

# Euler-karakteristik af fusionskategorier for Chevalley-grupper

Martin Wedel Jacobsen

11. februar 2011

Speciale for cand.scient graden i matematik. Institut for matematiske fag, Københavns  
Universitet.

Thesis for the Master degree in Mathematics. Department of Mathematical Sciences, University of  
Copenhagen.

Vejleder: Jesper Michael Møller.

RESUME. Formålet med projektet er at beregne Euler-karakteristikken af visse fusionskategorier for Chevalley-grupper. Jeg giver en kort introduktion til teorien for algebraiske grupper, og beskriver hvordan de endelige grupper af Lie-type kan konstrueres ud fra disse. Derefter introducerer jeg Euler-karakteristik af endelige kategorier, og beskriver hvordan Euler-karakteristikken af fusionskategorier kan beregnes. Jeg beregner dernæst Euler-karakteristikken af fusionssystemet ved  $p$  for Chevalley-gruppen  $\Sigma(q)$  i tilfældet hvor  $q$  er en potens af  $p$  og  $\Sigma$  er enten  $A_1$  eller  $A_2$ . Endelig beregner jeg denne karakteristik i tilfældet hvor  $p \mid q - 1$ ,  $p$  går ikke op i ordenen af Weyl-gruppen  $W(\Sigma)$  og  $\Sigma$  er enten  $A_n$ ,  $B_n$ ,  $C_n$  eller  $D_n$ .

ABSTRACT. The purpose of this project is to calculate the Euler characteristic of certain fusion categories for Chevalley groups. I present a brief introduction to the theory of algebraic groups, and describe how the finite groups of Lie type can be constructed from these. Then I introduce Euler characteristic of finite categories, and describe how the Euler characteristic of fusion categories can be calculated. I next calculate the Euler characteristic of the fusion category at  $p$  for the Chevalley group  $\Sigma(q)$  in the case where  $q$  is a power of  $p$  and  $\Sigma$  is either  $A_1$  or  $A_2$ . Finally I calculate this characteristic in the case where  $p \mid q - 1$ ,  $p$  does not divide the order of the Weyl group  $W(\Sigma)$ , and  $\Sigma$  is one of  $A_n$ ,  $B_n$ ,  $C_n$ , and  $D_n$ .

## Forord

Dette speciale er udarbejdet ved Institut for Matematiske Fag på Københavns Universitet, under vejledning af lektor Jesper Michael Møller. Jeg vil gerne takke Jesper for hans indsigtsfulde vejledning. Vores ugentlige møder har altid været produktive, og jeg værdsætter især den store hjælp jeg har fået med at overskue det omfattende baggrundsmateriale til specialet.

## Indledning

Et velkendt problem inden for gruppeteori er at undersøge om to givne endelige grupper er isomorfe. En delvis klassifikation af de endelige grupper er givet ved deres Sylow- $p$ -undergrupper for hvert primtal  $p$ , men der findes mange eksempler på grupper der ikke er isomorfe, men alligvel har isomorfe Sylow- $p$ -undergrupper for alle  $p$ . Denne klassifikation kan forbedres væsentligt ved at se på  $p$ -fusionssystemer i stedet for Sylow- $p$ -undergrupper.  $p$ -fusionssystemet indeholder ikke bare information om Sylow- $p$ -undergruppen, men også om hvilke undergrupper af denne der er indbyrdes konjugerede i hele gruppen.

Helt uafhængigt af disse overvejelser har Tom Leinster defineret en Euler-karakteristik for endelige kategorier. Et fusionssystem for en gruppe er netop en endelig kategori, og det er dermed muligt at beregne dens Euler-karakteristik. Det er så naturligt at spørge om hvilken information om den oprindelige gruppe der er indkodet i denne karakteristik.

I dette projekt undersøger jeg Euler-karakteristikken af fusionskategorier for Chevalley-grupper. Chevalley-grupperne udgør sammen med Steinberg- og Suzuki-Ree-grupperne de endelige grupper af Lie-type, en stor familie af endelige simple grupper. I første del af projektet præsenterer jeg et udsnit af teorien for algebraiske grupper, herunder klassifikation af semisimple algebraiske grupper ved brug af rodsystemer. I anden del beskriver jeg hvordan grupperne af Lie-type kan konstrueres ud fra simple algebraiske grupper.

I tredje del beskriver jeg definitionen af Euler-karakteristik for endelige kategorier og præsenterer et antal generelle sætninger om Euler-karakteristik af fusionskategorier. Herunder beregner jeg på hvilken måde versionen af en Chevalley-gruppe påvirker Euler-karakteristikken af dens fusionskategorier.

Fjerde del omhandler det kokarakteristiske tilfælde: Euler-karakteristikken af  $p$ -fusionskategorien for Chevalley-gruppen  $\Sigma(q)$ , hvor  $q$  er en potens af  $p$ . Dette viser sig at være ret omstændigt at beregne, selv for relativt små rodsystemer. Jeg beregner karakteristikken i det tilfælde hvor rodsystemet  $\Sigma$  er enten  $A_1$  eller  $A_2$ .

Femte del omhandler det krydskarakteristiske tilfælde: Euler-karakteristikken af  $r$ -fusionskategorien for  $\Sigma(q)$ , hvor  $r$  ikke går op i  $q$ . Der er her mange specialtilfælde; det letteste er det hvor  $r$  går op i  $q - 1$ , og  $r$  ikke går op i ordenen af Weyl-gruppen  $W(\Sigma)$ . Jeg beregner karakteristikken i dette tilfælde for Chevalley-grupper med rodsystem  $A_n$ ,  $B_n$ ,  $C_n$  eller  $D_n$ .

Følgende notation fastholdes gennem hele projektet.  $G \cong H$  angiver at grupperne  $G$  og  $H$  er isomorfe, og  $\mathcal{C} \simeq \mathcal{D}$  angiver at kategorierne  $\mathcal{C}$  og  $\mathcal{D}$  er ækvivalente. Når  $\mathcal{C}$  er en kategori og  $A$  og  $B$  er objekter i  $\mathcal{C}$ , angiver  $\mathcal{C}(A, B)$  mængden af afbildninger fra  $A$  til  $B$ .  $S_n$  er den symmetriske gruppe på  $n$  elementer, og  $C_n$  er den cykliske gruppe af orden  $n$ . Den trivielle gruppe betegnes med  $C_1$ . Når  $G$  er en endelig gruppe og  $p$  et primtal, angiver  $Op(G)$  den mindste undergruppe af  $G$  hvis indeks ikke er deleligt med  $p$ . Når  $g$  og  $x$  er elementer i gruppen  $G$  betegner  ${}^g x$  elementet  $gxg^{-1}$ , og  $x^g$  betegner  $g^{-1}xg$ . Der gælder således  ${}^g x = x^{g^{-1}}$ . Når  $H$  er en undergruppe af  $G$ , er  $C_G(H)$  centralisatoren i  $G$  af  $H$ , og når  $K$  er en anden undergruppe af  $G$ , er  $C_K(H) = K \cap C_G(H)$ . Når en gruppe  $G$  virker på en anden gruppe  $L$  og  $g$  er et element i  $G$ , er  $C_L(g)$  lig gruppen af elementer i  $L$  som er fikspunkter for  $g$ . For  $n \in \mathbb{N}$  er  $n! = \prod_{i=1}^n i$  og  $(2n-1)!! = \prod_{i=1}^n (2i-1)$ .

## Algebraiske grupper

Der findes en ganske omfattende teori for algebraiske grupper, og det ville føre for vidt at give et overblik over hele denne teori. Jeg præsenterer her en kort fremstilling af klassifikationen af semisimple algebraiske grupper samt et antal egenskaber der har relevans for beskrivelsen af grupper af Lie-type.

**Definition 1.** Lad  $\overline{\mathbb{F}}$  være et algebraisk afsluttet legeme. *Zariski-topologien* på  $GL_n(\overline{\mathbb{F}})$  er topologien defineret ved at de lukkede mængder er løsningsmængderne for systemer af polynomielle ligninger i matrixindgangene samt funktionen  $A \mapsto (\det A)^{-1}$ . En *algebraisk gruppe over  $\overline{\mathbb{F}}$*  er en undergruppe  $\overline{K}$  af  $GL_n(\overline{\mathbb{F}})$  som er lukket i Zariski-topologien. Zariski-topologien på  $\overline{K}$  er topologien nedarvet fra  $GL_n(\overline{\mathbb{F}})$ .

For en algebraisk gruppe  $\overline{K}$  defineres den *affine algebra*  $\overline{\mathbb{F}}[\overline{K}]$  til at være  $\overline{\mathbb{F}}$ -algebraen af funktioner  $\overline{K} \rightarrow \overline{\mathbb{F}}$  under punktvis operationer frembragt af matrixindgangene og funktionen  $d$ . Elementerne i  $\overline{\mathbb{F}}[\overline{K}]$  kaldes *polynomielle funktioner* på  $\overline{K}$ . En *morfi af algebraiske grupper*  $\varphi : \overline{K} \rightarrow \overline{H}$  er en gruppehomomorfi som opfylder at for enhver polynomiell funktion  $f$  på  $\overline{H}$  er  $f \circ \varphi$  en polynomiell funktion på  $\overline{K}$ .

Gruppen  $\overline{K}^\circ$  defineres til at være den sammenhængskomponent af  $\overline{K}$  i Zariski-topologien der indeholder identiteten.  $\overline{K}^\circ$  er da i sig selv en algebraisk gruppe. *Dimensionen* af en algebraisk gruppe  $\overline{K}$  er transcendensgraden over  $\overline{\mathbb{F}}$  for kvotientlegemet af  $\overline{\mathbb{F}}[\overline{K}^\circ]$ .

Algebraiske grupper har følgende grundlæggende egenskaber:

**Proposition 1.** *Lad  $\overline{K}$  og  $\overline{L}$  være algebraiske grupper. Da gælder:*

- Hvis  $\overline{H}$  er en lukket undergruppe af  $\overline{K}$ , så er  $\overline{H}$  en algebraisk gruppe, og inklusionen  $\overline{H} \rightarrow \overline{K}$  er en morfi.*
- Hvis ydermere  $\overline{H} \triangleleft \overline{K}$ , så kan  $\overline{K}/\overline{H}$  gives strukturen af en algebraisk gruppe på en sådan måde at projektionen  $\overline{K} \rightarrow \overline{K}/\overline{H}$  er en morfi, og enhver morfi  $\overline{K} \rightarrow \overline{L}$  hvis kerne indeholder  $\overline{H}$  kan faktoriseres unikt som en komposition af projektionen  $\overline{K} \rightarrow \overline{K}/\overline{H}$  og en morfi  $\overline{K}/\overline{H} \rightarrow \overline{L}$ .*
- Kernen og billedet af enhver morfi  $\overline{K} \rightarrow \overline{L}$  er lukkede undergrupper af henholdsvis  $\overline{K}$  og  $\overline{L}$ .*
- Det direkte produkt  $\overline{K} \times \overline{L}$  kan gives strukturen af en algebraisk gruppe på en sådan måde at inklusionerne  $\overline{K} \rightarrow \overline{K} \times \overline{L}$  og  $\overline{L} \rightarrow \overline{K} \times \overline{L}$  og projektionerne  $\overline{K} \times \overline{L} \rightarrow \overline{K}$  og  $\overline{K} \times \overline{L} \rightarrow \overline{L}$  er morfier.*
- Enhver endelig undergruppe af  $\overline{K}$  er lukket.*

*Bevis.* (a)-(d) er [GLS] Proposition 1.1.2(a)-(d). For at vise (e), lad  $\overline{K} \subseteq GL_n(\overline{\mathbb{F}})$  være en algebraisk gruppe, og lad  $A \in \overline{K}$  være en matrix med indgangene  $a_{ij}$ . Lad for hvert  $i$  og  $j$  med  $1 \leq i \leq n$  og  $1 \leq j \leq n$   $m_{ij} : GL_n(\overline{\mathbb{F}}) \rightarrow \overline{\mathbb{F}}$  være funktionen givet ved at  $m_{ij}(X)$  er indgang  $(i, j)$  i  $X$ . Da er  $A$  den unikke løsning til ligningssystemet bestående af de  $n^2$  ligninger  $m_{ij}(X) = a_{ij}$ , og dermed er mængden  $\{A\}$  lukket i Zariski-topologien. Enhver etpunktsmængde er altså lukket, og da endelige mængder er endelige foreninger af etpunktsmængder er disse også lukkede.  $\square$

**Definition 2.** For en algebraisk gruppe  $\overline{K}$  defineres *radikalet*  $R(\overline{K})$  til at være den største normale, lukkede, sammenhængende og opløselige undergruppe af  $\overline{K}$ . En sammenhængende algebraisk gruppe  $\overline{K}$  siges at være *semisimpel* hvis  $R(\overline{K}) = C_1$ , og  $\overline{K}$  siges at være *simpel* hvis  $[\overline{K}, \overline{K}] \neq C_1$  og enhver ægte lukket normal undergruppe af  $\overline{K}$  har dimension 0.

Om simple og semisimple algebraiske grupper gælder følgende sætning:

**Sætning 2.** *Lad  $\bar{K}$  være en sammenhængende algebraisk gruppe. Da gælder:*

- (a) *Hvis  $\bar{K}$  er simpel, er den semisimpel.*
- (b)  *$\bar{K}$  er semisimpel hvis og kun hvis der findes simple undergrupper  $\bar{K}_1, \dots, \bar{K}_s$  af  $\bar{K}$  som opfylder at  $\bar{K} = \bar{K}_1 \bar{K}_2 \cdots \bar{K}_s$  og  $[\bar{K}_i, \bar{K}_j] = C_1$  for  $i \neq j$ . Ydermere er undergrupperne  $\bar{K}_1, \dots, \bar{K}_s$  unikt bestemte i  $\bar{K}$ , og  $Z(\bar{K}) = Z(\bar{K}_1) \cdots Z(\bar{K}_s)$ .*
- (c) *Hvis  $\bar{K}$  er simpel, så er  $Z(\bar{K})$  endelig og indeholder enhver ægte lukket normal undergruppe af  $\bar{K}$ .*
- (d) *Billedet af en (semi)simpel algebraisk gruppe under en morfi er (semi)simpelt.*

*Bevis.* Dette er [GLS] Theorem 1.7.2 (h), (d), (e), (f) og (i). □

Bemærk at en algebraisk gruppe der er simpel ikke nødvendigvis er en simpel gruppe. Dog gælder at en simpel algebraisk gruppe med trivielt center er en simpel gruppe.

Undergrupperne  $\bar{K}_1, \dots, \bar{K}_s$  i Sætning 2(b) kaldes komponenterne af  $\bar{K}$ .  $\bar{K}$  er ikke nødvendigvis det direkte produkt af sine komponenter, da det er muligt at  $\bar{K}_i \cap \bar{K}_j \neq C_1$ . Men der gælder en lidt svagere sætning:

**Sætning 3.** *Lad  $\bar{K}$  være en algebraisk gruppe. Da er  $\bar{K}$  semisimpel hvis og kun hvis der findes simple algebraiske grupper  $\bar{K}_1, \dots, \bar{K}_s$  således at  $\bar{K} \cong (\bar{K}_1 \times \cdots \times \bar{K}_s)/Z$ , hvor  $Z$  er en undergruppe af  $Z(\bar{K}_1) \times \cdots \times Z(\bar{K}_s)$ .*

*Bevis.* Antag at  $\bar{K}$  er semisimpel, og lad  $\bar{K}_1, \dots, \bar{K}_s$  være komponenterne af  $\bar{K}$ . Da  $[\bar{K}_i, \bar{K}_j] = C_1$  findes der en gruppehomomorfi  $\varphi : \bar{K}_1 \times \cdots \times \bar{K}_s \rightarrow \bar{K}$  som opfylder  $\varphi(x_1, \dots, x_s) = x_1 \cdots x_s$  for enhver tuppel  $(x_1, \dots, x_s)$  med  $x_i \in \bar{K}_i$ . Denne homomorfi er surjektiv, da  $\bar{K} = \bar{K}_1 \cdots \bar{K}_s$ . Dermed er  $\bar{K} \cong (\bar{K}_1 \times \cdots \times \bar{K}_s)/\ker(\varphi)$ , og det skal så blot vises at  $\ker(\varphi) \subseteq Z(\bar{K}_1) \times \cdots \times Z(\bar{K}_s)$ .

Lad  $(x_1, \dots, x_s) \in \ker(\varphi)$ . Da gælder  $x_1 \cdots x_s = 1$ , og dermed  $x_1 = (x_2 \cdots x_s)^{-1}$ . Altså er  $x_1 \subseteq \bar{K}_2 \cdots \bar{K}_s$ . Per Sætning 2(b) gælder nu  $[\bar{K}_1, \bar{K}_i] = C_1$ , og så er  $\bar{K}_i \subseteq C_{\bar{K}}(\bar{K}_1)$ . Da dette gælder for alle  $i > 1$  fås  $\bar{K}_2 \cdots \bar{K}_s \subseteq C_{\bar{K}}(\bar{K}_1)$ . Dermed er  $x_1 \in C_{\bar{K}}(\bar{K}_1)$ , og da samtidig  $x_1 \in \bar{K}_1$  fås  $x_1 \in Z(\bar{K}_1)$ . Helt analogt vises  $x_i \in Z(\bar{K}_i)$  for alle andre  $i$ . Dermed er  $(x_1, \dots, x_s) \in Z(\bar{K}_1) \times \cdots \times Z(\bar{K}_s)$ , og så er  $\ker(\varphi) \subseteq Z(\bar{K}_1) \times \cdots \times Z(\bar{K}_s)$ .

Lad nu  $\bar{K}_1, \dots, \bar{K}_s$  være simple grupper, og lad  $\bar{K} = (\bar{K}_1 \times \cdots \times \bar{K}_s)/Z$ , hvor  $Z$  er en undergruppe af  $Z(\bar{K}_1) \times \cdots \times Z(\bar{K}_s)$ . Per Sætning 2(c) er  $Z(\bar{K}_1) \times \cdots \times Z(\bar{K}_s)$  endelig, så  $Z$  er også endelig og dermed lukket.  $\bar{K}$  er altså en algebraisk gruppe. Per Sætning 2(b) er  $\bar{K}_1 \times \cdots \times \bar{K}_s$  semisimpel med komponenter  $\bar{K}_1, \dots, \bar{K}_s$ , og da  $\bar{K}$  er billedet af  $\bar{K}_1 \times \cdots \times \bar{K}_s$  under projektionsmorfi med kerne  $Z$ , er  $\bar{K}$  også semisimpel per Sætning 2(d). □

For at kunne klassificere de forskellige simple algebraiske grupper er det nødvendigt at undersøge deres indre struktur nærmere. To typer af undergrupper viser sig at være særligt interessante i denne sammenhæng.

**Definition 3.** Den algebraiske gruppe  $GL_1(\bar{\mathbb{F}})$  betegnes også  $\bar{\mathbb{F}}^\times$ . En *torus* er en algebraisk gruppe isomorf med det direkte produkt af et antal kopier af  $\bar{\mathbb{F}}^\times$ . Hvis  $\bar{K}$  er en algebraisk gruppe, er en torus i  $\bar{K}$  en undergruppe af  $\bar{K}$  der er en torus. En *maksimal torus* i  $\bar{K}$  er en torus i  $\bar{K}$  der ikke er indeholdt i nogen større torus i  $\bar{K}$ . En *karakter* af en torus  $\bar{T}$  er en morfi  $\bar{T} \rightarrow \bar{\mathbb{F}}^\times$ , og en *kokarakter* er en morfi  $\bar{\mathbb{F}}^\times \rightarrow \bar{T}$ .

**Proposition 4.** *Billedet af en torus under en morfi er en torus. Hvis en torus  $\bar{T}$  er det direkte produkt af  $n$  kopier af  $\bar{\mathbb{F}}^\times$ , så har  $\bar{T}$  dimension  $n$ .*

*Bevis.* Dette er [GLS] Proposition 1.4.2(d) og (c). □

**Sætning 5.** *Lad  $\bar{K}$  være en algebraisk gruppe. Da gælder:*

- (a)  $\bar{K}$  indeholder en maksimal torus.
- (b) Alle maksimale torusser i  $\bar{K}$  er indbyrdes konjugerede.
- (c) Enhver torus i  $\bar{K}$  er indeholdt i en maksimal torus i  $\bar{K}$ .

*Bevis.* Dette er [GLS] Theorem 1.4.3(a)-(c). □

**Definition 4.** Undergruppen af  $GL_2(\bar{\mathbb{F}})$  bestående af matricerne på formen  $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$  betegnes med  $\bar{\mathbb{F}}^+$ . Elementet  $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$  i  $\bar{\mathbb{F}}^+$  betegnes også med  $t$ . En *énparametergruppe* er en algebraisk gruppe isomorf med  $\bar{\mathbb{F}}^+$ . En *parametrisering* af en énparametergruppe  $\bar{X}$  er en surjektiv homomorfi fra  $\bar{\mathbb{F}}^+$  til  $\bar{X}$ .

**Sætning 6.** *Lad  $\bar{X}$  være en énparametergruppe og lad  $x : \bar{\mathbb{F}}^+ \rightarrow \bar{X}$  være en parametrisering af  $\bar{X}$ . For ethvert  $c \in \bar{\mathbb{F}}^\times$  er  $t \mapsto x(ct)$  så også en parametrisering af  $\bar{X}$ , og enhver parametrisering af  $\bar{X}$  har denne form for passende  $c$ .*

*Bevis.* Dette er [GLS] Proposition 1.3.5(a). □

**Definition 5.** Lad  $\bar{K}$  være en algebraisk gruppe med maksimal torus  $\bar{T}$ . En  $\bar{T}$ -rodgruppe i  $\bar{K}$  er en énparametergruppe i  $\bar{K}$  der normaliseres af  $\bar{T}$ .

Interessen for  $\bar{T}$ -rodgrupper kommer af følgende resultat:

**Sætning 7.** *Lad  $\bar{K}$  være en semisimpel algebraisk gruppe med maksimal torus  $\bar{T}$ , og lad  $\mathcal{M}$  være mængden af  $\bar{T}$ -rodgrupper i  $\bar{K}$ . Da er  $\bar{K} = \langle \bar{X} \mid \bar{X} \in \mathcal{M} \rangle$ .*

*Bevis.* Per [GLS] Theorem 1.10.1(a) er  $\langle \bar{X} \mid \bar{X} \in \mathcal{M} \rangle = [\bar{K}, \bar{K}]$ , og per [GLS] Theorem 1.7.2(c) er  $\bar{K}$  produktet af  $[\bar{K}, \bar{K}]$  og  $Z(\bar{K})^\circ$ , så det skal blot bevises at  $Z(\bar{K})^\circ = C_1$ . Af Sætning 2(c) og (b) følger det at  $Z(\bar{K})$  er endelig. Proposition 1(e) giver så at enhver delmængde af  $Z(\bar{K})$  er lukket, og så må  $Z(\bar{K})^\circ = C_1$ . □

For at beskrive de nærmere relationer mellem  $\bar{T}$ -rodgrupperne er det nødvendigt først at gennemgå teorien for rodsystemer i Euklidiske rum. Det viser sig nemlig at mængden af  $\bar{T}$ -rodgrupper er i en-til-en-korrespondance med et sådant rodsystem, og rodsystemets struktur beskriver en række relationer mellem rodgrupperne.

## Rodsystemer

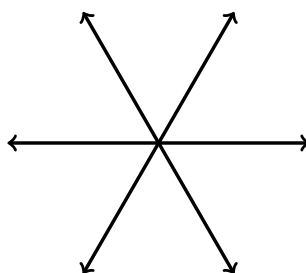
Lad  $\mathbb{E}^n$  betegne  $\mathbb{R}^n$  med et indre produkt  $(\cdot, \cdot)$ . For ethvert  $\alpha, \beta \in \mathbb{E}^n$  med  $\beta \neq 0$  definerer vi  $\langle \alpha, \beta \rangle = 2(\alpha, \beta)/(\beta, \beta)$ . Lad for ethvert  $\beta \in \mathbb{E}^n$  afbildningen  $r_\beta : \mathbb{E}^n \rightarrow \mathbb{E}^n$  være givet ved  $r_\beta(\alpha) = \alpha - \langle \alpha, \beta \rangle \beta$ . Da er  $r_\beta$  netop spejling i hyperplanen  $\beta^\perp$ , og dermed specielt en isometri.

**Definition 6.** Et *rodsystem* er en endelig mængde  $\Sigma$  af elementer i  $\mathbb{E}^n$ , alle forskellige fra 0, således at for ethvert  $\alpha \in \Sigma$  er  $r_\alpha(\Sigma) = \Sigma$ . En *isomorfi* mellem rodsystemer  $\Sigma$  og  $\Sigma'$  er en bijektion  $f : \Sigma \rightarrow \Sigma'$  som opfylder  $\langle f(\alpha), f(\beta) \rangle = \langle \alpha, \beta \rangle$  for alle  $\alpha, \beta \in \Sigma$ .  $\Sigma$  siges at være *reduceret* hvis det gælder at hvis  $\alpha \in \Sigma$ ,  $c \in \mathbb{R}$  og  $c\alpha \in \Sigma$ , så er  $c = \pm 1$ .  $\Sigma$  siges at være *krystallografisk* hvis  $\langle \alpha, \beta \rangle \in \mathbb{Z}$  for alle  $\alpha, \beta \in \Sigma$ . I resten af dette afsnit forudsættes det at alle rodsystemer er reducerede og krystallografiske.

Når  $X$  er en delmængde af  $\mathbb{E}^n$  betegner  $\mathbb{R}X$  delrummet af  $\mathbb{E}^n$  udspændt af  $X$ , og *dimensionen* af  $\Sigma$  defineres til at være dimensionen af  $\mathbb{R}\Sigma$ . *Weyl-gruppen* for  $\Sigma$  er  $\langle r_\alpha \mid \alpha \in \Sigma \rangle$ . Den er en undergruppe af gruppen af isometrier af  $\mathbb{E}^n$ , og en undergruppe af gruppen af permutationer på  $\Sigma$ .

En delmængde  $\Sigma_0$  af et rodsystem  $\Sigma$  siges at være *lukket* hvis det gælder at hvis  $\alpha, \beta \in \Sigma_0$  og  $\alpha + \beta \in \Sigma$ , så er  $\alpha + \beta \in \Sigma_0$ . Et *positivt delsystem*  $\Sigma^+$  af  $\Sigma$  er en lukket delmængde som opfylder at for ethvert  $\alpha \in \Sigma$  er  $\alpha \in \Sigma^+$  hvis og kun hvis  $-\alpha \notin \Sigma^+$ . Et *fundamentalt system* i  $\Sigma$  hørende til et positivt delsystem  $\Sigma^+$  er en delmængde  $\Pi$  af  $\Sigma^+$  med  $\dim(\Sigma)$  elementer som opfylder at ethvert element i  $\Sigma^+$  kan skrives som en linearkombination af elementerne i  $\Pi$  med ikke-negative koefficienter.

**Eksempel 1.** Rodsystemet  $A_2$  består af seks rødder, arrangeret som vist i  $\mathbb{E}^2$  med det sædvanlige indre produkt:



De seks rødder har koordinaterne  $(\pm 2, 0)$  og  $(\pm 1, \pm \sqrt{3})$ . Rodsystemet er oplagt reduceret, og det er også krystallografisk. Eksempelvis er  $\langle (2, 0), (-1, \sqrt{3}) \rangle = 2 \cdot \frac{((2,0),(-1,\sqrt{3}))}{((-1,\sqrt{3}),(-1,\sqrt{3}))} = 2 \cdot \frac{2 \cdot (-1) + 0 \cdot \sqrt{3}}{(-1)^2 + \sqrt{3}^2} = 2 \cdot \frac{-2}{4} = -1$ .

Rodsystemets dimension er 2, og dets Weyl-gruppe har orden 6 og er isomorf med den symmetriske gruppe  $S_3$ . Lad  $\alpha = (2, 0)$  og  $\beta = (-1, \sqrt{3})$ . Et muligt positivt delsystem er mængden  $\{\alpha, \beta, \alpha + \beta\}$ , og det tilhørende fundamentale system er  $\{\alpha, \beta\}$ . De tre øvrige rødder i  $A_2$  er netop  $-\alpha$ ,  $-\beta$  og  $-(\alpha + \beta)$ .

**Sætning 8.** Ethvert rodsystem  $\Sigma$  har mindst et positivt delsystem, og enhver positivt delsystem i  $\Sigma$  har et unikt tilhørende fundamentalt system. Ydermere permuterer  $W(\Sigma)$  de fundamentale systemer for  $\Sigma$  regulært. Med andre ord gælder at hvis  $\Pi$  er et fundamentalt system for  $\Sigma$ , så er ethvert fundamentalt system på formen  $w(\Pi)$  med  $w \in W$ , og der gælder  $w_1(\Pi) = w_2(\Pi)$  hvis og kun hvis  $w_1 = w_2$ .



*Bevis.* Dette er [GLS] Theorem 1.8.2. □

**Sætning 9.** Lad  $\Sigma$  være et rodsystem, og lad  $\Sigma^+$  være et positivt delsystem for  $\Sigma$  med tilhørende fundamentalt system  $\Pi$ . Da er  $-\Sigma^+ = \{-\alpha \mid \alpha \in \Sigma^+\}$  et positivt delsystem af  $\Sigma$  med tilhørende fundamentalt system  $-\Pi$ .

*Bevis.* Dette følger direkte af definitionerne af positivt delsystem og fundamentalt system. □

**Sætning 10.** Lad  $\Sigma$  være et rodsystem i  $\mathbb{E}^n$  med fundamentalt system  $\Pi$ . Da gælder:

- (a)  $\Pi$  er en basis for  $\mathbb{R}\Sigma$ .
- (b)  $(\alpha, \beta) \leq 0$  for alle  $\alpha, \beta \in \Pi$  med  $\alpha \neq \beta$ .
- (c)  $W = \langle r_\alpha \mid \alpha \in \Pi \rangle$ .
- (d) Lad  $\mathbb{E}$  være et delrum af  $\mathbb{E}^n$ ; da er  $\Sigma \cap \mathbb{E}$  et rodsystem.

*Bevis.* Dette er [GLS] Theorem 1.8.3(a), (b) og (g). □

**Definition 7.** En ortogonal dekomposition af et rodsystem  $\Sigma$  er en partition  $\Sigma = \Sigma_1 \cup \dots \cup \Sigma_k$  som opfylder at hvis  $\alpha \in \Sigma_i$ ,  $\beta \in \Sigma_j$  og  $i \neq j$ , så er  $\alpha \perp \beta$ . Et rodsystem siges at være *irreducibelt* hvis den eneste ortogonale dekomposition er den trivielle dekomposition ( $k = 1$ ).

**Sætning 11.** Lad  $\Sigma$  være et rodsystem. Da gælder:

- (a) Der findes en unik ortogonal dekomposition  $\Sigma_1 \cup \dots \cup \Sigma_k$  af  $\Sigma$  med hvert  $\Sigma_i$  irreducibelt. En delmængde  $\Pi$  af  $\Sigma$  er et fundamentalt system for  $\Sigma$  hvis og kun hvis  $\Pi \cap \Sigma_i$  er et fundamentalt system for  $\Sigma_i$  for hvert  $i$ .
- (b) Lad  $\Sigma$  og  $\Sigma'$  være rodsystemer med fundamentale systemer  $\Pi$  og  $\Pi'$  og antag at  $\Sigma$  er irreducibelt. Da er  $\Sigma$  og  $\Sigma'$  isomorfe hvis og kun hvis der findes en afbildning  $H : \mathbb{R}\Sigma \rightarrow \mathbb{R}\Sigma'$  bestående af en isometri efterfulgt af en skalering således at  $H(\Pi) = \Pi'$ . I dette tilfælde er  $H(\Sigma) = \Sigma'$ .
- (c) En bijektion  $f : \Sigma \rightarrow \Sigma'$  mellem rodsystemer er en isomorfi hvis og kun hvis den bevarer addition og negation, dvs. hvis og kun hvis  $f(-\alpha) = -f(\alpha)$  for ethvert  $\alpha \in \Sigma$  og  $f(\alpha + \beta) = f(\alpha) + f(\beta)$  for alle  $\alpha, \beta \in \Sigma$  med  $\alpha + \beta \in \Sigma$ .
- (d) Lad  $\Sigma^+$  være et positivt delsystem af  $\Sigma$  med tilhørende fundamentalt system  $\Pi$ , og lad  $\text{ht}_\Pi : \mathbb{R}\Sigma \rightarrow \mathbb{R}$  være den unikke lineære funktional der opfylder  $\text{ht}_\Pi(\alpha) = 1$  for alle  $\alpha \in \Pi$ . Da er  $\text{ht}_\Pi(\alpha)$  et heltal for alle  $\alpha \in \Sigma$ . Ydermere er  $\text{ht}_\Pi(\alpha) > 0$  hvis og kun hvis  $\alpha \in \Sigma^+$ .

*Bevis.* Dette er [GLS] Theorem 1.8.5, bortset fra påstanden om fortegnet af  $\text{ht}_\Pi(\alpha)$ . Denne påstand følger af definitionen på et fundamentalt system. Lad nemlig  $\alpha \in \Sigma^+$  og lad  $\alpha_1, \dots, \alpha_n$  være elementerne i  $\Pi$ . Da kan  $\alpha$  skrives på formen  $\sum_{i=1}^n c_i \alpha_i$  med  $c_i \geq 0$ . Så er  $\text{ht}_\Pi(\alpha) = \sum_{i=1}^n c_i \text{ht}_\Pi(\alpha_i) = \sum_{i=1}^n c_i \geq 0$ . Hvis  $\text{ht}_\Pi(\alpha) = 0$  ville der gælde  $c_i = 0$  for hvert  $i$ , og så ville  $\alpha = 0$ , hvilket er umuligt. Altså er  $\text{ht}_\Pi(\alpha) > 0$ . Endelig ses at hvis  $\alpha \notin \Sigma^+$ , så er  $-\alpha \in \Sigma^+$ , og så er  $\text{ht}_\Pi(\alpha) = -\text{ht}_\Pi(-\alpha) < 0$ . □

**Sætning 12.** Lad  $\Sigma_1 \cup \dots \cup \Sigma_k$  være en ortogonal dekomposition af  $\Sigma$ . Da er  $W(\Sigma) = W(\Sigma_1) \times \dots \times W(\Sigma_k)$  og  $\dim(\Sigma) = \dim(\Sigma_1) + \dots + \dim(\Sigma_k)$ .

*Bevis.* Påstandene bevises her i tilfældet  $k = 2$ ; det generelle tilfælde følger da ved induktion.

Lad  $\Sigma_1 \cup \Sigma_2$  være en ortogonal dekomposition af  $\Sigma$ . Da er  $W(\Sigma_1) = \langle r_\alpha \mid \alpha \in \Sigma_1 \rangle \subseteq \langle r_\alpha \mid \alpha \in \Sigma \rangle = W(\Sigma)$ , og tilsvarende er  $W(\Sigma_2) \subseteq W(\Sigma)$ . Ydermere er  $\langle W(\Sigma_1), W(\Sigma_2) \rangle = \langle r_\alpha \mid \alpha \in \Sigma_1 \cup \Sigma_2 \rangle = W(\Sigma)$ . Det er så tilstrækkeligt at vise at  $W(\Sigma_1) \cap W(\Sigma_2) = C_1$  og at ethvert element i  $W(\Sigma_1)$  kommuterer med ethvert element i  $W(\Sigma_2)$ .

Lad  $\alpha \in \Sigma_1$ . Da er  $\beta \perp \alpha$  for ethvert  $\beta \in \Sigma_2$ , og så er  $r_\alpha(\beta) = \beta$ . Da elementerne  $r_\alpha$  med  $\alpha \in \Sigma_1$  frembringer  $W(\Sigma_1)$  fås så  $w(\beta) = \beta$  for ethvert  $w \in W(\Sigma_1)$  og  $\beta \in \Sigma_2$ . Tilsvarende fås  $w(\beta) = \beta$  for ethvert  $w \in W(\Sigma_2)$  og  $\beta \in \Sigma_1$ . Såfremt  $w \in W(\Sigma_1) \cap W(\Sigma_2)$  gælder altså  $w(\beta) = \beta$  for ethvert  $\beta \in \Sigma_1 \cup \Sigma_2 = \Sigma$ , og  $w$  er hermed identitetselementet. Altså er  $W(\Sigma_1) \cap W(\Sigma_2) = C_1$ .

Lad nu  $\alpha \in \Sigma_1$  og  $\beta \in \Sigma_2$ , og lad  $x$  være et vilkårligt element i  $\mathbb{E}^n$ . Da er  $(\beta, \alpha) = 0$  idet  $\alpha \perp \beta$ , og der gælder

$$\begin{aligned} r_\alpha(r_\beta(x)) &= r_\alpha(x - \langle x, \beta \rangle \beta) = (x - \langle x, \beta \rangle \beta) - \langle x - \langle x, \beta \rangle \beta, \alpha \rangle \alpha \\ &= x - \langle x, \beta \rangle \beta - 2(x - \langle x, \beta \rangle \beta, \alpha) / (\alpha, \alpha) \alpha \\ &= x - \langle x, \beta \rangle \beta - 2((x, \alpha) - \langle x, \beta \rangle (\beta, \alpha)) / (\alpha, \alpha) \alpha \\ &= x - \langle x, \beta \rangle \beta - 2(x, \alpha) / (\alpha, \alpha) \alpha \\ &= x - \langle x, \beta \rangle \beta - \langle x, \alpha \rangle \alpha \end{aligned}$$

Med en tilsvarende udregning fås  $r_\beta(r_\alpha(x)) = x - \langle x, \alpha \rangle \alpha - \langle x, \beta \rangle \beta$ , og dermed er  $r_\beta(r_\alpha(x)) = r_\alpha(r_\beta(x))$  for alle  $x \in \mathbb{E}^n$ . Altså kommuterer  $r_\alpha$  med  $r_\beta$ . Idet  $W(\Sigma_1)$  er frembragt af elementerne  $r_\alpha$  med  $\alpha \in \Sigma_1$  og  $W(\Sigma_2)$  er frembragt af elementerne  $r_\beta$  med  $\beta \in \Sigma_2$  følger det at ethvert element i  $W(\Sigma_1)$  kommuterer med ethvert element i  $W(\Sigma_2)$ . Altså er  $W(\Sigma) = W(\Sigma_1) \times W(\Sigma_2)$ .

For ethvert  $\alpha \in \Sigma_1$  og  $\beta \in \Sigma_2$  gælder  $\alpha \perp \beta$ , hvoraf fås  $x \perp y$  for ethvert  $x \in \mathbb{R}\Sigma_1$  og  $y \in \mathbb{R}\Sigma_2$ . Specielt gælder at hvis  $x \in \mathbb{R}\Sigma_1 \cap \mathbb{R}\Sigma_2$ , så er  $x \perp x$ , og dermed er  $x = 0$ . Altså er  $\mathbb{R}\Sigma_1 \cap \mathbb{R}\Sigma_2 = \{0\}$ . Ydermere udspænder  $\mathbb{R}\Sigma_1$  og  $\mathbb{R}\Sigma_2$  tilsammen  $\mathbb{R}\Sigma$ , så  $\mathbb{R}\Sigma = \mathbb{R}\Sigma_1 \oplus \mathbb{R}\Sigma_2$ . Altså er  $\dim(\Sigma) = \dim(\Sigma_1) + \dim(\Sigma_2)$ .  $\square$

Det viser sig at ud fra et fundamentalt system for et rodsystem kan man rekonstruere hele rodsystemet. Den relevante information fra det fundamentale system kan indkodes i et såkaldt Dynkin-diagram.

**Definition 8.** *Dynkin-diagrammet* for et rodsystem  $\Sigma$  defineres som følger. Lad  $\Pi$  være et vilkårligt fundamentalt system for  $\Sigma$ . Knuderne i Dynkin-diagrammet er elementerne i  $\Pi$ , og to knuder  $\alpha$  og  $\beta$  er forbundet med en kant af vægt  $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle$ . Hvis  $|\alpha| > |\beta|$  og  $\alpha$  og  $\beta$  ikke står vinkelret på hinanden, så er kanten mellem  $\alpha$  og  $\beta$  orienteret i retning mod  $\beta$ ; i modsat fald er kanten ikke orienteret. En *isomorfi* mellem Dynkin-diagrammer er en bijektion mellem knudemængder der bevarer vægt og orientering af alle kanter.

