Anillos

Definición:

Un conjunto R con dos operaciones denotadas suma $(+)$ y producto $(\cdot)$ es un **anillo** si:

- $(R,+)$ es un grupo **abeliano**.
- $(R,\cdot)$ es un **semigrupo**. (es decir que es asociativo)
- Se tiene que para todos $a,b,c \in R$

$$\begin{aligned} a(b+c) &= ab+ac \\ (a+b)c &= ac+bc \end{aligned}$$

Notación:

Dado que un anillo tiene dos operaciones $(+,\cdot\,)$, donde cada operación tiene una identidad y podemos hablar de inversos para ambas operaciones, usamos la siguiente notación:

- 0 denota la identidad aditiva del anillo.
- 1_R denota la identidad multiplicativa (en caso de existir).
- $-a$ denota el inverso aditivo de un elemento $a \in R$.
- a^{-1} denota el inverso aditivo de un elemento $a \in R$. Notemos que a^{-1} no necesariamente existe para todo $a \in R$.
- R^* denota el conjunto de los elementos invertibles de R, esto es

$$R^* := \{a \in R : \exists a^{-1},\ a\cdot a^{-1} = a^{-1}\cdot a = 1_R\}$$

Propiedades:

- $0a = a0 = 0,\ \forall a \in R.$

$$\begin{aligned} 0a &= (1-1)a \\ &= 1a - 1a \\ &= a - a \\ &= 0 \\ &= a1 - a1 \\ &= a(1-1) \\ &= a0 \end{aligned}$$

- $(-a)b = a(-b) = -ab,\ \forall a,b \in R.$

$$\begin{aligned} ab + (-a)b &= (a+(-a))b \\ &= (0)b \\ &= 0 \\ &= a(0) \\ &= a(b+(-b)) \\ &= ab + a(-b) \end{aligned}$$

Como $ab+(-a)b = ab + a(-b) = 0$, entonces se tiene $a(-b) = (-a)b = -ab$.

- $(-a)(-b) = ab,\ \forall a,b \in R.$

$$\begin{aligned} (-a)(-b) &= a(-(-b)) \\ &= ab \end{aligned}$$

- $(na)b = a(nb) = n(ab),\ \forall a,b \in R,\ n \in \mathbb{Z}.$

Hacemos la prueba para los $n \geq 0$ por $\mathrm{P.I.M}$, los casos para $n < 0$ se heredan inmediatamente.

Sea $n = 0$, naturalmente

$$(0a)b = a(0b) = 0(ab) = 0$$

Ahora, supongamos que la propiedad se tiene para n y probemos que esto implica la propiedad para $n+1$:

$$\begin{aligned} [(n+1)a]b &= [na+a]b \\ &= (na)b + ab \\ &= a(nb) + ab \\ &= a[nb+b] \\ &= a[(n+1)b]^{**} \\ &= (na)b + ab \\ &= n(ab) + ab \\ &= (n+1)(ab)^{*} \end{aligned}$$

- $(\sum_{i=1}^n a_i)(\sum_{j=1}^m b_j) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$

Primero probemos que $k\sum_{i=1}^n a_i = \sum_{i=a}^n ka_i$ para todo $n \in \mathbb{N}^+$, esto lo haremos por inducción.

Para el caso $n = 1$, trivialmente tenemos que

$$\begin{aligned} k\sum_{i=1}^1 a_i &= ka_1 \\ &= \sum_{i=1}^1 ka_i \end{aligned}$$

Ahora, supongamos que tenemos la propiedad para n y veamos que esto implica la propiedad para $n+1$:

$$\begin{aligned} k\sum_{i=1}^{n+1} a_i &= k\left(\sum_{i=1}^n a_i + a_{n+1}\right) \\ &= k\sum_{i=1}^n a_i + ka_{n+1} \\ &= \sum_{i=1}^n ka_i + ka_{n+1} \\ &= \sum_{i=1}^{n+1} ka_i \end{aligned}$$

Quedando demostrada la propiedad. Ahora nuevamente por inducción, veamos **la propiedad principal**:

Para $n = 1$ tenemos que:

$$\begin{aligned} \sum_{i=1}^1 a_i \sum_{j=1}^m b_j &= a_1 \sum_{j=1}^m b_j \\ &= \sum_{j=1}^m a_1 b_j \\ &= \sum_{i=1}^1 \sum_{j=1}^m a_i b_j \end{aligned}$$

