Álgebra I

Lista 3

OBS:

1) Mostre que todo domínio finito é um corpo.

2) Mostre que um idempotente am um anel sem divisores de zero é igual a 0 ou igual a 1.

3) Seja R um anel e X um conjunto arbitrário para o qual exista uma função bijetiva $f : X \to R$. Mostre que podemos, com o auxílo desta bijeção, induzir uma estrutura de anel no conjunto X, com as operações:

$$x \oplus y = f^{-1}(f(x) + f(y)), \qquad x \odot y = f^{-1}(f(x) \cdot f(y)).$$

Quem é o zero? Quem é o inverso aditivo de um elemento $x \in X$? Se R tiver unidade, X terá unidade? Se R for comutativo, X também o será?

4) Seja R um anel e S e T sub-aneis de R, mostre que a intersecção $S \cap T$ também é sub-anel.

5) Seja R um anel, S um sub anel de R e T um sub anel de S. Mostre que T é sub anel de R.

6) Mostre que os seguintes subconjuntos são sub-aneis de $\mathbb{C}$:

a) $R_p = \{\frac{m}{n} \in \mathbb{Q} \,|\, m, n \in \mathbb{Z}$ e $p \nmid n\}$, para $p \in \mathbb{N}$ um número primo dado (note que este é sub-anel de $\mathbb{Q}$, que por sua vez é sub-anel de $\mathbb{C}$, então conclua usando a questão anterior).

b) $S = \mathbb{Z} + \mathbb{Z}\varepsilon + \mathbb{Z}\varepsilon^2 + \cdots + \mathbb{Z}\varepsilon^{n-1}$ onde $\varepsilon \in \mathbb{C}$ é uma raiz n-ésima da unidade, isto é, $\varepsilon^n = 1$.

7) Mostre que um elemento $a \in \mathbb{Z}_n$ é invertível se, e somente se, $\mathbf{mdc}(a, n) = 1$. Conclua que, para todo primo $p \in \mathbb{N}$, o anel $\mathbb{Z}_p$ é um corpo. Mostre também que se $n = a.b$ então $\mathbb{Z}_n$ possui divisores de zero.

8) Considere o anel de convolução das funções aritméticas, $\mathbf{Fun}(\mathbb{N}^*, \mathbb{R}) = \{f : \mathbb{N}^* \to \mathbb{R}\}$, onde $\mathbb{N}^*$ é o conjunto dos naturais não nulos, com as operações

$$(f + g)(n) = f(n) + g(n), \qquad (f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

a) Mostre que, de fato é um anel comutativo com unidade, que vamos denotar por 1_R (quem é este 1_R?).

b) Mostre que o conjunto das funções multiplicativas, isto é, o conjunto das funções $f : \mathbb{N}^* \to \mathbb{R}$ satisfazendo à condição que $f(mn) = f(m)f(n)$ sempre quando $\mathbf{mdc}(m, n) = 1$, é um sub-anel de $\mathbf{Fun}(\mathbb{N}^*, \mathbb{R})$.

c) Mostre que um elemento $f \in \mathbf{Fun}(\mathbb{N}^*, \mathbb{R})$ é invertível, se, e somente se, $f(1) \neq 0$.

d) A função de Möbius, $\mu : \mathbb{N}^* \to \mathbb{R}$ é definida como

$$\mu(n) = \begin{cases} 1 & \text{se} \quad n = 1, \\ (-1)^r & \text{se} \quad n = p_1 \dots p_r, \text{ com } p_i \text{ primos distintos dois a dois}, \\ 0 & \text{se} \quad \text{existe } p \text{ um número primo com } p^2 | n. \end{cases}$$

Mostre que a função de Möbius é multiplicativa e que $\mu * \mathbf{1} = 1_R$, onde $\mathbf{1}$ é a função constante igual a 1.

e) Sejam f e g duas funções no anel de funções aritméticas. Mostre que $f = \mu * g$ se, e somente se $g = \mu * f$.

f) Considere g e f funções aritméticas tais que

$$g(n) = \sum_{d|n} f(d),$$

mostre que

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Esta é a fórmula de inversão de Möbius (veja meu artigo na revista da ORM de 2014).

