2) Form Ringe und deren Darstellungen

(2.1) Bem+Def: Sei R ein Ring, V ein R-Linksmodul, A abelsche Gruppe.

(a) $Bil(V,A) := \{ \beta : V \times V \to A \mid \beta$ ist $\mathbb{Z}$-bilinear$\}$
ist ein $R \otimes_{\mathbb{Z}} R$ Rechtsmodul durch

$$\beta \cdot (r \otimes s) =: (v,w) := \beta(rv, sw) \quad \forall r,s \in R,\ v,w \in V,\ \beta \in Bil(V,A)$$

$\tau : Bil(V,A) \to Bil(V,A)$

$\beta^{\tau}(v,w) := \beta(w,v) \quad \forall \beta \in Bil(V,A),\ v,w \in V$
ist Involution auf der abelschen Gruppe $Bil(V,A)$

(b) $Quad_0(V,A) := \{ \phi : V \to A \mid$
$\phi(v+w+u) + \phi(v) + \phi(u) + \phi(w) = \phi(v+w) + \phi(v+u) + \phi(u+w) \}$

$= \{ \phi : V \to A \mid \lambda(\phi) \in Bil(V,A) \}$ wo

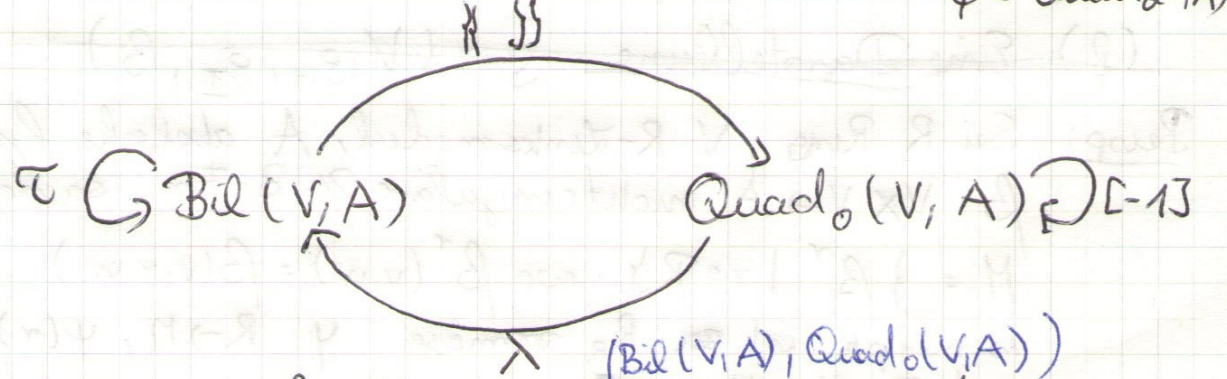
$\lambda(\phi)(v,w) := \phi(v+w) - \phi(v) - \phi(w)$ heißt die Gruppe des quadratischen Abb. von V nach A.

(c) $\exists$ Abb. $Quad_0(V,A) \times R \to Quad_0(V,A)$

$(\phi, r) \mapsto \phi[r]$ wo $\phi[r](v) := \phi(rv)$

für die gilt: $\phi[rs] = (\phi[r])[s] \quad \forall r,s \in R,\ \phi \in Quad_0(V,A)$

(d)



$\{\!\{\beta\}\!\}(v) := \beta(v,v)$ ist ein quadratisches Paar mit der Abb $\{\!\{\beta\}\!\}$ und λ
über R, d.h. es gilt

$$\text{(*)}\quad \begin{cases} \{\!\{\tau(m)\}\!\} = \{\!\{m\}\!\} & \forall\, m \in Bil(V,A) \\ \tau(\lambda(\phi)) = \lambda(\Phi(\phi)) & \forall\, \phi \in Quad_0(V,A) \\ \lambda(\{\!\{m\}\!\}) = m + \tau(m) & \forall\, m \in Bil(V,A) \\ \phi[r,s] := \phi[r+s] - \phi[r] - \phi[s] = \{\!\{\lambda(\phi)(r \otimes s)\}\!\} \end{cases}$$

Beisp: $A = V = \mathbb{R}$, $x \mapsto x^2 \in Quad_0(\mathbb{R},\mathbb{R})$, $\phi: V \to A$ Hom. abelsche Gruppen $\Rightarrow \phi \in Quad_0(V,A)$, $\lambda(\phi) = 0$

(2.2) Def (Form Ring)

Ein Quadrupel (R, M, ψ, Φ) heißt Form Ring falls

(a) R ist Ring

(b) M ist ein $(R \otimes R)$-Rechtsmodul mit einem Autom. $\tau: M \to M$, so daß $\tau(m \cdot (r \otimes s)) = \tau(m)(s \otimes r)$ $\forall$ $\tau^2 = 1$

