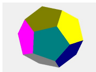
Elementær Gruppeteori



Ole Witt-Hansen 1981 (2018)

Indhold

1. Algebraiske strukturer

Vi skal her give en kort oversigt over nogle algebraiske begreber, nemlig *komposition*, *gruppe, ringe* og *legemer*. Disse begreber er blandt andet nødvendige for at indføre og beskrive de *komplekse* (imaginære) *tals legeme*.
Som udgangspunkt, vil vi se på egenskaberne ved de hele tal *Z*, de rationale tal *Q* (hele tal og brøker) og de reelle tal *R*, som omfatter de rationale tal, samt de irrationale tal (f.eks. $\sqrt{2}$ *og* π)

1.1 Komposition

Tallenes struktur er karakteriseret ved, at man for to vilkårlige (f.eks. rationale) tal *a* og *b* kan danne et nyt tal $a + b$, eller $a \cdot b$, som også er et rationalt tal.
Man siger at *addition* og *multiplikation* ("plus" og "gange") er *kompositioner* indenfor mængden af rationale tal.
Givet en mængde *M,* (som kan være næsten hvad som helst), så definerer man en komposition "*" indenfor mængden *M*, som en *afbildning* (en *funktion)* fra *M x M* ind i *M*.
I stedet for at skrive: $f(a,b) = c$, skriver man.

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

En komposition "*" er således en "regneregel", som til to vilkårlige elementer $a \in M, b \in M$ knytter netop et element $c \in M$, hvor: $c = a*b$

Eksempler

- Addition (+) er en komposition indenfor mængden af rationale tal: Hvis *a* og *b* er rationale tal er $c = a + b$ et rationalt tal.
- Multiplikation (·) er en komposition indenfor mængden af rationale tal: Hvis *a* og *b* er rationale tal er $c = a \cdot b$ et rationalt tal.
- Funktionssammensætning ($\circ$): $h = f \circ g \iff h(x) = f(g(x))$ er en komposition inden for mængden af afbildninger $f : R \to R$.
- Skalarproduktet: $\vec{a} \cdot \vec{b}$ er *ikke* en komposition indenfor mængden af vektorer, idet skalarproduktet er et tal og ikke en vektor. Krydsproduktet $\vec{a} \times \vec{b} = \vec{c}$ er derimod en (ikke kommutativ) komposition indenfor mængden af vektorer i rummet.
- Matrixmultiplikation er en (ikke kommutativ) komposition indenfor mængden af f.eks. 2 x 2 matricer, idet $\underline{\underline{C}} = \underline{\underline{A}}\ \underline{\underline{B}}$ er en 2 x 2 matrix.

Logiske operatorer
I det følgende vil vi ind imellem anvende nogle matematiske symboler, som tillader os at formulere sætninger på en kompakt og altid entydig måde.
De skrives mellem udsagn. (dvs. sætninger som enten er sande eller falske), hvis *p* og *q* er udsagn, gælder således:

"$p \wedge q$" *læses som* "*p og q*". (*Konjunktion*)
"$p \vee q$" *læses som* "*p eller q*" (*Disjunktion*)
"$\neg p$" *læses som* "*non p*" *eller* "*ikke p*, (*Negation*)
"$p \Rightarrow q$" *læses som* "*hvis p så q*" *eller* "*p medfører q*" (Implikation)
"$p \Leftarrow q$" *læses som* "*kun p hvis q*" (*Omvendt* Implikation)
"$p \Leftrightarrow q$" *læses som* "*p hvis og kun hvis q*" *eller* "*p er ensbetydende med q*" (*Dobbelt* Implikation)

Brug af kvantorer
Når man skal formulere matematiske sætninger, anvender man ofte to vendinger:

For ethvert x gælder: Dette skrives symbolsk med en *alkvantor*: $\forall x:$

Der findes et x for hvilket det gælder: Dette skrives symbolsk med en *eksistenskvantor*: $\exists x:$