**Eksempel 2.** Betragt igen rodsystemet  $A_2$  fra Eksempel 1, og betragt det fundamentale system  $\{\alpha, \beta\}$ . Der gælder  $(\alpha, \alpha) = 2^2 + 0^2 = 4$  og  $(\beta, \beta) = (-1)^2 + (\sqrt{3})^2 = 4$ , så  $\alpha$  og  $\beta$  har samme længde. Desuden er  $(\alpha, \beta) = (\beta, \alpha) = (-1) \cdot 2 + (\sqrt{3}) \cdot 0 = -2$ . Så er  $\langle \alpha, \beta \rangle = \frac{2(\alpha, \beta)}{(\beta, \beta)} = \frac{2 \cdot (-2)}{4} = -1$  og  $\langle \beta, \alpha \rangle = \frac{2(\beta, \alpha)}{(\alpha, \alpha)} = \frac{2 \cdot (-2)}{4} = -1$ , og dermed er  $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle = 1$ . Altså består Dynkin-diagrammet for  $A_2$  af to knuder forbundet af en ikke orienteret kant med vægt 1.

Sætning 8 giver at ethvert fundamentalt system kan føres over i ethvert andet fundamentalt system via en isometri, og Dynkin-diagrammet er dermed uafhængigt af valg af fundamentalt system.  $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle$  er et heltal da rodsystemet er krystallografisk, og der gælder  $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle =$

$4 \frac{(\alpha, \beta)(\beta, \alpha)}{(\beta, \beta)(\alpha, \alpha)} = 4 \left( \frac{(\alpha, \beta)}{|\alpha||\beta|} \right)^2 = 4 \cos^2 \theta$  hvor  $\theta$  er vinklen mellem  $\alpha$  og  $\beta$ . Dynkin-diagrammet indkoder dermed blot vinklerne mellem rødderne i et fundamentalt system samt nogle oplysninger om de relative længder af rødderne. Dette viser sig at være nok til at rekonstruere rodsystemet:

**Sætning 13.** *To rodsystemer  $\Sigma$  og  $\Sigma'$  er isomorfe hvis og kun hvis deres Dynkin-diagrammer er isomorfe. Mere præcist gælder at hvis  $\Pi$  og  $\Pi'$  er fundamentale systemer for hhv.  $\Sigma$  og  $\Sigma'$ , så kan en bijektion  $f : \Pi \rightarrow \Pi'$  udvides til en isomorfi fra  $\Sigma$  til  $\Sigma'$  hvis og kun hvis  $f$  er en isomorfi mellem Dynkin-diagrammerne for  $\Sigma$  og  $\Sigma'$ .*

*Bevis.* Dette er første del af [GLS] Theorem 1.8.7. □

Dynkin-diagrammet gør det også let at afgøre om et rodsystem er reducibelt:

**Sætning 14.** *Lad  $\Sigma_1 \cup \dots \cup \Sigma_k$  være en ortogonal dekomposition af  $\Sigma$ . Da er Dynkin-diagrammet for  $\Sigma$  en disjunkt forening af Dynkin-diagrammerne for  $\Sigma_1, \dots, \Sigma_k$ .*

*Bevis.* Lad  $\Pi$  være et fundamentalt system for  $\Sigma$ ; per Sætning 11 kan  $\Pi$  så skrives som en disjunkt forening  $\Pi_1 \cup \dots \cup \Pi_k$  hvor  $\Pi_i$  er et fundamentalt system for  $\Sigma_i$ . Givet  $\alpha, \beta \in \Pi_i$  gælder at forbindelsen mellem dem i Dynkin-diagrammet er fastlagt alene ud fra vinklen mellem dem og deres relative længde, og disse data ændrer sig ikke når  $\alpha$  og  $\beta$  betragtes som elementer af  $\Pi$  i stedet. Desuden gælder at hvis  $\alpha \in \Pi_i$  og  $\beta \in \Pi_j$  med  $i \neq j$ , så er  $\alpha \perp \beta$ . Dermed er  $\langle \alpha, \beta \rangle = 0$ , så der er ingen kant fra  $\alpha$  til  $\beta$  i Dynkin-diagrammet for  $\Sigma$ . Altså er Dynkin-diagrammet for  $\Sigma$  en disjunkt forening af Dynkin-diagrammerne for  $\Sigma_1, \dots, \Sigma_k$ . □

**Sætning 15.** *Lad  $D$  være Dynkin-diagrammet for  $\Sigma$ , og antag at  $D$  kan skrives som en disjunkt forening  $D_1 \cup \dots \cup D_k$ . Da gælder for hvert  $i$  at  $\mathbb{R}D_i$  er det samme rum uanset hvilket fundamentalt system for  $\Sigma$  der bruges til at konstruere Dynkin-diagrammet. Ydermere er  $(\mathbb{R}D_1 \cap \Sigma) \cup \dots \cup (\mathbb{R}D_k \cap \Sigma)$  en ortogonal dekomposition af  $\Sigma$ .*

*Bevis.* Påstanden bevises her i tilfældet  $k = 2$ ; det generelle tilfælde følger da ved induktion.

Lad  $\Pi$  være et fundamentalt system for  $\Sigma$ , og konstruer  $D$  ud fra  $\Pi$ . Antag at  $D$  kan skrives som en disjunkt forening  $D_1 \cup D_2$ , og lad  $\Pi_1 \cup \Pi_2$  være den tilhørende partition af  $\Pi$ . Lad  $\alpha \in \Pi_1$ ; da gælder  $\alpha \perp \beta$  for ethvert  $\beta \in \Pi_2$  idet der ikke er nogen kant fra  $\alpha$  til  $\beta$  i  $D$ . Dermed gælder også  $\alpha \perp x$  for ethvert  $x \in \mathbb{R}\Pi_2$ , og så er  $r_\alpha(x) = x$  for ethvert  $x \in \mathbb{R}\Pi_2$ . Specielt er  $r_\alpha(\mathbb{R}\Pi_2) = \mathbb{R}\Pi_2$ .

Definer nu  $\mathbb{E}_\alpha = \{x \in \mathbb{R}\Pi_1 \mid x \perp \alpha\}$ . Da kan ethvert element i  $\mathbb{R}\Pi_1$  unikt skrives på formen  $x + c\alpha$  med  $x \in \mathbb{E}_\alpha$  og  $c \in \mathbb{R}$ , og der gælder  $r_\alpha(x + c\alpha) = x - c\alpha$ . Altså er  $r_\alpha(\mathbb{R}\Pi_1) = \mathbb{R}\Pi_1$ . For ethvert  $\alpha \in \Pi_1$  gælder altså  $r_\alpha(\mathbb{R}\Pi_1) = \mathbb{R}\Pi_1$  og  $r_\alpha(\mathbb{R}\Pi_2) = \mathbb{R}\Pi_2$ , og på helt tilsvarende vis fås at dette også gælder for ethvert  $\alpha \in \Pi_2$ . Per Sætning 10(c) er  $W(\Sigma)$  frembragt af elementerne  $r_\alpha$  med  $\alpha \in \Pi_1 \cup \Pi_2$ , og dermed fås at for ethvert  $w \in W(\Sigma)$  er  $w(\mathbb{R}\Pi_1) = \mathbb{R}\Pi_1$  og  $w(\mathbb{R}\Pi_2) = \mathbb{R}\Pi_2$ .

Sætning 8 giver nu at hvis  $\Pi'$  er et andet fundamentalt system for  $\Sigma$ , så findes der et  $w \in W(\Sigma)$  så  $\Pi' = w(\Pi)$ . Hvis  $D$  konstrueres ud fra  $\Pi'$ , vil partitionen af  $\Pi'$  hørende til opdelingen  $D_1 \cup D_2$  så være  $w(\Pi_1) \cup w(\Pi_2)$ . Men nu gælder  $\mathbb{R}(w(\Pi_1)) = w(\mathbb{R}\Pi_1) = \mathbb{R}\Pi_1$ , så  $\mathbb{R}D_1$  er det samme rum uanset hvilket fundamentalt system der bruges til at konstruere  $D$ . Tilsvarende ses at  $\mathbb{R}D_2$  er uafhængigt af valget af fundamentalt system.

Da  $\alpha \perp \beta$  for ethvert  $\alpha \in \Pi_1$  og  $\beta \in \Pi_2$  gælder  $x \perp y$  for ethvert  $x \in \mathbb{R}D_1$  og  $y \in \mathbb{R}D_2$ . Specielt gælder  $\alpha \perp \beta$  for ethvert  $\alpha \in \mathbb{R}D_1 \cap \Sigma$  og  $\beta \in \mathbb{R}D_2 \cap \Sigma$ . Dermed er  $(\mathbb{R}D_1 \cap \Sigma) \cup (\mathbb{R}D_2 \cap \Sigma)$  en ortogonal dekomposition af  $\Sigma$  hvis ethvert element i  $\Sigma$  er indeholdt i enten  $\mathbb{R}D_1$  eller  $\mathbb{R}D_2$ .

Lad nu  $\alpha \in \Sigma$  og skriv  $\alpha$  på formen  $x + y$  med  $x \in \mathbb{R}D_1$  og  $y \in \mathbb{R}D_2$ ; dette kan lade sig gøre da  $\mathbb{R}D_1$  og  $\mathbb{R}D_2$  tilsammen udspænder  $\mathbb{R}\Sigma$ . Så gælder

$$\begin{aligned} r_\alpha(x) &= x - \langle x, \alpha \rangle \alpha = x - 2 \frac{(x, \alpha)}{(\alpha, \alpha)} \alpha = x - 2 \frac{(x, x) + (x, y)}{(\alpha, \alpha)} (x + y) \\ &= x - 2 \frac{(x, x)}{(\alpha, \alpha)} x - 2 \frac{(x, y)}{(\alpha, \alpha)} y \end{aligned}$$

Da  $r_\alpha \in W(\Sigma)$  er  $r_\alpha(\mathbb{R}D_1) = \mathbb{R}D_1$ ; specielt er  $r_\alpha(x) \in \mathbb{R}D_1$ . Da der oplagt gælder  $x - 2 \frac{(x, x)}{(\alpha, \alpha)} x \in \mathbb{R}D_1$  fås så  $2 \frac{(x, x)}{(\alpha, \alpha)} y \in \mathbb{R}D_1$ . Men da der også gælder  $2 \frac{(x, x)}{(\alpha, \alpha)} y \in \mathbb{R}D_2$  fås  $(2 \frac{(x, x)}{(\alpha, \alpha)} y) \perp (2 \frac{(x, x)}{(\alpha, \alpha)} y)$  og dermed  $2 \frac{(x, x)}{(\alpha, \alpha)} y = 0$ . Så må enten  $y = 0$  eller  $x = 0$ , og dermed er  $\alpha$  indeholdt i enten  $\mathbb{R}D_1$  eller  $\mathbb{R}D_2$ .  $\square$

Rodsystemer er således perfekt beskrevet ved Dynkin-diagrammer, og en ortogonal dekomposition af et rodssystem med irreducible komponenter svarer blot til en opdeling af Dynkin-diagrammet i sammenhængskomponenter. Tilbage er så kun at opskrive de mulige irreducible rodssystemer.

**Sætning 16** (Standardformer for irreducible rodssystemer). *Ethvert irreducibelt rodssystem er isomorft med netop ét af nedenstående rodssystemer. I denne liste er  $e_1, \dots, e_n$  en ortonormalbasis for  $\mathbb{E}^n$ , og  $\mathbf{S}_n$  er mængden af  $n$ -vektorer  $(\varepsilon_1, \dots, \varepsilon_n)$  som opfylder  $\varepsilon_i = \pm 1$  for hvert  $i$ . For et  $\varepsilon \in \mathbf{S}_n$  defineres  $e_\varepsilon$  ved  $e_\varepsilon = \frac{1}{2} \sum_{i=1}^n \varepsilon_i e_i$ .  $A_n$  er defineret for  $n \geq 1$ ,  $B_n$  for  $n \geq 2$ ,  $C_n$  for  $n \geq 3$  og  $D_n$  for  $n \geq 4$ . For hvert rodssystem angives desuden et muligt fundamentalt system  $\Pi$ .*

$$\begin{aligned} A_n: \Sigma &= \{\pm(e_i - e_j) \mid 1 \leq i < j \leq n + 1\} \\ \Pi &= \{e_i - e_{i+1} \mid 1 \leq i \leq n\} \end{aligned}$$

$$\begin{aligned} B_n: \Sigma &= \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\} \cup \{\pm e_i \mid 1 \leq i \leq n\} \\ \Pi &= \{e_i - e_{i+1} \mid 1 \leq i \leq n - 1\} \cup \{e_n\} \end{aligned}$$

$$\begin{aligned} C_n: \Sigma &= \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\} \cup \{\pm 2e_i \mid 1 \leq i \leq n\} \\ \Pi &= \{e_i - e_{i+1} \mid 1 \leq i \leq n - 1\} \cup \{2e_n\} \end{aligned}$$

$$\begin{aligned} D_n: \Sigma &= \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\} \\ \Pi &= \{e_i - e_{i+1} \mid 1 \leq i \leq n - 1\} \cup \{e_{n-1} + e_n\} \end{aligned}$$

$$\begin{aligned} E_8: \Sigma &= \{\pm e_i \pm e_j \mid 1 \leq i < j \leq 8\} \cup \{e_\varepsilon \mid \varepsilon \in \mathbf{S}_8, \prod_{i=1}^8 \varepsilon_i = 1\} \\ \Pi &= \{e_i - e_{i+1} \mid 2 \leq i \leq 7\} \cup \{e_7 + e_8, \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7 + e_8)\} \end{aligned}$$

$$\begin{aligned} E_7: \Sigma &= \{\alpha \in \Sigma(E_8) \mid \alpha \perp e_1 + e_2\} \\ \Pi &= \Pi(E_8) \setminus \{e_2 - e_3\} \end{aligned}$$

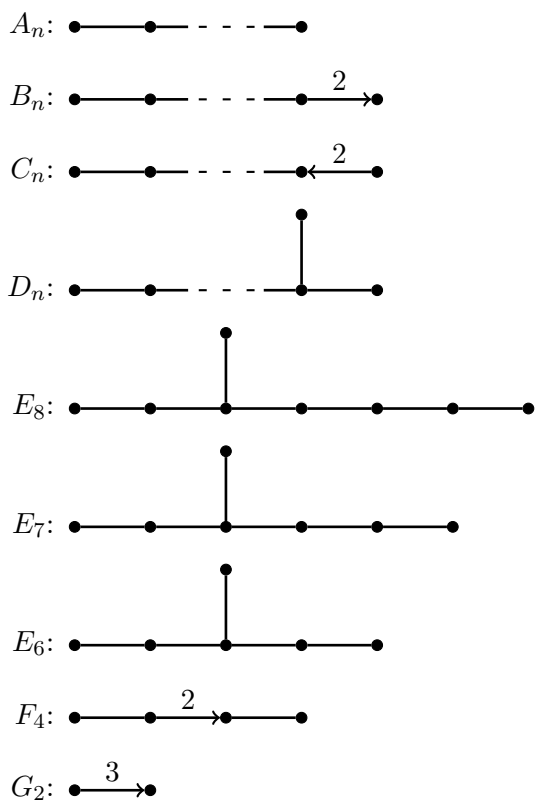
$$\begin{aligned} E_6: \Sigma &= \{\alpha \in \Sigma(E_7) \mid \alpha \perp e_2 - e_3\} \\ \Pi &= \Pi(E_8) \setminus \{e_2 - e_3, e_3 - e_4\} \end{aligned}$$

$$\begin{aligned} F_4: \Sigma &= \{\pm e_i \pm e_j \mid 1 \leq i < j \leq 4\} \cup \{\pm e_i \mid 1 \leq i \leq 4\} \cup \{e_\varepsilon \mid \varepsilon \in \mathbf{S}_4\} \\ \Pi &= \{e_2 - e_3, e_3 - e_4, e_4, \frac{1}{2}(e_1 - e_2 - e_3 - e_4)\} \end{aligned}$$

$$\begin{aligned} G_2: \Sigma &= \{\pm(e_1 - e_2), \pm(e_2 - e_3), \pm(e_3 - e_1), \pm(2e_1 - e_2 - e_3), \pm(2e_2 - e_3 - e_1), \pm(2e_3 - e_1 - e_2)\} \\ \Pi &= \{e_1 - e_2, 2e_2 - e_3 - e_1\} \end{aligned}$$

*Bevis.* Dette indgår i [GLS] Theorem 1.8.7 og Remark 1.8.8.  $\square$

**Sætning 17** (Dynkin-diagrammer for irreducible rodsystemer). *Dynkin-diagrammerne for de irreducible rodsystemer er som vist:*



*Bevis.* Dette indgår i [GLS] Theorem 1.8.7. □

I rodsystemerne  $A_n$ ,  $D_n$  og  $E_n$  har alle rødder samme længde. I de øvrige irreducible rodsystemer er der to forskellige rodlængder, og man taler om lange og korte rødder. I  $B_n$ ,  $C_n$  og  $F_4$  er forholdet mellem rodlængderne  $\sqrt{2}$ ; i  $G_2$  er forholdet  $\sqrt{3}$ .

Til ethvert rodsystem  $\Sigma$  kan der knyttes et dualt rodsystem  $\check{\Sigma}$ . Det duale rodsystem indgår i beskrivelsen af den indre struktur af de semisimple algebraiske grupper.

**Definition 9.** Lad  $\Sigma$  være et rodsystem. For hvert  $\alpha \in \Sigma$  defineres den duale rod  $\check{\alpha}$  ved  $\check{\alpha} = 2\alpha/(\alpha, \alpha)$ . Det *duale rodsystem*  $\check{\Sigma}$  er mængden  $\{\check{\alpha} \mid \alpha \in \Sigma\}$ .

**Sætning 18.**  $\check{\Sigma}$  er et rodsystem, og for alle  $\alpha, \beta \in \Sigma$  gælder  $\langle \check{\alpha}, \check{\beta} \rangle = \langle \beta, \alpha \rangle$ . Ydermere er  $\check{\check{\Sigma}} = \Sigma$ .

*Bevis.* Definer  $c_\alpha = \frac{2}{(\alpha, \alpha)}$ , således at  $\check{\alpha} = c_\alpha \alpha$ . Da er  $c_{\check{\alpha}} = \frac{2}{(\check{\alpha}, \check{\alpha})} = \frac{2}{(c_\alpha \alpha, c_\alpha \alpha)} = \frac{2}{c_\alpha^2 (\alpha, \alpha)} = c_\alpha^{-2} \cdot c_\alpha = c_\alpha^{-1}$ , og dermed er  $\check{\check{\alpha}} = c_{\check{\alpha}} \check{\alpha} = c_\alpha^{-1} c_\alpha \alpha = \alpha$ . Så er  $\check{\check{\Sigma}} = \Sigma$ .

For vilkårlige  $\alpha$  og  $\beta$  gælder nu  $\langle \alpha, \beta \rangle = c_\beta (\alpha, \beta)$ . Så fås  $\langle \check{\alpha}, \check{\beta} \rangle = c_{\check{\beta}} (\check{\alpha}, \check{\beta}) = c_\beta^{-1} (c_\alpha \alpha, c_\beta \beta) = c_\beta^{-1} c_\alpha c_\beta (\alpha, \beta) = c_\alpha (\beta, \alpha) = \langle \beta, \alpha \rangle$ .

Tilbage er kun at bevise at  $\check{\Sigma}$  er et rodsystem. Lad  $\alpha, \beta \in \Sigma$ ; da gælder

$$\begin{aligned}
(r_\beta(\alpha), r_\beta(\alpha)) &= (\alpha - \langle \alpha, \beta \rangle \beta, \alpha - \langle \alpha, \beta \rangle \beta) \\
&= (\alpha, \alpha) + \langle \alpha, \beta \rangle^2 (\beta, \beta) - 2\langle \alpha, \beta \rangle (\alpha, \beta) \\
&= (\alpha, \alpha) + \frac{4\langle \alpha, \beta \rangle^2}{(\beta, \beta)^2} (\beta, \beta) - \frac{4\langle \alpha, \beta \rangle}{(\beta, \beta)} (\alpha, \beta) \\
&= (\alpha, \alpha)
\end{aligned}$$

Specielt haves så  $c_{r_\beta(\alpha)} = c_\alpha$ . Så fås

$$\begin{aligned}
r_{\check{\beta}}(\check{\alpha}) &= \check{\alpha} - \langle \check{\alpha}, \check{\beta} \rangle \check{\beta} = c_\alpha \alpha - \langle \beta, \alpha \rangle c_\beta \beta \\
&= c_\alpha \alpha - c_\alpha (\beta, \alpha) c_\beta \beta = c_\alpha (\alpha - c_\beta (\alpha, \beta) \beta) \\
&= c_{r_\beta(\alpha)} (\alpha - \langle \alpha, \beta \rangle \beta) \\
&= c_{r_\beta(\alpha)} r_\beta(\alpha)
\end{aligned}$$

Da  $c_{r_\beta(\alpha)} r_\beta(\alpha)$  netop er den duale rod til  $r_\beta(\alpha)$  er den et element i  $\check{\Sigma}$ , og dermed er  $r_{\check{\beta}}(\check{\Sigma}) \subseteq \check{\Sigma}$ . Da  $\check{\Sigma}$  er endelig og  $r_\beta$  er injektiv, er så  $r_{\check{\beta}}(\check{\Sigma}) = \check{\Sigma}$ . Idet  $\Sigma$  er krystallografisk, er  $\check{\Sigma}$  det også, da der gælder  $\langle \check{\alpha}, \check{\beta} \rangle = \langle \beta, \alpha \rangle$ . Endelig er  $\check{\Sigma}$  reduceret: lad  $\check{\alpha}, \check{\beta} \in \check{\Sigma}$ , og antag  $\check{\alpha} = k\check{\beta}$  for et vist  $k \in \mathbb{R}$ . Da er  $c_\alpha \alpha = kc_\beta \beta$ , og dermed fås  $\alpha = kc_\beta c_\alpha^{-1} \beta$ . Da  $\Sigma$  er reduceret, må så  $kc_\beta c_\alpha^{-1} = \pm 1$ . Da  $\alpha = \pm \beta$  er  $(\alpha, \alpha) = (\beta, \beta)$ , og så er  $c_\alpha = c_\beta$ . Dermed er  $k = \pm 1$ , så  $\check{\alpha} = \pm \check{\beta}$ .  $\square$

**Sætning 19.** *Lad  $\Sigma^+$  være et positivt delsystem af  $\Sigma$  med tilhørende fundamentalt system  $\Pi$ . Da er  $\check{\Sigma}^+$  et positivt delsystem af  $\check{\Sigma}$  med tilhørende fundamentalt system  $\check{\Pi}$ .*

*Bevis.* Lad som før  $c_\alpha = \frac{2}{(\alpha, \alpha)}$ , således at  $\check{\alpha} = c_\alpha \alpha$ . Da er  $c_\alpha = c_{-\alpha}$ , og  $-\check{\alpha}$  er dermed den duale rod til  $-\alpha$ . Idet der gælder  $\alpha \in \Sigma^+$  hvis og kun hvis  $-\alpha \notin \Sigma^+$ , fås så at der gælder  $\check{\alpha} \in \check{\Sigma}^+$  hvis og kun hvis der gælder  $-\check{\alpha} \notin \check{\Sigma}^+$ .

Skriv nu  $\Pi = \{\alpha_1, \dots, \alpha_n\}$ , og lad  $\alpha \in \Sigma^+$ ; da findes der konstanter  $k_1, \dots, k_n$  med  $k_i \geq 0$  således at  $\alpha = \sum_{i=1}^n k_i \alpha_i$ . Så gælder  $c_\alpha \alpha = c_\alpha \sum_{i=1}^n k_i c_{\alpha_i}^{-1} (c_{\alpha_i} \alpha_i)$  og dermed fås  $\check{\alpha} = \sum_{i=1}^n c_\alpha k_i c_{\alpha_i}^{-1} \check{\alpha}_i$ . Da  $k_i \geq 0$  for hvert  $i$  og  $c_\beta > 0$  for hvert  $\beta \in \Sigma$  fås så  $c_\alpha k_i c_{\alpha_i}^{-1} \geq 0$  for hvert  $i$ . Dermed kan ethvert element i  $\check{\Sigma}^+$  skrives som en linearkombination af elementerne i  $\check{\Pi}$  med ikke-negative koefficienter. Ydermere har  $\check{\Pi}$   $\dim(\check{\Sigma})$  elementer, idet  $\Pi$  har  $\dim(\Sigma)$  elementer og der klart gælder  $\mathbb{R}\check{\Sigma} = \mathbb{R}\Sigma$  og dermed  $\dim(\check{\Sigma}) = \dim(\Sigma)$ .

Tilbage er kun at vise at  $\check{\Sigma}^+$  er lukket. Antag at dette ikke er tilfældet; da findes der  $\check{\alpha}, \check{\beta} \in \check{\Sigma}^+$  således at  $\check{\alpha} + \check{\beta} \notin \check{\Sigma}^+$ . Da gælder  $-(\check{\alpha} + \check{\beta}) \in \Sigma^+$ . Skriv nu  $\check{\alpha} = \sum_{i=1}^n k_i \check{\alpha}_i$ ,  $\check{\beta} = \sum_{i=1}^n l_i \check{\alpha}_i$  og  $-(\check{\alpha} + \check{\beta}) = \sum_{i=1}^n m_i \check{\alpha}_i$  med  $k_i \geq 0$ ,  $l_i \geq 0$  og  $m_i \geq 0$  for hvert  $i$ . Så fås  $\sum_{i=1}^n (k_i + l_i + m_i) \check{\alpha}_i = \check{\alpha} + \check{\beta} - (\check{\alpha} + \check{\beta}) = 0$ . Per Sætning 10(a) er  $\Pi$  en basis for  $\mathbb{R}\Sigma$ , og dermed specielt lineært uafhængigt, og da  $\check{\alpha}_i$  blot er en skalering af  $\alpha_i$  er  $\check{\Pi}$  så lineært uafhængigt. Så må  $k_i + l_i + m_i = 0$  for hvert  $i$ , og da alle tre led er ikke-negative fås  $k_i = l_i = m_i = 0$ . Men så er  $\alpha = \beta = 0$ , hvilket er umuligt. Altså er  $\check{\Sigma}^+$  lukket.  $\square$

**Sætning 20.** *Dynkin-diagrammet for  $\check{\Sigma}$  er identisk med Dynkin-diagrammet for  $\Sigma$ , bortset fra at alle orienterede kanter har omvendt retning.*

*Bevis.* Lad  $\Pi$  være et fundamentalt system for  $\Sigma$ , og konstruer Dynkin-diagrammet for  $\Sigma$  ud fra  $\Pi$  og Dynkin-diagrammet for  $\check{\Sigma}$  ud fra  $\check{\Pi}$ . Vægten af kanten mellem  $\check{\alpha}$  og  $\check{\beta}$  er  $\langle \check{\alpha}, \check{\beta} \rangle \langle \check{\beta}, \check{\alpha} \rangle$ ; dette

er lig vægten af kanten mellem  $\alpha$  og  $\beta$  da der gælder  $\langle \check{\alpha}, \check{\beta} \rangle \langle \check{\beta}, \check{\alpha} \rangle = \langle \beta, \alpha \rangle \langle \alpha, \beta \rangle$ . Ydermere haves  $|\check{\alpha}| = \left| \frac{2\alpha}{(\alpha, \alpha)} \right| = \frac{2|\alpha|}{|\alpha|^2} = \frac{2}{|\alpha|}$ . Dermed fås at hvis  $|\alpha| > |\beta|$ , således at kanten mellem  $\alpha$  og  $\beta$  er orienteret i retning mod  $\beta$ , så er  $|\check{\alpha}| = \frac{2}{|\alpha|} < \frac{2}{|\beta|} = |\check{\beta}|$ , således at kanten mellem  $\check{\alpha}$  og  $\check{\beta}$  er orienteret i retning mod  $\check{\alpha}$ . Endelig ses at hvis  $|\alpha| = |\beta|$ , således at kanten mellem  $\alpha$  og  $\beta$  er uorienteret, så er  $|\check{\alpha}| = \frac{2}{|\alpha|} = \frac{2}{|\beta|} = |\check{\beta}|$ , således at kanten mellem  $\check{\alpha}$  og  $\check{\beta}$  også er uorienteret.  $\square$

Med dette resultat er det let at beskrive de duale systemer til de irreducible rodsystemer.

**Sætning 21.** *Der gælder  $\check{A}_n \cong A_n$ ,  $\check{B}_n \cong C_n$  for  $n \geq 3$ ,  $\check{D}_n \cong D_n$ ,  $\check{E}_n \cong E_n$ ,  $\check{B}_2 \cong B_2$ ,  $\check{F}_4 \cong F_4$  og  $\check{G}_2 \cong G_2$ . Standardformerne i Sætning 16 er defineret således at ved at bruge disse former bliver de fire første af disse isomorfier til ligheder.*

*Bevis.* Første del følger af Sætning 20 og Sætning 17. Anden del fås ud fra Sætning 16 ved direkte beregning.  $\square$

Bemærk at selv om  $A_n$ ,  $D_n$ ,  $E_n$ ,  $B_2$ ,  $F_4$  og  $G_2$  alle er selvduale, adskiller de tre sidste systemer sig fra de øvrige i den måde de er selvduale. I  $A_n$ ,  $D_n$  og  $E_n$  er der kun én rodlængde, så afbildningen  $\alpha \mapsto \check{\alpha}$  er en isomorfi af rodsystemer. I  $B_2$ ,  $F_4$  og  $G_2$  er der to rodlængder, og isomorfien mellem rodsystemet og dets duale bliver derfor mere kompliceret. Helt præcist gælder at hvis  $\Sigma$  er enten  $B_2$ ,  $F_4$  eller  $G_2$ , så findes der en ikke-triviel automorfi af Dynkin-diagrammet for  $\Sigma$  som ikke respekterer orientering af kanter. Hvis  $\Pi$  er et fundamentalt system for  $\Sigma$  definerer denne automorfi en ikke-triviel permutation  $\rho$  af  $\Pi$ , og der findes så en isomorfi  $\Sigma \rightarrow \check{\Sigma}$  hvis restriktion til  $\Pi$  er afbildningen  $\alpha \mapsto \rho(\check{\alpha})$ .

## Klassifikation af semisimple algebraiske grupper

Med teorien for rodsystemer er det nu muligt at beskrive strukturen af de semisimple algebraiske grupper indgående, og at klassificere dem. Først haves et lille lemma om virkningen af den maksimale torus på rodgrupperne.

**Lemma 22.** *Lad  $\bar{T}$  være en maksimal torus af  $\bar{K}$ , og lad  $\bar{X}$  være en  $\bar{T}$ -rodgruppe i  $\bar{K}$ . Da findes der en unik karakter  $\chi$  af  $\bar{T}$  således at for enhver parametrisering  $x(t)$  af  $\bar{X}$  gælder  $x(t)^s = x(\chi(s)t)$  for alle  $t \in \bar{\mathbb{F}}$  og  $s \in \bar{T}$ .*

*Bevis.* Idet  $\bar{T}$  normaliserer  $\bar{X}$ , er afbildningen  $t \mapsto x(t)^s$  en parametrisering af  $\bar{X}$ . Per Sætning 6 har den så formen  $t \mapsto x(ct)$  for et vist  $c \in \bar{\mathbb{F}}^\times$ . Ved at sætte  $\chi(s) = c$  fås så en afbildning  $\chi: \bar{T} \rightarrow \bar{\mathbb{F}}^\times$  som opfylder  $x(t)^s = x(\chi(s)t)$  for ethvert  $t \in \bar{\mathbb{F}}$  og  $s \in \bar{T}$ . Ydermere gælder  $x(\chi(s_1 s_2)) = x(1)^{s_1 s_2} = x(\chi(s_1))^{s_2} = x(\chi(s_1)\chi(s_2))$ , og da  $x$  er injektiv fås  $\chi(s_1 s_2) = \chi(s_1)\chi(s_2)$ . Dermed er  $\chi$  en homomorfi.  $\square$

Karakteren  $\chi$  siges at være associeret til rodgruppen  $\bar{X}$ .

**Definition 10.** En  $\bar{T}$ -rod i  $\bar{K}$  er en karakter af  $\bar{T}$  associeret til en  $\bar{T}$ -rodgruppe i  $\bar{K}$ . Mængden af  $\bar{T}$ -rødder i  $\bar{K}$  betegnes med  $\Sigma(\bar{T})$ .

**Lemma 23.** *Til hver  $\bar{T}$ -rod af  $\bar{K}$  hører en unik  $\bar{T}$ -rodgruppe.*

*Bevis.* Dette er [GLS] Theorem 1.9.5(b).  $\square$

Der er således en én-til-én-korrespondance mellem  $\overline{T}$ -rodgrupper i  $\overline{K}$  og  $\overline{T}$ -rødder, og  $\Sigma(\overline{T})$  kunne derfor lige så vel defineres til at være mængden af  $\overline{T}$ -rodgrupper. Grunden til at man bruger  $\overline{T}$ -rødder i stedet er at  $\overline{T}$ -rødder kan betragtes som elementer i mængden af karakterer af  $\overline{T}$ . Denne mængde har struktur af en abelsk gruppe, og denne struktur kommer til at svare til den additive struktur i et rodsystem.

**Sætning 24.** *Lad  $\overline{K}$  være en semisimpel algebraisk gruppe med maksimal torus  $\overline{T}$ . Da findes der et reduceret krystallografisk rodsystem  $\Sigma$  og en bijektion mellem  $\Sigma$  og  $\Sigma(\overline{T})$  således at når man for ethvert  $\alpha \in \Sigma$  lader  $\chi_\alpha$  være elementet i  $\Sigma(\overline{T})$  hørende til  $\alpha$  og  $\overline{X}_\alpha$  være  $\overline{T}$ -rodgruppen af  $\overline{T}$  hørende til  $\overline{X}_\alpha$ , så gælder følgende:*

- (a) *Lad  $\alpha$  og  $\beta$  være elementer i  $\Sigma$  således at  $\alpha + \beta \in \Sigma$ . Da er  $\chi_\alpha(t)\chi_\beta(t) = \chi_{\alpha+\beta}(t)$  for alle  $t \in \overline{T}$ . For ethvert  $\alpha \in \Sigma$  gælder desuden  $\chi_{-\alpha}(t) = \chi_\alpha(t)^{-1}$  for alle  $t \in \overline{T}$ .*
- (b) *For hvert element  $\beta \in \Sigma$  findes en kokarakter  $h_\beta$  af  $\overline{T}$  således at for alle  $\alpha, \beta \in \Sigma$  gælder  $\chi_\alpha(h_\beta(t)) = t^{-\langle \alpha, \beta \rangle}$ .*
- (c) *Lad  $\overline{N} = N_{\overline{K}}(\overline{T})$ . Da findes der en isomorfi  $\overline{N}/\overline{T} \cong W(\Sigma)$  således at for ethvert  $n \in \overline{N}$  og ethvert  $\alpha \in \Sigma$  gælder  ${}^n(\overline{X}_\alpha) = \overline{X}_{w(\alpha)}$  hvor  $w$  er billedet af  $n\overline{T}$  i  $W(\Sigma)$  under ovenstående isomorfi.*
- (d)  $\overline{K} = \langle \overline{X}_\alpha \mid \alpha \in \Sigma \rangle$ .
- (e) *Lad  $\Sigma_1 \cup \dots \cup \Sigma_k$  være den unikke ortogonale dekomposition af  $\Sigma$  med irreducible  $\Sigma_i$ , og definer  $\overline{K}_i = \langle \overline{X}_\alpha \mid \alpha \in \Sigma_i \rangle$  for hvert  $i$ . Da er  $\overline{K}_1, \dots, \overline{K}_k$  komponenterne af  $\overline{K}$ , og  $\Sigma_i$  er rodsystemet for  $\overline{K}_i$  for hvert  $i$ .*

*Bevis.* (a)-(c) er [GLS] Theorem 1.9.5(d) og (f). (d) er Sætning 7, og (e) følger af (d) og [GLS] Theorem 1.10.1(b). Bemærk at jeg har ændret fortegnet på eksponenten i (b) for at sikre konsistens med Sætning 31. Dette ændrer ikke på sætningens indhold, for hvis  $h_\beta$  er defineret så der gælder  $\chi_\alpha(h_\beta(t)) = t^{\langle \alpha, \beta \rangle}$  for alle  $\alpha \in \Sigma$ , så kan man definere  $h'_\beta$  ved  $h'_\beta(t) = h_\beta(t^{-1})$ , og så gælder  $\chi_\alpha(h'_\beta(t)) = t^{-\langle \alpha, \beta \rangle}$  for alle  $\alpha \in \Sigma$ .  $\square$

**Eksempel 3.** Gruppen  $SL_3(\overline{\mathbb{F}})$ , den specielle lineære gruppe af dimension 3 over  $\overline{\mathbb{F}}$ , er en semisimpel algebraisk gruppe. En mulig maksimal torus er undergruppen  $\overline{T}$  bestående af diagonalmatricerne. En af  $\overline{T}$ -rodgrupperne består af alle matricer på formen

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

med  $x \in \overline{\mathbb{F}}$ . Skriv  $e_{ij}$  for matricen hvis indgang  $(i, j)$  er 1 og hvis andre indgange alle er 0, og lad  $I$  være identitetsmatricen. Da er ovenstående matrix altså  $I + xe_{12}$ , og  $\overline{T}$ -rodgruppen er lig  $\{I + xe_{12} \mid x \in \overline{\mathbb{F}}\}$ . Kald denne  $\overline{T}$ -rodgruppe for  $\overline{X}_{12}$ . Der findes fem andre  $\overline{T}$ -rodgrupper, som konstrueres analogt; beteg dem med  $\overline{X}_{13}$ ,  $\overline{X}_{21}$ ,  $\overline{X}_{23}$ ,  $\overline{X}_{31}$  og  $\overline{X}_{32}$ .

Lad nu  $\chi_{ij}$  og  $h_{ij}$  være karakteren og kokarakteren hørende til  $\overline{X}_{ij}$ . Lad  $t \in \overline{T}$  og skriv

$$t = \begin{bmatrix} t_1 & 0 & 0 \\ 0 & t_2 & 0 \\ 0 & 0 & t_3 \end{bmatrix}$$



Da er  $\chi_{ij}(t) = t_i^{-1}t_j$ . Ydermere gælder at hvis  $t = h_{ij}(s)$  for et vist  $s \in \overline{\mathbb{F}}^\times$ , så er  $t_i = s$ ,  $t_j = s^{-1}$ , og  $t_k = 1$  hvis  $k \neq i$  og  $k \neq j$ . Rodsystemet for  $SL_3(\overline{\mathbb{F}})$  er  $A_2$ ; med notationen fra Eksempel 1 er en mulig bijektion givet ved  $\alpha \mapsto \chi_{12}$ ,  $\alpha + \beta \mapsto \chi_{13}$ ,  $\beta \mapsto \chi_{23}$ ,  $-\alpha \mapsto \chi_{21}$ ,  $-(\alpha + \beta) \mapsto \chi_{31}$  og  $-\beta \mapsto \chi_{32}$ .

Normalisatoren  $\overline{N}$  af  $\overline{T}$  består af alle de matricer hvorom det gælder at netop én indgang i hver række og søjle er forskellig fra 1. Givet et  $n \in \overline{N}$  består sideklassen  $n\overline{T}$  netop af de matricer  $m$  hvorom det gælder at de indgange i  $m$  der er forskellige fra 0 er de samme som i  $n$ .  $\overline{N}/\overline{T}$  kan derfor opfattes som gruppen af permutationsmatricer i dimension 3, og derfor bliver  $\overline{N}/\overline{T}$  isomorf med  $S_3$ . Dette er netop Weyl-gruppen for  $A_2$ .

