

Soluções de exercícios seleccionados

Capítulo 1

1.9. *Seja D um domínio de integridade. Mostre que:*

- (a) *Para cada $d \in D - \{0\}$, a aplicação $\phi_d : D \rightarrow D$, definida por $\phi_d(x) = dx$, é injectiva.*
- (b) *Se D é finito, então D é um corpo.*

(a) Se $d \in D - \{0\}$, então para quaisquer $x, y \in D$,

$$dx = dy \Leftrightarrow dx - dy = 0 \Leftrightarrow d(x - y) = 0 \Rightarrow x - y = 0 \Leftrightarrow x = y,$$

o que mostra que ϕ_d é injectiva.

- (b) Se D é finito então, para cada $d \in D - \{0\}$, sendo injectiva, ϕ_d é imediatamente bijectiva. Portanto, existe $c \in D$ tal que $\phi_d(c) = 1$, isto é, $dc = 1$. Isto significa que qualquer $d \in D - \{0\}$ é invertível, e D é um corpo.

1.24. *Seja $(A, +, \cdot)$ um anel comutativo. Considere o conjunto*

$$\mathcal{N}(A) = \{a \in A \mid \exists n \in \mathbb{N}, a^n = 0\}.$$

(a) *Calcule $\mathcal{N}(\mathbb{Z})$ e $\mathcal{N}(\mathbb{Z}_{32})$.*

(b) *Mostre que:*

- (i) $\mathcal{N}(A)$ é um ideal de A .
- (ii) Para qualquer ideal primo I de A , $\mathcal{N}(A) \subseteq I$.
- (iii) $\mathcal{N}(A/\mathcal{N}(A)) = \{\mathcal{N}(A)\}$.

(a) $\mathcal{N}(\mathbb{Z}) = \{a \in \mathbb{Z} \mid \exists n \in \mathbb{N}, a^n = 0\} = \{0\}$.

$$\begin{aligned}\mathcal{N}(\mathbb{Z}_{32}) &= \{a \in \mathbb{Z}_{32} \mid \exists n \in \mathbb{N}, a^n = 0\} \\ &= \{a \in \mathbb{Z}_{32} \mid \exists n \in \mathbb{N}, 32 \text{ divide } a^n\}.\end{aligned}$$

Ora

$$32|a^n \Rightarrow a^n \text{ é par} \Rightarrow a \text{ é par} \Rightarrow a \text{ é par}.$$

Reciprocamente,

$$a \text{ é par } \Rightarrow 2|a \Rightarrow 2^5|a^5 \Rightarrow 32|a^5.$$

Portanto,

$$\begin{aligned} \mathcal{N}(\mathbb{Z}_{32}) &= \{a \in \mathbb{Z}_{32} \mid a \text{ é par}\} \\ &= \{0, 2, 4, 6, \dots, 30\}. \end{aligned}$$

(b)(i) $0^1 = 0$ pelo que $0 \in \mathcal{N}(A)$.

Sejam $a \in \mathcal{N}(A)$ e $x \in A$. Então $a^n = 0$ para algum $n \in \mathbb{N}$ e, consequentemente, $(ax)^n = a^n x^n = 0$, o que mostra que $ax \in \mathcal{N}(A)$.

Finalmente, sejam $a, b \in \mathcal{N}(A)$. Então $a^n = 0 = b^m$ para alguns naturais n e m . Pretendemos provar que $a - b \in \mathcal{N}(A)$. O caso $a = 0$ ou $b = 0$ é óbvio. Suponhamos então $a, b \neq 0$ (donde $n, m > 1$). Pela fórmula do binómio de Newton (que provámos ser verdadeira num anel comutativo qualquer),

$$\begin{aligned} (a - b)^{nm} &= \sum_{k=0}^{nm} \binom{nm}{k} a^k (-b)^{nm-k} \\ &= a^0 b^{nm} + \binom{nm}{1} a b^{nm-1} + \binom{nm}{2} a^2 b^{nm-2} + \dots + \binom{nm}{n-1} a^{n-1} b^{nm-n+1} + \\ &\quad + \binom{nm}{n} a^n b^{nm-n} + \dots + \binom{nm}{nm-1} a^{nm-1} b + a^{nm} b^0. \end{aligned}$$

Neste último somatório, as parcelas da linha de cima são todas nulas porque o expoente em b é sempre $\geq m$ (note que $nm - n + 1 = n(m - 1) + 1$ é $\geq m$ pois $n(m - 1) \geq m - 1$ uma vez que $m - 1 > 0$ e $n > 1$); na linha de baixo são também todas nulas porque o expoente em a é sempre $\geq n$.

Portanto, $(a - b)^{nm} = 0$, o que mostra que $a - b \in \mathcal{N}(A)$.

(ii) Seja I um ideal primo de A . Para cada $a \in \mathcal{N}(A)$, existe $n \in \mathbb{N}$ tal que $a^n = 0 \in I$. Como I é primo, então $a \in I$.

(iii) $A/\mathcal{N}(A) = \{a + \mathcal{N}(A) \mid a \in A\}$ pelo que

$$\begin{aligned} a + \mathcal{N}(A) \in \mathcal{N}(A/\mathcal{N}(A)) &\Leftrightarrow \exists n \in \mathbb{N} : (a + \mathcal{N}(A))^n = \mathcal{N}(A) \\ &\Leftrightarrow \exists n \in \mathbb{N} : a^n + \mathcal{N}(A) = \mathcal{N}(A) \\ &\Leftrightarrow \exists n \in \mathbb{N} : a^n \in \mathcal{N}(A) \\ &\Leftrightarrow \exists n \in \mathbb{N}, \exists m \in \mathbb{N} : (a^n)^m = 0 \\ &\Leftrightarrow \exists n, m \in \mathbb{N} : a^{nm} = 0 \\ &\Leftrightarrow a \in \mathcal{N}(A) \\ &\Leftrightarrow a + \mathcal{N}(A) = \mathcal{N}(A). \end{aligned}$$

Portanto $\mathcal{N}(A/\mathcal{N}(A)) = \{\mathcal{N}(A)\}$.

1.25. Prove que se A é um anel, I e J são ideais de A e P é um ideal primo de A , então

$$IJ \subseteq P \Rightarrow I \subseteq P \text{ ou } J \subseteq P.$$

Suponhamos que $IJ \subseteq P$ e $I \not\subseteq P$. Então existe $a \in I$ tal que $a \notin P$. Mas, para qualquer $b \in J$, $ab \in IJ \subseteq P$, o que implica, pela primalidade de P , que $a \in P$ ou $b \in P$. Como $a \notin P$, teremos que ter forçosamente $b \in P$, o que mostra que $J \subseteq P$.

1.32. Seja $A = (\mathbb{Q}, +, *)$, onde $+$ denota a adição usual de racionais e $*$ é definida por $a * b = 2ab$.

- (a) Mostre que A é um anel comutativo com identidade.
- (b) Determine um subanel de A que seja isomorfo ao anel usual $(\mathbb{Z}, +, \times)$ dos inteiros, descrevendo o isomorfismo (e justificando que se trata de facto de um isomorfismo).

(a) Uma vez que $+$ é a adição usual, o par $(\mathbb{Q}, +)$ é um grupo comutativo. Bastará então verificar que a operação $*$ é associativa, distributiva relativamente à adição e tem elemento neutro:

Associatividade: Para quaisquer $a, b, c \in \mathbb{Q}$ temos $a * (b * c) = a * (2bc) = 2a2bc = 4abc$ enquanto $(a * b) * c = (2ab) * c = 4abc$, pelo que se confirma a propriedade.

Distributividade: Como $*$ é comutativa basta verificar uma das condições de distributividade: para quaisquer $a, b, c \in \mathbb{Q}$, $a * (b + c) = 2a(b + c) = 2ab + 2ac = (a * b) + (a * c)$.

Elemento neutro: $1/2$ é elemento neutro de $*$ pois, para qualquer $a \in \mathbb{Q}$, $a * (1/2) = a$.

(b) Consideremos $S = \{a/2 : a \in \mathbb{Z}\} \subseteq \mathbb{Q}$, que é claramente um subanel de A : é não vazio e, para quaisquer $x = a/2, y = b/2 \in S$, tem-se $x - y = (a/2) - (b/2) = (a - b)/2 \in S$ e $x * y = 2xy = 2(a/2)(b/2) = ab/2 \in S$.

Também não é difícil ver que $(S, +, *) \cong (\mathbb{Z}, +, \cdot)$:

Como, para cada $x \in S$, $2x \in \mathbb{Z}$, podemos definir a função

$$\begin{aligned} f : (S, +, *) &\rightarrow (\mathbb{Z}, +, \cdot) \\ x &\mapsto 2x. \end{aligned}$$

É um homomorfismo de anéis: para quaisquer $x, y \in S$ tem-se $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$ e $f(x * y) = f(2xy) = 4xy = 2x2y = f(x)f(y)$.

É injectiva: $f(x) = f(y) \Leftrightarrow 2x = 2y \Leftrightarrow x = y$.

É sobrejectiva: para cada $a \in \mathbb{Z}$ seja $x = a/2 \in S$; evidentemente $f(x) = 2(a/2) = a$.

1.33. Seja $A = (\mathbb{Q}, +, *)$, onde $+$ denota a adição usual de racionais e $*$ é definida por $a * b = ab/3$.

(a) Mostre que A é um corpo.

(b) Determine um subanel de A que seja isomorfo ao anel usual $(\mathbb{Z}, +, \cdot)$ dos inteiros, descrevendo o isomorfismo.

(a) Uma vez que $+$ é a adição usual, o par $(\mathbb{Q}, +)$ é um grupo comutativo. Bastará então verificar que a operação $*$ é distributiva relativamente à adição, associativa, comutativa e tem elemento neutro e que todo o elemento diferente do zero tem inverso relativamente a esta operação:

Distributividade: Como $*$ é comutativa basta verificar uma das condições de distributividade: para quaisquer $a, b, c \in \mathbb{Q}$,

$$a * (b + c) = \frac{a(b + c)}{3} = \frac{ab + ac}{3} = \frac{ab}{3} + \frac{ac}{3} = (a * b) + (a * c).$$

Associatividade: Para quaisquer $a, b, c \in \mathbb{Q}$, $a * (b * c) = a * \frac{bc}{3} = \frac{abc}{9}$ enquanto $(a * b) * c = \frac{ab}{3} * c = \frac{abc}{9}$, pelo que se confirma a propriedade.

Comutatividade: Para quaisquer $a, b \in \mathbb{Q}$, $a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$.

Elemento neutro: 3 é elemento neutro de $*$ pois, para qualquer $a \in \mathbb{Q}$, $a * 3 = a$.

Existência de inversos: Para cada $a \neq 0$ em \mathbb{Q} , $\frac{9}{a}$ é o inverso de a pois $a * \frac{9}{a} = 3$.

(b) Consideremos $S = 3\mathbb{Z} \subseteq \mathbb{Q}$, que é claramente um subanel de A : é não vazio e, para quaisquer $x = 3a, y = 3b \in S$, tem-se $x - y = 3a - 3b = 3(a - b) \in S$ e

$$x * y = \frac{xy}{3} = \frac{3a3b}{3} = 3ab \in S.$$

Também não é difícil ver que $(S, +, *) \cong (\mathbb{Z}, +, \cdot)$: a função

$$f: (S, +, *) \rightarrow (\mathbb{Z}, +, \cdot) \\ x \mapsto \frac{x}{3}$$

é um homomorfismo de anéis: para quaisquer $x, y \in S$ tem-se

$$f(x + y) = \frac{x + y}{3} = \frac{x}{3} + \frac{y}{3} = f(x) + f(y) \quad \text{e} \quad f(x * y) = f\left(\frac{xy}{3}\right) = \frac{xy}{9} = f(x)f(y).$$

Além disso, é injectiva, pois

$$f(x) = f(y) \Leftrightarrow \frac{x}{3} = \frac{y}{3} \Leftrightarrow x = y,$$

e é sobrejectiva, pois para cada $a \in \mathbb{Z}$, tomando $x = 3a \in S$, tem-se evidentemente $f(x) = \frac{3a}{3} = a$.

1.35. *Seja D um domínio de integridade e considere no conjunto $S = D \times (D \setminus \{0\})$ a relação*

$$(a, b) \sim (c, d) \equiv ad = bc.$$

- (a) *Mostre que \sim é uma relação de equivalência em S .*
- (b) *Denote a classe de equivalência $\{(c, d) \in S \mid (c, d) \sim (a, b)\}$ por a/b (ou $\frac{a}{b}$) e o conjunto de todas as classes de equivalência $\{a/b \mid (a, b) \in S\}$ por K . Prove que*

$$a/b + c/d = (ad + bc)/bd \quad e \quad a/b \cdot c/d = ac/bd$$

definem operações em K que lhe dão uma estrutura de corpo (o chamado corpo das fracções ou quocientes de D).

- (c) *No caso $D = \mathbb{Z}$ que corpo é K ?*
- (d) *Mostre que $D' = \{a/1 \mid a \in D\}$ é um subanel de K isomorfo a D e que para cada $x \in K$ existem $a, b \in D'$ com $b \neq 0$ tais que $x = ab^{-1}$.*
- (e) *Seja D' um domínio de integridade contido num corpo L e*

$$K' = \{a'(b')^{-1} \mid a', b' \in D', b' \neq 0\}.$$

Prove que K' é o menor subcorpo de L que contém D' e qualquer isomorfismo de D em D' tem uma extensão única a um isomorfismo de K em K' .

