Apuntes de los días 17/10 y 20/10

Vamos a estudiar una noción de multiplicidad para puntos en una curva algebraica. Par motivar este estudio, empezamos por recordar la noción de multiplicidad de una raíz de un polinomio. Antes de ello, daremos la definición de cierto tipo de anillo que será de utilidad.

**Definición 0.1.** Decimos que un anillo conmutativo $D$ con identidad (en donde $1_D \neq 0_D$) es un *dominio entero* si para todo $a.b \in D$ se cumple que

$$ab = 0_D \implies a = 0_D \quad \text{o} \quad b = 0_D.$$

⧫

**Ejemplo 0.2.** Los siguientes son algunos ejemplos básicos de dominios enteros.

1. El anillo de enteros $\mathbb{Z}$ es un dominio entero.
2. Todo cuerpo $F$ es un dominio entero.
3. Si $D$ es un dominio entero, entonces los anillos de polinomios $D[x_1, ..., x_n]$ con $n \geq 1$ también son dominios enteros.

◇

Sea $D$ un dominio entero y sea $f \in D[x]$ con $\text{grad}(f) = n \geq 0$ ($f \neq 0$). En $D[x]$ se cumple el Teorema del Factor y además se cumple que $f(x)$ tiene a lo sumo $n$ raíces en $D$, entonces aplicando dicho teorema a $f(x)$ una cantidad finita de veces, vemos que para cada $c \in D$ existe un entero máximo $0 \leq m_c \leq \text{grad}(f)$ tal que

$$f(x) = (x - c)^m g(x)$$

para un $g(x) \in D[x]$ con $x - c \not| g(x)$, es decir que $g(c) \neq 0$.

Al entero se le llama la *multiplicidad* de la raíz $c$ de $f$ (aquí abusamos ligeramente del lenguaje puesto que si $m_c = 0$ entonces $c$ no sería una raíz de $f$). Si $c$ tiene multiplicidad $1$ entonces decimos que $c$ es una *raíz simple*. Si $c$ tieme multiplicidad $m - c > 1$ entonces decimos que $c$ es una *raíz múltiple* de $f$.

Utilizando la noción de derivada formal de un polinomio, podemos dar un criterio para determinar si un polinomio tiene raíces múltiples o no.

**Definición 0.3.** Sea $R$ un anillo conmutativo con identidad y sea $f \in R[x]$ dado por $f = \sum_{k=0}^{n} a_k x^k$. La *derivada formal* de $f$ es el polinomio $f' = f'(x) \in R[x]$ definido por:

$$f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$$

⧫

Note que en general $\text{grad}(f') < \text{grad}(f)$, sin embargo como el siguiente ejemplo muestra, no siempre se tendrá que $\text{grad}(f') = \text{grad}(f) - 1$.

**Ejemplo 0.4.** En $\mathbb{F}_2[x]$ observe que si $f = x^2 \in \mathbb{F}_2[x]$, su derivada $f'(x) = 2x = 0 \in \mathbb{F}_2[x]$. ◇

Ésta noción de derivada formal no utiliza el concepto de límite como en cálculo, sin embargo satisface las propiedades usuales que cumplen las derivadas de funciones usualmente estudiadas en cálculo.

**Proposición 0.5.** *Sea $R$ un anillo conmutativo con identidad. Entonces para todo $f.g \in R[x]$ y para todo $c \in R$ se tiene que:*

1. $(cf)' = cf'$.
2. $(f + g)' = f' + g'$.
3. $(f \cdot g)' = f' \cdot g + f \cdot g'$.
4. $(g^n)' = ng^{n-1}g'$, *para todo* $n \in \mathbb{Z}_{\geq 1}$.

*Demostración.* Ejercicio. □

El siguiente Teorema nos da un criterio para decidir si un polinomio tiene ráices múltiples o no.

**Teorema 0.6.** *Sea $D$ un dominio entero y suponga que $D$ es un subanillo de un dominio entero $E$. Para $f \in D[x]$ y $c \in E$ se cumple que:*

1. *$c$ es una raíz múltiple de $f$ si y sólo si $f(c) = 0$ y $f'(c) = 0$.*
2. *Si $D$ es un cuerpo y $f$ es primo relativo a $f'$ entonces $f$ no tiene raíces múltiples en $E$.*

*Demostración.* ($\Rightarrow$): Sea $m_c > 1$ la multiplicidad de $c$. Entonces existe $g(x) \in E[x]$ tal que $f(x) = (x-c)^{m_c} g(x)$ con $g(c) \neq 0$. Derivando o aplicando la derivada formal obtenemos:

$$f'(x) = m_c(x-c)^{m_c-1} g(x) + (x-c)^{m_c} g'(x)$$

Como $m_c > 1$ se tiene que $m_c - 1 > 0$ por lo tanto $f'(c) = 0$.
($\Leftarrow$): De nuevo si $m_c$ es la multiplicidad de $c$ y $f(c) = f'(c) = 0$ y por tanto $m_c \geq 1$, además $f'(x) = m_c(x-c)^{m_c-1} g(x) + (x-c)^{m_c} g'(x)$ para algún $g(x) \in E[x]$ con $g(c) \neq 0$. Si fuera que $m_c = 1$ entonces $f'(x) = g(x) + (x-c)g'(x)$, lo que implica que $0 = f'(c) = g(c) + 0$, es decir $g(c) = 0$, lo cual es una contradicción y por tanto $m_c > 1$. □

