T1 – Trabalho semanal 1 de Álgebra 3 – Semestre 2021-2

Semana: 31 de janeiro - 4 de fevereiro, 2022.
Prazo de entrega: 17 de fevereiro, 2022.

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 elemento $g := (1, 2, \ldots, n-2) \in S_n$, é um cíclo de comprimento $n-2$. Calcule a ordem do centralizador $C_{S_n}(g)$. [Use o princípio da contagem.]

   BONUS (não vale ponto): calcule a ordem $|C_{S_n}(g)|$ no caso em que g é o cíclo $(1, 2, \ldots, k)$, com k qualquer, $k \in \{1, 2, \ldots, n\}$.

2. Diga se existe uma ação transitiva de G sobre X nos casos seguintes.

   - $G = S_3$, $X = \{2, 4+n, 6-n, 8\}$.
   - $G = S_3$, $X = \{2+n, 3, 4+n, 9, 10+n, 11\}$.
   - $G = S_4$, $X = \{1, 2, 3, 4, 4+n, 5+2n\}$.
   - $G = S_5$, $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

3. Considere o grupo seguinte. Se trata de um subgrupo do produto direto $S_3 \times S_3$.

   $$G := \{(x, y) \in S_3 \times S_3 \ : \ x \equiv y \mod A_3\}.$$

   Encontre todas as classes de conjugação de G e o tamanho de cada classe.

4. Seja G um grupo de ordem coprima com 30, ou seja o MDC entre $|G|$ e 30 é igual a 1. Seja $H \leq G$ tal que $|G : H| = 7$. Mostre que $H \trianglelefteq G$.

[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 – Trabalho semanal 1 de Álgebra 3 - Resolução

1. Considere o elemento $g := (1, 2, \ldots, n-2) \in S_n$, é um cíclo de comprimento $n-2$. Calcule a ordem do centralizador $C_{S_n}(g)$. [Use o princípio da contagem.]

   BONUS (não vale ponto): calcule a ordem $|C_{S_n}(g)|$ no caso em que g é o cíclo $(1, 2, \ldots, k)$, com k qualquer, $k \in \{1, 2, \ldots, n\}$.

   Farei o caso k qualquer. O número de k-cíclos em S_n é $\binom{n}{k} \cdot (k-1)!$, pois para construir um k-cíclo precisamos escolher os k elementos mexidos pelo k-cíclo e em seguida precisamos contar os k-cíclos que é possível construir usando k elementos, digamos $\{1, \ldots, k\}$. Obviamente eles são todos do tipo

   $$(1 * * \ldots *)$$

   O número de k-cíclos em S_n é também igual ao número de conjugados de um k-cíclo fixado $g \in S_n$ pois no grupo S_n dois elementos são conjugados se e somente se eles têm a mesma estrutura cíclica. Segue que

   $$\frac{n!}{|C_G(g)|} = |S_n : C_G(g)| = |\{k\text{-cíclos}\}| = \binom{n}{k} \cdot (k-1)! = \frac{n!}{k(n-k)!},$$

   logo $|C_G(g)| = k \cdot (n-k)!$. Se $k = n-2$ então $|C_G(g)| = 2(n-2)$. A estrutura de $C_G(g)$ é $C_k \times S_{n-k}$. A ideia é que os elementos de S_n que comutam com o k-cíclo g são os produtos xy onde $x \in \langle g \rangle$ e y é um elemento de S_n que fixa todos os pontos não fixados por g.

2. Diga se existe uma ação transitiva de G sobre X nos casos seguintes.

   Como visto nas aulas, uma ação transitiva de um grupo G sobre um conjunto X de tamanho n é equivalente à ação de multiplicação à esquerda de G sobre $\{yH \ : \ y \in G\}$, onde H é o estabilizador de um $\alpha \in X$. Isso implica que G admite uma ação transitiva de *grau* n (ou seja, sobre um conjunto de tamanho n) se e somente se G tem um subgrupo de índice n. Observe que em particular se isso acontece então n divide $|G|$.

   - $G = S_3$, $X = \{2, 4+n, 6-n, 8\}$. Note que $|X| = 4$. Não existe porque $|X| = 4$ não divide $|G| = 6$.
   - $G = S_3$, $X = \{2+n, 3, 4+n, 9, 10+n, 11\}$. Se $n = 9$ (isso acontece no caso $a = b = c = 0$) temos que $2 + n = 11$ logo $|X| = 5$ e G não admite ações transitivas sobre X pois $|X| = 5$ não divide $|G| = 6$. Se $n \geq 10$ então $|X| = 6$, e G admite uma ação transitiva de grau 6 porque $\{1\}$ tem índice 6 em G.
   - $G = S_4$, $X = \{1, 2, 3, 4, 4+n, 5+2n\}$. Note que $|X| = 6$. S_4 age transitivamente sobre um conjunto de tamanho 6, de fato o grupo de Klein K tem índice 6 em G.

- $G = S_5$, $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Note que $|X| = 10$. Considere
$$H := \{g \in A_5 \ : \ g(5) = 5\} < S_5.$$
É claro que $H \cong A_4$, logo $|H| = 12$. Isso implica que $|S_5 : H| = |S_5|/|H| = 5!/12 = 10$.

3. Considere o grupo seguinte. Se trata de um subgrupo do produto direto $S_3 \times S_3$.
$$G := \{(x, y) \in S_3 \times S_3 \ : \ x \equiv y \mod A_3\}.$$
Encontre todas as classes de conjugação de G e o tamanho de cada classe.

Observe que $f : G \to S_3$, $f((x, y)) := x$ é um homomorfismo sobrejetivo cujo núcleo é $\{1\} \times A_3$, logo $G/\ker(f) \cong S_3$ e isso implica que $|G| = |\ker(f)| \cdot |S_3| = 3 \cdot 6 = 18$.

O elemento $(1, 1)$ tem apenas um conjugado pois $(r, s)(1, 1)(r, s)^{-1} = (1, 1)$ para todo $(r, s) \in G$. Segue que a classe de $(1, 1)$ é
$$\{(1, 1)\}.$$

Seja $x = (123)$, então um elemento $(r, s) \in G$ comuta com $(x, 1)$ se e somente se r comuta com x, ou seja $r \in A_3$. Como $r \equiv s \mod A_3$, segue que $s \in A_3$, logo $|C_G((x, 1))| = 3^2$ e $(x, 1)$ tem apenas $|G : C_G((x, 1))| = 18/9 = 2$ conjugados, que são $(x, 1)$ e $(x^2, 1)$ (de fato definido $t := (12) \in S_3$ temos $(t, t)(x, 1)(t, t)^{-1} = (x^2, 1)$ e $(t, t) \in G$). Encontramos a classe
$$\{((123), 1), ((132), 1)\}.$$

Analogamente, a classe de $(1, (123))$ é
$$\{(1, (123)), (1, (132))\}.$$

Seja $x = (123)$. Um elemento $(r, s) \in G$ comuta com (x, x) se e somente se r, s comutam com x, ou seja $(r, s) \in A_3 \times A_3$. Segue que $|C_G((x, x))| = 3^2$ e (x, x) tem apenas $|G : C_G((x, 1))| = 18/9 = 2$ conjugados, que são (x, x) e (x^2, x^2) (de fato definido $t := (12) \in S_3$ temos $(t, t)(x, 1)(t, t)^{-1} = (x^2, x^2)$ e $(t, t) \in G$). Encontramos a classe
$$\{((123), (123)), ((132), (132))\}.$$

Seja $x = (123)$. Um elemento $(r, s) \in G$ comuta com (x, x^2) se e somente se r comuta com x e s comuta com x^2, ou seja $(r, s) \in A_3 \times A_3$. Segue que $|C_G((x, x^2))| = 3^2$ e (x, x^2) tem apenas $|G : C_G((x, x^2))| = 18/9 = 2$ conjugados, que são (x, x^2) e (x^2, x) (de fato definido $t := (12) \in S_3$ temos $(t, t)(x, x^2)(t, t)^{-1} = (x^2, x)$ e $(t, t) \in G$). Encontramos a classe
$$\{((123), (132)), ((132), (123))\}.$$

Até agora temos encontrado $1 + 2 + 2 + 2 = 9$ elementos.

Seja $x = (12)$. Um elemento $(r, s) \in G$ comuta com (x, x) se e somente se r, s comutam com x, ou seja $r, s \in \langle x \rangle$. Mas sendo $r \equiv s \mod A_3$, deduzimos que $r = s = x$ ou $r = s = 1$. Segue que $|C_G((x, x))| = 2$ e (x, x) tem $|G : C_G((x, x))| = 18/2 = 9$ conjugados. Como $|G| = 18$, segue que os conjugados de (x, x) são todos os elementos que não foram encontrados nos casos anteriores, logo a classe de $((12), (12))$ é

$$\{((12), (12)), ((12), (13)), ((12), (23)),$$

$$((13), (12)), ((13), (13)), ((13), (23)),$$

$$((23), (12)), ((23), (13)), ((23), (23))\}.$$

Segue que G tem 6 classes de conjugação, elas têm tamanho $1, 2, 2, 2, 2, 9$.

4. Seja G um grupo de ordem coprima com 30, ou seja o MDC entre $|G|$ e 30 é igual a 1. Seja $H \leq G$ tal que $|G : H| = 7$. Mostre que $H \trianglelefteq G$.

   Sabemos que G/H_G é isomorfo a um subgrupo de S_7, que tem ordem 7!. Segue que $|G/H_G| = |G : H_G|$ divide 7! e $|G|$, logo divide o MDC entre $|G|$ e 7!, que é igual a 7 por hipótese. Logo $|G : H_G| \in \{1, 7\}$ e sendo $H_G \leq H \neq G$ deduzimos que $|G : H_G| = 7 = |G : H|$. Segue que

   $$7 = |G : H_G| = |G : H| \cdot |H : H_G| = 7 \cdot |H : H_G|,$$

   logo $|H : H_G| = 1$, ou seja $H = H_G \trianglelefteq G$.

T2 – Trabalho semanal 2 de Álgebra 3 – Semestre 2021-2

Semana: 7 de fevereiro - 11 de fevereiro, 2022.
Prazo de entrega: 24 de fevereiro, 2022.

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

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

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

Lembre-se que um grupo G é dito simples se os únicos subgrupos normais de G são $\{1\}$ e G.

1. Sejam p, q dois primos distintos e seja G um grupo tal que $|G| = pq$. Suponha que $p \not\equiv 1 \mod q$ e que $q \not\equiv 1 \mod p$. Mostre que G é cíclico.

2. Sejam G um grupo finito e $p \geq 5$ um número primo. Mostre que G não é simples em cada um dos seguintes casos.

$$|G| = 20p = 2^2 \cdot 5 \cdot p, \qquad 16 \cdot 5^n = 2^4 \cdot 5^n.$$

3. Seja G um grupo finito. Mostre que G não é simples em cada um dos seguintes casos.

$$|G| = 540 = 2^2 \cdot 3^3 \cdot 5, \qquad |G| = 560 = 2^4 \cdot 5 \cdot 7.$$

4. Seja N um subgrupo normal de G e seja P um subgrupo de Sylow de N. Seja $H = N_G(P) = \{x \in G \ : \ xPx^{-1} = P\} \leq G$. Mostre que $NH = G$. [Dica: dado $g \in G$, temos que gPg^{-1} está contido em N.]

[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 – Trabalho semanal 2 de Álgebra 3 - Resolução

1. Sejam p, q dois primos distintos e seja G um grupo tal que $|G| = pq$. Suponha que $p \not\equiv 1 \mod q$ e que $q \not\equiv 1 \mod p$. Mostre que G é cíclico.

   Sejam P um p-Sylow, Q um q-Sylow. Como n_p divide q temos $n_p \in \{1, q\}$, e sendo n_p congruente a 1 módulo p, e q não congruente a 1 módulo p, segue que $n_p = 1$, ou seja $P \trianglelefteq G$. Analogamente $n_q = 1$, logo $Q \trianglelefteq G$. Segue que $PQ \leq G$. Observe que $|PQ| = |P||Q|/|P \cap Q| = pq$ sendo $P \cap Q = \{1\}$, pois $|P \cap Q|$ divide $|P| = p$ e $|Q| = q$, que são números primos distintos. Como $|P|$ e $|Q|$ são números primos, P e Q são cíclicos. Sejam x um gerador de P, y um gerador de Q. Os elementos x, y comutam porque $xyx^{-1}y^{-1} \in P \cap Q = \{1\}$ (sendo $xyx^{-1} \in xQx^{-1} = Q$, $yx^{-1}y^{-1} \in yPy^{-1} = P$), e têm ordens coprimas, logo xy tem ordem pq. Segue que $G = \langle xy \rangle$.

