

GRUPPE TEORI

Flemming P. Pedersen

Afskrift af forelæsningsnoter ved Jens Jensen

(Ørsted Laboratoriet, NBIfAFG, april 2003)

Indholdsfortegnelse

1. Indledning	1
2. Gruppebegrebet	1
3. Den symmetriske gruppe	5
4. Ækvivalensrelation. Klasser af konjugerede elementer	8
5. Sideklasser	12
6. Invariante undergrupper	13
7. Homomorfi og isomorfi	16
8. Direkte produkt af grupper	20
9. Repræsentation af en gruppe ved lineære transformationer	22
10. Reducibel og irreducibel repræsentation	28
11. Schur's lemma og ortogonalitetsrelationerne	28
12. Kontinuerte grupper	36
Opgaver	43

1. Indledning

Lagrange kom omkring 1770 ind på gruppebegrebet i forbindelse med undersøgelse af algebraiske ligninger. Hans problem var det næsten klassiske: at løse en algebraisk ligning ved hjælp af rodstørrelser alene. Forskellige matematikere, deriblandt *Euler*, havde løst dette problem op til fjerdegradsligninger, men ingen var nået derudover. *Lagrange* brugte i sine undersøgelser permutationer af rødderne i en algebraisk ligning, og selv om han ikke explicit formulerede gruppebegrebet, kan hans resultater i dag bedst udtrykkes ved hjælp af *permutationsgrupper*.

Det blev imidlertid ikke *Lagrange*, som løste problemet. Den norske matematiker *Abel* og den italienske læge *Ruffini* viste på få detaljer nær, og uafhængigt af hinanden, at den almindelige algebraiske ligning af grad n , kan for $n \geq 5$, ikke løses ved rodstørrelser alene. Et vigtigt biprodukt ved Abels bevis var, at det inspirerede *Galois* til at give sig i kast med lignende problemer, og *Galois* indførte såvel glosen som begrebet *gruppe*. *Galois'* grupper var *endelige*, men senere kom også *uendelige grupper* ind i den matematiske forskning, og nordmanden *Sophus Lie* indførte i ca. 1870 *kontinuerte grupper*.

Dermed var gruppebegrebet vandret fra algebraen over geometrien og ind i den matematiske analyse og har siden bredt sig i næsten enhver matematisk disciplin.

Det bliver hurtigt for vidtløftigt at medtage flere detaljer om den historiske udvikling, men det skal lige nævnes at englænderen *Cayley* i ca. 1854 var blandt de første til at indføre gruppebegrebet ved et aksiomssystem – meget nær, som vi gør det i dag, samt at svenskeren *Frobenius* omkring 1890 prøvede på at karakterisere samtlige endelige grupper; herved indførte han, hvad vi nu kalder gruppekarakterer, et begreb, som næsten direkte er ansvarlig for, at gruppebegrebet i 1930'erne kom ind i kvantemekanikken.

2. Gruppebegrebet

Lad $(G, \circ)$ betegne en *organiseret mængde*; hermed mener vi en mængde G forsynet med en *kompositionsregel* $\circ$, der til et hvert ordnet par af elementer $a, b \in G$ knytter et element $a \circ b \in G$. Det skal fremhæves, at a og b kan være ens eller forskellige, og at i almindelighed er $a \circ b \neq b \circ a$.

$(G, \circ)$ kaldes en *gruppe*, når følgende tre aksiomer er opfyldt:

- 1) Den *associative lov* gælder, dvs. for alle $a, b, c \in G$ gælder $a \circ (b \circ c) = (a \circ b) \circ c$.
- 2) Der findes et neutralt element $e \in G$, således at for alle $a \in G$ gælder $a \circ e = e \circ a = a$.
- 3) Til ethvert $a \in G$ findes der et *inverst* element $a^{-1} \in G$, således at $a \circ a^{-1} = a^{-1} \circ a = e$.

Hvis yderligere $a \circ b = b \circ a$ for alle $a, b \in G$, kaldes gruppen *kommutativ* eller *abelsk*.

Vi skal først kommentere gruppeaksiomerne:

Undertiden medtager man i aksiomerne det krav, at mængden G er *stabil* eller *afsluttet* med hensyn til $\circ$; dvs. $a, b \in G \Rightarrow a \circ b \in G$; dette er her henlagt til begrebet organiseret mængde (se ovenfor).

Vedr. 1): Den associative lov kan udvides til at gælde for flere end tre faktorer; dette gøres fx ved induktion.

Tegnet $\circ$ udelades i det følgende, og $a \circ b$ betegnes blot ab .

Vedr. 2): En gruppe har kun et neutralt element. Antag nemlig at både e_1 og e_2 var neutrale elementer. Så var $e_1 = e_1 e_2 = e_2$.

Vedr. 3): Vi kan retfærdiggøre betegnelsen a^{-1} , idet der gælder, at ethvert element $a \in G$ har kun et inverst element. Antag nemlig, at både x og y , begge elementer i G , var inverse til a . Så var $x = xe = x(ay) = (xa)y = ey = y$.

Sætning (2.1)

I en gruppe har "divisionsligningerne"

$$ax = b \quad ; \quad ya = b$$

hver for sig netop én løsning.

Bevis: Hvis x er en løsning til $ax = b$, så er

$$a^{-1}(ax) = a^{-1}b \quad \text{og} \quad a^{-1}(ax) = (a^{-1}a)x = ex = x$$

og dermed

$$x = a^{-1}b,$$

En prøve viser, at $a^{-1}b$ er løsning til den første ligning, og dermed, at $ax = b \Leftrightarrow x = a^{-1}b$. Den anden ligning behandles tilsvarende; man finder

$$y = ba^{-1}.$$

Korollar (2.2)

I en gruppe gælder "forkortningsreglerne"

$$ax = ay \Rightarrow x = y \quad ; \quad xb = yb \Rightarrow x = y.$$

Korollar (2.3)

Lad $a \in G$ være et fastholdt element. Så er afbildningen givet ved $x \mapsto ax$ en enentydig afbildning af gruppen G på sig selv, $G \mapsto G$.

Definition: Hvis elementantallet i G er n , kaldes gruppen G *endelig af n 'te orden*. Hvis G indeholder uendelig mange elementer kaldes gruppen *uendelig*.

Definition: Lad H være en delmængde af en gruppe G , og antag at H er stabil med hensyn til kompositionsreglen i G ; så kaldes H en *undergruppe* i G , hvis den organiserede mængde H er en gruppe.

Idet vi henviser til gruppeaksiomerne kan vi straks formulere følgende kriterium:

Sætning (2.4)

En delmængde H af en gruppe G er en undergruppe, hvis og kun hvis følgende gælder:

- 1) $a, b \in H$ medfører $ab \in H$.
- 2) Det neutrale element $e \in G$ tilhører H .
- 3) $a \in H$ medfører $a^{-1} \in H$.

Definition: En endelig gruppe G kaldes *cyklisk*, hvis G indeholder et element a med den egenskab, at et vilkårligt element $b \in G$ kan skrives $b = aa \cdots a$ (p faktorer), eller kort $b = a^p$. Elementet a siges at *frembringe* gruppen.

I tilknytning til denne definition skal vi for grupper i almindelighed nævne, at man sædvanligvis fastsætter $a^0 = e$ og $a^{-p} = (a^{-1})^p$, p positivt helt tal. Det er da let at indse, at man kan benytte de sædvanlige potensregneregler:

$$a^r a^s = a^{r+s} \quad ; \quad (a^r)^s = a^{rs}$$

for *alle* hele tal r og s . Man udvider herefter begrebet cyklisk gruppe:

Definition: En gruppe G (endelig eller uendelig) kaldes cyklisk, hvis G indeholder et element a , så at et vilkårligt $b \in G$ kan skrives som en potens af a .

Øvelse 1: Vis, at i en abelsk gruppe G er $(ab)^n = a^n b^n$ (gælder ikke i almindelighed). Vis endvidere, at i en vilkårlig gruppe gælder $(ab)^{-1} = b^{-1} a^{-1}$.

Definition: Ved *ordenen* af et element $a \in G$ forstås ordenen af den af a frembragte (under)gruppe.

Vi skal illustrere denne definition med følgende bemærkninger:

Lad $a \in G$, så er potenserne $a^0 = e, a, a^1, a^2, \dots$ alle elementer i G . Hvis disse potenser er indbyrdes forskellige, så er G af uendelig orden, idet a frembringer en uendelig cyklisk (under)gruppe i G . I modsat fald er to potenser ens, fx $a^r = a^s$ ($r < s$) og $a^{s-r} = e$. I dette tilfælde slutter vi, at *ordenen h af elementet a er den laveste positive eksponent, for hvilken $a^h = e$* , og a frembringer en cyklisk undergruppe H af *h*te orden bestående af $\{e, a, a^2, \dots, a^{h-1}\}$. Thi

- 1) $a^r a^s = a^{r+s} = a^{r+s-h} \in H$
- 2) $a^0 = a^h = e \in H$
- 3) $(a^r)^{-1} = a^{-r} = a^{h-r} \in H$ (jvf. (2.4)).

Sætning (2.5)

Lad G være en endelig gruppe af orden g , H en undergruppe (i G) af orden h , så er h divisor i g .

Bevis: Sætningen er triviell, hvis h er en af de to *trivielle undergrupper* i G , dvs. hvis H er enten hele G eller gruppen bestående af det neutrale

element alene. Altså antager vi, at $1 < h < g$, og lad $a_1, a_2, \dots, a_h$ betegne elementerne i H . Vi kan nu vælge et element $b \in G$, men $b \notin H$. Så er $ba_1, ba_2, \dots, ba_h$ indbyrdes forskellige (følger af forkortningsreglerne) og *ikke* elementer i H ; dette sidste begrundes med, at hvis $ba_i = a_j$ så var $b = a_j a_i^{-1} \in H$ i modstrid med ovenfor. Hermed kender vi i alt $2h$ elementer i G , og hvis disse udtømmer G er sætningen vist. Ellers kan vi vælge et $c \in G$ og c forskellig fra de nævnte $2h$ elementer. Hertil kan vi som ovenfor bestemme yderligere h elementer i G : $ca_1, ca_2, \dots, ca_h$, og vi kender nu $3h$ elementer i G . Enten er G hermed udtømt og $g = 3h$, eller vi kan fortsætte på tilsvarende måde et endeligt antal gange (da G er endelig), og vi finder at g er et multiplum af h .

Korollar (2.6)

Ordenen af ethvert element i en endelig gruppe er divisor i gruppens orden.

Eksempel (2.7)

Lad $(G, +)$ være mængden af hele tal organiseret med sædvanlig addition som kompositionsregel. $(G, +)$ er da en kommutativ gruppe med 0 som neutralt element. Det inverse element til a er a 's modsatte, altså $-a$. Gruppen $(G, +)$ er cyklisk, idet ethvert helt tal er en "potens", her multiplum, af 1. Som eksempel på en undergruppe i $(G, +)$ kan nævnes $(H, +)$ bestående af alle *lige* tal. Også $(H, +)$ er cyklisk, idet den frembringes af 2. Af andre eksempler på additive, kommutative uendelige grupper kan nævnes:

de rationale tal

de reelle tal

de komplekse tal

ingen af disse 3 grupper er cykliske.

Eksempel (2.8)

Mængden af reelle tal $\neq 0$ organiseret med sædvanlig multiplikation som kompositionsregel er en kommutativ gruppe med 1 som neutralt element. De rationale tal $\neq 0$ er en undergruppe heri. Mængden bestående af 1 og -1 udgør en (multiplikativ) undergruppe af ordenen 2.

Eksempel (2.9)

Som eksempel på en endelig gruppe af n te orden kan vi nævne samlingen af de n enhedsrødder: $\exp(ip\frac{2\pi}{n})$, $p = 0, 1, 2, \dots, n-1$, organiseret med multiplikation af komplekse tal som kompositionsregel. Gruppen er abelsk, og for ethvert lige n indeholder den en undergruppe af orden 2 bestående af tallene 1 og -1 .

Eksempel (2.10)

Som en anvendelse af sætning (2.5) og dens korollar (2.6) kan vi nævne, at hvis ordenen for en gruppe G er et primtal p , så har G kun de to trivielle undergrupper $\{e\}$ og G selv. Heraf følger også, at G er cyklisk, idet for et vilkårligt gruppeelement $a \neq e$ gælder, at ordenen af a er lig p , og de p potenser af a : $a^0 = e, a, a^1, a^2, \dots, a^{p-1}$ fremstiller netop elementerne i G .

3. Den symmetriske gruppe S_n

Vi skal i denne paragraf indføre et vigtigt eksempel på en endelig gruppe; i en senere paragraf skal vi vende tilbage til emnet, når vores begrebsområde er blevet noget udvidet.

Lad M være en vilkårlig mængde og f en enentydig afbildning af M på M , dvs. til ethvert $x \in M$ findes der netop et billedelement $x' = f(x) \in M$, og omvendt til ethvert $x' \in M$ findes netop et $x \in M$ med $x' = f(x)$. En sådan enentydig afbildning kaldes også en *transformation* af M eller, når mængden M specielt er endelig en *permutation* af M .

Sammensætter man to sådanne transformationer får man igen en transformation af M . Den associative regel gælder i almindelighed for sammensætninger af transformationer. Desuden er den identiske afbildning e af M et eksempel på en transformation og sammensættes e med en vilkårlig transformation, ser man, at e optræder som neutralt element. Endelig svarer der til enhver transformation f en omvendt afbildning f^{-1} , som også er en transformation. Sammensætter man f og f^{-1} får man e . Hermed har vi indset, at mængden af transformationer af M med sammensætning som kompositionsregel udgør en gruppe. Specielt har vi:

Sætning (3.1)

Mængden S_n af permutationer af en endelig mængde (med n elementer) udgør en gruppe, når sammensætning af permutationer tages som kompositionsregel. Gruppen kaldes den symmetriske gruppe af n 'te grad.

Idet vi nu betegner elementerne i en endelig mængde M ved $a_1, a_2, \dots, a_n$ kan vi angive en permutation f af M fuldstændigt ved for ethvert a_i at angive dets billedelement $f(a_i)$; dette $f(a_i)$ er imidlertid atter et af elementerne i M , fx a_{j_i} , og afbildningen $f: a_i \mapsto a_{j_i}$ er derfor fastlagt ved indexafbildningen $i \mapsto j_i$. Man plejer derfor at betegne f ved

$$f: \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

hvor et index og dets billedindex står under hinanden i samme søjle. Anden række $j_1, j_2, \dots, j_n$ er en permutation af tallene $1, 2, \dots, n$ i den sædvanlige betydning af glosen, som brugt ved fx indførelsen af determinanter. Det er nu klart, at *samme* transformation f kan beskrives ved i alt $n!$ symboler af ovenstående type.

$$f: \begin{pmatrix} r_1 & r_2 & \cdots & r_n \\ s_1 & s_2 & \cdots & s_n \end{pmatrix}$$

fremkommet ved en permutation af søjleordenen. Det er ligeledes klart, at hvis vi holder ordenen i symbolets første række fast på $1, 2, \dots, n$, så svarer *forskellige* transformationer af M til forskellige permutationer $j_1, j_2, \dots, j_n$ i symbolets anden række; derfor er der i alt $n!$ elementer i S_n .

Eksempel (3.2)

S_1 indeholder kun den identiske permutation $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

S_2 indeholde det neutrale element $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ og $a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

S_3 indeholder følgende 6 elementer:

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & a &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & b &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ c &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & d &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & f &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

Ved sammensætning af to transformationer bestemmer vi deres "produkt", fx er

$$ad = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f$$

mens

$$da = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = c.$$

Gruppen S_3 er altså *ikke* abelsk. På lignende måde kan vi bestemme samtlige produkter af 2 elementer i S_3 . Resultaterne kan bekvemt opstilles i en *gruppetafle* (Cayley-tavle), hvor vi fx lader elementet i indgangssøjlen betyde venstre faktor i produktet:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

Af tavlen aflæser vi straks, at elementerne e , a , og b udgør en undergruppe (angivet med de fede typer i tavlen). Desuden ser vi, at elementerne c , d , og f har ordenen 2, mens $a^2 = b$ og $a^3 = ba = e$ viser, at a har ordenen 3; tilsvarende gælder, at b har ordenen 3.

Ved en *cyklus* skal vi forstå en permutation $(ijk \cdots p)$ som fører tallet $i \mapsto j$, og $j \mapsto k$, osv. og tallet $p \mapsto i$, mens de ikke nævnte tal afbildes i sig selv ved denne permutation. En cyklus siges at have *længden* r og at være en r -*cyklus*, hvis den har r elementer; den kan i ovennævnte notation skrives på r forskellige måder, svarende til at hvert element kan stå forrest. Forøvrigt er det let at indse, at en r -cyklus opfattet som gruppeelement har ordenen r .

Nu kan *enhver permutation skrives som et produkt af cykler uden fælles elementer*; man bestemmer dette produkt svarende til en permutation ved en fremgangsmåde, der lettest beskrives ved et eksempel:

Eksempel

Lad en permutation være givet ved $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix}$.

Af denne ser vi at $1 \mapsto 4 \mapsto 8 \mapsto 7 \mapsto 1$, hvilket kan skrives som cyklen $(1\ 4\ 8\ 7)$, desuden viser a , at $2 \mapsto 5 \mapsto 3 \mapsto 2$, altså cyklen $(2\ 5\ 3)$ og

endelig $6 \mapsto 6$, i alt har vi fundet $a = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$. Da disse cykler er uden fælles elementer, er rækkefølgen af cyklerne i produktet ligegyldig, men bortset herfra er opløsningen éntydig.

En cyklus af længden 2 kaldes en *transposition*; en cyklus af længden 3 kaldes en *tricyklus*. Om disse specielle cykler gælder en række sætninger, hvoraf vi blot nævner nogle få.

