

DISKRETINĖS MATEMATIKOS

Išankstinis egzaminas
1999.12.15, trečiadienis

1. Raskite vieneto šaknų grupės E_{30} eilę virš kūno $GF(8)$.
2. Pateikite primityviosios 30-ojo laipsnio vieneto šaknies virš kūno $GF(8)$ apibrėžimą. Kiek jų yra ?
3. Pateikite primityvaus baigtinio kūno $GF(q)$ elemento apibrėžimą. Kiek jų yra ?
4. Raskite polinomo $x^5 - 1 \in GF(7)[x]$ skaidymo kūną.
5. Virš kokio kūno primityviosios 5-ojo laipsnio vieneto šaknys virš kūno $GF(7)$ yra taip pat ir primityvūs kūno elementais.
6. Raskite skaičiaus 7 ciklotomines aibes moduliu 5.
7. Ką galite pasakyti apie polinomo $x^5 - 1$ skaidinį virš $GF(7)$?
8. Kiek neredukuojamų polinomų ir kokie jų laipsniai ciklotominio polinomo $Q_5(x) \in GF(7)[x]$ kanoniniame skaidinyje ?
9. Polinomas $x^6 + x + 2$ yra neredukuojamas virš kūno $GF(3)$. Ar bus šis polinomas neredukuojamas virš kūno $GF(81)$? Atsakymą pagrįskite.
10. Jeigu polinomas iš 9. yra neredukuojamas virš $GF(81)$, tai nurodykite bent du kūnus virš kurių jis liks neredukuojamu ir tris kūnus virš kurių jis taps redukuojamu ir nurodykite neredukuojamų polinomų skaičių kanoniniuose šio polinomo skaidiniuose virš šių kūnų.
Jeigu polinomas iš 9. yra redukuojamas virš $GF(81)$, tai nurodykite bent tris kūnus virš kurių jis taps neredukuojamu ir du kūnus virš kurių jis liks redukuojamu ir nurodykite neredukuojamų polinomų skaičių kanoniniuose šio polinomo skaidiniuose virš šių kūnų.

DISKRETIŅĒS MATEMATIKOS

Išankstinis egzaminas
1999.12.15, trečiadienis
Atsakymai

1. $m = 15$, nes $30 = 15 \cdot 2$.
2. 12.3 apibrėžimas. Jū yra $\varphi(15)$.
3. Tai generuojantis multiplikacinę grupę $GF(q)^*$ elementas. Jū yra $\varphi(q - 1)$.
4. $GF(7^4)$, nes $\text{ord}_5(7) = 4$.
5. Virš polinomo skaidymo kūno $GF(7^4)$.
6. $C_0 = \{0\}$, $C_1 = \{1, 2, 3, 4\}$.
7. Polinomo skaidinyje vienas pirmojo ir vienas ketvirtojo laipsnio neredukuojamas polinomas.
8. Vienas ketvirtojo laipsnio neredukuojamas polinomas.
9. Polinomas yra redukuojamas, nes $BDD(6, 4) = 2 > 1$.
10. Virš kūno $GF(81)$ polinomo kanoniame skaidinyje du trečiojo laipsnio polinomai.