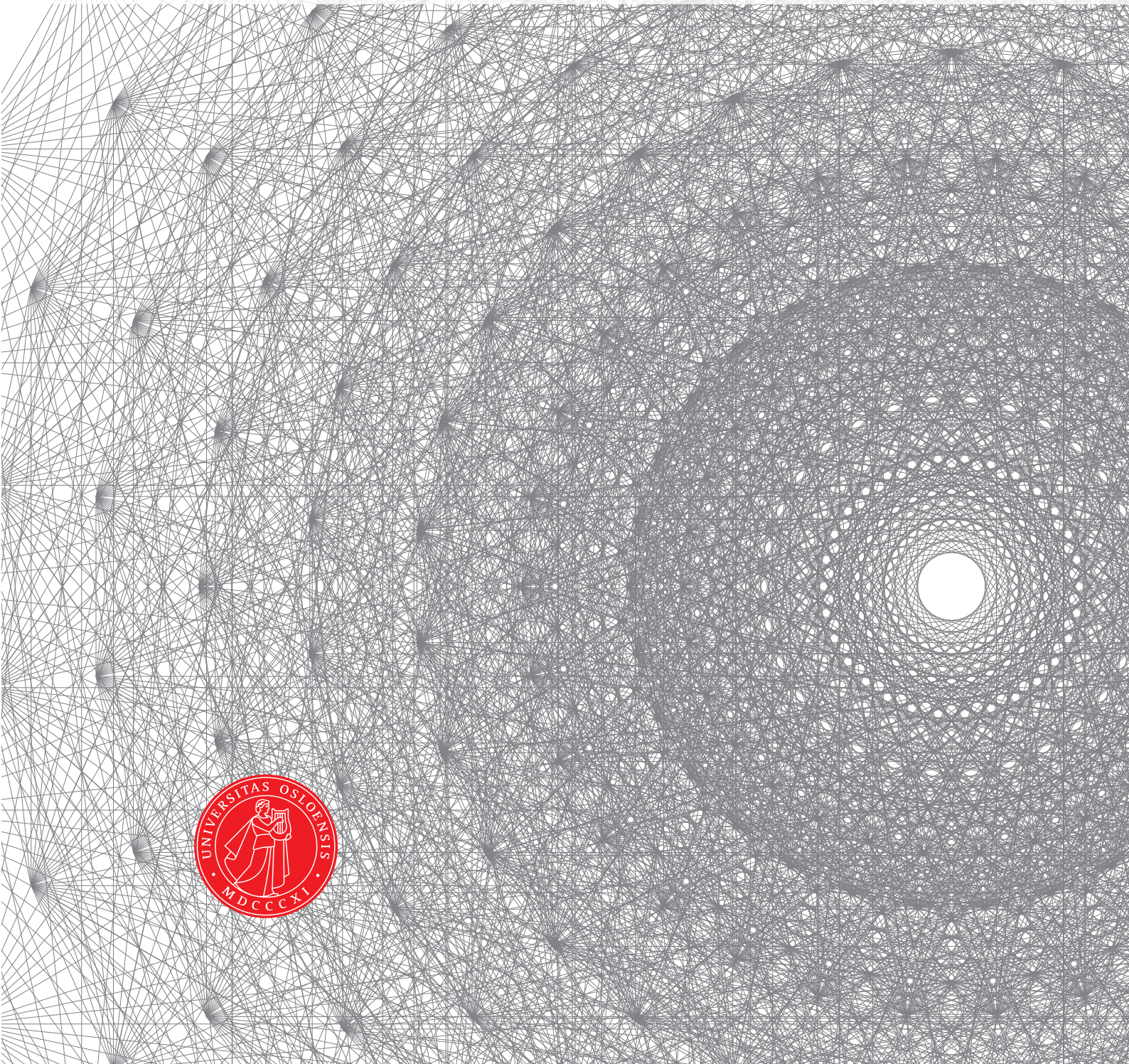
UiO : Matematisk institutt
Det matematisk-naturvitenskapelige fakultet

Representasjoner av den modulære gruppen

Joakim K. Haraldsen

Masteroppgave, våren 2019



Denne masteroppgaven er levert inn under masterprogrammet *Matematikk*, studieretning *Matematikk*, ved Matematisk institutt, Universitetet i Oslo. Oppgaven er normert til 60 studiepoeng.

Forsiden viser et utsnitt av rotsystemet til den eksepsjonelle liegruppen E_8, projisert ned i planet. Liegrupper ble oppfunnet av den norske matematikeren Sophus Lie (1842–1899) for å uttrykke symmetriene til differensiallikninger og spiller i dag en sentral rolle i flere deler av matematikken.

Innledning

Den modulære gruppen, ofte referert til ved bokstaven Γ, er generert av to elementer, det ene av orden 2 og det andre av orden 3. Det er ingen relasjoner mellom generatorene, og av den grunn er det svært enkelt å finne representasjoner av Γ.

Som forklart i oppgaven er det å gi en representasjon av Γ det samme som å gi en invertibel matrise og en "fordeling av multiplisiteter".

Som så ofte ellers i matematikken har man her noe som det er enkelt nok å gripe fatt i, men som likevel er noe stort og til dels uoversiktlig.

To grunnleggende begreper fo representasjonsteorien er "simpel" og "dimensjon". En representajon kan være simpel, og den har en dimensjon. Spesielt i høyere dimensjoner kan det være vanskelig finne de simple representasjonene. For den modulære gruppen har man god oversikt når dimensjonen er ≤ 5 (se for eksempel [3]), og i kapittel 6 gir vi en oversikt for dimensjon 2. Det gir oss anledning til å vise at det finnes ikke-isomorfe representasjoner med samme *karakter* Dette er ett eksempel på at representajonsteorien for uendelige grupper er mer komplisert enn for endelige. Et annet eksempel er at alle representasjoner av endelige grupper er *semisimple*. Den modulære gruppen byr på utfordringer (og muligheter) ved å ha representasjoner som *ikke* er semisimple.

Hovedfokuset i oppgaven er imidlertid de to nevnte komponentene som en representasjon av Γ består av, og hvordan disse relaterer seg til egenskaper ved representasjoner, slik som å være simpel eller semisimpel. I kapittel 4 viser vi et teorem som gjør oss i stand til å si at en representasjon ikke er simpel ved å kun se på fordelingen av multiplisiteter. I kapittel 3 beviser vi et resultat som plukker ut en klasse av semisimple representasjoner av Γ. Det viser seg at en representasjon er semisimpel dersom den invertible matrisen er unitær.

Innhold

1 Representasjonsteori **3**

2 Den modulære gruppen **8**

3 Eksempler **10**

4 Underrom stabilisert av én matrise **13**

5 Simple representasjoner og fordeling av multiplisiteter **16**

6 De 2-dimensjonale representasjonene av Γ **19**

7 Representasjoner av B_3 **24**

1 Representasjonsteori

1.1 En *representasjon* av en gruppe G er en homomorfi $G \to Aut(V)$, der V er et vektorrom. Vi skal begrense oss til endeligdimensjonale vektorrom over $\mathbb{C}$. Et valg av basis for $V \simeq \mathbb{C}^n$ og en homomorfi $G \to GL_n(\mathbb{C})$ bestemmer en representasjon av G. Vi kaller V for *representasjonsrommet*, og sier at representasjonen er n-dimensjonal.

En 1-dimensjonal representasjon av G er en homomorfi $G \to Aut(\mathbb{C}) \simeq \mathbb{C}^*$. For eksempel får man en 1-dimensjonal representasjon av en dihedral gruppe ved å sende rotasjonene på 1 og speilingene på -1.

En representasjon kan være injektiv (og for endelige grupper kan man alltid finne en injektiv representasjon), men som regel går informasjon tapt når man representerer. Til gjengjeld kan man gå løs på gruppen med alle de verktøy som lineæralgebraen tilbyr. En injektiv representajon kalles også *trofast*.

Ulike representasjoner kan svare til den samme homomorfien $G \to GL_n(\mathbb{C})$. Da er enten representasjonsrommene ulike, eller det er snakk om ulike basiser. De regnes imidlertid som *isomorfe*. For eksempel er alle *trivielle* representasjoner isomorfe så lenge dimensjonen er den samme. (Dette er representasjonene som sender alt på identiteten).

Jeg vil ofte la representasjonsrom og basis være uspesifisert og omtale en homomorfi $G \to GL_n(\mathbb{C})$ som en representasjon.

En representasjon av G tillegger hvert element $g \in G$ en lineærtransformasjon l_g. Man sier om et underrom $W \subseteq V$ at det *stabiliseres* av en representasjon $G \to Aut(V)$ dersom $l_g(W) \subseteq W$ for alle $g \in G$, og en representasjon kalles *simpel* dersom den bare stabiliserer 0 og V.

Man bruker også begrepet *irredusibel* om simple representasjoner. Her skal vi nøye oss med "simpel". Men en ikke-simpel representasjon vil jeg kalle *redusibel*.

Når jeg sier at en matrise $A \in M_n(\mathbb{C})$ stabiliserer et underrom $V \subseteq \mathbb{C}^n$, så mener jeg at $Av \in V$ for alle $v \in V$. En representasjon $\rho : G \to GL_n(\mathbb{C})$ er altså redusibel bare hvis det finnes et underrom $V \in \mathbb{C}^n$ som stabiliseres av alle matrisene i $\rho(G)$.

