Introducción esencial a la teoría de anillos

Álgebra homológica

10 de Enero de 2024

En este documento hacemos un resumen de las definiciones y resultados básicos de la teoría de anillos necesarios para un curso de álgebra homológica, sin demostraciones.

1 Elementos de la teoría de anillos conmutativos

Definición 1. Un **anillo** es un conjunto R con dos operaciones

$$+, \cdot \colon R \times R \to R$$

llamadas **suma** y **producto** que cumplen las siguientes propiedades.

1. $(R, +)$ es un grupo abeliano. Al elemento neutro lo denotamos 0.
2. El producto es asociativo.
3. El producto es distributivo respecto a la suma por ambos lados, es decir

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$c \cdot (a + b) = c \cdot a + c \cdot b$$

Cuando no haya lugar a confusión usaremos la concatenación de símbolos para denotar el producto, es decir $ab = a \cdot b$.

Definición 2. Se dice que un anillo es **conmutativo** si el producto es conmutativo.

Definición 3. Se dice que un anillo es **unitario** si existe un elemento neutro para el producto, el cual denotaremos mediante 1. También lo llamaremos un anillo con unidad.

La mayoría de los anillos que trataremos en este curso serán conmutativos, así que comenzamos con ejemplos de ellos.

Ejemplo 4. Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos con unidad con la suma y producto usual.

Ejemplo 5. Sea $n \geq 2$ entero. El conjunto $\mathbb{Z}/n$ es un anillo conmutativo con unidad con las operaciones dada por suma y producto de representantes, es decir:

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n \cdot [b]_n = [ab]_n$$

Ejemplo 6. Sea R un anillo conmutativo con unidad. El anillo de polinomios con coeficientes en R y variables $\{X_j\}_{j\in J}$ es el conjunto $R[X_j]_{j\in J}$ de sumas finitas

$$\sum r^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} X^{i_1}_{j_1} \ldots X^{i_n}_{j_n}$$

donde $i_k \in \mathbb{N}$, $j_k \in J$ y $r^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} \in R$. Debemos pensar que si $i_k = 0$, entonces X_{j_k} no aparece en ese monomio. Por ejemplo, el coeficiente $r^{1,3,0}_{j_1,j_2,j_3}$ de $X^1_{j_1} X^3_{j_2} X^0_{j_3}$ no es más que el coeficiente $r^{1,3}_{j_1,j_2}$.

También podemos pensar que en estas sumas aparecen todos los posibles monomios, pero que solo un número finito de ellos tienen coeficiente no nulo. La suma y el producto están definidos de la siguiente manera:

$$\sum r^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} X^{i_1}_{j_1} \ldots X^{i_n}_{j_n} + \sum s^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} X^{i_1}_{j_1} \ldots X^{i_n}_{j_n} = \sum (r^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} + s^{i_1,\ldots,i_n}_{j_1,\ldots,j_n}) X^{i_1}_{j_1} \ldots X^{i_n}_{j_n}$$

$$\left(\sum r^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} X^{i_1}_{j_1} \ldots X^{i_n}_{j_n}\right) \cdot \left(\sum s^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} X^{i_1}_{j_1} \ldots X^{i_n}_{j_n}\right) = \sum t^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} X^{i_1}_{j_1} \ldots X^{i_n}_{j_n}$$

donde

$$t^{i_1,\ldots,i_n}_{j_1,\ldots,j_n} = \sum r^{a_1,\ldots,a_n}_{j_1,\ldots,j_n} s^{b_1,\ldots,b_n}_{j_1,\ldots,j_n}$$

y la suma corre sobre las parejas de tuplas $[(a_1,\ldots,a_n),(b_1,\ldots,b_n)]$ tales que $a_k + b_k = i_k$ para todo k. Estas tuplas pueden incluir ceros.

Algunos autores piden que en un anillo R conmutativo con unidad se cumpla $1 \neq 0$. Esto se hace nada más para evitar el anillo $\{0\}$ pues si $1 = 0$ y $r \in R$, entonces

$$r = r \cdot 1 = r \cdot 0 = r \cdot (0+0) = r \cdot 0 + r \cdot 0 = r \cdot 1 + r \cdot 1 = r + r$$

de donde $r = 0$.

