ÖVNING 7 - DISKRET MATEMATIK

ERIC AHLQVIST

1. Gruppverkan

Låt G vara en grupp och S en mängd. En *gruppverkan* av G på S är en funktion

$$\begin{aligned} \varphi\colon G \times S &\to S \\ (g, s) &\mapsto \varphi(g, s) =: gs \end{aligned}$$

sådan att

(1) $(\mathrm{id}_G, s) \mapsto s$, $\forall s \in S$ och
(2) $g_2(g_1 s) = \varphi(g_2, g_1 s) = \varphi(g_2 g_1, s) = (g_2 g_1)s$, $\forall s \in S$, $\forall g_1, g_2 \in G$.

En delmängd på formen

$$Gs = \{s' \in S : s' = gs \text{ för något } g \in G\}$$

kallas för en *bana* och vi definierar *mängden av banor* som

$$S/G = \{Gs : s \in S\}\,.$$

Antalet banor under en gruppverkan av G på S ges då av $|S/G|$; storleken på mängden S/G.

VARNING! Att räkna antalet banor är att räkna antalet mängder på formen Gs (dvs Gs_1, Gs_2, Gs_3, $\ldots$, där det kan hända att $Gs_i = Gs_j$ även om $i \neq j$). Detta är INTE detsamma som att räkna antalet element i Gx!!!

1. $n\mathbb{Z}$-verkan på $\mathbb{Z}$. Visa att

$$n\mathbb{Z} = \{k \in \mathbb{Z} : k = ns \text{ för något } s \in \mathbb{Z}\}$$

är en grupp och att den verkar på $\mathbb{Z}$ (som mängd). Beskriv banorna som bildas under denna gruppverkan.

Lösning. Grupp-operationen ges av addition vilket är väldefinierat eftersom $ns + ns' = n(s + s') \in n\mathbb{Z}$. Identiteten är 0 och inversen till ns är $-ns$. Alltså är $n\mathbb{Z}$ en grupp. Den verkar på $\mathbb{Z}$ genom addition, dvs

$$\begin{aligned} n\mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (ns, t) &\mapsto t + ns\,. \end{aligned}$$

Två element $t, t' \in \mathbb{Z}$ ligger i samma bana om och endast om

$$\begin{aligned} \exists s \in \mathbb{Z} : t = t' + ns &\Leftrightarrow \exists s \in \mathbb{Z} : t - t' = ns \\ &\Leftrightarrow t - t' \equiv 0 \pmod{n}\,. \end{aligned}$$

Mängden av banor är alltså $\mathbb{Z}/n\mathbb{Z}$ betraktat som mängd (som ni vet så ärver denna mängd ringstrukturen från $\mathbb{Z}$, vilket följer av att $n\mathbb{Z}$ är ett så kallat *ideal*).

2. Burside's Lemma

Antag att G är en ändlig grupp och att S är en ändlig mängd. Det finns två sätt att räkna antalet banor $|S/G|$ som bildas av en gruppverkan av G på S. Det första är

$$|S/G| = \sum_{s\in S} \frac{1}{|Gs|} = \frac{1}{|G|}\sum_{s\in S} |G_s|\,,$$

där vi summerar över elementen i S och det andra är *Burnsides Lemma*:

$$|S/G| = \frac{1}{|G|}\sum_{g\in G} |S^g|\,,$$

där vi summerar över elementen i G.

VARNING! Blanda inte ihop S^g och G_s.

Extra Övn. 7 (6). Hur många element har gruppen av oktaederns symmetrirotationer? Finn storleken för dels stabilisator och dels bana för

(a) ett hörn och
(b) för mittpunkt av en sidoyta.

Lösning. Låt G vara gruppen av symmetrirotationer. För att svara på frågan om gruppens storlek, låt x vara ett hörn och y ett hörn som är granne till x. En symmetrirotation bestäms helt av bilden av x tillsammans med bilden av y. Det finns 6 hörn som x kan avbildas på och när bilden av x är bestämd så finns det 4 hörn som som y kan avbildas på (de som är grannar med bilden av x). Dvs det finns totalt $|G| = 6 \cdot 4 = 24$ symmetrirotationer.

Notera att G verkar dels på mängden H av hörn och dels på mängden S av mittpunkter på ytor (trianglar) till oktaedern. Vi har att $|H| = 6$ och $|S| = 8$. För varje hörn x' fins det en symmetirotation som tar x till x' (dvs $|Gx| = 6$) och det finns exakt 4 symmetrirotationer som fixerar hörnet x, nämligen alla rotationer kring axeln som går genom x och motstående hörn (dvs $|G_x| = 4$). Alltså har vi svarat på (a). Detta ger $|G| = |Gx||G_x| = 6\cdot 4 = 24$ vilket stämmer med argumentet ovan.

Vi kan på liknande sätt se att för varje par av mittpunkter $s, s' \in S$ så finns en symmetrirotation som tar s till s' (dvs $|Gs| = 8$) och det finns exakt 3 symmetrirotationer som fixerar s, nämligen alla rotationer kring axeln som går genom s och mittpunkten till motstående sidoyta (dvs $|G_s| = 3$). Alltså har vi svarat på (b). Detta ger att $|G| = |Gs||G_s| = 8 \cdot 3 = 24$ vilket stämmer med våra tidigare beräkningar.