- (f) *Conclua que o corpo dos quocientes K de um domínio de integridade D é o menor corpo (a menos de isomorfismo) contendo D (no sentido de que não existe nenhum corpo L tal que $D \subset L \subset K$).*

- (a) *As propriedades reflexiva e simétrica são imediatas. Suponhamos $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Então $ad = bc$ e $cf = de$. Isto implica $adf = bcf$ e $bcf = bde$ e portanto $adf = bde$. Cancelando d obtemos $af = be$, isto é, $(a, b) \sim (e, f)$. Assim, \sim é transitiva.*

- (b) A operação $+$ está bem definida: sejam $a/b, c/d, a'/b', c'/d' \in K$ e suponhamos $a/b = a'/b'$ e $c/d = c'/d'$. Então $ab' = ba'$ e $cd' = dc'$, pelo que $ab'dd' = ba'dd'$ e $cd'bb' = dc'bb'$. Portanto $ab'dd' + cd'bb' = ba'dd' + dc'bb'$ e conseqüentemente $(ad + bc)b'd' = bd(a'd' + b'c')$. Isto significa que

$$(ad + bc, bd) \sim (a'd' + b'c', b'd')$$

donde $(ad + bc)/bd = (a'd' + b'c')/b'd'$.

Uma prova análoga mostra que \cdot também está bem definida.

As propriedades associativa, comutativa e distributiva são simples de verificar. O elemento neutro de $+$ é $0/b$ e o elemento neutro de \cdot é b/b (onde $b \neq 0$). Para cada $a/b \in K$, o respectivo simétrico é a fracção $(-a)/b = a/(-b)$ e o inverso, quando $a/b \neq 0$ (isto é, $a \neq 0$), é a fracção b/a . Portanto, K é um corpo.

- (c) É evidente que o caso $D = \mathbb{Z}$ nos dá $K = \mathbb{Q}$. Assim, a construção de K a partir de D é uma generalização da construção clássica dos racionais como fracções de inteiros.
- (d) O facto de que D' é um subanel de K é evidente: $0 = 0/1 \in D'$ e para quaisquer $a/1, b/1 \in D'$, $a/1 - b/1 = (a - b)/1 \in D'$ e $a/1 \cdot b/1 = ab/1 \in D'$. Definindo $f : D \rightarrow D'$ por $f(a) = a/1$ para qualquer $a \in D$, temos

$$f(a + b) = (a + b)/1 = (a \cdot 1 + b \cdot 1)/1 \cdot 1 = a/1 + b/1 = f(a) + f(b)$$

e

$$f(ab) = ab/1 = a/1 \cdot b/1 = f(a) \cdot f(b).$$

Da definição de f , f é claramente sobrejectiva. Quanto à injectividade, basta observar que

$$a = b \Leftrightarrow a \cdot 1 = 1 \cdot b \Leftrightarrow a/1 = b/1 \Leftrightarrow f(a) = f(b).$$

Portanto, f é um isomorfismo de D em $D' \subseteq K$. O resto é óbvio: para cada $x = a/b \in K$, $b \neq 0$ (pelo que $b/1 \neq 0$) e

$$a/b = a/1 \cdot 1/b = a/1 \cdot (b/1)^{-1}.$$

- (e) É fácil verificar que K' é um subcorpo de L . É óbvio que se trata então do menor subcorpo de L que contém D' . Seja f um isomorfismo de D em D' e $a/b \in K$. Consideremos a função $g : K \rightarrow K'$ definida por $g(a/b) =$

$f(a)f(b)^{-1}$. Identificando o domínio D com o conjunto $\{a/1 \mid a \in D\}$, é claro que $f = g|_D$. Além disso,

$$\begin{aligned} a/b = c/d &\Leftrightarrow ad = bc \Leftrightarrow f(ad) = f(bc) \Leftrightarrow f(a)f(d) = f(b)f(c) \Leftrightarrow \\ &\Leftrightarrow f(a)f(b)^{-1} = f(c)f(d)^{-1} \Leftrightarrow g(a/b) = g(c/d). \end{aligned}$$

Portanto, g é injectiva. Da definição de g , segue também que g é sobrejectiva. Além disso,

$$\begin{aligned} g(a/b + c/d) &= g((ad + bc)/bd) \\ &= f(ad + bc)(f(bd))^{-1} \\ &= [f(a)f(d) + f(b)f(c)][f(b)^{-1}f(d)^{-1}] \\ &= f(a)f(b)^{-1} + f(c)f(d)^{-1} \\ &= g(a/b) + g(c/d) \end{aligned}$$

e

$$\begin{aligned} g(a/b \cdot c/d) &= g(ac/bd) \\ &= f(ac)(f(bd))^{-1} \\ &= [f(a)f(c)][f(b)^{-1}f(d)^{-1}] \\ &= f(a)f(b)^{-1}f(c)f(d)^{-1} \\ &= g(a/b)g(c/d) \end{aligned}$$

para quaisquer $a/b, c/d \in K$. Logo, g é um isomorfismo.

Seja g' outro isomorfismo de K em K' tal que $f = g'|_D$. Então, para qualquer $a/b \in K$,

$$\begin{aligned} g'(a/b) &= g'(a/1 \cdot (b/1)^{-1}) \\ &= g'(a/1)g'((b/1)^{-1}) \\ &= g'(a/1)g'(b/1)^{-1} \\ &= f(a)f(b)^{-1} \\ &= g(a/b). \end{aligned}$$

(f) A conclusão é imediata da alínea anterior.

Capítulo 2

2.8. Mostre que se $1+i$ é raiz de $p(x) \in \mathbb{R}[x]$, então $p(x)$ é divisível por $x^2 - 2x + 2$ em $\mathbb{R}[x]$.

Se $1 + i$ é raiz de $p(x)$, então o seu conjugado $1 - i$ também o é. Logo $p(x)$ é divisível por $(x - (1 + i))(x - (1 - i)) = x^2 - 2x + 2$.

2.9. *Seja K um corpo. Mostre que se $\varphi : K[x] \rightarrow K[x]$ é um isomorfismo tal que $\varphi(a) = a$ para qualquer $a \in K$, então $\varphi(x) = cx + d$ para algum par $c, d \in K$.*

Pelo algoritmo da divisão em $K[x]$, $\varphi(x) = q(x)x + d$ para algum $q(x) \in K[x]$ e algum $d \in K$. Como φ é sobrejectiva, existem $q_1(x)$ e $p(x)$ em $K[x]$ tais que $\varphi(q_1(x)) = q(x)$ e $\varphi(p(x)) = x$. Portanto,

$$\varphi(x) = \varphi(q_1(x))\varphi(p(x)) + \varphi(d) = \varphi(q_1(x)p(x) + d).$$

Agora, pela injectividade de φ , podemos concluir que $x = q_1(x)p(x) + d$, o que implica que $gr(q_1(x)p(x)) = 1$. Consequentemente, ou $gr(q_1(x)) = 1$ e $gr(p(x)) = 0$, ou $gr(q_1(x)) = 0$ e $gr(p(x)) = 1$. Suponhamos que acontece o primeiro caso. Então $p(x) = a \in K$, o que implica $x = \varphi(p(x)) = \varphi(a) = a$, uma contradição. Logo, ocorre necessariamente o segundo caso: $q_1(x) = c \in K$ e

$$\varphi(x) = \varphi(q_1(x)p(x) + d) = \varphi(cp(x) + d) = cx + d.$$

2.17. *Indique, justificando, quais dos seguintes polinómios são irredutíveis sobre \mathbb{Q} :*

$$p(x) = 5x^5 - 10x^3 + 6x^2 - 2x + 6, \quad q(x) = x^4 - x^2 - 2, \quad r(x) = 4x^3 - 3x - \frac{1}{2}.$$

$p(x)$, pelo critério de Eisenstein (com $p = 2$), é irredutível sobre \mathbb{Q} .

As possíveis raízes racionais de $q(x) = x^4 - x^2 - 2$ são $1, -1, 2$ e -2 . Nenhuma delas é raiz pelo que o polinómio não tem raízes racionais. Assim, a única hipótese dele ser redutível sobre \mathbb{Q} é factorizar-se na forma

$$q(x) = (x^2 + ax + b)(x^2 + cx + d)$$

para alguns racionais a, b, c, d . Resolvendo o sistema correspondente

$$\begin{cases} a + c = 0 \\ b + ac + d = -1 \\ ad + bc = 0 \\ bd = -2. \end{cases}$$

chega-se a uma solução:

$$q(x) = (x^2 + 1)(x^2 - 2).$$

Portanto, $q(x)$ é redutível sobre \mathbb{Q} .

$r(x)$ é irredutível sobre \mathbb{Q} se e só se $8x^3 - 6x - 1$ o for. As possíveis raízes racionais deste último polinómio são: $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$. Nenhuma delas é de facto uma raiz pelo que o polinómio, não tendo raízes em \mathbb{Q} e sendo de grau 3, é irredutível sobre \mathbb{Q} .

2.18. *Determine a factorização do polinómio $q(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ em factores irredutíveis.*

Sabemos já (pelo exercício anterior) que $q(x)$ não tem raízes racionais e $q(x) = (x^2 + 1)(x^2 - 2)$. Portanto, esta é a factorização de $q(x)$ em factores irredutíveis.

2.22.

(a) *Calcule o produto $(2x^2 + x + 1)(2x^2 + 3x + 2)$ em $\mathbb{Z}_m[x]$, para $m = 2, 3, 6$.*

(b) *$x^4 + 2x^3 + 2x + 2$ é irredutível em $\mathbb{Z}_3[x]$?*

(a)

$$\begin{aligned} (2x^2 + x + 1)(2x^2 + 3x + 2) &= 4x^4 + 6x^3 + 4x^2 + 2x^3 + 3x^2 + 2x + 2x^2 + 3x + 2 \\ &= 4x^4 + 8x^3 + 9x^2 + 5x + 2 \\ &= \begin{cases} x^2 + x & \text{se } m = 2 \\ x^4 + 2x^3 + 2x + 2 & \text{se } m = 3 \\ 4x^4 + 2x^3 + 3x^2 + 5x + 2 & \text{se } m = 6. \end{cases} \end{aligned}$$

(b) Não: pela alínea anterior, $x^4 + 2x^3 + 2x + 2 = (2x^2 + x + 1)(2x^2 + 3x + 2)$, e nenhum destes factores, sendo de grau 2, é uma unidade de $\mathbb{Z}_3[x]$.

2.23. *Seja K um corpo. Mostre que se $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ é irredutível em $K[x]$, também $a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ o é.*

Dado $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$, denotemos por $\overline{p(x)}$ o polinómio $a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$. Basta verificar que se $p(x) = q(x)r(x)$ então $\overline{p(x)} = \overline{q(x)} \overline{r(x)}$.

2.24. (b) *Conclua que se A é um corpo, então $p(x)$ é irredutível em $A[x]$ se e só se $p(x+c)$ o é.*

Se $p(x)$ é redutível então $p(x) = q(x)r(x)$ (onde $q(x)$ e $r(x)$ têm grau ≥ 1). Pela alínea (a), isto implica $p(x+c) = q(x+c)r(x+c)$, o que mostra que $p(x+c)$ é redutível (é evidente que os polinómios $q(x+c)$ e $r(x+c)$ continuam a ter grau

≥ 1). Reciprocamente, se $p(x+c) = q(x)r(x)$ então (novamente pela alínea (a)) $p(x) = q(x-c)r(x-c)$, o que mostra que $p(x)$ é redutível.

2.26. Para cada um dos seguintes ideais I de $\mathbb{Z}_2[x]$

(a) $\langle x^3 + x + 1 \rangle$

(b) $\langle x^2 \rangle$

justifique se $\mathbb{Z}_2[x]/I$ é um corpo. Construa as tabelas de $\mathbb{Z}_2[x]/\langle x^2 \rangle$.

$\mathbb{Z}_2[x]/I$ é um corpo se e só se o ideal $I = \langle p(x) \rangle$ é maximal, isto é, se e só se $p(x)$ é irredutível sobre \mathbb{Z}_2 .

(a) O polinómio $p(x) = x^3 + x + 1$ tem grau 3 e não tem raízes em \mathbb{Z}_2 logo é irredutível em $\mathbb{Z}_2[x]$ (de facto, $p(0) = p(1) = 1$). Portanto, o ideal $\langle x^3 + x + 1 \rangle$ é maximal em $\mathbb{Z}_2[x]$ e $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ é um corpo.

(b) O polinómio $p(x) = x^2$ tem uma raiz em \mathbb{Z}_2 ($p(0) = 0$) logo é redutível em $\mathbb{Z}_2[x]$. Portanto, o ideal $\langle x^2 \rangle$ não é maximal em $\mathbb{Z}_2[x]$ pelo que $\mathbb{Z}_2[x]/\langle x^2 \rangle$ não é um corpo.

