Wurzelgitter

Paula Cremerius, Julia Lust
Betreuer:
Simon Eisenbarth

14.04.2015

Seminar Gitter und Codes
Leitung: Prof. Dr. Gabriele Nebe

Inhaltsverzeichnis

1 Fundamentale Wurzelsysteme 4

2 Klassifizierung von irreduziblen Wurzelgittern 8

3 Konstruktion von Wurzelgittern aus binären linearen Codes 16

4 Betrachtungen zur Coxeter-Zahl 23

Einleitung

In der vorliegenden Ausarbeitung betrachten wir ausschließlich Wurzelgitter, also Gitter, die von Vektoren der Quadratnorm 2 erzeugt werden. In Kapitel 1.3 [1] haben wir schon ein Beispiel für ein solches gesehen: Es gilt, dass Γ_C für einen binären, linearen Code C ein Gitter im $\mathbb{R}^n$ ist. Für den im Kapitel 1.2 [1] betrachteten erweiterten Hamming-Code $\widetilde{H}$ ergibt sich sogar ein Wurzelgitter.
Zuerst werden wir feststellen, dass für jedes Wurzelgitter die Existenz einer Basis mit den speziellen Eigenschaften, dass die Quadratnorm aller Basisvektoren zwei ist und das Skalarprodukt von verschiedenen Basisvektoren miteinander entweder null oder minus eins ist. Die Identifikation eines Wurzelgitters mit seiner speziellen Basis ermöglicht eine übersichtliche graphische Darstellung der Gitter durch sogenannte Coxeter-Dynkin Diagramme.
Weiterhin stellen wir fest, dass jedes Wurzelgitter eine feinste Zerlegung in zueinander orthogonale, irreduzible Wurzelgitter besitzt. Diese irreduziblen Wurzelgitter werden wir klassifizieren und zu den verschiedenen Typen einen konstruktiven Existenzbeweis angeben.
Wir kommen anschließend wieder auf den Zusammenhang zwischen Codes und Gittern zurück und betrachten für welche Gitter - abgesehen von $\Gamma_{\widetilde{H}}$ - der Zusammenhang $\Gamma_C = \Gamma$ gilt.
Abschließend betrachten wir den Zusammenhang der Coxeter-Zahl, der Anzahl der Wurzeln eines Gitters $\Gamma \subset \mathbb{R}^n$ geteilt durch n, mit Skalarprodukten der Wurzeln von Γ.

1 Fundamentale Wurzelsysteme

Um die Existenz der in der Einleitung erwähnten speziellen Basis eines Wurzelgitters zu beweisen, führen wir in diesem Kapitel den Begriff des fundamentalen Wurzelsystems ein. Die Existenz dieser Basen benötigen wir im 2. Kapitel um Wurzelgitter über graphische Darstellungen klassifizieren zu können.

Definition *Ein Gitter im $\mathbb{R}^n$ ist eine Teilmenge $\Gamma \subset \mathbb{R}^n$ mit $\Gamma = \langle e_1, \ldots, e_n \rangle_{\mathbb{Z}}$ wobei $\{e_1, \ldots, e_n\}$ eine Basis von $\mathbb{R}^n$ ist.*

Definition 1.1 *Sei $\Gamma \subset \mathbb{R}^n$ ein gerades Gitter. Sei*

$$R := \{x \in \Gamma \mid (x,x) = 2\}.$$

*Ein Element $x \in R$ heißt **Wurzel**.*

Definition 1.2 *Ein gerades Gitter $\Gamma \subset \mathbb{R}^n$ heißt **Wurzelgitter**, wenn Γ von R erzeugt wird.*

Bemerkung 1.3 Sei Γ ein Wurzelgitter, R wie oben definiert und seien $x, y \in R$. Mit der Cauchy-Schwarz-Ungleichung

$$(x,y)^2 \leq (x,x) \cdot (y,y) = 4$$

folgt

$$(x,y) \in \{0, +1, -1, +2, -2\}.$$

In den folgenden Beweisen verwenden wir auch:

1. $(x,y) = \pm 2$ ist äquivalent zu $x = \pm y$.
   Im Fall $(x,y) = 2$ folgt dies aus $(x-y, x-y) = (x,x) - 2(x,y) + (y,y) = 0$ und somit $x = y$.
   Für $(x,y) = -2$ gilt $(x+y, x+y) = (x,x) + 2(x,y) + (y,y) = 0$ und somit $x = -y$.

2. $(x,y)=1$ ist äquivalent zu $x-y\in R$.
   Dies gilt wegen $(x-y,x-y)=(x,x)-2(x,y)+(y,y)=2$ für $(x,y)=1$.

Satz 1.4 *Sei $\Gamma\subset\mathbb{R}^n$ ein Wurzelgitter. Dann existiert eine Basis $\{x_1,\dots,x_n\}$ von Γ mit*

$$
\begin{aligned}
&(x_i,x_i)=2,\ \ 1\le i\le n\\
&(x_i,x_j)\in\{0,-1\},\ \ 1\le i,j\le n, i\neq j.
\end{aligned}
$$

Wir beweisen die Behauptung schrittweise.

Definition 1.5 *$S\subseteq R$ heißt **fundamentales Wurzelsystem**, falls gilt:*

1. *S ist eine Basis von Γ.*

2. *Jedes $\beta\in R$ kann als Linearkombination $\sum_{\alpha\in S}k_\alpha\alpha$ geschrieben werden, wobei die Koeffizienten k_α ganze Zahlen sind, die entweder alle nicht-negativ oder nicht-positiv sind.*

Sei S ein fundamentales Wurzelsystem. Wir zeigen, dass S dann die Bedingungen von Satz 1.4 erfüllt: Seien $\alpha,\beta\in S$ mit $\alpha\neq\beta$. Dann gilt $(\alpha,\beta)\le 0$, denn nach Bemerkung 1.3(1) liefert $(\alpha,\beta)=\pm 2$ einen Widerspruch zur Minimalitätseigenschaft der Basis S. $(\alpha,\beta)=1$ widerspricht 2. Also ist $(\alpha,\beta)\in\{0,-1\}$. Die erste Bedingung ist trivialerweise erfüllt, da $S\subset R$.
Um Satz 1.4 zu beweisen, genügt es also zu zeigen, dass jedes Wurzelsystem ein fundamentales Wurzelsystem enthält.
Sei $t\in\mathbb{R}^n$ mit $(t,\alpha)\neq 0$ für alle $\alpha\in R$. Solch ein Element existiert: R ist endlich, da R die Schnittmenge des Gitters, in welchem alle Punkte einen durch die Basis fest definierten kleinsten Abstand zueinander haben, mit einer kompakten Menge ($\{x\in\mathbb{R}^n\mid ||x||_2=\sqrt{2}\}$) ist. Die Menge

$$H_\alpha:=\{x\in\mathbb{R}^n\ \mid (x,\alpha)=0\}$$

mit $\alpha\in R$ ist eine Hyperebene in $\mathbb{R}^n$. Die Vereinigung endlich vieler Hyperebenen in $\mathbb{R}^n$ ergibt jedoch nie den vollen Raum $\mathbb{R}^n$, was die Existenz von t zeigt. Sei

$$R_t^+:=\{\alpha\in R\mid (t,\alpha)>0\}.$$

Dann gilt $R=R_t^+\cup(-R_t^+)$.

Definition 1.6 *Ein Element $\alpha \in R_t^+$ heißt **zerlegbar**, falls $\beta, \gamma \in R_t^+$ existieren mit $\alpha = \beta + \gamma$, sonst heißt α **unzerlegbar**. Sei S_t die Menge der unzerlegbaren Elemente von R_t^+.*

Proposition 1.7 *Die Menge S_t ist ein fundamentales Wurzelsystem von Γ. Außerdem gilt, falls S ein fundamentales Wurzelsystem ist, so existiert ein $t \in \mathbb{R}^n$ mit $(t, \alpha) > 0$ für alle $\alpha \in S$ und $S = S_t$.*

Mit Proposition 1.7 ist dann Satz 1.4 vollständig bewiesen, dazu beweisen wir nun 1.7 schrittweise.

