Bachelorprojekt i matematik.
Institut for matematiske fag, Københavns Universitet

Bachelor Thesis in Mathematics.
Department of Mathematical Sciences, University of Copenhagen

Burnside-ringen for endelige grupper

Forfatter:
Pernille L. BRUHN

Vejleder:
Prof. Jesper GRODAL

Afleveringsdato: 8. juni 2012

Resumé

Vi starter med at definere en endelig G-mængde som en endelig mængde M sammen med en venstre virkning ved en gruppe G på M, hvorefter vi viser at banerne for en G-mængde selv er G-mængder, der er isomorfe med G-mængder $G/H = \{gH|g \in G\}$. Herefter definerer vi konjugering som en G-virkning og viser at G-mængderne G/H og G/K er isomorfe hvis og kun hvis H er konjugeret til K i G. Efterfølgende defineres Burnside-ringen $A(G)$ som Grothendieckringen konstrueret ud fra semiringen $A^+(G)$ af isomorfiklasser for endelige G-mængder. En afbildning $\phi_H(S)$ defineres ved at tælle de elementer i S, der er invariante under H. Denne afbildning udvider vi til en homomorfi og kalder den markhomomorfien. Grundlæggende egenskaber ved denne afbildning vises, hvorefter det vises hvornår idempotenter i $\prod_{H\in C(G)} \mathbb{Z}$ ligger i $A(G)$. Efterfølgende defineres primidealspektret og det vises at primidealer i $A(G)$ er på formen $\mathbf{P}_{U,p} = \{x \in A(G)|\phi_U(x) \equiv 0 \bmod p\}$, hvilket leder os frem til en karakterisering af opløselige grupper. Så gives et eksempel med udgangspunkt i den alternerende gruppe af grad 5, A_5 og i denne finder vi enheder og idempotenter. Herefter vises at to ikke-isomorfe grupper godt kan have isomorfe Burnside-ringe. Til sidst gennemgås der i hovedtræk to artikler, hvor den første siger, at hvis grupperne er enten hamiltonske eller abelske, så vil de være isomorfe hvis deres Burnside-ringe er, og den anden siger at grupper med isomorfe Burnside-ringe har "de samme opløselige undergrupper".

Abstract

We begin by defining a finite G-set as a finite set M together with a left action of a group G on M and afterwards it is shown that the orbits of a G-set are G-set that are isomorfic to G-sets $G/H = \{gH|g \in G\}$. Next we define conjugation as a G-action and show that the G-sets G/H and G/K are isomorphic is and only is H i conjugated to K in G. Following this we define the Burnside ring $A(G)$ as the Grothendieck ring constructed from the semi-ring $A^+(G)$ of isomorphism classes of finite G-sets. A function $\phi_H(S)$ is defined by counting all the elements in S that are invariant under H. This function extends to a homomorphism which we call the markhomomorphism. Fundamental results about this function are shown and afterwards it is shown when idempotents in $\prod_{H\in C(G)} \mathbb{Z}$ are in $A(G)$. Afterwards the prime ideal spectrum is defined and it is shown that all prime ideals in $A(G)$ are on the form $\mathbf{P}_{U,p} = \{x \in A(G)|\phi_U(x) \equiv 0 \bmod p\}$ which leads us to a characterization of solvable groups. An example based on the alternating group of degree 5, A_5, is given and we find the units and idempotents. After this we show that two non-isomorphic groups can have isomorphic Burnside rings. At last some of the main points of two articles are discussed. The first article states that if the groups are either hamiltonian or abelian they will be isomorphic if their Burnside rings are, and the second article states that groups with isomorphic Burnside rings have "the same solvable subgroups".

Indhold

1 Indledning

Burnside-ringen for en endelig gruppe er en algebraisk konstruktion, der koder for de forskellige måde, hvorpå en gruppe kan virke på en mængde. Idéen om Burnside-ringen blev introduceret af William Burnside i slutningen af det 19. århundrede, men ringstrukturen kom først senere i 1967 på grund af Solomon. Burnside-ringen indeholder mange informationer omkring en gruppes G-mængder, og når man ser på den som en kommutativ ring, er der blevet vist mange ting om dens struktur. En af Burnside-ringens anvendeligheder er inden for karakterisering af opløselige grupper, som også vil blive berørt i denne opgave.
Et naturligt spørgsmål at stille sig selv i forbindelse med Burnside-ringen er, hvorvidt to ikke-isomorfe grupper kan have isomorfe Burnside-ringe, og dette spørgsmål har både positive og negative svar.

1.1 Notation

I opgaven får vi brug for en hel del notation, som jeg vil introducere her.

- $C(G)$ er mængden af konjugeringsklasser for en endelig gruppe G.
- For $T \in C(G)$ lader vi $\tilde{T}$ være klassen af konjugerede undergrupper $U \leqslant G$ med $T \simeq G/U$
- For $S, T \in C(G)$ skriver vi $S \prec T$ hvis der findes en G-homomorfi $S \to T$. (sagt på en anden måde, hvis enhver gruppe i $\tilde{T}$ indeholder en gruppe i $\tilde{S}$
- For $U \leqslant G$ lader vi $\tilde{U}$ betegne mængden af undergrupper, der er konjugerede til U.
- $[G/U]$ lader vi som tidligere betegne elementet $G/U \in A(G)$
- For $U, V \leqslant G$ skriver vi $U \sim V$ hvis U er konjugeret til V
- Og sidst, men ikke mindst skriver vi nogle gange $U \simeq V$ hvis U er underkonjugeret til V

2 Burnside-ringen for endelige G-mængder

I dette afsnit vil vi først definere en G-mængde. Derefter vil vi beskrive dennes baner, og dette vil give os en beskrivelse af G-isomorfiklasserne, som udgør en semi-ring, som vi kan udvide til en ring, som vi kalder Burnsideringen. Vi vil følge fremgangsmåden fra [10]

2.1 G-mængder

Definition 1. *En virkning af en gruppe G på en mængde S er en funktion $G \times S \to S$, så der for alle $x \in S$ og $g_1, g_2 \in G$ gælder at:*

$$ex = x \text{ og } (g_1 g_2)x = g_1(g_2 x)$$

hvor e er det neutrale element. Når en sådan virkning er givet, siger vi at G ***virker på*** *S.*

Normalt vil vi beskrive funktionen i ovenstående definition ved udtrykket $(g, x) \mapsto gx$, og vi ser altså at denne funktion skal være associativ, for at vi vil kalde det en gruppevirkning.

Definition 2. *En endelig G-mængde er en endelig mængde M sammen med en venstre virkning ved G på M.*

Proposition 1. *Lad G være en gruppe, der virker på en mængde M. Da er relationen på M defineret ved*

$$x \sim x' \Leftrightarrow gx = x' \text{ for et } g \in G$$

en ækvivalensrelation

Bevis: Lad $x \in M$. Så vil $ex = x$, hvor e er identiteten i G. Dvs. $x \sim x$ så $\sim$ er refleksiv. Antag nu $x \sim y$, dvs. der eksisterer $g \in G$ så $y = gx$, altså får vi $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = ex = x$, så $y \sim x$ og $\sim$ er altså symmetrisk. Til sidst antager vi at $x \sim y, y \sim z$. Så findes der $g, h \in G$ så $y = gx$ og $z = hy = h(gx) = (hg)x$ så $x \sim z$, så $\sim$ er transitiv.

Definition 3. *Ækvivalensklasserne for ækvivalensrelationen i proposition 1 kaldes banerne for G på M*

Det ses at en G-mængde er en disjunkt union af sine baner.

Proposition 2. *Banerne er transitive G-mængder og er isomorfe med G-mængder $G/H = \{gH | g \in G\}$*

Bevis: Per definition er banerne G-mængder. Lad B være en bane. Da banerne er ækvivalensklasser vil der gælde at for alle $x, y \in B$ findes $g \in G$ således at $gx = y$, hvilket vil sige at banerne er transitive G-mængder. Da vores G-mængder er fremkommet ud fra en venstrevirkning, ser vi at disse vil svare til sideklasserne $G/H = \{gH | g \in G\}$.

2.2 Konjugering

En af de vigtigste virkninger, vi skal bruge i denne opgave er *konjugering*.

Definition 4. *Lad H være en undergrupe af en gruppe G. En virkning af gruppen H på mængden G er givet ved $(h, x) \mapsto hxh^{-1}$. Denne virkning af $h \in H$ på G kaldes konjugering ved h og elementet hxh^{-1} siges at være den konjugerede til x.*

Vi kan ikke kun konjugere elementer i en gruppe. Vi kan også konjugere undergrupper på følgende måde: Lad K være en vilkårlig undergruppe af en gruppe G og lad $h \in H$. Da er hKh^{-1} en undergruppe af G, der er isomorf til K. Det vil sige, H virker på mængden S af alle undergrupper af G ved konjugering: $(h, K) \mapsto hKh^1$. Gruppen hKh^{-1} siges at være den **konjugerede** til K
Vi lader $C(G)$ betegne mængden af alle konjugeringsklasser for undergrupper for G

Hvis en gruppe G virker på sig selv ved konjugering kalder vi banen $\{gxg^{-1} | g \in G$ for $x \in G$ for **konjugeringsklassen** for x.

Proposition 3. *G/H og G/K er isomorfe hvis og kun hvis H er konjugeret til K i G*

Bevis: $\Rightarrow$: Lad G/H og G/K være isomorfe. Da må vi have at $[G : H] = [G : K]$, hvor $[G : \cdot]$ er indekset. Derudover må der eksistere en bijektion $\psi : G/H \to G/K$, så der for alle $x, g \in G$ gælder at $\psi(gxH) = g\psi(xH)$. Specielt må vi for alle $h \in H$ have at $\psi(H) = \psi(hH) = h\psi(H)$. Hvis $\psi(H) = xK$ betyder det at $HxK = xK$ eller at $x^{-1}Hx \subseteq K$. Specielt er vi nødt til at have at en konjugeret af H er indeholdt i K. Da G er endelig og H og K må have samme orden betyder det at H er konjugeret til K i G. Hvis $x^{-1}Hx = K$ må vi for enhver sideklasse have at $\psi(gH) = g\psi(H) = gxK$.
$\Leftarrow$: Lad nu omvendt H være konjugeret til K, det vil sige, vi har at $x^{-1}Hx = K$. Lad $\psi : G/H \to G/K$ være afbildingen defineret ved $gH \mapsto gxK$. Denne afbildning er veldefineret: Lad $yH = zH$, så skal vi have at $yxK = zxK$. Da $z^{-1}y \in H$, vil $x^{-1}z^{-1}yx \in x^{-1}Hx = K$, så $yxK = zxK$ som påstået. Hvis $gH \in G/H$ og $a \in G$ har vi at $\psi(a \cdot gH = \psi(agH) = agxK = a \cdot gxK = a\psi(gH)$, så ψ er en

homomorfi. Afbildningen fra $G/H \to G/K$ givet ved $gK \mapsto gx^{-1}K$ er altså en homomorfi og er den inverse til den tidligere afbildning, så ψ er altså en isomorfi fra $G/H \to G/K$, så G/H og G/K er altså isomorfe.
Samlet har vi altså vist at G/H og G/K er isomorfe hvis og kun hvis H er konjugeret til K i G.

Det er interessant at bemærke at ovenstående definition af ψ ikke er uafhængigt af valg af x. Hvis x og y er to forskellige elementer så $xHx^{-1} = yHy^{-1} = K$ så vil afbildningerne $\psi(gH) = gxK$ og $\phi(gH) = gyK$ være den samme afbildning hvis og kun hvis $y^{-1}x \in K$, det vil sige hvis og kun hvis x og y ligger i samme sideklasse for K. Så vi får én afbildning for hver sideklasse for K, der skærer mængden af elementer, der konjugerer H til K.

