Tarea 2 (MAT214)

Pedro Montero
pedro.montero@usm.cl

Sea A un anillo conmutativo. Si $\varphi : A \to B$ es un morfismo de anillos y $I \subseteq A$ es un ideal, denotaremos por $I \cdot B$ o por $\varphi(I) \cdot B$ al ideal generado por $\varphi(I)$.

Problema 1 (30 puntos)

El objetivo de este problema es estudiar unidades en un anillo y su relación con el ideal radical de Jacobson. Recordemos que una *unidad* en A es un elemento $a \in A$ tal que existe $b \in A$ de tal suerte que $ab = 1$. El conjunto de unidades de A forma un grupo multiplicativo y es denotado $A^\times$. Definimos el (ideal) *radical de Jacobson* del anillo A, $\mathrm{rad}(A)$, como la intersección de todos los ideales maximales de A.

1. Sea $a \in A$. Probar que $a \in \mathrm{rad}(A)$ si y sólo si $1 - ab$ es una unidad para todo $b \in A$.
2. Recordemos que $a \in A$ es *nilpotente* si existe $n \in \mathbb{N}^{\geq 1}$ tal que $a^n = 0$, es decir, $a \in \mathrm{nil}(A)$. Sea $a \in A$ nilpotente. Demostrar que $1 + a$ es una unidad en A y deducir que la suma de un elemento nilpotente y de una unidad es también una unidad.
3. Sea $A[x]$ el anillo de polinomios en una variable x con coeficientes en A y sea $f = a_0 + a_1 x + \ldots + a_n x^n \in A[x]$. Probar que f es nilpotente en $A[x]$ si y sólo si $a_0, \ldots, a_n$ son nilpotentes en A.
4. Sea $a \in A$ nilpotente y $\mathfrak{p} \subseteq A$ un ideal primo. Probar que $a \in \mathfrak{p}$.
5. Demostrar que $\mathrm{nil}(A[x]) = \mathrm{rad}(A[x])$.

Problema 2 (40 puntos)

El objetivo de este problema es estudiar algunas propiedades geométricas del *espectro de un anillo* al dotarlo de su topología [1] de Zariski. Se define el espectro del anillo A por

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subseteq A,\ \mathfrak{p} \text{ ideal primo}\}.$$

Por motivos sicológicos, es conveniente denotar a un ideal primo de A por la letra x cuando se le piensa como un punto de $X = \mathrm{Spec}(A)$, al cual denotaremos como $\mathfrak{p}_x$ cuando se le piensa como un ideal de A. Dado un subconjunto $S \subseteq A$, definimos

$$V(S) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid S \subseteq \mathfrak{p}\}.$$

1. Demostrar que si $I = \langle S \rangle$ es el ideal generado por un subconjunto $S \subseteq A$, entonces $V(S) = V(I) = V(\sqrt{I})$.
2. Verificar que los conjuntos $V(S)$ verifican los axiomas de los conjuntos cerrados en un espacio topológico. Dicha topología en $X = \mathrm{Spec}(A)$ será llamada **topología de Zariski**.
   Indicación : Para probar que la unión de dos cerrados es un conjunto cerrado, verificar que para dos ideales $I, J \subseteq A$ se tiene que $V(I) \cup V(J) = V(IJ)$.
3. Describir (e.g. dibujar) $\mathrm{Spec}(\mathbb{Z})$, $\mathrm{Spec}(\mathbb{R})$, $\mathrm{Spec}(\mathbb{C})$ y $\mathrm{Spec}(\mathbb{C}[x])$.
4. Recordemos que un espacio topológico X es *quasi-compacto* si todo cubrimiento abierto de X admite un subrecubrimiento finito. Demostrar que $\mathrm{Spec}(A)$ con la topología de Zariski es quasi-compacto.
   Indicación : Dado $f \in A$, denotamos por U_f el complemento de $V(f)$ en $\mathrm{Spec}(A)$. Notar que basta considerar cubrimientos abiertos de la forma $\{U_{f_i}\}_{i \in I}$ y probar que si $\mathrm{Spec}(A) = \cup_{i \in I} U_{f_i}$ entonces $\langle \{f_i\}_{i \in I} \rangle = A$ y por ende podemos escribir $1 = \sum_{i \in J} g_i f_i$ para cierto conjunto finito $J \subseteq I$ y ciertos $g_i \in A$. Concluir que $\mathrm{Spec}(A) = \cup_{i \in J} U_{f_i}$.
5. Sea $x \in \mathrm{Spec}(A)$. Probar que el conjunto $\{x\}$ (singleton) es cerrado para la topología de Zariski si y sólo si el ideal $\mathfrak{p}_x$ es maximal. Dar un ejemplo de un punto cerrado y de un punto no-cerrado en $\mathrm{Spec}(\mathbb{Z})$.

