ENUMERATION THEOREMS IN INFINITE ABELIAN GROUPS

by

Delmar L. Boyer
A. B., Kansas Wesleyan University, 1949
M. A., University of Kansas, 1952

Submitted to the Department of Mathematics and the Faculty of the Graduate School of the University of Kansas in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Advisory Committee:

Redacted Signature

Redacted Signature

Redacted Signature

Redacted Signature

July, 1955

Preface

This paper has been written while the author was a Research Assistant on the project supported by the National Science Foundation through Research Grant NSF-G1126. Thus this paper will appear both as report number 2 of this project and as a thesis submitted to the Graduate School of the University of Kansas in partial fulfillment of the requirements for the Ph.D. degree.

The author would like to express his gratitude to the National Science Foundation for their support. He would also like to express his deep gratitude for the kindly help and many suggestions offered by his thesis advisor, Professor William R. Scott, during the course of this work. In particular, the proof of lemma 2.1 is due to Professor Scott.

D. L. Boyer

TABLE OF CONTENTS

Preface i

Introduction 1

Chapter 1. Preliminaries 3

Chapter 2. Subgroups of a Countable Abelian Group 11

Chapter 3. Submodules of Modules 20

Chapter 4. The Order of the Automorphism Group 25

ENUMERATION THEOREMS IN INFINITE ABELIAN GROUPS

INTRODUCTION W. R. Scott has proved, [6, theorem 9][1], that if G is an Abelian group of order $A > \aleph_0$, then G has 2^A subgroups of order A and the intersection of all these subgroups is the identity. The present paper gives a partial extension of this theorem in one direction, and an extension of the theorem in another direction.

Firstly, in chapter 2, the case where G is a countable Abelian group is considered and a partial extension of the above-mentioned theorem is made by characterizing those countable Abelian groups that have a countable number of subgroups and by showing that all others have $2^{\aleph_0}$ subgroups. Secondly, in chapter 3, the above-mentioned theorem is extended to modules over a principal ideal ring[2] with a restriction on the order of the ring.

In chapter 4 the problem of determining the order of the automorphism group of an infinite Abelian group is considered and it is proved that the order of the automorphism group of a countable torsion Abelian group is $2^{\aleph_0}$.

The first chapter of this paper contains the necessary definitions and theorems which are well-known. They have been taken mainly from [4] and they have been listed, without proofs, for the convenience of the reader.

Hereafter when the word <u>group</u> is used it will mean an Abelian group unless it is used in the phrase <u>automorphism group</u> or unless the contrary is explicitly stated. The additive notation will be employed. In the

---

1. References of this type are to the bibliography.
2. cf. article 1.1.

statement of the theorems H. stands for hypothesis and C. stands for conclusion.

CHAPTER 1

PRELIMINARIES

ARTICLE 1.1 DEFINITIONS

A group is said to be a torsion group if every element has finite order. If every element has infinite order the group is said to be torsion-free. A group in which the order of each element is a power of a fixed prime p is called a primary group or a p-group. An element x of a group is said to be divisible by the integer n if there is some element y in the group such that ny = x. A group is said to be divisible[1] if every element of the group is divisible by every integer. A group is said to be reduced[2] if it contains no non-trivial subgroups which are divisible groups. A group is said to be free if it is a weak direct sum of infinite cyclic groups. A subgroup of a group is said to be inextensible[3] if g is in the subgroup whenever ng is, n being an integer. Since the intersection of a set of inextensible subgroups is inextensible, the intersection of all the inextensible subgroups containing a given set of elements of a group is an inextensible subgroup. This subgroup is said to be the extension of that set of elements.

Let S be a principal ideal ring, i.e. an integral domain in which every ideal is principal. Then a group M is said to be an S-module (or simply a module if no misunderstanding can arise) if there is a product λx defined for λ in S and x in M which satisfies

---

1. For the form of all divisible groups cf. theorem 1.3.
2. For an example of a reduced group cf. [4, remark (b), page 31] .
3. Notice that an inextensible subgroup contains the torsion subgroup.

$$\lambda(x + y) = \lambda x + \lambda y$$

$$(\lambda + \mu)x = \lambda x + \mu x$$

$$(\lambda\mu)x = \lambda(\mu x)$$

$$1 \cdot x = x.$$

A subset N of an S-module M is said to be a submodule of M if N is a subgroup of M which satisfies $\lambda S \subseteq S$ for every λ in S. An S-module C is said to be cyclic if C = Sx for some x in C. The order ideal of an element x of an S-module is that ideal of S which consists of all λ in S such that $\lambda x = O$. The collection of all elements of a module M that have a nonzero order ideal forms a submodule T which is said to be the torsion submodule of M. M is said to be a torsion module if T = M, and M is said to be torsion-free if T = O. An S-module M is said to be a primary module or a p-module if some power of the prime p, an element of S, belongs to the order ideal of each element of M. A module M is said to be of bounded order if the intersection of the order ideals of every element of M is nonzero.

ARTICLE 1.2 NOTATION

Throughout this paper we shall use the following notation: C_n will denote a cyclic group of order n. R^+ will denote the additive group of rational numbers. $Z(p^\infty)$ will denote the quotient group P/Z, where P is the the subgroup of R^+ whose denominators are powers of a fixed prime p, and Z is the additive group of integers. o (S) will denote the cardinal number of the set S. R(A) will denote the extension of the set A of elements of a group. s(G) will denote the number of subgroups (submodules) of the group (module) G. d will denote the cardinal $\aleph_0$. $A \cup B$ and $A \cap B$ will denote the set theoretic union and intersection, respectively. A + B will denote the group theoretic union and $A \oplus B$ will denote the direct sum. $\sum_{\alpha} \oplus A_{\alpha}$ will denote the weak direct sum of the groups (modules) A_{α}, and $\sum_{\alpha} \theta A_{\alpha}$ will denote the strong direct sum of the groups (modules) A_{α}. Hereafter, the words direct sum will mean the weak direct sum. A(G) will denote the automorphism group of G.

ARTICLE 1.3. THEOREMS

The following theorems are proved in [4]. For the history of these theorems see the Guide to the Literature, pages 73-80, of [4]. Although the theorems are stated for groups, they are valid for modules over a principal ideal ring, and we shall refer to them for both groups and modules.

THEOREM 1.1 H. G is a torsion group.

C. G is a unique direct sum of primary groups.

THEOREM 1.2 H. G is a group.

C. (i) G has a largest divisible subgroup, D.

(ii) $G = D \oplus R$, where R is reduced.

THEOREM 1.3 H. G is a divisible group.

