Algebra Abstracta: Tarea #5

Jonathan Andrés Niño Cortés

26 de febrero de 2015

1. Sea F un campo y sea $f(x)$ un polinomio no constante en $F[x]$. Describa el nilradical de $F[x]/(f(x))$ en términos de la factorización de $f(x)$

   Demostración. Como F es un campo tenemos que $F[x]$ es un dominio euclideano y por lo tanto es un D.I.P y un D.F.U. En primer lugar existe una factorización única de $f(x)$ en irreducibles. Sea dicha factorización $f(x) = \pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$. En un punto en una tarea anterior se demostró que el nilradical de R/I es igual a el rad I/I donde rad I es $\{r \in R | r^n \in I \text{ para algún} R \in \mathbb{Z}^+\}$

   Para nuestro caso rad $(f(x)) = (\pi_1 \cdots \pi_n)$ En efecto, para cualquier $r \in$ rad $(f(x))$ tenemos que $r^n = q\pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$. Entonces r también es divisible por los mismos irreducibles que r^n por lo que $r \in (\pi_1 \cdots \pi_n)$ y además $\pi_1 \cdots \pi_n \in$ rad $(f(x))$ pues $\pi_1^{\alpha} \cdots \pi_n^{\alpha} \in (f(x))$ para $\alpha = \text{máx}(\alpha_i)$.

   Por lo tanto el nilradical de $F[x]/(f(x))$ es $(\pi_1 \cdots \pi_n)/(f(x))$. □

2. *a*) Sean $F \subseteq K$ dos cuerpos y sean $p(x)$, $q(x)$ dos polinomios diferentes de cero en $F[x]$. Muestre que

   $$\text{m.c.d}_{F[x]}(p, q) = 1 \iff \text{m.c.d}_{K[x]}(p, q) = 1.$$

   Demostración. $F[x]$ y $K[x]$ son ambos dominios euclideos, y por lo tanto también son dominios de factorización única.

   $\Rightarrow$: m.c.d$_{F[x]}(p, q) = 1$ implica que existen $r, s \in P[x]$ tales que $pr + qs = 1$. Pero p, r, q y s petenecen a $K[x]$. Por lo tanto, m.c.d$_{K[x]}(p, q) = 1$.

   Observación: Tanto en $F[x]$ como en $K[x]$ las unidades son los polinomios de grado 0, es decir las constantes. Esto es una consecuencia de la norma euclidea asociada a estos anillos.

   $\Leftarrow$: Si suponemos por contradicción que $m =$ m.c.d$_{F[x]}(p, q) \neq 1$ entonces m es un polinomio de grado mayor a 0 que divide tanto a p como a q. Entonces extendiendo a $K[x]$, m sigue dividiendo tanto a p como a q y por lo tanto debe dividir a m.c.d$_{K[x]}(p, q)$, que por lo tanto no puede ser igual a 1 porque m no es una unidad en $K[x]$. □

b) Sea R un anillo conmutativo con identidad. La derivada formal en el anillo de polinomios $R[x]$ se define de la manera usual i.e., si $p(x) = a_0 + a_1x + \cdots + a_nx^n$ entonces

$$p'(x) := a_1 + 2a_2x^+3a_3x^2 \cdots + a_nnx^{n-1}$$

Sea F un cuerpo contenido en los números complejos y $p(x) \in F[x]$. Una raiz $\alpha \in \mathbb{C}$ de $p(x)$ se llama *raíz repetida* si $(x-\alpha)^2$ divide a $p(x)$ en $\mathbb{C}[x]$.
Sea $p(x) \in F[x]\backslash 0$ Muestre que m.c.d$(p, p') = 1$ si y sólo si p no tiene raíces repetidas.