Lemma 1.8 *Jedes Element aus R_t^+ ist eine Linearkombination von Elementen aus S_t mit Koeffizienten aus $\mathbb{Z}_{\geq 0}$.*

Beweis Angenommen, es existiert ein $\alpha \in R_t^+$ für das keine solche Linearkombination existiert. Da $(t, \beta) > 0$ ist für alle $\beta \in R_t^+$, kann α ohne Einschränkung so gewählt werden, dass (t, α) minimal ist. Dann ist α zerlegbar, sonst wäre $\alpha \in S_t$. Also existieren $\beta, \gamma \in R_t^+$ mit $\alpha = \beta + \gamma$, und es gilt

$$(t, \alpha) = (t, \beta) + (t, \gamma).$$

Aus $(t, \beta) > 0$ und $(t, \gamma) > 0$ folgt $(t, \beta) < (t, \alpha)$ und $(t, \gamma) < (t, \alpha)$. Da (t, α) minimal ist, können die Elemente β und γ als Linearkombination von Elementen aus S_t geschrieben werden, wobei die Koeffizienten nicht-negative ganze Zahlen sind. Also gilt dasselbe auch für α, ein Widerspruch zur Annahme. $\square$

Lemma 1.9 *Es gilt $(\alpha, \beta) \leq 0$ für alle $\alpha, \beta \in S_t \subset R_t^+$ mit $\alpha \neq \beta$.*

Beweis Nach Bemerkung 1.3 gilt für alle $x, y \in R \supset S_t : (x, y) \in \{0, +1, -1, +2, -2\}$. Der Fall $(x, y) = 2$ kann ausgeschlossen werden, da $\alpha \neq \beta$ vorausgesetzt ist (vgl. 1.3(1)). Im Fall $(\alpha, \beta) = 1$ folgt $\gamma := \alpha - \beta \in R$ (vgl. 1.3(2)) und somit entweder $\gamma \in R_t^+$, dann wäre α zerlegbar mit $\alpha = \beta + \gamma$, oder $-\gamma \in R_t^+$, also ist β zerlegbar mit $\beta = \alpha + (-\gamma)$. $\square$

Lemma 1.10 *Die Elemente aus S_t sind linear unabhängig.*

Beweis Angenommen $\sum_{\alpha \in S_t} a_\alpha = 0$ mit $a_\alpha \in \mathbb{R}$. Das ist äquivalent zu $\sum_{\beta \in S_{t1}} b_\beta \beta = \sum_{\gamma \in S_{t2}} c_\gamma \gamma$ mit $b_\beta, c_\gamma \in \mathbb{R}_{>0}$, wobei $S_{t1} \dot\cup S_{t2} = S_t$.
Sei $\lambda := \sum b_\beta \beta$, dann gilt

$$0 \leq (\lambda, \lambda) = \sum\nolimits_{\beta, \gamma} b_\beta c_\gamma (\beta, \gamma) \leq 0$$

nach Lemma 1.8. Hieraus folgt $\lambda = 0$ und damit $0 = (t, \lambda) = \sum b_\beta(t, \beta)$. Da $(t, \beta) > 0$ für alle β gilt, muss $b_\beta = 0$ für alle β gelten. Analog zeigt man $c_\gamma = 0$ für alle γ. Also sind die Elemente aus S_t linear unabhängig. □

Lemma 1.11 *Sei $\{\gamma_1, \dots, \gamma_n\}$ eine Basis von $\mathbb{R}^n$. Dann existiert ein $t \in \mathbb{R}^n$ mit $(t, \gamma_i) > 0$ für alle $1 \leq i \leq n$.*

Beweis Für $i = 1, \dots, n$ sei δ_i' das Bild von γ_i unter der orthogonale Projektion auf den Unterraum $U_i = \langle \gamma_1, \dots, \gamma_{i-1}, \gamma_{i+1}, \dots, \gamma_n \rangle$ und sei $\delta_i := \gamma_i - \delta_i'$. Dieser Vektor ist orthogonal zu U_i. Daraus folgt

$$(\delta_i, \gamma_j) = 0 \text{ für alle } 1 \leq j \leq n, i \neq j,$$

da $\gamma_j \in U_i$ ist. Da auch $\delta_i' \in U_i$ ist, gilt auch

$$(\delta_i, \gamma_i) = (\delta_i, \delta_i + \delta_i') = (\delta_i, \delta_i) > 0.$$

Somit hat $t := \sum_{i=1}^n r_i \delta_i$ mit $r_i > 0$ die gewünschte Eigenschaft. □

Beweis von **Proposition 1.7**
Dass S_t eine Basis von Γ ist, folgt nach Lemma 1.8 und Lemma 1.10, die zweite Bedingung für ein fundamentales Wurzelsystem folgt ebenfalls mit Lemma 1.8.
Sei umgekehrt S ein fundamentales Wurzelsystem von R, und sei $t \in \mathbb{R}^n$ mit $(t, \alpha) > 0$ für alle $\alpha \in S$. Ein solches Element existiert nach Lemma 1.11.
Sei R^+ die Menge aller Wurzeln, welche Linearkombinationen mit nicht-negativen ganzzahligen Koeffizienten von Elementen aus S sind. Dann gilt $R^+ \subset R_t^+$ und $(-R^+) \subset (-R_t^+)$. Hieraus folgt $R^+ = R_t^+$, da $R = R^+ \cup (-R^+)$ gilt.
Wir zeigen nun noch, dass die Elemente $\alpha_1, \dots, \alpha_n$ aus der Basis S unzerlegbar in R_t^+ sind. Angenommen $\alpha \in S$ ist zerlegbar mit $\alpha = \beta + \gamma$, wobei $\beta, \gamma \in R_t^+ = R^+$. Dann gilt

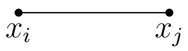
$$\alpha = \beta + \gamma = \sum_{i=1}^n b_i \alpha_i + \sum_{i=1}^n c_i \alpha_i$$

damit ergibt sich eine nichttriviale Linearkombination der Null, also wäre S keine Basis.
Da nun $S \subset S_t$ gilt, folgt mit $|S| = |S_t| \leq \infty$ dass $S = S_t$ ist. Somit ist der Beweis von Proposition 1.7 und damit auch der Beweis von Satz 1.4 vollständig. □

2 Klassifizierung von irreduziblen Wurzelgittern

Man kann die Basen $\{x_1, \ldots, x_n\}$, welche die Bedingungen von Satz 1.4 erfüllen, klassifizieren. Jeder solchen Basis kann man einen Graphen, das Coxeter-Dynkin-Diagramm, zuordnen, indem die Beziehung zwischen den Basiselementen folgendermaßen verdeutlicht wird $(i \neq j)$:

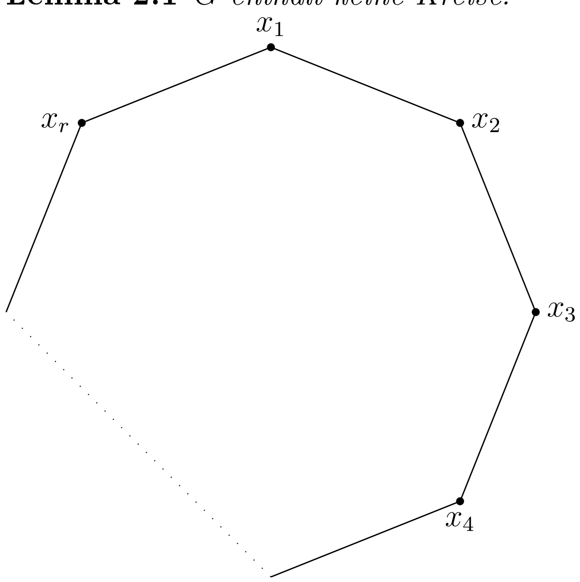
$(x_i, x_j) = -1 \ \Leftrightarrow$



$(x_i, x_j) = \ \ 0 \ \Leftrightarrow$

In diesem Kapitel ist G immer das Coxeter-Dynkin-Diagramm einer Basis $\{x_1, \ldots, x_n\}$, welche die Bedingungen von Satz 1.4 erfüllt.

