Gabarito da segunda prova de Álgebra 2 – 2021-1 – 28/10/2021.

Neste gabarito, a, b, c e p são números não negativos que dependem do número de matrícula do/a aluno/a, e $p \in \{3, 5, 7\}$.

1. (1 ponto) Fatore o polinômio $P(X) := X^3 + pX^2 - X - p$ em fatores irredutíveis em $\mathbb{Z}[X]$.

   Temos $P(X) = X^2(X + p) - (X + p) = (X^2 - 1)(X + p) = (X - 1)(X + 1)(X + p)$.

2. (1 ponto) Fatore $(p^2 + 1)(14 - p)$ em fatores irredutíveis em $\mathbb{Z}[i]$.

   Se $p = 3$ temos $10 \cdot 11 = 2 \cdot 5 \cdot 11$. Temos $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$, 11 é irredutível sendo um primo congruente a 3 módulo 4. Logo a fatoração é
   $$(1 + i) \cdot (1 - i) \cdot (1 + 2i) \cdot (1 - 2i) \cdot 11.$$

   Se $p = 5$ temos $26 \cdot 9 = 2 \cdot 3^2 \cdot 13$. Temos $2 = (1 + i)(1 - i)$, 3 é irredutível sendo um primo congruente a 3 módulo 4, e $13 = (2 + 3i)(2 - 3i)$. Logo a fatoração é
   $$(1 + i) \cdot (1 - i) \cdot 3^2 \cdot (2 + 3i) \cdot (2 - 3i).$$

   Se $p = 7$ temos $50 \cdot 7 = 2 \cdot 5^2 \cdot 7$. Temos $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$ e 7 é irredutível sendo um primo congruente a 3 módulo 4. Logo a fatoração é
   $$(1 + i) \cdot (1 - i) \cdot (1 + 2i)^2 \cdot (1 - 2i)^2 \cdot 7.$$

3. (1 ponto) Mostre que $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}((b + 2)i + \sqrt{3})$.

   Sejam $t := b + 2$ e $\alpha := ti + \sqrt{3} = ti + \sqrt{3}$. A inclusão $\supseteq$ é clara pois α é obtido a partir de i e $\sqrt{3}$ por meio de operações de corpo, sendo $\alpha = ti+\sqrt{3}$ e $t \in \mathbb{Z}$. Mostraremos agora a inclusão $\subseteq$. Temos $\alpha^2 = -t^2 + 3 + 2ti\sqrt{3}$, logo $i\sqrt{3} = (\alpha^2 + t^2 - 3)/2t \in \mathbb{Q}(\alpha)$. Como $ti + \sqrt{3}$ também pertence a $\mathbb{Q}(\alpha)$, obtemos que
   $$\mathbb{Q}(\alpha) \ni (ti + \sqrt{3})i\sqrt{3} = -t\sqrt{3} + 3i,$$
   logo
   $$\mathbb{Q}(\alpha) \ni \frac{ti + \sqrt{3}}{t} - \frac{-t\sqrt{3} + 3i}{3} = (1/t + t/3)\sqrt{3}$$
   Como $1/t+t/3 = (3+t^2)/(3t)$ é um número racional não nulo, deduzimos que $\sqrt{3} \in \mathbb{Q}(\alpha)$. Logo $i = (\alpha - \sqrt{3})/t \in \mathbb{Q}(\alpha)$ também.

4. (1 ponto) Seja $P(X) := X^5 + 1 \in \mathbb{F}_7[X]$. Seja F uma extensão de $\mathbb{F}_7$ e seja $\alpha \in F$ tal que $P(\alpha) = 0$ e $\alpha \neq -1$. Seja $K := \mathbb{F}_7(\alpha) \subseteq F$. Diga se α é um gerador do grupo multiplicativo cíclico $K - \{0\}$. [Dica: Tem como responder sem ter que fatorar $P(X)$.]

Como $\alpha^5 = -1$, temos $\alpha^{10} = 1$, logo a ordem de α é 1, 2, 5 ou 10. Se α fosse gerador de $K - \{0\}$ então teriamos $o(\alpha) + 1 = |K|$, uma potência de 7. Mas $1 + 1 = 2$, $2 + 1 = 3$, $5 + 1 = 6$ e $10 + 1 = 11$ não são potências de 7, logo $\langle\alpha\rangle \neq K - \{0\}$.