Historisk note: Indtil 1988 var anvendelsen af logiske operatorer og kvantorer integreret i matematikundervisningen i gymnasiet. Men efter 2000 fandtes der hverken logiske operatorer eller kvantorer i lærebøgerne, med én undtagelse, nemlig mine egne bøger: "Elementær Matematik 1 – 11", som kun findes på min hjemmeside.
Fordelene ved anvendelsen af kvantorer og logiske operatorer er naturligvis at man kan udtrykke sig på en kort, og altid på den samme entydige måde

En komposition * indenfor en mængde *M* siges at være ***kommutativ*** , hvis

(1.2) $$\forall a \in M \ \forall b \in M: \ a * b = b * a$$

En komposition indenfor en mængde *M* siges at være ***associativ*** , hvis

(1.3) $$\forall a \in M \quad \forall b \in M \quad \forall c : \in M \quad a * (b * c) = (a * b) * c$$

Hvilket ofte skrives kortere: $\forall a, b, c \in M: \ a * (b * c) = (a * b) * c$

Når det drejer sig om tal, plejer man at udtrykke associativitet, som "addendernes eller faktorernes rækkefølge er underordnet".

Et element *e* siges at være et ***neutralt element*** ved en komposition, hvis og kun hvis:

(1.4) $$\forall a \in M: \ a * e = e * a = a$$

Der kan kun være et neutralt element. Antages det nemlig, at e_1 og e_2 er neutrale elementer, så må der gælde:

$e_1 * e_2 = e_2$ fordi e_1 er neutralt og $e_1 * e_2 = e_1$ fordi e_2 er neutralt

Når det gælder tal, er det neutrale element ved addition som bekendt tallet 0, og det neutrale element ved multiplikation som bekendt tallet 1.

Et element *b* kaldes inverst til *a*, hvis der gælder:

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

Det inverse element til *a* kan betegnes a^{*-1} eller blot a^{-1} (hvis misforståelser kan undgås), men også andre betegnelser er mulige, f.eks. $-a$ eller $\frac{1}{a}$.

Hvis en komposition er associativ, kan et element højst have ét inverst element:
Antager vi nemlig, at et element *a*, har to inverse elementer b_1 og b_2 , for så må der gælde:

$$(b_1 * a) * b_2 = e * b_2 = b_2 \ = \ b_1 * (a * b_2) = b_1 * e = b_1$$

Hvis a har et inverst element, har ligningerne: $x * a = b \quad og \quad a * x = b$ netop en løsning

$$x * a = b \quad \Leftrightarrow \quad x * a * a^{*-1} = b * a^{*-1} \quad \Leftrightarrow \quad x = b * a^{*-1}$$

og tilsvarende

$$a * x = b \quad \Leftrightarrow \quad x = a^{*-1} * b$$

1.2 Homomorfi

Vi betragter først den algebraiske struktur: (R_+, $\cdot$) (positive reelle tal med kompositionerne "plus" og "gange"), samt den naturlige logaritme *ln*.

Den naturlige logaritme er en *bijektion* af (R_+, $\cdot$) på (R, +), som bevarer den algebraiske struktur, idet:

(1.6) $$x = \ln(a) \;\wedge\; y = \ln(b) \;\Rightarrow\; \ln(a \cdot b) = \ln(a) + \ln(b) = x + y$$

Dette begrunder definitionen af en ***homomorfi.***

En afbildning *f* kaldes en homomorfi af $(M,*)$ på $(H,\circ)$. (hvor M og H er to mængder med kompositionerne $*$ *og* $\circ$), hvis: $\forall a \in M \;\; \forall b \in M : f(a * b) = f(a) \circ f(b)$

Hvis *f* er en bijektion (som det er tilfældet med *ln*) så kaldes den en ***isomorfi***.
Lad $(M,*)$ og $(H,\circ)$ være to algebraiske strukturer. Og lad *f* være en isomorfi af $(M,*)$ på $(H,\circ)$.
Der gælder da en række temmelig indlysende sætninger:

