T1 – Trabalho semanal 1 de Álgebra 2 – Semestre 2021-1

Semana: 26-30 de julho, 2021.
Prazo de entrega: 12 de agosto, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := a + 2b + 3c + 9.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Considere o grupo C_m, cíclico de ordem m. Conte os elementos $x \in C_m$ tais que $\langle x \rangle = C_m$, nos casos seguintes: $m = n$, $m = n + 1$, $m = 3n + 6$.

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

2. Seja $G := S_4 = \mathrm{Sym}(\{1, 2, 3, 4\})$. Considere os conjuntos seguintes.

$$A := \{g \in G \ : \ g^{n+3} = 1\},$$

$$B := \{g \in G \ : \ g^{n+4} = 1\},$$

$$C := \{g \in G \ : \ g^{n+5} = 1\}.$$

   Para cada um deles, diga se é um subgrupo de G. Além disso, calcule as cardinalidades $|A|$, $|B|$, $|C|$.

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

3. Sejam G um grupo e N um subgrupo normal de G. Suponha que $g^2 \in N$ para todo $g \in G$. Mostre que o grupo quociente G/N é abeliano.

4. Sejam $G := S_4 = \mathrm{Sym}(\{1, 2, 3, 4\})$, $x := (123) \in G$, $y := (1234) \in G$, $z := (14) \in G$. Considere os elementos

$$g := x^a y^b z^c, \qquad h := x^{a+1} y^{b+1} z^{c+1}, \qquad k := x^{a+2} y^{b+2} z^{c+2}.$$

   Atenção: aqui a, b, c não são inteiros quaisquer, são os números definidos acima!

   Para cada um dos subgrupos H de G seguintes, determine se é normal em G. No caso em que o subgrupo considerado H é normal em G, responda à seguinte pergunta: o grupo quociente G/H é abeliano?

$$A = \langle g \rangle, \qquad B = \langle h \rangle, \qquad C = \langle k \rangle,$$

$$K = \{1, (12)(34), (13)(24), (14)(23)\}.$$

   No caso de K, mostre também que se trata de um subgrupo de G.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T1 – Álgebra 2 – 2021-1 - Gabarito.

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Considere o grupo C_m, cíclico de ordem m. Conte os elementos $x \in C_m$ tais que $\langle x \rangle = C_m$, nos casos seguintes: $m = n$, $m = n + 1$, $m = 3n + 6$.

   Seja g um gerador de $G := C_m$. Sabemos que $x \in G$ é um gerador de G se e somente se é do tipo g^k com $\mathrm{MDC}(m, k) = 1$, ou seja m e k são coprimos. Precisamos então contar os inteiros em $\{1, \ldots, m\}$ que são coprimos com m. Isso pode ser feito a mão para valores dados de m, mas pode também ser feito lembrando que o número de inteiros em $\{1, \ldots, m\}$ coprimos com m é indicado com $\varphi(m)$, e a função φ é a conhecida função de Euler. Lembre-se que se $m = \prod_{i=1}^{t} p_i^{a_i}$ onde os p_i são primos distintos e cada a_i é positivo, então

   $$\varphi(m) = \prod_{i=1}^{t} (p_i - 1) p_i^{a_i - 1}.$$

   Vou considerar os valores $m = 48$ e $m = 100$ como exemplo.

   $$\varphi(48) = \varphi(2^4 \cdot 3) = (2-1) \cdot 2^{4-1} \cdot (3-1) \cdot 3^{1-1} = 8 \cdot 2 = 16,$$

   $$\varphi(100) = \varphi(2^2 \cdot 5^2) = (2-1) \cdot 2^{2-1} \cdot (5-1) \cdot 5^{2-1} = 2 \cdot 4 \cdot 5 = 40.$$

2. Seja $G := S_4 = \mathrm{Sym}(\{1, 2, 3, 4\})$. Considere os conjuntos seguintes.

   $$A := \{g \in G \ : \ g^{n+3} = 1\},$$

   $$B := \{g \in G \ : \ g^{n+4} = 1\},$$

   $$C := \{g \in G \ : \ g^{n+5} = 1\}.$$

   Para cada um deles, diga se é um subgrupo de G. Além disso, calcule as cardinalidades $|A|$, $|B|$, $|C|$.

   Aqui temos conjuntos do tipo $X = \{g \in G \ : \ g^m = 1\}$. Lembre-se que os elementos de $G = S_4$ têm estruturas cíclicas 1, $(**)$, $(***)$, $(****)$, $(**)(**)$, logo os elementos de G têm ordem 1, 2, 3 ou 4. Lembre-se também que se g tem ordem k então $g^m = 1$ se e somente se k divide m. Vamos analizar alguns valores de m.

   $m = 30$. Se $g \in G = S_4$ então $g^{30} = 1$ se e somente se g tem ordem 1, 2 ou 3 (g não pode ter ordem 4 pois 4 não divide 30). Segue que neste caso X é o conjunto dos elementos de estrutura cíclica 1, $(**)$, $(***)$ ou $(**)(**)$, em outras palavras X é o conjunto dos elementos que não são 4-cíclos. Em $G = S_4$ tem exatamente $3! = 6$ 4-cíclos (são da forma $(1 * **)$), logo $|X| = |G| - 6 = 24 - 6 = 18$. Como 18 não divide $|G| = 24$, pelo teorema de Lagrange X não é um subgrupo de G.

$m = 31$. Se $g \in G = S_4$ então $g^{31} = 1$ se e somente se $g = 1$, porque 31 não é divisível pelas ordens dos elementos não triviais de G, que são 2, 3 e 4. Segue que $X = \{1\}$ neste caso, e obviamente $|X| = 1$ e $X \leq G$.

$m = 48$. Se $g \in G = S_4$ então $g^{48} = 1$, pois 48 é divisível por todas as ordens dos elementos de G: 1, 2, 3 e 4. Segue que $X = G$ neste caso, $|X| = |G| = 24$ e obviamente $X = G$ é subgrupo de G.

$m = 20$. Se $g \in G = S_4$ então $g^{20} = 1$ se e somente se a ordem de g divide 20, ou seja $o(g) \in \{1, 2, 4\}$. Segue que neste caso X é o conjunto dos elementos de estrutura cíclica 1, $(**)$, $(**)(**)$ ou $(***)$, em outras palavras X é o conjunto dos elementos que não são 3-cíclos. Em $G = S_4$ tem exatamente $4 \cdot 2 = 8$ 3-cíclos (são da forma $(*)(***)$, precisamos escolher o elemento fixado e depois precisamos formar um 3-cíclo usando os demais elementos), logo $|X| = |G| - 8 = 24 - 8 = 16$. Como 16 não divide $|G| = 24$, pelo teorema de Lagrange X não é um subgrupo de G.

$m = 45$. Se $g \in G = S_4$ então $g^{45} = 1$ se e somente se a ordem de g divide 45, ou seja $o(g) \in \{1, 3\}$. Segue que neste caso X é o conjunto contendo 1 e todos os 3-cíclos. Como G contém 8 3-cíclos, segue que $|X| = 1 + 8 = 9$. Como 9 não divide $|G| = 24$, pelo teorema de Lagrange X não é um subgrupo de G.

Obviamente, na discussão acima, para mostrar que X não é subgrupo de G era possível também encontrar dois elementos $x, y \in X$ tais que $xy \notin X$.

Erro comum. Atenção, o teorema de Lagrange fala que se $H \leq G$ então $|H|$ divide $|G|$, não fala o contrário, ou seja, se X é um subconjunto de G e $|X|$ divide $|G|$, você não pode deduzir que X é subgrupo de G.

3. Sejam G um grupo e N um subgrupo normal de G. Suponha que $g^2 \in N$ para todo $g \in G$. Mostre que o grupo quociente G/N é abeliano.

   Sejam $x, y \in G$. Precisamos mostrar que $xNyN = yNxN$. Sabemos que $x^2, y^2, (xy)^2 \in N$, ou seja $x^2N = N$, $y^2N = N$ e $(xy)^2N = N$. Essas igualdades podem ser escritas $xN = x^{-1}N$, $yN = y^{-1}N$, $xyN = y^{-1}x^{-1}N$. Segue que

   $$xNyN = xyN = y^{-1}x^{-1}N = y^{-1}Nx^{-1}N = yNxN.$$

   Uma curiosidade: segue do teorema fundamental dos grupos abelianos finitos que um grupo finito G tem a propriedade que $g^2 = 1$ para todo $g \in G$ se e somente se G é isomorfo a um produto direto $C_2 \times C_2 \times \ldots \times C_2$. A abelianidade de G segue do argumento acima, com $N = \{1\}$.

4. Sejam $G := S_4 = \mathrm{Sym}(\{1, 2, 3, 4\})$, $x := (123) \in G$, $y := (1234) \in G$, $z := (14) \in G$. Considere os elementos

   $$g := x^a y^b z^c, \qquad h := x^{a+1} y^{b+1} z^{c+1}, \qquad k := x^{a+2} y^{b+2} z^{c+2}.$$

Para cada um dos subgrupos H de G seguintes, determine se é normal em G. No caso em que o subgrupo considerado H é normal em G, responda à seguinte pergunta: o grupo quociente G/H é abeliano?

$$A = \langle g \rangle, \qquad B = \langle h \rangle, \qquad C = \langle k \rangle,$$

$$K = \{1, (12)(34), (13)(24), (14)(23)\}.$$

No caso de K, mostre também que se trata de um subgrupo de G.

Os elementos g, h, k são obtidos multiplicando permutações. Vamos dar o exemplo seguinte: $x^{101}y^{203}z^{271}$. Este elemento é calculado lembrando que se um elemento g tem ordem m então $g^a = g^b$ se e somente se $a \equiv b \mod m$. Como $x = (123)$ tem ordem 3, $y = (1234)$ tem ordem 4 e $z = (14)$ tem ordem 2, e $101 \equiv 2 \mod 3$, $203 \equiv 3 \mod 4$ e $271 \equiv 1 \mod 2$, obtemos que

$$x^{101}y^{203}z^{271} = x^2y^3z = (132)(1432)(14) = (123).$$

O subgrupo $H = \langle (123) \rangle$ não é normal em G. De fato, ele contém (123) mas não contém todos os seus conjugados! Lembre-se que os conjugados de (123) em $G = S_4$ são exatamente todos os 3-cíclos (de fato, $g(123)g^{-1} = (g(1), g(2), g(3))$) mas $\langle (123) \rangle = \{1, (123), (132)\}$ não contém todos os 3-cíclos, por exemplo não contém (124). O mesmo raciocínio mostra que subgrupos como $\langle (13) \rangle = \{1, (13)\}$ e $\langle (1423) \rangle = \{1, (1423), (12)(34), (1324)\}$ não são normais em $G = S_4$.

Na verdade o argumento acima mostra que o único subgrupo normal cíclico de S_4 é $\{1\}$. Observe que o quociente $G/\{1\}$ não é abeliano pois é isomorfo a $G = S_4$ pelo isomorfismo $G \to G/\{1\}$, $g \mapsto g\{1\}$.

Agora vamos analizar

$$K = \{1, A = (12)(34), B = (13)(24), C = (14)(23)\}.$$

Se trata de um subgrupo de G (*chamado de grupo de Klein*). Para mostrar isso, observe que os produtos dos elementos de K pertencem a K:

(a) $AB = (12)(34)(13)(24) = (14)(23) \in K$,

(b) $BA = (13)(24)(12)(34) = (14)(23) = AB \in K$,

(c) $AC = (12)(34)(14)(23) = (13)(24) \in K$,

(d) $CA = (14)(23)(12)(34) = (13)(24) = AC \in K$,

(e) $BC = (13)(24)(14)(23) = (12)(34) \in K$,

(f) $CB = (14)(23)(13)(24) = (12)(34) = BC \in K$.

Além disso, $1 \in K$ e os elementos de K têm ordem 1 ou 2, ou seja $x^2 = 1$ para todo $x \in K$, e isso implica que $x^{-1} = x \in K$ para todo $x \in K$. Isso conclui a demostração do fato que $K \leq G$.

K é normal em G porque os conjugados de um elemento $x \in K$ tem a mesma estrutura cíclica de x, e K consiste dos elementos de estrutura cíclica 1 ou $(**)(**)$.

O grupo quociente G/K tem ordem $|G/K| = |G|/|K| = 24/4 = 6$. Para mostrar que não é abeliano considere $x = (123)$, $y = (12)$. Mostraremos que $xKyK \neq yKxK$. Observe que

$$xKyK = xyK = (123)(12)K = (13)K,$$

$$yKxK = yxK = (12)(123)K = (23)K,$$

logo para concluir precisamos mostrar que $(13)K \neq (23)K$. Se fosse $(13)K = (23)K$ então teríamos $(23)^{-1}(13) \in K$, mas

$$(23)^{-1}(13) = (23)(13) = (123) \notin K.$$

T2 – Trabalho semanal 2 de Álgebra 2 – Semestre 2021-1

Semana: 02-06 de agosto, 2021.
Prazo de entrega: 19 de agosto, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := (9-a) + (9-b) + 3(9-c) + 8.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

Lembre-se que dois elementos x, y de um grupo G são ditos "conjugados em G" se existe $g \in G$ tal que $y = g \cdot x \cdot g^{-1}$.

1. Seja $G := A_4 < S_4$ o grupo alternado de grau 4 e sejam $x := (12)(34) \in G$, $y := (123)^n \in G$, $g := y \cdot x \cdot y^{-1} \in G$. Encontre todos os elementos $t \in G$ tais que $gt = tg$, ou seja os elementos do "centralizador"

$$C_G(g) := \{t \in G \ : \ gt = tg\}.$$

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

2. Seja $[x]$ o maior inteiro menor ou igual a x (por exemplo $[7] = 7$, $[7/2] = 3$) e seja $m := 10 - [b/2]$, onde b é o número definido acima. Encontre todas as ordens dos elementos do grupo alternado de grau m, ou seja o grupo A_m das permutações pares de $\{1, \ldots, m\}$.

   Atenção: aqui b não é um inteiro qualquer, é o número definido acima!

3. Para cada um dos seguintes inteiros m, calcule o máximo inteiro positivo k tal que existem elementos $x_1, \ldots, x_k \in S_n$, todos de ordem m, dois a dois não conjugados em S_n. $m = n + 1$, $m = n + 2$, $m = n + 3$.

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

   Um detalhe: o fato que $x_1, \ldots, x_k$ são "dois a dois não conjugados em S_n" significa o seguinte. Para todo $i, j \in \{1, \ldots, k\}$, $i \neq j$, os elementos x_i e x_j não são conjugados em S_n, ou seja não existe nenhum $g \in S_n$ tal que $x_j = g \cdot x_i \cdot g^{-1}$.

4. Seja m um inteiro positivo tal que no grupo simétrico S_m existem elementos de ordem n e tal que todos os elementos de ordem n são conjugados em S_m. Encontre o valor de m.

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T2 – Álgebra 2 – 2021-1 - Gabarito.

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

Lembre-se que dois elementos x, y de um grupo G são ditos "conjugados em G" se existe $g \in G$ tal que $y = g \cdot x \cdot g^{-1}$.

Lembre-se que um elemento g do grupo simétrico S_m tem "estrutura cíclica $(a_1, \ldots, a_t)$" se é produto de t cíclos disjuntos de comprimentos $a_1, \ldots, a_t$, onde os a_i são inteiros positivos e $\sum_{i=1}^{t} a_i = m$.

1. Seja $G := A_4 < S_4$ o grupo alternado de grau 4 e sejam $x := (12)(34) \in G$, $y := (123)^n \in G$, $g := y \cdot x \cdot y^{-1} \in G$. Encontre todos os elementos $t \in G$ tais que $gt = tg$, ou seja os elementos do "centralizador"

$$C_G(g) := \{t \in G \ : \ gt = tg\}.$$

   O elemento g é de tipo $(**)(**)$, sendo um conjugado de $x = (12)(34)$. Por exemplo, suponha que $g = (13)(24)$ (os outros casos são totalmente analogos). Seja $t \in G$ tal que $gt = tg$, ou seja $tgt^{-1} = g$, ou seja

$$(t(1), t(3)) \cdot (t(2), t(4)) = (13)(24).$$

   As possibilidades são:

   (a) $t(1) = 1$, $t(3) = 3$, $t(2) = 2$, $t(4) = 4$, que dá $t = 1 \in G$;
   (b) $t(1) = 3$, $t(3) = 1$, $t(2) = 2$, $t(4) = 4$, que dá $t = (13) \notin G$;
   (c) $t(1) = 3$, $t(3) = 1$, $t(2) = 4$, $t(4) = 2$, que dá $t = (13)(24) \in G$;
   (d) $t(1) = 1$, $t(3) = 3$, $t(2) = 4$, $t(4) = 2$, que dá $t = (24) \notin G$;
   (e) $t(1) = 2$, $t(3) = 4$, $t(2) = 1$, $t(4) = 3$, que dá $t = (12)(34) \in G$;
   (f) $t(1) = 2$, $t(3) = 4$, $t(2) = 3$, $t(4) = 1$, que dá $t = (1234) \notin G$;
   (g) $t(1) = 4$, $t(3) = 2$, $t(2) = 1$, $t(4) = 3$, que dá $t = (1432) \notin G$;
   (h) $t(1) = 4$, $t(3) = 2$, $t(2) = 3$, $t(4) = 1$, que dá $t = (14)(23) \in G$.

   Obtemos que

$$C_G(g) = \{1, (13)(24), (12)(34), (14)(23)\} = K.$$

   O centralizador dos elementos (12)(34), (14)(23) também é igual a K.

