Diskretna matematika 2

Zadaća 10

March 20, 2025

Borna Gojšić

---

1. a) Dokažite da je polinom $g(t) = t^2 + t + 1$ ireducibilan nad $\mathbb{Z}_2$.
   b) Odredite jedan generator multiplikativne grupe $\mathbb{F}_4^*$ polja $\mathbb{F}_4$ reprezentiranog kao $\mathbb{Z}_2[t]/(g(t))$.
   c) Je li aditivna grupa $\mathbb{F}_4$ izomorfna grupi $\mathbb{Z}_4$ ili $\mathbb{Z}_2 \times \mathbb{Z}_2$? Sve svoje tvrdnje dokažite.

Rj:

a) Očito je $g(0) = g(1) = 1$, pa $g(t)$ nema nultočaka u $\mathbb{Z}_2$. Dakle, $g(t)$ je ireducibilan nad $\mathbb{Z}_2$.

b) Svi elementi od $\mathbb{F}_4$ su $0, 1, t, t+1$. Neka je $a = t$. Tada je $a^2 = t^2 = -t - 1 = t + 1$ te je $a^3 = t^3 = t(t^2) = t(t+1) = t^2 + t = -1 = 1$. Dakle, a je generator multiplikativne grupe $\mathbb{F}_4^*$.

c) Neka je $\varphi : \mathbb{F}_4 \to \mathbb{Z}_4$ homomorfizam grupa. Tada je $\varphi(0) = 0$ jer je to neutralni element. Tada imamo

$$\varphi(0) = \varphi(1+1) = \varphi(1) + \varphi(1) = 2\varphi(1) = 0$$
$$\varphi(0) = \varphi(t+t) = \varphi(t) + \varphi(t) = 2\varphi(t) = 0$$

ali jedini elementi koji zadovoljavaju $2x = 0$ u $\mathbb{Z}_4$ su 0 i 2. Dakle, φ nije injekcija pa nije ni izomorfizam. S druge strane, $\mathbb{Z}_2 \times \mathbb{Z}_2$ ima elemente $(0,0), (0,1), (1,0), (1,1)$ te je jasno da je $\mathbb{F}_4$ izomorfna $\mathbb{Z}_2 \times \mathbb{Z}_2$. Npr. imamo $f : \mathbb{F}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ dan s $f(at + b) = (a, b)$ što je izomorfizam grupa.

2. a) Dokažite da je polinom $g(t) = t^3 + t^2 + 1$ ireducibilan nad $\mathbb{Z}_2$.
   b) Koliko generatora ima multiplikativna grupa $\mathbb{F}_8^*$ polja $\mathbb{F}_8$ reprezentiranog kao $\mathbb{Z}_2[t]/(g(t))$?
   c) Koliki je red elementa $t^2 + 1$ u $\mathbb{F}_8^*$?
   d) Odredite inverz elementa $t^2 + t + 1$ u $\mathbb{F}_8^*$.

Rj:

a) Očito je $g(0) = g(1) = 1$, pa $g(t)$ nema nultočaka u $\mathbb{Z}_2$. Dakle, $g(t)$ je ireducibilan nad $\mathbb{Z}_2$.

b) Grupa $\mathbb{F}_8^*$ ima točno $\varphi(8-1) = 6$ generatora.

c) Budući da je jedini ne generator u $\mathbb{F}_8^*$ element 1, red elementa $t^2 + 1$ je $8 - 1 = 7$.

d)

$$t^2 + t + 1 = (t^3 - 1)(t-1)^{-1} = (t^2)(t-1)^{-1} \implies (t^2 + t + 1)^{-1} = (t-1)(t^2)^{-1}$$

Nadalje,

$$(t^2)(t+1) = t^3 + t^2 = 1 \implies (t^2)^{-1} = t + 1$$

Dakle, $(t^2 + t + 1)^{-1} = (t-1)(t^2)^{-1} = (t-1)(t+1) = t^2 - 1 = t^2 + 1$.

