Gabarito da Prova Substitutiva
MAT231 -1o semestre 2020

1. Decida se os polinômios abaixo são irredutíveis e, quando não o for, decomponha-o em irredutíveis.

   (a) $f(t) = 8t^7 - 30t^4 + 60t^3 - 90t + 45$ em $\mathbb{Q}[t]$

   Podemos usar o Critério de Eisenstein com o primo $p = 5$. De fato, 5 não divide o coeficiente dominante, que é 8, divide todos os outros coeficientes, que são, em ordem decrescente de grau, $0, 0, -30, 60, 0, -90$ e 45, e $5^2 = 25$ não divide o coeficiente de grau 0, que é 45. Logo, pelo Critério de Eisenstein, segue que $f(t)$ é irredutível sobre $\mathbb{Q}[t]$.

   (b) $g(t) = t^5 - 4t^3 - t^2 + 4$ em $\mathbb{Q}[t]$, em $\mathbb{R}[t]$ e em $\mathbb{C}[t]$

   Pelo Teste da Raiz Racional, as raízes racionais do polinômio g, se existirem, são inteiras e dividem o coeficiente de grau 0, que é 4. Logo as raízes racionais, se existirem, só podem ser $-4, -2, -1, 1, 2$ ou 4. No caso, $g(1) = g(2) = g(-2) = 0$, ou seja, 1,2 e -2 são raízes de g. Logo tanto $(t-1)$ quanto $(t-2)$ e $(t+2)$ dividem $g(t)$, e portanto $(t-1)(t-2)(t+2) = t^3 - t^2 - 4t + 4$ divide $g(t)$. Efetuando a divisão, temos que $g(t) = (t^3 - t^2 - 4t + 4)(t^2 + t + 1)$. Note que $(t-1)$, $(t-2)$ e $(t+2)$ são todos irredutíveis (porque têm grau 1) e (t^2+t+1) é irredutível sobre $\mathbb{R}$ porque tem discriminante igual a -3, que é negativo. Logo $g(t)$ é redutível sobre $\mathbb{Q}$ e sobre $\mathbb{R}$ e sua decomposição em irredutíveis é $g(t) = (t-1)(t-2)(t+2)(t^2+t+1)$ em ambos esses conjuntos. Quanto aos complexos, temos que $(t^2+t+1) = (t-(\frac{-1+i\sqrt{3}}{2}))(t-(\frac{-1-i\sqrt{3}}{2}))$. (Isso pode ser visto usando a fórmula de Bháskara). Logo g é redutível sobre $\mathbb{C}$ e sua decomposição em irredutíveis nesse caso é $g(t) = (t-1)(t-2)(t+2)(t-(\frac{-1+i\sqrt{3}}{2}))(t-(\frac{-1-i\sqrt{3}}{2}))$.

   (c) $h(t) = t^6+t^5+t^4+4t^2+4t+4$ em $\mathbb{R}[t]$ e em $\mathbb{C}[t]$ (Obs. $1+i$ e $-1+i$ são raízes de $h(t)$).

   Como h tem coeficientes reais e tem $1+i$ e $-1+i$ como raízes, os conjugados dessas raízes, que são $1-i$ e $-1-i$, também são raízes de h. Portanto $(t-(1+i))(t-(1-i))(t-(-1+i))(t-(-1-i)) = (t^2-2t+2)(t^2+2t+2) = (t^4+4)$ divide $h(t)$. Efetuando a divisão, temos que $h(t) = (t^4+4)(t^2+t+1)$. Note que t^2-2t+2,t^2+2t+2 e t^2+t+1 são todos irredutíveis sobre $\mathbb{R}$, pois seus discriminantes, que são respectivamente -4,-4 e -3, são negativos. Logo $h(t)$ é redutível sobre $\mathbb{R}[t]$ e sua decomposição em irredutíveis nesse conjunto é $h(t) = (t^2 - 2t + 2)(t^2 + 2t + 2)(t^2 + t + 1)$. Vejamos sobre os complexos. Já sabemos que $(t^2 - 2t + 2)(t^2 + 2t + 2) = (t - (1 + i))(t - (1 - i))(t - (-1 + i))(t - (-1 - i))$. Usando a Fórmula de Bháskara, as raízes de t^2+t+1 são $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$ e $-\frac{1}{2}-i\frac{\sqrt{3}}{2}$. Logo $t^2+t+1 = (t-(-\frac{1}{2}+i\frac{\sqrt{3}}{2}))(t-(-\frac{1}{2}-i\frac{\sqrt{3}}{2}))$. Concluímos que $h(t)$ é redutível sobre $\mathbb{C}[t]$ e sua decomposição em irredutíveis é $h(t) = (t-(1+i))(t-(1-i))(t-(-1+i))(t-(-1-i))(t-(-\frac{1}{2}+i\frac{\sqrt{3}}{2}))(t-(-\frac{1}{2}-i\frac{\sqrt{3}}{2}))$.

