Tarea 4 – Aritmética

Profesor: Pedro Montero, Ayudante: Tobías Martínez

Departamento de Matemática, Universidad Técnica Federico Santa María

Fecha de entrega:[1] Hasta el Domingo 2 de Julio de 2023 a las 23h59.

Esta Tarea puede ser realizada en grupos de 1 o 2 personas, y se debe **indicar el nombre de cada integrante**. Deben escoger 2 de los 3 problemas para resolver. Además, es posible realizar la tarea en grupos de 3 personas, pero en tal caso deben realizar **todos** los problemas.

Problema A: Lema de Hensel

El objetivo de este problema es probar el famoso **Lema de Hensel** que, en términos simples, señala que si un polinomio en una variable tiene una raíz simple módulo un primo p, entonces esta raíz puede ser levantada a una raíz módulo p^n para todo n. Las ideas son muy similares al método de Newton-Raphson en Análisis Numérico.

Sea $\mathbf{K}$ un cuerpo completo respecto a un valor absoluto no-arquimedeano no-trivial $|\cdot|\colon \mathbf{K} \to \mathbf{R}^{\geq 0}$ y sea $v \in \mathrm{Pl}(\mathbf{K})$ el lugar asociado. Recordemos que

$$\mathscr{O}_v = \{x \in \mathbf{K},\ |x| \leq 1\},$$

el cual es un anillo local con ideal maximal $\mathfrak{m}_v = \{x \in \mathbf{K},\ |x| < 1\}$. Sea $f \in \mathscr{O}_v[X]$ tal que $f' \neq 0$ y sea $S \subseteq \mathbf{K}$ el conjunto de raíces de f'. Así, definimos la función

$$g : \mathbf{K} \setminus S \longrightarrow \mathbf{K},\ x \longmapsto x - \frac{f(x)}{f'(x)},$$

y denotamos $\mathscr{D} := \{x \in \mathscr{O}_v,\ |f(x)| < |f'(x)|^2\}$.

1. Pruebe que $\mathscr{D} \neq \emptyset$ si se cumple la condición siguiente:

   > Suponga que $|\cdot|$ está inducido por una valuación discreta sobreyectiva no-trivial $v : \mathbf{K} \to \mathbf{Z} \cup \{+\infty\}$ y que existe $x \in \mathscr{O}_v$ tal que $v(f(x)) \geq 2n+1$ y $v(f'(x)) \leq n$ para cierto $n \in \mathbf{N}^{\geq 1}$.

Para el resto de la discusión asuma que $\mathscr{D} \neq \emptyset$, fije $\alpha \in \mathscr{D}$.

2. Pruebe que para todo $x \in \mathscr{O}_v$ se tiene que X^2 divide a $f(x+X) - f(x) - Xf'(x) \in \mathscr{O}_v[X]$ y que X divide a $f'(x+X) - f'(x) \in \mathscr{O}_v[X]$.

3. Pruebe que para todo $x \in \mathscr{D}$ se tiene que $|f'(g(x))| = |f'(x)|$ y que

   $$\frac{|f(g(x))|}{|f'(g(x))|^2} \leq \left(\frac{|f(x)|}{|f'(x)|^2}\right)^2.$$

   Deducir que $g(\mathscr{D}) \subseteq \mathscr{D}$.

Definamos la sucesión $(\alpha_n)_{n\in\mathbf{N}} \subseteq \mathscr{D}$ mediante $\alpha_0 := \alpha$ y $\alpha_{n+1} = g(\alpha_n)$ para todo $n \in \mathbf{N}$.

4. Sea $\lambda := |f(\alpha)|/|f'(\alpha)|^2 < 1$. Demuestre que $|\alpha_{n+1} - \alpha_n| \leq \lambda^{2^n}$ y que la sucesión $(\alpha_n)_{n\in\mathbf{N}}$ converge en $\mathscr{D}$ a una raíz β de f.

5. Pruebe que $|\alpha - \beta| \leq \frac{|f(\alpha)|}{|f'(\alpha)|}$.

6. Sea $\beta' \neq \beta$ otra raíz de f. Demuestre que $|\beta' - \beta| \geq |f'(\alpha)|$.

Para concluir, consideremos en lo que sigue un número primo p y un polinomio $f \in \mathbf{Z}[X]$.

7. Sea $n \in \mathbf{N}^{\geq 1}$ y suponga que existe $\alpha \in \mathbf{Z}$ tal que

   $$f(\alpha) \equiv 0 \mod p^{2n+1} \text{ y tal que } f'(\alpha) \text{ no es divisible por } p^{n+1}.$$

   Pruebe que existe una *única* raíz $\beta \in \mathbf{Z}_p$ en el anillos de enteros p-ádicos, tal que $\beta \equiv \alpha \mod p^{2n+1}$.