g) Considere a função $\tau : \mathbb{N}^* \to \mathbb{R}$ dada por $\tau(n) = \#\{d \in \mathbb{N}^* \mid d|n\}$, isto é, o número de divisores de n. Mostre que τ é uma função multiplicativa e que $\tau = \mathbf{1} * \mathbf{1} = \sum_{d|n} 1$.

h) Considere a função $\sigma : \mathbb{N}^* \to \mathbb{R}$ dada por $\sigma(n) = \sum_{d|n} d$, isto é, a soma dos divisores de n. Mostre que σ é uma função multiplicativa e que $\sigma = \mathbf{1} * \mathbf{Id}_{\mathbb{N}^*}$.

i) Considere a função totiente de Euler $\varphi : \mathbb{N}^* \to \mathbb{R}$ dada por $\varphi(n) = \#\{1 \leq k \leq n \mid \mathbf{mdc}(k, n) = 1\}$. Mostre que φ é uma função multiplicativa e que $\mathbf{Id}_{\mathbb{N}} = \mathbf{1} * \varphi$.

j) Utilize a fórmula de inversão de Möbius para calcular os valores $\tau(n)$, $\sigma(n)$ e $\varphi(n)$ para $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.

Relações de equivalência

9) Considere a seguinte relação $\sim$ no conjunto $\mathbb{N} \times \mathbb{N}$: $(m, n) \sim (p, q)$ se $m + q = n + p$.

a) Mostre que, de fato, $\sim$ é relação de equivalência.

b) Descreva a classe de equivalência $[(m, n)]$ (considere por enquanto os casos $m \geq n$ e $m < n$ separadamente).

c) Mostre que o conjunto quociente $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ (sim, são os inteiros) é um anel comutativo com unidade, com as operações

$$[(m, n)] + [(p, q)] = [(m + p, n + q)], \qquad [(m, n)].[(p, q)] = [(mp + nq, mq + np)].$$

Note que, primeiramente tem que mostrar que as operações estão bem definidas, isto é independem de representante na classe de equivalência. Quem é o zero? quem é o inverso aditivo de um elemento $[(m, n)]$? Quem é a unidade?

d) Defina a função $\imath : \mathbb{N} \to \mathbb{Z}$ dada por $\imath(n) = [(n, 0)]$. Mostre que $\imath(m+n) = \imath(m)+\imath(n)$ e $\imath(m.n) = \imath(m).\imath(n)$. mostre também que $\imath$ é injetiva.

e) Mostre que todo elemento $[(m, n)] \in \mathbb{Z}$ pode ser escrito como $[(m, n)] = \imath(m) - \imath(n)$. Então, por um abuso de linguagem, podemos ver um número inteiro como a diferença de dois números naturais.

10) Considere a seguinte relação $\sim$ no conjunto $\mathbb{Z} \times \mathbb{Z}^*$, onde $\mathbb{Z}^*$ é o conjunto dos inteiros não nulos: $(m, n) \sim (p, q)$ se $m.q = n.p$.

a) Mostre que, de fato, $\sim$ é relação de equivalência.

b) Descreva a classe de equivalência $[(m, n)]$ (comece a denotar a classe $[(m, n)]$ como $\frac{m}{n}$, sim, é uma fração).

c) Mostre que o conjunto quociente $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ (sim, são os racionais) é um corpo, com as operações

$$\frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq}, \qquad \frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}.$$

Note que, primeiramente tem que mostrar que as operações estão bem definidas, isto é independem de representante na classe de equivalência. Quem é o zero? Quem é o inverso aditivo de um elemento $\frac{m}{n}$? Quem é a unidade? Quem é o inverso multiplicativo de um elemento $\frac{m}{n}$?

d) Defina a função $\imath : \mathbb{Z} \to \mathbb{Q}$ dada por $\imath(n) = \frac{n}{1}$. Mostre que $\imath(m + n) = \imath(m) + \imath(n)$ e $\imath(m.n) = \imath(m).\imath(n)$. Mostre também que $\imath$ é injetiva.

e) Mostre que todo elemento $\frac{m}{n} \in \mathbb{Q}$ pode ser escrito como $\frac{m}{n} = (\imath(m))(\imath(n))^{-1}$. Então, por um abuso de linguagem, podemos ver um número racional como a razão entre dois números inteiros. Mostre finalmente que dado qualquer número racional $\frac{m}{n} \in \mathbb{Q}$ podemos escolher, sem perda de generalidade, o denominador $n > 0$.