Grupper

$(G, *)$ er en gruppe dersom

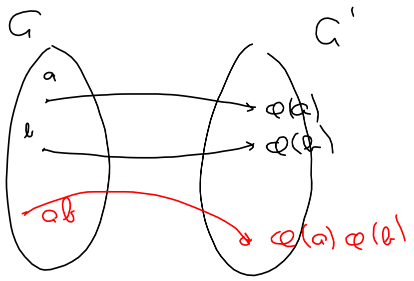
(i) $*$ er assosiativ

(ii) Vi har et nøytrall element e. $(a*e = e*a = a)$

(iii) Ethvert element a har et invers element a^{-1} $(a*a^{-1} = a^{-1}*a = e)$

Definisjon: Anta at G og G' er to grupper. En avbildning $\varphi : G \to G'$ kalles en homomorfi dersom

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{for alle } a, b \in G.$$



Setning: Anta at $\varphi : G \to G'$ er en homomorfi. Da er $\varphi(e) = e'$ (e er nøytrall element i G og e' er nøytrall element i G')

Bevis: $\varphi(\cancel{e})e' \overset{e' \text{ er nøytrall}}{=} \varphi(e) \underset{e \text{ er et nøytrall element}}{=} \varphi(ee) \overset{\varphi \text{ er en homomorfi}}{=} \varphi(\cancel{e})\varphi(e)$

Som gir $e' = \varphi(e)$.

Setning: Anta at $\varphi : G \to G'$ er en homomorfi. For alle $a \in G$ er da $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Bevis: Husk at $\varphi(a)^{-1}$ er det unike elementet y i G slik at $y\varphi(a) = e'$ og $\varphi(a)y = e'$. Vi må vise at $\varphi(a^{-1})$ har denne egenskapen.

Vi får

$$\varphi(a^{-1})\varphi(a) = \varphi(\underbrace{a^{-1}a}_{e}) = \varphi(e) = e'$$

$$\varphi(a)\varphi(a^{-1}) = \varphi(\underbrace{aa^{-1}}_{e}) = \varphi(e) = e'$$

Altså er $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Husk: $H \le G$ er en undergruppe av G dersom $(H,*)$ er en gruppe.

Dette er tilfellet når:

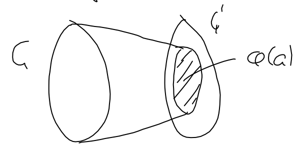
$$\varphi(G) = \{\varphi(a) : a \in G\}$$

(i) $e \in H$

(ii) Hvis $a,b \in H$, så er $a*b \in H$

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

Setning: Hvis $\varphi: G \to G'$, så er $\varphi(G)$ en undergruppe av G'.



Bevis: Sjekke kravene

(i) $e' \in \varphi(G)$: $e' = \varphi(e) \in \varphi(G)$

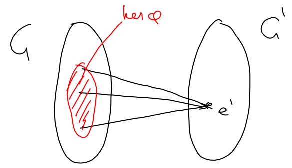
(ii) Anta at $a,b \in \varphi(G)$, må vise at $a*b \in \varphi(G)$.
Siden $a,b \in \varphi(G)$, finnes det $x,y \in G$ slik at $a = \varphi(x)$, $b = \varphi(y)$. Men da er

$$ab = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi(G)$$

(iii) Anta at $a \in \varphi(G)$. Må vise at $a^{-1} \in \varphi(G)$.
Siden $a \in \varphi(G)$, så finnes det en $x \in G$ slik at $a = \varphi(x)$. Dermed er $a^{-1} = \varphi(x)^{-1} = \varphi(x^{-1}) \in \varphi(G)$.

Def: $\varphi: G \to G'$ er en homomorfi, så er kjernen til φ, $\ker\varphi$, definert ved

$$\ker\varphi = \{x \in G : \varphi(x) = e'\}$$



Undergruppe:
(i) $e \in H$
(ii) $a,b \in H \Rightarrow ab \in H$
(iii) $a \in H \Rightarrow a^{-1} \in H$.