Sætning (3.3)

Enhver permutation kan (endda på uendelig mange måder) skrives som et produkt af transpositioner.

Bevis: Da en permutation kan opløses i cykler, er det tilstrækkeligt at betragte en cyklus. For en cyklus $(i_1 i_2 \cdots i_r)$ kan man efterprøve, at

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_1 i_3)(i_1 i_4) \cdots (i_1 i_r)$$

idet $i_1 \mapsto i_2$; $i_2 \mapsto i_1$ og $i_3 \mapsto i_1$ og $i_4 \mapsto i_1$, etc. Disse transpositioner kommuterer ikke, da de har fælles elementer. Man kan endvidere, hvor som helst i produktet på højre side, indskyde par af transpositioner $(ij)(ij)$, som svarer til at indskyde den identiske permutation det pågældende sted.

Korollar (3.4)

Ethvert element i den symmetriske gruppe S_n kan skrives som et produkt af transpositioner af den specielle form (12) , (13) , (14) , $\dots$, $(1n)$.

Bevis: En vilkårlig transposition (ij) kan omskrives til $(ij) = (1j)(1i)(1j)$.

Ved indførelsen af determinanter blev som nævnt side 5 glosen permutation brugt som synonym til en opstilling af tallene $1, 2, \dots, n$ i en eller anden rækkefølge. Disse opstillinger blev klassificerede som *lige* eller *ulige* eftersom *inversionsantallet* var lige eller ulige. Yderligere blev det fremhævet, at man altid kan komme fra én opstilling til en anden opstilling ved at udføre fx q ombytninger af to elementer; de to opstillinger vil så være i samme eller modsatte klasse eftersom q er lige eller ulige. I denne forbindelse skal vi bemærke følgende: Lad $a \in S_n$ være givet ved

$$a = \begin{pmatrix} 1 & 2 & \cdots & r & \cdots & s & \cdots & n \\ i_1 & i_2 & \cdots & i_r & \cdots & i_s & \cdots & i_n \end{pmatrix}$$

så er

$$a(i_r i_s) = \begin{pmatrix} 1 & 2 & \cdots & r & \cdots & s & \cdots & n \\ i_1 & i_2 & \cdots & i_s & \cdots & i_r & \cdots & i_n \end{pmatrix};$$

Sammensætningen af a med transpositionen $(i_r i_s)$ resulterer altså i en ombytning af elementerne i_r og i_s i symbolets anden række. Vi kan derfor – ifølge ovenstående bemærkninger – ved sammensætning af a med q transpositioner opnå, at

$$a(i_1 1)(i_2 2) \cdots (i_k i_l) = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = e$$

og altså

$$a = (i_k i_l) \cdots (i_2 2)(i_1 1).$$

Hermed er a opløst i q transpositioner, hvor q er (u)lige, når inversionstallet $I(i_1, i_2, \dots, i_n)$ er (u)lige. Enhver anden opløsning af a i p transpositioner svarer på samme måde til, at man ved p ombytninger af to af tallene $1, 2, \dots, n$ kan få disse opstillet som anden række $i_1, i_2, \dots, i_n$ i symbolet for a , og p og q må have samme paritet, dvs. p er lige netop når q er lige. Vi kan derfor fastsætte følgende

Definition: En permutation

$$a = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in S_n \quad (n > 2)$$

kaldes lige, hvis den kan skrives som et produkt af et *lige* antal transpositioner, og *ulige* ellers.

Korollar (3.5)

En permutation

$$a = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in S_n \quad (n > 2)$$

er lige eller ulige eftersom inversionstallet $I(i_1, i_2, \dots, i_n)$ er lige henholdsvis ulige.

Sætning (3.6)

Mængden A_n af lige permutationer af $n > 1$ elementer er en undergruppe i S_n .

Bevis: Idet vi benytter kriteriet i (2.4) ser vi, at

- 1) $a, b \in A_n$ medfører, ab kan skrives som et produkt af et lige antal transpositioner, og derfor $ab \in A_n$.
- 2) $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = e \in A_n$, idet $I(1, 2, \dots, n) = 0$.
- 3) $a \in A_n$ medfører, at a^{-1} kan skrives som produktet af de samme transpositioner som i a , men i modsat orden; altså $a^{-1} \in A_n$.

Gruppen A_n kaldes den *alternierende* gruppe; dens orden er $\frac{1}{2}n!$.

4. Ækvivalensrelation. Klasser af konjugerede elementer

Lad A og B være to mængder. Ved *mængdeproduktet* $A \otimes B$ forstås samlingen af ordnede par (a, b) hvor $a \in A, b \in B$. En delmængde R af $A \otimes B$ kaldes en *relation* fra A til B , og man skriver $a \varrho b$, hvis $(a, b) \in R$. Specielt taler man om en *relation i* A , hvis $A = B$.

Definition (4.1): En *ækvivalensrelation* i mængden A er en relation R , som opfylder 3 krav

- 1) *refleksivitet:* $(a, a) \in R$,
- 2) *symmetri:* $(a, b) \in R$ medfører $(b, a) \in R$,
- 3) *transitivitet:* $(a, b) \in R$ og $(b, c) \in R$ medfører $(a, c) \in R$.

Lad nu A være en (ikke-tom) mængde, for hvilke der er givet en samling (ikke-tomme) delmængder, hvis foreningsmængde er A , og som to og to er *disjunkte*, dvs. uden fælles elementer. En sådan samling af delmængder kaldes *klassedeling* af A , delmængderne kaldes *klasser*, og en klassedeling giver anledning til en ækvivalensrelation ϱ i A ; for to vilkårlige $a, b \in A$ lad $a \varrho b$ betyde at a og b er i samme klasse. Det er nemt ud fra (4.1) at eftervise, at ϱ er en ækvivalensrelation. (I stedet for ϱ betegnes en ækvivalensrelation ofte med $\sim$). Omvendt gælder også

Sætning (4.2)

Til en ækvivalensrelation $\sim$ i A svarer der en klassedeling af A , således at for $a, b \in A$ gælder $a \sim b$ netop når a og b er i samme klasse.

Bevis: Til ethvert element $a \in A$ betragter vi mængden A_a bestående af de elementer $x \in A$ for hvilke $a \sim x$. Elementet $a \in A_a$ iflg. 1) i (4.1), og mængderne A_a overdækker A . Lad dernæst A_a og A_b være to af disse mængder, og antag, at $c \in A$ er et fælles element i A_a og A_b . Så er $a \sim c$ og $b \sim c$, og dermed $a \sim b$ iflg. 2) og 3) i (4.1). Vi kan gå videre og på lignende måde vise, at for ethvert $x \in A_b$ gælder $a \sim x$, hvilket medfører, at A_b er indeholdt i A_a . Tilsvarende finder vi at A_a er indeholdt i A_b , og dermed at $A_a = A_b$. – Altså enten stemmer A_a og A_b overens eller også er de disjunkte. Til slut: det er klart, at for denne klassedeling er $a \sim b$ ensbetydende med at “ a og b er i samme klasse”.

Derefter skal vi gå over til grupper. Lad G være en gruppe, og $a, b \in G$. Elementet b kaldes *konjugeret til elementet a* , hvis der findes et element $t \in G$, således at $b = t^{-1}at$.

Sætning (4.3)

Konjugation er en ækvivalensrelation.

Bevis: Lad $b \sim a$ betegne, at b er konjugeret til a (idet vi foregriber resultatet). Så er

- 1) $a \sim a$, idet $a = e^{-1}ae$.
- 2) $b \sim a$ medfører $a \sim b$, idet $b \sim a$ betyder $b = t^{-1}at$ for et $t \in G$; men så er $a = (t^{-1})^{-1}bt^{-1}$, dvs. $a \sim b$, da $t^{-1} \in G$.
- 3) $b \sim a$ og $c \sim b$ betyder, at der findes $t, s \in G$, så at $b = t^{-1}at$ og $c = s^{-1}bs$, og derfor $c = (ts)^{-1}a(ts)$, hvor $ts \in G$, dvs. $c \sim a$.

Ifølge (4.2) foreligger der hermed en *klassedeling af G i klasser af konjugerede elementer*.

Vi vil betegne klassen bestemt ved at bestå af elementer konjugeret til a med K_a . Hvis G er kommutativ, udgør hvert element for sig en klasse. Hvis G ikke er abelsk, er klasserne ulige store, men det neutrale element e udgør altid en klasse for sig, idet $e = t^{-1}et$ for alle $t \in G$.

Sætning (4.4)

Elementerne i samme klasse har samme orden.

Bevis: Lad $a \in K_a$ have orden r . Betragter vi et vilkårligt element $b =$

$t^{-1}at \in K_a$, så er $(t^{-1}at)^m = t^{-1}at t^{-1}at \cdots t^{-1}at = t^{-1}a^m t$. Heraf ser vi, at $(t^{-1}at)^m$ bliver e , netop når $a^m = e$, dvs. $m = r$, og ordenen af b er lig r .

For endelige grupper vil et nærmere studium af konjugation i første omgang dreje sig om at bestemme 1) antallet af konjugationsklasser, 2) for en given klasse K_a antallet af elementer i K_a . – Men forinden skal vi se på et par eksempler fra S_n .

Eksempel (4.5)

Idet vi henviser til S_3 som behandlet i eksempel (3.2), vil vi bestemme klassen K_a .

$$\begin{array}{lll} e^{-1}ae = a & a^{-1}aa = a & b^{-1}ab = a \\ c^{-1}ac = b & d^{-1}ad = b & f^{-1}af = b \end{array}$$

Altså K_a består af elementerne a og b . Tilsvarende finder vi, at K_c består af c , d og f . Gruppen S_3 falder derfor i 3 klasser

$$\begin{aligned} K_e &= \{e\} \\ K_a &= \{a, b\} = \{(123), (132)\} \\ K_c &= \{c, d, f\} = \{(1)(23), (2)(13), (3)(12)\}. \end{aligned}$$

Eksempel (4.6)

I §3 nævnte vi, at enhver permutation $a \in S_n$ kan skrives som et produkt af cykler c_i uden fælles elementer: $a = c_1 c_2 \cdots c_r$. Lad $t \in S_n$; så er $t^{-1}at = (t^{-1}c_1 t)(t^{-1}c_2 t) \cdots (t^{-1}c_r t)$, og vi kan derfor beskrive $t^{-1}at$, når vi har udregnet en typisk faktor $t^{-1}ct$, hvor c er en cyklus. Vi sætter

$$\begin{aligned} c &= (i_1 i_2 \cdots i_m) = \begin{pmatrix} i_1 & i_2 & \cdots & i_m & i_{m+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{m+1} & \cdots & i_n \end{pmatrix}, \\ t^{-1} &= \begin{pmatrix} j_1 & j_2 & \cdots & j_m & j_{m+1} & \cdots & j_n \\ i_1 & i_2 & \cdots & i_m & i_{m+1} & \cdots & i_n \end{pmatrix} \text{ og} \\ t &= \begin{pmatrix} i_2 & i_3 & \cdots & i_m & i_1 & i_{m+1} & \cdots & i_n \\ j_2 & j_3 & \cdots & j_m & j_1 & j_{m+1} & \cdots & j_n \end{pmatrix} \end{aligned}$$

Så er

$$t^{-1}ct = \begin{pmatrix} j_1 & j_2 & \cdots & j_m & j_{m+1} & \cdots & j_n \\ j_2 & j_3 & \cdots & j_1 & j_{m+1} & \cdots & j_n \end{pmatrix} = (j_1 j_2 \cdots j_m)$$

eller sagt i ord: $t^{-1}ct$ er en cyklus lige som c , og den fås af c ved, at man anvender permutationen t på elementerne i parentesens, der fremstiller c . For eksempel $a = (6)(253)(1487)$ og $t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 1 & 3 & 8 & 6 & 7 \end{pmatrix}$, så er $t^{-1}at = (8)(435)(2176)$.

Eksempel (4.7)

Lad en permutation $a \in S_n$ være skrevet som et produkt af cykler: $a = c_1 c_2 \cdots c_r$ og antag, at af disse er p_1 1-cykler, p_2 2-cykler, p_3 3-cykler, $\dots$, p_n

n -cykler. Så siges a at være af typen $1^{p_1}2^{p_2}\dots n^{p_n}$. Da $a \in S_n$, og cyklerne tilsammen indeholder n elementer, er

$$(4.8) \quad p_1 + 2p_2 + \dots + np_n = n$$

Resultatet i Eks.(4.6) kan nu formuleres således:

Ved konjugation af en permutation bevarer dens type. Ved anvendelse af reglen i Eks.(4.6) ser man endvidere, at to permutationer af samme type er konjugerede, og i alt har man derfor:

Sætning

To permutationer i S_n er konjugerede, hvis og kun hvis de er af samme type; antallet af konjugationsklasser i S_n er derfor antallet af typer.

Antallet af typer er naturligvis lig antallet af (heltallige, ikke-negative) løsninger $(p_1, p_2, \dots, p_n)$ til ligningen (4.8). Hvis fx $n = 4$, så har (4.8) følgende løsninger

$$(p_1, p_2, p_3, p_4) = \begin{cases} (4, 0, 0, 0) \\ (2, 1, 0, 0) \\ (1, 0, 1, 0) \\ (0, 2, 0, 0) \\ (0, 0, 0, 1) \end{cases}$$

svarende til, at S_4 falder i 5 klasser.

Antallet h , af elementer i en given klasse af permutationer, altså af en given type $1^{p_1}2^{p_2}\dots n^{p_n}$, kan beregnes ved *Cauchy's formel*:

$$h = \frac{n!}{p_1!p_2!\dots p_n!2^{p_2}3^{p_3}\dots n^{p_n}},$$

thi, vi skal udfylde p_1 1-parenteser, p_2 2-parenteser, $\dots$, p_n n -parenteser med tallene $1, 2, \dots, n$ og optælle forskellige permutationer. Men af de ialt $n!$ permutationer af tallene $1, 2, \dots, n$ er mange ens med hensyn til type: for det første er rækkefølgen af de p_k cykler af længde k ($k = 1, 2, \dots, n$) ligegyldig, hvorfor vi får samme permutation (med hensyn til type) $p_1!p_2!\dots p_n!$ gange af de $n!$ opstillinger; for det andet kan en cyklus af længde k skrives på i alt k forskellige måder (jvf. side 7), og hver af de p_k k -cykler er talt med k^{p_k} gange ($k = 1, 2, \dots, n$), hvorfor vi får samme permutation (med hensyn til type) talt med $1^{p_1}2^{p_2}3^{p_3}\dots n^{p_n}$.

Ser vi igen specielt på eksemplet S_4 , så fandt vi ovenfor typerne

$$1^4, 1^2 2^1, 1^1 3^1, 2^2, 4^1$$

Antallet af elementer i hver af de 5 tilsvarende konjugationsklasser finder vi ved Cauchy's formel til henholdsvis

$$1 \text{ (nemlig } e), 6, 8, 3, 6.$$

5. Sideklasser

Lad G være en gruppe, og A og B to delmængder af G . Så skal AB betyde mængden af gruppeelementer af formen ab , hvor $a \in A$, $b \in B$, eller

$$AB = \{ab \mid a \in A, b \in B\}.$$

Specielt, for fastholdt $g \in G$ skal

$$gA = \{ga \mid a \in A\}.$$

Lad dernæst H være undergruppe i G , og betragt mængderne gH for vilkårligt valg af $g \in G$. Disse delmængder gH udgør, som vi nu skal vise, en klassedeling af G , og de kaldes (venstre) *sideklasser*.

Det er klart, at ethvert $g_0 \in G$ tilhører en sådan delmængde, fx $g_0 \in g_0H$; delmængderne gH overdækker altså gruppen G .

Hvis to delmængder g_1H og g_2H har et element g fælles, så findes der $h_1, h_2 \in H$, således at

$$g = g_1h_1 = g_2h_2.$$

Men så kan vi indse, at et vilkårligt element $g_1h \in g_1H$ også er indeholdt i g_2H ; thi

$$g_1h = (g_2h_2h_1^{-1})h = g_2h',$$

hvor $h' \in H$. På lignende måde indser vi, at et vilkårligt element $g_2h \in g_2H$ er indeholdt i g_1H , og i alt slutter vi, at de to mængder g_1H og g_2H indeholder de samme elementer. Hermed har vi vist, at to forskellige af mængderne gH er disjunkte.

Helt tilsvarende bemærkninger kan gøres om (højre) sideklasser Hg .

Da det neutrale element $e \in G$ tilhører $eH = H$, følger det af klassedelingen, at H er eneste undergruppe blandt dens sideklasser.

I sætning (2.5) viste vi for endelige grupper G , at G 's orden r er et multiplum af H 's orden s :

$$r = ns.$$

Her er n netop antallet af sideklasser og kaldes *index* for undergruppen H i G .

Eksempel (5.1)

Som eksempel på en undergruppe og dens sideklasser vil vi betragte begrebet *normalisator*. Vi vælger et vilkårligt element $a \in G$ og fastholder dette i de følgende overvejelser. Til a knytter vi mængden

$$N_a = \{g \in G \mid ga = ag\}.$$

Idet vi benytter (2.4) viser vi, at N_a er en undergruppe, thi

1) $g_1, g_2 \in N_a$ medfører $(g_1g_2)a = g_1(g_2a) = (g_1a)g_2 = a(g_1g_2)$, altså $g_1g_2 \in N_a$.

2) det er klart, at $e \in N_a$.

3) $g \in N_a$ medfører $g^{-1}(ga) = g^{-1}(ag)$, og $g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$, eller $ag^{-1} = g^{-1}a$, altså netop $g^{-1} \in N_a$.

