Universidad de Chile
Facultad de Ciencias Físicas y Matemáticas
Departamento de Ingeniería Matemática
MA1101-2 Introducción al Álgebra
30 de junio de 2023

Auxiliar 17: Trabajo dirigido para el C6

Profesor: Nicolás Hernández S.
Auxiliar: Pablo Zúñiga Rodríguez-Peña

P1. Sea $E = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Asuma que $(E, +, \cdot)$ es un anillo conmutativo, en particular, no necesita demostrarlo. Para este anillo:

a) Encuentre los neutros de la suma y el producto.

b) Pruebe que $(E, +, \cdot)$ no tiene divisores de cero.

c) Muestre que $(E, +, \cdot)$ no es un cuerpo.

P2. Sea $(G, *)$ un grupo abeliano y $H, K \subseteq G$ dos subgrupos de G. Se define el conjunto

$$H * K := \{h * k : h \in H, k \in K\}.$$

Pruebe que $(H * K, *)$ es subgrupo de $(G, *)$.

P3. Sea $(A, +, \cdot)$ un anillo conmutativo.

a) Demuestre que si $x \in A$ es divisor de cero, entonces x no posee inverso.

b) Suponga que $|A| < \infty$. Sea $x \in A \setminus \{0_A\}$ no invertible.

1) Muestre que para todo $k \in \mathbb{N} \setminus \{0\}$, $x^k \neq 1_A$. **Indicación:** contradicción.
2) Muestre que existen $n, m \in \mathbb{N} \setminus \{0\}$ tales que $x^n = x^m$. **Indicación:** contradicción.
3) Muestre que existen $r, s \in \mathbb{N} \setminus \{0\}$ tales que $x^s(1_A - x^r) = 0_A$. **Indicación:** parte 2).
4) Concluya que x es divisor de cero.

c) Demuestre que en $(\mathbb{Z}_n, +_n, \cdot_n)$[1] para $n \geq 1$, todo elemento no invertible para $\cdot_n$ es divisor de cero.

P4. Sea $(A, +, \cdot)$ un anillo y denote por 0 a su neutro aditivo y 1 a su neutro multiplicativo. Se define la *característica del anillo* $(A, +, \cdot)$ como el mínimo valor $n \in \mathbb{N} \setminus \{0\}$ tal que

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}} := n1 = 0.$$

Si tal n no existe, entonces se dice que el anillo tiene característica 0.

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

b) Muestre que si el anillo $(A, +, \cdot)$ tiene característica $n > 0$, entonces

$$\forall a \in A, \quad \underbrace{a + a + \cdots + a}_{n \text{ veces}} := na = 0.$$

c) Concluya que si un cuerpo (con $0 \neq 1$) tiene característica p, entonces $p = 0$ o p es primo.
Indicación: En el caso $p \neq 0$, descarte que $p = 1$ y luego use la descomposición prima de p.

[1] Página 136 del apunte versión pandemia.

En todo el resumen, $(G,*)$ es un grupo con neutro e_G, $(H,*)$ es un subgrupo de $(G,*)$, $(A,+_A,\cdot_A)$ y $(B,+_B,\cdot_B)$ son anillos.

Definición. Una estructura $(G,*)$ se dice **grupo**, si $*$ es asociativa, admite neutro en G y todo elemento en G posee inverso en G. Si además $*$ es conmutativa, $(G,*)$ se dice **grupo abeliano**.

Definición. Para $H \subseteq G$ no vacío, $(H,*)$ se dice **subgrupo de** $(G,*)$ si es también un grupo.

Teorema. $(H,*)$ es subgrupo de $(G,*)$ $\iff$ $H \subseteq G \wedge \forall x,y \in H, x * y^{-1} \in H$.

Proposición (Propiedades de grupos y subgrupos). Sea (K,Δ) una estructura y $f : G \to K$ un homomorfismo.

- Los neutros de $(G,*)$ y $(H,*)$ coinciden. Los inversos en $(G,*)$ y en $(H,*)$ coinciden.
- $(f(G),\Delta)$ es grupo y $(f(H),\Delta)$ es subgrupo de $(f(G),\Delta)$.
- Denotemos $e_K = f(e_G)$ el neutro en $(f(G),\Delta)$. Entonces f es inyectiva ssi $f^{-1}(\{e_k\}) = \{e_G\}$.

Definición. Una estructura $(A,+,\cdot)$ se dice **anillo** si

- $(A,+)$ es grupo abeliano, con neutro denotado 0_A (llamado **neutro aditivo**),
- $\cdot$ es asociativa,
- Existe neutro en $A \setminus \{0\}$ para $\cdot$, con neutro denotado 1_A (llamado **neutro multiplicativo**),
- $\cdot$ distribuye con respecto a $+$.

Si además $\cdot$ es conmutativa, $(A,+,\cdot)$ se dice **anillo conmutativo**.
Para $a \in A$ y $n \in \mathbb{N}$, se definen recursivamente

- **las potencias de** a, como $a^0 = 1$; $a^n = a^{n-1} \cdot a$ si $n \geq 1$.
  Además, si a posee inverso a^{-1} para $\cdot$, $a^{-n} = (a^n)^{-1}$.
- **los múltiplos de** a, como $0a = 0$; $na = (n-1)a + a$ si $n \geq 1$. Además, $-na = n(-a)$.

Proposición. Sea $(A,+,\cdot)$ un anillo, $x,y \in A$, $k,\ell \in \mathbb{Z}$ y $n \in \mathbb{N}$.

- $0_A \cdot x = x \cdot 0_A = 0_A$.
- $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$ y $(-x) \cdot (-y) = x \cdot y$.
- $-x = (-1) \cdot x = x \cdot (-1)$.
- $k(a+b) = ka + kb$, $(k+\ell)a = ka + \ell a$ y $(ka) \cdot (\ell b) = (k\ell)(a \cdot b)$.
- $x^{n+1} - 1_A = (x - 1_A) \cdot \sum_{k=0}^{n} x^k$. Si el anillo es conmutativo, $(x+y)^n = \sum_{k=0} \binom{n}{k} x^k \cdot y^{n-k}$.

Definición. Una función $f : A \to B$ se dice **homomorfismo de anillos** si para todo $x,y \in A$,

$$f(x +_A y) = f(x) +_B f(y), \quad f(x \cdot_A y) = f(x) \cdot_B f(y), \quad f(1_A) = 1_B.$$

Definición. Un elemento $a \in A \setminus \{0_A\}$ se dice **divisor de cero** si existe $b \in A \setminus \{0_A\}$ tal que $a \cdot_A b = 0_A$, o bien, $b \cdot_A a = 0_A$ (notar que en tal caso, b también sería divisor de cero).

Definición. Un anillo conmutativo y **sin** divisores de cero se llama **dominio de integridad**.

Definición. Una estructura $(K,+,\cdot)$ se dice **cuerpo** si $(K,+,\cdot)$ es un anillo conmutativo y todo elemento $x \in K \setminus \{0_K\}$ es invertible para $\cdot$.

Proposición. Todo cuerpo es un dominio de integridad. (y no viceversa)