Capítulo 12
Anillos conmutativos

En este capítulo vamos a ver algunas nociones básicas del **álgebra conmutativa**, la rama de álgebra que se dedica al estudio de anillos conmutativos.

12.1 Ideales primos y maximales

12.1.1. Definición. Sea R un anillo conmutativo.
Se dice que un ideal $\mathfrak{p} \subset R$ es **primo** si se cumplen las siguientes condiciones:

1) $\mathfrak{p}$ es un ideal propio: $\mathfrak{p} \neq R$,

2) para cualesquiera $x, y \in R$ si $xy \in \mathfrak{p}$, entonces $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$.

Se dice que un ideal $\mathfrak{m} \subset R$ es **maximal** si se cumplen las siguientes condiciones:

1) $\mathfrak{m}$ es un ideal propio: $\mathfrak{m} \neq R$,

2) $\mathfrak{m}$ es **maximal** respecto a la inclusión: para todo ideal $I \subseteq R$ tal que $\mathfrak{m} \subseteq I \subseteq R$ se cumple $I = \mathfrak{m}$ o $I = R$.

12.1.2. Comentario. Las letras $\mathfrak{p}$ y $\mathfrak{m}$ son p y m *góticas*. Esta notación es común en álgebra conmutativa y viene de la tradición alemana.

12.1.3. Notación. Sea R un anillo conmutativo. El conjunto de los ideales primos en R se llama el **espectro** de R y se denota por $\operatorname{Spec} R$:

$$\operatorname{Spec} R := \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ ideal primo}\}.$$

El conjunto de los ideales maximales se llama el **espectro maximal** y lo vamos a denotar por[*]

$$\operatorname{Specm} R := \{\mathfrak{m} \subset R \mid \mathfrak{m} \text{ ideal maximal}\}.$$

12.1.4. Ejemplo. El anillo nulo 0 no tiene ideales propios y entonces $\operatorname{Spec} 0 = \operatorname{Specm} 0 = \emptyset$. Más adelante vamos a ver que si $R \neq 0$, entonces $\operatorname{Spec} R \neq \emptyset$ y $\operatorname{Specm} R \neq \emptyset$. ▲

12.1.5. Ejemplo. En el anillo $\mathbb{Z}$ los ideales son de la forma $n\mathbb{Z}$ para $n = 0, 1, 2, 3, \ldots$ Tenemos $x \in n\mathbb{Z}$ si y solamente si $n \mid x$. Luego, $n\mathbb{Z}$ es un ideal primo si

1) $n \neq 1$,

[*] A diferencia de $\operatorname{Spec} R$, esta notación no es estándar. En la literatura también aparece Spec-max R y $\operatorname{Max} R$.

2) para cualesquiera $x, y \in \mathbb{Z}$ si $n \mid xy$, entonces $n \mid x$ o $n \mid y$.

Estas condiciones se cumplen para $n = 0$. Si $n \neq 0$, estas condiciones se cumplen si y solo si $n = p$ es un número primo. Entonces,

$$\operatorname{Spec} \mathbb{Z} = \{0\} \cup \{p\mathbb{Z} \mid p \text{ primo}\}.$$

Un ideal $n\mathbb{Z}$ es maximal si

1) $n \neq 1$,

2) para todo ideal $m\mathbb{Z} \subseteq \mathbb{Z}$ tal que $n\mathbb{Z} \subseteq m\mathbb{Z} \subseteq \mathbb{Z}$ se cumple $n\mathbb{Z} = m\mathbb{Z}$ o $m\mathbb{Z} = \mathbb{Z}$.

Recordamos que $n\mathbb{Z} \subseteq m\mathbb{Z}$ si y solo si $m \mid n$. Entonces, la condición 2) dice que si $m \mid n$, entonces $m = n$ o $m = 1$. Esto significa precisamente que $n = p$ es un número primo. Entonces,

$$\operatorname{Specm} \mathbb{Z} = \{p\mathbb{Z} \mid p \text{ primo}\}.$$

▲

En particular, este ejemplo demuestra que los ideales primos generalizan la noción de números primos. Tenemos la siguiente caracterización de ideales primos.

12.1.6. Proposición. *Sea R un anillo conmutativo. Las siguientes condiciones son equivalentes:*

1) $\mathfrak{p} \subset R$ es un ideal primo,

2) el anillo cociente $R/\mathfrak{p}$ es un dominio de integridad.

Demostración. Por la definición, $\mathfrak{p} \subset R$ es un ideal primo si y solo si 1) $\mathfrak{p} \neq R$ y 2) $xy \in \mathfrak{p}$ implica $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$. En términos del anillo cociente $R/\mathfrak{p}$, esto es equivalente a

1) $R/\mathfrak{p} \neq 0$,

2) si $(x + \mathfrak{p})(y + \mathfrak{p}) := xy + \mathfrak{p} = \overline{0}$[*], entonces $x + \mathfrak{p} = \overline{0}$ o $y + \mathfrak{p} = \overline{0}$.

En otras palabras, $R/\mathfrak{p}$ es un anillo conmutativo no nulo que no tiene divisores de cero. Es precisamente la definición de dominio de integridad. ■

Los ideales maximales tienen una caracterización parecida.

12.1.7. Proposición. *Sea R un anillo conmutativo. Las siguientes condiciones son equivalentes:*

1) $\mathfrak{m} \subset R$ es un ideal maximal,

2) el anillo cociente $R/\mathfrak{m}$ es un cuerpo.

Demostración. Recordemos que un anillo conmutativo S es un cuerpo si y solo si sus únicos ideales son 0 y S. Además, tenemos la siguiente descripción de los ideales en el anillo cociente $R/\mathfrak{m}$:

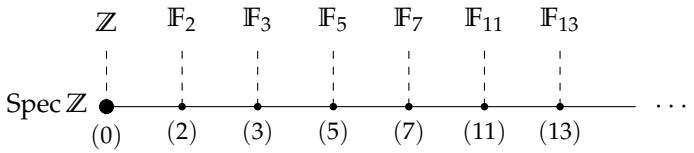
$$\{\text{ideales } \overline{I} \subseteq R/\mathfrak{m}\} \xrightarrow{\cong} \{\text{ideales } \mathfrak{m} \subseteq I \subseteq R\},$$
$$\overline{I} \mapsto \pi^{-1}(\overline{I}),$$

donde $\pi\colon R \to R/\mathfrak{m}$ denota la proyección canónica $x \mapsto x + \mathfrak{m}$.

En particular, los ideales $\overline{0}$ y $R/\mathfrak{m}$ en el cociente corresponden a los ideales $I = \mathfrak{m}$ e $I = R$ en R. El anillo $R/\mathfrak{m}$ no tiene otros ideales si y solamente si $\mathfrak{m} \subseteq I \subseteq R$ implica $I = \mathfrak{m}$ o $I = R$. Esto es precisamente la condición de la definición de ideales maximales. ■

[*]Aquí $\overline{0}$ denota la clase lateral $0 + \mathfrak{p}$ en el cociente $R/\mathfrak{p}$.

12.1.8. Ejemplo. El anillo cociente $\mathbb{Z}/n\mathbb{Z}$ es un dominio de integridad si y solo si $n = 0$ o $n = p$ es un número primo y es un cuerpo si y solo si $n = p$. Esto coincide con nuestra descripción de los ideales primos y maximales en $\mathbb{Z}$.



El espectro de $R = \mathbb{Z}$ con los anillos cociente correspondientes $R/\mathfrak{p}$

▲

12.1.9. Corolario. *Sea R un anillo conmutativo. Todo ideal maximal $\mathfrak{m} \subset R$ es un ideal primo.*

Demostración. Si $R/\mathfrak{m}$ es un cuerpo, en particular es un dominio de integridad. ■

12.1.10. Corolario. *Sea R un anillo conmutativo.*

1) *El ideal nulo 0 es primo en R si y solo si R es un dominio de integridad,*
2) *El ideal nulo 0 es maximal en R si y solo si R es un cuerpo.*

Demostración. $R/0 \cong R$. ■

12.1.11. Observación. *Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos.*

1) *Si $\mathfrak{p} \subset S$ es un ideal primo, entonces $f^{-1}(\mathfrak{p})$ es un ideal primo en R. En otras palabras, un homomorfismo de anillos $f\colon R \to S$ induce una aplicación entre los espectros*

$$\operatorname{Spec} S \to \operatorname{Spec} R, \quad \mathfrak{p} \mapsto f^{-1}(\mathfrak{p}).$$

2) *Si f es sobreyectivo y $\mathfrak{m} \subset S$ es un ideal maximal, entonces $f^{-1}(\mathfrak{m})$ es un ideal maximal en R.*

Demostración. Para un ideal $I \subseteq S$ podemos considerar el homomorfismo

$$R \xrightarrow{f} S \xrightarrow{\pi} S/I$$

donde $\pi\colon s \mapsto s + I$ es la proyección sobre el anillo cociente. Tenemos

$$\ker(\pi \circ f) = \{r \in R \mid f(r) \in I\} = f^{-1}(I).$$

Luego, el primer teorema de isomorfía implica que

$$R/f^{-1}(I) \cong \operatorname{im}(\pi \circ f) \subseteq S/I.$$

Ahora en la parte 1), si $I = \mathfrak{p}$ es un ideal primo, entonces $S/\mathfrak{p}$ es un dominio de integridad, y luego $\operatorname{im}(\pi \circ f) \cong R/f^{-1}(\mathfrak{p})$ es también un dominio de integridad, siendo un subanillo. Esto implica que $f^{-1}(\mathfrak{p})$ es un ideal primo en R.

En la parte 2), si f es un homomorfismo sobreyectivo, entonces $\operatorname{im}(\pi \circ f) = S/I$. Si $I = \mathfrak{m}$ es un ideal maximal, entonces $S/\mathfrak{m}$ es un cuerpo, y luego $S/\mathfrak{m} \cong R/f^{-1}(\mathfrak{m})$ es también un cuerpo y por lo tanto el ideal $f^{-1}(\mathfrak{m})$ es maximal en R. ■

12.1.12. Comentario. En general, para un homomorfismo de anillos $f\colon R \to S$, si $\mathfrak{m} \subset S$ es un ideal maximal, entonces $f^{-1}(\mathfrak{m})$ no tiene por qué ser un ideal maximal en R. Considere por ejemplo la inclusión $f\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$. El ideal nulo 0 es maximal en $\mathbb{Q}$, pero $0 = f^{-1}(0)$ no es un ideal maximal en $\mathbb{Z}$. En este sentido los ideales primos se comportan mejor que los maximales.

12.1.13. Proposición. *Sean R un anillo conmutativo, $I \subseteq R$ un ideal y $\pi\colon R \to R/I$ la proyección correspondiente sobre el anillo cociente. La biyección*

$$\begin{aligned} \{\text{ideales } \overline{J} \subseteq R/I\} &\leftrightarrow \{\text{ideales } I \subseteq J \subseteq R\}, \\ \overline{J} &\mapsto \pi^{-1}(\overline{J}), \\ J &\leftarrow\!\shortmid J/I \end{aligned}$$

se restringe a las biyecciones

$$\begin{aligned} \operatorname{Spec} R/I &\leftrightarrow \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}, \\ \operatorname{Specm} R/I &\leftrightarrow \{\mathfrak{m} \in \operatorname{Specm} R \mid I \subseteq \mathfrak{m}\}. \end{aligned}$$

Demostración. Para los ideales primos, ya vimos en 12.1.11 que si $\overline{\mathfrak{p}} \subset R/I$ es un ideal primo, entonces $\pi^{-1}(\overline{\mathfrak{p}}) \subset R$ es un ideal primo. Además, notamos que para un ideal primo $I \subseteq \mathfrak{p} \subset R$ el ideal $\mathfrak{p}/I \subset R/I$ es también primo. En efecto,

$$\mathfrak{p} \text{ es primo} \iff R/\mathfrak{p} \text{ es un dominio;} \quad \mathfrak{p}/I \text{ es primo} \iff (R/I)/(\mathfrak{p}/I) \text{ es un dominio,}$$

pero según el tercer teorema de isomorfía,

$$(R/I)/(\mathfrak{p}/I) \cong R/\mathfrak{p}.$$

De la misma manera, si $\overline{\mathfrak{m}} \subset R/I$ es un ideal maximal, entonces $\pi^{-1}(\overline{\mathfrak{m}})$ es un ideal maximal en R como notamos en 12.1.11 (usando que $\pi\colon R \to R/I$ es un homomorfismo sobreyectivo). Luego, para un ideal $I \subseteq \mathfrak{m} \subseteq R$ tenemos

$$\mathfrak{m} \text{ es maximal} \iff R/\mathfrak{m} \text{ es un cuerpo;} \quad \mathfrak{m}/I \text{ es maximal} \iff (R/I)/(\mathfrak{m}/I) \text{ es un cuerpo,}$$

y de nuevo, es suficiente aplicar el tercer teorema de isomorfía

$$(R/I)/(\mathfrak{m}/I) \cong R/\mathfrak{m}.$$

■

El siguiente resultado establece la existencia de ideales maximales.

12.1.14. Proposición. *Todo anillo conmutativo no nulo posee un ideal maximal.*

Para probarlo, necesitamos el lema de Zorn. El lector puede consultar el apéndice B para revisar el enunciado.

Demostración de 12.1.14. Sea R un anillo conmutativo no nulo y sea $\mathcal{P}$ el conjunto de los ideales propios $I \subsetneq R$. Esto es un conjunto parcialmente ordenado respecto a la inclusión $I \subseteq J$. Por la hipótesis, $R \neq 0$, así que $0 \in \mathcal{P}$ y por lo tanto $\mathcal{P} \neq \emptyset$. Un elemento maximal en $\mathcal{P}$ sería precisamente un ideal maximal en R. Para deducir la existencia de un elemento maximal, tenemos que probar que toda cadena en $\mathcal{P}$ es acotada.

Una cadena en $\mathcal{P}$ es una colección de ideales propios $\mathcal{S} = \{I_\alpha\}$ donde $I_\alpha \subseteq I_\beta$ o $I_\beta \subseteq I_\alpha$ para cualesquiera α, β. Se ve que la unión $I := \bigcup_\alpha I_\alpha$ es también un ideal en R[*]. Dado que $1 \notin I_\alpha$ para todo α, tenemos $1 \notin I$, así que I es también un ideal propio e $I \in \mathcal{P}$. Tenemos $I_\alpha \subseteq I$ para todo α. Este ideal I es una cota superior para $\mathcal{S}$. ■

[*]De hecho, $0 \in I_\alpha$ para todo α, así que $0 \in I$. Para $x, y \in I$ tenemos $x \in I_\alpha$ e $y \in I_\beta$ para algunos α, β. Sin pérdida de generalidad, $I_\alpha \subseteq I_\beta$, así que $x + y \in I_\beta$, dado que I_β es un ideal. Para todo $r \in R$ y $x \in I$ se tiene $x \in I_\alpha$ para algún α, y luego $rx \in I_\alpha \subseteq I$.