3. Kinesiska restsatsen

Skriver *mgm* för *minsta gemensamma multipel* och *sgd* för *största gemensamma delare.*

Sats 3.1 (Kinesiska restsatsen)**.** *Om $n_1, \dots n_k$ är positiva heltal sådana att $gcd(n_i, n_j) = 1$ då $i \neq j$ och $n = n_1 \cdots n_k$ så är avbildningen*

$$\begin{aligned} f\colon \mathbb{Z}/n\mathbb{Z} &\to Z/n_1\mathbb{Z} \times \dots \mathbb{Z}/n_k\mathbb{Z} \\ a \pmod n &\mapsto (a \pmod{n_1}, \dots, a \pmod{n_k}) \end{aligned}$$

en isomorfi.

Bevis. Bevisa själv att avbildningen är väldefinierad och en homomorfi av grupper. För att visa att f är injektiv, antag att a och b är positiva heltal sådana att

$$(a \pmod{n_1}, \dots, a \pmod{n_k}) = (b \pmod{n_1}, \dots, b \pmod{n_k})\,.$$

Detta betyder att $a - b$ är en multipel av n_i för varje $1 \leq i \leq k$ och därmed en multipel av

$$mgm(n_1, \ldots, n_k) = n\,.$$

Dvs, $a \pmod{n} \equiv b \pmod{n}$ och f är injektiv. Eftersom grupperna är ändliga och har samma storlek är f en isomorfi. □

Extra Övn. 7 (4). Betrakta kongruensen

$$x^3 - 7x^2 + 12x \equiv 0 \pmod{437}\,.$$

Vi har att $437 = 19 \cdot 23$. Finn alla $x \in \mathbb{Z}$ som uppfyller kongruensen.

Lösning. Eftersom 19 och 23 är (olika) primtal så är de relativt prima och vi kan därför använda kinesiska restsatsen KRS. Notera först att

$$x^3 - 7x^2 + 12x = x(x^2 - 7x + 12) = x(x-3)(x-4)$$

(vilket ger tre lösningar $x = 0, 3, 4$ till kongruensen). Enligt KRS har vi att

$$x(x-3)(x-4) \equiv 0 \pmod{437}$$

om och endast om

$$x(x-3)(x-4) \equiv 0 \pmod{19}$$

och

$$x(x-3)(x-4) \equiv 0 \pmod{23}$$

(vi säger här att ett element i $\mathbb{Z}/437\mathbb{Z}$ är 0 om och endast om dess bild i $\mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$ är noll) vilket i sin tur är sant om och endast om någon av faktorerna $x, (x-3), (x-4)$ uppfyller den första kongruensen (mod 19) och någon av faktorerna uppfyller den andra kongruensen (mod 23). Dvs $x \equiv i \pmod{19}$ och $x \equiv i \pmod{23}$ där $i, j \in \{0, 3, 4\}$. Detta ger alltså nio lösningar (element) $(i, j) \in \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$ och det återstår att ta reda på vilka element i $\mathbb{Z}/437\mathbb{Z}$ dessa svarar mot under isomorfin

$$\mathbb{Z}/437\mathbb{Z} \cong \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}\,.$$

För att hitta den inversa avbildningen

$$f^{-1} \colon \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z} \to \mathbb{Z}/437\mathbb{Z}$$

räcker det att notera att bestämma var generatorerna $(1, 0)$ och $(0, 1)$ ska avbildas. Notera att

$$\begin{aligned} 23 &= 19 + 4\,, \\ 19 &= 4 \cdot 4 + 3\,, \\ 4 &= 3 + 1\,, \end{aligned}$$

så att

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (19 - 4 \cdot 4) \\ &= -19 + 5 \cdot (23 - 19) \\ &= 5 \cdot 23 - 6 \cdot 19 \\ &= 115 - 114\,. \end{aligned}$$

Detta betyder att

$$\begin{matrix} 115 \equiv 1 \pmod{19} \\ 115 \equiv 0 \pmod{23} \end{matrix} \quad \text{och} \quad \begin{matrix} -114 \equiv 0 \pmod{19} \\ -114 \equiv 1 \pmod{23} \end{matrix}$$

så vi kan definiera $f^{-1}(1,0) = 115$ och $f^{-1}(0,1) = -114 = 437-114 = 323$. Därför har vi att inversavbildningen ges av $f^{-1}(a,b) = 115a - 114b \pmod{437}$, dvs

$$
\begin{aligned}
&f^{-1}(0,0) = 0 \\
&f^{-1}(0,3) = -3 \cdot 114 = -342 = 95 \\
&f^{-1}(0,4) = -4 \cdot 114 = -456 = -19 = 418 \\
&f^{-1}(3,0) = 3 \cdot 115 = 345 \\
&f^{-1}(3,3) = 3 \cdot 115 - 3 \cdot 114 = 3 \\
&f^{-1}(3,4) = 3 \cdot 115 - 4 \cdot 114 = 345 - 19 = 326 \\
&f^{-1}(4,0) = 4 \cdot 115 = 460 = 23 \\
&f^{-1}(4,3) = 4 \cdot 115 - 3 \cdot 114 = 23 + 95 = 118 \\
&f^{-1}(4,4) = 4\,.
\end{aligned}
$$

Lösningarna till kongruensen ges alltså av alla $x \in \mathbb{Z}$ sådana att $x = s + 437t$ där $t \in \mathbb{Z}$ och

$$s \in \{0, 3, 4, 23, 95, 118, 326, 345, 418\}\,.$$