Per Sætning 5 er to maksimale torusser i  $\overline{K}$  inbyrdes konjugerede. Dette faktum kan bruges til at bevise at rodsystemet  $\Sigma$  i Sætning 24 faktisk er uafhængigt af valget af maksimal torus.

**Sætning 25.** *Lad  $\overline{T}$  være en maksimal torus af  $\overline{K}$ , lad  $\alpha \mapsto \chi_\alpha$  være bijektionen mellem  $\Sigma$  og  $\Sigma(\overline{T})$  fra Sætning 24, og lad  $\overline{T}^g$  være en anden maksimal torus af  $\overline{K}$ . Da er  $\overline{T}^g$ -rodgrupperne i  $\overline{K}$  netop grupperne  $(\overline{X}_\alpha)^g$ , og  $\overline{T}^g$ -roden  $\chi_\alpha^g$  associeret til  $(\overline{X}_\alpha)^g$  er givet ved  $\chi_\alpha^g(t^g) = \chi_\alpha(t)$ . Ydermere er afbildningen  $\alpha \mapsto \chi_\alpha^g$  en bijektion mellem  $\Sigma$  og  $\Sigma(\overline{T}^g)$  som opfylder egenskaberne i Sætning 24.*

*Bevis.* Dette er [GLS] Theorem 1.9.5(c). □

Med dette resultat kan vi utvetydigt referere til  $\Sigma$  som rodsystemet for  $\overline{K}$ . Enhver semisimpel algebraisk gruppe har dermed et tilhørende rodsystem. Det næste spørgsmål må så være om der findes flere forskellige algebraiske grupper med samme rodsystem, og i givet fald hvor mange.

**Definition 11.** En isogeni er en surjektiv morfi af algebraiske grupper med endelig kerne.

**Proposition 26.** *Lad  $\varphi : \overline{K} \rightarrow \overline{H}$  være en isogeni af sammenhængende algebraiske grupper. Da er  $\ker(\varphi) \subseteq Z(\overline{K})$  og  $\varphi(Z(\overline{K})) = Z(\overline{H})$ . Ydermere gælder at hvis  $\overline{K}$  er semisimpel og  $\overline{T}$  er en maksimal torus af  $\overline{K}$ , så er  $\overline{H}$  semisimpel og  $\varphi(\overline{T})$  er en maksimal torus af  $\overline{H}$ .*

*Bevis.* Dette er [GLS] Proposition 1.10.3. □

**Sætning 27.** *Lad  $\Sigma$  være et reduceret krystallografisk rodsystem. Da findes der unikke semisimple algebraiske grupper  $\overline{K}_u(\Sigma)$  og  $\overline{K}_a(\Sigma)$  med følgende egenskaber:*

- (a)  $\overline{K}_u(\Sigma)$  og  $\overline{K}_a(\Sigma)$  har begge rodsystem  $\Sigma$ .
- (b) For enhver semisimpel algebraisk gruppe  $\overline{K}$  med rodsystem  $\Sigma$  findes isogener  $\overline{K}_u(\Sigma) \rightarrow \overline{K} \rightarrow \overline{K}_a(\Sigma)$ .
- (c)  $Z(\overline{K}_u(\Sigma))$  er endelig og  $Z(\overline{K}_a(\Sigma)) = C_1$ .

*Bevis.* Dette er [GLS] Theorem 1.10.4(b) og (d). □

**Sætning 28.** *Lad  $\Sigma$  være et rodsystem, og lad  $\Sigma_1 \cup \dots \cup \Sigma_k$  være en ortogonal dekomposition af  $\Sigma$ . Da er  $\overline{K}_u(\Sigma) \cong \overline{K}_u(\Sigma_1) \times \dots \times \overline{K}_u(\Sigma_k)$  og  $\overline{K}_a(\Sigma) \cong \overline{K}_a(\Sigma_1) \times \dots \times \overline{K}_a(\Sigma_k)$ .*

*Bevis.* Dette følger af [GLS] Proposition 1.10.6 ved induktion. □

De algebraiske grupper med rodsystem  $\Sigma$  er dermed netop grupperne  $\overline{K}_u(\Sigma)/Z$  hvor  $Z$  er en undergruppe af  $Z(\overline{K}_u(\Sigma))$ . For at afslutte klassifikationen er der kun tilbage at beskrive gruppen  $Z(\overline{K}_u(\Sigma))$  for de irreducible rodsystemer, samt at undersøge om der findes isomorfier mellem simple algebraiske grupper med forskellige rodsystemer.

**Sætning 29.** Lad  $\overline{K}_u$  være en universel simpel algebraisk gruppe med rodsystem  $\Sigma$ , lad  $\overline{T}$  være en maksimal torus af  $\overline{K}_u$ , og lad  $Z = Z(\overline{K}_u)$ . Da gælder  $Z \subseteq \overline{T}$ , og isomorfiklassen af  $Z$  ses i nedenstående liste. Her angiver  $\overline{\mathbb{F}}^{(n)}$  undergruppen af  $\overline{\mathbb{F}}^\times$  bestående af alle  $n$ 'te enhedsrødder.

$$A_n: Z \cong \overline{\mathbb{F}}^{(n+1)}.$$

$$B_n: Z \cong \overline{\mathbb{F}}^{(2)}.$$

$$C_n: Z \cong \overline{\mathbb{F}}^{(2)}.$$

$$D_n: \text{Hvis } n \text{ er lige, er } Z \cong \overline{\mathbb{F}}^{(2)} \times \overline{\mathbb{F}}^{(2)}. \text{ Hvis } n \text{ er ulige, er } Z \cong \overline{\mathbb{F}}^{(4)}.$$

$$E_8: Z \cong C_1$$

$$E_7: Z \cong \overline{\mathbb{F}}^{(2)}$$

$$E_6: Z \cong \overline{\mathbb{F}}^{(3)}$$

$$F_4: Z \cong C_1$$

$$G_2: Z \cong C_1$$

*Bevis.* Dette er [GLS] Theorem 1.9.5(h) og Theorem 1.12.5(c). □

**Sætning 30.** Lad  $\overline{K}$  være en simpel algebraisk gruppe, og lad  $\overline{K} \rightarrow \overline{H}$  være en isogeni. Da har  $\overline{K}$  og  $\overline{H}$  samme rodsystem, eller også er deres rodsystemer  $B_n$  og  $C_n$  og karakteristikkene af det underliggende legeme  $\overline{\mathbb{F}}$  er 2. Ydermere findes der bijektive morfier  $\overline{K}_a(B_n) \rightarrow \overline{K}_a(C_n)$  og  $\overline{K}_a(C_n) \rightarrow \overline{K}_a(B_n)$  af adjungerede algebraiske grupper over  $\overline{\mathbb{F}}_2$ .

*Bevis.* Dette er [GLS] Theorem 1.10.4(a) og Theorem 1.15.9, bortset fra påstanden om at morfierne mellem  $\overline{K}_a(B_n)$  og  $\overline{K}_a(C_n)$  er bijektive. Morfierne er surjektive ifølge Theorem 1.15.9, så det skal bare vises at de er injektive. Kernen for morfien  $\overline{K}_a(B_n) \rightarrow \overline{K}_a(C_n)$  er en lukket normal undergruppe af  $\overline{K}_a(B_n)$  per Proposition 1(c), og per Sætning 2(c) er kernen så enten hele  $\overline{K}_a(B_n)$  eller indeholdt i centeret for  $\overline{K}_a(B_n)$ . Kernen er ikke hele  $\overline{K}_a(B_n)$  da morfien så ikke ville være surjektiv, og per Sætning 27(c) fås så at kernen er triviel. Dermed er morfien  $\overline{K}_a(B_n) \rightarrow \overline{K}_a(C_n)$  injektiv. At den anden morfi er injektiv ses tilsvarende. □

Bemærk at selv om morfierne  $\overline{K}_a(B_n) \rightarrow \overline{K}_a(C_n)$  og  $\overline{K}_a(C_n) \rightarrow \overline{K}_a(B_n)$  er bijektive, er de ikke isomorfier af algebraiske grupper, da deres inverse afbildninger kun er gruppehomomorfier, og ikke morfier af algebraiske grupper.

Semisimple algebraiske grupper er dermed klassificeret ved deres rodsystem. Rodsystemet kan også bruges til at give en detaljeret beskrivelse af strukturen af grupperne.

**Sætning 31** (Chevalley-relationerne). Lad  $\overline{K}$  være en semisimpel algebraisk gruppe med maksimal torus  $\overline{T}$  og rodsystem  $\Sigma$ .  $\overline{T}$ -rodgrupperne  $\overline{X}_\alpha$  har parametriseringer  $x_\alpha(t)$  således at når man for hvert  $\alpha \in \Sigma$  og  $t \in \overline{\mathbb{F}}^\times$  definerer elementerne  $n_\alpha(t)$  og  $h_\alpha(t)$  ved

$$n_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$$

og

$$h_\alpha(t) = n_\alpha(t)n_\alpha(1)^{-1}$$

så er  $\overline{T} = \langle h_\alpha(t) \mid \alpha \in \Sigma, t \in \overline{\mathbb{F}}^\times \rangle$ , og følgende gælder for alle  $\alpha, \beta \in \Sigma$  og  $t, u \in \overline{\mathbb{F}}$  (med restriktionerne  $t \neq 0$  og/eller  $u \neq 0$  hvor dette er nødvendigt):

(a)  $x_\alpha(t)x_\alpha(u) = x_\alpha(t+u)$ .

(b) Hvis  $\alpha \neq \pm\beta$ , så er

$$[x_\alpha(t), x_\beta(u)] = \prod_{i,j} x_{i\alpha+j\beta}(c_{ij\alpha\beta}t^i u^j)$$

Produktet løber her over alle par af positive heltal  $i$  og  $j$  som opfylder  $i\alpha + j\beta \in \Sigma$ . Faktorerne optræder i en fast rækkefølge med  $i + j$  svagt voksende, uafhængigt af værdierne af  $t$  og  $u$ . Konstanterne  $c_{ij\alpha\beta}$  afhænger ikke af  $t$  og  $u$ , og er op til fortegn bestemt af strukturen af  $\Sigma \cap \mathbb{R}\{\alpha, \beta\}$ . Mere præcist gælder  $c_{ij\alpha\beta} = \pm 1$  med præcis følgende undtagelser:

(1)  $\Sigma \cap \mathbb{R}\{\alpha, \beta\} = B_2$ ,  $\alpha$  og  $\beta$  er korte og  $\alpha + \beta$  er lang; da er  $c_{11\alpha\beta} = \pm 2$ .

(2)  $\Sigma \cap \mathbb{R}\{\alpha, \beta\} = G_2$ ,  $\alpha$  og  $\beta$  er korte og  $\alpha + \beta$  er lang; da er  $c_{11\alpha\beta} = \pm 3$ .

(3)  $\Sigma \cap \mathbb{R}\{\alpha, \beta\} = G_2$ ,  $\alpha, \beta$  og  $\alpha + \beta$  er korte; da er  $c_{11\alpha\beta} = \pm 2$ ,  $c_{21\alpha\beta} = \pm 3$  og  $c_{12\alpha\beta} = \pm 3$ .

(4)  $\Sigma \cap \mathbb{R}\{\alpha, \beta\} = G_2$ ;  $\{\alpha, \beta\}$  er et fundamentalt system med  $\alpha$  kort; da er  $c_{32\alpha\beta} = \pm 2$ .

(c)  $[h_\alpha(t), h_\beta(u)] = 1$ .

(d)  $h_\alpha(t)h_\alpha(u) = h_\alpha(tu)$ .

(e) Lad  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  være et fundamentalt system i  $\Sigma$ , lad  $\alpha \in \Sigma$ , og skriv  $\check{\alpha} = \sum_{i=1}^n c_i \alpha_i$ . Da er  $h_\alpha(t) = \prod_{i=1}^n h_{\alpha_i}(t^{c_i})$ .

(f) Hvis  $\overline{K}$  er universel, så er  $\prod_{i=1}^n h_{\alpha_i}(t_i) = 1$  hvis og kun hvis  $t_i = 1$  for hvert  $i$ .

(g)  $x_\alpha(t)^{h_\beta(u)} = x_\alpha(u^{-\langle \alpha, \beta \rangle} t)$ .

(h)  $x_\alpha(t)^{n_\beta(1)} = x_{r_\beta(\alpha)}(c_{\alpha, \beta} t)$ . Her er  $c_{\alpha, \beta} = \pm 1$ , uafhængigt af  $t$ .

(i)  $h_\alpha(t)^{n_\beta(1)} = h_{r_\beta(\alpha)}(t)$ .

(j)  $n_\alpha(t)^{n_\beta(1)} = n_{r_\beta(\alpha)}(c_{\alpha, \beta} t)$ .

(k)  $n_\alpha(1)^2 = h_\alpha(-1)$ .

*Bevis.* Dette er [GLS] Theorem 1.12.1. Bemærk at forfatterne har begået to fejl i deres opskrivning af sætningen: der mangler et fortegn i eksponenten i (g), og konstanten  $c_\alpha$  skal ikke indgå i (i). De korrekte formler kan findes i [Ca] i beviset for Theorem 12.1.1.  $\square$

Funktionerne  $h_\alpha$  er netop kokaraktererne i Sætning 24(b). Per definitionen af  $\chi_\alpha$  gælder nemlig  $x_\alpha(t)^{h_\beta(u)} = x_\alpha(\chi_\alpha(h_\beta(u))t)$ , og relationen  $x_\alpha(t)^{h_\beta(u)} = x_\alpha(u^{-\langle \alpha, \beta \rangle} t)$  siger så netop at  $\chi_\alpha(h_\beta(u)) = u^{-\langle \alpha, \beta \rangle}$ .

**Eksempel 4.** Betragt igen gruppen  $SL_3(\overline{\mathbb{F}})$  fra Eksempel 3. Denne gruppe er den universelle semisimple algebraiske gruppe med rodsystem  $A_2$ . Et muligt valg af Chevalley-frembringere er

givet ved at  $\bar{X}_{ij}$  parametriseres ved  $x_{ij}(t) = (I + te_{ij})$ , hvor  $I$  og  $e_{ij}$  er som i Eksempel 3. Centeret for  $SL_3(\bar{\mathbb{F}})$  består af alle matricer på formen

$$\begin{bmatrix} s & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & s \end{bmatrix}$$

For at denne matrix har determinant 1, skal der gælde  $s^3 = 1$ . Dermed bliver centeret af  $SL_3(\bar{\mathbb{F}})$  isomorf med gruppen af tredje enhedsrødder i  $\bar{\mathbb{F}}^\times$ . Den adjungerede gruppe med rodsystem  $A_2$  er netop  $SL_3(\bar{\mathbb{F}})$  modulo dette center; den betegnes  $PSL_3(\bar{\mathbb{F}})$  og kaldes den projektive specielle lineære gruppe over  $\bar{\mathbb{F}}$ .

Chevalley-relationerne giver faktisk en præsentation af den algebraiske gruppe  $\bar{K}$ :

**Sætning 32.** *Lad  $\bar{K}$  være en semisimpel algebraisk gruppe, og lad  $\bar{K}_u$  og  $\bar{K}_a$  være den universelle hhv. adjungerede algebraiske gruppe med samme rodsystem som  $\bar{K}$ .*

- Chevalley-relationerne sammen med definitionerne af  $n_\alpha(t)$  og  $h_\alpha(t)$  udgør en præsentation af  $\bar{K}_u$ .*
- Ud fra denne præsentation af  $\bar{K}_u$  kan en præsentation af  $\bar{K}$  konstrueres ved at tilføje relationer af typen  $\prod_{\alpha \in \Sigma} h_\alpha(t_\alpha) = 1$ , hvor  $\prod_{\alpha \in \Sigma} h_\alpha(t_\alpha)$  er et element i kernen af isogenien  $\bar{K}_u \rightarrow \bar{K}$ .*
- Chevalley-frembringerne  $x_\alpha(t)$  af  $\bar{K}_u$ ,  $\bar{K}$  og  $\bar{K}_a$  kan vælges således at der findes isogener  $\bar{K}_u \rightarrow \bar{K} \rightarrow \bar{K}_a$  der begge afbilder  $x_\alpha(t)$  i  $x_\alpha(t)$  for alle  $\alpha$  og  $t$ .*

*Bevis.* Dette er [GLS] Theorem 1.12.4. □

**Sætning 33.** *Definer  $\bar{N} = N_{\bar{K}}(\bar{T})$ . Da er  $\bar{N} = \langle n_\alpha(t) \mid \alpha \in \Sigma, t \in \bar{\mathbb{F}}^\times \rangle$  hvor  $n_\alpha(t)$  er som i Sætning 31.*

*Bevis.*  $\bar{T}$  er frembragt af elementerne  $h_\alpha(t)$ , og per Sætning 31(h) er  $h_\alpha(t)^{n_\beta(1)} = h_{r_\beta(\alpha)}(t)$ . Konjugation med  $n_\beta(1)$  permuterer altså frembringerne, og  $n_\beta(1)$  må så normalisere  $\bar{T}$ . Nu gælder  $h_\beta(t) \in \bar{T} \subseteq \bar{N}$  og  $n_\beta(1) \in \bar{N}$ , og da  $n_\beta(t) = h_\beta(t)n_\beta(1)$  fås så  $n_\beta(t) \in \bar{N}$ . Dermed er  $\langle n_\alpha(t) \mid \alpha \in \Sigma, t \in \bar{\mathbb{F}}^\times \rangle \subseteq \bar{N}$ . Tilbage er så at vise at elementerne  $n_\alpha(t)$  frembringer hele  $\bar{N}$ .

Da  $\bar{T}$  er frembragt af elementerne  $h_\alpha(t) = n_\alpha(t)n_\alpha(1)^{-1}$ , må  $\bar{T} \subseteq \langle n_\alpha(t) \mid \alpha \in \Sigma, t \in \bar{\mathbb{F}}^\times \rangle$ . Det er så nok at vise at  $\langle n_\alpha(t) \mid \alpha \in \Sigma, t \in \bar{\mathbb{F}}^\times \rangle$  indeholder repræsentanter for alle sideklasser af  $\bar{T}$  i  $\bar{N}$ .

Per Sætning 31(h) er  $x_\alpha(t)^{n_\beta(1)} = x_{r_\beta(\alpha)}(c_{\alpha,\beta}t)$ , og dermed er  $(\bar{X}_\alpha)^{n_\beta(1)} = \bar{X}_{r_\beta(\alpha)}$ . Fra Sætning 31(k) og (d) fås nu  $n_\beta(1)^{-1} = h_\beta(-1)n_\beta(1)$ , og da  $\bar{T}$  normaliserer  $\bar{X}_\alpha$  haves  $n_\beta(1)(\bar{X}_\alpha) = (\bar{X}_\alpha)^{h_\beta(-1)n_\beta(1)} = (\bar{X}_\alpha)^{n_\beta(1)} = \bar{X}_{r_\beta(\alpha)}$ . Så er  $r_\beta$  billedet i  $W(\Sigma)$  af  $(n_\alpha(1))\bar{T}$  under isomorfien  $\bar{N}/\bar{T} \cong W(\Sigma)$  fra Sætning 24(c). Da elementerne  $r_\beta$  frembringer  $W(\Sigma)$ , må  $\langle n_\alpha(t) \mid \alpha \in \Sigma, t \in \bar{\mathbb{F}}^\times \rangle$  så indeholde repræsentanter for alle sideklasser af  $\bar{T}$  i  $\bar{N}$ . Dermed er  $\bar{N} = \langle n_\alpha(t) \mid \alpha \in \Sigma, t \in \bar{\mathbb{F}}^\times \rangle$ . □

**Sætning 34.** *Lad  $\Sigma^+$  være et positivt delsystem for  $\Sigma$  med tilhørende fundamentalt system  $\Pi$ , og definer  $\bar{U} = \langle \bar{X}_\alpha \mid \alpha \in \Sigma^+ \rangle$ . Da gælder:*

- For enhver total ordning af  $\Sigma^+$  gælder at ethvert element i  $\bar{U}$  har en unik fremstilling på formen  $\prod_{\alpha \in \Sigma^+} x_\alpha(t_\alpha)$  hvor faktorerne i produktet optræder i rækkefølgen defineret af den totale ordning.*

- (b) Lad  $\Sigma_1$  være en lukket delmængde af  $\Sigma^+$ , og definer  $\bar{U}_1 = \prod_{\alpha \in \Sigma_1} \bar{X}_\alpha$  hvor faktorerne optræder i vilkårlig rækkefølge. Da er  $\bar{U}_1$  en lukket undergruppe af  $\bar{U}$ .
- (c)  $\bar{U} = \langle \bar{X}_\alpha \mid \alpha \in \Pi \rangle$ .
- (d) Lad  $\Sigma_0^+$  være et andet positivt delsystem af  $\Sigma$ , og definer  $\bar{U}_0 = \langle \bar{X}_\alpha \mid \alpha \in \Sigma_0^+ \rangle$ . Da er  $\bar{U} \cap \bar{U}_0 = \langle \bar{X}_\alpha \mid \alpha \in \Sigma^+ \cap \Sigma_0^+ \rangle$ .

*Bevis.* (a)-(c) er [GLS] Theorem 1.12.7(a), (c) og (d), og (d) indgår i [GLS] Theorem 1.11.4.  $\square$

**Eksempel 5.** Betragt igen gruppen  $SL_3(\bar{\mathbb{F}})$  fra Eksempel 3, og lad  $A_2^+$  være det positive delsystem  $\{\alpha, \beta, \alpha + \beta\}$ . Gruppen  $\bar{U}$  bliver undergruppen af  $SL_3(\bar{\mathbb{F}})$  bestående af alle matricer på formen

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

Dette element er lig  $x_{23}(c)x_{13}(b)x_{12}(a)$ . Andre valg af rækkefølger for de tre rodgrupper i  $A_2^+$  kan give anderledes parametriseringer. Eksempelvis er ovenstående element også lig  $x_{12}(a)x_{23}(c)x_{13}(b - ac)$ . Et andet muligt positivt delsystem er mængden  $\{\beta, \alpha + \beta, -\alpha\}$ ; gruppen  $\bar{U}_0$  hørende til dette positive delsystem består af alle matricer på formen

$$\begin{bmatrix} 1 & 0 & b \\ a & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

$\{\alpha, \alpha + \beta\}$  er en lukket delmængde af  $A_2^+$ , og den tilhørende lukkede undergruppe bliver gruppen  $\bar{X}_{12}\bar{X}_{13}$  bestående af alle matricer på formen

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

**Sætning 35** (Bruhat-normalform). *Lad  $\Sigma^+$  være et positivt delsystem for  $\Sigma$  og definer  $\bar{U} = \langle \bar{X}_\alpha \mid \alpha \in \Sigma^+ \rangle$  og  $\bar{U}^- = \langle \bar{X}_\alpha \mid \alpha \in -\Sigma^+ \rangle$ . Definer for ethvert  $w \in W(\Sigma)$   $\bar{U}_w$  ved  $\bar{U}_w = \bar{U} \cap (\bar{U}^-)^n$  hvor  $n$  er et element i  $\bar{N}$  der afbildes i  $w$  under afbildningen  $\bar{N} \rightarrow \bar{N}/\bar{T} \cong W(\Sigma)$ . Da gælder:*

- (a)  $U_w$  afhænger ikke af valget af  $n$ , og  $\bar{U}_w = \langle \bar{X}_\alpha \mid \alpha \in \Sigma^+, w(\alpha) \notin \Sigma^+ \rangle$ .
- (b) Ethvert element  $g$  i  $\bar{K}$  har en unik fremstilling på formen  $g = unv$  hvor  $u \in \bar{U}$ ,  $n \in \bar{N}$ ,  $v \in \bar{U}_w$  og  $w$  er billedet af  $n$  under afbildningen  $\bar{N} \rightarrow \bar{N}/\bar{T} \cong W(\Sigma)$ .

*Bevis.* Lad  $n$  og  $n'$  være to elementer i  $\bar{N}$  der begge afbildes i  $w$  under afbildningen  $\bar{N} \rightarrow \bar{N}/\bar{T} \cong W(\Sigma)$ . Da er  $n$  og  $n'$  i samme sideklasse af  $\bar{T}$ , så der findes  $h \in \bar{T}$  så  $n' = hn$ . Idet  $\bar{T}$  normaliserer  $\bar{U}^-$  fås så  $(U^-)^{n'} = (U^-)^{hn} = (U^-)^n$ . Dermed er  $U_w$  uafhængig af valget af  $n$ . Resten af sætningen er [GLS] Theorem 1.11.5.  $\square$

## Grupper af Lie-type

Grupperne af Lie-type er en familie af endelige grupper der kan konstrueres som undergrupper af Lie-grupper. Interessen for dem kommer blandt andet af at mange af de simple grupper er grupper af Lie-type. I dette afsnit beskriver jeg hvordan grupperne af Lie-type konstrueres ud fra simple algebraiske grupper, og jeg præsenterer en række egenskaber ved Chevalley-grupper der nedarves fra de tilsvarende algebraiske grupper.

**Definition 12.** Lad  $\bar{K}$  være en algebraisk gruppe. En *Steinberg-endorphi* af  $\bar{K}$  er en endomorfi af  $\bar{K}$  med endelig fikspunktsmængde. Fikspunktsmængden for en Steinberg-endorphi  $\sigma$  betegnes med  $C_{\bar{K}}(\sigma)$ .

**Sætning 36.** Lad  $\bar{K}$  være en semisimpel algebraisk gruppe med isogener  $\bar{K}_u \rightarrow \bar{K} \rightarrow \bar{K}_a$ . Enhver Steinberg-endorphi af  $\bar{K}$  inducerer en unik Steinberg-endorphi af  $\bar{K}_a$  og kan løftes til en unik Steinberg-endorphi af  $\bar{K}_u$ . Ydermere er  $\sigma$  bijektiv og dermed en automorfi af  $\bar{K}$ .

*Bevis.* Dette er [GLS] Theorem 2.1.2(e) og (a). □

**Definition 13.** En *gruppe af Lie-type* er en endelig gruppe  $K$  hvorom det gælder at der findes en simpel algebraisk gruppe  $\bar{K}$  over  $\bar{\mathbb{F}}_p$  og en Steinberg-endorphi  $\sigma$  af  $\bar{K}$  således at  $K = O^{p'}(C_{\bar{K}}(\sigma))$ . Et  $\sigma$ -*setup* for en gruppe af Lie-type  $K$  er et par  $(\bar{K}, \sigma)$  bestående af en sådan simpel algebraisk gruppe  $\bar{K}$  og Steinberg-endorphi  $\sigma$  af  $\bar{K}$ .

**Sætning 37.** Lad  $K$  være en gruppe af Lie-type med  $\sigma$ -setup  $(\bar{K}, \sigma)$ , og lad  $\bar{K}_u$  og  $\bar{K}_a$  være de universelle hhv. adjungerede versioner af  $\bar{K}$ . Lad  $\sigma_u$  være den unikke Steinberg-endorphi på  $\bar{K}_u$  som  $\sigma$  kan løftes til, og lad  $\sigma_a$  være den unikke Steinberg-endorphi på  $\bar{K}_a$  induceret af  $\sigma$ . Definer  $K_u = O^{p'}(C_{\bar{K}_u}(\sigma_u))$  og  $K_a = O^{p'}(C_{\bar{K}_a}(\sigma_a))$ . Da findes der surjektive gruppehomomorfier  $K_u \rightarrow K \rightarrow K_a$  som fremkommer som restriktioner af isogenerne  $\bar{K}_u \rightarrow \bar{K} \rightarrow \bar{K}_a$ .

*Bevis.* Dette er en omformulering af [GLS] Theorem 2.2.6(a) og (b). □

Givet en gruppe af Lie-type  $K$  med  $\sigma$ -setup  $(\bar{K}, \sigma)$  findes der altså et antal forskellige versioner af  $K$ , svarende til versionerne af  $\bar{K}$ . Præcis som ved de algebraiske grupper er disse versioner netop grupperne  $K_u/Z$  hvor  $Z$  er en undergruppe af  $Z(K_u)$ . Bemærk dog at der godt kan være færre versioner af  $K$  end der er af  $\bar{K}$ . Dette forekommer hvis  $C_{\bar{K}}(\sigma)$  ikke indeholder hele  $Z(\bar{K})$ , således at  $Z(K)$  er mindre end  $Z(\bar{K})$ . I dette tilfælde vil der være versioner af  $\bar{K}$  som  $\sigma$  ikke kan defineres på, da de har formen  $\bar{K}_u/Z$  hvor  $Z$  opfylder  $\sigma(Z) \neq Z$ .

**Sætning 38.** Lad  $\bar{K}$  være en universel semisimpel algebraisk gruppe, og lad  $\sigma$  være en Steinberg-endorphi for  $\bar{K}$ . Da er  $O^{p'}(C_{\bar{K}}(\sigma)) = C_{\bar{K}}(\sigma)$ .

*Bevis.* Dette er [GLS] Theorem 2.2.6(e). □

Næste skridt er at beskrive de mulige Steinberg-endorfier af en simpel algebraisk gruppe.

**Sætning 39.** Lad  $\bar{K}$  være en semisimpel algebraisk gruppe over  $\bar{\mathbb{F}}_p$  med rodsystem  $\Sigma$ . For enhver potens  $q = p^n$  med  $n \in \mathbb{N}$  findes der en unik endomorfi  $\varphi_q$  af  $\bar{K}$  således at  $\varphi_n(x_\alpha(t)) = x_\alpha(t^q)$  for alle  $\alpha \in \Sigma$  og  $t \in \bar{\mathbb{F}}$ . Disse endomorfier er alle bijektive, og er dermed automorfier af  $\bar{K}$  som gruppe. De er ikke automorfier af  $\bar{K}$  som algebraisk gruppe, da deres inverse ikke er morfier af algebraiske grupper. De er alle Steinberg-endorfier, og der gælder  $\varphi_{q_1} \circ \varphi_{q_2} = \varphi_{q_1 q_2}$ .

*Bevis.* Dette er [GLS] Theorem 1.15.4(a). □

**Definition 14.** En *Chevalley-gruppe* er en gruppe af Lie-type med  $\sigma$ -setup  $(\overline{K}, \varphi_q)$ . Gruppen betegnes med  $\Sigma(q)$  hvor  $\Sigma$  er rodsystemet for  $\overline{K}$ .

For ethvert irreducibelt rodsystem  $\Sigma$  findes der således en familie af Chevalley-grupper  $\Sigma(q)$  hvor  $q$  løber over alle printalspotenser. Bemærk at de bijektive morfier mellem  $\overline{K}_a(B_n)$  og  $\overline{K}_a(C_n)$  når det underliggende legeme har karakteristisk 2 fører til isomorfier  $B_n(2^m) \cong C_n(2^m)$  for alle  $m \in \mathbb{N}$ .

**Eksempel 6.** Betragt igen gruppen  $SL_3(\overline{\mathbb{F}})$  fra Eksempel 3. Steinberg-endomorfien  $\varphi_q$  virker på denne gruppe ved

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \mapsto \begin{bmatrix} a^q & b^q & c^q \\ d^q & e^q & f^q \\ g^q & h^q & i^q \end{bmatrix}$$

Dens fikspunktsmængde er netop de matricer i  $SL_3(\overline{\mathbb{F}})$  hvis indgange ligger i  $\mathbb{F}_q$ , legemet med  $q$  elementer. Dette er netop gruppen  $SL_3(\mathbb{F}_q)$ . Da  $SL_3(\overline{\mathbb{F}})$  er universel, er  $SL_3(\mathbb{F}_q)$  så den universelle Chevalley-gruppe  $A_2(q)$ .

**Sætning 40.** Lad  $\overline{K}$  være universel eller adjungeret med rodsystem  $\Sigma$ , lad  $\Pi$  være et fundamentalt system for  $\Sigma$ , og lad  $\rho$  være en isometri af  $\mathbb{R}\Sigma$  der opfylder  $\rho(\Pi) = \Pi$ . Da findes der en unik automorfi  $\gamma_\rho$  af  $\overline{K}$  som opfylder  $\gamma_\rho(x_\alpha(t)) = x_{\rho(\alpha)}(t)$  for alle  $\alpha \in \pm\Pi$  og  $t \in \overline{\mathbb{F}}$ .

*Bevis.* Dette er [GLS] Theorem 1.15.2(a). □

$\gamma_\rho$  er ikke en Steinberg-automorfi, men den sammensatte afbildning  $\gamma_\rho\varphi_q$  er en Steinberg-automorfi for alle  $q$ .

**Definition 15.** En *Steinberg-gruppe* er en gruppe af Lie-type med  $\sigma$ -setup  $(\overline{K}, \gamma_\rho\varphi_q)$  hvor  $\rho$  er ikke-triviel. Gruppen betegnes med  ${}^d\Sigma(q)$  hvor  $\Sigma$  er rodsystemet for  $\overline{K}$  og  $d$  er ordnen af  $\rho$ .

Hvis  $\rho$  er en isometri med  $\rho(\Pi) = \Pi$ , så definerer  $\rho$  en automorfi af Dynkin-diagrammet for  $\Sigma$ . Konstruer nemlig Dynkin-diagrammet ud fra  $\Pi$ ; da inducerer  $\rho$  en permutation af knuderne i diagrammet. Da  $\rho$  er en isometri, bevarer den vinklerne mellem rødderne i  $\Pi$  samt deres indbyrdes længde, og så er den inducerede permutation netop en automorfi af Dynkin-diagrammet. På lignende vis ses at ud fra en automorfi af Dynkin-diagrammet kan man konstruere en isometri  $\rho$  med  $\rho(\Pi) = \Pi$ .

Dette gør det let at opskrive de mulige Steinberg-grupper. Dynkin-diagrammerne for  $A_n$  ( $n \geq 2$ ),  $D_n$  og  $E_6$  har ikke-trivielle automorfier af orden 2, hvilket giver de tre familier  ${}^2A_n(q)$ ,  ${}^2D_n(q)$  og  ${}^2E_6(q)$ . Desuden har Dynkin-diagrammet for  $D_4$  en ikke-triviel automorfi af orden 3, hvilket giver familien  ${}^3D_4(q)$ . (Dynkin-diagrammet for  $D_4$  har faktisk tre forskellige automorfier af orden 2, men de giver same isomorfiklasse af Steinberg-grupper. Tilsvarende for de to automorfier af orden 3.)

**Sætning 41.** Lad  $\overline{K}$  være enten  $B_2(\overline{\mathbb{F}}_2)$ ,  $F_4(\overline{\mathbb{F}}_2)$  eller  $G_2(\overline{\mathbb{F}}_3)$ . Lad  $\Sigma$  være rodsystemet for  $\overline{K}$  og lad  $\Pi$  være et fundamentalt system for  $\Sigma$ . Da findes der en unik isometri  $\rho: \check{\Sigma} \rightarrow \Sigma$  som opfylder  $\rho(\check{\Pi}) = \Pi$ , og der findes en unik endomorfi  $\psi$  af  $\overline{K}$  som opfylder  $\psi(x_\alpha(t)) = x_{\rho(\check{\alpha})}(t)$  hvis  $\alpha$  er lang og  $\psi(x_\alpha(t)) = x_{\rho(\check{\alpha})}(t^p)$  hvis  $\alpha$  er kort. Ydermere er  $\psi$  en Steinberg-automorfi af  $\overline{K}$ , og  $\psi^2 = \varphi_p$ .

*Bevis.* Dette er [GLS] Theorem 1.15.4(b). □

Grunden til at  $\Sigma$  skal være enten  $B_2$ ,  $F_4$  eller  $G_2$  er at dette netop er de selvduale irreducible rodsystemer med to rodlængder. Karakteristikken af det underliggende legeme er valgt så den er lig vægten af den orienterede kant i Dynkin-diagrammet. En lignende konstruktion kan i øvrigt gennemføres for de andre rodsystemer med to rodlængder. Herved fås morfier  $\psi_1 : B_n(\overline{\mathbb{F}}_2) \rightarrow C_n(\overline{\mathbb{F}}_2)$  og  $\psi_2 : C_n(\overline{\mathbb{F}}_2) \rightarrow B_n(\overline{\mathbb{F}}_2)$  som opfylder  $\psi_2\psi_1 = \varphi_2$  og  $\psi_1\psi_2 = \varphi_2$ .

**Definition 16.** En *Suzuki-Ree-gruppe* er en gruppe af Lie-type med  $\sigma$ -setup  $(\overline{K}, \psi\varphi_q)$ . Gruppen betegnes med  ${}^2\Sigma(p^{n+\frac{1}{2}})$  hvor  $p^n = q$ . Her tillades  $q = 1$ , og  $\psi\varphi_1$  er da lig  $\psi$ .

Der findes altså tre familier af Suzuki-Ree-grupper, nemlig  ${}^2B_2(2^{n+\frac{1}{2}})$ ,  ${}^2F_4(2^{n+\frac{1}{2}})$  og  ${}^2G_2(3^{n+\frac{1}{2}})$ . Det viser sig at Chevalley-grupperne, Steinberg-grupperne og Suzuki-Ree-grupperne tilsammen udgør alle grupper af Lie-type.

**Sætning 42.** *Lad  $K$  være en gruppe af Lie-type med  $\sigma$ -setup  $(\overline{K}, \sigma)$ . Ved at konjugere  $\sigma$  med en indre automorfi af  $\overline{K}$ , hvilket ikke ændrer isomorfiklassen af  $O^{p'}(C_{\overline{K}}(\sigma))$ , kan  $\sigma$  bringes på en af formerne  $\varphi_q$ ,  $\gamma_\rho\varphi_q$  og  $\psi\varphi_q$ . I de første to former er  $q$  en positiv potens af  $p$ ; i den sidste er  $q$  en ikke-negativ potens af  $p$ .*

*Bevis.* Dette er [GLS] Theorem 2.2.3. □

Enhver gruppe af Lie-type er således en Chevalley-, Steinberg- eller Suzuki-Ree-gruppe. De adjungerede versioner af disse grupper er næsten alle simple:

**Sætning 43.** *Den adjungerede version af en gruppe af Lie-type er simpel, med præcis følgende otte undtagelser.  $A_1(2)$ ,  $A_1(3)$ ,  ${}^2A_2(2)$  og  ${}^2B_2(\sqrt{2})$  er Frobenius-grupper af orden hhv  $3 \cdot 2$ ,  $4 \cdot 3$ ,  $9 \cdot 8$  og  $5 \cdot 4$ . I  $B_2(2)$ ,  $G_2(2)$ ,  ${}^2F_4(\sqrt{2})$  og  ${}^2G_2(\sqrt{3})$  er kommutatorundergruppen simpel og har indeks  $p$ .*

*Bevis.* Dette er [GLS] Theorem 2.2.7. Bemærk at forfatterne her bruger notation  ${}^2\Sigma(p^{2n+1})$  for Suzuki-Ree-grupperne. □

Kommutatorundergrupperne af  $B_2(2)$ ,  $G_2(2)$  og  ${}^2G_2(\sqrt{3})$  er isomorfe med hhv.  $A_1(9)$ ,  ${}^2A_2(3)$  og  $A_1(8)$ , og de kan derfor uden problemer behandles som grupper af Lie-type. Kommutatorundergruppen af  ${}^2F_4(\sqrt{2})$  er derimod ikke isomorf med en gruppe af Lie-type. Denne gruppe kaldes Tits-gruppen, og den henregnes undertiden til de sporadiske simple grupper.

Den indre struktur af Chevalley-grupperne er ret let at beskrive, da den minder meget om strukturen af de algebraiske grupper. Afbildningen  $t \mapsto t^q$  er en automorfi af  $\overline{\mathbb{F}}$  hvis fikspunktsmængde er et legeme af orden  $q$ ,  $\mathbb{F}_q$ , og elementet  $x_\alpha(t)$  i  $\Sigma(\overline{\mathbb{F}})$  er derfor et fikspunkt for  $\varphi_q$  netop hvis  $t \in \mathbb{F}_q$ . Ydermere har disse elementer orden  $p$ , og de er derfor indeholdt i  $\Sigma(q) = O^{p'}(C_{\varphi_q}(\Sigma(\overline{\mathbb{F}})))$ . Det viser sig at  $\Sigma(q)$  netop er frembragt af elementerne  $x_\alpha(t)$  med  $t \in \mathbb{F}_q$  og  $\alpha \in \Sigma$ .

