Universidad de Chile
Facultad de Ciencias Físicas y Matemáticas
Departamento de Ingeniería Matemática
MA1101-10 Introducción al Álgebra
30 de junio de 2023

Auxiliar 13: Anillos y Cuerpos
Profesor: Alexander Frank
Auxiliar: Gonzalo Ovalle

P1. Sea $(A, +, \cdot)$ un anillo conmutativo. Se tiene $G \subseteq A$ por:

$$G = \{a \in A : a \text{ tiene inverso para } \cdot\}$$

i) Muestre que $(G, \cdot)$ es grupo abeliano.

ii) Sea $H = \{a^2 : a \in G\}$. Pruebe que H es subgrupo de G.

iii) Si $(A, +, \cdot) = (\mathbb{Z}_7, +_7, \cdot_7)$, encuentre G y H.
<u>Recuerdo:</u> Es sabido que $(\mathbb{Z}_7, +_7, \cdot_7)$ es un anillo conmutativo.

P2. Sea $(\mathbb{K}, +, \cdot)$ un cuerpo. Definimos las siguientes operaciones sobre $\mathbb{K} \times \mathbb{K}$:

$$(a, b) \oplus (c, d) = (a + c, b + d) \qquad (a, b) \oplus (c, d) = (a \cdot c, b \cdot d)$$

Se sabe (no lo demuestre) que $(\mathbb{K} \times \mathbb{K}, \oplus, \odot)$ es un anillo conmutativo con unidad.

a) Encuentre el neutro para $\oplus$ y el neutro para $\odot$.

b) Demuestre que $\forall (a, b) \in (\mathbb{K} \times \mathbb{K}) \setminus \{0_{\mathbb{K}\times\mathbb{K}}\}$:

$$(a, b) \text{ es divisor del } 0 \iff (a, b) \text{ no es invertible}$$

c) ¿Es $(\mathbb{K} \times \mathbb{K}, \oplus, \odot)$ un cuerpo? Argumente.

P3. Sean $(A, +, \cdot)$ y $(B, \oplus, \odot)$ dos anillos. Sea $f : A \to B$ un morfismo de anillos, es decir:

$$f(x + y) = f(x) \oplus f(y) \qquad f(x \cdot y) = f(x) \odot f(y) \qquad f(1_A) = 1_B$$

a) Demuestre que para todo $a \in A$, $f(a^{-1}) = f(a)^{-1}$.
<u>Ind:</u> Notar que esto solo tiene sentido para los $a \in A$ que tienen inverso.

b) Demuestre que $f(0_A) = 0_B$.

c) Demuestre que si todo $a \in A$ es invertible salvo 0_A, entonces f es inyectiva.

P4. Sea $(A, +, \cdot)$ un anillo conmutativo. Se define la *caracteristica del anillo* $(A, +, \cdot)$ como el mínimo valor $n \in \mathbb{N} \setminus \{0\}$ tal que si se suma el 1 consigo mismo n veces, entonces esa suma es igual 0.
Si dicho n no existe, entonces se dice que el anillo tiene característica 0.

i) Encuentre la característica de $(\mathbb{Q}, +, \cdot)$ y de $(\mathbb{Z}_k, +_k, \cdot_k)$, con $k \geq 1$.

ii) Demuestre que si el anillo $(A, +, \cdot)$ tiene característica $n > 0$, entonces $\forall a \in A$, sumar a consigo mismo n veces es igual a 0.

iii) Demuestre que si un cuerpo tiene característica $p \in \mathbb{N}$, entonces $p = 0$ o p es primo.

Resumen

[Anillo] Una estructura $(A, +, \cdot)$ se llamara **anillo** si:

- $(A, +)$ es un grupo abeliano, cuyo neutro se denota 0.
- $\cdot$ es asociativa
- Existe un elemento neutro en $A \setminus \{0\}$ para $\cdot$ que se denota 1.
- $\cdot$ distribuye respecto a $+$.

[Convención] Usualmente cuando trabajamos con un anillo $(A, +, \cdot)$:

- Al neutro de $(A, +)$ lo denotaremos por 0, y para todo $x \in A$, a su inverso para la operación $+$, que es único pues $+$ es asociativa, se le denotará $-x$ y se le llamará **opuesto** o **inverso aditivo**.
- Si $x \in A$ posee inverso para la operación $\cdot$, entonces este es único pues la operación es asociativa y se le denotará x^{-1}.

[Homomorfismo entre anillos] Sean $(A, +_A, \cdot_A), (B, +_B, \cdot_B)$ dos anillos. La función $f : A \longrightarrow B$ es un homomorfismo de $(A, +_A, \cdot_A)$ en $(B, +_B, \cdot_B)$ si $\forall x, y \in A$:

$$f(x +_A y) = f(x) +_B f(y) \qquad f(x \cdot_A y) = f(x) \cdot_B f(y) \qquad f(1_A) = 1_B$$

[Prop] Si $(A, +, \cdot)$ es un anillo, entonces $\forall x, y \in A$ se cumple que:

i) $0 \cdot x = x \cdot 0 = 0$

ii) $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$

iii) $(-x) \cdot (-y) = x \cdot y$

iv) $-x = (-1) \cdot x = x \cdot (-1)$

[Def] Sea $(A, +, \cdot)$ un anillo. Para $a \in A, n \in \mathbb{N}$ se definen recursivamente potencias y multiplos de a que se denotan a^n y $n \cdot a$ recursivamente:

- $a^0 = 1$ y $a^{n+1} = a^n \cdot a, n \in \mathbb{N}, n \geq 0$. Si a posee inverso a^{-1}, entonces $a^{-n} = (a^{-1})^n$
- $0 \cdot a = 0,\ (n+1) \cdot a = n \cdot a + a$ y $(-n) \cdot a = n \cdot (-a), n \in \mathbb{N}, n \geq 0$.

[Divisores de cero] Sea $(A, +, \cdot)$ un anillo. Un elemento $a \in A, a \neq 0$ se dice divisor del 0 si $\exists y \in A \setminus \{0\}$ tal que $a \cdot y = 0$ o bien $y \cdot a = 0$.

[Dominio de integridad] Un anillo conmutativo y sin divisores de cero se dice dominio de integridad.

[Cuerpo] Una estructura $(\mathbb{K}, +, \cdot)$ se llamara cuerpo si:

- $(K, +, \cdot)$ es un anillo conmutativo.
- Todo elemento $a \in \mathbb{K} \setminus \{0\}$ es invertible para $\cdot$

Equivalentemente, $(\mathbb{K}, +, \cdot)$ es cuerpo si y solo si:

- $(\mathbb{K}, +)$ es grupo abeliano
- $(\mathbb{K} \setminus \{0\}, \cdot)$ es grupo abeliano.
- $\cdot$ distribuye respecto a $+$.

[Prop] Si $(\mathbb{K}, +, \cdot)$ es un cuerpo, entonces $\mathbb{K}$ no tiene divisores del cero.