4) Schattentheorie → Seminarvortrag / Übung

5) Clifford-Weil Gruppen

$\mathbb{F}_2$ $m \times m$ $\Rightarrow \begin{pmatrix} 1 & \cdots \\ 0 & \\ \vdots & \end{pmatrix}$

Beisp: $R = \mathbb{Z}/6\mathbb{Z}$, $C \leq R^N$ Code

$e := 3 + 6\mathbb{Z}$, $1-e = -2 + 6\mathbb{Z} \Rightarrow e^2 = e$, $(1-e)^2 = (1-e)$

$e \cdot (1-e) = 0 \Rightarrow$ orthogonale Idempotente

$C = \not{C}^{\perp} \leq R^N$ selbstadjungiert bzgl. Standardskalarprod.

$\Rightarrow C = eC \oplus (1-e)C \leq (eR)^N \oplus ((1-e)R)^N$

$C^{\perp} = eC^{\perp} \oplus (1-e)C^{\perp}$ $\quad (\mathbb{Z}/2\mathbb{Z})^N \oplus (\mathbb{Z}/3\mathbb{Z})^N$

$\beta(eR, (1-e)R) = \beta(e(1-e)R, R) = 0$

$\Rightarrow eC^{\perp} = (eC)^{\perp}$, $(1-e)C^{\perp} = ((1-e)C)^{\perp}$

(5.1) Bem V endl. ab. Gruppe, $\beta: V \times V \to \mathbb{Q}/\mathbb{Z}$ nicht singulär

$C \leq V \Rightarrow |C| \cdot |C^{\perp}| = |V|$

denn $C^{\perp} \cong \hat{(V/C)}$ nach (3.3)

(5.2) Def R Ring, $\overline{\ }: R \to R$, $x \mapsto x^{\overline{\ }}$ Involution

$e \in R$, $e^2 = e$ **symmetrisch** $\Leftrightarrow eR \cong e^{\overline{\ }}R$ als R-Rechtsmoduln

(5.3) Bem e symmetrisch $\Leftrightarrow \exists\, u_e \in eRe^{\overline{\ }}$, $v_e \in e^{\overline{\ }}Re$ mit

$u_e v_e = e$, $v_e u_e = e^{\overline{\ }}$

Bew: $\kappa: eR \to e^{\overline{\ }}R$ $\overset{\text{Hom}}{\text{Dsom.}}$ von R-Rechtsmoduln ist eind. best. durch $\kappa(e) =: v_e \in e^{\overline{\ }}R$

v_e erfüllt $v_e \cdot e = \kappa(e) \cdot e = \kappa(e \cdot e) = \kappa(e) = v_e$

also $v_e \in e^{\overline{\ }}Re$; $\kappa(ex) = v_e \cdot x$ $\forall x \in R$

Ist κ Dsmorphismus so erfüllt $u_e := \kappa^{-1}(e^{\overline{\ }})$

entsprechend $u_e \in eRe^{\overline{\ }}$, $\kappa^{-1}(e^{\overline{\ }}x) = u_e x$

$e = \kappa^{-1}(\kappa(e)) = \kappa^{-1}(v_e) = \kappa^{-1}(e^{\overline{\ }}v_e) = u_e \cdot v_e$

$$e = \kappa^{-1}(\kappa(e)) = \kappa^{-1}(v_e) = \kappa^{-1}(e^{\sharp} v_e) = u_e \cdot v_e$$
$$e^{\sharp} = \kappa(\kappa^{-1}(e^{\sharp})) = \kappa(u_e) = \kappa(e u_e) = v_e \cdot u_e$$

(5.4) Lemma: Sei (R, M, Φ, ψ) Formring

insbes. $\psi: R \xrightarrow{\sim} M_{1 \otimes R}$, $M \circlearrowright \tau$, $\tau(m \cdot (r \otimes s)) = \tau(m)(s \otimes r)$

$\varepsilon := \psi^{-1}(\tau(\psi(1)) \in R^*$ ($\tau(\psi(r))$)

(a) $\sharp: R \to R$, $r \mapsto r^{\sharp} = \psi^{-1}(\psi(1)(r \otimes 1))$

erfüllt $1^{\sharp} = 1$, $(rs)^{\sharp} = s^{\sharp} r^{\sharp}$ $\forall r, s \in R$

$\varepsilon^{\sharp} r^{\sharp^2} \cdot \varepsilon = r$ $\forall r \in R$, $\varepsilon^{\sharp} \cdot \varepsilon = 1$

$\varepsilon \in Z(R) \Rightarrow \sharp$ ist Involution

(b) $\mathcal{S} = (V, S_M, S_{\Phi}, \beta)$ endl. Darstellung $e \in R$ sym. Idemp.

$\beta_e: eV \times eV \to \mathbb{Q}/\mathbb{Z}$, $\beta_e(ex, ey) := \beta(ex, v_e y)$

wo v_e wie in (5.3) ist nicht singulär

Beweis: (a)

$$\psi(r) \cdot (s \otimes t) = \psi(1) \cdot (1 \otimes r)(s \otimes t) = \underbrace{\psi(1)(s \otimes 1)}_{\psi(s^{\sharp})}(1 \otimes rt)$$
$$= \psi(s^{\sharp} r t)$$

$$\psi((rs)^{\sharp}) = \psi(1)(r \otimes 1)(s \otimes 1) = \psi(r^{\sharp})(s \otimes 1) = \psi(s^{\sharp} r^{\sharp})$$
$$\Rightarrow (rs)^{\sharp} = s^{\sharp} r^{\sharp}$$

$$\tau(\psi(r)) = \tau(\psi(1)(1 \otimes r)) = \tau(\psi(1))(r \otimes 1) = \psi(\varepsilon)(r \otimes 1)$$
$$= \psi(r^{\sharp} \varepsilon)$$

$$\tau(\tau(\psi(r))) = \psi(r) \Rightarrow$$
$$\psi(r) = \tau(\psi(r^{\sharp} \varepsilon)) = \psi((r^{\sharp} \varepsilon)^{\sharp} \cdot \varepsilon) = \psi(\varepsilon^{\sharp} r^{\sharp^2} \varepsilon)$$

(4) Beweis: $\beta_e(ex, ey) := \beta(ex, v_e y) \quad \forall x, y \in V$

$= \beta(x, e^J v_e y) = \beta(x, v_e y)$.

