Bass eenheden in $\mathbb{Z}G$.

Hoofdstuk 1

Bass eenheden

1.1 Cyclotomische eenheden in $\mathbb{Z}(\epsilon_n)$

Als G een abelse groep is, dan zijn de bicyclische eenheden in $\mathbb{Z}G$ allemaal triviaal. We moeten in die situatie dus op zoek gaan naar andere constructies voor eenheden. Veronderstel dat ϵ_n een primitieve n-de wortel is uit 1, m.a.w $\epsilon_n = e^{\frac{2\pi i}{n}} = cos\frac{2\pi}{n} + i.\sin\frac{2\pi}{n}$. Beschouw de ring $\mathbb{Z}(\epsilon_n)$. Construeer nu

$$\eta_k(\epsilon_n) = \frac{\epsilon_n^k - 1}{\epsilon_n - 1} = 1 + \epsilon_n + \epsilon_n^2 + \cdots + \epsilon_n^{k-1}$$

Stelling 1.1. *Als k en n onderling ondeelbaar zijn, dan is $\eta_k(\epsilon_n)$ een eenheid en $\eta_k(\epsilon_n)^{-1} = \eta_l(\epsilon_n^k)$, waarbij $k.l \equiv 1$ mod n.*

Bewijs. Als k en n onderling ondeelbaar zijn, dan bestaat er een natuurlijk getal l zodat $k.l \equiv 1 \bmod n$.

$$\begin{aligned}(\eta_k(\epsilon_n))^{-1} =& \frac{\epsilon_n - 1}{\epsilon_n^k - 1}\\ =& \frac{\epsilon_n^{kl} - 1}{\epsilon_n^k - 1}\\ =& \frac{(\epsilon_n^k)^l - 1}{\epsilon_n^k - 1}\\ =& 1 + \epsilon_n^k + \epsilon_n^{2k} + \cdots + \epsilon_n^{(l-1)k}\\ =& \eta_l(\epsilon_n^k)\end{aligned}$$

□

Eenheden in $\mathbb{Z}(\epsilon_n)$ van de vorm $\eta_k(\epsilon_n)$, waarbij k en n onderling ondeelbaar zijn, noemen we *cyclotomische eenheden of circulaire eenheden* . Ze werden voor het eerst gebruikt door Kummer in 1847. De cyclotomische eenheden, samen met de triviale eenheden ϵ_n^k met $k \in \mathbb{Z}$, vormen een deelgroep van de groep van alle eenheden in $\mathbb{Z}(\epsilon_n)$. Deze deelgroep noemen we de *groep van de cyclotomische eenheden* . De index van deze deelgroep in de groep van alle eenheden van $\mathbb{Z}(\epsilon_n)$ is steeds eindig.

Een paar voorbeelden:

- De cyclotomische eenheden in $\mathbb{Z}(\omega)$, met ω een primitieve derdemachtswortel uit 1, zijn $\eta_1(\omega) = 1$ en $\eta_2(\omega) = 1 + \omega = -\omega^2$. De cyclotomische eenheden zijn allemaal triviaal.

- De cyclotomische eenheden in $\mathbb{Z}(i)$ zijn $\eta_1(i) = 1$ en $\eta_3(i) = i$. Ook hier zijn de cyclotomische eenheden zijn allemaal triviaal.

- De cyclotomische eenheden in $\mathbb{Z}(\epsilon_5)$ zijn $\eta_1(\epsilon_5) = 1$, $\eta_2(\epsilon_5) = 1 + \epsilon_5$, $\eta_3(\epsilon_5) = 1 + \epsilon_5 + \epsilon_5^2 = -\epsilon_5^3.\eta_2(\epsilon_5)$ en $\eta_4(\epsilon_5) = 1 + \epsilon_5 + \epsilon_5^2 + \epsilon_5^3 = -\epsilon_5^4$.