1. Hvis *f* er en isomorfi af $(M,*)$ på $(H,\circ)$, så er f^{-1} er en isomorfi af $(H,\circ)$ på $(M,*)$.
Bevis:

$$x = f(a) \;\Leftrightarrow\; a = f^{-1}(x) \quad og \quad y = f(b) \;\Leftrightarrow\; b = f^{-1}(y) \quad \Rightarrow$$

(1.7) $$a * b = f^{-1}(x) * f^{-1}(y)$$

$$f(a * b) = f(a) \circ f(b) = x \circ y \quad \Leftrightarrow \quad f^{-1}(x \circ y) = a * b = \; f^{-1}(x) * f^{-1}(y)$$

2. Hvis $*$ er kommutativ/associativ, så er også $\circ$ kommutativ/associativ.
Bevis:

(1.8) $$f(a * b) = f(b * a) = f(a) \circ f(b) = f(b) \circ f(a)$$

Associativiteten vises helt tilsvarende.

3. Sætning: Det neutrale element i (M, $*$) afbildes i det neutrale element i (H, $\circ$).
Bevis:

(1.9) $$f(a) = f(a * e_*) \; = f(a) \circ f(e_*) \;\Rightarrow\; f(e_*) = e_o$$

4. Det inverse element i (M, $*$) afbildes i det inverse element i (H, $\circ$).
Bevis:

$$f(e_*) = e_\circ = f(a * a^{*-1}) = f(a) \circ f(a^{*-1}) = x \circ y \;\Rightarrow\; y = x^{\circ -1}$$

2. Grupper, ringe og legemer

En algebraisk struktur $(G, *)$ kaldes en *gruppe*, hvis.

1. Kompositionen * er associativ.
2. Der findes et neutralt element *e*.
3. Ethvert element har et inverst element.

Eksempler:
Mængden af hele tal med kompositionen + $(Z, +)$ danner en gruppe.
Mængden af regulære matricer $(\underline{M}, \cdot)$ danner en gruppe. (F.eks. 2 x 2 matricer, hvor $\det(\underline{M}) \neq 0$)
Inden for en gruppe gælder forkortningsreglen:

$$x * a = y * a \Rightarrow x = y \quad og \quad a * x = a * y \Rightarrow x = y$$

Begge dele følger ved multiplikation med a^{*-1} fra venstre eller fra højre.

Den sidste betingelse er kun nødvendig, hvis * ikke er kommutativ

2.1 Algebraiske ringe

Lad os dernæst antage, at vi har en algebraisk struktur $(M, *, \circ)$, som er organiseret ved to kompositioner. $*$ siges at være distributiv med hensyn til $\circ$, hvis den distributive lov gælder:

(2.1)
$$\forall a,b,c \in M : a*(b \circ c) = a*b \circ a*c$$
$$\forall a,b,c \in M : (b \circ c)*a = b*a \circ c*a$$

Eksempel De hele tal *Z* er organiseret ved kompositionerne + og $\cdot$ (plus og gange), idet, der som bekendt for alle hele tal gælder:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Derimod er + ikke distributiv med hensyn til $\cdot$, idet der i almindelighed ikke gælder:

$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

En algebraisk struktur $(M, *, \circ)$ siges at udgøre en ***ring***, hvis:

- $(M, *)$ er en kommutativ gruppe.
- $\circ$ er kommutativ og associativ.
- * er distributiv mht. $\circ$, altså, hvis: $\forall a,b,c \in M : a*(b \circ c) = a*b \circ a*c$

Eksempel: $(Z, +, \cdot)$ udgør en ring. Det neutrale element ved addition er 0, og det neutrale element ved multiplikation er 1. Det inverse element til *a* betegnes $-a$.

I det følgende vil vi for overskuelighedens skyld skrive "+" i stedet for "*" og "·" i stedet for "$\circ$", også selv om det ikke drejer sig om tal.
Det neutrale element ved + betegnes herefter som 0, og hvis der findes et neutralt element ved · vil det blive betegnet med 1, også selv om det ikke betegner et tal.