Demostración. Por el literal anterior, esto es equivalente a demostrar que m.c.d$_{\mathbb{C}[x]}(p, p') = 1$ si y sólo si p no tienes raices repetidas.
$\Rightarrow$: Suponga que p tiene raices repetidas. Entonces $p(x) = (x-\alpha)^2q(x)$, donde $\alpha \in \mathbb{C}$ y $q(x) \in \mathbb{C}$. Por cálculo de variable compleja sabemos que la derivada es igual a $p'(x) = 2(x-\alpha)q(x) + (x-\alpha)^2q'(x)$. Concluimos que $(x-\alpha)$ divide tanto a p como a p'. Luego m.c.d$_{\mathbb{C}[x]}(p, p') \neq 1$.
$\Leftarrow$: Suponga que $p(x)$ no tiene raices repetidas. Luego $p = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. Además, sabemos que en $\mathbb{C}$ los polinomios de grado 1 son irreducibles por lo que esta es la factorización única en irreducibles de p. Entonces vamos a demostrar que níngun $x-\alpha_i$ divide a $p'(x)$ lo que implica que m.c.d$_{\mathbb{C}[x]}(p, p') = 1$., pues no tendrían factores irreducibles en común.
Obsérvese que $p(x) = (x-\alpha_i)q(x)$ donde $q(x)$ no es divisible por $(x-\alpha_i)$. Si $p'(x)$ fuera divisible por $(x-\alpha_i)$ entonces $q(x) = p'(x) - (x-\alpha_i)q'(x)$ sería divisible por $(x-\alpha_i)$ lo cual es una contradicción. Por lo tanto $p'(x)$ no es divisible por $x-\alpha_i$. Esto concluye la demostración. □

3. Sea R un D.F.U. y sea $a \in R$. De condiciones necesarias y suficientes sobre a de tal forma que $x^2 - a$ sea un polinomio irreducible en $R[x]$.

Demostración. La condición necesaria y suficiente para que $x^2 - a$ sea un polinomio irreducible en $R[x]$ es que a no sea un cuadrado perfecto. Por un lado es necesaria porque si $a = \alpha^2$ entonces $x^2 - a = (x-\alpha)(x+\alpha)$. Por otro lado es suficiente pues si suponemos que $x^2 - a$ es reducible, entonces existen polinomios que deben ser de grado 1, $(x+\alpha)(x+\beta)$ con $\alpha, \beta \in R$ tales que $(x+\beta)(x+\gamma) = x^2 - 1$. Por lo tanto, $x^2 + (\alpha+\beta)x + \alpha\beta = x^2 - 1$ de donde deducimos que $\alpha + \beta = 0$ y $\alpha\beta = -a$. Por lo tanto, $\alpha = -\beta$ y $-a = \alpha(-\alpha)$ de donde deducimos que $a = \alpha^2$ es un cuadrado perfecto.

□

4. Sea K un cuerpo y sea $f(x) \in K[x]$ un polinomio de grado al menos 1 que no es un cuadrado perfecto. Muestre que

$$K[x, y]/\langle y^2 - f(x)\rangle$$

es un dominio.

Demostración. Esto es una consecuencia del punto anterior, pues $K[x,y] = K[x][y]$ y nuestra suposición nos dice que $f(x)$ no es un cuadrado perfecto. Por lo tanto, $y^2 - f(x)$ es irreducible en $K[x,y]$. Pero además, como K es un cuerpo $K[x]$ sería un dominio euclideo y por lo tanto un D.F.U. y $K[x,y]$ sería un D.F.U. también por un teorema visto en clase. Por lo tanto como $y^2 - f(x)$ también es primo y por lo tanto $K[x,y]/\langle y^2 - f(x)\rangle$ es un dominio. □

5. Sea R un dominio con cuerpo de fracciones K. El anillo R se llama integralmente cerrado si todo $r \in K$ que es raiz de un polinomio mónico con coeficientes en R está en R.

   a) Muestre que todo D.F.U es integrálmente cerrado

   Demostración. Tome $p(x)$ un polinomio mónico en $R[x]$ y supongamos que $r \in K$ es una raíz de p. Entonces, $p(x)$ como polinomio en $K[x]$ es divisible por $(x-r)$, es decir que existen $q \in K[x]$ tal que $p(x) = (x-r)q(x)$. Como p es mónico q también tiene que ser mónico. Luego si q fuera de grado 0 tendría que ser 1, y esto implicaria que $p(x) = x - r$, pero como $p(x)$ pertenece a $R[x]$ esto implica que $r \in R$. Si $q(x)$ es de grado mayor entonces por el lema de Gauss (que podemos utilizar porque R es un D.F.U.) existen elementos $r, s \in F$ tales que $rq(x)$ y $s(x-r) \in R[x]$ y $p(x) = rq(x)s(x-r)$ pero como $p(x)$ es mónico esto implica que $rs = 1$, es decir $p(x) = q(x)(x-r)$ con $q(x)$ y $(x-r)$ en $R[x]$. Esto implica que $r \in R$. □

   b) Muestre que el anillo $\mathbb{C}[x,y]/\langle y^2 - x^3\rangle$ es un dominio que no es integralmente cerrado.

