3) Encontre o corpo de divisão para cada um dos seguintes polinômios: Corpo de divisão = corpo de Fatoração

a) $x^4 - 10x^2 + 21$ sobre $\mathbb{Q}$.

Se $y = x^2 \rightarrow y^2 - 10y + 21 = 0$ $\quad$ $\Delta = 10^2 - 84 = 16$ $\rightarrow y = \frac{10 \pm 4}{2}$ $\quad y' = 7$, $y'' = 3$

$x^4 - 10x^2 + 21 = (x^2-7)(x^2-3) = (x+\sqrt{7})(x-\sqrt{7})(x+\sqrt{3})(x-\sqrt{3})$

Temos que todas as raízes vivem em $\mathbb{Q}(\sqrt{7}, \sqrt{3})$, que é o corpo de decomposição de $(x^4 - 10x^2 + 21)$.

b) $x^4 + 1$ sobre $\mathbb{Q}$ $\quad x^4 = -1$ $\quad i = \sqrt{-1}$ $\quad x^2 = i$

$x^4 + 1 = (x^2 + \sqrt{-1})(x^2 - \sqrt{-1})$ $\quad x^2 = \sqrt[2]{-1}$ $\quad x^2 + i \Rightarrow x^2 = -i$ $\quad x = \sqrt{i}$

$= (x^2 + i)(x^2 - i)$ $\quad x = \sqrt{-i}$

$= (x + \sqrt{-i})(x - \sqrt{-i})(x + \sqrt{i})(x - \sqrt{i})$

Temos que todas as raízes vivem em $\mathbb{Q}(\sqrt{i}, \sqrt{-i})$, que é corpo de decomposição de (x^4+1).

c) $x^3 + 2x + 2$ sobre $\mathbb{Z}_3$. $\quad x^3 + 2x + 2 = 0$ $\quad x(x^2+2) + 2 = 0 \rightarrow x(x^2+2) = 2$ $\quad x^2 = -2$

$\mathbb{Z}_3 = \{0, 1, 2\}$ $\quad x = \sqrt{-2} = i\sqrt{2}$

$x \cdot i\sqrt{2} = 2$

$x = \frac{2}{i\sqrt{2}} \cdot \frac{i\sqrt{2}}{i\sqrt{2}} = \frac{2i\sqrt{2}}{-2}$

$x = -i\sqrt{2}$

$$\begin{array}{l|l} x^3 + 2x + 2 & x \\ \hline -x^3 & x^2 + 2 \\ \quad -2x & \\ \quad 2 & \end{array}$$

$$\begin{array}{l|l} x^3 + 2x + 2 & x+1 \\ \hline -x^3 - x^2 & x^2 - x + 3 \\ -x^2 + 2x & \\ +x^2 + x & \\ \quad 3x + 2 & \\ \quad -3x \quad -3/_{\ldots} & \end{array}$$

$$\begin{array}{l|l} x^3 + 2x + 2 & x+2 \\ \hline -x^3 - 2x^2 \cancel{+2x} & x^2 - 2x + 6 \\ +2x + 4x & \\ \quad 6x + 2 & \\ \quad -6x - 12 & \\ \quad\quad -10 & \end{array}$$

Dado o polinômio $f(x) = x^3 + 2x + 2 = (x+1)(x^2 - x + 3) - 1$, então a decomposição no corpo $F(x)$ deixa resto.

d) $x^3 - 3$ sobre $\mathbb{Q}$. $\quad x = \sqrt[3]{3} \rightarrow \mathbb{Q}(\sqrt[3]{3})$. Mas não é corpo de decomposição de $p(x)$, pois as outras raízes são complexas e não existem em $\mathbb{Q}(\sqrt[3]{3})$.

16) Temos F sendo um corpo de características p. Prove que $p(x) = x^p - a$ é irredutível em F ou na decomposição de F.

Vamos primeiro supor que o polinômio $p(x) = x^p - a$ é irredutível sobre F, neste caso está concluído. Agora vamos assumir que $p(x)$ não é irredutível, assim existe pelo menos uma raíz β do polinômio $p(x)$ no corpo F.

Dado β sendo uma raíz do polinômio $p(x)$, então $\beta^p = a$, o que implica que $p(x) = x^p - \beta^p$ e o corpo F é um corpo de característica de p.

$$(x-\beta)^p = \sum_{k=0}^{p} (C_k^p) x^{p-k} (\beta)^k = (C_0^p) x^p (\beta)^0 + \ldots + (C_p^p) x^{p-p} (\beta)^p =$$

$$x^p - \beta^p \; (C_0^p = C_p^p = 1)$$

Temos, agora todos os termos da expansão exceto o primeiro e o último termos de p como:

$$C_k^p = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\ldots(p-(k-1))}{k!}$$

Então $C_0^p = 1 = C_p^p$, assim todos os termos serão cancelados exceto o primeiro e o último porque eles contém os fatores de p. Então $p(x)$ pode ser escrito como $p(x) = (x-\beta)^p$, assim temos que F é um corpo de fatoração de $p(x)$.