Lemma 2.1 *G enthält keine Kreise.*



$(r \geq 3)$

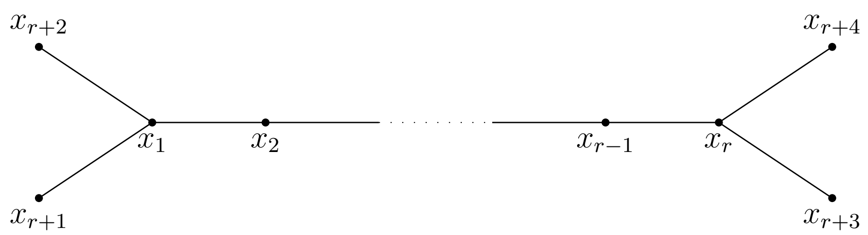
Fig. 1 Ein minimaler Kreis

Beweis Angenommen G enthält einen minimalen Kreis wie in Figur 1, in welchem $x_1, \ldots, x_r$ die zugehörigen Basisvektoren bezeichne.
Hieraus folgt

$$\begin{aligned}((x_1 + \cdots + x_r), (x_1 + \cdots + x_r)) &= \sum_{i=1}^{r} (x_i, x_i) + \sum_{i=1}^{r} \sum_{j=1, j\neq i}^{r} (x_i, x_j) \\ &= 2r + 2\sum_{i=1}^{r-1} (x_i, x_{i+1}) + 2(x_r, x_1) \\ &= 2r - 2r = 0,\end{aligned}$$

dann wäre $x_1 + \cdots + x_r = 0$ eine nichttriviale Linearkombination der Null. □

Lemma 2.2 *G enthält keinen Teilgraph, welcher die Form von Figur 2 hat.*



$(r \geq 1)$

Fig. 2 Ein Graph, der nicht als Dynkin-Diagramm eines Wurzelgitters vorkommt

Beweis Für die Basisvektoren, welche den Teilgraphen bilden, würde gelten:

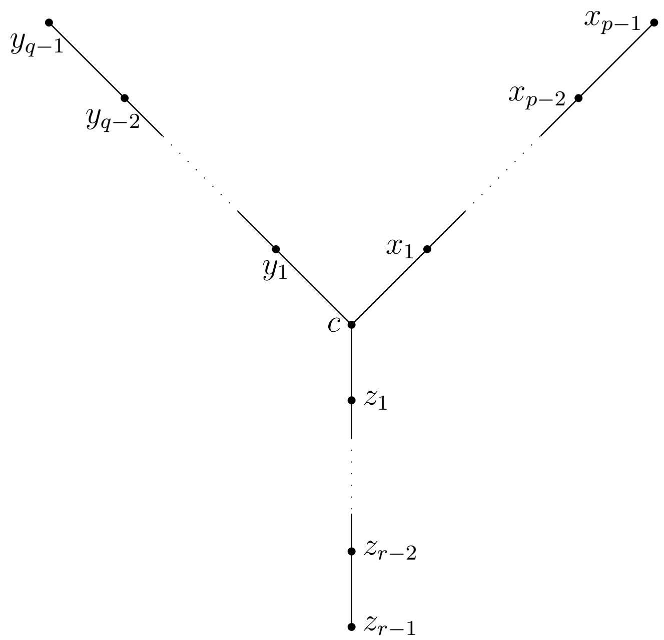
$$\begin{aligned}&(2x_1 + \cdots + 2x_r + x_{r+1} + \cdots + x_{r+4}, 2x_1 + \cdots + 2x_r + x_{r+1} + \cdots + x_{r+4}) \\ =&\sum_{i=1}^{r} 4(x_i, x_i) + \sum_{i=r+1}^{r+4} (x_i, x_i) + 8\sum_{i=1}^{r-1} (x_i, x_{i+1}) \\ &+ 4((x_1, x_{r+1}) + (x_1, x_{r+2}) + (x_r, x_{r+3}) + (x_r, x_{r+4})) \\ =&8r + 8 - 8(r-1) - 16 = 0\end{aligned}$$

□

Definition 2.3 *Ein Gitter Γ heißt **reduzibel**, wenn Γ die orthogonale direkte Summe $\Gamma = \Gamma_1 \perp \Gamma_2$ von zwei Gittern $\Gamma_1 \subset \mathbb{R}^{n_1}$, $\Gamma_2 \subset \mathbb{R}^{n_2}$ mit $n_1, n_2 \geq 1$ ist, andernfalls heißt es **irreduzibel**.*

Wenn das Coxeter-Dynkin-Diagramm eines Wurzelgitters Γ verbunden ist, dann ist das Gitter Γ irreduzibel. Dies liegt daran, dass die Zerlegung in irreduzible Teilgitter nach [2] eindeutig ist, somit basisunabhängig und es also einen Teilgraph geben müsste der mit dem restlichen Graphen nicht verbunden ist.

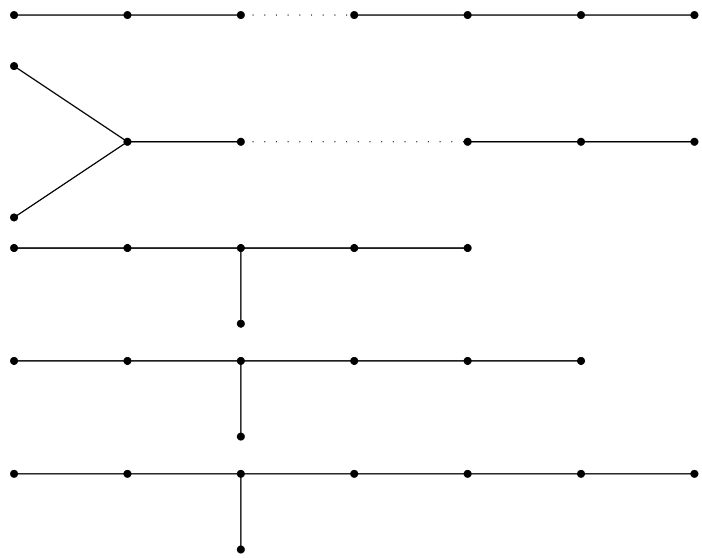
Nehmen wir nun an G ist verbunden, dann muss nach Lemma 2.1 und Lemma 2.2 der Graph die Form von Figur 3 haben.



$(p, q, r \geq 1)$

Fig. 3 Allgmeine Form eines verbundenen Coxeter-Dynkin Diagrammes

Bemerkung 2.4 *Der Graph eines irreduziblen Wurzelgitters muss eine der Formen der in Figur 4 aufgezeichneten Graphen haben.*



(n Knoten) A_n

(n Knoten) D_n $(n \geq 3)$ $(D_3 = A_3)$

E_6

E_7

E_8

Fig. 4 Coxeter-Dynkin Diagramm von den irreduziblen Wurzelgittern

Beweis Sei

$$\begin{aligned} w := c &+ \frac{1}{p}[(p-1)x_1 + (p-2)x_2 + \cdots + x_{p-1}] \\ &+ \frac{1}{q}[(q-1)y_1 + (q-2)y_2 + \cdots + y_{q-1}] \\ &+ \frac{1}{r}[(r-1)z_1 + (r-2)z_2 + \cdots + z_{r-1}]. \end{aligned}$$

Dann bilden die Vektoren

$$x_1, ..., x_{p-1}, y_1, \ldots, y_{q-1}, z_1, ..., z_{r-1}, w$$

eine Basis des $\mathbb{Q}$-Vektorraumes $\langle \Gamma \rangle_{\mathbb{Q}}$ über $\mathbb{Q}$. Aus der Skizze folgt, dass $x_i \perp y_j$, $x_i \perp z_k$, $z_k \perp y_j$ für alle $i \in \{1, \ldots, p-1\}, j \in \{1, \ldots, q-1\}, k \in \{1, \ldots, r-1\}$. Weiterhin gilt

$w \perp x_i$, $w \perp y_j$, $w \perp z_k$ für alle i, j, k, da:

$$\begin{aligned}
(w, x_1) &= (c, x_1) + \frac{p-1}{p}(x_1, x_1) + \frac{p-2}{p}(x_2, x_1) + 0 \\
&= \frac{-p + (p-1) \cdot 2 - (p-2)}{p} = 0 \\
(w, x_i) &= \frac{p-i}{p} \cdot 2 - \frac{(p-i+1)}{p} - \frac{p-i-1}{p} = 0, \;\; p-2 \geq i \geq 2, \\
(w, x_{p-1}) &= \frac{1}{p}(2 - (p - (p-2))) = 0.
\end{aligned}$$

