Eenheden in groepsringen over eindige cyclische groepen

Hoofdstuk 1

De basiseigenschappen

1.1 De groepsalgebra $\mathbb{Q}C_n$

Gegeven is de cyclische groep van orde n: $C_n = \{g : g^n = 1\}$. Neem voor elke deler d van n een primitieve d-de machtswortel uit 1 en noteer die met ϵ_d. Noteer de primitieve n-de machtswortel door ζ. Dan bestaat er een $k \in \mathbb{N}$ zodat $\epsilon_d = \zeta^k$. Definieer vervolgens de groepshomomorfismen

$$\rho_d : C_n \longrightarrow \mathbb{C} : g \longmapsto \epsilon_d$$

We kunnen deze groepshomomorfismen uitbreiden tot algebramorfismen tussen $\mathbb{Q}C_n$ en $\mathbb{Q}(\epsilon_d)$. Merk op dat ρ_1 de augmentatie afbeelding is. We weten dat de dimensie van $\mathbb{Q}(\epsilon_d)$ over $\mathbb{Q}$ gelijk is aan $\varphi(d)$.

Neem bijvoorbeeld $G = C_2$, dan definieren we:

$$\rho_1 : \mathbb{Q}C_2 \longrightarrow \mathbb{Q} : a + bg \longmapsto a + b$$
$$\rho_2 : \mathbb{Q}C_2 \longrightarrow \mathbb{Q} : a + bg \longmapsto a - b$$

Nu zijn deze homomorfismen niet injectief. Noteer de kern van ρ_d door K_d. Al deze kernen zijn idealen in de ring $\mathbb{Q}C_n$. Uit de isomorfismestellingen volgt dan dat

$$\frac{\mathbb{Q}C_n}{K_d} \cong \mathbb{Q}(\epsilon_d) = \mathbb{Q}(\zeta^k)$$

In het voorbeeld van $G = C_2$ is $K_1 = \mathbb{Q}(g-1)$ en $K_2 = \mathbb{Q}(g+1)$.

Stelling 1.1. *Als $G = C_n$, dan geldt*

$$\mathbb{Q}C_n \cong \prod_{d|n} \mathbb{Q}(\epsilon_d) = \prod_{k|n} \mathbb{Q}(\zeta^k)$$

Bewijs. Neem: $\rho : \mathbb{Q}C_n \longrightarrow \prod_{d|n} \mathbb{Q}(\epsilon_d) : x \longmapsto (\rho_1(x), \cdots, \rho_d(x), \cdots, \rho_n(x))$. Volgens de Chinese reststelling voor ringen is er voor elk element van $\prod_{d|n} \mathbb{Q}(\epsilon_d)$ een uniek element in $\mathbb{Q}C_n$ modulo $\cap_{d|n} K_d$. Bijgevolg is $\dfrac{\mathbb{Q}C_n}{\cap_{d|n} K_d} \cong \prod_{d|n} \mathbb{Q}(\epsilon_d)$. We weten dat de dimensie van $\mathbb{Q}(\epsilon_d)$ over $\mathbb{Q}$ gelijk is aan $\varphi(d)$. Het getal $\varphi(d)$ is ook het aantal generatoren van de cyclische groep C_d. Omdat ieder element van C_n een cyclische deelgroep genereert en de deelgroepen van C_n van de vorm C_d zijn waarin $d|n$, krijgen we $\sum_{d|n} \varphi(d) = n$. Daarom moet $\cap_{d|n} K_d = 0$ en geldt het gestelde.

□

Merk op dat, onder het gegeven isomorfisme ρ, het element g, in elke component, geprojecteerd wordt op de overeenkomstige primitieve wortel uit 1, namelijk ϵ_d. Enkele eenvoudige voorbeelden:

- $\mathbb{Q}C_2 \cong \mathbb{Q} \otimes \mathbb{Q}$.
- $\mathbb{Q}C_3 \cong \mathbb{Q} \otimes \mathbb{Q}(\omega)$.
- $\mathbb{Q}C_4 \cong \mathbb{Q} \otimes \mathbb{Q} \otimes \mathbb{Q}(i)$.
- $\mathbb{Q}C_5 \cong \mathbb{Q} \otimes \mathbb{Q}(\epsilon_5)$.
- $\mathbb{Q}C_6 \cong \mathbb{Q} \otimes \mathbb{Q} \otimes \mathbb{Q}(\omega) \otimes \mathbb{Q}(\omega)$.
- $\mathbb{Q}C_7 \cong \mathbb{Q} \otimes \mathbb{Q}(\epsilon_7)$.
- $\mathbb{Q}C_8 \cong \mathbb{Q} \otimes \mathbb{Q} \otimes \mathbb{Q}(i) \otimes \mathbb{Q}(\epsilon_8)$.

1.2 De groepsring $\mathbb{Z}C_n$ en zijn eenhedengroep

1.2.1 Algemene resultaten

We kunnen het isomorfisme ρ uit vorig deel ook beperken tot een ringhomomorfisme: $\rho : \mathbb{Z}C_n \longrightarrow \prod_{d|n} \mathbb{Z}(\epsilon_d)$. Nu is $\prod_{d|n} \mathbb{Z}(\epsilon_d)$ de ring der gehelen van $\prod_{d|n} \mathbb{Q}(\epsilon_d)$. De ring van de gehelen van $\mathbb{Q}C_n$ noteren we met H. Bijgevolg is $H \cong \prod_{d|n} \mathbb{Z}(\epsilon_d)$. Het is duidelijk dat $\mathbb{Z}C_n$ een deelring is van H.

We noteren met $U(\mathbb{Z}C_n)$ de groep der eenheden in de groepsring $\mathbb{Z}C_n$. De eenheden van $\mathbb{Z}C_n$ die augmentatie 1 noemen we genormaliseerde eenheden en we noteren de verzameling van alle genormaliseerde eenheden met $V(\mathbb{Z}C_n)$ of $U_1(\mathbb{Z}C_n)$. Het is duidelijk dat:

Stelling 1.2.

$$U(\mathbb{Z}C_n) = \pm V(\mathbb{Z}C_n)$$

.

We kunnen ρ nog verder beperken tot een groepshomomorfisme:
$\rho^* : U(\mathbb{Z}C_n) \longrightarrow U(\prod_{d|n} \mathbb{Z}(\epsilon_d)) = \prod_{d|n} U(\mathbb{Z}(\epsilon_d))$.

Stelling 1.3. *$u \in \mathbb{Z}C_n$ is een eenheid als en slechts als*

$$\forall d|n : \rho_d(u) \in U(\mathbb{Z}(\epsilon_d))$$

.

Het is dus zeer belangrijk de eenheden van $\mathbb{Z}(\epsilon_d)$ te kennen. Volgens Dirichlet's eenheden stelling is de eenheden groep van $\mathbb{Z}(\epsilon_d)$ gelijk aan $T \times F$ waarbij T de groep is van de wortels uit de eenheid in $\mathbb{Q}(\epsilon_d)$ en waarbij F een vrije abelse groep is van rang $\frac{1}{2}\varphi(p) - 1$. Het probleem is om voortbrengende elementen te vinden voor F.

We geven nu nog enkele algemene eigenschappen van de eenhedengroep van $\mathbb{Z}C_n$. We vermelden eerst een resultaat van Higman:

Stelling 1.4. *Elke torsie eenheid in $\mathbb{Z}C_n$ is triviaal.*

Via deze stelling kunnen we volgend resultaat opschrijven:

Stelling 1.5. *Als $n = 1, 2, 3, 4$ of 6, dan is $U(\mathbb{Z}C_n) = \pm C_n$.*

Bewijs. Als d een deler is van 1,2,3,4 of 6, dan is $\mathbb{Z}(\epsilon_d) = \mathbb{Z}, \mathbb{Z}(i)$ of $\mathbb{Z}(\omega)$. De eenhedengroepen van deze groepsringen zijn allemaal eindig. Omdat $U(\mathbb{Z}C_n)$

isomorf is met een deelgroep van $\prod_{d|n} U(\mathbb{Z}(\epsilon_d))$ is dus ook $U(\mathbb{Z}C_n)$ eindig. De stelling van Berman-Higman zegt dat elke centrale torsie eenheid triviaal is. Hieruit volgt het gestelde. □

Wat betreft de algemene structuur van $U(\mathbb{Z}C_n)$, vermelden we de stelling die Higman in 1940 in zijn doctoraatsthesis weergaf:

Stelling 1.6. *$U(\mathbb{Z}C_n) = \pm C_n \times F$, met F een vrij abelse groep met rang $r = \frac{1}{2}(n+1+t_2-2d(n))$. Hierbij is t_2 het aantal elementen in C_n van orde 2 en $d(n)$ het aantal delers van n.*

Noteer met $\Delta(C_n)$ de kern van de augmentatie afbeelding $\mathbb{Z}C_n \longrightarrow \mathbb{Z} : g \longmapsto 1$. Het is een additieve groep, voortgebracht door de elementen $g-1$ met $g \in \mathbb{Z}C_n$. De additieve groep $\Delta^2(C_n)$ wordt gegenereerd door de elementen $(g-1)(h-1)$ met $g, h \in C_n \setminus \{1\}$. Dan is

$$U_1(\mathbb{Z}C_n) = (1 + \Delta(C_n)) \cap U(\mathbb{Z}C_n)$$

Uit stelling 1.6 blijkt dat C_n een directe factor is van $U_1(\mathbb{Z}C_n)$ en dat elk complement van C_n in $U_1(\mathbb{Z}C_n)$ een vrije abelse groep F is. Stelling 1.6 geeft een expliciete formule voor de rang van F. Volgend resultaat van Cliff,Sehgal en Weiss, geeft een manier om een complement van C_n in $U_1(\mathbb{Z}C_n)$ te construeren:

Stelling 1.7. *Als $U_2(\mathbb{Z}C_n) = (1+\Delta^2(C_n)) \cap U(\mathbb{Z}C_n)$, dan is $U_1(\mathbb{Z}C_n) = C_n \times U_2$ en is $U_2(\mathbb{Z}C_n)$ vrij abels met rang $\frac{1}{2}(n+1+a_2-2l)$.*

1.2.2 Eenheden van $\mathbb{Z}(\epsilon_n)$.

Uit vorige eigenschappen is duidelijk dat de ring $\mathbb{Z}(\epsilon_n)$ een belangrijke rol speelt. Vandaar enkele eigenschappen.

- Het cyclotomisch veld $\mathbb{Q}(\epsilon_n)$ ontstaat door aan $\mathbb{Q}$ een primitieve n-de wortel uit de eenheid ϵ_n, toe te voegen.
- Een cyclotomisch veld is het ontbindingsveld van de cyclotomische veelterm
$$\Phi_n(x) = \prod_k (x - e^{2\pi i \frac{k}{n}})$$
en hierbij doorloopt k alle getallen kleiner dan n die onderling ondeelbaar zijn met n.
- De graad van de uitbreiding $\mathbb{Q}(\epsilon_n)$ over $\mathbb{Q}$ is gelijk aan $\varphi(n)$ en is dus gelijk aan de graad van de cyclotomische veelterm.

- De ring der gehelen van $\mathbb{Q}(\epsilon_n)$ is $\mathbb{Z}(\epsilon_n)$. De elementen hiervan, noemen we de cyclotomische gehelen.
- $\mathbb{Q}(\epsilon_n + \epsilon_n^{-1})$ is het maximale reële deelveld van $\mathbb{Q}(\epsilon_n)$.
- De uitbreidingsgraad van $\mathbb{Q}(\epsilon_n)$ over $\mathbb{Q}(\epsilon_n + \epsilon_n^{-1})$ is 2.
- De ring der gehelen van $\mathbb{Q}(\epsilon_n + \epsilon_n^{-1})$ is $\mathbb{Z}(\epsilon_n + \epsilon_n^{-1})$
- De eenheden groep van de ring der cyclotomische gehelen wordt genoteerd door $U(\mathbb{Z}(\epsilon_n))$.
- $U(\mathbb{Z}(\epsilon_n)) = \langle \pm\epsilon_n \rangle \times F$ waarbij F vrij is van rang $\frac{1}{2}\varphi(n) - 1$.
- Eenheden in $\mathbb{Z}(\epsilon_n)$ van de vorm $\frac{1-\epsilon_n^k}{1-\epsilon_n}$ met k en n onderling ondeelbaar noemen we cyclotomische eenheden of circulaire eenheden. Ze genereren, samen met de trivialen eenheden ϵ_n^k een deelgroep van $U(\mathbb{Z}(\epsilon_n))$. Deze deelgroep noemen we de groep van de cyclotomische eenheden. De index van deze deelgroep in $U(\mathbb{Z}(\epsilon_n))$ is steeds eindig als n een priemmacht is.
- De cyclotomische eenheden die in $\mathbb{Z}(\epsilon_n + \epsilon_n^{-1})$ liggen, noemen we de reële cyclotomische eenheden.
- De index van de deelgroep van de reële cyclotomische eenheden in $\mathbb{Z}(\epsilon_n + \epsilon_n^{-1})$ is het klassengetal van $\mathbb{Z}(\epsilon_n + \epsilon_n^{-1})$.
- De cyclotomische eenheden vormen een fundamenteel systeem eenheden van $U(\mathbb{Z}(\epsilon_n))$ als de reële cyclotomische eenheden een fundamenteel systeem vormen van $\mathbb{Z}(\epsilon_n + \epsilon_n^{-1})$ en dit gebeurt enkel als het klassengetal van $\mathbb{Z}(\epsilon_n + \epsilon_n^{-1})$ gelijk is aan 1.
- De deelgroep van de reële cyclotomische eenheden wordt voortgebracht door -1 en $\epsilon_n^{\frac{1-a}{2}} \frac{1-\epsilon_n^a}{1-\epsilon_n}$ met $1 < a < \frac{n}{2}$.
- $U(\mathbb{Z}(\epsilon_n)) = \langle \epsilon_n \rangle \times U(\mathbb{Z}(\epsilon_n + \epsilon_n^{-1}))$.

