Roosters

Mennema, I.

Ingela Mennema

Roosters

Bachelorscriptie

Scriptiebegeleider: Dr. R.M. van Luijk en H.D. Visse MSc

Datum Bachelorexamen: 28 juni 2016

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Inleiding

Iedereen kent het rooster $\mathbb{Z}^2$, maar wat is nou de precieze definitie van een rooster? In mijn scriptie ga ik die definitie geven en ook meerdere invarianten van een rooster definiëren. Het grootste deel van mijn scriptie besteed ik aan het bewijzen van de volgende stelling:

Stelling 4.2 *Zij E een geheel, unimodulair, indefiniet rooster, van type II met positieve index. Dan is E isomorf met $pU \oplus q\Gamma_8$, waarbij $p = \frac{1}{2}(r(E) - \tau(E))$ en $q = \frac{1}{8}\tau(E)$.*

Deze stelling is nu nog onbegrijpbaar, maar ik zal deze eigenschappen van een rooster definiëren in mijn scriptie. De bedoeling is dat na het lezen van mijn scriptie alles over deze stelling duidelijk is.
Voordat je deze stelling überhaupt kunt formuleren, moet je eerst weten of $\tau(E)$ wel deelbaar is door acht. Anders is q geen geheel getal. In het derde hoofdstuk wordt dit aangetoond door een groep $K(S)$ te construeren die voldoet aan de universele eigenschap van de Grothendieck groep.
In het laatste deel van mijn scriptie definieer ik een speciaal soort deelverzameling van een rooster, namelijk een wortelsysteem. Het wortelsysteem E_8 van dimensie 8, wordt hier ook beschouwd. Mijn hele scriptie is gebaseerd op hoofdstuk vijf van het boek "A course in Arithmetic van Serre"[1].

2 Roosters

2.1 Definities, invarianten en voorbeelden

Definitie 2.1. Een *rooster* is een eindig voortgebrachte vrije abelse groep E met een symmetrisch bilineaire vorm $\varphi : E \times E \to \mathbb{Q}$ zodanig dat
het homomorfisme $\varphi^* : E \to \mathrm{Hom}(E, \mathbb{Q})$ gegeven door $x \mapsto \varphi(x, \_)$ injectief is.
Notatie: $\varphi(x, y) = \langle x, y \rangle$.

Opmerking 2.2. We noteren $\langle \_, \_ \rangle_s$ als het standaardinproduct, oftewel

$$\langle x, y \rangle_s = \sum_{i=1}^{n} x_i y_i,$$

met $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{R}^n$.

Definitie 2.3. Een rooster E heet *geheel* als voor alle $x, y \in E$ geldt $\varphi(x, y) \in \mathbb{Z}$.

Definitie 2.4. Zij E een rooster. De *rang* van E is het getal $n \in \mathbb{N}$ waarvoor E als groep isomorf is met $\mathbb{Z}^n$.
Notatie: $r(E)$.

Definitie 2.5. Zij E een rooster. Laat $(v_1, ..., v_n)$ een basis zijn voor E. Zij $A := (\langle v_i, v_j \rangle)_{ij}$. De matrix A is congruent over $\mathbb{R}$ met een unieke matrix

$$C = \left(\begin{array}{c|c} I_s & 0 \\ \hline 0 & -I_t \end{array} \right),$$

waarbij s het aantal positieve eigenwaarden van de matrix A aangeeft en t het aantal negatieve eigenwaarden. De *index* van E is het getal $s - t$.
Notatie: $\tau(E)$.

Opmerking 2.6. De index van een rooster E is onafhankelijk van de gekozen basis.

Opmerking 2.7. Er geldt $r(E) = s + t$. Hieruit volgt $-r(E) \leq \tau(E) \leq r(E)$ en $r(E) \equiv \tau(E) \mod 2$.

Definitie 2.8. Zij E een eindig voortgebrachte vrije abelse groep of een vectorruimte, met een symmetrisch bilineaire vorm $\varphi : E \times E \to \mathbb{Z}$. Zij $B = (v_1, ..., v_n)$ een basis voor E. De matrix $A = (\langle v_i, v_j \rangle)_{ij}$ heet de *Gram matrix*. De *discrimant* van E is gelijk aan de determinant van de matrix A.
Notatie: $d(E)$.

Lemma 2.9. *De discriminant van een eindig voortgebrachte vrije abelse groep is onafhankelijk van de gekozen basis.*

Bewijs. Laat $C = (v'_1, ..., v'_n)$ een andere basis zijn voor E en zij $A' := (\langle v'_i, v'_j \rangle)_{ij}$. Er bestaan inverteerbare matrices $Q, Q' \in \mathrm{Mat}(n, \mathbb{Z})$ zodanig dat $A = Q^\top A' Q$ en $A' = Q'^\top A Q'$. Zij $x \in E$. Laat $x_B = (x_1, ..., x_n)$ en $x_C = (x'_1, ..., x'_n)$ zijn zodanig dat $x = x_1 v_1 + ... + x_n v_n$ respectievelijk $x = x'_1 v'_1 + ... + x'_n v'_n$. Merk op $x_C = Q x_B$ en $x_B = Q' x_C$. Hieruit volgt $QQ' = I$, oftewel

$$\det(Q) \det(Q') = \det(I) = 1.$$

Aangezien Q en Q' gehele coëfficiënten hebben, geldt er $\det(Q) = \det(Q') = \pm 1$. Hieruit volgt

$$\det(A) = \det(Q^\top)\det(A)\det(Q) = \det(Q)^2\det(A) = (\pm 1)^2\det(A) = \det(A').$$

□

Opmerking 2.10. Een Gram matrix van een rooster is afhankelijk van de gekozen basis, maar de invarianten van een rooster zijn onafhankelijk van de gekozen basis. We spreken daarom vaak over dé Gram matrix van een rooster.

Definitie 2.11. Een *unimodulair* rooster is een geheel rooster E waarvoor geldt $d(E) = \pm 1$.
Notatie: $S_n := \{\text{unimodulaire roosters van rang n}\}$ en $S := \bigcup_{n\in\mathbb{N}} S_n$.

Stelling 2.12. *Zij E een eindig voortgebrachte vrije abelse groep met een symmetrisch bilineaire vorm $\varphi : E \times E \to \mathbb{Z}$. Zij $d(E) \neq 0$. Dan is het homomorfisme $\varphi^* : E \to \mathrm{Hom}(E, \mathbb{Z})$ injectief.*

Bewijs. Laat $B = (v_1, ..., v_n)$ een basis zijn voor E. Zij $A = (\langle v_i, v_j\rangle)_{ij}$ en $x, y \in E$. Dan geldt $x = x_1v_1 + ... + x_nv_n$ en $y = y_1v_1 + ... + y_nv_n$ voor zekere $x_i, y_i \in \mathbb{Z}$. Er geldt

$$\begin{aligned}\langle x, y\rangle &= \left(\sum_i x_iv_i\right)\left(\sum_i y_iv_i\right)\\ &= \begin{pmatrix}x_1, ..., x_n\end{pmatrix} A \begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}\\ &= \langle x_B^\top A, y_B\rangle_s\end{aligned}$$

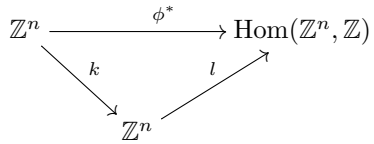
waarbij $x_B = (x_1, ..., x_n)$ en $y_B = (y_1, ..., y_n)$. Laat $f : \mathbb{Z}^n \to E$ gegeven worden door $(x_1, ..., x_n) \mapsto x_1v_1 + ... + x_nv_n$ en $f^\top : \mathrm{Hom}(E, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z})$ gegeven worden door $g \mapsto g \circ f$. Als we het bewijs volgen van Propositie 6.12 in het Lineaire Algebra 2 dictaat [3], vinden we dat $f^\top$ een isomorfisme is, omdat f een isomorfisme is.
Laat $\varphi^* : E \to \mathrm{Hom}(E, \mathbb{Z})$ gegeven worden door $x \mapsto \varphi(x, \_)$. Beschouw de afbeelding $\phi : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}$ die gegeven wordt door $(x, y) \mapsto \varphi(f(x), f(y))$. Laat $\phi^* : \mathbb{Z}^n \to \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z})$ gegeven worden door $x \mapsto \phi(x, \_)$. Het onderstaande diagram geeft deze afbeeldingen weer.

$$\begin{array}{ccc} E & \xrightarrow{\varphi^*} & \mathrm{Hom}(E, \mathbb{Z}) \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle f^\top} \\ \mathbb{Z}^n & \xrightarrow{\phi^*} & \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}) \end{array}$$

Het homomorfisme φ^* is injectief dan en slechts dan als ϕ^* injectief is. De afbeelding ϕ wordt ook gegeven door $(x, y) \mapsto y^T A'x$ met $A' = (\phi(e_i, e_j))_{i,j=1}^n$ waarbij $(e_1, ..., e_n)$ de standaardbasis is van $\mathbb{Z}^n$. Merk op dat geldt

$$A' = (\phi(e_i, e_j))_{i,j=1}^n = (\varphi(v_i, v_j))_{i,j=1}^n = A.$$

Er geldt $\phi^*(y) = \langle y^\top, A'x\rangle_s$. Laat $k : \mathbb{Z}^n \to \mathbb{Z}^n$ de afbeelding zijn die gegeven wordt door $x \mapsto A'x$. Laat $l : \mathbb{Z}^n \to \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z})$ de afbeelding zijn die gegeven wordt door $y \mapsto \phi(\_, y)$. Merk op $\phi^* = l \circ k$.



Als we het bewijs van propositie 4.31 volgen van het lineaire algebra 1 dictaat [2] vinden we dat de afbeelding l een bijectie is. Aangezien l een homomorfisme is, volgt nu dat de afbeelding l een isomorfisme is. Hieruit volgt dat ϕ^* injectief is dan en slechts dan als k injectief is.
Laat $k_{\mathbb{Q}} : \mathbb{Q}^n \to \mathbb{Q}^n$ de $\mathbb{Q}-$lineaire voortzetting zijn van k. Propositie 10.29 van het lineaire algebra 1 dictaat [2] geeft ons dat $k_{\mathbb{Q}}$ een isomorfisme is dan en slechts dan als $\det(k) \neq 0$. Hieruit volgt dat k op zijn minst injectief is, als $d(E) \neq 0$. □

Lemma 2.13. *Zij V een vectorruimte over een lichaam K met een symmetrisch bilineaire vorm $\varphi : V \times V \to K$. Laat $B = (v_1, ..., v_n)$ een basis zijn voor V en $A = (\varphi(v_i, v_j))_{ij}$ de Grammatrix van V zijn ten opzichte van de basis B. Er geldt $\det(A) \neq 0$ dan en slechts dan als het homomorfisme $\varphi^* : V \to \mathrm{Hom}(V, K)$ een isomorfisme is.*

Bewijs. We kunnen het grootste deel van het bewijs volgen van Stelling 2.12, waarbij we $\mathbb{Z}$ vervangen door K en injectief vervangen door isomorfisme. We vervolgen het bewijs na het tweede diagram.
Vanwege propositie 4.31 van het lineaire algebra 1 dictaat [2], volgt dat de afbeelding l een bijectie is. Aangezien l een homomorfisme is, volgt nu dat de afbeelding l een isomorfisme is. Hieruit volgt dat ϕ^* een isomorfisme is dan en slechts dan als k een isomorfisme is.
Propositie 10.29 van het lineaire algebra 1 dictaat [2] geeft ons dat k een isomorfisme is dan en slechts dan als $\det(A) \neq 0$. □