Geven we ook nog een paar eigenschappen:

Stelling 1.2. *Als k en n onderling ondeelbaar zijn, dan geldt*

$$\eta_{-k}(\epsilon_n) = -\epsilon_n^{-k}\eta_k(\epsilon_n)$$

.

Bewijs.

$$\begin{aligned}\eta_{-k}(\epsilon_n) =& \frac{\epsilon_n^{-k} - 1}{\epsilon_n - 1}\\ =& \frac{1 - \epsilon_n^k}{(\epsilon_n - 1)\epsilon_n^k}\\ =& -\epsilon_n^{-k}\eta_k(\epsilon_n)\end{aligned}$$

□

Stelling 1.3. *Als k en k_1 onderling ondeelbaar zijn met n, dan geldt*

$$k \equiv k_1 \ mod \ n \Leftrightarrow \eta_k(\epsilon_n) = \eta_{k_1}(\epsilon_n)$$

.

Bewijs. Uit $k \equiv k_1 \bmod n$ volgt dat $k = k_1 + p.n$ met $p \in \mathbb{Z}$.

$$\begin{aligned}
\eta_k(\epsilon_n) =& \frac{\epsilon_n^{k_1+pn} - 1}{\epsilon_n - 1} \\
=& \frac{\epsilon_n^{k_1}.\epsilon_n^{pn} - 1}{\epsilon_n - 1} \\
=& \frac{\epsilon_n^{k_1}. - 1}{\epsilon_n - 1} \\
=& \eta_{k_1}(\epsilon_n)
\end{aligned}$$

Omgekeerd, als $\eta_k(\epsilon_n) = \eta_{k_1}(\epsilon_n)$, dan is $\epsilon_n^k = \epsilon_n^{k_1}$. Hieruit volgt dat $k = k_1 + p.n$, wat moest bewezen worden. □

Stelling 1.4. *Als k onderling ondeelbaar is met n, dan is $\eta_k(\epsilon_n)$ een wortel uit 1 als en slechts als $k \equiv \pm 1$ mod n.*

Bewijs. Als $k = 1$, dan is $\eta_1(\epsilon_n) = 1$ en als $k = -1$, dan is $\eta_{-1}(\epsilon_n) = -\epsilon_n^{-1}$. In beide gevallen dus een wortel uit de eenheid.
Veronderstel omgekeerd dat $\eta_k(\epsilon_n)$ een wortel uit 1 is. Maar dan is $|\eta_k(\epsilon_n)| = 1$. Hieruit volgt dat $|\epsilon_n^k - 1| = |\epsilon_n - 1|$. Omdat alle machten van ϵ_n een regelmatige n-hoek vormen op de eenheidscirkel, betekent vorige gelijkheid dat ϵ_n^k op de eenheidscirkel ligt, evenver van 1 als ϵ_n. Dus moet $\epsilon_n^k = \epsilon_n$ of $\epsilon_n^k = \epsilon_n^{-1}$. Bijgevolg is $k = \pm 1$, wat moest bewezen worden. □

Uit vorige stellingen kan je afleiden dat de groep van de cyclotomische eenheden voortgebracht wordt door de eenheden $\pm\epsilon_n^k$ en door de eenheden $\eta_k(\epsilon_n)$ met $1 < k < \frac{n}{2}$. Zo is bijvoorbeeld een willekeurig element van de groep van de cyclotomische eenheden in $\mathbb{Z}(\epsilon_5)$ van de vorm $\pm\epsilon_5^p\eta_2(\epsilon_5)^q = \pm\epsilon_5^p(1+\epsilon_5)^q$, met $p, q \in \mathbb{Z}$.

