)

5. Sea K un cuerpo tal que K tiene característica 0 o K es finito. Muestre que K es perfecto. (Recuerde que un cuerpo es *perfecto* si cualquier extensión finita es separable.)

Demostración. En el primer caso, si K tiene característica 0, entonces tome L una extensión finita de K. Por una tarea anterior finita implica algebraica. Entonces cada elemento de L tiene asociado un polinomio irreducible de grado ≥ 1 en K. Entonces podemos utilizar el criterio de la derivada para demostrar que todos estos polinomios irreducibles asociados a cada elemento son separables. Sea $\alpha \in L$ y sea $p(x) \in K[x]$ tal que $p(\alpha) = 0$. Si tomamos $p'(x)$ obtenemos un polinomio de un grado menor y tal que es diferente de 0, pues ninguno de los coeficientes se cancelan como en el caso de caracteristica p.

Entonces como $p(x)$ es irreducible esto implica que al tomar el g.c.d con $p'(x)$ que es un grado menor y por lo tanto diferente de $p(x)$ concluimos que el g.c.d. es igual 1, porque de lo contrario el g.c.d sería un factor de grado >0 y diferente de $p(x)$ que divide a $p(x)$ y por lo tanto $p(x)$ no sería irreducible.

Ahora para el caso en que el campo es de característica p tenemos que si el campo K es finito entonces cualquier extensión L finita tiene un número finito de elementos. Pero en una tarea anterior demostramos que si L es finito entonces su cardinalidad es igual a p^n para algún $n \in \mathbb{N}$. Pero entonces por el punto anterior L sería el cuerpo de descomposición del polinomio $x^{p^n} - x$. Concluimos entonces que es separable. □

6. Sea $\alpha \in \mathbb{R}$ definido como $\alpha := \sum_{i \geq 0} \frac{1}{10^{i!}}$. Utilice el siguiente Teorema de Liouville para mostrar que α es transcendente sobre $\mathbb{Q}$: (*Sugerencia: Muestre que para todo entero* $N > 0$ *existen* $p, q \in \mathbb{Z}$ *con* $q > 1$ *tales que* $0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^N}$).

Demostración. Sea $N \in \mathbb{N}$ tal que $N > 0$ y considere la suma finita $\sum_{i=0}^{N} \frac{1}{10^{i!}}$. Como es una suma finita de racionales esta suma es racional. De hecho podemos escribirla de la forma p/q con $p, q \in \mathbb{Z}$ como

$$\sum_{i=0}^{N} \frac{1}{10^{i!}} = \frac{\sum_{i=0}^{N} 10^{N!-i!}}{10^{N!}}..$$

Ahora tenemos que $\sum_{i=0}^{\infty} \frac{1}{10^{i!}} - \sum_{i=0}^{N} \frac{1}{10^{i!}} = \sum_{i=N+1}^{\infty} \frac{1}{10^{i!}}$.

Si consideramos esta serie como una expansión decimal de α es fácil ver que

$$0 < \sum_{i=N+1}^{\infty} \frac{1}{10^{i!}} < \frac{2}{10^{(N+1)!}}.$$

Ahora tenemos que $(N+1)! = N!(N+1) = N!N + N!$. Por lo tanto $10^{(N+1)!} = (10^{N!})^N 10^{N!}$. Además, si $N > 0$ tenemos que $10^{N!} > 2$. Por lo tanto $(10^{N!})^N 10^{N!} > 2 * (10^{N!})^N$ y luego $\frac{1}{(10^{N}!)^N} > \frac{2}{10^{(N+1)!}}$.

Finalmente llegamos a la expresión deseada

$$0 < \sum_{i=N+1}^{\infty} \frac{1}{10^{i!}} = \alpha - \frac{\sum_{i=0}^{N} 10^{N!-i!}}{10^{N!}} < \frac{1}{10^{(N!)^N}}.$$

Si asumieramos que α es algebráico entonces esta expresión contradeciría el teorema de Liouville. Por lo tanto, concluimos que α es trascendente.

$\square$