2. Seja $[x]$ o maior inteiro menor ou igual a x (por exemplo $[7] = 7$, $[7/2] = 3$) e seja $m := 10 - [b/2]$, onde b é o número definido acima. Encontre todas as ordens dos elementos do grupo alternado de grau m, ou seja o grupo A_m das permutações pares de $\{1, \ldots, m\}$.

   Consideramos os grupos alternados A_m onde $m \in \{6, 7, 8, 9, 10\}$. Lembre-se que se um elemento g de S_m tem estrutura cíclica $(a_1, \ldots, a_t)$, onde cada a_i é um inteiro positivo e $\sum_{i=1}^{t} a_i = m$, então o sinal de g é $(-1)^a$ onde $a = \sum_{i=1}^{t}(a_i + 1)$. Segue que g é uma permutação par se e somente se $\sum_{i=1}^{t}(a_i + 1)$ é par. Com isso, podemos responder à pergunta.

(a) As estruturas cíclicas dos elementos de A_6 são 1, (3), (5), (2, 2) (2, 4), (3, 3). As relativas ordens são 1, 3, 5, 2, 4, 3.

(b) As estruturas cíclicas dos elementos de A_7 são 1, (3), (5), (7), (2, 2), (2, 4), (2, 2, 3), (3, 3). As relativas ordens são 1, 3, 5, 7, 2, 4, 6, 3.

(c) As estruturas cíclicas dos elementos de A_8 são 1, (3), (5), (7), (2, 2), (2, 4), (2, 6), (2, 2, 3), (2, 2, 2, 2), (3, 3), (3, 5), (4, 4). As relativas ordens são 1, 3, 5, 7, 2, 4, 6, 6, 2, 3, 15, 4.

(d) As estruturas cíclicas dos elementos de A_9 são 1, (3), (5), (7), (9), (2, 2), (2, 4), (2, 6), (2, 2, 3), (2, 2, 5), (2, 3, 4), (2, 2, 2, 2), (3, 3), (3, 5), (3, 3, 3), (4, 4). As relativas ordens são 1, 3, 5, 7, 9, 2, 4, 6, 6, 10, 12, 2, 3, 15, 3, 4.

(e) As estruturas cíclicas dos elementos de A_{10} são 1, (3), (5), (7), (9), (2, 2), (2, 4), (2, 6), (2, 8), (4, 6), (2, 2, 3), (2, 2, 5), (2, 3, 4), (2, 2, 2, 4), (2, 2, 2, 2), (2, 2, 3, 3), (3, 3), (3, 5), (3, 7), (3, 3, 3), (4, 4), (5, 5). As relativas ordens são 1, 3, 5, 7, 9, 2, 4, 6, 8, 12, 6, 10, 12, 4, 2, 6, 3, 15, 21, 3, 4, 5.

3. Para cada um dos seguintes inteiros m, calcule o máximo inteiro positivo k tal que existem elementos $x_1, \ldots, x_k \in S_n$, todos de ordem m, dois a dois não conjugados em S_n. $m = n + 1$, $m = n + 2$, $m = n + 3$.

   Observe que $m > n$, logo em S_n não existem m-ciclos. Segue que um elemento de S_n de ordem m é um elemento de estrutura cíclica $(a_1, \ldots, a_t)$ onde o menor múltiplo comum de $a_1, \ldots, a_t$ é igual a m, e $t \geq 2$. Em particular, se m é uma potência de um primo, então S_n não contém elementos de ordem m, pois na notação acima um dos a_i deveria ser igual a m). Por outro lado, se m não é uma potência de um primo, S_n pode conter muitos elementos de ordem m.

   Por exemplo considere $n = 12$. Como 13 é primo, S_{12} não contém elementos de ordem 13, logo se $m = 13$ então $k = 0$. Os elementos de S_{12} de ordem 14 são os elementos de estrutura cíclica $(2, 7)$, $(2, 2, 7)$, logo se $m = 14$ então $k = 2$. Os elementos de S_{12} de ordem 15 são os elementos de estrutura cíclica $(3, 5)$, $(3, 3, 5)$, logo se $m = 15$ então $k = 2$.

   Um outro exemplo é o seguinte: os elementos de S_{47} de ordem $48 = 2^4 \cdot 3$ são os elementos de estrutura cíclica $(a_1, \ldots, a_t, a_{t+1}, \ldots, a_k)$, com $\sum_{i=1}^{k} a_i = 47$, onde $a_1 = \ldots = a_t$ são potências de 2, pelo menos uma igual a $2^4 = 16$, e $a_{t+1}, \ldots, a_k$ são iguais a 3. Tem 1122 tais configurações. Neste caso bastava explicitar a estrutura dos elementos como fiz aqui.

   Por outro lado, em S_{47} não tem elementos de ordem $49 = 7^2$ porque 49 é uma potência de primo e $49 > 47$.

   Se n é grande, dependendo do valor de n as contas ficam muito complicadas. Usando um computador é possível calcular k facilmente. As seguintes

tabelas mostram alguns valores de k associados a $m = n + 1$.

n	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
k	1	0	0	0	2	0	6	0	3	4	0	0	9	0	22	6

n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
k	5	0	64	0	6	0	47	0	347	0	0	10	8	12	418

n	36	37	38	39	40	41	42	43	44	45	46	47	48	49
k	0	9	12	368	0	876	0	126	105	11	0	1122	0	53

4. Seja m um inteiro positivo tal que no grupo simétrico S_m existem elementos de ordem n e tal que todos os elementos de ordem n são conjugados em S_m. Encontre o valor de m.

   Vamos considerar alguns valores de n.

   $n = 12$. Suponha que em S_m existem elementos de ordem 12 e que todos os elementos de ordem 12 são conjugados em S_m. Como elementos de estruturas cíclicas (12) e $(3, 4)$ têm ordem 12 e não são conjugados em nenhum grupo simétrico, deduzimos que $m < 12$. Além disso em S_9 tem elementos do tipo $(2, 3, 4)$, de ordem 12, logo $m < 9$. Por outro lado nos grupos S_m com $m \in \{7, 8\}$ todos os elementos de ordem 12 têm estrutura cíclica $(3, 4)$. Logo os possíveis valores de m são 7 e 8.

   $n = 22$. Suponha que em S_m existem elementos de ordem 22 e que todos os elementos de ordem 22 são conjugados em S_m. Como elementos de estruturas cíclicas (22) e $(2, 11)$ têm ordem 22 e não são conjugados em nenhum grupo simétrico, deduzimos que $m < 22$. Além disso os elementos de tipo $(2, 2, 11)$ têm ordem 22, logo $m < 2 + 2 + 11 = 15$. Por outro lado se $m \in \{13, 14\}$ então os únicos elementos de S_m de ordem 22 são os de tipo $(2, 11)$, logo os valores possíveis de m são 13 e 14.

   $n = 41$. Suponha que em S_m existem elementos de ordem 41 (número primo) e que todos os elementos de ordem 41 são conjugados em S_m. Segue que $m < 82$, porque se $m \geq 82$ teria espaço em S_m para elementos de estrutura cíclica $(41, 41)$, que têm ordem 41 e não são conjugados aos 41-cíclos. Além disso, como S_m contém elementos de ordem 41 que é primo, é necessário que $m \geq 41$. Como 41 é primo, os elementos de ordem 41 são produtos de 41-cíclos disjuntos. Segue que se $41 \leq m \leq 81$ então todos os elementos de ordem 41 são 41-cíclos e são entre eles conjugados. Segue que os possíveis valores de m são 41, 42, ..., 81.

   $n = 45$. Suponha que em S_m existem elementos de ordem $45 = 3^2 \cdot 5$ e que todos os elementos de ordem 45 são conjugados em S_m. Como elementos de estruturas cíclicas (45) e $(5, 9)$ têm ordem 45 e não são conjugados em nenhum grupo simétrico, deduzimos que $m < 45$. Além disso os elementos de tipo $(5, 5, 9)$ têm ordem 45, logo $m < 5 + 5 + 9 = 19$. Segue que os valores possíveis de m são $9 + 5 = 14$, 15, 16, 17 e 18.

T3 – Trabalho semanal 3 de Álgebra 2 – Semestre 2021-1

Semana: 09-13 de agosto, 2021.
Prazo de entrega: 26 de agosto, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Seja $|x|$ o valor absoluto ("módulo") do número x, ou seja $|x| = x$ se $x \geq 0$ e $|x| = -x$ se $x < 0$ (por exemplo $|-2| = 2$, $|0| = 0$, $|3| = 3$). Defina

$$n := |a-5| + 2|b-5| + 3|c-5| + 7.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Sejam r, s inteiros positivos quaisquer. Escrevamos $C_r = \langle x \rangle$, $C_s = \langle y \rangle$. Mostre que todo homomorfismo $f : C_r \to C_s$ é do tipo $f(x^h) = y^{hk}$ para algum inteiro k tal que s divide $r \cdot \mathrm{MDC}(s, k)$. Bonus (não vale ponto): mostre que existem exatamente $\mathrm{MDC}(r, s)$ homomorfismos $C_r \to C_s$.

2. Um homomorfismo de grupos $f : A \to B$ é dito trivial se $f(x) = 1$ para todo $x \in A$. Construa homomorfismos não triviais (se existirem)

$$C_n \to S_3, \qquad S_3 \to C_{2n}$$

onde S_3 é o grupo simétrico de grau 3. No caso de $f : S_3 \to C_{2n}$, defina $x := (12)$, $y := (123)$ e observe que $xyx^{-1} = y^2$, ou seja $xyx^{-1}y^{-1} = y$. Calcule $f(y)$ usando essa formula e deduza que $\langle y \rangle \leq \ker(f)$. Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

Para construir um homomorfismo $A \to B$ pode fazer o seguinte: pode encontrar $N \trianglelefteq A$ e $H \leq B$ tais que $A/N \cong H$ e compor tal isomorfismo com a projeção $A \to A/N$ a esquerda e a inclusão $H \to B$ a direita.

3. Sejam $G := A_4$, $H_m := \{g \in G \ : \ g^m = 1\}$. Para cada um dos inteiros seguintes, responda às perguntas: H_m é um subgrupo de G? H_m é um subgrupo normal de G? Caso H_m seja um subgrupo normal de G, o quociente G/H_m é abeliano? $m = n$, $m = n + 1$, $m = n + 2$.

Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

4. Sejam $G := \mathbb{Z} \times \mathbb{Z}$ (produto direto dos grupos aditivos $\mathbb{Z}$ e $\mathbb{Z}$),

$$A := 2\mathbb{Z} \times 4\mathbb{Z} \trianglelefteq G, \qquad B := \langle (1, n) \rangle \trianglelefteq G, \qquad C := \langle (n, n) \rangle \trianglelefteq G.$$

Usando o teorema de isomorfismo, mostre que

$$G/A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \qquad G/B \cong \mathbb{Z}, \qquad G/C \cong \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Aqui a notação é a usual (aditiva), $m\mathbb{Z} = \{mz \ : \ z \in \mathbb{Z}\}$ em $\mathbb{Z}$ e $\langle (x, y) \rangle = \{(mx, my) \ : \ m \in \mathbb{Z}\}$ em $\mathbb{Z} \times \mathbb{Z}$. Bonus (não vale ponto): consegue calcular $\mathbb{Z} \times \mathbb{Z}/\langle (x, y) \rangle$ em geral?

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T3 – Álgebra 2 – 2021-1 - Gabarito.

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Sejam r, s inteiros positivos quaisquer. Escrevamos $C_r = \langle x \rangle$, $C_s = \langle y \rangle$. Mostre que todo homomorfismo $f : C_r \to C_s$ é do tipo $f(x^h) = y^{hk}$ para algum inteiro k tal que s divide $r \cdot \mathrm{MDC}(s, k)$. Bonus (não vale ponto): mostre que existem exatamente $\mathrm{MDC}(r, s)$ homomorfismos $C_r \to C_s$.

   Seja $f : C_r \to C_s$ um homomorfismo de grupos, onde $C_r = \langle x \rangle$ e $C_s = \langle y \rangle$. Como $f(x) \in \langle y \rangle$, existe um inteiro k tal que $f(x) = y^k$, segue que $f(x^h) = f(x)^h = (y^k)^h = y^{hk}$. Além disso, $(y^k)^r = f(x)^r = f(x^r) = f(1) = 1$ implica que a ordem de y^k divide r. Mas a ordem de y^k vale $s/\mathrm{MDC}(k, s)$, logo s divide $r \cdot \mathrm{MDC}(k, s)$.

   (**BONUS**) Vamos contar os homomorfismos $f : C_r \to C_s$. Um tal homomorfismo é determinado por $f(x) = y^k$ onde s divide $r \cdot \mathrm{MDC}(k, s)$. Mas isso é equivalente a dizer que s divide $d \cdot \mathrm{MDC}(k, s)$, onde $d = \mathrm{MDC}(r, s)$, equivalentemente s/d divide k. Deduzimos que $k = (s/d)i$ com $i \in \{1, 2, \ldots, d\}$ qualquer, logo temos d escolhas para k.

2. Um homomorfismo de grupos $f : A \to B$ é dito trivial se $f(x) = 1$ para todo $x \in A$. Construa homomorfismos não triviais (se existirem)

   $$C_n \to S_3, \qquad S_3 \to C_{2n}$$

   onde S_3 é o grupo simétrico de grau 3. No caso de $f : S_3 \to C_{2n}$, defina $x := (12)$, $y := (123)$ e observe que $xyx^{-1} = y^2$, ou seja $xyx^{-1}y^{-1} = y$. Calcule $f(y)$ usando essa formula e deduza que $\langle y \rangle \leq \ker(f)$.

   Considere o caso $f : C_n \to S_3$. Seja H a imagem de f, é um subgrupo de S_3. Lembre-se que $H \cong C_n/\ker(f)$, logo $|H|$ divide n. Como $H \leq S_3$, temos que $|H|$ divide $|S_3| = 6$ também. Logo se $\mathrm{MDC}(n, 6) = 1$ então $H = \{1\}$ e não existem homomorfismos não triviais $C_n \to S_3$.

   Agora suponha que 2 divide n. Defina $f : C_n \to S_3$ por $f(x^h) := (12)^h$. Se trata de uma função bem definida. De fato, suponha que $x^{h_1} = x^{h_2}$, vamos mostrar que $f(x^{h_1}) = f(x^{h_2})$. Sabemos que $x^{h_1 - h_2} = 1$ logo n divide $h_1 - h_2$, e sendo n par obtemos que $h_1 - h_2$ é par, logo $(12)^{h_1 - h_2} = 1$ e segue $(12)^{h_1} = (12)^{h_2}$ ou seja $f(x^{h_1}) = f(x^{h_2})$. Além disso f é homomorfismo porque $f(x^{h+k}) = (12)^{h+k} = (12)^h(12)^k = f(x^h)f(x^k)$.

   Agora suponha que 3 divide n. Defina $f : C_n \to S_3$ por $f(x^h) := (123)^h$. Se trata de uma função bem definida. De fato, suponha que $x^{h_1} = x^{h_2}$, vamos mostrar que $f(x^{h_1}) = f(x^{h_2})$. Sabemos que $x^{h_1 - h_2} = 1$ logo n divide $h_1 - h_2$, e sendo n divisível por 3 obtemos que $h_1 - h_2$ é divisível por 3, logo $(123)^{h_1 - h_2} = 1$ e segue $(123)^{h_1} = (12)^{h_2}$ ou seja $f(x^{h_1}) =$

$f(x^{h_2})$. Além disso f é homomorfismo porque $f(x^{h+k}) = (123)^{h+k} = (123)^h(12)^k = f(x^h)f(x^k)$.

Considere o caso $f : S_3 \to C_{2n}$. Usando a dica, temos

$$f(y) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = 1$$

pois C_{2n} é abeliano, logo $y \in \ker(f)$. Escrevendo $C_{2n} = \langle t \rangle$, o elemento t^n tem ordem 2, logo obtemos um homomorfismo não trivial por composição $S_3 \to S_3/\langle (123) \rangle \cong C_2 \cong \langle t^n \rangle \to \langle t \rangle$ onde $S_3 \to S_3/\langle (123) \rangle$ é a projeção canônica e $\langle t^n \rangle \to \langle t \rangle$ é a inclusão. Explicitamente, $f : S_3 \to C_{2n}$ manda σ para t^n se σ é ímpar e para 1 se σ é par.

3. Sejam $G := A_4$, $H_m := \{g \in G \ : \ g^m = 1\}$. Para cada um dos inteiros seguintes, responda às perguntas: H_m é um subgrupo de G? H_m é um subgrupo normal de G? Caso H_m seja um subgrupo normal de G, o quociente G/H_m é abeliano? $m = n$, $m = n + 1$, $m = n + 2$.

   Se m é par e não divisível por 3 então

   $$H_m = K = \{1, (12)(34), (13)(24), (14)(23)\}$$

   é um subgrupo normal de G (como visto na lista T1) e G/K tem ordem 3, logo $G/K \cong C_3$ é abeliano: todo grupo de ordem prima é cíclico (como vimos usando o teorema de Lagrange) e todo grupo cíclico é abeliano.

   Se m é ímpar e divisível por 3 então

   $$H_m = \{1, (123), (132), (124), (142), (134), (143), (234), (243)\}$$

   tem 9 elementos, e como 9 não divide $|G| = |A_4| = 4!/2 = 12$, pelo teorema de Lagrange H_m não é um subgrupo de G.