1.2 La oss finne de simple representasjonene av den symmetriske gruppen S_3. Av 1-dimensjonale har man den trivielle og den som sender rotasjonene på 1 og speilingene på -1. Alle 1-dimensjonale representasjoner er naturligvis simple.

Representasjonsteorien for endelige grupper har et resultat som går ut på at antall elementer i gruppen er lik kvadratsummen av dimensjonene til de ulike (opp til isomorfi) simple representasjonene. Det er klart at det ikke

finnes flere 1-dimensjonale enn de to nevnte, så vi er på utkikk etter en 2-dimensjonal representasjon.

Dersom man er gitt to vektorrom kan man lage et tredje ved direkte sum. Det samme gjelder for representasjoner. Man kunne tenke seg at det var mulig å lage den simple 2-dimensjonale representasjonen ved å sette den sammen fra 1-dimensjonale.

Først litt notasjon. En representasjon av $S_3 = \langle s, r \rangle$ er gitt ved to passende lineærtransformasjoner l_s og l_r. Etter et valg av basis for representasjonsrommet kan l_s og l_r identifiseres med hver sin matrise. Dersom matrisene er henholdsvis X og Y, betegner vi representasjonen ved (X, Y). Når jeg skriver (X, Y) uten å spesifisere representasjonsrom og basis, så tenker vi oss likevel at disse tingene foreligger, slik at det er én bestemt representasjon som betegnes.

La (X, Y) og (X', Y') være to representasjoner av S_3. De to blokk-matrisene nedenfor definerer da representasjonen $(X \oplus X', Y \oplus Y')$.

$$X \oplus X' = \begin{bmatrix} X & 0 \\ 0 & X' \end{bmatrix} \qquad\qquad Y \oplus Y' = \begin{bmatrix} Y & 0 \\ 0 & Y' \end{bmatrix}$$

På denne måten, enten det dreier seg om S_3 eller en annen gruppe, skaffer man seg en representasjon med representasjonsrom $W \oplus W'$ fra to representasjoner der den ene har representasjonsrom W og den andre W'. Man kaller den nye representasjonen en *direkte sum* av de gamle. En vanlig forenkling er å referere til representasjonene $G \to Aut(W)$ og $G \to Aut(W')$ som W og W', og den direkte summen av dem som $W \oplus W'$.

Opp til isomorfi er det tre 2-dimensjonale representasjoner av S_3 som er direkte summer av 1-dimensjonale. To av dem oppstår ved direkte sum av isomorfe representasjoner, og gir oss egentlig ingenting nytt. Men dersom

$$X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad\qquad Y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

så er (X, Y) en direkte sum av 1-dimensjonale uten å være *isotypisk*, dvs. uten å være en direkte sum av isomorfe representasjoner. Den er imidlertid ikke simpel. Representasjonen $W \oplus W'$ stabiliserer alltid underrommene $W \oplus 0$ og $0 \oplus W'$. Men de er en summer av simple, hvilket er å si at de er *semisimple*. Vi skal senere se (1.4) at representasjonene til endelige grupper alltid er semisimple.

Som nevnt kan man for endelige grupper alltid finne en trofast representasjon. Når det er snakk om dihedrale grupper, er det ikke vanskelig å finne en 2-dimensjonal injektiv representajon: symmetriene til en figur i planet er jo gitt ved matriser. Når det er flere enn to rotasjoner blant symmetriene,

den trivielle rotasjonen medregnet, står man overfor en simpel representasjon. (Til sammenligning vil symmetriene til en linje gjennom origo stabilisere ekte, ikke-trivielle underrom, nemlig linjen selv og dens ortogonale komplement). Dermed har S_3 en simpel representasjon $\rho = (X, Y)$, der

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad\qquad Y = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$$

Her og i resten av oppgaven er $\omega \neq 1$ en tredjerot av 1.

Sett nå at man er ute etter et rent algebraisk bevis for at denne 2-dimensjonale representasjonen er simpel. Det enkleste er da å se på egenvektorene til X og Y. Det er ingen felles egenvektorer, og dermed må ρ være simpel. Slik kan man alltid resonnere når det er snakk om 2-dimensjonale representasjoner. De direkte summene vi så på ovenfor er derimot gitt ved matriser som har alle egenvektorer til felles. (Det kunne ikke vært annerledes, for dersom matrisene hadde bare én linje av egenvektorer til felles ville man hatt en representasjon av en endelig gruppe som ikke er semisimpel).

Alternativt kan man vise at lineærtransformasjonen $\mathbb{C}[S_3] \to M_2(\mathbb{C})$ indusert av ρ er surjektiv. Her er $\mathbb{C}[S_3]$ grupperingen til S_3 over $\mathbb{C}$. Elementene ser slik ut:

$$\alpha + \beta s + \gamma r + \delta sr + \epsilon r^2 + \zeta sr^2$$

Koeffisientene $\alpha, \beta, \gamma, \delta, \epsilon, \zeta$ er komplekse tall. Elementene adderes og multipliseres som om de var polynomer, med det unntak at "variablene" s, r, rs, r^2, sr^2 multipliseres som i S_3. (Det bør nevnes at når man danner grupperingen til en uendelig gruppe er det vanlig å kreve at bare endelig mange koeffisienter er ulik 0). Det at lineærtransformasjonen $\mathbb{C}[S_3] \to M_2(\mathbb{C})$ er surjektiv er det samme som at alle matrisene i $M_2(\mathbb{C})$ er på formen

$$\alpha I + \beta X + \gamma Y + \delta XY + \epsilon Y^2 + \zeta XY^2 \qquad (*)$$

Det er enkelt å se hvordan man kan skrive A nedenfor som lineærkombinasjon av Y og I. En basis for $M_2(\mathbb{C})$ blir da

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad AX = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad XA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad I - A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

og det følger at alle matriser i $M_2(\mathbb{C})$ er på formen $(*)$. For å se at representasjonen dermed er simpel, anta at den stabiliserer et underrom $V \subseteq \mathbb{C}^2$ forskjellig fra 0 og $\mathbb{C}^2$, og at $v \in V$ er en vektor ulik 0. Velg en vektor $u \in \mathbb{C}^2$ som ikke ligger i V, og en matrise $M \in M_2(\mathbb{C})$ slik at $Mv = u$. Vi skriver M på formen $(*)$ og konkluderer (mot antagelsen) at representasjonen *ikke* stabiliserer V.

1.3 Representasjoner er mer enn representasjoner av grupper. En lineærtransformasjon $\mathbb{C}[G] \to End(V)$ er en representasjon av grupperingen $\mathbb{C}[G]$. Her er V fremdeles et endeligdimensjonalt vektorrom over $\mathbb{C}$, men også en $\mathbb{C}[G]$-modul. Når jeg snakker om en representasjon av en gruppering, vil jeg alltid mene en slik lineærtransformasjon. "Simpel representasjon" sammefaller nå med "simpel modul".

Det er klart at representasjoner av grupper og grupperinger er to sider av samme sak: Er man gitt det ene så er man gitt det andre, og en representasjon av G er simpel hvis og bare hvis den induserte representasjonen av $\mathbb{C}[G]$ er simpel.

Det hender at man kaller en representasjon av en gruppe G for en *modul* over G. Det klinger ikke så godt å si om en representasjon av G at den også er en representasjon av en annen gruppe, så i de tilfellene vil jeg si at man har en modul over G som også er en modul over en annen gruppe.

På slutten av forrige seksjon beviste vi i realiteten den ene retningen i en karakterisering av simple representasjoner:

Teorem 1 En representasjon av en gruppering $\mathbb{C}[G]$ er simpel hvis og bare hvis den er surjektiv.

Dette kalles Burnsides teorem. Vanligvis utleder man det fra mer generelle resultater, slik som Wedderburns teorem. Vårt bevis er derimot rett på sak. Det har likheter med beviset man finner i [1].

Bevis for Teorem 1. La R være bildet av representasjonen $\mathbb{C}[G] \to M_n(\mathbb{C})$, som vi antar er simpel. Da er R en underring av $M_n(\mathbb{C})$, og vår oppgave er å vise at $R = M_n(\mathbb{C})$. La og La $\mathfrak{a}_j$ være det venstresidede idealet i R som består av matrisene med bare nuller på de j første søylene, og sett $\mathfrak{a}_j(v) = \{Av : A \in \mathfrak{a}_j\}$, der $v \in \mathbb{C}^n$ og $e_1, e_2, ..., e_n$ er standardbasisen for $\mathbb{C}^n$. Da er $\mathfrak{a}_j(v)$ et underrom av $\mathbb{C}^n$ som stabiliseres av R (ikke bare av $\mathfrak{a}_j$). Spesielt har vi enten $\mathfrak{a}_j(e_{j+1}) = 0$ eller $\mathfrak{a}_j(e_{j+1}) = \mathbb{C}^n$ for $j < n$. Merk at hvis $\mathfrak{a}_j(e_{j+1}) = \mathbb{C}^n$ for $j = 0, 1, 2, ..., n-1$, så er $R = M_n(\mathbb{C})$. Foreløpig kan vi notere $\mathfrak{a}_0(e_1) = \mathbb{C}^n$, da $I \in R$.

La p_i være implikasjonen $Ae_i = A'e_i \Rightarrow Ae_{i+1} = A'e_{i+1}$, der A og A' er hvilke som helst matriser fra $\mathfrak{a}_{i-1}$. Sammen med en antagelse q_i om at $\mathfrak{a}_{i-1} = \mathbb{C}^n$ medfører p_i at vi kan definere en funksjon $f : \mathbb{C}^n \to \mathbb{C}^n$ ved $f(Ae_i) = Ae_{i+1}$, med A en hvilken som helst matrise fra R. Det er ikke vanskelig å se at f er lineær, slik at den har en egenvektor v med egenverdi λ. Det følger at hvis $Ae_i = v$, så er $Ae_{i+1} = \lambda v$. Dette skal vi nå vise at er umulig gitt at q_i er sann.