Denotando o elemento $p(x) + \langle x^2 \rangle$ de $\mathbb{Z}_2[x]/\langle x^2 \rangle$ por $\overline{p(x)}$ tem-se

$$\begin{aligned} \mathbb{Z}_2[x]/\langle x^2 \rangle &= \{\overline{p(x)} : p(x) \in \mathbb{Z}_2[x]\} \\ &= \{\overline{a_0 + a_1x} : a_0, a_1 \in \mathbb{Z}_2\} \end{aligned}$$

pois para cada $p(x) = x^2q(x) + r(x)$, $\overline{p(x)} = \overline{r(x)}$ (onde $gr(r(x)) \leq 2$). Portanto $\mathbb{Z}_2[x]/\langle x^2 \rangle = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$, com tabelas

$+$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$	\times	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	\overline{x}	$\overline{1}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$
\overline{x}	\overline{x}	$\overline{x+1}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{0}$	\overline{x}	$\overline{0}$	\overline{x}
$\overline{x+1}$	$\overline{x+1}$	\overline{x}	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	\overline{x}	$\overline{1}$

2.27. (b) Determine $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ e escreva as respectivas tabelas de anel.

Por definição, $\mathbb{Z}_2[x]/I = \{f(x) + I \mid f(x) \in \mathbb{Z}_2[x]\}$. Mas, dividindo $f(x)$ por $x^2 + x + 1$, obtemos $f(x) = (x^2 + x + 1)q(x) + r(x)$ onde $gr(r(x)) \leq 1$. É claro que então $f(x) + I = r(x) + I$. Portanto

$$\begin{aligned} \mathbb{Z}_2[x]/I &= \{r(x) + I \mid r(x) \in \mathbb{Z}_2[x], gr(r(x)) \leq 1\} \\ &= \{0 + I, 1 + I, x + I, 1 + x + I\} \end{aligned}$$

é constituído pelas classes definidas pelos restos da divisão dos polinómios de coeficientes em $\mathbb{Z}_2[x]$ por $x^2 + x + 1$.

Denotando $0 + I$ por 0 , $1 + I$ por 1 , $x + I$ por α e $1 + x + I$ por β , as tabelas das operações de L são as seguintes:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

\times	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Por exemplo,

$$\alpha + \beta = (x + I) + (1 + x + I) = 1 + I = 1$$

e

$$\alpha\beta = x(1 + x) + I = x + x^2 + I = 1 + I = 1.$$

2.28. Considere o polinómio $p(x) = x^3 + 2x^2 + 1 \in \mathbb{Z}_5[x]$.

- (a) Mostre que $K = \mathbb{Z}_5[x]/\langle p(x) \rangle$ é um corpo e descreva os seus elementos.
- (b) Determine o cardinal de K e a sua característica.

(a) O polinómio $p(x) = x^3 + 2x^2 + 1$ tem grau 3 e não tem raízes em \mathbb{Z}_5 logo é irredutível em $\mathbb{Z}_5[x]$ (de facto, $p(0) = 1$, $p(1) = 4$, $p(2) = 2$, $p(3) = 1$ e $p(4) = 2$). Portanto, o ideal $\langle p(x) \rangle$ é maximal em $\mathbb{Z}_5[x]$ e $K = \mathbb{Z}_5[x]/\langle p(x) \rangle$ é um corpo. Tem-se

$$\begin{aligned} K &= \{a_0 + a_1x + a_2x^2 + \langle p(x) \rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_5\} \\ &\cong \{a_0 + a_1\theta + a_2\theta^2 \mid a_0, a_1, a_2 \in \mathbb{Z}_5\} \end{aligned}$$

com $\theta^3 = -2\theta^2 - 1 = 3\theta^2 + 4$.

(b) Cada elemento de K admite uma única expressão $a_0 + a_1\theta + a_2\theta^2$, com $a_0, a_1, a_2 \in \mathbb{Z}_5$, pelo que $|K| = 5^3 = 125$. Como $\mathbb{Z}_5 \subseteq K$ e a característica de \mathbb{Z}_5 é 5, obtemos $car(K) = 5$.

2.33. Seja p um inteiro primo. Prove que o polinómio ciclotómico

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$$

é irredutível em $\mathbb{Q}[x]$.

Pelo Exercício 2.24, um polinómio $p(x)$ é irredutível se e só se $p(x+c)$ é irredutível (onde c é uma constante). Em particular, $\Phi_p(x)$ é irredutível se e só se

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$

é irredutível. Este último polinómio é igual a

$$x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{2}x + p.$$

Quando p é primo, observámos na demonstração da Proposição 1.5 que p divide $\binom{p}{i}$ (para $1 \leq i \leq p-1$). Basta agora aplicar o critério de Eisenstein.

Nota: Se n não é primo, então $\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$ factoriza-se em $\mathbb{Q}[x]$. Por exemplo,

$$x^3 + x^2 + x + 1 = (x+1)(x^2 + 1).$$

Capítulo 3

3.5. (d) Determine o inverso de $\theta^2 - 6\theta + 8$ na extensão simples $\mathbb{Q}(\theta)$, onde $\theta \neq 0$ é tal que $\theta^4 - 6\theta^3 + 9\theta^2 + 3\theta = 0$.

O polinómio $x^4 - 6x^3 + 9x^2 + 3x = x(x^3 - 6x^2 + 9x + 3)$, do qual θ é raiz, é redutível sobre \mathbb{Q} . Como $\theta \neq 0$, então θ é raiz do factor $x^3 - 6x^2 + 9x + 3$. Este polinómio é irredutível sobre \mathbb{Q} (pelo critério de Eisenstein, $p = 3$), logo é o polinómio mínimo $m(x)$ de θ sobre \mathbb{Q} . Seja $f(x) = x^2 - 6x + 8$. Uma vez que $m(x) = xf(x) + x + 3$ e $f(x) = (x-9)(x+3) + 35$ (o que confirma que $\text{mdc}(m(x), f(x)) = 1$), então

$$35 = f(x) - (x-9)(m(x) - xf(x)) = (x^2 - 9x + 1)f(x) - (x-9)m(x),$$

ou seja,

$$1 = \frac{1}{35}[(x^2 - 9x + 1)f(x) - (x-9)m(x)].$$

Substituindo x por θ obtemos $1 = \frac{1}{35}(\theta^2 - 9\theta + 1)f(\theta)$, o que mostra que

$$(\theta^2 - 6\theta + 8)^{-1} = f(\theta)^{-1} = \frac{1}{35}(\theta^2 - 9\theta + 1).$$

3.8. Seja L uma extensão dum corpo K e $\theta \in L$ um elemento algébrico de grau n sobre K . Prove que todo o elemento de $K(\theta)$ se pode exprimir de modo único na forma $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ com $a_i \in K$ ($i = 0, \dots, n-1$).

Como θ é algébrico sobre K , $K(\theta) = K[\theta] = \{f(\theta) \mid f(x) \in K[x]\}$, como vimos nas aulas. Seja $m(x)$ o polinómio mínimo de θ sobre K . Para cada elemento $f(\theta) \in K[\theta]$, consideremos o polinómio $f(x)$ a ele associado. Dividindo $f(x)$ por $m(x)$ obtemos $f(x) = q(x)m(x) + r(x)$, onde $\text{gr}(r(x)) < n$. Então

$$f(\theta) = q(\theta)m(\theta) + r(\theta) = r(\theta)$$

e $r(\theta)$ é da forma $a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$ com $a_i \in K$ ($i = 0, \dots, n-1$). A unicidade desta representação é também simples de provar:

Se $f(\theta) = r_1(\theta) = r_2(\theta)$, então $r_1(\theta) - r_2(\theta) = 0$. Consideremos o polinómio $h(x) = r_1(x) - r_2(x)$, que tem grau inferior a n e admite θ por raiz. Como o polinómio mínimo de θ sobre K tem grau n , superior ao de $h(x)$, este tem que ser igual a zero, donde $r_1(x) = r_2(x)$.

3.10. (b) *Determine o polinómio mínimo sobre \mathbb{Q} de $\sqrt{3} + \sqrt{5}$.*

Seja $\theta = \sqrt{3} + \sqrt{5} \in \mathbb{R}$. Como $\theta^2 = 8 + 2\sqrt{15}$ então $(\theta^2 - 8)^2 = 60$. Assim $\theta^4 - 16\theta^2 + 4 = 0$ pelo que θ é raiz de $x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. Este polinómio é irredutível em $\mathbb{Q}[x]$ e é assim o polinómio mínimo de θ sobre \mathbb{Q} . De facto:

- Não tem raízes racionais: as únicas possibilidades são $\pm 1, \pm 2, \pm 4$, nenhuma o é.
- Portanto, a única possibilidade de ser redutível é factorizar-se na forma

$$x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 + a'x + b').$$

Isto será possível precisamente se o sistema

$$\begin{cases} a + a' = 0 \\ b + aa' + b' = -16 \\ ab' + a'b = 0 \\ bb' = 4 \end{cases}$$

tiver solução em \mathbb{Q} . Resolvendo vem

$$\begin{cases} a' = -a \\ \text{-----} \\ a(b' - b) = 0 \Leftrightarrow a = 0 \vee b' = b \\ \text{-----} \end{cases}$$

O caso $a = 0$ implica $b + b' = -16$ e $bb' = 4$, ou seja, $b^2 + 16b + 4 = 0$, que não tem raízes racionais. Por outro lado, o caso $b' = b$ implica $b^2 = 4$, ou seja, $b = 2$ ou $b = -2$. Substituindo na segunda equação obtemos

$$-a^2 + 4 = -16 \Leftrightarrow a^2 = 20 \quad \text{ou} \quad -a^2 - 4 = -16 \Leftrightarrow a^2 = 12,$$

ambas impossíveis em \mathbb{Q} .

Em conclusão, o sistema é impossível.

3.12. *Seja L uma extensão finita de K . Prove que:*

- (a) *Se $[L : K]$ é um número primo, então L é uma extensão simples de K .*
- (b) *Se $\theta \in L$, então o grau de θ é um divisor de $[L : K]$. Conclua que se tem $L = K(\theta)$ se e só se o grau de θ coincidir com $[L : K]$.*
- (c) *Se $f(x) \in K[x]$ é irredutível sobre K e o grau de $f(x)$ é um número primo com $[L : K]$ e maior do que 1, então $f(x)$ não tem raízes em L .*

- (a) Se L é uma extensão finita de K todos os seus elementos são algébricos sobre K . Como $[L : K] = p > 1$, existe $\theta \in L \setminus K$. Pelo Teorema da Torre,

$$p = [L : K] = [L : K(\theta)][K(\theta) : K]. \quad (1)$$

Como $\theta \notin K$, $[K(\theta) : K] > 1$. Mas p é primo, donde só pode ser $[K(\theta) : K] = p$ e $[L : K(\theta)] = 1$. Esta última igualdade diz-nos que $L = K(\theta)$, pelo que L é uma extensão simples de K .

- (b) Como, por definição, o grau de θ coincide com $[K(\theta) : K]$, por (1) este é um divisor de $[L : K]$ e coincide com $[L : K]$ se e só se $[L : K(\theta)] = 1$, ou seja, $L = K(\theta)$.
- (c) Suponhamos, por absurdo, que $f(x)$ tinha uma raiz θ em L . Seja $m(x)$ o polinómio mónico associado a $f(x)$. Evidentemente, trata-se do polinómio mínimo de θ sobre K . Portanto, $[K(\theta) : K] = gr(f(x))$ seria um número primo com $[L : K]$, o que é absurdo por (1). Logo $f(x)$ não tem raízes em L .

3.15. (e) *Determine o grau sobre \mathbb{Q} e uma base da extensão $\mathbb{Q}(\alpha, \beta)$, onde $\alpha^3 - \alpha + 1 = 0$ e $\beta^2 - \beta = 1$.*

Pelo Teorema da Torre,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Como $x^3 - x + 1$ é irredutível sobre \mathbb{Q} (pois não tem raízes racionais), trata-se do polinómio mínimo de α sobre \mathbb{Q} . Assim, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $\{1, \alpha, \alpha^2\}$ é uma base desta extensão simples. Portanto, $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$. Por outro lado, β é raiz do polinómio $f(x) = x^2 - x - 1$. Será que este polinómio é

irredutível sobre $\mathbb{Q}(\alpha)$? Sim, pelo exercício anterior (alínea (c)): $f(x) \in \mathbb{Q}[x]$ é irredutível sobre \mathbb{Q} e o seu grau é um número primo com $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ e maior do que 1, pelo que não tem raízes em $\mathbb{Q}(\alpha)$. Como é de grau 3 será irredutível sobre $\mathbb{Q}(\alpha)$. Assim, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$ e $\{1, \beta\}$ é uma base desta extensão simples. Concluindo, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$ e $\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ é uma base da extensão dupla $\mathbb{Q}(\alpha, \beta)$ de \mathbb{Q} .

3.17. *Sejam $\alpha^3 = 2$, w uma raiz cúbica da unidade e $\beta = w\alpha$. Determine a dimensão e uma base de $\mathbb{Q}(\alpha, \beta)$ sobre \mathbb{Q} .*

Pelo Teorema da Torre,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Como $x^3 - 2$ é irredutível sobre \mathbb{Q} (pelo critério de Eisenstein), trata-se do polinómio mínimo de α sobre \mathbb{Q} . Assim, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $\{1, \alpha, \alpha^2\}$ é uma base desta extensão simples. Portanto,

$$\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}.$$

Por outro lado, β é também raiz do polinómio $f(x) = x^3 - 2$ (pois $\beta^3 = w^3\alpha^3 = 2$). Será que este polinómio é irredutível sobre $\mathbb{Q}(\alpha)$? Mas agora este polinómio já é redutível sobre $\mathbb{Q}(\alpha)$, uma vez que α é uma das suas raízes. Com efeito, $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$. Agora dois casos podem ocorrer, ou β é raiz do primeiro factor, ou é raiz do segundo factor:

Caso 1: $\beta = \alpha$. Neste caso $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ e o problema já está resolvido (a dimensão é 3 e a base é $\{1, \alpha, \alpha^2\}$).