**Sætning 44.** *Lad  $\Sigma(q)$  være en universel Chevalley-gruppe. Da er  $\Sigma(q)$  frembragt af elementerne  $x_\alpha(t)$  i  $\Sigma(\overline{\mathbb{F}}_q)$  med  $\alpha \in \Sigma$  og  $t \in \mathbb{F}_q$ , og Chevalley-relationerne for  $t, u \in \mathbb{F}_q$  udgør en præsentation af  $\Sigma(q)$ .*

*Bevis.* Dette er [GLS] Theorem 2.4.8 sammen med Remark 2.4.9(c). □

Det er også muligt at konstruere præsentationer af Steinberg- og Suzuki-Ree-grupperne ud fra Chevalley-relationerne, men disse er væsentligt mere komplicerede.

**Sætning 45.** *Lad  $K$  være en Chevalley-gruppe med  $\sigma$ -setup  $(\overline{K}, \varphi_q)$ . Da er  $Z(K) = Z(\overline{K}) \cap K$ .*



*Bevis.* Per [GLS] Proposition 2.5.9(a) er  $Z(K) \subseteq Z(\overline{K})$ , og da  $Z(K) \subseteq K$  må så  $Z(K) \subseteq Z(\overline{K}) \cap K$ . Da  $K \subseteq \overline{K}$  gælder samtidig  $Z(\overline{K}) \cap K = C_K(\overline{K}) \subseteq C_K(K) = Z(K)$ , og så må  $Z(K) = Z(\overline{K}) \cap K$ .  $\square$

**Sætning 46.** *Lad  $K$  være en Chevalley-gruppe med  $\sigma$ -setup  $(\overline{K}, \varphi_q)$ , lad  $\overline{T}$  være en maksimal torus af  $\overline{K}$ , og lad  $\overline{N} = N_{\Sigma(\mathbb{F}_q)}(\overline{T})$ . Definer  $H = \overline{T} \cap K$ ,  $N = \overline{N} \cap K$  og  $H_\alpha = \langle h_\alpha(t) \mid t \in \mathbb{F}_q^\times \rangle$  for hvert  $\alpha \in \Sigma$ . Da gælder:*

- (a)  $H = \langle H_\alpha \mid \alpha \in \Sigma \rangle$ , og for ethvert fundamentalt system  $\Pi$  i  $\Sigma$  er  $H = \langle H_\alpha \mid \alpha \in \Pi \rangle$ .
- (b) Hvis  $\Sigma(q)$  er universel, er  $H_\alpha \cong \mathbb{F}_q^\times$  for hvert  $\alpha \in \Sigma$ , og  $H$  er det direkte produkt af grupperne  $H_\alpha$ ,  $\alpha \in \Pi$ .
- (c)  $H \triangleleft N$  og  $N/H \cong W(\Sigma)$ . Denne isomorfi fremkommer som en restriktion af isomorfien  $\overline{N}/\overline{H} \cong W(\Sigma)$  til  $N$ .

*Bevis.* (a) og (b) er [GLS] Theorem 2.4.7(a) og (d). (c) er [GLS] Theorem 2.3.4(a).  $\square$

**Sætning 47.** *Lad  $K$  være en Chevalley-gruppe med  $\sigma$ -setup  $(\overline{K}, \varphi_q)$ , og definer  $X_\alpha = \overline{X}_\alpha \cap K$  for hvert  $\alpha \in \Sigma(W)$ . Da er  $X_\alpha = \langle x_\alpha(t) \mid t \in \mathbb{F}_q \rangle$ , og for ethvert  $n \in N$  gælder  ${}^n(X_\alpha) = X_{w(\alpha)}$  hvor  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W(\Sigma)$ .*

*Bevis.* Første del er indeholdt i [GLS] Theorem 2.4.1(b), anden del er [GLS] Theorem 2.3.8(b)  $\square$

**Sætning 48.** *Lad  $K$  være en Chevalley-gruppe med  $\sigma$ -setup  $(\overline{K}, \varphi_q)$ , og lad  $\Sigma^+$  være et positivt delsystem for  $\Sigma$  med tilhørende fundamentalt system  $\Pi$ . Lad  $\overline{U} = \langle \overline{X}_\alpha \mid \alpha \in \Sigma^+ \rangle$  og  $\overline{U}^- = \langle \overline{X}_\alpha \mid \alpha \in -\Sigma^+ \rangle$ , og definer  $U = \overline{U} \cap K$  og  $U^- = \overline{U}^- \cap K$ . Da gælder:*

- (a) For enhver total ordning af  $\Sigma^+$  gælder at ethvert element i  $U$  har en unik fremstilling på formen  $\prod_{\alpha \in \Sigma^+} x_\alpha(t_\alpha)$  hvor faktorerne i produktet optræder i rækkefølgen defineret af den totale ordning.
- (b) Definer for ethvert  $w \in W(\Sigma)$   $U_w$  ved  $U_w = U \cap (U^-)^n$  hvor  $n$  er et element i  $N$  der afbildes i  $w$  under afbildningen  $N \rightarrow N/H \cong W(\Sigma)$ . Da er  $U_w = \langle X_\alpha \mid \alpha \in \Sigma^+, w(\alpha) \notin \Sigma^+ \rangle$ . Specielt er  $U \cap U^- = C_1$ .
- (c)  $H$  normaliserer  $U$ , og  $H \cap U = C_1$ .
- (d) For ethvert  $n \in N$  er  $HU \cap (HU^-)^n = H(U \cap (U^-)^n) = HU_w$  hvor  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W(\Sigma)$ .
- (e)  $U$  er en Sylow- $p$ -undergruppe af  $K$ .

*Bevis.* (a) er [GLS] Theorem 2.3.7, (b) og (d) er [GLS] Theorem 2.3.8(b) og (c), og (c) og (e) er [GLS] Theorem 2.3.4(c) og (d).  $\square$

**Sætning 49** (Bruhat-normalform). *Ethvert element  $g$  i  $K$  har en unik fremstilling på formen  $g = unv$  hvor  $u \in U$ ,  $n \in N$ ,  $v \in U_w$ , og  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W(\Sigma)$ .*

*Bevis.* Dette er [GLS] Theorem 2.3.5.  $\square$

## Euler-karakteristik af fusionskategorier

I dette afsnit definerer jeg fusionskategorierne for en endelig gruppe og Euler-karakteristikken af en endelig kategori, og jeg beviser et antal sætninger om Euler-karakteristik af fusionskategorier. Definitionen af Euler-karakteristik for kategorier er hentet fra [Lei] og nogle af resultaterne er taget fra [Ja].

**Definition 17.** Lad  $G$  være en endelig gruppe og  $p$  et primtal der går op i ordenen af  $G$ . *Fusionskategorien for  $G$  ved  $p$*  betegnes med  $\mathcal{F}_p(G)$ . Dens objekter er de ikke-trivielle  $p$ -undergrupper af  $G$ , og dens afbildninger er gruppehomomorfier af formen  $x \mapsto {}^g x$  for et vist  $g \in G$ .

Lad  $P$  være en Sylow- $p$ -undergruppe af  $G$ . Kategorien  $\mathcal{F}_P(G)$  er da den fulde delkategori af  $\mathcal{F}_p(G)$  hvis objekter netop er de ikke-trivielle undergrupper af  $P$ .

De elementer  $g$  i  $G$  som giver anledning til en afbildning  $x \mapsto {}^g x$  er netop elementerne i transporteren  $N_G(H, K) = \{g \in G \mid {}^g H \subseteq K\}$ . To elementer  $g$  og  $g'$  giver samme afbildning netop hvis  $g'x = {}^g x$  for alle  $x \in H$ . Dette er ækvivalent med  $(g^{-1}g')x = x$  for alle  $x \in H$ , således at  $g^{-1}g' \in C_G(H)$ . Dermed giver  $g$  og  $g'$  samme afbildning netop hvis de er indeholdt i samme venstresideklasse af  $C_G(H)$ . Afbildningsmængden  $\mathcal{F}_p(G)(H, K)$  betegnes derfor også  $N_G(H, K)/C_G(H)$ .

Fusionskategorien defineres typisk således at også den trivielle gruppe er et objekt i kategorien. Da denne gruppe altid er et initialt objekt i kategorien, går der ikke noget information tabt ved at udelade den.

Kategorien  $\mathcal{F}_P(G)$  siges også at være et fusionssystem på  $P$ . Der findes en større teori for sådanne fusionssystemer på  $p$ -grupper; et overblik over denne teori præsenteres i [BLO].

**Sætning 50.**  $\mathcal{F}_P(G)$  er ækvivalent med  $\mathcal{F}_p(G)$ .

*Bevis.* Der findes en oplagt inklusionsfunctor  $\mathcal{F}_P(G) \rightarrow \mathcal{F}_p(G)$ , og per definitionen af  $\mathcal{F}_P(G)$  er denne functor bijektiv på afbildningsmængderne. Sylows anden sætning giver desuden at enhver  $p$ -undergruppe af  $G$  er indbyrdes konjugeret med en undergruppe af  $P$ , og dette betyder netop at ethvert objekt i  $\mathcal{F}_p(G)$  er isomorf i kategorien med et objekt i  $\mathcal{F}_P(G)$ .  $\square$

**Definition 18.** *Zeta-funktionen* for en endelig kategori  $\mathcal{C}$  er funktionen  $\zeta : \text{ob } \mathcal{C} \times \text{ob } \mathcal{C} \rightarrow \mathbb{Q}$  givet ved  $\zeta(A, B) = |\mathcal{C}(A, B)|$ . En *vægtning* på  $\mathcal{C}$  er en afbildning  $\kappa : \text{ob } \mathcal{C} \rightarrow \mathbb{Q}$  som opfylder  $\sum_{B \in \text{ob } \mathcal{C}} \zeta(A, B)\kappa(B) = 1$  for ethvert objekt  $A$  i  $\mathcal{C}$ . En *kovægtning* på  $\mathcal{C}$  er en afbildning  $\lambda : \text{ob } \mathcal{C} \rightarrow \mathbb{Q}$  som opfylder  $\sum_{A \in \text{ob } \mathcal{C}} \lambda(A)\zeta(A, B) = 1$  for ethvert objekt  $B$  i  $\mathcal{C}$ . En kategori har *Euler-karakteristik* hvis den har både en vægtning og en kovægtning, og i så fald er dens Euler-karakteristik givet ved  $\chi(\mathcal{C}) = \sum_{A \in \text{ob } \mathcal{C}} \kappa(A)$  hvor  $\kappa$  er en vilkårlig vægtning eller kovægtning.

Idet  $\mathcal{C}$  har endelige afbildningsmængder, er funktionen  $\zeta$  veldefineret, og da  $\mathcal{C}$  kun har endelig mange objekter, er summerne  $\sum_{B \in \text{ob } \mathcal{C}} \zeta(A, B)\kappa(B)$  og  $\sum_{A \in \text{ob } \mathcal{C}} \lambda(A)\zeta(A, B)$  veldefinerede. Euler-karakteristikken for  $\mathcal{C}$  afhænger ikke af valget af (ko)vægtning; dette følger af at der for enhver vægtning  $\kappa$  og kovægtning  $\lambda$  gælder

$$\sum_{A \in \text{ob } \mathcal{C}} \lambda(A) = \sum_{A \in \text{ob } \mathcal{C}} \sum_{B \in \text{ob } \mathcal{C}} \lambda(A)\zeta(A, B)\kappa(B) = \sum_{B \in \text{ob } \mathcal{C}} \kappa(B).$$

Hvis  $\mathcal{C}$  har både en vægtning og en kovægtning, har alle vægtninger og kovægtninger altså samme sum.

**Sætning 51.** *Lad  $\mathcal{C}$  og  $\mathcal{D}$  være ækvivalente kategorier. Hvis  $\mathcal{C}$  har Euler-karakteristik, har  $\mathcal{D}$  det også, og der gælder  $\chi(\mathcal{C}) = \chi(\mathcal{D})$ .*

*Bevis.* Dette er [Lei] Proposition 2.4b. □

**Sætning 52.**  *$\mathcal{F}_p(G)$  har Euler-karakteristik.*

*Bevis.* Dette er [Ja] Korollar 6. □

**Korollar 53.** *Lad  $P$  være en Sylow- $p$ -undergruppe af  $G$ . Da er  $\chi(\mathcal{F}_P(G)) = \chi(\mathcal{F}_p(G))$ .*

*Bevis.* Dette følger af Sætning 50 og Sætning 51. □

**Lemma 54.** *Lad  $H$  og  $K$  være objekter i  $\mathcal{F}_p(G)$ . Da gælder  $\zeta(H, K) = \frac{|N_K(H, K)|}{|C_G(H)|}$ .*

*Bevis.* Per definitionen af  $\mathcal{F}_p(G)$  består afbildningsmængden fra  $H$  til  $K$  netop af de gruppehomomorfier fra  $H$  til  $K$  der har formen  $x \mapsto {}^g x$  for et vist  $g \in G$ . For dette  $g$  gælder så  ${}^g H \subseteq K$ , således at  $g \in N_G(H, K)$ . Enhver afbildning fra  $H$  til  $K$  er således repræsenteret af et element i  $N_G(H, K)$ . Hvis to elementer  $g$  og  $g'$  i  $N_G(H, K)$  repræsenterer samme afbildning fra  $H$  til  $K$  gælder  ${}^g x = {}^{g'} x$  for alle  $x \in H$ . Så er  $x = {}^{g^{-1}g'} x$  for alle  $x \in H$ , således at  $g^{-1}g' \in C_G(H)$ . Dermed er  $g$  og  $g'$  indeholdt i samme venstresideklasse af  $C_G(H)$ .

Lad nu  $g \in N_G(H, K)$  og lad  $gc, c \in C_G(H)$ , være et vilkårligt element i samme venstresideklasse af  $C_G(H)$  som  $g$ . Da er  ${}^{gc} H = {}^g H \subseteq K$ , således at  $gc \in N_G(H, K)$ . Desuden haves  ${}^{gc} x = {}^g x$  for alle  $x \in H$ , så  $g$  og  $gc$  repræsenterer samme afbildning fra  $H$  til  $K$ . Altså er  $N_G(H, K)$  en forening af venstresideklasser af  $C_G(H)$ , og to elementer i  $N_G(H, K)$  repræsenterer samme afbildning hvis og kun hvis de ligger i samme sideklasse.  $N_G(H, K)$  indeholder dermed præcis  $|C_G(H)|$  repræsentanter for hver afbildning fra  $H$  til  $K$ , og så er  $|N_G(H, K)| = \zeta(H, K) \cdot |C_G(H)|$ . □

Det viser sig at det er muligt at beskrive kovægtninger på  $\mathcal{F}_p(G)$  og  $\mathcal{F}_P(G)$ , ved brug af Möbius-funktionen for endelige grupper.

**Definition 19.** Lad  $\mathcal{G}$  være mængden af alle endelige grupper. Möbius-funktionen  $\mu : \mathcal{G} \rightarrow \mathbb{Q}$  er givet ved ligningerne  $\mu(C_1) = 1$  og  $\sum_{H \subseteq G} \mu(H) = 0$  for  $G$  ikke-triviel.

De to ligninger giver en entydig induktiv definition af funktionen, da den anden ligning for enhver ikke-triviel gruppe  $G$  definerer  $\mu(G)$  ud fra værdierne  $\mu(H)$  hvor  $H$  har mindre orden end  $G$ .

Navnet kommer fra Möbius-funktionerne for partielt ordnede mængder. Til en endelig partielt ordnet mængde  $M$  hører en Möbius-funktion  $\mu$  defineret på alle par  $(a, b)$  med  $a, b \in M$  og  $a \leq b$ . Funktionen er defineret så den opfylder ligningerne  $\mu(a, a) = 1$  for ethvert  $a \in M$  og  $\sum_{a \leq x \leq b} \mu(a, x) = \sum_{a \leq x \leq b} \mu(x, b) = 0$  for ethvert par  $(a, b)$  med  $a, b \in M$  og  $a < b$ . Hvis  $M$  er den partielt ordnede mængde af alle undergrupper af en endelig gruppe  $G$  gælder specielt  $\mu_M(C_1, G) = \mu(G)$ , hvor  $\mu_M$  er Möbius-funktionen for  $M$  og  $\mu$  er Möbius-funktionen defineret ovenfor.

Værdierne af Möbius-funktionen er simple at udtrykke for  $p$ -grupper:

**Sætning 55.** *Lad  $G$  være en  $p$ -gruppe. Hvis  $G$  ikke er elementarabelsk, er  $\mu(G) = 0$ . I modsat fald er  $G \cong C_p^n$  for et passende  $n$ , og der gælder så  $\mu(G) = (-1)^n p^{n(n-1)/2}$ .*

*Bevis.* Dette er [Ja] Sætning 21 og Sætning 23. □

Det er nu muligt at give en eksplicit formel for en kovægtning.

**Sætning 56.** Lad  $G$  være en endelig gruppe med Sylow- $p$ -undergruppe  $P$ . En kovægtning på  $\mathcal{F}_p(G)$  er givet ved  $\lambda(H) = \frac{-\mu(H)}{|G:C_G(H)|}$ , og en kovægtning på  $\mathcal{F}_P(G)$  er givet ved  $\lambda(H) = \frac{-\mu(H)}{\zeta(H,P)}$ .

*Bevis.* Dette er [Ja] Sætning 13 og Sætning 25. □

**Korollar 57.** Lad  $\mathcal{S}_p(G)$  være mængden af ikke-trivielle  $p$ -undergrupper af  $G$ , og lad  $\mathcal{A}_p(G)$  være mængden af ikke-trivielle elementarabelske  $p$ -undergrupper af  $G$ . Da er

$$\chi(\mathcal{F}_p(G)) = \sum_{H \in \mathcal{S}_p(G)} \frac{-\mu(H)}{|G:C_G(H)|} = \sum_{H \in \mathcal{A}_p(G)} \frac{-\mu(H)}{|G:C_G(H)|}$$

Lad  $P$  være en Sylow- $p$ -undergruppe af  $G$ ; da gælder yderligere

$$\chi(\mathcal{F}_p(G)) = \sum_{H \in \mathcal{S}_p(P)} \frac{-\mu(H)}{\zeta(H,P)} = \sum_{H \in \mathcal{A}_p(P)} \frac{-\mu(H)}{\zeta(H,P)}$$

*Bevis.* Det første lighedstegn i hver af de to formler følger direkte af Sætning 56; det andet følger af Sætning 55. At man i den anden formel kan skrive  $\chi(\mathcal{F}_p(G))$  i stedet for  $\chi(\mathcal{F}_P(G))$  følger af Korollar 53. □

Der findes desuden et par specialtilfælde hvor  $\chi(\mathcal{F}_p(G))$  er lettere at beregne.

**Sætning 58.** Lad  $G$  være en endelig gruppe, og antag at  $p$  går op i ordenen af  $Z(G)$ . Da er  $\chi(\mathcal{F}_p(G)) = 1$ .

*Bevis.* Dette er [Ja] Sætning 8. □

**Sætning 59.** Lad  $G$  være en endelig gruppe med Sylow- $p$ -undergruppe  $P$ , og antag at  $P$  er normal i  $G$ . Da er  $\chi(\mathcal{F}_p(G)) = \frac{|\mathcal{M}|}{|G|}$ , hvor  $\mathcal{M} = \{x \in G \mid C_P(x) \neq C_1\}$ .

*Bevis.* Per [Ja] Sætning 35 er  $\chi(\mathcal{F}_p(G)) = \frac{|\mathcal{M}|}{|G|}$ , hvor  $\mathcal{M} = \{x \in G \mid p \mid |C_G(x)|\}$ . Nu gælder  $p \mid |C_G(x)|$  hvis og kun hvis  $C_G(x)$  har en ikke-triviell  $p$ -undergruppe. Da  $P$  er normal i  $G$ , er  $P$  den unikke Sylow- $p$ -undergruppe af  $G$ , og dermed indeholder  $P$  alle  $p$ -undergrupper af  $G$ . Så har  $C_G(x)$  en ikke-triviell  $p$ -undergruppe hvis og kun hvis  $C_P(x) = P \cap C_G(x)$  er ikke-triviell. Altså er  $\mathcal{M} = \{x \in G \mid C_P(x) \neq C_1\}$ . □

**Sætning 60.** Lad  $G$  være en endelig gruppe, og lad  $Z$  være en undergruppe af  $Z(G)$  hvis orden ikke er delelig med  $p$ . Da er  $\mathcal{F}_p(G)$  isomorf med  $\mathcal{F}_p(G/Z)$ .

*Bevis.* Lad  $r$  være ordenen af  $Z$ , og lad  $\pi : G \rightarrow G/Z$  være kvotientafbildningen. Der findes en oplagt funktor  $F_\pi : \mathcal{F}_p(G) \rightarrow \mathcal{F}_p(G/Z)$  givet ved  $F_\pi(H) = \pi(H)$  og  $F_\pi(x \mapsto {}^g x) = (x \mapsto \pi({}^g x))$ . Det skal så bevises at denne funktor er bijektiv på mængden af objekter og på afbildningsmængderne.

Lad  $H$  være en undergruppe af  $G/Z$  af orden  $p^n$ ,  $n \in \mathbb{N}$ ;  $\pi^{-1}(H)$  er da en undergruppe af  $G$  af orden  $p^n r$ . Lad nu  $L$  være en Sylow- $p$ -undergruppe af  $\pi^{-1}(H)$ . Da  $p \nmid r$ , har  $L$  orden  $p^n$ . Desuden er  $Z$  indeholdt i  $\pi^{-1}(H)$ , og da  $Z$  har orden  $r$ , er den et  $p$ -komplement i  $\pi^{-1}(H)$ . Så er  $Z \cap L = C_1$ , og da  $Z$  er kernen for  $\pi$ , er  $\pi$  injektiv på  $L$ .  $\pi(L)$  har dermed orden  $p^n$ , og da  $\pi(L) \subseteq H$  og  $H$  har orden  $p^n$ , er  $\pi(L) = H$ . Da  $L$  er en ikke-triviell  $p$ -gruppe, er den et objekt i  $\mathcal{F}_p(G)$ , og der gælder så  $F_\pi(L) = H$ . Dermed er  $F_\pi$  surjektiv på mængden af objekter.

Idet  $Z \subseteq Z(G)$ , er  $ab = ba$  for ethvert  $a \in L$  og  $b \in Z$ . Da  $L$  er en Sylow- $p$ -undergruppe af  $\pi^{-1}(H)$  og  $Z$  er et  $p$ -komplement i  $\pi^{-1}(H)$ , må  $\pi^{-1}(H)$  så være det direkte produkt af  $L$  og  $Z$ . Så er  $L$  den unikke Sylow- $p$ -undergruppe af  $\pi^{-1}(H)$ , og dermed den unikke undergruppe af  $\pi^{-1}(H)$  af orden  $p^n$ . Lad nu  $L'$  være en  $p$ -undergruppe af  $G$  der opfylder  $\pi(L') = H$ . Da er  $L'$  indeholdt i  $\pi^{-1}(H)$  og har orden  $p^m$  med  $m \geq n$ . Da  $\pi^{-1}(H)$  har orden  $p^{nr}$  med  $p \nmid r$  betyder dette at  $L'$  har orden  $p^n$ . Dermed er  $L' = L$ , og  $F_\pi$  er så injektiv og dermed bijektiv på mængden af objekter.

Lad nu  $H$  og  $K$  være  $p$ -undergrupper af  $G/Z$ , og lad  $H'$  og  $K'$  være de unikke Sylow- $p$ -undergrupper af henholdsvis  $\pi^{-1}(H)$  og  $\pi^{-1}(K)$ , således at  $F_\pi(H') = H$  og  $F_\pi(K') = K$ . Lad  $g$  være et element i  $G/Z$  således at  $(x \mapsto {}^g x) \in \mathcal{F}_p(G/Z)(H, K)$ , og lad  $g'$  være et element i  $G$  som opfylder  $\pi(g') = g$ . Da er  $\pi(g' H') = \pi(g')\pi(H') = {}^g H \subseteq K$ , og dermed er  $g' H' \subseteq \pi^{-1}(K)$ . Da  $g' H'$  er en  $p$ -gruppe, er den indeholdt i en Sylow- $p$ -undergruppe af  $\pi^{-1}(K)$ , og så er  $g' H' \subseteq K'$ . Altså er  $(x \mapsto {}^{g'} x) \in \mathcal{F}_p(G)(H', K')$ , og der gælder  $F_\pi(x \mapsto {}^{g'} x) = (x \mapsto {}^g x)$ . Dermed er  $F_\pi$  surjektiv på afbildningsmængderne.

Lad nu  $g'$  og  $g''$  være elementer i  $G$  således at  $(x \mapsto {}^{g'} x) \in \mathcal{F}_p(G)(H', K')$  og  $(x \mapsto {}^{g''} x) \in \mathcal{F}_p(G)(H', K')$ , og antag at  $F_\pi(x \mapsto {}^{g'} x) = F_\pi(x \mapsto {}^{g''} x) = (x \mapsto {}^g x)$ . Da gælder at  $\pi(g')x = {}^g x = \pi(g'')x$  for ethvert  $x \in H$ , og så fås  $\pi(g''^{-1}g')x = x$  for ethvert  $x \in H$ . Da gælder for ethvert  $x' \in H'$  at  $\pi(g''^{-1}g'x') = \pi(g''^{-1}g')\pi(x) = \pi(x)$ , og dermed er  $g''^{-1}g'x' = zx'$  for et vist  $z \in Z$ . Nu har  $zx'$  og  $x'$  samme orden, da konjugation med  $g''^{-1}g'$  er en isomorfi. Idet  $x' \in H'$  og  $H'$  er en  $p$ -gruppe, er ordenen af  $x'$  en potens af  $p$ , og så er ordenen af  $zx'$  også en potens af  $p$ . Men samtidig kommuterer  $z$  og  $x'$ , idet  $z \in Z \subseteq Z(G)$ , og ordenen af  $zx'$  er da lig mindste fælles multiplum af ordenerne af  $z$  og  $x'$ . Altså er ordenen af  $z$  en potens af  $p$ . Men da  $z \in Z$  og  $Z$  har orden ikke delelig med  $p$ , betyder dette at  $z$  har orden 1. Dermed er  $z$  identitetslementet, og så er  $g''^{-1}g'x' = x'$ . Heraf fås  $g'x' = g''x'$ . Da dette gælder for ethvert  $x' \in H'$  er  $(x \mapsto {}^{g'} x) = (x \mapsto {}^{g''} x)$ , og  $F_\pi$  er så injektiv og dermed bijektiv på afbildningsmængderne.  $\square$

Som en umiddelbar konsekvens fås:

**Korollar 61.** *Lad  $G$  være en endelig gruppe, og lad  $Z$  være en undergruppe af  $Z(G)$  hvis orden ikke er delelig med  $p$ . Da er  $\chi(\mathcal{F}_p(G)) = \chi(\mathcal{F}_p(G/Z))$ .*

Det er nu let at beskrive hvordan versionen af en Chevalley-gruppe påvirker Euler-karakteristikken af gruppens fusionskategorier.

**Sætning 62.** *Lad  $K$  være en Chevalley-gruppe og lad  $K_a$  være den adjungerede version af  $K$ . Hvis ordenen af  $Z(K)$  er delelig med  $p$ , er  $\chi(\mathcal{F}_p(K)) = 1$ ; i modsat fald er  $\chi(\mathcal{F}_p(K)) = \chi(\mathcal{F}_p(K_a))$ .*

*Bevis.* Hvis ordenen af  $Z(K)$  er delelig med  $p$  giver Sætning 58 at  $\chi(\mathcal{F}_p(K)) = 1$ . Hvis ordenen af  $Z(K)$  ikke er delelig med  $p$ , giver Korollar 61 at  $\chi(\mathcal{F}_p(K)) = \chi(\mathcal{F}_p(K/Z(K)))$ . Dette er netop det ønskede, da  $K/Z(K) \cong K_a$ .  $\square$

## Det kokarakteristiske tilfælde

I dette afsnit undersøges værdien af  $\chi(\mathcal{F}_p(\Sigma(q)))$ , hvor  $q$  er en potens af  $p$ . Dette viser sig at være temmelig vanskeligt, da  $\mathcal{F}_p(\Sigma(q))$  selv for små rodsystemer er meget kompliceret. Værdien af  $\chi(\mathcal{F}_p(\Sigma(q)))$  beregnes i det tilfælde hvor  $\Sigma$  er enten  $A_1$  eller  $A_2$ , ved brug af anden formel i Sætning 57 samt det faktum at  $U$  er en Sylow- $p$ -undergruppe af  $\Sigma(q)$ . I tilfældet  $\Sigma = A_1$  viser det sig at  $\zeta(L, U)$  har samme værdi for alle undergrupper  $L$  af  $U$ . I tilfældet  $\Sigma = A_2$  er det nødvendigt først at dele  $\mathcal{S}_p(U)$  op i et antal delmængder, således at  $\zeta(L, U)$  er bestemt af hvilken delmængde  $L$  er et element i.

I hele dette afsnit er  $K$  den universelle Chevalley-gruppe  $\Sigma(q)$  og  $\bar{K}$  den universelle semisimple algebraiske gruppe med rodsystem  $\Sigma$ .  $\bar{T}$  er en maksimal torus af  $\bar{K}$  med normalisator  $\bar{N}$ , og  $\bar{X}_\alpha$ ,  $\alpha \in \Sigma$  er  $\bar{T}$ -rodgrupperne i  $\bar{K}$ .  $\Sigma^+$  er et positivt delsystem af  $\Sigma$ ,  $\bar{U}$  er gruppen  $\langle \bar{X}_\alpha \mid \alpha \in \Sigma^+ \rangle$  og  $\bar{U}^-$  er gruppen  $\langle \bar{X}_\alpha \mid \alpha \in -\Sigma^+ \rangle$ . Endelig er  $H = \bar{T} \cap K$ ,  $N = \bar{N} \cap K$ ,  $U = \bar{U} \cap K$  og  $U^- = \bar{U}^- \cap K$ , og  $W$  er Weyl-gruppen for  $\Sigma$ . For ethvert  $w \in W$  defineres  $U_w = U \cap (U^-)^n$  og  $U'_w = U \cap U^n$  hvor  $n$  er et element der afbildes i  $w$  under afbildningen  $N \rightarrow N/H \cong W$ . For en gruppe  $G$  er  $\mathcal{S}_p(G)$  mængden af ikke-trivielle  $p$ -undergrupper af  $G$ .  $\zeta$  er zeta-funktionen for  $\mathcal{F}_p(K)$ , og  $\mu$  er Möbius-funktionen. Når  $L$  og  $M$  er undergrupper af  $K$ , er  $N_K(L, M)$  transportereren fra  $L$  til  $M$ .

Først haves nogle generelle lemmata.

**Lemma 63.**  $p \nmid |Z(K)|$ .

*Bevis.* Per Sætning 29 og Sætning 45 er  $Z(K)$  isomorf med en gruppe af enhedsrødder i  $\mathbb{F}_q$ , eller med det direkte produkt af to sådanne grupper. Men 1 er den eneste  $p$ 'te enhedsrod i et legeme af karakteristisk  $p$ , og så må  $p \nmid |Z(K)|$ .  $\square$

Per Sætning 62 er  $\chi(\mathcal{F}_p(K))$  så uafhængig af versionen af  $K$ . Det er derfor ikke nogen indskrænkning at fokusere på den universelle version.

**Lemma 64.**  $U'_w = \langle X_\alpha \mid \alpha \in \Sigma^+, w(\alpha) \in \Sigma^+ \rangle$ .

*Bevis.* Per Sætning 8 og Sætning 9 findes der et element  $w_0 \in W$  som opfylder  $w_0(-\Sigma^+) = \Sigma^+$ . Så fås for ethvert  $w \in W$  at  $U'_w = U \cap U^n = U \cap (U^-)^{n_0 n} = U_{w_0 w}$  hvor  $n_0$  og  $n$  er elementer i  $N$  der afbildes i hhv.  $w_0$  og  $w$ . Sætning 48(b) giver så  $U'_w = U_{w_0 w} = \langle x_\alpha \mid \alpha \in \Sigma^+, (w_0 w)(\alpha) \notin \Sigma^+ \rangle$ . Men der gælder  $(w_0 w)(\alpha) \notin \Sigma^+$  hvis og kun hvis  $w_0(w(\alpha)) \in -\Sigma^+$ , og dette gælder hvis og kun hvis  $w(\alpha) \in \Sigma^+$ . Dermed er  $U'_w = \langle x_\alpha \mid \alpha \in \Sigma^+, w(\alpha) \in \Sigma^+ \rangle$ .  $\square$

**Lemma 65.** Lad  $u_0 \in U$  og  $g \in K$ , og skriv  $g$  på Bruhat-normalform:  $g = unv$ . Der gælder  ${}^g u_0 \in U$  hvis og kun hvis  ${}^v u_0 \in U'_w$  hvor  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W$ .

*Bevis.* Antag først at  ${}^g u_0 \in U$  og lad  $u_1 = {}^g u_0 = unv u_0$ . Da er  ${}^{nv} u_0 = u^{-1} u_1 \in U$ , og så fås  ${}^v u_0 \in U^n$ . Da der samtidig gælder  $u_0 \in U$  og  $v \in U$  fås også  ${}^v u_0 \in U$ , og så er  ${}^v u_0 \in U'_w$ . Omvendt ses at hvis  ${}^v u_0 \in U'_w \subseteq U^n$ , er  ${}^{nv} u_0 \in U$ , og da  $u \in U$  fås så  ${}^g u_0 = unv u_0 \in U$ .  $\square$

**Lemma 66.** Lad  $U' \subseteq U$  være ikke-triviell. Da gælder  $\sum_{L \in \mathcal{S}_p(U')} -\mu(L) = 1$ .

*Bevis.* Idet  $U'$  er ikke-triviell, gælder per definitionen af Möbius-funktionen gælder  $\sum_{L \subseteq U'} \mu(L) = 0$ . Da  $U$  er en  $p$ -gruppe er  $U'$  det også. Så er alle undergrupper af  $U'$   $p$ -grupper, så  $\mathcal{S}_p(U')$  består af alle ikke-trivielle undergrupper af  $U'$ . Så fås

$$\sum_{L \in \mathcal{S}_p(U')} -\mu(L) = \mu(C_1) - \mu(C_1) - \sum_{L \in \mathcal{S}_p(U')} \mu(L) = 1 - \sum_{L \subseteq U} \mu(L) = 1$$

□

Nu undersøges tilfældet  $\Sigma = A_1$ .  $A_1$  består af de to rødder  $\alpha$  og  $-\alpha$ , og  $W$  har så præcis to elementer, nemlig identiteten  $e$  og reflektionen  $r_\alpha$ .

**Lemma 67.** *Lad  $\Sigma = A_1$ , og skriv  $W = \{e, r_\alpha\}$ . Der gælder  $U_e = C_1$ ,  $U_{r_\alpha} = U$ ,  $U'_e = U$  og  $U'_{r_\alpha} = C_1$ .*

*Bevis.* Lad  $\alpha$  være det unikke element i  $\Sigma^+$ ; da gælder  $e(\alpha) = \alpha \in \Sigma^+$  og  $r_\alpha(\alpha) = -\alpha \notin \Sigma^+$ . Resultatet følger nu af Sætning 48(b) og Lemma 64. □

**Lemma 68.** *Lad  $\Sigma = A_1$ . Da er  $|H| = q - 1$ .*

*Bevis.* Per Sætning 46(b) er  $H \cong (\mathbb{F}_q^\times)^{\dim(\Sigma)}$ , og da  $A_1$  har dimension 1, er  $H \cong \mathbb{F}_q^\times$ .  $\mathbb{F}_q^\times$  har orden  $q - 1$ , og så er  $|H| = q - 1$ . □

**Lemma 69.** *Lad  $\Sigma = A_1$  og lad  $x \in U$  være et element forskelligt fra identiteten. Da er  $N_K(x, U) = HU$ .*

*Bevis.* Lad  $g \in N_K(x, U)$  og skriv  $g$  på Bruhat-normalform:  $g = unv$ . Per Lemma 65 gælder så  ${}^v x \in U'_w$ , og da  $x$  ikke er identiteten, er  ${}^v x$  det heller ikke. Dermed er  $U'_w \neq C_1$ , og per Lemma 67 må så  $w = e$ . Dermed er  $n \in H$ . Yderligere er  $U_w = U_e = C_1$ , og da  $v \in U_w$  medfører dette at  $v$  er identiteten. Dermed gælder  $g = un$  hvor  $u \in U$  og  $n \in H$ , og så er  $g \in HU$ . Altså er  $N_K(x, U) \subseteq HU$ . Omvendt giver Sætning 48(c) at  $HU$  normaliserer  $U$ , og da  $x \in U$  må så  $HU \subseteq N_K(x, U)$ . Dermed er  $N_K(x, U) = HU$ . □

**Lemma 70.** *Lad  $\Sigma = A_1$  og lad  $x \in U$  være et element forskelligt fra identiteten. Da er  $C_K(x) = ZU$  hvor  $Z \subseteq H$  er en gruppe af orden  $\gcd(q - 1, 2)$ .*

*Bevis.* Idet  $x \in U$ , er  $C_K(x) \subseteq N_K(x, U) = HU$ . Lad nu  $g$  være et vilkårligt element i  $HU$  og skriv  $g = hu$  med  $h \in H$  og  $u \in U$ . Lad  $\alpha$  være det unikke element i  $\Sigma^+$ ; da gælder  $h = h_\alpha(s)$  og  $u = x_\alpha(s')$  for passende  $s \in \mathbb{F}_q^\times$  og  $s' \in \mathbb{F}_q$ , således at  $g = h_\alpha(s)x_\alpha(s')$ . Skriv  $x$  på formen  $x = x_\alpha(t)$  med  $t \in \mathbb{F}_q$  og  $t \neq 0$ . Da giver relationerne i Sætning 31 at

$${}^g x = h_\alpha(s)x_\alpha(s')x_\alpha(t) = h_\alpha(s)x_\alpha(t) = x_\alpha(s^{\langle \alpha, \alpha \rangle} t)$$

Idet  $\langle \alpha, \alpha \rangle = 2$  er så  ${}^g x = x_\alpha(s^2 t)$ . Da  $t \neq 0$  er dette lig  $x_\alpha(t)$  hvis og kun hvis  $s^2 = 1$ . Lad  $\mathbb{F}_q^{(2)}$  være undergruppen af  $\mathbb{F}_q^\times$  bestående af alle elementer  $s$  der opfylder  $s^2 = 1$ ; da  $\mathbb{F}_q^\times$  er cyklisk af orden  $q - 1$  har  $\mathbb{F}_q^{(2)}$  orden  $\gcd(q - 1, 2)$ . Lad nu  $Z = \{h_\alpha(s) \mid s \in \mathbb{F}_q^{(2)}\}$ ; da gælder altså  ${}^g x = x$  hvis og kun hvis  $h \in Z$ , mens  $u$  kan være et vilkårligt element i  $U$ . Altså er  $C_K(x) = ZU$ . □

Gruppen  $Z$  er faktisk centeret af  $K$ .