12.1.15. Corolario. *Sea R un anillo conmutativo y sea $I \subsetneq R$ un ideal propio. Entonces, R posee un ideal maximal $\mathfrak{m} \subset R$ tal que $I \subseteq \mathfrak{m}$.*

Demostración. Si $I \neq R$, entonces el anillo R/I no es nulo y según 12.1.14 posee un ideal maximal $\overline{\mathfrak{m}} \subset R/I$. Luego, como vimos en 12.1.13, este ideal corresponde a un ideal maximal $\mathfrak{m} = \pi^{-1}(\overline{\mathfrak{m}}) \subset R$ tal que $I \subseteq \mathfrak{m}$. ■

He aquí otro resultado sobre los ideales que puede ser demostrado mediante el lema de Zorn.

12.1.16. Proposición. *Sea R un anillo conmutativo. Entonces, su nilradical coincide con la intersección de los ideales primos en R:*

$$N(R) := \{r \in R \mid r^n = 0 \text{ para algún } n = 1, 2, 3, \ldots\} = \bigcap_{\mathfrak{p} \subset R \text{ primo}} \mathfrak{p}.$$

Demostración. Sea $r \in N(R)$ un nilpotente. Luego, $r^n = 0$ para algún n y por ende $r^n \in \mathfrak{p}$ para cualquier ideal primo $\mathfrak{p} \subset R$, lo que implica que $r \in \mathfrak{p}$. Entonces, r pertenece a cualquier ideal primo. Esto demuestra la inclusión

$$N(R) \subseteq \bigcap_{\mathfrak{p} \subset R \text{ primo}} \mathfrak{p}.$$

Para probar la otra inclusión, vamos a ver que si $r \notin N(R)$, entonces existe un ideal primo $\mathfrak{p} \subset R$ tal que $r \notin \mathfrak{p}$. Supongamos entonces que $r \in R$ satisface $r^n \neq 0$ para todo $n = 1, 2, 3, \ldots$ Sea $\mathcal{P}$ el conjunto de los ideales $I \subset R$ que no contienen ninguna potencia de r:

$$U \cap I = \emptyset, \quad \text{donde } U := \{r^n \mid n = 1, 2, 3, \ldots\}.$$

Esto es un conjunto parcialmente ordenado respecto a la inclusión. Notamos que $0 \in \mathcal{P}$, así que $\mathcal{P} \neq \emptyset$. Sea $\{I_\alpha\}$ una cadena en $\mathcal{P}$. Entonces, $I := \bigcup_\alpha I_\alpha$ es también un ideal, como ya notamos en la demostración en 12.1.14. Dado que $U \cap I_\alpha = \emptyset$ para todo α, tenemos $U \cap I = \emptyset$. Esto significa que $I \in \mathcal{P}$. El ideal I es una cota superior para la cadena $\{I_\alpha\}$. Ahora el lema de Zorn implica que existe un elemento maximal en $\mathcal{P}$; es decir, un ideal $\mathfrak{p} \subset R$ tal que[*]

1) $U \cap \mathfrak{p} = \emptyset$,

2) si $I \subset R$ es otro ideal que satisface $U \cap I = \emptyset$ y $\mathfrak{p} \subseteq I$, entonces $I = \mathfrak{p}$.

La notación "$\mathfrak{p}$" no es una coincidencia: ahora vamos a probar que esto es un ideal primo. Primero, $r \notin \mathfrak{p}$, así que esto es un ideal propio. Además, si $xy \in \mathfrak{p}$ para algunos $x, y \in R$, necesitamos probar que $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$. Supongamos que $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}$ para obtener una contradicción. En este caso

$$(x) + \mathfrak{p} \supsetneq \mathfrak{p}, \quad (y) + \mathfrak{p} \supsetneq \mathfrak{p},$$

lo que implica que

$$U \cap ((x) + \mathfrak{p}) \neq \emptyset, \quad U \cap ((y) + \mathfrak{p}) \neq \emptyset;$$

es decir, que existen algunas potencias

$$r^m = sx + p \in (x) + \mathfrak{p}, \quad r^n = ty + q \in (y) + \mathfrak{p}$$

para algunos $m, n \geq 1$, $s, t \in R$, $p, q \in \mathfrak{p}$. Tenemos

$$r^{m+n} = (sx + p)(st + q) = stxy + sxq + tyq + pq.$$

Dado que $\mathfrak{p}$ es un ideal y $xy \in \mathfrak{p}$, este elemento pertenece a $\mathfrak{p}$. Sin embargo, esto contradice la propiedad que $U \cap \mathfrak{p} = \emptyset$. Podemos concluir que $\mathfrak{p}$ es un ideal primo.

Entonces, existe un ideal primo $\mathfrak{p} \subset R$ tal que $U \cap \mathfrak{p} = \emptyset$, y en particular $r \notin \mathfrak{p}$. ■

[*] Cuidado: es un ideal maximal *respecto a la propiedad* $U \cap I = \emptyset$, pero no es necesariamente un ideal maximal en el anillo R.

12.1.17. Ejemplo. Los ideales en el anillo $\mathbb{Z}/12\mathbb{Z}$ corresponden a los ideales en $\mathbb{Z}$ que contienen a $12\mathbb{Z}$:

$$\mathbb{Z},\ 2\mathbb{Z},\ 3\mathbb{Z},\ 4\mathbb{Z},\ 6\mathbb{Z},\ 12\mathbb{Z}.$$

Los ideales primos en $\mathbb{Z}/12\mathbb{Z}$ corresponden a los ideales primos en la lista de arriba, así que son

$$2\mathbb{Z}/12\mathbb{Z} = \{[0],[2],[4],[6],[8],[10]\},$$
$$3\mathbb{Z}/12\mathbb{Z} = \{[0],[3],[6],[9]\}.$$

Su intersección es

$$2\mathbb{Z}/12\mathbb{Z} \cap 3\mathbb{Z}/12\mathbb{Z} = 6\mathbb{Z}/12\mathbb{Z} = \{[0],[6]\}$$

y se ve que $[0]$ y $[6]$ son precisamente los nilpotentes en $\mathbb{Z}/12\mathbb{Z}$. ▲

12.1.18. Ejemplo. Si R es un dominio de integridad, entonces (0) es un ideal primo y la intersección de todos los ideales primos $\mathfrak{p} \subset R$ es necesariamente nula. Esto coincide con el hecho de que un dominio de integridad no pueda tener nilpotentes. ▲

12.1.19. Corolario. *Sea R un anillo conmutativo y sea $I \subseteq R$ un ideal. Entonces, el radical de I coincide con la intersección de todos los ideales primos que contienen a I:*

$$\sqrt{I} := \{r \in R \mid r^n \in I \text{ para algún } n = 1,2,3,\ldots\} = \bigcap_{\substack{\mathfrak{p} \subset R \text{ primo} \\ I \subseteq \mathfrak{p}}} \mathfrak{p}.$$

Demostración. Si $r^n \in I$ para algún n e $I \subseteq \mathfrak{p}$ para un ideal primo $\mathfrak{p} \subset R$, entonces $r \in \mathfrak{p}$. Esto demuestra que $\sqrt{I}$ pertenece a la intersección. Viceversa, supongamos que $r \in \mathfrak{p}$ para todo ideal primo $\mathfrak{p}$ tal que $I \subseteq \mathfrak{p}$. Recordemos que los ideales primos $I \subseteq \mathfrak{p} \subset R$ están en biyección con los ideales primos en el anillo cociente R/I. Esta biyección implica que $r + I \in \overline{\mathfrak{p}}$ para todo ideal primo $\overline{\mathfrak{p}} \subset R/I$. Entonces,

$$r + I \in \bigcap_{\overline{\mathfrak{p}} \subset R/I \text{ primo}} \overline{\mathfrak{p}} = N(R/I).$$

Pero para $r + I$ ser nilpotente en R/I significa precisamente que $r \in \sqrt{I}$. ■

He aquí otra aplicación más del lema de Zorn.

12.1.20. Teorema (I.S. Cohen). *Sea R un anillo conmutativo. Supongamos que todo ideal primo en R es finitamente generado. Entonces, todos los ideales en R son finitamente generados.*

Demostración. Vamos a ver que si en R hay un ideal que no es finitamente generado, entonces en R hay un ideal primo que no es finitamente generado.

Sea $\mathcal{P}$ el conjunto de los ideales que no son finitamente generados, parcialmente ordenado respecto a la inclusión. Por nuestra hipótesis, $\mathcal{P} \neq \emptyset$. Para una cadena de tales ideales $\{I_\alpha\}$ la unión $I := \bigcup_\alpha I_\alpha$ es también un ideal y no es finitamente generado. De hecho, si $I = (x_1, \ldots, x_n)$ para $x_1, \ldots, x_n \in R$, entonces $x_1, \ldots, x_n \in I_\alpha$ para algún α (usando que $\{I_\alpha\}$ es una cadena), lo que implicaría que el ideal $I_\alpha = I$ es finitamente generado.

Ahora según el lema de Zorn, existe un ideal $\mathfrak{p} \subset R$ que es maximal respecto a la propiedad de no ser finitamente generado:

1) $\mathfrak{p}$ no es finitamente generado,

2) si $\mathfrak{p} \subseteq I \subset R$ para otro ideal I que no es finitamente generado, entonces $I = \mathfrak{p}$.

Vamos a probar que $\mathfrak{p}$ es un ideal primo. Primero, es un ideal propio, puesto que $R = (1)$ es finitamente generado. Supongamos que $xy \in \mathfrak{p}$ para algunos $x, y \in R$, pero $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}$. Luego,

$$(x) + \mathfrak{p} \supsetneq \mathfrak{p},$$

así que $(x) + \mathfrak{p}$ es un ideal finitamente generado:

$$(x) + \mathfrak{p} = (y_1, \ldots, y_n)$$

para algunos $y_1, \ldots, y_n \in (x) + \mathfrak{p}$. En particular, tenemos

$$y_i = r_i\, x + p_i$$

para algunos $r_i \in R$, $p_i \in \mathfrak{p}$. Notamos que

$$(x) + \mathfrak{p} = (x, p_1, \ldots, p_n).$$

De hecho, dado que $y_i \in (x, p_1, \ldots, p_n)$ para todo i, se cumple $(y_1, \ldots, y_n) \subseteq (x, p_1, \ldots, p_n)$. Viceversa, $x \in (x) + \mathfrak{p}$ y $p_i \in \mathfrak{p} \subsetneq (x) + \mathfrak{p}$ para todo $i = 1, \ldots, n$, así que $(x, p_1, \ldots, p_n) \subseteq (x) + \mathfrak{p} = (y_1, \ldots, y_n)$.

Para un elemento arbitrario $p \in \mathfrak{p}$ tenemos en particular $p \in (x) + \mathfrak{p} = (x, p_1, \ldots, p_n)$, y por ende

$$p = r\, x + r_1\, p_1 + \cdots + r_n\, p_n \tag{12.1}$$

para algunos $r, r_1, \ldots, r_n \in R$. Luego,

$$r\, x = p - (r_1\, p_1 + \cdots + r_n\, p_n),$$

así que

$$r \in \{s \in R \mid sx \in \mathfrak{p}\}.$$

Notamos que el último conjunto es un ideal y denotémoslo por I. Tenemos $\mathfrak{p} \subsetneq I$, dado que $\mathfrak{p}$ es un ideal e $y \in I$, pero $y \notin \mathfrak{p}$ por nuestra hipótesis. Entonces, por la maximalidad de $\mathfrak{p}$, el ideal I debe ser finitamente generado:

$$I = (z_1, \ldots, z_k)$$

para algunos $z_1, \ldots, z_k \in I$. Esto significa que todo elemento de $\mathfrak{p}$ puede ser escrito como

$$p = (a_1\, z_1 + \cdots + a_k\, z_k)\, x + (r_1\, p_1 + \cdots + r_n\, p_n),$$

y por ende

$$\mathfrak{p} \subseteq (z_1 x, \ldots, z_k x, p_1, \ldots, p_n).$$

Pero por la definición de I, aquí $z_i x \in \mathfrak{p}$ para todo $i = 1, \ldots, k$ puesto que $z_i \in I$, así que

$$\mathfrak{p} = (z_1 x, \ldots, z_k x, p_1, \ldots, p_n).$$

Esto contradice el hecho de que $\mathfrak{p}$ no sea finitamente generado. Entonces, $\mathfrak{p}$ debe ser un ideal primo. ■

La prueba de arriba de que $\mathfrak{p}$ sea primo usa cierto truco, pero el argumento general es una aplicación típica del lema de Zorn.

12.2 Localización

En esta sección vamos a estudiar una construcción importante para anillos conmutativos llamada **localización**. La idea es bien sencilla y puede ser motivada por la construcción de los números racionales $\mathbb{Q}$ a partir de los números enteros $\mathbb{Z}$. Los elementos de $\mathbb{Q}$ son fracciones $\frac{a}{b}$, donde $a, b \in \mathbb{Z}$ y $b \neq 0$. Tenemos

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' - a'b = 0. \tag{12.2}$$

La suma y producto de fracciones se definen mediante las fórmulas

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{12.3}$$

Notamos que si $\frac{a}{b} = \frac{a'}{b'}$, entonces

$$\frac{ad + cb}{bd} = \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c}{d} = \frac{a'd + cb'}{b'd}.$$

En efecto,

$$(ad + cb)\, b'd - (a'd + cb')\, bd = ab'd^2 + \cancel{cbb'd} - a'bd^2 - \cancel{cb'bd} = d^2\, (\underbrace{ab' - a'b}_{=0}) = 0.$$

De la misma manera, si $\frac{a}{b} = \frac{a'}{b'}$, entonces

$$\frac{ac}{bd} = \frac{a'c}{b'd}.$$

En efecto,

$$ac\, b'd - a'c\, bd = dc\, (\underbrace{ab' - a'b}_{=0}) = 0.$$

Esto verifica que las operaciones (12.3) están bien definidas: son compatibles con (12.2). Se ve que $\mathbb{Q}$ es un anillo conmutativo respecto a (12.3), y de hecho es un cuerpo.

Otro ejemplo relevante es el anillo

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \nmid b \right\}$$

para un primo fijo p. Este anillo consiste en las fracciones donde p no divide al denominador. Se ve que $\mathbb{Z}_{(p)}$ es un subanillo de $\mathbb{Q}$. Los elementos invertibles en $\mathbb{Z}_{(p)}$ son las fracciones $\frac{a}{b}$ donde $p \nmid a$ y $p \nmid b$. En este caso $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Nuestro objetivo es generalizar el cálculo de fracciones a cualquier anillo conmutativo R. Supongamos que queremos invertir ciertos elementos $u \in R$. En este caso hay que "extender" R a las fracciones $\frac{r}{u}$ donde u aparece en el denominador, así que $\left(\frac{u}{1}\right)^{-1} = \frac{1}{u}$. Antes de dar la construcción general, recordamos que si u y v son invertibles, entonces $u^{-1} v^{-1}$ es el inverso de uv, así que todo producto de elementos invertibles es también invertible.

12.2.1. Construcción. Sea R un anillo conmutativo y sea $U \subseteq R$ un **conjunto multiplicativo**; es decir, que satisface

a) $1 \in U$,

b) si $u, v \in U$, entonces $uv \in U$.