Caso 2: $\beta \neq \alpha$. Neste caso β é raiz de $x^2 + \alpha x + \alpha^2$. Agora, para indagarmos da sua irredutibilidade sobre $\mathbb{Q}(\alpha)$, não podemos utilizar o Exercício 3.12 (c), pois este polinómio não tem coeficientes racionais. Para verificarmos isso não temos outra hipótese senão investigar directamente se tem alguma raiz em $\mathbb{Q}(\alpha)$, ou seja, se existem racionais a, b e c tais que

$$(a + b\alpha + c\alpha^2)^2 + \alpha(a + b\alpha + c\alpha^2) + \alpha^2 = 0.$$

Efectuando os cálculos em $\mathbb{Q}(\alpha)$, esta equação é ainda equivalente a

$$(a^2 + 4bc + 2c) + (2ab + 2c^2 + a)\alpha + (2ac + b^2 + b + 1)\alpha^2 = 0.$$

Como $\{1, \alpha, \alpha^2\}$ é uma base do espaço vectorial $\mathbb{Q}(\alpha)$ (sobre \mathbb{Q}), obtemos

$$\begin{cases} a^2 + 4bc + 2c = 0 \\ 2ab + 2c^2 + a = 0 \\ 2ac + b^2 + b + 1, \end{cases}$$

que é um sistema impossível em \mathbb{Q} :

Se $a, c \neq 0$ então

$$\begin{cases} a^3 + 4abc + 2ac = 0 \\ 4abc + 4c^3 + 2ac = 0 \end{cases}$$

o que implica $a^3 = 4c^3$, ou seja, $a/c = \sqrt[3]{4} \notin \mathbb{Q}$!!!; para $a = 0$ ou $c = 0$ temos $b^2 + b + 1 = 0$, o que é impossível em \mathbb{Q} .

Portanto, $x^2 + \alpha x + \alpha^2$ é o polinómio mínimo de β sobre $\mathbb{Q}(\alpha)$. Concluindo, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$ e $\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ é uma base da extensão $\mathbb{Q}(\alpha, \beta)$ de \mathbb{Q} .

3.18. *Determine para quais dos seguintes polinómios $f(x) \in K[x]$ existem extensões $K(\alpha)$ tais que $f(x)$ é o polinómio mínimo de α :*

$$(a) x^2 - 4, \quad K = \mathbb{Q}. \quad (b) x^3 + x + 2, \quad K = \mathbb{Z}_3. \quad (c) x^2 + 1, \quad K = \mathbb{Z}_5.$$

(a) Como $x^2 - 4$ é redutível sobre \mathbb{Q} (pois tem raízes racionais), não existe nenhuma extensão $\mathbb{Q}(\alpha)$ tal que $x^2 - 4$ é o polinómio mínimo de α .

(b) $x^3 + x + 2$ também é redutível sobre \mathbb{Z}_3 (pois tem raízes neste corpo), logo não existe nenhuma extensão $\mathbb{Z}_3(\alpha)$ tal que $x^3 + x + 2$ é o polinómio mínimo de α .

(c) $x^2 + 1$ também é redutível sobre \mathbb{Z}_5 (pois tem raízes neste corpo), logo não existe nenhuma extensão $\mathbb{Z}_5(\alpha)$ tal que $x^2 + 1$ é o polinómio mínimo de α .

3.19. *Para cada uma das extensões de \mathbb{Q} indicadas averigúe se θ gera a mesma extensão:*

$$(a) \theta = 2 + \sqrt[3]{4}, \quad \mathbb{Q}(\sqrt[3]{2}).$$

$$(b) \theta = \sqrt{2} + \sqrt{3}, \quad \mathbb{Q}(\sqrt{2}).$$

$$(c) \theta = u^2 + u + 1, \quad \mathbb{Q}(u), \text{ com } u^2 + 5u - 5 = 0.$$

(a) $x^3 - 2$ é o polinómio mínimo de $\sqrt[3]{2}$ sobre \mathbb{Q} , logo $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Então $\theta \in \mathbb{Q}(\sqrt[3]{2})$, pelo que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$. Por outro lado, como $\theta - 2 = \sqrt[3]{4}$, então $(\theta - 2)^3 = 4$, ou seja, θ é raiz do polinómio $x^3 - 6x^2 + 12x - 12$. Como este polinómio é irredutível sobre \mathbb{Q} (pelo critério de Eisenstein), é o polinómio mínimo de θ sobre \mathbb{Q} , o que mostra que também $[\mathbb{Q}(\theta) : \mathbb{Q}]$ é igual a 3.

Concluindo, como $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$ e $\dim \mathbb{Q}(\theta) = \dim \mathbb{Q}(\sqrt[3]{2})$, as duas extensões coincidem.

- (b) Neste caso, as extensões são diferentes, pois $\theta \notin \mathbb{Q}(\sqrt{2})$. De facto, $\theta = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2})$ implicaria $\sqrt{2} + \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, ou seja, $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, o que é um absurdo, pois não existem racionais a e b tais que $\sqrt{3} = a + b\sqrt{2}$: $b = 0$ implicaria $\sqrt{3} \in \mathbb{Q}$; $a = 0$ e $b \neq 0$ implicariam $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$ e $a, b \neq 0$ implicariam $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}!!!$
- (c) Claramente $\theta \in \mathbb{Q}(u)$, donde $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(u)$. Por outro lado, $\theta = u^2 + u + 1 = 5 - 5u + u + 1 = 6 - 4u$, ou seja, $u = \frac{6-\theta}{4} \in \mathbb{Q}(\theta)$, o que mostra que também $\mathbb{Q}(\theta) \supseteq \mathbb{Q}(u)$. Portanto as extensões coincidem.

3.21. *É possível, usando régua (não graduada) e compasso, construir o ponto*

$$\left(\sqrt{5\sqrt{2}-3} + \sqrt{2-\sqrt[3]{2}}, 0 \right)$$

a partir dos pontos $(0,0)$ e $(1,0)$?

Sejam $\theta_1 = \sqrt{5\sqrt{2}-3}$ e $\theta_2 = \sqrt{2-\sqrt[3]{2}}$. É fácil de ver que θ_1 é raiz de $p(x) = x^4 + 6x^2 - 41$ e θ_2 é raiz de $q(x) = x^6 - 6x^4 + 12x^2 - 6 = 0$. O polinómio $q(x)$ é claramente irredutível sobre \mathbb{Q} (pelo critério de Eisenstein) pelo que $[\mathbb{Q}(\theta_2) : \mathbb{Q}] = 6$ e θ_2 não é construtível a partir dos pontos $(0,0)$ e $(1,0)$. Quanto ao polinómio $p(x)$, também é irredutível sobre \mathbb{Q} , mas dá mais trabalho a verificar isso:

Não tem raízes racionais (as únicas possibilidades, ± 1 e ± 41 , claramente não o são). Assim, se fosse redutível, a única possibilidade de factorização seria como produto de dois polinómios de grau 2:

$$x^4 + 6x^2 - 41 = (ax^2 + bx + c)(a'x^2 + b'x + c').$$

Desenvolvendo esta igualdade chegaremos a um sistema de equações, impossível em \mathbb{Q} , o que confirma que $p(x)$ é, de facto, irredutível sobre \mathbb{Q} . Portanto, $[\mathbb{Q}(\theta_1) : \mathbb{Q}] = 4$. Como o recíproco do Teorema 3.8 não é verdadeiro (observação feita a seguir à demonstração do Teorema) não podemos para já concluir da construtibilidade de θ_1 a partir dos pontos $(0,0)$ e $(1,0)$. No entanto, o que afirmámos na Observação ao Teorema 3.8 dá-nos a resposta: $\sqrt{5\sqrt{2}-3}$ é construtível pois obtém-se dos números racionais 2, 3 e 5 por sucessivas aplicações das operações de subtracção, multiplicação e raiz quadrada.

Concluindo, $\theta_1 + \theta_2$ não é construtível a partir dos pontos $(0,0)$ e $(1,0)$ (se fosse, como θ_1 é, também $(\theta_1 + \theta_2) - \theta_1 = \theta_2$ seria).

3.22. *Seja p um inteiro primo positivo.*

- (a) *Determine a dimensão e uma base da extensão $\mathbb{Q}(\sqrt{p+\sqrt{p}})$ de \mathbb{Q} .*

(b) Será possível construir o ponto $(\sqrt{p+\sqrt{p}}, \sqrt{p+\sqrt{p}})$ a partir dos pontos $(0,0)$ e $(1,0)$?

(a) Denotemos o número $\sqrt{p+\sqrt{p}}$ por θ . Como $\theta^2 = p+\sqrt{p}$, então $(\theta^2-p)^2 = p$, pelo que θ é raiz do polinómio

$$q(x) = (x^2 - p)^2 - p = x^4 - 2px^2 + p(p-1) \in \mathbb{Q}[x].$$

Pelo critério de Eisenstein, $q(x)$ é irredutível sobre \mathbb{Q} (basta considerar o primo p). Portanto, $q(x)$ é o polinómio mínimo de θ sobre \mathbb{Q} , pelo que $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4$ e $\{1, \theta, \theta^2, \theta^3\}$ é uma base desta extensão.

(b) Sim, pela Observação ao Teorema 3.8 (veja o exercício anterior).

3.24. Considere o polinómio $p(x) = 2x^7 + 12x^5 + 3x^3 + 6x + 6$ em $\mathbb{Q}[x]$.

(a) Prove que $p(x)$ tem uma raiz real α .

(b) Justifique se α é ou não um real construtível a partir dos racionais.

(a) Em $\mathbb{C}[x]$, $p(x)$ decompõe-se em 7 factores lineares (pois \mathbb{C} é um corpo algebricamente fechado) correspondentes às suas 7 raízes em \mathbb{C} . Além disso, como sabemos, as raízes complexas não reais aparecem aos pares. Então, como 7 é ímpar, uma das 7 raízes é necessariamente real.

(b) O polinómio $p(x)$ é irredutível sobre $\mathbb{Q}[x]$ (pelo critério de Eisenstein, $p = 3$). Então o polinómio mínimo de α sobre \mathbb{Q} é o polinómio mónico associado de $p(x)$, ou seja, o polinómio $x^7 + 6x^5 + \frac{3}{2}x^3 + 3x + 3$. Assim $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$. Como este número não é uma potência de 2, pelo critério algébrico estudado sobre a construtibilidade (por régua e compasso) de números, podemos concluir que α não é construtível a partir dos racionais.

3.25. Mostre que $x^2 + 1$ é irredutível sobre \mathbb{Z}_3 . Sendo u uma raiz deste polinómio determine o número de elementos de $\mathbb{Z}_3(u)$ e as tabelas de adição e multiplicação.

Para mostrar a irredutibilidade basta verificar que nenhum elemento de \mathbb{Z}_3 é raiz de $x^2 + 1$.

Pelo que vimos na página 69,

$$\mathbb{Z}_3(u) \cong \frac{\mathbb{Z}_3[x]}{\langle x^2 + 1 \rangle} = \{a_0 + a_1x + \langle x^2 + 1 \rangle \mid a_0, a_1 \in \mathbb{Z}_3\}.$$

Denotando $0 + \langle x^2 + 1 \rangle$, $1 + \langle x^2 + 1 \rangle$, $2 + \langle x^2 + 1 \rangle$, $x + \langle x^2 + 1 \rangle$, $2x + \langle x^2 + 1 \rangle$, $1 + x + \langle x^2 + 1 \rangle$, $1 + 2x + \langle x^2 + 1 \rangle$, $2 + x + \langle x^2 + 1 \rangle$ e $2 + 2x + \langle x^2 + 1 \rangle$ por, respectivamente, $0, 1, 2, u, a, b, c, d, f$, as tabelas das operações são as seguintes:

$+$	0	1	2	u	a	b	c	d	f	\cdot	0	1	2	u	a	b	c	d	f
0	0	1	2	u	a	b	c	d	f	0	0	0	0	0	0	0	0	0	0
1	1	2	0	b	c	d	f	u	a	1	0	1	2	u	a	b	c	d	f
2	2	0	1	d	f	u	a	b	c	2	0	2	1	a	u	f	d	c	b
u	u	b	d	a	0	c	1	f	2	u	0	u	a	2	1	d	b	f	c
a	a	c	f	0	u	1	b	2	d	a	0	a	u	1	2	c	f	b	d
b	b	d	u	c	1	f	2	a	0	b	0	b	f	d	c	a	2	1	u
c	c	f	a	1	b	2	d	0	u	c	0	c	d	b	f	2	u	a	1
d	d	u	b	f	2	a	0	c	1	d	0	d	c	f	b	1	a	u	2
f	f	a	c	2	d	0	u	1	b	f	0	f	b	c	d	u	1	2	a

3.27. Considere o polinómio $p(x) = 8x^3 - 6x - 1$ sobre \mathbb{Q} .

- (a) Mostre que $p(x)$ é irredutível sobre \mathbb{Q} .
 - (b) Construa uma extensão de decomposição de $p(x)$ e determine a sua dimensão.
- (a) As possíveis raízes racionais de $p(x)$ são: $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$. Nenhuma delas é de facto uma raiz pelo que o polinómio, não tendo raízes em \mathbb{Q} e sendo de grau 3, é irredutível sobre \mathbb{Q} .
- (b) Como $p(x)$ é irredutível sobre \mathbb{Q} ,

$$\begin{aligned} \mathbb{Q}[x]/\langle p(x) \rangle &= \{a(x) + \langle p(x) \rangle \mid a(x) \in \mathbb{Q}[x]\} \\ &= \{a(x) + \langle p(x) \rangle \mid a(x) \in \mathbb{Q}[x], \text{gr}(a(x)) \leq 2\} \\ &\cong \mathbb{Q}(\theta), \end{aligned}$$

onde $8\theta^3 - 6\theta - 1 = 0$. Como $x^3 - \frac{3}{4}x - \frac{1}{8}$ é o polinómio mínimo de θ sobre \mathbb{Q} , então $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$ pelo que

$$\mathbb{Q}(\theta) = \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\}.$$

Nesta extensão já o polinómio $8x^3 - 6x - 1$ tem uma raiz (precisamente o elemento θ) pelo que é redutível. Dividindo $8x^3 - 6x - 1$ pelo factor $x - \theta$ obtém-se:

$$8x^3 - 6x - 1 = (x - \theta)(8x^2 + 8\theta x + 8\theta^2 - 6).$$

Teremos agora que verificar se o factor $8x^2 + 8\theta x + 8\theta^2 - 6$ é ou não redutível sobre $\mathbb{Q}(\theta)$ para concluirmos se esta é ou não a extensão de decomposição do polinómio $p(x)$.

