ÁLGEBRA II (2014)–LISTA 1

Relações de equivalência – Números

(1) Seja A um conjunto e $\rho \subseteq A \times A$ um relação sobre A. Nos casos listados abaixo, diga quais relações são de equivalência, e nesse caso encontre se possivél a partição de A induzida por ρ:

- $A := \mathbb{N} \times \mathbb{N}$ e $\rho := \{((m,n),(r,s) : m+s = n+r\}$.
- $A := \{1,2,3,4\}$ e $\rho := \{(1,1),(1,3),(2,2),(3,1)\}$.
- $A := \mathbb{Z} \setminus \{0\}$ e $\rho := \{(x,y) : x \text{ divide } y\}$.
- $A := \{\text{retas de um plano cartesiano}\}$ e
$$\rho := \{(r_1, r_2) : R_1 \text{ é paralela e não igual á } r_2\}.$$
- $A := \mathbb{Z}$ e $\rho := \{(x,y) : x - y \text{ é par }\}$
- $A := \mathbb{Z}$ e $\rho := \{(x,y) : |x| = |y|\}$

(2) Verifique que com as operações introduzidas nas aulas, os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}[x]$ são aneis comutativos com unidades, isto é são conjuntos que satisfazem as propriedades listadas na página 2 das notas. Além disso, verifique que $\mathbb{Q}$ é um corpo (isto é todo elemento não nulo de $\mathbb{Q}$ é invertivel) e que $\mathbb{Q}[x]$ é um domínio (isto é se $f(x) \cdot g(x) = 0$ com $f, g \in \mathbb{Q}[x]$, logo ou $f = 0$ ou $g = 0$.

(3) É conhecido o seguinte resultado (*divisão entre intéiros*): *dados* $a, b \in \mathbb{Z}$, *com* $b \neq 0$, *existem únicos* $q, r \in \mathbb{Z}$ *tais que* $a = bq + r$, *com* $0 \leq r < |b|$. Prove o resultado citado quando $a \geq b \geq 0$. (Dica: use indução sobre o número natural a).

(4) Mostre que os invertíveis de $\mathbb{Z}$ são 1 e -1, isto é: 1 e -1 são os únicos elementos $a \in \mathbb{Z}$ tais que $a \cdot b = 1$, para algum $b \in \mathbb{Z}$.

(5) Um elemento $a \in \mathbb{Z}$ é dito *irredutível* se toda vez que escrevemos $a = b \cdot c$, logo ou b ou c é um invertível de $\mathbb{Z}$ (isto é, pelo exercício (4), ou $b \in \{1, -1\}$ ou $c \in \{1, -1\}$). Prove o seguinte resultado, que fornece a existência da fatoração de intéiros e que é conhecido como *teorema fundamental da aritmética*: Seja n um intéiro, $n > 1$. Logo é possível escrever n como produto de um número finito de potências de irredutíveis $p_1, \ldots, p_s$
$$n = p_1^{h_1} \cdots p_s^{h_s},$$
onde $p_i > 1$, $h_i \geq 1$ e $s \geq 1$.

(6) Usando o exercício (5), mostre que em $\mathbb{Z}$ existem infinitos números irredutiveis. (Dica: por contradição suponha que existam finitos irredutíveis $p_1, \ldots, p_N$. O intéiro $p_1 \cdot p_2 \cdots p_N + 1$ possui fatoração?).

(7) Usando o exercício (5), mostre que se p é um primo em $\mathbb{Z}$, logo $\sqrt{p}$ não é um número racional.

(8) Neste exercício construiremos o *anel dos intéiros modulo um intéiro n*. Seja $n \in \mathbb{Z}$ um intéiro fixado.

(i) Verifique que a seguinte relação sobre $\mathbb{Z}$ é uma relação de equivalência:

$$\rho_n := \{(a, b) : a - b = n \cdot h, \text{ para algum } h \in \mathbb{Z}\}.$$

A relação ρ_n é dita *relação de equivalência módulo n*. Se $a\rho_n b$, onde $a, b \in \mathbb{Z}$, escrevemos $a \equiv b \bmod n$. Denotaremos por $\mathbb{Z}_n := /\rho_n$ (o conjunto quociente).

(ii) Prove que as classes de equivalencia de ρ_n são $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. (Dica: use a divisão entre intéiros do exercício (3)). Note que portanto $\mathbb{Z}_n$ possui n elementos.

(iii) Verifique que as seguintes operações sobre $\mathbb{Z}_n$ independem dos representantes escolhidos:

$$\overline{a} + \overline{b} := \overline{a + b}, \;\; \overline{a} \cdot \overline{b} := \overline{a \cdot b},$$

onde $a + b$ e $a \cdot b$ são as operações de soma e produto de $\mathbb{Z}$.

(iv) Verifique que $\mathbb{Z}_n$ é um anel comutativo com unidade.

(v) Prove que $\mathbb{Z}_2$ e $\mathbb{Z}_3$ são corpos, e que $\mathbb{Z}_4$ não é um corpo.

(9) Seja n un inteiro positivo fixado. Prove que para todo $a, b, c \in \mathbb{Z}$ tais que $a \equiv b \bmod n$ valem as seguintes propriedades:

(i) $a + c \equiv b + c \bmod n$;

(ii) $a \cdot c \equiv b \cdot c \bmod n$;

(iii) $a^i \equiv b^i \bmod n$, para qualquer $i \in \mathbb{N}$.

(10) Seja $a \in \mathbb{Z}$. Escreva a no sistema decimal como

$$a = a_n a_{n-1} \ldots a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0.$$

Chamamos os $a_n, \ldots a_0$ de *algarismos* de a.

(i) Mostre que as seguintes relações valem:

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \bmod 9$$

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \bmod 3$$

Em particular, mostre que a é divisível por 9 (respectivamente por 3) se e somente se a soma das seus algarismos é divisivel por 9 (respectivamente por 3).

(ii) Mostre que a é divisível por 4 (respectivamente por 25) se e somente se $a_1 a_0 = a_1 \cdot 10 + a_0$ é divisível por 4 (respectivamente por 25). (Dica: use que 100 é equivalente a 0 módulo 4 e também módulo 25.)

(iii) Mostre que a é divisível por 11 se e somente se é divisível por 11 o número:

$$a_0 - a_1 + a_2 \cdot + (-1)^n \cdot a_n.$$

(Dica: observe que, para todo intéiro positivo i, temos que 10^i é equivalente a $(-1)^i$ módulo 11.)