Gabarito da Prova 1
MAT231 -1o semestre 2020

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

   (a) $f(t) = t^8 - 18t^4 + 30t^2 + 6t + 12$ em $\mathbb{Q}[t]$

   Podemos usar o Critério de Eisenstein com o primo $p = 3$. De fato, 3 não divide o coeficiente dominante, que é 1, divide todos os outros coeficientes, que são, em ordem decrescente de grau, $0, 0, 0, -18, 0, 30, 6$ e 12, e $3^2 = 9$ não divide o coeficiente de grau 0, que é 12. Logo, pelo Critério de Eisenstein, segue que $f(t)$ é irredutível sobre $\mathbb{Q}[t]$.

   (b) $g(t) = t^4 - 1$ 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 1. Logo as raízes racionais, se existirem, só podem ser ou 1 ou -1. No caso, $g(1) = g(-1) = 0$, ou seja, 1 e -1 são raízes de g. Logo tanto $(t-1)$ quanto $(t+1)$ dividem $g(t)$, e portanto $t^2 - 1 = (t-1)(t+1)$ divide $g(t)$. Efetuando a divisão, temos que $g(t) = (t^2 - 1)(t^2 + 1) = (t-1)(t+1)(t^2+1)$. Note que $(t-1)$ e $(t+1)$ são ambos irredutíveis (porque têm grau 1) e (t^2+1) é irredutível sobre $\mathbb{R}$ porque tem discriminante igual a -4, que é negativo. Logo $g(t)$ é redutível sobre $\mathbb{Q}$ e sobre $\mathbb{R}$ e sua decomposição em irredutíveis é $g(t) = (t-1)(t+1)(t^2+1)$ em ambos esses conjuntos. Quanto aos complexos, temos que $(t^2+1) = (t-i)(t+i)$. Logo g é redutível sobre $\mathbb{C}$ e sua decomposição em irredutíveis nesse caso é $g(t) = (t-1)(t+1)(t-i)(t+i)$.

   (c) $h(t) = t^4 - 3t^3 + 3t^2 + 2t + 6$ em $\mathbb{R}[t]$ e em $\mathbb{C}[t]$ (Obs. $2 + i\sqrt{2}$ é raiz de $h(t)$).

   Como h tem coeficientes reais e tem $2+i\sqrt{2}$ como raiz, o conjugado de $2+i\sqrt{2}$, que é $2-i\sqrt{2}$, também é raiz de h. Portanto $(t-(2+i\sqrt{2}))(t-(2-i\sqrt{2})) = t^2 - 4t + 6$ divide $h(t)$. Efetuando a divisão, temos que $h(t) = (t^2-4t+6)(t^2+t+1)$. Note que tanto t^2-4t+6 quanto t^2+t+1 são irredutíveis sobre $\mathbb{R}$, pois seus discriminantes, que são respectivamente -8 e -3, são negativos. Logo $h(t)$ é redutível sobre $\mathbb{R}[t]$ e sua decomposição em irredutíveis nesse conjunto é $h(t) = (t^2-4t+6)(t^2+t+1)$. Vejamos sobre os complexos. Já sabemos que $t^2 - 4t + 6 = (t-(2+i\sqrt{2}))(t-(2-i\sqrt{2}))$. 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 $h(t) = (t-(2+i\sqrt{2}))(t-(2-i\sqrt{2}))(t-(-\frac{1}{2}+i\frac{\sqrt{3}}{2}))(t-(-\frac{1}{2}-i\frac{\sqrt{3}}{2}))$.

2. Enuncie o algoritmo da divisão em $\mathbb{C}[t]$. Faça a divisão de $f(t) = (-1+i)t^4+2t^3+4it^2-3i$ por $g(t) = it^2 + 2t + 4$.