Trata-se de um polinómio de grau 2 pelo que bastará verificar se tem raízes em $\mathbb{Q}(\theta)$. Averiguemos então se existem racionais a, b, c tais que

$$8(a + b\theta + c\theta^2)^2 + 8\theta(a + b\theta + c\theta^2) + 8\theta^2 - 6 = 0.$$

Efectuando os cálculos obtemos

$$(8a^2 - 6) + (16ab + 8a)\theta + (8b^2 + 16ac + 8b + 8)\theta^2 + (16bc + 8c)\theta^3 + 8c^2\theta^4 = 0.$$

Mas $8\theta^3 = 6\theta + 1$ (donde $8\theta^4 = 6\theta^2 + \theta$) pelo que podemos ainda escrever

$$(8a^2 - 6 + 2bc + c) + (16ab + 8a + 12bc + 6c + c^2)\theta + (8b^2 + 16ac + 8b + 8 + 6c^2)\theta^2 = 0.$$

Então, como $1, \theta$ e θ^2 são linearmente independentes, esta igualdade é equivalente ao sistema

$$\begin{cases} 8a^2 - 6 + 2bc + c = 0 \\ 16ab + 8a + 12bc + 6c + c^2 = 0 \\ 8b^2 + 16ac + 8b + 8 + 6c^2 = 0. \end{cases}$$

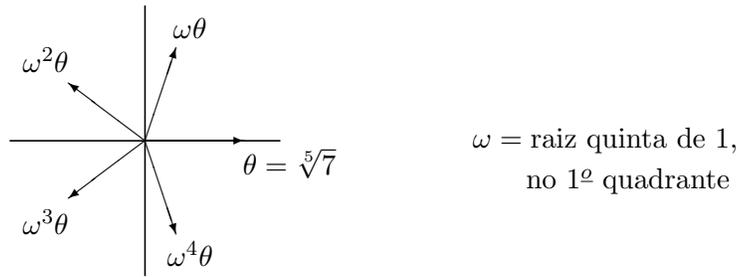
Este sistema não parece ser fácil de resolver. Tem no entanto uma solução fácil de encontrar após alguma procura e experimentação: $a = 1, b = 0, c = -2$. Isto mostra que o elemento $1 - 2\theta^2$ de $\mathbb{Q}(\theta)$ é uma raiz de $p(x)$ pois é raiz do seu factor $8x^2 + 8\theta x + 8\theta^2 - 6$. Portanto este factor é divisível por $x - (1 - 2\theta^2)$. Efectuando a divisão obtemos $8x^2 + 8\theta x + 8\theta^2 - 6 = (x - 1 + 2\theta^2)(8x + 8 + 8\theta - 16\theta^2)$. Em conclusão,

$$\begin{aligned} 8x^3 - 6x - 1 &= (x - \theta)(8x^2 + 8\theta x + 8\theta^2 - 6) \\ &= 8(x - \theta)(x - 1 + 2\theta^2)(x + 1 + \theta - 2\theta^2) \\ &= 8(x - \theta)(x - (1 - 2\theta^2))(x - (-1 - \theta + 2\theta^2)) \end{aligned}$$

o que mostra que $\theta, 1 - 2\theta^2$ e $-1 - \theta + 2\theta^2$ são as três raízes de $p(x)$ e que $\mathbb{Q}(\theta)$ é de facto a sua extensão de decomposição (que tem dimensão 3).

3.29. *Seja θ a raiz real do polinómio $x^5 - 7$. Determine o grupo de Galois da extensão $\mathbb{Q}(\theta)$ de \mathbb{Q} .*

É claro que $\theta = \sqrt[5]{7}$ (as outras 4 raízes não são reais):



Portanto, θ tem polinómio mínimo $x^5 - 7$ sobre \mathbb{Q} . Qualquer \mathbb{Q} -automorfismo de $\mathbb{Q}(\theta)$

$$\Phi : \mathbb{Q}(\theta) \rightarrow \mathbb{Q}(\theta)$$

mantém fixos os números racionais e transforma θ numa raiz do mesmo polinómio em $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[5]{7}) \subseteq \mathbb{R}$. Logo, necessariamente, $\Phi(\theta) = \theta$ e só existe um \mathbb{Q} -automorfismo de $\mathbb{Q}(\theta)$:

$$\begin{aligned} \Phi : \mathbb{Q}(\sqrt[5]{7}) &\rightarrow \mathbb{Q}(\sqrt[5]{7}) \\ a \in \mathbb{Q} &\mapsto a \\ \sqrt[5]{7} &\mapsto \sqrt[5]{7} \end{aligned}$$

que é a identidade. Assim, $Gal(\mathbb{Q}(\theta), \mathbb{Q})$ é o grupo trivial $S_1 = \{id\}$.

3.30. *Seja L uma extensão de \mathbb{Q} . Determine os \mathbb{Q} -automorfismos de L para:*

- (a) $L = \mathbb{Q}(\sqrt{2})$.
 - (c) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- (a) O elemento $\sqrt{2}$ tem polinómio mínimo $x^2 - 2$ sobre \mathbb{Q} . Pela Proposição 3.15, qualquer \mathbb{Q} -automorfismo $\Phi : L \rightarrow L$ transforma raízes deste polinómio em raízes do mesmo polinómio. Existem, pois, precisamente dois \mathbb{Q} -automorfismos:

$$\begin{array}{ccc} \Phi_{\sqrt{2}} : \mathbb{Q}(\sqrt{2}) &\rightarrow \mathbb{Q}(\sqrt{2}) & \Phi_{-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}) \\ a \in \mathbb{Q} &\mapsto a & a \in \mathbb{Q} \mapsto a \\ \sqrt{2} &\mapsto \sqrt{2} & \sqrt{2} \mapsto -\sqrt{2}. \end{array}$$

O primeiro é a identidade e o segundo aplica cada elemento $a + b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ em $a - b\sqrt{2}$.

- (c) Cada \mathbb{Q} -automorfismo $\Phi : L \rightarrow L$ é completamente determinado pela sua acção no conjunto $\{\sqrt{2}, \sqrt{3}\}$. A restrição $\Phi|_{\mathbb{Q}(\sqrt{2})} : \mathbb{Q}(\sqrt{2}) \rightarrow L$ é um homomorfismo injectivo que mantém fixos os elementos de \mathbb{Q} . Então, pela Proposição 3.15, só há duas possibilidades para esta restrição, como vimos

na alínea anterior: é a identidade ou aplica cada elemento $a + b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ em $a - b\sqrt{2}$. Portanto, Φ prolonga o isomorfismo identidade de $\mathbb{Q}(\sqrt{2})$ ou prolonga o isomorfismo $\Phi_{-\sqrt{2}}$ de $\mathbb{Q}(\sqrt{2})$. Usando novamente a Proposição 3.15, como $x^2 - 3$ é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$, estes dois isomorfismos de $\mathbb{Q}(\sqrt{2})$ só podem ser prolongados a $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ aplicando $\sqrt{3}$ em $\sqrt{3}$ ou $-\sqrt{3}$. Portanto, só existem 4 possibilidades para Φ : a identidade e

$$\Phi(\sqrt{2}) = -\sqrt{2}, \quad \Phi(\sqrt{3}) = \sqrt{3};$$

$$\Phi(\sqrt{2}) = \sqrt{2}, \quad \Phi(\sqrt{3}) = -\sqrt{3};$$

$$\Phi(\sqrt{2}) = -\sqrt{2}, \quad \Phi(\sqrt{3}) = -\sqrt{3}.$$

O grupo de Galois tem, pois, neste caso, 4 elementos, que designamos respectivamente por $\Phi_0, \Phi_1, \Phi_2, \Phi_3$:

$$\Phi_0(a + b\sqrt{2} + c\sqrt{3}) = a + b\sqrt{2} + c\sqrt{3},$$

$$\Phi_1(a + b\sqrt{2} + c\sqrt{3}) = a - b\sqrt{2} + c\sqrt{3},$$

$$\Phi_2(a + b\sqrt{2} + c\sqrt{3}) = a + b\sqrt{2} - c\sqrt{3},$$

$$\Phi_3(a + b\sqrt{2} + c\sqrt{3}) = a - b\sqrt{2} - c\sqrt{3}.$$

3.31.

- (a) Para as extensões L de \mathbb{Q} do exercício anterior, calcule os respectivos grupos de Galois, $\text{Gal}(L, \mathbb{Q})$.
- (b) Verifique em quais desses casos a correspondência de Galois entre os subgrupos do grupo de Galois e as extensões intermédias (entre \mathbb{Q} e L) é uma bijecção.

- (a) No primeiro caso, $\text{Gal}(L, \mathbb{Q}) = \{id, \Phi_{-\sqrt{2}}\}$ é um grupo isomorfo a \mathbb{Z}_2 .

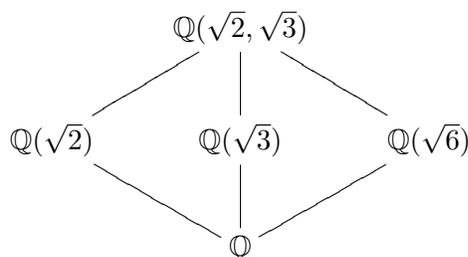
No terceiro caso, o grupo de Galois tem 4 elementos, sendo a tabela do grupo a seguinte:

\circ	Φ_0	Φ_1	Φ_2	Φ_3
Φ_0	Φ_0	Φ_1	Φ_2	Φ_3
Φ_1	Φ_1	Φ_0	Φ_3	Φ_2
Φ_2	Φ_2	Φ_3	Φ_0	Φ_1
Φ_3	Φ_3	Φ_2	Φ_1	Φ_0

Em conclusão, este grupo é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

- (b) No primeiro caso, as extensões intermédias são só os próprios \mathbb{Q} e $\mathbb{Q}(\sqrt{2})$. Como \mathbb{Z}_2 só tem os dois subgrupos triviais ($\{0\}$ e o próprio \mathbb{Z}_2), neste caso a correspondência de Galois é uma bijecção.

No segundo caso, o diagrama com as extensões intermédias é o seguinte:



A lista de subgrupos de $Gal(L, \mathbb{Q})$ é $\{\Phi_0\}$, $\{\Phi_0, \Phi_1\}$, $\{\Phi_0, \Phi_2\}$, $\{\Phi_0, \Phi_3\}$, $\{\Phi_0, \Phi_1, \Phi_2, \Phi_3\}$. Neste caso, também há bijecção.

3.32.