Problema 3 (30 puntos)

El objetivo de este problema es estudiar la *localización* de un anillo respecto a un subconjunto multiplicativo. Recordemos que un subconjunto $S \subseteq A$ es multiplicativo si $1 \in S$ y si $a, b \in S$ implica que $ab \in S$. Sea $S \subseteq A$ un subconjunto multiplicativo y definamos en el conjunto $A \times S$ la relación de equivalencia siguiente :

$$(a, s) \sim (a', s') \Leftrightarrow \exists t \in S,\ t(as' - a's) = 0.$$

Denotaremos por $S^{-1}A := (A \times S)/\sim$ al conjunto cociente, y por $\frac{a}{s}$ la clase de equivalencia de (a, s). Decimos que $S^{-1}A$ es la *localización* de A respecto a S.

1. Sea X un conjunto y sea $\tau = \{U_i\}_{i \in I}$ una familia de subconjuntos de X. Decimos que τ es una **topología** si $\emptyset \in \tau$ y $X \in \tau$, si toda unión arbitraria $\cup_{j \in J} U_j \in \tau$ para todo $J \subseteq I$, y si la intersección $U_1 \cap U_2 \in \tau$ para cualquier par $U_1, U_2 \in \tau$. Los elementos de τ son llamados **abiertos** y sus complementos **cerrados**.

1. Probar que si A es un dominio entonces $S = A\backslash\{0\}$ es multiplitícativo y $S^{-1}A = K_A$ es el cuerpo de fracciones de A. Probar que si $f \in A$ no es nilpotente, entonces $S = \{f^n\}_{n\in\mathbb{N}}$ es multiplicativo. En este último caso, denotamos $S^{-1}A$ por A_f.
2. Demostrar que la suma $\frac{a}{s} + \frac{b}{r} := \frac{ar+bs}{sr}$ y multiplicación $\frac{a}{s} \cdot \frac{b}{r} := \frac{ab}{rs}$ están bien definidas en $S^{-1}A$. Luego, $S^{-1}A$ es un anillo conmutativo (no es necesario probarlo). Probar que la aplicación $\iota : A \to S^{-1}A$ dada por $a \mapsto \frac{a}{1}$ es un morfismo de anillos y determinar $\ker(\iota)$.
3. Probar que la aplicación $\mathrm{Spec}(S^{-1}A) \to \{\mathfrak{q} \in \mathrm{Spec}(A) \mid \mathfrak{q} \cap S = \emptyset\}$ definida por $\mathfrak{p} \mapsto \iota^{-1}(\mathfrak{p}) \subseteq A$ es una biyección, cuya inversa está dada por $\mathfrak{q} \mapsto S^{-1}\mathfrak{q} := (S \times \mathfrak{q})/\sim = \mathfrak{q} \cdot S^{-1}A$, el ideal generado por $\iota(\mathfrak{q})$. Deducir que si $f \in A$ no es nilpotente, entonces hay una biyección entre $\mathrm{Spec}(A_f)$ y el abierto U_f de $\mathrm{Spec}(A)$ definido como el complemento de $V(f)$.
4. Demostrar que los elementos del conjunto $\iota(S)$ son unidades en el anillo $S^{-1}A$. En otras palabras, los elementos de S pasan a ser invertibles al localizar.
5. Demostrar la propiedad universal de la localización : Para todo morfismo de anillos $\varphi : A \to B$ tal que $\varphi(S) \subseteq B^\times$, existe un único morfismo $\hat{\varphi} : S^{-1}A \to B$ tal que

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & B \\ & S^{-1}A \arrow[ur, "\exists!\ \hat{\varphi}"'] & \end{tikzcd}$$

es un diagrama conmutativo (es decir, $\varphi = \hat{\varphi} \circ \iota$).
Indicación : Probar que necesariamente $\hat{\varphi}(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$ (unicidad) y que dicha expresión está bien definida (existencia).

