Universiteit Gent
Faculteit Wetenschappen
Vakgroep Wiskunde: Algebra en Meetkunde

Eenheden van Integrale Groepringen

Arjen Dujardin

UNIVERSITEIT
GENT

Academiejaar 2022-2023

Promotor: Prof. dr. Tom De Medts

Masterproef ingediend tot het behalen van de academische graad van Master in de Wiskunde.

Voorwoord

Ik heb veel getwijfeld bij het kiezen van een onderwerp voor mijn masterproef. Uiteindelijk heb ik gekozen voor groepringen. Ik heb dit onderwerp gekozen omdat een groepring op een zeer natuurlijke manier gedefinieerd is. Om de structuur van een groepring te bestuderen heeft men ook een mooie balans tussen groepentheorie en ringtheorie nodig, die me beide enorm interesseren.

Ik zou graag mijn promotor prof. dr. De Medts willen bedankten om me te begeleiden bij deze thesis. Ook wil ik al mijn vrienden bedanken waarmee ik het afgelopen semester tussen al het harde thesis werk door toch nog veel mooie momenten van ontspanning mee kon beleven. Specifiek wil ik mijn vriendin Christina bedanken voor het nalezen en alle steun die ik kreeg.

Arjen Dujardin
1 juni 2023

Inhoudsopgave

Voorwoord **iii**

Inleiding **vii**

1. Inleidende begrippen **8**
1.1. De transfer afbeelding . . . 8
1.2. Bi-geordende groepen . . . 12
1.3. Groepringen . . . 15
1.3.1. De augmentatieafbeelding . . . 17
1.4. Ordes . . . 18
1.5. Karakters . . . 20
1.5.1. Het karakterveld . . . 22

2. Groepringen van torsievrije groepen **26**
2.1. De Kaplansky problemen . . . 26

3. Groepringen van eindige groepen **31**
3.1. Karakterisatie van integrale groepringen met enkel triviale eenheden . . . 31
3.1.1. Bicyclische en Basseenheden . . . 31
3.1.2. Integrale groepringen met enkel triviale eenheden . . . 34
3.1.3. De stelling van Higman . . . 38
3.2. Het isomorfisme probleem . . . 39
3.2.1. De Zassenhaus vermoedens . . . 41
3.3. De HeLP methode . . . 42
3.3.1. Partiële augmentatie . . . 42
3.3.2. De HeLP methode . . . 49
3.4. De cut groepen . . . 51
3.4.1. De symmetrische groep S_n is cut . . . 53

Bibliografie **55**

Inleiding

Het doel van deze thesis is om een duidelijk zicht te geven op de theorie rondom eenheden van groepringen. We zullen voornamelijk integrale groepringen beschouwen van eindige groepen. Dit zijn groepringen waarbij de ring de gehele getallen $\mathbb{Z}$ is.

Om deze thesis op zichzelf staand te maken, beginnen we met een hoofdstuk inleidende begrippen. Dit hoofdstuk bevat verschillende secties gericht op groepentheorie of ringtheorie, die we zullen gebruiken in latere delen. We gaan er wel vanuit dat de lezer een basiskennis algebra heeft. We geven ook al een sectie over groepringen bij de inleidende begrippen. Deze sectie zal de belangrijke begrippen introduceren en dient een inzicht te geven in de structuur van een groepring.
In het tweede hoofdstuk werpen we een blik op groepringen van torsievrije groepen. In dit hoofdstuk trachten we te illustreren hoe verschillend het onderzoek naar eenheden van deze groepringen is ten opzichte van groepringen van eindige groepen.
Het derde en laatste hoofdstuk zal gaan over groepringen van eindige groepen. We zullen de groepen classificeren wiens integrale groepring slechts een eindig aantal eenheden bevat. De kennis die we opdoen over eenheden gebruiken we dan verder om het isomorfisme probleem te bespreken.

1 Inleidende begrippen

1.1 De transfer afbeelding

Definitie 1.1.1. (i) Zij G een groep en $H \leq G$ een deelgroep. **Een transversaal T van H in G** is een complete verzameling van nevenklasserepresentanten van G/H.

(ii) Zij R, S twee transversalen van H in G, dan definiëren we het element

$$d(R,S) = \prod_{\substack{r\in R, s\in S \\ Hr=Hs}} \pi(rs^{-1}),$$

waarbij $\pi : H \to H/[H,H]$ de canonieke projectie is.

Opmerking 1.1.2. Het element $d(S,R)$ is goed gedefinieerd omdat $H/[H,H]$ abels is.

In het volgend lemma bewijzen we enkele eigenschappen van dit element.

Lemma 1.1.3. *Zij G een groep, $H \leq G$ een deelgroep van G en R, S twee transversalen van H in G. We bewijzen de volgende eigenschappen voor het element $d(R,S)$ uit Definitie 1.1.1 (ii):*

(i) $d(R,S)^{-1} = d(S,R)$;

(ii) $d(R,S)d(S,T) = d(R,T)$ *voor elke transversaal T van H in G;*

(iii) $d(Rg,Sg) = d(R,S)$ *voor elke $g \in G$;*

(iv) $d(Rg,R) = d(Sg,S)$ *voor elke $g \in G$.*

Bewijs. De eerste drie eigenschappen zijn triviaal. Men hoeft hier enkel het feit dat π een morfisme is toe te passen. We bewijzen (iv) aan de hand van de vorige eigenschappen:

$$\begin{aligned} d(Rg,R) &\overset{(ii)}{=} d(Rg,S)d(S,R) \\ &\overset{(ii)}{=} d(Rg,Sg)d(Sg,S)d(S,R) \\ &\overset{(iii)}{=} d(R,S)d(S,R)d(Sg,S) \\ &\overset{(i)}{=} d(Sg,S). \end{aligned}$$

Merk op dat we bij de derde lijn ook gebruik maken van het feit dat $H/[H,H]$ abels is. ■

Gevolg 1.1.4. *Zij G een groep, $H \leq G$ een deelgroep van G en T een willekeurige transversaal van H in G. De afbeelding*

$$\nu : G \to H/[H,H], g \mapsto d(Tg,T)$$

is een groepsmorfisme en is onafhankelijk van de keuze van de transversaal T.

Bewijs. We rekenen $\nu(gh)$ uit:

$$\nu(gh) = d(Tgh, T) = d(Tgh, Th)d(Th, T) = d(Tg, T)d(Th, T) = \nu(g)\nu(h).$$

Dit bewijst dat ν een groepsmorfisme is. Lemma 1.1.3(iv) bewijst dat het morfisme ν onafhankelijk is van de keuze van de transversaal. ■

We hebben nu alles bewezen wat we nodig hebben om de transfer afbeelding te definiëren.

Definitie 1.1.5. Zij G een groep en $H \leq G$ een deelgroep van eindige index. De **transfer afbeelding van G in H** is het groepsmorfisme

$$\nu : G \to H/[H, H], g \mapsto d(Tg, g)$$

uit Gevolg 1.1.4, waarbij T een willekeurige transversaal van H in G is.

Opmerking 1.1.6. Zij G een groep, $H \leq G$ een deelgroep van eindige index n en $T = \{t_1, \ldots, t_n\}$ een transversaal van H in G. Zij $g \in G$, elk element $t \in Tg$ zullen we schrijven als $t = t_i g$, met $t_i \in T$. Stel dat $\sigma \in \mathrm{S}_n$ de permutatie is zodat $Ht_i g = Ht_{\sigma(i)}$ voor elke $i \in \{1, \ldots, n\}$. Nu is de transfer afbeelding ν van H in G het morfisme

$$\nu : G \to H/[H, H], \nu(g) = \prod_{i=1}^{n} \pi(t_i g t_{\sigma(i)}^{-1}).$$

We zullen via deze permutatie en zijn cykelstructuur het beeld van $g \in G$ onder de transfer afbeelding makkelijker kunnen berekenen.

Lemma 1.1.7. *Zij G een groep, $H \leq G$ een deelgroep van eindige index n en $T = \{x_1, \ldots, x_n\}$ een transversaal van H in G. Voor elk element $g \in G$ bestaat er een getal m, elementen $s_1, \ldots, s_m \in T$ en getallen $n_1, \ldots, n_m$ zodat $s_i^{-1} g^{n_i} s_i \in H, n_1 + \cdots + n_m = n$ en*

$$\nu(g) = \prod_{i=1}^{m} \pi(s_i g^{n_i} s_i^{-1}).$$

Bewijs. Stel dat $\sigma = c_1 c_2 \ldots c_m$, waarbij c_i paarsgewijs disjuncte cykels zijn van lengte n_i, met $i = 1, 2, \ldots, m$. Als we de actie van $\langle \sigma \rangle$ op T definiëren als $t_i^\sigma = t_{\sigma(i)}$ voor $i = \{1, \ldots, n\}$, zien we dat deze actie de verzameling T in m banen verdeelt, waarbij elke baan correspondeert met een disjuncte cykel c_i. We noteren deze banen als $S_i \subseteq T$ met $i \in \{1, \ldots, m\}$. Neem een vaste $i \in \{1, \ldots, m\}$ en stel dat $c_i = (j_1, j_2, \ldots, j_{n_i})$, dan is $S_i = \{t_{j_1}, t_{j_2}, \ldots, t_{n_i}\}$. Het is duidelijk dat

$$\sigma(j_k) = c_i(j_k) = \begin{cases} j_i \text{ als } k = n_i - 1 \\ j_{k+1} \text{ anders} \end{cases}.$$

Dit gebruiken we om het volgende product te vereenvoudigen:

$$\prod_{k=1}^{n_i} \pi(t_{j_k} g t_{\sigma(j_k)}^{-1}) = \pi(t_{j_1} g t_{j_2}^{-1}) \pi(t_{j_2} g t_{j_3}^{-1}) \ldots \pi(t_{j_{n_i - 1}} g t_{j_1}^{-1}) = \pi(t_{j_1} g^{n_i} t_{j_1}^{-1}).$$

We zien dat $s_i^{-1} g^{n_i} s_i \in H$ aangezien dit het product is van elementen uit H. We gebruiken nu het feit dat de bannen S_i een partitie vormen van T om te besluiten dat $n_1 + \cdots + n_m = n$ en dat

$$\nu(g) = \prod_{i=1}^{n} \pi(t_i g t_{\sigma(i)}^{-1}) = \prod_{i=1}^{m} \prod_{t_j \in S_i} \pi(t_j g t_{\sigma(j)}^{-1}) = \prod_{i=1}^{m} \pi(s_i g^{n_i} s_i^{-1}).$$

■

Lemma 1.1.8. *Zij G een groep zodat het centrum $Z(G)$ een deelgroep is van eindige index n. Voor elke twee elementen $g, h \in G$ geldt dat $(gh)^n = g^n h^n$. Met andere woorden dat $\cdot^n : G \to Z(G), g \mapsto g^n$ een morfisme is.*

Bewijs. Aangezien $Z(G)$ abels is, zien we dat $[Z(G), Z(G)] = \{1\}$, zodat de canonieke projectie $\pi : Z(G) \to Z(G)/[Z(G), Z(G)]$ de identieke afbeelding is. Uit Lemma 1.1.7 volgt dat er een $m \in \mathbb{N}^*$, getallen n_i met $\sum_{i=1}^{m} n_i = n$ en een deelverzameling $\{t_1, \ldots, t_m\}$ van een transversaal van $Z(G)$ bestaan zodat

$$\nu(g) = \nu(g) = \prod_{i=1}^{m} \pi(t_i g^{n_i} t_i^{-1}) = \prod_{i=1}^{m} t_i g^{n_i} t_i^{-1}.$$

We zagen ook dat voor elke $i \in \{1, \ldots, m\}$ het element $t_i g^{n_i} t_i^{-1} \in Z(G)$, zodat $g^{n_1} \in Z(G)$ omdat $Z(G)$ een normaaldeler van G is. Aangezien $g^{n_i} \in Z(G)$ geldt dat $t_i g^{n_i} t_i^{-1} = g^{n_i}$. Dit zorgt dat we $\nu(g)$ kunnen uitwerken als

$$\nu(g) = \prod_{i=1}^{m} t_i g^{n_i} t_i^{-1} = \prod_{i=1}^{m} g^{n_i} = g^{n_1 + \cdots + n_m} = g^n.$$

Het gestelde volgt nu uit het feit dat $\nu(g) = g^n$ en dat $\nu : G \to Z(G)$ een morfisme is. ■

We definiëren een deelverzameling van G die van groot belang zal zijn in zowel de stelling van Passman als de stelling van Connel in Hoofdstuk 2.

Definitie 1.1.9. Zij G een groep, dan noteren we de deelverzameling van alle elementen van G waarvan de centralisator een eindige index heeft in G als

$$\triangle(G) = \{g \in G \mid [G : C_G(g)] < \infty\}.$$

Notatie 1.1.10. Zij G een groep.

(i) We noteren de baan van een element $x \in G$ onder toevoeging als

$$x^G = \{x^g \mid g \in G\}.$$

(ii) Zij $A \subseteq G$ een deelverzameling van G, dan noteren we

$$A^{-1} = \{a^{-1} \mid a \in A\}.$$

Opmerking 1.1.11. Zij G een groep, dan zien we via de baan stabilisator formule dat

$$\triangle(G) = \{x \mid \left|x^G\right| < \infty\}.$$

De deelverzameling $\triangle(G)$ bestaat dus uit alle elementen van G die een eindige toevoegingsklasse hebben.

Lemma 1.1.12. *Zij G een groep, dan is $\triangle(G)$ een karakteristieke deelgroep.*

Bewijs. We bewijzen eerst dat $\triangle(G)$ een deelgroep is. Aangezien $G = C_G(1)$, is $1 \in \triangle(G)$. Stel dat $x, y \in \triangle(G)$, dan zien we dat $(xy^{-1})^g = x^g(y^g)^{-1}$ met $g \in G$. Dit geeft ons het volgende:

$$\begin{aligned}(xy^{-1})^G &\subseteq x^G(y^G)^{-1},\\ \left|(xy^{-1})^G\right| &\leq \left|x^G\right|\left|(y^G)^{-1}\right| < +\infty,\end{aligned}$$

zodat $xy^{-1} \in \triangle(G)$. Volgens het criterium voor deelgroepen is $\triangle(G)$ een deelgroep. We bewijzen nu dat $\triangle(G)$ een karakteristieke deelgroep is. Zij α een automorfisme van G, dan zien we gemakkelijk dat er voor elke $x \in G$ geldt dat:

$$\begin{aligned}\alpha(x)^G &= \alpha(x)^{\alpha(G)} = \alpha(x^G),\\ \left|\alpha(x)^G\right| &= \left|\alpha(x^G)\right| = \left|x^G\right|\end{aligned}$$

zodat

$$x \in \triangle(G) \quad \text{als en slechts als} \quad \alpha(x) \in \triangle(G).$$

Dit bewijst het gestelde. ■

Opmerking 1.1.13. Zij G een groep en H_1 en H_2 deelgroepen van G met eindige index, dan geldt

$$[G : H_1 \cap H_2] \leq [G : H_1][G : H_2].$$

De volgende stelling van Dietzman zal ons enorm helpen in de context van de deelgroep $\triangle(G)$.

Stelling 1.1.14 (Dietzman)**.** *Zij G een groep en $X \subseteq G$ een eindige deelverzameling die gesloten is onder toevoeging. Als er een n bestaat zodat $x^n = 1$ voor alle $x \in X$, dan is $\langle X\rangle$ een eindige deelgroep van G.*

Bewijs. Zij $S = \langle X\rangle$ en $s \in S$. Aangezien $x^{-1} = x^{n-1}$ voor elke $x \in X$ is s een eindig product van elementen uit X. We zullen bewijzen dat $s = \prod_{x\in X} x^k, 1 \leq k \leq n-1$, zodat $|S| \leq (n-1)\,|X|$. Stel dat

$$s = x_1x_2 \dots x_{l-1}xx_{l+1} \dots x_m.$$

We hervormen dit tot

$$\begin{aligned}s &= x(x^{-1}x_1x)(x_2xx^{-1}) \dots (x^{-1}x_{l-1}x)x_{l+1} \dots x_m\\ &= xx_1'x_2' \dots x_{l-1}'x_{l+1} \dots x_m.\end{aligned}$$

Bij de laatste stap hebben we gebruik gemaakt van het feit dat X gesloten is onder toevoeging. We hebben dus een x in de uitdrukking van s succesvol naar voor gebracht, zonder de lengte van die uitdrukking te veranderen. We zien dat wanneer we dit herhaaldelijk toepassen, we s kunnen hervormen tot een woord van de vorm $s = \prod_{x\in X} x^k, 1 \leq k \leq n-1$. ■

Lemma 1.1.15. *Stel dat G een torsievrije groep is waarvoor $\triangle(G) = G$, dan is G abels.*

Bewijs. Zij $x, y \in G = \triangle(G)$ en $S = \langle x, y\rangle$. We zien dat $Z(S) = C_G(x) \cap C_G(y)$ een eindige index heeft in G en dus ook in S. Zij $n := [Z(S) : S]$, dan is $s^n \in Z(S)$ voor elke $s \in S$ (Lemma 1.1.8). Specifiek is $[x, y]^n = [x^n, y^n] = 1$, zodat $[x, y] = 1$, aangezien G torsievrij is. We hebben nu bewezen dat $[x, y] = 1$ voor willekeurige $x, y \in G$, zodat G abels is. ■

Definitie 1.1.16.

$$\triangle^+(G) = \{x \in G \mid x \in \triangle(G) \text{ en er bestaat een } n \in \mathbb{N} \text{ zodat } x^n = 1\}$$

Lemma 1.1.17. *Zij G een groep dan is $\triangle^+(G)$ uit Definitie 1.1.16 een karakteristieke deelgroep van G.*

Bewijs. We hebben al bewezen dat $\triangle(G)$ een karakteristieke deelgroep is van G in Lemma 1.1.12. Dit samen met het feit dat elk automorfisme de orde van een element bewaart, geeft ons reeds dat $\triangle^+(G)$ invariant is onder elk automorfisme van G. We hoeven dus enkel te bewijzen dat $\triangle^+(G)$ een deelgroep is. We zullen bewijzen dat $xy^{-1} \in \triangle^+(G)$ voor alle $x, y \in \triangle^+(G)$. We weten al dat $\triangle(G)$ een groep is, zodat we enkel nog hoeven te bewijzen dat xy^{-1} een eindige orde heeft. Stel dat $n_x, n_y \in \mathbb{N}$ zodat $x^{n_x} = 1 = y^{n_y}$. Aangezien $x, y \in \triangle(G)$ is, zijn x^G en y^G eindig. We zien nu dat $x^G \cup y^G$ eindig is en dat voor alle $z \in x^G \cup y^G$ geldt dat $z^{n_x n_y} = 1$. We passen nu Stelling 1.1.14 toe, en bekomen dat $\langle x^G \cup y^G \rangle$ een eindige deelgroep is van G, zodat $xy^{-1} \in \langle x^G \cup y^G \rangle$ eindige orde heeft. Dit geeft ons dat $xy^{-1} \in \triangle^+(G)$, zodat $\triangle^+(G)$ een deelgroep is. We merkten al op dat $\triangle^+(G)$ invariant is onder automorfismen van G, zodat we kunnen besluiten dat $\triangle^+(G)$ een karakteristieke deelgroep is van G. ■

We geven nog een lemma over $\triangle^+(G)$ die van pas zal komen om de stelling van Connel in Hoofdstuk 2 te bewijzen.

Lemma 1.1.18. *Zij G een groep. Voor elke $x \in \triangle^+(G)$ is er een eindige normaaldeler $N \trianglelefteq G$ met $x \in N$.*

Bewijs. We zullen dit via de stelling van Dietzman bewijzen. Stel $x \in \triangle^+(G)$, dan is x^G een eindige verzameling met $y^n = 1$ voor elke $y \in x^G$, waarbij $n = |x|$. We kunnen dus Stelling 1.1.14 toepassen op $N := \langle x^G \rangle$. Dit geeft ons dat N eindig is. We zien dat

$$N = \{x^{h_1} x^{h_2} \dots x^{h_m} \mid m \in \mathbb{N} \text{ en } \{h_1, h_2 \dots, h_m\} \subseteq G\},$$

waaruit volgt dat $N^g = N$ voor elke $g \in G$, zodat N een normaaldeler is. ■

1.2 Bi-geordende groepen

Definitie 1.2.1. Een groep G noemen we een **bi-geordende groep** als er een totale orde $\leq$ bestaat op G waarvoor $g < h$ impliceert dat $zg < zh$ en $gz < hz$ voor elke $z \in G$. De orde $\leq$ noemen we een **bi-orde** van G.

Notatie 1.2.2. Zij G een bi-geordende groep. Wanneer we $g \leq h$ noteren, bedoelen we telkens de orde $\leq$ waarvoor de eigenschappen uit Definitie 1.2.1 gelden.

We geven eerst een aantal sterke eigenschappen die direct volgen uit de definitie van een bi-geordende groep.

Lemma 1.2.3. *Zij G een bi-geordende groep, dan gelden de volgende eigenschappen voor $g, g', h, h' \in G$ en $n \in \mathbb{N}^*$:*

(i) zij $g < h$ en $g' < h'$, dan is $gg' < hh'$;

(ii) zij $g^n = h^n$, dan is $g = h$.

Bewijs. (i) Stel dat $g < h$ en $g' < h'$, dan is $gg' < hg'$ en $hg' < hh'$, zodat $gg' < hg' < hh'$.
(ii) Stel dat $g \neq h$, dan kunnen we zonder verlies van algemeenheid stellen dat $g < h$. We kunnen eigenschap (i) herhaaldelijk toepassen om $g^n < h^n$ te bekomen, een contradictie. ■

Uit het vorig lemma volgt dat bi-geordende groepen torsievrij zijn. Omgekeerd is niet elke torsievrije groep G bi-geordend.

Voorbeeld 1.2.4. De groep $G = \langle a, b \mid a^2 = b^2 \rangle$ is torsievrij. Het is duidelijk dat Lemma 1.2.3(ii) niet geldt, zodat G niet bi-geordend is.

We zullen wel bewijzen dat elke torsievrije abelse groep G bi-geordend is.

Definitie 1.2.5. Zij G een bi-geordende groep. De **positieve kegel** van G is de verzameling

$$P(G) = \{x \in G \mid 1 < x\}.$$

We geven enkele eigenschappen van een positieve kegel.

Lemma 1.2.6. *Zij G een bi-geordende groep en $P := P(G)$ de positieve kegel van G. Dan geldt:*

(i) de positieve kegel P is gesloten onder vermenigvuldiging;

(ii) de groep G is de disjuncte unie $G = P \cup P^{-1} \cup \{1\}$;

(iii) de positieve kegel P is gesloten onder toevoeging in G.

Bewijs. (i) Zij $x, y \in P$, dan is $1 < x$ en $1 < y$, zodat we Lemma 1.2.3 kunnen toepassen om te bekomen dat $1 < xy$, zodat $xy \in P$.
(ii) We zullen bewijzen dat $P^{-1} = \{x \in G \mid x < 1\}$. Het gestelde volgt dan uit het feit dat $\leq$ een totale orde is op G. Stel dat $x \in P^{-1}$, dan is $x^{-1} \in P$. Aangezien $x \neq 1$, is $x < 1$ of $1 < x$, omdat $\leq$ een totale orde is. Stel dat $1 < x$, dan is $x \in P$. Maar dan is ook $x^{-1} \in P$, zodat we (i) kunnen toepassen, wat ons $xx^{-1} = 1 \in P$ zou geven, een contradictie.
(iii) Zij $x \in P$, dan hebben we $1 < x$. We passen toe dat G een bi-geordende groep is en vermenigvuldigen links met g^{-1} en rechts met g, voor een willekeurige $g \in G$, dan bekomen we dat $1 < g^{-1}xg$, zodat $g^{-1}xg \in P$. ■

We tonen nu aan dat G een bi-geordende verzameling is als G een deelverzameling heeft die aan de eigenschappen van Lemma 1.2.6 voldoet.

Lemma 1.2.7. *Zij G een groep en $P \subseteq G$ een deelverzameling waarvoor geldt:*

(i) P is gesloten onder vermenigvuldiging;

(ii) de groep G is de disjuncte unie $G = P \cup P^{-1} \cup \{1\}$;

(iii) P is gesloten onder toevoeging in G.

Dan bepaalt de orde $\leq$, gedefinieerd door $x < y$ als $yx^{-1} \in P$, een bi-orde op G met positieve kegel P.