   Um **erro comum** que vi é o seguinte: dados $G = A_4$ e por exemplo $H = H_{30}$, depois de provar que $H = G$, o/a aluno/a fala "G/H não é abeliano pois por exemplo $(123)H(12)(34)H \neq (12)(34)H(123)H$ sendo $(123)(12)(34) \neq (12)(34)(123)$". Isso está errado, o fato que dois elementos não comutam não implica que não comutam módulo H. De fato no caso específico temos $(123)H(12)(34)H = (12)(34)H(123)H$, ou seja $(123)(12)(34)H = (12)(34)(123)H$, porque em geral $xH = yH$ significa $y^{-1}x \in H$ e neste caso isso é óbviamente verdadeiro (com $x = (123)(12)(34)$, $y = (12)(34)(123)$), sendo $H = G$. G/G é abeliano porque $xGyG = yGxG$ para todo $x, y \in G$, sendo $xyG = yxG$ para todo $x, y \in G$, ou seja $(yx)^{-1}xy \in G$ (que é uma coisa óbvia, sendo $x, y \in G$).

4. Sejam $G := \mathbb{Z} \times \mathbb{Z}$ (produto direto dos grupos aditivos $\mathbb{Z}$ e $\mathbb{Z}$),

   $$A := 2\mathbb{Z} \times 4\mathbb{Z} \trianglelefteq G, \qquad B := \langle (1, n) \rangle \trianglelefteq G, \qquad C := \langle (n, n) \rangle \trianglelefteq G.$$

   Usando o teorema de isomorfismo, mostre que

   $$G/A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \qquad G/B \cong \mathbb{Z}, \qquad G/C \cong \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Aqui a notação é a usual (aditiva), $m\mathbb{Z} = \{mz \ : \ z \in \mathbb{Z}\}$ em $\mathbb{Z}$ e $\langle (x,y) \rangle = \{(mx, my) \ : \ m \in \mathbb{Z}\}$ em $\mathbb{Z} \times \mathbb{Z}$. Bonus (não vale ponto): consegue calcular $\mathbb{Z} \times \mathbb{Z}/\langle (x,y) \rangle$ em geral?

Antes de tudo, observe que uma função do tipo $\mathbb{Z} \times \mathbb{Z} \to A$, onde $A = \mathbb{Z}$ ou $A = \mathbb{Z}/m\mathbb{Z}$, definida por $f(s,t) := as + bt$ é sempre um homomorfismo de grupos aditivos, pois

$$\begin{aligned} f((s_1,t_1) + (s_2,t_2)) &= f(s_1 + t_1, s_2 + t_2) = a(s_1 + s_2) + b(t_1 + t_2) \\ &= (as_1 + bt_1) + (as_2 + bt_2) = f(s_1,t_1) + f(s_2,t_2). \end{aligned}$$

Além disso, é claro que se $f : A \to B$ e $h : A \to C$ são homomorfismos de grupos então $A \to B \times C$, $a \mapsto (f(a), h(a))$ é homomorfismo de grupos.

Defina

$$f_A : \mathbb{Z} \times \mathbb{Z} \to \frac{\mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 4\mathbb{Z}},$$
$$f_A(s,t) := (s + 2\mathbb{Z}, t + 4\mathbb{Z}).$$

Se trata de um homomorfismo de grupos aditivos e $f_A(s,t) = (0,0)$ se e somente se s é par e t é divisível por 4, ou seja $\ker(f_A) = A$. f_A é obviamente sobrejetivo. O resultado segue do teorema de isomorfismo.

Defina

$$f_B : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},$$
$$f_B(s,t) := ns - t.$$

Se trata de um homomorfismo de grupos aditivos e $f_B(s,t) = 0$ se e somente se $t = ns$, ou seja $(s,t) = (s,ns) = (1,n)s$. Em outras palavras $\ker(f_B) = B$. f_B é sobrejetivo pois se $z \in \mathbb{Z}$ então $f(0,-z) = z$. O resultado segue do teorema de isomorfismo.

Defina

$$f_C : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \frac{\mathbb{Z}}{n\mathbb{Z}},$$
$$f_C(s,t) := (s - t, s + n\mathbb{Z}).$$

Se trata de um homomorfismo de grupos aditivos. É sobrejetivo porque se $(u, v + n\mathbb{Z})$ pertence ao contradomínio então $f_C(v, v - u) = (u, v + n\mathbb{Z})$. Além disso $f_C(s,t) = (0,0)$ se e somente se $s = t$ e n divide s, ou seja $(s,t) = (nz, nz) = z(n,n)$ para algum $z \in \mathbb{Z}$, ou seja $\ker(f_C) = C$.

(**BONUS**) Dado $(x,y) \in \mathbb{Z} \times \mathbb{Z}$, vamos determinar o grupo

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (x,y) \rangle}$$

É claro que se $(x,y) = (0,0)$ então $\mathbb{Z} \times \mathbb{Z}/\langle (x,y) \rangle \cong \mathbb{Z} \times \mathbb{Z}$, agora suponha $(x,y) \neq (0,0)$. Se $x = 0$ então $\langle (x,y) \rangle = \langle (0,y) \rangle = \{0\} \times y\mathbb{Z}$ e temos, como no caso de $2\mathbb{Z} \times 4\mathbb{Z}$ acima,

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (0,y) \rangle} = \frac{\mathbb{Z} \times \mathbb{Z}}{\{0\} \times y\mathbb{Z}} \cong \mathbb{Z} \times \frac{\mathbb{Z}}{y\mathbb{Z}},$$

e analogamente se $y = 0$ então

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (x, 0) \rangle} = \frac{\mathbb{Z} \times \mathbb{Z}}{x\mathbb{Z} \times \{0\}} \cong \frac{\mathbb{Z}}{x\mathbb{Z}} \times \mathbb{Z}.$$

Agora suponha $x \neq 0 \neq y$. Mostraremos que

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (x, y) \rangle} \cong \mathbb{Z} \times \frac{\mathbb{Z}}{d\mathbb{Z}}$$

onde

$$d = \text{MDC}(x, y).$$

Para isso, observe que pelo Algoritmo de Euclides existem inteiros α, β tais que $\alpha x + \beta y = d$, em outras palavras

$$\alpha x/d + \beta y/d = 1.$$

Defina

$$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \frac{\mathbb{Z}}{d\mathbb{Z}}$$

$$f(s, t) := (tx/d - sy/d, \alpha s + \beta t + d\mathbb{Z}).$$

Se trata de um homomorfismo de grupos aditivos, que é sobrejetivo porque se $(u, v + d\mathbb{Z}) \in \mathbb{Z} \times (\mathbb{Z}/d\mathbb{Z})$ então

$$f(-u\beta + vx/d, u\alpha + vy/d) = (u, v + d\mathbb{Z}).$$

Mostraremos agora que $\ker(f) = \langle (x, y) \rangle$.

A inclusão $\langle (x, y) \rangle \leq \ker(f)$ é óbvia, agora mostraremos a outra inclusão, $\ker(f) \leq \langle (x, y) \rangle$. Se $(s, t) \in \ker(f)$ então $sy/d = tx/d$ e d divide $\alpha s + \beta t$. Como y/d divide tx/d, x/d divide sy/d e $\text{MDC}(x/d, y/d) = 1$, segue que y/d divide t e x/d divide s. Escrevendo $t = (y/d)a$ e $s = (x/d)b$ podemos re-escrever a igualdade $sy/d = tx/d$ como $a = b$. Segue que $(s, t) = a(x/d, y/d)$. Por outro lado d divide $\alpha s + \beta t = \alpha a x/d + \beta a y/d = a$, digamos $a = dw$. Segue que $(s, t) = a(x/d, y/d) = (wx, wy) \in \langle (x, y) \rangle$.

O resultado agora segue do teorema de isomorfismo.

T4 – Trabalho semanal 4 de Álgebra 2 – Semestre 2021-1

Semana: 16-20 de agosto, 2021.
Prazo de entrega: 02 de setembro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 3a + 2b + c + 8.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Conte os grupos abelianos de ordem m, a menos de isomorfismo, para cada um dos valores seguintes: $m = n$, $m = n + 1$, $m = n + 2$.

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

2. Um grupo G é dito "metacíclico" se admite um subgrupo normal N tal que N e G/N são grupos cíclicos. Para cada um dos grupos seguintes, diga se é metacíclico: S_3, S_4, $C_n \times C_{n+1} \times C_{n+2}$.

   Atenção: aqui n não é um inteiro qualquer, é o número definido acima!

3. Mostre que se G é um grupo metacíclico e $H \leq G$ então H é metacíclico.

4. O primeiro número primo é 2, o segundo é 3, o terceiro é 5, o quarto é 7, o quinto é 11, e assim diante. Seja $m := a + 3$ e seja p o m-esimo número primo.

   (a) Seja A o conjunto dos números racionais da forma r/s onde r, s são inteiros tais que $s \neq 0$ e p não divide s, ou seja

   $$A := \{r/s \ : \ r, s \in \mathbb{Z}, \ s \neq 0, \ p \text{ não divide } s\} \subseteq \mathbb{Q}.$$

   Mostre que A é um domínio de integridade com as operações usuais de soma e multiplicação em $\mathbb{Q}$. O que consegue dizer sobre o seu corpo de frações?

   (b) Seja $F := \mathbb{Z}/3\mathbb{Z}$ e considere o conjunto $A = F \times F$ com as operações seguintes.

   $$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
   $$(x_1, y_1) \cdot (x_2, y_2) = (-mx_1x_2 + x_1y_2 + x_2y_1, y_1y_2 - (m + 1)x_1x_2).$$

   (m é o número definido acima). Sabendo que A com essas operações é um anel comutativo unitário, encontre os elementos neutros de A e responda à pergunta: A é um domínio de integridade?

   Atenção: aqui a não é um inteiro qualquer, é o número definido acima!

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T4 – Álgebra 2 – 2021-1 - Gabarito.

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Conte os grupos abelianos de ordem m, a menos de isomorfismo, para cada um dos valores seguintes: $m = n$, $m = n + 1$, $m = n + 2$.

   Lembre-se que, pelo teorema fundamental sobre grupos abelianos finitos, todo grupo abeliano finito é isomorfo a um produto direto de grupos cíclicos finitos. Escrevendo $m = \prod_{i=1}^{t} p_i^{a_i}$ como produto de potências de primos, onde $p_i \neq p_j$ para todo $i \neq j$, como $C_r \times C_s \cong C_{rs}$ se $\mathrm{MCD}(r, s) = 1$, podemos decompor um grupo abeliano de ordem m como um produto direto $P_1 \times \ldots \times P_t$ onde $|P_i| = p_i^{a_i}$ para todo i. Desta forma, estamos reduzidos a determinar os grupos abelianos finitos de ordem uma potência de primo.

   Vamos analizar alguns valores de m.

   (a) $m = 19$. Neste caso m é primo, logo existe um único grupo abeliano de ordem 19, o grupo cíclico C_{19}.

   (b) $m = 20 = 2^2 \cdot 5$. As possibilidades são $C_4 \times C_5 \cong C_{20}$ e $C_2 \times C_2 \times C_5$. No total, temos 2 possibilidades.

   (c) $m = 72 = 2^3 \cdot 3^2$. As possibilidades são $P_1 \times P_2$ onde P_1 é isomorfo a C_8, $C_2 \times C_4$ ou $C_2 \times C_2 \times C_2$ (3 possibilidades) e P_2 é isomorfo a C_9 ou $C_3 \times C_3$ (2 possibilidades). No total, temos $3 \cdot 2 = 6$ possibilidades.

   (d) $m = 64 = 2^6$. Neste caso temos as 11 possibilidades seguintes. C_{64}, $C_2 \times C_{32}$, $C_4 \times C_{16}$, ${C_8}^2$, ${C_2}^2 \times C_{16}$, $C_2 \times C_4 \times C_8$, ${C_4}^3$, ${C_2}^3 \times C_8$, ${C_2}^2 \times {C_4}^2$, ${C_2}^4 \times C_4$, ${C_2}^5$.

2. Um grupo G é dito "metacíclico" se admite um subgrupo normal N tal que N e G/N são grupos cíclicos. Para cada um dos grupos seguintes, diga se é metacíclico: S_3, S_4, $C_n \times C_{n+1} \times C_{n+2}$.

   S_3 é metacíclico porque $A_3 = \{1, (123), (132)\} = \langle (123) \rangle$ é normal e cíclico em S_3 e S_3/A_3 é isomorfo a $\{1, -1\} \cong C_2$ (pelo teorema de isomorfismo aplicado ao homomorfismo "sinal" $S_3 \to \{1, -1\}$).

   S_4 não é metacíclico porque o único subgrupo normal cíclico de S_4 é $\{1\}$ e $S_4/\{1\} \cong S_4$ não é abeliano. Para mostrar que o único subgrupo normal cíclico de S_4 é $\{1\}$ pode se fazer da forma seguinte. Se $1 \neq g \in G = S_4$ então g tem ordem 2, 3 ou 4, logo $H = \langle g \rangle$ possui 2, 3 ou 4 elementos. Se H fosse normal então H deveria conter todos os conjugados de g em $G = S_4$, ou seja todos os elementos que têm a mesma estrutura cíclica de g. Mas isso não é possível pois se g tem estrutura $(2, 2)$ então possui 3 conjugados e $|H| = 2$, se g tem estrutura (2) então possui 6 conjugados e $|H| = 2$, se g tem estrutura (3) então possui 8 conjugados e $|H| = 3$, se g tem estrutura (4) então possui 6 conjugados e $|H| = 4$.

$G = C_n \times C_{n+1} \times C_{n+2}$ é metacíclico. Para ver isso, observe que n e $n+1$ são coprimos, logo $C_n \times C_{n+1} \cong C_{n(n+1)}$ e $G \cong C_{n(n+1)} \times C_{n+2}$. O subgrupo normal $N = C_{n(n+1)} \times \{1\} \trianglelefteq G$ tem a propriedade que $G/N \cong C_{n+2}$ (isso foi visto em geral na aula teórica sobre produtos diretos). No caso particular em que n é ímpar, G é, na verdade, cíclico, pois n, $n+1$ e $n+2$ são dois a dois coprimos, logo G é metacíclico pois o subgrupo trivial $\langle 1 \rangle$ é cíclico (gerado por 1) e $G/\{1\} \cong G$ é cíclico.

3. Mostre que se G é um grupo metacíclico e $H \leq G$ então H é metacíclico.

   Por hipótese existe $N \trianglelefteq G$ tal que N e G/N são cíclicos. Vamos mostrar que $H \cap N$ e $H/H \cap N$ são cíclicos. O grupo $H \cap N$ é cíclico pois é um subgrupo de N, que é cíclico. Pelo segundo teorema de isomorfismo $H/H \cap N \cong HN/N \leq G/N$, e G/N é cíclico, logo HN/N é cíclico, sendo um subgrupo de G/N. Como $H/H \cap N$ é isomorfo a um grupo cíclico, é cíclico também.

4. O primeiro número primo é 2, o segundo é 3, o terceiro é 5, o quarto é 7, o quinto é 11, e assim diante. Seja $m := a + 3$ e seja p o m-esimo número primo.

   (a) Seja A o conjunto dos números racionais da forma r/s onde r, s são inteiros tais que $s \neq 0$ e p não divide s, ou seja

   $$A := \{r/s \ : \ r, s \in \mathbb{Z}, \ s \neq 0, \ p \text{ não divide } s\} \subseteq \mathbb{Q}.$$

   Mostre que A é um domínio de integridade com as operações usuais de soma e multiplicação em $\mathbb{Q}$. O que consegue dizer sobre o seu corpo de frações?

   Primeiro, observe que as operações usuais são bem definidas em A. Para isso precisamos mostrar que se $r_1/s_1, r_2/s_2 \in A$ então $r_1/s_1 + r_2/s_2 = (r_1 s_2 + s_1 r_2)/(s_1 s_2) \in A$ e $(r_1/s_1)(r_2/s_2) = (r_1 r_2)/(s_1 s_2) \in A$. Para isso, precisamos mostrar que p não divide $s_1 s_2$, e isso segue do fato que p é primo e não divide s_1 nem s_2. Os elementos neutros de A são $0/1$ e $1/1$, os mesmos de $\mathbb{Q}$, e o inverso aditivo de $r/s \in A$ é $(-r)/s \in A$. Isso mostra que A é um subanel de $\mathbb{Q}$, porque as propriedades associativa e distributiva são herdadas de $\mathbb{Q}$ (não precisa verificar de novo!). Além disso, como $\mathbb{Q}$ é um corpo, A é um domínio, sendo subanel de um corpo. O corpo de frações de A é o próprio $\mathbb{Q}$, porque se $a/b \in \mathbb{Q}$ então $a = a/1 \in A$, $b = b/1 \in A$, logo $(a/1)/(b/1) = a/b$ pertence ao corpo de frações de A.

   (b) Seja $F := \mathbb{Z}/3\mathbb{Z}$ e considere o conjunto $A = F \times F$ com as operações seguintes.

   $$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
   $$(x_1, y_1) \cdot (x_2, y_2) = (-m x_1 x_2 + x_1 y_2 + x_2 y_1, y_1 y_2 - (m+1) x_1 x_2).$$

(m é o número definido acima). Sabendo que A com essas operações é um anel comutativo unitário, encontre os elementos neutros de A e responda à pergunta: A é um domínio de integridade?

Observe que os elementos neutros são, obviamente, $(0,0)$ e $(0,1)$. É claro que a única coisa que importa em relação a m é a classe de m módulo 3. Vamos considerar os três casos. Lembre-se que $F = \mathbb{Z}/3\mathbb{Z}$ é um corpo (sendo 3 um número primo), logo a lei de cancelamento vale em F.