2. (a) Mostre que em um domínio de integridade, a equação $x^2 - x$ possui apenas duas raízes (0 e 1).

   Suponha que em A é um domínio de integridade, e consideremos a equação $x^2-x = 0$, onde $x \in A$. Claramente, como $0^2 = 0$ e $1^2 = 1$, 0 e 1 são raízes dessa equação. Vejamos que não há outras. Se $x^2 - x = 0$, então $x(x-1) = 0$, e como A é domínio de integridade, segue que ou $x = 0$ ou $x - 1 = 0$. No primeiro caso, $x = 0$, e no segundo, $x = 1$. Logo 0 e 1 são de fato as únicas raízes.

   (b) Exiba um anel onde a equação $x^2 - x$ tenha mais do que 2 raízes.

Considere o anel $\mathbb{Z}_6$ dos inteiros módulo 6. Então, como já vimos no item a), $\overline{0}$ e $\overline{1}$ são raízes de $x^2 - x = 0$, mas neste anel também temos as raízes $\overline{3}$ e $\overline{4}$, já que $\overline{3}^2 = \overline{9} = \overline{3}$ e $\overline{4}^2 = \overline{16} = \overline{4}$. Não há outras raízes além das já mencionadas. Logo a equação $x^2 - x = 0$ tem quatro raízes em $\mathbb{Z}_6$.

3. Sejam A um anel e I um ideal de A. Dizemos que I é maximal se toda vez que tivermos $I \subseteq J \subseteq A$ com J ideal de A, então $J = I$ ou $J = A$. Mostre que se I for um ideal maximal de $\mathbb{Z}$, então existe um primo $p \in \mathbb{Z}$ tal que $I = p\mathbb{Z}$. (Nota. Lembre-se da caracterização dos ideais em $\mathbb{Z}$.)

   Pela caracterização dos ideais de $\mathbb{Z}$, existe $p \in \mathbb{Z}$ não negativo tal que $I = p\mathbb{Z}$. Resta provar que p é primo. Suponha por absurdo que não seja. Então existem $a, b \in \mathbb{Z}$ tais que $p = ab$ e $1 < a, b < p$. Como a divide p, todo múltiplo de p é também múltiplo de a. Logo $p\mathbb{Z} \subseteq a\mathbb{Z}$. Logo vale o seguinte: $I \subseteq a\mathbb{Z} \subseteq \mathbb{Z}$. Por hipótese, I é um ideal maximal, e por definição de ideal maximal, vale que ou $I = a\mathbb{Z}$ ou $a\mathbb{Z} = \mathbb{Z}$. Vamos dividir em casos:

   - Se $I = a\mathbb{Z}$, então $a \in a\mathbb{Z} = I = p\mathbb{Z}$, ou seja, existe $x \in \mathbb{Z}$ tal que $a = px$. Logo $a = abx$. Como $a > 1$, $bx = 0$, logo ou $b = 0$ ou $x = 0$. Se $b = 0$, então $p = ab = a0 = 0$, falso. Se $x = 0$, então $a = px = p0 = 0$, também falso. Logo temos um absurdo.
   - Se $a\mathbb{Z} = \mathbb{Z}$, então $1 \in \mathbb{Z} = a\mathbb{Z}$, ou seja, existe $y \in \mathbb{Z}$ tal que $1 = ay$. Como $\mathbb{Z}$ é comutativo, segue que $1 = ya$ e portanto que a é inversível em $\mathbb{Z}$. Logo ou $a = 1$ ou $a = -1$, absurdo, porque $a > 1$.

   Nos dois casos, temos um absurdo, portanto p deve ser primo, concluindo a demonstração.

4. Considere os anéis $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ e $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

   (a) Mostre que $\sqrt{2} \notin \mathbb{Q}[\sqrt{3}]$.