Denne gruppe N_a , som kaldes a 's *normalisator*, giver anledning til en klassedeling af G i (højre) sideklasser. Lad os sige, at G er endelig, og at *index* $N_a = j$. Dette antal er, som vi nu skal vise, netop antallet af elementer i konjugationsklassen K_a .

For at vise dette lader vi sideklasserne til N_a være henholdsvis $N_at_1, N_at_2, \dots, N_at_j$. Så vil det om to forskellige elementer, g_1t_1 og g_2t_1 fra samme sideklasse N_at_1 gælde:

$$(g_1t_1)^{-1}a(g_1t_1) = t_1^{-1}g_1^{-1}ag_1t_1 = t_1^{-1}at_1$$

og

$$(g_2t_1)^{-1}a(g_2t_1) = t_1^{-1}g_2^{-1}ag_2t_1 = t_1^{-1}at_1.$$

Dette viser, at a konjugeres til samme element i K_a af de to elementer g_1t_1 og g_2t_1 , eller tydeligere: *a konjugeres til samme element i K_a af ethvert element i N_at_1 .*

Derimod vil to elementer g_1t_1 og g_2t_2 fra forskellige sideklasser N_at_1 og N_at_2 konjugere a forskelligt; thi hvis

$$(g_1t_1)^{-1}a(g_1t_1) = t_1^{-1}at_1$$

og

$$(g_2t_2)^{-1}a(g_2t_2) = t_2^{-1}at_2$$

var ens, så var

$$(t_2t_1^{-1})a = a(t_2t_1^{-1}),$$

men den sidste relation udtrykker, at $t_2t_1^{-1} \in N_a$, og dette strider imod, at N_at_1 og N_at_2 var forskellige.

Hermed har vi indset, at man kan etablere en enentydig afbildning af elementerne i K_a på mængden af sideklasser N_at ; dette var netop, hvad der skulle vises.

6. Invariante undergrupper

Definition (6.1): En undergruppe H i en gruppe G kaldes *invariant* (eller *normal*), hvis det om dens sideklasser gælder, at $xH = Hx$ for alle $x \in G$.

Man kan ud fra denne definition formulere følgende kriterium:

Sætning (6.2)

En undergruppe er *normal*, når og kun når $a \in H$ medfører $t^{-1}at \in H$ for alle $t \in G$.

Bevis: Antag H er en invariant undergruppe og $a \in H$. Så er

$$t^{-1}(at) = t^{-1}(tb) = b$$

hvor $b \in H$; dette beviser den ene halvdel af sætningen. Ved beviset af den anden halvdel antager vi om en undergruppe H , at $a \in H$ medfører $t^{-1}at \in H$ for alle $t \in G$. Så er for alle $x \in G$

$$ax = x(x^{-1}ax) = xb$$

hvor $b \in H$, og derfor er Hx indeholdt i xH . På tilsvarende måde finder man, at xH er indeholdt i Hx , og derfor i alt $xH = Hx$, dvs. H er invariant.

Sætningen udtrykker, at en normal undergruppe med et element af en konjugationsklasse indeholder *hele* konjugationsklassen, og omvendt: hvis foreningsmængden af visse hele klasser udgør en undergruppe, så er denne invariant.

Det er klart, at i en abelsk gruppe G er enhver undergruppe invariant. Lidt mindre trivial er følgende

Sætning (6.3)

En undergruppe af index 2 er normal.

Bevis: Lad undergruppe H i G have index 2. Så er

- 1) $hH = Hh = H$ for ethvert $h \in H$.
- 2) $tH = Ht$ for ethvert $t \in G$ men $t \notin H$; thi G består af kun 2 højre sideklasser H og Ht ; altså består mængderne tH og Ht af de samme elementer.

Korollar (6.4)

Den alternerende gruppe A_n er en invariant undergruppe i den symmetriske gruppe S_n .

Eksempel (6.5)

I fortsættelse af eks.(4.5) vedrørende S_3 nævner vi, at elementerne e , a , og $a^2 = b$ udgør en (cyklisk) undergruppe (af 3. orden) i S_3 ; denne undergruppe er invariant – det er A_3 – den består af to “hele konjugationsklasser K_e og K_a ”. Elementerne e og c udgør en undergruppe af 2. orden; denne sidste undergruppe er ikke invariant, da fx c 's konjugerede elementer ikke er med.

Idet vi minder om definitionen i §5 af produktet AB af to delmængder A og B i en gruppe G , skal vi i det følgende behandle produkter af sideklasser; vi vil kun betragte tilfældet, hvor der er tale om sideklasser til en invariant undergruppe, og vi kan i det tilfælde nøjes med at se på fx højre sideklasser.

Sætning (6.6)

Om to vilkårlige sideklasser Ha og Hb til en invariant undergruppe H i gruppen G gælder $HaHb = Hab$.

Bevis: Vi bemærker først, at da H er invariant, består aH og Ha af de samme elementer i G . Idet

$$HaHb = \{xy \mid x \in Ha, y \in Hb\},$$

vil vi udregne xy , hvor $x = h_1a$, $y = h_2b$ og $h_1, h_2 \in H$:

$$xy = h_1ah_2b = h_1h'_2ab = hab, \quad \text{hvor } h'_2, h \in H;$$

thi $ah_2 \in aH = Ha$. Dette viste, at mængden $HaHb$ er indeholdt i Hab . For et vilkårligt element $z \in Hab$ gælder

$$z = hab = hah^{-1}hb = (hh'a)(hb) \in HaHb.$$

Dette viste, at mængden Hab er indeholdt i $HaHb$.

Sætning (6.7)

Samlingen af sideklasser til en normal undergruppe H i G udgør en gruppe, når den organiseres med multiplikation af delmængder i G som kompositionsregel.

Bevis: Lad os kalde samlingen af sideklasser til H for T . Så viser sætning (6.6), at T er stabil med hensyn til multiplikation af sideklasser. Det er uden videre klart fra definitionen, at multiplikation af delmængder i G er associativ, og man efterviser let, at sideklassen H er neutralt element i T ; endelig gælder

$$HaHa^{-1} = Haa^{-1} = H \quad \text{og} \quad Ha^{-1}Ha = Ha^{-1}a = H,$$

hvilket viser, at sideklassen Ha^{-1} er inverst element til Ha .

Definition (6.8): Gruppen T , hvis elementer er sideklasser til en normal undergruppe H i G kaldes *kvotientgruppen af G med hensyn til H* eller *faktorgruppen af H i G* . Den betegnes $G|H$; dens orden er $\text{index } H$.

Eksempel (6.9)

Lad G være den cykliske gruppe af orden 12 frembragt af elementet a , altså

$$G = \{a, a^2, \dots, a^{12} = e\}.$$

Lad endvidere H være undergruppen af 3. orden frembragt af a^4 :

$$H = \{a^4, a^8, a^{12} = e\}.$$

Da G er abelsk, er H invariant; dens index er 4, og dens sideklasser er

$$\begin{aligned} H &= \{a^4, a^8, e\} & Ha^2 &= \{a^6, a^{10}, a^2\} \\ Ha &= \{a^5, a^9, a\} & Ha^3 &= \{a^7, a^{11}, a^3\}. \end{aligned}$$

Gruppen $G|H$ er givet ved følgende Cayley-tavle:

	H	Ha	Ha^2	Ha^3
H	H	Ha	Ha^2	Ha^3
Ha	Ha	Ha^2	Ha^3	H
Ha^2	Ha^2	Ha^3	H	Ha
Ha^3	Ha^3	H	Ha	Ha^2

Eksempel (6.10)

Lad G være den *additive* gruppe af hele tal, og H undergruppen bestående af tal delelig med 3; da G er abelsk, er H invariant. Da kompositionsreglen er addition, plejer man at notere G/H med $G - H$. Sideklasserne bliver H , $H + 1$, $H + 2$:

$$\begin{aligned} H &= \{0, \pm 3, \pm 6, \dots\}, \\ H + 1 &= \{1, 4, -2, 7, -5, \dots\} \\ H + 2 &= \{2, 5, -1, 8, -4, \dots\}. \end{aligned}$$

Med andre ord: ethvert element i sideklassen $H + 1$ giver den principale rest 1 ved division med 3, mens ethvert element i $H + 2$ giver principal rest 2 ved division med 3. Cayley-tavlen ser således ud:

	H	$H + 1$	$H + 2$
H	H	$H + 1$	$H + 2$
$H + 1$	$H + 1$	$H + 2$	H
$H + 2$	$H + 2$	H	$H + 1$

7. Homomorfi og isomorfi

Lad $(G, \cdot)$ og $(G', \circ)$ være to grupper og f en afbildning af G ind i G' . Afbildningen f kaldes en *homomorfi*, hvis der for alle $a, b \in G$ gælder, at

$$f(a \cdot b) = f(a) \circ f(b).$$

Hvis vi betegner billedelementet $f(a)$ med a' , kan homomorfiegenskaben udtrykkes ved:

$$(a \cdot b)' = a' \circ b'.$$

Idet e er neutralt element i G , og

$$a' = (a \cdot e)' = a' \circ e',$$

ser vi, at $e' = f(e)$ er *neutralt element i G'* . Desuden er

$$e' = (a \cdot a^{-1})' = a' \circ (a^{-1})',$$

hvilket viser, at $(a')^{-1} = (a^{-1})'$ eller

$$[f(a)]^{-1} = f(a^{-1}).$$

Eksempel (7.1)

Lad $(G, \cdot)$ være den cykliske gruppe af orden 8 frembragt af elementet a , dvs.

$$G = \{a, a^2, \dots, a^8 = e\}.$$

Lad $(G', \div)$ være den additive restklassegruppe modulo 12, dvs.

$$G' = \{0, 1, \dots, 11\}$$

med addition modulo 12 betegnet ved $\dot{+}$. Vi definerer nu en afbildning f af G ind i G' ved

$$\begin{aligned} f(a) &= f(a^5) = 3 \\ f(a^2) &= f(a^6) = 6 \\ f(a^3) &= f(a^7) = 9 \\ f(a^4) &= f(a^8) = 0. \end{aligned}$$

Så er fx

$$f(a^2 \cdot a^3) = f(a^5) = 3 = 6 \dot{+} 9 = f(a^2) \dot{+} f(a^3).$$

Man kan nu vise alment, at for alle $x, y \in G$ er

$$f(x \cdot y) = f(x) \dot{+} f(y)$$

(prøv dette); en anden mulighed er at efterprøve direkte de 64 mulige produkter og derved indse, at f er en homomorfi af G i G' .

Eksempel (7.2)

Lad $G = GL_n$ være den multiplikative gruppe af regulære matricer af n te orden, G' den multiplikative gruppe af komplekse tal $\neq 0$. Med $\mathbf{M}, \mathbf{N}$ betegner vi matricer, elementer i GL_n , og $|\mathbf{M}|$ betegner $\mathbf{M}$'s determinant. Afbildningen $f(\mathbf{M}) = |\mathbf{M}|$ af G ind i G' er en homomorfi, idet

$$|\mathbf{MN}| = |\mathbf{M}| |\mathbf{N}|.$$

Idet vi benytter betegnelserne indført før de to eksempler kan vi nu vise:

Sætning (7.3)

Hvis f er en homomorfi af G ind i G' , så er mængden $f(G)$ af billedelementer en undergruppe i G' .

Bevis: Vi har allerede set, at det neutrale element $e' \in G'$ er indeholdt i $f(G)$, idet $e' = f(e)$. Homomorfigenskaberne viser direkte, at $f(G)$ er stabil. Ethvert element $a' \in f(G)$ har et inverst $(a^{-1})' \in f(G)$, og gyldigheden af den associative regel i $f(G)$ følger af dens gyldighed i G' .

Sætning (7.4)

Hvis f er en homomorfi af G ind i G' , er mængden:

$\ker f = \{x \in G \mid f(x) = e'\}$ en invariant undergruppe i G .

Bevis: Vi vil tillade os at undertrykke symbolet for kompositionsreglerne i G og G' . Idet $x, y \in \ker f$, gælder da $f(xy) = f(x)f(y) = e'e' = e'$, og derfor $xy \in \ker f$. Mængden $\ker f$ er derfor stabil. Den associative regel er trivielt opfyldt i $\ker f$ som delmængde i G . Det neutrale element $e \in \ker f$, da $f(e) = e'$, og om x^{-1} gælder, at $f(x^{-1}) = [f(x)]^{-1} = [e']^{-1} = e'$, og derfor $x^{-1} \in \ker f$. Hermed har vi vist, at $\ker f$ er en undergruppe. For at vise, at $\ker f$ er invariant, benytter vi (6.2): Lad t være et vilkårligt element i G , og $x \in \ker f$. Så er

$$f(t^{-1}xt) = f(t^{-1})e'f(t) = [f(t)]^{-1}f(t) = e' \quad \Rightarrow \quad t^{-1}xt \in \ker f.$$

Definition (7.5): En enentydig homomorfi f af en gruppe G på en gruppe G' kaldes en *isomorfi af G på G'* , og to grupper kaldes *isomorfe*, hvis der findes en isomorfi af den ene gruppe på den anden; vi skriver $G \equiv G'$.

Eksempel (7.1) viser, at en homomorfi behøver ikke at være en isomorfi; i eksemplet er f hverken enentydig eller på.

Når f er en isomorfi, er $f(G) = G'$, og $\ker f = \{e\}$. Omvendt gælder også, at $f(G) = G'$ og $\ker f = \{e\}$ medfører, at f er enentydig; thi $f(a) = f(b)$ medfører $f(ab^{-1}) = f(a)[f(b)]^{-1} = f(a)[f(a)]^{-1} = e'$, og derfor $ab^{-1} = e$, hvoraf følger $a = b$.

Definition (7.6): Hvis f er en homomorfi af gruppen G på gruppen G' , så kaldes G' en *repræsentation* af G . Hvis f er en isomorfi af gruppen G på gruppen G' , så kaldes G' en *tro repræsentation* af G .

Vi skal slutte denne paragraf med nogle eksempler på repræsentationssætninger.

Sætning (7.7) (Cayley)

Enhver endelig gruppe G af orden n er isomorf med en undergruppe i S_n .

Bevis: Lad elementerne i G være $g_1, g_2, \dots, g_n$. Så er elementerne $g_1g_i, g_2g_i, \dots, g_ng_i$ indbyrdes forskellige elementer i G og derfor blot G 's elementer i en eller anden rækkefølge: $g_{i_1}, g_{i_2}, \dots, g_{i_n}$. Vi kan derfor knytte en permutation til gruppemedlemmet g_i og derved fastlægge en afbildning f af G ind i S_n :

$$f(g_i) = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Afbildningen f er en homomorfi, idet

$$f(g_j) = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \cdots & i_u & \cdots & i_n \\ k_1 & k_2 & \cdots & k_u & \cdots & k_n \end{pmatrix}$$

giver for det første

$$f(g_i)f(g_j) = \begin{pmatrix} 1 & 2 & \cdots & u & \cdots & n \\ k_1 & k_2 & \cdots & k_u & \cdots & k_n \end{pmatrix}$$

og for det andet

$$g_u(g_i g_j) = (g_u g_i) g_j = g_{i_u} g_j = g_{k_u} \quad (u = 1, 2, \dots, n).$$

Altså er $f(g_i g_j) = f(g_i) f(g_j)$, og ifølge (7.3) er $f(G)$ en undergruppe i S_n . Denne afbildning er enentydig fordi forskellige gruppeelementer afbildes i forskellige permutationer; det gælder oven i købet, at $g_i \neq g_j$ medfører $i_u \neq j_u$ for $u = 1, 2, \dots, n$ i de tilhørende permutationer, thi $g_u g_i \neq g_u g_j$. Hermed er beviset færdigt.

Sætning (7.8)

Enhver cyklisk gruppe af orden n er isomorf med $(\mathbb{Z}_n, +)$, den additive restklassegruppe modulo n . Enhver uendelig cyklisk gruppe er isomorf med $(\mathbb{Z}, +)$, den additive gruppe af hele tal.

Bevis: 1) Lad G være en endelig, cyklisk gruppe af orden n , frembragt af elementet a . Definér en afbildning f af G i $\mathbb{Z}_n$ ved

$$f(a^m) = m \quad (\text{for } 0 \leq m < n).$$

Det skal fremhæves, at $a^0 = e$ og $f(a^0) = 0$. Afbildningen er enentydig, og

$$f(a^i a^j) = f(a^{i+j}) = f(a^r) = r,$$

hvor r er den principale rest af $i + j$ ved division med n . Men i $(\mathbb{Z}_n, +)$ er $i + j = r$, og derfor gælder

$$f(a^i a^j) = f(a^i) + f(a^j).$$

Afbildningen f er således en isomorfi.

2) Lad G være en uendelig cyklisk gruppe frembragt af elementet a :

$$G = \{a^k \mid k \text{ helt tal}\}.$$

Definér en afbildning f af $\mathbb{Z}$ på G ved $f(k) = a^k$.

Afbildningen f er enentydig, thi hvis $a^i = a^j$, men fx $i < j$, så var $a^{j-i} = e$. Sætter vi nu $j - i = m$, så gælder for ethvert helt tal k :

$$k = qm + r, \quad (0 \leq r < m) \quad \Rightarrow \quad a^k = a^{qm} a^r = a^r;$$

men heraf kunne vi slutte, at et vilkårligt element $a^k \in \{a^0, a^1, \dots, a^{m-1}\}$. Dette strider imod at G er uendelig. Afbildningen f er tillige en homomorfi, idet

$$f(s+t) = a^{s+t} = a^s a^t = f(s)f(t).$$

Altså er f en isomorfi.

Sætning (7.9)

Hvis H er en normal undergruppe i en gruppe G , så kan G afbildes homomorft på faktorgruppen G/H . Omvendt: hvis $G' = f(G)$ er det homomorfe billede af G ved homomorfien f , så er G' isomorf med faktorgruppen $G/\ker f$.

