Gabarito da Prova 2
MAT231 -1o semestre 2020

1. Sejam A um anel e $a \in A$ e considere o seguinte conjunto

$$S_a = \{x \in A : ax = xa\}$$

(a) Mostre que S_a é um subanel de A (indique as propriedades utilizadas)

Vamos provar que S_a é subanel de A. Note que S_a é não vazio porque claramente $a \in S_a$. É suficiente demonstrar três itens:

- Se $b, b' \in S_a$, então $b + b' \in S_a$:
  De fato, temos que:

$$\begin{aligned} a(b+b') &= ab + ab' && \text{(pela distributividade)} \\ &= ba + b'a && \text{(porque } b, b' \in S_a\text{)} \\ &= (b+b')a && \text{(pela distributividade)} \end{aligned}$$

  Portanto $b + b' \in S_a$ por definição.
- Se $b, b' \in S_a$, então $b.b' \in S_a$:
  Temos que:

$$\begin{aligned} a(bb') &= (ab)b' && \text{(pela associatividade)} \\ &= (ba)b' && \text{(porque } b \in S_a\text{)} \\ &= b(ab') && \text{(pela associatividade)} \\ &= b(b'a) && \text{(porque } b' \in S_a\text{)} \\ &= (bb')a && \text{(pela associatividade)} \end{aligned}$$

  Portanto $bb' \in S_a$ por definição.
- Se $b \in S_a$, então $-b \in S_a$:
  Temos que:

$$\begin{aligned} a(-b) &= -(ab) && \text{(pelo ex. 1b da Lista Unificada)} \\ &= -(ba) && \text{(porque } b \in S_a\text{)} \\ &= (-b)a && \text{(pelo ex. 1b da Lista Unificada)} \end{aligned}$$

  Portanto $-b \in S_a$ por definição.

(b) Se $A = M_2(\mathbb{R})$ e $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, descreva S_a.

Suponha que b $= \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{R})$. Então $b \in S_a \Leftrightarrow ab = ba \Leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ z & 0 \end{pmatrix} \Leftrightarrow y, z = 0$. Com isso acabamos de provar que:

$$S_a = \left\{ \begin{pmatrix} x & 0 \\ 0 & w \end{pmatrix} \in M_2(\mathbb{R}) : x, w \in \mathbb{R} \right\}$$

(c) O conjunto S_a é um ideal de A?

Em geral, não é ideal. Suponha, por absurdo, que sempre seja. No exemplo do item b) acima, temos que $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ pertence a S_a (basta tomar $x = 1$ e $w = 0$), e portanto, como S_a é ideal, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ também pertence a S_a. Mas esse produto é igual a $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, que não é uma matriz diagonal, contrariando a descrição feita no item b). Portanto S_a não é um ideal no exemplo acima.

2. Mostre que todo corpo é um domínio de integridade. Vale a recíproca?

Seja F um corpo. Vamos mostrar que F é um domínio de integridade. Claramente, porque F é um corpo, em particular é comutativo e tem unidade. Resta ver então que não tem divisores de zero. Sejam $a, b \in F$ com $ab = 0$. Se $a = 0$, acabou, então suponha $a \neq 0$. Então, como F é corpo, a tem inverso a^{-1}. Daí $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}.0 = 0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow 1.b = 0 \Rightarrow b = 0$. Portanto ou $a = 0$ ou $b = 0$, provando que F não tem divisores de zero.

Não vale porém que todo domínio de integridade seja um corpo. Um contraexemplo é o anel $\mathbb{Z}$ dos números inteiros. Sabemos que $\mathbb{Z}$ é comutativo, tem unidade e não tem divisores de zero, porém os únicos elementos que têm inverso são 1 e -1.

3. Sejam $f : A \to B$ um homomorfismo de anéis e J um ideal de B. Mostre que $I = f^{-1}(J) = \{x \in A : f(x) \in J\}$ é um ideal de A.