1.2 Bass eenheden

Hoe kunnen we het idee van de cyclotomische eenheden overbrengen naar $\mathbb{Z}G$? Neem $g \in G$ met $o(g) = n$ en k onderling ondeelbaar met n of met andere woorden er bestaat een l zodat $kl \equiv 1 \bmod n$.
Construeer dan $\chi_k(g) = 1 + g + g^2 + \cdots + g^{k-1}$. Nu is $\chi_k(g)$ geen eenheid in $\mathbb{Z}G$ omdat de augmentatieafbeelding $\chi_k(g)$ niet afbeeldt op 1. Er geldt immers $\operatorname{aug} \chi_k(g) = k$. Noteer verder $1 + g + g^2 + \cdots + g^{n-1} = \tilde{g}$

Stelling 1.5. *$g \in G$ met $o(g) = n$. Als k en k' onderling ondeelbaar zijn met n en $k \equiv k' \bmod n$ dan is $\chi_k(g) = \chi_{k'}(g) + s\tilde{g}$ met $s \in \mathbb{Z}$.*

Bewijs. Als $k \equiv k' \bmod n$, dan bestaat er een geheel getal s zodat $k' = k+sn$. Dan is $\chi_{k'}(g) = 1+g+\cdots+g^{n-1}+g^n+\cdots+g^{2n-1}+\cdots+g^{sn}+\cdots+g^{sn+k-1} = \tilde{g} + g^n\tilde{g} + \cdots + g^{(s-1)n}\tilde{g} + g^{sn}(1 + g + \cdots + g^{k-1}) = s\tilde{g} + \chi_k(g)$. ☐

We zouden dan, als eenheid, iets kunnen voorstellen van de vorm $u = \chi_k(g) + s\tilde{g}$. Om een eenheid te kunnen zijn moet $\operatorname{aug}(u) = k + sn = 1$. Om een gehele oplossing te hebben voor s zou $1 - k$ moeten deelbaar zijn door n of met andere woorden $k \equiv 1 \bmod n$. Dit is te beperkend voor k. Omdat k en n echter onderling ondeelbaar zijn, kunnen we gebruik maken van de stelling van Fermat die zegt $k^{\varphi(n)} \equiv 1 \bmod n$. Neem dan m, zodat $k^m \equiv 1 \bmod n$ en definieer vervolgens als kandidaat eenheid:

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

Stelling 1.6. $u_{1,m}(g) = 1$

Bewijs. $u_{1,m}(g) = 1 + \dfrac{1 - 1^m}{n}(1 + g + \cdots + g^{n-1}) = 1.$ ☐

Stelling 1.7. $r = \frac{1-k^m}{n}$ *is het unieke geheel getal zodat*

$$aug\left(\chi_k^m(g) + r(1 + g + \cdots + g^{n-1})\right) = 1$$

Bewijs. aug $(\chi_k^m(g) + r(1 + g + \cdots + g^{n-1})) = k^m + rn$. Dit wordt dus 1 als en slechts als $k^m + rn = 1$ Deze vergelijking heeft een unieke oplossing: $r = \frac{1-k^m}{n}$. Dat r een geheel getal is volgt uit een vorige opmerking over de stelling van Fermat. □

Stelling 1.8. $u_{n-1,m}(g) = g^{(n-1)m}$

Bewijs. $u_{n-1,m}(g) = \left(\tilde{g} - g^{n-1}\right)^m + r\tilde{g} = c\tilde{g} + (-g^{(n-1)m}$. Omdat de augmentatie van $u_{n-1,m}(g) = 1$ volgt hieruit dat $cn + (-1)^{(n-1)m)=1}$. Maar dan moet $c = 0$ en dus is $u_{n-1,m}(g) = g^{(n-1)m}$. □

Stelling 1.9. *Veronderstel $g \in G$, $o(g) = n$ en k, k' onderling ondeelbaar met n. Als $k \equiv k'$ mod n, dan is $u_{k,m}(g) = u_{k',m}(g)$*