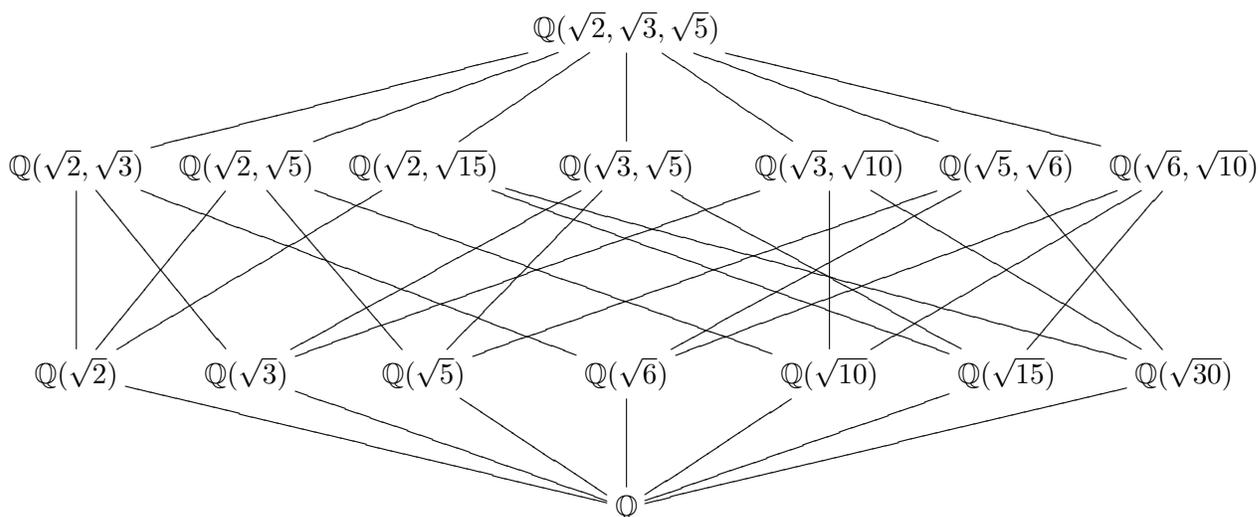
- (a) *Determine os corpos intermédios entre \mathbb{Q} e $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.*

- (b) *Calcule o respectivo grupo de Galois e compare os resultados.*

(a) Como $2 \times 3 \times 5 = 30$ tem como divisores 1, 2, 3, 5, 6, 10, 15 e 30, as extensões simples entre \mathbb{Q} e $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ são $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$ e $\mathbb{Q}(\sqrt{30})$. Quanto às extensões duplas, temos:

$$\begin{aligned}
 \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{6}) \\
 \mathbb{Q}(\sqrt{2}, \sqrt{5}) &= \mathbb{Q}(\sqrt{2}, \sqrt{10}) = \mathbb{Q}(\sqrt{5}, \sqrt{10}) \\
 \mathbb{Q}(\sqrt{2}, \sqrt{15}) &= \mathbb{Q}(\sqrt{2}, \sqrt{30}) = \mathbb{Q}(\sqrt{15}, \sqrt{30}) \\
 \mathbb{Q}(\sqrt{3}, \sqrt{5}) &= \mathbb{Q}(\sqrt{3}, \sqrt{15}) = \mathbb{Q}(\sqrt{5}, \sqrt{15}) \\
 \mathbb{Q}(\sqrt{3}, \sqrt{10}) &= \mathbb{Q}(\sqrt{3}, \sqrt{30}) = \mathbb{Q}(\sqrt{10}, \sqrt{30}) \\
 \mathbb{Q}(\sqrt{5}, \sqrt{6}) &= \mathbb{Q}(\sqrt{5}, \sqrt{30}) = \mathbb{Q}(\sqrt{6}, \sqrt{30}) \\
 \mathbb{Q}(\sqrt{6}, \sqrt{10}) &= \mathbb{Q}(\sqrt{6}, \sqrt{15}) = \mathbb{Q}(\sqrt{10}, \sqrt{15}).
 \end{aligned}$$

O diagrama seguinte mostra-nos todas as extensões intermédias entre \mathbb{Q} e $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$:



(b) Neste caso, $\text{Gal}(L, \mathbb{Q})$ é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

3.33. Considere a extensão $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \subseteq \mathbb{R}$ de \mathbb{Q} .

(a) Como se define o grupo de Galois de L (sobre \mathbb{Q})? Determine-o.

(b) Indique todas as extensões intermédias de \mathbb{Q} em L .

(c) L é uma extensão normal de \mathbb{Q} ? Justifique.

(a) Seja $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$. Cada $\Phi \in \text{Gal}(L, \mathbb{Q})$ é completamente determinado pela sua acção no conjunto $\{\sqrt{3}, \sqrt[3]{2}\}$. A restrição $\Phi|_{\mathbb{Q}(\sqrt{3})} : \mathbb{Q}(\sqrt{3}) \rightarrow L$ é um homomorfismo injectivo que mantém fixos os elementos de \mathbb{Q} . Então, pela Proposição 3.15, só há duas possibilidades para esta restrição: é a identidade ou aplica cada elemento $a + b\sqrt{3}$ de $\mathbb{Q}(\sqrt{3})$ em $a - b\sqrt{3}$. Portanto, Φ prolonga o isomorfismo identidade de $\mathbb{Q}(\sqrt{3})$ ou prolonga o isomorfismo $\Phi_{-\sqrt{3}}$ de $\mathbb{Q}(\sqrt{3})$. Pela Proposição 3.15, como $x^3 - 2$ é o polinómio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}(\sqrt{3})$, o número de prolongamentos de Φ a L é igual ao número de raízes distintas de $x^3 - 2$ em L , ou seja, um (que corresponde à única raiz $\sqrt[3]{2}$). Assim, os dois isomorfismos de $\mathbb{Q}(\sqrt{3})$ só podem ser prolongados a $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ aplicando $\sqrt[3]{2}$ em $\sqrt[3]{2}$, pelo que existem exactamente duas possibilidades para Φ : a identidade ou

$$\Phi(\sqrt{3}) = -\sqrt{3}, \quad \Phi(\sqrt[3]{2}) = \sqrt[3]{2}.$$

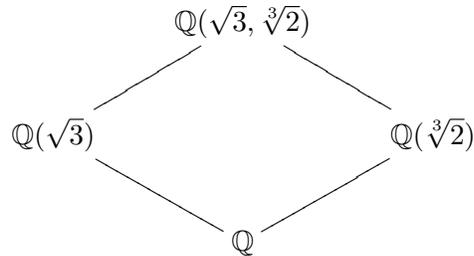
O grupo de Galois tem pois dois elementos:

$$\Phi_0(a + b\sqrt{3} + c\sqrt[3]{2}) = a + b\sqrt{3} + c\sqrt[3]{2},$$

$$\Phi_1(a + b\sqrt{3} + c\sqrt[3]{2}) = a - b\sqrt{3} + c\sqrt[3]{2}.$$

Neste caso, $Gal(L, \mathbb{Q})$ é isomorfo a \mathbb{Z}_2 .

(b) Note que $\mathbb{Q}(\sqrt{3}\sqrt[3]{2}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$, pelo que as únicas extensões intermédias de \mathbb{Q} em L são:



(c) Não, pois $[L : \mathbb{Q}] = 6$ mas $|Gal(L, \mathbb{Q})| = 2$ (e pelo Teorema 3.21, se $|Gal(L, K)|$ é diferente de $[L : K]$, então L não é uma extensão normal de K).

3.38. (b) Calcule o grupo de Galois do polinómio $f(x) = x^4 - 2$ sobre o corpo \mathbb{Q} .

Uma vez que o polinómio $f(x) = x^4 - 2$ tem raízes

$$\theta_1 = \sqrt[4]{2}, \theta_2 = -\sqrt[4]{2}, \theta_3 = \sqrt[4]{2}i, \theta_4 = -\sqrt[4]{2}i$$

então $L = \mathbb{Q}(\sqrt[4]{2}, i)$ é a extensão de decomposição de $f(x)$. Portanto, o grupo pedido é o grupo $Gal(L, \mathbb{Q}) = Gal(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q})$. Teremos então que determinar todos os \mathbb{Q} -automorfismos de L .

Cada \mathbb{Q} -automorfismo $\Phi : L \rightarrow L$ é completamente determinado pela sua acção no conjunto $\{\sqrt[4]{2}, i\}$ (uma vez que todo o elemento de L é uma combinação linear racional de potências de $\sqrt[4]{2}$ e i). A respectiva restrição $\Phi|_{\mathbb{Q}(\sqrt[4]{2})} : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L$ é um homomorfismo injectivo que mantém fixos os elementos de \mathbb{Q} (ou seja, é um prolongamento do isomorfismo $id : \mathbb{Q} \rightarrow \mathbb{Q}$). Estes podem ser determinados com o auxílio da Proposição 3.15:

O elemento $\sqrt[4]{2}$ tem polinómio mínimo $x^4 - 2$ sobre \mathbb{Q} , o que significa em particular que

$$\mathbb{Q}(\sqrt[4]{2}) = \{a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}.$$

Pela Proposição 3.15, o isomorfismo $id : \mathbb{Q} \rightarrow \mathbb{Q}$ pode ser prolongado a um homomorfismo injectivo $\phi : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L$ se e só se $x^4 - 2$ tem uma raiz em L , e o número desses prolongamentos é igual ao número de raízes distintas de $x^4 - 2$ em L , ou seja 4:

$$\begin{array}{lcl} \phi_1 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & L \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & \theta_1 = \sqrt[4]{2} \end{array} \qquad \begin{array}{lcl} \phi_2 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & L \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & \theta_2 = -\sqrt[4]{2} \end{array}$$

$$\begin{array}{lcl} \phi_3 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & L \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & \theta_3 = \sqrt[4]{2}i \end{array} \qquad \begin{array}{lcl} \phi_4 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & L \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & \theta_4 = -\sqrt[4]{2}i. \end{array}$$

Estes são pois os únicos homomorfismos injectivos $\mathbb{Q}(\sqrt[4]{2}) \rightarrow L$ que prolongam a $id : \mathbb{Q} \rightarrow \mathbb{Q}$ e, consequentemente, os $\Phi : L \rightarrow L$ que procuramos, quando restritos a $\mathbb{Q}(\sqrt[4]{2})$, coincidem necessariamente com um dos ϕ_i ($i = 1, 2, 3, 4$). Dito de outro modo, claramente equivalente, os $\Phi : L \rightarrow L$ que procuramos são os prolongamentos a L de cada um dos seguintes isomorfismos de corpos:

$$\begin{array}{lcl} \tilde{\phi}_1 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & \mathbb{Q}(\sqrt[4]{2}) \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \end{array} \qquad \begin{array}{lcl} \tilde{\phi}_2 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & \mathbb{Q}(\sqrt[4]{2}) \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} \end{array}$$

$$\begin{array}{lcl} \tilde{\phi}_3 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & \mathbb{Q}(\sqrt[4]{2}i) \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & \sqrt[4]{2}i \end{array} \qquad \begin{array}{lcl} \tilde{\phi}_4 : \mathbb{Q}(\sqrt[4]{2}) & \rightarrow & \mathbb{Q}(\sqrt[4]{2}i) \\ a \in \mathbb{Q} & \mapsto & a \\ \sqrt[4]{2} & \mapsto & -\sqrt[4]{2}i. \end{array}$$

$x^2 + 1 \in \mathbb{Q}[x]$ é o polinómio mínimo de i sobre $\mathbb{Q}(\sqrt[4]{2})$. Usando novamente a Proposição 3.15, como cada um dos $\tilde{\phi}_i$ mantém fixos os coeficientes de $x^2 + 1$ e este polinómio tem duas raízes distintas em L , podemos concluir que cada um dos isomorfismos $\tilde{\phi}_i$ vai ter dois prolongamentos a homomorfismos injectivos de extensões $L \rightarrow L$, um que transforma i em i e o outro transforma i na outra raiz $-i$.

Começando com $\tilde{\phi}_1$

$$\begin{array}{ccc} & L & \xrightarrow{\Phi=?} L \\ & \uparrow & \uparrow \\ \boxed{x^2 + 1} & \mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\tilde{\phi}_1=id} \mathbb{Q}(\sqrt[4]{2}) & \boxed{x^2 + 1} \end{array}$$

obtemos

$$\begin{array}{lcl} \Phi_1 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto \sqrt[4]{2} \\ & i & \mapsto i \end{array} \qquad \begin{array}{lcl} \Phi_2 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto \sqrt[4]{2} \\ & i & \mapsto -i. \end{array}$$

Φ_1 é simplesmente a identidade e Φ_2 é o isomorfismo definido por

$$a_0 + a_1 \sqrt[4]{2} + a_2 \sqrt[4]{4} + a_3 \sqrt[4]{8} + a_4 i + a_5 \sqrt[4]{2} i + a_6 \sqrt[4]{4} i + a_7 \sqrt[4]{8} i$$

↓

$$a_0 + a_1 \sqrt[4]{2} + a_2 \sqrt[4]{4} + a_3 \sqrt[4]{8} - a_4 i - a_5 \sqrt[4]{2} i - a_6 \sqrt[4]{4} i - a_7 \sqrt[4]{8} i.$$

Fazendo o mesmo para $\tilde{\phi}_2$, $\tilde{\phi}_3$ e $\tilde{\phi}_4$ obtemos sucessivamente

$$\begin{array}{lcl} \Phi_3 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} \\ & i & \mapsto i \end{array} \qquad \begin{array}{lcl} \Phi_4 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} \\ & i & \mapsto -i \end{array}$$

$$\begin{array}{lcl} \Phi_5 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto \sqrt[4]{2} i \\ & i & \mapsto i \end{array} \qquad \begin{array}{lcl} \Phi_6 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto \sqrt[4]{2} i \\ & i & \mapsto -i \end{array}$$

$$\begin{array}{lcl} \Phi_7 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} i \\ & i & \mapsto i \end{array} \qquad \begin{array}{lcl} \Phi_8 : & L & \rightarrow L \\ & a \in \mathbb{Q} & \mapsto a \\ & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} i \\ & i & \mapsto -i. \end{array}$$

Por exemplo,

$$\begin{aligned} \Phi_7(a_0 + a_1 \sqrt[4]{2} + a_2 \sqrt[4]{4} + a_3 \sqrt[4]{8} + a_4 i + a_5 \sqrt[4]{2} i + a_6 \sqrt[4]{4} i + a_7 \sqrt[4]{8} i) &= \\ &= a_0 - a_1 \sqrt[4]{2} i - a_2 \sqrt[4]{4} + a_3 \sqrt[4]{8} i + a_4 i + a_5 \sqrt[4]{2} - a_6 \sqrt[4]{4} i - a_7 \sqrt[4]{8} \\ &= a_0 + a_5 \sqrt[4]{2} - a_2 \sqrt[4]{4} - a_7 \sqrt[4]{8} + a_4 i - a_1 \sqrt[4]{2} i - a_6 \sqrt[4]{4} i + a_3 \sqrt[4]{8} i. \end{aligned}$$

Portanto, $Gal(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}) = \{\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6, \Phi_7, \Phi_8\}$. Observemos ainda como pode ser descrito como um subgrupo de \mathcal{S}_4 :

$$\begin{aligned} \Phi_1 &= \begin{pmatrix} \theta_1 & \theta_2 & \theta_3 & \theta_4 \\ \theta_1 & \theta_2 & \theta_3 & \theta_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id \\ \Phi_2 &= \begin{pmatrix} \theta_1 & \theta_2 & \theta_3 & \theta_4 \\ \theta_1 & \theta_2 & \theta_4 & \theta_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34) \end{aligned}$$

$$\Phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34), \quad \Phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$$

$$\Phi_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324), \quad \Phi_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$\Phi_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1423), \quad \Phi_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23).$$

Em conclusão:

$$\boxed{\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}) = \{id, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}}$$

3.42. Considere um polinómio $f(x)$ irredutível, de grau 3, escrito na sua forma reduzida $x^3 + px + q$, e as suas três raízes complexas distintas a , b , e c .

