1. Considere $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ e $g(x) = x^2 + 2x - 3$, em $\mathbb{F}_7[x]$. Encontre $q; r \in \mathbb{F}_7[x]$ tais que $f = g \cdot q + r$, com $r = 0$ ou $gr(r) < 2$.

2. (a) Decomponha o polinômio $f(x) = x^4 + 4$ em fatores irredutíveis de $\mathbb{F}_5[x]$.
   (b) Faça o mesmo para $f(x) = x^3 + 2x + 3$ em $\mathbb{F}_5[x]$.
   (c) O polinômio $f(x) = x^2 + 6x + 12$ é irredutível em $\mathbb{Q}[x]$? E em $\mathbb{R}[x]$? E em $\mathbb{C}[x]$?
   (d) Repita o ítem (c) para $g(x) = x^2 + 8x - 2$.

3. Encontre o mmc e o mdc entre os seguintes polinômios sobre o corpo $\mathbb{Q}$:
   (a) $f(x) = x^3 - 6x^2 + x + 4$ e $g(x) = x^5 - 6x + 1$.
   (b) $f(x) = x^2 + 1$ e $g(x) = x^6 + x^3 + x + 1$.

4. Mostre que:
   (a) $x^2 + x + 1$ é irredutível em $\mathbb{F}_2[x]$.
   (b) $x^2 + 1$ é irredutível em $\mathbb{F}_7[x]$.
   (c) $x^3 - 9$ é irredutível em $\mathbb{F}_{31}[x]$.
   (d) $x^3 - 9$ é irredutível em $\mathbb{F}_{11}[x]$.

5. Mostre que:
   (a) Mostre que $x^2 + 1$ é irredutível em $\mathbb{F}_{11}[x]$ e prove diretamente que $\frac{\mathbb{F}_{11}[x]}{<x^2+1>}$ é um corpo com 121 elementos.
   (b) Mostre que $x^2 + x + 4$ é irredutível em $\mathbb{F}_{11}[x]$ e prove diretamente que $\frac{\mathbb{F}_{11}[x]}{<x^2+x+4>}$ é um corpo com 121 elementos.
   (c) Os corpos $\frac{\mathbb{F}_{11}[x]}{<x^2+1>}$ e $\frac{\mathbb{F}_{11}[x]}{<x^2+x+4>}$ são isomorfos? Justifique.

6. Se $f(x) \in \mathbb{F}_p[x]$ é irredutível sobre $\mathbb{F}_p$, (p primo), de grau n. Mostre que $\frac{\mathbb{F}_p[x]}{<f>}$ é um corpo com p^n elementos.

7. Mostre que se p é um primo, então o polinômio $f(x) = x^n - p$ é irredutível sobre $\mathbb{Q}$, $n \geq 1$.

8. Verifique-se cada um dos polinômios $f(x) \in \mathbb{Z}[x]$ abaixo é irredutível sobre $\mathbb{Q}$ e, se for o caso, decomponha-o como produto de irredutíveis em $\mathbb{Q}[x]$.

   (a) $f(x) = x^5 + 2x^3 + 2x^2 + 2x + 2$

   (b) $f(x) = x^3 + 6x^2 + 5x + 25$

   (c) $f(x) = x^4 + 8x^3 + x^2 + 2x + 5$

   (d) $f(x) = x^8 + 10x^3 + 20x^2 + 30x + 22$

   (e) $f(x) = x^3 - 2x^2 + x + 15$

   (f) $f(x) = x^4 - 2$

   (g) $f(x) = x^4 - x + 1$

9. Considere o polinômio $f = x^4 + 15x^3 + 7 \in \mathbb{Z}[x]$. Use redução módulo 5 para concluir que f é irredutível sobre $\mathbb{Q}$. Mostre que f, considerado como um elemento de $\mathbb{F}_3[x]$, é redutível.

10. Mostre que o polinômio $x^n + 5x^{n-1} + 3$ é irredutível sobre $\mathbb{Z}$, para todo inteiro positivo $n \geq 1$.

11. Seja R domínio de integridade de característica $p > 0$.

    (a) Seja p primo positivo. Mostre que $p \mid \binom{p}{i}$, para todo $i, 1 \leq i < p$; onde $\binom{p}{i} = \frac{p!}{i!(p^i)!}$.

    (b) Mostre que $(x + y)^p = x^p + y^p$, para todo $x, y \in R$.