2. Sejam G um grupo finito e $p \geq 5$ um número primo. Mostre que G não é simples em cada um dos seguintes casos.

$$|G| = 20p = 2^2 \cdot 5 \cdot p, \qquad 16 \cdot 5^n = 2^4 \cdot 5^n.$$

   Para todo divisor primo p de $|G|$, indicaremos por n_p o número de p-subgrupos de Sylow de G. Usaremos o teorema de Sylow. Lembre-se que se $n_p = 1$ então existe um p-Sylow normal.

   Se $|G| = 20p$ e $p = 5$ então $|G| = 2^2 \cdot 5^2$ e n_5 divide 4 e é congruente a 1 módulo 5. Segue que $n_5 = 1$, logo G não é simples.

   Se $|G| = 20p$ e $p \geq 7$ então n_p divide 20 e é congruente a 1 módulo p. Se $n_p = 1$ então o p-Sylow é normal e G não é simples, suponha agora que $n_p \neq 1$. Os divisores de 20 diferentes de 1 são $2, 4, 5, 10, 20$, logo o fato que $n_p \equiv 1 \mod p$ implica que $p \in \{2, 3, 19\}$. Sendo $p \geq 5$, deduzimos que $p = 19$.

   Temos então $|G| = 20 \cdot 19 = 2^2 \cdot 5 \cdot 19$ e $n_{19} = 20$. Temos que n_5 divide $2^2 \cdot 19 = 76$ e é congruente a 1 módulo 5, logo $n_5 \in \{1, 76\}$. Se $n_5 = 1$ então o 5-Sylow é normal, suponha agora que $n_5 \neq 1$, assim $n_5 = 76$. O grupo G contém então $20 \cdot 18 = 360$ elementos de ordem 19 e $76 \cdot 4 = 304$ elementos de ordem 5, logo G contém pelo menos $360 + 304 = 664$ elementos. Isso contradiz o fato que $|G| = 20 \cdot 19 = 380$.

   Se $|G| = 16 \cdot 5^n$ então n_5 divide 16 e é congruente a 1 módulo 5. Se $n_5 = 1$ então o 5-Sylow é normal e G não é simples, logo podemos supor que $n_5 \neq 1$, assim $n_5 = 16$. Se G é simples então é isomorfo a um subgrupo de S_{16}, logo $|G|$ divide 16!, e isso é uma contradição porque $n \geq 7$.

3. Seja G um grupo finito. Mostre que G não é simples em cada um dos seguintes casos.

$$|G| = 540 = 2^2 \cdot 3^3 \cdot 5, \qquad |G| = 560 = 2^4 \cdot 5 \cdot 7.$$

Suponha G simples por contradição. Para todo divisor primo p de $|G|$, indicaremos por n_p o número de p-subgrupos de Sylow de G. Lembre-se que $n_p = |G : N_G(P)|$ sendo P um qualquer p-Sylow de G. Usaremos o teorema de Sylow. Lembre-se que se $n_p = 1$ então existe um p-Sylow normal, contradizendo o fato que G é simples.

Se

$$|G| = 540 = 2^2 \cdot 3^3 \cdot 5$$

então podemos supor que $n_5 \in \{6, 36\}$ e que $n_3 \in \{4, 10\}$. Se $n_5 = 6$ ou $n_3 = 4$ então G é isomorfo a um subgrupo de S_6, logo $|G|$ divide $6! = 2^4 \cdot 3^2 \cdot 5$, uma contradição. Segue que $n_5 = 36$ e $n_3 = 10$. Seja P um 5-Sylow, temos que $|G : N_G(P)| = n_5 = 36$ logo $|N_G(P)| = 540/36 = 15$. Pelo exercício 1, segue que $N_G(P)$ é cíclico, gerado por um elemento $g \in G$ de ordem 15. A ação A de conjugação de G no conjunto dos dez 3-subgrupos de Sylow dá o homomorfismo de Cayley $\gamma : G \to S_{10}$, que é injetivo sendo G simples. Como g tem ordem 15, $\gamma(g)$ também tem ordem 15 (sendo γ injetivo) logo a estrutura cíclica de $\gamma(g)$ é $(1, 1, 3, 5)$, logo $\gamma(g)$ tem dois pontos fixos. Em termos da ação A, isso significa que g normaliza dois 3-Sylow de G, seja Q um deles. Segue que $g \in N_G(Q)$, logo $o(g) = 15$ divide $|N_G(Q)|$ pelo teorema de Lagrange. Mas isso é uma contradição porque $10 = n_3 = |G : N_G(Q)|$ implica que $|N_G(Q)| = |G|/10 = 54$ e 54 não é divisível por 15.

Se

$$|G| = 560 = 2^4 \cdot 5 \cdot 7$$

então podemos supor que $n_5 \in \{16, 56\}$ e $n_7 = 8$. Seja P um 7-Sylow e seja $H := N_G(P)$. Temos que $|G : H| = n_7 = 8$, logo $|H| = |G|/8 = 2 \cdot 5 \cdot 7$ é da forma $2d$ com d ímpar. Como visto nas aulas, segue que H contém um subgrupo C de índice 2, ou seja ordem 35, e é cíclico pelo exercício 1, gerado por um elemento g. Como H tem índice 8, se G é simples então G é isomorfo a um subgrupo de S_8, e isso é uma contradição porque S_8 não contém elementos de ordem 35 (para ver isso basta pensar às possíveis estruturas cíclicas dos elementos de S_8).

4. Seja N um subgrupo normal de G e seja P um subgrupo de Sylow de N. Seja $H = N_G(P) = \{x \in G \ : \ xPx^{-1} = P\} \leq G$. Mostre que $NH = G$. [Dica: dado $g \in G$, temos que gPg^{-1} está contido em N.]

   É claro que $NH \subseteq G$, mostraremos a inclusão $G \subseteq NH$. Seja $g \in G$, mostraremos que $g \in NH$. Temos que gPg^{-1} e P têm a mesma ordem, e gPg^{-1} está contido em N (sendo N normal em G e $P \leq N$), logo gPg^{-1} é um p-Sylow de N (onde p é o divisor primo de $|P|$). Pelo teorema de Sylow, existe então $n \in N$ tal que $gPg^{-1} = nPn^{-1}$, em outras palavras $n^{-1}gPg^{-1}n = P$. Segue que

   $$P = n^{-1}gPg^{-1}n = (n^{-1}g)P(n^{-1}g)^{-1},$$

   logo $n^{-1}g \in N_G(P) = H$, logo $g \in nH \subseteq NH$.

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

Semana: 14 de fevereiro - 18 de fevereiro, 2022.
Prazo de entrega: 10 de março, 2022.

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

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

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 um grupo G é dito simples se os únicos subgrupos normais de G são $\{1\}$ e G.

1. Seja $n_p(G)$ o número de p-subgrupos de Sylow do grupo G. Calcule $n_5(A_5)$, $n_5(S_7)$ e $n_7(S_{10})$. [Dica. Cada grupo de ordem prima p é cíclico e contém $p-1$ elementos de ordem p.]

2. Sejam G um grupo finito cuja ordem é divisível pelo primo p, P um p-subgrupo de Sylow de G e H um subgrupo de G tal que $N_G(P) \leq H \leq G$. Mostre que $|G : H| \equiv 1 \mod p$. [Dica. Mostre que $N_G(P) = N_H(P)$.]

3. Seja G um grupo finito. Mostre que G não é simples em cada um dos seguintes casos.

$$|G| = 396 = 2^2 \cdot 3^2 \cdot 11, \qquad |G| = 3^n \cdot 35.$$

4. Seja G um grupo de ordem $|G| = 2000 = 2^4 \cdot 5^3$. Mostre que G não é simples da seguinte forma. Suponha G simples por contradição. Em particular G não é abeliano porque a sua ordem não é um número primo.

   (a) Sejam P, Q dois 5-Sylow distintos de G e seja $H := P \cap Q$. Usando o fato que $|PQ| \leq |G|$, mostre que $|H| = 25$. [Atenção: PQ não é um subgrupo de G em geral, mesmo assim vale $|PQ| = |P||Q|/|P \cap Q|$.]

   (b) Mostre que H é normal em P e em Q. [Dica: Aplique o teorema de Cayley generalizado aos quocientes P/H_P, Q/H_Q.]

   (c) Deduza uma contradição considerando $N_G(H)$.

[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 – Trabalho semanal 3 de Álgebra 3 - Resolução

Lembre-se que um grupo G é dito simples se os únicos subgrupos normais de G são $\{1\}$ e G.

1. Seja $n_p(G)$ o número de p-subgrupos de Sylow do grupo G. Calcule $n_5(A_5)$, $n_5(S_7)$ e $n_7(S_{10})$. [Dica. Cada grupo de ordem prima p é cíclico e contém $p-1$ elementos de ordem p.]

   Como $|A_5| = 5!/2 = 60$, $|S_7| = 7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ e $|S_{10}| = 10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$, nos três casos os subgrupos de Sylow interessados têm ordem p prima, respectivamente 5, 5 e 7. O grupo A_5 contém $4! = 24$ elementos de ordem 5, o grupo S_7 contém $\binom{7}{5} \cdot 4! = 504$ elementos de ordem 5 e o grupo S_{10} contém $\binom{10}{7} \cdot 6! = 86400$ elementos de ordem 7. Segue que

   $$\begin{cases} n_5(A_5) = 24/4 = 6, \\ n_5(S_7) = 504/4 = 126, \\ n_7(S_{10}) = 86400/6 = 14400. \end{cases}$$

2. Sejam G um grupo finito cuja ordem é divisível pelo primo p, P um p-subgrupo de Sylow de G e H um subgrupo de G tal que $N_G(P) \leq H \leq G$. Mostre que $|G : H| \equiv 1 \mod p$. [Dica. Mostre que $N_G(P) = N_H(P)$.]

   Temos $N_H(P) = H \cap N_G(P) = N_G(P)$ pois H contém $N_G(P)$. Logo $n_p(G) = |G : N_G(P)|$ e $n_p(H) = |H : N_H(P)| = |H : N_G(P)|$. Segue que

   $$\begin{aligned} n_p(G) &= |G : N_G(P)| = |G : H| \cdot |H : N_G(P)| \\ &= |G : H| \cdot |H : N_H(P)| = |G : H| \cdot n_p(H). \end{aligned}$$

   Como $n_p(G) \equiv 1 \mod p$ e $n_p(H) \equiv 1 \mod p$, reduzindo a igualdade acima módulo p obtemos $|G : H| \equiv 1 \mod p$.

3. Seja G um grupo finito. Mostre que G não é simples em cada um dos seguintes casos.

   $$|G| = 396 = 2^2 \cdot 3^2 \cdot 11, \qquad |G| = 3^n \cdot 35.$$

   Suponha que G é simples e que $|G| = 396 = 2^2 \cdot 3^2 \cdot 11$. Observe que $n_{11} \in \{1, 12\}$ pelo teorema de Sylow, e se $n_{11} = 1$ então o 11-Sylow é normal, logo podemos supor que $n_{11} = 12$. Seja P um 11-Sylow de G, então $12 = n_{11} = |G : H|$ onde $H = N_G(P)$, logo $|H| = 33 = 3 \cdot 11$. Sendo $11 \not\equiv 1 \mod 3$ e $3 \not\equiv 1 \mod 11$, temos que todo grupo de ordem 33 é cíclico, logo H é cíclico, gerado por um elemento $g \in G$ de ordem 33. Por outro lado $H_G = \{1\}$ (pois G é simples) logo pelo teorema de Cayley generalizado $G \cong G/H_G$ é isomorfo a um subgrupo de S_{12}, sendo $|G : H| = 12$. Mas isso é absurdo pois S_{12} não contém elementos de ordem 33, pois na estrutura cíclica de um tal elemento deveriam aparecer pelo menos um 3-cíclo e um 11-cíclo.

Suponha que G é simples e que $|G| = 3^n \cdot 35 = 3^n \cdot 5 \cdot 7$. Temos que $n_3 \in \{1, 7\}$ pelo teorema de Sylow, logo podemos supor que $n_3 = 7$. Segue que o normalizador $H = N_G(P)$ de um 3-Sylow P tem índice 7, logo $G \cong G/H_G$ é isomorfo a um subgrupo de S_7 pelo teorema de Cayley generalizado. Segue que $|G| = 3^n \cdot 5 \cdot 7$ divide $|S_7| = 7!$ e isso é um absurdo pois $n \geq 9$.

