Algebraiska strukturer, 6 februari

SIDOKLASSER

Låt $G = \mathbb{Z}$ (med addition). Kongruensen modulo n är en ekvivalensrelation på $\mathbb{Z}$ vars ekvivalensklasserna (kongruensklasserna) är $[0], [1], \ldots, [n-1]$ där

$[r] =$ alla heltal som lämnar resten r vid division med n,

dvs

$$[0] = \{kn, k \in \mathbb{Z}\}$$
$$[1] = \{kn + 1, k \in \mathbb{Z}\}$$
$$\ldots$$
$$[r] = \{kn + r, k \in \mathbb{Z}\}$$
$$\ldots$$
$$[n-1] = \{kn + (n-1), k \in \mathbb{Z}\}$$

Vi har $\mathbb{Z} = [0] \cup [1] \cup \ldots \cup [n-1]$. Dessutom är mängden $[0]$ en delgrupp till G och $[r] = [0] + r = \{a + r, a \in [0]\}$. $[0] + r$ kallas en högersidoklass till delgruppen $[0]$. Vi fick en uppdelning av $\mathbb{Z}$ i parvis disjunkta sidoklasser:

$$\mathbb{Z} = [0] \cup [0] + 1 \cup \ldots \cup [0] + (n-1)$$

Mängden $Hg = \{hg, h \in H\}$ (additivt: $H + g = \{h + g, h \in H\}$), där g är ett fixt element i G och H är en delgrupp till G kallas en **högersidoklass** till H i G. Man säger att g är en representant för Hg.

Vi har $a \equiv b \mod n$ omm $a - b \in [0]$, dvs $n|a - b$ och kongruensen modulo n definierar en ekvivalensrelation.

Sats 16.1. Låt H vara en delgrupp till en grupp G. Då är relationen $\sim$ på G definierade enligt

$$a \sim b \text{ omm } ab^{-1} \in H \text{ (additivt: } a - b \in H)$$

en ekvivalensrelation på G med ekvivalensklasserna Hg, $g \in G$ (additivt: $H + g$).

Bevis. Reflexiv: $x \sim x$ ty $xx^{-1} = e \in H$.

Symmetrisk: $x \sim y \Leftrightarrow xy^{-1} \in H \Leftrightarrow (xy^{-1})^{-1} \in H$. Eftersom $(xy^{-1})^{-1} = (y^{-1})^{-1}x^{-1} = yx^{-1}$ får vi $yx^{-1} \in H$ och därmed $y \sim x$.

Transitiv: $x \sim y$ och$y \sim z \Rightarrow xy^{-1} \in H$ och $yz^{-1} \in H$. Eftersom H är en delgrupp får vi att $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$ dvs $x \sim z$.

Altså är $\sim$ en ekvivalensrelation.

Ekvivalensklassen till $x \in G$ är

$$[x] = \{y \in G, y \sim x\} = \{y, yx^{-1} \in H\} = \{y, y \in Hx\} = Hx.$$

Enligt Sats.9.1. och Sats.16.1 får vi att högersidoklasserna bildar en partition av G dvs

- $G = \cup_{g \in G} Hg$,
- $Hg_1 \cap Hg_2 \neq \emptyset \Rightarrow Hg_1 = Hg_2$, dvs två högersidoklasser antingen är lika eller disjunkta.

Dessutom har vi att

- $g \in Hg$
- $g' \in Hg \Leftrightarrow Hg = Hg'$,
- $g' \in Hg \Leftrightarrow g'g^{-1} \in H$.

Exempel. Låt $G = \mathbb{R}^2$ vara gruppen av alla vektorer i planet med avseende på addition av vektorer. Låt H vara den delgrupp till G som består av alla vektorer på x-axeln. Om $\mathbf{v}$ är en vektor så består sidoklassen $H + \mathbf{v}$ av alla vektorer som man får genom att addera $\mathbf{v}$ till alla vektorer på x-axeln. Då får man alla vektorer som slutar på den linje som är parallell med x-axeln och som går igenom ändpunkten av $\mathbf{v}$. Olika sådana linjer svarar mot olika sidoklasser.

Man kan definiera **vänstersidoklasser** på samma sätt:

$$gH = \{gh, h \in H\}.$$

Om gruppen är abelsk har vi att $gH = Hg$. Alla egenskaper hos högersidoklasser visas analogt för vänstersidoklasser. Om gruppen inte är abelsk vänster- och högersidoklasser kan vara olika.

Proposition. Låt H vara en ändlig delgrupp till en grupp G. Då är $|Hg| = |H|$ för varje $g \in G$.

Bevis. Låt $H = \{h_1, \ldots, h_n\}$. Då är $Hg = \{hg_1, \ldots, hg_n\}$. Produkterna $h_i g$ är olika ty $h_i g = h_j g$ ger $h_i = h_j$. Detta visar att antalet element i H är lika med antalet element i Hg.

