Kapittel 20

Litt abstrakt algebra

Definisjon 20.1 Invers relasjon

Hvis R er en relasjon fra A til B, er den **inverse relasjonen** (*eng: inverse relation*) til R relasjonen $\{ \langle y, x \rangle \mid \langle x, y \rangle \in R\}$ fra B til A. Vi skriver R^{-1} for inversen til R.

Ets/

$R \subseteq A \times B$

$R = \{\langle 0, b\rangle, \langle 0, c\rangle, \langle 2, a\rangle\}$

$A = \{0, 1, 2\}$

$B = \{a, b, c\}$

$R^{-1} = \{\langle b, 0\rangle, \langle c, 0\rangle, \langle a, 2\rangle\}$

NØTT HVA HVIS $R = R^{-1}$?

$R \subseteq A \times A$ $\quad$ $R^{-1} \subseteq A \times A$

- $\Delta \subseteq \{ \langle x, x \rangle \mid x \in A \} = \Delta^{-1} = \{ \langle x, x \rangle \mid x \in A \}$
- $\emptyset = \emptyset^{-1}$

$R^{-1} = \{ \langle y, x \rangle \in A \times A \mid \langle x, y \rangle \in R \} = R$

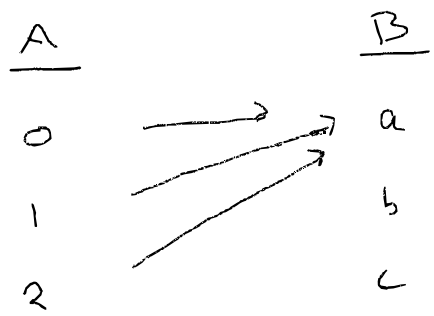
FØLGENDE ER EKVIVALENT: (TFAE) (ENGELSK: "THE FOLLOWING ARE EQUIVALENT")

- $R = R^{-1}$
- R ER SYMMETRISK

NØTT HVIS $R \subseteq A \times B$ ER EN FUNKSJON,

ER $R^{-1} \subseteq B \times A$ EN FUNKSJON?

IKKE UNØDVENDIGVIS Å



$R = \{(0,a), (1,a), (2,a)\}$

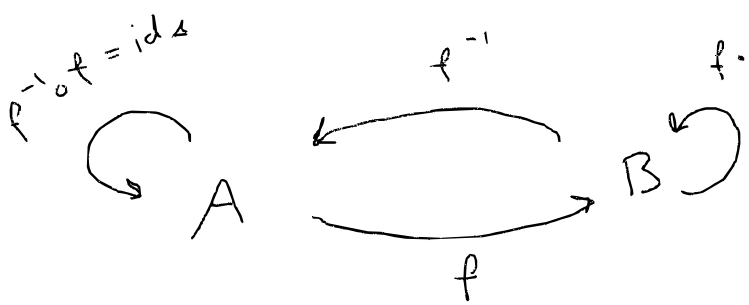
$R^{-1} = \{(a,0), (a,1), (a,2)\}$

TFAE:

- R^{-1} ER EN FUNKSJON
- R ER INJEKTIV OG SURJEKTIV, DVS BIJEKTIV. ✓

f ER FUNKSJONEN R

$f^{-1} = R^{-1}$



$f(a) = b$ $\quad \langle a,b \rangle \in R$

$f^{-1}(b) = a$ $\quad \langle b,a \rangle \in R^{-1}$

$f^{-1}(f(a)) = a$

$f(f^{-1}(b)) = b$

Definisjon 20.2 Invers funksjon

La f være en en-til-en korrespondanse fra mengden A til mengden B. Den **inverse funksjonen** (*eng: inverse function*) til f er funksjonen fra B til A som er slik at $f^{-1}(b) = a$ hvis $f(a) = b$. Vi skriver f^{-1} for den inverse funksjonen til f.