La $W_i = \{A(\lambda e_i - e_{i+1}) : A \in \mathfrak{a}_{i-1}\}$. Da er W_i et underrom av $\mathbb{C}^n$ som stabiliseres av R, slik at vi står mellom $W = 0$ og $W = \mathbb{C}^n$. Ettersom q_i er sann finnes det en matrise $A \in \mathfrak{a}_{i-1}$ slik at $A(e_i) \neq 0$. Ulike skaleringer av A viser at $W_i \neq 0$, og det kan konkluderes at $W = \mathbb{C}^n$. Antagelsen om at p_i er sann gjør det mulig å definere en funksjon $g : \mathbb{C}^n \to \mathbb{C}^n$ ved $g(Ae_i) = A(\lambda e_i - e_{i+1}) = \lambda Ae_i - f(Ae_i)$. Den er surjektiv som følge av at $W = \mathbb{C}^n$, og lineær. Dermed må kjernen til g være triviell. Men dette kommer i konflikt med at $g(v) = 0$, der v er den nevnte egenvektoren til f. Konklusjonen er at p_i er usann.

Anta nå at q_i er sann for for $i < k$. Det betyr at vi kan finne en matrise i R der de i første søylene er valgt helt fritt blant vektorene i $\mathbb{C}^n$. Vi har nettopp vist at q_{k-1} utelukker p_k, og dermed følger q_{i+1} fra antagelsen om at q_i er sann for $i < k$. Vi har allerede q_1, og dermed er teoremet bevist. □

Merk at vi brukte den algebraiske lukketheten til $\mathbb{C}$ der hvor vi antok at f har en egenvektor. En linærtransformasjon $\rho : \mathbb{R}[G] \to M_n(\mathbb{R})$ kan gjøre $\mathbb{R}^n$ til en simpel $\mathbb{R}[G]$-modul uten å være surjektiv. La for eksempel G være $\mathbb{Z}$ og $\rho(1)$ være en (invertibel) matrise uten reelle egenverdier.

Teoremet forteller oss at når en representasjonen ikke er surjektiv, så finnes det et stabilisert underrom. Man kunne ønsket seg et bevis som fortalte oss hvordan vi finner et slikt underrom i hvert enkelt tilfelle. Beviset i [1] gir ingen informasjon om dette. Beviset ovenfor er imidlertid laget i den hensikt å få ut litt informasjon: La $\rho : G \to GL_n(\mathbb{C})$ være en redusibel representasjon av G. Da er $\rho(G)$-banen til enten en av e_i-ene eller en vektor på formen $\lambda e_i - e_{i+1}$ et ekte, ikke-trivielt stabilisert underrom. Dette er ganske tynn informasjon da vi ikke vet noe om λ, men vi skal se (5.3) at den lar seg anvende.

Det er en umiddelbar konsekvens av teoremet at hvis g er i senteret til G, så vil en simpel representasjon tilegge g en matrise i senteret til $M_n(\mathbb{C})$, med andre ord en skalering av identiteten. Dette medfører at de simple representasjonene av abelske grupper er svært enkle å beskrive: De er alltid 1-dimensjonale!

1.4 Det er mer å si om redusible representasjoner enn at de ikke er simple. Vi har vært inne på begreper som *semisimpel* og *isotypisk* tidligere, og vi skal se på flere begreper i kapittel 3. Dersom alle redusible representasjoner av en gruppe er en direkte sum av representasjoner av lavere dimensjon, så er de semisimple, og omvendt. Representasjonsteorien for endelige grupper har nytt godt av følgende faktum:

Teorem 2 Representasjoner av endelige grupper er semisimple.

Bevis. Hvis et skalarprodukt $V \times V \to \mathbb{C}$ bevares av en lineærtransformasjon $l : V \to V$, så vil $l(W) \subseteq W$ implisere $l(W^\perp) \subseteq W^\perp$. Det betyr at hvis man finner et skalarprodukt som bevares av l_g for alle $g \in G$, så er teoremet bevist. Dersom $(u|v)$ er et vilkårlig skalarprodukt for V, så kan man definere et skalarprodukt med den ønskede egenskapen slik:

$$(u|v)' = \sum_{g \in G} (l_g(u)|l_g(v))$$

Definisjonen gir mening ettersom G er endelig. □

Bemerkning. Beviset er hentet fra [2]. I denne boken skisseres det også hvordan man etablerer et mer generelt resultat, nemlig at representasjoner av *kompakte* grupper er semisimple.

2 Den modulære gruppen

La $\mathbb{H}$ være det øvre komplekse halvplanet. Heltall a, b, c, d som tilfredsstiller $ad - bc = 1$ definerer en bijektiv funksjon $\mathbb{H} \to \mathbb{H}$ ved

$$z \mapsto \frac{az + b}{cz + d}$$

Mengden av slike funksjoner er lukket under sammensetning. Gruppen som dannes betegnes ved Γ og kalles *den modulære gruppen.*

La $\varphi : SL_2(\mathbb{Z}) \to \Gamma$ være funksjonen som sender matrisen $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ på elementet i Γ som er gitt ved a, b, c, d. Enkel regning viser at φ er en surjektiv homomorfi med kjerne $\{\pm I\}$, slik at $\Gamma \simeq PSL_2(\mathbb{Z})$.

En annen isomorfi, som får den modulære gruppen til å virke enkel og oversiktlig, er $\Gamma \simeq \mathbb{Z}_2 * \mathbb{Z}_3$. Vi skal gi et bevis, og som et første skritt i den retning skal vi se at $PSL_2(\mathbb{Z})$ er generert av S og T, der

$$S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad\qquad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Vi tar utgangspunkt i en vilkårlig matrise $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in PSL_2(\mathbb{Z})$. Takket være at determinanten er 1 og at a, b, c, d er heltall, er det en enkel sak å vise at $M \in \langle S, T \rangle$ dersom $a = 0$ eller $c = 0$. Så anta at både a og c er ulik 0. Ettersom $M = -M$ kan vi dessuten anta at $c > 0$. Endelig er $T^n M$ for passende n på formen $\left[\begin{smallmatrix} \zeta & * \\ c & * \end{smallmatrix}\right]$, med ζ et eller annet heltall større enn c, slik at vi kan anta $a > c$.

Matrisen $\left[\begin{smallmatrix} \alpha & \alpha\beta-1 \\ 1 & \beta \end{smallmatrix}\right]$ kan skrives $T^\alpha S T^\beta$, der $\alpha, \beta \in \mathbb{Z}$. Dette viser at dersom en matrise i $PSL_2(\mathbb{Z})$ har en 1-er i hjørnet nederst til venstre, så befinner den seg i $\langle S, T\rangle$. Nå fokuserer vi på søylen $v = \left[\begin{smallmatrix} \alpha \\ 1 \end{smallmatrix}\right]$. Ideen er å finne en matrise $A \in \langle S, T\rangle$ slik at $Av = \pm\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$. I så fall har $A^{-1}M$ en 1-er i hjørnet nederst til venstre, og vi kan konkludere at $M \in \langle S, T\rangle$.

For å finne en matrise $A \in \langle S, T\rangle$ med den ønskede egenskapen, ta i betraktning at hvis r_1 og r_2 er relative primtall, med $r_1 > r_2 > 0$, så er ligningene fra Euklids algoritme som følger:

$$\begin{aligned} r_1 &= q_1 r_2 + r_3 \\ r_2 &= q_2 r_3 + r_4 \\ &\vdots \\ r_n &= q_n r_{n+1} + 1 \end{aligned}$$

Dersom $A(r_1, r_2) = (T^{(-1)^n q_1} S)(T^{(-1)^{n-1} q_2} S)...(T^{q_{n-1}} S)(T^{-q_n} S)$, så er

$$A(r_1, r_2) \begin{bmatrix} r_{n+1} \\ 1 \end{bmatrix} = \pm \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}$$

Ved å sette $\alpha = r_{n+1}$ og observere at a og c er relative primtall (som følge av at determinanten til M er 1), finner vi en matrise med den ønskede egenskapen, nemlig $A(c, a)$.

Ettersom $PSL_2(\mathbb{Z}) = \langle S, T\rangle = \langle S, ST\rangle$, og $(ST)^3 = I$, er den modulære gruppen generert av to elementer, det ene av orden 2 og det andre av orden 3. En representasjon er altså gitt ved to matriser X og Y som tilfredsstiller $X^2 = Y^3 = I$ og som respekterer eventuelle relasjoner mellom de to generatorene. Teoremet nedenfor påstår at det ikke finnes noen slike relasjoner.

Teorem 3 Den modulære gruppen er isomorf med det frie produktet $\mathbb{Z}_2 * \mathbb{Z}_3$

Bevis. Anta at vi har et produkt av S-er og T-er, der alle forekomster av SS og $STSTST$ er blitt fjernet. Vi skal vise at dette produktet ikke kan settes lik I. Det er i så fall ingen relasjoner mellom S og ST, og teoremet er bevist.