Bevis: 1) Vi definerer en afbildning f_1 af G på G/H :

$$f_1(x) = Hx \quad (\text{for } x \in G).$$

Da H er normal, er ifølge (6.6)

$$f_1(xy) = Hxy = (Hx)(Hy) = f_1(x)f_1(y).$$

f_1 er altså en homomorfi af G på G/H ; f_1 kaldes den *naturlige* homomorfi af G på G/H . Vi kan bemærke, at $\ker f_1 = H$.

2) I beviset for den omvendte sætning er det bekvemt at betegne $\ker f$ med E . Vi vil så indføre en afbildning F af G/E på $G' = f(G)$ ved

$$F(Eg) = f(g).$$

Denne afbildning er en homomorfi, idet

$$F(Eg_1Eg_2) = F(Eg_1g_2),$$

fordi E er invariant ifølge (7.4); men

$$F(Eg_1g_2) = f(g_1g_2) = f(g_1)f(g_2) = F(Eg_1)F(Eg_2),$$

fordi f er en homomorfi. Afbildningen F er desuden enentydig; antog man nemlig, at $F(Eg_1) = f(g_1) = F(Eg_2)$, så ville

$$F((Eg_1)(Eg_2)^{-1}) = F(Eg_1g_2^{-1}) = f(g_1g_2^{-1}) = f(g_1)[f(g_2)]^{-1} = e'$$

hvor e' er neutralt element i G' ; dette ville betyde, at $g_1g_2^{-1} \in E$, og derfor $Eg_1 = Eg_2$. I alt har vi nu vist, at F er en isomorfi.

8. Direkte produkt af grupper

Lad G_1 og G_2 være to grupper. Ved det *direkte produkt* $G_1 \otimes G_2$ af G_1 og G_2 skal vi forstå mængdeproduktet af G_1 og G_2 forsynet med følgende kompositionsregel

$$(8.1) \quad (g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2),$$

hvor $g_1, h_1 \in G_1$ og $g_2, h_2 \in G_2$.

Idet mængdeproduktet af G_1 og G_2 består af ordnede par (g_1, g_2) ser vi, at $G_1 \otimes G_2$ er stabil med hensyn til kompositionsreglen i (8.1). Desuden er elementet (e_1, e_2) neutralt i $G_1 \otimes G_2$, idet e_1 (e_2) betegner neutralt element i G_1 (G_2). Endelig er (g_1^{-1}, g_2^{-1}) inverst element til (g_1, g_2) , og den associative lov er trivielt opfyldt i $G_1 \otimes G_2$. Det *direkte produkt* er således *en gruppe*.

Mængden

$$H_1 = \{(g_1, e_2) \mid g_1 \in G_1\}$$

efterves let at være en invariant undergruppe i $G_1 \otimes G_2$, og afbildningen f af H_1 på G_1 givet ved

$$f(g_1, e_2) = g_1$$

er en isomorfi af H_1 på G_1 . Tilsvarende finder man, at

$$H_2 = \{(e_1, g_2) \mid g_2 \in G_2\}$$

er en invariant undergruppe i $G_1 \otimes G_2$, og H_2 er isomorf med G_2 .

De to undergrupper H_1 og H_2 kommuterer, dvs. $H_1H_2 = H_2H_1$. Lad nemlig $a = (g_1, e_2) \in H_1$ og $b = (e_1, g_2) \in H_2$; så er

$$ab = (g_1, e_2)(e_1, g_2) = (g_1, g_2) = ba$$

Denne relation viser tillige, at ethvert element i $G_1 \otimes G_2$ kan skrives som produkt af et element fra H_1 og et fra H_2 . Desuden har H_1 og H_2 kun det neutrale element (e_1, e_2) fælles. Disse betragtninger leder til følgende:

Sætning (8.2)

En gruppe G er isomorf med det direkte produkt af to af dens undergrupper A og B , når og kun når A og B er invariante undergrupper i G med fællesmængden lig $\{e\}$ og med $AB = G$.

Bevis: Vi har allerede set ovenfor, at $A \otimes B$ indeholder isomorfe eksemplarer af A og B med de nævnte egenskaber. Antag derfor omvendt, at A og B er invariante undergrupper i G med fællesmængde $\{e\}$ og $AB = G$. Betragt så et element

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

hvor $a \in A$, $b \in B$. Dette ses at tilhøre både A og B , fordi disse er normale undergrupper, jvf. (6.2); derfor er

$$a^{-1}b^{-1}ab = e \quad \text{og} \quad ab = ba \quad \text{og} \quad AB = BA (= G).$$

Fremstillingen $g = ab$, hvor $a \in A$, $b \in B$, af et vilkårligt element $g \in G$ er éntydig, idet $a_1b_1 = a_2b_2$ medfører $a_2^{-1}a_1 = b_2b_1^{-1} \in \{e\}$, eller

$$a_2^{-1}a_1 = b_2b_1^{-1} = e \quad \Rightarrow \quad a_1 = a_2, \quad b_1 = b_2.$$

Men så er afbildningen f af G på $A \otimes B$ givet ved $f(g) = (a, b)$ en isomorfi, fordi

$$g_1g_2 = (a_1b_1)(a_2b_2) = (a_1a_2)(b_1b_2)$$

og

$$f(g_1g_2) = (a_1a_2, b_1b_2) = f(g_1)f(g_2).$$

Hermed er sætningen bevist.

Man omtaler ofte gruppen G i (8.2) som selve det direkte produkt af A og B . I denne formulering giver resultatet (8.2) følgende korollar, der ofte tages som definition af det direkte produkt:

Korollar (8.3)

En gruppe G er et direkte produkt $A \otimes B$ af to undergrupper A og B , hvis

- 1) *ethvert $g \in G$ kan skrives $g = ab$, $a \in A$, $b \in B$;*
- 2) *faktorerne a og b er éntydigt bestemt af g ;*
- 3) *ethvert $a \in A$ kommuterer med ethvert $b \in B$.*

Tilsvarende siger man $G \equiv A_1 \otimes A_2 \otimes \cdots \otimes A_k$ er et direkte produkt af undergrupperne $A_1, A_2, \dots, A_k$, når

- 1) *ethvert $g \in G$ kan skrives $g = a_1a_2 \cdots a_k$, $a_i \in A_i$;*
 - 2) *faktorerne a_i er éntydigt bestemt af g ;*
 - 3) *ethvert $a_i \in A_i$ kommuterer med ethvert $a_j \in A_j$ for i og $j = 1, 2, \dots, k$ og $i \neq j$.*
-

Eksempel (8.4)

Lad $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

og lad kompositionsreglen være multiplikation modulo 15. Herved får man en abelsk gruppe (vis dette!). G indeholder en cyklisk undergruppe af 4. orden frembragt af element 2:

$$C_4 = \{1, 2, 2^2 = 4, 2^3 = 8\},$$

og en cyklisk undergruppe af 2. orden frembragt af elementet 11:

$$C_2 = \{1, 11\}$$

Vi ser straks, at C_2 og C_4 har kun det neutrale element 1 fælles. Desuden er C_2 og C_4 normale, da G er abelsk, og

$$C_2 C_4 = \{1, 2, 4, 8, 11, 22, 44, 88\}.$$

Men her er $22 \equiv 7$, $44 \equiv 14$ og $88 \equiv 13$, altså modulo 15, og $C_2 C_4$ er derfor netop G . Ifølge (8.2) og bemærkningerne derefter kan vi derfor sige

$$G = C_2 \otimes C_4.$$

Eksempel (8.5)

Vi vil vise, at på nær isomorfier findes der kun to grupper af orden 4. Ifølge (2.6) kan ordenen af et element i en gruppe af orden 4 kun være 2 eller 4.

1) Hvis gruppen G indeholder et element a med ordenen 4, så er G cyklisk og $G = \{e, a, a^2, a^3\}$.

2) Hvis de tre elementer $a, b, c \neq e$ i gruppen har ordenen 2, så frembringer hver af disse tre elementer undergrupper af orden 2, hver af index 2 og derfor normale, ifl. (6.3). To vilkårlige af disse har kun $\{e\}$ fælles, og fx

$$\{e, a\}\{e, b\} = \{e, a, b, ab\} = G$$

da ab må være gruppens element c . Både $\{e, a\}$ og $\{e, b\}$ er cykliske og isomorfe med C_2 og derfor er $G = C_2 \otimes C_2$. G kaldes *Kleins fire-gruppe*.

9. Repræsentation af en gruppe ved lineære transformationer

Som allerede nævnt i (7.6) forstår vi ved *repræsentation* af gruppen G en ny gruppe G' , som er et homomorft billede af G , repræsentationen kaldes *tro*, hvis G' er isomorf med G . Vi skal i det følgende udelukkende beskæftige os med de tilfælde, hvor G' er en (under)gruppe af matricer i GL_n , se (7.2), og vi fastlægger derfor følgende

Definition (9.1): En repræsentation af n te grad af en gruppe G er en med G homomorf undergruppe G' i GL_n .

Man fastlægger altså repræsentationen G' ved til ethvert element $g \in G$ at opgive matricen $\mathbf{f}(g) \in G'$ svarende til g under homomorfien $\mathbf{f}$ af G på G' ; gruppen $G' = \mathbf{f}(G)$ er indeholdt i GL_n . Som illustration til denne definition kan vi nævne følgende:

Da GL_1 selv er isomorf med den multiplikative gruppe af komplekse tal $\neq 0$, så kan en repræsentation af 1. grad af en gruppe G opgives ved en (under)gruppe G' i den multiplikative gruppe af komplekse tal $\neq 0$, fx er $f(g) = 1$ for alle $g \in G$ en (ikke-tro) repræsentation af 1. grad af G .

En tilsvarende enkel repræsentation, men af n te grad, fås ved at sætte $\mathbf{f}(g) = \mathbf{E}$ for alle $g \in G$, hvor $\mathbf{E}$ er enhedsmatricen i GL_n .

Definition (9.2): Ved karakteren χ_f af en repræsentation $\mathbf{f}(G)$ af gruppen G forstås funktionen $\chi_f(g)$ defineret på G ved

$$\chi_f(g) = \text{spor } \mathbf{f}(g)$$

Karakteren er således (komplekse) tal. Hvis repræsentationen er af 1. grad er $\chi(g)$ lig med det komplekse tal $f(g)$; for en repræsentation i almindelighed gælder, at repræsentationens grad n er lig med $\chi_f(e)$, hvor e er det neutrale element i G .

Sætning (9.3)

Konjugerede elementer i en gruppe G har samme karakter; dvs. karakteren afhænger af G 's konjugationsklasser.

Bevis: Lad $g' = t^{-1}gt$, hvor $t, g \in G$. Så er

$$\mathbf{f}(g') = \mathbf{f}(t^{-1}gt) = [\mathbf{f}(t)]^{-1}\mathbf{f}(g)\mathbf{f}(t) \quad \text{og} \quad \text{spor } \mathbf{f}(g') = \text{spor } \mathbf{f}(g)$$

fordi matricerne $[\mathbf{f}(t)]^{-1}\mathbf{f}(g)\mathbf{f}(t)$ og $\mathbf{f}(g)$ har samme reduktionsdeterminant. Men dermed er

$$\chi_f(g') = \chi_f(g).$$

Lad nu $\mathbf{f}(G)$ repræsentere gruppen G i GL_n , og lad $\mathbf{S}$ være matricen hørende til en lineær transformation K^n på sig selv, dvs.

$$\underline{x}' = \mathbf{S} \underline{x},$$

hvor $\mathbf{S} \in GL_n$ og $\underline{x}, \underline{x}' \in K^n$. Så er afbildningen $\mathbf{f}'$ af G ind i GL_n givet ved

$$\mathbf{f}'(g) = \mathbf{S}^{-1}\mathbf{f}(g)\mathbf{S}$$

en homomorfi. Thi

$$\begin{aligned} \mathbf{f}'(g_1g_2) &= \mathbf{S}^{-1}\mathbf{f}(g_1g_2)\mathbf{S} = \mathbf{S}^{-1}\mathbf{f}(g_1)\mathbf{f}(g_2)\mathbf{S} \\ &= \mathbf{S}^{-1}\mathbf{f}(g_1)\mathbf{S}\mathbf{S}^{-1}\mathbf{f}(g_2)\mathbf{S} = \mathbf{f}'(g_1)\mathbf{f}'(g_2) \end{aligned}$$

Gruppen $\mathbf{f}'(G)$ er derfor også en repræsentation af n te grad af G . Repræsentationerne $\mathbf{f}(G)$ og $\mathbf{f}'(G)$ kaldes ækvivalente.

Sætning (9.4)

Ækvivalente repræsentationer har samme karakter.

Bevis: Idet $\mathbf{f}'(g) = \mathbf{S}^{-1} \mathbf{f}(g) \mathbf{S}$ ved vi fra matrix-regningen, at $\text{spor } \mathbf{f}'(g) = \text{spor } [\mathbf{S}^{-1} \mathbf{f}(g) \mathbf{S}] = \text{spor } \mathbf{f}(g)$, men det betyder netop $\chi_{\mathbf{f}'}(g) = \chi_{\mathbf{f}}(g)$.

I fortsættelse af sætning (7.7) skal vi her konstruere en tro repræsentation af n te grad til en endelig gruppe G af orden n . Idet vi benytter betegnelserne fra (7.7) knytter vi til elementet $g_i \in G$ matricen $\mathbf{F}(g_i)$ bestemt på følgende måde: første række består af lutter 0'er undtagen i søjle i_1 , hvor der skal stå 1; anden række består af lutter 0'er undtagen i søjle i_2 , hvor der skal stå 1, etc.; her er i_u bestemt ved, at $g_u g_i = g_{i_u}$. Matricen $\mathbf{F}(g_i)$ kaldes en *permutationsmatrix*, og man ser, at den er en ortogonal matrix ($[\mathbf{F}(g_i)]^{-1} = [\mathbf{F}(g_i)]^T$), og at den lineære transformation af K^n på sig selv givet ved

$$\underline{x}' = [\mathbf{F}(g_i)]^T \underline{x}$$

vil permutere en basis $\underline{b}_1, \underline{b}_2, \dots, \underline{b}_n$ for K^n til $\underline{b}_{i_1}, \underline{b}_{i_2}, \dots, \underline{b}_{i_n}$. Repræsentationen $\mathbf{F}(G)$ kaldes den *regulære repræsentation* af G . Vi skal fremhæve, at den eneste af matricerne $\mathbf{F}(g_i)$, som indeholder 1-taller i diagonalen, er $\mathbf{F}(e)$. Dette udtrykkes i følgende

Sætning (9.5)

Karakteren af den regulære repræsentation er repræsentationens grad på det neutrale element $e \in G$, og ellers 0, eller

$$\chi_F(e) = n, \quad \text{og} \quad \chi_F(g) = 0 \quad (g \in G, g \neq e).$$

Eksempel (9.6)

Vi betragter en cyklisk gruppe C_4 af orden 4 med elementer e, a, a^2, a^3 . Hvis $f(C_4)$ er en repræsentation af 1. grad, så er

$$f(e) = f(a^4) = [f(a)]^4 = 1$$

og $f(a)$ en enhedsrod af 4. orden. Der findes derfor 4 forskellige repræsentationer af 1. grad af C_4 :

	e	a	a^2	a^3
f_1	1	1	1	1
f_2	1	i	-1	$-i$
f_3	1	-1	1	-1
f_4	1	$-i$	-1	i

Af disse er $f_2(C_4)$ og $f_4(C_4)$ tro repræsentationer.

Eksempel (9.7)

Vi betragter *diedergruppen* D_3 , bestående af afbildninger af en ligesidet trekant på sig selv. Dens elementer betegner vi $e_1, c_3, c_3^2, d_1, d_2, d_3$, hvor c_3 er drejningen på 120° om normalen til trekantens plan gennem centrum, og hvor d_i er en 180° drejning om en af de tre højder i den ligesidede trekant. Gruppetavlen ser således ud:

	e	c_3	c_3^2	d_1	d_2	d_3
e	e	c_3	c_3^2	d_1	d_2	d_3
c_3	c_3	c_3^2	e	d_2	d_3	d_1
c_3^2	c_3^2	e	c_3	d_3	d_1	d_2
d_1	d_1	d_3	d_2	e	c_3^2	c_3
d_2	d_2	d_1	d_3	c_3	e	c_3^2
d_3	d_3	d_2	d_1	c_3^2	c_3	e

Man ser umiddelbart, at D_3 er isomorf med S_3 , se gruppetaflen i eksempel (3.2).

Ved en *repræsentation af 1. grad* af D_3 må det gælde, at d_i svarer til 1 eller -1 , da $d_i^2 = e$. Ligeledes må c_3 og c_3^2 svare til enhedsrødder af 3. orden. Endvidere er $d_1 c_3 d_1 = c_3^2$, hvilket medfører, at c_3 og c_3^2 svarer til samme enhedsrod af 3. orden, som derfor må være 1. Der er derfor to repræsentationer af 1. grad:

	e	c_3	c_3^2	d_1	d_2	d_3
f_1	1	1	1	1	1	1
f_2	1	1	1	-1	-1	-1

Ved en *repræsentation af 2. grad* er der til ethvert element i D_3 knyttet en regulær matrix af 2. orden; denne kan opfattes som en lineær transformation af planen $\mathbb{R}^2$. Nu afbilder ethvert element i D_3 netop trekantens plan i sig selv, og man kan derfor straks opskrive en sådan repræsentation efter valg af koordinatsystem. Lad fx et sædvanligt retvinklet koordinatsystem være valgt med nulpunkt i trekantens centrum og abskisseakse på en højde, således at en vinkelspids følger efter nulpunktet. Man finder da:

$$\begin{aligned} \mathbf{f}(e) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \mathbf{f}(c_3) &= \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} & \mathbf{f}(c_3^2) &= \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \\ \mathbf{f}(d_1) &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \mathbf{f}(d_2) &= \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} & \mathbf{f}(d_3) &= \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \end{aligned}$$

Vi bemærker, at $\chi_f(e) = 2$, altså graden af repræsentationen, at $\chi_f(c_3) = \chi_f(c_3^2) = -1$, og $\chi_f(d_i) = 0$; disse resultater stemmer med eksempel (4.5) og sætning (9.3).

