Vorlesung Gitter und Codes, WS 08/09

G. Nebe und M. Kirschmer

I Grundlagen

1 Gitter.

1.1 Einige grundlegende Definitionen.

Wir betrachten einen euklidischen Vektorraum $E = (V, (,))$ meist $E = (\mathbb{R}^{1\times n}, (,))$. Unsere Vektoren sind Zeilenvektoren.

Definition 1.1 *(i) Eine Teilmenge $L \subset V$ heißt* Gitter *, falls es ein linear unabhängiges Tupel $B = (b_1, \ldots, b_m) \in V^m$ gibt, mit*

$$L = \langle b_1, \ldots, b_m\rangle_{\mathbb{Z}} = \{\sum_{i=1}^{m} a_i b_i \mid a_i \in \mathbb{Z}\}.$$

B heißt dann auch eine Gitterbasis *von L und $m = dim(L)$ die* Dimension *von L. L heißt* volles Gitter in *E, falls $\dim(L) = \dim(V)$, also B eine Basis von V ist.*
(ii) Ist $B \in V^m$ eine Gitterbasis von L und $\mathcal{G}(B) := ((b_i, b_j)) \in \mathbb{R}^{m\times m}$ die Grammatrix *von B, so heißt*

$$\det(L) := \det(\mathcal{G}(B))$$

die Determinante *des Gitters L. $\mathcal{G}(B)$ nennt man auch eine Grammatrix von L.*

Beispiele auf Folie: hexagonales und quadratisches Gitter, Gitterbasen und Grammatrizen. Zugehörige Kugelpackung. Keplerpackung und kubisch flächenzentriertes Gitter.

Bemerkung 1.2 *Sei L ein Gitter in V und $B \in V^m$ eine Gitterbasis.*
(a) L ist ein volles Gitter in dem von ihm erzeugten Vektorraum $\mathbb{R}L := \langle B\rangle_{\mathbb{R}}$.
(b) $C \in V^m$ ist Gitterbasis von L genau dann wenn $\langle C\rangle_{\mathbb{R}} = \langle B\rangle_{\mathbb{R}}$ und die Basiswechselmatrix $T := {}_C\mathrm{id}_B \in \mathrm{GL}_m(\mathbb{Z})$ ist. Dann gilt $\mathcal{G}(C) = T\mathcal{G}(B)T^{tr}$. Insbesondere ist $\det(\mathcal{G}(C)) = \det(\mathcal{G}(B))$ und die Determinante von L ist wohldefiniert.
(c) Ist L ein volles Gitter, so ist $\sqrt{\det(L)} = vol(V/L)$ das Volumen des von einer Gitterbasis B aufgespannten Parallelepipeds $P(B) := \{\sum a_i b_i \mid 0 \le a_i \le 1\}$.
(d) Ist L ein volles Gitter, so ist $P(B)$ ein Fundamentalbereich *der Operation von L auf V, d.h.*

(i) Für alle $v \in V$ gibt es ein $\ell \in L$ mit $\ell + v \in P(B)$.
(ii) Sind $v \neq w \in P(B)$ so dass $v - w \in L$ liegt, dann liegen v und w auf dem Rand von $P(B)$.
(iii) $P(B)$ ist abgeschlossen.

Bemerkung 1.3 *Sei L ein volles Gitter in $E = (V, (,))$ mit Gitterbasis B. Dann ist*

$$L^{\#} := \{v \in V \mid (v, \ell) \in \mathbb{Z} \text{ für alle } \ell \in L\}$$

ebenfalls ein volles Gitter in E, das zu L duale Gitter. *Die Dualbasis $B^* = (b_1^*, \ldots, b_n^*)$ von B ist eine Gitterbasis von $L^{\#}$.*
Es gilt $\mathcal{G}(B)\mathcal{G}(B^*) = I_n$, $\det(L^{\#})\det(L) = 1$.
Ist $L \subset L^{\#}$, so nennt man das Gitter L auch ganz. *Dann ist die Faktorgruppe $L^{\#}/L$ eine endliche abelsche Gruppe der Ordnung $\det(L)$. Es gilt $B^*\mathcal{G}(B) \in L^n$ und $\mathcal{G}(B)$ ist eine Relationenmatrix von $L^{\#}/L$. Sind $(d_1, \ldots, d_n)$ die Invariantenteiler von $\mathcal{G}(B)$, so ist $L^{\#}/L \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$.*

Beweis. Sei $v \in V$. Dann ist

$$(\ell, v) \in \mathbb{Z} \text{ für alle } \ell \in L \Leftrightarrow a_i := (b_i, v) \in \mathbb{Z} \text{ für alle } 1 \leq i \leq n \Leftrightarrow v = \sum a_i b_i^* \in \langle b_1^*, \ldots, b_n^* \rangle_{\mathbb{Z}}.$$

Also ist das duale Gitter $L^{\#}$ genau das von der dualen Basis erzeugte Gitter. Weiter ist ${}_{B^*}\mathrm{id}_B = \mathcal{G}(B)$ die Basiswechselmatrix, d.h. $B^*\mathcal{G}(B) = B$. Damit ist $\mathcal{G}(B)$ die Relationenmatrix von $L^{\#}/L$ und $\det(\mathcal{G}(B)) = |L^{\#}/L|$. Die Elementarteiler von $\mathcal{G}(B) \in \mathbb{Z}^{n \times n}$ geben uns die Struktur der endlichen abelschen Gruppe $L^{\#}/L$ an. □

Definition 1.4 *Seien L und L' volle Gitter in E.*
(a) L und L' heißen isometrisch, *falls es ein $g \in O(E)$ gibt, mit $Lg = L'$.*
(b) $\mathrm{Aut}(L) := \{g \in O(E) \mid Lg = L\}$ heißt die Automorphismengruppe *von L.*

Bemerkung 1.5 *(a) Zwei Gitter L und L' sind isometrisch, genau dann wenn es Gitterbasen B und B' gibt, mit $\mathcal{G}(B) = \mathcal{G}(B')$. "Sie haben gleiche Grammatrizen". Ein Gitter L ist also bis auf Isometrie bestimmt durch jede seiner Grammatrizen. Umgekehrt bestimmt ein Gitter L eine $\mathrm{GL}_n(\mathbb{Z})$-Bahn $\{g\mathcal{G}(B)g^{tr} \mid g \in \mathrm{GL}_n(\mathbb{Z})\}$ von Grammatrizen.*
(b) Ist B eine Gitterbasis von L, so ist ${}_B\mathrm{Aut}(L)_B = \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid g\mathcal{G}(B)g^{tr} = \mathcal{G}(B)\}$.

Beispiel: $\mathrm{Aut}(\mathbb{A}_2)$. Das hexagonale Gitter hat Grammatrix $\mathcal{G}((b_1, b_2)) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

$${}_B\mathrm{Aut}(\mathbb{A}_2)_B = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{tr} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\}.$$

Die Bilder $(b_1 g = ab_1 + bb_2, b_2 g = cb_1 + db_2)$ unter den Automorphismen g durchlaufen genau die 12 Paare (c_1, c_2) von Gittervektoren, mit $(c_1, c_1) = 2, (c_1, c_2) = 1, (c_2, c_2) = 2$.

Algorithmus 1.6 *Das Gram-Schmidt-Orthogonalisierungsverfahren:*
EINGABE: *Eine Basis* $(b_1, \ldots, b_n)$ *von* V.
AUSGABE: *Eine Orthogonalbasis* $B' := (b'_1, \ldots, b'_n)$ *von* E *mit* $\langle b_1, \ldots, b_i\rangle_{\mathbb{R}} = \langle b'_1, \ldots, b'_i\rangle_{\mathbb{R}}$ *für alle* i.
ALGORITHMUS: *Für* $i = 1, \ldots, n$ *berechne sukzessive die Projektion* b'_i *von* b_i *auf* $\langle b_1, \ldots, b_{i-1}\rangle_{\mathbb{R}}^{\perp} = \langle b'_1, \ldots, b'_{i-1}\rangle_{\mathbb{R}}^{\perp}$. *Diese ergibt sich als*

$$b'_i := b_i - \sum_{j=1}^{i-1} \mu_{ij} b'_j$$

wo $\mu_{ij} = \frac{(b_i, b'_j)}{(b'_j, b'_j)}$.

Bemerkung 1.7 b'_i *ist die Projektion von* b_i *auf* $\langle b_1, \ldots, b_{i-1}\rangle^{\perp}$.
Die von B *und* B' *erzeugten Gitter haben die gleiche Determinante, nämlich* $\prod_{j=1}^{n}(b'_j, b'_j)$.
Da $(b'_j, b'_j) \leq (b_j, b_j)$ *ist, ergibt sich die folgende Hadamard Ungleichung.*

Folgerung 1.8 *Die Hadamard Ungleichung:*
Ist $B := (b_1, \ldots, b_n)$ *eine Gitterbasis von* L, *so ist* $\det(L) \leq \prod_{j=1}^{n}(b_j, b_j)$.

Beweis. Sei B' die in Algorithmus 1.6 berechnete Orthogonalbasis und

$$M := \begin{pmatrix} 1 & 0 & \ldots & 0 \\ \mu_{21} & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \mu_{n1} & \ldots & \mu_{n,n-1} & 1 \end{pmatrix}$$

Dann ist $\det(M) = 1$ und $MB' = B$. Also ist $\mathcal{G}(B) = M\mathcal{G}(B')M^{tr}$ und daher

$$\det(L) = \det(\mathcal{G}(B)) = \det(\mathcal{G}(B')) = \prod_{i=1}^{n}(b'_i, b'_i) \leq \prod_{i=1}^{n}(b_i, b_i).$$

□

Ende am 14.10.08

Satz 1.9 $L_{\leq S} := \{v \in L \mid (v, v) \leq S\}$ *ist endlich.*

Beweis. Sei B eine Gitterbasis von L und B', μ_{ij} wie in 1.6.
Ist $v = \sum_{j=1}^{n} a_j b_j \in L$, so ist $v = \sum_{j=1}^{n} \alpha_j b'_j$ mit $\alpha_j \in \mathbb{R}$,
$\alpha_n = a_n$, $\alpha_{n-1} = a_{n-1} - \mu_{n,n-1}a_n$, $\ldots$
Aus

$$(v, v) = \sum_{j=1}^{n} \alpha_j^2 (b'_j, b'_j) \leq S$$

folgt insbesondere $a_n^2(b'_n, b'_n) \leq S$. Also hat man nur endlich viele Möglichkeiten für $a_n \in \mathbb{Z}$. Allgemein gilt

$$\alpha_j^2(b'_j, b'_j) = (a_j - \sum_{i=j+1}^{n} \mu_{i,j} a_i)^2 (b'_j, b'_j) \leq S - \sum_{i=j+1}^{n} \alpha_i^2(b'_i, b'_i)$$

woraus man sukzessiv nur endlich viele Möglichkeiten für $a_j \in \mathbb{Z}$, $j = n, n-1, \ldots, 1$ erhält. □

Folgerung 1.10 $\mathrm{Aut}(L)$ *ist eine endliche Gruppe.*

Beweis. Sei $B = (b_1, \ldots, b_n)$ eine Gitterbasis von L und $S := \max\{(b_i, b_i) \mid 1 \leq i \leq n\}$. Ist $g \in \mathrm{Aut}(L)$, so ist g eindeutig bestimmt durch die Bilder der Basisvektoren $(b_1 g, \ldots, b_n g) \in L^n_{\leq S}$. Also gilt $|\mathrm{Aut}(L)| \leq |L_{\leq S}|^n$. □

1.2 Wurzelgitter

Definition 1.11 *(i) Ein ganzes Gitter L heißt* Wurzelgitter, *falls $L = \langle \{\ell \in L \mid (\ell, \ell) = 2\} \rangle_{\mathbb{Z}}$.*

(ii) $L_{=2} = R(L) := \{\ell \in L \mid (\ell, \ell) = 2\}$ heißt die Menge der Wurzeln *in L.*

(iii) Eine Teilmenge $S \subset R(L)$ heißt Fundamentalsystem von Wurzeln, *falls*
(a) S ist Gitterbasis von L.
(b) Jede Wurzel $\beta \in R(L)$ läss t sich schreiben als

$$\beta = \sum_{\alpha \in S} k_\alpha \alpha \text{ mit allen } k_\alpha \geq 0 \text{ oder allen } k_\alpha \leq 0.$$

Bemerkung: Sind α, β Wurzeln in einem Wurzelgitter so ist nach der Cauchy-Schwartz Ungleichung

$$(x, y)^2 \leq (x, x)(y, y) \text{ für alle } x, y \in E$$

$(\alpha, \beta) = 0, \pm 1, \pm 2$ und $(\alpha, \beta) = \pm 2$ genau dann wenn $\alpha = \pm\beta$.

Satz 1.12 *(Witt) Ist L ein Wurzelgitter, so hat L eine Gitterbasis $B = (b_1, \ldots, b_n)$ mit $(b_i, b_i) = 2$ und $(b_i, b_j) \in \{0, -1\}$ für $1 \leq i \neq j \leq n$. Jedes Fundamentalsystem von Wurzeln liefert eine solche Gitterbasis.*

Beweis. Sei S ein Fundamentalsystem von Wurzeln und $\alpha, \beta \in S$, $\alpha \neq \beta$. Ist $(\alpha, \beta) > 0$, so ist $(\alpha, \beta) = 1$ und $\gamma = \alpha - \beta \in R(L)$ eine Wurzel, deren Koeffizienten bzgl. S weder alle nichtnegativ noch alle nichtpositiv sind.
Es genügt also zu zeigen, dass ein Fundamentalsystem von Wurzeln existiert. Dies werden wir jetzt konstruieren:
Sei $t \in E$ so dass $(t, \alpha) \neq 0$ für alle $\alpha \in R(L)$. Solch ein t existiert, da die Menge

$$\{t \in E \mid \text{ es gibt ein } \alpha \in R(L) \text{ mit } (t, \alpha) = 0\}$$

als endliche Vereinigung von Hyperebenen nicht der gesamte Raum sein kann.
Sei $R_t^+ := \{\alpha \in R(L) \mid (t,\alpha) > 0\}$. Dann ist $R(L) = R_t^+ \cup -R_t^+$. Wir nennen ein Element $\alpha \in R_t^+$ zerlegbar, falls es $\beta, \gamma \in R_t^+$ gibt, mit $\alpha = \beta + \gamma$ und unzerlegbar sonst. Sei

$$S_t := \{\alpha \in R_t^+ \mid \alpha \text{ ist unzerlegbar } \}$$

Behauptung: S_t ist ein Fundamentalsystem von L. Dazu zeigen wir:

Lemma 1.13 *Jedes Element von R_t^+ ist eine Linearkombination von Elementen von S_t mit nichtnegativen ganzzahligen Koeffizienten.*

Beweis. Sonst gibt es ein $\alpha \in R_t^+$, das nicht diese Eigenschaft hat und Œwählen wir ein solches α mit (α, t) minimal. Dann ist α zerlegbar, da es sonst in S_t liegt. Also gibt es $\beta, \gamma \in R_t^+$ mit $\alpha = \beta + \gamma$. Dann ist $(t,\alpha) = (t,\beta) + (t,\gamma)$ und sowohl (t,β) als auch (t,γ) sind $< (t,\alpha)$. Also (wegen der Minimalität) sind β und γ nichtnegative Linearkombinationen von Elementen aus R_t^+, und damit auch α, ein Widerspruch. □

Lemma 1.14 *Für alle $\alpha \neq \beta \in S_t$ gilt $(\alpha, \beta) \leq 0$.*

Beweis. Sonst ist $(\alpha, \beta) = 1$ und somit $\gamma := \alpha - \beta \in R_t^+$ oder $-\gamma \in R_t^+$. Im ersten Fall ist $\alpha = \gamma + \beta$ zerlegbar und im zweiten Fall ist $\beta = \alpha + (-\gamma)$ zerlegbar. □

Lemma 1.15 *Die Elemente von S_t sind linear unabhängig.*

Beweis. Sei $\sum_{\alpha \in S} a_\alpha \alpha = 0$. Dann können wir diese Relation umschreiben als

$$\lambda := \sum b_\beta \beta = \sum c_\gamma \gamma$$

mit $b_\beta, c_\gamma > 0$ und alle β von allen γ verschieden sind. Es ist

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

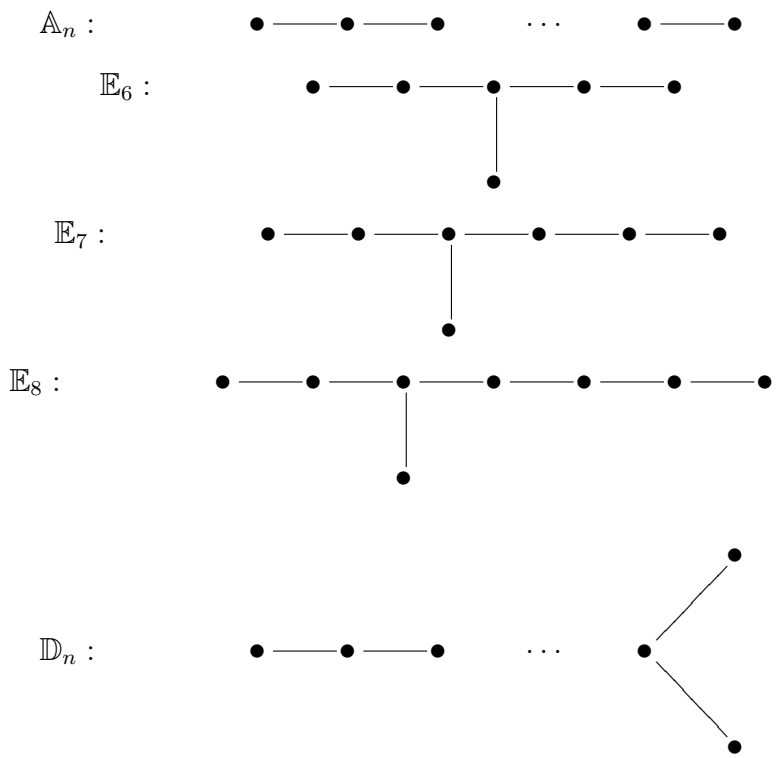
also $(\lambda, \lambda) = 0$ und somit $\lambda = 0$. Dann ist aber auch

$$(t, \lambda) = \sum b_\beta (t, \beta) = \sum c_\gamma (t, \gamma) = 0$$

also $b_\beta = c_\gamma = 0$ für alle β, γ. □

Dies beschließt den Beweis von Satz 1.12, denn nach Lemma 1.15 und Lemma 1.13 ist S_t ein Fundamentalsystem von Wurzeln und nach Lemma 1.14 auch eine Gitterbasis wie gefordert. □

Beispiel 1.16 *Die Grammatrix einer solchen Basis wird durch einen Graphen kodiert. Die Knoten entsprechen dabei den Basisvektoren. Zwei Knoten b_i, b_j sind durch eine Kante verbunden, genau dann wenn $(b_i, b_j) = -1$. Diese Graphen nennt man* Dynkin-Diagram.



Die zugehörigen Grammatrizen ergeben sich als

$$\mathcal{G}(\mathbb{A}_n) := \begin{pmatrix} 2 & -1 & 0 & \dots & \dots & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 \\ 0 & \dots & \dots & 0 & -1 & 2 \end{pmatrix}, \quad \mathcal{G}(\mathbb{D}_n) := \begin{pmatrix} 2 & -1 & 0 & \dots & \dots & 0 & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 & -1 \\ 0 & \dots & \dots & 0 & -1 & 2 & 0 \\ 0 & \dots & \dots & 0 & -1 & 0 & 2 \end{pmatrix}$$

$$\mathcal{G}(\mathbb{E}_6) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}, \quad \mathcal{G}(\mathbb{E}_7) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

$$\mathcal{G}(\mathbb{E}_8) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Es gilt $\det(\mathbb{E}_6) = 3$, $\det(\mathbb{E}_7) = 2$, $\det(\mathbb{E}_8) = 1$.
Ist $(e_1, \ldots, e_n)$ *eine Orthonormalbasis von* E, *so ist*

$$\mathbb{D}_n = \langle e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n, e_{n-1} + e_n \rangle_{\mathbb{Z}}.$$

Insbesondere ist $\det(\mathbb{D}_n) = 4$. *Weiter ist* $v := \frac{1}{2}(e_1 + \ldots + e_n) \in \mathbb{D}_n^{\#}$ *und* $e_1 \in \mathbb{D}_n^{\#}$. *Es gilt immer* $2e_1 \in \mathbb{D}_n$. *Es ist* $2v \in \mathbb{D}_n$ *genau dann, wenn* n *gerade ist. Dann ist* $\mathbb{D}_n^{\#}/\mathbb{D}_n \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, *ansonsten ist* $\mathbb{D}_n^{\#}/\mathbb{D}_n \cong \mathbb{Z}/4\mathbb{Z}$.
Für $\mathbb{A}_n$ *gilt:* $\det(\mathbb{A}_n) = n + 1$ *und* $\mathbb{A}_n^{\#}/\mathbb{A}_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$.
$\mathbb{A}_n$ *ist ein Teilgitter (kein volles Teilgitter) von* $\mathbb{Z}^{n+1}$: *Ist* $(e_1, \ldots, e_{n+1})$ *eine ON-Basis von* $\mathbb{R}^{n+1}$, *so ist* $(e_1 - e_2, e_2 - e_3, \ldots, e_n - e_{n+1})$ *eine Gitterbasis von* $\mathbb{A}_n$. *Das Gitter* $\mathbb{A}_n$ *erhält man als*

$$\mathbb{A}_n = \{\sum_{i=1}^{n+1} a_i e_i \in \mathbb{R}^{n+1} \mid a_i \in \mathbb{Z}, \sum a_i = 0\}$$

als $(e_1 + \ldots + e_{n+1})^{\perp}$ *in* $\mathbb{Z}^{n+1}$. *Der Vektor* $v := \frac{1}{n+1}(ne_1 - e_2 - \ldots - e_{n+1}) \in \mathbb{A}_n^{\#}$ *erfüllt* $(n+1)v \in \mathbb{A}_n$.

Gitter L	$\lvert R(L)\rvert$	$\det(L)$	$L^{\#}/L$	Dimension n
$\mathbb{A}_n$	$n(n+1)$	$n+1$	$\mathbb{Z}/(n+1)\mathbb{Z}$	≥ 1
$\mathbb{D}_n$	$2n(n-1)$	4	$\mathbb{Z}/4\mathbb{Z}$	≥ 4, ungerade
$\mathbb{D}_n$	$2n(n-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	≥ 4, gerade
$\mathbb{E}_6$	72	3	$\mathbb{Z}/3\mathbb{Z}$	6
$\mathbb{E}_7$	126	2	$\mathbb{Z}/2\mathbb{Z}$	7
$\mathbb{E}_8$	240	1	1	8

Ende am 16.10.08

Definition 1.17 *(i) Für zwei Gitter* L_1, L_2 *in* V_1 *bzw.* V_2 *bezeichnet* $L_1 \perp L_2$ *die (äussere)* orthogonale Summe . *Dies ist ein Gitter in* $V_1 \oplus V_2$ *der Dimension* $\dim(L_1) + \dim(L_2)$. *Sind* B *bzw.* C *Gitterbasen von* L_1 *bzw.* L_2, *so ist* $((b_1, 0), \ldots, (b_{n_1}, 0), (0, c_1), \ldots, (0, c_{n_2}))$ *eine Gitterbasis von* $L_1 \perp L_2$ *mit Grammatrix*

$$\begin{pmatrix} \mathcal{G}(B) & 0 \\ 0 & \mathcal{G}(C) \end{pmatrix}$$

(ii) Sind L_1, L_2 *Gitter in* V *und* $(\ell_1, \ell_2) = 0$ *für alle* $\ell_i \in L_i$, *so heißt* $L := L_1 \perp L_2 := \langle L_1, L_2 \rangle$ *die (innere)* orthogonale Summe.
(iii) Ein Gitter L *heißt* irreduzibel *oder auch* orthogonal unzerlegbar, *falls* L *nicht orthogonale Summe echter Teilgitter ist.*

Ohne Beweis möchte ich angeben:

Satz 1.18 *(vgl. Ebeling) Jedes Wurzelgitter ist orthogonale Summe von Wurzelgittern der Form* $\mathbb{A}_n$, $\mathbb{D}_m$ $(m \geq 4)$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$.

Satz 1.19 *(Kneser) Jedes Gitter lässt sich eindeutig schreiben als orthogonale Summe irreduzibler Gitter.*

Beweis. Dazu zunächst eine kleine Definition. Wir nennen einen Vektor $x \in L$ unzerlegbar, falls es keine $y, z \in L - \{0\}$ gibt mit $x = y + z$ und $(y, z) = 0$.
Dann gilt: Jeder Vektor $0 \neq x \in L$ ist Summe von unzerlegbaren Vektoren. Denn dies ist klar, wenn x unzerlegbar ist. Ist aber x nicht unzerlegbar, so ist $x = y + z$ mit $0 < (y, y) < (x, x)$ und $0 < (z, z) < (x, x)$. Ist einer der Summanden y oder z nicht unzerlegbar, so kann man ihn wiederum als Summe von Vektoren kleinerer Norm schreiben. Da $L_{<=(x,x)}$ endlich ist, terminiert dieses Verfahren nach endlich vielen Schritten.
Insbesondere wird L von unzerlegbaren Vektoren erzeugt.
Wir nennen zwei unzerlegbare Vektoren y, z verbunden, falls es unzerlegbare Vektoren $x_0 = y, x_1, \ldots, x_t = z$ in L gibt, mit $(x_i, x_{i+1}) \neq 0$ für alle i. Diese Äquivalenzrelation teilt die Menge der unzerlegbaren Vektoren in endlich viele Klassen $K_1, \ldots, K_s$.
Sei $L_i := \langle K_i \rangle_{\mathbb{Z}}$.
Dann ist $L = L_1 \perp \ldots \perp L_s$ eine Zerlegung in irreduzible Gitter und diese Zerlegung ist eindeutig. □

Mit dieser Definition liest sich also Satz 1.18 wie folgt: Jedes irreduzible Wurzelgitter ist von der Form $\mathbb{A}_n$, $\mathbb{D}_m$ $(m \geq 4)$, $\mathbb{E}_6$, $\mathbb{E}_7$ oder $\mathbb{E}_8$.

Wir kommen zu einigen interessanten und nützlichen Eigenschaften der Weyl-Gruppe $W(L)$ (siehe Bemerkung 1.20) eines irreduziblen Wurzelgitters.

Bemerkung 1.20 *Ist L ein ganzes Gitter und $\ell \in L$ mit $(\ell, \ell) = 2$, so ist die* Spiegelung σ_ℓ *entlang ℓ definiert durch*

$$v\sigma_\ell := v - 2\frac{(v, \ell)}{(\ell, \ell)}\ell = v - (v, \ell)\ell$$

für alle $v \in V$ eine orthogonale Abbildung die L festlässt, also $\sigma_\ell \in \mathrm{Aut}(L)$.
Ist L ein Wurzelgitter, so heißt

$$W(L) := \langle \sigma_\ell \mid \ell \in R(L) \rangle \leq \mathrm{Aut}(L)$$

die Weyl-Gruppe *von L. Da Konjugierte von Spiegelungen wieder Spiegelungen sind ($g^{-1}\sigma_\ell g = \sigma_{\ell g}$), ist die Weyl-Gruppe ein Normalteiler in $\mathrm{Aut}(L)$.*

Satz 1.21 *Sei L ein Wurzelgitter und $W(L)$ seine Weyl-Gruppe. Dann ist L irreduzibel, genau dann weinn $W(L)$* irreduzibel *auf $V := \mathbb{R}L$ operiert, d.h. jeder $W(L)$-invariante Teilraum $U \leq V$ ist entweder $\{0\}$ oder V.*

Beweis. $\Rightarrow$: Sei $\{0\} \neq U < V$ mit $Ug = U$ für alle $g \in W(L)$. Dann ist auch $U^\perp$ ein $W(L)$-invarianter Teilraum, da $W(L) \leq O(V)$ und $V = U \oplus U^\perp$. Sei $\alpha \in R(L)$. Wir wollen zeigen, dass entweder $\alpha \in U$ oder $\alpha \in U^\perp$ liegt. Das widerspricht dann der Irreduzibilität von L. Angenommen $\alpha \notin U$. Für $u \in U$ ist dann $u\sigma_\alpha = u - (u, \alpha)\alpha \in U$, da U invariant unter $W(L)$ ist. Also ist $(u, \alpha) = 0$ für alle $u \in U$ (da $\alpha \notin U$) und somit $\alpha \in U^\perp$.
$\Leftarrow$: Wir zeigen: Ist $L = L_1 \perp L_2$, so ist $U := \mathbb{R}L_1$ ein $W(L)$-invarianter Teilraum von V. Denn dann ist $R(L) = R(L_1) \cup R(L_2)$. Für $u \in U$ und $\alpha \in R(L_2)$ ist $u\sigma_\alpha = u \in U$ und für $\alpha \in R(L_1)$ ist $u\sigma_\alpha \in U$. □

Lemma 1.22 *Sei L ein irreduzibles Wurzelgitter. Dann operiert $W(L)$ transitiv auf $R(L)$, d.h. für je zwei Wurzeln $\alpha, \beta \in R(L)$ gibt es ein $g \in W(L)$ mit $\alpha g = \beta$.*

Beweis. Seien $\alpha, \beta \in R(L)$. Dann ist $U := \langle \alpha g \mid g \in W(L)\rangle_\mathbb{R}$ ein $W(L)$-invarianter Teilraum von $\mathbb{R}L = V$ und also nach Lemma 1.21 $U = V$. Die Bilder von α unter den Gruppenelementen erzeugen also den ganzen Raum. Daher gibt es ein $g \in W(L)$ mit $(\alpha g, \beta) \neq 0$. Indem wir α durch αg ersetzen, können wir annehmen, dass $(\alpha, \beta) \neq 0$. Ersetzt man α durch $-\alpha = \alpha\sigma_\alpha$, so kann man weiter annehmen, dass $(\alpha, \beta) > 0$ ist. Dann ist aber entweder $\alpha = \beta$ oder $(\alpha, \beta) = 1$ und $v := \alpha - \beta \in R(L)$. Im letzten Fall ist

$$\alpha\sigma_v = \alpha - (v, \alpha)v = \alpha - (\alpha - \beta) = \beta.$$

□

Ende am 17.10.2008

1.3 Reine Teilgitter.

Definition 1.23 *(i) Ein Gitter L heißt* gerade, *falls $(\ell, \ell) \in 2\mathbb{Z}$ für alle $\ell \in L$.*
(ii) Ein Gitter L heißt unimodular, *falls $L = L^\#$.*

Bemerkung 1.24 *(i) Ein gerades Gitter ist ganz.*
(ii) Ein ganzes Gitter ist gerade, genau dann wenn für alle Basisvektoren b_i in einer Gitterbasis gilt, dass $(b_i, b_i) \in 2\mathbb{Z}$.

Folgerung 1.25 *Wurzelgitter sind gerade Gitter.*
Das Gitter $\mathbb{E}_8$ ist ein gerades unimodulares Gitter.

Definition 1.26 *(i) Ist $L \leq M$ ein Teilgitter, so heißt*

$$L^{\perp,M} := L^\perp := \{m \in M \mid (\ell, m) = 0 \text{ für alle } \ell \in L\}$$

das Orthogonalgitter *von L in M.*
(ii) Ein Teilgitter $L \leq M$ heißt rein *, falls*

$$L = \{m \in M \mid m \in \langle L\rangle_\mathbb{R}\} = M \cap \mathbb{R}L.$$

Bemerkung 1.27 *Sei $L \leq M$ ein Teilgitter, $B = (b_1, \ldots, b_n)$ eine Gitterbasis von M, $C = (c_1, \ldots, c_k)$ eine Gitterbasis von L und $T = {}_C\mathrm{id}_B \in \mathbb{Z}^{k\times n}$ die Basiswechselmatrix. Dann ist L rein in $M \Leftrightarrow$ die Invariantenteiler von T sind alle gleich 1 $\Leftrightarrow M/L$ ist torsionsfrei $\Leftrightarrow C$ kann zu einer Gitterbasis von M ergänzt werden.*

Beweis. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gibt es eine Gitterbasis $B' = (b'_1, \ldots, b'_n)$ von M und Zahlen $d_1, \ldots, d_k \in \mathbb{Z}$ (die Invariantenteiler von T) so daß $C' = (d_1 b'_1, \ldots, d_k b'_k)$ eine Gitterbasis von L ist. Da $\mathbb{R}L \cap M$ aus der Menge aller ganzen Linearkombinationen der $(b'_1, \ldots, b'_k)$ besteht, gilt $\mathbb{R}L \cap M = L$ genau dann, wenn alle d_i gleich 1 sind. □

Satz 1.28 *Sei $V = U_1 \oplus U_2$, $\pi_i \in \mathrm{End}(V)$ die Projektionen auf U_i. Sei L ein volles Gitter in V, so dass $L_i := L \cap U_i$ ein volles Gitter in U_i ist ($i = 1, 2$). (dann ist $U_i = \mathbb{R}L_i$ und L_i ist reines Teilgitter in L.) Setze $L'_i := L\pi_i$. Dann ist $L_i \leq L'_i$ ($i = 1, 2$) und es gilt:*

$$L'_1/L_1 \cong L'_2/L_2 \cong L/(L_1 \oplus L_2) \cong L'_1 \oplus L'_2/L.$$

Beweis. Klar ist $L'_1/L_1 \cong L'_1 \oplus L_2/L_1 \oplus L_2 \cong L'_1 \oplus L'_2/L_1 \oplus L'_2$.
Wir betrachten zunächst die Projektion $\pi_1 : L \to L'_1$. Gefolgt vom natürlichen Epimorphismus $L'_1 \to L'_1/L_1$ liefert sie eine surjektive Abbildung $\overline{\pi_1} : L \to L'_1/L_1$. Sei

$$K_1 := \ker(\overline{\pi_1}) = \{\ell \in L \mid \ell\pi_1 \in L_1\}.$$

Für $\ell = x_1 + x_2 \in L$ mit $x_i \in U_i$ ist $\ell\pi_1 = x_1 \in L_1 = U_1 \cap L$ genau dann wenn $x_1 \in L$ und somit $x_2 = \ell - x_1 \in L \cap U_2 = L_2$ liegt. Also ist $K_1 = L_1 \oplus L_2$ und nach dem Homomorphiesatz gilt

$$L'_1/L_1 = \mathrm{Bild}(\overline{\pi_1}) \cong L/\ker(\overline{\pi_1}) = L/(L_1 \oplus L_2).$$

Ebenso erhält man $L'_2/L_2 \cong L/(L_1 \oplus L_2)$. Für die letzte Isomorphie zeigen wir, dass $L'_1 + L = L'_1 \oplus L'_2$. Denn dann ist nach dem Noetherschen Isomorphiesatz

$$(L'_1 \oplus L'_2)/L = (L'_1 + L)/L \cong L'_1/(L'_1 \cap L) = L'_1/L_1.$$

Nach Definition ist $L'_1 + L = \langle L'_1, L\rangle$. Es ist $x_1 \in L'_1$ genau dann wenn $x_1 \in U_1$ und es gibt ein $\ell \in L$, $x_2 \in U_2$ mit $\ell = x_1 + x_2$ (dann notwendigerweise $x_2 \in L'_2$). Also ist $L'_1 + L \subseteq L'_1 \oplus L'_2$. Umgekehrt liegt natürlich $L'_1 \subset L'_1 + L$ und obige Rechnung zeigt auch $L'_2 \subset L'_1 + L$ und damit $L'_1 + L = L'_1 \oplus L'_2$. □

Satz 1.29 *Sei M ein unimodulares Gitter und $L \leq M$ ein reines Teilgitter. Dann ist* $\det(L) = \det(L^\perp)$, *sogar $L^\# / L \cong (L^\perp)^\# / L^\perp$.*

Beweis. Wir wenden Satz 1.28 an auf $U_1 := \mathbb{R}L$, $U_2 = U_1^\perp = \mathbb{R}L^\perp$, $L_1 = L = U_1 \cap M$, $L_2 = L^\perp = U_2 \cap M$ und müssen nur noch zeigen, dass

$$L'_1 = M\pi_1 = L^\#,\ L'_2 = M\pi_2 = (L^\perp)^\#.$$

Ist nun $\ell \in L$ und $m \in M$, so ist $(\ell, m) = (\ell, m\pi_1) \in \mathbb{Z}$ und daher $M\pi_1 \subset L^\#$. Sei $(b_1, \ldots, b_k)$ eine Gitterbasis von L und ergänze diese zu Basis $B := (b_1, \ldots, b_k, b_{k+1}, \ldots, b_n)$ von M. Da $M = M^\#$ ist auch die duale Basis $B^* = (b_1^*, \ldots, b_k^*, b_{k+1}^*, \ldots, b_n^*)$ eine Gitterbasis von M. (Dabei ist $(b_{k+1}^*, \ldots, b_n^*)$ eine Gitterbasis von $L^\perp$.) Und $L^\# = \langle b_1^*\pi_1, \ldots, b_k^*\pi_1\rangle \subset M\pi_1$. □

Bemerkung 1.30 *Als Anwendung zeigen wir, dass* $\mathbb{A}_n^\#/\mathbb{A}_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$. *Setzt man* $L = \langle \ell := e_1 + \ldots + e_{n+1} \rangle \leq \mathbb{Z}^{n+1} = \langle e_1, \ldots, e_{n+1} \rangle_{\mathbb{Z}}$, *so ist* L *ein reines Teilgitter in dem Gitter* $M := \mathbb{Z}^{n+1}$ *mit* $\det(M) = 1$. *Weiter ist* $\mathbb{A}_n = L^\perp$. $\mathcal{G}(\ell) = (n+1) = ((\ell, \ell))$ *liefert* $L^\#/L \cong \mathbb{Z}/(n+1)\mathbb{Z}$, $L^\# = \langle \frac{1}{n+1}\ell \rangle$. *Mit Satz 1.29 findet man also auch* $\mathbb{A}_n^\#/\mathbb{A}_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$.

Als Übung konstruieren Sie $\mathbb{E}_7 = \langle b_7 \rangle^\perp$ und $\mathbb{E}_6 = \langle b_6, b_7 \rangle^\perp$ als Teilgitter von $\mathbb{E}_8$ und folgern so aus $\det(E_8) = 1$, dass $\det(\mathbb{E}_7) = 2$ und $\det(\mathbb{E}_6) = 3$. $\mathbb{E}_8$ kann man z.B. als Teilgitter von $\mathbb{A}_8^\# = \langle v, \mathbb{A}_8 \rangle$ erhalten, $\mathbb{E}_8 = \langle \mathbb{A}_8, 3v \rangle$.

2 Codes.

2.1 Lineare Codes.

Definition 2.1 *(i) Ein* linearer Code C *über* $\mathbb{F}_q$ *der Länge* n *ist ein linearer Teilraum* $C \leq \mathbb{F}_q^n$.
(ii) Auf $\mathbb{F}_q^n$ *definieren wir die nicht ausgeartete symmetrische Bilinearform* $x \cdot y := \sum_{i=1}^n x_i y_i$. *Dann ist für einen Code* $C \leq \mathbb{F}_q^n$ *der* duale Code *definiert als der Orthogonalraum* $C^\perp$ *von* C,

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ für alle } c \in C\}.$$

(iii) C *heißt* selbstdual , *falls* $C = C^\perp$ *und* selbstorthogonal , *falls* $C \subseteq C^\perp$.

Bemerkung 2.2 *Sei* $C \leq \mathbb{F}_q^n$ *ein Code der Dimension* k *und* $B = (b_1, \ldots, b_k)$ *eine Basis von* C, $H = (h_1, \ldots, h_{n-k})$ *eine Basis von* $C^\perp$. *Dann hat* C *zwei verschiedene Beschreibungen:*
(i) Die Matrix $G \in \mathbb{F}_q^{k \times n}$, *deren Zeilen genau die Zeilenvektoren* b_i *sind, nennt man eine* Erzeugermatrix *von* C. *Interpretiert man* G *als Matrix einer linearen Abbildung* $\mathrm{cod} : \mathbb{F}_q^k \to \mathbb{F}_q^n, x \mapsto xG$, *so ist* C *genau das Bild von* cod. *Diese Beschreibung eignet sich sehr gut zum* Codieren *der* q^k *Informationsworte.*
(ii) Die Matrix $P \in \mathbb{F}_q^{n \times (n-k)}$, *deren Spalten genau die Zeilenvektoren* h_i *sind, nennt man eine* Prüfmatrix *von* C. *Interpretiert man* P *als Matrix einer linearen Abbildung* $\mathrm{decod} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}, x \mapsto xP$, *so ist* C *genau der Kern von* decod. *Diese Beschreibung eignet sich sehr gut zum Testen, ob ein empfangenes Wort zum Code gehört.*
(iii) Ist P *eine Prüfmatrix für* C *und* $x \in \mathbb{F}_q^n$ *so nennt man* $xP \in \mathbb{F}_q^{n-k}$ *das* Syndrom *von* x *(unter* H*). Es ist* $x \in C$ *genau dann wenn sein Syndrom gleich 0 ist.*

Definition 2.3 *(i) Auf* $\mathbb{F}_q^n$ *definiert der* Hamming-Abstand

$$d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{Z}, d(x,y) := |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|$$

eine Metrik, *d.h. für alle* $x, y, z \in \mathbb{F}_q^n$ *gilt*
$d(x,y) \geq 0$ *und* $d(x,y) = 0 \Leftrightarrow x = y$,
$d(x,y) = d(y,x)$,
$d(x,y) + d(y,z) \geq d(x,z)$.
(ii) Das Gewicht *eines Wortes* $x \in \mathbb{F}_q^n$ *ist* $w(x) := d(x,0) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|$.
(iii) Das Minimalgewicht $d(C)$ *eines Codes* C *ist* $d(C) := \min\{w(c) \mid 0 \neq c \in C\}$.

Bemerkung.
(a) Es ist $d(C) = \min\{d(x,y) \mid x \neq y \in C\}$.
(b) Für $x, y, z \in \mathbb{F}_q^n$ ist $d(x+z, y+z) = d(x,y)$ (Translationsinvarianz der Metrik).
(c) Ein Code $C \leq \mathbb{F}_q^n$ der Dimension k und Minimalabstand $d = d(C)$ heißt $[n,k,d]_q$ Code. Ein Ziel der Codierungstheorie ist es, gute Codes zu finden, das sind Codes mit grossem Minimalabstand d, grosser Dimension k und kleiner Länge n.

Bemerkung 2.4 *Interpretiert man ein Codewort als lineare Abhängigkeit der Zeilen der Prüfmatrix, so sieht man, dass das Minimalgewicht des Codes $d(C)$ gleich der minmalen Anzahl linear abhängiger Zeilen einer jeden Prüfmatrix von C ist.*

Definition 2.5 *Sei $C \subseteq \mathbb{F}_q^n$ ein Code. Ein* minimal distance decoder *MDD ist eine Funktion $f : \mathbb{F}_q^n \to C$ mit*

$$d(f(a), a) = \min\{d(c,a) \mid c \in C\} \text{ für alle } a \in \mathbb{F}_q^n.$$

Bemerkung 2.6 *Sei $C \subseteq \mathbb{F}_q^n$ ein Code, $d := d(C)$, f ein MDD für C.*
(i) Ist $e < \frac{d}{2}$ und $v \in \mathbb{F}_q^n$ so gibt es höchstens ein Codewort $c \in C$ mit $d(v,c) \leq e$. Für jeden MDD f gilt also $f(v) = c$. (Der MDD kann e Übertragungsfehler korrigieren.)
(ii) Ist $e < d$ und $v \in \mathbb{F}_q^n$ für das es ein $c \in C$ gibt mit $d(v,c) = e$, so ist $v \notin C$. (Der MDD erkennt, daß die Übertragung fehlerhaft ist (decodiert aber nicht notwendig zum richtigen Codewort).)

Bemerkung 2.7 *Sei $C \leq \mathbb{F}_q^n$ ein linearer Code und $P \in \mathbb{F}_q^{n \times (n-k)}$ eine Prüfmatrix für C und $S := \{xP \mid x \in \mathbb{F}_q^n\} = \text{Bild}(P)$ die Menge der Syndrome von P.*
Dann gilt $\mathbb{F}_q^n = \dot{\cup}_{s \in S} V_s$ mit $V_s = (\{s\})P^{-1} = \{x \in \mathbb{F}_q^n \mid xP = s\}$.
Für $s \in S$ heißt $a_s \in V_s = a_s + C$ ein minimaler Vertreter, *falls $w(a_s) = \min\{w(x) \mid x \in V_s\}$. Wählt man für jedes $s \in S$ einen minimalen Vertreter a_s, so ist die Funktion $f : \mathbb{F}_q^n \to C$ definiert durch $f(a) := a - a_s$, falls $aP = s$ ist, ein MDD für C.*

Beispiel: $C \leq \mathbb{F}_5^5$ habe Erzeugermatrix

$$G := \begin{pmatrix} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 4 & 1 \end{pmatrix}$$

Dann ist

$$P := \begin{pmatrix} -2 & -3 \\ -1 & -1 \\ -4 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} =: \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

eine Prüfmatrix für C. P enthält keine Nullzeile, jedoch gilt $x_1 + 2x_3 = 0$, d.h. es gibt 2 l.a. Zeilen in P. Daher ist $(1,0,2,0,0) \in C$ und $d(C) = 2$. Zum MDD: Die Menge der Syndrome ist

$$S = \mathbb{F}_5^2 = \{(0,0)\} \cup \{as \mid s \in \{(1,0),(0,1),(1,1),(1,2),(1,3),(1,4)\}, a \in \mathbb{F}_5^*\}$$

Minimale Vertreter $v_{as} = av_s$ in V_{as} sind z.B. gegeben durch $v_{1,0} = (0,0,0,1,0), v_{0,1} = (0,0,0,0,1), v_{1,1} = (0,4,0,0,0), v_{1,2} = (0,0,0,1,2), v_{1,3} = (0,0,0,1,3), v_{1,4} = (0,0,1,0,0)$.

