

# Algebra

April 7 2006

## Definition

En **binär operation** på en mängd  $A$  är en funktion:

$$* : A \times A \rightarrow A.$$

## Exempel

- ▶  $+, \cdot$  på  $\mathbb{N}, \mathbb{Z}, \mathbb{Z}_n, M_2(\mathbb{Z})$ , där  $M_2(\mathbb{Z})$  är mängden av  $2 \times 2$  matriser med koefficienterna i  $\mathbb{Z}$ .
- ▶ Låt  $F(A)$  vara mängden av alla funktioner från  $A$  till  $A$ . Då är sammansättning  $\circ$  en binär operation på  $F(A)$ .
- ▶ multiplicationen  $\cdot$  mellan två permutationer är en binär operation på  $S_n$ .

## Definition

En **grupp** är en mängd  $G$  med en binär operation  $*$  ( d.v.s att  $a * b \in G$  för all  $a, b \in G$ ) sådan att:

1.  $*$  är associativ, d.v.s att

$$(x * y) * z = x * (y * z) \text{ för varje } x, y, z \in G.$$

2. Det finns en **identitet**, d.v.s. det finns ett element  $e \in G$  sådan att:

$$e * a = a * e = a \text{ för varje } a \in G.$$

3. Varje element har en invers, d.v.s. att för varje  $a \in G$  det finns ett element  $a'$  sådan att:

$$a * a' = a' * a = e.$$

Vi betecknar gruppen med  $(G, *)$ .

## Exempel

- ▶  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}_n, +)$ ,  $(M_2(\mathbb{Z}), +)$  är grupper. Notera att varken  $(\mathbb{N}, +)$  eller  $(\mathbb{Z}, \cdot)$  är en grupp.
- ▶  $(\mathbb{R} - \{0\}, \cdot)$  är en grupp men  $(M_2(\mathbb{R}), \cdot)$  inte är en grupp.
- ▶  $(S_n, \cdot)$  är en grupp.
- ▶ Låt  $G$  vara mängden av matriser av form:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

där  $a, b \in \mathbb{Z}_3$  och  $a \neq 0$ . Betrakta den vanliga matris-multiplicationen,  $\cdot$ .  $(G, \cdot)$  är en grupp.

När det är klart vilken operation betraktas på gruppen ska vi skriva:

$G$  istället av  $(G, *)$ .

$xy$  istället av  $x * y$ .

1 istället av identiteten  $e$

$x^{-1}$  istället av inversen  $x'$ .

## SATS

*Låt  $x, y, a$  vara element i en grupp  $G$ . Det gäller att:*

$$ax = ay \Rightarrow x = y$$

$$xa = yb \Rightarrow x = y.$$

Vi säger att en grupp  $G$  är **kommutativ** om

$$xy = yx \text{ för alla } x, y \in G.$$

## SATS

Låt  $G$  vara en grupp och  $a, b \in G$ . Ekvationen

$$ax = b$$

har en entydig lösning.

## Anmärkning

Låt  $G$  vara en grupp. Då är identiteten och inversen av varje element entydigt bestämda.

## Exempel

Låt  $G = \{1, a, b, c\}$  vara en grupp där  $a^2 = b^2 = c^2 = 1$ . Skriv en tabell som beskriver operationen på  $G$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	c	1

Om  $x \in G$  då betecknar vi  $xx\dots x$   $k$  gånger med  $x^k$  och vi sätter att  $x^0 = 1$ . Det är klart att:

$$x^{k+t} = x^k x^t, x^{kt} = (x^k)^t.$$

## Definition

Låt  $G$  vara en grupp med ändligt många element. Vi säger att  $\text{ord}(x) = n$  (ordning av  $x$ ) om  $n$  är det minsta positiva heltalet sådan att  $x^n = 1$ .

## Exempel

Betrakta  $\mathbb{Z}_6$ , då är  $1 = [0]$  och  
 $\text{ord}([0]) = 1, \text{ord}([1]) = 6, \text{ord}([2]) = 3, \text{ord}([3]) = 2,$   
 $\text{ord}([4]) = 3, \text{ord}([5]) = 6.$



## Exempel

Bestäm ordningen av  $\sigma = (13)(452) \in \mathcal{S}_5$ .

$$1 = id_5 = (1)(2)(3)(4)(5).$$

$$\sigma^2 = (1)(3)(425), \sigma^3 = (13)(4)(5)(2), \sigma^4 = (1)(2)(452),$$

$$\sigma^5 = (12)(425), \sigma^6 = (1)(2)(3)(4)(5).$$

Notera att  $ord((12)) = 2$ ,  $ord((456)) = 3$  och

$$ord(\sigma) = l.c.m(3, 2) = 6.$$

Det gäller alltid:

- ▶ För varje cykel  $\tau$  av längd  $k$  är  $ord(\tau) = k$ .
- ▶ Om  $\sigma = \tau_1\tau_2\dots\tau_k$  och längden av  $\tau_i$  är  $d_i$  då är

$$ord(\sigma) = l.c.m(d_1, \dots, d_k).$$

## Exempel

Låt  $G$  vara en kommutativ grupp och  $a, b \in G$ . Visa att om  $\text{ord}(a) = p_1$ ,  $\text{ord}(b) = p_2$  där  $p_1 \neq p_2$  är primtal då är

$$\text{ord}(ab) = \text{ord}(a)\text{ord}(b).$$