Ved en *repræsentation af 3. grad* skal der til ethvert element i D_3 knyttes en regulær matrix af 3. orden. Ligesom ovenfor ser vi, at elementerne i D_3 er afbildninger af $\mathbb{R}^3$, og efter valg af koordinatsystem kan man opskrive matricer for disse (prøv dette).

Ved den *regulære repræsentation* $\mathbf{F}(D_3)$ af D_3 skal der til ethvert element i D_3 knyttes en permutationsmatrix af 6. orden. Til e knyttes naturligvis $\mathbf{E}$, enhedsmatricen af 6. orden. For at bestemme $\mathbf{F}(c_3)$ skal vi ifl. opskriften ovenfor udregne $Gc_3 = \{g_1, \dots, g_6\}c_3 = \{e, c_3, c_3^2, d_1, d_2, d_3\}c_3 = \{c_3, c_3^2, e, d_3, d_1, d_2\} = \{g_2, g_3, g_1, g_6, g_4, g_5\}$. Dermed har $\mathbf{F}(c_3)$ et 1-tal i

2. søjle af 1. række, i 3. søjle af 2. række, i 1. søjle af 3. række, etc. Ved en tilsvarende udregning af $\mathbf{F}(d_2)$ fås:

$$\mathbf{F}(c_3) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{og} \quad \mathbf{F}(d_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

De øvrige matricer opskrives let ved at udnytte søjlerne i gruppetavlen. Man bekræfter, at fx $\mathbf{F}(c_3)\mathbf{F}(d_2) = \mathbf{F}(d_3)$ og at

$$\chi_F(e) = 6 \quad \text{mens} \quad \chi_F(d_i) = \chi_F(c_3) = \chi_F(c_3^2) = 0.$$

Vi vender nu tilbage til begrebet ækvivalente repræsentationer. Ifølge selve begrebet falder repræsentationer af samme grad for en given gruppe i klasser af indbyrdes ækvivalente repræsentationer, som hver for sig kan betragtes som kendt, når blot en enkelt repræsentant for en klasse er kendt. Problemet at bestemme samtlige repræsentationer af en gruppe (af en given grad) reduceres herved til en bestemmelse af klasserne af ækvivalente repræsentationer, eller med andre ord til en bestemmelse af et fuldstændigt system af ikke-ækvivalente repræsentationer. For endelige grupper har man her et afgørende hjælpemiddel i følgende sætning (9.8), hvorefter man kan begrænse undersøgelsen til *unitære repræsentationer*, dvs. repræsentationer givet ved unitære matricer.

Sætning (9.8)

Enhver klasse af ækvivalente repræsentationer for en endelig gruppe indeholder (mindst) en unitær repræsentation.

Vi vil føre beviset for denne sætning ved at bemærke, at den er en konsekvens af følgende

Sætning (9.9)

Til en vilkårlig endelig undergruppe af matricer $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_r$ i GL_n findes $\mathbf{S} \in GL_n$, således at matricerne $\mathbf{S}^{-1}\mathbf{A}_1\mathbf{S}, \mathbf{S}^{-1}\mathbf{A}_2\mathbf{S}, \dots, \mathbf{S}^{-1}\mathbf{A}_r\mathbf{S}$ alle er unitære.

Bevis: Vi begynder med nogle betegnelser:

$\mathbf{S}^T$ skal betyde $\mathbf{S}$ transponeret. $\mathbf{S}^H$ skal betyde $\mathbf{S}$ transponeret og komplekst konjugeret, $(\mathbf{S}^T)^*$. Så er $\mathbf{S}^{-1} = \mathbf{S}^H$ ensbetydende med, at $\mathbf{S}$ er unitær, mens $\mathbf{S} = \mathbf{S}^H$ er ensbetydende med, at $\mathbf{S}$ er hermitesk. En diagonalmatrix med elementer $\lambda_1, \lambda_2, \dots, \lambda_n$ vil vi her betegne med: $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$. Og nu beviset:

Lad

$$(9.10) \quad \mathbf{A} = \sum_j \mathbf{A}_j^H \mathbf{A}_j$$

Så er $\mathbf{A}^H = \mathbf{A}$ og formen

$$\underline{x}^H(\mathbf{A}\underline{x}) = \sum_j \underline{x}^H \mathbf{A}_j^H \mathbf{A}_j \underline{x} = \sum_j (\mathbf{A}_j \underline{x})^H \mathbf{A}_j \underline{x}$$

en positiv definit (og hermitesk).

Ifølge hovedsætningen om reduktion af hermiteske former findes der en *unitær* matrix $\mathbf{U}$, således at

$$(9.11) \quad \mathbf{U}^{-1} \mathbf{A} \mathbf{U} = \mathbf{\Lambda} = \{\lambda_1, \lambda_2, \dots, \lambda_n\},$$

hvor $\lambda_1, \lambda_2, \dots, \lambda_n$ er egenverdierne for $\mathbf{A}$, og hvor $\lambda_i > 0$. Vi sætter

$$\mathbf{B}_j = \mathbf{U}^{-1} \mathbf{A}_j \mathbf{U} \quad (j = 1, 2, \dots, r)$$

Så er ifølge (9.10) og (9.11):

$$(9.12) \quad \mathbf{\Lambda} = \sum_j \mathbf{B}_j^H \mathbf{B}_j \quad \text{og}$$

$$(9.13) \quad \mathbf{E} = \mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{\Lambda} \mathbf{\Lambda}^{-\frac{1}{2}}, \quad \text{hvor} \quad \mathbf{\Lambda}^{-\frac{1}{2}} = \{\lambda_1^{-\frac{1}{2}}, \lambda_2^{-\frac{1}{2}}, \dots, \lambda_n^{-\frac{1}{2}}\}.$$

Endelig sætter vi

$$(9.14) \quad \mathbf{D}_j = \mathbf{\Lambda}^{\frac{1}{2}} \mathbf{B}_j \mathbf{\Lambda}^{-\frac{1}{2}}, \quad \text{hvor} \quad \mathbf{\Lambda}^{\frac{1}{2}} = \{\lambda_1^{\frac{1}{2}}, \lambda_2^{\frac{1}{2}}, \dots, \lambda_n^{\frac{1}{2}}\}.$$

Vi viser dernæst, at $\mathbf{D}_j$ er unitær:

$$\begin{aligned} \mathbf{D}_j^H \mathbf{D}_j &= (\mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{B}_j^H \mathbf{\Lambda}^{\frac{1}{2}}) \mathbf{E} (\mathbf{\Lambda}^{\frac{1}{2}} \mathbf{B}_j \mathbf{\Lambda}^{-\frac{1}{2}}) \\ &= (\mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{B}_j^H \mathbf{\Lambda}^{\frac{1}{2}}) (\mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{\Lambda} \mathbf{\Lambda}^{-\frac{1}{2}}) (\mathbf{\Lambda}^{\frac{1}{2}} \mathbf{B}_j \mathbf{\Lambda}^{-\frac{1}{2}}) \\ &= \mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{B}_j^H \left(\sum_i \mathbf{B}_i^H \mathbf{B}_i \right) \mathbf{B}_j \mathbf{\Lambda}^{-\frac{1}{2}} \\ &= \mathbf{\Lambda}^{-\frac{1}{2}} \left[\sum_i (\mathbf{B}_i \mathbf{B}_j)^H (\mathbf{B}_i \mathbf{B}_j) \right] \mathbf{\Lambda}^{-\frac{1}{2}}. \end{aligned}$$

Nu udnytter vi, at $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_r$, og derfor også $\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_r$ udgør endelige grupper; dette medfører, at

$$\sum_i (\mathbf{B}_i \mathbf{B}_j)^H (\mathbf{B}_i \mathbf{B}_j) = \sum_i \mathbf{B}_i^H \mathbf{B}_i = \mathbf{\Lambda}.$$

Vi finder derfor

$$\mathbf{D}_j^H \mathbf{D}_j = \mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{\Lambda} \mathbf{\Lambda}^{-\frac{1}{2}} = \mathbf{E}.$$

Til slut bemærker vi at

$$\mathbf{D}_j = \mathbf{\Lambda}^{\frac{1}{2}} \mathbf{U}^{-1} \mathbf{A}_j \mathbf{U} \mathbf{\Lambda}^{-\frac{1}{2}},$$

og den i sætningen nævnte matrix $\mathbf{S}$ er derfor

$$\mathbf{S} = \mathbf{U} \mathbf{\Lambda}^{-\frac{1}{2}}.$$

Hermed er beviset færdigt for (9.9). Sætningen (9.8) følger af denne, idet vi sætter $\mathbf{f}(g_j) = \mathbf{A}_j$, $j = 1, 2, \dots, r$.

Eksempelvis kan vi nævne, at repræsentationen af 2. grad i eksempel (9.7) er unitær; i almindelighed gælder, at den regulære repræsentation er unitær.

Som følge af sætning (9.8) vil vi overalt i det følgende tænke os valgt unitære repræsentationer for endelige grupper, dvs. de indgående matricer er unitære.

10. Reducibel og irreducibel repræsentation

Vi tænker os nu givet en gruppe G og to repræsentationer $\mathbf{A}_j$ og $\mathbf{B}_j$ af grader henholdsvis m og n , dvs. $\mathbf{A}_j$ er (unitær) af orden m , og $\mathbf{B}_j$ er (unitær) af orden n , mens $j = 1, 2, \dots, r$, hvor r er gruppen G 's orden. Så kan vi danne, hvad vi vil kalde *diagonalblokmatricer*:

$$(10.1) \quad \{\mathbf{A}_j, \mathbf{B}_j\} = \begin{pmatrix} \mathbf{A}_j & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_j \end{pmatrix}$$

af orden $m + n$. Man efterviser let, at

$$\{\mathbf{A}_j, \mathbf{B}_j\} \cdot \{\mathbf{A}_k, \mathbf{B}_k\} = \{\mathbf{A}_j \mathbf{A}_k, \mathbf{B}_j \mathbf{B}_k\},$$

og heraf slutter man, at matricerne i (10.1) også er en repræsentation af G , men af grad $m + n$.

Tilsvarende kan man til tre repræsentationer givet ved matricer $\mathbf{A}_j, \mathbf{B}_j, \mathbf{C}_j$, danne en ny repræsentation ved hjælp af diagonalblokmatricer

$$(10.2) \quad \mathbf{D}_j = \{\mathbf{A}_j, \mathbf{B}_j, \mathbf{C}_j\} = \begin{pmatrix} \mathbf{A}_j & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_j & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{C}_j \end{pmatrix}$$

og så videre.

Nu er det egentlig den omvendte proces, der vil interessere os, nemlig den, hvorved en forelagt repræsentation, som fx (10.2), kan opspaltes i repræsentationer af lavere grader. Det er her væsentligt at bemærke, at repræsentationer, der er ækvivalente med fx $\mathbf{D}_j$ i (10.2) vil i almindelighed ikke fremstilles ved diagonalblokmatricer, idet $\mathbf{S}^{-1} \mathbf{D}_j \mathbf{S}$ ikke behøver at udvise diagonalblokstruktur. Men vi fastsætter:

Definition (10.3): En repræsentation $\mathbf{M}_j$ skal kaldes *reducibel*, hvis enten repræsentationen selv eller en med den ækvivalent repræsentation $\mathbf{S}^{-1} \mathbf{M}_j \mathbf{S}$ kan fremstilles ved diagonalblokmatricer. Hvis hverken matricerne $\mathbf{M}_j$ eller $\mathbf{S}^{-1} \mathbf{M}_j \mathbf{S}$ for noget som helst $\mathbf{S}$ er diagonalblokmatricer, siges $\mathbf{M}_j$ at være en *irreducibel* repræsentation.

Det er nu let at vise

Sætning (10.4)

Hvis en unitær repræsentation $\mathbf{D}_j$ af grad n lader et egentlig underrum V^p (af dimension $p > 0$) i K^n invariant, så er repræsentationen *reducibel*.

Her betyder udtrykket, at “ $\mathbf{D}_j$ lader V^p invariant”, at for ethvert $\underline{x} \in V^p$ vil

$$(10.5) \quad \underline{y} = \mathbf{D}_j \underline{x} \in V^p$$

Vi fører beviset ved først at vælge et nyt koordinatsystem i K^n bestemt ved koordinattransformationen

$$\underline{x} = \mathbf{S} \underline{x}_1, \quad \text{hvor} \quad \mathbf{S}^{-1} = \mathbf{S}^H.$$

Her skal de p første basisvektorer vælges som ortonormerede vektorer, der udspænder V^p , mens de $n - p$ sidste af de ialt n ortonormerede basisvektorer vil udspænde rummet $V^\perp$ bestående af vektorer ortogonale på V^p . Transformationen i (10.5) antager herved formen

$$\underline{y}_1 = \mathbf{S}^H \mathbf{D}_j \mathbf{S} \underline{x}_1,$$

hvor de p første søjler i matricen $\mathbf{S}^H \mathbf{D}_j \mathbf{S}$ er billedvektorerne af de p første basisvektorer, disse billedvektorer ligger imidlertid i V^p og har derfor 0'er på de sidste $n - p$ pladser i deres koordinatfremstilling. Endvidere er de sidste $n - p$ søjler i $\mathbf{S}^H \mathbf{D}_j \mathbf{S}$ billeder af basisvektorer i $V^\perp$; sådanne billedvektorer ligger også selv i $V^\perp$ og har derfor 0'er på deres p første koordinater. Matricen $\mathbf{S}^H \mathbf{D}_j \mathbf{S}$ har herefter udseendet

$$\mathbf{S}^H \mathbf{D}_j \mathbf{S} = \begin{pmatrix} \mathbf{A}_j & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_j \end{pmatrix},$$

hvor $\mathbf{A}_j$ er af orden p , og $\mathbf{B}_j$ af orden $n - p$. Repræsentationen $\mathbf{D}_j$ er hermed vist at være reducibel.

Bemærkning: I betragtning af (9.8) kan vi svække forudsætningerne i (10.4), således at den kommer til at lyde: *Hvis alle matricer af en repræsentation lader et egentligt underrum invariant, så er repræsentationen reducibel.* Det er uden videre klart, at den omvendte sætning gælder, idet man for en reducibel repræsentation kan benytte diagonalblokfremstillingen og deraf direkte aflæse invariante underrum.

I §9 indførte vi betegnelsen $\{l, l, \dots, l\} = l\mathbf{E}$. I forbindelse med (10.2) skal på lignende måde $\{h\mathbf{E}, k\mathbf{E}, l\mathbf{E}\}$ betyde en diagonalblokmatrix med samme bloktyper som $\{\mathbf{A}_j, \mathbf{B}_j, \mathbf{C}_j\}$.

Så betragter vi en vilkårlig repræsentation ækvivalent med $\mathbf{D}_j$ i (10.2), altså matricer af formen

$$\mathbf{D}'_j = \mathbf{S}^{-1} \{ \mathbf{A}_j, \mathbf{B}_j, \mathbf{C}_j \} \mathbf{S}$$

og i tilknytning hertil

$$\mathbf{T} = \mathbf{S}^{-1} \{ h\mathbf{E}, k\mathbf{E}, l\mathbf{E} \} \mathbf{S},$$

så kan vi let efterprøve, at

$$\mathbf{D}'_j \mathbf{T} = \mathbf{T} \mathbf{D}'_j$$

selv, når h, k, l er indbyrdes forskellige. Gyldigheden af disse betragtninger er uafhængigt af antallet af blokke i diagonalen i $\mathbf{D}_j$, og vi har derfor vist:

Sætning (10.6)

Hvis en repræsentation $\mathbf{D}'_j$ er reducibel, så findes der en matrix $\mathbf{T} \neq c\mathbf{E}$, således at $\mathbf{D}'_j \mathbf{T} = \mathbf{T} \mathbf{D}'_j$.

Den omvendte sætning gælder også:

Sætning (10.7)

Hvis der findes en matrix $\mathbf{T} \neq c\mathbf{E}$, således at $\mathbf{T}$ kommuterer med hver af matricerne $\mathbf{D}_j$ i en repræsentation, så er repræsentationen reducibel.

Ækvivalent med (10.7) er følgende:

Sætning (10.8)

Hvis der findes en matrix $\mathbf{T}$ som kommuterer med hver af matricerne $\mathbf{D}_j$ i en irreducibel repræsentation, så er $\mathbf{T} = c\mathbf{E}$.

Vi foretrækker at bevise den sidste formulering:

Bevis: Lad c være en egenverdi for $\mathbf{T}$, dvs. c er en rod i determinantligningen $|\mathbf{T} - t\mathbf{E}| = 0$. Svarende til c findes der et underrum V af K^n bestående af egenvektorer for vektorfunktionen $\underline{y} = \mathbf{T}\underline{x}$. Der gælder altså

$$(10.9) \quad \mathbf{T}\underline{x} = c\underline{x} \quad \text{for ethvert } \underline{x} \in V.$$

Dette underrum V er invariant over for $\mathbf{D}_j$, idet

$$\mathbf{T}\mathbf{D}_j\underline{x} = \mathbf{D}_j\mathbf{T}\underline{x} = \mathbf{D}_jc\underline{x} = c\mathbf{D}_j\underline{x}.$$

Denne relation viser nemlig, at vektoren $\mathbf{D}_j\underline{x}$ er en egenvektor for $\mathbf{T}$ svarende til egenverdien c , og $\mathbf{D}_j\underline{x}$ tilhører derfor V . Eftersom $\mathbf{D}_j$ er irreducibel må V være *hele* K^n (10.4). Ifølge (10.9) gælder altså

$$\mathbf{T}\underline{x} = c\underline{x} \quad \text{for ethvert } \underline{x} \in K^n,$$

hvilket medfører, at $\mathbf{T} = c\mathbf{E}$.

