ÁLGEBRA II 2014 – VR – 05/06/2014
GABARITO

PROFESSOR MARCO

Exercício 1. Prove que no anel de polinómios $\mathbb{Q}[x]$ existem infinitos polinómios irredutíveis.

Solução: Suponha por contradição que $f_1(x), \ldots, f_n(x)$ sejam todos os irredutíveis de $\mathbb{Q}[x]$. Considere o polinómio $g(x) = f_1(x) \cdot f_2(x) \cdots f_n(x) + 1$. Pelo teorema de fatoração em $\mathbb{Q}[x]$, temos que $g(x)$ é produto de um número finito de irredutíveis, logo existe um $f_i(x)$ que divide $g(x)$. Porém pela definição de $g(x)$, a divisão de $g(x)$ por $f_i(x)$ é igual a 1, o que implica um absurdo.

Exercício 2. Escreva o polinómio

$$f(x) = x^4 - x^3 + 5x - 2 \in K[x],$$

como produto de polinómios irredutíveis em $K[x]$, onde $K = \mathbb{Q}, \mathbb{Z}_2, \mathbb{Z}_3$.

Solução: Vamos ver que f é irredutível sobre $\mathbb{Q}$. As possíveis raizes racionais de f são ± 1 e ± 2, e se verifica facilmente que não são raizes. Logo, pelo teorema de Ruffini, se f é redutível sobre $\mathbb{Q}$, ele fatora como produto de dois polinómios de grau 2. Pelo o teorema de Gauss, isto implica que f é produto de dois polinómios de grau 2 com coeficientes intéiros. Vamos escluir que tal fatoração possa existir. Suponha por absurdo que

$$x^4 - x^3 + 5x - 2 = g(x)h(x)$$

$$g(x) = ax^2 + bx + c \quad \text{e} \quad h(x) = dx^2 + ex + f.$$

Logo $ad = 1$, e, a menos de mudar sinal em g e h, podemos supor que $a = d = 1$. Temos $f + be + c = 0$, $e + b = -1$ e $cf = -2$. Isto implica as seguintes relações:

$$c = -f - be = -f - (-e - 1)e = -f + e^2 + e$$

$$(-f + e^2 + e)f = -2.$$

Logo $e^2 f + ef + 2 - f^2 = 0$, que como polinómio em e deve ter soluções intéiras. Portanto o discriminate $\Delta := f^2 - 4f(2 - f^2) = 4f^3 + f^2 - 8f$ deve ser um intéiro. Porém a relação $cf = -2$ sobre os intéiros implica que $f \in \{-1, 1, -2, 2\}$, que implica que $\Delta \in \{5, -3, -12, 20\}$, isto é Δ nunca é intéiro, absurdo.

Sobre $\mathbb{Z}_2$ o polinómio é $f(x) = x^4 + x^3 + x = x(x^3 + x^2 + 1)$. O polinómio $x^3 + x^2 + 1$ é irredutível sobre $\mathbb{Z}_2$ pois é de grau 3 e não possui raizes sobre $\mathbb{Z}_2$.

Sobre $\mathbb{Z}_3$ o polinómio é $f(x) = x^4 + 2x^2 + 2x + 1$. O polinómios tem 1 como raiz, logo pelo teorema de Ruffini, $f(x)$ é divisível por $x - 1$. Fazendo a divisão, obtemos $f(x) = (x-1)(x^3+2)$. O polinómio x^3+2 tem 1 como raiz, logo de novo é divisível por $x - 1$. Temos $x^3 + 2 = (x - 1)(x^2 + x + 1) = (x - 1)(x^2 - 2x + 1) = (x-)^3$. Logo $f(x) = (x - 1)^4$.