1.2.3 Constructie mogelijkheden

De vraag stelt zich hoe we effectief eenheden van $U(\mathbb{Z}C_n)$ kunnen construeren. Volgens vorige stelling weten we dat er r eenheden $u_1, u_2, \cdots, u_r$ zijn in $U(\mathbb{Z}C_n)$ zodat elke eenheid u van $U(\mathbb{Z}C_n)$ te schrijven is als $u = \pm g^p . u_1^{n_1} . u_2^{n_2} . \cdots . u_r^{n_r}$ met g het voortbrengend element van C_n, $p \in \mathbb{N}$ en $n_i \in \mathbb{Z}$. We noemen $\{u_1, u_2, \cdots, u_r\}$ een fundamenteel systeem eenheden van $U(\mathbb{Z}C_n)$. We moeten dus proberen zo een fundamenteel systeem eenheden te vinden.

Om zo een fundamenteel systeem eenheden te vinden geven we nu enkele constructies van eenheden in $\mathbb{Z}C_n$:

- De eerste zijn de Bass eenheden of Bass cyclische eenheden, ontdekt door Hyman Bass. Veronderstel dat $g \in C_n$. Neem k onderling ondeelbaar met $|g|$ en m zo dat $k^m \equiv 1 \mod |g|$. Definieer dan:

$$u_{k,m}(g) = (1 + g + g^2 + \cdots + g^{k-1})^m + \frac{1 - k^m}{|g|}(1 + g + \cdots + g^{|g|-1})$$

De groep voortgebracht door alle Bass eenheden van $\mathbb{Z}C_n$ noteren we met $Bass(G)$. Deze groep wordt voortgebracht door een eindig aantal Bass eenheden, namelijk deze van de vorm u_{k,m_k} met m_k de orde van k in $U(\mathbb{Z}_{|g|})$ en $1 \leq k < |g|$. Alle Bass eenheden zijn torsie vrij, tenzij $k \equiv \pm 1 \mod |g|$.

Stelling 1.8. *Als $G = C_n$, dan heeft de groep $Bass(G)$ eindige index in $\mathbb{Z}C_n$.*

- Een andere interessante constructie van eenheden werd gegeven door Hoechsmann: Als i en j onderling ondeelbaar zijn met n en $ik \equiv 1 \mod n$, dan is $u_{i,j}(g)$ een eenheid van $\mathbb{Z}C_n$.

$$u_{i,j}(g) = (1+g^j+\cdots+g^{j(i-1)})(1+g^i+\cdots+g^{(k-1)i})+\frac{1-ik}{n}(1+g+\cdots+g^{n-1})$$

Hierbij is g het voortbrengend element van C_n. We noemen u een Hoechsmann eenheid of construeerbare eenheid. Met $H(C_n)$ noteren we de groep voortgebracht door alle eenheden van die vorm. Net als de de groep van de Bass eenheden, zal ook deze groep een eindige index hebben in $\mathbb{Z}C_n$. Alleen blijkt de index van groep van de Hoechmann eenheden veel kleiner dan de index van de groep van de Bass eenheden. Zowel de Bass eenheden als de Hoechsmann eenheden hebben steeds augmentatie 1.

Stelling 1.9. *Als $G = C_n$, dan heeft de groep $H(G)$ eindige index in $\mathbb{Z}C_n$.*

De verzameling $\{u_{i,j}\}$ is als voortbrengend deel van $H(C_n)$ veel te groot. Stel $m = \exp C_n$ en $H_m = \mathbb{Z}_m^\times/\{\pm 1\}$. Veronderstel dat H_m een cyclische groep is en dat $i \in \mathbb{Z}$ een generator van H_m induceert. Dan zal $H(C_n)$ gegenereerd worden door $\pm C_n$, samen met de elementen $u_{i,i}(z)$ waarbij z de groep C_n doorloopt.

1.2.4 Symmetrische eenheden

Als $u = \sum_{g \in C_n} u_g g$, dan definiëren we $u^* = \sum_{g \in C_n} u_g g^{-1}$. Een element u noemen we symmetrisch als $u = u^*$. De verzameling van alle symmetrische elementen is de deelring $\mathbb{Z}\left[g + g^{-1}\right]$ van $\mathbb{Z}C_n$. Hierbij is $|g| = n$. Deze deelring wordt ook genoteerd als ZC_n^+. De groep van de eenheden van deze deelring, noemt men ook wel de groep van de symmetrische eenheden, en is gedefinieerd als

$$U(ZC_n^+) = \{\gamma \in U(ZC_n) : \gamma = \sum_{i=0}^{n-1} \gamma_i g^i \text{ met } \gamma_i = \gamma_{n-i}\}$$

Stelling 1.10. *Elke $\gamma \in U(\mathbb{Z}C_n^+)$ kan geschreven worden als*

$$\gamma = \gamma_0 + \sum_{i=1}^{k} \gamma_i C_i \text{ met } C_i = g^i + g^{-i}$$

Bewijs. Als $n = 2k + 1$ is dit evident. Neem dan $n = 2k$, dan is $\gamma = \gamma_0 + \gamma'_k a^k + \sum_{i=1}^{k-1} \gamma_i C_i$. De augmentatie van γ (die ± 1 moet zijn) is dan gelijk aan $\gamma_0 + \gamma'_k + 2\sum_{i=1}^{k-1} \gamma_i$. Modulo 2 gerekend geeft dit dat $\gamma_0 + \gamma'_k \equiv 1 \mod 2$. Neem voor γ_0 een oneven getal, dan is γ'_k even en dus te schrijven als $\gamma'_k = 2\gamma_k$. Hieruit volgt dat $\gamma'_k g^k = \gamma_k(g^k + g^{-k})$. daarmee is het gestelde bewezen. □

Stelling 1.11. *Als $u \in U_2(\mathbb{Z}C_n)$ dan is u symmetrisch.*

Bewijs. Neem $u \in U(\mathbb{Z}C_n)$ en stel $v = u^* u^{-1}$. Dan is $\text{aug}(v) = \text{aug}(u)$. $(\text{aug}(u))^{-1} = 1$. Neem vervolgens $v.v^*$, dan is de coëfficiënt van 1 in $v.v^*$ gelijk aan $\sum_{g \in C_n} v_g^2$. Hieruit volgt dat $v.v^* = 1$ als en slechts als $v \in \pm C_n$. Maar omdat de augmentatie van $v.v^*$ gelijk is aan 1, zal dus $v.v^* \in C_n$. Als nu ook $u \in U_2(\mathbb{Z}C_n)$ zal ook v behoren tot $1 + \Delta^2(C_n)$. In het bijzonder zal $v \in C_n \cap (1 + \Delta^2(C_n))$. Volgens de stelling van Cliff,Sehgal,Weiss moet $v = 1$ en dus is $u = u^*$.

□

Als n oneven is is dan is $U(\mathbb{Z}C_n^+) = U_2(\mathbb{Z}C_n)$, en als $n = 2k$ dan is $U(\mathbb{Z}C_n^+) = \{g^k\} \times U_2(\mathbb{Z}C_n)$. Met andere woorden:

Stelling 1.12. *$U(\mathbb{Z}C_n)$ is het direct product van de triviale eenheden en een torsie vrije groep van symmetrische eenheden.*

Ook hier stelt het probleem zich om voldoende symmetrische eenheden te vinden. We onthouden volgend resultaat:

Stelling 1.13. *Als g een eindig element is met orde relatief priem met 6, dan is $u = g + g^{-1} - 1$ een symmetrische eenheid die geen positieve macht is van een andere eenheid.*

Hoofdstuk 2

$U(\mathbb{Z}C_p)$ met p priem

2.1 Enkele resultaten

Voor $p = 2$ en $p = 3$ weten we al dat er enkel triviale eenheden zijn . Veronderstellen we verder dus dat p een priemgetal groter dan 3 is.

Stelling 2.1.
$$\mathbb{Q}(C_p) \cong \mathbb{Q} \otimes \mathbb{Q}(\epsilon_p)$$

Bewijs. Omdat p een priemgetal is heeft het slechts 2 delers: 1 en p zelf. Hieruit volgt het gestelde. □

Noteer verder, in plaats van ρ_p, kortweg $\rho : \mathbb{Z}(C_p) \longrightarrow \mathbb{Z}(\epsilon_p) : g \longmapsto \epsilon_p$.

Stelling 2.2.
$$ker\ \rho = \mathbb{Z}(1 + g + \cdots + g^{p-1})$$

Bewijs. $x = \sum a_n g^n \in \ker\rho \Longleftrightarrow \sum a_n \epsilon_p^n = 0$. Omdat $1 + \epsilon_p + \cdots + \epsilon_p^{n-1} = 0$ volgt hieruit dat $a_0 = a_1 = \cdots = a_n$. Hieruit volgt het gevraagde. □

Stelling 2.3. $u \in U(\mathbb{Z}C_p) \Longleftrightarrow aug(u) = \pm 1$ *en* $\rho(u) \in U(\mathbb{Z}(\epsilon_p))$.

Over de eenheden van $\mathbb{Z}(\epsilon_p)$ weten we: $U(\mathbb{Z}(\epsilon_p)) = \pm\langle\epsilon_p\rangle \times F$ met F vrij abels van rang $\frac{1}{2}\varphi(p) - 1 = \frac{1}{2}(p-3)$. Er bestaan dus $r = \frac{1}{2}(p-3)$ eenheden $u_1, \cdots, u_r$ van $\mathbb{Z}(\epsilon_p)$ zodat elke eenheid kan geschreven worden onder de vorm

$u = (-\epsilon_p)^k . u_1^{n_1} .. u_2^{n_2} \cdots . u_r^{n_r}$. Zo een stel $\{u_1, \cdots, u_r\}$ noemen we een fundamenteel systeem van eenheden van $\mathbb{Z}(\epsilon_p)$. De cyclotomische eenheden genereren een deelgroep met eindige index in $U(\mathbb{Z}(\epsilon_p))$. In bepaalde gevallen vormen ze een fundamenteel systeem.

Stelling 2.4.

$$U(\mathbb{Z}C_p) = \pm C_p \times F \text{ met rang } F = \frac{1}{2}(p-3)$$

$$U(\mathbb{Z}C_p^+) = \pm C_p \times F^+ \text{ met rang } F^+ = \frac{1}{2}(p-3)$$

Bewijs. We weten dat $U(\mathbb{Z}C_n) = \pm C_n \times F$, met F een vrij abelse groep met rang $r = \frac{1}{2}(n+1+t_2-2d(n))$. Voor $n = p$ priem wordt $r = \frac{1}{2}(p+1+0-2.2) = \frac{1}{2}(p-3)$. Verder is $r^+ = \frac{1}{2}(p-1) - 1 = \frac{1}{2}(p-3)$. □

Stelling 2.5. *Het groepshomomorfisme ρ^* tussen $U(\mathbb{Z}C_p)$ en $U(\mathbb{Z}(\epsilon_p)$ is injectief.*

Bewijs. Veronderstel dat $u \in U(\mathbb{Z}C_p)$ en dat $\rho^*(u) = 1$. Dan is $u = 1 + k(1 + g + \cdots + g^{p-1})$ en $\text{aug}(u) = \pm 1$. Maar dan moet $1 + pk = \pm 1$. In het geval dat $1+kp = 1$, vinden we dat $k = 0$ en dus is $u = 1$. In het geval dat $1+kp = -1$, zou $kp = 2$ en omdat p een priemgetal is groter dan 2, is dit onmogelijk. Bijgevolg is $\ker(\rho^*) = 1$ en dus is ρ^* injectief. □

Stelling 2.6. *$\{u_1, u_2, \cdots, u_r\}$ met $r = \frac{1}{2}(p-3)$ is een fundamenteel systeem van eenheden voor $\mathbb{Z}C_p$ als en slechts als $\rho(\pm C_p, u_1, u_2, \cdots, u_r)$ een deelgroep is van $U(\mathbb{Z}(\epsilon_p))$ met index $\frac{1}{2}(p-1)$.*

Bewijs. Beschouw in de ring $\mathbb{Z}(\epsilon_p)$ het hoofdideaal $(\epsilon_p - 1)$. Nu is $-((p-1) + (p-2)\epsilon_p + \cdots + \epsilon_p^{p-2})(\epsilon_p - 1) = p$ zodat $(\epsilon_p - 1) \cap \mathbb{Z} = p\mathbb{Z}$ en dus is $(\epsilon_p - 1)$ een priemideaal is van $\mathbb{Z}(\epsilon_p)$. Bijgevolg is $\dfrac{\mathbb{Z}(\epsilon)}{(\epsilon_p - 1)} \cong \mathbb{F}_p$, het eindige veld met p elementen. Bestuderen we de doorsnede van deze restklassen met $U(\mathbb{Z}(\epsilon_p))$. De restklasse $(\epsilon_p - 1)$ heeft geen elementen met $U(\mathbb{Z}(\epsilon_p))$ gemeen, zodat er slechts $p-1$ restklassen zijn. Omdat $\epsilon_p^i = 1 + (\epsilon_p^i - 1) = 1 + (\epsilon_p - 1)(\epsilon_p^{i-1} + \cdots + \epsilon_p + 1)$ zal $\epsilon_p^i \equiv 1 \mod (\epsilon_p - 1)$. Voor $x = x_0 + x_1\epsilon_p + x_2\epsilon_p^2 + \cdots + x_{p-2}\epsilon_p^{p-2}$ vinden

we dat $x \equiv x_0 + x_1 + \cdots + x_{p-2} \mod (\epsilon_p - 1)$. We proberen nu te bewijzen dat $\rho^*(V(\mathbb{Z}(C_p))$ gelijk is aan de doorsnede van $U(\mathbb{Z}(\epsilon_p))$ met de restklasse $1 + (\epsilon_p - 1)$.