Stelling 2.14. *Zij E een geheel rooster. Dan geldt $E \in S_n$ dan en slechts dan als het homomorfisme $\varphi^* : E \to \mathrm{Hom}(E, \mathbb{Z})$ gegeven door $x \mapsto \langle x, \_\rangle$ een isomorfisme is.*

Bewijs. We volgen het bewijs van Stelling 2.12 tot de laatste alinea, waarbij we injectief vervangen door isomorfisme.
De afbeelding k is een isomorfisme dan en slechts dan als er een $B \in \mathrm{Mat}(n, \mathbb{Z})$ bestaat zodanig dat geldt $A'B = I_n = BA'$. We gaan nu allebei de implicaties bewijzen.
Zij φ^* een isomorfisme. Dan is ϕ^* een isomorfisme. Hieruit volgt dat k een isomorfisme is, oftewel er bestaat een $B \in \mathrm{Mat}(n, \mathbb{Z})$ zodanig dat $A'B = I_n$. Aangezien A' en B gehele coëfficiënten hebben geldt er $\det(A')\det(B) = 1$, oftewel $\det(A') = \pm 1$. Hieruit volgt $E \in S_n$.
Zij $E \in S_n$. Vanwege de Regel van Cramer geldt er

$$(A')^{-1} = \frac{1}{\det(A')} \left((-1)^{i+j} \det(A'_{ji})\right)_{i,j=1}^{n},$$

waarbij A_{ij} de matrix is die je krijgt als je de $i-$de rij en de $j-$de kolom weglaat in de matrix A. Merk op dat voor alle i en j geldt dat $\det(A'_{ji})$ geheel is, aangezien A gehele coëfficiënten heeft. Bovendien geldt er $\det(A') = \pm 1$. Hieruit volgt $(A')^{-1} \in \mathrm{Mat}(n, \mathbb{Z})$, oftewel k is een isomorfisme. We kunnen nu concluderen dat ϕ^* een isomorfisme is en daarmee φ^* ook. □

Definitie 2.15. Een rooster E is van *type II* als voor alle $x \in E$ geldt dat $\langle x, x\rangle$ even is. Als E niet van type II is, dan is E van *type I*.

Opmerking 2.16. Een rooster E van type II is een geheel rooster. Voor alle $x, y \in E$ geldt er

$$\langle x + y, x + y\rangle = \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle.$$

Aangezien $\langle x + y, x + y\rangle$, $\langle x, x\rangle$ en $\langle y, y\rangle$ even zijn, volgt nu dat $\langle x, y\rangle$ geheel moet zijn.

Opmerking 2.17. Een rooster is van type II dan en slechts dan als de Gram matrix alleen maar gehele coëfficiënten heeft en op de diagonaal allemaal even coëfficiënten staan.

Definitie 2.18. Een rooster E heet *positief definiet* als voor alle $x \in E$ geldt $\langle x, x\rangle \geq 0$ met gelijkheid dan en slechts dan als $x = 0$. Een rooster E heet *negatief definiet* als voor alle $x \in E$ geldt $\langle x, x\rangle \leq 0$ met gelijkheid dan en slechts dan als $x = 0$. Een rooster E heet *indefiniet* als het noch positief noch negatief definiet is.

Lemma 2.19. *Zij E en F roosters, waarvoor $r(E) = r(F) = n$ en $E \subset F$. Laat $B = (b_1, ..., b_n)$ een basis zijn voor F. Laat $A = (a_1, ..., a_n)$ een basis zijn voor E, waarbij $a_i = \sum_{k=1}^{n} \lambda_{ki} b_k$ voor zekere $\lambda_{ki} \in \mathbb{Z}$. Zij $M := (\lambda_{ki})_{i,j=1}^{n}$. Dan geldt $[F : E] = \det(M)$.*

Bewijs. Beschouw de afbeeldingen $\varphi_A : \mathbb{Z}^n \to E$ en $\varphi_B : \mathbb{Z}^n \to F$ gegeven door $(x_1, ..., x_n) \mapsto x_1a_1 + ... + x_na_n$ respectievelijk $(x_1, ..., x_n) \mapsto x_1b_1 + ... + x_nb_n$. Beschouw de injectieve afbeelding $I : E \to F$ die wordt gegeven door $a_i \mapsto a_i$. Beschouw nu de afbeelding $M : \mathbb{Z}^n \to \mathbb{Z}^n$ die wordt gegeven door $x \mapsto Mx$. Laat e_i het $i-$de standaard basiselement zijn van $\mathbb{Z}^n$. Er geldt

$$I(\varphi_A(e_i)) = I(a_i) = a_i = \varphi_B((\lambda_{1i}, ..., \lambda_{ni})) = \varphi_B(M(e_i)).$$

Hieronder staat een diagram ter verduidelijking.

$$\begin{array}{ccc} E & \xhookrightarrow{\ I\ } & F \\ {\scriptstyle\varphi_A}\uparrow\ \cong & & {\scriptstyle\varphi_B}\uparrow\ \cong \\ \mathbb{Z}^n & \xrightarrow{\ M\ } & \mathbb{Z}^n \end{array}$$

Hieruit volgt dat $F/E \cong \mathbb{Z}^n/\mathrm{im}\ M$, oftewel $[F : E] = \#(F/E) = \#(\mathbb{Z}^n/\mathrm{im}\ M)$. Er bestaan twee inverteerbare matrices $P, Q \in \mathrm{Mat}(n, \mathbb{Z})$ zodanig dat $D = PMQ$, waarbij $D = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix}$ voor zekere $d_1, ..., d_n \in \mathbb{Z}$ met $d_i | d_{i+1}$

voor alle $1 \leq i \leq n$. Dit heet de Smith normal form.
Er geldt im $M \cong$ im D, oftewel $\mathbb{Z}^n/\text{im } M \cong \mathbb{Z}^n/\text{im } D$. Merk op

$$\mathbb{Z}^n/\text{im } D \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n.$$

Er geldt $\#(\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n) = \prod_{i=1}^n d_i$. Aangezien $\det(D) = \prod_{i=1}^n d_i$, volgt er $\#(\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n) = \det(D)$. Hieruit volgt $[E : F] = \det(M)$, aangezien $\det(M) = \det(D)$. □

Gevolg 2.20. *Laat E en F twee roosters zijn, waarbij E een deelrooster is van F en $r(E) = r(F)$. Dan geldt*

$$[F : E]^2 \cdot d(F) = d(E).$$

Bewijs. Laat $B = (b_1, ..., b_n)$ een basis zijn voor F. Laat $A = (a_1, ..., a_n)$ een basis zijn voor E, waarbij $a_i = \sum_{k=1}^n \lambda_{ki} b_k$ voor zekere $\lambda_{ki} \in \mathbb{Z}$. Zij

$$M = (\lambda_{ki})_{i,j=1}^n,\ K = (\langle a_i, a_j \rangle)_{i,j=1}^n \text{ en } L = (\langle b_i, b_j \rangle)_{i,j=1}^n.$$

Merk op $K = MLM^\top$. Er geldt

$$\det(K) = \det(M)\det(L)\det(M^\top) = \det(M)^2 \det(L).$$

Vanwege 2.19 volgt er nu $d(E) = [F : E]^2 d(F)$. □

Definitie 2.21. Zij E een rooster. De duale van E is gelijk aan de verzameling

$$\{y \in E \otimes \mathbb{Q} \mid \forall x \in E : \langle x, y \rangle \in \mathbb{Z}\}.$$

Notatie: E^+.

Lemma 2.22. *Er geldt $E \subset E^+$ dan en slechts dan als E geheel is.*

Bewijs. Zij $E \subset E^+$. Dat betekent dat voor alle $x, y \in E$ geldt dat $\langle x, y \rangle \in \mathbb{Z}$, oftewel E is geheel.
Laat E een geheel rooster zijn. Zij $y \in E$. Voor alle $x \in E$ geldt er $\langle x, y \rangle \in \mathbb{Z}$, oftewel $y \in E^+$. Hieruit volgt $E \subset E^+$. □

Definitie 2.23. Laat E en F roosters zijn met bilineaire vorm $\varphi_E : E \times E \to \mathbb{Q}$ respectievelijk $\varphi_F : F \times F \to \mathbb{Q}$. Laat $E \oplus F$ het rooster zijn met bilineaire vorm $\varphi : E \oplus F \times E \oplus F \to \mathbb{Q}$ gegeven door

$$\varphi((x_1, x_2), (x_1', x_2')) = \varphi_E(x_1, x_1') + \varphi_F(x_2, x_2').$$

Zij $s, t \in \mathbb{N}$. We schrijven $sE \oplus tF$, als de directe som van s kopieën van E en t kopieën van F is.

Opmerking 2.24. Voor alle $(x_1, 0), (0, x_2) \in E \oplus F$ geldt $\varphi((x_1, 0), (0, x_2)) = 0$.

Opmerking 2.25. Zij E en F twee roosters. Laat $M = (a_1, ..., a_n)$ een basis zijn voor F en $N = (b_1, ..., b_m)$ een basis zijn voor F. Dan is

$$K = \left((a_i, 0)_{i=1}^n, (0, b_j)_{j=1}^m\right)$$

een basis voor het rooster $E \oplus F$. Hieruit volgt dat de Gram matrix van $E \oplus F$ wordt gegeven door

$$C = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right),$$

waarbij A en B de Gram matrices zijn van E respectievelijk F.

Opmerking 2.26. Zij $E \oplus F$ een rooster. Er geldt $(E \oplus F)^+ = E^+ \oplus F^+$. Dit volgt uit Opmerking 2.24.

Lemma 2.27. *Zij E een rooster met basis $A = (a_1, ..., a_n)$. Dan heeft het duale rooster E^+ een basis $A^+ = (a_1^+, ..., a_n^+)$, zodat voor alle i en j geldt dat $\langle a_i^+, a_j \rangle = \delta_{ij}$.*

Bewijs. Beschouw de vectorruimte $V = E \otimes \mathbb{Q}$. Merk op dat A ook een basis is voor V. De duale $\mathrm{Hom}(V, \mathbb{Q})$ van V heeft een basis $A' = (\rho_1, ..., \rho_n)$, waarvoor geldt $\rho_i(a_j) = \delta_{ij}$. Beschouw het isomorfisme $\mu : V \to \mathrm{Hom}(V, \mathbb{Q})$ gegeven door $x \mapsto \langle x, \_ \rangle_s$. Voor alle i bestaat er een $a_i^+ \in V$ zodanig dat geldt $\mu(a_i) = \rho_i$. Er geldt $\langle a_i^+, a_j \rangle = \rho_i(a_j) = \delta_{ij}$. Laat $A^+ = \{a_1^+, ..., a_n^+\}$. Merk op dat A^+ een basis is voor V.
Laat F het rooster zijn voortgebracht door A^+. We willen laten zien dat geldt $E^+ = F$.
Zij $x \in E$. Er geldt $x = \sum_{i=1}^n \beta_i a_i$ voor zekere $\beta_i \in \mathbb{Z}$. Voor alle j geldt er

$$\langle x, a_j^+ \rangle = \left\langle \sum_{i=1}^n \beta_i a_i, a_j^+ \right\rangle = \sum_{i=1}^n \beta_i \langle a_i, a_j^+ \rangle = \beta_j \in \mathbb{Z},$$

oftewel voor alle j geldt $a_j^+ \in E^+$. Hieruit volgt $F \subset E^+$.
Zij $y \in E^+ \subset V$. Er geldt $y = \sum_{i=1}^n \lambda_i a_i^+$ voor zekere $\lambda_i \in \mathbb{Q}$. Voor alle j geldt

$$\mathbb{Z} \ni \langle y, a_j \rangle = \left\langle \sum_{i=1}^n \lambda_i a_i, a_j \right\rangle = \sum_{i=1}^n \lambda_i \langle a_i, a_j \rangle = \lambda_j.$$

Elk element van E^+ is dus te schrijven als lineaire combinatie van elementen uit A^+ met gehele coëfficiënten. Hieruit volgt $E^+ \in F$.
We kunnen nu concluderen dat A^+ een basis is van E^+. □

Lemma 2.28. *De duale van E^+ van een rooster E is weer een rooster.*

Bewijs. Uit Lemma 2.27 volgt dat E^+ een eindig voortgebrachte vrije abelse groep is.
Beschouw de billinaire vorm $\varphi : E \times E \to \mathbb{Q}$. Zij $V = E \otimes \mathbb{Q}$. Beschouw de geinduceerde afbeelding $\phi : V \times V \to \mathbb{Q}$. Laat $\varphi_+ : E^+ \times E^+ \to \mathbb{Q}$ de afbeelding zijn waarvoor geldt $\phi_{|E^+} = \varphi_+$.
Beschouw de afbeelding $\varphi_+^* : E^+ \to \mathrm{Hom}(E^+, \mathbb{Q})$ gegeven door $\varphi_+(x, \_)$. Laat $x \in E^+$ zodanig dat $\varphi_+^*(x) = 0$.