(c) $\psi: R_R \to M_{1 \otimes R}$ ist ein Isomorphismus von R-Rechtsmoduln so daß $\varepsilon := \psi^{-1}(\tau(\psi(1))) \in R^*$

(d) Φ ist ein R-qModul, d.h. Φ ist abelsche Gruppe aus mit Abb. $[\,]: R \to End(\Phi)$ so daß

(i) $[1] = 1$

(ii) $[r] \cdot [s] = [rs]$

(iii) $[r+s+t] + [r] + [s] + [t] = [r+s] + [r+t] + [s+t]$

(e) $\exists$ Abb. $\lambda: \Phi \to M$, $\{\!\{\,\}\!\}: M \to \Phi$ die die 4 Bed. in (*) erfüllen (für M anstatt $Bil(V,A)$ und Φ " $Quad_0(V,A)$)

~~(f) Eine Darstellung $S = (V, S_M, S_\Phi, \beta)$~~

Beisp: Sei R Ring, V R-Linksmodul, A abelsche Gruppe $\beta: V \times V \to A$ nichtsinguläre $\mathbb{Z}$-BiFo so daß $M := \{\beta^r \mid r \in R\}$ wo $\beta^r(v,w) := \beta(v, rw)$ isomorph ist R_R vermöge $\psi: R \to M$, $\psi(r) := \beta^r$ und $\tau: M \to M$ * β.

Sei $\Phi := \{\!\{M\}\!\} \subseteq Quad_0(V,A) \Rightarrow$ (R, M, ψ, Φ) ist ein Form Ring.

Datum: Betr.:
Bearbeiter:
Blatt: Projekt Nr.: Auftr.Nr.:

(2.3) Def Sei $R=(R, M, \varphi, \Phi)$ ein Form Ring.

(a) Eine Darstellung von R ist ein Quadrupel

$\varrho = (V, \varrho_M, \varrho_\Phi, \beta)$ wo

(a) V ist ein R-Linksmodul

(b) $\varrho_M : M \to Bil(V, A)$ ein $R \otimes R$-Modul hom, verträglich mit τ

(c) $\varrho_\Phi : \Phi \to Quad_\circ(V, A)$ ein R-qModulhom.

(d) $\{\!\{\varrho_M(m)\}\!\} = \varrho_\Phi(\{\!\{m\}\!\})$

$\lambda(\varrho_\Phi(\phi)) = \varrho_M(\lambda(\phi))$

(e) $\beta := \varrho_M(\varphi(1))$ ist nichtsingulär.

(2) ϱ heißt endliche Darst, falls $|V|<\infty$, $A = \mathbb{Q}/\mathbb{Z}$.

(2.4) Beisp: $R = \mathbb{F}_2 = M$, $\varphi = id$, $\Phi = \mathbb{Z}/4\mathbb{Z}$ (R-qModul durch $0 \cdot \phi = 0 \; \forall \phi \in \mathbb{Z}/4\mathbb{Z}$, $1 \cdot \phi = \phi$)

$R(\mathbb{Z}_2) :=$

$\Rightarrow (R, M, \varphi, \Phi)$ ist Form Ring durch

$\tau = id$, $\{\!\{m\}\!\} := 2m$, $\lambda(\phi) := \phi \bmod 2$

$\varrho^{(\mathbb{Z}_2)} = (\mathbb{F}_2, \varrho_M, \varrho_\Phi, \beta)$ ist endl. Darst. wo

$\varrho_M(a)(v, w) := \frac{1}{2} v \cdot w \cdot a \qquad \forall a \in \mathbb{F}_2 = M,\ v, w \in \mathbb{F}_2 = V$

$\varrho_\Phi(a)(v) := \frac{1}{4} \cdot a \cdot v^2 \qquad \forall a \in \mathbb{Z}\Phi = \mathbb{Z}/4\mathbb{Z}$, $v \in V = \mathbb{Z}/2\mathbb{Z}$

Ist $N \in \mathbb{N}$ so ist $\varrho^{(\mathbb{Z}_2^N)} = (\mathbb{F}_2^N, \varrho_M, \varrho_\Phi, \beta)$ ebenso endl. Darst. wo

$\varrho_M(a)(v, w) := \frac{1}{2} a \sum_{i=1}^{N} v_i w_i$

$\varrho_\Phi(a)(v) := \frac{1}{4} \cdot a \sum_{i=1}^{N} v_i^2$.

1228-96

(2.5) Def: Sei $\varrho = (V, \varrho_M, \varrho_\Phi, \beta)$ eine Darstellung des Form Rings (R, M, γ, Φ).

(a) $\bar{\varrho} = (V, -\varrho_M, -\varrho_\Phi, -\beta)$ ist auch Darst. von R genannt, die zu ϱ konj. Darst.