(a) Verifique que
$$\begin{cases} a + b + c = 0 \\ ab + ac + bc = p \\ abc = -q. \end{cases}$$

(b) A partir da alínea anterior, mostre que $((a-b)(a-c)(b-c))^2 = -4p^3 - 27q^2$.

(c) Seja D o número $-4p^3 - 27q^2$ da alínea anterior. Prove que se $\sqrt{D} \in \mathbb{Q}$ e $\Phi \in \text{Gal}(f(x), \mathbb{Q})$, então $\Phi(\sqrt{D}) = \sqrt{D}$ e, portanto, $\text{Gal}(f(x), \mathbb{Q}) \cong \mathcal{A}_3$.

(d) Prove que se $\sqrt{D} \notin \mathbb{Q}$, então $\mathbb{Q}(\sqrt{D})$ está na extensão de decomposição de $f(x)$ e, portanto, $\text{Gal}(f(x), \mathbb{Q}) \cong \mathcal{S}_3$.

(a) Basta observar que $x^3 + px + q = (x-a)(x-b)(x-c)$ é equivalente a $x^3 + px + q = x^3 + (-c-a-b)x^2 + (ab+ac+bc)x - abc$.

(b) Basta, com um pouco de paciência, desenvolver ambos os membros (substituindo, no segundo, p por $ab+ac+bc$ e q por $-abc$), até as expressões coincidirem.

- (c) Pela Proposição 3.19, $Gal(f(x), \mathbb{Q})$ é isomorfo a um subgrupo de \mathcal{S}_3 . Seja $\Phi \in Gal(f(x), \mathbb{Q}) = Gal(\mathbb{Q}(a, b, c), \mathbb{Q})$. Por definição, Φ , sendo um \mathbb{Q} -automorfismo, terá que preservar os racionais, logo $\Phi(\sqrt{D}) = \sqrt{D}$, isto é, $\Phi((a-b)(a-c)(b-c)) = (a-b)(a-c)(b-c)$. Consequentemente,

$$(\Phi(a) - \Phi(b))(\Phi(a) - \Phi(c))(\Phi(b) - \Phi(c)) = (a-b)(a-c)(b-c). \quad (2)$$

Mas Φ permuta as raízes a , b e c entre si. Para que se cumpra (2), essa permutação não pode ser ímpar (se fosse ímpar teríamos

$$(\Phi(a) - \Phi(b))(\Phi(a) - \Phi(c))(\Phi(b) - \Phi(c)) = -(a-b)(a-c)(b-c).$$

Sobram assim só as 3 permutações pares para eventual definição de \mathbb{Q} -automorfismos de $\mathbb{Q}(a, b, c)$. Não é difícil ver que todas elas definem de facto \mathbb{Q} -automorfismos de $\mathbb{Q}(a, b, c)$, pelo que $Gal(\mathbb{Q}(a, b, c), \mathbb{Q}) \cong \mathcal{A}_3$. Esta conclusão também se pode tirar do seguinte: como, pelo Teorema 3.21, se tem $|Gal(\mathbb{Q}(a, b, c), \mathbb{Q})| = [\mathbb{Q}(a, b, c) : \mathbb{Q}]$, bastará mostrar que $[\mathbb{Q}(a, b, c) : \mathbb{Q}] \geq 3$, o que é simples:

$$[\mathbb{Q}(a, b, c) : \mathbb{Q}] = [\mathbb{Q}(a, b, c) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] \geq 3,$$

pois $[\mathbb{Q}(a) : \mathbb{Q}] = gr(f(x)) = 3$.

- (d) Neste caso, se $\sqrt{D} \notin \mathbb{Q}$, já $\Phi(\sqrt{D})$ não precisa de ser igual a \sqrt{D} , e as permutações ímpares também definem elementos de $Gal(\mathbb{Q}(a, b, c), \mathbb{Q})$. Consequentemente, $Gal(\mathbb{Q}(a, b, c), \mathbb{Q}) \cong \mathcal{S}_3$.

3.44. (a) *Sejam $p \geq 5$ um número primo, e $f(x) \in \mathbb{Q}[x]$ um polinómio irreduzível de grau p . Mostre que se $f(x)$ tem exactamente duas raízes complexas não reais, então $Gal(f(x), \mathbb{Q})$ é o grupo simétrico \mathcal{S}_p e portanto $f(x)$ não é resolúvel por radicais.*

Basta fazer o mesmo que na demonstração do Corolário 3.29 (Teorema de Abel-Ruffini).

3.45. *Mostre que os seguintes polinómios $f(x) \in \mathbb{Q}[x]$ não são resolúveis por radicais:*

(a) $2x^5 - 10x + 5$.

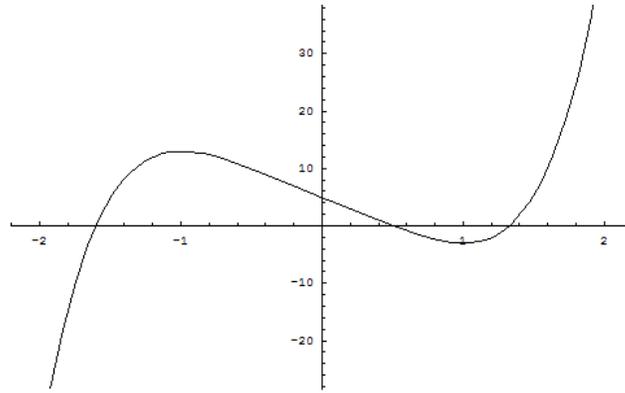
(c) $x^5 - 6x^2 + 5$.

(b) $2x^5 - 5x^4 + 20$.

(d) $x^7 - 10x^5 + 15x + 5$.

Fazendo o estudo e esboço das respectivas funções (ou, alternativamente, usando métodos da Matemática Numérica para localização de raízes, ou utilizando algum software como o Mathematica ou Maple) não é difícil confirmar que:

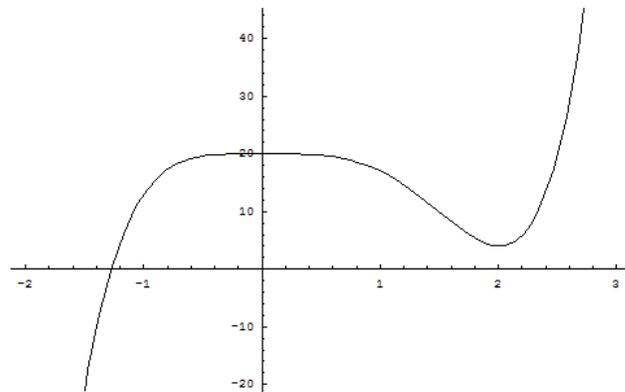
(a) Este polinómio tem exactamente 2 raízes complexas não reais:



$$2x^5 - 10x + 5$$

A conclusão segue do Exercício 3.44 (a).

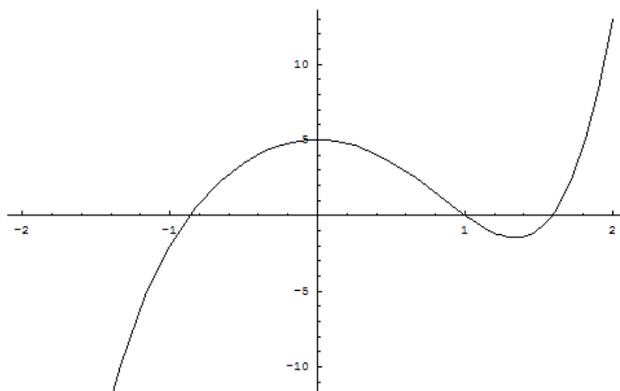
(b) Este polinómio tem exactamente 4 raízes complexas não reais:



$$2x^5 - 5x^4 + 20$$

A conclusão segue do Exercício 3.44 (b).

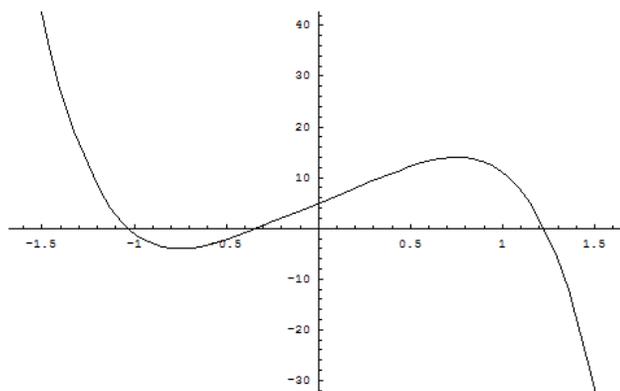
(c) Tem exactamente 2 raízes complexas não reais:



$$x^5 - 6x^2 + 5$$

A conclusão segue do Exercício 3.44 (a).

(d) Tem exactamente 2 raízes complexas não reais:



$$x^7 - 10x^5 + 15x + 5$$

A conclusão segue do Exercício 3.44 (a).

Capítulo 4

4.3. Seja F a extensão de decomposição de $x^2 - 2 \in \mathbb{Z}_3[x]$.

(a) Descreva o corpo F e indique um gerador de $F^* = F \setminus \{0\}$.

(b) Qual é o subcorpo primo de F ?

(a) F é o corpo $\frac{\mathbb{Z}_3[x]}{\langle x^2 - 2 \rangle} = \{a_0 + a_1x + \langle x^2 - 2 \rangle \mid a_0, a_1 \in \mathbb{Z}_3\}$. Denotando o elemento $a_0 + a_1x + \langle x^2 - 2 \rangle$ por a_0a_1 , as tabelas das operações de F são as seguintes:

+	00	01	02	10	11	12	20	21	22
00	00	01	02	10	11	12	20	21	22
01	01	02	00	11	12	10	21	22	20
02	02	00	01	12	10	11	22	20	21
10	10	11	12	20	21	22	00	01	02
11	11	12	10	21	22	20	01	02	00
12	12	10	11	22	20	21	02	00	01
20	20	21	22	00	01	02	10	11	12
21	21	22	20	01	02	00	11	12	10
22	22	20	21	02	00	01	12	10	11

.	00	01	02	10	11	12	20	21	22
00	00	00	00	00	00	00	00	00	00
01	00	20	10	01	21	11	02	22	12
02	00	10	20	02	12	22	01	11	21
10	00	01	02	10	11	12	20	21	22
11	00	21	12	11	02	20	22	10	01
12	00	11	22	12	20	01	21	02	10
20	00	02	01	20	22	21	10	12	11
21	00	22	11	21	10	02	12	01	20
22	00	12	21	22	01	10	11	20	02

O elemento 11 é um exemplo de gerador de F^* .

(b) $\{00, 10, 20\} \cong \mathbb{F}_3$.

4.6. *Construa um corpo finito de ordem 16 e determine todos os geradores do seu grupo multiplicativo.*

Recorde a construção do corpo M nas páginas 88-91. A lista dos elementos primitivos de M é c, f, g, h, i, j, l, n .

4.7. *Construa um corpo com 27 elementos.*

Uma vez que $27 = 3 \times 3 \times 3$, pelo processo de construção usado no exercício anterior (baseado no Teorema de Kronecker), teremos que começar com um polinómio de grau 3 irreduzível sobre \mathbb{F}_3 . Por exemplo, o polinómio $p(x) = x^3 + 2x + 1$. Seja L o corpo $\frac{\mathbb{Z}_3[x]}{\langle p(x) \rangle} = \{a_0 + a_1x + a_2x^2 + \langle p(x) \rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_3\}$ constituído pelas 27

classes definidas pelos restos da divisão dos polinômios de coeficientes em $\mathbb{Z}_3[x]$ por $p(x)$. Este corpo terá exactamente 27 elementos. Com um pouco de paciência não será difícil escrever as tabelas das operações de L .