Det inverse element til *a* ved +, betegnes –*a*, og hvis der findes et inverst element til *a* mht. til · , så vil det blive betegnet med a^{-1}.
Der gælder en række små sætninger.

1. $\forall a \in M : a \cdot 0 = 0$.
2. $\forall a, b \in M : a \cdot (-b) = (-a) \cdot b = -a \cdot b$
3. $\forall a, b \in M : (-a) \cdot (-b) = a \cdot b$

Bevis:

1. $a \cdot b = a \cdot (b + 0) = a \cdot b + a \cdot 0 \quad \Rightarrow \quad a \cdot 0 = 0$
2. $a \cdot (b + (-b)) = a \cdot 0 = 0 = a \cdot b + a \cdot (-b)$.
   $a \cdot (-b)$ er således det modsatte element til $a \cdot b$, altså lig med $-a \cdot b$.
3. $(-a) \cdot (b + (-b)) = 0 = -a \cdot b + (-a)(-b)$.
   $(-a)(-b)$ er således det modsatte tal til $-a \cdot b$ altså lig med $a \cdot b$, hvor vi har anvendt resultatet fra 2.
   At $-(-a) = a$ følger af at $-(-a)$ er det modsatte element til $(-a)$ altså lig med *a*.

Det er altså den universelle gyldighed af den distributive lov, der leverer forklaringen på hvorfor ”*minus*” gange ”*minus*” giver ”*plus*”.

Hvis $a \neq 0 \ \wedge \ b \neq 0$ og $a \cdot b = 0$ kaldes *a* og *b* for nuldivisorer.
Der findes ingen nuldivisorer i de reelle tal.
Hvis en ring ikke indeholder nuldivisorer, gælder *nulreglen* og forkortningsreglerne:
Nulreglen:

(2.2) $$a \cdot b = 0 \quad \Leftrightarrow \quad a = 0 \ \vee \ b = 0$$

Forkortningsreglen:

(2.3) $x \neq 0 \ \wedge \ x \cdot a = x \cdot b \ \Rightarrow \ a = b$ og tilsvarende: $x \neq 0 \ \wedge \ a \cdot x = b \cdot x \ \Rightarrow \ a = b$

Bevis:

$$x \neq 0 \ \wedge \ x \cdot a = x \cdot b \quad \Leftrightarrow \quad x \cdot a - x \cdot b = 0 \ \Leftrightarrow \ x \cdot (a - b) = 0 \ \Leftrightarrow \ a - b = 0 \ \Leftrightarrow \ a = b = 0$$

2.1 Algebraiske legemer

Et legeme (*L*, +, ·) kan karakteriseres som en mængde, hvor:

1. (*L*, +) er en kommutativ gruppe.
2. $(L \backslash \{0\}, \cdot)$ er en kommutativ gruppe.
3. Den distributive lov gælder: $\forall a, b, c \in M : a \cdot (b + c) = a \cdot b + a \cdot c$.

En mængde *M* siges at være et dellegeme af *L*, hvis $M \subseteq L$ og (*M*, +, ·) er et legeme.

De rationale tal *Q* et tal legeme, som indeholder de hele tal *Z*.
De reelle tal *R* er et tal legeme, som indeholder de rationale tal.

De komplekse tal *C* er et legeme, som har de reelle tal som del-legeme.

To legemer $(L, +, \cdot)$ og $(M, *, \circ)$ siges at være isomorfe, hvis der findes en bijektion φ, som opfylder kravene for en isomorfi.

(2.3) $\forall a,b \in L : \varphi(a+b) = \varphi(a) * \varphi(b)$ og $\forall a,b \in L : \varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$

Hvis to legemer er isomorfe er de algebraisk identiske. Man kan opfatte de to legemer (i algebraisk henseende), som det samme legeme, hvor blot elementerne har skiftet navn fra *a* til φ(*a*), og kompositionerne har skiftet navn fra "+" til "*" og fra "·" til "∘".

En mængde siges at være ordnet, hvis der findes en ordningsrelation (et sammenlignings-kriterium), der opfylder visse krav.