1) Consideremos la siguiente relación sobre el conjunto $R \times U$, motivada[*] por (12.2):

$$(r,u) \sim (r',u') \iff v\,(ru' - r'u) = 0 \text{ para algún } v \in U.$$

Esto es una relación de equivalencia: de hecho, tenemos $(r,u) \sim (r,u)$, puesto que

$$1 \cdot (ru - ru) = 0,$$

así que la relación es reflexiva. Si $(r,u) \sim (r',u')$, entonces $v\,(ru' - r'u) = 0$ para algún $v \in U$, y multiplicando esta identidad por -1, se obtiene $v\,(r'u - ru') = 0$, lo que significa que la relación es simétrica. En fin, supongamos que $(r,u) \sim (r',u')$ y $(r',u') \sim (r'',u'')$; es decir, que existen algunos $v, v' \in U$ tales que

$$v\,(ru' - r'u) = 0, \quad v'\,(r'u'' - r''u') = 0.$$

Ahora

$$0 = v'u'' \cdot v\,(ru' - r'u) + uv \cdot v'\,(r'u'' - r''u') = ru'u''vv' - \cancel{r'uu''vv'} + \cancel{r'uu''vv'} - r''uu'vv' \\ = vv'u'\,(ru'' - r''u),$$

donde $vv'u' \in U$, puesto que $v, v', u' \in U$, y luego $(r,u) \sim (r'',u'')$. Esto demuestra que la relación es transitiva.

2) Denotemos por $\frac{r}{u}$ la clase de equivalencia de (r,u) y sea

$$R[U^{-1}] := R \times U/\sim = \left\{ \frac{r}{u} \;\middle|\; r \in R,\ u \in U \right\}$$

el conjunto de las clases de equivalencia. Definamos el producto y la suma en $R[U^{-1}]$ mediante

$$\frac{r_1}{u_1} + \frac{r_2}{u_2} := \frac{r_1u_2 + r_2u_1}{u_1u_2}, \quad \frac{r_1}{u_1} \cdot \frac{r_2}{u_2} := \frac{r_1r_2}{u_1u_2}.$$

Comprobemos que estas operaciones están bien definidas sobre las clases de equivalencia. Supongamos que

$$\frac{r_1}{u_1} = \frac{r_1'}{u_1'} \iff v\,(r_1u_1' - r_1'u_1) = 0 \text{ para algún } v \in U.$$

Luego,

$$v\,((r_1u_2 + r_2u_1)\,u_1'u_2 - (r_1'u_2 + r_2u_1')\,u_1\,u_2) \\ = r_1u_1'u_2^2v + \cancel{r_2u_1u_1'u_2v} - r_1'u_1u_2^2v - \cancel{r_2u_1u_1'u_2v} = u_2^2\,v\,(r_1u_1' - r_1'u_1) = 0,$$

lo que significa que

$$\frac{r_1u_2 + r_2u_1}{u_1u_2} = \frac{r_1'u_2 + r_2u_1'}{u_1'u_2}.$$

De la misma manera,

$$v\,(r_1r_2u_1'u_2 - r_1'r_2u_1u_2) = r_2\,u_1\,\underbrace{v\,(r_1u_1' - r_1'u_1)}_{=0} = 0,$$

así que

$$\frac{r_1r_2}{u_1u_2} = \frac{r_1'r_2}{u_1'u_2}.$$

[*] En (12.2) no aparece el múltiplo v, pero este será necesario para probar la transitividad de la relación. Sin embargo, si R es un dominio de integridad y $0 \notin U$, este múltiplo siempre puede ser cancelado.

3) Notamos que $R[U^{-1}]$ es un anillo conmutativo respecto a estas dos operaciones, puesto que R es un anillo conmutativo (el lector que está convencido de que los números racionales forman un anillo conmutativo puede saltar estos cálculos).

- La adición es asociativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2}, \frac{r_3}{u_3} \in R[U^{-1}]$ tenemos

$$\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) + \frac{r_3}{u_3} = \frac{r_1u_2 + r_2u_1}{u_1u_2} + \frac{r_3}{u_3} = \frac{(r_1u_2 + r_2u_1)\,u_3 + r_3u_1u_2}{u_1u_2u_3} = \frac{r_1u_2u_3 + r_2u_1u_3 + r_3u_1u_2}{u_1u_2u_3},$$

y

$$\frac{r_1}{u_1} + \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right) = \frac{r_1}{u_1} + \frac{r_2u_3 + r_3u_2}{u_2u_3} = \frac{r_1u_2u_3 + (r_2u_3 + r_3u_2)\,u_1}{u_1u_2u_3} = \frac{r_1u_2u_3 + r_2u_3u_1 + r_3u_2u_1}{u_1u_2u_3},$$

así que

$$\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) + \frac{r_3}{u_3} = \frac{r_1}{u_1} + \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right).$$

- La multiplicación es asociativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2}, \frac{r_3}{u_3} \in R[U^{-1}]$ tenemos

$$\left(\frac{r_1}{u_1} \cdot \frac{r_2}{u_2}\right) \cdot \frac{r_3}{u_3} = \frac{r_1}{u_1} \cdot \left(\frac{r_2}{u_2} \cdot \frac{r_3}{u_3}\right) = \frac{r_1r_2r_3}{u_1u_2u_3}.$$

- La adición es conmutativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2} \in R[U^{-1}]$ se cumple

$$\frac{r_1}{u_1} + \frac{r_2}{u_2} = \frac{r_2}{u_2} + \frac{r_1}{u_1} = \frac{r_1u_2 + r_2u_1}{u_1u_2}.$$

- La multiplicación es conmutativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2} \in R[U^{-1}]$ se cumple

$$\frac{r_1}{u_1} \cdot \frac{r_2}{u_2} = \frac{r_2}{u_2} \cdot \frac{r_1}{u_1} = \frac{r_1r_2}{u_1u_2}.$$

- La fracción $\frac{0}{1}$ es el elemento nulo: para todo $\frac{r}{u} \in R[U^{-1}]$ se cumple

$$\frac{0}{1} + \frac{r}{u} = \frac{0 \cdot u + r \cdot 1}{u} = \frac{r}{u}.$$

  Notamos que

$$\frac{r}{u} = \frac{0}{1} \iff v\,r = 0 \text{ para algún } v \in U.$$

  En particular, $\frac{0}{u} = \frac{0}{1}$ para cualquier $u \in U$.

- La fracción $\frac{1}{1}$ es la identidad: para todo $\frac{r}{u} \in R[U^{-1}]$ se cumple

$$\frac{1}{1} \cdot \frac{r}{u} = \frac{1 \cdot r}{1 \cdot u} = \frac{r}{u}.$$

  Notamos que

$$\frac{r}{u} = \frac{1}{1} \iff v\,(r - u) = 0 \text{ para algún } v \in U.$$

En particular, $\frac{u}{u} = \frac{1}{1}$ para cualquier $u \in U$, y funciona la cancelación habitual en las fracciones:

$$\frac{ru'}{uu'} = \frac{r}{u}$$

para cualesquiera $r \in R, u, u' \in U$.

- Para todo $\frac{r}{u} \in R[U^{-1}]$ existe el elemento opuesto que es la fracción $\frac{-r}{u}$:

$$\frac{r}{u} + \frac{-r}{u} = \frac{ru - ru}{ru} = \frac{0}{ru} = \frac{0}{1}.$$

- la multiplicación es distributiva respecto a la adición: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2}, \frac{r_3}{u_3} \in R[U^{-1}]$ se cumple

$$\frac{r_1}{u_1} \cdot \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right) = \frac{r_1}{u_1} \cdot \frac{r_2}{u_2} + \frac{r_1}{u_1} \cdot \frac{r_3}{u_3}.$$

En efecto,

$$\frac{r_1}{u_1} \cdot \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right) = \frac{r_1}{u_1} \cdot \left(\frac{r_2u_3 + r_3u_2}{u_2u_3}\right) = \frac{r_1r_2u_3 + r_1r_3u_2}{u_1u_2u_3}$$

y

$$\frac{r_1r_2}{u_1u_2} + \frac{r_1r_3}{u_1u_3} = \frac{r_1r_2u_1u_3 + r_1r_3u_1u_2}{u_1^2u_2u_3} = \frac{u_1\left(r_1r_2u_3 + r_1r_3u_2\right)}{u_1\left(u_1u_2u_3\right)} = \frac{r_1r_2u_3 + r_1r_3u_2}{u_1u_2u_3}.$$

12.2.2. Definición. Para un anillo conmutativo R y un conjunto multiplicativo $U \subseteq R$, el anillo conmutativo $R[U^{-1}]$ se llama la **localización** de R en U.

Aunque la construcción de arriba no excluye las fracciones $\frac{r}{0}$, la presencia de 0 en los denoninadores implica que $R[U^{-1}] = 0$.

12.2.3. Observación. *$R[U^{-1}] = 0$ es el anillo trivial si y solo si $0 \in U$.*

Demostración. La localización es trivial si y solo si $\frac{1}{1} = \frac{0}{1}$; es decir, si $v\,(1 \cdot 1 - 0 \cdot 1) = 0$ para algún $v \in U$. Pero esto significa que $v = 0$. ■

12.2.4. Observación. *Supongamos que R es un dominio de integridad. Entonces, hay dos posibilidades:*

1) *$0 \in U$, y entonces $R[U^{-1}] = 0$;*
2) *$0 \notin U$, y entonces $R[U^{-1}]$ es también un dominio de integridad.*

Demostración. Supongamos que para $\frac{r_1}{u_1}, \frac{r_2}{u_2} \in R[U^{-1}]$ se tiene

$$\frac{r_1}{u_1}\,\frac{r_2}{u_2} = \frac{r_1r_2}{u_1u_2} = \frac{0}{1}.$$

Esto quiere decir que $v\,r_1\,r_2 = 0$ para algún $v \in U$. Si $0 \notin U$, entonces esto implica $r_1 = 0$ o $r_2 = 0$. ■

Es natural asociar a los elementos $r \in R$ las fracciones $\frac{r}{1} \in R[U^{-1}]$, pero en general la aplicación $r \mapsto \frac{r}{1}$ no es inyectiva.

12.2.5. Observación.

1) *La aplicación*

$$\phi\colon R \to R[U^{-1}], \quad r \mapsto \frac{r}{1}$$

es un homomorfismo de anillos.

2) *Tenemos*
$$\ker\phi = \left\{ r \in R \;\middle|\; \frac{r}{1} = \frac{0}{1} \right\} = \{ r \in R \mid v\,r = 0 \text{ para algún } v \in U \}.$$

3) *Si U no contiene divisores de cero, entonces ϕ es un monomorfismo y R es isomorfo al subanillo*
$$\operatorname{im}\phi = \left\{ \frac{r}{1} \;\middle|\; r \in R \right\} \subset R[U^{-1}].$$

4) *En particular, si R es un dominio de integridad y $0 \notin U$, entonces ϕ es un monomorfismo y R es isomorfo al subanillo* $\operatorname{im}\phi \subset R[U^{-1}]$.

Demostración. 1) y 2) está claro de las definiciones de arriba. La parte 3) sigue de 2). En fin, 4) es un caso especial de 3). ■

12.2.6. Ejemplo. Sea R un anillo conmutativo.

1) Para un elemento $x \in R$ consideremos
$$U := \{1, x, x^2.x^3, \ldots\}.$$
Este es un conjunto multiplicativo. La localización correspondiente se denota por
$$R[U^{-1}] =: R\left[\frac{1}{x}\right] \text{ o } R[x^{-1}] = \left\{ \frac{r}{x^n} \;\middle|\; r \in R,\ n = 0, 1, 2, 3, \ldots \right\}.$$
Por ejemplo, tenemos
$$\mathbb{Z}\left[\frac{1}{n}\right] := \left\{ \frac{a}{n^k} \mid a \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots \right\}.$$
Esta es la localización de $\mathbb{Z}$ en el conjunto de las potencias de n.
El resultado de 12.2.3 nos dice que $R[x^{-1}] = 0$ si y solo si x es un nilpotente.

2) Para un ideal $I \subseteq R$ consideremos $U := R \setminus I$. Entonces, U es un conjunto multiplicativo si $1 \in U$ y $u, v \in U$ implica $uv \in U$. Esto es equivalente a $I \neq R$ y que si $xy \in I$ para algunos $x, y \in R$, entonces $x \in I$ o $y \in i$; es decir, que $I = \mathfrak{p}$ es un ideal primo. En este caso la localización se denota por
$$R[(R \setminus \mathfrak{p})^{-1}] =: R_{\mathfrak{p}} = \left\{ \frac{r}{u} \;\middle|\; r, u \in R,\ u \notin \mathfrak{p} \right\}.$$
Por ejemplo, $\mathbb{Z}_{(p)}$ es la localización de $\mathbb{Z}$ en $U := \mathbb{Z} \setminus (p)$.
En general, si tomamos un subconjunto multiplicativo $U \subset R$, entonces $R \setminus U$ no tiene por qué ser un ideal (las condiciones sobre U se tratan de la multiplicación y no dicen nada sobre la adición), pero el ejercicio 12.9 nos dice que si $0 \notin U$, entonces existe un ideal primo $\mathfrak{p} \subset R$ tal que $U \cap \mathfrak{p} = \emptyset$.

3) Si R es un dominio de integridad, entonces el conjunto
$$U := R \setminus \{0\}$$
es multiplicativo. En este caso todo elemento no nulo en $R[U^{-1}]$ es invertible y este cuerpo se denota por
$$R[U^{-1}] =: K(R) = \left\{ \frac{r}{s} \;\middle|\; r, s \in R, s \neq 0 \right\}$$
y se llama el **cuerpo de fracciones** de R. La aplicación
$$\phi\colon R \to K(R), \quad r \mapsto \frac{1}{r}$$

es un monomorfismo. Notamos que R es un dominio de integridad si y solamente si el ideal nulo (0) es primo, y en este caso $K(R) = R_{\mathfrak{p}}$ donde $\mathfrak{p} = 0$, así que se trata de un caso muy particular de 2),

Por ejemplo, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$.

▲

12.2.7. Proposición. *Sea R un dominio de integridad. Para todo ideal maximal $\mathfrak{m} \subset R$ identifiquemos R con el subanillo*

$$\left\{ \frac{r}{1} \;\middle|\; r \in R \right\}$$

de la localización

$$R_{\mathfrak{m}} := R[(R \setminus \mathfrak{m})^{-1}] = \left\{ \frac{r}{u} \;\middle|\; r, u \in R,\ u \notin \mathfrak{m} \right\}$$

y $R_{\mathfrak{m}}$ con el subanillo del cuerpo de fracciones

$$K(R) = \left\{ \frac{r}{s} \;\middle|\; r, s \in R,\ s \neq 0 \right\}.$$

Entonces,

$$\bigcap_{\substack{\mathfrak{m} \subset R \\ \textit{maximal}}} R_{\mathfrak{m}} = R.$$

Demostración. Dado que $R \subseteq R_{\mathfrak{m}}$ para todo $\mathfrak{m} \subset R$, el anillo R está incluido en la intersección. En la otra dirección, sea $x \in K(R)$ un elemento tal que $x \notin R$. Consideremos el ideal

$$I := \{ r \in R \mid rx \in R \}.$$

Tenemos $1 \notin I$, así que I es un ideal propio. Luego, existe un ideal maximal $\mathfrak{m} \subset R$ tal que $I \subseteq \mathfrak{m}$. Supongamos que $x \in R_{\mathfrak{m}}$. Luego, $x = \frac{r}{u}$ para algunos $r, u \in R$, $u \notin \mathfrak{m}$. Tenemos entonces $u\,x = \frac{u}{1}\frac{r}{u} = \frac{r}{1} \in R$ y $u \in I$. Pero esto contradice nuestra elección de $\mathfrak{m}$. Entonces, $x \notin R_{\mathfrak{m}}$. ■

12.2.8. Ejemplo. Tenemos

$$\bigcap_{p \text{ primo}} \mathbb{Z}_{(p)} = \bigcap_{p \text{ primo}} \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \right\}$$
$$= \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \text{ para ningún primo } p \right\} = \mathbb{Z}.$$

▲

Ahora vamos a ver otro ejemplo más de cuerpos de fracciones.

