

Localización de $\mathbb{Z}/n\mathbb{Z}$

Alexey Beshenov (cadadr@gmail.com)

20 de septiembre de 2018

Consideremos el anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n donde

$$n = p_1^{k_1} \cdots p_s^{k_s}.$$

Los ideales maximales en $\mathbb{Z}/n\mathbb{Z}$ corresponden a los ideales maximales en \mathbb{Z} que contienen a (n) :

$$(n) \subseteq (p) \subseteq \mathbb{Z}.$$

Esto significa que $p \mid n$, así que los ideales maximales en $\mathbb{Z}/n\mathbb{Z}$ son precisamente

$$\mathfrak{m}_i := p_i\mathbb{Z}/n\mathbb{Z}, \text{ donde } i = 1, \dots, s.$$

Nuestro objetivo es calcular que

$$(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i} \cong \mathbb{Z}/p_i^{k_i}\mathbb{Z}.$$

Hay varios modos de hacerlo y aquí voy a presentar dos pruebas detalladas.

1 Propiedad universal de la localización

En general, para un anillo conmutativo R y un subconjunto multiplicativo $U \subseteq R$ el homomorfismo canónico de localización

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

satisface la siguiente propiedad universal.

1) Para todo $u \in U$ el elemento $\phi(u) = \frac{u}{1}$ es invertible en $R[U^{-1}]$.

Efectivamente, el inverso de $\frac{u}{1}$ es $\frac{1}{u}$.

2) Si $f: R \rightarrow S$ es otro homomorfismo de anillos tal que $f(u)$ es invertible en S para todo $u \in U$, entonces f se factoriza de modo único por ϕ : existe un homomorfismo único $\tilde{f}: R[U^{-1}] \rightarrow S$ tal que $f = \tilde{f} \circ \phi$.

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

Se ve que \tilde{f} necesariamente viene dado por $\frac{r}{u} \mapsto f(r) f(u)^{-1}$.

Esta propiedad universal caracteriza a $R[U^{-1}]$ de modo único salvo isomorfismo. De hecho, sea $\psi: R \rightarrow S$ otro homomorfismo de anillos que satisface la misma propiedad universal.

- 1) Para todo $u \in U$ el elemento $\psi(u)$ es invertible en S .
- 2) Si $f: R \rightarrow S'$ es otro homomorfismo de anillos tal que $f(u)$ es invertible en S' para todo $u \in U$, entonces f se factoriza de modo único por ψ .

$$\begin{array}{ccc} R & \xrightarrow{f} & S' \\ \psi \downarrow & \exists! \nearrow & \\ S & \xrightarrow{\tilde{f}} & \end{array}$$

Se ve que \tilde{f} necesariamente viene dado por $\frac{r}{u} \mapsto f(r) f(u)^{-1}$.

En este caso podemos aplicar la propiedad universal de ϕ a ψ

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \phi \downarrow & \exists! \nearrow & \\ R[U^{-1}] & \xrightarrow{\tilde{\psi}} & \end{array}$$

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

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R[U^{-1}] \\ \psi \downarrow & \exists! \nearrow & \\ S & \xrightarrow{\tilde{\phi}} & \end{array}$$

De esta manera se obtienen homomorfismos de anillos

$$\tilde{\phi}: R[U^{-1}] \rightarrow S, \quad \tilde{\psi}: S \rightarrow R[U^{-1}], \quad \psi = \tilde{\psi} \circ \phi, \quad \phi = \tilde{\phi} \circ \psi.$$

Ahora tenemos

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

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

$$\tilde{\psi} \circ \tilde{\phi} = \text{id}_S.$$

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

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

Podemos concluir que los homomorfismos $\tilde{\phi}$ y $\tilde{\psi}$ son mutuamente inversos y definen un isomorfismo

$$S \cong R[U^{-1}].$$

2 Primer cálculo de $(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i}$

Tenemos un homomorfismo canónico

$$\begin{aligned}\phi: \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/p_i^{k_i}\mathbb{Z}, \\ [x]_n &\mapsto [x]_{p_i^{k_i}}.\end{aligned}$$

Para probar que $(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i} \cong \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ bastaría probar que ϕ satisface la propiedad universal de la localización. Aquí estamos localizando respecto al conjunto $U := (\mathbb{Z}/n\mathbb{Z}) \setminus \mathfrak{m}_i$ que consiste en los elementos $[u]_n$ tales que $p_i \nmid u$.

Si $p_i \nmid x$, entonces x es invertible módulo $p_i^{k_i}$, y esto demuestra que $\phi([u]_n) \in (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ para todo $[u]_n \in U$.