4. Seja G um grupo de ordem $|G| = 2000 = 2^4 \cdot 5^3$. Mostre que G não é simples da seguinte forma. Suponha G simples por contradição. Em particular G não é abeliano porque a sua ordem não é um número primo.

   (a) Sejam P, Q dois 5-Sylow distintos de G e seja $H := P \cap Q$. Usando o fato que $|PQ| \leq |G|$, mostre que $|H| = 25$. [Atenção: PQ não é um subgrupo de G em geral, mesmo assim vale $|PQ| = |P||Q|/|P \cap Q|$.]

   Temos $|P| = |Q| = 5^3$. Como $P \cap Q$ é um subgrupo de P, temos $|H| = 5^k$ com $k \in \{0, 1, 2, 3\}$. Observe que

   $$2^4 \cdot 5^3 = |G| \geq |PQ| = \frac{|P| \cdot |Q|}{|H|} = \frac{5^6}{|H|} = 5^{6-k},$$

   logo $5^k \geq 5^3/2^4$ e isso implica que $k \geq 2$. Por outro lado $k \in \{0, 1, 2, 3\}$ e não pode ser $k = 3$ pois neste caso $|H| = |P| = |Q|$ implicaria $P = Q$, uma contradição, logo $k = 2$ e $|H| = 25$, ou seja $|P : H| = |Q : H| = 5$.

   (b) Mostre que H é normal em P e em Q. [Dica: Aplique o teorema de Cayley generalizado aos quocientes P/H_P, Q/H_Q.]

   Observe que $|P : H| = |Q : H| = 5$ pelo item anterior. Pelo teorema de Cayley generalizado, P/H_P é isomorfo a um subgrupo de S_5, logo $|P : H_P|$ divide $|S_5| = 120$. Por outro lado $|P : H_P|$ divide $|P| = 5^3$, logo $|P : H_P|$ é uma potência de 5 que divide 120, e é diferente de 1 pois $P \neq H_P$ sendo $H_P \leq H < P$ (sendo $|P : H| = 5$), logo $|P : H_P| = 5$. Por outro lado $5 = |P : H_P| = |P : H| \cdot |H : H_P| = 5|H : H_P|$, logo $|H : H_P| = 1$, ou seja $H = H_P$. Segue que $H = H_P \trianglelefteq P$. O argomento para Q é exatamente o mesmo.

   (c) Deduza uma contradição considerando $N_G(H)$.

   Como H é normal em P e em Q, o normalizador $K = N_G(H)$ contém P e Q. Segue que $|K|$ é divisível por $|P| = 5^3$ e $|K| \neq |P|$ (se fosse $|K| = |P|$ então como $P \leq K$ teriamos $P = K$ e isso contradiz o fato que $Q \leq K$). Como $|G| = 2^4 \cdot 5^3$, segue que $|K| = 2^t \cdot 5^3$ com $t \geq 1$, logo $|G : K| \in \{1, 2, 4, 8\}$. Se $|G : K| = 1$ então $G = K = N_G(H)$, em outras palavras $P \cap Q = H \trianglelefteq G$, contradizendo o fato que G é simples, pois $|H| = 25$. Se $|G : K| = 2$ então $K \trianglelefteq G$, absurdo. Se $|G : K| = 4$ então G é isomorfo a um subgrupo de S_4, logo $|G|$ divide $|S_4| = 24$, absurdo. Se $|G : K| = 8$ então G é isomorfo a um subgrupo de S_8, logo $|G|$ divide $|S_8| = 8!$, absurdo.

T4 – Trabalho semanal 4 de Álgebra 3 – Semestre 2021-2

Semana: 07 de março - 11 de março, 2022.
Prazo de entrega: 24 de março, 2022.

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

$$n := 4(9-a) + 4(9-b) + 4(9-c) + 6.$$

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

Pode usar o fato que se K é uma qualquer extensão de $\mathbb{Q}$ e $f : K \to K$ é um homomorfismo de aneis então $f(a) = a$ para todo $a \in \mathbb{Q}$.

1. Seja G um grupo finito de ordem $|G| = 4m$ com m ímpar e suponha que G admita um 2-subgrupo de Sylow cíclico. Mostre que existe $H \leq G$ tal que $|G : H| = 4$.

   [Dica. Mergulhe G em $\mathrm{Sym}(G)$ e considere $G \cap \mathrm{Alt}(G)$.]

2. Calcule o grau $|M : \mathbb{Q}|$ onde M é corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ em cada um dos casos seguintes.

   $$f(X) = X^3 - n, \qquad f(X) = X^4 + 13X^2 - (a+2)(a-11).$$

   Em cada caso, diga se a ação de $\mathcal{G}(M/K)$ sobre o conjunto das raízes complexas de $f(X)$ é transitiva.

3. Seja $K := \mathbb{Q}(\sqrt[8]{n})$. Determine todos os isomorfismos de aneis $K \to K$.

4. Seja p um número primo e seja M um corpo de decomposição de $f(X) = X^4 - p$ sobre $\mathbb{Q}$ (lembrando que $f(X)$ é irredutível em $\mathbb{Q}[X]$ pelo critério de Eisenstein). Mostre que o grupo de Galois $\mathcal{G}(M/\mathbb{Q})$ é isomorfo ao grupo diedral de ordem 8.

Atenção: a, b, c, n não são números quaisquer, são os números definidos 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 – Trabalho semanal 4 de Álgebra 3 – Semestre 2021-2
Resolução.
Aqui n é um inteiro positivo com $n > 4$ e $n \equiv 2 \mod 4$.

1. Seja G um grupo finito de ordem $|G| = 4m$ com m ímpar e suponha que G admita um 2-subgrupo de Sylow cíclico. Mostre que existe $H \leq G$ tal que $|G : H| = 4$.

   [Dica. Mergulhe G em $\mathrm{Sym}(G)$ e considere $G \cap \mathrm{Alt}(G)$.]

   A ação de G sobre G de multiplicação a direita dá a representação permutacional regular $\gamma : G \to \mathrm{Sym}(G)$, que é injetiva. Considere $H := \gamma(G) \cap A$, onde $A := \mathrm{Alt}(G)$ é o grupo alternado dentro $S = \mathrm{Sym}(G)$. Observe que $A \trianglelefteq S$, logo $A \leq \gamma(G)A \leq S$, e como $|S : A| = 2$ segue que $A = \gamma(G)A$ ou $\gamma(G)A = S$. O primeiro caso, $A = \gamma(G)A$, acontece se e somente se $\gamma(G) \subseteq A$. Mostraremos que isso é falso. Para isso, é suficiente construir um elemento de $\gamma(G)$ que não pertence a A. Por hipótese, G contém um 2-subgrupo de Sylow cíclico, ou seja existe $g \in G$ de ordem 4. É claro que $\gamma(g)$ é um produto de m 4-cíclos dois a dois disjuntos. Como m é ímpar, $\gamma(g)$ é uma permutação ímpar, logo $\gamma(g) \in \gamma(G)$ mas $\gamma(g) \notin A$.

   Segue que $\gamma(G) \not\subseteq A$, ou seja $H = \gamma(G) \cap A$ está propriamente contido em $\gamma(G)$. Além disso $\gamma(G)A = S$. Segue que $2|A| = |S| = |\gamma(G)A| = |\gamma(G)| \cdot |A|/|H|$, logo $|\gamma(G) : H| = 2$. Lembrando que $G \cong \gamma(G)$, segue que $|G : K| = 2$ onde $K := \gamma^{-1}(H)$. Segue que $|K| = |G|/2 = 2m$ com m ímpar, logo, como visto nas aulas, existe $L < K$ tal que $|K : L| = 2$. Segue que $|L| = |K|/2 = m$ e L é um subgrupo de G tal que $|G : L| = |G|/|L| = 4m/m = 4$.

2. Calcule o grau $|M : \mathbb{Q}|$ onde M é corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ em cada um dos casos seguintes.

$$f(X) = X^3 - n, \qquad f(X) = X^4 + 13X^2 - (a+2)(a-11).$$

   Em cada caso, diga se a ação de $\mathcal{G}(M/K)$ sobre o conjunto das raízes complexas de $f(X)$ é transitiva.

   Primeiro caso. $f(X) = X^3 - n$ é irredutível pelo critério de Eisenstein aplicado a 2, sendo $n \equiv 2 \mod 4$. As raízes de $f(X)$ são $t = \sqrt[3]{n}$, $t\rho$ e $t\rho^2$ onde $\rho = e^{i2\pi/3} = -1/2 + i\sqrt{3}/2$. Segue que $M = \mathbb{Q}(t, i\sqrt{3})$, $|\mathbb{Q}(t) : \mathbb{Q}| = 3$ e $i\sqrt{3} \notin \mathbb{Q}(t)$ sendo $\mathbb{Q}(t) \subseteq \mathbb{R}$, logo

$$|G| = |M : \mathbb{Q}| = |\mathbb{Q}(t, i) : \mathbb{Q}| = |\mathbb{Q}(t)(i) : \mathbb{Q}(t)| \cdot |\mathbb{Q}(t) : \mathbb{Q}| = 2 \cdot 3 = 6.$$

   A ação de G sobre o conjunto $\Omega = \{t, t\rho, t\rho^2\}$ das raízes de $f(X)$ é fiel, logo a representação permutacional associada $G \to \mathrm{Sym}(\Omega) \cong S_3$ é injetiva. Como $|G| = 6 = |\mathrm{Sym}(\Omega)|$, segue que $G \cong \mathrm{Sym}(\Omega)$, logo G age transitivamente sobre Ω.

   Segundo caso.

$$f(X) = X^4 + 13X^2 - (a+2)(a-11) = (X^2 - (-a-2)) \cdot (X^2 - (a-11)).$$

Como $r = -a-2$ e $s = a-11$ são negativos, os dois fatores são irredutíveis. As quatro raízes de $f(X)$ são $\pm\alpha$, $\pm\beta$ onde $\alpha = i\sqrt{a+2} \in i\mathbb{R}$ e $\beta = i\sqrt{11-a} \in i\mathbb{R}$. Observe que nenhum $\sigma \in G$ satisfaz $\sigma(\alpha) = \beta$ e a ação de G no conjunto das raízes não é transitiva. De fato, se existisse um tal σ, então teriamos

$$r = \sigma(r) = \sigma(\alpha^2) = \sigma(\alpha)^2 = \beta^2 = s,$$

e isso é falso, pois $r \neq s$.

Considere o caso $a = 2$. Neste caso $f(X) = (X^2+4)(X^2+9)$ e as raízes de $f(X)$ são $\pm 2i$, $\pm 3i$, logo $M = \mathbb{Q}(i)$ e $|M : \mathbb{Q}| = 2$.

Considere o caso $a = 3$. Neste caso $f(X) = (X^2+5)(X^2+8)$ logo $M = \mathbb{Q}(i\sqrt{5}, i\sqrt{2}) = \mathbb{Q}(\sqrt{5/2}, i\sqrt{2})$. Pelos argumentos usuais $|G| = |M : \mathbb{Q}| = 4$.

3. Seja $K := \mathbb{Q}(\sqrt[8]{n})$. Determine todos os isomorfismos de aneis $K \to K$.

   Seja $\alpha := \sqrt[8]{n}$, assim $\alpha^8 = n$. Observe que se $\varphi : K \to K$ é isomorfismo de aneis então

   $$\varphi(\alpha)^8 = \varphi(\alpha^8) = \varphi(n) = n,$$

   logo $\varphi(\alpha)$ é raiz de $X^8 - n$. Por outro lado $K \subseteq \mathbb{R}$, logo $\varphi(\alpha)$ é uma raiz real de $X^8 - n$. As únicas raízes reais de $X^8 - n$ são α e $-\alpha$, logo $\varphi(\alpha) = \pm\alpha$. Segue que existem exatamente dois isomorfismos de aneis $K \to K$, um é a identidade, o outro fixa os racionais e leva α para $-\alpha$, mais explicitamente, chamado de $\beta = -\alpha$, é a composição

   $$\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(X^8 - n) \cong \mathbb{Q}(\beta).$$

   Lembre-se que $X^8 - n$ é irredutível pelo critério de Eisenstein aplicado a 2, sendo n divisível por 2 mas não por 4.

4. Seja p um número primo e seja M um corpo de decomposição de $f(X) = X^4 - p$ sobre $\mathbb{Q}$ (lembrando que $f(X)$ é irredutível em $\mathbb{Q}[X]$ pelo critério de Eisenstein). Mostre que o grupo de Galois $\mathcal{G}(M/\mathbb{Q})$ é isomorfo ao grupo diedral de ordem 8.