Dersom produktet settes lik I, får vi (etter konjugering med S på begge sider av likhetstegnet dersom det trengs) den ene eller den andre av disse to ligningene:

$$(T^{\alpha_1} S)(T^{\alpha_2} S)...(T^{\alpha_m} S) = I \qquad \text{(i)}$$

$$S(T^{\alpha_1} S)(T^{\alpha_2} S)...(T^{\alpha_m} S) = I \qquad \text{(ii)}$$

Her er $\alpha_1, \alpha_2, ..., \alpha_m$ passende heltall.

Vi kan sette inn $T^{-1}ST^{-1}ST^{-1}S$ (som er lik I) hvor som helst i ligningen. Ved å sette det inn på plassen til høyre for hver forekomst av T^{α_i}, der i er et partall, og deretter fjerne faktorer som kansellerer hverandre, endrer (i) og (ii) form til henholdsvis (iii) og (iv) nedenfor. (Dette forutsetter at alle forekomster av STSTST er fjernet, slik at man for ingen i har både $\alpha_i = 1$ og $\alpha_{i+1} = 1$).

$$A(r_1, r_2) = I \tag{iii}$$
$$SA(r_1, r_2) = I \tag{iv}$$

Dette identifiserer r_1 med enten r_{n+1} eller -1, begge deler umulig. □

Algebraiske bevis for at $PSL_2(\mathbb{Z})$ er generert av S og T vil som regel ligne på det som ble gitt ovenfor. Det finnes også geometriske bevis, som utnytter at elementene i Γ er Möbiustransformasjoner. Vi hadde ikke behøvd å formulere relasjonen mellom Euklids algoritme og produkter av S og T så eksplisitt som vi gjorde, men det lot oss bevise $\Gamma \simeq \mathbb{Z}_2 * \mathbb{Z}_3$ uten å gå via et såkalt pingpong-lemma.

3 Eksempler

3.1 Representasjonene av S_3 svarer til representasjoner av Γ. Begge grupper er generert av et element av orden 2 og et element av orden 3, men er forskjellige ved at generatorene til S_3 står i en relasjon. Man kan skrive grupperingene slik:

$$\mathbb{C}[\Gamma] \simeq \frac{\mathbb{C}\langle x, y\rangle}{(x^2, y^3)} \qquad\qquad \mathbb{C}[S_3] \simeq \frac{\mathbb{C}\langle x, y\rangle}{(x^2, y^3, xyx - y^2)}$$

Her er $\mathbb{C}\langle x, y\rangle$ en ikke-kommutativ polynomring (dvs. variablene kommuterer ikke). Når I er et tosidig ideal i en ring R vil enhver R/I-modul også være en R-modul, og simple R/I-moduler er simple R-moduler. Vi har dermed allerede sett eksempler på simple og semisimple representasjoner av den modulære gruppen. I dette kapittelet skal vi se på noen andre typer simple og semisimple representasjoner, og møte vår første representasjon som er *hverken* simpel eller semisimpel.

Vi bruker (X, Y) som betegnelse på en representasjon av Γ, i analogi med notasjonen fra (1.2).

3.2 Ved å bruke at en matrise og dens Jordanform J er røtter til de samme polynomene, og at $J^n = I$ impliserer at J er diagonal, kan man fastslå at X og Y er diagonaliserbare. Dette betyr at når vi er gitt en representasjon (X, Y) av den modulære gruppen, så kan enten X eller Y antas å være diagonal, dvs. vi antar at det ble gjort et "lurt" valg av basis for representasjonsrommet.

Dersom v er en egenvektor for Y med egenverdi λ, vil $\lambda^3 v = Y^3 v = v$, så λ må være en tredjerot av 1. På samme måte viser man at X sine egenverdier er 1 eller -1.

For å spesifisere en representasjon av den modulære gruppen trengs med andre ord en håndfull kvadratrøtter og tredjerøtter av 1, samt en inverterbar matrise P. Nærmere bestemt lager vi en diagonalmatrise Y med tredjerøtter på diagonalen, og en diagonalmatrise D med kvadratrøtter på diagonalen, og setter $X = PDP^{-1}$. Da er $X^2 = Y^3 = I$, og vi får en representasjon (X, Y). Her er for eksempel en 3-dimensjonal representasjon:

$$X = P \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} P^{-1} \qquad\qquad Y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$$

Merk at søylene i P er egenvektorer til X.

Dersom man endrer rekkefølgen på D sine diagonalelementer, vil en korresponderende endring av rekkefølgen på søylene til P resultere i samme X. Og en endring av rekkefølgen på Y sine diagonalelementer svarer til en konjugasjon. Man går altså ikke glipp av noen representasjoner dersom man insisterer på at diagonalelementene har en bestemt rekkefølge. Så dersom man er enige om en bestemt rekkefølge (for eksempel i D sitt tilfelle at 1-erne står på de øverste radene), vil enhver representasjonene av Γ være gitt ved en invertibel matrise og en "fordeling av multiplisiteter". Det sistnevnte oppgir hvor mange forekomster av 1 og -1 man finner på diagonalen til D, og hvor mange forekomster av 1, ω og ω^2 man finner på diagonalen til Y.

3.3 Dersom P i den 3-dimensjonale representasjonen ovenfor er ortogonal, er X speilingen om planet spent opp av de to første søylene i P. Man kaller X en *Householder*-matrise. I det generelle tilfellet, dvs. for en hvilken som helst dimensjon, er Householder-matrisene speilingene om et eller annet hyperplan. Multiplisiteten til -1 er med andre ord alltid 1.

Vi skal senere (4.4) bevise at hvis X er Hermitisk og Y er diagonal, så er (X, Y) semisimpel. Som en forsmak tar vi for oss spesialtilfellet der X er en 3×3 Householder-matrise og Y har tre ulike elementer på diagonalen.

Det første å observere er at Y stabiliserer de tre akseplanene, da disse spennes opp av egenvektorer til Y. For å vise at dette er alle 2-dimensjonale

underrom av $\mathbb{C}^3$ stabilisert av Y, anta at V er et moteksempel. Da snitter V et akseplan i en linje gjennom origo som *ikke* er en av aksene. En matrise (eller en representasjon, for den saks skyld) stabiliserer alltid snittet av to rom som den stabiliserer. Ettersom aksene er samtlige av Y sine egenrom, får vi den umuligheten at Y stabiliserer en linje som ikke er spent opp av en egenvektor. Vi står derfor igjen med at aksene og akseplanene er de eneste ekte, ikke-trivielle underrommene stabilisert av Y.

Det er klart at X på sin side stabiliserer planet det speiles om og linjen spent opp av en normalvektor til planet. Så (X, Y) er redusibel dersom normalvektoren spenner opp en av aksene. I dette tilfellet stabiliserer X alle aksene, og vi kan fastslå at (X, Y) er en direkte sum av 1-dimensjonale representasjoner. Det er også en mulighet at normalvektoren ligger i et av akseplanene *uten* å spenne opp en akse. La oss si at det er xz-planet. Da finnes det en vektor i planet det speiles om (altså en egenvektor til X) som sammen med normalvektoren spenner opp xy-planet. Dermed stabiliseres xy-planet av (X, Y), slik at representasjonen er redusibel. Også z-aksen stabiliseres, så (X, Y) er en direkte sum av to representasjoner av lavere dimensjon. Imidlertid definerer (X, Y) en *simpel* representasjon inn i automorfiene av xy-planet: Det er ingen linjer i dette planet som stabiliseres av både X og Y. Endelig får man simple representasjoner dersom normalvektoren ikke ligger i noen av akseplanene.

3.4 I likhet med de 3-dimensjonale ikke-simple representasjonene som vi nettopp beskrev, er de ikke-simple representasjonene av S_3 direkte summer av representasjoner av lavere dimensjon. En representasjon med denne egenskapen kalles *dekomposabel*. En representasjon som ikke er dekomposabel kalles *indekomposabel*. Begrepene simpel og indekomposabel sammenfaller for endelige grupper, jf. (1.4). Merk at en representasjon kan være dekomposabel uten å være semisimpel, og semisimpel uten å være dekomposabel (dersom den er simpel).

La oss se om vi kan "modifisere" de 3-dimensjonale representasjonene vi diskuterte ovenfor på en måte som gir oss redusible indekomposable representasjoner. Anta at $X = PDP^{-1}$ er en speiling om xy-planet, og at Y er en diagonalmatrise med tre ulike elementer på diagonalen. Vi kan (dermed) anta at P er ortogonal, og finner enhetsvektoren e_3 som en av søylene til P. Erstatt denne med en vektor som hverken ligger i xy-planet eller på z-aksen. Etter denne endringen av X finnes det ikke lenger en linje utenfor xy-planet som stabiliseres av både X og Y, og (X, Y) er redusibel og indekomposabel. Den er dermed et eksempel på en representasjon som er hverken simpel eller semisimpel.

4 Underrom stabilisert av én matrise

4.1 I forrige kapittel så vi at en 3×3 diagonalmatrise med ulike elementer på diagonalen stabiliserer bare 0 og de rommene som spennes opp av egenvektorer. Dette kan generaliseres.

Teorem 4 Dersom $A \in M_n(\mathbb{C})$ stabiliserer $V \subseteq \mathbb{C}^n$, og $V \neq 0$, så har V en basis av generaliserte egenvektorer til A.