- $m \equiv 0 \mod 3$. Neste caso $(x_1, y_1) \cdot (x_2, y_2) = (0,0)$ se e somente se
$$x_1y_2 + x_2y_1 = 0, \qquad y_1y_2 - x_1x_2 = 0.$$
Multiplicando a primeira equação por x_1 e usando $x_1x_2 = y_1y_2$ obtemos
$$y_2(x_1^2 + x_2^2) = 0.$$
Se $y_2 = 0$ então $x_1x_2 = 0$ e se $x_2 \neq 0$ então $x_1 = 0$, logo $x_2y_1 = 0$ e $y_1 = 0$, o que implica $(x_1, y_1) = (0,0)$. Se, por outro lado, $x_2 = 0$ então $(x_2, y_2) = (0,0)$. Agora suponha $y_2 \neq 0$. Segue $x_1^2 + x_2^2 = 0$. Se $x_2 = 0$ então $(x_2, y_2) = (0,0)$, se por outro lado $x_2 \neq 0$ então podemos multiplicar a equação $x_1^2 + x_2^2 = 0$ por $x_2^{-2} \in F$, obtendo $t^2 + 1 = 0$ onde $t = x_1/x_2 \in F = \{0, 1, 2\}$. Mas isso é uma contradição porque, definindo $P(X) := X^2 + 1$, temos $P(0) = 1 \neq 0$, $P(1) = 2 \neq 0$ e $P(2) = 4 = 1 \neq 0$.
- $m \equiv 1 \mod 3$. Neste caso $(x_1, y_1) \cdot (x_2, y_2) = (0,0)$ se e somente se
$$-x_1x_2 + x_1y_2 + x_2y_1 = 0, \qquad y_1y_2 + x_1x_2 = 0.$$
Se $y_2 = 0$ então $x_1x_2 = 0$, logo se $x_2 \neq 0$ então $x_1 = 0$, segue $x_2y_1 = 0$ logo $y_1 = 0$ ou seja $(x_1, y_1) = (0,0)$ neste caso, se por outro lado $x_2 = 0$ então $(x_2, y_2) = (0,0)$. Segue que podemos supor $y_2 \neq 0$.
Usando a segunda equação, a primeira pode ser escrita $y_1y_2 + x_1y_2 + x_2y_1 = 0$, e multiplicando por x_1 obtemos $x_1y_1y_2 + x_1^2y_2 + x_1x_2y_1 = 0$. Lembrando que $x_1x_2 = -y_1y_2$ obtemos
$$y_2(x_1y_1 + x_1^2 - y_1^2) = 0.$$
Como $y_2 \neq 0$, deduzimos que $x_1y_1 + x_1^2 - y_1^2 = 0$ (*). Se $y_1 = 0$ então $x_1^2 = 0$ o que implica $(x_1, y_1) = (0,0)$, logo podemos supor $y_1 \neq 0$. Seja $t := x_1y_1^{-1} \in F$. Multiplicando (*) por y_1^{-1} obtemos $t^2 + t - 1 = 0$. Definindo $P(X) := X^2 + X - 1$, temos que $P(0) = -1 \neq 0$, $P(1) = 1 \neq 0$, $P(2) = 5 = 2 \neq 0$ em $F = \mathbb{Z}/3\mathbb{Z}$, uma contradição.
- $m \equiv 2 \mod 3$. Neste caso $(x_1, y_1) \cdot (x_2, y_2) = (0,0)$ se e somente se
$$x_1x_2 + x_1y_2 + x_2y_1 = 0, \qquad y_1y_2 = 0.$$

Da segunda equação segue $y_1 = 0$ ou $y_2 = 0$. No primeiro caso $x_1(x_2 + y_2) = 0$ e se $x_1 \neq 0$ então $x_2 + y_2 = 0$, logo escolhendo $(x_1, y_1) = (1, 0)$, $(x_2, y_2) = (1, 2)$ obtemos $(1, 0) \cdot (1, 2) = (0, 0)$ e A não é um domínio.

T5 – Trabalho semanal 5 de Álgebra 2 – Semestre 2021-1

Semana: 23-27 de agosto, 2021.
Prazo de entrega: 09 de setembro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 3(9-a) + 2(9-b) + (9-c) + 7.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Aplicando o algoritmo de Euclides, encontre $x, y \in \mathbb{Z}$ tais que

   $$mx + (m+8)y = \text{MDC}(m, m+8)$$

   nos casos seguintes: $m = n + 10$, $m = n + 11$.

   Atenção: n não é um inteiro qualquer, é o número definido acima!

2. Seja $D(X)$ o MDC (maior divisor comum) entre

   $$P_1(X) = X^3 + nX + 1 \qquad \text{e} \qquad P_2(X) = 2X^2 + X - n$$

   no anel $\mathbb{F}_7[X]$ (onde $\mathbb{F}_7$ é o corpo $\mathbb{Z}/7\mathbb{Z}$). Aplicando o algoritmo de Euclides, encontre $A_1(X), A_2(X) \in \mathbb{F}_7[X]$ tais que

   $$A_1(X)P_1(X) + A_2(X)P_2(X) = D(X).$$

   Atenção: n não é um inteiro qualquer, é o número definido acima!

3. Seja $m := (a+2)^2$ e seja A o anel $\mathbb{Z}/m\mathbb{Z}$. Encontre um anel comutativo unitário B não isomorfo a A (ou seja, não existe nenhum isomorfismo de aneis $A \to B$) e tal que $|A| = |B|$. [Não basta escrever quem é B, tem que mostrar que não é isomorfo a A.]

   Atenção: a não é um inteiro qualquer, é o número definido acima!

4. Seja p um número primo. Seja A o conjunto dos números racionais da forma r/s onde r, s são inteiros tais que $s \neq 0$ e p não divide s, ou seja

   $$A := \{r/s \ : \ r, s \in \mathbb{Z},\ s \neq 0,\ p \text{ não divide } s\} \subseteq \mathbb{Q}.$$

   (a) Seja I um ideal de A. Mostre que se $I \neq A$ então $I \subseteq (p)$, onde $(p) = pA$ é o ideal principal gerado por p. [Dica: use o fato que $I \neq A$ implica $1 \notin I$ (por quê?).]

   (b) Mostre que $A/(p) \cong \mathbb{Z}/p\mathbb{Z}$ (isomorfismo de aneis!) construindo um oportuno homomorfismo de aneis $A \to \mathbb{Z}/p\mathbb{Z}$ e usando o teorema de isomorfismo.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T5 – Álgebra 2 – 2021-1 - Gabarito.

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Aplicando o algoritmo de Euclides, encontre $x, y \in \mathbb{Z}$ tais que

$$mx + (m+8)y = \text{MDC}(m, m+8)$$

nos casos seguintes: $m = n + 10$, $m = n + 11$.

Vamos analizar alguns valores de m.

$m = 54$. Temos $\text{MDC}(54, 62) = 2$.

62	54	
1	0	62
0	1	54
1	-1	8
-6	7	6
7	-8	2

Segue que $7 \cdot 62 + (-8) \cdot 54 = 2$.

$m = 61$. Temos $\text{MDC}(61, 69) = 1$.

69	61	
1	0	69
0	1	61
1	-1	8
-7	8	5
8	-9	3
-15	17	2
23	-26	1

Segue que $23 \cdot 69 + (-26) \cdot 61 = 1$.

2. Seja $D(X)$ o MDC (maior divisor comum) entre

$$P_1(X) = X^3 + nX + 1 \qquad \text{e} \qquad P_2(X) = 2X^2 + X - n$$

no anel $\mathbb{F}_7[X]$ (onde $\mathbb{F}_7$ é o corpo $\mathbb{Z}/7\mathbb{Z}$). Aplicando o algoritmo de Euclides, encontre $A_1(X), A_2(X) \in \mathbb{F}_7[X]$ tais que

$$A_1(X)P_1(X) + A_2(X)P_2(X) = D(X).$$

Atenção: n não é um inteiro qualquer, é o número definido acima!

Vamos analizar alguns valores de n.

$n = 30 \equiv 2 \mod 7$. Temos $P_1(X) = X^3 + 2X + 1$, $P_2(X) = 2X^2 + X - 2$.

X^3+2X+1	$2X^2+X-2$	
1	0	X^3+2X+1
0	1	$2X^2+X-2$
1	$3X+2$	$5X+4$
$X+6$	$3X^2-X-1$	1

Os quocientes são $4X+5$ e $6X+1$. Escolhendo $A_1(X) = X+6$, $A_2(X) = 3X^2 - X - 1$ obtemos

$$A_1(X)P_1(X) + A_2(X)P_2(X) = 1.$$

O maior divisor comum mônico entre $P_1(X)$ e $P_2(X)$ é 1.

$n = 55 \equiv 6 \mod 7$. Temos $P_1(X) = X^3+6X+1$, $P_2(X) = 2X^2+X-6$.

X^3+6X+1	$2X^2+X-6$	
1	0	X^3+6X+1
0	1	$2X^2+X-6$
1	$3X+2$	$4X+3$
$3X+1$	$2X^2+2X+3$	4

Os quocientes são $4X+5$, $4X+6$. Escolhendo $A_1(X) = 2(3X+1)$, $A_2(X) = 2(2X^2+2X+3)$ obtemos

$$A_1(X)P_1(X) + A_2(X)P_2(X) = 2 \cdot 4 = 1.$$

O maior divisor comum mônico entre $P_1(X)$ e $P_2(X)$ é 1.

3. Seja $m := (a+2)^2$ e seja A o anel $\mathbb{Z}/m\mathbb{Z}$. Encontre um anel comutativo unitário B não isomorfo a A (ou seja, não existe nenhum isomorfismo de aneis $A \to B$) e tal que $|A| = |B|$. [Não basta escrever quem é B, tem que mostrar que não é isomorfo a A.]

   Aqui m é um número do tipo k^2 com $k \geq 2$. Considere o anel $B := \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ (produto direto de aneis, com as operações definidas por componentes). Os aneis A e B têm tamanho k^2 e não são isomorfos porque se existisse um isomorfismo de aneis $f : A \to B$ então f seria em particular um isomorfismo de grupos aditivos. Por outro lado os grupos aditivos A e B não são isomorfos porque A é cíclico e B não é cíclico, sendo $kb = 0$ para todo $b \in B$ e $|B| = k^2$.

   ERRO COMUM. Alguns alunos escreveram que se F é um corpo, o produto direto $F \times F$ é um corpo. Isso é falso! De fato, o elemento $(1,0) \in F \times F$ não é nulo (é diferente de $(0,0)$) e não admite inverso, porque em geral o inverso de (a,b), quando existe, é (a^{-1}, b^{-1}). Na verdade, $F \times F$ não é nem domínio de integridade, pois $(1,0) \cdot (0,1) = (0,0)$.

4. Seja p um número primo. Seja A o conjunto dos números racionais da forma r/s onde r, s são inteiros tais que $s \neq 0$ e p não divide s, ou seja

$$A := \{r/s \ : \ r, s \in \mathbb{Z},\ s \neq 0,\ p \text{ não divide } s\} \subseteq \mathbb{Q}.$$

(a) Seja I um ideal de A. Mostre que se $I \neq A$ então $I \subseteq (p)$, onde $(p) = pA$ é o ideal principal gerado por p. [Dica: use o fato que $I \neq A$ implica $1 \notin I$ (por quê?).]

Se $1 \in I$ então para todo $a \in A$ temos $a = a \cdot 1 \in I$, sendo I ideal. Segue que $I = A$. Logo se $I \neq A$ então $1 \notin I$. Segue que I não contém nenhum elemento inversível, porque se $t \in I$ é inversível então I contém $t \cdot t^{-1} = 1$, sendo I ideal. Os elementos inversíveis de A são do tipo r/s com $s/r \in A$, ou seja p não divide r. Segue que se $r/s \in I$ então p divide r, digamos $r = pz$ com $z \in \mathbb{Z}$. Segue que $r/s = p \cdot z/s \in (p)$. Isso mostra que $I \subseteq (p)$.

(b) Mostre que $A/(p) \cong \mathbb{Z}/p\mathbb{Z}$ (isomorfismo de aneis!) construindo um oportuno homomorfismo de aneis $A \to \mathbb{Z}/p\mathbb{Z}$ e usando o teorema de isomorfismo.

Defina $f : A \to \mathbb{Z}/p\mathbb{Z}$ por $f(r/s) := \overline{r} \cdot \overline{s}^{-1}$, onde a notação $\overline{z}$ significa $z \mod p$. Observe que f é bem definida pois se $r/s \in A$ então p não divide s, logo $\overline{s}$ admite inverso em $\mathbb{F}_p$. Por abuso de notação, indicaremos $\overline{z}$ simplesmente por z. Observe que

$$f\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) = f\left(\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\right) = (r_1 s_2 + r_2 s_1)(s_1 s_2)^{-1},$$

$$f\left(\frac{r_1}{s_1}\right) + f\left(\frac{r_2}{s_2}\right) = r_1 s_1^{-1} + r_2 s_2^{-1}$$

são iguais, e que

$$f\left(\frac{r_1}{s_1} \cdot \frac{r_2}{s_2}\right) = f\left(\frac{r_1 r_2}{s_1 s_2}\right) = (r_1 r_2)(s_1 s_2)^{-1},$$

$$f\left(\frac{r_1}{s_1}\right) \cdot f\left(\frac{r_2}{s_2}\right) = (r_1 s_1^{-1})(r_2 s_2^{-1})$$

são iguais. Além disso $f(1/1) = 1 \cdot 1^{-1} = 1$. Isso mostra que f é homomorfismo de aneis. É sobrejetivo porque $f(r/1) = r$ para todo $r \in \mathbb{Z}$. O seu núcleo é dado pelos elementos r/s tais que $\overline{r} \cdot \overline{s}^{-1} = 0$, ou seja p divide r. Em outras palavras $\ker(f) = pA = (p)$. O resultado segue do teorema de isomorfismo.

ERRO COMUM. Alguns alunos definiram $f : A \to \mathbb{Z}/p\mathbb{Z}$ por $f(r/s) := \overline{r}$, onde r/s está escrito na sua forma reduzida com r positivo e coprimo com s. Se trata claramente de uma função bem definida, mas não é homomorfismo de aneis! De fato, por exemplo, $f(p/(p-1) - 1/(p-1)) = f(1) = \overline{1}$ mas $f(p/(p-1)) - f(1/(p-1)) = \overline{p-1} \neq \overline{1}$.

T6 – Trabalho semanal 6 de Álgebra 2 – Semestre 2021-1

Semana: 30 de agosto - 03 de setembro, 2021.
Prazo de entrega: 16 de setembro, 2021.

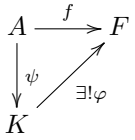
Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Seja $|x|$ o valor absoluto ("módulo") do número x, ou seja $|x| = x$ se $x \geq 0$ e $|x| = -x$ se $x < 0$ (por exemplo $|-2| = 2$, $|0| = 0$, $|3| = 3$). Defina

$$n := 3|a-5| + 2|b-5| + |c-5| + 7.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Seja $A \neq \{0\}$ um domínio de integridade e seja $K = K(A)$ o seu corpo de frações. Seja $\psi : A \to K$, $\psi(a) := a/1$. Seja F um corpo e seja $f : A \to F$ um homomorfismo injetivo de aneis.

   Mostre que **existe** um **único** homomorfismo de aneis $\varphi : K \to F$ tal que $\varphi \circ \psi = f$ (ou seja $\varphi(\psi(a)) = f(a)$ para todo $a \in A$).



2. Resolva os itens seguintes.
   (a) Mostre que $\mathbb{Q}[X]/(X - n) \cong \mathbb{Q}$.
   (b) Conte os ideais de $\mathbb{Z}/m\mathbb{Z}$ onde $m = n(n+1)$
   (c) Conte os ideais de $\mathbb{Q}[X]/(X^n(X^2 - 1))$.

3. Seja p um número primo. Seja A o conjunto dos números racionais da forma r/s onde r, s são inteiros tais que $s \neq 0$ e p não divide s, ou seja

   $$A := \{r/s \ : \ r, s \in \mathbb{Z},\ s \neq 0,\ p \text{ não divide } s\} \subseteq \mathbb{Q}.$$

   Mostre que os ideais não nulos de A são todos do tipo $(p^m) = p^m A$ onde m é um inteiro não negativo.

4. Diga se existem homomorfismos de aneis

   $$\mathbb{R} \to \frac{\mathbb{Z}}{n\mathbb{Z}}, \qquad \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \qquad \frac{\mathbb{Z}}{n\mathbb{Z}} \times \mathbb{Z} \to \mathbb{Q}, \qquad \mathbb{Z}[X] \to \mathbb{Q}, \qquad \mathbb{C} \to \mathbb{Z}[i].$$

   Perceba que a função nula não é homomorfismo de aneis pois todo homomorfismo de aneis manda 1 para 1. Aqui $A \times B$ denota o produto direto, com as operações definidas por componentes, e $\mathbb{Z}[i] = \{a + ib \ : \ a, b \in \mathbb{Z}\}$, onde i é a unidade imaginária: $i^2 = -1$.

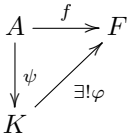
[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T6 – Trabalho semanal 6 de Álgebra 2 – Gabarito

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Seja $A \neq \{0\}$ um domínio de integridade e seja $K = K(A)$ o seu corpo de frações. Seja $\psi : A \to K$, $\psi(a) := a/1$. Seja F um corpo e seja $f : A \to F$ um homomorfismo injetivo de aneis.

   Mostre que **existe** um **único** homomorfismo de aneis $\varphi : K \to F$ tal que $\varphi \circ \psi = f$ (ou seja $\varphi(\psi(a)) = f(a)$ para todo $a \in A$).

   Observe que se $\varphi : K \to F$ é homomorfismo de aneis tal que $\varphi(a/1) = f(a)$ para todo $a \in A$, então

   $$\varphi\left(\frac{a}{b}\right) \cdot f(b) = \varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{b}{1}\right) = \varphi\left(\frac{a}{b} \cdot \frac{b}{1}\right) = \varphi\left(\frac{a}{1}\right) = f(a),$$

   logo necessariamente $\varphi(a/b)f(b) = f(a)$ para todo $a/b \in K$, e como $b \neq 0$ e f é injetiva, $f(b) \neq 0$, logo $f(b)$ é inversível em F (pois F é corpo), e $\varphi(a/b) = f(a)f(b)^{-1}$.