Hvis "<" er en ordningsrelation, så skal den opfylde følgende to krav:

1. $\forall a,b \in M : a \neq b \;\Rightarrow\; a < b \;\vee\; b < a$
2. $a < b \;\wedge\; b < c \;\Rightarrow\; a < c$ (Ordningsrelationen er transitiv)

De hele tal *Z*, de rationale tal *Q* samt de reelle tal *R* er ordnet efter ordningsrelationen "<", "mindre end". Der findes derimod ingen ordningsrelation for de komplekse tal, således at kravene 1. og 2. er opfyldt.

3. Et udvidelseslegeme til de rationale tal, hvor ligningen $x^2 = 2$ har en rod

Vi bemærker først, at intet rationalt tal kan være rod i ligningen $x^2 = 2$.
Antage nemlig at en *uforkortelig brøk* $x = \frac{p}{q}$, hvor *p* og *q* er hele positive tal er rod i ligningen, så vil der gælde: $(\frac{p}{q})^2 = 2 \;\Leftrightarrow\; p^2 = 2q^2$, så p^2 og dermed *p* må være et lige tal.
Vi sætter derfor:

$$p = 2r, \text{ og får: } (\tfrac{2r}{q})^2 = 2 \;\Leftrightarrow\; 4r^2 = 2q^2 \;\Leftrightarrow\; q^2 = 2r^2$$

Heraf slutter vi at q^2 og dermed *q* er et lige tal. Dette i strid med at brøken $x = \frac{p}{q}$ er uforkortelig, så $x = \frac{p}{q}$ kan ikke være et rationalt tal.

Lad os derfor antage, at der findes et tal som er rod i ligningen: $x^2 = 2$, som vi betegner med $\sqrt{2}$.
Ifølge ovenstående kan $\sqrt{2}$ ikke være et rationelt tal.

Vi vil da vise, at man kan udvide de rationale tals legeme il et legeme, hvor ligningen $x^2 = 2$, har en rod.
Foreløbig kan vi ikke vide om et sådant legeme eksisterer, men vi kan opstille visse krav, som en talmængde skal opfylde for at den udgør et legeme.
Det vi foretager kaldes en analyse, idet vi antager at der faktisk findes et udvidelseslegeme *L*, hvoraf vi så drager nogle nyttige konklusioner om strukturen af *L*.
Hvis $\sqrt{2}$ er et tal, så skal man kunne addere og multiplicere det med rationale tal efter de sædvanlige regneregler.
Heraf slutter vi, at hvis legemet *L* indeholder tallet $\sqrt{2}$, så må det også indeholde alle tallene

$q_1 + \sqrt{2}\, q_2$, hvor q_1 og q_2 er rationale tal.
Ved anvendelsen af de sædvanlige regneregler for tal, viser det sig, at denne talmængde faktisk udgør et legeme, som er det mindste tallegeme L, som indeholder tallet $\sqrt{2}$.
At kompositionerne plus "+" og gange "·" faktisk er kompositioner i L, kan ses af følgende, hvor p, q, r er rationale tal.

$$
\begin{aligned}
&(p_1+\sqrt{2}p_2)+(q_1+\sqrt{2}q_2) = p_1+q_1+\sqrt{2}(p_2+q_2) \\
(3.1) \qquad &(p_1+\sqrt{2}p_2)\cdot(q_1+\sqrt{2}q_2) = p_1q_1+2p_2q_2+\sqrt{2}(p_1q_2+p_2q_1)
\end{aligned}
$$

Heraf ses, at summen og produktet af to tal, som tilhører L også tilhører mængden L.
At summen og produkt er kommutative og associative er næsten indlysende, da de rationale tal netop har disse egenskaber.
Endvidere findes der et nul-element, nemlig $q_1 = q_2 = 0$. Der findes også et 1-element, nemlig $q_1 = 1$ og $q_2 = 0$. Det modsatte tal til $q_1 + \sqrt{2}\, q_2$, er indlysende - ($q_1 + \sqrt{2}\, q_2$).

