Algebraiske Strukturer og det komplekse tallsystemet

[UTKAST!]

MAT1100 – Grunnlagsemnet

Simen Foldvik, 21. okt. 2020

Binæroperasjoner

Def En binæroperasjon på en mengde $A \neq \emptyset$ er en avbildning $A \times A \to A$.

Notasjon Dersom $A \times A \xrightarrow{*} A$ er en binæroperasjon og $a, b \in A$, skriver man gjerne $a * b$ (eller bare "ab" når $*$ er veldefinert) i stedet for $*(a,b)$.

Eks Addisjon på $\mathbb{N}$, på $\mathbb{Z}$, på $\mathbb{Q}$, på $\mathbb{R}$, på $\mathbb{C}$, på vektorer i $\mathbb{R}^n$, på matriser, på funksjoner, ...

for eksempel, gitt heltall $m, n \in \mathbb{Z}$ har vi summen $m+n \in \mathbb{Z}$ av m og n. $\rightsquigarrow$ binop. $+: \begin{cases} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ (m,n) \mapsto m+n. \end{cases}$

Eks Multiplikasjon på $\mathbb{N}$, på $\mathbb{Z}$, på $\mathbb{Q}$, på $\mathbb{R}$, på $\mathbb{C}$, ... osv.

Eks $*: \begin{cases} \mathbb{R}\times\mathbb{R} \to \mathbb{R} \\ (x,y) \mapsto \max\{x,y\}. \end{cases}$

Dette er en binop. $\max: \mathbb{R}\times\mathbb{R} \to \mathbb{R}$.

Tilsvarende for $\min: \mathbb{R}\times\mathbb{R} \to \mathbb{R}$.

Eks $\begin{cases} \mathbb{C}\times\mathbb{C} \to \mathbb{C} \\ (z,w) \mapsto z\bar{w} \end{cases}$ er en binop. på $\mathbb{C}$.

Eks La $\mathcal{F}$ = mengden av alle funksjoner $\mathbb{R} \to \mathbb{R}$.

Gitt $f, g \in \mathcal{F}$ definerer vi funksjonen

$$f+g: \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto f(x)+g(x) \end{cases}$$

dvs. $f+g \in \mathcal{F}$ og $(f+g)(x) = f(x) + g(x)$ for alle $x \in \mathbb{R}$.

Da er $+$ en binop. på $\mathcal{F}$.

:

Eks $\mathcal{F}$ = mengden av funksjoner $\mathbb{R} \to \mathbb{R}$.

Komposisjon er en binop. på $\mathcal{F}$: $\circ: \begin{cases} \mathcal{F}\times\mathcal{F} \to \mathcal{F} \\ (f,g) \mapsto g\circ f \end{cases}$.

Nøytrale elementer

Def La $*: A \times A \to A$ være en binær op. på $A \neq \emptyset$.

$e \in A$ kalles et nøytralt element for $*$ eller et identitetselement for $*$, dersom:

$$a * e = e * a = a \quad \text{for alle } a \in A.$$

[Merk: $e * e = e$.]

Prop $*$ har høyst ét identitet.

Bevis Anta $e, e' \in A$ er nøytrale for $*$. Da er:

$$e = e * e' = e'. \quad \blacksquare$$

Eks 1 er identitetselementet for $\mathbb{R}$ under multiplikasjon:

$$1 \cdot x = x \cdot 1 = x \quad \text{for alle } x \in \mathbb{R}.$$

Tilsvarende for $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$.

Eks 0 er identitetselementet for $\mathbb{R}$ under addisjon:

$$0 + x = x + 0 = x \quad \text{for alle } x \in \mathbb{R}.$$

Tilsvarende for $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$.

Ex $M_n(\mathbb{R})$ = alle $n \times n$ – matriser over $\mathbb{R}$.

$$I_n := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \operatorname{diag}(\underbrace{1, \ldots, 1}_{n})$$

er identitetselementet for $M_n(\mathbb{R})$ under matrisemult.

Nullmatrisen er id. for $M_n(\mathbb{R})$ under addisjon.