2.3 Burnside-ringen

Mængden af G-isomorfiklasser for endelige G-mængder bliver en kommutativ semiring, $A^+(G)$ med identitet, hvor addition er givet ved disjunkte foreninger og multiplikation fremkommer ved at dekomponere $G/H \times G/K$ ud i baner. Disse baner svarer til de dobbelte sideklasser $HgK, g \in G$, som svarer til mængden af baner af G/K under en venstre H-virkning. Denne virkning kan beskrives således: Hvis X er en H-mængde vil H-banerne for X svare til G-banerne for Gx_Hx. Hvis vi derudover har at X er en G-mængde, så har vi en G-isomorfi $G/H \times X \to Gx_Hx$: $(g, x) \mapsto (g, g^{-1}x)$. Dette anvender vi på $X = G/K$. Specielt ser vi at den dobbelte sideklasse HgK svarer til banen gennem $(1, g)$.

At $A^+(G)$ er en semiring, betyder $(A^+(G), +)$ ikke er en abelsk gruppe. Derfor vil vi have en måde, hvorpå vi kan udvide $A^+(G)$ så den får den fulde ringstruktur og bliver en ring med identitet. Dette gør vi ved at konstruere en Grothendieck-gruppe ud fra det kommutative monoid $(A^+(G), +)$.

Lad M være et kommutativt monoid. V ser på det kartesiske produkt $M \times M$. De to koordinater skal repræsentere en positiv og en negativ del, således at $(m, n) \in M \times M$ svarer til $m - n$. Herpå definerer vi addition koordinatvist: $(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2 + n_2)$. Nu definerer vi en ækvivalensrelation på $M \times M$, hvor vi siger at (m_1, m_2) er ækvivalent med (n_1, n_2) hvis der for et $k \in M$ gælder at $m_1 + n_2 + k = m_2 + n_1 + k$ Nu har vi defineret addition, identiteten er elementer på formen (m, m) og den inverse til (m_1, m_2) er (m_2, m_1), så vi har altså en gruppe.

Definition 5. *Grothendieck-ringen konstrueret ud fra semiringen $A^+(G)$ skrives $A(G)$ og vi kalder den* ***Burnside-ringen for G****. Lad S være en endelig G-mængde.*

Da skriver vi dens billede i $A(G)$ som $[S]$.

Korollar 1. *$(A(G), +)$ er den frie abelske gruppe på isomorfiklasser af transitive G-mængder.*

Bevis: Per definition er $(A(G), +)$ en abelsk gruppe. Vi ser at $[G/H]$, hvor H gennemløber C(G) er en additiv $\mathbb{Z}$-basis for $A(G)$, så $(A(G), +)$ er altså en fri abelsk gruppe, da en fri abelsk gruppe har en ikke-tom basis.
Vi ser altså at $A(G)$ er et frit $\mathbb{Z}$-modul med basismængden $C(G)$, der består af alle elementer i $A(G)$ repræsenteret ved transitive G-mængder. Derudover ser vi at to G-mængder er isomorfe hvis og kun hvis de repræsenterer det samme element i $A(G)$.

3 Grundlæggende egenskaber ved Burnside-ringen

I dette afsnit vil vi undersøge nogle af egenskaberne ved Burnside-ringen for en endelig gruppe. Vi starter dette afsnit med et eksempel for at vise motivationen for det efterfølgende.

Eksempel 1. *Generelt set svarer isotropi-gruppen for $G/H \times G/K$ i (g_1H, g_2K) til $g_1Hg_1^{-1} \cap g_2Kg_2^{-1}$. Lad nu G være en abelsk grupppe. Da vil alle isotropi-grupperne være $H \cap K$. Derfor får vi*

$$[G/H] \cdot [G/K] = a[G/H \cap K]$$

hvor $a \in \mathbb{Z}$ fås ved at tælle antallet af elementer på begge sider. Specielt ser vi at

$$[G/H]^2 = |G/H|[G/H]$$

hvor $|G/H|$ er kardinaliteten af G/H. Vi ser altså at for abelske grupper er $[G/H]$ næsten idempotenter (husk at element e i en ring er idempotent såfremt $e^2 = e$).

Vi kan altså sige noget om Burnside-ringen for en abelsk gruppe allerede nu uden andre definitioner end de fra foregående afsnit. Dog er vi nødt til at definere en bestemt homomorfi - mark-homomorfien - for at vi kan opnå dybere resultater.

3.1 Mark-homomorfien

Lad $H < G$ og lad S, T være endelige G-mængder. Ser vi på kardinaliteten af fikspunktmængderne, får vi at

$$|S^H + T^H| = |S^H| + |T^H|$$

samt

$$|S^H \times T^H| = |S^H||T^H|.$$

Således kan afbildningen $S \mapsto |S^H|$ udvides til en homomorfi af ringe:

$$\phi_H : A(G) \to \mathbb{Z}$$

Da konjugerede undergrupper giver samme homomorfi, får vi ét ϕ_H for hvert $H \in C(G)$.

Sagt i ord kan vi altså bestemme værdien af ϕ_H ved at tælle de elementer i S, der er invariante under H . Vi ser at ϕ_H har følgende egenskaber:

(i) $\phi_{M+N} = \phi_M + \phi_N$

(ii) $\phi_{M\times N} = \phi_M \phi_N$

(iii) For $T \in C(G)$ har vi
$\phi_T(U) \neq 0 \Leftrightarrow$ der eksisterer en G-homomorfi $[G/U] \to T \Leftrightarrow G/H$
er konjugeret til en undergruppe af V, for $V \in \tilde{T}$.

På grund af den additive og multiplikative egenskab ovenfor, kan vi udvide ϕ_H til en ringhomomorfi $\phi : A(G) \to \prod_{H\in C(G)} \mathbb{Z}$. Dette gør vi således:

Definition 6. *Lad produktet af alle ϕ_H være defineret ved*

$$\phi = (\phi_H) : A(G) \to \prod_{H\in C(G)} \mathbb{Z}.$$

Denne homomorfi af ringe kaldes ***markhomomorfien****, og ringen $\prod_{H\in C(G)} \mathbb{Z}$ kaldes spøgelsesringen.*

En af egenskaberne ved markhomomorfien er, at den kan bruges til at vise, hvornår to G-mængder er isomorfe.

Lemma 1. *To G-mængder M og N er isomorfe hvis og kun hvis $\phi_U(M) = \phi_U(N)$ for alle $U \leqslant G$*

Bevis: $\Rightarrow$: Hvis $M \cong N$ må vi have at $\phi_U(M) = \phi_U(N)$ for alle $U \leqslant G$
$\Leftarrow$: Hvis $M = N$ er sætningen oplagt. Så antag nu $M \neq N$. Da M og N er sideklasser kan de begge skrives på formen $M = \sum_{T\in C(G)} m_T T$, og $N = \sum_{T\in C(G)} n_T T$. Da $M \neq N$ og $C(G)$ er endelig, må der findes et største $S \in C(G)$ så $m_s \neq n_s$. Vi

kan antage at $m_T = n_T = 0$ for $S \lneqq T$. Så får vi fra den additive og multiplikative egenskab ved ϕ_U at for $U \in \tilde{S}$:

$$\phi_U(M) = m_s\phi_U(S) \neq n_s\phi_U(S) = \phi_U(N).$$

Så to G-mængder er isomorfe hvis og kun hvis $\phi_U(M) = \phi_U(N)$

Tidligere har vi set at to G-mængder, G/H og G/K er isomorfe hvis og kun hvis $H \sim S$. Så ovenstående lemma, der også giver en karakterisering af isomorfe G-mængder, kæder altså markhomomorfien sammen med konjugering, hvilket også giver mening, da vi summerer over konjugeringsklasser.

Lemma 2. *Lad $U \leqslant G$ og lad M være en G-mængde. Da vil*

$$[G/U] \cdot M = \phi_U(M)[G/U] + \sum_{T \lneqq [G/U]} m_T T.$$

Bevis: Antag $[G/U] \cdot M = \sum m_T T$. Så vil $m_T \neq 0$ medføre at $T \prec [G/U]$. Så vi mangler blot at udregne $m_{[G/U]}$. Ved at benytte den multiplikative egenskab for ϕ_U får vi

$$\begin{aligned} \phi_U([G/U]M) = \phi_U([G/U] \cdot \phi_U(M) = \sum m_T\phi_U(T) = m_{[G/U]}\phi_U([G/U]) \\ \Rightarrow m_{[G/U]} = \phi_U(M) \end{aligned}$$

Vi ser altså at $m_{[G/U]} = \phi_U(M)$ og så får vi den ønskede formel.

En anden egenskab ved markhomomorfien er, at den er injektiv. For at vise dette, skal vi bruge et lemma:

Lemma 3. *Relationen $[G/H] \leqslant [G/K] \Leftrightarrow H$* er underkonjugeret til *K er en partiel ordning.*

Bevis: At H er underkonjugeret til K betyder, at H er konjugeret til en undergruppe af K. Vi skal altså vise, at denne relation er (i) refleksiv, (ii) anti-symmetrisk og (iii) transitiv.
(i) Da H trivielt er en undergruppe af H ser vi at H er konjugeret til en undergruppe af sig selv da, $H = eHe^{-1}$.
(ii) Lad $[G/H] \leqslant [G/K]$. Da er H konjugeret til en undergruppe af K. Lad os kalde denne undergruppe K'. Det vil sige $H = gK'g^{-1}, g \in G$. Antag også at $K = dH'd^{-1}, d \in G$, hvor H' er en undergruppe af H, hvilket er det samme som at $[G/K] \leqslant [G/H]$. Så må $H = K$ og relationen er anti-symmetrisk.
(iii) Lad $[G/H] \leqslant [G/K]$ og $[G/K] \leqslant [G/J]$. Dvs. $H = gK'g^{-1}, g \in GK' < K$ og $H = dJ'd^{-1}, d \in GJ' < J$. Da $K < K$ får vi:

$$H = gKg^{-1} = g(dJ'd^{-1})g^{-1} = (gd)J'(d^{-1}g^{-1})$$

så $[G/H] \leqslant [G/J]$

Theorem 1. *ϕ er en injektiv homomorfi af ringe.*

Bevis: Per definition er ϕ en homomorfi af ringe. Antag nu for modstrid at $x \neq 0 \in Ker(\phi)$. Da kan x skrives ud fra basen på denne måde: $x = \sum a_H[G/H]$. Nu benytter vi den partielle ordning fra lemma 3 og lader $[G/H]$ være maksimal blandt basiselementer med $a_H \neq 0$. Så vil $G/K^H \neq 0$ medføre at $[G/H] \leqslant [G/K]$, altså vil 0=$\phi(x) = a_H[G/H^H] = a_H|N_G(H)/H| \neq 0$, hvor N er normalisatoren, hvilket er en modstrid, så vi kan konkludere at ϕ er injektiv. Markhomomorfien er altså en monomorfi.

Definition 7. *Lad $\psi : N \to M$ være en homomorfi af ringe. Da er kokernen for ψ defineret ved $koker(\psi) = M/\psi(N)$*

Hvor kernen for en afbildning kan ses som mængden af "løsninger", kan man se kokernen som værende mængden af "hindringer"eller sagt på en anden måde: mængden af betingelser. Kokernens dimension er altså antallet af betingelser, der skal opfyldes for at problemet har en løsning.

