Resolução da segunda prova de Introdução à Álgebra (2019-1) 05/06/2019

1. Seja I um ideal de um anel comutativo unitário A e defina $\sqrt{I}$ (o radical de I) como o conjunto dos elementos $a \in A$ tais que existe um inteiro $n \geq 1$ tal que $a^n \in I$.

   (a) Mostre que $\sqrt{I}$ é um ideal de A contendo I.

   $\sqrt{I}$ contem I porque se $a \in I$ então $a^1 = a \in I$. Se $a \in \sqrt{I}$ e $x \in A$ então $a^n \in I$ para algum inteiro $n \geq 1$ logo $(ax)^n = a^n x^n \in I$ sendo $a^n \in I$ e I ideal. Se $a, b \in \sqrt{I}$ existem $n, m \geq 1$ inteiros com $a^n, b^m \in I$ logo

   $$(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}$$

   e em cada parcela $i \geq n$ ou então $n+m-i \geq m$, logo $(a+b)^{n+m}$ é uma soma de elementos do ideal I logo pertence a I.

   (b) Dados dois ideais I, J de A defina IJ como o ideal de A gerado por $\{ij \ : \ i \in I, \ j \in J\}$. Sabemos que $IJ \subseteq I \cap J$. Mostre que

   $$\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}.$$

   É verdade que $\sqrt{IJ} = \sqrt{I}\sqrt{J}$?

   Inclusão $\subseteq$. Seja $a \in \sqrt{IJ}$, e seja $n \geq 1$ tal que $a^n \in IJ$. Como IJ é o ideal gerado por S e $S \subseteq I \cap J$ (sendo I e J ideais) segue que $IJ \subseteq I \cap J$, logo $a^n \in I \cap J$ e isso implica $a \in \sqrt{I} \cap \sqrt{J}$.
   Inclusão $\supseteq$. Seja $a \in \sqrt{I} \cap \sqrt{J}$, e sejam $n, m > 1$ tais que $a^n \in I$ e $a^m \in J$. Segue $a^{n+m} = a^n a^m \in IJ$, logo $a \in \sqrt{IJ}$.
   Em geral $\sqrt{IJ} \neq \sqrt{I}\sqrt{J}$ por exemplo podemos escolher $A = \mathbb{Z}$, $I = J = (2)$, neste caso $IJ = (4)$ e $\sqrt{(2)} = (2)$, $\sqrt{(4)} = (2)$.

   (c) Lembre-se que se $a, b \in A$ definimos $(a, b) = \{ax + by \ : \ x, y \in A\} \trianglelefteq A$. Sejam $A = \mathbb{Z}[X]$ e $I = (2, X)$, $J = (3, X)$. Mostre que $IJ = (6, X)$. Neste caso IJ é igual a $\{ij \ : \ i \in I, \ j \in J\}$?

   Observe que $IJ = (2, X)(3, X) = (6, 2X, 3X, X^2)$. Olhando aos geradores temos que mostrar que $6, 2X, 3X, X^2 \in (6, X)$ (claro) e que $6, X \in IJ$. É claro que $6 = 3 \cdot 2 \in IJ$. A única coisa não trivial é mostrar que $X \in IJ$. Temos $X = 3X - 2X \in IJ$ sendo $3X, 2X \in IJ$ e IJ ideal.
   Temos que $IJ \neq \{ij \ : \ i \in I, \ j \in J\}$ pois $X \in IJ$ não pode ser escrito como ij com $i \in I$ e $j \in J$. De fato se fosse

   $$X = (2A(X) + XB(X)) \cdot (3C(X) + XD(X))$$

com $A(X)$, $B(X)$, $C(X)$, $D(X)$ em $\mathbb{Z}[X]$ substituindo $X = 0$ obteriamos $6A(0)C(0) = 0$. Suponha $A(0) = 0$ (o caso $C(0) = 0$ é analogo), temos então $A(X) = XE(X)$ com $E(X) \in \mathbb{Z}[X]$ e

$$X = X(2E(X) + B(X)) \cdot (3C(X) + XD(X))$$

ou seja

$$1 = (2E(X) + B(X)) \cdot (3C(X) + XD(X))$$

e substituindo $X = 0$ obtemos $1 = 3C(0) \cdot (2E(0) + B(0))$, contradição ($C(0)$, $E(0)$ e $B(0)$ são inteiros).

2. Mostre que $K = \mathbb{F}_3[X]/(X^2 + X + 2)$ é um corpo e encontre um gerador do grupo multiplicativo cíclico $K^* = K - \{0\}$.

   K é um corpo porque o ideal (X^2+X+2) de $\mathbb{F}_3[X]$ é maximal, sendo $\mathbb{F}_3[X]$ um domínio principal e $P(X) = X^2 + X + 2$ um polinômio irredutível de $\mathbb{F}_3[X]$ (tem grau 2 e não tem raizes em $\mathbb{F}_3$). Seja $\alpha = X + I \in K$ onde $I = (P(X))$. Sabemos pela teoria que $|K| = 3^2 = 9$ e que $P(\alpha) = 0$, ou seja $\alpha^2 = 2\alpha + 1$. Temos $\alpha^4 = (2\alpha + 1)^2 = \alpha^2 + \alpha + 1 = 2 \neq 0$ logo a ordem de α não é 2 e não é 4. Sendo $|K^*| = 9 - 1 = 8$ a ordem de α divide 8, logo $o(\alpha) = 8$ e $K^* = \langle \alpha \rangle$. Ou seja α é um gerador do grupo cíclico K^*.