12.2.9. Ejemplo. Para un cuerpo k el anillo de polinomios $k[X]$ tiene como su cuerpo de fracciones el cuerpo de las **funciones racionales**

$$k(X) := \left\{ \frac{f}{g} \;\middle|\; f, g \in k[X],\ g \neq 0 \right\}$$

Recordemos que en el anillo de las series formales $k[\![X]\!]$ una serie $g = \sum_{i \geq 0} a_i\, X^i$ es invertible si y solamente si $a_0 \neq 0$. Sin embargo, para una serie no nula $\sum_{i \geq 0} a_i\, X^i$ donde $a_n \neq 0$ es el primer coeficiente no nulo se puede escribir

$$\sum_{i \geq 0} a_i\, X^i = X^n \sum_{i \geq n} a_i\, X^{i-n} =: X^n\, h,$$

donde h es invertible: existe $h^{-1} \in k[\![X]\!]$ tal que $h\,h^{-1} = 1$. Luego, en el cuerpo de fracciones de $k[\![X]\!]$ para $f, g \in k[\![X]\!]$, $g \neq 0$ se tiene

$$\frac{f}{g} = \frac{f}{X^n\,h} = \frac{f\,h^{-1}}{X^n\,h\,h^{-1}} = \frac{f\,h^{-1}}{X^n}.$$

Esto quiere decir que en el cuerpo de fracciones de $k[\![X]\!]$ todo elemento puede ser representado como una fracción $\frac{f}{X^n}$ donde $f \in k[\![X]\!]$ y $n = 0, 1, 2, 3, \ldots$ Se ve que el cuerpo formado por estas fracciones es isomorfo al cuerpo

$$k((X)) := \left\{ \sum_{i \geq -n} a_i\,X^i \;\middle|\; a_i \in k,\ n = 0, 1, 2, 3, \ldots \right\}$$

(con las operaciones de suma y producto definidas de la manera habitual) que se llama el **cuerpo de las series de Laurent**. Tenemos inclusiones naturales de subanillos

$$\begin{array}{ccc} k[\![X]\!] & \hookrightarrow & k((X)) \\ \uparrow & & \uparrow \\ k[X] & \hookrightarrow & k(X) \end{array}$$

Las series de Laurent $\mathbb{C}((X))$ tienen mucha importancia en análisis complejo. ▲

La localización $R[U^{-1}]$ es la "extensión mínima" de R donde los elementos de U se vuelven invertibles.

12.2.10. Proposición (Propiedad universal de la localización). *Sea R un anillo conmutativo y $U \subseteq R$ un subconjunto multiplicativo. Consideremos el homomorfismo canónico*

$$\phi\colon R \to R[U^{-1}], \quad r \mapsto \frac{r}{1}.$$

Entonces

1) *para todo $u \in U$ el elemento $\phi(u) = \frac{u}{1}$ es invertible en $R[U^{-1}]$;*
2) *si S es otro anillo junto con un homomorfismo $f\colon R \to S$ tal que $f(u)$ es invertible en S para todo $u \in U$, entonces f se factoriza de modo único por ϕ:*

$$\begin{array}{ccc} R & \xrightarrow{\ f\ } & S \\ {\scriptstyle\phi}\downarrow & \nearrow_{\exists!\widetilde{f}} & \\ R[U^{-1}] & & \end{array}$$

Demostración. La parte 1) está clara: se tiene $\left(\frac{u}{1}\right)^{-1} = \frac{1}{u}$.

En la parte 2), sea $\widetilde{f}$ un homomorfismo que hace conmutar el diagrama; entonces

$$\widetilde{f}\left(\frac{r}{1}\right) = f(r)$$

para todo $r \in R$. Además, si $f(u)$ es invertible para todo $u \in U$, entonces

$$\widetilde{f}\left(\frac{1}{u}\right) = \widetilde{f}\left(\left(\frac{u}{1}\right)^{-1}\right) = \widetilde{f}\left(\frac{u}{1}\right)^{-1} = f(u)^{-1},$$

y para todo $\frac{r}{u} \in R[U^{-1}]$ se tiene necesariamente

$$\widetilde{f}\left(\frac{r}{u}\right) = \widetilde{f}\left(\frac{r}{1} \cdot \frac{1}{u}\right) = \widetilde{f}\left(\frac{r}{1}\right)\,\widetilde{f}\left(\frac{1}{u}\right) = f(r)\,f(u)^{-1}.$$

Esto demuestra la unicidad de $\widetilde{f}$.

Para la existencia, notamos que dado un homomorfismo $f\colon R \to S$ tal que $f(u)$ es invertible para todo $u \in U$, la aplicación

$$\widetilde{f}\colon R[U^{-1}] \to S, \quad \frac{r}{u} \mapsto f(r)\, f(u)^{-1}$$

es un homomorfismo de anillos que hace conmutar el diagrama. Evidentemente,

$$\widetilde{f}\left(\frac{1}{1}\right) = f(1)\, f(1)^{-1} = 1.$$

Para las sumas, se cumple

$$\widetilde{f}\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) = \widetilde{f}\left(\frac{r_1u_2 + r_2u_1}{u_1u_2}\right) = f(r_1u_2 + r_2u_1)\, f(u_1u_2)^{-1}$$
$$= f(r_1)\, f(u_1)^{-1} + f(r_2)\, f(u_2)^{-1} = \widetilde{f}\left(\frac{r_1}{u_1}\right) + \widetilde{f}\left(\frac{r_2}{u_2}\right),$$

y para los productos,

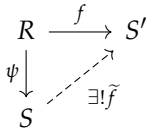
$$\widetilde{f}\left(\frac{r_1}{u_1} \cdot \frac{r_2}{u_2}\right) = \widetilde{f}\left(\frac{r_1r_2}{u_1u_2}\right) = f(r_1r_2)\, f(u_1u_2)^{-1} = f(r_1)\, f(u_1)^{-1}\, f(r_2)\, f(u_2)^{-1}$$
$$= \widetilde{f}\left(\frac{r_1}{u_1}\right) \cdot \widetilde{f}\left(\frac{r_2}{u_2}\right).$$

■

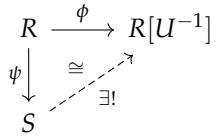
Como siempre, la propiedad universal caracteriza a $R[U^{-1}]$ de modo único salvo isomorfismo.

12.2.11. Proposición. *Supongamos que $\psi\colon R \to S$ es un homomorfismo de anillos que satisface la misma propiedad universal que el homomorfismo canónico de localización $\phi\colon R \to R[U^{-1}]$:*

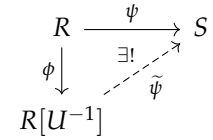
1) *para todo $u \in U$ el elemento $\psi(u)$ es invertible en S;*
2) *si S' es otro anillo junto con un homomorfismo $f\colon R \to S'$ tal que $f(u)$ es invertible en S' para todo $u \in U$, entonces f se factoriza de modo único por ψ:*



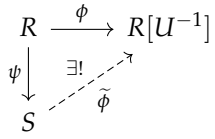
Entonces, existe un isomorfismo único $S \to R[U^{-1}]$ que hace conmutar el diagrama



Demostración. Podemos aplicar la propiedad universal de ϕ a ψ



y viceversa, aplicar la propiedad universal de ψ a ϕ:

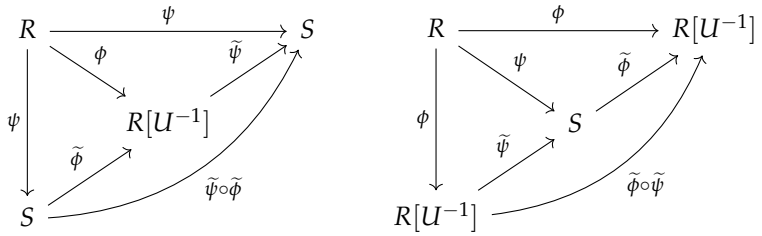


De esta manera se obtienen homomorfismos de anillos

$$\widetilde{\phi}\colon R[U^{-1}] \to S, \quad \widetilde{\phi}\colon S \to R[U^{-1}], \quad \psi = \widetilde{\psi} \circ \phi, \quad \phi = \widetilde{\phi} \circ \psi.$$

Ahora tenemos

$$\widetilde{\psi} \circ \widetilde{\phi} \circ \psi = \widetilde{\psi} \circ \phi = \psi, \quad \widetilde{\phi} \circ \widetilde{\psi} \circ \phi = \widetilde{\phi} \circ \psi = \phi.$$



Pero la propiedad universal de ψ en el primer diagrama de arriba postula que hay un homomorfismo *único* $f\colon S \to S$ tal que $f \circ \psi = \psi$. Funciona el homomorfismo identidad id_S, así que necesariamente

$$\widetilde{\psi} \circ \widetilde{\phi} = \mathrm{id}_S.$$

De la misma manera, la propiedad universal de ϕ implica que

$$\widetilde{\phi} \circ \widetilde{\psi} = \mathrm{id}_{R[U^{-1}]}.$$

Podemos concluir que los homomorfismos $\widetilde{\phi}$ y $\widetilde{\psi}$ son mutualmente inversos. ■

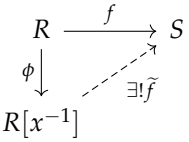
El siguiente resultado nos dice que invertir un producto xy es lo mismo que invertir x y luego invertir y.

12.2.12. Proposición. *Sea R un anillo conmutativo y sean $x, y \in R$ algunos elementos. Entonces, hay un isomorfismo natural*[*]

$$R[x^{-1}][y^{-1}] \cong R[(xy)^{-1}].$$

Demostración. Consideremos la propiedad universal de $R[x^{-1}]$. Notamos que si $f\colon R \to S$ es un homomorfismo tal que $f(x)$ es invertible en S, entonces $f(x^n) = f(x)^n$ es invertible para cualquier $n = 0, 1, 2, 3, \ldots$, así que es suficiente decir que

1) el elemento $\phi(u) = \frac{u}{1}$ es invertible en $R[x^{-1}]$;
2) si S es otro anillo junto con un homomorfismo $f\colon R \to S$ tal que $f(x)$ es invertible en S, entonces f se factoriza de modo único por ϕ:

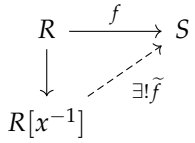


[*]Aquí $R[x^{-1}][y^{-1}]$ denota dos localizaciones consecutivas: primero $R \to R[x^{-1}]$, y luego $R[x^{-1}] \to R[x^{-1}][(y/1)^{-1}]$, donde $\frac{y}{1} \in R[x^{-1}]$.

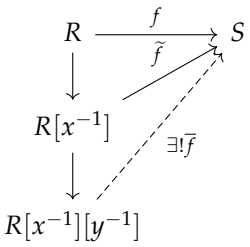
Ahora supongamos que $f\colon R \to S$ es un homomorfismo de anillos tal que $f(xy)$ es invertible en S. Entonces, $f(x)$ y $f(y)$ son también invertibles:

$$f(x)^{-1} = f(y)\,f(xy)^{-1}, \quad f(y)^{-1} = f(x)\,f(xy)^{-1},$$

así que f se factoriza de modo único por el homomorfismo canónico $R \to R[x^{-1}]$:



En este caso $\widetilde{f}\left(\frac{y}{1}\right) = f(y)$ es invertible en S, así que $\widetilde{f}$ se factoriza de modo único por el homomorfismo canónico $R[x^{-1}] \to R[x^{-1}][y^{-1}]$:



Acabamos de probar que la composición $R \to R[x^{-1}] \to R[x^{-1}][y^{-1}]$ satisface la propiedad universal de la localización $R \to R[(xy)^{-1}]$. Entonces, $R[x^{-1}][y^{-1}] \cong R[(xy)^{-1}]$. ■

El siguiente resultado interpreta la localización $R[x^{-1}]$ como un cociente del anillo de polinomios $R[T]$.

12.2.13. Proposición. *Sea R un anillo conmutativo y $x \in R$. Entonces, la composición de homomorfismos canónicos*

$$\phi\colon R \rightarrowtail R[T] \twoheadrightarrow R[T]/(xT-1)$$

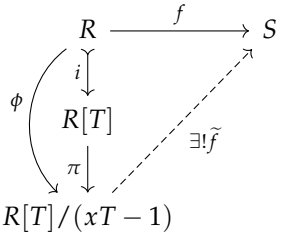
(donde $R[T]$ es el anillo de polinomios en T con coeficientes en R) satisface la propiedad universal de la localización $R \to R[x^{-1}]$, y por ende hay un isomorfismo natural

$$R[x^{-1}] \cong R[T]/(xT-1).$$

Demostración. Tenemos

$$x\,T \equiv 1 \pmod{xT-1},$$

así que $\phi(x)$ es invertible en $R[T]/(xT-1)$. Sea $f\colon R \to S$ otro homomorfismo de anillos tal que $f(x)$ es invertible en S. Supongamos que f se factoriza por ϕ:



Esto implica que para todo $a \in R$ se tiene

$$\widetilde{f}(\overline{a}) = f(a),$$

donde $\overline{a}$ denota el elemento representado por a en el cociente $R[T]/(xT-1)$. Además, para $\overline{T} \in R[T]/(xT-1)$ se tiene

$$\widetilde{f}(\overline{T}) = \widetilde{f}(\overline{x}^{-1}) = \widetilde{f}(\overline{x})^{-1} = f(x)^{-1}.$$

Pero esto ya define a $\widetilde{f}$ de modo único:

$$\begin{aligned}\widetilde{f}(\overline{a_n\,T^n + \cdots + a_1\,T + a_0}) &= \widetilde{f}(\overline{a_n}\cdot\overline{T}^n + \cdots + \overline{a_1}\cdot\overline{T} + \overline{a_0})\\ &= \widetilde{f}(\overline{a_n})\,\widetilde{f}(\overline{T})^n + \cdots + \widetilde{f}(\overline{a_1})\cdot\widetilde{f}(\overline{T}) + \widetilde{f}(\overline{a_0})\\ &= f(a_n)\,f(x)^{-1} + \cdots + f(a_1)\,f(x)^{-1} + f(a_0).\end{aligned}$$

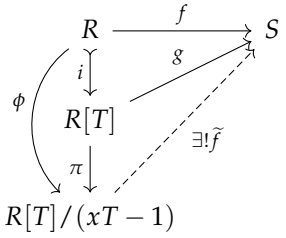
Viceversa, dado un homomorfismo $f\colon R \to S$ tal que $f(x)$ es invertible en S, se ve que

$$\begin{aligned}&g\colon R[T] \to S,\\ &\sum_i a_i\,T^i \mapsto \sum_i f(a_i)\,x^{-i}\end{aligned}$$

es un homomorfismo de anillos que cumple $g(a) = f(a)$ para todo $a \in R$ y $xT - 1 \in \ker g$, así que g induce un homomorfismo único

$$\widetilde{f}\colon R[T]/(xT-1) \to S, \quad \overline{p} \mapsto g(p)$$

tal que $\widetilde{f} \circ \pi = g$.