[1] Factor de retraso: 0.7 por 1 día de retraso, 0.55 por 2 días de retraso, 0.01 por 3 días de retraso.

Problema B: Teorema de Aproximación

Sea p un número primo. El objetivo de este problema es estudiar propiedades de los números p-ádicos $\mathbf{Q}_p$ y los enteros p-ádicos $\mathbf{Z}_p$.

1. Sea $\mathbf{K}$ un cuerpo completo respecto a un valor absoluto no-arquimedeano no-trivial $|\cdot|\colon \mathbf{K} \to \mathbf{R}^{\geq 0}$. Pruebe que la serie numérica $\sum_{n\in\mathbf{N}} a_n$ converge en $\mathbf{K}$ si y sólo si $\lim\limits_{n\to+\infty} a_n = 0$.

2. Pruebe que $\mathbf{Z}_p \overset{\text{def}}{=} \{x \in \mathbf{Q}_p,\ |x|_p \leq 1\}$ es la adherencia del anillo de enteros $\mathbf{Z}$ en $\mathbf{Q}_p$.

3. Pruebe que todo elemento $x \in \mathbf{Z}_p$ puede ser escrito de manera única de la forma

$$x = \sum_{n\in\mathbf{N}} a_n p^n$$

   donde $a_n \in \{0, 1, \ldots, p-1\}$ para todo $n \in \mathbf{N}$. Deducir (e.g. usando el argumento diagonal de Cantor) que los enteros p-ádicos $\mathbf{Z}_p$ no son un conjunto numerable.

4. Considere el conjunto de Cantor

$$\mathscr{C} := \left\{ \alpha \in \mathbf{R},\ \exists\, (a_n)_{n\in\mathbf{N}} \in \{0,2\}^{\mathbf{N}} \text{ tal que } \alpha = \sum_{n\in\mathbf{N}} a_n 3^{-(n+1)} \right\} \subseteq \mathbf{R}.$$

   Pruebe que $\varphi : \mathbf{Z}_2 \xrightarrow{\sim} \mathscr{C},\ \sum_{n\in\mathbf{N}} a_n 2^n \mapsto \sum_{n\in\mathbf{N}} 2a_n 3^{-(n+1)}$ es un homeomorfismo.

Por último, nos enfocaremos en demostrar el siguiente resultado:

> **Teorema de Aproximación débil:** Sea $\mathbf{K}$ un cuerpo y sean $|\cdot|_1, \ldots, |\cdot|_n$ valores absolutos no-triviales en $\mathbf{K}$ induciendo lugares diferentes en $\mathrm{Pl}(\mathbf{K})$. Entonces, dada cualquier n-tupla $(\alpha_1, \ldots, \alpha_n) \in \mathbf{K}^n$ y cualquier $\varepsilon \in \mathbf{R}^{>0}$, existe $\beta \in \mathbf{K}$ tal que $|\alpha_i - \beta|_i < \varepsilon$ para todo $i \in \{1, \ldots, n\}$.

Con la notación e hipótesis del Teorema anterior:

5. Pruebe que existen $a, b \in \mathbf{K}$ de tal suerte que $|a|_1 < 1$ y $|a|_n \geq 1$ (resp. $|b|_n < 1$ y $|b|_1 \geq 1$), y deducir que existe $c \in \mathbf{K}$ tal que $|c|_1 > 1$ y $|c|_n < 1$.

6. Demuestre, usando inducción en n, que existe $z \in \mathbf{K}$ tal que $|z|_1 > 1$ y $|z|_j < 1$ para todo $j \in \{2, \ldots, n\}$.

   Para ello, suponga que el resultado es cierto para $j = 2, \ldots, n-1$ (note que el caso $n = 2$ ya fue probado en el ítem anterior), es decir, existe $z \in \mathbf{K}$ tal que $|z|_1 > 1$ y $|z|_j < 1$ para $j = 2, \ldots, n-1$. Considere separadamente los siguientes casos:

(Caso 1) Si $|z|_n \leq 1$, demuestre usando el ítem (5) que existe $c \in \mathbf{K}$ y $m \in \mathbf{N}^{\geq 1}$ tal que $z' = z^m c$ cumple la propiedad deseada.

(Caso 2) Si $|z|_n > 1$, proceda como sigue:

(i) Demuestre que la sucesión

$$b_m = \frac{z^m}{1 + z^m}$$

converge a 1 con respecto a $|\cdot|_1, |\cdot|_n$ y converge a 0 con respecto a $|\cdot|_j$ para $j = 2, \ldots, n-1$.

(ii) De manera similar al Caso 1, demuestre que existe $c \in \mathbf{K}$ y $m \in \mathbf{N}^{\geq 1}$ tal que $z' = b_m c$ cumple la propiedad deseada.