3. Mostre que o polinômio $X^3 + 2X + 5$ é irredutível em $\mathbb{Q}[X]$.

   Pelo lema de Gauss basta mostrar que é irredutível em $\mathbb{Z}[X]$, e para isso basta mostrar que não admite raizes racionais (porque tendo grau 3 se fosse redutível admitiria um fator de grau 1, ou seja uma raiz racional). Sendo $P(X) = X^3 + 2X + 5$ mônico, toda raiz racional é inteira, logo basta mostrar que $P(X)$ não admite raizes inteiras. As candidatas raizes inteiras são os divisores de $P(0) = 5$, ou seja ± 1 e ± 5, e $P(1) = 8 \neq 0$, $P(-1) = 2 \neq 0$, $P(5) = 140 \neq 0$, $P(-5) = -130 \neq 0$.

4. Mostre que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

   Sejam $a = \sqrt{2}$, $b = \sqrt{3}$. É claro que $a + b$ pertence a $\mathbb{Q}(a, b)$ sendo $\mathbb{Q}(a, b)$ um corpo contendo a e b, precisamos mostrar que $a, b \in \mathbb{Q}(a + b)$. Temos $(a + b)^2 = 5 + 2\sqrt{6}$ logo $\sqrt{6} \in \mathbb{Q}(a + b)$. Segue que $\sqrt{6}(a + b) = 2b + 3a \in \mathbb{Q}(a + b)$. Isso implica que $2b + 3a$ e $a + b$ pertencem a $\mathbb{Q}(a + b)$ logo $2b + 3a - 2(a + b) = a \in \mathbb{Q}(a + b)$ logo $b = (a + b) - a \in \mathbb{Q}(a + b)$.

5. Seja E/F uma extensão de corpos e seja $\alpha \in E$. Seja $f(X) \in F[X]$ um polinômio não nulo tal que $f(\alpha) = 0$. $F[X]/(f(X))$ é isomorfo a $F[\alpha]$? Lembre-se que $F[\alpha] = \{P(\alpha) \ : \ P(X) \in F[X]\}$.

   Em geral não, por exemplo $F[X]/(X^2)$ não é isomorfo a $F[0] = F$ porque $F[X]/(X^2)$ não é um corpo: o seu elemento $\alpha = X + (X^2)$ verifica $\alpha \neq 0$ e $\alpha^2 = 0$.

   Erro comum: "Seja $P(X)$ o polinômio minimal de α sobre F, então $F[X]/(P(X)) \cong F[X]/(f(X))$ se e somente se $P(X)$ e $f(X)$ são associados, ou seja $(P(X)) = (f(X))$". Isso é falso porque por exemplo

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{R}(i) = \mathbb{C} = \mathbb{R}(2i) \cong \mathbb{R}[X]/(X^2+4)$$

   e X^2+1, X^2+4 não são associados, ou seja $(X^2+1) \neq (X^2+4)$.

6. Seja $P(X) = X^4 - 3X^2 - 3 \in \mathbb{Q}[X]$.

   (a) Mostre que $P(X)$ é irredutível em $\mathbb{Q}[X]$ e admite uma raiz real u.

   $P(X)$ é irredutível em $\mathbb{Q}[X]$ pelo critério de Eisenstein. Chamando de $Y = X^2$ e resolvendo $Y^2 - 3Y - 3 = 0$ obtemos $Y = (3 \pm \sqrt{21})/2$ logo $u = \sqrt{(3+\sqrt{21})/2}$ é uma raiz real de $P(X)$.

   (b) Calcule o grau de um corpo de decomposição M de $P(X)$ sobre $\mathbb{Q}$, ou seja calcule $|M : \mathbb{Q}|$.

   Uma outra raiz de $P(X)$ é $v = i\sqrt{(\sqrt{21}-3)/2} \in \mathbb{C} - \mathbb{R}$ e $v^2 = (3-\sqrt{21})/2 = 3 - u^2$. As raizes de $P(X)$ são $u, -u, v, -v$ onde $v \in \mathbb{C}$ verifica $v^2 = 3 - u^2$, em particular o grau de v sobre $\mathbb{Q}(u)$ é menor ou igual a 2 (sendo v raiz de $X^2 - (3-u^2)$), e não é 1 sendo $v \notin \mathbb{R}$ e $\mathbb{Q}(u) \subseteq \mathbb{R}$. Pela formula do grau

$$|M : \mathbb{Q}| = |\mathbb{Q}(u)(v) : \mathbb{Q}(u)| \cdot |\mathbb{Q}(u) : \mathbb{Q}| = 2 \cdot 4 = 8.$$

7. Seja $K = \mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. Seja $P(X) = X^4 + 6X^2 + 1 \in K[X]$. Calcule o grau de um corpo de decomposição de $P(X)$ sobre K.

   Resolvendo a equação biquadratica obtemos $P(X) = (X^2-3)(X^2-5)$ e $P(X)$ não tem raizes em K. Seja α um elemento (em uma oportuna extensão F de K) tal que $\alpha^2 = 3$ (por exemplo $F = K[X]/(X^2-3)$). Segue que $(2\alpha)^2 = 12 = 5$ logo $P(X) = (X-\alpha)(X+\alpha)(X-2\alpha)(X+2\alpha)$ logo $K(\alpha)$ é um corpo de decomposição de $P(X)$ sobre K. Como X^2-3 é irredutível em $K[X]$ (tem grau 2 e não tem raizes em K), é o polinômio minimal de α sobre K logo $|K(\alpha) : K| = 2$.