C. G is a direct sum of groups each isomorphic to R^{+} or to $Z(p^{\infty})$, for various primes, p.

THEOREM 1.4 H. G is a reduced, torsion group,

C. G has a finite cyclic direct summand.

THEOREM 1.5 H. H is a subgroup of a free group, G.

C. H is a free group with at most as many summands as G.

THEOREM 1.6 H. G is a group of bounded order.

C. G is the direct sum of cyclic groups.

ARTICLE 1.4 REMARKS

(1) The extension R(A) of a set A of elements in a group G is the set G' of all g in G such that some integral multiple of g can be written as a linear combination of elements from A.

Proof: Let g be an element of G', then $ng = a_{\alpha_1} x_{\alpha_1} + \cdots + a_{\alpha_r} x_{\alpha_r}$, x_{α_i} an element of A and n and the a_{α_i} are integers. Hence ng is in every subgroup containing A. In particular, ng is in R(A). Since R(A) is inextensible, g is also in R(A). Thus $G' \subset R(A)$.

Clearly, G' is a subgroup of G, and if ng is in G', then $(mn)g = m(ng) = a_{\alpha_1} x_{\alpha_1} + \cdots + a_{\alpha_r} x_{\alpha_r}$. Thus g is in G' and we have shown that G' is inextensible. Since $A \subset G'$, this means $R(A) \subset G'$, which proves (1).

(2) If B is the free group generated by a maximal set β of linearly independent elements in a group G then G / B is torsion.

Proof: For every g in G there is an integer n such that ng is a linear combination of the elements of β, for otherwise β would not be maximal. Hence ng is in B and G / B is torsion.

(3) If G is a free group with r cyclic summands, where $r < d$, then G has a countable number of subgroups.

Proof: By theorem 1.5 any subgroup of G will have at most r generators. But there are only d sets of elements of G that have exactly n elements, where n is any positive integer less than or equal to r. Hence $s(G) \leq d$. Also, since $o(G) = d$, $s(G) \geq d$. This proves (3).

(4) If R is a subgroup of R^+, then R has a countable number of subgroups if only a finite number of primes occur in the denominators of elements of R and R has 2^d subgroups otherwise.

Proof: This is an immediate consequence of [1, theorem 2, corollary 1]

(5) A subgroup R of R^+ is cyclic if and only if only a finite number of primes occur in the denominators of elements of R and each prime that occurs in the denominators has only a finite number of powers occurring in the denominators.

Proof: This is a restatement of [1, theorem 2, corollary 2]

(6) The number of subgroups in the direct sum $Z(p^\infty) \oplus Z(p^\infty)$ is 2^d.

Proof: Each of the sequences of elements: $(1/p, i/p)$, $i = 0, 1,$ $p - 1$; $(1/p^2, (i + jp)/p^2)$, $j = 0, 1,$ $p - 1$; $(1/p^3, (i + jp + kp^2)/p^3)$, $k = 0, 1, \cdots, p - 1$; generates a distinct subgroup and there are 2^d such sequences.

(7) If M is an S-module and S if a field, then $M = \sum_\alpha \oplus S_\alpha$, $S_\alpha \cong S$ for all α.

Proof: This is the well-known statement that every vector space has a Hamel basis.

(8) If $n < 3$ or p is odd, then the automorphism group of C_{p^n} is $C_{(p-1)p^{n-1}}$. For $n > 2$ the automorphism group of C_{2^n} is $C_{2^{n-2}} \oplus C_2$.

Proof: This is a statement of the results of paragraph 5, pages 115-116 of [8] .

(9) The automorphism group of a direct sum of groups $\sum_\alpha \oplus G_\alpha$ contains a subgroup which is isomorphic to the strong direct sum, $\sum_\alpha \oplus A(G_\alpha)$ of the automorphism groups of the summands.

Proof: This follows from the fact that under the definition $(\cdots, g_\alpha, \cdots) V = (\cdots, g_\alpha T_\alpha, \cdots)$, T_α in $A(G_\alpha)$, V is an automorphism of $\sum_\alpha \oplus G_\alpha$.

(10) The order of the automorphism group of the group $Z(p^\infty)$ is 2^d.

Proof: An automorphism of $Z(p^\infty)$ is given by a sequence of correspondences,

$$1/p \longrightarrow h/p;\ o \neq h < p$$
$$1/p^2 \longrightarrow k/p^2;\ k < p^2,\ k \equiv h(p)$$

Further, such a sequence can be obtained in 2^d ways, which proves (10).

ARTICLE 1.5 BACKGROUND FOR CHAPTER 4.

In this article a brief outline of the discussion and lemma given in article 11 of [4] will be given. This outline will be needed for chapter 4.

Let G be a countable, reduced p-group. Let $G_o = G$. For any ordinal α let $G_{\alpha+1} = pG_\alpha$, and for limit ordinals α let $G_\alpha = \bigcap_{\beta<\alpha} G_\beta$.

Since there will finally be an ordinal λ such that $G_\lambda = G_{\lambda+1}$, i.e. such that $G_\lambda = p\,G_\lambda$, G_λ is divisible. Hence, since G is reduced, $G_\lambda = 0$. Let P be the set of elements of G which are of order p. For any subgroup S of G let $S_\alpha = S \cap G_\alpha$. Since the quotient group $P_\alpha / P_{\alpha+1}$ may be regarded as a vector space over the integers mod p, it has a dimension which will be denoted by $f(\alpha)$. $f(\alpha)$ will be called the <u>αth Ulm invariant</u> of G.

For the elements of G let the <u>height</u>, $h(x)$, of the element $x \neq 0$ be α if x is in G_α but not in $G_{\alpha+1}$. Let $h(0) = \lambda + 1$. Now $h(x)$ has the following properties:

$$\text{if } h(x) < h(y), \text{ then } h(x+y) = h(x).$$

$$(1.5.1) \qquad \text{if } h(x) = h(y), \text{ then } h(x+y) \geqq h(x).$$

$$\text{if } x \neq 0, \text{ then } h(px) > h(x).$$

An element x of G will be called <u>proper</u> with respect to the subgroup S of G if $h(x) \geqq h(x+s)$ for every s in S.

Let S be any subgroup of G and let α be any ordinal. Let $S_\alpha^* = S_\alpha = S_\alpha \cap p^{-1} G_{\alpha+2}$ where $p^{-1} G_{\alpha+2}$ is the set of all z such that pz is in $G_{\alpha+2}$. Now for any x in S_α^*, there is a y in $G_{\alpha+1}$ such that $px = py$, and y may be changed by any element in $P_{\alpha+1}$. The mapping $x \longrightarrow x - y$, followed by the natural homomorphism from P_α to $P_\alpha / P_{\alpha+1}$ is a homomorphism of S_α^* into $P_\alpha / P_{\alpha+1}$, and the kernel is $S_{\alpha+1}$. Hence this defines an isomorphism U of $S_\alpha^* / S_{\alpha+1}$ into $P_\alpha / P_{\alpha+1}$.