4.8. *Indique, justificando, o número de corpos não isomorfos de ordem inferior a 100.*

Pelos Teoremas 4.1, 4.3 e 4.4 o conjunto de corpos não isomorfos de ordem inferior a 100 é $\{\mathbb{F}_{p^n} \mid p \text{ primo}, n \in \mathbb{N}, p^n < 100\}$. Portanto, o seu número é dado pelo número de potências de primos, inferiores a 100, ou seja 34:

$$2, 2^2, 2^3, 2^4, 2^5, 2^6, 3, 3^2, 3^3, 3^4, 5, 5^2, 7, 7^2 \\ 11, 13, 17, 19, 23, 29, 31, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

4.10. *Liste os subcorpos do corpo \mathbb{F}_{256} . Qual deles é o subcorpo primo?*

Basta usarmos o Teorema 4.5. Como $256 = 2^8$, a lista de subcorpos de \mathbb{F}_{256} é $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}, \mathbb{F}_{256}$. \mathbb{F}_2 é o subcorpo primo.

4.11. *Usando resultados sobre corpos finitos, mostre que se p é um número primo e r divide n , então $p^r - 1$ divide $p^n - 1$.*

Se p é um número primo e r divide n , então \mathbb{F}_{p^r} é um subcorpo de \mathbb{F}_{p^n} . Em particular,

$$(\mathbb{F}_{p^r})^* = (\mathbb{F}_{p^r} \setminus \{0\}, \cdot)$$

é um subgrupo de

$$(\mathbb{F}_{p^n})^* = (\mathbb{F}_{p^n} \setminus \{0\}, \cdot)$$

pelo que $|(\mathbb{F}_{p^r})^*| = p^r - 1$ divide $|(\mathbb{F}_{p^n})^*| = p^n - 1$.

4.12. *Determine o número de elementos do corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$.*

Uma vez que

$$\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle = \{p(x) + \langle x^2 + 1 \rangle \mid gr(p(x)) \leq 1\}$$

e existem precisamente $11 \times 11 = 121$ polinômios de grau menor que 2 em $\mathbb{F}_{11}[x]$, o corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$ tem 121 elementos.

4.13. *Mostre que:*

(a) *O corpo $\mathbb{F}_{11}[x]/\langle x^2 + x + 4 \rangle$ é isomorfo a $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$.*

(b) A soma de todos os elementos de um corpo finito, com a exceção de \mathbb{F}_2 , é 0.

(a) Como vimos no exercício anterior, o corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$ tem 121 elementos. Mas o corpo $\mathbb{F}_{11}[x]/\langle x^2 + x + 4 \rangle$ também tem 121 elementos, logo são necessariamente isomorfos (a $\mathbb{F}_{121} = \mathbb{F}_{11^2}$), pelo Teorema de Moore (Corolário 4.3).

(b) Qualquer corpo finito tem sempre um número de elementos igual a uma potência p^n de um primo p , e esse corpo é isomorfo a $\mathbb{F}_p[x]/\langle r(x) \rangle$ para qualquer polinómio $r(x)$ de grau n irredutível sobre \mathbb{F}_p . Os seus elementos são então as classes laterais $p(x) + \langle r(x) \rangle$ definidas pelos polinómios $p(x)$ de grau inferior a n :

Grau

0:	0	1	...	$p - 2$	$p - 1$
1:	x	$x + 1$...	$x + p - 2$	$x + p - 1$
	$2x$	$2x + 1$...	$2x + p - 2$	$2x + p - 1$
	\vdots	\vdots		\vdots	\vdots
	$(p - 2)x$	$(p - 2)x + 1$...	$(p - 2)x + p - 2$	$(p - 2)x + p - 1$
	$(p - 1)x$	$(p - 1)x + 1$...	$(p - 1)x + p - 2$	$(p - 1)x + p - 1$
2:	x^2	$x^2 + 1$...	$x^2 + p - 2$	$x^2 + p - 1$
	$x^2 + x$	$x^2 + x + 1$...	$x^2 + x + p - 2$	$x^2 + x + p - 1$
	$x^2 + 2x$	$x^2 + 2x + 1$...	$x^2 + 2x + p - 2$	$x^2 + 2x + p - 1$
	\vdots	\vdots		\vdots	\vdots
	$x^2 + (p - 2)x$	$x^2 + (p - 2)x + 1$...	$x^2 + (p - 2)x + p - 2$	$x^2 + (p - 2)x + p - 1$
	$x^2 + (p - 1)x$	$x^2 + (p - 1)x + 1$...	$x^2 + (p - 1)x + p - 2$	$x^2 + (p - 1)x + p - 1$
	$2x^2$	$2x^2 + 1$...	$2x^2 + p - 2$	$2x^2 + p - 1$
	$2x^2 + x$	$2x^2 + x + 1$...	$2x^2 + x + p - 2$	$2x^2 + x + p - 1$
	$2x^2 + 2x$	$2x^2 + 2x + 1$...	$2x^2 + 2x + p - 2$	$2x^2 + 2x + p - 1$
	\vdots	\vdots		\vdots	\vdots
	$2x^2 + (p - 2)x$	$2x^2 + (p - 2)x + 1$...	$2x^2 + (p - 2)x + p - 2$	$2x^2 + (p - 2)x + p - 1$
	$2x^2 + (p - 1)x$	$2x^2 + (p - 1)x + 1$...	$2x^2 + (p - 1)x + p - 2$	$2x^2 + (p - 1)x + p - 1$
	\vdots	\vdots		\vdots	\vdots
n-1:

Não vale a pena listar mais polinómios pois já dá para observar o seguinte:

Caso 1: $p > 2$: Neste caso p é ímpar, logo a soma (em $\mathbb{F}_p[x]$) dos polinômios em cada linha é sempre igual a 0 pois, como p é ímpar, $1 + 2 + \dots + p - 2 + p - 1$ é igual a

$$(1 + p - 1) + (2 + p - 2) + \dots + \left(\frac{p-1}{2} + \frac{p+1}{2}\right) = p + p + \dots + p = 0.$$

Portanto, a soma das respectivas classes em $\mathbb{F}_p[x]/\langle r(x) \rangle$ dá também 0.

Caso 2: $p = 2, n > 1$: Neste caso a lista de polinômios reduz-se a

Grau		
0:	0	1
1:	x	$x + 1$
2:	x^2 $x^2 + x$	$x^2 + 1$ $x^2 + x + 1$
3:	\dots	\dots
\vdots	\vdots	\vdots
n-1:	x^{n-1} $x^{n-1} + x$ $x^{n-1} + x^2$ \vdots	$x^{n-1} + 1$ $x^{n-1} + x + 1$ $x^{n-1} + x^2 + 1$ \vdots

Agora a soma em cada linha não é 0 mas sim 1. Mas, como o número total de linhas é par (pois o número de polinômios de grau p^{n-1} é igual ao número de polinômios de grau menor que $n - 1$), a soma total continua a dar 0. Portanto, a soma das respectivas classes em $\mathbb{F}_p[x]/\langle r(x) \rangle$ é também igual a 0.

4.15. *Através de um comando à distância de uma televisão podem ser efetuadas 20 operações: escolher entre 18 canais diferentes (0–17), aumentar (A) ou diminuir (D) o volume. A tabela indica três códigos decimais para transmitir essa informação.*

	0	1	2	...	9	10	11	...	17	A	D
C_1	00	01	02	...	09	10	11	...	17	18	19
C_2	0000	0101	0202	...	0909	1010	1111	...	1717	1818	1919
C_3	00000	01011	02022	...	09099	10109	11118	...	17172	18181	19190

- (a) *Determine a distância mínima de cada um dos três códigos.*
- (b) *Diga quais dos códigos detectam e/ou corrigem erros singulares.*
- (c) *Um receptor de televisão recebe informação do comando utilizando o terceiro código. Sempre que possível diga o efeito gerado pela recepção das seguintes mensagens: 15154, 13144, 19191.*

- (a) $\delta(C_1) = 1$, $\delta(C_2) = 2$ e $\delta(C_3) = 3$.
- (b) O código C_2 detecta, mas não corrige, erros singulares, enquanto C_3 detecta e corrige erros singulares.
- (c) A palavra 15154 pertence a C_3 pelo que o receptor efectua a operação correspondente: muda para o canal 15.

A palavra 13144 não pertence a C_3 pelo que o receptor detecta o erro; no entanto, não realiza nenhuma operação pois não tem capacidade para o corrigir, uma vez que se trata de um erro duplo: $d(13144, c) > 1$ para qualquer $c \in C_3$, havendo mais do que uma palavra a distância 2 de 13144 (nomeadamente, as palavras 13136, 14145 e 15154).

A palavra 19191 não pertence a C_3 pelo que o receptor detecta o erro; como $d(19190, 19191) = 1$, esse erro é singular e a mensagem correcta é 19190, correspondente à operação D (diminuir o volume).

4.16. *Seja \mathcal{C} o código $(7, 3)$ -linear binário definido pela matriz*

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

- (a) *Qual é o número de palavras de \mathcal{C} ?*
- (b) *Calcule a distância mínima $\delta(\mathcal{C})$. Poderá \mathcal{C} detectar erros singulares? E corrigir?*
- (c) *Corrija, caso tal seja possível, os erros nas seguintes mensagens: 0001000, 1011110.*
- (a) Trata-se de um código sobre \mathbb{F}_2 com palavras de comprimento 7, com 4 dígitos de controle. Assim, \mathcal{C} contém $|\mathbb{F}_2^3| = 8$ palavras: 0000000, 0010101, 0101110, 1001111, 1100001, 1011010, 0111011, 1110100.

- (b) $\delta(\mathcal{C}) = 3$. Corrige erros singulares.
- (c) A palavra correcta correspondente à mensagem 0001000 é 0000000, enquanto que a palavra correcta correspondente à mensagem 1011110 é 1011010.

4.19. As matrizes H_1 , H_2 e H_3 seguintes determinam três códigos lineares binários.

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad H_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Para cada um desses códigos, responda às seguintes questões:

- (a) Determine o comprimento do código e o número de dígitos de controlo.
- (b) Calcule a distância mínima e descreva o conjunto das mensagens.
- (c) Poderão estes códigos ser usados para detectar e/ou corrigir erros singulares?
- (d) Supondo que os três últimos dígitos da mensagem são 011, diga se esta mensagem pode pertencer ao código e determine a mensagem completa.
- (a) H_1 e H_2 definem códigos (5,2)-lineares enquanto H_3 define um código (7,3)-linear. Portanto, nos dois primeiros casos o comprimento é 5 e há 3 dígitos de controle, enquanto que no segundo o comprimento é 7 e tem 4 dígitos de controle.
- (b) (solução para H_2) A distância mínima é 3. Uma palavra $c = x_1x_2x_3x_4x_5$ faz parte do código se e só se $H_2c^T = 0$, ou seja,

$$\begin{cases} x_1 + x_5 = 0 \\ x_2 + x_4 + x_5 = 0 \\ x_3 + x_4 + x_5 = 0 \end{cases} \Leftrightarrow \begin{cases} x_1 = x_5 \\ x_2 = x_4 + x_5 \\ x_3 = x_4 + x_5. \end{cases}$$

Portanto, as mensagens são da forma

$$(x_5, x_4 + x_5, x_4 + x_5, x_4, x_5) = x_4(0, 1, 1, 1, 0) + x_5(1, 1, 1, 0, 1)$$

com $x_4, x_5 \in \mathbb{Z}_2$ (isto é, o conjunto das mensagens é o subespaço vectorial de \mathbb{Z}_2^5 gerado pelos vectores $(0, 1, 1, 1, 0)$ e $(1, 1, 1, 0, 1)$). O código é pois formado por 4 mensagens: $(0, 0, 0, 0, 0)$, $(0, 1, 1, 1, 0)$, $(1, 1, 1, 0, 1)$, $(1, 0, 0, 1, 1)$.

- (c) (*solução para H_2*) Sim, detecta e corrige erros singulares.
- (d) (*solução para H_2*) Sim: (1, 0, 0, 1, 1).

Bibliografia

- [1] E. Artin, *Galois Theory*, Dover, 1998.
- [2] R. L. Fernandes e M. Ricou, *Introdução à Álgebra*, IST Press, 2004.
- [3] William J. Gilbert, *Modern Algebra with Applications*, Wiley, 1976.
- [4] A. Gonçalves, *Introdução à Álgebra*, IMPA, Rio de Janeiro, 1979.
- [5] C.H. Hadlock, *Field Theory and Its Classical Problems*, The Carus Mathematical Monographs, 19, The Mathematical Association of America, 2000.
- [6] A. Hefez e M. L. Villela, *Códigos Correctores de Erros*, IMPA, Rio de Janeiro, 2002.
- [7] John M. Howie, *Fields and Galois Theory*, Springer, 2006.
- [8] T. W. Hungerford, *Algebra*, Springer-Verlag, 1980.
- [9] A. Jones, S. Morris e K. Pearson, *Abstract Algebra and Famous Impossibilities*, Universitext, Springer-Verlag, 1994.
- [10] R. Lidl e H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 2000.
- [11] J. Picado e M. Sobral, *Álgebra*, Textos de Apoio, Universidade de Coimbra, 2000.
- [12] I. Stewart, *Galois Theory*, Chapman & Hall, 1973 (3a ed. 2004).