Da ϕ er en injektion af undergrupper af maksimal rang er kokernen en endelig gruppe. Vi vil nu udregne dens orden.
Vi ser på dette diagram af injektive ringhomomorfier:

$$\begin{tikzcd} A(G) \arrow[r, "\phi"] \arrow[d] & \prod \mathbb{Z} \arrow[d] \\ A(G) \otimes \mathbb{Q} \arrow[r, "\phi_{\mathbb{Q}}"] & \prod \mathbb{Q} \end{tikzcd}$$

hvor ϕ_Q er den rationale udvidelse af ϕ

Som tidligere nævnt virker $WH = |N_G(H)/H|$ frit på G/H som gruppen af G-automorfier. Virkningen er givet ved

$$WH \times G/H \to G/H : (wH, gH) \mapsto gw^{-1}H$$

Det vil sige, at den virker frit på enhver fikspunktsmængde G/H^K. Særligt vil $|WH|$ gå op i $|G/H^K|$. Derfor vil $\phi_Q([G/H] \otimes |WH|^{-1})$ være indeholdt i $\prod \mathbb{Z}$. Dette bringer os frem til følgende sætning:

Proposition 4. *Elementerne*

$$\phi_{\mathbb{Q}}([G/H] \otimes |WH|^{-1}) =: x_H$$

danner en $\mathbb{Z}$-basis for $\prod \mathbb{Z}$. Ordnen af kokernen for ϕ er $\prod_{H \in C(G)} |WH|$.

Bevis: At x_H'erne danner en basis medfører at ordnen af kokernen for ϕ er $\prod_{H\in C(G)} |WH|$. Vi ser nu på elementerne i $\prod \mathbb{Z}$ som rækkevektorer. Da danner x_H'erne - når de er tilpas ordnede - en trekantsmatrix med 1'ere i diagonalen. Ved Cramers formel ved vi så at denne er invertibel, så x_H'erne danner altså en basis.

Bemærk at ϕ kan også findes fra $A(G)$'s ringstruktur på følgende måde:
Lad $x \in A(G)$. Da er x en ikke-nuldivisor hvis og kun hvis $\phi(x) \in \prod \mathbb{Z}$ ikke har nogle nul -komponenter. Derfor vil $A(G) \otimes \mathbb{Q}$ være den fulde kvotientring for $A(G)$, dvs. alle ikke-nuldivisorer gøres invertible.
Hvis $x \in A \otimes \mathbb{Q}$ er indlejret i $A(G)$, er komponenterne i $\phi_{\mathbb{Q}}(x)$ inlejret i $\mathbb{Z}$ og er altså hele tal.
Omvendt, $\prod \mathbb{Z}$ er indlejret i $\phi(A(G))$, fordi $\prod \mathbb{Z}$ er genereret af idempotente elementer, der er indlejrede i enhver delring. Herved ser vi at ϕ kan identificeres ved inklusionen af $A(G)$ ind i den indlejrede afslutning i dens fulde kvotientring.

3.2 Kongruenser mellem fikspunktmængder

I foregående afsnit har vi set at $\phi(A(G))$ er en undergruppe af maksimal rang i $\prod \mathbb{Z}$. I dette afsnit vil vi gerne se på dennes billede.

Lad $G = \mathbb{Z}/p\mathbb{Z}$ være den cykliske gruppe af orden p, hvor p er primisk. Så er $|S| \equiv |S^G| \mod p$, fordi banerne for S/S^G har kardinalitet p. Denne kongruens giver altså en betingelse for at et element ligger i billedet for ϕ. Vi vil nu generalisere sådanne kongruenser.
For at kunne gøre dette, har vi brug for at introducere nogle definitioner.

Definition 8. *Lad G være en gruppe. Et* ***venstre G-modul*** *består af en abelsk gruppe M og en ventre gruppevirkning.* $\rho : GxM \to M$, *så* $\rho \cdot (a+b) = \rho \cdot a + \rho \cdot b$, *hvor* $\rho \cdot a$ *betyder* $\rho(g,a)$. *Et* ***højre G-modul*** *defineres tilsvarende.*

Har vi et ventre G-modul kan vi lave et højre G-modul ved at definere $a \cdot g = g^{-1} \cdot a$. Det vil sige, at det i praksis ikke gør stor forskel om et G-modul er et højre eller venstre G-modul, så i det følgende vil vi blot benytte ordet G-modul.

Definition 9. *Lad V være et vektorrum over et legeme* $\mathbb{F}$. *Da er den* ***generelle lineære gruppe for V*** *gruppen af alle automorfier af V, dvs. mængden af alle bijektive lineære transformationer med kompositioner af funktionaler som gruppekomposition. Vi skriver* $GL(V)$.

Hvis V har endelig dimension er $GL(V)$ og $GL(n, \mathbb{F})$ isomorfe, hvor $GL(n, \mathbb{F})$ er gruppen af alle $n \times n$-matricer over $\mathbb{F}$, der er invertible. Da matricer over et legeme $\mathbb{F}$ er invertible hvis og kun hvis deres determinant ikke er lig nul, kan man også definere $GL(n, \mathbb{F})$ som gruppen af matricer med ikke-nul determinant.

Ud fra den generelle lineære gruppe, kan vi definere en *representation*:

Definition 10. *En* ***repræsentation*** *af en gruppe G på et vektorrum V over et legeme $\mathbb{F}$ er en gruppehomormorfi fra G til $GL(V)$. En repræsentation er altså en afbildning $\rho : G \to GL(V)$ så $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ for alle $g_1, g_2 \in G$.*

Her kalder vi V **repræsentationsrummet** og dimensionen af V kaldes dimensionen af repræsentationen. Et underrum W af V, der er invariant under gruppevirkningen, kaldes en underrepræsentation. Hvis V har præcis to underrepræsentationer, nemlig det nul-dimensionelle underrum og V selv, siges repræsentationen at være *irreducibel*.

Definition 11. *Lad nu V være et endelig-dimensionelt vektorrum over et legeme F og lad $\rho : G \to GL(V)$ være en repræsentation af en gruppe G på V.* ***Karakteren*** *af ρ er funktionen $\chi_\rho : G \to F$ defineret ved*

$$\chi_\rho(g) = Tr(\rho(g))$$

hvor Tr er sporet, som for en $n \times n$-matrix er defineret som summen af alle indgangene i hoveddiagonalen.

En karakter χ_ρ siges at være irreducibel, hvis ρ er en irreducibel repræsentation.

Definition 12. *For $g, h \in G$ er ortogonalitetsrelationen for karakterer er givet således:*

$$\sum_{\chi_i} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |C_G(g)| & \textit{hvis } g \textit{ og } h \textit{ er konjugerede} \\ 0 & \textit{ellers} \end{cases}$$

hvor vi summerer over alle irreducible karakterer for G og $|C_G(g)|$ er centralisatoren for G, som er defineret ved $C_G(g) = \{g \in G | hgh^{-1} = g\}$

Lad S være en endelig G-mængde og lad $V(S)$ være det komplekse vektorrum, der er udspændt af elementer i S. En G-virkning på en basis S for $V(S)$ inducerer en lineær virkning på $V(S)$. Heraf får vi et G-modul $V(S)$, som vi kalder permutationsrepræsentationen associeret med S. Karakteren af $V(S)$ er en funktion på G og vil blive beskrevet ved samme symbol. Ortogonalitetsrelationerne for karakterer siger særligt at for ethvert komplekst G-modul V svarer tallet $|G|^{-1} \sum_{g \in G} V(g)$ til dimensionen af V^G. Heraf får vi

$$\sum_{g \in G} V(S)(g) \equiv 0 \bmod |G| \tag{1}$$

Nu bemærker vi at

$$V(S)(g) = Tr(1_g : V(S) \to V(S) : v \mapsto gv) = |S^g| \tag{2}$$

Derfor kan (1) omskrives således:

$$\sum_{g \in G} \phi_{<g>}(x) \equiv 0 \bmod |G| \tag{3}$$

for ethvert $x \in A(G)$, og hvor $< g >$ er den cykliske gruppe genereret ved g.
Hvis H er en cyklisk undergruppe af G er antallet af elementer g med $< g >$ konjugeret til H

$$|H^*||G/N_G(H)| \tag{4}$$

hvor H^* er mængden af generatorer for H og $|G/N_G(H)|$ er antallet af grupper, der er konjugerede til H og N er normalisatoren. Derfor kan (3) omskrives til

$$\sum_{H cyklisk} |H^*||G/N_G(H)|\phi_H(x) \equiv 0 \bmod |G| \tag{5}$$

hvor der nu summeres over konjugeringsklasser af cykliske undergrupper for G i stedet for elementer i G.
Nu bruger vi samme argument på $V(S^H)$, når vi ser på denne som et $N_G(H)/H$-modul og får

$$\sum_{(K)} |K/H^*||N_G(K)/N_G(H) \cap N_G(K)|\phi_K(x) \equiv 0 \bmod |N_G(H)/H| \tag{6}$$

hvor vi her summerer over NH-konjugationsklasser K så H er normal i K og K/H er cyklisk. Dette kan også skrives som

$$\sum_K n(H,K)\phi_x \equiv 0 \bmod |N_G(H)/H| \tag{7}$$

hvor $n(H,K)$ er bestemte heltal med $n(H,H) = 1$, og som er antallet af G-konjugerede af K, der indeholder H. Vi summerer på samme måde.

Vi har altså her set at hvis vi summerer antallet af G-konjugerede undergrupper af K, der indeholder H over undergrupper $K \leqslant G$, så får vi 0 mod $|N_G(H)/H|$. Disse kongruenser vil vi beskrive nærmere, så i den næste sætning ser vi elementer i $\prod \mathbb{Z}$ som funktioner $C(G) \to \mathbb{Z}$.

Theorem 2. *Kongruenserne i (7) er en fuldstændig mængde af kongruenser for billedet af ϕ; i.e. $x \in \prod \mathbb{Z}$ er indeholdt i billedet for ϕ hvis og kun hvis*

$$\sum_K n(H, K)\phi_x \equiv 0 \bmod |N_G(H)/H| \tag{8}$$

for alle $H \in C(G)$.

Bevis: Vi har allerede set at elementer i billedet opfylder disse kongruenser. Kongruenserne i (7) er uafhængige, fordi de er givet ved en trekantsmatrix med 1'ere i diagonalen. Derfor beskriver de en undergruppe A med index $\prod |N_G(H)/H|$. Ved proposition 3 får vi altså at $A = \mathrm{im}(\phi)$.

3.3 Idempotenter

Idempotente elementer i $\prod \mathbb{Z}$ er funktionerne med værdierne 0 og 1. Vi vil bruge foregående afsnit til at se, hvornår sådanne funktioner kommer fra $A(G)$. I dette afsnit betragter vi $A(G)$som en delring af $\prod \mathbb{Z}$ via ϕ.

Først minder vi os om, hvad det vil sige, at en gruppe er opløselig:

Definition 13. *En gruppe G siges at være **opløselig**, hvis $G^{(n)} =< e >$ for et n.*

Enhver abelsk gruppe er trivielt opløselig.

Lemma 4. *Lad G være en gruppe. Da vil ethvert $H < G$ have en mindste normal undergruppe H^s således at H/H^S er opløselig.*

Bevis: Vi definerer $H^s = \cap\{K \lhd H | H/K$ er opløselig $\}$. Da H^s består af skæringen af normale undergrupper i H, må den selv være en normal undergruppe. Den må være den mindste, da den vil være indeholdt i alle de andre normale undergrupper, og den opfylder at H/H^s er opløseligt.

Theorem 3. *En idempotent $e \in \prod \mathbb{Z}$ er indeholdt i $A(G)$ hvis og kun hvis ligheden $e(H) = e(H_s)$ holder for alle $H \in C(G)$.*

Bevis: $\Rightarrow$: Antag $e \in A(G)$. Så opfylder e (7). Lad nu $K < G$. Ved lemma 4 ved vi, at der findes en mindste normal undergruppe, K^S. Vi ser på kæden

$$K^S = K_n \lhd K_{n-1} \lhd ... \lhd K_0 = K$$

sådan at K^i/K^{i+1} er cyklisk af primisk orden $p(i)$. Nu bruger vi (7) på gruppen K^{i+1} og så får vi at

$$e(K^i) \equiv e(K^{i+1}) \bmod p(i).$$

Da værdien af e er enten 0 eller 1 må vi have at $e(K^i) = e(K^{i+1})$ og derfor har vi at $e(H) = e(H_s)$.
$\Leftarrow$: Lad nu $e(K) = e(K_s)$ for alle K. Så må vi have at $e(H) = e(K)$ for alle $H \lhd K$ med K/H cyklisk så e opfylder (7).