Definición 7. Sea R un anillo con unidad y $r \in R$. Se dice que r es

- **Invertible por la izquierda** si existe $s \in R$ tal que $sr = 1$.
- **Invertible por la derecha** si existe $s \in R$ tal que $rs = 1$.
- **Invertible** si es invertible por la izquierda y por la derecha. También se dice que es una **unidad**.
- **Un divisor de cero por la izquierda** si $r \neq 0$ y existe $s \in R - \{0\}$ tal que $rs = 0$.

- **Un divisor de cero por la derecha** si $r \neq 0$ existe $s \in R - \{0\}$ tal que $sr = 0$.
- **Un divisor de cero** si es divisor de cero por alguno de los dos lados.
- **Nilpotente** si $r^n = 0$ para algún $n \in \mathbb{N}^{>0}$.

Las unidades de R forman un grupo que se denota $R^\times$. Con estos elementos especiales podemos definir algunos anillos que se comportan de manera bastante agradable.

Definición 8. Se dice que un anillo conmutativo con unidad R es un

- **Campo** si $1 \neq 0$ y cualquier elemento de $R - \{0\}$ es invertible.
- **Dominio entero** si $1 \neq 0$ y no tiene divisores de cero.

Definición 9. Sea R un anillo con unidad y $S \subseteq R$. Se dice que S es un subanillo si es un subgrupo de R que contiene al elemento unidad y que es cerrado bajo el producto de R. Denotamos $S \leq R$.

También se pueden considerar subanillos de anillos sin unidad, en cuyo caso no se le pide que contenga al elemento unidad. Incluso se pueden considerar subanillos sin unidad de anillos con unidad, pero esta generalidad no será necesaria para nosotros.

Definición 10. Sea R un anillo. Se dice que un subgrupo J de R es un

- **Ideal izquierdo** si para cada $r \in R$ y $x \in J$, se tiene $rx \in J$.
- **Ideal derecho** si para cada $r \in R$ y $x \in J$, se tiene $xr \in J$.
- **Ideal bilateral** si es un ideal izquierdo y derecho a la vez. También se le conoce simplemente como **ideal**.

Se denote $J \lhd_l R$, $J \lhd_r R$ y $J \lhd R$, respectivamente.

Ejemplo 11. $\{0\}$ siempre es un ideal bilateral de R, pero no es un subanillo a menos que $R = \{0\}$. También R es siempre un ideal bilateral de R, y un subanillo.

Ejemplo 12. Si n es un entero positivo mayor que uno, entonces $n\mathbb{Z}$ es un ideal bilateral de $\mathbb{Z}$.

Ejemplo 13. Si $a \in R$, entonces

$$\{p(X) \in R[X] \mid p(a) = 0\}$$

es un ideal bilateral de $R[X]$.

Algunas propiedades útiles de los ideales son las siguientes.

1. Si I es un ideal izquierdo (o derecho) que contiene algún elemento invertible de R, entonces $I = R$.

2. Un anillo conmutativo con unidad R es un campo si y solo si sus únicos ideales bilaterales son R y $\{0\}$.

3. Si $\{I_j\}_{j\in J}$ es una familia de ideales (izquierdos, derechos, bilaterales) de R, entonces $\bigcap_{j\in J} I_j$ es un ideal (izquierdo, derecho, bilateral) de R.

La última propiedad nos permite definir el ideal (izquierdo, derecho, bilateral) generado por un subconjunto X de R. Es simplemente la intersección de todos los ideales (izquierdos, derechos, bilaterales) de R que contienen a X. Lo denotamos mediante (X) y también se puede dar una descripción más explícita cuando R es un anillo conmutativo con unidad:

$$(X) = \left\{ \sum_{\text{finitas}} r_j x_j \,\middle|\, r_j \in R, x_j \in X \right\}$$

Definición 14. Un **ideal principal** es un ideal (izquierdo, derecho, bilateral) generado por un único elemento de R.

Si x es el elemento de R, usaremos la notación Rx, xR ó RxR para el ideal principal (izquierdo, derecho, bilateral) generado por x.