Exercício 3. Considere o grupo $G = (\mathbb{Q}, +)$ e sejam a e b dois intéiros primos entre se, isto é tais que $\mathrm{MDC}(a, b) = 1$. Mostre que o subgrupo de G gerado por $1/a$ e $1/b$ é ciclico gerado por $1/ab$, isto é mostre que vale

$$\left\langle \frac{1}{a}, \frac{1}{b} \right\rangle = \left\langle \frac{1}{ab} \right\rangle.$$

Solução: Vimos no curso que em um grupo G, o subgrupo $< x >$ gerado por um elemento é igual a $< x >= \{x^m : m \in \mathbb{Z}\}$. Além disso, o subgrupo $< x, y >$ gerado por dois elementos x e y é igual ao conjunto das palavras finitas que podem ser formadas com as letras x, y, x^{-1} e y^{-1}. Agora, se o grupo é comutativo, é claro que este subgrupo é igual a

$$< x, y >= \{x^m y^n : m, n \in \mathbb{Z}\}.$$

No nosso caso, $(\mathbb{Q}, +)$ é claramente comutativo, logo

$$\left\langle \frac{1}{a}, \frac{1}{b} \right\rangle = \left\{ m \cdot \frac{1}{a} + n \cdot \frac{1}{b} : m, n \in \mathbb{Z} \right\} = \left\{ \frac{mb + na}{ab} : m, n \in \mathbb{Z} \right\} \subseteq \left\langle \frac{1}{ab} \right\rangle.$$

Para provar a outra inclusão, vamos usar que, como a e b são coprimos, vale a identidade de Bezóut:

$$\alpha a + \beta b = 1, \text{ para algum } \alpha, \beta \in \mathbb{Z}.$$

Assim

$$\left\langle \frac{1}{ab} \right\rangle = \left\{ u\frac{1}{ab} : u \in \mathbb{Z} \right\} = \left\{ \frac{u(\alpha a + \beta b)}{ab} : u \in \mathbb{Z} \right\} = \left\{ u\alpha\frac{1}{b} + u\beta\frac{1}{a} : u \in \mathbb{Z} \right\} \subseteq \left\langle \frac{1}{a}, \frac{1}{b} \right\rangle$$

Exercício 4. Considere o subconjunto $S = \{A_1, A_2, A_3, A_4, A_5, A_6\}$ de $GL_3(\mathbb{R})$, onde

$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} A_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$
$$A_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} A_5 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} A_6 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

(i) Prove que S é um subgrupo de $GL_3(\mathbb{R})$;
(ii) Encontre as ordens dos elementos de S. O subgrupo S é ciclico?
(iii) O subgrupo S é isomorfo ao grupo simetrico S_3?

Solução: Seja (x, y, z) um vetor de $\mathbb{R}^3$. Temos

$$\begin{array}{lll} A_1(x,y,z) = (x,y,z) & A_2(x,y,z) = (y,x,z) & A_3(x,y,z) = (z,y,x) \\ A_4(x,y,z) = (x,z,y) & A_5(x,y,z) = (y,z,x) & A_6(x,y,z) = (z,x,y). \end{array}$$

Temos $A_1^{-1} = A_1$, $A_2^{-1} = A_2$, $A_3^{-1} = A_3$, $A_4^{-1} = A_4$, $A_5^{-1} = A_6$. Portanto é claro que $A_i A_j^{-1}$ está em S para todo $i, j \in \{1, 2, 3, 4, 5, 6\}$ e S é subgrupo de $GL_3(\mathbb{R})$.

(ii) Claramente a ordem de A_1 é 1, pois ela é a identidade. Pelo visto em (i) temos $A_2^2 = A_3^2 = A_4^2 = id$, logo A_2, A_3, A_4 possuem ordem 2, e $A_5^2 \neq id$, $A_6^2 \neq id$, $A_5^3 = A_6^3 = id$, logo A_5 e A_6 possuem ordem 3. O subgrupo S não pode ser ciclico pois se trata de um grupo de ordem 6 sem elementos de ordem 6.

(iii) O subgrupo é claramente isomorfo ao grupo S_3, com as notações (i), podemos por $x = 1$, $y = 2$, $z = 3$ e definir o isomorfismo $\psi \colon S \to S_3$ definido por $\psi(A_1) = id$, $\psi(A_2) = (12)$, $\psi(A_3) = (13)$, $\psi(A_4) = (23)$, $\psi(A_5) = (132)$, $\psi(A_6) = (123)$.