3.4 Noetherske ringe

I dette afsnit vil vi vise at $A(G)$ er en noethersk ring, for dette skal vi bruge senere.

Definition 14. *Vi kalder en ring R noethersk, såfremt de tre følgende (ækvivalente) egenskaber er opfyldt:*

(1) *Enhver ikke-tom mængde af idealer har et maksimalt element.*

(2) *Enhver stigende kæde af idealer er stationær*

(3) *Ethvert ideal er endeligt frembragt*

Det kan vises at disse betingelser er ækvivalente.

Proposition 5. *Lad*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

være en kæde af A-moduler. Da vil

M er noethersk ⇔ M' og M" er noetherske

Bevis: ⇒: En stigende kæde af undermoduler i M' (eller M'') giver anledning til en kæde i M, så kæden må altså være stationær, fordi M er noethersk.
⇐: Lad $(L_n)_{n\geqslant 1}$ være en stigende kæde af undermoduler i M. Da er $(\alpha^{-1}(L_n))$ en kæde i M' og $(\beta(L_n))$ er en kæde i M''. For tilpas store værdier af n, vil begge disse være stationære, og så følger det heraf at $(L_n)_{n\geqslant 1}$ er stationær.

Proposition 6. *Lad A være noethersk og lad a være et ideal i A. Da er A/a en noethersk ring.*

Bevis: Ved proposition 4 er A/a noethersk som et A-modul og derved er det også som et A/a-modul.

Dette leder os frem til følgende sætning:

Theorem 4. *Hvis A er en noethersk ring og ϕ er en homomorfi fra A til B, så er B også Noethersk.*

Bevis: Dette følger fra ovenstående proposition, da $B \simeq A/a$, hvor $a = Ker(\phi)$

Korollar 2. *Burnsideringen er en noethersk ring*

Bevis: Dette følger af sætningen ovenfor, da $\mathbb{Z}$ er en noethersk ring, og vi ved, at der findes en homomorfi mellem $\prod_{H\in C(G)} \mathbb{Z}$ og $A(G)$ og $\prod_{H\in C(G)} \mathbb{Z}$ er indlejret i $\prod \mathbb{Z}$.

4 Primidealspektrum

Hovedresultaterne i dette afsnit stammer fra Andreas Dress [3].I dette afsnit vil vi se på primidealerne i Burnside-ringen, og vi vil se, hvordan disse kan anvendes til at karaterisere opløselige grupper. Det betyder vi vil vise at ethvert primideal i Burnside-ringen er på formen
$\mathbf{P}_{U,p} = \{x \in A(G) | \phi_U(x) \equiv 0 \bmod p\}$. Efter at have slået primidealernes form fast, vil vi vise, hvornår to primidealer ligger i samme sammenhængskomponent for $\mathrm{Spec}(A(G))$, hvor $\mathrm{Spec}(A(G))$ er primidealspektret for Burnside -ringen.

4.1 Zariski-topologien

Definition 15. *For en kommutativ ring R definerer vi primidealspektret til at være mængden af alle egentlige primidealer i ringen. Vi noterer dette spektrum som* $\mathrm{Spec}(R)$. *Formelt kan vi skrive:*

$$\mathrm{Spec}(R) = \{\boldsymbol{P} \in R) \mid \boldsymbol{P} \textit{ er et primideal } \}$$

Lad S være en ring, og lad for hver delmængde E af S $V(E)$ være delmængden af $\mathrm{Spec}(S)$, der består af alle primidealer, der indeholder E.
Lad f være et element i S. Da skriver vi $D(f) = \mathrm{Spec}(S) \backslash V(f)$ for mængden af primidealer, der *ikke* indeholder f.
Da det ofte kan være en fordel at kunne kende forskel på primidealer i S og elementerne i mængden $\mathrm{Spec}(S)$, definerer vi $\mathbf{J}_x$ til at være primidealet, der svarer til elementet x i $\mathrm{Spec}(S)$.

Proposition 7. *Lad S være en ring.*

(i) *Vi har at $V(O) = \mathrm{Spec}(S)$ og $V(1) = \emptyset$.*

(ii) *For enhver samling af delmængder $\{\boldsymbol{A}_\alpha\}_{\alpha \in I}$ af idealer $\boldsymbol{A}_\alpha$ i S, har vi at*

$$\bigcap_{\alpha \in I} V(\boldsymbol{A}_\alpha) = V(\sum_{\alpha \in I} \boldsymbol{A}_\alpha).$$

(iii) *Lad $\boldsymbol{A}_1, \boldsymbol{A}_2, ..., \boldsymbol{A}_n$ være idealer i S. Da vil*

$$V(\boldsymbol{A}_1) \cup V(\boldsymbol{A}_2) \cup ... \cup V(\boldsymbol{A}_n) = V(\boldsymbol{A}_1 \boldsymbol{A}_2 \cdots \boldsymbol{A}_n)$$

Bevis: Punkterne (i) og (ii) ses fra vores definition af $V(E)$.
(iii): Kan vi vise det tredje punkt for $n = 2$, kan vi vise det for alle n ved induktion efter n. For at vise, at det gælder for $n = 2$ ser vi først og fremmest at inklusionen

$$V(\mathbf{A}_1) \cup V(\mathbf{A}_2) \subseteq V(\mathbf{A}_1 \mathbf{A}_2)$$

er klar. Men vi skal stadig vise den omvendte inklusion. Lad $\mathbf{P}$ være et primideal, der indeholder hverken $\mathbf{A}_1$ eller $\mathbf{A}_2$. Da kan vi finde elementer $f_1 \in \mathbf{A}_1 \backslash \mathbf{P}$ og $f_2 \in \mathbf{A}_1 \backslash \mathbf{P}$. Da $\mathbf{P}$ er et primideal følger det at f_1, f_2 ikke er indeholdt i $\mathbf{P}$. Derfor indeholder $\mathbf{P}$ ikke idealet $\mathbf{A}_1\mathbf{A}_2$, og vi får altså at $V(\mathbf{A}_1\mathbf{A}_2) \subseteq V(\mathbf{A}_1) \cup V(\mathbf{A}_2)$. Samlet giver det os altså $V(\mathbf{A}_1\mathbf{A}_2) = V(\mathbf{A}_1) \cup V(\mathbf{A}_2)$. Resten af beviset følger som sagt ved induktion.

Det følger fra Proposition 6, at samlingen af delmængder $X \backslash V(\mathbf{A})$ af $\text{Spec}(S)$ for alle idealer $\mathbf{A} \in S$ gør $\text{Spec}(S)$ til et topologisk rum, hvor de åbne mængder er $X \backslash V(\mathbf{A})$.

Definition 16. *Topologien defineret ovenfor kaldes **Zariski-topologien**.*

De lukkede mængder i topologien er mængderne $V(\mathbf{A})$ for alle idealer $\mathbf{A} \in S$ eller tilsvarende mængderne $V(E)$ for alle delmængder E i S.
Mængderne på formen $D(f)$ for $f \in S$ er åbne og samlingen af åbne mængder $\{D(f)\}_{f \in S}$ danner en basis for topologien på $\text{Spec}(S)$. Faktisk tager vi en åben delmængde $U = X \backslash V(\mathbf{A})$ af X og $x \in U$. Det vil sige $\mathbf{A} \subsetneq \mathbf{J}_x$. Da er der et element $f \in \mathbf{A} \backslash \mathbf{J}_x$, og derfor vil $x \in D(f)$ og $D(f) \subseteq X \backslash V(\mathbf{A}) = U$

Vi husker nu på, hvad det vil sige, at er topologisk tum er sammenhængende:

Definition 17. *Lad X være et topologisk rum. En separation af X er et par U, V af disjunkte, ikke-tomme åbne delmængder af X hvis foreningsmængde er X. Rummet X siges at være **sammenhængende** hvis der ikke eksisterer en separation af X.*

Når vi har defineret, havd det vil sige for et topologisk rum at være sammenhængende, kan vi også definere sammenhængskomponenterne:

Definition 18. *Givet et topologisk rum X, definerer vi en ækvivalensrelation på X ved at sige $x \sim y$ hvis der findes et sammenhængende delrum af X, der indeholder både x og y. Ækvivalensklasserne kaldes **sammenhængskomponenterne***

Bemærk at selvom jeg har kaldt ovenstående ækvivalensklasser for sammenhængskomponenter, har jeg ikke argumenteret for at de virkelig er sammenhængende. Dette argumenteres der for i følgende proposition:

Proposition 8. *X's sammenhængskomponenter er sammenhængende disjunkte delrum af X hvis union er X, således at ethvert ikke-tomt sammenhængende delrum af X kun skærer en af dem.*

Bevis:Da sammenhængskomponenterne er ækvivalensklasser er de disjunkte og deres union er X. Ethvert sammenhængende delrum A af X, kan kun skære en af dem, for hvis A skærer sammenhængskomponenterne C_1 og C_2 af X, lad os sige i punkterne x_1 og i x_2 vil vi per definition have at $x_1 \sim x_2$, og dette kan ikke ske

medmindre $C_1 = C_2$.
For at vise at sammenhængskomponentet C virkelig er sammenhængende, vælg et punkt $x_0 \in C$. For ethvert punkt $x \in C$ ved vi at $x_0 \sim x$, så der er et sammenhængende delrum A_x, der indeholder x_0 og x. Fra det resultat, vi lige har bevist tidligere i beviset ved vi at $A_x \subset C$. Derfor får vi

$$C = \bigcup_{x \in C} A_x.$$

Da delrummene A_x er sammenhængende og har punktet x_0 tilfælles vil deres forening også være sammenhængende.

Dette bringer os frem til følgende sætning

Theorem 5. *For en noethersk ring, R, vil* $\mathrm{Spec}(R) = X$ *være sammenhængende hvis og kun hvis de eneste idempotenter i R er 0 og 1 eller tilsvarende at R ikke er på formen* $R_1 \times R_2$.

Bevis: Hvis X ikke er sammenhængende, kan den skrives som en disjunkt union af to egentlige lukkede delrum defineret ved idealer I_1 og I_2. Da $V(I_1) \cup V(I_2) = X$ må vi have at $I_1 I_2$ er et ideal indeholdt i R's nilradikal, som er idealet, der består af alle nilpotente elementer i R. Ved at erstatte I_i med en potens af I_i, kan vi antage at $I_1 I_2 = 0$, hvor vi benytter at R er en noethersk ring.
På den anden side har vi at $V(I_1) \cap V(I_2) = \emptyset$, så vi får at $I_1 + I_2 = R$. Specielt får vi $I_1 = I_1(I_1 + I_2 = I_1^2$. Da I_i er endeligt frembragt (igen fordi ringen er noethersk) følger det fra Cayley-Hamilton at en-elementer $e_1 \in I_1$ virker som identitet på I_1. Specielt har vi at $e_1 \cdot e_1 = e_1$. Sæt $e_2 = 1 - e_1$. Lad $R_1 = Re_1, R_2 = Re_2$, så kan R skrives som direkte produkt af de to delringe.