**Ejemplo 0.7.** Sea $D = \mathbb{R}$ Y $E = \mathbb{C}$, y considere el polinomio $f(x) = (x^2+1)^2$. Éste polinimio no tiene raíces en $\mathbb{R}$. Sin embargo tiene dos ráices en $\mathbb{C}$: $c_1 = i$ y $c_2 = -i$, de multiplicidades $m_{c_1} = m_{c_2} = 2$. Note que

$$f'(x) = 2(x^2+1) \cdot 2x \in \mathbb{R}[x] \subset \mathbb{C}[x]$$

Y

$$f'(\pm i) = 2((\pm i)^2 + 1) \cdot 2 \cdot \pm i = 0$$

Lo que confirma que ambas raíces son múltiples. ◇

Ejercicio: Probar que si $c$ es una raíz de multiplicidad $m_c$ entonces $f(c) = f'(c) = f^{(2)}(c) = \cdots f^{(m_c-1)}(c) = 0$ y $f^{(m_c)}(c) \neq 0$. Donde el símbolo $f^{(n)}$ se define por inducción como $f^{(1)} = f'$ y $f^{(n)} = (f^{(n-1)})'$, lo que es conocido como la *derivada $n$-ésima o de orden $n$* de $f$.

**Definición 0.8.** Sea $R$ un anillo conmutativo con identidad. Para cada polinomio $F \in R[x_1, ..., x_n]$ y cada $i \in 1, ..., n$ se define la *derivada parcial* de $F$ con respecto a $x_i$ como la derivada formal de $F$ al considerar $F$ como un polinomio en $R[x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n][x_i]$, y se denota ésta derivada por $\frac{\partial F}{\partial x_i}$ ó $F_{x_i}$. ♦

**Proposición 0.9.** *Sea $R$ un anillo conmutativo con identidad, entonces para todo $F, G \in R[x_1, ..., x_n]$ y cualesquiera $a, b \in R$ se cumple lo siguiente:*

1. $\frac{\partial}{\partial x_i}(aF + bG) = a\frac{\partial F}{\partial x_i} + b\frac{\partial G}{\partial x_i}$.
2. *Si $F \in R[x_1, \cdots x_{i-1}, x_{i+1}, \cdots, x_n]$ entonces $\frac{\partial F}{\partial x_i} = 0 \in R[x_1, \cdots, x_n]$.*
3. $\frac{\partial}{\partial x_i}(F \cdot G) = \frac{\partial F}{\partial x_i} \cdot G + F \cdot \frac{\partial G}{\partial x_i}$.
4. $\frac{\partial}{\partial x_i}(F^n) = nF^{n-1}\frac{\partial}{\partial x_i}(F^{n-1})$, *para todo $n \geq 1$.*
5. *Si $G_1, \cdots G_n \in R[x]$ y $F \in R[x_1, \cdots x_n]$ entonces:*

$$\frac{\partial}{\partial x_i} F(G_1, \cdots, G_n) = \sum_{i=1}^{n} \frac{\partial}{\partial x_i} F(G_1, \cdot, G_n) \cdot \frac{\partial G_i}{\partial x}$$

6. *Si definimos:*

$$F_{x_i,x_j} := \frac{\partial}{\partial x_j}\left(\frac{\partial F}{\partial x_i}\right)$$

*Entonces hay igualdad de las derivadas cruzadas iteradas o cruzadas:*

$$F_{x_i,x_j} = F_{x_j,x_i}$$

*Es decir*

$$\frac{\partial}{\partial x_j}\left(\frac{\partial F}{\partial x_i}\right) = \frac{\partial}{\partial x_i}\left(\frac{\partial F}{\partial x_j}\right)$$

*Lo cual en una notación más compacta se suele escribir como*

$$\frac{\partial^2 F}{\partial x_i x_j} = \frac{\partial^2 F}{\partial x_i x_j}$$

*Demostración.* Ejercicio □

**0.1. Puntos múltiples y rectas tangentes.** Para el siguiente estudio que emprenderemos es conveniente redefinir el concepto de curva algebraica. Para ésto, si $k$ es un cuerpo, definimos una relación de equivalencia $\sim$ en el anillo $k[x, y]$ decretando que dos polinomios $F, G \in k[x, y]$ son equivalentes si y sólo si existe $\alpha \in k^\times$ tal que $F = \alpha G$. (Es un ejercicio para el lector verificar que ésta relación es de equivalencia).

