Ideales y Divisibilidad

Ana Ofelia Negrete Fernández

18 de julio 2021

1. Introducción

Ya se mencionó en una anterior entrada, que $\mathbb{Z}$ es un dominio entero. O lo que es mismo, es un *anillo conmutativo con unitario sin divisores de cero.* Los dominios enteros son estructuras algebraicas que generalizan ciertas "propiedades de divisibilidad" que observamos tienen los enteros, y algo similar va a suceder con los ideales. Digamos entonces que un dominio entero será un espacio donde trabajar, dotado con ciertas operaciones y propiedades, mientras que los ideales serán elementos que ahí vivan, subconjuntos del dominio entero, pero que cumplan unas condiciones adicionales a las de ser subanillos de un anillo (un dominio entero es un anillo). Habrán clasificaciones para ideales, destacándose los **ideales principales**, **ideales primos** e **ideales maximales**. Por ejemplo, los ideales primos en $\mathbb{Z}$ serán los subconjuntos de $\mathbb{Z}$ que sean múltiplos de un número primo dado. Es decir, son de la forma $p\mathbb{Z}$.

En la materia de Álgebra Moderna I del quinto semestre de la carrera de matemáticas se estudian los grupos, y se ve que en los enteros se pueden hallar tanto grupos, como subgrupos, subgrupos cíclicos, subgrupos normales o subgrupos factores. Se ven otros tipos de grupos, y además los "teoremas de isomorfismos en grupos". Ya un estudio riguroso de los anillos y por ende, también de los ideales, se da en Álgebra Moderna II. Para los anillos también existirán teoremas de isomorfismos y se podrá hacer la analogía de que los subgrupos normales de un grupo serán lo que los ideales a un anillo. Y así como, dado un subgrupo normal H de un grupo G se puede construir el "grupo cociente G/H", también sucederá que, dado un ideal I de un anillo R será posible construir el "anillo cociente R/I".

Este texto sólo planea ser una breve introducción al concepto de ideal, y aquí sería apropiado pensar en que $\mathbb{Z}$ es un anillo (más aún un dominio entero, y más aún, un dominio de ideales principales) y algunos de sus subconjuntos son ideales.

Intuitivamente sabemos que un entero n siempre se podrá expresar como producto de potencias de números primos y esta factorización es única (se demostrará pronto). Por ejemplo, $150 = (3 \cdot 2) \cdot 5^2$. Así, si quisieramos saber en qué ideal de $\mathbb{Z}$ vive el número 150, basta observar su factorización en primos. Tenemos que $150 \in 2\mathbb{Z}$, también $150 \in 3\mathbb{Z}$ y $150 \in 5\mathbb{Z}$.

A algunos polinomios $K[x]$, con coeficientes en un campo K, se les podrá factorizar como un producto de polinomios irreducibles en $K[x]$, donde la suma de los grados de estos polinomios sea menor al grado del polinomio inicial. Diremos que esos factores serán los ideales primos del anillo.

Y análogamente, en las extensiones cuadráticas, es decir anillos de la forma $Q[\sqrt{D}]$, también podremos hablar de los ideales, ideales primos e ideales maximales que ahí viven. Esa es la necesidad de extender la "divisibilidad" a algo más abstracto que los números enteros, pero la noción de dominio entero tiene sus raíces en cómo se comporta $\mathbb{Z}$.

Así que, lo que aquí sea tal vez mejor, será ir dando las definiciones de ciertas estructuras algebraicas relacionadas con los ideales, yendo desde lo más simple hasta lo más complicado, y hasta llegar a lo que queremos.

2. Resumen de estructuras algebraicas y motivación para la definición de ideal

Primero digamos qué son una operación binaria, un semigrupo, un monoide y un grupo:

Definición (Operación binaria). Sea A un conjunto no vacío. Una operación binaria $\star$ en A, es una función del producto cartesiano $A \times A$ en A. Se denota

$$\star : A \times A \longrightarrow A.$$

Definición (Semigrupo). Decimos que la operación $\star : A \times A \longrightarrow A$ es asociativa si

$$x \star (y \star z) = (x \star y) \star z, \ \ \forall \ x, y \in A.$$

Definición (Monoide). Una terna $(A, \star, e)$ es un monoide, si $(A, \star)$ es semigrupo y e es neutro para $\star$.

