

Lösningsförslag ls5, Diskret matematik, 11 oktober 2011

A1) $\pi \in S_{10}$ ges av $\pi = (1\ 6\ 2\ 5)(3\ 7\ 9)(4\ 10)$ och $G = \langle \pi \rangle$ genereras av π . Vi söker för varje $x \in X$ storleken av dels x 's bana, $|Gx|$, under G 's verkan och dels x 's stabilisator, $|G_x|$.

Lösning:

$|G| = \text{mgm}(4, 3, 2) = 12$ och $|Gx| \cdot |G_x| = |G|$ för alla $x \in X$, så om vi finner $|Gx|$ ger det $|G_x|$. Men $|Gx|$ är ju antalet element i X som x tas till genom upprepning av π , dvs längden av den cykel x ingår i.

Så vi får

x	$ Gx $	$ G_x $
8	1	12
4, 10	2	6
3, 7, 9	3	4
1, 2, 5, 6	4	3

Svar: Enligt tabellen.

A2) R är ringen $\mathbb{Z}_7[x]$ och vi (a.) söker produkten $(3x+2)(4x+5)$, (b.) söker kvot och rest då $x^2 + 5x + 1$ divideras med $2x^2 + 3$, (c.) skall avgöra vilka av $\alpha. x^2 + 3x + 3$, $\beta. x^2 + 3x + 6$, $\gamma. x^2 + 1$ som är irreducibla och (d.) skall avgöra om varje kropp F med $|F| = 49$ innehåller en " $\sqrt{-1}$ ".

Lösning:

a) Eftersom $3 \cdot 4 = 5$ etc i $\mathbb{Z}_7$ finner man $(3x+2)(4x+5) = 5x^2 + x + x + 3 = 5x^2 + 2x + 3$.

b) Eftersom $4 \cdot 2 = 1$ etc i $\mathbb{Z}_7$ får man $x^2 + 5x + 1 = (2x^2 + 3)4 + 5x + 3$, så kvoten är 4 och resten $5x + 3$.

c) Enligt faktorsatsen är ett andragradspolynom i $F[x]$ irreducibelt omm det saknar nollställena i F . För $x = 0, 1, 2, 3, 4, 5, 6 \in \mathbb{Z}_7$ fås $x^2 = 0, 1, 4, 2, 2, 4, 1$ och $x^2 + 3x = 0, 4, 3, 4, 0, 5, 5$, så $x^2 + 3x + 3$ har nollställena 1 och 3, medan $x^2 + 3x + 6$ och $x^2 + 1$ saknar nollställena. Bara de två senare är alltså irreducibla.

d) Enligt c. är $x^2 + 1$ irreducibelt i $\mathbb{Z}_7[x]$, så $\mathbb{Z}_7[x]/(x^2 + 1)$ är en kropp med $7^2 = 49$ element där $[x]^2 = -1$. Eftersom alla kroppar av given storlek är isomorfa (och varje isomorfi mellan kroppar tar -1 i ena kroppen till -1 i den andra) finns " $\sqrt{-1}$ " i alla kroppar med 49 element.

(-1 har en kvadratrots i alla kroppar F med $|F| = p^2$. Om $p = 2$ är $1^2 = 1 = -1$. Om p är udda har $F \setminus \{0\}$ precis $p^2 - 1 = (p+1)(p-1) = 4k$, något $k \in \mathbb{N}$, element och det finns $y \in F \setminus \{0\}$ av ordning $4k$. Då är $y^{2k} \neq 1$ och $(y^{2k})^2 = 1$, så $y^{2k} = (y^k)^2 = -1$.)

Svar: a): Produkten är $5x^2 + 2x + 3$, **b):** kvoten är 4 och resten $5x + 3$, **c):** $x^2 + 3x + 3$ är reducibelt och $x^2 + 3x + 6$ och $x^2 + 1$ båda irreducibla, **d)** Ja. så är det.

B1) $\pi \in S_{10}$ ges av $\pi = (1\ 8)(2\ 9\ 4\ 6)(5\ 10\ 7)$ och $G = \langle \pi \rangle$ genereras av π . Vi söker för varje $x \in X$ storleken av dels x 's bana, $|Gx|$, under G 's verkan och dels x 's stabilisator, $|G_x|$.

Lösning:

$|G| = \text{mgm}(2, 4, 3) = 12$ och $|Gx| \cdot |G_x| = |G|$ för alla $x \in X$, så om vi finner $|Gx|$ ger det $|G_x|$. Men $|Gx|$ är ju antalet element i X som x tas till genom upprepning av π , dvs längden av den cykel x ingår i.

Så vi får

x	$ Gx $	$ G_x $
3	1	12
1, 8	2	6
5, 7, 10	3	4
2, 4, 6, 9	4	3

Svar: Enligt tabellen.

B2) R är ringen $\mathbb{Z}_7[x]$ och vi (a.) söker produkten $(2x+3)(5x+4)$, (b.) söker kvot och rest då x^2+4x+1 divideras med $3x^2+2$, (c.) skall avgöra vilka av $\alpha. x^2+4x+6$ $\beta. x^2+1$ $\gamma. x^2+4x+2$ som är irreducibla och (d.) skall avgöra om varje kropp F med $|F| = 49$ innehåller en " $\sqrt{-1}$ ".

Lösning:

a) Eftersom $2 \cdot 5 = 3$ etc i $\mathbb{Z}_7$ finner man $(2x+3)(5x+4) = 3x^2 + x + x + 5 = 3x^2 + 2x + 5$.

b) Eftersom $5 \cdot 3 = 1$ etc i $\mathbb{Z}_7$ får man $x^2 + 4x + 1 = (3x^2 + 2)5 + 4x + 5$, så kvoten är 5 och resten $4x + 5$.

c) Enligt faktorsatsen är ett andragradspolynom i $F[x]$ irreducibelt omm det saknar nollställan i F . För $x = 0, 1, 2, 3, 4, 5, 6 \in \mathbb{Z}_7$ fås $x^2 = 0, 1, 4, 2, 2, 4, 1$ och $x^2 + 4x = 0, 5, 5, 0, 4, 3, 4$, så $x^2 + 4x + 2$ har nollställena 1 och 2, medan $x^2 + 4x + 6$ och $x^2 + 1$ saknar nollställan. Bara de två senare är alltså irreducibla.

d) Enligt c. är $x^2 + 1$ irreducibelt i $\mathbb{Z}_7[x]$, så $\mathbb{Z}_7[x]/(x^2 + 1)$ är en kropp med $7^2 = 49$ element där $[x]^2 = -1$. Eftersom alla kroppar av given storlek är isomorfa (och varje isomorfi mellan kroppar tar -1 i ena kroppen till -1 i den andra) finns " $\sqrt{-1}$ " i alla kroppar med 49 element.

(-1 har en kvadratrots i alla kroppar F med $|F| = p^2$. Om $p = 2$ är $1^2 = 1 = -1$. Om p är udda har $F \setminus \{0\}$ precis $p^2 - 1 = (p+1)(p-1) = 4k$, något $k \in \mathbb{N}$, element och det finns $y \in F \setminus \{0\}$ av ordning $4k$. Då är $y^{2k} \neq 1$ och $(y^{2k})^2 = 1$, så $y^{2k} = (y^k)^2 = -1$.)

Svar: a): Produkten är $3x^2 + 2x + 5$, **b):** kvoten är 5 och resten $4x + 5$, **c):** $x^2 + 4x + 2$ är reducibelt och $x^2 + 4x + 6$ och $x^2 + 1$ båda irreducibla, **d)** Ja. så är det.