Resolução 3ª Prova Álgebra 2. 30/06/2016

Ex. 1. Seja $K = \mathbb{F}_3[x]/I$ onde $I = (x^2+2x+2)$

(a) Mostre que K é um corpo e calcule $|K|$.

[K é um corpo pois o polinômio $P(x) = x^2+2x+2$ (gerador de I) é irredutível em $\mathbb{F}_3[x]$, de fato ele tem grau 2 e não tem raizes em $\mathbb{F}_3$: $P(0) = 2 \neq 0$, $P(1) = 2 \neq 0$, $P(2) = 1 \neq 0$. Seja $\alpha = x + I$. Sabemos pela teoria que os elementos de K são $a + b\alpha$ com $a, b \in \mathbb{F}_3 \Rightarrow |K| = 3 \cdot 3 = 9$.]

(b) Mostre que $\alpha = x + I$ é um gerador de K^*.

[$\alpha \in K^* = K - \{0\}$ e $|K^*| = 9 - 1 = 8$ logo $o(\alpha)$ é 1, 2, 4 ou 8. Temos que mostrar que $o(\alpha) = 8$. Para isso basta então mostrar que $o(\alpha) \neq 1, 2, 4$. Pela teoria sabemos que $\alpha^2 + 2\alpha + 2 = 0 \Rightarrow \alpha^2 = \alpha + 1$. Logo $\alpha^1 = \alpha \neq 1$, $\alpha^2 = \alpha + 1 \neq 1$ e $\alpha^4 = (\alpha^2)^2 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = 2 \neq 1$. Logo $o(\alpha) \neq 1, 2, 4 \Rightarrow o(\alpha) = 8$. (pois $o(\alpha)$ divide 8).]

(c) Encontre $a, b \in \mathbb{F}_3$ tais que $(\alpha+2)^{-1} = a + b\alpha$.

[Sabemos que $\alpha^2 + 2\alpha + 2 = 0$, logo $\alpha(\alpha+2) = -2 = 1$. Assim basta escolher a, b tais que $a + b\alpha = \alpha$: $\underline{a=0}, \underline{b=1}$]

Ex 2. Mostre que são irredutíveis em $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$:

(a) $x^4 - 6x^2 + 6$. É irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein aplicado a $p = 2$. Logo como é primitivo, pelo lema de Gauss é irredutível em $\mathbb{Z}[x]$.

(b) $x^3 + 4x - 1$. É primitivo, logo pelo lema de Gauss basta mostrar que é irredutível em $\mathbb{Z}[x]$. Se é redutível então como ele tem grau 3, existe um fator de grau 1. Como $P(x) = x^3 + 4x - 1$ é mônico, esse fator de grau 1 corresponde a uma raiz $a \in \mathbb{Z}$:
$P(a) = 0 \Rightarrow a^3 + 4a - 1 \Rightarrow a(a+4) = 1 \Rightarrow a$ divide 1.
Logo têm 2 possibilidades: $a = 1$ e $a = -1$. Mas $P(1) = 4 \neq 0$ e $P(-1) = -6 \neq 0$. Então $P(x)$ é irredutível.

Ex 3. Seja $\alpha = \sqrt{3 - \sqrt{3}} \in \mathbb{C}$.

(a) Mostre que α é algébrico sobre $\mathbb{Q}$.
Temos $\alpha^2 = 3 - \sqrt{3}$ logo $(\alpha^2 - 3)^2 = 3 \Rightarrow \alpha$ é raiz de $P(x) = x^4 - 6x^2 + 6 \Rightarrow \alpha$ é algébrico sobre $\mathbb{Q}$.

(b) O grau $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é igual ao grau do polinômio minimal de α sobre $\mathbb{Q}$. Pelo ponto (a), α é raiz de $P(x) = x^4 - 6x^2 + 6$ que é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein aplicado a $p = 2$. Logo $P(x)$ é o polinômio minimal de α sobre $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(c) Calcule o grau $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})]$.
Observe que $\alpha^2 = 3 - \sqrt{3} \Rightarrow \sqrt{3} \in \mathbb{Q}(\alpha)$. Logo $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$.
É claro que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Pela formula do grau

$$4 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 2.$$

Ex 4. Seja $E/\mathbb{F}_2$ extensão de corpos e $P(x) \in \mathbb{F}_2[x]$, $\alpha \in E$. Mostre que se $P(\alpha)=0$ então $P(\alpha^2)=0$.

[Temos $P(x) = \sum_{i=0}^{n} a_i x^i$ com $a_i \in \mathbb{F}_2 = \{0,1\}$. Em particular $a_i^2 = a_i$. Lembrando que $\phi: E \to E$, $\phi(a) = a^2$ é homomorfismo (isomorfismo de Frobenius) temos

$$0 = 0^2 = P(\alpha)^2 = \left(\sum_{i=0}^{n} a_i \alpha^i\right)^2 = \sum_{i=0}^{n} a_i^2 (\alpha^2)^i = P(\alpha^2)$$

$\hookrightarrow (= a_i)$

logo $P(\alpha^2)=0$. □]

Ex 5. Mostre que X^2+2 divide $X^{25}-X$ em $\mathbb{F}_5[x]$.

[$F = \mathbb{F}_5[x]/(x^2+2)$ é um corpo pois x^2+2 é irredutível em $\mathbb{F}_5[x]$ (tem grau 2 e não tem raízes em $\mathbb{F}_5$). Seja $\alpha = X + (x^2+2) \in F \Rightarrow \alpha$ é raiz de x^2+2. Mas x^2+2 é mônico e irredutível em $\mathbb{F}_5[x] \Rightarrow$ é o polinômio minimal de α sobre $\mathbb{F}_5$. Logo x^2+2 divide todos os polinômios $P(x) \in \mathbb{F}_5[x]$ tais que $P(\alpha)=0$. Logo basta mostrar que $P(x) = x^{25}-x$ verifica $P(\alpha)=0$. Mas $\alpha \in F^*$ e $|F^*| = 24 \Rightarrow \alpha^{24} = 1 \Rightarrow$ multiplicando por α, $\alpha^{25} = \alpha \Rightarrow \alpha$ é raiz de $X^{25}-X$. □]