   O algoritmo da divisão em $\mathbb{C}[t]$ pode ser enunciado da seguinte forma:

   Teorema. *Sejam $f(t), g(t)$ dois polinômios em $\mathbb{C}[t]$, com $g(t) \neq 0$. Então existem polinômios $q(t), r(t) \in \mathbb{C}[t]$ únicos com* grau$(r(t)) <$ grau$(g(t))$ *ou $r(t) = 0$ tais que $f(t) = g(t)q(t) + r(t)$.*

   Lembrando que a divisão de polinômios em $\mathbb{C}[t]$ é armada e efetuada da mesma forma como em $\mathbb{Q}[t]$, só que os coeficientes são complexos. Temos que

$$
\begin{array}{rrrrr|l}
(-1+i)t^4 & +2t^3 & +4it^2 & & -3i & it^2+2t+4 \\
\cline{6-6}
-(-1+i)t^4 & -(2i+2)t^3 & -(4i+4)t^2 & & & (i+1)t^2-2t \\
\cline{1-5}
 & -2it^3 & -4t^2 & & -3i & \\
 & 2it^3 & +4t^2 & +8t & & \\
\cline{2-4}
 & & & 8t & -3i & \\
\cline{4-5}
\end{array}
$$

Como o resto tem grau menor que o divisor, o algoritmo termina. Logo, se $q(t) = (i+1)t^2-2t$ e $r(t) = 8t-3i$, temos que $f(t) = g(t)q(t)+r(t)$, com grau$(r(t)) <$ grau$(g(t))$, tal como no enunciado do algoritmo da divisão.

3. Assuma que A seja um conjunto com uma operação $\circ$ que seja comutativa, associativa, que tenha um elemento neutro que indicaremos por e e que tenha a seguinte propriedade: dado um elemento $a \in A$, existe $\overline{a} \in A$ tal que $a \circ \overline{a} = e$. Mostre a lei do cancelamento em A, isto é, mostre que se $a \circ b = a \circ c$, onde a, b e c estão em A, então $b = c$. (Obs. Indique as propriedades usadas em cada passo).

   Sejam $a, b, c \in A$ tais que $a \circ b = a \circ c$. Provaremos que $b = c$. Por hipótese, existe um elemento $\overline{a} \in A$ tal que $a \circ \overline{a} = e$. Temos que:

$$
\begin{aligned}
a \circ b = a \circ c &\Rightarrow \overline{a} \circ (a \circ b) = \overline{a} \circ (a \circ c) && \text{(porque } \circ \text{ é uma operação)} \\
&\Rightarrow (\overline{a} \circ a) \circ b = (\overline{a} \circ a) \circ c && \text{(usando a associatividade de } \circ) \\
&\Rightarrow (a \circ \overline{a}) \circ b = (a \circ \overline{a}) \circ c && \text{(usando a comutatividade de } \circ) \\
&\Rightarrow e \circ b = e \circ c && \text{(usando a hipótese)} \\
&\Rightarrow b = c && \text{(porque } e \text{ é um elemento neutro de } \circ)
\end{aligned}
$$

   Isso conclui a demonstração.

4. Considere o conjunto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ com operações:

$$
\begin{aligned}
(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\
(a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2}
\end{aligned}
$$

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

   Como claramente $\sqrt{2} = 0 + 1\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, se por absurdo valesse que $\mathbb{Q} = \mathbb{Q}[\sqrt{2}]$, então $\sqrt{2} \in \mathbb{Q}$. Isso dá um absurdo, porque $\sqrt{2}$ não é racional. O fato de que $\sqrt{2}$ é irracional, por sua vez, segue do exercício 4 da Lista de Exercícios Unificada. No entanto, apenas para não depender desse exercício, para concluir este item vamos provar que $\sqrt{2}$ é irracional de uma maneira alternativa, usando o Critério de Eisenstein. Se $\sqrt{2}$ fosse racional, o polinômio $t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$ seria redutível sobre os racionais, absurdo, porque usando o Critério de Eisenstein com o primo $p = 2$, vemos que $t^2 - 2$ é irredutível sobre $\mathbb{Q}[t]$. De fato, 2 não divide o coeficiente dominante, que é 1, 2 divide os outros coeficientes, que são 0 e -2, e $2^2 = 4$ não divide o ceficiente de grau 0, que é -2.