Laat $A = v_1, .., v_n$ een basis zijn voor E. Dit is ook een basis voor $V = E \otimes \mathbb{Q}$. Er geldt $x = \lambda_1 a_1 + ... + \lambda_n a_n$ voor zekere $\lambda_i \in \mathbb{Q}$. Er geldt

$$\varphi_+^*(x) = \varphi_+(x, \_) = \sum_i \lambda_i \varphi_+(a_i, \_) = 0.$$

Beschouw de afbeelding $\varphi^* : E \to \mathrm{Hom}(E, \mathbb{Q})$ gegeven door $y \mapsto \varphi(y, \_)$. Merk op $\varphi^*(x) = \varphi_+^*(x)_{|E} = 0$. Schrijf $\lambda_i = \frac{\alpha_i}{\beta_i}$ met $\alpha_i \in \mathbb{Z}$ en $\beta_i \in \mathbb{Z} \setminus \{0\}$. Er geldt

$$\varphi^*(x) = \sum_i \lambda_i \varphi(a_i, \_) = \sum_i \frac{\alpha_i}{\beta_i} \varphi(a_i, \_) = \sum_i \alpha_i \prod_{j \neq i} \beta_j \varphi(a_i, \_) = 0.$$

Aangezien φ^* een isomorfisme is geldt er $\varphi^*(y) = 0$ dan en slechts dan als $y = 0$. Oftewel $\varphi(a_i, \_) = 0$ dan en slechts dan als $a_i = 0$. Voor alle $a_i \in A$ geldt $a_i \neq 0$, dus $\varphi(a_i, 0) \neq 0$. Aangezien voor alle j geldt $b_j \neq 0$ volgt er $\alpha_i = 0$ voor alle i. Hieruit volgt $\lambda_i = 0$ voor alle i, oftewel $x = 0$. We kunnen nu concluderen dat φ_+^* injectief is. □

Lemma 2.29. *Zij E een rooster en E^+ het duale rooster van E. Dan geldt*

$$\#\left(E^+/E\right) = |d(E)|.$$

Bewijs. Laat $A = (a_1, ..., a_n)$ een basis zijn voor E. Vanwege Lemma 2.27 bestaat er een basis $A^+ = (a_1^+, ..., a_n^+)$ voor E^+ zodanig dat geldt $\langle a_i, a_j \rangle = \delta_{ij}$. We kunnen elk element uit A schrijven als $a_i = \sum_{k=1}^n \lambda_{ki} a_k^+$ voor zekere $\lambda_{ki} \in \mathbb{Q}$, aangezien geldt $E \subset E^+$. Er geldt

$$\langle a_i, a_j \rangle = \left\langle \sum_{k=1}^n \lambda_{ki} a_k^+, a_j \right\rangle = \sum_{k=1}^n \lambda_{ki} \langle a_k^+, a_j \rangle = \lambda_{ji}.$$

Zij $B = (\langle a_i, a_j \rangle)_{ij} = (\lambda_{ji})_{ij}$. Merk op $B = M$, waarbij M is zoals gedefinieerd in Lemma 2.19. Vanwege Lemma 2.19 geldt er

$$[E^+ : E] = |\det(M)| = |\det(B)| = |d(E)|$$

□

Gevolg 2.30. *Zij E een geheel rooster. Dan geldt $E^+ = E$ dan en slechts dan als $E \in S$.*

Bewijs. Zij $E^+ = E$. Dan geldt $\#\left(E^+/E\right) = 1$. Vanwege Lemma 2.29 geldt nu $d(E) = \pm 1$, oftewel $E \in S$.
Zij $E \in S$. Dan geldt $|d(E)| = 1$. Vanwege Lemma 2.29 geldt nu $\#\left(E^+/E\right) = 1$, oftewel $E^+ = E$.

□

Zij $E \in S$ en $\bar{E} := E/2E$. Merk op dat $\bar{E}$ zelf geen rooster is, tenzij $E = 0$, want voor $e \in \bar{E}$ geldt $2e = 0$ in $\bar{E}$, dus $\bar{E}$ is geen vrije abelse groep. We kunnen $\bar{E}$ beschouwen als een vectorruimte over $\mathbb{F}_2$. Beschouw de afbeelding $\varphi_2 : \bar{E} \times \bar{E} \to \mathbb{Z}/2\mathbb{Z}$ die gegeven wordt door $(\bar{x}, \bar{y}) \mapsto \langle x, y \rangle \mod 2$, waarbij $x, y \in E$ zodanig zijn dat $x \equiv \bar{x} \mod 2E$ en $y \equiv \bar{y} \mod 2E$.
Er geldt $d(E) = \pm 1$. Bovendien geldt er $d(\bar{E}) \equiv d(E) \mod 2 \equiv 1 \mod 2$,

ongeacht welke basis je kiest voor $\bar{E}$. Oftewel $d(\bar{E}) \neq 0$. Vanwege Lemma 2.13 volgt nu dat de afbeelding $\varphi_2^* : \bar{E} \to \mathrm{Hom}(\bar{E}, \mathbb{Z}/2\mathbb{Z})$ gegeven door $\bar{x} \mapsto \langle \bar{x}, \_ \rangle$ een isomorfisme is.
Beschouw de afbeelding $f : \bar{E} \to \mathbb{Z}/2\mathbb{Z}$ die gegeven wordt door $\bar{x} \mapsto \langle \bar{x}, \bar{x} \rangle$. Voor alle $\bar{x}, \bar{y} \in \bar{E}$ geldt er

$$f(\bar{x} + \bar{y}) = \langle \bar{x}, \bar{x} \rangle + 2\langle \bar{x}, \bar{y} \rangle + \langle \bar{y}, \bar{y} \rangle = \langle \bar{x}, \bar{x} \rangle + \langle \bar{y}, \bar{y} \rangle = f(\bar{x}) + f(\bar{y}).$$

De afbeelding f is dus additief en hieruit volgt dat f een groepshomomorfisme is, oftewel $f \in \mathrm{Hom}(\bar{E}, \mathbb{Z}/2\mathbb{Z})$. Aangezien φ_2^* een isomorfisme is, bestaat er een unieke $\bar{u} \in \bar{E}$ zodanig dat $\varphi_2^*(\bar{u}) = f$. Voor alle $\bar{x} \in \bar{E}$ geldt nu

$$\langle \bar{x}, \bar{x} \rangle = f(\bar{x}) = \varphi_2^*(\bar{u})(\bar{x}) = \langle \bar{u}, \bar{x} \rangle.$$

Er bestaat een $u \in E$ zodanig dat $u \equiv \bar{u} \mod 2E$. Merk op dat deze uniek is modulo $2E$. Zij $u' = u + 2z$ met $z \in E$. Er geldt

$$\begin{aligned} \langle u', u' \rangle &= \langle u, u \rangle + 2\langle u, 2z \rangle + \langle 2z, 2z \rangle \\ &= \langle u, u \rangle + 4\langle u, z \rangle + 4\langle z, z \rangle \\ &= \langle u, u \rangle + 4\left(\langle u, z \rangle + \langle z, z \rangle\right). \end{aligned}$$

Merk op dat geldt

$$\begin{aligned} \langle u, z \rangle + \langle z, z \rangle &\equiv \langle \bar{u}, \bar{z} \rangle + \langle \bar{z}, \bar{z} \rangle \mod 2 \\ &\equiv 2\langle \bar{z}, \bar{z} \rangle \mod 2 \\ &\equiv 0 \mod 2. \end{aligned}$$

Hieruit volgt dat $\langle u, z \rangle + \langle z, z \rangle$ even is. Daarmee geldt $\langle u', u' \rangle \equiv \langle u, u \rangle \mod 8$.

Definitie 2.31. Laat E een rooster zijn en $u \in E$ zoals hierboven beschreven. Dan definiëren we $\sigma(E) := \langle u, u \rangle \mod 8$.

Boven Definitie 2.31 wordt laten zien dat σ welgedefinieerd is.

Opmerking 2.32. Stel $E \in S$ is van type II. Dan geldt $\sigma(E) = 0$, want voor alle $x \in E$ geldt $\langle \bar{x}, \bar{x} \rangle = 0$, oftewel $\bar{u} = 0$. We kunnen dus $u = 0$ kiezen, oftewel $\langle u, u \rangle \equiv 0 \mod 8$.

Lemma 2.33. *Zij $E, E_1, E_2 \in S$ zodanig dat $E = E_1 \oplus E_2$. Er geldt*

$$\begin{aligned} r(E) &= r(E_1) + r(E_2) \\ \tau(E) &= \tau(E_1) + \tau(E_2) \\ \sigma(E) &= \sigma(E_1) + \sigma(E_2) \\ d(E) &= d(E_1)d(E_2). \end{aligned}$$

Bewijs. Laat $M = (a_1, ..., a_n)$ een basis zijn voor E_1 en $N = (b_1, ..., b_m)$ een basis zijn voor E_2. Laat A, B en C de Gram matrices zijn van E_1 respectievelijk E_2 respectievelijk E.

Vanwege Opmerking 2.25 geldt dat $r(E) = r(E_1) + r(E_2)$.

Merk op $C = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I_m \end{array}\right)\left(\begin{array}{c|c} I_n & 0 \\ \hline 0 & B \end{array}\right)$. Er geldt ook

$$\det\left(\begin{array}{c|c} A & 0 \\ \hline 0 & I_m \end{array}\right) = \det(A) \text{ en } \det\left(\begin{array}{c|c} I_n & 0 \\ \hline 0 & B \end{array}\right) = \det(B).$$

Hieruit volgt $\det(C) = \det(A)\det(B)$, oftewel $d(E) = d(E_1)d(E_2)$.

Vanwege Definitie 2.5 is de matrix A respectievelijk B congruent met de matrix $A' = \left(\begin{array}{c|c} I_s & 0 \\ \hline 0 & -I_t \end{array}\right)$ respectievelijk $B' = \left(\begin{array}{c|c} I_{s'} & 0 \\ \hline 0 & -I_{t'} \end{array}\right)$ voor zekere $s, t, s', t' \in \mathbb{Z}$ zodanig dat $s + t = n$ en $s' + t' = n$. Hieruit volgt dat de matrix C congruent is met de matrix

$$C' = \left(\begin{array}{c|c|c} \begin{array}{c|c} I_s & 0 \\ \hline 0 & -I_t \end{array} & 0 & \\ \hline 0 & \begin{array}{c|c} I_{s'} & 0 \\ \hline 0 & -I_{t'} \end{array} & \end{array}\right),$$

oftewel $\tau(E) = \tau(E_1) + \tau(E_2)$.