En otras palabras, un monoide es un semigrupo en el que existe un elemento neutro.

Luego, a un grupo le pediremos aún más cosas. Será un semigrupo, pues cumplirá la asociatividad. Será un monoide, pues existirá un elemento neutro. La cerradura también la cumplirá (eso se hereda de que la operación $\star$ sea binaria). Y además de esto, pediremos que en un grupo existan elementos inversos:

Definición (Grupo). Un grupo es un conjunto no vacío G, en donde hay definida una operación binaria $\star$, que satisface:

1. $a \star b \in G \quad \forall \ a, b \in G.$ (cerradura)
2. $a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in G.$ (asociatividad)
3. $\exists \ e \in G$ tal que $a \star e = e \star a = a \quad \forall \ a \in G.$ (existencia del neutro)
4. $\forall \ a \in G, \ \exists \ a^{-1} \in G$ tal que $a \star a^{-1} = a^{-1} \star a = e.$ (existencia de inversos)

Ejemplo. $(\mathbb{Z}, \widehat{+})$ es un grupo. Es decir, cumple la definición de ser grupo, y más aún, cumple la propiedad de ser un **grupo conmutativo o abeliano:** $a \star b = b \star a \ \ \forall \ a, b \in G$.

Sin embargo, grupos hay muchos, como S_n el grupo de las permutaciones, D_n el grupo diédrico, Q el grupo de los cuaterniones, $\mu_{\mathbb{C}}$ el grupo de las transformaciones de Möbius, $PSL(2, \mathbb{C})$ el grupo de matrices complejas 2×2 con determinante módulo 1, Γ el grupo kleiniano, entre otros. De tal modo que $(\mathbb{Z}, \widehat{+})$, dentro de la teoría de grupos, simplemente será un caso particular de grupo.

Pero ya que estamos estudiando a los enteros, por ahora nos interesa centrar nuestra atención en $(\mathbb{Z}, \widehat{+})$, y también en $(\mathbb{Z}_n, \widehat{+})$ el grupo de los enteros módulo n. Y quizá también en alguna otra estructura numérica que involucre a los números enteros, como pudieran ser $Z[i]$ los enteros gaussianos, $\mathbb{Z}[x]$ los polinomios de coeficientes enteros o alguna otra cosa por el estilo.

Ahora veamos lo que es un subgrupo.

Definición (Subgrupo). Un subgrupo S de un grupo G es un subconjunto de G que también es grupo.

Ejemplos. $\mathbb{Z}$ es un subgrupo de sí mismo. También $\{\overline{0}\} \subseteq \mathbb{Z}$, es subgrupo de $\mathbb{Z}$. Y en realidad, todos los subgrupos de $\mathbb{Z}$ son de la forma:

$$\langle n \rangle := \{n\mathbb{Z} : n \in \mathbb{Z}\}.$$

Observamos que $n\mathbb{Z}$ se refiere a los múltiplos de algún n. De modo que, para $n = 0$, tenemos que $\langle 0 \rangle = \overline{0}$; para $n = 1$, se tiene $\langle 1 \rangle = 1 \cdot \mathbb{Z} = \mathbb{Z}$; para $n = 2$, $\langle 2 \rangle = 2\mathbb{Z}$ los enteros pares; para $n = 3$,

$\langle 3 \rangle = 3\mathbb{Z}$ los enteros múltiplos de 3, y así sucesivamente. Además de, por supuesto, la operación que acompaña a estos subgrupos es la suma.

Demostremos que

Teorema 1. Todos los subgrupos de $\mathbb{Z}$ son de la forma

$$\langle n \rangle := \{n\mathbb{Z} : n \in \mathbb{Z}\}.$$

Dem.- Sea H un subgrupo de $\mathbb{Z}$.

