

1. Pode existir um corpo com 6 elementos? E com 12 elementos? Quanto vale $1 + 1$ num corpo com 64 elementos?
2. Seja $K = \{0, 1, \alpha, \beta\}$ um corpo. Quanto valem $1 + 1$, $\alpha + \alpha$, $\beta + \beta$, $\alpha + 1$, $\beta + 1$, α^2 , β^2 e $\alpha \cdot \beta$? Construa as tabelas da adição e da multiplicação em K .
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 ?
4. Seja F a extensão de decomposição de $f(x) = x^{p^n} - x$ sobre \mathbb{F}_p .
 - (a) Mostre que o conjunto $R = \{a \in F \mid a^{p^n} = a\}$ das raízes de $f(x)$ é um subcorpo de F .
 - (b) Prove directamente, a partir da definição de raiz dupla, que todas as raízes de $f(x)$ são simples.
 - (c) Conclua que $R = F$.
5. Seja F um corpo com 81 elementos.
 - (a) Determine a característica de F , indique o seu corpo primo \mathbb{F}_p e determine $[F : \mathbb{F}_p]$.
 - (b) Justifique a afirmação “o único subcorpo próprio de F é o seu subcorpo primo”.
6. Construa um corpo finito de ordem 16 e determine todos os geradores do seu grupo multiplicativo.
7. Construa um corpo com 27 elementos.
8. Indique, justificando, o número de corpos não isomorfos de ordem inferior a 100.
9. Determine todos os subcorpos de um corpo com 32 e 64 elementos, respectivamente.
10. Liste os subcorpos do corpo \mathbb{F}_{256} . Qual deles é o subcorpo primo?
11. Usando resultados sobre corpos finitos, mostre que se p é um número primo e r divide n , então $p^r - 1$ divide $p^n - 1$.
12. Determine o número de elementos do corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$.
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 excepção de \mathbb{F}_2 , é 0.
14. Mostre que num código binário linear, ou todas as palavras têm peso par, ou metade das palavras tem peso par e metade tem peso ímpar.
15. 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	...	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.

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.

17. Seja \mathcal{C} um código binário de comprimento 7 com matriz

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

- (a) Mostre que a distância mínima de \mathcal{C} é 3.
 (b) Supondo que, no máximo, um erro singular é introduzido na transmissão, decodifique as mensagens 0010101 e 1000010.

18. Seja \mathcal{C} um código binário com matriz

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

- (a) Determine uma correspondência bijetiva entre líderes de classes laterais e síndromes.
 (b) Decodifique as seguintes mensagens: $r_1 = 10101$, $r_2 = 01111$, $r_3 = 11111$, $r_4 = 11100$.

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 controle.
 (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.
20. Para os códigos do Exercício ??, determine as síndromes e, se possível, corrija os erros das seguintes mensagens.
- (a) Código 1; mensagens: 00000, 11111, 01010.
- (b) Código 2; mensagens: 11011, 10011.
- (c) Código 3; mensagens: 1000000, 1110101.
21. Considere $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$, com $\alpha^4 = \alpha + 1$, e a matriz do código BCH

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}.$$

- (a) Faça uma estimativa para a distância mínima deste código.
- (b) Codifique a mensagem 1010101 e decodifique 110010110100110 e 100111000000000.
- (c) Mostre que se uma mensagem recebida r tem apenas um erro e esse erro é na posição i então $Hr = [\alpha^{i-1} \quad \alpha^{3(i-1)}]^T$.