# NORMAL SUBSETS OF FINITE GROUPS[1]

BY

Ernst Snapper

## Introduction

$G$ stands for a finite group of order $g$. If $T$ is a non-empty subset of $G$ and $n$ a rational integer, we denote the solution set of the equation $x^n \epsilon T$ by $S(T, n)$; i.e.,

$$S(T, n) = \{\sigma \mid \sigma \epsilon G, \sigma^n \epsilon T\}.$$

The absolute value sign $|T|$, $|S(T, n)|$, etc., indicates the number of elements in the set inside the sign. We refer to the following theorem as "the Frobenius theorem": *If $C$ is a class of conjugate elements of $G$, $|S(C, n)|$ is divisible by* $(|C|n, g)$. See [2, page 136], for an elegant proof of this theorem; the notation $S(T, n)$ is taken from the same source. (Square brackets refer to the references.)

The solution set $S(C, n)$ is closed under inner automorphism of $G$, i.e., it is a *normal subset* of $G$. Consequently, the Frobenius theorem gives information about the number of elements in certain normal subsets of the group. In the present paper, we obtain information about the size of many other normal subsets of $G$, most of which have nothing to do with solving equations.

The main tool is Theorem 1.1 of [4], reviewed in Section 1. It enables us to associate a numerical polynomial with many a normal subset of $G$ (Sections 2, 3); and this polynomial gives the information about the size of that set (Section 4). In Section 5, we discuss the connection with the Frobenius theorem.

## 1. Review of [4]

A permutation representation $(G, D)$ of $G$ consists of a finite, non-empty set $D$ on which $G$ acts on the left. The unit element of $G$ is unit operator and, if $\rho, \sigma \epsilon G$ and $d \epsilon D$, $(\rho\sigma)d = \rho(\sigma d)$. We introduce a variable $x_i$ for each divisor $i$ of $g$, and consider the polynomial ring $R$ in these variables with rational numbers as coefficients. (Divisor always means *positive* divisor, and $g = |G|$.) An element $\sigma \epsilon G$ gives rise to a permutation of the set $D$, and hence to the partitioning of $D$ into the cycles of that permutation. We refer to these cycles also as the cycles of $\sigma$. The monomial $M(\sigma) \in R$ of $\sigma$ is defined as $\prod_{[g]} x_i^{c_i(\sigma)}$; the product $\prod_{[g]}$ is taken over the set $[g]$ of all divisors $i$ of $g$, and $c_i(\sigma)$ is the number of cycles of $\sigma$ whose length is $i$. We observe that every cycle of $\sigma$ has a length which divides the order of $\sigma$, and

Received June 5, 1967.

[1] This research was supported in part by a National Science Foundation grant.