4.2 Primidealer

Definition 19. *Lad R være en ring. Hvis der findes et mindste* $n \in \mathbb{N}$*, så* $na = 0$ *for alle* $a \in R$*, siges R at have* ***karakteristik n****, og vi skriver charR = n. Hvis ikke et sådan n eksisterer, siges R at have karakteristik 0.*

Definition 20. *Et ideal* $\boldsymbol{P}$ *i en ring R, siges at være et primideal hvis* $\boldsymbol{P} \neq R$ *og hvis der for to vilkårlige idealer* $\boldsymbol{A}, \boldsymbol{B} \in R$ *gælder at*

$$\boldsymbol{AB} \subset \boldsymbol{P} \qquad \Rightarrow \qquad \boldsymbol{A} \subset \boldsymbol{P} \qquad or \qquad \boldsymbol{B} \subset \boldsymbol{P}.$$

Definition 21. *Et ideal M i en ring R siges at være* ***maksimal*** *hvis* $M \neq R$ *og hvis der for ethvert ideal N så* $M \subset N \subset R$ *enten til gælde at* $N = M$ *eller* $N = R$

Definition 22. *En gruppe hvori ethvert elements orden er en potens* ($\geqslant 0$) *af et fast primtal p, kaldes en p-gruppe.*

Lemma 5. *Hvis en gruppe H af orden p^n, hvor p er primisk, virker på en endelig mængde S og hvis $S_0 = \{x \in S \mid hx = x \text{ for alle } h \in H\}$, så er $|S| \equiv |S_0| \bmod p$.*

Bevis: En bane $\overline{x}$ indeholder præcist ét element hvis og kun hvis $x \in S_0$. Altså kan S skrives som en disjunkt union

$$S = S_0 \cup \overline{x_1} \cup \overline{x_2} \cup ... \cup \overline{x_n}$$

med $|\overline{x_i}| > 1$ for alle i. Heraf får vi

$$|S| = |S_0| + |\overline{x_1}| + |\overline{x_2}| + ... + |\overline{x_n}|.$$

Da $|\overline{x_i}| > 1$ får vi $p \mid |\overline{x_i}|$ for alle i, og $|\overline{x_i}| = [H : H_{x_i}]$ går op i $|H| = p^n$. Derfor får vi $|S| \equiv |S_0| \bmod p$.

Lemma 6. *Lad H være en p-undergruppe af en endelig gruppe G. Da er $[N_G(H) : H] \equiv (G : H) bmodp$.*

Bevis: Lad S være mængden af venstre sideklasser for H i G og lad H virke på S ved venstre-translation ($(h, x) \mapsto hx$). Så har vi per definition at $|S| = [G : H]$. Derudover har vi at

$$\begin{aligned} & & & xH \in S_0 \\ \Leftrightarrow & & hxH = xH & \quad \text{for alle } h \in H \\ \Leftrightarrow & & x^{-1}hxH = H & \quad \text{for alle } h \in H \\ \Leftrightarrow & & x^{-1}hx \in H & \quad \text{for alle } h \in H \\ & & & \Leftrightarrow xHx^{-1} = H \\ & & & \Leftrightarrow x \in N_G(H). \end{aligned}$$

Derfor er $|S_0|$ antallet af sideklasser xH med $x \in N_G(H)$, altså $|S_0| = (N_G(H) : H)$. Ved lemma 5 får vi så $[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \bmod p$.

Definition 23. *En undergruppe P af en gruppe G kaldes en Sylow p-undergruppe (p primisk) hvis P er en maksimal p-undergruppe af G. Det vil sige $P < H < G$, hvor H er en p-gruppe medfører $P = H$*

Vi kan nu gå videre til den første hovedsætning i dette afsnit. Denne sætning fortæller, at primidealerne i Burnside-ringen har den ønskede form, nemlig $\mathbf{P}_{U,p} = \{x \in A(G) | \phi_U(x) \equiv 0 \bmod p\}$.

Theorem 6. (a) *Lad $\boldsymbol{P}$ være et primideal i $A(G)$. Da vil mængden $C(G) - (C(G) \cap \boldsymbol{P})$ indeholde præcist ét minimalt element $T_{\boldsymbol{P}}$ og for $U \in \tilde{T}_{\boldsymbol{P}}$ og* char$A(G)/\boldsymbol{P}$ *får vi at $\boldsymbol{P} = \boldsymbol{P}_{U,p}$*

(b) *$\boldsymbol{P}_{U,p} \subseteq \boldsymbol{P}_{V,q}$ hvis og kun hvis $p = q$ og $\boldsymbol{P}_{U,p} = \boldsymbol{P}_{V,q}$ eller $p = 0, q \neq 0$ og $\boldsymbol{P}_{U,p} = \boldsymbol{P}_{V,q}$. Specielt har vi at $\boldsymbol{P}_{U,p}$ er minimal, resp. maksimal, hvis og kun hvis $p = 0$ resp. $p \neq 0$*

(c) *Hvis $p = 0$ har vi $\boldsymbol{P}_{U,0} = \boldsymbol{P}_{V,0}$ hvis og kun hvis $U \sim V$. Derudover har vi at $C(G) - (C(G) \cap \boldsymbol{P}_{U,0}) = \{T \in C(G) | U \prec T\}$, specielt har vi $T_{\boldsymbol{P}U,0} = [G/U]$*

(d) *Hvis $P \neq 0$ har vi at $\boldsymbol{P}_{U,p} = \boldsymbol{P}_{V,q}$ hvis og kun hvis $U^p \sim V^p$, hvor U^p den mindste normale undergruppe af U så U/U^p er en p-gruppe. I dette tilfælde har vi for $\boldsymbol{P} = \boldsymbol{P}_{U,p} : T_P = U_p$, hvor U_p er urbilledet i $N_G(U^p)$ af enhver Sylow p-undergruppe i $N_G(U^p)/U^p$.*

Bevis:

(a) Lad $S, T \in C(G)$ være minimale i $C(G) - (C(G) \cap \mathbf{P})$. Da er

$$S \cdot T = \sum_{R \prec S,T} n_R R \notin \mathbf{P}$$

og derfor vil vi have for mindst et $R \prec S, T$ at $R \notin \mathbf{P}$) og så må $R = T = S$. Derudover får vi for $T = [G/U]$ en udvidelse af formlen fra lemma 2 af ethvert element $x \in A(G)$:

$$T \cdot x = \phi_U(x)T + \sum_{R \in \mathfrak{T}, R \precneqq T} m_R R \equiv \phi_U(x)T \bmod \mathbf{P}$$

hvilket giver anledning til:

$$x \in \mathbf{P} \Leftrightarrow \phi_U(x) \equiv 0 \bmod \mathrm{char} A(G)/\mathbf{P} \Leftrightarrow x \in \mathbf{P}_{U,p}$$

for $p = \mathrm{char} A(G)/\mathbf{P}$

(b) Det er klart at ethvert primideal, der indeholder $\mathbf{P}_{U,0}$ er på formen $\mathbf{P}_{U,p}$ og ethvert primideal, der indeholder $\mathbf{P}_{U,p}$ for $p \neq 0$ er lig med $\mathbf{P}_{U,p}$ fordi $\mathbf{P}_{U,p}$ er maksimal.

(c) Det er nok at vise at $C(G) - (C(G) \cap \mathbf{P}_{U,0}) = \{T \in C(G) | U \prec T\}$, men dette er bare en omformulering af (iii) i afsnit 3.1.

(d) U^p er veldefineret og bestemt ved $\cap\{K \lhd U | U/K \text{er en p-gruppe}\}$.
Lad $W \trianglelefteq U$ hvor U/W er en p-gruppe. Da er

$$\phi_U M \equiv \phi_W M \bmod p$$

for alle M fordi $M^U \subseteq M^W$, M^W er U-invariant og $M^W - M^U$ er en disjunkt union af ikke-trivielle U/W-baner. Derfor vil $U^p \sim V^p$ medføre at $\phi_U M \equiv$

$\phi_{U^p} M = \phi_{V^p} M \equiv \phi_V M \bmod p$, altså $\mathbf{P}_{U,p} = \mathbf{P}_{V,p}$.
Antag nu at $\mathbf{P}_{U,p} = \mathbf{P}_{V,p} = \mathbf{P}$ og at $T = T_{\mathbf{P}}$.
Vi ved at $T = [G/W]$ hvis og kun hvis $\phi_U M \equiv \phi_{[G/W]} M \bmod p$ for alle M og $\phi_U[G/W] \equiv \phi_W[G/W] = [N_G(W) : W] \not\equiv 0 \bmod p$.
Men dette gælder generelt for urbilleder U_p for alle Sylow p-undergrupper af $N_G(U^p)/U^p$. Dette skyldes at $U^p = (U_p)^p$ er karakteristisk i U_p, og derfor $N_G(U_p) \subseteq N_G(U^p)$ og $p \nmid [N_G(U_p) : U_p]$.
Samtidig ser vi at $\phi_U M \equiv \phi_{U^p} M \equiv \phi_{U_p} M \bmod p$. Derfor vil $\mathbf{P}_{U,p} = \mathbf{P}_{V,p}$ medføre $U_p \sim V_p$ og så har vi $(U_p)^p = U^p \sim (V_p)^p = V^p$.

I det følgende lader vi U^p være den mindste normale undergruppe, så U/U^p er opløselig. Vi har tidigere set at denne er veldefineret.

Theorem 7. *To primidealer $\mathbf{P}_{U,p}$og $\mathbf{P}_{V,q}$ er i samme sammenhængskomponent i* $\mathrm{Spec}(A(G))$ *hvis og kun hvis $U^s \sim V^s$. Sammenhængskomponenterne for* $\mathrm{Spec}(A(G))$ *er derfor i en-til-en-korrespondance med klasserne af konjugerede undergrupper $U \leqslant G$ med $U = [U, U]$, som er kommutatorgruppen. Antallet af minimale primidealer i sammenhængskomponentet for $\mathbf{P}_{U,p}$ svarer altså til antallet af klasser af konjugerede undergrupper $V \leqslant G$ med $U^s \sim V^s$.*

Denne sætning giver altså en måde at bestemme antallet af minimale primidealer i Burnside-ringen på.

Bevis: Lad B være en noethersk ring. For ethvert primideal $P \in \mathrm{Spec}(B)$ lad da $\overline{\mathbf{P}} = \{\mathbf{Q} \mid \mathbf{Q} \in \mathrm{Spec}(B), \mathbf{P} \subseteq \mathbf{Q}\}$ være afslutningen af $\mathbf{P}$ i Spec(B). Så vil to primidealer $\mathbf{P}$ og $\mathbf{Q}$ ligge i samme sammenhængskomponent hvis og kun hvis der eksisterer en følge af minimale primidealer $\mathbf{P}_1, ..., \mathbf{P}_n$ med $\mathbf{P} \in \overline{\mathbf{P}}_1$, $\mathbf{Q} \in \overline{\mathbf{P}}_n$ og med $\overline{\mathbf{P}}_i \cap \overline{\mathbf{P}}_{i+1} \neq \varnothing$ for $i = 1, ..., n-1$.
Da vi har vist at $A(G)$ er en noethersk ring, kan vi nu sætte $B = A(G)$ og så får vi $\overline{\mathbf{P}}_{U,0} \cap \overline{\mathbf{P}}_{V,0} \neq \varnothing$ hvis og kun hvis $U^p \sim V^p$ for et p hvilket medfører $U^s = (U^p)^s \sim (V^p)^s = V^s$

Hvis $\mathbf{P}_{U,p}$ og $\mathbf{P}_{V,p}$ ligger i samme sammenhængskomponent får vi altså $U^s \sim V^s$

Samtidig vil $\mathbf{P}_{U,p}$ og $\mathbf{P}_{V,p}$ altid ligge i samme sammenhængskomponent da vi kan finde en kæde af normale undergrupper i U:
U=${}_0U \lhd_1 U \lhd_2 U \lhd ... \lhd_n U = U^s$ hvor ${}_{i-1}U/{}_iU$ er en p_i-gruppe for et primtal p_i for $i = 1, ..., n$. Dette betyder at:

$$\mathbf{P}_{U,p} \in \overline{\mathbf{P}}_{0U,p} \qquad \overline{\mathbf{P}}_{i-1U,0} \cap \overline{\mathbf{P}}_{iU,0} \neq \varnothing$$

for $i = 1, ..., n$.