   Temos $M = \mathbb{Q}(\alpha, i)$ onde $\alpha = \sqrt[4]{p}$. Como $X^4 - p$ é irredutível, $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$, além disso $i \notin \mathbb{Q}(\alpha)$ pois $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, logo i tem grau 2 sobre $\mathbb{Q}(\alpha)$. Segue então da formula do grau que

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

   Mas sabemos que $G = \mathcal{G}(M/\mathbb{Q})$ tem ordem $|G| = |M : \mathbb{Q}| = 8$. Além disso G age de forma fiel sobre o conjunto das quatro raízes de $f(X)$, que é $\Omega = \{\alpha, i\alpha, -\alpha, -i\alpha\}$. Isso dá uma representação permutacional injetiva $G \to S_4$, logo G é isomorfo a um subgrupo de S_4. Mas os subgrupos de S_4 de ordem 8 são exatamente os 2-Sylow de S_4, e vimos que são grupos diedrais de ordem 8.

T5 – Trabalho semanal 5 de Álgebra 3 – Semestre 2021-2

Semana: 14 - 18 de março, 2022.
Prazo de entrega: 31 de março, 2022.

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

$$n := 4(27 - a - b - c) + 2.$$

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 G um grupo finito, seja H um subgrupo de G e seja $x \in H$. Mostre que
$$|C_G(x) : C_H(x)| \leq |G : H|.$$

2. Seja $f(X) \in \mathbb{Q}[X]$ e seja M o corpo de decomposição de $f(X)$ contido em $\mathbb{C}$. Seja G o grupo de Galois de $M/\mathbb{Q}$. Calcule $|G|$ em cada um dos seguintes casos.
$$f(X) = X^4 + 1, \qquad f(X) = X^3 - n, \qquad f(X) = X^4 - n.$$

3. Considere $f(X) = X^4 + 1 \in \mathbb{Q}[X]$. Mostre que para todo primo p o polinômio $f(X)$ reduzido módulo p, $X^4 + 1 \in \mathbb{F}_p[X]$, é redutível em $\mathbb{F}_p[X]$ (aqui $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$).

   [Dica. Mostre que no corpo $\mathbb{F}_p$ tem $(p-1)/2$ quadrados não nulos, que formam um subgrupo de $\mathbb{F}_p^*$ de índice 2, e se dois elementos α, β de $\mathbb{F}_p$ não são quadrados, então $\alpha\beta$ é um quadrado.]

   [*Digressão.* Veja o teorema de densidade de Frobenius. Os típos de fatorações de $f(X)$ módulo os primos correspondem à estruturas cíclicas dos elementos do grupo de Galois. Em particular $f(X) \in \mathbb{Q}[X]$ de grau n é irredutível módulo p para algum primo p se e somente se o grupo de Galois de $f(X)$, visto como subgrupo de S_n, contém n-ciclos.]

4. Seja $f(X) \in \mathbb{Q}[X]$ e seja M o corpo de decomposição de $f(X)$ contido em $\mathbb{C}$. Seja $G := \mathcal{G}(M/\mathbb{Q})$ o grupo de Galois da extensão $M/\mathbb{Q}$. Mostre que se $|G|$ é ímpar então $M \subseteq \mathbb{R}$.

   [Dica: Seja $\sigma : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Mostre que $\sigma(M) = M$.]

[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 – Trabalho semanal 5 de Álgebra 3 – Resolução.

Aqui $n > 4$ e $n \equiv 2 \mod 4$.

1. Seja G um grupo finito, seja H um subgrupo de G e seja $x \in H$. Mostre que
$$|C_G(x) : C_H(x)| \leq |G : H|.$$

   Sejam
$$A := \{hxh^{-1} \ : \ h \in H\}, \qquad B := \{ghg^{-1} \ : \ g \in G\}.$$

   É claro que $A \subseteq B$, logo $|A| \leq |B|$. Mas pelo princípio da contagem,
$$|H : C_H(x)| = |A| \leq |B| = |G : C_G(x)|.$$

   Isso pode ser reformulado como $|C_G(x) : C_H(x)| \leq |G : H|$.

2. Seja $f(X) \in \mathbb{Q}[X]$ e seja M o corpo de decomposição de $f(X)$ contido em $\mathbb{C}$. Seja G o grupo de Galois de $M/\mathbb{Q}$. Calcule $|G|$ em cada um dos seguintes casos.
$$f(X) = X^4 + 1, \qquad f(X) = X^3 - n, \qquad f(X) = X^4 - n.$$

   $f(X) = X^4 + 1$. É irredutível porque $f(X + 1)$ é irredutível pelo critério de Eisenstein aplicado a 2, sendo
$$f(X + 1) = (X + 1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

   As raízes de $f(X)$ são $\pm(1 \pm i)/\sqrt{2}$, logo $M = \mathbb{Q}(i, \sqrt{2})$, $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$ $|G| = |M : \mathbb{Q}| = 4$ e $i \notin \mathbb{Q}(\sqrt{2})$ sendo $\mathbb{Q}(t) \subseteq \mathbb{R}$, logo
$$|G| = |M : \mathbb{Q}| = |\mathbb{Q}(t, i) : \mathbb{Q}| = |\mathbb{Q}(t)(i) : \mathbb{Q}(t)| \cdot |\mathbb{Q}(t) : \mathbb{Q}| = 2 \cdot 2 = 4.$$

   $f(X) = X^3 - n$ é irredutível pelo critério de Eisenstein aplicado a 2, sendo $n \equiv 2 \mod 4$. As raízes de $f(X)$ são $t = \sqrt[3]{n}$, $t\rho$ e $t\rho^2$ onde $\rho = e^{i2\pi/3} = -1/2 + i\sqrt{3}/2$. Segue que $M = \mathbb{Q}(t, i\sqrt{3})$, $|\mathbb{Q}(t) : \mathbb{Q}| = 3$ e $i\sqrt{3} \notin \mathbb{Q}(t)$ sendo $\mathbb{Q}(t) \subseteq \mathbb{R}$, logo
$$|G| = |M : \mathbb{Q}| = |\mathbb{Q}(t, i) : \mathbb{Q}| = |\mathbb{Q}(t)(i) : \mathbb{Q}(t)| \cdot |\mathbb{Q}(t) : \mathbb{Q}| = 2 \cdot 3 = 6.$$

   $f(X) = X^4 - n$ é irredutível pelo critério de Eisenstein aplicado a 2, sendo $n \equiv 2 \mod 4$. As raízes de $f(X)$ são $t = \sqrt[4]{n}$, $-t$, it, $-it$, logo $M = \mathbb{Q}(t, i)$, $|\mathbb{Q}(t) : \mathbb{Q}| = 4$ e $i \notin \mathbb{Q}(t)$ sendo $\mathbb{Q}(t) \subseteq \mathbb{R}$, logo
$$|G| = |M : \mathbb{Q}| = |\mathbb{Q}(t, i) : \mathbb{Q}| = |\mathbb{Q}(t)(i) : \mathbb{Q}(t)| \cdot |\mathbb{Q}(t) : \mathbb{Q}| = 2 \cdot 4 = 8.$$

3. Considere $f(X) = X^4 + 1 \in \mathbb{Q}[X]$. Mostre que para todo primo p o polinômio $f(X)$ reduzido módulo p, $X^4+1 \in \mathbb{F}_p[X]$, é redutível em $\mathbb{F}_p[X]$ (aqui $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$).

   [Dica. Mostre que no corpo $\mathbb{F}_p$ tem $(p-1)/2$ quadrados não nulos, que formam um subgrupo de $\mathbb{F}_p^*$ de índice 2, e se dois elementos α, β de $\mathbb{F}_p$ não são quadrados, então $\alpha\beta$ é um quadrado.]

   Seja $N := \{a^2 \,:\, a \in \mathbb{F}_p^*\}$. Se trata da imagem do homomorfismo de grupos $f : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^2$. Observe que $\ker(f) = \{x \in \mathbb{F}_p^* \,:\, x^2 = 1\} = \{-1, 1\}$, logo N é isomorfo a $\mathbb{F}_p^*/\{1, -1\}$. Segue que $|N| = (p-1)/2$, ou seja $|\mathbb{F}_p^* : N| = 2$. Temos então $\mathbb{F}_p^*/N = \{N, aN\}$ onde $a \in \mathbb{F}_p^*$ não é um quadrado, logo $aN = bN$ toda vez que a, b não são quadrados, assim neste caso $N = a^2N = (aN)^2 = (aN)(bN) = abN$, ou seja $ab \in N$ se $a, b \notin N$.

   Seja $f_p(X) := X^4 + 1 \in \mathbb{F}_p[X]$. Vamos buscar fatorações de $f_p(X)$ como produtos de dois fatores de grau 2.

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

   Existe uma tal fatoração se e somente se

$$a + c = 0, \quad d + ac + b = 0, \quad ad + bc = 0, \quad bd = 1.$$

   Se $a = 0$, então $c = 0$, $d = -b$ e $b^2 = -1$, logo neste caso existe uma tal fatoração se e somente se existe uma raiz quadrada de -1 em $\mathbb{F}_p$. Se $a \neq 0$, então $c = -a$, $d = b$, $2b = a^2$, $b^2 = 1$, logo $a^2 = \pm 2$ e existe uma tal fatoração se e somente se 2 ou -2 admite uma raiz quadrada em $\mathbb{F}_p$.

   Isso mostra que existe uma fatoração como acima se e somente se pelo menos um entre -1, 2 e -2 é um quadrado em $\mathbb{F}_p$. Mas se 2 e -1 não são quadrados, então $2 \cdot (-1) = -2$ é um quadrado. Logo, existe sempre uma tal fatoração.

4. Seja $f(X) \in \mathbb{Q}[X]$ e seja M o corpo de decomposição de $f(X)$ contido em $\mathbb{C}$. Seja $G := \mathcal{G}(M/\mathbb{Q})$ o grupo de Galois da extensão $M/\mathbb{Q}$. Mostre que se $|G|$ é ímpar então $M \subseteq \mathbb{R}$.

   [Dica: Seja $\sigma : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Mostre que $\sigma(M) = M$.]

   O argumento usual já usado muitas vezes nas aulas mostra que se $\alpha \in M$ é raiz de $f(X)$ então $\sigma(\alpha)$ também é raiz de $f(X)$, pois σ é um homomorfismo de aneis que fixa os racionais. Como M contém todas as raízes complexas de $f(X)$, segue que $\sigma(\alpha) \in M$. Como M é o corpo gerado pelas raízes complexas de $f(X)$, obtemos que $\sigma(M) \subseteq M$. Além disso $\sigma^{-1} = \sigma$, logo $\sigma^{-1}(M) \subseteq M$, ou seja $M \subseteq \sigma(M)$. Isso mostra que $\sigma(M) = M$. Considere a restrição $\tau := \sigma|_M$. Como $\sigma(M) = M$, temos $\tau \in G$. Sendo $\sigma^2 = 1$, temos $\tau^2 = 1$, ou seja a ordem de τ é 1 ou 2. Mas pelo teorema de Lagrange a ordem de τ divide $|G|$. Como $|G|$ é ímpar, obtemos que $\tau = 1$. Segue que $\tau(m) = m$ para todo $m \in M$, ou seja $M \subseteq \mathbb{R}$.

T6 – Trabalho semanal 6 de Álgebra 3 – Semestre 2021-2

Semana: 21 - 25 de março, 2022.
Prazo de entrega: 7 de abril, 2022.

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

$$n := 4(a + b + c) + 2.$$

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

1. Diga se $\mathbb{Q}(\alpha)/\mathbb{Q}$ é uma extensão de Galois nos casos seguintes.

$$\alpha = \sqrt{n} + \sqrt{n+4}, \qquad \alpha = \sqrt[n]{2}, \qquad \alpha = \sqrt{1 + \sqrt{n}}.$$

2. Seja $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \in \mathbb{R}$. Observe que as oito raízes do polinômio minimal de α sobre $\mathbb{Q}$ são

$$\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}.$$

   Mostre que $\mathbb{Q}(\alpha)/\mathbb{Q}$ é uma extensão de Galois.

   Dica. Observe que $(\sqrt{2}-1)\alpha = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$.