Ex $\mathcal{F}$ = alle funksjoner $\mathbb{R} \to \mathbb{R}$.

$\circ$: komposisjon av funksjoner.

$$id_{\mathbb{R}} : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto x \end{cases} \in \mathcal{F}$$ er nøytral for komposisjon:

$$f \circ id_{\mathbb{R}} = id_{\mathbb{R}} \circ f = f \quad \text{for alle } f \in \mathcal{F}.$$

Tilsvarende er id_A identitet for komposisjon

på mengden av alle avbildninger $A \to A$, hvor A er en mengde.

—

Kommutativitet og Assosiativitet

Def Binop. $A \times A \xrightarrow{*} A$ er:

i) kommutativ/abelsk: $a * b = b * a$ for alle $a, b \in A$.

ii) assosiativ: $(a * b) * c = a * (b * c)$

for alle $a, b, c \in A$.

Merk "Abelsk" etter Niels Henrik Abel.

Eks Addisjon/mult. på $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

er kommutative og assosiative op:

" $xy = yx$ og $(xy)z = x(yz)$ ".

Eks Multiplikasjon på $M_2(\mathbb{R})$ = 2×2-matriser over $\mathbb{R}$

er assosiativt men ikke kommutativt:

i) $(AB)C = A(BC)$ for alle $A, B, C \in M_2(\mathbb{R})$.

ii) Med $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ og $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ er

$$AB = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad \text{og} \quad BA = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

$\rightsquigarrow AB \neq BA$.

Inverser

Def La binop. $A \times A \xrightarrow{*} A$ ha nøytralt elem. $e \in A$.

La $a \in A$.

$b \in A$ er en invers for a (under/mhp. $*$)

dersom $a * b = b * a = e$.

Prop $*$ assosiativ og unital

$\Rightarrow$ alle $a \in A$ har høyst én invers.

Bevis La $e \in A$ være nøytral for $*$.

Anta $a \in A$ har inverser $b, b' \in A$.

Vi skal vise at $b = b'$:

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

$$= (b * a) * b' = e * b' = b'. \quad \blacksquare$$

Def Dersom $a \in A$ har invers $b \in A$, skriver vi

$$b = a^{-1}.$$

Dermed $a a^{-1} = a^{-1} a = e$ hvis a inverterbar.

Eks Alle elementer i $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ har inverser

mhp addisjon.

Eks Dersom $x \in \mathbb{R} \setminus \{0\}$, har x en multiplikativ invers $\frac{1}{x}$:

$$x\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)x = 1 .$$

Men $0 \in \mathbb{R}$ har ikke mult. invers: for dersom $y \in \mathbb{R}$ var en invers, måtte $0y = y0 = 1$, men vi har at

$$0y = y0 = 0 \quad \text{og} \quad 0 \neq 1.$$

Eks $1 \in \mathbb{Z}$ har mult. invers! $1 \cdot 1 = 1 \cdot 1 = 1$.

Men $2 \in \mathbb{Z}$ har ingen mult. invers i $\mathbb{Z}$:

for dersom $m \in \mathbb{Z}$ var en slik invers, måtte

$$2m = 1, \quad \text{og dermed} \quad m = \tfrac{1}{2},$$

som er en motsigelse: $\frac{1}{2} \notin \mathbb{Z}$.

Eks $M_2(\mathbb{R})$ = 2×2-mat. over $\mathbb{R}$. $\quad J := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Da er $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ den mult. identiteten for $M_2(\mathbb{R})$.

Men har at $J^2 = -I$. Dermed $J(-J) = (-J)J = I$,

så $J^{-1} = -J$.

Grupper, ringer, legemer

Def Gruppe: mengde $G \neq \emptyset$ med en binær op. $*$ og nøytralt element $e \in G$ slik at:

i) $*$ assosiativ: $(a*b)*c = a*(b*c)$ for alle $a, b, c \in G$.

ii) e nøytral: $g*e = e*g = g$ for alle $g \in G$.

iii) inverser: alle $g \in G$ har en invers i G:

$\exists h \in G \quad gh = hg = e \rightsquigarrow h = g^{-1}$.