Ahora supongamos que $f: \mathbb{Z}/n\mathbb{Z} \rightarrow S$ es un homomorfismo de anillos tal que $f([u]_n)$ es invertible en S para todo $[u]_n \in U$. Consideremos la identidad

$$[p_1]_n^{k_1} \cdots [p_i]_n^{k_i} \cdots [p_s]_n^{k_s} = [n]_n = [0]_n.$$

Al aplicar f , nos queda

$$f([p_1]_n)^{k_1} \cdots f([p_i]_n)^{k_i} \cdots f([p_s]_n)^{k_s} = 0_S.$$

Aquí $[p_j]_n \in U$ para todo $j \neq i$, así que $f([p_j]_n)$ son invertibles en S y al multiplicar la última identidad por los inversos nos queda

$$f([p_i]_n^{k_i}) = 0_S,$$

y por lo tanto

$$p_i^{k_i}\mathbb{Z}/n\mathbb{Z} \subseteq \ker f.$$

Esto implica que f se factoriza de modo único por el cociente de $\mathbb{Z}/n\mathbb{Z}$ por $p_i^{k_i}\mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{ccc}\mathbb{Z}/n\mathbb{Z} & \xrightarrow{f} & S \\ \downarrow & \nearrow \exists! & \\ \frac{\mathbb{Z}/n\mathbb{Z}}{p_i^{k_i}\mathbb{Z}/n\mathbb{Z}} & & \end{array}$$

Sin embargo, el tercer teorema de isomorfía nos dice que

$$\frac{\mathbb{Z}/n\mathbb{Z}}{p_i^{k_i}\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/p_i^{k_i}\mathbb{Z},$$

y respecto a esta identificación la flecha vertical en el diagrama coincide con ϕ . Podemos concluir que ϕ satisface la propiedad universal de la localización $(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i}$.

3 Segundo cálculo de $(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i}$

Para cualquier ideal $I \subseteq R$ hay un isomorfismo natural

$$R[U^{-1}]/IR[U^{-1}] \cong (R/I)[\bar{U}^{-1}],$$

donde $IR[U^{-1}]$ es el ideal en $R[\bar{U}^{-1}]$ generado por los elementos $\frac{x}{\bar{u}}$, $x \in I$ y el conjunto \bar{U} es la reducción de U módulo I .

Apliquemos este resultado a nuestra situación particular. Estamos localizando $\mathbb{Z}/n\mathbb{Z}$ en el conjunto $\bar{U} := (\mathbb{Z}/n\mathbb{Z}) \setminus \mathfrak{m}_i$, donde $\mathfrak{m}_i := p_i\mathbb{Z}/n\mathbb{Z}$. Pero esto es la reducción módulo n del conjunto $U := \mathbb{Z} \setminus (p_i)$. Entonces,

$$(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i} \cong \mathbb{Z}_{(p_i)}/n\mathbb{Z}_{(p_i)},$$

donde

$$\mathbb{Z}_{(p_i)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p_i \nmid b \right\} \subset \mathbb{Q}.$$

Hagamos un par de observaciones básicas.

Observación 1. Sea R un anillo conmutativo y $x \in R$. Si $u \in R^\times$ es un elemento invertible, entonces $(x) = (ux)$. *Demostración.* En efecto, tenemos $ux \in (x)$, así que $(ux) \subseteq (x)$. Viceversa, puesto que u es invertible, podemos escribir $x = u^{-1}ux \in (ux)$, así que $(x) \subseteq (ux)$. ■

Observación 2. Para todo primo p y $k = 1, 2, 3, \dots$ hay un isomorfismo $\mathbb{Z}_{(p)}/p^k\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^k\mathbb{Z}$.

Demostración. Definamos la aplicación

$$f: \mathbb{Z}_{(p)} \rightarrow \mathbb{Z}/p^k\mathbb{Z},$$

$$\frac{a}{b} \mapsto [a]_{p^k} \cdot [b]_{p^k}^{-1}.$$

Los elementos de $\mathbb{Z}_{(p)}$ son las fracciones $\frac{a}{b}$ donde $p \nmid b$, así que b tiene inverso módulo p^k y se ve que la aplicación está bien definida:

$$\frac{a}{b} = \frac{a'}{b'} \implies [a]_{p^k} \cdot [b]_{p^k}^{-1} = [a']_{p^k} \cdot [b']_{p^k}^{-1}.$$

Se comprueba fácilmente que f es un homomorfismo sobreyectivo de anillos y que su núcleo está generado por p^k . El primer teorema de isomorfía nos permite concluir que $\mathbb{Z}_{(p)}/p^k\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^k\mathbb{Z}$. ■

Volvamos a nuestro cálculo. Estamos tratando de identificar

$$(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i} \cong \mathbb{Z}_{(p_i)}/n\mathbb{Z}_{(p_i)} = \mathbb{Z}_{(p_i)}/p_1^{k_1} \cdots p_i^{k_i} \cdots p_s^{k_s}\mathbb{Z}_{(p_i)}.$$

Los números $p_j^{k_j}$ para $j \neq i$ son invertibles en $\mathbb{Z}_{(p_i)}$, así que la primera observación de arriba implica que $\mathbb{Z}_{(p_i)}/n\mathbb{Z}_{(p_i)} \cong \mathbb{Z}_{(p_i)}/p_i^{k_i}\mathbb{Z}_{(p_i)}$. La segunda observación nos dice que $\mathbb{Z}_{(p_i)}/p_i^{k_i}\mathbb{Z}_{(p_i)} \cong \mathbb{Z}/p_i^{k_i}\mathbb{Z}$.