3. Descreva as correspondências de Galois para $M/\mathbb{Q}$ no caso em que $M \subseteq \mathbb{C}$ é o corpo de decomposição sobre $\mathbb{Q}$ do polinômio $f(X) \in \mathbb{Q}[X]$ nos casos seguintes.

$$f(X) = X^3 - (a+3)^3, \qquad f(X) = (X^2+1)(X^2-n).$$

4. Seja $M/\mathbb{Q}$ uma extensão de Galois de grau finito com grupo de Galois $G = \mathcal{G}(M/\mathbb{Q})$ e sejam $L_1, L_2 \in [M/\mathbb{Q}]$ (ou seja L_i é um corpo com $\mathbb{Q} \leq L_i \leq M$ para $i = 1, 2$). Mostre que L_1 e L_2 são isomorfos (ou seja existe um isomorfismo de aneis $L_1 \cong L_2$) se e somente se os subgrupos $L_1', L_2' \leq G$ são conjugados em G, ou seja existe $g \in G$ tal que $gL_1'g^{-1} = L_2'$.

   [Dica. Usando um teorema que vimos nas aulas teóricas, mostre que o isomorfismo $L_1 \cong L_2$ pode ser extendido a um automorfismo de M.]

[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 3 – Resolução

Aqui $n > 2$ e $n \equiv 2 \mod 4$.

1. Diga se $\mathbb{Q}(\alpha)/\mathbb{Q}$ é uma extensão de Galois nos casos seguintes.

$$\alpha = \sqrt{n} + \sqrt{n+4}, \qquad \alpha = \sqrt[n]{2}, \qquad \alpha = \sqrt{1+\sqrt{n}}.$$

$\alpha = \sqrt{n} + \sqrt{n+4}$. Observe que n e $n+4$ não são quadrados inteiros pois $n \equiv 2 \mod 4$. As raízes de

$$\begin{aligned} f(X) &= (X^2 - 2n - 4)^2 - 4n(n+4) \\ &= X^4 - 2(2n+4)X^2 + (2n+4)^2 - 4n(n+4) \\ &= X^4 - 2(2n+4)X^2 + 16, \end{aligned}$$

são $\pm\sqrt{n} \pm \sqrt{n+4}$, ou seja $\pm\alpha$ e $\pm\beta$ onde $\beta = \sqrt{n} - \sqrt{n+4}$. Segue que

$$f(X) = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta),$$

além disso

$$\begin{aligned} &(X-\alpha)(X+\alpha) = X^2 - \alpha^2 = X^2 - 2n - 4 - 2\sqrt{n(n+4)} \notin \mathbb{Q}[X], \\ &(X-\alpha)(X-\beta) = X^2 - 2\sqrt{n} \cdot X - 4 \notin \mathbb{Q}[X], \\ &(X-\alpha)(X+\beta) = X^2 - 2\sqrt{n+4} \cdot X + 4 \notin \mathbb{Q}[X]. \end{aligned}$$

Isso implica que nenhum fator de grau 1 e nenhum produto de dois fatores de grau 1 é um fator de $f(X)$ em $\mathbb{Q}[X]$, logo $f(X)$ é irredutível em $\mathbb{Q}[X]$, ou seja é o polinômio minimal de α sobre $\mathbb{Q}$. Observe que $\alpha\beta = -4$, logo $\beta = -4/\alpha$ (faz sentido pois $\alpha \neq 0$). Segue que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ é corpo de decomposição para $f(X)$ sobre $\mathbb{Q}$, logo $\mathbb{Q}(\alpha)/\mathbb{Q}$ é extensão de Galois.

Nos próximos dois casos usarei o seguinte resultado, provado nas aulas teóricas: se M/K é extensão de Galois finita, $f(X) \in K[X]$ é irredutível em $K[X]$ e existe $u \in M$ tal que $f(u) = 0$ então $f(X)$ pode ser fatorado em fatores de grau 1 em $M[X]$.

$\alpha = \sqrt[n]{2}$. O polinômio minimal de α é $f(X) = X^n - 2$, que é irredutível pelo critério de Eisenstein e admite n raízes distintas. Delas, apenas duas são reais, $\pm\alpha$ (lembrando que n é par), logo $f(X)$ não pode ser fatorado em fatores de grau 1 em $\mathbb{Q}(\alpha)[X]$, sendo $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Segue que $\mathbb{Q}(\alpha)/\mathbb{Q}$ não é extensão de Galois.

$\alpha = \sqrt{1+\sqrt{n}}$. Seja $f(X) = (X^2-1)^2 - n = X^4 - 2X^2 + 1 - n$. Seja $\beta = i\sqrt{\sqrt{n}-1}$. Temos a fatoração

$$f(X) = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta).$$

Segue que $f(X)$ é irredutível em $\mathbb{Q}[X]$, pois f não tem raízes inteira e nenhum produto de dois fatores de grau 1 na fatoração acima tem coeficientes racionais. Observe que $\alpha \in \mathbb{R}$ e $\beta \notin \mathbb{R}$, logo $\mathbb{Q}(\alpha)$ não contém β. Segue que $\mathbb{Q}(\alpha)/\mathbb{Q}$ não é extensão de Galois.

2. Seja $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \in \mathbb{R}$. Observe que as oito raízes do polinômio minimal de α sobre $\mathbb{Q}$ são

$$\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}.$$

Mostre que $\mathbb{Q}(\alpha)/\mathbb{Q}$ é uma extensão de Galois.

Dica. Observe que $(\sqrt{2}-1)\alpha = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$.

Sejam

$$\beta := \sqrt{(2-\sqrt{2})(3+\sqrt{3})},\ \gamma := \sqrt{(2+\sqrt{2})(3-\sqrt{3})},$$

$$\delta := \sqrt{(2-\sqrt{2})(3-\sqrt{3})}.$$

As raízes do polinômio minimal $f(X)$ de α sobre $\mathbb{Q}$ são $\pm\alpha$, $\pm\beta$, $\pm\gamma$, $\pm\delta$, logo para mostrar que $\mathbb{Q}(\alpha)$ é extensão de Galois basta mostrar que $\beta, \gamma, \delta \in \mathbb{Q}(\alpha)$, pois isso implica que $\mathbb{Q}(\alpha)$ é corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Temos que

$$\alpha\beta = \sqrt{2}(3+\sqrt{3}), \quad \alpha\gamma = \sqrt{6}(2+\sqrt{2}), \quad \alpha\delta = \sqrt{2}\sqrt{6} = 2\sqrt{3},$$

logo para mostrar que $\beta, \gamma, \delta \in \mathbb{Q}(\alpha)$ basta mostrar que $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$. Como $\alpha^2 = (2+\sqrt{2})(3+\sqrt{3})$, obviamente $\sqrt{2} \in \mathbb{Q}(\alpha)$ se e somente se $\sqrt{3} \in \mathbb{Q}(\alpha)$. Basta então mostrar que $\sqrt{2} \in \mathbb{Q}(\alpha)$. Temos $(\alpha\delta)^2 = 12$, logo $\delta^2 \in \mathbb{Q}(\alpha)$ e isso implica que $\sqrt{6} = (\alpha^2 + \delta^2 - 12)/2 \in \mathbb{Q}(\alpha)$. Segue que

$$u = (\sqrt{2}+\sqrt{3})\sqrt{6} = 2\sqrt{3} + 3\sqrt{2} = \alpha^2 - 6 - \sqrt{6} \in \mathbb{Q}(\alpha),$$

logo $\sqrt{2} = (2\sqrt{3} + 3\sqrt{2}) - 2(\sqrt{3}+\sqrt{2}) = u - 2u/\sqrt{6} \in \mathbb{Q}(\alpha)$.

3. Descreva as correspondências de Galois para $M/\mathbb{Q}$ no caso em que $M \subseteq \mathbb{C}$ é o corpo de decomposição sobre $\mathbb{Q}$ do polinômio $f(X) \in \mathbb{Q}[X]$ nos casos seguintes.

$$f(X) = X^3 - (a+3)^3, \qquad f(X) = (X^2+1)(X^2-n).$$

Primeiro polinômio. $f(X) = X^3 - t^3$, onde $t = a + 3 > 0$. Observe que

$$\begin{aligned} f(X) = X^3 - t^3 &= (X-t)(X^2+tX+t^2) \\ &= (X-t)(X - t(-1+i\sqrt{3})/2)(X - t(-1-i\sqrt{3})/2). \end{aligned}$$

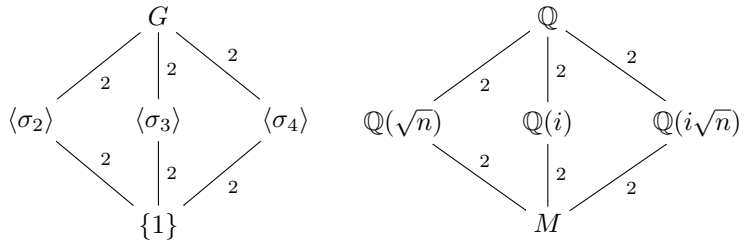
Seja $G := \mathscr{G}(M/\mathbb{Q})$. Segue que $M = \mathbb{Q}(i\sqrt{3})$ e $|G| = |M : \mathbb{Q}| = 2$, logo $G = \{1, \sigma\} \cong C_2$ e $\sigma(a + bi\sqrt{3}) = a - bi\sqrt{3}$. Os únicos subgrupos de G são $\{1\}$ e G e os únicos subcorpos de M são $\{1\}' = M$ e $G' = \mathbb{Q}$.

Segundo polinômio. $f(X) = (X^2+1)(X^2-n)$. Observe que os dois fatores são irredutíveis pois $i, \sqrt{n} \notin \mathbb{Q}$ (sendo $n \equiv 2 \mod 4$). Seja $G := \mathscr{G}(M/\mathbb{Q})$. Temos que $M = \mathbb{Q}(i, \sqrt{n})$ tem grau 4 sobre $\mathbb{Q}$ pela formula do grau, sendo $i \notin \mathbb{Q}(\sqrt{n}) \subseteq \mathbb{R}$. Segue que $|G| = |M : \mathbb{Q}| = 4$. Além disso, se $\sigma \in G$, então $\sigma(i) = \pm i$ e $\sigma(\sqrt{n}) = \pm\sqrt{n}$, logo, como M é gerado por i e $\sqrt{n}$, tem no máximo 4 possibilidades para σ. Como $|G| = 4$, cada possibilidade ocorre. Em outras palavras os quatro elementos σ_i, $i = 1, 2, 3, 4$, de G satisfazem a tabela seguinte.

	i	$\sqrt{n}$	Estrutura cíclica
σ_1	i	$\sqrt{n}$	Identidade
σ_2	$-i$	$\sqrt{n}$	$(i, -i)$
σ_3	i	$-\sqrt{n}$	$(\sqrt{n}, -\sqrt{n})$
σ_4	$-i$	$-\sqrt{n}$	$(i, -i)(\sqrt{n}, -\sqrt{n})$

Os elementos não triviais têm ordem 2 e $G \cong C_2 \times C_2$. Os subgrupos de G são $\{1\} = \{\sigma_1\}$, G e $\langle\sigma_i\rangle = \{1, \sigma_i\}$ para $i = 2, 3, 4$. É claro pela tabela que

$$\langle\sigma_2\rangle' = \mathbb{Q}(\sqrt{n}), \qquad \langle\sigma_3\rangle' = \mathbb{Q}(i), \qquad \langle\sigma_4\rangle' = \mathbb{Q}(i\sqrt{n}).$$



4. Seja $M/\mathbb{Q}$ uma extensão de Galois de grau finito com grupo de Galois $G = \mathcal{G}(M/\mathbb{Q})$ e sejam $L_1, L_2 \in [M/\mathbb{Q}]$ (ou seja L_i é um corpo com $\mathbb{Q} \leq L_i \leq M$ para $i = 1, 2$). Mostre que L_1 e L_2 são isomorfos (ou seja existe um isomorfismo de aneis $L_1 \cong L_2$) se e somente se os subgrupos $L_1', L_2' \leq G$ são conjugados em G, ou seja existe $g \in G$ tal que $gL_1'g^{-1} = L_2'$.

   [Dica. Usando um teorema que vimos nas aulas teóricas, mostre que o isomorfismo $L_1 \cong L_2$ pode ser extendido a um automorfismo de M.]