Vi kan straks give en anvendelse af den vigtige sætning:

Korollar (10.10)

En irreducibel repræsentation af en kommutativ gruppe G er af 1. grad.

Bevis: Lad $\mathbf{D}_j$ repræsentere G ; så er $\mathbf{D}_j\mathbf{D}_k = \mathbf{D}_k\mathbf{D}_j$, for $j = 1, 2, \dots, r$, hvor r er G 's orden. Ifølge (10.9) får vi så: $\mathbf{D}_k = c_k\mathbf{E}$. Men dette viser netop, at $\mathbf{E}$ må være af 1. orden, idet vi benytter at $\mathbf{D}_1, \mathbf{D}_2, \dots, \mathbf{D}_r$ er en irreducibel repræsentation af G , jvf. (10.3).

11. Schur's lemma og ortogonalitetsrelationerne

Som optakt til dette afsnit skal vi bevise en sætning, som er i slægt med (10.8); den omtales ofte som *Schur's lemma*:

Sætning (11.1)

Lad $\mathbf{A}_j$ og $\mathbf{B}_j$ være to irreducible repræsentationer af gruppen G af grader henholdsvis n og p , og lad $\underline{y} = \mathbf{T}\underline{x}$ være en lineær afbildning af K^n ind i K^p . Hvis det om matricerne $\mathbf{T}$, $\mathbf{A}_j$ og $\mathbf{B}_j$ gælder, at

$$(11.2) \quad \mathbf{T}\mathbf{A}_j = \mathbf{B}_j\mathbf{T} \quad (j = 1, 2, \dots, r),$$

hvor r er G 's orden, så er enten $\mathbf{T}$ en nulmatrix eller $p = n$, $\mathbf{T}$ regulær og $\mathbf{A}_j$ og $\mathbf{B}_j$ ækvivalente.

Bevis: Lad $V(\mathbf{T})$ betegne samlingen af billedvektorer i K^p under afbildning givet ved $\mathbf{T}$. Vi ved $V(\mathbf{T})$ er et vektorrum i K^p . Lad $\underline{y} \in V(\mathbf{T})$. Så er

$$\mathbf{B}_j\underline{y} = \mathbf{B}_j\mathbf{T}\underline{x} = \mathbf{T}\mathbf{A}_j\underline{x} \in V(\mathbf{T}).$$

Dette viser, at $V(\mathbf{T})$ er et invariant (under)rum over for $\mathbf{B}_j$. Ifølge bemærkning til (10.3) og ved at benytte, at $\mathbf{B}_j$ er irreducibel, kan vi slutte, at $V(\mathbf{T})$ er enten $\underline{0}$ eller hele K^p . I første tilfælde måtte $\mathbf{T}$ være nulmatricen, og vi var færdige. I andet tilfælde, hvor altså $V(\mathbf{T}) = K^p$, betragter vi

$$\ker \mathbf{T} = \{\underline{x} \in K^n \mid \mathbf{T}\underline{x} = \underline{0} \in K^p\}.$$

$\ker \mathbf{T}$ er et vektorrum (i K^n). Hvis $\underline{x} \in \ker \mathbf{T}$, så gælder

$$\mathbf{T}\mathbf{A}_j\underline{x} = \mathbf{B}_j\mathbf{T}\underline{x} = \mathbf{B}_j\underline{0} = \underline{0} \in K^p,$$

dvs. $\underline{x} \in \ker \mathbf{T}$ medfører $\mathbf{A}_j\underline{x} \in \ker \mathbf{T}$, eller med andre ord $\ker \mathbf{T}$ er et invariant (under)rum over for $\mathbf{A}_j$. Da $\mathbf{A}_j$ er irreducibel, må $\ker \mathbf{T}$ være $\underline{0}$ eller hele K^n .

Tilfældet $\ker \mathbf{T} = K^n$ strider mod, at $V(\mathbf{T}) = K^p$.

Tilfældet $\ker \mathbf{T} = \underline{0}$ medfører, at $\mathbf{T}$ er regulær, idet

$$1) \quad \mathbf{T}\underline{x}_1 = \mathbf{T}\underline{x}_2 \Rightarrow \mathbf{T}(\underline{x}_1 - \underline{x}_2) = \underline{0} \Rightarrow \underline{x}_1 = \underline{x}_2.$$

2) Af 1) følger, at $V(\mathbf{T})$ er n -dimensional; men $V(\mathbf{T})$ er hele K^p , og derfor er $p = n$.

Af (11.2) følger dernæst $\mathbf{A}_j = \mathbf{T}^{-1}\mathbf{B}_j\mathbf{T}$. Hermed er beviset ført.

Vi går dernæst over til de såkaldte *ortogonalitetsrelationer*, som ofte anvendes i fx kvantemekanikken.

Lad G være en gruppe af orden r bestående af elementerne $g_1, g_2, \dots, g_r$; lad to ikke-ækvivalente, irreducible, unitære repræsentationer være givet ved henholdsvis matricerne $\mathbf{A}^{(s)} = \mathbf{A}(g_s)$ af n te grad og $\mathbf{B}^{(s)} = \mathbf{B}(g_s)$ af p te grad, hvor $s = 1, 2, \dots, r$. Vi betegner elementerne i matricerne $\mathbf{A}^{(s)}$ og $\mathbf{B}^{(s)}$ med henholdsvis $a_{ij}^{(s)}$ og $b_{kl}^{(s)}$. Så gælder der

Sætning (11.3)

For vilkårlig valg af indices i, j, k, l er

$$(11.4) \quad \sum_{s=1}^r a_{ij}^{(s)} [b_{kl}^{(s)}]^* = 0$$

$$(11.5) \quad \sum_{s=1}^r a_{ij}^{(s)} [a_{kl}^{(s)}]^* = \frac{r}{n} \delta_{ik} \delta_{jl},$$

hvor δ_{ik} og δ_{jl} er Kronecker-symboler.

Bevis: Lad foreløbig $\mathbf{M}$ være en vilkårlig matrix af type (n, p) og konstruér matricen

$$\mathbf{S} = \sum_{s=1}^r \mathbf{A}(g_s) \mathbf{M} [\mathbf{B}(g_s)]^{-1}$$

For fastholdt $g_t \in G$ benytter vi dernæst dels, at $g_t g_s$ gennemløber G med g_s , dels at repræsentationsegenskaberne medfører fx

$$[\mathbf{B}(g_t g_s)]^{-1} = [\mathbf{B}(g_s)]^{-1} [\mathbf{B}(g_t)]^{-1}$$

så finder vi:

$$\begin{aligned} \mathbf{A}(g_t) \mathbf{S} &= \sum_{s=1}^r \mathbf{A}(g_t) \mathbf{A}(g_s) \mathbf{M} [\mathbf{B}(g_s)]^{-1} \\ &= \sum_{s=1}^r \mathbf{A}(g_t g_s) \mathbf{M} [\mathbf{B}(g_t g_s)]^{-1} \mathbf{B}(g_t) = \mathbf{S} \mathbf{B}(g_t) \end{aligned}$$

Denne matrix $\mathbf{S}$ tilfredsstiller altså (11.2) (med $\mathbf{A}$ og $\mathbf{B}$ ombyttede) og må ifølge Schur's lemma være nulmatricen, fordi $\mathbf{A}^{(s)}$ og $\mathbf{B}^{(s)}$ er irreducible repræsentationer. Med andre ord: for vilkårligt valg af $\mathbf{M}$ er

$$(11.6) \quad \sum_{s=1}^r \mathbf{A}(g_s) \mathbf{M} [\mathbf{B}(g_s)]^{-1} = \mathbf{0}.$$

Vi vælger nu $\mathbf{M}$ til den matrix, hvis element $\{\mathbf{M}\}_{jl} = 1$, mens alle andre elementer er 0; så giver (11.6)

$$(11.7) \quad \sum_{s=1}^r \{\mathbf{A}(g_s)\}_{ij} \{[\mathbf{B}(g_s)]^{-1}\}_{lk} = 0.$$

Da matricen $\mathbf{B}(g_s)$ er unitær, er elementer $\{[\mathbf{B}(g_s)]^{-1}\}_{lk} = [b_{kl}^{(s)}]^*$, og (11.7) bliver netop til (11.4).

Vi går tilsvarende frem med udledelsen af (11.5): Lad

$$\mathbf{T} = \sum_{s=1}^r \mathbf{A}(g_s) \mathbf{M} [\mathbf{A}(g_s)]^{-1},$$

hvor $\mathbf{M}$ er vilkårlig af type (n, n) . Så er $\mathbf{A}(g_t) \mathbf{T} = \mathbf{T} \mathbf{A}(g_t)$, og $\mathbf{T}$, ifølge (10.8), af formen $c\mathbf{E}$, altså

$$(11.8) \quad \mathbf{T} = \sum_{s=1}^r \mathbf{A}(g_s) \mathbf{M} [\mathbf{A}(g_s)]^{-1} = c\mathbf{E},$$

hvor $c = c(\mathbf{M})$. Igen vælger vi specielle matricer på $\mathbf{M}$'s plads: vi sætter $\{\mathbf{M}\}_{jl} = 1$, mens alle andre elementer i $\mathbf{M}$ sættes lig 0; den tilhørende c -værdi kalder vi c_{jl} . Så giver (11.8):

$$(11.9) \quad \sum_{s=1}^r \{\mathbf{A}(g_s)\}_{ij} \{[\mathbf{A}(g_s)]^{-1}\}_{lk} = c_{jl} \delta_{ik}.$$

Værdien c_{jl} kan vi beregne ved at sætte $i = k$ og summere over i fra 1 til n .

$$nc_{jl} = \sum_{i=1}^n \sum_{s=1}^r \{\mathbf{A}(g_s)\}_{ij} \{[\mathbf{A}(g_s)]^{-1}\}_{li} = \sum_{s=1}^r \{\mathbf{E}\}_{jl} = r \delta_{jl}.$$

Dette indsættes i (11.9) og benytter vi, at matricen $\mathbf{A}(g_s)$ er unitær, fås netop (11.5).

Relationerne (11.4) og (11.5) kan specielt skaffe oplysninger om gruppekarakterer: Først sætter vi $i = j$ og $k = l$ i de to formler:

$$(11.10) \quad \sum_{s=1}^r a_{ii}^{(s)} [b_{kk}^{(s)}]^* = 0$$

$$(11.11) \quad \sum_{s=1}^r a_{ii}^{(s)} [a_{kk}^{(s)}]^* = \frac{r}{n} \delta_{ik}.$$

I disse formler benytter vi dernæst, at gruppekarakteren

$$\chi_A(g_s) = \sum_{i=1}^n a_{ii}^{(s)},$$

og finder ved summation over både i og k :

$$(11.12) \quad \sum_{s=1}^r \chi_A(g_s) [\chi_B(g_s)]^* = 0$$

$$(11.13) \quad \sum_{s=1}^r \chi_A(g_s) [\chi_A(g_s)]^* = r.$$

Vi minder om, at repræsentationerne givet ved $\mathbf{A}$ -matricerne og $\mathbf{B}$ -matricerne er ikke ækvivalente ifølge forudsætningerne til sætning (11.3). Så kan vi ved hjælp af (11.12) bevise:

Sætning (11.14)

To ikke-ækvivalente, irreducible repræsentationer har forskellige karakterer.

Bevis: Hvis $\chi_A(g_s) = \chi_B(g_s)$ for ethvert $s = 1, 2, \dots, r$, så var ifølge (11.12):

$$\sum_{s=1}^r \chi_A(g_s) [\chi_A(g_s)]^* = 0$$

i strid med (11.13).

Ifølge (11.14) er der lige så mange forskellige karakterer som ikke-ækvivalente, irreducible repræsentationer. Vi skal nu sætte dette antal i forbindelse med antallet af konjugationsklasser i G . Allerede i (9.3) nævnte vi, at gruppeelementer i samme konjugationsklasse har samme karakter i en given repræsentation. Lad nu konjugationsklasserne i G være $K_1, K_2, \dots, K_h$, hvor K_i antages at indeholde r_i elementer; idet vi fx tænker os $K_1 = K_e$ er $r_1 = 1$.

Med disse betegnelser kan vi omskrive (11.12) og (11.13) til

$$(11.15) \quad \sum_{i=1}^h r_i \chi_A(K_i) [\chi_B(K_i)]^* = 0$$

$$(11.16) \quad \sum_{i=1}^h r_i \chi_A(K_i) [\chi_A(K_i)]^* = r.$$

Vi kan bekvemt udtrykke resultaterne i (11.15) og (11.16) ved hjælp af to vektorer:

$$\left(\sqrt{\frac{r_1}{r}} \chi_A(K_1), \sqrt{\frac{r_2}{r}} \chi_A(K_2), \dots, \sqrt{\frac{r_h}{r}} \chi_A(K_h) \right) \quad \text{og} \\ \left(\sqrt{\frac{r_1}{r}} \chi_B(K_1), \sqrt{\frac{r_2}{r}} \chi_B(K_2), \dots, \sqrt{\frac{r_h}{r}} \chi_B(K_h) \right)$$

Disse to vektorer er ifølge (11.15) og (11.16) ortonormerede (i det h -dimensionale komplekse rum K^h). Ud fra denne bemærkning slutter vi, at der *højst* kan være h forskellige karakterer hidrørende fra irreducible repræsentationer, simpelthen fordi h er det højeste antal indbyrdes ortogonale vektorer i K^h . *Antallet af ikke-ækvivalente irreducible repræsentationer er derfor også højst lig h .*

Vi nævner uden bevis, at der gælder følgende:

Sætning (11.17)

For en endelig gruppe G er antallet af ikke-ækvivalente, irreducible repræsentationer lig med antallet af konjugationsklasser.

Vi kan nu ifølge denne sætning bestemme ialt h ikke-ækvivalente, irreducible repræsentationer af grader henholdsvis $n_1, n_2, \dots, n_h$ ved matricerne

$A_1, A_2, \dots, A_r$ af orden n_1

$B_1, B_2, \dots, B_r$ af orden n_2

$\vdots$

$H_1, H_2, \dots, H_r$ af orden n_h

Så er ifølge (11.15) og (11.16) matricen

$$\begin{pmatrix} \sqrt{\frac{r_1}{r}} \chi_A(K_1) & \sqrt{\frac{r_2}{r}} \chi_A(K_2) & \cdots & \sqrt{\frac{r_h}{r}} \chi_A(K_h) \\ \sqrt{\frac{r_1}{r}} \chi_B(K_1) & \sqrt{\frac{r_2}{r}} \chi_B(K_2) & \cdots & \sqrt{\frac{r_h}{r}} \chi_B(K_h) \\ \vdots & \vdots & & \vdots \\ \sqrt{\frac{r_1}{r}} \chi_H(K_1) & \sqrt{\frac{r_2}{r}} \chi_H(K_2) & \cdots & \sqrt{\frac{r_h}{r}} \chi_H(K_h) \end{pmatrix}$$

unitær, og derfor er dens søjler ortonormerede, dvs.

$$\frac{\sqrt{r_i r_j}}{r} \left(\chi_A(K_i) [\chi_A(K_j)]^* + \cdots + \chi_H(K_i) [\chi_H(K_j)]^* \right) = \delta_{ij}$$

eller

(11.18)

$$\chi_A(K_i) [\chi_A(K_j)]^* + \chi_B(K_i) [\chi_B(K_j)]^* + \cdots + \chi_H(K_i) [\chi_H(K_j)]^* = \frac{r}{r_i} \delta_{ij}.$$

Af denne relation skal vi nøjes med at gøre en enkelt anvendelse: Vi vælger $i = j = 1$ og dermed $K_1 = K_e$ og $r_1 = 1$; så er ifølge (9.2)

$$\chi_A(K_e) = [\chi_A(K_e)]^* = n_1, \dots, \chi_H(K_e) = [\chi_H(K_e)]^* = n_h,$$

og (11.18) giver ved indsættelse:

$$(11.19) \quad n_1^2 + n_2^2 + \cdots + n_h^2 = \frac{r}{r_1} = r.$$

Denne relation kan i visse tilfælde benyttes til en bestemmelse af tallene $n_1, n_2, \dots, n_h$, når h og r er kendt.

Eksempel (11.20)

Vi vender tilbage til gruppen D_3 i (9.7). Her skal vi se på spørgsmålet om irreducibel repræsentationer og deres karakterer. Ifølge (11.17) er antallet af irreducible repræsentationer lig med antallet af konjugationsklasser, i dette tilfælde $h = 3$, idet D_3 har følgende klasser:

$$\begin{array}{ll} K_1 = \{e\} & r_1 = 1 \\ K_2 = \{c_3, c_3^2\} & r_2 = 2 \\ K_3 = \{d_1, d_2, d_3\} & r_3 = 3 \end{array}$$

De tre irreducible repræsentationer har grader n_1, n_2, n_3 , som tilfredsstiller (11.19):

$$n_1^2 + n_2^2 + n_3^2 = 6.$$

Denne ligning har som eneste heltallige, positive løsninger $n_1 = 1, n_2 = 1$, og $n_3 = 2$. Begge irreducible repræsentationer af 1. grad er anført i eksempel (9.7).

Ved den første afbildes hvert element i D_3 i tallet 1, og gruppekarakteren χ_A antager kun værdien 1; ved den anden repræsentation antager karakteren χ_B værdien 1 på K_1 og K_2 , men værdien -1 på K_3 .