■

En general, para cualquier conjunto multiplicativo $U \subset R$, se puede probar que

$$R[U^{-1}] \cong R[T_u \mid u \in U]/(u\,T_u - 1 \mid u \in U),$$

donde $R[T_u \mid u \in U]$ es el anillo de polinomios en las variables T_u indexadas por los elementos de U y $(u\,T_u - 1 \mid u \in U)$ es el ideal generado por los polinomios $u\,T_u - 1$. Algunos autores *definen* la localización $R[U^{-1}]$ como el anillo cociente $R[T_u \mid u \in U]/(u\,T_u - 1 \mid u \in U)$. Esta construcción es más concisa pero probablemente menos intuitiva para los principiantes que nuestra construcción con fracciones.

12.3 Ideales en la localización

En esta sección R denota un anillo conmutativo, $U \subseteq R$ un subconjunto multiplicativo y

$$\phi\colon R \to R[U^{-1}], \quad r \mapsto \frac{r}{1}$$

es el homomorfismo canónico de localización.

Notamos que la localización conmuta con los cocientes en el siguiente sentido.

12.3.1. Proposición. *Sea $I \subseteq R$ un ideal. Definamos el conjunto*

$$\overline{U} := \{\overline{u} := u + I \mid u \in U\} \subseteq R/I$$

y sea

$$IR[U^{-1}] := \phi(I)\, R[U^{-1}] := \textit{el ideal en } R[U^{-1}] \textit{ generado por } \frac{x}{1},\ x \in I.$$

Entonces,

1) *$\overline{U}$ es un subconjunto multiplicativo en R/I;*

2) *se tiene*
$$IR[U^{-1}] = \left\{ \frac{x}{u} \;\middle|\; x \in I,\ u \in U \right\};$$

3) *hay un isomorfismo natural*
$$(R/I)[\overline{U}^{-1}] \cong R[U^{-1}]/IR[U^{-1}].$$

La notación "$IR[U^{-1}]$" es un poco abusiva: en general R no puede ser encajado en $R[U^{-1}]$, tenemos solamente el homomorfismo canónico $\phi\colon R \to R[U^{-1}]$ que no es siempre inyectivo. Sería más correcto escribir "$\phi(I)\, R[U^{-1}]$", pero lo encuentro un poco incómodo.

Demostración. Tenemos $1 \in U$, así que $\overline{1} \in \overline{U}$. Si $u, v \in U$, entonces $uv \in U$, y luego $\overline{u} \cdot \overline{v} = \overline{uv} \in \overline{U}$. Esto verifica que $\overline{U}$ es un subconjunto multiplicativo en R/I.

Notamos que los elementos de la forma $\frac{x}{u}$ con $x \in I$ y $u \in U$ forman un ideal en $R[U^{-1}]$. En efecto, este conjunto contiene $\frac{0}{1}$. Para las sumas tenemos

$$\frac{x_1}{u_1} + \frac{x_2}{u_2} = \frac{x_1 u_2 + x_2 u_1}{u_1 u_2},$$

donde $x_1 u_2 + x_2 u_1 \in I$, puesto que I es un ideal, y para los productos por los elementos de $R[U^{-1}]$,

$$\frac{r}{u}\,\frac{x}{v} = \frac{rx}{uv},$$

donde $rx \in I$.

Todos los elementos $\frac{x}{1}$ están en este ideal, así que $IR[U^{-1}] \subseteq \left\{ \frac{x}{u} \;\middle|\; x \in I,\ u \in U \right\}$. Viceversa, todo elemento $\frac{x}{u}$ puede ser escrito como $\frac{1}{u} \cdot \frac{x}{1}$ y por ende pertenece al ideal $IR[U^{-1}]$.

Para obtener el isomorfismo $(R/I)[\overline{U}^{-1}] \cong R[U^{-1}]/IR[U^{-1}]$, se puede usar la propiedad universal de la localización, pero se puede definirlo de modo explícito. Consideremos la aplicación[*]

$$\begin{aligned} f\colon R[U^{-1}] &\to (R/I)[\overline{U}^{-1}], \\ r/u &\mapsto \overline{r}/\overline{u}. \end{aligned}$$

Esta aplicación está bien definida: si $r/u = r'/u'$, entonces $v\,(r\,u' - r'\,u) = 0$ para algún $v \in U$. Luego, reduciendo esta identidad módulo I, se obtiene $\overline{v}\,(\overline{r}\,\overline{u'} - \overline{r'}\,\overline{u}) = 0$, lo que significa que $\overline{r}/\overline{u} = \overline{r'}/\overline{u'}$ en $(R/I)[\overline{U}^{-1}]$. Este es un homomorfismo de anillos: la identidad en $(R/I)[\overline{U}^{-1}]$ es $\overline{1}/\overline{1}$; la adición viene dada por

$$\overline{r_1}/\overline{u_1} + \overline{r_2}/\overline{u_2} = (\overline{r_1}\,\overline{u_2} + \overline{r_2}\,\overline{u_1})/(\overline{u_1}\,\overline{u_2}) = (\overline{r_1 u_2 + r_2 u_1})/(\overline{u_1 u_2})$$

[*] Voy a escribir r/u en lugar de $\frac{r}{u}$, dado que $\overline{r}/\overline{u}$ se ve mejor que $\frac{\overline{r}}{\overline{u}}$.

y la multiplicación viene dada por

$$(\overline{r_1}/\overline{u_1}) \cdot (\overline{r_2}/\overline{u_2}) = (\overline{r_1}\,\overline{r_2})/(\overline{u_1}\,\overline{u_2}) = \overline{r_1 r_2}/\overline{u_1 u_2}.$$

Este homomorfismo es visiblemente sobreyectivo. Su núcleo viene dado por

$$\begin{aligned}\ker f = \{r/u \in R[U^{-1}] \mid \overline{r}/\overline{u} = \overline{0}/\overline{1} \text{ en } (R/I)[\overline{U}^{-1}]\} &= \{r/u \mid \overline{v}\,\overline{r} = \overline{0} \text{ para algún } \overline{v} \in \overline{U}\} \\ &= \{r/u \mid v\,r \in I \text{ para algún } v \in U\} = IR[U^{-1}].\end{aligned}$$

Para la última igualdad, notamos que si $vr \in I$, entonces $\frac{r}{u} = \frac{vr}{vu} \in IR[U^{-1}]$, y viceversa, para todo elemento $\frac{x}{u} \in IR[U^{-1}]$ se cumple claramente $f(x/u) = \overline{0}/\overline{u} = \overline{0}/\overline{1}$.

El primer teorema de isomorfía nos dice que f induce un isomorfismo

$$R[U^{-1}]/IR[U^{-1}] \xrightarrow{\cong} (R/I)[\overline{U}^{-1}].$$

■

12.3.2. Ejemplo. Consideremos el anillo $\mathbb{Z}/12\mathbb{Z}$. Tenemos

$$(\mathbb{Z}/12\mathbb{Z})_{(3)} \cong (\mathbb{Z}_{(3)}/12\mathbb{Z}_{(3)}),$$

donde $(\mathbb{Z}/12\mathbb{Z})_{(3)}$ denota la localización de $\mathbb{Z}/12\mathbb{Z}$ afuera del ideal maximal $3\mathbb{Z}/12\mathbb{Z}$, mientras que $\mathbb{Z}_{(3)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ 3 \nmid b \right\}$ es la localización de $\mathbb{Z}$ afuera del ideal maximal $3\mathbb{Z}$. Tenemos $4 \in \mathbb{Z}_{(3)}^{\times}$, así que $12\mathbb{Z}_{(3)} = 4^{-1} \cdot 12\mathbb{Z} = 3\mathbb{Z}$. Luego,

$$(\mathbb{Z}_{(3)}/12\mathbb{Z}_{(3)}) = \mathbb{Z}_{(3)}/3\mathbb{Z}_{(3)} \cong \mathbb{Z}/3\mathbb{Z}.$$

De la misma manera, se tiene

$$(\mathbb{Z}/12\mathbb{Z})_{(2)} \cong (\mathbb{Z}_{(2)}/12\mathbb{Z}_{(2)}) \cong (\mathbb{Z}_{(2)}/4\mathbb{Z}_{(2)}) \cong \mathbb{Z}/4\mathbb{Z}.$$

En general, para el anillo $\mathbb{Z}/n\mathbb{Z}$ con $n = p_1^{k_1} \cdots p_s^{k_s}$ tenemos la siguiente forma del teorema chino del resto:

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})_{(p_1)} \times \cdots \times (\mathbb{Z}/n\mathbb{Z})_{(p_s)}.$$

▲

Ahora una pregunta muy natural es qué sucede con los ideales de R al pasar a la localización $R[U^{-1}]$. Resulta que todos los ideales de $R[U^{-1}]$ provienen de los ideales de R en el siguiente sentido.

12.3.3. Proposición.

1) *Todo ideal $J \subseteq R[U^{-1}]$ es de la forma $IR[U^{-1}]$ para algún ideal $I \subseteq R$; específicamente,*

$$J = \phi^{-1}(J)\, R[U^{-1}].$$

2) *Un ideal $I \subseteq R$ es de la forma $\phi^{-1}(J)$ para algún $J \subseteq R[U^{-1}]$ si y solamente si los elementos de U no son divisores de cero en R/I. En otras palabras, si $ur \in I$ para algunos $u \in U$, $r \in R$, entonces $r \in I$. Específicamente, cuando se cumple esta condición, se tiene*

$$I = \phi^{-1}(IR[U^{-1}]).$$

Demostración. Consideremos un ideal $J \subseteq R[U^{-1}]$. Para todo elemento $\frac{r}{u} \in J$ se cumple $\frac{r}{1} = \frac{u}{1} \cdot \frac{r}{u} \in J$, así que $r \in \phi^{-1}(J)$, y luego $\frac{r}{u} = \frac{1}{u} \cdot \frac{r}{1} \in \phi^{-1}(U)$. Viceversa, todo elemento de $\phi^{-1}(J)R[U^{-1}]$ es de la forma $\frac{x}{u}$ donde $x \in \phi^{-1}(J)$ y $u \in U$; es decir, $\frac{x}{1} \in J$. Luego, $\frac{x}{u} = \frac{1}{u} \cdot \frac{x}{1}$. Esto establece la parte 1).

En la parte 2), consideremos un ideal $J \subseteq R[U^{-1}]$ y su preimagen

$$I := \phi^{-1}(J) = \left\{ r \in R \;\middle|\; \frac{r}{1} \in J \right\}.$$

Supongamos que para $u \in U$ y $r \in R$ se cumple $ur \in I$. Esto significa que $\frac{ur}{1} \in J$. Pero luego $\frac{1}{u} \cdot \frac{ur}{1} = \frac{r}{1} \in J$, así que $r \in I$.

Viceversa, asumamos que $I \subseteq R$ es un ideal tal que $ur \in I$ implica $r \in I$ para cualesquiera $u \in U$ y $r \in R$. Consideremos el ideal correspondiente

$$IR[U^{-1}] = \left\{ \frac{x}{u} \;\middle|\; x \in I,\ u \in U \right\}.$$

Luego,

$$\begin{aligned} \phi^{-1}(IR[U^{-1}]) &= \left\{ r \in R \;\middle|\; \frac{r}{1} = \frac{x}{u} \text{ para algunos } x \in I,\ u \in U \right\} \\ &= \left\{ r \in R \;\middle|\; vur = vx \text{ para algunos } x \in I,\ u, v \in U \right\}. \end{aligned}$$

Si $vur = vx$ donde $x \in I$, $u, v \in U$, entonces $vur \in I$, donde $vu \in U$, y por nuestra hipótesis $r \in I$, así que $\phi^{-1}(IR[U^{-1}]) \subseteq I$. La otra inclusión $I \subseteq \phi^{-1}(IR[U^{-1}])$ es evidente. ■

12.3.4. Comentario. Las biyecciones del resultado anterior preservan las inclusiones: si $J_1 \subseteq J_2 \subseteq R[U^{-1}]$, entonces $\phi^{-1}(J_1) \subseteq \phi^{-1}(J_2)$. De la misma manera si $I_1 \subseteq I_2 \subseteq R$, entonces $I_1 R[U^{-1}] \subseteq I_2 R[U^{-1}]$.

12.3.5. Corolario. *Hay una biyección entre los ideales primos*

$$\begin{aligned} \operatorname{Spec} R[U^{-1}] &\cong \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap U = \emptyset\}, \\ \mathfrak{q} &\mapsto \phi^{-1}(\mathfrak{q}), \\ \mathfrak{p}R[U^{-1}] &\hookleftarrow \mathfrak{p}. \end{aligned}$$

Demostración. Para un ideal primo $\mathfrak{q} \subset \operatorname{Spec} R[U^{-1}]$ su preimagen $\mathfrak{p} := \phi^{-1}(\mathfrak{q})$ es también un ideal primo, como para cualquier homomorfismo de anillos. La condición 2) del resultado anterior dice que los elementos de U no son divisores de cero en el anillo cociente $R/\mathfrak{p}$. Pero este cociente es un dominio de integridad y por lo tanto la condición nos dice precisamente que $\mathfrak{p} \cap U = \emptyset$. Esto verifica que la aplicación $\mathfrak{q} \mapsto \phi^{-1}(\mathfrak{q})$ está bien definida.

Sea $\mathfrak{p} \subset R$ un ideal primo. Como vimos en 12.3.1, se cumple

$$R[U^{-1}]/\mathfrak{p}R[U^{-1}] \cong (R/\mathfrak{p})[\overline{U}^{-1}].$$

Puesto que $R/\mathfrak{p}$ es un dominio de integridad, para la localización $(R/\mathfrak{p})[\overline{U}^{-1}]$ hay dos posibilidades (véase 12.2.4):

a) $\overline{0} \in \overline{U}$ (es decir, $\mathfrak{p} \cap U \neq \emptyset$), y entonces $(R/\mathfrak{p})[\overline{U}^{-1}] = 0$ (es decir, $\mathfrak{p}R[U^{-1}] = R[U^{-1}]$);

b) $\overline{0} \notin \overline{U}$ (es decir, $\mathfrak{p} \cap U = \emptyset$), y entonces $(R/\mathfrak{p})[\overline{U}^{-1}]$ es un dominio de integridad (es decir, $\mathfrak{p}R[U^{-1}] \subset R[U^{-1}]$ es un ideal primo).

