Grupper

Definisjon: En gruppe $(G,*)$ består av en ikke-tom mengde G og en binær operasjon $*$ på G slik at

(i) $*$ er assosiativ, dvs $(a*b)*c = a*(b*c)$

(ii) $*$ har et nøytralt element, dvs det finnes et element $e \in G$ slik at
$$x*e = e*x = x \quad \text{for alle } x \in G.$$

(iii) ethvert element $a \in G$ har et invers element a^{-1}, dvs et element slik at
$$a*a^{-1} = a^{-1}*a = e.$$

En gruppe som er kommutativ (dvs der $a*b = b*a$ for alle $a,b \in G$) kalles en abelsk gruppe.

Eksempel: (i) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ er alle grupper. nøytralt element 0 / invers element til x er $-x$

(ii) $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$ — " — nøytralt element 1, invers element til a er $\frac{1}{a}$.

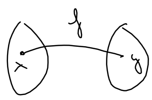
$(\mathbb{Z}\setminus\{0\},\cdot)$ er ikke en gruppe, mangler invers elementer.

(iii) G er alle inverterbare $n\times n$-matriser ($n \geq 2$). Er en ikke-kommutativ gruppe. $AB \neq BA$

Nøytralt element: $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, invers element: A^{-1}

Anta at X er en ikke-tom mengde og la

$$G = \{ f : X \to X : f \text{ er bijeksjon} \}$$



Operasjonen er sammensetning $f*g = f\circ g$, $f\circ g(x) = f(g(x))$

Setning $(G,\circ)$ er en gruppe.

Bevis: Sjekker aksiomene for grupper:

(ii) Nøytralt element: $id : X \to X$, $id(x) = x$ er et nøytralt element.

$$f\circ id(x) = f(id(x)) = f(x)$$
$$(id\circ f)(x) = id(f(x)) = f(x)$$

(iii) Omvendt element til f: f^{-1} omvendt funksjon: Må sjekke at
$$f\circ f^{-1} = id$$
$$f^{-1}\circ f = id$$

Sjekk: $(f\circ f^{-1})(x) = f(f^{-1}(x)) = x = id(x)$

$(f^{-1}\circ f)(x) = f^{-1}(f(x)) = x = id(x)$

(i) Assosiativ: Må sjekke at: $(f\circ g)\circ h = f\circ(g\circ h)$

$(f\circ g)\circ h\,(x) = (f\circ g)(h(x)) = f(g(h(x)))$

$f\circ(g\circ h)(x) = f((g\circ h)(x)) = f(g(h(x)))$

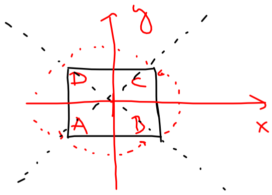
Spesialtilfelle: $X = \{1,2,3,\dots,n\}$

G = alle bijeksjoner $f : X \to X$ = alle permutasjoner av $\{1,2,\dots,n\}$

x	1	2	3	4	5
$f(x)$	4	2	1	5	3

G har $n!$ elementer. G har orden n

Grupper som transformasjoner:



Eksempel: Ser på et kvadrat i planet

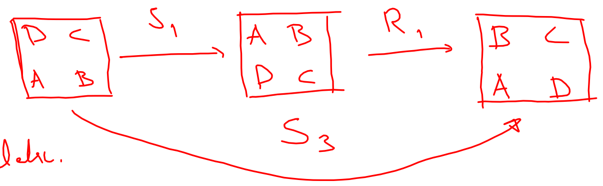
G vil bestå av operasjoner på kvadratet.

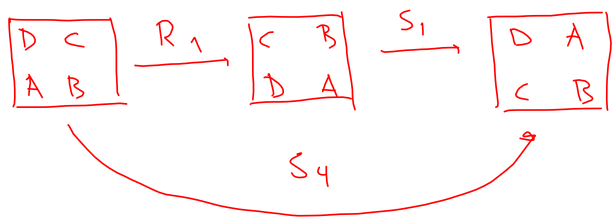
1. I gjør ingenting: D C / A B
2. R_1 90° rotasjon ↺: C B / D A
3. R_2 180° rotasjon: B A / C D
4. R_3 270° rotasjon: A D / B C
5. S_1 Speile om x-aksen: A B / D C
6. S_2 Speile om y-aksen: C D / B A
7. S_3 Speile om linjen $y=x$: B C / A D
8. S_4 Speiler om linjen $y=-x$: D A / C B

Bruker sammensetningsoperasjonen $\circ$ på G: $U \circ V$ = operasjonen V etterfulgt av U.