La J være Jordanformen til A. Dersom P er en matrise med den egenskapen at $A = PJP^{-1}$, så er søylene til P generaliserte egenvektorer. (Dette kan tenkes på som en foeløpig definisjon av begrepet *generalisert egenvektor*). Dersom A er diagonaliserbar, slik at J er diagonal, så vil alle generaliserte egenvektorer være vanlige egenvektorer. Før vi går i gang med beviset for teoremet ser vi på et eksempel der A *ikke* er diagonaliserbar.

$$J = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix} \quad P = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} \vdots & \vdots & \vdots \\ u & v_1 & v_2 \\ \vdots & \vdots & \vdots \end{bmatrix} \quad A = \begin{bmatrix} 3 & 2 & -2 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Vi ser at J består av to Jordan-blokker, den ene 1×1 og den andre 2×2. Tilhørende den førstnevnte har man den vanlige egenvektoren u, og tilhørende den sistnevnte har man den vanlige egenvektoren v_1 og den generaliserte egenvektoren v_2. Vi ser at $Av_2 = 2v_2 + v_1$, og dette illustrerer hvordan to nabo-søyler tilhørende samme Jordan-blokk alltid forholder seg til hverandre.

Definisjon En vektor $v \in \mathbb{C}^n$ er en *generalisert egenvektor* til $A \in M_n(\mathbb{C})$ med egenverdi λ dersom $v \neq 0$ og $(A - \lambda I)^r v = 0$ for en $r > 0$.

I beviset nedenfor tar vi i bruk følgende faktum: Dersom $As = \lambda s + t$, der $A \in M_n(\mathbb{C})$ er en vilkårlig matrise og t er en generalisert egenvektor for A med λ som egenverdi, så er s en generaliserte egenvektor for A. Dette er en umiddelbar konsekvens av definisjonen.

Bevis for teorem 4. Sett at A og en matrise $C \in M_n(\mathbb{C})$ er similære, dvs. det finnes en $B \in GL_n(\mathbb{C})$ slik at $C = BAB^{-1}$. Dersom $v_1, v_2, ..., v_m$ er en basis for V, og A stabiliserer V, så er $Bv_1, Bv_2, ..., Bv_m$ en basis for et rom stabilisert av C. Man har nemlig for $i = 1, 2, ..., m$ at

$$CBv_i = (BAB^{-1})(Bv_i) = BAv_i$$

og at Av_i kan skrives som en lineærkombinasjon av $v_1, v_2, ..., v_m$ (ettersom A stabiliserer V).

Videre er $B^{-1}u$ en generalisert egenvektor for A dersom u er det for C. For dersom J er Jordanformen til C (og dermed også til A), og man har en invertibel matrise Q slik at $C = QJQ^{-1}$, så kan vi skrive $A = B^{-1}QJ(B^{-1}Q)^{-1}$.

Betraktningene i de to foregående avsnittene gjelder spesielt når C er Jordanformen til A. Det holder derfor å vise teoremet for de tilfellene hvor A er på Jordanform.

La søylene i en $n \times m$-matrise M være en basis $v_1, v_2, ..., v_m$ for V. Etter søyleoperasjoner får man en matrise M' på redusert trappeform. Da finnes det m rader som har 1 ett sted og 0 alle andre steder, og de har 1-erne på ulike steder. De befinner seg på rad nummer $r_1, r_2, ...r_m$. Ettersom søylerom bevares av søyleoperasjoner, vil søylene til M' være en basis for V. La søylene være $u_1, u_2, ..., u_m$, der u_i har en 1-er på rad r_i og en 0 på rad r_j $(j \neq i)$. Ettersom M' har den formen den har, og A er på Jordanform og stabiliserer V, ser vi at $Au_i = \lambda u + \alpha u_{i-1}$, der λ er diagonalelementet i A som befinner seg på rad nummer r_i , og α er tallet man finner over dette diagonalelementet, altså enten 1 eller 0. (Vi kan ignorere u_{i-1} for $i = 1$, eller sette den lik 0, da u_1 nødvendigvis er en vanlig egenvektor). Grunnen til at u_i og u_{i-1} er de eneste M'-søylene som er med i lineærkombinasjonen som uttrykker Au_i, er at Au_i er 0 på rad r_j $(j \neq i)$, med mulig unntak av r_{i-1}. Ettersom u_1 må være en egenvektor, følger det av faktumet nevnt i forkant av beviset at også $u_2, u_3, ..., u_m$ er generaliserte egenvektorer. □

4.2 La oss finne underrommene stabilisert av matrisen $A = PJP^{-1}$ som ble diskutert i begynnelsen av kapittelet. Ettersom de to egenrommene til A er 1-dimensjonale, finnes det bare ett 2-dimensjonalt underrom som er spent opp av vanlige egenvektorer. Man kunne tenke seg at det likevel fantes uendelig mange 2-dimensjonale underrom som stabiliseres, ettersom det finnes uendelig mange rom på formen $Span\{u, \alpha v_1 + \beta v_2\}$. Her er $\alpha v_1 + \beta v_2$ en generalisert egenvektor som følge av at v_1 og v_2 er generaliserte egenvektorer tilhørende samme Jordan-blokk. Saken er imidlertid den at siden $Av_2 = 2v_2 + v_1$, så ligger ikke v_2 i et underrom stabilisert av A uten at også v_1 ligger der; og det samme gjelder for alle de andre ikke-vanlige generaliserte egenvektorene i $Span\{v_1, v_2\}$, da de er relatert til v_1 på akkurat samme måte. Til gjengjeld er det klart at det såkalte generaliserte egenrommet $Span\{v_1, v_2\}$ stabiliseres av A. Alt i alt er det bare seks underrom som stabiliseres av A, nemlig $0, \mathbb{C}^3, Span\{u, v_1\}, Span\{v_1, v_2\}$ og to 1-dimensjonale. Merk at dette antallet, og hvordan det er fordelt på de ulike dimensjonene, er noe som kan leses ut av Jordanformen til A.

4.3 La J være Jordanformen til en matrise A. I denne seksjonen er P_A en matrise med den egenskapen at $A = P_A J P_A^{-1}$, og s er en søyle i P_A. La $K(s)$ være rommet spent opp av s og alle søylene til venstre for s tilhørende samme Jordanblokk som s, og la $K'(s)$ være rommet spent opp av alle de andre søylene. Med matrisene diskutert tidligere (4.1) er for eksempel $K(v_2) = Span\{v_1, v_2\}$. Her er et par enkle observasjoner om slike rom:

(*i*) Hvis $s \in V$ og A stabiliserer V, så er $K(s) \subseteq V$.

(*ii*) A stabiliserer $K(s)$ og $K'(s)$.

Vi kan bruke teorem 4 og disse observasjonene til å bevise en karakterisering av de indekomposable representasjonene av den uendelige sykliske gruppen $\mathbb{Z}$. En representasjon av $\mathbb{Z}$ er gitt ved en invertibel matrise A og et valg av basis for representasjonsrommet. Ettersom A vil ha minst én egenvektor, er de simple representasjonene de 1-dimensjonale. Hvilke representasjoner som er indekomposable er mindre opplagt.

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

Jordanformen til en 5×5 matrise med bare én linje av egenvektorer.

Teorem 5 En representasjon av $\mathbb{Z}$ er indekomposabel hvis og bare hvis den stabiliserer kun én linje.

Bevis. For å vise "bare hvis"-retningen, anta at representasjonen er gitt ved matrisen $A \in GL_n(\mathbb{C})$ (og en eller annen basis for representasjonsrommet), og at A har minst to ulike linjer av egenvektorer. Da kan man lage en matrise P_A der det blant søylene finnes to vanlige egenvektorer. La t være den siste søylen i P_A. Da er $K(t)$ og $K'(t)$ begge ikke-trivielle, og teoremet følger av observasjon (ii) og det faktum at $K(s) \oplus k'(s) = \mathbb{C}^n$.

For å vise den andre retningen, anta at representasjonen er gitt ved en matrise A som har kun én linje av egenvektorer. Dersom t igjen er den siste søylen i en matrise P_A, så er $K(t)$ det eneste rommet av typen $K(s)$. I lys

av teorem 4 og observasjon (i) kan vi slå fast at det må dreie seg om en indekomposabel representasjon. □

4.4 La $H \in GL_n(\mathbb{C})$ være en Hermitisk matrise. Da er $V \subseteq \mathbb{C}^n$ spent opp av egenvektorer til H bare hvis det samme kan sies om det ortogonale komplementet $V^{\perp}$. (Dette er fordi H kan diagonaliseres via en unitær matrise). Teorem 4 medfører dermed at H stabiliserer et underrom bare hvis det ortogonale komplementet også stabiliseres.

Teorem 6 La (X, Y) være en representasjon av den modulære gruppen. Hvis X er en Hermitisk matrise og Y en diagonalmatrise, så er (X, Y) semisimpel.

Bevis. Det er en enkel konsekvens av betraktningene ovenfor at hvis X og Y er som beskrevet, så er (X, Y) dekomposabel. Det holder derfor å påpeke at blokk-matrisen $A \oplus B$ er Hermitisk bare hvis A og B er Hermitisk, og diagonal bare hvis A og B er diagonal.

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

□

I kapittel 3 så vi på de 3-dimensjonale representasjonene der X er en Householder-matrise og Y er diagonal med tre ulike elementer på diagonalen, og fant ut at slike representasjoner er semisimple. Teorem 6 generaliserer dette resultatet.

5 Simple representasjoner og fordeling av multiplisiteter

5.1 Vi har tidligere beskrevet de simple 3-dimensjonale representasjonene av den modulære gruppen for de tilfellene hvor X er en Householder-matrise og Y er diagonal med tre ulike elementer på diagonalen. Dersom elementene *ikke* er ulike, eller dimensjonen er høyere enn 3, er alle representasjoner av denne typen redusible. Dette er, som vi skal se, en konsekvens av at multiplisiteten til -1 i den karakteristiske ligningen til X per definisjon er 1 for alle dimensjoner.