We now restate lemma 13 of [4] as follows:

LEMMA 1.1 H. U is the mapping just defined.

C. The following two statements are equivalent:

(a) The range of U is not all of $P_{\alpha} / P_{\alpha+1}$.

(b) There exists in P_{α} an element of height α that is proper with respect to S.

CHAPTER 2

SUBGROUPS OF A COUNTABLE ABELIAN GROUP

This chapter will be devoted to characterizing those countable groups G with $s(G) = d$ and showing that otherwise $s(G) = 2^d$.

ARTICLE 2.1 THE THEOREM

We first prove the following lemma for a group G that is not necessarily abelian:

LEMMA 2.1 H. H is a finite, normal subgroup of G,

$s(G/H) = A \geqq d$.

C. $s(G) = A$.

Proof: Since each subgroup of G/H is associated with a subgroup of G, $s(G) \geqq A$. Assume $s(G) > A$ and let $\{K_a\}$ be the subgroups of G. Notice first that there is some $G_1 \subset G$ such that $H + K_a = G_1$ for more than A of the K_a; for otherwise, since $s(G/H) = A$, there would be only A of the K_a. Notice also that H is normal in G_1 and s $s(G_1/H) \leqq s(G/H) = A$. Since H is finite and $H + K_a = G_1$, $i_{G_1}(K_a) < d$. Hence for each K_a, there exists an $N_a \subset K_a$ such that N_a is normal in G_1 and $i_{G_1}(N_a) < d$. Hence there are only a finite number of K_a such that $N_a \subset K_a \subset G_1$, i.e. only a finite number of the K_a can correspond to a given N_a. Hence there are more than A of the N_a.

Now there is a subgroup $G_2 \subset G_1$ and a subgroup $H_1 \subset H$ such that $H + N_a = G_2$ and $H \cap N_a = H_1$ for more than A of the N_a, for otherwise there would be at most A of the N_α. Also notice that H_1 is normal in G_2. The situation is now as follows:

(i) H / H_1 is finite.

(ii) H / H_1 is normal in G_2 / H_1, since H is normal in G_2.

(iii) $(G_2/ H_1) / (H / H_1) \cong G_2 / H$ and $s(G_2 / H) \leqq A$.

(iv) $(N_\alpha / H_1) + (H / H_1) = G_2 / H_1$ and $(N_\alpha / H_1) \cap (H / H_1) = H_1 / H_1$ for more than A of the N_α, hence

$i_{G_2 / H_1}(N_\alpha / H_1) < d$.

For a fixed α, let $P_\beta / H_1 = (N_\alpha / H_1) \cap (N_\beta / H_1)$. Hence $i_{G_2 / H_1}(P_\beta / H_1) \leqq i_{G_2 / H_1}(N_\alpha / H_1) \cdot i_{G_2 / H_1}(N_\beta / H_1) < d$. Since $P_\beta / H_1 \subset N_\beta / H_1 \subset G_2 / H_1$ for every β, since there are more than A of the N_β, and since there are only a finite number of N_β / H_1 between a given P_β / H_1 and G_2 / H_1, there are more than A of the P_β. Hence $s(N_\alpha / H_1) > A$, since there are more than A of the P_β / H_1 such that $P_\beta / H_1 \subset N_\alpha / H_1$. But by (iii) and (iv) $N_\alpha / H_1 \cong (G_2 / H_1) / (H / H_1) \cong G_2 / H$ and $s(G_2 / H) \leqq A$, which is a contradiction. Hence $s(G) = A$.

Next the question will be settled for torsion groups as follows:

LEMMA 2.2 H. G is a countable torsion group.

C. (i) $s(G) = d$ if $G = Z(p_1^\infty) \oplus \cdots \oplus Z(p_n^\infty) \oplus F$, where $p_i \neq p_j$ for $i \neq j$ and F is finite.[1]

(ii) $s(G) = 2^d$ otherwise.

---

1. Hereafter the form of G given in C. (i) will be called countable form.

Proof: By theorem 1.2, $G = D \oplus R$, with D divisible and R reduced. Consider the following two cases:

case 1. R is countable. By theorem 1.1 R is the direct sum of primary groups. If there are d summands of R then $s(G) = 2^d$ since the direct sum of any collection of the summands forms a subgroup. If $R = R_{p_1} \oplus \cdots \oplus R_{p_n}$, where the R_{p_i} are primary with respect to the prime p_i, then at least one summand, say R_p, is countable since R is countable. By theorem 1.4 $R_p = C_{n_1} \oplus R'_p$; again by theorem 1.4 $R'_p = C_{n_2} \oplus R''_p$. Continuing in this way we get a sequence of finite cyclic groups $\{C_{n_i}\}$ such that no C_{n_i} is contained in the direct sum of any of the others. Hence the direct sum of any subcollection of these cyclic groups forms a subgroup of G and $s(G) = 2^d$. Thus it has been proved that if R is countable, then $s(G) = 2^d$.

case 2. R is finite. By theorem 1.3, $D = Z(p_1^{\infty}) \oplus \cdots \oplus Z(p_n^{\infty}) \oplus \cdots$, where by remark (6) if $p_i = p_j$ for $i \neq j$, then $s(G) = 2^d$. If there are d summands of D then by the reason used twice in case 1 $s(G) = 2^d$. Otherwise $D = Z(p_1^{\infty}) \oplus \cdots \oplus Z(p_n^{\infty})$ and G has countable form. This proves (ii).

Now assume G has countable form. Then by theorem 1.1 $G = Z(p_1^{\infty}) \oplus F_{p_1} \oplus \cdots \oplus Z(p_n^{\infty}) \oplus F_{p_n} \oplus F_{p_{n+1}} \oplus \ldots \oplus F_{p_m}$, where F_{p_i} is the primary subgroup of F with respect to p_i. If H is any subgroup of G, by theorem 1.1, $H = H_{p_1} \oplus \ldots \oplus H_{p_m}$ Hence $H_{p_i} \subset Z(p_i^{\infty}) \oplus F_{p_i}$ for $i = 1, \cdots, n$ and $H_{p_i} \subset F_{p_i}$ for $i = n+1, \cdots, m$. If K is any subgroup of $Z(p^{\infty}) \oplus F_p$ then $K / (K \cap Z(p^{\infty})) \cong (K + Z(p^{\infty})) / Z(p^{\infty}) \subset (Z(p^{\infty}) \oplus F_p) / Z(p^{\infty}) \cong F_p$. Hence $i_K (K \cap Z(p^{\infty})) \leqq o(F_p) < d$ and thus K admits the coset decomposition $K = (K \cap Z(p^{\infty}))\, g_1 \cup \cdots \cup (K \cap Z(p^{\infty}))\, g_r$.