Entonces, la aplicación $\mathfrak{p} \mapsto \mathfrak{p}R[U^{-1}]$ también está bien definida.
La parte 1) de la proposición anterior nos dice que para cualquier ideal $\mathfrak{q} \subset R[U^{-1}]$ se cumple

$$\mathfrak{q} = \phi^{-1}(\mathfrak{q})\, R[U^{-1}].$$

La parte 2) nos dice que si para un ideal primo $\mathfrak{p} \subset R$ se cumple $\mathfrak{p} \cap U = \emptyset$, entonces

$$\mathfrak{p} = \phi^{-1}(\mathfrak{p}R[U^{-1}]).$$

■

12.3.6. Comentario. El lector que no esté satisfecho con el argumento de arriba siempre puede escribir su propia demostración usando la definición de ideales primos de 12.1.1, sin considerar los cocientes $R[U^{-1}]/\mathfrak{p}R[U^{-1}]$ y $R/\phi^{-1}(\mathfrak{q})$.

12.3.7. Corolario. *Sea $\mathfrak{p} \subset R$ un ideal primo. Hay una biyección natural*

$$\begin{aligned} \operatorname{Spec} R_{\mathfrak{p}} &\cong \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \subseteq \mathfrak{p}\}, \\ \mathfrak{P} &\mapsto \phi^{-1}(\mathfrak{P}), \\ \mathfrak{q}R_{\mathfrak{p}} &\hookleftarrow \mathfrak{q}. \end{aligned}$$

En particular, el anillo $R_{\mathfrak{p}}$ tiene un único ideal maximal dado por $\mathfrak{p}R_{\mathfrak{p}}$.

Demostración. Por la definición, $R_{\mathfrak{p}} = R[U^{-1}]$ donde $U := R \setminus \mathfrak{p}$. Entonces, la condición $\mathfrak{q} \cap U = \emptyset$ es equivalente a $\mathfrak{q} \subseteq \mathfrak{p}$. Respecto al ideal maximal, basta notar que $\mathfrak{q} \subseteq \mathfrak{p}$ implica $\mathfrak{q}R_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}$. ■

12.3.8. Ejemplo. Los ideales primos en $\mathbb{Z}_{(p)}$ corresponden a los ideales primos $(q) \subseteq \mathbb{Z}$ tales que $(q) \subseteq (p)$. Esto implica que

$$\operatorname{Spec} \mathbb{Z}_{(p)} = \{(0), (p)\}.$$

▲

12.3.9. Definición. Un anillo que tiene un único ideal maximal se llama un **anillo local**.

Acabamos de probar que para cualquier ideal primo $\mathfrak{p} \subset R$ la localización $R_{\mathfrak{p}}$ es un anillo local. Los anillos locales son mucho más sencillos que los anillos conmutativos en general. Muy a menudo problemas se resuelven considerando diferentes localizaciones $R_{\mathfrak{p}}$ para $\mathfrak{p} \subset R$.

12.4 Anillos noetherianos

En practica, para especificar un ideal, es conveniente considerar una lista de elementos que lo generan. En este sentido mucha importancia tienen ideales finitamente generados. Notemos primero que algunas operaciones con ideales pueden ser expresadas en términos de los generadores.

12.4.1. Observación. *Sean $I = (x_1, \ldots, x_m)$ y $J = (y_1, \ldots, y_n)$ dos ideales finitamente generados. Entonces, su suma y producto son también finitamente generados; específicamente*

1) *$I + J$ está generado por los elementos $x_1, \ldots, x_m, y_1, \ldots, y_n$*

2) *IJ está generado por los productos $x_i y_j$ donde $i = 1, \ldots, m$ y $j = 1, \ldots, n$,*

Demostración. Para la suma, tenemos

$$I + J = \Big((x_1) + \cdots + (x_m)\Big) + \Big((y_1) + \cdots + (y_n)\Big) = (x_1, \ldots, x_m, y_1, \ldots, y_n)$$

y para el producto,

$$IJ = \Big((x_1) + \cdots + (x_m)\Big) \cdot \Big((y_1) + \cdots + (y_n)\Big) = \sum_{1 \le i \le m} \sum_{1 \le j \le n} (x_i) \cdot (y_j) = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} (x_i y_j).$$

Aquí hemos usado el hecho de que el producto de dos ideales principales (x) e (y) es el ideal generado por xy. ■

12.4.2. Observación. *Sea $f\colon R \to S$ un homomorfismo sobreyectivo de anillos conmutativos. Si $I = (x_1, \ldots, x_n) \subseteq R$ es un ideal finitamente generado, entonces $f(I) = (f(x_1), \ldots, f(x_n)) \subseteq S$ es también finitamente generado.*

En particular, si R es un anillo conmutativo y $I \subseteq R$ es un ideal, entonces para todo ideal finitamente generado $J \subseteq R$ el ideal correspondiente $J/I \subseteq R/I$ es también finitamente generado.

Demostración. Tenemos

$$I = \{r_1 x_1 + \cdots + r_n x_n \mid r_i \in R\}$$

y luego

$$f(I) = \{f(r_1)\, f(x_1) + \cdots + f(r_n)\, f(x_n) \mid r_i \in R\} = \{s_1\, f(x_1) + \cdots + s_n\, f(x_n) \mid s_i \in S\} \\ = (f(x_1), \ldots, f(x_n)),$$

dado que f es un homomorfismo sobreyectivo. ■

Resulta que la *intersección* de dos ideales finitamente generados no tiene por qué ser un ideal finitamente generado.

12.4.3. Ejemplo. Consideremos el anillo[*]

$$R := \mathbb{Z} + X^2\,\mathbb{Q}[X] := \{a_0 + a_2\, X^2 + \cdots + a_n\, X^n \mid a_0 \in \mathbb{Z},\ a_1 = 0,\ a_2, \ldots, a_n \in \mathbb{Q}\} \subset \mathbb{Q}[X].$$

Sea I el ideal generado por X^2 y sea J el ideal generado por X^3. Los elementos de I son los polinomios

$$a_2\, X^2 + a_4\, X^4 + a_5\, X^5 + \cdots + a_n\, X^n,$$

donde $a_2 \in \mathbb{Z}$ y $a_4, a_5, \ldots, a_n \in \mathbb{Q}$. Los elementos de J son los polinomios

$$a_3\, X^3 + a_5\, X^5 + a_6\, X^6 + \cdots + a_n\, X^n,$$

donde $a_3 \in \mathbb{Z}$ y $a_5, a_6, \ldots, a_n \in \mathbb{Q}$. Notamos que

$$I \cap J = X^5\,\mathbb{Q}[X] := \{a_5\, X^5 + a_6\, X^6 + \cdots + a_n\, X^n \mid a_i \in \mathbb{Q}\}.$$

Este ideal no es finitamente generado en R. En efecto, supongamos que $I \cap J = (f_1, \ldots, f_n)$ para algunos polinomios $f_1, \ldots, f_n \in I \cap J$. Escribamos $f_i = X^5\, g_i$ donde $g_i \in \mathbb{Q}[X]$. Podemos escribir el término constante de cada uno de estos polinomios como $g_i(0) = \frac{a_i}{b_i}$ donde a_i, b_i son números enteros coprimos.

[*]Este ejemplo curioso fue sugerido por un usuario del foro *Mathematics Stack Exchange*: http://math.stackexchange.com/questions/295875/

Consideremos el polinomio $g := \frac{1}{b_1 \cdots b_n + 1} X^5$. Tenemos $g \in I \cap J$. Sin embargo, $g \notin (f_1, \ldots, f_n)$. En efecto, si lo último fuera cierto, tendríamos algunos polinomios $h_1, \ldots, h_n \in R$ tales que

$$g = f_1 h_1 + \cdots + f_n h_n.$$

Aquí g y $f_1, \ldots, f_n$ son divisibles por X^5. Cancelando X^5 y poniendo $X = 0$ se obtiene

$$\frac{1}{b_1 \cdots b_n + 1} = \frac{a_1}{b_1} h_1(0) + \cdots + \frac{a_n}{b_n} h_n(0)$$

donde $h_i(0) \in \mathbb{Z}$. Esto es imposible, puesto que $b_i \nmid (b_1 \cdots b_n + 1)$ para ningún $i = 1, \ldots, n$.

Este ejemplo también demuestra que la preimagen de un ideal finitamente generado no es necesariamente un ideal finitamente generado. En efecto, tenemos el homomorfismo de inclusión $R \hookrightarrow \mathbb{Q}[X]$ y como acabamos de ver, el ideal $X^5\,\mathbb{Q}[X]$ no es finitamente generado en R. ▲

Entonces, aunque es cómodo trabajar con ideales finitamente generados, en general es fácil salir de su clase. Por esto sería interesante estudiar los anillos donde todos los ideales son finitamente generados.

12.4.4. Definición. Si en un anillo conmutativo R todo ideal es finitamente generado, se dice que R es **noetheriano**.

12.4.5. Ejemplo. En todo cuerpo k los únicos ideales son (0) y $(1) = k$, así que k es noetheriano.

El anillo $\mathbb{Z}$ es noetheriano: sus ideales son (n) para $n = 0, 1, 2, 3, \ldots$ ▲

El término "noetheriano" conmemora las contribuciones de la matemática alemana Emmy Noether (1882–1935) que fue una de los fundadores del álgebra moderna y entre otras cosas reconoció la importancia de anillos noetherianos. He aquí una condición equivalente.

12.4.6. Observación. *Un anillo R es noetheriano si y solamente si para toda cadena de ideales*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R$$

se tiene $I_n = I_{n+1}$ para n suficientemente grande.

Demostración. Supongamos que R es noetheriano y consideremos el ideal $I := \bigcup_{n \geq 0} I_n$. Tenemos $I = (x_1, \ldots, x_m)$ para algunos $x_1, \ldots, x_m \in I$, pero estos elementos necesariamente pertenecen a I_n para algún n. Luego, $I_n = I_{n+1} = I_{n+2} = \cdots = I$.

Viceversa, supongamos que R no es noetheriano y existe algún ideal $I \subset R$ que no es finitamente generado. Escojamos $x_0 \in I$. Tenemos $I \neq (x_0)$, así que se puede escoger $x_1 \in I \setminus (x_0)$. Luego, $I \neq (x_0, x_1)$ y existe $x_2 \in I \setminus (x_0, x_1)$, etcétera. De esta manera se obtiene una cadena

$$(x_0) \subsetneq (x_0, x_1) \subsetneq (x_0, x_1, x_2) \subsetneq \cdots \subset R.$$

■

12.4.7. Ejemplo. Sea R un anillo conmutativo. El anillo de polinomios $R[X_1, \ldots, X_n]$ puede ser visto como un subanillo de $R[X_1, \ldots, X_n, X_{n+1}]$. Tenemos una cadena de anillos

$$R[X_1] \subset R[X_1, X_2] \subset R[X_1, X_2, X_3] \subset \cdots$$

La unión nos da el anillo de polinomios en un número infinito de variables:

$$S := R[X_1, X_2, \ldots] := \bigcup_{n \geq 1} R[X_1, \ldots, X_n].$$

En cierto sentido, este anillo es demasiado grande para ser noetheriano: por ejemplo, se tiene una cadena de ideales

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots \subset S$$

Sin embargo, notamos que S es un dominio de integridad, y entonces S puede ser encajado en su cuerpo de fracciones $K(S)$. Siendo un cuerpo, $K(S)$ es noetheriano. Esto es un ejemplo tonto que demuestra que un subanillo de un anillo noetheriano no tiene por qué ser noetheriano. ▲

12.4.8. Ejemplo. Sea $\mathcal{C}(\mathbb{R})$ el anillo de las funciones continuas $f\colon \mathbb{R} \to \mathbb{R}$. Para $n = 0, 1, 2, 3, \ldots$ consideremos

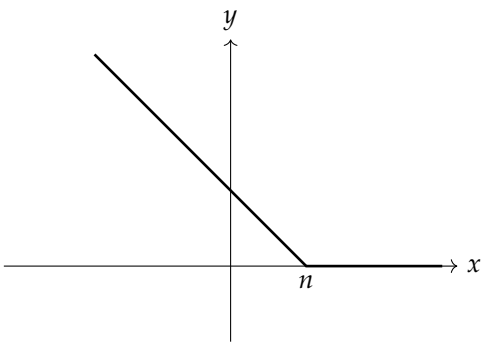
$$I_n := \{f \in \mathcal{C}(\mathbb{R}) \mid f(x) = 0 \text{ para } x \geq n\}.$$

Esto es un ideal en $\mathcal{C}(\mathbb{R})$ y se tiene una cadena infinita ascendente

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subset \mathcal{C}(\mathbb{R}).$$

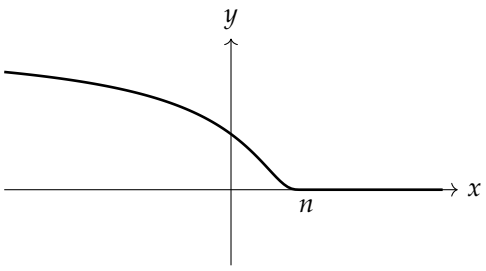
En efecto, es fácil encontrar una función continua $f_n\colon \mathbb{R} \to \mathbb{R}$ tal que $f_n \in I_n$, pero $f_n \notin I_{n-1}$. Por ejemplo, basta poner

$$f_n(x) := \begin{cases} n - x, & x < n, \\ 0, & x \geq n. \end{cases}$$



Podemos considerar el subanillo $\mathcal{C}^\infty(\mathbb{R}) \subset \mathcal{C}(\mathbb{R})$ cuyos elementos son las funciones infinitamente diferenciables. Las funciones que acabamos de definir no son diferenciables en $x = n$, pero se puede tomar

$$g_n(x) := \begin{cases} e^{1/(x-n)}, & x < n, \\ 0, & x \geq n. \end{cases}$$



Es un ejercicio de cálculo comprobar que g_n es infinitamente diferenciable en todos los puntos. Podemos tomar

$$J_n := \{f \in \mathcal{C}^\infty(\mathbb{R}) \mid f(x) = 0 \text{ para } x \geq n\} = I_n \cap \mathcal{C}^\infty(\mathbb{R}),$$

y luego $g_n \in J_n \setminus J_{n-1}$, lo que demuestra que existe una cadena infinita ascendente

$$J_0 \subsetneq J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots \subset \mathcal{C}^\infty(\mathbb{R}).$$

De la misma manera, las funciones holomorfas $\mathbb{C} \to \mathbb{C}$ forman un anillo $\mathcal{O}(\mathbb{C})$. Este anillo tampoco es noetheriano. Podemos considerar los ideales

$$I_n := \{f \in \mathcal{O}(\mathbb{C}) \mid f(k) = 0 \text{ para todo } k = n+1, n+2, \ldots\}.$$