Bewijs. Aangezien G gelijk is aan de disjuncte unie $G \overset{\text{(ii)}}{=} P \cup P^{-1} \cup \{1\}$, zien we dat

$$yx^{-1} \in G = P \cup P^{-1} \cup \{1\}$$

voor elke $x, y \in G$. Dit geeft ons dat alle elementen vergelijkbaar zijn met $\leq$, aangezien voor willekeurige $x, y \in G$ geldt dat

$$yx^{-1} \in P \qquad \text{of } (yx^{-1})^{-1} \in P \qquad \text{of } yx^{-1} = 1,$$

zodat $x < y$ of $y < x$ of $x = y$. Om te bewijzen dat $\leq$ een totale orde is hoeven we enkel nog te bewijzen dat $a < b < c$ impliceert dat $a < c$. Dit volgt uit het feit dat P gesloten is onder vermenigvuldiging (i). Namelijk uit $a < b$ volgt dat $ba^{-1} \in P$ en uit $b < c$ volgt dat cb^{-1}, zodat ook $ca^{-1} = (cb^{-1})(ba^{-1}) \in P$, dus $a < c$. We bewijzen nu dat de orde invariant is onder linker vermenigvuldiging. Stel $x < y$ zodat $yx^{-1} \in P$. Als we (iii) toepassen zien we dat

$$gyx^{-1}g^{-1} = (gy)(gx)^{-1} \in P,$$

zodat $gx < gy$ voor elke $g \in G$. We zien ook snel dat $\leq$ invariant is onder rechter vermenigvuldiging. Stel opnieuw dat $x < y$ zodat $yx^{-1} \in P$, dan is ook $xg < yg$ voor elke $g \in G$ aangezien $(yg)(xg)^{-1} = yx^{-1} \in P$. ■

De volgende stelling is een belangrijk resultaat voor abelse groepen. We zullen namelijk bewijzen dat abelse groepen een bi-orde hebben als en slechts als ze torsievrij zijn. Deze stelling maakt gebruik van het keuzeaxioma in de vorm van Zorn's lemma. Aangezien we abelse groepen beschouwen, zullen we de groepsoperatie additief noteren.

Stelling 1.2.8 (Levi, [Lev42])**.** *Zij G een torsievrije abelse groep, dan is G een bi-geordende groep.*

Bewijs. We trachten dit te bewijzen door een verzameling P te vinden die aan de condities van Lemma 1.2.7 voldoet. Merk op dat aangezien G abels is, de derde conditie (iii) uit Lemma 1.2.7 voor elke deelverzameling van G voldaan is. We zoeken een verzameling P, zodat $G = P \cup -P$ en $P \cap -P = \{0\}$ en zodat P gesloten is onder additie. Als we zo een verzameling P vinden dan voldoet $P' = P \setminus \{0\}$ aan de condities van Lemma 1.2.7, zodat het gestelde volgt.
We definiëren een verzameling $\mathcal{S}$ van deelverzamelingen van G als volgt:

$$\mathcal{S} := \{P \subseteq G \mid P + P = P \text{ en } P \cap -P = \{0\}\}.$$

Deze verzameling is niet ledig aangezien $\{0\} \in \mathcal{S}$. De inclusie $\subseteq$ is een partiële orde op $\mathcal{S}$ en elke ketting $\{P_i \in \mathcal{S} \mid i \in I\}$ heeft de bovengrens $\bigcup_{i \in I} P_i$. We kunnen dus Zorn's lemma toepassen zodat we een maximaal element P hebben van $\mathcal{S}$. Merk op dat elk element in $\mathcal{S}$, dus ook P gesloten is onder additie en dat $P \cap -P = \{0\}$. We hoeven dus enkel aan te tonen dat $G = P \cup -P$. Dit zullen we in twee stappen doen:

(i) voor elke $x \in G$ geldt dat, als $kx \in P$ voor een bepaalde $k \in \mathbb{N}^*$, dan is $x \in P$;

(ii) voor elke $x \in G$ geldt dat $x \in P$ of $-x \in P$.

Merk op dat (ii) equivalent is aan $G = P \cup -P$.

(i) We tonen aan dat

$$P = \{x \in G \mid kx \in P \text{ voor een bepaalde } k \in \mathbb{N}^*\}.$$

Stel $Q := \{x \in G \mid kx \in P \text{ voor een bepaalde } k \in \mathbb{N}^*\}$, dan is $P \subseteq Q$. Als we kunnen bewijzen dat $Q \in \mathcal{S}$, dan is $P = Q$ aangezien P maximaal is in $\mathcal{S}$. Zij $x, y \in Q$, dan is

$k_1x, k_2y \in P$ voor bepaalde $k_1, k_2 \in \mathbb{N}^*$, zodat ook $k_1k_2(x+y) \in P$, en dus $x+y \in Q$. De verzameling Q is dus gesloten onder additie. Stel nu dat $x \in Q \cap -Q$, dan is $k_1x \in P$ en $-k_2x \in P$ voor bepaalde $k_1, k_2 \in \mathbb{N}^*$, zodat zowel $-k_1k_2x \in P$ en $k_1k_2x \in P$, zodat $k_1k_2x = 0$. Dit geeft ons $x = 0$ omdat G torsievrij is. We hebben dus $Q + Q = Q$ en $Q \cap -Q = \{0\}$, zodat $Q \in \mathcal{S}$, wat ons $P = Q$ geeft en (i) bewijst.

(ii) Stel dat $-x \notin P$, we zullen bewijzen dat $x \in P$ door aan te tonen dat

$$P = P_x := \{y + nx \mid y \in P \text{ en } n \in \mathbb{N}\}.$$

Dit doen we opnieuw door na te gaan dat $P_x \in \mathcal{S}$, wat $P = P_x$ oplevert, aangezien $P \subseteq P_x$ en P maximaal is in $\mathcal{S}$. We bewijzen eerst dat P_x gesloten is onder additie. Stel dat $y_i \in P$ en $n_i \in \mathbb{N}$ met $i \in \{1, 2\}$, dan is

$$(y_1 + n_1x) + (y_2 + n_2x) = (y_1 + y_2) + (n_1{+}_2)x \in P_x,$$

omdat $y_1 + y_2 \in P$ en $n_1 + n_2 \in \mathbb{N}$. Kies nu $y \in P_x \cap -P_x$, dan is

$$\begin{aligned} y_1 + n_1x &= -(y_2 + n_2x) = y, \\ (y_1 + y_2) &= -(n_1 + n_2)x. \end{aligned}$$

Aan de linkerkant hebben we $y_1 + y_2 \in P$, maar aangezien $-x \notin P$, hebben we wegens (i) dat $n(-x) \notin P$ voor elke $n \in \mathbb{N}^*$, zodat

$$y_1 + y_2 = n_1 + n_2 = 0.$$

Aangezien $n_1, n_2 \in \mathbb{N}$ en $n_1 + n_2 = 0$, is $n_1 = n_2 = 0$. Er geldt ook dat $y_1 = -y_2 \in P \cap -P = \{0\}$, zodat $y = y_1 + n_1x = 0$. We hebben dus bewezen dat $P_x + P_x = P_x$ en $P_x \cap -P_x = \{0\}$, zodat $P_x \in \mathcal{S}$ en dus $P = P_x$; specifiek is $x \in P$.

Er bestaat dus een deelverzameling $P \subseteq G$ van G zodat $P+P = P$, $P \cup P = G$ en $P \cap -P = \{0\}$. We zien dat de verzameling $P' := P \setminus \{0\}$ voldoet aan de condities van Lemma 1.2.7, zodat G een bi-geordende groep is. ■

1.3 Groepringen

In deze sectie zullen we groepringen bespreken in het algemeen bespreken. We definiëren de belangrijke begrippen. In de volgende hoofdstukken zullen we dan specifieker gaan kijken naar groepringen van eindige en torsievrije groepen.

Definitie 1.3.1. Stel dat G een groep is en R een ring is, dan is de **groepring *RG*** de verzameling van eindige lineaire combinaties

$$\left\{ \sum_{g \in G} r_g g \mid r_g \in R, \text{ met slechts een eindig aantal } r_g \neq 0 \right\}$$

waar de operaties $(+, \cdot) : RG \times RG \to RG$ gedefinieerd zijn als:

$$\begin{aligned} \sum_{g \in G} r_g g + \sum_{h \in G} r'_h h &= \sum_{g \in G} (r_g + r'_g) g; \\ \sum_{g \in G} r_g g \cdot \sum_{h \in G} r'_h h &= \sum_{g,h \in G} (r_{g \cdot_R} r'_h)(g \cdot_G h). \end{aligned}$$

Merk op dat we elk element $g \in G$ kunnen identificeren met $1_R g \in RG$ en elk element $r \in R$ met $r1_g \in RG$. Vanaf nu zullen we dus ook verwijzen naar elementen van G en R als elementen van RG, dus $G, R \subseteq RG$. We voeren ook het begrip **support** in voor elementen $\alpha \in RG$:

$$\alpha = \sum_{g \in G} r_g g \qquad\qquad \text{supp}(\alpha) = \{g \in G | r_g \neq 0\}.$$

Merk op dat $\text{supp}(\alpha)$ telkens een eindige verzameling is. We zien dat $\alpha = \sum_{g \in \text{supp}(\alpha)} r_g g$. Het is duidelijk dat de groepring RG een additieve groep is met neutraal element 0. We zien ook dat 1 het neutraal element is van de vermenigvuldiging in RG en dat RG een vrij linker R-moduul is.

Opmerking 1.3.2. Het is duidelijk dat RG een commutatieve ring is als en slechts als R commutatief is en G abels is.

Opmerking 1.3.3. Groepringen RG hebben een universele eigenschap, namelijk dat voor elk ringmorfisme $\phi : R \to S$ en elk groepsmorfisme $\psi : G \to \mathcal{U}(S)$ er een uniek ringmorfisme $\pi : RG \to S$ bestaat dat zowel ϕ als ψ uitbreidt. Dit morfisme is gedefinieerd als

$$\pi(\sum_{g \in G} a_g g) = \sum_{g \in G} \phi(a_g)\psi(g).$$

Definitie 1.3.4. Als K een veld is, zien we dat KG de vectorruimte over K is met basis G. De groepring KG wordt dan ook een **groepalgebra** genoemd.

Voorbeeld 1.3.5. (i) Als C_n de cyclische groep van orde n is, dan is $RC_n \cong \frac{R[x]}{(x^n - 1)}$.

(ii) Als $\mathbb{Z}$ de ring van de gehele getallen is, dan is $R\mathbb{Z} \cong R[x, x^{-1}]$.

Opmerking 1.3.6. We zullen soms voor de duidelijkheid groepringen noteren als $R[G]$.

Lemma 1.3.7. *Stel dat R een commutatieve ring is en dat G, H groepen zijn, dan geldt*

$$R[G \times H] \cong RG \otimes RH.$$

Bewijs. Beide $R[G \times H]$ en $RG \otimes RH$ zijn vrije R-modules met basissen $\{(g, h) \mid g \in G, h \in H\}$ en $\{g \otimes h \mid g \in G, h \in H\}$ respectievelijk. Dit betekent dat we de bijectie $(g, h) \mapsto g \otimes h$ tussen de basissen R-lineair kunnen uitbreiden tot een isomorfisme. Het is makkelijk te controleren dat deze afbeelding ook multiplicatief is, zodat $R[G \times H] \cong RG \otimes RH$. ■

Lemma 1.3.8. *Als A een algebra over een commutatieve ring R is, dan geldt dat $A \otimes RG \cong AG$.*

Bewijs. We kunnen elk element van $A \otimes RG$ schrijven als

$$a \otimes \sum_{g \in G} r_g g = \sum_{g \in G} (r_g a \otimes g),$$

waarbij $a \in A$ en $\sum_{g \in G} r_g g \in RG$. Als $a_g := r_g a \in A$, dan zien we dat de afbeelding

$$A \otimes RG \to AG, a \otimes \sum_{g \in G} r_g g \mapsto \sum_{g \in G} a_g g$$

een multiplicatief isomorfisme is. ■

Gevolg 1.3.9. *Stel dat R een commutatieve ring is en dat G, H groepen zijn, dan geldt*

$$R[G \times H] \cong RG[H].$$

Bewijs. Dit volgt rechtstreeks uit Lemma 1.3.7 en Lemma 1.3.8. ■

Definitie 1.3.10. Stel dat R een ring is.

(i) Als a een element van R is zodat er een $x \in R$ bestaat met $ax = 0$ (resp. $xa = 0$), dan noemen we a een **linker nuldeler** (resp. **rechter nuldeler**). Een element dat ofwel een linker ofwel een rechter nuldeler is, noemen we een **nuldeler**.

(ii) Als $a \in R$ zodat er een $x \in R$ bestaat zodat $ax = 1$ (resp. $xa = 1$) dan noemen we a een **linker eenheid** (resp. **rechter eenheid**). Een element dat zowel een linker als rechter eenheid is, noemen we een **eenheid**.

Opmerking 1.3.11. We zullen ook verwijzen naar linker (resp. rechter) eenheden als links (resp. rechts) inverteerbare elementen. Eenheden zelf noemen we dan inverteerbaar.

Tot slot definiëren we de eenheidsgroep van een groepring. Dit begrip zal van groot belang zijn in deze thesis.

Definitie 1.3.12. Zij R een ring dan noemen we de volgende deelverzameling **de eenheidsgroep van R**:

$$\mathcal{U}(R) = \{a \in R \mid \exists b \in R \text{ zodat } ab = ba = 1\}.$$

Het is duidelijk dat dit een deelgroep van $(R, \cdot)$ is. Specifiek voor een groepring RG zien we dat $\{rg \in RG \mid g \in G, r \in \mathcal{U}(R)\} \subseteq \mathcal{U}(RG)$ aangezien de elementen rg als inverse $r^{-1}g^{-1}$ hebben. Dit soort eenheden noemen we **triviale eenheden**.

1.3.1 De augmentatieafbeelding

Definitie 1.3.13. Als RG een groepring is, dan definiëren we de **augmentatieafbeelding ω** als de afbeelding $\omega : RG \to R, \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g$.

Lemma 1.3.14. *De augmentatieafbeelding is het R-lineair ringmorfisme dat elk element $g \in G \subseteq RG$ naar 1 stuurt.*

Bewijs. Het is duidelijk dat $\omega(g) = 1$ voor alle $g \in G$. We moeten enkel nog aantonen dat $\omega(\alpha\beta) = \omega(\alpha)\omega(\beta)$ voor $\alpha, \beta \in RG$. Stel dat

$$\alpha = \sum_{g\in G} r_g g, \qquad \beta = \sum_{h\in G} r'_h h.$$

We berekenen $\omega(\alpha\beta)$:

$$\begin{aligned}\omega\left(\sum_{g\in G} r_g g \cdot \sum_{h\in G} r'_h h\right) &= \omega\left(\sum_{g,h\in G} r_g r'_h (gh)\right) = \sum_{g,h\in G} r_g r'_h \\ &= \sum_{g\in G} r_g \cdot \sum_{h\in G} r'_h = \omega(\sum_{g\in G} r_g g)\omega(\sum_{h\in G} r'_h h).\end{aligned}$$

■

Aangezien deze afbeelding een ringmorfisme is, hebben we dat $\omega : \mathcal{U}(RG) \to \mathcal{U}(R)$. Dit zullen we vaak gebruiken als nodige voorwaarde voor een eenheid in RG. We kunnen de augmentatieafbeelding als volgt veralgemenen voor elke normaaldeler N van G als volgt.

Definitie 1.3.15. Als R een ring is en G een groep met normaaldeler $N \trianglelefteq G$, dan definiëren we de **augmentatieafbeelding ω_N modulo N** als de afbeelding

$$\omega_N : RG \to R[G/N], \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g gN.$$

We zien gemakkelijk dat ω_N een ringmorfisme is en dat ω_G overeenkomt met ω.
Aan de hand van de augmentatieafbeelding kunnen we ook een deelgroep van de eenheidsgroep $\mathcal{U}(RG)$ van een groepring definiëren.

Definitie 1.3.16. Zij RG een groepring en $\mathcal{U}(RG)$ de eenheidsgroep. We noemen een eenheid $\alpha \in \mathcal{U}(RG)$ **genormaliseerd** als $\omega(\alpha) = 1$, waarbij ω de augmentatieafbeelding is. We noteren de verzameling van alle genormaliseerde eenheden als

$$\mathcal{V}(RG) = \{\alpha \in \mathcal{U}(RG) \mid \omega(\alpha) = 1\}.$$

Lemma 1.3.17. *Zij G een groep en R een commutatieve ring, dan geldt voor de eenheidsgroep $\mathcal{U}(RG)$ dat*

$$\mathcal{U}(RG) \cong \mathcal{U}(R) \times \mathcal{V}(RG)\,.$$

Bewijs. Zij $u \in \mathcal{U}(RG)$, dan is $\omega(u) \in \mathcal{U}(R)$ en $\omega(u)^{-1}u \in \mathcal{V}(RG)$, zodat $(\omega(u), \omega(u)^{-1}u) \in \mathcal{U}(R) \times \mathcal{V}(RG)$. Het gestelde volgt nu uit het volgende morfisme en zijn inverse.

$$\phi : \mathcal{U}(RG) \to \mathcal{U}(R) \times \mathcal{V}(RG)\,, u \mapsto (\omega(u), \omega(u)^{-1}u)$$
$$\phi^{-1} : \mathcal{U}(R) \times \mathcal{V}(RG) \to \mathcal{U}(RG)\,, (r, v) \mapsto rv$$

■

Voorbeeld 1.3.18. Voor de integrale groepring $\mathbb{Z}G$ van een groep G geldt dat

$$\mathcal{U}(\mathbb{Z}G) \cong \mathcal{V}(\mathbb{Z}G) \times C_2.$$

We zien dus dat $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{V}(\mathbb{Z}G)$. We zullen vaak eigenschappen bewijzen voor $\mathcal{V}(\mathbb{Z}G)$, maar deze vertalen zich dus gemakkelijk naar eigenschappen van $\mathcal{U}(\mathbb{Z}G)$.

1.4 Ordes

In deze sectie bespreken we kort ordes van eindig dimensionale $\mathbb{Q}$-algebra's. Deze zullen een rol spelen in het laatste deel over cut groepen. Het feit dat $\mathbb{Z}G$ een orde is van $\mathbb{Q}G$ kunnen we uitbuiten om via $\mathbb{Q}G$ info te verkrijgen over $\mathbb{Z}G$. Het boek *Maximal ordes* van Irving Reiner [Rei75] is een standaardwerk voor de theorie van ordes.

Definitie 1.4.1. Zij A een eindig dimensionale $\mathbb{Q}$-algebra en $\mathcal{O}$ een deelring van A. We noemen $\mathcal{O}$ een orde in A als de volgende eigenschappen gelden:

(i) $\mathcal{O}$ bevat een basis van A als $\mathbb{Q}$-algebra;

(ii) $\mathcal{O}$ is een eindig voortgebracht $\mathbb{Z}$-deelmoduul van A.

Opmerking 1.4.2. Zij A een eindig dimensionale $\mathbb{Q}$-algebra. Dan bestaat er altijd minstens één maximale orde (met betrekking tot $\subseteq$) van A, zie [Rei75] Sectie 10.

We geven een aantal belangrijke voorbeelden.

Voorbeeld 1.4.3. Zij A en B eindig dimensionale $\mathbb{Q}$-algebra's.

(i) Als $\mathcal{O}_A$ een orde is in A en $\mathcal{O}_B$ een orde in B, dan is $\mathcal{O}_A \times \mathcal{O}_B$ een orde in $A \times B$.

(ii) Als $\mathcal{O}$ een orde is van A, dan is $M_n(\mathcal{O})$ een orde in $M_n(A)$, waarbij $n \in \mathbb{N}$.

(iii) Zij G een eindige groep, dan is $\mathbb{Z}G$ een orde in $\mathbb{Q}G$.

Herinner dat een getallenveld een eindige velduitbreiding van $\mathbb{Q}$ is. De volgende stelling zal van groot belang zijn.

Stelling 1.4.4 (Eenheidstelling van Dirichlet)**.** *Zij F een getallenveld en $\mathcal{O}$ een orde in F. Stel dat F, r reële inbeddingen heeft en s paren complexe inbeddingen heeft, dan is*

$$\mathcal{U}(\mathcal{O}_F) = T \times A,$$

waarbij T de eindige cyclische groep is van de eenheidswortels uit F en A een vrije abelse groep van rang $r + s - 1$ is.

Zonder bewijs. ■

In het specifieke geval dat $\mathcal{U}(\mathcal{O})$ eindig is, is er een interessant gevolg van dit resultaat.

Gevolg 1.4.5. *Zij F een getallenveld en $\mathcal{O}$ een orde in F. Als $\mathcal{U}(\mathcal{O})$ eindig is, dan is*

$$F \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-d})\},$$

waarbij $d \in \mathbb{N}^*$.

Bewijs. We zagen dat $\mathcal{U}(\mathcal{O}) = T \times A$, waarbij T de eindige cyclische groep is en A een vrije abelse groep van rang $r + s - 1$. Aangezien $\mathcal{U}(\mathcal{O})$ eindig is, zien we dat $r + s - 1 = 0$. Dit geeft ons dat ofwel $r = 1$ en $s = 0$, ofwel $s = 1$ en $r = 0$. In het eerste geval zien we dat F slechts één reële inbedding heeft en geen complexe, zodat $F = \mathbb{Q}$. In het tweede geval heeft F slechts één paar complexe inbeddingen en geen reële, zodat $F = \mathbb{Q}(\sqrt{-d})$, met $d \in \mathbb{N}^*$. ■

Lemma 1.4.6. *Zij A een eindig dimensionale $\mathbb{Q}$-algebra en $\mathcal{O}$ een orde in A. Voor elke orde $\mathcal{O}'$ in A bestaat er een $r \in \mathbb{Z}$ zodat $r\mathcal{O}' \subseteq \mathcal{O}$.*

Bewijs. We weten dat $\mathcal{O}'$ eindig voortgebracht wordt als $\mathbb{Z}$-moduul. Stel dat $\{a_1, \ldots, a_n\}$ een voortbrengende verzameling is van $\mathcal{O}'$. De orde $\mathcal{O}$ bevat een basis van A als $\mathbb{Q}$-algebra. Elke generator a_i van $\mathcal{O}'$ is dus een lineaire combinatie van elementen uit $\mathcal{O}$ met coëfficiënten in $\mathbb{Q}$. Voor elke generator bestaat er dus een $s_i \in \mathbb{Z}$ zodat $s_i a_i \in \mathcal{O}$. We zien nu dat als $s := \prod_i^n s_i$, dan $sa_i \in \mathcal{O}$ voor elke $i \in \{1, \ldots, n\}$. Natuurlijk is nu ook $s\mathcal{O}' \subseteq \mathcal{O}$. ■

Lemma 1.4.7. *Zij A een eindig dimensionale $\mathbb{Q}$-algebra, B een $\mathbb{Q}$-deelalgebra van A en zij $\mathcal{O}, \mathcal{O}'$ ordes van A. Dan gelden de volgende uitspraken:eindig dimensionale $\mathbb{Q}$-algebra's.*

(i) de doorsnede $\mathcal{O} \cap \mathcal{O}'$ is een orde in A;

(ii) de doorsnede $\mathcal{O} \cap B$ is een orde in B.

Bewijs. (i) Het is duidelijk dat $\mathcal{O} \cap \mathcal{O}'$ een eindig voortgebracht $\mathbb{Z}$-deelmoduul is van A en een deelring is van A. We hoeven dus enkel te bewijzen dat $\mathcal{O} \cap \mathcal{O}'$ een basis van A bevat als $\mathbb{Q}$-algebra. Uit het vorig lemma volgt dat er een $s \in \mathbb{Z}$ bestaat zodat $s\mathcal{O}' \subseteq \mathcal{O} \cap \mathcal{O}'$. Het is duidelijk dat $s\mathcal{O}'$ een basis van A bevat als $\mathbb{Q}$-algebra, zodat hetzelfde geldt voor $\mathcal{O} \cap \mathcal{O}'$. Dit bewijst dat $\mathcal{O} \cap \mathcal{O}'$ een orde is van A.
(ii) Het is duidelijk dat $\mathcal{O} \cap B$ een deelring is van B en dat $\mathcal{O} \cap B$ een eindig voortgebracht $\mathbb{Z}$-deelmoduul van B is. De deelalgebra B heeft een eindige basis. Als we dezelfde redenering toepassen als in Lemma 1.4.6, dan vinden we een $r \in \mathbb{Z}$ zodat $rB \subseteq \mathcal{O}$. Dit maakt het duidelijk dat $\mathcal{O} \cap B$ een basis van B als $\mathbb{Q}$-algebra bevat. Dit bewijst dat $\mathcal{O} \cap B$ een orde in B is. ■

Gevolg 1.4.8. *Zij A een eindig dimensionale $\mathbb{Q}$-algebra en zij $\mathcal{O}$ een orde in A. Dan is het centrum $Z(\mathcal{O})$ een orde in $Z(A)$.*

Bewijs. We bewijzen dat $Z(A) \cap \mathcal{O} = Z(\mathcal{O})$. Het gestelde volgt dan uit Lemma 1.4.7. Het is duidelijk dat $Z(A) \cap \mathcal{O} \subseteq Z(\mathcal{O})$. Stel dat $a \in Z(\mathcal{O})$, dan commuteert a met een basis van A als $\mathbb{Q}$-algebra, zodat $a \in Z(A)$. Dit bewijst de omgekeerde inclusie, zodat $Z(A) \cap \mathcal{O} = Z(\mathcal{O})$. ■

Stelling 1.4.9. *Zij A een eindig dimensionale $\mathbb{Q}$-algebra en $\mathcal{O}, \mathcal{O}'$ ordes van A. Dan heeft $\mathcal{U}(\mathcal{O} \cap \mathcal{O}')$ een eindige index in $\mathcal{O}$.*

Bewijs. Wegens Lemma 1.4.7 is $\mathcal{O} \cap \mathcal{O}'$ een orde in A. We kunnen er dus vanuit gaan dat $\mathcal{O}' \subseteq \mathcal{O}$. Er bestaat volgens Lemma 1.4.6 een r zodat $r\mathcal{O} \subseteq \mathcal{O}'$. Merk op dat $\mathcal{O}/r\mathcal{O}$ een eindig voortgebracht torsie $\mathbb{Z}$-moduul is, zodat $\mathcal{O}/r\mathcal{O}$ eindig is. Stel dat $x, y \in \mathcal{U}(\mathcal{O})$ en $x \equiv y \mod r\mathcal{O}$. We zien dat $x - y \in r\mathcal{O}$, zodat $xy^{-1} - 1 \in r\mathcal{O} \subseteq \mathcal{O}'$. Hieruit volgt dat $xy^{-1} \in \mathcal{O}' \cap \mathcal{U}(\mathcal{O}) \subseteq \mathcal{O}'$. Uit $x \equiv y \mod r\mathcal{O}$ volgt dus dat $x \in y\mathcal{U}(\mathcal{O}')$, zodat

$$[\mathcal{U}(\mathcal{O}) : \mathcal{O}'] \leq [\mathcal{O} : r\mathcal{O}] < +\infty.$$

Wat het gestelde bewijst. ■

1.5 Karakters

In deze sectie bespreken we kort karakter. We gaan ervan uit dat de lezer enige voorkennis van representatie theorie heeft. In de context van deze thesis, is [Hup13] Hoofdstuk V aan te raden.