   Como $M/\mathbb{Q}$ é extensão de Galois de grau finito, existe $f(X) \in \mathbb{Q}[X]$ tal que M é corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Seja $\sigma : L_1 \to L_2$ um isomorfismo. Sabemos que σ fixa todos os racionais (todo homomorfismo de aneis cujo domínio contém os racionais fixa todos os racionais, como vimos nas aulas teóricas), logo $\widehat{\sigma}(f(X)) = f(X)$, onde $\widehat{\sigma}$ é o único isomorfismo $L_1[X] \to L_2[X]$ cuja restrição a L_1 é igual a σ. Por um teorema que vimos nas aulas teóricas, existe um isomorfismo $g : M \to M$

tal que $g|_{L_1} = \sigma$. Segue que $g \in G = \mathcal{G}(M/\mathbb{Q})$ (pois σ fixa os racionais). Mostraremos que $gL_1'g^{-1} = L_2'$. Observe que $L_2 = \sigma(L_1) = g(L_1)$, logo

$$\begin{aligned}
L_2' &= g(L_1)' \\
&= \{\gamma \in G \ : \ \gamma(g(\ell)) = g(\ell) \quad \forall \ell \in L_1\} \\
&= \{\gamma \in G \ : \ g^{-1}\left(\gamma\left(g(\ell)\right)\right) = \ell \quad \forall \ell \in L_1\} \\
&= \{\gamma \in G \ : \ g^{-1}\gamma g \in L_1'\} \\
&= \{\gamma \in G \ : \ \gamma \in gL_1'g^{-1}\} \\
&= gL_1'g^{-1}.
\end{aligned}$$

Agora suponha que $g \in G = \mathcal{G}(M/\mathbb{Q})$ é tal que $gL_1'g^{-1} = L_2'$. Mostraremos que $g(L_1) = L_2$. O argumento acima mostra que $gL_1'g^{-1} = g(L_1)'$, logo no nosso caso temos $L_2' = gL_1'g^{-1} = g(L_1)'$. Como $M/\mathbb{Q}$ é extensão de Galois, L_2 e $g(L_1)$ são fechados, logo $L_2 = L_2'' = g(L_1)'' = g(L_1)$. Seja $\sigma := g|_{L_1}$. Como $g(L_1) = L_2$, temos que σ é um isomorfismo $L_1 \cong L_2$.

T7 – Trabalho semanal 7 de Álgebra 3 – Semestre 2021-2

Semana: 28 de março - 1 de abril, 2022.
Prazo de entrega: 14 de abril, 2022.
Justifique todas as respostas.

1. (5 pontos) Considere os números reais positivos seguintes.

$$\alpha_1 := \sqrt{\left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)}, \qquad \alpha_2 := \sqrt{\left(2-\sqrt{2}\right)\left(3+\sqrt{3}\right)},$$

$$\alpha_3 := \sqrt{\left(2+\sqrt{2}\right)\left(3-\sqrt{3}\right)}, \qquad \alpha_4 := \sqrt{\left(2-\sqrt{2}\right)\left(3-\sqrt{3}\right)}.$$

Seja $M := \mathbb{Q}(\alpha_1)$. As oito raízes do polinômio minimal de α_1 sobre $\mathbb{Q}$ são $\pm\alpha_i$, $i = 1, 2, 3, 4$. Sejam $\alpha_5 = -\alpha_1$, $\alpha_6 = -\alpha_2$, $\alpha_7 = -\alpha_3$, $\alpha_8 = -\alpha_4$. Vimos no T6 que $M/\mathbb{Q}$ é extensão de Galois. Seja $G = \mathcal{G}(M/\mathbb{Q})$ o seu grupo de Galois.

   (a) Mostre que para todo $i \in \{1, \ldots, 8\}$ existe um único isomorfismo de aneis $f_i : M \to M$ tal que $f_i(\alpha_1) = \alpha_i$.

   (b) Mostre que $G = \{f_1, \ldots, f_8\}$.

   (c) Para todo $i, j \in \{1, \ldots, 8\}$ encontre o índice k tal que $f_i f_j = f_k$.

   (d) Determine todos os subcorpos de M e todos os subgrupos de G. [Mostre que g_5 pertence a todos os subgrupos não triviais de G.]

   Pode usar o fato que o polinômio minimal de α_1 sobre $\mathbb{Q}$ é

$$f(X) = X^8 - 24X^6 + 144X^4 - 288X^2 + 144.$$

   Se trata de um polinômio irredutível de $\mathbb{Q}[X]$ (não precisa mostrar isso).

   Se achar útil pode usar a fórmula, que vale para $0 \leq b \leq a^2$,

$$\sqrt{a \pm \sqrt{b}} = \sqrt{\frac{a+\sqrt{a^2-b}}{2}} \pm \sqrt{\frac{a-\sqrt{a^2-b}}{2}}.$$

2. (2.5 pontos) Conte os subcorpos de $\mathbb{Q}\left(\sqrt{37+\sqrt{37}}\right)$.

3. (2.5 pontos) Seja m um inteiro e seja M o corpo de decomposição de

$$f(X) = X^3 + 3X^2 + (3-m)X + m + 1 \in \mathbb{Q}[X]$$

   sobre $\mathbb{Q}$. Seja $G_m := \mathcal{G}(M/\mathbb{Q})$. Seja A_3 o grupo alternado de grau 3 e seja

$$Y := \{m \in \{0, 1, 2, \ldots, 60\} \ : \ G_m \cong A_3\}.$$

   Calcule $|Y|$.

T7 – Trabalho semanal 7 de Álgebra 3 – Resolução

1. (5 pontos) Considere os números reais positivos seguintes.

$$\alpha_1 := \sqrt{\left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)}, \qquad \alpha_2 := \sqrt{\left(2-\sqrt{2}\right)\left(3+\sqrt{3}\right)},$$

$$\alpha_3 := \sqrt{\left(2+\sqrt{2}\right)\left(3-\sqrt{3}\right)}, \qquad \alpha_4 := \sqrt{\left(2-\sqrt{2}\right)\left(3-\sqrt{3}\right)}.$$

Seja $M := \mathbb{Q}(\alpha_1)$. As oito raízes do polinômio minimal de α_1 sobre $\mathbb{Q}$ são $\pm\alpha_i$, $i = 1, 2, 3, 4$. Sejam $\alpha_5 = -\alpha_1$, $\alpha_6 = -\alpha_2$, $\alpha_7 = -\alpha_3$, $\alpha_8 = -\alpha_4$. Vimos no T6 que $M/\mathbb{Q}$ é extensão de Galois. Seja $G = \mathcal{G}(M/\mathbb{Q})$ o seu grupo de Galois.

(a) Mostre que para todo $i \in \{1, \ldots, 8\}$ existe um único isomorfismo de aneis $f_i : M \to M$ tal que $f_i(\alpha_1) = \alpha_i$.

(b) Mostre que $G = \{f_1, \ldots, f_8\}$.

(c) Para todo $i, j \in \{1, \ldots, 8\}$ encontre o índice k tal que $f_i f_j = f_k$.

(d) Determine todos os subcorpos de M e todos os subgrupos de G. [Mostre que g_5 pertence a todos os subgrupos não triviais de G.]

Pode usar o fato que o polinômio minimal de α_1 sobre $\mathbb{Q}$ é

$$f(X) = X^8 - 24X^6 + 144X^4 - 288X^2 + 144.$$

Se trata de um polinômio irredutível de $\mathbb{Q}[X]$ (não precisa mostrar isso).

Primeiramente observe que, como $f(X)$ é irredutível e G é o seu grupo de Galois sobre $\mathbb{Q}$, a ação de G sobre $\Omega = \{\alpha_1, \ldots, \alpha_8\}$ é transitiva, logo para todo $i \in \{1, \ldots, 8\}$ existe $f_i \in G$ tal que $f_i(\alpha_1) = \alpha_i$. Tal f_i é o único automorfismo de M que leva α_1 para α_i pois M é gerado por α_1 sobre $\mathbb{Q}$. A ordem de G é igual a $|G| = |M : \mathbb{Q}| = |\mathbb{Q}(\alpha_1) : \mathbb{Q}|$, igual ao grau de $f(X)$, que é 8. Logo G tem 8 elementos, por outro lado $f_1, \ldots, f_8$ são 8 elementos distintos de G. Segue que $G = \{f_1, \ldots, f_8\}$. O elemento neutro de G é f_1, que é a identidade $M \to M$.

Observe que α_1^2, α_2^2, α_3^2, α_4^2 são dois a dois distintos e $f_i(\sqrt{2}) = \pm\sqrt{2}$, $f_i(\sqrt{3}) = \pm\sqrt{3}$ para todo $i = 1, \ldots, 8$ pois $f_i(\sqrt{2})^2 = f_i(\sqrt{2}^2) = f_i(2) = 2$ e $f_i(\sqrt{3})^2 = f_i(\sqrt{3}^2) = f_i(3) = 3$. Como $f_i(\alpha_1^2) = f_i(\alpha_1)^2 = \alpha_i^2$ para todo $i = 1, \ldots, 8$, deduzimos que

$$\begin{array}{ll} f_1(\sqrt{2}) = f_5(\sqrt{2}) = \sqrt{2}, & f_1(\sqrt{3}) = f_5(\sqrt{3}) = \sqrt{3}, \\ f_2(\sqrt{2}) = f_6(\sqrt{2}) = -\sqrt{2}, & f_2(\sqrt{3}) = f_6(\sqrt{3}) = \sqrt{3}, \\ f_3(\sqrt{2}) = f_7(\sqrt{2}) = \sqrt{2}, & f_3(\sqrt{3}) = f_7(\sqrt{3}) = -\sqrt{3}, \\ f_4(\sqrt{2}) = f_8(\sqrt{2}) = -\sqrt{2}, & f_4(\sqrt{3}) = f_8(\sqrt{3}) = -\sqrt{3}. \end{array}$$

É claro que $\alpha_1\alpha_4 = \alpha_2\alpha_3$. Além disso

$$\begin{array}{lll} \frac{\alpha_2}{\alpha_1} = \sqrt{2}-1, & \frac{\alpha_3}{\alpha_1} = \frac{\sqrt{3}-1}{\sqrt{2}}, & \frac{\alpha_4}{\alpha_1} = \frac{(\sqrt{2}-1)(\sqrt{3}-1)}{\sqrt{2}}. \\ \frac{\alpha_1}{\alpha_2} = \sqrt{2}+1, & \frac{\alpha_1}{\alpha_3} = \frac{\sqrt{3}+1}{\sqrt{2}}, & \frac{\alpha_1}{\alpha_4} = \frac{(\sqrt{2}+1)(\sqrt{3}+1)}{\sqrt{2}}. \end{array}$$

Obtemos a seguinte tabela, que contém os valores $f_i(\alpha_j/\alpha_1)$.

	α_2/α_1	α_3/α_1	α_4/α_1
f_1, f_5	α_2/α_1	α_3/α_1	α_4/α_1
f_2, f_6	$-\alpha_1/\alpha_2$	$-\alpha_3/\alpha_1$	α_3/α_2
f_3, f_7	α_2/α_1	$-\alpha_1/\alpha_3$	$-\alpha_2/\alpha_3$
f_4, f_8	$-\alpha_1/\alpha_2$	α_1/α_3	$-\alpha_1/\alpha_4$

A partir desta tabela podemos calcular $f_i(\alpha_j)$ para todo i, j. Por exemplo $f_3(\alpha_4/\alpha_1) = -\alpha_2/\alpha_3$, logo

$$\begin{aligned} f_3(f_4(\alpha_1)) &= f_3(\alpha_4) = f_3((\alpha_4/\alpha_1)\alpha_1) = f_3(\alpha_4/\alpha_1)f_3(\alpha_1) \\ &= -(\alpha_2/\alpha_3)\alpha_3 = -\alpha_2 = f_6(\alpha_1), \end{aligned}$$

logo $f_3f_4 = f_6$. Como $f_2(\alpha_3/\alpha_1) = -\alpha_3/\alpha_1$ e $\alpha_1\alpha_4 = \alpha_2\alpha_3$,

$$\begin{aligned} f_2(f_3(\alpha_1)) &= f_2(\alpha_3) = f_2((\alpha_3/\alpha_1)\alpha_1) = f_2(\alpha_3/\alpha_1)f_2(\alpha_1) \\ &= -(\alpha_3/\alpha_1)\alpha_2 = -\alpha_4 = f_8(\alpha_1), \end{aligned}$$

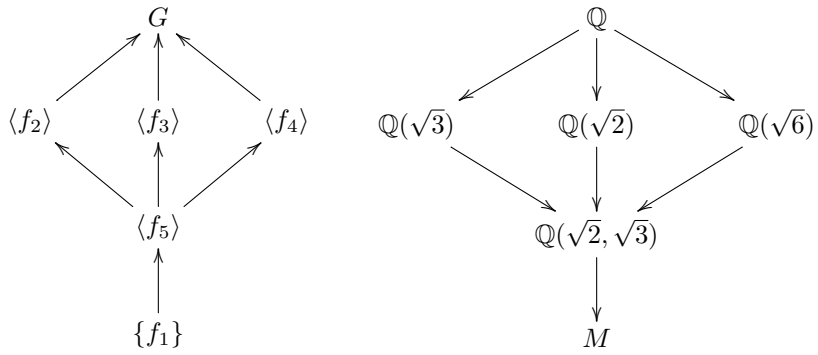
logo $f_2f_3 = f_8$.