3. a) Dokažite da je $t+1$ generator multiplikativne grupe $\mathbb{F}_{16}^*$ polja $\mathbb{F}_{16}$ reprezentiranog kao $\mathbb{Z}_2[t]/(h(t))$, gdje je $h(t) = t^4 + t + 1$ polinom ireducibilan nad $\mathbb{Z}_2$. Obrazložite!
   b) Je li $t^3 + t^2 + t + 1$ generator od $\mathbb{F}_{16}^*$?
   c) Odredite inverz elementa $t^3 + t^2 + t + 1$ u $\mathbb{F}_{16}^*$.

Rj:

a) Neka je $a = t + 1$. Moramo provjeriti a^d za sve d djelitelje od $16 - 1 = 15$. Dakle, imamo $d \in \{1, 3, 5\}$.

$$\begin{aligned}
a^1 &= t + 1 \\
a^2 &= (t+1)^2 = t^2 + 2t + 1 = t^2 + 1 \\
a^3 &= (t+1)^3 = (t+1)(t^2+1) = t^3 + t^2 + t + 1 \\
a^4 &= (t^2+1)^2 = t^4 + 2t^2 + 1 = t^4 + 1 = t \\
a^5 &= t(t+1) = t^2 + t
\end{aligned}$$

Dakle, $t + 1$ je generator multiplikativne grupe $\mathbb{F}_{16}^*$.

b) Budući da je $t^3 + t^2 + t + 1 = a^3$, a je generator i $3 \mid 15$, $t^3 + t^2 + t + 1$ nije generator.

c) Budući da je $t^3 + t^2 + t + 1 = a^3$ i $a^{15} = 1$, inverz elementa $t^3 + t^2 + t + 1$ je

$$\begin{aligned}
a^{12} = (a^5)^2 \cdot a^2 &= (t^2 + t)^2 \cdot (t^2 + 1) = (t^4 + 2t^3 + t^2) \cdot (t^2 + 1) = (t^4 + t^2) \cdot (t^2 + 1) \\
&= t^2(t^2 - 1)(t^2 + 1) = t^2(t^4 + 1) = t^2 \cdot t = t^3
\end{aligned}$$

4. a) Dokažite da je polinom $h(t) = t^2 + t + 2$ ireducibilan nad $\mathbb{Z}_3$.
   b) Dokažite da je $t+1$ generator multiplikativne grupe $\mathbb{F}_9^*$ polja $\mathbb{F}_9$ reprezentiranog kao $\mathbb{Z}_3[t]/(h(t))$, gdje je $h(t) = t^2 + t + 2$.
   c) Odredite preostale generatore multiplikativne grupe $\mathbb{F}_9^*$.
   d) Odredite inverz elementa $2t + 1$ u $\mathbb{F}_9^*$.
   e) Odredite podgrupu od $\mathbb{F}_9^*$ generiranu elementom $t + 2$.

Rj:

a) Imamo $h(0) = h(2) = 2$ i $h(1) = 1$ pa $h(t)$ nema nultočaka u $\mathbb{Z}_3$. Dakle, $h(t)$ je ireducibilan nad $\mathbb{Z}_3$.

b) Neka je $a = t + 1$. Moramo provjeriti a^d za sve d djelitelje od $9 - 1 = 8$. Dakle, imamo $d \in \{1, 2, 4\}$.

$$\begin{aligned}
a^1 &= t + 1 \\
a^2 &= (t+1)^2 = t^2 + 2t + 1 = t - 1 = t + 2 \\
a^4 &= (t+2)^2 = t^2 + 4t + 4 = t^2 + t + 1 = 2
\end{aligned}$$

Dakle, $t + 1$ je generator multiplikativne grupe $\mathbb{F}_9^*$.

c) Preostale generatore dobivamo kao a^m gdje je $\text{nzd}(m, 8) = 1$. Dakle, imamo $m \in \{3, 5, 7\}$.

$$\begin{aligned}
a^3 &= (t+2)(t+1) = t^2 + 3t + 2 = t^2 + 2 = -t = 2t \\
a^5 &= 2 \cdot (t+1) = 2t + 2 \\
a^7 &= 2(2t) = 4t = t
\end{aligned}$$

d) Budući da je $2t + 1 = -(t+2) = -a^2$, inverz elementa $2t + 1$ je

$$-a^6 = -a^4 \cdot a^2 = -2 \cdot (t+2) = t + 2$$

e) Podgrupa generirana elementom $t + 2$ je $\{1, t+2, 2, 2t+1\}$.