Si $H = 0$, entonces $0 \in \mathbb{Z}$ lo genera.

Así, sea H un subgrupo distinto del trivial. Como H es subgrupo, para todo elemento n en H, su inverso $-n$ también estará en H, y alguno ellos será positivo. Así aseguramos que existe $n \in H$ estrictamente positivo.

Observamos que $\{n\mathbb{Z} : n \in \mathbb{Z}\} \neq \emptyset$, pues $n \cdot 1$ está ahí. Y por el principio del buen orden, podemos tomar n el mínimo elemento positivo de este conjunto.

Ahora elijamos b un elemento arbitrario de H. Por el algoritmo de la división sabemos que podemos escribir $b = nq + r$, con $q, r \in \mathbb{Z}$, y tales que $0 \leq r < n$. Ya que $b \in H$ y $n \in H$, sabemos que $r = b - nq \in H$, por ser la operación cerrada en H. Como $0 \leq r < n$ y n es el mínimo elemento positivo de H, forzosamente $r = 0$. Así, $b = nq$. Esto demuestra que cualquier elemento de H es de la forma nq, con $q \in \mathbb{Z}$. Por lo tanto, cualquier subgrupo de $\mathbb{Z}$ es un $n\mathbb{Z}$.

□

Como veremos unos párrafos más abajo, la notación $\langle n \rangle$ indica que sólo se necesitará un único elemento en $\mathbb{Z}$ para generar todo un subgrupo de $\mathbb{Z}$.

Ahora veamos lo que es un subgrupo normal, más un teorema para caracterizar a los subgrupos normales de un grupo abeliano:

Definición (Subgrupo normal). Sea G un grupo. Uns subgrupo H de G se llama subgrupo normal de G, denotado $H \trianglelefteq G$, si $aH = Ha$.

Teorema 2. Sean G un grupo abeliano y $H \leq G$. Entonces $H \trianglelefteq G$.

No demostraremos el teorema 2 aquí, pero de él podemos concluir que, ya que $(\mathbb{Z}, \widehat{+})$ es grupo abeliano, entonces todos los subgrupos de $\mathbb{Z}$ son subgrupos normales.

Como ejercicio moral, piensa en si, para toda $n \in \mathbb{Z}$, se tiene que $(\mathbb{Z}_n, \widehat{+})$ es grupo e intenta encontrar los subgrupos y subgrupos normales de aquéllos $\mathbb{Z}_n$ que sí sean grupos. Esto tal vez pueda ser complicado, a falta de aún no haber estudiado rigurosamente los grupos aún, incluído dar más definiciones, teoremas y demostraciones, pero la respuesta a la pregunta es muy sencilla.

Al definir un grupo nada más necesitamos un conjunto y una sola operación. Para decir lo que es un anillo, ya requeriremos un conjunto A con DOS operaciones:

Definición (Anillo). Un anillo es una quinteta $(A, +, *, 0, 1)$ tal que:

1. $(A, +, 0)$ es un grupo conmutativo.
2. $(A, *, 1)$ es un monoide.
3. $*$ se distribuye sobre $+$, por ambos lados. Es decir:

$$a * (b + c) = (a * b) + (a * c), \quad \forall\ a, b, c \in A.$$
$$(b + c) * a = (b * a) + (c * a), \quad \forall\ a, b, c \in A.$$

Podemos abreviar la notación de anillo a $(A, +, *)$. Se entiende que hay un neutro para cada una de las operaciones $+$ y $*$, que son el 0 y 1, respectivamente. A veces esos no son los símbolos que denotan a los neutros. Se puede usar un e y un u, o cualquier otro símbolo que parezca apropiado, y por lo cual no hay que casarse con una notación, incluidos los símbolos que refieren a las operaciones. Coloquialmente se dice que un anillo posee una operación de suma y producto de sus elementos. Así, en la notación $(A, +, *)$, el símbolo $+$ se está refiriendo a "la suma", mientras que $*$ es el "producto".

Ejemplo. $(\mathbb{Z}_n, \widehat{+}, *)$ es un anillo.