7. Sea $z \in \mathbf{K}$ y b_m como en el ítem (6). Pruebe que la sucesión $(b_m)_{m\in\mathbf{N}}$ verifica que $b_m \xrightarrow{m\to+\infty} 1$ respecto a $|\cdot|_1$ y que $b_m \xrightarrow{m\to+\infty} 0$ respecto a $|\cdot|_j$ con $j \in \{2, \ldots, n\}$, i.e., existe $z_1 \in \mathbf{K}$ cercano a 1 resp. a $|\cdot|_1$ y cercano a 0 respecto al resto de los valores absolutos. Por simetría, construir $z_i \in \mathbf{K}$ tal que z_i es cercano a 1 respecto a $|\cdot|_i$ y cercano a 0 respecto al resto de los valores absolutos. Probar que

$$\beta := \alpha_1 z_1 + \ldots + \alpha_n z_n$$

   verifica la conclusión del Teorema de aproximación débil.

Observación: Notar que el Teorema de Aproximación débil está relacionado con el Teorema Chino del Resto. En efecto, si $\mathbf{K} = \mathbf{Q}$ y tenemos n valores absolutos p-ádicos diferentes $|\cdot|_{p_i}$ entonces para toda n-tupla de números racionales $(a_1, \ldots, a_n)$ podemos encontrar $x \in \mathbf{Q}$ de tal suerte que $|x - a_i|_{p_i} < \varepsilon$, i.e., $x - a_i \equiv 0 \pmod{p_i^k}$ para cualquier $k \in \mathbf{N}^{\geq 1}$. El **Teorema de Aproximación Fuerte** asegura que podemos encontrar $x \in \mathbf{Q}$ que, además de lo anterior, cumple $|x|_p \leq 1$ para todo $p \in \mathscr{P} \setminus \{p_1, \ldots, p_n\}$.

Problema C: Teorema de la función implícita

El objetivo de este problema es probar la versión no-arquimedeana del Teorema de la función implícita. Para ello considere $\mathbf{K}$ un cuerpo completo y *localmente compacto* respecto a un valor absoluto no-arquimedeano no-trivial $|\cdot|\colon \mathbf{K} \to \mathbf{R}^{\geq 0}$ y sea $v \in \mathrm{Pl}(\mathbf{K})$ el lugar asociado. Recordemos que

$$\mathscr{O}_v = \{x \in \mathbf{K},\ |x| \leq 1\},$$

el cual es un anillo local con ideal maximal $\mathfrak{m}_v = \{x \in \mathbf{K},\ |x| < 1\}$.

En todo lo que sigue, fijamos $n \in \mathbf{N}^{\geq 1}$ y dotamos a $\mathbf{K}^n$ de la topología producto. Además, para cada polinomio en varias variables $f \in \mathbf{K}[X_1, \ldots, X_n]$ definimos

$$V(f) := \{x \in \mathbf{K}^n,\ f(x) = 0\}.$$

En todo el problema, asumiremos que $V(f)$ *es suave en* $x = (x_1, \ldots, x_n) \in V(f)$, i.e., se verifica que

$$d_x f = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(x)\, dX_i \neq 0.$$

1. Pruebe que existe $i \in \{1, \ldots, n\}$ y una vecindad abierta W de x en $\mathbf{K}^n$ tal que $\frac{\partial f}{\partial X_i}(y) \neq 0$ para todo $y \in W$.

Con la notación del ítem (i), definimos $\pi : V(f) \to \mathbf{K}^{n-1},\ (y_1, \ldots, y_n) \mapsto (y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n)$. Además, fijemos $\xi \in \mathbf{K}$ tal que $|\xi| < 1$.

2. Pruebe que existen enteros $a, b \in \mathbf{N}$ tales que

$$g(X_1, \ldots, X_n) := \xi^a f(x_1 + X_1, \ldots, x_n + X_n)$$

verifica las siguientes condiciones:

(i) $g \in \mathscr{O}_v[X_1, \ldots, X_n]$.

(ii) $|g(y)| < |\frac{\partial g}{\partial X_i}(y)|^2$ para todo $y = (y_1, \ldots, y_n) \in \mathbf{K}^n$ con $y_j \in \langle \xi^b \rangle$ para todo $j \in \{1, \ldots, n\}$.

Indicación: Buscar $a \in \mathbf{N}$ *que cumpla (i), y luego adaptar* $b \in \mathbf{N}$ *para que cumpla (ii).*

3. Sea $V(g) := \{y \in \mathbf{K}^n,\ g(y) = 0\}$. Pruebe que la restricción de π a $V(g) \cap (\langle \xi^b \rangle, \ldots, \langle \xi^b \rangle)$ es sobreyectiva.

4. Pruebe que existe una vecindad compacta K de 0 tal que la restricción de π a $V(g) \cap K$ es un homeomorfismo.

5. Pruebe que existe una vecindad K' de $x \in V(f)$ tal que la restricción de π a $V(f) \cap K'$ es un homeomorfismo.