- Als $x \in \rho^*(V(\mathbb{Z}(C_p)))$ bestaat er een $u \in V(\mathbb{Z}(C_p))$ zodat $\rho^*(u) = x$ en aug $(u) = 1$. Stel $u = d_0 + d_1 g + \cdots + d_{p-1} g^{p-1}$, dan is $x = d_0 + d_1\epsilon_p + \cdots + d_{p-1}\epsilon_p^{p-1} \equiv d_0 + d_1 + \cdots + d_{p-1} \equiv 1 \mod (\epsilon_p - 1)$. Dus x zit in de doorsnede van $U(\mathbb{Z}(\epsilon_p))$ met de restklasse $1 + (\epsilon_p - 1)$.
- Neem omgekeerd x in de doorsnede van $U(\mathbb{Z}(\epsilon_p))$ met de restklasse $1+(\epsilon_p-1)$. Dan is $x = d_0+d_1\epsilon_p+\cdots+d_{p-1}\epsilon_p^{p-2}$ en $x \equiv 1+(\epsilon_p-1)$. Hieruit volgt dat $d_0+d_1+\cdots+d_{p-2} \equiv 1 \mod (\epsilon_p)$. Bijgevolg is $d_0+d_1+\cdots+d_{p-2} = 1+pk$. Construeer $u = (d_0 - k) + (d_1 - k)g + \cdots + (d_{p-2} - k)g^{p-2} - kg^{p-1}$. Dan is $\rho^*(u) = x$ en $\text{aug}(x) = 1$ en dus is $x \in \rho^*(V(\mathbb{Z}(C_p)))$

Het is dus duidelijk dat de index van $\rho^*(V(\mathbb{Z}(C_p)))$ in $U(\mathbb{Z}(\epsilon_p))$ gelijk is aan $p - 1$. De elementen met augmentatie -1 corresponderen met de doorsnede van $U(\mathbb{Z}(\epsilon_p))$ met de restklasse $-1 + (\epsilon_p - 1)$. Dus is de index $\rho^*(U(\mathbb{Z}(C_p)))$ in $U(\mathbb{Z}(\epsilon_p))$ gelijk is aan $\frac{1}{2}(p - 1)$ en hieruit volgt het gestelde. □

Noteren we met $U_1(\mathbb{Z}(\epsilon_p))$ de eenheden $\sum_{i=0}^{p-2} a_i\epsilon_p^i$ in $\mathbb{Z}(\epsilon_p)$ waarvoor geldt dat $a_0 + \cdots + a_{p-2} \equiv 1 \mod (\epsilon_p - 1)$, wat hetzelfde betekent als $a_0 + \cdots + a_{p-2} \equiv 1 \mod p$. Dan hebben we in vorige stelling bewezen dat

$$U_1(\mathbb{Z}C_p) \cong U_1(\mathbb{Z}(\epsilon_p))$$

Bovendien heeft $U_1(\mathbb{Z}(\epsilon_p))$ index $p - 1$ in $U(\mathbb{Z}(\epsilon_p))$.

2.2 Voorbeeld 1: $U(\mathbb{Z}(C_5))$

2.2.1 Werkwijze 1

Stelling 2.7. *$U(\mathbb{Z}(C_5)) = \pm C_5 \times F$ met F vrij abels van rang 1.*

Bewijs. Volgens stelling 2.4 is de rang van F gelijk aan $r = \frac{1}{2}(5 - 3) = 1$. □

Stelling 2.8. *$u \in \mathbb{Z}C_5$ is een eenheid als en slechts als aug$(u) = \pm 1$ en $\rho(u) = \pm\epsilon_5^k(1 + \epsilon_5)^l$ met $k, l \in \mathbb{Z}$.*

Bewijs. Volgens stelling 2.3 is $u \in \mathbb{Z}C_5$ een eenheid als en slechts als $\text{aug}(u) = \pm 1$ en $\rho(u) \in U(\mathbb{Z}\epsilon_5)$. De cyclotomische eenheden van $\mathbb{Z}(\epsilon_5)$ zijn $1, \epsilon_5 + 1, \epsilon_5^2 + \epsilon_5 + 1 = -\epsilon_5^3(1+\epsilon_5)$ en $\epsilon_5^3+\epsilon_5^2+\epsilon_5+1 = -\epsilon_5^4$. Uit de theorie van de cyclotomische

gehelen weten we dat de torsie vrije rang van de eenheden groep van $\mathbb{Z}(\epsilon_5)$ gelijk is aan $\frac{1}{2}(5-3)=1$ en dat $\{1+\epsilon_5\}$ een fundamenteel systeem eenheden van $U(\mathbb{Z}(\epsilon_5))$ is. Bijgevolg is elke eenheid van $\mathbb{Z}(\epsilon_5)$ van de vorm $\pm\epsilon_5^k(1+\epsilon_5)^l$ met $k,l\in\mathbb{Z}$. □

Stelling 2.9.

$$U(\mathbb{Z}C_5)=\pm C_5\times\langle g^2+g^3-1\rangle$$

Bewijs. Omdat de kern van ρ gelijk is aan $\mathbb{Z}(1+g+g^2+g^3+g^4)$, zal $u\in U(\mathbb{Z}C_5)$ als en slechts als $u=\pm g^k(1+g)^l+m(1+g+g^2+g^3+g^4)$ en $\mathrm{aug}(u)=\pm1$. We zoeken naar niet triviale eenheden, dus nemen we $k=0$. Als $l=1$, dan is $\mathrm{aug}(u)=2+5m$ en dit kan nooit gelijk zijn aan ±1 voor een gehele waarde van m. Neem $l=2$, dan is $\mathrm{aug}(u)=4+5m$ en dit wordt -1 voor $m=-1$. Dan is $u=(1+g)^2-(1+g+g^2+g^3+g^4)=-g(-1+g^2+g^3)$.

Stel $v=-1+g^2+g^3$, dan bewijzen we nog dat $\{v\}$ een fundamenteel systeem van eenheden is in $\mathbb{Z}C_5$. Hiervoor bewijzen we dat $\rho^*(\pm C_5,v)$ een deelgroep met index $\frac{1}{2}(5-1)=2$ is in $U(\mathbb{Z}(\epsilon_5))$. Uit $u=-gv$ volgt dat $\rho(v)=-\epsilon_5^4(1+\epsilon_5)^2$. Bijgevolg is $\rho^*(\pm C_5,v)$ de deelgroep van $U(\mathbb{Z}(\epsilon_5))$ met elementen van de vorm $\pm\epsilon_5^k(1+\epsilon_5)^{2l}$. Omdat elke eenheid in $\mathbb{Z}(\epsilon_5)$ van de vorm $(-\epsilon_5)^k(1+\epsilon_5)^l$ is met $k,l\in\mathbb{Z}$, heb je voor de exponent van ϵ_5+1 ofwel even getallen ofwel oneven getallen en dus is de index van $\rho^*(\pm C_5,v)$ in $U(\mathbb{Z}(\epsilon_5))$ inderdaad 2.

□

2.2.2 Werkwijze 2

We kunnen dit resultaat ook verkrijgen via een andere weg:

$$\begin{array}{ccc}\mathbb{Z}C_5 & \longrightarrow & \mathbb{Z}(\epsilon_5)\\ \downarrow & & \downarrow\\ \mathbb{Z} & \longrightarrow & \mathbb{Z}_5\end{array}$$

Het linkerhomomorfisme is de augmentatieafbeelding. Het rechts homomorfisme beeldt elk element af op de som van zijn coëfficiënten modulo 5. De elementen $a\in\mathbb{Z}$ en $\sum_{i=0}^3 a_i\epsilon_5^i\in\mathbb{Z}(\epsilon_5)$ hebben hetzelfde beeld als $\sum a_i=a+5k$. Hiermee correspondeert het unieke element $\sum_i a_ig^i-k(1+g+g^2+g^3+g^4)$ in $\mathbb{Z}C_5$. Dus:

Stelling 2.10. *$\mathbb{Z}C_5$ is het vezelproduct van $\mathbb{Z}(\epsilon_5)$ over $\mathbb{Z}$.*

Overgang naar de groep der eenheden geeft:

$$\begin{array}{ccc} U(\mathbb{Z}C_5) & \longrightarrow & U(\mathbb{Z}(\epsilon_5)) \\ \downarrow & & \downarrow \\ \{+1,-1\} & \longrightarrow & \mathbb{Z}_5^\times \end{array}$$

Elke eenheid van $\mathbb{Z}(\epsilon_5)$ geeft dan een eenheid van $\mathbb{Z}C_5$ als de som der coëfficiënten gelijk is aan $\pm 1 \mod 5$. Dit geeft dan hetzelfde resulaat dat we hierboven verkregen hebben.

2.2.3 Werkwijze 3

We kunnen ook werken met de groep van de symmetrische eenheden. Omdat die ook rang 1 heeft, volstaat het 1 symmetrische eenheid te vinden die de groep van alle symmetrische eenheden genereert. Nu heeft g orde 5 en dus een orde die relatief priem is met 6, dus geldt volgens stelling 1.13 :

Stelling 2.11.

$$U(\mathbb{Z}C_5) = \pm C_5 \times \langle g + g^4 - 1 \rangle$$

Merk ook op dat stelling 2.9 ook gegeven wordt met een symmetrische eenheid in het fundamenteel systeem en dat g^2+g^3-1 een macht moet zijn van $g+g^4-1$. Er geldt inderdaad dat $g^2 + g^3 - 1 = (g + g^4 - 1)^{-1}$.

We kunnen die symmetrische eenheid ook vinden zonder stelling 1.13 te gebruiken. Veronderstel dus dat γ een symmetrische eenheid is die een generator is van het torsievrij deel. Veronderstel ook dat γ augmentatie 1 heeft. Dan is

$$\gamma = \gamma_0 + \gamma_1(g + g^{-1}) + \gamma_2(g^2 + g^{-2})$$

met $\gamma_0 + 2\gamma_1 + 2\gamma_2 = 1$.

Noteer verder $\alpha = \epsilon_5 + \epsilon_5^{-1}$. Dan is het duidelijk dat $\epsilon_5^2 + \epsilon_7^{-2} = \alpha^2 - 2$. Omdat $1 + \epsilon_5 + \epsilon_5^2 + \epsilon_5^3 + \epsilon_5^4 = 0$ zal

$$\alpha^2 + \alpha - 1 = 0$$

Definieer tenslotte $\rho : \mathbb{Z}C_5 \longrightarrow \mathbb{Z}(\epsilon_5) : g \longmapsto \epsilon_5$. Dan is:

$$\begin{aligned} \rho(\gamma) =& \gamma_0 + \gamma_1\alpha + \gamma_2(-1-\alpha) \\ =& (\gamma_0 - \gamma_2) + (\gamma_1 - \gamma_2)\alpha \\ =& (1 - 2\gamma_1 - 3\gamma_2) + (\gamma_1 - \gamma_2)\alpha \end{aligned}$$

Omdat $\rho(\gamma)$ een eenheid is in $\mathbb{Z}[\alpha] = \{x + y\alpha$ met $x, y, z \in \mathbb{Z}$ en $\alpha^2 + \alpha - 1 = 0\}$ moeten we fundamantele eenheden zoeken in $\mathbb{Z}[\alpha]$. De torsie vrije rang van

$U(\mathbb{Z}[\alpha])$ is $\frac{1}{2}\varphi(5) - 1 = 1$. We hebben dus 1 fundamentele eenheid nodig en deze is α. Merk op dat $\alpha^{-1} = 1 + \alpha$. Dus is $U(\mathbb{Z}[\alpha]) = \langle\alpha\rangle$.

- $\rho(\gamma)$ kan nooit gelijk zijn aan α of α^{-1}. Dit kan je bewijzen door de coëfficiënten te vergelijken en het stelsel op te lossen.
- Voor $\rho(\gamma) = -\alpha^2$ vinden we $\gamma_0 = -1, \gamma_1 = 1, \gamma_2 = 0$. Dit geeft $\gamma = -1 + (g + g^{-1})$.
- Voor $\rho(\gamma) = -\alpha^{-2}$ vinden we $\gamma = g^2 + g^{-2} - 1$

En zo vinden we hetzelfde resultaat als vroeger.

2.2.4 Speciale eenheden

Waar bevinden zich de Bass-eenheden? We berekenen $u_{2,4}(g) = (1 + g)^4 + \frac{1 - 2^4}{5}(1+g+g^2+g^3+g^4) = -2+g+3g^2+g^3-2g^4 = g^2\big(3+(g+g^4)-2(g^2+g^3)\big)$ en we zullen deze eenheid verder noteren als u. Deze eenheid wordt door ρ afgebeeld op $(1 + \epsilon_5)^4$. In een vorig artikel over Bass eenheden vonden we bovendien dat:

k	g	g^2	g^3	g^4
1	1	1	1	1
2	u	$u^{-1}g$	$u^{-1}g^3$	ug^4
3	ug^2	u^{-1}	$u^{-1}g^4$	ug^2
4	g^3	g	g^4	g^2

Zo bekomen we volgend resultaat:

Stelling 2.12. *De index van $Bass(C_5)$ in $U(\mathbb{Z}(C_5))$ bedraagt 4. De index van $Bass(C_5)$ in $V(\mathbb{Z}(C_5))$ bedraagt 2.*

Als we de Hoechsmann eenheden berekenen voor $i = j = 2$ en $k = 3$, dan vinden we $u = 1 - g + g^2$. Dit is een genormaliseerde eenheid want $\rho^*(u) = -\epsilon_5^2(1 + \epsilon_5)^{-2} \in U(\mathbb{Z}(\epsilon_5))$ en $\text{aug(u)} = 1$. Uit het bewijs van stelling 2.9 volgt dan:

Stelling 2.13. *De index van $H(C_5)$ in $U(\mathbb{Z}(C_5))$ bedraagt 2. $H(C_5)$ genereert gans $V(\mathbb{Z}(C_5))$.*

2.3 Voorbeeld 2: $U(\mathbb{Z}(C_7))$

2.3.1 Werkwijze 1

Stelling 2.14. *$U(\mathbb{Z}(C_7)) = \pm C_7 \times F$ met F vrij abels van rang 2.*

Bewijs. Volgens stelling 2.4 is de rang van F gelijk aan $r = \frac{1}{2}(7-3) = 2$. □

Stelling 2.15. *$u \in \mathbb{Z}C_7$ is een eenheid als en slechts als $aug(u) = \pm 1$ en $\rho(u) = \pm\epsilon_7^k(\epsilon_7+1)^p(\epsilon_7^2+\epsilon_7+1)^q$ met $k,p,q \in \mathbb{Z}$.*

