Diskret matematik 2018-04-16 #11

Exempelbeskrivningar finns i PPT på Canvas

Grupper: de 4 gruppaxiomen

Vad är en grupp?

$(\mathbb{Z}, +)$, dvs mängden $\mathbb{Z}$ med operationen $+$, uppfyller:

1. För alla $a, b \in \mathbb{Z}$ så är $a+b \in \mathbb{Z}$
2. Det finns ett speciellt element $0 \in \mathbb{Z}$ sådant att $a+0=0+a=a$ för varje $a \in \mathbb{Z}$.
3. För varje $a \in \mathbb{Z}$ finns det ett element $-a \in \mathbb{Z}$ sådant att $a+(-a)=(-a)+a=0$.
4. För alla $a,b,c \in \mathbb{Z}$ gäller att $a+(b+c)=(a+b)+c$

Alla fyra egenskaper gäller även för $\mathbb{Q}^* = \{m/n : m,n \in \mathbb{Z};\ m,n \neq 0\}$ operatorn $\cdot$ (gånger)...

<u>Def</u>

Def^{n} En grupp $(G, \circ)$ består av en mängd G och en binär operation $\circ$ på G som uppfyller de 4 gruppaxiomen.

1. Slutenhet: $a \circ b \in G$ för alla $a, b \in G$.
2. Identitet: Det finns ett identitetselement $e \in G$ sådant att $a \circ e = e \circ a = a$ för varje $a \in G$
3. Inverser: För varje $a \in G$ finns det ett element $b \in G$ sådant att $a \circ b = b \circ a = e$, där e är ett identitetselement som i (2).
4. Associativitet: för alla $a,b,c \in G$ så är $a \circ (b \circ c) = (a \circ b) \circ c$.

Binär operation: en funktion från G till G.

$(\mathbb{Z}, -)$ är inte en grupp då associativiteten och identiteten inte håller.
$(\mathbb{R}^*, \cdot)$ är en grupp
$(P(\{1,2,3\}), \cup)$ är inte en grupp då endast den tomma mängden är inverterbar.
$(\mathbb{R}, +)$ är en grupp
$(\mathbb{Q}, \cdot)$ är inte en grupp då $0 \in \mathbb{Q}$ inte har någon invers (multiplikativt)
$(\mathbb{Z}_n, +)$ är en grupp

Sats (Kancelleringslagen)
Låt $(G, \circ)$ vara en grupp, och låt $a, x, y \in G$.
Om $x \circ a = y \circ a$, då är $x = y$ (högerkancellation)

Liknande har vi
Om $a \circ x = a \circ y$, då är $x = y$ (vänsterkancellation)

Obs! Om $x \circ a = a \circ y$ säger satsen ingenting

Om $\overbrace{x \circ a = y \circ a}^{\circledast}$ då är $x = y$.

I $(\mathbb{Z},+)$: Om $x+97 = y+97$, visa att $x = y$

Lägg till (-97) till båda sidorna:

$(x+97)+(-97) = (y+97)+(-97)$

$x+(97-97) = y+(97-97)$

$x+0 = y+0$

$x = y$

<u>Bevis</u> Låt $b \in G$ vara en invers till a, enligt gruppaxiom 3.

Gör operationen $\circ b$ på båda sidor av $\circledast$

$(x \circ a) \circ b = (y \circ a) \circ b$

Enligt associativitet:

$x \circ (a \circ b) = y \circ (a \circ b)$

för ett id-element e enligt (2)

Enligt def^{n} av invers i (3) så är $a \circ b = e$, så

$x \circ e = y \circ e$

Enligt gruppaxiom (2) så är $x \circ e = x$, $y \circ e = y$, så

$x = y$ $\blacksquare$

Fråga 13: Har alla möjliga kortblandningar uppstått sedan tidernas begynnelse.