Denne sætning giver os altså en måde vi kan karakterisere de opløselige grupper på. Det vil sige, at G er opløselig hvis og kun hvis 0 og 1 er de eneste idempotenter i $A(G)$.
Et korollar af foregående sætning er følgende:

Korollar 3. *G er minimal simpel hvis og kun hvis*

$$A(G) \simeq \mathbb{Z} \oplus A'(G)$$

for et $A'(G)$, med Spec($A(G)$ sammenhængende.

Dette vil jeg ikke bevise, men korollaret bliver diskuteret i det sidste afsnit.

5 Enheder og idempotenter

I dette afsnit vil vi se på enheder og idempotenter i Burnside-ringen og vise et eksempel med udgangspunkt i den alternerende gruppe af grad 5.

Vi husker at en enhed er et multiplikativt invertibelt element i en ring. Hvis A er en ring, lader vi A^* være den multiplikative gruppe af enheder.

Lad nu $e \in A$ være en idempotent. Da er $1 - 2e = u$ en enhed. Dette ses ved direkte udregning:

$$(1 - 2e)^2 = 1 + 4e^2 - 4e = 1 + 4e - 4e = 1.$$

Så $1 - 2e = u$ er endda sin egen inverse. Omvendt kan vi have et tilfælde, hvor vi for en enhed u, har at elementet $\frac{1-u}{2} = e$ er indeholdt i A. Så vil e være en idempotent, da

$$(1 - u)^2 = 2(1 - u)$$

for enhver enhed u.

Når vi ser på Burnside-ringen er $\frac{1-u}{2} \in \prod \mathbb{Z}$ men ikke nødvendigvis i $A(G)$. Dette vil vi se et eksempel på lige om lidt. Hvis G har ulige orden er coker(ϕ) ulige og så vil $(1 - u) \in A(G)$ og$\frac{1-u}{2} \in \prod \mathbb{Z}$ medføre at $\frac{1-u}{2} \in A(G)$. Da en ikke-opløselig gruppe har ikke-trivielle idempotenter, får vi sammen med konklusionen på forrige afsnit følgende sætning:

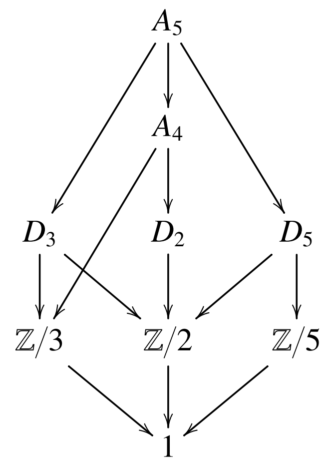
Theorem 8. *Hvis G er ikke-opløselig, så er $A(G)^* \neq \{\pm 1\}$. Hvis G er opløselig af ulige oden, da er $A(G)^* = \{\pm 1\}$*

Eksempel 2. Lad H være en undergruppe i G så $[G : H] = 2$. Vi husker på at indekset for en undergruppe i en gruppe er kardinaliteten af mængden af forskellige sideklasser. Da vil $H \lhd G$samt $[G/H]^2 = 2[G/H]$ (dette så vi tidligere) og derfor vil $u(H) := 1 - [G/H] \in A(G)^*$. Bemærk at $\frac{1-u(H)}{2}$ ikke ligger i $A(G)$. Dette var altså et eksempel på den situation vi beskrev tidligere.

5.1 Den alternerende gruppe af grad 5, A_5

Nu vil vi bruge det vi lige har fundet frem til på en konkret gruppe. Vi vil altså finde enheder og derefter idempotenterne.

Vi husker at den alternerede gruppe, A_n er defineret som mængden af alle lige permutationer i S_n, som er den cykliske gruppe af orden n. Vi ved at A_n er en normal undergruppe af S_n af indeks 2 og med orden $\frac{|S_n|}{2} = \frac{n!}{2}$. Specielt er A_n den eneste undergruppe i S_n med index 2. I dette afsnit vil vi fokusere på A_5. Et diagram over konjugeringsklasserne for denne gruppe ser således ud:



Her er D_n diedergruppen af orden 2n. Grupperne A_5, A_4, D_5, D_3 er deres egne normalisatorer, og for de andre får vi $N(\mathbb{Z}/n) = D_n$ og $N(D_2) = A_4 \cdot A(A_5)$ er mængden af funktioner $z : C(G) \to \mathbb{Z}$, der opfylder følgende:

(i) $z(H)$ arbitrær for H= A_5, A_4, D_5, D_3

(ii) $z(\mathbb{Z}/n) \equiv z(D_n)$ mod 2 for n=3,5

(iii) $z(D_2) \equiv z(A_4)$ mod 3

(iv) $z(1) + 20z(\mathbb{Z}/3) + 15z(\mathbb{Z}/2) + 24z(\mathbb{Z}/5) \equiv 0$ mod 60

Ringen $A(A_5)$ indeholder følgende enheder:

1	$\mathbb{Z}/2$	$\mathbb{Z}/3$	$\mathbb{Z}/5$	D_2	D_3	D_5	A_4	A_5
a	a	a	a	b	c	d	b	e

Her er $a, b, c, d, e \in \{\pm 1\}$ og anden linje i skemaet giver værdien af funktionen $u : C(G) \to \mathbb{Z}$ i elementet fra første linje. Kongruenserne (i)-(iv) viser at der ikke er nogle betingelser for enheder u i A_5, A_4 og D_3. Fra (iii) får vi at $u(D_2) = u(A_4)$. Ser vi på (iv) mod 3, mod 4 og mod 5 får vi

$$u(1) = u(\mathbb{Z}/2) = u(\mathbb{Z}/3) = u(\mathbb{Z}/5)$$

Undergrupperne 1 og A_5 er perfekte (perfekte undergrupper er de undergrupper, der er lig kommutatorgruppen). Derfor vil $A(A_5)$ indeholde idempotenterne $0, 1, e, 1-e$, hvor $\phi_{A_5}(e) = 1$ og $\phi_H(e) = 0$ for $H \neq A_5$.

Vi har altså nu bestemt enhederne og idempotenterne i Burnside-ringen for A_5 ved at kigge på konjugeringsklasserne for gruppen.

6 Isomorfier mellem Burnside-ringe

I dette afsnit vil vi undersøge isomorfier mellem Burnside-ringe. Det naturlige spørgsmål der opstår i den forbindelse er, hvorvidt to ikke-isomorfe grupper kan have isomorfe Burnside-ringe. Svaret på dette spørgsmål er ja, da Thévenaz har konstrueret uendeligt mange eksempler på ikke-isomorfe grupper med isomorfe Burnside-ringe.

6.1 Ikke-isomorfe grupper med isomorfe Burnside-ringe

Det viser sig at Burnside-ringe for ikke-isomorfe endelige grupper, godt kan være isomorfe. Dette eksempel blev konstrueret af Jacques Thévenaz i 1988 i [9].

Lad p, q være primtal så $q \mid p-1$. Lad $a, b \in \mathbb{Z}/p\mathbb{Z}$ være to forskellige primitive q'te enhedsrødder. Det vil sige at $a^n = 1$ for $n = q$ og $a^n \neq 1$ for $n = 1, 2, ..., q-1$ samt $b^n = 1$ for $n = q$ og $b^n \neq 1$ for $n = 1, 2, ..., q-1$. Lad Q være en cyklisk grupe af orden q så $G =< z >$ skrevet multiplikativt. Lad derudover $P_a = \mathbb{Z}/p\mathbb{Z}$ og $P_b = \mathbb{Z}/p\mathbb{Z}$ være to cykliske grupper af orden p - skrevet additivt - genereret ud fra x og y. Betragt Q-virkningen på $P_a \times P_b$ defineret ved

$$z \cdot x = ax$$
$$z \cdot y = by$$

Vi ser altså på to forskellige ikke-trivielle lineære repræsentationer af Q over $\mathbb{Z}/p\mathbb{Z}$.

Lad nu $G = G(a, b) = (P_a \times P_b) \rtimes Q$ være de semi-direkte produkt. Nu vil vi se på undergrupperne i denne gruppe. De oplagte undergrupper og deres konjugerede er

$$\{1\}, Q, P_a, P_b, P_a \rtimes Q P_b \rtimes Q, P_a \times P_b \text{ og } G$$

Derudover er der $\frac{p-1}{q}$ konjugeringsklasser af ikke-normale undergrupper af orden p. Dette er altså alle undergrupper i G.

Vi ved fra tidligere at G's Burnside-ring er entydigt bestemt ud fra matricen $(\phi_s(G/H))$, hvor S og H gennemløber $C(G)$. Vi har også vist at $(\phi_s(G/H) = |N_G(H)/H| n(S,H)$, hvor $n(S,H)$ som bekendt er antallet af G-konjugerede af H, der indeholder S. Alle disse heltal er allerede indregnet i vores eksempel og de afhænger ikke af valget af a og b. Det vil altså sige at Burnside-ringen for $G(a,b)$ ikke afhænger af a og b. Dog er vi nødt til at have at $a \neq b$ og $a \neq 1 \neq b$ for ellers ville vi have en helt anden undergruppestruktur.
Men antager vi at $a \neq b$ og $a \neq 1 \neq b$ mangler vi blot at vise at $G(a,b)$ ikke behøver være isomorf til $G(a',b')$for nogle a,b,a',b', for da Burnside-ringen for $G(a,b)$ ikke afhænger af a og b, må vi have at Burnside-ringen for $G(a,b)$ må være isomorf til Burnside-ringen for $G(a',b')$.

Ved at bytte om på x og y ser vi at

$$G(a,b) \cong G(b,a)$$

Da z er en generator for G må z^k også være det, så hvis k er indbyrdes primisk med q får vi også at

$$G(a,b) \cong G(a^k, b^k)$$

Vi vil nu vise at dette er de eneste mulige isomorfier. Lad f være en isomorfi mellem mellem $G = G(a,b) =< x,y,z >$ og $G' = G(a',b') =< x',y',z' >$. Af Sylows anden sætning er alle Sylow q-undergrupper af G' konjugerede, så vi kan komponere f med en indre-automorfi af G', hvor en indre-automorfi er en automorfi givet ved $\tau_g(x) = gxg^{-1}$. Dette giver os $f(z) \in Q'$, hvor $f(z) = (z')^k$, hvor k er indbyrdes primisk med q. Da a,b er egenværdier for virkningen af z på $P_a \times P_b$ vil de også være egenværdier for virkningen $f(z) = (z')^k$ på $P'_a \times P'_b$. Men da $(a')^k$ og $(b')^k$ er de to egenværdier for $(z')^k$ vil de to (uordnede) par

$$\{a,b\}, \{(a')^k, (b')^k\}$$

være ens.

Hvis q så er stor nok, findes der primitive q'te enhedsrødder a,b,a',b'med $a \neq b, a' \neq b'$ og $\{a,b\} \neq \{(a')^k, (b')^k\}$ for alle k. Derfor kan $G(a,b)$ og $G(a',b')$ ikke være isomorfe.
Et helt konkret eksempel på to sådanne grupper er $q = 5$ og $p = 11$, hvor vi får at $G(3,4) \ncong G(3,5)$

6.2 Videre diskussion

Nu har vi set et eksempel på ikke-isomorfe grupper med isomorfe Burnside-ringe, så vi kan altså ikke sige, at en gruppe er entydigt bestemt ud fra sin Burnside-ring. Der er dog kommet mange eksempler på tilfælde, hvor man faktisk kan konkludere at $A(G) \cong A(G') \Leftrightarrow G \cong G'$. Dette vil vi se nogle eksempler på her. Derudover kan man også vise, at hvis man har to grupper med isomorfe Burnside-ringe, så vil der eksistere en normaliserende isomorfi mellem grupperne, det vil sige en isomorfi $\Phi : A(G) \to A(G')$ så $\Phi(G/1) = G'/1$. Dette kan bruges til at klassificere de opløselige undergrupper yderligere.