5. Odredite produkt polinoma p i q u polju $\mathbb{F}_{2^8}$ definiranom kao $\mathbb{Z}_2[t]/(t^8 + t^4 + t^3 + t + 1)$ te prikažite polinome p, q i njihov produkt u heksadecimalnom zapisu ako je:
   a) $p(x) = x^6 + x^5 + x^3 + x^2 + 1$, $q(x) = x^5 + x^3 + x^2 + x + 1$,
   b) $p(x) = x^7 + x^5 + x^4 + x^2 + x + 1$, $q(x) = x^7 + x^5 + x^4 + x^2 + x$.

Rj: Znamo da je $t^8 + t^4 + t^3 + t + 1 = 100011011 = 11B_{16}$.

a) Polinomi p i q su $p = 01101101 = 6D_{16}$ i $q = 00101111 = 2F_{16}$. Njihov produkt je

$$\begin{aligned}
p(x) \cdot q(x) &= x^{11} + x^{10} + x^9 + 3x^8 + 3x^7 + 3x^6 + 4x^5 + 2x^4 + 3x^3 + 2x^2 + x + 1 \\
&= x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^3 + x + 1 = 111111001011 \\
&= 111111001011 \oplus 100011011000 = 11100010011 \\
&= 11100010011 \oplus 10001101100 = 1101111111 \\
&= 1101111111 \oplus 1000110110 = 101001001 \\
&= 101001001 \oplus 100011011 = 01010010 = 52_{16} = x^6 + x^4 + x
\end{aligned}$$

b) Polinomi p i q su $p = 10110111 = B7_{16}$ i $q = 10110110 = B6_{16}$. Njihov produkt je

$$\begin{aligned}
p(x)q(x) &= x^{14} + 2x^{12} + 2x^{11} + x^{10} + 4x^9 + 3x^8 + 3x^7 + 4x^6 + 3x^5 + 2x^4 + 2x^3 + 2x^2 + x \\
&= x^{14} + x^{10} + x^8 + x^7 + x^5 + x = 100010110100010 \\
&= 100010110100010 \oplus 100011011000000 = 1101100010 \\
&= 1101100010 \oplus 1000110110 = 101010100 \\
&= 101010100 \oplus 100011011 = 01001111 = 4F_{16} = x^6 + x^3 + x^2 + x + 1
\end{aligned}$$

6. Odredite parametre a, b, c takve da polinom $p(x) = x^6 + ax^4 + bx^3 + cx^2 + x + 1$ bude inverz polinoma $q(x) = x^3 + 1$ u polju $\mathbb{F}_{2^8}$ reprezentiranom kao $\mathbb{Z}_2[t]/(h(t))$, gdje je $h(t) = t^8 + t^4 + t^3 + t + 1$ polinom ireducibilan nad $\mathbb{Z}_2$.

Rj:

$$\begin{aligned}
1 = p(x) \cdot q(x) &= x^9 + ax^7 + bx^6 + cx^5 + x^4 + x^3 + x^6 + ax^4 + bx^3 + cx^2 + x + 1 \\
&= x^9 + ax^7 + (b+1)x^6 + cx^5 + (a+1)x^4 + (b+1)x^3 + cx^2 + x + 1 \\
&= x(x^4 + x^3 + x + 1) + ax^7 + (b+1)x^6 + cx^5 + (a+1)x^4 + (b+1)x^3 + cx^2 + x + 1 \\
&= x^5 + x^4 + x^2 + x + ax^7 + (b+1)x^6 + cx^5 + (a+1)x^4 + (b+1)x^3 + cx^2 + x + 1 \\
&= ax^7 + (b+1)x^6 + (c+1)x^5 + ax^4 + (b+1)x^3 + (c+1)x^2 + 1 \implies a = 0, b = 1, c = 1
\end{aligned}$$

Dakle, inverz polinoma $q(x)$ je $x^6 + x^3 + x^2 + 1$.