No final obtemos a seguinte tabela, que na linha i, coluna j, contém o índice k tal que $f_if_j = f_k$.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	5	8	3	6	1	4	7
3	3	4	5	6	7	8	1	2
4	4	7	2	5	8	3	6	1
5	5	6	7	8	1	2	3	4
6	6	1	4	7	2	5	8	3
7	7	8	1	2	3	4	5	6
8	8	3	6	1	4	7	2	5

Obviamente f_1 é a identidade. Se H é um subgrupo não trivial de G então existe $i \neq 1$ tal que $f_i \in H$, logo $f_i^2 \in H$. Como ${f_i}^2 = f_5$ para todo $i \neq 1, 5$, segue que f_5 pertence a todos os subgrupos não triviais de G. Além disso $f_i^4 = f_5^2 = f_1$ para todo $i \neq 1, 5$ logo tais elementos f_i têm ordem 4, em particular os subgrupos cíclicos $\langle f_i \rangle$ ($i \neq 1, 5$) são subgrupos cíclicos de G e de índice 2. Segue que se H é um subgrupo próprio de G que contém f_i para algum $i \neq 1, 5$ então $H = \langle f_i \rangle$. Por outro lado os

únicos subgrupos de G que não contêm elementos f_i com $i \neq 1, 5$ são $\{1\}$ e $\langle f_5 \rangle$. Segue que subgrupos de G são os seguintes.



O reticulado dos subcorpos de M é obtido da seguinte maneira. Com certeza $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ são subcorpos de M, de graus 2, 2, 2 e 4 respectivamente sobre $\mathbb{Q}$, e são dois a dois distintos. Estudando os valores $f_i(\sqrt{2})$, $f_i(\sqrt{3})$, é claro que os subcorpos correspondem aos subgrupos coerentemente com a posição no desenho.

Vou fazer uma *digressão*. O grupo G é chamado grupo dos quatérnios Q_8, de ordem 8. Normalmente, os seus elementos são indicados com ± 1, $\pm i$, $\pm j$, $\pm k$ com as relações $ij = k$, $ji = -k$, $i^2 = j^2 = k^2 = -1$, $(-1)^2 = 1$. Se trata de um grupo não abeliano cujos subgrupos são todos normais. Além disso, perceba que se um polinômio irredutível $f(X) \in \mathbb{Q}[X]$ tem grupo de Galois isomorfo a Q_8 então $f(X)$ tem grau 8. Isso é porque se Q_8 age de forma fiel e transitiva sobre um conjunto Ω então $|\Omega| = 8$. De fato se H é o estabilizador de um ponto $\omega \in \Omega$ para uma tal ação então H é normal em Q_8 (pois todo subgrupo de Q_8 é normal em Q_8) logo $H = H_{Q_8} = \{1\}$ e segue que $|\Omega| = |Q_8 : H| = |Q_8 : \{1\}| = 8$.

2. (2.5 pontos) Conte os subcorpos de $\mathbb{Q}\left(\sqrt{37 + \sqrt{37}}\right)$.

Seja $\alpha := \sqrt{37 + \sqrt{37}} \in \mathbb{R}$. Temos $(\alpha^2 - 37)^2 = 37$, logo α é raiz de

$$P(X) := X^4 - 74X^2 + 36 \cdot 37,$$

que é irredutível pelo critério de Eisenstein aplicado a $p = 37$. As quatro raízes complexas de $P(X)$ são $\pm\alpha$ e $\pm\beta$, onde $\beta := \sqrt{37 - \sqrt{37}}$. Observe que $\alpha\beta = \sqrt{37^2 - 37} = 6\sqrt{37} = 6(\alpha^2 - 37)$, logo $\beta = 6(\alpha^2 - 37)/\alpha \in \mathbb{Q}(\alpha)$. Isso implica que o corpo de decomposição M de $P(X)$ sobre $\mathbb{Q}$ contido em $\mathbb{C}$ é igual a $M = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ logo a ordem do grupo de Galois $G = \mathcal{G}(M/\mathbb{Q})$ é $|G| = |M : \mathbb{Q}| = |\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$. Seja g a composição

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

Então $g \in G$ e $g(\alpha) = \beta$. Segue que

$$g^2(\alpha) = g(\beta) = g(6(\alpha^2 - 37)/\alpha) = 6(\beta^2 - 37)/\beta = -6\sqrt{37}/\beta = -\alpha.$$

Em particular $g^2(\alpha) \neq \alpha$, logo $g^2 \neq 1$. Como $g \in G$ e $|G| = 4$, isso implica que g tem ordem 4, logo G é cíclico gerado por g. Segue que os subgrupos de G são $\{1\}$, $\langle g^2 \rangle$, $\langle g \rangle = G$, e as correspondências de Galois determinam uma bijeção entre os subgrupos de G e os subcorpos de M. Segue que M tem exatamente 3 subcorpos, que são $\mathbb{Q}$, $\mathbb{Q}(\sqrt{37})$ e M.

3. (2.5 pontos) Seja m um inteiro e seja M o corpo de decomposição de

$$f(X) = X^3 + 3X^2 + (3-m)X + m + 1 \in \mathbb{Q}[X]$$

sobre $\mathbb{Q}$. Seja $G_m := \mathcal{G}(M/\mathbb{Q})$. Seja A_3 o grupo alternado de grau 3 e seja

$$Y := \{m \in \{0, 1, 2, \ldots, 60\} \ : \ G_m \cong A_3\}.$$

Calcule $|Y|$.

Temos

$$\begin{aligned} h(X) := f(X-1) &= (X-1)^3 + 3(X-1)^2 + (3-m)(X-1) + m + 1 \\ &= X^3 - 3X^2 + 3X - 1 + 3X^2 - 6X + 3 + 3X - 3 - mX + m + m + 1 \\ &= X^3 - mX + 2m \end{aligned}$$

e como $f(X)$ e $h(X)$ têm o mesmo discriminante e o mesmo corpo de decomposição sobre $\mathbb{Q}$, podemos trabalhar com o polinômio $h(X)$. O seu discriminante é

$$D = -4(-m)^3 - 27(2m)^2 = 4m^2(m - 27),$$

logo é um quadrado em $\mathbb{Q}$ se e somente se $m = 0$ ou $m - 27$ é um quadrado em $\mathbb{Q}$. No caso em que $0 \leq m \leq 60$, isso acontece exatamente para os seguintes valores de m: 0, 27, 28, 31, 36, 43, 52.

Mas observe que não todos esses valores são aceitaveis, pois para que seja $G_m \cong A_3$ o polinômio $f(X)$ precisa ser *irredutível* em $\mathbb{Q}[X]$. Dos valores de m listados, 0 e 27 não são aceitáveis pois anulam o discriminante, e um polinômio de $\mathbb{Q}[X]$ com discriminante nulo é redutível, pois ter discriminante nulo é equivalente a ter raízes múltiplas (especificamente, se $m = 0$ então $f(X) = (X+1)^3$ e se $m = 27$ então $f(X) = (X-2)^2(X+7)$). Os valores $m = 28, 31, 43, 52$ são aceitáveis pois nesses casos $f(X)$ é irredutível pelo critério de Eisenstein aplicado a $h(X)$ com os primos 7, 31, 43, 13 respectivamente. No caso $m = 36$ o polinômio $h(X)$ (logo $f(X)$ também) é irredutível, isso pode ser mostrado a mão (mostrando que $h(d) \neq 0$ para todo divisor d de $2m = 72$) ou usando Wolfram Alpha. Segue que $Y = \{28, 31, 36, 43, 52\}$ logo $|Y| = 5$.

T8 – Trabalho semanal 8 de Álgebra 3 – Semestre 2021-2

Semana: 04 - 08 de abril, 2022.
Prazo de entrega: 21 de abril, 2022.

Justifique todas as respostas.

1. (2.5 pontos) Seja $f(X) \in \mathbb{Q}[X]$ e seja M um corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Encontre a estrutura do grupo de Galois de $M/\mathbb{Q}$ nos seguintes casos (NB. Não estou pedindo as correspondências de Galois).
   (a) (0,5 ponto) $f(X) = X^4 + 3X + 20$.
   (b) (0,5 ponto) $f(X) = X^4 + 24X + 73$.
   (c) (0,5 ponto) $f(X) = X^4 + 24X + 36$.
   (d) (1 ponto) $f(X) = X^4 + X + 1$. Neste caso, seja $\alpha \in M$ uma raiz de $f(X)$. Mostre que os únicos subcorpos de $\mathbb{Q}(\alpha)$ são $\mathbb{Q}$ e $\mathbb{Q}(\alpha)$.

2. (2.5 pontos) Sejam $r, s \in \mathbb{Q}$ e sejam
$$f(X) = X^4 + rX^2 + s \in \mathbb{Q}[X], \qquad R(X) = (X - r)(X^2 - 4s).$$
$R(X)$ é a resolvente cúbica de $f(X)$, $D = 16s(r^2 - 4s)^2$ é o discriminante de $f(X)$ e de $R(X)$. Suponha $f(X)$ irredutível em $\mathbb{Q}[X]$. Mostre que
   (a) Se s é um quadrado em $\mathbb{Q}$ então $G = K$ é o grupo de Klein.
   (b) Se s não é um quadrado em $\mathbb{Q}$ e $(r^2 - 4s)s$ é um quadrado em $\mathbb{Q}$ então $G \cong C_4$, o grupo cíclico de ordem 4.
   (c) Se s não é um quadrado em $\mathbb{Q}$ e $(r^2 - 4s)s$ não é um quadrado em $\mathbb{Q}$ então $G \cong D_8$, o grupo diedral de ordem 8.

3. (2.5 pontos) Sejam
$$\alpha := 2\cos(2\pi/9) \in \mathbb{R}, \qquad M := \mathbb{Q}(i, \alpha) \subseteq \mathbb{C}.$$
Mostre que $M/\mathbb{Q}$ é uma extensão de Galois e determine todos os subgrupos do grupo de Galois $\mathscr{G}(M/\mathbb{Q})$ e os corpos intermediários correspondentes (pelas correspondências de Galois).
[Dica. Mostre que $\alpha^3 = 3\alpha - 1$.]

4. (2.5 pontos) Seja m um inteiro positivo qualquer. Mostre que existe uma extensão de Galois $M/\mathbb{Q}$ de grau m.
[Dica. Considere o grupo de Galois de $E/\mathbb{Q}$ onde E é o corpo de decomposição de $X^n - 1$ para um n oportuno.]

Pode usar os fatos seguintes. Se M é um corpo de decomposição de $X^n - 1$ sobre $\mathbb{Q}$ então $\mathscr{G}(M/\mathbb{Q})$ é isomorfo a $U(\mathbb{Z}/n\mathbb{Z})$. Se $n = \prod_{i=1}^{k} p_i^{a_i}$ é a fatoração de n como produto de primos, com os p_i primos dois a dois distintos, então $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n) = \prod_{i=1}^{k} \left((p_i - 1)p_i^{a_i - 1}\right)$. O teorema de estrutura dos grupos abelianos finitos, ou seja o fato que todo grupo abeliano finito é isomorfo a um produto direto de grupos cíclicos.

T8 – Trabalho semanal 8 de Álgebra 3 – Resolução

1. (2.5 pontos) Seja $f(X) \in \mathbb{Q}[X]$ e seja M um corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Encontre a estrutura do grupo de Galois de $M/\mathbb{Q}$ nos seguintes casos (NB. Não estou pedindo as correspondências de Galois).

   (a) (0,5 ponto) $f(X) = X^4 + 3X + 20$. É redutível,

   $$f(X) = (X^2 + 3X + 4)(X^2 - 3X + 5).$$

   As suas raízes são geradas pelas raízes quadradas dos dois discriminantes, $\alpha = i\sqrt{7}$, $\beta = i\sqrt{11}$, logo $M = \mathbb{Q}(\alpha, \beta)$ e $|M : \mathbb{Q}| = 4$. Um elemento $\sigma \in G$ satisfaz $\sigma(\alpha) = \pm\alpha$, $\sigma(\beta) = \pm\beta$ logo existem no máximo 4 possibilidades para σ. Por outro lado $|G| = |M : \mathbb{Q}| = 4$ logo cada possibilidade ocorre. Em particular segue que as estruturas cíclicas dos elementos de G (vistos como permutações das raízes de $f(X)$) são 1, $(\alpha, -\alpha)$, $(\beta, -\beta)$, $(\alpha, -\alpha)(\beta, -\beta)$ e $G \cong C_2 \times C_2$ (não transitivo).

