103. On Certain Numerical Invariants of Mappings over Finite Fields. III

By Takashi ONO
Department of Mathematics, Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1980)

Introduction. This is again a continuation of my two preceding papers*) [3]. We shall be concerned with algebras with involution and Hopf maps.

§ 1. Algebras with involution. Let $K=F_q$ (q : odd) and let A be an associative algebra with involution α. (See [1] for basic facts on such algebras). Take an invertible element $\theta \in A$ such that

(1.1) $\theta^\alpha = \varepsilon\theta, \qquad \varepsilon = \pm 1$

and consider the mapping $F: A \to A$ given by

(1.2) $F(x) = x^\alpha \theta x, \qquad x \in A.$

Clearly, F is a quadratic mapping of the underlying vector space of A into itself. In this section, we shall determine invariants ρ_F, σ_F for this mapping when the algebra (A, α) is simple. Since all finite division rings are commutative, there are 4 types of such algebras, up to the change of ground fields:

(i) $A = K_r \oplus K_r, \quad (x, y)^\alpha = ({}^t y, {}^t x), \quad \tau(x, y) = \mathrm{tr}\,(x) + \mathrm{tr}\,(y),$

(ii) $A = K_r, \quad x^\alpha = S^{-1}\,{}^t x S, \quad {}^t S = S, \quad \tau(x) = \mathrm{tr}\,(x),$

(iii) $A = K_{2s}, \quad x^\alpha = J^{-1}\,{}^t x J, \quad J = \begin{pmatrix} 0 & 1_s \\ -1_s & 0 \end{pmatrix}, \quad \tau(x) = \mathrm{tr}\,(x),$

(iv) $A = L_r, \quad L = F_{q^2}, \quad x^\alpha = S^{-1}\,{}^t \bar{x} S, \quad {}^t \bar{S} = S, \quad \tau(x) = \mathrm{tr}\,(x) + \overline{\mathrm{tr}\,(x)}.$

(Here τ means the reduced trace of the algebra A over K, $\mathrm{tr}\,(x)$ means the trace of the matrix x and the bar means the conjugation of the quadratic extension L/K.) Note that the trace has the properties:

(1.3) $\tau(x^\alpha) = \tau(x)$, $\tau(xy) = \tau(yx)$, the mapping $(x, y) \mapsto \tau(x, y)$ is a non-degenerate symmetric bilinear form on A.

Therefore, to each $\lambda \in A^*$, the dual space of A, there corresponds uniquely an element $a = a_\lambda \in A$ such that $\lambda(x) = \tau(ax)$. Conversely, any $a \in A$ defines a linear form $\lambda = \lambda_a$ by $\lambda(x) = \tau(ax)$. We have

(1.4) $F_\lambda(x) = \lambda(F(x)) = \tau(a x^\alpha \theta x).$

Put

(1.5) $\langle x, y \rangle_\lambda = \dfrac{1}{2}(F_\lambda(x+y) - F_\lambda(x) - F_\lambda(y)).$

Then, we have

---

*) As in my former paper (II), (I. 2.3) will mean (2.3) in (I).