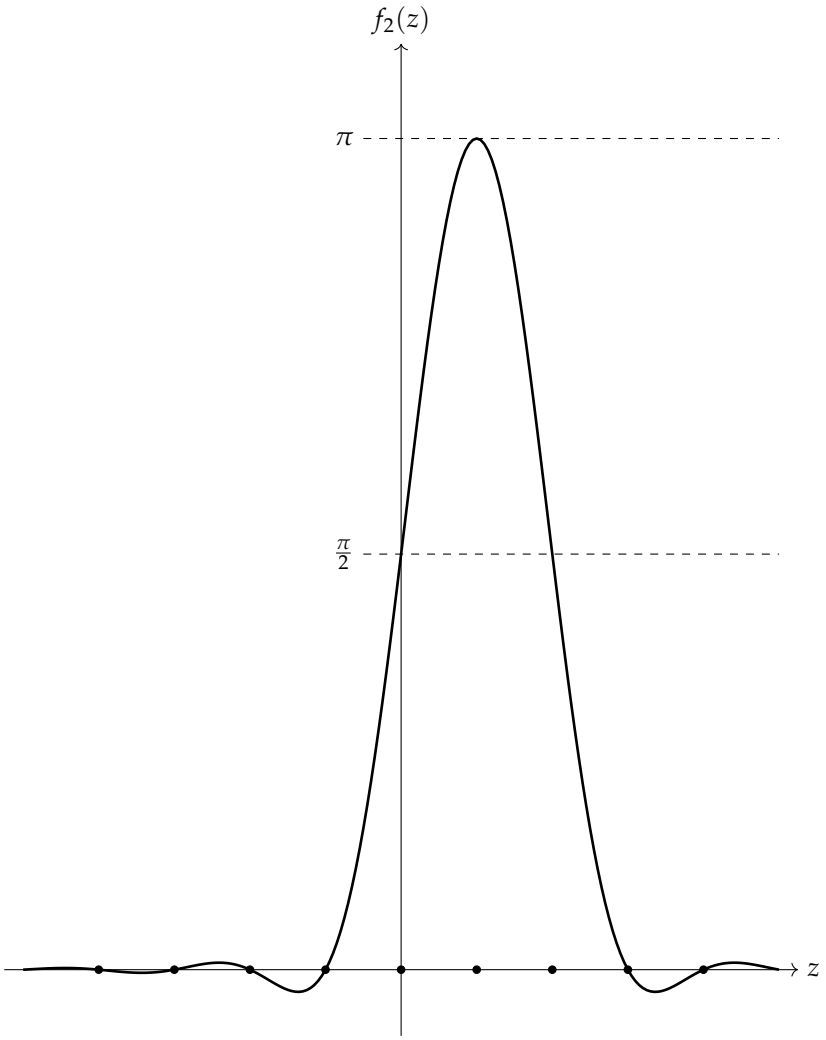
Estos forman una cadena

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \cdots \subset \mathcal{O}(\mathbb{C}).$$

Para las funciones

$$f_n := \frac{\sin \pi z}{z\,(z-1)\,(z-2)\cdots(z-n)}$$

se tiene $f_n \in I_{n+1} \setminus I_n$ (para entender este ejemplo, hay que conocer el análisis complejo).



La función $f_2(z) := \frac{\sin \pi z}{z\,(z-1)\,(z-2)}$

▲

Intuitivamente, los anillos $\mathcal{C}(\mathbb{R})$, $\mathcal{C}^\infty(\mathbb{R})$, $\mathcal{O}(\mathbb{C})$ son demasiado grandes para ser noetherianos: hay demasiadas funciones continuas, diferenciables, holomorfas. Intuitivamente, todos estos ejemplos se obtienen del hecho de que este tipo de funciones pueden tener muchos ceros. Las funciones polinomiales no constantes (en una variable) tienen un número finito de ceros. Aunque los anillos como $\mathcal{C}(\mathbb{R})$, $\mathcal{C}^\infty(\mathbb{R})$, $\mathcal{O}(\mathbb{C})$ tienen mucha importancia en análisis, en álgebra muy a menudo se trabaja con los anillos de polinomios $k[X_1, \ldots, X_n]$ donde k es un cuerpo, o en general con los anillos cociente $k[X_1, \ldots, X_n]/I$. Resulta que todos son noetherianos, y así se establece el siguiente hecho.

12.4.9. Teorema (El teorema de la base de Hilbert). *Si R es un anillo noetheriano, entonces el anillo de polinomios $R[X]$ es también noetheriano.*

12.4.10. Corolario. *Si R es un anillo noetheriano, entonces $R[X_1, \ldots, X_n]$ es también un anillo noetheriano.*

Demostración. Podemos usar el teorema de la base junto con la inducción sobre n y los isomorfismos $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$. ■

Demostración de 12.4.9. Consideremos una cadena ascendente de ideales

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R[X].$$

Necesitamos ver que esta se estabiliza; es decir, que existe un índice k tal que $I_k = I_{k'}$ para todo $k' \geq k$.

Sea $I_{k,d}$ el ideal de los elementos de R que aparecen como los coeficientes mayores de los polinomios de grado d en I_k; específicamente,

$$I_{k,d} := \{a \in R \mid \text{existe un polinomio } a\,X^d + \cdots \in I_k\} \cup \{0\}.$$

1) Verifiquemos que $I_{k,d}$ es un ideal.

   Para $a, b \in I_{k,d}$ hay que ver que $a + b \in I_{k,d}$. Esto es obvio si $a = 0$ o $b = 0$ o $a + b = 0$ y podemos descartar estos casos. Entonces, $a, b \in I_{k,d}$ significa que en I_k existen polinomios $f = a\,X^d + \cdots$ y $g = b\,X^d + \cdots$. Luego, $f + g = (a + b)\,X^d + \cdots \in I_k$ y $\deg(f + g) = d$ (asumiendo que $a + b \neq 0$), así que $a + b \in I_{k,d}$.

   Para los productos, si $f = a\,X^d + \cdots \in I_k$, entonces para cualquier elemento $c \in R$ el polinomio $cf = ca\,X^d + \cdots$ también está en I_k. Si $ca \neq 0$, entonces $\deg(cf) = d$ y $ca \in I_{k,d}$. Si $ca = 0$, tenemos $0 \in I_{k,d}$.

2) Verifiquemos que

   $$I_{k,d} \subseteq I_{k',d'} \quad \text{si } k \leq k' \text{ y } d \leq d'.$$

   Notamos que en nuestra cadena de ideales $I_k \subseteq I_{k'}$ para $k \leq k'$. Ahora si $a \in I_{k,d}$ y $a \neq 0$, esto significa que existe un polinomio $f = a\,X^d + \cdots \in I_k \subseteq I_{k'}$. Luego, $X^{d'-d} f = a\,X^{d'} + \cdots \in I_{k'}$, lo que demuestra que $a \in I_{k',d'}$.

3) Probemos que entre los $I_{k,d}$ hay solo un número finito de ideales distintos. En efecto, supongamos lo contrario. En este caso una familia infinita de ideales distintos corresponde a un subconjunto infinito de los índices dobles $(k, d) \in \mathbb{N} \times \mathbb{N}$ y entre ellos se puede escoger una cadena infinita* (k_ℓ, d_ℓ) con

   $$k_0 \leq k_1 \leq k_2 \leq \cdots, \quad d_0 \leq d_1 \leq d_2 \leq \cdots$$

   De aquí se obtiene una cadena ascendente

   $$I_{k_0,d_0} \subsetneq I_{k_1,d_1} \subsetneq I_{k_2,d_2} \subsetneq \cdots \subset R$$

   pero esto contradice nuestra hipótesis que R es noetheriano.

*Ejercicio 12.29.

4) Entonces, hay solo un número finito de ideales distintos $I_{k,d}$. Esto significa que existe un índice k tal que
$$I_{k,d} = I_{k+1,d} = I_{k+2,d} = \cdots$$
para todo d.

Supongamos que $k' \geq k$. Vamos a probar que $I_k = I_{k'}$. Tenemos una inclusión $I_k \subseteq I_{k'}$ y hay que ver que todo elemento de $I_{k'}$ pertenece a I_k. Para $f \in I_{k'}$ podemos proceder por inducción sobre $d = \deg f$. Como la base de inducción se puede considerar el caso de $d = -\infty$; es decir, $f = 0$. Para el paso inductivo, supongamos que todos los polinomios de $I_{k'}$ de grado $< d$ pertenecen a I_k. Luego, si $f = a\,X^d + \cdots \in I_{k'}$, entonces $a \in I_{k',d}$. Pero acabamos de ver que $I_{k',d} = I_{k,d}$, lo que implica que existe un polinomio $g = a\,X^d + \cdots \in I_k$. Ahora $\deg(f-g) < d$ y por ende $f - g \in I_k$ por la hipótesis de inducción. Pero en este caso $f = (f-g) + g \in I_k$. ■

Un poco de la historia. En el siglo XIX muchos algebristas se dedicaban a la **teoría de invariantes** que trata de encontrar generadores de ciertos ideales en casos particulares. Hilbert probó el teorema de arriba para deducir la existencia de un número finito de generadores en un caso general abstracto. Luego el matemático alemán Paul Gordan (1837–1912), conocido como *el rey de la teoría de invariantes* no aceptó el articulo de Hilbert a la revista *Mathematische Annalen*, diciendo que su argumento estaba poco claro y que "no era matemáticas, sino teología".

12.4.11. Digresión. Si R es un anillo noetheriano, entonces el anillo de series formales $R[\![X_1, \ldots, X_n]\!]$ es también noetheriano. Sin embargo, esto se demuestra de otra manera (a saber, $R[\![X_1, \ldots, X_n]\!]$ es una **completación** del anillo noetheriano $R[X_1, \ldots, X_n]$; la completación es otra construcción interesante, pero no la vamos a definir en este curso).

12.4.12. Proposición. *Si R es un anillo noetheriano, entonces toda localización $R[U^{-1}]$ es también un anillo noetheriano.*

Demostración. Como vimos en §12.3, para todo ideal $J \subseteq R[U^{-1}]$ se cumple $J = \phi^{-1}(J)\,R[U^{-1}]$ y la correspondencia $J \mapsto \phi^{-1}(J)$ es inyectiva y preserva inclusiones. Entonces, toda cadena de ideales
$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots \subset R[U^{-1}]$$
nos da una cadena de ideales
$$\phi^{-1}(J_0) \subseteq \phi^{-1}(J_1) \subseteq \phi^{-1}(J_2) \subseteq \cdots \subset R$$
que se estabiliza, puesto que R es noetheriano. Pero esto significa que la cadena en $R[U^{-1}]$ se estabiliza.

Otro modo de probar el resultado es notar que si todo ideal en R es finitamente generado, entonces para todo ideal $J \subseteq R[U^{-1}]$ se tiene
$$\phi^{-1}(J) = (x_1, \ldots, x_n),$$
para algunos $x_1, \ldots, x_n \in R$, y luego
$$J = \phi^{-1}(J)\,R[U^{-1}] = \left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right).$$
■

12.4.13. Ejemplo. Sea k un cuerpo. Para una colección de polinomios $f_i \in k[X_1, \ldots, X_n]$ consideremos el conjunto de sus ceros comunes en $\mathbb{A}^n(k)$:
$$V(\{f_i\}_{i\in I}) := \{x \in \mathbb{A}^n(k) \mid f_i(x) = 0 \text{ para todo } i \in I\}.$$

Este se llama un **conjunto algebraico**. Luego,

$$V(\{f_i\}_{i\in I}) = V(J) := \{x \in \mathbb{A}^n(k) \mid f(x) = 0 \text{ para todo } f \in J\},$$

donde $J \subseteq k[X_1, \ldots, X_n]$ es el ideal generado por los polinomios f_i. El teorema de la base nos dice que J es necesariamente finitamente generado: $J = (g_1, \ldots, g_m)$ y luego

$$V(\{f_i\}_{i\in I}) = V(J) = V(g_1, \ldots, g_m).$$

Esto significa que todo sistema de ecuaciones polinomiales en $k[X_1, \ldots, X_n]$ siempre equivale a un sistema de un número finito de ecuaciones polinomiales.

Lamentablemente, la prueba del teorema de la base no es constructiva: no sabemos cuáles son los generadores. Para hacer cálculos con conjuntos algebraicos, se usan sistemas especiales de generadores, llamados **bases de Gröbner**. ▲

12.4.14. Observación. *Sea $f\colon R \to S$ un homomorfismo sobreyectivo. Si R es noetheriano, entonces S es también noetheriano. De manera equivalente, todo cociente de un anillo noetheriano es noetheriano.*

Demostración. Véase 12.4.2. ■

12.4.15. Definición. Sean R un anillo conmutativo y A una R-álgebra conmutativa; es decir, un anillo A dotado de un homomorfismo $f\colon R \to A$. Se dice que A es una **R-álgebra finitamente generada** si existen elementos $x_1, \ldots, x_n$ tales que todo elemento de A puede ser expresado como un polinomio en $x_1, \ldots, x_n$ con coeficientes en R; es decir, como una suma finita

$$\sum_{i_1,\ldots,i_n\geq 0} r_{i_1,\ldots,i_n} \cdot x_1^{i_1} \cdots x_n^{i_n} := \sum_{i_1,\ldots,i_n\geq 0} f(r_{i_1,\ldots,i_n})\, x_1^{i_1} \cdots x_n^{i_n}.$$

El anillo de polinomios $R[X_1, \ldots, X_n]$ es una R-álgebra finitamente generada. En general, las R-álgebras finitamente generadas son precisamente los cocientes de estos anillos de polinomios.

12.4.16. Observación. *Una R-álgebra A es finitamente generada si y solo si existe un homomorfismo sobreyectivo $R[X_1, \ldots, X_n] \twoheadrightarrow A$ para algún n; es decir, si y solo si $A \cong R[X_1, \ldots, X_n]/I$ para algún n y algún ideal I.*

Demostración. Por la propiedad universal del álgebra de polinomios, la asignación $X_i \mapsto x_i$ define un homomorfismo único de R-álgebras:

$$\begin{aligned} f\colon R[X_1, \ldots, X_n] &\to A, \\ X_i &\mapsto x_i. \end{aligned}$$

El hecho de que los x_i generan a A como una R-álgebra significa precisamente que esto es una sobreyección. Luego, por el primer teorema de isomorfía

$$A \cong R[X_1, \ldots, X_n]/\ker f.$$

■

12.4.17. Observación. *Si R es un anillo noetheriano, entonces toda R-álgebra finitamente generada A es también un anillo noetheriano.*

Demostración. Se tiene $A \cong R[X_1, \ldots, X_n]/I$ donde $R[X_1, \ldots, X_n]$ es noetheriano por el teorema de la base, y luego todo cociente de un anillo noetheriano es también noetheriano. ■

En la geometría algebraica elemental, las propiedades de conjuntos algebraicos $X \subseteq \mathbb{A}^n(k)$ se estudian a través de las k-álgebras finitamente generadas $k[X_1, \ldots, X_n]/I(X)$, llamadas las **álgebras de funciones polinomiales sobre** X. Véase [Ful2008] para una introducción amigable a este tema. La geometría algebraica es una área inmensa de las matemáticas que ha sido una de las más influyentes a partir del siglo XX.

En este capítulo no hemos tocado ni siquiera la punta del iceberg del álgebra conmutativa. El lector interesado puede consultar [Sha2001], [Rei1995], [AM1969] (un libro de texto clásico) o [Eis2004] (una enciclopedia de 800 páginas).

12.5 Ejercicios

Ideales primos y maximales

Ejercicio 12.1. *Sea $\mathcal{C}(\mathbb{R})$ el anillo de las funciones continuas $f\colon \mathbb{R} \to \mathbb{R}$ con operaciones punto por punto. Demuestre que para cualquier $x \in \mathbb{R}$*

$$\mathfrak{m}_x := \{\text{funciones continuas } f\colon \mathbb{R} \to \mathbb{R} \mid f(x) = 0\}$$

es un ideal maximal en $\mathcal{C}(\mathbb{R})$.