Bewijs. Volgens stelling 2.3 is $u \in \mathbb{Z}C_7$ een eenheid als en slechts als $\text{aug}(u) = \pm 1$ en $\rho(u) \in U(\mathbb{Z}(\epsilon_7))$. De cyclotomische eenheden van $\mathbb{Z}(\epsilon_7)$ zijn $1, \epsilon_7+1, \epsilon_7^2+\epsilon_7+1, \epsilon_7^3+\epsilon_7^2+\epsilon_7+1 = -\epsilon_7^4(\epsilon_7^2+\epsilon_7+1), \epsilon_7^4+\epsilon_7^3+\epsilon_7^2+\epsilon_7+1 = -\epsilon_7^5(\epsilon_7+1)$ en $\epsilon_7^5+\epsilon_7^4+\epsilon_7^3+\epsilon_7^2+\epsilon_7+1 = -\epsilon_7^6$. Uit de theorie van de cyclotomische eenheden weten we dat de torsie vrije rang van de eenheden groep van $\mathbb{Z}(\epsilon_7)$ gelijk is aan $\frac{1}{2}(7-3) = 2$ en dat $\{\epsilon_7+1, \epsilon_7^2+\epsilon_7+1\}$ een fundamenteel systeem eenheden van $U(\mathbb{Z}(\epsilon_7))$ vormt. Bijgevolg is elke eenheid van $\mathbb{Z}(\epsilon_7)$ van de vorm $\pm\epsilon_7^k(\epsilon_7+1)^p(\epsilon_7^2+\epsilon_7+1)^q$ met $k,p,q \in \mathbb{Z}$. □

Stelling 2.16.

$$U(\mathbb{Z}C_7) = \pm C_7 \times \langle 1-g^2-g^5\rangle \times \langle 1+g-g^4\rangle$$

Bewijs. Omdat de kern van ρ gelijk is aan $\mathbb{Z}(1+g+g^2+g^3+g^4+g^5+g^6)$, zal $u \in U(\mathbb{Z}C_7)$ als en slechts als $u = \pm g^k(1+g)^p(1+g+g^2)^q) + m(1+g+g^2+g^3+g^4+g^5+g^6)$ en $\text{aug}(u) = \pm 1$. We zoeken naar niet triviale eenheden, dus nemen we $k = 0$. Voor $p = 3$ en $q = 0$ is aug $(u) = 8+7m$ en dat kan gelijk worden aan 1 voor $m = -1$. Dan is $u = 2g+2g^2-g^4-g^5-g^6$. Er zijn echter elegantere eenheden te vinden voor $p = 2, q = -1$ en $p = -1, q = 2$. De gevonden eenheden zijn dan respectievelijk $u = 1-g^2-g^5$ en $u = g(1+g-g^4)$. Neem $u = 1-g^2-g^5$ en $v = 1+g-g^4$, dan bewijzen we nog dat $\{u,v\}$ een fundamenteel systeem van eenheden is in $\mathbb{Z}C_7$. Hiervoor bewijzen we dat $\rho^*(\pm C_7, u, v)$ een deelgroep met index $\frac{1}{2}(7-1) = 3$ is in $U(\mathbb{Z}(\epsilon_7))$. Noteer $a = \epsilon_7+1$ en $b = \epsilon_7^2+\epsilon_7+1$. Nu is $\rho^*(u) = a^2b^{-1}$ en $\rho^*(v) = \epsilon_7^6a^{-1}b^2$. Bijgevolg is $\rho^*(\pm C_7, u, v)$ de deelgroep van $U(\mathbb{Z}\epsilon_7)$ met alle elementen van de vorm $\pm\epsilon_7^k a^x b^y$ waarbij $x \equiv y \mod 3$. De doorsnede van $U(\mathbb{Z}C_7)$ met de nevenklassen $2+(\epsilon_7-1)$ en $5+(\epsilon_7-1)$ is dan $a\rho^*(\pm C_7, u, v)$ en bevat alle elementen van de vorm $\pm\epsilon_7^k a^x b^y$

waarbij $x - y \equiv 1 \mod 3$. De doorsnede van $U(\mathbb{Z}C_7)$ met de nevenklassen $3 + (\epsilon_7 - 1)$ en $4 + (\epsilon_7 - 1)$ is dan $b\rho^*(\pm C_7, u, v)$ en bevat alle elementen van de vorm $\pm\epsilon_7^k a^x b^y$ waarbij $x - y \equiv 2 \mod 3$. Het is dus duidelijk dat de index van $\rho(\pm C_7, u, v)$ in $U(\mathbb{Z}(\epsilon_7))$ gelijk is aan 3. Hieruit volgt het gestelde.

□

2.3.2 Werkwijze 2

Omdat g orde 7 heeft en dat dit onderling ondeelbaar is met 6, weten we dat $g + g^{-1} - 1$ een fundamentele symmetrische eenheid is. Maar we hebben er 2 nodig. Veronderstel dus dat γ een symmetrische eenheid is die een generator is van het torsievrij deel. Veronderstel ook dat γ augmentatie 1 heeft. Dan is

$$\gamma = \gamma_0 + \gamma_1(g + g^{-1}) + \gamma_2(g^2 + g^{-2}) + \gamma_3(g^3 + g^{-3})$$

met $\gamma_0 + 2\gamma_1 + 2\gamma_2 + 2\gamma_3 = 1$.

Noteer verder $\alpha = \epsilon_7 + \epsilon_7^{-1}$. Dan is het duidelijk dat $\epsilon_7^2 + \epsilon_7^{-2} = \alpha^2 - 2$ en $\epsilon_7^3 + \epsilon_7^{-3} = \alpha^3 - 3\alpha$. Omdat $1 + \epsilon_7 + \epsilon_7^2 + \epsilon_7^3 + \epsilon_7^4 + \epsilon_7^5 + \epsilon_7^6 = 0$ zal

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$$

Definieer tenslotte $\rho : \mathbb{Z}C_7 \longrightarrow \mathbb{Z}(\epsilon_7) : g \longmapsto \epsilon_7$. Dan is:

$$\begin{aligned}\rho(\gamma) =& \gamma_0 + \gamma_1\alpha + \gamma_2(\alpha^2 - 2) + \gamma_3(\alpha^3 - 3\alpha)\\ =& (\gamma_0 - 2\gamma_2) + (\gamma_1 - 3\gamma_3)\alpha + \gamma_2\alpha^2 + \gamma_3\alpha^3\\ =& (1 - 2\gamma_1 - 4\gamma_2 - \gamma_3) + (\gamma_1 - \gamma_3)\alpha + (\gamma_2 - \gamma_3)\alpha^2\end{aligned}$$

Omdat $\rho(\gamma)$ een eenheid is in $\mathbb{Z}[\alpha] = \{x + y\alpha + z\alpha^2$ met $x, y, z \in \mathbb{Z}$ en $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0\}$ moeten we de fundamantele eenheden zoeken in $\mathbb{Z}[\alpha]$. Omdat $\frac{1}{2}\varphi(7) - 1 = 2$ hebben we 2 fundamentele eenheden nodig. Dit zijn $\alpha + 1$ en $\alpha^2 - 1$. Omdat $\alpha^3 + \alpha^2 - \alpha - 1 = \alpha$ en dus $\alpha = (\alpha + 1)(\alpha^2 - 1)$ is ook α een eenheid en is $U(\mathbb{Z}[\alpha]) = \langle \alpha, \alpha^2 - 1 \rangle$.

- $\rho(\gamma)$ kan nooit gelijk zijn aan $\alpha, \alpha^{-1}, \alpha^2 - 1$ of $(\alpha^2 - 1)^{-1}$. Hierbij is $\alpha^{-1} = \alpha^2 + \alpha - 2$ en $(\alpha^2 - 1)^{-1} = \alpha^2 + \alpha - 1$. Dit kan je bewijzen door de coëfficiënten te vergelijken en het stelsel op te lossen.
- $\rho(\gamma)$ kan evenmin het product zijn van twee factoren uit $\alpha, \alpha^{-1}, \alpha^2 - 1$ en $(\alpha^2 - 1)^{-1}$. Verklaring idem.
- Bij dubbele producten lukt het wel: $\rho(\gamma) = \alpha^3$ als $\gamma_0 = -1, \gamma_1 = 2, \gamma_2 = -1$ en $\gamma_3 = 0$. Dit geeft $\gamma = -1 + 2(g + g^{-1}) - (g^2 + g^{-2})$.
- Bij $\rho(\gamma) = \alpha^{-1}(\alpha^2 - 1)^2 = \alpha - 1$ vinden we $\gamma = g + g^{-1} - 1$

Stelling 2.17.

$$U(\mathbb{Z}C_7) = \pm C_7 \times \langle -1 + g + g^{-1} \rangle \times \langle -1 + 2(g + g^{-1}) - (g^2 + g^{-2}) \rangle$$

Hoofdstuk 3

$U(\mathbb{Z}C_n)$ met n een priemmacht

3.1 Enkele resultaten

Ten opzichte van de situatie met p priem zijn er een aantal zaken die veranderd zijn. Noteer $n = p^m$, met p een priemgetal.

Stelling 3.1.

$$\mathbb{Q}(C_n) = \prod_{k=0}^{m} \mathbb{Q}(\epsilon_{p^k}).$$

Bijgevolg bestaat $\mathbb{Q}C_n$ uit $m+1$ componenten. Verder is duidelijk dat:

Stelling 3.2. *$u \in \mathbb{Z}C_n$ is een eenheid als en slechts als $\forall k \in \{0, 1, \cdots, m\}$ geldt dat $\rho_{p^k}(u) \in U(\mathbb{Z}(\epsilon_{p^k}))$.*

Over de eenheden van $\mathbb{Z}(\epsilon_{p^k})$ weten we: $U(\mathbb{Z}(\epsilon_{p^k})) = \pm\langle\epsilon_{p^k}\rangle \times F$ met F abels vrij van rang $\frac{1}{2}\varphi(p^k) - 1 = \frac{1}{2}p^{k-1}(p-1) - 1$. Rest dan nog een fundamenteel systeem van eenheden te vinden.

Stelling 3.3. *Als $n = 2^m$, dan geldt:*

$$U(\mathbb{Z}C_n) = \pm C_n \times F \text{ met rang } F = \frac{1}{2}(2^m - 2m)$$

$$U(\mathbb{Z}C_n^+) = \pm C_n \times F^+ \text{ met rang } F^+ = 2^{m-2} - 1$$

Bewijs. Om de torsievrije rang r van $U(\mathbb{Z}C_n)$ te berekenen gebruiken we de formule $r = \frac{1}{2}(n+1+a_2-2l)$. Hieruit volgt dat $r = \frac{1}{2}(2^m+1+1-2(m+1) = \frac{1}{2}(2^m - 2m)$. Verder is $r^+ = \frac{1}{2}\varphi(2^m) - 1 = \frac{1}{2}2^{m-1}(2-1) - 1 = 2^{m-2} - 1$. □

Stelling 3.4. *Als $n = p^m$ met p oneven, dan geldt:*

$$U(\mathbb{Z}C_n) = \pm C_n \times F \text{ met rang } F = \frac{1}{2}(p^m - 2m - 1)$$

$$U(\mathbb{Z}C_n^+) = \pm C_n \times F^+ \text{ met rang } F^+ = \frac{1}{2}p^{m-1}(p-1) - 1$$

Bewijs. Om de torsievrije rang r van $U(\mathbb{Z}C_n)$ te berekenen gebruiken we de formule $r = \frac{1}{2}(n+1+a_2-2l)$. Hieruit volgt dat $r = \frac{1}{2}(p^m+1+0-2(m+1)) = \frac{1}{2}(p^m - 2m - 1)$. Verder is $r^+ = \frac{1}{2}\varphi(p^m) - 1 = \frac{1}{2}p^{m-1}(p-1) - 1$. □

We besluiten met een resultaat naar analogie met stelling 2.6. Noteer met ρ het homomorfisme tussen $\mathbb{Z}C_n$ en $\mathbb{Z}(\epsilon_n)$ dat g afbeeldt op ϵ_n.

Stelling 3.5. *$\{u_1, u_2, \cdots, u_r\}$ met r uit vorige stellingen is een fundamenteel systeem van eenheden voor $\mathbb{Z}C_n$ als en slechts als $\rho(\pm C_p, u_1, u_2, \cdots, u_r)$ een deelgroep is van $U(\mathbb{Z}(\epsilon_n))$ met index $\frac{1}{2}(p^{m-1}(p-1))$.*

3.2 Voorbeeld 1: $U(\mathbb{Z}(C_8))$

3.2.1 Werkwijze 1

Om te starten weten we dat $\mathbb{Q}C_8 \cong \mathbb{Q} \otimes \mathbb{Q} \otimes \mathbb{Q}(i) \otimes \mathbb{Q}(\epsilon_8)$. Hierbij is $\mathbb{Q}(\epsilon_8) = \{a + b\epsilon_8 + c\epsilon_8^2 + d\epsilon_8^3 \text{ met } a, b, c, d \in \mathbb{Q}\}$ en $\epsilon_8^4 = -1$.