   Segue que a existência e unicidade de φ segue se conseguirmos mostrar que $\varphi : K \to F$ definida por $\varphi(a/b) := f(a)f(b)^{-1}$ é homomorfismo de aneis. Se trata de uma função bem definida pois, sendo f injetiva e $b \neq 0$, temos $0 \neq f(b) \in F$ logo existe o inverso de $f(b)$ em F (sendo F corpo). Além disso, se $a/b = c/d$, então $ad = bc$, logo $f(ad) = f(bc)$, ou seja $f(a)f(d) = f(b)f(c)$, e isso implica que $f(a)/f(b) = f(c)/f(d)$, ou seja $\varphi(a/b) = \varphi(c/d)$.

   É claro que $\varphi(1/1) = f(1)f(1)^{-1} = 1$. Além disso

   $$\begin{aligned}\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \varphi\left(\frac{ad+bc}{bd}\right) &= f(ad+bc) \cdot f(bd)^{-1} \\ &= (f(a)f(d) + f(b)f(c))(f(b)^{-1}f(d)^{-1}) \\ &= f(a)f(b)^{-1} + f(c)f(d)^{-1} = \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right).\end{aligned}$$

   $$\begin{aligned}\varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \varphi\left(\frac{ac}{bd}\right) &= f(ac)f(bd)^{-1} = f(a)f(c)f(b)^{-1}f(d)^{-1} \\ &= f(a)f(b)^{-1} \cdot f(c)f(d)^{-1} = \varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right).\end{aligned}$$

2. Resolva os itens seguintes.

(a) Mostre que $\mathbb{Q}[X]/(X-n) \cong \mathbb{Q}$.

(b) Conte os ideais de $\mathbb{Z}/m\mathbb{Z}$ onde $m = n(n+1)$

(c) Conte os ideais de $\mathbb{Q}[X]/(X^n(X^2-1))$.

Item a. Seja $f : \mathbb{Q}[X] \to \mathbb{Q}$ definida por $f(P(X)) := P(n)$. Se trata de um homomorfismo de aneis (é um homomorfismo de substituição). f é sobrejetiva pois se $y \in \mathbb{Q}$ então $f(y) = y$. Para terminar, pelo teorema de isomorfismo, basta mostrar que $\ker(f) = (X-n)$. A inclusão $\supseteq$ é clara, pois se um polinômio é da forma $(X-n)Q(X)$ com $Q(X) \in \mathbb{Q}[X]$, então $f((X-n)Q(X)) = (n-n)Q(n) = 0$. Para mostrar a inclusão $\subseteq$ considere $P(X) \in \ker(f)$, a divisão com resto entre $P(X)$ e $X-n$ é $P(X) = (X-n)Q(X) + r$ com $r \in \mathbb{Q}$. Temos $0 = P(n) = r$, logo $P(X) = (X-n)Q(X) \in (X-n)$.

Item b. Considere por exemplo $n = 50$. Então $m = 50 \cdot 51 = 2 \cdot 3 \cdot 17 \cdot 5^2$. Os divisores de m são do tipo $2^{a_1} \cdot 3^{a_2} \cdot 17^{a_3} \cdot 5^{a_4}$ com $a_1, a_2, a_3 \in \{0,1\}$ e $a_4 \in \{0,1,2\}$. Segue que m admite exatamente $2^3 \cdot 3 = 24$ divisores inteiros positivos, logo $\mathbb{Z}/m\mathbb{Z}$ admite exatamente 24 ideais.

Item c. Analogamente ao caso anterior, $\mathbb{Q}[X]/(X^n(X^2-1))$ tem exatamente $4(n+1)$ divisores, que são os divisores de $X^n(X-1)(X+1)$.

3. Seja p um número primo. Seja A o conjunto dos números racionais da forma r/s onde r, s são inteiros tais que $s \neq 0$ e p não divide s, ou seja

$$A := \{r/s \ : \ r, s \in \mathbb{Z},\ s \neq 0,\ p \text{ não divide } s\} \subseteq \mathbb{Q}.$$

Mostre que os ideais não nulos de A são todos do tipo $(p^m) = p^m A$ onde m é um inteiro não negativo.

Seja I um ideal de A e suponha que $I \neq \{0\}$. Assim existe $r/s \in I$ com $r \neq 0$ e escrevendo $r = p^t \cdot h$ com h não divisível por p, temos $s/h \in U(A)$, logo $p^t = (r/s) \cdot s/h \in I$. A existência de tal elemento mostra que o número seguinte é bem definido: seja m o menor inteiro não negativo tal que $p^m \in I$. Mostraremos que $I = (p^m)$. A inclusão $\supseteq$ é clara por definição de ideal, sendo $p^m \in I$, e para mostrar a inclusão $\subseteq$ considere $r/s \in I$ não nulo, e escreva $r = p^t \cdot h$ com h não divisível por p. Sendo $p^t = (r/s) \cdot s/h \in I$, temos que $t \geq m$ por definição de m. Logo $r/s = p^{t-m} \cdot p^m \cdot h/s \in (p^m)$.

4. Diga se existem homomorfismos de aneis

$$\mathbb{R} \to \frac{\mathbb{Z}}{n\mathbb{Z}}, \qquad \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \qquad \frac{\mathbb{Z}}{n\mathbb{Z}} \times \mathbb{Z} \to \mathbb{Q}, \qquad \mathbb{Z}[X] \to \mathbb{Q}, \qquad \mathbb{C} \to \mathbb{Z}[i].$$

Perceba que a função nula não é homomorfismo de aneis pois todo homomorfismo de aneis manda 1 para 1. Aqui $A \times B$ denota o produto direto, com as operações definidas por componentes, e $\mathbb{Z}[i] = \{a + ib \ : \ a, b \in \mathbb{Z}\}$, onde i é a unidade imaginária: $i^2 = -1$.

(a) Se existe um homomorfismo de aneis $f : \mathbb{R} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ então

$$f(n) = f(1 + 1 + \ldots + 1) = f(1) + f(1) + \ldots + f(1) = n \cdot f(1) = 0,$$

logo $1 = f(1) = f(n \cdot (1/n)) = f(n) \cdot f(1/n) = 0$, uma contradição. Isso mostra que f não existe.

(b) A função $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $f(z) := (z, z)$ é homomorfismo de aneis.

(c) A função $f : \frac{\mathbb{Z}}{n\mathbb{Z}} \times \mathbb{Z} \to \mathbb{Q}$ definida por $f(\overline{x}, y) := y$ é homomorfismo de aneis, sendo a composição entre a projeção na segunda componente $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ e a inclusão $\mathbb{Z} \to \mathbb{Q}$.

(d) A função $f : \mathbb{Z}[X] \to \mathbb{Q}$ definida por $f(P(X)) := P(0)$ é um homomorfismo de aneis sendo a composição entre o homomorfismo de substituição $v_0 : \mathbb{Z}[X] \to \mathbb{Z}$ e a inclusão $\mathbb{Z} \to \mathbb{Q}$.

(e) Se existe um homomorfismo de aneis $f : \mathbb{C} \to \mathbb{Z}[i]$ então seja $\alpha := \sqrt{2} \in \mathbb{C}$, temos

$$f(\alpha)^2 = f(\alpha^2) = f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2,$$

logo $f(\alpha) = \pm\sqrt{2}$. Mas este elemento não pertence a $\mathbb{Z}[i]$, pois $\pm\sqrt{2}$ como número complexo tem parte real igual a $\pm\sqrt{2}$, que não é um inteiro. Logo f não existe.

T7 – Trabalho semanal 7 de Álgebra 2 – Semestre 2021-1

Semana: 06 de setembro - 10 de setembro, 2021.
Prazo de entrega: 23 de setembro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 3a + 2b + c + 7.$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Lembre-se que se A é um anel comutativo unitário então $U(A)$ denota o grupo multiplicativo dos elementos de A que admitem inverso multiplicativo. Dê um exemplo de um anel comutativo unitário A tal que $U(A[X])$ contém pelo menos um polinômio de grau n, onde n é o número definido acima.

2. Seja p o $(b+4)$-esimo número primo. Seja $F := \mathbb{Z}/p\mathbb{Z}$. Considere o produto direto $A = F \times F$ (como anel). Mostre que os únicos ideais de A são
$$\{(0,0)\}, \qquad \{0\} \times F, \qquad F \times \{0\}, \qquad A.$$
[Dica: Seja I ideal de A. Se existe um elemento $(a, b) \in I$ com $a \neq 0 \neq b$ então ...]

   BONUS (não vale ponto): consegue generalizar? Quais são os ideais do produto direto $A \times B$ em geral, se A e B são aneis comutativos unitários quaisquer?

3. Seja I o ideal principal de $\mathbb{Q}[X]$ gerado por $X^2 - n^2$, onde n é o número definido acima. Mostre que o anel $\mathbb{Q}[X]/I$ é isomorfo (como anel!) ao produto direto $\mathbb{Q} \times \mathbb{Q}$.

4. Considere o homomorfismo de aneis
$$f : \mathbb{Q}[X] \to \mathbb{C}, \qquad f(P(X)) := P(1 + a - i),$$
onde a é o número definido acima e i é a unidade imaginária, $i^2 = -1$. Encontre um polinômio $H(X) \in \mathbb{Q}[X]$ tal que $\ker(f) = (H(X))$, ou seja $\ker(f)$ é o ideal principal gerado por $H(X)$.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T7 – Trabalho semanal 7 de Álgebra 2 – Gabarito

Neste gabarito, a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Lembre-se que se A é um anel comutativo unitário então $U(A)$ denota o grupo multiplicativo dos elementos de A que admitem inverso multiplicativo. Dê um exemplo de um anel comutativo unitário A tal que $U(A[X])$ contém pelo menos um polinômio de grau n, onde n é o número definido acima.

   Seja $A = F[X]$ onde $F = \mathbb{Z}/4\mathbb{Z}$ e seja $P(X) = 2X^n + 1 \in A$. Então $P(X)(1 - 2X^n) = 1 - 4X^{2n} = 1$ logo $P(X)^{-1} = 1 - 2X^n$ e $P(X)$ é inversível.

2. Seja p o $(b + 4)$-esimo número primo. Seja $F := \mathbb{Z}/p\mathbb{Z}$. Considere o produto direto $A = F \times F$ (como anel). Mostre que os únicos ideais de A são
$$\{(0, 0)\}, \quad \{0\} \times F, \quad F \times \{0\}, \quad A.$$
   [Dica: Seja I ideal de A. Se existe um elemento $(a, b) \in I$ com $a \neq 0 \neq b$ então ...]

   Seja I um ideal de A diferente de $\{(0, 0)\}$. Se existe um elemento $(a, b) \in I$ com $a \neq 0 \neq b$ então $(a, b)(a^{-1}, b^{-1}) = (1, 1) \in I$ pois I é ideal. Como $(1, 1) \in I$, o ideal I contém todo elemento (x, y) de A pois $(x, y) = (1, 1) \cdot (x, y)$, logo $I = A$. Agora suponha que I não contém nenhum elemento (a, b) com $a \neq 0 \neq b$. Em particular, I não pode conter simultaneamente dois elementos do tipo $(a, 0)$ e $(0, b)$ com $a \neq 0 \neq b$ pois se os contivesse então, sendo ideal, conteria também $(a, 0) + (0, b) = (a, b)$. Logo temos duas possibilidades.

   (a) Todo elemento de I é do tipo $(a, 0)$ com $a \in F$, ou seja $I \subseteq F \times \{0\}$. Neste caso, como $I \neq \{(0, 0)\}$, existe $a \in F$ tal que $a \neq 0$ e $(a, 0) \in I$. Se $r \in F$ então $(r, 0) = (ra^{-1}, 0)(a, 0) \in I$, e isso implica que $F \times \{0\} \subseteq I$, logo $I = F \times \{0\}$.

   (b) Todo elemento de I é do tipo $(0, b)$ com $b \in F$, ou seja $I \subseteq \{0\} \times F$. Neste caso, como $I \neq \{(0, 0)\}$, existe $b \in F$ tal que $b \neq 0$ e $(0, b) \in I$. Se $r \in F$ então $(0, r) = (0, rb^{-1})(0, b) \in I$, e isso implica que $\{0\} \times F \subseteq I$, logo $I = \{0\} \times F$.

   BONUS (não vale ponto): consegue generalizar? Quais são os ideais do produto direto $A \times B$ em geral, se A e B são aneis comutativos unitários quaisquer?

   Todo ideal de $A \times B$ é do tipo $I \times J$ onde I é ideal de A e J é ideal de B. De fato, seja L um ideal de $A \times B$ e sejam $\pi_A : A \times B \to A$, $\pi_A(a, b) := a$,

$\pi_B : A \times B \to B$, $\pi_B(a,b) := b$, as projeções canônicas, $I := \pi_A(L)$, $J := \pi_B(L)$. Como π_A e π_B são homomorfismos sobrejetivos de aneis, I é ideal de A e J é ideal de B. Além disso, é claro que $L \subseteq I \times J$. Falta mostrar que $I \times J \subseteq L$. Seja $(i,j) \in I \times J$, assim existem $a \in A$, $b \in B$ tais que $(a,j), (i,b) \in L$ (por definição de I e de J). Como L é ideal, segue que

$$L \ni (i,b) \cdot (1,0) + (a,j) \cdot (0,1) = (i,0) + (0,j) = (i,j).$$

3. Seja I o ideal principal de $\mathbb{Q}[X]$ gerado por $X^2 - n^2$, onde n é o número definido acima. Mostre que o anel $\mathbb{Q}[X]/I$ é isomorfo (como anel!) ao produto direto $\mathbb{Q} \times \mathbb{Q}$.

   Seja $f : \mathbb{Q}[X] \to \mathbb{Q} \times \mathbb{Q}$, $f(P(X)) = (P(n), P(-n))$. Se trata de um homomorfismo de aneis que é sobrejetivo pois

$$f\left(\frac{(X+n)a - (X-n)b}{2n}\right) = (a,b).$$

   O núcleo de f é dado pelos polinômios $P(X)$ tais que $P(n) = 0$ e $P(-n) = 0$. Fazendo a divisão com resto com $X^2 - n^2$ obtemos

$$P(X) = (X^2 - n^2)Q(X) + R(X),$$

   onde o grau de $R(X)$ é menor que 2, digamos $R(X) = rX + s$. Segue que $0 = P(n) = R(n) = rn + s$ e $0 = P(-n) = R(-n) = -rn + s$, logo $r = s = 0$, ou seja $P(X)$ é divisível por $X^2 - n^2$. Reciprocamente, se um polinômio é divisível por $X^2 - n^2$ então obviamente pertence ao núcleo de f. Segue que $\ker(f) = (X^2 - n^2)$ e o resultado agora segue do teorema de isomorfismo.

4. Considere o homomorfismo de aneis

$$f : \mathbb{Q}[X] \to \mathbb{C}, \qquad f(P(X)) := P(1 + a - i),$$

   onde a é o número definido acima e i é a unidade imaginária, $i^2 = -1$. Encontre um polinômio $H(X) \in \mathbb{Q}[X]$ tal que $\ker(f) = (H(X))$, ou seja $\ker(f)$ é o ideal principal gerado por $H(X)$.

   Seja $\alpha = 1 + a - i$. Observe que $\alpha - 1 - a = -i$, logo $(\alpha - 1 - a)^2 = (-i)^2 = -1$, isso pode ser escrito como

$$\alpha^2 + (1+a)^2 - 2\alpha(1+a) = -1,$$

   logo α é raiz do polinômio

$$H(X) = X^2 - 2(1+a)X + (1+a)^2 + 1 \in \mathbb{Q}[X].$$

   Já sabemos que $H(\alpha) = H(1 + a - i) = 0$, fazendo uma simples divisão deduzimos que

$$H(X) = (X - \alpha)(X - \overline{\alpha}) = (X - (1 + a - i))(X - (1 + a + i)).$$

Mostraremos que $\ker(f) = (H(X))$. A inclusão $\supseteq$ está clara. Agora suponha que $P(X) \in \ker(f)$, fazendo a divisão com resto entre $P(X)$ e $H(X)$ obtemos

$$P(X) = H(X)Q(X) + rX + s$$

onde $r, s \in \mathbb{Q}$. Como $P(\alpha) = H(\alpha) = 0$, obtemos que $r\alpha + s = 0$, o que implica $r = s = 0$, pois caso contrário $\alpha = -s/r \in \mathbb{Q}$, o que é uma contradição. Logo $P(X) = H(X)Q(X) \in (H(X))$. Isso termina a demonstração.

T8 – Trabalho semanal 8 de Álgebra 2 – Semestre 2021-1

Semana: 13 de setembro - 17 de setembro, 2021.
Prazo de entrega: 30 de setembro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 2(9-a) + 2(9-b) + 2(9-c) + 7,$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Escreva os elementos seguintes de $A = \mathbb{Z}[i]$ como produto de elementos irredutíveis.

$$n+i, \qquad n, \qquad 5+9i, \qquad 5-9i.$$

2. Faça a divisão com resto entre $n+2i$ e $a+1+i$ em $\mathbb{Z}[i]$.

3. Aplique o algoritmo de Euclides para encontrar $x, y \in \mathbb{Z}[i]$ tais que

$$(n+i)x + (n-i)y = d,$$

onde d é o MDC entre $n+i$ e $n-i$ em $\mathbb{Z}[i]$.