Since $Z(p^{\infty})$ is countable and $s(Z(p^{\infty})) = d$, $K \cap Z(p^{\infty})$ and $g_1, \cdots, g_r$ can be obtained in at most d ways. Hence $Z(p^{\infty}) \oplus F_p$ has d subgroups, and, since $s(G) = s(Z(p_1^{\infty}) \oplus F_{p_1}) \cdot \cdots \cdot s(Z(p_n^{\infty}) \oplus F_{p_n}) \cdot s(F_{p_{n+1}}) \cdot \cdots \cdot s(F_{p_m})$, it follows that $s(G) = d$. This completes the proof.

Now for the general case let $\mathcal{B}$ be a maximal set of linearly independent elements in the countable group G and let B be the free group generated by the elements of $\mathcal{B}$. With this notation we prove the following theorem:

THEOREM 2.1 H. G is a countable group.

C. (i) $s(G) = d$ if $o(\mathcal{B}) < d$ and G/B has countable form.

(ii) $s(G) = 2^d$ otherwise.

Proof: If $o(\mathcal{B}) = d$, then $s(G) = 2^d$ since any two distinct subsets of $\mathcal{B}$ generate distinct subgroups of G. By remark (2) G/B is torsion, hence lemma 2.2 implies $s(G) = 2^d$ if G/B does not have countable form. This proves (ii).

Conversely, assume $o(\mathcal{B}) < d$ and G/B has countable form. Let H be any subgroup of G such that $H \not\subset B$ and $B \not\subset H$. Now consider $R(H \cap B)$. By remark (1) $R(H \cap B)/H \cap B$ is torsion. Also, since for every g in G, there is some integer m such that mg is in B, $R(H \cap B)/(R(H \cap B) \cap B)$ is torsion. However, $R(H \cap B)/(R(H \cap B) \cap B) \cong (R(H \cap B) + B)/B \subset G/B$; hence $s(R(H \cap B)/(R(H \cap B) \cap B)) \leq d$. Since B is free, it follows from theorem 1.5 that $R(H \cap B) \cap B$ and $H \cap B$ are also free groups. Now, since for each generator g_i of $R(H \cap B) \cap B$ there is an integer n_i such that $n_i g_i$ is in $H \cap B$, there are only a finite number of cosets of of $H \cap B$ in $R(H \cap B) \cap B$, i.e. $(R(H \cap B) \cap B) / (H \cap B)$ is finite. Further, $(R(H \cap B) / (H \cap B)) / ((R(H \cap B) \cap B) / (H \cap B)) \cong R(H \cap B) / (R(H \cap B) \cap B)$, which has at most d subgroups. Hence, by lemma 2.1, $s(R(H \cap B) / (H \cap B)) \leqq d$. For any h in H, nh is in B for some integer n; hence nh is in $H \cap B$ and this implies, by remark (1), that h is in $R(H \cap B)$. Thus $H \cap B \subset H \subset R(H \cap B)$. Thus it has been proved that for each subgroup B' of B there are at most d subgroups H of G such that $H \cap B = B'$. Since, by remark (3), B has d subgroups, it follows that $s(G) \leqq d$. Also, since G is countable, $s(G) \geqq d$. Hence $s(G) = d$, which was to be proved.

ARTICLE 2.2 EXAMPLE

One may be tempted to conjecture that if $o(\mathfrak{B}) < d$ and $s(G) = d$, where G is a countable group, then G is a direct sum of rational groups, i.e. subgroups of R^+ or R^+ / Z, where Z is the additive group of integers. However, this conjecture is defeated by the following example, which is a modification of the example given in the proof of theorem 19 of [4] .

Let u and v be two symbols, let p be a prime, and let G be the group of all finite linear combinations over the integers of the expressions v, w_1 / p, w_2 / p^3, $\cdots$, $w_n / p^{((n-1)/2)(n+2)+1}$, $\cdots$ where $w_n = u + (1 + p^2 + p^5 + \cdots + p^{((n-1)/2)(n+2)})v$. Let H be the subgroup generated by u and v. Now u and v form a maximal linearly independent set of elements in G; and it is clear by the association, $(w_1/p) + H \longleftrightarrow 1/p$; $(w_2/p^2) + H \longleftrightarrow 1/p^2$; $(w_2/p^3) + H \longleftrightarrow 1/p^3$;——;——; $(w_3/p^6) + H \longleftrightarrow 1/p^6$; $\cdots$, that $G/H = Z(p^\infty)$. Hence by theorem 2.1, $s(G) = d$.

Observe the following properties of G:

1) v / p is not in G.

Proof: Assume v / p is in G. Then $p(v / p) = v$, i.e.

$$p(a_0 v + a_1 w_{n_1} / p^{\beta(n_1) + 1} + \cdots + a_r w_{n_r} / p^{\beta(n_r) + 1}) = v, \text{ where}$$

$n_1 < \cdots < n_r$, n_r is minimal, and $\beta(n) = ((n - 1) / 2)(n + 2)$. Multiplying by $p^{\beta(n_r)}$ gives $au + bv = 0$. Hence $a = 0$, i.e. $p^{\beta(n_r) - \beta(n_1)} a_1 + p^{\beta(n_r) - \beta(n_2)} a_2 + \cdots + a_r = 0$. Now if $r = 0$ or $r = 1$, then $pa_0 = 1$. Hence $r \geqq 2$ and it follows that $p^{\beta(n_r) - \beta(n_{r-1})} \mid a_r$. Hence

$$a_r w_{n_r} / p^{\beta(n_r) + 1} = a_r' w_{n_{r-1}} / p^{\beta(n_{r-1}) + 1} + a_r' p^z v, \text{ which}$$

contradicts the minimality of n_r. Hence v / p is not in G.

2) No element of G is divisible of q^a for every a with $q \nmid p$, q a prime.