Ahora, supongamos la propiedad para n y veamos que esta implica la propiedad para $n+1$:

$$\begin{aligned} \sum_{i=1}^{n+1} a_i \sum_{j=1}^m b_j &= \left(\sum_{i=1}^n a_i + a_{n+1}\right)\sum_{j=1}^m b_j \\ &= \sum_{i=1}^n a_i \sum_{j=1}^m b_j + a_{n+1}\sum_{j=1}^m b_j \\ &= \sum_{i=1}^n \sum_{j=1}^m a_i b_j + \sum_{j=1}^m a_{n+1} b_j \\ &= \sum_{i=1}^{n+1} \sum_{j=1}^m a_i b_j \end{aligned}$$

Así, queda la propiedad demostrada.

Ejemplos:

Anillo de Automorfismos de un grupo abeliano:

Definimos

$$\mathrm{Aut}(G) := \{f : G \to G \mid f(a+b) = f(a) + f(b),\ \forall a,b \in G\}$$

Ahora, veamos que $(\mathrm{Aut}(G), +, \circ)$ es un anillo:

- Primero veamos que $(\mathrm{Aut}(G), +)$ es un grupo abeliano:
  - **Asociatividad:** Sean $f,g,h \in \mathrm{Aut}(G)$, se tiene que

$$\begin{aligned} [(f+g)+h](x) &= (f+g)(x) + h(x) \\ &= [f(x)+g(x)] + h(x) \\ &= f(x) + [g(x)+h(x)] \\ &= f(x) + (g+h)(x) \\ &= [f+(g+h)](x) \end{aligned}$$

    Para todo $x \in G$, donde usamos el hecho de que $f(x), g(x), h(x) \in G$ y que G es un grupo por lo tanto es asociativo.
  - **Elemento neutro:** Existe el automorfismo $\bar{e} \in \mathrm{Aut}(G)$ definido como:

$$\begin{aligned} \bar{e} : G &\to G \\ x &\mapsto e \end{aligned}$$

    tal que para todo $f \in \mathrm{aut}(G)$,

$$\begin{aligned} (f+\bar{e})(x) &= f(x) + \bar{e}(x) \\ &= f(x) + e \\ &= f(x) \end{aligned}$$

  - **Inversos:** Para un elemento arbitrario $f \in \mathrm{Aut}(G)$, podemos definir

$$\begin{aligned} f^{-1} : G &\to G \\ x &\mapsto (f(x))^{-1} \end{aligned}$$

    Ahora tenemos que comprobar que $f^{-1} \in \mathrm{Aut}(G)$. Sean dos elementos $h,k \in G$, tenemos que

$$\begin{aligned} f^{-1}(h+k) &= (f(h+k))^{-1} \\ &= (f(h)+f(k))^{-1} \\ &= (f(k))^{-1} + (f(h))^{-1} \\ &= (f(h))^{-1} + (f(k))^{-1} \\ &= f^{-1}(h) + f^{-1}(k) \end{aligned}$$

    Donde usamos que f es un automorfismo y G un grupo abeliano. También sabiendo que la suma de funciones es abeliana, queda demostrado que $(\mathrm{Aut}(G), +)$ es un grupo abeliano.
- Ahora, veamos que $(\mathrm{Aut}(G), \circ)$ es un monoide:
  - **Asociatividad:** En efecto dado que los elementos de $\mathrm{Aut}(G)$ son funciones, la asociatividad se tiene garantizada.
  - **Elemento neutro:** Existe el automorfismo identidad I_G, donde se puede ver fácilmente que $I_G \circ f = f \circ I_G = f$.
  - Como nota adicional, dado que no todos los automorfismos son biyectivos, luego no todo elemento tiene inverso en composición.
- Por último veamos las distributivas entre suma y composición:
  - $f(g+h) = f\circ g + f \circ h$: Sean estos 3 elementos de $\mathrm{Aut}(G)$, se tiene que

$$\begin{aligned} [f(g+h)](x) &= f(g(x)+h(x)) \\ &= f(g(x)) + f(h(x)) \\ &= (f\circ g)(x) + (f\circ h)(x) \end{aligned}$$

    Para todo $x \in G$ y haciendo uso de que f es un automorfismo, luego se tiene la igualdad.
  - $(f+g)\circ h = f\circ h + g \circ h$: Se tiene del álgebra usual de funciones.

Concluimos que es un anillo, como no es cierto que $f\circ g = g \circ f$, particularizamos a un anillo no conmutativo.