Definitie 1.5.1. Zij G een eindige groep.

(i) Een **representatie van G** is een groepsmorfisme $\rho : G \to \mathrm{GL}(V)$, waarbij V een n-dimensionale $\mathbb{C}$-vectorruimte is.

(ii) Als ρ een representatie is van G, dan definiëren we het **karakter van ρ** als de afbeelding

$$\chi : G \to \mathbb{C}, g \mapsto \mathrm{sp}(\rho(g)).$$

De verzameling karakters van G noteren we als $\mathrm{Kar}(G)$.

Definitie 1.5.2. Zij G een eindige groep. Een representatie $\rho : G \to \mathrm{GL}_n(V)$ noemen we **irreducibel** als er geen deelruimte $W \leq V$ bestaat zodat $W^{\rho(g)} = W$ voor alle $g \in G$. Het karakter van een irreducibele representatie noemen we ook irreducibel. De verzameling van irreducibele representaties van een groep zullen we noteren als $\mathrm{Irr}(G)$. We zullen ook misbruik maken van deze notatie en $\chi \in \mathrm{Irr}(G)$ noteren voor een karakter χ wanneer χ irreducibel is.

Opmerking 1.5.3. Voor een irreducibel karakters χ is de representatie uniek bepaald. We zullen dus in dit geval vaak spreken over de representatie van een karakter.

Stelling 1.5.4 (Maschke)**.** *Zij G een eindige groep en zij F een veld van karakteristiek q. Als $q \nmid |G|$, dan is de groepalgebra FG semisimpel.*

Zonder bewijs. Zie [Lan05], Hoofdstuk XVIII Stelling 1.2. ∎

Stelling 1.5.5 (Artin-Wedderburn)**.** *Zij A een eindig-dimensionale algebra. Als A semisimpel is, dan bestaat er een $k \in \mathbb{N}$ zodat*

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k),$$

waarbij D_i een lichaam is voor elke $i \in \{1, \ldots, k\}$.

Deze uitdrukking van een semisimpele algebra als direct product van matrixringen noemt men ook de Wedderburn-decompositie.

Opmerking 1.5.6 ([Hup13] Hoofdstuk V Stelling 4.5.). Zij G een eindige groep. Wegens de stelling van Maschke geeft is de groepalgebra $\mathbb{Q}G$ semisimpel is. er geldt dus dat

$$\mathbb{Q}G \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

Men kan bewijzen dat $k = |\mathrm{Irr}(G)|$. In het geval van $\mathbb{C}G$ geldt zelfs dat

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C}).$$

Zij F een deelveld van $\mathbb{C}$, met decompositie $F \cong \prod_{i=1}^{k} M_{n_i}(D_i)$. Stel dat $\rho \in \mathrm{Irr}(G)$, dan geldt er dat

$$\rho(FG) \cong M_{n_j}(D_j), \qquad \ker(\rho) = \prod_{\substack{i=1,\\ i\neq j}}^{k} M_{n_i}(D_i),$$

$$FG \cong \prod_{\rho \in \mathrm{Irr}(G)} \rho(FG).$$

Op die manier verkrijgen we de Wedderburn decompositie uit de irreducibele karakters. Er is dus een 1 op 1 relatie tussen de componenten van de Wedderburn-decompositie en de irreducibele representaties van G. Aangezien er ook een 1 op 1 relatie is tussen de irreducibele karakters en de representaties zullen we voor een irreducibel karakter χ ook spreken van het component gelinkt aan χ.

Lemma 1.5.7. *Zij G een eindige groep. De volgende uitspraken gelden voor elk karakter χ van G.*

(i) Als $g \sim h$, dan is $\chi(g) = \chi(h)$.

(ii) $\chi(g^{-1}) = \overline{\chi(g)}$.

Zonder bewijs. [Hup13] Hoofdstuk V Stelling 5.9. ■

Notatie 1.5.8. Zij G een eindige groep en R een ring.

(i) Zij $g, h \in G$. Als er een $x \in G$ bestaat waarvoor $x^{-1}gx = h$, dan noteren we dit als $g \sim h$.

(ii) Zij $u, v \in RG$. Als er een $\alpha \in \mathcal{U}(RG)$ bestaat waarvoor $\alpha^{-1}u\alpha = v$, dan noteren we dit als $u \sim_R v$.

We breiden deze definities uit voor deelverzamelingen $H, H' \leq \mathcal{V}(RG)$. We noteren $H \sim_R H'$ wanneer er een $\alpha \in \mathcal{U}(RG)$ bestaat zodat $\alpha^{-1}H\alpha = H'$.

1.5.1 Het karakterveld

We definiëren een specifieke velduitbreiding voor een veld gegeven een karakter van een groep. We zullen zien dat deze natuurlijk opduikt in de Wedderburn-decompositie.

Definitie 1.5.9. Zij G een eindige groep en F een veld. Voor elk karakter χ van G definiëren we het **karakterveld,** $\mathbb{Q}(\boldsymbol{\chi})$ als de kleinste velduitbreiding van $\mathbb{Q}$ die alle karakterwaarden $\chi(g)$ bevat, namelijk

$$\mathbb{Q}(\chi) := \mathbb{Q}(\chi(g) \mid g \in G).$$

Lemma 1.5.10. *Zij G een groep van orde n. Dan is voor elk karakter χ het karakterveld $\mathbb{Q}(\chi)$ een deelveld van $\mathbb{Q}(\zeta)$, met ζ een primitieve n-de eenheidswortel.*

Bewijs. Zij χ het karakter van de representatie $\rho : G \to GL_k(\mathbb{C})$. Voor elke $g \in G$ is $g^n = 1$, zodat $\rho(g)^n = \rho(g^n) = \rho(1) = I_k$. We zien dus dat $\rho(g)$ een matrix is van eindige orde. Dit geeft ons dat $\rho(g)$ diagonaliseerbaar is, zodat $\rho(g) = P^{-1}DP$, met D een diagonaalmatrix. Stel dat

$$D = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_k \end{pmatrix},$$

dan zijn $\{\lambda_1, \ldots, \lambda_k\}$ precies de eigenwaarden van $\rho(g)$. Aangezien

$$\rho(g)^n = (P^{-1}DP)^n = P^{-1}D^nP = I_k,$$

zien we dat $D^n = I_k$. We zien dat het i-de diagonaal element van D^n juist λ_i^n is zodat $D^n = I_k$ ons $\lambda_i^n = 1$ voor elke $i \in \{1, \ldots, k\}$ geeft. Aangezien $\chi(g)$ de som van deze λ_i is, zien we dat $\mathbb{Q}(\chi(g)) \leq \mathbb{Q}(\zeta)$. Aangezien g en χ willekeurig waren, geldt dat $\mathbb{Q}(\chi) \leq \mathbb{Q}(\zeta)$. ■

Als gevolg van dit lemma zien we dat $\mathbb{Q}(\chi)/\mathbb{Q}$ een Galois-uitbreiding is.

Gevolg 1.5.11. *Zij G een eindige groep van orde n, ζ een primitieve n-de eenheidswortel en χ een karakter van G. De volgende uitspraken gelden:*

(i) de velduitbreiding $\mathbb{Q}(\chi)/\mathbb{Q}$ is een Galois-uitbreiding;

(ii) elk automorfisme $\sigma_\chi \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ kan uitgebreid worden tot een automorfisme

$$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Bewijs. Uit het vorig lemma volgt dat $\mathbb{Q} \leq \mathbb{Q}(\chi) \leq \mathbb{Q}(\zeta)$. Omdat de Galoisgroep van $\mathbb{Q}(\zeta)/\mathbb{Q}$ abels is ([Lan05] Hoofdstuk VI, Stelling 3.1), zien we via de hoofdstelling van de Galoistheorie dat $\mathbb{Q}'/\mathbb{Q}$ een Galois-uitbreiding is voor elk tussenveld $\mathbb{Q} \leq \mathbb{Q}' \leq \mathbb{Q}(\zeta)$. Specifiek is dus ook $\mathbb{Q}(\chi)/\mathbb{Q}$ een Galois-uitbreiding. De tweede eigenschap volgt nu uit de eerste en uit het feit dat $\mathbb{Q}(\chi)$ een tussenveld is van $\mathbb{Q}$ en $\mathbb{Q}(\zeta)$. ■

Opmerking 1.5.12. Zij χ een irreducibel karakter van een eindige groep G en $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. Dan is $\chi^\sigma := \sigma \circ \chi$ ook een irreducibel karakter van G.

Lemma 1.5.13. *Zij G een eindige groep en*

$$\mathbb{Q}G \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

de Wedderburn-decompositie van $\mathbb{Q}G$. Zij χ een irreducibel karakter van G en $M_{n_i}(D_i)$ het component gelinkt aan χ. Dan is het karakterveld $\mathbb{Q}(\chi)$ gelijk aan het centrum $Z(D_i)$, namelijk

$$\mathbb{Q}(\chi) = Z(D_i).$$

Bewijs. We bewijzen eerst dat $Z(D_i) \subseteq \mathbb{Q}(\chi)$. Zij ρ de representatie van χ, dan is $\rho(\mathbb{Q}G) = M_{n_i}(D_i)$. Stel dat $z \in Z(D_i)$, dan is $\rho(\alpha) = zI_{n_i}$ voor een zekere $\alpha \in \mathbb{Q}G$. Er geldt dat $\chi(\alpha) = nz$, zodat $z \in \frac{1}{n}\chi(\alpha)$. Zij $\alpha = \sum_{g\in G} a_g g$, dan is $\chi(\alpha) = \sum_{g\in G} a_g \chi(g)$ want χ is lineair, zodat $\chi(\alpha) \in \mathbb{Q}(\chi)$ en bijgevolg ook $z \in \mathbb{Q}(\chi)$. Dit bewijst dat $Z(D_i) \subseteq \mathbb{Q}(\chi)$. Om de omgekeerde inclusie te bewijzen, beschouwen we voor een willekeurige $x \in G$, het element $\tilde{x} := \sum_{g\in x^G} x^g \in \mathbb{Q}G$. Het is duidelijk dat $\tilde{x}^g = \tilde{x}$ voor elke $g \in G$, zodat $\tilde{x}$ commuteert met heel G, en bijgevolg met heel de groepalgebra $\mathbb{Q}G$, waaruit volgt dat $\tilde{x} \in Z(\mathbb{Q}G)$. Hieruit volgt dat $\rho(\tilde{x}) \in Z(M_{n_i}(D_i))$, zodat $\rho(\tilde{x}) = zI_{n_i}$ voor een $z \in Z(D_i)$. We zien dat $\chi(\tilde{x}) = n_i z$. Herinner dat toegevoegde elementen in G hetzelfde beeld onder een karakter hebben, zodat $\chi(\tilde{x}) = \left|x^G\right| \chi(x)$. Dit geeft ons dat $\left|x^G\right| \chi(x) = n_i z$, zodat $\chi(x) = \frac{n_i}{|x^G|} z \in Z(D_i)$, wat ons de inclusie $\mathbb{Q}(\chi(x)) \subseteq Z(D_i)$ geeft. Aangezien $x \in G$ willekeurig gekozen was, zien we dat $\mathbb{Q}(\chi) \subseteq Z(D_i)$, zodat beide inclusies bewezen zijn en we $\mathbb{Q}(\chi) = Z(D_i)$ bekomen.

■

We voeren eerst een aantal begrippen in die we nodig zullen hebben om de orthogonaliteit stelling van Schur te bewijzen.

Definitie 1.5.14. Zij χ en ψ twee karakters van een eindige groep G.

(i) Voor elke $g \in G$ definiëren we de afbeelding

$$T_g : \mathrm{Kar}(G) \to \mathbb{C},\ \chi \mapsto \chi(g).$$

Merk op dat voor $g \sim h$ de afbeeldingen T_g en T_h samenvallen.

(ii) We definiëren het inproduct tussen twee karakters als

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g\in G} \chi(g)\overline{\psi(g)}.$$

(iii) We definiëren het inproduct tussen twee afbeeldingen T_g, T_h als

$$\langle T_g, T_h \rangle = \frac{1}{|h^G|} \sum_{\chi\in \mathrm{Irr}(G)} T_g(\chi) T_h(\overline{\chi}).$$

We geven nu een zeer gekend resultaat binnen de karaktertheorie, namelijk Schur's orthogonale relaties.

Stelling 1.5.15 (Schur). *Zij χ en ψ irreducibele karakters van G, dan geldt dat*

$$\langle \chi, \psi \rangle = \begin{cases} 1 & \text{als } \chi = \psi, \\ 0 & \text{anders.} \end{cases}, \qquad \langle T_g, T_h \rangle = \begin{cases} 1 & \text{als } g \sim h, \\ 0 & \text{anders.} \end{cases}$$

Bewijs. Zie bijvoorbeeld [Hup13] Hoofdstuk V Stelling 5.8. ■

Gevolg 1.5.16. *Zij G een eindige groep.*

(i) De irreducibele karakters van G zijn lineair onafhankelijk.

(ii) De afbeeldingen T_g zijn lineair onafhankelijk, met $g \in G$.

Bewijs. Stel dat $\sum_{\chi \in \mathrm{Irr}(G)} \lambda_\chi \chi = 0$ met $\lambda_\chi \in \mathbb{C}$. Beschouw voor elke $\chi \in \mathrm{Irr}(G)$ het inproduct

$$0 = \langle 0, \chi \rangle = \langle \sum_{\chi \in \mathrm{Irr}(G)} \lambda_\chi \chi, \chi \rangle = \lambda_\chi \langle \chi, \chi \rangle = \lambda_\chi.$$

We zien dan dat alle coëfficiënten λ_χ gelijk aan nul zijn, wat de lineaire onafhankelijkheid bewijst. Het bewijs voor de lineaire onafhankelijkheid van de afbeeldingen T_g is volledig analoog. ■

Lemma 1.5.17 ([MS84]). *Zij G een eindige groep. Als $F \leq K$ twee oneindig grote velden zijn, dan zijn $\alpha, \beta \in FG$ toegevoegd in FG als en slechts als ze toegevoegd zijn in KG.*

Bewijs. We zullen enkel de niet-triviale implicatie bewijzen, namelijk

$$\alpha \sim_K \beta \implies \alpha \sim_F \beta.$$

We zoeken dus een eenheid $u \in \mathcal{U}(FG)$ zodat $u^{-1}\alpha u = \beta$. We zoeken eerst een element u waarvoor $\alpha u = u\beta$. Stel dat $G = \{g_1, \ldots, g_n\}$, dan is elke $u \in FG$ te schrijven als $u = \sum_1^n r_i g_i$. Nu levert de vergelijking $\alpha u - u\beta = 0$ het volgende stelsel van lineaire vergelijkingen:

$$MX = 0, \qquad M \in M_n(F), \qquad X = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n.$$

Aangezien $M \in M_n(F)$ bestaan er l onafhankelijke vectoren $\{v_1, \ldots, v_l\} \subseteq F^n$ zodat elke oplossing $X \in F^n$ (respectievelijk $X \in K^n$) een lineaire combinatie van $v_1, \ldots, v_l$ is, met coëfficiënten in F (respectievelijk K). We weten dat $1 \leq l$ omdat uit het gegeven volgt dat er een $u' \in \mathcal{U}(KG)$ bestaat zodat $\alpha u' = u'\beta$. Het feit dat $1 \leq l$ geeft dus dat er een elementen $u \in FG$ bestaat zodat $\alpha u = u\beta$. We hoeven enkel nog zo'n element te vinden dat ook inverteerbaar is. Aangezien FG een eindig dimensionale algebra is, weten we dat elk element ofwel een eenheid of een nuldeler is. Zij ρ de reguliere representatie van G en $\rho(X) := x_1\rho(g_1) + \cdots + x_n\rho(g_n)$, voor $X = (x_1, \ldots, x_n)^T \in K^n$. We zien dat $u = x_1 g_1 + \cdots + x_n g_n \in KG$ een nuldeler is als en slechts als $\det \rho(X) = 0$. Een oplossing $u \in KG$ van $\alpha u = u\beta$ is telkens van de vorm $u = x_1 g_1 + \cdots + x_n g_n$ met $X = s_1 v_1 + \cdots + s_l v_l$ waarbij $s_i \in K$. Zo'n oplossing is een nuldeler als

$$\phi(s_1, \ldots, s_l) := \det\left(s_1\rho(v_1) + \cdots + s_l\rho(v_l)\right) = 0.$$

Het is duidelijk dat $\phi(s_1, \ldots, s_l)$ een n-de-graadspolynoom is met coëfficiënten in F aangezien $\rho(v_i) \in M_n(F)$ voor elke i. We weten dat niet elk coëfficiënt nul is aangezien het gegeven ons een inverteerbaar element $v \in \mathcal{U}(KG)$ geeft waarvoor $\alpha v = v\beta$. Omdat F een oneindig veld is, en ϕ een niet-nulpolynoom is, zullen er $r_1, \ldots, r_l$ bestaan waarvoor $\phi(r_1, \ldots, r_l) \neq 0$. Dit geeft ons een $u \in FG$ waarvoor $\alpha u = u\beta$ die geen nuldeler is. Deze u is inverteerbaar, zodat $u^{-1}\alpha u = \beta$. We zien dus dat $\alpha \sim_F \beta$, hetgeen we wouden bewijzen. ■

Lemma 1.5.18. *Zij G een eindige groep en zij $u, v \in \mathcal{U}(\mathbb{Z}G)$. De eenheden u en v zijn rationeel toegevoegd aan elkaar als en slechts als $\rho(u)$ en $\rho(v)$ toegevoegd zijn voor elke irreducibele complexe representatie ρ.*

Bewijs. We beschouwen de Wedderburn decompositie van $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$ en we weten dat

$$\Phi := \prod_{\rho \in \mathrm{Irr}(G)} \rho,\ x \mapsto \rho_1(x) \times \cdots \times \rho_k(x),$$

een expliciet isomorfisme is, waarbij $\{\rho_1, \ldots, \rho_k\} = \mathrm{Irr}(G)$. Veronderstel dat $u \sim_{\mathbb{Q}} v$ voor $u, v \in \mathcal{U}(\mathbb{Z}G)$. Dan is ook $u \sim_{\mathbb{C}} v$. Dit betekent dat $\Phi(u)$ en $\Phi(v)$ ook toegevoegd zijn aan elkaar, zodat voor elke irreducibele complexe representatie ρ geldt dat $\rho(u)$ en $\rho(v)$ toegevoegd zijn. Omgekeerd veronderstellen we nu dat voor elke irreducibele complexe representatie ρ geldt dat $\rho(u)$ en $\rho(v)$ toegevoegd zijn. Zij M_ρ het element waarvoor $M_\rho^{-1}\rho(u)M_\rho = \rho(v)$. Dan zien we dat

$$M^{-1}\Phi(u)M = \Phi(v) \qquad \text{waarbij } M := M_{\rho_1} \times \cdots \times M_{\rho_k},$$

zodat $(\Phi^{-1}(M))^{-1}u(\Phi^{-1}(M)) = v$. We zien dus dat $u \sim_{\mathbb{C}} v$. Uit Lemma 1.5.17 volgt dat

$$u \sim_{\mathbb{Q}} v,$$

hetgeen we wouden bewijzen. ■

2 Groepringen van torsievrije groepen

In dit hoofdstuk werpen we een blik op groepringen van groepen die torsievrij zijn. Deze situatie is helemaal anders dan wanneer de groep eindig is. Men ziet dit al direct aan het feit dat men geen wedderburn-decompositie heeft. Dit hoofdstuk zal korter zijn en eerder dienen als referentie om de theorie van groepringen van torsievrije groepen en eindige groepen te vergelijken. We zullen ons voornamelijk richten op de Kaplansky problemen. Dit zijn een aantal problemen rondom de structuur van een groepalgebra KG waarbij G torsievrij is en K een veld. We sommen de problemen op en geven de onderlinge verbanden ertussen. Voor dit hoofdstuk heeft men een basiskennis ringtheorie nodig, zie bijvoorbeeld [Lam01].

2.1 De Kaplansky problemen

Probleem 2.1.1 (Idempotenten). Zij G een torsievrije groep en K een veld. Bevat de groepalgebra KG enkel triviale idempotenten?

Probleem 2.1.2 (Nuldeler). Zij G een torsievrije groep en K een veld. Is KG een domein?

Probleem 2.1.3 (Eenheden). Zij G een torsievrije groep en K een veld. Heeft de groepalgebra KG enkel triviale eenheden, zodat

$$\mathcal{U}(KG) = \{\lambda g \mid \lambda \in K, g \in G\}?$$

Probleem 2.1.4 (Semisimpel). Zij G een torsievrije groep en K een veld. Is de groepalgebra KG semisimpel, i.e. $J(KG) = \{0\}$?

Deze problemen worden toegekend aan Kaplansky. Hij vermoedde een positief antwoord op deze problemen. Men spreekt daarom ook over de Kaplansly vermoedens, de bekendste zijnde het eenhedenvermoeden en het nuldelervermoeden. Deze verschenen samen in [Kap70]. Wij verwoorden het als problemen aangezien er al tegenvoorbeelden gevonden zijn voor de meeste problemen. Recent vond Gilles Gardam in [Gar21] een tegenvoorbeeld voor het eenhedenprobleem. Het nuldelervermoeden is nog steeds open.

Stelling 2.1.5. *Zij G een torsievrije groep en K een veld. Dan zijn de Kaplansky problemen als volgt verbonden:*

$$2.1.4 \impliedby 2.1.3 \implies 2.1.2 \implies 2.1.1.$$

Merk op dat de implicatie tussen nuldelers en idempotenten triviaal is. Als $e \in KG$ een idempotent is, dan volgt namelijk dat $e(1-e) = 0$, zodat een niet-triviaal idempotent het toelaat een niet-triviale nuldeler te vormen. We zullen eerst aantonen dat als KG enkel triviale eenheden heeft, de algebra dan ook semisimpel is.

Stelling 2.1.6. *Zij G een torsievrije groep en K een veld. Als de groepalgebra KG geen niet-triviale eenheden heeft dan is $J(KG) = \{0\}$, i.e. KG is semisimpel.*

Bewijs. Stel dat $\alpha \in J(KG)$, dan is $1 - r\alpha s$ inverteerbaar voor alle $r, s \in KG$. Volgens onze aanname is elke eenheid triviaal, zodat voor alle $r, s \in KG$ het element $1 - r\alpha s$ van de vorm λg met $\lambda \in K^*$ en $g \in G$. We passen dit toe en bekomen het volgende:

$$\begin{aligned} &1 - \alpha = \lambda g; \\ &1 - \alpha g = \mu h, && \text{waarbij } g, h \in G \text{ en } \lambda, \mu \in K^*, \end{aligned}$$

zodat

$$1 - (1 - \lambda g)g = 1 - g + \lambda g^2 = \mu h.$$

We zien dat h een lineaire combinatie is van $\{1, g, g^2\}$ met coëfficiënten in K^*. Aangezien $g, h \in G$ basiselementen zijn, zien we dat $1 = g = h$ en $\lambda = 1$, zodat $\alpha = 0$. Hieruit volgt dat $J(KG) = \{0\}$, hetgeen we wouden bewijzen. ■

Om de implicatie tussen het eenhedenprobleem en het nuldelerprobleem te bewijzen, zullen we nog een aantal lemma's nodig hebben. Herinner dat we bewezen dat elke bi-geordende groep G torsievrij is. We zullen bewijzen dat voor deze soort torsievrije groepen de Kaplansky problemen een positief antwoord hebben.

