Lista 3

1. (a) Determine todos os homomorfismos de anéis de $\mathbb{Z}$ em $\mathbb{Z}$.
   (b) Caracterize $Aut(\mathbb{Z})$, $Aut(\mathbb{Q}), Aut(\mathbb{R})$.
   (c) Caracterize $Aut(\mathbb{Q}(\sqrt{n}))$

2. Seja G o grupo de Galois de K sobre $\mathbb{Q}$, onde K é o corpo de decomposição do polinômio $f(x) = x^3 - 2$.
   (a) Determine todos os automorfismos de G.
   (b) Mostre que G é isomorfo a S_3.
   (c) Para cada um dos subgrupos de G, determine o corpo fixo correspondente.

3. Seja G o grupo de Galois de $f(x) = x^4 - 2$ sobre $\mathbb{Q}$. Seja θ raiz quarta positiva de 2 então G é o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$, onde $\mathbb{K} = \mathbb{Q}(\theta, i)$.
   (a) Descreva todos os automorfismos de G.
   (b) Mostre que G é isomorfo ao grupo dihedral de ordem 8.
   (c) O grupo G possui dois subgrupos normais N_1 e N_2, não cíclicos, de ordem 4. Explicite os elementos de N_1 e N_2 e mostre que os correspondentes corpos fixos são extensões normais de $\mathbb{Q}$.

4. (a) Encontre o grupo de Galois de $x^4 - 2$ sobre $\mathbb{F}_3$.
   (b) Encontre o grupo de Galois de $x^4 - 2$ sobre $\mathbb{F}_7$.

5. Determine todos os subgrupos do grupo de Galois $Gal(L/\mathbb{Q})$, onde L é o corpo de decomposição do polinômio $f(x) \in \mathbb{Q}[x]$ assim como todos os corpos intermediários M, $\mathbb{Q} \subseteq M \subseteq L$.
   (a) $f(x) = (x^2 - 2)(x^2 - 5)$
   (b) $f(x) = x^5 - 1$
   (c) $f(x) = x^4 + 1$
   (d) $f(x) = x^3 - 5$
   (e) $f(x) = x^4 + x^2 - 1$

6. Seja $\zeta_n = e^{\frac{2\pi i}{n}}$. Para $n \in \{3, 4, 5, 7, 8, 9, 11, 13\}$, determine o grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ e para cada um dos subgrupos do grupo de Galois determine o seu corpo fixo. (os casos $n = 11$ e 13 podem ser um pouco trabalhosos.)

7. Neste exercício mostramos uma demonstração do Teorema Fundamental da Álgebra utilizando Teoria de Galois. Seja K extensão finita de $\mathbb{R}$.

   (a) Assuma que a extensão $K/\mathbb{R}$ seja Galoisiana. Mostre que existe uma cadeia de corpos

   $$\mathbb{R} \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$$

   com $[K_{i+1} : K_i] = 2, 1 \leq i \leq n-1$, e $[K_1 : \mathbb{R}]$ ímpar.

   (b) Mostre que se $[K : \mathbb{R}] = 2$ então K é isomorfo a $\mathbb{C}$.

   (c) Prove que se $[K : \mathbb{R}]$ é ímpar então $K = \mathbb{R}$.

   (d) Conclua que, ou $K = \mathbb{R}$ ou $K = \mathbb{C}$.

8. Seja K o corpo de decomposição do polinômio $f(x) = (x^2 - 2)(x^2 - 3)$.

   (a) Determine o grupo de Galois da extensão $K/\mathbb{Q}$.

   (b) Mostre que $Gal(K/\mathbb{Q})$ é isomorfo ao grupo de Klein de ordem 4 $(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

   (c) Utilizando a correspondência de Galois, apresente a decomposição de $f(x)$ sobre cada corpo intermediário L, $\mathbb{Q} \subseteq L \subseteq K$.

