Soluções de exercícios seleccionados (capítulos 3 e 4)

3.6. (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 $mdc(m(x), f(x)) = 1$), 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

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

3.9. 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 $a_i \in K$ $(i = 0, ..., n - 1)$.

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 $gr(r(x)) < n$. Então $f(\theta) = q(\theta)m(\theta) + r(\theta) = r(\theta)$ e $r(\theta)$ é da forma $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ com $a_i \in K$ $(i = 0, ..., n - 1)$. 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 $r_1(x) = r_2(x)$.

3.13. 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,

$$p=[L:K]=[L:K(\theta)][K(\theta):K]. \tag{1}$$

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.

3.17. (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 $\mathbb{Q}$.

3.19. 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 1: $\beta \neq \alpha$. 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 3.13 (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

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

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 $\mathbb{Q}$.

3.20. 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) $x^2 - 4, \quad K = \mathbb{Q}.$ (b) $x^3 + x + 2, \quad K = \mathbb{Z}_3.$ (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 $Q(\alpha)$ 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.

3.21. 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) $\theta = u^2 + u + 1, \quad \mathbb{Q}(u)$, 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 $b \neq 0$ implicaria $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$ e $a, b \neq 0$ implicaria $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$!!!

(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.

3.23. 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 84 dos Apontamentos,

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

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
0	0	1	2	u	a	b	c	d	f
1	1	2	0	b	c	d	f	u	a
2	2	0	1	d	f	u	a	b	c
u	u	b	d	a	0	c	1	f	2
a	a	c	f	0	u	1	b	2	d
b	b	d	u	c	1	f	2	a	0
c	c	f	a	1	b	2	d	0	u
d	d	u	b	f	2	a	0	c	1
f	f	a	c	2	d	0	u	1	b

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

3.25. 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 $q(x)=x^6-6x^4+12x^2-10=0$. 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).

3.26. 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).

3.29. 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 $\Phi : L \to L$ transforma raízes deste polinómio em raízes do mesmo polinómio. Existem, pois, precisamente dois $\mathbb{Q}$-automorfismos:

$$\begin{array}{rccc} \Phi_{\sqrt{2}}: & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{2} & \mapsto & \sqrt{2} \end{array} \quad \text{e} \quad \begin{array}{rccc} \Phi_{-\sqrt{2}}: & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{2} & \mapsto & -\sqrt{2}. \end{array}$$

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 $\Phi : L \to L$ é completamente determinado pela sua acção no conjunto $\{\sqrt{2}, \sqrt{3}\}$. A restrição $\Phi|_{\mathbb{Q}(\sqrt{2})} : \mathbb{Q}(\sqrt{2}) \to L$ 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

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

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

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

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

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

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

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

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

3.30.

(a) Para as extensões L de $\mathbb{Q}$ do exercício anterior, calcule os respectivos grupos de Galois, $Gal(L, \mathbb{Q})$.

(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, $Gal(L, \mathbb{Q}) = \{id, \Phi_{-\sqrt{2}}\}$ é um grupo isomorfo a $\mathbb{Z}_2$.

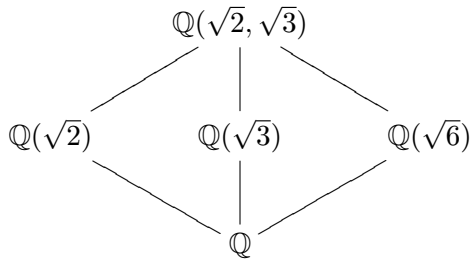
No segundo caso, o grupo de Galois tem 4 elementos, sendo a tabela do grupo a seguinte:

$\circ$	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.