Bewijs. $u_{k',m}(g) = \chi_{k'}^m(g) + r\tilde{g}$ met $r = \dfrac{1-k'^m}{n}$. Uit stelling 1.5 volgt dan dat: $u_{k',m}(g) = (\chi_k(g)+s\tilde{g})^m + r\tilde{g} = \chi_k^m(g) + \binom{m}{1}\chi_k^{m-1}(g)s\tilde{g} + \cdots + s^m\tilde{g}^m + r\tilde{g}$.
Omdat $\tilde{g}^a = a\tilde{g}$, kunnen we vorige gelijkheid herschrijven als:
$u_{k',m}(g) = \chi_k^m(g) + \binom{m}{1}\chi_k^{m-1}(g)s\tilde{g} + \cdots + m.s^m\tilde{g} + r\tilde{g}$. Nu geldt ook dat:
$r\tilde{g} = \dfrac{1-k'^m}{n}\tilde{g} = \dfrac{1-(k+sn)^m}{n}\tilde{g} = \dfrac{1-k^m-\binom{m}{1}k^{m-1}sn - \cdots - s^mn^m}{n}\tilde{g}$.
In de uitwerking van $u_{k',m}(g)$ komen twee termen voor met $\binom{m}{1}$. Als we die samenbrengen dan bekomen we: $\binom{m}{1}.\left(\chi_k^{m-1}(g)s\tilde{g} - k^{m-1}s\tilde{g}\right)$. Omdat $\chi_k^{m-1}(g)\tilde{g} = k^{m-1}\tilde{g}$ wordt de term met $\binom{m}{1}$ gelijk aan 0. Analoog voor alle andere termen met $\binom{m}{p}$. Uiteindelijk blijft er dus nog over :
$u_{k',m}(g) = \chi_k^m(g) + \dfrac{1-k^m}{n}\tilde{g} = u_{k,m}(g)$.

□

Stelling 1.10. *Veronderstel $g \in G$, $o(g) = n$ en k, l onderling ondeelbaar met n en $kl \equiv 1 \bmod n$. Dan is :*

$$u_{k,m}^{-1}(g) = u_{l,m}(g^k)$$

Bewijs. Noteer $u_{k,m}(g).u_{l,m}(g^k) = A$. We moeten enkel bewijzen dat $A = 1$. Welnu $A = \Big((1 + g + \cdots + g^{k-1})^m + \dfrac{1-k^m}{n}\tilde{g}\Big).\Big((1 + g^k + \cdots + g^{k(l-1)})^m + \dfrac{1-l^m}{n}\tilde{g^k}\Big)$. Zeker is $\tilde{g^k} = \tilde{g}$. Gebruikmakend van de distributiviteit krijgen we vier termen in de uitrekening van A. Eerst hebben we, gebruikmakend van $kl \equiv 1 \bmod n$, dat $\Big((1+g+\cdots+g^{k-1}).(1+g^k+\cdots+g^{k(l-1)})\Big)^m = \Big(1+g^k+\cdots+g^{k(l-1)}+g+g^{k+1}+\cdots+g^{k(l-1)+1}+\cdots+g^{k-1}+g^{k-1+k}+\cdots+g^{k(l-1)+k-1}\Big)^m = \chi_{kl}^m(g)$. De andere drie termen in de uitrekening van A bevatten allen een factor $\tilde{g}$. Uitgerekend krijgen we, via $g^a.\tilde{g} = \tilde{g}$, dat de som van die drie termen gelijk is aan: $\Big(k^m\dfrac{1-l^m}{n} + l^m\dfrac{1-k^m}{n} + \dfrac{(1-k^m)(1-l^m}{n}\Big)\tilde{g} = \dfrac{1-k^m l^m}{n}\tilde{g}$. Omdat het beeld van A onder de augmentatie afbeelding gelijk is aan $(kl)^m + \dfrac{1-k^m l^m}{n}.n = 1$, is $A = u_{kl,m}(g)$. Volgens stelling 1.8 en 1.6 is dan $A = u_{1,m}(g) = 1$. Hiermee is het gestelde bewezen.

