

Matematik, KTH

B.Ek

Svarsförslag för lappskrivning 3B, torsdag 4 december 2014
i SF1630(/1631) Diskret matematik, för D (m.fl.)

(Tryckfel kan förekomma.)

a-versionen (b-versionen på andra sidan):

a1a. (1p) Karakteristiken för en ändlig kropp F är det minsta $p \in \mathbb{N} \setminus \{0\}$ som uppfyller $\underbrace{1 + 1 + \dots + 1}_{p \text{ st}} = 0$ i F , dvs den additiva ordningen för elementet 1.

a1b. (1p) $f(x) \in F[x]$ med $\deg f(x) = n$ kan inte ha fler nollställen än n (ty enligt faktorsatsen innehåller $f(x)$ faktorn $x - \alpha$ för varje nollställe α). Om $k \leq n$ och $\alpha_i \in F$ är olika för $i = 1, 2, \dots, k$ har polynomet $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)^{n-k+1}$ grad n och precis k olika nollställen. Det visar att alla värden $1, 2, \dots, \min(|F|, n)$ är möjliga ($\min(|F|, n)$ är det minsta av $|F|$ och n).

a1c. (1p) Eftersom $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp av ordning $n-1$ förekommer alla positiva delare till $n-1$ som ordningar bland dess element (om a har ordning $n-1$ och $d \mid (n-1)$, $d > 0$, har $a^{\frac{n-1}{d}}$ ordning d).

a1d. (1p) Ett polynom $f(x) \in F[x]$ är irreducibelt precis om det är av grad minst 1 och det inte kan faktoriseras i två polynom av grad ≥ 1 . Alternativt: om $f(x) = g(x)h(x)$ ($g(x), h(x) \in F[x]$) måste precis en av $g(x)$ och $h(x)$ vara en konstant.

a2. $k(x) = x^3 + 4x + 1 \in \mathbb{Z}_5[x]$ och $R = \mathbb{Z}_5[x]/(k(x))$.

Vi söker (a, 1p) $|R|$, (b, 1p) $[2x^2 + 4x + 1] + [4x^2 + 3x + 2]$,

(c, 1p) $[2x^2 + 4x + 1] \cdot [4x + 3]$ och (d, 1p) nolldelare i R .

Lösning: a. Antalet element i R = antalet polynom av grad ≤ 2 i $\mathbb{Z}_5[x]$ (ty varje ekvivalensklass innehåller precis ett polynom med grad $< \deg k(x)$), så $|R| = 5^3 = 125$.

b. $[2x^2 + 4x + 1] + [4x^2 + 3x + 2] = [(2x^2 + 4x + 1) + (4x^2 + 3x + 2)] = [x^2 + 2x + 3]$.

c. $[2x^2 + 4x + 1] \cdot [4x + 3] = [(2x^2 + 4x + 1)(4x + 3)] = [3x^3 + 2x^2 + x + 3] = [3x^3 + 2x + 3] + [2x^2 + 4x] = [2x^2 + 4x + 3 \cdot k(x)] = [2x^2 + 4x]$.

d. Nolldelare i R motsvarar icke-trivial faktorisering av $k(x)$.

$k(0) = 1$, $k(1) = 1$, $k(2) = 2$, men $k(3) = 0$, så $(x - 3) = (x + 2) \mid k(x)$. Division ger $k(x) = (x + 2)(x^2 + 3x + 3)$, så $[x + 2] \cdot [x^2 + 3x + 3] = [0]$ i R .

Svar a: $|R| = 125$, b: $[x^2 + 2x + 3]$, c: $[2x^2 + 4x]$,

d: $[x + 2]$ och $[x^2 + 3x + 3]$ är nolldelare i R .

b-versionen:

b1a. (1p) De möjliga värdena för $|F|$ då F är en ändlig kropp är p^r , där p är ett primtal och $r \in \mathbb{N} \setminus \{0\}$ (dvs det är ett positivt heltal).

b1b. (1p) Då $(F, +, \cdot)$ är en ändlig kropp av karakteristik p har identitets-elementet 0 den additiva ordningen 1 och elementet 1 har ordning $p \neq 1$. Om $a \in F \setminus \{0\}$ är $\underbrace{a + \dots + a}_{k \text{ st}} = \underbrace{(1 + \dots + 1)}_{k \text{ st}} \cdot a = 0$ omm $\underbrace{1 + \dots + 1}_{k \text{ st}} = 0$, så a har ordning p . Antalet värden för ordningen är alltså två (1 och p).

b1c. (1p) Ett primitivt element i en ändlig kropp F är en generator för gruppen $(F \setminus \{0\}, \cdot)$ (som alltid är cyklisk).

b1d. (1p) Om F är en kropp och $k(x)$ ett polynom i $F[x]$ är ringen $F[x]/(k(x))$ en kropp precis om $k(x)$ är irreducibelt.

b2. $k(x) = x^3 + 4x + 4 \in \mathbb{Z}_5[x]$ och $R = \mathbb{Z}_5[x]/(k(x))$.

Vi söker (a, 1p) $|R|$, (b, 1p) $[2x^2 + 3x + 2] + [4x^2 + 2x + 4]$,

(c, 1p) $[2x^2 + 3x + 2] \cdot [4x + 2]$ och (d, 1p) nolldelare i R .

Lösning: a. Antalet element i $R =$ antalet polynom av grad ≤ 2 i $\mathbb{Z}_5[x]$ (ty varje ekvivalensklass innehåller precis ett polynom med grad $< \deg k(x)$), så $|R| = 5^3 = 125$.

b. $[2x^2 + 3x + 2] + [4x^2 + 2x + 4] = [(2x^2 + 3x + 2) + (4x^2 + 2x + 4)] = [x^2 + 1]$.

c. $[2x^2 + 3x + 2] \cdot [4x + 2] = [(2x^2 + 3x + 2)(4x + 2)] = [3x^3 + x^2 + 4x + 4] = [(3x^3 + 2x + 2) + x^2 + 2x + 2] = [x^2 + 2x + 2 \cdot k(x)] = [x^2 + 2x + 2]$.

d. Nolldelare i R motsvarar icke-trivial faktorisering av $k(x)$.

$k(0) = 4$, $k(1) = 4$, men $k(2) = 0$, så $(x - 2) = (x + 3) \mid k(x)$. Division ger $k(x) = (x + 3)(x^2 + 2x + 3)$, så $[x + 3] \cdot [x^2 + 2x + 3] = [0]$ i R .

Svar a: $|R| = 125$, **b:** $[x^2 + 1]$, **c:** $[x^2 + 2x + 2]$,

d: $[x + 3]$ och $[x^2 + 2x + 3]$ är nolldelare i R .