Stelling 3.6. *$U(\mathbb{Z}(C_8)) = \pm C_8 \times F$ met F vrij abels van rang 1.*

Bewijs. Volgens stelling 3.3 is de rang van F gelijk aan $r = \frac{1}{2}(2^3+1+1-2.4) = 1$. □

Stelling 3.7. *$u \in \mathbb{Z}(C_8)$ is een eenheid als en slechts als $aug(u) = \pm 1, \rho_2(u) = \pm 1, \rho_4(u) = \pm 1$ of $\pm i$ en $\rho_8(u) = \pm\epsilon_8^k(1+\epsilon_8+\epsilon_8^2)^p$ met $k, p \in \mathbb{Z}$.*

Bewijs. Volgens stelling 3.2 is u een eenheid als en slechts als $\rho_{2^k}(u) \in U(\mathbb{Z}(\epsilon_{2^k}))$ voor $k \in \{0,1,2,3\}$. We weten dat we voor de eerste drie componenten enkel triviale eenheden krijgen. Rest nog $U(\mathbb{Z}(\epsilon_8))$. De cyclotomische eenheden van $\mathbb{Z}(\epsilon_8)$ zijn $1, \epsilon_8^2+\epsilon_8+1, \epsilon_8^4+\epsilon_8^3+\epsilon_8^2+\epsilon_8+1 = \epsilon_8(\epsilon_8^2+\epsilon_8+1), \epsilon_8^6+\epsilon_8^5+\epsilon_8^4+\epsilon_8^3+\epsilon_8^2+\epsilon_8+1 = -\epsilon_8^7$. Uit de theorie van de cyclotomische gehelen weten we dat de torsie vrije rang van de eenheden groep van $\mathbb{Z}(\epsilon_8)$ gelijk is aan $\frac{1}{2}\varphi(8)-1 = \frac{1}{2}.4-1 = 1$ en dat $\{\epsilon_8^2+\epsilon_8+1\}$ een fundamenteel systeem eenheden vormt van $U(\mathbb{Z}(\epsilon_8))$. Hieruit volgt het gestelde. □

Stelling 3.8. *Het groepshomomorfisme ρ^* tussen $U(\mathbb{Z}C_8)$ en $U(\mathbb{Z}(\epsilon_8)$ is niet injectief.*

Bewijs. Veronderstel $u \in \mathbb{Z}C_8$ en $u \in \ker \rho^*$, dan is $\rho^*(u) = 1$. Omdat $U(\mathbb{Z}C_8) \subset U(\mathbb{Z}) \times U(\mathbb{Z}) \times U(\mathbb{Z}(i)) \times U(\mathbb{Z}(\epsilon_8))$ moet u dus een torsie eenheid zijn, en dus is u triviaal. Het is duidelijk dat $\ker(\rho^*) = \{1, -g^4\}$. □

Stelling 3.9.

$$U(\mathbb{Z}(C_8)) = \pm C_8 \times \langle g^6 + 2g^5 + g^4 - g^2 - g - 1 \rangle$$

Bewijs. We berekenen de kern van $\rho_8 : \mathbb{Z}C_8 \longrightarrow \mathbb{Z}(\epsilon_8) : g \longmapsto \epsilon_8$. Stel $x = \sum_{i=0}^{7} a_i g^i$, dan is $\rho_8(x) = (a_0 - a_4) + (a_1 - a_5)\epsilon_8 + (a_2 - a_6)\epsilon_8^2 + (a_3 - a_7)\epsilon_8^3 = 0$ als en slechts als $a_0 = a_4, a_1 = a_5, a_2 = a_6$ en $a_3 = a_7$. Hieruit volgt dat $\ker(\rho_8) = (a_0 + a_1 g + a_2 g^2 + a_3 g^3)(1 + g^4)$.

$u \in U(\mathbb{Z}(C_8))$ als en slechts als $u = \pm g^k(1+g+g^2)^p + (a_0 + a_1 g + a_2 g^2 + a_3 g^4)(1+g^4)$ en $\text{aug}(u) = \pm 1$, $\rho_2(u) = \pm 1$ en $\rho_4(u) = \pm 1$ of $\pm i$. Neem $k = 0$ en $p = 2$, dan moet:

$$\begin{cases} 9 + 2(a_0 + a_1 + a_2 + a_3) = \pm 1 \\ 1 + 2(a_0 - a_1 + a_2 - a_3) = \pm 1 \\ (-1 + 2a_0 - 2a_2) + (2a_1 - 2a_3)i = \pm 1 \text{ of } \pm i \end{cases}$$

Dit is eigenlijk een verzameling van 16 stelsels. Er is een oplossing voor $a_0 = a_1 = a_3 = -1$ en $a_2 = -2$. In dat geval is $u = (1+g+g^2)^2 + (-1-g-2g^2-g^3)(1+g^4) = -g(g^6+2g^5+g^4-g^2-g-1)$. Bovendien is $\rho(u) = (-1,-1,1,a^2)$. Hierbij is $a = \epsilon_8^2 + \epsilon_8 + 1$.
Noteer $v = g^6 + 2g^5 + g^4 - g^2 - g - 1$. We willen nu nog bewijzen dat $\{v\}$ een set fundamentele eenheden is van $\mathbb{Z}(C_8)$. Daarvoor moeten we bewijzen dat $\rho_8^*(\pm C_8, u)$ een deelgroep van $U(\mathbb{Z}(\epsilon_8))$ is van index 2.
Nu is $\rho_8^*(\pm C_8, u) = \langle \pm\epsilon_8, a^2 \rangle = \{\pm \epsilon_8^k a^{2p} : k, p \in \mathbb{Z}\}$. Dit is inderdaad een deelgroep van $U(\mathbb{Z}(\epsilon_8))$ en omdat $U(\mathbb{Z}(\epsilon_8)) = \pm\epsilon_8^k a^p$ is de index inderdaad 2.
□

3.2.2 Werkwijze 2

We weten dat $\epsilon_8 = \frac{\sqrt{2}}{2}(1+i)$. Neem $a = \sum_{i=0}^{7}$ een torsie vrije eenheid in $\mathbb{Z}C_8$. Omdat $\epsilon_8^4 = -1$ is $\rho_8(a) = (a_0 - a_4) + (a_1 - a_5)\epsilon_8 + (a_2 - a_6)\epsilon_8^2 + (a_3 - a_7)\epsilon_8^3$.

Neem $H = \{1, g^4\}$ en definieer $\varphi : \mathbb{Z}C_8 \longrightarrow \mathbb{Z}C_8/H : \sum_{i=0}^{7} a_i g^i \longmapsto \sum_{i=0}^{7} a_i g^i H$. Omdat $\mathbb{Z}C_8/H \cong C_4$ heeft $\mathbb{Z}C_8/H$ enkel triviale eenheden. Bijgevolg is $\varphi(a) = H$ en geldt er dat $a_0 + a_4 = 1$ en $a_i + a_{i+4} = 0$ $\forall i \in \{1,2,3\}$. Maar dan is $\rho_8(a) = (2a_0 - 1) + 2a_1\epsilon_8 + 2a_2\epsilon_8^2 + 2a_3\epsilon_8^3 = (2a_0 - 1) + 2a_1\left(\frac{\sqrt{2}}{2}(1+i)\right) + 2a_2 i + 2a_3\left(\frac{\sqrt{2}}{2}(-1+i)\right) = (2a_0 - 1) + (a_1 - a_3)\sqrt{2} + (a_1 + a_3)\sqrt{2}i + 2a_2 i$.

Stelling 3.10. *$\gamma = a + b\sqrt{2} + 2ci + di\sqrt{2}$ is een torsievrije eenheid in de deelring $A = \{a + b\sqrt{2} + 2ci + di\sqrt{2} : a,b,c,d \in \mathbb{Z}\}$ als en slechts als $c = d = 0$ en $a^2 - 2b^2 = 1$.*

Bewijs. We definieren voor elke torsievrije eenheid $\gamma = a + b\sqrt{2} + 2ci + di\sqrt{2}$ de uitdrukking $\tilde{\gamma} = a - b\sqrt{2} + 2ci - di\sqrt{2}$. Neem het groepshomomorfisme $f : U(A) \longrightarrow U(\mathbb{Z}(i)) : \gamma \longmapsto \gamma.\tilde{\gamma}$. Dan geldt er dat $f(\gamma) = (a^2 - 2b^2 - 4c^2 + 2d^2) + (4ac - 4bd)i$. Omdat γ torsie vrij is en omdat $\mathbb{Z}(i)$ enkel triviale eenheden heeft moet $f(\gamma) = 1$ en dus is $a^2 - 2b^2 - 4c^2 + 2d^2 = 1$ en $ac = bd$. Noteer $ac = bd = k$ en veronderstel $k \neq 0$ dan is $c = \frac{k}{a}$ en $d = \frac{k}{b}$. Als we dat invullen in de voorwaarde $a^2 - 2b^2 - 4c^2 + 2d^2 = 1$ vinden we dat $a^2 - 2b^2 = \frac{a^2b^2}{a^2b^2 + 2k^2}$. Omdat het rechterlid hiervan tussen 0 en 1 ligt kan het linkerlid geen geheel

getal zijn en klopt de voorwaarde $k \neq 0$ niet. Bijgevolg is $ac = bd = 0$. Uit $a^2 - 2b^2 - 4c^2 + 2d^2 = 1$ volgt dan dat $c = d = 0$ en $a^2 - 2b^2 = 1$.

Omgekeerd, als $c = d = 0$ en $a^2 - 2b^2 = 1$, dan is $\gamma = a + b\sqrt{2}$ met $a^2 - 2b^2 = 1$. Uit de getallentheorie volgt dan dat γ een torsievrije eenheid is in $\mathbb{Z}(\sqrt{2})$. $\square$

Bovendien weten we dat elke eenheid in $\mathbb{Z}(\sqrt{2})$ van de vorm $(1+\sqrt{2})^k$. Omdat $\rho_8(a) = (2a_0 - 1) + (a_1 - a_3)\sqrt{2} + (a_1 + a_3)\sqrt{2}i + 2a_2 i$ een torsie vrije eenheid is moet dus, volgens vorige stelling, $a_2 = a_1 + a_3 = 0$ en $(2a_0 - 1)^2 - 2(a_1 - a_3)^2 = 1$. Dus is $a_2 = 0$, $a_3 = -a_1$ en $(2a_0 - 1)^2 - 8a_1^2 = 1$. Bovendien moet er een $k \in \mathbb{Z}$ bestaan zodat $(2a_0 - 1)^2 + 2a_1\sqrt{2} = (1 + \sqrt{2})^k$. Voor $k = 1$ heb je geen oplossingen, maar als je $k = 2$ neemt moet $a_0 = 2, a_1 = 1, a_2 = 0$ en $a_3 = -1$. Dan is $a_4 = -1, a_5 = -1, a_6 = 0$ en $a_7 = +1$ Bijgevolg is $a = 2 + g - g^3 - g^4 - g^5 + g^7 = g^3(g^6 + 2g^5 + g^4 - g^2 - g - 1)$.We vinden dus hetzelfde resultaat als met werkwijze 1.

3.2.3 Werkwijze 3

De oplossing uit vorig hoofdstuk kan je ook schrijven als $a = 2 + g - g^3 - g^4 - g^5 + g^7 = g^4\Big(-1 - (g + g^{-1}) + (g^3 + g^{-3}) + 2g^4\Big)$. Hierbij is $-1 - (g + g^{-1}) + (g^3 + g^{-3}) + 2g^4$ een symmetrische eenheid. Gebruiken we nu de methode van de onbepaalde coëfficiënten op een willekeurige symmetrische eenheid $a = p + q(g + g^{-1}) + r(g^2 + g^{-2}) + s(g^3 + g^{-3}) + 2tg^4$. Volgen we dezelfde stappen als hierboven:

- Uit $\epsilon_8 = \frac{\sqrt{2}}{2}(1 + i)$ volgt dat $\rho_8(g + g^{-1}) = \sqrt{2}$, $\rho_8(g^2 + g^{-2}) = 0$ en $\rho_8(g^3 + g^{-3}) = -\sqrt{2}$. Verder is $1 + \sqrt{2} = 1 + \epsilon_8 + \epsilon_8^{-1}$.
- Dus is $\rho_8(a) = (p - 2t) + (q - s)\sqrt{2}$.
- Neem $H = \{1, g^4\}$ en definieer $\varphi : \mathbb{Z}C_8 \longrightarrow \mathbb{Z}C_8/H : \sum_{i=0}^{7} a_i g^i \longmapsto \sum_{i=0}^{7} a_i g^i H$. Omdat $\mathbb{Z}C_8/H \cong C_4$ heeft $\mathbb{Z}C_8/H$ enkel triviale eenheden. Bijgevolg is $\varphi(a) = H$ en $p + 2t = 1, q + s = 0$ en $r = 0$.
- Dit geeft uiteindelijk dat $\rho_8(a) = (2p - 1) + 2q\sqrt{2}$
- Elke eenheid in $\mathbb{Z}(\sqrt{2})$ van de vorm $\pm(1 + \sqrt{2})^k$. Dus moet er een $k \in \mathbb{Z}$ bestaan zodat $(2p - 1) + 2q\sqrt{2} = (1 + \sqrt{2})^k$. Voor $k = 1$ vinden we geen gehele oplossingen voor p en q. Maar voor $k = 2$ en een -teken ervoor is $p = -1$ en $q = -1$.
- Uit vorige vergelijkingen volgt dan dat $r = 0$, $s = 1$ en $t = 1$.
- Dus is $a = -1 - (g + g^{-1}) + (g^3 + g^{-3}) + 2g^4$ en krijgen we hetzelfde resultaat dan hierboven.

3.2.4 Werkwijze 4

$$\begin{array}{ccc} \mathbb{Z}C_8 & \longrightarrow & \mathbb{Z}(\epsilon_8) \\ \downarrow & & \downarrow \\ \mathbb{Z}C_4 & \longrightarrow & \mathbb{Z}_2C_4 \end{array}$$

Het linkerhomomorfisme beeldt g^4 af op 1. Voor het rechts homomorfisme moet je ϵ_8 vervangen door g en de coëfficiënten modulo 2 nemen. De elementen $a + bg + cg^2 + dg^3 \in \mathbb{Z}C_4$ en $\sum_{i=0}^{3} a_i\epsilon_8^i \in \mathbb{Z}(\epsilon_8)$ hebben hetzelfde beeld als $a_0 = a + 2k, a_1 = b + 2l, a_2 = c + 2m$ en $a_3 = d + 2n$. Hiermee correspondeert het unieke element $\sum_{i=0}^{3} a_i g^i - (k+lg+mg^2+ng^3)(1+g^4)$ in $\mathbb{Z}C_8$. Dit betekent dus:

Stelling 3.11. *$\mathbb{Z}C_8$ is het vezelproduct van $\mathbb{Z}(\epsilon_8)$ over $\mathbb{Z}C_4$.*

Overgang naar de groep der eenheden geeft:

$$\begin{array}{ccc} U(\mathbb{Z}C_8) & \longrightarrow & U(\mathbb{Z}(\epsilon_8)) \\ \downarrow & & \downarrow \\ \pm C_4 & \longrightarrow & \pm C_4 \end{array}$$

Neem de eenheid $(1 + \epsilon_8 + \epsilon_8^2)^2$ in $\mathbb{Z}(\epsilon_8)$ dan is het beeld door het rechter homomorfisme in $\pm C_4$ gelijk aan g^2. Als we in $U(\mathbb{Z}C_4)$ de eenheid $-g^2$ nemen, dan vinden we $k = 0, l = 1, m = 2$ en $n = 1$. Dit geeft dan hetzelfde resultaat dat we vroeger verkregen hebben.