(unik)

Eks $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$, $M_n(\mathbb{R})$, $\mathbb{F}$

er grupper under addisjon.

Disse er abelske/kommutative: $gh = hg$.

Eks $A \neq \emptyset$. Mengden av alle bijeksjoner $A \to A$

er en gruppe under komposisjon.

Generelt ikke abelsk.

Eks Følgende er grupper under multiplikasjon:

i) $\mathbb{Q}\setminus\{0\}$,

ii) $\mathbb{R}\setminus\{0\}$,

iii) $\mathbb{C}\setminus\{0\}$.

↑ Abelske

iv) $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A \text{ inverterbar}\}$

= mengden av inverterbare $n \times n$ – matr. over $\mathbb{R}$.

Generelt ikke abelsk.

v) $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ under mult.

Def Ring: mengde $R \neq \emptyset$ utstyrt med to binop. $+$ og $\cdot$ som er "kompatible":

i) $(R, +)$ abelsk gruppe med id. 0_R.

ii) $\cdot$ er assosiativ og unitær:

$(xy)\cdot z = x\cdot(y\cdot z)$ for $x, y, z \in R$,

man har et elem. $1_R \in R$ s.a.

$x \cdot 1_R = 1_R \cdot x = x$ for alle $x \in R$.

iii) $\cdot$ distribuerer over $+$:

$$\left.\begin{aligned} x\cdot(y+z) &= (x\cdot y) + (x\cdot z), \\ (x+y)\cdot z &= (x\cdot z) + (y\cdot z) \end{aligned}\right\} \text{ for alle } x, y, z \in R.$$

Def En ring $(R, +, \cdot)$ er kommutativ dersom

$$x \cdot y = y \cdot x \quad \text{for alle} \quad x, y \in R.$$

Def En kropp er en kommutativ ring $(R, +, \cdot)$

hvor $1_R \neq 0_R$ og alle elementer i $R \setminus \{0_R\}$

har en multiplikativ invers.

$$\forall x \in R \setminus \{0_R\} \quad \exists y \in R \quad x \cdot y = y \cdot x = 1_R.$$

Eks $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, er ringer (kommutativ).

Alle er kropper utenfor $\mathbb{Z}$: eksempelvis har

$2 \in \mathbb{Z}$ ingen mult. invers.

Eks $\mathbb{Z}/n = \{0, 1, \ldots, n-1\}$ er en kommutativ ring

under "addisjon og multiplikasjon modulo n".

$\mathbb{Z}/n$ er en kropp $\Leftrightarrow$ n er et primtall.

Obs $M_n(\mathbb{R})$ = $n \times n$ – matr. over $\mathbb{R}$ er en ring under

matrisadd. og – mult. ikke kommutativ;

(når n ≥ 2)

og det finnes $A \in M_n(\mathbb{R})$ som ikke er inverterbar

(dvs $\det A = 0$).

Senere i notatet skal vi konstruere kroppen $\mathbb{C}$

fra kroppen $\mathbb{R}$.

Homomorfi, isomorfi, innbedding

Homomorfi: strukturbevarende avbildning.

Def G, H grupper.

Gruppehomomorfi: avbildning

$f: G \to H$ slik at $f(gg') = f(g)f(g')$

for alle $g, g' \in G$.

Prop Dersom $f: G \to H$ gruppehomomorfi:

$f(e_G) = e_H$ og $f(g^{-1}) = f(g)^{-1}$.

Def R, S: ringer.

Ringhomomorfi: avbildning $f: R \to S$ slik at:

$$\left.\begin{aligned} f(r+r') &= f(r) + f(r'), \\ f(rr') &= f(r)f(r'), \end{aligned}\right\} \text{ for alle } r, r' \in R.$$

$$f(1_R) = 1_S.$$

Dette definerer også "homomorfi av kropper".

Def Bijektiv homomorfi = enbidding.