    (c) Mostre que a aplicação $\Phi : R \to R$, definida por $\Phi(a) = a^p$, é um homomorfismo de anéis (denominado homomorfismo de Frobenius).

    (d) Mostre que se R for um domínnio de integridade finito de característica $p > 0$ então o homomorfismo de Frobenius é um automorfismo de R.

    (e) Dado $p \in \mathbb{Z}$ primo, provar que o único automorfismo de $\mathbb{F}_p$ em $\mathbb{F}_p$ é o automorfismo idêntico. Deduza daí que $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}$.

    (f) Provar que se p não divide a então $a^{p-1} \equiv 1 \pmod{p})$. Este último resultado é conhecido como Pequeno Teorema de Fermat.

12. Calcule $[E : F]$ e encontre uma base de E como $F-$espaço vetorial, nos seguintes casos. Determine também $u \in E$ tal que $E = F(u)$.

    (a) $E = \mathbb{Q}(\sqrt{2}), F = \mathbb{Q}$;

    (b) $E = \mathbb{Q}(\sqrt{3}, i), F = \mathbb{Q}$;

    (c) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}), F = \mathbb{Q}$

    (d) $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}), F = \mathbb{Q}$

    (e) $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}), F = \mathbb{Q}$

    (f) $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24}), F = \mathbb{Q}$

    (g) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}), F = \mathbb{Q}(\sqrt{3})$

    (h) $E = \mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}), F = \mathbb{Q}(\sqrt{3} + \sqrt{5})$

13. Seja $\varepsilon \in \mathbb{C}, \varepsilon^3 = 1$. Calcule $[\mathbb{Q}(\varepsilon) : \mathbb{Q}]$.

14. Prove que $f(x) = x^2 - 3$ é um polinômio irredutível sobre $\mathbb{Q}(\sqrt[3]{2})$.

15. Prove que $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$. Generalize.

16. Seja $L = K(u)$, onde $u \in L$ é algébrico sobre K e $[L : K]$ é ímpar. Mostre que $L = K(u^2)$.

17. Mostre que se L/K é uma extensão finita de corpos tal que $[L : K]$ seja um número primo, então $L = K(\alpha)$, para qualquer $\alpha \in L \setminus K$.

18. (Um exemplo de extensão algébrica que não é finita)

    Seja $E = \mathbb{Q}(\sqrt{2},)\sqrt{3}, \cdots, \sqrt{p}, \cdots)$ o subcorpo de $\mathbb{R}$ gerado por $\mathbb{Q}$ e pelas raízes quadradas de todos os números primos positivos.

    (a) Mostre que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \cdots$ é uma cadeia ascendente própria de subcorpos de $\mathbb{R}$ e, portanto, $E = \mathbb{Q}$ não é extensão finita. (Sugestão: Mostre que se $p_1; \cdots, p_n; p_{n+1}$ são os primeiros $n + 1$ primos então $\sqrt{p_{n+1}} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_n})$, usando indução em n.)

    (b) Mostre que $E/\mathbb{Q}$ é uma extensão algébrica.

19. Para cada inteiro $n \geq 1$, seja $L_n = \mathbb{Q}(\sqrt[n]{2})$.

    (a) Mostre que $[L_n : \mathbb{Q}] = n$;

(b) Se $m \geq 1$ divide n, mostre que $L_m \subseteq L_n$ e, determine $[L_n : L_m]$.

(c) Se $mdc(m; n) = 1$, mostre que $L_{mn} = \mathbb{Q}(\sqrt[m]{2}, \sqrt[n]{2})$.

20. Seja L/K uma extensão de corpos e sejam $u, v \in L$ elementos algébricos sobre K tais que $[K(u) : K] = n$ e $[K(v) : K] = m$.

    (a) Mostre que se $mdc(n, m) = 1$ então $Irr(v; K)$ é irredutível sobre $K(u)$.

    (b) Mostre que se $mdc(n, m) = 1$ então $[K(u, v) : K] = nm$.

    (c) Calcule $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}]$.

21. Sejam $\beta_1, \beta_2, \cdots, \beta_n$ números complexos tais que $\beta_i^2 \in \mathbb{Q}, i = 1, \cdots, n$. Seja $L = \mathbb{Q}(\beta_1, \cdots, \beta_n)$. Mostre que $x^3 - 3$ é irredutível em $L[x]$.