

6. POLJA GALOISA

1. U aditivnoj grupi $\mathbf{Z}_6 = (Z_6, +_6)$ odrediti ciklične podgrupe.

Rešenje. Formirajmo tablicu aditivne grupe $\mathbf{Z}_6 = (Z_6, +_6)$:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Iz tablice aditivne grupe \mathbf{Z}_6 zaključujemo da je posmatrana grupa izomorfna cikličnoj grupi \mathbf{C}_6 . Budući da podgrupa ciklične grupe može biti samo ciklična, imamo redom sledeće ciklične podgrupe:

$$\begin{aligned}
 \langle 0 \rangle &= (\{0\}, +_6) \cong \mathbf{C}_1, \\
 \langle 1 \rangle &= (\{0, 1, 2, 3, 4, 5\}, +_6) \cong \mathbf{C}_6, \\
 \langle 2 \rangle &= (\{0, 2, 4\}, +_6) \cong \mathbf{C}_3, \\
 \langle 3 \rangle &= (\{0, 3\}, +_6) \cong \mathbf{C}_2, \\
 \langle 4 \rangle &= (\{0, 2, 4\}, +_6) \cong \mathbf{C}_3, \\
 \langle 5 \rangle &= (\{0, 1, 2, 3, 4, 5\}, +_6) \cong \mathbf{C}_6.
 \end{aligned}$$

2. Nad $GF(2)$ odrediti sve ireducibilne polinome stepena 2 i 3.

Rešenje. Polazeći od $Z_2 = GF(2)$ primetimo da su polinomi stepena jedan dati kao polinomi x i $x + 1$. Oni su ujedno i ireducibilni polinomi. Svi polinomi stepena dva sa koeficijentima iz Z_2 su dati sledećom tablicom:

$$\begin{aligned}
 (1) \quad & x^2 + 0 \cdot x + 0 = x^2, \\
 & x^2 + 0 \cdot x + 1 = x^2 + 1, \\
 & x^2 + 1 \cdot x + 0 = x^2 + x, \\
 & x^2 + 1 \cdot x + 1 = \underline{x^2 + x + 1}.
 \end{aligned}$$

Formirajmo sve polinome stepena dva pomoću polinoma stepena jedan:

$$\begin{aligned}
 (2) \quad & x \cdot x = x^2, \\
 & x \cdot (x + 1) = x^2 + x, \\
 & (x + 1) \cdot (x + 1) = x^2 + 1.
 \end{aligned}$$

Na osnovu (1) i (2) zaključujemo da je polinom $x^2 + x + 1$ jedini nesvodljiv polinom drugog stepena. Svi polinomi stepena tri sa koeficijentima iz Z_2 su dati sledećom tablicom:

$$\begin{aligned}
 (3) \quad & x^3 + 0 \cdot x^2 + 0 \cdot x + 0 = x^3, \\
 & x^3 + 0 \cdot x^2 + 0 \cdot x + 1 = x^3 + 1, \\
 & x^3 + 0 \cdot x^2 + 1 \cdot x + 0 = x^3 + x, \\
 & x^3 + 0 \cdot x^2 + 1 \cdot x + 1 = \underline{x^3 + x + 1}, \\
 & x^3 + 1 \cdot x^2 + 0 \cdot x + 0 = x^3 + x^2, \\
 & x^3 + 1 \cdot x^2 + 0 \cdot x + 1 = \underline{x^3 + x^2 + 1}, \\
 & x^3 + 1 \cdot x^2 + 1 \cdot x + 0 = x^3 + x^2 + x, \\
 & x^3 + 1 \cdot x^2 + 1 \cdot x + 1 = x^3 + x^2 + x + 1.
 \end{aligned}$$

Formirajmo sve polinome stepena tri pomoću polinoma stepena jedan i svih polinoma stepena dva:

$$\begin{aligned}
 (4) \quad & x \cdot x^2 = x^3, \\
 & x \cdot (x^2 + 1) = x^3 + x, \\
 & x \cdot (x^2 + x) = x^3 + x^2, \\
 & x \cdot (x^2 + x + 1) = x^3 + x^2 + x, \\
 & (x + 1) \cdot x^2 = x^3 + x^2, \\
 & (x + 1) \cdot (x^2 + 1) = x^3 + x^2 + x + 1, \\
 & (x + 1) \cdot (x^2 + x) = x^3 + x, \\
 & (x + 1) \cdot (x^2 + x + 1) = x^3 + 1.
 \end{aligned}$$

Na osnovu (3) i (4) zaključujemo da su polinomi $x^3 + x + 1$ i $x^3 + x^2 + 1$ jedini ireducibilni polinomi trećeg stepena.