□

De kandidaat eenheid $u_{k,m}(g)$ is dus effectief een eenheid van $\mathbb{Z}G$. We noemen het een *Bass eenheid* of een *Bass cyclische eenheid* . Volgens stelling 1.8 kunnen we bij een Bass eenheid $u_{k,m}(g)$ dus steeds veronderstellen dat $1 \leq k < n$.

Stelling 1.11. *Veronderstel $g \in G$, $o(g) = n$ en k onderling ondeelbaar met n. Dan is :*

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

Bewijs. Het linkerlid is gelijk aan:
$\Big((1 + g + \cdots + g^{k-1})^m + r\tilde{g}\Big)\Big((1 + g + \cdots + g^{k-1})^{m_1} + r_1\tilde{g}\Big) =$

$(1+g+\cdots+g^{k-1})^{m+m_1}+\Big((1+g+\cdots+g^{k-1})^m r_1+(1+g+\cdots+g^{k-1})^{m_1} r+rr_1 n\Big)\tilde{g}.$
Berekenen we nu de tweede term in die som:
$(k^m r_1+k^{m_1} r+rr_1 n)\tilde{g} = \Big(k^m \frac{1-k^{m_1}}{n}+k^{m_1}\frac{1-k^m}{n}+\frac{(1-k^{m_1})(1-k^m)}{n}\Big)\tilde{g} = \frac{1-k^{mm_1}}{n}$. Bijgevolg is het volledige linkerlid gelijk aan $u_{k,m+m_1}(g)$.

□

Bijgevolg zijn alle Bass eenheden van de vorm $u_{k,m}(g)$ machten van de Bass eenheid $u_{k,m_k}(g)$, waarbij m_k de orde is van k in de multiplicatieve groep $\mathbb{Z}_n^{\times}$. De groep voortgebracht door de eenheden $u_{k,m}(g)$, voor een bepaalde g, wordt dus eindig voortgebracht door de eenheden van de vorm $u_{k,m_k}(g)$, met $1 \leq k < |g|$.

Stelling 1.12. *Veronderstel $g \in G$, $o(g) = n$ en k, l onderling ondeelbaar met n. Dan is :*

$$u_{k,m}(g).u_{l,m}(g^k) = u_{kl,m}(g)$$

Bewijs. $u_{k,m}(g).u_{l,m}(g^k) = \Big((1+g+\cdots+g^{k-1})^m + \frac{1-k^m}{n}\tilde{g}\Big)\Big((1+g^k+\cdots+g^{k(l-1)})^m + \frac{1-l^m}{n}\tilde{g}\Big)$. Analoog aan stelling 1.10 geeft dit als resultaat $(1+g+\cdots+g^{kl-1})^m + \frac{1-(kl)^m}{n}\tilde{g} = u_{kl,m}(g)$. □

Gevolg 1.13. *Als $(-1)^m \equiv 1 \bmod n$, dan is $u_{n-k,m}(g) = u_{k(n-1),m}(g) = u_{k,m}(g)u_{n-1,m}(g^k) = u_{k,m}(g)g^{-km}$*

Gevolg 1.14. *Als $(k-1)m$ deelbaar is door n, dan is $u_{-1,m}(g)u_{k,m}(g^{-1}) = u_{-k,m}(g) = u_{n-k,m}(g) = u_{k,m}(g)g^{-km}$. Omdat $u_{-1,m} = g^{(n-1)m}$ volgt hieruit dat $u_{k,m}(g^{-1})g^{n+k-1)m} = u_{k,m}(g)$. Zodat $u_{k,m}(g^{-1}) = u_{k,m}(g)$.*

Nemen we als voorbeeld C_5, de cyclische groep van orde 5, voortgebracht door g.