Lagranges sats. Låt H vara en delgrupp till en ändlig grupp. Då är $o(H)|o(G)$.

Bevis. Högersidoklasserna Hg bildar en partition av G, dvs $G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n$ och $Hg_i \cap Hg_j = \emptyset$. Då är

$$o(G) = |Hg_1| + |Hg_2| + \ldots + |Hg_n| =$$
$$(\text{ enligt propositionen ovan }) = |H| + |H| + \ldots + |H| = n|H|$$

vilket ger nu att $|H| (= o(H))$ delar $o(G)$.

INDEX

Beviset av Lagranges sats visar att antalet högersidoklasser är lika med $o(G) : o(H)$. När man bevisar Lagranges sats med hälp av vänstersidoklasser i stället för högersidoklasser får man att $o(G) : o(H)$ är lika med antalet vänstersidoklasser.

Antalet högersidoklasser (eller vänstersidoklasser) till H i G kallas för **index** av H i G. Indexet betecknas ofta med $[G : H]$.

Följdsatser.

- **1.** Låt G vara en ändlig grupp, $a \in G$. Då $o(a)|o(G)$.

- **2.** Om $o(G) = p$, där p är ett primtal, så saknar G äkta delgrupper H dvs $H \neq \{e\}, G$.
- **3.** Varje grupp av primtalsordning är cyklisk.
- **4.** Om $o(G) = N$ och $a \in G$ så är $a^N = e$.

Bevis. 1. Om $a \in G$ så ordningen $o(a)$ av a lika med ordningen av delgruppen $\langle a \rangle$ genererad av a. Enligt Lagranges sats är alltså $o(a)$ en delare till $o(G)$.

2. Följer direkt från Lagranges sats ty varje primtal p saknar delare $\neq 1, p$.

3. Om $a \in G$, $a \neq e$ så är $\langle a \rangle$ en delgrupp till G och $\langle a \rangle \neq \{e\}$. Enligt **2** är $\langle a \rangle = G$.

4. Om $a \in G$ så är $o(a)|N$ enligt **1** och $N = no(a)$ för något heltal n. Vidare, $a^N = a^{no(a)} = (a^{o(a)})^n = e^n = e$.

Exempel. Med häjlp av Lagranges sats skall vi beskriva delgrupper till S_3.

$o(S_3) = 3! = 6$ och $S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

Enligt Lagranges sats är de eventuella ordningarna av delgrupper till S_3 lika med 1, 2, 3, 6.

Det är klart att $o(H) = 1$ ger $H = \{(1)\}$ och $o(H) = 6$ ger $H = S_3$.

Om $o(H) = 2$ så måste $H = \{(1), g\}$ där g har ordning 2. Det finns 3 sådana : $(1,2)$, $(1,3)$, $(2,3)$. Alltså har vi tre delgrupper av ordning 2: $\{(1), (1,2)\}$, $\{(1), (1,3)\}$, $\{(1), (2,3)\}$.

Om $o(H) = 3$ så är $H = \{(1), g, g^2\}$ där $o(g) = 3$. Det finns 2 sådana element: $(1,2,3)$ och $(1,3,2)$. Eftersom $(1,2,3)(1,2,3) = (1,3,2)$, genererar de samma delgruppen $\{(1), (1,2,3), (1,3,2)\}$.

Varning. I allmänhet är det inte sant att om d är en delare till $o(G)$ så har G en delgrupp av ordning d. Men det gäller för cykliska grupper.

Sats. Låt G vara en ändlig cyklisk grupp av ordning n: $G = \langle a \rangle = \{e, a, \ldots . a^2\}$. Då gäller följande:

- Varje delgrupp till G är cyklisk
- Om $1 \leq k < n$ så genererar a^k en delgrupp av ordning $n/SGD(n,k)$.
- För varje positiv delare d till n har G precis en delgrupp av ordning d. Den är $\langle a^{n/d} \rangle$.

Exempel. Vilka delgrupper har $\mathbb{Z}_{16}$?

Enligt satsen ovan varje delgrupp av $\mathbb{Z}_{16}$ är cyklisk och för varje delare d till 16 finns det precis en delgrupp av ordning d.

Positiva delarna till 16: 1, 2, 4, 8, 16. Det finns 5 delgrupper:
$H_1 = \langle [0] \rangle$,
$H_2 = \langle \frac{16}{2}[1] \rangle = \{[0], [8]\}$,
$H_3 = \langle \frac{16}{4}[1] \rangle = \{[0], [4], [8], [12]\}$,
$H_4 = \langle \frac{16}{8}[1] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14]\}$,
$H_5 = \langle \frac{16}{16}[1] \rangle = \mathbb{Z}_{16}$.