3. Nad $GF(3)$ odrediti sve ireducibilne polinome stepena 1 i 2.

Rešenje. Polazeći od $Z_3 = GF(3)$ primetimo da su polinomi stepena jedan dati kao polinomi x , $x + 1$ i $x + 2$. Oni su ujedno i ireducibilni polinomi. Svi polinomi stepena dva sa koeficijentima iz Z_3 su dati sledećom tablicom:

$$\begin{aligned}
 (1) \quad & x^2 + 0 \cdot x + 0 = x^2, \\
 & x^2 + 0 \cdot x + 1 = \underline{x^2 + 1}, \\
 & x^2 + 0 \cdot x + 2 = x^2 + 2, \\
 & x^2 + 1 \cdot x + 0 = x^2 + x, \\
 & x^2 + 1 \cdot x + 1 = x^2 + x + 1, \\
 & x^2 + 1 \cdot x + 2 = \underline{x^2 + x + 2}, \\
 & x^2 + 2 \cdot x + 0 = x^2 + 2x, \\
 & x^2 + 2 \cdot x + 1 = x^2 + 2x + 1, \\
 & x^2 + 2 \cdot x + 2 = \underline{x^2 + 2x + 2}.
 \end{aligned}$$

Formirajmo sve polinome stepena dva pomoću polinoma stepena jedan:

$$\begin{aligned}
 (2) \quad & x \cdot x = x^2, \\
 & x \cdot (x + 1) = x^2 + x, \\
 & x \cdot (x + 2) = x^2 + 2x, \\
 & (x + 1) \cdot (x + 1) = x^2 + 2x + 1, \\
 & (x + 1) \cdot (x + 2) = x^2 + 2, \\
 & (x + 2) \cdot (x + 2) = x^2 + x + 1.
 \end{aligned}$$

Na osnovu (1) i (2) zaključujemo da su polinomi $x^2 + 1$, $x^2 + x + 2$ i $x^2 + 2x + 2$ jedini ireducibilni polinomi drugog stepena.

4. Ispitati da li je polinom $x^4 + x^2 + 1$ svodljiv nad poljem $GF(4)$. Odrediti nule ovog polinoma u istom polju.

Rešenje. Konstruišimo polje $GF(4)$. Primitimo da polinomi stepena ne većeg od 1 sa koeficijentima iz $GF(2)$ su 0, 1, x i $x + 1$. Ispisivanjem svih mogućih faktorizacija:

$$\begin{aligned}x \cdot x &= x^2 \\x \cdot (x + 1) &= x^2 + x \\(x + 1) \cdot x &= x^2 + x \\(x + 1) \cdot (x + 1) &= x^2 + 1\end{aligned}$$

zaključujemo da je polinom $Q(x) = x^2 + x + 1$ nesvodljiv. Ako označimo $\alpha = x$ i $\beta = x + 1$, tada formirajmo po modulu nesvodljivog polinoma $Q(x)$ CAYLEYevu tablicu operacija \oplus i \odot :

\oplus	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

\odot	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Primitimo da su $(GF(4), \oplus)$ i $(GF(4) \setminus \{0\}, \odot)$ ciklične grupe. Dalje koristimo za \oplus i \odot uobičajne oznake $+$ i \cdot . Polinom $P(x) = x^4 + x^2 + 1$ je svodljiv jer važi:

$$P(x) = x^4 + x^2 + 1 = x^4 + x^2 + 1^2 + 2x^4 \cdot x^2 + 2x^4 \cdot 1^2 + 2x^2 \cdot 1^2 = (x^2 + x + 1)^2 = Q(x)^2.$$

Iz tablice:

1	x	x^2	$Q(x)$	$P(x)$
1	0	0	1	1
1	1	1	1	1
1	α	β	0	0
1	β	α	0	0

zaključujemo da polinom $P(x)$ ima dve nule u tom polju: $x_1 = \alpha$ i $x_2 = \beta$.

5. U multiplikativnoj grupi polja $GF(8)$ odrediti elemente koji su sami sebi inverzni (reprezentovati $GF(8)$ kao algebru polinoma po modulu nesvodljivog polinoma $x^3 + x + 1$ u $GF(2)$).

Rešenje. I način. Multiplikativna grupa polja $GF(8)$ je ciklična grupa sa 7 elemenata: 1, x , $x + 1$, x^2 , $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$. Svi elementi sem jediničnog elementa 1 te grupe su reda 7. Odatle je jedinični element 1 jedini sam sebi inverzan.

