LISTA 1

Operações Binárias, Estruturas Algébricas e Corpos

Operações

1 — Dado $\circ$ uma operação binária em A. Mostre que:

- a Se e é a identidade para $\circ$, então e é idempotente.
- b Se $\circ$ é associativa e comutativa e a, b são idempotentes então $a \circ b$ é idempotente.
- c Se $\circ$ é associativa e a, b invertíveis então $a \circ b$ é invertível.

2 — Suponha que $\circ$ é uma operação binária associativa em A. Seja x um elemento fixo de A. Definimos outra relação binária $\circ^x$ em A por

$$a \circ^x b := a \circ (x \circ b)$$

Mostre que $\circ^x$ é associativa.

Grupos

3 — Seja G seja um grupo. Mostre que

- a cancelamento - para todos $g, h, j \in G$, se $gh = gj$, ou $hg = jg$, então $h = j$
- b para todos $g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$, e $(g^{-1})^{-1} = g$
- c A equação $gx = j$ possui uma única solução $x = g^{-1}j$

4 — Suponha que G seja um grupo e que $|G| = 2$. Mostre que $g * g = e$ para todo $g \in G$.

5 — Suponha que G seja um grupo e que $|G| = 3$. Mostre que $g * g * g = e$ para todo $g \in G$.

6 — Suponha que $x * y = e$ mostre que $y * x = e$.

Corpos

7 — Mostre que $\mathbb{Q}(\sqrt{2})$ é um corpo.

8 — Seja $(\mathbb{K}, +, \cdot)$ um corpo. Mostre que:

- a Se 0_1 e 0_2 são elementos de $\mathbb{K}$ satisfazendo:

  $$x + 0_1 = x \text{ e } x + 0_2 = x, \ \forall x \in \mathbb{K},$$

  então $0_1 = 0_2$. Em outras palavras, existe um único elemento neutro da soma num corpo que denotamos por 0.
- b Dado $x \in \mathbb{K}$, se x_1 e x_2 são elementos de $\mathbb{K}$ satisfazendo:

  $$x + x_1 = 0 \text{ e } x + x_2 = 0,$$

  então $x_1 = x_2$. Em outras palavras, num corpo cada elemento x possui um único oposto, denotado por $-x$.
- c Se x_1 e x_2 são elementos de $\mathbb{K}$ que satisfazem:

  $$x_1 \cdot x = x \text{ e } x_2 \cdot x = x, \ \forall x \in \mathbb{K},$$

  então $x_1 = x_2$. Em outras palavras, um corpo possui uma única unidade, que é denotada por 1.
- d Dado $x \in \mathbb{K}$ com $x \neq 0$, se x_1 e x_2 são elementos de $\mathbb{K}$ satisfazendo:

  $$x \cdot x_1 = 1 \text{ e } x \cdot x_2 = 1,$$

então $x_1 = x_2$. Em outras palavras, num corpo cada elemento não nulo x possui um único inverso multiplicativo, denotado por x^{-1}.

9 — Seja $(\mathbb{K}, +, \cdot)$ um corpo. Mostre que:

- a $0 \cdot x = 0$, para todo $x \in \mathbb{K}$.
- b Se x_1 e x_2 são elementos de $\mathbb{K}$ com $x_1 \cdot x_2 = 0$, então $x_1 = 0$ ou $x_2 = 0$.
- c $-x = (-1) \cdot x$, para todo $x \in \mathbb{K}$.
- d Se x, x_1 e x_2 são elementos de $\mathbb{K}$ com $x \neq 0$ e $x \cdot x_1 = x \cdot x_2$, então

$$x_1 = x_2.$$

10 — Sejam $\mathbb{K}$ um corpo e $\mathbb{F}$ um subcorpo de $\mathbb{K}$. Mostre que:

- a O elemento neutro da soma de $\mathbb{F}$ coincide com o elemento neutro da soma de $\mathbb{K}$;
- b A unidade multiplicativa de $\mathbb{F}$ coincide com a unidade multiplicativa de $\mathbb{K}$.

11 — Mostre que todo subcorpo de $\mathbb{C}$ contém $\mathbb{Q}$.

12 — Mostre que se um corpo tem característica zero, então ele é infinito.

13 — Dado $Q = (a, b)$ com $a, b \in \mathbb{Z}$ e $b \neq 0$. Definimos a relação R em Q por

$$(a, b)R(c, d) \text{ see } ad = cb$$

- a Mostre que R é uma relação de equivalência.
- b Ache três elementos em $[(1, 3)]_R$
- c Mostre que $\forall n \in \mathbb{Z}$, $n \neq 0$, $[(x, y)]_R = [(nx, ny)_R$.
- d Seja $\square$ a operação binária em $[Q]_R$ definida por:

$$[(x, y)]_R \square [(m, n)]_R = [(\text{xm}, \text{yn})]_R$$

Mostre que a operação está bem definida, i.e., se $[(x, y)]_R = [(z, w)]_R$ e $[(m, n)]_R = [(p, q)]_R$ então

$$[(x, y)]_R \square [(m, n)]_R = (z, w)]_R \square [(p, q)]_R.$$

- e Desta vez tentamos definir uma relação binária $\oplus$ em $[Q]_R$ por:

$$[(x, y)]_R \oplus [(m, n)]_R = [(x + m, y + n)]_R$$

Mostre que $\oplus$ não está bem definida, ou seja não é realmente uma operação binária em $[Q]_R$

- f Seja $\boxplus$ a operação binária em $[Q]_R$ definida por:

$$[(x, y)]_R \boxplus [(m, n)]_R = [(xn + ym, \text{yn})]_R$$

Mostre que a operação está bem definida.

- g O que é Q?

Aneis

14 — Quais são os elementos invertíveis de $\mathbb{Z}/12\mathbb{Z}$ com respeito a adição e a multiplicação induzidas.

15 — Seja n um inteiro positivo que não é primo. Mostre que o anel $\mathbb{Z}/n\mathbb{Z}$ não é um domínio.

16 — Seja $p(x) \in \mathbb{K}[x]$. Então α é uma raiz de multiplicidade m de $p(x)$ se e somente se $p^{(m-1)}(\alpha) = 0$ mas $p^{(m)}(\alpha) \neq 0$, onde $p^{(k)}(x)$ denota a k-ésima derivada de $p(x)$.

17 — Sejam $p, q \in \mathbb{K}[x]$ não nulos, mostre que:

a Se $p \neq -q$ então $\deg(p+q) \leq \max\{\deg(p), \deg(q)\}$

b $\deg(p \cdot q) = \deg(p) + \deg(q)$

18 — Sejam $p_1, \ldots, p_n \in \mathbb{K}[x]$ polinômios coprimos dois a dois (i.e., $\mathrm{mdc}(p_i, p_j) = 1$ para todo $i \neq j$) tais que $p_i \mid q$ para todo i, onde $q \in \mathbb{K}[x]$. Mostre que $p_1 \cdot \ldots \cdot p_n \mid q$.