MERK: HVIS f HAR EN INVERSFUNKSJON SÅ MÅ f VÆRE BIJEKTIV

ALGEBRA

HUSK EN OPERASJON ER EN FUNKSJON FRA EN MENGDE TIL SEG SELV, MED ARITET.

$$f : A \to A$$
$$g : A \times A \to A$$
$$h : A^4 \to A$$

ALGEBRA ER, GROVT SETT, STUDIET AV STRUKTURER SOM BESTÅR AV OPERASJONER MED BESTEMTE EGENSKAPER (GJØRNE AKSIOMATISERT VED ALLKVANTIFISERTE LIGNINGER)

Eks $\Sigma = \langle e ; f:2 ; =:2 \rangle$

ϕ : $\forall x \forall y \forall z \; f(x, f(y,z)) = f(f(x,y), z)$

ψ : $f(e,x) = x \wedge f(x,e) = x$ (VI LAR ALLKVANTOREN $\forall x$ VÆRE IMPLISITT)

$\Pi = \{\phi, \psi\}$

MODELL FOR Π: $|M|$

SLIK AT $M \models \Pi$

$f^M : |M| \times |M| \to |M|$

$e^M \in |M|$

Eks:

1) $|M| = \mathbb{N}$

$f^M = +$

$e^M = 0$

$x + (y + z) = (x + y) + z$

$0 + x = x$

$x + 0 = x$

2) $|M| = \mathbb{N}$

$f^M = \cdot$

$e^M = 1$

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$

$1 \cdot x = x \cdot 1 = x$

Definisjon 20.4 Assosiativ

En binær operasjon $*$ på en mengde S er **assosiativ** (*eng: associative*) hvis det for alle $x, y, z \in S$ er slik at $x*(y*z) = (x*y)*z$.

Definisjon 20.6 Identitetselement

La en binær operasjon $*$ på en mengde S være gitt. Hvis $x*e = e*x = x$ for alle $x \in S$, sier vi at e er et **identitetselement** (*eng: identity element*) eller et **nøytralt element** (*eng: neutral element*) for operasjonen $*$.

MERK IDENTITETSELEMENTET ER UNIKT.

BEVIS: ANTA AT e OG e' ER IDENTITETSELEMENT.

$e = e * e' = e'$

e ER IDENTITETSELEMENT

e' ER IDENTITETSELEMENT.

EN Π-MODELL, ALTSÅ EN MENGDE MED EN ASSOSIATIV BINÆR OPERASJON $\circ$, ET IDENTITETSELEMENT, KALLES EN MONOIDE

(DETTE BEGREPET, ALTSÅ SELVE NAVNET, ER IKKE PENSUM, MEN EKSEMPLENE ER PENSUM RELEVANTE)

FLER EKS:

GITT EN MENGDE X

MODELL $\mathcal{M}$, $|\mathcal{M}| = \mathcal{P}(X)$

1) $f^{\mathcal{M}} = \cup$

$e^{\mathcal{M}} = \emptyset$

$A \cup (B \cup C) = (A \cup B) \cup C$

$A \cup \emptyset = A = \emptyset \cup A$

2) $f^{\mathcal{M}} = \cap$

$e^{\mathcal{M}} = X$

$A \cap (B \cap C) = (A \cap B) \cap C$

$A \cap X = A = X \cap A$

UNIVERSELL MENGDE $\mathcal{U}$

$X \subseteq \mathcal{U}$

$A \subseteq X \subseteq \mathcal{U}$

$A \cap \mathcal{U} = A$

MEN $\mathcal{U}$ KAN IKKE VÆRE ENHETSELEMENTET, FOR $\mathcal{U}$ ER IKKE ET ELEMENT I $\mathcal{P}(X)$ - MED MINDRE $\mathcal{U} = X$, DA.

— FOR ALLE EKSEMPLER SÅ LANGT HAR VI AT DET HOLDER AT

$f(x,y) = f(y,x)$.

MEN DETTE ER IKKE EN LOGISK KONSEKVENS AV Π.

Definisjon 20.3 Kommutativ
En binær operasjon $*$ på en mengde S er **kommutativ** (*eng: commutative*) hvis det for alle $x, y \in S$ er slik at $x * y = y * x$.

G : $\forall x \forall y \quad f(x,y) = f(y,x)$

Eks: — DE VI HAR SETT SÅ LANGT.

"FRIE" MONOIDER

(DETTE BEGREPET ER HELLER IKKE PENSUM, MEN IGJEN SÅ ER EKSEMPLENE UNDER PENSUM RELEVANTE)

1) SKAL LAGE MONOIDE.

MÅ HA IDENTITETS ELEMENT e

$e * e = e$ – NØDVENDIGVIS.

$(e * e) * e = e = (e * e) * e$ ASSOSIATIV.