Tatt i betraktning at enhver representasjon av Γ er gitt ved en invertibel matrise og en fordeling av multiplisiteter, slik det ble forklart i seksjon (3.2), er det naturlig å spørre om det finnes fordelinger av multiplisiteter som er slik at ingen representasjoner med denne fordelingen er simpel. Vi skal bevise et teorem som gir svar på dette.

Med "multiplisitetene til Y" mener jeg multiplisitetene til $1, \omega$ og ω^2 som røtter i det karakteristiske polynomet til Y, inkludert multiplisitet null for dem som eventuelt *ikke* er en rot. Multiplisitetene til X defineres tilsvarende.

Teorem 7 La ρ være en representasjon (X, Y) av den modulære gruppen. Dersom h er den høyeste av multiplisitetene til Y, og l den laveste av multiplisitetene til X, så impliserer $h > l$ at ρ stabiliserer en linje.

Bevis. Vi kan anta at Y er diagonal. Da har Y en egenverdi λ med h forekomster på diagonalen. Sett $X = PDP^{-1}$, der D er diagonal. Da er søylene til P egenvektorer til X. Man kan utføre søyleoperasjoner på søyler som tilhører samme egenverdi uten å endre X. Ettersom X har maksimalt to ulike egenverdier kan vi finne $n - l$ søyler tilhørende samme egenverdi (der n er dimensjonen til representasjonen. Søyleoperasjoner gir oss dermed en egenvektor til X som har nuller på alle rader unntagen $n - (n - l - 1) = l + 1$ fritt valgte rader. For å unngå at denne vektoren også er egenvektor til Y, er det nødvendig at $l + 1 > h$. □

Man kan utlede teorem 7 fra et mer generelt resultat i en artikkel av B. W. Westbury [4]. Tilpasset den modulære gruppen og vår terminologi kan vi lese at dersom $h > l$, så er det ikke bare utelukket at representajonen er simpel; den er heller ikke indekomposabel. La oss verifisere dette for 3-dimensjonale representasjoner.

$$D = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \nu \end{bmatrix} \qquad Y = \begin{bmatrix} \eta & 0 & 0 \\ 0 & \eta & 0 \\ 0 & 0 & \mu \end{bmatrix}$$

Her er $\lambda, \nu \in \{1, -1\}$ og $\eta, \mu \in \{1, \omega, \omega^2\}$. Vi skal vise at (X, Y) er dekomposabel når $X = PDP^{-1}$ for en vilkårlig valgt matrise $P \in GL_3(\mathbb{C})$. Vi kan utføre søyleoperasjoner på de to første søylen til P uten å endre på X, så vi kan anta at P er på formen

$$P = \begin{bmatrix} * & \alpha & \alpha \\ * & \beta & \beta \\ 0 & * & * \end{bmatrix}$$

Første søyle er nå en egenvektor til både X og Y, og planet spent opp av de to resterende søylene er også spent opp av e_3 og $\alpha e_1 + \beta e_2$, to egenvektorer til Y. Representasjonen stabiliserer altså et plan og en linje som ikke ligger i planet, og er således dekomposabel.

5.2 La oss nå anta at vi har kommet over en 4-dimensjonal representasjon $\rho = (X, Y)$, der $X = PDP^{-1}$ for en eller annen invertibel matrise P, og

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \qquad Y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega \end{bmatrix}$$

Teorem 7 utelukker ikke at dette er en simpel representasjon. Som vi skal se er den ikke desto mindre redusibel.

Et av de kraftigere verktøyene vi har for å avgjøre hvorvidt en representasjon er simpel, er teorem 1. Nå skal vi bruke det for å vise at ρ er redusibel. Teoremet forteller oss at ρ er simpel hvis og bare hvis $\rho(\Gamma)$ inneholder en basis for $M_4(\mathbb{C})$ som vektorrom over $\mathbb{C}$. Det betyr at ρ er simpel bare dersom man kan finne 16 lineært uavhengige elementer i $M_4(\mathbb{C})$ som er produkter av X og Y. Jeg vil kalle slike produkter for *monomer*, da de svarer til monomer i $\mathbb{C}\langle x, y\rangle/(x^2, y^3)$.

Man kan vise at det i vårt tilfelle vil finnes maksimalt 15 lineært uavhengige monomer. Første trinn er å observere at $Y^2 = -\omega^2 Y - \omega I$, slik at man kan konsentrere seg om monomene som er uten forekomster av Y^2.

Neste trinn er å bruke Cayley-Hamilton, dvs. at man for enhver matrise $A \in M_n(\mathbb{C})$ med karakteristisk polynom f har at $f(A) = 0$. Den karakteristiske ligningen til en matrise fra $M_4(\mathbb{C})$ er av grad fire, så når u er et monom kan vi skrive u^4 som lineærkombinasjon av I, u, u^2 og u^3. Det betyr at når vi ser etter lineært uavhengige monomer, så kan vi se bort fra de med en faktor på formen u^4. Monomene våre av grad åtte eller høyere som er uten forekomster av Y^2 må, med unntak av I, ha en faktor på formen u^4. Da står vi igjen med 15 stykker, altså én for lite.

5.3 Dersom Y har en egenverdi λ med multiplisitet større enn summen av multiplisitetene til de to andre (potensielle) egenverdiene, så er (X, Y) redusibel som følge av teorem 7. Anta at vi har en representasjon (X, Y) som teoremet ikke utelukker at er simpel, og at Y er diagonal. Da kan vi endre rekkefølgen på diagonalelementene og unngå at to like elementerstår ved siden av hverandre. Som bemerket etter beviset for teorem 1 er representasjonen $\rho : G \to GL_n(\mathbb{C})$ redusibel bare hvis $\rho(G)$-banen til enten en av e_i-ene eller en

vektor på formen $\mu e_i - e_{i+1}$ stabiliseres av ρ. Ettersom diagonalelementene til Y på rad i og $i+1$ er ulike, må e_i og e_{i+1} kunne skrives som lineærkombinasjon av $\mu e_i - e_{i+1}$ og $Y(\mu e_i - e_{i+1})$ dersom (X, Y) stabiliserer banen til $\mu e_i - e_{i+1}$. Det betyr at hvis (X, Y) er simpel, så kan vi slå fast at den er simpel ved å se på banene til e_i-ene. Dette gir også en god strategi for å finne et stabilisert underrom dersom (X, Y) er redusibel.

6 De 2-dimensjonale representasjonene av Γ

6.1 I dette kapittelet skal vi lage en oversikt over de 2-dimensjonale representasjonene av den modulære gruppen. Vi begynner med en karakterisering av simple representasjoner.

Proposisjon 8 La ρ være en 2-dimensjonal representasjon (X, Y) av den modulære gruppen. Da er ρ simpel hvis og bare hvis I, X, Y, XY er en basis for $M_2(\mathbb{C})$.

Bevis. Som en konsekvens av teorem 1 er ρ simpel hvis og bare hvis det finnes fire lineært uavhengige monomer. Vi antar at ρ er simpel, og viser at I, X, Y, XY i så fall er lineært uavhengige. Som følge av Cayley-Hamilton kan vi se bort fra monomer med en faktor opphøyd i annen potens, slik at vi står igjen med $I, X, Y, XY, YX, XYX, YXY$. Fire av disse danner altså basis for $M_2(\mathbb{C})$. Det er klart at I, X, Y må være lineært uavhengige, slik at disse tre sammen med én av de andre danner basis. Dersom I, X, Y, YX er uavhengige, så vil konjugasjon med X på hver av disse monomene bringe oss over til I, X, Y, XY. Dersom I, X, Y, XYX er uavhengige, så vil multiplikasjon med X (fra venstre eller høyre) bringe oss over til I, X, YX, XY. Multiplikasjon med en invertibel matrise bevarer lineær uavhengighet. Dermed kan ikke *både* XY og YX være en lineærkombinasjon av I, X og Y, og det kan konkluderes at I, X, Y, XY er lineært uavhengige. Vi kan dessuten utelukke at I, X, Y, YXY er uavhengige, da venstremultiplikasjon med X bringer oss over til $I, X, XY, (XY)^2$. □

Dersom man er gitt en 2-dimensjonal representasjon (X, Y) kan man som følge av proposisjonen avgjøre om den er simpel ved å sette opp en 4×4 matrise og sjekke om den er invertibel. (Det er naturligvis enklere å finne ut om X og Y har en felles egenvektor).

$$\begin{bmatrix} 1 & x_{11} & y_{11} & x_{11}y_{11} + x_{12}y_{21} \\ 0 & x_{21} & y_{21} & x_{21}y_{11} + x_{22}y_{21} \\ 0 & x_{12} & y_{12} & x_{11}y_{12} + x_{12}y_{22} \\ 1 & x_{22} & y_{22} & x_{21}y_{12} + x_{22}y_{22} \end{bmatrix}$$

En matrise som er invertibel hvis og bare hvis I, X, Y, XY er lineært uavhengige.