Setning: Hvis $\varphi: G \to G'$ er en homomorfi, så er $\ker\varphi$ en undergruppe av G.

Bevis: (i) $e \in \ker\varphi$: $\varphi(e) = e'$ OK.

(ii) Må vise at hvis $a,b \in \ker\varphi$, så er $ab \in \ker\varphi$.
Siden $a,b \in \ker\varphi$, så er $\varphi(a) = \varphi(b) = e'$. Dermed er

$$\varphi(ab) = \varphi(a)\varphi(b) = e'e' = e',$$

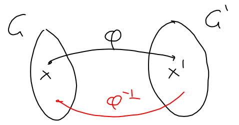
som viser at $ab \in \ker\varphi$

(iii) Må vise at hvis $a \in \ker\varphi$, så er $a^{-1} \in \ker\varphi$.
Vet at $\varphi(a) = e'$, så

$$\varphi(a^{-1}) = \varphi(a)^{-1} = (e')^{-1} = e'$$

som viser at $a^{-1} \in \ker\varphi$.

Definisjon: En homomorfi som er bijektiv, kalles en isomorfi



En isomorfi har alltid en omvendt funksjon $\varphi^{-1}: G' \to G$.

Setning: Den omvendte funksjonen φ^{-1} til en isomorfi er selv en isomorfi.

Bevis: Siden den omvendte funksjonen er en bijeksjon, holder det å vise at den er en homomorfi, altså $\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)$

Vi har $\varphi(\varphi^{-1}(ab)) = ab$ siden φ og φ^{-1} er omvendte funksjoner.

$$\varphi(\varphi^{-1}(a)\varphi^{-1}(b)) = \underbrace{\varphi(\varphi^{-1}(a))}_{a}\,\underbrace{\varphi(\varphi^{-1}(b))}_{b} = ab$$

Dette betyr at

$$\varphi(\varphi^{-1}(ab)) = \varphi(\varphi^{-1}(a)\varphi^{-1}(b))$$

Siden φ er injektiv, må

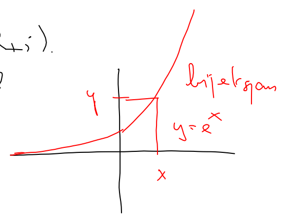
$$\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)$$

som vi skulle vise.

Eksempel: Ser på gruppene $(\mathbb{R},+)$ og $(\mathbb{R}_+,\cdot)$.
Vi kan definere en isomorfi $\varphi: \mathbb{R} \to \mathbb{R}_+$ ved

$$\varphi(x) = e^x.$$

$$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x)\varphi(y)$$



Kongruenskonstruksjoner

G og G' er to grupper, $\varphi: G \to G'$ en homomorfi.

Definerer en relasjon $\sim$ på G ved

$$x \sim y \iff \underline{\varphi(x) = \varphi(y)}.$$

<u>Lemma</u>: $\sim$ er en ekvivalensrelasjon.

<u>Bevis</u>: Vi må sjekke tre krav

(i) <u>Refleksiv</u>: $x \sim x$ for alle x: Ok siden $\varphi(x) = \varphi(x)$

(ii) <u>Symmetri</u>: $x \sim y \Rightarrow y \sim x$: OK siden $\varphi(x) = \varphi(y) \Longrightarrow \varphi(y) = \varphi(x)$ dvs $y \sim x$

(iii) <u>Transitiv</u>: $x \sim y$ og $y \sim z \Rightarrow x \sim z$: Ok siden $\varphi(x) = \varphi(y)$ og $\varphi(y) = \varphi(z)$, som medfører $\varphi(x) = \varphi(z)$.

<u>Lemma</u>: Hvis $x \sim x'$ og $y \sim y'$, så $xy \sim x'y'$

<u>Bevis</u>: Vi har $\varphi(x) = \varphi(x')$ og $\varphi(y) = \varphi(y')$. Dermed er

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi(x')\varphi(y') = \varphi(x'y')$$

dvs $xy \sim x'y'$

La $G/\sim$ være mengden av alle ekvivalensklasser. Vi vil definere en operasjon $*$ på $G/\sim$ slik at $(G/\sim, *)$ er en gruppe.