   (b) (0,5 ponto) $f(X) = X^4+24X+73$, irredutível em $\mathbb{Q}[X]$. A resolvente cúbica é

   $$R(X) = X^3 - 292X - 576 = (X + 2)(X + 16)(X - 18)$$

   logo $G = K$ (grupo de Klein).

   (c) (0,5 ponto) $f(X) = X^4+24X+36$, irredutível em $\mathbb{Q}[X]$. A resolvente cúbica é

   $$R(X) = X^3 - 144X - 576,$$

   irredutível em $\mathbb{Q}[X]$, e o seu discriminante é

   $$D = -4 \cdot (-144)^3 - 27 \cdot (-576)^2 = 2985984 = 1728^2,$$

   um quadrado em $\mathbb{Q}$. Segue que $G = A_4$.

   (d) (1 ponto) $f(X) = X^4 + X + 1$. Neste caso, seja $\alpha \in M$ uma raiz de $f(X)$. Mostre que os únicos subcorpos de $\mathbb{Q}(\alpha)$ são $\mathbb{Q}$ e $\mathbb{Q}(\alpha)$.

   Temos que $f(X)$ é irredutível em $\mathbb{Q}[X]$ e a sua resolvente cúbica é $R(X) = X^3 - 4X - 1$, irredutível em $\mathbb{Q}[X]$, e o seu discriminante é $D = 229$, não um quadrado em $\mathbb{Q}$ (é um número primo), logo $G = S_4$. Se existisse um corpo L tal que $\mathbb{Q} < L < \mathbb{Q}(\alpha)$ então teriamos $\mathbb{Q}(\alpha)' < L' < G = S_4$, e $\mathbb{Q}(\alpha)'$ é o estabilizador de um ponto em S_4. Isso contradiz o fato que em S_4 os estabilizadores dos pontos são subgrupos maximais.

2. (2.5 pontos) Sejam $r, s \in \mathbb{Q}$ e sejam

   $$f(X) = X^4 + rX^2 + s \in \mathbb{Q}[X], \qquad R(X) = (X - r)(X^2 - 4s).$$

   $R(X)$ é a resolvente cúbica de $f(X)$, $D = 16s(r^2 - 4s)^2$ é o discriminante de $f(X)$ e de $R(X)$. Suponha $f(X)$ irredutível em $\mathbb{Q}[X]$. Mostre que

(a) Se s é um quadrado em $\mathbb{Q}$ então $G = K$ é o grupo de Klein.

(b) Se s não é um quadrado em $\mathbb{Q}$ e $(r^2 - 4s)s$ é um quadrado em $\mathbb{Q}$ então $G \cong C_4$.

(c) Se s não é um quadrado em $\mathbb{Q}$ e $(r^2 - 4s)s$ não é um quadrado em $\mathbb{Q}$ então $G \cong D_8$.

Primeiramente, observe que como $f(X)$ é irredutível em $\mathbb{Q}[X]$, o discriminante do polinômio

$$h(T) = T^2 + rT + s,$$

obtido a partir de $f(X)$ com a substituição $T = X^2$ (ou seja $f(X) = h(X^2)$), não pode ser um quadrado em $\mathbb{Q}$, em outras palavras

$$r^2 - 4s \quad \text{não é um quadrado em } \mathbb{Q}.$$

Mais em geral, se F é uma extensão de $\mathbb{Q}$ e $r^2 - 4s$ é um quadrado em F então $h(T)$ é redutível em $F[X]$, logo $f(X) = h(X^2)$ também é redutível em $F[X]$.

Se s é um quadrado em $\mathbb{Q}$, digamos $s = t^2$ com $t \in \mathbb{Q}$, então

$$R(X) = (X - r)(X - 2t)(X + 2t)$$

logo G é o grupo de Klein. Suponha que s não é um quadrado em $\mathbb{Q}$.

Temos que $\mathbb{Q}(\sqrt{s})/\mathbb{Q}$ é corpo de decomposição de $R(X)$ sobre $\mathbb{Q}$. Usando as notações da aula teórica, temos que $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{s})$. Como $R(X)$ é redutível, temos que G é isomorfo a C_4 (grupo cíclico de ordem 4) ou D_8 (grupo diedral de ordem 8). Além disso $G \cong D_8$ se e somente se $f(X)$ é irredutível em $\mathbb{Q}(\sqrt{s})[X]$.

Se $(r^2-4s)s$ é um quadrado em $\mathbb{Q}$, digamos u^2 com $u \in \mathbb{Q}$, então $r^2-4s = (u/\sqrt{s})^2$ é um quadrado em $\mathbb{Q}(\sqrt{s})$ logo $h(T)$ é redutível em $\mathbb{Q}(\sqrt{s})[T]$ logo $f(X) = h(X^2)$ é redutível em $\mathbb{Q}(\sqrt{s})[X]$ e G é cíclico.

Agora suponha que $(r^2-4s)s$ não é um quadrado em $\mathbb{Q}$. Queremos mostrar que $f(X)$ é irredutível em $\mathbb{Q}(\sqrt{s})[X]$, assim G é isomorfo a D_8. Suponha por contradição $f(X)$ redutível em $\mathbb{Q}(\sqrt{s})[X]$, assim $f(X)$ se decompõe como (1)(3) ou (2)(2). Observe que se existe uma fatoração (1)(3) então existe uma fatoração (2)(2), de fato se a é uma raiz de $f(X)$ em $\mathbb{Q}(\sqrt{s})$ então $-a$ também é raiz, sendo $f(-a) = f(a) = 0$, e obviamente $a \neq -a$ sendo $f(0) \neq 0$, logo $(X-a)(X+a) = X^2-a^2$ divide $f(X)$ em $\mathbb{Q}(\sqrt{s})[X]$. Segue que nos dois casos existe uma fatoração (2)(2), ou seja existem $a, b, c, d \in \mathbb{Q}(\sqrt{s})$ tais que

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

Segue que

$$a + c = 0, \quad d + ac + b = r, \quad ad + bc = 0, \quad bd = s.$$

Se $a \neq 0$ então $b = d$, $b^2 = s$ e $2b - a^2 = r$, mas isso implica que $\pm 2\sqrt{s} = 2b = r + a^2$ ou seja podemos escrever $\pm 2\sqrt{s} = (t + u\sqrt{s})^2 + r$ com t, u racionais, assim $tu = \pm 1$ e $t^2 + su^2 + r = 0$ e isso implica $t^2 + s/t^2 + r = 0$ ou seja $t^4 + rt^2 + s = 0$ ou seja $f(t) = 0$, contradizendo o fato que $f(X)$ é irredutível em $\mathbb{Q}[X]$.

Agora suponha $a = 0$, segue que $r = d + b$, $s = bd$, logo

$$r^2 - 4s = (b + d)^2 - 4bd = (b - d)^2.$$

Isso implica que $r^2 - 4s = (t + u\sqrt{s})^2 = t^2 + u^2 s + 2tu\sqrt{s}$ para alguns $t, u \in \mathbb{Q}$, logo $tu = 0$. Se $u = 0$ então $r^2 - 4s = t^2$, se $t = 0$ então $r^2 - 4s = u^2 s$. O primeiro caso não acontece pois $r^2 - 4s$ não é um quadrado em $\mathbb{Q}$, e no segundo caso $(r^2 - 4s)s = (us)^2$ é um quadrado em $\mathbb{Q}$, contradição.

3. (2.5 pontos) Sejam

$$\alpha := 2\cos(2\pi/9) \in \mathbb{R}, \qquad M := \mathbb{Q}(i, \alpha) \subseteq \mathbb{C}.$$

Mostre que $M/\mathbb{Q}$ é uma extensão de Galois e determine todos os subgrupos do grupo de Galois $\mathscr{G}(M/\mathbb{Q})$ e os corpos intermediários correspondentes (pelas correspondências de Galois).

[Dica. Mostre que $\alpha^3 = 3\alpha - 1$.]

Seja $\theta = 2\pi/9$, então, lembrando que valem as formulas

$$\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b),$$
$$\sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b),$$

temos

$$\begin{aligned} -\frac{1}{2} &= \cos(2\pi/3) = \cos(3\theta) = \cos(\theta + 2\theta) \\ &= \cos(\theta)\cos(2\theta) - \sin(\theta)\sin(2\theta) \\ &= \cos(\theta)(\cos^2(\theta) - \sin^2(\theta)) - 2\sin^2(\theta)\cos(\theta) \\ &= \cos^3(\theta) - \cos(\theta)(1 - \cos^2(\theta)) - 2\cos(\theta)(1 - \cos^2(\theta)) \\ &= 4\cos^3(\theta) - 3\cos(\theta) = \frac{1}{2}\alpha^3 - \frac{3}{2}\alpha, \end{aligned}$$

logo $\alpha^3 = 3\alpha - 1$. Ou seja α é raiz de $f(X) = X^3 - 3X + 1$, que tem grupo de Galois A_3 sobre $\mathbb{Q}$ pois o seu discriminante é

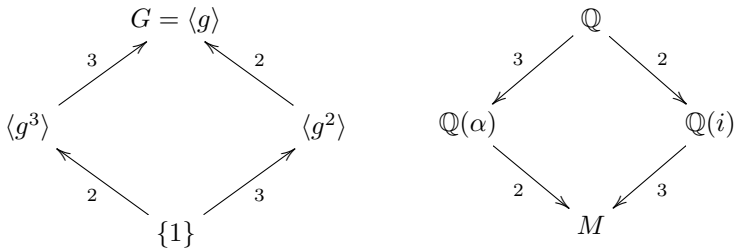
$$D = -4(-3)^3 - 27 = 3 \cdot 27 = 81 = 9^2.$$

Segue que $\mathbb{Q}(\alpha)/\mathbb{Q}$ é extensão de Galois. Sejam $L_1 = \mathbb{Q}(\alpha)$, $L_2 = \mathbb{Q}(i)$, $K = \mathbb{Q}$, $M = \mathbb{Q}(\alpha, i)$. Temos que M é corpo de decomposição sobre $\mathbb{Q}$ para $(X^3 - 3X + 1)(X^2 + 1)$ logo $M/\mathbb{Q}$ é extensão de Galois e $L_1/\mathbb{Q}$,

$L_2/\mathbb{Q}$ também são extensões de Galois, pois L_1 é corpo de decomposição de X^3-3X+1 sobre $\mathbb{Q}$ e L_2 é corpo de decomposição de X^2+1 sobre K. Sejam α,β,γ as 3 raízes de X^3-3X+1. Se $g\in G$ então $g(\alpha)\in\{\alpha,\beta,\gamma\}$ e $g(i)\in\{i,-i\}$ logo temos no máximo 6 possibilidades para g. Por outro lado

$$|G|=|M:\mathbb{Q}|=|M:\mathbb{Q}(i)|\cdot|\mathbb{Q}(i):\mathbb{Q}|=3\cdot 2=6$$

logo cada possibilidade ocorre. Em particular existe $g\in G$ tal que $g(\alpha)=\beta$ e $g(i)=-i$, assim g tem estrutura cíclica $(\alpha,\beta,\gamma)(i,-i)$ logo g tem ordem 6 e $G=\langle g\rangle$. É claro que $\langle g^2\rangle=\mathbb{Q}(i)'=L_2'$ e $\langle g^3\rangle=\mathbb{Q}(\alpha)'=L_1'$.



4. (2.5 pontos) Seja m um inteiro positivo qualquer. Mostre que existe uma extensão de Galois $M/\mathbb{Q}$ de grau m.

   [Dica. Considere o grupo de Galois de $E/\mathbb{Q}$ onde E é o corpo de decomposição de X^n-1 para um n oportuno.]

   Seja $n=m^2$. Observe que m divide $\varphi(n)$. De fato escrevendo $m=\prod_i p_i^{a_i}$ temos $n=\prod_i p_i^{2a_i}$ logo

$$\varphi(n)=\prod_i (p_i-1)p_i^{2a_i-1},$$

   logo m divide $\varphi(n)$ sendo $a_i\leq 2a_i-1$ para todo i. O grupo $G=\mathscr{G}(M/\mathbb{Q})$ é isomorfo ao grupo abeliano $U(\mathbb{Z}/n\mathbb{Z})$, logo admite um subgrupo H de ordem $\varphi(n)/m$ (pelo teorema de estrutura dos grupos abelianos finitos). Como G é abeliano, H é normal em G e H' é estável, segue que $H'/\mathbb{Q}$ é uma extensão de Galois de grau

$$|H':\mathbb{Q}|=|G:H|=\frac{\varphi(n)}{\varphi(n)/m}=m.$$