Ejemplo. El conjunto $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ de los números complejos, con su suma y producto usual es un anillo.

Ejemplo. $\mathbb{Z}[i] \subset \mathbb{C}$, el conjunto de los **enteros gaussianos**, definido por

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\},$$

es un anillo con la suma y producto usuales para números complejos.

Más aún diremos que $\mathbb{Z}[i]$ es un subanillo de $\mathbb{C}$. Pues un subanillo es un subconjunto de un anillo, que también es anillo. O equivalentemente, un criterio para verificar que algo es subanillo será:

Definición (Subanillo). Sean $(A, +, *)$ anillo y $S \subseteq A$. Diremos que S es subanillo de A si para cualesquiera $a, b \in S$ se cumplen las siguientes condiciones:

1. $a + (-b) \in S$, y
2. $a * b \in S$.

Y de aquí vamos a decir que, dependiendo de qué propiedades adicionales a la de ser anillo existan en una estructura algabraica dada, podremos clasificarlos así:

A un anillo $(A, +, *)$ se le llama:

- **Anillo conmutativo**, si la operación $*$ es conmutativa.
- **Dominio entero** si $(A\backslash\{0\}, *)$ es un monoide donde vale la ley de cancelación.
- **Anillo con división** si $(A\backslash\{0\}, *, 1)$ es un grupo.
- **Campo**, si $(A\backslash\{0\}, *, 1)$ es un grupo abeliano.

Notamos entonces que pudieran haber anillos conmutativos que no fueran dominios enteros o dominios enteros que no fueran anillos conmutativos. Que pudieran haber anillos con división que no fueran dominios enteros y viceversa, que todo campo es dominio entero pero no todo dominio entero es campo, etc.

También observamos que decir que un dominio entero es un monoide con ley de la cancelación, es totalmente equivalente a la definición de un dominio entero como un anillo conmitativo con unitario sin divisores de cero.

Un ejemplo de un dominio entero que no es anillo con división es $(\mathbb{Z}, \widehat{+}, *)$, pues $\mathbb{Z}$ con el producto no es grupo. Y mucho menos puede ser grupo abeliano con el producto, por lo que $(\mathbb{Z}, \widehat{+}, *)$ **no es** campo.

Un ejemplo de un campo es $\mathbb{Z}_n$ para n un número entero primo. y se puede demostrar el siguiente teorema:

Teorema 3. $\mathbb{Z}_n$ es campo si y sólo si n es primo.

3. Definición de ideal y ejemplos

Para definir los ideales, habremos de méncionar qué es un ideal por la derecha y un ideal por la izquierda. Luego, un **ideal** será un subanillo que es ideal por la derecha y por la izquierda:

Definición (Ideal por la derecha). Dado un anillo A, un subanillo $I \subseteq A$ se llama un ideal por la derecha si $(I, +)$ es subgrupo aditivo, y para toda $r \in A$ y $x \in I$ se cumple que $xr \in I$.

Análogamente,

Definición (Ideal por la izquierda). Dado un anillo A, un subanillo $I \subseteq A$ se llama un ideal por la derecha si $(I, +)$ es subgrupo aditivo, y para toda $r \in R$ y $x \in I$ se cumple que $rx \in I$.

Así,

Definición (Ideal) Dado un anillo A, a un subanillo $I \subseteq A$ se llama un ideal si es ideal por la izquierda e ideal por la derecha.

Ejemplo. $3\mathbb{Z} = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$ es un ideal: Primero vemos que $3\mathbb{Z}$ es subgrupo de $\mathbb{Z}$ con la operación suma:

1. Ya que $3z + 3z' = 3(z + z')$, para $z, z' \in \mathbb{Z}$, sumar múltiplos de tres siempre es múltiplo de tres. Por lo que la suma es cerrada en $3\mathbb{Z}$.
2. La asociatividad también se tiene, pues se hereda de la de $\mathbb{Z}$.
3. El neutro, que es el 0, está en $3\mathbb{Z}$.
4. Como para todo número positivo en $3\mathbb{Z}$, se tiene que su negativo también está en el conjunto, podemos decir que existen inversos.