3.3 Voorbeeld 2: $U(\mathbb{Z}(C_9))$

3.3.1 Werkwijze 1

Om te starten weten we dat $\mathbb{Q}C_9 \cong \mathbb{Q} \otimes \mathbb{Q}(\omega) \otimes \mathbb{Q}(\epsilon_9)$. Hierbij is $\mathbb{Q}(\epsilon_9) = \{a + b\epsilon_9 + c\epsilon_9^2 + d\epsilon_9^3 + e\epsilon_9^4 + f\epsilon_9^5$ met $a, b, c, d, e, f \in \mathbb{Q}\}$ en $\epsilon_9^6 = -\epsilon_9^3 - 1$.

Stelling 3.12. *$U(\mathbb{Z}(C_9)) = \pm C_9 \times F$ met F vrij abels van rang 2.*

Bewijs. Volgens stelling 3.3 is de rang van F gelijk aan $r = \frac{1}{2}(3^2 + 1 - 2.3) = 2$. □

Stelling 3.13. *$u \in \mathbb{Z}(C_9)$ is een eenheid als en slechts als $aug(u) = \pm 1, \rho_3(u) = \pm 1, \pm\omega$ of $\pm\,\omega^2$ en $\rho_9(u) = \pm\epsilon_9^k(1+\epsilon_9)^p(1+\epsilon_9+\epsilon_9^2+\epsilon_9^3)^p$ met $k, p \in \mathbb{Z}$.*

Bewijs. Volgens stelling 3.2 is u een eenheid als en slechts als $\rho_{3^k}(u) \in U(\mathbb{Z}(\epsilon_{3^k}))$ voor $k \in \{0,1,2\}$. We weten dat we voor de eerste twee componenten enkel triviale eenheden krijgen. Rest nog $U(\mathbb{Z}(\epsilon_9))$. De cyclotomische eenheden van $\mathbb{Z}(\epsilon_9)$ zijn $1, \epsilon_9+1, \epsilon_9^3+\epsilon_9^2+\epsilon_9+1, \epsilon_9^4+\epsilon_9^3+\epsilon_9^2+\epsilon_9+1 = -\epsilon_9^5(\epsilon_9^3+\epsilon_9^2+\epsilon_9+1), \epsilon_9^6+\epsilon_9^5+\epsilon_9^4+\epsilon_9^3+\epsilon_9^2+\epsilon_9+1 = -\epsilon_9^7(\epsilon_9+1), \epsilon_9^7+\epsilon_9^6+\epsilon_9^5+\epsilon_9^4+\epsilon_9^3+\epsilon_9^2+\epsilon_9+1 = -\epsilon_9^8$. Uit de theorie van de cyclotomische gehelen weten we dat de torsie vrije rang van de eenheden groep van $\mathbb{Z}(\epsilon_9)$ gelijk is aan $\frac{1}{2}\varphi(9) - 1 = \frac{1}{2}.6 - 1 = 2$ en dat $\epsilon_9^3+\epsilon_9^2+\epsilon_9+1$ en ϵ_9+1 een fundamenteel systeem eenheden vormt van $U(\mathbb{Z}(\epsilon_9))$. Hieruit volgt het gestelde. □

Stelling 3.14. *Het groepshomomorfisme ρ^* tussen $U(\mathbb{Z}C_9)$ en $U(\mathbb{Z}(\epsilon_9))$ is injectief.*

Bewijs. Veronderstel $u \in \mathbb{Z}C_9$ en $u \in \ker \rho^*$, dan is $\rho^*(u) = 1$. Omdat $U(\mathbb{Z}C_9) \subset U(\mathbb{Z}) \times U(\mathbb{Z}(\omega)) \times U(\mathbb{Z}(\epsilon_9))$ moet u dus een torsie eenheid zijn, en dus is u triviaal. Het is duidelijk dat $\ker(\rho^*) = \{1\}$ en dus is ρ^* injectief. □

Stelling 3.15.

$$U(\mathbb{Z}(C_9)) = \pm C_9 \times \langle 1 - g^2 + g^4 - g^6 + g^8 \rangle \times \langle g^6 + g^5 + g^4 - g - 1 \rangle$$

Bewijs. We berekenen de kern van $\rho : \mathbb{Z}C_9 \longrightarrow \mathbb{Z}(\epsilon_9) : g \longmapsto \epsilon_9$. Stel $x = \sum_{i=0}^{8} a_i g^i$, dan is $\rho(x) = (a_0 - a_6) + (a_1 - a_7)\epsilon_9 + (a_2 - a_8)\epsilon_9^2 + (a_3 - a_6)\epsilon_8^4 + (a_5 - a_8)\epsilon_9^5 = 0$ als en slechts als $a_0 = a_3 = a_6, a_1 = a_4 = a_7$ en $a_2 = a_5 = a_8$. Hieruit volgt dat $\ker(\rho) = (a_0 + a_1 g + a_2 g^2)(1 + g^3 + g^6)$.
$u \in \mathbb{Z}(C_9)$ als en slechts als $u = \pm g^k(1+g)^p(1+g+g^2+g^3)^q + (a_0 + a_1 g + a_2 g^2)(1 + g^3 + g^6)$ en $\text{aug}(u) = \pm 1$, $\rho_3(u) = \pm 1$ of $\pm\,\omega$. Neem $k = 0$, $p = 2$ en $q = -1$, dan moet:

$$\begin{cases} -8 + 3(a_0 + a_1 + a_2) = \pm 1 \\ 3(a_0 - a_2) + (1 + 3a_1 - 3a_2)\omega = \pm 1 \text{ of } \pm\,\omega \end{cases}$$

Dit is eigenlijk een verzameling van 8 stelsels. Er is een oplossing voor $a_0 = a_1 = a_2 = 1$. In dat geval is $u = 1 - g^2 + g^4 - g^6 + g^8$. Bovendien is $\rho(u) = (1, \omega, a^2 b^{-1})$.

Hierbij is $b = \epsilon_9^3 + \epsilon_9^2 + \epsilon_9 + 1$ en $a = \epsilon_9 + 1$

Neem vervolgens $k = 0$, $p = -1$ en $q = 2$, dan moet:

$$\begin{cases} 8 + 3(a_0 + a_1 + a_2) = \pm 1 \\ 3(a_0 - a_2) + (1 + 3a_1 - 3a_2)\omega = \pm 1 \text{ of } \pm\omega \end{cases}$$

Ook dit is een verzameling van 8 stelsels. Er is een oplossing voor $a_0 = a_1 = a_2 = -1$. In dat geval is $u = -g^2(g^6 + g^5 + g^4 - g - 1)$. Bovendien is $\rho(u) = (-1, \omega, a^{-1}b^2)$.
Noteer $u_1 = 1 - g^2 + g^4 - g^6 + g^8$ en $u_2 = g^6 + g^5 + g^4 - g - 1$. We willen nu nog bewijzen dat $\{u_1, u_2\}$ een set fundamentele eenheden is van $\mathbb{Z}(C_9)$. Daarvoor moeten we bewijzen dat $\rho^*(\pm C_9, u_1, u_2)$ een deelgroep van $U(\mathbb{Z}(\epsilon_9))$ is van index 3.
Nu is $\rho^*(\pm C_9, u_1, u_2) = \langle \pm\epsilon_9, a^2b^{-1}, a^{-1}b^2 \rangle$. Dit geeft alle elementen van de vorm $\pm\epsilon_9^k(a^2b^{-1})^p(a^{-1}b^2)^q = \pm\epsilon_9^k a^{2p-q}b^{2q-p}$. Het verschil van de exponenten van a en b is steeds een drievoud. Dit is een deelgroep van $U(\mathbb{Z}\epsilon_9)$ en omdat $U(\mathbb{Z}\epsilon_9) = \{\epsilon_9^k a^p b^q\}$ is de index inderdaad 3.

□

3.3.2 Werkwijze 2

Veronderstel dat γ een symmetrische eenheid is die een generator is van het torsievrij deel. Veronderstel ook dat γ augmentatie 1 heeft. Dan is

$$\gamma = \gamma_0 + \gamma_1(g + g^{-1}) + \gamma_2(g^2 + g^{-2}) + \gamma_3(g^3 + g^{-3}) + \gamma_4(g^4 + g^{-4})$$

met $\gamma_0 + 2\gamma_1 + 2\gamma_2 + 2\gamma_3 + 2\gamma_4 = 1$.

Neem $H = \{1, g^3, g^6\}$ en $\varphi : \mathbb{Z}C_9 \longrightarrow \mathbb{Z}C_9/H : g \longmapsto gH$. Omdat $\mathbb{Z}C_9/H \cong \mathbb{Z}C_3$ en $\mathbb{Z}C_3$ enkel triviale eenheden heeft moet $\varphi(\gamma) = H$. Hieruit volgt dan dat $\gamma_0 + 2\gamma_3 = 1$ en $\gamma_1 + \gamma_2 + \gamma_4 = 0$.

Noteer verder $\alpha = \epsilon_9 + \epsilon_9^{-1}$. We weten ook dat $\epsilon_9^6 + \epsilon_9^3 + 1 = 0$. Dan is het duidelijk dat $\epsilon_9^2 + \epsilon_9^{-2} = \alpha^2 - 2$, $\epsilon_9^3 + \epsilon_9^{-3} = -1$ en $\epsilon_9^4 + \epsilon_9^{-4} = 2 - \alpha - \alpha^2$. En natuurlijk is $\alpha^3 + 3\alpha + 1 = 0$

Defineer tenslotte $\rho : \mathbb{Z}C_9 \longrightarrow \mathbb{Z}(\epsilon_9) : g \longmapsto \epsilon_9$. Dan is:

$$\begin{aligned} \rho(\gamma) =& \gamma_0 + \gamma_1\alpha + \gamma_2(\alpha^2 - 2) - \gamma_3 + \gamma_4(2 - \alpha - \alpha^2) \\ =& (1 - 2\gamma_3) - (\gamma_2 + \gamma_4)\alpha + \gamma_2(\alpha^2 - 2) - \gamma_3 + \gamma_4(2 - \alpha - \alpha^2) \\ =& (1 - 2\gamma_2 - 3\gamma_3 + 2\gamma_4) - (\gamma_2 - 2\gamma_4)\alpha + (\gamma_2 - \gamma_4)\alpha^2 \end{aligned}$$

Omdat $\rho(\gamma)$ een eenheid is in $\mathbb{Z}[\alpha] = \{x + y\alpha + z\alpha^2$ met $x, y, z \in \mathbb{Z}$ en $\alpha^3 - 3\alpha + 1 = 0\}$ moeten we de fundamantele eenheden zoeken in $\mathbb{Z}[\alpha]$. Dit zijn $\alpha - 1$ en $\alpha^2 + \alpha - 1$.

- $\rho(\gamma)$ kan nooit gelijk zijn aan $\alpha-1, (\alpha-1)^{-1}, \alpha^2+\alpha-1$ of $(\alpha^2+\alpha-1)^{-1}$. Hierbij is $(\alpha-1)^{-1} = \alpha^2+\alpha-2$ en $(\alpha^2+\alpha-1)^{-1} = \alpha^2-2$. Dit kan je bewijzen door de coëfficiënten te vergelijken en het stelsel op te lossen.
- $\rho(\gamma)$ kan evenmin het product zijn van twee factoren uit $\alpha-1, (\alpha-1)^{-1}, \alpha^2+\alpha-1$ en $(\alpha^2+\alpha-1)^{-1}$. Verklaring idem.
- Bij dubbele producten lukt het wel: $\rho(\gamma) = (\alpha-1)^3$ als $\gamma_0 = 1, \gamma_1 = 1, \gamma_2 = 1, \gamma_3 = 0$ en $\gamma_4 = -2$. Dit geeft $\gamma = 1+(g+g^{-1})+(g^2+g^{-2})-2(g^4+g^{-4})$.
- Bij $\rho(\gamma) = (\alpha-1)(\alpha^2+\alpha-1)^2$ vinden we $\gamma = 1+(g+g^{-1})-(g^4+g^{-4})$.

Stelling 3.16.

$$U(\mathbb{Z}C_9) = \pm C_9 \times \langle 1+(g+g^{-1})-(g^4+g^{-4})\rangle \times$$
$$\langle 1+(g+g^{-1})+(g^2+g^{-2})-2(g^4+g^{-4})\rangle$$

Hoofdstuk 4

$U(\mathbb{Z}C_n)$ met n geen priemmacht

4.1 Op verkenning

Het bepalen van een fundamenteel systeem van eenheden voor $U(\mathbb{Z}C_n)$ ligt nu wat moeilijker omdat er niet altijd een fundamenteel systeem van eenheden is voor $U(\mathbb{Z}(\epsilon_n))$. Voor $n = 2$ tot $n = 9$ hebben we de eenheden groep in de vorige hoofdstukken bepaald. Om een idee te krijgen hoe we de situatie moeten aanpakken als n geen priemmacht is, concentreren we ons op de gevallen waarvoor $10 \leq n \leq 20$. In volgende tabel geven we hiervoor de waarden van r, de torsie vrije rang van $U(\mathbb{Z}C_n)$, en r^+, de torsie vrije rang van $U(\mathbb{Z}(\epsilon_n))$.

n	r	r^+
10	2	1
11	4	4
12	1	1
13	5	5
14	4	2
15	4	3
16	4	3
17	7	7
18	4	2
19	8	8
20	5	3

- Zoals gezien in hoofdstuk 2 is $r = r^+$ voor priemwaarden van n. De snelste manier om dan een fundamenteel stel eenheden te bepalen is werken met de symmetrische eenheden. Deze gevallen gaan we hier niet behandelen.