II način. Glavna dijagona CAYLEYjeve tablice multiplikativne grupe je data sledećim zapisom:

\odot	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2					
$x+1$	$x+1$		x^2+1				
x^2	x^2			x^2+x			
x^2+1	x^2+1				x^2+x+1		
x^2+x	x^2+x					x	
x^2+x+1	x^2+x+1						$x+1$

Odatle jedinični element 1 te grupe je jedini sam sebi inverzan.

6. Neka je dato polje GALOISA $GF(m)$. Odrediti dva međusobno različita polinoma nad posmatranim poljem koji imaju iste vrednosti za svaku vrednost nezavisne promenljive. Neka su $P_k(x)$ i $Q_n(x)$ dva proizvoljna polinoma nad poljem $GF(m)$ stepena k i n respektivno, pri čemu je ispunjeno: $m > \max\{k, n\}$. Dokazati da su polinomi $P_k(x)$ i $Q_n(x)$ sa jednakim koeficijentima ako i samo ako imaju iste vrednosti za svaki element $x \in GF(m)$.

Rešenje. Budući da je multiplikativna grupa polja $GF(m)$ ciklična važi: $x^{m-1} = 1$. Odatle polinom $P_m(x) = x^m$ i $Q_1(x) = x$ imaju iste vrednosti za svaki element $x \in GF(m)$. Dalje neka su $P_k(x)$ i $Q_n(x)$ dva proizvoljna polinoma nad poljem $GF(m)$ stepena k i n respektivno, pri čemu je ispunjeno: $m > \max\{k, n\}$. Ako su polinomi $P_k(x)$ i $Q_n(x)$ sa jednakim koeficijentima tada oni imaju iste vrednosti za svaki element $x \in GF(m)$. Obratno neka je ispunjeno: $P_k(x) = Q_n(x)$ za svaki element $x \in GF(m)$. Tada ako polinomi $P_k(x)$ i $Q_n(x)$ nisu sa jednakim koeficijentima posmatrajmo nenulti polnom $H(x) = P_k(x) - Q_n(x)$ koji ima m nula jer ga anuliraju svi elementi $x \in GF(m)$. Odatle je $H(x) = P_k(x) - Q_n(x)$ sa jedan strane stepena m , a sa druge strane je stepena $\max\{k, n\}$. Budući da je $m > \max\{k, n\}$ svodjenjem na kontradikciju dokazano je tvrđenje.

7. Dokazati savršenost sledećeg linearanog koda u \mathbf{Z}_3 :

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}$$

(kodne reči su određene kolonama). Odrediti generatorsku matricu koda.

Rešenje. Neka je $\mathcal{A} = \mathbf{Z}_3 = \{0, 1, 2\}$ i neka je kod C koji se sastoji od prethodno određenih kodnih reči $A_i = (a_{1i}, a_{2i}, a_{3i}, a_{4i}) \in \mathcal{A}^4$ ($i = 1, \dots, 9$). Navedene kodne reči ispunjavaju uslov:

$$(\forall i, j) d(A_i, A_j) = 3$$

jer se svake dve reči koda C razlikuju na tačno 3 pozicije. Dalje, neka je kodna reč $A'_i = (a_{1i}, a_{2i}, a_{3i}, a_{4i})$ u kugli $K_i = K[A_i, 1]$ sa centrom u kodnoj reči A_i i poluprečnikom 1 ($i = 1, \dots, 9$). Tada svaka kugla K_i obuhvata:

$$\underset{(a'_{1i} \neq a_{1i})}{2} + \underset{(a'_{2i} \neq a_{2i})}{2} + \underset{(a'_{3i} \neq a_{3i})}{2} + \underset{(a'_{4i} \neq a_{4i})}{2} + \underset{(A_i = A'_i)}{1} = 9$$

raznih reči ($i = 1, \dots, 9$). Odatle, na osnovu činjenice da važi:

$$|\bigcup_{i=1}^9 K_i| = 9 \cdot 9 = 81 = 3^4 = |\mathcal{A}^4|,$$

zaključujemo da je linearan kod C savršen. Budući da su kodne reči $A_2 = (0, 1, 2, 1)$ i $A_3 = (0, 2, 1, 2)$ linearno nezavisne tada jedna generatorska matrica linearnog koda C data na sledeći način:

$$M = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 0 & 2 & 1 & 2 \end{bmatrix}.$$