**Sætning 71.** *Lad  $\Sigma = A_1$  og lad  $L \in \mathcal{S}_p(U)$ . Der gælder  $\zeta(L, U) = \frac{q-1}{\gcd(q-1, 2)}$ .*

*Bevis.* Da  $L$  er en ikke-triviell undergruppe af  $U$ , giver Lemma 69 at  $N_K(L, U) = HU$ , og Lemma 70 giver at  $C_K = ZU$ . Per Sætning 48(c) er  $H \cap U = C_1$ , så  $|HU| = |H| \cdot |U|$  og  $|ZU| = |Z| \cdot |U|$ . Så fås

$$\zeta(L, U) = \frac{|N_K(L, U)|}{|C_K(L)|} = \frac{|HU|}{|ZU|} = \frac{|H| \cdot |U|}{|Z| \cdot |U|} = \frac{|H|}{|Z|} = \frac{q-1}{\gcd(q-1, 2)}$$

hvor sidste lighedstegn følger af Lemma 68. □

**Sætning 72.** Lad  $\Sigma = A_1$ . Da er  $\chi(\mathcal{F}_p(K)) = \frac{\gcd(q-1,2)}{q-1}$ .

*Bevis.* Per Sætning 48(e) og Korollar 57 er  $\chi(\mathcal{F}_p(K)) = \sum_{L \in \mathcal{S}_p(U)} \frac{-\mu(L)}{\zeta(L,U)}$ . Med Sætning 71 og Lemma 66 fås så

$$\begin{aligned} \chi(\mathcal{F}_p(K)) &= \sum_{L \in \mathcal{S}_p(U)} \frac{-\mu(L)}{\zeta(L,U)} = \sum_{L \in \mathcal{S}_p(U)} \frac{-\mu(L) \cdot \gcd(q-1,2)}{q-1} \\ &= \frac{\gcd(q-1,2)}{q-1} \sum_{L \in \mathcal{S}_p(U)} -\mu(L) = \frac{\gcd(q-1,2)}{q-1} \end{aligned}$$

□

Lad nu  $\Sigma = A_2$ . Per Sætning 16 består  $\Sigma$  så af vektorerne  $e_i - e_j$  med  $i, j \in \{1, 2, 3\}$ . Definer  $\alpha = e_2 - e_3$ ,  $\beta = e_1 - e_2$  og  $\gamma = \alpha + \beta = e_1 - e_3$ ; da er  $\Sigma^+ = \{\alpha, \beta, \gamma\}$  et positivt delsystem i  $\Sigma$  og  $\Pi = \{\alpha, \beta\}$  er det tilhørende fundamentale system. Denne notation fastholdes i resten af afsnittet. Nu giver Sætning 48(a) at ethvert element i  $U$  har en unik fremstilling på formen  $x_\alpha(a)x_\beta(b)x_\gamma(c)$  med  $a, b, c \in \mathbb{F}_q$ . Ved brug af Chevalley-relationerne fås så at der gælder  $(x_\alpha(a)x_\beta(b)x_\gamma(c))(x_\alpha(a')x_\beta(b')x_\gamma(c')) = x_\alpha(a+a')x_\beta(b+b')x_\gamma(c+c' \pm a'b)$ . Fortegnet på  $a'b$  kan ikke læses ud af Chevalley-relationerne, men det kan faktisk vælges frit. Definer nemlig  $x'_\gamma$  og  $x'_{-\gamma}$  ved  $x'_\gamma(c) = x_\gamma(-c)$  og  $x'_{-\gamma}(c) = x_{-\gamma}(-c)$ ; da giver [GLS] Remark 1.12.10 at ved at udskifte  $x_\gamma$  og  $x_{-\gamma}$  med  $x'_\gamma$  og  $x'_{-\gamma}$  fås et nyt sæt af frembringere der opfylder Chevalley-relationerne. Direkte udregning viser så at denne udskiftning fører til at fortegnet på  $a'b$  i ovenstående udregning ændres.

Nu fastlægges  $x_\gamma$  således at fortegnet på  $a'b$  i ovenstående udregning er positivt. For at lette notationen skrives nu  $\omega(a, b, c)$  for  $x_\alpha(a)x_\beta(b)x_\gamma(c)$ . Da består  $U$  netop af elementerne  $\omega(a, b, c)$  med  $a, b, c \in \mathbb{F}_q$ , og der gælder  $\omega(a, b, c)\omega(a', b', c') = \omega(a+a', b+b', c+c'+a'b)$ .

**Lemma 73.** Lad  $\Sigma = A_2$  og lad  $\omega(a, b, c)$  være et vilkårligt element i  $U$ . Lad  $u \in U$  og skriv  $u = \omega(x, y, z)$ ; da gælder  ${}^u\omega(a, b, c) = \omega(a, b, c + ay - bx)$ . Lad  $h \in H$  og skriv  $h = h_\alpha(s)h_\beta(t)$ ; da gælder  ${}^h\omega(a, b, c) = \omega(at^{-1}s^2, bt^2s^{-1}, cts)$ .

*Bevis.* Bemærk først at der gælder  $\omega(x, y, z)^{-1} = \omega(-x, -y, -z + xy)$ , idet

$$\omega(x, y, z)\omega(-x, -y, -z + xy) = \omega(x - x, y - y, z + (-z + xy) + (-y)x) = \omega(0, 0, 0)$$

Så fås

$$\begin{aligned} {}^u\omega(a, b, c) &= \omega(x, y, z)\omega(a, b, c) = \omega(x, y, z)\omega(a, b, c)\omega(-x, -y, -z + xy) \\ &= \omega(x, y, z)\omega(a - x, b - y, c - z + xy - xb) \\ &= \omega(a, b, c + xy - xb + (a - x)y) = \omega(a, b, c + ay - bx) \end{aligned}$$

Ved direkte udregning ses nu at der gælder  $\langle \alpha, \alpha \rangle = 2$ ,  $\langle \beta, \alpha \rangle = -1$ ,  $\langle \gamma, \alpha \rangle = 1$ ,  $\langle \alpha, \beta \rangle = -1$ ,  $\langle \beta, \beta \rangle = 2$  og  $\langle \gamma, \beta \rangle = 1$ . Så giver Sætning 31(g) at:

$$\begin{aligned} {}^h\omega(a, b, c) &= h_\alpha(s)h_\beta(t)\omega(a, b, c) = h_\alpha(s)\omega(at^{\langle \alpha, \beta \rangle}, bt^{\langle \beta, \beta \rangle}, ct^{\langle \gamma, \beta \rangle}) \\ &= h_\alpha(s)\omega(at^{-1}, bt^2, ct) = \omega(at^{-1}s^{\langle \alpha, \alpha \rangle}, bt^2s^{\langle \beta, \alpha \rangle}, cts^{\langle \gamma, \alpha \rangle}) \\ &= \omega(at^{-1}s^2, bt^2s^{-1}, cts) \end{aligned}$$

□



**Lemma 74.** Lad  $\Sigma = A_2$ . Da er  $W = \{e, r_\alpha, r_\beta, r_\gamma, r_\alpha r_\beta, r_\beta r_\alpha\}$ , og der gælder  $r_\gamma = r_\alpha r_\beta r_\alpha = r_\beta r_\alpha r_\beta$ . Værdierne af  $w(\delta)$  for  $w \in W$  og  $\delta \in \Sigma^+$  ses i nedenstående tabel.

$w$	$e$	$r_\alpha$	$r_\beta$	$r_\gamma$	$r_\alpha r_\beta$	$r_\beta r_\alpha$
$\alpha$	$\alpha$	$-\alpha$	$\gamma$	$-\beta$	$\beta$	$-\gamma$
$\beta$	$\beta$	$\gamma$	$-\beta$	$-\alpha$	$-\gamma$	$\alpha$
$\gamma$	$\gamma$	$\beta$	$\alpha$	$-\gamma$	$-\alpha$	$-\beta$

*Bevis.* At opskrive tabellen er rent regnearbejde. Eksempelvis er  $r_\alpha(\gamma) = \gamma - \langle \beta, \alpha \rangle \alpha = \gamma - \alpha = (\alpha + \beta) - \alpha = \beta$ , og de andre udregninger er meget tilsvarende. Når dette er gjort, er det let at konstatere at  $r_\gamma = r_\alpha r_\beta r_\alpha = r_\beta r_\alpha r_\beta$ , da det blot skal verificeres at disse elementer virker ens på rødderne i  $\Sigma$ . Med disse relationer kan det så vises at der ikke findes yderligere elementer i  $W$ . Eksempelvis er  $(r_\gamma)(r_\alpha r_\beta) = (r_\alpha r_\beta r_\alpha)(r_\alpha r_\beta) = r_\alpha r_\beta (r_\alpha r_\alpha) r_\beta = r_\alpha r_\beta r_\beta = r_\alpha$ , og de andre udregninger er meget tilsvarende.  $\square$

**Lemma 75.** Lad  $\Sigma = A_2$ . Værdierne af  $U_w$  og  $U'_w$  for  $w \in W$  ses i nedenstående tabel.

$w$	$e$	$r_\alpha$	$r_\beta$	$r_\gamma$	$r_\alpha r_\beta$	$r_\beta r_\alpha$
$U_w$	$C_1$	$X_\alpha$	$X_\beta$	$U$	$X_\beta X_\gamma$	$X_\alpha X_\gamma$
$U'_w$	$U$	$X_\beta X_\gamma$	$X_\alpha X_\gamma$	$C_1$	$X_\alpha$	$X_\beta$

*Bevis.* Dette følger af Sætning 48(b), Lemma 64 og Lemma 74.  $\square$

**Definition 20.** Lad  $\Sigma = A_2$ . Definer for hvert  $x \in \mathbb{F}_q^\times$   $U_x = \{\omega(a, ax, c) \mid a, c \in \mathbb{F}_q\}$ , og definer  $U_0 = \{\omega(a, 0, c) \mid a, c \in \mathbb{F}_q\}$  og  $U_\infty = \{\omega(0, b, c) \mid b, c \in \mathbb{F}_q\}$ . Definer yderligere  $Y = \{\omega(0, 0, c) \mid c \in \mathbb{F}_q\}$  og definer for hvert  $y \in \mathbb{F}_q$   $V_y^0$  og  $V_y^\infty$  ved  $V_y^0 = \{\omega(a, 0, ya) \mid a \in \mathbb{F}_q\}$  og  $V_y^\infty = \{\omega(0, b, yb) \mid b \in \mathbb{F}_q\}$ . Definer endelig  $\mathcal{S}'_p(U) = \mathcal{S}_p(U) \setminus (\bigcup_{x \in \mathbb{F}_q \cup \{\infty\}} \mathcal{S}_p(U_x))$ ,  $\mathcal{S}'_p(U_x) = \mathcal{S}_p(U_x) \setminus \mathcal{S}_p(Y)$  for hvert  $x \in \mathbb{F}_q^\times$ ,  $\mathcal{S}'_p(U_0) = \mathcal{S}_p(U_0) \setminus (\mathcal{S}_p(Y) \cup (\bigcup_{y \in \mathbb{F}_q} \mathcal{S}_p(V_y^0)))$  og  $\mathcal{S}'_p(U_\infty) = \mathcal{S}_p(U_\infty) \setminus (\mathcal{S}_p(Y) \cup (\bigcup_{y \in \mathbb{F}_q} \mathcal{S}_p(V_y^\infty)))$ .

Ved direkte udregning ses at  $U_x, Y, V_y^0$  og  $V_y^\infty$  alle er undergrupper af  $U$ . Det er desuden klart at der gælder  $Y \subset U_x$  for hvert  $x \in \mathbb{F}_q \cup \{\infty\}$  og  $V_y^0 \subset U_0$  og  $V_y^\infty \subset U_\infty$  for hvert  $y \in \mathbb{F}_q$ .

Bemærk i øvrigt at der gælder  $X_\alpha = V_0^0$ ,  $X_\beta = V_0^\infty$ ,  $X_\gamma = Y$ ,  $X_\alpha X_\gamma = U_0$  og  $X_\beta X_\gamma = U_\infty$ .

Pointen med alle disse definitioner ses i følgende lemma:

**Lemma 76.** Lad  $\Sigma = A_2$ .  $\mathcal{S}_p(U)$  er en disjunkt forening af mængderne  $\mathcal{S}'_p(U)$ ,  $\mathcal{S}'_p(U_x)$  for  $x \in \mathbb{F}_q \cup \{\infty\}$ ,  $\mathcal{S}_p(V_y^0)$  for  $y \in \mathbb{F}_q$ ,  $\mathcal{S}_p(V_y^\infty)$  for  $y \in \mathbb{F}_q$  og  $\mathcal{S}_p(Y)$ .

*Bevis.* Lad  $G$  være et vilkårligt element i  $\mathcal{S}_p(U)$ , så  $G$  er en ikke-triviell undergruppe af  $U$ . Hvis  $G \not\subseteq U_x$  for alle  $x \in \mathbb{F}_q \cup \{\infty\}$ , er  $G$  et element i  $\mathcal{S}'_p(U)$ , men ikke i nogle af de andre mængder. Hvis der findes forskellige  $x, x' \in \mathbb{F}_q \cup \{\infty\}$  så  $G \subseteq U_x$  og  $G \subseteq U_{x'}$ , så er  $G \subseteq U_x \cap U_{x'}$ . Ved direkte beregning ses  $U_x \cap U_{x'} = Y$ , så  $G \subseteq Y$ . Dermed er  $G$  et element i  $\mathcal{S}_p(Y)$ . Desuden er  $G$  ikke et element i  $\mathcal{S}'_p(U)$  eller  $\mathcal{S}'_p(U_x)$  for noget  $x \in \mathbb{F}_q \cup \{\infty\}$ , på grund af den måde disse mængder er defineret. Ved direkte beregning ses desuden  $Y \cap V_y^0 = C_1$  og  $Y \cap V_y^\infty = C_1$  for alle  $y \in \mathbb{F}_q$ , så  $G$  er heller ikke et element i  $\mathcal{S}_p(V_y^0)$  eller  $\mathcal{S}_p(V_y^\infty)$  for noget  $y \in \mathbb{F}_q$ . Igen ses så at  $G$  er et element i netop én af mængderne i listen.

Tilbage er nu muligheden at der gælder  $G \subseteq U_x$  for netop ét  $x \in \mathbb{F}_q \cup \{\infty\}$ . Da er  $G \not\subseteq Y$ , da  $Y \subseteq U_x$  for alle  $x \in \mathbb{F}_q \cup \{\infty\}$ . Betragt først tilfældet  $x \in \mathbb{F}_q^\times$ ; da er  $G$  et element i  $\mathcal{S}'_p(U_x)$ , men ikke i nogle af de andre mængder. Tilbage er så tilfældene  $x = 0$  og  $x = \infty$ . Betragt tilfældet  $x = 0$ ; tilfældet  $x = \infty$  er helt analogt. Da gælder  $G \subseteq U_0$  og  $G \not\subseteq Y$ . For forskellige  $y, y' \in \mathbb{F}_q$  fås ved direkte beregning  $V_y^0 \cap V_{y'}^0 = C_1$ , så der findes højst ét  $y \in \mathbb{F}_q$  så  $G \subseteq V_y^0$ . Hvis et sådant  $y$  findes, er

$G$  et element i  $\mathcal{S}_p(V_y^0)$ , men ikke i nogle af de andre mængder; hvis ikke, er  $G$  et element i  $\mathcal{S}'_p(U_0)$ , men ikke i nogle af de andre mængder. I alle tilfælde ses altså at  $G \in \mathcal{S}_p(U)$  er et element i netop én af mængderne i listen, så  $\mathcal{S}_p(U)$  er en disjunkt forening af disse mængder.  $\square$

Ideen er nu at beregne  $\chi(\mathcal{F}_p(K))$  med Korollar 57 ved at dele summen op som i Lemma 76.

**Sætning 77.** Lad  $\Sigma = A_2$  og  $L \in \mathcal{S}'_p(U)$ . Da er  $\mu(L) = 0$ .

*Bevis.* Lad  $\omega(a, b, c)$  være et vilkårligt element i  $L$  som opfylder at  $a$  og  $b$  ikke begge er 0; dette kan lade sig gøre da  $G \not\subseteq Y$ . Definer  $x$  ved  $x = ba^{-1}$  hvis  $a \neq 0$  og  $x = \infty$  hvis  $a = 0$ ; da er  $\omega(a, b, c) \in U_x$ . Yderligere ses at hvis  $\omega(a', b', c')$  er et element i  $L$  der opfylder  $ab' = a'b$ , så er  $\omega(a', b', c') \in U_x$ . Hvis  $a \neq 0$  fås nemlig  $b' = a'ba^{-1} = a'x$ ; dette giver at  $\omega(a', b', c') \in U_x$ . Hvis  $a = 0$  fås i stedet  $a'b = 0$ , og da det blev antaget at  $a$  og  $b$  ikke begge er 0, fås så  $b \neq 0$  og dermed  $a' = 0$ . Så er  $\omega(a', b', c') \in U_\infty$ .

Hvis ethvert andet element  $\omega(a', b', c') \in L$  opfylder  $ab' = a'b$  fås altså  $L \subseteq U_x$  for passende  $x$ . Men da  $L \in \mathcal{S}'_p(U)$  er  $L \not\subseteq U_x$  for alle  $x \in \mathbb{F}_q \cup \{\infty\}$ , og der må derfor findes et  $\omega(a', b', c') \in L$  som opfylder  $ab' \neq a'b$ . Så fås  $\omega(a, b, c)\omega(a', b', c') = \omega(a + a', b + b', c + c' + ab)$  og  $\omega(a', b', c')\omega(a, b, c) = \omega(a + a', b + b', c + c' + ab')$ . Da  $ab' \neq a'b$  er disse to elementer forskellige, så  $\omega(a, b, c)$  og  $\omega(a', b', c')$  kommuterer ikke. Dermed er  $L$  ikke abelsk, og Sætning 55 giver så  $\mu(L) = 0$ .  $\square$

Som et umiddelbart korollar fås:

**Korollar 78.** Lad  $\Sigma = A_2$ . Da er  $\sum_{L \in \mathcal{S}'_p(U)} \frac{-\mu(L)}{\zeta(L, U)} = 0$ .

**Sætning 79.** Lad  $\Sigma = A_2$ ,  $x \in \mathbb{F}_q^\times$  og  $L \in \mathcal{S}'_p(U_x)$ . Da er  $N_K(L, U) = HU$ .

*Bevis.* Da  $L \in \mathcal{S}'_p(U_x)$  er  $L \subseteq U_x$  og  $L \not\subseteq Y$ . Derfor findes der et element  $\omega(a, ax, c) \in L$  med  $a \neq 0$ . Lad nu  $g \in N_K(L, U)$ , og skriv  $g$  på Bruhat-normalform:  $g = unv$ . Da er  ${}^g\omega(a, ax, c) \in U$ , og per Lemma 65 haves så  ${}^v\omega(a, ax, c) \in U'_w$  hvor  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W$ . Da  $v \in U$  giver Lemma 73 at  ${}^v\omega(a, ax, c)$  har formen  $\omega(a, ax, c')$  for passende  $c'$ . Da  $a \neq 0$  og  $x \neq 0$  medfører dette at  ${}^v\omega(a, ax, c)$  ikke er indeholdt i nogle af grupperne  $X_\alpha, X_\beta, X_\gamma, X_\alpha X_\gamma$  og  $X_\beta X_\gamma$ . Så giver Lemma 75 at  $w = e$ , og så er  $n \in H$  og  $v \in U_e = C_1$ . Altså har  $g$  formen  $un$  med  $u \in U$  og  $n \in H$ , så  $g \in HU$ . Dermed er  $N_K(L, U) \subseteq HU$ .

Af Sætning 48(c) fås at  $HU$  normaliserer  $U$ , og da  $L \subset U$  må så  $HU \subseteq N_K(L, U)$ . Altså er  $N_K(L, U) = HU$ .  $\square$

**Sætning 80.** Lad  $\Sigma = A_2$ ,  $x \in \mathbb{F}_q^\times$  og  $L \in \mathcal{S}'_p(U_x)$ . Da er  $C_K(L) = ZU_x$  hvor  $Z$  er en undergruppe af  $H$  af orden  $\gcd(q-1, 3)$ .

*Bevis.* Da  $L \subseteq U$  er  $C_K(L) \subseteq N_K(L, U) = HU$ . Lad nu  $\omega(a, ax, c)$  være et vilkårligt element i  $L$  som opfylder  $a \neq 0$ , og lad  $hu$  være et vilkårligt element i  $HU$  og skriv  $h = h_\alpha(s)h_\beta(t)$  og  $u = \omega(a', b', c')$ . Per Lemma 73 gælder så

$${}^{hu}\omega(a, ax, c) = {}^h\omega(a, ax, c + ab' - axa') = \omega(at^{-1}s^2, axt^2s^{-1}, (c + ab' - axa')ts)$$

Hvis dette skal være lig  $\omega(a, b, c)$  skal der for det første gælde  $at^{-1}s^2 = a$ ; da  $a \neq 0$  medfører dette  $t^{-1}s^2 = 1$ . Dermed er  $t = s^2$ . Ligeledes skal der gælde  $axt^2s^{-1} = ax$ , og da  $ax \neq 0$  medfører dette  $t^2s^{-1} = 1$ . Ved at kombinere disse to ligninger fås  $s^3 = (s^2)^2s^{-1} = t^2s^{-1} = 1$ , så  $s$  er en tredje enhedsrod. Definer så  $Z = \{h_\alpha(s)h_\beta(s^2) \mid s^3 = 1\}$ ; det er så nødvendigt at  $h \in Z$ .

Det skal nu også gælde at  $(c + ab' - axa')ts = c$ . Af  $t = s^2$  og  $s^3 = 1$  fås  $ts = s^2s = s^3 = 1$ , så denne ligning reduceres til  $c + ab' - axa' = c$ . Heraf fås  $ab' = axa'$ , og da  $a \neq 0$ , haves så  $b' = xa'$ . Men dette betyder netop at  $u \in U_x$ . Dermed er  $hu \in ZU_x$ , og så er  $C_K(L) \subseteq ZU_x$ . Omvendt ses at hvis  $hu$  er et vilkårligt element i  $ZU_x$ , så viser ovenstående udregninger at der gælder  ${}^{hu}\omega(a, ax, c) = \omega(a, ax, c)$  for ethvert  $\omega(a, ax, c) \in L$ , og så må  $hu \in C_K(L)$ . Dermed er  $ZU_x \subseteq C_K(L)$ , og så fås  $C_K(L) = ZU_x$ .

Endelig ses at hvis  $3 \mid q-1$  har  $\mathbb{F}_q^\times$  en undergruppe af orden 3, så der findes 3 tredje enhedsrødder i  $\mathbb{F}_q$ . Hvis derimod  $3 \nmid q-1$  har  $\mathbb{F}_q^\times$  ikke nogen undergruppe af orden 3, så den eneste tredje enhedsrod i  $\mathbb{F}_q$  er 1. Dermed har  $Z$  orden  $\gcd(q-1, 3)$ .  $\square$

Som i tilfældet  $\Sigma = A_1$  er  $Z$  faktisk lig centeret for  $K$ .

**Sætning 81.** *Lad  $\Sigma = A_2$  og  $x \in \mathbb{F}_q^\times$ . Da er  $\sum_{L \in \mathcal{S}'_p(U_x)} \frac{-\mu(L)}{\zeta(L, U)} = 0$ .*

*Bevis.*  $\mathcal{S}_p(U_x)$  er en disjunkt forening af  $\mathcal{S}'_p(U_x)$  og  $\mathcal{S}_p(Y)$ , så der gælder

$$\sum_{L \in \mathcal{S}_p(U_x)} -\mu(L) = \sum_{L \in \mathcal{S}'_p(U_x)} -\mu(L) + \sum_{L \in \mathcal{S}_p(Y)} -\mu(L)$$

Per Lemma 66 er  $\sum_{L \in \mathcal{S}_p(U_x)} -\mu(L) = 1$  og  $\sum_{L \in \mathcal{S}_p(Y)} -\mu(L) = 1$ , og så fås  $\sum_{L \in \mathcal{S}'_p(U_x)} -\mu(L) = 0$ . Så gælder:

$$\sum_{L \in \mathcal{S}'_p(U_x)} \frac{-\mu(L)}{\zeta(L, U)} = \sum_{L \in \mathcal{S}'_p(U_x)} \frac{-\mu(L) \cdot |ZU_x|}{|HU|} = \frac{|ZU_x|}{|HU|} \sum_{L \in \mathcal{S}'_p(U_x)} -\mu(L) = 0$$

$\square$

**Lemma 82.** *Lad  $\Sigma = A_2$ . Da er  $Z(U) = Y$ .*

*Bevis.* Lad  $u_0 \in Z(U)$ ; for ethvert  $u \in U$  gælder så  ${}^u u_0 = u_0$ . Skriv  $u = \omega(x, y, z)$  og  $u_0 = \omega(a, b, c)$ ; Lemma 73 giver så at der gælder  $\omega(a, b, c + ay - bx) = \omega(a, b, c)$ . Dette medfører  $ay - bx = 0$ . Men dette skal gælde for vilkårlige  $x, y \in \mathbb{F}_q$ , så ved at sætte  $x = 0$  og  $y = 1$  fås  $a = 0$ , og ved at sætte  $y = 0$  og  $x = -1$  fås tilsvarende  $b = 0$ . Dermed har  $u_0$  formen  $\omega(0, 0, c)$ , og da  $Y$  netop består af de elementer i  $U$  der har denne form, er  $u_0 \in Y$ . Dermed er  $Z(U) \subseteq Y$ . Omvendt gælder at hvis  $u_0 = \omega(0, 0, c)$  er et vilkårligt element i  $Y$ , så viser ovenstående udregninger at  $u_0 \in Z(U)$ . Dermed er  $Y \subseteq Z(U)$ , og så er  $Z(U) = Y$ .  $\square$

**Sætning 83.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}_p(Y)$ . Lad  $g \in K$  og skriv  $g$  på Bruhat-normalform:  $g = unv$ . Der gælder  $g \in N_K(L, U)$  hvis og kun hvis  $n$  afbildes i  $e$ ,  $r_\alpha$  eller  $r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ .*

*Bevis.* Per Lemma 65 gælder  $g \in N_K(Y, U)$  hvis og kun hvis  ${}^v u_0 \in U'_w$  for alle  $u_0 \in L$  hvor  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W$ . Da  $u_0 \in L \subseteq Y$  og  $v \in U$  giver Lemma 82 at der gælder  ${}^v u_0 = u_0$  uanset værdien af  $v$ . Dermed skal der blot gælde  $u_0 \in U'_w$  for alle  $u_0 \in L$ . Da  $L$  er en ikke-triviel undergruppe af  $Y = X_\gamma$  giver Lemma 75 så at  $w$  skal være enten  $e$ ,  $r_\alpha$  eller  $r_\beta$ .  $\square$

**Sætning 84.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}_p(Y)$ . Der gælder  $C_K(L) = RU$  hvor  $R = C_H(Y)$ .*

*Bevis.* Lad  $g \in C_K(L)$  og skriv  $g$  på Bruhat-normalform:  $g = unv$ . For ethvert  $u_0 \in L$  gælder så  $unv u_0 = u_0$ , og så fås  $nv u_0 = u^{-1} u_0$ . Da  $u_0 \in L \subseteq Y$  og  $v, u \in U$  giver Lemma 82 at ligningen kan reduceres til  ${}^n u_0 = u_0$ . Specielt gælder så  ${}^n L = L$ . Lad nu  $w$  være billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W$ ; da gælder  ${}^n X_\gamma = X_{w(\gamma)}$ . Idet  $L \subseteq Y = X_\gamma$  fås så  $L = {}^n L \subseteq {}^n X_\gamma = X_{w(\gamma)}$ , så der skal gælde  $L \subseteq X_{w(\gamma)}$ . Dette gælder kun hvis  $w(\gamma) = \gamma$ , og per Lemma 74 medfører dette at  $w = e$ . Så er  $n \in H$  og  $v \in U_e = C_1$ , og  $g$  har formen  $un$  med  $u \in U$  og  $n \in H$ . Altså er  $g \in HU$ .

Skriv nu  $g = hu$  med  $h \in H$  og  $u \in U$ , og lad  $u_0$  være et element i  $L$  som ikke er identiteten. Skriv  $u_0 = \omega(0, 0, c)$  og  $h = h_\alpha(s)h_\beta(t)$ . Ved brug af Lemma 82 og Lemma 73 fås så  ${}^g u_0 = {}^{hu} u_0 = {}^h u_0 = \omega(0, 0, cts)$ . Dette er lig  $u_0$  hvis og kun hvis  $t = s^{-1}$ , mens  $u$  kan være vilkårlig. Definer  $R = \{h_\alpha(s)h_\beta(s^{-1}) \mid s \in \mathbb{F}_q^\times\}$ ; da haves altså  $g \in RU$ . Dermed er  $C_K(L) \subseteq RU$ . Omvendt viser disse udregninger også at hvis  $g \in RU$  vil  ${}^g u_0 = u_0$  for ethvert element  $u_0$  i  $L$ . Dermed er  $RU \subseteq C_K(L)$ , og så er  $C_K(L) = RU$ .

Tilbage er kun at vise at  $R = C_H(Y)$ . Dette følger af udregningen  ${}^h \omega(0, 0, c) = \omega(0, 0, cts)$ , da denne ligning netop giver at  $h \in H$  centraliserer de ikke-trivielle elementer i  $Y$  hvis og kun hvis  $h \in R$ .  $\square$

**Lemma 85.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}_p(Y)$ . Der gælder  $|N_K(L, U)| = q^3(q-1)^2(2q+1)$  og  $|C_K(L)| = q^3(q-1)$ .*

*Bevis.* Per Sætning 83 er  $N_K(L, U)$  foreningen af mængderne  $UHU_e$ ,  $U(n_1H)U_{r_\alpha}$  og  $U(n_2H)U_{r_\beta}$  hvor  $n_1$  og  $n_2$  afbildes i hhv.  $r_\alpha$  og  $r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ . Idet Bruhat-normalformen er unik, er dette en disjunkt forening, og ydermere gælder  $|UHU_e| = |U| \cdot |H| \cdot |U_e|$ ,  $|U(n_1H)U_{r_\alpha}| = |U| \cdot |n_1H| \cdot |U_{r_\alpha}|$  og  $|U(n_2H)U_{r_\beta}| = |U| \cdot |n_2H| \cdot |U_{r_\beta}|$ . Af Sætning 46(b) fås  $H \cong (\mathbb{F}_q^\times)^2$ , så  $|H| = (q-1)^2$ . Så må også  $|n_1H| = |n_2H| = (q-1)^2$ . Af Lemma 75 fås  $U_{r_\alpha} = X_\alpha$  og  $U_{r_\beta} = X_\beta$ , og da  $X_\alpha$  og  $X_\beta$  begge er isomorfe med  $\mathbb{F}_q^+$  fås så  $|U_{r_\alpha}| = |U_{r_\beta}| = |\mathbb{F}_q^+| = q$ . Samme lemma giver også  $|U_e| = |C_1| = 1$ . Endelig giver Sætning 48(a) at  $U$  er i én-til-én-korrespondance med  $(\mathbb{F}_q)^\times$ , og så må  $|U| = q^3$ . Samlet haves altså  $|N_K(L, U)| = q^3 \cdot (q-1)^2 \cdot 1 + q^3 \cdot (q-1)^2 \cdot q + q^3 \cdot (q-1)^2 \cdot q = q^3(q-1)^2(2q+1)$ .

Per Sætning 84 er  $C_K(L) = RU$ , og per Sætning 48(c) er  $R \cap U = C_1$ . Så er  $|C_K(L)| = |R| \cdot |U|$ , og igen er  $|U| = q^3$ .  $R$  består af elementerne  $h_\alpha(s)h_\beta(s^{-1})$  med  $s \in \mathbb{F}_q^\times$ , og per Sætning 46(b) er disse elementer alle indbyrdes forskellige. Dermed er  $|R| = |\mathbb{F}_q^\times| = q-1$ , og så fås  $|C_K(L)| = q^3(q-1)$ .  $\square$

**Sætning 86.** *Lad  $\Sigma = A_2$ . Da er  $\sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{1}{(q-1)(2q+1)}$ .*

*Bevis.* Per Lemma 66 er  $\sum_{L \in \mathcal{S}_p(Y)} -\mu(L) = 1$ . Så giver Lemma 85 at:

$$\begin{aligned} \sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{\zeta(L, U)} &= \sum_{L \in \mathcal{S}_p(Y)} \frac{|C_K(L)| \cdot (-\mu(L))}{|N_K(L, U)|} = \sum_{L \in \mathcal{S}_p(Y)} \frac{q^3(q-1) \cdot (-\mu(L))}{q^3(q-1)^2(2q+1)} \\ &= \sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{(q-1)(2q+1)} = \frac{1}{(q-1)(2q+1)} \sum_{L \in \mathcal{S}_p(Y)} -\mu(L) \\ &= \frac{1}{(q-1)(2q+1)} \end{aligned}$$

$\square$

**Sætning 87.** *Lad  $\Sigma = A_2$  og lad  $V$  være en af grupperne  $V_y^0$ ,  $y \in \mathbb{F}_q$ , eller  $V_y^\infty$ ,  $y \in \mathbb{F}_q$ . Da er  $\sum_{L \in \mathcal{S}_p(V)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{1}{(q-1)(2q+1)}$ .*

*Bevis.* Betragt først tilfældet  $V = V_0^0$ ; da er  $V = X_\alpha$ . Desuden er  $Y = X_\gamma$ , og per Lemma 74 er  $r_\beta(\gamma) = \alpha$ . Lad nu  $n \in N$  være et element der afbildes i  $r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ . Da er  ${}^nX_\gamma = X_{r_\beta(\gamma)} = X_\alpha$ , og dermed er  ${}^nY = V$ . Så er afbildningen  $L \mapsto {}^nL$  en bijektion fra  $\mathcal{S}_p(Y)$  til  $\mathcal{S}_p(V)$ . Ydermere gælder at  $L$  og  ${}^nL$  er isomorfe objekter i  $\mathcal{F}_p(K)$ , da afbildningen  $x \mapsto {}^nx$  er en afbildning i  $\mathcal{F}_p(K)$  fra  $L$  til  ${}^nL$  med den inverse afbildning  $x \mapsto {}^{n^{-1}}x$ . Dette medfører at der er en én-til-én-korrespondance mellem afbildninger fra  $L$  til  $U$  og afbildninger fra  ${}^nL$  til  $U$ , således at  $\zeta(L, U) = \zeta({}^nL, U)$ . Ved brug af Sætning 86 fås så

$$\sum_{L \in \mathcal{S}_p(V)} \frac{-\mu(L)}{\zeta(L, U)} = \sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{\zeta({}^nL, U)} = \sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{1}{(q-1)(2q+1)}$$

Lad nu  $x \neq 0$  og betragt  $V_x^0$ .  $V_x^0$  består af elementerne  $\omega(a, 0, ax)$  for alle  $a \in \mathbb{F}_q$  og  $V_0^0$  består af elementerne  $\omega(a, 0, 0)$  for alle  $a \in \mathbb{F}_q$ . Definer nu  $u = \omega(0, x, 0)$ ; da giver Lemma 73 at  ${}^u\omega(a, 0, 0) = \omega(a, 0, ax)$ , og dermed er  ${}^uV_0^0 = V_x^0$ . Samme ræsonnement som før giver så

$$\sum_{L \in \mathcal{S}_p(V_x^0)} \frac{-\mu(L)}{\zeta(L, U)} = \sum_{L \in \mathcal{S}_p(V_0^0)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{1}{(q-1)(2q+1)}$$

Tilfældet  $V_x^\infty$  er meget analogt. Først ses at  $V_0^\infty = X_\beta$ , således at når  $n \in N$  afbildes i  $r_\alpha$  gælder  ${}^nY = {}^nX_\gamma = X_{r_\alpha(\gamma)} = X_\beta = V_0^\infty$ . Så fås også  $\sum_{L \in \mathcal{S}_p(V_0^\infty)} \frac{-\mu(L)}{\zeta(L, U)} = \sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{1}{(q-1)(2q+1)}$ . Endelig ses at når  $u = \omega(-x, 0, 0)$  er  ${}^uV_0^\infty = V_x^\infty$ , og så fås  $\sum_{L \in \mathcal{S}_p(V_x^\infty)} \frac{-\mu(L)}{\zeta(L, U)} = \sum_{L \in \mathcal{S}_p(V_0^\infty)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{1}{(q-1)(2q+1)}$ .  $\square$

**Lemma 88.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}'_p(U_0)$ . Da indeholder  $L$  to elementer  $\omega(a, 0, c)$  og  $\omega(a', 0, c')$  som opfylder  $a \neq 0$  og  $ac' \neq a'c$ .*

*Bevis.* Vælg et element i  $u \in L$  på formen  $u = \omega(a, 0, c)$  med  $a \neq 0$ ; dette kan lade sig gøre da  $L \not\subseteq Y$ . Definer så  $x = ca^{-1}$ ; da er  $u \in V_x^0$ . Lad nu  $v = \omega(a', 0, c')$  være et element i  $L$  der ikke ligger i  $V_x^0$ ; et sådant element findes da  $L \not\subseteq V_x^0$ . Hvis der gælder  $ac' = a'c$ , haves  $c' = a'ca^{-1} = a'x$ , og så må  $v \in V_x^0$ . Da dette ikke er tilfældet, gælder  $ac' \neq a'c$ .  $\square$

**Sætning 89.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}'_p(U_0)$ . Lad  $g \in K$  og skriv  $g$  på Bruhat-normalform:  $g = unv$ . Der gælder  $g \in N_K(L, U)$  hvis og kun hvis  $n$  afbildes i  $e$  eller  $r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ .*

*Bevis.* Per Lemma 88 findes der elementer  $u_0 = \omega(a, 0, c)$  og  $u_1 = \omega(a', 0, c')$  som opfylder  $a \neq 0$  og  $ac' \neq a'c$ . Lemma 65 giver nu at hvis  $g \in N_K(L, U)$ , er  ${}^v u_0$  og  ${}^v u_1$  elementer i  $U'_w$  hvor  $w$  er billedet af  $n$  under afbildningen  $N \rightarrow N/H \cong W$ . Skriv  $v = \omega(i, j, k)$ ; da giver Lemma 73 at  ${}^v u_0 = \omega(a, 0, c + aj)$  og  ${}^v u_1 = \omega(a', 0, c' + a'j)$ . Antag nu at  $c + aj$  og  $c' + a'j$  begge er lig 0. Da er  $0 = a'(c + aj) = a'c + aa'j$ , og så er  $a'c = -aa'j$ . Ligeledes er  $0 = a(c' + a'j) = ac' + aa'j$ , og så er også  $ac' = -aa'j$ . Men så er  $a'c = ac'$ , hvilket er i modstrid med valget af  $u_0$  og  $u_1$ . Altså er enten  $c + aj$  eller  $c' + a'j$  forskellig fra 0. Desuden er  $a \neq 0$ , og Lemma 75 giver så at  $w$  må være enten  $e$  eller  $r_\beta$ . Omvendt ses at hvis  $w$  er enten  $e$  eller  $r_\beta$ , så viser ovenstående udregninger at der gælder  ${}^v u_0 \in X_\alpha X_\gamma \subseteq U'_w$  for alle  $u_0 \in L$ , og så er  $g \in N_K(L, U)$ .  $\square$

**Sætning 90.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}'_p(U_0)$ . Da er  $C_K(L) = ZU_0$ .*

*Bevis.* Idet  $L \subseteq U$  er  $C_K(L) \subseteq N_K(L, U)$ . Lad nu  $g \in C_K(L)$  og skriv  $g$  på Bruhat-normalform:  $g = unv$ . Sætning 89 giver så at  $n$  afbildes i  $e$  eller  $r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ . Antag først at  $n$  afbildes i  $r_\beta$ .

Af Sætning 31(h) ses at  $n_\beta(1)$  er et element i  $N$  der afbildes i  $r_\beta$ . Desuden gælder  $\omega(a, 0, c)^{n_\beta(1)} = \omega(k_1c, 0, k_2a)$  hvor  $k_1$  og  $k_2$  er 1 eller  $-1$ . Yderligere giver Sætning 31(k) at  $n_\beta(1)^2 = h_\beta(-1)$ , og så fås

$$\omega(a, 0, c)^{h_\beta(-1)} = \omega(a, 0, c)^{n_\beta(1)^2} = \omega(k_1c, 0, k_2a)^{n_\beta(1)} = \omega(k_1k_2a, 0, k_1k_2c)$$

Men nu gælder  $h_\beta(-1)^{-1} = h_\beta((-1)^{-1}) = h_\beta(-1)$ , og ved brug af Lemma 73 fås så

$$\omega(a, 0, c)^{h_\beta(-1)} = \omega(a, 0, c)^{h_\beta(-1)^{-1}} = h_\beta(-1)\omega(a, 0, c) = \omega(-a, 0, -c)$$

Dermed er  $\omega(k_1k_2a, 0, k_1k_2c) = \omega(-a, 0, -c)$ , så  $k_1k_2 = -1$ . Altså er et af de to tal lig 1 og det andet lig  $-1$ . Hvis  $k_1 = 1$  og  $k_2 = -1$  defineres  $n_0 = n_\beta(1)^{-1}$ , således at der gælder

$$n_0\omega(a, 0, c) = n_\beta(1)^{-1}\omega(a, 0, c) = \omega(a, 0, c)^{n_\beta(1)} = \omega(c, 0, -a)$$

Hvis i stedet  $k_1 = -1$  og  $k_2 = 1$  defineres  $n_0 = n_\beta(1)^{-1}h_\beta(-1)$ , og så fås på tilsvarende vis at der også i dette tilfælde gælder  $n_0\omega(a, 0, c) = \omega(c, 0, -a)$ . I begge tilfælde er  $n_0$  i samme sideklasse af  $H$  som  $n_\beta(1)^{-1}$ , og derfor afbildes  $n_0$  i  $r_\beta^{-1} = r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ .

Lad nu igen  $g = unv$  og skriv  $n$  på formen  $n_0h$  med  $h \in H$ . Skriv  $u = \omega(x, y, z)$  og  $h = h_\alpha(s)h_\beta(t)$ . Per Lemma 75 er  $v \in U_{r_\beta} = X_\beta$ , så  $v$  har formen  $v = \omega(0, m, 0)$ . Per Lemma 88 indeholder  $L$  nu elementer  $\omega(a, 0, c)$  og  $\omega(a', 0, c')$  med  $a \neq 0$  og  $ac' \neq a'c$ . Lemma 73 giver nu:

$$\begin{aligned} g u_0 &= {}^{un_0h} \omega(a, 0, c) = {}^{un_0h} \omega(a, 0, c + am) = {}^{un_0} \omega(at^{-1}s^2, 0, (c + am)ts) \\ &= {}^u \omega((c + am)ts, 0, -at^{-1}s^2) = \omega((c + am)ts, 0, -at^{-1}s^2 + y(c + am)ts) \end{aligned}$$

Da  $g \in C_K(L)$  gælder så  $a = (c + am)ts$ . Denne ligning kan omskrives til  $a = cts + amts$ , og derefter til  $a(1 - mts) = cts$ . Ved at betragte  $g u_1$  fås helt tilsvarende at der gælder  $a'(1 - mts) = c'ts$ . Ved at gange disse ligninger sammen fås  $ac'(1 - mts)ts = a'c(1 - mts)ts$ , og da  $ac' \neq a'c$  må så  $(1 - mts)ts = 0$ . Da  $t, s \in \mathbb{F}_q^\times$  medfører dette at  $1 - mts = 0$ . Dette indsættes nu i ligningen  $a(1 - mts) = cts$ , og så fås  $cts = 0$ . Da igen  $t, s \in \mathbb{F}_q^\times$  fås så  $c = 0$ . Ved på tilsvarende vis at betragte ligningen  $a'(1 - mts) = c'ts$  fås  $c' = 0$ . Men så er  $ac' = 0 = a'c$ , hvilket er i modstrid med den måde  $u_0$  og  $u_1$  blev defineret. Dermed gælder at hvis  $g \in C_K(L)$ , må  $n$  afbildes i  $e$ .

Skriv nu igen  $g = unv$ . Idet  $n$  afbildes i  $e$  er  $n \in H$  og  $v \in U_e = C_1$ , så  $g = un$  med  $u \in U$  og  $n \in H$ . Dermed er  $g \in HU$ .

Lad nu  $g = hu$  med  $h \in H$  og  $u \in U$ , og lad som før  $h = h_\alpha(s)h_\beta(t)$  og  $u = \omega(x, y, z)$ . Lad  $u_0 = \omega(a, 0, c)$  og  $u_1 = \omega(a', 0, c')$  være som før. Så gælder

$$g u_0 = {}^{hu} \omega(a, 0, c) = {}^h \omega(a, 0, c + ay) = \omega(at^{-1}s^2, 0, (c + ay)ts)$$

Da  $g \in C_K(L)$  er nu  $c = (c + ay)ts$ . Denne ligning kan omskrives til  $c = cts + ayts$  og derefter til  $c(1 - ts) = ayts$ . Ved at betragte  $u_1$  fås tilsvarende  $c'(1 - ts) = a'yts$ . Ved at gange disse to ligninger sammen fås så  $ac'yts(1 - ts) = a'cyts(1 - ts)$ . Da  $ac' \neq a'c$  medfører dette at  $yts(1 - ts) = 0$ . Så er enten  $yts = 0$  eller  $1 - ts = 0$ . Hvis  $1 - ts = 0$  er  $ayts = c(1 - ts) = 0$ , og da  $a \neq 0$  fås så alligevel  $yts = 0$ . Altså er  $yts = 0$ , og da  $s, t \in \mathbb{F}_q^\times$  fås så  $y = 0$ . Dermed er  $u \in U_0$ .

Ved at indsætte  $y = 0$  fås nu  $g u_0 = \omega(at^{-1}s^2, 0, cts)$ , og det skal så gælde at  $a = at^{-1}s^2$  og  $c = cts$ . Da  $a \neq 0$  giver den første ligning at  $1 = t^{-1}s^2$  og så er  $t = s^2$ . Nu gælder  $c = cts$  og  $c' = c'ts$ ,

og da  $ac' \neq a'c$  er enten  $c$  eller  $c'$  forskellig fra 0. Så fås  $1 = ts$ , og dermed er  $s^3 = s^2s = ts = 1$ . Da således  $s^3 = 1$  og  $t = s^2$ , er  $h \in Z$ . Altså er  $g = hu \in ZU_0$ , og der gælder  $C_K(L) \subseteq ZU_0$ .

Endelig ses at hvis  $g \in ZU_0$  viser ovenstående udregninger at der gælder  ${}^g u_0 = u_0$  for alle  $u_0 \in L$ . Dermed er  $ZU_0 \subseteq C_K(L)$ , og så er  $C_K(L) = ZU_0$ .  $\square$

**Lemma 91.** *Lad  $\Sigma = A_2$  og lad  $L \in \mathcal{S}'_p(U_0)$ . Der gælder  $|N_K(L, U)| = q^3(q-1)^2(q+1)$  og  $|C_K(L)| = \gcd(q-1, 3)q^2$ .*

*Bevis.* Per Sætning 89 er  $N_K(L, U)$  foreningen af mængderne  $UHU_e$  og  $U(n_s H)U_{r_\beta}$  hvor  $n$  afbildes i  $r_\beta$  under afbildningen  $N \rightarrow N/H \cong W$ . Idet Bruhat-normalformen er unik, er dette en disjunkt forening, og ydermere gælder  $|UHU_e| = |U| \cdot |H| \cdot |U_e|$  og  $|U(n_s H)U_{r_\beta}| = |U| \cdot |n_s H| \cdot |U_{r_\beta}|$ . Som tidligere fås  $|H| = |\mathbb{F}_q^\times|^2 = (q-1)^2$ , og så må også  $|n_s H| = (q-1)^2$ . Af Lemma 75 fås  $|U_{r_\beta}| = |X_\beta| = q$  og  $|U_e| = |C_1| = 1$ , og endelig er  $|U| = |\mathbb{F}_q|^3 = q^3$ . Samlet haves altså  $|N_K(L, U)| = q^3 \cdot (q-1)^2 \cdot 1 + q^3 \cdot (q-1)^2 \cdot q = q^3(q-1)^2(q+1)$ .

Per Sætning 90 er  $C_K(L) = ZU_0$ , og per Sætning 48(c) er  $Z \cap U_0 = C_1$ . Så er  $|C_K(L)| = |Z| \cdot |U_0|$ , og det er tidligere set at  $|Z| = \gcd(q-1, 3)$ . Desuden gælder  $U_0 = X_\alpha X_\gamma$ , og så er  $|U_0| = |X_\alpha| \cdot |X_\gamma| = q^2$ . Så fås  $|C_K(L)| = \gcd(q-1, 3)q^2$ .  $\square$

**Sætning 92.** *Lad  $\Sigma = A_2$ . Da er  $\sum_{L \in \mathcal{S}'_p(U_0)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{-\gcd(q-1, 3)}{(q-1)^2(q+1)}$ .*

*Bevis.*  $\mathcal{S}_p(U_0)$  er en disjunkt forening af mængderne  $\mathcal{S}'_p(U_0)$ ,  $\mathcal{S}_p(Y)$  og  $\mathcal{S}_p(V_x^0)$  for  $x \in \mathbb{F}_q$ , så der gælder

$$\sum_{L \in \mathcal{S}_p(U_0)} -\mu(L) = \sum_{L \in \mathcal{S}'_p(U_0)} -\mu(L) + \sum_{L \in \mathcal{S}_p(Y)} -\mu(L) + \sum_{x \in \mathbb{F}_q} \sum_{L \in \mathcal{S}_p(V_x^0)} -\mu(L)$$

Per Lemma 66 er  $\sum_{L \in \mathcal{S}_p(U_0)} -\mu(L) = 1$ ,  $\sum_{L \in \mathcal{S}_p(Y)} -\mu(L) = 1$  og  $\sum_{L \in \mathcal{S}_p(V_x^0)} -\mu(L) = 1$ , og så fås

$$1 = \sum_{L \in \mathcal{S}'_p(U_0)} -\mu(L) + 1 + \sum_{x \in \mathbb{F}_q} 1$$

Dermed er  $\sum_{L \in \mathcal{S}'_p(U_0)} -\mu(L) = -\sum_{x \in \mathbb{F}_q} 1 = -q$ . Så giver Lemma 91:

$$\begin{aligned} \sum_{L \in \mathcal{S}'_p(U_0)} \frac{-\mu(L)}{\zeta(L, U)} &= \sum_{L \in \mathcal{S}'_p(U_0)} \frac{|C_K(L)| \cdot (-\mu(L))}{|N_K(L, U)|} = \sum_{L \in \mathcal{S}'_p(U_0)} \frac{\gcd(q-1, 3)q^2 \cdot (-\mu(L))}{q^3(q-1)^2(q+1)} \\ &= \sum_{L \in \mathcal{S}'_p(U_0)} \frac{\gcd(q-1, 3) \cdot (-\mu(L))}{q(q-1)^2(q+1)} = \frac{\gcd(q-1, 3)}{q(q-1)^2(q+1)} \sum_{L \in \mathcal{S}'_p(U_0)} -\mu(L) \\ &= \frac{\gcd(q-1, 3)}{q(q-1)^2(q+1)} \cdot (-q) = \frac{-\gcd(q-1, 3)}{(q-1)^2(q+1)} \end{aligned}$$

$\square$

**Sætning 93.** *Lad  $\Sigma = A_2$ . Da er  $\sum_{L \in \mathcal{S}'_p(U_\infty)} \frac{-\mu(L)}{\zeta(L, U)} = \frac{-\gcd(q-1, 3)}{(q-1)^2(q+1)}$ .*

*Bevis.* Beviset for dette er helt analogt til beregningen af summen over  $\mathcal{S}'_p(U_0)$ . Den eneste forskel er at rollerne af  $\alpha$  og  $\beta$  er byttet om.  $\square$

**Sætning 94.** *Lad  $\Sigma = A_2$ . Da er  $\chi(\mathcal{F}_p(K)) = \frac{1}{q-1} - \frac{2 \gcd(q-1, 3)}{(q-1)^2(q+1)}$ .*

*Bevis.* Per Sætning 48(e), Korollar 57 og Sætning 76 gælder

$$\begin{aligned}
\chi(\mathcal{F}_p(K)) &= \sum_{L \in \mathcal{S}'_p(U)} \frac{-\mu(L)}{\zeta(L, U)} + \sum_{x \in \mathbb{F}_q^\times} \sum_{L \in \mathcal{S}'_p(U_x)} \frac{-\mu(L)}{\zeta(L, U)} \\
&+ \sum_{L \in \mathcal{S}_p(U_0)} \frac{-\mu(L)}{\zeta(L, U)} + \sum_{L \in \mathcal{S}_p(U_\infty)} \frac{-\mu(L)}{\zeta(L, U)} + \sum_{L \in \mathcal{S}_p(Y)} \frac{-\mu(L)}{\zeta(L, U)} \\
&+ \sum_{y \in \mathbb{F}_q} \sum_{L \in \mathcal{S}'_p(V_y^0)} \frac{-\mu(L)}{\zeta(L, U)} + \sum_{y \in \mathbb{F}_q} \sum_{L \in \mathcal{S}'_p(V_y^\infty)} \frac{-\mu(L)}{\zeta(L, U)}
\end{aligned}$$

Nu indsættes værdierne fra Korollar 78 og Sætning 81, 86, 87, 92 og 93:

$$\begin{aligned}
\chi(\mathcal{F}_p(K)) &= 0 + \sum_{x \in \mathbb{F}_q^\times} 0 + \frac{-\gcd(q-1, 3)}{(q-1)^2(q+1)} + \frac{-\gcd(q-1, 3)}{(q-1)^2(q+1)} + \frac{1}{(q-1)(2q+1)} \\
&+ \sum_{y \in \mathbb{F}_q} \frac{1}{(q-1)(2q+1)} + \sum_{y \in \mathbb{F}_q} \frac{1}{(q-1)(2q+1)} \\
&= \frac{-2 \gcd(q-1, 3)}{(q-1)^2(q+1)} + \frac{1}{(q-1)(2q+1)} + q \cdot \frac{1}{(q-1)(2q+1)} \\
&+ q \cdot \frac{1}{(q-1)(2q+1)} \\
&= \frac{-2 \gcd(q-1, 3)}{(q-1)^2(q+1)} + \frac{2q+1}{(q-1)(2q+1)} \\
&= \frac{1}{q-1} - \frac{2 \gcd(q-1, 3)}{(q-1)^2(q+1)}
\end{aligned}$$

□



## Det krydskararakteristiske tilfælde

I dette afsnit undersøges værdien af  $\chi(\mathcal{F}_r(\Sigma(q)))$ , hvor  $r$  er et primtal der ikke går op i  $q$ . Det letteste tilfælde er det hvor  $r \mid q - 1$  og  $r \nmid |W|$ , da det så viser sig at  $H$  indeholder en Sylow- $r$ -undergruppe af  $\Sigma(q)$ . Værdien af  $\chi(\mathcal{F}_r(\Sigma(q)))$  beregnes i det tilfælde hvor  $r \mid q - 1$ ,  $r \nmid |W|$  og  $\Sigma$  er enten  $A_n$ ,  $B_n$ ,  $C_n$  eller  $D_n$ . Det bevises først at hvis  $x \mapsto {}^g x$  er en konjugationsafbildning mellem undergrupper af  $H$ , så findes der et  $n \in N$  der repræsenterer samme afbildning. Dette gør det muligt at anvende Sætning 59. Herefter anvendes isomorfien  $N/H \cong W$  til at konstruere en gruppevirkning af  $W$  på  $H$ , og det vises at  $\chi(\mathcal{F}_r(\Sigma(q)))$  kan udtrykkes ud fra antallet af elementer i  $W$  der har et fikspunkt i  $H$  forskelligt fra identitets-elementet. Endelig beregnes isomorfiklassen af  $W$ , og det beskrives præcis hvilke elementer der har andre fikspunkter end identiteten.

I hele dette afsnit er  $K$  den universelle Chevalley-gruppe  $\Sigma(q)$  og  $\bar{K}$  den universelle semisimple algebraiske gruppe med rodsystem  $\Sigma$ .  $\bar{T}$  er en maksimal torus af  $\bar{K}$  med normalisator  $\bar{N}$ , og  $\bar{X}_\alpha$ ,  $\alpha \in \Sigma$  er  $\bar{T}$ -rodgrupperne i  $\bar{K}$ .  $\Sigma^+$  er et positivt delsystem af  $\Sigma$ ,  $\bar{U}$  er gruppen  $\langle \bar{X}_\alpha \mid \alpha \in \Sigma^+ \rangle$  og  $\bar{U}^-$  er gruppen  $\langle \bar{X}_\alpha \mid \alpha \in -\Sigma^+ \rangle$ . Endelig er  $H = \bar{T} \cap K$ ,  $N = \bar{N} \cap K$ ,  $U = \bar{U} \cap K$  og  $U^- = \bar{U}^- \cap K$ , og  $W$  er Weyl-gruppen for  $\Sigma$ . For ethvert  $w \in W$  defineres  $U_w = U \cap (U^-)^n$  hvor  $n$  er et element der afbildes i  $w$  under afbildningen  $N \rightarrow N/H \cong W$ .

Først haves en observation omkring versionerne af  $K$ .

**Sætning 95.** *Antag  $r \mid q - 1$  og  $r \nmid |W|$ . Da er  $r \nmid |Z(K)|$ .*

*Bevis.*  $W$  er frembragt af elementerne  $r_\alpha$  med  $\alpha \in \Sigma$ ; disse elementer har alle orden 2, da de er reflektioner. Da  $W$  indeholder elementer af orden 2, må  $2 \mid |W|$ , og da  $r \nmid |W|$  fås så  $r \neq 2$ . Per Sætning 29 og Sætning 45 gælder nu at hvis  $\Sigma \neq A_n$  har  $Z(K)$  orden 1, 2 eller 4. Da  $r \neq 2$  fås så  $r \nmid |Z(K)|$ . Hvis  $\Sigma = A_n$  fås i stedet at ordenen af  $Z(K)$  er en faktor i  $n + 1$ . I Sætning 115 vil det blive bevist at hvis  $\Sigma = A_n$ , er  $W \cong S_{n+1}$ , så der gælder  $|W| = (n + 1)!$ . Betingelsen  $r \nmid |W|$  medfører så  $r > n + 1$ , og så fås  $r \nmid |Z(K)|$ .  $\square$

Per Sætning 62 er  $\chi(\mathcal{F}_p(K))$  så uafhængig af versionen af  $K$ , og det er derfor ikke nogen indskrænkning at fokusere på den universelle version.

Lad nu  $r$  være et primtal der går op i  $q - 1$ . Idet  $H$  er abelsk har den en unik Sylow- $r$ -undergruppe  $H_r$ . Denne gruppes struktur er let at beskrive:

**Lemma 96.**  $H_r \cong (C_{r^k})^{\dim(\Sigma)}$  hvor  $r^k$  er den største potens af  $r$  der går op i  $q - 1$ .

*Bevis.* Per Sætning 46(b) er  $H$  det direkte produkt af  $\dim(\Sigma)$  grupper isomorfe med  $\mathbb{F}_q^\times$ .  $\mathbb{F}_q^\times$  er cyklisk af orden  $q - 1$ , så dens Sylow- $r$ -undergruppe er dermed netop cyklisk af orden  $r^k$ . Så er  $H_r$  isomorf med det direkte produkt af  $\dim(\Sigma)$  kopier af  $C_{r^k}$ .  $\square$

Det viser sig at hvis  $r$  ikke går op i ordenen af  $W$ , er  $H_r$  faktisk en Sylow- $r$ -undergruppe af  $K$ .

**Sætning 97.** *Antag  $r \mid q - 1$  og  $r \nmid |W|$ . Da er  $H_r$  en Sylow- $r$ -undergruppe af  $K$ .*

*Bevis.* Per [GLS] Theorem 2.2.9 findes der et polynomium  $f(x)$  bestemt alene af rodsystemet  $\Sigma$  som opfylder at ordenen af  $K$  er lig  $f(q)$ , og  $f(x)$  har formen  $x^N \prod_{i=1}^n (x^{d_i} - 1)$  hvor  $N$  og  $d_1, \dots, d_n$  er passende positive heltal og  $n = \dim(\Sigma)$ . Så gælder

$$f(x) = x^N \prod_{i=1}^n (x^{d_i} - 1) = x^N \prod_{i=1}^n \left( (x - 1) \sum_{j=0}^{d_i-1} x^j \right) = x^N (x - 1)^n \prod_{i=1}^n \left( \sum_{j=0}^{d_i-1} x^j \right).$$

For ethvert  $d \in \mathbb{N}$  ses nu at polynomiet  $f_d(x) = \sum_{j=0}^{d-1} x^j$  opfylder  $f_d(1) = d$ , således at 1 ikke er en rod af  $f_d$ . Dermed går  $x - 1$  ikke op i  $f_d(x)$ , hvoraf fås at  $(x - 1)$  går op i  $f(x)$  præcis  $n = \dim(\Sigma)$  gange.

Lad nu  $R$  være en Sylow- $r$ -undergruppe af  $K$ . Per [GLS] Theorem 4.10.2(a) har  $R$  en normal abelsk undergruppe  $R_T$  som opfylder at  $R/R_T$  er isomorf med en undergruppe af  $W$ . Da  $R/R_T$  er en  $r$ -gruppe og  $r \nmid |W|$ , må  $R/R_T = C_1$ , således at  $R = R_T$ . Idet  $r \mid q - 1$  giver [GLS] Theorem 4.10.2(c) desuden at  $R_T$  er homocyklisk med eksponent  $r^k$  og rang  $n$  hvor  $r^k$  er den største potens af  $r$  der går op i  $q - 1$  og  $n$  er antallet af gange  $x - 1$  går op i polynomiet  $f(x)$ . Det er netop vist at  $n = \dim(\Sigma)$ , og dermed fås  $R = R_T \cong (C_{r^k})^{\dim(\Sigma)} \cong H_r$ . Altså er  $H_r$  isomorf med en Sylow- $r$ -undergruppe af  $K$ , og den er dermed selv en Sylow- $r$ -undergruppe af  $K$ .  $\square$

**Definition 21.** Lad  $r$  være et primtal der går op i  $q - 1$ . Den unikke Sylow- $r$ -undergruppe af  $\mathbb{F}_q^\times$  betegnes med  $\mathbb{F}_q^{(r)}$ .

Bemærk at dette ikke er den samme notation som i Sætning 29. I Sætning 29 betegner  $\overline{\mathbb{F}}^{(r)}$  mængden af elementer i  $\overline{\mathbb{F}}$  der opfylder  $x^r = 1$ ; her betegner  $\mathbb{F}_q^{(r)}$  mængden af elementer i  $\mathbb{F}_q$  der opfylder  $x^{(r^a)} = 1$  for mindst et  $a \in \mathbb{N}$ .

**Lemma 98.** Lad  $h = \prod_{\alpha \in \Sigma} h_\alpha(t_\alpha)$  være et element i  $H$ . Hvis  $t_\alpha \in \mathbb{F}_q^{(r)}$  for alle  $\alpha \in \Sigma$ , er  $h \in H_r$ . Omvendt gælder at hvis  $h \in H_r$ , kan  $h$  skrives på formen  $h = \prod_{\alpha \in \Pi} h_\alpha(t_\alpha)$  hvor  $t_\alpha \in \mathbb{F}_q^{(r)}$  for alle  $\alpha \in \Pi$  og  $\Pi$  er et fundamentalt system for  $\Sigma$ .

*Bevis.* Lad  $r^k$  være ordenen af  $\mathbb{F}_q^{(r)}$ . Da gælder  $h^{r^k} = \prod_{\alpha \in \Sigma} h_\alpha(t_\alpha)^{r^k} = \prod_{\alpha \in \Sigma} h_\alpha(t_\alpha^{r^k})$ . Hvis  $t_\alpha \in \mathbb{F}_q^{(r)}$  fås så  $t_\alpha^{r^k} = 1$ , så når dette gælder for hvert  $\alpha \in \Sigma$  fås  $h = \prod_{\alpha \in \Sigma} h_\alpha(1) = 1$ . Dermed er ordenen af  $h$  en divisor i  $r^k$ , og så er  $h \in H_r$ .

Antag nu  $h \in H_r$  og skriv  $h = \prod_{\alpha \in \Pi} h_\alpha(t_\alpha)$ ; dette kan lade sig gøre per Sætning 31(e). Idet  $h \in H_r$  er  $h^{r^k} = 1$ , således at der gælder  $\prod_{\alpha \in \Pi} h_\alpha(t_\alpha^{r^k}) = 1$ . Så giver Sætning 46(b) at der gælder  $t_\alpha^{r^k} = 1$  for hvert  $\alpha \in \Pi$ . Men dette betyder netop at  $t_\alpha \in \mathbb{F}_q^{(r)}$  for hvert  $\alpha \in \Pi$ .  $\square$

Næste skridt er at undersøge konjugationsafbildningerne fra  $K$  mellem undergrupperne af  $H_r$ .

**Lemma 99.** Lad  $\Sigma_0$  være en lukket delmængde af  $\Sigma^+$  og lad  $U_0 = \langle X_\alpha \mid \alpha \in \Sigma_0 \rangle$ . Lad  $u \in U_0$  og  $h \in H$ . Da findes der  $u' \in U_0$  så  ${}^u h = hu'$ .

*Bevis.* Der gælder  ${}^u h = uhu^{-1} = h(u^h)u^{-1}$ . Da  $H$  normaliserer  $U_0$  er  $(u^h)u^{-1} \in U_0$ .  $\square$

**Lemma 100.** Lad  $h_0, h_1 \in H$  og  $g \in K$  være elementer således at  ${}^g h_0 = h_1$ , og lad  $n \in N$  være den midterste faktor i Bruhat-normalformen for  $g$ . Da gælder  ${}^n h_0 = h_1$ .

*Bevis.* Skriv  $g$  på Bruhat-normalform:  $g = unv$  med  $u \in U$ ,  $n \in N$ ,  $v \in U_w$ . Da gælder  ${}^{unv} h_0 = h_1$  og dermed  ${}^{nv} h_0 = u^{-1} h_1$ . Per Lemma 99 findes nu  $u' \in U$  og  $v' \in U_n$  så  $v h_0 = h_0 v'$  og  $u^{-1} h_1 = h_1 u'$ . Dermed haves  ${}^n(h_0 v') = h_1 u'$ , hvoraf fås  ${}^n h_0 \cdot {}^n v' = h_1 u'$ . Nu er  $v' \in U_w \subseteq (U^-)^n$ , og dermed fås  ${}^n v' \in {}^n U_w \subseteq U^-$ . Altså er  ${}^n h_0 \cdot {}^n v'$  indeholdt i  $HU^-$  mens  $h_1 u'$  er indeholdt i  $HU$ . Da disse elementer er ens, er de så indeholdt i  $HU^- \cap HU$ , og per Sætning 48(d) og (b) er  $HU^- \cap HU = H(U^- \cap U) = H$ . Dermed er  $h_1 u' \in H$ , og da også  $h_1 \in H$ , er  $u' \in H$ . Men der gælder også  $u' \in U$ , og per Sætning 48(c) er  $H \cap U = C_1$ , hvoraf følger  $u' = 1$ . Tilsvarende er  ${}^n h_0 \cdot {}^n v' \in H$  og  ${}^n h_0 \in H$ , og dermed er  ${}^n v' \in H$ . Da samtidig  ${}^n v' \in U^-$  og  $H \cap U^- = C_1$  må så  ${}^n v' = 1$ . Dermed reduceres ligningen  ${}^n h_0 \cdot {}^n v' = h_1 u'$  til  ${}^n h_0 = h_1$ , som ønsket.  $\square$

**Sætning 101.** *Antag  $r \mid q - 1$  og  $r \nmid |W|$ . Da er  $\mathcal{F}_r(K) \simeq \mathcal{F}_r(N)$ .*

*Bevis.* Per Sætning 50 er  $\mathcal{F}_r(K) \simeq \mathcal{F}_{H_r}(K)$  og  $\mathcal{F}_r(N) \simeq \mathcal{F}_{H_r}(N)$ , så det er tilstrækkeligt at vise  $\mathcal{F}_{H_r}(K) = \mathcal{F}_{H_r}(N)$ . Objekterne i de to kategorier er de samme, da de netop er de ikke-trivielle undergrupper af  $H_r$ . Lad nu  $L_1$  og  $L_2$  være ikke-trivielle undergrupper af  $H_r$ . Enhver afbildning i  $\mathcal{F}_{H_r}(N)(L_1, L_2)$  har formen  $(x \mapsto {}^n x)$  for et vist  $n \in N$ , og denne afbildning er også et element i  $\mathcal{F}_{H_r}(K)(L_1, L_2)$ , idet  $n \in N \subset K$ . Lad nu omvendt  $(x \mapsto {}^g x)$  være en afbildning i  $\mathcal{F}_{H_r}(K)(L_1, L_2)$ , og skriv  $g$  på Bruhat-normalform:  $g = unv$  med  $n \in N$ . For ethvert  $x \in L_1$  er nu  ${}^g x \in L_2 \subseteq H$ , og Lemma 100 giver så  ${}^n x = {}^g x$  for alle  $x \in L_1$ . Dermed er  $(x \mapsto {}^g x) = (x \mapsto {}^n x)$ , og så er  $(x \mapsto {}^g x)$  også et element i  $\mathcal{F}_{H_r}(N)(L_1, L_2)$ . Altså er  $\mathcal{F}_{H_r}(K)(L_1, L_2) = \mathcal{F}_{H_r}(N)(L_1, L_2)$ , og dermed er  $\mathcal{F}_{H_r}(K) = \mathcal{F}_{H_r}(N)$ .  $\square$

**Lemma 102.** *Lad  $W$  virke på  $H$  ved  ${}^w h = {}^n h$  hvor  $n$  er et element i  $N$  der afbildes i  $W$  under afbildningen  $N \rightarrow N/H \cong W$ . Dette er en veldefineret gruppevirkning.*

*Bevis.* Lad  $n$  og  $n'$  være elementer i  $N$  der begge afbildes i  $w$  af afbildningen  $N \rightarrow N/H \cong W$ . Da repræsenterer  $n$  og  $n'$  samme sideklasse af  $H$ , så der findes  $h_0 \in H$  så  $n' = nh_0$ . Idet  $H$  er abelsk, fås så  ${}^{n'} h = {}^{nh_0} h = {}^n h$  for ethvert  $h \in H$ . Dermed er  ${}^w h$  entydigt defineret.  $\square$

**Lemma 103.** *Der gælder  ${}^w h_\alpha(t) = h_{w(\alpha)}(t)$  for ethvert  $\alpha \in \Sigma$ ,  $w \in W$  og  $t \in \mathbb{F}_q^\times$ .*

*Bevis.* Lad  $n \in N$  være et element der afbildes i  $w$  under afbildningen  $N \rightarrow N/H \cong W$ . Per Sætning 46(c) og Sætning 24(c) gælder så  ${}^n X_\alpha = X_{w(\alpha)}$  for alle  $\alpha \in \Sigma$ . Sætning 31(h) giver nu  ${}^{n_\beta(1)^{-1}} x_\alpha(t) = x_\alpha(t)^{n_\beta(1)} = x_{r_\beta(\alpha)}(c_{\alpha, \beta} t)$ , hvoraf fås  ${}^{n_\beta(1)^{-1}} X_\alpha = X_{r_\beta(\alpha)}$  for ethvert  $\alpha \in \Sigma$ . Dermed er  $r_\beta$  billedet af  $n_\beta(1)^{-1}$  under afbildningen  $N \rightarrow N/H \cong W$ . Så giver Sætning 31(i) at

$$r_\beta h_\alpha(t) = {}^{n_\beta(1)^{-1}} h_\alpha(t) = h_\alpha(t)^{n_\beta(1)} = h_{r_\beta(\alpha)}(t)$$

for ethvert  $\alpha \in \Sigma$  og  $t \in \mathbb{F}_q^\times$ . Da dette gælder for ethvert  $\beta \in \Sigma$  og elementerne  $r_\beta$  frembringer  $W$ , fås  ${}^w h_\alpha(t) = h_{w(\alpha)}(t)$  for ethvert  $w \in W$ .  $\square$

**Sætning 104.** *Antag  $r \mid q - 1$  og  $r \nmid |W|$ . Da er  $\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|}$  hvor  $\mathcal{M} = \{w \in W \mid C_{H_r}(w) \neq C_1\}$ .*

*Bevis.* Da  $H_r$  er den unikke Sylow- $r$ -undergruppe af  $H$  og  $H$  er normal i  $N$ , er  $H_r$  normal i  $N$ . Så giver Sætning 59 at  $\chi(\mathcal{F}_r(N)) = \frac{|\mathcal{M}_0|}{|N|}$  hvor  $\mathcal{M}_0 = \{n \in N \mid C_{H_r}(n) \neq C_1\}$ . Lad nu  $\mathcal{M} = \{w \in W \mid C_{H_r}(w) \neq C_1\}$ , lad  $w$  være et element i  $W$ , og lad  $n \in N$  være et element der afbildes i  $w$  under afbildningen  $N \rightarrow N/H \cong W$ . Da er  $C_{H_r}(w) = \{h \in H_r \mid {}^w h = h\} = \{h \in H_r \mid {}^n h = h\} = C_{H_r}(n)$ , og dermed er  $w \in \mathcal{M}$  hvis og kun hvis  $n \in \mathcal{M}_0$ . Dermed er  $\mathcal{M}_0$  netop Urbilledet af  $\mathcal{M}$  under afbildningen  $N \rightarrow N/H \cong W$ , og så må  $|\mathcal{M}_0| = |H| \cdot |\mathcal{M}|$ . Idet  $W \cong N/H$  fås yderligere  $|N| = |H| \cdot |N/H| = |H| \cdot |W|$ , og dermed er  $\chi(\mathcal{F}_r(N)) = \frac{|\mathcal{M}_0|}{|N|} = \frac{|H| \cdot |\mathcal{M}|}{|H| \cdot |W|} = \frac{|\mathcal{M}|}{|W|}$ . Endelig giver Sætning 101 og Sætning 51 at  $\chi(\mathcal{F}_r(K)) = \chi(\mathcal{F}_r(N))$ , og dermed er  $\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|}$ .  $\square$

Det er nu interessant at undersøge for hvilke  $w \in W$  der gælder  $C_{H_r}(w) \neq C_1$ . Det viser sig at være lettest først at beskrive en isomorfi mellem  $H_r$  og en undergruppe af  $(\mathbb{F}_q^\times)^l$  for passende  $l$ , da  $W$  kan bringes til at virke på  $(\mathbb{F}_q^\times)^l$  på en måde der er lettere at beskrive.

**Definition 22.** Lad  $\Sigma \subset \mathbb{E}^n$  og lad  $\gamma$  være en vektor i  $\mathbb{E}^n$ .  $\gamma$  siges at være *kompatibel* med  $\Sigma$  hvis der gælder  $(\gamma, \alpha) \in \mathbb{Z}$  for alle  $\alpha \in \Sigma$ .

**Sætning 105.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$  og definer  $\sigma_\gamma : H \rightarrow \mathbb{F}_q^\times$  ved  $\sigma_\gamma(h_\alpha(t)) = t^{(\gamma, \check{\alpha})}$ . Da er  $\sigma_\gamma$  en veldefineret homomorfi.

*Bevis.* Idet  $(\gamma, \check{\alpha}) \in \mathbb{Z}$  er udtrykket  $t^{(\gamma, \check{\alpha})}$  veldefineret.  $H$  er frembragt af elementerne  $h_\alpha(t)$  med relationerne i Sætning 31(c), (d) og (e), og per Sætning 31(f) gælder der ikke yderligere relationer i  $H$ . Det skal altså blot vises at  $\sigma_\gamma$  respekterer disse tre relationer. For 31(c) gives

$$\sigma_\gamma(h_\alpha(t)h_\beta(u)) = t^{(\gamma, \check{\alpha})}u^{(\gamma, \check{\beta})} = u^{(\gamma, \check{\beta})}t^{(\gamma, \check{\alpha})} = \sigma_\gamma(h_\beta(u)h_\alpha(t)).$$

For 31(d) gives

$$\sigma_\gamma(h_\alpha(t)h_\alpha(u)) = t^{(\gamma, \check{\alpha})}u^{(\gamma, \check{\alpha})} = (tu)^{(\gamma, \check{\alpha})} = \sigma_\gamma(h_\alpha(tu)).$$

For 31(e) gives

$$\begin{aligned} \sigma_\gamma(h_\alpha(t)) &= t^{(\gamma, \check{\alpha})} = t^{(\gamma, \sum_{i=1}^n c_i \check{\alpha}_i)} = t^{\sum_{i=1}^n c_i (\gamma, \check{\alpha}_i)} \\ &= \prod_{i=1}^n (t^{c_i})^{(\gamma, \check{\alpha}_i)} = \prod_{i=1}^n \sigma_\gamma(h_{\alpha_i}(t^{c_i})) = \sigma_\gamma\left(\prod_{i=1}^n h_{\alpha_i}(t^{c_i})\right) \end{aligned}$$

□

**Lemma 106.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$ . Da er  $-\gamma$  kompatibel med  $\Sigma$ , og der gælder  $\sigma_{-\gamma}(h) = \sigma_\gamma(h)^{-1}$  for ethvert  $h \in H$ .

*Bevis.* Da  $\gamma$  er kompatibel med  $\Sigma$  fås  $(-\gamma, \check{\alpha}) = -(\gamma, \check{\alpha}) \in \mathbb{Z}$  for hvert  $\alpha \in \Sigma$ . Dermed er  $-\gamma$  kompatibel med  $\Sigma$ . Skriv nu  $h$  på formen  $\prod_{\alpha \in \Sigma} h_\alpha(t_\alpha)$ ; da gælder

$$\begin{aligned} \sigma_{-\gamma}(h) &= \sigma_{-\gamma}\left(\prod_{\alpha \in \Sigma} h_\alpha(t_\alpha)\right) = \prod_{\alpha \in \Sigma} t_\alpha^{(-\gamma, \check{\alpha})} = \prod_{\alpha \in \Sigma} t_\alpha^{-(\gamma, \check{\alpha})} \\ &= \prod_{\alpha \in \Sigma} \left(t_\alpha^{(\gamma, \check{\alpha})}\right)^{-1} = \sigma_\gamma\left(\prod_{\alpha \in \Sigma} h_\alpha(t_\alpha)\right)^{-1} = \sigma_\gamma(h)^{-1} \end{aligned}$$

□

**Lemma 107.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$  og lad  $h \in H_r$ . Da er  $\sigma_\gamma(h) \in \mathbb{F}_q^{(r)}$ .

*Bevis.* Per Lemma 98 er det muligt at skrive  $h = \prod_{\alpha \in \Pi} h_\alpha(t_\alpha)$  hvor  $t_\alpha \in \mathbb{F}_q^{(r)}$  for hvert  $\alpha \in \Pi$  og  $\Pi$  er et fundamentalt system for  $\Sigma$ . Per definitionen af  $\sigma_\gamma$  gælder så  $\sigma_\gamma(h) = \prod_{\alpha \in \Pi} t_\alpha^{(\gamma, \check{\alpha})}$ , og da  $(\gamma, \check{\alpha}) \in \mathbb{Z}$  for hvert  $\alpha$ , er så  $\sigma_\gamma(h) \in \mathbb{F}_q^{(r)}$ . □

**Sætning 108.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$  og lad  $w \in W$ . Da er  $w^{-1}(\gamma)$  kompatibel med  $\Sigma$ , og der gælder  $\sigma_\gamma(w h) = \sigma_{w^{-1}(\gamma)}(h)$  for ethvert  $h \in H$ .

*Bevis.* Idet  $w$  er en isometri af  $\mathbb{E}^n$  gælder  $(\alpha, w(\beta)) = (w^{-1}(\alpha), \beta)$  for alle  $\alpha, \beta \in \mathbb{E}^n$ . Specielt gælder så  $(w^{-1}(\gamma), \check{\alpha}) = (\gamma, w(\check{\alpha}))$  for ethvert  $\alpha \in \Sigma$ . Nu er  $w(\check{\alpha})$  den duale rod til  $w(\alpha)$ , og da  $w(\alpha) \in \Sigma$  og  $\gamma$  er kompatibel med  $\Sigma$ , fås så  $(\gamma, w(\check{\alpha})) \in \mathbb{Z}$ . Dermed er  $w^{-1}(\gamma)$  kompatibel med  $\Sigma$ .