Definition 2.8 *Zwei Codes $C, C' \leq \mathbb{F}_q^n$ heißen* äquivalent, *falls es eine Umordnung σ von $\{1, \ldots, n\}$ gibt sowie $a := (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$, mit*

$$C' = C(\sigma, a) := \{(a_1 c_{\sigma(1)}, a_2 c_{\sigma(2)}, \ldots, a_n c_{\sigma(n)}) \mid (c_1, \ldots, c_n) \in C\}.$$

Sie heißen permutationsäquivalent *falls*

$$C' = C\sigma := \{(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)}) \mid (c_1, \ldots, c_n) \in C\}$$

für ein $\sigma \in S_n$. $\mathrm{Aut}(C) := \{\sigma \in S_n \mid C\sigma = C\}$ heißt die Automorphismengruppe *von C.*

Beachten Sie: Permutationsäquivalenz erhält Orthogonalität, Äquivalenz jedoch i.a. nicht. Es ist

$$C(\sigma, a)^\perp = C^\perp(\sigma, a^{-1}).$$

2.2 Hamming Codes.

Definition 2.9 *Sei $n = \frac{q^r - 1}{q - 1}$ für ein $r \in \mathbb{N}$. Sei $P \in \mathbb{F}_q^{n \times r}$ eine Matrix, in deren Zeilen gerade alle Erzeuger x_i aller eindimensionalen Teilräume von $\mathbb{F}_q^r$ stehen:*

$$P = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Jeder Code C mit Prüfmatrix P heißt Hamming Code *der Länge n, $C = H(\mathbb{F}_q, r)$.*

Bemerkung 2.10 *$H(\mathbb{F}_q, r)$ ist bis auf Äquivalenz eindeutig bestimmt, also unabhängig von der Wahl der n Erzeuger der 1-dimensionalen Teilräume von $\mathbb{F}_q^r$ und deren Reihenfolge. $d(H(\mathbb{F}_q, r)) = 3$.*

Beweis. Je 2 Zeilen der Prüfmatrix von $H(\mathbb{F}_q, r)$ sind linear unabhängig. □

Beispiel: $q = r = 2 \Rightarrow n = 3$ und

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Der Hamming-Code hat Dimension 1 und Erzeugermatrix $G = (1, 1, 1)$.
$r = 3 \Rightarrow n = 7$ und

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Der Hamming Code hat Dimension 4 = 7-3 und Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Definition 2.11 *Ein Code $C \leq \mathbb{F}_q^n$ heißt* perfekt, *falls es eine Zahl e gibt, so daß zu jedem $a \in \mathbb{F}_q^n$ genau ein $c \in C$ existiert mit $d(a,c) \leq e$.*

Beispiel: (i) $C = \mathbb{F}_q^n$ ist ein perfekter Code mit $e = 0$.
(ii) Ist $A = \mathbb{F}_2$ und n ungerade, so ist der Wiederholungscode $C = \{(0,\ldots,0),(1,\ldots,1)\}$ ein perfekter Code mit $e = \frac{n-1}{2}$.
(iii) Der Hamming Code $H(\mathbb{F}_2, 3)$ ist ein perfekter Code mit $e = 1$.

Satz 2.12 *Hamming Codes sind perfekte Codes mit $e = 1$.*

Beweis. Sei C der Hamming Code der Länge $n = q^r - 1$ mit Prüfmatrix P und $a \in \mathbb{F}_q^n$. Dann gilt entweder $aP = 0$ oder $aP = \alpha x_i = \alpha e_i P$ ist ein Vektor $\neq 0$ in $\mathbb{F}_q^r$ und damit gleich dem Vielfachen einer Zeile (der i-ten) von P. D.h. entweder $a \in C$, oder $a - \alpha e_i \in C$. Da $d(a - \alpha e_i, a) = w(\alpha e_i) = 1$ ist, gibt es also zu jedem $a \in \mathbb{F}_q^n$ ein $c \in C$ mit $d(a,c) \leq 1$. Die Eindeutigkeit eines solchen c folgt, da $d(C) = 3$ ist. □

Ende am 24.10.

2.3 Von Codes zu Gittern.

Definition 2.13 *Sei p eine Primzahl und $C \leq \mathbb{F}_p^n$ ein Code. Sei $(e_1,\ldots,e_n)$ eine Orthogonalbasis von $(\mathbb{R}^n,(,))$ mit $(e_i,e_i) = \frac{1}{p}$ und $M := \langle e_1,\ldots,e_n\rangle_{\mathbb{Z}}$. Dann ist $\pi : M \to \mathbb{F}_p^n, e_i \mapsto (0,\ldots,0,1,0,\ldots,0)$ ein Epimorphismus mit Kern $\ker(\pi) = pM$. Dann heißt $L_C := \pi^{-1}(C) \leq M$ das* Codegitter *zu C.*

Bemerkung 2.14 *(i) $pM = M^{\#} \leq L_C \leq M$.*
(ii) $L_C^{\#} = L_{C^\perp}$. Insbesondere ist L_C ganz genau dann wenn $C \subset C^\perp$ (also C ein selbstorthogonaler Code ist) und L_C unimodular genau dann, wenn $C = C^\perp$ (ein selbstdualer Code).
(iii) L_C ist gerade, genau dann wenn $p = 2$ und C ein sogenannter doppelt-gerader Code *ist, d.h. $w(c) \in 4\mathbb{Z}$ für alle $c \in C$.*

Beweis. Nur (ii) bedarf eines Beweises. Es ist $L_C/pM \cong C$, insbesondere ist $\det(L_C) = p^{n-2k}$, falls $k = \dim(C)$. Da $\dim(C^\perp) = n - k$ ist, gilt $\det(L_{C^\perp}) = p^{n-2(n-k)} = p^{2k-n} = \det(L_C^{\#})$. Es genügt also zu zeigen, dass $L_{C^\perp} \subset L_C^{\#}$. Klar ist $pM = M^{\#} \subset L_C^{\#}$. Sei $c = (c_1,\ldots,c_n) \in C^\perp$ und $\ell = \sum_{i=1}^n a_i e_i \in L_C$. Dann ist $(a_1 + p\mathbb{Z},\ldots,a_n + p\mathbb{Z}) \in C$ und daher $\sum a_i c_i \equiv_p 0$. Also ist auch $(\sum c_i e_i, \sum a_i e_i) = \frac{1}{p}\sum a_i c_i \in \mathbb{Z}$. □

Bemerkung 2.15 *Definiert man das* Minimum *eines Gitters L als*

$$\min(L) := \min\{(\ell, \ell) \mid 0 \neq \ell \in L\}$$

so gilt für einen Code $C \leq \mathbb{F}_p^n$

$$\min(L_C) \geq \min\{p, \frac{1}{p}d(C)\}$$

mit "=", falls $p = 2$ oder $p = 3$ ist. Es gilt immer $pe_1 \in L_C$ ein Vektor der Quadratlänge p.

Die Konstruktion des Codegitters L_C aus dem Code $C \leq \mathbb{F}_p^n$ nennt man auch manchmal Konstruktion A .

Beispiel 2.16 *Der erweiterte Hamming-Code e_8 und $\mathbb{E}_8$.*
Für einen Code $C \leq \mathbb{F}_q^n$ definiert man den erweiterten Code *$\tilde{C} \leq \mathbb{F}_q^{n+1}$ als*

$$\tilde{C} = \{(c_1, \ldots, c_n, -\sum_{i=1}^{n} c_i) \mid c = (c_1, \ldots, c_n) \in C\}.$$

Dann ist $\dim(C) = \dim(\tilde{C})$.
Ist $C = H(\mathbb{F}_2, 3)$ mit Erzeugermatrix G wie oben, so hat $\tilde{C} =: e_8 \leq \mathbb{F}_2^8$ die Erzeugermatrix

$$\tilde{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Es gilt $\tilde{C} = \tilde{C}^{\perp}$. Also ist $L_{\tilde{C}}$ ein unimodulares Gitter. Es gilt $L_{\tilde{C}} \cong \mathbb{E}_8$.

Bitte beachten Sie: Jeder Code $C \leq \mathbb{F}_p^n$ definiert ein Codegitter $L_C \leq \mathbb{R}^n$. Umgekehrt liefert aber nicht jedes Gitter einen Code und manche Gitter liefern auch mehrere Codes. Der genaue Zusammenhang ist wie folgt.

Bemerkung 2.17 *Sei L ein Gitter in $\mathbb{R}^n$ und $B := (b_1, \ldots, b_n)$ ein p-frame von L, das ist eine Orthogonalbasis mit $b_i \in L$ und $(b_i, b_i) = p$ für alle i, so dass*

$$X := \langle b_1, \ldots, b_n \rangle_{\mathbb{Z}} \leq L \leq \langle \frac{1}{p}b_1, \ldots, \frac{1}{p}b_n \rangle_{\mathbb{Z}} = \frac{1}{p}X.$$

Dann ist $\frac{1}{p}X/X \cong \mathbb{F}_p^n$ und

$$L/X = \{(a_1 \pmod p, \ldots, a_n \pmod p) \mid \frac{1}{p}\sum_{i=1}^{n} a_i b_i \in L\}$$

ein Code $C \leq \mathbb{F}_p^n$ mit $L_C = L$.
Die Codes $C \leq \mathbb{F}_p^n$ mit $L_C = L$ stehen also in Bijektion zu den $\mathrm{Aut}(L)$-Bahnen auf der Menge der p-frames B in L. Insbesondere ist das Gitter L genau dann ein Codegitter für einen Code $C \leq \mathbb{F}_p^n$, wenn ein p-frame in L existiert.

2.4 Wurzelgitter als Codegitter.

In diesem Abschnitt wollen wir sehen, welche Wurzelgitter von der Form L_C für einen Code $C \leq \mathbb{F}_p^n$ sind. Da Wurzelgitter gerade Gitter sind, ist notwendigerweise $p = 2$ und C ein doppelt gerader Code.

Satz 2.18 *Sei L ein irreduzibles Wurzelgitter der Dimension n. Dann sind äquivalent:*
(a) $L = L_C$ für einen Code $C \leq \mathbb{F}_p^n$.
(b) $L = L_C$ für einen doppelt geraden Code $C \leq \mathbb{F}_2^n$.
(c) L enthält n paarweise orthogonale Wurzeln, d.h. ein Teilgitter isometrisch zu $\mathbb{A}_1^n := \mathbb{A}_1 \perp \ldots \perp \mathbb{A}_1$.
(d) $-1 \in W(L)$.
(e) $2L^\# \subset L$.
(f) $L \cong \mathbb{A}_1$, $\mathbb{D}_n$ mit $n \geq 4$ gerade, $\mathbb{E}_7$ oder $\mathbb{E}_8$.

Beweis. (a) $\Leftrightarrow$ (b) haben wir in Bemerkung 2.17 gesehen.
(b) $\Rightarrow$ (c) klar aus Konstruktion von L_C.
(c) $\Rightarrow$ (d): Sind $\alpha_1, \ldots, \alpha_n$ die paarweise orthogonalen Wurzeln, so gilt für

$$g := \sigma_{\alpha_1} \ldots \sigma_{\alpha_n}$$

dass $\alpha_i g = -\alpha_i$ ist $(1 \leq i \leq n)$. Da $(\alpha_1, \ldots, \alpha_n)$ eine $\mathbb{R}$-Basis von $\mathbb{R}L$ ist folgt daraus $g = -1 \in W(L)$.
(d) $\Rightarrow$ (e): Sei $x \in L^\#$ und $\alpha \in R(L)$. Dann ist $(x, \alpha) \in \mathbb{Z}$ und daher

$$x\sigma_\alpha = x - (x, \alpha)\alpha \in x + L$$

d.h. $x - x\sigma_\alpha \in L$. Daher folgt für beliebiges $g \in W(L)$, dass $x - xg \in L$. Insbesondere gilt dies für $g = -1 \in W(L)$ und somit ist $x - (-x) = 2x \in L$. Da $x \in L^\#$ beliebig war, folgt daraus $2L^\# \subset L$.
(e) $\Rightarrow$ (f): Folgt aus Satz 1.18.
(f) $\Rightarrow$ (b): Durch explizite Angabe eines Codes C:
$\mathbb{A}_1$: $C = \{0\} \leq \mathbb{F}_2^1$.
$\mathbb{D}_n$ $(n \geq 4)$, gerade: Setze

$$C' := \{(c_1, \ldots, c_{n/2}) \mid \sum c_i = 0\} \leq \mathbb{F}_2^{n/2}$$

und

$$C := \{(c_1, c_1, c_2, c_2, \ldots, c_{n/2}, c_{n/2}) \mid (c_1, \ldots, c_{n/2}) \in C'\}.$$

Eine Basis mit Grammatrix wie in Abschnitt 1.2 erhält man z.B. als Zeilen der Matrix

$$\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots \\
1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & \ldots \\
-2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & -1 & 1 & 1 & 1 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & 1 & -1 & 1 & 1 & \ldots \\
0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & \ldots \\
\vdots & & & & & \vdots & & &
\end{array}$$

$\mathbb{E}_7$: $C = H(\mathbb{F}_2, 3)^{\perp}$.
$\mathbb{E}_8$: $C = e_8 = H(\mathbb{F}_2, 3)$. □

3 Zyklische Codes

3.1 Zyklische Codes.

Im gesamten Abschnitt bezeichnet $q := p^f$ eine Potenz einer Primzahl p und $\mathbb{F}_q$ den Körper mit q Elementen.

Definition 3.1 *Ein linearer Code $C \leq \mathbb{F}_q^N$ heißt* zyklisch, *falls*

$$(c_1, \ldots, c_N) \in C \Rightarrow (c_N, c_1, c_2, \ldots, c_{N-1}) \in C$$

Satz 3.2 *(i) Die Abbildung $\varphi : \mathbb{F}_q^N \to \mathbb{F}_q[x]/(x^N - 1)$ definiert durch $(a_1, \ldots, a_N) \mapsto a_1[x]_{(x^N-1)}^{N-1} + a_2[x]_{(x^N-1)}^{N-2} \ldots + a_{N-1}[x]_{(x^N-1)} + a_N$ definiert einen $\mathbb{F}_q$-Vektorraum Isomorphismus.*
(ii) $C \leq \mathbb{F}_q^N$ ist ein zyklischer Code, genau dann wenn $\varphi(C) \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ ein Ideal ist.

Beweis. (i) Nachrechnen: Zu zeigen ist, daß die Abbildung $\mathbb{F}_q$-linear und bijektiv ist.
(ii) Es ist $[x]_{(x^N-1)}(a_N + a_{N-1}[x]_{(x^N-1)} + \ldots + a_1[x]_{(x^N-1)}^{N-1})$
$= a_N[x]_{(x^N-1)} + a_{N-1}[x]_{(x^N-1)}^2 + \ldots + a_1[x]_{(x^N-1)}^N$
$= a_N[x]_{(x^N-1)} + a_{N-1}[x]_{(x^N-1)}^2 + \ldots + a_1 \cdot 1$
$= a_1 + a_N[x]_{(x^N-1)} + a_{N-1}[x]_{(x^N-1)}^2 + \ldots + a_2[x]_{(x^N-1)}^{N-1}$.
$\varphi(C)$ ist immer ein $\mathbb{F}_q$-Teilvektorraum von $\mathbb{F}_q[x]/(x^N - 1)$. Damit $\varphi(C)$ ein Ideal ist, muß zusätzlich noch $[x]_{(x^N-1)}\varphi(c) \in \varphi(C)$ sein für alle $c \in C$. Dies ist nach obiger Rechnung aber genau die Bedingung dafür, daß C ein zyklischer Code ist. □

Im folgenden werden wir stets voraussetzen, daß N nicht durch p teilbar ist. Dann gilt:

$$\mathrm{ggT}(x^N - 1, \frac{d}{dx}(x^N - 1)) = \mathrm{ggT}(x^N - 1, Nx^{N-1}) = \mathrm{ggT}(x^N - 1, x^{N-1}) = 1$$

da $x \cdot x^{N-1} - (x^N - 1) = 1$ ist. D.h. das Polynom $x^N - 1$ hat keine mehrfachen Nullstellen und läßt sich eindeutig schreiben als Produkt

$$x^N - 1 = f_1(x) \cdot \ldots \cdot f_t(x)$$

mit $f_1, \ldots, f_t \in \mathbb{F}_q[x]$ normiert, irreduzibel und paarweise verschieden.

Beispiel
$N = 15$, $q = 2$:

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \in \mathbb{F}_2[x].$$

$N = 6,\ q = 3$:

$$x^6 - 1 = (x-1)^3(x+1)^3 \in \mathbb{F}_3[x].$$

$N = 4,\ q = 3$:

$$x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{F}_3[x].$$

Diese Faktorisierungen kann man z.B. mit MAPLE berechnen mit dem Befehl

$$\text{Factor}(x^4 - 1) \bmod 3$$

Die Ideale in $\mathbb{F}_q[x]/(x^N-1)$ sind dann genau die Hauptideale $(f_{i_1\ldots i_s})$ wo $f_{i_1\ldots i_s} := [f_{i_1}(x) \cdot \ldots \cdot f_{i_s}(x)]_{(x^N-1)}$ für $s \le t$ und $1 \le i_1 < i_2 < \ldots < i_s \le t$. Der Ring hat also genau 2^t Ideale.

Sei $g := f_{i_1} \cdot \ldots \cdot f_{i_s}$ und $d := \text{Grad}(g)$. Dann ist $([g]) = \{[a][g] \mid [a] \in \mathbb{F}_q[x]/(x^N-1)\}$. Jedes Element $[a][g] \in ([g])$ läßt sich schreiben als $[b][g]$ mit $\text{Grad}(b) \le N-d-1$. Dazu sei $h \in \mathbb{F}_q[x]$ mit $gh = x^N - 1$. Dann ist $\text{Grad}(h) = N-d$. Polynomdivision mit Rest liefert $a = a_1 h + b$ mit einem Rest b vom Grad $\le N-d-1$. In $\mathbb{F}_q[x]/(x^N-1)$ gilt dann $[a][g] = [a_1 h + b][g] = [b][g]$, da $[h][g] = 0$ ist. Also ist $([g], [x][g], \ldots, [x]^{N-d-1}[g])$. eine Basis von $([g]) \trianglelefteq \mathbb{F}_q[x]/(x^N-1)$ und $\dim([g]) = N-d$.

Beispiel
$N = 4,\ q = 3$:

$$x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{F}_3[x].$$

$I_{123} = ([(x-1)(x+1)(x^2+1)]) = (0)$,
$I_{12} = (f_{12}) = ([(x-1)(x+1)]) = ([x]^2 - 1)$ hat Dimension 2 und $\mathbb{F}_3$-Basis $(f_{12}, [x]f_{12})$. Denn es ist
$I_{12} = \{(a_0 + a_1[x] + a_2[x]^2 + a_3[x]^3)([x]^2-1) \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_3\} = \{a_0([x]^2-1) + a_1[x]([x]^2-1) + a_2[x]^2([x]^2-1) + a_3[x]^3([x]^2-1) \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_3\}$. Nun ist $[x]^2([x]^2-1) = [x]^4 - [x]^2 = 1 - [x]^2$ und $[x]^3([x]^2-1) = -[x]([x]^2-1)$. Daher ist $I_{12} = \{(a_0 + a_1[x])([x]^2-1) \mid a_0, a_1 \in \mathbb{F}_3\}$.
Der I_{12} entsprechende Code C_{12} hat die Erzeugermatrix

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

Shiftet man die 2. Zeile dieser Matrix noch einmal nach rechts, so erhält man das negative der ersten Zeile.

Die Ergebnisse fassen wir in dem folgenden Satz zusammen:

Satz 3.3 *Sei N nicht durch p teilbar, und $x^N - 1 = f_1(x) \cdot \ldots \cdot f_t(x)$ mit paarweise verschiedenen, normierten, irreduziblen Polynomen $f_1, \ldots, f_t \in \mathbb{F}_q[x]$.*
(i) Setzt man $f_{i_1\ldots i_s} := [f_{i_1}(x) \cdot \ldots \cdot f_{i_s}(x)]_{(x^N-1)}$ für $s \le t$ und $1 \le i_1 < i_2 < \ldots < i_s \le t$ so sind die Hauptideale $(f_{i_1\ldots i_s})$ genau die Ideale von $\mathbb{F}_p[x]/(x^N-1)$. Der Ring hat also genau 2^t Ideale. Ist $d_i := \text{Grad}(f_i)$ der Grad des irreduziblen Faktors f_i ($d_1 + \ldots + d_t = N$), so gilt

$$\dim([f_{i_1}(x) \cdot \ldots \cdot f_{i_s}(x)]) = N - (d_{i_1} + \ldots + d_{i_s}).$$

(ii) Das Polynom $g := f_{i_1} \cdot \ldots \cdot f_{i_s}$ heißt Erzeugerpolynom *des zyklischen Codes $C_g :=$*

$\varphi^{-1}((f_{i_1\dots i_s}))$. *Ist* $[g] = \sum_{j=0}^{N-k} g_j[x]^j$, *so ist*

$$G_g := \begin{pmatrix} g_{N-k} & g_{N-k-1} & \dots & g_0 & 0 & 0 & \dots & 0 \\ 0 & g_{N-k} & \dots & g_1 & g_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_{N-k} & g_{N-k-1} & \dots & \dots & g_0 \end{pmatrix} \in \mathbb{F}_q^{k\times N}$$

eine Erzeugermatrix von C_g *und* $k = \dim(C_g) = N - Grad(g)$.
(iii) Ist g *wie in (ii) ein Erzeugerpolynom des zyklischen Codes* C_g, *so heißt das Polynom* $h \in \mathbb{F}_q[x]$ *mit* $gh = x^N - 1$ *ein* Prüfpolynom *von* C_g. *Es gilt* $\mathrm{Grad}(h) + \mathrm{Grad}(g) = N$. *Weiter liegt* $a \in \mathbb{F}_q[x]/(x^N-1)$ *genau dann in* C_g, *falls* $a[h] = 0$ *ist.*
(iv) Sei h *wie in (iii) ein Prüfpolynom von* C_g. *Ist* $[h] = \sum_{j=0}^{k} h_j[x]^j$, *so ist die Matrix*

$$G'_h := \begin{pmatrix} h_0 & h_1 & \dots & h_k & 0 & 0 & \dots & 0 \\ 0 & h_0 & \dots & h_{k-1} & h_k & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & h_0 & h_1 & \dots & \dots & h_k \end{pmatrix} \in \mathbb{F}_q^{(N-k)\times N}$$

eine Erzeugermatrix von $C_g^\perp$ *und daher* $(G'_h)^{tr}$ *eine Prüfmatrix von* C_g. *Sei* $\hat{g} = x^{N-\mathrm{Grad}(g)}h(x^{-1})$. *Dann ist* $C_g^\perp = C_{\hat{g}}$.

Beweis. (ii) Eine $\mathbb{F}_q$-Basis von C_g ist $[x]^{k-1}[g], [x]^{k-2}[g], \dots, [x][g], [g]$, diese Elemente entsprechen genau den Zeilen der Erzeugermatrix.
(iii) Klar ist $\mathrm{Grad}(h) + \mathrm{Grad}(g) = \mathrm{Grad}(hg) = N$. Außerdem gilt für $a \in \mathbb{F}_q[x]$:

$$[a]_{(x^N-1)}[h]_{(x^N-1)} = 0 \Leftrightarrow (x^N-1) \text{ teilt } ah \Leftrightarrow gh \text{ teilt } ah \Leftrightarrow g \text{ teilt } a \Leftrightarrow [a] \in ([g]) = C_g$$

(iv) $x^N - 1 = gh = (\sum_{j=0}^{N-k} g_j x^j)(\sum_{i=0}^{k} h_i x^i) = \sum_{l=0}^{N}(\sum_{j=0}^{l} g_j h_{l-j})x^l$. Durch Koeffizientenvergleich folgt für $0 < l < N$, daß $\sum_{j=0}^{l} g_j h_{l-j} = 0$. Setzt man nämlich $g_i = 0$ falls $i \notin \{0, \dots, N-k\}$ und $h_i = 0$ falls $i \notin \{0, \dots, k\}$ so ist das Produkt der j-ten Zeile von G_g mit der i-ten Spalte von $(G'_h)^{tr}$ gleich

$$\sum_{l=1}^{N} g_{N-k+i-l}h_{l-j}$$

also der Koeffizient von $x^{N-k+i-j}$ in $gh = x^N - 1$. Da $1 \le i \le k$ und $1 \le j \le N-k$ ist, ist $1 \le N-k+i-j \le N-1$, also ist dieser Koeffizient gleich 0. Damit stehen die Zeilen von G'_h senkrecht auf denen von G_g. Aus Dimensionsgründen erzeugt also G'_h daher $C_g^\perp$. □

Beispiel 3.4 $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1) \in \mathbb{F}_2[x]$. *Sei* $g := x^3+x+1$. *Dann hat der zyklische Code* $C_g = ([g]) \trianglelefteq \mathbb{F}_2[x]/(x^7-1)$ *Länge 7, Dimension 4 und Erzeugermatrix*

$$G_g := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Da $h = (x+1)(x^3+x^2+1) = x^4+x^2+x+1$ *findet man eine Erzeugermatrix von* $C_g^\perp$ *als*

$$G'_h := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Man kann zeigen, daß $C_g = H(\mathbb{F}_2, 3)$ *ein Hamming Code ist.*

3.2 Ein Codierer für zyklische Codes

Sei $C \leq \mathbb{F}_q^N$ ein Code der Dimension k mit Erzeugermatrix $G := (I_k, P_{N-k})$. Codierung besteht dann darin, einem Informationswort $u := (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ ein Codewort

$$(c_1, \ldots, c_N) = (u_1, \ldots, u_k, c_{k+1}, \ldots c_N) = uG \in C$$

zuzuordnen. Dabei sind die ersten k Komponenten des Codeworts die Informationssymbole, die anderen $(N-k)$-Komponenten Kontrollsymbole.

Beispiel:
$C \leq \mathbb{F}_2^4$ mit Erzeugermatrix $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Mit C kann man 4 Informationsworte übertragen:
$u_{00} = (00)$ wird codiert zu $(0000) \in C$
$u_{10} = (10)$ wird codiert zu $(1011) \in C$
$u_{01} = (01)$ wird codiert zu $(0101) \in C$
$u_{11} = (11)$ wird codiert zu $(1110) \in C$.

Bei zyklischen Codes kann man die Kontrollsymbole als Rest einer Polynomdivision berechnen:

Satz 3.5 *Sei* $g = \sum_{i=0}^{N-k} g_i x^i \in \mathbb{F}_q[x]$ *ein Teiler von* $x^N - 1$ *und* $C := C_g \trianglelefteq \mathbb{F}_q[x]/(x^N-1)$ *der zyklische Code mit Erzeugerpolynom* g. *Sei* $u := \sum_{i=1}^{k} u_i x^{k-i}$ *ein Informationswort. Dann gibt es ein eindeutig bestimmtes Polynom* $r = \sum_{i=1}^{N-k} r_i x^{N-k-i} \in \mathbb{F}_q[x]$ *mit* $\mathrm{Grad}(r) < N-k = \mathrm{Grad}(g)$, *so daß*

$$ux^{N-k} = gf + r$$

für ein $f \in \mathbb{F}_q[x]$. *Dann ist* $[gf] = [u][x]^{N-k} - [r] =$

$$\sum_{i=1}^{k} u_i [x]^{N-i} - \sum_{i=1}^{N-k} r_i [x]^{N-k-i} \equiv (u_1, u_2, \ldots, u_{k-1}, u_k, -r_1, \ldots, -r_{N-k-1}, -r_{N-k}) \in C_g$$

Beispiel $g := x^4 + x + 1 \in \mathbb{F}_2[x]$ teilt $x^{15} - 1 \in \mathbb{F}_2[x]$. Betrachten $C = C_g \trianglelefteq \mathbb{F}_2[x]/(x^{15} - 1)$. Dann ist $C \cong H(\mathbb{F}_2, 4)$ der Hamming Code der Länge $15 = 2^4 - 1$ und Dimension $15 - 4 = 11$. Der Codierer ordnet jedem 11-Tupel $(u_1, u_2, \ldots, u_{11}) \in \mathbb{F}_2^{11}$ ein Codewort $(u_1, u_2, \ldots, u_{11}, r_1, r_2, r_3, r_4) \in \mathbb{F}_2^{15}$ zu, wo

$$(\sum_{i=1}^{11} u_i x^{11-i}) x^4 = gh + \sum_{i=1}^{4} r_i x^{4-i}$$

ist. Ist z.B. $u = (11010011010)$, so kann man die Division mit Rest mechanisch wie folgt durchführen:

$$
\begin{array}{ccccccccccccccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \;:\; 10011 \\
1 & 0 & 0 & 1 & 1 & & & & & & & & & & \\
\cline{1-5}
 & 1 & 0 & 0 & 1 & 0 & & & & & & & & & \\
 & 1 & 0 & 0 & 1 & 1 & & & & & & & & & \\
\cline{2-6}
 & & & & & 1 & 1 & 1 & 0 & 1 & & & & & \\
 & & & & & 1 & 0 & 0 & 1 & 1 & & & & & \\
\cline{5-10}
 & & & & & & 1 & 1 & 1 & 0 & 0 & & & & \\
 & & & & & & 1 & 0 & 0 & 1 & 1 & & & & \\
\cline{6-11}
 & & & & & & & 1 & 1 & 1 & 1 & 0 & & & \\
 & & & & & & & 1 & 0 & 0 & 1 & 1 & & & \\
\cline{7-12}
 & & & & & & & & 1 & 1 & 0 & 1 & 0 & & \\
 & & & & & & & & 1 & 0 & 0 & 1 & 1 & & \\
\cline{8-13}
 & & & & & & & & & 1 & 0 & 0 & 1 & 0 & \\
 & & & & & & & & & 1 & 0 & 0 & 1 & 1 & \\
\cline{9-14}
 & & & & & & & & & & 0 & 0 & 0 & 0 & 1 \; 0
\end{array}
$$

Also ist der Rest x und $c = (110100110100010) \in C$ das zu u gehörende Codewort.

3.3 Der Minimalabstand zyklischer Codes

Der Minimalabstand zyklischer Codes ist im allgemeinen schwer zu bestimmen, man hat jedoch eine untere Schranke:

Eine Nullstelle α von $x^N - 1 \in \mathbb{F}_q[x]$ heißt primitive N-te Einheitswurzel, falls $N = \min\{n \in \mathbb{N} \mid n \geq 1 \text{ und } \alpha^n = 1\}$. Man beachte, daß α nicht notwendig in $\mathbb{F}_q$ liegen muß sondern eventuell in einem größeren Körper.

Satz 3.6 *Sei g ein Teiler von $x^N - 1 \in \mathbb{F}_q[x]$ und α eine primitive N-te Einheitswurzel. Sind die r aufeinanderfolgenden Potenzen α^b, α^{b+1}, α^{b+2}, ..., α^{b+r-1} Nullstellen von g, so gilt für den zyklischen Code $C_g := ([g]_{x^N-1}) \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ daß $d(C_g) \geq r + 1$.*

Beweis. Sei $c := \sum_{i=0}^{N-1} c_i[x]^i \in C_g$ ein Codewort vom Gewicht $s \leq r$ und seien $c_{t_1}, \ldots, c_{t_s}$ alle von 0 verschiedenen Einträge von c. Da $c \in C_g$ ein Vielfaches von g ist und $\alpha^b, \ldots, \alpha^{b+r-1}$ Nullstellen von g sind gilt $c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+r-1}) = 0$. D.h. es gilt

$$
\begin{array}{ccccccc}
c_{t_1}\alpha^{bt_1} & + & \ldots & + & c_{t_s}\alpha^{bt_s} & = & 0 \\
c_{t_1}\alpha^{(b+1)t_1} & + & \ldots & + & c_{t_s}\alpha^{(b+1)t_s} & = & 0 \\
\vdots & & & & \vdots & & \vdots \\
c_{t_1}\alpha^{(b+r-1)t_1} & + & \ldots & + & c_{t_s}\alpha^{(b+r-1)t_s} & = & 0
\end{array}
$$

Setzt man

$$H := \begin{pmatrix} \alpha^{bt_1} & \dots & \alpha^{bt_s} \\ \alpha^{(b+1)t_1} & \dots & \alpha^{(b+1)t_s} \\ \vdots & \vdots & \vdots \\ \alpha^{(b+s-1)t_1} & \dots & \alpha^{(b+s-1)t_s} \end{pmatrix}$$

so gilt also insbesondere $H(c_{t_1}, \dots, c_{t_s})^{tr} = 0$, d.h. c ist im Kern von H. Die Determinante von H ist aber

$$\det(H) = \alpha^{bt_1}\alpha^{bt_2} \cdot \ldots \cdot \alpha^{bt_s} \det \begin{pmatrix} 1 & \dots & 1 \\ \alpha^{t_1} & \dots & \alpha^{t_s} \\ (\alpha^{t_1})^2 & \dots & (\alpha^{t_s})^2 \\ \vdots & \vdots & \vdots \\ (\alpha^{t_1})^{s-1} & \dots & (\alpha^{t_s})^{s-1} \end{pmatrix} = \alpha^{bt_1}\alpha^{bt_2} \cdot \ldots \cdot \alpha^{bt_s} \prod_{i<j} (\alpha^{t_j} - \alpha^{t_i})$$

nach einer Übungsaufgabe in der Linearen Algebra. Da α eine primitive N-te Einheitswurzel ist, ist $\alpha^{t_i} \neq \alpha^{t_j}$ und $\det(H) \neq 0$. Also ist $\ker(H) = \{0\}$ und $c = 0$. □

Beispiel:
$N = 7$: $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \in \mathbb{F}_2[x]$. Sei $g := x^3 + x + 1$. Dann ist jede Nullstelle α von g ein primitives Element von $\mathbb{F}_2[x]/(x^3 + x + 1) = \mathbb{F}_8$ also eine primitive 7-te Einheitswurzel. Da $g \in \mathbb{F}_2[x]$ gilt $0 = \mathrm{Frob}(g(\alpha)) = g(\mathrm{Frob}(\alpha)) = g(\alpha^2)$, für den Frobenius Automorphismus Frob. Der Code C_g aus Beispiel 3.4 von oben hat also Minimalabstand $\geq 2 + 1 = 3$.
Beispiel:
$N = 23$, $x^{23} - 1 = (x+1)g_1g_2 \in \mathbb{F}_2[x]$ mit

$$g_1 = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

$$g_2 = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

Sei α eine Nullstelle von g_1. Dann ist $\alpha \neq 1$ und $\alpha^{23} = 1$, d.h. α ist eine primitive 23-te Einheitswurzel. Indem man den Frobenius Automorphismus mehrfach auf α anwendet findet man die Nullstellen

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32} = \alpha^9, \alpha^{18}, \alpha^{36} = \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}$$

von g_1. Insbesondere hat g_1 die 4 aufeinanderfolgenden Nullstellen $\alpha, \alpha^2, \alpha^3, \alpha^4$, also hat $C_g \leq \mathbb{F}_2[x]/(x^{23} - 1)$ Minimalabstand ≥ 5. Tatsächlich ist $C_g = \mathcal{G}_{23}$ der Golay-Code der Länge 23 und $d(C_g) = 7$.

Zyklische Codes, für die Satz 3.6 eine gute untere Abschätzung liefern sind die sogenannten BCH-Codes. Das Erzeugerpolynom eines BCH-Codes, ist das Polynom g kleinsten Grades, für das $g(\alpha^b) = g(\alpha^{b+1}) = \ldots = g(\alpha^{b+r-1}) = 0$ für eine primitive N-te Einheitswurzel α:

Definition 3.7 *Ein* BCH-Code *(Bose, Chandhuri, Hocquenghem) mit* designiertem Minimalabstand δ *über $\mathbb{F}_q$ der Länge N ist ein zyklischer Code $C_g \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ für den es eine primitive N-te Einheitswurzel α und $b \in \mathbb{Z}$ gibt, so daß $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ Nullstellen von $g \in \mathbb{F}_q[x]$ sind und g keinen irreduziblen Faktor h hat mit $h(\alpha^b) \neq 0, h(\alpha^{b+1}) \neq 0, \dots$ und $h(\alpha^{b+\delta-2}) \neq 0$.*
Ist $N = q^m - 1$ (also α ein primitives Element von $\mathbb{F}_{q^m}$), so heißt der BCH-Code primitiv.

Aus Satz 3.6 folgt direkt:

Bemerkung 3.8 *Ist C ein BCH-Code mit designiertem Minimalabstand δ, so ist $d(C) \geq \delta$.*

3.4 Unvollständiges Decodieren von zyklischen Codes

Sei C ein BCH-Code der Länge N über $\mathbb{F}_q$ mit designiertem Minimalabstand $\delta = 2t + 1$. Dann gibt es zu jedem $a \in \mathbb{F}_q^N$ höchstens ein $c \in C$ mit $d(a, c) \leq t$, da C t Fehler korrigieren kann. Wir wollen ein Verfahren angeben, wie man zu einem $a \in \mathbb{F}_q^N$ ein solches $c \in C$ bestimmt, falls es so ein c gibt. Dieses Verfahren nennt man "unvollständige" Decodierung, da der Decodierer im Fall daß mehr als t Fehler aufgetreten sind, unter Umständen keine Antwort gibt.

Sei der Einfachheit halber $C = C_g \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ ein zyklischer Code der Länge N, $\alpha \in \mathbb{F}_{q^m}$ eine primitive N-te Einheitswurzel (dazu muß N ein Teiler von $q^m - 1$ sein), so daß α, α^2, α^3, ..., α^{2t} Nullstellen von g sind.

Sei

$$c = (c_1, \ldots, c_N) \equiv c(x) := c_1 x^{N-1} + c_2 x^{N-2} + \ldots + c_N$$

ein gesendetes Codewort und

$$r = (r_1, \ldots, r_N) \equiv r(x) := r_1 x^{N-1} + r_2 x^{N-2} + \ldots + r_N$$

das empfangene Wort. Dann ist der Fehler

$$f = r - c = (r_1 - c_1, \ldots, r_N - c_N) = (f_1, \ldots, f_N) \equiv$$
$$f(x) = r(x) - c(x) = f_1 x^{N-1} + f_2 x^{N-2} + \ldots + f_N$$

Wir kennen r und wollen daraus c (bzw. f) bestimmen, falls höchstens t Komponenten f_i ungleich 0 sind. Wir definieren nun die unbekannten Größen

$$M := \{i \mid f_i \neq 0\},\ e := |M| = \text{Anzahl der Fehler}$$
$$\sigma(z) := \prod_{i \in M} (1 - \alpha^{-i} z),\ \omega(z) := \sum_{i \in M} f_i \alpha^{-i} z \prod_{j \in M - \{i\}} (1 - \alpha^{-j} z)$$

Dann ist $\text{Grad}(\sigma) = e$ und $\text{Grad}(\omega) \leq e$. Kennt man $\sigma(z)$ und $\omega(z)$, so kennt man den Fehler f, denn es ist $f_i \neq 0 \Leftrightarrow \sigma(\alpha^i) = 0$ und dann ist

$$f_i = \frac{-\omega(\alpha^i)\alpha^{-i}}{\sigma'(\alpha^i)}.$$

Es ist

$$\frac{\omega(z)}{\sigma(z)} = \sum_{i \in M} \frac{f_i \alpha^{-i} z}{1 - \alpha^{-i} z} = \sum_{i \in M} f_i \sum_{l=1}^{\infty} (\alpha^{-i} z)^l = \sum_{l=1}^{\infty} z^l \Big(\sum_{i \in M} f_i (\alpha^{-i})^l\Big) = \sum_{l=1}^{\infty} z^l f(\alpha^l)$$

Beachten Sie, daß $\alpha^{N-i} = \alpha^{-i}$ gilt. Für $1 \leq l \leq 2t$ gilt $f(\alpha^l) = r(\alpha^l)$, da $c(\alpha^l) = 0$ ist für diese l. Somit kennt man die ersten $2t + 1$ Koeffizienten der Potenzreihenentwicklung von $\frac{\omega(z)}{\sigma(z)}$.

Satz 3.9 *Es gibt höchstens ein Paar von Polynomen*

$$\sigma(z) = \sum_{j=0}^{t} \sigma_j z^j, \ \omega(z) = \sum_{j=0}^{t} \omega_j z^j$$

mit $\sigma_0 = 1$, $\omega_0 = 0$ *und* $\mathrm{Grad}(\omega) \leq \mathrm{Grad}(\sigma)(= e) \leq t$, *so daß die Potenzreihenentwicklung von* $\frac{\omega(z)}{\sigma(z)}$ *mit* $\sum_{l=1}^{2t} z^l r(\alpha^l)$ *beginnt.*

Beweis. (als Übung), explizites Ausmultiplizieren ergibt nach Koeffizientenvergleich ein lineares Gleichungssystem mit $2t$ Gleichungen und $2t$ Unbekannten $(\sigma_1, \ldots, \sigma_t, \omega_1, \ldots, \omega_t)$. Die Determinante dieses Gleichungssystems ist $\neq 0$, also hat das System genau eine Lösung.
□

Die in Satz 3.9 beschriebene Lösung existiert, wenn höchstens t Fehler aufgetreten sind und liefert dann den Fehlervektor f wie oben beschrieben. Als Test sollte man dann noch überprüfen, ob $r - f$ wirklich im Code liegt.

Beispiel:
Sei $g := x^3 + x + 1 \in \mathbb{F}_2[x]$ und $C_g \trianglelefteq \mathbb{F}_2[x]/(x^7 - 1)$ der Code aus Beispiel 3.4. Sei $\beta \in \mathbb{F}_8$ eine Nullstelle von g. Dann ist auch $g(\beta^2) = 0$. Sei $r = (0000011) = 1 + x$ ein empfangenes Wort. Wir wollen das Codeswort $c \in C_g$ bestimmen mit $d(r, c)$ minimal, wobei wir annehmen, daß höchstens 1 Fehler aufgetreten ist. Es ist

$$r(\beta) = 1 + \beta, \quad r(\beta^2) = 1 + \beta^2.$$

Setzen $\omega(z) := \omega_1 z + \omega_0$, $\sigma(z) := \sigma_1 z + 1$. Dann ist

$$\frac{\omega(z)}{\sigma(z)} = \frac{\omega_1 z + \omega_0}{\sigma_1 z + 1} = (1 + \beta)z + (1 + \beta^2)z^2 + \text{ höhere Terme}$$

also

$$\omega_1 z + \omega_0 = (1 + \beta)z + ((1 + \beta^2) + \sigma_1(1 + \beta))z^2$$

und damit

$$\omega_1 = 1 + \beta, \ \ \omega_0 = 0, \ \ \sigma_1 = (1 + \beta^2)/(1 + \beta) = (1 + \beta^2)\beta^4 = \beta^3.$$

Die Nullstelle von $\sigma(z) = \beta^3 z + 1$ ist $z = \beta^4 = \beta^{-3}$. Also ist nur $f_4 \neq 0$ (an der 4. Stelle ist ein Fehler aufgetreten). Wegen $\sigma'(z) = \beta^3$ ist

$$f_4 = \frac{-\omega(\beta^4)\beta^3}{\beta^3} = (1 + \beta)\beta^4 = \beta^7 = 1.$$

Also ist das richtige Codewort $c = (0001011)$. Es ist $\varphi(c) = x^3 + x + 1 = g$ also $c \in C_g$.

4 Schranken für Codes.

Definition 4.1 *Ein $[N,k,d]$ Code C über $\mathbb{F}_q$ ist ein linearer Code $C \leq \mathbb{F}_q^N$ der Dimension k mit Minimalabstand d. Sei $K_q(N,d) := \max\{k \mid$ es gibt einen $[N,k,d]-$ Code über $\mathbb{F}_q\}$*

Ziel dieses Abschnitts ist es, zwei einfache obere Schranken und eine untere Schranke für die Dimension $K_q(N,d)$ eines linearen Codes in $\mathbb{F}_q^N$ mit Minimalabstand d anzugeben.