Ethvert element q i $L\backslash\{0\}$ har endvidere et inverst element, som er løsning til ligningen:

$$
xq = 1 \;\Leftrightarrow\; x(q_1+\sqrt{2}q_2) = 1 \;\Leftrightarrow\; x = \frac{1}{(q_1+\sqrt{2}q_2)} = \frac{(q_1-\sqrt{2}q_2)}{(q_1^2-2q_2^2)} = \frac{q_1}{q_1^2-2q_2^2} - \sqrt{2}\frac{q_2}{q_1^2-2q_2^2}
$$

Hvoraf ses, at det inverse element til q også tilhører L. (Det inverse element til $\sqrt{2}$ er $\frac{\sqrt{2}}{2}$).
Det bemærkes, at: $q_1^2 - 2q_2^2 = 0 \;\Rightarrow\; q_1 = q_2 = 0 \;\vee\; (\frac{q_1}{q_2})^2 = 2$, hvilket er umuligt, da $(\frac{q_1}{q_2})$ er et rationalt tal.
Til slut bemærker vi, at den distributive lov gælder; $q(r+p) = qr + qp$, hvor p, q, r tilhører L.

$$
\begin{aligned}
&(q_1+\sqrt{2}q_2)((r_1+\sqrt{2}r_2)+(p_1+\sqrt{2}p_2) = \\
&(q_1+\sqrt{2}q_2)((r_1+p_1)+\sqrt{2}(r_2+p_2)) = \\
(3.2) \qquad &q_1(r_1+p_1)+2q_2(r_2+p_2)+\sqrt{2}(q_2(r_1+p_1)+q_1(r_2+p_2)) = \\
&q_1r_1+2q_2r_2+\sqrt{2}(q_2r_1+q_1r_2)+q_1p_1+2q_2p_2+\sqrt{2}(q_2p_1+q_1p_2) = \\
&(q_1+\sqrt{2}q_2)(r_1+\sqrt{2}r_2)+(q_1+\sqrt{2}q_2)(p_1+\sqrt{2}p_2)
\end{aligned}
$$

Bemærk at gyldigheden af den distributive lov udelukkende hviler på de opstillede regneregler.

Ud fra denne analyse, kan man opstille en mere formel udvidelse af de rationale tal til et legeme, hvor ligningen: $x^2 = 2$, har en rod.
Formelt vil man (på grund af vores analyse) gå frem som følger:

Vi betragter en mængde af talpar (q_1, q_2), hvor q_1 og q_2 er rationale tal.
For disse talpar definerer man kompositionerne $\oplus$ og $\otimes$ på følgende måde:

$$(3.2)\qquad \begin{aligned}(q_1,q_2)\oplus(p_1,p_2)&=(q_1+p_1,q_2+p_2)\\(q_1,q_2)\otimes(p_1,p_2)&=(q_1p_1+2q_2p_2,p_1q_2+q_2p_1)\end{aligned}$$

Men den analyse, vi allerede har lavet er det så indlysende, at vise at mængden:

$$L=\{(q_1,q_2)\,|\,q_1\in Q\wedge q_2\in Q\}$$

Udgør et tallegeme.
Det skulle også være klart, hvilket kan umiddelbart verificeres, at mængden:

$Q_1=(q_1,0)\,|\,q_1\in Q\,\}$ er isomorf (identisk med) de rationale tals legeme.

Det er klart at nul-elementet i L er (0,0) og ét elementet i L er (1,0).