Skriv nu  $h$  på formen  $\prod_{\alpha \in \Sigma} h_{\alpha}(t_{\alpha})$ . Da gælder

$$\begin{aligned}\sigma_{\gamma}({}^w h) &= \sigma_{\gamma} \left( \prod_{\alpha \in \Sigma} {}^w h_{\alpha}(t_{\alpha}) \right) = \sigma_{\gamma} \left( \prod_{\alpha \in \Sigma} h_{w(\alpha)}(t_{\alpha}) \right) = \prod_{\alpha \in \Sigma} t_{\alpha}^{(\gamma, w(\tilde{\alpha}))} \\ &= \prod_{\alpha \in \Sigma} t_{\alpha}^{(w^{-1}(\gamma), \tilde{\alpha})} = \sigma_{w^{-1}(\gamma)} \left( \prod_{\alpha \in \Sigma} h_{\alpha}(t_{\alpha}) \right) = \sigma_{w^{-1}(\gamma)}(h)\end{aligned}$$

□

**Definition 23.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$ , og lad  $\{\gamma_1, \dots, \gamma_l\}$  være banen for  $\gamma$  under virkningen fra  $W$ . *Diagonalafbildningen* hørende til  $\gamma$  er afbildningen  $\sigma : H \rightarrow (\mathbb{F}_q^{\times})^l$  givet ved  $\sigma(h) = (\sigma_{\gamma_1}(h), \dots, \sigma_{\gamma_l}(h))$ .

**Eksempel 7.** Betragt gruppen  $SL_3(\mathbb{F}_q)$  fra Eksempel 6. Denne gruppe er Chevalley-gruppen  $A_2(q)$ , og  $H$  består i dette tilfælde af elementerne

$$t = \begin{bmatrix} t_1 & 0 & 0 \\ 0 & t_2 & 0 \\ 0 & 0 & t_3 \end{bmatrix}$$

med  $t_i \in \mathbb{F}_q^{\times}$ . Skriv  $A_2$  på standardform, og fastlæg bijektionen mellem  $\Sigma$  og  $\Sigma(\overline{T})$  ved  $e_i - e_j \mapsto \chi_{ij}$ , hvor  $\chi_{ij}$  er som i Eksempel 3. Da er  $e_1$  kompatibel med  $A_2$ , og dens bane under  $W$  er  $\{e_1, e_2, e_3\}$ . Diagonalafbildningen hørende til  $e_1$  er givet ved  $\sigma(t) = (\sigma_{e_1}(t), \sigma_{e_2}(t), \sigma_{e_3}(t)) = (t_1, t_2, t_3)$ . Heraf navnet "diagonalafbildningen".

**Lemma 109.** Lad  $\{\gamma_1, \dots, \gamma_l\}$  være banen for  $\gamma$  under virkningen fra  $W$ , og lad for  $w \in W$  og  $1 \leq i \leq l$   $w(i)$  være det unikke tal således at  $w(\gamma_i) = \gamma_{w(i)}$ . Lad  $W$  virke på  $(\mathbb{F}_q^{\times})^l$  ved  $w(s_1, \dots, s_l) = (s_{w^{-1}(1)}, \dots, s_{w^{-1}(l)})$ . Dette er en veldefineret gruppevirkning.

*Bevis.* Lad  $e$  være identitetslementet i  $W$ ; da gælder  $\gamma_{e(i)} = e(\gamma_i) = \gamma_i$ , således at  $e(i) = i$  for alle  $i$ . Så er  $e(s_1, \dots, s_l) = (s_1, \dots, s_l)$ .

For vilkårlige  $v, w \in W$  gælder nu  $\gamma_{(vw)(i)} = (vw)(\gamma_i) = v(w(\gamma_i)) = v(\gamma_{w(i)}) = \gamma_{v(w(i))}$ , således at  $(vw)(i) = v(w(i))$  for ethvert  $i$ . Så fås:

$$\begin{aligned}(vw)(s_1, \dots, s_l) &= (s_{(vw)^{-1}(1)}, \dots, s_{(vw)^{-1}(l)}) = (s_{(w^{-1}v^{-1})(1)}, \dots, s_{(w^{-1}v^{-1})(l)}) \\ &= (s_{w^{-1}(v^{-1}(1))}, \dots, s_{w^{-1}(v^{-1}(l))}) = v(s_{w^{-1}(1)}, \dots, s_{w^{-1}(l)}) \\ &= v(w(s_1, \dots, s_l))\end{aligned}$$

Dermed er  $w(s_1, \dots, s_l) = (s_{w^{-1}(1)}, \dots, s_{w^{-1}(l)})$  en veldefineret gruppevirkning. □

**Sætning 110.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$ . *Diagonalafbildningen* hørende til  $\gamma$  bevarer virkningen fra  $W$ .

*Bevis.* For ethvert  $h \in H$  og  $w \in W$  gælder:

$$\begin{aligned}w(\sigma(h)) &= w(\sigma_{\gamma_1}(h), \dots, \sigma_{\gamma_l}(h)) = (\sigma_{\gamma_{w^{-1}(1)}}(h), \dots, \sigma_{\gamma_{w^{-1}(l)}}(h)) \\ &= (\sigma_{\gamma_1}({}^w h), \dots, \sigma_{\gamma_l}({}^w h)) = \sigma({}^w h)\end{aligned}$$

□

**Lemma 111.** Lad  $W$  virke på  $(\mathbb{F}_q^\times)^l$  og lad  $s = (s_1, \dots, s_l)$  være et element i  $(\mathbb{F}_q^\times)^l$ . Der gælder  $s \in C_{(\mathbb{F}_q^\times)^l}(w)$  hvis og kun hvis  $s_i = s_{w(i)}$  for hvert  $i$ .

*Bevis.* Der gælder  $s \in C_{(\mathbb{F}_q^\times)^l}(w)$  hvis og kun hvis  $s = w(s)$ , altså hvis  $(s_1, \dots, s_l) = w(s_1, \dots, s_l) = (s_{w^{-1}(1)}, \dots, s_{w^{-1}(l)})$ . Dette gælder præcis hvis  $s_i = s_{w^{-1}(i)}$  for hvert  $i \in \{1, \dots, l\}$ . Når  $i$  løber over mængden  $\{1, \dots, l\}$  vil  $w(i)$  løbe over samme mængde, da  $w$  er en permutation af denne mængde. Så fås  $s \in C_{(\mathbb{F}_q^\times)^l}(w)$  hvis og kun hvis  $s_{w(i)} = s_{w^{-1}(w(i))} = s_i$  for hvert  $i$ .  $\square$

**Sætning 112.** Lad  $\gamma \in \mathbb{E}^n$  være kompatibel med  $\Sigma$ , og lad  $\sigma : H \rightarrow (\mathbb{F}_q^\times)^l$  være diagonalafbildningen hørende til  $\gamma$ . Lad  $r$  være et primtal der opfylder  $r \mid q - 1$  og  $r \nmid |W|$ . Hvis  $\sigma$  er injektiv på  $H_r$ , er  $\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|}$  hvor  $\mathcal{M} = \{w \in W \mid C_{\sigma(H_r)}(w) \neq C_1\}$ .

*Bevis.* Idet  $\sigma$  er injektiv på  $H_r$ , er  $\sigma : H_r \rightarrow \sigma(H_r)$  en isomorfi, og per Sætning 110 bevarer den virkningen fra  $W$ . Dermed er  $C_{H_r}(w) \cong C_{\sigma(H_r)}(w)$  for alle  $w \in W$ . Resultatet følger nu af Sætning 104.  $\square$

Pointen med alt dette er at  $W$  virker på  $\sigma(H_r)$  ved at permutere koordinaterne, og det er derfor lettere at beskrive fikspunktsmængden for et element  $w \in W$ . Yderligere kan man ved passende valg af  $\gamma$  opnå at  $\sigma$  har en lille kerne, således at  $\sigma$  faktisk bliver injektiv på  $H_r$ .

Næste skridt er at beregne Weyl-gruppen for de forskellige rodsystemer.

**Lemma 113.** Lad  $\Sigma$  være enten  $A_{n-1}$ ,  $B_n$ ,  $C_n$  eller  $D_n$ , og lad  $\Sigma$  være på standardform. Da er  $e_1$  kompatibel med  $\Sigma$ . Ydermere gælder at  $W$  stabiliserer mængden  $\{\pm e_1, \dots, \pm e_n\}$ .

*Bevis.* Lad  $\alpha \in \Sigma$ ; da har  $\alpha$  formen  $\alpha = e_i - e_j$ ,  $\alpha = \pm(e_i + e_j)$ ,  $\alpha = \pm e_i$  eller  $\alpha = \pm 2e_i$ . I de to første tilfælde gælder  $\tilde{\alpha} = \alpha$ ; hvis  $\alpha = \pm e_i$  er  $\tilde{\alpha} = \pm 2e_i$ , og hvis  $\alpha = \pm 2e_i$  er  $\tilde{\alpha} = \pm e_i$ . I alle tilfælde fås at  $(e_1, \tilde{\alpha})$  er enten  $-2$ ,  $-1$ ,  $0$ ,  $1$  eller  $2$ , afhængigt af værdierne af  $i$  og  $j$  samt valget af fortegn. Dermed er  $e_1$  kompatibel med  $\Sigma$ .

Lad nu  $\alpha$  have formen  $\alpha = e_i - e_j$ . Ved direkte udregning fås  $r_\alpha(\pm e_i) = \pm e_j$ ,  $r_\alpha(\pm e_j) = \pm e_i$  og  $r_\alpha(\pm e_k) = \pm e_k$  for  $k \neq i$  og  $k \neq j$ . Dermed stabiliserer  $r_\alpha$  mængden  $\{\pm e_1, \dots, \pm e_n\}$ .

Hvis  $\alpha$  har formen  $\alpha = \pm(e_i + e_j)$  fås tilsvarende  $r_\alpha(\pm e_i) = \mp e_j$ ,  $r_\alpha(\pm e_j) = \mp e_i$  og  $r_\alpha(\pm e_k) = \pm e_k$  for  $k \neq i$  og  $k \neq j$ , således at  $r_\alpha$  også i dette tilfælde stabiliserer  $\{\pm e_1, \dots, \pm e_n\}$ .

Endelig ses at hvis  $\alpha = \pm e_i$  eller  $\alpha = \pm 2e_i$  gælder  $r_\alpha(\pm e_i) = \mp e_i$  og  $r_\alpha(\pm e_k) = \pm e_k$  for  $k \neq i$ , så  $r_\alpha$  stabiliserer  $\{\pm e_1, \dots, \pm e_n\}$ . Dermed gælder at  $r_\alpha$  stabiliserer  $\{\pm e_1, \dots, \pm e_n\}$  for hvert  $\alpha \in \Sigma$ , og da disse elementer frembringer  $W$ , må  $W$  stabilisere  $\{\pm e_1, \dots, \pm e_n\}$ .  $\square$

**Lemma 114.** Lad  $I$  være gruppen af alle isometrier af  $\mathbb{E}^n$  der stabiliserer mængden  $\{\pm e_1, \dots, \pm e_n\}$ . Da gælder  $\iota(-e_i) = -\iota(e_i)$  for ethvert  $\iota \in I$  og  $1 \leq i \leq n$ . Ydermere findes der undergrupper  $I_1$  og  $I_2$  af  $I$  således at  $I_1 \cong S_n$  og  $I_1$  er gruppen af alle isometrier der stabiliserer mængden  $\{e_1, \dots, e_n\}$ ,  $I_2 \cong C_2^n$  og  $I_2$  er gruppen af alle isometrier der stabiliserer mængden  $\{e_i, -e_i\}$  for hvert  $i$ , og  $I$  er et semidirekte produkt  $I_2 \rtimes I_1$  hvor  $I_1$  virker på  $I_2$  ved at permutere de  $n$  frembringere.

*Bevis.* Lad  $\iota \in I$ . Da  $\iota$  er en isometri, er den specielt en lineær afbildning, så der gælder  $\iota(-x) = -\iota(x)$  for alle  $x \in \mathbb{E}^n$ . Dette gælder så også når  $x = e_i$ .

Idet mængden  $\{e_1, \dots, e_n\}$  udspænder  $\mathbb{E}^n$ , er ethvert element i  $I$  unikt defineret ved sin virkning på disse elementer. Lad nu  $I_1$  være gruppen af isometrier af  $\mathbb{E}^n$  der stabiliserer  $\{e_1, \dots, e_n\}$ ; da er ethvert element i  $I_1$  unikt defineret ved hvilken permutation af  $\{e_1, \dots, e_n\}$  det inducerer. Dermed

er  $I_1$  isomorf med en undergruppe af  $S_n$ . Men idet mængden  $\{e_1, \dots, e_n\}$  er en ortonormalbasis for  $\mathbb{E}^n$ , kan enhver permutation af den udvides til en isometri af  $\mathbb{E}^n$ . Dermed er  $I_1 \cong S_n$ .

Lad nu  $r_i$  være reflektionen i hyperplanen ortogonal med  $e_i$ . Da gælder  $r_i(\pm e_i) = \mp e_i$  og  $r_i(\pm e_k) = \pm e_k$  for  $k \neq i$ . Dermed er  $r_i \in I$ , og  $r_i$  stabiliserer hver af mængderne  $\{e_k, -e_k\}$ . Definer  $I_2 = \langle r_i \mid 1 \leq i \leq n \rangle$ ; da vil  $I_2$  også stabilisere hver af mængderne  $\{e_k, -e_k\}$ . For  $i \neq j$  gælder nu  $(r_i r_j)(\pm e_i) = r_i(r_j(\pm e_i)) = r_i(\pm e_i) = \mp e_i = r_j(\mp e_i) = r_j(r_i(\pm e_i)) = (r_j r_i)(\pm e_i)$ , og tilsvarende fås  $(r_i r_j)(\pm e_j) = \mp e_j = (r_j r_i)(\pm e_j)$  og  $(r_i r_j)(\pm e_k) = \pm e_k = (r_j r_i)(\pm e_k)$  for  $k \neq i$  og  $k \neq j$ . Dermed er  $r_i r_j = r_j r_i$ . Da alle frembringerne for  $I_2$  således kommuterer, er  $I_2$  abelsk. Desuden har elementerne  $r_i$  alle orden 2, da de er reflektioner. Et vilkårligt element  $\iota \in I_2$  har så en fremstilling på formen  $\iota = \prod_{i=1}^n r_i^{n_i}$  hvor hvert  $n_i$  er enten 0 eller 1. Ved direkte udregning ses at der gælder  $\iota(e_i) = e_i$  hvis og kun hvis  $n_i = 0$ . Dermed er  $\iota$  identitetslementet hvis og kun hvis  $n_i = 0$  for hvert  $i$ , og så må  $I_2 \cong C_2^n$ .

Antag nu at  $\iota$  stabiliserer hver af mængderne  $\{e_i, -e_i\}$ . Definer  $n_i$  ved  $n_i = 0$  hvis  $\iota(e_i) = e_i$  og  $n_i = 1$  hvis  $\iota(e_i) = -e_i$ . Da er  $\iota = \prod_{i=1}^n r_i^{n_i}$ , da de to elementer tager samme værdi på hver af vektorerne  $e_i$ . Altså er  $\iota \in I_2$ , og  $I_2$  er gruppen af alle isometrier der stabiliserer hver af mængderne  $\{e_i, -e_i\}$ .

Lad  $\iota \in I_2$  og  $v \in I$  være vilkårlige. Lad  $c_i = 1$  hvis  $\iota(v^{-1}(e_i)) = v^{-1}(e_i)$  og  $c_i = -1$  hvis  $\iota(v^{-1}(e_i)) = -v^{-1}(e_i)$ , således at  $\iota(v^{-1}(e_i)) = c_i v^{-1}(e_i)$ . Så gælder  $v \iota(\pm e_i) = v(\iota(v^{-1}(\pm e_i))) = \pm v(\iota(v^{-1}(e_i))) = \pm v(c_i v^{-1}(e_i)) = \pm c_i v(v^{-1}(e_i)) = \pm c_i e_i$ , så  $v \iota$  stabiliserer mængden  $\{e_i, -e_i\}$ . Da dette gælder for hvert  $i$ , er  $v \iota \in I_2$ . Dermed er  $I_2$  normal i  $I$ .

Lad nu  $\iota \in I_1 \cap I_2$ . Da  $\iota \in I_1$  er  $\iota(e_i) \in \{e_1, \dots, e_n\}$ , og da  $\iota \in I_2$ , er  $\iota(e_i) \in \{e_i, -e_i\}$ . Så må  $\iota(e_i) = e_i$ , og da dette gælder for hvert  $i$ , er  $\iota$  identitetslementet. Altså er  $I_1 \cap I_2 = C_1$ .

Lad  $v \in I$  være vilkårlig, og definer  $\iota \in I_2$  ved  $\iota(e_i) = e_i$  hvis  $v(e_i) \in \{e_1, \dots, e_n\}$  og  $\iota(e_i) = -e_i$  hvis  $v(e_i) \in \{-e_1, \dots, -e_n\}$ . Hvis  $v(e_i) \in \{e_1, \dots, e_n\}$  fås så  $(v \iota)(e_i) = v(\iota(e_i)) = v(e_i) \in \{e_1, \dots, e_n\}$ , og hvis  $v(e_i) \in \{-e_1, \dots, -e_n\}$  fås  $(v \iota)(e_i) = v(\iota(e_i)) = v(-e_i) = -v(e_i) \in \{e_1, \dots, e_n\}$ . I begge tilfælde haves altså  $(v \iota)(e_i) \in \{e_1, \dots, e_n\}$ , og da dette gælder for alle  $i$  er  $v \iota \in I_1$ . Da  $\iota \in I_2$  har  $\iota$  orden 2, og så gælder  $v = (v \iota) \iota \in I_1 I_2$ . Dermed er  $I = I_1 I_2$ .

Nu haves  $I = I_1 I_2$ ,  $I_1 \cap I_2 = C_1$  og  $I_2 \triangleleft I$ . Så er  $I$  et semidirekte produkt  $I_2 \rtimes I_1$ . Tilbage er kun at beskrive virkningen af  $I_1$  på  $I_2$ .

Lad  $v \in I_1$  og lad  $v(i)$  være det unikke tal der opfylder  $v(e_i) = e_{v(i)}$ . Da gælder  ${}^v r_i(e_{v(i)}) = v(r_i(v^{-1}(e_{v(i)}))) = v(r_i(e_i)) = v(-e_i) = -e_{v(i)}$ . Hvis  $k \neq v(i)$  er  $e_k \neq v(e_i)$  og dermed  $v^{-1}(e_k) \neq e_i$ . Så er  $i \neq v^{-1}(k)$ , og dermed fås  ${}^v r_i(e_k) = v(r_i(v^{-1}(e_k))) = v(r_i(e_{v^{-1}(k)})) = v(e_{v^{-1}(k)}) = e_k$ . Dermed er  ${}^v r_i = r_{v(i)}$ , så  $I_1$  virker på  $I_2$  ved at permuterer frembringermængden  $\{r_1, \dots, r_n\}$ .  $\square$

**Sætning 115.**  $W(A_{n-1}) = I_1$ .

*Bevis.* Lad  $\alpha = e_i - e_j$  være et vilkårligt element i  $A_n$ . Ved direkte udregning ses at  $r_\alpha(e_i) = e_j$ ,  $r_\alpha(e_j) = e_i$  og  $r_\alpha(e_k) = e_k$  hvis  $k \neq i$  og  $k \neq j$ . Dermed stabiliserer  $r_\alpha$  mængden  $\{e_1, \dots, e_n\}$ , og da elementerne  $r_\alpha$ ,  $\alpha \in A_{n-1}$  frembringer  $W(A_{n-1})$  må  $W(A_{n-1})$  stabilisere  $\{e_1, \dots, e_n\}$ . Dermed er  $W(A_{n-1}) \subseteq I_1$ . Disse udregninger viser desuden at hvis  $\alpha = e_i - e_j$ , er  $r_\alpha$  netop transpositionen der ombytter  $e_i$  og  $e_j$ . Transpositionerne frembringer som bekendt hele den symmetriske gruppe, og dermed er  $W(A_{n-1}) = I_1$ .  $\square$

**Sætning 116.**  $W(B_n) = I$ .

*Bevis.* Idet  $W(B_n)$  stabiliserer  $\{\pm e_1, \dots, \pm e_n\}$ , er  $W(B_n) \subseteq I$ .

Lad som før  $r_i$  være reflektionen i hyperplanen ortogonal med  $e_i$ . Hvis  $\alpha = e_i$  er  $\alpha \in B_n$  og  $r_\alpha = r_i$ , og så fås  $r_i \in W(B_n)$ . Da dette gælder for hvert  $i$  og elementerne  $r_i$  frembringer  $I_2$ , er  $I_2 \subseteq W(B_n)$ .

$A_{n-1}$  består af vektorerne  $e_i - e_j$  med  $1 \leq i \leq n$  og  $1 \leq j \leq n$ , og disse vektorer er også elementer i  $B_n$ . Dermed ses at hvis  $\alpha \in A_{n-1}$  er  $r_\alpha \in W(B_n)$ , og da elementerne  $r_\alpha$ ,  $\alpha \in A_{n-1}$  frembringer  $W(A_{n-1})$  fås  $W(A_{n-1}) \subseteq W(B_n)$ . Per Sætning 115 er  $W(A_{n-1}) = I_1$ , og dermed er  $I_1 \subseteq W(B_n)$ .

Da  $I_1 \subseteq W(B_n)$  og  $I_2 \subseteq W(B_n)$  fås  $I = I_1 I_2 \subseteq W(B_n)$ . Da der også gælder  $W(B_n) \subseteq I$ , er  $W(B_n) = I$ .  $\square$

**Sætning 117.**  $W(C_n) = I$ .

*Bevis.* Da  $r_\alpha$  er reflektionen i hyperplanen ortogonal med  $\alpha$  og  $\check{\alpha}$  er parallel med  $\alpha$ , er  $r_{\check{\alpha}} = r_\alpha$ . Idet  $C_n = \check{B}_n$  fås så  $W(C_n) = \langle r_\alpha \mid \alpha \in C_n \rangle = \langle r_{\check{\alpha}} \mid \alpha \in B_n \rangle = \langle r_\alpha \mid \alpha \in B_n \rangle = W(B_n)$ . Da  $W(B_n) = I$  er så  $W(C_n) = I$ .  $\square$

**Sætning 118.** Definer en homomorfi  $\varphi : I_2 \rightarrow C_2 = \{1, -1\}$  ved  $\varphi(r_i) = -1$  for hvert  $i$ , og lad  $I'_2 = \ker(\varphi)$ . Da er  $W(D_n) = I'_2 \rtimes I_1$ .

*Bevis.* Bemærk først at der gælder  $\varphi(\prod_{i=1}^n r_i^{n_i}) = \prod_{i=1}^n (-1)^{n_i} = (-1)^{\sum_{i=1}^n n_i}$ , så  $I'_2$  består netop af de elementer  $\prod_{i=1}^n r_i^{n_i} \in I_2$  som opfylder at  $\sum_{i=1}^n n_i$  er lige. Idet  $I_1$  virker på  $I_2$  ved at permutere frembringerne  $r_i$ , fås så at hvis  $\iota \in I'_2$  og  $v \in I_1$  vil også  $v\iota \in I'_2$ . Altså kan virkningen af  $I_1$  på  $I_2$  indskrænkes til en virkning på  $I'_2$ , og dermed er  $I'_2 \rtimes I_1$  en veldefineret undergruppe af  $I$ .

Lad nu  $\iota = \prod_{i=1}^n r_i^{n_i}$  være et vilkårligt element i  $I'_2$ . Idet  $\sum_{i=1}^n n_i$  er lige og hvert  $n_i$  er enten 0 eller 1, kan  $\iota$  så skrives som et produkt af faktorer af formen  $r_i r_j$  hvor  $i \neq j$ . Altså er  $I'_2$  frembragt af elementerne  $r_i r_j$ .

Lad nu  $\alpha$  være et element i  $D_n$  på formen  $\alpha = e_i - e_j$ . Da gælder  $r_\alpha(e_i) = e_j$ ,  $r_\alpha(e_j) = e_i$  og  $r_\alpha(e_k) = e_k$  for  $k \neq i$  og  $k \neq j$ . Dermed er  $r_\alpha \in I_1 \subset I'_2 \rtimes I_1$ .

Lad nu i stedet  $\alpha$  have formen  $\alpha = \pm(e_i + e_j)$ . Da gælder  $r_\alpha(e_i) = -e_j$ ,  $r_\alpha(e_j) = -e_i$  og  $r_\alpha(e_k) = e_k$  for  $k \neq i$  og  $k \neq j$ . Lad  $\beta = e_i - e_j$ , således at  $r_\beta \in I_1$  er transpositionen der ombytter  $e_i$  og  $e_j$ . Da haves  $(r_i r_j r_\beta)(e_i) = r_i(r_j(r_\beta(e_i))) = r_i(r_j(e_j)) = r_i(-e_j) = -e_j = r_\alpha(e_i)$ , og tilsvarende fås  $(r_i r_j r_\beta)(e_j) = -e_i = r_\alpha(e_j)$  og  $(r_i r_j r_\beta)(e_k) = e_k = r_\alpha(e_k)$  for  $k \neq i$  og  $k \neq j$ . Dermed er  $r_\alpha = r_i r_j r_\beta$ . Da  $r_i r_j \in I'_2$  og  $r_\beta \in I_1$  fås så  $r_\alpha \in I'_2 \rtimes I_1$ .

Altså haves  $r_\alpha \in I'_2 \rtimes I_1$  for hvert  $\alpha \in D_n$ . Da disse elementer frembringer  $W(D_n)$  fås  $W(D_n) \subseteq I'_2 \rtimes I_1$ .

Ethvert element i  $A_{n-1}$  er også et element i  $D_n$ , og dermed fås  $W(A_{n-1}) = \langle r_\alpha \mid \alpha \in A_{n-1} \rangle \subseteq \langle r_\alpha \mid \alpha \in D_n \rangle = W(D_n)$ . Da  $W(A_{n-1}) = I_1$ , er så  $I_1 \subseteq W(D_n)$ .

Lad nu  $i \neq j$ , og lad  $\alpha = e_i + e_j$  og  $\beta = e_i - e_j$ . Da er  $\alpha, \beta \in D_n$ , og de foregående udregninger viser  $r_\alpha r_\beta = r_i r_j r_\beta^2 = r_i r_j$ . Da  $r_\alpha r_\beta \in W(D_n)$  fås  $r_i r_j \in W(D_n)$ . Da elementerne  $r_i r_j$  frembringer  $I'_2$  fås  $I'_2 \subseteq W(D_n)$ .

Nu haves  $I_1 \subseteq W(D_n)$  og  $I'_2 \subseteq W(D_n)$ . Så må  $I'_2 \rtimes I_1 \subseteq W(D_n)$ , og dermed er  $W(D_n) = I'_2 \rtimes I_1$ .  $\square$

**Lemma 119.** Hvis  $\Sigma = A_{n-1}$  er banen for  $e_1$  under  $W$  lig  $\{e_1, \dots, e_n\}$ ; hvis  $\Sigma = B_n$ ,  $\Sigma = C_n$  eller  $\Sigma = D_n$  er banen for  $e_1$  under  $W$  lig  $\{\pm e_1, \dots, \pm e_n\}$ .

*Bevis.* Banen for  $e_1$  er i alle tilfælde indeholdt i  $\{\pm e_1, \dots, \pm e_n\}$ , da  $W$  stabiliserer denne mængde.



Hvis  $\Sigma = A_{n-1}$  er  $W = I_1$ , og  $I_1$  er gruppen af alle permutationer af  $\{e_1, \dots, e_n\}$ . Så må banen for  $e_1$  under  $W$  være  $\{e_1, \dots, e_n\}$ . I de andre tre tilfælde gælder  $I_1 \subset W$ , så mængden  $\{e_1, \dots, e_n\}$  må indgå i banen for  $e_1$ . Men i disse tilfælde gælder at  $W$  for hvert  $i$  indeholder et element der afbilder  $e_i$  i  $-e_i$ , så elementerne  $-e_i$  må også indgå i banen for  $e_1$ . Dermed er banen for  $e_1$  netop  $\{\pm e_1, \dots, \pm e_n\}$ .  $\square$

Fremover sorteres banen for  $e_1$  i rækkefølgen  $\{e_1, \dots, e_n, -e_1, \dots, -e_n\}$ , således at når  $\sigma$  er diagonalafbildningen hørende til  $e_1$ , så er  $\sigma(h) = (\sigma_{e_1}(h), \dots, \sigma_{e_n}(h), \sigma_{-e_1}(h), \dots, \sigma_{-e_n}(h))$ . For at lette notationen skrives  $\sigma_i$  for  $\sigma_{e_i}$  og  $\sigma_{-i}$  for  $\sigma_{-e_i}$ . Et element  $s$  i  $(\mathbb{F}_q^\times)^{2n}$  betegnes med  $s = (s_1, \dots, s_n, s_{-1}, \dots, s_{-n})$ , således at hvis  $s = \sigma(h)$  er  $s_i = \sigma_i(h)$  og  $s_{-i} = \sigma_{-i}(h)$  for hvert  $i$  med  $1 \leq i \leq n$ . I tilfældet  $\Sigma = A_{n-1}$  udelades anden halvdel af disse lister, således at  $\sigma(h) = (\sigma_1(h), \dots, \sigma_n(h))$  og et element  $s$  i  $(\mathbb{F}_q^\times)^n$  betegnes med  $(s_1, \dots, s_n)$ .

**Sætning 120.** *Antag  $r \mid q - 1$  og  $r \nmid |W|$ , lad  $\Sigma = A_{n-1}$  og lad  $\sigma : H_r \rightarrow (\mathbb{F}_q^\times)^n$  være restriktionen til  $H_r$  af diagonalafbildningen hørende til  $e_1$ . Da er  $\ker(\sigma) = C_1$  og  $\text{Im}(\sigma) = \{(s_1, \dots, s_n) \mid s_i \in \mathbb{F}_q^{(r)}, \prod_{i=1}^n s_i = 1\}$ .*

*Bevis.* Lad  $\alpha_i = e_i - e_{i+1}$  for  $1 \leq i \leq n - 1$ ; da er  $\Pi = \{\alpha_1, \dots, \alpha_{n-1}\}$  et fundamentalt system for  $\Sigma$  per Sætning 16. Per Lemma 98 gælder at  $H_r$  netop består af elementerne  $\prod_{i=1}^{n-1} h_{\alpha_i}(t_i)$  med  $t_i \in \mathbb{F}_q^{(r)}$ .

Lad nu  $h = \prod_{i=1}^{n-1} h_{\alpha_i}(t_i)$  være et vilkårligt element i  $H_r$ . Ved direkte udregning fås så  $\sigma_1(h) = t_1$ ,  $\sigma_i(h) = t_i t_{i-1}^{-1}$  for  $2 \leq i \leq n - 1$  og  $\sigma_n(h) = t_{n-1}^{-1}$ . Antag nu  $\sigma(h) = 1$ ; da gælder  $\sigma_i(h) = 1$  for hvert  $i$ . Så fås  $t_1 = \sigma_1(h) = 1$ , og det kan nu vises ved induktion at  $t_i = 1$  for ethvert  $i$ . Antag nemlig  $t_{i-1} = 1$  for  $2 \leq i \leq n - 1$ ; da fås  $t_i = t_i t_{i-1}^{-1} = \sigma_i(h) = 1$ . Dermed er  $h = 1$ , og så må  $\ker(\sigma) = C_1$ .

Skriv nu  $\sigma(h) = (\sigma_1(h), \dots, \sigma_n(h))$ . Da gælder  $\prod_{i=1}^n \sigma_i(h) = t_1 \cdot \prod_{i=2}^{n-1} (t_i t_{i-1}^{-1}) \cdot t_{n-1}^{-1} = t_1 \cdot \prod_{i=2}^{n-1} t_i \cdot \prod_{i=2}^{n-1} t_{i-1}^{-1} \cdot t_{n-1}^{-1} = \prod_{i=1}^{n-1} t_i \cdot \prod_{i=2}^n t_{i-1}^{-1} = \prod_{i=1}^{n-1} t_i \cdot \left(\prod_{i=1}^{n-1} t_i\right)^{-1} = 1$ . Desuden giver Lemma 107 at  $\sigma_i(h) \in \mathbb{F}_q^{(r)}$  for hvert  $i$ , og så er  $\text{Im}(\sigma) \subseteq \{(s_1, \dots, s_n) \mid s_i \in \mathbb{F}_q^{(r)}, \prod_{i=1}^n s_i = 1\}$ .

Lad nu  $s = (s_1, \dots, s_n)$  være et vilkårligt element i  $(\mathbb{F}_q^\times)^n$  som opfylder  $s_i \in \mathbb{F}_q^{(r)}$  for hvert  $i$  og  $\prod_{i=1}^n s_i = 1$ . Lad  $\beta_i = e_i - e_n$  for hvert  $i$  med  $1 \leq i \leq n - 1$ , og definer  $h = \prod_{i=1}^{n-1} h_{\beta_i}(s_i)$ . Da er  $h \in H_r$  per Lemma 98. Ved direkte udregning fås  $\sigma_i(h) = s_i$  for  $1 \leq i \leq n - 1$  og  $\sigma_n(h) = \prod_{j=1}^{n-1} s_j^{-1} = \left(\prod_{j=1}^{n-1} s_j\right)^{-1} \cdot s_n = s_n$ . Dermed er  $\sigma(h) = s$ , og da  $s$  var vilkårlig fås så  $\text{Im}(\sigma) = \{(s_1, \dots, s_n) \mid s_i \in \mathbb{F}_q^{(r)}, \prod_{i=1}^n s_i = 1\}$ .  $\square$

**Sætning 121.** *Antag  $r \mid q - 1$  og  $r \nmid |W|$ , lad  $\Sigma = B_n$  og lad  $\sigma : H_r \rightarrow (\mathbb{F}_q^\times)^{2n}$  være restriktionen til  $H_r$  af diagonalafbildningen hørende til  $e_1$ . Da er  $\ker(\sigma) = C_1$  og  $\text{Im}(\sigma) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .*

*Bevis.* Bemærk først at da  $r \nmid |W|$  og  $W$  indeholder elementer af orden 2, er  $r \neq 2$ . Dermed er  $\mathbb{F}_q^{(r)}$  cyklisk af ulige orden.

Lad  $\alpha_i = e_i - e_{i+1}$  for  $1 \leq i \leq n - 1$  og  $\alpha_n = e_n$ ; da er  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  et fundamentalt system for  $\Sigma$  per Sætning 16. Per Lemma 98 gælder at  $H_r$  netop består af elementerne  $\prod_{i=1}^n h_{\alpha_i}(t_i)$  med  $t_i \in \mathbb{F}_q^{(r)}$ .

Lad nu  $h = \prod_{i=1}^n h_{\alpha_i}(t_i)$  være et vilkårligt element i  $H_r$ . Ved direkte udregning fås så  $\sigma_1(h) = t_1$ ,  $\sigma_i(h) = t_i t_{i-1}^{-1}$  for  $2 \leq i \leq n - 1$  og  $\sigma_n(h) = t_n^2 t_{n-1}^{-1}$ . Antag nu  $\sigma(h) = 1$ ; da gælder  $\sigma_i(h) = 1$  for ethvert  $i$ . Som i beviset for Sætning 120 fås så  $t_i = 1$  hvis  $1 \leq i \leq n - 1$ . Desuden gælder

$t_n^2 = t_n^2 t_{n-1}^{-1} = \sigma_n(h) = 1$ . Men nu er  $t_n \in \mathbb{F}_q^{(r)}$ , og da  $\mathbb{F}_q^{(r)}$  har ulige orden medfører  $t_n^2 = 1$  at  $t_n = 1$ . Dermed er  $h = 1$ , og så må  $\ker(\sigma) = C_1$ .

Per Lemma 107 gælder  $\sigma_i(h) \in \mathbb{F}_q^{(r)}$  og per Lemma 106 gælder  $\sigma_{-i}(h) = \sigma_i(h)^{-1}$ . Så må  $\text{Im}(\sigma) \subseteq \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .

Lad nu  $s = (s_1, \dots, s_n, s_1^{-1}, \dots, s_n^{-1})$  være et vilkårligt element i  $\{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ . Idet  $\mathbb{F}_q^{(r)}$  er cyklisk af ulige orden, er afbildningen  $x \mapsto x^2$  en automorfi af  $\mathbb{F}_q^{(r)}$ . Så findes der for hver  $i$  et  $s'_i \in \mathbb{F}_q^{(r)}$  som opfylder  $s_i'^2 = s_i$ . Lad nu  $\beta_i = e_i$  og definer  $h = \prod_{i=1}^n h_{\beta_i}(s'_i)$ . Per Lemma 98 er så  $h \in H_r$ , og ved direkte udregning fås  $\sigma_i(h) = s_i'^2 = s_i$  og  $\sigma_{-i}(h) = s_i'^{-2} = s_i^{-1}$  for  $1 \leq i \leq n$ . Altså er  $\sigma(h) = s$ , og dermed er  $\text{Im}(\sigma) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .  $\square$

**Sætning 122.** *Antag  $r \mid q-1$  og  $r \nmid |W|$ , lad  $\Sigma = C_n$  og lad  $\sigma : H_r \rightarrow (\mathbb{F}_q^\times)^{2n}$  være restriktionen til  $H_r$  af diagonalafbildningen hørende til  $e_1$ . Da er  $\ker(\sigma) = C_1$  og  $\text{Im}(\sigma) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .*

*Bevis.* Lad  $\alpha_i = e_i - e_{i+1}$  for  $1 \leq i \leq n-1$  og  $\alpha_n = 2e_n$ ; da er  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  et fundamentalt system for  $\Sigma$  per Sætning 16. Per Lemma 98 gælder at  $H_r$  netop består af elementerne  $\prod_{i=1}^n h_{\alpha_i}(t_i)$  med  $t_i \in \mathbb{F}_q^{(r)}$ .

Lad nu  $h = \prod_{i=1}^n h_{\alpha_i}(t_i)$  være et vilkårligt element i  $H_r$ . Ved direkte udregning fås så  $\sigma_1(h) = t_1$  og  $\sigma_i(h) = t_i t_{i-1}^{-1}$  for  $2 \leq i \leq n$ . Som i beviset for Sætning 120 fås så  $t_i = 1$  for alle  $i$ , og så er  $h = 1$ . Så må  $\ker(\sigma) = C_1$ .

Som i beviset for Sætning 121 ses at der gælder  $\text{Im}(\sigma) \subseteq \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .

Lad nu  $s = (s_1, \dots, s_n, s_1^{-1}, \dots, s_n^{-1})$  være et vilkårligt element i  $\{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ . Definer  $\beta_i = 2e_i$  og lad  $h = \prod_{i=1}^n h_{\beta_i}(s_i)$ . Per Lemma 98 er så  $h \in H_r$ , og ved direkte udregning fås  $\sigma_i(h) = s_i$  og  $\sigma_{-i}(h) = s_i^{-1}$  for  $1 \leq i \leq n$ . Altså er  $\sigma(h) = s$ , og dermed er  $\text{Im}(\sigma) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .  $\square$

**Sætning 123.** *Antag  $r \mid q-1$  og  $r \nmid |W|$ , lad  $\Sigma = D_n$  og lad  $\sigma : H_r \rightarrow (\mathbb{F}_q^\times)^{2n}$  være restriktionen til  $H_r$  af diagonalafbildningen hørende til  $e_1$ . Da er  $\ker(\sigma) = C_1$  og  $\text{Im}(\sigma) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .*

*Bevis.* Lad  $\alpha_i = e_i - e_{i+1}$  for  $1 \leq i \leq n-1$  og  $\alpha_n = e_{n-1} + e_n$ ; da er  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  et fundamentalt system for  $\Sigma$  per Sætning 16. Per Lemma 98 gælder at  $H_r$  netop består af elementerne  $\prod_{i=1}^n h_{\alpha_i}(t_i)$  med  $t_i \in \mathbb{F}_q^{(r)}$ .

Lad nu  $h = \prod_{i=1}^n h_{\alpha_i}(t_i)$  være et vilkårligt element i  $H_r$ . Ved direkte udregning fås så  $\sigma_1(h) = t_1$ ,  $\sigma_i(h) = t_i t_{i-1}^{-1}$  for  $2 \leq i \leq n-1$ ,  $\sigma_{n-1}(h) = t_n t_{n-1} t_{n-2}^{-1}$  og  $\sigma_n(h) = t_n t_{n-1}^{-1}$ . Som i beviset for Sætning 120 fås så  $t_i = 1$  for alle  $1 \leq i \leq n-1$ . Så gælder  $t_n t_{n-1} = t_n t_{n-1} t_{n-2}^{-1} = \sigma_{n-1}(h) = 1$  og  $t_n t_{n-1}^{-1} = \sigma_n(h) = 1$ , og dermed er  $t_n^2 = (t_n t_{n-1})(t_n t_{n-1}^{-1}) = 1 \cdot 1 = 1$ . Da  $\mathbb{F}_q^{(r)}$  har ulige orden fås så  $t_n = 1$ . Da  $t_n t_{n-1} = 1$  gælder så også  $t_{n-1} = 1$ , og dermed er  $t_i = 1$  for hvert  $i$ . Så er  $h = 1$ , og så må  $\ker(\sigma) = C_1$ .