Satz 4.2 *(Singleton Schranke)* $K_q(N,d) \leq N - d + 1$

Beweis. Sei $C \leq \mathbb{F}_q^N$ ein $[N,k,d]$-Code. Sei $\pi : \mathbb{F}_q^N \to \mathbb{F}_q^{N-d+1}$ die Projektion auf die ersten $N-d+1$ Komponenten, $\pi(a_1,\ldots,a_N) := (a_1,\ldots,a_{N-d+1})$. Dann ist π eine lineare Abbildung. Weiter sind die Bilder unter π der q^k verschiedenen Codeworte in C alle verschieden, da C Minimalabstand d hat. Also ist

$$|C| = q^k \leq q^{N-d+1}$$

und somit $k = \dim(C) \leq N - d + 1$. □

Definition 4.3 *Für $a \in \mathbb{F}_q^N$ seien*

$$B_r(a) := \{x \in \mathbb{F}_q^N \mid d(x,a) \leq r\}$$
$$S_r(a) := \{x \in \mathbb{F}_q^N \mid d(x,a) = r\}$$

der Ball *bzw. die* Sphäre *um a mit Radius r bzgl. der Hamming-Metrik.*

Satz 4.4 *(a)* $|S_r(a)| = \binom{N}{r}(q-1)^r$
(b) $|B_r(a)| = \sum_{i=0}^{r}\binom{N}{i}(q-1)^i =: V_q(N,r)$

Beweis. Da $S_r(a) - a = \{x - a \mid x \in S_r(a)\} = S_r(0)$ ist, genügt es die Behauptung für $a = 0$ zu zeigen. Dann ist

$$S_r(0) = \{(x_1,\ldots,x_N) \mid \exists 1 \leq i_1 < \ldots < i_r \leq N \text{ so dass } x_j \neq 0 \Leftrightarrow j \in \{i_1,\ldots,i_r\}\}$$

Für die Teilmengen $\{i_1,\ldots,i_r\}$ von $\{1,\ldots,N\}$ hat man genau $\binom{N}{r}$ Möglichkeiten. Legt man eine Teilmenge fest, so hat man für jedes x_{i_j} genau $q-1 = |\mathbb{F}_q - \{0\}|$ Möglichkeiten, insgesamt also $|S_r(a)| = \binom{N}{r}(q-1)^r$.
(b) folgt aus (a), da $B_r(a)$ die disjunkte Vereinigung der Sphären $S_i(a)$ mit $0 \leq i \leq r$ ist. □

Satz 4.5 *(Hamming Schranke) Ist $d = 2t+1$ ungerade, so ist*

$$K_q(N,d) \leq N - \log_q(V_q(N,t))$$

Beweis. Ist $d = 2t+1$ ungerade und $C \leq \mathbb{F}_q^N$ ein $[N,k,d]$-Code, so sind die Kugeln $B_t(c)$ mit Radius t um die Codeworte $c \in C$ disjunkt. Also ist

$$q^N = |F_q^N| \geq \sum_{c \in C} |B_t(c)| = |C| V_q(N,t) = q^k V_q(N,t).$$

Nimmt man den Logarithmus zur Basis q so ergibt sich die Behauptung. □

Beispiel: Ist $C = H(\mathbb{F}_q, m)$ der Hamming-Code der Länge $N = (q^m - 1)/(q-1)$, so ist $d(C) = 3$, $\dim(C) = N - m$ und $|V_q(N,1)| = 1 + N(q-1) = 1 + (q^m - 1)$. Es ergibt sich $|C| \cdot |V_q(N,1)| = q^{N-m} + q^N - q^{N-m} = q^N$. Die Dimension der Hamming-Codes erreicht also genau die Hamming-Schranke. Allgemeiner gilt dies genau für alle perfekten Codes.

Die letzte Schranke gibt eine untere Schranke für den maximalen Minimalabstand eines linearen Codes $C \leq \mathbb{F}_q^N$ der Dimension k an. Der Satz sagt aus, dass gute Codes existieren und gibt sogar eine Konstruktionsmöglichkeit an:

Satz 4.6 *(Gilbert-Varshamov-Schranke) Ist $q^{N-k+1} > V_q(N, d-1)$, so gibt es einen $[N,k,d]$-Codes über $\mathbb{F}_q$.*

Beweis. Per Induktion über $k = \dim(C)$. Für $k = 0$ ($C := \{0\}$) ist die Behauptung trivial. Sei nun $k > 0$ und C_{k-1} ein $[N, k-1, d]$ Code über $\mathbb{F}_q$. Dann gilt

$$|C_{k-1}| \cdot V_q(N, d-1) = q^{k-1} V_q(N, d-1) < q^{k-1} q^{N-k+1} = q^N.$$

Also ist die Vereinigung der Bälle mit Radius $d-1$ um die Codeworte von C_{k-1} nicht ganz $\mathbb{F}_q^N$ und es gibt daher ein

$$a \in \mathbb{F}_q^N - \bigcup_{c \in C_{k-1}} B_{d-1}(c).$$

Setze

$$C_k := \langle C_{k-1}, a \rangle = \{c + sa \mid c \in C_{k-1}, s \in \mathbb{F}_q\}.$$

Dann ist $d(C_k) \geq d$, denn für $c \in C_{k-1}$ und $s \in \mathbb{F}_q$ ist $w(c+sa) = w(c) \geq d$ falls $s = 0$ ist. Sonst ist $w(c+sa) = w(-s^{-1}c - a) = d(-s^{-1}c, a) \geq d$, da mit $c \in C_{k-1}$ auch $-s^{-1}c \in C_{k-1}$ ist und a von allen Codeworten Abstand $\geq d$ hatte. □

Kombiniert man die Gilbert-Varshamov-Schranke mit der Hamming-Schranke so ergibt sich für die maximale Dimension $K_q(N,d)$ eines linearen Codes $C \leq \mathbb{F}_q^N$ mit Minimalabstand $d = 2t+1$ die folgende Abschätzung.

Folgerung 4.7 *Ist $d = 2t+1$ so ist*

$$N - \log_q(V_q(N,t)) \leq K_q(N,d) \leq N - \log_q(V_q(N,d-1))$$

II Gewichtszähler und Thetareihen

5 Gewichtszähler von Codes.

Definition 5.1 *Sei $C \leq \mathbb{F}_q^n$ ein linearer Code. Der* vollständige Gewichtszähler $p_C \in \mathbb{C}[x_a \mid a \in \mathbb{F}_q] = \mathbb{C}[x_0, \ldots, x_{q-1}]$ *ist*

$$p_C(x) := \sum_{c \in C} \prod_{i=1}^{n} x_{c_i}.$$

Der Hamming Gewichtszähler $h_C \in \mathbb{C}[x, y]$ *ist*

$$h_C(x, y) := \sum_{c \in C} x^{n-w(c)} y^{w(c)}.$$

Bemerkung 5.2 *Der Gewichtszähler eines Codes $C \leq \mathbb{F}_q^n$ ist ein homogenes Polynom vom Grad n. Es ist $h_C(x, y) = p_C(x, y, \ldots, y)$.*

Beispiel: $p_{H(\mathbb{F}_2,3)} = x_0^7 + 7x_0^4x_1^3 + 7x_0^3x_1^4 + x_1^7$
$p_{e_8} = x_0^8 + 14x_0^4x_1^4 + x_1^8$.

Satz 5.3 *(MacWilliams Identität) Sei $C \leq \mathbb{F}_p^n$ ein linearer Code, p eine Primzahl. Dann ist*

$$p_{C^\perp}(x_0, \ldots, x_{p-1}) = \frac{1}{|C|} p_C(y_0, \ldots, y_{p-1})$$

wo $y_i = \sum_{j=0}^{p-1} \zeta_p^{ij} x_j$, $\zeta_p = \exp(2\pi i/p)$ eine primitive p-te Einheitswurzel in $\mathbb{C}$.

Beweis. Sei $\epsilon : \mathbb{F}_p^n \to \{0, 1\}$ die Indikatorfunktion von $C^\perp$, d.h. $\epsilon(v) = 1$ falls $v \in C^\perp$ und 0 sonst. Dann ist

$$p_{C^\perp} = \sum_{v \in \mathbb{F}_p^n} \epsilon(v) \prod_{i=1}^{n} x_{v_i}.$$

Wir wollen jetzt die Funktion ϵ kompliziert schreiben. Für $v, w \in \mathbb{F}_p^n$ sei $\zeta_v(w) := \prod_{i=1}^n \zeta_p^{v_i w_i} = \zeta_p^{v \cdot w}$. Dann gilt für $v \in \mathbb{F}_p^n$

$$\frac{1}{|C|} \sum_{c \in C} \zeta_v(c) = \epsilon(v).$$

Denn ist $v \in C^\perp$ so ist die linke Seite gleich 1. Ist $v \notin C^\perp$, so ist $\varphi_v : C \to \mathbb{F}_p, c \mapsto c \cdot v$ eine nichttriviale, also surjektive lineare Abbildung und daher $C = \dot{\cup}_{a=0}^{p-1} \varphi_v^{-1}(\{a\})$ disjunkte Vereinigung gleich großer Mengen. Daher ist in dem Fall

$$\sum_{c \in C} \zeta_v(c) = \frac{|C|}{p} \sum_{a=0}^{p-1} \zeta_p^a = 0.$$

Also ist

$$p_{C^\perp}(x_0,\dots,x_{p-1}) = \sum_{a_1=0}^{p-1}\dots\sum_{a_n=0}^{p-1}\epsilon((a_1,\dots,a_n))x_{a_1}\cdots x_{a_n} = \sum_{a_1=0}^{p-1}\dots\sum_{a_n=0}^{p-1}\frac{1}{|C|}\sum_{c\in C}\prod_{i=1}^{n}\zeta_p^{a_i c_i}x_{a_1}\cdots x_{a_n} = \frac{1}{|C|}\sum_{c\in C}\prod_{i=1}^{n}(\sum_{j=0}^{p-1}\zeta_p^{jc_i}x_j) = \frac{1}{|C|}p_C(y_0,\dots,y_{p-1}).$$

□

Folgerung 5.4 *Für den Hamming Gewichtszähler eines Codes $C \le \mathbb{F}_p^n$ gilt:*

$$h_{C^\perp}(x,y) = \frac{1}{|C|}h_C(x+(p-1)y, x-y).$$

Beweis. $h_{C^\perp}(x,y) = p_{C^\perp}(x,y,\dots,y) = \frac{1}{|C|}p_C(z_0,\dots,z_{p-1})$ mit $z_i = x + \sum_{j=1}^{p-1}\zeta_p^{ij}y$. Ist $i=0$, so erhält man $z_0 = x+(p-1)y$. Für $i \in \mathbb{F}_p^*$ durchläuft mit j auch ij ganz $\mathbb{F}_p^*$ also ist für $i \in \{1,\dots,p-1\}$ $\sum_{j=1}^{p-1}\zeta_p^{ij} = \sum_{j=1}^{p-1}\zeta_p^{j} = -1$ und daher $z_i = x-y$. □

Bemerkung 5.5 *Mit derselben Strategie erhält man den Gewichtszähler von $C^\perp$ aus dem von C durch geeignete Variablensubstitution auch für allgemeinere Ringe (z.B. $\mathbb{F}_q$, $q=p^f$, aber auch $\mathbb{Z}/p^m\mathbb{Z}$).*

Beispiel 5.6 *Für $p=2$ liest sich die MacWilliams Identität als*

$$p_{C^\perp}(x_0,x_1) = \frac{1}{|C|}p_C(x_0+x_1, x_0-x_1)$$

und für $p=3$ erhält man

$$p_{C^\perp}(x_0,x_1,x_2) = \frac{1}{|C|}p_C(x_0+x_1+x2, x_0+\omega x_1+\omega^2 x_2, x_0+\omega^2 x_1+\omega x_2)$$

wobei $\omega = \zeta_3 = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist.

Bemerkung 5.7 *Gewichtszähler selbstdualer Codes.*
Ist $C = C^\perp \le \mathbb{F}_p^n$ so ist $|C| = p^{n/2}$. Dann liest sich Folgerung 5.4 als

$$h_C(x,y) = h_{C^\perp}(x,y) = h_C((x+(p-1)y)/\sqrt{p}, (x-y)/\sqrt{p})).$$

Das Polynom $h_C(x,y)$ ist also invariant unter der Variablensubstitution $x \mapsto \frac{1}{\sqrt{p}}(x+(p-1)y)$, $y \mapsto \frac{1}{\sqrt{p}}(x-y)$, als Matrix $\frac{1}{\sqrt{p}}\begin{pmatrix}1 & p-1\\ 1 & -1\end{pmatrix}$. Dies schränkt die Menge der möglichen Gewichtszähler selbstdualer Codes ein, sie liegen alle in dem Teilraum der unter dieser Variablensubstitution invarianten Polynome.
Ist $p=2$, so kann man noch mehr sagen. Jeder selbstduale Code $C = C^\perp \le \mathbb{F}_2^n$ erfüllt natürlich $c\cdot c = 0$, also ist die Anzahl der Einsen in $c \in C$ immer gerade und somit $w(c) \in 2\mathbb{Z}$. Also ist $p_C(x_0,x_1) = p_C(x_0,-x_1)$ und p_C invariant unter der Gruppe von Variablensubstitutionen

$$\langle\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\rangle =: G_I \cong D_{16}.$$

Für doppelt gerade Codes gilt sogar $w(c) \in 4\mathbb{Z}$ und somit $p_C(x_0, x_1) = p_C(x_0, ix_1)$. Der Gewichtszähler eines binären selbstdualen doppelt geraden (oder auch Typ II) Codes ist also invariant unter

$$\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rangle =: G_{II}$$

einer Gruppe der Ordnung 192.

Mit Hilfe der Invariantentheorie erhält man den folgenden Satz, den ich nur zitieren möchte (vgl. z.B. Sturmfels):

Satz 5.8 *(I) Ist $p(x_0, x_1)$ ein unter G_I invariantes Polynom so ist p ein Polynom in $f := x_0^2 + x_1^2 = p_{\langle(1,1)\rangle}$ und $g := p_{e_8} = x_0^8 + 14x_0^4x_1^4 + x_1^8$. oder alternativ in f und*

$$\delta := \frac{1}{4}(f^4 - g) == x_0^6x_1^2 - 2x_0^4x_1^4 + x_0^2x_1^6 = x_0^2x_1^2(x_0^2 - x_1^2)^2.$$

(II) Ist $p(x_0, x_1)$ ein unter G_{II} invariantes Polynom so ist p ein Polynom in $g := p_{e_8} = x_0^8 + 14x_0^4x_1^4 + x_1^8$ und $\Delta := x_0^4x_1^4(x_0^4 - x_1^4)^4$.

Satz 5.9 *(Gleason) Ist $C = C^\perp \leq \mathbb{F}_2^n$, $n = 8a + 2b$ mit $0 \leq b \leq 3$ so gibt es eindeutig bestimmte Zahlen $k_i \in \mathbb{Z}$, $i = 0, \ldots, a$ mit $k_0 = 1$ so daß*

$$p_C(x_0, x_1) = \sum_{i=0}^{a} k_i f^{4(a-i)+b} \delta^i.$$

Ist C zusätzlich doppelt gerade, so ist $n = 24t + 8s$ durch 8 teilbar und es gibt eindeutig bestimmte Zahlen $\ell_i \in \mathbb{Z}$ $(i = 0, \ldots, t)$ mit $\ell_0 = 1$ so daß

$$p_C(x_0, x_1) = \sum_{i=0}^{t} \ell_i g^{3(t-i)+s} \Delta^i.$$

Folgerung 5.10 *Ist $C = C^\perp \leq \mathbb{F}_2^n$ so ist $d(C) \leq 2\lfloor \frac{n}{8} \rfloor + 2$.*
Ist C zusätzlich doppel gerade so findet man sogar $d(C) \leq 4\lfloor \frac{n}{24} \rfloor + 4$.

Beweis. Sei $n = 8a + 2b$ und $C = C^\perp \leq \mathbb{F}_2^n$. Die Bedingung $d(C) \geq 2\lfloor \frac{n}{8} \rfloor + 2 = 2a + 2$ liefert $a+1$ lineare Gleichungen an die Koeffizienten k_i von p_C in der Basis $(f^{4(a-i)+b}\delta^i : i = 0, \ldots, a)$, wodurch die k_i eindeutig bestimmt sind. Sei

$$f = \sum_{i=0}^{a} k_i f^{4(a-i)+b} \delta^i = x_0^n + A_{2a+2} x_0^{n-2a-2} x_1^{2a+2} + \ldots$$

das durch diese Koeffizienten bestimmte Polynom. Dann ist zu zeigen, das $A_{2a+2} \neq 0$ ist, indem man diesen Koeffizienten als Linearkombination der k_i ausdrückt. Dies ist etwas mühsam, aber machbar.
Für doppelt gerade Codes verfährt man analog. □

Definition 5.11 *Ist $C = C^\perp$ ein binärer doppelt gerader Code mit $d(C) = 4\lfloor \frac{n}{24} \rfloor + 4$, so heißt C* extremal.

Bemerkung 5.12 *(a) e_8 ist ein extremaler Code.*
(b) Der Gewichtszähler eines extremalen Codes ist eindeutig bestimmt.
(c) Man kennt bisher nur 2 extremale Codes, deren Länge ein Vielfaches von 24 ist, nämlich den binären Golay Code der Länge 24, den wir im nächsten Abschnitt konstruieren und den Quadratischen Restcode der Länge 48. Dies sind auch die einzigen extremalen Codes in Länge 24 und 48.

5.1 Der binäre Golay Code und das Leech Gitter.

Satz 5.13 *Es gibt einen extremalen doppeltgeraden selbstdualen binären Code $\mathcal{G}_{24}$ der Länge 24. Dieser heißt der* Golay Code *der Länge 24.*

Beweis. Wir geben J.H. Conway's Konstruktion des Golay Codes aus dem Hexacode, $h_6 \leq \mathbb{F}_4^6$ mit Erzeugermatrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{pmatrix}$$

an. Es gilt $h_6 = \overline{h_6}^\perp$ (Hermitesch selbstdual) wobei $\overline{\ }$ der nichttriviale Galoisautomorphismus von $\mathbb{F}_4$ ist ($\overline{x} = x^2$). Da $x\overline{x} = 1$ für $x \in \mathbb{F}_4, x \neq 0$, sind die Hamming Gewichte aller Codeworte in h_6 gerade. Insbesondere hat h_6 kein Wort von Gewicht 3 oder 5. Die Worte c vom Gewicht 2 in h_6 sind Linearkombinationen von 2 Erzeugern. Aus Symmetriegründen können wir annehmen, dass $c = b_1 + ab_2$ ist mit $a \in \{0, 1, \omega, \omega^2\}$. Diese Worte haben aber alle Gewicht 4, also ist $d(h_6) = 4$. Der Hamming Gewichtszähler von h_6 ist

$$h_{h_6} = x^6 + 45x^2y^4 + 18y^6.$$

(Die Worte vom Gewicht ≤ 5 sind von der Form $ab_i + bb_j$ mit $1 \leq i < j \leq 3$ und $(a, b) \in \mathbb{F}_4^2 - \{0\}$. Davon gibt es $3 \cdot (16 - 1) - 9 = 36$ Stück. Von den Linearkombinationen von 3 Basisvektoren mit Koeffizienten $\neq 0$, also $ab_1 + bb_2 + cb_3$ mit $a, b, c \in \mathbb{F}_4 - \{0\}$ haben 18 Gewicht 6 und 9 Gewicht 4.)

Identifiziert man $\mathbb{F}_2^{24}$ mit $\mathbb{F}_2^{4\times 6}$ in der offensichtlichen Weise so ist

$$\mathcal{G}_{24} = \{(x_{ij}) \in \mathbb{F}_2^{4\times 6} \mid \begin{array}{l} \sum_{i=1}^4 x_{ij} = \sum_{k=1}^6 x_{1k} \quad \text{für alle } j = 1, \ldots, 6 \\ x_2 + \omega x_3 + \overline{\omega} x_4 \in h_6 \end{array} \}.$$

Wir zeigen dazu, dass der in der Menge beschriebene lineare Code Dimension 12 hat und Minimalabstand ≥ 8.

Die $\mathbb{F}_2$-lineare Abbildung

$$\mathbb{F}_2^3 \to \mathbb{F}_4, \ x \mapsto x_1 + \omega x_2 + \overline{\omega} x_3$$

hat Kern $\langle (1, 1, 1) \rangle = \{(0, 0, 0), (1, 1, 1)\}$. Also gibt es zu jedem $c \in h_6$ genau 2^6 Matrizen $(X_{ij}) \in \mathbb{F}_2^{3\times 6}$ mit $X_1 + \omega X_2 + \omega^2 X_3 = c$. Die Urbilder werden genau durch die Spaltensummen

$\in \mathbb{F}_2^6$ unterschieden. Wählt man sich also eine beliebige erste Zeile $(x_{11}, \ldots, x_{16}) \in \mathbb{F}_2^6$ und ein beliebiges Wort $c \in h_6$ so enthält $\mathcal{G}_{24}$ genau eine Matrix (x_{ij}) mit dieser ersten Zeile und so dass $x_2 + \omega x_3 + \overline{\omega} x_4 = c$. Also ist $|\mathcal{G}_{24}| = 2^6 \cdot 4^3 = 2^{12}$.

Zum Minimalgewicht: Sei $X := (x_{ij}) \in \mathcal{G}_{24}$. Ist $\sum_{j=1}^{6} x_{1j}$ gerade und $c \neq 0$, so ist $\mathrm{wt}(c) \geq 4$ und X hat mindestens 4 Spalten $\neq 0$, in denen dann 2 oder 4 Einsen stehen müssen. Daher $\mathrm{wt}(X) \geq 2 \cdot 4 = 8$. Ist $c = 0$ und die erste Zeile nicht 0, so enhält diese mindestens 2 Einsen. Die zugehörigen Spalten sind dann aber $(1,1,1,1)^{tr}$ also $\mathrm{wt}(X) \geq 8$. Ist $\sum_{j=1}^{6} x_{1j}$ ungerade so steht in jeder Spalte mindestens eine 1, da die Spaltensummen alle ungerade sein müssen. Also ist $\mathrm{wt}(X) \geq 6$. Ist $\mathrm{wt}(X) = 6$, so ist $c \in h_6$ ein Wort vom Gewicht 5, was nicht existiert.
Da mir kein cleveres Argument einfällt, um schnell zu sehen, dass alle Gewichte in dem konstruierten Code durch 4 teilbar sind, gebe ich einfach 12 linear unabhängige Vektoren in dem Code an. Dazu betrachte ich die $\mathbb{F}_2$-Basis des Hexacodes, die aus den 3 Zeilen der Erzeugermatrix und den 3 mit ω multiplizierten Zeilen besteht und finde zu jedem dieser 6 Hexacodeworte ein Golaycodewort mit diesem Bild:

$$\begin{array}{cccccc}
100111 & 100100 & 000011 & 000000 & \mapsto & 1001\omega\omega \\
010111 & 010010 & 000101 & 000000 & \mapsto & 010\omega1\omega \\
001111 & 001001 & 000110 & 000000 & \mapsto & 001\omega\omega1 \\
100111 & 000000 & 100100 & 000011 & \mapsto & \omega00\omega\omega^2\omega^2 \\
010111 & 000000 & 010010 & 000101 & \mapsto & 0\omega0\omega^2\omega\omega^2 \\
001111 & 000000 & 001001 & 000110 & \mapsto & 00\omega\omega^2\omega^2\omega
\end{array}$$

Dies sind sicherlich 6 linear unabhängige Vektoren in $\mathcal{G}_{24}$, da ihre Bilder in h_6 $\mathbb{F}_2$-linear unabhängig sind. Daraus lässt sich also dann jedes Hexacodewort linear kombinieren. Es genügt jetzt, weitere 6 linear unabhängige Elemente aus dem Kern der Abbildung $X \mapsto x_2 + \omega x_3 + \omega^2 x_4$ anzugeben.

$$\begin{array}{cccc}
110000 & 110000 & 110000 & 110000 \\
101000 & 101000 & 101000 & 101000 \\
100100 & 100100 & 100100 & 100100 \\
100010 & 100010 & 100010 & 100010 \\
100001 & 100001 & 100001 & 100001 \\
111110 & 000001 & 000001 & 000001
\end{array}$$

Nun sieht man, dass alle Basisvektoren Gewicht 8 haben und paarweise Skalarprodukt 0.
□

Man kann zeigen, dass der Golay Code der einzige extremale Code der Länge 24 ist, für einen Beweis verweise ich auf das Buch von Ebeling.

Definition 5.14 *(Leech Gitter) Sei*

$$M := L_{\mathcal{G}_{24}} = \{\sum_{i=1}^{24} a_i x_i \mid (a_1 + 2\mathbb{Z}, \ldots, a_{24} + 2\mathbb{Z}) \in \mathcal{G}_{24}\}$$

wobei $(x_1, \ldots, x_{24})$ eine OG-Basis ist mit $(x_i, x_i) = 1/2$ das Codegitter (vgl. Definition 2.13) zu $\mathcal{G}_{24}$. Dann ist $\min(M) = 2$ und $S(M) = \{\pm 2x_1, \ldots, \pm 2x_{24}\}$. Sei $M_0 := \{m \in M \mid$

$(m, \sum_{i=1}^{24} x_i) \in 2\mathbb{Z}\} \leq M$ *und* $M_1 := \{m \in M \mid (m, \sum_{i=1}^{24} x_i) \in 1 + 2\mathbb{Z}\} \subset M$ *und setze*

$$\Lambda_{24} := M_0 \cup (\frac{1}{2}\sum_{i=1}^{24} x_i + M_1).$$

Λ_{24} *heißt das* Leech Gitter.

Satz 5.15 Λ_{24} *ist ein gerades unimodulares Gitter mit* $\min(\Lambda_{24}) = 4$.

Beweis. Es ist klar, dass M_0 ein Teilgitter vom Index 2 in dem geraden unimodularen Gitter M ist. Da $S(M) \not\subset M_0$, ist $\min(M_0) \geq 4$. Die Elemente $y := \frac{1}{2}\sum_{i=1}^{24} x_i + m$ mit $m \in M_1$ erfüllen

- $(y, y) = \frac{12}{4} + (\sum_{i=1}^{24} x_i, m) + (m, m) \in 2\mathbb{Z}$.
- $y = \sum a_i x_i$ mit allen $a_i \in \frac{1}{2} + \mathbb{Z}$.
- $(y, y) \geq 3$.
- $y_1 + y_2 = \sum_{i=1}^{24} x_i + m_1 + m_2 \in M_0$ für $y_1, y_2 \in \frac{1}{2}\sum_{i=1}^{24} x_i + M_1)$.

Also ist Λ_{24} ein gerades Gitter und $\min(\Lambda_{24}) \geq 4$. Da M_0 ein Teilgitter von Index 2 in Λ_{24} ist, ist Λ_{24} unimodular. □

Vektoren der Quadratlänge 4 in Λ_{24}:

wo	Typ	Anzahl	
M_0 :	$\pm 1^8 0^{16}$	$759 \cdot 2^7 =$	97152
	$\pm 2^2 0^{22}$	$4\binom{24}{2} =$	1104
$\frac{1}{2}\sum x_i + M_1$:	$(\pm 1/2)^{23} \pm 3/2$	$24 \cdot 2^1 2 =$	98304
			196560

5.2 Quadratische Rest Codes.

Dieser Abschnitt hätte ergänzt das Kapitel zyklische Codes um ein wichtiges Beispiel, die Quadratischen Rest Codes. Der Einfachheit halber betrachten wir nur binäre QR-Codes.

Lemma 5.16 *Sei* p *eine Primzahl und* $Q := \{a \in \{1, \ldots, p-1\} \mid$ *es gibt* $b \in \mathbb{F}_p, a \equiv_p b^2\}$ *die Menge aller Quadrate in* $\mathbb{F}_p$ *und* $N := \{1, \ldots, p-1\} - Q$ *die Menge der Nichtquadrate. Sei* $\zeta \in \mathbb{F}_{2^{p-1}}$ *eine primitive* p*-te Einheitswurzel. Dann ist*

$$(X^p - 1) = \prod_{i=0}^{p-1}(X - \zeta^i) = (X-1)\prod_{i \in Q}(X - \zeta^i) \cdot \prod_{i \in N}(X - \zeta^i) = p_0 p_Q p_N.$$

Es gilt immer $p_Q \in \mathbb{F}_4[X]$ *und ebenso* $p_N \in \mathbb{F}_4[X]$. *Es ist* $p_Q \in \mathbb{F}_2[X]$ *genau dann wenn* $2 \in Q$, *also wenn* $p = 8m \pm 1$ *für ein* $m \in \mathbb{N}$ *ist.*

Beweis. Wir betrachten den Frobeniusautomorphismus

$$F_4 \in \mathrm{Aut}_{\mathbb{F}_4}(\mathbb{F}_{2^{p-1}}), a \mapsto a^4$$

und setzen F_4 auf dem Polynomring fort, indem wir ihn auf die Koeffizienten der Polynome anwenden. Dies liefert wieder einen $\mathbb{F}_4$-linearen Ringautomorphismus $F_4 \in \mathrm{Aut}_{\mathbb{F}_4}(\mathbb{F}_{2^{p-1}}[X])$. Es ist $f \in \mathbb{F}_4[X]$, genau dann wenn $F_4(f) = f$ ist. Nun ist

$$F_4(p_Q) = F_4(\prod_{i \in Q}(X - \zeta^i)) = \prod_{i \in Q}(X - \zeta^{4i}) = p_Q,$$

da $4 = 2^2 \in Q$ ist. Ist sogar $2 \in Q$, so gilt eine analoge Überlegung für $F_2 : a \mapsto a^2$ und es sind p_Q und p_N in $\mathbb{F}_2[X]$. □

Wir müssen uns zunächst über Quadrate in endlichen Primkörpern klar werden.

Bemerkung 5.17 *Sei p eine ungerade Primzahl. Dann ist das eindeutige Element -1 der Ordnung 2 in $(\mathbb{F}_p)^*$ ein Quadrat genau dann wenn $|((\mathbb{F}_p)^*)^2| = \frac{p-1}{2}$ gerade ist genau dann wenn $p \equiv 1 \pmod 4$.*

Schwieriger ist es bei der Zahl 2. Klar ist eine nicht durch p teilbare Zahl a ein Quadrat modulo p genau dann wenn $a^{(p-1)/2} \equiv 1 \pmod p$ ist und kein Quadrat wenn $a^{(p-1)/2} \equiv -1 \pmod p$ ist.

Satz 5.18 *2 ist ein Quadrat modulo der ungeraden Primzahl p, genau dann wenn $p^2 \equiv 1 \pmod 8$.*

Beweis. Sei K ein Erweiterungskörper von $\mathbb{F}_p$, der eine primitive 8-te Einheitswurzel enthält, also ein Element α mit $\alpha^4 = -1$. Definiert man $\tau := \alpha + \alpha^{-1}$ so ist

$$\tau^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = 2$$

da $\alpha^{-2} = -\alpha^2$ gilt. Also ist

$$2^{(p-1)/2}\tau = \tau^p = \alpha^p + \alpha^{-p} = (-1)^{(p^2-1)/8}\tau$$

also $2^{(p-1)/2} = (-1)^{(p^2-1)/8}$ in $\mathbb{F}_p$. Um $\alpha^p + \alpha^{-p} = (-1)^{(p^2-1)/8}\tau$ zu sehen machen wir Fallunterscheidung. Ist $p \equiv \pm 1 \pmod 8$, so ist $\alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = \tau$. Ist $p \equiv \pm 3 \pmod 8$, so ist

$$\alpha^p + \alpha^{-p} = \alpha^3 + \alpha^{-3} = -\alpha^{-1} - \alpha = -\tau$$

da $\alpha^4 = -1$ ist. □

Definition 5.19 *Sei p eine Primzahl der Form $p = 8m \pm 1$ für ein $m \in \mathbb{N}$. Dann heisst der zyklische Code $\mathcal{Q}$ der Länge p mit Erzeugerpolynom $p_Q \in \mathbb{F}_2[X]$ der* Quadratische Restcode, *$\mathcal{Q} = \mathrm{QR}(\mathbb{F}_2, p)$. (Dieser hängt von der Wahl von ζ ab, aber verschiedene ζ liefern äquivalente Codes.)*

Beispiel 5.20 *Sei $p = 7$. Dann ist $\mathbb{F}_7^* = \langle 3 \rangle$ und $Q = \{2, 4, 1\}$, $N = \{3, 6, 5\}$ und $\mathrm{QR}(\mathbb{F}_2, 7)$ ein binärer Code der Länge 7 mit Minimalabestand 3.*

Lemma 5.21 *Sei $p \equiv -1 \pmod 8$ und $C := \mathrm{QR}(\mathbb{F}_2, p)$.*
Sei $0 \neq a \in C$ ein Wort vom Gewicht $\mathrm{wt}(a) = d$.
(a) Ist d ungerade, so ist $d^2 - d + 1 \geq p$ und $d \equiv 3 \pmod 4$
(b) Ist d gerade, so ist $d \equiv 0 \pmod 4$.

Beweis. Da $p \equiv -1 \pmod 8$ ist -1 kein Quadrat modulo p also $N = p - Q$. Sei $a(x) = \sum_{i=1}^{d} x^{k_i}$ ein Codewort vom Gewicht d, wobei die $k_i \in \mathbb{Z}/p\mathbb{Z}$ paarweise verschieden sind. Da $a(x) \in C_{pQ(x)}$ gilt $a(\zeta^q) = 0$ für $q \in Q$ und $a(\zeta^{-n}) = 0$ für $n \in N$.
Sei zunächst $d = \mathrm{wt}(a)$ ungerade. Dann ist $a(1) \neq 0$ und daher

$$a(x)a(x^{-1}) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1 \in \mathbb{F}_2[x]/(x^p - 1).$$

Hier ist $a(x^{-1}) = \sum_{i=1}^{d} x^{p-k_i}$. Insbesondere ist $a(x)a(x^{-1})$ ein Wort vom Gewicht p. Ausmultiplizieren liefert d^2 Terme von denen d (nämlich die $x^{k_i}x^{-k_i}$) übereinstimmen also ist

$$d^2 - d + 1 \geq p.$$

Genauer ist $p = d^2 - d + 1 - |A|$ wobei

$$A = \{[(i, j), (l, m)] \mid i \neq j, l \neq m, (i, j) \neq (l, m) \text{ und } k_i - k_j \equiv k_l - k_m \pmod p\}$$

Mit $[(i, j), (l, m)] \in A$ ist jedoch auch $[(l, m), (i, j)]$, $[(j, i), (m, l)]$ und $[(m, l), (j, i)]$ in A, also ist $|A|$ durch 4 teilbar und daher

$$d^2 - d + 1 \equiv p \pmod 4 \Leftrightarrow d \equiv 2 - p \equiv 3 \pmod 4.$$

Ist d gerade so ist auch $a(1) = 0$ und daher $a(x)a(-x) = 0$ in $\mathbb{F}_p[x]/(x^p - 1)$. Wie eben erhalten wir durch explizites Ausmultiplizieren $d^2 - d - |A| = 0$ (hier fehlt $+1$, da $\sum_{i=1}^{d} x^{k_i}x^{-k_i} = d = 0 \in \mathbb{F}_2$ ist) und also $d^2 - d \equiv 0 \pmod 4$ und somit ist d durch 4 teilbar. □

Definition 5.22 *Sei $p \equiv \pm 1 \pmod 8$. Der* erweiterte Quadratische Restcode *ist $\widetilde{\mathrm{QR}}(\mathbb{F}_2, p) = \{(c, \sum_{i=1}^{p} c_i) \mid c \in \mathrm{QR}(\mathbb{F}_2, p)\} \leq \mathbb{F}_2^{p+1}$.*

Satz 5.23 *Ist $p \equiv -1 \pmod 8$, so ist $\widetilde{\mathrm{QR}}(\mathbb{F}_2, p)$ ein selbstdualer doppelt gerader Code.*

Beweis. Wegen $\dim(\widetilde{\mathrm{QR}}(\mathbb{F}_2, p)) = \frac{p+1}{2}$ genügt es zu zeigen, dass die Gewichte in $\widetilde{\mathrm{QR}}(\mathbb{F}_2, p)$ alle durch 4 teilbar sind. Dies folgt aber aus Lemma 5.21. □

Beispiel:

Quadrate modulo 23:

$$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

Also $d := d(\mathrm{QR}(\mathbb{F}_2, 23)) \geq 5$ und wegen Lemma 5.21 sogar $d \geq 7$ und somit $d(\widetilde{\mathrm{QR}}(\mathbb{F}_2, 23)) \geq 8$ und wegen Folgerung 5.10 $d(\widetilde{\mathrm{QR}}(\mathbb{F}_2, 23)) = 8$. Es gilt $\widetilde{\mathrm{QR}}(\mathbb{F}_2, 23) \cong \mathcal{G}_{24}$ ist der binäre Golay Code der Länge 24.

Satz 5.24 *Sei*

$$c(x) := \sum_{q \in Q} x^q \in \mathbb{F}_2[x]/(x^p - 1) = \sum_{i=0}^{p-1} c_i x^i.$$

Dann ist

$$G := \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ c_0 & c_1 & \dots & c_{p-1} & 1 \\ c_{p-1} & c_0 & \dots & c_{p-2} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_1 & c_2 & \dots & c_0 & 1 \end{pmatrix} \in \mathbb{F}_2^{(p+1)\times(p+1)}$$

eine Erzeugermatrix von $\widetilde{\mathrm{QR}}(\mathbb{F}_2, p)$ *(vom Rang* $\frac{p+1}{2}$*).*

Beweis. Da $2 \in Q$ ist gilt

$$c(x)^2 = (\sum_{q \in Q} x^q)^2 \stackrel{\star}{=} \sum_{q \in Q} x^{2q} = c(x) \in \mathbb{F}_2[x]/(x^p - 1)$$

wobei die Gleichheit $\star$ gilt, da sie für alle Elemente $x \in \mathbb{F}_{2^{p-1}}$ gilt und damit insbesondere für die p-ten Einheitswurzeln. $c(x)$ ist also ein Idempotent in dem Ring

$$\mathbb{F}_2[x]/(x^p - 1) = \mathbb{F}_2[x]/(x - 1) \oplus \mathbb{F}_2[x]/(p_Q) \oplus \mathbb{F}_2[x]/p_N.$$

Da $-1 \in N$ ist gilt $c(x) + c(x^{-1}) = \sum_{i=1}^{p-1} x^i$ also ist für jede primitive p-te Einheitswurzel β $c(\beta) + c(\beta^{-1}) = 1$. Außerdem ist für $r \in Q$, $c(\beta) = c(\beta^r)$. Also ist c konstant auf $\{\zeta^q \mid q \in Q\}$ und auch konstant auf $\{\zeta^n \mid n \in N\}$ und $c(1) = |Q| \pmod 2 = \frac{p-1}{2} \pmod 2 = 1$. Da $c(x)^2 = c(x)$ ist gilt $c(\alpha) \in \{0, 1\}$ für alle α und damit entweder $c(\zeta^q) = 0$ für alle $q \in Q$ oder $c(\zeta^n) = 0$ für alle $n \in N$. Indem wir ζ durch ζ^{-1} ersetzen können wir annehmen, dass $c(\zeta^q) = 0$ für alle $q \in Q$ und damit $c \in (p_Q) \trianglelefteq \mathbb{F}_2[x]/(x^p - 1)$. Nach dem chinesischen Restsatz ist c genau die Projektion auf das von p_Q erzeugte Ideal, insbesondere ist $cp_Q = p_Q$ und c ein weiterer Erzeuger von (p_Q). □

Wir wollen zum Abschluss eine Untergruppe der Automorphismengruppe der erweiterten quadratischen Restcodes angeben. Dazu identifizieren wir die $p + 1$ Stellen des Codes mit den $p + 1$ eindimensionalen Teilräumen von $\mathbb{F}_p^2$:

$$\mathcal{T} := \{\langle(0, 1)\rangle, \langle(1, 1)\rangle, \dots \langle(p - 1, 1)\rangle, \langle(1, 0)\rangle\}.$$

Die Gruppe $PGL_2(\mathbb{F}_p)$ operiert in natürlicher Weise als Permutationsgruppe auf $\mathcal{T}$.

Satz 5.25 $PSL_2(\mathbb{F}_p) \leq \mathrm{Aut}(\widetilde{\mathrm{QR}}(\mathbb{F}_2, p))$.

Beweis. $PSL_2(\mathbb{F}_p) = \langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} =: T, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} =: S \rangle$ Das Element T operiert durch zyklische Vertauschung auf den ersten p Stellen von $\widetilde{\mathrm{QR}}(\mathbb{F}_2, p)$, lässt den Code also invariant. Zur Operation von S: Identifiziert man $\mathcal{T}$ mit $\mathbb{F}_p \cup \infty$ durch $\langle(a, b)\rangle \mapsto \frac{a}{b}$ $(= \infty$, falls $b = 0)$, so operiert S durch $z \mapsto -\frac{1}{z}$. Wir nummerieren die Zeilen der Matrix G aus Satz 5.24 auch mit den Elementen $\infty, 0, 1, \dots, p - 1$ und setzen $H := (h_{ij})$ mit $h_{ij} = g_{-1/i,-1/j}$. Wir müssen zeigen, dass die Zeilen von H Linearkombinationen der Zeilen von G sind. Das ist elementares Nachrechnen. Einen expliziten Beweis finden Sie z.B. in Ebeling's Buch auf Seite 84. □

Folgerung 5.26 *$d(\mathrm{QR}(\mathbb{F}_2, p))$ ist ungerade.*

Beweis. Sei $0 \neq c \in \widetilde{\mathrm{QR}}(\mathbb{F}_2, p)$ ein Wort minimalem Gewichts $4m$. Dann gibt es, da die Gruppe $PSL_2(p)$ zweifach transitiv auf $\mathcal{T}$ operiert, also insbesondere transitiv, ein $g \in \mathrm{Aut}(\widetilde{\mathrm{QR}}(\mathbb{F}_2, p))$ so dass cg an der letzten Stelle eine 1 stehen hat. Das zu cg gehörende Wort in $\mathrm{QR}(\mathbb{F}_2, p)$ hat dann Gewicht $4m - 1$, also ungerades Gewicht. □

Sei $d + 1 = d(\widetilde{\mathrm{QR}}(\mathbb{F}_2, p))$, also $d = d(\mathrm{QR}(\mathbb{F}_2, p))$. Dann ist

$$d \equiv 3 \pmod 4 \text{ und } d^2 - d + 1 \geq p$$

und mit Folgerung 5.10 findet man:

Folgerung 5.27 *Sei $C = \widetilde{\mathrm{QR}}(\mathbb{F}_2, p)$. Dann ist C extremal, falls*

$$p \in \{7, 23, 31, 47\}.$$

Man kann zeigen, dass $d(\widetilde{\mathrm{QR}}(\mathbb{F}_2, 71) = 12$.

Beweis. Für $p = 47$: $d^2 - d + 1 \geq 47$ liefert $d \geq 8$. Da $d \equiv 3 \pmod 4$ findet man sogar $d \geq 11$ und somit $d + 1 = d(\widetilde{\mathrm{QR}}(\mathbb{F}_2, 47)) \geq 12$. Gleichheit folgt aus Folgerung 5.10. □

6 Thetareihen von Gittern.

Definition 6.1 *Sei L ein ganzes Gitter in $(\mathbb{R}^n, (,))$. Die formale Potenzreihe*

$$\Theta_L := \sum_{\ell \in L} q^{(\ell,\ell)} = \sum_{m=0}^{\infty} a_m q^m \in \mathbb{C}[[q]]$$

mit $a_m = |L_{=m}|$ heißt Theta-Reihe *von L. Analog definiert man für jede (geeignete) Teilmenge $T \subset \mathbb{R}^n$ (z.B. $T = v + L$, eine Restklasse nach einem Gitter L) die Theta-Reihe $\Theta_T := \sum_{t \in T} q^{(t,t)}$.*

Beispiel 6.2 $\Theta_{\mathbb{Z}} = \sum_{a \in \mathbb{Z}} q^{a^2} = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$.
Sind L, M Gitter, so gilt

$$\Theta_{L \perp M} = \Theta_L \Theta_M.$$

Ist $a \in \{0, \ldots, p-1\}$ so sei $\theta_{a,p} := \sum_{z \in \mathbb{Z}, z \equiv_p a} q^{z^2/p}$. Ist $e \in \mathbb{R}^n$ ein Vektor mit $(e, e) = 1/p$ so ist $\theta_{a,p} = \Theta_{ae + \langle pe \rangle_{\mathbb{Z}}}$.

