Algebra

April 18 2006

Grupper

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:

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

Grupper

Vi beteknar 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 vanlig matris-multiplicationen,* $\cdot$. $(G, \cdot)$ *är en grupp.*

Grupper

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} instället av inversen x'.
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 $x, y, a, b \in G$.

- *Det gäller att:*

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

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

- *Ekvationen*

$$ax = b$$

har en entydig lösning.

Anmärkning

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

Exempel

Låt $(G, *), (G', @)$ *två grupper. Man kan definiera en binär operation på* $G \times G'$:

$$(a, x)(b, y) = (a * b, x@y)$$

$G \times G'$, *med den här operationen, är en grupp.*

Om $x \in G$ då betecknar vi $xx...x$ 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 e grupp med änligt många element. Vi säger att $ord(x) = n$ (ordning av x) om n är det minsta positiva heltalet sådan att $x^n = 1$.

Ordning

Exempel

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

Exempel

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

Ordning

Det gäller alltid:

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

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

Exempel

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

$$ord(ab) = ord(a)ord(b).$$

Grupphomomorfi

Definition

Låt $(G, *)$ och $(G', @)$ vara två grupper. En **grupphomomorfi** mellan G och G' är en funktion $f : G \to G'$ som respekterar operationerna, d.v.s

$$f(a * b) = f(a)@f(b) \text{ för varje } a, b \in G.$$

Exempel

Funktionen $[\,]_n : \mathbb{Z} \to \mathbb{Z}_n$ *är en grupphomomorfi mellan* $(\mathbb{Z}, +)$ *och* $(\mathbb{Z}_n, +)$.

Grupphomomorfi

Definition

En **gruppisomorfi** mellan två grupper G och G' är en grupphomorfi f där funktionen f är bijektiv. Det vill säga att $f : G \to G'$ är en isomorfi om:

1. f är injektiv.
2. f är surjektiv.
3. $f(a * b) = f(a) @ f(b)$ för varje $a, b \in G$.

Vi säger att två grupper G, G' är **isomorfa**, och vi skriver $G \cong G'$, om det finns en isomorfi mellan G och G'.

Exempel

Betrakta:

$$G = \left(\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right), a, b \in \mathbb{R}, \quad G' = \mathbb{R} \times \mathbb{R}.$$

Låt $+$ denote den matrisaddition för G och den vanlig addition av två par för G'. Betrakta funktionen:

$$f : G \to G', \quad f\left(\left(\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right) \right) = (a, b).$$

$(G, +), (G', +)$ *är grupper. Är f en gruppisomorfi?*