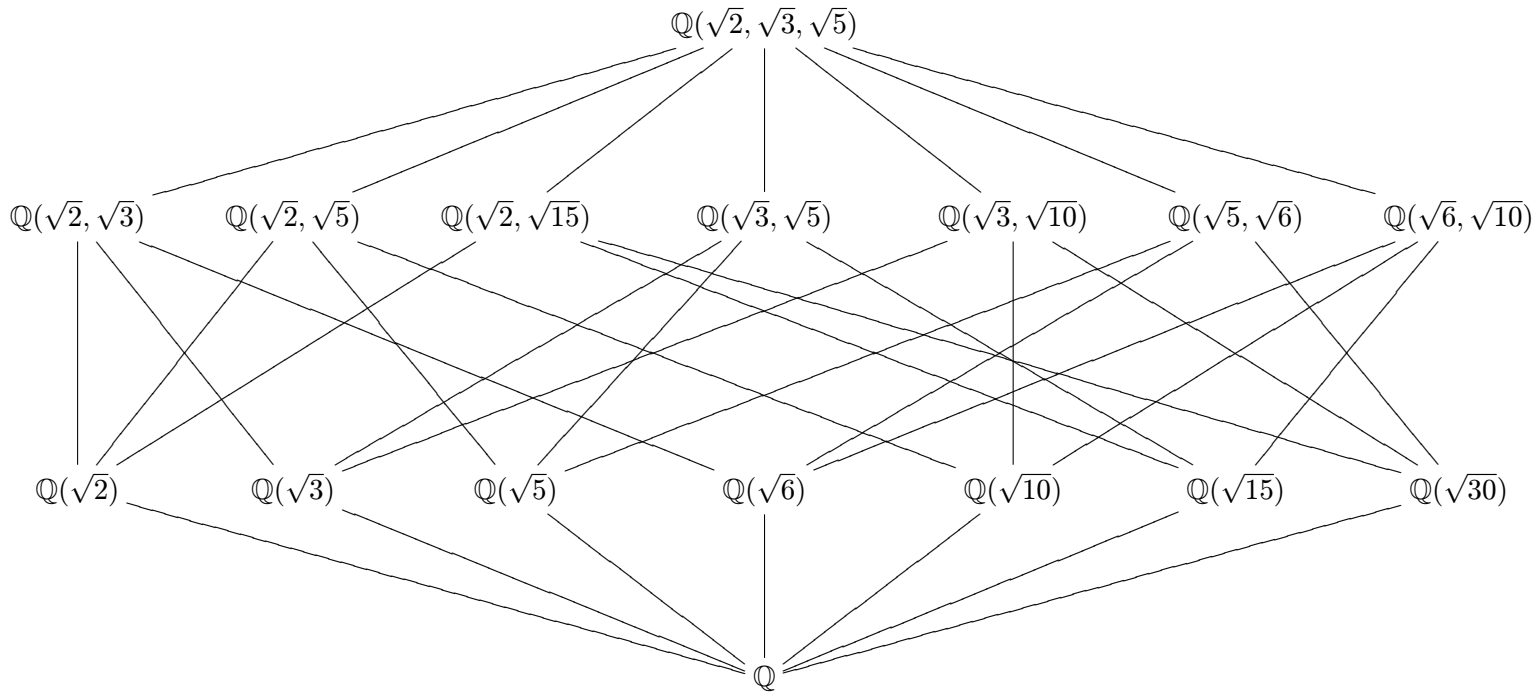
3.31.

(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:
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{6})$
$\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{10}) = \mathbb{Q}(\sqrt{5}, \sqrt{10})$
$\mathbb{Q}(\sqrt{2}, \sqrt{15}) = \mathbb{Q}(\sqrt{2}, \sqrt{30}) = \mathbb{Q}(\sqrt{15}, \sqrt{30})$
$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{15}) = \mathbb{Q}(\sqrt{5}, \sqrt{15})$
$\mathbb{Q}(\sqrt{3}, \sqrt{10}) = \mathbb{Q}(\sqrt{3}, \sqrt{30}) = \mathbb{Q}(\sqrt{10}, \sqrt{30})$
$\mathbb{Q}(\sqrt{5}, \sqrt{6}) = \mathbb{Q}(\sqrt{5}, \sqrt{30}) = \mathbb{Q}(\sqrt{6}, \sqrt{30})$
$\mathbb{Q}(\sqrt{6}, \sqrt{10}) = \mathbb{Q}(\sqrt{6}, \sqrt{15}) = \mathbb{Q}(\sqrt{10}, \sqrt{15})$.