Satz 6.3 *Sei $C \leq \mathbb{F}_p^N$ ein Code und $L_C \leq \mathbb{R}^N$ das zugehörige Codegitter. Dann ist*

$$\Theta_{L_C} = p_C(\theta_{0,p}, \theta_{1,p}, \ldots, \theta_{p-1,p}).$$

Beweis. Sei $M := \langle x_1, \ldots, x_N \rangle$ mit $(x_i, x_j) = 1/p\delta_{ij}$, $pM \subset L_C \subset M$ genauer

$$L_C = \{\sum a_i x_i \mid (a_1 + p\mathbb{Z}, \ldots, a_N + p\mathbb{Z}) \in C = \dot{\cup}_{c \in C} \sum c_i x_i + pM.$$

Also ist

$$\Theta_{L_C} = \sum_{c \in C} \Theta_{\sum c_i x_i + pM} = \sum_{c \in C} \prod_{i=1}^{N} \theta_{c_i, p}.$$

□

Beispiel 6.4 *Sei $p = 2$ und*

$$A := \theta_{0,2} = 1 + 2\sum_{a=1}^{\infty} q^{2a^2}, \; B := \theta_{1,2} = \sum_{a=0}^{\infty} 2q^{(2a+1)^2/2}.$$

Dann ist

$$\Theta_{E_8} = \Theta_{L_{e_8}} = p_{e_8}(A, B) = A^8 + 14A^4B^4 + B^8.$$

$A = 1 + 2q^2 + 2q^8 + \ldots$, also $A^4 = 1 + 8q^2 + 4 \cdot 6q^4 + \ldots$ und $A^8 = 1 + 16q^2 + 4 \cdot 28q^4 + \ldots$. Weiter ist $B = 2q^{1/2} + 2q^{9/2} + \ldots$ und daher $B^4 = 16q^2 + 4 \cdot 16q^6 + \ldots$ und $B^8 = 2^8 q^4 + \ldots$. Daher ist

$$\Theta_{E_8} = 1 + (16 + 14 \cdot 16)q^2 + (112 + 14 \cdot 128 + 256)q^4 + \ldots = 1 + 240q^2 + 2160q^4 + \ldots.$$

Lemma 6.5 *Sei L ein Gitter. Setzt man $q = \exp(\pi i z)$ mit $z \in \mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$ so ist die Reihe $\Theta_L : \mathbb{H} \to \mathbb{C}$ absolut und uniform konvergent auf jedem Streifen $\Im(z) \geq v_0 > 0$ und somit eine holomorphe Funktion.*

Beweis. Sei $L = \mathbb{Z}^n M$ für ein $M \in \mathrm{GL}_n(\mathbb{R})$ und $\epsilon := \min_{xx^{tr}=1} xMM^{tr}x^{tr}$. Dann ist $\epsilon > 0$ und $xMM^{tr}x^{tr} \geq \epsilon xx^{tr}$ für alle $x \in \mathbb{R}^n$. Daher erhält man

$$\sum_{\ell \in L} |\exp(\pi i z(\ell, \ell))| = \sum_{x \in \mathbb{Z}^n} |\exp(\pi i z(xM, xM))| \leq \sum_{x \in \mathbb{Z}^n} \exp(-\pi v_0 \epsilon(x, x)) = (\sum_{r=-\infty}^{\infty} \exp(-\pi v_0 \epsilon r^2))^n < \infty.$$

□

Bemerkung 6.6 *Ist L ganz, so ist $\Theta_L(z+2) = \Theta_L(z)$ für alle $z \in \mathbb{H}$ und ist L sogar gerade, so gilt $\Theta_L(z+1) = \Theta_L(z)$.*

Satz 6.7 *(Poisson Summations Formel) Sei $f : \mathbb{R}^n \to \mathbb{C}$ eine Funktion, die die Bedingungen (V1), (V2), (V3) erfüllt. Dann ist für jedes volle Gitter $\Gamma \leq \mathbb{R}^n$*

$$\sum_{x \in \Gamma} f(x) = \det(\Gamma)^{-1/2} \sum_{y \in \Gamma^{\#}} \hat{f}(y)$$

wobei

$$\hat{f}(y) = \int_{\mathbb{R}^n} f(x) \exp(-2\pi i x y^{tr}) dx$$

die Fourier-Transformierte *von f ist und die Bedingungen (V1), (V2), (V3) wie folgt sind:*

(V1) $\int_{\mathbb{R}^n} |f(x)|dx < \infty$ *(damit* $\hat{f}$ *existiert).*

(V2) Die Reihe

$$F(u) := \sum_{x\in\Gamma} f(x+u)$$

konvergiert absolut und uniform auf jedem Kompaktum (damit $F(u)$ *stetig ist).*

(V3) Die Reihe $\sum_{y\in\Gamma^\#} \hat{f}(y)$ *konvergiert absolut.*

Beweis. Wir beweisen den Satz zunächst für $\Gamma = \mathbb{Z}^n$.
Die Funktion $F(u) := \sum_{x\in\mathbb{Z}^n} f(x+u)$ ist nach Voraussetzung (V2) stetig und periodisch in u, $F(u+x) = F(u)$ für $x \in \mathbb{Z}^n$. Also hat F eine Fourier-Entwicklung

$$F(u) = \sum_{y\in\mathbb{Z}^n} \exp(2\pi i(u,y))a(y)$$

wobei $a(y) = \int_{[0,1]^n} F(t)\exp(-2\pi i(t,y))dt$. Wir zeigen, $\hat{f}(y) = a(y)$. Dann gilt nämlich wegen (V3), dass

$$F(0) = \sum_{x\in\mathbb{Z}^n} f(x) = \sum_{y\in\mathbb{Z}^n} \hat{f}(y).$$

Es ist für $y \in \mathbb{Z}^n$

$$\begin{aligned} a(y) &= \int_{[0,1]^n} \sum_{x\in\mathbb{Z}^n} f(x+t)\exp(-2\pi i(t,y))dt \\ &= \sum_{x\in\mathbb{Z}^n} \int_{[0,1]^n} f(x+t)\exp(-2\pi i((x+t),y))dt \\ &= \sum_{x\in\mathbb{Z}^n} \int_{x+[0,1]^n} f(t)\exp(-2\pi i(t,y))dt = \hat{f}(y). \end{aligned}$$

Im allgemeinen Fall ist $\Gamma = \mathbb{Z}^n M$ mit $M \in \mathrm{GL}_n(\mathbb{R})$ und $\Gamma^\# = \mathbb{Z}^n M^{-tr}$. Also ist

$$\sum_{x\in\Gamma} f(x) = \sum_{x\in\mathbb{Z}^n} f(xM) = \sum_{x\in\mathbb{Z}^n} f_M(x) = \sum_{y\in\mathbb{Z}^n} \hat{f}_M(y)$$

wobei

$$\hat{f}_M(y) = \int_{\mathbb{R}^n} f(tM)\exp(-2\pi i(t,y))dt = \frac{1}{|\det(M)|}\int_{\mathbb{R}^n} f(t)\exp(-2\pi i(tM^{-1},y))dt = \det(\Gamma)^{-1/2}\hat{f}(yM^{-tr}$$

□

Satz 6.8 *(Theta Transformationsformel) Es gilt für ein volles Gitter* $L \leq \mathbb{R}^n$

$$\Theta_L(-1/z) = (z/i)^{n/2}\det(L)^{-1/2}\Theta_{L^\#}(z).$$

Beweis. Beide Seiten sind holomorphe Funktionen auf $\mathbb{H}$. Daher genügt es die Identität für $z = it$ mit $t > 0$ nachzuweisen. Die Fouriertransformierte von $f(x) = \exp(\frac{-\pi}{t}(x,x))$ ist $\hat{f}(y) = t^{n/2}\exp(-\pi t(y,y))$ (Übung). Daher erhalten wir mithilfe von Poisson Summation:

$$\begin{aligned} &\Theta_L(\tfrac{-1}{it}) = \textstyle\sum_{x\in L}\exp(\frac{-\pi}{t}(x,x)) = \\ &\det(L)^{-1/2}\textstyle\sum_{y\in L^\#} t^{n/2}\exp(-\pi t(y,y)) = t^{n/2}\det(L)^{-1/2}\Theta_{L^\#}(it). \end{aligned}$$

□

Bemerkung 6.9 *Die Gruppe*

$$\mathrm{SL}_2(\mathbb{Z}) := \langle S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$$

operiert auf der oberen Halbebene durch Möbiustransformationen:

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z := \frac{az+b}{cz+d}.$$

Insbesondere ist

$$Tz = z + 1 \text{ und } Sz = \frac{-1}{z}.$$

Definition 6.10 *Sei $k \in 2\mathbb{Z}_{\geq 0}$. Eine holomorphe Funktion $f : \mathbb{H} \to \mathbb{C}$ heißt* Modulform vom Gewicht *k falls*

(i) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ *für alle* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *und*

(ii) f *hat eine Potenzreihenentwicklung* $f(z) = \sum_{n=0}^{\infty} a_n \exp(2\pi i n z)$.

Bemerkung 6.11 *Eine holomorphe Funktion $f : \mathbb{H} \to \mathbb{C}$ ist genau dann eine Modulform, falls $f(z) = f(z+1)$ und $f(-1/z) = z^k f(z)$ und die wegen der ersten Bedingung existierende Fourierentwicklung $f(z) = \sum_{-\infty}^{\infty} a_n \exp(2\pi i n z)$ die Bedingung $a_n = 0$ für $n < 0$ erfüllt.*

Satz 6.12 *Ist $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter, so ist n durch 8 teilbar.*

Beweis. Sei L so ein Gitter. Angenommen n ist nicht durch 8 teilbar. Indem wir L durch $L \perp L$ oder $L \perp L \perp L \perp L$ ersetzen können wir annehmen, dass $n \equiv_8 4$ ist. Dann ist

$$\Theta_L(-1/z) = (-1)^{n/4} z^{n/2} \Theta_L(z) = -z^{n/2} \Theta_L(z).$$

Also ist

$$\Theta_L((TS)z) = -z^{n/2} \Theta_L(z).$$

Da $(TS)z = (z-1)/z$ und $(TS)^2 z = 1/(1-z)$ ist, ergibt sich daraus

$$\begin{aligned} &\Theta_L((TS)^3 z) = \Theta_L((TS)(TS)^2 z) = -(1/(1-z))^{n/2} \Theta_L((TS)^2 z) \\ &= z^{-n/2} \Theta_L((TS)z) = -\Theta_L(z) \end{aligned}$$

ein Widerspruch da $(TS)^3 = I_2$. □

Satz 6.13 *Ist $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter, so ist Θ_L eine Modulform vom Gewicht $n/2$.*

Beweis. Sei $f := \Theta_L$. Dann ist $f(z) = f(z+1)$, da L ein gerades Gitter ist und f hat eine Fourierentwicklung wie in 6.10 (ii). Wegen der Theta Transformaionsformel ist $f(-1/z) = z^{n/2} f(z)$ (da n durch 8 teilbar ist), also ist f eine Modulform vom Gewicht $n/2$. □

Bemerkung 6.14 *Bezeichne*

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) := \bigoplus_{k=0}^{\infty} \mathcal{M}_k$$

den Ring der Modulformen wobei $\mathcal{M}_k$ den $\mathbb{C}$-Vektorraum der Modulformen vom Gewicht k bezeichnet. Für $f \in \mathcal{M}_k$ und $g \in \mathcal{M}_l$ ist $fg \in \mathcal{M}_{k+l}$, also ist $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ eine $\mathbb{Z}$-graduierte $\mathbb{C}$-Algebra.

Satz 6.15 *(ohne Beweis) $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}[E_4, E_6]$, wo*

$$E_4 = \theta_{E_8} = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n} \in \mathcal{M}_4 \text{ und } E_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^{2n} \in \mathcal{M}_6$$

die Eisensteinreihen bezeichnen. Dabei ist $\sigma_t(n) = \sum_{0<d|n} d^t$ die Summe der t-ten Potenzen der Teiler von n.

Beweis. Ein Beweis findet man in Ebeling, Abschnitte 2.5 und 2.6. □

Folgerung 6.16 *Sei*

$$\Delta := \frac{1}{1728}(E_4^3 - E_6^2) = q^2 \prod_{i=1}^{\infty} (1 - q^{2i})^{24} \in \mathcal{M}_{12}.$$

Ist $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter mit $n = 24a + 8b$, so gibt es Zahlen $c_i \in \mathbb{Q}$ mit

$$\Theta_L = \sum_{i=0}^{a} c_i E_4^{n/8-3i} \Delta^i.$$

Definition 6.17 *Eine Modulform f vom Gewicht k heißt* Spitzenform *, falls $f = \sum_{n=1}^{\infty} q^{2n}$. Bezeichnung: $f \in \mathcal{S}_k$.*

Bemerkung 6.18 *$\mathcal{S} := \bigoplus_{k=1}^{\infty} \mathcal{S}_k = \Delta \mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ ist das von Δ erzeugte Hauptideal in $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.*

6.1 Extremale gerade unimodulare Gitter

Bemerkung 6.19 *Der Raum $\mathcal{M}_{12a+4b}$ $(0 \leq b \leq 2)$ enthält genau eine* extremale Modulform

$$f^*_{12a+4b} = 1 + 0q^2 + \ldots + 0q^{2a} + a^*_{2a+2} q^{2a+2} + \ldots = 1 + \sum_{i=a+1}^{\infty} a^*_{2i} q^{2i}.$$

Beweis. f ist ein Polynom in E_4 und Δ. $f = \sum_{i=0}^{a} c_i E_4^{3a+b-3i} \Delta^i$. Die $a + 1 = \dim(\mathcal{M}_{12a+4b})$ Bedingungen, dass die Koeffizienten von q^{2i} gleich 0 sind $(1 \leq i \leq a)$ und der von q^0 gleich 1 sind linear unabhängig und bestimmen daher die Koeffizienten c_i eindeutig. □

Satz 6.20 *(ohne Beweis) Man kann zeigen, dass der Koeffizient a^*_{2a+2} in der extremalen Modulform von Null verschieden ist.*

Beweis. C.L. Siegel, Berechnung von Zetafunktionen an ganzzahligen Stellen. Nachr. Akad. Wiss. Göttingen, 87-102 (1969). □

Folgerung 6.21 *Sei $L \leq \mathbb{R}^{24a+8b}$ ein gerades unimodulares Gitter mit $0 \leq b \leq 2$. Dann ist $\min(L) \leq 2 + 2a$. Ist $\min(L) = 2a + 2$, so heißt L* extremal.

Die Thetareihe Θ_L eines extremalen Gitters L ist genau die extremale Modulform und insbesondere eindeutig bestimmt. Man kann wieder beweisen, dass für großes Gewicht k, ($k > 20500$) der Koeffizient a^*_{2a+4} in der extremalen Modulform negativ wird (Mallows, Odlysko, Sloane: Upper bounds for modular forms, lattices and codes, J. Algebra 68-76 (1975)). Also gibt es wieder nur endlich viele extremale gerade unimodulare Gitter. In durch 24 teilbaren Dimensionen kennt man bisher 4 solcher Gitter, das Leech Gitter Λ_{24} und 3 gerade unimodulare Gitter in Dimension 48 mit Minimum 6, P_{48p}, P_{48q} und P_{48n}. Ebenso wie bei Codes ist 72 die erste Dimension, in der man nicht weiss, ob ein extremales Gitter existiert.

III Bewertungsringe, insbesondere p-adische Zahlen.

7 Diskrete Bewertungsringe, p-adische Zahlen.

7.1 Lokalisierung

Definition 7.1 *Ein kommutativer Ring heißt* lokal*, falls er nur ein maximales Ideal besitzt.*

Bemerkung 7.2 *Ein kommutativer Ring R ist genau dann lokal, falls $R - R^*$ ein Ideal ist.*

Beweis. Angenommen R besitzt nur ein maximales Ideal $\mathfrak{m}$. Da jedes $x \in R - R^*$ nach Zorns Lemma in einem maximalen Ideal enthalten ist, folgt $x \in \mathfrak{m}$. Also $\mathfrak{m} = R - R^*$. Ist umgekehrt $I := R - R^*$ ein Ideal in R, so enthält I jedes andere Ideal von R. Also ist I das einzige maximale Ideal von R.

Definition 7.3 *Sei R ein Integritätsbereich und $S \subset R$ eine multiplikative Teilmenge, d.h. $0 \notin S$, $1 \in S$ und $xy \in S$ für alle $x, y \in S$. Dann ist $S^{-1}R := \{\frac{r}{s} \in \mathrm{Quot}(R) \mid s \in S\}$ die Lokalisierung von R an S. Via $r \mapsto \frac{r}{1}$ bettet sich R in $S^{-1}R$ ein.*

Ist $S = R - \mathfrak{p}$ für ein Primideal $\mathfrak{p}$ von R so schreiben wir auch $R_\mathfrak{p}$ (lies: die Lokalisierung von R an $\mathfrak{p}$).

Bemerkung 7.4 *Die Lokalisierung $S^{-1}R$ ist der kleinste Teilring von $\mathrm{Quot}(R)$ der R enthält und in dem alle Elemente aus S invertierbar sind. Weiter gibt es eine Bijektion*

$$\begin{array}{ccc} \{\mathfrak{p} \trianglelefteq R \mid \mathfrak{p} \text{ prim und } \mathfrak{p} \cap S = \emptyset\} & \longleftrightarrow & \{I \trianglelefteq S^{-1}R \mid I \text{ prim}\} \\ \mathfrak{p} & \longrightarrow & \mathfrak{p} \cdot (S^{-1}R) = \{\frac{r}{s} \mid s \in S, r \in \mathfrak{p}\} \\ I \cap R & \longleftarrow & I \end{array}$$

Beweis. Daß $S^{-1}R$ ein Teilring von $\mathrm{Quot}(R)$ ist, rechnet man leicht nach. Dann ist es per Definition auch der kleinste Teilring von $\mathrm{Quot}(R)$ der $R \cup \{\frac{1}{s} \mid s \in S\}$ umfaßt.

Zeigen wir nun die Bijektion der Primideale. Sei $\varphi\colon R \to S^{-1}R, r \mapsto \frac{r}{1}$ der kanonische Monomorphismus. Dann ist $\varphi^{-1}(I) = I \cap R$ für jedes Primideal I von $S^{-1}R$ ebenfalls ein Primideal. Weiter ist $S \cap \varphi^{-1}(I) = \emptyset$, denn andernfalls existiert ein $s \in S$ mit $\frac{s}{1} \in I$. Aber dann wäre $I = S^{-1}R$ was nicht sein kann.

Sei umgekehrt $\mathfrak{p}$ ein Primideal von R mit $\mathfrak{p} \cap S = \emptyset$. Setze $I := \mathfrak{p} \cdot S^{-1}R = \{\frac{r}{s} \mid s \in S, r \in \mathfrak{p}\}$. Dies ist wohldefiniert, denn ist $\frac{r}{s} = \frac{r'}{s'}$ mit $s, s' \in S$, so gilt wegen $s, s' \notin \mathfrak{p}$:

$$\frac{r}{s} \in I \iff r \in \mathfrak{p} \iff rs' \in \mathfrak{p} \overset{rs'=r's}{\iff} r's \in \mathfrak{p} \iff r' \in \mathfrak{p} \iff \frac{r'}{s'} \in I$$

Sicher ist I ein Ideal. Wir wollen nun zu zeigen, daß I ein Primideal ist. Sicher ist $I \neq S^{-1}R$, denn sonst gäbe es ein $s \in S$ mit $1 = \frac{s}{s} \in I$ was der Wahl von I widerspricht. Seien nun $\frac{r}{s}, \frac{r'}{s'} \in S^{-1}R$ mit $\frac{r}{s} \notin I$ aber $\frac{rr'}{ss'} \in I$. Dann ist $r \notin \mathfrak{p}$ aber $rr' \in \mathfrak{p}$, also $r' \in \mathfrak{p}$ und damit $\frac{r'}{s'} \in I$. Weiter ist $\varphi^{-1}(I) = I \cap R = \mathfrak{p}$ und für ein Primideal J von $S^{-1}R$ ist $\varphi^{-1}(J) \cdot S^{-1}R = J$. Also sind die beiden Zuordnungen invers zueinander.

Folgerung 7.5 *Ist $\mathfrak{p}$ ein Primideal von R, so ist $R_\mathfrak{p}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$ und es ist $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$.*

Beweis. Die Primideale von $R_\mathfrak{p}$ sind gegeben durch $\mathfrak{q}R_\mathfrak{p}$ wobei $\mathfrak{q}$ ein Primideal von R ist mit $\mathfrak{q} \subseteq \mathfrak{p}$. Also ist $\mathfrak{p}R_\mathfrak{p}$ das einzige maximale Ideal von $R_\mathfrak{p}$. Sei $R \to R_\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ die Komposition der kanonischen Morphismen. Die Abbildung ist nicht 0 und damit surjektiv da $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ ein Körper ist. Weiter ist der Kern gerade $R \cap \mathfrak{p}R_\mathfrak{p} = \mathfrak{p}$.

Beispiel 7.6 *Sie p eine Primzahl. Dann ist $\mathbb{Z}_{(p)} = \{\frac{r}{s} \mid r, s \in \mathbb{Z}, p \nmid s\}$ die Lokalisierung von $\mathbb{Z}$ an $(p) = p\mathbb{Z}$. Das maximale Ideal ist $p\mathbb{Z}_{(p)}$ und es ist $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$.*

7.2 Diskrete Bewertungen

Definition 7.7 *Sei K ein Körper. Eine surjektive Abbildung $v\colon K \to \mathbb{Z} \cup \{\infty\}$ heißt* diskrete Bewertung *von K, falls für alle $x, y \in K$ gilt*

1. $v(x) = \infty \iff x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \geq \min\{v(x), v(y)\}$

In diesem Fall ist $R_v := \{x \in K \mid v(x) \geq 0\} = v^{-1}(\mathbb{Z}_{>0} \cup \{\infty\})$ der Bewertungsring von v.

Ein Integritätsbereich R heißt diskreter Bewertungsring, *falls es eine diskrete Bewertung w des Quotientenkörpers* $\mathrm{Quot}(R)$ *gibt mit $R = R_w$.*

Bemerkung 7.8 *Sei $v\colon K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung.*

1. *Es ist R_v ein lokaler Ring mit Einheitengruppe $R_v^* := v^{-1}(\{0\})$ und maximalem Ideal $\mathfrak{m}_v := v^{-1}(\mathbb{Z}_{>0} \cup \{\infty\})$.*
2. *Sind $x, y \in K$ mit $v(x) \neq v(y)$, so ist $v(x + y) = \min\{v(x), v(y)\}$.*

Beweis.

1. Sicher ist $0 \in R_v$. Wegen $v(1) = v(1) + v(1)$ ist $v(1) = 0$, also $1 \in R_v$. Sind weiter $x, y \in R_v$ d.h. $v(x), v(y) \geq 0$ so ist auch $v(xy) = v(x) + v(y) \geq 0$ und $v(x + y) \geq \min\{v(x), v(y)\} \geq 0$. Also ist R_v ein Teilring von K.

Weiter gilt für jedes $x \in K^*$: $0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1})$ also $v(x^{-1}) = -v(x)$. Damit folgt $u \in R_v^* \iff u, u^{-1} \in R \iff v(u), v(u^{-1}) \geq 0 \iff v(u) = 0$.

Also ist $R_v^* := v^{-1}(\{0\})$ und damit ist $\mathfrak{m}_v = R_v - R_v^*$. Genauso wie zu Beginn des Beweises zeigt man, daß $\mathfrak{m}_v$ ein Ideal von R_v ist. Daher ist R_v lokal.

2. Seien $x, y \in K$ mit $v(x) < v(y)$. Dann folgt

$$v(x) = v((x+y) - y) \geq \min\{v(x+y), v(y)\} \geq \min\{\min\{v(x), v(y)\}, v(y)\} = v(x) \, .$$

Also ist $v(x) = \min\{v(x+y), v(y)\}$ und somit $v(x+y) = v(x)$.

Der Quotient $k_v := R_v/\mathfrak{m}_v$ ist also ein Körper, der sogenannte Restklassenkörper von v.

Beispiel 7.9

1. *Sei p eine Primzahl. Dann ist jedes $x \in \mathbb{Q}^*$ von der Form $x = p^{v_p(x)} \frac{r}{s}$ mit $v_p(x) \in \mathbb{Z}$ und $p \nmid r,\ p \nmid s$. Setzen wir noch $v_p(0) = \infty$, so ist v_p eine diskrete Bewertung auf $\mathbb{Q}$ (sog. p-adische Bewertung) mit Bewertungsring $\mathbb{Z}_{(p)}$. Ferner sind alle diskreten Bewertungen von $\mathbb{Q}$ von dieser Gestalt (Übung).*

2. *Im allgemeinen wird nicht jede diskrete Bewertung von Primidealen induziert:*
Sei $K(X)$ der Körper der rationalen Funktionen über einem Körper K. Dann ist $v\colon K(X) \mapsto \mathbb{Z} \cup \{\infty\},\ \frac{f}{g} \mapsto \deg(f) - \deg(g)$ eine diskrete Bewertung mit Bewertungsring $\{\frac{f}{g} \mid f, g \in K[X], \deg(g) \leq \deg(f)\} \neq K[X]_{(f)}$ für alle irreduziblen $f \in K[X]$.

Wir geben nun eine Charakterisierung von diskreten Bewertungsringen:

Satz 7.10 *Es sei R ein Ring aber kein Körper. Dann sind folgende Aussagen äquivalent.*

1. *R ist diskreter Bewertungsring.*
2. *R ist Hauptidealbereich mit genau einem Primideal.*
3. *R ist ein lokaler Hauptidealbereich.*
4. *R ist ein noetherscher, lokaler Integritätsbereich und das maximale Ideal ist ein Hauptideal.*
5. *R ist lokaler Integritätsbereich mit maximalem Ideal $\mathfrak{m}$. Dieses ist ein Hauptideal und erfüllt $\bigcap_{k=0}^{\infty} \mathfrak{m}^k = (0)$.*
6. *R ist Integritätsbereich und es existiert ein $\pi \in R$ so, daß jedes $x \in R - \{0\}$ eine eindeutige Faktorisierung $x = \pi^k u$ mit $k \in \mathbb{N}_0$ und $u \in R^*$ besitzt.*
7. *R ist lokaler noetherscher Integritätsbereich mit maximalem Ideal $\mathfrak{m}$. Weiter bilden $\mathfrak{m}^k$ $(k \in \mathbb{N}_0)$ alle von (0) verschiedenen Ideale von R.*

Beweis. Es gilt 2. $\Rightarrow$ 3. da maximale Ideale Primideale sind. Da Hauptidealbereiche noethersch sind folgt 3. $\Rightarrow$ 4.. Ebenso ist 6. $\Rightarrow$ 7. klar.

1. $\Rightarrow$ 2.: Wähle $\pi \in R$ mit $v(\pi) = 1$. Ist $I \neq (0)$ ein Ideal von R, so setze $k := \min\{v(r) \mid r \in I\}$. Dann gilt für alle $r \in I$, daß $v(r\pi^{-k}) = v(r) - k \geq 0$. Daher ist $r\pi^{-k} \in R$ und somit $I \subseteq (\pi^k)$. Umgekehrt gibt es ein $r \in I$ mit $v(r) = k$. Dann ist $v(\pi^k r^{-1}) = 0$ und somit $\pi^k r^{-1} \in R^*$. Damit ist $\pi^k \in (r) \subseteq I$. Zusammen folgt $I = (\pi^k)$. Wir haben also gezeigt, daß alle Ideale $I \neq (0)$ von R gegeben sind durch $\{(\pi^k) \mid k \in \mathbb{N}_0\}$. Daher ist R ein Hauptidealbereich und (π) sein einziges Primideal.

4. $\Rightarrow$ 5.: Sei $\mathfrak{m} = (\pi)$. Weiter sei $x \in \mathfrak{m}^k$ für alle $k \geq 0$. Dann existieren $r_k \in R$ mit $x = r_k\pi^k$. Also ist $r_k\pi^k = r_{k+1}\pi^{k+1}$ und somit $(r_k) = (\pi r_{k+1}) \subseteq (r_{k+1})$. Die Kette $(r_1) \subseteq (r_2) \subseteq \ldots$ stabilisiert bei einem Index i. Dann ist $(r_{i+1}) = (r_i) = \pi(r_{i+1})$, was wegen $\pi \notin R^*$ aber $(r_{i+1}) = 0$ impliziert. Damit ist $x = 0$.

5. $\Rightarrow$ 6.: Sei $\mathfrak{m} = (\pi)$ und $0 \neq x \in R$. Dann ist $k := \max\{i \geq 0 \mid x \in \mathfrak{m}^i\}$ endlich. Also ist $x = \pi^k u$ mit $u \in R$. Wegen $x \notin \mathfrak{m}^{k+1}$ ist $u \in R - \mathfrak{m} = R^*$. Angenommen es wäre $\pi^k u = \pi^\ell v$ mit $\ell \in \mathbb{N}_0$ und $v \in R^*$. Ohne Einschränkung ist $k \geq \ell$. Es folgt $R = (\pi^{k-\ell})$ und damit $k = \ell$ was $v = u$ impliziert.

7. $\Rightarrow$ 6.: Das maximale Ideal $\mathfrak{m}$ ist endlich erzeugt, sagen wir $\mathfrak{m} = (r_1, \ldots, r_t)$ mit t minimal. Ist $t > 1$, so wäre $(r_1, \ldots, r_{t-1}) = \mathfrak{m}^k$ und $(r_t) = \mathfrak{m}^\ell$ für $k, \ell \geq 0$. Aber dann ist $\mathfrak{m}^k \subseteq \mathfrak{m}^\ell$ oder aber $\mathfrak{m}^\ell \subseteq \mathfrak{m}^k$. Das widerspricht der Minimalität von t. Also ist $t = 1$ und $\mathfrak{m} = (\pi)$ somit ein Hauptideal. Damit besitzt jedes Element in R eine geforderte Faktorisierung. Die Eindeutigkeit dieser zeigt man wie zuvor,

6. $\Rightarrow$ 1.: Jedes $0 \neq x \in \mathrm{Quot}(R)$ besitzt also eine eindeutige Darstellung der Form $u\pi^{v(x)}$ mit $u \in R^*$ und $v(x) \in \mathbb{Z}$. Setzen wir noch $v(0) = \infty$, so ist v eine diskrete Bewertung mit $R_v = R$.

Zusammenfassung Ist v eine diskrete Bewertung auf einem Körper K und $\pi \in R_v$ mit $v(\pi) = 1$, so sind alle Ideale von R_v ungleich (0) gegeben durch $\{\pi^k R_v \mid k \in \mathbb{N}_0\}$. Weiter hat jedes $x \in K$ eine eindeutige Darstellung der Form $x = \pi^k u$ mit $u \in R_v^*$ und $k \in \mathbb{Z}$. Das Element π ist dann ein Primelement von R_v.

7.3 Vollständige diskrete Bewertungen

Sei v eine diskrete Bewertung auf einem Körper K. Wir setzen $|x|_v := \exp(-v(x))$ für $x \in K$. Dann ist $d\colon K \to \mathbb{R}_{>0},\ (x, y) \mapsto |x - y|_v$ eine Metrik auf K. (Die von $(x, y) \mapsto a^{-v(x-y)}$ mit $a > 1$ induzierte Topologie auf K ist unabhängig von a. Die Wahl $a = \exp(1)$ ist also willkürlich.)

Es ist also $x \in K$ nah bei 0, falls $v(x)$ groß ist.

Definition 7.11 *Sei v eine diskrete Bewertung auf einem Körper K.*

1. *Eine Folge $(a_n)_{n\in\mathbb{N}}$ in K heißt* Cauchy-Folge, *falls es zu jedem $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt mit $|a_n - a_{n+i}|_v \leq \varepsilon$ für alle $n \geq N$ und $i \in \mathbb{N}$.*

2. *Eine diskrete Bewertung v auf einen Körper K heißt vollständig, falls die durch v induzierte Topologie vollständig ist, d.h. jede Cauchy-Folge in K besitzt einen Grenzwert in K.*

Bemerkung 7.12 *Sei v eine diskrete Bewertung auf einem Körper K.*

1. *Die Abbildung $|\ |_v \colon K \to \mathbb{R}_{\geq 0}$ ist ein Betrag, der die verschärfte Dreiecksungleichung erfüllt. D.h. für $x, y \in K$ gilt:*
   (a) $|x|_v = 0 \iff x = 0$.
   (b) $|xy|_v = |x|_v \cdot |y|_v$.
   (c) $|x + y|_v \leq \max\{|x|_v, |y|_v\}$ *und es gilt Gleichheit, falls* $|x|_v \neq |y|_v$.
2. *Eine Folge $(a_n)_{n\in\mathbb{N}}$ in K ist genau dann eine Cauchy-Folge, falls $|a_n - a_{n+1}|_v \to 0$ für $n \to \infty$.*
3. *Ist $(a_n)_{n\in\mathbb{N}}$ in K eine Cauchy-Folge, so ist $(|a_n|_v)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $\mathbb{R}$.*

Beweis.

1. Folgt aus Definition 7.7 und Bemerkung 7.8.
2. Ist $\varepsilon > 0$ so existiert ein $N > 0$ mit $|a_k - a_{k+1}|_v \leq \varepsilon$ für alle $k \geq N$. Für $n \geq N$ und $i \in \mathbb{N}$ ist dann
$$\begin{aligned} |a_n - a_{n+i}|_v &= |(a_n - a_{n+1}) + (a_{n+1} - a_{n+2}) + \cdots + (a_{n+i-1} - a_{n+i})|_v \\ &\leq \max\{|a_k - a_{k+1}|_v \mid n \leq k \leq n + i - 1\} \leq \varepsilon\,. \end{aligned}$$
   Also ist (a_n) eine Cauchy-Folge.
3. Sind $x, y \in K$ so ist $|x|_v \leq |x - y|_v + |y|_v$ also $|x|_v - |y|_v \leq |x - y|_v$. Durch Vertauschen von x und y erhalten wir dann $||x|_v - |y|_v| \leq |x - y|_v$.
   Damit ist $||a_n|_v - |a_{n+i}|_v| \leq |a_n - a_{n+i}|_v \leq \varepsilon$ für $i \in \mathbb{N}$ und n genügend groß.

Satz 7.13 *Sei v eine diskrete Bewertung auf K. Dann gibt einen Oberkörper $\hat{K}$ von K und eine vollständige diskrete Bewertung w auf $\hat{K}$ mit $w|_K = v$ so, daß K dicht in $\hat{K}$ liegt. Man nennt $\hat{K}$ die Vervollständigung (oder Komplettierung) von K. Weiter haben die beiden Bewertungen v und w isomorphe Restklassenkörper.*

Beweis. Idee: Bezeichne $\mathcal{X}$ den Ring der Cauchy-Folgen in K und $\mathcal{N}$ das Ideal der Nullfolgen. Wir behaupten, daß $\mathcal{N}$ ein maximales Ideal ist. Denn ist $(a_n) \in \mathcal{X} - \mathcal{N}$, so existiert $\delta > 0$ und ein $N \in \mathbb{N}$ mit $|a_n|_v \geq \delta$ für alle $n \geq N$ (Übung). Wir setzen $b_n := a_n^{-1}$ für $n \geq N$ und $b_n = 0$ sonst. Dann ist (b_n) eine Cauchy-Folge, denn $|b_n - b_{n+1}|_v = \frac{|a_{n+1} - a_n|_v}{|a_n|_v \cdot |a_{n+1}|_v} \leq \delta^{-2}|a_{n+1} - a_n|_v \to 0$ für $n \to \infty$. Weiter ist dann $(1) + \mathcal{N} = (a_n)(b_n) + \mathcal{N}$ d.h. das von $\mathcal{N}$ und (a_n) erzeugte Ideal ist $\mathcal{X}$. Da (a_n) beliebig war, ist $\mathcal{N}$ maximal, also $\hat{K}$ ein Körper.

Die Menge $\{|x|_v \mid x \in K\} = \{0\} \cup \{\exp(k) \mid k \in \mathbb{Z}\}$ ist diskret und 0 ihr einziger Häufungspunkt. Ist $(a_n) \in \mathcal{X} - \mathcal{N}$, so konvergiert $(|a_n|_v)_n$ in $\mathbb{R}$, aber nicht gegen 0, da die Folge (ab einem gewissen Index) nach unten beschränkt ist. Damit wir $(|a_n|_v)_n$ konstant. Also existiert $w((a_n)+\mathcal{N}) := \lim_{n\to\infty} v(a_n)$ (in $\mathbb{Z}$!) und ist nach Bemerkung 7.7 unabhängig von der Wahl des Vertreters. Betten wir K via $a \mapsto \iota(a) := (a)_{n\in\mathbb{N}} + \mathcal{N}$ in $\hat{K}$ ein, so ist w eine Fortsetzung von v und man rechnet nach, daß w eine diskrete Bewertung auf $\hat{K}$ ist.

Zeigen wir nun, daß K dicht liegt in $\hat{K}$. Seien dazu $x := (a_n) + \mathcal{N} \in \hat{K}$ und $\varepsilon > 0$ beliebig. Dann existiert ein $N \in \mathbb{N}$ mit $|a_n - a_{n+i}|_v \leq \varepsilon$ für alle $i \in \mathbb{N}$ und $n \geq N$. Dann ist $|x - \iota(a_n)|_w = \lim_{i\to\infty} |a_i - a_n|_v \leq \varepsilon$ für alle $n \geq N$. Also konvergiert $(\iota(a_n))_n$ gegen die Restklasse x.

Mit dieser Bemerkung zeigen wir nun, daß $\hat{K}$ vollständig ist. Sei dazu $(x_n)_n$ eine Cauchy-Folge in $\hat{K}$. Nach dem gerade Gezeigten existieren $a_n \in K$ mit $|x_n - \iota(a_n)|_w < 1/n$. Zu einem $\varepsilon > 0$ gibt es dann $N > 1/\varepsilon > 0$ mit $|x_n - x_{n+i}|_w < \varepsilon$. Für $i \in \mathbb{N}$ und $n > N$ gilt dann

$$|a_n - a_{n+i}|_v \leq |\iota(a_n) - x_n|_w + |x_n - x_{n+i}|_w + |x_{n+i} - \iota(a_{n+i})|_w < 1/n + \varepsilon + 1/(n+i) \leq 3\varepsilon$$

Also ist $(a_n)_n \in \mathcal{X}$. Setzen wir $a := (a_n)_n + \mathcal{N} \in \hat{K}$ so ist

$$|x_n - a|_w \leq |x_n - \iota(a_n)|_w + |\iota(a_n) - a|_w \to 0 \text{ für } n \to \infty\,.$$

Sei nun π ein Primelement in R_v. Dann ist dies auch ein Primelement von R_w und es gilt $\pi R_v = R_v \cap \pi R_w$. Damit hat $R_v \xrightarrow{\iota} R_w \to R_w/\pi R_w$ den Kern πR_v und die Abbildung ist nicht 0, da die Einselemente aufeinander abgebildet werden. Damit ist $R_v/\pi R_v \cong R_w/\pi R_w$.

Hinweis: Man kann auch zeigen, daß $\hat{K}$ im Wesentlichen eindeutig ist.

Beispiel 7.14 *Sei $\mathbb{Q}$ versehen mit der p-adischen Bewertung. Die Vervollständigung $\mathbb{Q}_p$ heißt der* Körper der p-adischen Zahlen. *Wir bezeichnen den zugehörigen Bewertungsring mit $\mathbb{Z}_p$. Dann ist $p\mathbb{Z}_p$ das maximale Ideal von $\mathbb{Z}_p$ und es ist $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$.*

Wir beschreiben nun die Elemente in $\mathbb{Q}_p$ genauer. Sei zunächst $x \in \mathbb{Z}_p$. Wegen $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ existiert ein $a_0 \in \{0,\ldots,p-1\}$ mit $x - a_0 \in p\mathbb{Z}_p$ (wir fassen $\mathbb{Q}$ als Teilkörper von $\mathbb{Q}_p$ auf). Dann ist $p^{-1}(x-a_0) \in \mathbb{Z}_p$ und es existiert ein $a_i \in \{0,\ldots,p-1\}$ mit $x - a_0 - pa_1 \in p\mathbb{Z}_p$ usw. Damit konvergiert die Folge (x_n) mit $x_n := \sum_{i=0}^{n} a_i p^i \in \mathbb{Q}$ in $\mathbb{Q}_p$ gegen x. Also ist $x = \sum_{i=0}^{\infty} a_i p^i$ mit $0 \leq a_i < p$ stets. Sei nun $x \in \mathbb{Q}_p$. Dann existiert ein $k \geq 0$ mit $xp^k \in \mathbb{Z}_p$.

Also ist jedes $x \in \mathbb{Q}_p$ von der Gestalt $x = \sum_{i=k}^{\infty} a_i p^i$ mit $0 \leq a_i < p$ und $k \in \mathbb{Z}$ (sog. p-adische Entwicklung*). Weiter ist die p-adische Bewertung von x gerade* $\min\{i \geq k \mid a_i \neq 0\}$.

Diese p-adische Entwicklung von x entspricht genau der Dezimalentwicklung von reellen Zahlen. Mit dem wichtigen Unterschied, daß die Darstellung bei p-adischen Zahlen eindeutig ist. Denn, definieren $x_{k+n} := \sum_{i=k}^{n} a_i p^i$ und $x'_{k'+n} := \sum_{i\geq k'}^{n} a'_i p^i$ zwei verschiedene Folgen von Partialsummen mit $0 \leq a_i, a'_i \leq p-1$, so ist ohne Einschränkung $k = k'$. Wähle nun i minimal mit $a_i \neq a'_i$. Ohne Einschränkung ist dann $1 \leq a_i - a'_i \leq p-1$, also $x_n - x'_n \notin p^i\mathbb{Z}_p$ für alle $n \geq k+i$. Somit konvergieren die beiden Folgen nicht gegen denselben Grenzwert.

Mit dieser Reihendarstellung kann man z.B. leicht $-\frac{1}{4} \in \mathbb{Z}_7$ bestimmen. Denn es ist $7^2 - 1 = 4 \cdot 12$, also

$$-\frac{1}{4} = 12 \cdot (1-7^2)^{-1} = \sum_{i=0}^{\infty} 12 \cdot 7^{2i} = \sum_{i=0}^{\infty} (5 \cdot 7^0 + 7^1) \cdot 7^{2i}\,.$$

Eine wichtige Eigenschaft von vollständigen Bewertungen ist die Tatsache, daß man Nullstellen liften kann.

Satz 7.15 (Hensels Lemma) *Sei v eine vollständige diskrete Bewertung mit Bewertungsring R. Weiter sei $f(x) \in R[x]$ und $a_0 \in R$ mit*

$$v(f(a_0)) > 2v(f'(a_0)).$$

Dann konvergiert die durch

$$a_n := a_{n-1} - f(a_{n-1})/f'(a_{n-1}) \text{ für alle } n \in \mathbb{N}$$

definierte Folge gegen ein $a \in R$ mit $f(a) = 0$.

Beweis. Es ist $f(x) = \sum_{i=0}^{m} f_i x^i$ und $f'(x) = \sum_{i=1}^{m} i f_i x^{i-1}$.

Dann ist $f(x + a_0) = f(a_0) + c_1 x + x^2 g(x)$ mit $c_1 \in R$ und $g(x) \in R[x]$. Der Koeffizient von x in $f(x + a_0)$ ist $\sum_{i=1}^{m} f_i \binom{i}{1} a_0^{i-1} = f'(a_0)$, also ist

$$f(x + a_0) = f(a_0) + f'(a_0)x + x^2 g(x)\,.$$

Sei $b_n := a_n - a_{n-1} = -f(a_{n-1})/f'(a_{n-1})$. Dann ist

$$v(b_1) = v(f(a_0)) - v(f'(a_0)) > v(f'(a_0)) \geq 0 \text{ und } v(b_1) > \frac{1}{2} v(f(a_0)) \geq 0.$$

Insbesondere gilt $b_1 \in R$ und somit $a_1 = a_0 + b_1 \in R$. Weiter ist

$$v(f(a_1)) = v(f(a_0 + b_1)) = v(\underbrace{f(a_0) + f'(a_0)b_1}_{=0} + b_1^2 g(b_1)) \geq 2v(b_1) > v(f(a_0)).$$

Analog ist $f'(x + a_0) = f'(a_0) + xh(x)$ mit $h(x) \in R[x]$. Damit wird

$$v(f'(a_1)) = v(f'(a_0 + b_1)) = v(f'(a_0) + b_1 h(b_1)) = \min\{v(f'(a_0)), v(b_1) + v(h(b_1))\} = v(f'(a_0))$$

da $v(b_1) > v(f'(a_0))$. Also erfüllt $a_1 = a_0 + b_1$ die Voraussetzung des Satzes und das Verfahren konstruiert eine Folge von Zahlen $a_0, a_1, \ldots$ mit

$$v(f(a_0)) < v(f(a_1)) < \ldots$$

d.h. $f(a_n) \to 0$ mit $n \to \infty$.

Wegen $v(a_{n+1} - a_n) = v(b_{n+1}) > \frac{1}{2} v(f(a_n)) \to \infty$ mit $n \to \infty$ ist (a_n) nach Bemerkung 7.12 eine Cauchy-Folge in K. Also konvergiert sie gegen ein $a \in K$. Wegen $a_n \in R$ ist $|a_n|_v \leq 1$ für alle $n \geq 0$ also auch $|a|_v \leq 1$ und somit $a \in R$.

In den Übungen zeigen wir einige Abschätzungen über die Güte der n-ten Näherung a_n.

Beispiel 7.16 *Sei $p \equiv 1 \mod 4$ eine Primzahl. Wir wollen $-1 \in (\mathbb{Z}_p^*)^2$ zeigen.*

Es bezeichne v die p-adische Bewertung auf $\mathbb{Q}_p$ und wir setzen $f(x) = x^2 + 1$. Dann existiert ein $a_0 \in \mathbb{Z} - p\mathbb{Z}$ mit $f(a_0) \equiv 0 \mod p$ wie wir bereits wissen. Nun ist $v(f'(a_0)) = v(2a_0) = 0$ aber $v(f(a_0)) \geq 1$. Also liftet diese Nullstelle a_0 zu einer Nullstelle $a \in \mathbb{Z}_p$.