Problema opcional (30 puntos)

El objetivo de este problema es definir y estudiar algunas propiedades del *anillo de enteros p–ádicos* $\mathbb{Z}_p$. Para ello comenzamos definiendo la noción de límite proyectivo asociado a un sistema proyectivo :

Sea $(I, \leq)$ un conjunto de índices ordenados. Un **sistema proyectivo** de conjuntos indexados por I es una familia $\{A_i\}_{i\in I}$ de conjuntos dotados de funciones $f_{ij} : A_i \to A_j$ para cada par de índices $i \geq j$ y de tal suerte que $f_{jk} \circ f_{ij} = f_{ik}$ y $f_{ii} = \mathrm{id}_{A_i}$. Definimos el **límite proyectivo** del sistema proyectivo como el subconjunto siguiente del producto $\prod_{i\in I} A_i$:

$$\varprojlim_{i\in I} A_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} A_i \;\middle|\; \forall i \geq j,\ x_j = f_{ij}(x_i) \right\}.$$

Si suponemos que los A_i son anillos (resp. grupos), entonces el producto $\prod_{i\in I} A_i$ es naturalmente un anillo (resp. grupo) y $\varprojlim_{i\in I} A_i$ es un subanillo (resp. subgrupo).

Sea p un número primo y consideremos $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}$ el sistema proyectivo de anillos indexado por $I = \mathbb{N}$, donde $f_{nm} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ es la proyección canónica si $n \geq m$. El límite proyectivo

$$\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

es llamado el **anillo de enteros p-ádicos**. Denotaremos por $\iota : \mathbb{Z} \to \mathbb{Z}_p$ el morfismo de anillos dado por la fórmula $\iota(a) = (a \mod p^n)_{n\in\mathbb{N}}$, por $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ la proyección sobre el factor $\mathbb{Z}/p^n\mathbb{Z}$ y definiremos la **valuación p-ádica** mediante $\nu(a) := \max\{n \in \mathbb{N} \mid \pi_n(a) = 0\}$ donde $a \in \mathbb{Z}_p \setminus \{0\}$.

1. Demostrar que $\ker(\pi_n) = \{a \in \mathbb{Z}_p \mid \nu(a) \geq n\} = \iota(p)^n\mathbb{Z}_p$.
2. Probar que $\iota : \mathbb{Z} \to \mathbb{Z}_p$ es inyectivo y que induce isomorfismos $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/\iota(p)^n\mathbb{Z}_p$ para todo $n \in \mathbb{N}$.
3. Probar que $\mathbb{Z}_p$ es un dominio y que $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid \nu(a) = 0\}$.
4. Demostrar que los ideales de $\mathbb{Z}_p$ son todos de la forma $\iota(p)^n\mathbb{Z}_p$ para cierto $n \in \mathbb{N}$. En particular, todo ideal de $\mathbb{Z}_p$ puede ser generado por un elemento y $\mathbb{Z}_p$ posee un único ideal maximal.

Comentario anexo : Se puede demostrar que $\mathbb{Z}_p$ es un anillo compacto y totalmente discontinuo (de hecho, son homeomorfos al conjunto de Cantor), donde la topología está generada por abiertos de la forma

$$a + p^n\mathbb{Z}_p = \{z \in \mathbb{Z}_p \mid \nu(z - a) \geq n\},$$

donde $a \in \mathbb{Z}_p$ y $n \in \mathbb{N}$, que es además la topología asociada a la distancia p-ádica $|a - b| := p^{-\nu(a-b)}$. Más aún, $\mathbb{Z}_p$ es la completación (en sentido de espacios métricos) de $\mathbb{Z}$ respecto a la distancia p-ádica, es decir, $\mathbb{Z}$ es denso en $\mathbb{Z}_p$ y los límites de sucesiones de Cauchy en $\mathbb{Z}$ convergen en $\mathbb{Z}_p$.