5. (2 pontos) Seja

$$\alpha := \sqrt{2 + \sqrt{10}} \in \mathbb{R}_{>0}.$$

   (a) Calcule $|\mathbb{Q}(\alpha) : \mathbb{Q}|$.
   Temos $\alpha^2 = 2 + \sqrt{10}$, logo α é raiz de $(X^2 - 2)^2 - 10 = X^4 - 4X^2 - 6$, irredutível pelo critério de Eisenstein aplicado ao primo 2. Segue que $P(X)$ é o polinômio minimal de α sobre $\mathbb{Q}$.

   (b) Seja $E \subseteq \mathbb{C}$ o corpo de decomposição do polinômio minimal de α sobre $\mathbb{Q}$. Calcule $|E : \mathbb{Q}|$.
   As raízes de $P(X) = X^4 - 4X^2 - 6$ são $\pm\alpha$ e $\pm\beta$ onde $\alpha = \sqrt{2 + \sqrt{10}}$, $\beta := i\sqrt{\sqrt{10} - 2}$. Observe que $\alpha^2 - 2 = \sqrt{10}$, logo $\beta^2 = 2 - \sqrt{10} = 2 - (\alpha^2 - 2)$. Segue que β é raiz de $X^2 + \alpha^2 - 4 \in \mathbb{Q}(\alpha)[X]$. Segue que $|\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)| \leq 2$, por outro lado esse grau não é 1 pois $\beta \notin \mathbb{Q}(\alpha)$, sendo $\beta \in \mathbb{C} - \mathbb{R}$ e $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Segue que o grau do corpo de decomposição $E = \mathbb{Q}(\alpha, \beta)$ sobre $\mathbb{Q}$ é

$$|E : \mathbb{Q}| = |E : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}| = 2 \cdot 4 = 8.$$

6. (1 pontos) Considere $K := \mathbb{Q}(\alpha)$ onde $\alpha := i\sqrt{p}$. Escreva o inverso de $\alpha + 1$ como polinômio de $\mathbb{Q}[X]$ avaliado em α.

   Temos $\alpha^2 = -p$, ou seja $\alpha^2 - 1 = -p - 1$. Segue que $(\alpha + 1)(\alpha - 1) = -p - 1$, e isso implica que $(\alpha + 1)^{-1} = -\frac{1}{p+1}(\alpha - 1)$.

7. (1 ponto) Mostre que existem dois polinômios irredutíveis $P_1(X), P_2(X) \in \mathbb{Q}[X]$ ambos de grau p e tais que $P_1(X) + P_2(X) = X + 1$.

   $P_1(X) := X^p + 3X + 3$, $P_2(X) := X^p - 2X - 2$. Critério de Eisenstein.

8. (1 ponto) Seja $\alpha \in \mathbb{C}$ uma raiz de

$$P(X) := X^7 + 7X + 6.$$

   Mostre que $\alpha \in \mathbb{Q}(\alpha^3)$.

   Seja $\beta := \alpha^3$. Temos $P(\alpha) = \alpha^7 + 7\alpha + 6 = 0$, que pode ser escrito $\alpha(\beta^2 + 7) + 6 = 0$. Segue que $\beta^2 + 7 \neq 0$ (pois caso contrário teriamos $6 = 0$, absurdo), logo $\alpha = -6/(\beta^2 + 7) \in \mathbb{Q}(\beta)$.

9. (1 ponto) Sejam E_1, E_2 duas extensões de $\mathbb{Q}$ contidas em $\mathbb{C}$. É verdade que se $|E_1 : \mathbb{Q}| = |E_2 : \mathbb{Q}|$ então os corpos E_1, E_2 são isomorfos?

   Não, por exemplo $\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(i)$. Para ver isso observe que se $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(i)$ é isomorfismo de aneis então $f(\sqrt{2})^2 = f(2) = 2$, mas $\mathbb{Q}(i)$ não contém nenhum elemento $a + ib$ cujo quadrado é 2, de fato se $(a + ib)^2 = 2$ então $a^2 - b^2 = 2$ e $2ab = 0$, que implica $a^2 = 2$ ou $-b^2 = 2$, absurdo.