CHAPTER I

INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field of q elements, with q being a power of the prime p. A permutation polynomial (over $\mathbb{F}_q$), abbreviated as PP, is a polynomial which is a bijection of $\mathbb{F}_q$ onto itself. The problem of finding necessary and/or sufficient conditions for permutation polynomials has been a subject of numerous investigations, see e.g. [1, 2, 3, 4, 5, 6, 7]. The best known and most used criterion is due to Hermite, see e.g. Theorem 7.4 of [4], which states that $f(x) \in \mathbb{F}_q[x]$ is a PP if and only if the following two conditions hold:

(i) f has exactly one root in $\mathbb{F}_q$;

(ii) for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q-2$.

In a number of situations, it is necessary to consider not only PP's but its natural generalization, referred to here as *quasi-permutation polynomial*, abbreviated by QPP, which we now define.

Let S and T be two nonempty subsets of $\mathbb{F}_q$ with the same number of elements $s = |S| = |T|$; this terminology will be kept fixed throughout the entire thesis. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called an (S,T)-*quasi-permutation polynomial*, abbreviated by (S,T)QPP or simply QPP if both S and T are left understood, if $\{P(c); c \in S\} = T$. When $S = T = \mathbb{F}_q$, then $P(x)$ is the usual PP. Without imposing any structure on the sets S and T, it seems hardly possible to extract any useful information about QPP's. It is thus surprising that a quite general criterion for QPP can be derived irrespective of what the sets S and T are and this is carried out in Chapter III. Yet, most anticipated results are valid only when subjected to certain structures of the sets S and T. Note also that merely imposing the structure of being a group under multiplication on either S or T

already forces it to contain its multiplicative inverse because each nonzero element $\alpha \in \mathbb{F}_q$ satisfies $\alpha^{q-1} = 1$. Therefore, imposing too many structures on either the set S or T, such as being a ring would turn it into a field, which is never considered here as it is a part of the PP's situation.

In the next chapter, we collect definitions and results, mainly without proof, to be used in the later chapter and gather basic properties of QPP. In Chapter III, general criteria for a polynomial to be a QPP are derived and characterizations of QPP's using the concept of characters are proved. In Chapter IV, other types of QPP's, such as linearized polynomials, monomials and binomails are found, while Chapter V deals with counting the number of QPP's of a fixed degree. The final chapter concludes with all important results of QPP's in which we derive on this thesis.