Stelling 2.1.7. *Zij G een bi-geordende groep en K een veld dan is de groepalgebra RG een domein en alle eenheden zijn triviaal.*

Bewijs. Zij $\alpha, \beta \in RG \backslash \{0\}$ en stel dat $\operatorname{supp}(\alpha) = \{g_1, g_2, \ldots, g_m\}$ en $\operatorname{supp}(\beta) = \{h_1, h_2, \ldots, h_n\}$ zodat

$$\begin{aligned} \alpha &= \sum_{i=1}^{m} a_i g_i && g_1 < g_2 < \cdots < g_m \\ \beta &= \sum_{i=1}^{n} b_i h_i && h_1 < h_2 < \cdots < h_n. \end{aligned}$$

Toepassen dat $\leq$ een bi-orde is op G geeft dat $g_1 h_1 \leq g_i h_j \leq g_m h_n$ voor $i \in \{1, \ldots, m\}$ en $j \in \{1, \ldots, n\}$. Specifiek zien we dat $g_1 h_1 = g_i h_j$ als en slechts als $i = j = 1$, zodat de coëfficiënt van $g_1 h_1$ in $\alpha\beta$ gelijk is aan $a_1 b_1 \neq 0$. Dit bewijst dat KG een domein is. We zullen nu bewijzen dat $\mathcal{U}(KG) = \{\lambda g \mid \lambda \in K \text{ en } g \in G\}$ door aan te tonen dat, als $\alpha \in \mathcal{U}(KG)$, dan $|\operatorname{supp}(\alpha)| = 1$. Stel dat $\alpha\beta = 1$. We bewezen al dat $g_1 h_1 \in \operatorname{supp}(\alpha\beta)$. Op dezelfde manier zien we dat de coëfficiënt van $g_m h_n$ in $\alpha\beta$ gelijk is aan $a_m b_n \neq 0$, maar $\operatorname{supp}(\alpha\beta) = \operatorname{supp}(1) = \{1\}$ geeft ons dat $g_1 h_1 = g_m h_n$, zodat $m = n = 1$ en $\alpha \in \{\lambda g \mid \lambda \in K \text{ en } g \in G\}$. ■

Stelling 2.1.8. *Zij G een groep en K een veld. Als G een torsievrije abelse groep is, dan is KG een domein en is elke eenheid van de groepalgebra triviaal.*

Bewijs. Dit is het gevolg van twee stellingen die we al eerder bewezen, namelijk Stelling 1.2.8 (Levi) en Stelling 2.1.7. ■

Definitie 2.1.9. Zij G een groep en H een deelgroep van G. We definiëren de afbeelding

$$\pi_H : KG \to KH, \sum_{g \in G} r_g g \mapsto \sum_{h \in H} r_h h.$$

Lemma 2.1.10. *Zij G een groep en H een deelgroep van G. De afbeelding π_H uit Definitie 2.1.9 is een (KH, KH)-bimoduul morfisme.*

Bewijs. Om te bewijzen dat π_H een (KH, KH)-bimoduul morfisme is hoeven we enkel aan te tonen dat

$$\pi_H(\gamma_1\alpha\gamma_2) = \gamma_1\pi_H(\alpha)\gamma_2 \qquad \text{voor } \gamma_1, \gamma_2 \in KH \text{ en } \alpha \in KG.$$

Stel dat

$$\gamma_1 = \sum_{h\in H} r_h h \qquad \gamma_2 = \sum_{h\in H} r'_h h \qquad \alpha = \sum_{g\in G} a_g g.$$

Om het gestelde te bewijzen splitsen we α in twee delen $\alpha = \sum_{g\in G\setminus H} a_g g + \sum_{g\in H} a_g g$ en rekenen we het product simpelweg uit:

$$\begin{aligned}
\gamma_1\alpha\gamma_2 &= \sum_{h\in H} r_h h\Big(\sum_{g\in G\setminus H} a_g g + \sum_{g\in H} a_g g\Big)\sum_{h\in H} r'_h h \\
&= \sum_{h\in H} r_h h\Big(\sum_{g\in G\setminus H} a_g g\Big)\sum_{h'\in H} r'_{h'} h' + \sum_{h\in H} r_h h\Big(\sum_{g\in H} a_g g\Big)\sum_{h'\in H} r'_{h'} h' \\
&= \sum_{\substack{g\in G\setminus H \\ h,h'\in H}} r_h a_g r'_{h'} hgh' + \sum_{g,h,h'\in H} r_h a_g r'_{h'} hgh'.
\end{aligned}$$

Aangezien $hgh' \in G \setminus H$ voor alle $h, h' \in H$ en $g \in G \setminus H$, zien we dat

$$\pi_H(\gamma_1\alpha\gamma_2) = \sum_{g,h,h'\in H} r_h a_g r'_{h'} hgh' = \gamma_1\pi_H(\alpha)\gamma_2,$$

wat we wouden bewijzen. ■

Dit zal ons een belangrijke eigenschap over groepringen helpen te bewijzen. Namelijk dat als voor een groep H een element $\alpha \in RH$ niet inverteerbaar (respectievelijk geen nuldeler is) dat men geen "grotere groep" $G \geq H$ kan vinden zodat $\alpha \in KG$ wel inverteerbaar (respectievelijk een nuldeler) is.

Stelling 2.1.11. *Zij R een ring, G een groep en $H \leq G$ een deelgroep dan zijn de volgende uitspraken equivalent voor een element $\alpha \in RH$.*

(a) α is inverteerbaar (respectievelijk een nuldeler) in RH.

(b) α is inverteerbaar (respectievelijk een nuldeler) in RG.

Bewijs. Voor beide gevallen (inverteerbaar en nuldeler) is de richting $(a) \implies (b)$ triviaal. Namelijk als $\alpha, \beta \in RH \subseteq RG$, dan is het product $\alpha\beta \in RH \subseteq RG$ zodat α een eenheid (respectievelijk nuldeler) is in beide groepringen. Omgekeerd, stel dat α een eenheid (respectievelijk een nuldeler) is in RG. Stel dat $\beta \in RG \setminus \{0\}$ zodat $\alpha\beta = \beta\alpha = \delta$, met $\delta \in \{0, 1\}$. Als we Lemma 2.1.10 gebruiken, zien we dat

$$\begin{aligned}
\delta = \pi_H(\delta) = \pi_H(\alpha\beta) = \alpha\pi_H(\beta) \\
\delta = \pi_H(\delta) = \pi_H(\beta\alpha) = \pi_H(\beta)\alpha
\end{aligned}$$

zodat α een eenheid in RH, aangezien $\pi_H(\beta) \in RH$. We zien ook dat α een nuldeler is in RH als $\pi_H(\beta) \neq 0$. In het geval dat $\pi_H(\beta) = 0$ nemen we het element βg, waarbij $g \in G$ gekozen is zodat $1 \in \operatorname{supp}(\beta g)$ wat ervoor zorgt dat $\pi_H(\beta g) \neq 0$ en $\alpha\pi_H(\beta g) = 0$. ■

Stelling 2.1.12 (Passman). *Zij G een groep met elementen γ_1, γ_2 waarvoor $\gamma_1(RG)\gamma_2 = \{0\}$, dan is*

$$\pi_{\triangle(G)}(\gamma_1)\pi_{\triangle(G)}(\gamma_2) = 0.$$

Bewijs. We zullen de afbeelding $\pi_{\triangle(G)}$ noteren als $\pi_\triangle$. We bewijzen dat

$$\pi_\triangle(\gamma_1)\gamma_2 = 0.$$

Het gestelde volgt hieruit omdat $\pi_\triangle(\pi_\triangle(\gamma_1)\gamma_2) = \pi_\triangle(\gamma_1)\pi_\triangle(\gamma_2)$. We ontleden γ_1 als $\gamma_1 = \alpha + \beta$, waarbij

$$\begin{aligned} \alpha &= a_1 g_1 + \cdots + a_k g_k & g_1, \ldots, g_k &\in \triangle(G) \\ \beta &= b_1 g_1' + \cdots + b_r g_r' & g_1', \ldots, g_r' &\notin \triangle(G) \\ \gamma_2 &= c_1 h_1 + \cdots + c_s h_s & h_1, \ldots, h_s &\in G \end{aligned}$$

Per definitie is $\pi_\triangle(\gamma_1) = \alpha$. De deelgroep $C := \cap_{i=1}^k C_G(u_i)$ heeft een eindige index in G. Stel dat T een willekeurige transversaal is van C. Voor $x \in C$ hebben we $x^{-1}\alpha x = \alpha$, zodat $x^{-1}\alpha x\gamma_2 = \alpha\gamma_2$. Volgens het gestelde is $\gamma_1 RG\gamma_2 = \{0\}$, zodat:

$$\begin{aligned} &x^{-1}\gamma_1 x\gamma_2 \in x^{-1}(\gamma_1 RG\gamma_2) = \{0\}, \\ &x^{-1}(\alpha+\beta)x\gamma_2 = \alpha\gamma_2 + x^{-1}\beta x\gamma_2 = 0, \\ &\alpha\gamma_2 = -x^{-1}\beta x\gamma_2 = -x^{-1}(b_1 g_1' + \cdots + b_r g_r')x(c_1 h_1 + \cdots + c_s h_s). \end{aligned}$$

Stel dat $\alpha\gamma_2 \neq 0$, dan zien we dat elke $g \in \operatorname{supp}(\alpha)$ geschreven kan worden als $g = x^{-1} g_i' x h_j$ voor zekere $i \in \{1, \ldots, r\}, j \in \{1, \ldots, s\}$. Dit geeft ons dat $g h_j^{-1} = x^{-1} g_i' x$, zodat g'^x bevat is in $\operatorname{supp}(\alpha)\operatorname{supp}(\gamma_2)^{-1}$, voor elke $x \in C$. Hieruit volgt dat:

$$\begin{aligned} \left|g_i'^C\right| &\leq \left|\operatorname{supp}(\alpha)\operatorname{supp}(\gamma_2)^{-1}\right| \leq |\operatorname{supp}(\alpha)|\,|\operatorname{supp}(\gamma_2)| \leq +\infty \\ \left|g_i'^G\right| &= \left|\bigcup_{t\in T} g_i'^{Ct}\right| \leq +\infty. \end{aligned}$$

Hieruit volgt dat de baan van g_i' onder G eindig is, zodat $g_i' \in \triangle(G)$, een contradictie. ■

We geven nu een sterk resultaat van Connel. dit resultaat zal de nodige en voldoende condities geven opdat KG priem is. Herinner dat een ring R priem is als voor $a, b \in R$ het feit dat $aRb = \{0\}$ impliceert dat ofwel $a = 0$, ofwel $b = 0$.

Stelling 2.1.13 (Connel [Con63]). *Zij G een groep en K een veld. Dan zijn de volgende uitspraken equivalent:*

(a) KG is priem;

(b) $Z(KG)$ is priem;

(c) G bevat geen niet-triviale eindige normaaldelers;

(d) $\triangle^+(G) = \{1\}$.

Bewijs. $(a) \implies (b)$ Zij $\alpha, \beta \in Z(KG)$ zodat $\alpha Z(KG)\beta = \{0\}$, dan is $\alpha\beta = 0$ omdat $1 \in Z(KG)$. We beschouwen nu $\alpha KG\beta$ en passen toe dat α, β centraal zijn in KG om te zien dat

$$\alpha KG\beta = \alpha\beta KG = \{0\}.$$

Aangezien KG priem is, is $\alpha = 0$ of $\beta = 0$, zodat ook $Z(KG)$ priem is.
$(b) \implies (c)$ Stel dat $N \trianglelefteq G$ een eindige normaaldeler van G is. We zien dat $\hat{N} \in Z(KG)$ een centraal niet-nul element is van de groepring. Omdat $Z(KG)$ abels en priem is, bevat het geen nuldelers. Uit $\hat{N}^2 = \hat{N}\,|N|$ volgt er dat

$$\hat{N}(\hat{N} - |N|) = 0.$$

omdat $\hat{N}, \hat{N} - |N| \in Z(KG)$ en $Z(KG)$ geen nuldelers bevat, bekomen we $\hat{N} = |N|$. Dit is enkel mogelijk als N triviaal is.
$(c) \implies (d)$ Stel dat $x \in \triangle^+(G)$. Dan bestaat er volgens Lemma 1.1.18 een eindige normaaldeler N met $x \in N$. Eigenschap (c) eist echter dat $N = \{1\}$, zodat $x = 1$ en $\triangle^+(G) = \{1\}$.
$(d) \implies (a)$ We zullen dit bewijzen uit het ongerijmde. Stel dat $\gamma_1 KG\gamma_2 = \{0\}$ met $\gamma_1 \neq 0 \neq \gamma_2$. Aangezien beide $\gamma_i \neq 0$ kunnen we $g_i \in \mathrm{supp}(\gamma_i)$ nemen met $i \in \{1, 2\}$. Als we de elementen $\gamma_1' := g_1^{-1}\gamma_1$ en $\gamma_2' = \gamma_2 g_2^{-1}$ definiëren, zien we dat $\gamma_1' KG\gamma_2' = \{0\}$ en $1 \in \mathrm{supp}(\gamma_i')$ voor $i \in \{1, 2\}$. We kunnen de Stelling 2.1.12 (Passman) toepassen, en bekomen dat $\pi_{\triangle(G)}(\gamma_1')\pi_{\triangle(G)}(\gamma_2') = 0$. We zagen dat $1 \in \mathrm{supp}(\gamma_i')$ voor $i \in \{1, 2\}$, zodat $\pi_{\triangle(G)}(\gamma_1') \neq 0 \neq \pi_{\triangle(G)}(\gamma_2')$. De groep $\triangle(G)$ is torsievrij, aangezien $\triangle^+(G)$ triviaal is volgens (d). Aangezien ook $\triangle(\triangle(G)) = \triangle(G)$ kunnen we Lemma 1.1.15 toepassen, zodat $\triangle(G)$ abels is. We zien nu dat $\triangle(G)$ een torsievije abelse groep is. We kunnen dus Stelling 2.1.8 toepassen om te bekomen dat de groepalgebra $K\triangle(G)$ een domein is. Dit geeft echter een contradictie aangezien $\pi_{\triangle(G)}(\gamma_1'), \pi_{\triangle(G)}(\gamma_2') \in K\triangle(G)^*$, en

$$\pi_{\triangle(G)}(\gamma_1')\pi_{\triangle(G)}(\gamma_2') = 0.$$

Dit vervolledigt ons bewijs. ■

Via de stelling van Connel kunnen we makkelijk aantonen dat het eenhedenvermoeden het nuldelervermoeden impliceert.

Stelling 2.1.14. *Zij G een torsievrije groep en K een veld. Als elke eenheid van KG triviaal is, dan is de groepalgebra KG een domein.*

Bewijs. Omdat G torsievrij is, zien we gemakkelijk dat conditie (c) uit Stelling 2.1.13 voldaan is zodat KG priem is. Stel dat $\alpha, \beta \in KG^*$ en $\alpha\beta = 0$. Aangezien KG priem is, geldt dat $\beta KG\alpha \neq \{0\}$, zodat we een $\gamma \in KG$ kunnen vinden waarvoor $\beta\gamma\alpha \neq 0$. Het is duidelijk dat

$$\begin{aligned}(\beta\gamma\alpha)^2 &= \beta\gamma(\alpha\beta)\gamma\alpha = 0\\ (1 - \beta\gamma\alpha)(1 + \beta\gamma\alpha) &= 1 - (\beta\gamma\alpha)^2 = 1.\end{aligned}$$

We zien dus dat $1-\beta\gamma\alpha$ een eenheid is die volgens onze aanname van de vorm $1-\beta\gamma\alpha = \lambda g$ is, met $\lambda \in K$ en $g \in G$. Dit zou betekenen dat $\beta\gamma\alpha = 1+\lambda g$ zodat $(\beta\gamma\alpha)^2 = (1+\lambda g)^2 = 1+2\lambda g+\lambda^2 g^2$. We zagen dat $(\beta\gamma\alpha)^2 = 0$, zodat in de lineaire combinatie van basiselementen $1 + 2\lambda g + \lambda^2 g^2$ elk coëfficiënt nul moet zijn. Dit geeft ons dat $g = 1$ omdat G torsievrij is. Er geldt dus dat $(1+\lambda)^2 = 0$. Aangezien K een veld is, is $1 + \lambda = 0$, zodat $\lambda = -1$, maar dan is $\beta\gamma\alpha = 0$, een contradictie. ■

3 Groepringen van eindige groepen

In deze sectie zullen we het hebben over groepringen RG, waarbij G een groep van eindige orde is en R een ring. Hierover is al veel gekend en sommige open vragen rondom groepringen van niet noodzakelijk eindige groepen zijn relatief gemakkelijk te beantwoorden wanneer we stellen dat de groep torsie-elementen bevat, wat natuurlijk zo is bij een eindige groep. Een groot verschil is bijvoorbeeld dat we voor elke eindige deelgroep $H \leq G$ met $h \neq \{1\}$ een nuldeler kunnen vormen. We zien namelijk dat $(1-h)\sum_{h' \in H} h' = 0$ voor alle $h \in H$. Deze zijn niet-triviale nuldelers wanneer $h \neq 1$. Dit geeft ons eenheden van de vorm $1-(1-h)\sum_{h' \in H} h'$, met inverse $1+(1-h)\sum_{h' \in H} h'$. We zullen ons vooral richten op groepringen $\mathbb{Z}G$, waarbij $\mathbb{Z}$ de gehele getallen zijn. Groepringen over $\mathbb{Z}$ worden ook wel integrale groepringen genoemd. Deze sectie is vooral gebaseerd op het boek [JD15] van Eric Jespers en Angél del Rio.

3.1 Karakterisatie van integrale groepringen met enkel triviale eenheden

Het eerste grote resultaat dat we zullen bewijzen zal Stelling 3.1.20 zijn. Deze stelling geeft ons een volledige karakterisatie van de integrale groepringen met triviale eenheden.

3.1.1 Bicyclische en Basseenheden

We gaven al een kort voorbeeld van een type nuldelers waarmee we ook eenheden konden vormen. Om deze eenheden makkelijker te beschrijven, zullen we de volgende notatie invoeren.

Notatie 3.1.1. Als G een groep is met $H \leq G$ en $g \in G$, dan voeren we de volgende notatie in voor elementen van RG:

$$\hat{H} := \sum_{h \in H} h, \qquad \hat{g} := \sum_{g' \in \langle g \rangle} g',$$
$$b(h, \hat{g}) := 1 + (1-g)h\hat{g}, \qquad b(\hat{g}, h) := 1 + \hat{g}h(1-g).$$

Definitie 3.1.2. De eenheden van de vorm $b(h, \hat{g})$ en $b(h, \hat{g})$ worden de **bicyclische eenheden** genoemd en werden geïntroduceerd door Ritter en Seghal in [RS89].

Opmerking 3.1.3. We breiden de notie van een centralisator uit tot de hele groepring. Voor elke $\alpha \in RG$ hebben we dus dat

$$C_G(\alpha) = \{g \in G \mid g\alpha = \alpha g\}.$$

Lemma 3.1.4. *Zij G een eindige groep, $H \leq G$ en $g, h \in G$.*

(i) $C_G(\hat{H}) = N_G(H)$.

(ii) De eenheden $b(h, \hat{g})$ en $b(\hat{g}, h)$ zijn triviaal als en slechts als $h \in N_G(\langle g \rangle)$.

(iii) De eenheden $b(h,\hat{g})$ en $b(\hat{g},h)$ zijn torsie als en slechts als ze triviaal zijn.

Bewijs. (i) De inclusie $N_G(H) \subseteq C_G(\hat{H})$ is triviaal. Stel dat $g \in C_G(\hat{H})$, dan is $\hat{H}^g = \hat{H}$ en dus $\hat{H} - \hat{H}^g = 0$ in RG. Aangezien de elementen van G een basis vormen voor RG geldt er dat in de lineaire combinatie $\hat{H} - \hat{H}^g$ alle coëfficiënten 0 moeten zijn, of dus dat $h^g \in H$ voor alle $h \in H$. (ii) De eenheden $b(h,\hat{g})$ zijn triviaal als en slechts als $h \in C_G(1-g) \cup C_G(\hat{g})$. We zien dat $C_G(1-g) \subseteq C_G(\hat{g})$, omdat $h(1-g) = (1-g)h$ impliceert dat $hg = gh$. Dit samen met (i) geeft ons dat $b(h,\hat{g})$ triviaal is als en slechts als $h \in N_G(\langle g \rangle)$. (iii) We bewijzen enkel de niet-triviale implicatie. Stel dat $b(h,\hat{g})$ geen triviale eenheid is, dan hebben we $b(h,\hat{g})^k = (1+(1-g)h\hat{g})^k = 1 + k(1-g)h\hat{g} \neq 1$ voor elke $k \in \mathbb{Z}$. Dit geeft ons dat $b(h,\hat{g})$ een oneindige orde heeft. Het is duidelijk dat de bewijzen analoog zijn voor $b(\hat{g},h)$. ■

We hebben dus bewezen dat niet-triviale bicyclische eenheden nooit torsie zijn. Als G abels is, dan zijn alle bicyclische eenheden triviaal. In dit geval moeten niet-triviale eenheden op een andere manier geconstrueerd worden. De volgende manier is geïnspireerd op getaltheorie.

Definitie 3.1.5. Als ξ een complexe eenheidswortel is met orde $n > 1$, dan noemen we de eenheden $n_k(\xi) = \frac{\xi^k - 1}{\xi - 1} = 1 + \xi + \cdots + \xi^{k-1} \in \mathbb{Z}[\xi]$ de **cyclotomische eenheden**.

In het geval dat er een l bestaat zodat $kl \equiv 1 \mod n$, hebben we

$$n_k(\xi)^{-1} = \frac{\xi - 1}{\xi^k - 1} = \frac{\xi^{kl} - 1}{\xi^k - 1} = 1 + \xi^k + \cdots + \xi^{(l-1)k} = n_l(\xi^k).$$

Dit willen we reconstrueren in $\mathbb{Z}\langle g \rangle$, waarbij g een element is van orde $n > 1$. We noteren

$$\chi_k(g) = 1 + \cdots + g^{k-1} \in \mathbb{Z}\langle g \rangle.$$

Als $k \neq 1$, dan is dit geen inverteerbaar element aangezien $\omega(\chi_k(g)) = k$ niet inverteerbaar is in $\mathbb{Z}$. We proberen dit element aan te passen zodat het beeld onder de augmentatieafbeelding inverteerbaar is in $\mathbb{Z}$. Opnieuw stellen we dat k en n copriem zijn en dat er dus een m bestaat zodat $k^m \equiv 1 \mod n$. We definiëren het element

$$u_{k,m}(g) = \chi_k(g)^m + \frac{1 - k^m}{n}\hat{g}.$$

We zien dat $\omega(u_{k,m}(g)) = k^m + \frac{1-k^m}{n}n = 1$, maar dit bewijst niet dat $u_{k,m}(g)$ inverteerbaar is. Hiervoor zullen we nog wat werk moeten verrichten.

Opmerking 3.1.6. (i) We zien dat $r_{k,m} := \frac{1-k^m}{n}$ juist de unieke coëfficiënt is zodat

$$\omega\left(\chi_k(g)^m + r_{k,m}\hat{g}\right) = 1.$$

We zullen deze eigenschap vaak uitbuiten om te tonen dat een element $u = \chi_k(x)^m + r\hat{g}$ met $r \in \mathbb{Z}$ en $\omega(u) = 1$ gelijk moet zijn aan $u_{k,m}(g)$.

(ii) Het element $\hat{g}$ heeft de eigenschap dat $g^i\hat{g} = \hat{g}$ voor elke $i \in \mathbb{Z}$, dus is ook $u_{k,m}(g)\hat{g} \in \mathbb{Z}\hat{g}$.

Deze twee opmerkingen zullen we gebruiken om de drie vergelijkingen uit het volgend lemma te bewijzen.

Lemma 3.1.7. *Zij G een groep. Stel dat $g \in G$ een element is van orde n, zij k een element is dat copriem is met n, en dat $m \in \mathbb{N}$ zodat $k^m \equiv 1 \mod n$. Dan geldt:*

(i) $u_{k,m}(g) = u_{k',m}(g)$ *als* $k \equiv k' \mod n$*;*

(ii) $u_{k,m}(g)u_{k',m}(g^k) = u_{kk',m}(g)$*;*

(iii) $u_{k,m_1}(g)u_{k,m_2}(g) = u_{k,m_1+m_2}(g)$.