Y tomando cualquier $z, z' \in \mathbb{Z}$ se tendrá que $z(3z') = (3z')z = 3(zz')$. Es decir, multiplicar un elemento que estaba en $\mathbb{Z}$ por un elemento en $3\mathbb{Z}$, está en $3\mathbb{Z}$. Y esto pasa si la multiplicación se hace por la izquierda o la derecha. De este modo se concluye que $3\mathbb{Z}$ es un ideal.

Ejemplo. $\mathbb{Z}$ es subanillo de $\mathbb{Q}$. Pero $\mathbb{Z}$ **no es** ideal de $\mathbb{Q}$:

1. $\mathbb{Z} \subset \mathbb{Q}$, y sabemos que la suma es cerrada en $\mathbb{Z}$ al igual que la multiplicación. Además, $\mathbb{Z}$ es subgrupo con la operación suma. Es decir, tomar elementos $a, b, -b \in \mathbb{Z}$ y sumarlos o multiplicarlos arroja elementos en $\mathbb{Z}$. Por lo que $\mathbb{Z}$ es subanillo de $\mathbb{Q}$.
2. Tomando $\frac{1}{7} \in \mathbb{Q}$ y $3 \in \mathbb{Z}$, obtenemos que $\frac{3}{7} \notin \mathbb{Z}$. Por lo que $\mathbb{Z}$ no es ideal de $\mathbb{Q}$.

Definición (Ideal Principal). Sean A un anillo e $I \subset A$ un ideal. A I se le llama ideal principal, si existe $r \in A$ tal que $rA = I$.

Dicho de otro modo, un ideal es principal si puede ser generado por un sólo elemento del anillo; denotándose esto por $I = \langle a \rangle$.

Se podrá hacer la analogía de que un ideal principal es a un anillo, lo que un subgrupo cíclico es a un grupo, pues los grupos cíclicos también son generados por un único elemento y se usa la misma notación $\langle a \rangle$ para referirlos. Además, los subgrupos cíclicos de $\mathbb{Z}$ coinciden ser los ideales principales de $\mathbb{Z}$ y viceversa.

4. Resultados para ideales y divisibilidad

Ahora demostraremos que todos los ideales de $\mathbb{Z}$ son principales; es decir, todo ideal de $\mathbb{Z}$ puede generado por un único elemento.

Teorema 4. Todos los ideales de $\mathbb{Z}$ son ideales principales.

Dem.- En primer lugar, observamos que cualquier ideal de $\mathbb{Z}$ tiene que ser subgrupo con la operación suma. Ya sabemos por el teorema 1, que todos los subgrupos de $\mathbb{Z}$ son de la forma $\{n\mathbb{Z} : n \in \mathbb{Z}\}$. Lo que faltaría demostrar es que todos estos subgrupos cumplen la propiedad multiplicativa rI e Ir.

En segundo lugar, ya demostramos (o lo hiciste tú de tarea) que $\mathbb{Z}$ es un anillo conmutativo; es decir, la multiplicación conmuta. De esto se desprende que $rI = Ir$, para todo ideal $I \subset \mathbb{Z}$ y todo r elemento de $\mathbb{Z}$.

Sabiendo esto, demostremos que todo ideal en $\mathbb{Z}$ cumple la propiedad "de absorber la multiplicación", sin importar de qué lado se haga ésta.

Tomemos I un ideal de $\mathbb{Z}$.

Si $I = 0$, entonces 0 genera I; $0 \cdot 0 = \{0\}$. Este es el caso trivial.

Supongamos entonces que $I \neq 0$, y sea a el elemento positivo más pequeño en I.

Afirmamos que a genera I. Para demostrarlo, primero notamos que $\langle a \rangle \neq \emptyset$: ya que $\langle a \rangle = \{ar : r \in \mathbb{Z}\}$, y como I es ideal, $ar \in I$; y tomando $r = 1$, se obtiene lo que queremos, $a \in I$.