Med hensyn til repræsentationer af 2. grad, så har vi allerede angivet én i (9.7). Lad

$$\mathbf{T} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

være en vilkårlig matrix, og antag, at $\mathbf{T}$ kommuterer med matricerne i repræsentationen af 2. grad i (9.7). Så regner man let efter, at

$$\begin{aligned} \mathbf{T}\mathbf{f}(d_1) &= \mathbf{f}(d_1)\mathbf{T} &\Rightarrow & b = c = 0, \\ \mathbf{T}\mathbf{f}(c_3) &= \mathbf{f}(c_3)\mathbf{T} &\Rightarrow & a = d. \end{aligned}$$

Ialt finder man derfor, at $\mathbf{T} = a\mathbf{E}$. Ifølge sætning (10.6) har vi dermed vist, at den anførte repræsentation er irreducibel.

Vi kan herefter opstille følgende *karaktertavle* for D_3 :

	K_1	$(2)K_2$	$(3)K_3$
χ_A	1	1	1
χ_B	1	1	-1
χ_C	2	-1	0

Ud fra denne tavle kan vi illustrere relationerne (11.15), (11.16) og (11.18); først (11.15):

$$r_1\chi_A(K_1)\chi_B(K_1) + r_2\chi_A(K_2)\chi_B(K_2) + r_3\chi_A(K_3)\chi_B(K_3) = 1 + 2 - 3 = 0.$$

En illustration af (11.16) er:

$$r_1|\chi_C(K_1)|^2 + r_2|\chi_C(K_2)|^2 + r_3|\chi_C(K_3)|^2 = 1 \cdot 4 + 2 \cdot 1 + 3 \cdot 0 = 6 = r$$

Og (11.18) kan belyses ved følgende to relationer:

$$\begin{aligned} |\chi_A(K_2)|^2 + |\chi_B(K_2)|^2 + |\chi_C(K_2)|^2 &= 1 + 1 + 1 = 3 = \frac{r}{r_2} \\ \chi_A(K_2)[\chi_A(K_3)]^* + \chi_B(K_2)[\chi_B(K_3)]^* + \chi_C(K_2)[\chi_C(K_3)]^* &= \\ &= 1 \cdot 1 + 1 \cdot (-1) + (-1) \cdot 0 = 0. \end{aligned}$$

12. Kontinuerte grupper

En behandling af ikke-endelige grupper støder på vanskeligheder af forskellig art, som fx (1) elementerne har ikke nødvendigvis endelig orden; (2) summation over alle gruppens elementer, repræsenteret ved matricer, har ikke umiddelbart mening.

For endelige grupper skal her omtales nogle få træk ved de kontinuerte eller topologiske grupper; deres placering inden for gruppebegrebet er antydnet ved følgende opstilling:

$$\text{grupper} \begin{cases} \text{endelige} \\ \text{uendelige} \begin{cases} \text{diskrete} \\ \text{topologiske} \begin{cases} \text{Lie-grupper} \end{cases} \end{cases} \end{cases}$$

En gruppe kaldes *topologisk*, når mængden af dens elementer udgør et såkaldt topologisk rum; dvs. hvert gruppeelement g er tilordnet (uendelig mange) delmængder $U(g)$ af gruppen; disse kaldes *omegne* af g . Omegnene skal opfylde visse nærliggende krav; ved hjælp af omegnsbegrebet udtrykkes topologiske begreber som *åben* mængde og *afsluttet* (eller lukket) mængde, ligesom

kontinuitet af gruppemultiplikationen formuleres på grundlag af omegnsbegrebet. I den forbindelse kan vi som eksempel på “nærliggende krav” nævne:

$$\begin{aligned} \text{a)} \quad h \in U_1(g) &\Rightarrow h^{-1} \in U_2(g^{-1}) \\ \text{b)} \quad k \in U_1(g) \quad \wedge \quad l \in U_2(h) &\Rightarrow kl \in U_3(gh) \end{aligned}$$

Eksempel (12.1)

Den additive gruppe $\mathbb{R}$ af alle reelle tal x kan opfattes som en topologisk gruppe, idet “omegn af x ” betyder et (vilk.) åbent interval, der indeholder det reelle tal x . En topologisk gruppe kaldes *kompakt*, når enhver overdækning af gruppen med åbne mængder kan udtyndes til en endelig overdækning. For kompakte rum gælder, at enhver reel kontinuert funktion defineret på det kompakte rum er begrænset og antager såvel supremum som infimum. Gruppen $\mathbb{R}$ er ikke kompakt, jvf. funktionen $f(x) = x$.

Blandt topologiske grupper spiller *Lie-grupperne* en vigtig rolle, fordi begrebet dels er tilstrækkeligt omfattende til at indeholde vigtige eksempler i geometri, analyse og fysik, og dels tilstrækkeligt snævert til, at metoder fra differentiaalligningernes teori kan anvendes ved undersøgelser i Lie-grupper.

En topologisk gruppe kaldes Lie-gruppe, når hvert af dens elementer kan beskrives ved et endeligt antal parametre; det mindste antal parametre nødvendige for denne beskrivelse kaldes gruppens *dimension*.

Som indledning lad os betragte en (kontinuert) gruppe, hvis elementer $g(t)$ kan beskrives ved en enkel, reel parameter t . Idet disse elementer opfylder det første gruppeaksiom, skal der til ethvert par af reelle tal t og s findes et éntydigt bestemt reelt tal u således, at

$$g(u) = g(t)g(s)$$

Gruppetavlen bliver herefter en relation til fastlæggelse af u fra t, s :

$$u = f(t, s).$$

Den associative lov pålægger denne funktion, at

$$f(u, f(t, s)) = f(f(u, t), s).$$

Yderligere må der svarende til gruppens neutrale element e , findes en parameterværdi ω , som opfylder:

$$e = g(\omega) \quad \wedge \quad f(t, \omega) = f(\omega, t) = t;$$

da ethvert gruppeelement har et inverst, er der til enhver parameterværdi t knyttet et $\bar{t}$ med

$$f(t, \bar{t}) = f(\bar{t}, t) = \omega.$$

Kontinuitetskravet – at gruppemultiplikationen er kontinuert – medfører, at $f(t, s)$ er kontinuert i begge variable, og at $\bar{t}$ er en kontinuert funktion af t .

Sædvanligvis pålægger man parameterfunktionerne – overfor funktionen f – yderligere differentiabilityskrav, før man taler om en Lie-gruppe, fx at parameterfunktionerne er vilkårligt ofte differentiable.

Eksempel (12.2)

Lad os betragte den multiplikative gruppe af matricer af 2. orden, hvor gruppeelementet $\mathbf{g}(t)$ har formen

$$\mathbf{g}(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

$\mathbf{g}(0)$ er det neutrale element; $\mathbf{g}(-t)$ er inverst til $\mathbf{g}(t)$, og funktionen ovenfor bliver her

$$u = f(t, s) = t + s.$$

Eksempel (12.3)

Lad os betragte gruppen af lineære afbildninger af $\mathbb{R}$ ind i $\mathbb{R}$, hvor gruppeelementet $g = g(t_1, t_2)$ afbilder x i x' , så at

$$x' = t_1 x + t_2 \quad (t_1 \neq 0)$$

Hvis $x'' = s_1 x' + s_2$ og ved indsættelse: $x'' = r_1 x + r_2$, så finder man

$$r_1 = s_1 t_1 \quad \text{og} \quad r_2 = s_1 t_2 + s_2.$$

Gruppens neutrale element er afbildningen, hvorved

$$x' = t_1 x + t_2 \quad \text{med} \quad t_1 = 1, t_2 = 0.$$

Til $x' = t_1 x + t_2$ svarer $x = \bar{t}_1 x' + \bar{t}_2$, hvor

$$\bar{t}_1 = \frac{1}{t_1} \quad \text{og} \quad \bar{t}_2 = -\frac{t_2}{t_1}.$$

Gruppen er ikke-abelsk og to-dimensional.

Eksempel (12.4)

Akse-rotationsgruppen af drejninger af $\mathbb{R}^3$ om z -aksen har elementer givet ved

$$a : \begin{cases} x' = x \cos \phi_a - y \sin \phi_a \\ y' = x \sin \phi_a + y \cos \phi_a \\ z' = z \end{cases} \quad (0 \leq \phi_a < 2\pi).$$

Der er en gruppeparameter, ϕ_a ; gruppens neutrale element er elementet svarende til $\phi_a = 0$. Gruppemultiplikationen – dvs. sammensætningen af drejninger – bliver i parameteren: $\phi_c = \phi_a + \phi_b \pmod{2\pi}$, og det inverse a^{-1} til a har parameter $\phi_{-a} = -\phi_a \pmod{2\pi}$. Gruppen er kommutativ.

Vi genoptager udviklingen af begreberne for enkeltparametergrupperne: Ligesom det for endelige grupper i forbindelse med fx omtalen af karakterer var hensigtsmæssigt at indføre en gruppealgebra: summer af gruppeelementer og

multiplikation af gruppeelementer med en skalar, således er det også i kontinuerte grupper hensigtsmæssigt at gøre det muligt at tale om linearkombinationer af gruppeelementer. Dette finder først og fremmest anvendelse ved indførelse af en *infinitesimal operator*; denne defineres som den afledede af gruppeelementet mht. gruppeparameteren og beregnet i parameterværdien ω svarende til det neutrale element. Altså er infinitesimaloperatoren I defineret ved

$$I = \lim_{h \rightarrow 0} \frac{g(\omega + h) - g(\omega)}{h} = \left[\frac{dg}{dt} \right]_{\omega}.$$

I eksempel (12.2) ovenfor finder man $I = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Den afledede i en vilkårlig parameterværdi defineres ved

$$\frac{dg}{dt} = \lim_{h \rightarrow 0} \frac{g(t+h) - g(t)}{h}.$$

Heri er $g(t+h) = g(\omega + \epsilon)g(t)$, idet

$$t+h = f(\omega + \epsilon, t) = f(\omega, t) + \epsilon \frac{\partial f(s, t)}{\partial s} \Big|_{s=\omega} + o(\epsilon^2).$$

På nær led af højere orden end ϵ^1 gælder:

$$h = \epsilon \frac{\partial f(s, t)}{\partial s} \Big|_{s=\omega}.$$

Men heraf slutter vi, at

$$\frac{dg}{dt} = \lim_{h \rightarrow 0} \frac{[g(\omega + h) - g(\omega)]g(t)}{h} = \lim_{\epsilon \rightarrow 0} \frac{g(\omega + \epsilon) - g(\omega)}{\epsilon} \frac{g(t)}{\frac{\partial f(s, t)}{\partial s} \Big|_{s=\omega}}$$

eller

$$\frac{dg(t)}{dt} = Ig(t) \left[\frac{\partial f(s, t)}{\partial s} \right]_{s=\omega}^{-1}.$$

Definition: En Lie-gruppe (med r parametre) er en topologisk gruppe, hvis elementer afhænger kontinuert af r reelle, uafhængige parametre, således at visse krav er opfyldt:

Vi betegner gruppens elementer med g , parametrene med $\underline{s}$, $\underline{t}$, $\underline{u}$, osv., idet $\underline{s} = (s_1, s_2, \dots, s_r) \in \mathbb{R}^r$. Gruppemultiplikationen:

$$g(\underline{u}) = g(\underline{t})g(\underline{s}) \quad \text{oversættes da til} \quad \underline{u} = \underline{f}(\underline{t}, \underline{s}),$$

hvor $\underline{f}$ har r koordinatfunktioner $f_1, f_2, \dots, f_r$, der hver er analytiske i $\underline{t}$ og $\underline{s}$. Uden indskrænkninger kan vi tænke os, at parameterområdet i $\mathbb{R}^r$, som et definitionsområde for gruppen, er "normeret", således at $g(\underline{0}) = e$ (gruppens neutrale element), dvs.

$$\underline{s} = \underline{f}(\underline{0}, \underline{s}) = \underline{f}(\underline{s}, \underline{0}).$$

Den associative lov lægger følgende bånd på $\underline{f}$:

$$\underline{f}(\underline{u}, \underline{f}(\underline{t}, \underline{s})) = \underline{f}(\underline{f}(\underline{u}, \underline{t}), \underline{s}).$$

Og endelig vil vi betegne $[g(\underline{t})]^{-1}$ med $g(\underline{\bar{t}})$, således at

$$g(\underline{0}) = g(\underline{\bar{t}})g(\underline{t}) = g(\underline{t})g(\underline{\bar{t}}) \quad \text{og} \quad \underline{f}(\underline{\bar{t}}, \underline{t}) = \underline{f}(\underline{t}, \underline{\bar{t}}) = \underline{0}.$$

De hyppigst forekommende Lie-grupper er enten matrixgrupper (dvs. grupperne tillader en matrixrepræsentation) eller afbildningsgrupper [af afbildninger af m -dimensionale (topologiske) rum ind i n -dimensionale (topologiske) rum]. I det følgende vil vi kun betragte matrixgrupper. For kortheds skyld betegner vi matricerne som gruppenelementerne $\mathbf{g}(\underline{s})$ og de enkelte elementer i matricen $\mathbf{g}(\underline{s})$ betegner vi $g_{ij}(\underline{s})$. Hvis vi med $U(\underline{0})$ betegner en omegn af $\underline{0} \in \mathbb{R}^r$ og med $U(\mathbf{e})$ en omegn af det neutrale element i gruppen (altså enhedsmatricen), så er $\mathbf{g}(\underline{s})$ bijektive afbildninger af $U(\underline{0})$ ind i $U(\mathbf{e})$.

Ved rækkeudvikling af koordinatfunktionerne for $\underline{f}$ finder vi for den i te koordinat til parametervektoren $\underline{u}$:

$$\begin{aligned} u_i = f_i(\underline{t}, \underline{s}) &= f_i(\underline{0}, \underline{0}) + \sum_{\mu} t_{\mu} \frac{\partial f_i(\underline{t}, \underline{0})}{\partial t_{\mu}} \Big|_{\underline{t}=\underline{0}} + \sum_{\nu} s_{\nu} \frac{\partial f_i(\underline{0}, \underline{s})}{\partial s_{\nu}} \Big|_{\underline{s}=\underline{0}} + \dots \\ &= t_i + s_i + \sum_{\nu, \mu} a_{\nu\mu}^{(i)} s_{\nu} t_{\mu} + \epsilon^{(i)}, \end{aligned}$$

hvor

$$\epsilon^{(i)} \approx o(s_i^3, t_i^3) \quad \text{og} \quad a_{\nu\mu}^{(i)} = \frac{\partial^2 u_i}{\partial s_{\nu} \partial t_{\mu}} \Big|_{\underline{s}=\underline{t}=\underline{0}}.$$

Man ser, at op til led af 2. orden i s_{ν} , t_{μ} er gruppen kommutativ ("i første tilnærmelse"), og hvis gruppen er abelsk, så er $a_{\nu\mu}^{(i)} = a_{\mu\nu}^{(i)}$. Der indføres derfor et mål for gruppens afvigelse fra at være kommutativ ved de såkaldte *strukturkonstanter*:

$$c_{\nu\mu}^{(i)} = a_{\nu\mu}^{(i)} - a_{\mu\nu}^{(i)} \quad \text{med} \quad c_{\nu\mu}^{(i)} = -c_{\mu\nu}^{(i)}.$$

Desuden ser man, at

$$\bar{t}_i = -t_i + \sum_{\nu, \mu} a_{\nu\mu}^{(i)} t_{\nu} t_{\mu} + \epsilon^{(i)}.$$

Infinitesimale operatorer (eller transformationer) indføres nu ved

$$\mathbf{I}_k = \frac{\partial \mathbf{g}(\underline{s})}{\partial s_k} \Big|_{\underline{s}=\underline{0}} \quad (k = 1, 2, \dots, r).$$

$\mathbf{I}_k$ er således en matrix af samme type som $\mathbf{g}(\underline{s})$.

Hvis vi anvender $\mathbf{g}(\underline{s})$ på en vektor $\underline{v}$, som er uafhængig af $\underline{s}$

$$\underline{x} = \mathbf{g}(\underline{s})\underline{v}$$

så vil $\underline{x}$ afhænge af $\underline{s}$ og tilfredsstille visse differentialligninger. Først bemærker vi, at

$$\mathbf{g}(\underline{t})\underline{x} = \mathbf{g}(\underline{t})\mathbf{g}(\underline{s})\underline{v} = \mathbf{g}(\underline{u})\underline{v}$$

Ved differentiation mht. t_p og ved at sætte $\underline{t} = \underline{0}$ (dvs. $\underline{s} = \underline{u}$) får vi

$$\mathbf{I}_p \underline{x} = \sum_{j=1}^r \frac{\partial \mathbf{g}(\underline{u})\underline{v}}{\partial u_j} \Big|_{\underline{u}=\underline{s}} \frac{\partial u_j}{\partial t_p} \Big|_{\underline{t}=\underline{0}}$$

eller

$$\mathbf{I}_p \underline{x} = \sum_{j=1}^r \frac{\partial u_j}{\partial t_p} \Big|_{\underline{t}=\underline{0}} \frac{\partial \underline{x}}{\partial s_j}.$$

Denne kan løses mht.

$$(12.5) \quad \frac{\partial \underline{x}}{\partial s_j} = \sum_{p=1}^r \frac{\partial t_p}{\partial u_j} \Big|_{\underline{u}=\underline{s}} \mathbf{I}_p \underline{x}$$

med begyndelsesbetingelse $\underline{x}|_{\underline{s}=\underline{0}} = \underline{v}$.