Som i beviset for Sætning 121 ses at der gælder  $\text{Im}(\sigma) \subseteq \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .

Lad nu  $s = (s_1, \dots, s_n, s_1^{-1}, \dots, s_n^{-1})$  være et vilkårligt element i  $\{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ . Definer  $\beta_i = e_i - e_{i+1}$  for  $1 \leq i \leq n-1$  og  $\beta_n = e_{n-1} + e_n$ , og lad  $s_0 = s_n \prod_{i=1}^{n-2} s_i$ .

Som før er afbildningen  $x \mapsto x^2$  en automorfi af  $\mathbb{F}_q^{(r)}$ , og der findes så  $u, v \in \mathbb{F}_q(r)$  som opfylder  $u^2 = s_{n-1}s_0^{-1}$  og  $v^2 = s_{n-1}s_0$ . Da gælder  $u^2v^2 = (s_{n-1})^2$ , således at  $uv = s_{n-1}$ , og  $u^{-2}v^2 = s_0^2$ , således at  $u^{-1}v = s_0$ . Lad nu  $h = \prod_{i=1}^{n-2} h_{\beta_i}(s_i) \cdot h_{\beta_{n-1}}(u)h_{\beta_n}(v)$ ; da giver Lemma 98 at  $h \in H_r$ . Desuden fås ved direkte udregning  $\sigma_i(h) = s_i$  for  $1 \leq i \leq n-2$ ,  $\sigma_{n-1}(h) = uv = s_{n-1}$  og  $\sigma_n(h) = \prod_{i=1}^{n-2} s_i^{-1} \cdot u^{-1}v = \prod_{i=1}^{n-2} s_i^{-1} \cdot s_0 = s_n$ . Per Lemma 106 gælder så også  $\sigma_{-i}(h) = s_i^{-1}$  for  $1 \leq i \leq n$ , således at  $\sigma(h) = s$ . Dermed er  $\text{Im}(\sigma) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ .  $\square$

**Sætning 124.** *Antag  $r \mid q-1$  og  $r \nmid |W|$ , lad  $\Sigma = A_{n-1}$ , og lad  $w \in W$ . Der gælder  $C_{\sigma(H_r)}(w) = C_1$  hvis og kun hvis  $w$  er en  $n$ -cyklus.*

*Bevis.* Bemærk først at da  $W = I_1 \cong S_n$  er  $n \mid |W|$ , og da  $r \nmid |W|$  fås  $r \nmid n$ .

Per Sætning 120 er  $\sigma(H_r) = \{(s_1, \dots, s_n) \mid s_i \in \mathbb{F}_q^{(r)}, \prod_{i=1}^n s_i = 1\}$ . Lad nu  $w \in W$  være en  $n$ -cyklus, og lad  $s \in C_{\sigma(H_r)}(w)$ . Ved brug af Lemma 111 fås så  $s_1 = s_{w(1)} = s_{w^2(1)} = \dots$ , og ved induktion fås  $s_1 = s_{w^k(1)}$  for alle  $k \in \mathbb{N}$ . Idet  $w$  er en  $n$ -cyklus kan ethvert  $i \in \{1, \dots, n\}$  skrives på formen  $i = w^k(1)$  for passende  $k$ . Dermed er  $s_1 = s_i$  for alle  $i$ . Idet  $s \in \sigma(H_r)$  have nu  $s_1^n = \prod_{i=1}^n s_1 = \prod_{i=1}^n s_i = 1$ . Da  $r \nmid n$  er afbildningen  $x \mapsto x^n$  en automorfi af  $\mathbb{F}_q^{(r)}$ , så  $s_1^n = 1$  medfører  $s_1 = 1$ . Dermed er  $s_i = s_1 = 1$  for ethvert  $i$ , så  $s = 1$ . Så må  $C_{\sigma(H_r)}(w) = C_1$ .

Antag nu at  $w$  ikke er en  $n$ -cyklus. Da består  $w$  af mindst to cyklusser, og summen af disse cyklussers længde er  $n$ . Da  $r \nmid n$  har mindst en af disse cyklusser længde ikke delelig med  $r$ . Lad  $j \in \{1, \dots, n\}$  være et element i en cyklus af længde  $m$  med  $r \nmid m$ . Lad  $x, y \in \mathbb{F}_q^{(r)}$  og definer  $s = (s_1, \dots, s_n)$  ved  $s_i = x$  hvis  $i$  er i samme cyklus i  $w$  som  $j$  og  $s_i = y$  hvis  $i$  og  $j$  ikke er i samme cyklus i  $w$ . Da giver Lemma 111 at  $w(s) = s$ . Lad nu  $y \neq 1$  være fastholdt. Idet  $r \nmid m$  er afbildningen  $x \mapsto x^m$  en automorfi af  $\mathbb{F}_q^{(r)}$ . Det er så muligt at vælge  $x \in \mathbb{F}_q^{(r)}$  således at  $x^m = y^{m-n}$ . Så gælder  $\prod_{i=1}^n s_i = x^m y^{n-m} = y^{m-n} y^{n-m} = 1$ , således at  $s \in \sigma(H_r)$ . Da  $y \neq 1$  er  $s \neq 1$ , og  $s$  er dermed et ikke-trivielt element i  $C_{\sigma(H_r)}(w)$ . Altså er  $C_{\sigma(H_r)}(w) \neq 1$ .  $\square$

**Sætning 125.** *Antag  $r \mid q-1$  og  $r \nmid |W|$ , og lad  $\Sigma = A_{n-1}$ . Da er  $\chi(\mathcal{F}_r(K)) = 1 - \frac{1}{n}$ .*

*Bevis.* Per Sætning 112 og Sætning 124 er  $\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|}$  hvor  $\mathcal{M}$  er mængden af alle elementer i  $W$  der ikke er  $n$ -cyklusser. Idet  $W \cong S_n$  er  $|W| = n!$ . Lad nu  $w \in W$  være en  $n$ -cyklus; da er elementerne  $w(n), w^2(n), \dots, w^{n-1}(n)$  indbyrdes forskellige og forskellige fra  $n$ . Så må listen  $w(n), w^2(n), \dots, w^{n-1}(n)$  indeholde hver af elementerne i  $\{1, \dots, n-1\}$  netop én gang. Det er så muligt at definere en permutation  $v$  af mængden  $\{1, \dots, n-1\}$  ved  $v(i) = w^i(n)$  for  $1 \leq i \leq n-1$ . Omvendt gælder at en  $n$ -cyklus  $w$  i  $W$  er unikt defineret ved værdierne  $w^i(n)$  for  $1 \leq i \leq n-1$ , og  $w$  er en  $n$ -cyklus netop hvis listen  $w(n), w^2(n), \dots, w^{n-1}(n)$  indeholder hver af elementerne i  $\{1, \dots, n-1\}$  netop en gang. Givet en permutation  $v$  af  $\{1, \dots, n-1\}$  er det så muligt at definere en  $n$ -cyklus  $w$  i  $W$  ved  $w^i(n) = v(i)$  for  $1 \leq i \leq n-1$ . Dermed er der en én-til-én-korrespondance mellem  $n$ -cyklusser i  $W$  og permutationer af  $\{1, \dots, n-1\}$ . Da der er  $(n-1)!$  sådanne permutationer, indeholder  $W$  netop  $(n-1)!$   $n$ -cyklusser, og så må  $|\mathcal{M}| = n! - (n-1)!$ . Så fås

$$\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|} = \frac{n! - (n-1)!}{n!} = \frac{n!}{n!} - \frac{(n-1)!}{n!} = 1 - \frac{1}{n}$$

$\square$

**Sætning 126.** *Antag  $r \mid q-1$  og  $r \nmid |W|$ , lad  $\Sigma = B_n$ ,  $\Sigma = C_n$  eller  $\Sigma = D_n$ , og lad  $w \in W$ . Der gælder  $C_{\sigma(H_r)}(w) = C_1$  hvis og kun hvis der for ethvert  $i \in \{1, \dots, n\}$  findes et  $k \in \mathbb{N}$  således at  $w^k(i) = -i$ ; alternativt, hvis og kun hvis  $i$  og  $-i$  er i samme cyklus i  $w$  for ethvert  $i \in \{1, \dots, n\}$ .*

*Bevis.* Bemærk først at per definitionen på cyklus er  $i$  og  $-i$  i samme cyklus i  $w$  hvis og kun hvis der findes et  $k \in \mathbb{N}$  så  $w^k(i) = -i$ . Dermed er de to betingelser ækvivalente.

Per Sætning 121, 122 og 123 er  $\sigma(H_r) = \{(s_1, \dots, s_n, s_{-1}, \dots, s_{-n}) \mid s_i \in \mathbb{F}_q^{(r)}, s_{-i} = s_i^{-1}\}$ . Lad nu  $w \in W$ , og antag at der for hvert  $i \in \{1, \dots, n\}$  findes et  $k \in \mathbb{N}$  således at  $w^k(i) = -i$ . Lad  $s = (s_1, \dots, s_n, s_{-1}, \dots, s_{-n})$  være et element i  $C_{\sigma(H_r)}(w)$ . Så giver Lemma 111 at  $s_i = s_{w^k(i)} = s_{-i}$  for hvert  $i$ , og da  $s \in \sigma(H_r)$  gælder også  $s_i^{-1} = s_{-i}$ . Så fås  $s_i = s_i^{-1}$  og dermed  $s_i^2 = 1$ . Da  $\mathbb{F}_q^{(r)}$  har ulige orden, medfører dette  $s_i = 1$ . Da  $s_i^{-1} = s_{-i}$  gælder også  $s_{-i} = 1$ , og så er  $s = 1$ . Altså er  $C_{\sigma(H_r)}(w) = C_1$ .

Lad nu  $w \in W$  og antag at der findes et  $j \in \{1, \dots, n\}$  således at  $w^k(j) \neq -j$  for alle  $k \in \mathbb{N}$ . Dette betyder at  $j$  og  $-j$  ikke er i samme cyklus i  $w$ . Lad nu  $x \in \mathbb{F}_q^{(r)}$  og definer  $s = (s_1, \dots, s_n, s_{-1}, \dots, s_{-n})$  ved at der for hvert  $i \in \{\pm 1, \dots, \pm n\}$  gælder  $s_i = x$  hvis  $i$  er i samme cyklus i  $w$  som  $j$ ,  $s_i = x^{-1}$  hvis  $i$  er i samme cyklus i  $w$  som  $-j$ , og  $s_i = 1$  ellers. Da giver Lemma 111 at  $w(s) = s$ . Antag nu at  $s_i = x$ ; da findes der  $k \in \mathbb{N}$  så  $i = w^k(j)$ . Ifølge Lemma 114 gælder nu  $w(-i) = -w(i)$  for hvert  $i$ , og specielt haves så  $-i = -w^k(j) = w^k(-j)$ . Dermed er  $-i$  i samme cyklus i  $w$  som  $-j$ , og så er  $s_{-i} = x^{-1} = s_i^{-1}$ . Tilsvarende fås at hvis  $s_i = x^{-1}$  er  $s_{-i} = x = s_i^{-1}$ . Endelig ses at hvis  $s_i = 1$  viser disse argumenter at  $s_{-i}$  hverken kan være  $x$  eller  $x^{-1}$ , og så er  $s_{-i} = 1 = s_i^{-1}$ . Dermed er  $s_{-i} = s_i^{-1}$  for alle  $i$ , og så er  $s \in \sigma(H_r)$ . Dermed fås at hvis  $x$  vælges til at være forskellig fra 1, så er  $s$  et ikke-trivielt element i  $C_{\sigma(H_r)}(w)$ . Altså er  $C_{\sigma(H_r)}(w) \neq C_1$ .  $\square$

**Sætning 127.** Antag  $r \mid q-1$  og  $r \nmid |W|$ , og lad  $\Sigma = B_n$  eller  $\Sigma = C_n$ . Da er  $\chi(\mathcal{F}_r(K)) = 1 - \frac{(2n-1)!!}{2^n \cdot n!}$ .

*Bevis.* Per Sætning 112 og Sætning 124 er  $\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|}$  hvor  $\mathcal{M}$  er mængden af alle elementer  $w$  i  $W$  hvorom det gælder at der findes et  $i \in \{1, \dots, n\}$  som opfylder at  $i$  og  $-i$  ikke er i samme cyklus i  $w$ . Definer nu  $\mathcal{M}' = W \setminus \mathcal{M}$ , således at  $\mathcal{M}'$  består af alle elementer  $w$  i  $W$  hvorom det gælder at for hvert  $i \in \{1, \dots, n\}$  er  $i$  og  $-i$  i samme cyklus i  $w$ . Så haves

$$\chi(\mathcal{F}_r(K)) = \frac{|\mathcal{M}|}{|W|} = \frac{|W| - |\mathcal{M}'|}{|W|} = \frac{|W|}{|W|} - \frac{|\mathcal{M}'|}{|W|} = 1 - \frac{|\mathcal{M}'|}{|W|}$$

Det skal så vises at  $|\mathcal{M}'| = (2n-1)!!$  og  $|W| = 2^n \cdot n!$ .

Per Sætning 116 og 117 er  $W = I$ , og per Lemma 114 er  $W$  så et semidirekte produkt  $W = I_2 \rtimes I_1$ . Idet  $I_1 \cong S_n$  og  $I_2 \cong C_2^n$ , er  $|I_1| = n!$  og  $|I_2| = 2^n$ . Så fås  $|W| = |I_2| \cdot |I_1| = 2^n \cdot n!$ .

Da  $I_2$  er normal i  $W$ , findes der en kvotientafbildning  $\pi : W \rightarrow W/I_2$ . Denne afbildning kan beskrives på følgende måde: Idet  $w(-i) = -w(i)$  for alle  $i$ , gælder  $w(\{i, -i\}) = \{w(i), w(-i)\} = \{w(i), -w(i)\}$  for alle  $i$ , således at  $w(\{i, -i\})$  har formen  $\{j, -j\}$  for passende  $j$ . Så virker  $W$  på mængden af mængder  $\{\{1, -1\}, \dots, \{n, -n\}\}$ . Lad  $S_n$  være gruppen af alle permutationer af denne mængde; gruppevirkningen fra  $W$  giver så en afbildning  $\pi : W \rightarrow S_n$ . Kernen af denne afbildning består af de elementer i  $W$  der stabiliserer  $\{i, -i\}$  for hvert  $i$ ; dette er netop gruppen  $I_2$ , således at  $\pi(W) \cong W/I_2$ . Lad nu  $v$  være et vilkårligt element i  $S_n$ ; da gælder for ethvert  $i \in \{1, \dots, n\}$  at der findes et unikt  $j \in \{1, \dots, n\}$  som opfylder  $v(\{i, -i\}) = \{j, -j\}$ . Det er så muligt at definere et element  $w \in W$  ved for hvert  $i \in \{1, \dots, n\}$  at sætte  $w(i) = j$  og  $w(-i) = -j$  hvor  $j \in \{1, \dots, n\}$  er det unikke tal der opfylder  $v(\{i, -i\}) = \{j, -j\}$ . Så gælder  $w \in I_1$  da  $w$  stabiliserer  $\{1, \dots, n\}$ , og ydermere er  $\pi(w) = v$ . Dermed er  $\text{Im}(\pi) = S_n$ , og der gælder  $W/I_2 \cong S_n$ .

For at lette notationen skrives nu  $i$  for mængden  $\{i, -i\}$ , således at  $S_n$  virker på  $\{1, \dots, n\}$ . Der haves så en surjektiv homomorfi  $\pi : W \rightarrow S_n$  med kerne  $I_2$ , og for hvert  $w \in I_1$  gælder  $\pi(w)(i) = w(i)$  for alle  $i \in \{1, \dots, n\}$ .

Lad nu  $v \in S_n$  og definer  $\mathcal{M}'_v = \mathcal{M}' \cap \pi^{-1}(v)$ . Da er  $\mathcal{M}'$  en disjunkt forening af mængderne  $\mathcal{M}'_v$ ,  $v \in S_n$ , og der gælder

$$\chi(\mathcal{F}_r(K)) = 1 - \frac{|\mathcal{M}'|}{|W|} = 1 - \frac{1}{2^n \cdot n!} \sum_{v \in S_n} |\mathcal{M}'_v|$$

Idet  $\ker(\pi) \cap I_1 = I_2 \cap I_1 = C_1$ , er  $\pi$  injektiv på  $I_1$ . Desuden er det blevet vist at for ethvert  $v \in S_n$  findes der et  $w \in I_1$  således at  $\pi(w) = v$ . Så indeholder  $I_1 \cap \pi^{-1}(v)$  altid netop ét element. Lad  $w_0$  være dette element; da består  $\pi^{-1}(v)$  af elementerne  $w_0 \iota$ ,  $\iota \in I_2$ . Beviset for Lemma 114 giver desuden at  $\iota$  har en unik fremstilling på formen  $\iota = \prod_{i=1}^n r_i^{n_i}$  hvor hvert  $n_i$  er enten 0 eller 1 og  $r_i$  er givet ved  $r_i(\pm i) = \mp i$  og  $r_i(\pm j) = \pm j$  for  $j \neq i$ . Der gælder så  $\iota(i) = (-1)^{n_i} i$  for alle  $i \in \{1, \dots, n\}$ .

Lad nu  $v \in S_n$  og  $i \in \{1, \dots, n\}$ , og antag at  $i$  indgår i en cyklus af længde  $c$  i  $v$ . Der gælder så  $v^c(i) = i$  og  $v^k(i) \neq i$  for  $1 \leq k \leq c-1$ . Lad  $w$  være et vilkårligt element i  $\pi^{-1}(v)$ , og skriv  $w = w_0 \prod_{i=1}^n r_i^{n_i}$  med  $w_0 \in I_1$ . Antag  $w \in \mathcal{M}'_v$ ; da findes der et  $k \in \mathbb{N}$  således at  $w^k(i) = -i$ . Dette medfører  $\pi(w^k)(i) = i$  og dermed  $v^k(i) = i$ , og så må  $k \geq c$ . Altså er  $w^k(i) \neq -i$  for  $1 \leq k \leq c-1$ . Yderligere ses at da  $v^c(i) = i$  er  $w^c(i) = i$  eller  $w^c(i) = -i$ . Hvis  $w^c(i) = i$  indgår  $i$  så i en cyklus af længde  $c$  i  $w$ , og da  $w^k(i) \neq -i$  for  $1 \leq k \leq c-1$  indeholder denne cyklus ikke  $-i$ . Altså må  $w^c(i) = -i$ .

Nu gælder  $w(i) = (w_0 \prod_{i=1}^n r_i^{n_i})(i) = w_0((-1)^{n_i} i) = (-1)^{n_i} w_0(i) = (-1)^{n_i} v(i)$ . På tilsvarende vis fås  $w^2(i) = w((-1)^{n_i} v(i)) = (-1)^{n_i} w(v(i)) = (-1)^{n_i} (-1)^{n_{v(i)}} v^2(i) = (-1)^{n_i + n_{v(i)}} v^2(i)$ , og ved induktion fås  $w^k(i) = (-1)^{\sum_{j=0}^{k-1} n_{v^j(i)}} v^k(i)$  for alle  $k \in \mathbb{N}$ . Specielt haves så

$$w^c(i) = (-1)^{\sum_{j=0}^{c-1} n_{v^j(i)}} v^c(i) = (-1)^{\sum_{j=0}^{c-1} n_{v^j(i)}} i.$$

Dette er lig  $-i$  netop hvis  $\sum_{j=0}^{c-1} n_{v^j(i)}$  er ulige. Da  $i$  indgår i en cyklus af længde  $c$  i  $v$ , er tallene  $i, v(i), v^2(i), \dots, v^{c-1}(i)$  alle forskellige. Der findes nu  $2^{c-1}$  måder at vælge værdien af tallene  $n_i, n_{v(i)}, n_{v^2(i)}, \dots, n_{v^{c-2}(i)}$ , og uanset hvilken måde der vælges findes der netop én værdi af  $n_{v^{c-1}(i)}$  der gør summen  $\sum_{j=0}^{c-1} n_{v^j(i)}$  ulige.

Såfremt  $\sum_{j=0}^{c-1} n_{v^j(i)}$  er ulige, gælder altså  $w^c(i) = -i$ . Så fås  $w^c(w^k(i)) = w^k(w^c(i)) = w^k(-i) = -w^k(i)$  for alle  $k \in \mathbb{N}$ , og dermed gælder  $w^c(j) = -j$  hvis  $j$  indgår i samme cyklus som  $i$  i  $v$ . Dermed ses at hvis  $\sum_{j=0}^{c-1} n_{v^j(i)}$  er ulige, er  $j$  og  $-j$  i samme cyklus i  $w$  hvis  $j$  og  $i$  er i samme cyklus i  $v$ , og hvis  $\sum_{j=0}^{c-1} n_{v^j(i)}$  er lige er  $i$  og  $-i$  ikke i samme cyklus i  $w$ . Lad nu  $N_v \subseteq \{1, \dots, n\}$  være en mængde af repræsentanter for cyklusserne i  $v$ , og lad for hvert  $i \in N_v$   $c_i$  være længden af den cyklus  $i$  indgår i. Ovenstående medfører så at der gælder  $w \in \mathcal{M}'_v$  hvis og kun hvis  $\sum_{j=0}^{c_i-1} n_{v^j(i)}$  er ulige for alle  $i \in N_v$ .

På grund af den måde  $N_v$  og  $c_i$  er defineret gælder at når  $i$  løber over  $N_v$  og  $j$  løber fra 0 til  $c_i - 1$ , så løber  $v^j(i)$  over alle elementerne i  $\{1, \dots, n\}$  netop én gang. Dermed er et element i  $\pi^{-1}(v)$  unikt fastlagt af værdien af tallene  $n_{v^j(i)}$ ,  $0 \leq j \leq c_i - 1$ ,  $i \in N_v$ . Det er tidligere set at der findes  $2^{c_i-1}$  måder at vælge tallene  $n_{v^j(i)}$ ,  $0 \leq j \leq c_i - 1$  så  $\sum_{j=0}^{c_i-1} n_{v^j(i)}$  bliver ulige. Antallet af elementer i  $\mathcal{M}'_v$  bliver så

$$\prod_{i \in N_v} 2^{c_i-1} = 2^{\sum_{i \in N_v} (c_i-1)} = 2^{(\sum_{i \in N_v} c_i - \sum_{i \in N_v} 1)} = 2^{n - |N_v|}$$

Definer for ethvert  $v \in S_n$   $c_v$  ved  $c_v = |N_v|$ , således at  $c_v$  er antallet af cyklusser i  $v$ . Da gælder

$$\chi(\mathcal{F}_r(K)) = 1 - \frac{1}{2^n \cdot n!} \sum_{v \in S_n} |\mathcal{M}'_v| = 1 - \frac{1}{2^n \cdot n!} \sum_{v \in S_n} 2^{n-c_v}$$

Tilbage er så at vise at  $\sum_{v \in S_n} 2^{n-c_v} = (2n-1)!!$ . Dette gøres ved induktion over  $n$ .

Lad først  $n = 1$ . Da indeholder  $S_n$  netop ét element,  $e$ , og der gælder  $c_e = 1$ . Så er  $\sum_{v \in S_n} 2^{n-c_v} = 2^{n-c_e} = 2^0 = 1 = 1!!$ .

Lad det nu være givet at  $\sum_{w \in S_{n-1}} 2^{(n-1)-c_w} = (2n-3)!!$ . Definer  $R_n = \{v \in S_n \mid v(n) = n\}$  og  $R'_n = \{v \in S_n \mid v(n) \neq n\}$ , og definer en funktion  $\rho : S_n \rightarrow S_{n-1}$  ved at  $\rho(v)$  er den permutation der fremkommer ved at skrive  $v$  på cyklusform og fjerne elementet  $n$ . (Med andre ord er  $\rho(v)(i) = v(i)$  hvis  $v(i) \neq n$  og  $\rho(v)(i) = v^2(i)$  hvis  $v(i) = n$ .) Dette er ikke en gruppehomomorfi, blot en afbildning af mængder. Da ses at for et vilkårligt  $w \in S_{n-1}$  er  $|\rho^{-1}(w) \cap R_n| = 1$  og  $|\rho^{-1}(w) \cap R'_n| = n-1$ . Der findes nemlig  $k$  måder at indsætte elementet  $n$  i en cyklus af længde  $k$ , så der er  $n-1$  måder at indsætte  $n$  i en eksisterende cyklus, hvilket giver et element i  $R'_n$ . Desuden er der præcis én måde at indsætte  $n$  i en ny cyklus, hvilket giver et element i  $R_n$ .

Nu gælder at hvis  $v \in R_n$  er  $c_{\rho(v)} = c_v - 1$ , da  $\rho$  fjerner cyklussen kun bestående af  $n$ . Så gælder

$$\begin{aligned} \sum_{v \in R_n} 2^{n-c_v} &= \sum_{w \in S_{n-1}} \sum_{v \in \rho^{-1}(w) \cap R_n} 2^{(n-1)-(c_v-1)} = \sum_{w \in S_{n-1}} \sum_{v \in \rho^{-1}(w) \cap R_n} 2^{(n-1)-c_w} \\ &= \sum_{w \in S_{n-1}} |\rho^{-1}(w) \cap R_n| \cdot 2^{(n-1)-c_w} = \sum_{w \in S_{n-1}} 2^{(n-1)-c_w} \\ &= (2n-3)!! \end{aligned}$$

Hvis  $v \in R'_n$ , er  $c_{\rho(v)} = c_v$ , da  $n$  indgår i en cyklus med mindst et andet element, så  $\rho$  modificerer blot en cyklus uden at fjerne den. Så gælder

$$\begin{aligned} \sum_{v \in R'_n} 2^{n-c_v} &= \sum_{w \in S_{n-1}} \sum_{v \in \rho^{-1}(w) \cap R'_n} 2 \cdot 2^{(n-1)-c_v} = \sum_{w \in S_{n-1}} \sum_{v \in \rho^{-1}(w) \cap R'_n} 2 \cdot 2^{(n-1)-c_w} \\ &= \sum_{w \in S_{n-1}} 2|\rho^{-1}(w) \cap R'_n| \cdot 2^{(n-1)-c_w} = \sum_{w \in S_{n-1}} 2(n-1) \cdot 2^{(n-1)-c_w} \\ &= (2n-2) \sum_{w \in S_{n-1}} 2^{(n-1)-c_w} = (2n-2) \cdot (2n-3)!! \end{aligned}$$

Samlet fås nu

$$\begin{aligned} \sum_{v \in S_n} 2^{n-c_v} &= \sum_{v \in R_n} 2^{n-c_v} + \sum_{v \in R'_n} 2^{n-c_v} = (2n-3)!! + (2n-2) \cdot (2n-3)!! \\ &= (2n-1) \cdot (2n-3)!! = (2n-1)!! \end{aligned}$$

og dermed haves

$$\chi(\mathcal{F}_r(K)) = 1 - \frac{1}{2^n \cdot n!} \sum_{v \in S_n} 2^{n-c_v} = 1 - \frac{(2n-1)!!}{2^n \cdot n!}$$

□

**Sætning 128.** Antag  $r \mid q-1$  og  $r \nmid |W|$ , og lad  $\Sigma = D_n$ . Da er  $\chi(\mathcal{F}_r(K)) = 1 - \frac{(n-1) \cdot (2n-3)!!}{2^n \cdot n!}$ .

*Bevis.* Beviset for dette er meget analogt til beviset for Sætning 127. I dette tilfælde er  $W = I'_2 \rtimes I_1$ , og da  $|I'_2| = 2^{n-1}$  fås  $|W| = 2^{n-1} \cdot n!$ . Som før defineres en surjektiv afbildning  $\pi : W \rightarrow S_n$ , denne

gang med kerne  $I'_2$ , og restriktionen af  $\pi$  til  $I_1$  bliver igen en naturlig isomorfi. Igen defineres  $\mathcal{M}' = W \setminus \mathcal{M}$  og  $\mathcal{M}'_v = \mathcal{M}' \cap \pi^{-1}(v)$ , og på samme måde som før fås

$$\chi(\mathcal{F}_r(K)) = 1 - \frac{1}{2^{n-1} \cdot n!} \sum_{v \in S_n} |\mathcal{M}'_v|$$

Lad nu igen  $w = w_0 \prod_{i=1}^n r_i^{n_i}$  være et element i  $\pi^{-1}(v)$ , lad  $N_v$  være en mængde af repræsentanter for cyklusserne i  $v$ , lad for  $i \in N_v$   $c_i$  være længden af den cyklus i  $v$  i indgår i, og lad  $c_v = |N_v|$ . På samme måde som før ses at  $w \in \mathcal{M}'_v$  hvis og kun hvis der for hvert  $i \in N_v$  gælder at  $\sum_{j=0}^{c_i-1} n_{vj(i)}$  er ulige. Dermed fås igen at der er  $2^{n-c_v}$  mulige valg af tallene  $n_i$  som giver  $w \in \mathcal{M}'_v$ . Det skal så undersøges hvor mange af disse valgmuligheder der opfylder at  $\sum_{i=1}^n n_i$  er lige, således at  $w$  faktisk er et element i  $W = I'_2 \times I_1$ .

Antag nu at  $c_v$  er lige. Idet  $\sum_{j=0}^{c_i-1} n_{vj(i)}$  er ulige for hvert  $i \in N_v$  fås så at  $\sum_{i=1}^n n_i = \sum_{i \in N_v} \sum_{j=0}^{c_i-1} n_{vj(i)}$  er lige, således at  $\prod_{i=1}^n r_i^{n_i}$  er indeholdt i  $I'_2$ . Dette medfører at  $w$  faktisk er indeholdt i  $W$ , og så er  $|\mathcal{M}'_v| = 2^{n-c_v}$ .

Antag nu at  $c_v$  er ulige. Idet  $\sum_{j=0}^{c_i-1} n_{vj(i)}$  er ulige for hvert  $i \in N_v$  fås så at  $\sum_{i=1}^n n_i = \sum_{i \in N_v} \sum_{j=0}^{c_i-1} n_{vj(i)}$  er ulige, hvilket medfører  $\prod_{i=1}^n r_i^{n_i} \notin I'_2$ . Dermed er  $w \notin W$ , og så fås  $|\mathcal{M}'_v| = 0$ . Lad nu  $\mathbf{LS}_n$  være mængden af elementer  $v \in S_n$  hvorom det gælder at  $c_v$  er lige. Så have altså

$$\chi(\mathcal{F}_r(K)) = 1 - \frac{1}{2^{n-1} \cdot n!} \sum_{v \in S_n} |\mathcal{M}'_v| = 1 - \frac{1}{2^{n-1} \cdot n!} \sum_{v \in \mathbf{LS}_n} 2^{n-c_v}$$

Det skal så vises at  $\sum_{v \in \mathbf{LS}_n} 2^{n-c_v} = (n-1) \cdot (2n-3)!!$ .

Lad nu  $\mathbf{US}_n$  være mængden af elementer  $v \in S_n$  hvorom det gælder at  $c_v$  er ulige, således at  $S_n$  er en disjunkt forening af  $\mathbf{LS}_n$  og  $\mathbf{US}_n$ . Ved induktion vises det at  $\sum_{v \in \mathbf{LS}_n} 2^{n-c_v} = (n-1) \cdot (2n-3)!!$  og  $\sum_{v \in \mathbf{US}_n} 2^{n-c_v} = n \cdot (2n-3)!!$ .

Lad først  $n = 2$ . Så indeholder  $\mathbf{LS}_n$  netop ét element, nemlig identiteten  $e$ , og der gælder  $c_e = 2$ . Så er  $\sum_{v \in \mathbf{LS}_n} 2^{n-c_v} = 2^{n-c_e} = 2^0 = 1 = (2-1) \cdot 1!!$ . Ligeledes indeholder  $\mathbf{US}_n$  netop ét element, nemlig transpositionen  $g$ , og der gælder  $c_g = 1$ . Så er  $\sum_{v \in \mathbf{US}_n} 2^{n-c_v} = 2^{n-c_g} = 2^1 = 2 = 2 \cdot 1!!$ .

Lad det nu være givet at  $\sum_{v \in \mathbf{LS}_{n-1}} 2^{(n-1)-c_v} = (n-2) \cdot (2n-5)!!$  og  $\sum_{v \in \mathbf{US}_{n-1}} 2^{(n-1)-c_v} = (n-1) \cdot (2n-5)!!$ . Definer som før  $R_n = \{v \in S_n \mid v(n) = n\}$  og  $R'_n = \{v \in S_n \mid v(n) \neq n\}$ , og definer igen funktionen  $\rho : S_n \rightarrow S_{n-1}$  ved at  $\rho(v)$  er den permutation der fremkommer ved at skrive  $v$  på cyklusform og fjerne elementet  $n$ . Definer også  $\mathbf{LR}_n = \mathbf{LS}_n \cap R_n$ ,  $\mathbf{UR}_n = \mathbf{US}_n \cap R_n$ ,  $\mathbf{LR}'_n = \mathbf{LS}_n \cap R'_n$  og  $\mathbf{UR}'_n = \mathbf{US}_n \cap R'_n$ . Nu ses at hvis  $w \in \mathbf{US}_{n-1}$ , er  $|\rho^{-1}(w) \cap \mathbf{LR}_n| = 1$  og  $|\rho^{-1}(w) \cap \mathbf{UR}'_n| = n-1$ . Der findes nemlig igen  $n-1$  måder at indsætte  $n$  i en eksisterende cyklus; dette ændrer ikke antallet og cyklusser, og derfor fås et element i  $\mathbf{UR}'_n$ . Desuden er der præcis én måde at indsætte  $n$  i en ny cyklus; dette forøger antallet af cyklusser med 1, og derfor fås et element i  $\mathbf{LR}_n$ . Helt analogt fås at hvis  $w \in \mathbf{LS}_{n-1}$ , er  $|\rho^{-1}(w) \cap \mathbf{UR}_n| = 1$  og  $|\rho^{-1}(w) \cap \mathbf{LR}'_n| = n-1$ .

Lad nu  $v \in \mathbf{UR}_n$ ; da er  $c_{\rho(v)} = c_v - 1$ , da  $\rho$  fjerner cyklusen kun bestående af  $n$ . Så er  $\rho(v) \in \mathbf{LS}_{n-1}$ , og der gælder

$$\begin{aligned} \sum_{v \in \mathbf{UR}_n} 2^{n-c_v} &= \sum_{w \in \mathbf{LS}_{n-1}} \sum_{v \in \rho^{-1}(w) \cap \mathbf{UR}_n} 2^{(n-1)-(c_v-1)} = \sum_{w \in \mathbf{LS}_{n-1}} \sum_{v \in \rho^{-1}(w) \cap \mathbf{UR}_n} 2^{(n-1)-c_w} \\ &= \sum_{w \in \mathbf{LS}_{n-1}} |\rho^{-1}(w) \cap \mathbf{UR}_n| \cdot 2^{(n-1)-c_w} = \sum_{w \in \mathbf{LS}_{n-1}} 2^{(n-1)-c_w} \\ &= (n-2) \cdot (2n-5)!! \end{aligned}$$

Tilsvarende ses at hvis  $v \in \mathbf{UR}'_n$ , er  $c_{\rho(v)} = c_v$ , da  $n$  indgår i en cyklus med mindst et andet element, så  $\rho$  modificerer blot en cyklus uden at fjerne den. Så er  $\rho(v) \in \mathbf{US}_{n-1}$ , og der gælder

$$\begin{aligned} \sum_{v \in \mathbf{UR}'_n} 2^{n-c_v} &= \sum_{w \in \mathbf{US}_{n-1}} \sum_{v \in \rho^{-1}(w) \cap \mathbf{UR}_n} 2 \cdot 2^{(n-1)-c_w} = \sum_{w \in \mathbf{S}_{n-1}} \sum_{v \in \rho^{-1}(w) \cap \mathbf{UR}_n} 2 \cdot 2^{(n-1)-c_w} \\ &= \sum_{w \in \mathbf{US}_{n-1}} 2|\rho^{-1}(w) \cap \mathbf{UR}_n| \cdot 2^{(n-1)-c_w} = \sum_{w \in \mathbf{US}_{n-1}} 2(n-1) \cdot 2^{(n-1)-c_w} \\ &= (2n-2) \sum_{w \in \mathbf{US}_{n-1}} 2^{(n-1)-c_w} = (2n-2) \cdot (n-1) \cdot (2n-5)!! \end{aligned}$$

Samlet fås nu

$$\begin{aligned} \sum_{v \in \mathbf{US}_n} 2^{n-c_v} &= \sum_{v \in \mathbf{UR}_n} 2^{n-c_v} + \sum_{v \in \mathbf{UR}'_n} 2^{n-c_v} \\ &= (n-2) \cdot (2n-5)!! + (2n-2) \cdot (n-1) \cdot (2n-5)!! \\ &= ((n-2) + (2n-2) \cdot (n-1)) \cdot (2n-5)!! \\ &= (n-2 + 2n^2 - 4n + 2) \cdot (2n-5)!! = (2n^2 - 3n) \cdot (2n-5)!! \\ &= n \cdot (2n-3) \cdot (2n-5)!! = n \cdot (2n-3)!! \end{aligned}$$

For  $\mathbf{LR}_n$  og  $\mathbf{LR}'_n$  fås tilsvarende

$$\begin{aligned} \sum_{v \in \mathbf{LR}_n} 2^{n-c_v} &= \sum_{w \in \mathbf{US}_{n-1}} 2^{(n-1)-c_w} \\ &= (n-1) \cdot (2n-5)!! \end{aligned}$$

og

$$\begin{aligned} \sum_{v \in \mathbf{LR}'_n} 2^{n-c_v} &= 2(n-1) \sum_{w \in \mathbf{LS}_{n-1}} 2^{(n-1)-c_w} \\ &= (2n-2) \cdot (n-2) \cdot (2n-5)!! \end{aligned}$$

og samlet havs så

$$\begin{aligned} \sum_{v \in \mathbf{LS}_n} 2^{n-c_v} &= \sum_{v \in \mathbf{LR}_n} 2^{n-c_v} + \sum_{v \in \mathbf{LR}'_n} 2^{n-c_v} \\ &= (n-1) \cdot (2n-5)!! + (2n-2) \cdot (n-2) \cdot (2n-5)!! \\ &= ((n-1) + (2n-2) \cdot (n-2)) \cdot (2n-5)!! \\ &= (n-1 + 2n^2 - 6n + 4) \cdot (2n-5)!! = (2n^2 - 5n + 3) \cdot (2n-5)!! \\ &= (n-1) \cdot (2n-3) \cdot (2n-5)!! = (n-1) \cdot (2n-3)!! \end{aligned}$$

Hermed er induktionsbeviset gennemført, og der gælder

$$\chi(\mathcal{F}_r(K)) = 1 - \frac{1}{2^n \cdot n!} \sum_{v \in \mathbf{LS}_n} 2^{n-c_v} = 1 - \frac{(n-1) \cdot (2n-3)!!}{2^n \cdot n!}$$

□



## Litteratur

- [BLO] Carles Broto, Ran Levi, Bob Oliver: The theory of  $p$ -local groups: a survey. *Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic K-theory*, 51–84. Contemporary Mathematics 346, American Mathematical Society, 2004.
- [Ca] Roger Carter: Simple Groups of Lie Type. John Wiley & Sons, 1972.
- [GLS] Daniel Gorenstein, Richard Lyons, Ronald Solomon: The Classification of the Finite Simple Groups, Number 3. The American Mathematical Society, 1998.
- [Ja] Martin Wedel Jacobsen: Euler-karakteristik for fusionskategorier.
- [Lei] Tom Leinster: The Euler characteristic of a category. *Documenta Mathematica*, Vol. 13 (2008), 21–49.