Folglich gilt:

$$\begin{aligned}
0 < (w, w) = (w, c) &= 2 - \frac{p-1}{p} - \frac{q-1}{q} - \frac{r-1}{r} \\
&= -1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{r}
\end{aligned}$$

Hieraus folgt die notwendige Bedingung an p, q, r:

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1.$$

Für $p \leq q \leq r$ hat diese Ungleichung folgende Lösungen:

$$(p, q, r) \in \{(1, q, r) |\; q \leq r \in \mathbb{N}\} \;\cup\; \{(2, 2, r) |\; 2 \leq r \in \mathbb{N}\} \;\cup\; \{(2, 3, 3), (2, 3, 4), (2, 3, 5)\}.$$

□

Ein Wurzelgitter Γ ist die orthogonale direkte Summe von Gittern Γ_i, welche zu den jeweiligen Zusammenhangskomponenten G_i des Graphen gehören. Also haben wir den folgenden Satz, bis auf die Existenz der verbundenen Komponenten, schon bewiesen.

Satz 2.5 *Jedes Wurzelgitter ist eine orthogonale direkte Summe von irreduziblen Wurzelgittern mit Coexter-Dynkin Diagrammen wie in Fig.1.7.*

Beweis Nun noch zur Existenz dieser irreduziblen Wurzelgitter:

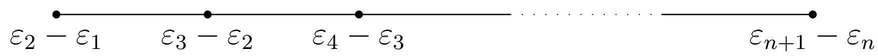
1. $\mathbf{A_n}$:
Sei $(\varepsilon_1, \ldots, \varepsilon_{n+1})$ die Standardbasis des $\mathbb{R}^{n+1}$. Sei $e = \varepsilon_1 + \cdots + \varepsilon_{n+1} = (1, \ldots, 1) \in \mathbb{R}^{n+1}$ und

$$\Gamma = \{x = (x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid (x, e) = x_1 + \cdots + x_{n+1} = 0\}.$$

Dann ist Γ ein Gitter in $e^{\perp} \cong \mathbb{R}^n$. Γ wird erzeugt von den $n(n+1)$ Elementen

$$\varepsilon_i - \varepsilon_j \text{ für} 1 \leq i, j \leq n+1, i \neq j,$$

die Wurzeln in Γ sind. Eine Basis von Γ bildet dann die Menge $\{\varepsilon_2 - \varepsilon_1, \varepsilon_3 - \varepsilon_2, .., \varepsilon_{n+1} - \varepsilon_n\}$ mit dem zugehörigen Coxeter-Dynkin Diagramm



Zusätzliche Betrachtung der Diskriminante von Γ:
Zur Erinnerung: $\operatorname{disc}(\Gamma) = \det((e_i, e_j))_{1 \leq i,j \leq n}$ für $\{e_1, \ldots, e_n\}$ Basis von Γ.
Sei A die Matrix der Skalarprodukte dieser Basiselemente und A' das Resultat von Zeilen und Spaltenumformungen auf A.

$$A = \begin{pmatrix} 2 & -1 & & 0 \\ -1 & 2 & \ddots & \\ & \ddots & \ddots & -1 \\ 0 & & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} \frac{2}{1} & -1 & & 0 \\ 0 & \frac{3}{2} & \ddots & \\ & \ddots & \ddots & -1 \\ 0 & & 0 & \frac{n+1}{n} \end{pmatrix} = A'$$

somit ist $\operatorname{disc}(A_n) = \det A = \det A' = \prod_{i=1}^{n} \frac{i+1}{i} = \frac{n+1}{1} = n+1$.

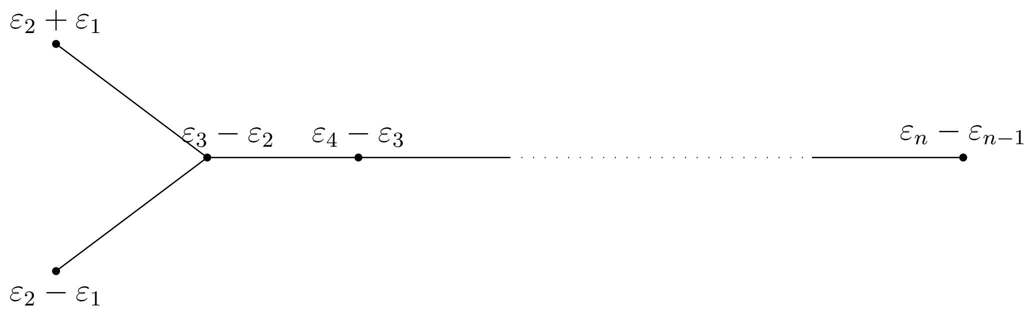
2. $D_{\mathbf{n}}$**:** Für $n \geq 3$ sei

$$\Gamma = \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \ (x_1 + \cdots + x_n) \text{ gerade}\}.$$

Anschaulich erhält man Γ, indem man die Gitterpunkte des $\mathbb{Z}^n$ abwechselnd schwarz und weiß färbt und dann die schwarzen Punkte betrachtet („Schachbrettgitter“). Dann ist Γ ein Gitter im $\mathbb{R}^n$, das aus den $2n(n-1) = 2 \cdot (\binom{n}{2} + \binom{n}{2})$ Wurzeln

$$\pm\varepsilon_i \pm \varepsilon_j \text{ und } \pm \varepsilon_i \mp \varepsilon_j \text{ für} 1 \leq i, j \leq n+1, i \neq j$$

erzeugt wird. Hier bildet die Menge $\{\varepsilon_2 - \varepsilon_1, \varepsilon_3 - \varepsilon_2, .., \varepsilon_n - \varepsilon_{n-1}, \varepsilon_1 + \varepsilon_2\}$ eine Basis von Γ mit dem zugehörigen Coxeter-Dynkin Diagramm:



In diesem Fall ist Γ ein Gitter vom Index 2 in $\mathbb{Z}^n$, also ist

$$\operatorname{disc}(D_n) = \operatorname{vol}(\mathbb{R}^n / D_n)^2 = (\operatorname{vol}(\mathbb{R}^n / \mathbb{Z}^n) \cdot | \mathbb{Z}^n / D_n |)^2 = 4.$$

Alternativ kann D_n auch wie folgt konstruiert werden: Betrachte den gerade gewichteten Code

$$C = \{(u_1, \ldots, u_n) \in \mathbb{F}_2^n \mid u_1 + \cdots + u_n = 0\},$$

welcher der Kern der linearen Abbildung $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2,\ (u_1, \ldots, u_n) \mapsto u_1 + \cdots + u_n$ ist. Sei

$$\rho : \mathbb{Z}^n \longrightarrow (\mathbb{Z}/2\mathbb{Z})^n, (x_1, \ldots, x_n) \mapsto (x_1 \bmod 2, \ldots, x_n \bmod 2)$$

die mod-2-Reduktion. Dann ist

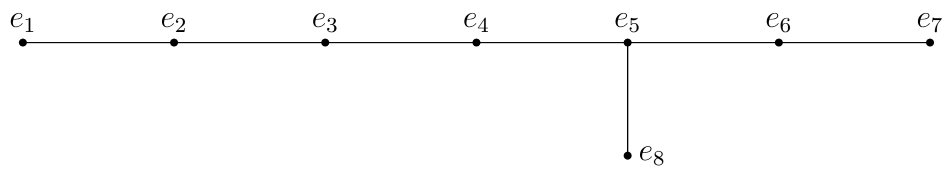
$$\Gamma = \rho^{-1}(C) = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 + \cdots + x_n \equiv 0 \mod 2\}.$$

Es gilt also

$$\mathbb{Z}^n/\rho^{-1}(C) \cong \mathbb{F}_2^n/C \cong \mathbb{Z}/2\mathbb{Z}$$

und somit bekommen wir wieder disc(D_n)=4.