IV Quadratische Formen

8 Quadratische Formen.

8.1 Symmetrische Bilinearformen.

Sei A ein kommutativer Ring mit 1, also z.B. A ein Körper ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_q$) oder ein Hauptidealbereich ($\mathbb{Z}$, $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}$ oder auch die Komplettierung $\mathbb{Z}_p$, der Ring der p-adischen ganzen Zahlen.) und sei E ein endlich erzeugter A-Modul.

Definition 8.1 *$b : E \times E \to A$ heißt* symmetrische Bilinearform*, falls für alle $x, y, z \in E, a \in A$ gilt*

$$b(x, y) = b(y, x) \text{ und } b(ax + y, z) = ab(x, z) + b(y, z).$$

Sind (E, b) und (E', b') bilineare A-Moduln, so heißt eine injektive A-lineare Abbildung $\varphi : E \to E'$ eine Isometrie*, falls $b'(\varphi(x), \varphi(y)) = b(x, y)$ für alle $x, y \in E$.*
(E, b) und (E', b') heißen isometrisch*, falls eine bijektive Isometrie $\varphi : E \to E'$ existiert.*
$O(E) := \{\varphi : E \to E \mid \varphi$ ist bijektive Isometrie $\}$ heißt die orthogonale Gruppe von E.

Beispiele für bilineare Moduln sind:
Gitter: $E = L, b = (,), A = \mathbb{Z}$
Codes: $E = \mathbb{F}_q^n, b = \cdot, A = \mathbb{F}_q$

Definition 8.2 *Sei (E, b) ein bilinearer A-Modul.*
(a) $x, y \in E$ heißen orthogonal*, falls $b(x, y) = 0$.*
(b) Für $F \subset E$ sei $F^\perp := \{x \in E \mid b(x, y) = 0$ für alle $y \in F\}$ der orthogonale Untermodul*.*
(c) E heißt orthogonale Summe*, $E = E_1 \perp \ldots \perp E_n$, falls $E = E_1 \oplus \ldots \oplus E_n$ eine direkte Summe ist und $b(x, y) = 0$ für $x \in E_i, y \in E_j, i \neq j$.*
(d) $E^* := \mathrm{Hom}_A(E, A)$ heißt der zu E duale Modul*.*
(e) Für $x \in E$ und $F \leq E$ sei $b_F(x) : F \to A, y \mapsto b(x, y) \in F^*$.

Bemerkung 8.3 *Sei $F \leq E$. $b_F : E \to F^*, x \mapsto b_F(x)$ ist ein A-Modulhomomorphismus mit $\ker(b_F) = F^\perp$.*

Lemma 8.4 *Sei $F \leq E$. Dann ist $E = F \perp F^\perp$ genau dann wenn $b_F(E) = b_F(F)$ und $F \cap F^\perp = \{0\}$.*

Beweis. $\Rightarrow$ ist klar. Für $\Leftarrow$ müssen wir zeigen, dass jedes $x \in E$ als Summe $x = y + y'$ mit $y \in F$ und $y' \in F^\perp$ geschrieben werden kann. Aber die Bedingung $b_F(E) = b_F(F)$ sagt aus, dass es ein $y \in F$ gibt mit $b_F(x) = b_F(y)$, mit anderen Worten $x - y \in \ker(b_F) = F^\perp$. $\square$

Definition 8.5 *(a)* (E, b) *heißt* nicht ausgeartet, *falls* b_E *injektiv ist, also falls* $E^\perp = \{0\}$ *ist.*
(b) (E, b) *heißt* regulär, *falls* b_E *bijektiv ist.*

Bemerkung 8.6 *(a) Ist* A *ein Körper und* E *endlich dimensional über* K*, so ist* (E, b) *genau dann nicht ausgeartet, wenn* (E, b) *regulär ist, genau dann wenn sein* Radikal $E^\perp := \{e \in E \mid b(e, x) = 0 \text{ für alle } x \in E\}$ *gleich 0 ist.*
(b) Jedes ganze $\mathbb{Z}$*-Gitter* $L \leq (\mathbb{R}^n, (,))$ *im Euklidischen Raum nicht ausgeartet.* L *ist regulär, genau dann wenn* $L = L^\#$

Satz 8.7 *Ist* $F \leq E$ *so dass* $(F, b_{|F\times F})$ *regulär ist, dann ist* $E = F \perp F^\perp$

Beweis. F ist regulär genau dann wenn $b_F : F \to F^*$ bijektiv ist. Also ist dann auch $b_F(E) = b_F(F)$ und $\ker((b_F)_{|F}) = F \cap F^\perp = \{0\}$ und damit $E = F \perp F^\perp$ nach Lemma 8.4. □

Beispiel: Ist L ein ganzes Gitter und $M \leq L$ ein Teilgitter (nicht vollen Rangs) so dass $M \leq \mathbb{R}M$ mit der Einschränkung des Skalarprodukts von L ein unimodulares Gitter ist, so ist $L = M \perp M^\perp$.

Bemerkung 8.8 *Der duale Modul der direkten Summe* $E := \bigoplus_{i=1}^n E_i$ *ist* $E^* \cong \bigoplus_{i=1}^n E_i^*$*. Insbesondere ist* $E = \perp_{i=1}^n E_i$ *nicht ausgeartet (bzw. regulär), genau dann wenn* E_i *nicht ausgeartet (bzw. regulär) ist für alle* i*.*

Satz 8.9 *Sei* E *ein freier* A*-Modul über einem lokalen Ring* A *mit maximalem Ideal* I*. Dann ist* $E = E_1 \perp \ldots \perp E_r \perp F$ *mit* $b(F, F) \subset I$*,* E_i *regulär* $\dim(E_i) = 1$ *oder* 2*. Ist* $2 \in A^*$*, so können alle* E_i *eindimensional gewählt werden. Es gilt:* E *ist regulär genau dann wenn* $F = 0$*.*

Beweis. Induktion über $n := \dim(E)$.
$n = 0$: Dann ist nichts zu zeigen.
Sein $n > 0$. (a) Ist $b(E, E) \subset I$, so setze $F := E$ und wir sind fertig.
(b) Ist $b(E, E) \not\subset I$, so gibt es entweder ein $e \in E$ mit $b(e, e) \in A^*$. Dann ist aber $\langle e\rangle$ regulär und damit $E = \langle e\rangle \perp \langle e\rangle^\perp$ und $\dim\langle e\rangle^\perp = n - 1$. Mit Induktion folgt dann die Behauptung.
(c) Bleibt der Fall wo $b(e, e) \in I$ liegt für alle $e \in E$ aber $b(E, E) \not\subset I$. Dann gibt es $e, f \in E$ mit $b(e, f) \in A^*$ und es ist $\langle e, f\rangle =: H \leq E$ ein regulärer Teilmodul mit $E = H \perp H^\perp$. Da $\dim(H^\perp) = n - 2$ folgt die Behauptung wieder mit Induktion.
Der Fall (c) tritt für $\mathrm{char}(A/I) \neq 2$ nicht auf, da dann mit $b(e, f)$ auch $2b(e, f) \in A^*$ ist jedoch

$$2b(e, f) = b(e + f, e + f) - b(e, e) - b(f, f) \in I$$

einen Widerspruch liefert. □

8.2 Reguläre Bilineare Räume über endlichen Körpern.

Sei $A = \mathbb{F}_q$, $\mathrm{char}(A) = p$, $q = p^f$.

Lemma 8.10 *Seien $x, y \in \mathbb{F}_q^*$. Dann ist $\{xa^2 + yb^2 \mid a, b \in \mathbb{F}_q\} = \mathbb{F}_q$. Insbesondere ist jedes Element von $\mathbb{F}_q$ eine Summe von zwei Quadraten:*

Beweis. Dies ist klar, falls $p = 2$ ist, da dann schon $\mathbb{F}_q = \{a^2 \mid a \in \mathbb{F}_q\}$.
Sei also q ungerade, $c \in \mathbb{F}_q$, und betrachte die beiden Mengen

$$Q := \{xa^2 \mid a \in \mathbb{F}_q\} \quad C := \{c - yb^2 \mid b \in \mathbb{F}_q\}.$$

Es ist $|Q| = \frac{q-1}{2} + 1 = \frac{q+1}{2} = |C|$. Da beides Teilmengen von $\mathbb{F}_q$ sind und $|Q| + |C| = q + 1 > q$ ist gilt $C \cap Q \neq \emptyset$, also gibt es $a, b \in \mathbb{F}_q$ mit $xa^2 + yb^2 = c$. □

Folgerung 8.11 *Sei $p \neq 2$ und sei (E, b) ein regulärer endlicher bilinearer Raum über $\mathbb{F}_q$. Dann gibt es $a \in \mathbb{F}_q^*$ sowie eine Basis $B := (b_1, \ldots, b_n)$ von E mit*

$$Gram(B) = \mathrm{diag}(1, \ldots, 1, a).$$

Die Zahl a ist modulo Quadraten in $\mathbb{F}_q^*$ eindeutig bestimmt, die Determinante $\det(E, b) \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$.

Beweis. Nach Satz 8.9 hat (E, b) eine Orthogonalbasis $C = (c_1, \ldots, c_n)$ mit $Gram(C) = \mathrm{diag}(a_1, \ldots, a_n) \in \mathrm{GL}_n(\mathbb{F}_q)$. Ist $\dim(E) \geq 2$, so gibt es nach Lemma 8.10 Zahlen $x, y \in \mathbb{F}_q$ mit $a_1x^2 + a_2y^2 = 1$. Setze $b_1 := xc_1 + yc_2$ und mache weiter mit $< b_1 >^\perp$. □

Klar ist die Determinante $\det(Gram(B)) =: \det(b) \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ eine Invariante der Isometrieklasse von (E, b). Also gilt

Folgerung 8.12 *Sei q eine ungerade Primzahlpotenz. Zu jeder Dimension n gibt es bis auf Isometrie genau zwei reguläre bilineare Räume über $\mathbb{F}_q$ die durch ihre Determinante ($\in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2 \cong C_2$) unterschieden werden.*

Satz 8.13 *Sei q eine Potenz von 2 und (E, b) ein regulärer endlicher bilinearer Raum über $\mathbb{F}_q$.*
(a) Gibt es ein $e \in E$ mit $b(e, e) \neq 0$, so hat (E, b) eine Orthonormalbasis.
(b) Gilt $b(e, e) = 0$ für alle $e \in E$, so ist E eine orthogonale Summe von hyperbolischen Ebenen, $\mathbb{H} = \langle e, f \rangle$ mit $b(e, e) = b(f, f) = 0$ und $b(e, f) = 1$.

Beweis. (a) Hier verfahren wir wie im Beweis von Satz 8.9 und spalten $\langle e \rangle$ als orthogonalen Summanden ab, falls $a := b(e, e) \neq 0$ ist. Da q gerade ist, gibt es immer ein $\alpha \in \mathbb{F}_q$ mit $\alpha^2 = a$. Indem wir e durch $\alpha^{-1}e$ ersetzen, erhalten wir $b(e, e) = 1$. Jetzt müssen wir noch garantieren, dass ein $f \in \langle e \rangle^\perp$ existiert, mit $b(f, f) \neq 0$. Gibt es kein solches f, so ist $b(e + f, e + f) = 1$ für alle $f \in e^\perp$. Da E und somit auch $e^\perp$ regulär ist, gibt es ein

Paar $f, f' \in e^\perp$ mit $b(f,f') = 1$. Ersetzt man e durch $e' = e + f$, so ist $b(e',e') = 1$, $b(e', e+f') = b(e+f,e) + b(e,f') + b(f,f') = 1+0+1 = 0$ und also $e+f' \in \langle e' \rangle^\perp$ ein Vektor mit Norm 1.
(b) In dem Fall kann man nach Satz 8.9 den Raum E als orthogonale Summe 2-dimensionaler regulärer Räume schreiben. Wir können also Œ annehmen, dass $E = \langle e, f \rangle$ mit $b(e,e) = b(f,f) = 0$. Dann muss $a := b(e,f) \neq 0$ sein und $E = \langle e, \frac{1}{a} f \rangle \cong \mathbb{H}$. □

8.3 Quadratische Formen.

Definition 8.14 *(a) Eine* quadratische Form *auf einem A-Modul E ist eine Abbildung $q : E \to A$ mit*
(i) $q(ae) = a^2 q(e)$ für alle $a \in A, e \in E$.
(ii) $b_q : E \times E \to A$ definiert durch $b_q(x,y) := q(x+y) - q(x) - q(y)$ ist eine Bilinearform.
(b) (E,q) heißt regulär *(bz.w* nicht ausgeartet*), falls (E, b_q) regulär (bzw. nicht ausgeartet) ist.*
(c) $\varphi : (E,q) \to (E',q')$ heißt Isometrie*, falls φ ein injektiver A-Modulhomomorphismus ist mit $q'(\varphi(e)) = q(e)$ für alle $e \in E$.*
(d) (E,q) und (E',q') heißen isometrisch*, falls eine bijektive Isometrie $\varphi : E \to E'$ existiert. $O(E,q) := \{\varphi : E \to E \mid \varphi$ ist bijektive Isometrie $\}$ heißt die* orthogonale Gruppe *von E.*
(f) $(E,q) \perp (E',q')$ ist der quadratische Modul $(E \oplus E', q \perp q')$ mit $(q \perp q')(x,x') = q(x) + q'(x')$ und heisst die orthogonale Summe.

Bemerkung 8.15 *(a) Ist $b : E \times E \to A$ eine symmetrische Bilinearform, so ist $q_b : E \to A, q_b(x) := b(x,x)$ eine quadratische Form mit $b_{q_b} = 2b$.*
(b) Ist $q : E \to A$ eine quadratische Form, so gilt $b_q(x,x) = 2q(x)$ für alle $x \in E$.
(c) Ist 2 eine Einheit in A, so sind die Begriffe "quadratische Form" und "symmetrische Bilinearform" äquivalent.

Beispiel 8.16 *Sei $E = \bigoplus_{i=1}^n Ae_i$ ein freier A-Modul und $q : E \to A$ eine quadratische Form. Dann gilt*

$$q(\sum_{i=1}^n x_i e_i) = \sum_{i=1}^n x_i^2 q(e_i) + \sum_{i<j} x_i x_j b_q(e_i,e_j) = (x_1,\ldots,x_n) Q (x_1,\ldots,x_n)^{tr}$$

wo Q die obere Dreiecksmatrix mit Diagonaleinträgen $q(e_i) = Q_{ii}$ und $b_q(e_i,e_j) = Q_{ij}$ für $i < j$. Wir schreiben auch abkürzend $(E,q) = [Q]$. Ist 2 kein Nullteiler in A, so schreiben wir auch $(E,q) = [Q] = \langle B \rangle$, wo B die Grammatrix von b_q ist, also $B_{ij} = b_q(e_i,e_j)$.
$(E,q) = \langle 2 \rangle = [1]$ für $E = Ae$, $q(e) = 1$.
Die hyperbolische Ebene *ist der 2-dimensionale freie quadratische A-Modul*

$$\mathbb{H}(A) = (E,q) = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} = \left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle .$$

Satz 8.17 *Sei $E = \bigoplus_{i=1}^n Ae_i$ ein freier quadratischer A-Modul mit ungeradem Rang. Ist $2 \notin A^*$, so ist (E,q) nicht regulär.*

Beweis. Sei B die Grammatrix von b_q. Dann ist $B \in A^{n\times n}$ eine symmetrische Matrix, deren Diagonaleinträge $B_{ii} = 2a_i$ durch 2 teilbar sind.
Beh. Ist n ungerade, so gibt es ein Polynom $P_n \in \mathbb{Z}[x_i, y_{ij}]$ so dass für jedes gerade symmetrische B, die Determinante $\det(B) = 2P_n(a_i, b_{ij})$, wobei $b_{ij} := b_q(e_i, e_j)$ für $i < j$.
Beweis. Mit der Leibniz Regel:

$$\det(B) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} B_{i,\pi(i)}.$$

Sei $S := \{\pi \in S_n \mid \pi = \pi^{-1}\}$ und $T := \{\pi \in S_n \mid \pi \neq \pi^{-1}\} = X \dot\cup \{\pi^{-1} \mid \pi \in X\}$. Für $\pi \in X$ ist

$$\prod_{i=1}^{n} B_{i,\pi(i)} = \prod_{i=1}^{n} B_{\pi(i),i} = \prod_{j=1}^{n} B_{j,\pi^{-1}(j)}$$

und für $\pi \in S$ gibt es immer ein $i \in \{1, \dots, n\}$ mit $i = \pi(i)$, da n ungerade ist. Insgesamt gilt also

$$\det(B) = \sum_{\pi\in S} \operatorname{sgn}(\pi) \prod_{i=1}^{n} B_{i,\pi(i)} + 2\sum_{\pi\in X} \operatorname{sgn}(\pi) \prod_{i=1}^{n} B_{i,\pi(i)} = 2P_n(a_i, b_{ij}).$$

□

Klar: $P_n(a_i, b_{ij})$ hängt modulo $(A^*)^2$ nicht von der gewählten Basis ab.

Definition 8.18 *Sei $E = \bigoplus_{i=1}^{n} Ae_i$ ein freier quadratischer A-Modul mit ungeradem Rang. Dann setzen wir $d'(E, q) := P_n(q(e_i), b_q(e_i, e_j))(A^*)^2$, die* Halbdeterminante *von (E, q) und nennen (E, q)* halbregulär*, falls $d'(E, q) \neq 0$.*

Klar: Ist $2 \in A^*$ so sind halbregulär und regulär äquivalente Begriffe.
Ist $E = E_1 \perp E_2$ frei, $\dim(E_1)$ gerade, $\dim(E_2)$ ungerade, so ist $d'(E) = \det(E_1)d'(E_2)$.

Satz 8.19 *Sei A ein Körper und (E, q) ein endlich dimensionaler quadratischer A-Vektorraum. Dann gibt es $E_1, \dots, E_r, F_1, \dots, F_s, G \leq E$ mit*
- $\dim(E_i) = 2$, *$(E_i, q_{|E_i})$ regulär für alle $1 \leq i \leq r$.*
- $\dim(F_j) = 1$, *$(F_j, q_{|F_j})$ halbregulär für alle $1 \leq j \leq s$.*
- $q(G) = \{0\}$

so dass

$$E = E_1 \perp \ldots \perp E_r \perp F_1 \perp \ldots \perp F_s \perp G.$$

Ist $\operatorname{char}(A) \neq 2$, so kann $r = 0$ gewählt werden und E ist genau dann regulär, wenn $G = \{0\}$. Ist $\operatorname{char}(A) = 2$, so ist A^2 ein Teilkörper von A und es kann $s \leq [A : A^2]$ gewählt werden. (Es ist $A = A^2$, falls A endlich.) Dann ist E regulär genau dann wenn $s = 0$ und $G = \{0\}$ und halbregulär, wenn $s = 1$ und $G = \{0\}$.

Beweis. Für Körper der Charakteristik $\neq 2$ folgt der Satz direkt aus Satz 8.9. Sei also $\mathrm{char}(A) = 2$. Dann ist $A^2 := \{a^2 \mid a \in A\} \leq A$, da $(a+b)^2 = a^2 + b^2$. Ist $|A| < \infty$ so ist $A = A^2$, is aber z.B. $A = \mathbb{F}_2(x)$, so ist $A^2 = \mathbb{F}_2(x^2)$ und $[A : A^2] = 2$. Nach Satz 8.9 gilt $(E, b_q) = E_1 \perp \ldots \perp E_r \perp F$ mit E_i regulär und $\dim(E_i) = 2$ und $b_q(F, F) = 0$. Es bleibt den Raum F zu zerlegen. Für $x, y \in F$ ist $b_q(x, y) = q(x+y) - q(x) - q(y) = 0$, also ist $q : F \to A$ additiv und $q(ax) = a^2 q(x)$. Also ist $G := \{x \in F \mid q(x) = 0\} \leq F$ ein Teilraum von F und $q(F)$ ein A^2-Teilraum von A. Also ist $\dim(F/G) \leq [A : A^2]$. Ergänzt man eine A-Basis $(g_1, \ldots, g_t)$ zu einer A-Basis $(g_1, \ldots, g_t, f_1, \ldots, f_s)$ von F, so sind die $F_i := \langle f_i \rangle$ halbregulär. □

Beispiel: Ist $A = \mathbb{F}_2(X)$, so ist $[A : A^2] = 2$ und $(1, x)$ ist eine A^2-Basis von A. Ist $E = A^3$ mit $q(t_1, t_2, t_3) = t_1^2 + x * t_2^2 + x^2 * t_3^2$, so ist $d'(E) = 4x^3 = 0$ also E nicht halbregulär, $G = \langle (x, 0, 1) \rangle$, $e_1 := (1, 0, 0)$, $e_2 = (0, 1, 0)$, dann

$$E = \langle e_1 \rangle \perp \langle e_2 \rangle \perp G \cong [1, x, 0].$$

Definition 8.20 *(a) Ein Teilmodul $F \leq (E, q)$ heißt* scharf primitiv*, falls F ein freier A-Modul ist und $(b_q)_F(E) = F^*$.*
(b) Ist G ein freier A-Modul endlichen Rangs so sei

$$\mathbb{H}(G) := (G \oplus G^*, q : x + x^* \mapsto x^*(x))$$

der durch G definierte hyperbolische Modul*.*

Bemerkung 8.21 *Jeder reguläre Teilmodul von (E, q) ist scharf primitiv.*
$\mathbb{H}(G)$ ist ein regulärer quadratischer A-Modul.
G ist ein scharf primitiver Teilmodul von $\mathbb{H}(G)$.
Ist $F \leq (E, q)$ ein scharf primitiver Teilmodul mit $q(F) = \{0\}$ (total isotrop), dann enthält (E, q) einen Teilmodul isometrisch zu $\mathbb{H}(F)$.

Beweis. Nur die letzte Aussage bedarf eines Beweises. Sei $(f_1, \ldots, f_n)$ eine A-Basis von F und $e_1, \ldots, e_n \in E$ so dass $f \mapsto b_q(e_i, f)$ die Dualbasis von F^* ist. $b_q(e_i + a f_j, e_j) = b_q(e_i, e_j) + a$ gilt können wir die Vektoren e_i durch Addition von Vektoren in F so abändern, dass $b_q(e_i, e_j) = 0$ ist für alle i, j. Setzt man dann $f_i' := e_i - q(e_i) f_i$, so ist $F' := \langle f_1', \ldots, f_n' \rangle \leq E$ mit $F \oplus F' \cong \mathbb{H}(F)$. □

8.4 Die orthogonale Gruppe und der Satz von Witt.

Definition 8.22 *Sei (E, q) ein quadratischer A-Modul. Dann ist $O(E, q) := \{\varphi \in \mathrm{Aut}_A(E) \mid q(\varphi(x)) = q(x)$ für alle $x \in E\}$ die* orthogonale Gruppe *von E.*
Für $x \in E$ mit $q(x) \in A^*$ heißt

$$\sigma_x : E \to E, \sigma_x(e) := e - \frac{b_q(x, e)}{q(x)} x$$

die Spiegelung *entlang x.*

Bemerkung 8.23 *Es ist $\sigma_x \in O(E,q)$, $\sigma_x^2 = 1$, $\sigma_x(x) = -x$, $\sigma_x(e) = e$ falle $e \in x^\perp$. Für $g \in O(E,q)$ ist $g\sigma_x g^{-1} = \sigma_{g(x)}$, also ist*

$$S(E) := \langle \sigma_e \mid e \in E, q(e) \in A^* \rangle \trianglelefteq O(E,q)$$

ein Normalteiler in $O(E,q)$, der Spiegelungsnormalteiler.

Satz 8.24 *(Witt) Sei A ein lokaler Ring mit $2 \in A^*$ und (E,q) ein freier quadratischer A-Modul, $F \leq E$ ein regulärer Teilmodul und $\varphi : F \to E$ eine Isometrie. Dann gibt es $\tilde{\varphi} \in O(E,q)$ mit $\varphi = \tilde{\varphi}_{|F}$.*

Beweis. Induktion nach $\dim(F)$, so ist $F = Af$ mit $q(f) \in A^*$. Sei $f' := \varphi(f)$. Dann ist $q(f') = q(f) \in A^*$. Weiter ist

$$q(f - f') + q(f + f') = 2q(f) + 2q(f') = 4q(f) \in A^*.$$

Also ist entweder $q(f - f')$ oder $q(f + f') \in A^*$. Ist $q(f - f') \in A^*$, so ist $\tilde{\varphi} = \sigma_{f-f'}$ eine Fortsetzung von φ, denn $\sigma_{f-f'}(f) = f'$.
Ist $q(f + f') \in A^*$, so ist $\tilde{\varphi} = \sigma_{f'} \circ \sigma_{f+f'}$ eine solche Fortsetzung.
Sei nun $\dim(F) = m > 1$, $F = Af_1 \perp \ldots \perp Af_m$, mit $q(f_i) \in A^*$ für alle i. Dann gibt es nach Induktionsvoraussetzung ein $g \in O(E,q)$ mit $g(f_i) = \varphi(f_i)$ für $i = 1, \ldots, m-1$. Die Isometrie $g^{-1} \circ \varphi$ lässt also $f_1, \ldots, f_{m-1}$ fest und überführt den zu ihnen orthogonalen Vektor $f := f_m$ in $g^{-1}(\varphi(f_m)) =: f'$. Nach Induktionsanfang ist $w(f) = f'$, wobei $w = \sigma_{f-f'}$ oder $w = \sigma_{f'} \circ \sigma_{f+f'}$. In beiden Fällen ist w die Identität auf $\langle f, f' \rangle^\perp$ und lässt daher $f_1, \ldots, f_{m-1} \in f^\perp \cap (f')^\perp$ fest. □

Folgerung 8.25 *(Wittscher Kürzungssatz) Sei A ein lokaler Ring mit $2 \in A^*$ und F, G_1, G_2 quadratische A-Moduln mit F regulär so dass $F \perp G_1 \cong F \perp G_2$. Dann ist $G_1 \cong G_2$.*

Beweis. Wir können Œ annehmen dass $E := F_1 \perp G_1 = F_2 \perp G_2$ mit $F_1 \cong F_2$ regulär. Die Isometrie $\varphi : F_1 \to F_2$ können wir zu einer Isometrie $\tilde{\varphi}$ von E fortsetzen. Diese bildet aber den Orthogonalraum $G_1 = F_1^\perp$ auf den Orthogonalraum des Bildes $\varphi(F_1)^\perp = F_2^\perp = G_2$ ab. □

Satz 8.26 *Sei (E,q) ein quadratischer Modul über einem lokalen Ring A, $F, G, H \leq E$, F, G seien frei von endlichem Rang und es gelte*

$$b_F(H) = F^*, b_G(H) = G^*. \qquad (1)$$

Sei $t : F \to G$ eine bijektive Isometrie mit

$$t(x) \equiv x \pmod{H} \text{ für alle } x \in F. \qquad (2)$$

Dann gibt es $\tilde{t} \in O(E,q)$ mit $\tilde{t}(x) \equiv x \pmod{H}$ für alle $x \in E$ und $\tilde{t}(x) = x$ für alle $x \in H^\perp$.

Folgerung 8.27 *(Satz von Witt für beliebige lokale Ringe) Sind F, G scharf primitive freie Teilmoduln des quadratischen A-Moduls (E, q) über dem lokalen Ring A und ist Sei $t : F \to G$ eine bijektive Isometrie so gibt es $\tilde{t} \in O(E, q)$ mit $t = \tilde{t}_{|F}$.*

Beweis. Setze $H = E$ in Satz 8.26. □

Folgerung 8.28 *Der Wittsche Kürzungssatz gilt für beliebige lokale Ringe.*

Bemerkung 8.29 *Ist (E, q) ein quadratischer A-Modul endlichem Rangs und sind F_1, F_2 zwei total isotrope ($q(F_i) = \{0\}$) scharf primitive Teilmoduln gleicher Dimension, dann gibt es ein $g \in O(E, q)$ mit $g(F_1) = F_2$. Insbesondere ist die Dimension jedes maximal total isotropen scharf primitiven Teilmoduls immer gleich und heisst der* Witt-Index $\mathrm{ind}(E)$ *von (E, q).*
Ist $n := \mathrm{ind}(E)$, so ist

$$(E, q) \cong \mathbb{H}(A^n) \perp (F, q_{|F})$$

mit $\mathrm{ind}(F) = 0$. Ist (E, q) ein regulärer A-Vektorraum über einem Körper A, so ist der Teilraum $(F, q_{|F})$ anisotrop ($v \in F$, $q(v) = 0 \Rightarrow v = 0$) und heißt der anisotrope Kern *von (E, q).*

Beispiel 8.30 *Der Witt'sche Kürzungssatz gilt nicht für Bilinearformen, denn sei $A = \mathbb{F}_2$, $E = A^3$, $b(x, y) = x_1y_1 + x_2y_2 + x_3y_3$. $F_1 = \langle(1, 0, 0)\rangle$, $F_2 = \langle(1, 1, 1)\rangle$. Dann ist $F_1 \cong F_2$ aber $F_1^\perp \cong \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ nicht isometrisch zu $F_2^\perp \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ da $b(x, x) = 0$ für alle $x \in F_2^\perp$.*

Beispiel 8.31 *Auch die scharfe Primitivität des Teilraums ist notwendig: Denn sei (E, q) ein 3-dimensionaler quadratischer Raum mit OG-Basis (e_1, e_2, e_3), $q(e_1) = 1, q(e_2) = -1, q(e_3) = 0$ also $(E, q) \cong [1, -1, 0]$. Sei $F_1 = \langle e_1 + e_2\rangle$ und $F_2 = \langle e_3\rangle$. Dann ist $F_2 = E^\perp \cong F_1$, jedoch gibt es keine Isometrie von E, die F_1 auf F_2 abbildet.*

Beispiel 8.32 *(quadratische Formen über endlichen Körpern) Sei $A = \mathbb{F}_\ell$ ein endlicher Körper, $\ell = p^f$, $p = \mathrm{char}(A)$.*
(1) Für Dimension 1 gibt es bis auf Isometrie genau $|A^*/(A^*)^2|$ verschiedene reguläre bzw. halbreguläre quadratische A-Vektorräume, also 2, falls $p > 2$ und genau einen, falls $p = 2$ ist.
(2) Sei $K = \mathbb{F}_{\ell^2}$ die quadratische Erweiterung von A. Dann ist K ein 2-dimensionaler A-Vektorraum und die Normform $N : K \to A, x \mapsto x^{\ell+1}$ ist eine quadratische Form mit $N(K) = A$ und $\mathrm{ind}(K, N) = 0$.
(3) Ist (E, q) ein 2-dimensionaler regulärer A-Vektorraum, so ist entweder $\mathrm{ind}(E) = 1$ und $(E, q) \cong \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$ eine hyperbolische Ebene, oder aber $\mathrm{ind}(E) = 0$ und (E, q) ist anisotrop.
In letzterem Fall ist $(E, q) \cong (K, N)$. **Denn***: Sei (b_1, b_2) eine Basis von E und $q(xb_1 + yb_2) = a_1x^2 + a_{12}xy + a_2y^2$. Dann ist $a_1 = q(b_1) \neq 0$ und das Polynom $f(x) := x^2 + ax + b$ mit $b = \frac{a_2}{a_1}$ und $a = \frac{a_{12}}{a_1}$ in $A[x]$ irreduzibel, sein Zerfällungskörper also isomorph zu $K = \mathbb{F}_{\ell^2}$. Also gibt es ein $\alpha \in K$ mit*

$$q(xb_1 + yb_2) = a_1(x - \alpha y)(x - \alpha^\ell y) = a_1N(x - \alpha y).$$

Da $N(K) = A$ ist, gibt es ein $\beta \in K$ mit $N(\beta) = a_1$ und die Abbildung

$$xb_1 + yb_2 \mapsto \beta(x - \alpha y)$$

ist eine Isometrie zwischen (E, q) und (K, N).

Satz 8.33 *(Klassifikation der regulären und halbregulären endlichen quadratischen Vektorräume) Sei A ein endlicher Körper und (E, q) ein regulärer oder halbregulärer quadratischer A-Vektorraum der Dimension n. Dann ist (E, q) isometrisch zu genau einem der folgenden quadratischen Räume:*
(a) $n = 2m$ gerade und $(E, q) \cong \mathbb{H}^m$, mit Wittindex m und Determinante $(-1)^m$.
(b) $n = 2m$ gerade und $(E, q) \cong \mathbb{H}^{m-1} \perp (K, N)$ wo K der Erweiterungskörper von A vom Grad 2 bezeichnet und N die Normform. Hier ist der Wittindex gleich $m - 1$ und die Determinante $(-1)^m \epsilon$.
(c) $n = 2m + 1$ ungerade und $(E, q) \cong \mathbb{H}^m \perp [a]$ mit Wittindex m und Halbdeterminante $(-1)^m a$. Es gibt genau $[A^* : (A^*)^2]$ solche quadratische Räume, parametrisiert durch die Vertreter a der Quadratklassen.

Beweis. als Übung. Beachten Sie, dass $(K, N) \perp [a] \cong \mathbb{H} \perp [b]$ ist, da $(K, N) \perp [a]$ den scharf primitiven Teilraum $\langle(\alpha, 1)\rangle$ enthält, wo $\alpha \in K$, mit $N(\alpha) = -a$. □

Beweis. (von Satz 8.26) (aus Kneser's Buch) Sei $\overline{A} = A/I$ der Restklassenkörper von A und $\overline{q} : \overline{E} \to \overline{A}$ die zugehörige quadratische Form, etc.
Wir wollen die Fortsetzung $\tilde{t}$ als Produkt von Spiegelungen σ_h mit $h \in H$ konstruieren, die dann automatisch (2) erfüllen und auf $H^\perp$ die Identität sind. Wir zeigen genauer:
$\tilde{t}$ kann als Produkt von Spiegelungen σ_h mit $h \in H$ gewählt werden, falls eine der folgenden beiden Bedingungen erfüllt ist:

$$\overline{A} \neq \mathbb{F}_2, \overline{q}(\overline{H}) \neq \{0\} \qquad (3)$$

oder

$$\overline{A} = \mathbb{F}_2, \overline{q}(\overline{H}^\perp) \neq \{0\} \qquad (4).$$

Wir zeigen zunächst 8.26 unter der Voraussetzung, dass (3) oder (4) gilt durch Induktion über $r := \dim(F) = \dim(G)$.
Für $r = 1$ sei $F = Af$ und $G = Ag$ mit $g = t(f) = f + h$. Dann ist

$$q(h) = q(g-f) = q(g)+q(f)-b_q(f,g) = 2q(f)-b(f,g) = b(f,f)-b(f,g) = -b(f,h) = b(h,g).$$

Ist $q(h) \in A^*$, so ist also

$$\sigma_h(f) = f - \frac{b(f,h)}{q(h)}h = f + h = g$$

und somit σ_h die gewünschte Fortsetzung.
Ansonsten haben wir

$$q(h) = -b(f,h) = b(g,h) \in I \qquad (5)$$

und suchen $e, d \in H$ mit $g = s_e(f) + d$, also

$$d = b(f,e)q(e)^{-1}e + h,\ q(d) = b(f,e)b(g,e)q(e)^{-1} + q(h).$$

Ist außer $q(e)$ auch noch $q(d)$ inwertierbar, so ist $\sigma_d(\sigma_e(f)) = g$ und $\tilde{t} := \sigma_d \circ \sigma_e$ ist die gewünschte Fortsetzung.
Wegen (5) suchen wir also einen Vektor $e \in H$ mit

$$q(e) \notin I, b(f,e) \notin I, b(g,e) \notin I.$$

Setze

$$\overline{H}_1 := \{x \in \overline{H} \mid \overline{b}(\overline{f}, x) = 0\},\ \overline{H}_2 := \{x \in \overline{H} \mid \overline{b}(\overline{g}, x) = 0\}.$$

Dann ist $\overline{h} \in \overline{H}_1 \cap \overline{H}_2$ und wegen (1) ist $\dim(\overline{H}_1) = \dim(\overline{H}_2) = \dim(\overline{H}) - 1$. Da man zu jedem $\overline{e} \in \overline{H}$ einen Vertreter $e \in H$ finden kann, haben wir zu zeigen, dass $\overline{q}$ auf dem Komplement $\overline{H} - (\overline{H}_1 \cup \overline{H}_2)$ nicht identisch verschwindet. Nehmen wir an, das sei doch der Fall. Für beliebige

$$a \in \overline{A}, x \in \overline{H}_1 \cap \overline{H}_2, y \in \overline{H} - (\overline{H}_1 \cup \overline{H}_2)$$

liegt dann $ax + y$ nicht in $\overline{H}_1 \cup \overline{H}_2$ so dass

$$\overline{q}(ax + y) = a^2\overline{q}(x) + a\overline{b}(x,y) + \overline{q}(y) = 0$$

Hat $\overline{A}$ mindestens 3 Elemente, so folgt daraus, dass

$$\overline{q}(x) = \overline{b}(x,y) = \overline{q}(y) = 0 \qquad (6)$$

Wegen (5) können wir speziell $x = \overline{h}$ setzen und erhalten

$$\overline{b}(\overline{h}, \overline{H} - (\overline{H}_1 \cup \overline{H}_2)) = \{0\}$$

also, da $\langle \overline{H} - (\overline{H}_1 \cup \overline{H}_2)\rangle = \overline{H}$ auch $\overline{b}(\overline{h}, \overline{H}) = \{0\}$. Wegen $g = f + h$ folgt daraus $\overline{H}_1 = \overline{H}_2$ und jeder Vektor in $\overline{H}$ liegt entweder in $\overline{H}_1 \cap \overline{H}_2 = \overline{H}_1$ oder in $\overline{H} - (\overline{H}_1 \cup \overline{H}_2) = \overline{H} - \overline{H}_1$. Dann ist aber $\overline{q}(\overline{H}) = \{0\}$ ein Widerspruch zur Voraussetzung (3).
Ist $\overline{A} = \mathbb{F}_2$, so erhalten wir (6) für die x, y die zusätzlich noch in $\overline{H}^\perp$ liegen. Da aber $\overline{H}_1 \cap \overline{H}^\perp = \overline{H}_2 \cap \overline{H}^\perp$ folgt wiederum aus (6) dass $q(\overline{H}^\perp) = \{0\}$ ist, ein Widerspruch zur Voraussetzung (4).
Induktionsschluss. Sei nun $r > 1$ und $(f_1, \ldots, f_r)$ eine Basis von F. Nach Voraussetzung (1) gibt es Vektoren $(h_1, \ldots, h_r) \in H^r$ mit $b(f_i, h_j) = \delta_{ij}$. Sei $D := F^\perp \cap H$ Sei nun $r > 1$ und $(f_1, \ldots, f_r)$ eine Basis von F. Nach Voraussetzung (1) gibt es Vektoren $(h_1, \ldots, h_r) \in H^r$ mit $b(f_i, h_j) = \delta_{ij}$. Sei $D := F^\perp \cap H$. Dann ist $H = D \oplus \langle h_1, \ldots, h_r\rangle$. Sei $F' := \langle f_1, \ldots, f_{r-1}\rangle$. Dann erfüllt F' die Bedingung (1) und die Einschränkung von t auf F' die Bedingung (2), also gibt es nach Induktionsvoraussetzung ein Produkt von Spiegelungen $\sigma := \prod \sigma_h$ mit geeigneten $h \in H$, so dass $t(f_i) = \sigma(f_i)$ für $i = 1, \ldots, r-1$. Indem wir t durch $\sigma^{-1}t$ ersetzen, können wir annehmen, dass $t(f_i) = f_i$ für alle $i = 1, \ldots, r-1$. Für $x \in F$ und $i = 1, \ldots, r-1$ ist dann aber

$$b(tx - x, f_i) = b(tx, tf_i) - b(x, f_i) = 0$$

also ist

$$tx \equiv x \pmod{Ah_r \oplus D}.$$

Wir wenden jetzt den Induktionsanfang an auf Af_r anstelle von F und $Ah_r \oplus D$ anstelle von H und erhalten so ein Produkt σ' von Spiegelungen $\sigma_{h'}$ mit $h' \in Ah_r \oplus D$, mit $\sigma'(f_r) = t(f_r)$. Da $\sigma_{h'}(f_i) = f_i$ für $i = 1, \ldots, r-1$ und $h' \in Ah_r \oplus D$ gilt, haben wir insgesamt die Abbildung t als Produkt von Spiegelungen entlang Vektoren von H geschrieben.

Es bleibt noch nachzutragen, dass Af_r und $Ah_r \oplus D$ die Bedingungen (1), (2), (3), (4) erfüllt. Für (1) und (2) haben wir dies gerade gesehen, wir zeigen nun, dass bei geeigneter Wahl der Basis $(f_1, \ldots, f_r)$ von F auch die Bedingungen (3) bzw. (4) für $Ah_r \oplus D$ gilt. Nach Voraussetzung gibt es jedenfalls einen Vektor $\overline{h} \in \overline{H}$ bzw. $\overline{H}^{\perp}$ mit $\overline{q}(\overline{h}) \neq 0$. Wir wählen $0 \neq \overline{h}_r \in \overline{H} - \overline{D}$, so dass dieser Vektor $\overline{h} \in \overline{Ah}_r \oplus \overline{D}$ und ergänzen $\overline{h}_r$ zu einer Basis $(\overline{h}_1, \ldots, \overline{h}_r)$ von $\overline{H} \pmod{\overline{D}}$. Repräsentanten $h_1, \ldots, h_r$ der $\overline{h}_i$ bilden eine Basis von $H \pmod{D}$ un die duale Basis $(f_1, \ldots, f_r)$ von F hat die gewünschten Eigenschaften.

Zum Abschluss müssen wir noch zeigen, dass der Satz auch ohne die Bedingungen (3) und (4) gilt. Dazu betrachten wir $E' := E \perp (Ae \oplus Af)$, wobei $q(xe + yf) = xy$. Wegen $q(e + f) = 1$ können wir den schon bewiesenen Teil des Satzes auf E', $F' := F \perp Ae$, $G' := G \perp Ae$, $H' := H \perp A(e + f)$ und $t' := t \perp \mathrm{id}_{Ae}$ anwenden. Wir erhalten eine Fortsetung u' (als Produkt von Spiegelungen entlang Vektoren von H') von t' die ausser e wegen $b(H', e-f) = 0$ auch $e - f$ festlässt. Also ist $u' = u \perp \mathrm{id}_{Ae+Af}$ und u ist die gewünschte Fortsetzung von t. □

9 Die Massformel für selbstduale Codes.

9.1 Massformeln.

Das Prinzip für Massformeln ist leicht beschrieben. Sei G eine Gruppe, die auf einer endlichen Menge M operiert. Seien $m_1, \ldots, m_h$ ein Vertetersystem der Bahnen $B_1, \ldots, B_h$ von G auf M und $S_i = \mathrm{Stab}_G(m_i)$. Dann ist

$$M = \dot{\cup}_{i=1}^{h} B_i, \text{ also } |M| = \sum_{i=1}^{h} |B_i| = \sum_{i=1}^{h} \frac{|G|}{|S_i|}.$$

Also ergibt sich die sogenannte Massformel

$$\sum_{i=1}^{h} \frac{1}{|S_i|} = \frac{|M|}{|G|}$$

wobei man in der Regel davon ausgeht, dass $|M|$ und $|G|$ bekannt sind.

Wollen wir also z.B. eine Massformel für selbstduale Codes, so ist

$$M := M(n, \ell) := \{C = C^{\perp} \leq \mathbb{F}_{\ell}^{n}\}$$

$G = S_n$ (falls wir Permutationsäquivalenzklassen zählen wollen) oder $G = C_2 \wr S_n$ (für monomiale Äquivalenz, falls ℓ ungerade). Achtung, allgemeine monomiale Äquivalenz erhält nicht die Selbstdualität, die Multiplikatoren müssen $a_i^2 = 1$ erfüllen, also ± 1 sein, falls ℓ ungerade

und 1 falls ℓ gerade ist. Sind $C_1, \ldots, C_h$ Vertreter der Äquivalenzklassen selbstdualer Codes dann findet man mit der Massformel

$$\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(C_i)|} = \frac{|M(n,q)|}{|G|}$$

wobei $|G| = n!$ bzw. $|G| = 2^n n!$.

Wir müssen also nur noch $|M(n,q)|$ bestimmen, dazu benutzen wir den Satz von Witt: Jeder selbstduale Code ist ein maximal isotroper Teilraum in dem bilinearen Raum $(\mathbb{F}_q^n, \cdot)$. Die orthogonale Gruppe $O(\mathbb{F}_q^n, \cdot)$ operiert nach dem Satz von Witt transitiv auf $M(n,q)$, also ist $|M(n,q)|$ der Index des Stabilisators eines maximal isotropen Teilraums in der orthogonalen Gruppe.

9.2 Orthogonale Gruppen über endlichen Körpern.

Sei (E,q) ein regulärer oder halbregulärer Vektorraum der Dimension n über dem endlichen Körper $\mathbb{F}_\ell$. Nach Satz 8.33 gibt es die folgenden orthogonalen Gruppen:

(a) Ist $(E,q) \cong \mathbb{H}^m$, $n = 2m$, so ist $O(E,q) =: O^+_{2m}(\mathbb{F}_\ell)$.
(b) $(E,q) \cong \mathbb{H}^{m-1} \perp (\mathbb{F}_{\ell^2}, N)$, $n = 2m$, so ist $O(E,q) =: O^-_{2m}(\mathbb{F}_\ell)$.
(c) $n = 2m+1$ ungerade, dann ist $(E,q) \cong \mathbb{H}^m \perp [a]$ mit $a = (-1)^m \det'(E,q)$. Ist $\epsilon \in \mathbb{F}_\ell^* - (\mathbb{F}_\ell^*)^2$, so ist $(E, \epsilon q) = \mathbb{H}^m \perp [\epsilon a]$ und $O(E,q) = O(E,\epsilon q) =: O_{2m+1}(\mathbb{F}_\ell)$.