4. Seja I o ideal principal de $A = \mathbb{Z}[i]$ gerado por n. Considere a função

$$f : A \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$f(x+iy) := (x + n\mathbb{Z}, y + n\mathbb{Z}).$$

Aplicando o teorema de isomorfismo para grupos, calcule a cardinalidade $|A/I|$. Atenção: f não é homomorfismo de aneis em geral.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T8 – Trabalho semanal 8 de Álgebra 2 – Gabarito

Aqui n, a, b, c são inteiros não negativos que dependem do número de matrícula do/a aluno/a. n é ímpar.

1. Escreva os elementos seguintes de $A = \mathbb{Z}[i]$ como produto de elementos irredutíveis.

$$n+i, \qquad n, \qquad 5+9i, \qquad 5-9i.$$

Lembre-se que os elementos inversíveis de $\mathbb{Z}[i]$ são 1, -1, i, $-i$, e os elementos irredutíveis de $\mathbb{Z}[i]$ são os elementos cuja norma $N(a+ib) = a^2+b^2$ é um número primo e os números inteiros positivos primos congruentes a 3 módulo 4.

Vamos analisar o caso $n = 45$. Neste caso $N(45+i) = 45^2+1 = 2026 = 2 \cdot 1013$ e 1013 é um número primo congruente a 1 módulo 4, logo pode ser escrito como soma de dois quadrados. Temos $1013 = 22^2 + 23^2$, logo

$$N(45+i) = 2026 = 2 \cdot 1013 = (1+i)(1-i)(22+23i)(22-23i),$$

e $(1+i)(22+23i) = -1+45i$. Segue que $45+i = -i(-1+45i) = -i(1+i)(22+23i) = (1-i)(22+23i)$ é a fatoração de $45+i$ em elementos irredutíveis.

A fatoração de 45 em inteiros irredutíveis é $45 = 3^2 \cdot 5$, e como 3 é irredutível em $\mathbb{Z}[i]$ e $5 = (2+i)(2-i)$, a fatoração de 45 em $\mathbb{Z}[i]$ é $45 = 3^2(2+i)(2-i)$.

Temos $N(5+9i) = 5^2+9^2 = 25+81 = 106 = 2 \cdot 53$ e $53 = 2^2+7^2$, logo

$$N(5+9i) = 2 \cdot 53 = (1+i)(1-i)(2+7i)(2-7i).$$

Temos $(1+i)(2+7i) = -5+9i$, logo $5+9i = \overline{-(-5+9i)} = \overline{-(1+i)(2+7i)} = -(1-i)(2-7i) = (-1+i)(2-7i)$ é a fatoração de $5+9i$ em elementos irredutíveis. Além disso

$$5-9i = \overline{5+9i} = \overline{(-1+i)(2-7i)} = (-1-i)(2+7i)$$

é a fatoração de $5-9i$ em elementos irredutíveis.

2. Faça a divisão com resto entre $n+2i$ e $a+1+i$ em $\mathbb{Z}[i]$.

Vamos analisar o caso $n = 45$, $a = 8$. Precisamos fazer a divisão com resto entre $\alpha = 45+2i$ e $\beta = 9+i$. Temos

$$\frac{45+2i}{9+i} = \frac{(45+2i)(9-i)}{(9+i)(9-i)} = \frac{407-27i}{82} = \frac{407}{82} - \frac{27}{82}i.$$

Queremos $q = x+iy \in \mathbb{Z}[i]$ tal que $|x - \frac{407}{82}| \leq \frac{1}{2}$ e $|y - \frac{27}{82}| \leq \frac{1}{2}$. Seja então $q := 5$ e seja $r = \alpha - q\beta = 45+2i-5(9+i) = -3i$. Uma divisão com resto é

$$45+2i = 5(9+i) - 3i.$$

Observe que $N(r) = 9 < 82 = N(\beta)$.

3. Aplique o algoritmo de Euclides para encontrar $x, y \in \mathbb{Z}[i]$ tais que

$$(n+i)x + (n-i)y = d,$$

onde d é o MDC entre $n+i$ e $n-i$ em $\mathbb{Z}[i]$.

Sejam $\alpha = n+i$, $\beta = n-i$. Temos

$$\frac{n+i}{n-i} = \frac{(n+i)^2}{(n+i)(n-i)} = \frac{n^2-1+2i}{n^2+1} = \frac{n^2-1}{n^2+1} + i\frac{2}{n^2+1}.$$

Escolhendo $q_1 = 1$ (primeiro quociente) temos $r_1 = \alpha - q_1\beta = n+i-(n-i) = 2i$ (primeiro resto).

$$\frac{n-i}{2i} = \frac{-2i(n-i)}{4} = -\frac{1}{2} - i\frac{n}{2}.$$

Escolha $q_2 = -i(n+1)/2$ (segundo quociente) e $r_2 = n-i+i((n+1)/2)2i = -1-i$ (segundo resto). Observe que $q_2, r_2 \in \mathbb{Z}[i]$ pois n é ímpar.

$$\frac{2i}{-1-i} = \frac{2i(-1+i)}{(-1-i)(-1+i)} = i+1,$$

e podemos escolher $q_3 = i+1$ (terceiro quociente) e $r_3 = 0$ (terceiro resto). Segue que o MDC$(n+i, n-i)$ é (associado a) $-1-i$.

$n+i$	$n-i$	
1	0	$n+i$
0	1	$n-i$
1	-1	$2i$
$i(n+1)/2$	$1-i(n+1)/2$	$-1-i$

Em outras palavras

$$(n+i)\cdot i\cdot\frac{n+1}{2} + (n-i)\cdot\left(1 - i\cdot\frac{n+1}{2}\right) = -1-i.$$

Observe que $(n+1)/2 \in \mathbb{Z}$ pois n é ímpar.

4. Seja I o ideal principal de $A = \mathbb{Z}[i]$ gerado por n. Considere a função

$$f : A \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$f(x+iy) := (x+n\mathbb{Z}, y+n\mathbb{Z}).$$

Aplicando o teorema de isomorfismo para grupos, calcule a cardinalidade $|A/I|$. Atenção: f não é homomorfismo de aneis em geral.

f é homomorfismo sobrejetivo de grupos aditivos e $\ker(f) = (n) \trianglelefteq \mathbb{Z}[i]$. Pelo teorema de isomorfismo, $A/I \cong \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ (isomorfismo de grupos aditivos, apenas!) logo $|A/I| = n^2$.

T9 – Trabalho semanal 9 de Álgebra 2 – Semestre 2021-1

Semana: 20 de setembro - 24 de setembro, 2021.
Prazo de entrega: 07 de outubro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 2|5-a| + 2|5-b| + 2|5-c| + 6,$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Fatore o polinômio $P(X) = X^2 + (n+1)X + 1$ em fatores irredutíveis em $\mathbb{F}_q[X]$ para todo $q \in \{3, 5, 7, 11\}$ (aqui $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$).

2. Seja p o $(a+3)$-esimo número primo. Fatore o polinômio

$$P(X) = \frac{1}{2}X^3 + X - p$$

em fatores irredutíveis em $\mathbb{Q}[X]$.

3. Encontre todos os valores de $r \in \mathbb{Z}$ tais que $P(X) = X^3 + rX + a + 3$ é redutível em $\mathbb{Q}[X]$ (aqui a é o número definido acima).

4. Seja $A = \mathbb{Z}[1/n] = \{P(1/n) \ : \ P(X) \in \mathbb{Z}[X]\}$. Se trata de um subanel de $\mathbb{Q}$ (não precisa mostrar isso). Seja

$$\varphi : \mathbb{Z}[X] \to A$$

$$\varphi(P(X)) := P\left(\frac{1}{n}\right).$$

É um homomorfismo de aneis (não precisa mostrar isso).

Seja $P(X) \in \ker(\varphi)$.

   (a) Mostre que $X - \frac{1}{n}$ divide $P(X)$ em $\mathbb{Q}[X]$.

   (b) Usando o lema de Gauss, deduza que se $P(X)$ tem grau maior que 1 então é redutível em $\mathbb{Z}[X]$.

   (c) Mostre que $P(X)$ pertence ao ideal principal $I = (nX - 1)$ de $\mathbb{Z}[X]$. [Fatore $P(X)$ em irredutíveis e use o item acima.]

   (d) Deduza que $A \cong \mathbb{Z}[X]/(nX - 1)$.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T9 – Trabalho semanal 9 de Álgebra 2 – Gabarito

Aqui a, b, c, n são números inteiros não negativos que dependem do número de matrícula do/a aluno/a.

1. Fatore o polinômio $P(X) = X^2 + (n+1)X + 1$ em fatores irredutíveis em $\mathbb{F}_q[X]$ para todo $q \in \{3, 5, 7, 11\}$ (aqui $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$).

   Vamos analisar o valor $n = 50$. Neste caso a redução de $P(X)$ módulo $3, 5, 7, 11$ é $P_3(X) = X^2+1$, $P_5(X) = X^2+X+1$, $P_7(X) = X^2+2X+1$ e $P_{11}(X) = X^2+7X+1$, respectivamente. Como se trata de um polinômio de grau 2, fatorá-lo significa encontrar as suas raízes. Podemos usar a fórmula de Bhaskara, obtendo que as raízes pertencem a $\mathbb{F}_q$ se e somente se o discriminante $\Delta = b^2 - 4ac = 51^2 - 4 = 7^2 \cdot 53$ é um quadrado em $\mathbb{F}_q$. De fato, as soluções da equação $P_q(X) = 0$ são

   $$x_{1,2} = \frac{-(n+1) \pm \sqrt{\Delta}}{2}$$

   e essa formula faz sentido pois 2 é inversível módulo q, sendo q ímpar. Se $q = 3$ então $\Delta = 2$ não é um quadrado em $\mathbb{F}_3$, logo $P_3(X)$ é irredutível em $\mathbb{F}_3[X]$. Se $q = 5$ então $\Delta = 2$ não é um quadrado em $\mathbb{F}_5[X]$ logo $P_5(X)$ é irredutível em $\mathbb{F}_5[X]$. Se $q = 7$ então o discriminante é nulo e $P_7(X) = (X+1)^2$. Se $q = 11$ então $\Delta = 1$ é um quadrado e $P_{11}(X) = X^2 + 7X + 1 = (X+3)(X+4)$.

2. Seja p o $(a+3)$-esimo número primo. Fatore o polinômio

   $$P(X) = \frac{1}{2}X^3 + X - p$$

   em fatores irredutíveis em $\mathbb{Q}[X]$.

   Temos

   $$P(X) = \frac{1}{2}X^3 + X - p = \frac{1}{2}Q(X), \qquad Q(X) = X^3 + 2X - 2p.$$

   É claro que $P(X)$ é irredutível em $\mathbb{Q}[X]$ se e somente se $Q(X)$ é irredutível em $\mathbb{Q}[X]$ (eles são associados). Se $Q(X)$ é redutível em $\mathbb{Q}[X]$ então admite um fator de grau 1, que corresponde a uma raíz racional de $Q(X)$. Como $Q(X) \in \mathbb{Z}[X]$, essa raíz racional é inteira, seja ela r. Temos então $Q(r) = 0$, ou seja $r^3 + 2r - 2p = 0$, e isso implica que $r(r^2+2) = 2p$, logo r divide $2p$. Mas os divisores de $2p$ são ± 1, ± 2, $\pm p$, $\pm 2p$ e para esses valores temos que $Q(r) \neq 0$. Logo $P(X)$ é irredutível em $\mathbb{Q}[X]$.

3. Encontre todos os valores de $r \in \mathbb{Z}$ tais que $P(X) = X^3 + rX + a + 3$ é redutível em $\mathbb{Q}[X]$ (aqui a é o número definido acima).

Vamos analisar o caso $a = 6$. Neste caso $P(X) = X^3 + rX + 9 \in \mathbb{Z}[X]$ é um polinômio primitivo, logo é redutível em $\mathbb{Q}[X]$ se e somente se é redutível em $\mathbb{Z}[X]$, pelo lema de Gauss. Escrevendo

$$\begin{aligned} X^3 + rX + 9 = P(X) &= (dX + e)(fX^2 + gX + h) \\ &= dfX^3 + (dg + ef)X^2 + (dh + eg)X + eh \end{aligned}$$

obtemos que $df = 1$ logo $d = f = \pm 1$ e, a menos de trocar os sinais dos fatores, podemos supor que $d = f = 1$. Segue que $P(-e) = 0$, ou seja $-e^3 - re + 9 = 0$ e isso implica que $9 = e^3 + re = e(e^2 + r)$, logo $e \in \mathbb{Z}$ divide 9. Os divisores de 9 são ± 1, ± 3, ± 9. Segue que os valores de r são dados pelas igualdades $P(t) = 0$, $t \in \{\pm 1, \pm 3, \pm 9\}$, ou seja $r + 10 = 0$, $-r + 8 = 0$, $36 + 3r = 0$, $-18 - 3r = 0$, $738 + 9r = 0$, $-720 - 9r = 0$. Logo $P(X)$ é redutível em $\mathbb{Q}[X]$ se e somente se $r \in \{-10, 8, -12, -6, -82, -80\}$.

4. Seja $A = \mathbb{Z}[1/n] = \{P(1/n) \ : \ P(X) \in \mathbb{Z}[X]\}$. Se trata de um subanel de $\mathbb{Q}$ (não precisa mostrar isso). Seja

$$\varphi : \mathbb{Z}[X] \to A$$

$$\varphi(P(X)) := P\left(\frac{1}{n}\right).$$

É um homomorfismo de aneis (não precisa mostrar isso).

Seja $P(X) \in \ker(\varphi)$.

(a) Mostre que $X - \frac{1}{n}$ divide $P(X)$ em $\mathbb{Q}[X]$.

Isso é imediáto fazendo a divisão com resto entre $P(X)$ e $X - 1/n$ e substituindo $X = 1/n$, lembrando que $P(1/n) = 0$.

(b) Usando o lema de Gauss, deduza que se $P(X)$ tem grau maior que 1 então é redutível em $\mathbb{Z}[X]$.

Pelo lema de Gauss, um polinômio de $\mathbb{Z}[X]$ é irredutível em $\mathbb{Z}[X]$ se e somente se é primitivo em $\mathbb{Z}[X]$ e irredutível em $\mathbb{Q}[X]$. Pelo item anterior $P(X)$ é redutível em $\mathbb{Q}[X]$, logo pelo lema de Gauss $P(X)$ é redutível em $\mathbb{Q}[X]$.

(c) Mostre que $P(X)$ pertence ao ideal principal $I = (nX - 1)$ de $\mathbb{Z}[X]$. [Fatore $P(X)$ em irredutíveis e use o item acima.]

Se $P(X)$ tem grau 1 então $P(X) = rX + s$ com $r, s \in \mathbb{Z}$ e o fato que $P(1/n) = 0$ significa que $r/n + s = 0$, ou seja $r = -ns$. Substituindo obtemos que $P(X) = -nsX + s = -s(nX - 1)$ logo $P(X)$ pertence a I. Agora suponha que $P(X)$ tem grau maior que 1. Pelo item anterior, $P(X)$ é redutível, e podemos escrever a sua fatoração em irredutíveis como $c \cdot q_1 \cdots q_t$ onde $c = c(P)$ é o conteúdo de $P(X)$ (o MDC dos coeficientes de $P(X)$) e $q_1, \ldots, q_t$ são polinômios irredutíveis de $\mathbb{Z}[X]$ de grau maior que zero. Como $P(1/n) = 0$, existe

$i \in \{1, \ldots, t\}$ tal que $q_i(1/n) = 0$, logo q_i, sendo irredutível, tem grau 1 pelo item anterior. Já vimos que os polinômios de grau 1 em $\ker(\varphi)$ pertencem a $(nX - 1)$, logo q_i pertence a $(nX - 1)$, e sendo irredutível segue que é associado a $nX - 1$. Segue que $nX - 1$ divide $P(X)$ em $\mathbb{Z}[X]$.

(d) Deduza que $A \cong \mathbb{Z}[X]/(nX - 1)$.

Pelos itens anteriores $\ker(\varphi) = (nX - 1)$, logo o resultado segue do teorema de isomorfismo.

T10 – Trabalho semanal 10 de Álgebra 2 – Semestre 2021-1

Semana: 27 de setembro - 01 de outubro, 2021.
Prazo de entrega: 14 de outubro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 4a + 3b + 2c + 3,$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Seja p o $(b+4)$-esimo número primo. Construa um corpo com p^2 elementos.

2. Mostre que $K = \mathbb{F}_5[X]/(X^2 + 2)$ é um corpo e diga se os elementos seguintes são geradores do grupo cíclico K^*:

$$nX + n + 1 + I, \qquad (n + 1)X + n + 2 + I,$$

   onde n é o número definido acima identificado com a sua redução mod 5.

3. Seja p o $(b + 4)$-esimo número primo. Encontre um gerador do grupo multiplicativo cíclico $K^* = K - \{0\}$ onde

$$K = \mathbb{F}_3[X]/(X^3 + 2X + p).$$

   Aqui p é identificado com a sua redução módulo 3.

4. Considere

$$P(X) := X^4 + X + 1$$

   como polinômio em $\mathbb{Q}[X]$, $\mathbb{F}_5[X]$. Em cada caso, calcule a sua fatoração em fatores irredutíveis.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T10 – Trabalho semanal 10 de Álgebra 2 – Gabarito

Aqui a, b, c, n são inteiros não negativos que dependem do número de matrícula do/a aluno/a.