- $n = 12$ is het enige overblijvende geval waar de torsie vrije rang 1 is. We behandelen dit geval apart.

- We werken het geval $n = 10$ uit en zullen de gevonden methode ook gebruiken in de andere situaties.

We vermelden enkele resultaten dat we meermaals zullen gebruiken in volgende secties:

Stelling 4.1. *Als H een deelgroep is van C_n en φ het natuurlijk ring morfisme is van $\mathbb{Z}C_n \longrightarrow \mathbb{Z}(C_n/H) : \sum \gamma_g g \longmapsto \sum \gamma_g (gH)$ en als $C_n/H \cong C_2, C_3, C_4$ of C_6, dan geldt voor elke torsie vrije eenheid γ van $\mathbb{Z}C_n$ dat $\varphi(\gamma) = H$.*

Stelling 4.2. *H een deelgroep is van C_n met $H = \langle x \rangle$. De index van H in G is gelijk aan p en $\gamma = \sum_{i=0}^{d-1} a_i x^i \in U(\mathbb{Z}H)$. Dan is*

$$\gamma^* = \sum_{i=0}^{d-1} a_i x^{pi} \in U(\mathbb{Z}C_n)$$

4.2 De eenhedengroep $U(\mathbb{Z}C_{12})$

4.2.1 Parametrisatie van torsie vrije eenheden

Stelling 4.3. *Als $\gamma = \sum \gamma_i g^i$ een torsie vrije eenheid is van $V(\mathbb{Z}C_{12})$, dan kan γ uitgedrukt worden met behulp van 4 parameters.*

Bewijs. Neem $H = \{1, g^6\}$. Omdat $C_{12}/H \cong C_6$ geldt volgens stelling 4.1 dat $\varphi(\gamma) = H$. Hieruit volgt dat $\gamma_0 + \gamma_6 = 1$ en $\gamma_i + \gamma_{i+6} = 0$ voor $i = 1, 2, 3, 4$.
Neem $K = \{1, g^4, g^8\}$. Omdat $C_{12}/K \cong C_4$ geldt volgens stelling 4.1 dat $\varphi(\gamma) = K$. Hieruit volgt dat $\gamma_0 + \gamma_4 + \gamma_8 = 1$ en $\gamma_i + \gamma_{i+4} + \gamma_{i+8} = 0$ voor $i = 1, 2, 3$.
We kunnen alle γ_i's uitrekenen in functie van $\gamma_0, \gamma_1, \gamma_2$ en γ_3. We vinden:

$$\gamma_4 = 1 - \gamma_0 + \gamma_2$$
$$\gamma_5 = -\gamma_1 + \gamma_3$$
$$\gamma_6 = 1 - \gamma_0$$
$$\gamma_7 = -\gamma_1$$
$$\gamma_8 = -\gamma_2$$
$$\gamma_9 = -\gamma_1 - \gamma_3$$
$$\gamma_{10} = -1 + \gamma_0 - \gamma_2$$
$$\gamma_{11} = \gamma_1 - \gamma_3$$

□

4.2.2 Projectie in $\mathbb{Z}C_{12}$

Omdat $x^{12} - 1 = (x^2 + 1)(x^4 - x^2 + 1)(x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$ vinden we dat

$$\epsilon_{12} = \frac{\sqrt{3} + i}{2}$$

Verder geldt ook dat $\epsilon_{12}^6 = -1$.
Definieer $\rho : \mathbb{Z}C_{12} \longrightarrow \mathbb{Z}(\epsilon_{12}) : \sum \gamma_i g^i \longmapsto \sum \gamma_i \epsilon_{12}^i = \sum_{i=0}^{i=6} (\gamma_i - \gamma_{i+6})\epsilon_{12}^i$.

Als γ een torsie vrije eenheid is van $\mathbb{Z}C_{12}$, dan kunnen we gebuik maken van de parametrisatie uit het vorige deel en we vinden dat:
$\rho(\gamma) = (2\gamma_0 - 1) + 2\gamma_1\epsilon_{12} + 2\gamma_2\epsilon_{12}^2 + 2\gamma_2\epsilon_{12}^3 + (1 - \gamma_0 + \gamma_2)\epsilon_{12}^5 + 2(\gamma_3 - \gamma_1)\epsilon_{12}^5$.
Vervangen we hierin ϵ_{12} door $\frac{\sqrt{3}+i}{2}$, dan krijgen we:

$$\rho(\gamma) = (3\gamma_0 - 2) + (2\gamma_1 - \gamma_3)\sqrt{3} + 3\gamma_3 i - (1 - \gamma_0 + 2\gamma_2)\sqrt{3}i$$

$\rho(\gamma)$ is dan een torsie vrije eenheid in de deelring $\tilde{\mathbb{Z}}(\sqrt{3}, i) = \{a + b\sqrt{3} + 3ci + d\sqrt{3}i : a, b, c, d \in \mathbb{Z}\}$ van de ring $\mathbb{Z}(\sqrt{3}, i)$.

Stelling 4.4. *$\gamma = a + b\sqrt{3} + 3ci + di\sqrt{3}$ is een torsievrije eenheid in de deelring $A = \{a + b\sqrt{3} + 3ci + di\sqrt{3} : a, b, c, d \in \mathbb{Z}\}$ als en slechts als $c = d = 0$ en $a^2 - 3b^2 = 1$.*

Bewijs. We definiëren voor elke torsievrije eenheid $\gamma = a + b\sqrt{3} + 3ci + di\sqrt{3}$ de uitdrukking $\tilde{\gamma} = a - b\sqrt{3} + 3ci - di\sqrt{3}$. Neem het groepshomomorfisme $f : U(A) \longrightarrow U(\mathbb{Z}(i) : \gamma \longmapsto \gamma.\tilde{\gamma}$. Dan geldt er dat $f(\gamma) = (a^2 - 3b^2 - 9c^2 + 3d^2) + (6ac - 6bd)i$. Omdat γ torsie vrij is en omdat $\mathbb{Z}(i)$ enkel triviale eenheden heeft moet $f(\gamma) = 1$ en dus is $a^2 - 3b^2 - 9c^2 + 3d^2 = 1$ en $ac = bd$. Noteer $ac = bd = k$ en veronderstel $k \neq 0$ dan is $c = \frac{k}{a}$ en $d = \frac{k}{b}$. Als we dat invullen in de voorwaarde $a^2 - 3b^2 - 9c^2 + 3d^2 = 1$ vinden we dat $a^2 - 3b^2 = \frac{a^2b^2}{a^2b^2+3k^2}$. Omdat het rechterlid hiervan tussen 0 en 1 ligt kan het linkerlid geen geheel

getal zijn en klopt de voorwaarde $k \neq 0$ niet. Bijgevolg is $ac = bd = 0$. Uit $a^2 - 3b^2 - 9c^2 + 3d^2 = 1$ volgt dan dat $c = d = 0$ en $a^2 - 3b^2 = 1$.

Omgekeerd, als $c = d = 0$ en $a^2 - 3b^2 = 1$, dan is $\gamma = a + b\sqrt{3}$ met $a^2 - 3b^2 = 1$. Uit de getallentheorie volgt dan dat γ een torsievrije eenheid is in $\mathbb{Z}(\sqrt{3})$. $\square$

4.2.3 Eenheden in $\mathbb{Z}C_{12}$

Als γ een torsievrije eenheid is in $\mathbb{Z}C_{12}$, dan moet $\rho(\gamma) = (3\gamma_0 - 2) + (2\gamma_1 - \gamma_3)\sqrt{3} + 3\gamma_3 i - (1 - \gamma_0 + 2\gamma_2)\sqrt{3}i$ een eenheid zijn in $\{a + b\sqrt{3} + 3ci + di\sqrt{3} : a, b, c, d \in \mathbb{Z}\}$. Volgens voorgaande stelling moet dan $\gamma_3 = 1 - \gamma_0 + 2\gamma_2 = 0$ en $(3\gamma_0 - 2)^2 - 3(2\gamma_1 - \gamma_3)^2 = 1$. Dus is $\rho(\gamma) = (3\gamma_0 - 2) + 2\gamma_1\sqrt{3} \in U(\mathbb{Z}(\sqrt{3}))$. Nu weten we dat elke eenheid van $\mathbb{Z}(\sqrt{3}))$ van de vorm $\pm(2 + \sqrt{3})^k$ is met $k \in \mathbb{Z}$. Voor $k = 1$ heeft het stelsel met vergelijkingen $3\gamma_0 - 2 = 2$ en $2\gamma_1 = 1$ geen oplossingen in $\mathbb{Z}$. Voor $k = 2$ wel en dan zal $\gamma_0 = 3$ en $\gamma_1 = 2$. Hieruit volgt dat $\gamma_2 = 1$ en $\gamma_3 = 0$. Via de parametrisatieformules vinden we de waarden van $\gamma_4 \cdots \gamma_{11}$. We besluiten:

Stelling 4.5. $U(\mathbb{Z}C_{12}) = \pm C_{12} \times \langle 3 + 2(g + g^{-1}) + (g^2 + g^{-2}) - (g^4 + g^{-4}) - 2(g^5 + g^{-5}) - 2g^6 \rangle$.

4.3 De eenhedengroep $U(\mathbb{Z}C_{10})$

4.3.1 Op verkenning

- $\mathbb{Q}C_{10} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\epsilon_5) \oplus \mathbb{Q}(\epsilon_{10})$. Hierbij is $\mathbb{Q}(\epsilon_{10}) = \{a + b\epsilon_{10} + c\epsilon_{10}^2 + d\epsilon_{10}^3$ met $a, b, c, d \in \mathbb{Q}\}$ met $\epsilon_{10}^5 = -1$ en $\epsilon_{10}^4 - \epsilon_{10}^3 + \epsilon_{10}^2 - \epsilon_{10} + 1 = 0$.
- Het is duidelijk dat $\mathbb{Q}(\epsilon_{10}) \cong \mathbb{Q}(\epsilon_5)$ via $\epsilon_{10} = -\epsilon_5$.
- $\mathbb{Z}C_{10}$ is isomorf met een deel van $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}(\epsilon_5) \oplus \mathbb{Z}(\epsilon_{10})$. De eerste twee componenten hebben enkel triviale eenheden. We kennen een fundamentele eenheid van $\mathbb{Z}(\epsilon_5)$. Omdat $\mathbb{Z}(\epsilon_{10}) \cong \mathbb{Z}(\epsilon_5)$ kunnen we ook een fundamentele eenheid vinden voor $\mathbb{Z}(\epsilon_{10})$.
- We weten dat $1 + \epsilon_5$ een fundamentele eenheid is van $\mathbb{Z}(\epsilon_5)$, maar we kunnen ook $-\epsilon_5^2(1 + \epsilon_5)$ kiezen of het inverse daarvan: $-1 - \epsilon_5^2 - \epsilon_5^3$. Als we nu ϵ_5 vervangen door $-\epsilon_{10}$ dan krijgen we $-1 - \epsilon_{10}^2 + \epsilon_{10}^3$ of $1 + \epsilon_{10}^2 - \epsilon_{10}^3$ als mogelijke fundamentele eenheid in $\mathbb{Z}(\epsilon_{10})$.
- $U(\mathbb{Z}C_{10}) = \pm C_{10} \times F$ met rang F $= \frac{1}{2}(10 + 1 + 1 - 2.4) = 2$.
- $U(\mathbb{Z}C_{10})$ is ook het direct product van triviale eenheden en een torsie vrije groep van symmetrische eenheden.

- Omdat de orde van het element g^2 gelijk is aan 5, en dus onderling ondeelbaar is met 6, is, volgens stelling 1.13 $g^2 + g^8 - 1$ een eenheid van $\mathbb{Z}C_{10}$, die geen (positieve) macht is van een andere symmetrische eenheid van $\mathbb{Z}C_{10}$.

4.3.2 Parametrisatie van symmetrische eenheden

- Veronderstel dat γ een symmetrische torsie vrije eenheid is van $\mathbb{Z}C_{10}$. Stel

  $$\gamma = \gamma_0 + \gamma_1(g + g^{-1}) + \gamma_2(g^2 + g^{-2}) + \gamma_3(g^3 + g^{-3}) + \gamma_4(g^4 + g^{-4}) + 2\gamma_5 g^5$$

- $H = \langle g^2 \rangle = \{1, g^2, g^4, g^6, g^8\}$ is een deelgroep van C_{10} met $C_{10}/H \cong C_2$. Volgens stelling 4.1 is dan $\begin{cases} \gamma_0 + 2\gamma_2 + 2\gamma_4 = 1 \\ 2\gamma_1 + 2\gamma_3 + 2\gamma_5 = 0 \end{cases}$

- Stel $\gamma_2 = p, \gamma_3 = q, \gamma_4 = r$ en $\gamma_5 = s$, dan is $\gamma_0 = 1 - 2p - 2q$ en $\gamma_1 = -q - s$.

- Als γ een symmetrische torsie vrije eenheid is dan moet $\rho_1(\gamma) = \pm 1$, $\rho_2(\gamma) = \pm 1$. Ook moeten $\rho_5(\gamma)$ en $\rho_{10}(\gamma)$ respectievelijk eenheden zijn in $\mathbb{Z}(\epsilon_5)$ en $\mathbb{Z}(\epsilon_{10})$. Je kan gemakkelijk narekenen dat $\rho_1(\gamma) = \rho_2(\gamma) = 1$.

4.3.3 Projectie in $\mathbb{Z}C_{10}$

- Noteer $\epsilon_{10} + \epsilon_{10}^{-1} = \alpha$, dan geldt $\epsilon_{10}^2 + \epsilon_{10}^{-2} = \alpha^2 - 2$, $\epsilon_{10}^3 + \epsilon_{10}^{-3} = \alpha^3 - 3\alpha = 2 - \alpha^2$ en $\epsilon_{10}^4 + \epsilon_{10}^{-4} = -\alpha$. Verder geldt dat $\alpha^2 = \alpha + 1$.