- Het element g heeft orde 5 en $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$. De ordes van die elementen in $\mathbb{Z}_5^\times$ zijn respectievelijk $1, 4, 4, 2$.
- Neem $k = 2$, dan berekenen we de Bass eenheid $u_{2,4}(g) = (1+g)^4 + \dfrac{1-2^4}{5}(1+g+g^2+g^3+g^4) = -2+g+3g^2+g^3-2g^4$.
- We zullen deze eenheid verder noteren als u.
- De inverse van u is dan $u^{-1} = u_{3,4}(g^2) = 1+g-2g^2+3g^3-2g^4$.
- Elke andere waarde van m in $u_{2,m}(g)$ moet voldoen aan $2^m \equiv 1 \bmod 5$. Dus moet m een viervoud zijn. Uit stelling 1.10 volgt dan dat $u_{2,4p}(g) = u_{2,4}^p(g)$.
- Neem $k = 3$, dan berekenen we de Bass eenheid $u_{3,4}(g) = (1+g+g^2)^4 + \dfrac{1-3^4}{5}(1+g+g^2+g^3+g^4) = 1-2g-2g^2+g^3+3g^4$. Maar volgens gevolg 1.13 is $u_{3,4}(g) = u_{2,4}(g).g^2$
- Neem $k = 4$, dan berekenen we de Bass eenheid $u_{4,2}(g) = (1+g+g^2+g^3)^2 + \dfrac{1-4^2}{5}(1+g+g^2+g^3+g^4) = g^3$. Deze Bass eenheid is dus triviaal.
- In volgende tabel berekenen we alle Bass eenheden met $m = 4$:

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

- De Bass cyclische eenheden bepalen altijd een deelgroep van eindige index in $U(\mathbb{Z}(G))$. In dit geval is elke eenheid van $\mathbb{Z}C_5$ te schrijven in de vorm $g^p.u^q$.

Van bicyclische eenheden weten we dat ze ofwel triviaal zijn , ofwel oneindige orde hebben (torsievrij). Kunnen we een gelijkaardig resultaat vinden voor de Bass eenheden?

Stelling 1.15. *Een Bass eenheid $u_{k,m}(g)$ is torsie als en slechts als $k \equiv \pm 1 mod\ |g|$.*

Bewijs.

- Als $k \equiv +1 \bmod |g|$, dan is volgens stelling 1.6 en 1.8 $u_{k,m}(g) = 1$. Dus een torsie element.
- Veronderstel $|g| = n$. Als $k \equiv -1 \text{mod } |g|$, dan is $k = n-1$ en $m = 2$ omdat $(n-1)^2 = n^2 - 2n + 1 \equiv 1 \bmod n$. Bijgevolg is $u_{k,m}(g) = (1 + g + \cdots + g^{n-2})^2 + \frac{1-(n-1)^2}{n}\tilde{g} = (\tilde{g} - g^{n-1})^2 + (2-n)\tilde{g} = g^{2n-1}$ en dit is duidelijk een torsie element.
- Veronderstel omgekeerd dat $u_{k,m}(g)$ een torsie element is. Breidt het groepshomomorfisme f dat g afbeeldt op ϵ_n uit tot een ring homomorfisme tussen $\mathbb{Z}\langle g \rangle$ en $\mathbb{C}$. dan is $f(\tilde{g}) = 1 + \epsilon_n + \cdots + \epsilon_n^{n-1} = 0$, zodat $f(u_{k,m}(g)) = \eta_k^m(\epsilon_n)$. Omdat $u_{k,m}(g)$ een torsie element is, zal $f(u_{k,m}(g))$ dat ook zijn en dus is ook $\eta_k^m(\epsilon_n)$ een torsie element en dus een wortel uit de eenheid. Bijgevolg is $|1+\epsilon_n+\cdots+\epsilon_n^{k-1}| = |\frac{\epsilon_n^k - 1}{\epsilon_n}| = 1$. Hieruit volgt dat $|\epsilon_n^k - 1| = |\epsilon_n|$. Maar dan is $\epsilon_n^k = \epsilon_n$ of $\epsilon_n^k = \epsilon_n^{-1}$. Dus $k \equiv \pm 1 \text{mod } |g|$.

$\square$