1. Seja p o $(b{+}4)$-esimo número primo. Construa um corpo com p^2 elementos.

   Seja $\alpha \in \mathbb{F}_p$ tal que $\alpha \neq t^2$ para todo $t \in \mathbb{F}_p$. Então o polinômio $X^2 - \alpha \in \mathbb{F}_p[X]$ é irredutível, logo $K := \mathbb{F}_p[X]/(X^2 - \alpha)$ é um corpo. Além disso, os elementos de K têm a forma $rX + s + I$ onde $r, s \in \mathbb{F}_p$ e I é o ideal principal de $\mathbb{F}_p[X]$ gerado por $X^2 - \alpha$. Como visto nas aulas teóricas, duas classes $r_1X + s_1 + I$, $r_2X + s_2 + I$ são distintas se e somente se os pares (r_1, s_1), (r_2, s_2) são distintos, pois I é gerado por um polinômio de grau 2. Segue que $|K| = p^2$ (temos p escolhas para r e, para cada uma delas, p escolhas para s). Isso mostra que precisamos encontrar um $\alpha \in \mathbb{F}_p$ que não é um quadrado em $\mathbb{F}_p$. Isso pode ser feito calculando explicitamente os quadrados. Por exemplo se $p = 29$ então os quadrados em $\mathbb{F}_{29}$ são

   $$0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 16, 5^2 = 25,\ 6^2 = 7,\ 7^2 = 20,\ 8^2 = 6,$$

   $$9^2 = 23,\ 10^2 = 13,\ 11^2 = 5,\ 12^2 = 28,\ 13^2 = 24,\ 14^2 = 22,\ 15^2 = 22,$$

   $$16^2 = 24,\ 17^2 = 28,\ 18^2 = 5,\ 19^2 = 13,\ 20^2 = 23,\ 21^2 = 6,\ 22^2 = 20,$$

   $$23^2 = 7,\ 24^2 = 25,\ 25^2 = 16,\ 26^2 = 9,\ 27^2 = 4,\ 28^2 = 1.$$

   Segue que podemos escolher por exemplo $\alpha = 2$.

2. Mostre que $K = \mathbb{F}_5[X]/(X^2 + 2)$ é um corpo e diga se os elementos seguintes são geradores do grupo cíclico K^*:

   $$nX + n + 1 + I, \qquad (n + 1)X + n + 2 + I,$$

   onde n é o número definido acima identificado com a sua redução mod 5.

   K é um corpo porque o polinômio $X^2 + 2$ é irredutível em $\mathbb{F}_5[X]$. Além disso $|K| = 5^2 = 25$. Segue que $G := K^*$ é um grupo cíclico de ordem $|G| = |K| - 1 = 24 = 3 \cdot 8$.

   Seja $\alpha := X + I \in G$. Nas contas que segue usa-se que $\alpha^2 = 3$. Observe que $\beta \in G$ gera G se e somente se $o(\beta) = 24$, e isso é equivalente a $\beta^8 \neq 1 \neq \beta^{12}$. Seja $\beta_m := (m - 1)\alpha + m$ para $m \in \{1, 2, 3, 4, 5\}$. Obviamente $\beta_1 = 1$ tem ordem 1, logo não gera G.

   $$\begin{array}{lll} \beta_2 = \alpha + 2, & {\beta_2}^8 = 4\alpha + 2, & {\beta_2}^{12} = 1. \\ \beta_3 = 2\alpha + 3, & {\beta_3}^8 = 4\alpha + 2, & {\beta_3}^{12} = 4. \\ \beta_4 = 3\alpha + 4, & {\beta_4}^8 = \alpha + 2, & {\beta_4}^{12} = 1. \\ \beta_5 = 4\alpha, & {\beta_5}^8 = 1, & {\beta_5}^{12} = 4. \end{array}$$

   Segue que β_1,β_2,β_4,β_5 não geram G e β_3 gera G.

3. Seja p o $(b+4)$-esimo número primo. Encontre um gerador do grupo multiplicativo cíclico $K^* = K - \{0\}$ onde

$$K = \mathbb{F}_3[X]/(X^3 + 2X + p).$$

Aqui p é identificado com a sua redução módulo 3.

Observe que $P(X) := X^3 + 2X + p$ é irredutível em $\mathbb{F}_3[X]$ pois $P(0) = P(1) = P(2) = p \not\equiv 0 \mod 3$ pois p é um número primo maior do que 3. Seja $\alpha := X + I$, onde $I = (P(X)) \trianglelefteq \mathbb{F}_3[X]$. Suponha primeiro que $p \equiv 1 \mod 3$. Vamos mostrar que α é gerador de K^*. É claro que $\alpha^2 \neq 1$, pois X^3+2X+1 não divide X^2-1 em $\mathbb{F}_3[X]$. Como $|K^*| = 27-1 = 26 = 2\cdot 13$, para mostrar que $\langle\alpha\rangle = K^*$ basta mostrar que $o(\alpha) \neq 13$, e para isso basta mostrar que $\alpha^{13} \neq 1$. Lembrando que $\alpha^3 = -2\alpha - 1 = \alpha - 1$, temos

$$(\alpha-1)^4 = \alpha^4 - 4\alpha^3 + 6\alpha^2 - 4\alpha + 1 = \alpha(\alpha-1) - (\alpha-1) - \alpha + 1 = \alpha^2 - 1,$$

$$\alpha^{13} = (\alpha^3)^4\alpha = (\alpha-1)^4\alpha = (\alpha^2-1)\alpha = \alpha - 1 - \alpha = -1 \neq 1.$$

Agora suponha que $p \equiv 2 \mod 3$. Neste caso, $-\alpha$ é raiz de $P(-X) = -X^3 - 2X + 2 = -(X^3 + 2X + 1)$, ou seja $-\alpha$ é raiz de $X^3 + 2X + 1$. A discussão acima mostra que toda raiz de $X^3 + 2X + 1$ é um gerador de K^*, logo $K^* = \langle -\alpha\rangle$ neste caso.

4. Considere

$$P(X) := X^4 + X + 1$$

como polinômio em $\mathbb{Q}[X]$, $\mathbb{F}_5[X]$. Em cada caso, calcule a sua fatoração em fatores irredutíveis.

- Considere o caso de $\mathbb{Q}[X]$. Como $P(X)$ é um polinômio primitivo de $\mathbb{Z}[X]$, pelo lema de Gauss $P(X)$ é irredutível em $\mathbb{Q}[X]$ se e somente se é irredutível em $\mathbb{Z}[X]$. Sabemos que a existência de um fator de grau 1 em $\mathbb{Z}[X]$ corresponde à existência de uma raiz inteira b, e $P(b) = 0$ implica que $b(b^3 + 1) = -1$ logo $b = \pm 1$ (sendo b inteiro), mas $P(1) = 3 \neq 0$ e $P(-1) = 1 \neq 0$. Isso mostra que $P(X)$ não tem fatores de grau 1. Se $P(X)$ admite fatores de grau 2 então pode ser escrito na forma

$$\begin{aligned} P(X) = X^4 + X + 1 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a+c)X^3 + (d + ac + b)X^2 + (ad + bc)X + bd, \end{aligned}$$

onde $a, b, c, d \in \mathbb{Z}$. Obtemos $a + c = 0$, $d + ac + b = 0$, $ad + bc = 1$ e $bd = 1$. Como $bd = 1$ e b, d são inteiros, $b = d = \pm 1$. Como $c = -a$ e $b = d$, temos que $1 = ad + bc = ad - ad = 0$, uma contradição. Segue que $P(X)$ é irredutível em $\mathbb{Q}[X]$.

- Considere o caso de $\mathbb{F}_5[X]$. Neste caso $P(3) = 0$ logo $X - 3$ divide $P(X)$, e fazendo a divisão com resto obtemos

$$P(X) = (X - 3)(X^3 + 3X^2 + 4X + 3).$$

Essa é a fatoração de $P(X)$ em fatores irredutíveis em $\mathbb{F}_5[X]$: o fator $Q(X) = X^3 + 3X^2 + 4X + 3$ é irredutível porque tem grau 3 e não tem raízes em $\mathbb{F}_5$, sendo $Q(0) = 3$, $Q(1) = 1$, $Q(2) = 1$, $Q(3) = 4$, $Q(4) = 1$.

T11 – Trabalho semanal 11 de Álgebra 2 – Semestre 2021-1

Semana: 04 de outubro - 08 de outubro, 2021.
Prazo de entrega: 21 de outubro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 4(9-a) + 2(9-b) + 2(9-c) + 4,$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

Lembre-se que se E/F é uma extensão de corpos e $\alpha \in E$ então

$$F[\alpha] = \mathrm{Im}(v_\alpha) = \{P(\alpha) \ : \ P(X) \in F[X]\},$$
$$F(\alpha) = \mathrm{Frac}(F[\alpha]) = \left\{ \tfrac{P(\alpha)}{Q(\alpha)} \ : \ P(X), Q(X) \in F[X], \ Q(\alpha) \neq 0 \right\}.$$

Vimos que se α é algébrico sobre F então $F(\alpha) = F[\alpha]$. É um corpo.

1. Mostre que os polinômios seguintes são irredutíveis em $\mathbb{Q}[X]$.

   $$P_1(X) := X^n - 20, \qquad P_2(X) := X^n + nX + 6, \qquad P_3(X) := X^8 + 1.$$

   No caso de $P_3(X)$, use o argumento seguinte: $P(X)$ é irredutível se e somente se $P(X+1)$ é irredutível.

   BONUS (não vale ponto). Mostre que $X^m + 1$ é irredutível em $\mathbb{Q}[X]$ se e somente se m é uma potência de 2.

2. Seja p o $(a+4)$-esimo número primo e seja $\alpha := \sqrt{p + \sqrt{p}} \in \mathbb{R}$. Para cada uma das afirmações seguintes, diga se é verdadeira ou falsa, justificando a resposta.

   $$i \in \mathbb{Q}(\alpha), \qquad \sqrt{p} \in \mathbb{Q}(\alpha), \qquad \sqrt{2} \in \mathbb{Q}(\alpha^2).$$

3. Seja $\beta := i(1 + \sqrt{2}) \in \mathbb{C}$. Encontre o polinômio minimal de β sobre $\mathbb{Q}$ e calcule o grau $|\mathbb{Q}(\beta) : \mathbb{Q}|$.

4. Sejam

   $$\gamma := \sqrt[3]{2} \in \mathbb{R}, \qquad \delta := \gamma^2 + \gamma + b - 10 \in \mathbb{Q}[\gamma],$$

   onde b é o número definido acima. Sabemos que $\mathbb{Q}[\gamma]$ é um corpo e que o polinômio minimal de γ sobre $\mathbb{Q}$ é $X^3 - 2$. Observe que $\delta \neq 0$, pois se fosse $\delta = 0$ então γ seria raiz de um polinômio de $\mathbb{Q}[X]$ de grau 2.

   Calcule o inverso de δ em $\mathbb{Q}[\gamma]$, ou seja expresse δ^{-1} como polinômio com coeficientes em $\mathbb{Q}$ avaliado em γ. [Aplique o algoritmo de Euclides a $X^3 - 2$ e $X^2 + X + b - 10$, em seguida substitua $X = \gamma$.]

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T11 – Trabalho semanal 11 de Álgebra 2 – Gabarito

Neste gabarito, n, a, b, c são números não negativos que dependem do número de matrícula do/a aluno/a. n é par.

1. Mostre que os polinômios seguintes são irredutíveis em $\mathbb{Q}[X]$.

   $$P_1(X) := X^n - 20, \qquad P_2(X) := X^n + nX + 6, \qquad P_3(X) := X^8 + 1.$$

   No caso de $P_3(X)$, use o argumento seguinte: $P(X)$ é irredutível se e somente se $P(X+1)$ é irredutível.

   $P_1(X) := X^n - 20$ é irredutível pelo critério de Eisenstein aplicado ao primo $p = 5$. $P_2(X) := X^n + nX + 6$ é irredutível pelo critério de Eisenstein aplicado ao primo $p = 2$, sendo n um número par. Para mostrar que $P_3(X) := X^8 + 1$, Observe que $P_3(X) = A(X)B(X)$ (com $A(X), B(X) \in \mathbb{Q}[X]$) se e somente se $P_3(X+1) = A(X+1)B(X+1)$ e a substituição $X \mapsto X + 1$ preserva os graus dos fatores. Isso implica que $P_3(X)$ é irredutível em $\mathbb{Q}[X]$ se e somente se $P_3(X+1)$ é irredutível em $\mathbb{Q}[X]$. O polinômio $P_3(X+1) = (X+1)^8 + 1$ é igual a

   $$X^8 + 8X^7 + 28X^6 + 56X^5 + 70X^4 + 56X^3 + 28X^2 + 8X + 2.$$

   É irredutível pelo critério de Eisenstein aplicado a $p = 2$.

   BONUS (não vale ponto). Mostre que $X^m + 1$ é irredutível em $\mathbb{Q}[X]$ se e somente se m é uma potência de 2.

   Escrevamos $m = rs$ com r ímpar e s uma potência de 2. Se $r > 1$ então seja $T := X^s$. O polinômio $Q(T) := T^r + 1$ é redutível pois $Q(-1) = 0$, logo é divisível por $T + 1$ e podemos escrever $T^r + 1 = (T+1)L(T)$ com $L(T) \in \mathbb{Q}[X]$ de grau positivo. Segue que $X^m + 1 = Q(X^s) = (X^s + 1)L(X^s)$ e $X^m + 1$ é redutível. Agora suponha $r = 1$, ou seja $m = s$ é uma potência de 2, digamos $m = 2^k$. Aplicando a ideia acima, mostraremos que $H(X) := (X+1)^{2^k} + 1$ é irredutível pelo critério de Eisenstein aplicado a $p = 2$. Observe que o termo de grau máximo é 1, não divisível por 2, e o termo de grau zero $H(0) = 2$ não é divisível por $p^2 = 4$. Falta mostrar que os outros coeficientes são pares. Para isso, basta mostrar que $(X+1)^{2^k} + 1 \equiv X^{2k} \mod 2$, ou seja que $(X+1)^{2^k} \equiv X^{2^k} + 1 \mod 2$. Isso pode ser mostrado por indução sobre k, sendo óbvio para $k = 1$ e, se vale para k, então

   $$(X+1)^{2^{k+1}} = ((X+1)^{2^k})^2 \equiv (X^{2^k} + 1)^2 \equiv X^{2^{k+1}} + 1 \qquad \mod 2.$$

2. Seja p o $(a+4)$-esimo número primo e seja $\alpha := \sqrt{p + \sqrt{p}} \in \mathbb{R}$. Para cada uma das afirmações seguintes, diga se é verdadeira ou falsa, justificando a resposta.

   $$i \in \mathbb{Q}(\alpha), \qquad \sqrt{p} \in \mathbb{Q}(\alpha), \qquad \sqrt{2} \in \mathbb{Q}(\alpha^2).$$

Seja $K := \mathbb{Q}(\alpha)$. Observe que $\alpha \in \mathbb{R}$ implica que $K \subseteq \mathbb{R}$, logo i não pertence a K, pois $i \in \mathbb{C} - \mathbb{R}$. O elemento $\sqrt{p}$ é igual a $\alpha^2 - p$, logo pertence a K, pois K é um corpo que contém α e p.

Temos $\alpha^2 = p + \sqrt{p}$, logo $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{p})$ e os elementos deste corpo são do tipo $r + s\beta$ onde $\beta = \sqrt{p}$ e $r, s \in \mathbb{Q}$. Se $\sqrt{2} \in \mathbb{Q}(\alpha^2)$ então existem $r, s \in \mathbb{Q}$ tais que $r + s\beta = \sqrt{2}$. Elevando ao quadrado, $r^2 + ps^2 + 2rs\beta = 2$. Como 1 e β são linearmente independentes sobre $\mathbb{Q}$, segue que $rs = 0$, ou seja $r = 0$ ou $s = 0$. Se $r = 0$ então $ps^2 = 2$, contradizendo o fato que p é um primo maior que 2, e se $s = 0$ então $r^2 = 2$, contradizendo $r \in \mathbb{Q}$. Segue que $\sqrt{2} \notin \mathbb{Q}(\alpha^2)$.

3. Seja $\beta := i(1 + \sqrt{2}) \in \mathbb{C}$. Encontre o polinômio minimal de β sobre $\mathbb{Q}$ e calcule o grau $|\mathbb{Q}(\beta) : \mathbb{Q}|$.

   Observe que $\beta^2 = -3 - 2\sqrt{2}$, logo $(\beta^2 + 3)^2 - 8 = 0$. Segue que β é raiz do polinômio
   $$P(X) := X^4 + 6X^2 + 1.$$
   Observe que $P(X)$ é não admite fatores de grau 1 em $\mathbb{Q}[X]$ pois é mônico, com coeficientes inteiros e os divisores inteiros de $P(0) = 1$ não são raízes de $P(X)$, sendo $P(1) = P(-1) = 8$. Para mostrar que $P(X)$ é irredutível, usando o lema de Gauss, precisamos mostrar que $P(X)$ não admite nenhuma fatoração do tipo
   $$\begin{aligned} P(X) &= (X^2 + rX + s)(X^2 + tX + u) \\ &= X^4 + (r + t)X^3 + (u + rt + s)X^2 + (ru + st)X + su \end{aligned}$$
   com $r, s, t, u \in \mathbb{Z}$. Se $P(X)$ admitisse uma tal fatoração então teriamos
   $$\begin{cases} r + t = 0 \\ u + rt + s = 6 \\ ru + st = 0 \\ su = 1 \end{cases}$$
   Como r, s são inteiros, $rs = 1$ implica que $r = s = \pm 1$. Se $r = s = 1$ então $t = -1$, logo $6 = u + rt + s = u - 1 + 1 = u$ e isso contradiz $ru + st = 0$. Se $r = s = -1$ então $t = 1$, logo $6 = u + rt + s = u - 1 - 1 = u - 2$, logo $u = 8$ e isso contradiz $ru + st = 0$.