- De ring der gehelen in het maximale reële deelveld van $\mathbb{Z}(\epsilon_{10})$ wordt gegeven door $\mathbb{Z}(\epsilon_{10} + \epsilon_{10}^{-1}) = \mathbb{Z}(\alpha) = \{a + b\alpha : a, b \in \mathbb{Z} \text{ en } \alpha^2 - \alpha - 1 = 0\}$.

- De torsie vrije rang van de eenheden groep van $\mathbb{Z}(\epsilon_{10} + \epsilon_{10}^{-1})$ is dezelfde als de torsie vrije rang van de eenhden groep van $\mathbb{Z}(\epsilon_{10})$ en is gelijk aan $\frac{1}{2}\varphi(10) - 1 = 1$.

- α is een fundamentele eenheid in $\mathbb{Z}(\alpha)$, met andere woorden $U(\mathbb{Z}(\alpha)) = \{\pm\alpha^p\}$.

- Definieer $\rho_{10} : U(\mathbb{Z}C_{10}^+) \longrightarrow \mathbb{Z}(\epsilon_{10} + \epsilon_{10}^{-1}) : g \longmapsto \epsilon_{10}$.

- Veronderstel dat γ een symmetrische torsie vrije eenheid is dan is $\rho_{10}(\gamma) = \gamma_0 + \gamma_1\alpha + \gamma_2(\alpha^2 - 2) - \gamma_3(\alpha^2 - 2) - \gamma_4\alpha - 2\gamma_5 = (\gamma_0 - \gamma_2 + \gamma_3 - 2\gamma_5) + (\gamma_1 + \gamma_2 - \gamma_3 - \gamma_4)\alpha$.

- Als we de parametrisatie uit vorige paragraaf invullen dan is $\rho_{10}(\gamma) = (1 - 3p + q - 2r - 2s) + (p - 2q - r - s)\alpha$.

- $a\alpha + b$ behoort tot het bereik van ρ_{10} als en slechts als er gehele getallen p en q bestaan waarvoor $\begin{cases} p - 2q - r - s = a \\ 1 - 3p + q - 2r - 2s = b \end{cases}$.

- Uit de eerste vergelijking volgt dat $p = a + 2q + r + s$. Ingevuld in de tweede vergelijking geeft dit : $b = 1-3a-5q-5r-5s$. Dus moet $1-3a-b$ een vijfvoud zijn.

- Omdat $a\alpha+b$ een eenheid is in $\mathbb{Z}(\alpha)$ moet $a\alpha+b$ van de vorm $\pm\alpha^t$ zijn met $t \in \mathbb{Z}$. De kleinste positieve waarde van t waarvoor $1-3a-b$ een vijfvoud is, blijkt 2 te zijn. Inderdaad $-\alpha^2 = -\alpha-1$ en dan is $1-3a-b = 1+3+1 = 5$.

- Verder kan men gemakkelijk narekenen dat als $a\alpha + b$ en $c\alpha + d$ allebei vijfvouden zijn, dat ook hun product een vijfvoud is. Dus is $\text{Im } \rho_{10} = \langle -\alpha^2 \rangle$.

- Berekenen we ook de kern van het groephomomorfisme ρ_{10}. Nu is $\rho_{10}(\gamma) = 1 \iff \begin{cases} p - 2q - r - s = 0 \\ 1 - 3p + q - 2r - 2s = 1 \end{cases}$. Hieruit volgt dat $p = q = -r - s$. Dit geeft dan $\gamma = 1 + 2s + r(g + g^{-1}) + (-r - s)(g^2 + g^{-2}) + (-r - s)(g^3 + g^{-3}) + r(g^4 + g^{-4}) + 2sg^5$.

4.3.4 Projectie in $\mathbb{Z}C_5$

- Noteer $\epsilon_5 + \epsilon_5^{-1} = \beta$, dan geldt $\epsilon_5^2 + \epsilon_5^{-2} = \beta^2 - 2$. Verder geldt dat $\beta^2 = 1 - \beta$.

- De ring der gehelen in het maximale reële deelveld van $\mathbb{Z}(\epsilon_5)$ wordt gegeven door $\mathbb{Z}(\epsilon_5 + \epsilon_5^{-1}) = \mathbb{Z}(\beta) = \{a + b\beta : a, b \in \mathbb{Z} \text{ en } \beta^2 + \beta - 1 = 0\}$.

- De torsie vrije rang van de eenheden groep van $\mathbb{Z}(\epsilon_5 + \epsilon_5^{-1})$ is dezelfde als de torsie vrije rang van de eenhden groep van $\mathbb{Z}(\epsilon_5)$ en is gelijk aan $\frac{1}{2}\varphi(5) - 1 = 1$.

- β is een fundamentele eenheid in $\mathbb{Z}(\beta)$, met andere woorden $U(\mathbb{Z}(\beta)) = \{\pm\beta^p\}$.

- Definieer $\rho_5 : U(\mathbb{Z}C_5^+) \longrightarrow \mathbb{Z}(\epsilon_5 + \epsilon_5^{-1}) : g \longmapsto \epsilon_5$.

- Veronderstel dat γ een symmetrische torsie vrije eenheid is dan is $\rho_5(\gamma) = \gamma_0 + \gamma_1\beta + \gamma_2(-1-\beta) + \gamma_3(-1-\beta) + \gamma_4\beta + 2\gamma_5 = (\gamma_0 - \gamma_2 - \gamma_3 + 2\gamma_5) + (\gamma_1 - \gamma_2 - \gamma_3 + \gamma_4)\beta$.

- Gebruikmakend van de gegeven parametrisatie geeft dit: $\rho_5(\gamma) = (1 - 3p - q - 2r + 2s) + (-p - 2q - s + r)\beta$

- $a\beta + b$ behoort tot het bereik van ρ_5 als en slechts als er gehele getallen p en q bestaan waarvoor $\begin{cases} -p - 2q - s + r = a \\ 1 - 3p - q - 2r + 2s = b \end{cases}$.

- Uit de eerste vergelijking volgt dat $p = -2q - s + r - a$. Ingevuld in de tweede vergelijking geeft dit : $b = 1+3a+5q-5r+5s$. Dus moet $b-1-3a$ een vijfvoud zijn.

- Omdat $a\beta + b$ een eenheid is in $\mathbb{Z}(\beta)$ moet $a\beta + b$ van de vorm $\pm\beta^t$ zijn met $t \in \mathbb{Z}$. De kleinste positieve waarde van t waarvoor $b - 1 - 3a$ een vijfvoud is, blijkt 2 te zijn. Inderdaad $-\beta^2 = \beta - 1$ en dan is $b - 1 - 3a = -1 - 1 - 3 = -5$.

- Verder kan men gemakkelijk narekenen dat als $a\beta + b$ en $c\beta + d$ allebei vijfvouden zijn, dat ook hun product een vijfvoud is. Dus is Im $\rho_5 = \langle -\beta^2 \rangle$.

4.3.5 Eindspel

- We maken gebruik van een isomorfisme stelling uit de theorie der groepen die zegt dat

$$U(\mathbb{Z}C_{10}^+)/\text{ ker } \rho_{10} \cong \text{ Im } \rho_{10}$$

- Eerst zoeken we een eenheid in $\mathbb{Z}C_{10}^+$ die, door ρ_{10}, afgebeeld wordt op het genererende element $-\alpha^2$ van Im ρ_{10}. Dit element moet door ρ_5 ook afgebeeld worden op een eenheid van $\mathbb{Z}(\epsilon_5)$. We kennen al zo een element, namelijk $g^2 + g^8 - 1$.

- We kunnen uiteraard ook een ander element zoeken. In de projectie in $\mathbb{Z}(\epsilon_{10})$ moet $a = b = -1$, zodat $\gamma = (-1+2s)+(r-1)(g+g^{-1})+(1-r-s)(g^2+g^{-2})+(1-r-s)(g^3+g^{-3})+r(g^4+g^{-4})+2sg^5$. De projectie in $\mathbb{Z}(\epsilon_5)$ geeft dan $\rho_5(\gamma) = (-1+2s)+(r-1)\beta+(1-r-s)(-1-\beta)+(1-r-s)(-1-\beta)+r\beta+2s = (-3+2r+6s)+(-3+4r+2s)\beta$. Om een eenheid te zijn moet $-3+2r+6s-1-3(-3+4r+2s)$ een vijfvoud zijn. Dit is altijd zo. Dus kunnen we r en s vrij kiezen. Neem bijvoorbeeld $r = s = 1$ dan vinden we $u = 1 - (g^2 + g^{-2}) - (g^3 + g^{-3}) + (g^4 + g^{-4}) + 2g^5$.

- Vervolgens zoeken we een element van de kern van ρ_{10}, dat door ρ_5 afgebeeld wordt op een genererend element van $\rho_5(\text{ ker } \rho_{10})$.

- Neem $\gamma = 1+2s+r(g+g^{-1})+(-r-s)(g^2+g^{-2})+(-r-s)(g^3+g^{-3})+r(g^4+g^{-4})+2sg^5$ een element van de kern van ρ_{10}, dan is $\rho_5(\gamma) = 1+2s+r\beta+(-r-s)(-1-\beta)+(-r-s)(-1-\beta)+r\beta+2s = (1+2r+6s)+(4r+2s)\beta$. De eerste macht van $-\beta^2$, waarvoor een gehele r en s kan gevonden worden is $-\beta^6$. Aldus is $\rho_5(\text{ ker } \rho_{10}) = \langle -\beta^6 \rangle$.

- Het element van $\mathbb{Z}C_{10}^+$ dat hiermee overeen komt voldoet aan $(1 + 2r + 6s) + (4r + 2s)\beta = -\beta^6 = 8\beta - 5$ en dus is $\begin{cases} 4r + 2s = 8 \\ 1 + 2r + 4s = -5 \end{cases}$. Hieruit volgt dat $s = -2$ en $r = -1$. Het overeenkomstige element is $v = -3 + 3(g^{g-1}) - (g^2 + g^{-2}) - (g^3 + g^{-3}) + 3(g^4 + g^{-4}) - 4g^5$.

Stelling 4.6. $U(\mathbb{Z}C_{10}) = \pm C_{10} \times \langle g^2 + g^8 - 1\rangle \times \langle -3 + 3(g + g^{-1}) - (g^2 + g^{-2}) - (g^3 + g^{-3}) + 3(g^4 + g^{-4}) - 4g^5\rangle$.

4.3.6 Vezelproduct

- Bekijken we eerst volgend commutatief diagramma:

$$\begin{array}{ccc} \mathbb{Z}C_{10} & \xrightarrow{f} & \mathbb{Z}(C_5) \oplus \mathbb{Z}C_2 \\ \downarrow g & & \downarrow i \\ \mathbb{Z}(\epsilon_{10}) & \xrightarrow{j} & \mathbb{Z}_2(\epsilon_5) \oplus \mathbb{Z}_5 \end{array}$$

  Noteer $a = \sum_{i=0}^{9} a_i g^i$, dan is de eerste component van $f(a)$ gelijk aan $(a_0 + a_5) + (a_1 + a_6)g + (a_2 + a_7)g^2 + (a_3 + a_8)g^3 + (a_4 + a_9)g^4$. De tweede component is dan $(a_0 + a_2 + a_4 + a_6 + a_8) + (a_1 + a_3 + a_5 + a_7 + a_9)g$. Verder is $g(a) = (a_0 - a_4 - a_5 + a_9) + (a_1 + a_4 - a_6 - a_9)\epsilon_{10} + (a_2 - a_4 - a_7 + a_9)\epsilon_{10}^2 + (a_3 + a_4 - a_8 - a_9)\epsilon_{10}^3$. Om het beeld te berekenen onder i van de eerste component, moeten we g vervangen door ϵ_5 en de coëfficiënten modulo 2 uitrekenen. Voor de twee component vervangen we g door -1 en rekenen we modulo 5. Om de eerste component van het j-beeld te bepalen vervangen we ϵ_{10} door ϵ_5 en rekenen we modulo 2. Voor de tweede component, vervangen ϵ_{10} door 1 en rekenen we modulo 5.

- Bekijken we nu het commutatief diagramma met de eenhedengroepen :

$$\begin{array}{ccc} U(\mathbb{Z}C_{10}) & \xrightarrow{f} & U(\mathbb{Z}(C_5)) \oplus U(\mathbb{Z}C_2) \\ \downarrow g & & \downarrow i \\ U(\mathbb{Z}(\epsilon_{10})) & \xrightarrow{j} & U(\mathbb{Z}_2(\epsilon_5)) \oplus U(\mathbb{Z}_5) \end{array}$$

  We zoeken nu naar elementen in $U(\mathbb{Z}(\epsilon_{10}))$ en $U(\mathbb{Z}(C_5)) \oplus U(\mathbb{Z}C_2)$ die door respectievelijk j en i hetzelfde beeld hebben.

- We vinden:

$$\begin{array}{ccc} u & \xrightarrow{f} & ((-1 + g^2 + g^3)^2, g) \\ \downarrow g & & \downarrow i \\ (1 + \epsilon_{10}^2 - \epsilon_{10}^3)^2 & \xrightarrow{j} & (\epsilon_5^2 + \epsilon_5^3, -1 \end{array}$$

  en nog een tweede mogelijkheid:

$$\begin{array}{ccc} v & \xrightarrow{f} & ((-1 + g^2 + g^3)^3, 1) \\ \downarrow g & & \downarrow i \\ 1 & \xrightarrow{j} & (1, 1) \end{array}$$

- Het expliciet uitrekenen van u en v geeft :
  $u = 2 + (g + g^5 + g^9) - (g^2 + g^3 + g^7 + g^8)$
  $v = -3 - 4g^5 - (g + g^4 + g^6 + g^9) + 3(g^2 + g^3 + g^7 + g^8)$.

Stelling 4.7. $U(\mathbb{Z}C_{10}) = \pm C_{10} \times \langle 2 + (g + g^5 + g^9) - (g^2 + g^3 + g^7 + g^8)\rangle \times \langle -3 + 3(g + g^{-1}) - (g^2 + g^{-2}) - (g^3 + g^{-3}) + 3(g^4 + g^{-4}) - 4g^5\rangle$.