Sei $ey \in (eV)^{\perp_{\beta_e}} \Rightarrow v_e \cdot y \in V^{\perp_\beta}$ d.h. $v_e y = 0$

$\Rightarrow ey = 0$ da $z \mapsto v_e z$ $\quad eV \to e^J V$ Dsom.

d.h. $ey \mapsto (ex \mapsto \beta(ex, v_e y))$

$eV \hookrightarrow \mathrm{Hom}(eV, \mathbb{Q}/\mathbb{Z})$ injektiv

$|V|$ endlich $\Leftrightarrow$ bijektiv

$\mathrm{ord}|eV| = |\mathrm{Hom}(eV, \mathbb{Q}/\mathbb{Z})|$?

(5) Beitrag: Sei R endlich, e sym. Idempotent bzgl. J

$\Rightarrow 1-e$ sym. bzgl. J.

Beweis: $R = eR \oplus (1-e)R \overset{\text{wg}}{\cong} e^J R \oplus (1-e^J)R$

e sym $\Rightarrow eR \cong e^J R$ als R-Rechtsmodul

$\Rightarrow (1-e)R \cong (1-e^J)R$

$\Uparrow$ Krull Remak Schmidt da R endl (s. Übung)

(6) Satz: Vor. wie bei (5). $C \leq V$ Code

$\Rightarrow e C^{\perp,\beta} = (eC)^{\perp,\beta_e}$.

Beweis "$\subseteq$" Sei $x \in C^\perp, y \in C$

$\Rightarrow \beta_e(ex, ey) = \beta(\underbrace{ex}_{\in C^\perp}, \underbrace{v_e y}_{\in C}) = 0$ also

$eC^{\perp,\beta} \subseteq (eC)^{\perp,\beta_e}$

ebenso: $(1-e)C^{\perp,\beta} \subseteq ((1-e)C)^{\perp,\beta_{1-e}}$

"$=$" folgt aus Ordnungsgründen:

$|C| = |eC| \cdot |(1-e)C|$

$|C^\perp| = |eC^\perp| \cdot |(1-e)C^\perp|$

$|V| = |C| \cdot |C^\perp|$, ~~$|eV| = 1$~~

$= |eV| \cdot |(1-e)V| = |eC| \cdot |(eC)^{\perp,\beta_e}| \, |(1-e)C| \, |((1-e)C)^{\perp,\beta_{1-e}}|$

$|C^\perp| = |(eC)^{\perp,\beta_e}| \cdot |((1-e)C)^{\perp,\beta_{1-e}}|$

$\Uparrow$ $=$

(5.7) Satz (Version der MacWilliams Identität)
Ver. wie bei (5.4)

$$\mathrm{fwe}(C^\perp) = \mathrm{fwe}\big((eC)^{\perp,\beta_e} \oplus (1-e)C^\perp\big)$$

$$= \frac{1}{|eC|} \sum_{v \in (1-e)C^\perp} \sum_{w \in eV} \underbrace{\sum_{u \in eC} \exp(2\pi i \beta_e(u,w))}_{= \begin{cases} |eC| & w \in (eC)^{\perp,\beta_C} \\ 0 & \text{sonst} \end{cases}} e_{w+(1-e)v}$$

Ist insbesondere $C = C^\perp$ so ist
$\mathrm{fwe}(C)$ invariant unter

$$e_v \mapsto \frac{1}{\sqrt{|K|V|}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e \cdot v))\, e_{(1-e)v+w}$$

Ist $C = C^\perp \leq V^N \Rightarrow \mathrm{cwe}(C)$ invariant unter

$$h_{e,u_e,v_e} : x_v \mapsto \frac{1}{|eV|^{1/2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v) \cdot x_{(1-e)v+w}$$

(5.8) Def: Sei (R, Π, Φ, ψ) Formring, $\varrho = (V, \varrho_\Pi, \varrho_\Phi, \beta)$ endl. Darst. Die zugehörige Clifford-Weil Gruppe ist

$$\mathcal{C}(\varrho) = \langle m_r, d_\phi, h_{e,u_e,v_e} \mid r \in R^*, \phi \in \Phi, u_e \cdot v_e = e, \; v_e \cdot u_e = e^{\gamma} \text{ sym. Bd. von } R \rangle$$

$$\leq GL_{|V|}(\mathbb{C}) \quad \text{wo}$$

$$m_r : x_v \mapsto x_{rv}, \quad d_\phi : x_v \mapsto \exp(2\pi i\, \varrho_\Phi(\phi)(v)) \quad (v \in V)$$

(5.9) Bem: $C = C^\perp$ isotroper selbstdualer Code in ϱ^N (Code vom Typ ϱ)
$\Rightarrow \mathrm{cwe}(C) \in \mathrm{Inv}(\mathcal{C}(\varrho))$ homogen, Grad N

Satz (Nebe, Rains, Sloane) R endl. direktes Prod. von Matrixringen über Kettenringen $\Rightarrow$

$$\mathrm{Inv}(\mathcal{C}(\varrho)) = \langle \mathrm{cwe}(C) \mid C \text{ vom Typ } \varrho \rangle$$