De manera más general, si A es un anillo y $I \subseteq A$ es un ideal, el límite proyectivo $\widehat{A}_I = \varprojlim_{n\in\mathbb{N}} A/I^n$ se llama la **completación I-ádica de A**, siendo muy utilizada en teoría de números y geometría algebraica.

Addendum : Intuición detrás de los límites proyectivos

El objetivo de esta sección es motivar y dar un poco de intuición sobre límites proyectivos y enteros p-ádicos.

Desde un punto de vista topológico, los límites proyectivos son una generalización de las intersecciones. A modo de ejemplo, considerar la familia $\{X_n\}_{n\in\mathbb{N}}$ junto con las funciones $f_{nm} : X_n \to X_m$ dadas por inclusiones

$$X_0 \supseteq X_1 \supseteq X_2 \supseteq \ldots$$

En este caso, se verifica que por definición $\varprojlim_{n\in\mathbb{N}} X_n = \bigcap_{n\in\mathbb{N}} X_n$. La idea clave en el ejemplo es que un punto en la intersección nos da un punto en x_n en cada X_n de tal suerte que x_{n+1} va a parar a x_n (que es el mismo punto). De manera más general, si tenemos funciones $f_{nm} : X_n \to X_m$ que no son necesariamente inclusiones

$$X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \ldots$$

Entonces un punto en $\varprojlim_{n\in\mathbb{N}} X_n$ es una colección de puntos $(x_n)_{n\in\mathbb{N}}$, uno por cada X_n, de tal suerte que x_{n+1} va a parar a x_n. Por ejemplo, si X_0 es un conjunto con 1 elemento (e.g. $\mathbb{Z}/2^0\mathbb{Z} = \{0\}$), X_1 es un conjunto con 2 elementos (e.g. $\mathbb{Z}/2\mathbb{Z}$), X_2 es un conjunto con 4 elementos (e.g. $\mathbb{Z}/4\mathbb{Z}$), etc. y cada función $X_{n+1} \to X_n$ es 2 :1 (i.e., cada punto tiene 2 preimagenes, entonces un punto en el límite proyectivo puede ser pensado como una elección de una de estas dos preimagenes (e.g. 0 o 1) para cada $n \in \mathbb{N}$.

Un segundo ejemplo motivador, más algebraico, es el siguiente :

Supongamos que queremos resolver la ecuación $x^2 = -1$ en $\mathbb{Z}$, y olvidemos por un instante que sabemos que esto es imposible. Notamos que si dicha solución existe en $\mathbb{Z}$ entonces también existe en $\mathbb{Z}/p^n\mathbb{Z}$ para todo primo p y todo $n \in \mathbb{N}$ (ver que en tal caso $x^2 \equiv -1 \mod p^n$). Para fijar ideas, supongamos que $p = 5$:

En $\mathbb{Z}/5\mathbb{Z}$ la ecuación $x^2 = -1$ tiene solución (de hecho, dos $x_1 = 2$ y $x_2 = 3$, que son la misma salvo por un signo). Tomemos por ejemplo $x \equiv 2 \mod 5$. Así, queremos hallar $x \in \mathbb{Z}$ tal que $x^2 = -1$ y $x \equiv 2 \mod 5$. Un tal x es de la forma $x = 5y + 2$ con $y \in \mathbb{Z}$. Al reemplazar en la ecuación obtenemos

$$(5y + 2)^2 = -1 \Leftrightarrow 25y^2 + 20y = -5 \Leftrightarrow 5y^2 + 4y = -1.$$

Luego, $20y \equiv -5 \mod 5^2$ y $4y \equiv -1 \mod 5$. Así, $y \equiv 1 \mod 5$ y al substituir obtenemos

$$x \equiv 5y + 2 \equiv 5 \cdot 1 + 2 = 7 \mod 5^2$$

Si continuamos de este modo y escribimos $x = 25z + 7$ con $z \in \mathbb{Z}$, al reemplazar en $x^2 = -1$ obtenemos que $z \equiv 2 \mod 5$ y luego $x \equiv 57 \mod 5^3$. Vale la pena destacar que $57 \equiv 7 \mod 5^2$ y que $7 \equiv 2 \mod 5$. Si continuamos con este proceso, obtenemos un elemento $x = (2, 7, 57, \ldots) \in \mathbb{Z}_5$ que resuelve la ecuación $x^2 = -1$.