Bewijs. We bewijzen (i) door op te merken dat $\chi_{k'}(g) = \chi_{sn+k}(g) = s\hat{g} + \chi_k(g)$, aangezien $k \equiv k' \mod n$. Wanneer we dit invullen in de definitie van $u_{k',m}(g)$, verkrijgen we

$$u_{k',m}(g) = \chi_{k'}(g)^m + r_{k',m}\hat{g} = (\chi_k(g) + s\hat{g})^m + r_{k'}\hat{g} = \chi_k(g)^m + \sum_{i=0}^{m-1} \binom{m}{i} \chi_k(g)^i \hat{g}^{m-i} + r_{k'}\hat{g}.$$

We hoeven dit niet uit te rekenen, maar slechts op te merken dat $\chi_k(g)^i\hat{g}^{m-i} \in \mathbb{Z}\hat{g}$ aangezien $g^i\hat{g} = \hat{g}$ voor alle $i \in \mathbb{Z}$. Dit geeft ons dat $u_{k',m}(g) = \chi_k(g) + r\hat{g}$ met $r \in \mathbb{Z}$. Omdat het beeld onder ω gelijk is aan 1, hebben we $u_{k,m}(g) = u_{k',m}(g)$. Om (ii) te bewijzen schrijven we het product $u_{k,m}(g)u_{k',m}(g^k)$ als volgt uit

$$\begin{aligned} u_{k,m}(g)u_{k',m}(g^k) &= (\chi_k(g)^m + r_{k,m}\hat{g})(\chi_{k'}(g^k)^m + r_{k',m}\hat{g}) = (\chi_k(g)\chi_{k'}(g^k))^m + r\hat{g} \\ &= (\sum_{i=0}^{k-1} g^i \sum_{j=0}^{k'-1} g^{jk})^m + r\hat{g} = (\sum_{j=0}^{k'-1}\sum_{i=0}^{k-1} g^{jk+i})^m + r\hat{g} = (\sum_{i=0}^{kk'-1} g^i)^m + r\hat{g} \\ &= \chi_{kk'}(g)^m + r\hat{g}. \end{aligned}$$

Aangezien $\omega(\chi_{kk'}(g)^m + r\hat{g}) = \omega(u_{k,m}(g)u_{k',m}(g^k)) = 1$ hebben we $u_{k,m}(g)u_{k',m}(g^k) = u_{kk'}(g)$. Ook (iii) volgt direct wanneer we het product $u_{k,m_1}(g)u_{k,m_2}(g) = u_{k,m_1+m_2}(g)$ uitschrijven en ω toepassen. ■

Dit lemma geeft ons alles wat we nodig hebben om te bewijzen dat $u_{k,m}(g)$ inverteerbaar is. Als we even terugkijken naar de cyclotomische eenheden, dan hadden we dat $n_k(\xi)^{-1} = n_l(\xi^k)$, waarbij $lk \equiv 1 \mod n$. Daardoor lijkt $u_{l,m}(g^k)$ een goeie kandidaat als inverse voor $u_{k,m}(g)$. De volgende stelling bevestigt dit.

Stelling 3.1.8. *Stel dat g een element is van orde $n > 1$, stel dat k, m, l getallen zijn zodat $k^m \equiv 1 \mod n$ en dat $lk \equiv 1 \mod n$. Dan geldt het volgende:*

(i) de elementen $u_{k,m}(g)$ zijn inverteerbaar, met $u_{k,m}(g)^{-1} = u_{l,m}(g^k)$;

(ii) voor alle elementen van de vorm $u_{k,m}(g)$ geldt $u_{k,m}(g) = u_{k',m'}(g)^s$, waarbij $k \equiv k' \mod n$ en m' de orde is van k in $(\mathbb{Z}/n\mathbb{Z})^\times$ met $0 < k' < n$ en $m = sm'$.

Bewijs. Voor (i) gebruiken we Lemma 3.1.7 om het product $u_{k,m}(g)u_{l,m}(g^k)$ te schrijven als $u_{k,m}(g)u_{l,m}(g^k) = u_{kl,m}(g) = u_{1,m}(g) = 1$. (ii) Stel nu dat $k \equiv k' \mod n$ en stel dat m' de orde is van k in $(\mathbb{Z}/n\mathbb{Z})^\times$, met $0 < k' < n$ en $m = sm'$. Door opnieuw gebruik te maken van het vorig lemma krijgen we $u_{k,m}(g) = u_{k',m}(g) = u_{k',m'}(g)^s$. ■

Definitie 3.1.9. De eenheden van de vorm $u_{k,m}(g)$ worden de **Basseenheden** genoemd, vernoemd naar Hyman Bass [Bas66].

We zagen dat de bicyclische eenheden enkel torsie zijn wanneer ze de eenheid zelf zijn. Het volgend lemma geeft een nodige en voldoende voorwaarde opdat een Basseenheid torsie is.

Lemma 3.1.10. *Een Basseenheid $u_{k,m}(g)$ is torsie als en slechts als $k \equiv \pm 1 \mod n$.*

Bewijs. Stel dat $k \equiv \pm 1 \mod n$. Het geval $k \equiv 1 \mod n$ is triviaal aangezien we dan $u_{1,m}(g) = 1$ hebben. Stel nu dat $k \equiv -1 \mod n$, dan weten we dat $u_{k,m}(g) = (u_{n-1,2}(g))^s$ (Stelling 3.1.8). We zien dat

$$u_{n-1,2}(g) = \chi_{n-1}(g)^2 + \frac{1-(n-1)^2}{n}\hat{g} = (\hat{g} - g^{n-1})^2 + (2-n)\hat{g} = n\hat{g} - 2\hat{g} + g^{-2} + (2-n)\hat{g} = g^{-2}.$$

Dit geeft ons dat $u_{k,m}(g)$ een torsie element is wanneer $k \equiv -1 \mod n$. Stel nu dat $u_{k,m}(g)$ torsie is. Als $\xi_n \in \mathbb{C}$ de n-de eenheidswortel is, dan kunnen we het isomorfisme $\langle g \rangle \to \langle \xi_n \rangle$ uitbreiden tot een ringmorfisme $f : \mathbb{Z}\langle g \rangle \to \mathbb{C}$. Aangezien $u := u_{k,m}(g)$ torsie is, is ook $f(u)$ torsie en dus een eenheidswortel. Dan is ook $(n_k(\xi_n)) = f(u)^{\frac{1}{m}}$ een eenheidswortel. We beschouwen $1 = |n_k(\xi_n)| = \frac{|\xi^k - 1|}{|\xi - 1|}$, dus ξ^k en ξ op gelijke afstand van 1 liggen. Dit betekent dat $\xi^k = \bar{\xi}$ zodat $k \equiv \pm 1 \mod n$. ∎

3.1.2 Integrale groepringen met enkel triviale eenheden

In deze subsectie zullen we voor een aantal families van groepen bewijzen dat hun integrale groepringen enkel triviale eenheden bevatten. Later zullen we dan bewijzen dat deze de enige soorten groepen zijn waarvoor dit geldt.

Lemma 3.1.11. *Er geldt dat $\mathcal{U}(\mathbb{Z}G) = \pm G$ als en slechts als $\mathcal{U}(\mathbb{Z}[G \times C_2]) = \pm(G \times C_2)$.*

Bewijs. Als alle eenheden van $\mathbb{Z}[G \times C_2]$ triviaal zijn, dan zijn ook alle eenheden van $\mathbb{Z}G$ triviaal. Dit zien we duidelijk als we $\mathbb{Z}G$ identificeren met $\mathbb{Z}[G \times \{1\}] \subseteq \mathbb{Z}[G \times C_2]$. Omgekeerd stellen we nu dat $\mathbb{Z}G$ enkel triviale eenheden heeft. Uit Gevolg 1.3.9 volgt dat $\mathbb{Z}[G \times C_2] = \mathbb{Z}G[C_2]$. Stel dat $C_2 = \{1, x\}$, dan kunnen we elk element van $\mathbb{Z}G[C_2]$ schrijven als $ax + b$, met $a, b \in \mathbb{Z}G$. Beschouw de eenheid $ax + b$, met inverse $cx + d$. We schrijven dit product uit als

$$1 = (ax + b)(cx + d) = (ad + bc)x + (ac + bd).$$

Hieruit krijgen we dat $ac + bd = 1$ en $ad + bc = 0$. Aangezien $(a + b)(c + d) = (a - b)(c - d) = ac + bd = 1$, zijn $a+b$ en $a-b$ eenheden van $\mathbb{Z}G$. Volgens de veronderstelling zijn alle eenheden van $\mathbb{Z}G$ triviaal, dus $a+b = \pm g$ en $a-b = \pm g'$ voor bepaalde $g, g' \in G$. Als we deze twee vergelijkingen optellen, verkrijgen we dat $2a = \pm g + \pm g'$. We zien dat $g = g'$, want de coëfficiënten van $2a \in \mathbb{Z}G$ moeten even zijn. Dit geeft ons dat $a \in \{0, \pm g\}$ en $b \in \{0, \pm g\} \setminus \{a\}$, zodat $ax + b \in \{\pm gx, \pm g\}$ een triviale eenheid is in $\mathbb{Z}G[C_2]$. ∎

De volgende stelling is wellicht één van de belangrijkste binnen de theorie van integrale groepringen. We zullen deze doorheen verschillende secties nodig hebben.

Lemma 3.1.12 (Berman-Higman)**.** *Stel dat G een eindige groep is en dat a een torsie-element is van $\mathbb{Z}G$.*

(i) Als $1 \in \operatorname{supp}(a)$, dan is $a = \pm 1$.

(ii) Als a centraal is in $\mathbb{Z}G$, dan is a een triviale eenheid.

Bewijs. (i) Stel dat $|G| = n$, dan beschouwen we de links reguliere representatie $\rho_G : G \to GL_n(\mathbb{Q})$, die we uitbreiden tot een morfisme $\rho : \mathbb{Z}G \to GL_n(\mathbb{Q})$. Aangezien $a = \sum_{g\in\mathrm{supp}(a)} a_g g$ torsie is, hebben we dat $\rho(a)$ ook torsie is en bijgevolg diagonaliseerbaar is. Omdat $\rho(a)$ torsie is, zijn de eigenwaarden $\xi_1, \ldots, \xi_n$ eenheidswortels. Aangezien elke $\xi_i \in \mathbb{Q}$, geldt er dat $\xi_i = \pm 1$ voor elke $i \in \{1, \ldots, n\}$. Als we het spoor van $\rho(a)$ nemen, zien we dat

$$\mathrm{sp}(\rho(a)) \sum_{i=1}^{n} \xi_i = \sum_{g\in \mathrm{sp}\, a} a_g \,\mathrm{sp}(\rho(g)) = n a_1.$$

Aangezien $a_1 \in \mathbb{Z}$ en $\xi_i = \pm 1$, zien we dat $a_1 \in \{-1, 0, 1\}$. We hebben echter verondersteld dat $a_1 \neq 0$, zodat elke ξ_i hetzelfde teken heeft en $\rho(a) = \pm I_n$. Aangezien ρ injectief is, zien we dat $u = \pm 1$. (ii) Als a centraal is, dan zien we dat voor $g \in \mathrm{supp}(a)$, het element ag^{-1} ook torsie is. We passen (i) toe op ag^{-1} en krijgen dat $ag^{-1} = \pm 1$, zodat $a = \pm g$. ■

Gevolg 3.1.13. *Als G abels is en $\mathcal{U}(\mathbb{Z}G)$ eindig is, dan is $\mathcal{U}(\mathbb{Z}G) = \pm G$.*

Bewijs. Als G abels is, dan is ook $\mathbb{Z}G$ abels en is elk element dus centraal. Omdat $\mathcal{U}(\mathbb{Z}G)$ eindig is, is ook elke eenheid torsie, zodat we via Stelling 3.1.12 krijgen dat elke eenheid van $\mathbb{Z}G$ triviaal is. ■

De voorwaarde dat G abels is, is echter niet noodzakelijk. Dit zullen we ook later zien in Stelling 3.1.20. Het volgend lemma zal de eenheden van ringen bespreken die geen groepringen zijn. Toch zullen deze ringen ons veel kunnen helpen bij het bepalen van eenheden van groepringen.

Notatie 3.1.14. (i) We noteren het lichaam van de quaternionen over $\mathbb{R}$ als $\mathcal{H}$.

(ii) We noteren $\mathbb{Z}_{\mathcal{L}} := \{a \in \mathcal{H} \mid a = a_1 + a_i i + a_j j + a_k k, \text{ met } a_1, a_i, a_j, a_k \in \mathbb{Z}\}$. Deze worden ook wel de Lipschitz quaternionen genoemd.

Opmerking 3.1.15. We zullen niet zeer gedetailleerd zijn over $\mathcal{H}$, aangezien dit te veel zou afwijken van deze thesis. Als men verduidelijking nodig heeft, dan is het derde hoofdstuk uit [Lam04] aan te raden.

Lemma 3.1.16. *(i) De ring $\mathbb{Z}_{\mathcal{L}}$ bevat enkel de eenheden $\{\pm 1, \pm i, \pm j, \pm k\}$.*

(ii) De ring $\mathbb{Z}[i]$ bevat enkel de eenheden $\{\pm 1, \pm i\}$.

(iii) Als ξ_3 een primitieve derdemachtswortel is, dan bevat de ring $\mathbb{Z}[\xi_3]$ slechts een eindig aantal eenheden. Specifiek is $\mathcal{U}(\mathbb{Z}[\xi_3]) = \langle \xi_6 \rangle$.

Bewijs. (i) We bewijzen dit via de normafbeelding $N : \mathcal{H} \to \mathbb{R}, a \mapsto a\bar{a}$. Als $a = a_1 + a_i i + a_j j + a_k k$, dan is $N(a) = a_1^2 + a_i^2 + a_j^2 + a_k^2$. Stel dat $a \in \mathcal{U}(\mathbb{Z}_{\mathcal{L}})$. Aangezien N een morfisme is, krijgen we dat $N(a) = a_1^2 + a_i^2 + a_j^2 + a_k^2 \in \mathcal{U}(\mathbb{Z}) = \{\pm 1\}$. Elke coëfficiënt van a is een geheel getal, zodat hun kwadraat een natuurlijk getal is. De som van natuurlijke getallen is altijd positief en enkel gelijk aan 1 als één term 1 is, en de andere termen nul zijn. Stel dat $a_x^2 = 1$ voor een $x \in \{1, i, j, k\}$, dan is $a_x = \pm 1$ en zijn de andere coëfficiënten van a nul. Dit geeft ons dat $a \in \{\pm 1, \pm i, \pm j, \pm k\}$.

(ii) Dit volgt uit (i), aangezien $\mathbb{Z}[i]$ een deelring van $\mathbb{Z}_{\mathcal{L}}$ is.

(iii) Zonder verlies van algemeenheid stellen we dat $\xi_3 = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$. Aangezien $\xi_3^2 = -1 - \xi_3$ zien we dat $\{1, \xi_3\}$ een basis is voor $\mathbb{Z}[\xi_3]$. Elk element $x \in \mathbb{Z}[\xi_3]$ kunnen we dus uitdrukken als $a + b\xi_3$, met $a, b \in \mathbb{Z}$. Aangezien $x = a + b\xi_3 \in \mathbb{Z}[\xi_3] \subseteq \mathbb{C}$ kunnen we $|x|^2$ berekenen als:

$$|x|^2 = |a + b\xi_3|^2 = \left|(a - \frac{b}{2}) + \frac{\sqrt{3}b}{2}i\right|^2 = \frac{(2a-b)^2 + 3b^2}{4} = a^2 - ab + b^2 \in \mathbb{Z}. \quad (3.1)$$

We zien dat de norm van elementen uit $\mathbb{Z}[\xi_3]$ telkens een geheel getal is. Dit vertelt ons dat $\mathbb{Z}[\xi_3]$ topologisch discreet is in $\mathbb{C}$, want de afstand tussen twee elementen van $\mathbb{Z}[\xi_3]$ is steeds een natuurlijk getal. Stel nu dat $u \in \mathcal{U}(\mathbb{Z}[\xi_3])$ een eenheid is en inverse $v \in \mathcal{U}(\mathbb{Z}[\xi_3])$ heeft. We kunnen de norm $|.|$ toepassen op $uv = 1$, wat ons $|u|\,|v| = 1$ geeft. Zonder verlies van algemeenheid kunnen we stellen dat $|u|^2 \leq |u| \leq 1$. We zagen dat voor alle elementen $x \in \mathbb{Z}[\xi_3]$ geldt dat $|x|^2 \in \mathbb{Z}$, zodat voor alle eenheden $u \in \mathcal{U}(\mathbb{Z}[\xi_3])$ geldt dat $|u|^2 = |u| = 1$. Dit samen met het feit dat $\mathbb{Z}[\xi_3]$ discreet is, geeft ons al dat er slechts een eindig aantal eenheden in $\mathbb{Z}[\xi_3]$ zijn. Om te bekomen dat $\mathcal{U}(\mathbb{Z}[\xi_3]) = \langle \xi_6 \rangle$ hoeft men enkel de vergelijking $|x|^2 \overset{3.1}{=} a^2 - ab + b^2 = 1$, met $a, b \in \mathbb{Z}$ op te lossen, die $x \in \langle \xi_6 \rangle$ oplevert.

■

Notatie 3.1.17. Stel dat R een ring is en dat f_i afbeeldingen $R \to S_i$ zijn voor elke $i \in I$, waarbij I een eindige indexverzameling is. Als we $\prod_{i\in I} f_i$ noteren, dan bedoelen wij hiermee de afbeelding

$$\prod_{i\in I} f_i : R \to \prod_{i\in I} S_i, r \mapsto \prod_{i\in I}(f_i(r)).$$

De volgende stelling zal tonen dat de integrale groepring van bepaalde cyclische groepen enkel triviale eenheden bevat.

Stelling 3.1.18. *$\mathcal{U}(C_n^k) = \pm C_n^k$ voor $n \in 2, 3, 4, 6$ en $k \in \mathbb{N}$.*

Bewijs. We merken eerst op dat we de stelling slechts hoeven te bewijzen voor $n \in \{3, 4\}$. Het geval $n = 2$ volgt uit Lemma 3.1.11 en het geval $n = 6$ volgt uit het geval $n = 3$ en Lemma 3.1.11, omdat $C_6^k = C_3^k \times C_2^k$. We zullen de gevallen $n = 3$ en $n = 4$ bewijzen via inductie op k. Stel dus dat $k = 1$, en dat $n \in \{3, 4\}$, we schrijven $C_n = \langle g \rangle$. Voor elke deler d van n nemen we een vaste primitieve d-de machtswortel ξ_d. We kunnen het groepsmorfisme $C_n \to \mathcal{U}(\mathbb{C})$ bepaald door $g \mapsto \xi_d$ uitbreiden tot een ringmorfisme $\rho_d : \mathbb{Q}C_n \to \mathbb{Q}(\xi_d)$. We zien dat ρ_d surjectief is, en dat $K_d := \ker(\rho_d)$ een maximaal ideaal is van $\mathbb{Q}C_n$, want $\mathbb{Q}(\xi_d) \cong \mathbb{Q}C_n/K_d$ is een veld. Voor twee verschillende delers d, d' van n zijn ook de deelgroepen $\langle g^d \rangle$ en $\langle g^{d'} \rangle$ van C_n verschillend. Hiermee zien we dat $C_n \cap (1 + K_d) = \langle g^d \rangle \neq \langle g^{d'} \rangle = C_n \cap (1 + K_{d'})$, zodat ook $K_d \neq K_{d'}$. We kunnen de Chinese reststelling toepassen op de idealen K_d waarbij $d \mid n$, aangezien deze als verschillende maximale idealen ook copriem zijn. Dit geeft ons het volgend isomorfisme :

$$\mathbb{Q}C_n/\cap_{d|n} K_d \cong \prod_{d|n} \mathbb{Q}C_n/K_d \cong \prod_{d|n} \mathbb{Q}(\xi_d).$$

Men kan bewijzen dat $\dim_{\mathbb{Q}}(\mathbb{Q}(\xi_d)) = \phi(d)$ ([Lan05] hoofdstuk VI, stelling 3.1). Dit gebruiken we om de dimensie van $\mathbb{Q}C_n/\cap_{d|n} K_d$ als volgt te berekenen:

$$\dim\left(\mathbb{Q}C_n/\cap_{d|n} K_d\right) = \dim\left(\prod_{d|n} \mathbb{Q}(\xi_d)\right) = \sum_{d|n} \phi(d) = n = \dim\left(\mathbb{Q}C_n\right),$$

zodat $\cap_{d|n} K_d = 0$ en $\mathbb{Q}C_n \cong \prod_{d|n} \mathbb{Q}(\xi_d)$. We noteren het isomorfisme als $\rho := \prod_{d|n} \rho_d : \mathbb{Q}C_n \to \prod_{d|n} \mathbb{Q}(\xi_d)$ en zien duidelijk dat $\rho(\mathbb{Z}C_n) \subseteq \prod_{d|n} \mathbb{Z}[\xi_d]$. Als we ρ beperken tot de eenheden van $\mathbb{Z}C_n$ krijgen we dat $\rho(\mathcal{U}(\mathbb{Z}C_N)) \subseteq \prod_{d|n} \mathcal{U}(\mathbb{Z}[\xi_d])$, waarbij elke $\mathcal{U}(\mathbb{Z}[\xi_d])$ eindig is wegens Lemma 3.1.16. Omdat ρ injectief is, is ook $\mathcal{U}(\mathbb{Z}C_n)$ eindig, zodat Gevolg 3.1.13 ons geeft dat alle eenheden triviaal zijn. Dit bewijst onze inductiebasis voor $n \in \{3, 4\}$. Stel nu dat $k > 1$, dan schrijven we $C_d^k = C_d^{k-2} \times \langle g_1 \rangle \times \langle g_2 \rangle$, waarbij $|g_1| = |g_2| = d$. Stel nu dat $d = 4$, dan beschouwen we de normaaldelers

$$N_1 = \langle 1 \times g_1^2 \times 1 \rangle, \qquad N_2 = \langle 1 \times 1 \times g_2^2 \rangle, \qquad N_3 = \langle 1 \times g_1^2 \times g_2^2 \rangle.$$

Met deze normaaldelers definiëren we het morfisme

$$\omega_N := \prod_{i=1}^{3} \omega_{N_i} : \mathbb{Z}G \to \prod_{i=1}^{3} \mathbb{Z}[G/N_i].$$

We zien dat $\ker \omega_N = \cap_{i=1}^3 \ker \omega_{N_i}$ en we zullen bewijzen dat deze triviaal is. Uit Gevolg 1.3.9 volgt dat $\mathbb{Z}G = \mathbb{Z}[C_4^{k-2} \times \langle g_1 \rangle \times \langle g_2 \rangle] \cong \mathbb{Z}C_4^{k-2}[\langle g_1 \rangle \times \langle g_2 \rangle]$, zodat we de elementen $a \in \mathbb{Z}G$ kunnen schrijven als $a = \sum_{i,j=0}^{3} a_{ij}(g_1^i \times g_2^j)$, waarbij $a_{ij} \in \mathbb{Z}C_4^{k-2}$. We drukken de condities uit op a waarvoor $a \in \ker \omega_{N_i}$ voor $i \in \{1, 2, 3\}$.

$$a_{ij} = -a_{i+2,j} \text{ voor } i \in \{0, 1\} \text{ en } j \in \{0, 1, 2, 3\} \text{ als } a \in \ker \omega_{N_1}, \tag{3.2}$$

$$a_{ij} = -a_{i,j+2} \text{ voor } i \in \{0, 1, 2, 3\} \text{ en } j \in \{0, 1\} \text{ als } a \in \ker \omega_{N_2}, \tag{3.3}$$

$$a_{ij} = -a_{i+2,j+2} \text{ voor } i \in \{0, 1\} \text{ en } j \in \{0, 1\} \text{ als } a \in \ker \omega_{N_3}. \tag{3.4}$$

Stel nu dat $a \in \ker \omega_N$, dan verkrijgen we voor $i, j \in \{0, 1\}$

$$a_{ij} \overset{3.2}{=} -a_{i+2,j} \overset{3.3}{=} a_{i+2,j+2} \overset{3.4}{=} -a_{ij},$$

zodat $a_{ij} = 0$ voor $i, j \in \{0, 1\}$. Als we 3.4 toepassen, krijgen we dat $a_{ij} = 0$ voor alle $i, j \in \{0, 1, 2, 3\}$, zodat $a = 0$. Dit geeft ons dat ω_N injectief is. Aangezien ω_N een morfisme is, zien we dat $\omega_N(\mathcal{U}(\mathbb{Z}G)) \subseteq \mathcal{U}\left(\prod_{i=1}^3 \mathbb{Z}[G/N_i]\right)$. Voor elke $i \in \{1, 2, 3\}$ is $G/N_i \cong C_4^{k-1} \times C_2$. Via de inductiehypothese en Lemma 3.1.11 zien we dat $\mathcal{U}(\mathbb{Z}[G/N_i)]$ eindig is voor elke $i \in \{1, 2, 3\}$. Aangezien ω_N injectief is, is ook $\mathcal{U}(\mathbb{Z}G)$ eindig en wegens Gevolg 3.1.13 triviaal. Het geval $n = 3$ zullen we op een gelijkaardig manier bewijzen. We beschouwen de normaaldelers

$$N_1 = \langle 1 \times g_1 \times 1 \rangle \qquad N_2 = \langle 1 \times 1 \times g_2 \rangle \qquad N_3 = \langle 1 \times g_1 \times g_2 \rangle \qquad N_4 = \langle 1 \times g_1 \times g_2^2 \rangle.$$

Opnieuw definiëren we het morfisme

$$\omega_N := \prod_{i=1}^{4} \omega_{N_i} : \mathbb{Z}G \to \prod_{i=1}^{4} \mathbb{Z}[G/N_i].$$

