Algebraiska strukturer, 4 februari

GRUPPER

Några enkla egenskapper hos grupper. Låt G vara en grupp. Då gäller följande

- $a, b, c \in G$ och $ab = ac \Rightarrow b = c$;
- $a, b, c \in G$ och $ba = ca \Rightarrow b = c$;
- $a, b \in G \Rightarrow$ ekvationen $ax = b$ ($xa = b$) har precis en lösning $x = a^{-1}b$ (respektive $x = ba^{-1}$);
- $a \in G \Rightarrow (a^{-1})^{-1} = a$;
- $a, b \in G \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

Bevis=Övning.

Antalet element i en ändlig grupp kallas **gruppens ordning** och betecknas $o(G)$ eller $|G|$. Om G har oändligt många element säger vi att G har oändlig ordning och skriver $o(G) = \infty$ eller $|G| = \infty$.

CYKLISKA GRUPPER

Låt G vara en grupp, $a \in G$. Vi vill bestämma den minsta delgrupp till G som innehåller a. Den måste innehålla

$$a, aa = a^2, aaa = a^3, \ldots, \underbrace{aa\ldots a}_{n \text{ gånger}} = a^n,$$

identitetselementet $e = a^0$

$$a^{-1}, (aa)^{-1} = a^{-1}a^{-1} = a^{-2}, \ldots \underbrace{(aa\ldots a)}_{n \text{ ggr}}{}^{-1} = \underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{n \text{ ggr}} = a^{-n}.$$

Det är lätt att visa att $a^n a^m = a^{n+m}$ och $(a^n)^{-1} = a^{-n}$ för varje $m, n \in \mathbb{Z}$. Enligt Sats 7.1 mängden $\{a^n, n \in \mathbb{Z}\}$ är en delgrupp till G ($a^n a^m = a^{n+m} \in \{a^n, n \in \mathbb{Z}\}$, $(a^n)^{-1} = a^{-n} \in \{a^n, n \in \mathbb{Z}\}$). Denna delgrupp kallas för **delgruppen genererad av** a och betecknas med $\langle a \rangle$. Med den additiva notationen måste man ersätta a^n med $na (= \underbrace{a + a + \ldots + a}_{n \text{ ggr}}$ då $n > 0$ och $\underbrace{(-a) + (-a) \ldots + (-a)}_{n \text{ ggr}}$ då $n < 0$).

Om H är en grupp och $H = \langle a \rangle$ för något element $a \in H$ så kallas H för en **cyklisk grupp**.

Exempel 1. Låt $G = \{-1, 1\}$ med den vanliga multiplikationen som operation. Då är $G = \langle -1 \rangle = \{(-1)^n, n \in \mathbb{Z}\} \neq \langle 1 \rangle$.

2. Låt $G = \mathbb{C} \setminus \{0\}$, $a = i$. Vi får

$$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, i^6 = -1, \ldots$$

så att vi endast får fyra olika tal. Å andra sidan är $i^{-1} = i^3$ så att varje negativ potens är lika med en positiv. Vi får $\langle i \rangle = \{1, i, -1, -i\}$.

3. Låt $G = \mathbb{Z}$ med additionen som operation. Då är $\mathbb{Z} = \{n \cdot 1, n \in \mathbb{Z}\} = \langle 1 \rangle$. $\mathbb{Z}$ är oändlig.

Det finns två möjligheter för potenser a^n i G:

- $a^n \neq a^m$ för alla $n \neq m$ (i detta fall är $\langle a \rangle$ oändlig).
- det finns $r < s$ så att $a^r = a^s$ (enligt sats 14.3 är $\langle a \rangle$ ändlig).

Sats 14.3. Låt G vara en grupp, $a \in G$. Antag att det finns $r < s$, $r, s \in \mathbb{Z}$ så att $a^r = a^s$. Då gäller följande:

- (i) Det finns ett minsta positiva heltal n så att $a^n = e$.
- (ii) Om $t \in \mathbb{Z}$ så gäller $a^t = e$ om och endast om $n|t$.
- (iii) Elementen $e = a^0, a, \ldots, a^{n-1}$ är olika och

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Bevis. (i) $a^r = a^s, r < s \Leftrightarrow a^{s-r} = e, s - r > 0$. Detta visar att det finns ett positivt heltal $n \in \mathbb{Z}$ så att $a^n = e$. Eftersom mängden av de positiva heltalen är nedåt begränsad finns det minsta positiva heltal som uppfyller $a^n = e$.

(ii) Låt $a^t = e$, $t > 0$. Då är $t \geq n$. Divisionen av t med n ger $t = nq + r$, där $0 \leq r < n$. Vi får då

$$e = a^t = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = a^r,$$

som medför att $r = 0$, dvs $t = nq$ och $n|t$.

Om n delar t så är $t = nq$ och $a^t = (a^n)^q = e$.

(iii) Låt $r < s \leq n$. Antag att $a^r = a^s$. Då är $a^{s-r} = e$ och $0 < s - r < n$ vilket är omöjligt, ty n är det minsta positiva heltal så att $a^n = e$. Detta visar att $e, a, \ldots, a^{n-1}$ är olika.

Vidare, varje a^N är lika med en av potenserna $a^0, a^1, \ldots, a^{n-1}$, ty $N = qn + r$, $0 \leq r < n$ och $a^N = a^{qn+r} = a^r$. Detta betyder att $\langle a \rangle = \{e, a, \ldots a^{n-1}\}$.

Det minsta positiva heltal n så att $a^n = e$ (additivt: $na = e$) kallas för **ordningen** av a och betecknas $o(a)$. Om sådant n inte existerar skriver vi $o(a) = \infty$. Enligt sats 14.3 är

$$o(a) = |\langle a \rangle|$$

Exempel 1. $G = (\mathbb{C} \setminus \{0\}, \cdot)$. Då är $o(i) = 4$ (se exemplet ovan).

2. $G = (\mathbb{Z}_6, \oplus)$. $2[3] = [3] \oplus [3] = [6] = [0]$, dvs $o([3]) = 2$. $2[2] = [4] \neq [0]$, $3[2] = [6] = [0]$ och $o([2]) = 3$.

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.