3. $\mathbf{E_8}$: Im Abschnitt 1.2 Codes [1] wurde dieses Gitter aus dem erweiterten Hamming-Code mit Länge 8 konstruiert. Wir wissen zudem, dass dieses Gitter unimodular ist. Das Gitter hat folgendes Coxeter-Dynkin Diagramm:



4. $\mathbf{E_7}$: Wir betrachten das Gitter E_8 mit dem fundamentalen Wurzelsystem $(e_1, \ldots, e_8)$ mit dem Conxeter-Dynkin Diagramm wie im Bild darüber. Sei

$$\nu := 2e_1 + 3e_2 + 4e_3 + 5e_4 + 6e_5 + 4e_6 + 2e_7 + 3e_8.$$

Dann ist ν eine Wurzel in E_8. Das Gitter

$$\Gamma := \{x \in E_8 | (x, \nu) = 0\}$$

ist in dem orthogonalen Komplement des Vektors ν in $\mathbb{R}^8$ enthalten. $\nu^\perp$ ist isomorph zu $\mathbb{R}^7$. Da $(e_i, \nu) = 0$ ist für $i = 2, \ldots, 8$, sind die fundamentalen Wurzeln von $e_2, \ldots, e_8$ E_8 auch in Γ enthalten. Für $x \in \Gamma \subset E_8$ kann man x darstellen als $x = \sum_{i=1}^8 a_i e_i$. Mit $x \in \Gamma$

und $(e_1, \nu) = 1$ gilt $0 = 8(x, \nu) = \sum_{i=1}^{8} a_i(e_i, \nu) = a_1$, also gilt $a_1 = 0$ für alle $x \in \Gamma$. Das heißt $e_2, \ldots, e_8$ ist eine Basis von Γ und das zugehörige Coxeter-Dynkin Diagramm, das zu diesen Wurzeln gehört, ist vom Typ E_7. Da $E_8/E_7 \cong \langle e_1 \rangle_{\mathbb{Z}}$ frei ist als $\mathbb{Z}$-Modul, erhalten wir mit Proposition 1.2 aus Kapitel 1.1 [1]

$$\operatorname{disc}(E_7) = \operatorname{disc}(\langle v \rangle_{\mathbb{Z}}) = \operatorname{disc}(A_1) = 2.$$

5. $\mathbf{E_6}$: Wir betrachten wieder das Gitter E_8 mit fundamentalem Wurzelsystem $(e_1, \ldots, e_8)$ und setzen $\nu_1 = \nu$ und $\nu_2 = -e_1$. Dann gilt $(\nu_1, \nu_2) = -1$. Man definiert wieder

$$\Gamma := \{x \in E_8 \mid (x, \nu_1) = (x, \nu_2) = 0\}.$$

Dann ist Γ im orthogonalen Komplement der beiden Vektoren ν_1 und ν_2 in $\mathbb{R}^8$ enthalten. $\langle \nu_1, \nu_2 \rangle^{\perp}$ ist isomorph zu $\mathbb{R}^6$. Da für $(e_i, \nu_2) = 0$ ist für $i = 3, \ldots, 8$ und zudem wieder $(e_i, \nu) = 0$ gilt, sind die fundamentalen Wurzeln $e_3, \ldots, e_8$ von E_8 auch in Γ enthalten. Wie oben bilden $e_3, \ldots, e_8$ wieder eine Basis von Γ. Das Coxeter-Dynkin Diagramm, das zu diesen Wurzeln gehört, ist vom Typ E_6. Mit Proposition 1.2 erhalten wir auch wie oben:

$$\operatorname{disc}(E_6) = \operatorname{disc}(A_2) = 3.$$

Damit haben wir nun die Existenz von zugehörigen Gittern zu den Coxeter-Dynkin Diagrammtypen A_n, D_n, E_6, E_7 und E_8 gezeigt und damit ist der Beweis von Satz 2.5 beendet. $\square$

3 Konstruktion von Wurzelgittern aus binären linearen Codes

Im Kapitel 1.2 [1] haben wir das Gitter $E_8 = \Gamma_C$ aus einem passenden binären linearen Code C konstruiert. Nun stellen wir uns die Frage: Für welches der irreduziblen Wurzelgitter Γ existiert ein solcher binärer linearer Code, sodass $\Gamma = \Gamma_C$? Bis jetzt wissen wir dies nur für E_8. Im Fall D_n wissen wir, dass $\Gamma = \rho^{-1}(C)$ gilt, nicht aber $\Gamma = \Gamma_C = \frac{1}{\sqrt{2}}\rho^{-1}(C)$. Die folgende Proposition 3.6 liefert eine präzise Antwort auf diese Frage. Hierfür benötigen wir jedoch noch eine weitere Definition:

Definition 3.1 *Sei Γ ein Wurzelgitter in $\mathbb{R}^n$ und α eine Wurzel. Betrachte den Automorphismus*

$$s_\alpha : \ \mathbb{R}^n \to \mathbb{R}^n, \quad x \longmapsto x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha = x - (x,\alpha)\alpha.$$

Dies ist eine Spiegelung an der Hyperebene $\alpha^\perp$, welche orthogonal zu α ist.
s_α lässt $\alpha^\perp$ punktweise fest und bildet jeden Vektor, der orthogonal zur Hyperebene $\alpha^\perp$ ist, auf sein Negatives ab.
Sei W(Γ) eine Untergruppe der GLn($\mathbb{R}$), welche von den Spiegelungen s_α erzeugt wird, wobei α eine Wurzel von Γ ist. Diese Gruppe nennt man die **Weyl-Gruppe** von Γ.

Bemerkung 3.2 *Für $x, y \in \mathbb{R}^n$, ist das Standardskalarprodukt invaviant unter der Weyl-Gruppe, das heißt $(\omega(x), \omega(y)) = (x, y)$ für alle $\omega \in$ W(Γ).*

BEWEIS Es genügt die Aussage für die Erzeuger s_α von W(Γ) zu zeigen:

$$\begin{aligned}
(s_\alpha(x), s_\alpha(y)) =& (x - (x,\alpha)\alpha, y - (y,\alpha)\alpha) \\
=& (x,y) - (x,(y,\alpha)\alpha) - (y,(x,\alpha)\alpha) + (x,\alpha)(y,\alpha)(\alpha,\alpha) \\
=& (x,y) - 2(x,\alpha)(y,\alpha) + 2(x,\alpha)(y,\alpha) \\
=& (x,y)
\end{aligned}$$

Lemma 3.3 *Sei $\Gamma \subseteq \mathbb{R}^n$ ein irreduzibles Wurzelgitter. Dann operiert die Weyl-Gruppe irreduzibel auf $\mathbb{R}^n$, das heißt, falls U ein $\mathrm{W}(\Gamma)-$invarianter Unterraum von $\mathbb{R}^n$ ist, gilt entweder $U = 0$ oder $U = \mathbb{R}^n$.*

Beweis Sei U ein nichtleerer Unterraum von $\mathbb{R}^n$, welcher invariant unter $\mathrm{W}(\Gamma)$ ist. Das orthogonale Komplement $U^\perp$ von U in $\mathbb{R}^n$ ist auch $\mathrm{W}(\Gamma)-$invariant und es gilt $\mathbb{R}^n = U \oplus U^\perp$. Sei $\alpha \in \Gamma$ eine Wurzel. Angenommen es ist $\alpha \notin U$. Sei $u \in U$ beliebig. Da $s_\alpha(U) = U$ gilt, ist $u - (u, \alpha)\alpha \in U$. Dies impliziert, dass $(u, \alpha) = 0$ ist. Da dies für jedes $u \in U$ gilt, folgt $\alpha \in U^\perp$. Somit ist jede Wurzel in U oder in $U^\perp$. Da Γ von R erzeugt wird, gilt $\Gamma = (U \cap \Gamma) \perp (U^\perp \cap \Gamma)$. Doch dies impliziert, dass $U^\perp \cap \Gamma = \{0\}$ gilt, da Γ irreduzibel ist. Darum gilt $\Gamma = U \cap \Gamma$, und somit $U = \mathbb{R}^n$, da $\mathbb{R}^n$ von Γ erzeugt wird. □