Def $G \xrightarrow{f} H$ homomorfi av grupper/ringer

$\rightsquigarrow$ f er en isomorfi hvis $\exists$ homomorfi $g: H \to G$

s.a. $f \circ g = id_H \wedge g \circ f = id_G$.

Dette forekommer hvis og bare hvis f er en bijektiv homomorfi. (Sjekk!)

Def Man skriver $G \simeq H$ hvis $\exists$ isomorfi $G \to H$.

Prop $\simeq$ er en ekvivalens: for alle G, G', G'':

i) $G \simeq G$, ii) $G \simeq G' \Rightarrow G' \simeq G$, iii) $G \simeq G' \wedge G' \simeq G''$
$\Rightarrow G \simeq G''$.

De kompleksе tallene

* Vi har for gitt at $\mathbb{R}$ er en kropp under ordinær addisjon og multiplikasjon av reelle tall.

* Vi skal konstruere kroppen $\mathbb{C}$ av kompleksе tall fra kroppen $\mathbb{R}$ av reelle tall..

Def $\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(x,y) : x,y \in \mathbb{R}\}$:

Elementer i $\mathbb{C}$: "kompleksе tall".

Def Vi har projeksjoner $Re, Im : \mathbb{C} \to \mathbb{R}$:

$$Re(x,y) = x, \quad Im(x,y) = y, \quad (x,y) \in \mathbb{C}.$$

Re: "realdel"; Im: "imaginærdel".

Def $1_{\mathbb{C}} := (1,0)$ og $i := (0,1)$,

hvor $0, 1 \in \mathbb{R}$.

Def $0_{\mathbb{C}} := (0,0)$.

* Vi definerer nå addisjon og mult. på $\mathbb{C}$:

Def $(a,b) + (c,d) := (a+c, b+d)$,

$(a,b)(c,d) := (ac - bd, ad + bc)$.

[for alle $(a,b), (c,d) \in \mathbb{C}$.]

Prop $(\mathbb{C}, +)$ er en abelsk gruppe med identitet $0_{\mathbb{C}}$:

i) $(z + z') + z'' = z + (z' + z'')$, $z, z', z'' \in \mathbb{C}$.

ii) $z + z' = z' + z$.

iii) $z + 0_{\mathbb{C}} = 0_{\mathbb{C}} + z$.

} for alle $z, z' \in \mathbb{C}$

iv) $-(a,b) = (-a, -b)$.

Prop $i^2 = -1_{\mathbb{C}}$.

Bevis $i^2 = (0,1)(0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$

$= -(1,0) = -1_{\mathbb{C}}$. ∎

Prop $1_{\mathbb{C}} z = z 1_{\mathbb{C}}$ for alle $z \in \mathbb{C}$.

Bevis $1_{\mathbb{C}} z = (1,0)(a,b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a)$

$= (a,b) = z$, og til svarende for $z 1_{\mathbb{C}}$. ∎

Prop $\mathbb{C}$ er en kommut. ring.

Bevis Har tidligere/påstått at $\mathbb{C}$ er en abelsk gruppe under addisjon.

Må sjekke at multiplikasjon er kompatibelt.

"Ring":

i) $(zz')z'' = z(z'z'')$.

ii') $1_{\mathbb{C}} z = z 1_{\mathbb{C}} = z$.

iii') $z(z' + z'') = zz' + zz''$,

$(z + z')z'' = zz'' + z'z''$.

for alle $z, z', z'' \in \mathbb{C}$.

iv) $zz' = z'z$ for alle $z, z' \in \mathbb{C}$.

("kommut. ring"). ∎

Prop $\mathbb{C}$ er en kropp.

Bevis Det gjenstår å vise at alle $z \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$ har en multt. invers.

Så la $z = (a,b) \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$. (så $(a,b) \neq (0,0)$.)

La $w := \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$.

Sjekk at $zw (= wz) = 1_{\mathbb{C}}$. ∎

Embedding $\mathbb{R} \hookrightarrow \mathbb{C}$

$\mathbb{R}$ og $\mathbb{C}$ er kropper.