We trachten te bewijzen dat ω_N injectief is. We kunnen de elementen van $\mathbb{Z}G$ schrijven als

$$\sum_{i,j=0}^{2} a_{ij}(g_1^i \times g_2^j),$$

waarbij $a_{ij} \in \mathbb{Z}C_3^{k-2}$ en we bekomen het volgende:

$$\begin{aligned}
a_{00} + a_{10} + a_{20} = a_{01} + a_{11} + a_{21} = a_{02} + a_{12} + a_{22} = 0 \quad &\text{als } a \in \ker \omega_{N_1}, \\
a_{00} + a_{01} + a_{02} = a_{10} + a_{11} + a_{12} = a_{20} + a_{21} + a_{22} = 0 \quad &\text{als } a \in \ker \omega_{N_2}, \\
a_{00} + a_{11} + a_{22} = a_{01} + a_{12} + a_{20} = a_{10} + a_{21} + a_{02} = 0 \quad &\text{als } a \in \ker \omega_{N_3}, \\
a_{00} + a_{12} + a_{21} = a_{01} + a_{10} + a_{22} = a_{02} + a_{11} + a_{20} = 0 \quad &\text{als } a \in \ker \omega_{N_4}.
\end{aligned}$$

Als $a \in \ker \omega_N$, dan kan men uitrekenen dat $a_{ij} = 0$ voor alle $i, j \in \{0, 1, 2\}$, zodat $a = 0$ en ω_N dus injectief is. We zien dat $G/N_i \cong C_3^{k-1}$ zodat we de inductiehypothese kunnen toepassen op $\mathbb{Z}G/N_i$ voor $i \in \{1, 2, 3, 4\}$. Verder is de redenering volledig analoog als bij het geval $n = 4$. ■

Stelling 3.1.19. *Als $Q_8 = \langle x, y \mid x^4 = y^2x^2 = 1, xyx^{-1} = x^{-1}\rangle$ de quaternionengroep is, dan is $\mathcal{U}(\mathbb{Z}Q_8) = \pm Q_8$.*

Bewijs. Stel dat $a = \sum_{g \in Q_8} a_g g \in \mathcal{U}(\mathbb{Z}Q_8)$. We zullen bewijzen dat $a \in \pm Q_8$. In Lemma 3.1.16 zagen we dat $\mathcal{U}(\mathbb{Z}_{\mathcal{L}}) \cong Q_8$. Dit isomorfisme breiden we uit naar het morfisme

$$\rho : \mathbb{Z}Q_8 \to \mathbb{Z}_{\mathcal{L}}, \sum_{g \in Q_8} a_g g \mapsto (a_1 - a_{x^2}) + (a_x - a_{x^3})i + (a_y - a_{x^2y})j + (a_{xy} - a_{x^3y})k.$$

Omdat $a \in \mathcal{U}(\mathbb{Z}Q_8)$ zal $\rho(a) \in \mathcal{U}(\mathbb{Z}_{\mathcal{L}})$. We kunnen dit expliciet uitdrukken als

$$\rho(a) = (a_1 - a_{x^2}) + (a_x - a_{x^3})i + (a_y - a_{x^2y})j + (a_{xy} - a_{x^3y})k \in \{\pm 1, \pm i, \pm j, \pm k\}.$$

We kunnen $g \in Q$ kiezen zodat voor $a' := ga$ geldt dat $\rho(a') = 1$. Hieruit volgt dat

$$a'_1 - a'_{x^2} = 1, \tag{3.5}$$
$$a'_x - a'_{x^3} = a'_y - a'_{x^2y} = a'_{xy} - a'_{x^3y} = 0. \tag{3.6}$$

Stel dat $N := (x^2) \trianglelefteq Q_8$, dan is $H := Q_8/N \cong C_2 \times C_2$. Stelling 3.1.18 geeft ons dat $\mathcal{U}(\mathbb{Z}H) = \pm H$. Als we ω_N, de augmentatieafbeelding modulo N toepassen op a' geeft dit ons $\omega_N(a') \in \pm H$. We schrijven dit uit:

$$\omega_N(a') = (a'_1 + a'_{x^2})N + (a'_x + a'_{x^3})xN + (a'_y + a'_{x^2y})yN + (a'_{xy} + a'_{x^3y})xyN \in \{\pm N, \pm xN, \pm yN, \pm xyN\}.$$

Dit geeft ons dat $a'_g + a'_{x^2g} \in \{-1, 0, 1\} =: A$ voor $g \in \{1, x, y, xy\}$. Als we de vergelijkingen (3.5) en (3.6) hierbij eens optellen en eens aftrekken, bekomen we de vergelijkingen

$$(a'_1 + a'_{x^2}) + (a'_1 - a'_{x^2}) = 2a'_1 \in \{0, 1, 2\}, \quad (a'_1 + a'_{x^2}) - (a'_1 - a'_{x^2}) = 2a'_{x^2} \in \{-2, -1, 0\},$$

en voor $g \in \{x, y, xy\}$

$$(a'_g + a'_{x^2g}) + (a'_g - a'_{x^2g}) = 2a'_g \in A, \qquad (a'_g + a'_{x^2g}) - (a'_g - a'_{x^2g}) = -2a'_{x^2g} \in A.$$

Merk op dat $a'_g \in \mathbb{Z}$, zodat $2a'_g \in 2\mathbb{Z}$ voor elke $g \in Q_8$. Als we hiermee rekening houden, bekomen we dat $a'_g = 0$ voor alle $g \in \{x, y, xy\}$ aangezien dat $A \cap 2\mathbb{Z} = 0$. We zien ook dat $a_1 \in \{0, 1\}$ en $a_{x^2} \in \{-1, 0\}$. Uit vergelijking (3.5) volgt dat ofwel $a'_{x^2} = 0$, ofwel $a'_1 = 0$, zodat $a' = 1$ of $a' = -x^2$. Aangezien $a = a'g$ voor een bepaalde $g \in Q_8$ zien we dat $a \in \pm Q_8$, exact wat we wouden bewijzen. ■

3.1.3 De stelling van Higman

We zijn nu klaar om de groepen G waarvoor geldt dat $\mathcal{U}(\mathbb{Z}G) = \pm G$ te classificeren.

Stelling 3.1.20 (Higman[Hig40]). *Als G een eindige groep is, dan zijn de volgende drie voorwaarden equivalent:*

(a) $\mathcal{U}(\mathbb{Z}G) = \pm G$;

(b) $|\mathcal{U}(\mathbb{Z}G)| < \infty$;

(c) G is abels en de exponent van G deelt 4 of 6 of $G \cong Q_8 \times A$ met A een elementair abelse 2-groep.

Bewijs. $(a) \implies (b)$ is triviaal aangezien G eindig is.
$(b) \implies (c)$ Als $\mathcal{U}(\mathbb{Z}G)$ eindig is, dan bevat het enkel torsie elementen. Dit betekent dus dat alle bicyclische en Basseenheden torsie zijn. We zagen dat torsie bicyclische eenheden triviaal zijn, dus $b(g, \hat{h}) = 1$ voor elke $g, h \in G$. Dus Lemma 3.1.4 geeft ons dat $g \in N_G(\langle h \rangle)$ voor alle $g, h \in G$. Voor elke deelgroep $H \subseteq G$ hebben we nu $N_G(H) = G$, zodat elke deelgroep een normaaldeler is. Dit betekent dat G een Hamiltoniaanse groep is. Deze soort groepen werd geclassificeerd door Dedekind en Baer in [RGH96, 5.3.7.]. Zij vonden dat elke Hamiltoniaanse groep G ofwel abels is of $G \cong Q_8 \times A \times B$ waarbij A een elementair abelse groep is en B een abelse groep is van oneven orde. Om (c) te bewijzen hoeven we enkel aan te tonen dat de exponent van G een deler is van 4 of 6. Stel $g \in G$ met $|g| = n \nmid 4$ of 6. Aangezien we weten dat de Basseenheden torsie zijn, geeft Lemma 3.1.10 ons dat $k = \pm 1 \mod n$ voor alle k die copriem zijn met n. Dit betekent dat als ϕ de Euler totiënt-functie is, dan $\phi(n) \leq 2$, zodat $n \in \{1, 2, 3, 4, 6\}$. Dit bewijst dat de exponent van G een deler is van 4 of 6.
$(c) \implies (a)$ Het geval dat $G \cong Q_8 \times A$ met A een elementair abelse 2-groep volgt uit Stelling 3.1.19 en Lemma 3.1.11. Als G abels is en de exponent van G 4 of 6 deelt dan geldt dat $G \cong C_d^k \times A$ met $d = 3$ of $d = 4$ en A een elementair abelse 2-groep. In Stelling 3.1.18 bewezen we dat $\mathcal{U}\left(\mathbb{Z}C_d^k\right) = \pm C_d^k$ met $d = 3$ of $d = 4$ zodat we enkel nog Lemma 3.1.11 hoeven toe te passen om $\mathcal{U}(\mathbb{Z}G) = \pm G$ te bekomen. ■

3.2 Het isomorfisme probleem

Probleem 3.2.1. Zij G en H eindige groepen. Geldt de volgende implicatie:

$$\mathbb{Z}G \cong \mathbb{Z}H \implies G \cong H?$$

We zullen naar deze vraag verwijzen als (ISO).

Men kan deze vraag natuurlijk stellen voor elke ring R. Het probleem wordt echter "makkelijker" naar mate men de ring "groter" maakt. Dit ziet men zeer duidelijk uit het feit dat

$$SG \cong S \otimes_R RG$$

wanneer er een ringmorfisme $R \to S$ bestaat. We zien bijvoorbeeld ook dat het gemakkelijker wordt om eenheden te vinden wanneer we de ring uitbreiden.

Voorbeeld 3.2.2. De complexe groepalgebra van de cyclishe groep $C_2 = \{1, g\}$ bevat niet-triviale eenheden, i.e. $\mathcal{U}(\mathbb{C}C_2) \neq \pm C_2$. We zien bijvoorbeeld dat het element $u = \sqrt{2}g + 1$ inverteerbaar is, met inverse $u^{-1} = \sqrt{2}g - 1$.

We zullen ons vaker richten op de torsie-elementen van een groepring. Om deze gemakkelijker te kunnen noteren voeren we een notatie in.

Notatie 3.2.3. Voor en groep G zullen we de deelverzameling van elementen van eindige orde noteren als

$$T(G) = \{g \in G \mid g^n = 1 \text{ voor een bepaalde } n \in \mathbb{N}^*\}.$$

Het onderzoeken van de eenheden van een groepring is relevant voor het isomorfisme probleem. We zullen namelijk bewijzen dat de integrale groepring bepaald wordt door zijn eenheden. Om dit te bewijzen hebben we eerst twee hulpstellingen nodig die een gevolg zijn van Stelling 3.1.12 (Berman-Higman).

Definitie 3.2.4. Zij G een groep en R een ring. We noemen $H \subseteq RG$ een **eenheidsgroep**, als $H \subseteq \mathcal{U}(RG)$ en H een groep is onder de vermenigvuldiging van RG. We zullen dit noteren als $H \leq RG$.

Stelling 3.2.5. *Zij $H \leq \mathcal{V}(\mathbb{Z}G)$ een eindige eenheden deelgroep, dan is H $\mathbb{Q}$-onafhankelijk (als deelverzameling van $\mathbb{Q}G$).*

Bewijs. We weten dat H eindig is, dus stel $|H| = m$ en noteer $H = \{h_1, \ldots, h_{,m}\}$. Stel dat H lineair afhankelijk is, zodat

$$h_j = \sum_{\substack{i=1 \\ i \neq j}}^{m} \lambda_{h_i} h_i.$$

Neem een $h \in H \setminus \{h_j\}$, waarvoor $\lambda_h \neq 0$, dan is $1 \in \operatorname{supp} h_j h^{-1}$. Aangezien H een eindige groep is, kunnen we Lemma (i) toepassen op $h_j h^{-1} \in H$, zodat $h_j h^{-1} = 1$. Dit betekent dat $h = h_j$, een contradictie. ■

Gevolg 3.2.6. *Zij G een eindige groep en $H \leq \mathbb{Z}G$ een eindige eenheidsgroep. Als $|H| = |G|$, dan is $^1\mathbb{Z}H = \mathbb{Z}G$.*

Bewijs. Per definitie is $\mathbb{Z}H \subseteq \mathbb{Z}G$. Omgekeerd zien we via de vorige Stelling 3.2.5 dat $\mathbb{Q}H = \mathbb{Q}G$, zodat $\mathbb{Z}G \subseteq \mathbb{Q}H$. Dit geeft ons direct dat er een $N \in \mathbb{N}$ bestaat zodat $Ng \in \mathbb{Z}H$ voor elke $g \in G$. Stel dus $g = \sum_{h \in H} z_h h$ met $z_h \in \mathbb{Z}$ voor elke $h \in H$. Voor elke $h \in H$ zien we dat

$$Ngh^{-1} = z_h + \sum_{h' \in H \setminus h} z_{h'} h' h^{-1}.$$

Merk op dat elke $h'h^{-1} \in H$ torsie is aangezien H eindig is. We kunnen dus Stelling 3.1.12 toepassen, die ons $1 \notin \operatorname{supp}(h'h^{-1})$ oplevert aangezien $h \neq h'$. Dit geeft ons dat z_h het coëfficiënt is van 1 in Ngh^{-1}. Dit geeft ons dat $N \mid z_h$ voor elke $h \in H$, zodat $g \in \mathbb{Z}H$. Het is nu duidelijk dat $\mathbb{Z}H = \mathbb{Z}G$. ■

Merk op dat dit de mogelijke ordes van een torsie-element van $\mathbb{Z}G$ beperkt. De orde van een torsie-element kan dus niet groter zijn dan de orde van de groep. Later zullen we nog bewijzen dat de orde van een torsie-element uit de groepring steeds een deler is van de orde van de groep. We hebben nu voldoende werk verricht om de volgende stelling te bewijzen. We zullen namelijk bewijzen dat integrale groepringen bepaald worden door hun eenheden.

Stelling 3.2.7 ([Tem19])**.** *Zij G, H eindige groepen. De volgende uitspraken zijn equivalent:*

(a) $\mathbb{Z}G \cong \mathbb{Z}H$;

(b) $\mathcal{U}(\mathbb{Z}G) \cong \mathcal{U}(\mathbb{Z}H)$;

(c) $\mathcal{V}(\mathbb{Z}G) \cong \mathcal{V}(\mathbb{Z}H)$.

[1] Met $\mathbb{Z}H$ bedoelen we de deelgroep van $\mathbb{Z}G$, verkregen door H met $\mathbb{Z}$ op te spannen.

Bewijs. (a) $\implies$ (b) Dit is triviaal.
(b) $\implies$ (c) Dit volgt uit het feit dat voor een groep G geldt dat $\mathcal{U}(\mathbb{Z}G) \cong \mathcal{V}(\mathbb{Z}G) \times C_2$ (Voorbeeld 1.3.18).
(c) $\implies$ (a) Stel dat f een isomorfisme $\mathcal{V}(\mathbb{Z}G) \to \mathcal{V}(\mathbb{Z}H)$ is. Aangezien $G \leq \mathcal{V}(\mathbb{Z}G)$, is ook $f(G) \leq \mathbb{Z}H$ een eindige eenheidsgroep. Gevolg 3.2.6 geeft ons dat $\mathbb{Z}f(G) = \mathbb{Z}H$. We zien dus dat we f kunnen uitbreiden tot een isomorfisme tussen $\mathbb{Z}G$ en $\mathbb{Z}H$. ■

We kunnen ook gemakkelijk controleren dat het isomorfisme probleem een positief antwoord heeft voor abelse groepen. We geven dit als gevolg van de Berman-Higman stelling.

Gevolg 3.2.8. *Zij G een abelse groep en H een groep zodat $\mathbb{Z}G \cong \mathbb{Z}H$, dan is $G \cong H$.*

Bewijs. Aangezien een groepring $\mathbb{Z}G$ commutatief is als en slechts als de groep G abels is, zien we dat H abels is. Als we kijken naar $T(\mathcal{V}(\mathbb{Z}G))$ (respectievelijk $T(\mathcal{V}(\mathbb{Z}H))$), zien we dat deze een deelgroep vormen aangezien $\mathcal{V}(\mathbb{Z}G)$ (respectievelijk $\mathcal{V}(\mathbb{Z}H)$) abels is. Het is duidelijk dat $T(\mathcal{V}(\mathbb{Z}G)) \cong T(\mathcal{V}(\mathbb{Z}H))$ aangezien $\mathcal{V}(\mathbb{Z}G) \cong \mathcal{V}(\mathbb{Z}H)$ en de orde bewaart blijft onder een morfisme. We hoeven nu enkel nog de Berman-Higman Stelling 3.1.12 toe te passen om te bekomen dat

$$G \cong T(\mathcal{V}(\mathbb{Z}G)) \cong T(\mathcal{V}(\mathbb{Z}H)) \cong H.$$

■

3.2.1 De Zassenhaus vermoedens

Opmerking 3.2.9. Zij G een eindige groep. Het isomorfisme probleem is equivalent aan het probleem of elke eenheidsgroep $H \subseteq \mathbb{Z}G$, die een basis van $\mathbb{Z}G$ vormt, isomorf is aan G.

Als u een eenheid is van een integrale groepring dan is voor elke $g \in G$ het element $u^{-1}gu$ een torsie-element in $\mathbb{Z}G$. Dit geeft aanleiding tot de vraag of elke torsie-element van $\mathbb{Z}G$ van deze vorm is. Higman had in zijn thesis al opgemerkt dat dit voor de symmetrische groep S_3 niet geldde. Dit werd opnieuw bewezen in [HP72] door Ian Hughes en Kenneth Pearson. Zij bewezen echter dat elk torsie-element van $\mathbb{Z}S_3$ toegevoegd was in $\mathbb{Q}G$ aan een $g \in G$. In [Zas74] uitte Hans Zassenhaus het vermoeden dat voor elke eindige groep G, elk torsie-element van $\mathcal{V}(\mathbb{Z}G)$ toegevoegd zou zijn aan een $g \in G$ binnenin de groepalgebra $\mathbb{Q}G$. Gelijkaardige uitspraken worden ook toegekend aan Zassenhaus. Deze uitspraken zullen wij als problemen verwoorden aangezien er al bewezen is dat deze vermoedens niet gelden.

Probleem 3.2.10. Zij G een eindige groep. De volgende problemen worden toegewijd aan Zassenhaus.

(ZC_1) Als $u \in T(\mathcal{V}(\mathbb{Z}G))$ bestaat er dan een $g \in G$ waarvoor $u \sim_{\mathbb{Q}} g$?

(ZC_2) Zij $H \subseteq \mathbb{Z}G$ een eenheidsgroep die een basis vormt voor $\mathbb{Z}G$. Geldt er dat $H \sim_{\mathbb{Q}} G$?

(ZC_3) Zij $H \subseteq \mathbb{Z}G$ een eenheidsgroep. Geldt er dat $H \sim_{\mathbb{Q}} G'$ voor een deelgroep $G' \leq G$?

Merk op dat een positief antwoord op (ZC_2) ook een positief antwoord op het isomorfisme probleem geeft. In 2001 gaf Martin Hertweck echter een tegenvoorbeeld voor (ISO) in [Her01]. Zijn tegenvoorbeeld bestond uit twee groepen van orde $2^{21}.97^{28}$. Het is nog altijd een open vraag of dat (ISO) geldt voor groepen van oneven orde. Het tegenvoorbeeld voor (ISO) betekende natuurlijk dat beide (ZC_2) en (ZC_3) een negatief antwoord hebben. Het eerste Zassenhaus vermoeden hield langer stand, maar in 2017 vonden F. Eisele en L. Margolis een tegenvoorbeeld [EM17].

3.3 De HeLP methode

In deze sectie zullen we wat gekend staan als de "HeLP" methode bespreken. Dit is een methode die men toepast op een specifieke groep om info te verkrijgen over de eenheden van zijn integrale groepring. Deze methode gebruikt men onder andere om $(\mathrm{ZC}) := (\mathrm{ZC}_1)$ te bewijzen voor specifieke groepen.

3.3.1 Partiële augmentatie

In deze subsectie zullen we de nodige theorie opbouwen voor de "HeLP" methode. In de komende stellingen zullen we met het Lie-product werken. We geven de definitie en introduceren de notatie. Het Lie-product is gedefinieerd over een ring, maar aangezien wij G als deelverzameling zien van de ring $\mathbb{Z}G$ zal de notatie $[g, h]$ met $g, h \in G$ voorkomen. Wij waarschuwen de lezer om deze notatie in deze sectie niet te verwarren met de commutator. We definiëren een afbeelding die een hoofdrol zal spelen binnenin deze sectie.

Definitie 3.3.1. Zij G een eindige groep en R een ring. De partiële augmentatieafbeelding is de afbeelding

$$\varepsilon_x : RG \to R, \sum_{g\in G} a_g g \mapsto \sum_{y\in x^G} a_y.$$

Notatie 3.3.2. Zij G een eindige groep. We zullen een complete verzameling van representanten van de toevoegingsklassen van G telkens noteren als $\mathrm{cl}(G)$.

Het is duidelijk dat voor een groepring RG de augmentatieafbeelding ω juist de som $\sum_{x\in \mathrm{cl}(G)} \varepsilon_x$ is. De HeLP methode is gebaseerd op verschillende stellingen die informatie geven over de partiële augmentatie van een torsie element $u \in \mathcal{V}(\mathbb{Z}G)$ van willekeurige orde n. De methode zal dan een aantal gelijkheden en ongelijkheden opleveren met als onbekende de partiële augmentaties van u. Als deze tot contradicties leiden kan men besluiten dat er geen elementen van orde n bestaan. We zullen zelfs aan de hand van de partiële augmentaties kunnen bewijzen of (ZC) geldt.

Definitie 3.3.3. Zij R een ring. Voor twee elementen $a, b \in R$ van de ring definiëren we het **Lie-product** als

$$[a, b] = ab - ba.$$

We definiëren ook

$$[R, R] = \{\sum_{i=1}^{n} r_i[a_i, b_i] \mid a_i, b_i \in R, n \in \mathbb{N}\}.$$

Het volgend lemma bewijst de formule van Cliff. Deze zal van pas komen voor verschillende bewijzen in deze sectie.

Lemma 3.3.4 ([Cli80])**.** *Zij R een ring van karakteristiek p^n, waarbij p priem is en $n \in \mathbb{N}^*$. Voor elk getal $k \geq n$ geldt dat*

$$(\sum_{i=1}^{m} a_i)^{p^k} = \sum (a_{i_1} a_{i_2} \dots a_{i_s})^{p^k - n+1} + \lambda, \tag{3.7}$$

waarbij $s = p^{n-1}$, $\lambda \in [R, R]$ en de som genomen wordt over alle s-tupels $(i_1, i_2, \dots, i_s)$ zodat $1 \leq i_j \leq m$.

Bewijs. We weten dat

$$(\sum_{i}^{m} a_i)^{p^k} = \sum (a_{i_1} a_{i_2} \dots a_{i_{p^k}}) \tag{3.8}$$

waarbij de som genomen wordt over alle p^k-tupels $(i_1, i_2, \dots, i_{p^k})$. Zij

$$S := \{(a_{i_2} \dots a_{i_{p^k}}) \mid 1 \leq i_j \leq m\}$$

de verzameling woorden van lengte p^k bestaande uit $\{a_1, \dots, a_{p^k}\}$, waarbij we even de relaties tussen de $a_i \in A$ vergeten. We definiëren de actie σ op S als

$$\sigma\left((a_{i_1} a_{i_2} \dots a_{i_{p^k}})\right) = (a_{i_2} \dots a_{i_{p^k}} a_{i_1}).$$

Het is duidelijk dat $|\langle\sigma\rangle| = p^k$, zodat de baan van een element $s \in S$ lengte p^l heeft met $l \leq k$. Als $\sigma^{p^l}(x) = x$, dan is $x = (a_{i_1} a_{i_2} \dots a_{i_{p^l}})^{p^{k-l}}$. Zo zien we dat als de baan van $x \in S$ kleiner is dan of gelijk aan p^{n-1}, we $\sigma^{p^{n-1}}(x) = x$ hebben, zodat $x = (a_{i_1} a_{i_2} \dots a_{i_{p^{n-1}}})^{p^{k-n+1}}$. Als de lengte van de baan van x onder σ groter is dan p^{n-1}, dan is deze lengte een veelvoud van p^n. Merk op dat $x - \sigma(x) \in [R, R]$ zodat $x^{\langle\sigma\rangle} \subseteq x + [R, R]$. Om de formule (3.7) te bekomen hoeft men enkel de som van het rechterlid van (3.8) op te splitsen in twee delen.

Een deel met alle $x \in S$ waarvoor $\left|x^{\langle\sigma\rangle}\right| \leq p^{n-1}$ en het tweede deel alle $x \in S$ met $\left|x^{\langle\sigma\rangle}\right| \geq p^n$. Het eerste deel zal een som zijn van elementen van de vorm $(a_{i_1} a_{i_2} \dots a_{i_p^{n-1}})^{p^{k-n+1}}$. In het tweede deel groepeer je de banen onder σ, aangezien deze allemaal dezelfde waarde hebben modulo $[R, R]$ en de grootte van deze banen telkens een veelvoud is van p^n, resulteert het tweede deel slechts in een element $\lambda \in [R, R]$. ∎

Het volgend lemma zal van groot belang zijn aangezien het ons toelaat om veel partiële augmentaties gelijk aan nul te stellen.

