80. On Certain Numerical Invariants of Mappings over Finite Fields. I

By Takashi ONO

Department of Mathematics, Johns Hopkins University

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

Introduction. Let X be a finite set, Y be a vector space over a finite field $K=F_q$ and F be a mapping $X\to Y$. Using a non-trivial multiplicative character χ of K, we shall define invariants $\rho_F(\chi)$ and $\sigma_F(\chi)$, and prove a simple relation (1.11) between them. If $\dim Y=1$, then $\rho_F(\chi)$ is nothing but the square of the absolute value of the character sum

$$S_F(\chi)=\sum_{x\in X}\chi(F(x)).$$

When X is also a vector space over K, F is a quadratic mapping and χ is a quadratic character, then the computation of $\sigma_F(\chi)$ is generally much easier than that of $\rho_F(\chi)$.*) On the other hand, when the degree of a polynomial mapping F is higher than 2, then, even in the case of the quadratic character, $\sigma_F(\chi)$ involves usually difficult ingredients such as the trace of the Frobenius endomorphism; however, there are cases where $\rho_F(\chi)$ can be computed easily. In such a case, we can use the equality (1.11) to get some informations about the ingredients of $\sigma_F(\chi)$. We shall discuss here a simple example of this type.

§ 1. Statement of a theorem. Let K be the finite field with q elements: $K=F_q$ and χ be a non-trivial character of the multiplicative group $K^\times$ of K. We extend χ to K by putting $\chi(0)=0$. Let X be a finite set, Y be a vector space over K of finite dimension $m\geqq 1$ and F be any mapping $X\to Y$. For non-zero vectors $u, v\in Y$, we write $u\|v$ when they are propotional to each other, i.e. when there is an $a\in K^\times$ such that $v=au$. When that is so, we write $a=v:u$. Hence, we have $(u:v)(v:u)=1$ and $\chi(u:v)=\bar{\chi}(v:u)$ where $\bar{\chi}$ is the complex conjugate of χ. Denote by P the set of pairs $(x, y)\in X^2$ such that $F(x)\neq 0$, $F(y)\neq 0$ and $F(x)\|F(y)$. In this paper, we shall be interested in the number

(1.1) $\rho_F(\chi)=\sum_{(x,y)\in P}\chi(F(x):F(y)).$

(1.2) **Remark.** When P is empty, i.e. when $F(x)=0$ for all $x\in X$, we simply put $\rho_F(\chi)=0$.

(1.3) **Remark.** $\rho_F(\chi)$ is an invariant in the sense that, for another

*) In the second paper of the same title as this one, we shall obtain explicit values of the invariants for quadratic mappings arising from pairs of quadratic forms, algebras with involution, Hopf maps, etc.