   Suponha por absurdo que $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$. Então existem $a, b \in \mathbb{Q}$ tais que $\sqrt{2} = a + b\sqrt{3}$. Daí $(\sqrt{2})^2 = (a + b\sqrt{3})^2 \Rightarrow 2 = a^2 + 2ab\sqrt{3} + 3b^2 \Rightarrow 2 - a^2 - 3b^2 = 2ab\sqrt{3}$. Se $ab \neq 0$, então $\sqrt{3} = \frac{2-a^2-3b^2}{2ab}$, e daí, como $a, b \in \mathbb{Q}$, $\sqrt{3}$ seria racional, absurdo. Logo $ab = 0$, ou seja, ou $a = 0$ ou $b = 0$. Se $a = 0$, então $2 - a^2 - 3b^2 = 2ab\sqrt{3} \Rightarrow 2 - 3b^2 = 0 \Rightarrow b = \pm\sqrt{\frac{2}{3}}$, absurdo, porque b é racional e $\sqrt{\frac{2}{3}}$ não é. (Para provar que $\sqrt{\frac{2}{3}}$ não é racional, basta ver que esta é uma raiz do polinômio $3t^2 - 2$, que é irredutível sobre $\mathbb{Q}$ pelo Critério de Eisenstein). Portanto $a \neq 0$ e devemos ter $b = 0$. Mas daí $2 - a^2 - 3b^2 = 2ab\sqrt{3} \Rightarrow 2 - a^2 = 0 \Rightarrow a = \pm\sqrt{2}$, absurdo porque a é racional e $\sqrt{2}$ não é. Então chegamos a um absurdo de qualquer forma, provando que $\sqrt{2} \notin \mathbb{Q}[\sqrt{3}]$.

   (b) Mostre que $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{3}]$ não são isomorfos. (Obs. Para o item (b), pode usar o item (a) mesmo sem demonstrá-lo e também o fato de que se $f : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$ for um homomorfismo não nulo, então $f(r) = r$ para todos os racionais r.)

   Suponha, por absurdo, que exista um isomorfismo $f : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$. Temos que vale a seguinte relação em $\mathbb{Q}[\sqrt{2}]$: $(\sqrt{2})^2 = 2$. Aplicando f dos dois lados, temos que $f((\sqrt{2})^2) = f(2)$. Usando que f é isomorfismo e a observação do enunciado, temos que $(f(\sqrt{2}))^2 = 2$. Ou seja, $f(\sqrt{2}) \in \mathbb{Q}[\sqrt{3}]$ é raiz da equação $t^2 - 2 = 0$. Em $\mathbb{R}$, essa equação tem apenas duas raízes, $\sqrt{2}$ e $-\sqrt{2}$, e como $\mathbb{Q}[\sqrt{3}] \subseteq \mathbb{R}$, segue que a equação $t^2 - 2$ pode ter no máximo duas raízes em $\mathbb{Q}[\sqrt{3}]$, sendo essas raízes ou $\sqrt{2}$ ou $-\sqrt{2}$. Concluímos dessa discussão que $f(\sqrt{2}) = \pm\sqrt{2}$ e que portanto ou $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$ ou $-\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$. Como $\mathbb{Q}[\sqrt{3}]$ é um anel, de qualquer forma devemos

ter $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$, mas já vimos no item a) que isso é absurdo. Portanto não existe o isomorfismo f tal como acima.

5. (a) Exiba um exemplo de um corpo que tenha um número finito de elementos (isto é, um corpo finito).

   Seja $p \in \mathbb{N}$ um número primo. Consideramos o anel $\mathbb{Z}_p$ dos inteiros módulo p. Sabemos que $\mathbb{Z}_p$ tem unidade, é comutativo, e graças ao exercício 6 da Lista Unificada para a Prova 1, todo elemento não nulo admite inverso. Portanto $\mathbb{Z}_p$ é um corpo para todo primo p. Além disso, ele é finito porque possui exatamente p elementos.

   Para o que segue, seja $\mathbb{K}$ um corpo finito.

   (b) Mostre que existe um inteiro positivo n tal que se somarmos n vezes a unidade 1, o resultado será igual a 0.

   Para simplificar, vamos denotar a soma de n vezes o elemento por $n.1$, ou seja, $n.1 \doteq 1 + 1 + \ldots + 1$, onde a soma tem n parcelas. Note que a sequência 1, 2.1, 3.1, etc., é uma sequência de elementos de $\mathbb{K}$. Mas como $\mathbb{K}$ é finito, essa sequência precisará se repetir em algum momento. Logo existirão $m, m' \in \mathbb{N}$ distintos tais que $m.1 = m'.1$. Podemos supor sem perda de generalidade que $m < m'$. Note agora que, como $m < m'$, $m'.1 = m.1 + (m' - m).1$. Logo $m.1 = m'.1 = m.1 + (m' - m).1$. Cancelando $m.1$ dos dois lados, temos que $(m' - m).1 = 0$. Logo basta tomar $n = m' - m$ que obteremos $n.1 = 0$.

   (c) Mostre que se n é como no item (b) e se $x \in \mathbb{K}$, então a soma de n vezes o elemento x também é 0.

   Somando n vezes o elemento x, pela distributividade, temos que:

$$x + x + \ldots + x = x(1 + 1 + \ldots + 1) = x.0 = 0$$

   Logo a soma de n vezes o elemento x também dá 0.