Anillo de matrices $\mathcal{M}_n(A)$.

Como comentario, no voy a profundizar en la demostración. Sólo recordando que es un anillo no abeliano pues el producto de matrices no conmuta (en general).

Anillo de $\wp(U)$ (PUNTO DE TALLER).

Sea un conjunto U, definimos las siguientes operaciones sobre su conjunto de partes:

$$A + B := A \triangle B, \quad A\cdot B := A \cap B$$

- Primero, tenemos que ver que $(\wp(U), +)$ es un grupo abeliano:

  Recordemos que

$$A\triangle B = (A-B)\cup(B-A)$$

  Y por notación, definimos el *complemento relativo* de un elemento $x \in \wp(U)$ como

$$x^c := U - x$$

  Donde tenemos que

$$A \triangle B = (A\cup B)\cap(A^c \cup B^c)$$

  - **Asociatividad:** Sean $A,B,C \in \wp(U)$, tenemos que

$$\begin{aligned} (A\triangle B)\triangle C &= \{(A\triangle B)\cup C\} \cap \{(A\triangle B)^c \cup C^c\} \\ &= \{[(A\cup B)\cap(A^c\cup B^c]) \cup C\} \\ &\cap \{[(A^c\cup B)\cap(A\cup B^c)]\cup C^c\} \\ &= \{(A\cup B\cup C)\cap(A^c\cup B^c\cup C)\} \\ &\cap\{(A^c\cup B\cup C^c)\cap(A\cup B^c\cup C^c)\} \\ &= (A\cup B\cup C)\cap(A^c\cup B^c\cup C) \\ &\cap(A^c\cup B\cup C^c)\cap(A\cup B^c\cup C^c) \\ &= (B\cup C\cup A)\cap(B\cup C^c\cup A^c) \\ &\cap(B^c\cup C^c\cup A^c)\cup(B^c\cup C^c\cup A) \\ &= (B\triangle C)\triangle A \\ &= A\triangle(B\triangle C) \end{aligned}$$

    Usando el hecho que $\triangle$ es **conmutativo**. (detallado más adelante)
  - **Elemento neutro:** Tenemos que $\varnothing \in \wp(U)$ y para un x arbitrario del conjunto se tiene que:

$$\begin{aligned} x\triangle\varnothing &= (x\cup\varnothing)\cap(x^c\cup\varnothing^c) \\ &= x\cap(x^c\cup U) \\ &= x\cap U \\ &= x \\ &= \varnothing\triangle x \end{aligned}$$

  - **Inversos:** Para un elemento arbitrario $x \in \wp(U)$, veamos que

$$\begin{aligned} x\triangle x &= (x\cup x)\cap(x^c\cup x^c) \\ &= x\cap x^c \\ &= \varnothing \end{aligned}$$

  - **Conmutatividad:** Dados dos elementos $x,y \in \wp(U)$, tenemos que

$$\begin{aligned} x\triangle y &= (x\cup y)\cap(x^c\cup y^c) \\ &= (y\cup x)\cap(y^c\cup x^c) \\ &= y\triangle x \end{aligned}$$

- Ahora, veamos que $(\wp(U), \cdot)$ es un monoide:
  - **Asociatividad:** Sean $x,y,z \in \wp(U)$,

$$\begin{aligned} (x\cdot y)\cdot z &= (x\cap y)\cap z \\ &= x\cap y\cap z \\ &= x\cap(y\cap z) \\ &= x\cdot(y\cdot z) \end{aligned}$$

  - **Elemento neutro:** Existe $U \in \wp(U)$ tal que para todo x,

$$\begin{aligned} x\cdot U &= x\cap U \\ &= x \end{aligned}$$

  - Como nota adicional, dado que $\varnothing\cap X = \varnothing$ para todo conjunto X, $\cdot$ no admite inversos para todos sus elementos y sin embargo, si es abeliano en tanto $x\cap y = y\cap x$.
- Por último, verifiquemos las propiedades distributivas de la suma y el producto:
  - $x(y+z) = xy+xz$: En efecto,

$$\begin{aligned} x(y+z) &= x\cap(y+z) \\ &= x\cap[(y\cup z)-(y\cap z)] \\ &= [x\cap(y\cup z)] - [x\cap(y\cap z)] \\ &= [(x\cap y)\cup(x\cap z)] - [(x\cap y)\cap(x\cap z)] \\ &= [(xy)\cup(xz)] - [(xy)\cap(xz)] \\ &= xy + xz \end{aligned}$$

  - $(x+y)z = xy+xz$: Dado que $(\wp(U),\cdot)$ es abeliano y ya demostramos la otra distributiva, se da que

$$\begin{aligned} (x+y)z &= z(x+y) \\ &= zx + zy \\ &= xz + yz \end{aligned}$$

Así, queda demostrado que $(\wp(U), +, \cdot)$ es un anillo abeliano con unidad.