Satz 9.1

$$\textit{(a)}\ |O^+_{2m}(\mathbb{F}_\ell)| = 2\ell^{m(m-1)}(\ell^m - 1)\prod_{i=1}^{m-1}(\ell^{2i}-1).$$

$$\textit{(b)}\ |O^-_{2m}(\mathbb{F}_\ell)| = 2\ell^{m(m-1)}(\ell^m + 1)\prod_{i=1}^{m-1}(\ell^{2i}-1).$$

$$\textit{(c)}\ |O_{2m+1}(\mathbb{F}_\ell)| = z\ell^{m^2}\prod_{i=1}^{m-1}(\ell^{2i}-1)\ \textit{mit}\ z = |O_1(\mathbb{F}_\ell)| = \begin{cases} 1 & p = 2 \\ 2 & p \neq 2. \end{cases}$$

Beweis. (a) ((b) und (c) gehen ähnlich, Übung). Schreibe $(E,q) = H \perp V$ mit $H = \langle h_1, h_2\rangle \cong \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$. Sei $U_1 := \operatorname{Stab}_{O(E,q)}(h_1)$, $U_2 := \operatorname{Stab}_{U_1}(h_2)$. Dann ist

$$|O(E,q)| = |O(E,q)h_1||U_1| = |O(E,q)h_1||U_1h_2||U_2|.$$

Nach dem Satz von Witt ist $U_2 \cong O(V) \cong O^+_{2(m-1)}(\mathbb{F}_\ell)$ und $|U_2|$ nach Induktion bekannt.
Die Länge der Bahn von h_2 unter U_1 ergibt sich wie folgt: Ist $u \in U_1$, dann ist $u(h_1) = h_1$ und $u(h_2) = h$ mit $b_q(h_1, h) = 1$, $q(h) = 0$. Also ist $h = h_2 + ah_1 + v$ mit $a \in \mathbb{F}_\ell$, $v \in V$, $q(v) = -a$, oder umgekehrt $a = -q(v)$ durch v eindeutig bestimmt, also

$$U_1h_2 = \{h_2 - q(v)h_1 + v \mid v \in V\}$$

und $|U_1 h_2| = |V| = \ell^{2m-2}$.
Die Länge der Bahn von h_1 unter der vollen orthogonalen Gruppe ist nach dem Satz von Witt gleich der Anzahl a_m isotroper (scharf primitiver) Vektoren in (E, q), wobei für $n \in \mathbb{N}$

$$a_n := s(\mathbb{H}^n) = |\{0 \neq x \in \mathbb{H}^n \mid q(x) = 0\}|.$$

Ist $0 \neq x = y + z \in E$ mit $q(x) = 0$ und $y \in V$, $z = z_1 h_1 + z_2 h_2 \in H$ so ist $q(x) = q(y) + z_1 z_2 = 0$ genau dann wenn entweder
$y = 0$ und $z_1 z_2 = 0$, aber $(z_1, z_2) \neq (0, 0)$ $(2(\ell - 1)$ Möglichkeiten)
oder
$y \neq 0$, $q(y) = 0$, $z_1 z_2 = 0$ $(a_{m-1}(2\ell - 1)$ Möglichkeiten)
oder
$q(y) \neq 0$, $z_1 = -q(y)/z_2$ $((\ell^{2m-2} - 1 - a_{m-1})(\ell - 1)$ Möglichkeiten)
Also erhält man

$$\begin{aligned} a_m &= 2(\ell - 1) + a_{m-1}(2\ell - 1) + (\ell^{2m-2} - 1 - a_{m-1})(\ell - 1) \\ &= \ell a_{m-1} + \ell^{2m-1} - \ell^{2m-2} + \ell - 1 \end{aligned}$$

also $a_m - \ell^{2m-1} + 1 = \ell(a_{m-1} - \ell^{2m-3} + 1)$. Setzt man $x_m := a_m - \ell^{2m-1} + 1$, so efüllt die Folge $(x_n)_{n \in \mathbb{N}_0}$ die Rekursion $x_m = \ell x_{m-1}$ also $x_m = \ell^m x_0$. Da $a_0 = 0$ ist, findet man $x_0 = 1 - \ell^{-1}$ und

$$a_m = \ell^{2m-1} - 1 + \ell^m - \ell^{m-1} = (\ell^m - 1)(\ell^{m-1} + 1).$$

Also ergibt sich

$$|O^+_{2m}(\mathbb{F}_\ell)| = |O^+_{2m-2}(\mathbb{F}_\ell)| a_m |V| = (\ell^m - 1)(\ell^{m-1} + 1)\ell^{2m-2} |O^+_{2m-2}(\mathbb{F}_\ell)| = \prod_{j=1}^{m} (\ell^j - 1)(\ell^{j-1} + 1)\ell^{2j-2}.$$

□

Satz 9.2 *Sei $A = \mathbb{F}_\ell$ ein endlicher Körper und $(E, q) := \mathbb{H}(A^m) = \langle c_1, \ldots, c_m, b_1, \ldots, b_m \rangle$ mit $q(\sum a_i c_i) = q(\sum a_i b_i) = 0$ und $b_q(b_i, c_j) = \delta_{ij}$. Sei $C = \langle c_1, \ldots, c_m \rangle$ ein maximal isotroper Teilraum von E. Dann ist*

$$|\operatorname{Stab}_{O(E,q)}(C)| = |\operatorname{GL}(C)| \ell^{m(m-1)/2} = \ell^{m(m-1)} \prod_{j=1}^{m} (\ell^j - 1)$$

Beweis. Sei $S := \operatorname{Stab}_{O(E,q)}(C)$. Jedes Element aus $\operatorname{GL}(C)$ lässt sich nach dem Satz von Witt zu einer orthogonalen Abbildung fortsetzen, d.h. die Abbildung $S \to \operatorname{GL}(C), \varphi \mapsto \varphi_{|C}$ ist surjektiv. Ihr Kern besteht aus den orthogonalen Abbildungen φ von E, mit $\varphi(c_i) = c_i$ für alle $1 \leq i \leq m$. Dann ist $\varphi(b_j) = b_j + d_j$ für gewisse

$$d_j = \sum_{k=1}^{m} a_{jk} c_k \in C^\perp = C.$$

Damit φ eine Isometrie ist, muss gelten

$$q(b_j + d_j) = q(b_j) + q(d_j) + b_q(b_j, d_j) = 0 + 0 + a_{jj} = 0$$

sowie für $i \neq j$

$$b_q(b_i + d_i, b_j + d_j) = b_q(b_i, d_j) + d_q(d_i, b_j) = a_{ij} + a_{ji} = 0.$$

Damit können wir also die Zahlen a_{ij} mit $1 \leq i < j \leq m$ frei wählen und $|S| = |\operatorname{GL}(C)|\ell^{m(m-1)/2}$. □

Folgerung 9.3 *Die Anzahl der maximal isotropen Teilräume des quadratischen $\mathbb{F}_\ell$ Raums $\mathbb{H}(\mathbb{F}_\ell)^m$ ist*

$$\prod_{j=0}^{m-1}(\ell^j + 1).$$

Für ungerades ℓ können wir diese Formel direkt auf die selbstdualen Codes anwenden, da jeder selbstduale Code $C = C^\perp \leq (\mathbb{F}_\ell^n, \cdot)$ auch bzgl. der zugehörigen quadratischen Form maximal total isotrop ist.

Folgerung 9.4 *Sei ℓ eine ungerade Primzahlpotenz. Ist $\ell \equiv 1 \pmod 4$, so enthält $(\mathbb{F}_\ell^n, \cdot)$ einen selbstdualen Code, genau dann wenn n gerade ist. Ist $\ell \equiv 3 \pmod 4$, so enthält $(\mathbb{F}_\ell^n, \cdot)$ einen selbstdualen Code, genau dann wenn n durch 4 teilbar ist. In den Fällen ist*

$$|M(n, \ell)| = |\{C = C^\perp \leq (\mathbb{F}_\ell^n, \cdot)\}| = \prod_{j=0}^{n/2-1}(\ell^j + 1).$$

Beweis. Die Standardbasis ist eine ON-Basis von $\mathbb{F}_\ell^n$, also ist die Determinante von $\mathbb{F}_\ell^n$ gleich 1. Daher ist $\mathbb{F}_\ell^n \cong \mathbb{H}^{n/2}$ genau dann wenn n gerade ist und $(-1)^{n/2}$ ein Quadrat. Also genau dann wenn entweder n durch 4 teilbar oder $\ell \equiv 1 \pmod 4$ und n gerade. □

Wir betrachten nun die doppeltgeraden selbstdualen binären Codes. Sei also $\ell = 2$, $\mathbf{1} := (1, \ldots, 1) \in \mathbb{F}_2^n$, n durch 4 teilbar. Ist $C \subset C^\perp$ ein selbstdualer Code in $\mathbb{F}_2^n$, dann ist $\mathbf{1} \in C^\perp$, da $c \cdot \mathbf{1} = c \cdot c$ ist. Jeder selbstduale Code enthält also $\mathbf{1}$ und ist daher ein Teilmodul des $n-2$-dimensionalen $\mathbb{F}_2$-Vektorraums $E_n := \mathbf{1}^\perp/\langle \mathbf{1} \rangle$. Auf E_n ist die Bilinearform

$$b : E_n \times E_n \to \mathbb{F}_2, b(c + \langle \mathbf{1} \rangle, c' + \langle \mathbf{1} \rangle) := c \cdot c'$$

wohldefiniert. Definieren

$$q : E_n \to \mathbb{F}_2, q(c + \langle \mathbf{1} \rangle) := (\frac{1}{2}\operatorname{wt}(c)) + 2\mathbb{Z}.$$

Dann gilt $b = b_q$ und (E_n, q) ist ein regulärer quadratischer $\mathbb{F}_2$-Vektorraum der Dimension $n-2$. Die doppelt geraden selbstdualen Codes $C = C^\perp \leq \mathbb{F}_2^n$ entsprechen genau den maximal total isotropen Teilräumen $C/\langle \mathbf{1} \rangle$ von (E_n, q).

Satz 9.5 *Sei $M(n, II) := \{C = C^\perp \leq \mathbb{F}_2^n \mid \operatorname{wt}(C) \subset 4\mathbb{Z}\}$ die Menge aller selbstdualen doppeltgeraden Codes in $\mathbb{F}_2^n$. Dann ist $M(n, II) \neq \emptyset$ genau dann wenn $n \in 8\mathbb{Z}$ ist. In dem Fall ist*

$$|M(n, II)| = \prod_{j=0}^{n/2-2}(2^j + 1).$$

Für die einfachgeraden binären Codes verfolgen wir eine einfachere Strategie:

Satz 9.6 *Sei ℓ eine Potenz von 2 und $n \in \mathbb{N}$ gerade. Sei weiter*

$$M(n, \mathbb{F}_\ell) := \{C = C^\perp \leq \mathbb{F}_\ell^n\}$$

die Menge aller selbstdualen Codes in $\mathbb{F}_\ell^n$. Dann ist $|M(n, \mathbb{F}_\ell)| = \prod_{i=1}^{n/2-1}(\ell^i + 1)$.

Beweis. Zunächst eine Vorbemerkung: Da Quadrieren ein Körperautomorphismus von $\mathbb{F}_\ell$ ist, gilt für $c \in \mathbb{F}_\ell^n$:

$$c \cdot c = \sum_{i=1}^{n} c_i^2 = (\sum_{i=1}^{n} c_i)^2 = (c \cdot \mathbf{1})^2$$

insbesondere gilt für $C \in M(n, \mathbb{F}_\ell)$ dass

$$\mathbf{1} \in C \subset \langle \mathbf{1} \rangle^\perp = \{c \in \mathbb{F}_\ell^n \mid c \cdot c = 0\} =: E_0.$$

Sei

$$S(n, k) := \{\mathbf{1} \in C \subset C^\perp \leq \mathbb{F}_\ell^n \mid \dim(C) = k\}.$$

Dann ist $S(n, n/2) = M(n, \mathbb{F}_\ell)$. Jedem Code $C \in S(n, k)$ entspricht ein Teilraum $C/\langle \mathbf{1} \rangle \leq E_0/\langle \mathbf{1} \rangle$ der Dimension $(k-1)$.
Behauptung. Für alle $1 \leq k \leq n/2$ ist

$$|S(n, k)| = \prod_{j=1}^{k-1} \frac{\ell^{n-2j} - 1}{\ell^j - 1}.$$

Denn $|S(n, 1)| = 1$ ist klar.
Für den Induktionsschluss sei $k < \frac{n}{2}$ und $C \in S(n, k)$. Dann ist jeder Code $\langle C, c \rangle$ mit $c \in C^\perp - C$ in $S(n, k+1)$. Da $\dim(C^\perp/C) = n - 2k$ ist, gibt es genau

$$\frac{\ell^{n-2k} - 1}{\ell - 1}$$

Codes in $S(n, k+1)$, die C enthalten. Umgekehrt enthält jeder Code $C \in S(n, k+1)$ genau

$$\frac{\ell^k - 1}{\ell - 1}$$

Teilcodes D mit $\mathbf{1} \in D$. Also ist

$$|S(n, k+1)| = \frac{\ell^{n-2k} - 1}{\ell^k - 1} |S(n, k)| = \ldots = \prod_{j=1}^{k} \frac{\ell^{n-2j} - 1}{\ell^j - 1}.$$

Ist nun speziell $k = n/2$ so ergibt sich dieses Produkt als

$$|S(n, n/2)| = \prod_{j=1}^{n/2-1} \frac{\ell^{2j} - 1}{\ell^j - 1} = \prod_{j=1}^{n/2-1} (\ell^j + 1).$$

□

Daraus ergeben sich die folgenden Massformeln

Satz 9.7 *Sei $(C_1, \ldots, C_h)$ ein Vertretersystem der Permutationsäquivalenzklassen selbstdualer Codes in $\mathbb{F}_\ell^n$. Dann ist*

$$\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(C_i)|} = \frac{\prod_{j=1}^{n/2-1}(\ell^j+1)}{n!} z \text{ mit } z = \begin{cases} 2 & \ell \text{ ungerade} \\ 1 & \ell \text{ gerade} \end{cases}$$

Für doppeltgerade binäre Codes gilt

$$\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(C_i)|} = \frac{\prod_{j=0}^{n/2-2}(2^j+1)}{n!}$$

Die Maßformel für die selbstdualen binären Codes.

n	h	mass	sum
2	1	1/2	$1/2$
4	1	1/8	$1/8$
6	1	1/48	$1/48$
8	2	3/896	$384^{-1} + \mathbf{1344}^{-1}$
10	2	17/26880	$2688^{-1} + 3840^{-1}$
12	3	17/107520	$10752^{-1} + 23040^{-1} + 46080^{-1}$
14	4	17/301056	$64512^{-1} + 46080^{-1} + 56448^{-1} + 645120^{-1}$
16	7	731/24084480	$516096^{-1} + 184320^{-1} + 112896^{-1} + 73728^{-1}$ $+10321920^{-1} + \mathbf{3612672}^{-1} + \mathbf{5160960}^{-1}$

Daraus ergeben sich recht einfach die Klassifikationen der selbstdualen binären Codes bis zur Länge 12. Sei $i_2 := \langle (1,1) \rangle \leq \mathbb{F}_2^2$ der Wiederholungscode. Dann ist $\operatorname{Aut}(\perp^m i_2) = C_2 \wr S_m$ von Ordnung $2^m m!$ $(= 2, 8, 48, 384, 3840, 46080, 645120, 10321920$ für $m = 1, .., 8)$. Von Länge 8 gibt es mindestens einen weiteren selbstdualen Code, e_8, der doppeltgerade ist und also nicht isomorph zu i_2^4. Es ist $|\operatorname{Aut}(e_8)| = 1344$. Codes der Länge 10 sind $i_2 \perp e_8$ und i_2^5 mit Automorphismengruppenordnung $2 \cdot 1344$ und 3840. In Länge 12 erhält man neben $i_2^2 \perp e_8$ und i_2^6 mit Automorphismengruppen der Ordnung $8 \cdot 1344 = 10752$ und 46080 noch einen weiteren Code, d_{12}^+. Man erhält ihn, indem man zum doppeltgeraden Teilcode d_{12} von i_2^6 noch einen weiteren Vektor aus $d_{12}^\perp - i_2^{12}$ hinzufügt. Es ist $\operatorname{Aut}(d_{12}^+) = C_2^5 : S_6$ von Ordnung $2^5 6! = 23040$. Die Massformel zeigt in jedem Fall, dass die Liste der Permutationsäquivalenzklassen von Codes vollständig ist.

9.3 Klassifikation selbstdualer Codes mit der Kneserschen Nachbarschaftsmethode.

Wir wollen hier eine Methode kennenlernen, um algorithmisch ein Vertretersystem der Äquivalenzklassen selbstdualer Codes zu finden, dessen Vollständigkeit man dann mit Hilfe der Massformeln verifiziert.

Definition 9.8 *Auf $\mathcal{M}(n,q) := \{C = C^\perp \leq \mathbb{F}_q^n\}$ der Menge aller selbstdualen Codes der Länge n über dem Körper $\mathbb{F}_q$ definieren wir einen Graphen $\Gamma := \Gamma(n,q)$ mit Eckenmenge*

$\mathcal{M}(n,q)$. *Zwei Ecken* C *und* D *in* Γ *sind durch eine Kante verbunden, falls* $\dim(C \cap D) = \frac{n}{2} - 1$.

Bemerkung 9.9 *Ist* $C \in \mathcal{M}(n,q)$ *gegeben, so erhält man alle zu* C *in* Γ *mit einer Kante verbundenen Codes* D*, indem man alle* $\frac{q^{n/2}-1}{q-1}$ *Teilräume* E *der Dimension* $n/2-1$ *von* C *durchläuft und alle* $D \in \mathcal{M}(n,q)$ *bestimmt mit* $D \cap C = E$ *als Urbilder der isotropen eindimensionalen Teilräume von* $E^\perp/E$.

Satz 9.10 Γ *ist zusammenhängend.*

Beweis. Definieren einen Abstand d auf $\mathcal{M}(n,q)$ durch $d(C,D) = n/2 - \dim(C \cap D) \in \{0,\ldots,n/2\}$. Dann ist d eine Metrik und wir wollen zeigen, dass $d(C,D)$ genau die Länge $\ell(C,D)$ eines kürzesten Weges in Γ von C nach D ist. Dazu nutzen wir Induktion über $d(C,D)$. Ist $d(C,D) = 1$, so sind C und D in Γ durch eine Kante verbunden. Sei also $d(C,D) = k > 1$. Sei $C \cap D < X \leq D$ ein Teilraum von D mit $\dim(X/(C \cap D)) = 1$. Dann ist $C + X > C$ und $E := (C+X)^\perp \leq C$ ein Teilraum von C der Codimension 1. Setze $C_1 := X + (C+X)^\perp$. Dann ist
(a) $C_1 = C_1^\perp$.
Denn $C_1 \subset C_1^\perp$ und $\dim(C_1) = \dim((C+X)^\perp) + 1$.
(b) $(C+X)^\perp = C_1 \cap C$, also $d(C_1, C) = 1$ und C_1 und C durch eine Kante in Γ verbunden.
(c) $C_1 \cap D = X$, also $d(C_1, D) = d - 1$.
Nach Induktion ist also $d(C_1, D) = \ell(C_1, D) = k-1$ und da ℓ die Dreiecksungleichung erfüllt ist auch $\ell(C,D) \leq k$.
Das zeigt schon, dass Γ zusammenhängend ist. $\ell = d$ zeigen Sie in der Übung. □

Übungsaufgabe: Schränkt man den Graphen $\Gamma(n,2)$ auf die Eckenmenge der doppeltgeraden binären selbstdualen Codes ein, so ist der daraus resultierende Teilgraph wieder zusammenhängend.

Um den Nachbarschaftsgraphen auszurechnen, geht man meist zur Menge $\mathcal{M}(n,q)/S_n$ der Äquivalenzklassen selbstdualer Codes in $\mathbb{F}_q^n$ über. Die Gruppe S_n operiert auf Γ als Graphautomorphismen, da $d(C,D) = d(\pi(C), \pi(D))$ ist für alle $\pi \in S_n$. Also ist der Quotient Γ/S_n wieder ein zusammenhängender Graph mit Eckenmenge $\{[C] \mid C \in \mathcal{M}(n,q)\}$.

Ein MAGMA Programm zur Berechnung dieses Graphen ist auf der homepage erhältlich.

Algorithmus.
Eingabe. n, q sowie einen Code $C \in M(n,q)$.
Ausgabe. $V := \{C_1,\ldots,C_h\}$ ein Vertretersystem der Äquivalenzklassen von Codes in $M(n,q)$.
Algorithmus. Setze $V := \{C\}$, $akt := 1$, $anz := 1$.
Solange $akt \leq anz$ wiederhole
$C := V[akt]$
für alle maximalen Teilräume $E \leq C$
(ist $q = 2$, so genügen auch die Teilräume E, die $\mathbf{1}$ enhalten.)
bestimme die Codes $D \in M(n,q)$ mit $C \cap D = E$ als volle Urbilder der isotropen eindimensionalen Teilräume von $E^\perp/E$.
für jedes solche D vergleiche, ob es äquivalent zu einem Element von V ist.

Ist D neu, so füge D zu V hinzu und setze $anz := anz + 1$.
end solange.

Damit kann man die folgenden Klassifikationen erhalten:

N	I	II	III	IV
2	1(1)	–	–	1(1)
4	1(1)	–	1(1)	1(1)
6	1(1)	–	–	2(1)
8	2(1)	1(1)	1(1)	3(1)
10	2	–	–	5(2)
12	3(1)	–	3(1)	10
14	4(1)	–	–	21(1)
16	7	2(2)	7(1)	55(4)
18	9	–	–	244(1)
20	16	–	24(6)	(2)
22	25(1)	–	–	
24	55	9(1)	338(2)	
26	103	–	–	
28	261	–	(6931)	
30	731	–	–	
32	3295	85(5)		
34	24147	–	–	

N bezeichnet hier die Länge der Codes, in Klammern ist die Anzahl der extremalen Codes angegeben. Die erste Spalte gibt die Anzahl der selbstdualen binären Codes an, die 2. Spalte nur die doppeltgeraden. Die 3. Spalte listet die Anzahl monomialer Äquivalenzklassen selbstdualer ternärer Codes $C = C^{\perp} \leq \mathbb{F}_3^N$ auf und die letzte Spalte gibt die sogenannten Typ IV Codes an, das sind hermitesch selbstduale Codes $C = \overline{C}^{\perp} \leq \mathbb{F}_4^N$ bis auf monomiale Äquivalenz.

10 Wittgruppen.

Definition 10.1 *Sei A ein kommutativer Ring. Auf der Menge der Isometrieklassen regulärer quadratischer A-Moduln definieren wir eine Addition durch die orthogonale Summe. Zwei reguläre quadratische A-Moduln (E_1, q_1) und (E_2, q_2) heißen* Witt äquivalent*, falls es hyperbolische Moduln H_1 und H_2 gibt, mit*

$$E_1 \perp H_1 \cong E_2 \perp H_2.$$

Die Wittgruppe *$WQ(A)$ von A ist die Menge der Äquivalenzklassen regulärer quadratischer A-Moduln mit der Addition $[E] + [F] := [E \perp F]$.. Das neutrale Element in $WQ(A)$ ist die Klasse der hyperbolischen Moduln und $-[(E, q)] = [(E, -q)]$.*

Bemerkung 10.2 *(a) Ein Modul (E, q) heißt* metabolisch*, falls $E = N \oplus P$ mit $N = N^{\perp}$ und $q(N) = \{0\}$. Wegen Bemerkung 8.21 sind metabolische Moduln gleich 0 in $WQ(A)$.*

(b) Gilt der Wittsche Kürzungssatz für A, so hat jede Klasse in $WQ(A)$ einen eindeutigen anisotropen Vertreter.

Beispiel 10.3 *Ist K ein algebraisch abgeschlossener Körper, so ist $WQ(K) \cong C_2$, falls $\mathrm{char}(K) \neq 2$ und $WQ(K) = \{0\}$, falls $\mathrm{char}(K) = 2$ ist. Denn jede quadratische Form von Dimension 2 ist isotrop: ist $q(x,y) = ax^2+bxy+cy^2$ so hat das quadratische Polynom $q(x,1)$ eine Nullstelle in K, also gibt es einen Vektor $0 \neq v$ mit $q(v) = 0$. Dann aber spaltet der Raum die hyperbolische Ebene ab, ist also gleich 0 in $WQ(K)$.*

Beispiel 10.4 *$WQ(\mathbb{R}) \cong \mathbb{Z}$ vermöge der Signatur.*

Beispiel 10.5

$$WQ(\mathbb{F}_q) \cong \begin{cases} C_2 \times C_2 & q \equiv 1 \pmod 4 \\ C_4 & q \equiv -1 \pmod 4 \\ C_2 & q \equiv 0 \pmod 2 \end{cases}$$

Dies ergibt sich aus der Klassifikation der quadratischen Räume in Satz 8.33. Ist nämlich $q \equiv -1 \pmod 4$, so ist $[1] \perp [1] = (\mathbb{F}_{q^2}, N)$ der eindeutig bestimmte anisotrope Raum der Dimension 2 und $[1]$ hat Ordnung 4 in $WQ(\mathbb{F}_q)$. Ist $q \equiv 1 \pmod 4$, so ist $[1] \perp [1] = \mathbb{H}$ und $WQ(\mathbb{F}_q) = \langle [1] \rangle \times \langle [\epsilon] \rangle$ wobei ϵ kein Quadrat in $\mathbb{F}_q^*$ ist. Ist q gerade, so hat jeder reguläre quadratische Raum gerade Dimension und $WQ(\mathbb{F}_q) = \langle (\mathbb{F}_{q^2}, N) \rangle \cong C_2$.

10.1 Die Wittgruppe endlicher abelscher Gruppen.

Definition 10.6 *Sei A eine endliche abelsche Gruppe. Eine reguläre symmetrische Bilinearform $b : A \times A \to \mathbb{Q}/\mathbb{Z}$ ist eine biadditive Abbildung mit $b(x,y) = b(y,x)$ für alle $x, y \in A$ so dass $b_A : A \to A^* := \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}), a \mapsto (x \mapsto b(a,x))$ ein Isomorphismus ist.*
Eine reguläre quadratische Form $q : A \to \mathbb{Q}/\mathbb{Z}$ ist eine Abbildung mit $q(na) = n^2 q(a)$ für alle $n \in \mathbb{Z}$ so dass $b_q : (x,y) \mapsto q(x+y) - q(x) - q(y)$ eine reguläre symmetrische Bilinearform ist.

Identifiziert man den endlichen Primkörper $\mathbb{F}_p$ mit $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$, so ist jeder endlich dimensionale reguläre $\mathbb{F}_p$-Vektorraum auch eine reguläre endliche abelsche Gruppe.

Beispiel 10.7 *(Diskriminantengruppe) Sei L ein ganzes $\mathbb{Z}$-Gitter in einem regulären $\mathbb{Q}$-Vektorraum (V,b), so induziert b eine reguläre Bilinearform*

$$\overline{b} : L^\#/L \times L^\#/L \to \mathbb{Q}/\mathbb{Z}, \overline{b}(x+L, y+L) := b(x,y) + \mathbb{Z}$$

auf der Diskriminantengruppe $(L^\#/L, \overline{b})$. Ist L sogar gerade, so erhalten wir eine reguläre quadratische Form

$$q : L^\#/L \to \mathbb{Q}/\mathbb{Z}, x + L \mapsto \frac{1}{2} b(x,x) + \mathbb{Z}$$

mit zugehöriger symmetrischer Bilinearform $b_q = \overline{b}$.

Lemma 10.8 *Sei (A,b) eine reguläre endliche bilineare Gruppe. Dann ist $(A,b) = \perp_p (A_p, b)$ wobei A_p die p-Sylowgruppe von A bezeichnet. Analoges gilt für quadratische Formen.*

Beweis. Es genügt zu zeigen, dass für verschiedene Primzahlen p und q die Sylowgruppen A_p und A_q senkrecht aufeinander stehen. Sei also $x \in A_p$ und $y \in A_q$ und wähle $k, \ell \in \mathbb{N}$ mit $p^k x = q^\ell y = 0$, sowie $c, d \in \mathbb{Z}$ mit $cp^k + dq^\ell = 1$. Dann ist

$$b(x,y) = cp^k b(x,y) + dq^\ell b(x,y) = cb(p^k x, y) + db(x, q^\ell y) = 0 + 0 = 0.$$

□

Definition 10.9 *Sei (A,b) eine endliche abelsche Gruppe mit regulärer symmetrischer Bilinearform. Ist $N \leq A$ eine Untergruppe von A, so auch*

$$N^\perp := \{a \in A \mid b(a,n) = 0 \text{ für alle } n \in N\}.$$

(A,b) heisst schwach metabolisch*, falls es eine Untergruppe $N \leq A$ gibt mit $N = N^\perp$.*
Für quadratische Formen fordert man zusätzlich, dass $q(N) = \{0\}$ ist.
Die Wittgruppe *W der symmetrischen Bilinearformen (bzw. WQ der quadratischen Formen) auf endlichen abelschen Gruppen ist die Grothendieckgruppe der Menge aller Isometrieklassen regulärer endlicher abelscher Gruppen, modulo der schwach metabolischen. Die Klasse von (A,b) in W wird mit $[A,b]$ bezeichnet.*
Es ist $(A,b) \perp (A,-b)$ schwach metabolisch, da die Diagonale $N := \{(a,a) \mid a \in A\}$ eine selbstduale Untergruppe ist. Also ist $-[A,b] = [A,-b]$.
Für eine Primzahl p bezeichne $W(p)$ bzw. $WQ(p)$ die Wittgruppe der endlichen abelschen p-Gruppen mit regulärer Bilinearform bzw. quadratischer Form.

Bemerkung 10.10 *$W \cong \prod_p W(p)$ und $WQ \cong \prod_p WQ(p)$.*

Bemerkung 10.11 *Ist (A,b) regulär und $N \leq A$, so ist $(N^\perp)^\perp = N$.*

Beweis. Dies liegt daran, dass die Einschränkung $r_N : A^* \to N^*, \varphi \mapsto \varphi_{|N}$ surjektiv ist. Jeder Homomorphismus von N nach $\mathbb{Q}/\mathbb{Z}$ lässt sich zu einem von A nach $\mathbb{Q}/\mathbb{Z}$ fortsetzen, da $\mathbb{Q}/\mathbb{Z}$ divisibel ist.
Es ist klar, dass $N \subset (N^\perp)^\perp$ gilt. Aber $|A| = |N||N^\perp|$, da $N^\perp$ der Kern der Komposition von b_A mit r_N ist. Ebenso gilt $|A| = |N^\perp||(N^\perp)^\perp|$, da $(N^\perp)^\perp = \ker(r_{N^\perp} \circ b_A)$. □

Lemma 10.12 *Sei $N \leq (A,b)$ mit $N \subset N^\perp$. Dann induziert b eine reguläre symmetrische Bilinearform $\overline{b}$ auf $N^\perp/N$ definiert durch*

$$\overline{b}(x+N, y+N) := b(x,y) \text{ für alle } x, y \in N^\perp$$

und $(A,b) \perp (N^\perp/N, -\overline{b})$ ist schwach metabolisch. Analoges gilt für quadratische Formen, wenn man zusätzlich fordert, dass $q(N) = \{0\}$. (Übung, $\overline{q}$ ist wohldef. ...)

Beweis. $\overline{b}$ ist wohldefiniert und regulär, da $(N^\perp)^\perp = N$. Die Untergruppe $U := \{(x, \overline{x}) \mid x \in N^\perp\}$ in $(A, b) \perp (N^\perp/N, -\overline{b})$ erfüllt sicherlich $U \subset U^\perp$. Aber $|U| = |N^\perp| = \frac{|A|}{|N|} = |U^\perp|$ da $|A \times N^\perp/N| = |A|\frac{|A|}{|N|}\frac{1}{|N|} = |U|^2$. □

Satz 10.13 *Jedes Element von W (bzw. WQ) hat einen anisotropen Vertreter.*

Beweis. Sei (A, b) ein Vetreter von $[A, b]$ mit $|A|$ minimal. Angenommen es gibt ein $x \in A$ mit $x \neq 0$ aber $b(x, x) = 0$. Dann betrachten wir $N := \langle x \rangle \leq A$. Es ist $N \subset N^\perp$ also nach Lemma 10.12 $[A, b] = [N^\perp/N, \overline{b}]$ ein Widerspruch zur Minimalität von $|A|$. □

Bemerkung 10.14 *Jeder anisotrope Vertreter (A, b) in W hat quadratfreien Exponenten.*

Beweis. Sei $x \in A$, $n \in \mathbb{N}$, $n > 1$ mit $n^2 x = 0$. Dann ist $b(nx, nx) = b(n^2 x, x) = b(0, x) = 0$ also $nx = 0$, da (A, b) anisotrop war. □

Folgerung 10.15 *Es ist $W(p) = WQ(p) \cong WQ(\mathbb{F}_p)$ falls $p \neq 2$. Es ist $W(2) \cong C_2$.*

Beweis. Für $p \neq 2$ sind quadratische Formen und symmetrische Bilinearformen äquivalente Konzepte.

$$WQ(\mathbb{F}_p) \to WQ(p), (q : V \to \mathbb{F}_p) \mapsto (\frac{1}{p}q : V \to \mathbb{Q}/\mathbb{Z})$$

ist eine kanonische Abbildung, es genügt also eine Inverse zu konstruieren. Sei (A, q) ein anisotroper Vertreter in $WQ(p)$. Dann ist nach Bemerkung 10.14 A ein $\mathbb{F}_p$-Vektorraum und $q : A \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$, also $(A, pq) \in W(\mathbb{F}_p)$. Dass dies einen wohldefinierten Gruppenisomorphismus liefert zeigen Sie als Übung. Für $W(2) = C_2$ zeigen wir, dass jeder reguläre bilinear $\mathbb{F}_2$-Vektorraum (V, b) der Dimension > 1 isotrop ist. Angenommen (V, b) anisotrop. Dann ist für $x \neq y \in V - \{0\}$ $b(x, x) = b(y, y) = 1$ und $b(x + y, x + y) = 0$ ein Widerspruch. □

Es genügt also jetzt noch $WQ(2)$ zu bestimmen.

Satz 10.16 $WQ(2) \cong C_8 \times C_2$.

Dazu benötigen wir sogenannte Gauss-Summen auf endlichen quadratischen Gruppen.

Definition 10.17 *Sei $e(t) := \exp(2\pi i t)$. Dann ist $e : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^*$ ein Gruppenhomomorphismus.*
Für eine endliche quadratische Gruppe (A, q) sei

$$\Gamma(A, q) := \frac{1}{\sqrt{|A|}} \sum_{a \in A} e(q(a)),\ \gamma_p(A, q) := \frac{1}{\sqrt{|A_p|}} \sum_{a \in A_p} e(q(a)).$$

Lemma 10.18 $\Gamma(A,q) = \prod_p \gamma_p(A,q)$.
$\Gamma((A_1,q_1) \perp (A_2,q_2)) = \Gamma(A_1,q_1) \cdot \Gamma(A_2,q_2))$.
Ist (A,q) schwach metabolisch, so ist $\gamma_q(A,q) = 1$ für alle p.
Insbesondere definiert γ_p einen Gruppenhomomorphismus $\gamma_p : WQ \to \mathbb{C}^*$.

Beweis. Die ersten beiden Aussagen sind klar. Sei nun (A,q) schwach metabolisch. Dann ist auch (A_p,q) schwach metabolisch, da die p-Sylowgruppe N_p von $N = N^\perp \leq (A,q)$, $q(N) = \{0\}$ ebenson $N_p = N_p^\perp \leq (A_p,q)$ und $q(N_p) = \{0\}$ erfüllt. Also Œ $A = A_p$ und N eine selbstduale total isotrope Untergruppe. Sei $A = \dot{\bigcup}_{i=1}^k a_i + N$ mit $a_1 = 0$. Dann ist

$$\sum_{a\in A} e(q(a)) = \sum_{i=1}^k \sum_{n\in N} e(q(a_i+n)) = \sum_{i=1}^k \sum_{n\in N} e(q(a_i)+b_q(a_i,n)) = \sum_{i=1}^k e(q(a_i)) \sum_{n\in N} e(b_q(a_i,n)).$$

Ist $a_i \notin N = N^\perp$, so ist $n \mapsto b_q(a_i,n)$ ein nichttrivialer Gruppenhomomorphismus von N nach $\mathbb{Q}/\mathbb{Z}$. Es gibt also $n_0 \in N$ mit $b_q(a_i,n_0) \neq 0$. Dann ist aber

$$\sum_{n\in N} e(b_q(a_i,n)) = \sum_{n\in N} e(b_q(a_i,n+n_0)) = e(b_q(a_i,n_0)) \sum_{n\in N} e(b_q(a_i,n)).$$

Also ist für $i \neq 1$ die Summe $\sum_{n\in N} e(b_q(a_i,n)) = 0$. Für $i = 1$ ist $b_q(a_1,n) = b_q(0,n) = 0$ für alle $n \in N$, also $\sum_{n\in N} e(b_q(a_i,n)) = |N| = \sqrt{|A|}$. □

Definition 10.19 *Für $k = 1,3$ und $\ell = 1,3,5,7$ sei*

$$\phi_k := (\mathbb{Z}/2\mathbb{Z}, q), \text{ mit } q(1) = \frac{k}{4} + \mathbb{Z}, \text{ sowie } \psi_\ell := (\mathbb{Z}/4\mathbb{Z}, q), \text{ mit } q(1) = \frac{\ell}{8} + \mathbb{Z}.$$

Weiter sei

$$\chi := (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, q) = (\mathbb{F}_4, \frac{1}{2}N) = \begin{bmatrix} 1/2 & 1/2 \\ & 1/2 \end{bmatrix}$$

mit $q(x) = \frac{1}{2}$ für alle $x \neq 0$.

Bemerkung 10.20 *ϕ_k und ψ_ℓ sind reguläre quadratische Gruppen. Es ist*

$$\gamma_2(\phi_1) = \frac{1}{\sqrt{2}}(1 + e(\frac{1}{4})) = \frac{1+i}{\sqrt{2}} = \zeta_8,$$

$$\gamma_2(\psi_1) = \frac{1}{2}(1 + \zeta_8 + \zeta_8^4 + \zeta_8^9) = \zeta_8,$$

$$\gamma_2(\chi) = \frac{1}{2}(1 + (-1) + (-1) + (-1)) = -1.$$

Lemma 10.21 *In $WQ(2)$ gilt*

(1) $8[\phi_1] = 0$.

(2) $2[\phi_1] = 2[\psi_1]$.

(3) $k[\psi_1] = [\psi_{k \pmod 8}]$ *für ungerade* k.

(4) $4[\psi_1] = [\chi]$.

(5) $[\phi_1] + [\phi_3] = 0$.

Beweis. (1) Sei $(a_1, \ldots, a_8)$ eine Basis von $\perp^8 \phi_1$ und

$$N := \langle a_1 + a_2 + a_3 + a_4, a_3 + a_4 + a_5 + a_6, a_5 + a_6 + a_7 + a_8, a_1 + a_3 + a_5 + a_7 \rangle.$$

Dann ist $N \leq N^\perp$, $q(N) = \{0\}$ und $|N| = 2^4$, also $N = N^\perp$ und $\perp^8 \phi_1$ ist (schwach) metabolisch.
(2) Sei (a_1, a_2) eine Basis von $\psi_1 \perp \psi_1$ und $e := 2a_1 + 2a_2$. Dann ist $q(e) = 0$ und $\langle e \rangle^\perp = \langle 2a_1, 2a_2, a_1 + a_2 \rangle$. Also bilden $a_1 + a_2, a_1 + 3a_2$ eine Basis von $\langle e \rangle^\perp / \langle e \rangle \cong \phi_1 \perp \phi_1$.
(3)-(5) Als Übung. Es ist $[\psi_1] + [\psi_7]$ schwach metabolisch, also gleich 0, also $[\psi_7] = -[\psi_1] = 7[\psi_1]$ nach (1) und (2). □

Beweis. (von Satz 10.16) Wir zeigen, dass

$$WQ(2) = \langle [\phi_1] \rangle \oplus \langle [\phi_1] - [\psi_1] = [\phi_1] + [\psi_7] \rangle \cong C_8 \times C_2.$$

Nach obigem Lemma und Bemerkung hat $[\phi_1]$ Ordnung 8 und $4[\phi_1] \neq [\phi_1] + [\psi_7]$. Da die Ordnung der zugrundeliegenden abelschen Gruppe von $[\phi_1] + [\psi_7]$, nämlich $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ kein Quadrat ist, ist $[\phi_1] + [\psi_7]$ nicht schwach metabolisch und also hat nach dem Lemma $[\phi_1] + [\psi_7]$ die Ordnung 2. Es bleibt zu zeigen, dass

$$WQ(2) = \langle [\phi_k], [\psi_\ell], [\chi] \mid k = 1, 3, \ell = 1, 3, 5, 7 \rangle =: X.$$

Sei also (A, q) eine anisotrope quadratische 2-Gruppe. Wir zeigen, dass $[A, q] \in X$ ist durch Induktion über $|A|$. Zunächst ist der Exponent von A ein Teiler von 4. Enthält A nämlich ein Element $x \in A$ der Ordnung 8, so ist

$$q(4x) = 16q(x) = 8b_q(x, x) = b_q(8x, x) = 0$$

also $4x$ isotrop, ein Widerspruch dazu, dass A anisotrop ist.
Ist nun $a \in A$ ein Element der Ordnung 4, so ist $q(a) = \frac{k}{8} + \mathbb{Z}$ für $k \in \{1, 3, 5, 7\}$ da zum einen $b_q(4a, a) = 8q(a) = 0$ und zum anderen $q(2a) = 4q(a) \neq 0$ ist. Dann ist aber $A = \langle a \rangle \perp \langle a \rangle^\perp$ und $\langle a \rangle \cong \psi_k$.
Also können wir annehmen, dass der Exponent von A gleich 2 ist. Falls ein $a \in A$ existiert, mit $q(a) = \frac{k}{4}$ für ungerades k, so können wir die reguläre Form ϕ_k als orthogonalen Summanden abspalten. Also bleibt der Fall, $q(A - \{0\}) = \{\frac{1}{2} + \mathbb{Z}\}$ zu betrachten. Dann ist aber $(A, 2q \pmod{2\mathbb{Z}})$ ein anisotroper quadratischer Raum über $\mathbb{F}_2$ also isometrisch zu $(\mathbb{F}_4, N)$, also $A \cong \chi$. □

Folgerung 10.22 *Da* WQ *Exponenten 8 hat, ist für jede Primzahl* p *der Homomorphismus* $\gamma_p : WQ \to \langle \zeta_8 \rangle \leq \mathbb{C}^*$.

10.2 Die Wittgruppe von $\mathbb{Q}$.

Satz 10.23 $WQ(\mathbb{Q}) \cong WQ(\mathbb{R}) \oplus W \cong \mathbb{Z} \oplus \bigoplus_p W(p)$.