Definición 15. Sea I un ideal de un anillo conmutativo con unidad R. El anillo cociente R/I es el grupo cociente R/I con el producto

$$(a + I)(b + I) = ab + I$$

El anillo cociente vuelve a ser un anillo conmutativo con unidad.

Definición 16. Sean R, S anillos. Una función $f\colon R \to S$ es un **homomorfismo de anillos** si es un homomorfismo de grupos y satisface $f(rr') = f(r)f(r')$. Si R y S son anillos con unidad, también se requiere que $f(1) = 1$. Un **isomorfismo de anillos** es un homomorfismo de anillos biyectivo, equivalentemente si tiene una inversa que es un homomorfismo de anillos.

Al igual que en homomorfismos de grupos, podemos definir el núcleo e imagen de un homomorfismo de anillos $f\colon R \to S$.

$$\operatorname{Ker}(f) = \{r \in R \mid f(r) = 0\}$$
$$\operatorname{Im}(f) = \{f(r) \in S \mid r \in R\}$$

Es fácil comprobar que $\operatorname{Ker}(f)$ es un ideal bilateral de R y $\operatorname{Im}(f)$ es un subanillo de S. Al igual que en teoría de grupos (ya que los anillos son grupos abelianos y los homomorfismos de anillos en particular son homomorfismos de grupos), un homomorfismo es inyectivo si y solo si su núcleo es igual a $\{0\}$.

Ejemplo 17. Sea $a \in R$ y consideremos el mapeo de evaluación

$$\begin{aligned} \mathrm{ev}_a \colon R[X] &\to R \\ p(X) &\mapsto p(a) \end{aligned}$$

Es un homomorfismo de anillos.

Ejemplo 18. Si J es un ideal bilateral de R, hay un homomorfismo

$$\begin{aligned} \pi \colon R &\to R/J \\ r &\mapsto r + J \end{aligned}$$

llamado el **homomorfismo cociente**. Por ejemplo, si tomamos $R = \mathbb{Z}$ y $J = n\mathbb{Z}$, este cociente $\mathbb{Z} \to \mathbb{Z}/n$ es el morfismo de reducción módulo n.

Teorema 19 (Propiedad universal del homomorfismo cociente)**.** *Sea $f \colon R \to S$ un homomorfismo de anillos conmutativos con unidad y sea I un ideal de R que está contenido en $Ker(f)$. Entonces existe un único homomorfismo de anillos $F \colon R/I \to S$ tal que $F\pi = f$.*

Aunque no incluiré la demostración aquí, consiste en probar que $F(r + I) = f(r)$ define un homomorfismo que cumple esas propiedades.

Teorema 20 (Primer teorema de isomorfismo)**.** *Si $f \colon R \to S$ es un homomorfismo de anillos conmutativos con unidad, hay un isomorfismo de anillos*

$$R/Ker(f) \cong Im(f)$$

Teorema 21 (Segundo teorema de isomorfismo)**.** *Si S es un subanillo de un anillo conmutativo con unidad R y J es un ideal de R, entonces $J \cap S$ es un ideal de S y hay un isomorfismo de anillos*

$$\frac{S + J}{J} \cong \frac{S}{S \cap J}$$

Teorema 22 (Tercer teorema de isomorfismo)**.** *Dados ideales I, J de un anillo conmutativo con unidad R con $I \subseteq J$, se tiene que J/I es un ideal de R/I y hay un isomorfismo de anillos*

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

Teorema 23 (Teorema de la correspondencia)**.** *Si R es un anillo conmutativo con unidad, hay dos correspondencias biyectivas que preservan el orden dado por contención.*

$$\{\textit{Subanillos de } R/I\} \cong \{\textit{Subanillos de } R \textit{ que contienen a } I\}$$

$$\{\textit{Ideales de } R/I\} \cong \{\textit{Ideales de } R \textit{ que contienen a } I\}$$

El siguiente resultado nos permite tener una manera de escribir cualquier anillo conmutativo con unidad en términos de anillos de polinomios que son más concretos y conocemos mejor.