Som eksempel, vil vi vise, at $\left(\frac{q_1}{q_1^2-2q_2^2},-\frac{q_2}{q_1^2-2q_2^2}\right)$ er det inverse element til (q_1,q_2)

$$(q_1,q_2)\ \otimes\ \left(\frac{q_1}{q_1^2-2q_2^2},-\frac{q_2}{q_1^2-2q_2^2}\right)=$$

$$(3.3)\qquad \left(q_1\frac{q_1}{q_1^2-2q_2^2}-2q_2\frac{q_2}{q_1^2-2q_2^2},q_2\frac{q_1}{q_1^2-2q_2^2}-q_1\frac{q_2}{q_1^2-2q_2^2}\right)=(1,0)$$

Til slut vil vi udregne elementet: $(0,1)\otimes(0,1)=(2,0)$
Hvis vi betegner (0,1) med symbolet $\sqrt{2}$ og identificerer (2,0) med det rationale tal 2,(på grund af den nævnte isomorfi), gælder det åbenbart at: $(0,1)=\sqrt{2}\in L$ og $(\sqrt{2})^2=2$.

Hermed er det faktisk lykkedes at udvide de rational tals legeme til et legeme, hvor ligningen:

$$x^2=2$$

har en rod.

3.1 De komplekse tals legeme

Efter helt de samme retningslinier, kan man vise, at man kan udvide de reelle tals legeme til et legeme til et tallegeme, hvor ligningen:

$$x^2 = -1$$

har en rod. Dette tallegeme kaldes som bekendt de komplekse tal, og de to rødder i ligningen betegnes i og $-i$, hvor der så gælder at $i^2 = -1$.

For et komplekst tal skriver man $(a_1, a_2) = a_1+ia_2$ i stedet for $(q_1, q_2) = q_1+\sqrt{2}q_2$

Fra et algebraisk synspunkt, er der ingen strukturel forskel på de to udvidelser.

Hvis vi ubekymret regner med de komplekse tal, som med reelle tal, idet vi husker at $i^2 = -1$ får vi:

(3.5)
$$a + b = a_1 + ia_2 + (b_1 + ib_2) = a_1 + b_1 + i(a_2 + b_2)$$
$$a - b = a_1 + ia_2 - (b_1 + ib_2) = a_1 - b_1 + i(a_2 - b_2)$$

(3.6)
$$a \cdot b = (a_1 + ia_2) \cdot (b_1 + ib_2) = a_1b_1 - a_2b_2 + i(a_2b_1 + a_1b_2)$$

At dette virkelig er kompositioner, som udgør et kommutativt og associativt legeme, er relativt let at vise. Den distributive lov vises ligesom ovenfor.
At 0 og 1 er de neutrale elementer ved addition og multiplikation er indlysende ud fra (3.5) og (3.6)

For at vise, at ethvert element forskelligt fra nul har et inverst element vises lettest, ved at indføre det komplekst konjugerede $\overline{a}$ til et komplekst tal $a = (a_1 + ia_2)$.

(3.7)
$$\overline{a} = a_1 - ia_2$$

Det følger så:

(3.7)
$$a \cdot \overline{a} = |a|^2 = (a_1 + ia_2)(a_1 - ia_2) = a_1^{\ 2} + a_2^{\ 2}$$

(3.8)
$$|a| = \sqrt{a_1^{\ 2} + a_2^{\ 2}}$$

Kaldes for modulus eller den numeriske værdi af et komplekst tal.

For et komplekst tal $a + ib$, skal vi altså bestemme et komplekst tal $x + iy$, således, at:

$$(a + ib)(x + iy) = 1$$

Multiplicerer vi denne ligning med det komplekst konjugerede til $a + ib$, får vi:

(3.9)
$$(a^2 + b^2)(x + iy) = a - ib \quad \Rightarrow \quad x + iy = \frac{a - ib}{(a^2 + b^2)}$$

Der er tradition for at man aldrig skriver et komplekst tal i nævneren af en brøk, så hvis vi skal udregne $\frac{a}{b}$, hvor $a = (a_1 + ia_2)$ og $b = (b_1 + ib_2)$ er komplekse tal, ganger man blot med det komplekst konjugerede til b i tæller og nævner: $\frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} = \frac{a\overline{b}}{|b|^2} = \frac{(a_1 + ia_2)(b_1 - ib_2)}{b_1^{\ 2} + b_2^{\ 2}}$

De komplekse tal bliver mere udførligt behandlet i heftet: Komplekse tal, som findes på min hjemmeside under matematik.