Anillos

Aitor Moreno Rebollo

01/05/2021

Def. Un anillo es una terna $(A, +, \cdot)$ en la que se cumple:
i) $(A, +)$ es grupo abeliano.
ii) $(a \cdot b)c = a \cdot (b \cdot c)\ \forall a, b, c \in A$
iii)$a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a\ \forall a, b, c \in A$
Denotaremos la operación definida en el grupo abeliano por $+$, es decir, con notación aditiva. La operación $\cdot$ la denotaremos frecuentemente mediante yuxtaposición para simplificar notación.

Un anillo se dice unitario si existe un elemento $1_A \in A$ tal que $1_A \cdot a = a \cdot 1_A = a \quad \forall a \in A$.
Un anillo se dice conmutativo o abeliano si sus elementos conmutan respecto de la operación producto, es decir, si $ab = ba\ \forall a, b \in A$:

Def. Si A es un anillo, $a \in A$, $n \in \mathbb{N}$, definimos $na = \underbrace{a + ... + a}_{\text{n veces}}$, y $(-n)a = \underbrace{(-a) + ... + (-a)}_{\text{n veces}} \overset{\text{not}}{=} -a - ... - a$.

Definimos también $0 \cdot a = 0_A$.

Prop. A un anillo, si $a, b \in A$, y $n, m \in \mathbb{Z}$, entonces se cumple:
i) $(n + m)a = na + ma$
ii)$(nm)a = n(ma)$
iii) $n(a + b) = na + nb$
La demostración es trivial 'contando' la cantidad de veces que aparecen los elementos a y b y sus inversos en cada lado de las igualdades.

Def. A un anillo, $a \in A$, $n \in \mathbb{N}$, definimos $a^n = \underbrace{a \cdots a}_{\text{n veces}}$, y definimos también $a^0 = 1_A$.

Def. A un anillo, se dice que $a \in A$ es una unidad (o que es inversible), si existe un elemento $a' \in A$ tal que $aa' = a'a = 1_A$. Denotaremos $a' = a^{-1}$ y lo llamaremos inverso multiplicativo.

Not. El conjunto de unidades de A es $\mathfrak{U}(A) = \{a \in A \mid \exists a^{-1} \in A,\ a^{-1}a = aa^{-1} = 1_A\}$

Def. Sea $a \in \mathfrak{U}(A)$, $n \in \mathbb{N}$, definimos $a^{-n} = (a^{-1})^n$

Prop. A un anillo, $a, b \in \mathfrak{U}(A)$, $n, m \in \mathbb{Z}$, entonces:
i) $a^{n+m} = a^n a^m$
ii) $a^{nm} = (a^n)^m$
iii) Si a y b conmutan, entonces $(ab)^n = a^n b^n$
La demostración, una vez más, es trivial 'contando' la cantidad de veces que aparecen los elementos en los productorios de derecha e izquierda de las igualdades, y utilizando que $a^{-n} = (a^{-1})^n$ y $a^0 = 1_A$. Para exponentes positivos, esta proposición se cumple para cualesquiera elementos de A.

Prop. A un anillo unitario. Entonces $\mathfrak{U}(A)$ es un grupo respecto de la operación multiplicativa definida en A.

> **Dem.** La operación producto es asociativa. Es evidente que el producto de inversibles es inversible: $a, b \in \mathfrak{U}(A)$, $(ab)^{-1} = b^{-1}a^{-1}$. Además, $1_A \in \mathfrak{U}(A)$ por ser A unitario.

Si A es anillo abeliano, entonces $\mathfrak{U}(A)$ es anillo abeliano trivialmente.

Prop. A un anillo, $a, b \in A$, $n \in \mathbb{Z}$. Entonces:
i) $0_A a = a 0_A$
ii) $a(-b) = (-a)b = -(ab)$
iii) $(-a)(-b) = ab$
iv) $na = (n1_A)a$

Dem.
i) $0_Aa = (0_A)a = (0_A + 0_A)a = 0_Aa + 0_Aa \Longleftrightarrow 0_A = 0_Aa$
ii) $a(-b) + ab = a(-b + b) = a0_A0 = 0_A \Longrightarrow a(-b) = -(ab)$. Análogamente, $(-a)b = -(ab)$
iii) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$
iv) $(n1_A)a = (\underbrace{1_A + ... + 1_A}_{\text{n veces}})a = \underbrace{(1_Aa) + ... + (1_Aa)}_{\text{n veces}} = \underbrace{a + ... + a}_{\text{n veces}} = na$

Def. A un anillo, $a, b \in A \setminus \{0_A\}$ y satisfacen que $ab = 0_A$. Entoncesse dice que a es un divisor de cero a izquierda y b es un divisor de cero a derecha. Si A es abeliano, se dice simplemente que a y b son divisores de cero.

