

6. Übung Codes und Invariantentheorie

Prof. Dr. G. Nebe

(WS 22/23)

Aufgabe 10. Voraussetzungen wie bei Aufgabe 8. Sei zusätzlich $\rho := (V, \rho_M, \rho_\Phi, \beta)$ eine (für (iii) endliche) Darstellung von (R, M, ψ, Φ) . Zeigen Sie, daß für alle $r \in R, x, y \in V$ gilt:

- (i) $\beta(y, rx) = \beta(x, r^J \epsilon y)$ insbesondere $\beta(y, x) = \beta(x, \epsilon y)$
- (ii) $\beta(rx, y) = \beta(x, r^J y)$
- (iii) Ist $e = u_e v_e$ ein symmetrisches Idempotent in R , so gilt

$$h_{e, u_e, v_e}^{-1} = h_{e, -\epsilon^{-1} u_e^J, -v_e^J \epsilon}.$$

Aufgabe 11. (Skalare Elemente in der Clifford-Weil Gruppe) Sei e ein symmetrisches Idempotent, $\phi \in \Phi$.

- (i) Das Element

$$H_{e, u_e, v_e} d((1, \phi)) = \left(\begin{pmatrix} 1 - e^J & v_e \\ -u_e & 1 - 2e \end{pmatrix}, \begin{pmatrix} 0 & -\psi(\epsilon e) \\ -\phi[-1] \end{pmatrix} \right)$$

der hyperbolischen co-unitären Gruppe hat Ordnung 3.

- (ii) $(h_{e, u_e, v_e} d_\phi)^3 \in \mathcal{C}(\rho)$ operiert als Skalarmultiplikation mit

$$\gamma_\rho(\phi) := |eV|^{-1/2} \sum_{v \in eV} \exp(2\pi i \rho_\Phi(\phi)(v)).$$

(Benutzen Sie Satz 6.14, dass die offensichtliche Abbildung von $\mathcal{U}(R, \Phi)$ nach $\mathcal{C}(\rho)$ eine projektive Darstellung ist.)

- (iii) Sei $q = p^f \equiv 3 \pmod{4}$ und $R(q^E) := (R, M, \psi, \Phi) = (\mathbf{F}_q, \mathbf{F}_q, \text{id}, \mathbf{F}_q)$ der Form Ring mit $\tau := \text{id}$, $\mathfrak{F} := \text{id}$ und $\lambda := \text{id}$ und $\rho(q^E) := (V, \rho_M, \rho_\Phi, \beta)$ die Darstellung von $R(q^E)$ mit $V = \mathbf{F}_q$,

$$\rho_M(a)(x, y) = \frac{1}{p} \text{Tr}(axy)$$

für alle $a \in M = \mathbf{F}_q$, $x, y \in V = \mathbf{F}_q$ wo Tr die Spur von \mathbf{F}_q nach \mathbf{F}_p bezeichnet.

Berechnen Sie $\gamma_\rho(\phi)$ aus (ii) für den Fall $e = \text{diag}(1, 0, \dots, 0) \in \mathbf{F}_q^{n \times n}$
 $\phi = \text{diag}(u, 0, \dots, 0)$ wo $u \in \mathbf{F}_q$ mit $\text{Tr}(u) = 1$.

Folgern Sie, dass die Länge eines selbstdualen Codes über \mathbf{F}_q durch 4 teilbar ist, wenn $q \equiv 3 \pmod{4}$.