Ahora tomemos cualquier $b \in I$. Si $b = 0$, entonces $b = a \cdot 0$. Así, $b \in \langle a \rangle$.

Si $b \neq 0$, podemos suponer sin pérdida de generalidad, que $b > 0$. Entonces, usando el algoritmo de la división, sabemos que

$$b = aq + r.$$

Más aún, $0 \leq r < a$, con $q, r \in \mathbb{Z}$.

Así, $r = b - aq \in I$, ya que $a, b \in I$. Pero, como $r < a$ y a era el elemento más pequeño en I, concluimos $r = 0$.

De este modo, $b = aq \in I$. Hemos expresado cualquier $b \in I$ como un múltiplo de a. Es decir, $\langle a \rangle = I$, o lo que es mismo, a genera I.

□

Ya dijimos que los ideales son subgrupos aditivos, es decir, con la suma son un subgrupo de un anillo. Y en los subgrupos podíamos definir a las clases laterales de un grupo, también llamados "cosets de un grupo". Por ello podemos decir quiénes son los cosets de un ideal con respecto a la suma. Esto es:

Definición (Clases laterales de un ideal). Sean $I \subseteq R$ un ideal de un anillo R y $r \in R$. El coset asociado a R es

$$r + I := \{r + a : a \in I\}.$$

Ejemplo. Para los enteros módulo n, podemos identificar a $r + I$ con $\overline{r}$, la clase de equivalencia inducida por el residuo r. Por ejemplo, para $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, cada $n \in \mathbb{Z}_5$ es un entero de la forma $5q, 5q + 1, 5q + 2, 5q + 3$ o $5q + 4$, que pertenece a las clases $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ o $\overline{4}$, respectivamente.

Y podemos hacer aritmética con los cosets, de la manera en que establece el siguiente teorema:

Teorema 5. Sean R un anillo, $I \subseteq R$ un ideal, y $s, t \in R$. Entonces, para cualquier $s_1 \in s + I$ y $t_1 \in t + I$, tenemos:

- $s_1 + t_1 \in (s + t) + I$,
- $s_1 t_1 \in st + I$.

Dem.- Para verificar el primer inciso, tomemos $s_1 = s + i_1$ y $t_1 = t + i_2$, con $i_1, i_2 \in I$. De este modo, $s_1 + t_1 = (s + i_1) + (t + i_2)$. Podemos reordenar los téminos ya que la suma es conmutativa, y de que I es subanillo tenemos que $(i_1 + 1_2) \in I$. Así,

$$s_1 + t_1 = (s + t) + (i_1 + i_2) = (s + t) + I.$$

Para el segundo inciso, tomemos $s_1 = s + i_1$ y $t_1 = t + i_2$, con $i_1, i_2 \in I$. De este modo, $s_1 t_1 = (s+i_1)(t+i_2) = st + si_2 + i_1 t + i_1 i_2$. Como I es ideal por la izquierda, $si_2 \in I$. Como I es ideal por la derecha, $i_1 t \in I$, y sumar ambos es un elemento en I, por ser $(I, +)$ grupo. También $i_1 i_2 \in I$, por ser I subanillo. Así, $(si_2 + i_1 t) + (i_1 i_2) \in I$. De lo que se concluye que $s_1 t_1 = st + I$.

□

Corolario. Sea R un anillo e $I \subseteq R$ un ideal. Entonces el conjunto de cosets $\{r + I : r \in R\}$ forma un anillo con las operaciones

- $(s + I) + (t + I) = (s + t) + I$
- $(s + I)(t + I) = st + I$.

A este anillo se le llama el **anillo factor** R (mód I), -equivalentemente, anillo cociente-, y se denota por R/I.

Lo que este corolario hace es darnos una manera de construir más anillos a partir de algún anillo R que ya tengamos y un subconjunto I de R que sea un ideal. Sólo si I es ideal, el cociente R/I será anillo.

Ejemplo. Sean $R = \mathbb{Z}$, e $I = 5\mathbb{Z}$.