6.2 De simple 2-dimensjonale representasjonene er fordelt på uendelig mange isomorfiklasser, så vi kan ikke bare liste dem opp. Isteden skal vi tillegge hvert punkt $t \in \mathbb{C}$ en representasjon $\rho(t) = (X(t), Y(t))$, der

$$X_t = \begin{bmatrix} f_{11}(t) & f_{12}(t) \\ f_{21}(t) & f_{22}(t) \end{bmatrix} \qquad Y = \begin{bmatrix} g_{11}(t) & g_{12}(t) \\ g_{21}(t) & g_{22}(t) \end{bmatrix}$$

Her er $f_{ij}, g_{ij} \in \mathbb{C}[t]$. Som et utgangspunkt tenker vi oss at parametriseringen skal tilfredsstille følgende betingelser:

(i) Hvis ρ er en simpel 2-dimensjonal representasjon av Γ, så finnes det en $t \in \mathbb{C}$ slik at ρ er isomorf med $\rho(t)$.

(ii) Hvis $\rho(t)$ er isomorf med $\rho(s)$, så er $t = s$.

(iii) $\rho(t)$ er simpel for alle $t \in \mathbb{C}$

Dette er imidlertid umulig. Det finnes simple representasjoner når trasen til Y er $1 + \omega, 1 + \omega^2$ eller $\omega + \omega^2$, og bare i de tilfellene, Kontinuiteten til $g_{11} + g_{22}$ skaper dermed konflikt mellom (i) og (iii).

Som følge av teorem 7 er (X, Y) redusibel ved mindre X har trase 0 og Y har en av trasene $1 + \omega, 1 + \omega^2, \omega + \omega^2$, eller mer konsist $-\omega^k$ for $k = 0, 1, 2$. I resten av kapittelet vil traser spille en sentral rolle. Jeg skal bruke T_A som betegnelse på trasen til $A \in M_n(\mathbb{C})$.

Dersom (X, Y) er en 2-dimensjonal representasjon med $T_y = -\omega^k$, så er $(X, \omega Y)$ en representasjon med $T_{\omega Y} = -\omega^{k+1}$. En parametrisering begrenset til en av trasene $-\omega^k$ er på denne måten relatert til hver av de to andre ved en bijeksjon mellom de to mengdene av parametriserte representasjoner. Ettersom Y og ωY har samme egenvektorer tar bijeksjonen simple representasjoner på simple representasjoner. Dermed kan vi like godt holde oss til én av trasene. La trasen til $Y(t)$ være $-\omega^2$ og erstatt (i) med den følgende betingelsen:

$(i)^*$ Hvis (X, Y) er en simpel 2-dimensjonal representasjon med $T_Y = -\omega^2$, så finnes det en $t \in \mathbb{C}$ slik at ρ er isomorf med $\rho(t)$.

Det skal imidlertid vise seg at det fremdeles er umulig å tilfredsstille alle betingelsene.

Når vi setter inn f_{ij} for x_{ij} i 4×4 matrisen fra forrige seksjon, blir determinanten et polynom $h \in \mathbb{C}[t]$. Med andre ord er $\rho(t)$ simpel hvis og bare hvis $h(t) \neq 0$, slik at vi finner de simple representasjonene i en åpen mengde av $\mathbb{C}$ (i Zariski-topologien). Det er rimelig å anta at h er ikke-konstant, slik at den åpne mengden er forskjellig fra $\mathbb{C}$. I så fall er $(i)^*$ og (iii) uforenlige.

La oss nå se om vi kan finne en parametrisering som i det minste tilfredsstiller $(i)^*$ og (ii). Vi kan anta at $Y(t)$ er diagonal. La derfor $Y(t)$ være matrisen $\left[\begin{smallmatrix} 1 & 0 \\ 0 & \omega \end{smallmatrix}\right]$ for alle $t \in \mathbb{C}$. Egenvektorene til $Y(t)$ er dermed hele tiden e_1 og e_2. Det betyr at $X(t)$ og $Y(t)$ har en felles egenvektor bare i tilfellene hvor enten $f_{12} = 0$ eller $f_{21} = 0$.

For å finne en parametrisering som tilfredsstiller $(i)^*$ må man sørge for at dersom $X \in M_2(\mathbb{C})$ har $x_{12}, x_{21} \neq 0$ og $X^2 = I$, så finnes det en $t \in \mathbb{C}$ slik at (X, Y) er isomorf med $(X(t), Y(t))$. De to representasjonene er isomorfe dersom man kan finne en invertibel matrise A slik at $X = AX(t)A^{-1}$ og $Y = AY(t)A^{-1}$. Som vanlig kan vi anta at Y er diagonal. Og siden vi kan bytte om rekkefølgen på diagonalelementene ved hjelp av en konjugasjon, kan vi til og med anta at $Y = Y(t)$. Det er ikke vanskelig å se at hvis $AYA^{-1} = Y$, så er A en diagonalmatrise $\left[\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right]$ med $\alpha, \beta \in \mathbb{C}^*$. La $X \in M_2(\mathbb{C})$ være slik at $x_{12}, x_{21} \neq 0$ og $X^2 = I$. Nå vil

$$AXA^{-1} = \begin{bmatrix} x_{11} & \frac{\beta}{\alpha} x_{12} \\ \frac{\alpha}{\beta} x_{21} & x_{22} \end{bmatrix}$$

Det betyr at vi kan sette $f_{12}(t) = 1$ uten å gå glipp av noen isomorfiklasser av simple representasjoner. Ved å også sette $f_{11}(t) = t$, er resten av $X(t)$ bestemt av at trasen er 0 og at $X(t)^2 = I$. Dermed får vi en parametrisering som tilfredsstiller $(i)^*$, og for øvrig også (ii), nemlig den som tillegger hvert punkt $t \in \mathbb{C}$ en representasjon $(X(t), Y(t))$, der

$$X(t) = \begin{bmatrix} t & 1 \\ 1 - t^2 & -t \end{bmatrix} \qquad\qquad Y(t) = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}$$

Punktene på den komplekse linjen tillegges dermed simple representasjoner med unntak av $t = \pm 1$. De to unntakene svarer til indekomposable representasjoner, da $X(1)$ og $X(-1)$ har e_1 som egenvektor, men ikke e_2.

Man kunne ønsket å gi et mer komplett bilde av indekomposable representasjoner, redusible såvel som simple, ved å erstatte $(i)^*$ med en ny betingelse:

$(i)^{**}$ Hvis (X, Y) er en indekomposabel 2-dimensjonal representasjon med $t_Y = 1 + \omega$, så finnes det en $t \in \mathbb{C}$ slik at ρ er isomorf med ρ_t.

Det er imidlertid ikke til å unngå at $(i)^{**}$ kommer i konflikt med (ii). Dette vil fremgå av neste seksjon.

Parametriseringen ovenfor skal vi fra nå av betegne $\{\rho_2(t)\}$. Representasjonen man får når $\{\rho_2(t)\}$ evalueres i en bestemt parameterverdi betegnes $\rho_2(t)$, og er gitt ved $(X(t), Y_2)$. Generelt er $\{\rho_k(t)\}$ parametriseringen som fanger opp isomorfiklassen til en hvilken som helst simpel representasjon (X, Y) med $T_Y = -\omega^k$. Nærmere bestemt er $\rho_k(t) = (X(t), Y_k)$, der

$$X(t) = \begin{bmatrix} t & 1 \\ 1 - t^2 & -t \end{bmatrix} \qquad\qquad Y_k = \omega^k \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$$

6.3 Et mer komplett bilde av de 2-dimensjonale representasjonene av Γ kan oppnås ved å parametrisere *karakterer*.

Definisjon La $\rho : G \to GL_n(\mathbb{C})$ være en representasjon. Funksjonen $\chi(\rho) : G \to \mathbb{C}$ gitt ved $g \mapsto t_{\rho(g)}$ er *karakteren* til ρ.

Begrepet *karakter* er veldefinert ettersom similære matriser har samme trase, og det er klart (av samme grunn) at isomorfe representasjoner har lik karakter. For endelige grupper gjelder også den omvendte implikasjonen [2], men proposisjonen nedenfor viser at dette ikke generelt er tilfelle.

Proposisjon 9 La ρ være en redusibel 2-dimensjonal representasjon (X, Y) av Γ. Da er $\chi(\rho) = \chi(\nu) + \chi(\sigma)$, der ν og σ er 1-dimensjonale representasjoner av Γ.

Representasjonene $\rho_k(1)$ og $\rho_k(-1)$ fra paramteriseringen vår er redusible og indekomposable. Proposisjonen medfører dermed at det finnes en indekomposabel representasjon med samme karakter som en dekomposabel, og således at det finnes ikke-isomorfe representasjoner med samme karakter. Funksjonen $\chi(\nu) + \chi(\sigma)$ er nemlig karakteren til den direkte summen $\nu \oplus \sigma$.

Bevis for proposisjon 9 Vi trenger å vise at $\chi(\rho) = \chi(\nu) + \chi(\sigma)$ i de tilfellene hvor ρ er indekomposabel. Vi kan anta at Y er diagonal. Dersom ρ er indekomposabel, må X være enten øvre eller nedre triangulær. Det gjelder generelt at hvis to matriser $A, B \in M_2(\mathbb{C})$ er øvre triangulære, så er AB øvre triangulær, og at hjørnene a_{12} og b_{12} er uten innvirkning på trasen til

AB. Tilsvarende dersom $A, B \in M_2$ er nedre triangulære. Dermed har ρ den samme karakteren som en representasjon (D, Y), der D er diagonalmatrisen man oppnår fra X ved å sette enten x_{12} eller x_{21} lik null. Ettersom D og Y begge er diagonalmatriser, må (D, Y) være dekomposabel. □

Proposisjon 10 Simple 2-dimensjonale representasjoner av Γ med samme karakter er isomorfe.