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



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

3.32. 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 de Galois de $\mathbb{Q}$? Justifique.

(a) Seja $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$. Cada $\Phi \in Gal(L,\mathbb{Q})$ é completamente determinado pela sua acção no conjunto $\{\sqrt{3}, \sqrt[3]{2}\}$. A restrição $\Phi|_{\mathbb{Q}(\sqrt{3})} : \mathbb{Q}(\sqrt{3}) \to L$ 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

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

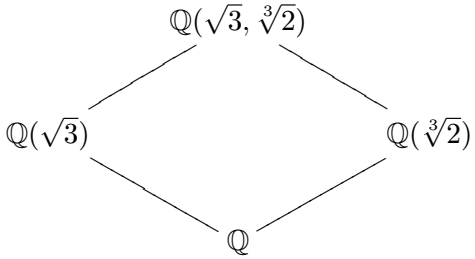
O grupo de Galois tem pois dois elementos:

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

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

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 de Galois de K).

3.42. Mostre que se $f(x)$ é um polinómio irredutível de grau 3, então $Gal(f(x),\mathbb{Q}) \cong \mathcal{A}_3$ ou $Gal(f(x),\mathbb{Q}) \cong \mathcal{S}_3$.

Ver solução do Exercício 3.43.

3.43. 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 $\Phi \in Gal(f(x),\mathbb{Q})$, então $\Phi(\sqrt{D}) = \sqrt{D}$ e, portanto, $Gal(f(x),\mathbb{Q}) \cong \mathcal{A}_3$.

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

(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,

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

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, $Gal(\mathbb{Q}(a,b,c),\mathbb{Q}) \cong \mathcal{S}_3$.

3.47. (a) Sejam p um número primo, e $f(x) \in \mathbb{Q}[x]$ um polinómio irredutível 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 3.28 (Teorema de Abel-Ruffini).

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

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

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

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

(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. A conclusão segue do Exercício 3.47 (a).

(b) este polinómio tem exactamente 4 raízes complexas não reais. A conclusão segue do Exercício 3.47 (b).

(c) tem exactamente 2 raízes complexas não reais. A conclusão segue do Exercício 3.47 (a).

(d) tem exactamente 2 raízes complexas não reais. A conclusão segue do Exercício 3.47 (a).

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

$$\frac{\mathbb{Z}_3[x]}{\langle x^2 - 2\rangle} = \{a_0 + a_1 x + \langle x^2 - 2\rangle \mid a_0, a_1 \in \mathbb{Z}_3\}.$$

Denotando o elemento $a_0 + a_1 x + \langle x^2 - 2\rangle$ por $a_0 a_1$, 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

$\cdot$	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.

Relembre a construção do corpo M nas páginas 88-90 dos Apontamentos. 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 irredutível sobre $\mathbb{F}_3$. Por exemplo, o polinómio $p(x) = x^3 + 2x + 1$. Seja L o corpo

$$\frac{\mathbb{Z}_3[x]}{\langle p(x)\rangle} = \{a_0 + a_1 x + a_2 x^2 + \langle p(x)\rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_3\}$$

constituído pelas 27 classes definidas pelos restos da divisão dos polinómios 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 a lista de corpos não isomorfos de ordem inferior a 100 é a seguinte:

$$\mathbb{F}_{p^n} \ : \ p \text{ primo}, n \in \mathbb{N}, \ p^n < 100.$$

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

4.13. Através de um comando à distância de uma televisão podem ser efectuadas 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	$\cdots$	9	10	11	$\cdots$	17	A	D
C_1	00	01	02	$\cdots$	09	10	11	$\cdots$	17	18	19
C_2	0000	0101	0202	$\cdots$	0909	1010	1111	$\cdots$	1717	1818	1919
C_3	00000	01011	02022	$\cdots$	09099	10109	11118	$\cdots$	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).

4.14. 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 000000, enquanto que a palavra correcta correspondente à mensagem 1011110 é 1011010.

4.17. 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: $(1,0,0,1,1)$.