Lemma 3.3.5 ([MRSW87]). *Zij G een eindige groep, $x \in G$, en $u \in T(\mathcal{V}(\mathbb{Z}G))$ een torsie-element. Als er een priemgetal p bestaat zodat $p \mid |x|$ en $p \nmid |u|$, dan is $\varepsilon_x(u) = 0$.*

Bewijs. Aangezien $p \nmid |u|$, is p inverteerbaar modulo $|u|$, zodat er oneindig veel $k \in N^*$ zijn zodat $|u| \mid (p^k - 1)$. Neem een $k > n$ waarvoor $|u| \mid (p^k - 1)$ vast. Merk op dat $u^{p^k} = u$, deze identiteit samen met de formule van Cliff (3.7) geeft ons:

$$\begin{aligned} u &= \sum_{g \in G} u_g g = (\sum_{g \in G} u_g g)^{p^k} \\ &= \sum (u_{i_1} u_{i_2} \dots u_{i_s})^{p^{k-n+1}} (g_{i_1} g_{i_2} \dots g_{i_s})^{p^{k-n+1}} + \lambda, \end{aligned}$$

met $\lambda \in \Lambda + p^n \mathbb{Z}G$, $s = p^{n-1}$. We kunnen k groot genoeg nemen zodat de ordes van alle mogelijke $h := (g_{i_1} g_{i_2} \dots g_{i_s})^{p^{k-n+1}}$ copriem met p is. Aangezien deze ordes copriem zijn met p kunnen deze elementen niet toegevoegd zijn aan x, zodat $\varepsilon_x(u) \equiv 0 \mod p^n$. We kunnen echter n groot genoeg nemen zodat $\varepsilon_x(u) = 0$, hetgeen we wouden bewijzen. ∎

Notatie 3.3.6. We zullen voortaan voor een groep G de notatie $\Lambda := [\mathbb{Z}G, \mathbb{Z}G]$ gebruiken. Merk op dat aangezien voor $\alpha = \sum_{g \in G} a_g g$ en $\beta = \sum_{g \in G} b_g g$ geldt dat

$$[\alpha, \beta] = \sum_{g,h \in G} a_g b_h (gh - hg) = \sum_{g,h \in G} a_g b_h [g, h].$$

Zodat Λ juist de $\mathbb{Z}$-lineaire span is van de elementen $[g, h]$, waarbij we steeds het Lie-product bedoelen en niet de commutator.

Lemma 3.3.7. *Zij $\mathbb{Z}G$ een integrale groepring van een groep G, dan geldt er dat*

$$\{[g,h] \mid g,h \in G \subseteq \mathbb{Z}G\} = \{x - x^g \mid x,g \in G\}.$$

Bewijs. We zien gemakkelijk voor elke $g,h \in G$ dat $[g,h] = gh - hg = gh - (gh)^g$. Omgekeerd ziet men voor elke $x,g \in G$ dat het element $x - x^g$ te schrijven is als het Lie-product $[g, g^{-1}x]$. ■

We bewijzen nu een aantal eigenschappen die ons enorm zullen helpen.

Lemma 3.3.8 ([Seh78])**.** *De volgende drie eigenschappen gelden in een integrale groepring $\mathbb{Z}G$ van een eindige groep G:*

$$\Lambda = \{\alpha \in \mathbb{Z}G \mid \varepsilon_x(\alpha) = 0 \text{ voor elke } x \in G\}; \tag{3.9}$$

$$\Lambda = [\mathbb{Q}G, \mathbb{Q}G] \cap \mathbb{Z}G; \tag{3.10}$$

$$(\sum_{g\in G} a_g g)^p \equiv \sum_{g\in G} a_g g^p \mod \Lambda + p\mathbb{Z}G, \quad \Lambda^p \subseteq \Lambda + p\mathbb{Z}G. \tag{3.11}$$

Bewijs. (i) Stel dat $\lambda \in \Lambda$, dan is λ een $\mathbb{Z}$-lineaire combinatie van Lie-producten $[g,h]$. Deze Lie-producten zijn volgens Lemma 3.3.7 telkens het verschil van twee toegevoegde elementen. Aangezien $\varepsilon_y(x - x^g) = 0$ en ε $\mathbb{Z}$-lineair is voor elke $y \in G$ zal ook $\varepsilon_y(\lambda) = 0$ voor elke $y \in G$, zodat de inclusie $\subseteq$ bewezen is. Stel nu dat $\alpha = \sum_{g\in G} a_g g$ met $\varepsilon_x(\alpha) = 0$ voor elke x. We herschrijven α als volgt:

$$\begin{aligned}\alpha &= \sum_{x\in \mathrm{CL}(G)} \sum_{g\in x} a_{x^g} x^g \\ &= \sum_{x\in \mathrm{CL}(G)} \sum_{g\in x} \underbrace{\operatorname{sgn} a_{x^g}(x^g + \cdots + x^g)}_{|a_{x^g}| \text{keer}}\end{aligned}$$

omdat $\varepsilon_x(\alpha) = 0$ kunnen we koppels $(g,h) \in G \times G$ vormen zodat α te schrijven is als

$$= \sum_{x\in \mathrm{CL}(G)} \sum_{g,h\in G} c_{(g,h)}(x^g - x^h),$$

waarbij $c_{(g,h)} \in \mathbb{N}$. Opnieuw zien we via Lemma 3.3.7 dat $\alpha \in \Lambda$, zodat ook $\supseteq$ bewezen is, wat (3.9) bewijst.

(ii) Stel dat $\mu \in [\mathbb{Q}G, \mathbb{Q}G]$, dan bestaat er een $N \in \mathbb{N}^*$ zodat $N\mu \in \Lambda$. Als we gebruik maken van (3.9) zien we dat $N\mu \in \{\alpha \in \mathbb{Z}G \mid \varepsilon_x(\alpha) = 0 \text{ voor elke } x \in G\}$. Hieruit volgt dat

$$[\mathbb{Q}G, \mathbb{Q}G] \subseteq \{\alpha \in \mathbb{Q}G \mid \varepsilon_x(\alpha) = 0 \text{ voor elke } x \in G\},$$

zodat

$$\begin{aligned}[\mathbb{Q}G, \mathbb{Q}G] \cap \mathbb{Z}G &\subseteq \{\alpha \in \mathbb{Q}G \mid \varepsilon_x(\alpha) = 0 \text{ voor elke } x \in G\} \cap \mathbb{Z}G. \\ &= \{\alpha \in \mathbb{Z}G \mid \varepsilon_x(\alpha) = 0 \text{ voor elke } x \in G\} \\ &= \Lambda.\end{aligned}$$

Dit bewijst dat $[\mathbb{Q}G, \mathbb{Q}G] \cap \Lambda \subseteq \Lambda$, maar het is duidelijk dat de omgekeerde inclusie ook geldt, zodat we een gelijkheid hebben.

(iii) We weten dat voor elke $a \in \mathbb{Z}$ geldt dat $a^p \equiv a \mod p\mathbb{Z}$, en dus ook $a^p = a \mod p\mathbb{Z}G$. We passen gewoon de formule van Cliff (3.7) toe, wat ons geeft dat er voor elke $\alpha = \sum_{g\in G} a_g g$ geldt dat

$$\begin{aligned}(\sum_{g\in G} a_g g)^p &\equiv \sum_{g\in G} (a_g g)^p \mod \Lambda + p\mathbb{Z}G \\ &\equiv \sum_{g\in G} a_g g^p \mod \Lambda + p\mathbb{Z}G,\end{aligned}$$

wat we wouden bewijzen.

■

Lemma 3.3.9. *Zij G een eindige groep, $x \in G$ en $u \in T(\mathcal{V}(\mathbb{Z}G))$, dan zijn de volgende uitspraken equivalent.*

(a) $\varepsilon_x(u) = 1$ *en* $\varepsilon_y(u) = 0$ *voor elke* $y \in G \setminus x^G$*;*

(b) $u \equiv x \mod \Lambda$.

Bewijs. Stel dat $x \in G$ zodat $\varepsilon_x(u) = 1$ en $\varepsilon_y(u) = 0$ voor elke $y \in G \setminus x^G$. Dan kunnen we u schrijven als $u = x + (-x + u)$, aangezien $-x + u \in \Lambda$ zien we dat $u \equiv x \mod \Lambda$. Omgekeerd stel dat $u \equiv x \mod \Lambda$. Dan is $u = x + \lambda$, met $\lambda \in \Lambda$. We zien dat er voor elke $z \in G$ geldt dat $\varepsilon_z(u) = \varepsilon_z(x + \lambda) = \varepsilon_z(x) + \varepsilon(\lambda)$, zodat uit (3.9) volgt dat $\varepsilon_x(u) = 1$ en $\varepsilon_y(u) = 0$ voor $y \in G \setminus x^G$. ■

We zullen bewijzen dat, als u een torsie-element is van een groepring $\mathbb{Z}G$, dan de orde van u de orde van G deelt. We hebben wel nog wat hulpstellingen nodig.

Stelling 3.3.10 ([CL65])**.** *Zij G een eindige groep, $u \in T(\mathcal{V}(\mathbb{Z}G))$ en p een priemgetal. Zij voor elke $l \in \mathbb{N}^*$*

$$\begin{aligned}T_l &= \{g \in G \mid \left|g^{p^l}\right| = 1\}; \\ \tilde{T}_l &= \sum_{g\in T_l} u_g.\end{aligned}$$

Dan zijn de volgende uitspraken equivalent:

(a) het torsie-element u heeft orde p^k;

(b) $\tilde{T}_k \not\equiv 0 \mod p\mathbb{Z}G$.

Bewijs. Zij $l \in \mathbb{N}$. We beschouwen u^{p^l} en passen de formule van Cliff (3.7) toe:

$$u^{p^l} \equiv (\sum_{g\in G} u_g g)^{p^l} = \sum_{g\in G} u_g g^{p^l} + \lambda \mod p\mathbb{Z}G,$$

met $\lambda \in \Lambda$. Uit (3.9) volgt dat $\varepsilon_1(\lambda) = 0$, zodat het coëfficiënt van 1 in λ gelijk aan nul is. Zij $u_1(l) := u_1^{p^l}$ het coëfficiënt van 1 in u^{p^l}, dan is

$$u_1(l) \equiv \sum_{i\leq l} \tilde{T}_i \mod p. \tag{3.12}$$

We weten dat u torsie is, zodat ook u^{p^l} torsie is voor elke $l \in \mathbb{N}$. Via de stelling van Berman-Higman 3.1.12 zien we dat als $u_1(l) \neq 0$ we $u^{p^l} = 1$ hebben zodat $|(|\, u) \leq p^l$. $(a) \implies (b)$ Stel dat $|u| = p^k$,

dan is $u_1(l) = 0$ voor alle $l < k$. Specifiek is ook $u_1(l) \equiv 0 \mod p$ voor $l < k$. Dit samen met (3.12) geeft ons

$$1 = u_1^{p^k} \equiv \tilde{T}_k \mod p,$$

zodat $\tilde{T}_k \not\equiv 0 \mod p$.
(b) $\implies$ (a) Stel dat $\mu_k \not\equiv 0 \mod p$ voor een $k \in \mathbb{N}^*$. Kies $k' \in \mathbb{N}^*$ minimaal, zodat $\mu_k \not\equiv 0 \mod p$. We beschouwen $u_1(k')$:

$$u_1(k') \overset{(3.12)}{\equiv} \tilde{T}_{k'} \mod p,$$

want door de minimaliteit van k' is $\tilde{T}_l \equiv 0 \mod p$ voor $l < k'$. Aangezien $u_1(k') \neq 0$ is $1 \in \operatorname{supp}(u^{p^{k'}})$. De Berman-Higman Stelling 3.1.12 geeft ons dus $u^{p^{k'}} = 1$. Als $l < k'$, dan is $\tilde{T}_l \equiv 0 \mod p$ zodat $u_1(l) \equiv 0 \mod p$. Zo zien we dat $u^{p^l} \neq 1$ voor $l < k'$, zodat $|u| = p^{k'}$. Om ons bewijs af te ronden hoeven we enkel nog te bewijzen dat $k' = k$. We doen dit door te bewijzen dat k' het unieke getal is waarvoor $\tilde{T}_{k'} \not\equiv 0 \mod p$. We namen al aan dat k' minimaal is, zodat we enkel nog $\tilde{T}_l \equiv 0 \mod p$ voor $l > k$ hoeven te bewijzen. We bewijzen per inductie dat $\tilde{T}_{k'+n} \equiv 0 \mod p$ voor alle $n \in \mathbb{N}^*$. Herinner dat $1 = u_1(k') \equiv \tilde{T}_{k'} \mod p$. We beschouwen $u^{p^{k'+1}}$ en zien dat

$$u^{p^{k'+1}} = 1 = u_1(k'+1) \overset{(3.12)}{\equiv} \tilde{T}_{k'} + \tilde{T}_{k'+1} \mod p$$

waaruit volgt dat $\tilde{T}_{k'+1} \equiv 0 \mod p$ want $\tilde{T}_{k'} \equiv 1 \mod p$. Stel nu dat $\mu_{k'+m} \equiv 0 \mod p$ voor alle $m < n$, dan is

$$1 = u^{p^{k'+n}} = u_1(k'+n) \overset{(3.12)}{\equiv} \tilde{T}_{k'} + \sum_{k'<i\leq n} \tilde{T}_i \mod p,$$

zodat ook $\tilde{T}_{k'+n} \equiv 0 \mod p$. Zo bewezen we dus dat k' uniek is en k en k' dus samenvallen zodat $|u| = p^k$ en het gestelde bewezen is. ■

Gevolg 3.3.11. *Zij G een eindige groep en $u \in T(\mathcal{V}(\mathbb{Z}G))$ een eenheid met een priemmacht als orde. Als $|u| = p^k$, dan bestaat er een $g \in G$ met $|g| = p^k$.*

Bewijs. Dit volgt rechtstreeks uit de vorige stelling. ■

We zijn nu klaar om de volgende stelling te bewijzen die de mogelijke ordes van een torsie-element van $\mathbb{Z}G$ zal beperken.

Stelling 3.3.12 ([CL65])**.** *Zij G een groep van eindige orde en $u \in T(\mathcal{V}(\mathbb{Z}G))$ een torsie-element. De orde van u deelt de orde van G.*

Bewijs. Zij $|u| = k$ en

$$|u| = p_1^{k_1} \dots p_m^{k_m}$$

de priemfactorisatie van k. Voor elke priemdeler p_j van k definiëren we $p'_j := \prod_{\substack{i=1 \\ i\neq j}}^{m} q_i^{k_i}$. Merk op dat $u^{p'_j}$ een element van orde p^j is. Uit Gevolg 3.3.11 volgt nu dat G een element van orde p^j bevat. Dit betekent ook dat $p^j \mid |G|$. We kunnen dus besluiten dat $k \mid |G|$. ■

We zijn nu klaar om de belangrijkste stelling van deze sectie te bewijzen. Deze stelling laat ons toe om de karaktertabel uit te buiten van een groep om informatie te verkrijgen over de partiële augmentaties.

Opmerking 3.3.13. Zij G een eindige groep en χ een karakter van G. Zij $\alpha \in RG$, dan is

$$\chi(\alpha) = \sum_{x \in \mathrm{cl}(G)} \varepsilon_x(\alpha)\chi(x).$$

Opmerking 3.3.14. Zij F een veld en K/F een Galois-uitbreiding. Dan is het Galoisspoor van K/F de K-lineaire afbeelding

$$\mathrm{Sp}_{K/F} : K \to F,\ a \mapsto \sum_{\sigma \in \mathrm{Gal}(K/F)} a^\sigma.$$

Stelling 3.3.15 ([LP89])**.** *Zij G een eindige groep, $u \in T(\mathcal{V}(\mathbb{Z}G))$ een torsie-element van orde k en $\zeta \in \mathbb{C}^*$ een primitieve k-de eenheidswortel. Als ρ een irreducibele representatie is van G en χ zijn karakter is, dan geldt voor elke $l \in \mathbb{Z}$ dat de multipliciteit van ζ^l als eigenwaarde van $\rho(u)$ (genoteerd als $\mu_l(u,\chi)$) gegeven wordt door*

$$\mu_l(u,\chi) = \frac{1}{k}\sum_{d|k} \mathrm{Sp}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\chi(u^d)\zeta^{-dl}). \tag{3.13}$$

Bewijs. Aangezien $u \in \mathcal{V}(\mathbb{Z}G)$ orde k heeft kunnen we $\rho(u)$ diagonaliseren en zien we dat alle eigenwaarden van $\rho(u)$ eenheidswortels van orde kleiner of gelijk aan k zijn. We zullen de multipliciteit van de eigenwaarde ζ^l noteren als μ_l. Merk op dat $\chi(u) = \sum_{i=0}^{k-1} \mu_i\zeta^i$ en algemener $\chi(u^r) = \sum_{i=0}^{k-1} \mu_i\zeta^{ir}$ voor elke $r \in \mathbb{Z}$. We berekenen het volgende

$$\begin{aligned}\sum_{r=0}^{k-1} \chi(u^r)\zeta^{-rl} &= \sum_{r=0}^{k-1}\sum_{i=0}^{k-1} \mu_i\zeta^{ir}\zeta^{-rl} = \sum_{r=0}^{k-1}(\mu_l + \sum_{\substack{i=0\\ i\neq l}}^{k-1} \mu_i\zeta^{r(i-l)}) \\ &= k\mu_l + \sum_{\substack{i=0\\ i\neq l}}^{k-1}\sum_{r=0}^{k-1} \zeta^{r(i-l)} = k\mu_l.\end{aligned}$$

Bij de laatste stap maakten we gebruik van het feit dat $\sum_{r=0}^{k-1} \zeta^{r(i-l)} = \frac{\zeta^{k(i-l)}-1}{\zeta^{i-l}-1} = 0$ voor elke $i \neq l$. Dit geeft ons dat $\frac{1}{k}\sum_{r=0}^{k-1} \chi(u^r)\zeta^{-rl} = \mu_l$. We kunnen deze som opsplitsen als

$$\mu_l = \frac{1}{k}\sum_{d|k} \sum_{\substack{r \bmod k/d\\ \gcd(r,k/d)=1}} \chi(u^{dr})\zeta^{-drl}.$$

Aangezien $\chi(u)$ de som van k-de eenheidswortels is, is $\chi(u^d)$ de som van k/d-de eenheidswortels. Stel dus dat $\chi(u^d) = \eta_1 + \cdots + \eta_n$, met elke η_i een k/d-de eenheidswortel. Aangezien $\chi(u^{dr}) = \eta_1^r + \cdots + \eta_n^r$, zien we dat $\chi(u^{dr}) = (\chi(u^d))^{\sigma_r}$, waarbij σ_r het automorfisme $\zeta^d \mapsto \zeta^{dr}$ van $\mathbb{Q}(\zeta^d)$ is. Dit geeft ons exact wat we wouden bewijzen, namelijk

$$\mu_l = \frac{1}{k}\sum_{d|k} \mathrm{Sp}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\chi(u^d)\zeta^{-dl}).$$

■

Als men zoals in Opmerking 3.3.13 $\chi(u)$ met $u \in \mathcal{V}(\mathbb{Z}G)$ uitdrukt in termen van partiële augmentaties ε_x verkrijgt men een stelsel ongelijkheden door op te merken dat $\mu_l(u,\chi) \in \mathbb{N}$. Deze stelling laat toe om een karaktertabel van een groep uit te buiten om info te verkrijgen over de partiële augmentaties. Op basis van deze stelling bewezen Luthar en Passi (ZC) voor A_5 [LP89]. Voor veel groepen zal deze echter niet genoeg zijn. In 2007 bewees Hertweck de volgende stelling die toelaat om ook de p-Brauer representaties van een groep uit te buiten.

Stelling 3.3.16 ([Her07]). *Zij G een eindige groep, $u \in T(\mathcal{V}(\mathbb{Z}G))$ een torsie-element van orde k en $\zeta \in \mathbb{C}^*$ een primitieve k-de eenheidswortel. Als ρ een p-Brauer representatie is van G, met $p \nmid k$ en χ het karakter van ρ. Zij verder $\zeta \mapsto \bar{\zeta}$ een vast isomorfisme is tussen de groep van k-de eenheidswortels in karakteristiek 0 en de k-de eenheidswortels in karakteristiek p. Er geldt voor elke $l \in \mathbb{Z}$ dat de multipliciteit van $\bar{\zeta}^l$ als eigenwaarde van $\rho(u)$ (genoteerd als $\mu_l(u,\chi)$) gegeven wordt door*

$$\mu_l(u,\chi) = \frac{1}{k} \sum_{d|k} \mathrm{Sp}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\chi(u^d)\zeta^{-dl}). \tag{3.14}$$

Zonder bewijs. Zie [Her07]. ■

Deze stelling vormt samen met de Stelling 3.3.15 de basis van de HeLP methode. Ook de benaming "HeLP" slaat op Hertweck, Luthar en Passi.

Gevolg 3.3.17. *Zij G een eindige groep en $u, v \in T(\mathcal{V}(\mathbb{Z}G))$ eenheden van orde k, dan zijn de volgende uitspraken equivalent:*

(a) $u \sim_{\mathbb{Q}} v$;

(b) $\varepsilon_x(u^d) = \varepsilon_x(v^d)$ *voor elke* $x \in G$ *en* $d \mid k$.

Bewijs. Stel dat $\varepsilon_x(u^d) = \varepsilon_x(v^d)$ voor elke $x \in G$ en $d \mid k$. Als we (3.13) uit Stelling 3.3.15 beschouwen, zien we dat $\mu_l(u,\chi) = \mu_l(v,\chi)$ voor elke $l \in \mathbb{Z}$ en elk irreducibel karakter χ van G. Herinner dat $\mu_l(u,\chi)$ de multipliciteit van ζ^l als eigenwaarde van $\rho(u)$ uitdrukte, waarbij $\rho : \mathbb{C}G \to M_n(\mathbb{C})$ de representatie van χ is, en ζ een primitieve k-de eenheidswortel. Aangezien elke eigenwaarde van $\rho(u)$ en $\rho(v)$ van de vorm ζ^l is, en $\mu_l(u,\chi) = \mu_l(v,\chi)$ voor elke l, zien we dat $\rho(u)$ en $\rho(v)$ dezelfde diagonaalmatrix hebben. Dit geeft ons dat $\rho(u)$ en $\rho(v)$ toegevoegd zijn in $M_n(\mathbb{C})$. Als we Lemma 1.5.18 toepassen verkrijgen we dat $u \sim_{\mathbb{Q}} v$ hetgeen we wouden bewijzen.

Stel nu dat $u \sim_{\mathbb{Q}} v$ en dat $\alpha \in \mathbb{Q}G$ zodat $v = u^\alpha$, dan zien we dat

$$u - v = u - \alpha^{-1}u\alpha = [\alpha, \alpha^{-1}u] \in [\mathbb{Q}G, \mathbb{Q}G].$$

Dit geeft ons dat $u - v \in [\mathbb{Q}G, \mathbb{Q}G] \cap \mathbb{Z}G$, zodat $u - v \in [\mathbb{Z}G, \mathbb{Z}G]$ volgens (3.10). Als we nu (3.9) toepassen zien we dat $\varepsilon_x(u - v) = 0$ voor alle $x \in G$, zodat $\varepsilon_x(u) = \varepsilon_x(v)$ voor elke $x \in G$. Aangezien $u \sim_{\mathbb{Q}} v$ is ook $u^d \sim_{\mathbb{Q}} v^d$ voor elke $d \in \mathbb{Z}$ zodat we op dezelfde manier $\varepsilon_x(u^d) = \varepsilon_x(v^d)$ bekomen voor elke $d \in \mathbb{Z}$, specifiek ook voor de delers $d' \mid k$ zodat het gestelde bewezen is. ■

We kunnen nog een iets sterkere uitspraak doen in het geval dat $u \in \mathbb{Z}G$ en $v = g \in G$.

Stelling 3.3.18 ([MRSW87]). *Zij G een eindige groep. Zij $g \in G$ en $u \in \mathcal{V}(\mathbb{Z}G)$ met $|u| = k = |g|$. De volgende uitspraken zijn equivalent:*

(a) $u \sim_{\mathbb{Q}} g$;

(b) Voor elke deler $d \mid k$ bestaat er een $x \in G$ zodat $\varepsilon_x(u^d) = 1$ en $\varepsilon_y(u^d) = 0$ voor alle $y \in G \setminus x^G$.