Bevis. Vi bruker parametriseringen $\{\rho_2(t)\}$. Den er gitt ved $\rho_2(t) = (X(t), Y_2)$, der $X(t) = \left[\begin{smallmatrix} t & 1 \\ 1-t^2 & -t \end{smallmatrix}\right]$ og $Y_2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \omega \end{smallmatrix}\right]$ Trasen til $X(t)Y$ er $t(1-\omega)$. Det betyr at karakteren er ulik for ulike parameterverdier. Ettersom parametriseringen tilfredsstiller $(i)^*$, og isomorfe representasjoner har samme karakter, er to simple representasjoner (X, Y) og (X', Y') med $T_Y = T'_Y = -\omega^2$ isomorfe bare hvis karakteren er den samme. Tilsvarende viser man proposisjonen i tilfellene hvor $T_Y = T'_Y = -\omega$ og $T_Y = T'_Y = -1$. Det er klart at når proposisjonen holder for disse tre tilfellene, så holder den generelt. □

En 2-dimensjonal representasjon $\rho = (X, Y)$ med en karakter som ikke utelukker at den er indekomposabel vil ha $T_X = 0$ og $T_Y = -\omega^k$. Vi fokuserer på tilfellet $T_Y = -\omega^2$, og tillegger hvert punkt $t \in \mathbb{C}$ karakteren $\chi(\rho_2(t))$. Fra beviset av proposisjon 10 vet vi at ulike parameterverdier gir ulike karakterer.

Dersom ρ er simpel, så finnes det en $t \in \mathbb{C}$ slik at $\chi(\rho) = \chi(\rho_2(t))$. Vi vet jo at det finnes en $t \in \mathbb{C}$ slik at ρ er isomorf med $\rho_2(t)$.

Dersom ρ er redusibel vil ikke nødvendigvis parametriseringen inneholde en representasjon som er isomorf med ρ, men det vil finnes en $t \in \mathbb{C}$ slik at $\chi(\rho) = \chi(\rho_2(t))$. Dette kommer frem av beviset for proposisjon 9. Eventuelt kan man bruke selve proposisjonen og resonnere på følgende måte. Vi har $\chi(\rho) = \chi(\nu) + \chi(\sigma)$, der ν og σ er 1-dimensjonale, og med $T_X = 0$ og $T_Y = -\omega^2 = 1 + \omega$ er det bare to muligheter:

$\nu(x)$	$\nu(y)$	$\sigma(x)$	$\sigma(y)$
1	1	-1	ω
1	ω	-1	1

Her er x og y generatorene til Γ som ρ sender på henholdsvis X og Y. Radene i tabellen viser hvilke verdier ν og σ sender generatorene til, og utgjør de to eneste mulighetene for ν og σ som stemmer med $\chi(\rho) = \chi(\nu) + \chi(\sigma)$. Det er enkelt å verifisere at $\chi(\rho_2(1))$ og $\chi(\rho_2(-1))$ svarer til nettopp disse to mulighetene.

Vi kan nå slå fast at karakteren til ρ fanges opp av parametriseringen som tillegger hvert punkt $t \in \mathbb{C}$ karakteren $\chi(\rho_2(t))$, enten ρ er simpel eller redusibel. Det samme ville vært tilfelle dersom T_Y var $-omega$ eller -1, bare med $\{\rho_2(t)\}$ erstattet med enten $\{\rho_0(t)\}$ eller $\{\rho_1(t)\}$. På den måten har vi altså tre linjer med karakterer som fanger opp alle de "interessante" karakterene, nemlig de som ikke er garantert å tilhøre redusible representasjoner.

7 Representasjoner av B_3

7.1 Gruppen med presentasjonen $\{x, y : x^2 = y^3\}$ kalles B_3. Til sammenligning har den modulære gruppen presentasjonen $\{x, y : x^2 = 1, y^3 = 1\}$, mens S_3 har $\{x, y : x^2 = 1, y^3 = 1, xyxy = 1\}$. Som nevnt i kapittel 1 er S_3-modulene også Γ-moduler; og ettersom $x^2 = 1$ og $y^3 = 1$ impliserer $x^2 = y^3$, ser vi at alle Γ-modulene er B_3-moduler. Man kan si det slik at S_3 stiller de strengeste kravene til generatorene, Γ de nest strengeste, og B_3 de mildeste.

Det kan hevdes at Γ og B_3 står nærmere hverandre enn Γ og S_3. For dersom vi bare er interessert i simple og semisimple representasjoner, går det ut på ett om vi ser på Γ eller B_3. For å utdype dette trenger vi en annen presentasjon av B_3, nemlig $\{a, b : aba = bab\}$. Den er relatert til presentasjonen $\{x, y : x^2 = y^3\}$ på følgende vis:

$$\begin{aligned} x &\mapsto aba & \qquad a &\mapsto y^2x \\ y &\mapsto ab & \qquad b &\mapsto xy^2 \end{aligned}$$

En representasjon $\rho : B_3 \to GL_n(\mathbb{C})$ bestemmes av to matriser $\rho(a) = A$ og $\rho(b) = B$ som tilfredsstiller $ABA = BAB$. Sammen med assosiativiteten til matriseproduktet gir $ABA = BAB$ at $ABABAB$ ligger i senteret til $\rho(B_3)$.

$$\begin{aligned} (ABABAB)A = A(BABABA) = A(ABABAB) \\ (ABABAB)B = (BABABA)B = B(ABABAB) \end{aligned}$$

Dersom ρ er simpel har vi fra teorem 1 at senteret til $\rho(B_3)$ er inneholdt i senteret til $M_n(\mathbb{C})$, slik at $ABABAB$ må være en skalering av identiteten. Det betyr at hvis vi setter $x = aba$ og $y = ab$, så er $\rho(x^2) = \rho(y^3) = \alpha I$, der $\alpha \in \mathbb{C}$. Dermed sendes x på βX og y på γY, der $\beta^2 + \gamma^3 = \alpha$ og $X^2 = Y^3 = I$. Da er (X, Y) en simpel representasjon av Γ. På den måten gir ρ opphav til simple representasjoner av Γ. Ettersom X og Y er skaleringer av henholdsvis $\rho(x)$ og $\rho(y)$, er det klart at det ikke er noen vesentlige forskjeller på representasjoner av B_3 og Γ så lenge vi holder oss til de simple og semisimple.

Man kaller B_3 en *flettegruppe*. Dette er fordi elementene kan tenkes på som fletter laget av tre tråder. Generelt er B_n flettegruppen for n tråder, og

er generert av $n-1$ elementer. Artingruppene generaliserer flettegruppene, og blant disse finner man gruppene $G(p,q)$ presentert ved $\{x,y : x^p = y^q\}$ for relative primtall p og q. Her er altså $B_3 = G(2,3)$. Som vi så er det en nær forbindelse mellom de simple representasjonene av B_3 og de simple representasjonene av $\Gamma \simeq \mathbb{Z}_2 * \mathbb{Z}_3$, og man finner den samme nære forbindelsen mellom $G(p,q)$ og $\mathbb{Z}_p * \mathbb{Z}_q$.

7.2 En god del i denne oppgaven har kretset rundt det faktumet at en representasjon av Γ er gitt ved en invertibel matrise sammen med det jeg har kalt en fordeling av multiplisiteter. Noe tilsvarende kan sies om en representasjon av B_3. En slik representasjon er bestemt av to matriser A og B som tilfredsstiller fletterelasjonen $ABA = BAB$. (Det samme kan naturligvis sies om en representasjon (X,Y) av den modulære gruppen. Denne er bestemt av de to matrisene Y^2X og XY^2, som tilfredsstiller fletterelasjonen). Det følger av $ABA = BAB$ at $A = (AB)^{-1}B(AB)$, slik at A og B er similære. Dermed har de samme Jordanform. Representasjonen er altså bestemt av Jordanformen og en invertibel matrise. (Imidlertid er det ikke slik at en hvilken som helst Jordanform J og invertibel matrise P gir oss to matriser J og PJP^{-1} som tilfredsstiller fletterelasjonen.)

Det er ingenting ved fletterelasjonen som tvinger A og B til å være diagonaliserbare. Dermed vil Jordanformen inneholde mer informasjon enn en "fordeling av multiplisiteter". Nå har man også egenromsdimensjonene å forholde seg til. (Multiplisitet og egenromsdimensjon sammenfaller for diagonaliserbare matriser). Man kan dermed se for seg et teorem som sier at egenromsdimensjonene til A og B må være slik og slik dersom representasjonen er simpel. Faktisk finner man et resultat av denne typen i en artikkel av I. Tuba og H. Wenzl [3]. Der kan man lese at for representasjoner av dimensjon ≤ 5 må egenrommene til A og B alle sammen være 1-dimensjonale. Det er ikke vanskelig å se dette når dimensjonen er ≤ 3. I dimensjon 3 vil to plan nødvendigvis snitte hverandre, så hvis A og B har hvert sitt 2-dimensjonale egenrom vil de ha en felles egenvektor.

Referanser

[1] T.Y. Lam, *A Theorem of Burnside on Matrix Rings.* The American Mathematical Monthly, 105(7): 651-653. 1998.

[2] J.-P. Serre, *Linear Representations of Finite Groups.* Springer-Verlag New York, 1977.

[3] I. Tuba og H. Wenzl, *Representations of the braid group B_3 and of $SL(2, Z)$.* Pacific Journal of Mathematics, 197(2): 491-510. 2001.

[4] B. Westbury, *On the character varieties of free products of cyclic groups.* Preprint, University of Warwick. 2001.