(b) $N \in \mathbb{N} \Rightarrow N\cdot\varrho := (V^N, \varrho_M^N, \varrho_\Phi^N, \beta^N)$ heißt die N-fache orthogonale Summe von ϱ.

wo $$\varrho_M^N(m)((v_1,\dots,v_N),(w_1,\dots,w_N)) := \sum_{i=1}^N \varrho_M(m)(v_i,w_i)$$

$$\varrho_\Phi^N(\phi)(v_1,\dots,v_N) = \sum_{i=1}^N \varrho_\Phi(\phi)(v_i).$$

(d) Ein Code vom Typ ϱ der Länge N ist ein selbstduales isotroper R-Teilmodul $C \subseteq V^N$ d.h.

$$C = C^\perp = \{ v \in V^N \mid \beta^N(v,c) = 0 \ \forall c \in C \}$$
(selbstdual)

und $\phi(c) = 0 \quad \forall c \in C, \ \phi \in \Phi \varrho_\Phi^N(\Phi)$
(isotrop)

(c) Sei $C \subseteq V^N$ ein R-Teilmodul.

$C^\perp = C^{\perp,\beta} := \{ v \in V^N \mid \beta^N(v,c) = 0 \ \forall c \in C \}$

C selbstdual in $N\varrho$ $:\Leftrightarrow C = C^\perp$

C selbstorthogonal $:\Leftrightarrow C \subseteq C^\perp$

C isotrop (oder Code in $N\varrho$) $:\Leftrightarrow$ C selbstorthogonal und $\phi(c) = 0 \ \forall \phi \in \varrho_\Phi^N(\Phi), c \in C$.

(2.6) Bem: (Ver. wie bei 2.4) $C \subseteq V^N$ R-Teilmodul, $m \in M$

(a) $\varrho_M^N(m)(c',c'') = 0 \ \forall c'' \in C, c' \in C^\perp$, $\forall m \in M$
($\varrho_M^N(m)(c',c) = (\beta^N)^{\perp}(c',c) = \beta^N(c',rc) = 0$ da $rc \in C$ $(r = \gamma^{-1}(m) \in R)$)

(b) $(C^\perp)^\perp = C$, $C^\perp \subseteq V^N$ ist R-Teilmodul
($v_1, v_2 \in C^\perp \Rightarrow v_1 + v_2 \in C^\perp$ da β $\mathbb{Z}$-Bilinearform.
$v \in C^\perp, r \in R \Rightarrow \beta^N(rv, w) = (\beta^N)^{\perp}(v, rw) = 0$ }
($\beta^N \in \varrho_\Pi(M)$, $rw \in C$)

Datum: Betr.:
Bearbeiter:
Blatt: Projekt Nr.: Auftr.Nr.:

(2.7) Beisp: Sei $R(2_{II}) = (\mathbb{F}_2, \mathbb{F}_2, id, \mathbb{Z}/4\mathbb{Z})$ der Form Ring aus Beisp(2.4)

C Code vom Typ $S(2_{II})$ der Länge N $\Leftrightarrow$

$$C = C^{\perp} = \{ v \in \mathbb{F}_2^N \mid \frac{1}{2} \cdot \sum_{i=1}^{N} v_i c_i \in 2\mathbb{Z} \ \forall c \in C \}$$

und C isotrop, d.h. $\sum_{i=1}^{N} \frac{1}{4} c_i^2 \in 2\mathbb{Z} \quad \forall c \in C$

d.h. C ist selbstdualer doppeltgerader binärer Code.
(s. Ü. A4)

(2.8) Beisp: Typ von $C = C^{\perp} \leq \mathbb{F}_q^N$, $(1,\dots,1) \in C$, $q = p^{\beta}$, $p > 2$

$R(\mathbb{F}_q) = (\mathbb{F}_q, \mathbb{F}_q, id, \mathbb{F}_q \oplus \mathbb{F}_q)$

$q \overset{E}{\to} 1$

$S(q_1^E)$: $V = \mathbb{F}_q$, $\quad s_M(a)(x,y) := \frac{1}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}(axy)$

$$s_{\Phi}(a,b)(x) := \frac{1}{p}\left(Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax + bx^2)\right)$$

Sei die Operationen von R auf M bzw Φ fest, ebenso wie $\{\!\{\}\!\}$ und λ

$$\{\!\{ s_M(a) \}\!\}(x) = \frac{1}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2) \Rightarrow \{\!\{a\}\!\} = (0,a) \ \forall a \in M$$

$$\lambda(s_{\Phi})(a,b)(x,y) = \frac{1}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(x+y) + b(x+y)^2)$$

$$- \frac{1}{p} Tr(ax+bx^2) - \frac{1}{p} Tr(ay+by^2) = 2 \cdot \frac{1}{p} Tr(bxy)$$

$$= 2 \cdot s_M(b) \quad \Rightarrow \quad \lambda((a,b)) = 2b \in M \ \forall (a,b) \in \Phi$$

$\tau: M \to M$ ist $\tau = id_M$

$r \in \mathbb{F}_q = R$, $(a,b) \in \Phi \Rightarrow (a,b)[r] = (ra, r^2 b)$