Beweis. Da $\mathbb{Q} \subset \mathbb{R}$ liefert die Signatur einen kanonischen Epimorphismus $S : WQ(\mathbb{Q}) \to WQ(\mathbb{R}) \cong \mathbb{Z}$. Wir wollen jetzt einen kanonischen Epimorphismus $F : W(\mathbb{Q}) \to W$ konstruieren. Dazu sei (V, b) ein bilinearer $\mathbb{Q}$-Vektorraum und L ein volles ganzes Gitter in V. Dann liefert b eine reguläre symmetrische Bilinearform

$$b_L : L^\# / L \times L^\# / L \to \mathbb{Q}/\mathbb{Z}.$$

Wir möchten (V, b) auf $(L^\#/L, b_L) \in W$ abbilden. Dazu müssen wir zeigen, dass die Klasse von $(L^\#/L, b_L)$ in W nicht von der Wahl des ganzen Gitters L in V abhängt.
Ist nämlich $L_0 \leq L$ ein Teilgitter, so ist $L/L_0 \leq L_0^\#/L_0$ eine Untergruppe mit dualer Gruppe $(L/L_0)^\perp = L^\#/L_0$ und nach Lemma 10.12 ist $[L_0^\#/L_0, b_{L_0}] = [L^\#/L, b_L]$.
Sind allgemeiner L_1, L_2 zwei ganze Gitter in V, so ist auch $L_0 := L_1 \cap L_2$ ein ganzes Gitter und nach obigem

$$[L_1^\#/L_1, b_{L_1}] = [L_0^\#/L_0, b_{L_0}] = [L_2^\#/L_2, b_{L_2}].$$

Um zu zeigen, dass $WQ(\mathbb{Q}) \cong WQ(\mathbb{R}) \oplus W$ betrachten wir die Untergruppe

$$U_k = \langle [a] \mid a \in \mathbb{Z}, \text{ alle Primfaktoren von } a \text{ sind } \leq k \rangle \leq WQ(\mathbb{Q})$$

Klar ist die Signatur S ein Isomorphismus $S : U_1 \cong \mathbb{Z} \cong WQ(\mathbb{R})$ und $U_1 \leq \ker(F)$. Die Untergruppe $U_2 = \langle [1], [-1, 2] \rangle$ ist kanonisch isomorph zu $WQ(\mathbb{R}) \times W(2) \cong \mathbb{Z} \times C_2$. Dazu müssen wir nur einsehen, dass $[-1, 2] \leq \ker(S)$ Ordnung 2 in $WQ(\mathbb{Q})$ hat, denn $[-1, 2, -1, 2]$ enthält den selbstorthogonalen Teilraum $\langle (1, 1, 1, 0), (0, 1, 2, 1) \rangle$.
Per Induktion über k möchten wir zeigen, dass $U_k \cong WQ(\mathbb{R}) \bigoplus_{p \leq k} W(p)$.
Für $k = 1$ und $k = 2$ haben wir dies bereits gesehen. Ausserdem ist klar, dass $U_k = U_{k-1}$ ist, falls k keine Primzahl ist. Ist nun $k = p$ eine Primzahl, so genügt es zu zeigen dass

Lemma 10.24 *Sei p eine ungerade Primzahl. Die Abbildung $\delta_p : WQ(\mathbb{Q}) \to WQ(\mathbb{F}_p)$, definiert für $a \in \mathbb{Z}, p \not| a$ durch $\delta_p([a]) = 0$ und $\delta_p([pa]) := [\overline{a}]$ liefert einen Isomorphismus $U_p/U_{p-1} \to WQ(\mathbb{F}_p)$.*

Beweis. δ_p ist klar surjektiv mit U_{p-1} im Kern. Es bleibt zu zeigen, dass $U_{p-1} = \ker((\delta_p)_{U_p})$. Sind $a_1, \ldots, a_r \in \mathbb{Z}$ mit $|a_i| \leq p - 1$ und $a \in \mathbb{Z}$, $0 < |a| < p$ mit $a_1 \cdots a_r \equiv_p a$, so ist

$$[ap] \equiv [a_1 \cdots a_r p] \pmod{U_{p-1}}.$$

Wir beweisen das wieder mit Induktion über r. Für $r = 1$ ist nichts zu zeigen. Für $r = 2$ sei $a_1 a_2 = a + kp$ mit $k \in \mathbb{Z}$. Ist $k = 0$, so ist wieder nichts zu zeigen. Ist $k \neq 0$, so ist $0 < |k| < p$ und

$$[a, kp] \cong [a + kp, (a + kp)akp] = [a_1 a_2, a_1 a_2 akp]$$

da $[a, kp]$ die Zahl $a + kp$ darstellt und beide Formen die gleiche Determinante haben. Multipliziert man diese Gleichheit mit p, so erhalten wir

$$[ap, k] \cong [a_1 a_2 p, a_1 a_2 ak]$$

also $[ap] \equiv [a_1 a_2 p] \pmod{U_{p-1}}$. Für beliebiges r liefert diese Überlegung den Induktionsschritt. Wir haben also gezeigt, dass $U_p = \langle U_{p-1}, [ap] \mid 1 \leq |a| < p \rangle$.
Um das Lemma zu beweisen genügt es also zu zeigen, dass die Formen $[ap]$ modulo U_{p-1} dieselben Relationen erfüllen wie die Formen $[\overline{a}]$ in $W(\mathbb{F}_p)$. Ist $\overline{a} = \overline{b}\overline{c}^2$, so ist $[\overline{a}] = [\overline{b}] \in W(\mathbb{F}_p)$, aber auch $[ap] \equiv [bc^2 p] = [bp]$ modulo U_{p-1}. Also genügt es die Klassen $[p]$ und $[\epsilon p]$ zu betrachten, wo $\epsilon \in \mathbb{F}_p^* - (\mathbb{F}_p^*)^2$. Ist -1 ein Quadrat, so gibt es ein $z \in \{1, \ldots, p-1\}$ mit $z^2 = (-1) + kp \equiv_p -1$. Dann ist aber der Vektor $e_1 + ze_2$ in $[p] \perp [p]$ von Norm kp^2, also $[p] \perp [p] \cong [k] \perp [\ell] \in U_{p-1}$. Ebenso $[\epsilon p] \perp [\epsilon p] \in U_{p-1}$.
Kann man $\epsilon = -1$ wählen, so ist $[p] + [-p] = 0$ in $W(\mathbb{Q})$, d.h. $[\epsilon p] = -[p]$ und es genügt zu zeigen, dass $[p] + [p] + [p] + [p] \equiv 0 \pmod{U_{p-1}}$, bzw. $[p] + [p] \equiv [\epsilon p] \perp [\epsilon p] \pmod{U_{p-1}}$. Es gibt aber $a, b \in \{1, \ldots, p-1\}$ mit $a^2 + b^2 = \epsilon + kp$. Der Vektor $ae_1 + be_2 \in [p] \perp [p]$ ist also von Norm $\epsilon p + kp^2$, also $[p, p] \equiv [\epsilon p, \epsilon p] \pmod{U_{p-1}}$. □ □

Folgerung 10.25 *Zwei rationale symmetrische bilineare Räume (E_1, b_1) und (E_2, b_2) sind isometrisch, genau dann wenn $\dim(E_1) = \dim(E_2)$, $\operatorname{sgn}(b_1) = \operatorname{sgn}(b_2)$ und $\delta_p(b_1) = \delta_p(b_2)$ für alle Primzahlen p.*

Beweis. Die Bedingungen liefern die Gleichheit von $[E_1, b_1]$ und $[E_2, b_2]$ in $WQ(\mathbb{Q})$, das heisst es gibt hyberbolische Moduln $\mathbb{H}_1$, $\mathbb{H}_2$ mit

$$(E_1, b_1) \perp \mathbb{H}_1 \cong (E_2, b_2) \perp \mathbb{H}_2.$$

Da $\dim(E_1) = \dim(E_2)$ ist, folgt $\mathbb{H}_1 = \mathbb{H}_2$ und da der Satz von Witt gilt damit auch $(E_1, b_1) \cong (E_2, b_2)$. □

10.3 Die Wittgruppe von $\mathbb{Q}_p$.

Definition 10.26 *Sei A ein Integritätsbereich mit Quotientenkörper K. Sei (V, b) ein regulärer bilinearer endlich dimensionaler K-Vektorraum. Eine Teilmenge $L \subset V$ heißt volles A-Gitter in V, falls eine K-Basis $(b_1, \ldots, b_n)$ von V existiert mit $L = \bigoplus_{i=1}^n Ab_i$. Das* duale Gitter *ist dann $L^\# := \{v \in V \mid b(v, L) \subset A\}$ wieder ein A-Gitter in V mit der Dualbasis als Gitterbasis.*

Zunächst Liften von Isometrien:

Satz 10.27 *Zwei reguläre quadratische $\mathbb{Z}_p$-Gitter (L_i, q_i) sind genau dann isometrisch wenn sie modulo p isometrisch sind.*

Beweis. Sei für $k \geq 1$ die Abbildung $u : L_1 \to L_2$ eine Isometrie modulo p^k, d.h. u ist ein Isomorphismus von L_1 nach L_2 (Nakayama) und $q_2(ux) \equiv q_1(x) \pmod{p^k}$. Wir wollen einen Isomorphismus $u' : L_1 \to L_2$ konstruieren mit $u'x \equiv ux \pmod{p^k L_2}$ und

$$q_2(u'x) \equiv q_1(x) \pmod{p^{2k}}.$$

Dazu setzen wir $u'(x) = u(x) + p^k v(x)$ an für eine gesuchte Abbildung $v : L_1 \to L_2$.

$$q_2(u'(x)) - q_1(x) = q_2(u(x)) - q_1(x) + p^{2k} q_2(v(x)) + p^k b_2(u(x), v(x))$$

Schreibt man $q_2(u(x)) - q_1(x) =: p^k a(x,x)$ für eine (nicht unbedingt symmetrische) Bilinearform $a : L_1 \times L_1 \to \mathbb{Z}_p$ und berücktsichtigt man das $2k \geq k+1$ ist, so suchen wir eine lineare Abbildung $v : L_1 \to L_2$ mit

$$b_2(u(y), v(x)) \equiv a(y,x) \pmod{p^k} \text{ für alle } x, y \in L_1$$

In Matrizen bzgl. Gitterbasen von L_1 und L_2 liest sich dies als

$$UB_2V^{tr} = A \Leftrightarrow V^{tr} = B_2^{-1}U^{-1}A.$$

Da U und B_2 invertierbar sind, ist diese Gleichung in $\mathbb{Z}_p$ lösbar. Wir erhalten so eine Cauchy-Folge von Abbildungen, die modulo p^k ($k = 1, 2, 4, 8, \ldots$) Isometrien sind. Da mit $\mathbb{Z}_p$ auch der Matrixring $\mathbb{Z}_p^{n\times n}$ vollständig ist, konvergiert diese Folge gegen eine Isometrie. □

Folgerung 10.28 *$WQ(\mathbb{Z}_p) \cong WQ(\mathbb{F}_p)$.*

Satz 10.29 *Jedes $\mathbb{Z}_p$-Gitter L in einem regulären $\mathbb{Q}_p$-Vektorraum (V, b) läßt sich schreiben als orthogonale Summe*

$$L = (L_a, p^a b_a) \perp (L_{a+1}, p^{a+1} b_{a+1}) \perp \ldots \perp (L_c, p^c b_c)$$

für eindeutige $a \leq c \in \mathbb{Z}$, so dass (L_i, b_i) reguläre $\mathbb{Z}_p$ Gitter (eventuell $= 0$, falls $a < i < c$). (sogenannte Jordanzerlegung).
Ist p ungerade, so sind die Jordankomponenten (L_i, b_i) sind bis auf Isometrie eindeutig und nach Satz 10.27 durch Dimension n_i und Determinante d_i eindeutig bestimmt. Sei $\epsilon_i \in \pm 1$ mit $\epsilon_i := -1 \Leftrightarrow d_i$ ist kein Quadrat. Dann erhalten wir ein p-adisches Symbol für L:

$$L = [(p^a)^{\epsilon_a n_a}, (p^{a+1})^{\epsilon_{a+1} n_{a+1}}, \ldots, (p^c)^{\epsilon_c n_c}].$$

Beweis. Die Existenz folgt durch sukzessives Anwenden von Satz 8.9. Da (V, b) ein regulärer endlich dimensionaler $\mathbb{Q}_p$-Vektorraum ist, gibt es eine eindeutig bestimmte Zahl $a \in \mathbb{Z}$ so dass mit $b' := p^{-a} b$ gilt: $b'(L, L) \subset \mathbb{Z}_p$ und es gibt ein $\ell \in L$ mit $b'(\ell, \ell) \in \mathbb{Z}_p^*$. Nach Satz 8.9 (angewandt auf den bilinearen $\mathbb{Z}_p$-Modul (L, b'), gibt es ein reguläres $\mathbb{Z}_p$-Gitter (L_a, b') mit $(L, b') = (L_a, b') \perp (L', b')$ so dass $b'(L', L') \subset p\mathbb{Z}_p$. Mache weiter mit $(L', p^{-a'} b')$ und erhalte so die Jordanzerlegung. Zur Eindeutigkeit beachte man, dass $E := (L/pL, \overline{b'})$ ein bilinearer $\mathbb{F}_p$-Vektorraum ist mit Radikal $E' = L'/pL'$. Die Determinante von (L_a, b') ist modulo p genau die des bilinearen Raums $(E/E', \overline{b'})$ und damit modulo $(\mathbb{Z}_p^*)^2$ eindeutig bestimmt. Da Dimension und Determinante nach Satz 10.27 das reguläre $\mathbb{Z}_p$-Gitter (L_a, b') eindeutig festlegen folgt daraus die Eindeutigkeit der Jordankomponenten. □

Satz 10.30 *Sei $p \neq 2$. Dann ist $WQ(\mathbb{Q}_p) \cong WQ(\mathbb{F}_p) \oplus WQ(\mathbb{F}_p)$.*

Beweis. Wir definieren zwei Abbildungen δ_p, δ'_p: $WQ(\mathbb{Q}_p) \to W(p) \cong WQ(\mathbb{F}_p)$ wie folgt. Ist (V,q) ein regulärer $\mathbb{Q}_p$-Vektorraum, so wähle ein ganzes $\mathbb{Z}_p$-Gitter L mit $pL^\# \subset L \subset L^\#$. (jedes maximal ganze Gitter erfüllt diese Bedingung) Wie bei $WQ(\mathbb{Q})$ definieren wir

$$\delta_p([V,q]) := [L^\#/L, q_L] \in WQ(p)$$

und

$$\delta'_p([V,q]) := [L/pL^\#, q] \in WQ(\mathbb{F}_p).$$

Es ist $[V,q] \in \ker(\delta_p)$ genau dann wenn jedes maximal ganze Gitter in (V,q) unimodular ist, also ein reguläres bilineares (oder auch quadratisches, da $p \neq 2$) $\mathbb{Z}_p$-Gitter. Dann ist aber $[L,q] \in WQ(\mathbb{Z}_p)$ schon durch $[L/pL,q] = \delta'_p([V,q]) \in WQ(\mathbb{F}_p)$ bestimmt. Klar kann man reguläre quadratische Formen über $\mathbb{F}_p$ zu regulären quadratischen Formen über $\mathbb{Z}_p$ liften, also haben wir δ_p surjektiv und $\ker(\delta_p) \cong WQ(\mathbb{Z}_p) \cong WQ(\mathbb{F}_p)$. Um die Direktheit zu zeigen, brauchen wir eine Untergruppe U von $WQ(\mathbb{Q}_p)$ mit $\delta'_p(U) = \{0\}$ und $\delta_p(U) = W(p)$. Dazu liften wir jede Form aus $WQ(\mathbb{F}_p)$ (mit anisotropen Vertreter A der Dimension 1 bzw. 2) zu einer regulären Form (E,q) in $WQ(\mathbb{Z}_p)$ der gleichen Dimension und betrachten den Raum $V = \mathbb{Q}_p \otimes E$ mit der quadratischen Form pq. In diesem Raum ist (E,pq) ein maximal ganzes Gitter mit $E^\#/E \cong A$. □

	$[1]$	$[\epsilon]$	$[p]$	$[\epsilon p]$
δ_p	0	0	$[1]$	$[\epsilon]$
δ'_p	$[1]$	$[\epsilon]$	0	0

Satz 10.31 $WQ(\mathbb{Q}_2) \cong C_8 \oplus C_2 \oplus C_2$

Beweis. Die Wittgruppe von $\mathbb{Q}_2$ wird erzeugt von den eindimensionalen Formen $[a]$ wo a durch ein Vertretersystem der Quadratklassen $a \in \{1,3,5,7,2,6,10,14\}$ läuft. Da $[a,b] \cong [a+b, ab(a+b)]$ und $[1,7] \sim [3,5] \sim \mathbb{H}$ ist finden wir die folgende Relationenmatrix

$[1]$	$[3]$	$[5]$	$[7]$	$[2]$	$[6]$	$[10]$	$[14]$		$[1]$	$[3]$	$[5]$	$[7]$	$[2]$	$[6]$	$[10]$	$[14]$
1	0	0	1	0	0	0	0		1	0	0	1	0	0	0	0
0	1	1	0	0	0	0	0		0	1	1	0	0	0	0	0
1	0	0	1	−1	0	0	−1		0	0	1	1	0	0	1	−3
1	−1	0	0	1	−1	0	0	$\sim$	0	0	0	2	0	0	0	−2
1	−1	0	0	0	0	1	−1		0	0	0	0	1	0	0	1
1	0	0	−1	0	1	−1	0		0	0	0	0	0	1	−1	−2
2	0	0	0	−2	0	0	0		0	0	0	0	0	0	2	2
0	0	2	0	0	0	−2	0		0	0	0	0	0	0	0	8

Also ist $WQ(\mathbb{Q}_2)$ ein epimorphes Bild von $C_8 \times C_2 \times C_2$. Wir zeigen noch, dass $|WQ(\mathbb{Q}_2)| \geq 32$ ist. Die Abbildung

$$\alpha : WQ(\mathbb{Q}_2) \to WQ(2) \cong C_8 \times C_2,\ [V,q] \mapsto [L^\#/L, \overline{q}]$$

ist ein Epimorphismus. Der Kern von α hat Ordnung ≥ 2, da $(\mathbb{Q}_2^2, q(x,y) := x^2 + xy + y^2)$ ein Element $\neq 0$ im Kern dieser Abbildung ist. □

Bemerkung 10.32 *Den Satz 10.31 hätten wir auch wie folgt einsehen können: Ist $[V,q]$ ein quadratischer Raum über $\mathbb{Q}_2$ so wähle ein maximal gerades $\mathbb{Z}_2$-Gitter L in V. Dann liefert die quadratische Form eine reguläre quadratische Form $\overline{q} : x + L \mapsto q(x) + \mathbb{Z}$ auf der endlichen abelschen Gruppe $L^{\#}/L$. Die Wittklasse von $(L^{\#}/L, \overline{q}) \in WQ(2)$ ist unabhängig von der Wahl von L und wir erhalten so eine Abbildung $\delta_{2,q} : WQ(\mathbb{Q}_2) \to WQ(2)$, die klar surjektiv ist. Der Kern von $\delta_{2,q}$ besteht aus den quadratischen Räumen, die ein gerades unimodulares Gitter enthalten, also ein Gitter L, so dass (L,q) ein regulärer quadratischer $\mathbb{Z}_2$-Modul ist. Dann ist (L,q) aber schon durch $(L/2L, q + 2\mathbb{Z}_2) \in WQ(\mathbb{F}_2) \cong C_2$ bestimmt, also erhalten wir insgesamt $WQ(\mathbb{Q}_2) \cong WQ(2) \times WQ(\mathbb{F}_2) \cong C_8 \times C_2 \times C_2$.*

10.4 Das lokal-global Prinzip für rationale quadratische Formen.

Die Abbildung $\delta_p : WQ(\mathbb{Q}) \to W(p)$ faktorisiert über $WQ(\mathbb{Q}_p)$,

$$WQ(\mathbb{Q}) \to WQ(\mathbb{Q}_p) \to W(p), [V,q] \mapsto [\mathbb{Q}_p \otimes V, q] \mapsto [L^{\#}/L, b_L].$$

Also ergibt sich der folgende Satz von Hasse und Minkowski.

Folgerung 10.33 *(Hasse-Minkowski, schwache Form) Eine rationale quadratische Form ist hyperbolisch, genau dann wenn alle ihre Vervollständigungen hyperbolisch sind.*
Zwei reguläre rationale quadratische Räume (E_1, q_1) und (E_2, q_2) sind isometrisch genau dann wenn $(\mathbb{R} \otimes E_1, q_1) \cong (\mathbb{R} \otimes E_2, q_2)$ und $(\mathbb{Q}_p \otimes E_1, q_1) \cong (\mathbb{Q}_p \otimes E_2, q_2)$ für alle Primzahlen p.

Es gilt sogar der folgende starke Satz von Hasse und Minkowski für dessen Beweis (der nicht so schwierig ist) auf Kneser's Buch oder auch auch auf Scharlau verweisen.

Satz 10.34 *Sei (V,q) ein regulärer quadratischer $\mathbb{Q}$-Vektorraum. Genau dann ist der Witt-Index $\operatorname{ind}(V,q) > 0$ wenn $\operatorname{ind}(V \otimes \mathbb{R}, q) > 0$ ist und $\operatorname{ind}(V \otimes \mathbb{Q}_p, q) > 0$ ist für alle Primzahlen p.*

Folgerung 10.35 *(a)* $\operatorname{ind}(V,q) = \min\{\operatorname{ind}(V \otimes \mathbb{Q}_p, q) \mid p\} \cup \{\operatorname{ind}(V \otimes \mathbb{R}, q)\}$
(b) Jede indefinite rationale quadratische Form der Dimension ≥ 5 ist isotrop.
(c) Eine reguläre rationale quadratische Form stellt eine Zahl $t \in \mathbb{Q}^*$ dar, genau dann wenn sie über $\mathbb{R}$ und allen $\mathbb{Q}_p$ die Zahl t darstellt.

10.5 Zusammenfassung: Quadratische Formen und orthogonale Gruppen.

Ein Teilmodul $F \leq (E,q)$ heißt scharf primitiv, falls F ein freier A-Modul ist und $(b_q)_F(E) = F^*$.

Der Satz von Witt. Sind F, G scharf primitive freie Teilmoduln des quadratischen A-Moduls (E,q) über dem lokalen Ring A und ist Sei $t : F \to G$ eine bijektive Isometrie so gibt es $\tilde{t} \in O(E,q)$ mit $t = \tilde{t}_{|F}$.

Zusatz: Die Abbildung $\tilde{t}$ kann als Produkt von Spiegelungen gewählt werden, wenn $2 \in A^*$ und $q(E)$ nicht im maximalen Ideal von A liegt.

Als Folgerung ergibt sich der
Wittscher Kürzungssatz Sei A ein lokaler Ring und F, G_1, G_2 quadratische A-Moduln mit F regulär so dass $F \perp G_1 \cong F \perp G_2$. Dann ist $G_1 \cong G_2$.

Eine weitere wichtige Folgerung ist die Definition des Witt-Index, $\mathrm{ind}(E, q)$, als die Dimension jedes maximal total isotropen scharf primitiven Teilmoduls von (E, q). Ist $n := \mathrm{ind}(E)$, so ist

$$(E, q) \cong \mathbb{H}(A^n) \perp (F, q_{|F})$$

mit $\mathrm{ind}(F) = 0$. Dabei ist der hyperbolische Modul $\mathbb{H}(A^n) = \langle e_1, \ldots, e_n, f_1, \ldots, f_n \rangle$ mit $q(e_i) = q(f_i) = 0$ für alle i und $b_q(f_i, e_j) = \delta_{ij}$.

Eine weitere Folgerung der Witt'schen Theorie ist die Einführung von Wittgruppen. Die Addition in der Wittgruppe ist die orthogonale Summe und wir setzen die hyperbolischen Moduln gleich 0. Dann hat jede Klasse einen eindeutigen anisotropen Vertreter nach dem Satz von Witt und es gilt $-[(E, q)] = [(E, -q)]$. Wir haben die Wittgruppen von $\mathbb{Q}$ und allen $\mathbb{Q}_p$ bestimmt. Wesentlich hier war dass die Klasse (in der Wittgruppe der endlichen quadratischen Gruppen, die wir etwas anders definieren mussten als für Körper) der Diskriminantengruppe eines ganzen Gitters in (E, q) unabhängig von der Wahl des Gitters war.

Insbesondere erhalten wir das lokal-global Prinzip für quadratische Formen, der schwache Satz von Hasse und Minkowski.

Der Diagonalisierungssatz 8.9 sagt aus dass jeder freie A-Modul über einem lokalen Ring A mit maximalem Ideal I von der Form

$$E = E_1 \perp \ldots \perp E_r \perp F$$

mit $b(F, F) \subset I$, E_i regulär $\dim(E_i) = 1$ oder 2 ist. Ist $2 \in A^*$, so können alle E_i eindimensional gewählt werden. Es gilt: E ist regulär genau dann wenn $F = 0$.

Zusammen mit dem Satz von Witt lieferte dies uns eine Klassifikation der orthogonalen Gruppen über endlichen Körpern, ein Verfahren zur rekursiven Berechnung der Gruppenordnung, welche wir dann benutzt haben, um die Massformeln für selbstduale Codes herzuleiten.

Ziel wäre nun ein analoges Ergebnis für Gitter. Dazu müssen wir zunächst einmal eine Menge von Gittern auszeichnen, auf denen eine Gruppe transitiv operiert und welche aus endlich vielen Isometrieklassen besteht. Der richtige Begriff hier ist das Geschlecht, genauer noch das Spinorgeschlecht. Zwei Gitter (L_1, q_1) und (L_2, q_2) gehören zum gleichen Geschlecht, falls für alle Primzahlen p gilt

$$(\mathbb{Z}_p \otimes L_1, q_1) \cong (\mathbb{Z}_p \otimes L_2, q_2)$$

und $(\mathbb{R} \otimes L_1, q_1) \cong (\mathbb{R} \otimes L_2, q_2)$.

Ein Geschlecht von Gittern besteht nach Folgerung 11.7 aus endlich vielen Isometrieklassen. Die Gruppe, die transitiv auf dem Geschlecht operiert ist die adelische orthogonale Gruppe.

Der Adelering $\mathbb{A}$ wurde eingeführt um formal korrekt "lokal überall" zu sagen.

$$\mathbb{A} = \{(a_\infty, a_2, a_3, a_5, \ldots) \in \mathbb{R} \times \prod_p \mathbb{Q}_p \mid a_p \in \mathbb{Z}_p \text{ für fast alle } p\}.$$

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist diagonal eingebettet in den Adelering. Ist (V, q) ein quadratischer $\mathbb{Q}$-Vektorraum, so wird $\mathbb{A} \otimes_{\mathbb{Q}} V$ durch Forsetzung quadratischen Form zu einem $\mathbb{A}$-Modul. Die orthogonale Gruppe $O(\mathbb{A} \otimes V, q)$ operiert auf der Menge aller Gitter in V wie folgt:

Jedes $\mathbb{Z}$-Gitter L in V ist durch die Menge seiner Vervollständigungen $\{\mathbb{Z}_p \otimes L \mid p \in \P\}$ eindeutig bestimmt. Ist $L \leq V$ ein $\mathbb{Z}$-Gitter, und $g = (g_\infty, g_2, g_3, g_5, \ldots) \in O(\mathbb{A} \otimes V, q)$ so sei $M := Lg$ das Gitter in V mit $M \otimes \mathbb{Z}_p = (L \otimes \mathbb{Z}_p)g_p$ für alle p. Man beachte hierbei, dass $(L \otimes \mathbb{Z}_p)g_p = L \otimes \mathbb{Z}_p$ für alle bis auf endlich viele p. Die Bahn von L unter der adelischen orthogonalen Gruppe ist dann genau das Geschlecht von L.

Der Stabilisator von L ist

$$G := \{(g_\infty, g_2, g_3, g_5, \ldots) \mid g_p \in O(L \otimes \mathbb{Z}_p) \text{ für alle } p\}$$

Zwei Gitter $L, M \leq (V, q)$ sind isometrisch, wenn sie in derselben Bahn unter der orthogonalen Gruppe $O(V, q)$ liegen. Die Isometrieklassen von Gittern im Geschlecht von L entsprechen also den Doppelnebenklassen $[Lx_i] \mapsto Gx_iO(V, q)$

$$O(\mathbb{A} \otimes V, q) = \dot{\cup}_{i=1}^{h} Gx_iO(V, q).$$

Ist $L_i := Lx_i$ ein Vertreter der i-ten Isometrieklasse im Geschlecht von L, so ist $\mathrm{Stab}_{O(\mathbb{A}\otimes V,q)}(L) = x_i^{-1}GX_i =: G_i$ und die Automorphismengruppe von L_i der Schnitt $\mathrm{Aut}(L_i) = G_i \cap O(V, q)$.

Darauf werden wir später nochmal zurückkommen und die Herleitung der Minkowski-Siegel Massformel für

$$\sum_{i=1}^{h} |\mathrm{Aut}(L_i)|^{-1}$$

skizzieren. Näheres finden Sie in dem Buch A. Weil, Adeles and algebraic groups. oder dem Artikel von M. Kneser, Semi-simple algebraic groups.

11 Geschlechter von Gittern.

11.1 Die Endlichkeit der Klassenzahl.

Für $\mathbb{Q}$ gilt nach dem Satz von Hasse und Minkowski das sogenannte lokal-global-Prinzip, rationale quadratische Räume sind isometrisch, genau dann wenn alle ihre Komplettierungen isometrisch sind. Dies gilt für Gitter im allgemeinen nicht.

Definition 11.1 *Zwei $\mathbb{Z}$-Gitter (L_1, q_1) und (L_2, q_2) heißen* rational äquivalent*, falls die zugrundeliegenden quadratischen $\mathbb{Q}$-Vektorräume $(\mathbb{Q} \otimes L_1, q_1)$ und $(\mathbb{Q} \otimes L_2, q_2)$ isometrisch sind. (L_1, q_1) und (L_2, q_2) gehören* zum gleichen Geschlecht*, falls für alle Primzahlen p gilt*

$$(\mathbb{Z}_p \otimes L_1, q_1) \cong (\mathbb{Z}_p \otimes L_2, q_2)$$

und $(\mathbb{R} \otimes L_1, q_1) \cong (\mathbb{R} \otimes L_2, q_2)$.

Bemerkung 11.2 *Seien* (L_1, q_1) *und* (L_2, q_2) *im gleichen Geschlecht.*
Dann sind die beiden Gitter auch rational äquivalent und es gilt $L_1^\# / L_1 \cong L_2^\# / L_2$.

Beispiel. Die 2-dimensionalen Gitter mit Grammatrizen $\begin{pmatrix} 2 & 1 \\ 1 & 12 \end{pmatrix}$ und $\begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}$ gehören zum gleichen Geschlecht, sind aber nicht isometrisch.

Lemma 11.3 *(Gleichheit von Gittern ist eine lokale Eigenschaft.) Sei* V *ein endlich dimensionaler* $\mathbb{Q}$*-Vektorraum,* $L \leq V$ *ein volles* $\mathbb{Z}$*-Gitter in* V*. Die Abbildungen*

$$M \mapsto \{\mathbb{Z}_p \otimes M \mid p \in \mathbb{P}\}, \quad \{M_p \mid p \in \mathbb{P}\} \mapsto \bigcap_{p \in \mathbb{P}} (V \cap M_p)$$

sind zueinander inverse Bijektionen von der Menge $\mathcal{L}(V)$ *der vollen* $\mathbb{Z}$*-Gitter* M *in* V *und der Menge* $\mathcal{F}(L)$ *aller Folgen* $\{M_p \mid p \in \mathbb{P}\}$ *von vollen* $\mathbb{Z}_p$*-Gittern* M_p *in* $V \otimes \mathbb{Q}_p$ *, für die* $M_p = L \otimes \mathbb{Z}_p$ *gilt für alle bis auf endlich viele* p*.*

Beweis. Ist $M \leq V$ ein volles $\mathbb{Z}$-Gitter, so ist die Basiswechselmatrix A zwischen einer Gitterbasis von L und einer Gitterbasis von M in $\mathrm{GL}_n(\mathbb{Q})$. Die Nenner ihrer Einträge involvieren nur endlich viele Primzahlen und ebenso der Zähler ihrer Determinante. Also ist $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ für alle bis auf endlich viele Primzahlen p und für diese p ist dann $M \otimes \mathbb{Z}_p = L \otimes \mathbb{Z}_p$. Ist umgekehrt $\{M_p \mid p \in \mathbb{P}\} \in \mathcal{F}(L)$, so ist der Durchschnitt $\bigcap_{p \in \mathbb{P}} (V \cap M_p)$ ein volles Gitter in V. Denn nach Voraussetzung ist $M_p = L \otimes \mathbb{Z}_p$ für fast alle p. Für die übrigen Primzahlen p gibt es Zahlen a_p und $b_p \in \mathbb{Z}$ mit

$$p^{a_p}(L \otimes \mathbb{Z}_p) \subset M_p \subset p^{b_p}(L \otimes \mathbb{Z}_p).$$

Also ist

$$\prod_p p^{a_p} L \subset \bigcap_{p \in \mathbb{P}} (V \cap M_p) \subset \prod_p p^{b_p} L$$

zwischen zwei Gittern eingefangen und damit selbst ein Gitter.
Es bleibt zu zeigen, dass die Komposition der beiden Abbildungen die Identität ergibt.
Für $M \in \mathcal{L}(V)$ ist $M = \bigcap_{p \in P} (V \cap (M \otimes \mathbb{Z}_p))$. Ist nämlich $(b_1, \ldots, b_n)$ eine Gitterbasis von M, so ist $\sum_{i=1}^n a_i b_i \in V \cap (M \otimes \mathbb{Z}_p)$ genau dann wenn $a_i \in \mathbb{Q}$ sind und die Nenner von a_i nicht durch p teilbar ($a_i \in \mathbb{Q} \cap \mathbb{Z}_p$). Es ist aber $\bigcap_{p \in \mathbb{P}} (\mathbb{Q} \cap \mathbb{Z}_p) = \mathbb{Z}$.
Andersherum sei $\{M_p \mid p \in \mathbb{P}\} \in \mathcal{F}(L)$. Es ist zu zeigen, dass für alle Primzahlen q gilt $M_q = \mathbb{Z}_q \otimes (\bigcap_{p \in \mathbb{P}} (V \cap M_p))$. Klar ist $M_q \supset \mathbb{Z}_q \otimes (\bigcap_{p \in \mathbb{P}} (V \cap M_p))$. Umgekehrt sei $M := \bigcap_{p \in \mathbb{P}} (V \cap M_p) \in \mathcal{L}(V)$ und $B := (b_1, \ldots, b_n)$ eine Gitterbasis von M. Da B eine $\mathbb{Q}$-Basis von V bildet und somit auch eine $\mathbb{Q}_q$-Basis von $V \otimes \mathbb{Q}_q$, lässt sich jedes Element von M_q schreiben als $\sum_{i=1}^n a_i b_i$ mit $a_i \in \mathbb{Q}_q$. Schreibe $a_i = a_i' + a_i''$ mit $a_i' = \frac{c_i}{q^m}$, $c_i \in \mathbb{Z}$ für geeignetes $m \in \mathbb{Z}$, $a_i'' \in \mathbb{Z}_q$, so ist jedenfalls $\sum_{i=1}^n a_i'' b_i \in \mathbb{Z}_q \otimes M \subset M_q$. Damit ist aber auch $\sum_{i=1}^n a_i' b_i \in M_q$. Da $a_i' \in \mathbb{Q}$ ist, gilt sogar

$$\sum_{i=1}^n a_i' b_i \in M_q \cap V$$

Die Nenner der a_i sind alles Potenzen von q und daher ist auch für $p \neq q$

$$\sum_{i=1}^{n} a_i' b_i \in (M \otimes \mathbb{Z}_p) \cap V \subset M_p \cap V$$

also $\sum_{i=1}^{n} a_i b_i \in M + \mathbb{Z}_q \otimes M = \mathbb{Z}_q \otimes M$. □

Folgerung 11.4 *Zwei Gitter $L, L' \leq V$ sind genau dann gleich, wenn $L \otimes \mathbb{Z}_p = L' \otimes \mathbb{Z}_p$ für alle Primzahlen p.*

Lemma 11.5 *Sei $r \geq 1$, $s \geq 0$. Dann gibt es eine Konstante $T := T(r,s) > 0$, so dass jedes ganze Gitter L in einem rationalen bilinearen Raum (V, b) der Dimension $n = r + s$ und Signatur $r - s$ einen Vektor $a \in L$ enhält mit*

$$0 < b(a,a) \leq T |\det(L)|^{1/n}$$

Man kann $T^n = 3^s (4/3)^{n(n-1)/2}$ wählen.

Beweis. Sei $d := |\det(L)|$. Induktion über n.
$n = 1$ Klar.
$n > 1$: Sei $q := q_b$ und $m := \min\{q(a) \mid a \in L, q(a) > 0\}$ und $a_1 \in L$ mit $m = q(a_1) = b(a_1, a_1)$. Ergänze a_1 zu einer Gitterbasis $(a_1, a_2, \ldots, a_n)$ von L. Dann ist

$$mq(\sum_{i=1}^{n} x_i a_i) = (mx_1 + z_2 x_2 + \ldots + z_n x_n)^2 + q'(\sum_{i=2}^{n} x_i a_i)$$

(quadratische Ergänzung), in Matrizen:

$$mB = \begin{pmatrix} m^2 & mz_2 & \ldots & mz_n \\ mz_2 & & & \\ \vdots & & A & \\ mz_n & & & \end{pmatrix} = \begin{pmatrix} m \\ z_2 \\ \vdots \\ z_n \end{pmatrix} (m, z_2, \ldots, z_n) + \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}$$

mit $B'_{ij} = A - z_i z_j$ für alle $2 \leq i, j \leq n$. Also ist

$$\det(mB) = m \det \begin{pmatrix} m & mz_2 & \ldots & mz_n \\ z_2 & & & \\ \vdots & & A & \\ z_n & & & \end{pmatrix} = m \det \begin{pmatrix} m & 0 & \ldots & 0 \\ z_2 & & & \\ \vdots & & B' & \\ z_n & & & \end{pmatrix} = m^2 \det(B').$$

Es ist $|\det(mq)| = m^n d$, also $|\det(q')| = m^{n-2} d$, $\dim(q') = n - 1$.
1) Ist $r > 1$, so gilt unsere Voraussetzung auch für q' und es gibt ein $b' \in \langle a_2, \ldots, a_n \rangle$ mit

$$0 < q'(b') \leq T'(m^{n-2} d)^{1/(n-1)}.$$

Setze $b := x_1 a_1 + b' = \sum x_i a_i$ mit $|mx_1 + \sum_{j=2}^{n} z_j x_j| \leq \frac{1}{2} m$. Dann ist

$$m^2 \leq mq(b) \leq \frac{1}{4} m^2 + T'(m^{n-2} d)^{1/(n-1)}$$

also $\frac{3}{4}m^2 \leq T'(m^{n-2}d)^{1/(n-1)}$ und somit $(m^2)^{n-1} \leq (\frac{4}{3}T')^{n-1}dm^{n-2}$, oder auch

$$m^n \leq (\frac{4}{3}T')^{n-1}d.$$

2) Ist $r = 1$, so ist q' negativ definit, aber dann gilt unsere Induktionsvoraussetzung für $-q'$. D.h. es gibt ein $b' \in \langle a_2, \ldots, a_n\rangle_{\mathbb{Z}}$ mid $0 < -q(b') \leq T''(m^{n-2}d)^{1/(n-1)}$, wobei $T'' = T(s, 0)$ ist. Nun wählen wir $b = x_1a_1 + b' = \sum x_ia_i \in L$ so dass $\frac{1}{2}m \leq |mx_1 + \sum_{j=2}^n z_jx_j| \leq m$. Dann ist

$$q(b) = \frac{1}{m}|mx_1 + \sum_{j=2}^{n} z_jx_j|^2 + \frac{1}{m}q'(b') < m$$

also $q(b) \leq 0$ wegen der Wahl von m. Damit ist

$$0 \leq -q(b)m \leq \frac{1}{4}m^2 + (-q'(b')) \leq \frac{1}{4}m^2 + T''(m^{n-2}d)^{1/(n-1)}.$$

Also

$$m^n \leq (4T'')^{n-2}d.$$

Beachten Sie, der Fall 2) kommt genau dann einmal vor, wenn $s > 0$ ist. □

Satz 11.6 *Für gegebene Determinante $d \neq 0$ und Dimension n gibt es bis auf Isometrie nur endlich viele ganze $\mathbb{Z}$-Gitter.*

Beweis. Zu gegebenen d, n gibt es nur endlich viele rationale Räume (V, b). Also Œ (V, b) fest, b nicht negativ definit (sonst $-b$ betrachten) und $L \leq (V, b)$ ein ganzes Gitter mit $\det(L) = d$. Dann gibt es nach Lemma 11.5 ein $a \in L$ mit

$$0 < m =: q(a) \leq T|d|^{\frac{1}{n}}.$$

Für $m \in \mathbb{Z}$ gibt es nur endlich viele Möglichkeiten. Sei $(a = a_1, a_2, \ldots, a_n)$ eine Gitterbasis von L und

$$mq(\sum_{i=1}^{n} x_ia_i) = (mx_1 + z_2x_2 + \ldots + z_nx_n)^2 + q'(\sum_{i=2}^{n} x_ia_i)$$

Addiert man geeignete Vielfache von a zu den a_i $(2 \leq i \leq n)$ so kann man erreichen, dass alle $|z_j| < m$ sind $(2 \leq j \leq n)$. Also hat man nur endlich viele Möglichkeiten für die z_j. Da $\det(q') = m^{n-2}d$ ist, gibt es nur endlich viele Möglichkeiten für q' bis auf Isometrie. □

Folgerung 11.7 *Jedes Geschlecht von Gittern enthält nur endlich viele Isometrieklassen.*

Beweis. Dimension und Determinante sind Geschlechtsinvarianten. □

Beispiel: Positiv definite Gitter der Dimension 2 mit Determinante 23: 4 Isometrieklassen, 2 Geschlechter:

$$\begin{pmatrix} 1 & 0 \\ 0 & 23 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 1 & 8 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 12 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}.$$

$d = 23, n = 2, s = 0 \Rightarrow m \leq 2\sqrt{23}/\sqrt{3} \sim 5.5$. Brauchen also alle Matrizen $\begin{pmatrix} m & b \\ b & c \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ mit $m = 1, 2, 3, 4, 5$, $0 \leq b \leq m/2$, $m \leq c$, $mc - b^2 = 23$.

11.2 Unimodulare Gitter.

Beispiel 11.8 *Unimodulare Gitter kleiner Dimension. Ist $L = L^{\#}$ ein positiv definites unimodulares Gitter der Dimension $n \leq 5$, so enthält L nach der Hermite Ungleichung einen Vektor $a \neq 0$ mit $b(a,a) \leq (4/3)^{(n-1)/2} \leq \frac{16}{9} < 2$. Also ist $b(a,a) = 1$ und $L = \langle a \rangle \perp M$ mit $M = M^{\#}$, $\dim(M) = n-1$. Somit erhalten wir $L = \mathbb{Z}^n$, es gibt also nur eine Klasse unimodularer Gitter der Dimension $n \leq 5$.*

Satz 11.9 *Sind L, M gerade unimodulare Gitter gleicher Signatur (r,s), so liegen L und M im gleichen Geschlecht.*

Beweis. $\mathbb{R} \otimes L \cong \mathbb{R} \otimes M$, da beide Räume die gleiche Signatur haben. Außerdem gilt $\det(L) = \det(M) = (-1)^s$. Also sind die regulären quadratischen Räume L/pL und M/pM für alle ungeraden Primzahlen p isometrisch. Nach Satz 10.27 gilt dies daher auch für die p-adischen Gitter $\mathbb{Z}_p \otimes L$ und $\mathbb{Z}_p \otimes M$.
Für $p = 2$ hilft uns die Determinante modulo 2 wenig. Jedoch sind $\mathbb{Z}_2 \otimes L$ und $\mathbb{Z}_2 \otimes M$ orthogonale Summe 2-dimensionaler regulärer quadratischer $\mathbb{Z}_2$-Moduln. Davon gibt es genau 2, nämlich

$$\mathbb{H} := \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \text{ und } N := \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$$

mit Determinante -1 bzw. 3 (in $\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2$). Es ist $N \perp N \cong \mathbb{H} \perp \mathbb{H}$. Ein Vergleich der Determinanten zeigt also, dass

$$\mathbb{Z}_2 \otimes L \cong \mathbb{Z}_2 \otimes M \cong \mathbb{H}^{(r+s)/2}$$

ist. □

Bemerkung. Insbesondere ergibt sich aus dem obigen Beweis, dass $(-1)^s = (-1)^{(r+s)/2}$ also $r - s \equiv 0 \pmod 4$ sein. Es gilt sogar $r - s \equiv 0 \pmod 8$.

Lemma 11.10 *Sind L, M unimodulare Gitter gleicher Signatur so gilt $\mathbb{Q}L \cong \mathbb{Q}M$ und $\mathbb{Z}_p \otimes L \cong \mathbb{Z}_p \otimes M$ für alle Primzahlen $p \neq 2$.*

Beweis. $\mathbb{Q}L \cong \mathbb{Q}M$ wegen Folgerung 10.25, denn beide Räume haben die gleiche Signatur und triviales δ_p für alle Primzahlen p. Die p-adische Isometrie folgt wie in Satz 11.9, da $2 \in \mathbb{Z}_p^*$ für ungerades p. □

Lemma 11.11 *Jedes ungerade unimodulare $\mathbb{Z}_2$-Gitter L hat eine Orthogonalbasis $(e_1, \ldots, e_n)$ (vgl. Satz 8.13 (a)). Diese kann so gewählt werden, dass $b(e_i, e_i) = \pm 1$ ist für $i = 1, \ldots, n-1$. $b(e_n, e_n)$ ist dann durch die Determinante von L festgelegt.*

Beweis. Zunächst konstruieren wir die Orthogonalbasis analog zum Beweis von Satz 8.13 (a). Sei $e_1 \in L$ mit $b(e_1, e_1) \in \mathbb{Z}_2^*$. Dann ist $L = \langle e_1 \rangle \perp M$ mit einem unimodularen Gitter M. Ist M ungerade, so können wir mit M weitermachen. Sonst ist $b(m,m) \in 2\mathbb{Z}_2$ für alle $m \in M$ und es gibt $m_1, m_2 \in M$ mit $b(m_1, m_2) = 1$. Ersetze nun e_1 durch $e_1' := e_1 + m_1$. Dann ist $b(e_1', e_1')$

immer noch ungerade, und daher $L = \langle e_1' \rangle \perp M'$ mit einem unimodularen Gitter M'. Aber jetzt ist M' ungerade, was man wie im Beweis von 8.13 sieht, denn $m' := e_1 - b(e_1, e_1)m_2 \in M'$ erfüllt $b(m', m') = b(e_1, e_1) + b(e_1, e_1)^2 b(m_2, m_2) \in \mathbb{Z}_2^*$.
So erhält man also rekursiv eine OG-Basis $(e_1, \ldots, e_n)$ von L. Sei $a_i := b(e_i, e_i)$. Ist $a_i \equiv \pm 1 \pmod 8$, so kann man e_i durch te_i ersetzen so dass $t^2 a_i = \pm 1$ ist, da jedes Element in $1 + 8\mathbb{Z}_2 = (\mathbb{Z}_2^*)^2$. Ist $a_i \equiv \pm 3 \pmod 8$ und $i < n$, so ersetze e_i durch $e_i' = e_i + 2e_n$ mit $b(e_i', e_i') \equiv_8 a_i + 4 \equiv_8 \pm 1$. □

Bemerkung 11.12 *Hat L aus Lemma 11.11 die Determinante ± 1, so hat L eine OG-Basis $(e_1, \ldots, e_n)$ mit $b(e_i, e_i) = \pm 1$. Also ist $L = \mathbb{Z}_2 \otimes I_{r,s}$ mit $I_{r,s} = (\mathrm{diag}(1^r, (-1)^s))$.*

Daraus ergibt sich direkt der folgende Satz.