Proof: Assume the element g is divisible by q^a for every a, i.e. for every a there is a g' such that $q^a g' = g$; or, expressed more fully,

$$(1) \quad q^a(a_0 v + a_1 w_{n_1} / p^{\beta(n_1) + 1} + \cdots + a_r w_{n_r} / p^{\beta(n_r) + 1}) =$$
$$b_0 v + b_1 w_{m_1} / p^{\beta(m_1) + 1} + \cdots + b_s w_{m_s} / p^{\beta(m_s) + 1}.$$

Now, if $n_r \geqq m_s$, by multiplying both sides of (1) by $p^{\beta(n_r) + 1}$ and equating the coefficients of u on both sides, it follows that

$$(2) \quad q^a(a_1 p^{\beta(n_r) - \beta(n_1)} + \cdots + a_r) = p^{\beta(n_r) - \beta(m_s)} (b_1 p^{\beta(m_s) - \beta(m_1)} + \cdots + b_s).$$

If $n_r < m_s$, by multiplying both sides of (1) by $p^{\beta(m_s)+1}$ and equating the coefficients of u on both sides, it follows that

$$(3) \quad q^{\alpha}(a_1 p^{\beta(m_s) - \beta(n_1)} + \cdots + a_r) = (b_1 p^{\beta(m_s) - \beta(m_1)} + \cdots + b_s).$$

Hence it must be that $q^{\alpha} \mid (b_1 p^{\beta(m_s) - \beta(m_1)} + \cdots + b_s)$ for all α, which is impossible unless $b_1 = b_2 = \cdots = b_s = 0$, in which case, by (1), $q^{\alpha} \mid b_o$ for all α, a contradiction.

3) No element of G is divisible by all powers of p.

Proof:[1] Assume there is an element g of G which is divisible by all powers of p. Let $g = a_0 v + a_1 w_{n_1} / p^{\beta(n_1)+1} + \cdots + a_r w_{n_r} / p^{\beta(n_r)+1}$. Thus $g = (au + bv) / p^{\beta(n_r)+1}$. Since g is divisible by all powers of p, so is au + bv. In particular, au + bv is divisible by $p^{\beta(n)+1}$ for every n, i.e. $(au + bv) / p^{\beta(n)+1}$ is in G for every n. Hence $(au + bv) / p^{\beta(n)+1} - aw_n / p^{\beta(n)+1} = ((b - a(1 + p^2 + \cdots + p^{\beta(n)})) / p^{\beta(n)+1}) \cdot v$ is in G for every n. Hence, by 1), it must be that

$$(4) \quad b - a(1 + p^2 + \cdots + p^{\beta(n)}) \equiv 0 \pmod{p^{\beta(n)+1}}, \text{ for every } n.$$

It will be shown that there is no pair of integers a and b such that (4) is satisfied for every n. Assume there is such a pair.

---

1. Computations will be made in the group Ra(u) ⊕ Ra(v) where Ra(x) is the group of all rational multiples of x.

Then $b = a(1 + p^2 + \cdots + p^{\beta(n)}) + a_n p^{\beta(n) + 1}$ and $b = a(1 + p^2 + \cdots + p^{\beta(n - 1)}) + a_{n - 1} p^{\beta(n - 1) + 1}$. Subtracting the second equation from the first, we obtain $p^{\beta(n - 1) + 1}(ap^{n - 1} + a_n p^n - a_{n - 1}) = 0$, since $\beta(n) = \beta(n - 1) + n$. Hence $p^{n - 1} \mid a_{n - 1}$ and it is seen that the sharpened congruence

$$(5) \quad b - a(1 + p^2 + \cdots + p^{\beta(n)}) \equiv 0 \pmod{p^{\beta(n + 1)}}$$

must be satisfied for all n. But if n is chosen such that $p^n > |a| + |b|$, it follows that $p^{\beta(n + 1)} = p^n \cdot p^{\beta(n) + 1} > (|a| + |b|) \cdot p^{\beta(n) + 1} > (|a| + |b|)((p^{\beta(n) + 1} - 1) / (p - 1)) = (|a| + |b|)(1 + p + p^2 + \cdots + p^{\beta(n)}) > |b| + |a| (1 + p^2 + p^5 + \cdots + p^{\beta(n)}) \geqq |b - a(1 + p^2 + \cdots + p^{\beta(n)})|$, which proves that the congruence (5) is not possible for all n unless $b - a(1 + p^2 + \cdots + p^{\beta(n)}) = 0$ for all n, which would imply $(1 + p^2 + \cdots + p^{\beta(n)}) \mid b$ for all n, a contradiction. This proves 3).

Assume G is a direct sum of rational groups, i.e. subgroups of R^+, since G is torsion-free. Also, since $\{u, v\}$ is a maximal linearly independent set of elements, and since the number of elements is the same for every such set, G must be the direct sum of two rational groups. Further, since $s(G) = d$, it follows from remark (4) that the denominators of each summand can have only a finite number of primes. Also by 2), 3), and remark (5), together with the fact that if no element of a subgroup of R^+ is divisible by all powers of a prime, then the denominators of that subgroup have only a finite number of powers of that prime, it follows that the summands are cyclic. Hence G is free with two summands and by theorem 1.5 and the definition of H, H is also free with two summands. Hence G/H is finite, which contradicts the fact that $G/H \cong Z(p^{\infty})$. Thus G can not be a direct sum of rational groups.

The problem of determining the number of subgroups of a finite group was solved simultaneously by Yeh, [7] , and Delsarte, [2] , and later by Kinosita [5] .

CHAPTER 4

SUBMODULES OF MODULES

In this chapter [6, theorem 9] will be extended to modules over a principal ideal ring with the restriction that the order of the ring is less than the order of the module. The proofs are made by translating the proofs in [6] into module language.

Let M be a module over a principal ideal ring, S.

DEFINITION 3.1[1] $L(p^r)$ is the set of all elements in M whose order ideals contain p^r

$L(\infty)$ is the set of all elements in M whose order ideals contain only zero.

Clearly, $L(p^r)$ is a submodule of M.

LEMMA 3.1 H. M is a primary module with respect to the prime, p.

C. $o(L(p^r)) \leqq o(L(p^{r-1}))\cdot o(L(p)) \leqq (o(L(p)))^r$, $r = 1, 2,$

Proof: If $pg_1 = pg_2$, then $p(g_1 - g_2) = o$; and if $p(g_1 - g_2) = pg_1 - pg_2 = 0$, then $pg_1 = pg_2$, where g_1 and g_2 are elements of M. Hence if g is in M, the number of solutions of $px = g$ is less than or equal to $o(L(p))$. Thus the number of x in M such that px is in $L(p^{r-1})$ is at most $o(L(p^{r-1}))(o(L(p)))$, i.e. $o(L(p^r)) \leqq o(L(p^{r-1}))\cdot o(L(p))$. For the second inequality, the first inequality and induction is used to get

---

1. Here p is a prime in S.

$o(L(p^{r-1}))\cdot o(L(p)) \leqq o(L(p^{r-2}))\cdot (o(L(p)))^2 \leqq \cdots \leqq (o(L(p)))^r.$

COROLLARY H. M is a p-module.