Lemma 3.4 *Sei $\Gamma \subset \mathbb{R}^n$ ein irreduzibles Wurzelgitter. Dann operiert die Weyl-Gruppe* $\mathrm{W}(\Gamma)$ *transitiv auf der Menge der Wurzeln R.*

Beweis Seien α, β beliebige Wurzeln von Γ. Da $\mathrm{W}(\Gamma)$ eine Gruppe ist und somit das Erzeugnis der Elemente $w(\alpha)$ mit $w \in \mathrm{W}(\Gamma)$ invariant ist unter $\mathrm{W}(\Gamma)$, können wir Lemma 3.3 anwenden: die Elemente $w(\alpha)$ erzeugen $\mathbb{R}^n$. Das heißt, es existiert ein $w \in \mathrm{W}(\Gamma)$ sodass $w(\alpha)$ nicht orthogonal zu β ist. Ist α orthogonal zu β, ersetze α mit einem solchen $w(\alpha)$. Zusätzlich kann man voraussetzen, dass α, β unterschiedlich sind und $\alpha \neq -\beta$ gilt, denn andernfalls folgt schon die Behauptung. Also gilt nach Bemerkung 1.3(1) $(\alpha, \beta) = \pm 1$. Im Fall $(\alpha, \beta) = -1$ ersetze β mit $-\beta = s_\beta(\beta)$, sodass $(\alpha, \beta) = 1$ gilt. Dann gilt $s_\alpha s_\beta s_\alpha(\beta) = s_\alpha s_\beta(\beta - \alpha) = s_\alpha(\beta - \alpha - \beta) = \alpha$. Falls zuvor α durch $w(\alpha)$ ersetzt wurde, muss man auf beide Seiten der Gleichung $w^{-1} \in \mathrm{W}(\Gamma)$ anwenden. Also folgt die Behauptung. □

Bemerkung 3.5 *Lemma 3.4 impliziert, dass bei der Konstruktion der Gitter E_7, E_6 jede Wurzel v und jedes Paar von Wurzeln v_1', v_2' mit $(v_1, v_2) = -1$ verwendet werden kann.*

Beweis Für E_7 existiert zu einem beliebigen $v' \in \Gamma$ ein $g \in \mathrm{W}(\Gamma)$ mit $g(v') = v$, da die Weyl-Gruppe $\mathrm{W}(\Gamma)$ transitiv auf Γ operiert. Nun kann man analog zu der Konstruktion in Satz 2.5 eine Basis konstruieren,indem man e_i anstatt $g(e_i)$ für alle $i = 1, \dots, 8$ verwendet. Die Vektoren $\{g(e_2), \dots, g(e_8)\}$ sind linear unabhängig, da g ein Automorphismus ist. Mit Bemerkung 3.2 erfüllt die neue Basis auch wieder Satz 1.4 und das Coxeter-Dynkin Diagramm behält seine Form.
Die Konstruktion von E_6 kann man analog verändern, nur verwendet man hier zusätzlich eine weitere Spiegelung $g_2 \in \mathrm{W}(\Gamma)$, welche und $g(v_1')$ festlässt und $g(v_2')$ auf $v2$ abbildet.

Proposition 3.6 *Sei $\Gamma \subset \mathbb{R}^n$ ein irreduzibles Wurzelgitter. Dann sind die folgenden Aussagen äquivalent:*

(i) Es existiert ein binärer linearer Code $C \subset \mathbb{F}_2^n$ mit $\Gamma = \Gamma_C$.
(ii) Γ enthält n paarweise orthogonale Wurzeln.
(iii) $nA_1 = A_1 \perp \cdots \perp A_1 (n\ mal) \subset \Gamma$.
(iv) $-1 \in W(\Gamma)$.
(v) $2\Gamma^* \subset \Gamma$.
(vi) Γ ist vom Typ $A_1,\ D_n\ (n \geq 4, n\ gerade), E_7$ oder E_8.

Beweis
(i)⇒(ii): Sei $\Gamma = \Gamma_C$ für einen binären Code $C \subset \mathbb{F}_2^n$, und sei $(\varepsilon_1, \ldots, \varepsilon_n)$ die Standardbasis von $\mathbb{R}^n$. Dann ist $\frac{1}{\sqrt{2}} 2\varepsilon_i \in \Gamma_C$ für alle $1 \leq i \leq n$, da diese im Kern der Abbildung ρ liegen. Dies sind paarweise orthogonale Wurzeln.

(ii)⇔(iii): Gilt, da eine einzelne Wurzel ein Gitter vom Typ A_1 aufspannt.

(ii)⇔(iv): Seien $\alpha_1, \ldots, \alpha_n$ paarweise orthogonale Wurzeln von Γ. Dann bilden $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{R}-$Basis des Vektorraumes $\mathbb{R}^n$. Sei $x \in \mathbb{R}^n$. Dann kann x geschrieben werden als $x = \sum_i \xi_i \alpha_i$ mit $\xi_i \in \mathbb{R}$. Somit gilt:

$$\begin{aligned} s_{\alpha_1} s_{\alpha_2} \ldots s_{\alpha_n}(x) &= s_{\alpha_1} s_{\alpha_2} \ldots s_{\alpha_n} \left(\sum_i \xi_i \alpha_i \right) \\ &= - \sum_i \xi_i \alpha_i \\ &= -x, \end{aligned}$$

also folgt:

$$\begin{aligned} s_{\alpha_1} s_{\alpha_2} \ldots s_{\alpha_n}(x) =& s_{\alpha_1} s_{\alpha_2} \ldots s_{\alpha_n} \left(\sum_i \xi_i \alpha_i \right) \\ =& \sum_i \xi_i s_{\alpha_1} s_{\alpha_2} \ldots s_{\alpha_n}(\alpha_i) \\ =& - \sum_i \xi_i \alpha_i \\ =& - x \end{aligned}$$

und damit: $-1 = s_{\alpha_1} s_{\alpha_2} \ldots s_{\alpha_n} \in W(\Gamma)$.

(iv)⇒(v): Sei $-1 \in W(\Gamma)$. Dann gilt $-1 = s_{\beta_1} s_{\beta_2} \ldots s_{\beta_k}$ für gewisse Wurzeln $\beta_1, \ldots, \beta_k \in \Gamma$. Sei $x \in \Gamma^*$. Dann ist

$$-x = s_{\beta_1} s_{\beta_2} \dots\ s_{\beta_k}(x) = s_{\beta_1} s_{\beta_2} \dots s_{\beta_{k-1}}(x - (x, \beta_k)\beta_k) = x + y$$

mit $y \in \Gamma$, da $(x, \beta_k) \in \mathbb{Z}$. Daher ist $((x, \beta_k)\beta_k) \in \Gamma$ und somit folgt $y \in \Gamma$ induktiv. Somit ist

$$2x = -y \in \Gamma.$$

(v)⇔(vi): Der Quotient Γ^*/Γ ist eine endliche abelsche Gruppe der Ordnung

$$\mid \Gamma^*/\Gamma \mid = \operatorname{disc}(\Gamma)$$

.

Da $2\Gamma^* \subset \Gamma$ äquivalent ist zu $2 \in \operatorname{Ann}(x)$ für alle $x \in \Gamma^*/\Gamma$, gilt mit dem Hauptsatz über endlich erzeugte abelsche Gruppen:

$$\Gamma^*/\Gamma \cong (\mathbb{Z}\,/2\,\mathbb{Z})^l, \operatorname{disc}(\Gamma) = 2^l,$$

für ein $l \geq 0$.

