

Svarsförslag för lappskrivning 3B, onsdag 30 november 2016
i SF1630(/SF1631) Diskret matematik, för D (m.fl.)

(Tryckfel kan förekomma.)

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

a1a. (1p) Då $f(x) = 3x^3 + 2x^2 + 4$ delas med $g(x) = x^2 + 4x + 2$ i $\mathbb{Z}_7[x]$ blir kvoten $3x + 4$ och resten $6x + 3$, ty $3x^3 + 2x^2 + 4 - 3x(x^2 + 4x + 2) = 4x^2 + x + 4$ och $4x^2 + x + 4 - 4(x^2 + 4x + 2) = 6x + 3$.

a1b. (1p) Karakteristiken för en ändlig kropp F är det minsta $p \in \mathbb{Z}_+$ som uppfyller $\underbrace{1 + 1 + \dots + 1}_{p \text{ st}} = 0$ i F , dvs den additiva ordningen för elementet 1.

a1c. (1p) Faktorsatsen säger att om $f(x) \in F[x]$, där F är en kropp, gäller för alla $\alpha \in F$ att $(x - \alpha) \mid f(x)$ omm $f(\alpha) = 0$.

a1d. (1p) $0^{21} = 0 \neq 1$ och $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp med 63 element. Eftersom $21 \mid 63$ uppfylls $x^{21} = 1$ enligt känd sats av **precis 21 element i F** .

a2. (4p) $R = \{c_2\alpha^2 + c_1\alpha + c_0 \mid c_2, c_1, c_0 \in \mathbb{Z}_5\}$, där $\alpha \notin \mathbb{Z}_5$ uppfyller $(\alpha + 1)(\alpha^2 + 1) = 3\alpha + 4$. Vi ska avgöra om $(R, +, \cdot)$ är en kropp.

Lösning: $(\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1 = 3\alpha + 4$ ger $\alpha^3 + \alpha^2 + 3\alpha + 2 = 0$, så $R = \mathbb{Z}_5[x]/(k(x))$ med $k(x) = x^3 + x^2 + 3x + 2$. R är en kropp omm $k(x)$ är irreducibelt. $k(0) = 2$, $k(1) = 2$, $k(2) = 0$, så $k(x)$ är (faktorsatsen) delbart med $x - 2 = x + 3$ och alltså reducibelt. R är således inte en kropp.

Svar: R är inte en kropp.

b-versionen:

b1a. (1p) Karakteristiken för en ändlig kropp F är det minsta $p \in \mathbb{Z}_+$ som uppfyller $\underbrace{1 + 1 + \dots + 1}_{p \text{ st}} = 0$ i F , dvs den additiva ordningen för elementet 1.

b1b. (1p) Då $f(x) = 4x^3 + x^2 + 2$ delas med $g(x) = x^2 + 3x + 4$ i $\mathbb{Z}_7[x]$ blir kvoten $4x + 3$ och resten $3x + 4$, ty $4x^3 + x^2 + 2 - 4x(x^2 + 3x + 4) = 3x^2 + 5x + 2$ och $3x^2 + 5x + 2 - 3(x^2 + 3x + 4) = 3x + 4$.

b1c. (1p) $0^{20} = 0 \neq 1$ och $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp med 80 element. Eftersom $20 \mid 80$ uppfylls $x^{20} = 1$ enligt känd sats av **precis 20 element i F** .

b1d. (1p) Faktorsatsen säger att om $f(x) \in F[x]$, där F är en kropp, gäller för alla $\alpha \in F$ att $(x - \alpha) \mid f(x)$ omm $f(\alpha) = 0$.

b2. (4p) $R = \{c_2\alpha^2 + c_1\alpha + c_0 \mid c_2, c_1, c_0 \in \mathbb{Z}_5\}$, där $\alpha \notin \mathbb{Z}_5$ uppfyller $(\alpha + 1)(\alpha^2 + 1) = 4\alpha + 2$. Vi ska avgöra om $(R, +, \cdot)$ är en kropp.

Lösning: $(\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1 = 4\alpha + 2$ ger $\alpha^3 + \alpha^2 + 2\alpha + 4 = 0$, så $R = \mathbb{Z}_5[x]/(k(x))$ med $k(x) = x^3 + x^2 + 2x + 4$. R är en kropp omm $k(x)$ är irreducibelt. $k(0) = 4$, $k(1) = 3$, $k(2) = 0$, så $k(x)$ är (faktorsatsen) delbart med $x - 2 = x + 3$ och alltså reducibelt. R är således inte en kropp.

Svar: R är inte en kropp.