   Demostración. Sea $R = \mathbb{C}[x]\mathbb{C}[x,y]/\langle y^2 - x^3\rangle$
   x^3 no es cuadrado perfecto en $\mathbb{C}[x]$. Por lo tanto, el punto 4 nos permite concluir que R es un dominio. Notese que $x^3 \equiv y^2 \bmod \langle y^2 - x^3\rangle$. Ahora para demostrar que no es integralmente cerrado tomese el polinomio mónico $z^2 - x$. Este polinomio es irreducible en $R[z]$ pues claramente x no es un cuadrado perfecto de R. Pero si tomamos $K[z]$ donde K es el campo de fracciones de R. Entonces $y/x \in K$ sería una raiz del polinomio. En efecto $(y/x)^2 - x = y^2/x^2 - x$, pero $y^2 = x^3$, por lo tanto, $y^2/x^2 - x = x^3/x^2 - x = x - x = 0$. Esto demuestra que R no es un integralmente cerrado. □

   c) Sean m y n enteros positivos y suponga que m no es una potencia n-ésima perfecta (por ejemplo 32 no es un cuadrado perfecto y 25 no es un cubo perfecto.) Muestre que $\sqrt[n]{m}$ es irracional.

   Demostración. Por el punto a) tenemos que $\mathbb{Z}[x]$ es integralmente cerrado. Entonces considere el polinomio $x^n - m$, que es un polinomio mónico con coeficientes en $\mathbb{Z}$. $\sqrt[n]{m}$ es precisamente una raiz de este polinomio en $\mathbb{R}[x]$. Ahora si suponemos

que $\sqrt[n]{m}$ es racional entonces por el literal a) tendriamos que $\sqrt[n]{m}$ sería un entero. Es decir que $m = z^n$ para $z = \sqrt[n]{m} \in \mathbb{Z}$, lo que contradice nuestra suposición que m no es potencia n-ésima perfecta. □

6. Un anillo conmutativo con unidad R se llama anillo local si R tiene un único ideal maximal.

   a) Sean R un anillo conmutativo con identidad, M un ideal maximal de R y n un entero positivo. Muestre que R/M^n es un anillo local.

   b) Sea R un D.I.P y sea $I \neq 0$ un ideal de R. Muestre que R/I es isomorfo a un producto finito de anillos locales.

   Demostración. Por un punto realizado en una tarea anterior tenemos que si N es un ideal máximal en R/M^n entonces $N^* = \pi^{-1}(N)$ es un ideal máximal en R donde π es el homomorfismo natural entre R y R/M^n que claramente es sobreyectivo.

   Pero vemos que $M^n \subseteq N^*$ y que además como N^* es máximal entonces es primo. Ahora por un teorema visto en clase concluimos que $M \subseteq N^*$ o que $M^{n-1} \subseteq N^*$. Repitiendo este proceso n veces llegamos a que $M \subseteq N^*$. Pero como M es máximal esto significa que N^* debe ser igual a M. Por lo tanto, M/M^n es el único ideal máximal de R/M^n, es decir que es un anillo local. □

   Demostración. En primer lugar, como R es un D.I.P también es un D.F.U. Si $I = (1)$ no hay nada que demostrar pues $R/I = \{0\}$ es trivialmente un anillo local. Entonces, sea $I = (\alpha)$ y sea $\pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$ la factorización de α en irreducibles. Como π_i es irreducible entonces es primo, pero además como estamos en un D.I.P primo implica maximal. Luego cada (π_i) es máximal. Además $(\pi_i^{\alpha_i})$ y $(\pi_j^{\alpha_j})$ son comaximales pues sus generadores no tienen factores irreducibles en común. Luego por el teorema chino del residuo tenemos que $R/I \cong R/(\pi_1^{\alpha_1}) \times \cdots \times R/(\pi_n^{\alpha_n})$ donde cada $R/(\pi_i^{\alpha_i})$ es un anillo local por el punto a). □