6.2.1 Abelske og hamiltonske grupper

I 1991 udgav Satya Deo og K. Varadarajan artiklen "Isomorphic Burnside Rings" [2], hvor de netop kigger på nogle af de tilfælde, hvor man har at to grupper med isomorfe Burnside-ring må være isomorfe. Mere præcist definerer de $\mathcal{A}$ til at være klassen af endelige abelske grupper. Herefter lader de G og H være grupper i $\mathcal{A}$. Herefter viser de, at hvis $A(G)$ og $A(H)$ er isomorfe som ringe, så vil der for ethvert primtal p gælde at antallet af p-undergrupper af G svarer til antallet af p-undergrupper af H. Dette er interessant, da det viser at, når vi kigger på grupper i $\mathcal{A}$, så vil grupper med grupper med isomorfe Burnside-ringe altså have nogle egenskaber tilfælles. Herefter lader de $\mathcal{A}_2$ være klassen af endelige abelske grupper G med den egenskab, at for ethvert p, er den p-primære torsion $t_p(G)$ af G en *direkte sum af højest to cykliske grupper*. For grupper G, H i $\mathcal{A}_2$ viser de at $A(G)$ og $A(H)$ er isomorfe hvis og kun hvis G og H er isomorfe som grupper. Til sidst lader de A^+ være semiringen, der består af elementer fra $A(G)$ repræsenteret som G-mængder, som vi også selv definerede det tidligere i opgaven.For ethvert primtal p, lader de så $\mathcal{C}(p)$ være klassen af endelige abelske p-grupper. For to vilkårlige grupper G og H i $\mathcal{C}(p)$ viser de at der eksisterer en ring-homomorfi $\alpha : A(G) \to A(H)$, der ydermere opfylder at $\alpha(A^+(G)) = A^+(H)$ hvis og kun hvis G og H er isomorfe som grupper.

Her har vi altså nogle eksempler på grupper med isomorfe Burnside-ringe, hvor grupperne også er isomorfe. Men der er mange restriktioner på grupperne og beviserne, de har lavet for deres sætninger er meget lange. Beviserne fremkommer ved at de først kigger på homomorfier mellem Burnside-ringe, hvorefter de indfører $L_p(G) = \{H | H \leqslant G, \text{ H er en } p\text{-gruppe}\}$, og viser hovedresultatet, som siger, at hvis G og G' er endelige abelske grupper med isomorfe burnside-ringe, så er $|L_p(G)| = |L_p(G')|$ for ethvert primtal p. Stort set alle beviserne i artiklen er bygget op omkring homorfier mellem Burnside-ringe og benytter kategori-teori.

Jeg vælger ikke at gå i detaljer med dette, da det for det første er for kompliceret og for lang til at kunne indgå i denne opgave, og fordi Alberto Raggi-Cárdenas og Ernesto Vallejo i 1992 [6] viste at mange af disse restriktioner kan undværes. Som hovedresultat har de sætningen:

Theorem 9. *Lad G og H være endelige grupper, der begge udelukkende har normale undergrupper. Da eksisterer der en isomorfi $A(G) \cong A(H)$ hvis og kun hvis G og H er isomorfe.*

En gruppe med med udelukkende normale undergrupper kaldes en dedekind-gruppe. Trivielt set er alle abelske grupper dedekind-grupper. En ikke-abelsk dedekind-gruppe kaldes hamiltonsk. Det vil sige, at denne sætning siger, at hvis G, H er abelske (eller hamiltonske) grupper så gælder der at

$$A(G) \cong A(H) \Leftrightarrow G \cong H$$

Så når G og H er abelske eller hamiltonske, så er disse gruppers isomorfiklasser entydigt bestemt ud fra deres Burnside-ringe.

I denne artikel bruges en anden fremgangsmåde i beviserne. Jeg vil ikke gå i dybden med beviset, men blot beskrive fremgangsmåde og fremhæve enkelte resultater. Først reduceres problemet til problemer om p-grupper ved at bruge en generalisering af et resultat af Krämer fra [5]. Herefter vises der ved hjælp af et resultat fra Kratzer og Thévenaz (bevist af Dress og Vallejo i [4] om ordenen af idempotenter), at hvis G og H er p-grupper, der er dedekind-grupper og har isomorfe Burnside-ringe, da er antallet af undergrupper med en given kardinalitet det samme i begge grupper, så allerede her har vi at grupperne må have noget tilfælles, når deres Burnside-ringe er isomorfe.

Herefter benytter de en sætning af Delsarte fra [1]

Theorem 10. *Lad G være en abelsk gruppe med signatur $(s_1, ..., s_l, ...)$. Da er antallet af undergrupper af G med signatur $r = r_1, ..., r_k, ...)$, med $r_i \leqslant s_i$, og $r_j = 0$ for $j > k$, er*

$$N(G, r) := \frac{\mathcal{F}_r(p^{s_1}, ..., p^{s_k})}{\mathcal{F}_r(p^{r_1}, ..., p^{r_k})}$$

Denne sætning bringer dem frem til deres eget korollar:

Korollar 4. *Lad G og H være abelske p-grupper, der opfylder at $n_p(G, k) = n_p(H, k)$ for alle $k \geqslant 0$. Så er $G \cong H$*

Her er $n_p(G, k) := \#\{U \leqslant G || U| = p^k\}$, altså antallet af undergrupper i G med orden p^k.

Bevis: Lad $(s_1, ..., s_n, ...)$ og $(t_1, ..., t_n, ...)$ være signaturerne for G og H respektivt. Vi vil ved induktion vise at $s_i = t_i$ for alle i. Undergrupperne af G med signatur (1) er præcis undergrupperne af orden p. Derfor har vi induktionsstarten: $N(G, (1)) = N(H, (1))$ og det følger af foregående sætning at

$$\frac{p^{s_1} - 1}{p - 1} = \frac{p^{t_1} - 1}{p - 1}$$

så $s_1 = t_1$. Antag nu $k > 1$ og $s_i = t_i$ for $1 \leqslant i < k$. Per antagelse har vi

$$\sum_r N(G, r) = n_p(G, k) = n_p(H, k) = \sum_r N(H, r), \tag{9}$$

hvor r løber over alle signaturer $(r_1, ..., r_k, ...)$ således at $\sum r_i = k$. Lad $z = (1, ..., 1)$ være signaturen for den cykliske gruppe $\mathbb{Z}_{p^k}$. For en signatur $r = (r_1, ..., r_k, ...)$ med $\sum r_i = k$ har vi at $r_k \neq 0$ hvis og kun hvis $r = z$. Det vil altså sige, at hvis $r \neq z$, så vil $N(G, r) = N(H, r)$ da begge tal kun afhænger af $s_1 = t_1, ..., s_{k-1} = t_{k-1}$. Derfor vil (9) medføre at $N(G, z) = N(H, z)$. I dette tilfælde er polynomiet givet som

$$\mathcal{F}_z(X_1, ..., X_k) = X_1 \cdots X_{k-1}(X_k - 1);$$

derfor får vi

$$\frac{p^{s_1} \cdots p^{s_{k-1}}(p^{s_k} - 1)}{p^{k-1}(p - 1)} = \frac{p^{t_1} \cdots p^{t_{k-1}}(p^{t_k} - 1)}{p^{k-1}(p - 1)}.$$

Fjerner vi alt, der går ud med hinanden får vi $p^{s_k} = p^{t_k}$, hvilket giver at $S_k = t_k$.

Dette korollar er en stor del af beviset for hoedsætningen i det abelske tilfælde. I det tilfælde hvor ingen af grupperne er abelske benytter man at enhver hamiltonsk 2-gruppe G er isomorf til $G \times \mathbb{Z}_2^r$, for et $r \geqslant 0$ og hvor Q er gruppen af quaternioner. Til sidst vises resultatet i det tilfælde, hvor kun én af grupperne er abelsk ved modstrid.

6.2.2 Normaliserende isomorfier

I 2004 udgav Alberto G. Raggi-Cárdenas og Luis Valero-Elizondo artiklen "Normalizing isomorphisms between Burnside rings" [7]. Denne artikel går videre med at beskrive Burnside-ringens anvendelse inden for karakterisering af opløselige grupper. Igen vil jeg ikke gennemgå beviserne fuldstændigt, da det vil være for omfangsrigt.

Artiklen starter med at definere markhomomorfien, som vi også selv har set det. Til markhomomorfien knytter de følgende formel:

$$\phi_U([G/T]) = \frac{|N_G(U)|}{|T|}\beta(U,T),$$

hvor $\beta(U,T)$ er antallet af undergrupper T, der er G-konjugerede til U. Dette bruger de til at se på de primitive idempotenter i $\prod_{H\in C(G)}\mathbb{Z}$ (spøgelsesringen), hvor de for en undergruppe U i G lader e_U^G være den primitive idempotent i spøgelsesringen, som hører til U. De giver også en explicit formel for den primitive idempotent:

$$e_U^G = \frac{1}{|N_G(U)|}\sum_{T\leqslant U}\mu(T,U)|T|G/T,$$

μ er Möbiusfunktionen til undergruppelatticen for G. Herefter definerer de

$$x_U^G = [U : G'(U)]_0\frac{|N_G(U)|}{|U|}e_U^G,$$

hvor $G'(U)$ er kommutatorundergruppen for U og n_0 er produktet af alle primdivisorer af det hele tal n. Da indekset altid vil være et helt tal, giver dette udtryk mening. Fra Dress og Vellejo ved vi at x_U^G er det mindste heltallige multiplum af e_U^G, der ligger i Burnside-ringen. Bemærk at en isomorfi mellem to burnside-ringe $A(G)$ og $A(G')$ sender hvert x_U^G til et $x_{U'}^{G'}$, så vi får en bijektion $U \mapsto U'$ mellem konjugeringsklasser for undergrupper af G og konjugeringsklasser for undergrupper af G'.