Como $\mathbb{Z}$ es anillo y $5\mathbb{Z}$ es ideal de $\mathbb{Z}$, se satisfacen las condiciones del corolario y aseguramos que $\mathbb{Z}/5\mathbb{Z}$ es un anillo. Un elemento $x \in \mathbb{Z}/5\mathbb{Z}$ es de la forma $r + 5z$, con $r \in \mathbb{Z}$ y $5z \in 5\mathbb{Z}$.

Más aún, todo elemento en $\mathbb{Z}/5\mathbb{Z}$ vivirá en una y sólo una de las siguientes clases laterales:

$$\{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}.$$

Ya que "otros elementos" que surgen de hacer variar $n \in \mathbb{Z}$, como podría ser $6 + 5\mathbb{Z}$, ya están tomados en cuenta en la lista anterior, pues serían congruentes a alguna de esas clases laterales. $6 + 5\mathbb{Z}$ es congruente a $1 + 5\mathbb{Z}$, dado que $6 = 5 \cdot 1 + 1$. Es decir, el resultado de dividir 6 entre 5 deja residuo 1.

De acuerdo a las reglas de suma y multiplicación descritas en el corolario, obtenemos cómo operar con las clases laterales. Por ejemplo, $(2+5\mathbb{Z})+(4+5\mathbb{Z}) = (2+4)+5\mathbb{Z} = 6+5\mathbb{Z} = 1+5\mathbb{Z}$. Mientras que la multiplicación sería $(2 + 5\mathbb{Z})(4 + 5\mathbb{Z}) = (2 \cdot 4) + 5\mathbb{Z} = 8 + 5\mathbb{Z} = 3 + 5\mathbb{Z}$.

Las demás operaciones se muestran en las tablas.

Tabla de suma:

$+$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$

Tabla de multiplicación:

$*$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$4+5\mathbb{Z}$	$1+5\mathbb{Z}$	$3+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$1+5\mathbb{Z}$	$4+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$3+5\mathbb{Z}$	$2+5\mathbb{Z}$	$1+5\mathbb{Z}$

En particular la tabla de la multiplicación ilustra que, bajo esta operación, $\mathbb{Z}/5\mathbb{Z}$ (isomorfo a $\mathbb{Z}_5$) es un grupo abeliano. Donde el neutro multiplicativo del grupo es $1+5\mathbb{Z}$, y cada clase lateral distinta

de cero tiene un inverso multiplicativo. $2+5\mathbb{Z}$ es inverso de $3+5\mathbb{Z}$, pues multiplicarlos resulta en $1+5\mathbb{Z}$. Mientras que, $1+5\mathbb{Z}$ es su propio inverso, y lo mismo pasa con $4+5\mathbb{Z}$.

No debería ser sorpresa que $\left(\mathbb{Z}/_{5\mathbb{Z}},\ *\right)$ sea grupo abeliano. Simplemente se verifica lo que ya nos decía un teorema: Como 5 es primo, $\mathbb{Z}_5$ es campo.

Definición (Ideal primo). Sea R un anillo conmutativo e $I \subset R$ un ideal propio. Decimos que I es un ideal primo si para cualesquiera $a, b \in R$ tales que $ab \in I$ tenemos que $a \in I$ o $b \in I$.

La noción de ideal primo se parece a la de número primo entero: teníamos que $p \in \mathbb{Z}$ es un número primo si para toda $m, n \in \mathbb{Z}$, si $p \mid nm$, entonces $p \mid n$, o $p \mid m$.

Ejemplo. $n\mathbb{Z}$ es un ideal primo si y sólo si n es primo. Pues $k \in p\mathbb{Z}$ si y sólo si $p \mid k$ y $p\mathbb{Z}$ tiene a todos los múltiplos de p. Si n fuera compuesto, existirían l, k tales que $1 < l, k < n$, tales que $n = lk$, y esto implicaría que $lk \in n\mathbb{Z}$, pero eso implicaría que l o k estarían en $n\mathbb{Z}$, lo que es imposible, pues l, k son menores a n.