9. (a) Sejam $\pm\alpha, \pm\beta$ as raízes do polinômio $x^4 + ax^2 + b \in \mathbb{Z}[x]$. Mostre que $f(x)$ é irredutível sobre $\mathbb{Z}$ se e somente $\alpha^2, \alpha \pm \beta$ não pertencem a $\mathbb{Q}$.

   (b) Suponha $f(x)$ irredutível sobre $\mathbb{Z}$ e seja G o grupo de Galois de $f(x)$. Prove que:

      i. G é isomorfo ao grupo de Klein, se e somente se, b é um quadrado em $\mathbb{Q}$, se e somente se, $\alpha\beta \in \mathbb{Q}$.

      ii. G é isomorfo ao grupo cíclico de ordem 4, se e somente se, $b(a^2 - 4b)$ é um quadrado em $\mathbb{Q}$, se e somente se, $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

iii. G é isomorfo ao grupo dihedral de ordem 8, se e somente se, b e $b(a^2 - 4b)$ não são quadrados em $\mathbb{Q}$, se e somente se, $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

10. Existem cinco grupos não isomorfos de ordem 8, a citar, o grupo cíclico $\mathbb{Z}_8$, os produtos $\mathbb{Z}_4 \times \mathbb{Z}_2$, (grupo 4$-$ de Klein), $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, o grupo dihedral de ordem 8 e o grupo quatérnion de ordem 8. Para cada um destes grupos construa uma extensão de corpos galoisisiana $K \supset \mathbb{Q}$ possuindo ela como grupo de Galois.

11. Mostre que a extensão de corpos $K/\mathbb{Q}$, onde $K = \mathbb{Q}(\alpha)$ e $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ é galoisiana e mostre que o grupo de Galois da extensão $K/\mathbb{Q}$ é isomorfa ao grupo quatérnion de ordem 8.

12. Existem cinco grupos não isomorfos de ordem 12, a citar, o grupo cíclico $\mathbb{Z}_{12}$, o produto $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 (= \mathbb{Z}_2 \times \mathbb{Z}_6))$ e três grupos não abelianos: o grupo alternado A_4, o grupo dihedral $D_6 (= \mathbb{Z}_2 \times S_3)$ e o grupo dicíclico Dic_3(também chamado dihedral binário). Este último subgrupo pode ser visto como subgrupo dos quatérnions gerado por $\varepsilon = e^{\frac{\pi i}{3}}$ e j satisfazendo as relações $\varepsilon^6 = 1, j^2 = -1$ e $\varepsilon j \varepsilon = j$. Para cada um destes grupos construa uma extensão de corpos galoisiana $K \supset \mathbb{Q}$ possuindo ela como grupo de Galois.

    (Observação: $Dic_3 = \langle \varepsilon, j \rangle$, ε gera um grupo cíclico de ordem 6 e j gera um grupo cíclico de ordem 4 e $\varepsilon j \varepsilon = j$. O polinômio procurado possui corpo de decomposição contendo o corpo de decomposição de uma cúbica com grupo S_3 e uma quártica com grupo C_4 cuja intersecção é o único corpo quadrático (todos os três sobre $\mathbb{Q}$). Observe com relação ao grupo dihedral, $D_6 = \langle \varepsilon, s \mid \varepsilon^6 = 1, s^2 = 1, \varepsilon s \varepsilon = s \rangle$)

13. Seja p inteiro primo e K corpo numérico real.

    (a) Prove que se $f(x) \in K[x]$ é um polinômio irredutível de grau p com $p-2$ raízes reais e duas raízes complexas (não reais) então seu grupo de Galois é S_p.

    (b) Mostre que a equação $x^5 - p^2x - p = 0$, p inteiro primo, não é solúvel por radicais sobre $\mathbb{Q}$.

    (c) Mostre que o polinômio $f(x) = (x^2+4)(x-2)(x-4)\cdots(x-2(p-2)) - 2$ é irredutível sobre $\mathbb{Q}$ e possui exatamente $p-2$ raízes reais (o que mostra que o seu grupo de Galois é S_p)