Satz 11.13 *Zu jedem Paar $(r, s) \in \mathbb{N}_0 \times \mathbb{N}_0$ gibt es genau ein Geschlecht ungerader unimodularer Gitter der Signatur (r, s). Dieses wird durch das Gitter $I_{r,s} = (\mathrm{diag}(1^r, (-1)^s))$ repräsentiert.*

11.3 Darstellungen über $\mathbb{Z}$.

Nach dem starken Satz von Hasse-Minkowski ist

$$t \in q(V) \Leftrightarrow t \in q(V \otimes \mathbb{Q}_p) \text{ für alle } p \in \mathbb{P} \cup \{\infty\}.$$

Über $\mathbb{Z}$ gilt der folgende Satz:

Satz 11.14 *Sei L ein $\mathbb{Z}$-Gitter im regulären quadratischen $\mathbb{Q}$-Vektorraum (V, q), $t \in \mathbb{Q}^*$ mit $t \in q(\mathbb{R} \otimes L)$ und $t \in q(\mathbb{Z}_p \otimes L)$ für alle $p \in \mathbb{P}$. Dann gibt es ein Gitter M im Geschlecht von L mit $t \in q(M)$.*

Beweis. Da $t \in q(L \otimes \mathbb{Z}_p) \subset q(V \otimes \mathbb{Q}_p)$ ist für alle $p \in \mathbb{P} \cup \{\infty\}$ folgt nach dem Satz von Hasse-Minkowski (starke Form), dass es ein $v \in V = \mathbb{Q} \otimes L$ gibt mit $q(v) = t$. Dann ist $v = \sum a_i b_i$ für eine Gitterbasis $(b_1, \ldots, b_n)$ von L und in den Nennern der a_i treten nur endlich viele Primteiler auf. Bezeichne S die Menge dieser Primzahlen. Dann ist S endlich. Für $p \in S$ sei $x_p \in L \otimes \mathbb{Z}_p$ mit $q(x_p) = t$. Aus dem Satz von Witt folgt, dass es ein $u_p \in O(V \otimes \mathbb{Q}_p)$ gibt mit $u_p(x_p) = v$. Jetzt betrachten wir

$$M := \bigcap_{p \notin S} (V \cap (L \otimes \mathbb{Z}_p)) \cap \bigcap_{p \in S} (u_p(L \otimes \mathbb{Z}_p) \cap V).$$

Dann ist M nach Lemma 11.3 ein Gitter in V und es gilt $M \otimes \mathbb{Z}_p = L \otimes \mathbb{Z}_p$ für $p \notin S$ und $M \otimes \mathbb{Z}_p = u_p(L \otimes \mathbb{Z}_p) \cong L \otimes \mathbb{Z}_p$ für $p \in S$. Also liegt M im Geschlecht von L und es ist $x \in M$. □

Folgerung 11.15 *Besteht das Geschlecht von L nur aus der Klasse von L, so stellt auch L die Zahl t dar.*

Da die Geschlechter von $\mathbb{Z}^n$ für $n = 1, 2, 3, 4, 5$ nur aus einer Klasse bestehen ergeben sich insbesondere die folgenden klassischen Resultate.

Folgerung 11.16 *(Euler 1749) Eine Zahl $t \in \mathbb{Z} - \{0\}$ ist genau dann Summe von 2 Quadraten in $\mathbb{Z}$, wenn $t > 0$ und t keine Primzahl $p \equiv_4 3$ zu einer ungeraden Potenz enthält.*

Folgerung 11.17 *(Gauß 1801) Eine Zahl $t \in \mathbb{Z} - \{0\}$ ist genau dann Summe von 3 Quadraten in $\mathbb{Z}$, wenn $t > 0$ nicht von der Form $t = 4^a(8b + 7)$ ist.*

Folgerung 11.18 *(Lagrange 1770) Jede positive ganze Zahl ist Summe von 4 Quadraten.*

12 Clifford Algebren und die Spinornorm.

12.1 Die Clifford Algebra.

Sei K ein Körper der Charakteristik $\neq 2$ und (E, q) ein regulärer quadratischer K-Vektorraum. Dann ist die orthogonale Gruppe

$$O(E, q) := \{\varphi \in \mathrm{GL}(E) \mid q(\varphi(x)) = q(x) \text{ für alle } x \in E\}$$

nach dem Beweis vom Satz von Witt von Spiegelungen erzeugt. Jede orthogonale Abbildung hat Determinante ± 1, jede Spiegelung hat Determinante -1, also ist

$$O(E, q) = S(E) > SO(E, q) = \langle \sigma_x \sigma_y \mid x, y \in E, q(x)q(y) \neq 0 \rangle$$

ein Normalteiler vom Index 2 in $O(E, q)$. Wir wollen neben der Determinante eine weitere Abbildung $O(E, q) \to K^*/(K^*)^2$ konstruieren, die sogenannte Spinornorm.

Definition 12.1 *Für den Vektorraum E definieren wir die* Tensoralgebra

$$T(E) := K \oplus E \oplus E \otimes E \oplus \ldots = \bigoplus_{j=0}^{\infty} \otimes^j E$$

Dies ist eine unendlich dimensionale $\mathbb{N}_0$-graduierte Algebra mit Multiplikation definiert durch die distributive Fortsetzung von

$$\otimes^j E \times \otimes^k E \to \otimes^{j+k} E, (t, s) \mapsto t \otimes s.$$

Die Clifford Algebra *von (E, q) ist die Faktoralgebra von $T(E)$ modulo dem von $\{x \otimes x - q(x)1 \mid x \in E\}$ erzeugten zweiseitigen Ideal*

$$\mathcal{C}(E, q) := T(E)/\langle x \otimes x - q(x)1 \mid x \in E \rangle.$$

Bemerkung 12.2 *Da $q(x + y) = q(x) + q(y) + b_q(x, y)$ ist, gilt für alle $x, y \in E$*

$$xy + yx = b_q(x, y), x^2 = q(x) \in \mathcal{C}(E, q).$$

Insbesondere antikommutieren orthogonale Vektoren und jedes $x \in E$ mit $q(x) \neq 0$ besitzt ein Inverses $x^{-1} = q(x)^{-1}x$.

Vergleichen Sie das mit den Spiegelungen, die auch nur dann definiert sind, wenn $q(x)$ eine Einheit ist.

Satz 12.3 *Die Abbildung $\iota : V \to \mathcal{C}(V,q)$ hat folgende universelle Eigenschaft:*
Ist A eine K-Algebra und $f : V \to A$ eine K-lineare Abbildung mit $f(x)^2 = q(x)$, so gibt es genau einen K-Algebrenhomomorphismus $g : \mathcal{C}(V,q) \to A$ mit $f = g \circ \iota$.

Beweis. Dies folgt aus der universellen Eigenschaft der Tensoralgebra. Nach dieser gibt es einen eindeutigen K-Algebrenhomomorphismus $h : T(V) \to A$ mit $h(v) = f(v)$ für alle $v \in V$. Da aber $f(v)^2 = q(v)$ gilt liegt das Ideal $I(q)$ im Kern von h, also faktorisiert h über $T(V)/I(q) = \mathcal{C}(V,q)$. □

Beispiel 12.4 $\mathcal{C}([a]) \cong K[X]/(X^2 - a)$.

Bemerkung 12.5 *Die Clifford-Algebra erbt von der Tensoralgebra eine natürliche $\mathbb{F}_2$-Graduierung, da $I(q)$ von Elementen geraden Grades erzeugt wird. Setzt man für $\epsilon = 0, 1$*

$$T_\epsilon(V) := \bigoplus_{n=0}^{\infty} \otimes^{2n+\epsilon} V,\ I_\epsilon(q) := I(q) \cap T_\epsilon(V)$$

so ist $I(q) = I_0(q) \oplus I_1(q)$ und mit $\mathcal{C}_\epsilon(V,q) := T_\epsilon / I_\epsilon$ wird $\mathcal{C}(V,q) = \mathcal{C}_0(V,q) \oplus \mathcal{C}_1(V,q)$.

Definition 12.6 *Das* graduierte Tensorprodukt *zweier $\mathbb{F}_2$-graduierter K-Algebren $A = A_0 \oplus A_1$, $B = B_0 \oplus B_1$ ist die graduierte K-Algebra $C = A \hat{\otimes} B$ mit*

$$C_0 = A_0 \otimes B_0 \oplus A_1 \otimes B_1,\ C_1 = A_0 \otimes B_1 \oplus A_1 \otimes B_0.$$

Die Multiplikation ist auf den Erzeuger $a_i \otimes b_j$ mit $a_i \in A_i$, $b_j \in B_j$ von C wie folgt definiert:

$$(a_i \otimes b_j)(a'_l \otimes b'_k) = (-1)^{jl} a_i a'_l \otimes b_j b'_k.$$

Insbesondere gilt

$$(a_i \otimes 1)(1 \otimes b_j) = (-1)^{ij}(1 \otimes b_j)(a_i \otimes 1).$$

Wie das Tensorprodukt erfüllt auch das graduierte Tensorprodukt eine universelle Eigenschaft:
Ist D eine graduierte K-Algebra und $f : A \to D$, $g : B \to D$ graduierte K-Algebrenhomomorphismen mit

$$f(a_i)g(b_j) = (-1)^{ij} g(b_j) f(a_i) \text{ für alle } a_i \in A_i, b_j \in B_j, i, j = 0, 1.$$

Dann gibt es einen eindeutig bestimmten K-Algebrenhomomorphismus $h : A \hat{\otimes} B \to D$ mit $f(a) = h(a \otimes 1)$ und $g(b) = h(1 \otimes b)$ für alle $a \in A$, $b \in B$.

Aus der universellen Eigenschaft der Clifford-Algebra und des graduierten Tensorprodukts ergibt sich direkt das folgende Lemma.

Lemma 12.7 $\mathcal{C}((V_1, q_1) \perp (V_2, q_2)) \cong \mathcal{C}(V_1, q_1) \hat{\otimes} \mathcal{C}(V_2, q_2)$.

Satz 12.8 *Ist $(v_1, \ldots, v_n)$ eine Basis von V, so bilden die Produkte*

$$\{v_{i_1} \ldots v_{i_s} \mid s \in \mathbb{N}_0, i_1 < \ldots < i_s\}$$

eine Basis von $\mathcal{C}(V,q)$, insbesondere ist $\dim(\mathcal{C}(V,q)) = 2^{\dim(V)}$.

Beweis. Folgt aus Beispiel 12.4 und Lemma 12.7. □

12.2 Das Zentrum der Clifford Algebra.

Sei $(v_1, \ldots, v_n)$ eine OG-Basis des regulären quadratischen Raums (V,q). Für $J = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$ mit $i_1 < \ldots < i_s$ bezeichne $v_J = v_{i_1} \cdots v_{i_s}$. Dann gilt

$$(v_i v_j)(\sum_{J \subset \{1,\ldots,n\}} a_J v_J)(v_i v_j)^{-1} = \sum_{J \subset \{1,\ldots,n\}} \epsilon_J a_J v_J$$

mit $\epsilon_J = 1$ genau dann wenn beide oder keines der $\{i,j\}$ in J liegt und $\epsilon_J = -1$ falls genau eines der beiden zu J gehört. Da $\mathcal{C}_0(V,q)$ von den Produkten $v_i v_j$ erzeugt wird, ist v_J genau dann mit allen Elementen aus $\mathcal{C}_0(V,q)$ vertauschbar, wenn $J = \{1, \ldots, n\} =: \underline{n}$. Es ist

$$v_i v_{\underline{n}} v_i^{-1} = (-1)^{n-1} v_{\underline{n}}.$$

Also ergibt sich der folgende Satz.

Satz 12.9 *Sei*

$$C := C_{\mathcal{C}(V,q)}(\mathcal{C}_0(V,q)) := \{c \in \mathcal{C}(V,q) \mid cx = xc \text{ für alle } x \in \mathcal{C}_0(V,q)\}$$

Dann ist $C := K \oplus K(v_1 \cdots v_n)$.
Weiter ist das Zentrum

$$Z := Z(\mathcal{C}(V,q)) = \begin{cases} K & n \text{ gerade} \\ K \oplus K(v_1 \cdots v_n) = C & n \text{ ungerade} \end{cases}$$

12.3 Die Spinornorm.

Definition 12.10 *Sei $\sigma \in O(V,q)$. Dann gilt $q(\sigma(v)) = q(v)$ für alle $v \in V$, also definiert σ einen eindeutig bestimmten K-Algebrenautomorphismus $c(\sigma) \in \mathrm{Aut}(\mathcal{C}(V,q))$. Dies liefert einen Gruppenhomomorphismus*

$$c : O(V,q) \to \mathrm{Aut}(\mathcal{C}(V,q)),\ \sigma \mapsto c(\sigma).$$

Beispiel. Sei $\gamma := c(-\mathrm{id})$. Dann ist $\gamma_{|\mathcal{C}_0} = \mathrm{id}$, $\gamma_{|\mathcal{C}_1} = -\mathrm{id}$.

Die Gruppe

$$\Gamma_0 := \Gamma_0(V,q) := \{s \in \mathcal{C}_0(V,q) \mid s \text{ invertierbar }, sVs^{-1} = V\} \leq \mathcal{C}_0(V,q)^*$$

ist offensichtlich eine Untergruppe der Einheitengruppe der Clifford Algebra.

Lemma 12.11 *Sei* $\alpha : \Gamma_0 \to \mathrm{Aut}(V), s \mapsto (v \mapsto svs^{-1})$. *Dann ist* $\ker(\alpha) = K^*$.

Beweis. Da V die Clifford Algebra erzeugt, folgt aus $svs^{-1} = v$ für alle $v \in V$, dass $s \in Z(\mathcal{C}(V,q)) \cap \mathcal{C}_0(V,q)^* = K^*$. □

Definition 12.12 *Wegen der universellen Eigenschaft von* $\mathcal{C}(V,q)$ *gibt es genau einen Antiautomorphismus* † *von* $\mathcal{C}(V,q)$, *der die Identität auf* V *induziert und die Graduierung respektiert. Es gilt für* $v_1, \ldots, v_t \in V$ *dass* $(v_1 \cdots v_t)^\dagger = v_t \cdots v_1$ *ist. Definiert man*

$$N : \mathcal{C}(V,q) \to \mathcal{C}_0(V,q), x \mapsto x^\dagger x$$

so gilt $N(v) = q(v)$ *für* $v \in V$.

Lemma 12.13 *Ist* $s \in \Gamma_0$, *so ist* $N(s) \in K^*$. *Die Norm definierte einen Gruppenhomomorphismus* $N : \Gamma_0 \to K^*$.

Beweis. $sV = Vs$ liefert $s^\dagger V = Vs^\dagger$ und somit auch $s^\dagger \in \Gamma_0$. Nach Lemma 12.11 genügt es zu zeigen, dass $\alpha(ss^\dagger) = \mathrm{id}$. Für $x \in V$ ist

$$s^\dagger x s^{-\dagger} = (s^\dagger x s^{-\dagger})^\dagger = s^{-1} x s.$$

□

Definition 12.14 $\mathrm{Spin}(V,q) := \{s \in \Gamma_0 \mid N(s) = 1\}$ *heißt die* Spingruppe *von* (V,q).

Satz 12.15 *Das Bild von* α *ist genau die spezielle orthogonale Gruppe von* V,

$$SO(V,q) := \{\varphi \in \mathrm{GL}(V) \mid q(\varphi(v)) = q(v) \text{ für alle } v \in V \text{ und } \det(\varphi) = 1\}$$

Beweis. Für $s \in \Gamma_0$ und $x \in V$ ist

$$q(s^{-1}xs) = (s^{-1}xs)(s^{-1}xs)^\dagger = s^{-1}xss^\dagger xs^{-\dagger} = N(s)N(s)^{-1}q(x) = q(x).$$

Also ist $\alpha(\Gamma_0) \subset O(V,q)$.
Die Gruppe $SO(V,q)$ ist ein Normalteiler von $O(V,q)$ vom Index 2. Da $O(V,q)$ von Spieglungen erzeugt wird und Spiegelungen Determinante -1 haben, wird $SO(V,q)$ von Produkten einer geraden Anzahl von Spiegelungen erzeugt.
Ist $v \in V$ mit $q(v) \neq 0$, so gilt für $x \in V$:

$$vxv^{-1} = (b_q(v,x) - xv)v^{-1} = -x + \frac{b_q(v,x)}{q(v)}v = -\sigma_v(x).$$

Insbesondere ist $\alpha(vw) = \sigma_v\sigma_w$ und somit α surjektiv. □

Definition 12.16 *Die Spinornorm* $\mathrm{SN} : SO(V,q) \to K^*/(K^*)^2$ *ist definiert durch*

$$\mathrm{SN}(\alpha(s)) = N(s)(K^*)^2$$

für alle $s \in \Gamma_0$. $O'(V,q)$ *bezeichne den Kern der Spinornorm, also* $O'(V,q) = \alpha(\mathrm{Spin}(V,q))$

$$\{\pm 1\} \to \mathrm{Spin}(V,q) \xrightarrow{\alpha} O'(V,q) \to 1.$$

Es gilt

$$\mathrm{SN}(\sigma_{f_1} \dots \sigma_{f_{2m}}) = q(f_1) \dots q(f_{2m})(K^*)^2.$$

Beispiel 12.17 *Die hyperbolische Ebene,* $\mathbb{H} = \langle e, f\rangle$ $q(e) = q(f) = 0$, $q(e+f) = b_q(e+f) = 1$. *Dann ist* $\{x \in \mathbb{H} \mid q(x) = 0\} = \{ae, af \mid a \in K\}$ *und die möglichen orthogonalen Transformationen von* $\mathbb{H}$ *sind*

$$t_a : e \mapsto ae, f \mapsto a^{-1}f,\ s_a = \sigma_{e-af} : e \mapsto af, f \mapsto a^{-1}e.$$

Somit ist $SO(\mathbb{H}) = \{t_a \mid a \in K^*\} \cong K^*$ *und* $t_a = \sigma_{e-f}\sigma_{e-af}$. *Also ist* $\mathrm{SN}(t_a) = q(e-f)q(e-af) = (-1)(-a) = a$.
Es ist $O'(\mathbb{H}) = \{t_a \mid a \in (K^*)^2\} = \{\sigma_v\sigma_w \mid q(v) = q(w)\}$.

Satz 12.18 *Ist* $\mathrm{ind}(V,q) > 0$, *so gilt*

$$\mathrm{Spin}(V) = \langle ef \mid e, f \in V, q(e)q(f) = 1\rangle =: U.$$

Beweis. $U \subset \mathrm{Spin}(V)$ ist klar. Weiter ist $U \trianglelefteq \mathrm{Spin}(V)$ ein Normalteiler, da für $s \in \Gamma_0$

$$sefs^{-1} = (ses^{-1})(sfs^{-1}) = e'f'$$

mit $e' = \alpha(s)(e) \in V$, $f' = \alpha(s)(f) \in V$, $q(e') = q(e)$, $q(f') = q(f)$.
Nach Voraussetzung spaltet V eine hyperbolische Ebene ab, $V = W \perp \mathbb{H}$. Ist $s = f_1 \cdots f_{2m} \in \mathrm{Spin}(V)$, so gibt es $h_i \in \mathbb{H}$ mit $q(h_i) = q(f_i)$. Dann ist $sU = h_1 \cdots h_{2m}U$ und die Behauptung folgt aus Beispiel 12.17. □

13 Spinorgeschlechter.

13.1 Der starke Approximationssatz.

Erinnerung: Zwei $\mathbb{Z}$-Gitter $L \subset (V,q)$ und $M \subset (W,q')$ gehören zur **gleichen Klasse**, wenn es eine Isometrie $\varphi : V \to W$ gibt, mit $\varphi(L) = M$.
Sie gehören zum **gleichen Geschlecht**, wenn es für jedes $p \in \mathbb{P} \cup \{\infty\}$ eine Isometrie $\varphi_p : \mathbb{Q}_p \otimes V \to \mathbb{Q}_p \otimes W$ gibt, mit $\varphi_p(\mathbb{Z}_p \otimes L) = \mathbb{Z}_p \otimes M$.

Definition 13.1 *L und M gehören zum* gleichen Spinorgeschlecht*, wenn es eine Isometrie $\varphi : V \to W$ und Automorphismen $\varphi_p \in O'(V \otimes \mathbb{Q}_p)$ gibt mit*

$$\mathbb{Z}_p \otimes M = \varphi(\varphi_p(L \otimes \mathbb{Z}_p)) \text{ für alle } p \in \mathbb{P} \cup \{\infty\}.$$

Ohne Beweis zitiere ich den starken Approximationssatz für Spingruppen (den man z.B. in Kneser's Buch Abschnitt 23 und 24 findet). Dazu sei (V, q) ein regulärer $\mathbb{Q}$-Vektorraum,

$$O'(V, q) := \{\varphi \in O(V, q) \mid \det(\varphi) = 1,\ \mathrm{SN}(\varphi) = 1\}$$

der Kern von Determinante und Spinornorm. Für eine endliche Menge T von Primzahlen und ein Gitter L in V sei

$$\begin{aligned} O(L, T) &:= \{\varphi \in O(V) \mid \varphi(L) \otimes \mathbb{Z}_p = L \otimes \mathbb{Z}_p \text{ für alle } p \notin T\} \\ O'(L, T) &:= O(L, T) \cap O'(V, q) \\ \mathrm{Spin}(L, T) &:= \{u \in \mathrm{Spin}(V, q) \mid u \in \mathcal{C}_0(L \otimes \mathbb{Z}_p) \text{ für alle } p \notin T\} \end{aligned}$$

$O(L, T)$ sind also die orthogonalen Abbildungen von V, deren Matrix bezüglich einer Gitterbasis von L Nenner hat deren sämtliche Primteiler in T liegen.

Satz 13.2 *(Starker Approximationssatz für Spingruppen) Sei (V, q) ein regulärer $\mathbb{Q}$-Vektorraum, $n := \dim(V) \geq 3$, $\infty \in T \subset \mathbb{P} \cup \{\infty\}$ endlich, $\ell \in T$ mit $\mathrm{ind}(V \otimes \mathbb{Q}_\ell) > 0$. Dann sind für jedes $\mathbb{Z}$-Gitter L in V die Einbettungen*

$$\mathrm{Spin}(L, T) \hookrightarrow \prod_{p \in T - \{\ell\}} \mathrm{Spin}(V \otimes \mathbb{Q}_p),\ O'(L, T) \hookrightarrow \prod_{p \in T - \{\ell\}} O'(V \otimes \mathbb{Q}_p)$$

dicht. Dabei ist $\ell = \infty$ zugelassen.

Satz 13.3 *Sei (V, q) ein regulärer quadratischer $\mathbb{Q}$-Vektorraum mit $\dim(V) \geq 3$, $\mathrm{ind}(V \otimes \mathbb{R}) > 0$. Dann enthält jedes Spinorgeschlecht von Gittern in V genau eine Klasse.*

Beweis. Seien L und M Gitter in V, die zum gleichen Spinorgeschlecht gehören und $\varphi \in O(V, q)$, $\varphi_p \in O'(V \otimes \mathbb{Q}_p)$ mit

$$\varphi^{-1}(M) \otimes \mathbb{Z}_p = \varphi_p(L \otimes \mathbb{Z}_p) \text{ für alle } p \in \mathbb{P} \cup \{\infty\}.$$

Dann gibt es eine endliche Menge $T \subset \mathbb{P}$ mit $\varphi^{-1}(M) \otimes \mathbb{Z}_p = L \otimes \mathbb{Z}_p$ für alle $p \in \mathbb{P} - T$. Da V indefinit ist, kann man den starken Approximationssatz auf $T \cup \{\infty\}$ mit $\ell = \infty$ anwenden und erhält so ein $\psi \in O'(L, T)$ mit

$$\psi(L \otimes \mathbb{Z}_p) = \varphi_p(L \otimes \mathbb{Z}_p) = \varphi^{-1}(M) \otimes \mathbb{Z}_p \text{ für alle } p \in T.$$

Da die Nenner von ψ sämtliche Primteiler in T haben gilt weiterhin

$$\psi(L \otimes \mathbb{Z}_p) = L \otimes \mathbb{Z}_p = \varphi^{-1}(M) \otimes \mathbb{Z}_p \text{ für alle } p \notin T.$$

Also ist $\varphi(\psi(L)) \otimes \mathbb{Z}_p = M \otimes \mathbb{Z}_p$ für alle p und damit $M = \varphi(\psi(L))$ und $u := \varphi \circ \psi \in O(V)$ eine Isometrie zwischen L und M. □

Mit ganz analogem Beweis erhält man

Satz 13.4 *Sei (V, q) ein regulärer quadratischer $\mathbb{Q}$-Vektorraum mit $\dim(V) \geq 3$, $\ell \in \mathbb{P}$ mit $\mathrm{ind}(V \otimes \mathbb{Q}_\ell) > 0$. Dann enthält jede Klasse im Spinorgeschlecht eines Gitters $L \subset V$ ein Gitter $M \subset V$ mit $M \otimes \mathbb{Z}_p = L \otimes \mathbb{Z}_p$ für alle $p \in \mathbb{P}$, $p \neq \ell$.*

Sehr oft stimmen Spinorgeschlechter und Geschlechter überein, es gilt z.B.

Satz 13.5 *(ohne Beweis, s. Kneser (25.4))*
Sei L ein ganzzahliges Gitter in einem regulären $\mathbb{Q}$-Vektorraum, so dass für jede Primzahl p das Gitter $L \otimes \mathbb{Z}_p$ eine mindestens 2-dimensionale Jordankomponente hat. Dann besteht das Geschlecht von L aus genau einem Spinorgeschlecht.

13.2 Der Knesersche Nachbarschaftsalgorithmus.

Basierend auf dem Approximationssatz liefert uns Satz 13.4 ein Verfahren um eine Vertretersystem der Isometrieklassen von Gittern im Spinorgeschlecht von L zu bestimmen. Dabei ist die Einschränkung $\dim(V) = n \geq 3$ nicht wirklich gravierend, da für $\dim(V) = 2$, ein Vertretersystem der Klassen von Gittern gegebener Determinante leicht mit Hilfe der Reduktionstheorie (siehe Abschnitt 11.1) bestimmen kann. Ist dann L ein ganzes Gitter in V und $2 \neq p \in \mathbb{P}$ eine Primzahl, die nicht die Determinante von L teilt, so ist $L \otimes \mathbb{F}_p$ regulär und isotrop also auch $L \otimes \mathbb{Z}_p$ und somit $\mathrm{ind}(V \otimes \mathbb{Q}_p) > 0$. Nach Satz 13.4 enthält jede Klasse im Spinorgeschlecht von L ein Gitter M mit

$$[L : L \cap M] = [M : L \cap M] = p^d$$

für ein $d \in \mathbb{N}_0$.

Definition 13.6 *(a) Sei*

$$\mathcal{G}_p(L) := \{M \leq V \mid M \text{ ist im Spinorgeschlecht von } L, [L : L \cap M] = [M : L \cap M] = p^d \text{ für ein } d \in \mathbb{N}_0\}$$

Dann ist für $M, M' \in \mathcal{G}_p(L)$ der Index $[M : M \cap M'] = [M' : M \cap M']$ eine Potenz von p und wir definieren den Abstand $d(M, M') := \log_p([M : M \cap M'])$.
(b) Sei $\Gamma_p(L)$ der Graph mit Eckenmenge $\mathcal{G}_p(L)$ und Kanten (M, M') für $d(M, M') = 1$.
(c) Zwei Gitter $M, M' \in \mathcal{G}_p(L)$ heißen benachbart*, falls $d(M, M') = 1$ ist.*

Satz 13.7 *$\Gamma_p(L)$ ist zusammenhängend. Genauer ist für $M, M' \in \mathcal{G}_p(L)$ der Abstand $d(M, M')$ genau die Länge eines kürzesten Weges in $\Gamma_p(L)$ von M nach M'.*

Zum Beweis benötigen wir ein Lemma.

Lemma 13.8 *Sei $L \leq V$ ein ganzes Gitter und $p \in \mathbb{P}$ kein Teiler der Determinante von L. Ist $y \in L - pL$ mit $b(y, y) \in p^2\mathbb{Z}$, so ist*

$$L(y) := \langle L_y, \frac{1}{p} y \rangle \text{ mit } L_y := \{x \in L \mid b(x, y) \in p\mathbb{Z}\}$$

in $\mathcal{G}_p(L)$ ein Nachbar von L und jeder Nachbar von L in $\mathcal{G}_p(L)$ ist von dieser Form.
Ist $p = 2$ und L ein gerades Gitter, so muss man zusätzlich fordern, dass $b(y, y) \in 8\mathbb{Z}$ ist.
Ist $p = 2$ und L ein ungerades Gitter, so muss man nur die $L(y)$ betrachten, die auch wieder ungerade sind.

Beweis. (der Einfachheit halber für $p \neq 2$). $L(y)$ ist ein ganzes Gitter mit $L \cap L(y) = L_y$ und $[L : L_y] = p = [L(y) : L_y]$. Klar ist $L(y) \otimes \mathbb{Z}_r = L \otimes \mathbb{Z}_r$ für $r \neq p$. $L(y) \otimes \mathbb{Z}_p$ ist ein reguläres $\mathbb{Z}_p$-Gitter gleicher Determinante wie $L \otimes \mathbb{Z}_p$, also ist $L(y)$ im Geschlecht von L.
Sei umgekehrt $M \in \mathcal{G}_p(L)$ mit $[L : M \cap L] = [M : M \cap L] = p$. Wähle ein beliebiges $y \in pM - pL$. Dann ist

$$L_y = \{\ell \in L \mid b(\ell, y) \in p\mathbb{Z}\} \subset L$$

ein echtes Teilgitter von L und $M \cap L \subset L_y$. Somit $M \cap L = L_y$. Weiter ist $\frac{y}{p} \in M - L \cap M$, also $M = \langle L_y, \frac{y}{p} \rangle = L(y)$. □

Beweis. (von Satz 13.7) Analog zu Satz 9.10 konstruieren wir für $M, M' \in \mathcal{G}_p(L)$ mit Abstand $d = d(M, M')$ eine Folge $(M = M_0, M_1, \ldots, M_d = M')$ von Gittern $M_i \in \mathcal{G}_p(L)$ mit $d(M_{i-1}, M_i) = 1$ für $i = 1, \ldots, d$. Daraus ergibt sich der Zusammenhang von $\Gamma_p(L)$ und dass die Länge eines kürzesten Weges in $\Gamma_p(L)$ von M nach M' kleiner oder gleich $d(M, M')$ ist. Die Gleichheit ist dann recht einfach zu sehen (Übung).
Der Beweis ist eine Induktion über den Abstand $d := d(M, M')$.
Ist $d = 1$, so ist nichts zu zeigen.
Für $d > 1$ wähle ein Element $\tilde{y} + (M \cap M')$ der Ordnung p in $M'/(M \cap M')$ mit zugehörigem Vertreter $\tilde{y} \in M'$. Setze $y := p\tilde{y} \in pM'$. Dann ist $y \in M$ da $\tilde{y} + (M \cap M')$ Ordnung p hat und $y \notin pM$. Weiter ist $b(y, y) = p^2 b(\tilde{y}, \tilde{y})$ durch p^2 teilbar (im Fall $p = 2$ und M, M' gerade sogar durch 8) und wir können den Nachbarn $N := M(y)$ bilden. Dieser hat einen echt kleineren Abstand zu M', denn ist $x \in M \cap M'$, dann ist $b(\tilde{y}, x) \in \mathbb{Z}$ und daher $x \in M_y$. Also $M \cap M' \subset N \cap M'$. Es ist jedoch $\tilde{y} \in N \cap M' - M \cap M'$, so dass der Abstand echt kleiner wird. □

Bemerkung 13.9 *(a) $L(y) = L(y')$ falls $y' = y + pz$ mit $z \in L_y$.*
(b) Jede Isometrie $u \in O(L)$ induziert eine Isometrie zwischen den Nachbarn $L(y)$ und $L(uy)$.
(c) Sei $p \neq 2$ kein Teiler der Determinante von L. Jede Klasse $x+pL$ mit $b(x, x) \in p\mathbb{Z}$ enthält einen Vektor $y = x + pz$ mit $b(y, y) \in p^2\mathbb{Z}$. Für dieses y gilt: Ist $z \in L$ und $y' = y + pz$ so dass $b(y', y') \in p^2\mathbb{Z}$, so ist $z \in L_y$.
(d) Ist $p = 2$ und L gerade, so muss $b(y, y) \in 4\mathbb{Z}$ liegen, damit man y so abändern kann, dass $b(y + 2z, y + 2z)$ durch 8 teilbar wird für ein $z \in L$ und so dann $L(y + 2z)$ wieder ein gerades Gitter wird.
(e) Die Nachbarn $L(y)$ von L stehen also in Bijektion zu den isotropen Klassen $y + pL$ von L/pL wobei man für $p = 2$ und L gerade den Raum $L/2L$ als quadratischen $\mathbb{F}_2$-Vektorraum betrachten muss.

Beweis. Von (c): Es ist $b(x + pz, x + pz) = b(x, x) + 2pb(x, z) + p^2 b(z, z)$. Da $x \notin pL$ ist, gibt es also ein $z \in L$ mit $b(x, z) \notin p\mathbb{Z}$. Durch Addition eines geeigneten Vielfachen von z erreicht man, dass $b(x + pz, x + pz) \in p^2\mathbb{Z}$. Ist $b(x, x) \in p^2\mathbb{Z}$ so ist $b(x + pz, x + pz) \in p^2\mathbb{Z}$ genau dann wenn $p \mid b(x, z)$ also genau dann wenn $z \in L_x$ ist. □

Satz 13.10 *Die ganzzahligen 2-Nachbarn von I_n sind bis auf Isometrie genau die Gitter $D_m^+ \perp I_{n-m}$ mit $m \in 4\mathbb{Z}$, $4 < m \leq n$.*

Beweis. Sei $L = I_n(y)$ ein 2-Nachbar von I_n mit $y = \sum_{i=1}^n y_i e_i$, $y_i \in \mathbb{Z}$ nicht alle durch 2 teilbar. Ist $y_i \in 2\mathbb{Z}$, so ersetzt man y durch $y' := y - y_i e_i$ und erhält $I_n(y) = I_n(y')$. Ist $y_i = 4z_i \pm 1$ ungerade, so kann man durch Subtraktion von $4z_i e_i$ erreichen, dass $y_i \in \pm 1$ ist. Nun ist $O(I_n) \cong C_2 \wr S_n$, so dass wir $y_i = 1$ für $i = 1, \ldots, m$ und $y_i = 0$ für $i = m+1, \ldots, n$ erreichen können. Dann ist $y =: y(m) = \sum_{i=1}^m e_i$ und $b(y,y) = m$. Also muss m durch 4 teilbar sein. Es ist $L_y = D_m \perp I_{n-m}$ und damit $L(y) = D_m^+ \perp I_{n-m}$ mit $D_4^+ \cong I_4$ und $D_8^+ \cong E_8$. □

Satz 13.11 *Die 2-Nachbarn von E_8 sind I_8 und E_8.*

Beweis. Sei $L := E_8$. Dann ist L ein gerades unimodulares Gitter und also $L/2L$ ein regulärer quadratischer Raum mit Witt Index 4 (2-adische Determinanten vergleichen). Insbesondere ist die orthogonale Gruppe $O(L/2L)$ von Spiegelungen entlang anisotroper Vektoren erzeugt. Die Anzahl solcher anisotroper Vektoren ist $b_4 = 2^8 - 1 - a_4$, wobei a_4 die Anzahl isotroper Vektoren bezeichnet, die wir im Beweis von Satz 9.1 ausgerechnet haben, also

$$a_4 = (2^4 - 1)(2^3 + 1) = 2^7 + 2^4 - 2^3 - 1.$$

Also ist $b_4 = 2^8 - 2^7 - 2^4 + 2^3 = 120$. Das Gitter E_8 hat genau 240 Wurzeln. Sind $v, w \in E_8$ Wurzeln mit $v + 2E_8 = w + 2E_8$, so ist $v \pm w = 2z \in 2E_8$. Nehmen wir an, dass $(v,w) \geq 0$ ist, dann ist $(v-w, v-w) \geq 2 + 2 = 4$ also $z := (v-w)/2$ ein Vektor der Norm ≤ 1 in E_8, also $z = 0$ und somit $v = w$. Die Wurzeln in $v + 2E_8$ sind also nur v und $-v$ und somit sind die 120 verschiedenen Klassen $\{v + 2E_8 \mid v \in E_8, (v,v) = 2\}$ genau die 120 anisotropen Vektoren von $E_8/2E_8$. Die Spiegelungen entlang dieser Vektoren erzeugen aber $W(E_8)$ und auch $O(E_8/2E_8)$. Also ist die Reduktion modulo 2 von $W(E_8)$ auf $O(E_8/2E_8)$ surjektiv und $W(E_8)$ transitiv auf den isotropen Vektoren in $E_8/2E_8$. $E_8 = D_8^+$ hat also nur eine Isometrieklasse von geraden Nachbarn, und dieser ist wieder isometrisch zu $E_8 = D_8^-$. □

Folgerung 13.12 *Für $n \leq 8$ ist I_n bis auf Isometrie das einzige ungerade positiv definite unimodulare Gitter.*
Es gibt genau ein gerades unimodulares Gitter der Dimension 8, nämlich das Wurzelgitter E_8.

Satz 13.13 *Für $n = 9, 10, 11$ sind $E_8 \perp I_{n-8}$ und I_n die einzigen unimodularen Gitter.*

Beweis. Als Übung. Die Nachbarn von I_n haben wir schon alle bestimmt, es genügt also die Nachbarn von $E_8 \perp I_{n-8}$ zu berechnen. □

Satz 13.14 *(Gitter mit Determinante 3). Die Geschlechter von A_2, E_6 und $E_8 \perp A_2$ bestehen aus jeweils einer Klasse.*

Beweis. Für A_2 folgt aus der Schranke in Lemma 11.5, dass A_2 das einzige gerade Gitter der Dimension 2 und Determinante 3 ist. Für E_6 und $E_8 \perp A_2$ könnte man leicht die Nachbarn ausrechnen um die Einklassigkeit zu erhalten. Jedoch können wir auch die obigen Ergebnisse über unimodulare Gitter benutzen.
Ist M ein Gitter im Geschlecht von E_6, so ist $M \perp A_2$ ein Teilgitter eines geraden unimodularen Gitters, also $M \perp A_2 \leq E_8$ und damit $M = A^\perp$ für ein zu A_2 isometrisches Teilgitter von E_8. Nun ist $W(E_8)$ transitiv auf den zu A_2 isometrischen Teilgittern von E_8 und daher $M \cong E_6$.
Für Dimension 10 benutzen wir die Klassifikation der 11-dimensionalen unimodularen Gitter, indem wir beobachten, dass $E_8 \perp A_2 \perp (3) \leq E_8 \perp I_3$ ein Teilgitter von Index 3 ist. Also ist auch für jedes Gitter L im Geschlecht von $E_8 \perp A_2$ die orthogonale Summe $L \perp (3)$ ein Teilgitter von $E_8 \perp I_3$ oder von I_{11}. Weiter ist L ein gerades Gitter und das orthogonale Komplement eines Vektors der Länge 3 in einem der beiden Gitter $E_8 \perp I_3$ oder I_{11}. In I_{11} haben Vektoren der Länge 3 keine geraden orthogonalen Komplemente. Die Vektoren $v + w \in E_8 \perp I_3$ mit Länge 3 sind entweder $0 + w$ mit $w \in I_3$ der Länge 3 oder $(v, v) = 2$ und $(w, w) = 1$. In letzterem Fall enthält $\langle v + w \rangle^\perp$ noch Vektoren der Länge 1. Im ersten Fall ist $E_8 \leq \langle w \rangle^\perp$ und damit $L = E_8 \perp A$ mit einem geraden Gitter A der Dimension 2 und Determinante 3, also $A = A_2$. □

13.3 Gerade und ungerade Gitter.

Dies ist ein schöner und sehr nützlicher Trick, welcher z.B. von Richard Borcherds benutzt wurde, um die ungeraden unimodularen Gitter der Dimension 24 zu klassifizieren.

Sei L ein ungerades positiv definites unimodulares Gitter. Dann bestimmt L sein gerades Teilgitter

$$L_0 := \{\ell \in L \mid (\ell, \ell) \in 2\mathbb{Z}\}$$

welches von Index 2 in L ist. Die Diskriminantengruppe $L_0^\#/L_0$ hat also Ordnung 4.

Lemma 13.15 *Sei L ein ungerades positiv definites unimodulares Gitter der Dimension n. Dann gilt für sein gerades Teilgitter L_0*

$$L_0^\#/L_0 \cong D_n^\#/D_n \cong \begin{cases} C_2 \times C_2 & n \text{ gerade} \\ C_4 & n \text{ ungerade} \end{cases}$$

Ist n gerade, so liegen zwischen $L_0^\#$ und L_0 also 3 Gitter, L, M_1, M_2. Diese sind alle ganz und damit unimodular, wenn n durch 4 teilbar ist, ansonsten ist $M_1^\# = M_2$. Ist n sogar durch 8 teilbar, so sind M_1 und M_2 gerade unimodulare Gitter.

Beweis. Die Eigenschaften im Lemma sind alles lokale Eigenschaften. Sie gelten für alle Gitter im Geschlecht von L, wenn sie für ein Gitter im Geschlecht von L gelten. Also genügt es, diese für $L = I_n$ zu überprüfen. Das gerade Teilgitter von I_n ist D_n und die Gitter M_1, M_2 sind gerade die Gitter D_n^+ und D_n^- für gerade n. □

Lemma 13.16 *Sei $n \in 8\mathbb{Z}$ und $\Gamma_2(n)$ der 2-Nachbarschaftsgraph der geraden unimodularen positiv definiten Gitter der Dimension n. Sind M_1, M_2 Nachbarn in $\Gamma_2(n)$, $X := M_1 \cap M_2$, so ist X ein gerades Gitter mit $X^\# / X \cong C_2 \times C_2$. Die Gitter zwischen $X^\#$ und X sind genau M_1, M_2 und ein drittes Gitter L. Dieses ist unimodular und ungerade.*

Beweis. Es ist nur zu zeigen, dass L ungerade ist ($L = L^\#$, da auch $L^\#$ ein Gitter zwischen $X^\#$ und X ist und weder gleich M_1 noch gleich M_2). Es ist aber $X^\# = L \cup M_1 \cup M_2$. Wäre L ein gerades Gitter, so bestünde $X^\#$ aus Vektoren gerader Norm. Damit wäre aber dann auch $X^\#$ ein ganzes Gitter, ein Widerspruch, da die Determinante von $X^\#$ gleich $1/4$ ist und also nicht ganz. □

Satz 13.17 *Die ungeraden positiv definiten unimodularen Gitter der Dimension $8m$ stehen in Bijektion zu den Kanten in $\Gamma_2(8m)$.*

Beispiel. Dimension 8: E_8 und I_8.
Dimension 16: 2 gerade unimodulare Gitter: $E_8 \perp E_8$ und D_{16}^+. Die Kante $(E_8 \perp E_8, E_8 \perp E_8)$ liefert das ungerade Gitter $I_8 \perp E_8$.
Eine weitere Kante $(E_8 \perp E_8, E_8 \perp E_8)$ liefert $I_2 \perp L_{14}$ für das unzerlegbare unimodulare Gitter L_{14} der Dimension 14.
$(E_8 \perp E_8, D_{16}^+)$ liefert liefert das unzerlegbare ungerade unimodulare Gitter L_{16}.
(D_{16}^+, D_{16}^-) liefert das ungerade Gitter I_{16}.
Zwei weitere Kanten (D_{16}^+, D_{16}^-) liefern $I_4 \perp D_{12}^+$ und $I_1 \perp L_{15}$.
In Dimension 24 gibt es 24 gerade unimodulare Gitter und 273 ungerade unimodulare Gitter. Die ungeraden unimodularen Gitter sind vollständig klassifiziert bis in Dimension 25. In Dimension 26,27,28 kennt man alle ungeraden unimodularen Gitter mit Minimum ≥ 3.