Soluções de exercícios

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

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 $27 = 3\times3\times3$, 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 $\frac{\mathbb{Z}_3[x]}{\langle p(x)\rangle} = \{a_0 + a_1x + a_2x^2 + \langle p(x)\rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_3\}$ constituído pelas 27 classes definidas pelos restos da divisão dos 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 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 $11 \times 11 = 121$ polinómios 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 excepção 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	$\cdots$	$p-2$	$p-1$
1:	x	$x+1$	$\cdots$	$x+p-2$	$x+p-1$
	$2x$	$2x+1$	$\cdots$	$2x+p-2$	$2x+p-1$
	$\vdots$	$\vdots$		$\vdots$	$\vdots$
	$(p-2)x$	$(p-2)x+1$	$\cdots$	$(p-2)x+p-2$	$(p-2)x+p-1$
	$(p-1)x$	$(p-1)x+1$	$\cdots$	$(p-1)x+p-2$	$(p-1)x+p-1$
2:	x^2	x^2+1	$\cdots$	x^2+p-2	x^2+p-1
	x^2+x	x^2+x+1	$\cdots$	$x^2+x+p-2$	$x^2+x+p-1$
	x^2+2x	x^2+2x+1	$\cdots$	$x^2+2x+p-2$	$x^2+2x+p-1$
	$\vdots$	$\vdots$		$\vdots$	$\vdots$
	$x^2+(p-2)x$	$x^2+(p-2)x+1$	$\cdots$	$x^2+(p-2)x+p-2$	$x^2+(p-2)x+p-1$
	$x^2+(p-1)x$	$x^2+(p-1)x+1$	$\cdots$	$x^2+(p-1)x+p-2$	$x^2+(p-1)x+p-1$
	$2x^2$	$2x^2+1$	$\cdots$	$2x^2+p-2$	$2x^2+p-1$
	$2x^2+x$	$2x^2+x+1$	$\cdots$	$2x^2+x+p-2$	$2x^2+x+p-1$
	$2x^2+2x$	$2x^2+2x+1$	$\cdots$	$2x^2+2x+p-2$	$2x^2+2x+p-1$
	$\vdots$	$\vdots$		$\vdots$	$\vdots$
	$2x^2+(p-2)x$	$2x^2+(p-2)x+1$	$\cdots$	$2x^2+(p-2)x+p-2$	$2x^2+(p-2)x+p-1$
	$2x^2+(p-1)x$	$2x^2+(p-1)x+1$	$\cdots$	$2x^2+(p-1)x+p-2$	$2x^2+(p-1)x+p-1$
	$\vdots$	$\vdots$		$\vdots$	$\vdots$
n-1:	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

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 polinómios em cada linha é sempre igual a 0 pois, como p é ímpar, $1+2+\cdots+p-2+p-1$ é igual a

$$(1+p-1)+(2+p-2)+\cdots+(\frac{p-1}{2}+\frac{p+1}{2}) = p+p+\cdots+p = 0.$$

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 polinómios reduz-se a

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

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 polinómios de grau p^{n-1} é igual ao número de polinómios 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 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).

4.16. *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: $(1,0,0,1,1)$.