We moeten nu alleen nog laten zien dat geldt $\sigma(E) = \sigma(E_1) + \sigma(E_2)$. Zij $u \in E$ zodanig dat $\sigma(E) \equiv \langle u, u\rangle \mod 8$. We kunnen u ook schrijven als (u_1, u_2) met $u_1 \in E_1$ en $u_2 \in E_2$. Merk op dat u_1 en u_2 zodanig zijn dat geldt $\sigma(E_1) \equiv \langle u_1, u_1\rangle \mod 8$ en $\sigma(E_2) \equiv \langle u_2, u_2\rangle \mod 8$, aangezien de bilineaire vormen op E_1 en E_2 onafhankelijk van elkaar zijn. Er geldt

$$\begin{aligned} \sigma(E) &\equiv \langle u, u\rangle \mod 8 \\ &\equiv \langle (u_1, u_2), (u_1, u_2)\rangle \mod 8 \\ &\equiv \langle u_1, u_1\rangle + \langle u_2, u_2\rangle \mod 8 \\ &= \sigma(E_1) + \sigma(E_2) \end{aligned}$$

□

Opmerking 2.34. Zij E, E_1, E_2 roosters met $E = E_1 \oplus E_2$. Er geldt E is van type II dan en slechts dan als E_1 en E_2 van type II zijn.

Voorbeeld 2.35. Het rooster U is een element van S_2 met Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Merk op dat U van type II is. Er geldt

$$r(U) = 2,\ \tau(U) = 0,\ d(U) = -1,\ \sigma(U) = 0.$$

Voorbeeld 2.36. De roosters I_+ en I_- zijn elementen van S_1 met Gram matrices $\begin{pmatrix} 1 \end{pmatrix}$ respectievelijk $\begin{pmatrix} -1 \end{pmatrix}$. Merk op dat I_+ en I_- van type I zijn.
We gaan nu $\sigma(I_+)$ en $\sigma(I_-)$ bepalen. Beschouw $\bar{I_+} = I_+/2I_+$. We willen een $\bar{u} \in \bar{I_+}$ vinden zodanig dat voor alle $\bar{x} \in \bar{I_+}$ geldt $\langle \bar{u}, \bar{x}\rangle = \langle \bar{x}, \bar{x}\rangle$. Aangezien $\bar{I_+}$ alleen de elementen 0 en 1 bevat, vinden we $\bar{u} = 1$. Neem nu $u = 1$, dan geldt $\sigma(I_+) \equiv \langle 1, 1\rangle \mod 8 = 1$. Voor I_- vinden we op dezelfde wijze ook $u = 1$,

alleen nu geldt $\sigma(I_-) \equiv \langle 1,1\rangle \mod 8 \equiv -1 \mod 8$.
Zij $s,t \in \mathbb{Z}_{\geq 0}$. Beschouw het rooster $sI_+ \oplus tI_-$. De invarianten van dit rooster zijn

$$r = s+t,\ \tau = s-t,\ d = (-1)^t,\ \sigma \equiv s-t \mod 8.$$

Voorbeeld 2.37. Zij $k \in \mathbb{Z}_{\geq 0}$ en $n = 4k$. Laat $V = \mathbb{Q}^n$ een vectorruimte zijn met een bilineaire vorm die $(x_1,...x_n),(y_1,...,y_n) \in V$ stuurt naar $\sum_{i=1}^n x_i y_i$. Laat $E_1 = \mathbb{Z}^n$ de ondergroep van V zijn met de geïnduceerde bilineaire vorm. Merk op dat geldt $E_1 \in S_n$ en $E_1 \cong nI_+$.
Laat E_0 het deelrooster zijn van E_1 gegeven door $E_0 := \{x \in E_1 : \langle x,x\rangle \equiv 0 \mod 2\}$. Merk op dat $\sum_{i=1}^n x_i^2 = \langle x,x\rangle \equiv 0 \mod 2$ hetzelfde is als zeggen dat $\sum_{i=1}^n x_i \equiv 0 \mod 2$, aangezien $x_1^2 + ...x_n^2 \equiv x_1 + ...x_n \mod 2$.
Beschouw het homomorfisme $f : E_1 \to \mathbb{Z}/2\mathbb{Z}$ dat gevegeven wordt door $(x_1,...,x_n) \mapsto \sum_{i=1}^n x_i \mod 2$. Merk op $\ker(f) = E_0$. Hieruit volgt

$$[E_1 : E_0] = [E_1 : \ker(f)] = |\mathrm{im}(f)| = |\mathbb{Z}/2\mathbb{Z}| = 2.$$

Laat E het deelmoduul van V zijn, voortgebracht door E_0 en $b = (\frac{1}{2},...,\frac{1}{2})$, oftewel elke element van E kunnen we schrijven als $a + sb$ voor zekere $s \in \mathbb{Z}$ en $a = (a_1,...,a_n) \in E_0$. Er geldt $\langle 2b, 2b\rangle = n$ en aangezien $n \equiv 0 \mod 4$, geldt nu $2b \in E_0$. Er geldt $b \notin E_0$, want $E_0 \subset E_1 \subset \mathbb{Z}^n$ en $b \notin \mathbb{Z}^n$. Hieruit volgt $[E : E_0] = 2$.
Zij

$$V^\bullet := \{(x_1,...,x_n) \in V : 2x_i \in \mathbb{Z},\ x_i - x_j \in \mathbb{Z},\ \sum_{i=1}^n x_i \in 2\mathbb{Z}\}.$$

Zij $x = (x_1,...,x_n) \in V$. We willen laten zien dat geldt $V^\bullet = E$. Stel $x \in E$. Er geldt $2x_i = 2a_i + 2s\frac{1}{2} = 2a_i + s$. Aangezien $a_i, s \in \mathbb{Z}$ geldt er $2x_i \in \mathbb{Z}$. Er geldt $x_i - x_j = a_i + s\frac{1}{2} - a_j - s\frac{1}{2} = a_i - a_j \in \mathbb{Z}$. Er geldt

$$\sum_{i=1}^n x_i = \sum_{i=1}^n (a_i + sb_i) = \sum_{i=1}^n a_i + s\sum_{i=1}^n \frac{1}{2} = \sum_{i=1}^n a_i + s\frac{1}{2}n = \sum_{i=1}^n a_i + 2sk.$$

Aangezien $\sum_{i=1}^n a_i \equiv 0 \mod 2$, geldt er $\sum_{i=1}^n x_i \in 2\mathbb{Z}$. Hieruit volgt $x \in V^\bullet$, oftewel $E \subseteq V^\bullet$.
Zij $x = (x_1,...,x_n) \in V^\bullet$. Aangezien voor alle i en j geldt $2x_i \in \mathbb{Z}$ en $x_i - x_j \in \mathbb{Z}$, volgt dat voor alle i geldt $x_i \in \mathbb{Z}$ óf $x_i \in \mathbb{Z} + \frac{1}{2}$.
Laat $x_i \in \mathbb{Z}$ voor alle i. Dan volgt uit $\sum_{i=1}^n x_i \equiv 0 \mod 2$ dat geldt $x \in E_0 \subset E$.
Laat $x_i \in \mathbb{Z} + \frac{1}{2}$ voor alle i. We kunnen x schrijven als $x = c + b$, waarbij $c = (c_1,...,c_n) \in E_1$. Er geldt

$$\sum_{i=1}^n x_i = \sum_{i=1}^n (c_i + \frac{1}{2}) = \sum_{i=1}^n c_i + \sum_{i=1}^n \frac{1}{2} = \sum_{i=1}^n c_i + 2k.$$

Er geldt $\sum_{i=1}^n c_i \in 2\mathbb{Z}$, aangezien geldt $\sum_{i=1}^n c_i + 2k \in 2\mathbb{Z}$. Hieruit volgt dat $c_i \in E_0$, oftewel x is van de vorm $a + sb$ met $a \in E_0$ en $s = 1$. Hieruit volgt $x \in E_0$. Er geldt $x \in E$, oftewel $V^\bullet \subseteq E$.
Er geldt dus $x \in E$ dan en slechts dan als

$$2x_i \in \mathbb{Z}, \quad x_i - x_j \in \mathbb{Z} \text{ en } \sum_{i=1}^n x_i \in 2\mathbb{Z}. \tag{1}$$

Er geldt $\langle x,b\rangle = \frac{1}{2}\sum_{i=1}^{n} x_i \in \mathbb{Z}$ en $\langle b,b\rangle = \frac{1}{4}n = k$. Hieruit volgt dat voor alle $x,y \in E$ geldt $\sum_{i=1}^{n} x_i y_i \in \mathbb{Z}$, oftewel E is een geheel rooster. Bovendien heeft E_0 dezelfde index in E_1 als in E en vanwege Lemma 2.20 volgt nu dat $d(E) = d(E_1) = 1$. Aangezien $d(E) = 1$, geldt nu $E \in S_n = S_{4k}$.
Schrijf $\Gamma_n := E$. Zij k even, oftewel $n \equiv 0 \mod 8$. Dan geldt $\langle b,b\rangle \equiv 0 \mod 2$. Aangezien voor alle $x \in E_0$ geldt $\langle x,x\rangle \equiv 0 \mod 2$, volgt nu dat Γ_n van type II is.
Zij $k = 2m$. Er geldt $r(\Gamma_{8m}) = 8m$. Bovendien geldt $\tau(\Gamma_{8m}) = 8m$, want de bilineaire vorm $\sum_{i=1}^{n} x_i y_i$ is positief definiet. Aangezien Γ_{8m} van type II is, volgt er $\sigma(\Gamma_8) = 0$.
Beschouw het rooster Γ_8. Beschouw de elementen

$$v_1 = \frac{1}{2}(e_1+e_8)-\frac{1}{2}(e_2+...+e_7),\ \ v_2 = e_1+e_2 \text{ en } v_{i+1} = e_i - e_{i-1} \text{ voor } 2 \le i \le 7,$$

waarbij $e_1,...,e_8$ de standaard basis is voor $\mathbb{Q}^8$. Er geldt

$$(\langle v_i,v_j\rangle)_{i,j=1}^{8} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Merk allereerst op dat de elementen voldoen aan (1), oftewel voor alle i geldt $v_i \in \Gamma_8$. Er geldt $\lambda_1 v_1 + ... + \lambda_8 v_8 = 0$ met $\lambda_i \in \mathbb{Q}$ dan en slechts dan als voor alle i geldt $\lambda_i = 0$. Hieruit volgt dat de elementen $v_1,...,v_8$ lineair onafhankelijk zijn. We moeten nu alleen nog aantonen dat $(v_1,...,v_8)$ Γ_8 opspant. Stel $(v_1,...,v_8)$ spant Γ_8 niet op. Aangezien $v_1,...,v_8$ lineair onafhankelijk zijn, spannen ze wel een ander rooster F op van rang acht, waarvoor geldt $F \subset \Gamma_8$. Dan geldt vanwege Gevolg 2.20 dat

$$[\Gamma_8 : F]d(\Gamma_8) = d(F).$$

Er geldt $d(E) = \det((\langle v_i,v_j\rangle)_{i,j=1}^{8}) = 1$. We hadden al aangetoond dat geldt $d(\Gamma_8) = 1$. Hieruit volgt dat $[\Gamma_8 : F] = 1$, oftewel $\Gamma_8 = F$. We kunnen nu concluderen dat $(v_1,...,v_8)$ een basis vormt voor Γ_8.
De bijbehorende matrix van Γ_8 wordt gegeven door $(\langle v_i,v_j\rangle)_{i,j=1}^{8}$.