Ejercicio 12.2. *Determine si el ideal generado por el polinomio $X^2 + 1$ es primo o maximal en el anillo*

$$\mathbb{R}[X], \quad \mathbb{C}[X], \quad \mathbb{Z}[X], \quad \mathbb{F}_2[X].$$

Ejercicio 12.3. *Sea R un anillo conmutativo y sea $\mathfrak{p} \subset R$ un ideal primo. Demuestre que si $x^n \in \mathfrak{p}$ para algún $x \in R$ y $n = 1, 2, 3, \ldots$, entonces $x \in \mathfrak{p}$.*

Ejercicio 12.4. *Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos. Para un ideal primo $\mathfrak{p} \subset S$ verifique directamente que $f^{-1}(\mathfrak{p})$ es un ideal primo en R.*

Ejercicio 12.5. *Sea R un anillo conmutativo y sea $\mathfrak{p} \subset R$ un ideal primo.*

1) *Demuestre que para dos ideales $I, J \subseteq R$, si $IJ \subseteq \mathfrak{p}$, entonces $I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$.*
2) *Demuestre que si para un ideal $I \subseteq R$ se tiene $I^n \subseteq \mathfrak{p}$ para algún $n = 1, 2, 3, \ldots$, entonces $I \subseteq \mathfrak{p}$.*

Ejercicio 12.6. *Sean R un anillo conmutativo e $I \subseteq R$ un ideal.*

1) *Demuestre que*

$$I[X] := \Big\{ \sum_i a_i X^i \in R[X] \;\Big|\; a_i \in I \}$$

es un ideal en el anillo de polinomios $R[X]$ y

$$R[X]/I[X] \cong (R/I)[X].$$

2) *Demuestre que si $\mathfrak{p} \subset R$ es un ideal primo, entonces el ideal $\mathfrak{p}[X]$ es primo en $R[X]$.*
3) *Demuestre que si $\mathfrak{m} \subset R$ es un ideal maximal, entonces el ideal $\mathfrak{m}[X]$ no es maximal en $R[X]$.*

Ejercicio 12.7. *Sea R un anillo conmutativo. Para un subconjunto $S \subseteq R$ sea $V(S)$ el conjunto de los ideales primos que contienen a S:*

$$V(S) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq S\}.$$

1) *Demuestre que para $S_1 \subseteq S_2 \subseteq R$ se tiene $V(S_2) \subseteq V(S_1)$.*
2) *Demuestre que $V(S) = V(I)$ donde $I = (S)$ es el ideal generado por S.*
3) *Demuestre que $V(0) = \operatorname{Spec} R$ y $V(1) = \emptyset$.*
4) *Demuestre que $V(I) \cup V(J) = V(IJ)$ para ideales $I, J \subseteq R$.*
5) *Demuestre que $\bigcap_k V(I_k) = V(\sum_k I_k)$ para ideales $I_k \subseteq R$.*

Ejercicio 12.8. *Sean R y S anillos conmutativos. Consideremos el producto $R \times S$ con las proyecciones canónicas*

$$\begin{array}{ccccc} R & \xleftarrow{\pi_1} & R \times S & \xrightarrow{\pi_2} & S \\ r & \longleftarrow & (r,s) & \longmapsto & s \end{array}$$

1) *Si $\mathfrak{p} \subset R$ y $\mathfrak{q} \subset S$ son ideales primos, demuestre que*

$$\mathfrak{p} \times S := \pi_1^{-1}(\mathfrak{p}) = \{(x,s) \mid x \in \mathfrak{p},\ s \in S\}, \quad R \times \mathfrak{q} = \pi_2^{-1}(\mathfrak{q}) := \{(r,y) \mid r \in R,\ y \in \mathfrak{q}\}$$

son ideales primos en el producto $R \times S$.

2) *Demuestre que si $\mathfrak{P} \subset R \times S$ es un ideal primo, entonces $\mathfrak{P}$ es de la forma $\mathfrak{p} \times S$ o $R \times \mathfrak{q}$ como en 1).*
Indicación: para $e_1 := (1_R, 0_S)$ y $e_2 := (0_R, 1_S)$ note que $e_1 e_2 \in \mathfrak{P}$, así que $e_1 \in \mathfrak{P}$ o $e_2 \in \mathfrak{P}$.

Ensto nos da una biyección natural $\operatorname{Spec}(R \times S) \cong \operatorname{Spec} R \sqcup \operatorname{Spec} S$.

Lema de Zorn

Ejercicio 12.9. *Sea R un anillo conmutativo. Sea $U \subset R$ un subconjunto no vacío tal que $0 \notin U$ y si $x, y \in U$, entonces $xy \in U$.*

1) *Deduzca del lema de Zorn que existe un ideal $\mathfrak{p} \subset R$ que satisface las siguientes propiedades:*
   - *$U \cap \mathfrak{p} = \emptyset$,*
   - *Si $\mathfrak{p} \subseteq I$ para otro ideal I que satisface $U \cap I = \emptyset$, entonces $I = \mathfrak{p}$.*
2) *Demuestre que $\mathfrak{p}$ es un ideal primo.*

Indicación: basta revisar y entender nuestra prueba de que $N(R) = \bigcap_{\mathfrak{p} \subset R \text{ primo}} \mathfrak{p}$.

Ejercicio 12.10. *Sean R un anillo conmutativo no nulo e $I \subset R$ un ideal propio.*

1) *Sea $R \supset \mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq I$ una cadena descendente de ideales primos que contienen a I. Demuestre que $\mathfrak{p} := \bigcap_i \mathfrak{p}_i$ es un ideal primo que contiene a I.*
2) *Deduzca del lema de Zorn que en R existen **ideales primos minimales sobre** I; es decir, ideales primos $I \subseteq \mathfrak{p} \subset R$ tales que si $\mathfrak{q} \subseteq \mathfrak{p}$ para otro ideal primo $I \subseteq \mathfrak{q} \subset R$, entonces $\mathfrak{q} = \mathfrak{p}$.*

Ejercicio 12.11. *Sea R un anillo conmutativo noetheriano. En este ejercicio vamos a probar que para todo ideal propio no nulo $I \subset R$ (es decir, $I \neq R$, $I \neq 0$)*

(*) *existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \neq 0$ tales que $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I$.*

Para llegar a una contradicción, asumamos que esto es falso y existen ideales propios no nulos que no cumplen la propiedad (*).

1) *Demuestre usando el lema de Zorn que en este caso existe un ideal propio no nulo I que es maximal entre los ideales que no cumplen la propiedad (*). Demuestre que I no es primo, así que existen $x, y \in R$ tales que $xy \in I$, pero $x \notin I$ e $y \notin I$.*
2) *Demuestre que para los ideales $A := I + (x)$ y $B := I + (y)$ se tiene $AB \subseteq I$ y son ideales propios no nulos.*
3) *Demuestre que A y B cumplen la propiedad (*): se tiene*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m \subseteq A, \quad \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq B$$

para algunos ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{q}_n \subset R$. Deduzca que $\mathfrak{p}_1 \cdots \mathfrak{p}_m\, \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq I$.

Concluya que hemos obtenido una contradicción.

Localización

Ejercicio 12.12. *En el cuerpo de las series de Laurent $\mathbb{Q}((X))$, encuentre el elemento inverso de $X - X^2$.*

Ejercicio 12.13. *Describa los cuerpos de fracciones $K(R)$ para los anillos*

$$R = \mathbb{Z}[\sqrt{-1}],\ \mathbb{Z}[\sqrt{5}],\ \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big].$$

Ejercicio 12.14. *Sea $R \times S$ un producto de anillos conmutativos no nulos. Consideremos $e := (1,0)$. Demuestre que $(R \times S)[e^{-1}] \cong R$.*
Sugerencia: nota que $\frac{(r,s)}{(1,0)} = \frac{(r,s)}{(1,1)} = \frac{(r,0)}{(1,1)}$ para cualesquiera $r \in R$ y $s \in S$.

Ejercicio 12.15. *Consideremos el anillo finito $R = \mathbb{Z}/n\mathbb{Z}$ donde $n = p_1^{k_1} \cdots p_s^{k_s}$.*

1) *Demuestre que los ideales maximales en R son $\mathfrak{m}_i = p_i\,\mathbb{Z}/n\mathbb{Z}$ para $i = 1, \ldots, s$.*
2) *Demuestre que $R \cong R_{\mathfrak{m}_1} \times \cdots \times R_{\mathfrak{m}_s}$.*

Sugerencia: demuestre que la aplicación canónica $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ satisface la propiedad universal de la localización $\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i}$.

Ejercicio 12.16. *Sean R un anillo conmutativo, $U \subseteq R$ un subconjunto multiplicativo y $\phi\colon R \to R[U^{-1}]$ el homomorfismo canónico de localización.*

1) *Para un ideal primo $\mathfrak{p} \subset R$ tal que $\mathfrak{p} \cap U = \emptyset$ compruebe directamente que el ideal $\mathfrak{p}R[U^{-1}] \subset R[U^{-1}]$ (es decir, que $\mathfrak{p}R[U^{-1}] \neq R[U^{-1}]$ y $\frac{r}{u} \cdot \frac{s}{v} \in \mathfrak{p}R[U^{-1}]$ implica $\frac{r}{u} \in \mathfrak{p}R[U^{-1}]$ o $\frac{s}{v} \in \mathfrak{p}R[U^{-1}]$).*
2) *Para un ideal primo $\mathfrak{q} \subset R[U^{-1}]$ compruebe directamente que $\phi^{-1}(\mathfrak{q}) \cap U = \emptyset$ (use la definición original de ideales primos).*

Ejercicio 12.17. *He aquí una generalización de las ideas que hemos ocupado para caracterizar los ideales en $R[U^{-1}]$. Para un homomorfismo de anillos $f\colon R \to S$ e ideales $I \subseteq R$, $J \subseteq S$ definamos*

$$I^e := f(I)\,S \subseteq S, \quad J^c := f^{-1}(J) \subseteq R$$

*(el ideal I^e se llama la **extensión** de I y el ideal J^c se llama la **contracción** de J). Verifique las siguientes propiedades de estas operaciones:*

1) *Si $I_1 \subseteq I_2$, entonces $I_1^e \subseteq I_2^e$.*
2) *Si $J_1 \subseteq J_2$, entonces $J_1^c \subseteq J_2^c$.*
3) *$(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.*
4) *$I \subseteq I^{ec}$, $J \supseteq J^{ce}$. Encuentre ejemplos cuando las inclusiones son estrictas.*
5) *$J^c = J^{cec}$, $I^e = I^{ece}$.*

Ejercicio 12.18. *Sea $n = p_1^{k_1} \cdots p_s^{k_s}$. Describa los ideales primos en el anillo*

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{ \frac{a}{n^k} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots \Big\}.$$

Ejercicio 12.19. *Sea R un anillo conmutativo y $U \subseteq R$ un subconjunto multiplicativo.*

1) *Para un ideal $I \subseteq R$ y un elemento $x \in R$ verifique que $(I : x) := \{r \in R \mid xr \in I\}$ es un ideal en R.*

2) *Demuestre que hay una biyección entre los ideales en la localización $R[U^{-1}]$ y los ideales en R tales que $(I : u) = I$ para todo $u \in U$.*

Ejercicio 12.20. *Sea R un anillo conmutativo. Denotemos por*

$$N(R) := \{x \in R \mid x^n = 0 \text{ para algún } n = 1, 2, 3, \ldots\}$$

el nilradical. Demuestre que para todo subconjunto multiplicativo $U \subseteq R$ se tiene

$$N(R[U^{-1}]) = N(R)R[U^{-1}].$$

Ejercicio 12.21. *Sean R un anillo conmutativo y $x \in R$ algún elemento no nulo.*

1) *Demuestre que $\operatorname{Ann}(x) := \{r \in R \mid rx = 0\}$ es un ideal propio en R.*

2) *Demuestre que existe un ideal maximal $\mathfrak{m} \subset R$ tal que $\frac{x}{1} \neq \frac{0}{1}$ en la localización $R_{\mathfrak{m}}$.*

Anillos locales

Ejercicio 12.22. *Sea R un anillo local y sea $\mathfrak{m}$ su único ideal maximal. Demuestre que para cualquier $x \in R$ se cumple $x \in R^\times$ o $1 - x \in R^\times$.*

Ejercicio 12.23. *Demuestre que un anillo es local si y solo si todos los elementos no invertibles en R forman un ideal.*

Ejercicio 12.24. *Sea k un cuerpo.*

1) *Demuestre que el anillo de series formales $k[\![X]\!]$ es local y su ideal maximal es (X).*
   Indicación: véase el ejercicio anterior.

2) *Demuestre que si R es un anillo local con ideal maximal $\mathfrak{m}$, entonces $R[\![X]\!]$ es también local con ideal maximal $\mathfrak{m} + (X)$.*

3) *Use la parte anterior para probar que $k[\![X_1, \ldots, X_n]\!]$ es local y su ideal maximal es $(X_1, \ldots, X_n)$.*

Ejercicio 12.25. *Demuestre que si R es un anillo local, entonces el cociente R/I por cualquier ideal $I \subsetneq R$ es también un anillo local.*

Ejercicio 12.26.

1) *Demuestre que para cualquier cuerpo k el anillo de polinomios $k[X]$ no es local.*

2) *Demuestre que el anillo de series de potencias $\mathbb{Z}[\![X]\!]$ no es local.*

Anillos noetherianos

Ejercicio 12.27. *Sea R un anillo conmutativo noetheriano y $U \subseteq R$ un subconjunto multiplicativo. Demuestre que la localización $R[U^{-1}]$ es también un anillo noetheriano.*

Ejercicio 12.28. *Se dice que un anillo es* ***artiniano***[*] *si toda cadena* descendente *de ideales*

$$R \supseteq I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

se estabiliza. Note que $\mathbb{Z}$ es un anillo noetheriano, pero no es artiniano.

Ejercicio 12.29. *Sea X un subconjunto infinito de $\mathbb{N} \times \mathbb{N}$. Demuestre que en X hay un subconjunto infinito de pares (k_ℓ, d_ℓ) para $\ell = 0, 1, 2, 3, \ldots$ tal que*

$$k_0 \leq k_1 \leq k_2 \leq \cdots, \quad d_0 \leq d_1 \leq d_2 \leq \cdots$$

[*] Emil Artin (1898–1962), algebrista y teórico de números alemán.

Bibliografía

[AM1969] Michael Francis Atiyah and I. G. MacDonald, *Introduction to commutative algebra.*, Addison-Wesley-Longman, 1969.

[Eis2004] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Addison-Wesley-Longman, 2004.
http://dx.doi.org/10.1007/978-1-4612-5350-1

[Ful2008] William Fulton, *Algebraic curves. An introduction to algebraic geometry*, 2008.
http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[Rei1995] Miles Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, Cambridge University Press, 1995.
http://dx.doi.org/10.1017/CBO9781139172721

[Sha2001] Rodney Y. Sharp, *Steps in commutative algebra*, 2 ed., London Mathematical Society Student Texts, Cambridge University Press, 2001.
http://dx.doi.org/10.1017/CBO9780511623684