$o(M) > d.$

C. $o(L(p)) = o(M).$

Proof: If $o(L(p))$ is finite, then by the lemma $o(L(p^r)) \leqq (o(L(p)))^r$ which is finite for all r. Hence $o(M) \leqq d$. Hence $o(L(p)) \geqq d$ and it follows that $o(M) \leqq \sum_{i=1}^{\infty} o(L(p^i)) \leqq o(L(p)) + o(L(p)) + \cdots = o(L(p))$. Hence $o(M) = o(L(p))$.

Now let R be the set of submodules M_β of M with $o(M_\beta) = o(M)$ and let D be the intersection of all the submodules of R. With this notation the following lemma is proved:

LEMMA 3.2 H. M is a module over a principal ideal ring, S.

$\sum_\alpha \oplus H_\alpha \subset M$, $\alpha \in U$; $o(U) = o(M) \geqq d$.

C. (i) $o(R) = 2^{o(M)}$.

(ii) $D = e$.

Proof: Since there are $2^{o(M)}$ subsets of M, $o(R) \leqq 2^{o(M)}$. Next it is shown that there are $2^{o(M)}$ subsets U' of U of order $o(M)$. Assume there are less than $2^{o(M)}$. Then there are $2^{o(M)}$ subsets of order less than $o(M)$. But the complement of each of these is of order $o(M)$, a contradiction. Hence there are $2^{o(M)}$ subsets U' of U of order $o(M)$. Now let $N(U') = \sum_{\alpha \in U'} \oplus H_\alpha$. Then $o(N(U')) = o(M)$, and if $U' \neq U''$ then

$N(U') \neq N(U'')$. Hence $o(R) = 2^{o(M)}$. Also $D \subset \cap N(U') = e$, which proves the lemma.

The main result of this chapter is the following theorem:

THEOREM 3.1 H. M is a module over the principal ideal ring S.

$o(M) \geq d$; $o(S) < o(M)$.

R is the set of submodules M_β of M with

$o(M_\beta) = o(M)$.

D is the intersection of all the submodules of R.

C. (i) $o(R) = 2^{o(M)}$.

(ii) $D = e$.

Proof: If $o(M) = d$, then o(S) is finite and S is a field. Hence by remark (7) $M = \sum_{\alpha \in U} \oplus S_\alpha$, $S_\alpha \cong S$. Since $o(M) = d$, $o(U) = d$. Hence by lemma 3.2, the theorem follows.

Hence it may be assumed that $o(M) > d$. Now let T be the torsion submodule of M. The following two cases are considered:

case 1. $o(T) < o(M)$. In this case $o(L(\infty)) = o(M)$. Let $\mathfrak{B}$ be a maximal set of linearly independent elements, and let B be the module generated by the elements of $\mathfrak{B}$. It will be shown that $o(\mathfrak{B}) = o(L(\infty))$. Assume $o(\mathfrak{B}) < o(L(\infty))$. Then[1] $o(B) \leq o(\mathfrak{B}) \cdot o(S) < o(L(\infty)) = o(M)$. For a fixed $\lambda \neq o$ in S, let $\lambda x = \lambda y$, then $\lambda(x - y) = o$. Hence $x - y$ is in T. Thus there are at most o(T) solutions of $\lambda x = b$ for fixed λ in S and fixed b in B. Therefore the number of x's for which λx is in B, allowing λ to vary, is $o(T) \cdot o(S) \cdot o(B) < o(M)$. Hence there is an x in $L(\infty) - B$ such

---

1. For $o(\mathfrak{B})$ and o(S) both finite, the first inequality is not true, but in this case $o(B) < o(L(\infty)$ since $o(L(\infty))$ is infinite and o(B) is finite.

that $\mathcal{B} \cup \{x\}$ is an independent set, which contradicts the maximality of $\mathcal{B}$. Thus $o(\mathcal{B}) = o(L(\infty)) = o(M)$, and the theorem follows from lemma 3.2 since B is of the form $\sum_{\alpha} \oplus H_{\alpha}$.

case 2. $o(T) = o(M)$. From theorem 1.1, $T = \sum_{p \in S} \oplus T_p$, where the T_p are primary modules.

case 2.1. $o(T_p) = o(T)$ for some p. Then by the corollary of lemma 3.1, $o(L(p)) = o(M)$. Now by theorem 1.6, $L(p) = \sum \oplus C_{\alpha}$, C_{α} cyclic. However, $o(C_{\alpha}) \leqq o(S) < o(M)$; hence there are $o(M)$ of the C_{α} and by lemma 3.2 the theorem follows.

case 2.2 $o(T_p) < o(T)$ for all p. Let $U = \sum \oplus T_{p_i}$ for all primes p_i with $o(T_{p_i}) > d$. Now the number of elements of U with one nonzero component is $\sum o(T_{p_i})$. The number of elements of U with two nonzero components is $\sum o(T_{p_i}) \cdot \sum{}' o(T_{p_i}) = \sum o(T_{p_i})$ where $\sum{}'$ denotes the sum $\sum$ with some one summand omitted. Continuing in this way we see that the number of elements of U with n nonzero components is $\sum o(T_{p_i})$ for every n. Hence $o(U) = \sum o(T_{p_i})$. Also $o(U) = o(T)$ for clearly $o(U) \leqq o(T)$ and $o(U) < o(T)$ implies $o(W) = o(T)$ where $W = \sum \oplus T'_{p_i}$ for all primes p_i with $o(T'_{p_i}) \leqq d$. But this is impossible since there are at most $o(S) < o(T)$ of the T'_{p_i}. Now by case 2.1 each of the T_{p_i} has $2^{o(T_{p_i})}$ submodules H(i) of order $o(T_{p_i})$. For each i, choose an $H(i) \subset T_{p_i}$ with $o(H(i)) = o(T_{p_i})$. Then $V = \sum \oplus H(i)$ is a submodule of U with $o(V) = o(U)$. The number of submodules formed in this way is clearly $\prod 2^{o(T_{p_i})} = 2^{\sum o(T_{p_i})} = 2^{o(U)} = 2^{o(M)}$. Also since $\bigcap H(i) = e$ for a fixed i, the intersection of all the V's is the identity. This proves the theorem.

COROLLARY H. $o(G) > d$ and G is a group.

R is the set of subgroups G_a of G with $o(G_a) = o(G)$.