2.2 Gehele unimodulaire roosters

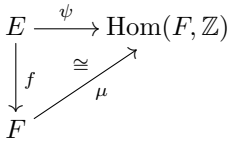
Lemma 2.38. *Zij $E \in S$ en F een deelmoduul van E. Zij*

$$F' = \{x \in E \mid \forall y \in F : \langle x,y\rangle = 0\}.$$

Dan geldt $F \in S$ dan en slechts dan als $E = F \oplus F'$.

Bewijs. Merk op dat F een eindig voortgebrachte vrije abelse groep is met bilinaire vorm $\Phi : F \times F \to \mathbb{Q}$ zodanig dat $\Phi = \varphi_{|F}$.

Zij $E = F \oplus F'$. Er geldt $\pm 1 = d(E) = d(F)d(F')$, oftewel $d(F) = \pm 1$. Vanwege stelling 2.12 volgt nu dat Φ^* injectief is, oftewel F is een rooster. Vanwege stelling 2.14 volgt nu $F \in S$.
Zij $F \in S$. Uit stelling 2.14 volgt nu dat het homomorfisme $\mu : F \to \mathrm{Hom}(F, \mathbb{Z})$ gegeven door $x \mapsto \langle x, \_ \rangle$ een isomorfisme is. Laat $\psi : E \to \mathrm{Hom}(F, \mathbb{Z})$ gegeven zijn door $x \mapsto \langle x, \_ \rangle$. Er geldt $\psi_{|F} = \mu$. Merk op dat geldt $F' = \ker(\psi)$ en $F \cap F' = \ker(\mu)$. Aangezien μ een isomorfisme is geldt $F \cap F' = 0$. Beschouw de afbeelding $f : E \to F$ die gegeven wordt door $f(x) = \mu^{-1}(\psi(x))$.



Zij $x \in E$. Laat $x_0 \in F$ zodanig dat $f(x) = x_0$. Er geldt

$$f(x) = \mu^{-1}(\psi(x)) = x_0,$$

oftewel $\psi(x) = \mu(x_0) = \psi_F(x_0)$. We krijgen $\psi(x) = \psi(x_0)$, aangezien geldt $x_0 \in F$. Oftewel $\psi(x - x_0) = 0$. Hieruit volgt $x - x_0 \in F'$ oftewel er bestaat een $x_1 \in F'$, namelijk $x_1 = x - x_0$ zodanig dat $x = x_0 + x_1$ met $x_0 \in F$ en $x_1 \in F'$. Hieruit volgt $E = F \oplus F'$. □

Definitie 2.39. Zij E een rooster en F een deelrooster van E. Het *orthogonale rooster van* F wordt gegeven door $F^\perp = \{x \in E |\ \forall y \in F : \langle x, y \rangle = 0\}$.

Definitie 2.40. Zij E een groep. Een element $x \in E$ heet *ondeelbaar* als er voor geen enkele $n \in \mathbb{N}_{\geq 2}$ een $y \in E$ bestaat zodanig dat $x = ny$. Als E niet ondeelbaar is, dan noemen we E *deelbaar*.

Lemma 2.41. *Zij E een unimodulair rooster. Als $x \in E$ ondeelbaar is, dan bestaat er een $y \in E$ zodanig dat $\langle x, y \rangle = 1$.*

Bewijs. Zij $x \in E$ ondeelbaar. Beschouw de lineaire afbeelding $f_x : E \to \mathbb{Z}$ gegeven door $y \mapsto \langle x, y \rangle$. Stel dat f_x deelbaar in de groep $\mathrm{Hom}(E, \mathbb{Z})$. Dan bestaat er een $g \in \mathrm{Hom}(E, \mathbb{Z})$ zodanig dat $ng = f_x$ voor zekere $n \in \mathbb{N}$. Aangezien $E \to \mathrm{Hom}(E, \mathbb{Z})$ gegeven door $x \mapsto f_x$ een isomorfisme is, bestaat er een $x' \in E$ zodanig dat $f_x = ng = nf_{x'}$, oftewel voor alle $y \in E$ geldt $\langle x, y \rangle = \langle nx', y \rangle$. Aangezien $E \to \mathrm{Hom}(E, \mathbb{Z})$ gegeven door $x \mapsto f_x$ een isomorfisme is, geldt dan $x = nx'$. Dit geeft een tegenspraak, oftewel f_x is ondeelbaar. Aangezien E en $\mathbb{Z}$ groepen zijn en f_x een groepshomomorfisme is, geldt dat $f_x[E]$ een ondergroep is van $\mathbb{Z}$. Alle ondergroepen van $\mathbb{Z}$ worden gegeven door $a\mathbb{Z}$ voor zekere $a \in \mathbb{N}_{\geq 0}$. Stel $f_x[E] = a\mathbb{Z}$ voor $a \neq 1$, dan zou f_x deelbaar zijn door a. Tegenspraak. Hieruit volgt $f_x[E] = \mathbb{Z}$, oftewel f_x is surjectief. Er bestaat dus een $y \in E$ zodanig dat $\langle x, y \rangle = 1$. □

Stelling 2.42. *Zij $E \in S$ indefiniet. Dan bestaat er een $x \in E$ met $x \neq 0$ zodanig dat $\langle x, x \rangle = 0$.*

Het bewijs voor Stelling 2.42 valt buiten de inhoud van deze scriptie. Het bewijs is terug te vinden in [1] bovenaan bladzijde 56.

Lemma 2.43. *Zij $E \in S_n$ indefiniet en van type I. Dan bestaat er een $F \in S_{n-2}$ zodanig dat $E \cong I_+ \oplus I_- \oplus F$.*

Bewijs. Vanwege Stelling 2.42 bestaat er een $x \in E$ met $x \neq 0$ zodanig dat $\langle x, x\rangle = 0$. Aangezien we x mogen delen door een geheel getal, kunnen we aannemen dat x ondeelbaar is. Vanwege Lemma 2.41 bestaat er een $y \in E$ zodanig dat $\langle x, y\rangle = 1$.
Stel $\langle y, y\rangle$ is even. Aangezien E van type I is, bestaat er een $t \in E$ zodanig dat $\langle t, t\rangle$ oneven is. Zij $y' = t + ky$ met $k = 1 - \langle x, t\rangle$. Merk op $\langle x, y'\rangle = 1$. Er geldt

$$\langle y', y'\rangle = \langle t, t\rangle + 2\langle t, ky\rangle + k^2\langle y, y\rangle \equiv \langle t, t\rangle \mod 2.$$

Hieruit volgt dat $\langle y', y'\rangle$ oneven is. We kunnen dus altijd een $y \in E$ vinden met $\langle x, y\rangle = 1$, waarbij $\langle y, y\rangle$ oneven is. Neem aan $\langle y, y\rangle = 2m + 1$. Zij $v_1 = y - mx$ en $v_2 = y - (m + 1)x$. Merk op $\langle v_1, v_1\rangle = 1$, $\langle v_1, v_2\rangle = 0$ en $\langle v_2, v_2\rangle = -1$. Laat G het deelrooster zijn van E voortgebracht door $\{v_1, v_2\}$. Er geldt $G \cong I_+ \oplus I_-$, oftewel $G \in S$. Lemma 2.38 geeft ons nu dat $E \cong I_+ \oplus I_- \oplus F$ voor zekere $F \in S_{n-2}$, namelijk $F = G^\perp$. □

Stelling 2.44. *Zij $E \in S$ indefiniet en van type I. Dan geldt $E \cong sI_+ \oplus tI_-$ voor zekere $s, t \in \mathbb{N}_{>0}$.*

Bewijs. Merk allereerst op dat $E \cong I_+ \oplus I_- \oplus F$ vanwege Lemma 2.43 voor zekere $F \in S_{n-2}$. We gaan gebruik maken van volledige inductie. Stel $n = 2$. Er geldt $F \in S_0$, oftewel $F = 0$. Hieruit volgt $E \cong I_+ \oplus I_-$.
Zij $N \in \mathbb{N}_{>2}$. Neem aan dat voor alle $n < N$ en voor alle $E \in S_n$ geldt $E \cong sI_+ \oplus tI_-$ voor zekere $s, t \in \mathbb{N}_{>0}$.
Zij $n = N$. Er geldt $F \neq 0$. Merk op $I_+ \oplus F$ en $I_- \oplus F$ zijn allebei van type I. Bovendien is of $I_+ \oplus F$ indefiniet of $I_- \oplus F$. Zonder verlies van algemeenheid nemen we aan dat $I_+ \oplus F$ indefiniet is. Aangezien er geldt $I_+ \oplus F \in S_{n-1}$ volgt nu vanwege de inductieveronderstelling $I_+ \oplus F \cong aI_+ \oplus bI_-$ voor zekere $a, b \in \mathbb{N}_{>0}$. Hieruit volgt

$$E \cong I_+ \oplus I_- \oplus F \cong I_- \oplus aI_+ \oplus bI_- \cong aI_+ \oplus (b + 1)I_-.$$

□

Voorbeeld 2.45. Beschouw het rooster $U \oplus I_+$. Merk allereerst op dat $U \oplus I_+$ een indefiniet rooster is van type I. Vanwege Lemma 2.43 weten we dat geldt $U \oplus I_+ \cong I_+ \oplus I_- \oplus F$ voor zekere $F \in S$. De matrix die hoort bij het rooster $U \oplus I_+$ wordt gegeven door $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. De bilinaire vorm wordt dus gegeven door

$$\varphi((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_2 + x_2y_1 + x_3y_3.$$

Om die F te vinden gaan we het bewijs van Lemma 2.43 volgen. Zij $x = (1, 0, 0)$ en $y = (0, 1, 0)$. Merk op dat geldt $\langle x, x\rangle = 0$, $\langle x, y\rangle = 1$ en $\langle y, y\rangle = 0$. We willen een y' vinden zodanig dat $\langle y', y'\rangle$ oneven is en $\langle x, y'\rangle = 1$. Er bestaat een t zodanig dat $\langle t, t\rangle$ oneven is, namelijk $(0, 0, 1)$. Laat $y' = t + ky$ met k zodanig dat geldt $k = 1 - \langle x, t\rangle$, oftewel

$$y' = (0, 0, 1) + 1(0, 1, 0) = (0, 1, 1).$$

Merk op dat geldt $\langle x, y' \rangle = 1$ en $\langle y', y' \rangle = 1$. Neem nu $v_1 = y' = (0, 1, 1)$ en $v_2 = y' - x = (-1, 1, 1)$. Merk op

$$\langle v_1, v_1 \rangle = 1,\ \langle v_2, v_2 \rangle = -1 \text{ en } \langle v_1, v_2 \rangle = 0.$$

Het rooster G voortgebracht door $\{v_1, v_2\}$ is isomorf met het rooster $I_+ \oplus I_-$. Laat $G^\perp$ het orthogonale rooster zijn van G. Het rooster $G^\perp$ wordt voortgebracht door $\{(1, 0, -1)\}$. Merk op $\langle (1, 0, -1), (1, 0, -1) \rangle = 1$, oftewel $G^\perp \cong I_+$. Vanwege Lemma 2.38 volgt nu $U \oplus I_+ \cong I_+ \oplus I_- \oplus G^\perp$, oftewel $U \oplus I_+ \cong 2I_+ \oplus I_-$. Merk op dat hieruit niet volgt dat $U \cong I_+ \oplus I_-$, aangezien U van type II is en $I_+ \oplus I_-$ van type I. De roosters U en $I_+ \oplus I_-$ worden gegeven door de matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ respectievelijk $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Deze matrices zijn blijkbaar niet congruent over $\mathbb{Z}$.