Teorema 24. *Sea R un anillo conmutativo con unidad. Existe una familia de variables $\{X_j\}_{j\in J}$ y un ideal I de $\mathbb{Z}[X_j]_{j\in J}$ tal que*

$$\frac{\mathbb{Z}[X_j]_{j\in J}}{I} \cong R$$

Idea de la demostración: Sea $J = R - \{0\}$ y consideremos el único homomorfismo de anillos que satisface

$$\begin{aligned} f\colon \mathbb{Z}[X_j]_{j\in J} &\to R \\ X_j &\mapsto j \end{aligned}$$

Es claro que f es sobreyectiva, así que por el primer teorema de isomorfismo se tiene

$$\frac{\mathbb{Z}[X_j]_{j\in J}}{\mathrm{Ker}(f)} \cong R$$

□

Este isomorfismo se conoce como una **presentación** de R. En lugar de $J = R - \{0\}$ también podríamos haber tomado un conjunto de generadores multiplicativos de R, es decir un subconjunto X que cumpla que cualquier elemento de R se puede expresar como una suma finita de productos finitos de elementos de X. Esto daría lugar a una presentación más sencilla de R.

Sea R un dominio entero. Consideremos

$$F = R \times (R - \{0\}/\sim$$

donde

$$(a, b) \sim (c, d) \qquad \text{si } ad = bc$$

Es fácil comprobar que esto define una relación de equivalencia y denotamos

$$\frac{a}{b} = [(a, b)]$$

Definimos

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

Con estas operaciones F es un campo que contiene el subanillo

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

el cual es isomorfo a R mediante el isomorfismo que envía r a $\frac{r}{1}$. Identificamos r con $r/1$ para ver a R dentro de F. A F se le conoce como el **campo de fracciones** de R.

Ejemplo 25. El campo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.

Teorema 26 (Propiedad universal del campo de fracciones)**.** *Sea $\iota\colon R \to F$ la inclusión de un dominio entero en su campo de fracciones y sea $h\colon R \to S$ un homomorfismo de anillos que envía $R - \{0\}$ dentro de $S^\times$. Entonces existe un único homomorfismo de anillos $H\colon F \to S$ tal que $H\iota = h$.*

2 Anillos no conmutativos

En esta sección damos algunos ejemplos de anillos no conmutativos.

Ejemplo 27. El conjunto $\mathbb{H}$ de cuaterniones es un anillo con unidad que no es conmutativo.

Ejemplo 28. Si R es un anillo conmutativo con unidad, el conjunto $M_{n\times n}(R)$ de matrices cuadradas con n filas y entradas en R forman un anillo con unidad, que no necesariamente es conmutativo.

Ejemplo 29. Sea R un anillo conmutativo con unidad. El anillo de polinomios con coeficientes en R y variables $\{X_j\}_{j\in J}$ que no conmutan es el conjunto $R\langle X_j\rangle_{j\in J}$ de sumas finitas

$$\sum r_{j_1,\ldots,j_n}^{i_1,\ldots,i_n} X_{j_1}^{i_1}\ldots X_{j_n}^{i_n}$$

donde $i_k \in \mathbb{N}$, $j_k \in J$ y $r_{j_1,\ldots,j_n}^{i_1,\ldots,i_n} \in R$. La suma y el producto están definidos de manera similar al caso de variables que conmutan, solo que no agrupamos las potencias de una misma variables a menos que estén contiguas. Por ejemplo $X_1X_2X_1$ es diferente de $X_1^2X_2$. La importancia de estos anillos es que cualquier anillo con unidad es isomorfo a un cociente de un anillo de la forma $\mathbb{Z}\langle X_j\rangle_{j\in J}$.

Ejemplo 30. Sea G un grupo y R un anillo conmutativo con unidad. El anillo de grupo de G con coeficientes en R es el conjunto RG de sumas finitas

$$\sum r_g g$$

donde $g \in G$ y $r_g \in R$. La suma y el producto están definidas mediante

$$\sum r_g g + \sum s_g g = \sum (r_g + s_g) g$$

$$\left(\sum r_g g\right)\left(\sum s_g g\right) = \sum_{g\in G}\left(\sum_{h\in G} r_h s_{h^{-1}g}\right) g$$

Este anillo será conmutativo si y solo si G es conmutativo.