Def. Se llama dominio de integridad o anillo íntegro a un anillo conmutativo sin divisores de cero.

Def. Se llama cuerpo a un anillo conmutativo A en el que $\mathfrak{U}(A) = A \setminus \{0_A\}$. El anillo trivial $\{0\}$ no es un cuerpo.

Prop. Si A es cuerpo, entonces A es dominio de integridad.
Dem. Si A es cuerpo entonces es conmutativo y no trivial. Además, todos sus elementos, salvo el 0_A, admiten inverso multiplicativo. Sea $a \in A \setminus \{0_A\}$. Sea $b \in A$. Consideramos la ecuación $ab = 0_A$ y veamos que $b = 0_A$. En efecto, $ab = 0_A \Longrightarrow a^{-1}ab = a^{-1}0_A = 0_A \Longrightarrow b = 0_A$.

Obviamente, el recíproco no es cierto, esto es, existen dominios de integridad que no son cuerpos. Un ejemplo es $(\mathbb{Z}, +, \cdot)$. Sin embargo, se propone probar la siguiente proposición:

Prop (PROPUESTA). Si A es un dominio de integridad finito, entonces A es cuerpo.
Dem. Utilizaremos primero un pequeño
Lema. $a, b \in A$, ab es inversible si y solo si tanto a como b lo son.
Dem. $(ab)(ab)^{-1} = 1_A \Longrightarrow (ab)(ab^{-1}) = a(b(ab)^{-1})) = 1_A$, y por tanto $b(ab)^{-1} = a^{-1}$.
Por ser A conmutativo se concluye que $b^{-1} = a(ab)^{-1}$.
La otra implicación ya la hemos visto.
Ahora, $A = \{1_A, 0_A, a_1, ..., a_n\}$, y $a_ia_j = 0_A \Longleftrightarrow$ o bien $a_i = 0_A$, o bien $a_j = 0_A$. Todo esto por ser A dominio de integridad finito. Sean ahora dos elementos $a_i, a_j \in A \setminus \{0_A\}$, y consideramos su producto. Si $a_ia_j = 1_A$, entonces son inversos entre sí. Si no, llamamos $a_ia_j = a_{k_1}$, que es distinto de 0_A por elección de a_i y a_j. Consideramos la sucesión $\{a_{k_l}\}_{l\in\mathbb{N}}$, de forma que $a_{k_{l-1}} = a_{k_l}^2$, es decir, $a_{k_l} = (a_ia_j)^l$. Es evidente que $\{a_{k_l}\} \subseteq A \setminus \{0_A\}$, y como este conjunto es finito, entonces necesariamente $a_{k_t} = a_{k_s}$ para ciertos $s, t \in \mathbb{N}$, $s < t$, y por tanto, $a_{k_t} = a_{k_s} \Longrightarrow (a_ia_j)^t = (a_ia_j)^s(a_ia_j)^{t-s} = (a_ia_j)^s \Longrightarrow (a_ia_j)^s(a_ia_j)^{t-s} - (a_ia_j)^s = 0_A \Longrightarrow (a_ia_j)^s((a_ia_j)^{t-s} - 1_A) = 0_A \Longrightarrow (a_ia_j)^{t-s} - 1_A = 0_A \Longrightarrow (a_ia_j)^{t-s} = 1_A \Longrightarrow (a_ia_j)(a_ia_j)^{t-s-1} = 1_A$, y por tanto $(a_ia_j)^{t-s-1}$ es el inverso de (a_ia_j), y es no nulo, pues $(a_ia_j)(a_ia_j)^{t-s-1} = 1_A$. Por tanto a_i es inversible para cada i.

Def. $(A, +\cdot)$, $(B, +, \cdot)$ anillos, se dice que $(B, +, \cdot)$ es subanillo de A si:
i) $(B.+)$ es subgrupo de $(A, +)$
ii) $ab \in B \ \ \forall a, b \in B$
iii) $1_A \in B$, y por tanto, $1_A = 1_B$
Cuando se sobreentienden las operaciones, diremos sencillamente que B es subanillo de A. Se propone como ejercicio ver que la condición iii) no se deduce de la i) y la ii).

Ejercicio (PROPUESTO). Ver que, en la definición de subanillo, la tercera condición no se deduce de las dos anteriores.
Lo más sencillo es dar un contraejemplo. $(3\mathbb{Z}/6\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}/6\mathbb{Z}, +)$. Consideramos los respectivos anillos con el producto usual de coclases. Se satisface la condición ii), pues los únicos elementos de $3\mathbb{Z}/6\mathbb{Z}$ son $\overline{0}$ y $\overline{3}$, y el producto es $\overline{0} = 0_{\mathbb{Z}/6\mathbb{Z}}$. Sin embargo $1_{\mathbb{Z}/6\mathbb{Z}} = \overline{1} \notin 3\mathbb{Z}/6\mathbb{Z}$.