**Definición 0.10** (Curva algebraica afín)**.** Diremos que una *curva algebraica afín plana* es una clase de equivalencia de polinomios no constantes en $k[x, y]/\sim$. ⧫

Para no recargar mucho el lenguaje, nos referiremos a un polinomio dado $F$ como una curva, en lugar de estar haciendo mención de la clase de equivalencia de $F$. Por ejemplo, escribiremos "la curva plana $y - x^2$".

**Definición 0.11.** El *grado* de una curva (bajo ésta nueva definición) es el grado de cualquier polinomio en la clase de equivalencia que la define. ⧫

**Definición 0.12.** Si $F \in k[x, y]$ se factoriza en factores irreducibles como $F = F_1^{e_1} \cdots F_r^{e_r}$, decimos que los $F_i$ son las *(curvas) componentes* de $F$ y que $e_i$ es la *multiplicidad* de la componente $F_i$.
Además si $e_i = 1$ decimos que $F_i$ es una componente *simple* y si $e_i > 1$ entonces es *múltiple* ⧫

**Definición 0.13** (Punto simple o no singular)**.** Sea $F$ una curva y sea $P = (a, b) \in k^2$ un punto en $F$ (es decir $F(P) = 0$). Decimos que $P$ es un punto *simple o no singular* si

$$\left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P)\right) \neq (0, 0)$$

⧫

Un punto que no es simple se llama *múltiple o singular*. Decimos que una curva que no tiene puntos singulares es una curva no singular.
Si $F \in k[x, y]$ es una curva, denotamos el conjunto de puntos singulares en $F$ como

$$\begin{aligned}\operatorname{sing}(F) &:= \{P \in k^2 \mid P \text{ es un punto singular de } F\} \\ &= \{P \in k^2 \mid \left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P)\right) = (0, 0)\}\end{aligned}$$

**Definición 0.14.** Sea $F$ una curva y sea $P = (a, b) \in k^2$ un punto en $F$. Si $P$ es simple la *recta tangente* a $F$ en $P$ se define por la curva

$$\frac{\partial F}{\partial x}(P)(x - a) + \frac{\partial F}{\partial y}(P)(y - b) = 0$$

⧫

## EJERCICIOS

**Ejercicios de la sección 0.**

0.1 Demuestre la Proposición 0.5

0.2 Demuestre la Proposición 0.9.

0.3 Sea $f \in \mathbb{F}_2[x]$. Demuestre lo siguiente.

(a) $f'$ es un cuadrado perfecto en $\mathbb{F}_2[x]$ (es decir, que existe $g \in \mathbb{F}_2[x]$ tal que $f' = g^2$).
(b) $f$ es un cuadrado perfecto en $\mathbb{F}_2[x]$ sí y solo sí $f' = 0$.

0.4 Sea $k$ un cuerpo y sea $F := ax + by \in k[x, y]$, con $a, b \in k$. Demuestre que

$$F = x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y}.$$

0.5 Sea $k$ un cuerpo y sea $F := ax^2 + bxy + cy^2 \in k[x, y]$, con $a, b, c \in k$. Demuestre que

$$2F = x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y}.$$

0.6 (**Identidad de Euler para polinomios homogéneos**) Sea $k$ un cuerpo y sea $F \in k[x_1, \ldots, x_n]$ un polinomio homogéneo de grado $m$. Demuestre que

$$mF = \sum_{i=1}^{n} x_i \frac{\partial F}{\partial x_i}$$

0.7 En este ejercicio se demuestra una versión más refinada del resultado de la parte a) del Teorema 0.6. Sea $D$ un dominio entero y suponga que $D$ es un subanillo de un dominio entero $E$. Si $f \in D[x]$ y $c \in E$, entonces $c$ es una raíz de $f$ de multiplicidad $m$ si y sólo si $f(c) = f'(c) = \cdots = f^{(m-1)}(c) = 0$ y $f^{(m)}(c) \neq 0$.

Los siguientes dos ejercicios nos llevan a una definición alternativa pero equivalente de la derivada formal de un polinomio, que se parece a la definición usual de derivada estudiada en cálculo.

0.8 Sea $R$ un anillo conmutativo con identidad. Demuestre que $y - x$ divide a $y^n - x^n$ en $R[x, y]$ para todo $n \in \mathbb{Z}_{\geq 0}$. Use esto para demostrar que $y - x$ divide a $f(y) - f(x)$ en $R[x, y]$ para todo polinomio en una variable $f \in R[T]$.

0.9 Sea $R$ un anillo conmutativo con identidad. El resultado del ejercicio anterior demuestra que si $f \in R[T]$, entonces

$$\Delta_f(x, y) := \frac{f(y) - f(x)}{y - x} \in R[x, y].$$

Este cociente es como el cociente de diferencias utilizado al calcular derivadas en cálculo diferencial. Demuestre que la derivada formal de $f$ es dada por $f'(x) = \Delta_f(x, x)$. (**Sugerencia:** Verifique primero que el resultado es cierto para algunos polinomios particulares como $f = T^2$, $f = T^3 + 2T - 1$, etc.)