Vi kan identifisere en kopi av $\mathbb{R}$ i $\mathbb{C}$ som følger.

Def Definer $j : \mathbb{R} \to \mathbb{C}$ ved

$$j(x) := (x, 0) \quad \text{for alle } x \in \mathbb{R}.$$

Prop j er en embedding av $\mathbb{R}$ i $\mathbb{C}$.

Bevis j er opplagt injektiv.

Man sjekker at j er en ringhomomorfi:

$$\left.\begin{aligned} &\text{i)} \quad j(x+y) = j(x) + j(y), \\ &\text{ii)} \quad j(xy) = j(x)\, j(y), \\ &\text{iii)} \quad j(1) = 1_{\mathbb{C}}. \end{aligned}\right\} \quad \text{for alle } x, y \in \mathbb{R}.$$

■

Def La $\tilde{\mathbb{R}} := j(\mathbb{R}) = \{ j(x) : x \in \mathbb{R} \} = \{ (x, 0) : x \in \mathbb{R} \}$.

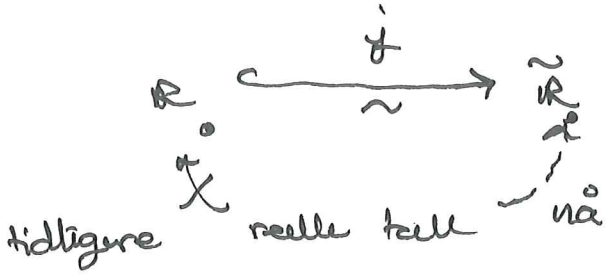
Siden j er en embedding $\mathbb{R} \hookrightarrow \mathbb{C}$, er

$\mathbb{R} \simeq \tilde{\mathbb{R}}$ som kropper.

* Dermed har vi $\tilde{\mathbb{R}} \subseteq \mathbb{C}$.

Gitt $x \in \mathbb{R}$ "identifiserer vi x med $j(x) = (x,0) \in \tilde{\mathbb{R}}$".

Skjematisk: reelle tall:



* Prop Under identifikasjonen $x \overset{j}{=} (x,0)$ har vi:

$$x + iy = (x,y) \quad \text{for alle} \quad x, y \in \mathbb{R}.$$

$$\rightsquigarrow \quad \mathbb{C} = \{ x + iy : \ x, y \in \mathbb{R} \}.$$

Bevis Gitt $x, y \in \mathbb{R}$:

$$x + iy \overset{j}{=} (x,0) + (0,1)(y,0)$$

$$= \cdots = (x,y). \quad \blacksquare$$

Alternativ konstruksjon

* Man kan også representere $\mathbb{C}$ som en undering av $M_2(\mathbb{R})$.

$M_2(\mathbb{R})$ = 2×2 – mat. over $\mathbb{R}$ er en ring.

Ikke abelsk/kommu. Identitet $I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for mult.

* La $J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Sjekk: $J^2 = JJ = -I$.

* La $K := \{ aI + bJ : a, b \in \mathbb{R} \}$

$$= \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R}).$$

Man sjekker at K er en ring. (Faktisk en legeme.)

under operasjonene indusert fra $M_2(\mathbb{R})$.

Prop $\mathbb{C} \simeq K$.

Bevis Avbildningen $\varphi : \mathbb{C} \to K$ gitt ved

$$\varphi(z) := \begin{bmatrix} \operatorname{Re} z & -\operatorname{Im} z \\ \operatorname{Im} z & \operatorname{Re} z \end{bmatrix}, \quad z \in \mathbb{C},$$

er en isomorfi $\mathbb{C} \xrightarrow{\sim} K$.

Dermed er K en kropp isomorf med $\mathbb{C}$. ∎

* Man sjekker at $\Phi(z_{\mathbb{C}}) = I$ og $\Phi(i) = J$.

Dermed kan vi representere komplekse tall som visse typer 2×2-mat. av reelle tall. ∎

$1 \leftrightarrow I$, $\quad i \leftrightarrow J$.

—