D is the intersection of the groups in R.

C. (i) $o(R) = 2^{o(G)}$.

(ii) $D = e$.

This is the statement of [6, theorem 9] .

Proof: A group is a module over the ring of integers by means of the multiplication already defined, i. e. $ng = g + g + \cdots + g$, with n summands. Also since $o(G) > d$, the condition on the order of the ring is satisfied. Hence the corollary follows from theorem 3.1.

CHAPTER 4

THE ORDER OF THE AUTOMORPHISM GROUP

In this chapter it will be shown that the order of the automorphism group of a countable torsion group is 2^d. The foundation laid in article 1.5 will be built on to attain this goal.

ARTICLE 4.1 THE THEOREM

First a lemma will be proved which is patterned after the proof of Ulm's theorem in [4] However, here automorphisms are being considered and since it is desired to obtain 2^d automorphisms, they will be built up step by step such that all but at most one step can be taken in two ways.

LEMMA 4.1 H. G is a countable, reduced, p-group.

S and T are finite subgroups of G.

V is an isomorphism of S onto T which preserves heights with respect to G.

x is an element of G such that x is not in S but px is in S.

$h(x) = \alpha \leqq \lambda - 2$[1].

S' is the subgroup generated by S and x.

x is proper with respect to S.

h(px) is maximal among all x's that are proper with respect to S.

---

1. λ is as in article 1.5.

C. There exist finite subgroups $T' \supset T$ and $T'' \supset T$ and height-preserving isomorphisms, V' of S' onto T' and V'' of S' onto T'', such that $V' \neq V''$ and V' and V'' are extensions of V.

Proof: Let $(px)V = z$. Now two elements, w and w_1, that are not in T must be found such that $pw = pw_1 = z$, $h(w) = h(w_1) = \alpha$, w and w_1 are proper with respect to T, and $w \neq w_1$. If such elements can be found, then the conclusion can be obtained by defining $(s + rx)V' = sV + rw$ and $(s + rx)V'' = sV + rw_1$.

In searching for the elements w and w_1 the following two cases are considered:

case 1. $h(z) = \alpha + 1$. Hence $z \neq 0$ and consequently $px \neq 0$. Since $h(z) = \alpha + 1$, z is in $G_{\alpha + 1}$; therefore there exists an element w in G_α such that $pw = z$. Since $P_{\alpha + 1} \neq 0$, there is a nonzero element w' of $P_{\alpha + 1}$, which is a subgroup of G_α. Hence $p(w + w') = pw + 0 = z$. Also notice that w is not in $P_{\alpha + 1}$, since $z \neq 0$; hence $w \neq w'$.

It is now claimed that the elements w and $w_1 = w + w'$ satisfy the requirements. First notice that $h(w) \geq \alpha$ and $h(w_1) \geq \alpha$ since w and w_1 are in G_α. To see that $h(w) = \alpha$ assume $h(w) > \alpha$. Hence $h(w) \geq \alpha + 1$, which implies $h(z) = h(pw) > h(w) \geq \alpha + 1$, a contradiction. Hence $h(w) = \alpha$. Exactly the same argument shows $h(w_1) = \alpha$. Next it is shown that w is not in T. Assume w is in T. Now $w = yV$, y in S. Hence $pw = (py)V = z$. But $(px)V = z$; therefore $px = py$. Also $x - y$ is not in S for if it were then x would be also. Since x is proper with respect to S, $\alpha = h(x) \geq h(x - y)$. Also, since $h(y) = h(w) = \alpha$, $h(x - y) \geq h(x) = \alpha$; hence $h(x - y) = \alpha$ and $x - y$ is proper with respect to S. However, $h(p(x - y)) = h(o) > \alpha + 1$, which contradicts the maximality of $h(px)$.

Thus w is not in T. As before exactly the same argument works to show that w_1 is not in T. All that remains to be shown is that w and w_1 are proper with respect to T. To this end assume w is not proper with respect to T, i.e. there exists a t in T such that $h(w + t) \geq \alpha + 1$, $t = sV$, s is in S. Notice that $h(p(w + t)) \geq \alpha + 2$. Since $(px)V = z = pw$ and $(ps)V = pt$, it follows that $(px + ps)V = pw + pt$. Therefore $h(p(w + t)) = h(p(x + s)) \geq \alpha + 2$. Since $h(t) < \alpha$ implies $h(w + t) < \alpha$ we have $h(t) \geq \alpha$. Therefore $h(s) = h(t) \geq \alpha$ and $h(x + s) \geq \alpha$, but $h(x + s) \leq \alpha$. Hence $h(x + s) = \alpha$, i.e. $x + s$ is proper with respect to S and $h(p(x + s)) \geq \alpha + 2$ which contradicts the maximality of h(px). Therefore w is proper with respect to T. Again the same argument shows that w_1 is proper with respect to T. Thus w and w_1 satisfy the requirements and V' and V'' can be obtained as described above.

case 2. $h(z) > \alpha + 1$. Hence $h(px) > \alpha + 1$, which implies $px = pv$, where v is in $G_{\alpha + 1}$. Hence $x - v$ is in P_α. Since x is not in $G_{\alpha + 1}$, neither is $x - v$; therefore $h(x - v) = \alpha$. Since for every s in S, $h(x + s) \leq \alpha$, and since $h(-v) \geq \alpha + 1$, it follows that $h(x + s) < h(-v)$ for every s in S. Therefore $h(x + s - v) = h(x + s) \leq \alpha$ and so $x - v$ is proper with respect to S. Now since S is finite, so is $S^*_\alpha / S_{\alpha + 1}$, and since $x - v$ satisfies (b) in lemma 1.1 it follows that the dimension[1] of $S^*_\alpha / S_{\alpha + 1}$ is less than $f(\alpha)$. Further, since V is height preserving, it maps S_α onto T_α, S^*_α onto T^*_α, and $S^*_\alpha / S_{\alpha + 1}$ onto $T^*_\alpha / T_{\alpha + 1}$; hence the dimension of $T^*_\alpha / T_{\alpha + 1}$ is less than $f(\alpha)$. Hence lemma 1.1, (a), is satisfied for T and therefore there is an element w' such that $pw' = o$, $h(w') = \alpha$, and w' is proper with respect to T. Also since $h(z) > \alpha + 1$, there there is an element w'' in $G_{\alpha + 1}$ such that $pw'' = z$. Now let $w = w' + w''$

---

1. As a vector space over the integers (mod p).

and it follows that $pw = z$ and $h(w) = h(w' + w'') = h(w') = \alpha$, since $h(w') < h(w'')$. Further, for any t in T, $h(w' + t) \leqq h(w') = \alpha$ and $h(w'') \geqq \alpha + 1$; therefore $h(w' + t + w'') = h(w' + t) \leqq \alpha = h(w' + w'')$ and $w' + w''$ is proper with respect to T. Now let $w''' \neq 0$ be any element of $P_{\alpha + 1}$ and let $w_1 = w + w'''$. (Notice that if $z = 0$, it will suffice to let $w = w'$ and $w_1 = w' + w''$). Now $w \neq w_1$ and $pw_1 = pw = z$. Also $h(w_1) = h(w + w''') = h(w) = \alpha$ since $h(w) < h(w''')$. Finally, since w is proper with respect to T, for any t in T it follows that $h(w + t) \leqq h(w) = \alpha$, and since $h(w''') \geqq \alpha + 1$, $h(w + t + w''') = h(w + t) \leqq \alpha = h(w_1)$. Therefore w_1 is proper with respect to T and this concludes the proof of lemma 4.1.

