

Lösningssförslag ls3B, SF1630 Diskret matematik, 23 november 2012

a1) Vi skall faktorisera polynomet $f(x) = x^4 + 2x^2 + 2x + 2$ i irreducibla faktorer i $\mathbb{Z}_3[x]$.

Lösning:

För att undersöka om $f(x)$ har någon förstgradsfaktor söker vi först nollställen. $f(0) = 2$, $f(1) = 1$, men $f(2) = 0$, så $x - 2 = x + 1$ är en faktor i $f(x)$. Division ger $f(x) = (x + 1)g(x)$, där $g(x) = x^3 + 2x^2 + 2$. Eftersom $f(0), f(1) \neq 0$ är $g(0), g(1) \neq 0$, men man finner att $g(2) = 0$, så $x + 1$ delar också $g(x)$. Division ger $g(x) = (x + 1)h(x)$, där $h(x) = x^2 + x + 2$. ($h(0), h(1) \neq 0$ och $h(2) = 2$, så $h(x)$ är irreducibelt (andragradspolynom utan nollställen är irreducibla), så en sökt faktorisering är $f(x) = (x + 1)^2(x^2 + x + 2)$.

Svar: $f(x) = (x + 1)^2(x^2 + x + 2)$ är en sådan faktorisering.

a2) F är en kropp med 27 element och $a, b \in F \setminus \{0\}$, $a \neq b$.

Vi söker dels (a, 2p) alla möjliga värden för $|\{ma + nb \mid m, n \in \mathbb{N}\}|$ och dels (b, 2p) alla möjliga värden för $|\{a^m b^n \mid m, n \in \mathbb{N}\}|$.

Lösning:

$27 = 3^3$, så $(F, +) \approx C_3 \times C_3 \times C_3$, ett 3-dimensionellt vektorrum över $\mathbb{Z}_3$. Eftersom $a, b \neq 0$ spänner de upp ett delrum av dimension 1 eller 2. Antalen element i sådana är 3 respektive 9. (Alternativt: $(F, +)$ är en abelsk grupp av ordning 27 och den betraktade mängden är en delgrupp, så bara 1, 3, 9 och 27 är tänkbara. $a \neq 0$, så inte 1. $|\{ma\}| = 3 = |\{nb\}|$, så inte 27. Om $b = a + a$ fås 3, annars inte, så 9.)

$(F \setminus \{0\})$ är cyklisk av ordning $27 - 1 = 26 = 2 \cdot 13$ och den betraktade mängden är en delgrupp, så antalet element är en delare till 26. 1 är inte möjligt, ty $a \neq b$, men det är de andra (det finns enligt känd sats cykliska delgrupper av alla dessa ordningar och a kan t.ex. vara en generator och b ett godtyckligt annat element i delgruppen).

Svar: De möjliga antalen är a: 3 och 9, b: 2, 13 och 26.

b1) Vi skall faktorisera polynomet $f(x) = x^4 + x^3 + x^2 + 2$ i irreducibla faktorer i $\mathbb{Z}_3[x]$.

Lösning:

För att undersöka om $f(x)$ har någon förstgradsfaktor söker vi först nollställena. $f(0) = 2 = f(1)$, men $f(2) = 0$, så $x - 2 = x + 1$ är en faktor i $f(x)$. Division ger $f(x) = (x + 1)g(x)$, där $g(x) = x^3 + x + 2$. Eftersom $f(0), f(1) \neq 0$ är $g(0), g(1) \neq 0$, men man finner att $g(2) = 0$, så $x + 1$ delar också $g(x)$. Division ger $g(x) = (x + 1)h(x)$, där $h(x) = x^2 + 2x + 2$. ($h(0), h(1) \neq 0$ och $h(2) = 1$, så $h(x)$ är irreducibelt (andragradspolynom utan nollställena är irreducibla), så en sökt faktorisering är $f(x) = (x + 1)^2(x^2 + 2x + 2)$.

Svar: $f(x) = (x + 1)^2(x^2 + 2x + 2)$ är en sådan faktorisering.

b2) F är en kropp med 125 element och $a, b \in F \setminus \{0\}$, $a \neq b$.

Vi söker dels (a, 2p) alla möjliga värden för $|\{ma + nb \mid m, n \in \mathbb{N}\}|$ och dels (b, 2p) alla möjliga värden för $|\{a^m b^n \mid m, n \in \mathbb{N}\}|$.

Lösning:

$27 = 5^3$, så $(F, +) \approx C_5 \times C_5 \times C_5$, ett 3-dimensionellt vektorrum över $\mathbb{Z}_5$. Eftersom $a, b \neq 0$ spänner de upp ett delrum av dimension 1 eller 2. Antalet element i sådana är 5 respektive 25. (Alternativt: $(F, +)$ är en abelsk grupp av ordning 125 och den betraktade mängden är en delgrupp, så bara 1, 5, 25 och 125 är tänkbara. $a \neq 0$, så inte 1. $|\{ma\}| = 5 = |\{nb\}|$, så inte 125. Om $b \in \{ma \mid m \in \mathbb{N}\}$ fås 5, annars inte, så 25.)

$(F \setminus \{0\})$ är cyklisk av ordning $125 - 1 = 124 = 2 \cdot 2 \cdot 31$ och den betraktade mängden är en delgrupp, så antalet element är en delare till 124. 1 är inte möjligt, ty $a \neq b$, men det är de andra (det finns enligt känd sats cykliska delgrupper av alla dessa ordningar och a kan t.ex. vara en generator och b ett godtyckligt annat element i delgruppen).

Svar: De möjliga antalen är a: 5 och 25, b: 2, 4, 31, 62 och 124.