MENGDEN ER $\{e\}$.

OPERASJONEN ER $\{e\} \times \{e\} \longrightarrow \{e\}$

$\langle e, e \rangle \longmapsto e$.

DETTE ER EN MONOIDE.

TRIVIELT KOMMUTATIV.

---

2) GITT OBJEKT a. LAG MONOIDE DER a ER MED.

MÅ HA IDENTITETS ELEMENT e.

MÅ HA ELEMENTER FOR ALLE DISSE: LA OSS HA FORSKJELLIGE

$e * a = a * e = a$

KAN SKRIVE a^1

$a * a$

$(a * a) * a = a * (a * a) = a * a * a$

$a * a * a * a$

$\vdots$

TA STRENGER PÅ $\{a\}$.

$*$ ER KONKATENERING (DF 9.8, $s * t = st$)

$e = \Lambda$ DEN TOMME STRENGEN

DETTE ER EN MONOIDE.

DEN ER KOMMUTATIV

3) TO ELEMENTER a, b

MENGDE – MENGDEN AV STRENGER PÅ $\{a, b\}$

IDENTITETS ELEMENT – Λ – TOMME STRENGEN

OPERASJON – KONKATENERING.

$(ab + bb) * (aab) = abbbaab = aabb * (bbbaab)$

ASSOSIATIV.

MONOIDE.

IKKE KOMMUTATIV, FOR $a * b = ab$

$b * a = ba$

BEMERKNING

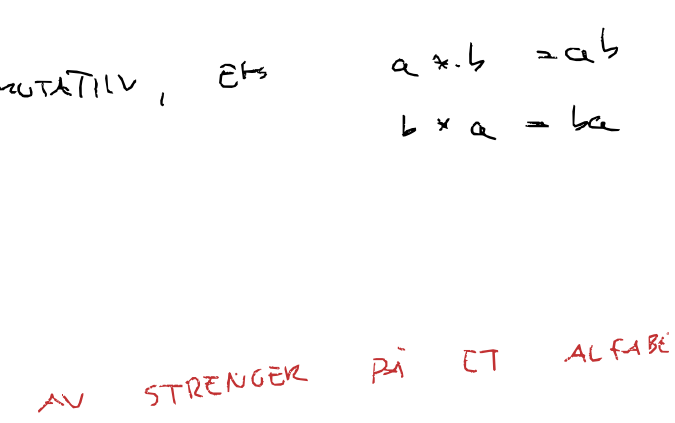
– MONOIDEN AV STRENGER PÅ ET ALFABET $\{a_0, \dots, a_{n-1}\}$ KALLES "DEN FRIE MONOIDEN GENERERT AV n ELEMENTER".

DISSE SPILLER EN VIKTIG ROLLE HVIS MAN SKAL GRUNDIGERE PÅ MONOIDER, MEN DET ER IKKE PENSUM, SÅ DETTE ER BARE EN BEMERKNING.

EN SLIK MONOIDE ER "GENERERT" FRA $\{a_0, \dots, a_{n-1}\}$ SIDEN ALT ER BYGD OPP AV ELEMENTER FRA DENNE MENGDEN OG OPERASJONEN, OG DEN ER "FRI" I DEN FORSTAND AT ALT SOM GENERERES ER FORSKJELLIG. VI HAR INGEN EKSTRA LIKHETER SOM F.EKS. $a_0 * a_1 = a_2$

– MERK AT SLIKE MONOIDER SÅ ER STRENGER PÅ $\{a\}$ "STRUKTURLIK" MED $\mathbb{N}$ (MED + OG 0)

MAN KAN OVERSETTE



SLIK AT + SVARER TIL KONKATENERING.

VI KOMMER TILBAKE TIL BEGREPET "STRUKTURLIK" (ISOMORF) I FORBINDELSE MED GRAFER.

Definisjon 20.7 Inverse elementer

La en binær operasjon $*$ på en mengde S være gitt, og anta at e er et identitetselement for $*$. Hvis $a * b = b * a = e$, sier vi at a og b er **inverse** (*eng: inverse*) elementer. Vi sier også at **inversen til** a er b og skriver $a^{-1} = b$.

MERK I EN MONOIDE ER INVERSER UNIKE.