THEOREM 4.1 H. G is a countable, torsion group.

C. $o(A(G)) = 2^d$.

Proof: Clearly, $o(A(G)) \leqq 2^d$. By theorem 1.2, $G = D \oplus R$. If $D \neq 0$ then by theorem 1.3 D is a direct sum of $Z(p^\infty)$ groups. In this case the theorem follows from remarks (9) and (10). Hence the only case remaining to be considered is the one in which G = R. By theorem 1.1, R is a direct sum of primary groups, and if there are d primary summands of R, then by theorem 1.4 each summand has a finite cyclic direct summand. In this case the theorem follows from remarks (8) and (9). The only case remaining to be considered is the one in which R is the direct sum of a finite number of primary groups. In this case there will be a prime p such that the order of the corresponding primary group is d. Hence it must be shown that if R_p is a countable reduced p-group, then the order of the automorphism group of R_p is 2^d.

To this end first order the elements of R_p in some order, o, g_1, g_2, $\cdots$. Let S = T be the cyclic subgroup generated by g_1 and let V be the identity correspondence. V will be extended by induction to an automorphism of R_p. At the (2n - 1)th stage S will be extended to include g_n and at the 2nth stage T will be extended to include g_n. Moreover it will be shown that the extension can be made in two distinct ways at all but at most one stage. This will show that V can be extended to an automorphism of R_p in 2^d ways. Since all of the arguments required for the induction are the same as the one for extending S, say, to include g_2, only this argument will be given.

If g_2 is in S, there is nothing to prove. If not then the order of g_2 is p^n, i.e. $p^n g_2 = o$. Let r be the smallest positive integer such that $p^{r+1} g_2$ is in S, but $p^r g_2$ is not in S. Now S will be extended to include $p^r g_2$. Clearly, it will suffice to extend S to include $p^r g_2 + s_i$, where s_i is in S. Let $p^r g_2 + s$ be such that $p^r g_2 + s$ is proper with respect to S and let $h(p(p^r g_2 + s))$ be maximal among all $p^r g_2 + s_i$ which are proper with respect to S. This is possible since S is finite. Now assuming $h(p^r g_2 + s) \leqq \lambda - 2$, S can be extended to include $p^r g_2 + s$, and hence to include $p^r g_2$, by using lemma 4.1. Continuing by induction S can be extended to include $p^{r-1} g_2$, $p^{r-2} g_2$, $\cdots$, pg_2, and finally g_2 itself, making the extension in two ways at each stage provided the heights of the elements involved are all at most $\lambda - 2$.

Thus it has been seen that the only thing that could possibly hinder the extension at any given stage is to have to extend to include an element x which satisfies all the hypotheses of lemma 4.1 except $h(x) \leqq \lambda - 2$, i.e. x is such that $h(x) = \lambda - 1$. In this case px = o and hence z = o. Now since $P_{\lambda - 1} \neq 0$, w can be taken as any element in $P_{\lambda - 1}$ such that w is not in T. This will fail only if $P_{\lambda - 1} \subset T$, but this implies $o(P_{\lambda - 1})$ is finite and hence $P_{\lambda - 1} \subset S$ also since V is height-preserving. However, x is in $P_{\lambda - 1}$, and hence x is in S, a contradiction. Therefore $P_{\lambda - 1} \not\subset T$ and w may be taken as any element of $P_{\lambda - 1}$ that is not in T. Also w may be changed by any nonzero element of $P_{\lambda - 1}$ and it will still satisfy the requirements. Hence the only case in which the extension can be made in only one way is when $h(x) = \lambda - 1$ and $P_{\lambda - 1} = C_2$. Thus the required extension can be made in two distinct ways at all but at most one stage, which proves that the order of the automorphism group of R_p is 2^d. Now the proof of theorem 4.1 is completed by invoking remark (9).

The problem considered in this chapter has not been solved for finite groups. It has been shown however, [3] , that if p^{n+1} divides $o(G)$, where p is a prime, then $p^n(p - 1)$ divides the order of the automorphism group of G where G is a finite group.

ARTICLE 4.2 UNSOLVED PROBLEMS

The author has been unable to solve the problem of determining the number of submodules of a module over a principal ideal ring where the order of the ring is equal to the order of the module. He has also been unable to determine the order of the automorphism group of a general group. It is his opinion that the answers to these questions are not as simple as the answers given to the questions in chapters 3 and 4 of the present paper.

Bibliography

Beaumont, R. A. and Zuckerman, H. S.

1. "A characterization of the subgroups of the additive rationals." Pacific Journal of Mathematics Vol. 1 (1951) pp. 169-177.

Delsarte, S.

2. "Fonctions de Möbius sur les groupes abeliens finis." Annals of Mathematics (2) Vol. 49 (1948) pp. 600-609.

Hilton, H.

3. "On the order of the group of automorphisms of an Abelian group." Messenger of Mathematics (2) Vol. 38 (1909) pp. 132-134.

Kaplansky, Irving.

4. Infinite Abelian groups. University of Michigan Press, Ann Arbor, 1954.

Kinosita, Yosihisa.

5. "On an enumeration of certain subgroups of a p-group." Journal of the Osaka Institute of Science and Technology (Kinki University) Part 1. Mathematics and Physics Vol. 1 (1949) pp. 13-20.

Scott, W. R.

6. "Groups and cardinal numbers." American Journal of Mathematics Vol. 74 No. 1 (1952) pp. 187-197.

Yeh, Yenchien

7. "On prime power Abelian groups." Bulletin of the American Mathematical Society Vol. 54 (1948) pp. 323-327.

Zassenhaus, Hans

8. The Theory of Groups. Chelsea, New York, 1949.