(b) Encontre o elemento inverso de $3-\sqrt{2}$ (isto é, encontre $c+d\sqrt{2}$ em $\mathbb{Q}[\sqrt{2}]$ tal que $(3-\sqrt{2})(c+d\sqrt{2})=1$).

Para encontrar o inverso, vamos entender que $3-\sqrt{2}$ é um número real e usar a técnica por vezes chamada de *racionalização*:

$$\frac{1}{3-\sqrt{2}}=\frac{(3+\sqrt{2})}{(3-\sqrt{2})(3+\sqrt{2})}=\frac{3+\sqrt{2}}{9-2}=\frac{3+\sqrt{2}}{7}=\frac{3}{7}+\frac{1}{7}\sqrt{2}$$

Isso foi feito apenas para encontrar o inverso, mas, a rigor, devemos provar que este é, de fato, um inverso:

$$(3-\sqrt{2})(\frac{3}{7}+\frac{1}{7}\sqrt{2})=(3.\frac{3}{7}+2.(-1).\frac{1}{7})+(3.\frac{1}{7}+(-1).\frac{3}{7})\sqrt{2}=\frac{9-2}{7}+\frac{3-3}{7}\sqrt{2}=1$$

Como a multiplicação em $\mathbb{Q}[\sqrt{2}]$ é comutativa, isso prova que o inverso de $3-\sqrt{2}$ é $\frac{3}{7}+\frac{1}{7}\sqrt{2}$.

(c) Ache o inverso de um elemento não nulo $a+b\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$ em termos de a e b.

Como $a+b\sqrt{2}\neq 0$, também vale que $a-b\sqrt{2}\neq 0$ e portanto $(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2\neq 0$. Novamente, usamos o processo de racionalização para encontrar a fórmula:

$$\frac{1}{a+b\sqrt{2}}=\frac{(a-b\sqrt{2})}{(a+b\sqrt{2})(a-b\sqrt{2})}=\frac{a-b\sqrt{2}}{a^2-(b\sqrt{2})^2}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}$$

Agora procedemos formalmente para provar que este é, de fato, um inverso de $a+b\sqrt{2}$:

$$\begin{aligned}(a+b\sqrt{2})&(\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2})\\&=(a.\frac{a}{a^2-2b^2}+2b.\frac{-b}{a^2-2b^2})+(a.\frac{-b}{a^2-2b^2}+b.\frac{a}{a^2-2b^2})\sqrt{2}\\&=\frac{a^2-2b^2}{a^2-2b^2}+\frac{-ab+ba}{a^2-2b^2}\sqrt{2}=1\end{aligned}$$

E como a multiplicação de $\mathbb{Q}[\sqrt{2}]$ é comutativa, $(\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2})(a+b\sqrt{2})=1$. Portanto o elemento não-nulo $a+b\sqrt{2}$ tem inverso $\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}$.

(d) Mostre que $\mathbb{Q}[\sqrt{2}]$ não tem divisores de zero.

Suponha por absurdo que $\mathbb{Q}[\sqrt{2}]$ tenha divisores de zero. Então existem dois elementos $a+b\sqrt{2}, c+d\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$, ambos não-nulos, tais que $(a+b\sqrt{2})(c+d\sqrt{2})=0$. Pelo item c), como $a+b\sqrt{2}\neq 0$, existe $e+f\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$ tal que $(e+f\sqrt{2})(a+b\sqrt{2})=1$. Daí:

$$\begin{aligned}&(a+b\sqrt{2})(c+d\sqrt{2})=0\\&\Rightarrow(e+f\sqrt{2})((a+b\sqrt{2})(c+d\sqrt{2}))=(e+f\sqrt{2}).0\\&\Rightarrow((e+f\sqrt{2})(a+b\sqrt{2}))(c+d\sqrt{2})=(e+f\sqrt{2}).0\\&\Rightarrow 1.(c+d\sqrt{2})=0\\&\Rightarrow c+d\sqrt{2}=0\end{aligned}$$

Mas isso é absurdo, porque já supusemos antes que $c + d\sqrt{2} \neq 0$. Logo $\mathbb{Q}[\sqrt{2}]$ não tem divisores de zero.