Tipos de anillos:

Dado un anillo $(R,+,\cdot\,)$, este se puede clasificar más particularmente dependiendo de qué cómo se comporta $(R,\cdot\,)$ como estructura algebráica, entendiendo de entrada que es asociativa.

- Si $(R,\cdot\,)$ tiene un elemento neutro (1_R), R es un **anillo con unidad**.
- Además, si $(R,\cdot)$ tiene inversos, decimos que R es un **anillo de división**.
- Si $(R,\cdot\,)$ es abeliano, R es un **anillo conmutativo**.
- Si $(R,\cdot\,)$ no tiene divisores de 0, R es un **dominio de integridad**.

  Podemos interpretar no tener divisores de 0 como

$$ab = 0 \implies a = 0 \lor b = 0$$

  Y como equivalencia se tiene que para todos $a,b,c \in R$

$$ab = ac \implies b = c$$

  Es decir, que se tiene la propiedad cancelativa.

  Naturalmente, ***todo anillo de división es un dominio de integridad***.
- Si R es un **anillo de división conmutativo**, decimos que R es un **cuerpo**.

Resumiendo en el siguiente gráfico:

$$(R,+,\cdot\,)$$

$$\begin{tikzcd}
 & \text{Anillo} \arrow[dl, bend right, "ab=ba,\ \forall a,b\in R"'] \arrow[dr, bend left, "\exists 1_R, \forall a\in R,\ 1_R a = a 1_R = a"] & \\
\text{Anillo conmutativo} \arrow[ddddr, bend right] & & \text{Anillo con unidad} \arrow[d, "ab=0 \implies a=0\lor b=0"] \\
 & & \text{Dominio de integridad} \arrow[d, "\forall a, \exists a^{-1},\ aa^{-1}=a^{-1}a=1_R"] \\
 & & \text{Anillo de división} \arrow[ddl, bend left] \\
 & & \\
 & \text{Cuerpo} &
\end{tikzcd}$$

Característica de un anillo:

Definición:

Sea un anillo $(R,+,\cdot\,)$. Si existe un entero positivo mínimo n tal que $na = 0, \forall a \in R$, entonces decimos que R tiene **característica** n. Si tal n no existe, decimos que R tiene **característica** 0.

La característica de un anillo es denotada $\mathrm{char}(A) = n$.

Propiedades:

Sea n la característica de un anillo R con unidad, se tiene que

- Dado el homomorfimo

$$\begin{aligned} \varphi : \mathbb{Z} &\to R \\ z &\mapsto z1_R \end{aligned}$$

  Donde 1_R es la identidad multiplicativa de R, entonces $\ker(f) = \{nk : k \in \mathbb{Z}\}$.
- Si R no tiene divisores de 0, n es primo.

Homomorfismos de Anillos:

Definición:

Una función $f : R_1 \to R_2$ se dice un **homomorfismo de anillos** si para todos $a,b \in R$

- $f(a+b) = f(a) + f(b)$
- $f(a\cdot b) = f(a)\cdot f(b)$
- $f(1_{R_1}) = 1_{R_2}$

Propiedades:

Análogo a los homomorfismos de grupos, se tienen las siguientes **propiedades**:

- $f(0_{R_1}) = 0_{R_2}$
- $f(-a) = -f(a)$, para todo $a \in R_1$
- $f(a_1 - a_2) = f(a_1) - f(a_2)$, para todos $a_1, a_2 \in R_1$

Además, tenemos que

- $a \in A_1^* \implies f(a) \in A_2^*$
- $f(a^{-1}) = (f(a))^{-1}$, para todo $a \in R_1$

Igualmente, diremos que

- si f es **sobreyectiva**, f es un **epimorfismo**
- si f es **inyectiva**, f es una **inmersión**
- si f es **biyectiva**, f es un **isomorfismo de anillos**

Por último también tenemos los conjuntos

- $\ker(f) := \{x \in R_1 : f(x) = 0_{R_2}\}$
- $\mathrm{Im}(f) := \{y \in R_2 : \exists x \in R_1, f(x) = y\}$