Vamos provar que $f^{-1}(J)$ é um ideal de A. Como f é um homomorfismo, $f(0) = 0 \in J \Rightarrow 0 \in f^{-1}(J)$, mostrando que $f^{-1}(J)$ é não vazio. É suficiente agora mostrar três propriedades:

- Se $a, b \in f^{-1}(J)$, então $a + b \in f^{-1}(J)$:
  Como $a, b \in f^{-1}(J)$, $f(a), f(b) \in J$. Como J é ideal, $f(a) + f(b) \in J$. Como f é homomorfismo, $f(a + b) = f(a) + f(b) \in J$. Logo $a + b \in f^{-1}(J)$ pela definição.
- Se $a \in f^{-1}(J)$, então $-a \in f^{-1}(J)$:
  Como $a \in f^{-1}(J)$, $f(a) \in J$. Como J é ideal, $-f(a) \in J$. Como f é homomorfismo, $f(-a) = -f(a) \in J$. Logo $-a \in f^{-1}(J)$ pela definição.
- Se $a \in f^{-1}(J)$ e $b \in A$, então $ab, ba \in f^{-1}(J)$:
  Como $a \in f^{-1}(J)$, $f(a) \in J$. Como J é ideal, $f(a)f(b) \in J$ e $f(b)f(a) \in J$. Como f é homomorfismo, tanto $f(ab) = f(a)f(b)$ quanto $f(ba) = f(b)f(a)$ pertencem a J. Logo ab e ba pertencem a $f^{-1}(J)$ por definição.

4. Decreva todos os possíveis homomorfismos $f : \mathbb{C} \to \mathbb{C}$. **Nota.** Utilize o fato de que se $f : \mathbb{C} \to \mathbb{C}$ for um homomorfismo não nulo, então $f(r) = r$ para todos os números reais r.

Sabemos que a função nula $f : \mathbb{C} \to \mathbb{C}$ é sempre um homomorfismo, então vamos supor que $f : \mathbb{C} \to \mathbb{C}$ seja um homomorfismo não nulo.

Seja $z = a + bi \in \mathbb{C}$ um número complexo qualquer, com $a, b \in \mathbb{R}$. Então, usando o fato escrito no enunciado, $f(a) = a$ e $f(b) = b$. Como f é homomorfismo,

$$f(z) = f(a + bi) = f(a) + f(b).f(i) = a + b.f(i) \tag{1}$$

Isso indica que se determinarmos quanto vale $f(i)$, então saberemos $f(z)$ para qualquer z.

Sabemos que $i^2 = -1$. Então usando novamente que f é homomorfismo e o fato do enunciado, temos que $f(i^2) = f(-1) \Rightarrow f(i)^2 = -1$. Logo $f(i)$ é raiz da equação $t^2 = -1$, ou seja, $f(i) = i$ ou $f(i) = -i$. Combinando essa afirmação com a relação 1 acima, temos que ou $f(z) = a + bi = z$ ou $f(z) = a + b(-i) = \overline{z}$. ($\overline{z}$ denota o conjugado de z). Concluímos que só existem três homomorfismos $f : \mathbb{C} \to \mathbb{C}$, que estão descritos abaixo:

$$
\begin{aligned}
&f_1 : \mathbb{C} \to \mathbb{C} \\
&\qquad f_1(z) = 0 \text{ para todo } z \in \mathbb{C} \\
&f_2 : \mathbb{C} \to \mathbb{C} \\
&\qquad f_2(z) = z \text{ para todo } z \in \mathbb{C} \\
&f_3 : \mathbb{C} \to \mathbb{C} \\
&\qquad f_3(z) = \overline{z} \text{ para todo } z \in \mathbb{C}
\end{aligned}
$$

(A rigor, seria preciso mostrar que f_2 e f_3 são de fato homomorfismos, mas essa verificação é direta).