Für $\Gamma = A_n$, also

$$\Gamma = \left\{ (x_1, x_2, \dots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid \sum_i x_i = 0 \right\},$$

wird Γ^* von Γ und $x := g(\frac{n}{n+1}, -\frac{1}{n+1}, -\frac{1}{n+1}, \dots, -\frac{1}{n+1})$ erzeugt. Dies gilt, da somit

$$\mid \Gamma^*/\Gamma \mid = \mid \{k \cdot x \mid k \in \{0, \dots, n\}\} \mid = n + 1 = \operatorname{disc}(A_n)$$

wie gewünscht erfüllt ist. Weitere mögliche Basiselemente lägen also alle in Γ. Da diese Gruppe zyklisch ist, folgt:

$$\Gamma^*/\Gamma \cong \mathbb{Z}\,/(n+1)\,\mathbb{Z}\,.$$

Für $\Gamma = D_n$ ist

$$\Gamma = \left\{ (x_1, \dots, x_n) \in \mathbb{Z}^n \mid \sum_i x_i \text{ gerade} \right\},$$

$$\Gamma^* = \mathbb{Z}^n + \mathbb{Z}\left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right)$$

und

$$\Gamma^*/\Gamma \cong \begin{cases} (\mathbb{Z}\,/2\,\mathbb{Z}) \times (\mathbb{Z}\,/2\,\mathbb{Z}), & \text{für } n \text{ gerade} \\ (\mathbb{Z}\,/4\,\mathbb{Z}) & \text{, für } n \text{ ungerade} \end{cases}.$$

Hierbei wird Γ^*/Γ von $\omega_1 = (1, 0, \ldots, 0)$ und $\omega_2 = (\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$ erzeugt, wenn n gerade ist und von ω_2, wenn n ungerade ist. Dies gilt da $\omega_1 = 2\omega_2 \pmod{\Gamma}$ ist, wenn n ungerade ist.

Für $\Gamma = E_6$ ist $\mathrm{disc}(E_6) = 3$, aber es gilt $3 \neq 2^l$.
Für $\Gamma = E_7$ bzw. $\Gamma = E_8$ gilt $\mathrm{disc}(E_7) = 2$ und $\mathrm{disc}(E_8) = 1$, also sind die zugehörigen Gruppen Γ^*/Γ isomorph zu $\mathbb{Z}/2\,\mathbb{Z}$ bzw. $\{0\}$.

Da aus $\Gamma^*/\Gamma = (\mathbb{Z}/2\,\mathbb{Z})^l$ auch folgt, dass $2 \in \mathbb{Z}$ alle Elemente des $\mathbb{Z}-$Moduls annihiliert, gilt somit $2\Gamma^* \subset \Gamma$ genau dann, wenn $\Gamma \in \{A_1, D_n\ (n \leq 4, n \text{ gerade}), E_7, E_8\}$.

(vi)⇒(i): Wir finden einen binären linearen Code C mit $\Gamma_C = \Gamma$ für alle aufgelisteten Fälle:
A_1: Sei C=$\{0\} \subset \mathbb{F}_2$, dann ist $\rho^{-1}(C) = \langle 2 \rangle_{\mathbb{Z}}$ und somit $\Gamma = \langle \frac{1}{\sqrt{2}} 2 \rangle_{\mathbb{Z}}$ vom Typ A_1.
D_n $(n \geq 4, n$ gerade): Hier ist C das „Doppelte" des gerade gewichteten Codes $\tilde{C} \subset \mathbb{F}_2^{n/2}$, das heißt für C und $\widetilde{C}$ gilt:

$$\begin{aligned} \tilde{C} &= \left\{ (u_1, \ldots u_{n/2}) \in \mathbb{F}_2^{n/2} \mid \sum u_i = 0 \right\} \subset \mathbb{F}_2^{n/2} \\ C &= \{ \nu \in \mathbb{F}_2^n \mid \nu = (u_1, u_1, \ldots, u_{n/2}, u_{n/2}),\ u = (u_1, u_2, \ldots, u_{n/2}) \in \widetilde{C} \}. \end{aligned}$$

$E_7:\ C = H^\perp \subset \mathbb{F}_2^7$, wobei H den Hamming-Code bezeichnet. Dieser Code besteht aus 0 und gen sieben Codewörtern vom Hamming-Gewicht 4.
$E_8:\ C = \widetilde{H} \subset \mathbb{F}_2^8$, wobei $\widetilde{H}$ den erweiterten Hamming-Code bezeichnet, wie wir ihn im Kapitel 1.2 Codes [1] gesehen haben. Somit ist Proposition 3.6 bewiesen. □

Nun wollen wir einen zweiten, direkten Beweis von (i)⇒(v) von Proposition 3.6 geben. Für diesen Beweis benötigen wir ein weiteres Lemma:

Lemma 3.7 *Sei $C \subset \mathbb{F}_2^n$ ein binärer linearer Code. Dann gilt:*

$$\Gamma_C^* = \Gamma_{C^\perp}.$$

Beweis Zu zeigen ist $\Gamma_{C^\perp} \subset \Gamma_C^*$, also dass $(x, y) \in \mathbb{Z}$ ist für alle $x \in \Gamma_C$ und $y \in \Gamma_{C^\perp}$. Sei dazu $\rho : \mathbb{Z}^n \longrightarrow \mathbb{F}_2^n$ die mod-2-Reduktion. Sei $y \in \Gamma_{C^\perp}$ und $x \in \Gamma_C$. Dann gilt $y = \frac{1}{\sqrt{2}}\widetilde{y}$, $x = \frac{1}{\sqrt{2}}\widetilde{x}$ mit $\widetilde{y} \in \rho^{-1}(C^\perp), \widetilde{x} \in \rho^{-1}(C)$. Sei ρ' die mod-2-Reduktion $\mathbb{Z} \to \mathbb{Z}/2\,\mathbb{Z}$. Nun gilt $0 = (\rho(\widetilde{x}, \rho(\widetilde{y})) = \rho'(\widetilde{x}_1) \cdot \rho'(\widetilde{y}_1) + \cdots + \rho'(\widetilde{x}_n) \cdot \rho'(\widetilde{y}_n) = \rho'((\widetilde{x}, \widetilde{y}))$. Daher ist

$(\widetilde{x}, \widetilde{y}) \in 2\,\mathbb{Z}$, und somit gilt $(x, y) \in \mathbb{Z}$. Dies beweist $\Gamma_{C^\perp} \subset \Gamma_C^*$.
Sei nun $k = \dim C$. Dann

$$\mu = \mathrm{vol}(\mathbb{R}^n\,/\Gamma_C) = \frac{2^{n-k}}{2^{n/2}} = 2^{\frac{n}{2}-k}.$$

Analog folgt

$$\mathrm{vol}(\mathbb{R}^n\,/\Gamma_{C^\perp}) = 2^{k-\frac{n}{2}}$$

und außerdem

$$\mu^* = \mathrm{vol}(\mathbb{R}^n\,/\Gamma_C^*) = \frac{1}{\mu} = 2^{k-\frac{n}{2}},$$

dies impliziert, dass $\Gamma_{C^\perp} = \Gamma_C^*$. □

Beweis zu **Proposition 3.6 (i) $\Rightarrow$ (v):**
Sei $\Gamma = \Gamma_C$ für einen binären linearen Code $C \subset \mathbb{F}_2^n$. Dann gilt $\Gamma^* = \Gamma_{C^\perp}$ nach Lemma 3.7. Sei $x \in \Gamma_C^*$ mit $x = \frac{1}{\sqrt{2}}(c + 2y)$ für $c \in C^\perp$ und $y \in \mathbb{Z}^n$. Dann ist $2x = \frac{1}{\sqrt{2}}(0 + 2z)$, mit $z \in \mathbb{Z}^n$. Also ist $2x \in \Gamma_C = \Gamma$, was zu zeigen war. □

In Tabelle 1.1 sind die Gruppen Γ^*/Γ und die zugehörigen Ordnungen in den einzelnen Fällen aufgelistet. Zusätzlich ist die Anzahl der Wurzeln $|R|$ aufgelistet. Diese erhalten wir folgendermaßen: Für A_n und D_n siehe Existenzbeweis von Satz 2.5. Die Anzahl der Wurzeln von E_8 entnehmen wir Kapitel 1.3 [1]. Die Anzahl der Wurzeln von E_7 erhält man, indem man verwendet, dass $E_7 = \Gamma_{H^\perp}$, wobei mit H der Hamming-Code der Länge 7 bezeichnet wird. Für die Zahlen bezüglich E_6 siehe Beispiel 5.1 und Übung 5.1 [1].

Definition 3.8 *Sei $\Gamma \subset \mathbb{R}^n$ ein Wurzelgitter und sei R die Menge der Wurzeln. Dann heißt die Zahl*

$$h := \frac{|R|}{n}$$

*die **Coxeter-Zahl** von Γ.*

Die Coxeter-Zahlen der irreduziblen Wurzelgitter sind in der letzten Spalte der folgenden Tabelle aufgelistet.