Ejemplo. En $\mathbb{Z}[i]$, $\langle 2 \rangle$ **no es** un ideal primo, pues $2 = (1-i)(1+i)$, y ni $(1-i)$ o $(1+i)$ están en $\langle 2 \rangle$.

Definición (Ideal maximal). Sea R un anillo conmutativo e $I \subset R$ un ideal propio. Diremos que I es un ideal maximal si para todo ideal J tal que $I \subseteq J \subseteq R$ se tiene que $J = I$ o $J = R$.

Proposición. $I \subset R$ es un ideal maximal si y sólo si para cualquier $a \in {}^{R}/_{I}$ tenemos que

$$R = I + \langle a \rangle = \{i + ra : i \in I, r \in R\}.$$

En particular, si R es un anillo conmutativo, esto nos está diciendo que deben existir $i \in I$ y $r \in R$ tales que $ar + i = 1$.

Ejemplo. En $\mathbb{Z}$, los ideales primos son ideales maximales y viceversa.

Ejemplo. En $\mathbb{Z}[x]$, $\langle x \rangle$ es un ideal primo pero no es maximal:

Sea $f(x)g(x) \in \langle x \rangle$. Entonces existe $h(x) \in \mathbb{Z}[x]$ tal que $f(x)g(x) = xh(x)$. Lo que implica que ninguno de los polinomios f o g puede tener una constante distinta de cero. Sin pérdida de generalidad, sea g el polinomio sin término constante. Entonces $g \in \langle x \rangle$. Lo que significa que $\langle x \rangle$ es un ideal primo.

Sin embargo, observamos que $\langle 2, x \rangle = \{2r + xs : r, s \in \mathbb{Z}[x]\}$ es un ideal propio de $\mathbb{Z}[x]$ que contiene propiamente a $\langle x \rangle$. Mejor dicho, $\langle x \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$, por lo que $\langle x \rangle$ no es maximal.

Proposición. Si R es un anillo conmutativo con unitario e $I \subset R$ es un ideal maximal, entonces I es un ideal primo.

Dem.- Sean $a, b \in R$ tales que $ab \in I$. Si $a \in I$, I sería primo y no habría nada que demostrar. Supongamos pues que $a \notin I$. Esto implica que existen $r \in R$, $i \in I$ tales que $ar + i = 1$. Y multiplicando por b la ecuación obtenemos $abr + bi = b$. Ya que $ab \in I$ e I es ideal, entonces $(ab)r \in I$. Análogamente, $i \in I$ implica que $bi \in I$. Así, la suma de ambos está en I. Así, $b \in I$. Esto muestra que I es primo.

□

Tres resultados importantes que ya no demostraremos, pero que valdría la pena mencionarlos y ya se puede entender qué es lo que quieren decir son los siguientes:

Teorema 6. Sean R un anillo conmutativo con unitario, e I un ideal de R. ${}^{R}/_{I}$ es un dominio entero si y sólo si I es primo.

Teorema 7. Sean R un anillo conmutativo con unitario e I un ideal de R. R. ${}^{R}/_{I}$ es un campo si y sólo si I es maximal.

Teorema 8. Sean R un campo, e I un ideal de R. ${}^{R}/_{I}$ es un campo si y sólo si I es primo.

5. Ejercicios

- Demuestra que $\mathbb{Z}_p$ es campo si y sólo si p es primo.
- Muestra que el polinomio $x^2 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$.
- Demuestra que $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ es campo.
- ¿Quiénes son todos los elementos de $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$?
- Sean $\mathbb{R}[x]$ el anillo de los polinomios con coeficientes reales y $\langle x^2+1\rangle = \{p(x)(x^2+1) : p(x) \in \mathbb{R}[x]\}$. Simplifica el siguiente término:

$$5x^3 + 4x^2 - 2x + 3 + \langle x^2 + 1\rangle \in \mathbb{R}[x]/\langle x^2 + 1\rangle.$$

- Demuestra que $x^3 + 3$ es un ideal primo en $\mathbb{Q}[x]$.