$52! \approx 8 \times 10^{67}$

100 peta-FLOPs/sek 100×10^{12} operationer per sekund

Låt oss anta att 10 miljarder superdatorer har hållt på att blanda kort sedan the Big Bang (14×10^{9} år)

Sek sedan Big Bang: $14 \times 366 \times 24 \times 60 \times 60 = 45 \times 10^{17}$ sek

Möjliga operationer: $\underbrace{(10 \times 10^{9})}_{\text{antal datorer}} \times \underbrace{(100 \times 10^{12})}_{\text{op/sek}} \times \underbrace{(4{,}5 \times 10^{17})}_{\text{sek}}$

$= 4{,}5 \times 10^{41}$

Inte möjligt!

I $(\mathbb{Z}_p^{x'}, \bullet)$: om $ax=ay$ i $\mathbb{Z}_p$ $(a\neq 0)$, då är $x=y$.

I $\mathbb{Z}_p$ sade vi att inverser var unika:
lösningen till $ax=1$ i $\mathbb{Z}_p$ är unik $(ax+mp=1)$

Sats (Id är unikt)
Låt $(G, \circ)$ vara en grupp. Då finns det ett unikt identitetselement i G, dvs bara ett element $e\in G$ som uppfyller identitetsaxiomet.

Sats (Inverser är unika)
För varje $a\in G$ finns det ett unikt element $b\in G$ som uppfyller inversaxiomet. Detta element kallas a:s invers och betecknas a^{-1}.

Bevis Låt $b \,\&\, c\in G$ vara element som uppfyller inversaxiomet för a, dvs

$$a\circ b = b\circ a = e$$
$$a\circ c = c\circ a = e$$

Eftersom $b\circ a = c\circ a$ så är $b=c$, enligt högerkancellationssatsen $\boxtimes$

Ex 7 Grupptabeller

Grupptabellen för $(\mathbb{Z}_6, +_6)$: addition mod 6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- Slutenhet: endast elementen från $\mathbb{Z}_6$ står med i tabellen.
- Identitet: Vi ser att elementet 0 är identitetselementet.
- Inverser: 0 står med i varje rad och varje kolonn.
- Associativitet: ..

Def^n Låt $(G, \circ)$ vara en grupp. Dess grupptabell är då tabellen med rader och kolonner båda indexerade av elementen i G, där värdet i rad a och kolonn b, för $a, b\in G$, ges av $a\circ b$.

Ex $G=\{e,a,b,c,d\}$ identitetselement: e

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	$a\circ a$	$a\circ b$	$a\circ c$	$a\circ d$
b	b	$b\circ a$	$b\circ b$	$b\circ c$	$b\circ d$
c	c	$c\circ a$	$c\circ b$	$c\circ c$	$c\circ d$
d	d	$d\circ a$	$d\circ b$	$d\circ c$	$d\circ d$

Sats Låt $(G, \circ)$ vara en grupp. I gruppens grupptabell står varje element i G med en och endast en gång i varje rad. Samma sak gäller för kolonnerna.

Bevis Varför står varje element med i varje rad? Varför står elementet c med i raden för a? Vilken kolonn står c med i?

Att c står i kolonn b (i rad a) innebär att $c = a \circ b$. Så c står med i kolonn $b = a^{-1} \circ c$

(a^{-1} är a:s unika invers, så i kolonn $b = a^{-1} \circ c$, rad a har vi enligt def^n elementet
$$a \circ b = a \circ (a^{-1} \circ c) = (a \circ a^{-1}) \circ c = e \circ c = c.$$

Ex 11 (Tidigare tentafråga)

Sluten: Sammansättning av två bijektioner är en bijektion.
Identitetselement: Identitetsfunktionen $e = id$, $id: A \to A$, $id(x) = x$
Inverser: Inversfunktionen. Alla bijektiva funktioner har en invers.
Associativitet: ...

Kommutativitet

Def^n Låt $(G, \circ)$ vara en grupp. Om
$$a \circ b = b \circ a \text{ för alla } a, b \in G$$
kallas gruppen kommutativ eller abelsk. Annars kallas den icke-kommutativ eller icke-abelsk.

Symmetrier

En triangel har sex symmetrier
- identitetstransformationen
- 2 rotationer
- 3 speglingar

$(Symm_\Delta, \circ)$ är en grupp – se presentation på Canvas