Herefter gentager de en masse resultater om automorfier af Burnside-ringe. De vigtigste resultater dette afsnit er de to følgende sætninger, begge handler om, hvad der sker med de abelske og normale undergrupper af kvadratfri orden med henoldsvis ulige og lige orden, når der findes en automorfi af $A(G)$, der sender x_U^G til x_1^G:

Theorem 11. *Lad G være en endelig gruppe og lad U være en abelsk normal undergruppe af G. Antag at U's orden er ulige og kvadratfri. Da har G ingen anden undergruppe af samme orden som U hvis og kun hvis der findes en automorfi af* $A(G)$*, der sender* x_U^G *til* x_1^G*.*

Theorem 12. *Lad G være en endelig gruppe og lad U være en abelsk normal undergruppe af G. Antag at U's orden er lige og kvadratfri. Da er de følgende to udsagn ækvivalente:*

(i) *G har præcis én undergruppe af orden p for enhver ulige primdivisor p i $|U|$, og Sylow 2-undergruppen af U er indeholdt i enhver undergruppe af G af orden 4.*

(i) *Der eksisterer en automorfi af $A(G)$, der sender x_U^G til x_1^G.*

I det efterfølgende afsnit begynder de at se på isomorfier mellem Burnside-ringe. De vigtigste sætninger, der bruges i beviset for hovedsætningen er de tre følgende:

Proposition 9. *Lad G, G' være endelige grupper og lad $\psi : A(G) \to A(G')$ være en isomorfi mellem deres Burnside-ringe. Hvis $\psi(x_1^G) = x_{U'}^{G'}$ og $\psi^{-1}(x_1^{G'}) = x_{T'}^G$, så er $|U'| = |T|$. Derudover, hvis $|U'|$ er lige, så eksisterer der en isomorfi fra $A(G)$ til $A(G')$, der sender x_1^G til $x_{U_2'}^{G'}$, hvor U_2' er Sylow 2-undergruppen af U'.*

Denne sætning bruges til at konkludere at de egenskaber U' har ved G bliver ført over på G':

Korollar 5. *Lad G, G' være endelige grupper og lad $\psi : A(G) \to A(G')$ være en isomorfi mellem deres Burnside-ringe. Antag $\psi(x_1^G) = x_{U'}^{G'}$, hvor U's orden er ulige. Hvis p er primdivisor i $|U'|$, så har G' en unik undergruppe af orden p. Derudover har G' ingen anden undergruppe af samme orden som U'.*

Den sidste sætning ser på tilfældet, hvor U har lige orden:

Proposition 10. *Lad G, G' være endelige grupper og lad $\psi : A(G) \to A(G')$ være en isomorfi mellem deres Burnside-ringe. Antag $\psi(x_1^G) = x_{U'}^{G'}$. Hvis U' har lige orden, så er Sylow 2-undergruppen af U' en normal undergruppe af G' af orden 2, og den er indeholdt i alle undergrupper af orden 4.*

Disse sætninger giver os mulighed for at bevise vores hovedresultat: at enhver isomorfi mellem to Burnside-ringe kan normaliseres:

Theorem 13. *Lad G, G' være endelige grupper. Hvis deres Burnside-ringe er isomorfe, så findes der en normaliseret isomorfi mellem dem; det vil sige en isomorfi $\Phi : A(G) \to A(G')$ så $\Phi(G/1) = G'/1$.*

Bevis: Lad $\psi : A(G) \to A(G')$ være en isomorfi mellem to Burnside-tinge og lad U' være den abelske normale undergruppe af G' med kvadratfri orden så $\psi(x_1^G) = x_{U'}^{G'}$. Hvis U' har ulige orden får vi fra korollar 4 at G' ikke har andre undergrupper af samme orden som U'. Ved theorem 11 eksisterer der en automorfi α af $A(G')$, så $\alpha(x_{U'}^{G'}) = x_1^{G'}$. Sæt $\Phi = \alpha \otimes \psi$.
Hvis U' har lige orden ved vi af proposition 9, at der eksisterer en isomorfi ρ fra $A(G)$ til $A(G')$, der sender x_1^G til $x_{U_2'}^{G'}$, hvor U_2' er Sylow 2-undergruppen af U'.

Ved proposition 10 ved vi, at U'_2 er en undergruppe af G' af orden 2, og som er indeholdt i alle undergrupper af orden 4 af G'. Ved theorem 12 eksisterer der en automorfi β af $A(G')$, der sender $x^{G'}_{U'_2}$ til $x^{G'}_1$. Sæt $\Phi = \beta \otimes \rho$.

I det næste afsnit benytter de resultaterne fra de tidligere afsnit til nærmere at beskrive de opløselige undergrupper.

Theorem 14. *Lad G, G' være endelige grupper og lad $\Phi : A(G) \to A(G')$ være en normaliseret isomorfi mellem deres Burnside-ringe. For en vilkårlig undergruppe D af G, lad D' være en undergruppe af G' så $\Phi(x_D) = x_{D'}$. Lad U være en opløselig undergruppe af G. Da er U' opløselig, $|U'| = |U|, |N_{G'}(U')| = |N_G(U)|$ og $\Phi(G/U) = G'/U' + \sum_{T \in S_U} a_T G'/T$, hvor S_U er familien af opløselige undergrupper T af G' så $|T|$ er en egentlig divisor i $|U|$.*

Denne sætning er alt for lang til at vise her, men beviset kører efter induktion på ordnen af den opløselige undergruppe U. Tilfældet $|U| = 1$ svarer bare til at Φ er normaliseret, og dette har vi antaget, så induktionsstarten er klar.

Theorem 13 og 14 leder os til sidst frem til følgende korollar:

Korollar 6. *Lad G og G' være to endelige grupper med isomorfe Burnside-ringe. Da er der en én-til-én-korresondance mellem deres konjugeringsklasser af opløselige undergrupper af G og G', der bevarer orden af undergrupper og kardinalitet konjugeringsklasser. Vi kan altså definere en bijektion mellem familierne af opløselige undergrupper af G og G'.*

Bevis: Ved theorem 11 kan vi antage at der eksisterer en normaliseret isomorfi fra $A(G)$ til $A(G')$. Ved theorem 12 ser vi at afbildingen

$$U \mapsto U'$$

giver den ønskede korrespondance.

Det vil altså sige at grupper med isomorfe Burnside-ringe har "de samme opløselige undergrupper".

6.3 En lille løs ende omkring karakterisering af opløselige grupper

I [3], der ligger til grund for mit afsnit om primidealpektrum påstår Dress en gruppe G er minimal simpel hvis og kun hvis dens Burnside-ring har to ikke-dekomposable sammenhængskomponenter og en af dem er isomorf til ringen af hele tal. Hvis dette var sandt ville det heraf følge, at enhver gruppe hvis Burnside-ring er isomorf til Burnside-ringen for en minimal simpel gruppe selv må være en minimal simpel gruppe. Men det viser sig, at der er lille fejl i Dress' argument, som bliver beskrevet af Alberto G. Raggi-Cárdenas of Luis Valero-Elizondo i artiklen "Groups with isomorphic Burnside-rings"fra 2005 [8]. Det er ikke noget, der har indflydelse på det, jeg benytter i opgaven, men for fuldstændighedens skyld er det værd at nævne.

Burnside-ringen for en minimal simpel gruppe må være på formen som beskrevet ovenfor, men Raggi-Cárdenas og Valero-Elizondo kommer med følgende påstand:

Påstand 1. *Burnside-ringen for en gruppe har ovenstående form hvis og kun hvis gruppen er perfekt og alle den egentlige undergrupper er opløselige.*

Bevis: $\Leftarrow$: Hvis G er en perfekt gruppe (det vil sige en er lig sin egen kommutatorgruppe) og alle dens undergrupper er opløselige, så vil G have præcis to konjugeringsklasser af perfekte undergrupper, nemlig sig selv og den trivielle undergruppe og derfor har den Burnside-ring $A(G)$ to primitive idempotenter. Derudover, da G er perfekt følger det at den indekomposable sammenhængskomponent er isomorf til ringen af hele tal.
$\Rightarrow$: Hvis nu omvendt G er en endelig gruppe hvis Burnside-ring har to indekomposable sammenhængskomponenter, hvoraf den ene er isormorf til ringen af hele tal, så har G præcis to konjugeringsklasser af perfekte undergrupper, så G er ikke opløselig, for endelige grupper er kun opløselige såfremt de ikke har nogle ikke-trivielle perfekte undergrupper. Men G må altså have en ikke-triviel perfekt undergruppe, lad os kalde denne undergruppe H. Den indekomposable sammenhængskomponent, der svarer til H må være den, der er isomorf til ringen af hele tal, så $H = N_G(H)$, som nævnt tidligere. Da G ikke er opløselig, må vi have at $H = O^s(G)$, som er den mindste normale undergruppe så kvotientgruppen er en s-gruppe. Men dette er en normal undergruppe af G så $H = N_G(H) = G$ er perfekt. Derudover må enhver egentlig undergruppe af G være i det andet sammenhængskomponent, altså det opløselige sammenhængskomponent, der hører til den trivielle undergruppe. Det vil sige, at alle egentlige undergrupper af G er opløselige. Men dette betyder ikke nødvendigvis at G er simpel. Det kan vi se af følgende modeksempel:

Vi har tidligere i opgaven set på den generelle lineære gruppe. Den specielle lineær gruppe af grad n over et legeme $\mathbb{F}$ er mængden af $n \times n$-matricer med determinant 1. Det er altså en undergruppe af den generelle lineær gruppe. Mere præcist er en normal undergruppe af den trivielle undergruppe. Lad nu G være den specielle lineær gruppe $SL_2(\mathbb{F}_5)$. Det vil sige, at G er mængden af 2×2-matricer med indgange i legemet med 5 elementer. Vi ser først og fremmest at G har orden 120, da vi ved at bruge formlen

$$|SL_2(F_q)| = q^3 - q$$

og så får vi $5^3 - 5 = 120$. Derudover ser at vi at $SL_2(\mathbb{F}_5)$ er perfekt, da vi generelt har at for $n = 2$, så er $SL_n(\mathbb{F}_q)$ perfekt hvis $q > 3$. Dette kommer af at den specielle lineær gruppe er genereret af elementære matricer (matricer på formen $E_{i,j}(\lambda)$, hvor $\lambda \in \mathbb{F}_q, 1 \leqslant i, j \leqslant n, i \neq j$) og enhver elementær $n \times n$-matrix er en kommutator for to elementer i $SL_n(\mathbb{F}_q)$. Derudover kan man vise at G er den eneste perfekte gruppe af orden 120. Dette springer vi over. Undergruppen

$$H = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}\}$$

er centrum for G og den har orden 2 og er isomorf til den cykliske gruppe af orden 2; $\mathbb{Z}/2\mathbb{Z}$. Det kan derudover vises at kvotientgruppen G/H er isomorf til den alternerede gruppe af grad 5; A_5, som vi har set på tidligere. Dette vil tilsammen sige, at kompositionsfaktorerne for G er A_5 og $\mathbb{Z}/2\mathbb{Z}$. Samtidig ser vi at G ikke er simpel, da centret er en normal ikke-triviel undergruppe. Da G er perfekt, har G ingen undergrupper, der er isomorfe til A_5. Derfor har G præcis to konjugeringsklasser af perfekte undergrupper, nemlig den selv og den trivielle undergruppe. Det vil sige at dens Burnside-ring vil have to indekomposable sammenhængskomponenter, hvoraf den ene er isomorf til ringen af hele tal.
Det vil sige, at vi nu har set et eksempel på en gruppe, som ikke er simpel, men som stadig har to indekomposable sammenhængskomponenter, der opfører sig som vi ønskede.

7 Litteraturliste

Litteratur

[1] S. Delsarte. Fonctions de Möbius sur les groupes abeliens finis. *Ann. of Math. (2)*, 49:600–609, 1948.

[2] Satya Deo and K. Varadarajan. Isomorphic Burnside rings. *J. Algebra*, 139(2):468–483, 1991.

[3] Andreas Dress. A characterisation of solvable groups. *Math. Z.*, 110:213–217, 1969.

[4] Andreas W. M. Dress and Ernesto Vallejo. A simple proof for a result by Kratzer and Thévenaz concerning the embedding of the Burnside ring into its ghost ring. *J. Algebra*, 154(2):356–359, 1993.

[5] Helmut Krämer. Über die Automorphismengruppe des Burnsideringes endlicher abelscher Gruppen. *J. Algebra*, 30:279–293, 1974.

[6] Alberto Raggi-Cárdenas and Ernesto Vallejo. Abelian and Hamiltonian groups with isomorphic Burnside rings are isomorphic. *Arch. Math. (Basel)*, 58(2):121–125, 1992.

[7] Alberto G. Raggi-Cárdenas and Luis Valero-Elizondo. Normalizing isomorphisms between Burnside rings. *J. Algebra*, 277(2):643–657, 2004.

[8] Alberto G. Raggi-Cárdenas and Luis Valero-Elizondo. Groups with isomorphic Burnside rings. *Arch. Math. (Basel)*, 84(3):193–197, 2005.

[9] Jacques Thévenaz. Isomorphic Burnside rings. *Comm. Algebra*, 16(9):1945–1947, 1988.

[10] Tammo tom Dieck. *Transformation groups and representation theory*, volume 766 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979.