Lemma 2.46. *Zij $E \in S$ indefiniet en van type II. Dan bestaat er een $F \in S_{n-2}$ zodanig dat $E \cong U \oplus F$.*

Bewijs. Op dezelfde wijze als bij het bewijs van Lemma 2.43 vinden we een $x \in E$ met $x \neq 0$ en x ondeelbaar zodanig dat $\langle x, x \rangle = 0$. Zij $y \in E$ zodanig dat $\langle x, y \rangle = 1$. Stel $\langle y, y \rangle = 2m$. Vervang y door $y' = y - mx$. Merk op dat $\langle y', y' \rangle = 0$ en $\langle x, y' \rangle = 1$. Laat G het deelrooster zijn van E voortgebracht door $\{x, y'\}$. Er geldt $G \cong U$. Lemma 2.38 geeft ons nu $E \cong U \oplus F$ voor zekere $F \in S_{n-2}$, namelijk $G^\perp$. □

Lemma 2.47. *Zij $F_1, F_2 \in S$. Stel F_1 en F_2 zijn van type II en er geldt $I_+ \oplus I_- \oplus F_1 \cong I_+ \oplus I_- \oplus F_2$. Dan geldt $U \oplus F_1 \cong U \oplus F_2$.*

Bewijs. Schrijf $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$ en $V_i = E_i \otimes \mathbb{Q}$ voor $i \in \{1, 2\}$. Laat E_i^0 de ondergroep zijn van E_i gegeven door $E_i^0 := \{x \in E_i : \langle x, x \rangle \equiv 0 \mod 2\}$. Beschouw het homomorfisme $f : E_i \to \mathbb{Z}/2\mathbb{Z}$ dat gegeven wordt door $x \mapsto \langle x, x \rangle \mod 2$. Merk op $\ker(f) = E_i^0$. Hieruit volgt

$$[E_i : E_i^0] = [E_i : \ker(f)] = |\mathrm{im}(f)| = |\mathbb{Z}/2\mathbb{Z}| = 2.$$

Voor $x \in E_i^0$ geldt $x = (x_1, x_2)$ met $x_1 \in W$ en $x_2 \in F_i$ zodanig dat geldt $\langle x_1, x_1 \rangle + \langle x_2, x_2 \rangle$ is even. Aangezien F_i van type II is geldt voor alle $a \in F_i$ dat $\langle a, a \rangle$ even is. We willen dus $x_1 \in W$ zodanig dat $\langle x_1, x_1 \rangle$ even is. Zij

$$W^0 := \{x \in W : \langle x, x \rangle \equiv 0 \mod 2\}.$$

Er geldt $E_i^0 = W^0 \oplus F_i$. Merk op W^0 wordt voortgebracht door $(1, 1)$ en $(1, -1)$. Zij $\left(E_i^0\right)^+$ de duale van E_i^0. Vanwege Opmerking 2.26 en Opmerking 2.30 geldt nu $(E_i^0)^+ = (W^0)^+ \oplus F_i$.
Claim: Er geldt $(W^0)^+ = \{(x_1, x_2) \in W \otimes \mathbb{Q} : 2x_1, 2x_2, x_1 - x_2 \in \mathbb{Z}\} =: T$.
Bewijs: "$(W^0)^+ \subseteq T$"
Zij $(x_1, x_2) \in (W^0)^+$. Voor alle $(y_1, y_2) \in W^0$ geldt nu

$$\langle (x_1, x_2), (y_1, y_2) \rangle = x_1 y_2 - x_2 y_2 \in \mathbb{Z}$$

is geheel. Neem $(y_1, y_2) = (2, 0)$. Dan volgt $2x_1 \in \mathbb{Z}$. Neem $(y_1, y_2) = (0, 2)$. Dan volgt $2x_2 \in \mathbb{Z}$. Neem $(y_1, y_2) = (1, 1)$. Dan volgt $x_1 - x_2 \in \mathbb{Z}$. Hieruit

volgt $(x_1, x_2) \in T$.
"$(W^0)^+ \supseteq T$"
Zij $(x_1, x_2) \in T$. We willen dat voor alle $(y_1, y_2) \in W^0$ geldt dat

$$\langle (x_1, x_2), (y_1, y_2) \rangle = x_1 y_2 - x_2 y_2$$

geheel is. Beschouw $(1, 1) \in W^0$. Er geldt $\langle (x_1, x_2), (1, 1) \rangle = x_1 - x_2 \in \mathbb{Z}$. Beschouw $(1, -1) \in W^0$. Er geldt $\langle (x_1, x_2), (1, -1) \rangle = x_1 + x_2 = x_1 - x_2 + 2x_2 \in \mathbb{Z}$. Er geldt $(x_1, x_2) \in (W^0)^+$, aangezien W^0 wordt voortgebracht door $(1, 1)$ en $(1, -1)$.

Er geldt

$$\left(E_i^0\right)^+ / E_i^0 \cong \left((W^0)^+ \oplus F_i\right) / \left(W^0 \oplus F_i\right) \cong (W^0)^+ / W^0.$$

Merk op

$$\left(W^0\right)^+ / W^0 := \left\{(0,0), \left(\tfrac{1}{2}, \tfrac{1}{2}\right), \left(\tfrac{1}{2}, -\tfrac{1}{2}\right), (1,0)\right\}.$$

De groep $(W^0)^+ / W^0$ bestaat uit een eenheidselement en drie elementen van orde twee. Hiermee is $(W^0)^+ / W^0$ de viergroep van Klein. Hieruit volgt dat $\left(E_i^0\right)^+ / E_i^0$ ook de viergroep van Klein is.
Het quotiënt $\left(E_i^0\right)^+ / E_i^0$ heeft drie ondergroepen van orde twee. Vanwege Stelling 8.1 uit het Algebra 1 dictaat [4] volgt dat er drie groepen van index twee tussen $(E_i^0)^+$ en E_i^0 zitten. Één daarvan is E_i en de andere twee noemen we E_i' en E_i''. Er bestaan $W', W'' \subset (W^0)^+$ zodanig dat $E_i' = W' \oplus F_i$ en $E_i'' = W'' \oplus F_i$. Neem als basis voor W' de vectoren $a = (\frac{1}{2}, \frac{1}{2})$ en $b = (1, -1)$. Merk op $\langle a, a \rangle = \langle b, b \rangle = 0$ en $\langle a, b \rangle = 1$. Neem als basis voor W'' de vectoren $a = (\frac{1}{2}, -\frac{1}{2})$ en $b = (1, 1)$. Merk op $\langle a, a \rangle = \langle b, b \rangle = 0$ en $\langle a, b \rangle = 1$. Hieruit volgt $W' \cong U \cong W''$.
Gegeven is dat $E_1 \cong E_2$, oftewel er bestaat een isomorfisme $f : W \oplus F_1 \to W \oplus F_2$. Het isomorfisme f stuurt E_1^0 naar E_2^0 en daarmee is $(E_1^0)^+$ ook isomorf met $(E_2^0)^+$. Hieruit volgt dat het paar E_1', E_1'' wordt gestuurd naar het paar (E_2', E_2''), oftewel $E_1' \cong E_2'$ óf $E_1' \cong E_2''$ Aangezien W' en W'' allebei isomorf zijn met U, volgt er $U \oplus F_1 \cong U \oplus F_2$. □

3 De groep K(S)

Definitie 3.1. Zij $E, E' \in S$. De roosters E en E' heten *stabiel isomorf* als er een $F \in S$ bestaat zodanig dat geldt $E \oplus F \cong E' \oplus F$.
Notatie: $E \sim E'$

Opmerking 3.2. De relatie $\sim$ is een equivalentierelatie. De reflexieve en symmetrische eigenschap volgen direct. De transitieve eigenschap is iets minder duidelijk. Zij $E, E', E'' \in S$ met $E \sim E'$ en $E' \sim E''$. Laat $F, G \in S$ zodanig zijn dat geldt $E \oplus F \cong E' \oplus F$ en $E' \oplus G \cong E'' \oplus G$. Er geldt

$$E \oplus F \oplus G \cong E' \oplus F \oplus G \cong E' \oplus G \oplus F \cong E'' \oplus G \oplus F \cong E'' \oplus F \oplus G.$$

Hieruit volgt $E \sim E''$, door $F \oplus G$ te nemen als in Definitie 3.1.

Zij $E \in S$. We schrijven $(E) := \{E' \in S : E \sim E'\}$ voor de equivalentieklasse van E. Laat $K_+(S) := S/\sim$ het quotiënt zijn van S met de relatie $\sim$. Definieer $+$ op het quotient zodanig dat geldt $(E \oplus E') = (E) + (E')$.
We moeten aantonen dat deze operatie welgedefinieerd is. Zij $E, F \in (E)$ en $E', F' \in (E')$. Er bestaan een $G, G' \in S$ zodanig dat $E \oplus G \cong F \oplus G$ en $E' \oplus G' \cong F' \oplus G'$. Er geldt $G \oplus E \oplus E' \oplus G' \cong G \oplus F \oplus F' \oplus G'$. Hieruit volgt $E \oplus E' \sim F \oplus F'$, oftewel $(E \oplus E') = (F \oplus F')$.
Merk op dat de operatie $+$ op $K_+(S)$ commutatief en associatief is, vanwege de commutativiteit en associativiteit van $\oplus$. Bovendien heeft $+$ als neutraal element op $K_+(S)$ de klasse 0 van het rooster $0 \in S$.

Lemma 3.3. *Zij $x, y, z \in K_+(S)$ zodanig dat geldt $x + z = y + z$. Dan geldt $x = y$.*

Bewijs. Laat $E \in x$, $E' \in y$ en $F \in z$. Er bestaat een $G \in S$ zodanig dat $E \oplus F \oplus G \cong E' \oplus F \oplus G$. Merk op $F \oplus G \in S$. Hieruit volgt $E \sim E'$, oftewel $x = y$. □

Zij $(x, y), (x', y') \in K_+(S) \times K_+(S)$. Definieer $\triangle$ door: $(x, y) \triangle (x', y')$ dan en slechts dan als $x + y' = y' + x$. Merk op dat dit een equivalentierelatie is. We hebben Lemma 3.3 nodig om de transitiviteit te bewijzen van $\triangle$. We schrijven $[(x, y)]$ voor de equivalentieklasse van (x, y). Laat $K(S) := K_+(S) \times K_+(S)/\triangle$ het quotiënt zijn van $K_+(S) \times K_+(S)$ met de relatie $\triangle$. Definieer op $K(S)$ de optelling $+$ zodanig dat geldt

$$[(x, y)] + [(x', y')] = [(x + x', y + y')].$$

We moeten nog nagaan dat deze operatie welgedefinieerd is. Zij

$$(x, y), (x, y), (a, b), (a', b') \in K_+(S) \times K_+(S)$$

zodanig dat geldt $(x, y) \triangle (a, b)$ en $(x', y') \triangle (a', b')$. We willen dat geldt

$$(x + x', y + y') \triangle (a + a', b + b').$$

Aangezien er geldt $x + b = y + a$ en $x' + b' = y' + b'$, volgt er

$$x + b + x' + b' = y + a + y' + a'.$$

Hieruit volgt $x + x' + b + b' = y + y' + a + a'$, oftewel

$$(x + x', y + y') \triangle (a + a', b + b').$$

Stelling 3.4. *$K(S)$ is een commutatieve groep.*

Bewijs. Het element $(0, 0) \in K(S)$ is het eenheidselement, waarbij $0 \in K_+(S)$ het neutrale element is voor de operatie $+$ in $K_+(S)$. De commutativiteit en associativiteit volgen uit de commutativiteit en associativiteit van de operatie $+$ in $K_+(S)$. Zij $[(x, y)] \in K(S)$. Aangezien $x + y = y + x$ geldt, volgt er

$$[(x, y)] + [(y, x)] = [(x + y, y + x)] = [0, 0] = [(y + x, x + y)] = [(y, x)] + [(x, y)].$$