Bewijs. (a) $\implies$ (b) Dit volgt uit de vorige Stelling 3.3.17. (b) $\implies$ (a) Stel dat $\varepsilon_g(u) = 1$ en $\varepsilon_h(u) = 0$ voor $h \not\sim g$. Zij p een priemgetal dan geeft Lemma 3.3.9 ons

$$\begin{aligned} u &\equiv g \mod \Lambda \\ u^p &\equiv g^p \mod \Lambda + p\mathbb{Z}G \qquad \text{via (3.11)} \end{aligned}$$

Volgens (b) bestaat er een $h \in G$ zodat $\varepsilon_h(u^p) = 1$ en $\varepsilon_y(u^p) = 0$ voor alle $y \not\sim h$. Als we opnieuw Lemma 3.3.9 toepassen zien we dat $u^p \equiv h \mod \Lambda$. Dit geeft ons

$$g^p \equiv h \mod \Lambda + \mathbb{Z}G,$$

waaruit we kunnen besluiten dat $g^p \sim h$ aangezien beide $g^p, h \in G$. We hebben dus $u^p \equiv g^p \mod \Lambda$. Dit argument kan men herhaaldelijk toepassen voor elk priemgetallen p. Zo bekomen we

$$u^k \equiv g^k \mod \Lambda.$$

Als we opnieuw Lemma 3.3.9 toepassen zien we dat $\varepsilon_x(u^k) = \varepsilon_x(g^k)$ voor elke $k \in \mathbb{N}$. Dit laat ons toe om Gevolg 3.3.17 toe te passen. Dit geeft ons $u \sim_{\mathbb{Q}} g$, hetgeen we wouden bewijzen. ■

Deze stelling geeft dus de nodige condities voor een torsie-element u om toegevoegd te zijn in $\mathbb{Q}G$ aan een element $g \in G$. We hebben nu de belangrijkste stellingen waarop de "HeLP" methode steunt bewezen. In de volgende subsectie zullen we uitleggen hoe deze gebruikt wordt.

3.3.2 De HeLP methode

In deze subsectie herhalen we de belangrijke resultaten van de vorige subsectie en tonen we hoe deze exact gebruikt worden binnen de methode. Zij G een eindige groep. Stel dat we (ZC) willen aantonen voor G. We weten dat een torsie-element $u \in T(\mathcal{V}(\mathbb{Z}G))$ niet zomaar elke orde kan hebben. Het moet namelijk volgens Stelling 3.3.12 telkens een deler zijn van de orde van G. De volgende stelling verwoordt wanneer (ZC) geldt voor een groep G.

Stelling 3.3.19. *Zij G een eindige groep. Het Zassenhaus probleem heeft een positief antwoord voor G als en slecht als de volgende twee uitspraken gelden:*

(i) De ordes van de eenheden $u \in T(\mathcal{V}(\mathbb{Z}G))$ vallen samen met de ordes van $g \in G$.

(ii) Zij $u \in \mathcal{V}(\mathbb{Z}G)$ met $|u| = |g|$ voor een bepaalde $g \in G$. Voor elke deler $d \mid |u|$ bestaat er een $x \in G$ zodat $\varepsilon_x(u^d) = 1$ en $\varepsilon_y(u^d) = 0$ voor alle $y \not\sim x$.

Bewijs. Stelling 3.3.18 ■

We veronderstellen dat een eenheid $u \in \mathcal{V}(\mathbb{Z}G)$ van orde $k \mid |G|$ bestaat. We gaan inductief te werk. We beginnen met de ordes k die zo weinig mogelijk verschillende delers hebben. Dit zorgt dat we de formule (3.13) kunnen schrijven als

$$\begin{aligned} \mu_l(u, \chi) = \frac{1}{k} \sum_{d|k} \mathrm{Sp}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\chi(u^d)\zeta^{-dl}) \\ \frac{1}{k} \sum_{x \in \mathrm{CL}(G)} \varepsilon_x(u)\, \mathrm{Sp}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\chi(x)\zeta^{-l}) + a_l(u, \chi) \end{aligned}$$

met

$$a_l(u,\chi) = \sum_{\substack{d|k \\ d\neq 1}} \mathrm{Sp}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\chi(u^d)\zeta^{-dl}),$$

waarbij we er vanuit gaan dat de $a_l(u,\chi)$ gekend zijn. Zo krijgen we voor elke $\chi \in \mathrm{Irr}(G)$ en $l \in \{0,1,\ldots,k\}$ de ongelijkheden $\mu_l(u\chi) \in \mathbb{N}$ met als onbekenden $\{\varepsilon_x(u) \mid x \in \mathrm{cl}(G)\}$. Veel van deze onbekenden kunnen we gelijk aan nul stellen aan de hand van de volgende stelling.

Stelling 3.3.20. *Zij G een eindige groep. Zij $u \in \mathcal{V}(\mathbb{Z}G)$ een eenheid van orde $k \neq 1$.*

(i) Via de Berman-Higman Stelling 3.1.12 hebben we $\varepsilon_1(u) = 0$.

(ii) $\varepsilon_x(u) = 0$ voor elke $x \in G$ waarvoor er een priemgetal p bestaat zodat $p \mid |x|$ en $p \nmid k$ (Lemma 3.3.5).

We willen met deze ongelijkheden een contradictie bekomen wanneer $k = |u|$ niet samenvalt met de orde van een element uit G. Als k wel overeenkomt met de orde van een element uit G, dan willen we Stelling 3.3.18(b) aantonen. Merk op dat, aangezien we inductief te werk gaan, we er vanuit kunnen gaan dat Stelling 3.3.18(b) voldaan is voor alle u^d met $d \mid k$. Zo hoeven we enkel aan te tonen dat er slechts één element van $\{\varepsilon_x(u) \mid x \in \mathrm{cl}(G)\}$ niet gelijk aan nul is.

Het Zassenhaus probleem voor A_5

De HeLP methode werd voor het eerst gebruikt door Luthar en Passi in [LP89]. In deze paper bewezen ze Stelling 3.3.15, en introduceerden ze dus een nieuwe aanpak om (ZC) te bewijzen. In die paper gebruikten ze het om (ZC) te bewijzen voor de alternerende groep A_5. We zullen een deel van de methode uitwerken, zodat het duidelijk is hoe men de methode toepast.

Opmerking 3.3.21. De volgende verzameling is een complete verzameling van representanten van de toevoegingsklassen van A_5

$$\{(1),(12)(34),(123),(12345),(13524)\}.$$

De alternerende groep A_5 heeft de volgende karaktertabel:

Class	1	$(12)(34)$	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Stelling 3.3.22. *Alle genormaliseerde eenheden u van de groepring $\mathbb{Z}A_5$ van orde $k \in \{2,3,5\}$ zijn toegevoegd in $\mathbb{Q}A_5$ aan een element $g \in G$.*

Bewijs. Stel dat $u \in \mathcal{V}(\mathbb{Z}A_5)$ met $|u| = k$, waarbij $k \in \{2,3,5\}$. Merk op dat aangezien $k \neq 1$ we via de Berman-Higman stelling $\varepsilon_1(u) = 0$ hebben.

Geval $k \in \{2, 3\}$: Er is maar 1 toevoeginsklasse met elementen van orde k. Aangezien k priem is kunnen we Lemma 3.3.5 toepassen om $\varepsilon_x(u) = 0$ te bekomen voor alle $x \not\sim u$. Wegens Stelling 3.3.18 hebben we nu $u \sim_{\mathbb{Q}} g$ voor een $g \in G$.

Geval $k = 5$: We kunnen opnieuw Lemma 3.3.5 toepassen om $\varepsilon_x(u) = 0$ te bekomen voor alle $|x| \neq 5$. Stel $x = (12345)$ en $x' = (13524)$, we noteren $\nu_5 := \varepsilon_x(u)$ en $\nu_5' := \varepsilon_{x'}(u)$. Aangezien $u \in \mathcal{V}(\mathbb{Z}A_5)$ is $\omega(u) = 1$, zodat $\omega(u) = \nu_5 + \nu_5' = 1$. We trachten te bewijzen dat ν_5 of $\nu_5' = 0$. Zij $\zeta = e^{\frac{2\pi i}{5}}$. We beschouwen formule (3.13):

$$\begin{aligned}\mu_l(u, \chi_3) =& \frac{1}{5}\left(3 + \mathrm{Sp}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{-l}(\nu_5\chi_3(x) + \nu_5'\chi_3(x')))\right) \\ =& \begin{cases} \nu_5 & \text{als } l = 1, \\ \nu_5' & \text{als } l = 2. \end{cases}\end{aligned}$$

Aangezien $\mu_l(u, \chi_3) \in \mathbb{N}$ voor elke l, volgt er uit $\nu_5 + \nu_5' = 1$ dat $\nu_5 = 0$ of $\nu_5' = 0$ aangezien beide ν_5 en ν_5' natuurlijke getallen zijn. We zien dus opnieuw via Stelling 3.3.18 dat $u \sim_{\mathbb{Q}} x$ of $u \sim_{\mathbb{Q}} x'$.

■

We bewijzen nu dat de groepring $\mathbb{Z}A_5$ geen torsie-elementen heeft waarvan de orde niet samenvalt met de orde van een element uit A_5.

Stelling 3.3.23. *Als $u \in \mathcal{V}(\mathbb{Z}A_5)$ een torsie-element is, met $|u| = k$, dan is $k \in \{1, 2, 3, 5\}$.*

Bewijs. Uit Stelling 3.3.12 volgt dat $k \mid |A_5| = 60$, zodat

$$k \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}.$$

We hoeven enkel te bewijzen dat $k \notin \{4, 6, 10, 15\}$ omdat $\left|u^l\right| = \frac{k}{l}$.

Geval $k = 4$: Aangezien dit een priemmacht is, kunnen we Gevolg 3.3.11 toepassen. Dit geeft ons een element $g \in A_5$ van orde 4, een contradictie.

Geval $k \in \{6, 10, 15\}$: We laten dit als oefening om de gepaste karakters $\chi \in \mathrm{Irr}(A_5)$ en $l \in \mathbb{Z}$ te kiezen in de vergelijking (3.13). Men kan ook [LP89] raadplegen.

■

Stelling 3.3.24. *Elk torsie-element $u \in \mathbb{Z}A_5$ is toegevoegd in $\mathbb{Q}G$ aan een $g \in G$. Met andere woorden het Zassenhaus probleem heeft een positief antwoord voor de alternerende groep A_5.*

Bewijs. Dit volgt rechtstreeks uit de vorige twee stellingen. ■

3.4 De cut groepen

Deze sectie zal gaan over cut groepen. Dit zijn groepen wiens integrale groepring slechts een eindig aantal eenheden heeft die centraal zijn in de groepring. Voor deze sectie zal Sectie 1.4 over ordes van groot belang zijn.

Definitie 3.4.1. We noemen een groep G **cut** als $\mathcal{V}(\mathbb{Z}G) \cap Z(\mathbb{Z}G)$ eindig is.

Aangezien $G \subseteq \mathcal{V}(\mathbb{Z}G)$ commuteert een $u \in Z(\mathcal{V}(\mathbb{Z}G))$ met heel G en bijgevolg met heel $\mathbb{Z}G$. Zo zien we dat $Z(\mathcal{V}(\mathbb{Z}G)) = \mathcal{V}(\mathbb{Z}G) \cap Z(\mathbb{Z}G)$. De term "cut" verscheen eerst in [BMP17] en is afgeleid van "central units trivial". Dit verwijst naar de stelling van Berman en Higman 3.1.12 waarin we bewezen dat een centraal torsie-element triviaal is. Dit zorgt ervoor dat de cut groepen G juist de groepen zijn zodat

$$Z(\mathcal{V}(\mathbb{Z}G)) = Z(G).$$

Als een groep G cut is, dan is ook zijn centrum $Z(G)$ cut, zodat $Z := Z(G)$ een abelse groep is, waarvoor $\mathcal{U}(\mathbb{Z}Z)$ eindig. Deze groepen zijn door de stelling van Higman 3.1.20 geclassificeerd. De term cut is slechts recent geïntroduceerd, maar groepen waarvan de integrale groepring enkel triviale centrale eenheden heeft zijn al veel eerder onderzocht. Ritter en Seghal publiceerde [RS90] in 1990 waarin ze de volgende stelling bewezen:

Stelling 3.4.2. *Zij G een eindige groep dan zijn de volgende condities equivalent.*

(a) De groep G is cut;

(b) Als $\mathbb{Q}G \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ de Wedderburn decompositie is, dan is $Z(D_i) \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-d})\}$ met $d \in \mathbb{N}^*$ voor elke $i \in \{1, \ldots, n\}$;

(c) Voor elke $x \in G$ en elk natuurlijk getal j copriem met $|G|$ is ofwel $x \sim x^j$ ofwel $x^{-1} \sim x^j$.

Bewijs. We bewijzen eerst dat (a) equivalent is aan (b). Zij $\mathbb{Q}G \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ de Wedderburn decompositie dan zien we dat $Z(\mathbb{Q}G) \cong Z(D_1) \times \cdots \times Z(D_k)$. We weten dat $Z(\mathbb{Z}G)$ een orde is in $Z(\mathbb{Q}G)$. Zij voor elke $i \in \{1, \ldots, k\}$, $\mathcal{O}_i$ een orde in $Z(D_i)$, dan bepaalt

$$\mathcal{O} := \mathcal{O}_i \times \cdots \times \mathcal{O}_k$$

een orde in $Z(\mathbb{Q}G)$ die we ook als $\mathcal{O}$ noteren. Wegens Stelling 1.4.9 is

$$[\mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathcal{O} \cap Z(\mathbb{Z}G))] < +\infty.$$

De groep eenheden $\mathcal{U}(Z(\mathbb{Z}G))$ is dus eindig als en slechts als $\mathcal{U}(\mathcal{O})$ eindig is. Aangezien

$$\mathcal{U}(\mathcal{O}) = \mathcal{U}(\mathcal{O}_i) \times \cdots \times \mathcal{U}(\mathcal{O}_k)\,,$$

is $\mathcal{U}(Z(\mathbb{Z}G))$ eindig als en slechts als $\mathcal{U}(\mathcal{O}_i)$ eindig is voor elke $i \in \{1, \ldots, k\}$. Uit Gevolg 1.4.5 van de eenheidstelling van Dirichlet (1.4.4) volgt dat $\mathcal{U}(\mathcal{O}_i)$ eindig is als en slechts als $Z(D_i) \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-d})\}$ met $d \in \mathbb{N}^*$. Zo hebben we bewezen dat $\mathcal{U}(Z(\mathbb{Z}G))$ eindig is als en slechts als er voor elke $i \in \{1, \ldots, k\}$ geldt dat $Z(D_i) \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-d})\}$. Dit bewijst dat (a) equivalent is aan (b). We zullen nu aantonen dat (b) equivalent is aan (c). Hiervoor merken we op dat via Lemma 1.5.13, (b) equivalent is met $\mathbb{Q}(\chi) \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-d})\}$ voor elk irreducibel karakter χ.
(b) $\Longrightarrow$ (c):
In Lemma 1.5.10 zagen we dat $\mathbb{Q}(\chi) \leq \mathbb{Q}(\zeta)$, met ζ een primitieve eenheidswortel van orde $n := |G|$. Stel dat $j \in \mathbb{N}$ copriem is met n en bekijk het automorfisme $.^j : \zeta \mapsto \zeta^j$ van $\mathbb{Q}(\zeta)$. Stel dat σ de restrictie van $.^j$ is tot $\mathbb{Q}(\chi)$. In het bewijs van Lemma 1.5.10 zagen we dat $\chi(g)$ de som van de eigenwaarden van $\rho(g)$ zijn, die allemaal n-de eenheidswortels zijn. Zij $\{\lambda_1, \ldots, \lambda_{n_i}\}$ de eigenwaarden van $\rho(g)$, dan is $\chi^\sigma(g) = \sum_{l=1}^{n_i} \lambda_l^j$. We zien nu dat λ_l^j juist de eigenwaarden zijn van $\rho(g)^j = \rho(g^j)$, zodat

$$\chi^\sigma(g) = \chi(g^j).$$

Uit (b) volgt dat voor elk automorfisme σ van $\mathbb{Q}(\chi)/Q$ geldt dat

$$\chi^\sigma(g) = \overline{\chi(g)} \qquad \text{of} \qquad \chi^\sigma(g) = \chi(g)$$

zodat

$$\chi(g^j) = \chi(g^{-1}) \qquad \text{of} \qquad \chi(g^j) = \chi(g),$$

Waaruit we kunnen besluiten dat

$$T_{g^j} + T_{g^{-j}} = T_g + T_{g^{-1}}.$$

Uit de lineaire onafhankelijkheid van de afbeeldingen T_g volgt nu dat $T_{g^j} = T_g$ of $T_{g^j} = T_{g^{-1}}$ zodat $g^j \sim g$ of $g^j \sim g^{-1}$, wat de eerste richting bewijst.
(c) $\implies$ (b):
Stel dat $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}$, we breiden σ uit tot een automorfisme van $\mathbb{Q}(\zeta)/\mathbb{Q}$ (Gevolg 1.5.11). Dit automorfisme heeft de vorm $.^j : \zeta \mapsto \zeta^j$. We zien nu dat voor elk karakter $\chi \in \mathrm{Irr}(G)$ geldt dat

$$\chi^\sigma(g) = \chi(g^j).$$

Als we hier (c) toepassen, zien we dat

$$\chi^\sigma(g) = \chi(g) \qquad \text{of} \qquad \chi^\sigma(g) = \chi(g^{-1})$$

zodat

$$\chi^\sigma + \overline{\chi^\sigma} = \chi + \overline{\chi}.$$

Aangezien χ^σ ook een irreducibel karakter is, kunnen we de onafhankelijkheid van de irreducibele karakters gebruiken om te besluiten dat $\chi^\sigma = \chi$ of $\chi^\sigma = \overline{\chi}$. Hieruit volgt dat

$$[\mathbb{Q} : \mathbb{Q}(\chi)] = |\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})| \leq 2$$

en in het geval dat $[\mathbb{Q} : \mathbb{Q}(\chi)] = 2$ weten we dat $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ bestaat uit complexe toevoeging en de identieke afbeelding. We kunnen dus besluiten dat $\mathbb{Q}(\chi)$ ofwel $\mathbb{Q}$ is ofwel een complexe kwadratische uitbreiding. Dit bewijst dat (b) en (c) equivalent zijn. ■

3.4.1 De symmetrische groep S_n is cut

In deze subsectie tonen we kort aan dat de symmetrische groep S_n cut is voor elke $n \in \mathbb{N}$.

Opmerking 3.4.3. Voor een willekeurige cykel $c = (i_1, i_2, \ldots, i_k) \in S_n$ geldt er voor alle $\sigma \in S_n$ dat

$$c^\sigma = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)).$$

Hieruit volgt dat twee cykels uit S_n toegevoegd zijn als en slechts als ze dezelfde lengte hebben. Zij $\sigma, \sigma' \in S_n$ met $\sigma = c_1 c_2 \ldots c_k$, $\sigma' = c_1' c_2' \ldots c_l'$ hun decompositie in disjuncte cykels. Zij ν_i (respectievelijk ν_i') de lengte van c_i (respectievelijk c_i'). We gaan er van uit dat de c_i en c_i' geordend zijn zodanig dat $\nu_1 \leq \cdots \leq \nu_k$ en $\nu_1' \leq \cdots \leq \nu_l'$. De permutaties σ en σ' zijn toegevoegd aan elkaar als en slechts als $k = l$ en $\nu_i = \nu_i'$ voor elke $i \in \{1, \ldots, k\}$.

Lemma 3.4.4. *Zij $\sigma \in S_n$ met $|\sigma| = k$. Als l copriem is met k, dan is $\sigma \sim \sigma^l$.*

Bewijs. Stel dat $\sigma = c_1 c_2 \ldots c_s$ waarbij de c_i paarsgewijs disjuncte cykels zijn. De lengte $\nu_i := \ell(c_i)$ is voor elke $i \in \{1, \ldots, s\}$ een deler van k. De lengtes ν_i zijn dus copriem met l, zodat c_i^l opnieuw een cykel van lengte ν_i is. Zo zien we dat $\sigma \sim \sigma^l$. ■

Stelling 3.4.5. *Zij χ een karakter van S_n, dan is $\chi(g) \in \mathbb{Q}$ voor alle $g \in \mathbb{Q}$.*

Bewijs. Uit het vorig Lemma 3.4.4 volgt dat Stelling 3.4.2(c) geldt zodat $\mathbb{Q}(\chi) \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-d})\}$ met $d \in \mathbb{N}^*$. Zij $g \in S_n$ met $|g| = n$, via Lemma 3.4.4 zien we dat $g \sim g^{n-1} = g^{-1}$. Dit geeft ons dat

$$\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}.$$

Zo zien we dat $\chi(g) \in \mathbb{R}$ is voor elke $g \in G$. We hebben dus dat $\mathbb{Q}(\chi) = \mathbb{Q}$ wat de stelling bewijst. ■

Opmerking 3.4.6. Zo zien we via Stelling 3.4.2 dat S_n cut is. Zo zien we dat

$$Z(\mathcal{U}(\mathbb{Z}S_n)) = \pm Z(S_n) = \pm\{1\}.$$

Groepen G waarvoor $\mathbb{Q}(\chi) = \mathbb{Q}$ voor elk karakter $\chi \in \mathrm{Irr}(G)$ worden ook wel rationele groepen genoemd.

Bibliografie

[Bas66] Hyman Bass. The dirichlet unit theorem, induced characters, and whitehead groups of finite groups. *Topology*, 4(4):391–410, 1966.

[BMP17] Gurmeet K. Bakshi, Sugandha Maheshwary, and Inder Bir S. Passi. Integral group rings with all central units trivial. *Journal of Pure and Applied Algebra*, 221(8):1955–1965, 2017.

[CL65] James A. Cohn and Donald Livingstone. On the structure of group algebras, i. *Canadian Journal of Mathematics*, 17:583–593, 1965.

[Cli80] Gerald H. Cliff. Zero divisors and idempotents in group rings. *Canadian Journal of Mathematics*, 32(3):596–602, 1980.

[Con63] Ian G. Connell. On the group ring. *Canadian Journal of Mathematics*, 15:650–685, 1963.

[EM17] Florian Eisele and Leo Margolis. A counterexample to the first zassenhaus conjecture, 2017.

[Gar21] Giles Gardam. A counterexample to the unit conjecture for group rings. *Annals of Mathematics*, 194(3), nov 2021.

[Her01] Martin Hertweck. A counterexample to the isomorphism problem for integral group rings. *Annals of Mathematics. Second Series*, 1, 07 2001.

[Her07] Martin Hertweck. Partial augmentations and brauer character values of torsion units in group rings, 2007.

[Hig40] Graham Higman. The units of group-rings. *Proceedings of the London Mathematical Society*, s2-46(1):231–248, 1940.

[HP72] I. Hughes and K. R. Pearson. The group of units of the integral group ring zs3. *Canadian Mathematical Bulletin*, 15(4):529–534, 1972.

[Hup13] B. Huppert. *Endliche Gruppen I.* Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[JD15] Eric Jespers and Angel Del Rio Mateos. *Group Ring Groups: Vol 1: Orders and Generic Constructions of Units*, volume 1. De Gruyter, 2015.

[Kap70] Irving Kaplansky. ”problems in the theory of rings”revisited. *The American Mathematical Monthly*, 77(5):445–454, 1970.

[Lam01] T.Y. Lam. *A First Course in Noncommutative Rings.* Graduate Texts in Mathematics. Springer New York, 2001.

[Lam04] T. Y. Lam. *Introduction to Quadratic Forms over Fields.* American Mathematical Society, 2004.

[Lan05] S. Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2005.

[Lev42] F. W. Levi. Ordered groups. *Proceedings of the Indian Academy of Sciences - Section A*, 6:256–263, 1942.

[LP89] I. S. Luthar and I. B. S. Passi. Zassenhaus conjecture fora5. *Proceedings of the Indian Academy of Sciences - Mathematical Sciences*, 99(1):1–5, 1989.

[MRSW87] Z Marciniak, J Ritter, S.K Sehgal, and A Weiss. Torsion units in integral group rings of some metabelian groups, ii. *Journal of Number Theory*, 25(3):340–352, 1987.

[MS84] César Polcino Milies and Sudarshan K. Sehgal. Torsion units in integral group rings of metacyclic groups. *Journal of Number Theory*, 19(1):103–114, 1984.

[Rei75] I. Reiner. *Maximal Orders*. Institute for Research on Poverty Monograph Series. Academic Press, 1975.

[RGH96] D. Robinson, F.W. Gehring, and P.R. Halmos. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 1996.

[RS89] Jürgen Ritter and Sudarshan K. Sehgal. Construction of units in integral group rings of finite nilpotent groups. *Bulletin (New Series) of the American Mathematical Society*, 20(2):165 – 168, 1989.

[RS90] Jürgen Ritter and Sudarshan K. Sehgal. Integral group rings with trivial central units. *Proceedings of the American Mathematical Society*, 108(2):327–329, 1990.

[Seh78] S.K. Sehgal. *Topics in Group Rings*. Monographs and textbooks in pure and applied mathematics. M. Dekker, 1978.

[Tem19] Doryan Temmerman. *Fixed point properties for low rank linear groups over orders and applications to integral group rings*. PhD thesis, Vrije Universiteit Brussel, 2019.

[Zas74] H. Zassenhaus. On the torision units of finite group rings. *In Studies in mathematics*, 1974.