THE CYCLOTOMY OF FINITE COMMUTATIVE P.I.R.'s

BY
PHILIP C. KUTZKO[1]

Introduction

In recent years the term "cyclotomy" has been used to refer to various structures bearing only formal resemblance to the structure of nth division points on the circle whence the term derives [3], [7], [15]. Thus there is discussion of the cyclotomy of finite fields [9] or of "Galois Domains" [15] or even of Kloosterman or hyper-Kloosterman sums [11], [12]. It is the purpose of this paper to provide a unified theory of cyclotomy which will include the examples given above as special cases.

Following an approach used by Hall [9] we discuss in Sections 1–3 the conjugacy class structure and representations of finite split metabelian groups and under certain restrictions describe a certain duality between the classes and representations. In Section 4 we consider the group which is the split extension of the additive group of a finite commutative principal ideal ring by its group of units, the action being that of multiplication, and by applying the theory developed in Sections 1–3 are able to define generalized cyclotomic classes, periods, and numbers for the ring in question. In Section 5 we utilize the theory of finite dimensional Fourier transforms to generalize the classical Gauss and Jacobi sums and prove appropriate theorems concerning them. In Section 6.1 and Section 6.2 we compute the cyclotomy of a finite field and of a "Galois Domain" and show that our definitions coincide with those usually given. Finally, in Section 6.3, we show that by considering the cyclotomy of the ring which is a direct sum of n-copies of a given finite field we may determine the "cyclotomic" properties of Kloosterman and hyper-Kloosterman sums alluded to in [11] and [12].

We assume throughout a knowledge of the elementary properties of complex characters such as may be found in Chapter 1 of [5].

1. Preliminaries

All groups discussed will be finite and all characters will be complex. Unless otherwise noted, A will denote a multiplicatively written abelian group and G will denote a multiplicatively written abelian group of automorphisms of A.

Received October 16, 1973.

[1] The author was partially supported by a National Science Foundation grant. The author wishes to thank the University of Maine, Farmington, for providing him with an office for part of the summer of 1973.