Da de blandede afledede af 2. orden af $\underline{x}$ mht. s_p og s_q ikke afhænger af differentiationsordenen, er størrelserne $\mathbf{I}_p$ bundne til at tilfredsstille visse relationer: Ved indsættelse af $\partial^2 \underline{x} / \partial s_p \partial s_q = \partial^2 \underline{x} / \partial s_q \partial s_p$ finder man:

$$\frac{\partial \mathbf{I}_p \underline{x}}{\partial s_q} \Big|_{\underline{s}=\underline{0}} - \frac{\partial \mathbf{I}_q \underline{x}}{\partial s_p} \Big|_{\underline{s}=\underline{0}} = (\mathbf{I}_p \mathbf{I}_q - \mathbf{I}_q \mathbf{I}_p) \underline{v} = - \sum_{j=1}^r c_{pq}^{(j)} \mathbf{I}_j \underline{v}$$

for vilkårligt $\underline{v}$ og dermed

$$(12.6) \quad \mathbf{I}_p \mathbf{I}_q - \mathbf{I}_q \mathbf{I}_p = - \sum_{j=1}^r c_{pq}^{(j)} \mathbf{I}_j \quad (p, q = 1, 2, \dots, r)$$

Man kan vise, at (12.5) har én løsning; altså givet de infinitesimale operatorer $\mathbf{I}_p$ og koefficienterne $\partial t_p / \partial u_j|_{\underline{u}=\underline{s}}$ (som afledes af gruppeoperationerne), så findes der en éntydig bestemt afbildning $\mathbf{g}(\underline{s})$.

Mængden af infinitesimale operatorer for gruppen består af alle linearkombinationer af de oprindelige r operatorer $\mathbf{I}_p$. At $\mathbf{I}_1, \mathbf{I}_2, \dots, \mathbf{I}_r$ er lineært uafhængige følger af lineær uafhængighed af de r parametre $s_1, s_2, \dots, s_r$. — $\{\mathbf{I}_p \mid p = 1, 2, \dots, r\}$ udspænder derfor et vektorrum af dimension r . Selv om $\mathbf{I}_i$ kan operere på $\mathbf{I}_j$ vil resultatet ikke nødvendigvis tilhøre $\{\mathbf{I}_p\}$, men, som vi så ovenfor er det såkaldte Lie-produkt

$$[\mathbf{I}_p, \mathbf{I}_q] = \mathbf{I}_p \mathbf{I}_q - \mathbf{I}_q \mathbf{I}_p$$

en infinitesimal operator. Dette produkt er anti-kommutativt

$$[\mathbf{I}_p, \mathbf{I}_q] = -[\mathbf{I}_q, \mathbf{I}_p]$$

og opfylder *Jacobi identiteten*

$$[[\mathbf{I}_p, \mathbf{I}_q], \mathbf{I}_k] + [[\mathbf{I}_q, \mathbf{I}_k], \mathbf{I}_p] + [[\mathbf{I}_k, \mathbf{I}_p], \mathbf{I}_q] = 0;$$

denne algebra er derfor ikke-associativ.

$\mathcal{O}(3)$ -drejningsgruppen består af gruppen af drejninger om begyndelsespunktet i et 3-dimensionalt rum. Da disse kan repræsenteres ved egentlige ortogonale matricer, der har 9 elementer og disse udfylder 6 relationer, er drejningsgruppen afhængig af 3 parametre. Her kan man fx vælge de tre Euler-vinkler:

- 1) drejning om z -akse gennem vinkel α ($0 \leq \alpha < 2\pi$) $\Rightarrow y$ -akse $\mapsto y'$ -akse
- 2) drejning om y' -akse gennem vinkel β ($0 \leq \beta < \pi$) $\Rightarrow (z, z')$ -akse $\mapsto z''$ -akse
- 3) drejning om z'' -akse gennem vinkel γ ($0 \leq \gamma < \pi$).

Man kunne også repræsentere drejninger ved koordinaterne til drejningsvektoren $\underline{\phi} = (\phi_1, \phi_2, \phi_3)$, afsat fra begyndelsespunktet ud af drejningsaksen og proportional med drejningsvinklen, som fx vælges i intervallet $-\pi \leq |\underline{\phi}| < \pi$. Herved får vi én til én korrespondance mellem elementer i drejningsgruppen og punkterne i en kugle V med radius π .

Vi skal nu bestemme gruppens infinitesimale operatorer og dens strukturkonstanter. For at finde $\mathbf{I}_1$ sætter vi $\phi_2 = \phi_3 = 0$ og betragter drejningen

$$\mathbf{g}(\phi_1, 0, 0) : \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \phi_1 & -\sin \phi_1 \\ 0 & \sin \phi_1 & \cos \phi_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

og

$$\mathbf{I}_1 = \left. \frac{\partial \mathbf{g}}{\partial \phi_1} \right|_{\phi_1=0} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

Tilsvarende finder vi

$$\mathbf{I}_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix} \quad \mathbf{I}_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Derefter kan vi finde Lie-produkterne:

$$[\mathbf{I}_1, \mathbf{I}_2] = \mathbf{I}_3 \quad [\mathbf{I}_2, \mathbf{I}_3] = \mathbf{I}_1 \quad [\mathbf{I}_3, \mathbf{I}_1] = \mathbf{I}_2.$$

Heraf kan strukturkonstanterne aflæses. For eksempel er

$$c_{12}^{(1)} = c_{12}^{(2)} = 0 \quad \text{og} \quad c_{12}^{(3)} = -1.$$

I fysikken er det sædvanen i stedet for $\mathbf{I}_j$ at indføre matricer $\mathbf{A}_k$ fastlagt ved fx:

$$\mathbf{A}_1 = -\mathbf{I}_2 + i\mathbf{I}_1 \quad \mathbf{A}_2 = \mathbf{I}_2 + i\mathbf{I}_1 \quad \mathbf{A}_3 = i\mathbf{I}_3$$

og dermed ($\mathbf{A}_1 = \mathbf{L}_+$, $\mathbf{A}_2 = \mathbf{L}_-$ og $\mathbf{A}_3 = \mathbf{L}_z$)

$$[\mathbf{A}_3, \mathbf{A}_1] = \mathbf{A}_1 \quad [\mathbf{A}_3, \mathbf{A}_2] = -\mathbf{A}_2 \quad [\mathbf{A}_1, \mathbf{A}_2] = 2\mathbf{A}_3.$$

Andre valg af infinitesimale operatorer kommer på tale, fx infinitesimale drejninger om basisvektorer i et retvinklet koordinatsystem multipliceret med i . Herved fås hermiteske operatorer $\mathbf{L}_x, \mathbf{L}_y, \mathbf{L}_z$ med $[\mathbf{L}_x, \mathbf{L}_y] = i\mathbf{L}_z$, som anvendes inden for kvantemekanikken.

Opgaver

1. Hvor mange forskellige frembringere har en cyklisk gruppe af 6. orden?
2. Vis, at elementerne af endelig orden i en vilkårlig abelsk gruppe udgør en undergruppe.
3. Vis, at en gruppe af lige orden indeholder et ulige antal elementer af ordenen 2.
4. Et element a i en gruppe er af n te orden. Er a^{-1} og a^2 også af n te orden?
5. Om to elementer a og b i en endelig gruppe er det givet, at der findes to hele positive tal m og n , således at

$$ba = a^m b^n$$

Vis, at i dette tilfælde har $a^m b^{n-2}$, $a^{m-2} b^n$ og ab^{-1} samme orden.

6. Undersøg om følgende multiplikative grupper er cykliske:
 - a) 1, 2, 3, 4, 5, 6 modulo 7
 - b) 1, 3, 5, 7 modulo 8
 - c) 1, 2, 4, 5, 7, 8 modulo 9
7. I en gruppe G , som bl.a. indeholder elementerne a og b , skal man bevise, at elementerne ab og ba har samme orden.
8. I en gruppe G tænkes givet, at elementerne a , b , ab har ordenen 2. Vis, at $ab = ba$.
9. Udgør mængden af matricer af formen

$$\mathbf{M}(a) = \begin{pmatrix} a+1 & a \\ a & a+1 \end{pmatrix}$$

med sædvanlig matrixmultiplikation som kompositionsregel en gruppe?

Besvar samme spørgsmål om matricerne

$$\mathbf{M}(a) = \begin{pmatrix} 4a & 48a \\ a & 12a \end{pmatrix} \quad (a \neq 0)$$

10. Lad M betegne mængden af regulære matricer af orden n med matrixmultiplikation som kompositionsregel. Idet $a \in M$ betegner et fastholdt element skal man vise, at de $x \in M$, som kommuterer med a , udgør en gruppe.
11. Vis, at ethvert element i den alternerende gruppe A_n kan skrives som et produkt af 3-cykler af typerne (123) , (124) , $\dots$, $(12n)$.
12. Bestem konjugationsklasserne i A_4 .
13. Skriv følgende permutationer som produkt af disjunkte cykler:
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}$
 - $\begin{pmatrix} a & b & c & d & e & f \\ c & e & d & f & b & a \end{pmatrix}$
 - $(abc \cdots k)(al)$
 - $(a_1 a_2 \cdots a_r x y b_1 b_2 \cdots b_s)(a_r a_{r-1} \cdots a_1 x y c_1 c_2 \cdots c_t)$
 - $(a_1 a_2 \cdots a_r x y z b_1 b_2 \cdots b_s)(a_r a_{r-1} \cdots a_1 x y z c_1 c_2 \cdots c_t)$
- Angiv ordenen af permutationerne under a) og c).
14. Find antallet af konjugationsklasser i S_5 , og bestem deres typer og elementantal.
15. Givet følgende 3 elementer i S_9

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 8 & 3 & 6 & 2 & 1 & 5 & 4 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 5 & 6 & 3 & 4 & 1 & 7 & 8 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 5 & 6 & 3 & 2 & 1 & 7 & 8 \end{pmatrix}$$

Vis, at $a \sim c$, men $a \not\sim b$ og $b \not\sim c$.

Find en permutation t , således at $at = tc$.

Bestem typen af b og antallet af elementer i konjugationsklassen K_b .

Undersøg om K_a og K_b er indeholdt i A_9 .

Bestem ordenen af elementerne a , b og c .

16. Undersøg konjugationsklasserne i en cyklisk gruppe.
17. Lad G være en gruppe af regulære matricer med matrixmultiplikation som kompositionsregel. Vis, at sporet af forskellige matricer i samme konjugationsklasse er ens.
18. I S_4 finder man bl.a. konjugationsklasserne

$$K_e = \{e\} \quad \text{og} \quad K = \{(12)(34), (13)(24), (14)(23)\}$$

Vis, at foreningsmængden V af K_e og K udgør en invariant undergruppe i S_4 , og opstil dens Cayley-tavle.

Bestem sideklasserne til V , og vis, at gruppen $S_4|V$ er isomorf med S_3 .

19. Vis, at A_n er eneste undergruppe i S_n af index 2, når $n = 2, 3, 4$.
20. Lad G være en gruppe, og

$$\mathcal{C} = \{x \in G \mid xg = gx \text{ for alle } g \in G\}.$$
 Mængden $\mathcal{C}$ kaldes gruppens centrum. Vis, at $\mathcal{C}$ er en invariant undergruppe i G .
21. Bevis, at hvis centrum $\mathcal{C}$ for en gruppe G har index j , så har ethvert element i G højst j konjugerede elementer.
22. Lad $(G, \cdot)$ være en gruppe og v et fastholdt element i G . Mængden G forsynes med endnu en kompositionsregel $\circ$, der til ethvert ordnet par af elementer $a, b \in G$ knytter $a \circ b = v \cdot a \cdot b$.
 Vis, at $(G, \circ)$ er en gruppe, når og kun når v tilhører centrum $\mathcal{C}$ i gruppen $(G, \cdot)$ [det kan forudsættes bekendt, at $(\mathcal{C}, \cdot)$ er en undergruppe i $(G, \cdot)$, se opgave 20].
23. I gruppen $G = GL_n$ af regulære matricer (med komplekse elementer) af orden n med matrixmultiplikation som kompositionsregel skal N betegne mængden af matricer, hvis determinant har modulus 1; desuden skal $\mathbb{R}_+$ betegne den multiplikative gruppe af positive, reelle tal.
 Vis, at N er en normal undergruppe i G .
 Beskriv kvotientgruppen $G|N$ og vis, at $G|N$ er isomorf med $\mathbb{R}_+$.
24. Lad G være en cyklisk gruppe af orden 12 frembragt af elementet a , og H undergruppen frembragt af a^4 . Bestem den naturlige homomorfi af G på $G|H$. Bestem alle normale undergrupper i G .
25. Vis, at hvis G er en cyklisk gruppe og H undergruppe i G , så er H og $G|H$ begge cykliske.
26. Lad G være en cyklisk gruppe af orden 8. Find alle homomorfier af G ind i G . Hvilke af disse er isomorfier?
27. Vis, at relationen $\cong$, "isomorf med", er en ækvivalensrelation på mængden af alle endelige grupper.
28. Find centrum i S_2 (se opgave 20) og vis, at centrum i S_n er $\{e\}$ for $n \geq 3$.
29. Hvilke elementer i S_n kommuterer med alle elementer i S_n ?
30. Hvor mange elementer indeholder gruppen G af alle de drejninger, ved hvilke et givet kvadrat overføres i sig selv? Opstil en Cayley-tavle for gruppen.
 Vis, at de af elementerne i G , der er (egentlige) flytninger i kvadratets plan udgør en undergruppe i G .
 Er denne undergruppe invariant?

31. Vis, at mængden af afbildninger

$$f(x) = ax + b \quad (a \neq 0)$$

af de reelle tals mængde på sig selv udgør en gruppe, når sammensætning af afbildninger er kompositionsregel.

Vis, at denne gruppe ikke er kommutativ

Vis, at de specielle afbildninger, der fremkommer for $a = 1$, udgør en undergruppe i gruppen.

Vis, at denne undergruppe er en invariant undergruppe og beskriv dens faktorgruppe.

32. Nogle grupper har den egenskab, at det for ethvert element g gælder, at g og g^{-1} er konjugerede, dvs. ligger i samme klasse. Undersøg om følgende (punkt)grupper har den omtalte egenskab:

- Den cykliske gruppe C_n af drejninger om en akse ($n \geq 2$).
- Diedergruppen D_n ($n \geq 3$) af drejninger i rummet, der afbilder en regulær n -kant i sig selv.
- Tetraedergruppen T af drejninger i rummet, der afbilder et regulært tetraeder i sig selv.

33. Lad G være en endelig gruppe, $\mathbf{f}(G)$ en unitær repræsentation af G , og lad χ være den tilsvarende karakter, dvs.

$$\chi(g) = \text{spør } \mathbf{f}(g) \quad (g \in G).$$

Vis, at hvis g og g^{-1} er konjugerede, er $\chi(g)$ reel.

34. $ABC - A_1B_1C_1$ er et regulært tresidet prisme, dvs. endefladerne er ligesidede trekanter, og sidefladerne er vinkelrette på endefladerne. Med G betegnes gruppen af samtlige afstandsbevarende transformationer, der overfører prismet i sig selv.

Vis, at G har 12 elementer, hvoraf 6 er egentlige flytninger.

Angiv for ethvert element dets orden.

Er G kommutativ?

Bestem klasserne af konjugerede elementer.

Angiv antallet af ikke-ækvivalente irreducible repræsentationer af G , og bestem disse repræsentationers grader.

35. Lad G være en gruppe, og $\chi(g)$ en karakter svarende til en unitær repræsentation $\mathbf{f}(G)$ af n te grad. Vis, at

$$|\chi(g)| \leq n \quad \text{for alle } g \in G.$$

36. Lad G være en endelig gruppe, og $\chi(g)$ en karakter svarende til en eller anden repræsentation af G . Vis, at

$$\chi(g) = [\chi(g^{-1})]^* \quad \text{for alle } g \in G.$$

37. Vis, at tetraedergruppen T er isomorf med A_4 .
38. Konstruér en homomorfi af tetraedergruppen T på den cykliske gruppe C_3 .
39. Den cykliske gruppe C_{12} ønskes skrevet som et direkte produkt af to faktorer.
40. Vis, at for $n = 2, 3, 4$ har S_n netop to 1-dimensionale repræsentationer. (Benyt opgave 19).
41. Bestem centret $\mathcal{C}$, se opgave 20, i den multiplikative gruppe af alle regulære matricer af n te orden.
42. Der er givet mængden G af alle afbildninger af det komplekse n -dimensionale vektorrum V^n på sig selv, der er bestemt ved en lineær inhomogen substitution:

$$(1) \quad \underline{y} = \mathbf{A}\underline{x} + \underline{b},$$

hvor $\mathbf{A}$ er en vilkårlig, regulær matrix af n te orden med elementerne a_{ij} , og $\underline{b} = (b_1, b_2, \dots, b_n)$ er en vilkårlig n -dimensional vektor.

Vis, at denne mængde er en gruppe, når sammensætning af afbildninger tages som kompositionsregel.

Vis, at den afbildning, der til elementet i (1) fra G lader svare matricen:

$$\begin{pmatrix} \mathbf{A} & \underline{b} \\ \underline{0} & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & b_n \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

er en tro repræsentation af G .

43. Der er givet følgende afbildning $\mathbf{f}(C_4)$ af en cyklisk gruppe C_4 af orden 4, frembragt af elementet a :

$$\begin{aligned} \mathbf{f}(e) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \mathbf{f}(a) &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ \mathbf{f}(a^2) &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} & \mathbf{f}(a^3) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

Vis, at $\mathbf{f}(C_4)$ er en tro repræsentation af C_4

Angiv karakteren χ_f af elementerne i denne repræsentation og afgør om repræsentationen er unitær.

Vis, at repræsentationen er reducibel og opstil de forskellige irreducible repræsentationer for C_4 .

Find den regulære repræsentation af C_4 svarende til rækkefølgen e, a, a^2, a^3 af elementerne i C_4 .