Zij $(a,b) \in K_+(S)$ zodanig dat geldt

$$[(x,y)] + [(a,b)] = [0,0] = [(a,b)] + [(x,y)].$$

Dan geldt $[(x,y)] + [(a,b)] = [(x,y)] + [(y,x)]$, oftewel

$$x + a + y + x = y + b + x + y.$$

Hieruit volgt $x + a = y + b$, oftewel $(y,x) \triangle (a,b)$. □

Er bestaat een injectief homomorfisme $j : K_+(S) \to K(S)$ dat gegeven wordt door $x \mapsto [(x,0)]$. Elk element in $K(S)$ kan geschreven worden als het verschil van twee elementen uit $K_+(S)$, met andere woorden $(E) - (F)$ met $E, F \in S$. Namelijk, zij $[(x,y)] \in K(S)$. Dan geldt

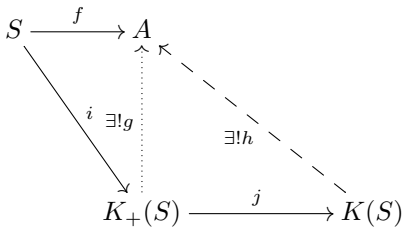
$$\begin{aligned} [(x,y)] &= [(x,0) + (0,y)] \\ &= [(x,0)] + [(0,y)] \\ &= [(x,0)] - [(y,0)] \\ &= x - y. \end{aligned}$$

Er geldt $(E) - (F) = (E') - (F')$ dan en slechts dan als er een $G \in S$ bestaat zodanig dat $E \oplus F' \oplus G \cong E' \oplus F \oplus G$, oftewel $E \oplus F' \sim E' \oplus F$.

Zij A een abelse groep en laat $f : S \to A$ een functie zijn zodanig dat geldt $f(E) = f(E_1) + f(E_2)$, als $E \cong E_1 \oplus E_2$. We noemen f dan *additief*. Er geldt $0 \cong 0 \oplus 0$, oftewel $f(0) = f(0) + f(0)$. Hieruit volgt $f(0) = 0$. Zij $E, E' \in S$ zodanig dat geldt $E \sim E'$. Er bestaat een $G \in S$ zodanig dat $E \oplus G \cong E' \oplus G$. Bovendien geldt er $E \oplus G \cong E' \oplus G \oplus 0$, oftewel $f(E \oplus G) = f(E' \oplus G) + f(0)$. Hieruit volgt $f(E \oplus G) = f(E' \oplus G)$. Er geldt

$$f(E) + f(G) = f(E \oplus G) = f(E' \oplus G) = f(E') + f(G).$$

Hieruit volgt $f(E) = f(E')$. Er bestaat een afbeelding $g : K_+(S) \to A$ zodanig dat $f(E) = g(i(E))$ waarbij $i : S \to K_+(S)$ gegeven wordt door $i(E) = (E)$. De afbeelding g is uniek, omdat g wordt vastgelegd door f en i.
Zij $(x,y), (x',y') \in K_+(S) \times K_+(S)$ zodanig dat geldt $(x,y) \triangle (x,y')$, oftewel $x + y' = y + x'$. Er geldt $g(x) + g(y') = g(x') + g(y)$ en aangezien A een groep is, volgt er $g(x) - g(y) = g(x') - (y')$. Er bestaat dus een unieke afbeelding $h : K(S) \to A$ die gegeven wordt door $x - y \mapsto g(x) - g(y)$ zodanig dat geldt $h \circ j = g$, oftewel $f = h \circ j \circ i$.



Beschouw de afbeelding $k : S \to K(S)$ gegeven door $k = j \circ i$. Voor elke additieve afbeelding $f : S \to A$, waarbij A een abelse groep is, bestaat er een

uniek groepshomomorfisme $h : K(S) \to A$ zodanig dat geldt $f = h \circ k$. Dit is de universele eigenschap van een Grothendieck groep. Hieruit volgt dat $K(S)$ de Grothendieck groep is van S met de operatie $\oplus$.

Opmerking 3.5. Vanwege Lemma 2.33 weten we dat de invarianten r, t, σ, d additief zijn. De invarianten $r,\ \tau\ , d$ en σ definiëren homomorfismen

$$r : K(S) \to \mathbb{Z},\ \tau : K(S) \to \mathbb{Z},\ d : K(S) \to \{\pm 1\} \text{ en } \sigma : K(S) \to \mathbb{Z}/8\mathbb{Z}.$$

Stelling 3.6. *De groep $K(S)$ is een vrije abelse groep met basis $[(I_+), 0]$ en $[(I_-), 0]$.*

Bewijs. Zij $E \in S$ met E niet nul. De roosters $E \oplus I_+$ en $E \oplus I_-$ zijn van type I. Er geldt $E \oplus I_+$ of $E \oplus I_-$ is indefiniet. Neem zonder verlies van algemeenheid aan dat $E \oplus I_-$ indefiniet is. Vanwege Stelling 2.44 geldt nu $E \oplus I_- \cong sI_+ \oplus tI_-$ voor zekere $s, t \in \mathbb{Z}_{\geq 1}$. Het beeld van E in $K(S)$ is dan gelijk aan een lineaire combinatie van $[(I_+), 0]$ en $[(I_-), 0]$. Hieruit volgt dat $K(S)$ wordt voortgebracht door $[(I_+), 0]$ en $[(I_-), 0]$.
Beschouw de afbeelding $(r, \tau) : K(S) \to \mathbb{Z} \times \mathbb{Z}$ gegeven door $x \mapsto (r(x), \tau(x))$. Er geldt $(r(I_+), \tau(I_+)) = (1, 1)$ en $(r(I_-), \tau(I_-)) = (1, -1)$. Merk op dat $(1, 1)$ en $(1, -1)$ lineair onafhankelijk zijn, dus $[(I_+), 0]$ en $[(I_-), 0]$ zijn ook lineair onafhankelijk. Hieruit volgt dat $[(I_+), 0]$ en $[(I_-), 0]$ een basis vormen voor $K(S)$. □

Opmerking 3.7. Alle $x \in K(S)$ kunnen worden geschreven als

$$x = s\,[(I_+), 0] + t\,[(I_-), 0]$$

met $s, t \in \mathbb{Z}$. Er geldt $r(x) = s + t$ en $\tau(x) = s - t$. De gehele getallen s, t worden dus bepaald door de rang en de index.

Opmerking 3.8. De rang van een element uit $K(S)$ kan negatief zijn, bijvoorbeeld $r([0, I_-]) = -1$. Dit in tegenstelling tot de rang van een rooster.

Gevolg 3.9. *Zij B de ondergroep van $\mathbb{Z} \times \mathbb{Z}$ gegeven door*

$$B := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \mod 2\}.$$

De afbeelding $(r, \tau) : K(S) \to B$ gegeven door $x \mapsto (r(x), \tau(x))$ is een isomorfisme.

Bewijs. Zij $x, y \in K(S)$. Schrijf

$$x = s_1\,[(I_+), 0] + t_1\,[(I_-), 0] \text{ en } y = s_2\,[(I_+), 0] + t_2\,[(I_-), 0]$$

voor zekere $s_1, s_2, t_1, t_2 \in \mathbb{Z}$. Zij $(r, \tau)(x) = (r, \tau)(y)$. Dan geldt $r(x) = r(y)$ en $\tau(x) = \tau(y)$, oftewel $s_1 + t_1 = s_2 + t_2$ en $s_1 - t_1 = s_2 - t_2$. Hieruit volgt $s_1 = s_2$ en $t_1 = t_2$, oftewel $x = y$. De afbeelding (r, τ) is dus injectief.
Zij $(a, b) \in B$. Beschouw $x = \frac{a+b}{2}\,[(I_+), 0] + \frac{b-a}{2}\,[(I_-), 0] \in K(S)$. Er geldt

$$(r, \tau)(x) = (r(x), \tau(x)) = \left(\tfrac{a+b}{2} + \tfrac{b-a}{2}, \tfrac{a+b}{2} - \tfrac{b-a}{2}\right) = (a, b).$$

Hieruit volgt dat de afbeelding (r, τ) surjectief is. □

Gevolg 3.10. *Zij $E, E' \in S$. Er geldt $E \sim E'$ dan en slechts dan als E en E' dezelfde rang en index hebben.*

Bewijs. Zij $E \sim E'$. Dan geldt $E, E' \in x$ met $x \in K_+(S)$. Vanwege Gevolg 3.9 volgt nu $(r(E), \tau(E)) = (r(E'), \tau(E'))$.
Zij $r(E) = r(E')$ en $\tau(E) = \tau(E')$. Zij $E \in x$ en $E' \in x$ met $x, x' \in K_+(S)$. Er geldt

$$(r, \tau)([x, 0]) = (r(E), \tau(E)) = (r(E'), \tau(E')) = (r, \tau)([x', 0]).$$

Vanwege Gevolg 3.9, geldt er $[x, 0] = [x', 0]$, oftewel $x = x'$, oftewel $E \sim E'$. □

Stelling 3.11. *Voor alle $E \in S$ geldt er $\sigma(E) \equiv \tau(E) \mod 8$.*

Bewijs. Laat $\tau_8 : K(S) \to \mathbb{Z}/8\mathbb{Z}$ gegeven worden door $x \mapsto \tau(x) \mod 8$. Er geldt $\tau_8(I_+) = 1$ en $\tau_8(I_-) = 7$. We hebben in Voorbeeld 2.36 laten zien dat $\sigma(I_+) = 1$ en $\sigma(I_-) = 7$. We hebben nu twee homomorfismen τ_8 en σ van $K(S) \to \mathbb{Z}/8\mathbb{Z}$ die op de voortbrengers van $K(S)$ hetzelfde zijn. Hieruit volgt $\tau_8 = \sigma$, oftewel $\sigma(E) \equiv \tau(E) \mod 8$. □

Gevolg 3.12. *Zij E van type II, dan geldt $\tau(E) \equiv 0 \mod 8$.*

Bewijs. Als E van type II is, weten we vanwege Opmerking 2.32 dat geldt $\sigma(E) = 0$. Uit Stelling 3.11 volgt nu $\tau(E) \equiv 0 \mod 8$. □

4 Hoofdstelling

Lemma 4.1. *Zij $E_1, E_2 \in S$ indefiniet en van type II. Als E_1 en E_2 dezelfde rang en index hebben, dan geldt $E_1 \cong E_2$.*