På grunn av lemmaet kan vi definere en operasjon $*$ på $G/\sim$ ved

$$[x] * [y] = [xy]$$

<u>Er dette lov?</u> Er operasjonen veldefinert?

Ja, det er den pga. lemmaet.

<u>Potensielt problem</u>: Hva hvis $x' \sim x$, $y' \sim y$, da er jo $[x'] = [x]$ og $[y'] = [y]$. Da er jo også

$$[x'] * [y'] = [x'y']$$
$$[x] * [y] = [xy]$$

Må være like for at operasjonen skal være veldefinert.

<u>Teorem</u> $(G/\sim, *)$ er en gruppe.

<u>Bevis</u>: (i) <u>Assosiativ</u>: $([a]*[b])*[c] = [a]*([b]*[c])$

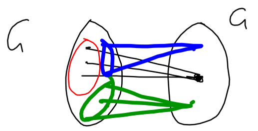
Vi har $(\underbrace{[a]*[b]}_{[ab]})*[c] = [ab]*[c] = [(ab)c] \overset{G \text{ er assos.}}{=} [a(bc)]$
$= [a]*[bc] = [a]*([b]*[c])$

(ii) <u>Nøytralt element</u>: $[e]$ er et nøytralt element i $G/\sim$.

$$[a] * [e] = [\underbrace{ae}_{a}] = [a]$$
$$[e] * [a] = [ea] = [a].$$

(iii) <u>Inverse elementer</u>: $[a]$ har invers element $[a^{-1}]$.

<u>Sjekk</u>: $\left.\begin{array}{l} [a] * [a^{-1}] = [aa^{-1}] = [e] \\ [a^{-1}] * [a] = [a^{-1}a] = [e] \end{array}\right\}$ nøytralt element i $G/\sim$.



RINGER

Definisjon: En ring $(R,+,\cdot)$ består av en ikke-tom mengde R og to binære operasjoner $+$ og $\cdot$ på R slik at.

(i) (addisjon er assosiativ) $(a+b)+c = a+(b+c)$

(ii) (addisjon er kommutativ) $a+b = b+a$

(iii) (eksistens av nullelement) Det finnes et element $0 \in R$ slik at $a+0=a$ for alle $a \in R$.

(iv) (det finnes inverse elementer) For alle $a \in R$ finnes det et element $-a$ slik at $a+(-a)=0$.

$(R,+)$ er en abelsk gruppe.

(v) (multiplikasjon er assosiativ) $(ab)c = a(bc)$

(vi) (eksistens av enhetselement) Det finnes et $1 \in R$ slik at $a \cdot 1 = 1a = a$ for alle $a \in R$.

(vii) (distributive lover) For alle $a,b,c \in R$, er $a(b+c) = ab+ac$ og $(b+c)a = ba+ca$.

Dersom $ab=ba$ for alle $a,b \in R$, så kalles R en kommutativ ring.

Eksempler: (i) $\mathbb{Z}$ mengden av hele tall. (kommutativ ring)

(ii) $\mathbb{Z}/(t)$ er kommutative ringer. $\mathbb{Z}/(6) = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$

(iii) $n \times n$-matriser danner en ikke-kommutativ ring.

(iv) Alle funksjoner $f: X \to \mathbb{R}$ er en ring. $(f+g)(x) = f(x)+g(x)$, $(f \cdot g)(x) = f(x)g(x)$

(v) Alle polynomer $p: \mathbb{R} \to \mathbb{R}$ danner en ring.

(vi) $\mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ er også ringer, men her har alle ikke-null elementer en multiplikativ invers, så dette er kropper og ikke ~~ringer~~ bare ringer. Det samme gjelder $\mathbb{Z}/(p)$ når p er et primtall.