DVS, GITT a, HVIS b OG c ER INVERSER TIL a SÅ MÅ c = b.

$$c = e * c = (b * a) * c = b * (a * c) = b * e = b$$

ASSOSIATIV

Eks

1) $(\mathbb{N}, +, 0)$ FINNES DET INVERSER?

$4 + ? = 0$ GÅR IKKE

$0 + 0 = 0$ BARE 0 HAR INVERS.

2) $(\mathbb{Z}, +, 0)$

$4 + (-4) = 0$

$n + (-n) = 0$

3) $(\mathbb{N}, \cdot, 1)$ $4 \cdot ? = 1$ GÅR IKKE, VI TRENGER BRØKER

4) $(\mathbb{Q}, \cdot, 1)$

$4 \cdot \frac{1}{4} = 1$

$0 \cdot ? = 1$ GÅR IKKE. 0 HAR INGEN INVERS.

5) $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ $x \cdot \frac{1}{x} = 1$

FEKS $\frac{1}{4} \cdot \frac{1}{\frac{1}{4}} = \frac{1}{4} \cdot 4 = 1$.

- MERK SIDEN $e \circ e = e$ HAR e ALLTID INVERS, OG

$e^{-1} = e$.

Definisjon 20.8 Gruppe

La en binær operasjon $\bullet$ på en mengde G være gitt. Da er $\langle G, \bullet \rangle$ en **gruppe** (*eng: group*) hvis følgende betingelser, kalt **gruppeaksiomene** (*eng: group axioms*), er oppfylt.

- Operasjonen $\bullet$ er assosiativ.
- Det finnes et identitetselement for $\bullet$.
- Alle elementer har en invers.

Hvis vi i tillegg har at $\bullet$ er kommutativ, kalles gruppen **abelsk** (*eng: abelian*).

DVS EN GRUPPE ER EN MONOIDE DER ALLE ELEMENTER HAR EN INVERS

Eks
- $(\mathbb{Z}, +, 0)$
- $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$
- $(\{e\}, +, h)$

EBS

EN "NY" GRUPPE:

START MED $(\mathbb{Z}, +, 0)$

TA EKVIVALENS RELASJON E $x \sim y$ HVIS BEGGE ER PARTALL, ELLER BEGGE ODDE.

KVOTIENTMENGDEN

$$\mathbb{Z}/_{\sim} = \{ [0], [1] \}$$

DEFINER $* : \mathbb{Z}/_{\sim} \times \mathbb{Z}/_{\sim} \longrightarrow \mathbb{Z}/_{\sim}$

$$([x], [y]) \longmapsto [x+y]$$

VELDEFINERT FORDI

PARTALL + PARTALL = PARTALL

ODDE + -II- = ODDE

PARTALL + ODDE = ODDE

ODDE + ODDE = PARTALL

SÅ

$[0] + [0] = [0]$

$[1] + [0] = [1]$

$[0] + [1] = [1]$

$[1] + [1] = [0]$

ASSOSIATIV ✓

$[0]$ IDENTITET ✓

$[0]^{-1} = [0]$

$[1]^{-1} = [1]$

GRUPPE

ETT EKSEMPEL TIL / OPPGAVE

– LA X VÆRE EN MENGDE, OG LA $fun(X, X)$ VÆRE MENGDEN AV FUNKSJONER FRA X TIL X (så mengden av ulike operasjoner)

SJEKK AT DETTE ER EN MONOIDE HVIS OPERASJONEN ER FUNKSJONSSAMMENSETNING OG IDENTITETS ELEMENTET ER $id_X : X \to X$

– LA $BIJ(X)$ VÆRE MENGDEN AV BIJEKSJONER PÅ X.

SJEKK AT DETTE ER EN GRUPPE.

Definisjon 20.5 Idempotent

En unær operasjon f på en mengde S er **idempotent** (*eng: idempotent*) hvis det for alle $x \in S$ er slik at $f(f(x)) = f(x)$. En binær operasjon $*$ på en mengde S er **idempotent** (*eng: idempotent*) hvis det for alle $x \in S$ er slik at $x * x = x$.

Eks

UNÆR IDEMPOTENT:

$f : \mathbb{N} \to \mathbb{N}$

$n \mapsto 9$

$f(f(4)) = f(9)$

$= 9$

BINÆR IDEMPOTENT: $\cap : \mathcal{P}(X) \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$

$\langle A, B \rangle \longmapsto A \cap B$

$A \cap A = A$