Então $x^p - a$ pode ser escrito como $(x-\beta)^p$, onde β é uma raíz de $p(x)$.

---

18) Se todo polinômio irredutível $p(x)$ em $F[x]$ é linear, mostre que F é um corpo algebricamente fechado.

O conjunto $\{\alpha \in E \mid \alpha$ é algébrico sobre $F\}$ é o fecho algébrico de E sobre F, se $f(\alpha) = 0$ para $f(x) \in F[x]$.

Teorema: O fecho algébrico de E sobre F é subcorpo de F.

F é dito algebricamente fechado se todas as raízes de polis em $F[x]$ vivem em F, Nesse caso, se $f(x) \in F[x]$ e $\alpha_1, \ldots, \alpha_n \in F$ são raízes de $f(x)$, então:

$$f(x) = (x-\alpha_1)\ldots(x-\alpha_n) \in F[x]$$

Um polinômio linear, é um polinômio que pode ser escrito como combinação linear de outros polinômios, em geral um polinômio de grau maior ou igual a 2.

Tomamos $p(x)$ sendo um polinômio em $F[x]$, se ele é irredutível então ele não pode ser decomposto ou não pode ser escrito em fatores como combinação linear.
Agora assumimos que $p(x)$ é linear, ou seja, pode ser escrito em fatores de menor grau como combinação linear, logo é redutível.
Então deve existir pelo menos uma raiz, denotamos por α, no corpo F, o que implica que $p(x)$ pode ser escrito como:

$p(x) = (x-\alpha)\, q(x)$, onde $q(x)$ é um polinômio de grau $(n-1)$ em $F[x]$

Novamente se $q(x)$ é irredutível então poderá ser um polinômio linear da forma: $q(x) = a+bx$, o que implica que:

$$p(x) = (x-a)(a+bx)$$

Novamente se $q(x)$ é redutível, então teremos uma raiz "β" no corpo F e $p(x)$ pode ser escrito como:

$p(x) = (x-a)(x-\beta).r(x)$, onde $r(x)$ é um polinômio de grau $n-2$.

Este processo pode se repetir várias vezes até chegarmos em um polinômio irredutível:

$p(x) = (x-\alpha)(\alpha-\beta)(c+dx)$ ou $p(x) = (x-\alpha)(x-\beta)(x-y)\,s(x)$

E podemos parar ou continuar decompondo em fatores para uma combinação linear, isto significa que todo polinômio em $F[x]$ pode ser decomposto em fatores lineares no corpo F.

Assim conclui-se que um corpo F é algebricamente fechado, se e somente se, todo polinômio em $F[x]$ tem fatores completamente linear em F. Então F é um corpo algebricamente fechado.

21) Temos E sendo uma extensão algébrica de um corpo F, e temos σ sendo um automorfismo de E deixando F fixado. Mostre que σ induz uma permutação do conjunto de zeros do polinômio minimal de α que está em E.

Automorfismo: $E \to E$, domínio = contradomínio

Temos que E é uma extensão algébrica de um corpo F, e E é um automorfismo de E e fixando os elementos de F, logo:

$$\sigma: E \to E \quad e \quad F \subset E \to a \in F \quad e \quad \sigma(a) = a$$

Assim σ induz uma permutação no conjunto das raízes que estão em E, assim:

$F \subset E$, $\sigma: E \to E$ e $\sigma(a) = a \ \forall a \in F$

$\alpha \in E \to m_\alpha(x) \in F[x]$ e $grau(m_\alpha) = N \to N$ raízes.

Assim: $r_1, \dots, r_N$ são as raízes de $m_\alpha(x)$ e $S = \{r_1, \dots, r_N\}$

1) $\sigma(r_i) = r_j$ ∴ envia raiz em raiz

$m_\alpha(\sigma(r_i)) = a_0 + a_1(\sigma(r_i)) + a_2(\sigma(r_i))^2 + \dots + a_N(\sigma(r_i))^N$, mas σ é um automorfismo, ou seja, um homomorfismo bijetor

$\sigma(a)^N = \sigma(a^N)$

Então:

$m_\alpha(\sigma(r_i)) = a_0 + a_1(\sigma(r_i)) + a_2(\sigma(r_i))^2 + \dots + a_N(\sigma(r_i))^N = a_0 + a_1(\sigma(r_i)) + a_2(\sigma(r_i^2)) + \dots + a_N(\sigma(r_i^N))$,

Mas os $a_i \in F$, então:

$$\begin{aligned} m_\alpha(\sigma(r_i)) &= \sigma(a_0) + \sigma(a_1)\sigma(r_i) + \sigma(a_2)\sigma(r_i^2) + \dots + \sigma(a_N)\sigma(r_i^N) \\ &= \sigma(a_0 + a_1 r_i + a_2 r_i^2 + \dots + a_N r_i^N) \\ &= \sigma(m_\alpha(r_i)) = \sigma(0) = 0 \end{aligned}$$

Então σ leva raiz em raiz e $\sigma: S \to S$.

Como é um automorfismo, σ é uma bijeção. Assim é uma permutação de S.