PEMMF.
Estructuras algebraicas
Ayudantías.
Rocío Acevedo

UNIVERSIDAD DE CHILE

Ayudantía 9 ✹

Pequeño repaso

Definición de Anillo

Un **anillo** es un conjunto R junto con dos operaciones: la *suma* $+$ y la *multiplicación* $\cdot$, tales que:

- Cerradura bajo la primera operación.
- La primera operación es asociativa.
- Existe un elemento neutro para la primera operación.
- Para todo elemento existe inverso.
- Conmuta.
- La segunda operación es cerrada.
- La segunda operación es asociativa.
- Existe neutro para la segunda operación.
- La segunda operación es distributiva respecto a la primera por la derecha: $a \times (b + c) = (a \times b) + (a \times c)$.
- La segunda operación es distributiva respecto a la primera por la izquierda: $(b + c) \times a = (b \times a) + (c \times a)$.

Si R es un anillo y existe un elemento $1 \in R$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in R$, decimos que R es un **anillo con unidad**.

Tipos de Anillos

Anillo Conmutativo

Un anillo R es **conmutativo** si la multiplicación es conmutativa, es decir, para todos $a, b \in R$:

$$a \cdot b = b \cdot a.$$

Anillo de División

Un **anillo de división** es un anillo en el que cada elemento distinto de cero tiene inverso multiplicativo, aunque no necesariamente es conmutativo.

Anillo con divisores de cero

Un anillo R tiene **ceros divisores** si existen $a, b \in R$ con $a \neq 0$ y $b \neq 0$ tales que $a \cdot b = 0$.

Ideales

Un **ideal** de un anillo R es un subconjunto $I \subseteq R$ tal que:

- $(I, +)$ es un subgrupo de $(R, +)$.
- Si $r \in R$ y $i \in I$, entonces $r \cdot i \in I$ y $i \cdot r \in I$.

Ideales Principales

Un ideal I de un anillo R se dice **principal** si existe un elemento $a \in R$ tal que

$$I = \{r \cdot a : r \in R\}.$$

El ideal generado por a se denota como (a).

Tipos de Ideales

Ideal Izquierdo y Derecho

- Un **ideal izquierdo** I de R es un subconjunto tal que $r \cdot i \in I$ para todo $r \in R$ y $i \in I$.
- Un **ideal derecho** I de R es un subconjunto tal que $i \cdot r \in I$ para todo $r \in R$ y $i \in I$.

Ideal Primo

Un ideal $P \subset R$ es un **ideal primo** si $P \neq R$ y, para $a, b \in R$, si $a \cdot b \in P$, entonces $a \in P$ o $b \in P$.

Ideal Maximal

Un ideal $M \subset R$ es un **ideal maximal** si $M \neq R$ y si no existe un ideal $J \subset R$ tal que $M \subset J \subset R$.

Ejercicios

1. Un elemento a de un anillo R se dice idempotente sí $a^2 = a$. Muestre que el conjunto de los idempotentes en un anillo conmutativo es cerrado bajo multiplicación. Encuentre los idempotentes de $\mathbb{Z}_6 x \mathbb{Z}_{12}$. Muestre que en un anillo de división hay exactamente 2 idempotentes.

   Dem:
   Sea $a, b \in I$, con I el conjunto de los idempotentes. Así,

   $$(ab)^2 = (ab)(ab) = (aa)(bb) = a^2 b^2 = ab.$$

   Para los idempotentes del conjunto J de $\mathbb{Z}_6$ y $\mathbb{Z}_{12}$, identificamos cada uno por separado.

Para $\mathbb{Z}_6$, se tiene 0. Para $\mathbb{Z}_{12}$, se tiene 0. Así, quedarán los siguientes pares ordenados.

$$J = \{(0,0)\}$$

Para un anillo de división, se tiene que un idempotente $a(a-1) = 0$. Las soluciones posibles sólo son $a = 1, a = 0$. Es necesaria la condición del anillo de división, ya que en caso contrario existiría un $a \neq 0, b \neq 0$ tal que $ab = 0$.

2. Sea p primo. Demuestre que en el anillo $\mathbb{Z}_p$ se cumple $(a+b)^p = a^p + b^p$ para todo $a, b \in \mathbb{Z}_p$.

   Se tiene:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

   Así, se tiene que

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

   Por esto, se tiene

$$\sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} b + ... + \binom{p}{p-1} a^1 b^{p-1} + \binom{p}{p} b^p$$

   Así, con $1 \leq k \leq p-1$ todos los coeficientes serán múltiplos de p, por lo que serán 0 en $\mathbb{Z}_p$. Por ello, queda:

$$(a+b)^p = a^p + b^p$$

3. Sea R un anillo conmutativo con unidad y de característica prima p. Demuestre que la función $f_p : R \to R$ dada por $f_p(a) = a^p$ es un homomorfismo.

   P.d:

   $f_p(a+b) = f_p(a) + f_p(b)$ para todo $a, b \in R$ y $f_p(ab) = f_p(a)f_p(b)$ para todo $a, b \in R$

   Dem:

   Para la suma:

   $$f_p(a+b) = (a+b)^p = a^p + b^p = f_p(a) + f_p(b).$$

   Para la multiplicación:

   $$f_p(ab) = (ab)^p = a^p \cdot b^p = f_p(a) \cdot f_p(b).$$

   Por lo tanto, es homomorfismo de anillos.