Bewijs. Zij $r(E_1) = r(E_2)$ en $\tau(E_1) = \tau(E_2)$. Vanwege Lemma 2.46 geldt $E_1 \cong U \oplus F_1$ en $E_2 \cong U \oplus F_2$ voor zekere $F_1, F_2 \in S$. Merk op dat U van type II is en vanwege Opmerking 2.34 moeten F_1 en F_2 ook van type II zijn. Bovendien gelden

$$r(E_1) = r(U) + r(F_1) \text{ en } r(E_2) = r(U) + r(F_2).$$

Hieruit volgt $r(F_1) = r(F_2)$. Op dezelfde wijze volgt $\tau(F_1) = \tau(F_2)$. Beschouw de roosters $G_1 := I_+ \oplus I_- \oplus F_1$ en $G_2 := I_+ \oplus I_- \oplus F_2$. Aangezien het rooster $I_+ \oplus I_-$ van type I is, geldt er dat G_1 en G_2 ook van type I zijn. Merk op dat G_1 en G_2 ook dezelfde rang en index hebben, omdat F_1 en F_2 dezelfde rang en index hebben. Bovendien zijn G_1 en G_2 indefiniet. Stelling 2.44 geeft ons nu dat

$$G_1 \cong s_1 I_+ \oplus t_1 I_- \text{ en } G_2 \cong s_2 I_+ \oplus t_2 I_-,$$

voor zekere $s_1, t_1, s_2, t_2 \in \mathbb{N}_{>0}$. Aangezien G_1 en G_2 dezelfde rang en index hebben, geldt

$$s_1 + t_1 = s_2 + t_2 \text{ en } s_1 - t_1 = s_2 - t_2.$$

Hieruit volgt dat $s_1 = s_2$ en $t_1 = t_2$, oftewel $G_1 \cong G_2$. Uit Lemma 2.47 volgt nu $U \oplus F_1 \cong U \oplus F_2$, oftewel $E_1 \cong E_2$. □

Stelling 4.2. *Zij $E \in S$ indefiniet, van type II met $\tau(E) \geq 0$. Dan is E isomorf met $pU \oplus q\Gamma_8$, waarbij $p = \frac{1}{2}(r(E) - \tau(E))$ en $q = \frac{1}{8}\tau(E)$.*

Bewijs. Er geldt

$$r(pU \oplus q\Gamma_8) = 2\left(\tfrac{1}{2}\left(r(E) - \tau(E)\right)\right) + 8\left(\tfrac{1}{8}\tau(E)\right) = r(E)$$

en

$$\tau(pU \oplus q\Gamma_8) = 0\left(\tfrac{1}{2}\left(r(E) - \tau(E)\right)\right) + 8\left(\tfrac{1}{8}\tau(E)\right) = \tau(E).$$

Merk op dat U en Γ_8 van type II zijn, dus $pU \oplus q\Gamma_8$ is ook van type II. Bovendien is $pU \oplus q\Gamma_8$ indefiniet. Nu geeft Lemma 4.1 ons dat $E \cong pU \oplus q\Gamma_8$. □

5 Wortelsysteem

Definitie 5.1. Zij E een rooster. De *spiegeling* door $0 \neq \alpha \in E$ wordt gegeven door

$$\sigma_\alpha(\beta) = \beta - \frac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle}\alpha.$$

Opmerking 5.2. Voor alle $y, z \in E$ geldt $\langle\sigma_x(y), \sigma_x(z)\rangle = \langle y, z\rangle$, oftewel een spiegeling is een isometrie.

Definitie 5.3. Een deelverzameling R van E heet een *wortelsysteem in E* als
(1) R is eindig, spant E op en $0 \notin R$
(2) Voor alle $\alpha \in R$ geldt dat voor alle $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ geldt $n\alpha \notin R$.
(3) Voor alle $\alpha \in R$ geldt dat voor alle $\beta \in R$ geldt $\sigma_\alpha(\beta) \in R$.
(4) Voor alle $\alpha, \beta \in R$ geldt $\frac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle} \in \mathbb{Z}$.

Voorbeeld 5.4. Zij $E_8 := \{x \in \Gamma_8 : \langle x, x\rangle = 2\}$. Beschouw de vectoren $\pm e_i \pm e_j$ $(i \neq j)$ en $\frac{1}{2}\sum_{i=1}^8 \epsilon_i e_i$, waarbij $\epsilon_i = \pm 1$, $\prod_{i=1}^8 \epsilon_i = 1$ en $e_1, ..., e_8$ de standaard basis is van $\mathbb{Q}^8$. De eis $\prod_{i=1}^8 \epsilon_i = 1$ zegt dat het aantal negatieve ϵ_i even moet zijn. We noemen een element $x \in \mathbb{Q}^8$ van type $((\pm 1)^2, 0^6)$, als de vector twee coëfficiënten ± 1 heeft en de andere zes coëfficiënten 0 zijn. We noemen een element $x \in \mathbb{Q}^8$ van type $((\pm\frac{1}{2})^8)_2$, als de vector acht coëfficiënten $\pm\frac{1}{2}$ heeft met een even aantal coëfficiënten $-\frac{1}{2}$. Zij

$$H := \left\{x \in \mathbb{Q}^8 : \ x \text{ is van type } ((\pm 1)^2, 0^6) \text{ óf van type } ((\pm\tfrac{1}{2})^8)_2\right\}.$$

We gaan laten zien dat $H = E_8$.
Allereerst moeten we laten zien dat voor iedere $x \in H$ geldt $x \in \Gamma_8$. Zij $x \in H$. Stel x is van de type $((\pm 1)^2, (0)^6)$. Het is duidelijk dat voor iedere x_i geldt $2x_i \in \mathbb{Z}$. Er geldt $x_i - x_j \in \{-2, -1, 0, 1, 2\} \subset \mathbb{Z}$ en $\sum_{i=1}^8 x_i \in \{-2, 0, 2\} \subset 2\mathbb{Z}$. Stel x is van type $((\pm\frac{1}{2})^8)_2$. Het is duidelijk dat voor iedere x_i geldt $2x_i \in \mathbb{Z}$. Er geldt $x_i - x_j \in \{-1, 0, 1\} \subset \mathbb{Z}$ en $\sum_{i=1}^8 x_i \in \{-4, -2, 0, 2, 4\} \subset 2\mathbb{Z}$. Hieruit volgt $x \in \Gamma_8$.
Om aan te tonen dat $H \subseteq E_8$ moeten we laten zien dat voor alle $x \in H$ geldt $\langle x, x\rangle = 2$. Zij x van type $((\pm 1)^2, (0)^6)$. Dan geldt $\langle x, x\rangle = (\pm 1)^2 + (\pm 1)^2 = 2$. Zij x van type $((\pm\frac{1}{2})^8)_2$. Dan geldt $\langle x, x\rangle = 8(\pm\frac{1}{2})^2 = 8 \cdot \frac{1}{4} = 2$. Hieruit volgt $H \subseteq E_8$.
Het laatste wat we nog aan moeten tonen is dat $E_8 \subseteq H$. Zij $x \in E_8$. Laat $I = \{1, ..., 8\}$ zijn. Aangezien $x \in E_8 \subset \Gamma_8$, moet voor alle $i, j \in I$ gelden dat

$$2x_i \in \mathbb{Z}, \quad x_i - x_j \in \mathbb{Z} \text{ en } \sum_{i=1}^8 x_i \in 2\mathbb{Z}.$$

Vanwege de eerste eis $2x_i \in \mathbb{Z}$ geldt er voor alle $i \in I$ dat $x_i \in \mathbb{Z}$ of $x_i \in \mathbb{Z} + \frac{1}{2}$. Bovendien geldt er $\langle x, x \rangle = 2$, oftewel $\sum_{i=1}^{8} x_i^2 = 2$. Hieruit volgt $|x_i| \leq \sqrt{2}$, oftewel $x_i \in \{0, \pm\frac{1}{2}, \pm 1\}$. Aangezien voor alle $i, j \in I$ geldt $x_i - x_j \in \mathbb{Z}$, geldt er voor alle $i \in I$ dat $x_i \in \{0, \pm\frac{1}{2}\}$ óf $x_i \in \{0, \pm 1\}$. Stel $x_i = \pm 1$. Dan geldt $x_j = \pm 1$ voor een zekere $j \in I \setminus \{i\}$ en $x_l = 0$ voor alle $l \in I \setminus \{i, j\}$, omdat $\sum_{i=1}^{8} x_i^2 = 2$. Hieruit volgt $x \in H$. Stel $x_i = \pm\frac{1}{2}$. Dan geldt voor alle $j \in I$ dat $x_j = \pm\frac{1}{2}$, want $\sum_{i=1}^{n} x_i^2 = 2$. Stel voor $2n + 1$ aantal $i \in I$ geldt $x_i = -\frac{1}{2}$. Dan geldt

$$\sum_{i=1}^{n} x_i = (8 - (2n+1))\,\frac{1}{2} + (2n+1)\left(-\frac{1}{2}\right) = 3 - 2n \notin 2\mathbb{Z}.$$

Voor de volledigheid laat ik nog zien dat er wel elementen van type $((\pm\frac{1}{2})^8)_2$ bestaan. Stel voor $2n$ aantal $i \in I$ geldt $x_i = -\frac{1}{2}$. Dan geldt

$$\sum_{i=1}^{n} x_i = (8 - 2n)\,\frac{1}{2} + 2n\left(-\frac{1}{2}\right) = 4 - 2n \in 2\mathbb{Z}.$$

Hieruit volgt $x \in H$. We kunnen nu concluderen dat $H = E_8$.

Opmerking 5.5. De deelverzameling E_8 van Γ_8 heeft 240 elementen. Er bestaan $4\binom{8}{2} = 112$ elementen van type $((\pm 1)^2, (0)^6)$ en

$$\binom{8}{0} + \binom{8}{2} + \binom{8}{4} + \binom{8}{6} + \binom{8}{8} = 128$$

elementen van type $((\pm\frac{1}{2})^8)_2$.

Stelling 5.6. *De verzameling E_8 is een wortelsysteem in Γ_8.*

Bewijs. **(1)** Opmerking 5.5 geeft ons dat E_8 eindig is. Beschouw de basis $(v_1, ..., v_8)$ voor Γ_8, zoals beschreven is in Voorbeeld 2.37. Merk op $v_i \in E_8$ voor alle i. Hieruit volgt dat Γ_8 wordt opgespannen door E_8. Bovendien geldt er $0 \notin E_8$.
(2.) Het is duidelijk dat zowel voor x van type $((\pm 1)^2, (0)^6)$ als voor x van type $((\pm\frac{1}{2})^8)_2$ geldt dat voor alle $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ geldt dat $n\alpha \notin R$.
(3.) Zij $x \in R$. Voor alle $y \in R$ geldt dan

$$\langle \sigma_x(y), \sigma_x(y) \rangle = \langle y, y \rangle = 2.$$

Hieruit volgt $\sigma_x(y) \in R$.
(4.) Zij $x, y \in E_8$. Er geldt $\frac{2\langle x,y \rangle}{\langle x,x \rangle} = \langle x, y \rangle$. Aangezien Γ_8 een geheel rooster is, geldt voor alle $x, y \in \Gamma_8$ dat $\langle x, y \rangle \in \mathbb{Z}$. Hieruit volgt dat $\langle x, y \rangle \in \mathbb{Z}$. □

Referenties

[1] Serre, Jean-Pierre, *A course in Arithmetic*, 1973, Springer-Verlag New York.

[2] Stoll, Michael, van Luijk, Ronald *Linear Algebra I*, 2015.
Beschikbaar via
`http://pub.math.leidenuniv.nl/~luijkrmvan/linalg/2015/LinearAlgebra1_2015.pdf`

[3] Stoll, Michael, *Linear Algebra II*, 2007.
Beschikbaar via
`http://websites.math.leidenuniv.nl/algebra/linalg2.pdf`

[4] Stevenhagen, Peter *Algebra I*, 2016.
Beschikbaar via
`http://websites.math.leidenuniv.nl/algebra/algebra1.pdf`

[5] Humphreys, James, *Introduction to Lie algebras and Representation Theory*, 1972, Springer.