Γ	Γ^*/Γ	$\lvert\Gamma^*/\Gamma\rvert$	$\lvert R\rvert$	h
A_n	$\mathbb{Z}/(n+1)\,\mathbb{Z}$	$n+1$	$n(n+1)$	$n+1$
D_n	$\begin{cases} (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2\,\mathbb{Z}), & \text{für } n \text{ gerade} \\ (\mathbb{Z}/4\,\mathbb{Z}) & \text{, für } n \text{ ungerade} \end{cases}$	4	$2n(n-1)$	$2(n-1)$
E_6	$\mathbb{Z}/3\,\mathbb{Z}$	3	72	12
E_7	$\mathbb{Z}/2\,\mathbb{Z}$	2	126	18
E_8	$\{0\}$	1	240	30

Tabelle 1.1 Auflistung der Gruppen Γ^*/Γ

4 Betrachtungen zur Coxeter-Zahl

Durch eine genauere Betrachtung der Weyl-Gruppe und einer quadratischen Form können wir in diesem Kapitel den folgenden Zusammenhang beweisen.

Proposition 4.1 *Sei $\Gamma \subset \mathbb{R}^n$ ein irreduzibles Wurzelgitter. Dann gilt für ein festes $y \in \mathbb{R}^n$*

$$\sum_{x \in R} (x, y)^2 = 2 \cdot h \cdot (y, y),$$

wobei h die Coxeter-Zahl von Γ ist.

Für den Beweis dieser Proposition benötigen wir etwas Vorbereitung:

Definition 4.2 *Sei $P \in \mathbb{C}[y_1, \ldots, y_n]$ ein komplexes Polynom in n Variablen $y_1, \ldots, y_n$. Ein solches Polynom heißt **harmonisch**, wenn $\Delta P = 0$. Hier ist*

$$\Delta = \sum_{i=1}^{n} \frac{\partial}{\partial y_i^2}$$

der Laplace-Operator.

Sei nun $\Gamma \subset \mathbb{R}^n$ ein Wurzelgitter und sei R die Menge der Wurzeln. Wir definieren das Polynom

$$f(y) := \sum_{x \in R} \left((x, y)^2 - \frac{1}{n}(x, x)(y, y) \right)$$

in den Variablen $y_1, \ldots, y_n$. Da

$$\begin{aligned}
\Delta f =& \sum_{x \in R} \left(\Delta(x_1 y_1 + \cdots + x_n y_n)^2 - \frac{1}{n} \Delta((x, x)(y_1^2 + \cdots + y_n^2)) \right) \\
=& \sum_{x \in R} \left(2(x_1^2 + \cdots + x_n^2) - \frac{2n}{n}(x, x) \right) = 0
\end{aligned}$$

ist das Polynom f harmonisch.
Zusätzlich benötigen wir noch das folgende Lemma.

Lemma 4.3 *Sei* $\Gamma \subset \mathbb{R}^n$ *ein irreduzibles Wurzelgitter und sei* $\mathrm{W}(\Gamma)$ *die Weyl-Gruppe von* Γ*. Dann gilt:*
(i) Jeder Endomorphismus von $\mathbb{R}^n$*, der mit jedem Element von* $\mathrm{W}(\Gamma)$ *vertauscht, ist ein skalares Vielfaches der Identität.*
(ii) Sei $b \neq 0$ *eine Bilinearform auf* $\mathbb{R}^n$ *die invariant unter* $\mathrm{W}(\Gamma)$ *ist, das heißt* $b(x,y) = b(\omega(x),\omega(y))$ *für alle* $x, y \in \mathbb{R}^n,\ \omega \in \mathrm{W}(\Gamma)$*. Dann existiert ein* $\rho \in \mathbb{R},\ \rho \neq 0$*, sodass*

$$b(x,y) = \rho(x,y)$$

für alle $x, y \in \mathbb{R}^n$ *gilt.*

Beweis
(i) Sei g ein Endomorphismus von $\mathbb{R}^n$, der mit jedem Element von $\mathrm{W}(\Gamma)$ vertauscht. Sei $\alpha \in \Gamma$ eine Wurzel und sei $L = \langle \alpha \rangle_{\mathbb{R}}$. Wir zeigen, dass $g(L) \subset L$ gilt. Da

$$L = \{x \in \mathbb{R}^n \mid s_\alpha x = -x\}$$

ist, gilt für alle $x \in L$, dass

$$s_\alpha g(x) = g(s_\alpha x) = g(-x) = -g(x)$$

ist. Darum existiert ein $\rho \in \mathbb{R}$, sodass $g(\alpha) = \rho\alpha$ und somit $g(x) = \rho x$ ist für alle $x \in L$. Sei U der Kern von $g - \rho \cdot \mathrm{Id}$. Dann ist U ein Unterraum von $\mathbb{R}^n$, welcher invariant unter $\mathrm{W}(\Gamma)$ ist, da $g(\omega(u)) = \omega(g(u)) = \omega(\rho u) = \rho\omega(u)$ gilt. Zudem ist U ungleich Null, da er L enthält. Daher gilt nach Lemma 3.3 $U = \mathbb{R}^n$, also $g = \rho \cdot \mathrm{Id}$ für alle $x \in \mathbb{R}^n$. Das beweist (i).
(ii) Sei $b \neq 0$ eine Bilinearform auf $\mathbb{R}^n$, die invariant unter $\mathrm{W}(\Gamma)$ ist. Aus der linearen Algebra wissen wir, dass ein Endomorphismus g auf $\mathbb{R}^n$ existiert, sodass

$$b(x,y) = (g(x), y)$$

für alle $x, y \in \mathbb{R}^n$. Da b invariant unter $\mathrm{W}(\Gamma)$ ist, vertauscht der Endomorphismus g mit allen Elementen von $\mathrm{W}(\Gamma)$: Seien $x, y \in \mathbb{R}^n$ und $w \in \mathrm{W}(\Gamma)$, dann gilt mit Bemerkung 3.2

$$(g(w(x)), y) = b(w(x), y) = b(x, w^{-1}(y)) = (g(x), w^{-1}(y)) = (w(g(x)), y),$$

und somit $g(w(x)) = w(g(x))$ da y beliebig. Nach (i) existiert ein $\rho \in \mathbb{R}$ mit $g = \rho \cdot \mathrm{Id}$. Folglich ist

$$b(x,y) = \rho(x,y)$$

für alle $x, y \in \mathbb{R}^n$, was (ii) beweist. □

Beweis von **Proposition 4.1**
Das Polynom $f(y)$ ist homogen und somit eine quadratische Form in $y_1, \ldots, y_n$, also auch eine Bilinearform. Da alle Erzeuger s_α von W(Γ) Bijektionen auf der Menge der Wurzeln R darstellen und mit Bemerkung 3.2, folgt $f(s_\alpha(y)) = f(y)$ für alle Erzeuger s_α von W(Γ) und alle $y \in \mathbb{R}^n$:

$$\begin{aligned}
f(s_\alpha(y)) =& \sum_{x \in R} \left((x, s_\alpha(y))^2 - \frac{1}{n}(x,x)(s_\alpha(y), s_\alpha(y)) \right) \\
=& \sum_{x \in R} \left((s_\alpha^{-1}(x), y)^2 - \frac{1}{n}(x,x)((y),(y)) \right) \\
=& f(y)
\end{aligned}$$

f(y) ist also invariant unter der Weyl-Gruppe W(Γ). Daher gilt nach Lemma 4.3 (ii) $f(y) = a(y,y)$ für ein $a \in \mathbb{R}$. Da f harmonisch ist und $\Delta(y,y) = 2n$ gilt, ist $a = 0$, da der Laplaceoperator linear ist. Dann gilt auch f=0. Nach Konstruktion von f liefert dies den Beweis von Proposition 4.1. □

Quellenverzeichnis

[1]: [Lattices and Codes von Wolfgang Ebeling nach einer Vorlesung von Friedrich Hirzebruch]

[2]: [Zur Theorie der Kristallgitter, Martin Kneser]