5. Seja $A = \mathbb{R}[t]$ o anel de polinômios com coeficientes em $\mathbb{R}$ e seja J o ideal de A formado pelos polinômios que são múltiplos de $p(t) = 3t^2 - 2t$, isto é, $J = (3t^2 - 2t)\mathbb{R}[t]$. Considere o quociente B do anel A pelo ideal J, isto é, o anel $B = \mathbb{R}[t]/(3t^2 - 2t)\mathbb{R}[t]$.

   (a) Descreva os elementos de B.

   Primeiramente, seja $f(t) \in \mathbb{R}[t]$ um polinômio de grau maior ou igual a 2. Pelo algoritmo da divisão em $\mathbb{R}[t]$, existem $q(t), r(t) \in \mathbb{R}[t]$ com $r(t) = 0$ ou $\operatorname{grau} r(t) < \operatorname{grau} p(t) = 2$ tais que $f(t) = p(t)q(t) + r(t)$. Tomando as classes de equivalência no quociente B, temos que $\overline{f(t)} = \overline{p(t)q(t) + r(t)} = \overline{p(t)}.\overline{q(t)} + \overline{r(t)} = \overline{0}.\overline{q(t)} + \overline{r(t)} = \overline{r(t)}$. Ou seja, dado $f(t)$ qualquer, existe $r(t)$ nulo ou de grau menor ou igual a 1 tais que as classes de equivalência de $f(t)$ e de $r(t)$ são iguais no quociente B.

   Por outro lado, suponha que $f(t)$ e $g(t)$ tenham a mesma classe de equivalência no quociente B, onde $f(t)$ e $g(t)$ são polinômios distintos nulos ou de grau menor ou igual a 1. Então $f(t) - g(t)$ seria um polinômio não nulo de grau menor ou igual a 1, e por outro lado seria um múltiplo não nulo de $p(t)$. Porém um múltiplo não nulo de $p(t)$ tem grau pelo menos 2, absurdo. Concluímos dessa discussão que não há como dois polinômios distintos nulos ou de grau menor ou igual a 1 terem a mesma classe de equivalência no quociente B.

   Resumindo, o quociente $B = \mathbb{R}[t]/p(t)\mathbb{R}[t]$ é igual ao conjunto das classes de equivalência dos polinômios de grau menor ou igual a 1 e do polinômio 0. Além disso, tais classes são distintas entre si.

   (b) Encontre em B as classes de equivalência dos elementos $f(t) = 6t^3 - t^2 - 2t + 2$ e $(f(t))^2$.

   Note que $f(t) = 6t^3 - t^2 - 2t + 2 = 2t(3t^2 - 2t) + (3t^2 - 2t) + 2 = (2t+1)(3t^2 - 2t) + 2$. (Esta conta também pode ser feita pelo algoritmo da divisão). Portanto $f(t) - 2 = (2t + 1)p(t)$ é um múltiplo de $p(t)$, e portanto $f(t)$ e 2 estão na mesma classe de equivalência no quociente B. Portanto $\overline{f(t)} = \overline{2}$ em B.

   Disso segue que $\overline{(f(t))^2} = \overline{f(t)}^2 = \overline{2}^2 = \overline{4}$. Logo $\overline{(f(t))^2} = \overline{4}$ em B.

   (c) Exiba dois polinômios distintos de grau 4 que pertençam à classe $\overline{t}$ no quociente B.

Temos por exemplo que $p(t).t^2 = 3t^4 - 2t^3 = (3t^4 - 2t^3 + t) - t$. Isso prova que $3t^4 - 2t^3 + t$ e t diferem por um múltiplo de $p(t)$, e que assim $\overline{3t^4 - 2t^3 + t} = \overline{t}$ em B. Outra possibilidade é $p(t)(2t^2) = 6t^4 - 4t^3 = (6t^4 - 4t^3 + t) - t$. Portanto, da mesma forma que antes, $\overline{6t^4 - 4t^3 + t} = \overline{t}$ em B.