   Segue que $P(X)$ é um polinômio de $\mathbb{Q}[X]$ mônico, irredutível e admite β como raiz. Logo $P(X)$ é o polinômio minimal de β sobre $\mathbb{Q}$ e isso implica que $|\mathbb{Q}(\beta) : \mathbb{Q}|$ é igual ao grau de $P(X)$, ou seja 4.

4. Sejam
   $$\gamma := \sqrt[3]{2} \in \mathbb{R}, \qquad \delta := \gamma^2 + \gamma + b - 10 \in \mathbb{Q}[\gamma],$$
   onde b é o número definido acima. Sabemos que $\mathbb{Q}[\gamma]$ é um corpo e que o polinômio minimal de γ sobre $\mathbb{Q}$ é $X^3 - 2$. Observe que $\delta \neq 0$, pois se fosse $\delta = 0$ então γ seria raiz de um polinômio de $\mathbb{Q}[X]$ de grau 2.

Calcule o inverso de δ em $\mathbb{Q}[\gamma]$, ou seja expresse δ^{-1} como polinômio com coeficientes em $\mathbb{Q}$ avaliado em γ. [Aplique o algoritmo de Euclides a X^3-2 e $X^2+X+b-10$, em seguida substitua $X=\gamma$.]

Seja $m := b-10$. Aplicando o algoritmo de Euclides como sugerido, obtemos

$$(X^3-2)A(X)+(X^2+X+m)B(X) = m^3-6m+6.$$

$$A(X) := (m-1)X+2m-3,$$
$$B(X) := (m-1)^2+(X-1)((1-m)X-2m+3).$$

Substituindo $X=\gamma$ obtemos que

$$\begin{aligned}\delta^{-1} &= \frac{B(\gamma)}{m^3-6m+6} = \frac{(m-1)^2+(\gamma-1)((1-m)\gamma-2m+3)}{m^3-6m+6} \\ &= \frac{1-m}{m^3-6m+6}\gamma^2+\frac{2-m}{m^3-6m+6}\gamma+\frac{m^2-2}{m^3-6m+6}.\end{aligned}$$

T12 – Trabalho semanal 12 de Álgebra 2 – Semestre 2021-1

Semana: 11 de outubro - 15 de outubro, 2021.
Prazo de entrega: 28 de outubro, 2021.

Sejam a, b, c os últimos três digitos do seu número de matrícula, nesta ordem! [1] Defina

$$n := 4|5-a| + 2|5-b| + 3|5-c| + 3,$$

Atenção: errar no cálculo do número n implicará nota nula.
Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.

1. Calcule o grau de um corpo de decomposição sobre $\mathbb{Q}$ dos polinômios

$$P_1(X) := X^4 - 8X^2 + 15, \qquad P_2(X) := X^4 + X^2 - 1.$$

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

3. Sejam $\alpha \in \mathbb{C}$ uma raiz de $P(X) = X^3 - 3X + 1$ e seja M o corpo de decomposição de $P(X)$ contido em $\mathbb{C}$. Calcule $|M : \mathbb{Q}|$. [Dica: dada uma raiz $\alpha \in \mathbb{C}$ de $P(X)$, calcule $P(\alpha^2 - 2)$.]

4. Sejam

$$\alpha := \sqrt[3]{2} \in \mathbb{R}, \qquad \rho := e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{C} - \mathbb{R}.$$

   As raízes de $P(X) := X^3 - 2 \in \mathbb{Q}[X]$ são α, $\rho\alpha$, $\rho^2\alpha$, em particular $P(X)$ admite uma raiz real e duas complexas conjugadas. Como $K := \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, isso implica que K não é corpo de decomposição de $P(X)$ sobre $\mathbb{Q}$.

   Mostre que K não é corpo de decomposição sobre $\mathbb{Q}$ de nenhum polinômio de $\mathbb{Q}[X]$. Para fazer isso, siga a estratégia seguinte (se quiser).

   (a) Mostre que existe $f : K \cong \mathbb{Q}(\alpha\rho)$ (isomorfismo de corpos!). [Dica: os dois são isomorfos a...]

   (b) Mostre que $f(x) = x$ para todo $x \in \mathbb{Q}$.

   (c) Mostre que se $x \in K$ então $f(x) \in \mathbb{R}$ se e somente se $x \in \mathbb{Q}$.

   (d) Mostre que se $\beta \in K$ é raiz de um polinômio $L(X) \in \mathbb{Q}[X]$, então $L(f(\beta)) = 0$. [Use o item (b)]

   (e) Mostre que se $K = \mathbb{Q}(\alpha)$ é corpo de decomposição de $L(X) \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$ então todas as raízes de $L(X)$ são reais. Deduza uma contradição.

[1] Por *exemplo*, se o seu número de matrícula é 210123456 então $a = 4$, $b = 5$, $c = 6$ (mas esse é *apenas um exemplo*!!).

T12 – Trabalho semanal 12 de Álgebra 2 – Gabarito

Neste gabarito a, b, c, n são números não negativos que dependem do número de matrícula do/a aluno/a.

1. Calcule o grau de um corpo de decomposição sobre $\mathbb{Q}$ dos polinômios

$$P_1(X) := X^4 - 8X^2 + 15, \qquad P_2(X) := X^4 + X^2 - 1.$$

Observe que $P_1(X) = (X^2 - 3)(X^2 - 5)$, logo um corpo de decomposição de $P_1(X)$ é $E := \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Temos

$$|E : \mathbb{Q}| = |E : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2 \cdot |E : \mathbb{Q}(\sqrt{2})|.$$

Falta calcular $d := |E : \mathbb{Q}(\sqrt{2})| = |\mathbb{Q}(\sqrt{2})(\sqrt{5}) : \mathbb{Q}(\sqrt{2})|$. Observe que $d \leq 2$ pois $\sqrt{5}$ é raiz de $X^2 - 5 \in \mathbb{Q}(\sqrt{2})[X]$. Para mostrar que $d = 2$ basta então mostrar que $d \neq 1$, ou seja que $E \neq \mathbb{Q}(\sqrt{2})$. Isso é equivalente a dizer que $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$. Se fosse $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$ então existiriam $r, s \in \mathbb{Q}$ tais que

$$\sqrt{5} = r + s\sqrt{2},$$

e elevando ao quadrado teriamos $5 = r^2 + 2s^2 + 2rs\sqrt{2}$. Isso implica $rs = 0$, ou seja $r = 0$ ou $s = 0$. Se $r = 0$ então $5 = 2s^2$, e se $s = 0$ então $5 = r^2$. Temos então uma contradição em ambos os casos.

Considere agora $P_2(X) = X^4 + X^2 - 1$. Ele não tem fatores de grau 1 em $\mathbb{Q}[X]$ pois (usando o argumento usual) $P_2(\pm 1) = 1 \neq 0$. Para mostrar que $P_2(X)$ não tem fatores de grau 2, pelo lema de Gauss basta mostrar que não existem $r, s, t, u \in \mathbb{Z}$ tais que

$$\begin{aligned} X^4 + X^2 - 1 &= (X^2 + rX + s)(X^2 + tX + u) \\ &= X^4 + (r + t)X^3 + (u + rt + s)X^2 + (ru + st)X + su. \end{aligned}$$

Temos o sistema de equações

$$\begin{cases} r + t = 0 \\ u + rt + s = 1 \\ ru + st = 0 \\ su = -1 \end{cases}$$

Segue que $s = \pm 1$. Se $s = 1$ então $u = -1$ e $-r + t = 0$, $r + t = 0$, segue que $r = t = 0$ e isso contradiz $u + rt + s = 1$. Se $s = -1$ então $u = 1$ e $r - t = 0$, $r + t = 0$, segue que $r = t = 0$ e isso contradiz $u + rt + s = 1$.

Segue que $P_2(X)$ é irredutível em $\mathbb{Q}[X]$. As raízes de $P_2(X)$ podem ser calculadas resolvendo $T^2 + T - 1 = 0$, onde $T = X^2$. São $\pm\alpha$ e $\pm\beta$ onde

$$\alpha := \sqrt{\frac{\sqrt{5} - 1}{2}}, \qquad \beta := i\sqrt{\frac{\sqrt{5} + 1}{2}}.$$

O corpo de decomposição de $P(X)$ sobre $\mathbb{Q}$ é $M := \mathbb{Q}(\alpha, \beta)$ e temos

$$|M : \mathbb{Q}| = |M : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}|.$$

Observe que $\alpha \in \mathbb{R}$ e $\beta \in \mathbb{C} - \mathbb{R}$, logo $\beta \notin \mathbb{Q}(\alpha)$, em outras palavras $M \neq \mathbb{Q}(\alpha)$, ou seja $|M : \mathbb{Q}(\alpha)| > 1$. Além disso $\sqrt{5} = 2\alpha^2 + 1 = -2\beta^2 - 1$, ou seja $\beta^2 = -\alpha^2 - 1$, e isso implica que β é raiz do polinômio $X^2 + \alpha^2 + 1 \in \mathbb{Q}(\alpha)[X]$, logo $|M : \mathbb{Q}(\alpha)| = |\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)| \leq 2$. Sendo $|M : \mathbb{Q}(\alpha)| > 1$, segue que $|M : \mathbb{Q}(\alpha)| = 2$. Além disso, como $P(X)$ é irredutível em $\mathbb{Q}[X]$ e de grau 4, temos $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$. Segue que

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

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

   Sejam $L := \mathbb{Q}(i, \sqrt{2})$, $K := \mathbb{Q}(ni + i\sqrt{2})$. Para mostrar que $L = K$ basta mostrar que cada gerador de um deles pertence ao outro, ou seja $i \in K$, $\sqrt{2} \in K$ e $ni + i\sqrt{2} \in L$. Seja $\alpha := ni + i\sqrt{2} = i(n + \sqrt{2})$. Obviamente $\alpha \in L$, sendo $i, \sqrt{2} \in L$ e L um corpo. Temos $\alpha^2 = -(n^2 + 2 + 2\sqrt{2}n)$, segue que $\sqrt{2} = (-\alpha^2 - n^2 - 2)/(2n) \in \mathbb{Q}(\alpha)$. Segue que $n + \sqrt{2} \in \mathbb{Q}(\alpha)$ logo $i = \alpha/(n + \sqrt{2}) \in \mathbb{Q}(\alpha)$.

3. Sejam $\alpha \in \mathbb{C}$ uma raiz de $P(X) = X^3 - 3X + 1$ e seja M o corpo de decomposição de $P(X)$ contido em $\mathbb{C}$. Calcule $|M : \mathbb{Q}|$. [Dica: dada uma raiz $\alpha \in \mathbb{C}$ de $P(X)$, calcule $P(\alpha^2 - 2)$.]

   Observe que $P(X)$ é irredutível em $\mathbb{Q}[X]$ pois tem grau 3, tem coeficientes inteiros e não tem raízes inteiras. Temos $\alpha^3 = 3\alpha - 1$, logo

$$\begin{aligned} P(\alpha^2 - 2) &= (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 \\ &= \alpha^6 - 6\alpha^4 + 12\alpha^2 - 8 - 3\alpha^2 + 6 + 1 \\ &= (3\alpha - 1)^2 - 6\alpha(3\alpha - 1) + 9\alpha^2 - 1 = 0. \end{aligned}$$

   Segue que α e $\beta = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$ são raízes de $P(X)$ e pertencem ambas a $\mathbb{Q}(\alpha)$. Fazendo a divisão com $X - \alpha$ e com $X - \beta$ em seguida, no anel $\mathbb{Q}(\alpha)[X]$, obtemos que existe $\gamma \in \mathbb{Q}(\alpha)$ tal que

$$P(X) = (X - \alpha)(X - \beta)(X - \gamma).$$

   Podemos facilmente calcular γ pois o argumento acima mostra que se u é raiz então $u^2 - 2$ é raiz, logo

$$\begin{aligned} \gamma = \beta^2 - 2 = (\alpha^2 - 2)^2 - 2 &= \alpha^4 - 4\alpha^2 + 2 \\ &= \alpha(3\alpha - 1) - 4\alpha^2 + 2 = -\alpha^2 - \alpha + 2. \end{aligned}$$

   Segue que $M = \mathbb{Q}(\alpha)$ e $|M : \mathbb{Q}| = 3$. Além disso $M = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$. Observe também que a composição dos isomorfismos de corpos

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(P(X)) \cong \mathbb{Q}(\beta)$$

é um isomorfismo de corpos $f : M \to M$ que fixa os elementos de $\mathbb{Q}$ e manda α para β. Vimos que as três raízes de $P(X)$ são α, $f(\alpha)$ e $f(f(\alpha))$, logo tem uma "ciclicidade" das raízes. Isso é explicado pelo fato que $\langle f \rangle$ é exatamente igual ao grupo de todos os isomorfismos de corpos $M \to M$, com a composição, que então é um grupo cíclico de ordem 3. Neste caso, ele coincide com o grupo de Galois da extensão $M/\mathbb{Q}$.

4. Sejam

$$\alpha := \sqrt[3]{2} \in \mathbb{R}, \qquad \rho := e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{C} - \mathbb{R}.$$

As raízes de $P(X) := X^3 - 2 \in \mathbb{Q}[X]$ são α, $\rho\alpha$, $\rho^2\alpha$, em particular $P(X)$ admite uma raiz real e duas complexas conjugadas. Como $K := \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, isso implica que K não é corpo de decomposição de $P(X)$ sobre $\mathbb{Q}$.

Mostre que K não é corpo de decomposição sobre $\mathbb{Q}$ de nenhum polinômio de $\mathbb{Q}[X]$. Para fazer isso, siga a estratégia seguinte (se quiser).

(a) Mostre que existe $f : K \cong \mathbb{Q}(\alpha\rho)$ (isomorfismo de corpos!). [Dica: os dois são isomorfos a...]

Os dois são isomorfos a $\mathbb{Q}[X]/(P(X))$, pois α e $\alpha\rho$ são raízes de $P(X)$.

(b) Mostre que $f(x) = x$ para todo $x \in \mathbb{Q}$.

Como f é homomorfismo de aneis, $f(1) = 1$ e f é aditiva, logo $f(m) = m$ para todo $m \in \mathbb{N}$, sendo todo número natural uma soma de uns. Além disso $f(-m) = -f(m) = -m$ para todo $m \in \mathbb{N}$, logo f fixa todos os inteiros. Além disso se m, k são dois inteiros com $k \neq 0$ então $f(m/k) = f(m)/f(k) = m/k$, logo f fixa todos os racionais.

(c) Mostre que se $x \in K$ então $f(x) \in \mathbb{R}$ se e somente se $x \in \mathbb{Q}$.

Se $x \in \mathbb{Q}$ então $f(x) = x \in \mathbb{Q} \subseteq \mathbb{R}$, logo $f(x) \in \mathbb{R}$. Vice-versa, suponha $x \notin \mathbb{Q}$, mostraremos que $f(x) \notin \mathbb{R}$. Observe que se fosse $f(x) \in \mathbb{Q}$ então teriamos $\mathbb{Q}(\alpha\rho) = f(\mathbb{Q}(x)) \subseteq \mathbb{R}$, uma contradição, logo $f(x) \notin \mathbb{Q}$. Temos então as inclusões $\mathbb{Q} \subseteq \mathbb{Q}(f(x)) \subseteq \mathbb{Q}(\alpha\rho)$ e a primeira dessas inclusões é própria. Pela formula do grau

$$3 = |\mathbb{Q}(\alpha\rho) : \mathbb{Q}| = |\mathbb{Q}(\alpha\rho) : \mathbb{Q}(f(x))| \cdot |\mathbb{Q}(f(x)) : \mathbb{Q}|.$$

Como 3 é um número primo e $|\mathbb{Q}(f(x)) : \mathbb{Q}| > 1$, segue que $\mathbb{Q}(f(x)) = \mathbb{Q}(\alpha\rho) \not\subseteq \mathbb{R}$, logo $f(x) \notin \mathbb{R}$.

(d) Mostre que se $\beta \in K$ é raiz de um polinômio $L(X) \in \mathbb{Q}[X]$, então $L(f(\beta)) = 0$. [Use o item (b)]

Escreva $L(X) = \sum_{i=0}^{m} a_i X^i$ com $a_i \in \mathbb{Q}$ para todo $i = 0, 1, \ldots, m$.

Temos $f(a_i) = a_i$ para todo $i = 0, \ldots, m$, pelo item (b). Segue que

$$\begin{aligned} L(f(\beta)) &= \sum_{i=0}^{m} a_i f(\beta)^i = \sum_{i=0}^{m} f(a_i) f(\beta)^i = \sum_{i=0}^{m} f(a_i) f(\beta^i) \\ &= \sum_{i=0}^{m} f(a_i \beta^i) = f\left(\sum_{i=0}^{m} a_i \beta^i \right) = f(L(\beta)) = f(0) = 0. \end{aligned}$$

(e) Mostre que se $K = \mathbb{Q}(\alpha)$ é corpo de decomposição de $L(X) \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$ então todas as raízes de $L(X)$ são reais. Deduza uma contradição.

Se $K = \mathbb{Q}(\alpha)$ é corpo de decomposição de $L(X) \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$ então K contém todas as raízes complexas de $L(X)$, pois K é gerado por elas. Como $K \subseteq \mathbb{R}$, segue que todas as raízes de $L(X)$ são reais. Seja $\beta \in K$ uma qualquer raiz de $L(X)$. Pelo item (c), $f(\beta)$ é uma raiz complexa de $L(X)$, logo pertence a K, que está contido em $\mathbb{R}$, logo $f(\beta) \in \mathbb{R}$. Pelo item (c), $\beta \in \mathbb{Q}$. Isso mostra que todas as raízes complexas de $L(X)$ são racionais. Como K é gerado pelas raízes de $L(X)$, segue que $K \subseteq \mathbb{Q}$, contradição.