Eksempler på operasjoner:

$$\left.\begin{array}{l} R_1 \circ S_1 = S_3 \\ \\ S_1 \circ R_1 = S_4 \end{array}\right\} \text{ikke-kommutative.}$$





Skriver ab istedenfor $a*b$

Setning: Hvis G er en gruppe, så har ligningen $ax=b$ har en nøyaktig én løsning $x=a^{-1}b$

Bevis: Sjekker først at $x=a^{-1}b$ er en løsning:

Setter inn: $ax = a(a^{-1}b) \underset{\text{assos}}{=} (aa^{-1})b = eb = b$

Anta så at x er en vilkårlig løsning:

$$ax=b \Rightarrow a^{-1}(ax)=a^{-1}b \Rightarrow \underbrace{(a^{-1}a)}_{e}x = a^{-1}b \Rightarrow ex=a^{-1}b \Rightarrow x=a^{-1}b.$$

Setning: Dersom $ab=ac$, så er $b=c$ (forkortningsregel)

Bevis: $ab=ac \Rightarrow a^{-1}(ab)=a^{-1}(ac) \Rightarrow (a^{-1}a)b=(a^{-1}a)c \Rightarrow eb=ec \Rightarrow b=c.$

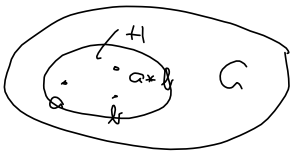
Undergrupper

Noen grupper ligger "inni" andre. $(\mathbb{Q},+)$ er en del av $(\mathbb{R},+)$

I eksemplet med kvadratet utgjør (I,R_1,R_2,R_3) en egen gruppe som ligger inni hele G.

Definisjon: Anta at $(G,*)$ er en gruppe og at $H \subseteq G$. Da kaller vi H en undergruppe av G dersom $(H,*)$ er en gruppe.

(OBS: For at $*$ skal være en binær operasjon på H, må $a,b\in H$ medføre at $a*b\in H$).



Setning: $H \subseteq G$ er en undergruppe hvis og bare hvis følgende krav er oppfylt:

(i) $e \in H$

(ii) Hvis $a,b\in H$, så $a*b\in H$

(iii) Hvis $a\in H$, så er $a^{-1}\in H$.

Eksempel: $X=\{1,2,..,n\}$ G alle permutasjoner av X.

H er alle permutasjoner som ikke endrer n, dvs $f(n)=n$.

Lagranges teorem

Hvis G er en endelig gruppe, så er ordenen til G antall elementer i G

Eksempel: G = alle permutasjoner av $\{1,..,n\}$, ordenen til G er $n!$

Lagranges teorem: Hvis H er en undergruppe av G, så er ordenen til G delelig med ordenen til H.

Bevis: Definer en relasjon $\sim$ på G ved:

$$x \sim y \iff x^{-1}y \in H$$

Sjekker at $\sim$ er en ekvivalensrelasjon:

(i) Refleksiv $x \sim x \iff x^{-1}x \in H$ OK siden $x^{-1}x = e \in H$.

(ii) Symmetrisk $x\sim y \Rightarrow y \sim x$ dvs $x^{-1}y \in H \Rightarrow y^{-1}x \in H$

Anta at $x^{-1}y \in H$, også er $(x^{-1}y)^{-1} \in H$, dvs at $y^{-1}(x^{-1})^{-1} \in H$

Altså er $y^{-1}x \in H$, dvs $y \sim x$.

(iii) Transitiv

Vi må vise at dersom $x \sim y$ og $y \sim z$, så $x \sim z$.

Anta at $x\sim y$ og $y \sim z$, dvs $x^{-1}y \in H$ og $y^{-1}z \in H$ (skal vise at $x^{-1}z \in H$).

Vi ser at $\underbrace{(x^{-1}y)(y^{-1}z)}_{x^{-1}z} \in H$

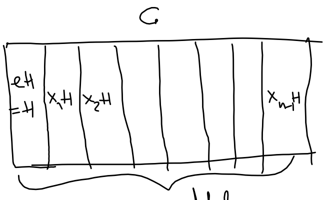
Kladderegning: $(x^{-1}y)(y^{-1}z)$

$= x^{-1}(y(y^{-1}z)) = x^{-1}(\underbrace{(yy^{-1})}_{e}z)$

$= x^{-1}(ez) = x^{-1}z$

dvs $x \sim z$.

Siden $\sim$ er en ekvivalensrelasjon, vet vi at ekvivalensklassene danner en partisjon av G.



n restklasser.

Hvordan ser ekvivalensklassen til x ut?

$[x] = \{y : x \sim y\} = \{y : x^{-1}y \in H\}$

$= \{xh : h \in H\} = xH$

↑ definisjon.

$x^{-1}y = h \Rightarrow y = xh$

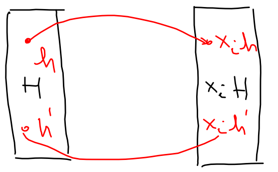
Påstand at enhver restklasse har like mange elementer som H.

Spesielt:

$[e] = eH = \{eh : h \in H\} = \{h : h \in H\} = H$.

Vi ser at

$$|G| = n|H| \Rightarrow \frac{|G|}{|H|} = n \text{ - antall restklasser.}$$



$h \in H$

$x_ih = x_ih' \Rightarrow h = h'$